

The Threat of Optical Transmission Jamming

Marcin Kowalczyk, Michał Marzecki, and Jerzy Siuzdak

Warsaw University of Technology, Warsaw, Poland

<https://doi.org/10.26636/jtit.2023.4.1402>

Abstract — In this paper, we investigate how data transmissions may be affected by various types of optical interference introduced into the fiber on purpose, via a clip-on coupler. The research proved that transmissions may be jammed completely using inexpensive equipment readily available on the market, provided that the attacker has physical access to the fiber optic cable. The most dangerous attacks rely on a typical, slowly modulated communication laser with a rectangular waveform. This study urges further research aimed at counteracting such attacks.

Keywords — *clip-on coupler, optical communication jamming, optical networks vulnerability*

1. Introduction

At first glance, fiber optic communication seems to be safe in comparison with wireless or cable connections. On the one hand, this results from the lack of the so-called electromagnetic corona, making it difficult to remotely eavesdrop information sent via a fiber optic cable. On the other hand, the fiber optic transmissions simply cannot be jammed remotely due to the complete immunity of the optical fiber to electromagnetic interference (EMI). This creates an illusion about the security of optical fiber data transfers. Unfortunately, the security of fiber optic transmission ends when an unauthorized person gains direct physical access to the fiber optic cable or to optical/optoelectronic devices used to establish network connections.

For example, in 2003, an illegal eavesdropping device in Verizon's fiber optic network was detected [1], [2]. In 2000, three of the main fiber optic lines of Deutsche Telekom were attacked in a similar manner at the Frankfurt, Main airport [2]. According to [1], transmissions using underwater cables can be eavesdropped as well. For this purpose, a submarine may be modified by adding a special compartment to which a cable can be connected to install listening devices [2].

To prevent the threats mentioned above, the methods that are available should be reviewed in the first place. Here, we limit ourselves to an analysis of the attacks affecting the physical layer, omitting higher OSI layer breach attempts, which are possible as well. The issues of countering attacks and mitigating their outcomes are beyond the scope of this work too. The attacks this paper is concerned with may be divided into two main groups: passive and active. Eavesdropping and traffic analysis are two basic types of attacks belonging to

the former category. The attacks are intended to be invisible to legitimate network users and the eavesdropping devices installed should be difficult to locate. Even if the listening device introduces some attenuation in the signal path, the margin of the power level along the optical path is usually so high that the wiretapping does not affect the quality of service and does not raise alarms in the network.

Active attacks focus on disrupting the operation of the network, for instance by significantly degrading the quality of service (QoS), all the way to completely blocking transmission in a single link or the network node. The attacker attempts to mask the location (or locations) of the attack. Hence, such an attack is not easy to detect and isolate from an event consisting in the failure of a given network component.

The paper is organized as follows. Section 2 presents the potential attacks on optical network infrastructure, identifying a specific type of attack, i.e. jamming the transmission by using a clip-on coupler. The possibility of such an attack is mentioned in [3], but without any details given. Therefore, this paper aims to close this gap. The setup of the attack is described in Section 3. Section 4 presents the results of a measurement campaign, with a discussion contained in Section 5. Finally, conclusions are drawn in Section 6.

2. Attacks on Optical Infrastructure

Attacks on the optical infrastructure may be classified as passive attacks involving transmission eavesdropping, and active attacks which consists in disrupting the transmission, i.e., by jamming.

2.1. Passive Attacks

In order to wiretap the optical path, direct physical access to the optical fiber is required. Two cases differing by the location at which the wiretapping device is installed, may be distinguished: at the network nodes, such as couplers/splitters, optical amplifiers, optical transfer multiplexers like optical add/drop multiplexers (OADMs), optical distribution boxes i.e., optical cross connects (OXC) or at any location along the fiber optic cable. While network nodes can be protected against unauthorized access by mechanical security or electronic supervision, it is impossible to effectively protect fiber optic cables spanning the distances of tens or even thousands of kilometers.

Two approaches to such an attack may be distinguished. The first one consists in installing an asymmetric 1×2 optical splitter along the optical fiber path. Alternatively, a cable theft attempt may be made to install the coupler and quickly restore the transmission restoration before an intervention is made.

Such a splitter is a small and inexpensive device that does not require any power supply. It has one optical input and two optical outputs. The device consumes, from the optical path, a small portion (10–20%) of the power of the transmitted signal and introduces only a slight attenuation increase in the legitimate path (less than 1 dB), which may be easily overlooked by the supervision system. It is easy to install during construction works, or may be placed in the so-called dark optical fibers which are not used for transmitting information yet. The situation is different if the path is used for data transmission, as the installation of a splitter requires cutting the optical fiber and welding its optical connectors. This interrupts the transmission and triggers alarms in the management system, allowing the location of the attack using fiber optic reflectometers (OTDR) to be determined.

The second method of eavesdropping does not require cutting the optical fiber. Here, having access to the fiber cable, the attacker removes its protective coating using commercially available stripping tools. With transparent coatings, the removal is not even necessary. Then, the bare fiber is inserted into a clip on the coupler device. It is a readily available piece of equipment that may be acquired for one thousand dollars and is used in normal operations to detect optical fiber transmissions. It is also used for maintenance purposes. The clip-on coupler takes a portion of the signal transmitted via the tapped fiber and directs it through an additional optical fiber, where it can be connected to an eavesdropping device. The clip-on coupler exploits the fact that in a sharply bent optical fiber, part of the light goes outside the fiber [4], [5]. An example of a clip-on coupler is shown in Fig. 1. It consists of a matched pair of clamps made of transparent plastic: the upper one is convex, while the bottom one is concave. The concave clamp has a V-shaped groove for precise positioning of the fiber. The GRIN fiber optic lens receives the leaked signal and is connected to another optical fiber. Typical commercial devices [6], [7] allow to achieve an insertion loss in the tapped fiber of not more than 7 dB at 1550 nm,

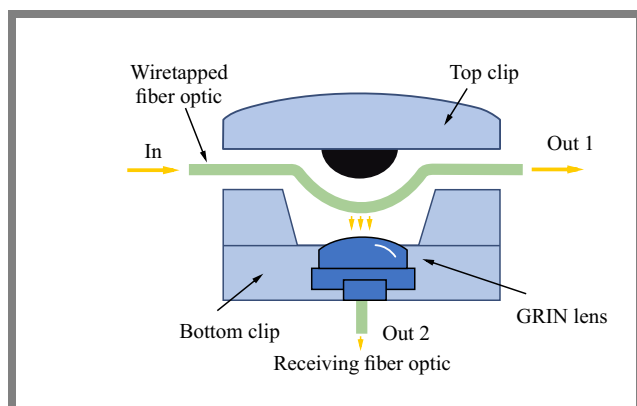


Fig. 1. Optical clip-on coupler.

(at 1310 nm, it equals only 3 dB) and coupling efficiency of 13–17 dB (1550 nm) and 17–22 dB (1310 nm). This parameter determined by how much the power of the intercepted signal is lower than the power of the signal in the tapped fiber. In this context, it is worth stressing that it is not always easy to make sure that the clip-on coupler operates as required, because the strength of the tapped signal depends on the bend sensitivity of the attacked fiber. Incorrect application may result in either too low a power level of the tapped signal or a high power loss of the useful signal in the original fiber. Due to the fact that the level of signal power decreases as the distance from the source increases, the installation of such a device near the transmitter is more vulnerable to wiretapping carried out in the manner described above.

If the link power budget is tight, e.g., it operates with a very low loss margin, eavesdropping using passive optical couplers and clip-on couplers may not be feasible at all. This is a consequence of additional link attenuation introduced by such devices, and stems from the fact that a certain portion of useful signal power is extracted in this process, meaning that consequently a smaller portion thereof reaches the receiver. The risk is that the loss of signal (LoS) alarm may be activated. For instance, on a relatively short fiber link (up to 10 km) operating with a tight loss margin budget of (2–3 dB), and with a sensitive APD receiver with attenuation set to such a level that there is no power signal margin available which could be extracted without any loss of signal quality at the receiver, the attacker cannot install any passive devices without raising an alarm. Only extremely low-loss devices may be used for this purpose and under such conditions. However, this means that the extracted weak signal must be amplified with an EDFA device to render it useful. This threat may be protected against by using signal wavelengths outside of EDFA bandwidth, e.g., 1310 or 1490 nm [8]. Alternatively, advanced methods may be relied upon to create a low-loss tap by polishing the fiber to gain access to its core, or Bragg grating writing may be used. However, all these methods are suitable for use in laboratory conditions and may be rather difficult to implement in the field. Unfortunately, a data link set up in this manner is very sensitive to jamming.

Another simple method of gaining access to signals transmitted via optical fibers is to connect to the optical monitoring ports present in all active devices within the optical network infrastructure, such as optical amplifiers, wave selective optical distribution boxes (WSS), or optical transfer add/drop multiplexers (OADM). Such a possibility of eavesdropping exists also in some passive network elements, e.g., optical splitters. In each of such cases, physical access to the device is required. Security problems of this nature occur in PON type access networks (GPON or GEAPON), especially for downstream transmissions, since all subscribers receive data sent to all other users due to the broadcasting nature of the communication. Therefore, encryption algorithms are used for securing the transmission. The upstream link, e.g., from subscribers to the data exchange, is not encrypted due to the directionality of the network's logical structure. As it turns out, this assumption is not entirely correct. In [9], it

was proved that a subscriber with legal access to the network may intercept the signal sent by another party in the reverse (upstream) direction. For this purpose, the signal reflected from the optical splitter through which both subscribers (the tapped and the eavesdropper) are connected to the PON network may be used. In [9], it was shown that the level of the reflected signal depends on the type of the splitter, the connectors (PC/APC) used and whether the said connectors are closed or open. By installing an optical amplifier and a receiver with a very sensitive avalanche-type photodiode (APD), the eavesdropper was able to flawlessly receive signals sent by the legitimate subscriber.

Having legal access to the network, it is also possible to eavesdrop on information using crosstalk signals between adjacent communication channels [10], [11]. The attacker legally leases a transmission channel with a given wavelength, and does not send any data there [12]. Without transmitting in the aforementioned wave channel, crosstalk signals from adjacent channels appear, which can be amplified and received [12]. This is possible in WDM multiplexing networks, where different wavelengths are used by many users.

2.2. Active Attacks

The purpose of active attacks is to disrupt or even block transmissions in part of or even in the entire network. Due to transparency of optical networks, attacks of this type tend to spread quickly beyond the attacked section of the network [13]. Two kinds of such a method may be distinguished. The first one involves physical damage to the infrastructure i.e., cutting a cable or destroying the equipment which is relatively easy to locate and repair.

The other type of intrusion is an action consisting in intentionally introducing a high-power jamming signal into the network, significantly stronger than typical signals used for transmission. It can be injected at the same positions as discussed in the wiretapping section, and may also be using the so-called alien channel.

The clip-on coupler can also be used to introduce an interfering signal to the receiving optical fiber, in the same manner as in eavesdropping. It should be mentioned that the attenuation of such an interfering signal in a clip-on coupler is in the range of 13–22 dB for commercially available equipment, depending on the transmission window. So, to effectively influence the transmission, the attacker must have a high-power light source.

To conduct the attack, a 2×1 optical coupler can also be inserted in the transmission path, directing a useful signal and interference to its inputs, but this can only be done confidentially at the installation stage. During normal operation, the insertion of such a device triggers appropriate alarms. However, the attacker may take the risk if they are able to restore traffic quickly.

Connecting a jamming signal to optical monitoring ports or to unused output ports in the network nodes is possible as well, but such an approach is less effective than tapping on the same ports. This is due to the fact that the interfering sig-

nal injected in this way will propagate to the transmitter, i.e., in the opposite direction to the useful signal [14], and only the part of the interfering signal that will be reflected in the network components, and will be concurrent with the useful signal, will pose a threat. Due to the high isolation levels offered by network infrastructures, the power level required to carry out an effective attack equals approximately +30 dBm or even more, which is very high value. The intruder will find it more beneficial to use device ports that are not suitable for eavesdropping, i.e., an unused input port on any type of an optical distribution box. In this case, a very high-power signal that is by approx. 20 dB stronger than a normal signal is used [15]. The jamming signal passing through the optical distribution box exploits crosstalk jamming and then appears not only on the output port to which it has been redirected, but also as a crosstalk signal on the port/ports to which the signal has been switched. Attacks of this type tend to spread beyond the network paths directly connected to the attacked switch, although it should also be noted that as they propagate in the network, their impact weakens [16].

Judging by the position of the interfering signal band versus the interfering signal, all attacks can be categorized as out-of-band attacks if the ranges of the mentioned bands are different, and as in-band attacks if both signals are within the same frequency range.

In-band attacks are more dangerous than out-of-band attacks, because out-of-band attacks can be easily eliminated by using pass-only optical filters. In-band attacks cannot be prevented in this way. Additionally, in an out-of-band attack, both signals (jamming and useful) are incoherent, which means that their powers add up, and no mixing of both frequencies takes place in the optoelectronic detector. In contrast, with an in-band attack, the two signals add coherently i.e., their amplitudes are added, taking into account their phase difference. As a result, intermodulation components of both frequencies appear at the receiver. Therefore, the power of the attacker signal required to interfere with the transmission is relatively low.

In-band attacks can be conducted both directly and indirectly. In the first case, the interfering signal is introduced in the same transmission path as the channel being the target e.g., through the previously discussed clip-on coupler. Indirect attacks, in turn, use channel crosstalk in the network nodes, such as distribution boxes.

A special type of the out-of-band attack is the gain competition in optical amplifiers, including EDFA amplifiers [17]. This type of attack exploits the fact that the introduction of a very high optical power of the attacking signal to the input of the optical amplifier reduces the amplification gain in the other device channels, which in turn reduces their optical signal-to-noise ratio (OSNR), leading to a deterioration in the quality of service or even to interruption of the transmission. The competition gain attack can be difficult to control if the optical power is additionally modulated by amplitude keying, with the appropriate frequency in the attack channel [18]. Due to the time delays affecting the gain control loop in the amplifiers and in the optical receivers, amplitude keying may lead

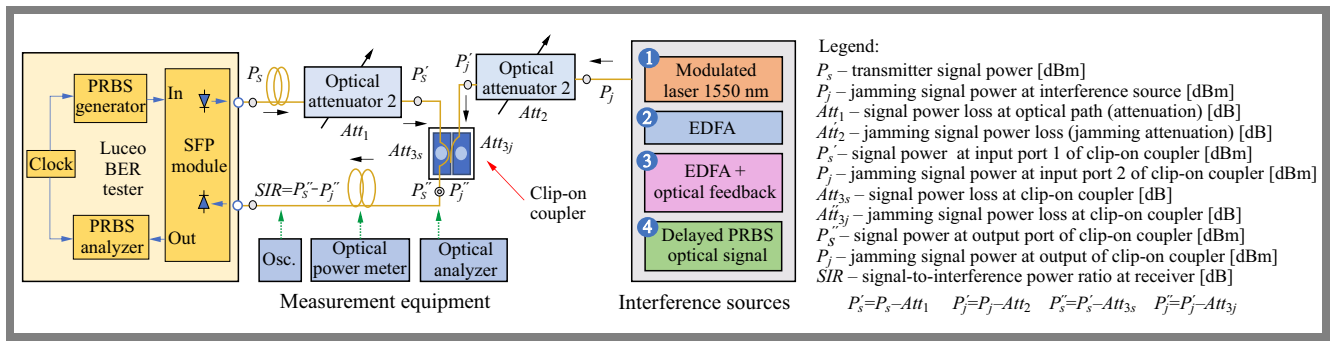


Fig. 2. Block diagram of the measurement setup.

to unstable operation caused by gain variations [18], which temporarily lowers the OSNR in the usable channels below the minimum value, thus causing a distortion in receiver circuits. The effects of an active attack involving disruption of the transmission are obvious and visible to the control room via QoS or BER metrics. The problem is that it is difficult to distinguishing between an attack and a hardware failure and to discover the location of the damage. The injection of a jamming signal to unused ports of an optical cross junction box, as well as the addition of optical splitters are practically impossible to discover using a reflectometer. Signal jamming may be combined with eavesdropping/tapping to launch a very effective attack, namely correlated jamming, in which case the attacker taps the signal and then injects interference downstream, by means of clip-on couplers. Here, the total power propagating in the optical fiber remains unchanged, thus preventing loss of signal (LoS). To conceal the jamming, the attacker may also use a part of the useful signal and introduce a delay (or multiple delays) and may then inject the delayed signal back to the optical fiber, which looks, at the receiver side, like naturally occurring multiple reflections (multipath). The traces of tapping usually visible in OTDR may be difficult to differentiate from other sources of attenuation/reflection, such as splices and fiber bends.

3. Experimental Setup

The goal of this research was to use the clip-on coupler in an active attack aiming to degrade services. The bit error rate (BER) determined for several types of jamming signals was used as a signal degradation measure. To do this, we connected a light source instead of the receiver at an extra fiber termination, simultaneously reversing the coupler’s direction. In this way, we were able to insert the interfering signal into the operating fiber link towards the receiver. The block diagram of the model and the measurement setup are shown in Fig. 2. The central part of the setup is the bit error rate tester (BERT Luceo Ebert 6), serving both as the transmitter and receiver of the tested link. A pseudo-random bit sequence (PRBS) of $2^{15} - 1$ length (L-6001-EPG10-6) was generated using a 1.25 Gb/s modulation rate (L-6001-CLK20-2) that drove a 1550 nm laser i.e., LightOptics SFP 1.25 G 1550 nm 40 km LO-SF-1G-EX. Such a modulation scheme was selected,

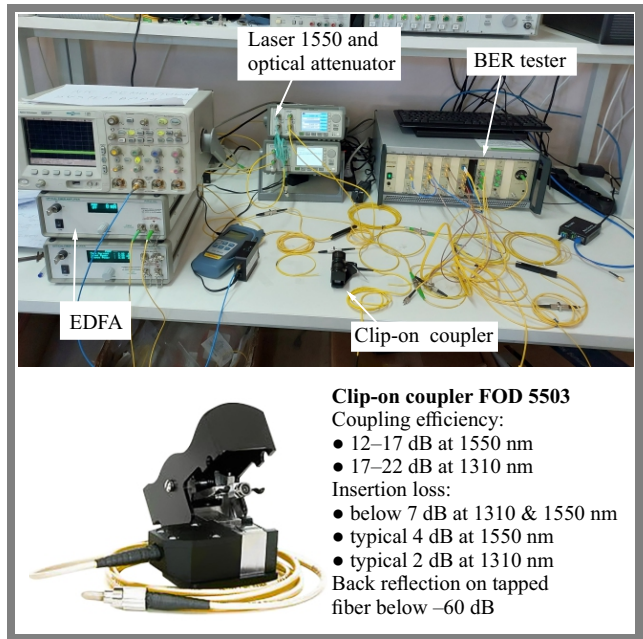


Fig. 3. Image of the test stand and specification of the clip-on coupler used.

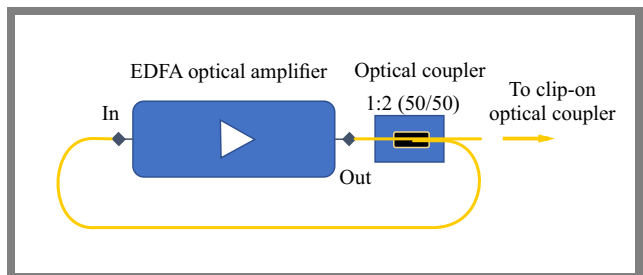


Fig. 4. EDFA amplifier with optical feedback.

as it is typical in subscriber access and LAN networks. The optical signal was fed from the transmitter to an adjustable optical attenuator (Agilent 8163B) that modeled variable link losses. Next, the useful signal was transferred to the clip-on coupler (Fig. 3).

Next, an interfering signal was fed to the third optical port of the coupler. The setup allowed for the adjustment of power for both the useful signal and optical interference. Then, the combined signals were transferred to the optical input of the BER tester. In the setup used, an optical power meter (OPM-0681550) may be connected ahead of the BERT receiver.

4. Results

The measurement results are depicted in Fig. 9, where BER is shown against SIR for various types of interference and different useful optical signal powers at the receiver. The obtained curves are quite typical, with each type of interference being characterized by similarly shaped curves, but not being identical. This means that a sole SIR value cannot entirely describe the receiver's behavior, since it does not take into account the receiver noise. Thus, BER depends also on the ratio of the useful signal power to the receiver noise power, which is a function of the signal power and not SIR.

5. Discussion

Figure 9 proves that the SIR level required to effectively affect the transmission is very low, i.e., high interference level is required. This is even more pronounced, considering the rather high attenuation of the clip-on coupler (typically 17–22 dB [5], [6]) inserted by the attacker and affecting the interference signal. Considering the permissible losses of many contemporary optical fiber links, which are in the 20–30 dB range, the attenuation of the interfering signal introduced by the clip-on coupler does not prevent it from jamming the link. The differences in the efficiency of various jamming signals stem from how the interference affects the receiver's operation.

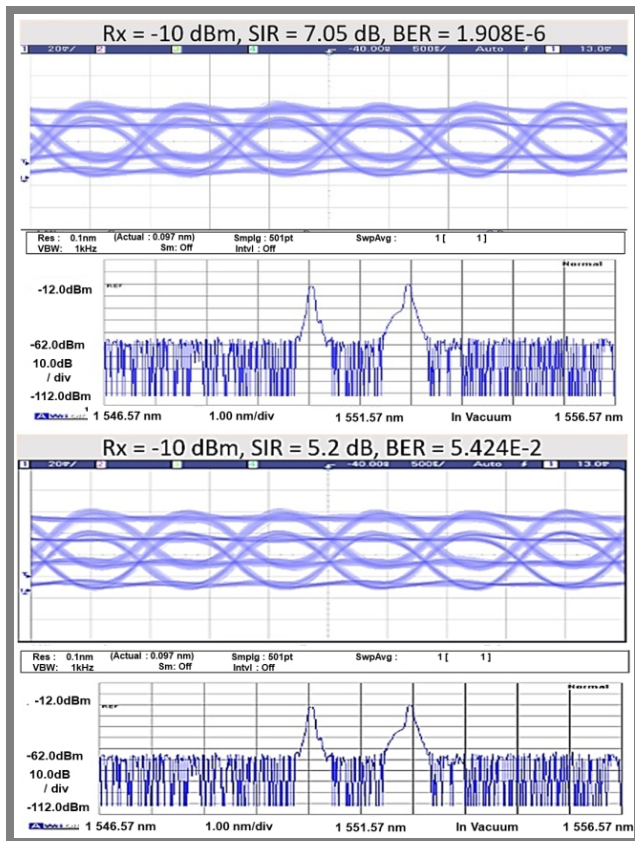


Fig. 5. Eye diagrams and spectra of the received signal for laser modulated with a 1 MHz rectangle shape waveform as source of interference.

Thanks to this, the optical powers of the data signal and interference could be measured separately. Alternatively, an Agilent DSO6104A 1 GHz 4 GS/s oscilloscope and an Anritsu MS9740A optical spectrum analyzer may be connected to visualize the waveform and optical spectrum of the received signal. By varying either the signal or interference attenuation, we were able to change the SIR of useful signal and measure the corresponding BER values. Four types of interfering signals were used in the course of the measurement campaign:

- 1550 nm laser modulated with a 1 MHz rectangular wave;
- optical wideband noise generated by an EDFA amplifier (Pritel FA-23), where the interference level was varied by changing the EDFA pump current;
- optical interference generated by the EDFA amplifier with optical feedback in the configuration shown in Fig. 4. Compared with the previous case, the interfering signal generated had a much narrower spectrum;
- 1.25 Gb/s optical PRBS signal, with a delayed version of the original BERT PRBS used to avoid cross-correlation between the signal and interference.

The representative instances of the received signal time forms and the optical spectra obtained for all four types of interference applied are shown in Figs. 5–8, respectively.

The optical spectra and jamming signals do overlap, because a delayed version of the useful signal was used as the interference (Fig. 8).

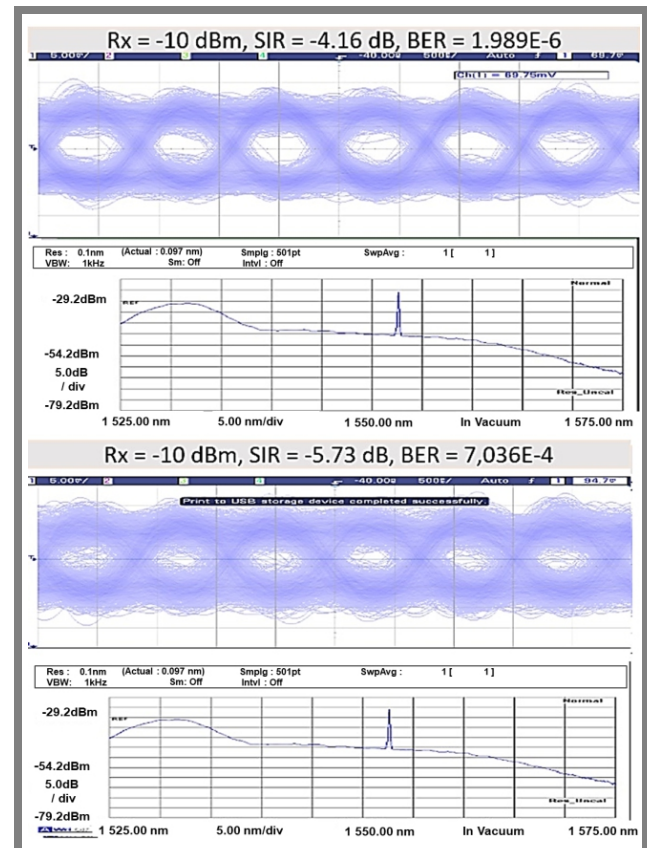


Fig. 6. Eye diagrams and spectra of the received signal EDFA wideband optical noise as interference.

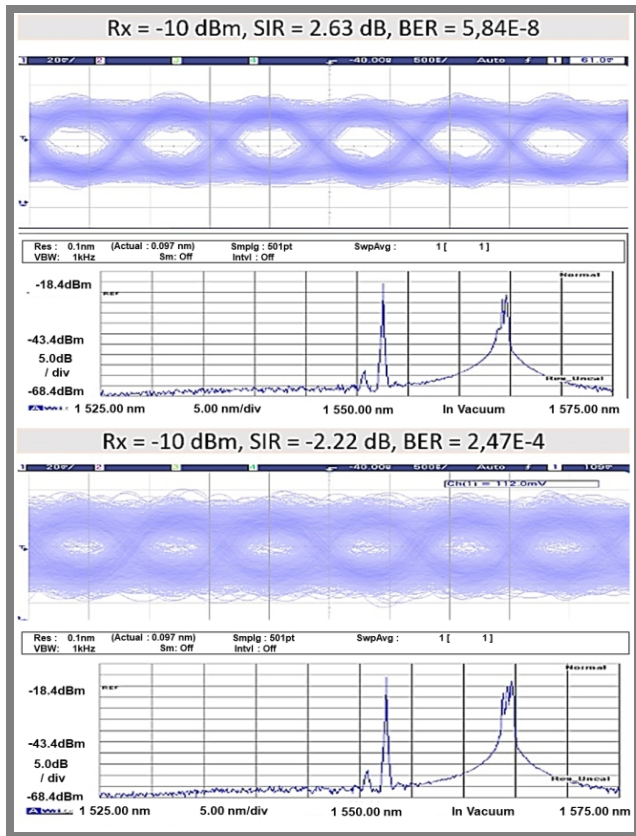


Fig. 7. Eye diagrams and spectra of the received signal for EDFA with an optical feedback signal.

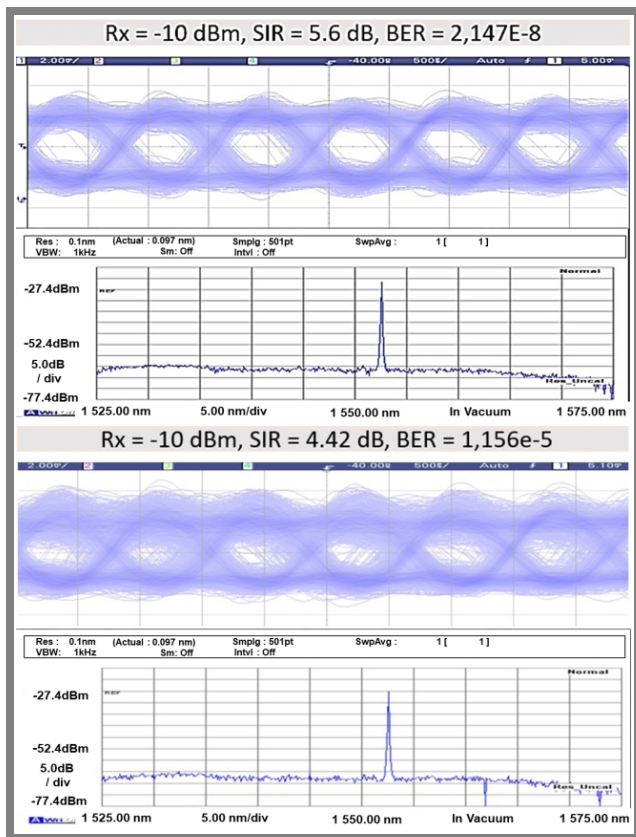


Fig. 8. Eye diagrams and spectra of the received signal for 1.25 Gb/s optical PRBS as interference signal.

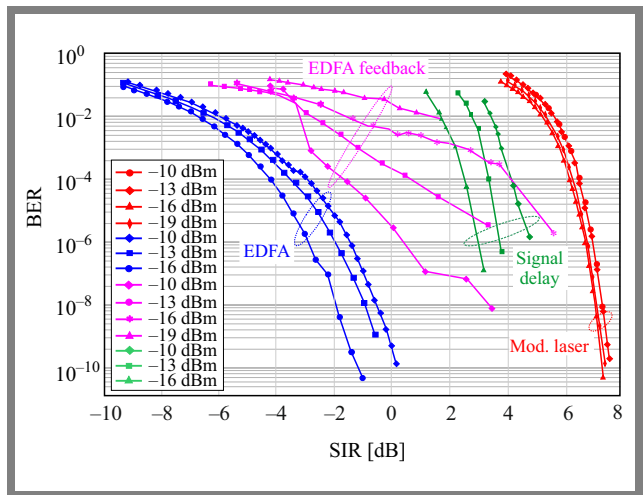


Fig. 9. BER vs. SIR for various types of interference induced.

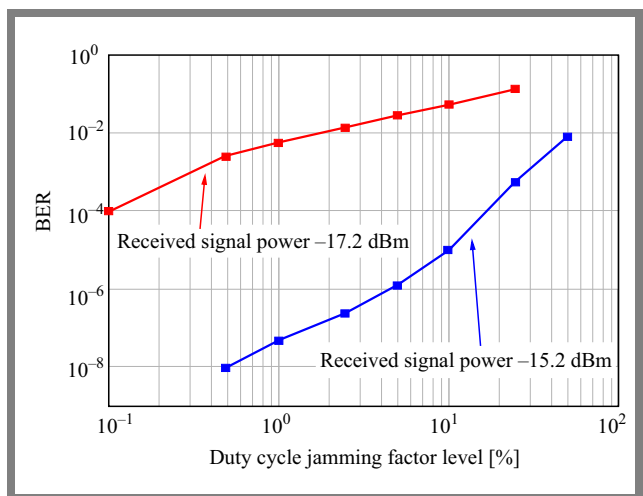


Fig. 10. Typical results of BER vs. jamming signal duty cycle measurements for useful signal powers of -17.2 dBm (upper curve), and -15.2 dBm (lower curve), and the jamming signal power of -16.8 dBm for a 50% duty cycle (all measured at the receiver).

The DC offset of the jamming signal may change the operating point of the receiver photodiode and the front-end stage. It is the least dangerous case, because the optical power required to saturate the receiver input is usually high.

Moreover, if the interference signal is of the noisy type or varies fast, it is moved into the electrical passband of the receiver via a photodetector. Then, the receiver's signal-to-interference + noise ratio (SINR) is reduced, which affects BER.

Let us consider a case in which interference is transferred from the optical to the electrical domain.

The rule is that the photodetector current is proportional to the optical power. This implies that the electrical power is proportional to the square of the optical power, meaning that photodetection is a nonlinear process. Let us assume that an interfering optical signal is added to the optical data signal and their sum is photo detected. Apart from the data signal, the sensor is affected by electrical interference resulting from the mix of optical interference and data signal. The quadratic detection method is why the electrical interference spectrum

is a product of mixing two signals. Therefore, the optical and electrical spectra are tightly linked. In particular, the higher optical bandwidth of the interference, the broader the electrical spectrum of the jamming signal. Let us assume we have two optical jamming signals with the same power but different optical bandwidths. Then, after photodetection, the one with a lower bandwidth will approximately preserve it in the electrical domain and will have a greater electrical spectral density. Therefore, interference with a higher power would pass through the filter in the receiver, affecting its operation to a greater extent than in the case of the signal with a wider bandwidth. When comparing various optical jamming techniques, the most dangerous is the one with a narrower interference spectrum. The DC offset is mostly irrelevant.

The above conclusions are illustrated by the results shown in Fig. 9. In the case of EDFA optical noise, optical bandwidth of the interfering signal is the widest (Fig. 6) and, hence, its interference impact is the lowest. The noise spectrum of the EDFA with the feedback shown in Fig. 7 is more compact; in such a case, this type of interference exerts a bigger impact. The worst scenario involves a signal occupying the same bandwidth as the useful one (here, it is the delayed version of the data signal), because apart from its DC component, the rest of its spectrum lies within the receiver's bandwidth.

Papers [14], [18] prove that the most dangerous attack consists in adding a relatively slowly modulated interference to the data signal. Here, it is a 1 MHz rectangular wave form. The same conclusion may be drawn from Fig. 9. Such a signal may additionally interact with the receiver's gain control circuit, causing extra errors.

Since the modulated laser is the most efficient jamming source, we tried to establish how the modulated signal's duty cycle impacts this efficiency. We employed a setup similar to that shown in Fig. 2. This time, a 5 Gb/s pseudo-random bit sequence (PRBS) was used as the useful signal, whereas a 1550 nm laser modulated with an adjustable duty cycle 10 MHz rectangular wave was the jamming source. The experiment proved that the 50% duty cycle deteriorated the BER value the most. Examples of results are shown in Fig. 10. Such a behavior came as no surprise, because the higher duty factor caused a rise in the jamming signal power.

6. Conclusions

In this paper, we have proved that the clip-on coupler may be used not only for passive attacks (data tapping), but also for active attacks resulting in partial or complete jamming. No advanced equipment is necessary. Apart from the coupler itself, only a slowly modulated laser source is required. Moreover, no physical access to the network nodes is needed — any location with access to the fiber cable is sufficient. Once installed, the jamming circuit may be left inactive and may be activated at any time in the future. Therefore, detecting such inactive devices and determining their location is of utmost importance for network security. It may not pose a problem if a clip-on coupler similar to the one used in

our experiment is used. Such a device has an insertion loss of a few decibels and may be relatively easily detected and located by an optical time domain reflectometer. However, military/intelligence grade clip-on couplers allegedly have much lower insertion losses (0.5 dB according to [18]), and their detection/localization may be quite difficult.

Another problem is the proper reaction i.e., identification and localization to the ongoing attack. Both issues should be the topics of further research. We should emphasize that the jamming signal would be most probably delivered from a location other than the tapping point, as the respective equipment needs a power supply and may be bulky, and this requires the associated jamming signal transmission losses to be considered. However, this does not mean that the issue of protecting optical networks against attacks was not investigated in the literature in the past. Therefore, a short summary of the state-of-the-art is included below.

Due to the variety of attacks that can be carried out and their differing impact on network transmissions, the detection and identification of threats at the physical layer is a great challenge, because those attacks differ significantly from conventional network failures [13]. First of all, attacks can appear randomly at any point [13]. The intruder may avoid simple detection methods that are not sensitive enough to detect minor transmission quality degradation [13].

Furthermore, an attack that was mistakenly identified as a component failure may continue to propagate through the network, causing additional failures and triggering further alarms [13]. Another difficulty is that due to the transparency of optical networks [3], not all of their nodes are monitored, which makes it easy for attacks to spread and makes it difficult to locate the injection point. To detect an intrusion, one may rely on standard equipment used to monitor optical paths. It allows to measure the level of the transmitted and received signal and, in some cases, path attenuation. Any changes in one of these parameters exceeding a threshold value raise an alarm. The problem is that an attacker can effectively disrupt the transmission without influencing the monitored parameters in such a way that would trigger the alarm.

Another tool that can be used to examine the integrity of the optical path is an optical time domain reflectometer (OTDR). In addition to determining attenuation, reflectance, and component's location, the device is also capable of detecting any changes in the optical parameters of the link caused, for example, by the addition of hostile devices. By default, OTDR works with a path in which no other transmission is carried out, but this limitation can be overcome by using different wave ranges for transmission and OTDR and by introducing a wave coupler/splitter (WDM). However, OTDR is an expensive device, and it is hard to imagine a case in which each fiber optic path is permanently connected to its own OTDR that checks the integrity of the system.

Another device that can be used to detect an attack is an optical spectrum analyzer (OSA) [19]. It allows to detect variations in the shape of the signal spectrum, even if the total optical power remains unchanged. However, the use of this equipment requires comparing spectrum samples from dif-

ferent time periods, which slows down the analysis process. Moreover, OSAs are expensive devices, which makes them unsuitable for ensuring security on larger scale networks. Another solution is to rely on well-designed fiber optic cables [20]. In the first variant, the transmission fiber is surrounded by optical fibers carrying monitoring signals only. Any attempt to reach the internal fiber leads to a loss of power of the monitoring signals and triggers an alarm. The second variant involves the integration of electrical conductors into a fiber optic cable. Any interference with the cable causes capacitance variations between these conductors and triggers an alarm. Another possibility is to use an optical fiber that breaks while bent [3], which makes the use of the clip-on coupler impossible/difficult. Finally, the optical fiber itself can be designed in a way that prevents devices such as a clip-on coupler from being attached unnoticed [22]. Another option for continuous monitoring of the state of the optical path is the transmission of a pilot tone or tones [19], [22] using different wavelengths. In such a scenario, bending will cause significant difference in attenuation of the pilot signals. Since network-related threats are very complex and highly variable, machine learning (ML) methods [23], [24] seem to be an adequate tool for ensuring a proper level of security. In this approach, typical optical parameters monitored by coherent transceivers during their normal operation are used as input for ML algorithms. The detection and identification of the attack itself is treated as a classification problem. For the 8 tested classification methods, the best results were obtained using artificial neural networks, which are characterized by an accuracy level of over 99.9% [23]. They are capable of detecting and identifying high and medium intensity jamming attacks with 100% precision [23]. In [23], the important role of selecting a subset of monitored parameters was pointed out. Other works, e.g. [15], indicate that it is possible to detect the sources of attacks (in this case based on crosstalk) using a relatively small number of monitoring components in selected network nodes [15], and present suitable node preselection methods.

An alternative approach to the security of optical networks is to design them in such a way as to minimize the effects of potential attacks [11], [25]. Such a process involves the selection of routing and wavelength assignment algorithms at the network planning stage to limit the interaction between optical channels and, consequently, the propagation of attacks within the network [11], [25]. This is a complex optimization problem and, hence, the authors of [25] formulated it as an integer linear programming problem (ILP) and showed that simulated annealing is a good heuristic algorithm in this case. The proposed routing and wavelength assignment methods significantly limit the ability of an attack to propagate within the network and limit its impact on network operation [25]. A similar approach was presented in [11], where attempts were made to minimize the risk of cross-channel attacks in a WDM network. An optimal algorithm was developed there, with scalability with the network size, and for larger networks – a heuristic approach was adopted as well in the form of a reduced overlapping paths routing algorithm (ROPRA). This

methodology also includes [3] an appropriate design of the network architecture itself, and its protection ensuring that, if necessary, the attacked path can be switched to a reserve one. The simplest example of such an architecture is a ring, which always offers two different routes between two nodes.

Acknowledgments


The authors gratefully acknowledge the financial support from the Warsaw University of Technology under grant no. 1820/341/Z01/POB3/2021.

References


- [1] Opterna and iDefence, “Threats to Fiber Optic Infrastructures”, *A Blackhat Federal Briefing, Tech. Rep.*, 2003 [Online]. Available: <https://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-gross-up.pdf>
- [2] Deloitte, “Tapping of Fiber Networks”, *Deloitte Touche Tohmatsu Ltd., Tech. Rep.*, 2017 [Online]. Available: https://zybersafe.com/wordpress/wp-content/uploads/2017/04/Deloitte_Fiber_tapping_Q1_2017_English.pdf
- [3] M. Medard, D. Marquis, R.A. Barry, and S.G. Finn, “Security Issues in All-optical Networks”, *IEEE Network*, vol. 11, no. 3, pp. 42–48, 1997 (<https://doi.org/10.1109/65.587049>).
- [4] T. Uematsu, H. Hirota, T. Kawano, T. Kiyokura, and T. Manabe, “Design of a Temporary Optical Coupler Using Fiber Bending for Traffic Monitoring”, *IEEE Photonics Journal*, vol. 9, no. 6, 2017 (<https://doi.org/10.1109/JPHOT.2017.2762662>).
- [5] H. Hirota *et al.*, “Optical Cable Changeover Tool with Light Injection and Detection Technology”, *Journal of Lightwave Technology*, vol. 34, no. 14, pp. 3379–3388, 2016 (<https://doi.org/10.1109/JLT.2016.2568221>).
- [6] Go4Fiber Ltd., “PFC 1000, Passive Fiber Clip-on Coupler”, Tech. Specification, Available: https://spec.go4fiber.com/testing_equipment/pfc_1000.pdf
- [7] Fiber Optic Devices Ltd., “Clip-On Coupler FOD5516”, Tech. Specification, Available: <https://www.fods.com/pdf/4/5516DS.pdf>
- [8] A. Salim, S.S. Carroll, and J. Atai, “Limits of Intrusion Detection Systems in a Gigabit Optical Link”, *Optical Engineering*, vol. 49, no. 4, pp. 1–4, 2010 (<https://doi.org/10.1117/1.3407426>).
- [9] C. Mendonca, M. Lima, and A. Teixeira, “Security Issue Due to Reflection in PON Physical Medium”, *14th International Conference on Transparent Optical Networks (ICTON)*, Coventry, UK, 2012 (<https://doi.org/10.1109/ICTON.2012.6254487>).
- [10] M.P. Fok, Z. Wang, Y. Deng, and P.R. Prucnal, “Optical Layer Security in Fiber-optic Networks”, *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 725–736, 2011 (<https://doi.org/10.1109/TIFS.2011.2141990>).
- [11] S. Yuan and D. Stewart, “Protection of Optical Networks Against Inter-channel Eavesdropping and Jamming Attacks”, *International Conference on Computational Science and Computational Intelligence*, Las Vegas, USA, 2014 (<https://doi.org/10.1109/CSCI.2014.14>).
- [12] S. Krishnan and A. Borude, “Security Issues in All-optical Networks”, *Annual SRII Global Conference*, San Jose, USA, 2011 (<https://doi.org/10.1109/SRII.2011.108>).
- [13] R. Rejeb, M.S. Leeson, and R.J. Green, “Fault and Attack Management in All-optical Networks”, *IEEE Communications Magazine*, vol. 44, no. 11, pp. 79–86, 2006 (<https://doi.org/10.1109/MCOM.2006.248169>).
- [14] D. Dahan and U. Mahlab, “Security Threats and Protection Procedures for Optical Networks”, *IET Optoelectronics*, vol. 11, no. 5, pp. 186–200, 2017 (<https://doi.org/10.1049/iet-opt.2016.0150>).
- [15] T. Wu and A.K. Somani, “Cross-talk Attack Monitoring and Localization in All-optical Networks”, *IEEE/ACM Transactions on Networking*, vol. 13, no. 6, pp. 1390–1401, 2005 (<https://doi.org/10.1109/TNET.2005.860103>).

- [16] Y. Peng, K. Long, Z. Sun, and S. Du, "Propagation of All-optical Crosstalk Attack in Transparent Optical Networks", *Optical Engineering*, vol. 50, no. 8, 2011 (<https://doi.org/10.1117/1.3607412>).
- [17] T. Deng and S. Subramaniam, "Analysis of Optical Amplifier Gain Competition Attack in a Point-to-point WDM Link", *Proc. of SPIE*, vol. 4874, pp. 249–261, 2002 (<https://doi.org/10.1117/12.475302>).
- [18] N.S. Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical Layer Security in Evolving Optical Networks", *IEEE Communications Magazine*, vol. 54, no. 8, pp. 110–117, 2016 (<https://doi.org/10.1109/MCOM.2016.7537185>).
- [19] National Communications System, "All-optical Networks", *Technical Information Bulletin 00-7*, 2000 <https://www.hsdl.org/?view&did=440833>.
- [20] M.Z. Iqbal, H. Fathallah, and N. Belhadj, "Optical Fiber Tapping: Methods and Precautions", *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, Riyadh, SA, pp. 164–168, 2011 (<https://doi.org/10.1109/HONET.2011.6149809>).
- [21] European Patent Office, "Optical Fiber Design for Secure Tap Proof Transmission", Bulletin 2004/30, European patent application EP1256826A2, 2004 [Online] Available: <https://data.epo.org/gpi/EP1256826A2-Optical-fiber-design-for-secure-tap-proof-transmission>
- [22] K. Shaneman and S. Gray, "Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for Detection and Prevention", *IEEE Military Communications Conference MILCOM*, Monterey, USA, 2004 (<https://doi.org/10.1109/MILCOM.2004.1494884>).
- [23] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and M. Furdek, "Experimental Study of Machine-Learning-Based Detection and Identification of Physical-Layer Attacks in Optical Networks", *Journal of Lightwave Technology*, vol. 37, no. 16, pp. 4173–4182, 2019 (<https://doi.org/10.1109/JLT.2019.2923558>).
- [24] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and M. Furdek, "Field Demonstration of Machine-Learning-Aided Detection and Identification of Jamming Attacks in Optical Networks", *European Conference on Optical Communication (ECOC)*, Rome, Italy, 2018 (<https://doi.org/10.1109/ECOC.2018.8535155>).
- [25] K. Manousakis and G. Ellinas, "Attack-aware Planning of Transparent Optical Networks", *Optical Switching and Networking*, vol. 19, pp. 97–109, 2016 (<https://doi.org/10.1016/j.osn.2015.03.005>).


Marcin Kowalczyk, D.Sc.

Faculty of Electronics and Information Technology
 <https://orcid.org/0000-0001-6137-0580>
 E-mail: Marcin.Kowalczyk@pw.edu.pl
 Warsaw University of Technology, Warsaw, Poland
<https://www.elka.pw.edu.pl/eng>

Michał Marzecki, Ph.D.

Faculty of Electronics and Information Technology
 <https://orcid.org/0000-0002-8526-7622>
 E-mail: Michal.Marzecki@pw.edu.pl
 Warsaw University of Technology, Warsaw, Poland
<https://www.elka.pw.edu.pl/eng>

Jerzy Siuzdak, Prof.

Faculty of Electronics and Information Technology
 <https://orcid.org/0000-0003-3829-2160>
 E-mail: Jerzy.Siuzdak@pw.edu.pl
 Warsaw University of Technology, Warsaw, Poland
<https://www.elka.pw.edu.pl/eng>