9:00am - 9:30am (Invited)
FE3

Secure Optical Communications.

Muriel Médard, CSRL, University of Illinois at Urbana-Champaign.[1]

Optical communications cover a wide area of technologies, from electro-optic networks, which are in widespread use, to experimental all-optical networks. The transition of technology from the latter to the former occurs rapidly, with such technology as WDM being widely commercially available. In this paper, we address issues concerned with the optical portions of communications networks. The security issues we address are particularly germane to all-optical networks, but many are also applicable to the optical portions of electro-optic networks. Optical communication, by virtue of the high rates and low BERs they offer, suffer particularly strenuously from denial of service attacks. A short attack, which might only affect a small number of bits in a slower electronic network, may affect a very large number of bits in optical communications. The very light coding and simple signaling, such as OOK, commonly used on optical transmissions renders them vulnerable to service degradations. Overviews of optical security issues may be found in [MMBF:97, MMFB:98].

Because of such features, **characterization** is particularly important. At the component level, crosstalk in optical components, which may already be a challenge in systems without attackers, may become a tool for nefarious users to disrupt operations. Coherent crosstalk in wavelength routers, for instance within wavelength selective switches for WDM systems, can allow a user on λ_1 on one fiber to jam or eavesdrop upon another user on the same wavelength and another fiber. While –25 dB crosstalk may be sufficient to maintain low BERs for two users at 20 dB SNR, this separation may not be sufficient if an attacker comes in at 5-10 dB higher SNR. EDFAs also suffer from crosstalk, this time among different wavelengths, owing to limited gain. In a WDM system, a user at λ_1 may come in at a high power and reduce the gain of users at other wavelengths. If λ_1 is in the 1530 nm range, i.e. in the peak of an unflattened EDFA, then a signal which is even 10-20 dB below signals in the flat 1539-1550 nm range may significantly reduce the gain of the legitimate signals. Such a reduction in gain occurs not only at steady state, but is particularly marked in transients ([Chi:98]). The response to a step function in the input includes, over several ms, an output transient at λ_1 with a peak over 10 dB higher than the input and significant gain degradation at other wavelengths. Hence, the transient may significantly affect Mbits of data and also create an amplified attack travelling downstream to other EDFAs. Fibers are also vulnerable to crosstalk, for instance via wavelength mixing. More importantly, while components for routing or amplifying may be not be easily accessible, a significant portion of the existing fiber is unprotected and may be accessed by simple removal of cladding. Fiber may not only be tapped in the well-known manner, but it may also suffer from jamming attacks in which an attacker uses a portion of the signal he has previously tapped, in combination with a source of white noise, such as ASE from an EDFA. The attacker does not need to photodetect the signal he taps, but only needs an attenuator, an ASE source, and a phase shift. Such an attack only requires an accuracy of approximately 0.2 cm for attacks over a wavelength carrying data at a rate of 10 Mbits/s. Finally, attacks may not only exploit the weaknesses of components and infrastructure, but also those of architectures. Rings, which are a common way of providing redundancy in SONET/SDH systems, force common trunks which may lead to catastrophic failure on the case of an attack which spreads, such as an EDFA jamming attack. If a single attack leads to a series of failures, backup traffic may be provided as for a single failure, possibly causing disruption in areas of the network which were not even directly reached by an attack.

The above discussion motivates the need for **preventing** attacks on optical communications. Components may be "hardened" by including guards against users entering some portion of the network with excessive power. Such measures might involve passing measuring average per-wavelength power and disconnecting users with excessive power. Attackers at the 1530 nm range may be avoided by the use of notch filters. While electronic equalization of the gain in EDFAs might be sufficient to counteract the steady-state effects of gain competition, it may not be adequate to prevent transient attacks. Optically gain-clamped EDFAs offer superior resistance from attacks ([Chi:98]), at the expense of total gain provided. Another aspect of prevention concerns maintaining the semantic security of data in the network, rather than ensuring the physical operation of components. In order to perform cryptography, the timing, format and power of the bits must be known, so that a sequence, generally a pseudo-noise (PN) sequence, may be overlaid on them to mask them from an eavesdropper. Optical cryptography might thus be well-suited to a TDM system. While streams of data might be individually encrypted before being multiplexed onto an

[1] This work was funded by DARPA at the MIT Lincoln Laboratory Advanced Networks group.

0-7803-4947-4/98/$10.00 ©1998 IEEE

optical stream, the ability to encrypt directly high-speed streams gives optical communications greater control over the security of its transmissions. Since the rates which can be achieved by electronics are significantly below those of optical communications, using only multiplexed streams generated by electronic logic restricts the types of PN sequences we may generate. Using optical logic to generate PN sequences directly is an attractive alternative. Reconfigurable Feedback Shift Registers, which leverage off the complexity of electronic controls to exploit the speed of optical logic, generate PN sequences at optical rates with attractive period and complexity features.

Since preventing all attacks may be impossible or economically unfeasible, and since attacks have the potential to metastize in optical networks, **detecting and localizing** attacks is useful. Detection in optical comunications is particularly difficult in the case of transparent networks. Lack of electronic regeneration avoids electronic bottlenecks, but removes checks on the integrity of the data at network nodes. If the data is only checked at the periphery of an optical portion of the network, latency in the network and its peripheral nodes may entail that many bits may be affected before appropriate action can be undertaken by the network management. Current supervisory methods are designed to detect failures, e.g. EDFA failures or fiber cuts. Such methods may be thwarted by attackers seeking to disrupt service. Most current supervisory methods fall in two main categories: statistical tests and methods relying on measurements of supervisory signals. The first category includes such techniques as power detection, OSAs and BERTs. The second encompasses pilot tones and OTDRs. The first category suffers from the fact that many attacks, such as sporadic attacks or attacks which affect the integrity of the data without changing its statistics, e.g. flipping bits in a random sequence, will not be detected. The second category suffers from the fact that other attacks may occur without affecting the probe signals, e.g. coherent crosstalk in wavelength routers would not affect an out of-band pilot tone. Checking the integrity of data node by node at transparent optical nodes may be achieved by using all-optical comparators ([MCS:98]). Not only must individual nodes be able to realize whether or not they have been attacked, but in order to prevent reaction to the artifacts of a single spreading attack, the alarms generated by individual optical nodes must be processed to allow for localization. A distributed algorithm which processes alarms in downstream direction avoids the possibility of incorrect diagnosis due to race conditions in the network ([BMC:98]).

Finally, in case of attacks which present a significant threat to the operation of optical communications, reaction to attacks is required. Reaction which depends on extensive software processing may be desirable for long-term solutions but will not ensure rapid response in ultrafast communications. For this reason, existing high-speed communications systems, such as SONET/SDH, use automatic recovery by providing dual-fed communications with automatic switching between the two or by single-fed recovery using automatic rerouting onto dedicated back-up channels. These approaches are attractive for all-optical networks, also. However, for security reasons as well for economical network planning, the usual SONET/SDH building blocks of rings and diversity protection may be replaced by mesh networks. In such networks, the protection of multicast applications, such as dissemination of video or other high-bandwidth applications to many users, is of particular interest. Indeed, multicast applications are easily implemented in optics by simple splitting and amplification. While SONET offers an useful framework for recovery in optical systems, WDM systems with single-fed loop-back protection differ in several important aspects from SONET systems. In particular, WDM-based recovery, where wavelengths back up wavelengths, differs from SONET fiber-based recovery and cannot be performed by the same techniques.

Acknowledgements: The author wishes to acknowledge the contribution of Dr. R. Barry, Dr. R. Bergman, Pr. A. Chan, S. Chan, Dr. V. Chan, Dr. S. Chinn, Dr. S. Finn, Pr. R. Gallager, Dr. K. Hall, D. Marquis, Dr. J. Moores, S. Parikh, Dr. K Rauschenbach and P. Saengudomlert.

Bibliography.

[BMC:98] R. Bergman et al., "Distributed Algorithms for Attack Localization for All-Optical Networks", *1998 Network and Distributed System Security Symposium*, sponsored by the Internet Society.

[Chi:98] S.R. Chinn, "Simplified Modeling of Transients in Gain-Clamped Erbium-Doped Fiber Amplifiers", *JLT*, vol. 16, no. 6, June 1998.

[MCS:98] M. Médard et al., "Attack Detection in All-Optical Networks", *OFC 98.*

[MCM:98]] M. Médard et al., "Ultrafast Cryptography Using Optical Logic in Reconfigurable Feedback Shift Registers", *SPIE Proceedings*, November 1997, Dallas, Texas.

[MMBF:97] M. Médard et al., "Security Issues in All-Optical Networks", IEEE Network Mag., May 1997.

[MMFB:98] D. Marquis et al., "Physical Security Considerations in All-Optical Networks", *SPIE Proceedings*, November 1997, Dallas, Texas.