WDM optical steganography based on amplified spontaneous emission noise

Ben Wu,* Alexander N. Tait, Matthew P. Chang, and Paul R. Prucnal

Lightwave Communication Laboratory, Department of Electrical Engineering, Princeton University, Princeton, New Jersey 08544, USA

**Corresponding author: benwu@princeton.edu*

Received July 9, 2014; revised August 22, 2014; accepted September 18, 2014; posted September 18, 2014 (Doc. ID 214819); published October 10, 2014

We propose and experimentally demonstrate a wavelength-division multiplexed (WDM) optical stealth transmission system carried by amplified spontaneous emission (ASE) noise. The stealth signal is hidden in both time and frequency domains by using ASE noise as the signal carrier. Each WDM channel uses part of the ASE spectrum, which provides more flexibility to apply stealth transmission in a public network and adds another layer of security to the stealth channel. Multi-channel transmission also increases the overall channel capacity, which is the major limitation of the single stealth channel transmission based on ASE noise. The relations between spectral bandwidth and coherence length of ASE carrier have been theoretically analyzed and experimentally investigated.

OCIS codes: (060.2330) Fiber optics communications; (060.4785) Optical security and encryption.
http://dx.doi.org/10.1364/OL.39.005925

Optical steganography has been studied to transmit stealth data in a public network [1–3]. Compared with optical encryption, which encrypts data as unreadable signals but still expose the existence of the signals [4–7], optical steganography hides the very existence of the stealth channel in both time and frequency domains. Without knowing the existence of the stealth channel, the eavesdropper will not try to decrypt the stealth signal. Recently, an optical steganography method based on amplified spontaneous emission (ASE) noise has been theoretically studied and experimentally demonstrated [8–10]. This method uses the amplifier noise that widely exists in fiber optic networks to carry signals. The spectrum of the ASE carrying signal is exactly the same as the spectrum of the original ASE noise, which hides the signal in the frequency domain. Moreover, because the ASE has short coherence length, the eavesdropper cannot detect the phase modulated data without pre-known information of the optical delay, which hides the signal in the time domain.

Optical steganography based on ASE noise effectively hides the stealth signal in the public network; however, the capacity of the stealth channel is limited [8,10]. As the signal is carried by spontaneous emission noise with random phase, the data rate is limited by the noise properties of ASE [10]. The previous approach used the entire ASE spectrum to carry the stealth channel, so the steganography system only has a single channel. To achieve multi-channel and multi-user steganography capabilities, the ASE spectrum must be divided and deployed in a more efficient way.

In this Letter, we propose and experimentally demonstrate a WDM optical steganography system. The stealth signal is carried by a filtered spectrum of ASE noise and multi-channel with different wavelengths is achieved. The multi-channel transmission increases the capacity of the stealth channel dramatically and allows different users to access the steganography system simultaneously. Moreover, using a partial ASE spectrum gives more flexibility to introduce stealth channels to a public network. The stealth channel can only be introduced when cumulative ASE noise in the existing public channel is above a certain power level [10]. Since the ASE power may vary at different wavelengths of the spectrum, stealth channels based on partial ASE spectra could be deployed more efficiently in practice.

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. An optical bandpass filter with central wavelength 1548.5 nm and full width half-maximum (FWHM) 1.1 nm is used to obtain part of the ASE spectrum to feed into the stealth transmitter. An amplifier is used to boost the ASE noise before modulation and to compensate the loss from the stealth transmitter. The modulated ASE noise is then combined with the rest of the ASE noise and public channel for transmission through the public network. At the receiver, the same optical bandpass filter is used to separate the stealth channel from the public channel. The stealth transmitter and receiver form a Mach–Zehnder interferometer [8]. The light path between the modulated ASE and reference ASE at the stealth transmitter has 10 m length difference. To demodulate the stealth data at the receiver, the optical delay (t2) needs to match the 10 m length difference, creating a time-domain key space (Fig. 1). The stealth signal is phase-modulated signal with data rate 500 Mb/s. The public channel is also phase-modulated, with a data rate of 10 Gb/s. The carrier of the public channel is distributed feedback laser with wavelength 1555.3 nm.

The spectra measured before and after adding the stealth channel show that the stealth channel is hidden in the ASE noise spectrum (Fig. 2). Figure 2(a) is the spectrum of public channel with accumulated ASE noise and corresponds to point A in Fig. 1. Figure 2(b) is the stealth channel carried by filtered ASE noise and corresponds to point B in Fig. 1. Figure 3(c) is the combined spectrum of stealth channel, public channel and ASE noise, which corresponds to point C in Fig. 1. Comparing Figs. 2(a) and 2(c), we can see that the stealth channel is well hidden in the public channel noise, which adds another layer of security. The eavesdropper needs to search

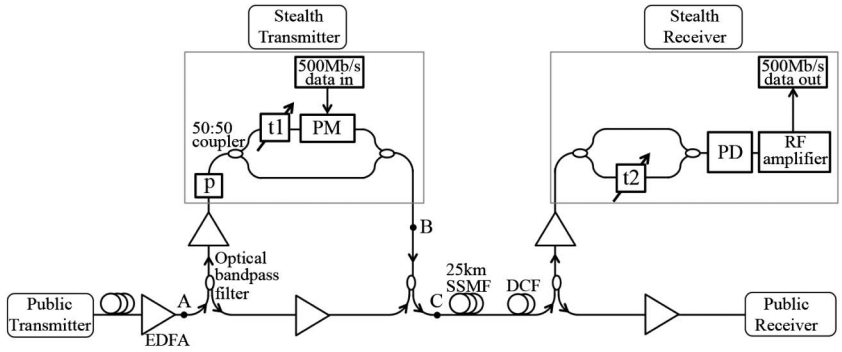

Fig. 1. Experimental setup (EDFA, erbium-doped fiber amplifier; p, polarizer; t, optical time delay; PM, phase modulator; SSMF, standard single mode fiber; DCF, dispersion compensation fiber; PD, photo diode; RF, radio frequency).

for the entire ASE spectrum between 1520 and 1560 nm to find which part carries the stealth signal. To search each part of the spectrum, the eavesdropper needs to scan the optical delay to find the coherence peak [8]. The eavesdropper may perform a blind attack on the system and guess which part of the spectrum carries the stealth channel. If the guessed spectrum is partially overlapped with the spectrum of the stealth channel, the part of spectrum that is not overlapped with the stealth channel will become noise for searching the optical delay. The amplitude of the interference peak for optical delay matching is proportional to the amount of overlap between the guessed spectrum and stealth spectrum. As a summary, to match either the spectrum or the optical delay does not indicate the existence of the stealth channel. Both of the spectrum and optical delay have to be matched and form a two-dimensional key space.

The small notches of the combined spectrum come from the mismatch between the optical bandpass filters and combiners used for splitting and combination. However, in WDM networks, public channels also use filters to add and drop channels, which also cause the notches. An eavesdropper cannot tell whether the notch comes from a public channel or a stealth channel.

A clear eye diagram with minimum BER of 2×10^{-8} is achieved (Fig. 3). The BER performance versus received signal power is measured [Fig. 3(b)]. Forward error correction (FEC) with Reed-Solomon codes can be used to reduce the BER below 10^{-3} to where it is error free. The received power of the stealth channel with BER 10^{-3} is only −14.5 dBm [Fig. 3(b)].

Multi-channel transmission can be achieved by using different parts of the ASE spectrum [Fig. 4(a)]. Figure 4(b) shows the spectrum of three stealth channels with central wavelength 1548.5, 1550.1, and 1551.7 nm with FWHM 1.1 nm. The channel interval is 1.6 nm and the ASE spectrum between 1520 and 1560 nm supports a maximum number of 25 channels. Multiple stealth channels can be added to the public network, either in parallel or in series, whenever a sufficient level of ASE noise is present.

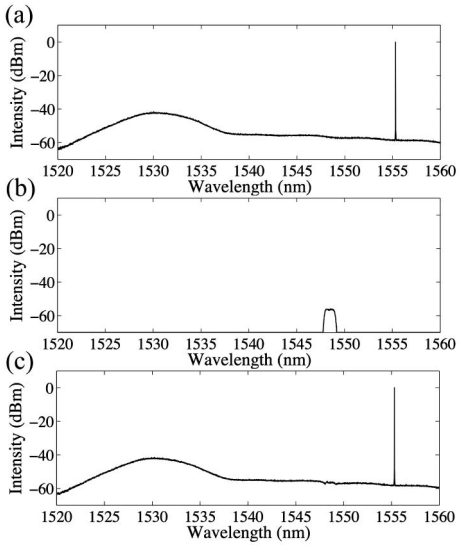

Fig. 2. Spectra that show the stealth channel hidden in the public noise (a), (b), and (c) correspond to the spectrum at points A, B, and C in Fig. 1.

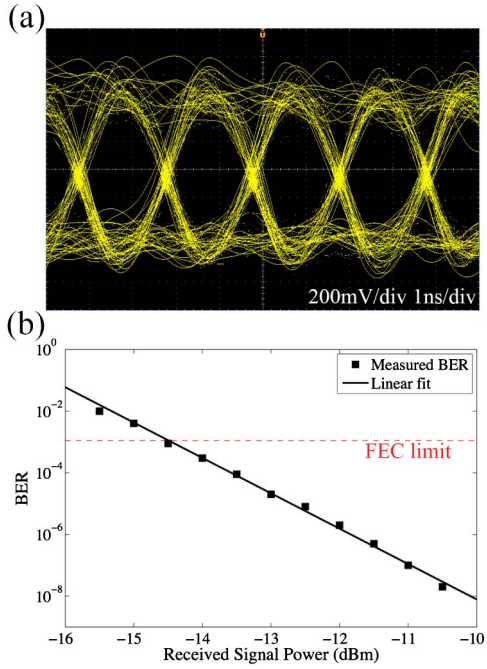

Fig. 3. (a) Eye diagram of the stealth channel and (b) BER performance versus received signal power (FEC: forward error correction).

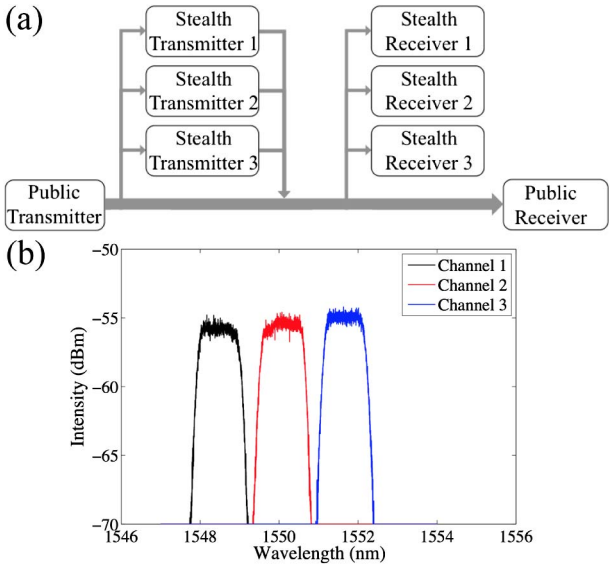

Fig. 4. (a) Schematic diagram of hiding multiple stealth channels in the public network and (b) spectra of WDM stealth channels.

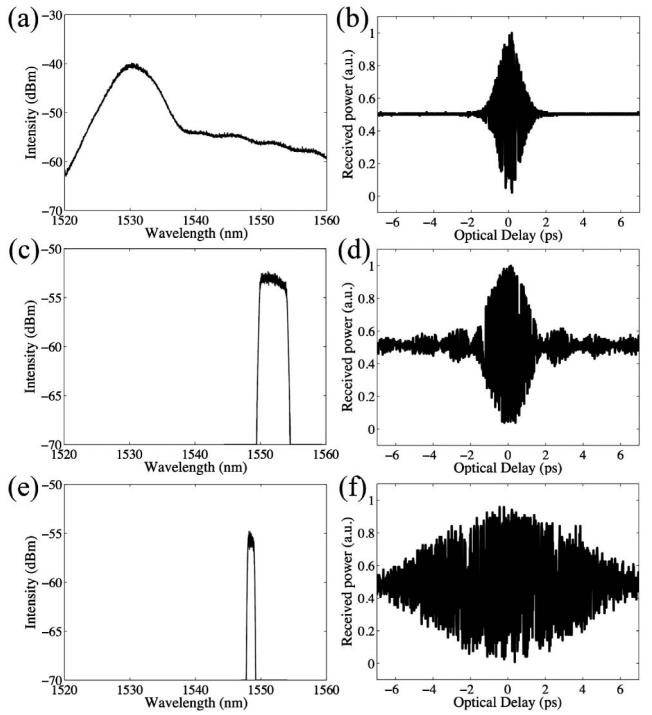

Fig. 5. Spectra of the stealth channel with different bandwidths and the corresponding coherence peaks. (a) the entire ASE spectrum from 1520 to 1560 nm; (b) coherence peak of the entire ASE spectrum; (c) ASE spectrum with 5 nm bandwidth and central wavelength at 1552 nm; (d) coherence peak of the ASE with 5 nm bandwidth; (e) ASE spectrum with 1.1 nm bandwidth and central wavelength at 1548.5 nm; (f) coherence peak of the ASE with 1.1 nm bandwidth.

Deploying a partial spectrum of ASE noise as the signal carrier adds another dimension of security; however, as a trade-off, the filtered spectrum has longer coherence length. To study the mechanism between the spectral bandwidth and the coherence length, coherence lengths of different ASE spectra are measured (Fig. 5). The coherence lengths are measured by scanning one of the tunable delays in Fig. 1 through the matching condition and using a power meter to measure the optical power at the stealth receiver. Constructive and destructive interference form a coherence peak whose FWHM gives the coherence length. The coherence length of the entire ASE spectrum is 1.2 ps [Figs. 5(a) and 5(b)]. The coherence length of the filtered ASE spectrum with 5 nm width is 2.2 ps [Figs. 5(c) and 5(d)]. The coherence length of the filtered ASE spectrum with 1.1 nm width is 8.5 ps [Figs. 5(e) and 5(f)]. The measured results show that the envelope of the coherence peak is the Fourier transform of the spectrum. When the filters are of the same shape, the coherence length is inversely proportional to the bandwidth of the filter. The spectrum in Fig. 5(b) is about four times wider than the spectrum in Fig. 5(c). The corresponding coherence length in Fig. 5(e) is thus 1/4 of the coherence length in Fig. 5(f). The coherence length of the entire ASE spectrum is about half of the coherence length of the ASE spectrum with 5 nm band pass filter. This is because the power of the ASE spectrum mainly comes from the peak around 1530 nm, with FWHM 10 nm [10], which is twice of 5 nm bandwidth. When using rectangle filters [Fig. 5(b)], the envelope of the coherence peak has side lobes because the Fourier transform of a rectangle function is a sinc function. The side lobes are undesirable and can be suppressed by using filters with Gaussian shape transfer functions [11,12].

Although the filtered spectra have increased coherence lengths, the coherence length is still short compared with the optical delay length difference at the transmitter. When a filter with 1.1 nm bandwidth is used, the coherence length is 8.5 ps or 2.55 mm in terms of free-space optical delay. The optical path difference at the transmitter is 10 m of fiber, which means the eavesdropper needs to find 2.55 mm in a 10 m range in order to demodulate the stealth data, and the optical delay difference can be changed before the eavesdropper can find the correct value. 10 m is a demonstrated value in this experiment. Since the phase of ASE noise is completely random [13,14], there is no limit on the optical path difference at the transmitter. If longer optical path difference is applied, faster changing speed is needed when changing the optical path difference.

We experimentally demonstrate a stealth transmission system using filtered ASE noise with FWHM bandwidth 1.1 nm. WDM stealth transmission is achieved by using filtered ASE noise as the signal carrier, which not only increases the capacity of a stealth channel but also allows multiple users to share the stealth system at the same time. Using filtered ASE noise as the signal carrier adds another layer of security. To find the existence of the stealth channel, the eavesdropper must find 1.1 nm in a 40-nm range. The filtered ASE stealth transmission also has more flexibility. A stealth channel can be added to the public network in bands where the power of ASE noise is large enough to carry stealth signals.

The authors would like to gratefully acknowledge the support of the Princeton intellectual property accelerator fund. The authors also would like to thank Bhavin J. Shastri in the Lightwave Communications Laboratory

at Princeton University for help with lab and equipment maintenance.

References

1. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, IEEE Trans. Inf. Forensics Secur. **6**, 725 (2011).
2. B. Wu, B. J. Shastri, and P. R. Prucnal, in *Emerging Trends in ICT Security*, B. Akhgar and H. Arabnia, eds. (Elsevier, 2014), pp. 173–183.
3. Z. Wang and P. R. Prucnal, IEEE Photon. Technol. Lett. **23**, 48 (2011).
4. B. Wu, M. P. Chang, B. J. Shastri, Z. Wang, and P. R. Prucnal, Opt. Express **22**, 14568 (2014).
5. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Nature **438**, 343 (2005).
6. M. Jinno and T. Matsumoto, Opt. Lett. **16**, 220 (1991).
7. K. Chan, C. K. Chan, L. K. Chen, and F. Tong, IEEE Photon. Technol. Lett. **16**, 897 (2004).
8. B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, Opt. Express **21**, 2065 (2013).
9. B. Wu, Z. Wang, B. J. Shastri, M. P. Chang, N. A. Frost, and P. R. Prucnal, Opt. Express **22**, 954 (2014).
10. B. Wu, B. J. Shastri, and P. R. Prucnal, IEEE Photon. Technol. Lett. **26**, 1920 (2014).
11. A. V. Tikhonravov and M. K. Trubetskov, Appl. Opt. **41**, 3176 (2002).
12. L. Poladian, Opt. Lett. **26**, 7 (2001).
13. N. A. Olsson, J. Lightwave Technol. **7**, 1071 (1989).
14. E. Desurvire, Appl. Opt. **29**, 3118 (1990).