jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 4, PP. 969–977
Manuscript received June 27, 2024; revised October 2024. doi: 10.24425/ijet.2024.152084

Jamming of optical network operation in physical layer

Jerzy Siuzdak, Marcin Kowalczyk, and Michał Marzecki

***Abstract*—The paper presents the existing possibilities of disrupting the operation of optical/optoelectronic telecommunication networks in a physical layer, distinguishing between passive and active attacks. The latter relay on jamming the operation of the optical network, ranging from the deterioration of the quality of service to the complete prevention of transmission. Passive attacks, on the other hand, are aimed at eavesdropping on transmissions. The paper discusses the various types of attacks, which are specific to the physical layer of optical networks, as well as capabilities of detection and prevention them based on the machine learning approach among others. Finally, a realistic scenario of an active attack by using of a clip-on coupler has been examined in the context of a local area optical network. The results confirm a very disruptive impact on the transmission quality if the power of the jamming signal is comparable with the power of useful signal.**

***Keywords*—jamming and transmission eavesdropping; optical network security; passive and active attacks; physical layer attacks; prevention with machine learning**

I. Introduction

At first glance, fiber optic communications seem safer than radio or wired communications using metal (copper) cables. On the one hand, it is due to the lack of the so-called electromagnetic corona, i.e., the impossibility of remotely eavesdropping on information transmitted in a fiber optic cable, and on the other hand, the impossibility of remotely disturbing fiber optic transmission, as it is not sensitive to Electro Magnetic Interference (EMI). It creates a false belief in the complete security of this type of information transmission [1], [2]. It should be clearly stated that the security of fiber-optic transmission ends when the attackers gain direct, physical access to the fiber-optic cable itself or optical/optoelectronic devices located in the fiber-optic path or network nodes.

The active attacks aim to disrupt the operation of the network, ranging from deterioration of the quality of services (QoS) to ultimately preventing transmission in a single link or part of the network. The attacker tries to mask the place or places of the attack. Therefore, such an attack is not easy to distinguish from an event involving the failure of some network element.

The work has been financed by internal grant of the Warsaw University of Technology No. 820/341/Z01/POB3/2021.

J. Siuzdak, M. Kowalczyk, and M. Marzecki are with Warsaw University of Technology, Warsaw, Poland (e-mail: {Jerzy.Siuzdak, Marcin.Kowalczyk, Michal.Marzecki}@pw.edu.pl).

In this work, we will discuss the more important types of attacks one by one, starting with passive attacks (eavesdropping). It should be noted, however, that we will limit ourselves only to attacks in the physical layer, specific to the optical transmission medium such as optical fiber. Attacks carried out at higher OSI layers, although they may affect optical systems, will not be discussed here. Examples of the latter include security threats occurring in the GPON network [3]–[5]: intercepting network control messages (PLOAM - Physical Layer Operation Administration and Maintenance) and changing or resending them to the network, impersonating other users (ONU - Optical Network Unit, or OLT - Optical Line Termination), and finally, theft of services, which can be done by a user impersonating another ONU.

II. Eavesdropping

As already mentioned, one needs physical access to the optical infrastructure to install wiretapping. Generally, we can distinguish two cases resulting from the place of installation of the wiretapping: the first one - anywhere in the fiber-optic cable and the second one - in the network nodes containing elements such as couplers/splitters, optical amplifiers, optical add-drop multiplexers (OADMs), or optical cross-connects (OXCs). While network nodes can be made reasonably safe against unauthorized access by increasing the protection of these places (e.g., mechanical security, electronic supervision), this is impossible in the case of fiber-optic cables that run for tens or even thousands of kilometers. Therefore, we will start discussing eavesdropping methods with wiretapping on fiber-optic cables.

A. Eavesdropping in fiber optic cables

There are two main attack methods here. The first involves installing an asymmetrical 1x2 optical splitter in the fiber optic path. Such a splitter is an inexpensive and small device that does not require a power supply and has one optical input and two optical outputs. A specific, usually small (e.g., 10% or 20%) part of the power of the signal is transmitted from the optical path to the attacker's receiving device by using of it. Such a device introduces only slight attenuation in the path (less than 1 dB), which the supervision system can easily overlook. It is easy to install at the infrastructure construction stage or the so-called dark fiber (on which transmission still needs to be carried out). The situation is different when the fiber is used for

data transmission because installing such an element requires cutting the optical fiber and welding/connecting the splitter in its place. It interrupts the transmission, triggers relative alarms in the network management system, and allows for accurate determination of the place of attack, e.g., using fiber optic time domain reflectometers (OTDR).

The second method of eavesdropping is more dangerous because it does not require cutting the optical fiber, which may trigger alarms. According to this method, the attackers act as follows. Having access to a fiber optic cable, they identify the optical fiber of interest. Next, they remove all coatings protecting the optical fiber over a certain length, leaving the bare fiber without cutting it. Tools intended for this purpose (fiber optic stripping tools) are commercially available and inexpensive, as they are used in routine installation works (e.g., connecting optical fibers). In many cases (transparent coatings), their removal is unnecessary. Having a sufficiently long section of the bare fiber available, the attacker inserts it into a so-called clip-on coupler. The device is readily available since it is used regularly to detect optical transmission in fiber optics and for service communications. The clip-on coupler taps a part of the signal transmitted in the eavesdropped fiber into an additional optical fiber that can be connected to other attacker devices.

The clip-on coupler employs the fact that in a sharply bent optical fiber, some of the light goes outside the fiber. The exact structure of this type of device is described in [6]–[8]. The scheme of the clip-on coupler is shown in Fig. 1 [6].

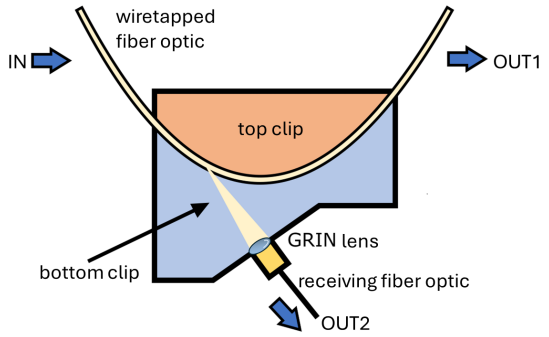

Fig. 1. An optical clip-on coupler schematic

It consists of a matched pair of clamps made of transparent plastic: convex and concave. The concave clamp is a V-shaped groove that allows accurate optical fiber positioning (in a 250 µm diameter clear coating). A gradient-index optics fiber optic lens (GRIN) is used to receive the signal. It is connected to an optical fiber, sending the received signal outside. The solution presented in [6] employs a multi-mode optical fiber, but single-mode optical fibers are also found in commercial devices. The GRIN lens is glued in a place that absorbs the largest power of light leaking from the telecommunications fiber. The choice of the radius of curvature is also essential: the smaller it is, the greater the attenuation of the signal remaining in the telecommunication's optical fiber, but at the same time, the greater the power transferred outside the optical fiber. Typical parameters of commercial devices [5], [9] are insertion loss (in tapped fiber) not exceeding 7 dB (at 1550 nm, at 1310 nm it is much lower, e.g., 3 dB) and coupling efficiency of 13 -17 dB (1550 nm) and 17 -22 dB (1310 nm). The last parameter indicates the attenuation of the eavesdropped signal with regard to the input signal in the tapped fiber. The values of these parameters depend on the wavelength, which results from the corresponding changes in the mode field diameter (MFD). At a wavelength of 1550 nm, the diameter of the mode field is larger, causing a stronger coupling of the guided mode(s) to the cladding and, consequently, a higher power of the tapped signal and a more significant attenuation of the useful signal in the tapped fiber.

Because the signal power level decreases during propagation, places near the transmitter are more vulnerable to eavesdropping in the manner described above.

In the open sources, one can find descriptions of using clip-on couplers to monitor/eavesdrop on transmitted data. We will briefly describe two examples here [8], [11]. In the first experiment, video transmission over optical Ethernet was eavesdropped [11]. After removing the coatings, the bare optical fiber was placed in the clip-on coupler. The signal acquired in this way was fed via an additional optical fiber to a unidirectional Ethernet signal converter, where the Ethernet frames were captured (via the Wire-Shark protocol analyzer). Then, the video transmission was successfully reconstructed from them (using the Chaosreader) on the attached computer, where it could later be replayed. All components required to carry out the attack (especially software) were readily available [11]. In the other work [8], the signal obtained from eavesdropping was used to monitor traffic in the Gigabit Ethernet PON network (GEPON). With a signal extraction efficiency of -17 dB (using a clip-on coupler), the captured signal's bit error rate (BER) was measured. The obtained results indicated no loss of quality of this signal.

B. Eavesdropping in network nodes

Another relatively simple method of gaining access to signals transmitted in optical fiber is to connect an eavesdropping device to optical monitoring ports, which are present in virtually all active optical network devices, such as optical amplifiers, optical wavelength selective switches (WSS), or optical add-drop multiplexers (OADM). This possibility of eavesdropping also exists in some passive network elements, e.g., optical splitters. In the latter, one can connect to one of the output ports as long as it is not used.

If one has more advanced equipment, one can eavesdrop on the signal while having legal access to the network. This problem occurs in PON access networks (e.g., GPON or GEPON). It is well known for the downstream transmission (i.e., from the exchange office to the subscribers), as all subscribers receive data sent to all other subscribers due to the broadcasting nature of the transmission. For this reason, encryption algorithms should be used for transmission privacy. Transmission in the reverse direction (up-stream) is usually not encrypted due to the directionality of the network. As it turns out, this assumption needs to be corrected. In [12], it was shown that a subscriber with legal access to the network

can eavesdrop on the signal sent in the reverse direction by an-other subscriber(s). For this purpose, the signals reflected from the optical splitter (connecting both the eavesdropped subscriber and the eavesdropper to the PON net-work) may be used. In [12], it was shown that the level of the reflected signal depends on the type of splitter, the connectors used, and whether the said connectors are terminated or not. By installing an optical amplifier and a receiver with an avalanche photodiode (APD) further on, the eavesdropper was able to receive the signals sent by the eaves-dropped subscriber with virtually no errors when PC connectors were used in the splitter. It should be noted, however, that the cited study [12] only indicates the danger of eavesdropping and does not document this possibility. It is because the research was carried out at a wavelength of 1550 nm, while in real PON networks, the upstream transmission is usually carried on in the second transmission window, i.e., in the wavelength range of 1260-1360 nm. Such possibility has been documented, among others, in [13].

Having legal access to the network, one can eavesdrop using cross-talk signals between adjacent channels [14], [15]. The attacker legally obtains a transmission channel of a specific wavelength and then does not send any data there [16]. Therefore, the mentioned wave channel carries cross-talk signals from neighboring channels, which can be amplified with an optical amplifier and received [16]. It is possible in WDM networks where different users use different wavelengths. Cross-talk may occur either as a result of nonlinear interactions in the optical fiber (for instance, four-wave mixing, cross-phase modulation, Raman scattering) or due to the non-ideal transfer characteristics of wave demultiplexers, where part of the power of the demultiplexed signal is transferred to channels of adjacent frequencies, creating inter-channel cross-talk. An alternative place for such cross-talk is the optical switch shown in Figure 2, where the non-ideal nature of the switch causes it. The attacker, having access to the neighboring channel, optically filters out signals that are not interesting to him, leaving the eaves-dropped channel, which may be amplified optically before receiving it on his device. The effectiveness of eavesdropping depends directly on the strength of the eavesdropped signal and the level of cross-talk in network nodes. For these reasons, it is more effective near transmitters, where the cross-talk signal is stronger.

To conclude, it is worth mentioning the reports of direct cross-talk between parallel optical fibers in optical ribbon fiber cables [17]. This phenomenon was confirmed experimentally [17] by connecting a sensitive superconductive single photon detector (SSPD) to a dark optical fiber located near (direct or second neighbor in the ribbon) the active optical fiber. The cause of this cross-talk appeared to be photon leakage between optical fibers at the cable bends. It is still being determined whether such cross-talk is common or only occurred in the tested cable, as no other reports con-firm the discovered phenomenon. This slight cross-talk can only be detected using very sensitive photodetectors capable of detecting single photons. Despite this, it may significantly negatively impact the operation of Quantum Key Distribution (QKD) systems [17].

III. Active attacks

Active attacks aim to disrupt or prevent transmission in part or even in the entire network. A huge problem of optical networks is that due to the transparency of such networks, attacks of this type tend to quickly spread beyond the attacked section of the network [18]. There are two types of such attacks.

The first one involves physical damage to the infrastructure, e.g., cutting a cable or intentionally destroying equipment. This type of attack, although annoying and primitive, is relatively simple to locate and repair.

Attacks involving introducing an intentional jamming signal into the network are much more dangerous and challenging to locate. Such a signal can be inserted in the same places mentioned when discussing wiretapping. It usually has a high power that significantly exceeds the typical power used for transmission. Another possible attack is the use of the so-called alien channel. We will briefly discuss these possibilities.

The already mentioned clip-on coupler can also insert an interfering signal. It is sufficient to connect the jamming signal to the receiving optical fiber (which was previously used for eavesdropping) and change the direction of the coupler connection (in the arrangement shown in Fig.1, the jamming signal would be sent towards the transmitter, which means that the attacker would not achieve the intended goal). We should mention right away that the initial attenuation of such a jamming signal is in the order of 13...22 dB (commercially available equipment) depending on the transmission window, so in order to effectively disrupt the transmission, the attacker must have a light source of significant power at his/her disposal. A very dangerous variant of this attack is the so-called correlated jamming [16], [19]. It involves using a (clip-on) coupler to simultaneously eavesdrop on the signal and disrupt it further down the link [16], [19]. In this case, the eavesdropped part of the useful signal is replaced by interference or an-other signal so that the total power of the signal (usable + interference), which continues to propagate down the path, does not change, which makes it difficult to detect the threat by measuring the power at the receiving node. This attack is perilous if the (O)SNR value of the attacked user is relatively low [19].

One can also insert a 2x1 type optical coupler in the path for attack purposes, directing the useful signal and interference to its inputs. However, this may only be un-noticed at installation, as cutting the fiber is necessary. However, an attacker can risk triggering an alarm if he/she can quickly (i.e., before the arrival of the maintenance crew) perform the entire operation and restore traffic (he/she can attack later).

Connecting an interfering signal in network nodes to optical monitoring ports or unused output ports, although entirely possible, is less effective than eavesdropping on the same ports. This is because the interfering signal introduced in this way will prop-agate to the transmitter, i.e., in the direction opposite to the propagation of the useful signal [20]. Only the part of the interfering signal reflected in the network element and propagated with the useful signal in the same direction will threaten the latter signal. However, due to the high isolation

levels in network elements, the required powers to carry out an effective attack are +30 dBm, which is very high. A better way for an eavesdropper to carry out such an attack is to use those device ports that are unsuitable for eavesdropping. An example of such a port is an unused input port in any optical node, e.g., a switch. This type of attack is shown in Fig. 2.

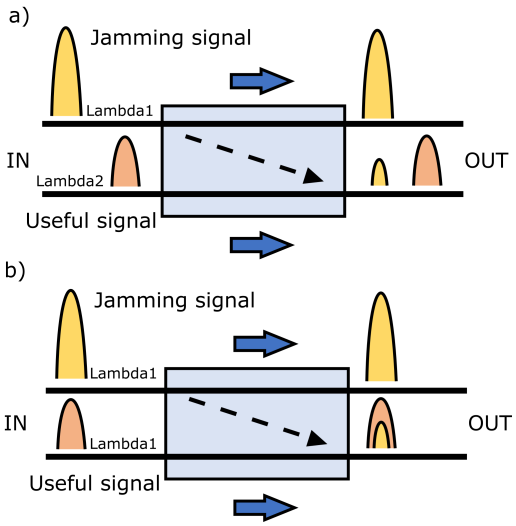

Fig. 2. Attack using cross-talk and implemented at an unused input port of the optical switch: a) out-of-band attack, b) in-band attack

In this case, the attacker uses a signal with very high power (about 20 dB more than the attacked signal) [20]. The attacker's signal passing through the optical switch uses the cross-talk existing in such elements: the attacker's signal appears not only on the output port to which it was directed but also as a cross-talk signal on the port/ports to which the usable signal/signals was/were transferred. It should be noted that this type of attack tends to spread beyond the optical paths directly connected to the attacked node [21], although it must also be said that as the attack spreads in the network, its impact weakens [22]. An example of the propagation of an attack using cross-talk in the network is shown in Fig.3.

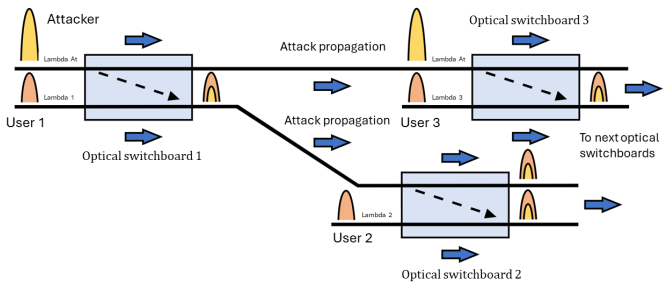

Fig. 3. Cross-talk attack propagation in the optical network

Interoperability in the optical layer of the network is required to ensure easy up-grades and effective implementation of high-speed connections based on the existing infrastructure. It can be implemented using the so-called alien wavelengths, i.e., signals of specific wavelengths coming from transponders that are not under the direct control of the optical network operator [19]. This approach eliminates the need to use wavelengths native to the operator's system and reduces the operator infrastructure. It has many other advantages, including reduced network latency and power consumption [20]. On the other hand, alien wavelengths lead to a potentially serious threat to net-work security since the operator often does not control either the wavelength or the power of alien signals, which allows them to be used for active attacks. They are even more dangerous because, unlike the previously described attacks, the alien signals are not suppressed when introduced into the network. Therefore, high optical power is unnecessary to carry out an effective attack. Having access to a single optical fiber, an attacker using advanced techniques can remotely disrupt all traffic in the network node to which this optical fiber leads [19]. It can be done using a multi-wavelength signal or one in which the wavelength hops between channels to disrupt useful signals for the maximum number of outputs [19].

In this context, one should note that all types of PON of any architecture are most vulnerable to attacks from users with legal access to the network [14]. An attacker can introduce a jamming signal upstream at any point in the network to which he has legal access [14]. This disturbance may be of low magnitude, merely in-creasing the error rate in the demodulated signal. It may also take the form of an un-modulated high-power signal, the purpose of which is to saturate the receiver in the central node [14]. In the case of passive PON networks (e.g., GPON, EPON), adequate saturation of the receiver in the central node turns off all transmissions in the reverse direction from all users and, consequently, the entire network for all its users. Another attack possibility [19] is the use of an OOK (on-off keying) signal with a modulation that is fast enough so that the threshold level in the receiver is unable to adapt to it but not so fast that it is filtered by filter in the receiver [19].

Let us consider the position of the interfering signal band as related to the useful signal. All attack types can be divided into out-of-band attacks (if the ranges of the mentioned bands are different) and in-band attacks (if both signals occupy the same frequency range). An example of both types of attacks is shown in Fig.2.

The in-band attack is much more dangerous than the out-of-band attack. Firstly, the out-of-band attack can be easily eliminated using appropriate optical filters, i.e., filters that only allow the useful signal to pass through. The in-band attack cannot be eliminated in this way. Secondly, in the case of an out-of-band attack, both signals, i.e., useful and interfering, are incoherent, which means that their powers add, and no beating signal arises in the optoelectronic receiver. As a result, the interference signal powers necessary to disrupt transmission are relatively high. In this case, a loss of reception sensitivity of 1 dB occurs when the power level of the interfering signal exceeds -12...-13 dB about the power of the useful channel [19]. In contrast, with the in-band attack, both signals are added coherently (i.e., considering the phase difference), which creates an electric signal in the receiver resulting from the beating of both frequencies. Therefore, the attacking signal powers required to disrupt the transmission are relatively low: a loss of reception sensitivity of 1 dB occurs at a power level

of the interfering signal above -30 dB compared to the power of the useful signal.

In-band attacks can be carried out directly or indirectly. In the first case, the interfering signal is inserted in the same transmission path as the targeted channel (e.g., via the previously discussed clip-on coupler). In turn, the indirect attacks use cross-talk in network nodes such as switches.

Special attention should be paid to the out-of-band attack using the optical fiber's nonlinear properties [11] intended for jamming coherent transmission. It involves intentionally introducing an OOK signal with high power and relatively low bit rate (e.g., 10 Gbit/s) with a wavelength near the attacked channels with very high bit rates (100 ... 200 Gbit/s) using coherent multi-value modulation. The OOK signal introduces cross-talk in the above coherent signals through cross-phase modulation (XPM) and/or cross-polarization modulation (XPolM). It was shown in [20] that the effective band-width of the attacking channel increases with its power and the size of the constellation of interfered coherent signals. For example, with the interference signal power of +15 dBm, the jamming bandwidth of this channel is from 1.2 to 3.1 THz for DP-QPSK and DP-16QAM (DP - dual polarization) modulations, respectively.

A particular type of out-of-band attack is an attack using gain competition in optical amplifiers, including EDFA amplifiers. This phenomenon has been described, for ex-ample, in [23]. This type of attack takes advantage of the fact that introducing a very high-power jamming signal to the input of an optical amplifier reduces the amplification of other (attacked) channels. Consequently, these channels' OSNR (optical signal-to-noise ratio) values are reduced, leading to service quality deterioration or even transmission interruption. Undetected, such a jamming signal propagates in the net-work as if it were a signal from a legitimate source, depriving other useful channels of power along its path [18]. This attack is hazardous in the case of amplifiers operating in the regime of ensuring constant output power [20]. Optical amplifiers equipped with automatic gain control (AGC) can protect useful channels against OSNR reduction (deterioration of transmission quality), but only if the power of the attacking signal does not exceed a certain threshold [23]. The research results published in [23] also indicate that using a larger number of amplifiers provides greater protection of useful channels against this type of attack for a fixed track length. Increasing the power of useful channels has a similar effect [23]. The gain competition attack may prove very difficult to manage if the optical power in the attacking channel is additionally keyed at an ap-propriate frequency [24]. Due to the time delays of the gain control loop in the amplifiers themselves and the optical receivers, keying may lead to unstable operation of the entire gain path (transient states [24]). On the one hand, it may cause temporary drops in OSNR in the useful channels below the minimum values, and on the other hand, temporary distortion in receivers in these channels.

One of the methods of limiting the propagation of high-power jamming attacks is the use of adjustable and wave-selective attenuators in network nodes [24], [25], which are typically employed to equalize the power of optical signals passing through a given node. In this case, the high-power attack signal will be suppressed in the first node with such functionality [24], limiting its propagation in the network. However, this will not prevent disruptions in the section from the point of introduction of the attack to the mentioned node or disruption of the operation of the channel in which the attack is carried out [24]. Let us emphasize once again that in older types of nodes, without the possibility of selective power regulation (such as fixed optical add-drop multiplexers - FOADM [24]), a high-power attack propagates without any obstacles in the network up to the node, where the signal(s) is/are subject to regeneration.

A. *Hidden attacks*

An important subcategory of active attacks is hidden attacks. In general, these attacks are carried out to deteriorate the QoS rather than sabotage the network's operation altogether. The main intention of the attacker is to make it difficult for the network operator to detect that such an attack is being carried out. We will briefly discuss two types of such attacks. The first one is called a low-power QoS attack [26]. It involves including an optical splitter in the path to degrade the useful signal's power level and reduce OSNR as a result. As shown in [26], a clever attacker can cause transmission quality degradation alarms to appear in network locations very distant from the actual location of the attack, which causes difficulties in the management system diagnostics. This attack is most effective if carried out close to the transmitter [26] because it affects the largest part of the path. Moreover, signal loss alarms appear not in part with the splitter but in further sections of the link that have yet to be directly attacked [26]. As indicated in [16], this type of attack may propagate in networks with protection against high-power jamming attacks (active equalizers in network nodes [16]). As for installing such a splitter, a possible scenario is presented in the report [27] (albeit about installing a wiretapping). A detailed description of this action scenario has been provided at [27] among others.

The second type of hidden attack was first described in [28]. It may affect the transmission of coherent signals with very high bit rates using polarization multiplexing (PolMux). The attack involves applying a rapidly changing transverse pressure to the attacked optical fiber, which introduces appropriate changes in stress in the optical fiber, causing variable birefringence of the fiber because the fiber material itself has elasto-optic properties. The easiest way is to use a piezoelectric transducer into which an uncoated optical fiber is inserted. The attack leads to rapid changes in the polarization of the transmitted signal. Suppose they are fast enough (above several million radians per second [28]). In that case, the digital signal processing algorithm in the coherent system receiver that separates polarizations cannot correctly split transmitted signals with orthogonal polarizations. Unlike the clip-on couplers discussed in the wiretapping context, the piezoelectric transducer does not introduce any attenuation and it's extremely difficult to locate.

IV. Experimental Research

Based on the discussed attack patterns that disrupt optical networks, this paper's authors carried out several experimental studies in this area. Various attack scenarios were examined using the optical clip-on coupler to insert the interfering signal into the optical path for various types of jamming sources [29]. The paper presents previously never unpublished research results regarding the jamming of optical transmission in the 1000Base (Ethernet) standard with an optical signal modulated with a low-frequency rectangular signal (10 MHz) generated by an external laser. The chosen method of attack is straightforward and, at the same time, highly effective. The selection of the transmission standard resulted from its popularity in the local area networks. The examined standard is also characterized by high resistance to interference.

A. Demonstration setup

The setup we used in our experiment is shown in Fig. 4, and its photography in Fig. 5

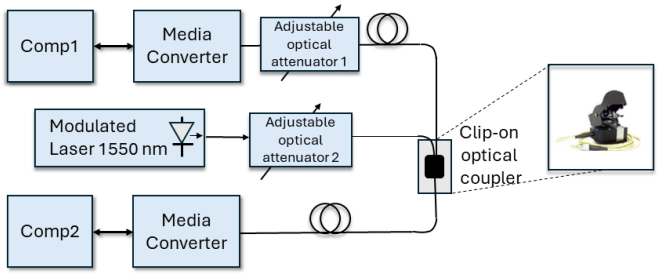

Fig. 4. A block diagram of experimental setup

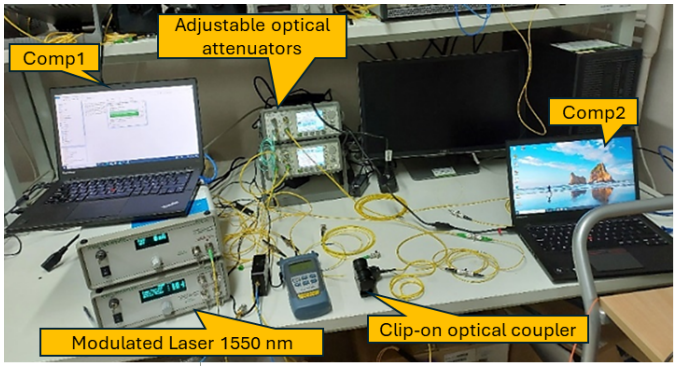

Fig. 5. A photography of experimental setup

In principle, the setup was used to transmit huge binary files between two portable computers (Comp1, Comp2), which were connected via an optical 1000Base (Ethernet) system. To this end, we employed two media converters 10/100/1000 Base-TX to 1000 Base-FX (LightOptics). A standard single mode (SM) optical fiber was a trans-mission medium with the converter lasers operating in the 1550 nm window. The optical jamming signal was inserted into the fiber via the clip-on coupler (FOD 5503). The photo of the clip-on coupler and its parameters are depicted in Fig.6 .

Clip-on coupler FOD 5503
Coupling efficiency:
- 12–17 dB at 1550 nm
- 17–22 dB at 1310 nm

Insertion loss:
- below 7 dB at 1310 & 1550 nm
- typical 4 dB at 1550 nm
- typical 2 dB at 1310 nm

Back reflection on tapped fiber below –60 dB

Fig. 6. A clip-on coupler photography and its specification

A 1550 nm laser light source (Agilent 8163) modulated with a 10 MHz rectangular signal was used as the jamming signal. Two optical attenuators adjusted the useful signal and jamming signal powers, respectively. The link data throughput in Mbytes/s assessed the transmission quality. The built-in Windows network monitoring software reported the latter. During the measurement session, we changed both the useful and jamming signal powers by adjusting the respective attenuators and recorded the corresponding throughput.

B. Measurement results

The obtained results are shown in Fig.7 and Fig.8.

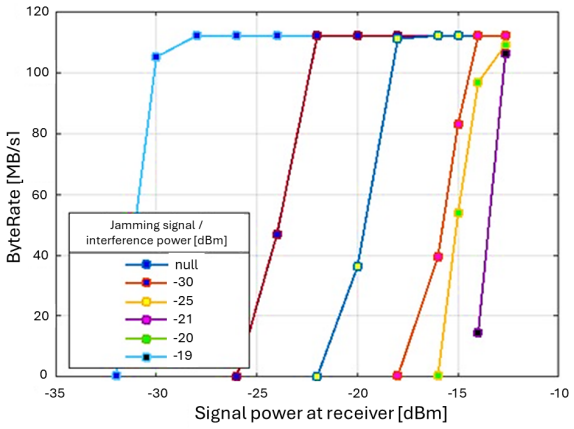

Fig. 7. Useful signal throughput (in Mbytes/s) as a function of the useful signal power received at receiver for various level of jamming signal power arriving to the receiver together with it.

C. Results discussion

The measurement shows that the successful attack requires the jamming signal power to be slightly less (around 3…6 dB less) than the useful signal power, whereas both are measured at the receiver. Considering the significant attenuation of the clip-on coupler for the jamming signal (12. . . 22 dB depending on the wavelength), it appears at first glance that a successful attack requires a rather prohibitively high power of the jamming source. It is so if the ingress point is close to the transmitter. The situation is different if the clip-on coupler is inserted not far from the receiver, and the link loss is typical for medium or long-range systems (15.. . 30 dB). Then a typical off-the-shelf laser modulated with a low-frequency rectangular wave is very effective as the transmission jammer.

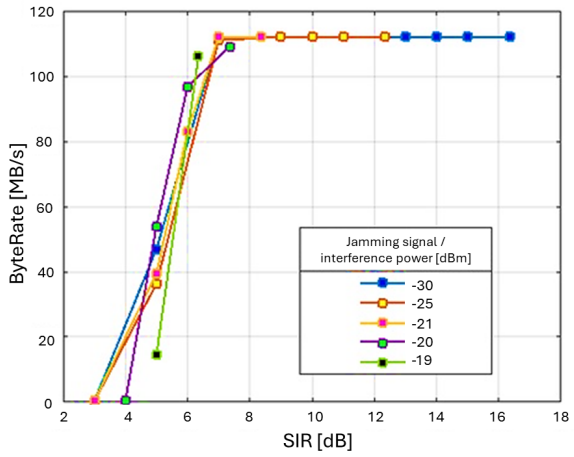

Fig. 8. Useful signal throughput (in Mbytes/s) as a function of the ratio of the useful signal power to the interfering signal power (SIR) in dBs measured at the receiver for various interfering signal powers

It is necessary to stress that the clip-on coupler may be inserted into the link and left inactive, waiting for the right moment to switch on the jamming signal. Detection of such a device lying in wait may be difficult since its OTDR response may be similar to that of an optical connector, as shown in Fig.9. It is necessary to emphasize that only an example is depicted there; other configurations may yield different results.

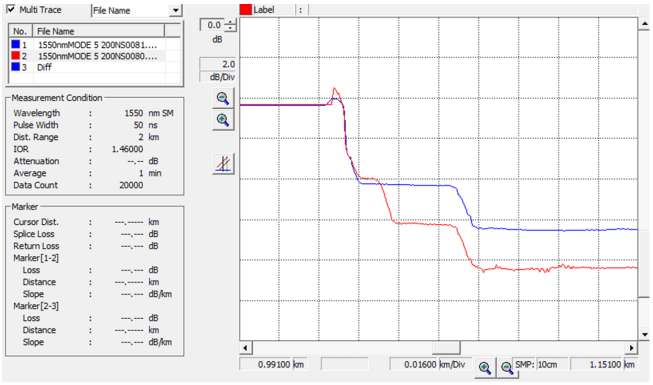

Fig. 9. An exemplary OTDR response to the clip-on coupler sandwiched between two optical connectors: upper trace (black) connectors only, lower trace (red) connectors plus clip-on coupler

The carried-out research proved that the optical clip-on coupler is a dangerous and effective device for optical transmission jamming, provided it is used not far from the receiver. If its location is relatively close to the receiver, even the use of generally available commercial laser light sources modulated with a low-frequency rectangular signal is sufficient for an effective attack. What is particularly important to accomplish such an attack is that the rogue party does not require access to any network node. The access to the fiber plant, which can be hundreds or thousands of kilometers long, is sufficient. It makes it very difficult to secure such a network fully. Since the described attack is very efficient and may ultimately disrupt the link/network services, the methods of attack detection and localization are of utmost importance for network security.

V. Attacks Prevention

Due to the variety of attacks that can be carried out and their potentially cata-strophic impact on network transmission, the appropriate detection and identification of attacks in the physical layer is indispensable. It should be emphasized that attacks of this type differ significantly from conventional network failures [18]. First, attacks can appear sporadically and disappear at any point in the network. The attacker can also avoid simple detection methods, which are not sensitive enough to detect small and sporadic transmission quality degradation. Moreover, an attack mistakenly identified as a component failure may continue propagating through the network, causing additional failures and triggering further alarms [18].

Attack patterns in optical networks can be very complex. Therefore, their real-time detection and identification can be a non-trivial task for the network management system. The standard methods of optical network protection used so far, which are aimed at failure detection and identification, may often need to be revised to detect the purposeful attack properly. Therefore, more advanced detection and countermeasure methods are required. Thus, many recently published scientific papers indicate that this can be achieved using machine learning (ML). For in-stance, classification (identification) models based on deep learning neural networks may be used here. It is facilitated by a huge increase of interest in this technique and thus its dissemination in many areas of science and business, resulting in many new solutions in this area. In this respect, it should be emphasized that using protection mechanisms based on ML methods shifts the methods of designing and operating op-tical networks toward the so-called intelligent networks [30]. What is equally important is that this technique can be used both for the physical layer and higher OSI layers, including, among others, transport and network layers. The use of ML methods to protect optical networks can be classified as follows: controlling the operation of optical net-works, resource management, monitoring how the network operates, and detecting undesirable events such as all types of attacks [31].

The last group is particularly interesting in terms of this paper's scope. In this aspect, the ability of this type of algorithm to perpetually learn and improve based on continuously supplied data is particularly important. It creates the possibility of introducing intelligence into the network, which is capable of learning new attack pat-terns. It is done without the need for significant modifications introduced to the system by the operator, which is beneficial not only for the security of the optical network itself but also for optimizing the maintenance costs of such a network.

Focusing on the recently published works in this area, the papers [28], [32]–[36] are worth mentioning. We will begin the review from [28], [32]. These papers focus on using various ML-based algorithms to detect and identify a jamming attack. It is done by classifying the received optical signals

as disrupted or not, based on the monitored parameters of coherent transmitters/receivers during their normal operation. According to the authors of the works, using a solution based on a neural network as a classifier ensures the detection of active jamming attacks of high and medium intensity at a level exceeding 99.9%. Unlike the works [28], [32], the paper [33] uses machine learning to detect and locate network eavesdropping sites. For this purpose, a classifier of the presence of optical link eavesdropping was developed using data obtained from the network quality monitoring system, including eye patterns of received signals and their deterioration in the point-to-point Coherent Optical Orthogonal Frequency Division Multiplexing (CO-OFDM) system. It was possible to detect changes in the eye pattern and thus reveal eavesdropping and its location using convolutional neural networks (CNN). This method ensured the correct detection of wiretapping with an accuracy of 100% and the correct location of its location with an accuracy of 92.7%. Data from the optical network quality monitoring system are also used in [34] for ML-based eavesdropping detection and its location. However, unlike the previous approach [33], the detector module was developed based on the K-means classification algorithm. According to the authors, this approach resulted in 100% detection efficiency of both its presence and location for many scenarios of wiretapping. The paper [35] also focuses on detecting eavesdropping in optical networks implemented with an optical clip-on coupler. Its authors propose [35] an approach based on the extraction of a number of metrics of the signal received in the time domain for the CO-OFDM trans-mission system, and then using them as a vector of input parameters for a classifier model based on the Long Short-Term Memory (LSTM) recurrent neural network. The authors state that the method efficiency reaches 95.83% when used to detect eaves-dropping attacks in a 60-km single-mode fiber transmission link. The paper [36] presents research results on the effectiveness of various types of ML algorithms in de-tecting, localization, and preventing high-power jamming attacks for out-of-band jamming signals in a WDM optical network. The scenario concentrates on employing high-power interfering signals transmitted at a wavelength λ different from the wave-length of optical carrier waves used to transmit useful signals. The paper reviews the following ML techniques: artificial neural networks (ANN), support vector machine (SVM), logistic regression (LR), K-nearest neighbors (KNN), decision tree (DT), and Naive Bayesian classifier (NB). Data from the network monitoring system were used. The effectiveness of individual algorithms was studied for a network with four transmitting nodes, 32 light wavelengths, and the third transmission window (1550 nm). For the best research scenario (the richest set of training data), the effectiveness of detecting a jamming attack was close to 99% for the ANN-based classifier. Using SVM, LR, and KNN algorithms ensured an efficiency of 90%. In the case of DT, only 56% was achieved. However, the authors point out that the final effectiveness of the tested algorithms depends largely on the quality of the data set used in both their training and those that can be used during their work. Therefore, in many other scenarios, the correct detection efficiency was lower. This work also verified the possibility of the correct location of the site of the jamming attack. In this regard, solutions based on ANN and SVM algorithms were characterized by the highest effectiveness, almost 99%, when attacks occurred. However, even these algorithms had problems correctly identifying the so-called false-positive misclassification cases, i.e., when a disruptive attack was indicated but did not actually occur. Therefore, there is a need for further work in this area. The obtained results made it possible to propose approaches to limit the impact of the attack based on appropriate, automatic channel switching and traffic changes in the tested optical network.

Applying ML algorithms combined with data from optical network monitoring systems can produce spectacular results, as the cited papers show. One can even say that the use of machine learning may revolutionize this area. However, one should be aware that the effectiveness of these algorithms depends largely on the quality of the data available, which is the basis for their operation. Therefore, this should be considered when designing modern intelligent optical network solutions capable of self-defense. Thus, it is desirable to implement additional monitoring/protection mechanisms, such as spectral analysis or measuring signal parameters in the time do-main. It should increase the security of optical networks and thus limit the ability to carry out attacks and minimize their effects in real time. For the latter, an immediate redirection of network traffic may be used.

Moreover, creating better conditions for the effective operation of ML algorithms (e.g., better data for learning) may be fruitful. An example of this type of action may be introducing a mechanism for controlling unexpected changes in the polarization of the electromagnetic field components of a light wave transmitted in an optical fiber as an optical carrier, which was proposed in [37]. Such advanced protection mechanisms should also be used beyond physical OSI layers.

VI. Conclusions

Attacks in optical networks pose a serious threat to the security of information flow/data transmission. They are even more dangerous because, due to the high bit rates used, very large volumes of this data are lost or compromised in the event of a successful attack. In today's world torn apart by conflicts, wars, and terrorism, this threat cannot be ignored. The current work reviews methods of combating network attacks in three aspects: attack prevention, detection, and response to a detected attack. Some of the presented methods can be used at the stage of network design and allocation of resources, while others are concerned with physical security or modulation. Others show how to best use data from the management system for the purposes discussed. Many of the presented algorithms lead to complex optimization or interpretation issues, which, due to their complexity, often require the use of machine learning. A realistic scenario attack in the optical local area network by using of the clip-on coupler for this purpose has been presented to strength the message of the presented content.

VII. Acknowledgment

The work financed by internal grant of the Warsaw University of Technology No. 820/341/Z01/POB3/2021

References

[1] Spurny, V.; Munster, P.; Tomasov, A.; Horvath, T.; Skaljo, E. Physical Layer Components Security Risks in Optical Fiber Infrastructures, *Sensors* 2022, Volume 22, pp.1-15, Available: https://doi.org/10.3390/s22020588

[2] Furdek, M.; Chan, V.W.S.; Natalino, C.; Wosinska, L. Network-Wide Localization of Optical-Layer Attacks, Optical Network Design and Modeling, ONDM 2019, Springer 2020, Volume 11616, Available: https://doi.org/10.1007/978-3-030-38085-4

[3] Horvath, T.; Malina, L.; Munster, P. On Security in Gigabit Passive Optical Networks, In Proceedings of the 2015 Interna-tional Workshop on Fiber Optics in Access Network (FOAN), 2015, https://doi.org/10.1109/FOAN.2015.7320479.

[4] Horvath, T.; Munster, P.; Oujezsky, V.; Vojtech, J.; Holik, M.; Dejdar, P.; Latal, M. GPON Network with Simulated Rogue ONU, In Proceedings of the 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2019, Available: https://doi.org/10.23919/SOFTCOM.2019.8903811

[5] Atan, F.M.; Zulkifli, N.; Idrus, S. M.; Zin, N.A.M.; Ismail, N. A.; TCP Capacity Utilization In Next Generation Passive Optical Network During Degradation Attack, In Proceedings of the 2022 IEEE 6th International Symposium on Telecommunication Technologies (ISTT), 2022, Available: https://doi.org/10.1109/ISTT56288.2022.9966544

[6] Uematsu, T.; Hirota, H.; Kawano, T.; Kiyokura, T.; Manabe, T. Design of a Temporary Optical Coupler Using Fiber Bending for Traffic Monitoring, *IEEE Photonics Journal.*, Volume 9, 2017, Available: https://doi.org/10.1109/JPHOT.2017.2762662

[7] irota, H; et al. Optical Cable Changeover Tool with Light Injection and Detection Technology, J. of Lightwave Technology, 2016, Volume 34(14), pp. 3379-3388, Available: https://doi.org/10.1109/JLT.2016.2568221

[8] Uematsu, T.; Hirota, H.; Kawano, T.; Iida, H.; Noto, K.; Katayama, K. Temperature-Independent Temporary Optical Coupler Using Fiber Bending Technique, *J. of Lightwave Technology*, 2023, Volume 41(9), pp. 2834-2839, Available: https://doi.org/10.1109/JLT.2023.3237372

[9] Kingfisher International, OPT130, Optical Clip-on Coupler, kingfisher.com.au

[10] o4Fiber Ltd., PFC 1000, Passive Fiber Clip-on Coupler, www.go4fiber.com

[11] Iqbal, M.Z.; Fathallah, H.; Belhadj, N. Optical Fiber Tapping: Methods and Precautions, In Proceedings of the 8th Interna-tional Conference on High-capacity Optical Networks and Emerging Technologies, 19-21 December 2011, Riyadh, pp. 164-168, 2011, Available: https://doi.org/10.1109/HONET.2011.6149809

[12] Malina, L.; Horvath,T.; Munster, P.; Hajny, J. Security solution with signal propagation measurement for Gigabit Passive Optical Networks, *Optik*, 2016, Volume 127(16), pp. 6715-6725, Available: https://doi.org/10.1016/j.ijleo.2016.04.069

[13] Spurny, V.; Munster, P.; Horvath, T.; Skaljo, E. Leakage of Information Through Passive Components in Optical Fiber In-frastructures, In Proceedings of the 13th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 2021, Available: https://doi.org/10.1109/ICUMT54235.2021.9631702

[14] Fok, M.P.; Wang, Z.; Deng, Y.; Prucnal, P.R. Optical Layer Security in Fiber-Optic Networks, *IEEE Trans. on Information Forensics and Security*, 2011, Volume 6(3), pp. 725-736, Available: https://doi.org/10.1109/TIFS.2011.2141990

[15] Yuan, S.; Steward, D. Protection of Optical Networks against Interchannel Eavesdropping and Jamming Attacks, In Pro-ceedings of the 2014 International Conference on Computational Science and Computational Intelligence, 2014, pp. 34-38, Available: https://doi.org/10.1109/CSCI.2014.14

[16] Krishnan, S.; Borude, A. Security issues in all-optical networks, In Proceedings of the 2011 Annual SRII Global Conference, 2011, pp. 790-794, Available: https://doi.org/10.1109/SRII.2011.108.

[17] Fujiwara, M.; Miki, S.; Yamashita, T.; Wang, Z.; Sasaki, M. Photon level cross-talk between parallel fibers installed in urban area, *Optics Express*, 2010, Volume 18(21), pp. 22199-22207, Available: https://doi.org/10.1364/OE.18.022199

[18] Rejeb, R.; Leeson, M.S.; Green, R.J. Fault and Attack Management in All-Optical Networks, *IEEE Communications Magazine*, 2006, pp. 79-86, Available: https://doi.org/10.1109/MCOM.2006.248169

[19] Medard, M.; Marquis, D.; Barry, R.A.; Finn, S.G. Security Issues in All-Optical Networks, *IEEE Network*, 1997, pp. 42-48, Available: https://doi.org/10.1109/65.587049.

[20] Dahan, D.; Mahlab, U. Security threats and protection procedures for optical networks, *IET Optoelectronics*, 2017, Volume 11(5), pp. 186-200, Available: https://doi.org/10.1049/iet-opt.2016.0150

[21] Wu, T.; Somani, A.K. Cross-Talk Attack Monitoring and Localization in All-Optical Networks, *IEEE/ACM Trans. on Net-working*, 2005, Volume 13(6), pp. 1390-1401, Available: https://doi.org/10.1109/TNET.2005.860103

[22] Peng, Y.; Sun, Z.; Du, S.; Long, K. Propagation of all-optical cross-talk attack in transparent optical networks, *Optical Engineering*, 2011, Volume 5(8), pp. 085002-1-4, Available: https://doi.org/10.1117/1.3607412

[23] Deng, T.; Suresh, S. Analysis of optical amplifier gain competition attack in a point-to-point WDM Link, In Proceedings of SPIE, 2002, Volume 4874, pp. 249-261, Available: https://doi.org/10.1117/12.475302

[24] Skorin-Kapov, N.; Furdek, M.; Zsigmond, S.; Wosinska, L. Physical Layer Security in Evolving Optical Networks, *IEEE Communications Magazine*, 2016, pp. 110-117, Available: https://doi.org/10.1109/MCOM.2016.7537185

[25] Manousakis, K.; Ellinas, G. Attack-aware planning of transparent optical networks, *Optical Switching and Networking*, 2016, Volume 19, pp. 97-109, Available: https://doi.org/10.1016/j.osn.2015.03.005

[26] Deng, T.; Subramaniam, S. Covert Low-Power QoS Attack in All-Optical Wavelength Routed Networks, In Proceedings of the Globecom, 2004, Volume 3, pp. 1948-1952, Available: https://doi.org/10.1109/GLOCOM.2004.1378333

[27] Deloitte Touche Tohmatsu Ltd., Tapping of fibre networks, 2017.

[28] Natalino, C.; Schiano, M.; Di Giglio, A.; Wosinska, L.; Furdek, M. Experimental Study of Machine-Learning-Based Detection and Identification of Physical-Layer Attacks in Optical Networks, *J. Of Lightwave Techn.*, 2019, Volume 37(16), pp. 4173-4182, Available: https://doi.org/10.1109/JLT.2019.2923558

[29] Kowalczyk, M.; Marzecki, M.; Siuzdak, J. The Threat of Optical Transmission Jamming, *J. of Telecommunications and Information Technology*, 2023, Volume 4(4), pp. 93–101, Available: https://doi.org/10.26636/jtit.2023.4.1402

[30] Furdek, M. Towards Secure and Self-Diagnosable Optical Networks, In Proceedings of the Photonics in Switching and Computing (PSC), 19-21 September 2018, Available: https://doi.org/10.1109/PS.2018.8751355

[31] Khan, F. N. Data perspectives in AI-assisted fiber-optic communication networks, *IEEE Network*, 2023, pp. 1-8, Available: https://doi.org/10.1109/MNET.130.2200413

[32] Natalino, C.; Schiano, M.; Di Giglio, A.; Wosinska, L.; Furdek, M. Field Demonstration of Machine-Learning-Aided Detection and Identification of Jamming Attacks in Optical Networks, In Proceedings of the 2018 European Conference on Optical Communication (ECOC), 2018, Available: https://doi.org/10.1109/ECOC.2018.8535155

[33] Kang, X.; Wang, R.; Jiang, M.; Li E.; Li, Y.; Yan, X.; Wang, T.; Ren Z. Experimental study of machine-learning-based detection and location of eavesdropping in end-to-end optical fiber communications, *Optical Fiber Technology*, 2022, Volume 68(102807), Available: https://doi.org/10.1016/j.yofte.2021.102669

[34] Song, H.; Lin, R.; Sgambelluri, A.; Cugini, F.; Li, Y.; Zhang, J.; Monti, P. Cluster-based Method for Eavesdropping Identifi-cation and Localization in Optical Links, In Proceedings of the Asia Communications and Photonics Conference (ACP), 2023, Available: https://doi.org/10.48550/arXiv.2309.14541

[35] Song, H.; Lin, R.; Li, Y.; Lei, Q.; Zhao, Y.; Wosinska, L.; Monti, P.; Zhang J. Machine-learning-based method for fiber-bending eavesdropping detection, *Optics Letters*, 2023, Volume 48(12/15), pp. 3183-3186, Available: https://doi.org/10.1364/OL.487214

[36] Bensalem, M.; Singh, S. K., and Jukan, A. On Detecting and Preventing Jamming Attacks with Machine Learning in Optical Networks, In Proceedings of the IEEE Global Communications Conference (GLOBECOM), pp. 1-6, 2019, Available: https://doi.org/10.20944/preprints201901.0311.v1.

[37] Tomasov, A.; Dejdar, P.; Horvath, T.; Munster P. Physical fiber security by the state of polarization change detection, In Proceedings of SPIE 12105, Fiber Optic Sensors and Applications XVIII, 1210507, 2022, Available: https://doi.org/10.1117/12.2618490