Two Dimensional Encrypted Optical Steganography Based on Amplified Spontaneous Emission Noise

Ben Wu, Zhenxing Wang, Bhavin J. Shastri, Yue Tian, and Paul R. Prucnal
Lightwave Communications Laboratory, Department of Electrical Engineering, Princeton University,Princeton, New Jersey 08544, USA
benwu@princeton.edu

Abstract: We demonstrate an optical steganography method with two dimensional encryption to dramatically improve the privacy of optical networks. The transmitted stealth signal carried by noise is secretly hidden under the public channel.
OCIS codes: (060.2330) Fiber optics communications; (060.4785) Optical security and encryption.

1. Introduction

The aim of optical steganography is to hide signals in the public fiber optic communication channels. The hidden signal is called the stealth channel [1,2]. We have recently developed a method of using amplified spontaneous emission (ASE) noise as the carrier of the stealth channel [3]. With the optical spectrum identical to the noise that originally exists in the system, an ASE carried signal can be secretly hidden in the public channel. However, if we assume that the eavesdropper suspects the stealth channel exists, he/she can employ a scanning technique to find and track the key and interpret the stealth channel. Therefore, the key space needs to be large enough to prevent the eavesdropper from tracking the key.

In this paper, we propose a method to encrypt the modulated ASE noise in a two dimensional key space. The expansion to two dimensions increases the key space in a geometrical progression. The first dimension is optical delay. Benefiting from the short coherence length of the ASE noise, the delay length has to be exactly matched at the receiver to demodulate the data. The second dimension is dispersion. Extra dispersion is deliberately added at the transmitter of the stealth channel. Without knowing the amount of dispersion used at the transmitter, the eavesdropper has to search for different values to match the dispersion. Moreover, the two dimensions are orthogonal, which means finding the matching condition in only one dimension does not give any hint to the stealth channel. The stealth channel can only be detected when both optical delay and dispersion are matched.

2. Experiment setup

The structure of the stealth channel is a Mach-Zehnder interferometer (Fig. 1). The carrier for the stealth channel is ASE noise that comes directly from an EDFA. Phase modulation is used for the stealth channel. Because the coherence length of ASE noise is only 372μm (as detailed in the next paragraph), the optical path lengths of the interferometer 1→3 and 2→4 have to be exactly matched in order for the data to be demodulated. The length difference between path 1 and 2 is 6m, and the eavesdropper needs to search this entire difference to find a window of 372μm and demodulate the signal. This forms the first key pair at the transmitter and receiver. The second key pair is the extra dispersion introduced at the transmitter of the stealth channel. The extra dispersion flattens the rising and trailing edges of the modulated signal. To receive the signal, dispersion compensation has to be used to generate the same amount of dispersion with opposite sign. In this paper, we use single mode fiber and dispersion compensating fiber to get extra dispersion. To achieve larger dispersion, photonic crystal fiber can be used [4].

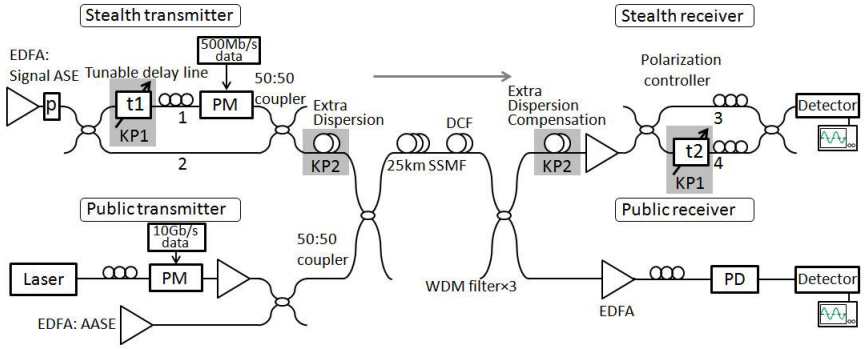

Fig. 1 Experiment Setup (KP: key pair; EDFA: erbium-doped fiber amplifier; P: polarizer; ASE: amplified spontaneous emission; PM: phase modulator; PD: phase demodulator; SSMF: standard single mode fiber; DCF: dispersion compensation fiber; WDM: wavelength division multiplexer).

3. Results and analysis

The BER measurements of the stealth channel show that the BER reaches a minimum of 10^{-9} when both the dispersion and optical delay are matched (Fig. 2(a)). The BER increases dramatically when one of the matching conditions is not satisfied. To measure the coherence length of ASE noise, we scan the length difference between path 3 and 4 at a constant speed and detect the optical power at the receiver (Fig. 1). Constructive and destructive interference is obtained within the coherence length (Figs. 2(b) and (c)), which is 372μm measured from the full width at half maximum of the peak in Fig. 2 (b). If the optical delay difference is larger than the coherence length, the phase modulated data cannot be received.

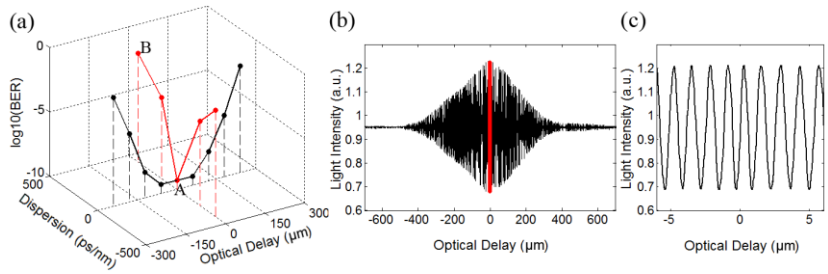

Fig. 2 (a) BER measurement at different dispersion and delay (b) Coherence peaks for the ASE (c) Enlarged view of the red region in (b)

The eye diagrams of the stealth channel show that even if the optical delay is matched, the extra dispersion still prevents the eavesdropper from detecting the stealth channel. When the matching condition is disturbed and 410ps/nm extra dispersion is introduced, the eye opening becomes smaller (Figs. 3(a) and (b)). When the extra dispersion is increased to 820ps/nm, the signal noise ratio degrades to the noise floor (Fig. 3(c)). The stealth channel can be buried further by increasing the bit rate. At 2Gb/s, only noise exists with 410ps/nm extra dispersion. When the extra dispersion goes up to 820nm/ps at 2Gb/s, the received signal is exactly same as ASE noise without modulation (Figs. 2(f) and (g)), which means the eavesdropper cannot detect the existence of the stealth channel. Our measurements show that at 2Gb/s, the BER of the stealth channel can still reach 10^{-4}, which can be recovered by the forward error correction with Reed-Solomon codes.

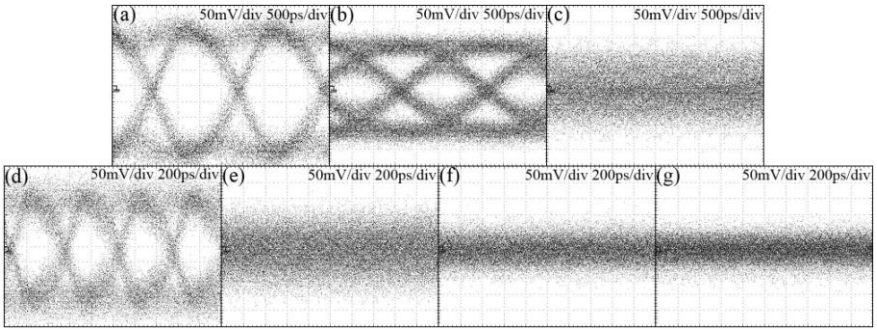

Fig. 3 Eye diagram for (a) 500Mb/s with dispersion matched, which correspond to point A in Fig. 2(a) (b) 500Mb/s with 410ps/nm extra dispersion, which correspond to point B in Fig. 2(a) (c) 500Mb/s with 820ps/nm dispersion (d) 2Gb/s with dispersion matched (e) 2Gb/s with 410ps/nm extra dispersion (f) 2Gb/s with 820ps/nm extra dispersion (g) ASE noise without modulation

4. Conclusion

We propose and experimentally demonstrate a two dimensional encryption method to improve the security of a steganography system based on ASE noise. The key space is dramatically increased. Our experiment results show that without matching both the optical delay and dispersion, the stealth channel can neither be detected nor interpreted by the eavesdropper.

Reference

[1] B. Wu, and E. E. Narimanov, "A method for secure communications over a public fiber-optical network," Opt. Express **14**, 3738-3751 (2006).

[2] Z. Wang, and P. R. Prucnal, "Optical steganography over a public DPSK channel with asynchronous detection," IEEE Photon. Technol. Lett. **23**, 48-50 (2011).

[3] B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, "Optical steganography based on amplified spontaneous emission noise," Opt. Express **21**, 2065-2071 (2013).

[4] M. A. Islam and M. S. Alam, "Design optimization of equiangular spiral photonic crystal fiber for large negative flat dispersion and high birefringence," J. Lightwave Technol. **30**, 3545-3551(2012).