Vulnerabilities and Security Issues in Optical Networks

Marija Furdek[1,2], Nina Skorin-Kapov[3], Szilard Zsigmond[4], and Lena Wosinska[1]
[1]KTH Royal Institute of Technology, ICT School, Electrum 229, 164 40 Kista, Sweden
[2]University of Zagreb, Faculty of Electrical Engineering and Computing, Unska 3, 10 000 Zagreb, Croatia
[3]Centro Universitario de la Defensa (CUD), Base Aérea de San Javier Santiago de la Ribera, Spain
[4]Alcatel Lucent, 600-700 Mountain Av. Murray Hill, New Jersey, US
Tel: (46) 8 790 4213, e-mail: marifur@kth.se

ABSTRACT

The paper provides a comprehensive overview of security issues in state-of-the-art optical networks. It identifies and describes the main vulnerabilities of today's and future networks and outlines potential methods of attack which could exploit these vulnerabilities.

Keywords: optical network security, eavesdropping, high-power jamming, signal insertion, alien wavelengths, architecture on demand, network hijacking, latency attacks.

1. INTRODUCTION

We are witnessing the evolution of optical networks towards highly heterogeneous, flexible networks with a widening area of application. As the bandwidth and reliability performance requirements of mission-critical applications tighten, and the amount of carried data grows, issues related to optical network security become increasingly important. Optical networks are vulnerable to several types of security breaches or attacks, typically aimed at disrupting the service or gaining unauthorized access to carried data, *i.e.*, eavesdropping [1]. Depending on the aim of the attack, security breaches can induce financial losses to the clients or cause network-wide service disruption, possibly leading to huge data and revenue losses. Therefore, awareness of security vulnerabilities and attack methods is a prerequisite for designing effective optical network security solutions. This paper provides an overview of potential security issues and attack methods targeting current and future optical networks.

2. EAVESDROPPING IN OPTICAL NETWORKS

Although optical fibres are immune to electro-magnetic interference and do not radiate carried signals to the environment, the exposure of optical networks to eavesdropping poses a considerable security threat. Eavesdropping in general is aimed at gaining unauthorized access to data in order to collect or analyze traffic. In today's digital era, eavesdropping occurs on all network layers from the application to the physical layer, with new instances being revealed at almost daily basis [2], [3]. Several occurrences of eavesdropping at the optical layer have been recorded, primarily targeting governments and the financial, energy, transport or pharmaceutical sectors [4]. Based on the method of realization, eavesdropping attacks can be classified into attacks with direct access to the unencrypted optical channel and those based on breaching the encryption key in encrypted optical systems.

2.1 Eavesdropping via Channel Access (ECA)

A common method of realizing eavesdropping attacks is directly accessing the optical channel via fibre tapping, *i.e.*, removing the fibre cladding and bending the fibre to cause the signal to leak out of the core and onto the photo detector, capturing the information [5]. Tapping devices which can be clipped onto the fibre and cause micro-bends to leak signals and deliver them into the hands of the eavesdropper are easily accessible on the market. Furthermore, existing tapping devices cause losses below 1 dB and can go undetected by commonly used network management systems (NMSs). To detect such intrusions, NMS needs to be enhanced with intrusion detection alarms triggered by insertion loss changes on fibre connections. Obviously such detections require an active monitoring system running across the network. Another possible way of accessing the channel is via monitoring ports, which are typically present at different network components, such as amplifiers, wavelength selective switches (WSSs) or (de)multiplexers. The optical signal is mirrored by an optical splitter to allow connection of monitoring devices without traffic interruption. By obtaining onsite access, an attacker could use these ports to listen to the carried traffic.

2.2 Eavesdropping via Key Access (EKA)

In order to protect the carried data from eavesdropping, encryptions methods are used, implemented in optical transponders. Such encryption cards are commercially available by most vendors. An example solution by Alcatel Lucent [6] relies on encryption of the data packets using encryption keys which are transferred over the NMS isolated from the data payload. Typically, encryption keys are managed by the end user. However, key management software is installed on the user side which can serve as another point of attack reaching the operator NMS system.

978-1-4799-5601-2/14/$31.00 ©2014 IEEE

3. SERVICE DEGRADATION METHODS

The goal of service degradation attacks at the optical layer is to degrade the quality of service or cause service denial, typically by insertion of harmful signals into the network.

3.1 High-Power Jamming (HPJ) Attacks

High-power jamming is realized by inserting an optical signal of excessive power (*e.g.*, 5 – 10 dB above other, legitimate signals) on a legitimate wavelength used in the network. In networks comprised of fixed Optical Add-Drop Multiplexers (OADMs) without any wavelength blocking functionality (*e.g.*, variable optical attenuators), high-power signals can damage the co-propagating user signals inside their common optical fibres, amplifiers and switches, as shown in Fig. 1a. In optical switches, jamming signals can affect legitimate signals at the same wavelength (denoted as User 1 in Fig. 1a) by increasing the in-band crosstalk [7]. Signals traversing common physical links with the jamming signal can suffer from out-of-band effects in optical fibres and amplifiers [8]. In fibres, jamming signals give rise to out-of-band crosstalk by leaking to neighbouring channels and/or increasing non-linear effects (User 2 in Fig. 1a). In erbium-doped fibre amplifiers (the most commonly used type of amplifiers), a jamming signal out of the working range can cause so-called gain competition, in which weaker legitimate signals (Users 2 and 3 in the figure) are robbed of gain by the stronger jamming signal, while the attacking signal gets additionally amplified.

3.2 Alien Wavelength Attacks (AWA)

In order to allow for network upgrades and efficient transmission of high-capacity connections over the existing infrastructure, operators are forced to implement alien wavelengths in their network. Figure 1b shows a multi-vendor network with and without alien wavelength support. When there is no alien wavelength support, each connection is terminated and regenerated by a node at the edge of the domain (node B1 for the green connection in Fig. 1b). Alien wavelengths, on the other hand, can traverse multiple domains without optical/electronic/optical (O/E/O) conversions (red connection in Fig. 1b). Another example of alien wavelength usage is to upgrade legacy line systems with 100G new generation transponders. Such solutions are quite widely used in current deployments.

The presence of alien wavelength can create a significant vulnerability to network security depending on the management of alien wavelengths. About 40% of networks today are still simple fixed OADM based point-to-point networks where the control and management system has no information on the performance of the alien channels. Consequently, signal power and frequency cannot be controlled. Furthermore, if network nodes are based on splitters and WSSs in a broadcast & select configuration, alien wavelengths are launched in the network unfiltered [10]. In such systems, alien wavelengths can be exploited to realize various methods of attacks (*e.g.*, jamming) and present a big risk for network providers. In more intelligent networks, the alien wavelengths are managed by the NMS, *i.e.*, a channel is configured as a friendly wavelength, allowing the management system to have information of signal parameters, but still no control over their values. In newer generation networks, a dedicated interface is defined to host alien wavelengths with the role to tune its power levels but still will not have control of the frequency of the alien channel.

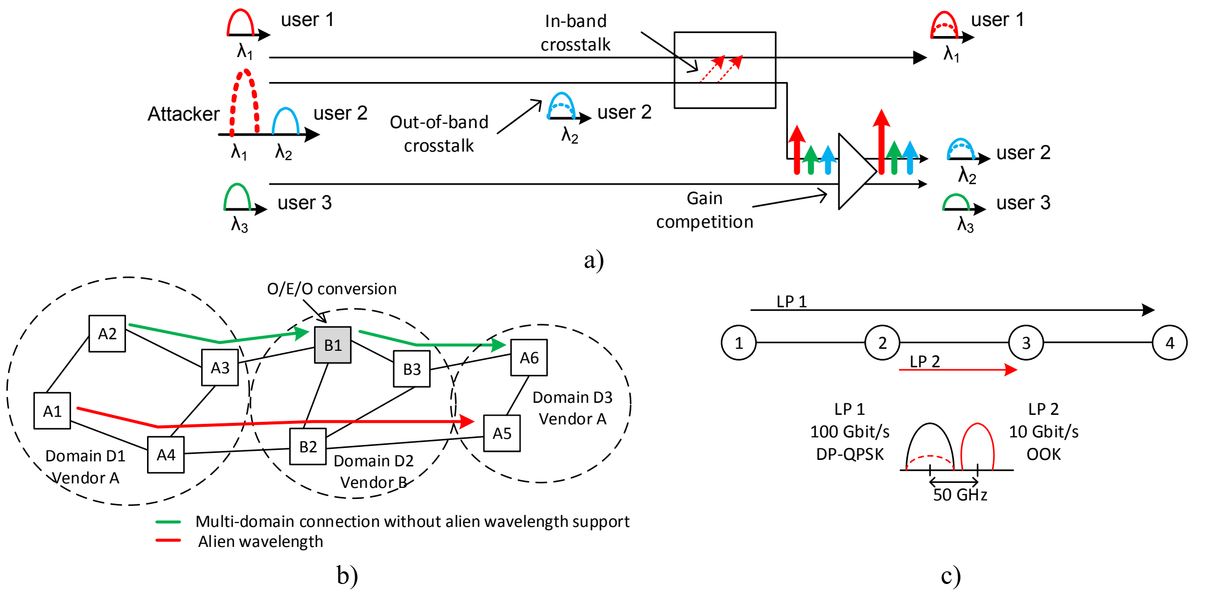

Figure 1: (a) Effects of a high-power jamming signal inside optical fibres, switches and amplifiers; (b) Unmanaged alien wavelengths in multi-vendor network which can act as jamming signals; (c) Signal insertion attack in a multi-line rate network – phase-modulated 100 Gbit/s signal suffers increased XPM effects from an amplitude-modulated 10 Gbit/s signal.

3.3 Signal Insertion Attacks in Mixed Line Rate (SIA-MLR) Networks

Mixed line rate (MLR) networks represent an intermediate, cost-efficient solution for gradual network upgrade from legacy 10 Gbit/s lightpaths to 40/100/200 Gbit/s by allowing the coexistence of different modulation formats over the existing infrastructure. A key security vulnerability of MLR networks stems from nonlinear effects between 40/100/200G signals and legacy 10G neighbouring channels. Namely, amplitude-modulated on-off-keyed (OOK) 10G channels strongly deteriorate the quality of the higher bit-rate, phase modulated channels due to cross phase modulation (XPM). In case of polarization multiplexed channels, cross-polarization modulation (XPolM) additionally affects optical transmission – in dispersion managed networks even more dominantly then XPM [11]. Although it is technically possible to have 10G and 40/100/200G channels in 50 GHz spacing, this imposes an extra OSNR penalty for the 40/100/200G channels. The severity of such penalty depends on the modulation format, channel launch power and guard bands [12]. In most of the deployed networks it is not possible to change the modulation format or launch powers, leaving only the option of using guard bands between 40/100/200G and 10G channels. A possible service degradation attack in MLR networks, shown in Fig. 1c could be inflicted by inserting an OOK channel nearby a 40/100/200G channel, without allowing for enough guard band. Thus, the attacking signal could significantly deteriorate the OSNR of the legitimate signals.

3.4 Signal Insertion on Monitoring ports (SIM) Attacks

As mentioned in Section 2.1, all-optical components are equipped with external monitoring ports, which give rise to certain security vulnerabilities. In addition to providing a means for potential eavesdropping, monitoring ports could also be used to insert signals into the network and damage live traffic.

4. SECURITY ISSUES IN FUTURE NETWORKS

The evolution of optical networks by incorporating software programmable control and management functionalities with highly flexible node architecture, as well as the expansion of data centre networks, introduce new, specific security vulnerabilities.

4.1 Software Defined Networks

Introduction of software-defined networking (SDN) enables decoupling the data and the control planes, which are vertically integrated in currently used network equipment, and logically centralizes the control plane [13]. Alongside numerous benefits, such as simplified and automated end-to-end service provisioning, better utilization of network resources via infrastructure customization to user requirements, and increased network flexibility, SDN might also introduce certain vulnerabilities to network security. The most important part of software-defined networks, in general and from a security perspective, is the SDN controller, which serves as a control interface between the hardware and a large set of SDN applications, including applications which perform traffic engineering or gathering data [14]. Gaining control over such functionalities might represent a desirable target for malicious attacks. SDN controllers could be used to insert viruses, *e.g.*, harmful applications which connect to the controller, and gaining access to the data, or potentially hijacking the network.

4.2 Networks Based on Architecture on Demand

As a response to limited flexibility, scalability and upgradeability of hard-wired reconfigurable add/drop multiplexer (ROADM) architectures, a new concept of programmable, synthetic ROADMs implemented by Architecture on Demand (AoD) has been proposed in [15]. AoD node uses an optical backplane (*e.g.* 3D MEMS or piezoelectric optical switch matrices) to support interconnections between individual optical modules inside the node (*e.g.*, optical splitters, amplifiers, or WSSs), as shown in Fig. 2a. Thus, each connection can bypass unnecessary components and use only those modules which are required to fulfil the switching and processing specifications. New modules are added in the node when and where needed by simply plugging them in the optical backplane. In addition to improving flexibility, scalability, energy efficiency and reliability of the network, this modularity may also expose the network to new security vulnerabilities. Namely, AoD allows for easy insertion of a harmful device (*e.g.*, an eavesdropping or jamming device) before or after a module used by legitimate connections as shown in Fig. 2a. For example, a tapping device could be placed at an unused output of a splitter or after an optical amplifier. Unused WSS ports could also be utilized to insert harmful jamming signals.

4.3 Data Centre Networks

Today's businesses rely on using multiple data centres located in mutually distant physical locations in order to ensure disaster recovery and business continuity in the presence of failures. To guarantee for quick disaster recovery, the stored data and applications must be replicated in multiple data centres. Synchronous replication, in which the storage array which initiates replication waits for the acknowledgment of successful transfer by the receiving storage array, allows for the greatest reduction of data losses in the presence of failures [15]. Due to the fact that each transfer must be acknowledged before the next one can initiate, the process is very sensitive to the

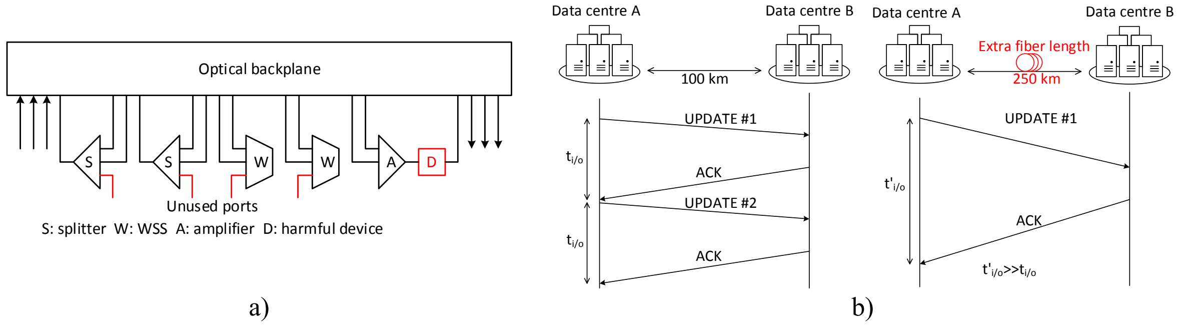

Figure 2: (a) A harmful device inserted in an optical node implemented by AoD; (b) Latency attack in a data centre network: insertion of extra fibre length causes excessive delays in synchronous replication between data centres.

network latency, limiting the maximum distance suitable for synchronous replications to 100 – 200 km. The replication process can be targeted by attackers who aim at gaining unauthorized access to the data or at service disruption. By inserting an extra length of fibre, the network can suffer a latency attack, as depicted in Fig. 2b. Although optical transport network (OTN) frames include the definition of latency measurement, real-time monitoring of latency is not implemented in most networks, which complicates detectability of such attacks.

5. CONCLUSIONS

Optical networks are vulnerable to various types of attacks aimed at eavesdropping and/or service disruption which can lead to high data or revenue losses. Furthermore, the evolution towards software programmable and flexible node architectures creates new security vulnerabilities which need to be identified and taken into account during network design and operation. This paper provides an overview of potential security issues in current and future optical networks and identifies possible attack methods exploiting the associated vulnerabilities.

ACKNOWLEDGEMENTS

This work was supported by the EC FP7 grant No. 318137 DISCUS.

REFERENCES

[1] R. Rejeb, M.S. Leeson, and R.J. Green, “Fault and attack management in all-optical networks”, *IEEE Commun. Mag*., vol. 44, no. 11, pp. 79-86, Nov. 2006.

[2] D. Campbell, “London at the centre of eavesdropping scandal”, *Le Monde*, Jun. 2013.

[3] I. Allen, “Western spy agencies tapped major undersea fiber optic cable”, Intelnews.org, Aug. 2013.

[4] S.K. Miller, “Fiber optic networks vulnerable to attack*”, Information Security Magazine*, Apr. 2006.

[5] B. Everett, “Tapping into fibre optical cables”, *Network Security*, vol. 207, no. 5, pp. 13-16, May 2007.

[6] Alcatel Lucent, 1830 Photonic Service Switch, available online: http://www.alcatel-lucent.com/products/1830-photonic-service-switch, accessed Apr. 2014.

[7] C. Mas, I. Tomkos, and O. Tonguz, “Failure location algorithm for transparent optical networks,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 8, pp. 1508-1519, Aug. 2005.

[8] Y. Peng, Z. Sun, S. Du, and K. Long, “Propagation of all-optical crosstalk attack in transparent optical networks,” *Optical Engineering*, vol. 50, no. 8, 085002.1-3, Aug. 2011.

[9] K. Perlicki, “Impact of an alien wavelength on wavelength division multiplexing transmission quality”, *Photonics Letters of Poland*, vol. 4, no. 3, pp. 110-120, Sept. 2012.

[10] A. Bononi, P. Serena, N. Rossi, and D. Sperti, “Which is the dominant nonlinearity in long-haul PDM-QPSK coherent transmissions?”, in *Proc. ECOC 2010*, Torino, Italy, paper Th.10.E.1, Sept. 2010.

[11] R. Aparicio-Pardo, P. Pavon-Marino, and S. Zsigmond, “Mixed line rate virtual topology design considering non-linear interferences between amplitude and phase modulated channels”, *Photonic Netw. Commun.*, vol. 22, no. 3, pp. 230-239, Jul. 2011.

[12] M. Channegowda, R. Nejabati, and D. Simeonidou, “Software-defined optical networks technology and infrastructure: Enabling software-defined optical network operations”, *J. Opt. Commun. Netw.*, vol. 5, no. 10, pp. A274-A282, Oct. 2013.

[13] Ashton, Metzler & Associates, “Ten things to look for in an SDN controller”, white paper, available online www.necam.com/Docs/?id=23865bd4-f10a-49f7-b6be-a17c61ad6fff, accessed Apr. 2014.

[14] N. Amaya, G. Zervas, and D. Simeonidou, “Architecture on demand for transparent optical networks”, in *Proc. ICTON 2011*, Stockholm, Sweden, pp. 1-4, June 2011.

[15] Cisco MDS 9000 Family Acceleration Services: Enhance Synchronous Replication Performance, 2009.