Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

Intrusion detection in optical fiber link: A novel technique

Sudad Selman Ahmed

Department of Physics, Faculty of Science, University of Baghdad, Baghdad, Iraq
soudadbassam@gmail.com

Abstract

Because of the complexity of the observation of the eavesdropping process in optical fiber link, a new technique is suggested. A WDM is utilized as a part of optical fiber intrusion detection system. The implemented setup is capable to observe eavesdropping soon. The PC unit supports the system and it offers a suitable tool to observe or detect the leakage information. The minimum detectable attenuation value due to the intrusion is about (0.04 dB) while the optical power leakage is about 0.1 dB.

Keywords: Intrusion, optical link, detection, eavesdropping.

Introduction

The utilization of optical communications has been common for many years. From the time of the most primitive civilization, man has employed artificial optical techniques to send information over a long distance (Keiser, 2000). The novelty of modern optical communication system is that the optical signal is usually guided and signaling rates are very high (Kawaniski *et al.,* 1995). Because of the communication spying, a great proportion of important secrets and information must pass through communication network data security, and at the same time becomes an important target for intruders (Bennett *et al.,* 2000). The data leakage is considered the most important ways of spying process in the optical fiber link and then intrusion detector must be used. The emergence of the dense wavelength division multiplexer (DWDM) is one of the most recent and important phenomena in the development of fiber optic transmission technology.

This WDM avoids many of the constraints and implementation difficulties that limit the performance of time division multiplexing (TDM) systems; it still plays an important role in optical communication capacity. An intrusion-alarmed optical communication system in which two separate model groups are launched into a single graded index transmission fiber. The system includes 2 light sources and a lens to focus the light sources into the transmission fiber. A spatial filter is used to selectively limit the angles of incidence of the light on the fiber and operates in conjunction with the lens to launch light from one source at appropriate angles and points of excitation to excite higher-order modes in the fiber, and to launch light from the other source at appropriate angles and points of excitation to excite lower-order modes in the fiber (Charles *et al.,* 1993).

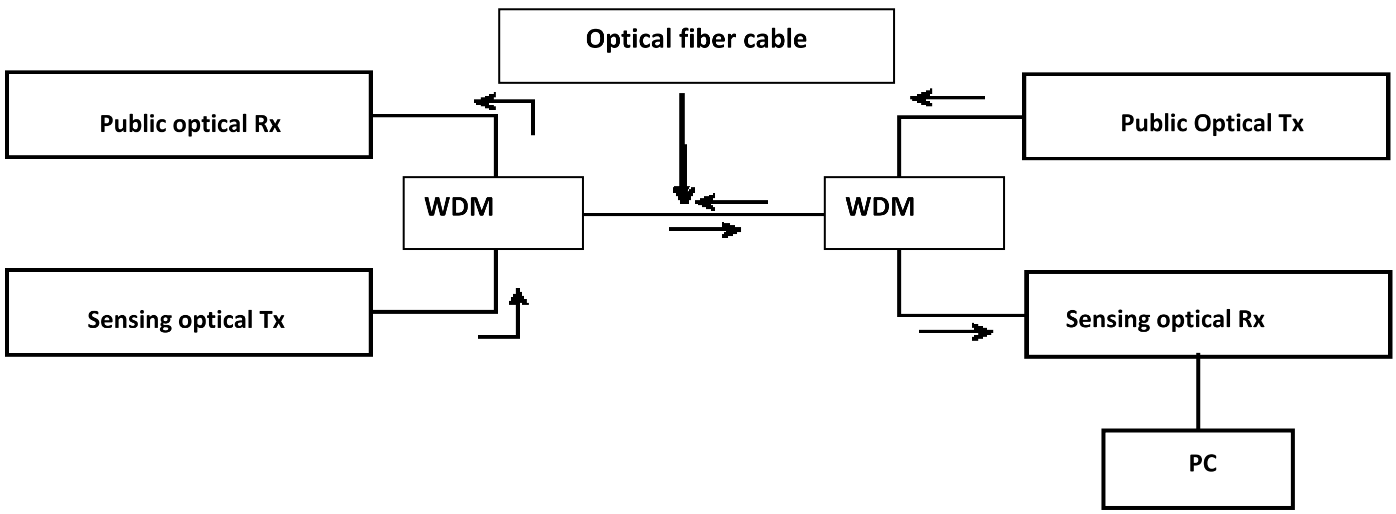
The optical fibers are easily tapped and that the data stream can be intercepted. The more evasive methods do not require a physical intrusion into the light path which makes intrusion detection by the transmission system difficult and unreliable. A relatively simple non-interruptive tapping method involves placing a bend coupler on the fiber to be tapped. Bend couplers are not exotic pieces of equipment; they are readily available in the form of standard, inexpensive optical test and measurement gear from a variety of manufacturers. To avoid the intrusion process power measuring intrusion detection systems must be utilized to detect this loss in optical power and to provide warning alarms (Technical report, 2005). The aim of this work is to utilize the WDM as a part of the optical fiber intrusion system in order to achieve the security task.

Intrusion monitoring technique

There are many reasons for optical power leakage in optical fiber link such as micro bending, modified cladding, splicing zone in the fiber cable, connectors, repeaters, etc. Thus, the leaked optical power could be detected by eavesdropping. Because of the complexity of the observation of the eavesdropping process, a well established technique must be used. Using a WDM in optical link permits an optical fiber to carry many different wavelengths of light simultaneously without mutual interference. Each wavelength represents an optical channel within the fiber. Networks in which individual fiber carry more than 100 independent optical channels using the WDM are commercially available (Mollenauer & Licktman, 1992). As well as those in which a bi-directional use in most of the fiber. Fig. 1 shows the experimental setup that implemented in this work to observe the eavesdropping immediately.

Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

Fig. 1. The experimental setup.



The setup consists of two links namely sensing link and public link. The sensing link consist of 1.55 µm optical transmitter operates with 1 Mb/s bit rate and the PIN photo detector with 1 ns rise time. The output of the detector is connected with the personal computer via the interfacing unit supported by a computer program written in a visual basic language. The software gives all information about the dropping process (i.e. the received power, time of dropping, sensitivity & minimum detected power). All these information are noticed by the PC which is connected to the system. The sensing link is combined with public optical link (STM 1 i.e. 155 Mbit/s transmission rate) and 1.3 µm wavelength transmitter via a pair of WDMs. Because of the combination of these 2 links by a single mode optical fiber and two WDMs, the system operates as a full duplex technique. In order to examine the performance of the sensing channel, a circular bending of the optical fiber is achieved. By setting the interface program, to detect the power variance within the 0.1 dBm (sensitivity), the monitoring link become very sensitive against any effect that happen on the optical fiber. During the dropping process, the voice and visual alarm and dropping time are enrolled in the PC unit. Besides the sensing channel the public channel is worked instantaneously. The sensing channel may be used for measuring and testing the optical fiber in the system without any reduction in the system performance. To analyze the power budget in the presented system, we will consider a two WDMs form a biconical tapered fiber coupler (Fig. 2). The injected optical power Po being the input power and, P1 and P2 the output power, the splitting ratio (Ps) is:

Ps = (p2 /p1+p2)*100%

A coupler could be made in which almost all the optical power at 1.55 µm goes to one port and almost all the energy around 1.3 µm goes to the other port. The insertion loss refers to the loss for a particular port-to- port path. The insertion loss in dB is:

Insertion loss (dB) = 10 log (p input/p output)

The cross talk measures the degree of isolation between the input at one port and the optical power scattered or reflected back in to the other input port. That is, it is a measure of optical power value P3 shown in Fig. 2 then:

Cross talk = 10 log (P3/Po)

Fig. 2. The cross-sectional view of a 2X2 optical fiber coupler.

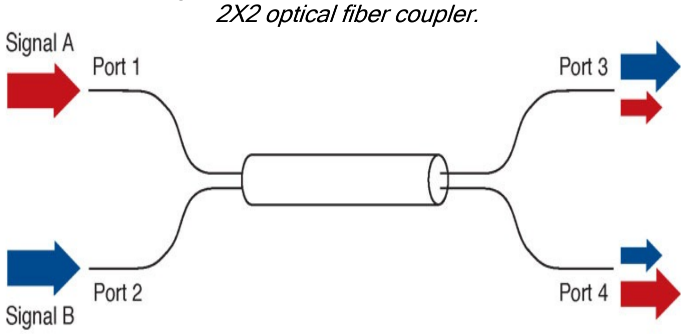


Fig. 3. Optical fiber bending effect on the transmitted optical power.

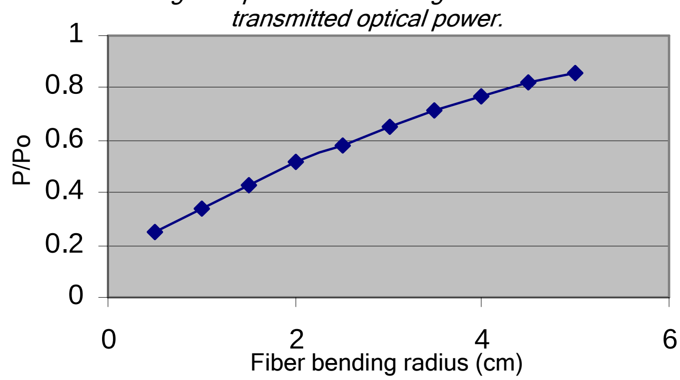
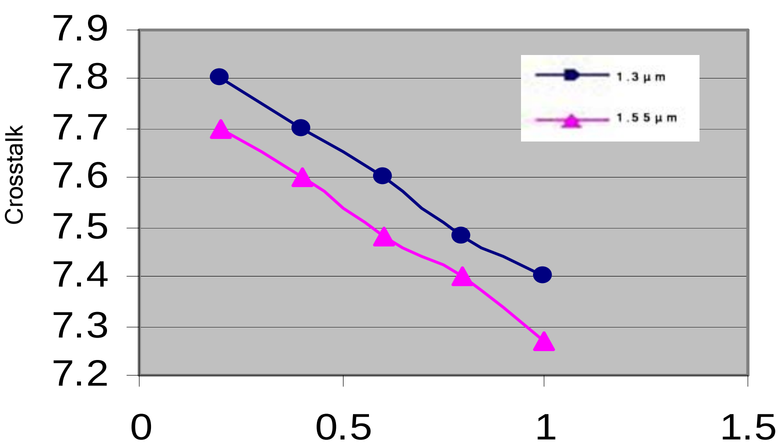


Fig. 3 shows the relation between the measured received power and the fiber bending radius (i.e. the insertion loss) with the lunched power Po is about -10 dBm for 1.3 µm and 1.55 µm wavelengths. The crosstalk behaviour with the optical fiber bending radius is illustrated in Fig. 4, for both wavelengths. The crosstalk decreased by increasing the fiber bending radius, this mean that the additional power could be added to the detected power via port 3, this leads to the sensitivity of the system is increased by increasing the bending radius. If a cladding-to cladding coupling is made using a special intercept fiber the intercepted light, which is detected by a sensitive receiver, can easily be 20 or 30 dB down from the power in the fiber core. This results in a loss of received optical power of only 0.04 or 0.004 dB and is impossible to detect reliably by power measurement methods.

Fig. 4. Crosstalk Vs. the optical fiber bending radius.



Conclusion

Although the eavesdropping capabilities of the intrusion process the presented work offers suitable tool to observe and detect the eavesdropping process without any disruption of the data steam. The presented technique based on the WDM is a continuous real time and protocol independent of optical fiber network connection.

Acknowledgment

The author thanks R. M. Jiad and N. D. Selman for their assistant during this work.

References

1. Bennett CH and Di Vincenzo DP (2000) Quantum information and computation: Review article on Macmillan magazines Ltd., 404, 247-255.
2. Charles K (1993) Bimodel intrusion detection in an optical fiber communication system using graded index fiber. US patent no. 398/44.
3. Kawaniski S, Takara H, Kamatani O and Morioka T (1995) 100 Gbit/s, 500 Km optical transmission experiment. *Elect. Lett*. 31(9), 737-745.
4. Keiser G (2000) Optical fiber communications. 3rd Edn., McGraw Hill, Inc.
5. Mollenauer LF, Licktman E, Harvey GT, Neubelt MJ and Nyman BM (1992) Demonstration of error-free soliton transmission over more than 15000 km at 5 Gbit/s, single channel WDM and over more than 11000 km at 10 Gbit/s in tow channels WDM. *Elect. lett*. 28(8), 792-794.
6. Technical report (2005) Fiber optic intrusion detection systems. Network integrity systems.