Phase-Mask Covered 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: Phase mask encryption is proposed to improve the transmission privacy of an optical steganography system. The stealth signal carried by amplified spontaneous emission noise is encrypted by a fast changing code.

1. Introduction

Optical steganography aims at transmitting stealth signals in public fiber optic communication channels without being detected [1,2]. We have recently proposed and demonstrated a method of using amplified spontaneous emission (ASE) noise to carry the stealth channel data [3]. Benefitting from the short coherence length of the ASE noise, the optical delay length can be the key between the transmitter and the receiver. However, in the demonstration, the delay lengths are controlled by mechanical delay lines, which limit the rate of changing the key. Using a fast scanning technique, an eavesdropper can find the delay length before it changes. Therefore, the stealth channel needs to be further protected by a fast changing key.

In this paper, we propose a method to encrypt each bit in the stealth channel with phase mask codes which can be changed at the bit rate of the stealth channel. The eavesdropper needs to match both the delay length and the code of the phase mask in order to receive the data from the stealth signal. The phase mask code is encrypted on the stealth channel by a pair of phase modulators at the transmitter and the receiver. The code can be changed quickly and easily by switching to another binary sequence to drive the phase mask. Benefiting from the noise property of ASE, the phase mask encrypted data is hidden under the ASE noise.

2. Experimental setup

Phase modulation is used for both the stealth channel and the phase mask (Fig. 1 (a)). The bit rate of the stealth channel is 250Mb/s while the bit rate of the phase mask is 4Gb/s, so each stealth bit is divided into 16 chips. The carrier for the stealth channel is ASE noise with coherence length of 372μm [3]. The optical path lengths of the interferometer 1→3 and 2→4 have to be exactly matched in order to demodulate the stealth channel (Fig. 1(a)). The phase mask further protects the stealth channel data. If the eavesdropper tries to receive the code of the phase mask, the high frequency noise from ASE, which overlaps with the phase mask bit rate, can protect the code from being detected. If the eavesdropper uses a low pass filter to remove both high frequency noise and the phase mask, because the stealth bits are already corrupted by the phase mask, the amplitude of the stealth bit is only 20%-25% of its original value (Fig. 1(b)) and merged into the noise from the ASE.

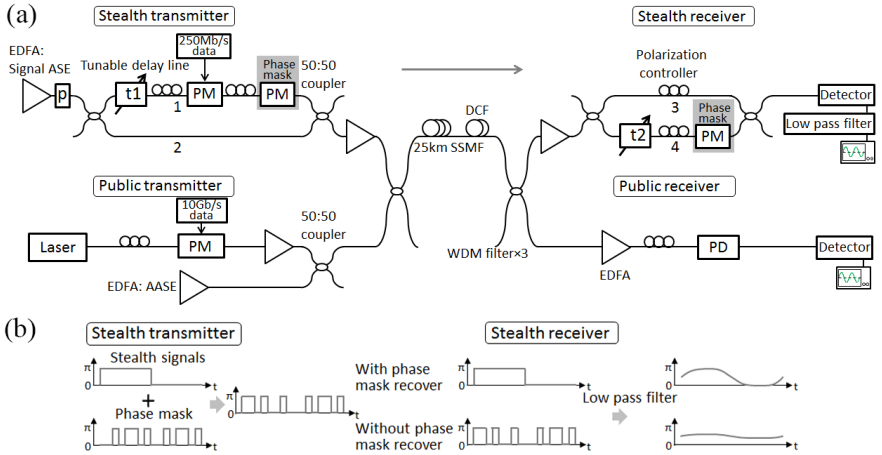

Fig. 1. Experimental Setup (EDFA: erbium-doped fiber amplifier; P: polarizer; ASE: amplified spontaneous emission; PM: phase modulator; PD: phase demodulator; SSMF: standard single mode fiber; DCF: dispersion compensation fiber; WDM: wavelength division multiplexer). (b) Schematic diagram of the experiment, only 8 chips are drawn for each bit

978-1-4577-1507-5/13/$26.00 ©2013 IEEE

3. Results and analysis

The optical spectrum of the ASE carrying the stealth signals covers a wide range from 1520nm to 1560nm (Fig. 2 (a)). This is identical to the ASE noise that originally exists in the public channel and hides the stealth channel in the spectral domain. The wide spectrum enables a short coherence length, so the delay lengths need to be matched in order to detect the stealth channel, which hides the stealth channel in the time domain.

The radio frequency spectrum shows the noise property of the ASE (Fig. 2 (b)). The flat spectrum indicates the existence of both the low frequency noise and the high frequency noise. An increase in the bit rate will lower the signal to noise ratio (SNR). Our experiment shows that the bit error rate (BER) is higher than 0.05 at a bit rate of 4Gb/s (Fig. 3 (c)). By changing the code rapidly, even if the eavesdropper guesses part of the code correct, he/she cannot follow the changes in the code. Our simulation of the 16 chip code shows that more than 5000 codes are available to reduce the stealth eye opening to less than 25% of its original amplitude.

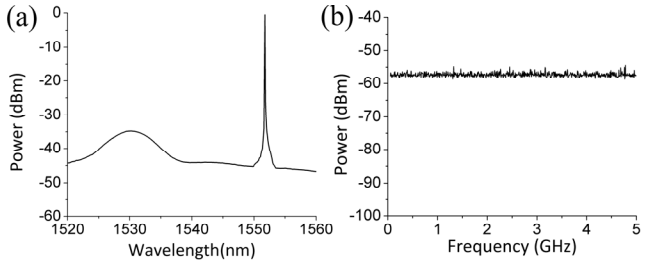

Fig. 2 (a) Optical spectrum of ASE and public channel (b) RF noise spectrum of ASE

The eye diagrams of the stealth channel show that even if the optical delay is matched, the phase mask still protects the data of the stealth data from being detected. Without information about the phase mask code, the code cannot be separated from the high frequency noise (Fig. 3 (c)), so the eavesdropper cannot detect the code directly. To achieve the best SNR, the receiver needs a low pass RF filter to remove the high frequency noise. In our experiment, a low pass filter with 3dB cut-off frequency 600MHz is used at the receiver. A BER of 2×10^{-7} is achieved in this way (Fig. 3 (a) and (d)). If the eavesdropper uses the same receiver without recovering the phase mask, the low pass filter will average both the stealth data and the phase mask code and reduce the amplitude of the eye diagram to 25% of its original value, which is buries the stealth data into the ASE noise (Fig. 3 (b) and (e)).

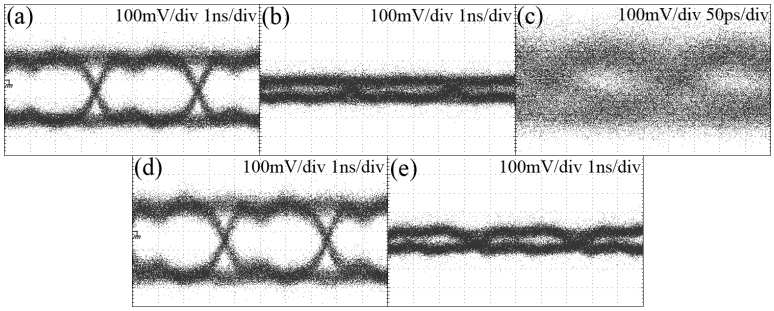

Fig. 3 (a) Eye diagram of code 1010101010101010 with phase mask recovery (b) Eye diagram of code 1010101010101010 without phase mask recovery (c) Eye diagram of 4G/s bit rate (d) Eye diagram of code 1101010100101010 with phase mask recovery (e) Eye diagram of code 1101010100101010 without phase mask recovery

4. Conclusion

We propose and experimentally demonstrate a phase mask encryption method to improve the security of a steganography system based on ASE noise. The changing delay length protects the stealth channel from being detected. The fast-changing phase mask code mixes the stealth channel with noise and protects the stealth data from being demodulated.

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).