Dispersion Deployment and Compensation for Optical Steganography Based on Noise

Ben Wu, *Student Member, IEEE*, Matthew P. Chang, Bhavin J. Shastri, *Member, IEEE*, Phillip Y. Ma, and Paul R. Prucnal, *Fellow, IEEE*

Abstract T

I. Introduction

PITCAL steganography based on noise has been experimentally demonstrated to effectively hide a stealth channel in both the spectral domain and the time domain [1], [2]. The stealth channel is carried by amplified spontaneous emission (ASE) noise emanating from erbium doped fiber amplifiers (EDFAs), and has the same spectrum as the amplifier noise in the public network. In the time domain, because the ASE noise has a short coherence length, the optical delays at the transmitter and receiver have to be exactly matched in order to detect the existence of the phase modulated stealth signal. The optical delay provides a large key space for the transmitter and hides the stealth channel in the time domain [1].

The wide spectrum and random phase of ASE noise are advantages for hiding the stealth signals effectively. However,

Fig. 2. Experimental measurement (black dots) and theoretical fitting of a rising edge in the stealth channel (black curve). (a) Without extra dispersion; (b) With extra dispersion.

of the interferometer have to be matched in order to receive the phase-modulated data [1]. Extra dispersion is applied to the stealth transmitter to study effect of dispersion on the stealth channel. The extra dispersion is generated by SSMF and DCF. The carrier of the stealth channel is ASE noise and comes from an EDFA without input. The stealth signal is added to the stealth channel by phase modulation. Both programmed data and a pseudorandom binary sequence (PRBS) with length 2^{31}-1 are tested as the signal in the stealth channel. The data rate of the stealth channel is 500Mb/s. The signals from the stealth transmitter are sent over 25km SSMF with the corresponding DCF. The stealth channel can be transmitted through longer distance in the public network by sharing the optical amplifiers of the public channels [8].

III. Experimental Results and Discussion

A. Effect of Dispersion on the Stealth Signal

The stealth channel has a larger optical bandwidth compared with the public channel and thus the effect of dispersion is much stronger on the stealth channel than on the public channel. A rising edge, formed from eights bits of continuous “0”s followed by eight bits of continuous “1”s, is used to quantify the effect of dispersion on the stealth channel. The stealth signal is received by a photodiode with bandwidth of 12GHz. The extra dispersion at the stealth transmission is generated by 25km SSMF with 410ps/nm. No low pass electric filter is used at the electric output of the photodiode which could preclude the delay effect from the frequency response of the electric filter. The black grainy dots in the background are the measured signal (Fig. 2). The measured signal with and without 410ps/nm dispersion shows that a sharp rising edge contorts to a slope when extra dispersion is applied.

i32J 0d..(2421..(0.3rent.8)80)2n3377o]TJ 61.(r)8sdn7

adding time delays according to (1) and (2). The vertical axis of the calculated distribution is same as the measured result and shows the received voltage with the units of 50mV/div. The horizontal axis of the calculated distribution shows the probability density of the received signals with arbitrary units.

When the dispersion is compensated, a clear eye diagram is achieved and the experimentally measured bit error rate (BER) is 10^{-9}. The probability density also shows two separate peaks for “1” and “0” (Fig. 3(a)). When 410ps/nm of extra dispersion is applied (Fig. 3(b)), the eye opening narrows and becomes noisier, and the corresponding measured BER increases to 3×10^{-2} [5]. The two peaks of

applied by the eavesdropper has to be accurate enough to indicate the existence of the signal. The accuracy of the dispersion matching condition depends on the data rate of the stealth channel (Fig. 4(b)). The blue dash-dot line in Fig. 4(b) is the minimum amount of dispersion required to hide the signal. In the area between the blue dash-dot line and the red dashed line (Fig. 4(b)), eavesdropper cannot decrypt the signal but begins to suspect the existence of the stealth channel.

The dispersion adds another dimension to the key space of the stealth channel. An eavesdropper has to find the right optical delay first [1], before he/she can use a brute-force approach to search for the dispersion. Both the optical delay and dispersion have to be matched in order to detect the existence of the stealth channel and these two independent parameters can be changed while the eavesdropper does the search.

IV. Conclusion

We experimentally demonstrated the effect of dispersion on optical steganography based on ASE noise, and deployed the dispersion effect to improve the security of the stealth channel. Based on the experimental results, we found the bandwidth of ASE-carried signal is 100 times wider than the laser-carried signals, so the ASE carried signal has a much stronger dispersion effect. We calculated the probability distribution of the received stealth signal when different amounts of dispersion are applied. The shape of the probability distribution divides the amount of dispersion in to three regions and guides the operation of the stealth channel. The regions are: the dispersion compensation tolerance region, which shows the maximum dispersion that a stealth channel can tolerate with FEC; the optical encryption region, which encrypts the stealth data as a noisy signal; and optical steganography region, which hides the stealth data by making the data have a similar probability distribution as pure noise.

References

[1] B. Wu *et al.*, "Optical steganography based on amplified spontaneous emission noise," *Opt. Exp.*, vol. 21, no. 2, pp. 2065–2071, Jan. 2013.

[2] B. Wu, Z. Wang, B. J. Shastri, M. P. Chang, N. A. Frost, and P. R. Prucnal, "Temporal phase mask encrypted optical steganography carried by amplified spontaneous emission noise," *Opt. Exp.*, vol. 22, no. 1, pp. 954–961, Jan. 2014.

[3] E. Desurvire, "Chapter 5 gain, saturation and noise characteristics of erbium-doped fiber amplifiers," in *Erbium-Doped Fiber Amplifiers, Principles and Applications*, 2nd ed. Hoboken, NJ, USA: Wiley, 2002, pp. 355–357.

[4] E. Desurvire, "Analysis of noise figure spectral distribution in erbium doped fiber amplifiers pumped near 980 and 1480 nm," *Appl. Opt.*, vol. 29, no. 21, pp. 3118–3125, Jul. 1990.

[5] B. Wu, Z. Wang, B. J. Shastri, Y. Tian, and P. R. Prucnal, "Two dimensional encrypted optical steganography based on amplified spontaneous emission noise," in *Proc. CLEO*, Jun. 2013, pp. 1–2, paper AF1H.5.

[6] M. A. Islam and M. S. Alam, "Design optimization of equiangular spiral photonic crystal fiber for large negative flat dispersion and high birefringence," *J. Lightw. Technol.*, vol. 30, no. 22, pp. 3545–3551, Nov. 15, 2012.

[7] I. B. Djordjevic, A. H. Saleh, and F. Küppers, "Design of DPSS based fiber Bragg gratings and their application in all-optical encryption, OCDMA, optical steganography, and orthogonal-division multiplexing," *Opt. Exp.*, vol. 22, no. 9, pp. 10882–10897, Apr. 2014.

[8] B. Wu, B. J. Shastri, and P. R. Prucnal, "System performance measurement and analysis of optical steganography based on noise," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1920–1923, Oct. 1, 2014.

[9] G. P. Agrawal, "Chapter 2 optical fibers," in *Fiber-Optic Communication Systems*