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

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)).



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

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