Optical steganography based on amplified spontaneous emission noise

Ben Wu,[*] Zhenxing Wang, Yue Tian, Mable P. Fok, Bhavin J. Shastri, Daniel R. Kanoff, and Paul R. Prucnal

Lightwave Communications Laboratory, Department of Electrical Engineering, Princeton University, Princeton, New Jersey 08544, USA
[*] *benwu@princeton.edu*

Abstract: We propose and experimentally demonstrate an optical steganography method in which a data signal is transmitted using amplified spontaneous emission (ASE) noise as a carrier. The ASE serving as a carrier for the private signal has an identical frequency spectrum to the existing noise generated by the Erbium doped fiber amplifiers (EDFAs) in the transmission system. The system also carries a conventional data channel that is not private. The so-called "stealth" or private channel is well-hidden within the noise of the system. Phase modulation is used for both the stealth channel and the public channel. Using homodyne detection, the short coherence length of the ASE ensures that the stealth signal can only be recovered if the receiver closely matches the delay-length difference, which is deliberately changed in a dynamic fashion that is only known to the transmitter and its intended receiver.

OCIS codes: (060.2330) Fiber optics communications; (060.4785) Optical security and encryption; (060.2920) Homodyning.

References and links

1. K. Chan, C. K. Chan, L. K. Chen, and F. Tong, "Demonstration of 20-Gb/s all-optical XOR gate by four-wave mixing in semiconductor optical amplifier with RZ-DPSK modulated inputs," IEEE Photon. Technol. Lett. **16**(3), 897–899 (2004).
2. K. Vahala, R. Paiella, and G. Hunziker, "Ultrafast WDM logic," IEEE J. Sel. Top. Quantum Electron. **3**(2), 698–701 (1997).
3. J. M. Castro, I. B. Djordjevic, and D. F. Geraghty, "Novel super structured Bragg gratings for optical encryption," J. Lightwave Technol. **24**(4), 1875–1885 (2006).
4. B. B. Wu and E. E. Narimanov, "A method for secure communications over a public fiber-optical network," Opt. Express **14**(9), 3738–3751 (2006). http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-14-9-3738.
5. Z. Wang and P. R. Prucnal, "Optical steganography over a public DPSK channel with asynchronous detection," IEEE Photon. Technol. Lett. **23**(1), 48–50 (2011).
6. K. Kravtsov, B. Wu, I. Glesk, P. Prucnal, and E. Narimanov, "Stealth transmission over a WDM network with detection based on an all-optical thresholder," in Proceedings of IEEE/LEOS Annual Meeting, 480–481 (2007).
7. B. Wu, A. Agrawal, I. Glesk, E. Narimanov, S. Etemad, and P. Prucnal, "Steganographic fiber-optic transmission using coherent spectral-phase-encoded optical CDMA," in Proc. CLEO/QELS, San Jose, CA, Paper CEF5 (2008).
8. Y.-K. Huang, B. Wu, I. Glesk, E. E. Narimanov, T. Wang, and P. R. Prucnal, "Combining cryptographic and steganographic security with self-wrapped optical code division multiplexing techniques," Electron. Lett. **43**(25), 1449–1451 (2007).
9. X. Hong, D. Wang, L. Xu, and S. He, "Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering," Opt. Express **18**(12), 12415–12420 (2010). http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-18-12-12415.
10. M. P. Fok and P. R. Prucnal, "A compact and low-latency scheme for optical steganography using chirped fiber Bragg gratings," Electron. Lett. **45**(3), 179–180 (2009).
11. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic network," IEEE Trans. Inf. Forensics Security **6**(3), 725–736 (2011).
12. G. D. VanWiggeren and R. Roy, "Communication with chaotic lasers," Science **279**(5354), 1198–1200 (1998).
13. A. Argyris, D. Syvridis, L. Larger, V. A. Lodi, P. Colet, I. Fischer, J. G. Ojalvo, C. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fiber-optic links," Nature **438**, 343–346 (2006).

#178601 - $15.00 USD Received 31 Oct 2012; revised 2 Jan 2013; accepted 3 Jan 2013; published 18 Jan 2013

14. J. Liu, Z. M. Wu, and G. Q. Xia, "Dual-channel chaos synchronization and communication based on unidirectionally coupled VCSELs with polarization-rotated optical feedback and polarization-rotated optical injection," Opt. Express **17**(15), 12619–12626 (2009), http://8.18.37.105/oe/abstract.cfm?uri=oe-17-15-12619.
15. G. P. Agrawal, *Fiber-Optic Communication Systems* (Wiley, 2002), Chap. 6.
16. W. Wells, R. Stone, and E. Miles, "Secure communication by optical homodyne," IEEE J. Sel. Areas Comm. **11**(5), 770–777 (1993).
17. S. Yin, P. B. Ruffin, and F. T. S. Yu, *Fiber Optic Sensors* (CRC, 2008), Chap. 2.

1. Introduction

With the increased accessibility of optical networks in the last decade, it is important that the communications over optical networks are properly secured. Recently, all-optical data encryption [1–3] and optical steganography [4–10] have been explored for securing networks at the optical layer. Optical encryption enables low latency and high speed encryption without the generating electromagnetic signatures [11]. In particular, optical chaos encryption has been widely studied during the past decade [12–14]. Using spread spectrum techniques to encrypt data in a broadband chaotic signal, optical chaos encryption enhances the robustness and privacy of the system. Optical steganography, on the other hand, provides a way to hide private data within the existing public channel so no one, apart from the intended recipient, knows the existence of the message [4]. Transmitting such private data is called a "stealth channel." Without knowing information about the encryption process in the stealth channel, the eavesdropper can neither demodulate the private data nor know the existence of the stealth channel. Previous approaches to optical steganography based on stretching an optical pulse through chromatic dispersion [5], combined with different modulation methods of public channel, have been studied [5–10]. Although widely stretched and low amplitude pulses can be buried in the system noise, the optical spectrum of the stealth channel signal is still not sufficiently wide to perfectly match the spectrum of the system noise. A better solution is not to mimic the system noise, but to use the system noise directly to transmit the stealth signal.

Erbium doped fiber amplifiers (EDFAs) are widely deployed in today's optical communication systems. Although amplified spontaneous emission (ASE) noise from EDFAs is undesirable from the perspective of system performance [15], we can benefit from it in the area of photonic network security. We propose to add private signals on top of the ASE noise and thus hide them plain sight. Since ASE already exists as noise in optical systems, and ASE carrying signals have identical spectra as the original noise ASE, an eavesdropper will not be able to differentiate whether it is "signal ASE" or "noise ASE" by observing the spectrum. Another benefit of ASE noise is its short coherence length. Using optical homodyne detection [16], the optical delay length has to be exactly matched at the receiver for the signal to be demodulated. This enables the system to have a key for modulation and demodulation. An eavesdropper has to search a large range of delay lengths to satisfy the matching condition and demodulate the signal.

In this paper, we make use of ASE noise as the source of the stealth channel. Utilizing the short coherence length characteristic of ASE noise, we use DPSK modulation for the stealth channel at the transmitter, and use homodyne detection to demodulate the signal at the receiver. The optical delay length difference at the transmitter is the key for demodulation, which can be several meters. To demodulate the signal without knowing the length difference, the eavesdropper needs to scan the entire length difference to search for the matching condition. The scan has to be precise enough to observe the coherenc length of ASE noise, which is only 372μm. To further prevent the delay length difference from being detected, we use motorized controlled delay lines at both the transmitter and receiver. Controlled by two separate computers, the receiver delay line can follow the movement of the transmitter delay—a "hopping" key. As a consequence, even if the eavesdropper can scan delay line difference and find the matching condition, this process will not be fast enough to find the matching condition before the key changes. Moreover, DPSK is used in the pubic channel. The phase modulated public channel provides both signal and noise with constant power to the system, so the stealth channel can hide in the noise secretly all the time.

#178601 - $15.00 USD Received 31 Oct 2012; revised 2 Jan 2013; accepted 3 Jan 2013; published 18 Jan 2013

2. Experimental setup

The experimental setup makes use of the short coherence length of ASE noise, and the structure of the stealth channel is a Mach-Zehnder (MZ) interferometer (see Fig. 1). The carrier for the stealth channel comes directly from an EDFA. The EDFA generates ASE noise which has the same characteristics as the ASE noise that exists in the pubic channel. The ASE noise is then input into the MZ interferometer. The stealth signal is modulated onto one arm of the interferometer using a phase modulator. The public channel employs DPSK modulation using a laser source having wavelength 1551.72 nm. To simulate the ASE noise that would be introduced by EDFAs in a long distance transmission system, additional ASE is added at the public channel transmitter. The public channel and stealth channel are combined by a 50:50 coupler and sent over 25 km of standard single mode fiber (SSMF), followed by dispersion compensation fiber (DCF). Three wavelength division multiplexer (WDM) filters are connected in series to spectrally separate the stealth channel from the public channel. The stealth channel receives the signal from the reflection output of the third WDM filter. The public channel receives the transmission output of the first WDM filter. The transmitter and receiver of the stealth channel actually represent a large Mach-Zehnder interferometer. There are two pairs of optical paths: path 1→3, 2→4 and path 1→4, 2→3 (see Fig. 1). Line 1 is 6m longer than line 2. Because ASE noise has a very short coherence length, which we measured to be 372 μm (as detailed in Section 3), interference can only occur when the length of one pair of the light paths matches exactly with that of the corresponding other pair. In this experiment, light path 1→3 and light path 2→4 have the same length. Two tunable delay lines are used. One is at the transmitter and the other is at the receiver. They are controlled by two separate computers which share a secret key. Thus, if tunable delay 1 (T1) moves to a new position, tunable delay 2 (T2) is instructed to mimic that movement, and reestablish the matching condition.

Fig. 1. Experimental Setup (EDFA: erbium-doped fiber amplifier; P: polarizer; ASE: amplified spontaneous emission; PM: phase modulator; PD: phase demodulator; SSMF: standard single mode fiber; DCF: dispersion compensation fiber; WDM: wavelength division multiplexer).

The fiber-based Mach-Zehnder interferometer is sensitive to temperature and mechanical vibration [17]. The temperature and mechanical vibrations can cause the eye diagram and bit error rate (BER) at the receiver of the stealth channel to vary as a function of time. To minimize these effects, we: (1) packaged the interferometers both at the transmitter and receiver of the stealth channel; and (2) Physically stabilized all the fibers. Using this method, the eye diagram can stay stable for up to 5 s, which is long enough to measure the BER at a given signal power. For deployed transmission systems, industry standards for stability control would be required.

#178601 - $15.00 USD Received 31 Oct 2012; revised 2 Jan 2013; accepted 3 Jan 2013; published 18 Jan 2013

3(a)) and on (see Fig. 3(b)). The power of the signal ASE is 14.5 dB lower than the public channel, so the power change with and without

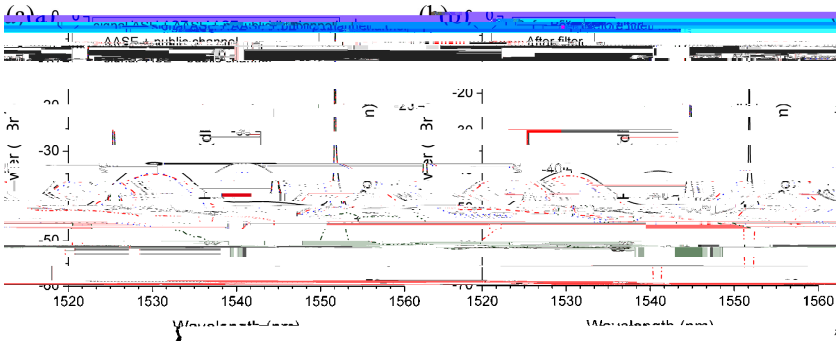

Fig. 4 (a) Spectrum of the signal before entering the 25 km of SSMF and DCF. (AASE: additional ASE) (b) Spectrum before and after the WDM filter.

3.3 Power penalty of the system

The BER measurements of the stealth channel show that adding the public channel to the system does not result in a power penalty of stealth channel. In Fig. 5(a), the BER curves of the stealth channel with and without the public channel are indistinguishable. This is because the ASE noise covers a large range of spectrum from 1520 nm to 1560 nm (see Fig. 4(a)), whereas the public channel is only at a single wavelength of 1551.72 nm, which can easily be filtered from the stealth channel. However, we note that there is a power penalty of 6.5 dBm when additional ASE with the same power as the signal ASE is added. This is because additional ASE has the same spectrum as ASE carrying stealth signals. They cannot be separated by optical filters, so more power is required to reach the same BER when additional ASE is added. The BER reaches a noise floor at 10^{-6}. The power penalty is qualitatively observed from the degradation in the eye diagram of the stealth channel in Fig. 3(e) with more jitter and smaller eye opening. The additional ASE saturates the EDFA of the stealth channel and causes the amplitude of eye to be smaller.

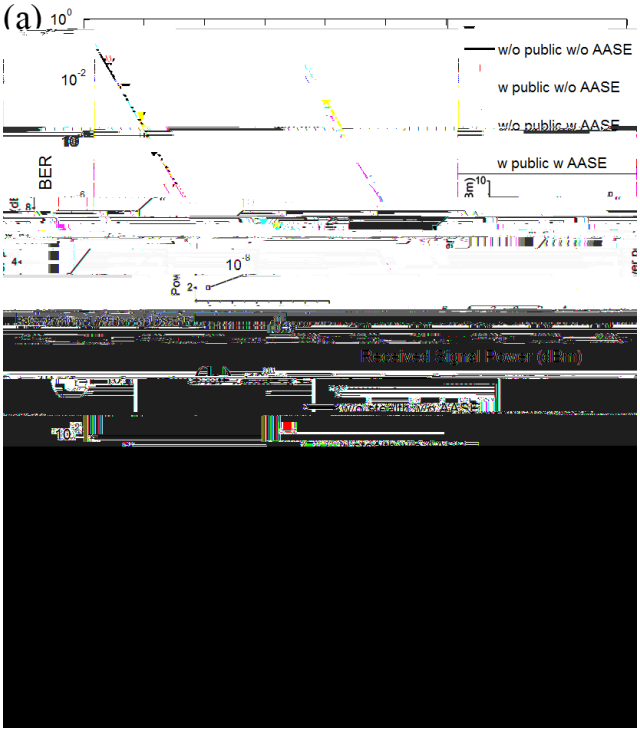

Fig. 5. BER performance versus received signal power for: (a) the stealth channel with and without public channel and AASE, data after the noise floor is not considered in the linear fit with AASE. The inset shows the penalty from additional ASE at different ratio of addition ASE to signal ASE. (b) The public channel with and without the stealth channel and additional ASE.