Global Information Assurance Certification Paper

Securing Optical Networks

Adria Crum
GIAC Level 1 Security Essentials Practical
NS2000 Monterey, CA Oct 20-22,2000

What is an all-optical or photonic network?

The quest for greater bandwidth has led to the birth of the All-Optical Network. An all-optical or photonic network has the function of a traditional communications network but is run with various optical components. Optical transmitters and receivers or IR (infrared) transmissions take the place of conventional fiber cables. Optical signals are transmitted through the air and are converted to electrical signals and back to transmit data and the diagnose network integrity.

Why would you want to have an optical network? There are many benefits as: increased bandwidth since photons move faster than electricity, up to and beyond gigabit speeds, there are shorter transmission delays making data sharing and real time calculations quicker, the thousands of signals can be compressed into a single beam by using frequency division multiplexing, and a single strand of fiber, if needed can carry several wavelengths embedded into one beam by means of wavelength division multiplexing, which makes the network flexible. Several streams of data can be contained in one beam. Efficiency and speed also help give this network less packet loss.

There are two types of commercially offered all-optical network functions: wavelength division multiplexing and time division multiplexing. Wavelength division multiplexing currently has more of a commercial appeal though time division multiplexing has great speed.

Types of All-Optical Network Functions

Function #1:
WDM – Wavelength Division Multiplexing
Multiple channels of network traffic are separated it's own wavelength.

Function #2
TDM – Time Division Multiplexing
Multiple channels of network traffic are separated into its own time slot. It gives the network bandwidth on demand.

Hardware Components

The following are various components that make up an optical network. The components can vary per network design, purpose and technological innovation.

Cabling Fiber – single or multi mode
A cable made out of shielded glass and used to transport signals.
Optical receivers
It is hardware that receives the optical signal. It can either be a relay or at a customer site.
Optical transmitters
It is hardware that transmits the optical signal.
Spatial switch
Lets a signal pass through or drop out and can switch signals between fibers.
Optical Amplifier
Acts as a signal booster or repeater to increase signal strength.
Multiplexer
Combines signal from many fibers into one fiber.
Demultiplexer
Separates many signals from one fiber into one signal per fiber (many fibers).
Splitter
Split one signal into more than one signal.
Combiner
Combines many signals in to one single signal.

Methods of Attacks

Physical security, data integrity and data availability are important to any network. An attacker can use different methods of breaking into a network. Below are a few methods and examples of attacks.

Data Delay

All-optical networks are immune to this type of attack where the attacker would intercept and either divert or delay data due to the lack of optical memory.

Denial of Service & QoS Degradation

Denial of Service attacks are when an attacker affects the network availability.
Quality of Service attacks are when an attacker threatens network integrity.
Both of these attacks are a type of service disruption of which optical networks are prone. Tightening up the network topology and cryptography are two methods that can be used against those attacks.

Traffic Analysis & Eavesdropping

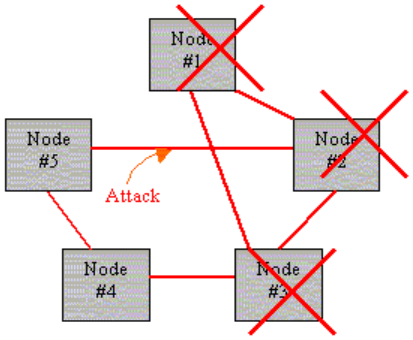
Traffic analysis is when an attacker collects communication patterns, not content from a network.
Eavesdropping is when the content of the traffic is collected and scanned by the attacker.

Spoofing

Spoofing attacks are not feasible in an all-optical network if encryption methods are used. Pretending to be a trusted entity in this case would be difficult if not impossible without intimate knowledge of the network.

In Band Jamming

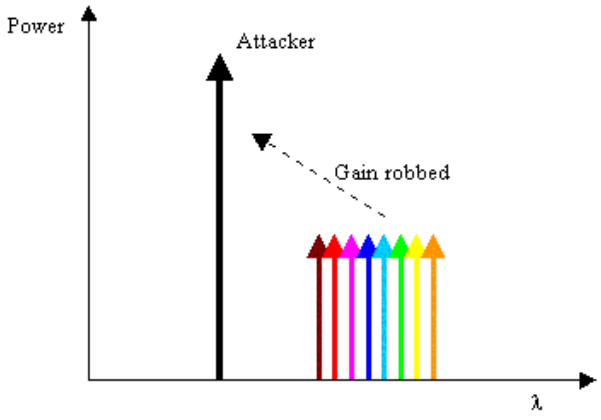
In band jamming is a type of denial of service attack, where the attacker inserts a signal into your in order to disrupt the receivers ability to process the signal correctly. If an attacker were to use a single high powered signal on a specific optical link. It could damage that optical link. If redundancy of the network were employed, or blocking or filtering of that signal were used this would not be an issue.



picture from Kaius Nevaste ,"Optical Network Security"

Out-of-Jamming

Out of band Jamming is also a type of denial of service attack, where the attacker diminishes the transmission or flow of a signal by exploiting components with crosstalk leaks or cross modulation effects. If an attacker were to introduce another signal at a different wavelength than the network the optical amplifier will accept the signal unless it were filtered out. Since the Optical amplifier cannot distinguish between a legitimate signal and an attack signal the attack can be successful.
Those photons provided by the attacker can rob the gain available to the signal and allow it to propagate to other nodes on the network.



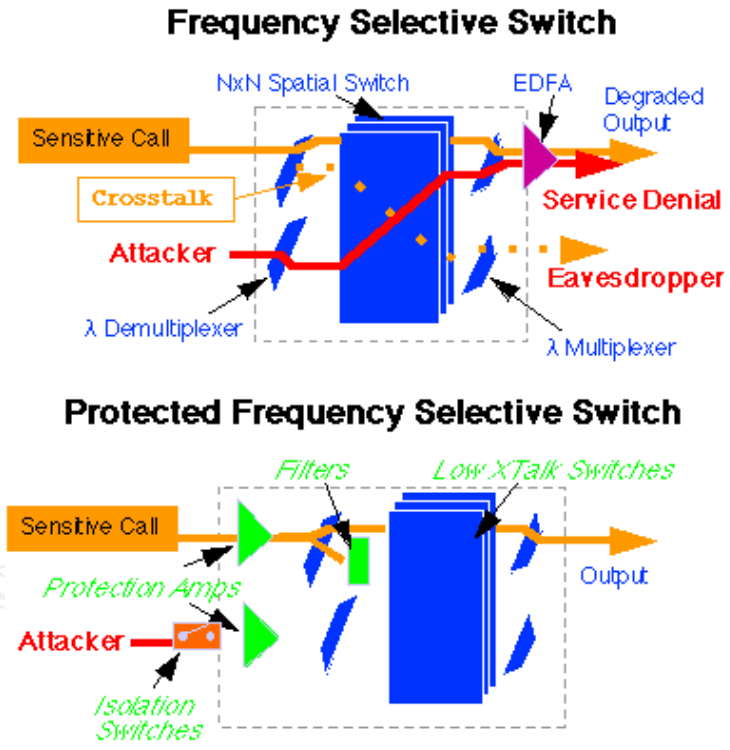
picture from Kaius Nevaste ,"Optical Network Security"

Unauthorized Observation

Unauthorized observation is a form of eavesdropping where the attacker listens to the crosstalk leaking from an adjacent signal through a shared resource. The attacker can gain information helpful to breach the network. Demultiplexer can exhibit cross talk at 0.03% - 1.0% making this a low level threat.

Examples of other hardware and vulnerabilities

EDFA, Erbium Doped Fiber Amplifiers can be subject to jamming. They are an optical amplifier. Modulation in the signals going over the network leaves it vulnerable to attack.
Frequency selective switches are susceptible to eavesdropping. An attacker can introduce a signal into your in order to disrupt the receivers ability to process the signal correctly. See diagram below for an example of this.



picture from MIT Library "Advanced Network Group Secure All-Optical Networking"

Encryption

Since some forms of encryption can cause a bottleneck in the all-optical network because they are complex and take up a large amount of time to complete. The method of dual transmission encryption was developed to speed up the process and add a method of security to the network. This method of encryption reminds me of public key encryption in the traditional network setting.

Two data streams are sent over a single optical carrier link. They are combined to make a single signal that is modified from the original signal and embedded within the optical carrier phase. By using differential phase shift keying (DPSK) and frequency shift keying (FSK) together this form of encryption is accomplished.

An optical data encryptor encrypts inputted data signal, then frequency to frequency coding is done be fore sending the data, by using the differential frequency shift Keying (DFSK) logic signals. On the receiving end there is a frequency modulation unit that processes the DFSK logic signals and a pair of key bits to translate the signal. This operation encrypts the optical transmission.

Conclusion

In this paper we described an all-optical network, explained the hardware components and depicted a few attacks and vulnerabilities of this high-speed network. Though this type of network is still evolving and there were no clear ways to avoid an attack. Like a traditional network the ideology of prevent, protect, react applies to both this and a traditional network. Since this is a high-speed network attacks need to be detected sooner and prevention has to be built in to the network and architecture.

References

Books
Ramaswami, Rajiv and Sivarajan, Kumar N. (1998). Optical Networks: A Practical Perspective. United States of America: Academic Press.
Northcutt, Stephen, (1999) Network Intrusion Detection: An Analyst's Handbook. United States of America: New Riders Publishing.

Internet Sources:
Nevaste, Kaius, Department of Computer Science, Helsinki University of Technology, 1999 "Optical Network Security," knevaste@cc.hut.fi
http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/optical_netsec/onetsec.html

Sadot, Dan, Department of Electrical & Computer Engineering, Department of Communication System Engineering, Ben-Gurion University of Negrev, Patent Status Worldwide Application, "A System and A Method for Information Security in Optical Communication Network"
http://www.bgu.ac.il/bgn/security.html
Content updated June 1999

Information Technology Office of Defense Advanced Research Projects Agency (DARPA),, MIT Lincoln Laboratory, Copyright 1998 "Advanced Networks Group Secure All-Optical Networking,"
http://www.ll.mit.edu/aon/secureaon.html
Last modified July 2, 1998

Lennon, William, National Transparent Optical Network, Lawrence Livermore National Laboratories, Science & Technology Magazine April 1997, "Optical Networks: The wave of the future,"
wjlennon@llnl.gov
http://www.llnl.gov/str/Lennon.html

Last Updated: July 28th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event