International Journal of Engineering Sciences Paradigms and Researches Vol. 10, Issue 01, December 2013
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Review of Optical Fiber

Pulkit Berwal

Electronics and Communication Department
pulkit.berwal123@gmail.com

Abstract
Optical fibers are widely used in the area of communication due to their utility and potential. The major issue with any communication system is security. As the fiber optics gaining popularities in the communication field than large amount of security threats also arise by which system privacy and reliability is affecting. In the communication network the network reliability and privacy is very important. In this review paper I concentrate on security threats and then the methodology behind such threats, further more the detection and the counter measures are explained. The concept of encoding the data over the channel is also explained as the solution to security issues.
Keywords: *Optical Fiber, Physical Security, Service Disruption Attacks.*

1. Introduction

Service disruption and information steeling are major issues cracking the quality and reliability of the optical fiber channels. Now a days the major issue of each communication system is security. Hackers have developed devices to crackdown optical fibers either for extracting military/commercial information or disrupting the services. Such devices basically depend on the phenomenon of fiber bending and crosstalk interference which remain to be undeniable properties of optical fiber cables.
This paper is organized as follows: section 2 describes problem statement. section 3,4,5 describes physical security, attack detection and attack prevention respectively. The paper is then concluded in section 6.

2. Problem Statement

Along with the passage of time optical fibers are becoming the widely used communication channel all over the globe as they provide a better solution to reliability and bottle neck bandwidth issues. A major issue behind every communication channel is the protection of data over the channel. These days' optical channels are also facing different security issues such as information steeling as well as service disruption. This term paper will give sum remedies to avoid such security threats. To provide secure and reliable AONs, various security issues should be considered including physical security and information security. Physical security prevents unauthorized access to network resources. Information security, on the other hand, prevents unauthorized access to information, and assures confidentiality and integrity of the information[1].

3. Physical Security

Service disruption and tapping are the two most common threats to the physical security of AONs(All optical networks). The most commonly used AON components including optical fiber cables, Combiners, splitters, multiplexers, de- multiplexers, optical amplifiers, optical transmitters, and optical receivers are susceptible to service disruption and tapping attack.

3.1 Service Disruption Attacks:

Service disruption attacks causes data decay service denial and QoS(Quality of service) degradation. Under normal operating conditions, optical fibers radiate a negligible amount of power from the fiber compared to other wave-guide media such as coaxial cable. However, like coaxial cable, service can be easily disrupted if optical fiber is cut or disrupted by any way. Light may be radiated into or out by making a slight bend in the fiber by such less disruptive attack. Two other most widely used methods of service disruption attacks are in-band jamming and out-of-band jamming.

- In in-band jamming, an attacker injects a signal which is specifically designed in order to reduce to interpretation of receiver. The attack can degrade the whole transmission signal. This is due to the easily access that AON'S provide.

- In out-of-band jamming, an attacker reduces communication signal component by exploiting leaky components or cross-modulation effects. An out-of-band jamming attack can be used to exploit crosstalk in various components. In this type of attack, an attacker injects a signal at a different wavelength from the communication bands, but within the amplifier pass-band. The amplifier provides gain to attack signals and legitimate network communication signals indiscriminately from a finite supply of gain because it cannot distinguish between those signals. [1].

3.2 Tapping Attack: -

Tapping can be used to gain unauthorized access to information that may be used for spy or traffic analysis. Tapping attacks can be done at many points due to which the problem of cross talk arises. For example, contemporary de-multiplexers within network nodes separate each individual signal (or wavelength) received from a single fiber on to separate physical paths. These de-multiplexers may exhibit cross-talk levels between 0.03% and 1.0%. These cross-talk levels allow a little of each signal to leak onto the wrong path. Yet these signals may have enough fidelity to permit an attacker to detect their presence and recover a portion of data. At high signal levels, such as at the output of an optical amplifier, fibers exhibit some cross-talk that may be used for tapping by co-propagating a signal on the fiber. Tapping can also be combined with jamming for very powerful service disruption attack. As delay may vary gradually with respect to data rates, an attacker may tap a signal and also inject a signal downstream of the point of tapping. This type of attack is called a correlated jamming attack. This attack is very harmful to users with very low Signal to Noise
Ratio (SNR). [1]

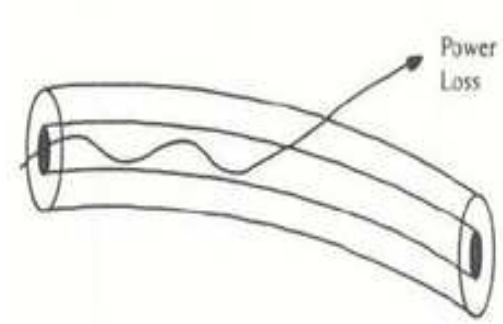

Fig 1: power loss by fiber bending [1]

4. Attack Detection

There are various existing supervisory techniques and automatic diagnostics which can be applied to detect attacks upon AONs. Supervisory techniques are classified into two categories; methods that perform statistical analysis of data, and methods that measure a signal devoted to diagnostic purposes. [1]

A. Power Detection methods:

These methods are based on the comparison of received optical signal power to the expected value of optical signal power. Any change in the received optical signal power with respect to the expected signal power could be used to determine security attacks. There are two major drawbacks of these methods.
Firstly, a slight decrease in optical signal power is difficult to detect. Secondly, small but detectable changes in optical signal power resulting from component aging and fiber repairs may not be attributable to attacks, and may not adversely affect optical signals.

B. Optical spectrum analysis methods:

These methods measure the spectrum of an optical signal. They are able to detect a change in spectrum shape, even if that change in shape does not involve a change in power over the whole channel. Optical spectrum analysis methods provide more information than power detection methods. However, they rely on statistical comparisons between sample averages and statistical averages that require additional processing time that makes them slower than some other attack detection methods.

C. Pilot tone methods:

These methods use highly defined and unique signals, called Pilot tones, which travel along the same links and nodes as the communications data. They are used to detect transmission disruptions.

D. Optical time domain reflectometry methods:

Optical time domain reflectometry methods are a special application of pilot tones. They analyze the pilot tone's echo. These methods are typically used to detect attacks that involve fiber tampering.

5. Attack Prevention

Some hardware measures can be employed to alleviate service disruption such as following:

1. Optical Limiting Amplifier (OLA) limits the output power to a specified maximum. Setting limits on light power also limits crosstalk and, therefore, crosstalk detection.

2. Band-limiting filters can be utilized in order to discard signals outside certain bandwidth. This can prevent gain competition attacks in optical amplifiers.

3. Alarming and physical strengthening of the cladding or ways to detect minute power losses may prevent a physical tap in the fiber. However, physical strengthening and alarming the cladding needs tremendous changes in the existing infrastructure, and that entail significant expense. Additionally, physically securing optical fiber against physical tapping does not provide protection against tapping via crosstalk. As an alternative, devices with lower crosstalk may diminish both service disruptions and tapping attacks.

4. Separate data paths for trusted and non-trusted users may also prevent security threats[1].

6. Encoding the Data

This data protection technique encodes the data at the transmitter side with a specific understandable key for the receiver; this data over the channel is only understandable by the specific receiver .The encoding of the data is done by coding done at the transmitter end and the process of decoding done at the receiver end. This technique indeed minimizes the threat of data privacy exploitation over the optical channel. Some users are reluctant to implement encryption unless absolutely necessary because generating keys and processing encryption slows down their computer systems. The processing speed due to the encryption is affected due to which performance issues arise. Other users implement encryption but are frustrated by the resulting slowdowns[4].

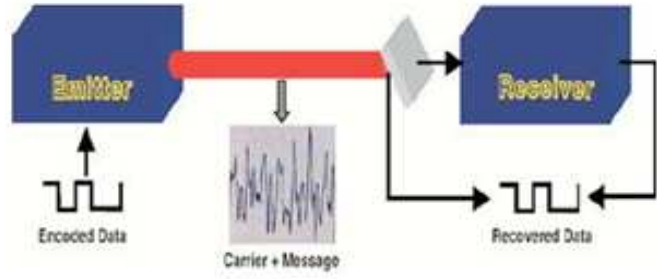

Fig 2 : Encoding/Decoding Block Diagram [4]

7. Conclusion

The security is the main issue of any communication system. Optical fiber is the key element of the all optical networks therefore it is necessary to manage the protection against tapping and detection is the major aspect of this. The physical strengthening of the fiber optic channel may protect the channel from the intruders but this increase the cost of the whole system by which the optical communication will be expensive. Therefore the encryption of the data at the transmitter end will be more feasible solution within the existing condition by which the privacy can be achieved up to a better level.

References

[1] Mathias Bischoff, Manfred N. Huber, Oliver Jahreis, Siemens AG, Frown Derr and Fachhochschule Ulm, “Operation and Maintenance for an All-Optical Transport Network,” IEEE Communications Magazine, Nov. 1996.

[2] C.H. Bennet and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing” Proc. Int’l Conference. Computers, Systems & Signal Processing, CS Press, 1984, pp. 175–179.

[3] H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel, “Practical aspects of quantum key distribution”, J. Cryptology Nov 1998 , pp. 1-14

[4] S. Donati and C. Mirasso Eds., “Optical Chaos and Applications to Cryptography”, IEEE Journal of Quantum Electronics, Sep 2002.