Optical Engineering

SPIEDigitalLibrary.org/oe

Attack propagation of high-powered intrachannel crosstalk in transparent optical networks

Zeyu Sun
Yunfeng Peng
Keping Long

SPIE

Attack propagation of high-powered intrachannel crosstalk in transparent optical networks

Zeyu Sun,[a] Yunfeng Peng,[b] and Keping Long[b,c]
[a]Chongqing University of Posts and Telecommunications, College of Communication and Information Engineering, Chongqing, 400065 China
[b]University of Science Technology Beijing, School of Computer and Communication Engineering, Institute of Advanced Network Technology and New Services, Beijing, 100083 China
[c]University of Electronic Science and Technology of China, Research Centre for Optical Internet Mobile Information Networks, Chengdu, 611731 China
E-mail: shouxiansun@163.com

Abstract. Transparent optical networks (TON) are becoming increasingly attractive, but transparency introduces security threats, e.g., intrachannel crosstalk attack, to optical networks. In this letter, three attack scenarios, i.e., attack propagation within an optical cross connect (OXC), the secondary attacker traverses successive OXCs and original attacker traverses successive OXCs, are investigated. The scenarios accompanied with gain competition attack are also simulated as comparison. Bit-error-rate (BER), and eye diagram penalties are estimated via VPItransMaker™. Our work proved that the attack signal will propagate intrachannel crosstalk attack to successive three OXCs but with limited two stages of optical switches in each OXC. The BER will be somewhat higher in case gain competition attack exists. The results will be useful for future managing, planning, and designing on TONs. [DOI: 10.1117/1.3641411]

Subject terms: intrachannel crosstalk attack; attack propagation; gain competition attack.

Paper 110693LR received Jun. 20, 2011; revised manuscript received Aug. 24, 2011; accepted for publication Aug. 31, 2011; published online Sep. 29, 2011.

1 Introduction

The transparent optical network (TON) is an attractive network paradigm offering high data rates without expensive O-E-O conversion, and will be more available to public users as fiber-to-the-home (FTTH) getting increasingly popular. However, transparency will also introduce attack threats to TON, e.g., malicious users can gain more chances to access to the network, and then inject a beam of light at a high power being 20 dB or even higher than a normal one, which will result in crosstalk attack on normal signals.[1–5] Especially in the optical switch architectures, such as optical cross connect (OXC), a high-powered attack signal will leak significant power to normal channels working at the same wavelength, resulting in intrachannel crosstalk attack.

A model to describe the propagation of intrachannel crosstalk attack in a TON is proposed as shown in Fig. 1.[1,3] In this figure, a high-powered signal (Attacker) will leak power to the legitimate signal (User 1) through intrachannel crosstalk, and such significant leakage will enable User 1 the attack capability. The attack capability in User 1 will in turn affect User 2 in the next switch, therefore more stages of switches will be affected.[1,3,5] The high-powered signal will also rob the gain of adjacent channels in an optical amplifier and become stronger,[4,6] which will make the attack propagation of intrachannel crosstalk more serious.

In this letter, we present three scenarios of intrachannel crosstalk attack, attack propagation within the first OXC, the secondary attacker traversing successive OXCs, and the original attacker traversing successive OXCs. Via VPItransmaker™, analysis on bit-error-rate (BER) and eye diagram penalties imposed by attack signals with different switch crosstalk intensities and detection methods are presented. The penalties accompanied with gain competition attack are also given. The simulation proved that the original attacker will cause the propagation effect of intrachannel crosstalk attack within three successive OXCs but with a limited two stages of switches in each OXC. The results also proved that the polluted signals (i.e., the polluted secondary attacker) do not have enough attack capabilities to propagate intrachannel crosstalk attack to the next OXC. The simulation also indicates that if gain competition attack exists, the BER will be somewhat higher.

2 Simulation Analysis and Setup

Figure 2 depicts the simulated TON system, in which four wavelengths are multiplexed in a fiber and all four laser transmitters (TxExtModLaser) transmit at a power of 1 mW. All the transmitted signals are nonreturn to zero non-return-to-zero (NRZ) formats at a rate of 10 Gbit/s and modulated on four wavelength channels λ_0, λ_1, λ_2, and λ_3 according to ITU 100 GHz grid from 193.00 to 193.30 THz at C-band. The grid spacing is wide enough to suppress four-wave mixing and cross-phase modulation (XPM)[6] to focus on intrachannel crosstalk attack. However, the extremely high-powered signal will cause serious self-phase modulation (SPM), which causes the broadening of the signal spectrum and power degradation of the attack signal.[7] The statistics of phase-difference between legitimate and crosstalk signal which dominates the BER performance[8] is also difficult to determine due to serious SPM, thus multisimulations are carried out by adjusting phase shift in optical switch and we select the worst BER. All segment fibers are nonlinear dispersive fibers

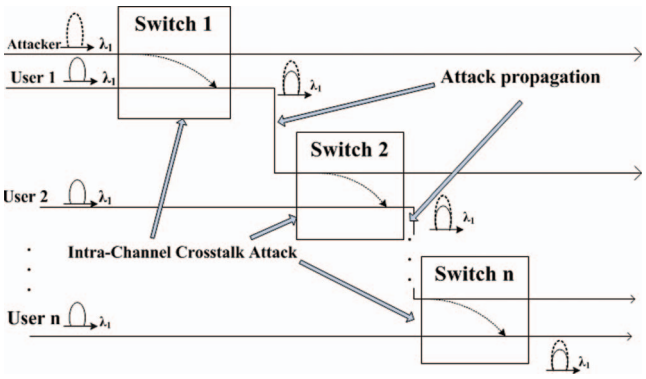

Fig. 1 The propagation of intrachannel crosstalk in an OXC.

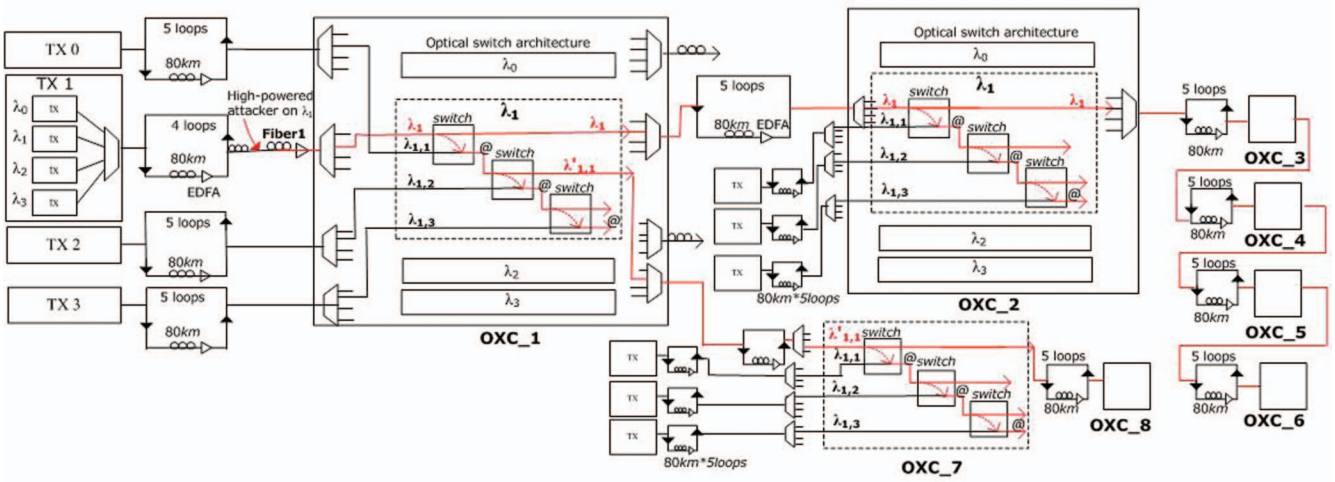

Fig. 2 Simulation setup demonstrates propagation of intrachannel crosstalk attack.

(NLS) with 0.2 dB/km attenuation and $2.6 \times 10^{-20}\,\mathrm{m}^2/\mathrm{W}$ nonlinear index. The dispersion for all NLS segments is set identical $2.0 \times 10^{-3}\,\mathrm{ps/nm/km}$ also without compensation so that we can concentrate on the crosstalk attack. We employ erbium doped fiber amplifier (EDFA) (AmpSysOpt) as an amplifier with 16 dB fix gain to avoid gain competition attack and 4 dB noise figure. Multiplexer and switch are with 2 dB insertion loss. Node spacings are set to 400 km including five loops of 80 km NLS segments.[9]

We assume that the attacker injects a high-powered signal modulated at the same 10 Gbit/s NRZ format as legitimate signals on wavelength λ_1 at a power of 500 mW and the injection point is 15 km before OXC-1.[2] In each OXC, three cascaded 2×2 optical switches (SwitchDos-Y-Two) are set for channel λ_1. Let $\lambda_{1,n}$ represent the legitimate signal on wavelength λ_1 passing the n'th stage of an optical switch. The high-powered attacker on wavelength λ_1 will attack legitimate signals $\lambda_{1,1}$, $\lambda_{1,2}$ and $\lambda_{1,3}$ from OXC-1 to OXC-6, as shown in Fig. 2. The polluted signal in OXC-1 directly traverses OXC-7 and OXC-8. At the egress points of each switches (i.e., the point labeled as @), BERs and eye diagrams are detected using RxBERs and ViScopes.

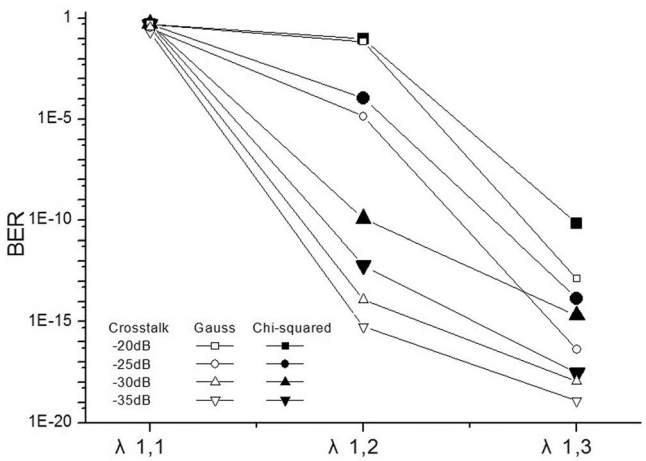

Fig. 3 BER for intrachannel crosstalk attack within OXC-1 with different switch crosstalk intensities and crosstalk detection methods.

3 Simulation and Discussion

3.1 *Intrachannel Crosstalk Attack Propagation Within OXC*

We assume the crosstalk to be Gaussian distribution to achieve the upper bound of system BER (Ref. 10) and the statistics of the received optical signal will follow one of a family of Chi-squared probability densities,[11,12] and then the Chi-squared method is set to estimate the BER at the receivers. As a comparison, the Gaussian method is also implemented, in which the statistics of the received optical signal are assumed to be Gaussian distribution. Switch crosstalk intensity is a parameter representing the amount of power leakage between two channels in an optical switch, which determines how much crosstalk noise will be added in the received optical signals. Figure 3 illustrates the BER of signals $\lambda_{1,1}$, $\lambda_{1,2}$, and $\lambda_{1,3}$ in OXC-1. As switch crosstalk intensity decreases from -20 to -35 dB in four grades, i.e., -20, -25, -30, and -35 dB,[4] the BERs for $\lambda_{1,1}$ are affected between 0.1 and 0.5, and those for $\lambda_{1,2}$, are distinguishingly distributed. However, BERs for $\lambda_{1,3}$ are all kept lower. Eye diagrams for $\lambda_{1,2}$ with different switch crosstalk intensities under Chi-squared detection are also given in Fig. 4. The result reveals that the extent of intrachannel attack propagation within an OXC is different with switch crosstalk intensities but with limited two stages of switches. The result also indicates that as the crosstalk increases, there will be less difference between detection methods. Compared to the Gaussian method, the Chi-squared method will overestimate the system BER.

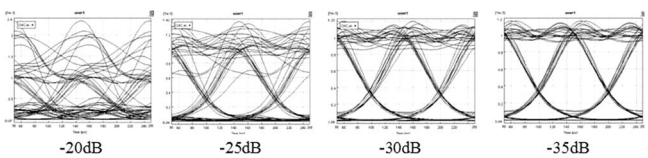

Fig. 4 Eye diagrams for $\lambda_{1,2}$ within OXC-1 under the Chi-squared detection method with different switch crosstalk intensities of optical switches (-20, -25, -30, and -35 dB).

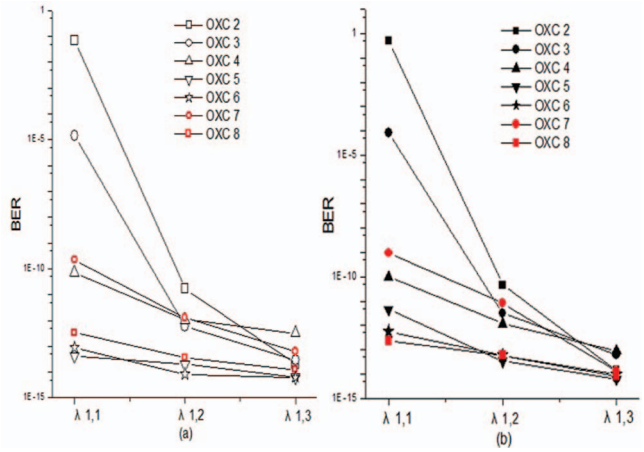

Fig. 5 BER of signals $\lambda_{1,1}$, $\lambda_{1,2}$, and $\lambda_{1,3}$ in OXC-2 to OXC-8: (a) with fix gain in EDFA and (b) accompanied with gain competition attack.

3.2 *Original Attacker Traversing Successive OXCs*

To investigate the intrachannel crosstalk attack spanning multiple OXCs, the original attack signal is set to traverse from OXC-1 to OXC-6. The switch crosstalk intensity is set to be identically -25 dB at all switches. Figure 5(a) shows the BERs of $\lambda_{1,1}$, $\lambda_{1,2}$, and $\lambda_{1,3}$ in OXC-2 to OXC-6, respectively. The BERs of $\lambda_{1,1}$ at OXC-2 and OXC-3 are 0.3 and 1.05×10^{-5}, respectively. The BER of $\lambda_{1,1}$ at OXC-4, -5, and -6 are all quickly dropped. Those BERs of $\lambda_{1,2}$ and $\lambda_{1,3}$ at five OXCs are all less than 1.0×10^{-10}. Eye diagrams of $\lambda_{1,1}$ in OXC-2 to OXC-5 are shown in Fig. 6. By setting EDFA to power model, a gain competition effect can be achieved. Figure 5(b) shows the BER penalties accompanied with gain competition attack, in which we can see that the robbed gain in EDFA will make the BER of $\lambda_{1,1}$ in OXC-2 to OXC-6 a little worse for the reason that -25 dB of the robbed power will be leaked to the legitimate channels. The results also indicate that only the first stage of switches will be affected worse if gain competition attack exists. The results indicate that the high-powered original intrachannel crosstalk can propagate its attack effect to successive three OXCs and the BER will be somewhat higher in case there is gain competition attack.

3.3 *Secondary Attacker Traversing Successive OXCs*

The intrachannel crosstalk propagation caused by the polluted signal (secondary attacker) is also simulated. As illustrated in Fig. 2, the secondary attacker from OXC-1 traverses OXC-7 and OXC-8 and attacks $\lambda_{1,1}$, $\lambda_{1,2}$, and $\lambda_{1,3}$ in the OXCs with BERs all being below 1.0×10^{-9} as shown in Fig. 5(a). If gain competition attack exists, as shown in Fig. 5(b), the BER of $\lambda_{1,1}$ in OXC-7 and OXC-8 are getting a little higher. The simulation indicates that the polluted secondary attacker does not have enough capabilities to propagate intrachannel attack to successive OXCs even if gain competition attack exists, for the reason that insertion loss in optical components and nonlinear effect in fibers cause power degradation of the secondary attacker.

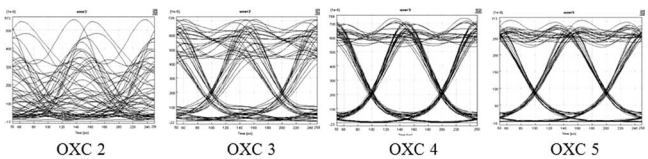

Fig. 6 Eye diagrams of $\lambda_{1,1}$ in OXC-2 to OXC-5.

4 Conclusions

In this letter, three attack scenarios of intrachannel crosstalk accompanied with gain competition attack have been presented and investigated via VPItransMaker^{TM}. We found that the high-powered signal will propagate an intrachannel crosstalk attack to successive three OXCs but with limited two stage switches within each OXC, and this propagation extent depends on switch crosstalk intensity and detection method. The secondary attacker does not have enough attack capability to propagate this attack. We also found if gain competition exists, the system BER will be somewhat higher.

Acknowledgments

This work is supported by Chang Jiang Scholars Program of the Ministry of Education of China, National Science Fund for Distinguished Young Scholars (No. 60725104), 973 Program (No. 2007CB 310706), National Natural Science Foundation of China (No. 61071101), 863 Program (2009AA01Z254, 2009AA01Z215), and NCET Program of MoE of China.

1. T. Wu and A. K. Somani, "Cross-talk attack monitoring and localization in all-optical networks," *IEEE/ACM Trans. Netw.* **13**(6), 1390–1401 (2005).
2. M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security issues in all-optical networks," *IEEE Network* **11**(3), 42–48 (1997).
3. N. Skorin-Kapov and M. Furdek, "Limiting the propagation of intra-channel crosstalk attacks in optical networks through wavelength assignment," in *Optical Fiber Communication Conference*, San Diego, California, March 22, 2009, OSA Technical Digest (CD), Optical Society of America (2009).
4. M. Furdek, N. Skorin-Kapov, M. Bosiljevac, and Z. Sipus, "Analysis of crosstalk in optical couplers and associated vulnerabilities," in MIPRO, Opatija, Croatia, pp. 467–472 (2010).
5. P. Yunfeng, S. Zeyu, D. Shu, and L. Keping, "Propagation of all-optical crosstalk attack in transparent optical networks," *Opt. Eng.* **50**, 085002 (2011).
6. T. Deng and S. Subramaniam, "Analysis of optical amplifier gain competition attack in a point-to-point WDM link," *Proc. SPIE* **4874**, 249–261 (2002).
7. R. H. Stolen, "Nonlinearity in fiber transmission," *Proc. IEEE* **68**(10), 1232–1236 (1980).
8. A. Arie, M. Tur, and E. L. Goldstein, "Probability-density function of noise at the output of a two-beam interferometer," *J. Opt. Soc. Am. A* **8**, 1936–1942 (1991).
9. J. D. Downie and A. B. Ruffin, "Analysis of signal distortion and crosstalk penalties induced by optical filters in optical networks," *J. Lightwave Technol.* **21**, 1876–1886 (2003).
10. K.-P. Ho, C.-K. Chan, F. Tong, and L. K. Chen, "Exact analysis of homodyne crosstalk induced penalty in WDM networks," *IEEE, PTL* **10**, 457–458 (1998).
11. D. Marcuse, "Derivation of analytical expressions for the bit-error probability in lightwave systems with optical amplifiers," *J. Lightwave Technol.* **8**(12), 1816–1823 (1990).
12. F. Abramovich and P. Bayvel, "Some statistical remarks on the derivation of BER in amplified optical communications systems," *IEEE Trans. Commun.* **45**(9), 1032–1034 (1997).