Stealth Transmission of Time Domain Spectral Phase Encoded OCDMA Signal over WDM System

Zhensen Gao[1], Xu Wang[1] and Nobuyuki Kataoka[2] and Naoya Wada[2]

1. Joint Research Institute for Integrated Systems, EPS, Heriot-Watt University, UK, Email: x.wang@hw.ac.uk
2. National Institute of Information and Communications Technology (NICT), Tokyo, Japan

Abstract: 1.25Gbps time domain spectral phase encoded OCDMA signal with 32-chip, 40Gchip/s optical codes has been stealthily transmitted over public 10Gbps WDM channel. Error-free transmission has been achieved for both the public and stealth channels.

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

1. Introduction

Optical code division multiple access (OCDMA) technique has drawn considerable research interest over the past decade due to its unique advantages of high speed all-optical processing, fully asynchronous transmission with low-latency access, soft capacity on demand and so on [1]. Among all the other potential advantages, OCDMA is also considered as a potential candidate to provide secure communication in future network since each user is assigned an optical code from a large code space in OCDMA system and different users are distinguished by its unique code [2]. Recently, we proposed a novel time domain spectral phase en/decoding (SPED) OCDMA scheme, and experimentally demonstrated 1.25Gbps OOK data transmission with 16-chip, 20Gchip/s optical codes by using a pair of dispersive fibres and a high speed phase modulator [3]. This technique is very robust to the wavelength drift of the laser source. By using a linearly chirped fibre Bragg grating (LCFBG) to serve as a dispersive device, the SPED-OCDMA scheme is more compact and stable. Moreover, this scheme is very flexible in reconfiguring the optical codes and compatible with the fibre optical system, exhibiting the potential to enhance the network security.

On the other hand, optical steganography is proposed to provide additional layer of network security by hiding the existence of data transmission underneath public channel, making it imperceptible in the public channel [4]. In optical steganography, a large amount of group velocity dispersion (GVD) is used to spread the stealth signal over time, and therefore, the peak power of the stealth signal becomes sufficiently below the level of the system noise [5]. It is very difficult for an eavesdropper to restore the stealth signal from the public channel without the knowledge of the spreading function.

In this paper, we proposed and experimentally demonstrated security enhancement of the stealth channel by combining the time domain spectral phase en/decoding OCDMA technique and conventional group velocity dispersion based approach. The stealth channel is achieved by temporally broadening the pulse via GVD using LCFBG and phase modulation with 32-chip, 40Gchip/s optical code using a high speed phase modulator. The generated OCDMA signal in the stealth channel can be fully hidden into the public WDM channel and spectrally phase encoded simultaneously, making our scheme more compact and secure to stealthily transmit the OCDMA signal over a public WDM system.

2. Principle and experimental setup

Figure 1 shows the experimental setup for the proposed stealth transmission of time domain spectral phase encoded OCDMA signal over a public WDM channel. In the experiment, the WDM signal is generated by a CW laser

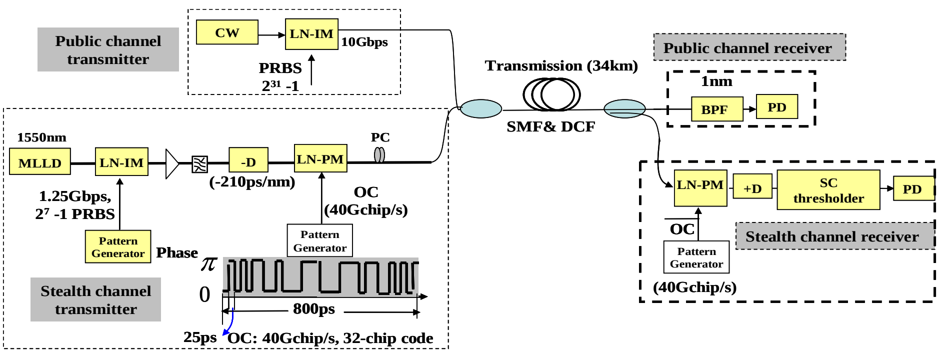

Fig.1 Experimental setup for the stealth OCDMA signal transmission over WDM public channel

followed by an intensity modulator driven by 2^{31}-1 pseudorandom bit sequence (PRBS) OOK data operating at 10Gbps. In the stealth channel, a mode locked laser diode (MLLD) centered at 1550.28nm is used to generate a series of optical pulse trains with FWHM of 4ps at repetition rate of 10GHz. An intensity modulator driven by 2^{7}-1 PRBS data is then used to modulate the pulse trains and generate the 1.25Gbps OOK data. The modulated pulse trains are temporally stretched in the whole bit period through GVD by cascading three identical LCFBGs with total dispersion of -210ps/nm for stealth channel hiding and optical encoding. Different spectral components spread into different position in time domain. No obvious overlap between two adjacent broadened pulses has been observed due to the unique spectral response of the LCFBGs which act as a dispersive device and band-pass filter simultaneously. The broadened pulse is then directed into a phase modulator driven by 32chips, 40Gchip/s optical code patterns (corresponding to 32chips, 15GHz/chip spectral code patterns) to generate the time domain spectral phase encoded stealth OCDMA signal. An optical delay line is used to guarantee the code patterns precisely modulate the phase of the desired spectral component of the broadened pulse. Four different Gold codes with 31chips plus a zero are used in the experiment: OC1: 10001100001111001111010101001110, OC2: 11101011001100011011110111111000, OC3: 00100101001010110010110010010000 and OC4: 10111001000111 100000111001000110. The auto-correlation of the four codes exhibit well defined needle peak and the average power contrast ratio (P/C) increases up to 10 by using the 32-chip, 40Gchip/s code patterns.

At the receiver side, a portion of the received signal is passed through a BPF with 3dB bandwidth of 1nm for public channel detection using a conventional energy detector. While another portion is launched into the second phase modulator driven by the complementary code $\overline{OC}$ for the stealth signal detection. Synchronization between the encoding and decoding is highly required in order to correctly decode the stealth signal. Even if the stealth signal is revealed, it is still very difficult for an eavesdropper to correctly decode the stealth OCDMA signal without knowledge of the code used in the stealth channel and accurate time coordination. After that, the other LCFBGs with opposite dispersion of +210ps/nm are used to compress the correctly decoded signal, such that the stealth channel appears above the public channel. Finally, a super-continuum (SC) based optical thresholder composed of a preamplifier EDFA and a piece of 2000m dispersion-flattened-fiber (DFF) followed by a 5nm BPF is used to extract the stealth OCDMA signal from the public WDM system.

3. Results and discussion

In the experiment, the stealth signal is firstly input into the LCFBGs for pulse broadening and then directed into the phase modulator for optical encoding to generate the spectral phase encoded OCDMA signal. By properly adjusting the optical attenuator and polarization controller, the stealth OCDMA signal is temporally hidden underneath the public WDM channel. The power ratio (*Pr*) of the public channel and stealth channel is about 13dB. The eye diagram of the public WDM channel with and without the stealth OCDMA channel are shown in Figure 2 (a) and (b), respectively. The two eye diagrams are indistinguishable and the stealth channel can not be observed in Fig. 2 (a). Amplified spontaneous emission (ASE) noise from an erbium doped fiber amplifier has been launched into the system to spectrally hide the stealth channel into the public channel. The spectra of the public WDM channel with and without stealth channel are shown in Fig. 2 (c) (i) and (ii), respectively. The two spectra are indistinguishable as well. The spectrum of the stealth OCDMA signal with ASE noise is shown in Fig.2 (c) (iii). The power spectra of the stealth signal and ASE noise are 40dB lower than the public channel. Therefore, the waveform and the spectrum of the stealth channel are fully hidden into the public channel. A span of single mode fiber (SMF) and dispersion compensation fiber (DCF) with total length of 34km are used for transmission.

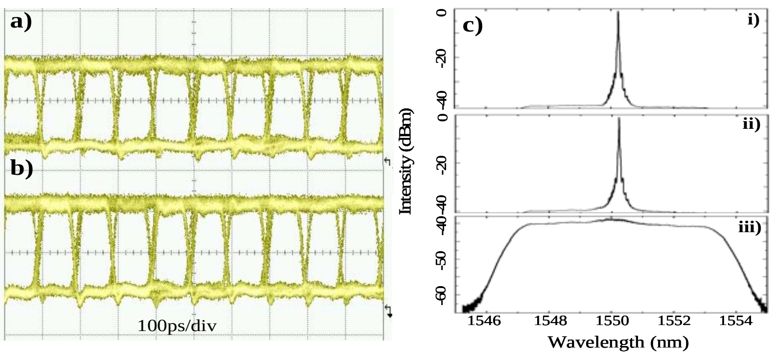

Fig.2 (a) Eye diagram of public WDM channel with OCDMA stealth channel (b) Eye diagram of public WDM channel without OCDMA stealth channel (c) Spectrum of public WDM channel without (i) and with (ii) OCDMA channel and (iii) spectrum of OCDMA stealth channel with ASE noise

In the stealth channel detection, the public WDM channel will also be phase modulated and then temporally broadened by the LCFBGs, and as a result, the public signal exhibits like a noise in time domain. Figure 3 (a) shows the correctly decoded signal for OC2 with WDM signal. The stealth OCDMA signal has been recovered above the public WDM signal. The extracted OCDMA signal after the SC based optical thresholder for the correctly decoded signal (a) is shown in Fig.3 (b). The public WDM signal has been significantly suppressed by the optical thresholding. Fig. 3(c) shows the waveform of the incorrectly decoded signal with public WDM signal. In this case, the incorrectly decoded signal still submerges in the public channel. As the SC generation requires high input peak power, the incorrectly decoded stealth OCDMA signal can not be extracted from the public channel.

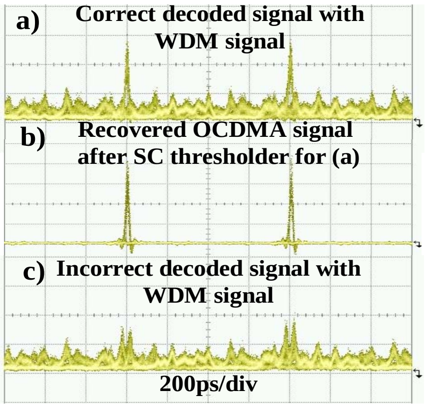

Fig.3 (a) Autocorrelation signal for OC2 with WDM channel. (b) Recovered stealth channel signal after SC thresholder and (c) Cross-correlation signal for OC2 with WDM channel

Figure 4 (a) shows the measured bit-error-rate (BER) of the stealth OCDMA signal. Error free transmission has been achieved for the stealth channel with four different codes. In the absence of the stealth signal en/decoding, there is only 1dB power penalty in the existence of the WDM signal. The en/decoding induces ~2dB power penalty due to the non-ideal decoding. The measured BER for the public WDM channel with different power ratio is shown in Fig.4 (b), from which one can see that the effect of the OCDMA signal on the public channel is very small, and less than 1dB power penalty is obtained when vary the power ratio (*Pr*) between 10dB to 15dB. To investigate the influence of public channel on the stealth channel, the BER performance of the stealth channel for different power ratio is also measured as shown in Fig. 4 (c). As the power ratio increases from 13dB to 19dB, the BER of the stealth channel gradually degrade from 10^{-10} to 10^{-2}. By utilizing identical phase modulator in the encoding and decoding side to improve the decoding performance of the OCDMA signal, higher power ratio can be supported.

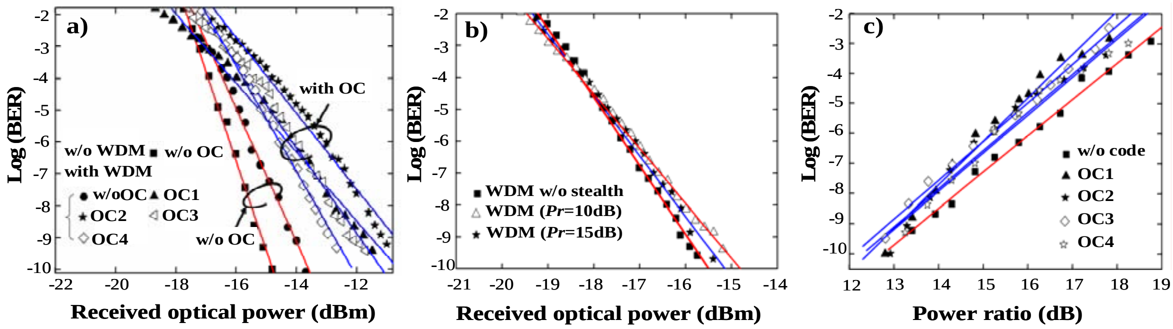

Fig. 4 (a) BER for stealth OCDMA channel (b) BER for public WDM channel (c) BER versus power ratio for stealth channel

4. Conclusions

We have proposed and experimentally demonstrated an approach to secure a 1.25Gbps stealth OCDMA channel transmission over a 10Gbps public WDM channel based on the time domain spectral phase en/decoding techniques and group velocity dispersion. The stealth OCDMA channel is spectral phase encoded in time domain using chirped fiber Bragg grating and a phase modulator. The LCFBG is used not only for temporally broadening the stealth channel signal but also for the spectral phase encoding. The stealth channel is fully hidden into the public channel in both spectral and time domain. Error free transmission has been achieved for both the stealth OCDMA channel and the public WDM channel. The proposed technique provides an effective and attractive approach for secure optical communication over an existing public WDM system.

5. References

[1] Xu Wang and Ken-ichi Kitayama, “Analysis of Beat Noise in Coherent and Incoherent Time-Spreading OCDMA”, J.Lightwave Technol. vol.22, no.10, pp. 2226-2235, Oct.2004
[2] A. Stock and E. H. Sargent, “The role of optical CDMA in access networks”, IEEE Commun Mag, vol.40, pp. 83-87, Sep.2002.
[3] Xu Wang and Naoya Wada, “Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA application”, Optics Exp. vol.15, no.12, pp.7319~ 7326, 2007
[4] K. Kravtsov, *et al*. “Stealth transmission over a WDM network with detection based on an all-optical thresholder”, Proc. LEOS, WH2, 2007.
[5] M. P. Fok,. *et al*. “Providing Network Security with Optical Signal Processing”, ICOCN, Singapore, Dec. 2008.