High-powered optical attack propagation in transparent optical networks

Yunfeng Peng, Zeyu Sun, and Keping Long

The deleterious effects of a malicious attack propagating through a transparent optical network are shown to be limited to the first few switching stages.

Transparent optical networks (TONs) can provide hundreds of high-speed optical channels using one hair-like fiber, without the need for expensive optical-electrical-optical conversion at intermediate network nodes. Unfortunately, a malicious user may attack other users by injecting a high-powered beam of light, causing intra- and interchannel crosstalk and disrupting legitimate optical signals sharing the same fiber links and switching modules. Although this security issue has been understood for years, little attention has been paid to it over the past decade due to the ambiguous future of TONs.

Figure 1 shows a theoretical model of intrachannel crosstalk. Inside Switch 1, some of the energy of the attacker’s high-powered optical beam leaks into an adjacent fiber, where it damages the signal of any user who happens to be transmitting on the same frequency as the attacker. That user’s polluted signal then leaks energy into additional fibers at the next switch, damaging other signals that are also using that frequency. In fact, damage is not limited to signals on the same frequency as the attacker. In a related phenomenon called interchannel crosstalk, the energy of the attack beam leaks into nearby frequencies, either within a single fiber (direct interchannel crosstalk) or between adjacent fibers inside an optical switch (indirect interchannel crosstalk).

It is recognized that a given attack can only affect a limited number of users, since as the signal propagates, its energy is dissipated. However, the exact point beyond which the attack will no longer have an effect on legitimate transmissions has not been well understood. To study this question, we created the experimental setup shown in Figure 2. Each optical cross-connect (OXC A, B, and C) consisted of a set of cascaded 2 × 2 optical switches. Ingress and egress at each switch were on a single wavelength. All fiber segments between OXCs were 80km nonlinear dispersive fibers with 0.2dB/km attenuation and a nonlinear index of 2.6 × 10⁻²⁰m²/W, set to 2.6 × 10⁻³ps/nm/km without compensation. The erbium-doped fiber amplifiers were

Continued on next page
set to 16dB gain and a 4dB noise figure, and the optical switches were set at a cross talk of –25dB.

Using VPItransmissionMaker™ simulation tools, we multiplexed the signals from four lasers into one fiber link. The frequencies chosen (λ₀ = 193.00THz, λ₁ = 193.10THz, λ₂ = 193.20THz, and λ₃ = 193.30THz) were selected from the 100GHz grid of the International Telecommunication Union’s C-Band, which subdivides a portion of the electromagnetic spectrum into discrete channels for optical communications use. User signals were 10Gb/s non-return-to-zero at 1mW. The attack beam was injected into Fiber 1 on channel λ₁ (193.10THz).

Figure 3 compares the bit error rates (BERs) of three users due to intrachannel crosstalk when the attack power was 100, 200, 500, and 700mW. Each BER was detected at the corresponding egress port of the switch shown in Figure 1. User 1 is seen to suffer the worst BER (0.5), while User 3, whose lowest BER is near 10⁻¹⁵, is affected only slightly.

As mentioned, interchannel crosstalk causes the degradation of signals whose frequencies differ from the one chosen by the attacker. The eye diagrams in Figure 4 show legitimate channel λ₂ at various points along Fiber 1, revealing direct interchannel crosstalk from a 500mW attack signal on adjacent channel λ₁ within that same fiber. The attack causes serious damage as it propagates through the first three fiber segments, rapidly attenuating after that. The eye diagrams in Figure 5 show how indirect interchannel crosstalk affects channel λ₂ on other fibers, as detected at @5, @6, and @7, respectively. The signal quality at @5 and @6 is clearly worse than that at @7.

The simulation shows that under this scenario, which features two-stage OXCs, significant degradation of legitimate signals by intra- and interchannel crosstalk is limited to the first three OXCs. This result applies to the original attack signal only and not to the polluted user signals, which can barely propagate the attack past even a single OXC. As TONs become increasingly available to public users, further study will be required. Our future work will examine attack awareness, locating, and control.

This work was supported by the Chang Jiang Scholars Program of the Ministry of Education of China, National Science Fund for Distinguished Young Scholars (60725104), National Natural Science Foundation of China (61071101).

Author Information

Yunfeng Peng and Keping Long
University of Science Technology Beijing
Beijing, China

Zeyu Sun
Chongqing University of Posts and Telecommunications
Chongqing, China

Yunfeng Peng received his PhD in communication and information systems from Shanghai Jiaotong University (2007). His research interests are in fiber communication networks, optical Internet architecture and its control technologies, theory and

Continued on next page
applications of complex networks, and pervasive network technologies and their implementation.

References