Research Article Open Access

Ben Wu*, Matthew P. Chang, Naomi R. Caldwell, Myles E. Caldwell, and Paul R. Prucnal

Amplifier Noise Based Optical Steganography with Coherent Detection

Abstract: We summarize the principle and experimental setup of optical steganography based on amplified spontaneous emission (ASE) noise. Using ASE noise as the signal carrier, optical steganography effectively hides a stealth channel in both the time domain and the frequency domain. Coherent detection is used at the receiver of the stealth channel. Because ASE noise has short coherence length and random phase, it only interferes with itself within a very short range. Coherent detection requires the stealth transmitter and stealth receiver to precisely match the optical delay, which generates a large key space for the stealth channel. Several methods to further improve optical steganography, signal to noise ratio, compatibility with the public channel, and applications of the stealth channel are also summarized in this review paper.

Keywords: Amplified spontaneous emission, optical fiber communication, optical steganography

DOI 10.2478/coph-2014-0003
Received July 31, 2014; accepted October 26, 2014

1 Introduction

The open access and multi-user communication network requires transmitted information to be properly controlled and secured. Tremendous effort has been spent to secure communication networks with software. However, software solutions are based on and also limited by the existing functions of physical layer network. As the bottom layer in the open system interconnection (OSI) model [1], the properties of the physical layer determine the performance of the network. Instead of consuming the capacity of the existing network, providing security control in the physical layer creates more resources [2]. Moreover, instead of being limited by the available functions of the physical layer that may not be designed for security purpose, physical layer security changes existing hardware and designs new hardware for solving the security issue. Since optical fiber components are major constituents of the communication network, and fiber network forms the backbone of the Internet [3], optical and photonic layer security is especially important to control and secure communication networks.

Optical encryption and optical steganography are two effective approaches to protect optical networks [3]. Optical encryption changes the transmitted data into unreadable signals [4–6], so without knowing the key for the encryption process, an eavesdropper cannot decrypt the signal and recover the data. Compared with a traditional software based encryption method, optical encryption can achieve higher speed and lower latency. Optical encryption is also more secure since it does not radiate electromagnetic signatures in the encryption process and confines the light wave signals within fibers [2, 3]. Optical XOR logic, optical chaos encryption and optical interference encryption are different encryption techniques that have previously been studied. Optical XOR uses a fiber component to achieve the XOR function, which encrypts the transmitted signal sequence with the encryption sequence [5–11]. 20 Gb/s real time encryption has been achieved by optical XOR logic [6]. Optical chaos communication is another approach for optical encryption. By injecting the data into a chaos system, the optical chaos transmitter encrypts the data into noise-like signals [12–14]. Compared with optical XOR logic, the benefit of optical chaos encryption is that it encrypts the signal as analog noise. If the eavesdropper cannot decrypt the data when receiving the signal, he will lose the data and cannot use post-processing techniques to digitize and recover the signal.

Optical interference encryption has recently been proposed and experimentally demonstrated [15, 16]. It has the same advantages as optical chaos encryption in that it en-

***Corresponding Author: Ben Wu:** Princeton University, E-mail: benwu@princeton.edu
Matthew P. Chang: Princeton University, E-mail: mpchang@princeton.edu
Naomi R. Caldwell: Princeton University, E-mail: naomirosecaldwell@gmail.com
Myles E. Caldwell: Princeton University, E-mail: mycaldwell@optonline.net
Paul R. Prucnal: Princeton University, E-mail: prucnal@princeton.edu

crypts the data as analog noise. This encryption technique is based on an interference cancellation technique that has been widely studied [17–20]. The transmitted signal is covered with analog interference of larger amplitude, so without matching the phase and amplitude of the interference at the receiver, the eavesdropper cannot cancel the interference and recover the noise. The phase and amplitude forms a dynamic two-dimensional key space for the encryption process. Compared with chaos encryption and optical XOR logic, this method is easiest to deploy and does not require strong optical power to generate the nonlinear effect. Although optical encryption protects the transmitted data, it still exposes the existence of the signals. Once the eavesdropper knows that the signal exists, he can search the key space and try to recover the signal. Sometimes, just the existence of the encrypted signal exposes the communication between the transmitter and the receiver and can lead to malicious attacks [2]. In the present case, a stealth channel is required to hide the transmitted signal in plain sight, which is called optical steganography.

Optical steganography was first proposed in 2006 [21] and experimentally demonstrated in 2007 [22]. When it was first proposed, the stealth channel used a mode locked laser with low power to transmit signals [23]. Strong dispersion is applied to the stealth channel so that a stealth pulse is stretched into noise-like signals. Because the power of the original pulse is already 15 – 20 dB lower than the public channel, the stretched pulse has an amplitude low enough to be merged into the noise of the public channel. The stealth channel has been demonstrated to be compatible with the public channel with different modulation formats [24–31]. In 2013, a new optical steganography method was experimentally demonstrated [32, 33]. Instead of mimicking the noise, this method uses the amplified spontaneous emission (ASE) noise that already exists in the system to transmit the stealth signals. In the spectral domain, the ASE noise carrying the stealth signal has the same spectrum as the ASE noise from the erbium doped fiber amplifier that originally existed. In the time domain, the stealth channel benefits from the short coherence length of the ASE noise combined with the fact that the receiver has to match the optical delay in order to detect the existence of the phase modulated data.

In this paper, we summarize the most recent developments of optical steganography based on ASE noise and analyze their applications to network security.

2 Principle of Optical Steganography

2.1 Optical steganography with coherent detection

The experimental setup for a stealth transmitter and stealth receiver is shown in Fig. 1(a). The transmitter and receiver form a Mach-Zehnder interferometer [32]. ASE noise comes from an EDFA without input. The stealth signal is carried by ASE noise using phase modulation (red light path in Fig. 1(b)). Because the ASE noise has completely random phase, it is only coherent to itself within a very short coherence length. To phase demodulate the stealth signal, a copy of ASE noise without modulation is also sent by the transmitter (blue light path in Fig. 1(b)). If the red light path and the blue light path match the optical delay within the coherence length of the ASE noise, interference occurs at the detector and the stealth channel can be demodulated. If the red light path and the blue light path do not match the optical delay length, the stealth channel is exactly the same as ASE noise and is hidden in the time domain.

In the experiment, the tunable optical delay (t1 in Fig. 1(b)) creates an additional 10m of optical delay length difference at the transmitter, so the blue path at the receiver needs to compensate the 10m to incur the interference effect and demodulate the stealth signal. To enable this, another optical delay (t2 in Fig. 1(b)) is added to the blue light path at the receiver, allowing the red light path and blue light path in Fig. 1(b) to have the same length. The optical splitter cannot differentiate the modulated signal and reference signal, so they can also be split in the way shown in Fig. 1(c). In this case, the red light path is 20 m longer than the blue light path. Since 20 m is much longer than the coherence length of ASE noise, which is 370 μm [32], these two paths in Fig. 1(c) do not cause interference to the stealth signal; however, they will introduce more ASE beating noise.

2.2 Improvement of optical steganography – phase mask

The short coherence length of ASE noise provides a large key space for hiding the stealth channel, and dynamic control to the optical delay length has been demonstrated by using tunable optical delays. However, changing the optical delays requires mechanical devices and the rate of the delay length change is limited to the order of several sec-

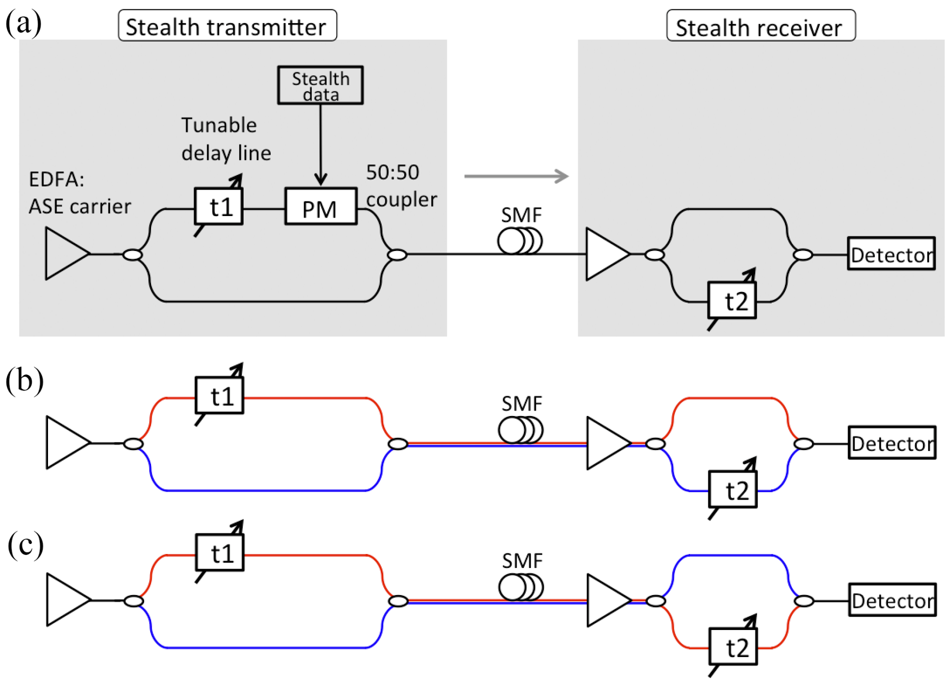

Figure 1: (a) System demonstration of hiding the stealth channel in the public network (EDFA: erbium doped fiber amplifier; T: optical tunable time delay; PM: phase modulator; SMF: single mode fiber) (b) and (c) Two possible light paths for the stealth channel.

onds. Even piezoelectric ceramic controlled fiber stretchers, which improve the tuning rate to the order of milliseconds, are still slow compared with the stealth data rate, which ranges from 250 Mb/s to 2 Gb/s. Moreover, the tunable range of the piezoelectric ceramic controlled fiber stretcher is limited by its rate of change. To improve the security of the stealth channel and protect it against potential eavesdroppers that may use brute force to scan the key space, a faster key changing technique is required.

A temporal phase mask has been proposed and experimentally demonstrated to provide a fast changing key for the stealth channel [34, 35]. The phase mask can change at the same rate as the data of the stealth channel.

The principle of the phase mask utilizes the white noise properties for the ASE noise [34]. The phase mask is added by having another phase modulator in series with the phase modulator for the stealth signal in Fig. 1(a). The data rate of the stealth channel is 250 Mb/s, and the data rate of the phase mask is 4 Gb/s, so each stealth bit is divided into 16 chips by the phase mask (Figs. 2(a) and (b)). Because the ASE noise band is flat up to at least 5GHz [35], a phase mask with a data rate 16 times higher than the stealth channel is 16 times noisier than the stealth channel. The stealth channel can reach a bit error rate (BER) of 10^{-6}, while the phase mask cannot be directly measured [34]. If an eavesdropper tries to use a low pass fil-

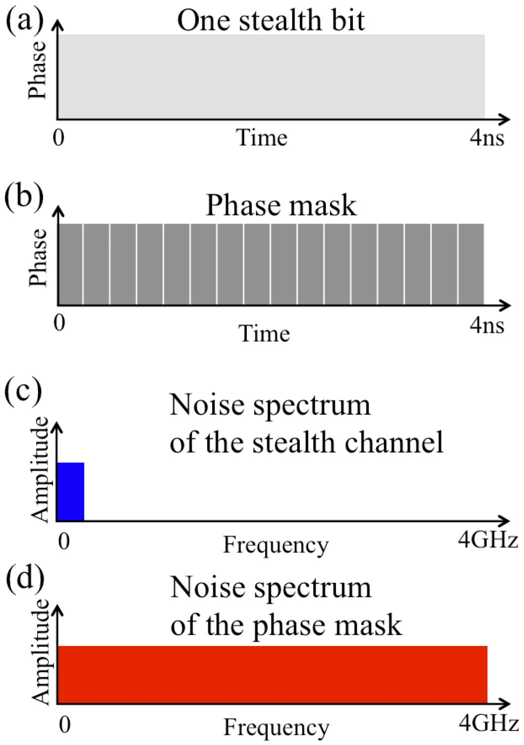

Figure 2: Schematic diagram of the temporal phase mask (a) A stealth bit (b) A phase mask for the stealth bit (c) Noise comes with the stealth signal in the frequency domain (d) Noise comes with the phase mask in the frequency domain.

ter to remove the phase mask, this process also corrupts the stealth data, causing the stealth bit to have its amplitude reduced and phase randomized. For a 16-bit sequence, more than 18,000 codes out of 216 combinations can be used for the phase mask [34].

The phase mask is controlled by an electric signal that is injected into the phase modulator. Changing the phase mask can be easily achieved by programing the electric signals applied to it. Since the phase mask is protected by the noise properties of ASE, it is especially important to analyze the signal to noise ratio (SNR) of the stealth channel, which is summarized in section 3.

2.3 Improvement of optical steganography – multichannel

The data rate and capacity of the stealth channel is limited by the noise properties of the ASE used. The maximum data rate of the stealth channel based on the interferometer structure in Fig. 1 is 2 Gb/s, which needs forward error correction (FEC) techniques to reduce the BER of 10^{-4} to error free. The FEC also introduces redundancy to the stealth channel and further affects the capacity of the stealth channel. To increase the capacity, multichannel or wavelength divisional multiplexing (WDM) stealth transmission is needed.

WDM stealth transmission has been demonstrated by using part of the ASE spectrum to carry a stealth channel [36]. The ASE spectrum is divided using a bandpass optical filter with full width half maximum (FWHM) of 1.1 nm. Multi-stealth channels with channel interval of 1.6 nm have been demonstrated. Since the ASE spectrum spans from 1520 nm to 1560 nm, the 40 nm spectrum range supports a maximum of 25 stealth channels.

Besides increasing the capacity of the stealth channel, WDM optical steganography also improves the security of the stealth channel. The eavesdropper needs to find which part of the spectrum has been deployed to carry the stealth channel [36]. The WDM optical steganography also improves the flexibility of utilizing the stealth channel in the public network. Since the ASE noise may not accumulate at the same rate in the entire ASE spectrum, the WDM optical steganography system can pick up the band that accumulates the desired amount of ASE noise to carry stealth signals.

The drawback of using part of the ASE spectrum is that it increases the coherence length of the stealth signals [36]. Since the spectrum is the Fourier transform of the time domain signal, a decrease of the spectrum width leads to an increase of the coherence length. However, this can be compensated by using a longer optical delay length difference at the transmitter. Because the phase of the ASE noise is completely random, there is no limit on the optical delay length difference that can be applied at the transmitter. The increased coherence length is only 2.5 mm when the optical spectrum has a 1.1 nm width. It is practical to generate an optical delay on the order of a kilometer by single mode fiber with an optical loss of 0.2 dB/km

3 Signal to Noise Ratio Analysis of Optical Steganography

Since the stealth channel is carried by ASE noise, both the signal and the noise of the stealth channel are related to the power of the ASE noise [37]. The calculation of SNR of the stealth channel is fundamentally different from the calculation of SNR of the public channel. In the public channel, the noise comes from thermal noise, shot noise, and beating noise from ASE after the public signal goes through optical amplifiers [38, 39]. The shot noise variance is proportional to the optical signal power of the public channel, while the thermal noise and beating noise do not depend on the signal power of the public channel. Since the power of the signal current is proportional to the square of the optical signal power of the public channel, the SNR of the public channel always increases with the signal power. The case is different for the stealth channel. The SNR saturates when the signal power of the stealth channel keeps increasing [37]. This is because both the beating noise variance and the signal current power are proportional to the square of the ASE noise power. When the signal power, which is also the ASE noise power, increases to a certain level where the ASE beating noise dominates, the SNR does not increase with the signal power and saturates at a constant. The saturation level depends on the ratio of optical bandwidth of the ASE noise to the electrical bandwidth of the stealth system [37, 40, 41]. The saturation ASE power depends on the thermal noise level of the receiver.

4 Optical Steganography in Public Network

4.1 Hiding stealth channels in the public network

The stealth channel can be introduced to the public network when the public channel goes through optical am-

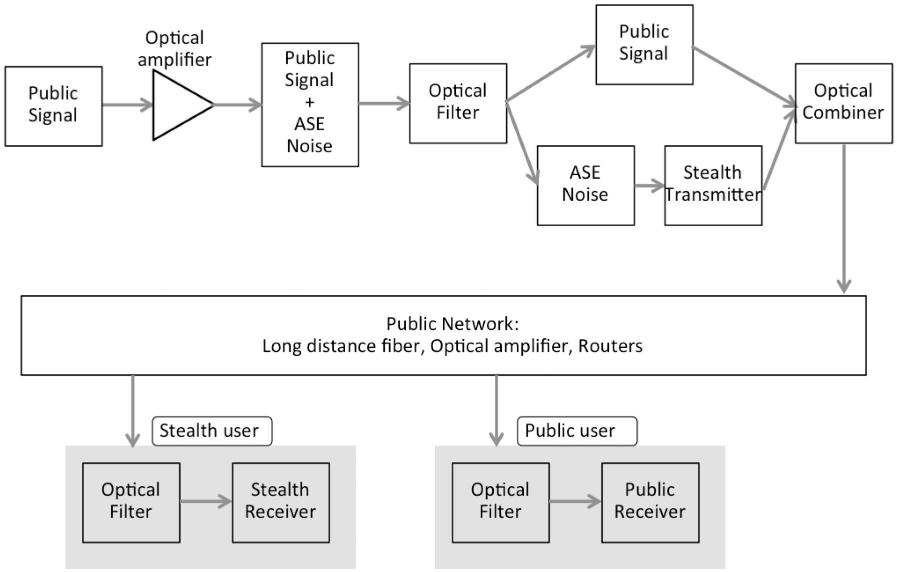

Figure 3: Schematic diagram of hiding stealth channels in the public network.

plifiers, and the ASE noise accumulates to a certain level [36, 37]. Fig. 3 shows the schematic diagram of introducing a stealth channel into the public network. The optical amplifiers that amplify the public channels also generate the ASE noise. An optical filter can be used to separate the ASE noise from the public channels. The public channels go through the stealth transmitter without loss, while the stealth signals are carried by the ASE noise in the stealth transmitter. The stealth signal can be amplified and injected back to the public channel so that the optical spectra before and after the stealth channel is added are the same [36]. The stealth channel can share the standard single mode fiber and fiber amplifiers in the public network to transmit over long distances. At the receiver, the same optical filter can be used to separate the stealth channel from the public network. The optical delay need to be matched to recover the stealth signals.

4.2 Applications of optical steganography

Optical steganography provides an extra channel with high level of security but small capacity. The stealth channel can be used for key distribution for the public channels (Fig. 4). The key for the encryption process is usually shorter than transmitted data, while it needs a higher security level than the data, so the stealth channel can be used for key distribution between the public transmitter and receiver. Besides key distribution, the stealth channel can also carry user authorization information to identify users in the public channels.

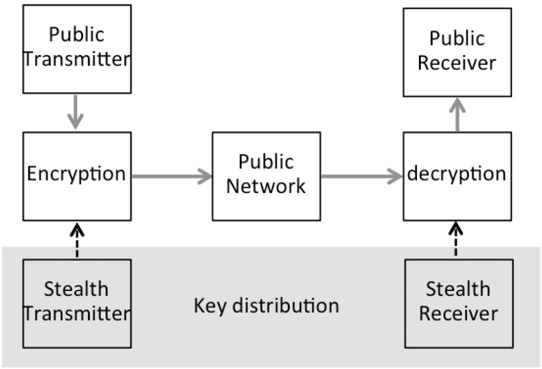

Figure 4: Schematic diagram of applying stealth channels for key distribution.

5 Conclusion

We summarize the principle of the optical steganography based on ASE noise. The stealth channel is carried by ASE noise, which hides the signal in both time domain and frequency domain. Coherent detection is applied at the stealth receiver. Two techniques to improve the performance of the stealth channel are introduced. The phase mask technique provides a fast changing key to the stealth channel. WDM optical steganography increases the capacity and flexibility of the stealth channels.

We also analyze the system performance of the stealth channel. Using ASE noise as the signal carrier, the system performance of the stealth channel is fundamentally different from the public channel. Since both the signal power and noise power increase with ASE noise, the SNR saturates when ASE beating noise dominates the noise in the stealth channel.

The stealth channels can be introduced into the public network when the public signal goes through optical amplifiers, which generate ASE noise. The stealth channels can share single mode fiber and optical amplifiers with the public channels for long distance transmission. Because optical steganography provides a high level of security, the stealth channel can be used to transmit the private key for encryption processes and authorization information for public channels.

References

[1] H. Zimmermann, IEEE T. Commun. 28, 425 (1980).

[2] B. Wu, B. J. Shastri, and P. R. Prucnal, In: B. Akhgar and H. Arabnia, ed. Waltham (Ed.), Emerging trends in ICT security, Elsevier, MA, 2014) 173.

[3] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, IEEE Trans. Inf. Forensics Security, 6, 725 (2011).

[4] Z. Wang, M. P. Fok and P. R. Prucnal, Journal of Cyber Security and Mobility, 83 (2012).

[5] K. Vahala, R. Paiella, and G. Hunziker, IEEE J. Sel. Toptics Quantum Electron. 3, 698 (1997).

[6] K. Chan, C. K. Chan, L. K. Chen, and F. Tong, IEEE Photon. Technol. Lett. 16, 897 (2004).

[7] M. P. Fok and P. R. Prucnal, Opt. Lett. 34, 1315 (2009).

[8] M. P. Fok and P. R. Prucnal, IEEE Photon. Technol. Lett. 22, 1096 (2010).

[9] H. Soto, D. Erasme, and G. Guekos, IEEE Photon. Technol. Lett. 13, 335 (2001).

[10] J. H. Kim, Y. M. Jhon, Y. T. Byun, S. Lee, D. H. Woo, and S. H. Kim, IEEE Photon. Technol. Lett. 14, 1436 (2002).

[11] M. Jinno and T. Matsuoto, Opt. Lett. 16 220 (1991).

[12] G. D. VanWiggeren and R. Roy, Science 279, 1198 (1998).

[13] A. Argris, D. Syvridis, L. Larger, V. A. Lodi, P. Colet, I. Fischer, J. G. Ojalvo, C. R. Mirasso, L. Pesquera and K. A. Shore, Nature 438, 343 (2006).

[14] L. Yang, L. Zhang, R. Yang, L. Yang, B. Yue, P. Yang, Opt. Commun. 285, 143 (2012).

[15] B. Wu. M. P. Chang, B. J. Shastri, Z. Wang, and P. R. Prucnal, Opt. Express 22, 14568 (2014). http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-22-12-14568

[16] B. Wu, M. P. Chang, Z. Wang, B. J. Shastri, P. R. Prucnal, Proc. CLEO, Jun. 2014, San Jose, US (OSA 2014) AW3P.5.

[17] J. Suarez, and P. R. Prucnal, IEEE Microw. Wirel. Co. 21, 507 (2011).

[18] J. Suarez, K. Kravtsov, and P. R. Prucnal, IEEE Trans. Instrum. Meas. 60 598 (2011).

[19] M. P. Chang, M. Fok, A. Hofmaier, and P. R. Prucnal, IEEE Microw. Wirel. Co. 23, 99 (2013).

[20] J. Chang, and P. R. Prucnal, IEEE Microw. Wirel. Co. 23, 377 (2013).

[21] B. B. Wu and E. E. Narimanov, Opt. Express 14, 3738 (2006).

[22] K. Kravtsov, B. B. Wu, I. Glesk, P. R. Prucnal, and E. Narimanov, Proc. IEEE/LEOS Annual Meeting, Oct 21-25, 2007, (Lasers and Electro-Optics Society 2007) 480.

[23] Z. Wang and P. R. Prucnal, IEEE Photon. Technol. Lett. 23, 48 (2011).

[24] P. R. Prucnal, M. P. Fok, K. Kravtsov, and Z.Wang, Proc. the 16th Int. Conf. Digital Signal Processing (DSP), Jul. 5-7 2009, (IEEE 2009) T3B.4.

[25] B. B. Wu, P. R. Prucnal, and E. E. Narimanov, IEEE Photon. Technol. Lett. 18, 1870 (2006).

[26] B. B. Wu and E. E. Narimanov, Opt. Express 15, 289 (2007).

[27] X. Hong, D. Wang, L. Xu and S. He, Opt. Express 18, 12415 (2010). http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-18-12-12415

[28] B. B. Wu, A. Agrawal, I. Glesk, E. Narimanov, S. Etemad, and P. Prucnal, in Proc. CLEO/QELS, May 4-9, 2008, San Jose, US, (OSA, 2008) CFF5.

[29] Y.-K. Huang, B. B. Wu, I. Glesk, E. E. Narimanov, T. Wang, and P. R. Prucnal, Electron. Lett. 43, 1449 (2007).

[30] Z. Wang, M. P. Fok, L. Xu, J. Chang, and P. R. Prucnal, Opt. Express 18, 6079 (2010).

[31] M. P. Fok and P. R. Prucnal, Electron. Lett. 45 179 (2009).

[32] B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, Opt. Express 21, 2065 (2013). http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-21-2-2065

[33] B. Wu, Z. Wang, B. J. Shastri, Y. Tian, and P. R. Prucnal, Proc. CLEO, Jun 9-14, 2013, San Jose, US, (OSA, 2013) AF1H.5.

[34] B. Wu, Z. Wang, B. J. Shastri, M. P. Chang, N. A. Frost, P. R. Prucnal, Opt. Express, 22, 954 (2014). http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-22-1-954

[35] B. Wu, Z. Wang, B. J. Shastri, Y. Tian and P. R. Prucnal, Proc. IEEE Photonics Conference, Sep. 8-12, 2013, Bellevue, US, (IEEE, 2013) MG3.3.

[36] B. Wu, A. N. Tait, M. P. Chang, P. R. Prucnal, Opt. Letters 39, 5925 (2014). http://www.opticsinfobase.org/ol/abstract.cfm?uri=ol-39-20-5925

[37] B. Wu, B. J. Shastri, P. R. Prucnal, Photon. Technol. Lett. 26, 1920 (2014) http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6866870&tag=1

[38] R. C. Steele, G. R. Walker, and N. G. Walker, IEEE Photon. Technol. Lett. 3, 545 (1991).

[39] N. A. Olsson, J. Lightw. Technol. 7, 1071(1989).

[40] E. Desurvire, Erbium-doped fiber ampplifiers, principle and applications, 2nd ed., (Wiley-Interscience, Hoboken, NJ, 2002) 355.

[41] E. Desurvire, Applied Optics 29, 3118 (1990).