photonics

MDPI

Review

Fiber Tapping in Optical Networks: Attack Techniques, Detection, and Mitigation

Krzysztof Borzycki * and Mirosław Klinkowski

National Institute of Telecommunications, ul. Szachowa 1, 04-894 Warsaw, Poland; m.klinkowski@il-pib.pl
* Correspondence: k.borzycki@il-pib.pl; Tel.: +48-225128124

Abstract

Initially considered secure against interception, fiber-optic networks were subsequently found susceptible to covert tapping, although such attacks require different coupling mechanisms and components than those used for twisted pair and coaxial cables. Fiber-optic networks carry the majority of data and voice traffic worldwide, including backhaul and fronthaul traffic in 4G and 5G radio networks, connections between data centers, and submarine cable systems. Consequently, physical access to fibers for interception has attracted the attention of intelligence agencies and industrial spies. This vulnerability is facilitated by the fact that single-mode optical fibers (SMFs) used in telecommunication networks have evolved relatively little over the last 40 years. Fibers of substantially different designs—anti-resonant hollow core fibers (HCF) and multi-core fibers (MCF)—made their commercial debut around 2023, and their susceptibility to tapping may differ substantially from that of conventional SMFs. New promising fiber monitoring techniques based on polarization measurements have also been demonstrated recently. While established tapping techniques remain feasible for conventional fibers, new fiber designs and monitoring technologies can make covert interception difficult. This review examines physical fiber tapping techniques and their practical feasibility, with particular emphasis on optical power constraints, introduced loss, detectability, and implementation limitations. It also reviews prevention and monitoring approaches, including optical time-domain reflectometry, received-power monitoring, and state-of-polarization (SOP) monitoring, and provides a prospective engineering assessment of the susceptibility of MCFs and HCFs to physical tapping.

Keywords: optical fiber tapping; fiber coupler; bending coupler; evanescent coupler; prevention of fiber tapping; fiber monitoring; OTDR monitoring of live fiber; SOP-based fiber monitoring; tapping of multi-core fiber; tapping of hollow-core fiber

1. Introduction

1.1. Fundamentals

Optical fibers are often regarded as inherently resistant to physical-layer attacks, particularly: (i) interception of transmitted data (eavesdropping or tapping), (ii) jamming through interference with link operation, and (iii) spoofing by replacing the original data stream with a modified one. Indeed, optical fibers, unlike the active equipment at both ends of a fiber optic link, are immune to external Electro-Magnetic Interference (EMI), except for rotation of the polarization plane of radiation guided in the fiber caused by a magnetic field, known as the Faraday effect, and do not produce high-frequency emissions known as Radio Frequency Interference (RFI). They therefore meet stringent Electro-Magnetic Compatibility (EMC) requirements relevant, for example, to radar systems, radio sites,

Check for updates

Received: 8 September 2026
Revised: 7 October 2026
Accepted: 9 October 2026
Published: 15 October 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

or high-voltage power networks. Additionally, crosstalk between neighboring fibers in the same cable is exceptionally low, with measured values close to –115 dB at 1550 nm wavelength in a single-mode cable link 90 km long [1].

Electromagnetic immunity, however, does not imply immunity to deliberate physical access to the optical transmission path. Tapping of data transmitted over optical fiber and jamming of such transmission are both possible in principle. In the case of interception, a passive coupler can divert a small part of the signal power to an eavesdropper's receiver and data analyzer, whereas jamming requires coupling of externally generated radiation from a powerful source into the fiber link. Passive taps with good optical performance can be installed using commercially available fiber couplers [2,3], fusion splicers, and tools used for legitimate installation or repairs of fiber networks.

This review focuses primarily on techniques for covert optical coupling to fibers carrying information of interest. A fiber tap, arranged in the appropriate direction, can be used either for data interception or jamming, as illustrated in Figure 1. Spoofing requires a more complicated arrangement including a receiver, data processor, and transmitter, as well as a means of inserting modified data into the targeted data stream. This work also considers related issues of prevention and detection of fiber tapping; see Sections 3 and 4, respectively. Attacks on active devices in fiber networks, such as switches, routers, and optical line terminals (OLTs) typically involve modified software, control commands, or internal electrical circuits and are outside the scope of this review.

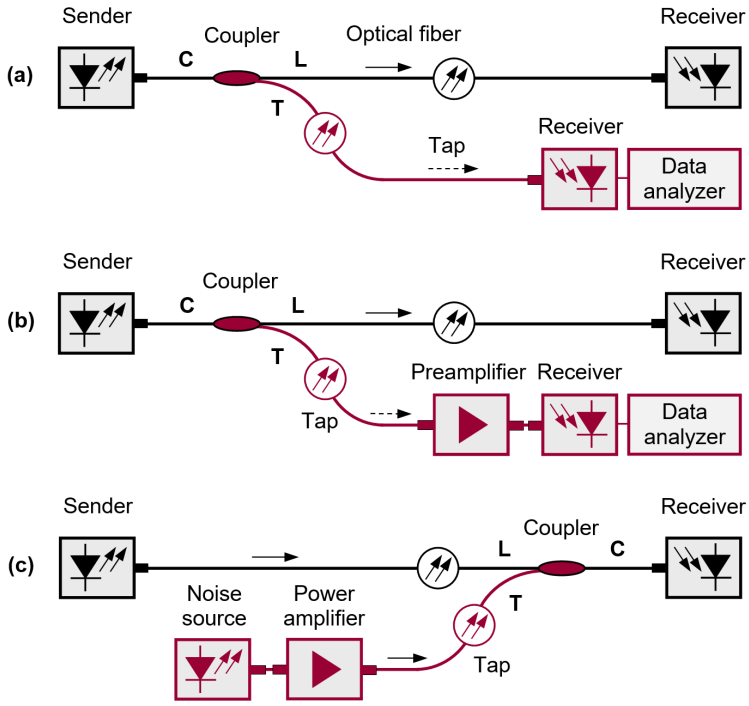


Figure 1. Fiber taps for one direction of transmission: (**a**) passive for eavesdropping, (**b**) with optical preamplifier for eavesdropping, (**c**) for jamming. Note the reversed direction of coupling in (**c**). Normal parts of the fiber-optic link are shown in black, and attack-related components in red. Arrows indicate direction of light propagation. Depending on tap location and receiver characteristics, power amplifier may not be necessary for jamming.

The dominant data transmission technology in telecom networks and data centers is currently packet-based Ethernet at multiple data rates [4]. This has enabled the development of versatile and effective equipment for deep packet inspection operating at data rates of at least 100 Gb/s [5] and capable of searching for selected content, including data contents, sender, and recipient, in real time. While data encryption prevents direct inspec-

tion of protected information, data stream can still be recorded for offline analysis using a supercomputer or future more effective decryption techniques. Encryption therefore provides a complementary layer of protection, whereas this review focuses on the physical interception of the optical signal itself.

Passive interception and active interference differ substantially in their potential for covert operation. While passive interception of data transmitted via optical fiber can be done continuously for a long time, active interference cannot be, as it is relatively easy to detect. Effective jamming shall be either a one-time action at a critical moment, e.g., at the beginning of an armed conflict, or sporadic at random moments of time, e.g., to falsely convince the user of faulty operation of his fiber link and the need to use an alternative, less secure solution like a radio link.

Tapping a small portion of optical power from the fiber under attack for interception and analysis, including deep packet inspection or traffic analysis, is performed by passive coupling to an external fiber or photodetector. The complete tap may include an optical amplifier, usually an erbium-doped fiber amplifier (EDFA), to raise the low power of the tapped signal to a level compatible with the receiver used, as shown in Figure 1b. The amplifier requires electric power and is larger than a coupler, so it is preferably located away from the attacked cable to hide it. Fiber amplifiers with low noise figure (NF $\leq$7 dB) suitable for this purpose have limited optical bandwidths [6]:

- BDFA: ≈1300–1480 nm;
- EDFA: ≈1530–1565 nm or ≈1570–1610 nm;
- TDFA: ≈1900–2020 nm (for use with hollow-core fibers).

This limitation enables protection of fiber optic links against eavesdropping by employing wavelengths for which low-noise amplifiers are not available.

Thus, the susceptibility of a fiber-optic link to physical interception cannot be inferred solely from the electromagnetic properties of the fiber medium. It depends on the coupling mechanism, optical power available at the tapping point, loss introduced into the legitimate signal path, operating wavelength and possible optical amplification, as well as the capabilities of the monitoring techniques employed. These interdependent factors provide the basis for the critical comparison of tapping techniques, prevention measures, and detection methods undertaken in this review.

1.2. Evolution of Fiber Tapping Research and Scope of the Review

The history of research on fiber tapping can be broadly divided into three stages. The first stage dates to the late 1990s, when Medard et al. [7] and others analyzed attack scenarios and possible defensive techniques for optical networks. These early studies established fiber tapping as a physical-layer security problem, although the techniques and countermeasures were later developed beyond the initial scenarios.

A second stage, approximately covering the 2000–2011 period, established much of the technical basis for the analysis of tapping and jamming in fiber links. The fundamental mechanisms and possible countermeasures were presented in several publications [8–10], and selected tapping techniques were also patented [11–13]. During this period, the idea of "starving" a fiber tap with a minimized link power budget was described [14]. Non-invasive bending couplers were developed to facilitate fiber installation and servicing [15] and became commercially available [16–20]. In fact, bending couplers were introduced considerably earlier, in the 1980s, as components of Light Injection and Detection (LID) type fusion splicers for single-mode fibers.

A third stage, beginning circa 2015, has been characterized by increasing attention to the detection of physical intrusion (fiber tap). In particular, new methods for detection of fiber taps based on monitoring of State of Polarization (SOP) have been developed and ex-

perimentally evaluated, showing increased efficiency with respect to Optical Time Domain Reflectometry (OTDR) and monitoring of receiver input power [21–26]. Machine Learning methods have also been applied to improve the accuracy of intrusion detection [23,25–27]. In parallel, security regulations for physical protection of critical cables have been introduced by the National Security Agency (NSA) [28].

The strategic relevance of physical access to fiber infrastructure is particularly evident for submarine cable systems. Tapping of submarine fiber cables became the subject of a high-profile report in The Wall Street Journal in 2001 [29], which discussed the use of the U.S. Seawolf-class nuclear submarine SSN-23 Jimmy Carter. The submarine has been extensively modified for special underwater operations by the addition of 2500 t, 31 m long hull section known as a Multi-Mission Platform, intended for clandestine operations including work on cables and support for divers and submarine vehicles, at a cost close to $1 billion [30,31]. As mentioned in [31], the only other country with comparable capability is Russia. Even though information on intelligence operations is limited, such reports should be interpreted as indirect evidence of the strategic importance of access to submarine cables.

More recent reports emphasize both the increasing dependence of national and international communications on submarine fiber cables and their vulnerability to physical interference [31,32]. They also describe a progressive geopolitical separation of submarine cable infrastructure, routes, and suppliers [33] of two opposing alliances. Such developments may increase the strategic importance of obtaining physical access to cable systems that do not traverse territories controlled by the interested party.

Against this background, the present review provides a critical synthesis of the physical mechanisms that enable fiber tapping and the factors governing practical feasibility and detectability of fiber taps. Particular attention is given to the optical power budget constraints of passive taps, the relative merits and limitations of different coupling techniques, and the effectiveness of available prevention and monitoring approaches. The review also compares conventional OTDR and received-power monitoring with more recent SOP-based methods and examines the extent to which emerging multi-core and hollow-core fibers may alter physical-layer threats. For MCF and HCF, the discussion is explicitly framed as a prospective engineering assessment based on their known optical properties and on established tapping mechanisms for conventional fibers.

The review is based on material published between 1998 and 2026, with source collection completed on 7 October 2026. The sources considered include scientific and technical publications, standards, patents, product data sheets, and selected media reports and websites addressing the topics covered by this review.

The next chapters present the following subjects: principles and techniques of fiber tapping (2), link design ideas for preventing fiber tapping (3), methods for detecting and locating fiber taps (4), prospects for tapping MCF and HCF (5). The paper ends with a discussion of findings (6) and conclusions (7).

2. Fiber Tapping

2.1. General

The arrangement for interception of data from optical fiber (Figure 1) includes:

- Passive coupling (tapping) of a part of the signal power out of the fiber;
- (optional) optical amplification of tapped signal;
- Equipment for reception of tapped signal and analysis of received data stream;
- Means of delivery of captured data of interest to the attacker.

We will focus on methods of extracting the signal from the fiber (Figure 1a,b) in order to analyze the data stream. Telecom networks as well as backhaul and fronthaul infrastructure in radio access networks (4G, 5G, 6G) and high-speed links between data

centers are built exclusively with single-mode fibers of several types [34–36] (Section 2.5.1); therefore, descriptions and technical data below apply to single-mode fibers.

2.2. Power Calculations of Fiber Tap

We consider the situation when a factory-made coupler [2,3] is installed in the fiber optic link under attack as shown in Figure 2. It splits the optical power incoming at its Common (C) port between Line (L) and Tap (T) ports. The proportion of incoming power routed from common port C to tap port T (tap ratio) is specified in percent:

$$TR = (P_T/P_C) \times 100\%, \quad (1)$$

where:

TR—tap ratio [%];
P_T—optical power exiting the T port [W];
P_C—optical power entering the C port [W].

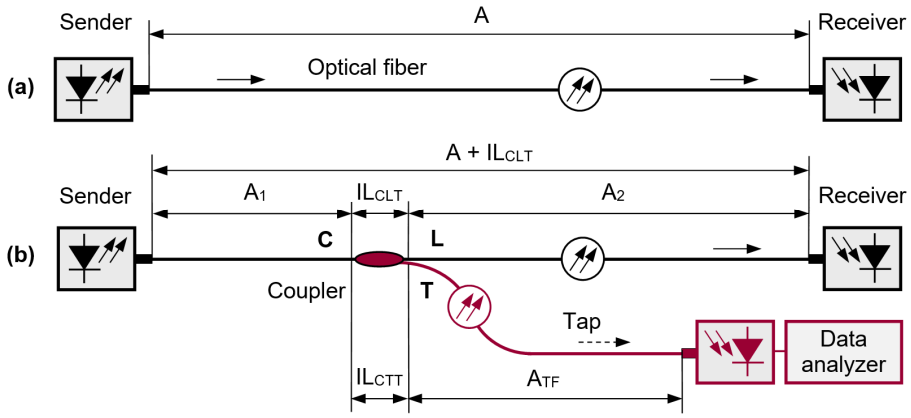


Figure 2. Fiber optic link (**a**) before and (**b**) after installation of passive tap for eavesdropping. Components of the losses of the link and tap are shown in the upper and lower parts of drawing (**b**), respectively. Normal parts of the fiber optic link are shown in black, and the attacker's hardware in red. Arrows indicate direction of light propagation. Loss parameters are defined in the text and formulas below.

Data sheets of fiber couplers include "split ratio": nominal percentages of power at the C port directed to L and T ports. Tap ratio of 10% corresponds to split ratio of 10/90% or 10–90; the sum is always 100%. Commercial couplers are manufactured with several values of tap ratio. The tap ratio of most other couplers is adjusted during field assembly of the tap—see Section 2.3—and remains fixed throughout its existence.

Theoretical insertion losses of the fiber coupler resulting from the split of optical power between L and T ports: IL_{CT} (for C-T path) and IL_{CL} (for C-L path) are calculated as follows:

$$IL_{CT} = 10 \log (100/TR) = 10 \log (P_C/P_T) \text{ [dB]}. \quad (2)$$

$$IL_{CL} = 10 \log [100/(100 - TR)] = 10 \log (P_C/P_L) \text{ [dB]}. \quad (3)$$

The latter is the localized loss added to the initial one of the fiber under attack. However, actual losses of C-T and C-L paths are higher, as two extra components are added:

- Added loss of the coupler resulting from structural imperfections (IL_S): 0.2–0.5 dB, corresponding to the coupler's optical efficiency (OE) between 89% and 96%;
- Loss of fusion splices or connectors to fiber under attack (IL_C): 2 × (0.1–0.5) dB.

Optical efficiency of coupler OE is defined as the proportion of light power removed from tapped fiber (P_R) delivered to tap port T (P_T):

$$OE = (P_T/P_R) \times 100\% \quad (4)$$

It is often convenient to use a logarithmic scale instead, e.g., during measurements:

$$OE = 10 \log (P_T/P_R) \quad (5)$$

Tap couplers other than factory-made fused or planar waveguide couplers [2,3] often have low efficiency; this applies particularly to bend couplers where only a small proportion of light escaping a bent fiber can be collected.

Total insertion loss added to the C-L path is:

$$IL_{CLT} = IL_{CL} + IL_S + IL_C \text{ [dB]}. \quad (6)$$

For a 10–90 coupler having IL_{CL} of 0.46 dB (and any other with a lower tap ratio), extra losses exceed the insertion loss resulting from the split of the incoming signal. When the link shown in Figure 2 is tested with an OTDR, the instrument detects a single localized loss IL_{CLT}. When the coupler is installed close to a connector at an optical distribution frame (ODF), at a distance shorter than the spatial resolution of the OTDR, there is no separate lossy "event" on the fiber trace, but the loss of the connector is apparently rises by IL_{CLT}. Increased tap ratio TR is accompanied by larger insertion loss added to C-L path IL_{CL}, undesirable because tap detection is easier. Examples are shown in Table 1.

Table 1. Insertion loss of 100% efficient fiber coupler for typical tap ratios. For the installed coupler, added loss resulting from splices, connectors and coupler imperfections of 0.5 dB is assumed.

Split Ratio	Theoretical Insertion Loss		Total Insertion Loss	
	IL_{CT}	IL_{CL}	IL_{CTT}	IL_{CLT}
%	dB	dB	dB	dB
1–99	20.00	0.04	20.05	0.54
2–98	16.99	0.09	17.49	0.59
3–97	15.23	0.13	15.73	0.63
5–95	13.01	0.22	13.51	0.72
7–93	11.55	0.32	12.05	0.82
10–90	10.00	0.46	10.50	0.96
15–85	8.24	0.71	8.74	1.21
20–80	6.99	0.97	7.49	1.47
25–75	6.02	1.25	6.52	1.75
50–50	3.01	3.01	3.51	3.51

Notes: parameters of couplers are wavelength-dependent and have production tolerances in the order of ±0.3 dB; real test data can be found in paper [21]; calculations above cannot be made for most fiber taps other than factory-made couplers, as they have low optical efficiency and high extra losses, e.g., 10 dB.

The formula for calculating insertion loss of installed coupler in the C–T path is similar, but values are much larger than in the C–L path, as shown in Table 1:

$$IL_{CTT} = IL_{CT} + IL_S + IL_C \text{ [dB]}. \quad (7)$$

Power delivered to the attacker's receiver P_{TAP} depends on losses of: (1) part of the fiber link (fibers, splices, connectors, WDM devices, etc.) extending from the transmitter to

just before coupler A_1 (see Figure 2.), (2) tap coupler and splices or connectors added during its installation, IL_{CLT} (4), and (3) tap fiber linking port T of the coupler to the receiver (A_{TF}):

$$P_{TAP} = P_{TX} - A_1 - IL_{CLT} - A_{TF} \text{ [dBm]}, \quad (8)$$

where:

P_{TX}—power launched into fiber by link transmitter (sender).

This calculation proves that that:

- A tap working in one direction is best installed near the transmit end of the link, to minimize A_1 loss,
- Installing two taps for both directions of transmission at the same location in the middle of a long link is difficult, because the loss of each tap from the sender to the attacker's receiver is increased by approx. half of link loss A, and the power P_{TAP} delivered to this receiver may be too low for error-free reception. The attacker may have to install taps at two separate locations to meet the condition above.

When a tap is installed near the transmitter (the best location), the required tap ratio TR in linear scale [%] is approximately equal to the inverse of product of link power budget PB—the ratio of transmitter power P_{TX} and receiver sensitivity P_{RXMIN} in Watts, and the optical efficiency OE. For TR and OE in %, the calculation is made as follows:

$$TR \approx 1/(PB \times OE) = P_{RXMIN}/(P_{TX} \times OE) \quad (9)$$

With all parameters in logarithmic scale (dB for ratios, dBm for powers), the formula becomes:

$$TR \approx P_{RXMIN} - P_{TX} - OE \quad (10)$$

or:

$$TR \approx -(PB + OE) \quad (11)$$

It is assumed that the power margin of the tap equals one of the links being tapped.

Loss of installed outdoor single-mode fiber A [dB] having attenuation α [dB/km] and length L [km], with fusion splices having loss IL_S (approx. 0.1 dB) every 1–2 km can be estimated in accordance with the following formula:

$$A \approx L\,(\alpha + 0.05 \text{ dB/km}) \quad (12)$$

Attenuation α depends on wavelength; typical values are:

- Single-mode fiber at 1310 nm: 0.30–0.35 dB/km;
- Single-mode fiber at 1550 nm: 0.16–0.25 dB/km;
- Single-mode fiber at 1625 nm: 0.18–0.27 dB/km.

2.3. Methods of Covert Coupling to Fiber Under Attack

The basic list of methods for covert coupling to single-mode optical fiber was given in the 2004 paper by Shaneman and Gray [8], and patents [11–13]:

(a–c) **splicing or insertion of a coupler** (a ready-made component) into the fiber path, which can be done in several ways;

(d) **bending** of fiber at radius low enough to cause partial escape of light;

(e) **evanescent coupling** of light to another fiber or photodetector after partial removal of cladding to within 10–15 μm of fiber's core;

(f) **collection of scattered light** leaking from the fiber as a result of Rayleigh scattering. This applies also to light propagated in lossy higher-order modes;

(g) **V-groove** cut into fiber's cladding close to core, at distance as in (e). For single-mode fiber, this is a special type of evanescent coupling;

(h) **FBG**: making a blazed and chirped Bragg grating in the fiber's core by irradiation with ultraviolet (UV) laser and phase mask. This grating reflects a part of guided light out of the fiber.

Methods (g) and (h) are difficult and time-consuming, requiring clean conditions and dedicated, costly instruments, thus are unlikely candidates for field installation of taps. The most useful (in the author's view) methods are (a–c), (e) and maybe (f) illustrated in Figure 3.

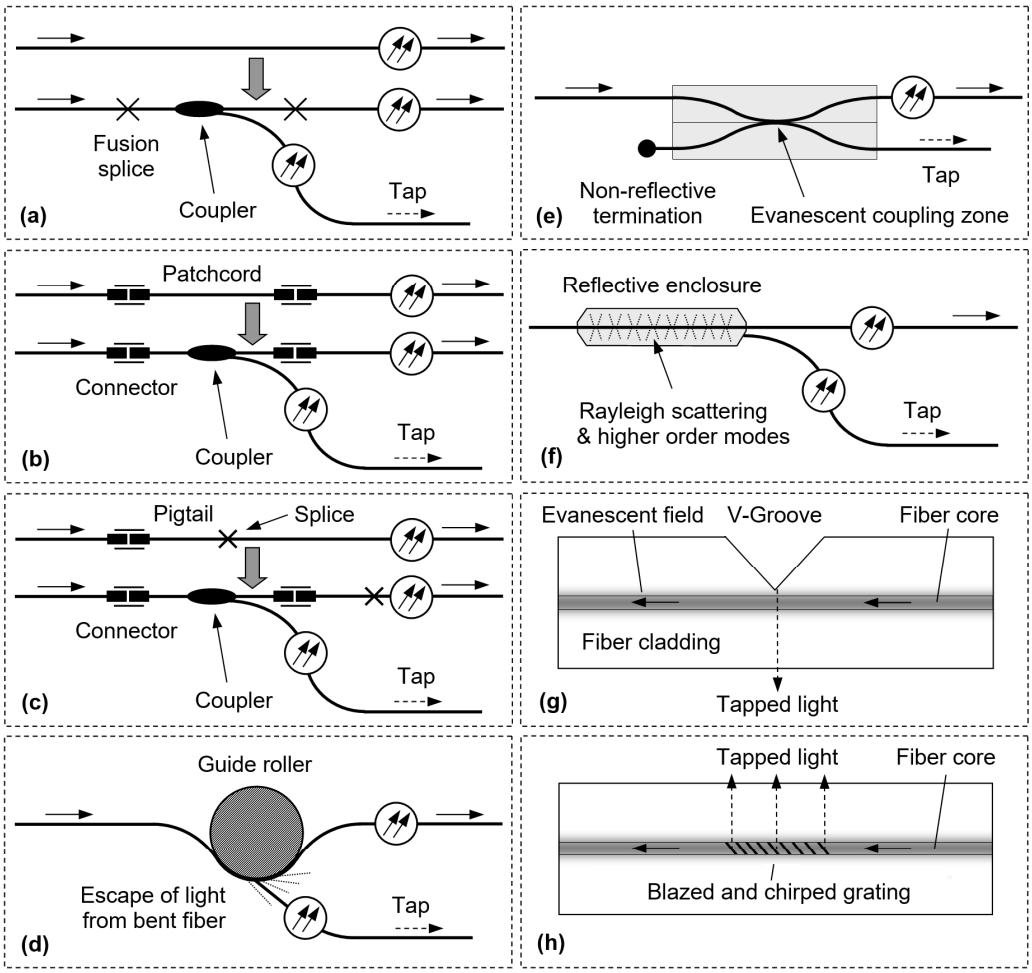


Figure 3. Basic types of fiber taps for one direction of transmission: (**a**) splicing of fiber coupler into the link; (**b**) replacement of patchcord with connectorized coupler; (**c**) insertion of connectorized coupler; (**d**) bending of fiber to cause escape of light; (**e**) evanescent coupling of light to another fiber; (**f**) collection of scattered light leaking from the fiber; (**g**) V-groove tap; (**h**) making chirped and blazed Bragg grating in the fiber. In arrangement (**f**), the photodetector may be placed inside a reflective enclosure for improved coupling efficiency. The "X" sign means a fusion splice. Arrows indicate direction of light propagation.

Note: tapping multi-core and hollow core fibers is different and reviewed in Section 5.

Most techniques shown in Figure 3 require direct access to a short length of fiber in primary protective coating, ca. 50–100 mm. The fiber must be extracted from a fiber optic cable by localized removal of sheath from the cable and protective tubes or tight buffers from the fiber(s), with two exceptions:

- Installation of connectorized coupler (b, c);
- Bending of buffered fiber (d).

Eavesdropper's work is simpler when individual fibers are already extracted, in particular in a joint closure between two lengths of cable (typically located every 1–3 km along the cable line, and re-enterable) or in an optical distribution frame or box located at each end of the line. Joint closure or distribution frame in a metropolitan network often holds hundreds of fibers from multiple cables, and a compact coupler [2,3] added as shown in Figure 3a, b may be difficult to find during visual inspection.

The bending method (d) is not affected by the colored coating of the fiber, because the organic dyes used are transparent at infrared wavelengths longer than ≈800 nm.

It is possible to make a special fiber having middle layer of cladding doped with UV–absorbing oxide of transitory metal like nickel [37]. This prevents making a blazed and chirped Bragg grating (Figure 3h). Unfortunately, nickel oxide-doped glass absorbs infrared radiation in the 1300–1600 nm band some 400 times less than a 220–250 nm UV one. A 30–40 μm thick layer of glass with 2% nickel content introduces loss of about 1 dB, too low to prevent tapping using methods (d), (e) and (f).

Comments specific to each coupling method shown in Figure 3 are as follows:

(a) Splicing of coupler into fiber path

A commercially available pigtailed fiber optic coupler [2,3] is installed by cutting the fiber of interest and making two fusion or mechanical splices to this fiber. Loss of fusion splices is low ($\leq$0.20 dB), stable and almost independent of wavelength. Loss of fiber continuity during installation lasts 2–4 min and an OTDR-based monitoring system making periodic measurements, e.g., every 10 min, may fail to detect it, but the receiver of the affected link will generate an alarm. The direction of transmission and schedule of the OTDR monitoring system (sending pulses in a direction opposite to the transmitter) can be established with a bend-based live fiber identifier [20].

No special components and tools are needed. Installation of the tap in a cassette for fusion splices requires two additional splice protectors and one fiber coupler of similar shape and size (but in metallic case), hard to find among hundreds of splices in high-capacity joint closure. The tapped signal can be sent out via a "dark" (unused) fiber in the same cable.

(b) Replacement of patchcord with connectorized coupler

Connection of a coupler having pigtails made of indoor cables and connectorized into the optical path of the targeted link. This coupler can substitute a patchcord, especially in data centers, where links between racks are long—up to 50 m or more; patchcords and most of their lengths lie in cable trays together with numerous other cables. An attacker's coupler can be placed there and hidden under cables, which is critical because couplers with indoor cables have characteristic rectangular cases. The original patchcord is removed or hidden to eliminate signs of tampering.

(c) Insertion of connectorized coupler at ODF

In telecom systems, the best location for a coupler is an Optical Distribution Frame (ODF) near the link's transmitter. One of coupler's connectors replaces the original one at the ODF bulkhead, while the other is connected to it in an adapter hidden between fiber cables. The attacker must have access to the cable plant side of the ODF. A connectorized coupler may also replace a patchcord linking the transmitter to the ODF, being hidden in a bunch of cables or coiled extra lengths of them.

Advantages of methods (b) and (c) are speed—loss of transmission lasts about 10 s, and no need for tools or fusion splicing.

(d) Bending of fiber

Fiber is extracted from the cable; it may remain in a tight buffer, but not in a loose tube or ribbon holding multiple fibers. A commercially available clip-on coupler [15–17] is attached to it. Inside the coupler, the fiber is bent on a small radius (R ≈ 2–4 mm); a part of guided radiation escapes from it and is collected by the tap fiber. A detailed description of this device is in paper [18]. This method is less invasive than (a): the fiber is not cut, and the coupler can be removed without a trace, unless the cable sheath and tubes were removed.

Problems include: (a) rapid increase in loss introduced by the bend and proportion of tapped light with wavelength: the same bend introduces approximately 3–fold higher loss at 1550 nm than at 1310 nm, (b) variable behavior of different fibers.

To tap a single-mode fiber conforming to ITU-T Recommendation G.652.D [34] or G.654 [35], a single partial bend at ≈4–5 mm radius is necessary, applied by a roller and conformant fiber guide. "Bending-tolerant" and "bending insensitive" fibers of G.657.A1/A2 categories [36], frequently found in microcables and access networks, require a tighter bend, down to 2 mm, for similar effect. Bending of 125 μm fused silica fiber at a radius smaller than 2 mm frequently results in fiber break [18]. The "bending-insensitive" fibers of G.657.B3 category can break before a useful leak of radiation is produced, particularly if the tap is to operate for months or years.

NTT team developing a clip-on coupler for maintenance of single-mode fiber networks [18] assumed an acceptable loss introduced into the fiber link (Figure 2) in the C-L direction (IL_{CL}) of 2 dB at 1550 nm; this value is within the power margin of a conventionally designed telecom fiber link. In this situation, the loss of a fiber tap (C-T direction) from a G.652 single-mode fiber is ≈15–18 dB to multimode tap fiber—fibers with 50, 62.5 and 105 μm diameter cores were tested—and ≈22 dB to single-mode fiber at 1310 nm. Coupling of the leaking light beam to the tap fiber was assisted with a GRIN lens. In fact, such a coupler is easily detected with a 1650 nm OTDR as localized loss of about 5 dB. Commercially available clip-on couplers [15–17] have similar tap losses between two G.652 single-mode fibers: 13–17 dB at 1310 nm and 17–22 dB at 1550 nm, but the losses introduced to the fiber link (C-L) are high: 3–8 dB at the same wavelengths.

These parameters depend on the sensitivity of the tapped fiber to macrobending. To avoid introducing high loss into a bending-sensitive fiber like G.654 and causing an alarm, the guide roller shall be pushed slowly against the fiber under attack, while the power of the tapped signal is controlled with an optical power meter. A good clip-on coupler shall allow adjustment of bending radius, e.g., by selecting one of several guide rollers of different diameters.

Optical efficiency of the clip-on coupler as defined in Section 2.2 (Formulas (4) and (5)), is very low. For a C–L loss of 2 dB, theoretical loss of tap (C–T) is less than 6 dB. Data listed above correspond to efficiencies of only 3–12%, or between −15 dB and −9 dB, while the efficiency of fiber couplers of fused or planar design, used in methods (a–c), is typically 90–95% [2,3].

Interestingly, analysis [38] shows that the efficiency of tapping can be highest for the "bending-insensitive" fibers conforming to the G.657 standard [38], specifically because a smaller radius is required. One consequence is a shorter length of bent fiber emitting light collected by the attacker, and more efficient coupling of a narrower light beam to the tap fiber.

While tapping of fiber links with clip-on couplers is the method most frequently described in the literature on security of fiber networks, it is in fact of little use for professional eavesdropping due to the low efficiency of the coupler and easy detection of the tap.

Additionally, a clip-on coupler is a device with no other applications today, constituting a tampering evidence.

(e) Evanescent coupling

The fiber to be tapped is stripped of all coatings and glued with epoxy to a curved guide having a 2–10 mm radius, dependent on fiber category and bend sensitivity. Once the glue is cured, partial removal of fiber cladding is performed by lapping and polishing it away; continuity of fiber core is retained at all times [9]. The tap fiber is earlier prepared in the same way on another, identical guide. Finally, guides with both fibers are precisely aligned and fixed with a thin layer of epoxy glue between them.

With guides of proper bend radius for a given fiber, a coupler of this design is suitable for any type of telecom single-mode and multimode fiber. The power of the tapped signal rises with depth of polishing and must be periodically measured with an optical power meter. Interestingly, correct alignment of both fibers can be felt by the person holding both guides, because fused silica is harder than epoxy and the fiber slightly protrudes [11]. Making such "evanescent coupler" as shown in Figure 3e is time-consuming, while insertion loss introduced by this device is reportedly at least 1–2 dB [8]. The author is sure a lower loss is achievable, but careful work in clean conditions is essential; use of multimode fiber for the tap side is helpful for reduction in loss and easier assembly. Besides curved fiber guides, all tools, epoxy glue and polishing materials are commercially available for assembly of fiber optic connectors.

(f) Collection of scattered light

A section of fiber 50–100 mm long, straight and with coating, is surrounded by a highly reflective (at the link operating wavelength!) enclosure made of two halves, and with tap fiber attached. At each point along the fiber, a small part of the guided radiation is lost due to Rayleigh scattering [12], and the power of the tapped signal is proportional to the length of the reflective enclosure. This radiation is collected by a fiber or photodetector at the end of the enclosure facing the link receiver. Light collected at the opposite end or on the side is affected by dispersion resulting from differences in optical path lengths, up to 0.5 ns for a 50 mm long enclosure; this prevents reception at 10 Gb/s and higher data rates. This tap is undetectable: fiber loss and OTDR signature do not change because the attacker only collects light normally lost from the fiber. A big drawback is that only a very low part of power of signal propagating in the fiber is scattered. Assuming 100% efficient light collection, approximate values for a 50 mm long fiber are:

- –58 dB (single-mode fiber, 1550 nm),
- –55 dB (single-mode fiber, 1310 nm),
- –44 dB (OM2/3/4/5 multimode fiber, 850 nm).

This method can be useful for tapping links with high-power EDFA optical amplifiers, e.g., long submarine links, at locations close to them. An optical preamplifier may be required, as shown in Figure 1b. In most terrestrial networks, one cannot tap optical power large enough for data reception this way. A tap installed very close to the sender or booster amplifier can also collect radiation propagating in lossy higher-order modes, but the proportion of additional power tapped this way varies a lot, depending on fiber and quality of splices, as offset of cores results in excitation of higher-order modes.

The proportion of tapped power can be substantially increased when a short length of the fiber is stripped and tapered while remaining straight, using a fusion splicer. Experiments reported by Bradley et al. [39] involved tapers on fibers of G.652 and G.657.A1 types. The complete up-and-down transition was 12 mm long and had a waist length of 2 mm; the total taper length was 26 mm. Tapering of 125 μm clad fiber, down to 25 μm, allowed adjustment of the tap ratio (TR) over a wide range. Tapping of G.657.A1 fiber in this manner was more efficient than G.652 one: a 45 μm taper extracted 1% of power

from the fiber (−20 dB), while loss introduced to the signal path (IL_{CL}) was 0.45 dB. For a G.652 fiber, a 50 μm taper introduced IL_{CL} = 0.5 dB, but only 0.03% (−35 dB) of power was extracted. This difference is explained by the much larger diameter of the outer part of the mode field in tapered G.657 fiber. These data do not account for the collection efficiency of the enclosure.

However, while making a taper does not break the fiber, heating it to temperatures in excess of 1400 °C produces reversible high loss and a short (seconds) break in transmission, resulting in "loss of signal" alarm at the receiver.

(g) V-groove tap

The fiber is extracted from the cable and stripped of all polymeric coatings. Next, a V-groove with surfaces oriented at an angle to the fiber axis larger than half of the acceptance angle of the fiber, $\geq$ 8 degrees for telecom-type single-mode fiber, is cut into the cladding. The tip of the V-groove may not enter the fiber core, but is close enough to the core, ≈10 μm, to intersect a part of the evanescent field (periphery of mode field), and reflect a portion of radiation guided by the fiber. Reflected radiation passes through the core and cladding, emerging on the opposite side of the fiber. During cutting, tapped power must be frequently monitored with an optical power meter. In multimode fibers, the evanescent field is shallow with respect to radius of core, and some penetration of the V-groove into the core is needed to tap enough of signal power. The other side of the V-groove shall be slanted similarly to the first one; otherwise, the tap will produce strong reflection, up to −15 dB, easily detectable with OTDR. This method requires precise cutting equipment with a diamond blade, clean conditions, good lighting, and a lot of time. Fiber break during this operation is likely. Advantages include uninterrupted transmission and high efficiency of the coupler. The finished V-groove must be protected from the entry of condensing humidity, glue, or jelly from the cable.

(h) Fiber Bragg Grating

This method is based on reflection of some light guided in the core by a Fiber Bragg Grating (FBG) created by exposure to ultraviolet radiation, e.g., at 248 nm wavelength, produced by a laser and passing through a phase mask. The FBG must be blazed to ensure escape of reflected light from the fiber instead of sending it back to the transmitter and chirped to reflect light in a certain range of wavelengths. Before this operation, the fiber must be removed from the cable and very carefully cleaned. For best FBG quality, removal of fiber coating is desirable. Tapped light is collected on the side of the fiber, as in method (g). This is the most difficult and least practical of methods described in the literature, requiring costly equipment, mains (or generator) power, a skilled worker, and a long time, especially as sensitization of fiber with high-pressure (e.g., 100 bars) hydrogen is rather impossible. The other drawback is difficult matching of FBG characteristic wavelength to operating wavelength of link's transmitter. In a single-wavelength link, the sender usually exhibits large wavelength tolerance like ±20 nm or even more, and temperature sensitivity in the 0.1–0.5 nm/K range; additionally, low-cost transceivers with directly modulated Fabry–Perot lasers emit at multiple wavelengths occupying a range typically 10 nm wide. Considering this, the only realistic application is tapping a single channel from a DWDM link, where carrier wavelengths are precisely controlled. Additionally, the grating emits reflected radiation as a linear source, and dedicated optics for effective coupling it to tap fiber is needed.

2.4. Other Tapping-Related Issues

The tap shall be installed in a way minimizing introduced reflections, which allow detection of tap with OTDR, using Angled Physical Contact (APC) connectors and arc fusion splicing if possible.

Irrespective of the technology employed to install a fiber tap, the attacker usually must deliver the tapped signal to his data analyzer using 1 or 2 fibers. The analyzer is rather bulky and requires electric power and a safe space for installation. Instead of laying or pulling a concealed new cable for this purpose, one may utilize "dark" fibers from existing cable leading to a safe location for installing the attacker's equipment, accessible at a joint closure (especially a branching one) or an optical distribution frame. Such occasions exist particularly at large telecom facilities offering colocation. A brazen way of installing a complete eavesdropping system is to place the data analyzer at the same facility, by renting colocation space and internet access through a shell company, or by bribing an employee of the company present there, familiar with the particular facility.

Invasive installation of a tap, including fiber cut or disconnection, as shown in Figure 3a–c, can be done undetected when the link (and its monitoring devices, too) are temporarily out of service for reasons like equipment upgrades, loss of electric power, or deliberate cable cut at location between tap place and OTDR test head, purportedly to steal a copper cable passing through the same manholes.

When the link to be attacked operates in one of the wavelength bands covered by fiber amplifiers, either EDFA: ≈1528–1565 nm and ≈1570–1605 nm, or BDFA (still largely in development): ≈1300–1480 nm, it is possible to install a long (10 s of kilometers) tap fiber exhibiting a large loss, fed by an EDFA installed near the coupler, with its T port connected to the EDFA input, as in Figure 1b. Gain up to 30 dB is possible, but EDFA requires electric power. Instead of an amplifier, a repeater can be installed. If local power is not available, the EDFA can be remotely pumped with 1480 nm radiation delivered via another fiber from a safe location with a data analyzer and other attacker's equipment.

Tapping of a selected channel („lambda") from a DWDM or CWDM wavelength-multiplexed link (with fixed, equally spaced spectral arrangement of channels) is possible by adding a suitable wavelength demultiplexer between the T port of the coupler and the attacker's receiver, as both of those devices are not spectrally selective. EDFA is useful for tapping a DWDM link because the DWDM multiplexer introduces loss of 3–7 dB. It is of limited use for attacks on CWDM links, as only 3 of 8 commonly used carrier wavelengths: 1531, 1551 and 1571 nm can be amplified with it.

2.5. Fibers in Telecommunications and Data Transmission Networks

2.5.1. Single-Mode Fibers

Descriptions here apply primarily to tapping of single-mode fibers made of solid fused silica currently used in terrestrial telecom and data networks, predominantly of the following categories standardized by ITU-T:

- general purpose G.652.D [34];
- loss-minimized with undoped core G.654.E [35];
- bending tolerant G.657.A1 [36]; and
- bending insensitive G.657.A2 [36].

Fibers listed above are also covered by the IEC standard 60793-50 [40]. IEC fiber category designations are a little different, e.g., B-652.D instead of G.652.D.

Fibers for submarine networks are standardized as categories G.654.A-D in ITU-T G.654 recommendation [35]; one of their properties important here is reduced bending tolerance in comparison to most common fibers conforming to the ITU-T G.652.D standard. This is caused by a larger mode field diameter (MFD) and undoped core, features adopted to reduce fiber attenuation and optical nonlinearity.

Conversely, fibers belonging to G.657.A1 category tolerate lower radius of bending at the same bending loss and proportion of light escaping the fiber which can be collected by

the attacker. G.657.A2 fibers tolerate even stronger bending. Bending radii specified for testing of single-mode fibers are 30 mm, 15 mm, 10 mm and 7.5 mm, respectively.

Single-mode fibers rated for 5 mm and even 3 mm bending radius exist, designated as G.657.B3 category [36], but are used relatively little, primarily for indoor segments of access networks where cables can be installed using crude techniques like stapling and work in harsh mechanical conditions, e.g., being routed around corners. Bending of G.657.B3 fiber at decreasing radius may result in fiber break before introduction of easily detectable bending loss like 0.5 dB.

Different bending sensitivities of fibers are important for this type of tapping. With the current and legacy variety of deployed fibers, it is impossible to make a bending-based coupler exhibiting desired insertion loss and coupling efficiency with every type of fiber, unless the geometry of bend is adjustable or fiber category known. Luckily for spies, fiber category is required in standards to be marked on cable sheath.

2.5.2. 50/125 μm Multimode Fibers

Fundamental techniques and physics of tapping apply also to multimode fibers (MMF), currently almost exclusively of 50/125 μm graded index type, with standardized products [41,42] known as OM2, OM3, and OM4 for transmission at single wavelength close to 850 nm, and OM5 for CWDM transmission at 4 wavelengths: 850, 880, 910, and 940 nm [42]. Main differences important for tapping are as follows:

- Telecom multimode fibers have a larger core: 50 μm vs. 4.5–13 μm in single-mode fibers and are better for collecting light escaping from tapped fiber. However, long-wavelength (1260–1620 nm) transponders may be incompatible with them due to the small diameter of the photodetector active area.
- Multimode fibers have a larger numerical aperture (NA): ≈0.25 vs. ≈0.14 in single-mode fibers and a larger acceptance angle; again, this improves collection of light escaping from the fiber being tampered with.
- Transmission over multimode fibers employs wavelengths close to 850 nm vs. several bands (O, E, S, C, L, U) between 1260 and 1675 nm used in single-mode networks. Different photodetectors/transceivers and components, e.g., couplers, are required. Silicon Avalanche Photodiodes (APDs) useful at 850 nm are considerably more sensitive than InGaAs photodiodes required for wavelengths above 1100 nm due to substantially lower dark current.
- Due to modal dispersion and large attenuation ≈2.5 dB/km at 850 nm, multimode fibers are limited to transmission at short distances, usually less than 2 km, primarily within data centers and commercial buildings with Local Area Network (LAN).

3. Link Design for Prevention of Fiber Tapping

3.1. Recommended Solutions and Practices

There are no 100% effective defenses against professional, well-equipped, and trained state or corporate spies, especially when the operator's budget is limited and existing facilities (cable lines, ODFs, repeater sites, etc.) are to be reused for carrying sensitive data, including shared public infrastructure. Still, the author recommends some measures which can make tapping of fiber networks significantly harder. Each of them can be employed independently of others.

1. Reduction in link loss budget, with receiver's power margin ≤2 dB. Optical transceivers shall have the highest sensitivity available commercially for a given data rate, wavelength, and type of fiber. Input power to the receiver shall be suitably adjusted with an optical attenuator (Figure 4) installed at the **transmitter's** optical port, in a locked and monitored room or enclosure. The attacker usually will be unable

to buy a more sensitive receiver. For error-free reception of the tapped signal, he will need to tap a large proportion of the signal from the fiber, up to 30–50% when the link is short, e.g., 3 km with total loss ≈2 dB @ 1310 nm or ≈1.5 dB @ 1550 nm. Such a tap introduces loss ≈3 dB (Table 1), exceeding link's power margin, causing link failure. It is also easy to detect.

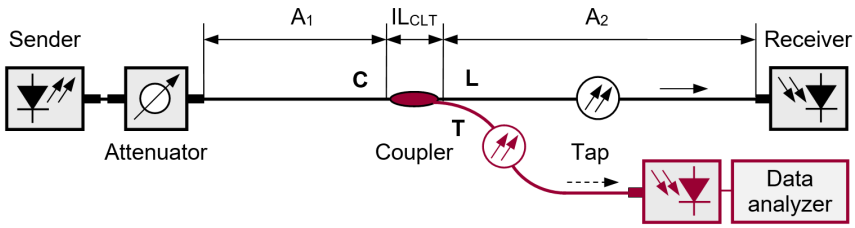


Figure 4. Optical fiber link with minimized power margin P_M. Situation after installation of passive tap for eavesdropping. Normal parts of the fiber-optic link are shown in black, and attack-related components in red. Arrows indicate direction of light propagation. The sum of A_1 and A_2 losses equals the original loss of the fiber link A.

2. Avoiding transmission in the C and L bands (1525–1610 nm), where EDFA pre-amplifiers can significantly improve the sensitivity of the attacker's receiver (Figure 1b). 1511 nm transceivers manufactured for CWDM networks can be used instead. Although experimental bismuth-doped fiber amplifiers (BDFA) for O, E and the short-wave part of S band exist, they exhibit low gain at this wavelength, but higher at 1310 nm.
3. Use of connectors with a security lock requiring a dedicated key to disconnect [43]. It makes an attack using the method shown in Figure 3a impossible or at least complicated.
4. Limiting the number of ODFs and rooms the cables and fibers are passing through, and the number of connectors between sender and receiver.
5. All ODFs, racks, joint closures and rooms shall be locked and periodically inspected. Monitoring of rooms and manholes is strongly recommended.
6. Optical monitoring of fiber links. Several methods exist—see Section 4.
7. Avoid colocation facilities accessible to numerous operators, ISPs, installers, and service teams—some of them may work for attackers.
8. Set up several fiber paths, preferably without common nodes or cables, except for terminals, and switch sensitive traffic between them at random times. Their end-to-end loss shall be equalized with attenuators installed at the transmit end to allow use of measure (1). A break in transmission or change in optical loss shall trigger instant switchover to another fiber path, and investigation of the problem.
9. Up-to-date encryption of transmitted data, forming a second line of defense: fiber may be tapped, but data are unreadable. Encryption is outside the scope of this paper.

3.2. Minimized Loss Budget

Method (1) listed in Section 3.1, simple and relatively inexpensive, but counter-intuitive, deserves more detailed description here. Proper design of the link loss budget can make tapping enough optical power for error-free reception by the attacker's equipment impossible, or easily detectable due to the high additional loss introduced.

For simplicity, it is assumed below that the attacker's receiver has sensitivity identical to one in the link being tapped. This sensitivity can be improved by adding a low-noise optical preamplifier—see Figure 1b. EDFA amplifiers, best for this purpose (NF ≈ 5 dB), operate in a limited spectral range, approx. 1525–1610 nm, which shall be avoided in single-wavelength links carrying secret data—see Section 3.1, p. 2.

A fiber link carrying sensitive information shall have a receiver of high sensitivity, defined as minimum input power P_{RXMIN} [dBm] ensuring specified error rate, e.g., $\leq 10^{-12}$. Power launched from the transmitter into the fiber P_{TX} shall be adjusted such that the input power at the receiver port in normal (tap-free) conditions P_{RX} corresponds to a link loss margin P_M of only ≈2 dB:

$$P_M = P_{RX} - P_{RXMIN} \approx 2 \text{ dB} \quad (13)$$

A sensitive receiver is usually part of a transceiver including a transmitter with high output power P_{TX}, such that link power budget PB defined by the formula:

$$PB = P_{TX} - P_{RXMIN} \quad (14)$$

is too large in short links. For example, SFP-10G-ZR-S SFP+ modules for 80 km long 1550 nm 10 Gb/s single-mode links [44] have PB = 24 dB. With such transceivers, the power margin of a 30 km long single-mode link having loss about 9 dB at 1550 nm is around 15 dB. In a short link, e.g., 10 km (≈3 dB loss), such transponders would not work, because the guaranteed receiver overload level is −7 dBm, while P_{RX} close to –3 dBm is expected.

The power margin of the link is reduced to 2 dB or another desirable value by inclusion of an adjustable optical attenuator between the transmitter and corresponding end of optical fiber, as shown in Figure 4. During attenuator adjustment, measurement of actual receiver sensitivity (usually better than declared by the manufacturer) shall be made first, and later the attenuator setting reduced to increase P_{RX} by a desired margin P_M, e.g., 2 dB.

The receiver's input power P_{RX} must be checked with an optical power meter.

So why use costly high-performance optical modules in a short link?

With low power margin P_M and power of signal in the fiber in location where the tap is made, the larger part of it must be branched to attacker's data analyzer. According to the data shown in Table 1, this results in higher loss introduced into the path towards the link receiver. Figure 5 shows these dependencies for the most favorable (for attacker) installation of a tap at the beginning of the fiber link ($A_1 \approx 0$ dB in Figure 2). With suitably low power margin P_M and link loss A (typical for short campus and urban networks), installation of a coupler delivering enough power to the attacker's receiver ($\geq P_{RXMIN}$) will result in transmission break and "loss of signal" alarm: the signal is too weak to be properly received both at the destination and by the attacker. More detailed analysis for Gigabit Ethernet (GbE) link can be found in paper [14]. Even when the receiver still works, loss introduced by the tap IL_{CLT} (Section 2.2) is easy to detect. A typical OTDR-based fiber monitoring system can reliably detect and locate discrete loss of 1 dB. If the fiber is monitored and P_M = 2 dB, the tap will be detected for link loss A ≤ 8 dB, and length up to 25 km (at 1310 nm).

In most situations, it is desirable for the eavesdropper to access data streams transmitted in both directions of transmission, for which (with the exception of wavelength-multiplexed fiber access systems) two separate fibers from the same cable are employed. To simplify preparations, the attacker tries to find a location along the line where the power of signals transmitted in both directions is large enough for tapping. The signal launched from the transmitter (sender) is steadily attenuated along the line, in proportion to fiber loss between transmitter and location of tap. The portion of signal power that must be tapped TR to ensure power reaching the tap receiver is larger than its sensitivity P_{RXMIN} rises with an increase in accumulated loss A_1 (Figure 4) and a decrease in link power margin P_M.

With $P_M \leq 2$ dB, installation of a tap in a short line with loss below 2 dB, corresponding to a length of about 5 km at 1310 nm, is impossible anywhere (Figure 5): TR ≥50% is required, leading to added loss of ≥3.5 dB (Table 1). The link will stop working or have a high bit error ratio (or packet loss ratio), and an alarm will be raised.

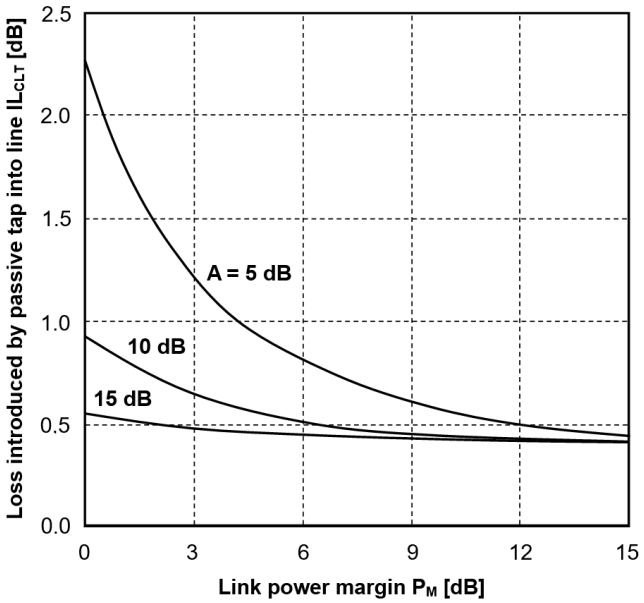


Figure 5. Minimum loss added to fiber optic link by a tap (IL_{CLT}) installed close to transmitter end as a function of link power margin (P_M) and end-to-end loss of this link (A). See Figure 4.

Prospects for successfully making a tap improve with length and total loss A of the fiber link targeted, provided the tap is installed close to the transmit end.

The best location for tapping both directions is in the middle of the link ($A_1 = A_2$) but work on outdoor cable in the field is needed. Alternatively, two taps can be installed at both ends of the line, with extra difficulty to obtain access there.

Figures 5 and 6 demonstrate clearly that a fiber optic link with a large (and desirable for reliability reasons) power margin P_M is a perfect target for installing a difficult-to-detect passive tap with a low tap ratio TR—see data in Section 2.2.

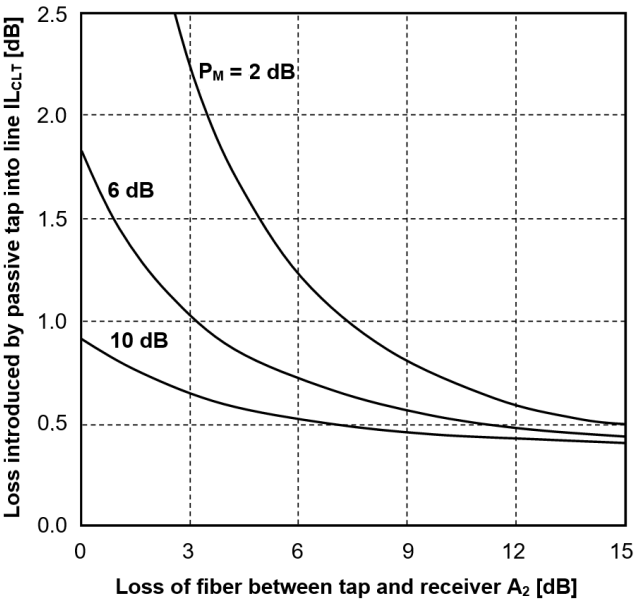


Figure 6. Minimum loss introduced by a tap (IL_{CLT}) installed near link transmitter as a function of link power margin (P_M) and loss of fiber path between tap and receiver (A_2). See Figure 4. Low P_M precludes installation of a tap near the receiver end.

4. Detection and Location of Fiber Taps

4.1. Inspection of Facilities

The complete route of cable(s) carrying secret traffic and all passive (joint closures, optical distribution frames, manholes, cable storage boxes, indoor cabling, . . .) and active devices (transceivers, routers, switches, . . .) in the signal path shall be inspected for:

- Signs of illegal access and tampering, e.g., damaged locks, discarded pieces of tubes, cable jackets, fusion splice protectors with fibers inside, etc.;
- Signs of work on cables, in particular removal of sheath or jacket;
- Unexpected devices, e.g., splitters or filters in metallic, tubular cases in joint closures or ODFs;
- New cables, patch cords, couplers, or electronics absent in network documentation;
- Signs of digging along the route of underground cable,
- Proper locking of all facilities and equipment;
- Proper operation of burglary alarms, security cameras, etc.

This excludes active devices which cannot access the data stream carried by protected fibers: power supply devices, batteries, air conditioners, lamps, etc. However, associated power and control cabling may be used to hide tap fibers, and is worth a close look.

As certain categories of tapping and data analysis equipment are easily removable on short notice, inspections shall not be carried out at predetermined dates known to all personnel (including one worker bribed by the attackers, maybe), but randomly, with a mandated maximum duration between them.

While requirements of NSA standard CNSSI No. 7003 [28] appear extreme, they are worth a review. NSA does a lot of SIGINT work, and they know how to do it.

4.2. OTDR Monitoring

An optical time-domain reflectometer is widely used for testing of fiber optic networks, including detection and location of localized faults exhibiting added loss or reflectance. Typical examples of the latter are cable or fiber cuts, poor-quality splices and connectors with excessive loss and/or reflectivity, fiber bends, and deteriorated cables.

OTDR tests a complete fiber link having access to only one end of it (unless true loss of splices is to be measured), and distance to the event of interest is calculated by converting time between launching a laser pulse and reception of echo, if the effective refractive index of fiber (n_{eff}) and helix factor (HF) (ratio of fiber length to cable length) are known. In principle, any number of "events" can be detected and located, but only when the distance between them is longer than the pulse width of the OTDR. Otherwise, two or more events are displayed as one, and the OTDR indicates a sum of their losses. Detailed descriptions of OTDR and its use can be found in the book [45].

The monitoring system performs periodic measurements of the monitored fiber, e.g., every 10 min with the same settings of the OTDR, including wavelength, pulse width, acquisition time, max. distance, n_{eff}, and helix factor (HF) [45]. Fiber traces are saved on the server of the monitoring systems and compared with a reference trace acquired for the link in good condition. If at any point the level difference between current and reference traces exceeds a set threshold, e.g., 1 dB, the distance to the beginning of the affected zone is measured and an alarm raised (Figure 7). To avoid false alarms, repair or modification of the fiber link requires acquisition of a new reference. Systems of this kind are primarily intended for automatic detection and location of cable cuts, constituting $\approx$ 85% of all fiber faults. To reduce costs, the system monitors multiple fiber cables, making measurements of one "dark" fiber in each cable with a remotely controlled OTDR test head (OTDR module without display and keyboard) and a fiber optic switch connecting each fiber under test to

the OTDR port. This arrangement is unsuitable for detection of tapping, as the attackers tap only live fibers carrying traffic.

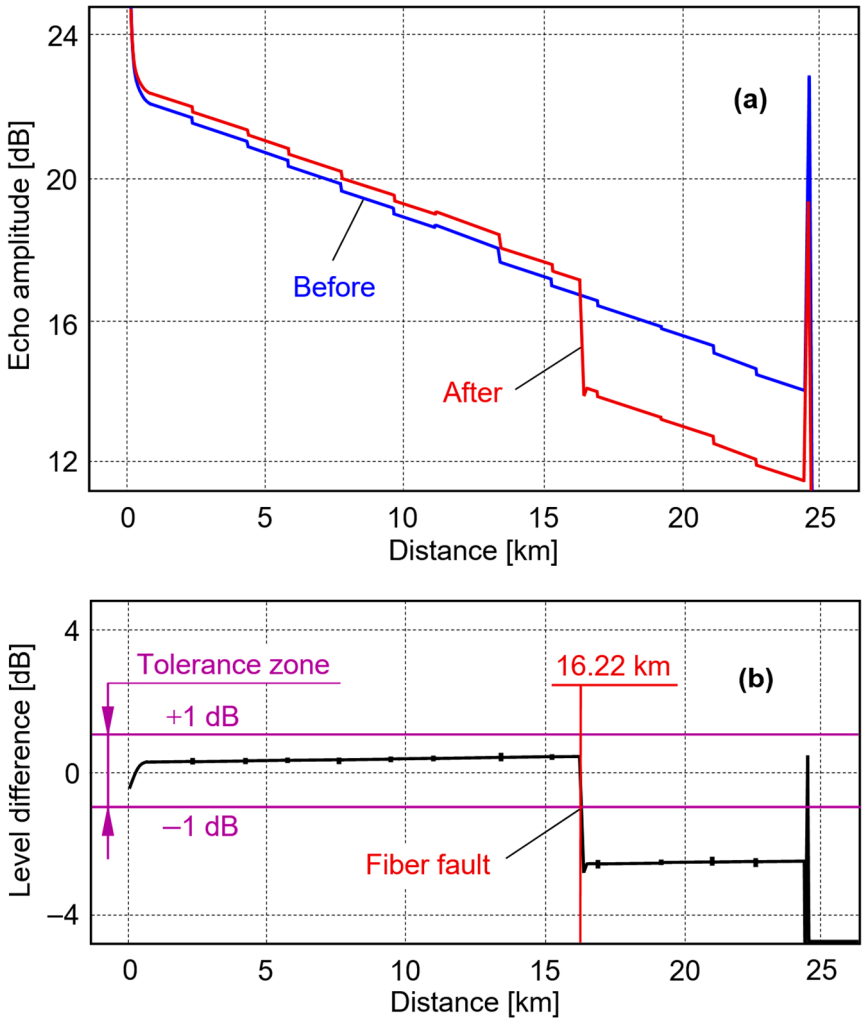


Figure 7. (**a**) Simulated OTDR traces of a single-mode fiber line before (blue) and after (red) localized damage introducing loss of 3 dB, e.g., fiber bend. (**b**) The difference between them and the tolerance band of ±1 dB; an alarm is raised when this limit is exceeded. The graph also shows variations between current and reference measurements caused by temperature, cable aging, unstable coupling of OTDR to fiber, etc. The tolerance zone is adjustable, depending on the amplitude of such variations expected or experienced in a particular fiber link. A too-narrow tolerance band results in frequent false alarms. Advanced systems perform additional trace processing, like sectional fitting to the reference trace to minimize variations observed in the first (pre-anomaly) part of the trace, e.g., to compensate for variable loss of fiber switch or power of OTDR laser. Reduction in tolerance zone to ±0.2 dB for monitoring medium-length (15–40 km) links with underground cables may be possible. Larger tolerance zone like ±1–2 dB is adequate for detection of cable cuts, particularly in aerial networks subjected to vibrations, ice loads, and large temperature swings, without false alarms.

OTDR can detect and locate fiber taps, seen as localized loss (step) on fiber trace, possibly accompanied by a reflection produced in the coupler. Depending on location and reflectance, a fiber tap can be indicated as:

(a) Increased loss of existing splice or connector—when the tap is close to it;
(b) Localized loss without reflectance—as for a fusion splice;
(c) Localized loss with reflectance (magnitude varies)—as for connector.

A typical OTDR is able to detect loss (or change in it) of ≈0.10 dB; lower loss is frequently masked by noisy appearance of fiber trace resulting from combined longitudinal non-uniformity of fiber and receiver electronic noise; the latter rises with length and attenuation of fiber between OTDR port and event. Additionally, loss of splice or connector is to some extent affected by temperature, vibration, or aging.

Data in Table 1 indicate that detection of a tap having a small 1–99% or 2–98% split ratio (tap ratio) is difficult when the splicing to the attacked fiber is done well, and total loss introduced into the line is ≈0.2 dB.

To monitor a live fiber, an arrangement similar to one shown in Figure 8 is implemented. OTDR operates at wavelength longer than the monitored link: 1530–1570 nm or 1625–1675 nm (OTDR), and 1260–1360 nm (link). OTDR and link transceiver access the fiber via Wavelength Division Multiplexing (WDM) couplers (multiplexers) installed at both ends of the link. Two of them increase link loss by 2–2.5 dB; the link power budget must be verified, and the launched power in the tapping-resistant link with minimized budget loss (Section 3.2) adjusted again.

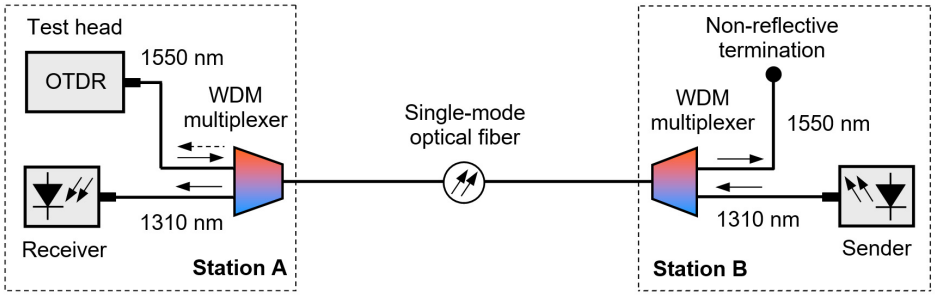


Figure 8. Basic hardware arrangement for monitoring live fiber with OTDR. Arrows indicate direction of light propagation.

Simultaneous propagation of pulses from the OTDR and the link transmitter in the same single-mode fiber having a small core effective area A_{eff} = 50–130 μm^2 results in their intermodulation at high power density, particularly due to Stimulated Raman Scattering (SRS) in fused silica [46,47]. Intermodulation in a fiber made of fused silica is strongest when the wavelength at which OTDR operates, recommended to be a long one, e.g., 1625 nm, in order to improve detection of fiber bends, is 70–120 nm longer than the wavelength at which the link transmitter operates, e.g., 1550 nm, and weak when it operates at 1310 nm. For co-propagating signals, several detrimental phenomena are observed:

- Attenuation of the link's signal synchronous with the launching of OTDR pulses;
- Amplification of OTDR pulses along the fiber and decrease in indicated loss;
- Increase in noise in OTDR traces, and difficult measurements of small loss.

Counter-propagation of pulses emitted by the OTDR and the link's transmitter (sender) shown in Figure 8 considerably reduces amplitude modulation and distortions of fiber traces, because maximum power of link's signal, corresponding to strongest intermodulation effects, takes place at the opposite end of link with respect to location of OTDR test head. This allows monitoring of live fiber or plurality of them, if an optical switch is added. Fiber tap of suitably large loss, see Table 1, can be detected as added loss at certain distance from OTDR. Monitoring of live fiber carrying signal in the other direction is possible, too, if the link loss is less than half of the OTDR dynamic range. To do so, the OTDR in Station A shall be connected to a dark fiber, and this fiber connected to the OTDR port of the WDM coupler at the other end of the link in Station B. Note: distances indicated will be different and need re-calculation.

Considering results of analysis in Sections 2.2 and 2.3, the most likely locations of taps are near transmit ends of each of (usually) two fibers of the link. Installation of taps near existing splices or connectors is to be expected. By doing so, the attacker:

- Has easy access to fibers extracted from cables, e.g., in ODF;
- Avoids adding new events in fiber but only changes their loss and reflectivity.

4.3. Power Monitoring

The power of the signal at the receive end of the fiber is periodically measured, either with an optical power meter and coupler installed before the input of the optical receiver of the link (monitoring tap) and linked to the server of the monitoring system, or with the link's receiver, reporting measured values to the network management system. Unfortunately, accuracy and range of the latter measurements are considerably inferior [21].

Main advantages of this method are:

- Almost continuous loss monitoring, e.g., every 1 s, and ability to detect and log even very short breaks in optical continuity, unlike with OTDR (4.2);
- Low cost, especially when transceivers have this function built-in;
- Large dynamic range—link of every practical length can be monitored;
- Little or no change to fiber loss.

Disadvantages include:

- No location of added loss;
- No ability to monitor reflectance;
- Need for software for importing and processing data from the management system.

4.4. State of Polarization Monitoring

This is a relatively new fiber monitoring technique. Instead of power, as in (4.3), or fiber loss, as in (4.2), the State of Polarization (SOP) of the signal at the receive end is measured with a dedicated polarization analyzer (polarimeter) at short intervals, typically $\leq$1 ms. To monitor a working link, the polarimeter must be fitted with a monitoring tap Results of measurements are logged, processed, and subjected to classification of detected anomalies [22]. Measurements are made at one (receive) end of the protected fiber link. The idea of such monitoring for detection of fiber manipulation necessary to install a tap was first described in a U.S. patent application published in 2006 [48].

The transmitter launches a signal of relatively stable polarization state into the fiber, but SOP at the receive end is affected by mechanical disturbances acting on the fiber: twisting, bending, vibration, expansion or contraction of cable elements with temperature, pressure against shaped surfaces, e.g., when the fiber is touched or gripped during work on the cable or movement of patchcords inside an optical distribution frame. Actions on optical fiber that considerably change SOP often do not cause a detectable change in attenuation. One example is disconnection of a fiber patchcord from an adapter, and its re-connection after this patchcord was inadvertently rotated by 360 degrees (one turn). The author's experience with testing of fiber patchcords shows that change in loss will typically be $\leq$ 0.05 dB, too small for reliable detection with OTDR (4.2). However, a rotation of the polarization plane by $\approx$7% of the twist applied to single-mode fiber ($\approx$25°) will be produced by the elasto-optic effect in fused silica [49,50].

The SOP is fully described with a 4-element Stokes vector, measured with commercial polarimeters [22], which are available as compact modules having no display, keyboard, etc. Modules for inline SOP monitoring have a tap coupler built in, with typical insertion loss in the order of 1 dB [51,52]. Low-cost devices do not include a tap and have analog outputs of voltages proportional to the power of each polarization component [53].

Manufacturers usually offer matched motherboards providing amplification, digitization and data interface, e.g., of Ethernet type [52,53]. Maximum sampling frequencies are between 4 kHz [51] and 50 kHz [52,53]. Operating wavelengths vary: one supplier claims a 450–2500 nm range [53], potentially useful for monitoring hollow-core fibers; another only 1550 nm and 1310 nm [52], with a bandwidth of nstrument limited to ±30–50 nm with respect to the central wavelength. Instrument [51] features a 1260–1650 nm band and better accuracy, with a desktop version available.

To reduce complexity and cost of monitoring equipment, full SOP analysis is frequently reduced to extraction of light at two orthogonal polarizations with a polarization beamsplitter and two power detectors; the ratio of their outputs is analyzed [22,23]. Besides simplicity, the latter technique enables monitoring of SOP variations at higher frequencies, with sampling rates up to 192 kHz reported [22]; ordinary sound cards for PCs are suitable for this role.

Unlike OTDR and power monitoring systems, SOP-based monitoring systems must ignore the slow evolution of SOP caused by varying environmental conditions like daily temperature fluctuations or vibrations produced by ordinary activities near fiber cables: car traffic, people walking, working fans, refrigerators, air conditioners, etc. For this, the system is sensitive only to the AC components of SOP changes in a certain frequency band.

The main advantage of SOP monitoring is high sensitivity and the ability to detect a minuscule bending or shaking of fibers, even inside an intact cable or closed container when touched, moved or bent, or when the vibrations are transferred from adjacent locations, e.g., when someone opens the doors to the communications room or walks around [21,23]. This usually happens before any measurable increase in fiber loss takes place. Demodulated polarization changes, predominantly in the audio frequency range up to ≈10 kHz [22] can be analyzed for signatures of known activities [21,22] and filtered to remove narrowband interference, e.g., from motors and machinery producing vibrations at fixed frequencies. It helps that the strongest components of SOP variations during handling of fibers and opening ODFs, joint closures, doors, etc., are located below ≈50 Hz [23].

Similar techniques have been successfully developed for detection of submarines, perimeter protection of important facilities, detection of distant earthquakes, etc. In the last two cases, ordinary land and submarine fiber optic cables serve as sensing elements.

Transmission fiber becomes a type of distributed acoustic sensor (DAS), sensitive to disturbances along the full length of the fiber, but without location functionality. Machine learning was successfully used for analysis of demodulated SOP [23,25–27].

SOP monitoring has two major disadvantages:

- Location of tampering is impossible;
- Interference from polarization variations caused by vibrations of cables and components, especially joint closures holding splices and coiled lengths of fibers.

Suitability of this technique for protection of aerial cables subject to vibrations induced by wind (with frequency proportional to wind velocity) or cables laid on bridges and viaducts with heavy traffic or near railways is rather unlikely. In such conditions, fusion splices and connectors with core offset or lengths of fibers coiled in splice cassettes act as "polarization hinges", changing SOP in the length of fiber after them in response to small mechanical disturbances [54]. Reported experiments were so far limited to cables up to 2 km long installed in a campus environment [22].

The other limitation of SOP monitoring is applicability to single-mode fibers only.

4.5. Conclusions and Warnings

The fundamental limitation of the methods presented in Sections 4.2 and 4.3 is that they detect only changes in a given optical parameter of the fiber path after the acquisition

of reference data was made. If the tap existed before, the related loss (IL_{CL}) will be recorded in the reference data and no alarm will be generated. One conclusion is that fiber taps are best installed during construction of a fiber link for carrying secret data. SOP monitoring (Section 4.4) is limited to momentary variations in this parameter, but comparisons to signatures of past events can reveal and date abnormal changes in link behavior.

The same applies to trespass detection and camera systems: they cannot detect tampering done before their activation. This leaves:

(1) Inspections of facilities for unexpected components, equipment and evidence of unplanned work on cables, ODFs, or transmission equipment (Section 4.1);
(2) Manual analysis of OTDR traces for lossy and reflective events in places other than line terminals and splice locations recorded in link documentation;
(3) Analysis of "loss of signal" or "errors" alarms generated by receivers in the link, and their temporal correlation with data from OTDR or SOP monitoring.

The labor-intensive task (2) can be automated by employing an Artificial Intelligence (AI) system, as symptoms of tapping in OTDR traces are simple. One question: who controls the AI working on protection of your secret communications network?

5. Tapping of Multi-Core and Hollow-Core Fibers

5.1. The Fibers

Two new classes of optical fibers introduced commercially in 2021–2023 after long periods of experiments are totally different in design and properties. Therefore, their tapping will be reviewed separately. This subject has not yet been analyzed in the literature known to the authors. Those new fibers are:

- Multi-Core Fiber (MCF): fiber made of solid fused silica with several single-mode, few-mode or multimode cores: 2 or 4 in fibers currently manufactured, up to 31 in experimental fibers. Commercially available MCFs with 2 and 4 cores have a standard 125 µm cladding diameter and single-mode cores similar to those found in conventional single-mode fibers conforming to ITU-T recommendation G.657A1/A2 [35] ("bending tolerant" and "bending insensitive")—for terrestrial networks, or G.654 [34]—for transoceanic submarine networks. To reduce crosstalk between single-mode cores in long-distance systems, a 40–55 µm spacing between cores surrounded by a moat (layer of low-index glass) is required for "uncoupled" fibers, and transmission in opposite directions over adjacent cores is preferred [55,56]. Except for crosstalk and splicing, other properties of "uncoupled" MCFs are essentially identical to conventional single-mode fibers with a single core. A Multi-Source Agreement (MSA) for 4-core MCFs operating at 1310 nm and intended for data center cabling was recently issued [57].
- Hollow-Core Fiber (HCF): fiber with a single empty core in the center, surrounded by an anti-resonant structure made of 4–8 nested, thin-walled (0.4–1.2 µm) tubes blocking escape of light from the core by means of optical antiresonance in tube walls called "membranes". This structure, blocking escape of light, is surrounded by a thick-walled tube constituting fiber jacket, providing mechanical strength and hermeticity, but having no optical function. The gas inside has low pressure, ≈20% of the atmospheric pressure. All glass parts of HCFs are made of undoped fused silica (SiO_2). Most HCFs have a large core diameter: 28–40 µm and cladding: ≈200 µm.

  Cross-sections of typical MCFs and HCFs are shown in Figures 9 and 10, respectively.

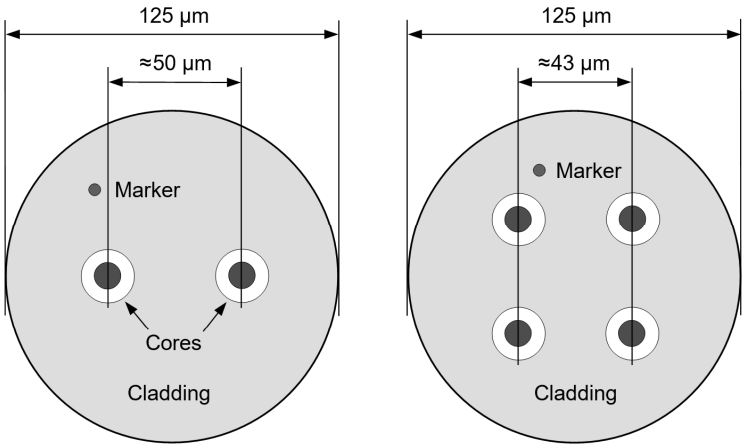


Figure 9. Cross-sections of single-mode multi-core fibers: 2-core (**left**) and 4-core (**right**). Protective coating not shown—its typical diameter is 190 or 245 µm. Marker locations may be different. Parts with higher refractive index are shown darker.

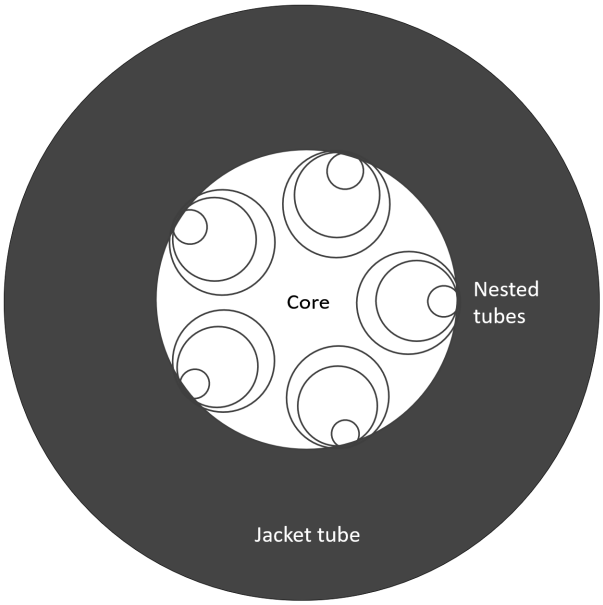


Figure 10. Cross-section of a hollow-core fiber with 5 doubly nested tubes. Jacket diameter is ca. 200 µm. Protective coating not shown. Glass is rendered dark and air white.

MCFs with 6, 7, and more cores were developed, but despite extensive research, are not produced in quantity. Numerous types of HCFs exist, differentiated mostly by:

- Number of tubes ("capillaries") forming a photonic barrier around an empty core (4–8);
- Nesting of these tubes or addition of extra parts.

Several earlier designs of HCFs are currently obsolete and abandoned, mostly because of high attenuation and complicated manufacturing. See review papers [58,59] for more information on HCFs and their technical evolution.

5.2. Tapping of Multi-Core Fibers

Which methods described in Section 2.3 and shown in Figure 3 can be effective?

Splicing or insertion of a coupler (Figure 3a–c) will work with MCF, provided the attacker identifies the core(s) to be tapped, which is not a problem when the fiber is cut or disconnected. The most versatile way is installation of couplers for all cores and directions of transmission, but such components are costly and bulky, unless advanced assembly and packaging techniques are applied.

Bending (d) will cause leakage of radiation from all cores, as their bending radii are almost identical, but the angle at which light escapes from the fiber depends on the direction of transmission. In the case of a 2-core MCF with counter-directional transmission, light incoming from opposite directions can be separated by a narrow-angle coupling system collecting light for a tap fiber or photodiode. An increase in tap loss (IL_{CT}) can be expected, and a correct setup will require some experimentation and monitoring of tapped power. When MCF carries two or more signals of the same wavelength in the same direction, tapping any of them may be impossible due to interference at the receiver.

Evanescent coupling (e) shall work and can be made faster than for SMF due to thinner cladding over MCF cores (Figure 9) and shorter polishing time. Some difficulty will be with identification of the core to be tapped, requiring observation of one fiber side under a microscope with light directed from the opposite side.

Collection of scattered light (f) is useless because the reflective enclosure mixes radiation escaping from all cores, unless wavelengths are different and bandpass filters can separate them.

V-groove (g) and **FBG** (h) methods allow selective tapping of any single core from a 2-core or 4-core MCF when the fiber is incised (g) or irradiated with a UV laser and phase mask (h) at the proper angle. Tapping may be impossible when the fiber has cores arranged in two or more layers, and the core of interest is located deep, e.g., the central one in a 7-core MCF. However, both methods are unattractive for reasons presented in Section 2.3.

5.3. Tapping of Hollow-Core Fibers

Here we review the effectiveness of different tapping methods as in Section 5.2. Results are different.

Splicing or insertion of a coupler (a–c) works with HCF, but additional fusion splices or connectors, especially with HCF–SMF transition, introduce higher loss than their SMF–SMF equivalents, and the tap is easier to detect. Entry of air at atmospheric pressure during fusion splicing results in a characteristic local rise in backscattering seen with OTDR.

However, the majority of HCF links include HCF–SMF transition joints at both ends to allow connections to transceivers with ordinary SMF pigtails. The attacker may tap them more easily than HCF.

Bending (d) looks promising. Hollow core fibers can carry large optical powers, at least in the 1–10 W (+30. . .+40 dBm) range, with negligible optical nonlinearities. Consequences for tapping depend on link power budget—see Section 2.2 and Formulas (9)–(11).

Reliable tapping of a link designed for medium bit rate, large transmit power, large loss budget and long reach, e.g., 100 Gb/s, +33 dBm (2 W), 50 dB, and 500 km, respectively, will be possible at TR = 0.003% (IL_{CT} = −45 dB, 5 dB tap margin), if the tap is made near the transmitter (Figure 2b). Theoretical loss introduced by tapping 0.003% of power from the fiber is only 0.00013 dB, making detection of the tap with OTDR or power monitoring impossible, even when tap optical efficiency OE is only 1–5%.

The situation is different when the attacked link is designed for medium reach and very high data capacity, e.g., in a core DWDM network. For 200 channels of 800 Gb/s rate each, −23 dBm receiver sensitivity, 30 dB loss budget, +33 dBm transmit power, and 5 dB tap margin, the eavesdropper must tap at least +3 dBm (2 mW). While the net tap ratio is still low TR = 0.1%, it rises to 2% for OE = 5% (−13 dB).

Installation of bending taps will be complicated by the use of multiple non-standardized types of HCFs [58] exhibiting:

- Variable sensitivity to macrobending, including irregular characteristics of bend loss (and power escaping light) vs. radius for small bend radii [60];

- Dependence of bending loss on the angle between bending plane and axis of nearest tube (capillary) [61];
- Different spectral characteristics of bending loss, including situations when loss falls considerably with wavelength, unlike solid-core single-mode fibers, where only limited oscillations are observed in the loss spectrum [62] (Annex D).

The situation will be complicated further after introduction of HCF designs including non-circular parts in the photonic barrier, currently subject to computer simulations [63].

If the type and characteristics of tapped HCF are not known beforehand, the bending radius shall be adjustable in a wide range, e.g., 40–150 mm, to match the characteristics of particular HCF at the transmission wavelength. Careful monitoring of tapped power with an optical power meter will be required during tuning of such a tap. Additionally, a limited rotation of the fiber is desirable to maximize tap ratio at a given bend radius.

Evanescent coupling (e) must be rejected because, to tap enough power, the whole thickness of the glass jacket must be removed, and then some 30–50% of the nested tube(s). The tubes are empty, so polishing slurry or powder, and humidity will enter the core, producing large, localized loss and reflection; tampering will be quickly detected.

Collection of scattered light (f) fails with straight HCF due to very weak scattering. However, it may work if the HCF inside the reflective enclosure is bent without introduction of detectable loss—being a variant of bending (d) with different hardware.

V-groove method (g) must be rejected, because cutting through the jacket and partly the tubes (Figure 10) causes entry of air, humidity, dust, etc., as in method (e).

FBG method (h) may be feasible when Bragg grating is formed in the membrane of the largest tube facing the core and exposed to relatively high density of optical power. One difficulty is distortion of the projected pattern of UV radiation by several membranes closer to the jacket tube and the uneven inner surface of the jacket tube fused with them (Figure 10).

6. Discussion

Published literature provides a technical basis for assessing tapping mechanisms, optical power constraints, and monitoring techniques, but openly documented cases of operational fiber tapping remain scarce. While no documented cases of fiber tapping were reported in the last 20 years, indirect evidence, such as very costly preparations for tapping submarine cables [29,30], proves this happens in secrecy. Consequently, we have analyzed possible methods of fiber tapping and protections against such attacks, based on very limited literature (except for optical fibers and fiber monitoring) and our own technical experience.

Review of tapping mechanisms considered in this review shows that no single technique is universally preferable. Coupler-based methods provide high, predictable optical coupling efficiency and can introduce relatively small additional loss at low tap ratios but require interrupting of transmission path during installation. Bending-based coupling avoids cutting the fiber and has therefore attracted considerable attention in the literature [15–18,38], but its practical performance depends strongly on fiber type, bend radius, wavelength, and coupling efficiency; commercially available clip-on couplers introduce large losses. Evanescent coupling can potentially provide more controlled extraction of radiation from fiber, but tap preparation is time-consuming. Collection of scattered light has the advantage of introducing no additional loss, but the tapped power is ver low. V-groove and FBG-based approaches appear substantially less attractive for field use because of their complexity and required precision. Thus, practical relevance depends not simply on whether optical coupling is physically possible, but on the combined requirements of sufficient tapped power, low introduced loss, physical accessibility, and installation complexity.

The reviewed evidence also does not support treating bending-insensitive fibers conforming to ITU-T G.657 Recommendation [36] as particularly resistant to tapping. Indeed, published comparisons indicate that tapping of G.657 fibers is feasible and, under some conditions, can exhibit favorable coupling characteristics [38,39]. Generally, all conventional single-mode and multimode fibers can be tapped using the same methods with minor adjustments.

Large-scale adoption of hollow-core fibers, together with further development of polarization-based fiber monitoring systems, may substantially affect the feasibility and detectability of established fiber-tapping techniques. The different light-guiding structure of HCFs is expected to make some methods developed for conventional SMFs less effective or impossible, although few methods, particularly bending-based, remain applicable. If novel, more effective tapping methods are developed, they are likely to remain classified and absent from the open literature for a long time.

Another takeaway from this review is that different tapping prevention and detection measures should be considered complementary rather than individually sufficient. Physical protection can reduce the likelihood of unauthorized access to the fiber infrastructure, while appropriate link design can reduce the optical power available for covert extraction or increase the loss introduced by a tap. Monitoring techniques add another layer of protection by detecting changes in optical loss, reflectance, received power, or polarization state, while encryption limits the consequences of successful physical interception. Because these measures address different aspects of the threat, using them together provides a more robust protection strategy than relying on any single countermeasure.

Quantum key distribution (QKD) is outside the scope of this review, which focuses on physical tapping and protection of conventional fiber-optic transmission. Nevertheless, QKD is relevant to the broader problem of fiber network security, since practical QKD networks still require protection of their physical nodes and optical links, particularly against jamming. The interaction between QKD, physical-layer monitoring, and fiber-tapping countermeasures therefore represents a direction for further research, particularly on optical infrastructures carrying both quantum and conventional communication channels.

Our analysis also indicates that the feasibility of fiber tapping is strongly influenced by prior knowledge of several parameters of the targeted link, including:

- Complete cable route and the facilities through which it passes;
- Identification of the fiber(s) in use, e.g., 2 out of 240 in a cable and/or ODF;
- Operating wavelength(s);
- Type of fiber used (standard, bending-tolerant, bending-insensitive, etc.);
- Power and loss budget of the link; and
- Transmission standard and bit rate.

From a defense perspective, telecom operators, corporations, or government institutions preparing fiber networks for the transmission of classified data should therefore restrict access to such information, including access by their own personnel who may be bribed. Controlled dissemination of well-fabricated false network data, rather than reliance solely on traditional secrecy, may also be considered as an additional proactive measure. Installing OTDR- or SOP-based systems to monitor live fibers is likewise recommended. While the latter are not yet commercially available, such systems can be built relatively cheaply in accordance with descriptions in the literature [21–23,25,26], using dedicated polarimeter modules [51–53]. However, readers must be warned that a Machine Learning (ML) model satisfactorily monitoring one type of fiber network for tampering can fail when applied to another kind of fiber, type of cable, and method of its installation (aerial/duct/indoor), etc. A possible solution was proposed in paper [64].

Several gaps in research were found during this review. First, experimental comparisons of tapping mechanisms under typical conditions remain limited, particularly with respect to introduced loss, coupling efficiency, or disturbance during installation. Second, the practical performance of SOP-based monitoring requires further evaluation with longer links and in mechanically noisy environments. Third, direct experimental studies of tapping and intrusion detection in MCF and HCF links are needed to distinguish feasible mechanisms from those inferred only from fiber geometry and optical principles. Finally, integrated evaluations of security, reliability, and operational cost are needed, since measures that improve resistance to tapping, such as reducing the optical power margin or increasing monitoring sensitivity, may reduce operational robustness or increase the rate of false alarms. These issues represent a more immediate research need than speculation about undisclosed tapping techniques, for which no verifiable technical evidence is currently available.

7. Conclusions

Since the late 1990s, the development of fiber-tapping techniques has outpaced conventional protective measures like OTDR and optical power monitoring systems. Development and deployment of SOP-based fiber monitoring may represent an important advance in this respect because of its high sensitivity and ability to detect and identify mechanical disturbances to cables, fibers, and components in the monitored fiber link, even when fiber continuity and loss remain unchanged. However, this advantage may be substantially reduced in mechanically noisy environments characterized by vibrations, wind, temperature swings, etc., where environmental disturbances can lead to a high rate of false alarms.

Tapping techniques other than those reviewed in this paper may exist, particularly for use against high-value targets, but their operational use is difficult to assess because such information is rarely publicly available. As optical fibers, including newly introduced HCF and MCF, continue to replace legacy twisted pair and coaxial cables, along with most microwave links, the security of fiber infrastructure and particularly the development of effective tapping detection and mitigation techniques are likely to remain important research and operational subjects.

8. Materials and Methods

This paper is a review type, based on data already published between 1998 and 2026. Data gathering was stopped on 7 October 2026. Data collected during work on this paper include the following:

1. Scientific and technical publications, standards and product data sheets;
2. Copies of media reports and websites covering subjects of this review;
3. Patents and patent applications.

Generative artificial intelligence (GenAI) was not used for the literature search, collection of source materials, technical analysis, interpretation of the reviewed evidence, or preparation of the original manuscript. GenAI was used only for language and stylistic editing of selected parts of Sections 1, 6 and 7 during manuscript revision. The authors reviewed and approved all AI-assisted changes and take full responsibility for the final content.

Author Contributions: Conceptualization, K.B.; methodology, K.B. and M.K.; investigation, K.B.; data curation, K.B.; writing—original draft preparation, K.B.; writing—review and editing, M.K.; visualization, K.B.; funding acquisition, M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Polish Ministry of Science and Higher Education through funding for the statutory activities of the National Institute of Telecommunications (no specific contract number). The work of Krzysztof Borzycki was carried out within Project No. 12.30.002.6 "Design of photonic structures, including diffractive optical components for fiber optic communications and measurements". The work of Mirosław Klinkowski was supported by the National Science Centre, Poland, under Grant No. 2024/53/B/ST7/02482.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Krzysztof Borzycki will maintain a full set of data gathered for the purpose of writing this paper indefinitely. Availability to third parties, however, is restricted by the fact that a large proportion of these materials is not of "open access" type. All other data are available to anyone upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

APC	Angled Physical Contact (type of single-mode fiber connector)
APD	Avalanche Photo-Diode
BDFA	Bismuth-Doped Fiber Amplifier
C band	1530–1565 nm optical band (Conventional Band)
CWDM	Coarse Wavelength Division Multiplexing (with 20 nm channel spacing)
DAS	Distributed Acoustic Sensor (made of optical fiber)
DNANF	Double-Nested Anti-Resonant Nodeless Fiber (type of HCF)
DWDM	Dense Wavelength Division Multiplexing
E Band	1360–1460 nm optical band (Extended Wavelength Band)
EDFA	Erbium–Doped Fiber Amplifier
EMI	Electro-Magnetic Interference
FBG	Fiber Bragg Grating
HCF	Hollow Core Fiber
ITU-T	International Telecommunication Union–Technical Standardization Sector
LAN	Local Area Network
L Band	1565–1625 nm optical band (Longwave Band)
MCF	Multi-Core Fiber
ML	Machine Learning
MMF	Multimode Fiber (with solid core)
MSA	Multi-Source Agreement
NF	Noise Figure (of amplifier)
NSA	National Security Agency (U.S. intelligence agency)
OADM	Optical Add-Drop Multiplexer
O Band	1260–1360 nm optical band (Old Band—the first one used with SMF)
ODF	Optical Distribution Frame
OTDR	Optical Time Domain Reflectometer
QKD	Quantum Key Distribution
RFI	Radio Frequency Interference
S Band	1460–1530 nm optical band (Shortwave Band)
SIGINT	SIGnal INTelligence
SMF	Single Mode Fiber (with solid core)
SOP	State Of Polarization
SRS	Stimulated Raman Scattering

TDFA	Thulium–Doped Fiber Amplifier
U Band	1625–1675 nm optical band (Ultralong Wavelength Band)
UV	Ultraviolet (radiation; 10–380 nm wavelength range)
WDM	Wavelength Division Multiplexing

References

1. Fujiwara, M.; Miki, S.; Yamashita, T.; Wang, Z.; Sasaki, M. Photon level crosstalk between parallel fibers installed in urban area. *Opt. Express* **2010**, *18*, 22199–22207. [CrossRef] [PubMed]
2. Fibrain Asymmetric Integrated Splitters (FAIS). Fibrain. 27 February 2023. Available online: https://fibrain.com/product/asymmetric-integrated-splitters/ (accessed on 4 July 2026).
3. Optical Elements—PON: CPL FBT (Fused Biconical Tapering) Splitters/Couplers. Fibrain. 2021. Available online: https://fibrain.com/product/fbt-splitters-couplers-in-abs-pipe-housing/ (accessed on 4 July 2026).
4. *IEEE Std. 802.3-2022*; IEEE Standard for Ethernet. IEEE Computer Society: New York, NY, USA, 2022. [CrossRef]
5. InfiniStreamNG Hardware Appliance: Smart Visibility for Network and Application Performance Management and Cybersecurity (Data Sheet). Netscout Systems. 10 December 2025. Available online: https://www.netscout.com/resources/datasheets/infinistreamng-hardware-appliance (accessed on 19 March 2026).
6. Borzycki, K. Recent Progress in Development of Hollow-Core Fibers for Telecommunications and Data Transmission Applications. *Photonics* **2026**, *13*, 494. [CrossRef]
7. Médard, M.; Marquis, D.; Chinn, S.R. Attack Detection Methods for All-Optical Networks. In Proceedings of the 5th Networks and Distributed System Security (NDSS) Symposium 1998, Carlsbad, CA, USA, 12 March 1998. Available online: https://www.ndss-symposium.org/wp-content/uploads/2017/09/Attack-Detection-Methods-for-All-Optical-Networks.pdf (accessed on 10 July 2026).
8. Shaneman, K.; Gray, S. Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for Detection and Prevention. In Proceedings of the 2004 IEEE Military Communications Conference (MILCOM 2004), Monterey, CA, USA, 31 October–3 November 2004. [CrossRef]
9. Miller, S.K. Hacking at the Speed of Light. *Security Solutions Magazine*, 1 April 2006.
10. Iqbal, M.Z.; Fathallah, H.; Belhadj, N. Optical Fiber Tapping: Methods and Precautions. In Proceedings of the 8th International Conference on High-Capacity Optical Networks and Emerging Technologies (HONET 2011), Riyadh, Saudi Arabia, 19–21 December 2011; pp. 164–168. [CrossRef]
11. Palmer, J.P.; General Dynamics. Method of Fabrication of Fiber Optic Coupler. U.S. Patent 4,431,260, 14 February 1984.
12. Walter, H.; Deutsche Telekom AG. Method and Device for Extracting Signals out of a Glass Fiber. U.S. Patent 6,265,710, 24 July 2001.
13. Pi, B.; Zhao, S.; Chen, Z.; Morse, R.; Li, J.; Oluma Inc. Fiber Tap Monitor Based on Evanescent Coupling. U.S. Patent 6,744,948, 1 June 2004.
14. Salim, A.; Carroll, S.S.; Atai, J. Limits of intrusion detection systems in a gigabit optical link. *Opt. Eng.* **2010**, *49*, 045005. [CrossRef]
15. Clip-On Coupler FOD5516. LIFODAS, UAB. 7 March 2023. Available online: https://lifodas.lt/images/Products/Accessories/ds_5516.pdf (accessed on 27 June 2026).
16. *PFC 1000 Passive Fiber Clip-on Coupler (Data Sheet)*; Go4Fiber: Hong-Kong, China; Shenzhen, China; Shanghai, China; Beijing, China, 2006. Available online: https://www.go4fiber.com/passive-fiber-clip-on-coupler (accessed on 11 March 2026).
17. Optical Clip-On Coupler OPT130. Kingfisher International. 13 September 2016. Available online: https://gigatest.bg/html/upload/files/OPT130.pdf (accessed on 27 June 2026).
18. Uematsu, T.; Hirota, H.; Kawano, T.; Kiyokura, T.; Manabe, T. Design of a Temporary Optical Coupler Using Fiber Bending for Traffic Monitoring. *IEEE Photonics J.* **2017**, *9*, 710613. [CrossRef]
19. KI 021 Handheld Optical Talk Set Rev. 6. Kingfisher International. 21 March 2011. Available online: https://kingfisherfiber.com/media/2332/021-optical-talk-set.pdf (accessed on 27 June 2026).
20. OFI-400 Optical Fiber Identifier. AFL. 29 October 2025. Available online: https://www.aflhyperscale.com/product/ofi-400-optical-fiber-identifier/#specs (accessed on 27 June 2026).
21. Spurny, V.; Munster, P.; Tomasov, A.; Horvath, T.; Skaljo, E. Physical Layer Components Security Risks in Optical Fiber Infrastructures. *Sensors* **2022**, *22*, 588. [CrossRef] [PubMed]
22. Ruzicka, M.; Jabloncik, L.; Dejdar, P.; Tomasov, A.; Spurny, V.; Munster, P. Classification of Events Violating the Safety of Physical Layers in Fiber-Optic Network Infrastructures. *Sensors* **2022**, *22*, 9515. [CrossRef] [PubMed]
23. Tomasov, A.; Dejdar, P.; Munster, P.; Horvath, T.; Barcik, P.; Da Ros, F. Enhancing fiber security using a simple state of polarization analyzer and machine learning. *Opt. Laser Technol.* **2023**, *167*, 109668. [CrossRef]

24. Karlsson, S.; Lin, R.; Wosińska, L.; Monti, P.; Andersson, M. Detection of abnormal activities on SM or MM fiber. In Proceedings of the 2023 Optical Fiber Communications Conference and Exhibition (OFC-2023), San Diego, CA, USA, 5–9 May 2023; paper M3Z.6 (poster version). [CrossRef]
25. Tomasov, A.; Dejdar, P.; Munster, P.; Horvath, T. Utilizing a State of Polarization Change Detector and Machine Learning for Enhanced Security in Fiber-Optic Networks. In Proceedings of the Conference on Lasers and Electro-Optics (CLEO) 2024, Charlotte, NC, USA, 5–10 May 2024; paper JTu2A.217. [CrossRef]
26. Sadighi, L. Detection of Optical Network Breaches through ML-Based State of Polarization Analysis. Ph.D. Thesis, Chalmers University of Technology, Gothenburg, Sweden, 2026. Available online: https://research.chalmers.se/publication/551267/file/551267_Fulltext.pdf (accessed on 4 July 2026).
27. Song, H.; Li, Y.; Liu, M.; Wang, K.; Li, J.; Zhang, M.; Zhao, Y.; Zhang, J. Experimental study of machine-learning-based detection and location of eavesdropping in end-to-end optical fiber communications. *Opt. Fiber Technol.* **2022**, *68*, 1026692021. [CrossRef]
28. CNSSI No. 7003: Protected Distribution Systems (PDS). National Security Agency, CNSS Secretariat (IE414). September 2015. Available online: https://www.dcsa.mil/Portals/91/documents/ctp/nao/CNSSI_7003_PDS_September_2015.pdf (accessed on 27 June 2026).
29. King, N., Jr. In Digital Age, U.S. Spy Agency Fights to Keep from Going Deaf. *The Wall Street Journal*. This Article Was Also Distributed with Changes Under a Title: Deep Secrets: As Technology Evolves, Spy Agency Struggles To Preserve Its Hearing. 23 May 2001. Available online: https://www.wsj.com/articles/SB990563785151302644 (accessed on 27 June 2026).
30. Balestrieri, S. The Navy SEALs Have a Submarine That Costs More Than Most Countries' Entire Navy—and Nobody Knows What It Does. *19FortyFive*. 24 March 2026. Available online: https://www.19fortyfive.com/2026/03/the-navy-seals-have-a-submarine-that-costs-more-than-most-countries-entire-navy-and-nobody-knows-what-it-does/ (accessed on 11 July 2026).
31. Ireland, O.; Copeland, T.; Gardner, F. UK says Russia ran submarine operation over cables and pipelines. *BBC News*. 9 April 2026. Available online: https://www.bbc.com/news/articles/cre13qn9z7do (accessed on 14 July 2026).
32. Engelbrecht, C. Cable Wars: From Spy Subs to Fiber-Splicing Spies. *Domino Theory*. 19 April 2023. Available online: https://dominotheory.com/cable-wars-from-spy-subs-to-fiber-splicing-spies/ (accessed on 27 February 2026).
33. Engelbrecht, C. Why We'll Soon See Underwater Combat Over Internet Cables. *Domino Theory*. 21 April 2023. Available online: https://dominotheory.com/why-well-soon-see-underwater-combat-over-internet-cables/ (accessed on 27 February 2026).
34. *ITU-T G.652 (08/2024)*; Characteristics of a Single-Mode Optical Fibre and Cable. ITU: Geneva, Switzerland, 2024. Available online: https://www.itu.int/myworkspace/t-rec/item?id=16060&lang=en (accessed on 27 June 2026).
35. *ITU-T G.654 (08/2024)*; Characteristics of a Cut-Off Shifted Single-Mode Optical Fibre and Cable. ITU: Geneva, Switzerland, 2024. Available online: https://www.itu.int/myworkspace/t-rec/item?id=16061&lang=en (accessed on 14 July 2026).
36. *ITU-T G.657 (08/2024)*; Characteristics of a Bending-Loss Insensitive Single-Mode Optical Fibre and Cable. ITU: Geneva, Switzerland, 2024. Available online: https://www.itu.int/myworkspace/t-rec/item?id=16037&lang=en (accessed on 27 June 2026).
37. MacChesney, J.B.; Stockert, T.E.; Wisk, P.W.; Yan, M.F.; Furukawa Electric North America Inc. Optical Fiber Design for Secure Tap Proof Transmission. U.S. Patent 6,801,700, 5 October 2004.
38. Karlsson, S.; Lin, R.; Wosińska, L.; Monti, P. Eavesdropping G.652 vs. G.657 fibres: A performance comparison. In Proceedings of the 2022 International Conference on Optical Network Design and Modeling (ONDM 2022), Warsaw, Poland, 16–19 May 2022. [CrossRef]
39. Bradley, T.D.; van den Hout, M.; Kalla, B.; van Vliet, V.; Bigot-Astruc, M.; Correa, A.A.; Sillard, P.; Weiner, G.; Winzer, P.; Okonkwo, C. Fiber Eavesdropping Using Tapers in Standard and Trench-Assisted Single-Mode Fibers. *IEEE Photonics Technol. Lett.* **2024**, *36*, 15. [CrossRef]
40. *IEC 60793-2-50:2025*; Optical Fibres—Part 2–50: Product Specifications—Sectional Specification for Class B Single-Mode Fibres. International Electrotechnical Commission: Geneva, Switzerland, 2025. Available online: https://webstore.iec.ch/en/publication/77555 (accessed on 23 July 2026).
41. *IEC 60793-2-10*; Optical Fibres—Part 2–10: Product Specifications-Sectional Specification for Category A1 Multimode Fibres. International Electrotechnical Commission: Geneva, Switzerland, 2025. Available online: https://webstore.iec.ch/en/publication/62020 (accessed on 23 July 2026).
42. *TIA-492AAAE*; Detail Specification for 50-um Core Diameter/125-um Cladding Diameter Class 1a Graded-Index Multimode Optical Fibers with Laser-Optimized Bandwidth Characteristics Specified for Wavelength Division Multiplexing. Telecommunications Industry Association: Arlington, VA, USA, 2016. Available online: https://store.accuristech.com/standards/tia-tia-492aaae?product_id=2592718 (accessed on 23 July 2026).
43. *Secure Locking SC Connector (Data Sheet v. 2.2)*; Optical Fiber Packaging Ltd.: Suffolk, UK, 2024. Available online: https://www.ofpgco.com/_files/ugd/2718f3_346f41e210aa4dd59c1b4e910833425e.pdf (accessed on 30 July 2026).
44. Cisco 10GBASE SFP+ Modules (Data Sheet). Cisco. 1 July 2026. Available online: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html (accessed on 31 July 2026).

45. Anderson, D.R.; Johnson, L.; Bell, F.G. *Troubleshooting Optical-Fiber Networks: Understanding and Using Your Optical Time-Domain Reflectometer*, 2nd ed.; Academic Press: San Diego, CA, USA; London, UK, 2004; pp. 1–437. ISBN 0-12-0586614.
46. Scheerer, C. OTDR pulse power limit in on-line monitoring of optical fibres owing to stimulated Raman scattering. *Electron. Lett.* **1996**, *32*, 679–680. [CrossRef]
47. Chen, H.; Leblanc, M.; Plomteux, O. *Live-Fiber OTDR Testing: Traffic and Measurement Impairments*; Technical Note 022; EXFO: Quebec, QC, Canada, 2011. Available online: https://www.exfo.com/contentassets/01fd605f57ba4b16953cf58332663a30/exfo_tnote022_otdr-testing-traffic-measurement-impairments_en.pdf (accessed on 13 August 2026).
48. Murphy, C.; Vokey, D.; Bridges, M.; Network Integrity Systems Inc. Intrusion Detection System for Use on Single Mode Optical Fiber Using a Simplified Polarimeter. U.S. Patent 2006/0153491 A1, 10 January 2012.
49. Ulrich, R.; Simon, A. Polarization optics of twisted single-mode fibers. *Appl. Opt.* **1979**, *18*, 2241–2251. [CrossRef] [PubMed]
50. Barlow, A.J.; Payne, D.N. The Stress-Optic Effect in Optical Fibers. *IEEE J. Quantum Electron.* **1983**, *QE-19*, 834–839. [CrossRef]
51. Fiber-Coupled Polarimeters POL-APx Series. APEX Technologies. 3 April 2026. Available online: https://apex-t.com/wp-content/uploads/2026/04/APEX-Datasheet-POL_v2.5.pdf (accessed on 6 October 2026).
52. High Speed In-line Polarimeter—PolaDetect (POD). General Photonics Corp. 5 August 2020. Available online: https://shop.amstechnologies.com/media/96/b7/c1/1720716910/POD-Polarimeter-General-Photonics-Datasheet.pdf (accessed on 6 October 2026).
53. Agiltron High Speed In-line Polarimeter: 450–2500 nm ± 50 nm, 50 kHz Speed, Rev 09/07/26. Optowares Corporation. 7 September 2026. Available online: https://agiltron.com/dlc/specs/High_Speed_In-line_Polarimeter.pdf (accessed on 6 October 2026).
54. Brodsky, M.; Frigo, N.J.; Boroditsky, M.; Tur, M. Polarization Mode Dispersion of Installed Fibers. *J. Light. Technol.* **2006**, *24*, 4584–4599. [CrossRef]
55. Tandon, P.; Bennett, K.; Tuggle, M.; Butler, D.; de Pedro, H.; Hebgen, P.; Sutton, C.; Matthews, H.B.; Drake, M.; Johnson, S.; et al. Record Low Loss 0.144 dB/km 2-Core Optical Fiber for Submarine Transmission. *J. Light. Technol.* **2024**, *42*, 4213–4221. [CrossRef]
56. Takahashi, M.; Maeda, K.; Aiso, K.; Mukasa, K.; Sugizaki, R.; Soma, D.; Takahashi, H.; Tsuritani, T.; Mitrovic, M.; Pálsdóttir, B.; et al. Uncoupled 4-core fibre with ultra-low loss and low inter core crosstalk. In Proceedings of the 2020 European Conference on Optical Communications (ECOC), Brussels, Belgium, 6–10 December 2020; pp. 1–4. [CrossRef]
57. SDM4 Multicore Fiber MSA Technical Specifications, Version 1.0, 17 September 2026 AFL. Corning Inc., Sumitomo Electric Industries, TeraHop. Available online: https://sumitomoelectric.com/sites/default/files/2026-09/download_documents/SDM4%20Multicore%20Fiber%20MSA%20Technical%20Specifications%20Version%201.0_1.pdf (accessed on 30 September 2026).
58. Borzycki, K.; Osuch, T. Hollow-Core Optical Fibers for Telecommunications and Data Transmission. *Appl. Sci.* **2023**, *13*, 10699. [CrossRef]
59. Komanec, M.; Dousek, D.; Suslov, D.; Zvanovec, S. Hollow-Core Optical Fibers. *Radioengineering* **2020**, *29*, 417–430. [CrossRef]
60. Gao, S.-F.; Wang, Y.-Y.; Liu, X.-L.; Ding, W.; Wang, P. Bending loss characterization in nodeless hollow-core anti-resonant fiber. *Opt. Express* **2016**, *24*, 14801–14811. [CrossRef] [PubMed]
61. Eltaieb, R.A.; Morency, S.; Messaddeq, Y.; LaRochelle, S.; Rusch, L.A. Impact of bending angle on antiresonant fibers with optimized symmetric geometries. *Opt. Fiber Technol.* **2025**, *90*, 104071. [CrossRef]
62. *IEC 60793-1-47*; Optical Fibres—Part 1–47: Measurement Methods and Test Procedures—Macrobending Loss. IEC: Geneva, Switzerland, 2017. Available online: https://webstore.iec.ch/en/publication/27706 (accessed on 30 September 2026).
63. Li, Y.; Zhang, Z.; Guo, Y.; Guo, H.; Zhang, Z. Design and numerical analysis of a gap-compensated low loss hollowcore antiresonant fiber with nested elliptical tubes. *Sci. Rep.* **2025**, *15*, 19817. [CrossRef] [PubMed]
64. Sadighi, L.; Karlsson, S.; Natalino, C.; Eshghie, M.; Usmani, F.; Kenny, E.; Wosinska, L.; Monti, P.; Furdek, M.; Ruffini, M. Variational autoencoder domain adaptation for cross-system generalization in ML-based SOP monitoring. *J. Opt. Commun. Netw.* **2026**, *18*, C149–C159. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.