

Optical Sensing and Signature Analysis of Fiber intrusions

Priyamvada V.C, P.Anguswamy, K.R.Suresh Nair
 NeST Research and Development Centre, Plot #43,
 Cochin Special Economic Zone, Cochin-682030, Kerala, INDIA
 E-mail: suresh@nestcorp.net

Introduction

Lightwave communication through optical fibers was considered to be secure for any type of unauthorized tapping. But it can be seen that this is not true^{1,2} and one can easily tap data by introducing micro bends in the fiber. Thus an intruder who can reach up to a clear-coated communication fiber channel can take the data signal or inject the signal into the fiber. The end user will be quite unaware of the loss of the data since the communication is never interrupted by such attempts due to the normal availability of optical signal budgets. We have developed a new physical layer intrusion prevention system- FiberSentinel SystemTM-that can identify the attempt to tap the data from the singlemode fiber optic transmission channel. The system provides an alternate safe backup channel for the further data transmission whenever it notices an attempt to tap the initial path of communication.

The system is able to take the decision by the real time monitoring of the communication channel optical signal. The guard wavelength passing through the channel is utilized for making the decision to switch over to the backup channel whenever the path is intruded using fiber bend devices like clip-on coupler. A pair of the monitoring devices is provided at each end of the communication channel (Figure 1) to protect the data channels from different types of optical power degradations and attacks. Traditional intrusion detection systems focus on application layer and software-based solutions are provided to identify the unauthorized entry into the communication channels. Such systems usually do not prevent the intrusion attempts on the communication channels. By the development of FiberSentinel System we are providing an effective solution to identify and prevent optical communication channel intrusion attempts. In addition to this the system is able to identify optical events such as optical signal injection, cable breaks, transients, receiver overloads, loss of data signal and low light level at receiver. It reports to the Network operator about the event type that has occurred in the channel and gives alarm to take proper corrective measures.

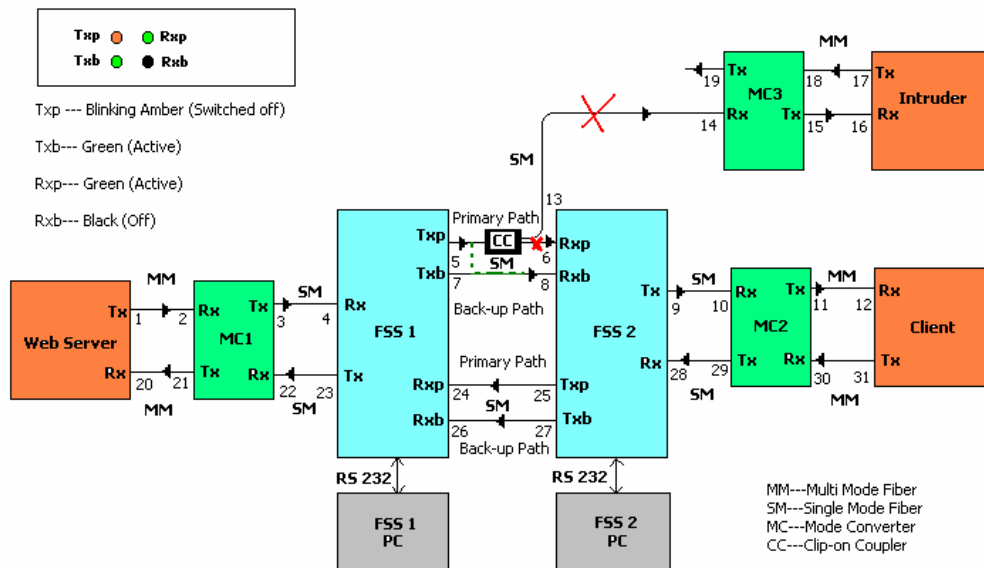


Figure 1: Fiber Sentinel SystemTM monitoring the communication channel

Physical Layer Attacks

The proven method is to bend the fiber^{3, 4,5} slightly and collect the leaked output using an optical slab placed below the bent fiber. Study has been carried out to establish the signature of such intrusions. The experimental results of the type of the power level degradation that occur while such devices are inserted in a communication channel are analyzed to develop an algorithm. This signature-analyzing algorithm effectively identifies and prevents the attempt to intrude an optical communication channel by the real time monitoring of the communication channel.

Traffic analyzing devices are available in the market to test the optical fiber communication channel with out terminating the data transmission. Such devices simply bend the fiber and detect the presence of the signal in the channel. But it has been proved that these devices can be effectively used for tapping the data from the communication channel. One such device is a clip-on coupler. A clip-on coupler can be used for tapping data from a clear-coated optical fiber. These are small, passive devices that bend fiber slightly and press it against an optical block with a refractive index matching gel in between. The collected radiation is channeled through a connectorised single mode optical fiber.

Experimental evidences⁶ are there for the refractive index modulation in the core of the fiber when a periodic microbend is applied on its surface. The periodic thickness variation inturn produces a grating structure inside the core. When the grating spacing satisfies the condition for resonant core-cladding mode coupling, signal flowing through the fiber can be deflected out of the core to the cladding. The phenomenon can also be explained in terms of Frustrated Total Internal Deflection. The direction of the coupled power out of the fiber can also be pre determined by knowing about the grating structure introduced inside the core. Forward coupling is expected in the case of long period grating formation and reverse coupling is in the case of short period grating.

If we place a side polished single mode fiber close to the microbent fiber both immersed in refracitve index matching gell the core power coupled to the cladding can easily be rerouted through the side polished fiber. Even though by this method only (1-2)% of the original power can be tapped, this is sufficient to reproduce the data carried by the signal. Hence the possibility of deliberate attempts to take data out of the fiber cannot be ignored. Devices like clip-on couplers are inducing resonant mode coupling in the transmission channel to extract the modulated optical power out of the communication channel. The same method can also be implemented for injecting fake signals into the optical network systems.

Observations

We have studied the effect of a tapping device on the optical signal transmitted though the communication channel. The optical signal output is sampled at very high frequencies and the time evolution of the signal is recorded. The transmitting fiber is then subjected to different external perturbations and power level change with respect to time is recorded same as in the previous case. For the convenience of the comparison the plots obtained are given with the same reference axes in figure 2.

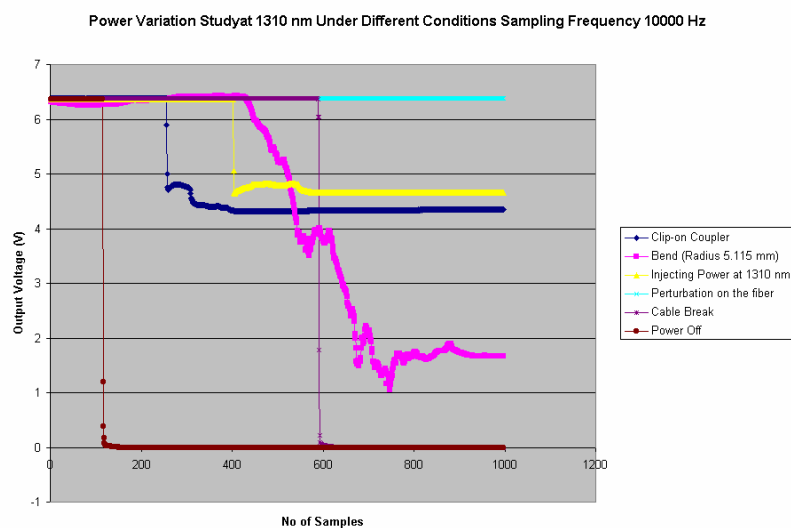


Figure 2: Power Level Variation Under Different Conditions at 1310 nm

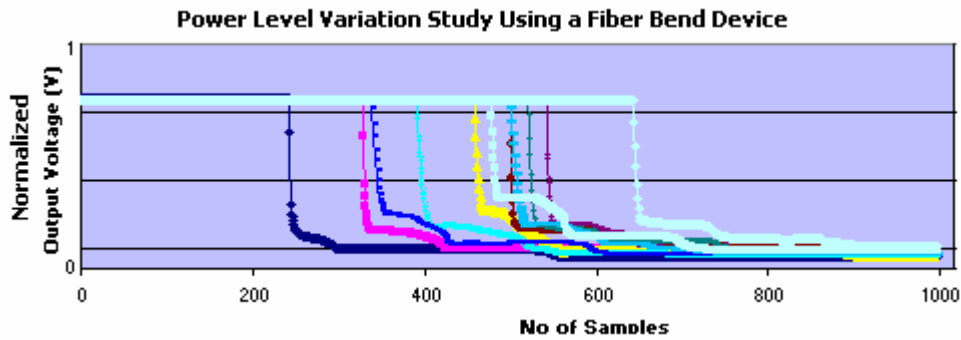


Figure 3: Power Level Variation Study using fiber bend device at 1310 nm

The power level variation with respect to time is found to be repeatable for different types of external perturbation upon the fiber. For example, the fiber bend devices that tap the optical signal always produce a pattern as shown in figure 3. The steady power abruptly drops and then a gradual variation in drop is observed and then again a steady lower power level is reached. Figure 4 shows the typical individual pattern observed by using a clip-on coupler on a transmitting singlemode fiber.

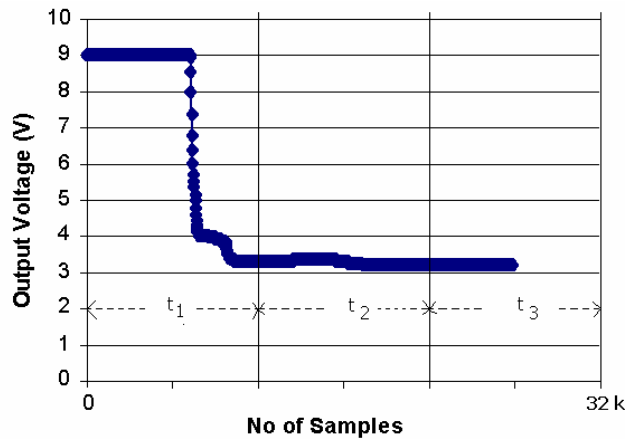


Figure 4: Power level variation in an intruded singlemode fiber output at 1310 nm

Similarly the transmitting fiber is broken and the signature obtained is analyzed. The repeatable pattern observed for this event is as given in figure 5.

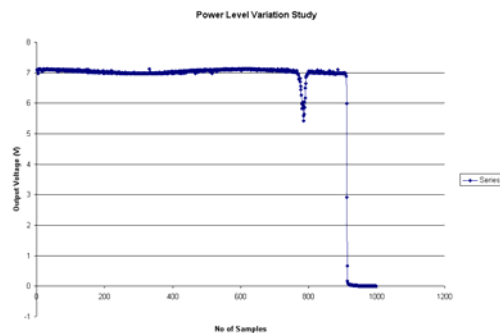


Figure 5: Power drop observed when the singlemode transmission channel is broken

As mentioned in the previous cases, we have collected the experimental data of power fluctuation occurring in a communication channel for numerous different types of external perturbations. The time evolution of the power level variation has been analyzed critically for each event type. We could develop an algorithm based on the

results obtained from the analysis. This algorithm is effectively implemented in the FiberSentinel System, which successfully identifies different event types that occur in a singlemode communication channel, which transmits signal at 1310 nm. We have carried out experiments with 1550 nm also and the observed results (Figure 6) can be directly implemented to protect a communication channel at 1550 nm also.

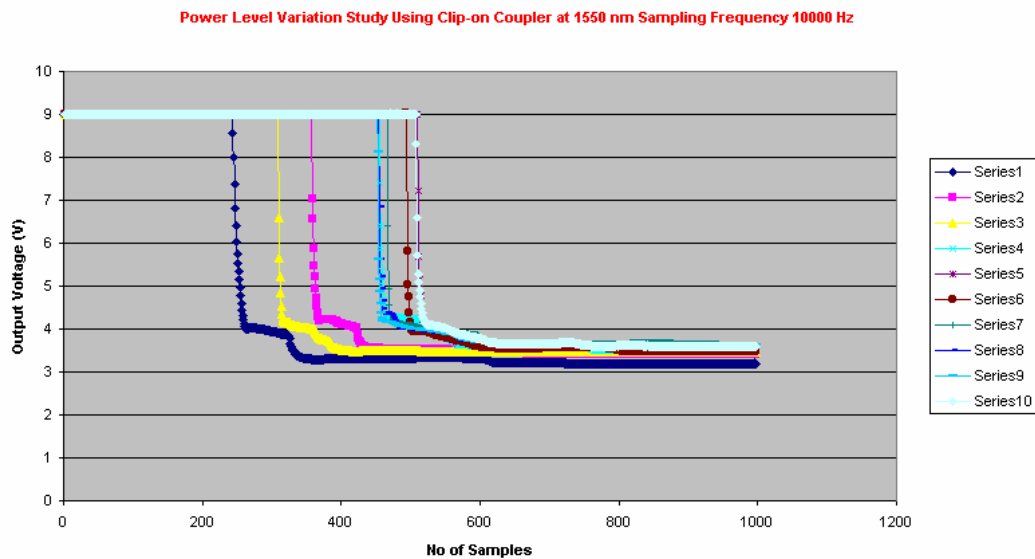


Figure 6: Power Level Variation Study using fiber bend device at 1550 nm

More complicated frequency domain analysis of various types of optical power fluctuation, which is the intended future work, will be powerful enough to identify even a minute external perturbation upon the transmitting fiber. This will help us in developing a distributed vibration sensor that can sense the fiber disturbances by the real time monitoring of the fiber output. The learning network architecture will be an added feature, which will identify exactly the type of perturbation introduced upon the optical fiber.

References

1. M.Medard, D. Marquis, R.A. Barry, S.G. Finn, "Security Issues in All Optical Networks", IEEE Network Magazine, May 1997
2. M.Medard, D. Marquis, R.A. Barry, S.G. Finn, "Physical Security Considerations in All-Optical Networks", SPIE Proceedings, November 1997, Dallas, Texas
3. W. H. G. Horsthuis and J. H. J. Fluitman, The Development of Fiber Optic Microbend Sensors, Sensors and Actuators, 3, 99-110, 1982-83
4. K. Nakamura, T. Yoshino, Nondestructive Optical Fiber Modulation Using Radiation Mode Coupling Phenomena, Journal of Lightwave Technology, Vol.15, No. 2, February 1997
5. L. Faustini, G.Martini, Bend Loss in Singlemode Fibers, Journal of Lightwave Technology, Vol.15, No.4, April 1997
6. Vivek Arya, Kent. A. Murphy, Anbo Wang, Richard. O. Claus, Microbend Losses in Singlemode Optical Fibers: Theoretical and Experimental Investigation, Journal of Lightwave Technology, Vol.13, No.10, October 1995