OPTICAL NETWORK SECURITY: TECHNICAL ANALYSIS OF FIBER TAPPING MECHANISMS AND METHODS FOR DETECTION & PREVENTION

By

Keith Shaneman & Dr. Stuart Gray
Corning Inc.
Corning, New York

ABSTRACT

Increasing emphasis on reliable data transmission for homeland security and network-centric operations makes secure communications a critical component of national security. While fiber optic cables are immune to typical EMI/RFI issues associated with TEMPEST-related compromising emanations, it is possible to successfully intercept an optical signal if risk areas are not understood and if detection and/or prevention mechanisms are not actively integrated into network management practices.

There are several ways to 'tap' into an optical fiber including fiber bending, splitting, evanescent coupling, scattering, and V-grooves. Many of these techniques would require the use of cumbersome and sophisticated equipment to alter the physical characteristics of the fiber in the field with a significant risk of damaging or breaking the fiber and having the optical intercept be detected by the end user. Out of all the techniques, the bent fiber tap is the most easily deployed to couple light out of the fiber with minimal risk of damage or detection. This paper will focus on quantifying the bend loss required to successfully tap a signal propagating in a single mode fiber and analyzing the properties of the bend that could be used to detect that a bent fiber tap is occurring.

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 optical amplifiers with embedded tamper detection features and enhanced optical time domain reflectometer applications for localization of suspected tapping events. These monitoring techniques will be reviewed with detailed analysis of each method's effectiveness in detecting bent fiber taps and cost-effectiveness for integration into optical networks.

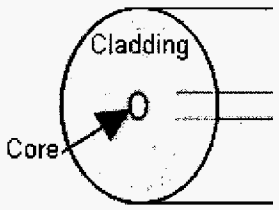
SECURITY OF OPTICAL FIBER

For decades, Compromising Emanations (CE) of copper cabling and equipment has been a major threat to the secure transmission of National Security Information over data networks. In order to mitigate this threat and comply with TEMPEST regulations, the Committee on National Security Systems has established specific physical installation guidelines to protect sensitive information from being compromised intentionally or unintentionally through CE. Since copper cables are very susceptible to electromagnetic and radio-frequency interference, they must be installed maintaining strict separation guidelines by classification, and be encased by electro-magnetic tubing (EMT) to control CEs and provide physical deterrence and protection from intruders.

In contrast, fiber optical cables are not susceptible to electromagnetic and radio-frequency interference and produce no compromising emanations since the signal being transmitted is optical instead of electrical. However, depending on the installation and regional threat-level, often fiber optic cables are still installed inside of EMT to provide greater physical deterrence and protection of the secure infrastructure.

FIBER TAPPING OVERVIEW

While fiber optic cables are exponentially more secure than comparable copper cables, it is still possible to intercept the optical signals being transmitted across a network. However, all forms of fiber tapping and optical intercepts involve accessing the fibers contained within an optical cable. In order to understand the various methods to intercept optical signals, it is important to first understand how optical fiber and cable is constructed.



Optical fiber contains two primary components: the core and cladding. The core of the optical fiber is the area in which light is carried from one end of the network to the other. The cladding protects the core of the fiber, and creates a boundary layer along the outer edge of the core that allows the light to reflect inside of the core - resulting in very little loss or attenuation as the optical signal is transmitted over long

0-7803-8847-X/04/$20.00 ©2004 IEEE

distances and creating a condition called 'Total Internal Reflection.'

In order for an optical signal to be tapped or intercepted, the core of the fiber carrying the traffic must be compromised or 'tapped.' In order to access the core of a fiber, an intruder must first physically access the fibers within the optical cable.

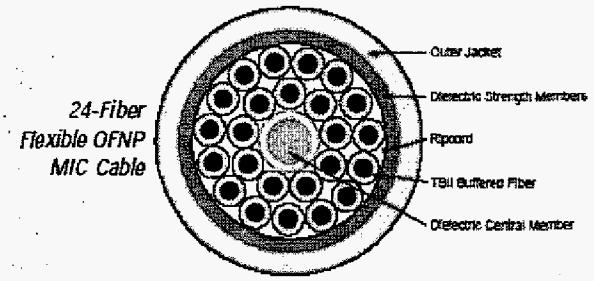


Figure 1. Optical Cable Cross-Section

The figure above depicts a standard indoor, dielectric cable with 24-fibers. In order to access the fibers, an intruder would have to either access a terminated end of the cable where the fibers are exposed (usually inside of a Controlled Access Area and/or Red Equipment Area) or gain mid-span access to the cable. While accessing the terminated ends of a fiber would be preferred, this is also the area with the highest degree of security and personnel scrutiny; so mid-span access to a cable is a more likely threat. To perform a 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 individual fibers in the center 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 field. It involves stripping an individual fiber down to the cladding and bending it to compromise the Total Internal Reflection and allowing a fraction of the optical signal to be coupled out. The power of the tapped signal will depend upon the radius (R) and angle (θ) of the bend.

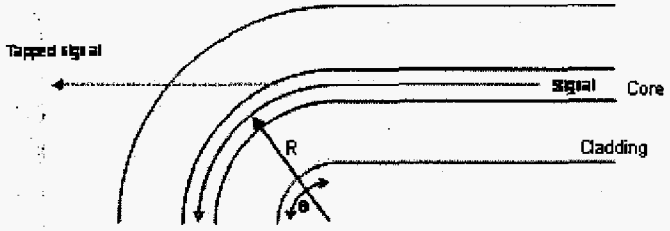


Figure 2. Fiber Bend Tap Mechanics

The goal of an intruder would be to use the minimum bend loss required to tap a discernable 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 Security 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 testing.

*2) **Optical Splitting:*** An optical splitter works very much in the same manner as a coax splitter for televisions - it 'splits' a single optical signal into two identical signals. However, in order for the device to be installed, the target fiber must be cut and both ends spliced onto the optical splitter. Once the fibers are accessed within the cable, the splicing of the fibers onto the optical splitter could take as little 2-3 minutes depending on the splicing method used.

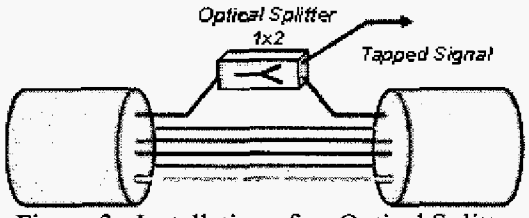


Figure 3. Installation of an Optical Splitter

The biggest drawback to using an optical splitter is that the installation of such a device will cause an interruption of service which should result in a security response exposing the sytem breach. The loss of the splitter will not necessarily be high. If the splitter is installed in a part of the system where the optical power in the fiber is relatively high it may only be necessary to tap a few percent of the signal with less than 1 dB loss. A lossless splitter could be used to over come this loss if desired but then the optical splitter requires a source of power—making it even more noticeable during visual inspections.

*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 1x2 optical splitter rather than using a pre-manufactured device. By polishing the cladding very close to the fiber core 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 than a human

hair and the core size of singlemode fiber is less than an eighth of a 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.

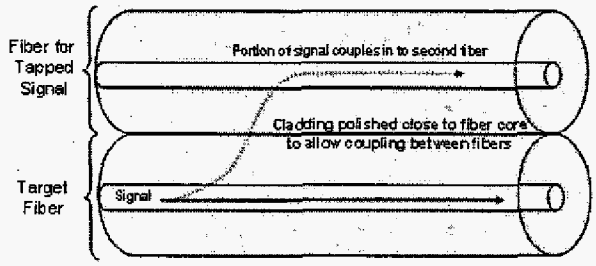


Figure 4. Evanescent Coupling

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 between the signal propagating in the fiber and the face of the V-groove is greater than the critical angle for total internal reflection. When this 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.

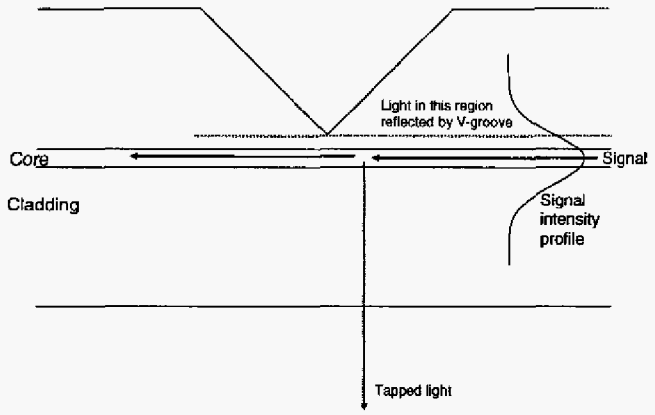


Figure 5. V-Groove Cut Cross-Section

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, since this process requires actually cutting into (but not breaking) an optical fiber, it is also the riskiest method for achieving a fiber tap in the field.

5) Scattering: The use of a Fiber Bragg Grating to achieve a fiber tap is the most advanced field technique discussed, and also 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 interfering field of UV rays that subsequently 'etches' a Bragg Grating onto the fiber core. The grating then reflects a portion of the optical signal out of the target fiber into a capture fiber.

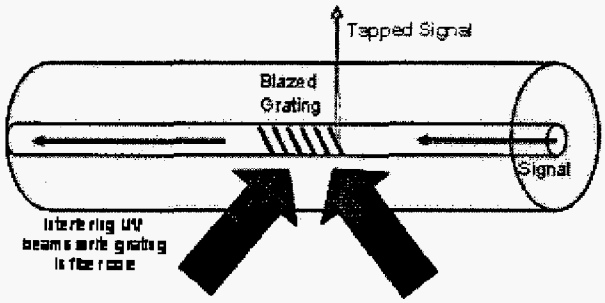


Figure 6. Scattering through a Fiber Bragg Grating

The benefit of the Scattering approach is that it does not require cutting into a fiber (such as in a V-Groove tap). However, this method requires the most precision equipment of any and is the most difficult to implement in a field environment without detection.

Note: Each of the methods discussed above depict 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.

DETECTION OF OPTICAL INTERCEPTS

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 processes to prevent and/or detect such intrusions. All of the fiber tap methods listed above would result in some measurable change that could be detected using standard optical test equipment. An optical test set, which measures optical attenuation (dB), and an Optical Time Domain Reflectometer, which measures reflective and non-reflective 'events' in an optical circuit, are very effective tools for network testing and monitoring. The remainder of this paper will focus on (1) the capabilities of each of these tools, (2) their ability to detect each of the various fiber tap methods discussed, and (3) the various methods in which they could be integrated into a optical network architecture to facilitate periodic network testing.

Optical Tester: Optical Testers have been used since the early deployment of fiber optic networks to measure the amount of attenuation (dB) or optical loss of the network. Optical testers consist of an optical source, which generates a very precise amount of optical signal at various wavelengths, and an optical meter, which is calibrated for precise measurement of the optical signal

received. 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:

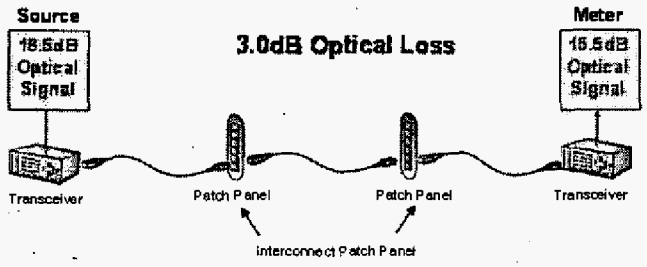


Figure 7. Calculating Optical Loss (dB)

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

Optical Time Domain Reflectometer (OTDR): An OTDR acts very similar to radar in that it sends out very precise and measured pulses of light at various wavelengths and then measures the amount of time it takes to receive the signal back and the intensity of the returning signal. By tracking both the time and intensity of the returning signal, the OTDR is able to 'trace' the entire 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 enhances security response times to potential network intrusions. When combined with GIS-based information, this function becomes increasingly powerful in its ability to hone in on potential security breaches and high-risk areas.

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

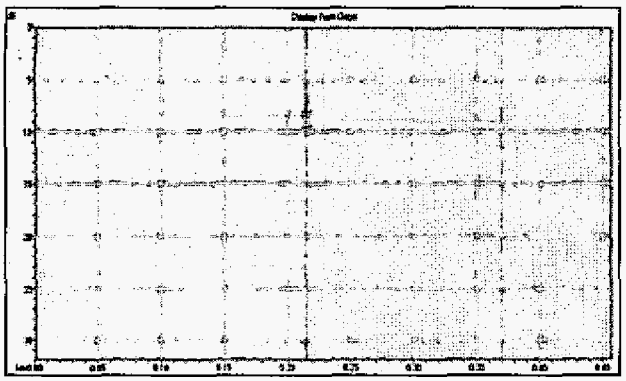
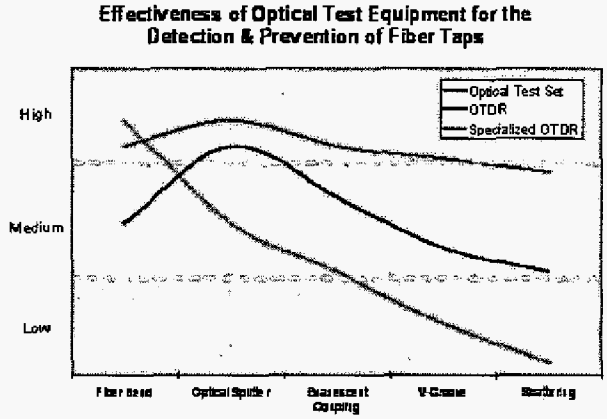


Figure 8. Sample OTDR Trace

TESTING EFFECTIVENESS VS. FIBER TAPS

Since the Optical Test Set and the OTDR perform very differently, they each have varying degrees of effectiveness in detecting and preventing optical intercepts. The chart below provides a relative depiction of each tools' effectiveness in identifying the various fiber tap methods discussed. The Optical Tester provides fairly good detection capabilities for those fiber tap methods that are 'easy' to implement in the field. However, it is relatively weak in detecting the more advanced fiber taps. The OTDR, however, provides strong-to-moderate detection capabilities across the board because of its ability to identify discrete loss points, possibly corresponding to a tap, along a fiber link. Finally, specialized OTDRs, such as Brillouin-OTDR and polarization-OTDR, are available which test for birefringence, stress and other optical deformities caused by all forms of fiber taps. The specialized OTDRs provided the best detection capability across all fiber tap methods.



.Figure 9. Detection Effectiveness of Test Equipment

LAB EXPERIMENT: MEASURING IMPACT OF OPTICAL CABLE TYPE ON ABILITY TO DETECT FIBER TAPS

In addition to the various types of OTDR equipment that offer varying degrees of effectiveness in detecting fiber taps, there are also different cable designs that could enhance the detection of fiber taps as well. Optical cable types can be broken down into three primary catagories: loose-tube, tight-buffered, or ribbon construction.

Loose-tube cables are comprised of a circular arrangement of individual buffer tubes – each containing up to twelve 250um optical fibers. This composition is typically found in OSP deployments and is also

predominantly used by Department of Defense and Federal agrencies in their LAN/WAN deployments.

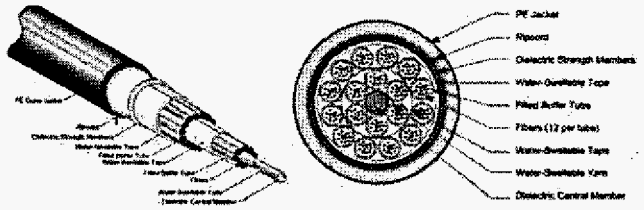


Figure 10: Loose-Tube Cable Design

Tight-buffered cables are comprised of a circular arrangement of individual 900um buffered fibers. This composition is predominatly used by Department of Defense and fecderal agencies in LAN deployments – mostly inside of buildings.

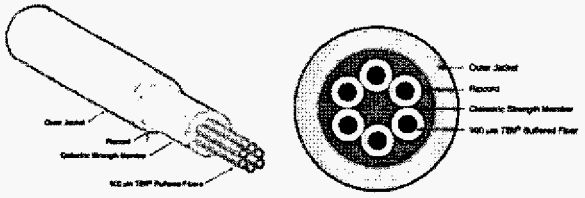


Figure 11: Tight-buffered Cable Design

Ribbon cables are comprised of a single or multiple 'stacks' of ribbons – which are comprised of 12 optical fibers encapsulated at precise intervals in a ribbon matrix. Ribbon cables are used heavily by telco and CATV companies for OSP deployments to (1) reduce deployment cost and complexity, and (2) accelerate network restoration activities. To date, ribbon cables have not been widely used by the Department of Defense despite wide-scale deployment in the commercial sector.

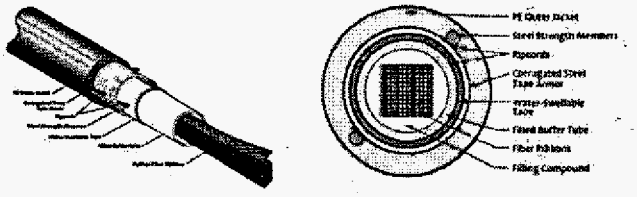


Figure 12: Ribbon Cable Design

In order to evaluate the impact that cable design has on fiber tap dectectability, a side-by-side experiment was conducted on each cable type. The experiment used a standard OTDR to quantify any attenuation change that could be detected on singlemode fiber at 1550nm while (1) a mid-span sheath access was performed on each cable, (2) an individual fiber was accessed from within a buffer tube or ribbon matrix, and (3) the fiber was stripped in preparation for a fiber tap.

As the chart below depicts, the only cable design that provided any enhanced detectability of suspect fiber tap activity was the ribbon cable. Neither the loose-tube or tight-buffered cable designs provided any advantage for network security or monitoring. In fact, the only significant attenuation change that was detected during the experiment for loose-tube cables was when a technician mistakenly crimped the buffer tube he was trying to access fibers in.

	Mid-Span Sheath Access	Fiber Isolation	Fiber Stripping
Loose-Tube Cable	None	Low	None
Tight-Buffered Cable	None	None	None
Ribbon Cable	None	High	None

Figure 13: Fiber-Tap Experiment Results

Because ribbon cables encapsulate 12 individual optical fibers inside a ribbon matrix, the ribbon matrix must be removed prior to an individual fiber being accessed in preparation for a fiber tap. It is during the removal of the ribbon matrix that a significant attenuation change can be detected as noted by the OTDR trace overlay shown below:

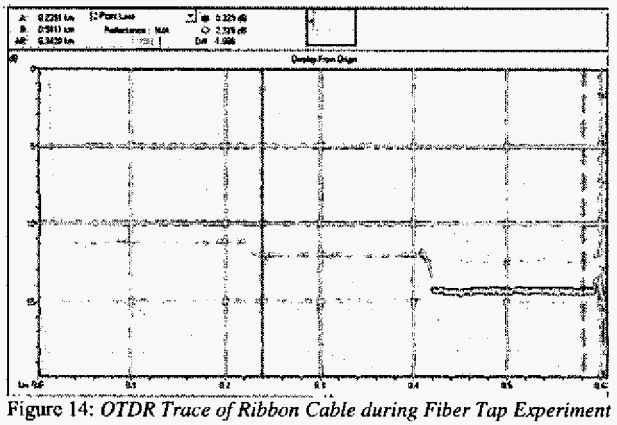


Figure 14: *OTDR Trace of Ribbon Cable during Fiber Tap Experiment*

The top line (orange) on the trace shows the baseline trace of the ribbon cable prior to the experiment beginning. The bottom line (yellow) shows the 2.2dB attenuation change that was detected when the technician tried to separate an individual fiber out of the ribbon matrix using a ribbon splitter tool.

In comparison, the chart below shows the undetectable change in attenuation that was measured while accessing a single fiber in a loose-tube cable:

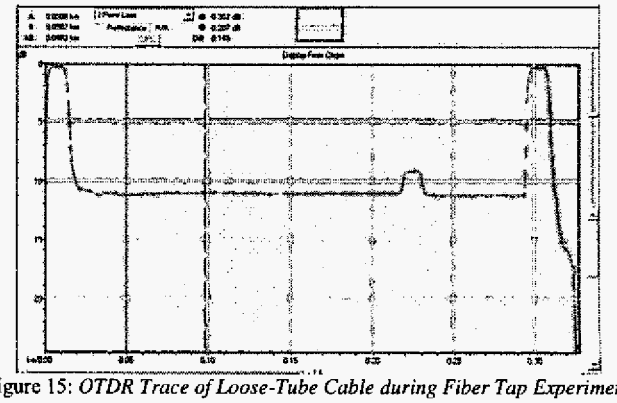


Figure 15: *OTDR Trace of Loose-Tube Cable during Fiber Tap Experiment*

As a result of this experiment, it is clear that ribbon cables offer a significant advantage over other cable designs when it comes to enhancing network security and/or monitoring for unautorized cable access and installation of fiber taps.

NETWORK INTEGRATION OF DETECTION & PREVENTION CAPABILITIES

The different optical test equipment options can be integrated into any network architecture. The only questions that have to be addressed are how intrusive of testing are end users willing to tolerate and how much the resulting solution will cost. There are two main categories of network 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 for degradation of service and possible optical intercepts. This method also provides a degree of protection *directly* corresponding to the amount of personnel resources dedicated to testing optical networks using an OTDR or Optical Test Set. Passive testing is performed by having a stand-alone OTDR and/or Optical Test Set to periodically test and document the optical circuits running between and through secure facilities. Because this testing utilizes stand-alone equipment, it offers the most cost-effective protection with varying degrees of transparency to network operations. Passive testing has normally been viewed as very intrusive to network operations in that it required each network circuit to be dark and disconnected from the switch in order to facilitate testing. While this approach is still valid today, it does create a great deal of complexity that has to be managed and is not recommended. A better approach to Passive Testing is the integration of passive test points into Red and Black Equipment areas. These test points are continuously linked to the optical circuits and provide ready access to the lit circuits without disrupting service or requiring the circuit to be disconnected from the switch. By utilizing different wavelengths for testing, an OTDR or Optical test Set can test a fiber while it is still in operation. This alleviates the concern with taking a network down for testing and enables Network testing and Monitoring to be more random and not as forecasted or predictable.

Automated Monitoring: To achieve a more proactive and automated approach to Network Testing and Monitoring, test equipment can be directly integrated into the network architecture and combined with an optical switch to allow a single set of test equipment to be connected to multiple optical circuits in the facility. Due to the increased equipment requirements and the need for an optical switch, the Automated Monitoring approach is very costly—but is the only approach that can automatically monitor network performance and highlight any potential optical intercepts / fiber taps. Unfortunately, many equipment vendors have bundled this capability with other capabilities that may be extraneous to the management of secure optical networks.

The highest level of security can only be achieved by continuous monitoring of the network. This could be achieved by propagating several wavelength channels dedicated to monitoring the security of a system alongside data carrying channels in a way analagous to the optical supervisory channels (OSC) in DWDM systems. For example, the loss of the bent fiber tap described above exhibits a strong wavelength dependence. The power ratio of two well separated wavelengths propagating in the fiber would change dramatically if a bent fiber tap was suddenly placed in the link. Continuous monitoring of this ratio would immediately show that a tap was occuring and could instruct the netwrk management system to shut down the link or re-route the data.

CONCLUSION

While fiber optics are 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 fiber's core which is challenging if not impossible to discretely accomplish in the field. Regardless of the method used, fiber taps and optical intercepts can be detected by using standard optical test equipment such as an OTDR or Optical Test Set. Detection of fiber taps can also be greatly enhanced by the use of ribbon cables instead of loose-tibe or tight-buffered cables. Depending on the threat level or degree of protection desired, network monitoring and testing can either be either passive using stand-alone test equipment or automated using an integrated network monitoring capability. Regardless of the approach taken, network monitoring and testing has to be an integral component of network management to prevent and detect optical intercepts before they result in the compromise of National Security Information .