Compact Optical Steganography Based on Amplified Spontaneous Emission Noise

Ben Wu, Matthew P. Chang, Bhavin J. Shastri, Alexander N. Tait, and Paul R. Prucnal
Lightwave Communications Laboratory, Department of Electrical Engineering, Princeton University,Princeton, New Jersey 08544, USA
benwu@princeton.edu

Abstract: We experimentally demonstrate a compact optical steganography method using chirped fiber Bragg gratings. The stealth signals are carried by wide band amplified spontaneous emission noise, which has strong dispersion effect for pulse stretching.

1. Introduction

Optical stealth transmission carried by amplified spontaneous emission (ASE) has been proved to be an effective way to hide the signal in both the time domain and the spectral domain [1]. Since ASE noises widely exist in the fiber optics networks, adding the stealth channel to the network does not introduce extra power consumption. The spectrum of the stealth channel is exactly the same as the ASE noise that originally exists, so the eavesdropper cannot detect the existence of the stealth channel by identifying the spectrum.

In the time domain, the stealth channel is protected by the short coherence length property of the ASE noise and the previous approach uses homodyne detection to recover the stealth signal. The homodyne detection hide the signal in the time domain, however, interferometer structure over fiber is required in the homodyne detection and this structure is sensitive to temperature and mechanical vibrations [2]. Although the system performance can be improved by providing temperature control and mechanical stabilization, for commercial applications, a more robust and compact design is needed.

In this paper, we protect the stealth channel by chirped fiber Bragg gratings (CFBG) generated dispersion. The stealth channel does not have interferometer structure over fiber and is not sensitive to temperature and mechanical vibration. The stealth bit is stretched by dispersion in the time domain. The stretched signal has its amplitude low enough to be merged into the noises. The ASE noise has much wider spectrum bandwidth than laser, so the dispersion effect is stronger [3]. With the CFBG as the dispersion component, the stealth transmitter and receiver can be packaged in a relatively smaller footprint. The amount of dispersion generated from CFBG is used as the key for hiding and recovering the stealth channel. The stealth channel is carried ASE noise accumulated from the public channel and thus does not cause extra power cost.

2. Experimental setup

The experimental setup is shown in Fig. 1. The signal carrier of the stealth channel comes from the accumulated ASE noise of the public channel. A CFBG with circulator is used to filter part of the ASE spectrum from the public channel. The bandwidth of the CFBG is 0.9nm and the center wavelength is 1530nm. The filtered ASE noise is first amplified and then passed through an intensity modulator, which adds the stealth signal with the data rate of 3Gb/s. A PRBS with length 2^{31}-1 is used as the stealth signal. Another CFBG with the same bandwidth as the filter CFBG is used to generate the 2034ps/nm dispersion. An erbium doped fiber amplifier (EDFA) is used to compensate the signal attenuation from the intensity modulator and CFBG. We place the EDFA before the intensity modulator, so the ASE generated from this EDFA is also modulated and carry signals. Another EDFA is used in the stealth transmitter for public channels. This EDFA compensates the signal attenuation of the public channel from the CFBG and optical combiner. After the stealth channel is combined with the public channel, the spectrum of the combined signal is the same as the spectrum of public channel and system noise before the stealth channel is added [4]. The combined signals are sent over an optical link of a 25km single mode fiber with dispersion compensating fiber (DCF).

The stealth receiver uses a CFBG with the same bandwidth and inverse dispersion to the CFBG at the transmitter to filter the stealth channel and compensate for dispersion (Fig. 1). The recovered stealth signal is first amplified by an EDFA and then received by a photo diode. Compared with traditional public channels in the fiber optics networks, the only extra component in the stealth channel is a pair of CFBG in the transmitter and receiver. The CFBG used in the experiment is less then 20cm long and can be easily packaged without the requirement of temperature control and mechanical stabilization. The stealth channel can be built to be more compact and lower cost than the public channel because the stealth channel does not need a separate optical power source.

978-1-4799-7465-8/15/$31.00 ©2015 IEEE

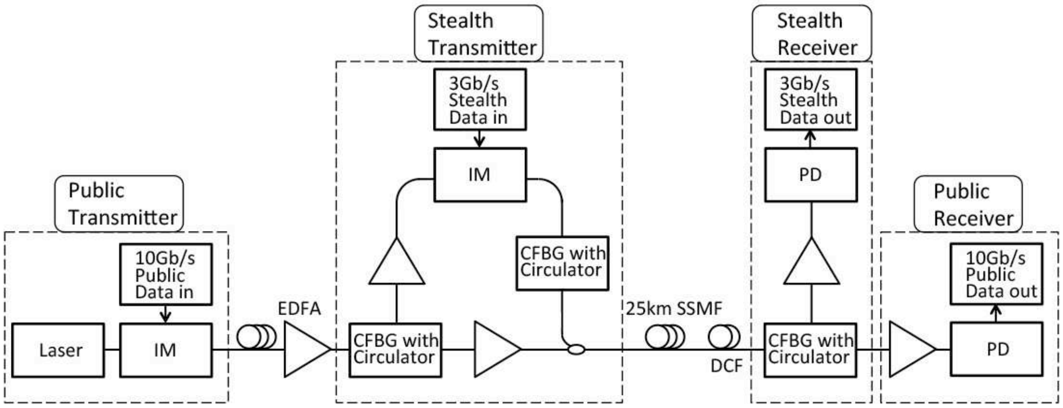

Fig. 1. Experimental Setup (IM: Intensity Modulator; EDFA: erbium-doped fiber amplifier; CFBG: chirped fiber Bragg grating; SSMF: standard single mode fiber; DCF: dispersion compensating fiber; PD: photo diode).

3. Results and analysis

Fig. 2 shows the measured eye diagrams with and without the dispersion matched. The measurement shows that when the dispersion is matched, the stealth channel has a clear eye diagram (Fig. 2(a)) and when the dispersion is not matched with 2034ps/nm extra dispersion, the stealth channel is pure noise and even the period of the stealth signal cannot be identified (Fig. 2(b)).

To protect the system with only dispersion gives the stealth channel less protection compared with the setup using homodyne detection. However, to remove the requirement of optical delay matching enables the system to be less sensitive to mechanical vibrations and temperature fluctuations. There is a tradeoff between perfect security and system complexity. The aim of this paper is to build a compact stealth transmitter and receiver pair that is robust and can be made as a commercial product.

The stealth transmitter and receiver and be plugged into the public network without affecting the performance of the existing public channels. This technique can be applied by local area network (LAN) providers or the industrial partners that require private communication between data centers.

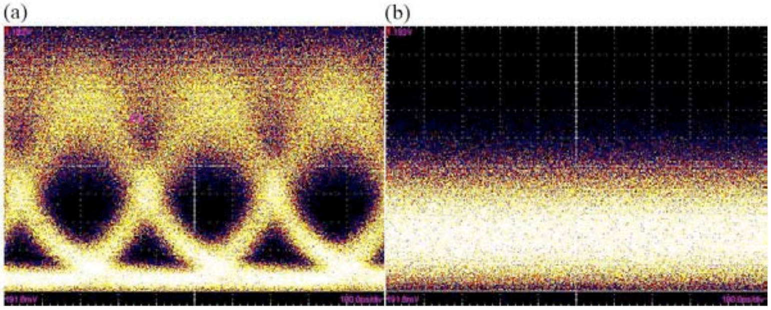

Fig. 2. Eye diagrams of the stealth channel with (a) and without (b) the dispersion matched.

4. Conclusion

We proposed and experimentally demonstrated an pair of compact stealth transmitter and receiver. The aim is to build a stealth channel with compact components so the stealth channel can be commercialized. The stealth channel uses the accumulated ASE noise from the public channel as the signal carrier and does not need extra power consumption. The stealth channel is effectively protected by the dispersion generated by the CFBG, which has a small physical size and is easy to be packaged in the stealth transmitter and receiver.

Reference

[1] 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).

[2] S.Yin, P. B. Ruffin,and F.T.S.Yu, *Fiber Optic Sensors* (CRC, 2008), Chap. 2.

[3] E. Desurvire, "Analysis of noise figure spectral distribution in erbium doped fiber amplifiers pumped near 980 and 1480 nm," Appl. Opt., 29, 3118-3125 (1990).

[4] B. Wu, A. N. Tait, M. P. Chang, and P. R. Prucnal, "WDM optical steganography based on amplified spontaneous emission noise," Opt. Lett. **39**, 5925-5928 (2014).