A Review of Fiber Tapping Mechanisms

Ritu Vyas*, Aapurva Kaul*, Ritambhara*, Kriti M Sharda*

*(Assistant Professor, Department of Electronics and Communication, JECRC Jaipur Email: rituvyas.ece@jecrc.ac.in, aapurvakaul.ece@jecrc.ac.in, ritambhara.ece@jecrc.ac.in, kritisharda.ece@jecrc.ac.in)

Abstract: Nowadays technology has increased the data rate with high speed of reliable data tra nsmission both for domestic security and network-centric operations and makes secure communications is a critical issue of present day security It is also possible to successfully tap an optical signal, if detection and or prevention mechanisms are not actively integrated into network management. . Mean while fiber optic cables are having huge bandwidth, large data rate and immune to typical interference issues. This paper focus on quantifyin g the loss required to successfully tap a signal propagating in a fiber and analyzing the properties of the techniques that could be used to detect a fiber splitting and bending.

Index Terms: Optical fiber, Optical splitting, Evanescent coupling, Vgroove cut, Optical Scattering, OTDR, WDM

INTRODUCTION

There are different methods to tap into an fiber optic cable including fiber bending, splitting, evane scent coupling, scattering, and V-grooves[1]. In order to change the physical characteristics of the fiber, most of the techniques requi re the use of sophisticated and cumbersome equipment. Out of all the techniques, the bent fiber ta p, coupling, splitting are the most easily deployed to couple light out of the fiber with minimal ri sk of damage or detection. The methods of quantifying the loss required to successfully tap a sign al propagating in a single and multimode fiber and characterizing each of the techniques with diffe rent parameters that could be used to detect a fiber splitting and bending [1] are analyzed.

Understanding the mechanisms used for fiber tapping provides greater insight into ways to actively detect unauthorized optical intercepts or compromised network security. Enhanced monitoring techniques enable the detection and localization of fiber taps. These techniques include enhanced optical time domain reflectometer applications for localization of suspected tapping events and simulated results obtained using OPTI SIM. these monitoring techniques will be reviewed with detailed analysis of the methods effectiveness in detecting the taps and cost effectiveness for integration into optical networks

For decades, the major threat to the secure transmission of Information over data networks is the copper cabling and equipment[2]. since copper cables are very susceptible to electromagnetic and radio frequency interference, they must be installed maintaining strict separation guidelines and provi deprotection from intruders.

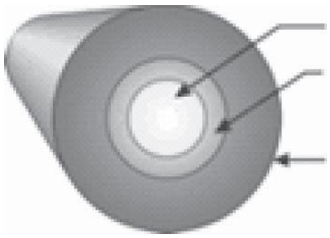
In contrast, fiber optical cables are not susceptible to electromagnetic and radio-frequency interference, since the signal being transmitted is optical instead of electrical. However, d epending on the installation and regional threat-level, often fiber optic cables are still installed to provide greater physical protection of the securei nfrastructure.

While fiber optic cables are exponentially more secured when compared with copper cables, it is st ill possible to intercept the optical signals being transmitted across a network (WDM). However, all forms of fiber tapping and optical intercepts involve accessing the fiber contained within an optica

l cable. In order to understand the various methods to intercept optical signals, it is important to f irst understand how optical fiber and cable is constructed.

Optical fiber contains two primary components: the core and the cladding. The core of the optical fiber is the area in which the light is carried from one end of the network to the other. The clad ding protects the core of the fiber and creates a boundary along the outer edge of the core that a llows the light to reflect inside the core which results in a very little loss or attenuation as the o ptical signal is transmitted over long distances and creating a condition called 'Total Internal Reflec tion'[2].

For the optical signal to be tapped or intercepted, the core of the fiber in a WDM Network carryi ng the traffic must be compromised or tapped. In order to access the fiber an intruder must first physically access the fiber within the optical cable.



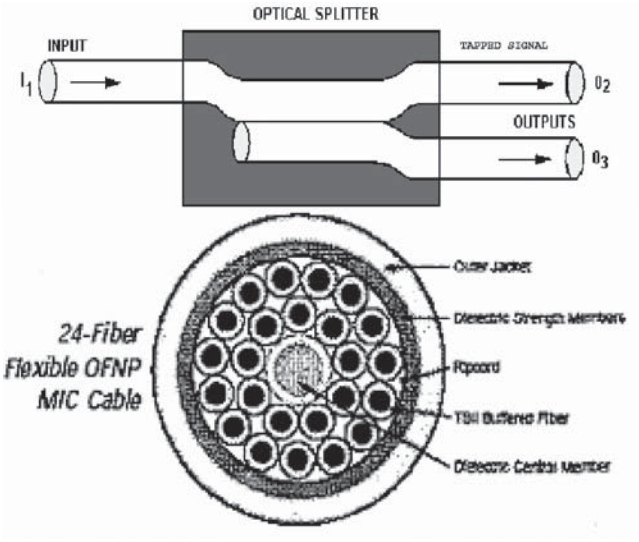
Cross Section of Fiber

The biggest drawback of the using the optical splitter is that installation of such a device will cau se an interruption of service which should result in a security response exposing the system breach. The loss of the splitter will not be necessarily be high. If the splitter is installed in a pat of th e system where the optical fiber is relatively high it may only be necessary to tap afew percent o f the signal with less than I dB loss[1][2]. A lossless splitter could be used to over come this if desired but then the optical splitter requires a source of power making it even more noticeable dur ing visual inspection
or Red Equipment Area) or gain mid span access to the cable. While accessing the terminated end s the fiber end would be preferred, this is also the area with the highest degree of security and p ersonnel scrutiny; so mid –
span access, the intruder would first have to cut through and strip away at least 12-
24" of the outer jacket in order to have enough room to access the individuals fibers in the cente r of the cable. Once the individual fibers are accessed, an intruder has several options in which to intercept or 'tap' the optical signal. These methods include (1) Fiber Bending (2) Optical Splitting (3) Evanescent Coupling (4) V-groove Cut, and (5) Optical scattering.

(1) *Fiber Bending:* A fiber bend loss tap is the easiest tapping method to implement in the fi eld. It involves stripping an individual fiber down to the cladding and bending it to compare the Total Internal Reflection and allowing a fraction of the signal to be coupled out. The power of t he tapped signal will depend upon the radius (R) and angle () of the bend[1].

The aim of the an intruder would be to use the minimum bend loss required to tap a discer nable data signal without interrupting the optical signal in its entirety or damaging the fiber(both of which would create an interruption of signal alarm from the connecting switch and result in Se curity services being dispatched.). If an optimal fiber bend tap is achieved, the signal degradation will be minimal and only detectable through on going network monitoring and resulting.

(2) *Optical splitting*: An optical splitter works very much in the same manner as a coax splitt er for televisions; it splits



Optical Splitter

(3) *Evanescent Coupling :* Very similar to the optical splitter method, evanescent coupling utilizes the same process without requiring the target fiber to be cut and field constructs a 1 × 2 optical splitter rather than using a pre manufacturing device. By polishing the cladding very close to the fiber on both the target and capture fibers, it reduces the reflectivity of the core cladding boundary and allows a portion of the optical signal to be captured by the tap fiber. While this approach appears to have significant advantages over the optical splitter method (i.e. no system interruption, no external splitter device, etc.), it is extremely difficult to implement in a field environment and still results in a noticeable optical loss (1-2dB). An optical fiber is smaller then a human hair and the core size of single mode fiber is less than an eight of an human hair making it almost impossible to achieve the precision required in the field without sophisticated and cumbersome equipment and a great deal of uninterrupted time to install the tap.

(4) *V-Groove Cut:* In this method a V-groove is cut in the cladding of the optical fiber close to the core. The v-groove is cut so that the angle and the face of the groove is greater than the critical angle for the Total Internal reflection. When the condition is met the fraction of the signal traveling in the cladding and overlapping with the V-groove undergoes total internal reflection and is coupled out through the side of the fiber.

Once again a precision cut required in the fiber as well as the subsequent polishing would require precision equipment and a great deal of uninterrupted time to install such a tap. However, this method could result in very little optical loss and would be very difficult to detect. Finally this process requires actually cutting into an optical fiber it is also the riskiest method for achieving a fiber tap in the fiber.

(5) *Scattering:* The use of the fiber Bragg grating to achieve a fiber tap in a WDM Network is the most advanced field technique discussed, and a loss the most difficult to detect via periodic network testing and monitoring . this process requires the use of an excimer UV laser to create an overlapping and interfacing field of UV rays that subsequently ‘etches’ a Bragg grating on to the fiber core. The grating then reflects a portion of the optical signal out of the target fiber into a capture fiber. The benefit of the scattering approach is that it does not require cutting into fiber (such as in a V-groove tap). How ever this method requires he most precession equipment of any and is most difficult to implement in a field environment without detection.

Note: Each of the methods discussed above a specific method for tapping into an optical signal. What has not been discussed however is how that signal is then routed out of the facility or captured locally for interpretation and analysis by the enemy. Several scenarios are feasible, but are very specific to the installation in question and are outside the scope of this paper.

By understanding the various methods an enemy could use to compromise the integrity of a secure optical network, it is easier to plan and implement network architectures, infrastructure, and processors to prevent and/or detect such intrusions. All of the fiber tab methods listed above would result

in same measurable change that could be detected using standard optical test equipment. An optica l test set, which measures optical attenuation (dB), and an Optical Time Domain Reflectometer[4], which measures reflective and non-
reflective 'events' in an optical circuit, are very effective tools for network testing and monitoring.

Optical tester: Optical testers have been used since the early deployment of fiber optic netwo rks to measure the amount of attenuation (dB) or optical loss of the network. Optical testers cons ist of an optical source, which generates a very precise amount of optical signal at various wavel engths, and an optical meter, which is calibrated for precise measurement of the optical signal rec eived. By knowing the amount of optical signal inserted into a network and the amount received on the other end, it is possible to derive the optical loss of the segment as depicted below:

By recording the various attenuation readings for each individual fiber tested over time, it is possible to track network degradation and identify and discrepancies the may be indicative of optic al network intercepts (i.e. fiber taps).

Optical Time Domain Reflectometer (OTDR): An OTDR acts very similar to radar in that i t sends out very precise and measured pulses of light at various wavelengths and then measures t he amount of time it takes to receive the signal back and the intensity of the returning signal. B y tracking both the time and intensity of the returning signal, the OTDR is able to 'trace' the en tire length of the optical circuit-
showing all splices, connectors, and potential intercepts in the trace window. Another key function of an OTDR is its ability to identify the distance to any cable cut or intercept, which greatly e nhances security response times to potential network intrusions. When combined with GIS based in formation, this function becomes increasingly powerful in its ability to hone in on potential securit y breaches and high risk areas.

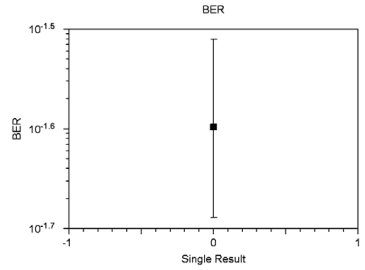
An example of an OTDR trace is shown. By testing and storing the traces from an ORDR, e nd users have the ability to monitor changes in network circuits and identify any potential optical intercepts.

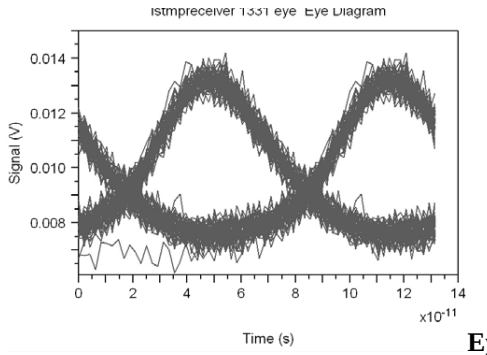
Network integration of detection &prevention capabilities: The different optical test equipme nt options can be integrated into any network architecture. The only questions that have to be add ressed are how intrusive of testing are end users willing to tolerate and how main categories of n etwork testing and monitoring: passive testing and automated monitoring.

Passive testing: Passive testing is the most cost-
effective method of documenting, testing, and monitoring secure networks [2][5] for degradation o f services and possible optical intercepts. This method also provides a great degree of protection d irectly corresponding to the amount of personal resources dedicated to testing optical networks usin g an OTDR or optical Test set. Passive testing is performed by having by having a stand alone OTDR and/or Optical test Set to periodically test and document the optical circuits running betwee n and through secure facilities. Because this testing utilizes stand alone equipment, it offers the m ost cost effective protection with varying degrees of transparency to network operations. Passive tes ting has normally been viewed as very intrusive.

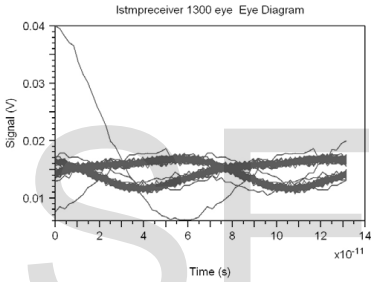
The possible theft for optical power in WDM networks [2] using optical fiber is analyzed by usin g the optical coupler with different transmission coefficients. The resulting Bit error rate [6][7] and Noise margin [6][7] is calculated for the network with different wavelengths at 1330nm and 2000nm. The noise margin is heavy for the higher wavelengths and the tapping increases the syste m bit error rate and is obtained using OPTISIM software[3]. The situation is so worse with the o ptical attenuator with the attenuation to the level of -
2.5dB and the resulting eye patterns and optical power for two different lengths namely 2010m and 210m lengths are plotted.

Bit Error Rate for Fiber of Length of 210m

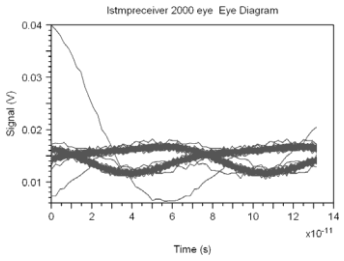




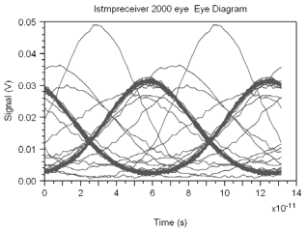
Eye Pattern for Wavelength of 1330nm for Length of 210 m



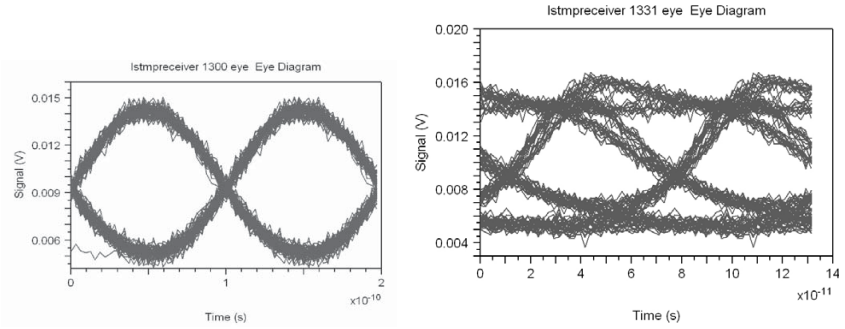
Eye Pattern for Wavelength of 1330nm for Length of 2010m



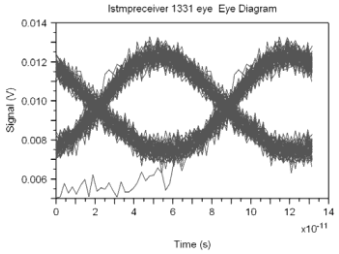
Eye Pattern for Wavelength of 2000nm for Length of 210m



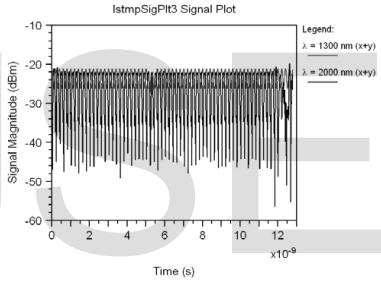
Eye Pattern for Wavelength of 2000nm forLength of 2010m



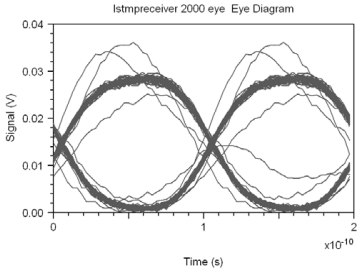
Eye Pattern for Wavelength of 1330nm for Length of 2010m of Transmission Coefficient of 1



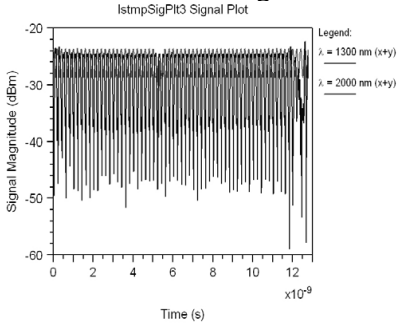
Eye Pattern for Wavelength of 1330nm for Length of 210m fro Transmission Coefficient of 1



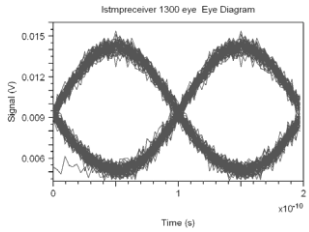
Output Optical Signal Magnitude without Attenuation



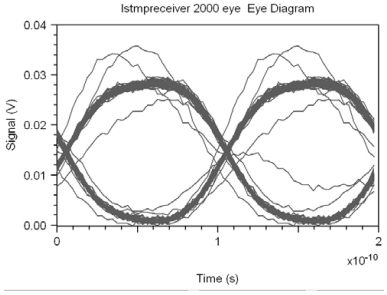
Eye Pattern for Wavelength of 2000nm for Length of 2010m without Attenuation



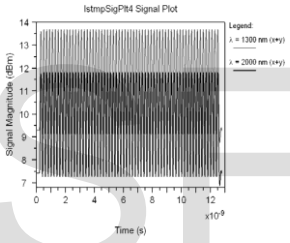
Output Optical Signal Magnitude with Attenuation of -2.5 dB



Eye Pattern for Wavelength of 1330nm for Length of 2010m with Attenuation of -2.5dB



Eye Pattern for Wavelength of 2000nm for Length of 2010m with Attenuation of -2.5dB



Input Optical Signal Magnitude

While fiber optics is exponentially more secure than copper cables, there are still ways that enemies can tap into and intercept classified information traveling across optical networks. A majority of fiber tapping methods require some degree of access to an optical fibers core which not only successfully taps the reliable information but it produces considerable damage to the fibers. As a result of these simulations, it is clear that, the techniques analyzed offer significant advantage in designing cables when it comes to enhancing network security and or monitoring for unauthorized cable access and installation of fiber taps.

REFERENCES:

1. S. K. Sarkar, "Optical Fibre and Fibre Optic Communication System": S. Chand and Company Ltd. (2003).
2. Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for Detection & Prevention Keith Shaneman & Dr. Stuart Gray Coming Inc. Coming, New York MILCOM 2004-2004 IEEE Military Communications Conference.
3. C. Siva Ram Murthy and Mohan Gurusamy, "WDM Optical Networks Concepts, Design, and Algorithms" : Prentice-Hall of India Private Limited (2002).
4. M. Jamshidi, N. Vadiee, and T. J. Rose, Fuzzy Logic and Control: Software and Hardware Applications, PTR Prentice Hall, Englewood Cliffs, New Jersey 07632.

5. [5] Zang Hui, Jue Jason P.,Sahasrabuddhe Laxman, Ramamurthy R. and Mukherjee B., "D ynamic Light path Establishment in Wavelength Routed WDM Networks", *IEEE Communic ation Magazine*, 2001.

[6] Zang Hui, Sahasrabuddhe L., Jue, Jason P., Ramamurthy S. and Mukherjee B., "Connection Management for Wavelen gth-Routed WDM Network", Global Telecommunication Conference- Globecom'99.

[7] Li Ling and Arun, K.Somani, "Dynamic Wavelength Routing using Congestion and Neighborhood Information", IEEE/ ACM Transactions on Networking, 1063-6692(99), 08252-7, 779-786.

[8] Birman Alexander, "Computing Approximate Blocking Probabilities for a Class of all Optical Networks", *IEEE Journa ls on Selected Areas in Communications*, **14**(5), 1996.

v