Various Security Impediments of All-Optical Networks:A Review

Simarpreet Kaur[1,a], Simranjit Singh[1,b]

[1]Research Scholar, Dept. of ECE, Punjabi University, Patiala
[2]Assistant Professor, Dept. of ECE, Punjabi University, Patiala

Abstract: This communication presents a review of security snags in all optical networks. Physical and Service attacks have been reviewed. The vulnerabilities in AONs due to different potholes lead to component attacks, optical switching node attacks, attacks due to ultra high powers etc have been reviewed.

Keywords: AONs, Security attacks, network vulnerabilities, All Optical Networks.

I. INTRODUCTION

All optical networks are emerging as a promising technology for terabit per second class telecommunication and data networks. AONs provide huge transmission capacitiesand are mainly characterized by their transparency to thetransmitted traffic. However, they are intrinsically different from electro-optical networks, particularly because they data do notundergo optical-to-electrical conversion within the network. Composed of wavelength-division- multiplexed(WDM) links [5] and all-optical switching nodes, AONs provide huge transmission capacities exceeding 1 Tb/s overeach fiber [1–3,5]. This makes AONs a promising technology to accommodate the explosive growth of Internet trafficand satisfy the ever-increasing demands on throughput,delay, and overall network performance [5]. In additionto the high transmission capacity feature, AONs are characterized by their transparency to the transmitted traffic[1,3,6–9]. This development takes speed to new pinnacle and with these new approaches comes new vulnerabilities. Although they offer many advantages for high data ratecommunications, AONs come with new challenges in terms of network security that do not exist in traditional communication networks [1,3,6 –9,11,12]. In particular, AON components have different accessibility and vulnerabilitiesfrom electronic components. For example, it is quite easyto tap or jam signals at a specific wavelength by bendingan optical fiber slightly and either radiating light out ofit or coupling light into it. Besides, the optical transmissiontechnology allows for different attack opportunities. Forinstance, the crosstalk level in switches may be sufficientlylow for normal operation but may not be low enough toprevent an eavesdropping attack. In addition, the transparency feature allows an intruder that has gained accessto one component to simply pass a signal right through allthe components that handle the associated lightpath. Thismeans that a signal can be injected into the network at aremote location and, by attentive choice of wavelength, affect various parts of the network. This widespread effect ishard to realize in conventional networks because signalsare regenerated at every node, and, therefore, a maliciousphysical signal can be trapped at the ends of a link.Finally, the high data rates employed in AONs make themvery sensitive to communication failures because large amounts of data can be affected even with failures of veryshort duration. Since even short failures can cause large amountsof data to be lost, the need for securing and protectingAONs has become increasingly significant [1,3,8,9,11,12].Different studies have addressed the security issuesin the development of the all-optical networking technology. Actually, various methods have been proposed for attack prevention, detection, localization, and reaction[1–4,6,8,10,13].Nevertheless, no robust standardsor techniques exist to date for guaranteeing the qualityof service (QOS) in these networks, and hence the majority of AON security issues are still under study [8]. In this article we are reviewing the status of possible vulnerabilities, their causes and possible solutions if any available.

II. VULNERABILITIES OF AONs

Vulnerability is a flaw ora weakness that may be exploited by an attackertocarry out a security attack. AONs provide transparencycapabilities allowing routing and switching of traffic without regeneration of signals within the network AONs.Although transparency, in AONs, offers many advantagesfor high data rate communications, it manifests new security vulnerabilities.

First and foremost, the transparency feature of AONs acts as a major vulnerability along with its capability to offer very high speeds. Actually, theabsence of signal interpretation and regeneration withinthe network allows for transmission impairments (crosstalk, power increase, etc.) and attack signals to propagatethrough parts of the network without being discarded atsuch intermediate nodes. Allowing the propagation of malicious signals throughthe network, the transparency feature allows an intruder that has gained access to one component to simply pass asignal right through all the components that handle theassociated lightpath. This means that an intruder caninsert a malicious signal into the network at a remotelocation and consequently affect many different parts ofthe network.

Second major susceptibility point in an AON is its component vulnerability. Use of optical components like optical fibers and optical amplifiers make it a point of intrusion. For instance the use of optical fiber may allow a physical attack if it remains unshielded or if someone gains physical access to it. Attacker can easily cut the fiber or bend it slightly, so that thelight can be radiated into or out of the fiber [1,3,4,7,9].

Similarly, under high-power input or long distances, fibers exhibitcertain nonlinear characteristics causing channel crosstalkeffects between WDM channels. Crosstalk is a phenomenon in which a small portion of a wavelength channel leaksonto an adjacent channel. Crosstalk effects may beexploited by an attacker to tap a wavelength channel orto perform an attack by injecting a high-power malicioussignal into the network.

Further, the use of amplifiers like EDFA can also make it possible for attacker to enter into network very easily. e fiber, it gets attenuated and its power leveldecreases. Optical amplifiers are used to transparentlyamplify optical signals and restore their power to anacceptable level. he gain competition phenomenon may make AONsvulnerable to various forms of SD attacks. Actually, transmitted over an EDFA amplifier, a high-powered malicioussignal may exploit amplifier gaincompetition to bothdeprive legitimate signals of power and increase its ownpower. Having an increased power downstream of theamplifier, the malicious signal could transparently spreadthrough the network and affect different data channelsover the network.

Other components like optical switching nodes etc. may also be raised finger at for security issues due to introduction of significant crosstalk levels, which makeAONs vulnerable to various attacks.

In addition to these physical attacks, security attacks can also be present in a network. A network security attack may be defined as an intentional action against the ideal and secure functioning ofthe network [6,11]. A network security attack can be performed at the physical layer, exploiting vulnerabilities of the physical network infrastructures, or at higher networklayers, exploiting vulnerabilities of network protocols[1,4,7,9].

While some available management mechanisms can beused in different types of network architectures, many ofthese are not applicable to AONs. In particular, due tothe huge bit rates in AONs, large amounts of informationare lost even in the case of attacks of extremely shortduration [1 –4,7 –9,11,12]. Therefore, in the case of a security attack, network restoration should take place as fastas possible avoiding critical delays and traffic loss, andensuring timely recovery. This requires the developmentof specific mechanisms allowing fast detection, accurateidentification, and quick reaction to security attacks. Inaddition to the attack management difficulties caused bythe high transmission capacity feature, the transparencyfeature, which refers to the fact that an optical signal istransmitted through the network without interpretationor regeneration, makes attack management in AONs morechallenging [1 –4,8,9,11,12]. Actually, due to the transparency feature, a security attack may spread rapidly all overthe network leading to multiple failures propagating rapidly throughout the network without any restoration. Thisin particular makes crucial the localization and identification of attacks in AONs. Therefore, specific methods able todetect and identify multiple-point failures are needed toaddress the failure management issue in AONs.Performance management is germane to successful AON operation since it provides signal quality measurements at very low BERs and fault diagnostic support [14]. PN sequences with very long periods using optical logic has been generated having advantage of being scalable and independent of usage of number of gates in optics to provide long period [15]. Use of rapid reconfigurable bit-by-bit code scrambling and code shifting technologies for secure optical communication has been studied. Security improvements for both the OOK and DPSK data modulation formats at various data rates are achieved. The optical code reconfigurable techniques provide an attractive approach for secure optical communication, exhibiting the potential to realize even one time pad [16].

Table-1 Remarks of reviewed papers

S no	Papers	Remarks
1.	M. Medard *et.al* [1]	Physical security issues namely service denial and tapping have been studied.
2.	M. Medard *et.al* [2]	By virtue of the high rates and low BERs optical communication suffer particularly strenuously from denial of service attacks.
3.	J.K. Patel *et.al* [3]	An optical signal undergoes many transmission impairments throughout its entire path in an AOTN
4.	M. Medard *et.al* [4]	Various methods for detecting intentional attacks upon the infrastructure of an all-optical network are enlisted.
5.	A. Lzzez *et.al* [5]	AONs including WDM system have transmission capacity upto 1Tb/s.
6.	C.M. Machuca *et.al* [6]	A failure location algorithm that aims to locate single and multiple failures in transparent optical networks is presented
7.	S. Singh *et.al* [7]	The scheme of a single module for simultaneous operation of all-optical computing circuits, namely half adder and half subtractor, are realized using semiconductor optical amplifier (SOA) based logic gates is presented.
8.	R. Rejeb *et.al* [8]	An algorithm for multiple attack localization and identification that can participate in some tasks for fault management of all-optical networks is designed.
9.	M. Furdek *et.al* [9]	Methods for attack detection and localization, as well as various countermeasures against attacks at physical layer are described.
10.	J.S. Yeom *et.al* [10]	Results with simple vulnerability and attack scenarios in order to demonstrate how the self-organization helps to adapts against new vulnerabilities and avoid attacks are presented.
11.	R. Rejeb *et.al* [11]	A framework has been designed for the realization of an appropriate management system that can meet the challenges posed by all-optical networks.
12.	R. Rejeb *et.al* [12]	A novel approach based on a link-by-link test method for detecting performance degradation in wavelength-routed WDM optical networks, which can participate in fault and performance management of AONs is proposed.
13.	G. Castañón *et.al* [13]	The use of MPR as an instinct immediate network reaction to failures and attacks in transparent networks; after the nodes transmit the data and causes of failure are classified, better self organized decisions can be used based on changing routing output priorities to reach destination is proposed.
14.	R. Rejeb *et.al* [14]	Management issues with particular emphasis on complications that arise due to the unique characteristics and peculiar behaviors of transparent network components is considered.

15.	M. Medard *et.al* [15]	High- speed electro-optic scheme for reconfigurable feedback shift registers (RFSRs) that relies upon electronic encryption circuits to reconfigure a sequence of optical logic gates and which makes use of the latency in the optical gates as memory is proposed.
16.	X. Wang *et.al* [16]	Security improvements for both the OOK and DPSK data modulation formats at various data rates are achieved

III. CONCLUSION

We have investigated the main challenging issues facing the efficient management of security attacks in AONs, presented a deep analysis of thesecurity challenges of AONs that distinguish them from traditional communication networks. In particular, we have focused on the physical security aspect that differs significantly from that in electro-optic and electronic networks and that directly impacts the physical infrastructure of AONs.

REFERENCES

[1] M. Médard, D. Marquis, R. A. Barry, and S. G. Finn, “Security issues in all-optical networks,” *IEEE Netw. Mag.*, vol. 11, no. 3, pp. 42 –48, May 1997.

[2] M. Médard, “Secure optical communications,” in *Lasers and Electro-Optics Society Annu. Meeting*, pp. 323 –324, Dec. 1998.

[3] J. K. Patel, S. U. Kim, D. H. Su, S. Subramaniam, and H.A. Choi, “A framework for managing faults and attacks in WDM optical networks,” in *Proc. of the DARPA Information Survivability Conf. and Expo.* (DISCEX), Anaheim, CA, vol. 2, pp. 137 –145, June, 2001.

[4] M. Médard, D. Marquis, and S. R. Chinn, “Attack detection methods for all-optical networks,” in *Network and Distributed System Security Symp., session 3,* San Diego, CA, Mar. 11 –13, 1998, paper 2.

[5] A. Lazzez, N. Boudriga, and M. S. Obaidat, “ Optical switching techniques in WDM optical networks,” in *The Handbook of Computer Networks, H. Bidgoli, Ed.*, vol. 1, part 3. Wiley,2007, pp. 909 –928.

[6] C. M. Machuca, 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.

[7] S. Singh, R.S. Kaler, and R. Kaur, ”Realization of high speed all optical half adder and half subtractor using SOA based logic gates,” *Optical Society of Korea*, Vol.18, no.6, pp.633-638, 2014

[8] 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.

[9] M. Furdek and N. Skorin-Kapov, “Physical layer attacks in transparent optical networks,” www.intechopen.com., Oct. 2015.

[10] J.S. Yeom, O. Tonguz, and G. Castanon, “Security in alloptical networks: Self-organization and attack avoidance,” in *IEEE Int. Conf. on Communications (ICC)*, Glasgow, Scotland, June 2007.

[11] R. Rejeb, M. S. Leeson, C. Mas Machuca, and I. Tomkos, “Control and management issues in all-optical networks,” J. Netw. , vol. 5, no. 2, pp. 132 –139, Feb. 2010.

[12] R. Rejeb, I. Pavlosoglou, M. S. Leeson, and R. J. Green, "Securing all-optical networks," in *The 5th Int. Conf. on Transparent Optical Networks*, June 29 –July 3, 2003.

[13] G. Castañón, I. Razo-Zapata, C. Mex, R. Ramirez-Velarde, and O. Tonguz, "Security in all-optical networks: Failure and attack avoidance using self-organization," in *Int. Conf. of Transparent Optical Networks –Mediterranean Winter (ICTON-MW)*, Marrakech, Morocco, Dec. 2008.

[14] R. Rejeb, M.S. Leeson and R.J. Green," Fault and Attack Management in All-Optical Networks" *IEEE Communication Magazine*, vol. 44, no.11, pp. 79-86, Nov. 2006.

[15] M. Medard, A.H. Chan, J.D. Moores, K.L.Hall, K.A.Rauschenbach and S. Parikh," Ultrafast Cryptography using optical logic in reconfigurable feedback shift registers,"*Proc. SPIE 3228, Multimedia Networks: Security, Displays, Terminals, and Gateways, 342*, doi:10.117/12.300905; Feb. 1998.

[16] X. Wang, Z. Gao, B. Dai, N. Kataoka and N. Wada," Secure Optical Communication based on optical code reconfiguration scheme," *Proc. SPIE 8331, Photonics and Optoelectronics Meetings (POEM) 2011: Optical Communication Systems and Networking*, 83310F, doi: 10.1117/12.924049, Jan. 2012.