A novel real-time Remote Fiber Monitoring System

Samuel Varghese, Priyamvada, Majo Mary Mathew, Swarish and Suresh Nair
NeST Research & Development Centre, Plot #43, CSEZ, Cochin, INDIA
E-mail: samuel@nestcorp.net, suresh@nestcorp.net

ABSTRACT
Conventional Remote Fiber Monitoring Systems (RFMS), based on Optical Time Domain Reflectometric (OTDR) technique, perform time-shared probing of multiple fiber paths through optical switching methods. Here any momentary events in a particular path will go undetected, when the system operates elsewhere, which may be an early indication of an upcoming problem. We propose a more efficient, real-time fiber monitoring technique to detect the problems and use of OTDR for the localization of faults, only when an anomaly is detected. The monitoring engine is modified to identify events like optical injection, unauthorized tapping etc. Thus the new system offers a comprehensive real-time security and monitoring package for advanced fiber optic networks.

Keywords: Fiber Monitoring, OTDR, and Intrusion Prevention

Introduction
Integrated network monitoring is essential for today’s converged multi-service fiber optic networks. Remote Fiber Monitoring Systems (RFMS) help to provide zero defect service, to meet the expanding customer expectations on fiber optic network availability. RFMS helps the service providers to maintain the Quality of Service (QoS) while providing services without any intervention and to track the degradations that can lead to eventual failures. RFMS enables easier fiber cable testing and monitoring, through access to the entire fiber cable network from a central location for analysis and troubleshooting. It also helps in providing overall view of the network, resulting from the continuous and dynamic evaluation of network performance. Thus RFMS offers a cost effective operation resulting from the early diagnosis of fiber degradation or fiber faults.

Different methods for monitoring fiber optic links are implemented today. The dark fiber method uses a distinct fiber to monitor the communication’s quality within the cable, based on the assumption that a dark fiber’s quality is representative of the whole cable’s situation. The dark fiber method monitors catastrophic failures that represent between 80% and 90% of the fiber break cases, and therefore does not account for potential loss discrepancies between fibers within the same cable. But, when tests have to be conducted on live fibers – the wavelength chosen for monitoring must be different from the one used for transmission. Here in this work we concentrate on systems compatible for both active and dark fiber monitoring.

Traditional fiber monitoring systems are based on optical time domain reflectometric (OTDR) techniques, in combination with optical switches. These systems do not offer real time monitoring and the time between successive testing depends on the number of fibers to be tested and the rate of switching. Since, the fibers are not continuously monitored, transitory events that occur when the OTDR is connected elsewhere will go undetected, that are often an early warning of a developing problem. More over the life of the testing unit is seriously affected due to the successive switching and due to the continual use of OTDRs. Also the OTDR based systems are not suited for monitoring of branched networks, as in passive optical networks.

Remote Fiber Monitoring System - Architecture
A standard RFMS consists of multiple remote test units (RTUs), each of them having their own monitoring footprints, connected to the RFMS server via LAN connections. RTUs, which acts as the interface between the monitored fiber and RFMS server, do the necessary tests, analyze the events, identify the faults and forward the necessary alarms to the RFMS Server. A macroscopic footprint of a typical RFMS system is shown in figure 1. Typical RTU consists of an OTDR, Optical Switch, passive optical modules for coupling the signal to the fibers and a test system controller, which controls the access to the monitoring fiber. The system controls both the switch and the OTDR to coordinate the delivery of a test signal into the proper fiber for probing the link health. The controller require a control interface, such as a remote GUI, to identify the proper fiber, setup the RTU with appropriate test parameters and access the appropriate
fiber with switch. Finally when an anomaly is detected, the controller must provide notification to the appropriate end. Introducing the monitoring wavelength on a given live fiber involves adding a coupler at the other end of the link and a filter to separate the monitoring wavelength from the communication channel. Typical 2dB to 3dB losses associated with these components necessitate proper budgeting in the system.

To coordinate the RFMS functions, it’s important to have a centralized management. In order to perform the required monitoring, the RFMS must have certain amount of information about the fibers that it is expected to test / monitor and the cables that contain those fibers. Details such as the type of fiber, refractive index, PMD, baseline traces etc are examples of information must have to do monitoring and detect alarm conditions. With greater than one RTU, alarm surveillance centralization is a must, maintaining a common operating configuration at each RTUs, and providing centralized management. The server has a centralized alarm management system complemented with fiber plant and geographic information details such as fiber routes splice points on the route, connector types, landmarks etc.

The RTUs provide the diagnostic capability of fault detection, where OTDR would cycle through each fiber associated with the optical switch and detects a fault. This fault identification is based on the difference between the fiber length measured by the reference trace made at the time the fiber was commissioned and the current measurement. The limitation of this cyclic testing model is obvious: the time for each test multiplied by number of fibers under test is the possible delay before a fault is detected in a particular fiber.

For active fibers, the RFMS need to support a WDM-based access to fibers to introduce an out-of-band OTDR test signal to the fiber so it would not interfere with the service wavelength. This OTDR testing of service fibers can be done to detect degradation, but does still suffer from the delay introduced by the time required for each OTDR measurement and comparison. Active fiber monitoring with high power OTDR signals some times cause noise due to Spontaneous Raman Scattering effects. Strong OTDR signals can deplete the traffic signal amplitude and thus affecting the bit error rate.

Monitoring at 1625nm is preferred because kinks and bends have a greater impact on signals at 1625nm than at 1550nm. Also the out of band 1625nm wavelength window allows the testing on both active and dark fibers and preserves the in band wavelength for maximum bandwidth. The higher sensitivity of the 1625nm wavelength window to losses resulting from bends, H₂ and OH⁻ absorption, and its lower sensitivity to core axis misalignment puts the monitoring at these higher wavelengths on a safer side. A signal at 1625nm is almost not affected by its passage through an active EDFA and the low attenuation level in an EDFA (0.1 dB/m) allows the signal to pass through faulty or inactive EDFAs.
Real-time remote fiber-monitoring engine

An ideal solution for dark and active fiber monitoring is to monitor each fiber individually, providing a continuous monitoring of the fibers, for a change in optical signal power. A generic RFMS architecture that includes this power monitoring capability is shown in Figure 2. Power monitoring detects a loss of optical signal; the OTDR is then activated (with the help of a WDM and the optical switch) to measure the distance to an actual fiber fault. For active fibers, we use an out-of-band signal power detection or modulated power detection and for dark fibers, a dedicated power monitoring at suitable wavelength. A low power indication derived from a threshold violation may be the first indication of a problem and alarm is routed for immediate action. In the case of a transitory situation where the threshold violation is not persistent is logged on and is thoroughly investigated. The new design of monitoring provides accessibility to both ends of the monitored section of the fiber plant. The origin and termination of the monitoring section of fiber, at the same location allows bi-directional probing and could judge the events more logically. The monitoring wavelength is routed over the monitoring path with special passive optical modules. The use of special passive bypass modules at repeater or node points, make the next segment of the link visible for tracing and also helps to maximise the monitoring footprint of each RTUs. This practice of guiding the monitoring wavelength enables the monitoring of any type of network in an efficient way.

The beauty of the new configuration lies in its monitoring adaptability for any network topologies such as ring, star or bus. This makes this monitoring suitable for passive optical networks, which is basically a branched network. Also, in the new RFMS architecture, the risk of degradation of transmission quality from the launch of high power OTDR signal is greatly reduced. The designed system covers a monitoring distance upto 90 km, with a single monitoring path, and the maximum attenuation in the path is of the order of 25 dB. Eight such monitoring units are integrated in a single RTU. The OTDR is integrated to identify the location of fault, which is activated once an anomaly is detected. The monitoring paths associated with each RTU can be up to 64 or 128, depending on the number of fibers to be monitored.

It is to be noted that a simple power monitoring is not sufficient to identify and predict the nature of optical events happening on the fiber link. It is proved that with conventional network test equipments such as clip on couplers can be used to tap the information on fiber optic link with out the knowledge of the service provider. Conventional remote fiber monitoring systems are not designed to detect such intrusion attempts and do not provide successive preventive alarms. An intelligent hacker may not simply tap the light, but also inject the same amount of light – active tapping. It is possible to identify the presence of such tapping through an intelligent power level signature analysis. Monitoring is done based on moving power level baselines to keep real time tracking to predict the events correctly. We have modified the RFMS monitoring engine to take care of such minute power level changes of the order of less than 0.01dB, to track any intrusion attempts. This intelligent engine can identify events such as cable breaks, unauthorized tapping, optical injection, optical transients etc.

We recommend the use of OTDR at 1625nm for RTUs. The RTU sensitivity to different optical events is better than 0.01dB. This type of monitoring systems helps us in instantaneous detection of events including any unauthorized access, optical transients, cable breaks and long term performance degradation. The dual functionality with OTDR and real time power monitoring offers the most reliable fiber monitoring system. Optical Spectrum Analyzer (OSA) included to RFMS engine can monitor the health of each DWDM channels.

To control the cost effectiveness of the RFMS system, RTU location is optimized to extend the coverage of monitoring footprints. The fibers paths are looped in a logical manner to traverse maximum distance with a single monitoring path, using special modules, which helps in controlling the required number of RTUs.

<table>
<thead>
<tr>
<th>Features</th>
<th>Old Method</th>
<th>New Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Technique</td>
<td>OTDR based</td>
<td>Intelligent power monitoring and supported with OTDR</td>
</tr>
<tr>
<td>PON Adaptability</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Intrusion Detection &amp; Intelligent Optical Event Analysis</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 1: Comparison of the new method and conventional method
Conclusion

In this paper we propose a new monitoring system, which is a comprehensive solution for both active and dark fiber monitoring as well as for the identification of any intrusion attempts on fiber links. This is achieved through dedicated intelligent power monitoring, where the RTUS are optimized for their location and its monitoring footprints. The events are analyzed in a real-time manner and are constantly tracked in time with reference to moving baselines for detecting the optical events. The variation in the power level is interpreted for identifying various optical events in the physical layer as well as for long-term degradation. The dual functionality with OTDR and real time power monitoring offers the most reliable fiber monitoring system.

References

Acknowledgement

The authors would like to thank Mr. N. Jehangir (Managing Director, NeST) & Mr. U. M. Shafi (Sr. Vice President, NeST) for their support and encouragements.