

Using a Fibre Sentinel System for Physical Layer Security

Dr. Suresh Nair



Plot No.2, Cochin Special Economic Zone

Kochi-682037

Introduction

Information Security has been one of the hot topics in this age of information warfare. While security service providers are developing newer and newer means to protect the data, the hackers on the side are working around tools to attack the protective layer and hack in to the network. The profile of hackers has changed from mere “getting into news” to being economically motivated. There has been several cases of credit card information being stolen, personal details have been compromised and online banking accounts hacked. The application note discusses, the vulnerabilities on optical fibres and how Fibre Sentinel System may be used to protect the optical fibre being used as physical layer. The software configurations needed and typical network architecture is also discussed.

Vulnerabilities over Optical Network

We have often considered optical network as being secure from eaves dropping. But it is well known, by those skilled in this technology that Optical network can easily be compromised. The more evasive methods do not even require a physical intrusion into the light path and hence the detection and prevention of these attacks is much more complex. A relatively simple non interruptive tapping method involves placing bend couplers on the fibre to be tapped. They are inexpensive and commercially available too. Figure 1 shows some of the bend couplers commercially available.



Figure 1

These bend couplers places a controlled bend on an active fibre and a small portion of the optical signal is leaked out. These leaked out optical signal contains valid information which may be decoded by any commercially available sniffer software.

Fibre Sentinel System

If the physical layer is compromised, there are a lot of free and open sources software available to decode the data to useful information. However encrypted the data is, there are ways to decrypt them and the increased computing power of today’s systems has helped it a lot.

Opterna's fibre sentinel system protects the optical line from intrusions of any kind and informs the administrator about the intrusion in real time. Moreover, if configured to use a backup line, the system automatically cuts the compromised optical line and switches to backup. The system can detect and filter eight event types like optical injections, transients, cable breaks, receiver over loads, etc. Please refer to "A white paper on Fibre Sentinel system" by Dr. Suresh Nair, for more detailed description of events. The product is shown in figure 2



Figure 2

Network Architecture

The Fibre Sentinel system operates in full duplex mode as to effectively monitor the Fibre optic network. FSS are inserted in pairs to the existing network that operates in definite wavelength. Depending on the Data Signal wavelength viz, 1310nm and 1550nm, the different variants of Fibre sentinel systems are available. The FSS selection also depends on the mode of the optical fibre, that is multimode or single mode. Figure 3 shows typical network architecture with Fibre sentinel system.

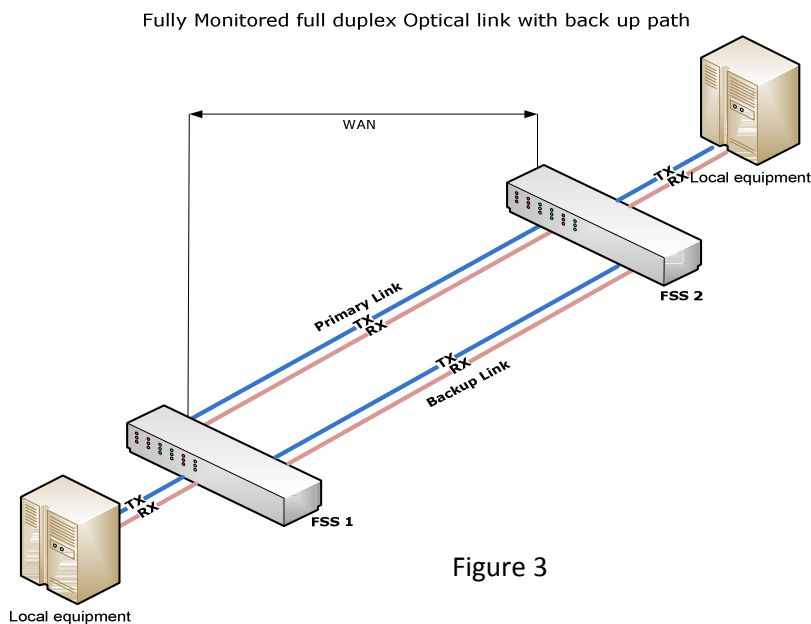


Figure 3

Configuration

The Configuration of Fibre sentinel system is relatively simple. The Sensitivity of the Fibre sentinel system can be adjusted to pre configured values from 1 to 10. The Hyper terminal window is used for the same and the common serial port is available in the front panel of the FSS for the configuration. Moreover, the same settings can be configured on a user friendly window which is discussed later in this chapter. The network parameters like IP, Default FSS names etc may also be configured using the Serial port. Once configured the FSS pairs are ready for use.

Administration of FSS

An SNMP based Event monitoring is available on FSS. The Administrator is informed of the event, using this software tool. The Management may even be done remotely, of course connected to the FSS network by any means.

The screen shot of the Management software is shown in figure 4

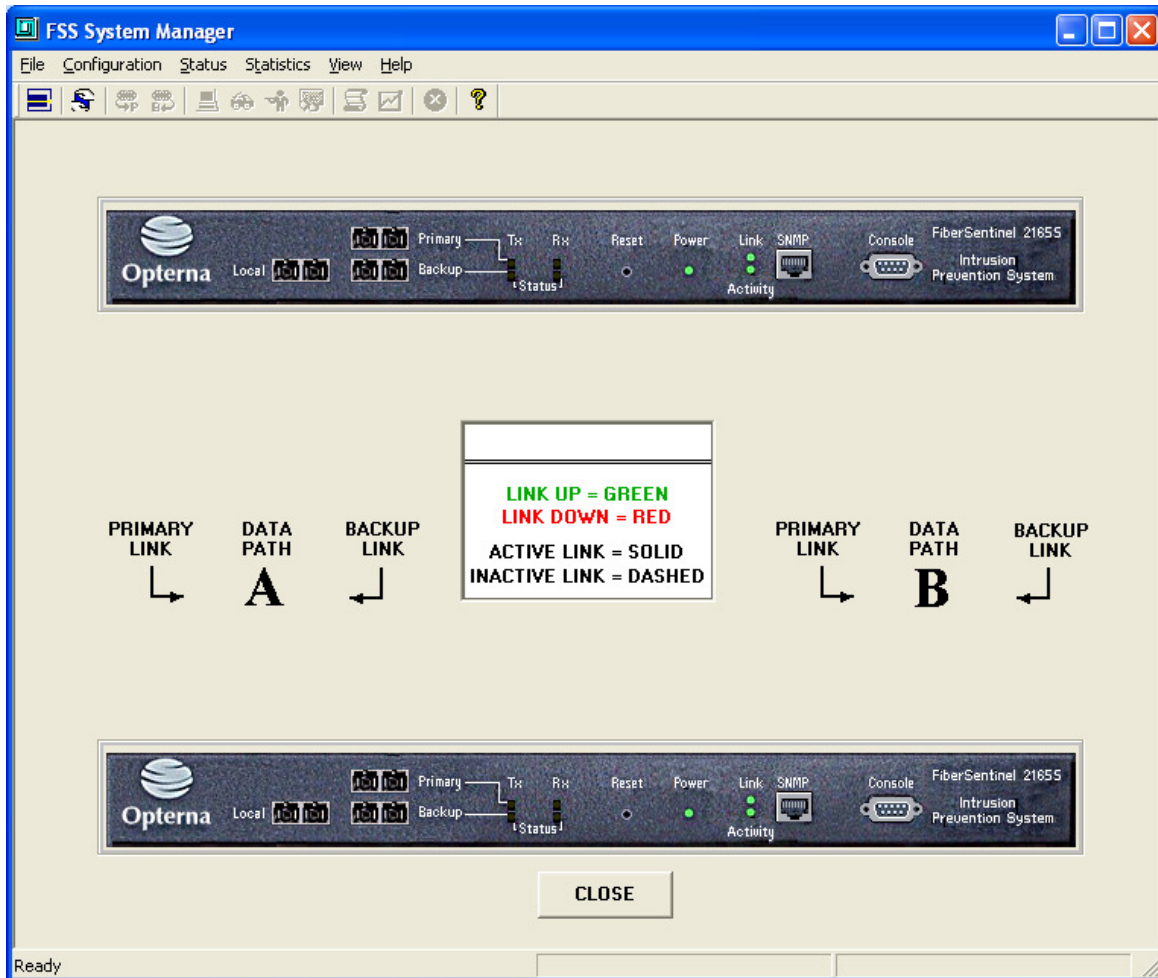


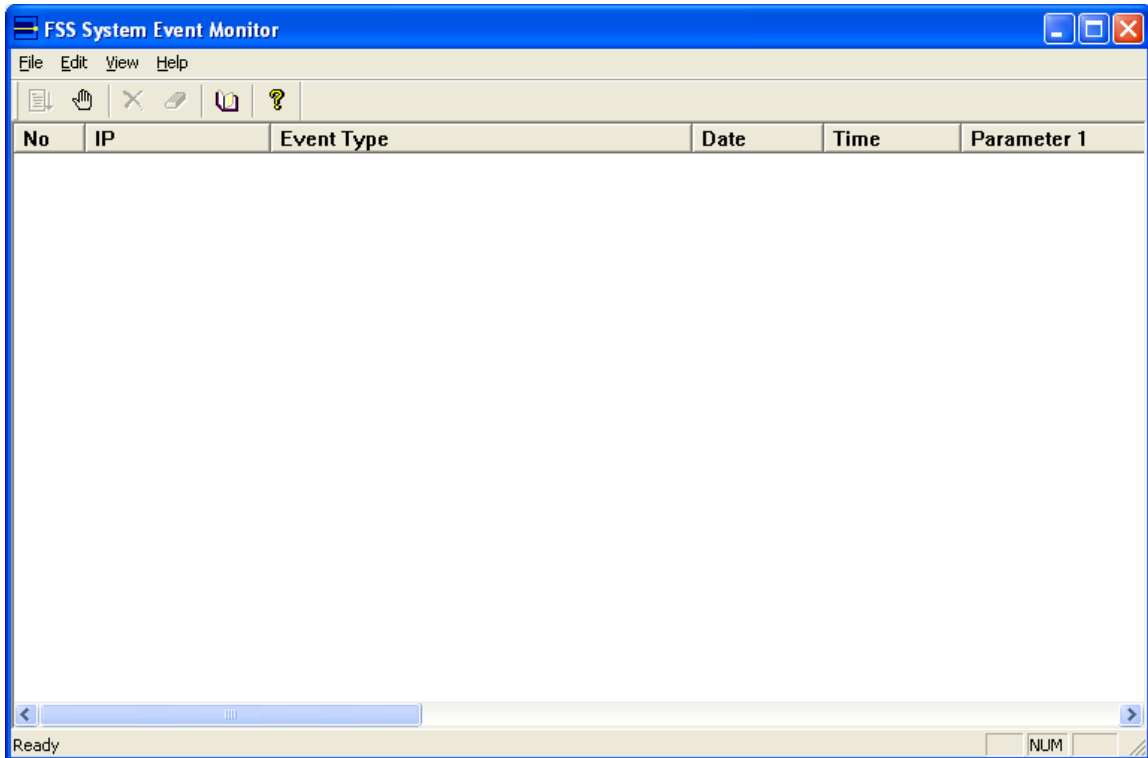
Figure 4

Please refer to the User manual of FSS for more detailed information.

Event Monitor

FSS can detect and categorize eight different events as discussed earlier. An SNMP based event monitor is also available that helps identify the events which may be kept as a log for later use.

A screen shot of the event monitor is shown in figure 5



Technical specifications

Dimensions

Figure 5
19 rack mountable, 1U
17" x 13" x 1.75"

Electrical

Power Input interface

IEC 320, 3 position

Input Voltage

100 – 240V, 60/50Hz

Environmental

Operating Temp

0° C to 55° C (32° F to 130° F)

Storage Temp

-10° C to 65° C (14° F to 150° F)

Humidity (operational)

0% - 90%, non condensing

Humidity (storage)

0% - 95%, non condensing

Diagnostic LEDs

Power status, Tx & Rx status

Primary and backup paths

Link/Activity, Ethernet SNMP Port

General

Operating wavelength

1310nm

Protocols supported

Protocol independent

Insertion loss

1.5dB typical, 2.4dB maximum

Minimum Channel strength

-45dBm

Maximum Channel strength

+5dBm

Monitoring resolution

0.02dB

Intrusion shutdown time

25ms typical

Backup Path switching time

< 4ms

Data channel cable type

singlemode/multimode

Data channel connector type

SC duplex, FC (optional), ST (optional)

Network management

SNMP via Ethernet interface, RS232c console port

Summary

This application note tries to discuss the vulnerability in an optical fibre and how Opterna's Fibre Sentinel system is useful to protect the optical fibre from intrusions. The configuration and Event monitor screen shots of the application is also shown. The technical specifications is also given.

Supplementary Reading and References

1. A white paper on Fibre Sentinel System by Dr. Suresh Nair, Director, NeST Research & Development, Cochin
2. User manual of Fibre Sentinel System
3. Technical Brochure- Fibre Sentinel system
4. A white paper on VoIP Vulnerabilities and the need of physical layer security

About the Author

Dr. Suresh Nair is currently the Chief Technology Officer (CTO), NeST Group, heading the R&D activities including product development. Dr. Suresh is a Gold medallist in M.Tech Micro Electronics with 1st Rank and PhD from Indian Institute of Technology, Bombay. He started his career at Tata Institute of Fundamental Research, and later on, was heading the Optoelectronics Group at SAMEER, Ministry of Information Technology, Government of India. He was instrumental in setting up a Design and Engineering Centre for Integrated Optics at SAMEER with many "first time" planar light wave communication products in the country. Dr. Suresh's expertise in RF & Microwaves and Computer simulations has made him to be the key design member of Indian MST Radar, installed at Tirupati. Dr. Suresh led the NeST team in developing and commercializing various products, The awards, honours and fellowships of Dr. Suresh Nair Include

- *IETE CEOT award for outstanding contribution in Optoelectronics.*
- *Baliga Award for outstanding contributions in Electronics in R&D and industry.*
- *Research Council member of CGCRI, CSIR, Govt of India.*
- *Working Group and Steering committee member in various committees of Ministry of Information Technology, Govt of India.*
- *Member, Board of Studies, Cochin University*
- *Member IEEE*
- *Fellow OSI*
- *Fellow IETE.*
- *Executive Council member of Optical Society of India*
- *85 Papers, 120 Technical Reports and a few patents to his credit, Co-authored a book.*