Optics Communications 407 (2018) 1–8

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Multi-bit wavelength coding phase-shift-keying optical steganography based on amplified spontaneous emission noise

Cheng Wang [a], Hongxiang Wang [a,b], Yuefeng Ji [a,b,*]

[a] State Key Laboratory of Information Photonics and Optical Communications, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] Beijing Advanced Innovation Center for Future Internet Technology, Beijing University of Technology, Beijing 100124, China

ARTICLE INFO

Keywords:
Optical steganography
Amplified spontaneous emission
Wavelength selection switch
Phase-shift-keying

ABSTRACT

In this paper, a multi-bit wavelength coding phase-shift-keying (PSK) optical steganography method is proposed based on amplified spontaneous emission noise and wavelength selection switch. In this scheme, the assignment codes and the delay length differences provide a large two-dimensional key space. A 2-bit wavelength coding PSK system is simulated to show the efficiency of our proposed method. The simulated results demonstrate that the stealth signal after encoded and modulated is well-hidden in both time and spectral domains, under the public channel and noise existing in the system. Besides, even the principle of this scheme and the existence of stealth channel are known to the eavesdropper, the probability of recovering the stealth data is less than 0.02 if the key is unknown. Thus it can protect the security of stealth channel more effectively. Furthermore, the stealth channel will results in 0.48 dB power penalty to the public channel at 1×10^{-9} bit error rate, and the public channel will have no influence on the receiving of the stealth channel.

1. Introduction

With the dramatic increase in network usage [1,2], ensuring the communications over optical network are secured becomes more and more important. Several approaches have been researched to enhance the security of optical communication networks at the optical layer [3], such as all-optical data encryption [4–6], optical steganography [7–15], optical chaos encryption [16–18] and quantum key distribution [19–21]. Optical XOR logic can encrypt the data with high speed and low latency, but the encrypted signal is still digitized and carries all information of the original data. If an eavesdropper records the encrypted data in a long time, the original data may be recovered by post-processing technique. Optical chaos encryption uses wideband chaotic analog signal to encrypt the transmitted data, and it can enhance the robustness and privacy of the system. However, the requirement of synchronization between the transmitter and the receiver is rigorous. Quantum key distribution can indicate the existence of an eavesdropper trying to obtain any information about the key, but the transmission range and data rate are limited by the noise and the severe attenuation in the single photo transmission channel [22].

Optical steganography can enhance the privacy of communication by hiding the stealth signal under the public signal and system noise, thus no one else knows the existence of stealth signal except the intended recipient. Most previous optical steganography schemes are based on stretching optical pulses and decreasing the peak power, through group velocity dispersion [7] or spectral-phase encoding [8]. However, the spectrum of the stealth signal is not sufficiently wide to match the spectrum of system noise, thus it is relative easier to detect the stealth signal in the spectral domain. To solve this problem, a good approach is to use the system noise to transmit signal directly.

In the past few years, several optical steganography schemes which use amplified spontaneous emission (ASE) noise as a carrier have been theoretically studied and experimentally demonstrated [9–13]. In 2013, an optical steganography scheme which utilizing the short coherence length characteristic of ASE noise has been proposed [9]. To further enhance the security of this scheme, a motorized controlled delay line is used to generate a “hopping” key. However, the changed speed of the delay length is limited to several seconds, thus the key based on optical delay is vulnerable to brute-force attack if an eavesdropper deploys a faster scanning technique. In 2014, a complementary encoder based on wavelength selection switch (WSS) has been proposed [10]. In

[*] Corresponding author at: State Key Laboratory of Information Photonics and Optical Communications, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China.
E-mail addresses: ee08b038@bupt.edu.cn (C. Wang), wanghx@bupt.edu.cn (H. Wang), jyf@bupt.edu.cn (Y. Ji).

http://dx.doi.org/10.1016/j.optcom.2017.08.054
Received 31 May 2017; Received in revised form 4 July 2017; Accepted 22 August 2017
0030-4018/© 2017 Elsevier B.V. All rights reserved.

this scheme, the modulated “signal ASE” is concealed under the public channel well in time domain. But in one bit cycle, the “signal ASE” only occupies half of wavelength channels in WSS. If an eavesdropper record the spectrum of modulated “signal ASE” in many different bit cycle, he can decide whether the transmitted bit is “1” or “0” by using real-time spectrum analyzer. Besides, the spectrum efficiency of the stealth channel is relatively lower as this method uses the entire channels in WSS to send only one bit information in a clock cycle.

In this paper, we propose a multi-bit wavelength coding phase-shift-keying (PSK) optical steganography method based on ASE noise. With the process of wavelength encoding and phase modulation, components in each wavelength channel have a phase shift 0 or π according to the assignment codes of WSS and corresponding data bits. The spectrum of “signal ASE” covers the whole channel in WSS all the time, thus the power spectrum of “signal ASE” remains unchanged. Besides, the stealth channel is not only encrypted by channels assignment codes, but also by the optical delay length differences at the transmitter. It forms a dynamic two-dimensional key space, hence the key space is enlarged considerably. Furthermore, we can increase the spectrum efficiency of stealth channel by sending multiple bits information simultaneously, and we will prove that it can reduce the probability of obtaining the stealth data for an eavesdropper at the same time.

2. Complementary coding PSK optical steganography system

The principle of complementary coding PSK optical steganography system is shown in Fig. 1. The ASE noise, as a carrier of the stealth channel, is split into two branches by a WSS. The WSS, which has 96 channels in total and the channel space is 50 GHz, allocates some channels to the first port according to code1 and distributes other channels to the second port according to code2 (the code describes the on/off state of corresponding wavelength, “1” represents the corresponding wavelength channel is turned on while “0” represents that is turned off). The PSK process of encoded ASE is similar to the process in [9]. The encoded signal by code1 inputs into a Mach–Zehnder interferometer (MZI). The signal from the upper arm of MZI is delayed by T_{tx1} via an optical tunable delay line (OTDL), and then modulated by the sequence of stealth data using a phase modulator. The signal from the lower arm is unmodulated. Similarly, for the encoded signal by code2, the signal in the upper arm of MZI is delayed by T_{tx2} via another OTDL and then phase modulated by the sequence of complementary stealth data. Furthermore, to guarantee the characteristic of modulated “signal ASE” is similar to ”original ASE” in time and spectral domain, the equalization of power and the synchronization between two branches of “signal ASE” are required. Hence, an additional OTDL and a variable optical attenuation (VOA) are used in two arms. After that, two modulated signals are coupled by a 50:50 coupler.

The optical delay T_{tx1} and T_{tx2} are much larger than the coherence time of encoded ASE noise, to make the signals from both arms of MZI are not interfere coherently. The ASE power is mainly concentrate on the spectral peak around 1530 nm with a full width half-maximum (FWHM) bandwidth of 10 nm [23], the measured coherence time is 1.24 ps [9]. During the wavelength encoding process, the profile of the spectrum and the bandwidth of ASE carrier are not altered, thus the coherence time is unchanged (i.e. $\tau_c = 1.24$ ps). The power of modulated signal is independent of the transmit bit as phase modulation is employed [24]. Thus the eavesdropper cannot determine whether “1” or “0” is transmitted in the time domain.

At the end of transmission, the authorized receiver uses a WSS which has the same configuration as transmitter to select related channels according to code1. Besides, he also needs to use another MZI and an OTDL with a delay shift T_{rx}, to compensate for the optical path difference (OPD) between the upper and the lower arms of MZI at the transmitter. If $\left|T_{tx1} - T_{rx}\right| \ll \tau_c$, the stealth data can be demodulated by coherent detection. Similarly, if we select related channels according to code2 and compensate for the delay of T_{tx2}, the complementary stealth data can be recovered using the same approach. Two common methods of coherent detection are homodyne balanced detection and phase diversity detection. We will analyze the performance of these two approaches as follows. We take the decoded signal according to code1 as an example, and assuming that the attenuation and dispersion can be compensated for completely.

We assume that the ASE noise from EDFA has an electrical field with complex amplitude $\boldsymbol{x}(t)$, and that of the encoded ASE by code1 after WSS is $\boldsymbol{x}_1(t)$. The autocorrelation function of $\boldsymbol{x}(t)$, $\boldsymbol{x}_1(t)$ are $R_x(t)$ and $R_{x_1}(t)$ respectively. $R_x(t)$ is defined as $R_x(\tau) \triangleq E\left[\boldsymbol{x}^*(t) \cdot \boldsymbol{x}(t+\tau)\right]$, where $E[.]$ represents the expected value over time and τ denotes the delay time. As described in [24], $\boldsymbol{x}(t)$ and $\boldsymbol{x}_1(t)$ can be modeled as a circular complex Gaussian bandpass process, thus $R_x(\tau)$ and $R_{x_1}(\tau)$ approximate to 0 when τ is much larger than the coherence time of ASE. The average power of encoded ASE by code1 can be represented as:

$$P_{in} = \frac{1}{2} E\left[\left|\boldsymbol{x}_1(t)\right|^2\right] = \frac{1}{2} E\left[\boldsymbol{x}_1^*(t) \cdot \boldsymbol{x}_1(t)\right] = \frac{1}{2} R_{x_1}(0). \tag{1}$$

The phase-modulated ASE signal by code1 has an electrical field with complex amplitude $\boldsymbol{y}(t)$, which can be given by:

$$\boldsymbol{y}(t) = \frac{1}{2}\left[-\boldsymbol{x}_1(t) + \boldsymbol{x}_1\left(\boldsymbol{t} - \boldsymbol{T}_{\boldsymbol{tx}1}\right) \cdot e^{-j \cdot 2\pi f_c \cdot T_{tx1}} \cdot e^{j\varphi_{mod}(t)}\right] \tag{2}$$

where f_c is the center frequency of ASE carrier that encoded by code1, $\varphi_{mod}(t) \in \{0, \pi\}$ is the phase shift according to the stealth data (i.e. $\varphi_{mod} = 0$ for binary 0, $\varphi_{mod} = \pi$ for binary 1).

At the receiver, we assume that the output voltage after the coherent detection is $V_{out}(t)$. If the coherent detection module uses a homodyne balanced detector configuration (see Fig. 1 in [24]), the electrical fields at both output ports of MZI can be written as $\boldsymbol{z}_1(\boldsymbol{t}) = \frac{1}{2}\left[\boldsymbol{y}(\boldsymbol{t}) - \boldsymbol{y}\left(\boldsymbol{t} - \boldsymbol{T}_{\boldsymbol{rx}}\right) \cdot e^{-j \cdot 2\pi f_c \cdot T_{rx}}\right]$, $\boldsymbol{z}_2(\boldsymbol{t}) = \frac{1}{2}\left[\boldsymbol{y}(\boldsymbol{t}) + \boldsymbol{y}\left(\boldsymbol{t} - \boldsymbol{T}_{\boldsymbol{rx}}\right) \cdot e^{-j \cdot 2\pi f_c \cdot T_{rx}}\right]$ respectively. A pair of photodiodes in this module are assumed to be perfectly linear with an identical responsivity R, and the gain of electrical amplifier after photodiodes is G, then we can obtain the expected value of demodulated output:

$$\begin{aligned} E\left[V_{out}(t)\right] &= RG \cdot E\left[\left|\boldsymbol{z}_1(\boldsymbol{t})\right|^2 - \left|\boldsymbol{z}_2(\boldsymbol{t})\right|^2\right] \\ &= \begin{cases} \frac{1}{4} RG \cdot R_{x_1}(\tau) \cdot \cos 2\pi f_c \tau & b_n = 0\left(\varphi_{mod} = 0\right) \\ -\frac{1}{4} RG \cdot R_{x_1}(\tau) \cdot \cos 2\pi f_c \tau & b_n = 1\left(\varphi_{mod} = \pi\right) \end{cases} \end{aligned} \tag{3}$$

where $\tau = \left|T_{tx1} - T_{rx}\right|$ is the total OPD between modulated signal and unmodulated signal, b_n is the nth bit. The output voltage reaches maximum value when the total OPD is zero ($T_{tx1} = T_{rx}$). From Eq. (3), we can obtain the modulated phase in each bit period. However, the output voltage is unstable because of the factor $\cos 2\pi f_c \tau$ [24]. Some phase synchronization mechanism can solve this problem, such as by applying a feedback loop [25] or a frequency dithering technique [26], but these approaches are rather complicated and difficult to be realized.

Phase diversity receiver can stabilized the output voltage in an easier way. The principle of phase diversity detection is explained in Fig. 5 in [24]. It contains a 90° hybrid and two differential pairs of photodiodes. Compared with homodyne balanced detection, the output voltage is more stable because the harmonic $\cos 2\pi f_c \tau$ disappeared. Otherwise, using the method of phase diversity detection can only obtain the relative phase between adjacent bit cycles. Hence, the transmit bit sequence should be differentially encoded before phase modulation.

3. Multi-bit wavelength coding PSK optical steganography system

Discussion presented above uses all the 96 wavelength channels in WSS to send only one bit information in a clock cycle. In other words, we use two output ports of WSS, with each port containing 48 channels, then two encoded ASE are phase modulated by data sequence and complementary data sequence respectively. In the following, we will discuss the case that using WSS to send multiple bits information simultaneously. We take two-bit wavelength encoding PSK optical