Temporal phase mask encrypted optical steganography carried by amplified spontaneous emission noise

Ben Wu,* Zhenxing Wang, Bhavin J. Shastri, Matthew P. Chang, Nicholas A. Frost, and Paul R. Prucnal

Lightwave Communications Laboratory, Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

benwu@princeton.edu

Abstract: A temporal phase mask encryption method is proposed and experimentally demonstrated to improve the security of the stealth channel in an optical steganography system. The stealth channel is protected in two levels. In the first level, the data is carried by amplified spontaneous emission (ASE) noise, which cannot be detected in either the time domain or spectral domain. In the second level, even if the eavesdropper suspects the existence of the stealth channel, each data bit is covered by a fast changing phase mask. The phase mask code is always combined with the wide band noise from ASE. Without knowing the right phase mask code to recover the stealth data, the eavesdropper can only receive the noise like signal with randomized phase.

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

References and links

1. 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).
2. 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).
3. 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 *Proceeding CLEO/QELS*, (Optical Society of America, 2008), Paper CEF5.
4. 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).
5. 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).
6. 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).
7. 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**(2), 2065–2071 (2013).
8. 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 *Proceeding CLEO*, (Optical Society of America, 2013), paper AF1H.5.
9. B. Akhgar and H. R. Arabnia, *Emerging Trends in Information and Communication Technologies Security* (Elsevier, 2013) (to be published).
10. 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).
11. 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).
12. Z. Wang, M. P. Fok, L. Xu, J. Chang, and P. R. Prucnal, "Improving the privacy of optical steganography with temporal phase masks," Opt. Express **18**(6), 6079–6088 (2010).
13. B. Wu, Z. Wang, B. J. Shastri, Y. Tian, and P. R. Prucnal, "Phase-mask covered optical steganography based on amplified spontaneous emission noise," in *Proceedings of IEEE Photonics Conference* (Institute of Electrical and Electronics Engineering, Bellevue, Washington, 2013), paper MG3.3.

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014

1. Introduction

The substantial increase in the usage of fiber optic networks requires proper protection of the sensitive information that may be carried. Optical steganography is an effective way to provide secure data transmission in the physical layer of a network. Hiding signals in the system noise of the public channel, optical steganography prevents the eavesdropper from detecting the existence of the signals [1]. The hidden signal is called a "stealth channel". Previous approaches to optical steganography were based on temporally stretching the optical pulse by chromatic dispersion [2–6]. The stretched pulse had a sufficiently low amplitude so the signal is buried under the noise floor of the system. Recently, a new method has been experimentally demonstrated [7,8]. The stealth data is carried by the amplified spontaneous emission (ASE) noise from an erbium doped fiber amplifier (EDFA). The ASE-carrying signals inherently have the same spectrum as the system's ASE noise. In the time domain, because the ASE has a short coherence length, the optical delay at the transmitter and receiver need to be exactly matched to detect the signal, which provides a large key space for the stealth channel. However, mechanical delay lines are required to achieve optical delays with large bandwidth. This limited the speed at which the delay could be changed on the order of seconds [7]. If an eavesdropper deploys a faster scanning technique, then the key pair based on optical delays is vulnerable to a threat. Therefore, a method employing a fast changing key is needed to further protect the stealth data from being detected.

Another method to protect the data transmission in the physical layer is optical encryption [9]. Optical encryption provides a fast encryption process that enables both changing the key at the rate of data transmission and real time data processing with zero latency [10,11]. The requirement of having a fast changing key in optical steganography can be satisfied by optically encrypting the stealth data, and provides further protection of the stealth channel. In previous work, optical encryption has been applied to the steganography system based on stretching optical pulses by chromatic dispersion [12]. Optical encryption was achieved by covering each stretched pulse with a temporal phase mask. Although this method can improve the security of the stealth channel, the phase mask itself is unsecure if an eavesdropper matches the dispersion. The eavesdropper can compare a stretched pulse and a phase mask covered pulse to retrieve the phase mask.

In this paper, a phase mask encryption method is proposed based on ASE-carried stealth signals. This method offers two unique advantages that are missing in previous systems. First, the phase mask code, which was previously unsecured, is protected by the noisy properties of ASE. Designed to have bandwidth much wider than the stealth data, the phase mask is indistinguishable from the wideband noise of ASE. Without a *priori* knowledge of the phase mask code, the receiver cannot separate the noise and phase mask code. Second, the phase mask can change with every bit of the stealth signal, which is on the order of several nanoseconds. This rate of change is a billion times faster than the rate of changing optical delays mechanically. Even the if an eavesdropper with a fast scanning technique could match the optical delay, he could not follow the rapidly changing phase mask code.

2. Experimental setup and principle

The experimental setup utilizes the short coherence length and noise properties of ASE [Fig. 1(a)]. These two properties provide two levels of protection to the stealth channel. The first level corresponds to the short coherence length of ASE noise. Experimental results show that the coherence length of ASE noise is 372μm [7]. The optical delay length difference between the light path 1 and 2 is designed to be 10m in this experiment, so the eavesdropper needs to search for the 372μm length in the 10m range to demodulate the data. Even if the eavesdropper deploys a fast scanning technique and finds the coherence length before the transmitter changes the optical delay, the data is still protected by the second level of security, which is the phase mask. The phase mask technique benefits from the noise properties of the ASE. The ASE noise has a flat bandwidth that goes up to at least 5GHz [13]. In the experiment, both the stealth data transmission and the phase mask encryption are

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014

implemented by modulating the phase of the ASE noise at the transmitter [Fig. 1(b)]. The data rates of the stealth channel and phase mask are 250Mb/s and 4Gb/s, respectively. The bandwidth of the phase mask data is 16 times wider than the bandwidth of the stealth data, so the phase mask data is 16 times noisier than the stealth data. The extra noise protects the phase mask, and they are indistinguishable if the phase mask code is not known. Only by using the same phase mask code to recover the signal at the receiver can the phase difference in the two light paths 1→3 and 2→4 be cancelled [Fig. 1(a)]. The phase mask also corrupts the stealth data. If the eavesdropper tries to use an electronic low-pass filter to remove both the phase mask and the high frequency noise, the remaining amplitude of the stealth signal is low enough to be submerged in the noise.

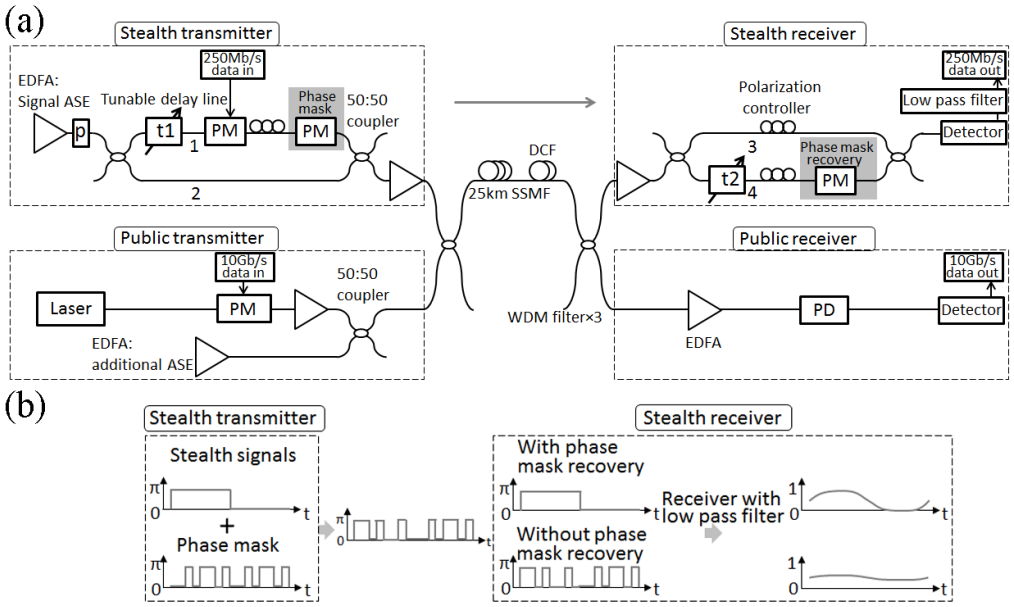

Fig. 1. Experimental Setup (EDFA: erbium-doped fiber amplifier; P: polarizer; ASE: amplified spontaneous emission; PM: phase modulator; PD: phase demodulator; SSMF: standard single mode fiber; DCF: dispersion compensation fiber; WDM: wavelength division multiplexer). (b) Schematic diagram of the stealth channel; only 8 chips are drawn for each bit.

The stealth transmitter and receiver pair is a fiber-based Mach-Zehnder interferometer and the phase and polarization of the stealth signal are sensitive to temperature and mechanical vibration. The temperature and mechanical vibration can cause the amplitude of the eye diagram change with time and degrade the bit error rate (BER). To minimize the effect of mechanical vibration, all the fibers are physically stabilized either on an optical table or in packaged boxes. To minimize the effect of temperature fluctuation, the stealth transmitter and receiver are packaged separately and a temperature control system is provided for the packages.

The eye diagrams show that the received signal amplitude is greatly reduced without phase mask recovery [Figs. 2(a)-2(d)]. A low-pass filter with a −3dB cut off frequency 250MHz is used at the receiver. Clear eye diagrams are shown with the phase mask recovery [Figs. 2(a) and 2(c)]. If phase mask recovery is not used, the phase mask at the transmitter corrupts the stealth data, and the stealth signal at the receiver becomes low enough to be buried under the noise [Figs. 2 (b) and 2(d)]. If the eavesdropper does not use a low-pass filer and tries to receive the phase mask code directly [Fig. 2(e)], the code is covered by the noise from 0Hz to the bandwidth of phase mask code, which is 4GHz. The signal is noisy enough that the bit error rate (BER) cannot be measured [Fig. 2(e)].

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014

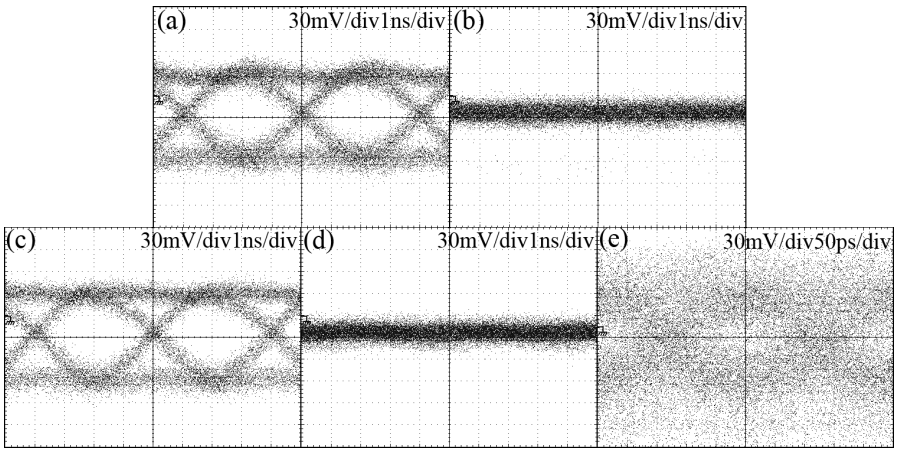

Fig. 2. Comparison of eye diagrams with and without phase mask recovery. (a) Phase mask code 1010101010101010 with phase mask recovery. (b) Phase mask code 1010101010101010 without phase mask recovery. (c) Phase mask code 1010100101101001 with phase mask recovery. (d) Phase mask code 1010100101101001 without phase mask recovery. (e) Eye diagram of receiving phase mask data directly.

3. Experiment results and analysis

3.1 Hidden signals in the public channel

The receiver of the public channel cannot detect the existence of the stealth channel in either the time or the spectral domain [Fig. 3]. The public channel employs DPSK modulation with a data rate of 10Gb/s. A distributed feedback laser with wavelength 1551.72nm is used as the signal carrier of the public channel. The signal in the public channel is pseudorandom binary sequence (PRBS) with length 2^{31}-1. An EDFA to provide additional ASE is added in the public transmitter to simulate the system noise in the public channel [Fig. 1]. The power of the stealth channel is designed to be much lower than the power of the public channel. In this experiment, the power of the stealth channel is 21dB lower than the public channel. Moreover, the spectrum of ASE noise-carrying stealth channel ranges from 1520nm to 1560nm. Wavelength division multiplexer (WDM) filters with a −3dB bandwidth of 0.5 nm are used to separate the public channel and the stealth channel [Fig. 1(a)]. Only the ASE noise in this 0.5nm spectral range interferes with the public channel. Therefore, there is no difference between the eye diagrams of the public channel with the stealth channel [Fig. 3(a)] and without the stealth channel [Fig. 3(b)]. The stealth channel only causes a 0.2 to 0.3 dBm power penalty to the public channel [7]. In the spectral domain, the ASE carrying the stealth data has the same spectrum as the ASE noise in the public channel, so the eavesdropper cannot tell whether it is the stealth channel or the system noise that already exists in the public channel [Fig. 3(c)]. In the experiment, an additional EDFA is used to emulate the noise in the public channel [Fig. 1(a)].

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014

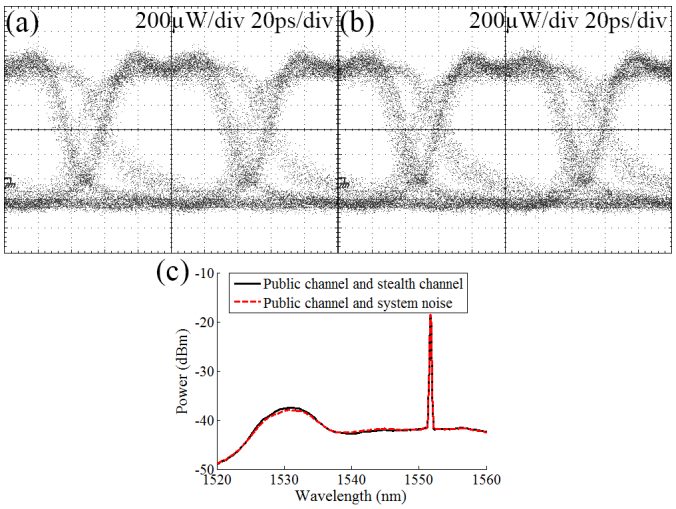

Fig. 3. (a) Eye diagram of public channel with stealth channel. (b) Eye diagram of public channel without stealth channel. (c) Spectrum of public channel with and without stealth channel.

3.2 Code space analysis

The fast changing phase mask code requires a large code space. In this section, we demonstrate that more than 18,000 codes are available for the phase mask. Each stealth channel bit is divided into 16 chips by the phase mask, so the available combination is 2^{16} = 65,536. The best codes for the phase mask are the codes that can reduce the amplitude of the stealth signal to a small value. We simulate all 65,536 codes and plot how many codes are available to reduce the signal amplitude lower than a certain value [Figs. 4(a) and 4(b)]. In the simulation, the stealth data is a 2^{15}-1 = 32,767 bit pseudorandom binary sequence (PRBS), and a low-pass filter with cut-off frequency 250MHz is used at the receiver. The reduced signals from several sample codes are experimentally measured to compare with the simulation results. Figure 4(c) shows the original signal amplitude without using the phase mask code. Figures 4(d)–4(h) show that the sample codes reduce the amplitude of the signal in Fig. 4(c) to 5%, 10%, 15%, 20% and 25%, which corresponds to the red dots in the simulation results [Fig. 4(b)]. The measured signals show that if the eye diagram amplitude is reduced to lower than 15% of its original value [Figs. 4(d)–4(f)], then there is no eye opening, and the number of available codes for this is more than 4,000 [Fig. 4(b)]. If the eye diagram amplitude is reduced to lower than 25%, but higher than 15%, the data rate of the stealth channel can be roughly measured, but the bit error rate of the stealth data is still undetectable [Figs. 4(g) and 4(h)]. The number of available codes in this range is more than 14,000 [Fig. 4(b)].

The codes not only reduce the amplitude but also randomize the phase of each stealth bit [Fig. 4(h)]. The position of the peak in each stealth data bit depends on both the stealth data and the phase mask code [Fig. 5(a)]. Comparing the distribution of stealth data peaks with and without using the phase mask, the simulation of 2^{15}-1 stealth bits shows that the phase mask code randomizes the distribution of peaks in each stealth data bit [Fig. 5(b)]. Without using the phase mask recovery, the peak position of the stealth bit changes with every bit, which makes it impossible for an eavesdropper to find the sampling position to detect the data. In summary, the noise-like signal in Figs. 4(d)–4(h) results from both the reduction of the signal amplitude and the randomization of the signal phase. There are more than 18,000 codes that can reduce the signal amplitude to lower than 25% of its original value and also randomize the phase.

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014

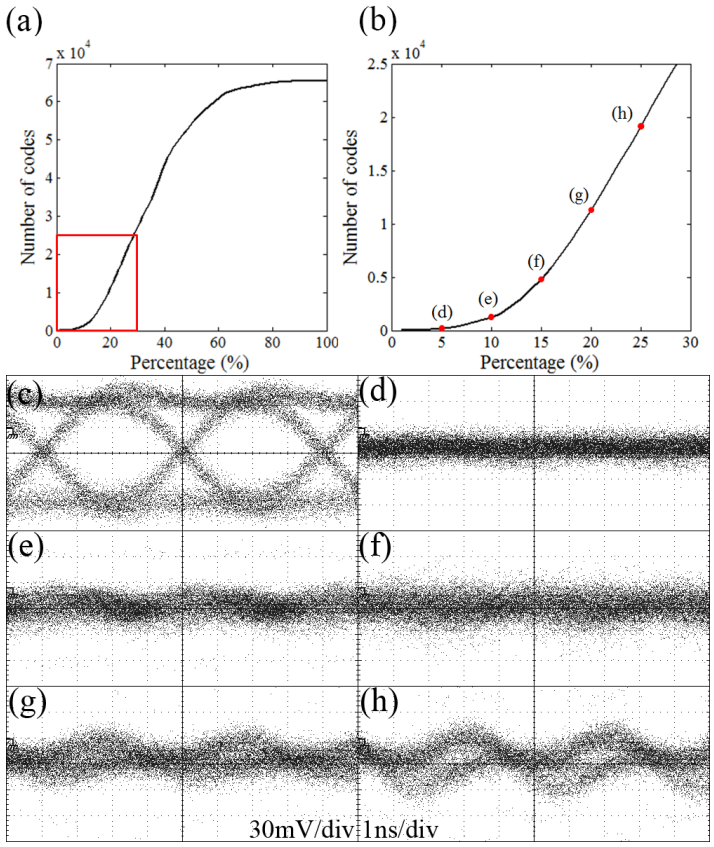

Fig. 4. (a) The number of available codes that can reduce the eye amplitude below a certain percentage. (b) Enlarged view of the region marked by red in (a); the red spots correspond to (d)-(h). (c) Eye diagram of the stealth channel without phase mask. (d) Phase mask code 1010100101101001 can reduce eye amplitude to 5% of the amplitude in (c). (e) Phase mask code 1100011001011001 can reduce eye amplitude to 10%. (f) Phase mask code 1101011001001110 can reduce eye amplitude to 15%. (g) Phase mask code 0011011010101100 can reduce eye amplitude to 20%. (h) Phase mask code 1011100010010101 can reduce eye amplitude to 25%.

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014

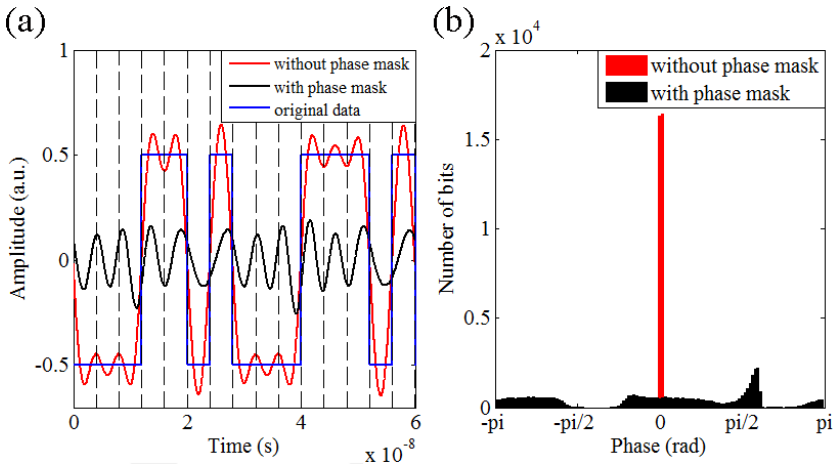

Fig. 5. Simulation of the stealth signal with phase mask code 1011100010010101, which is the code used in Fig. 4(h). (a) Comparison of temporal signal with and without phase mask encryption. (b) Distribution of the signal peaks in the stealth bit.

3.3 Power penalty of the phase mask

The phase mask causes a 0.3dBm power penalty to the stealth channel at a BER of 10^{-6} [Fig. 6]. In the experiment, a PRBS with length 2^{31}-1 is used as the signal of the stealth channel. The stealth channel is designed to include noise and is not error-free. The noise in the stealth channel comes from ASE, and when the phase mask recovery is not used, the stealth signal with reduced amplitude can be buried in the noise. In addition, as discussed in section 2, the noise also protects the phase mask. As the bandwidth of the phase mask code is 16 times wider than the stealth data, the noise accompanying the phase mask is 16 times stronger than the noise accompanying the stealth channel. Forward error correction with Reed-Solomon codes can be used to correct a BER of 10^{-6} to be error free. The power penalty of the phase mask is caused by the misalignment of the phase mask at the transmitter and the receiver. The misalignment could exist in both the time and the modulation depth. The 0.3dBm power penalty is low because the power of the public channel is 21dB higher than the power of the stealth channel.

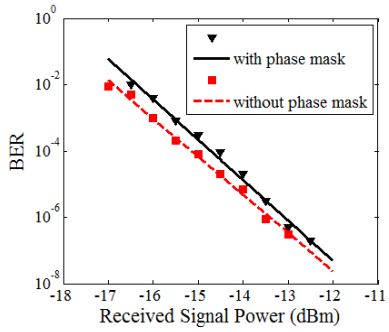

Fig. 6. BER performance versus received signal power for stealth channel with and without using phase mask encryption.

3.4 Data rate and transmission distance analysis

Since the stealth channel is carried by the full spectrum of ASE noise, which spans from 1520nm to 1560nm [Fig. 3(c)], the system has less tolerance to dispersion compared with traditional fiber optics systems. This limits both the data rate of the phase mask and the

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014

transmission distance without the dispersion compensation. We experimentally measured that if the DCF is not used, the dispersion from 25km standard single mode fiber (SSMF) expends the sharp rising edge of a signal to one with 3ns rising. By using the criterion $B\Delta T<1$, where B is the data rate of the phase mask, which is 4Gb/s, the time delay (ΔT) caused by the dispersion has to be less then 250ps. Considering both the rising edge and the falling edge, the system can only tolerate uncompensated dispersion from 1km SSMF. Although this limits resilience of this system in a dynamic network, the precise requirement of dispersion compensation can actually provide another layer of security. We have demonstrated that the dispersion can expend the key space for optical steganography [8].

Besides dispersion, the wide optical spectrum of ASE noise also limits the signal to noise ratio for long distance transmission. When an optical amplifier is used to amplify the signal in a traditional long distance communication system, an optical filter is deployed to remove the ASE noise from the optical amplifier. However, if ASE carries the signal, the optical filter cannot be used. The ASE carrying signals cannot be separated from the new generated noise ASE.

The ASE also has wide band radio frequency noise, which protect the phase mask from being detected. As a tradeoff, the wide band radio frequency noise limits the data rate of both the stealth channel and the phase mask. The stealth channel with a higher data rate is accompanied with more ASE noise. Our experiment shows that the BER increase while the stealth channel date rate increases [Fig. 7]. The data rate of the phase mask is designed to be high enough so that the ASE noise with the same bandwidth accompanied can protect the phase mask data from being detected. However, the data rate of the phase mask cannot be too high because the receiver needs to temporally overlap the received phase mask with the recovery phase mask. If the phase mask is accompanied by more noise, it will degrade the recovery process and cause more power penalty.

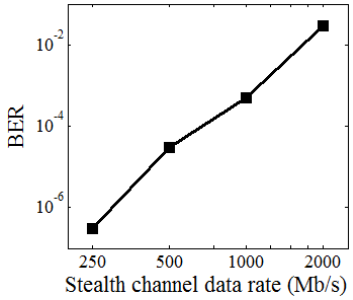

Fig. 7. Measurement of BER for different stealth channel data rates.

4. Conclusion

We have proposed and experimentally demonstrated a phase mask encryption method to cover stealth data bits and protect the security of the stealth channel. The phase mask is implemented by imposing phase modulation on the ASE noise, and can be easily changed by using different codes in the phase modulation. The phase mask code itself is protected by the wideband noise from the ASE, which is designed to be 16 times stronger than the noise in the stealth data. More than 18,000 codes are available for the phase mask. Without knowing the right phase mask code to recover the signal, the received signal has its amplitude reduced to less than 25% of its original value, in addition to having a randomized phase. Furthermore, the phase mask introduces only a 0.3 dBm power penalty to the stealth channel.

Acknowledgment

The authors would like to thank Yue Tian and John Chang in the Lightwave Communications Research Laboratory of Princeton University for their assistance. We are also grateful for the helpful comments of the reviewers.

#197344 - $15.00 USD Received 9 Sep 2013; revised 20 Nov 2013; accepted 26 Dec 2013; published 9 Jan 2014