Network Physical Layer Attack in the Very High Capacity Networks

David GRENAR[1], *Jakub FROLKA*[1], *Karel SLAVICEK*[2], *Otto DOSTAL*[2], *Martin KYSELAK*[3]

[1]Department of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, 612 00 Brno, Czech Republic
[2]Institute of Computer Science - IT Infrastructure Division, Masaryk University, Botanicka 554/68a, 602 00 Brno, Czech Republic
[3]Department of Electrical Engineering, Faculty of Military Technology, University of Defence, Kounicova 65, 662 10 Brno, Czech Republic

xgrena04@vutbr.cz, frolka@vutbr.cz, slavicek@ics.muni.cz, dostal@ics.muni.cz, martin.kyselak@unob.cz

DOI: 10.15598/aeee.v21i1.4973

Article history: Received Dec 15, 2022; Revised Dec 27, 2022; Accepted Jan 16, 2023; Published Mar 31, 2023.

Abstract. *This paper focuses on the analysis of fiber optic line eavesdropping options based on cheap and easy-to-use equipment - for example, the commonly used fiber optic splitters with suitable optical power division ratios. The fiber optic splitter takes a small portion of the optical power sufficient for the eavesdropper to read the data and lets as much signal power as possible pass in the original direction. We attempted to detect the presence of fiber optic splitter-based eavesdropping points on the communication line by using common techniques designated for fiber optic quality measurement and fault detection. The results are summarised in this paper.*

Keywords

Eavesdropping detection, fiber optics, very high capacity network, network traffic eavesdropping.

1. Introduction

With the constant development of new communications services that place greater demands on transmission parameters, optical networks are massively used in access networks. The security concerns are enormous - each year, companies spend billions of dollars securing their networks, and each year billions of dollars are lost due to intrusions into those same networks. At first, fiber optic networks were touted as one of the most secure infrastructure options. In the last couple of years, it has been suggested that fiber is almost as easy to tap as copper [1] and [2]. Today, there are millions of miles of fiber cable spanning the globe. Large amount of data are being transmitted across these cables daily, including sensitive government data, and personal financial, and medical information. Fiber optic communication is widely and publicly understood as a medium that is difficult to eavesdrop on. Unfortunately, this common conception is far from the technical reality. In this paper, we study some cheap and easily accessible tools for eavesdropping on fiber optic communications and explore the chances for the automatic detection of their placement on live fiber optic lines.

It is very likely that, in a couple of years, contemporary cryptography used to protect communication will be vulnerable due to the current progress in quantum computing. For the time being, communication protection relies on protecting physical lines against eavesdropping until new cryptography algorithms are developed. Research in this field is mainly focused on advanced techniques based on leading but costly technology [3]. However, the threat of cheap and easy eavesdropping is more or less unnoticed. This paper intends to illuminate this possibility.

In order to ensure communication security, it is necessary to focus on physical access to the communication infrastructure. In case of a server and delivery infrastructure, access is located in data centers that are under the constant supervision of provisioning operators.

An unimaginable amount of data, including sensitive data, are being transmitted across these cables daily. If the wiring is in a publicly-accessible space, this data may be compromised. Thus, tighter access control to the cabling must be implemented. More companies need to employ physical layer security systems in conjunction with their existing data layer security systems because physical layer security systems are better able to detect and deal with intrusions to the cables that do not involve an easily measurable amount of data interruption [4]. Also, it may be advantageous to not publish fiber optic communication infrastructures on the Internet. This can provide a roadmap and bring attention to fiber optic vulnerabilities.

Access networks are often located in public areas but are not properly secured. To gain access to data transported over the fiber, it is enough to connect an optical splitter to the transmission path. Then it is possible to eavesdrop on all traffic. In order to totally block cyber-attacks and hacking, the access network should be protected. If a company encrypts its transmitted data, it could prove to be a stumbling block for intruders. Depending on the encryption methods used, it may only be a matter of time before the intruder breaks the encryption and obtains their desired data.

Our motivation for this work is the MeDiMed infrastructure used for medicine picture data transport and processing (documented in [5], [6], [7], [8], [9], and many others). MeDiMed is a shared regional Picture Archiving and Communication System (PACS) serving hospitals in Brno and the surrounding area. The system facilitates fast and secure communication among individual hospitals, enables delivery of some services through the computer network, and offers other capabilities of today's computer systems and data networks to medical users [10]. The system deals with the secure transmission, archiving, and sharing of medical image data originating from various modalities (computed tomography, magnetic resonance, mammography, etc.). The security needs of the MeDiMed system are the motivation for this article. In this research, we have made use of the experience gained during the development and deployment of the optical backbone of the Czech NREN network CESNET [11], [12], [13] and [14].

1.1. State of the Art and Related Work

Currently, scientific papers focus mainly on sophisticated fiber optic line eavesdropping technologies. For example, in [15], advanced deep learning algorithms are discussed. In [16], the authors focus on eavesdropping and respective defense measures using fiber bending and similar technologies. In [17], the possible utilization of in-band crosstalk for optical transport line eavesdropping is discussed. In [18], the authors discuss possibilities of fiber optics bending utilization.

All of these related works utilize relatively expensive technology and complicated procedures. However, the biggest risk for currently used fiber optic networks lies in cheap and easy-to-use technologies. This paper demonstrates the eavesdropping capabilities of very simple equipment - a fiber optic power splitter. There are several related works dealing with fiber optics infrastructure security in general, [19] and [20], related technologies [21], [22] and [3], or security in DWDM backbone networks ([23] and access networks - GPON [24] and [25]. Our focus is enterprise and metropolitan networks. These networks commonly use gigabit and ten-gigabit ethernet over singlemode fiber and are more susceptible to attacks as the protection of cabinets with patch panels is not as strict as in the case of backbone transport networks, and the technology is not as tight as in the case of GPON networks.

An attacker can use any maintenance window to install fiber optic splitters into the line of interest. Another factor working for the eventual attacker is a higher frequency of changes in this type of network so that even short unannounced interrupts can pass without notice from the side of the network operator and adequate security checks. We have experimentally approved that in the case of gigabit ethernet even a splitter with a 5:95 optical power distribution can provide enough optical power for an eavesdropper, allowing him or her to capture data traffic using common network equipment without the need for optical amplification or any other advanced tool or gear.

2. Technology for Optical Networks Eavesdropping

This section discusses the key technologies and processes suitable for cost-effective optical network eavesdropping.

The main advantage of physical line eavesdropping is the long-term availability of data. Once the eavesdropping point is installed, it can provide a copy of all the data transported until it is discovered and removed. The main drawback of eavesdropping is that the attacker cannot gain access to any data they choose, but only that transported over the affected communication media. Of course, the attacker has to fully understand the communication protocol stack in use and needs enough computing power to reassemble the sensitive data from communications protocols, packets, and frames.

Gaining access to data transported over the fiber optic line is much easier than commonly believed. An essential tool is a general fiber optic splitter with the proper coupling ratio. An example of such a splitter is in Fig. 1. Equipped with the proper fiber type and casing, it is difficult to distinguish the splitter from the patchcord if placed into a fiber optic rack. This component is available in several e-shops for less than 15 USD. As mentioned before, we focus on cheap and easy-to-use eavesdropping equipment. This kind of equipment can be used in many instances and doesn't require in-depth knowledge of its users. For this reason, we consider this kind of eavesdropping risk severe compared to other, more advanced technologies.

Fig. 1: An example of a fiber optic splitter equipped with proper fiber type and casing, making it difficult to be detected in a fiber optic rack.

The same component, usually encased in a rack-mountable chassis, is commonly used by security incident response teams for network traffic analysis. The technology used by security monitoring teams to gain network traffic samples for analysis and the technology used by attackers for network traffic eavesdropping is almost the same. The main differences are the encasing and, of course, the reason for tapping the network traffic.

The following sections discuss possible ways of detecting splitters inside a fiber optic line. As discussed later, the technical capabilities for detecting splitters in fiber optic lines are limited. There is no way to distinguish the reason for the presence of a splitter. However, even for network traffic analysis performed by the network operator, the network monitoring device has access to the whole data traffic, like an illegal eavesdropper, but commonly only provides aggregate output in the form of network and flow statistics, like Netflow or IPFIX. The way of utilizing a network monitor is, to some extent, up to the conscience and choices of the network operator.

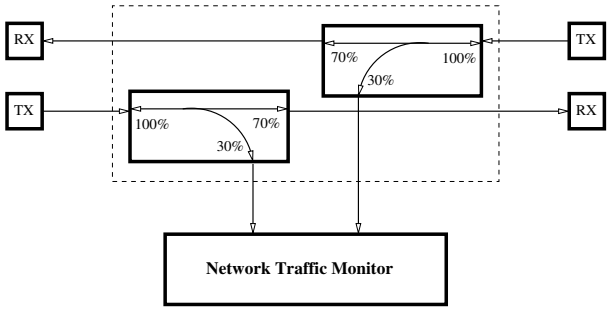

Fig. 2: An example of a typical network traffic monitoring TAP connection.

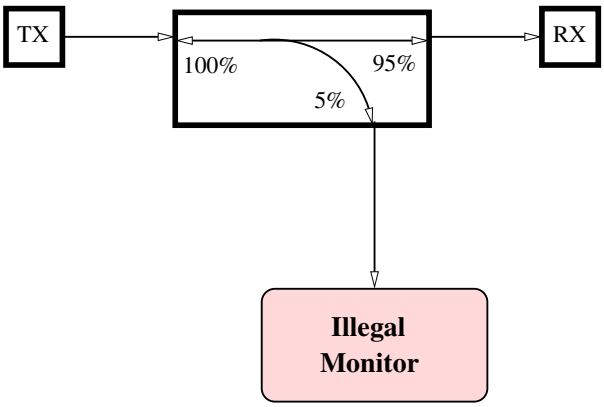

Fig. 3: Basic eavesdropping TAP connection.

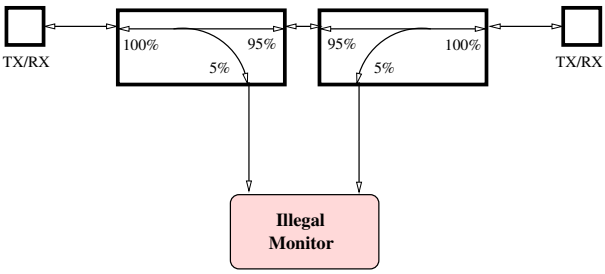

Fig. 4: Bidirectional eavesdropping TAP connection.

3. Eavesdropping Point Detection

The cost of an optical splitter is insignificant, and its installation is almost effortless. Let us consider the options for optical splitter detection

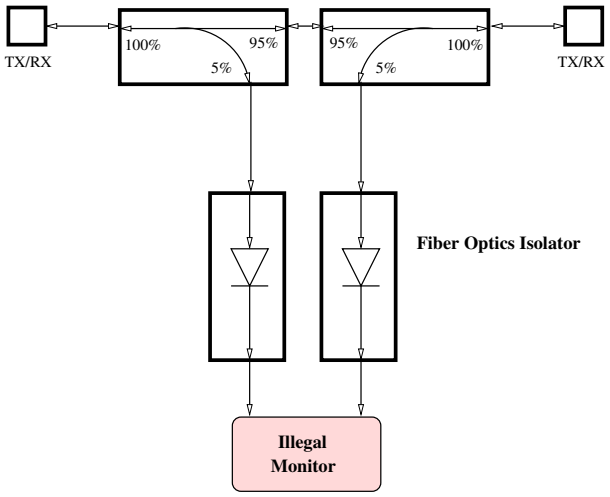

Fig. 5: Eavesdropping TAP with protection against the OTDR detector.

utilizing equipment and techniques commonly used in telecommunication network deployment and operation. The first and probably the most obvious way is optical performance monitoring. The second method is Optical Time-Domain Reflectometer (OTDR) utilization. We have set up a simple testing scenario based on a simple transmitter and receiver using the SFP module with a 1550 nm wavelength and fiber optic lines used as part of the physical network infrastructure in the computer center. We installed a fiber optic splitter inside the line instead of the patchcord. A splitter with a coupling ratio of 5:95 was used, and gigabit ethernet traffic was successfully eavesdropped on and read by the simulated bootleg device. All tests were performed on legacy ITU-T G.652 fiber optic lines and patchcords based on a G.657 fiber.

We performed a set of measurements to analyze the differences in detecting the splitter by both optical performance monitoring and OTDR measurements. The EXFO FTB-7300D-234B-EI OTDR was used for our experiments. This type of OTDR is used for the daily operation of the university's fiber optic network. We used three scenarios of splitter placements, as shown in Fig. 3, Fig. 4 and Fig. 5, where Fig. 5 is relevant only for OTDR measurements. To demonstrate the real capabilities of fiber optic eavesdropping components and the limited possibilities for their detection, we set up a lab model and performed a set of measurements. The lab model is shown in Fig. 6. The results are summarized in the following sections.

We used three local optical loops: two of them simulating communication lines on the figure denoted as lines 1–2 and 3–4, and one used as a simulation of an attacker on the figure line 5–6. A fixed attenuator of 5 dB was inserted in the middle of line 1–2; another attenuator of 10 dB was inserted in the middle of line 3–4; line 5–6 was straight. The overall attenuation of line 1–2 was 8.6 dB, the attenuation of line 3–4 was 12.7 dB, and the attenuation of line 5–6 was 1.4 dB.

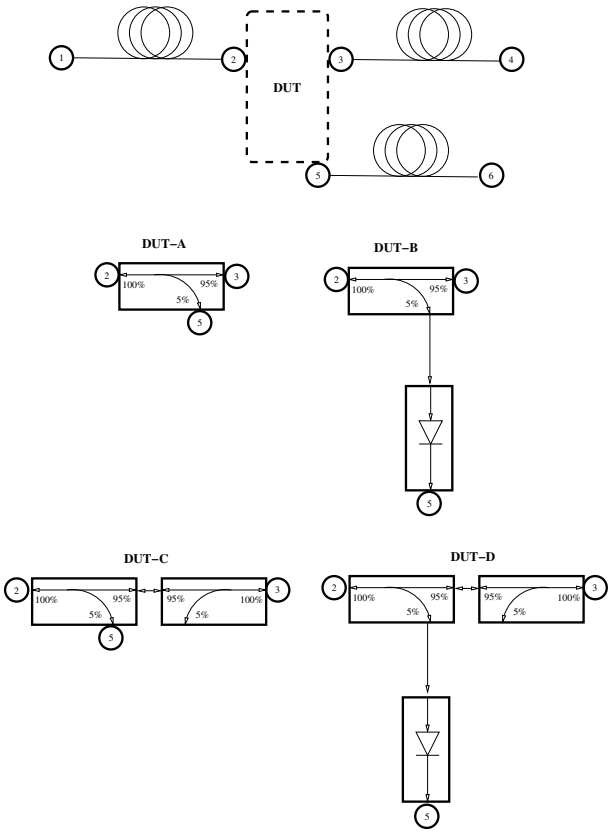

Fig. 6: LAB model used for optical eavesdropping components analysis.

3.1. Eavesdropping Point Detection by Optical Performance Monitoring

The optical splitter introduces additional insertion loss into the fiber optic line. The added insertion loss is given by the connectors and the coupling ratio of the inserted splitter.

The line insertion losses for the cases of the straight line, one splitter usage, and two splitter usage for gaining independence on the transmission direction are given in the following Tab. 1:

Tab. 1: Splitter insertion loss balance.

Line setup	Attenuation	Attenuation increment
straight (patchcord only)	21.8 dB	–
single splitter (Fig. 3)	22.3 dB	0.5 dB
two splitters (Fig. 4)	22.9 dB	0.9 dB

Tab. 2: Gigabit ethernet SFP optical performance monitoring precision analysis.

	DUT TX (dBm)	DUT RX (dBm)	Pwrmeter RX (dBm)	DUT RX balanced (dBm)
min	2.45	−13.90	−13.90	−14.32
max	2.45	−12.72	−13.86	−13.10
avg	2.45	−13.32	−13.88	−13.72
stddev	0 dB	0.22 dB	0.01 dB	0.22 dB

It is easy to see that the attenuation increment is not large. Further, we analyzed the optical performance monitoring precision of some commonly-used SFP modules. We measured the gigabit ethernet modules used for traffic eavesdropping in our experiment, a multi-rate 100 Mbps to 2.4 Gbps SFP module, and a ten-gigabit ethernet SPF+, all of them transmitting on a precise wavelength in a 100 GHz DWDM grid. These SFP and SFP+ modules will be also called a Device Under Test (DUT).

For measurement, we used the lab setup presented in Fig. 7. The output of the measured SPF was attenuated by a fixed 10 dB attenuator.

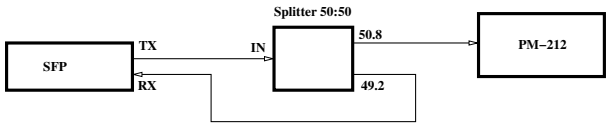

Fig. 7: SFP module optical performance measurement precision analysis.

To obtain precise measurements, we first analyzed the coupling ratio of the splitter used in this setup. The coupling ratio of the splitter (A:B) was determined to be 49.2:50.8. The results from our measurements are summarized in Tab. 2, Tab. 3, and Tab. 4. The original measured data are available upon request for verification or further processing. In all cases, the measurement was 20 minutes long with a 10 s time delay. This was enough to see the instability of the SFP module measurement results.

Tab. 3: Multirate SFP optical performance monitoring precision analysis.

	DUT TX (dBm)	DUT RX (dBm)	Pwrmeter RX (dBm)	DUT RX balanced (dBm)
min	1.91	−13.30	−13.70	−13.43
max	1.96	−13.21	−13.61	−13.39
avg	1.93	−13.26	−13.66	−13.41
stddev	0.01 dB	0.02 dB	0.02 dB	0.01 dB

From the above-mentioned measurements, it is evident that the commonly used optical performance measurement offered by SFP optical modules is not precise enough to reliably detect optical line performance decreases caused by eavesdropping equipment insertion. The only exception is the multi-rate SFP. Moreover, the attenuation of the fiber optic line changes in time due to the change of mechanical stress caused by, for example, temperature changes or other external influences. In our long-term experience, the daily variation of a 40 km long optical line attenuation is about 0.6 dB. Adding a simple fiber optic splitter causes only a very small increase in the communication line insertion loss (0.5 dB). This insertion loss is typically below the common daily fluctuation of communication line insertion loss. Moreover, the precision of typical optical performance monitoring performed by SFP and similar optical modules is beyond this margin as well. For this reason, a simple analysis of optical performance is not enough to detect a fiber optic splitter inserted into the communication line. For a more sophisticated construction based on two optical splitters, the insertion loss increase (0.9 dB) is somewhat detectable, but a basic optimization of the constructed eavesdropping equipment can slightly decrease the inserted loss and make this construction almost invisible as well.

Tab. 4: Tengigabit ethernet SFP+ optical performance monitoring precision analysis.

	DUT TX (dBm)	DUT RX (dBm)	Pwrmeter RX (dBm)	DUT RX balanced (dBm)
min	1.43	−14.88	−15.33	−14.63
max	1.49	−14.01	−14.43	−14.48
avg	1.45	−14.41	−14.84	−14.54
stddev	0.02 *dB*	0.18 *dB*	0.19 *dB*	0.03 *dB*

3.2. Eavesdropping Point Detection by OTDR

The utilization of OTDR could be used to detect eavesdropping points inside a fiber optic line. We tested the lab setup as described in Fig. 6 with OTDR as well. To achieve the best possible resolution, we used the smallest possible pulse duration offered by OTDR. The measurement was performed on three commonly used wavelengths: 1310 nm, 1550 nm, and 1625 nm. The results were almost identical. To improve the readability of the graphs and tables, we used the 1550 nm measurement in the following explanation and discussion. According to the short length of the tested fiber, we used the shortest available pulse duration (5 ns), corresponding to a pulse length of 1 m. The length of the launch cable used was 500 m and the measurement averaging period was 30 s.

We used the test setup described in Fig. 6. The tested fiber optic lines were simulated on several looped room-to-room cables in our computer center. We had two cables available, with lengths of 20 m and 30 m, respectively. Several lines from these

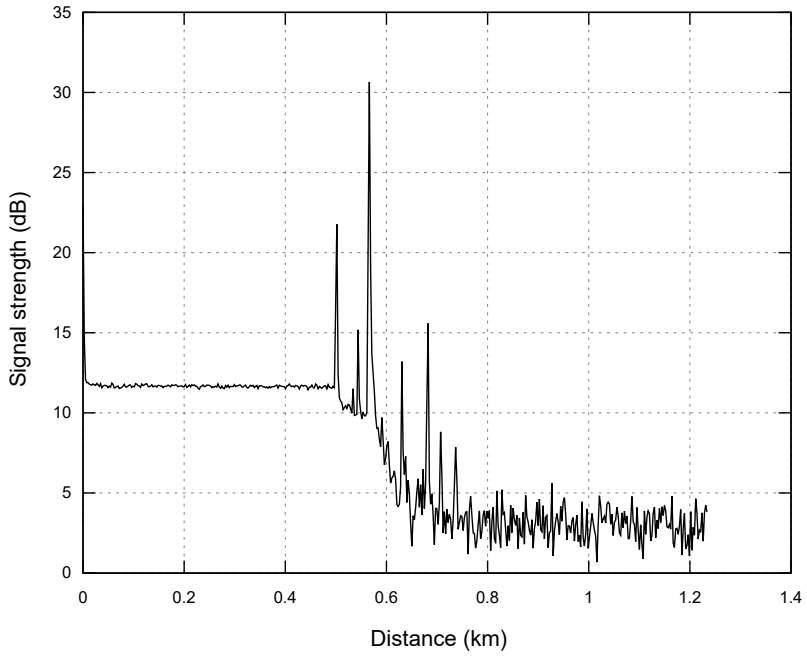

Fig. 8: Reference measurement of eavesdropped line.

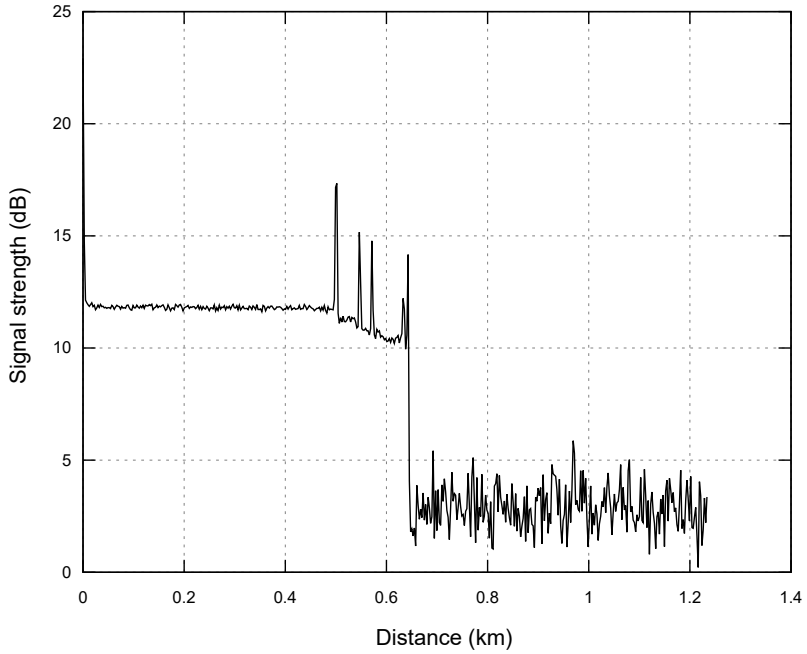

Fig. 9: Reference measurement of an eavesdropper.

cables were interconnected by patchcables terminating in either APC polished connectors (E2000) if we intended the connector to be almost invisible on a reflectogram, or PC polished connectors (PC/APC) if we intended the connector to be strongly visible. The first segment (1–2 in Fig. 6) was 64 m in length with APC connectors only and simulated a clean segment from the attacked data source. The second segment (3–4) simulated a continuation of the line from the eavesdropping point toward the data destination under attack. This line had a total length of 232 m and PC connectors after 64 m, then 50 m and 25 m with a 5 dB attenuator inserted. Line 5–6 simulated the path from the fiber optic splitter toward the active eavesdropper device. This line contained 3 PC-based interconnections for better visibility on the OTDR.

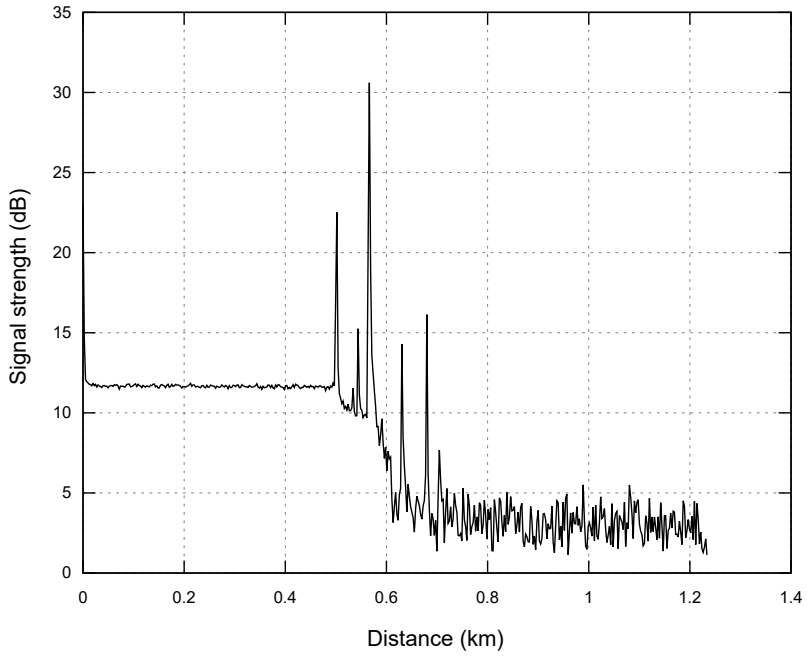

Fig. 10: Eavesdropping equipment variant A - simple optical splitter.

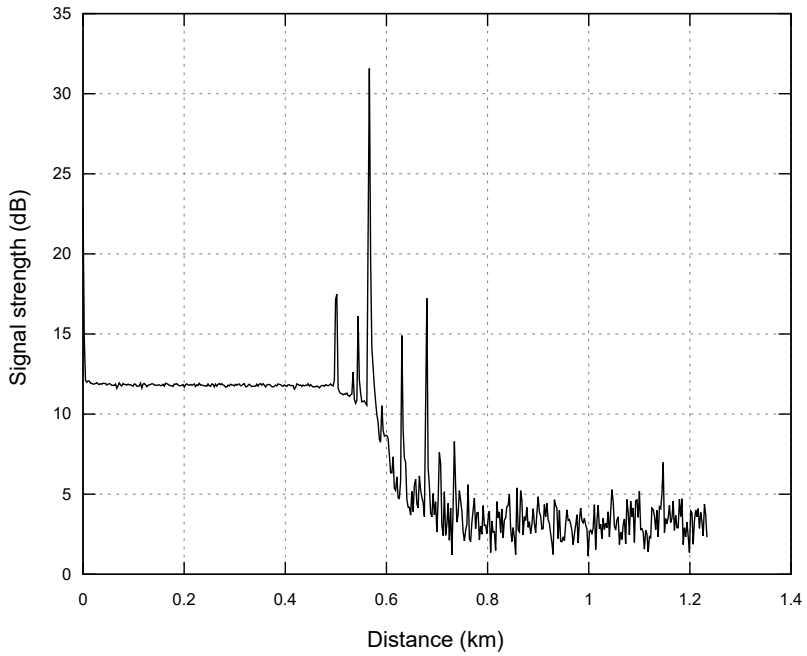

Fig. 11: Eavesdropping equipment variant B - simple optical splitter equipped with a circulator used as an isolator.

The reference OTDR measurement on lines 1–2 and 3–4 interconnected via a simple 2 m patchcable is shown in Fig. 8. The first 500 m segment is the launch cable. The first peak is the beginning of the emulated communication line. The big peak represents the end of the clean line and the beginning of the segment with imperfect connectors. The most important part of the measurement is emphasized by the dashed box. It represents the part where the optical patchcord was replaced by a fiber optic splitter or a set of splitters and circulators as denoted in Fig. 6.

Line 5–6 was used to emulate the eavesdropper communication line. The reference OTDR measurement is presented in Fig. 9. Interestingly, lines with imperfect connectors, such as this setup, can cause better reflections in OTDR. It is expected that the pattern in the dashed box will be present on reflectograms from setups using fiber optic splitters.

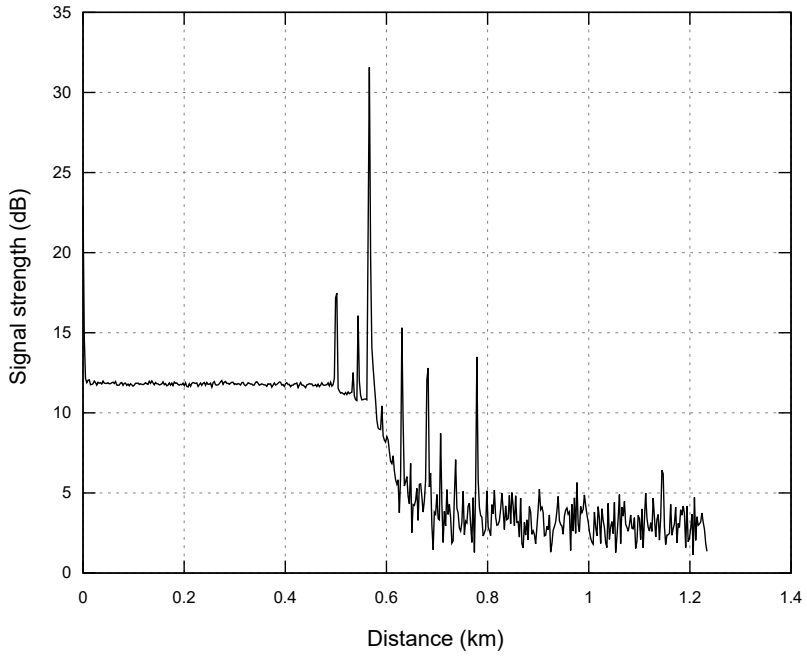

Fig. 12: Two optical splitters connected in opposite directions to obtain direction-independent eavesdropping.

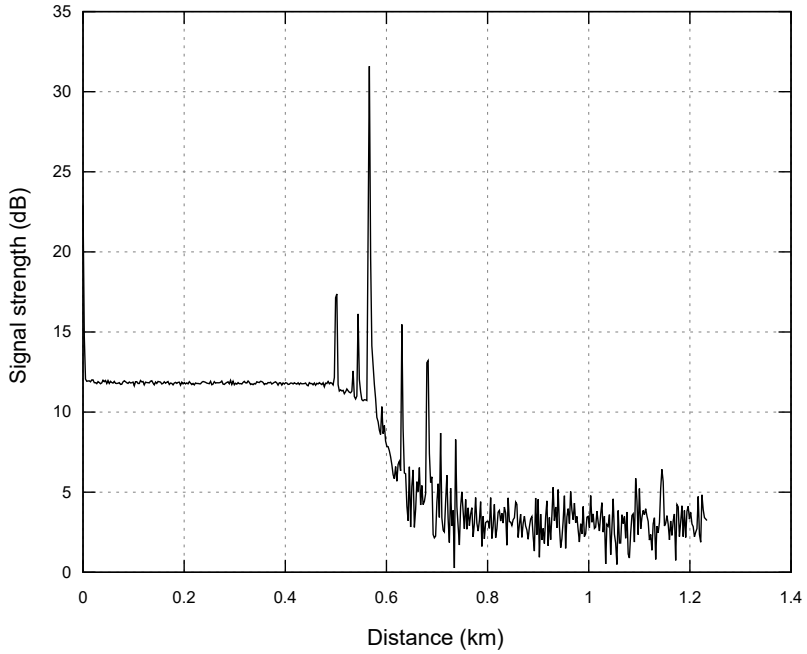

Fig. 13: Two optical splitters equipped with an optical circulator.

The OTDR measurements of the four possible modes of eavesdropping as depicted in Fig. 6 and referred to as connections A, B, C, and D are in Fig. 10, Fig. 11, Fig. 12 and Fig. 13, respectively. It is easy to see that the pattern of the eavesdropper's communication line represented in Fig. 9 is difficult to find in the reflectograms; this is true, especially in the case of circulator utilization, where this line is completely invisible on the reflectograms.

Even when utilizing a splitter directly without hiding the eavesdropping communication line behind an isolator or circulator, it is not easy to notice the eavesdropping point. If an isolator or circulator is used, the splitter is almost invisible to commonly used measurements as can easily be seen from reflectograms Fig. 10, Fig. 11, Fig. 12 and Fig. 13 - emphasized by the dashed box.

All the optical equipment used are easy to acquire from many online component stores for very low prices compared to commonly used network equipment. The active networking devices needed for optical communication eavesdropping might be the same as the ones used for rightful network traffic monitoring. Eavesdropping on optical communication lines is technically much easier and, at the same time, cheaper than most of its users commonly believe. Moreover, detecting optical eavesdropping is very difficult and almost impossible to achieve using common measurement equipment, as the key components behave too similarly to general optical patchcables.

4. Discussion

We have measured the properties of fiber optic splitters and their simple constructions which could be used for fiber optic communication eavesdropping. As expected, even a rather strong split ratio (only 5 % of optical power used for the eavesdropper) is enough to obtain a good quality signal for the attacker while minimizing the impact of the eavesdropped line itself. The splitter is almost undetectable by common measurement equipment like OTDR and/or analysis of the optical power level. Simply modifying this element (adding an optical isolator or circulator) can make it mostly invisible to common measurements. Although the installation of this type of eavesdropping equipment needs some specific knowledge and physical access to the cabling infrastructure, the simplicity and price availability, together with the progress in quantum computing needed for contemporary cryptographic protection mitigation, will make this threat very serious in the near future.

The aim of this paper is to point out the problem of communication networks' physical infrastructure security and especially to emphasize the risk of eavesdropping on fiber optic communication lines. The technical equipment needed to tap the network traffic is of very low cost. The cost of the equipment needed to analyze the tapped traffic corresponds to the used communication protocol and the cost of the equipment used by the eavesdropping victim. The most important property of optical network eavesdropping in this context is the fact that it is almost undetectable by commonly used measurement equipment. To maintain privacy, the use of strong cryptography is necessary, even in the case of communications over fiber optic lines. It is expected that contemporary encryption algorithms will be no more secure in the near future. Currently, properly inspecting fiber optic lines and enforcing the replacement of dismantlable connections (connectors) by non-dismantlable ones (splices) will be crucial.

Acknowledgment

This work was supported by the grant project of the Ministry of Interior of the Czech Republic, no. VI20192022140.

Author Contributions

K.S. conceived of the presented idea, D.G. developed the theoretical formalism and performed the experimental work. Evaluation of the experiment was by J.F. and K.S. verified the analytical and numerical methods. D.G., M.K., and J.F. contributed to the final version of the manuscript. O.D. supervised the project.

References

[1] SKOUBY, K. E., P. DHOTRE, I. WILLIAMS and K. K. HIRAN. *5G, Cybersecurity and Privacy in Developing Countries*. 1st ed. Boca Raton: CRC Press, 2022. ISBN 978-87-7022-647-9.

[2] FUHR, P. L. A Separate Network for Control System CyberSecurity. In: *6th International Symposium for ICS & SCADA Cyber Security Research 2019 (ICS-CSR)*. Athens: Science open, 2019, pp. 144–156. DOI: 10.14236/ewic/icscsr19.18.

[3] NOVOTNY, V., P. SYSEL, J. PRINOSIL, J. MEKYSKA, K. SLAVICEK and I. LATTENBERG. Critical Infrastructure Monitoring System. In: *2021 IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA)*. Langkawi: IEEE, 2021, pp. 165–170. ISBN 978-1-66541-484-5. DOI: 10.1109/CSPA52141.2021.9377303.

[4] CHYAD, R. M., A. H. ALI, N. H. KHALEF, A. A. HAMAD, A. I. MAHMOOD, B. R. MAHDI, W. H. RASHID and N. K. SHAIEE. Design and Construction of Security Monitoring System for Optical Fibre Communications. *Journal of Physics: Conference Series*. 2019, vol. 1234, iss. 1, pp. 1–7. ISSN 1742-6596. DOI: 10.1088/1742-6596/1234/1/012008.

[5] WANG, D. *Selected Topics on Computed Tomography*. 1st ed. London: IntechOpen, 2013. ISBN 978-953-51-7147-8.

[6] SLAVICEK, K., M. JAVORNIK and O. DOSTAL. Extension of the shared regional PACS Center MeDiMed to smaller healthcare institutions. In: *The Eleventh International Conference on Networks (ICN 2012)*. Saint Gilles: IARIA XPS Press, 2012, pp. 83–87. ISBN 978-1-61208-183-0.

[7] JAVORNIK, M., O. DOSTAL and K. SLAVICEK. Regional Medical Imaging System. 2011, vol. 7, iss. 5, pp. 733–737. DOI: 10.5281/ZENODO.1329793.

[8] DOSTAL, O. and K. SLAVICEK. Wireless Technology in Medicine Applications. In: *Personal Wireless Communications*. Boston: Springer US, 2007, pp. 316–324. ISBN 978-0-387-74158-1. DOI: 10.1007/978-0-387-74159-8_30.

[9] AGALLIU, R. and M. LUCKI. Transmission Transparency and Potential Convergence of Optical Network Solutions at the Physical Layer for Bit Rates from 2.5 Gbps to 256 Gbps. *Advances in Electrical and Electronic Engineering*. 2018, vol. 15, iss. 5, pp. 877–884. ISSN 1804-3119. DOI: 10.15598/aeee.v15i5.2502.

[10] KYSELAK, M., F. DVORAK, J. MASCHKE and C. VLCEK. Optical Birefringence Fiber Temperature Sensors in the Visible Spectrum of Light. *Advances in Electrical and Electronic Engineering*. 2018, vol. 15, iss. 5, pp. 885–889. ISSN 1804-3119. DOI: 10.15598/aeee.v15i5.2419.

[11] FAJKUS, M., J. NEDOMA, L. BEDNAREK, J. FRNDA and V. VASINEK. Analysis of the Applicability of Singlemode Optical Fibers for Measurement of Deformation with Distributed Systems BOTDR. *Advances in Electrical and Electronic Engineering*. 2016, vol. 14, iss. 4, pp. 453–459. ISSN 1804-3119. DOI: 10.15598/aeee.v14i4.1785.

[12] SLAVICEK, K. and V. NOVAK. Fiber optics transport infrastructure of cesnet backbone. In: *Proceedings of the 6th WSEAS international conference on Applied computer science*. Canary Islands: WSEAS, 2006, pp. 323–328. ISBN 978-960-8457-57-7.

[13] SLAVICEK, K., V. NOVAK and J. LEDVINKA. CESNET Fiber Optics Transport Network. In: *2009 Eighth International Conference on Networks*. Gosier: IEEE, 2009, pp. 403–408. ISBN 978-1-4244-3470-1. DOI: 10.1109/ICN.2009.80.

[14] SMOTLACHA, V. and J. VOJTECH. Czech Optical Infrastructure CITAF. In: *2022 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS)*. Paris: IEEE, 2022, pp. 1–3. ISBN 978-1-66549-718-3. DOI: 10.1109/EFTF/IFCS54560.2022.9850853.

[15] LIU, M., Y. LI, H. SONG, Z. TU, Y. ZHAO and J. ZHANG. Experimental Demonstration of Optical Fiber Eavesdropping Detection Based on Deep Learning. In: *2019 Asia Communications and Photonics Conference (ACP)*. Chengdu: IEEE, 2019, pp. 1–3. ISBN 978-1-943580-70-5.

[16] SI, H., H. LIU and H. MA. Optical Fiber Communication Network Eavesdropping and Defensive Measures. In: *Proceedings of the 2nd International Forum on Management, Education and Information Technology Application (IFMEITA 2017)*. Shenzhen: Atlantis Press, 2018, pp. 307–310. ISBN 978-94-6252-464-4. DOI: 10.2991/ifmeita-17.2018.53.

[17] FURDEK, M., N. SKORIN-KAPOV, S. ZSIGMOND and L. WOSINSKA. Vulnerabilities and security issues in optical networks. In: *2014 16th International Conference on Transparent Optical Networks (ICTON)*. Graz: IEEE, 2014, pp. 1–4. ISBN 978-1-4799-5601-2. DOI: 10.1109/ICTON.2014.6876451.

[18] IQBAL, M. Z., H. FATHALLAH and N. BELHADJ. Optical fiber tapping: Methods and precautions. In: *8th International Conference on High-capacity Optical Networks and Emerging Technologies*. Riyadh: IEEE, 2011, pp. 164–168. ISBN 978-1-4577-1169-5. DOI: 10.1109/HONET.2011.6149809.

[19] FOK, M. P., Z. WANG, Y. DENG and P. R. PRUCNAL. Optical Layer Security in Fiber-Optic Networks. *IEEE Transactions on Information Forensics and Security*. 2011, vol. 6, iss. 3, pp. 725–736. ISSN 1556-6021. DOI: 10.1109/TIFS.2011.2141990.

[20] SPURNY, V., P. MUNSTER, A. TOMASOV, T. HORVATH and E. SKALJO. Physical Layer Components Security Risks in Optical Fiber Infrastructures. *Sensors*. 2022, vol. 22, iss. 2, pp. 1–15. ISSN 1424-8220. DOI: 10.3390/s22020588.

[21] HUDCOVA, L., O. WILFERT and A. DOBESCH. Interferometric method for the relative variance of the optical power measurement. In: *2014 24th International Conference Radioelektronika*. Bratislava: IEEE, 2014, pp. 1–4. ISBN 978-1-4799-3714-1. DOI: 10.1109/Radioelek.2014.6828449.

[22] KOLKA, Z., V. BIOLKOVA, O. WILFERT, D. BIOLEK, M. KUBICEK and P. BARCIK.

Modeling Output Signals of Solid-State Photomultiplier with Capacitive Coupling. In: *2020 New Trends in Signal Processing (NTSP)*. Demanovska dolina: IEEE, 2020, pp. 1–4. ISBN 978-1-72816-155-6. DOI: 10.1109/NTSP49686.2020.9229534.

[23] KOUDELKA, P., P. SISKA, J. LATAL, R. POBORIL, L. HAJEK, S. KEPAK and V. VASINEK. Security risk assessment of the primary layer of wavelength division multiplexing passive optical network. Prague: SPIE, 2015, pp. 1–7. DOI: 10.1117/12.2070468.

[24] ABBAS, H. S. and M. A. GREGORY. The next generation of passive optical networks: A review. *Journal of Network and Computer Applications*. 2016, vol. 67, iss. 1, pp. 53–74. ISSN 10848045. DOI: 10.1016/j.jnca.2016.02.015.

[25] DIAA, M., M. SHALABY, A. A. MOHAMED, K. M. M. HASSAN and A. M. MOKHTAR. Undetectable Tapping Methods for Gigabit Passive Optical Network (GPON). In: *2018 14th International Computer Engineering Conference (ICENCO)*. Cairo: IEEE, 2018, pp. 52–57. ISBN 978-1-5386-5117-9. DOI: 10.1109/ICENCO.2018.8636110.

About Authors

David GRENAR (corresponding author) received his master's degree from the Faculty of Electrical Engineering and Communication at the Brno University of Technology. He works in a multidisciplinary team doing research concerning the application of new communication systems.

Jakub FROLKA received his master's degree from the Faculty of Electrical Engineering and Communication at the Brno University of Technology. His work covers end-user experience in ICT services with a focus on application security.

Karel SLAVICEK finished his habilitation (2020) in Telemedical systems at the Faculty of Electrical Engineering and Communication at the Brno University of Technology. His current research is focused on optical systems for sensor applications. Currently, he is head of national and international research projects. His main research fields include the application of the new methodology in measurement processing.

Otto DOSTAL is the vice director for research and development at the Institute of Computer Science at Masaryk University. He has a huge experience with integrating new communication systems in optical infrastructure

Martin KYSELAK finished his habilitation (2019) in Optical communication at the Faculty of Electrical Engineering at the University of Defence. His current research is focused on the technology of special PM fiber applications. Currently, he is an associate professor in the Department of Electrical Engineering, University of Defence. His main research fields include polarization in optical communication and polarization of light for sensing purposes.