# 5

# Physical-Layer Attacks in Transparent Optical Networks

Marija Furdek and Nina Skorin-Kapov
*University of Zagreb*
*Croatia*

## 1. Introduction

For the past decades, network traffic has been showing immense growth trends, as we are witnessing the rapid development of network applications such as Internet Protocol TV (IPTV), peer-to-peer traffic, grid computing, multi-player gaming etc. Optical fiber, with its huge capacity of up to 50 THz, low bit error rate of $10^{-12}$, low loss of 0.2 dB/km and low noise and interference characteristics has been widely accepted as a viable future-proof solution to meet the ever-increasing network bandwidth demands. In comparison with the available fiber capacity, the speed of edge electronic equipment of only a few Gb/s creates a bottleneck, so fiber bandwidth is divided into independent wavelength sets, each capable of carrying traffic between a pair of nodes at different speeds. This is the underlying principle of Wavelength Division Multiplexing (WDM), where different wavelengths supporting communication between different end users are multiplexed and carried simultaneously over the same physical fiber. Under normal operating conditions, carried wavelengths do not significantly interfere with each other inside the fiber. At the receiver's side, they are demultiplexed or filtered to ensure that every receiver receives the intended wavelength. An illustration of WDM principle is shown in figure 1.

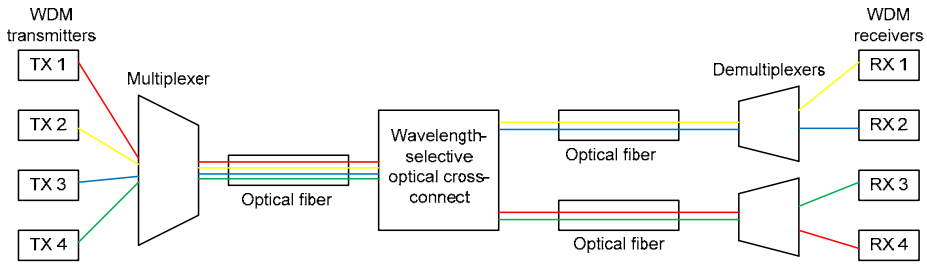



Fig. 1. Example of a simple WDM system.

In Transparent Optical Networks (TONs), signals do not undergo optical-electronical-optical (OEO) conversion at the intermediate nodes they traverse. Communication takes place entirely in the optical domain, via all-optical channels called lightpaths. The process of establishing lightpaths consists of finding a physical route and assigning a wavelength to

each of them, called Routing and Wavelength Assignment (RWA). The set of established lightpaths then comprises a so-called virtual topology over the given physical topology. Intermediate nodes perform wavelength-switching without regenerating or even interpreting the carried signals. Namely, full 3R (re-amplification, re-shaping, re-timing) signal regeneration in the optical domain is still in the experimental phase. Therefore, optical signals can only be re-amplified (1R) in the optical domain, while re-shaping and re-timing require OEO conversion. We are currently witnessing the evolution of optical networking from opaque networks with all-electronic switching, implying OEO conversion at every node, to transparent networks with all-optical switching and no OEO conversions at intermediate nodes. Networks in which most of the nodes are transparent and some of them are strategically equipped with 2R and/or 3R regenerators to improve the quality of analog optical signals are called translucent (Shen & Tucker, 2007).

The absence of lightpath regeneration in transparent optical networks not only provides signal transparency to bit rates, protocols and modulation formats but also reduces the costs and energy consumption associated with OEO conversion. However, transparency introduces significant changes to the security paradigm of optical networks by allowing signals whose characteristics fall out of the protocol-specific bounds or component working ranges to propagate through the network undetected. This creates a security vulnerability which can be exploited by a malevolent user to perform deliberate attacks aimed at degrading the proper functioning of the network. Due to the high data rates and latency employed in back-bone optical networks, even sporadic attacks of short duration can cause large data and revenue losses.

Section 2 gives an overview of different types and methods of physical-layer attacks in TONs, along with experimental evaluation of some of the vulnerabilities of network components that can be exploited by malicious users. Section 3 gives an overview of the current issues and trends in attack management and control in TONs, as well as some methods and guidelines for increasing network resilience to attacks. Finally, Section 4 concludes this chapter.

## 2. TON vulnerabilities to physical-layer attacks

The high data rates employed by TONs make them extremely sensitive to communication failures, whether they result from component malfunctions caused by external factors or fatigue, or from deliberate attacks. However, the differences between component faults and deliberate attacks make their consequences and recovery scenarios fundamentally different. Namely, disruption caused by component faults is restricted to the connections passing through the affected component, so rerouting these connections using classical survivability mechanisms usually solves the problem until the component is replaced/fixed. On the other hand, attacks can propagate to many users and different parts of the network, significantly complicating their detection and localization. Furthermore, the traffic itself can be the source of attack so rerouting affected connections may even worsen the consequences of the attack, instead of alleviating them. Furthermore, attacks, unlike failures, may appear sporadically so as to avoid detection.

Overviews of various physical-layer attacks in TONs can be found in (Fok et al., 2011; Mas et al., 2005; Médard et al., 1997). An attacker can gain access to the physical network

components as a legitimate user (or impersonating one) or by otherwise breaching into the network. The attacker may be an outsider or, equally likely, a person with inside access to the network facilities, according to (Richardson, 2008).

Depending on the intentions of the attacker, physical-layer attacks can be divided into two main groups:

a. Tapping attacks - aimed at gaining unauthorized access to data and using it for traffic analyses or eavesdropping purposes.
b. Service Disruption attacks - aimed at degrading the Quality of Service (QoS) or causing service denial.

Tapping attacks imply breaches in communication privacy and confidentiality. Occurrences of these attacks have been recorded in the past, e.g. in 2000 when three main trunk lines of the Deutsche Telekom network were breached at Frankfurt Airport in Germany or when an illegal eavesdropping device was discovered attached to Verizon's optical network in 2003 (Miller, 2007). The most likely purpose of these attacks was industrial espionage. Estimates indicate that only in the year 2000, corporate espionage cost US companies approximately $20 billion in purely technical means (Oyster Optics Inc., 2002).

The goal of service disruption attacks is to deteriorate the signal quality of legitimate communication channels. Depending on the severity of these attacks, their consequences may range from slight deterioration of the signal-to-noise ratio (SNR) to complete loss of service availability. They can also be aimed at manipulating communication by injecting false information or undermining the integrity of the transmitted data. Most commonly, these attacks are realized by injecting a malicious high-powered jamming signal which interferes with legitimate signals inside various network components. Methods of exploiting the vulnerabilities of the key building blocks of TONs (i.e. optical fibers, amplifiers and switches) to perform tapping and service disruption attacks are described in the following subsections.

### 2.1 Optical fibers

Optical fibers are immune to electromagnetic interference, which eliminates the possibility of eavesdropping through observation of side-channel effects, but, unless shielded, they are still susceptible to eavesdropping through other means. Namely, under normal operating conditions, light is kept inside the fiber core through total internal reflection, where the angle between the light beam and the core inner surface exceeds the critical angle and the beam is totally reflected back into the core. Bending the fiber violates the condition of total internal reflection of light inside the fiber core and causes part of the signal to be radiated out of the fiber, as shown in figure 2. If a photodetector is placed at the fiber bend, it can pick up such leakage and deliver the transmitted content to the intruder. Commercial tapping devices which introduce losses below 0.5 dB can be found on the market. There are also techniques which introduce losses below 0.1 dB, making such attacks extremely difficult to detect by network monitoring systems.

Some of these devices may cause a short interruption of service due to the necessity of cutting the fiber in order to install the device, after which the transmission is re-established. If this interruption is noticed, the technical personnel is quite likely to find the location of

the tap, making this method short-lived (Witcher, 2005). However, some eavesdropping devices can be clamped onto the fiber and create micro bends causing leakage without actually cutting the fiber. Retrieval and interpretation of tapped data may require more sophisticated methods, depending on the signal wavelength, polarization, modulation format and other characteristics, but a well equipped attacker should be able to overcome these obstacles.

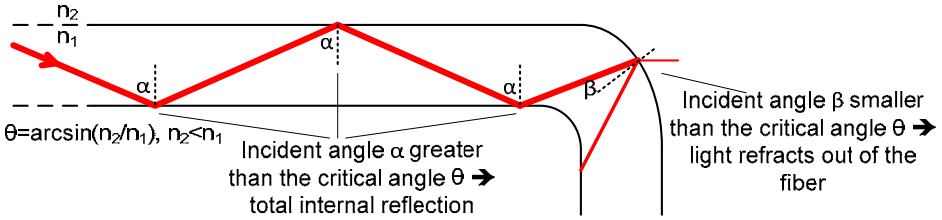



Fig. 2. Bending the fiber violates the conditions of total internal reflection and causes light to leak outside the fiber core.

Bending the fiber also enables a jamming signal to be inserted into the network. Under normal operating conditions, transmission effects in fibers are fairly linear, but high distances or high input powers increase the nonlinear effects among signals, of which four-wave mixing and cross-phase modulation are the most significant. A powerful jamming signal injected into the fiber enhances these effects and deteriorates the SNR of other signals. Due to the low attenuation of optical fibers, such a jamming signal can propagate from the entry point to other network components without losing its power and cause damage inside optical amplifiers and switches. This may be especially significant in new optical fiber access networks, where splitters and fibers are largely placed in public areas, with easy access to anyone.

### 2.2 Optical amplifiers

Erbium-doped fiber amplifiers (EDFAs) are the most commonly used optical amplifiers in today's WDM networks. They use an erbium-doped optical fiber core as gain medium to amplify optical signals. The energy of ionized erbium atoms can change between discrete levels. Atoms in lower energy levels have less energy and they can be raised to a higher level by absorbing an amount of energy equal to the difference between the two levels. Equivalently, a transition from a higher to a lower energy level results in the emission of a photon whose energy equals the difference between the two levels. In a normal state, the amount of erbium ions in the ground energy level is much higher than those in upper levels. To achieve amplification, the gain medium is pumped with an external source of energy which causes the number of ions in higher energy levels to exceed their number in lower levels, i.e. obtaining population inversion. When light of the appropriate frequency passes through such a medium, its photons stimulate the transition of excited electrons to lower energy levels, resulting in the stimulated emission of photons which have the same frequency, direction of propagation, phase and polarization as the incident photons. In this way, the incoming optical signal is amplified.

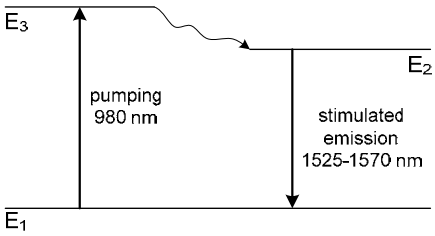



Fig. 3. Three energy levels of $Er^{3+}$ ions in silica glass for 980 nm pumping. Each discreet energy level represents a continuous energy band.

Figure 3 shows three energy levels – $E_1$, $E_2$ and $E_3$ of $Er^{3+}$ ions in silica glass. In reality, the energy levels shown here as discreet are spread into a continuous energy band. The energy difference between levels $E_1$ and $E_3$ corresponds to the energy of photons of light at 980 nm. When light at that wavelength is pumped into the erbium-doped fiber, its absorption causes the transition of ions from $E_1$ to $E_3$. Light at 1480 nm can also be used for pumping, but the pumping process is more efficient at 980 nm, resulting in a higher gain for the same pump power (Ramaswami & Sivarajan, 2002). The excited ions stay at the $E_3$ level for a very short time and then quickly transit to level $E_2$. The lifetime of the transition from level $E_2$ to $E_1$ is much longer, about 10 ms, and it is accompanied by the emission of photons on a wavelength between 1525 and 1570 nm. With pumping power high enough, the ions which fall back to level $E_1$ are quickly raised to $E_3$. The result of the synergy of these two processes is that most of the ions can be found at level $E_2$, i.e. population inversion between levels $E_2$ and $E_1$ is achieved. Under such conditions, light on wavelengths of 1525-1570 nm is amplified by stimulated emission from level $E_2$ to level $E_1$.

An optical amplifier is characterized by its gain, gain bandwidth, gain saturation, polarization sensitivity and amplifier noise (Mukherjee, 2006). The gain is defined as the ratio between the power of the signal at the output of the amplifier and its power at the input. Gain bandwidth specifies the frequency range over which the amplifier is effective. This parameter limits the number of wavelengths available in a network for a given channel spacing. Gain saturation is the value of output power after which an increase in input power no longer causes an increase in output power. It is usually defined as the output power at which there is a 3 dB reduction in the amplifier gain. Polarization sensitivity measures the difference in gain between two orthogonal polarizations of the dominant signal mode ($HE_{11}$ mode). The prevailing component of amplifier noise for EDFAs is Amplifier Spontaneous Emission (ASE), which arises from spontaneous transitions of ions from energy level $E_2$ to $E_1$, independent of any external radiation. Although the radiated photons have the same energy as the incoming optical signal, their frequency, phase, polarization and direction do not match.

EDFAs have several advantages over other types of optical amplifiers, such as Raman and semiconductor optical amplifiers. They provide high gain, are capable of simultaneous amplification of WDM signals independent of the light polarization state, have a low noise figure and low sensitivity to temperature (Laude, 2002). However, they also have drawbacks such as additional noise (ASE), dependency of gain on the spectrum and power of the incoming signal, and transients which occur when individual WDM channels are dropped.

If we consider each of the discrete energy levels in the doped fiber as a continuous energy band, then EDFAs are capable of simultaneously amplifying signals on several different wavelengths. As mentioned before, they most commonly amplify signals within the 1525-1570 nm wavelength range. However, due to the fact that the distribution of excited electrons is not uniform at various levels within a band, the gain of an EDFA depends on the wavelength of the incoming signal, with a peak around 1532 nm (Ramaswami & Sivarajan, 2002). This can be compensated for by employing passive or dynamic gain equalization (Bae et al., 2007; Laude, 2002). However, the limited number of available upper-state photons necessary for signal amplification must be divided among all incoming signals. Each of the signals is granted photons proportional to its power level, which can lead to so-called *gain competition*, where stronger incoming signals receive more gain, while weaker signals receive less. Due to the large number of input channels and high data rates employed in today's WDM networks, the dependency of EDFA gain assignment on the spectrum and power of the incoming signals can have a significant impact on network functioning.

Gain competition can be exploited to create service disruption as described in (Mas et al., 2005; Médard et al., 1998). In an *out-of-band jamming attack*, a malicious user injects a powerful signal (e.g. 20 dB above normal) on a wavelength different from those of other, legitimate signals, but still within the pass-band of the amplifier. The amplifier, unable to distinguish between the attacking signal and legitimate data signals, provides gain to each signal indiscriminately. The stronger, malicious signal will get more gain than the weaker, legitimate signals, robbing them of power. Thereby, the QoS level on the legitimate signals will deteriorate, potentially leading to service denial. Furthermore, the power of the attacking signal will have an additional increase downstream of the amplifier, allowing it to spread through other transparent nodes and affect other signals at their common EDFAs.

### 2.2.1 Laboratory assessment of gain competition

The impact of the jamming signal depends on its power level and wavelength. We tested this relation in laboratory setting (Furdek et al., 2010a) using two EXFO IQ-2600 tunable lasers sources, variable attenuators EXFO IQ-3100 to attenuate the signals and simulate losses in the optical fiber and an EDFA with 36 m of erbium-doped fiber Lucent Technologies HE-980 as the gain medium, pumped with a 980 nm pump signal from an Agilent FPL4812/C laser pump. One of the laser sources represented a legitimate signal with constant power (-25,51 dBm before entering the EDFA) and wavelength (1549,74 nm), while the other represented a powerful jamming signal with varying power and wavelength. Figure 4 shows the dependence of the amount of gain given to the legitimate signal on the power of the jamming signal on the next WDM channel, at 1549,05 nm. The power of the interfering signal was increased in 2 dB increments from the same level as the legitimate signal, until it was 20 dB stronger. The pump power was set to 40 mW. The measurements in figure 4 show how the amount of gain of the legitimate signal decreases in response to an increase in the power of the interfering signal. This is due to the fact that the interfering signal, as it becomes more powerful, consumes more and more upper-state photons in the EDFA, and thus robs the legitimate signal of gain.

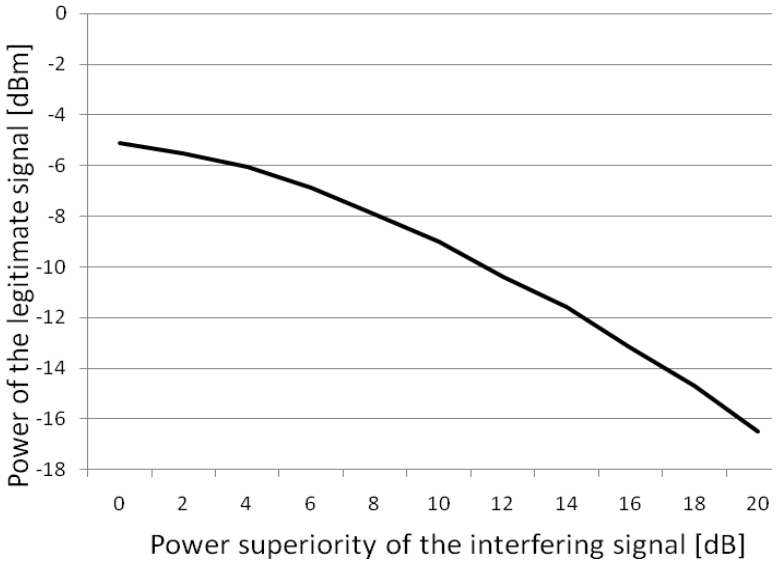



Fig. 4. The power of the legitimate signal at the output of the EDFA as a function of the power superiority of the interfering signal on the neighboring WDM channel, at 40 mW EDFA pumping power.

The gain of the legitimate signal also depends on variations in the wavelength of the interfering signal of constant, high power. Figure 5 shows this dependency for the legitimate signal at 1549,74 nm and a 20 dB stronger interfering signal whose nominal wavelength varies from 1530 nm to 1550 nm, in 5 nm increments. The influence of different operating points of the EDFA on the output power of the legitimate signal in this scenario was investigated by changing the pump power from 40 mW to 80 mW. In figure 5, *P_legit* denotes the power of the legitimate signal, and *P_interfering* the power of the interfering signal at the EDFA output. Power levels measured for pump powers of 40 mW and 80 mW have suffixes *_40mWpump* and *_80mWpump*, respectively. From figure 5, it can be seen that the amount of gain robbed from the legitimate signal by the high-powered jamming signal increases as their wavelength separation decreases.

Table 1 summarizes the influence of wavelength separation and power superiority of the interfering signal over the legitimate signal at 1549,74 nm. In the first case, the wavelength of the interfering signal matches the used EDFA gain peak at 1531 nm. In the second case, it is at the first neighboring WDM channel, i.e. at 1549,08 nm. For both cases, we investigate the gain of the legitimate signal for jamming signal power levels 10 dB and 20 dB higher than the legitimate signal. For two pump powers, i.e. 40 mW and 80 mW, the first row in the table shows the gain of the legitimate signal when no jamming signal is present. The values in the table clearly show that the presence of a strong signal results in weaker amplification of the signal at lower power level. The gain of the legitimate signal drops as the power of the interfering signal increases. Furthermore, for a given power level of the interfering signal, its harmful effect to the legitimate signal is more intense when their wavelengths are close in the spectrum, as highlighted in the table.

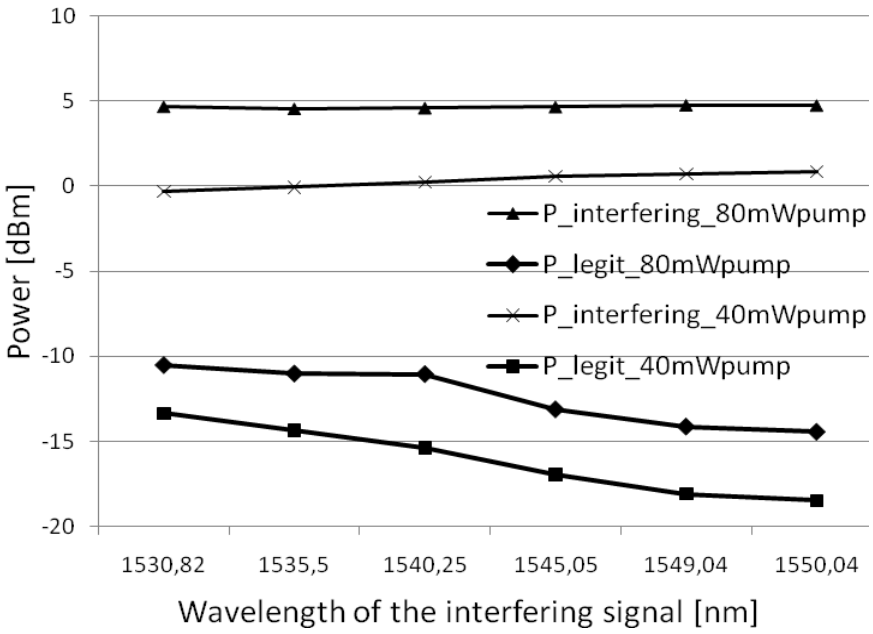



Fig. 5. The power of the legitimate and interfering signal at the output of the EDFA as a function of the wavelength of the interfering signal, at 40 mW and 80 mW EDFA pumping power and the interfering signal 20 dB stronger than the legitimate.

Out-of-band jamming can also be used to tap a signal. In some optical amplifiers, gain competition occurs at the modulation rate, which enables tapping by observing cross-modulation effects.

| EDFA pump power [mW] | Power superiority of the interfering signal [dB] | Wavelength of the interfering signal [nm] | Gain of the legitimate signal [dB] |
|---|---|---|---|
| 40 | - | - | 20,34 |
| | 10 | 1530,84 | 17,51 |
| | | 1549,08 | **15,38** |
| | 20 | 1530,84 | 12,62 |
| | | 1549,08 | **8,01** |
| 80 | - | - | 22,68 |
| | 10 | 1530,84 | 20,61 |
| | | 1549,08 | **20,03** |
| | 20 | 1530,84 | 15,63 |
| | | 1549,08 | **11,59** |

Table 1. An overview of the gain of the legitimate signal at 1549,74 nm for different test scenarios, with the power of the interfering signal at 10 and 20 dB above that of legitimate signal.

### 2.2.2 Amplifier cascades

When EDFAs are used in a cascade, the flatness of their gain becomes a critical issue. Namely, slight differences between the amounts of gain available for signals at different wavelengths get multiplied as they traverse the cascaded amplifiers. Because of this, signals on certain wavelengths might get amplified several times, while others may suffer from significant SNR deterioration (Ramaswami & Sivarajan, 2002). This situation is shown in figure 6. There are several ways of dealing with this issue. For example, signals on different wavelengths can be pre-equalized, so that the signals on wavelengths with higher gain are attenuated, and those with lower gain are amplified before entering the cascaded amplifier segment. Another way of dealing with the problem is to introduce gain equalization at each amplifier stage.

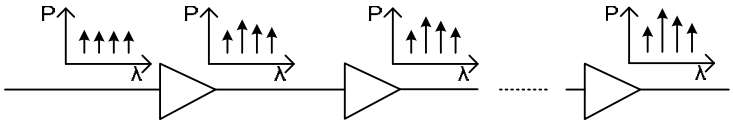



Fig. 6. The cumulative effect of unequal amplifier gain at different wavelengths after a cascade of amplifiers.

In case of cascaded EDFAs, power transients potentially present a great security threat. Due to the fact that the amplifier gain depends on the total input power, the failure of one channel will lead to surviving channels getting more gain and, thus, have higher power when they arrive to their receivers. This means that setting up or tearing a channel down affects other channels that share amplifiers with it (Karásek & Vallés, 1998). This effect may cause serious problems in dynamic optical networks where suppression of transients becomes increasingly important. A typical amplifier implementation used in today's networks consists of two EDFA stages working in gain mode, where setting up a new channel will not affect power levels of existing channels (Zsigmond, 2011). Automatic gain control (AGC) solves the problem of transients by monitoring the power levels in different ways and keeping the output power per channel constant, regardless of the input power. In such a network, high-power signals could not propagate. However, this is only valid for deviations of power within a certain window defined by the component specifications. If the difference between the power of the jamming signal and the normal users' signals exceeds this range, amplifiers with AGC may not be able to provide power equalization. (Way et al., 1993) proposed optical limiting amplifiers able to limit the output power of all signals within a dynamic range of input power and thwart the propagation of jamming attacks, but at a trade-off with a higher price of such equipment. Today, most commercially available amplifiers are capable of monitoring channel power and reducing the excessive power levels of jamming signals (Zsigmond, 2011). However, (Deng & Subramaniam, 2004) describe an attack which can affect even networks with ability to equalize excessive power levels. It is referred to as a *low power QoS attack*. Amplifier placement along the link usually ensures compensation for the preceding fiber span. If an attacker attacks a splitter at the beginning of a link, they are able to attenuate the power of the signal more than the amplifier is able to compensate for. Such induced attenuation can significantly degrade the performance metrics of attacked lightpaths. The attenuation at the end of the link on which the splitter is installed may not be significant enough to generate an alarm at that exact location, but it

may cause other network elements with power equalization capabilities (e.g., switches) to reduce the power of other signals in an effort to maintain an even distribution of power among channels. Hence, other lightpaths suffer from attenuation and may cause the same effect in other parts of the network. When service degradation along a lightpath finally crosses the preset threshold, the location of the raised alarm may be far from the original placement of the attached splitter. This type of an attack may be especially significant for networks employing Raman amplifiers, whose usage is increasing in long haul transmission suffering from high attenuation (Zsigmond, 2011). Security advantages of Raman amplifiers include more reliable amplification, higher saturation power than EDFA and more accurate monitoring, resulting in faster generation of alarms in case of signal anomalies (Islam, 2003). However, output powers of Raman amplifiers are high and require splicing. Multiple splices can cause the Raman pumps to be reflected and, thus, highly reduce the amplifier gain. This vulnerability can be a target of a planned attack, possibly leading to a link outage (Zsigmond, 2011). Furthermore, Raman amplifiers require high-power pump sources at the right wavelength and an attacker with inside access to an amplifier may endanger the amplification process by tampering with any of these parameters.

### 2.3 Optical switches

The main functions of wavelength-selective optical cross-connects (OXC), also referred to as reconfigurable wavelength routing switches, can include lightpath provisioning, wavelength switching, protection switching (rerouting connections), wavelength conversion and performance monitoring. Such optical switches usually consist of demultiplexers, photonic switching fabric and multiplexers. A typical architecture of a wavelength-selective OXC is shown in figure 7.

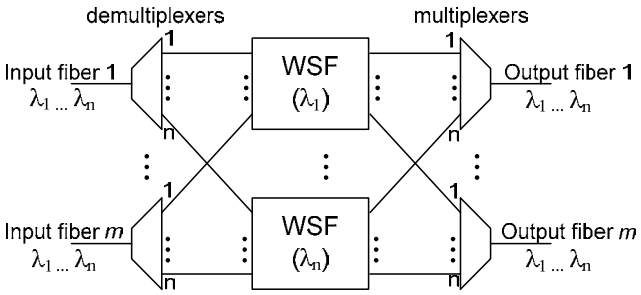



Fig. 7. The typical architecture of a wavelength-selective OXC, consisting of multiplexers, demultiplexers and wavelength switching fabric (WSF).

The incoming signal is first decomposed by demultiplexers into constituent wavelengths, which are then directed each onto their own switching fabric. Multiplexing and demultiplexing can be realized using Arrayed Waveguide Gratings (AWGs), Thin-Film Filters (TFF), Mach-Zehnder Interferometers (MZIs), Fiber Bragg Gratings (FBG) and other. The Wavelength Switching Fabric (WSF), i.e., the central part of the node, performs transparent switching of WDM channels from their input to output ports. Optical switches can be implemented using 2D or 3D Micro-Electro-Mechanical Systems (MEMS), semiconductor optical amplifier (SOA) gates, holographic switches, liquid crystal, and

thermo-optical or electro-optical technologies (Tzanakaki et al., 2004). The WSF can be reconfigurable or fixed. A fixed or non-reconfigurable switching fabric has manually hard-wired connections between input and output ports, which cannot be changed on demand. On the other hand, connections between input and output ports of reconfigurable WSFs can be dynamically reconfigured in times ranging from several milliseconds (MEMS, bubble, liquid crystal, opto-mechanical, thermo-optic switch), several microseconds (acousto-optic switch) to several nanoseconds (electro-optic, SOA-based switch) (Papadimitriou et al., 2003; Rohit et al., 2011). After switching is performed, wavelengths intended to each output fiber are combined by multiplexers.

The main security vulnerability of optical switches arises from their proneness to signal leaking, giving rise to crosstalk. Almost all TON components, i.e., filters, multiplexers, demultiplexers and switches, introduce crosstalk in one form or another. Malicious users can take advantage of this phenomenon to cause service degradation and/or perform eavesdropping.

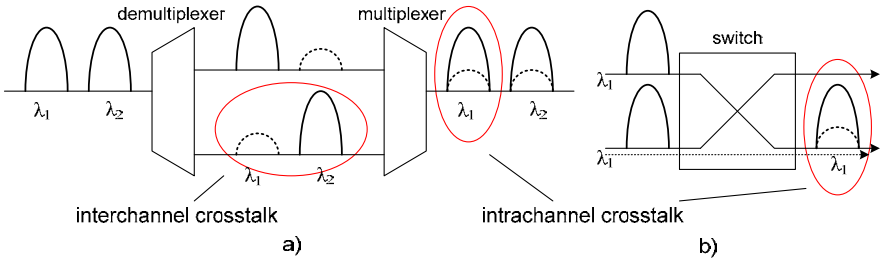



Fig. 8. (a) An optical multiplexer/demultiplexer and (b) an optical switch as sources of interchannel and intrachannel crosstalk.

In general, there are two types of crosstalk in transparent optical networks – interchannel and intrachannel crosstalk. Interchannel crosstalk occurs between signals on sufficiently spaced wavelengths, i.e. such that they do not fall inside each other's receiver pass-bands. Adjacent channels are usually the primary sources of crosstalk, while the influence of channels with higher wavelength separation is usually negligible. Inside OXCs, this type of crosstalk arises from non-ideal demultiplexing, where one channel is selected while the others are not perfectly dropped. This scenario is shown in figure 8(a). Depending on the implementation of the (de)multiplexers, their levels of crosstalk may range from 12 dB for TFF to 30 dB for AWG, MZI and FBG (Mukherjee, 2002). Intrachannel crosstalk occurs among signals on the same wavelength, or signals whose wavelengths fall within each other's receiver pass-band.

Multiplexers, demultiplexers and optical switches can all be sources of intrachannel crosstalk. Namely, when demultiplexers separate incoming signals at different wavelengths, a small portion of each signal leaks onto ports reserved for signals at other wavelengths. After switching, when multiple signals at different wavelengths are multiplexed back onto the same output fiber, small portions of a certain wavelength that had leaked onto other wavelengths can leak back onto the common fiber (Rejeb et al., 2006b). Consequently, the signal on that wavelength will have crosstalk originating from its very own components carrying the same information, but suffering from different delays and phase shifts, as

shown in figure 8(a). Intrachannel crosstalk can also arise in optical switches due to non-ideal switching. Namely, switching ports are not perfectly isolated from each other, so components of different signals transmitted on the same wavelength can leak and interfere with each other. Since the damaging signal is on the same wavelength as the legitimate signal, intrachannel crosstalk cannot be filtered out by optical filters or removed by demultiplexers (Deng et al., 2004). Figure 8(b) shows an optical switch as a source of intrachannel crosstalk. Crosstalk levels of optical switches range from 35 dB (SOA, liquid crystal, electro-optical, thermo-optical and holographic switches) to 55 dB for MEMS.

Optical couplers are the basic building blocks of optical switches, multiplexers and demultiplexers, modulators, filters and wavelength converters (Ramaswami & Sivarajan, 2002) and are the source of a significant amount of inter/intra-channel crosstalk. Generally, an optical coupler is a device used to combine or split signals in an optical network and can be passive or active. In passive couplers, employed in TONs, signals are redistributed without opto-electrical conversion and do not require any external power.

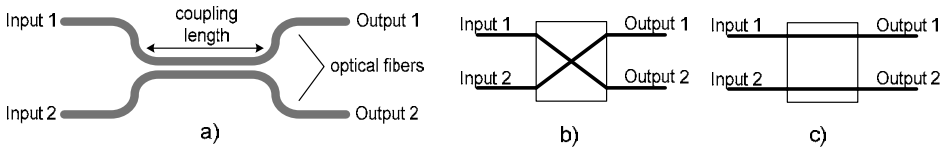



Fig. 9. A (a) directional coupler and its two states: (b) cross state and (c) bar state.

A passive directional 2×2 coupler is shown in figure 9(a). It consists of a pair of parallel optical waveguides in close proximity. The most commonly used couplers, called fused fiber couplers, are made by fusing two fibers together in the middle (Ramaswami & Sivarajan, 2002). The fraction of the signal power that is transferred from the input to the output of an optical waveguide is defined by the coupling ratio α, denoting that a fraction α of the power of the signal at the input of a waveguide is transferred to its output, while the remaining 1-α of the power is directed to the output of the other waveguide. Ideally, all the input power on one waveguide of a directional coupler is coupled to the other waveguide for the cross state, while in the bar state there should be no coupling between the two waveguides.

Figures 9(b) and (c) show the cross state and the bar state of an optical coupler, respectively. In reality, however, light is not perfectly coupled and components of signals from different waveguides leak onto unintended outputs, giving rise to crosstalk. Non-ideal signal coupling also causes signal losses and attenuation, which can be compensated by placing optical amplifiers at the splice output. In this way, however, the desired part of the signal will be amplified as well as the undesired part, which makes crosstalk the main deficiency of optical couplers (Vaez & Lea, 2000). Crosstalk in a directional coupler is defined as the ratio of light power at the undesired output port to the power at the desired output port with crosstalk levels varying between -20 dB and -30 dB. It can occur for various reasons, including waveguide asymmetry, absorption loss, non-optimal coupling length, unequal excitation of the symmetric and asymmetric modes at the input, or fabrication variations (Chinni et al., 1995).

Couplers can be wavelength selective, and they are often used to combine signals at 1310 nm and 1550 nm onto a single fiber, or to split them from the same incoming fiber to two

different outputs. In the latter case, due to crosstalk, small portions of the signal passing through the coupler are directed onto unintended outputs, deteriorating the Signal to Noise Ratio (SNR) of the signal which was intended for that output. Levels of this crosstalk depend on the exact wavelengths of the incoming signals.

### 2.3.1 Laboratory assessment of crosstalk in optical couplers

We tested the crosstalk of couplers in a laboratory setting from (Furdek et al., 2010b), using a FIS WDM13500129U coupler/splitter with SMF28 Singlemode fiber, operating at wavelengths 1310/1550 nm +/- 20 nm. This coupler was used as a wavelength-selective splitter for dividing the incoming WDM signal from the input port into its constituent wavelengths to two different output ports, i.e. one for signals at 1310 nm, and the other one for 1550 nm.

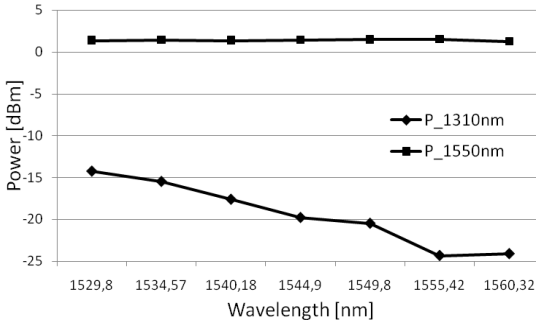



Fig. 10. Power at the coupler outputs dedicated to wavelengths at 1310 and 1550 nm for different wavelength of the incoming signal.

Figure 10 shows the effects of imperfect splitting of the incoming signal to ports dedicated to wavelengths at 1310 and 1550 nm, i.e. the power of the incoming signal at various wavelengths near 1550 nm present at the 1310 nm output. As the wavelength of the incoming signal decreases from 1560,32 nm to 1529,90 nm (in 5 nm steps), and approaches the central frequency of the 1310 nm output, the undesirable leakage intensifies.

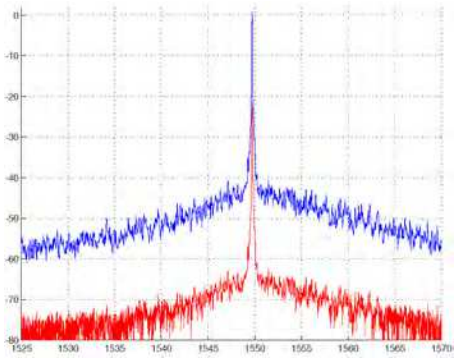


Fig. 11. The spectrum of the incoming signal at 1550 nm on the output port corresponding to 1550 nm (upper line) and on the output port corresponding to 1310 nm (lower line).

Figure 11 shows this effect for incoming signal at a nominal wavelength of 1550 nm. The upper line shows the spectrum of the signal at the output port corresponding to wavelengths around 1550 nm, while the lower line shows the spectrum at the output port corresponding to wavelengths around 1310 nm. The peak of the signal recorded at the 1310 nm-output clearly indicates the amount of the signal at 1550 nm that had leaked onto the unintended output. The signal power level of 1,48 dBm at the 1550 nm port, combined with -20,50 dBm at the 1310 nm port, indicates that the level of crosstalk is -21,98 dB. This value by itself is not large enough to significantly impact signal quality. However, many network components consist of several cascaded optical couplers, which all contribute to the overall level of crosstalk. Furthermore, signals traverse numerous components on their path from source to destination. When these factors combine, enough crosstalk can accumulate over the propagation path of a signal for the risk of service degradation to increase significantly even in cases when there is no high-powered jamming signal. When such a signal is present in the network, it causes an additional increase in the leakage inside couplers and components they comprise, resulting in a significant damage to co-propagating user signals.

### 2.3.2 Crosstalk attacks

Although crosstalk originating from direct couplers can have a significant impact on the overall Quality of Service (QoS) in the network, problems caused by crosstalk in optical networks can go beyond such signal quality deterioration. Namely, a malevolent user can take advantage of crosstalk to perform attacks aimed at eavesdropping, tapping, and/or degrading the quality of service (QoS) of other users. An overview of methods using crosstalk for attack purposes can be found in (Mas et al., 2005).

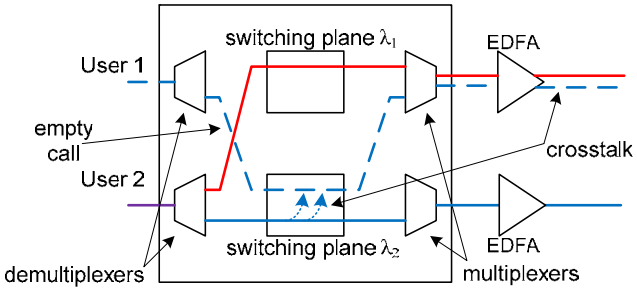



Fig. 12. An example of a tapping attack exploiting intra-channel crosstalk in a wavelength-selective switch.

Figure 12 shows an example of a tapping attack exploiting intrachannel crosstalk in a wavelength-selective switch, as described in (Médard et al., 1997). The upper input port is not used, while the bottom port receives incoming signals on wavelengths $\lambda_1$ and $\lambda_2$. Each of the signals on those two wavelengths is switched on its own switching fabric. Due to mechanisms of intrachannel crosstalk in demultiplexers, multiplexers and switching fabric described in the previous sections, components of both signals leak onto unintended outputs and get amplified by the power amplifier (EDFA). If a tapper gains access to one of the unused output ports, e.g. the upper output port in figure 12, part of the signal at $\lambda_2$ is delivered straight into his hands. This problem can be solved by individually amplifying only signals on connections which are

registered at the network management system. However, an attacker can still request a legitimate data channel and then not send any information over it, but use it to tap other signals at the same wavelength. In figure 12, the tapper is User 1, whose false data connection at wavelength $\lambda_2$ picks up components of User 2's legitimate connection at the same wavelength that had leaked inside their common switch.

Intrachannel crosstalk enables *in-band jamming*, an attack method in which an attacker inserts a powerful signal within the signal window of the legitimate user he is trying to affect. Consequently, two signals may undesirably exchange information at their common switch.

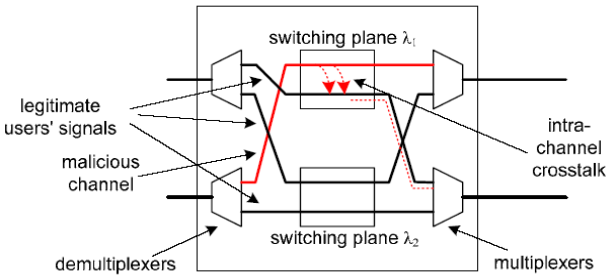



Fig. 13. An example of a jamming attack exploiting intra-channel crosstalk in an optical switch.

Figure 13 shows an example of a jamming attack via intrachannel crosstalk in optical switches. Here, an attacker injects a high-powered signal on the same wavelength as other, legitimate data signals. Components of the high-powered signal will leak onto adjacent channels inside their common optical switches, impairing the quality of the transmission on those signals. If the attacking signal is strong enough, it is possible that enough power is transferred onto adjacent channels inside their common switch, for them to gain attacking capabilities. Consequently, the attacked signal becomes an attacker itself, allowing the attack to propagate through the network, affecting signals which do not even share any physical components with the original attacking signal. This type of attack is shown in figure 14. Via intra-channel crosstalk in switches, the attacker managed to affect not only user 1's legitimate signal, but the attack also propagated to users 2 and 3, which share no common physical components with the original attacker. This type of attack is particularly hazardous to network operation since the nature of its propagation makes localization of the original source of attack very difficult.

Jamming attack exploiting intrachannel crosstalk in switches has been previously identified in the literature by (Wu & Somani, 2005), and recently (Peng et al., 2011) provided an experimental validation of the proposed attack model. They proved through simulation that high-power jamming attacks indeed possess propagation capabilities in affecting other lightpaths at the same wavelength via intrachannel crosstalk inside their common switches and lightpaths at different wavelengths via interchannel crosstalk inside their common fibers. The propagation of intrachannel crosstalk attacks ends after at most three stages of optical switches, while interchannel crosstalk attacks get attenuated after traversing three fiber segments. This means that, in the scenario from figure 14, the signal quality of user 3 would not suffer from serious BER degradation from the attacker's jamming signal.

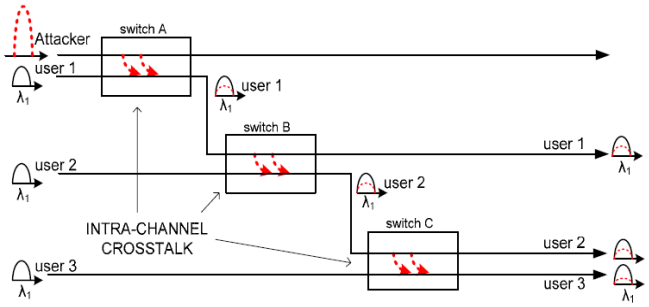



Fig. 14. Propagation of intra-channel crosstalk attacks in an all-optical network.

The vulnerability of TONs to high-power jamming attacks depends on employed hardware components and node architectures, as well as the architecture of the established virtual topology. Besides the wavelength-selective (WS) realization of OXCs, they can also be implemented as broadcast-and-select (B&S) devices. In B&S architecture, the wavelength switching fabric is replaced by passive splitters and couplers which connect the incoming signal to tunable filters. After filtering the desired wavelength, the signals from filter outputs are coupled onto the desired OXC output port. (Arbués et al., 2007) report that B&S architectures exhibit greater vulnerability to in-band jamming due to low isolation of tunable filters. WS architecture performs slightly better due to improved isolation at the multiplexing and demultiplexing stages.

(Liu & Ji, 2007) studied the impact of the physical topology in conjunction with its constituent devices and the network traffic on the network resilience to in-band jamming attacks. Under the assumption of a fully connected virtual topology, i.e. a connection between each node pair and assuming that jamming attack propagation is not possible, they find that fully-connected mesh, star and ring physical topologies are the least resilient to attacks. The main cause of low resilience of a fully-connected mesh is its high nodal degree and, hence, a high expected number of affected channels at each node. The latter is also the reason why star networks are highly susceptible to attacks. For ring topologies, their vulnerability stems from large route lengths. A chord network topology is distinguished as the most resilient to attacks, with a logarithmic increase in resilience loss for a linear growth of the network size.

## 3. Security in TONs

As previously mentioned, the high data rates and huge throughput associated with transparent optical networks make them extremely sensitive to communication failures caused by component faults or deliberate attacks. A secure network should provide physical security of communication, i.e. provide service availability, guarantee a certain level of QoS and protect data integrity and privacy of communication. It should also ensure semantic security, i.e. protect the confidentiality and the meaning of data through authentication and cryptography mechanisms. Transparent optical transmission and the properties of attacks as described in the previous section impose a new set of demands on the network management system (NMS), responsible for network configuration, performance engineering, fault handling and the secure and safe functioning of the network (Rejeb et al,. 2010; Li et al., 2002).

The headstone of an efficient NMS in TONs is a flexible and robust control plane, which relies on accurate and timely monitoring in the optical domain. Control plane functions can roughly be divided into following tasks (Rejeb et al., 2010; Saha et al., 2003):

- Resource management – accurate information on resource availability must be available at all times and updated upon lightpath establishment or tear-down.
- Lightpath provisioning – initially, the topology and resources must be automatically discovered. For each incoming lightpath demand, the control plane should calculate a physical route based on the available resources and tentative QoS requirements. For this, accurate information regarding resource availability and the associated service quality is crucial.
- Signaling – information exchange regarding connection establishment, maintenance and tear-down between nodes, as well as the management of alarms in cases of failures, must be present.

Optical network security requires protective and/or preventive measures which minimize network accessibility to attackers, limit attack propagation and reduce the damage proportions inflicted by attacks. However, when an attack occurs in spite of these mechanisms, the NMS needs to undertake the following steps:

- Detect the attack – discover a deterioration of signal quality, an intrusion in the fiber, a loss of service or any other direct consequence of an attack. After detecting the presence of an attack, its exact location must be determined and the source of the attack must be identified.
- React to the attack – by triggering reaction mechanisms, the attacker's access point must be isolated and the harmful effects must be neutralized. The affected connections must be restored and communication should resume as fast as possible.

### 3.1 Protection and prevention of attacks

The risks and damage associated with physical-layer attacks can be alleviated through careful network planning, employment of additional equipment, quick and accurate post-attack recovery and optical cryptography. Achieving complete protection requires large investments by the network operator and may be economically unviable. Thus, an advantageous trade-off between the costs and achieved protection must be found. Attack protection may include the following measures (Fok et al., 2011; Médard et al., 1997):

- Hardware measures – shielding the fiber to protect from tapping, introducing additional equipment in the network capable of limiting excessive power (e.g. optical limiting amplifiers or variable optical attenuators), or using optical fuses which melt under high power (Shuto et al., 2004) to protect from high-power jamming. Using components with lower crosstalk levels also helps reduce the risk from jamming and tapping attacks.
- Transmission schemes – applying different modulation and coding techniques or limiting the bandwidth and power of certain signals may help against tapping and jamming.
- Architecture and protocol design – identifying and avoiding risky links or assigning different routes and wavelengths to separate trusted from untrusted users may decrease the risk. Here, assessment of link risk and user trustworthiness is crucial, which may be extremely complicated.

- Optical encryption – protects communication confidentiality by making it incomprehensible to an eavesdropper.
- Optical steganography – protects communication privacy by hiding the transmission between a pair of users underneath the public transmission channel. In this way, an attacker is unaware of the existence of communication, which makes it extremely difficult to perform tapping or jamming. However, the overall network vulnerability to jamming attacks may result in hidden communication being a collateral victim of jamming public channels.
- Optical network survivability – intelligent protection schemes can increase resilience to attacks by switching the signals under attack to unaffected parts of the spectrum or to physically disjoint backup paths.

Prevention may play a significant role in enhancing TON resilience to attacks, as well as the reduction of the deteriorating effects of attacks. The concept of attack-aware optical networks planning to reduce attack consequences was introduced in (Skorin-Kapov et al., 2010). By determining the mutual jamming attack relations between lightpaths, a novel objective criterion for the routing and wavelength assignment problem was defined, called the Lightpath Attack Radius (LAR). By minimizing the LAR of each lightpath through judicious routing, the maximum possible damage caused by such attacks can be reduced. In (Furdek et al., 2010c), a similar approach was developed for minimizing crosstalk effects caused by in-band jamming through judicious wavelength assignment. Our current ongoing work in attack-aware optical network planning is focused on survivability mechanisms and node power equalization placement.

### 3.2 Attack detection

Detection of an attack relies closely on reliable and accurate monitoring methods. In TONs, real-time monitoring must take place in the optical domain, without electronically interpreting the carried data. Descriptions of techniques for monitoring various optical signal parameters can be found in (Ho & Chen, 2009; Kilper et al., 2004). Depending on the technology, monitoring methods should be capable of measuring parameters such as channel power (peak and average) and aggregate WDM signal power, eye diagram, optical spectrum, polarization state, phase, pulse shape, Q-factor, chromatic and polarization-mode dispersion (PMD) etc. The measured parameters indicate the level of quality of aggregate WDM layer parameters, as well as individual signal quality parameters. Due to high prices of monitoring equipment, placing their minimal number in strategic locations and establishing supervisory channels able to detect as many faults as possible remains an important network planning problem. Today, there are commercially available reconfigurable optical switches which provide per-channel power and wavelength monitoring, such as that from (Cisco, 2011). Furthermore, they are usually equipped with variable optical attenuators and are, thus, able to dynamically react to excessive power levels on individual channels and thwart jamming attacks. However, these devices are not yet widely deployed. Currently, around 80% of deployed network nodes consist of fixed optical switches and add-drop multiplexers (FOADMs) whose power settings are determined in the system commissioning phase and do not offer the capability of dynamically managing power level fluctuations of incoming signals. Current market trends show a tendency of reconfigurable node usage increasing to 50% of

network nodes in the next few years, while the remaining nodes will still consist of FOADMs (Zsigmond, 2011).

Some monitoring methods which can detect specific attack scenarios are elaborated in (Médard et al., 1997). These methods can rely on statistical analysis of the optical properties of transmitted signals or they can use special, dedicated signals. Statistical methods include wideband power detection and optical spectrum analysis. The first method measures the power over a wide bandwidth and reacts to deviations from statistically computed expected power levels. It may be able to detect a high-powered in-band jamming attack, but sporadic jamming attacks, jamming attacks which deteriorate the SNR without changing the power levels in the affected signals or tapping attacks which tap a very small amount of the total signal power may not be detectable by this method. The second method, i.e. optical spectrum analysis, measures the shape of optical signal spectrum. It is able to detect an out-of-band jamming attack causing gain competition, but in-band jamming may go undetected if the attacking signal doesn't introduce significant spectrum changes. This method isn't very helpful at detecting tapping attacks, unless the analyzer is placed on the link which drains the tapped portion of the signal and under the condition that it is able to distinguish authorized from unauthorized communication.

Two of the most common monitoring methods which use dedicated signals are the pilot tone method and optical time domain reflectometry (OTDR). Pilot tones are special signals dedicated to detecting transmission interruption. They may be carried along the legitimate signal's path at a different frequency. Their application in detecting in-band jamming requires very complex scenarios, because a pilot tone can only detect jamming on the very same frequency. Furthermore, pilot tones may be jammed themselves, creating an opportunity to mask jamming on legitimate lightpaths. Gain competition attacks may be discovered by pilot tones, but only if they receive amplification from the same EDFA as affected lightpaths. Even in this case, the BER degradation of the pilot tone caused by gain competition may go undetected because their main purpose is only to assert availability of communication, and not the available QoS. Pilot tones provide little help in detection of tapping, which would require a significant degradation of the signal quality. The main principle of OTDR is to inject pilot tones onto a link and analyze its echo in order to determine fiber cuts or losses, which makes attack detection abilities of these two methods similar. Detection of in-band jamming differs from the pilot-tone method only in its occurrence at the front-end of the link. Due to the fact that EDFAs are unidirectional, the OTDR method will not be able to detect gain competition. On the other hand, it may be successful in detecting tapping, which causes discontinuities in the reflected pilot tone.

### 3.3 Reaction to attacks

Once the presence of an attack is detected in the network, the NMS will try to eliminate it as soon as possible and re-establish reliable communication. Reaction from an attack at the optical layer should be fast and recovery should take place before the upper, slower network layers activate their reaction mechanisms. In most cases, the link on which the presence of an attack was detected will be switched off, which will trigger mechanisms for network survivability. Survivability mechanisms include protection, where resources are reserved for pre-computed backup paths of each of the working paths at lightpath setup time, and restoration, in which backup paths are computed upon a failure of the working

path. Protection can be dedicated, where each backup path has its own dedicated resources, or shared, where resource sharing among backup paths of link-disjoint working paths is allowed. After finding a backup path for the affected connections, transmission will resume. Finding the exact location of the attack and disabling the attacker before re-establishing transmission of affected connections is crucial for this step. If these conditions are not met, protection resources may be wasted and switching the transmission to backup paths may even enhance attack propagation and worsen its effects.

A standardized approach for attack management has not yet been established. The main reason for this is the fact that optical monitoring technology hasn't yet reached its maturity and cannot provide reliable attack detection (Rejeb et al., 2006b), as well as the fact that the fault and localization methods design highly depends on the specific physical layer details (Rejeb et al., 2006a). Several frameworks for managing physical-layer attacks have been proposed in the literature. Reliable attack detection in some of them is based on the currently unrealistic assumption that all nodes are able to provide per channel monitoring, while others propose efficient monitoring placement policies, matching more realistic network scenarios.

Initial works on attack source identification date from the late 90's. In (Bergman et al., 1998), the authors propose a distributed algorithm for localizing jamming attacks based on the relation between the signal power metrics at the output and input of each node. Neighboring nodes exchange messages and determine the presence of an attack. The nodes are aware of their positions along every connection (i.e., whether they are upstream or downstream from the neighboring node they exchange messages with) so the algorithm is able to find the most upstream node which detects an attack along a connection, and thus can identify the source of the attack.

In the next decade, (Wu & Somani, 2005) provide a model of jamming attacks exploiting intrachannel crosstalk in optical switches with propagation capabilities, which enable affected lightpaths to acquire attacking capabilities and spread the attack to lightpaths which do not share any common physical components with the original attacker. They identify the assumption of all nodes being able to monitor all channels as unrealistic due to the high costs of this solution and propose a monitoring node model, their sparse placement, an additional test connection setup policy and a lightpath routing policy which is able to localize the source of a single crosstalk attack in the network.

In (Mas et al., 2005), the problem of finding the exact location of the failure is extended to the presence of single and multiple failures in cases where alarms can be false and/or lost. This problem is NP-complete even when no false or lost alarms exist. The algorithm is based on building a binary tree whose branches correspond to sets of network elements which will raise an alarm when a particular network component fails. Alarms differ according to the type of the failure and equipment used. When alarms are raised during network operation, the location of the failure is determined by traversing the binary tree and finding the components whose corresponding failures justify the received alarms. The authors also propose an optimal monitoring placement scheme for minimizing the number of network elements which are candidates to have a failure and, thus, minimizing the result given by the failure location algorithm.

(Rejeb et al., 2006a) investigate the local correlation of security failures and attacks at each OXC node and mechanisms to discover the tracks of multiple attacks through the network using as little monitoring information as possible. The correct functioning of this distributed algorithm relies on a reliable NMS which provides correct message passing and processing at local nodes. Namely, the algorithm uses updated connection and monitoring information at the input and output sides of any OXC node in the network. In order to decrease these tight requirements on monitoring information, the health of lightpaths which simultaneously propagate through OXC nodes is estimated through correlation with other lightpaths. When a node detects serious performance degradation along a lightpath at its output side, it runs a generic procedure for localizing the set of lightpaths which traverse this node and are most likely to be the offender. The localization procedure is then delegated to the next upstream node along each of these lightpaths which also registers performance degradation, and this is repeated until no such node is found.

In (Stanic & Subramaniam, 2011), the authors propose a fault localization scheme which collects monitoring information from lightpaths which carry traffic and from additionally established supervisory lightpath, achieving complete fault localization coverage. The authors consider a monitoring model where each OXC node is capable of detecting in-band loss–of-light faults. The problem of deciding which supervisory lightpaths will be added to the given set of traffic lightpaths is formulated as an Integer Linear Program (ILP) and an efficient heuristic approach for computing the optimal set of supervisory lightpaths is proposed.

## 4. Conclusion

This chapter presents an overview of the vulnerabilities of Transparent Optical Networks (TONs) to various physical-layer attacks. Furthermore, methods for attack detection and localization, as well as various countermeasures against attacks are described. As a result of the vulnerabilities associated with TONs stemming from optical components, transparency and high speed, new approaches to network security are increasingly needed as networks migrate to all-optical transmission. Such security frameworks require new, tailored attack detection, localization and network restoration mechanisms. In addition to upgrading existing ways of dealing with network failures and attacks, significant attention should be paid to prevention mechanisms, attack-aware planning and improved optical monitoring methods.

## 5. Acknowledgements

This work was supported by projects “A Security Planning Framework for Optical Networks (SAFE)”, funded by the Unity Through Knowledge Fund (UKF) in Croatia, and 036-0362027-1641, funded by the Ministry of Science, Education and Sports, Croatia.

## 6. References

Arbués, P.G., Mas Machuca, C. & Tzanakaki, A. (2007). Comparative Study of Existing OADM and OXC Architectures and Technologies from the Failure Behavior

Perspective. *Journal Of Optical Networking*, Vol. 6, No. 2, (February 2007), pp. (123-133), ISSN 1536-5379

Bae, J.K., Koh, D., Kim, S.H., Park, N. & Lee, S.B. (2007). Automatic EDFA Gain Spectrum Equalization Using LPFGs on Divided Coil Heaters, *Proceedings of Optical Fiber Communication and the National Fiber Optic Engineers Conference* (OFC/NFOEC), ISBN 1-55752-831-4, Anaheim, USA, March 2007

Chinni, V.R., Huang, T.C, Wai, P.-K.A., Menyuk, C.R. & Simmonis, G.J. (1995). Crosstalk in a Lossy Directional Coupler Switch, *Journal of Lightwave Technology*, Vol.13, No. 7, (July 1995), pp. (1530-1535), ISSN 0733-8724

Cisco (2011.) Cisco ONS 15454 Multiservice Transport Platform. Available from <http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/ps5320/product_data_sheet09186a00801849e7.html>

Deng, T. & Subramaniam, S. (2004). Covert Low-Power QoS Attack in All-Optical Wavelength Routed Networks, *Proceedings of IEEE GLOBECOM '04*, ISBN 0-7803-8595-3, Dallas, USA, November 2004

Deng, T., Subramaniam, S. & Xu, J. (2004). Crosstalk-aware wavelength assignment in dynamic wavelength-routed optical networks, *Proceedings of BroadNets'04*, ISBN 0-7695-2221-1, San Jose, USA, December 2004

Fok, M.P., Wang, Z., Deng, Y. & Prucnal, P.R. (2011). Optical Layer Security in Fiber-Optic Networks. *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, (September 2011), pp. (725-736), ISSN 1556-6013

Furdek, M., Bosiljevac, M., Skorin-Kapov, N. & Šipuš, Z. (2010a). Gain Competition in Optical Amplifiers: A Case Study. *Proceedings of International Convention on Information and Communication Technology, Electronics and Microelectronics* (MIPRO 2010), ISBN 978-1-4244-7763-0, Opatija, Croatia, May 2010

Furdek, M., Skorin-Kapov, N., Bosiljevac, M. & Šipuš, Z. (2010b). Analysis of Crosstalk in Optical Couplers and Associated Vulnerabilities. *Proceedings of International Convention on Information and Communication Technology, Electronics and Microelectronics* (MIPRO 2010), ISBN 978-1-4244-7763-0, Opatija, Croatia, May 2010

Furdek, M., Skorin-Kapov, N. & Grbac, M. (2010c). Attack-Aware Wavelength Assignment for Localization of In-band Crosstalk Attack Propagation. *IEEE/OSA Journal of Optical Communications and Networking*, Vol. 2, No. 11, (November 2010), pp. (1000-1009), ISSN 1943-0620

Ho, S.-T. & Chen, L.-K. (2009). Monitoring of Linearly Accumulated Optical Impairments in All-Optical Networks. *IEEE/OSA Journal of Optical Communications and Networking*, Vol. 1, No. 1, (June 2009), pp.(125-141), ISSN 1943-0620

Islam, M. N. (2003). Information Assurance and System Survivability in All-Optical Networks, Available from <www.eecs.umich.edu/OSL/Islam/SecureComm-WP.pdf>

Karásek, M. & Vallés, J.A. (1998). Analysis of Channel Addition/Removal Response in All-Optical Gain- Controlled Cascade of Erbium-Doped Fiber Amplifiers. *Journal of Lightwave Technologies*, Vol. 16, No. 10, (October 1998), pp. (1795-1803), ISSN 0733-8724.

Kilper, D.C., Bach, R., Blumenthal, D.J., Einstein, D., Landolsi, T., Ostar, L., Preiss, M. & Willner, A. E. (2004). Optical Performance Monitoring. *Journal of Lightwave Technologies*, Vol. 22, No. 1, (January 2004), pp. (294-304), ISSN 0733-8724.

Laude, J.-P. (2002). *DWDM Fundamentals, Components, and Applications*, Artech House, Inc., ISBN 1-58053-177-6, Norwood

Li, G., Yates, J., Wang, D. & Kalmanek, C. (2002). Control Plane Design for Reliable Optical Networks. *IEEE Communications Magazine*, Vol. 40, No. 2, (February 2002), pp. (90-96), ISSN 0136-6804

Liu, G. & Ji, C. (2007). Resilience of All-Optical Network Architectures under In-Band Crosstalk Attacks: A Probabilistic Graphical Model Approach. *IEEE Journal on Selected Areas in Communications*, Vol. 25, No. 4, (April 2007), pp. (2-17), ISSN 0733-8716

Mas, C., Tomkos, I. & Tonguz, O. (2005). Failure Location Algorithm for Transparent Optical Networks. *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 8, (August 2005), pp. (1508-1519), ISSN 0733-8716

Médard, M., Marquis, D., Barry, R.A. & Finn, S.G. (1997). Security Issues in All-Optical Networks. *IEEE Network,* Vol. 11, No. 3, (May/June 1997), pp. (42-48), ISSN 0890-8044

Médard, M., Marquis, D. & Chinn, S.R. (1998). Attack Detection Methods for All-Optical Networks, *Proceedings of Network and Distributed System Symposium (NDSS '98),* ISBN 1-891562-01-0, San Diego, USA, March 1998.

Miller, S.K. (10 July 2007). Fiber Optic Security a Necessity, In: *SearchTelecom.com,* Available from <http://searchtelecom.techtarget.com/news/1263785/Fiber-optic-network-security-a-necessity>

Mukherjee, B. (2006.) *Optical WDM Networks*, Springer Science+Business Media, Inc., ISBN 978-0387-29055-3, New York.

Oyster Optics, Inc. (2002) Securing Fiber Optic Communications against Optical Tapping Methods, Available from <http://www.rootsecure.net/content/downloads/pdf/fiber_optic_taps.pdf>

Papadimitriou, G.I., Papazoglou, C. & Pomportsis, A.S. (2003). Optical Switching: Switch Fabrics, Techniques and Architectures. *Journal of Lightwave Technology*, Vol. 21, No. 2, (February 2003), pp. (384-405), ISSN 0733-8724

Peng, Y., Sun, Z., Du, S. & Long, K. (2011). Propagation of All-Optical Crosstalk Attack in Transparent Optical Networks. *Optical Engineering*, Vol. 50, No. 8, (August 2011), 085002, ISSN 0091-3286

Ramaswami, R. & Sivarajan, K.N. (2002). *Optical Networks: A Practical Perspective* (2nd edition), Morgan Kaufmann Publishers, ISBN 1-55860-655-6, San Francisco

Rejeb, R., Leeson, M.S & Green, R.J. (2006a). Multiple Attack Localization and Identification in All-Optical Networks. Optical Switching and Networking, Vol. 3, No. 1, (July 2006), pp. (41-49), ISSN 1573-4277

Rejeb, R., Leeson, M.S. & Green, R.J. (2006b). Fault and Attack Management in All-Optical Networks. *IEEE Communications Magazine*, Vol. 44, No. 11, (November 2006), pp. (79-86), ISSN 0163-6804

Rejeb, R., Leeson, M.S., Mas Machuca, C. & Tomkos, I. (2010). Control and Management Issues in All-Optical Networks. *Journal of Networks*, Vol. 5, No. 2, (February 2010), pp. (132-139), ISSN 1796-2056

Richardson, R. (2008). CSI Computer Crime & Security Survey, Available from: <http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf>

Rohit, A., Albores-Mejia, A., Calabretta, N., Leijtens, X., Robbins, D.J., Smit, M.K. & Williams, K. (2011). Fast Remotely Reconfigurable Wavelength Selective Switch, *Proceedings of Optical Fiber Communication Conference* (OFC 2011), Los Angeles, USA, ISBN 978-1-4577-0213-6

Saha, D., Rajagopalan, B. & Bernstein, G. (2003). The optical network control plane: state of the standards and deployment. *IEEE Communications Magazine*, Vol. 41, No. 8, (August 2003), pp. (S29-S34), ISSN 0163-6804

Shen, G. & Tucker, R.S. (2007.) Translucent Optical Networks: The Way Forward. *IEEE Topics in Optical Communications*, Vol. 45, No. 2, (February 2007), pp. (48-54), ISSN 0163-6804

Shuto, Y., Yanagi, S., Asakawa, S., Kobayashi, M. & Nagase, R. (2004). Fiber Fuse Phenomenon in Step-index Single-mode Optical Fibers. *IEEE Journal of Quantum Electronics*, Vol. 40, No. 8, (August 2004), pp. (1113-1121), ISSN 0018-9197

Skorin-Kapov, N., Chen, J. & Wosinska, L. (2010). A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment. *IEEE/ACM Transactions on Networking*, Vol. 18, No. 3, (June 2010), pp. (750-760), ISSN 1063-6692

Stanic, S. & Subramaniam, S. (2011). Fault Localization in All-Optical Networks with User and Supervisory Lightpaths. *Proceedings of IEEE International Conference on Communications (ICC 2011)*, ISBN 978-1-61284-232-5, Kyoto, Japan, June 2011

Tzanakaki, A., Zacharopoulos, I. & Tomkos, I. (2004). Broadband Building Blocks [Optical Networks]. *IEEE Circuits and Devices Magazine*, Vol. 20, No. 2, (March/April 2004), pp. (32-37), ISSN 8755-3996

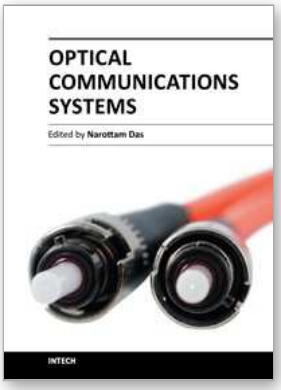
Vaez, M.M. & Lea, C.-T. (2000). Strictly Nonblocking Directional-Coupler-Based Switching Networks Under Crosstalk Constraint, *IEEE Transactions on Networking*, Vol. 48, No. 2, (February 2000), pp. (316-323), ISSN 1036-6692

Way, I.W., Chen, D., Saifi, M.A., Andrejco, M.J., Yi-Yan, A., von Lehman, A.& Lin, C. (1991). High Gain Limiting Erbium-Doped Fiber Amplifier With Over 30 dB Dynamic Range, *IEEE Electronic Letters*, Vol. 27, No. 3, (January 1991), pp. (211-213), ISSN 0013-5194

Witcher, K. (2005). Fiber Optics and its Security Vulnerabilities. SANS Institute, Available from: <http://www.sans.org/reading_room/whitepapers/physcial/>

Wu, T. & Somani, A.K. (2005). Cross-Talk Attack Monitoring and Localization in All-Optical Networks, *IEEE/ACM Transactions on Networking*, Vol. 13, No. 6, (December 2005), pp.(1390-1401), ISSN 1036-6692

Zsigmond, S. (2011). External Report on Physical-Layer Attacks in Optical Networks. Technical report, project SAFE (http://www.fer.unizg.hr/tel/en/research/safe), supported by the Unity through Knowledge Fund (UKF), Ministry of Science, Education and Sports, Croatia, 2011




**Optical Communications Systems**

Edited by Dr. Narottam Das

ISBN 978-953-51-0170-3
Hard cover, 262 pages
**Publisher** InTech
**Published online** 07, March, 2012
**Published in print edition** March, 2012

Optical communications systems are very important for all types of telecommunications and networks. They consists of a transmitter that encodes a message into an optical signal, a channel that carries the signal to its destination, and a receiver that reproduces the message from the received optical signal.This book presents up to date results on communication systems, along with the explanations of their relevance, from leading researchers in this field. Its chapters cover general concepts of optical and wireless optical communication systems, optical amplifiers and networks, optical multiplexing and demultiplexing for optical communication systems, and network traffic engineering. Recently, wavelength conversion and other enhanced signal processing functions are also considered in depth for optical communications systems. The researcher has also concentrated on wavelength conversion, switching, demultiplexing in the time domain and other enhanced functions for optical communications systems. This book is targeted at research, development and design engineers from the teams in manufacturing industry; academia and telecommunications service operators/ providers.

**How to reference**

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Marija Furdek and Nina Skorin-Kapov (2012). Physical-Layer Attacks in Transparent Optical Networks, Optical Communications Systems, Dr. Narottam Das (Ed.), ISBN: 978-953-51-0170-3, InTech, Available from: http://www.intechopen.com/books/optical-communications-systems/physical-layer-attacks-in-transparent-optical-networks

INTECH
open science | open minds

**InTech Europe**
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

**InTech China**
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821