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*— The system tolerance to the dispersion of optical steganography and the deployment of dispersion to enhance secure transmission has been experimentally demonstrated and theoretically studied. Since the stealth signal is carried by amplified spontaneous emission noise, which has a much wider bandwidth compared with the laser carrier, the stealth channel is more sensitive to dispersion and has less tolerance to the uncompensated dispersion. On the other hand, the dispersion effect in the stealth channel can be employed to hide the stealth signal in the time domain. The extra dispersion at the transmitter and the receiver functions as a key pair for the optical encryption and the optical steganography.**

***Index Terms*— Amplified spontaneous emission, optical fiber communication, optical steganography.**

I. INTRODUCTION

OPITCAL 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, as the spectrum of the ASE noise is more than a 100 times wider than the bandwidth of public channels, the stealth channel is also a 100 times more sensitive to dispersion than the public channels. The spectral width of ASE noise is around 10 nm [3], [4], which is about 1.3THz in terms of frequency. In comparison, a standard public channel has a bandwidth of 10GHz. A wider bandwidth results in a larger optical delay with the same amount of dispersion, so the stealth channel has less tolerance to uncompensated dispersion.

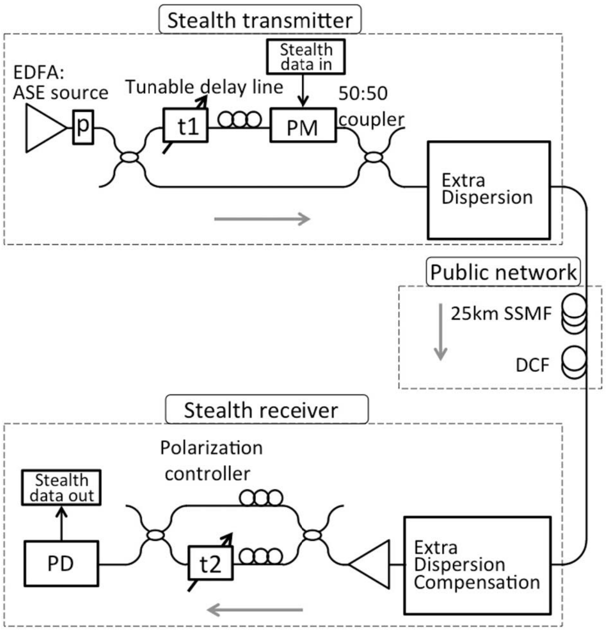

Fig. 1. Experiment setup (EDFA: erbium doped fiber amplifier; ASE: amplified spontaneous emission; PM: phase modulator; SSMF: Standard single mode fiber; DCF: dispersion compensation fiber; PD: photo diode).

While uncompensated dispersion is undesirable for long haul transmission, it can be employed to enhance the security of the stealth channel. Dispersion expands the signal making it noise-like, which adds another dimension to the key space of the stealth channel [5]. Even if the eavesdropper matches the optical delay, he still needs to find the right dispersion in order to recover the signal. The extra dispersion used to encrypt and hide the stealth channel can be achieved by adding the extra length of standard single mode fiber (SSMF), dispersion compensation fiber (DCF), chirped fiber Bragg grating [6], or photonic crystal fibers [7].

In this letter, we study the effect of dispersion on the stealth channel. Based on experimental results, we calculate the tolerance of the stealth channel to the uncompensated dispersion and the required amount of dispersion for hiding the signal. The quantitative criterion is summarized for the required dispersion at different data rates.

II. EXPERIMENTAL SETUP

The experimental setup includes a stealth transmitter and receiver pair (Fig. 1). The transmitter and receiver pair is a Mach-Zehnder interferometer and because the ASE noise has short coherent length, the optical delays between the two paths

Manuscript received September 28, 2015; revised October 22, 2015; accepted October 26, 2015. Date of publication November 3, 2015; date of current version January 13, 2016.

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: benwu@princeton.edu; mpchang@princeton.edu; bshastri@princton.edu; yechim@princeton.edu; prucnal@princeton.edu).

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LPT.2015.2496957

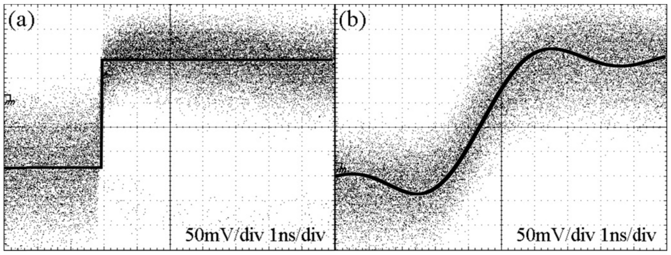

Fig. 2. Experimental measurement (black dots) and theoretical fitting of a rising edge in the stealth channel (black curve). (a) Without extra dispersion; (b) With extra dispersion.

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.

To precisely measure the slope in the time domain, we fit the measured results with theoretical calculations (shown as the black curves in Fig. 2). The theoretical calculation considers the same data sequence with eights bits of continuous “0”s followed by eight bits of continuous “1”s. We use eight bits instead of one bit to give the delayed signal enough time to reach it full amplitude. A low pass filter is used to generate the slope of the rising edge. Since the delay in the time domain corresponds to the cut off frequency in the frequency domain with relation:

$$\Delta T = \frac{1}{\Delta f} \tag{1}$$

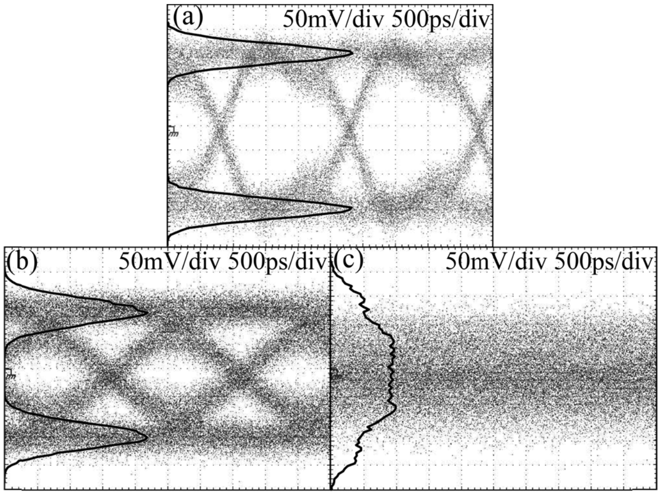

Fig. 3. Experimental measurement of the eye diagram (black dots) and the corresponding theoretically calculated probability distribution of the received signals (black curves). (a) Dispersion is matched. (b) 410ps/nm of extra dispersion. (c) 820ps/nm of extra dispersion.

where ΔT is the time delay and Δf is the cut off frequency. The time delay is optimized to fit the theoretically calculated curve to the measured results (Fig. 2(b)).

The theoretical fit shows that the 410ps/nm dispersion generates a $\Delta T = 3.6$ns delay to a rising edge of the stealth channel. The optical bandwidth of the ASE spectrum can be calculated as [9]:

$$\Delta \lambda = \frac{LD}{\Delta T} \tag{2}$$

where $L = 25$km is the fiber length, D=16.4ps/nm-km is the dispersion parameter and $\Delta \lambda$ is the optical bandwidth of the ASE noise, which is calculated as 8.8nm. Because the power of the ASE spectrum mainly comes from the peak around 1530nm with full width half maximum around 10nm, the result in (2) matches with the bandwidth of ASE in [8]. The 8.8nm equals 1.1THz in the unit of frequency. Compared with the public channel, which has an exemplary bandwidth of 10GHz, the ratio of bandwidth between the stealth channel and public channel is:

$$\frac{1.1THz}{10GHz} = 110 \tag{3}$$

Since the bandwidth of the stealth channel is 100 times wider than the public channel, the effect of dispersion on the stealth channel is also 100 times stronger than on the public channel.

The effect of dispersion on the stealth channel is further experimentally studied by using a 2^{31}-1 PRBS as the stealth signal with different amounts of dispersion applied. The data rate of the stealth signal is 500Mb/s, and an electric low pass filter with 3dB cutoff frequency 600MHz is used to remove the high frequency noise. The eye diagrams shown in black are the experimental measurements (Fig. 3); the black curves are the theoretically calculated distribution of the received signal when the eye has the maximum opening in each data bit. The theoretical calculation use PRBS with length 2^{15}-1 as the stealth signal. The signals in the center of each bit are sampled and the distributions of the sampled signals are calculated. Different amounts of dispersion are simulated by 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 the probability density also become closer and wider. When 820ps/nm of extra dispersion is applied, there is no eye opening, and the BER cannot be measured. The two peaks of the probability density merge, and the received signal is completely noisy.

B. Deployment and Compensation of the Dispersion Effect

The effect of dispersion has to be compensated in order to receive the signal. On the other hand, the strong dispersion of the stealth channel can be deployed to hide the signal from malicious attack. Based on the different amounts of dispersion applied to the stealth channels, we summarized the stealth signals into three cases, which are dispersion compensation tolerance limit, optical encryption and optical steganography (Fig. 4). We theoretically calculate the distributions of the stealth signals when different amounts of dispersion and data rates are applied. The theoretical calculation uses PRBS with length 2^{15}-1 as the stealth signal. Different amounts of dispersion are simulated by adding time delays according to (2). The criteria to separate the different cases are defined based on the BER and the distribution of the received signals (Fig. 4(a)).

The case of dispersion compensation tolerance limit is indicated by black solid curves in both Figs. 4(a) and 4(b). To receive a readable signal, the BER has to be lower than the forward error correction (FEC) limit, which is 1.1×10^{-3} using a Reed-Solomon code. The distribution of the received signal is two separate peaks in this case (Fig. 4(a)). The black solid curve in Fig. 4(b) shows the maximum dispersion that the stealth channel can tolerate. The curves in Fig. 4(b) are calculated by scanning the data rate and finding the required dispersion to satisfy the criteria defined by Fig. 4(a).

When the dispersion increases and the BER is higher than the FEC limit, the two peaks in the distribution merge and it first forms a flat region in the middle (Fig. 3(c)) and then becomes one peak with shape similar to a Gaussian distribution (red dashed line in Fig. 4(a)). The eye diagram has no opening and the received signal is completely noisy. Optical encryption is achieved in this case. If the eavesdropper cannot find the right dispersion compensation, he cannot decrypt the data and only receives a noise-like signal. The minimum required dispersion for optical encryption is shown by the red dashed line in Fig. 4(b), which is also the minimum amount of dispersion that enable the distribution to be Gaussian shape.

The received signal for the encrypted signal is completely noisy, however, if the eavesdropper measures the distribution of the received signal, the standard deviation of the encrypted signal (red dashed line in Fig. 4(a)) is much larger than the standard deviation of the ASE noise without modulation (green solid line in Fig. 4(a)). This means although the eavesdropper cannot decrypt the signal, he knows the existence of the signal, which is the drawback of optical encryption [10]. To hide the existence of the stealth channel and achieve optical steganography, the dispersion needs to be increased further, which leads to the distribution of stealth signal (blue dash-dot line in Fig. 4(a)) having a similar shape to the distribution of the pure ASE noise. This minimum amount of dispersion required to achieve optical steganography is shown by the blue dash-dot line in Fig. 4(b). The ASE noise is not considered when calculating the distribution of the stealth signal. The required dispersion for optical steganography at the data rate of 3Gb/s is 1435ps/nm, which is still a practical value. The required dispersion can be decreased by flattening the spectrum of ASE noise, which achieves a wider optical bandwidth [11], [12].

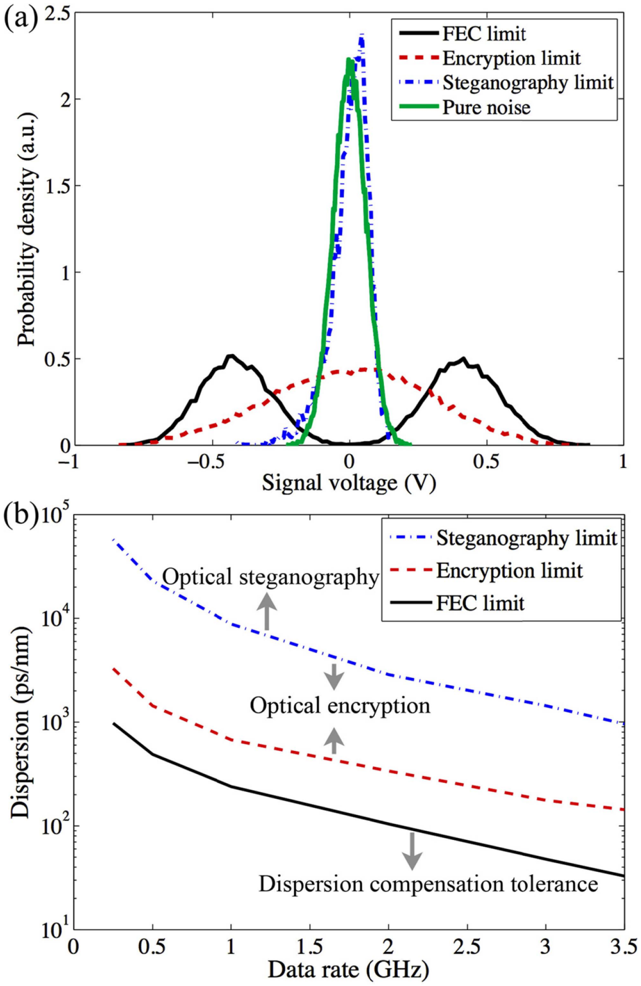

Fig. 4. (a) Theoretical calculation of the distribution of the received stealth signal. (b) Dependence of dispersion limit on the data rate.

C. Secure Analysis

If the eavesdropper uses a brute-force approach to search the right dispersion compensation, the compensated dispersion 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*. Hoboken, NJ, USA: Wiley, 2002, pp. 38–39.

[10] B. Wu, B. J. Shastri, and P. R. Prucnal, "Secure communication in fiber-optic networks," in *Emerging Trends in ICT Security*, B. Akhgar and H. R. Arabnia, Eds. Waltham, MA, USA: Elsevier, 2014, pp. 173–183.

[11] Y. B. Lu, P. L. Chu, A. Alphones, and P. Shum, "A 105-nm ultrawide-band gain-flattened amplifier combining C- and L-band dual-core EDFAs in a parallel configuration," *IEEE Photon. Technol. Lett.*, vol. 16, no. 7, pp. 1640–1642, Jul. 2004.

[12] C. L. Lee and Y. Lai, "Evolutionary programming synthesis of optimal long-period fiber grating filters for EDFA gain flattening," *IEEE Photon. Technol. Lett.*, vol. 14, no. 11, pp. 1557–1559, Nov. 2002.