IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 26, 2019, accepted November 18, 2019, date of publication November 22, 2019,
date of current version December 10, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2955226

Performance Analysis of Multi-User Optical Steganography Transmission System Based on Filtered Amplified Spontaneous Emission Noise

GUORUI SU, TAO PU, JILIN ZHENG, AND YETENG TAN
College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China

Corresponding author: Tao Pu (nj_putao@163.com)

This work was supported in part by the Photonics Information Technology Laboratory, and in part by the National Natural Science Foundation of China under Grant 61475193, Grant 61177065, and Grant 61174199.

ABSTRACT We propose a multi-user optical steganography transmission system based on the filtered amplified spontaneous emission (ASE) noise for the first time. The stealth signal can be hidden in the public channel in the time and frequency domain. The proposed multi-user transmission system can improve the capacity of stealth channel through increasing the number of stealth users, in order to overcome the major limitation of the single stealth channel transmission based on the ASE noise. Meanwhile, system performance of optical steganography system is theoretically analyzed and simulation demonstrated. The signal-to-noise ratio (SNR) of the stealth channel and the public channel are derived and analyzed. The interaction between the public channel and the stealth channel is investigated based on bit rate, transmission distance, optical bandwidth of the stealth user, and power spectral density of the ASE noise, which can affect the capacity of the stealth channel. In addition, the additional layer security of the stealth channel is analyzed in the proposed multi-user optical steganography system, and simulation results show that this approach is efficient and the security of the stealth user can be guaranteed.

INDEX TERMS Optical fiber transmission, amplified spontaneous emission, optical steganography.

I. INTRODUCTION

With the increased accessibility of optical networks, it is more and more important to promise the security of the optical communication network. Various approaches to enhance the security had been researched in optical network [1]–[5], e.g., chaos-based encryption, quantum cryptography and optical encryption method based on wideband analog noise. Different from the above, optical steganography aims at transmitting data secretly through a stealth channel hidden under public optical communication.

In the existing work, the optical steganography transmission system based on amplified spontaneous emission (ASE) noise has been theoretically analyzed and experimental demonstrated [6]–[8]. The carrier of the stealth channel is the ASE noise generated by Erbium doped fiber amplifier (EDFA), whose spectrum is widely existed in the optical networks. The spectrum of the modulated ASE carrier is identical with that of the original ASE noise in the public channel, which means the stealth signal can be hidden in frequency domain. Moreover, the widely stretched pulse of the modulated ASE noise has a lower amplitude through the chromatic dispersion device [9], [10] or optical code-division multiple-access (OCDMA) encoder [11], [12]. The processed pulse of the stealth channel hidden under the public channel will not be found in the time domain. At the same time, the spectrum of super-continuum (SC) light source is widely exists in the public channel, which is the same as that of the ASE noise. Optical steganography transmission system based on SC light source is also investigated in [13]. At the same time, both amplitude modulation [7], [8], [10], [12], [13] and phase modulation [6], [8], [11], [14] optical stealth transmission systems are studied by researchers. The results show that the stealth signal can be hidden in the time and frequency domain of the public channel in the above optical steganography transmission system.

Optical steganography based on ASE noise effectively hide the stealth signal in the public network, however, the capacity

The associate editor coordinating the review of this manuscript and approving it for publication was Rene Essiambre.

of the stealth channel is limited [8]. In order to increase the stealth capacity, multi-channel transmission is realized by using different parts of the ASE noise. The experiment results indicate that the maximum error-free transmission of 25 stealth channel is achieved at 2.5 Gb/s, when the forward error correction (FEC) with Reed-Solomon codes is used.

Without knowing the existence of the stealth channel in both the time and frequency domain, the privacy of the steganography transmission system has been realized in the existing researches. Meanwhile, the confidentiality of steganography system can be supported by optical processing technology without generating an electrical signature [14], [15], which includes the chromatic dispersion processing and the OCDMA technology.

Although the privacy and the confidentiality are promised in the optical steganography system, the stealth signal will be found when the ASE carrier of the stealth channel is detected by the eavesdropper. Another approach is needed to solve the security issue for the stealth channel. The carrier spectral of the stealth user must be divided as small as possible, and employed in an efficient way.

In this paper, a multi-user optical steganography transmission system is firstly proposed to further improve the capacity of the stealth channel. Using the filtered ASE noise as the signal carrier, the stealth signal can be hidden in the public channel in the time and frequency domain. We find that the capacity of the stealth channel can be improved in the proposed scheme, when the multiple stealth users are adopted. The proposed system model is introduced and the signal-to-noise ratio (SNR) formula of the public channel and stealth channel is derived. When the beat noise is dominant, the SNR of the public channel and stealth channel is influenced by the system parameters. In addition, simulation results show that different system parameters have influence on the capacity of the stealth channel, such as bit rate, transmission distance, optical bandwidth of the stealth user, and power spectral density of the ASE noise. At last, we introduce the additional layer security of the stealth channel based on the privacy and the confidentiality of the stealth channel. Simulation results show that the security of the stealth user can be guaranteed in the proposed system.

II. PRINCIPLE OF PROPOSED SCHEME

A. MODEL OF THE MULTI-USER OPTICAL STEGANOGRAPHY TRANSMISSION SYSTEM

To our knowledge, the previous researches have pay attention to investigating whether the eavesdropper can find the existence of the stealth signal in the time and frequency domain when the public signal and stealth signal are combined. The interaction between public channel and stealth channel is studied by using different modulations and optical sources. No attention is paid to the capacity of the stealth channel.

The current model of optical steganography transmission system is to use the entire ASE spectrum to carry the stealth channel. Actually, optical steganography based on ASE noise

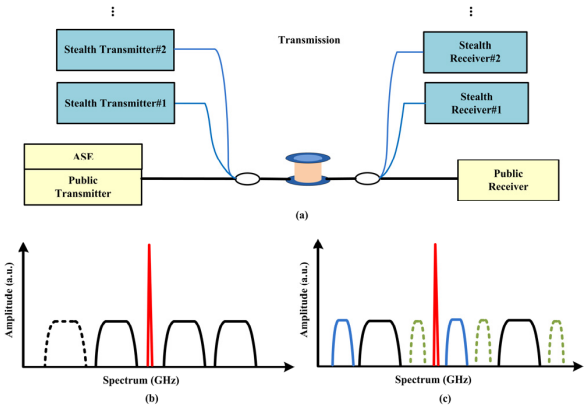


FIGURE 1. (a) The scheme of multi-user optical steganography transmission system; (b) and (c) the spectra of optical steganography system with multiple stealth users.

effectively hides the stealth signal in the public channel. However, the capacity of the stealth channel is limited, since the data rate is limited by the random phase of ASE light source.

In order to increase the stealth user and stealth capacity, the scheme of multi-user optical steganography transmission system is first proposed, which is shown in Fig. 1(a). After transmitting a span of fiber, the public channel of error-free transmission is realized. It is worth mentioning that an ASE noise is added into the public transmitter in this scheme, which aims to hide the stealth channel in frequency domain through increasing the noise level of the public channel. Multi-user stealth signals are injected into the public channel in the transmitter, and the signal of every stealth user is carried by part of ASE noise generated from EDFA. Note that the spectrum of the additional ASE noise is dependent on the spectrum of the stealth channel. In the proposed system, the spectrum of the additional ASE noise is complementary to the carrier of stealth channel. In the receiver, the received stealth signal is accepted through the optical band-pass filter according to spectral characteristics. And the signal processing and detection is realized in the stealth receiver.

The spectra of multiple stealth users can be presented in different forms in this multi-user optical steganography transmission system. The carrier of the stealth user can be a part of the ASE noise, which is shown in Fig. 1(b). Meanwhile, it also can be a combination of two parts of the ASE noise, as shown by the blue line in Fig. 1(c). As shown by the green line in Fig. 1 (c), three or four parts of ASE noise may also be used as stealth carriers. The spectrum width of stealth user is identical in order to achieve maximum number of users. Note that the spectra of stealth users are independent with each other and evenly distributed in the noise of the public channel.

B. SNR OF THE PUBLIC CHANNEL AND THE STEALTH CHANNEL

SNR is an important factor to measure the reliability of communication system. The communication quality can be

improved when SNR element is modified. In the multi-user optical steganography transmission system, a filtered ASE noise is adopted as the carrier of the stealth channel. The power spectral density and the optical bandwidth of each stealth user can affect the transmission performance of the stealth channel. The SNR formulas of the public channel and the stealth channel are derived in this situation, and the influencing factors to both channels are analyzed.

Based on the proposed transmission system model, the SNR of the public channel and stealth channel is given by

$$SNR_{pub} = \frac{\langle I_{pub}\rangle^2}{\sigma^2_{thermal} + \sigma^2_{shot} + \sigma^2_{ASE-ASE} + \sigma^2_{I_{pub}-ASE}} \quad (1)$$

$$SNR_{stealth} = \frac{\langle I_{stealth}\rangle^2}{\sigma^2_{thermal} + \sigma^2_{shot} + \sigma^2_{ASE-ASE}} \quad (2)$$

where $\langle I_{pub}\rangle$ and $\langle I_{stealth}\rangle$ are the average current of public and stealth receiver, $\sigma^2_{thermal}$ is the thermal noise, σ^2_{shot} is the shot noise, $\sigma^2_{ASE-ASE}$ is the beat noise among ASE noise, and $\sigma^2_{I_{pub}-ASE}$ is the beat noise between the public signal and ASE noise. Note that the public channel will not beat with the stealth channel in the stealth channel, because the public channel is filtered at the stealth receiver. And the beat noise only comes from the ASE beating with itself.

The thermal, shot and beat noise can be expressed as [16], [17],

$$\begin{aligned} \sigma^2_{thermal} &= \left(4k_BT/R_L\right)F_nB_e \\ \sigma^2_{shot} &= 2qR\left(2S_{ASE}B_{opt}\right)B_e \\ \sigma^2_{ASE-ASE} &= R^2S^2_{ASE}\left(2B_{opt} - B_e\right)B_e \\ \sigma^2_{I_{pub}-ASE} &= 4R^2S_{ASE}P_{pub}B_e \end{aligned} \quad (3)$$

where k_B is the boltzmann constant, T is the room temperature, R_L is the load resistance of the photodiode, F_n is the amplification ratio of the electric amplifier at the receiver, B_e is the electric bandwidth of the photodiode, q is the electron charge, R is the responsivity of the photodiode, S_{ASE} is the power spectral density of ASE noise, B_{opt} is the optical bandwidth of the filtered ASE noise, and P_{pub} is the power of public channel. It should be emphasized that the power spectral density of the ASE noise added to the public transmitter is equal to that of the ASE carrier of the stealth channel.

The difference between the signal received by the stealth channel and the signal received by the public channel is the signal power term. Due to the signal of the stealth channel is carried by ASE noise, the electrical signal power of stealth channel is proportional to the square of the ASE noise spectral density

$$\langle I_{stealth}\rangle^2 = 2\left(RS_{ASE}B_{opt}\right)^2 \quad (4)$$

$$\langle I_{pub}\rangle^2 = \left(RP_{pub}\right)^2 \quad (5)$$

In this multi-user optical steganography transmission system, the SNR of the stealth channel is affected by the thermal noise, shot noise and beat noise. In order to ensure error-free transmission of the stealth channel, the spectral density of ASE noise is increased to a certain value, and the beat noise dominates in this situation.

The SNR of the public channel Eq. (6) can be got through the Eq. (1), (3) and (5). The denominator comprises the thermal noise, shot noise, beat noise among ASE noise and beat noise between the public signal and ASE noise, which is shown in Eq. (6), when the numerator is set as the optical power of the public channel P_{pub}. Since the power of the public signal is far larger than that of the stealth signal, the dominate noise of the public channel becomes the beat noise between the public signal and ASE noise.

$$SNR_{pub} = \frac{P_{pub}}{\frac{4k_BTF_nB_e}{R_LR^2P_{pub}} + \frac{4qS_{ASE}B_{opt}B_e}{RP_{pub}} + \frac{S^2_{ASE}(2B_{opt}-B_e)B_e}{P_{pub}} + 4S_{ASE}B_e} \quad (6)$$

Based on the above analysis, when the beat noise dominates, the denominator of (6) can be simplified as:

$$SNR_{pub} = \frac{P_{pub}}{4S_{ASE}B_e} \quad (7)$$

It can be seen from (7) that the SNR of public channel is proportional to the power of the public channel, and inversely proportional to the spectral density of the ASE noise, in the case that the electrical bandwidth of receiver is constant. We can find that SNR of the public channel is only affected by the ASE noise spectral density when the power of public channel is fixed.

The ASE carrier of the stealth channel is large enough to realize the error-free transmission for the stealth channel in the multi-user optical steganography transmission system. The beat noise dominates in this situation:

$$SNR_{stealth} = \frac{B_{opt}}{B_e\left(\frac{(4k_BT/R_L)F_n}{2(RS_{ASE})^2B_{opt}} + \frac{2q}{RS_{ASE}} + 1\right)} \quad (8)$$

$$SNR_{stealth} = \frac{B_{opt}}{B_e} \quad (9)$$

We can see that the dominate position of beat noise is guaranteed in the stealth channel of multi-user transmission system. As a conclusion of the theory, when the electric bandwidth of receiver is fixed, the SNR of the stealth channel saturates at a constant only related to optical bandwidth of ASE light source.

III. RESULTS AND ANALYSES

Based on the multi-user optical steganography transmission system model, the transmission performance of the public channel and the stealth channel is analyzed. A public OOK transmission link is established and the stealth signal is added into the system. The schematic diagram of simulation is displayed in Fig. 2. The Mach-Zehnder modulator (MZM) is used to modulate a distributed feedback laser (DFB) beam

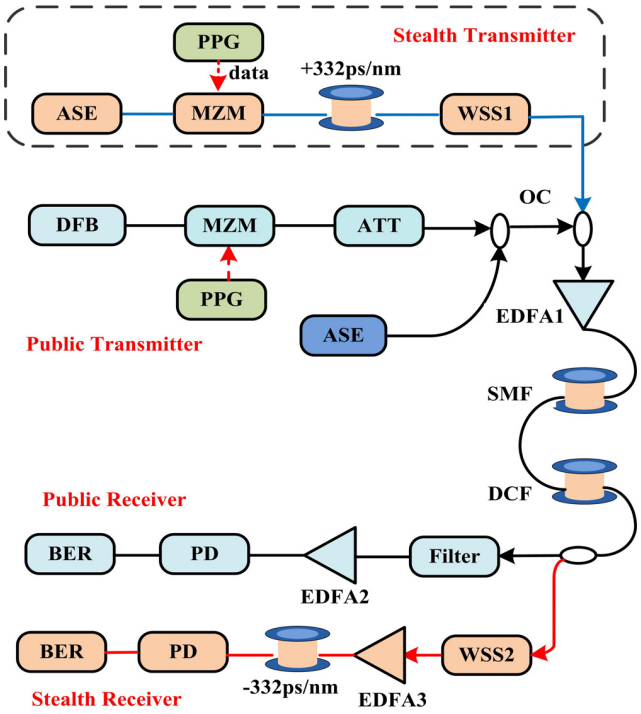


FIGURE 2. Schematic diagram of optical stealth transmission system, PPG, pulse pattern generator; ASE, amplified spontaneous emission noise; MZM, Mach-Zehnder modulator; WSS, wavelength selective switch; DFB, distributed feedback laser; ATT, attenuator; OC, optical coupler; EDFA, Erbium-doped fiber amplifier; SMF, single-mode fiber; DCF, dispersion compensation fiber; PD, photonic detector.

with a 2^{31}-1 pseudorandom binary sequence (PRBS), to generate the public OOK signal. The center wavelength of the laser is at 1550.2 nm.

The ASE noise generated by Erbium-doped fiber amplifier (EDFA) is used as the carrier of the stealth channel. With the optical source modulated by the electronic stealth data, the generated optical pulse is stretched passes through a span of fiber with 332 ps/nm chromatic dispersion [18]. A piece of modulated ASE noise is filtered by the wavelength selective switch1 (WSS1), which can be regarded as the stealth spectrum for the stealth user. Then the stealth channel is injected into the public channel through optical coupler. An additional ASE noise is attached to the public transmitter to simulate the system noise from real optical networks. Moreover, it can improve the noise level of public channel and reduce SNR of the public signal. The stealth signal can be hidden under the noise of the public channel.

As shown in Fig. 3, the stealth signal can be hidden in the noise of the public channel in the frequency and time domain based on the added ASE noise in the public transmitter and the dispersion device in the stealth transmitter. Fig. 3(a) shows the spectrum of the public channel only. There is no influence on the spectrum of the public channel except the noise level when the stealth channel is injected, as shown in Fig. 3(b). We can find that the noise level of the public channel is improved 10 dB after introducing the stealth channel. At the same time, Fig. 3(c) and 3(d) show the

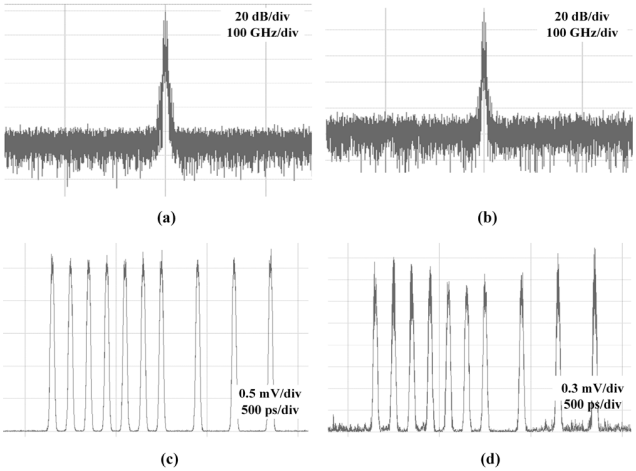


FIGURE 3. Spectrum of the public channel, (a) without and (b) with stealth channel; waveform of the public channel, (c) without and (d) with stealth channel.

waveforms of the public channel without and with the stealth channel, respectively. No obviously difference can be noticed by comparing Fig. 3(c) with 3(d), which means the stealth signal can be hidden well under the public channel in time domain.

After transmitting 100 km single mode fiber (SMF) and matched dispersion compensation fiber (DCF), the mixed signal is detected in the receiver. The public signal can be detected after filtering the received signal. Meanwhile, the spectrum of the stealth channel can be filtered by WSS2, which has the same wavelength range as WSS1. After amplification and dispersion compensation, the post-processing signal is detected, and the BER curves of the transmission system can be measured.

A. TRANSMISSION PERFORMANCE OF THE MULTI-USER OPTICAL STEGANOGRAPHY SYSTEM

In the following part, the interaction between the public channel and stealth channel is investigated based on the system parameters, e.g., the bit rate, the transmission distance, the optical bandwidth of the stealth user, and the power spectral density of the ASE noise. The initial values of the transmission distance, the optical bandwidth, and the power spectral density are 100 km, 200 GHz, and 5×10^{-16} W/Hz, respectively. The parameters in the simulation are shown in the Table 1.

The bit rate of transmission system is an important factor which can influence the performance of the system. In order to evaluate the interaction between the stealth channel and the public channel, the BER curves with different data rate are analyzed in this part.

As we all know, the bit rate of the public channel and the stealth channel are 2.5 Gb/s or 10 Gb/s in the previous experiment. As a result, there are three combinations between the bit rate of the public channel and that of the stealth channel, which can be written as (2.5 Gb/s, 2.5 Gb/s), (10 Gb/s, 2.5 Gb/s) and (10 Gb/s, 10 Gb/s), respectively. If the bit rate of

TABLE 1. Reference value and optimum value of system parameters.

Parameters	Reference value	Optimum value
Bit rate of the stealth channel	2.5 / 10 Gb/s	2.5 Gb/s
Bit rate of the public channel	2.5 / 10 Gb/s	2.5 Gb/s
Transmission distance	50 / 100 / 150 km	50 km
Optical bandwidth of the stealth user	200 / 100 / 80 / 50 GHz	80 GHz
Power spectral density	5×10^{-16} / 2×10^{-15} / 5×10^{-15} / 1×10^{-14} / 2×10^{-14} W/Hz	5×10^{-16} W/Hz

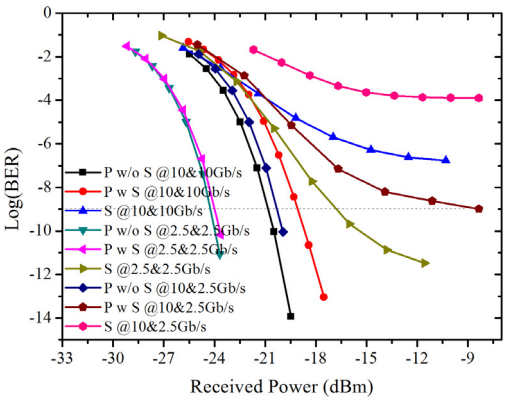


FIGURE 4. Simulated BER curves with different bit rate of the public channel and the stealth channel. P, public channel; S, stealth channel; w, with; w/o, without.

the stealth channel is higher than that of the public channel, multiple stealth pulses will appear in the bit interval of the public channel, which means that the stealth signal will be found. We can conclude that the bit rate of the stealth channel must be no bigger than that of the public channel.

When the bit rate of the public channel and the stealth channel are both 2.5 Gb/s or 10 Gb/s simultaneously, the simulated BER curves are shown in Fig. 4. The BER curves of the public channel with and without the stealth channel at 2.5 Gb/s are indistinguishable. However, there is a 1.5 dB power penalty when the bit rate of the public channel and the stealth channel are 10 Gb/s. This is because the same SNR has a different influence on the transmission system with different bit rate.

For the stealth channel, the simulation results show that the stealth channel hidden under the public channel can achieve the error-free transmission when the data rate is 2.5 Gb/s. In contrast, the BER of the stealth channel can only reach 10^{-7} when the bit rate is 10 Gb/s. We can conclude that the performance of the transmission system deteriorates with the data rate increases.

Fig. 4 also shows the simulated BER curves of the optical stealth transmission system, when the bit rate of the public channel and the stealth channel are 10 Gb/s and 2.5 Gb/s, respectively. The BER of the public channel with the stealth channel can be reached to 10^{-9}, and 12 dB power penalty

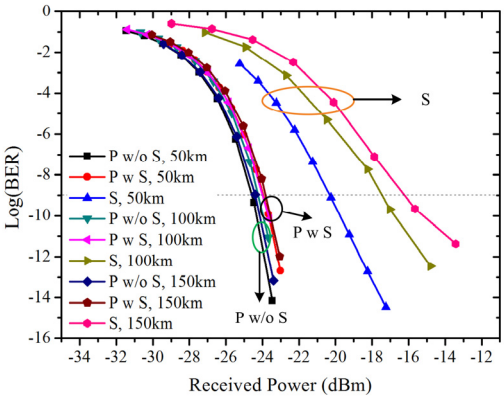


FIGURE 5. Simulated BER curves with different transmission distance. P, public channel; S, stealth channel; w, with; w/o, without.

is introduced by comparing the BER curves of the public channel without and with the stealth channel. At the same time, the public channel has an important effect on the stealth channel, and the BER of the stealth channel can only reach 10^{-4}. It can be found that the BER of the stealth channel gets worse when the bit rate of the stealth carrier increases.

Comparing the simulated BER curves of the stealth channel and the public channel with different data rate, the best combined transmission performance is selected. When the bit rate of the stealth channel and the public channel are both 2.5 Gb/s, simultaneously, the optical steganography system can be reached to optimal.

To further analyze the effect of the stealth channel to the public channels, the simulated BER curves with different transmission distance are shown in Fig. 5. We can find that there is no obviously difference between the BER curves of public channel without and with the stealth channel, when the transmission length is 50 km, 100km, and 150km, respectively. However, the transmission distance is an important factor for the performance of the stealth channel. The receiver sensitivity of the stealth channel with 50 km transmission is -20.5 dBm. It can be clearly seen from Fig. 5 that the power penalty becomes larger with the increase of transmission distance. This is because the number of the EDFA rises with the increase of transmission distance, the additional ASE noise generated by EDFA also increases in this situation.

As a result, the transmission distance has an effect on the stealth channel hidden under the public channel. The BER performance of the stealth channel will be better when the transmission distance is short. We will select the 50 km SMF transmission in the next simulation.

As mentioned above, the carrier of every stealth user is a part of ASE noise in the multi-user optical steganography transmission system. Subsequently, this section analyzes the impact of the optical spectral bandwidth of the stealth user on transmission performance.

In the simulation, the power spectral density of the ASE noise added in the public transmitter and the ASE carrier of the stealth user are equal and constant in the multi-user optical steganography system. The power contrast ratio between the

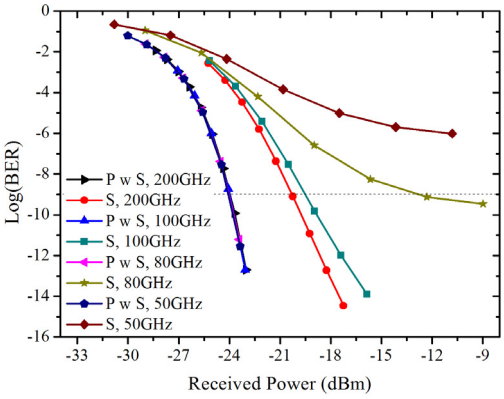


FIGURE 6. Simulated BER curves with different optical bandwidth of single stealth user. P, public channel; S, stealth channel; w, with; w/o, without.

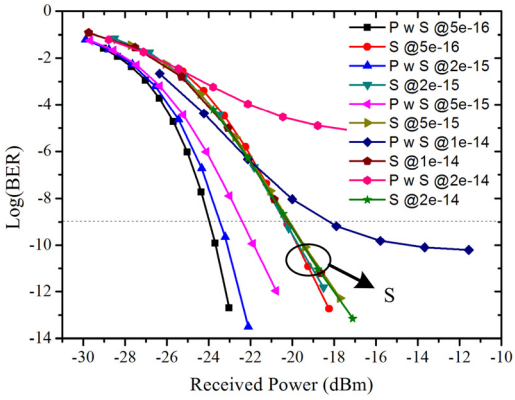


FIGURE 7. Simulated BER curves with different power spectral density of the ASE noise. P, public channel; S, stealth channel; w, with; w/o, without.

public channel and the stealth channel does not change when the optical bandwidth of a stealth user changes. Fig. 6 shows the simulated BER curves with different optical bandwidth of single stealth user. The BER curves of the public channel with the stealth channel are substantially unchanged no matter how the optical bandwidth of the stealth channel changed. However, the transmission performance of the stealth channel is seriously affected by the optical bandwidth of the stealth user.

It can be seen from Fig. 6 that the stealth channel achieves error-free transmission with a receiver sensitivity of -19 dBm, when the optical bandwidth of the single stealth user is 200 GHz. As the optical bandwidth reduces, the transmission performance of the stealth channel deteriorates. The BER of the stealth user is just reached to 10^{-9} under the condition that the optical bandwidth of the stealth user reduces to 80 GHz. The BER performance of the stealth channel gets worse with the further reduction of optical bandwidth. In summary, the simulation results show that the transmission performance of the stealth channel is proportional to its optical bandwidth, which is the same as (9). And the simulation results show that the minimum bandwidth of stealth channel is 80 GHz, which can realize the error-free transmission for the stealth channel.

The influence of the power spectral density of the ASE noise on the transmission performance of the public channel and the stealth channel is also analyzed based on the simulation platform.

Since the carrier of the stealth channel is one part of the ASE noise of the public channel, the SNR of the public channel is changed with power spectrum density of the ASE noise, and the power contrast ratio between the public channel and the stealth channel is also changed. The transmission performance of the stealth channel and the public channel is simulated under the condition that the optical bandwidth of the stealth user is 200GHz, and the simulated BER curves are displayed in Fig. 7. The power spectral density of the ASE noise can be set as 5×10^{-16} W/Hz, 2×10^{-15} W/Hz, 5×10^{-15} W/Hz, 1×10^{-14} W/Hz and 2×10^{-14} W/Hz, respectively.

It can be seen that the change of power spectral density has no effect on the BER curve of the stealth channel. In contrast, the power spectral density of the ASE noise has a great effect on the transmission performance of the public channel. The BER performance of the public channel deteriorates with the power spectral density increases. When the power spectral density arises to 1×10^{-14} W/Hz, error-free transmission for public channel is just achieved. And the public channel cannot be transmitted when the power spectral density of ASE noise is no less than 2×10^{-14} W/Hz. Therefore, through the comparative analysis of the simulation results, we find that the BER performance of public channel gets worse when the power spectral density increases, which is consistent with (6).

It should be emphasized that the limit value of the power spectral density of ASE noise cannot be used in the experiment, when analyzing the influence of the power spectral density in the multi-user optical steganography transmission system. In this case, if other noise is added, the transmission performance of the public channel cannot be guaranteed. As a result, the power spectral density of the ASE noise needs to be low to ensure the SNR of the public channel. So, the power spectral density of the ASE noise is set to be 5×10^{-16} W/Hz in the simulation.

In conclusion, the minimum bandwidth satisfying error-free transmission of every stealth user in the simulation is 80 GHz when the bit rate of the stealth channel is 2.5 Gb/s. The ASE spectrum of the stealth channel can range from 1520 nm to 1560 nm. Consequently, the multi-user optical steganography transmission system can accommodate 62 stealth users at the same time with error-free transmission. And the capacity is improved obviously.

Under the same simulation condition, the simulated BER curves versus the stealth user with different bit rates of the stealth channel are shown in Fig. 8, when the 10 Gb/s public channel is adopted. We can find that the number of the stealth user for error-free transmission is influenced by the bit rate of the stealth channel. This is because the higher bit rate of the transmit signal is, the higher requirement of SNR is. The transmission performance of 2.5 Gb/s stealth channel is better than that of 5 Gb/s stealth channel under the same simulation

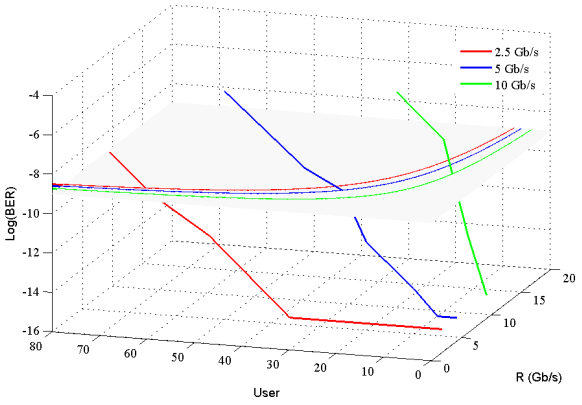


FIGURE 8. Simulated BER curves versus stealth user with different bit rates of the stealth channel when the public channel is 10Gb/s.

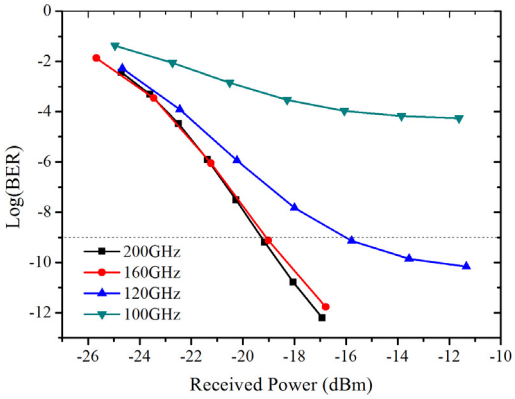


FIGURE 9. Simulated BER curves with different total optical bandwidth of the stealth user with two non-adjacent ASE source.

parameters (SNR). Then the minimum bandwidth for every stealth user to achieve error-free transmission and the number of the supported user are different when the bit rate of the stealth channel changes. As shown in Fig. 8, when the bit rate of the stealth channel is 2.5 Gb/s, 5 Gb/s, and 10 Gb/s, respectively, the corresponding number of the stealth user can be up to 62, 25, and 9, respectively.

In order to compare the channel capacity of the stealth channel more clearly, equal channel capacity lines are adopted in three cases, which is shown as the curves in the gray plane of Fig. 8. The simulation results obviously show that the maximum capacity of the stealth channel is 155 Gb/s when the bit rate is 2.5 Gb/s. And the capacity of the stealth channel decreases with the bit rate increases.

When the ASE spectrum of a single stealth user is discontinuous, as shown the blue line in Fig.1(c), two non-adjacent ASE lights are used as their carrier. The transmission performance of the stealth channel based on the two non-adjacent ASE spectra with the same optical bandwidth in this part is analyzed. With the optical bandwidth of the stealth carrier increases, the BER curves of the stealth channel are shown in Fig. 9. We can realize that the BER performance of the stealth channel is improved with the two non-adjacent optical bandwidth increases. And the stealth channel realizes error-free transmission, when the total optical bandwidth of the two-adjacent ASE optical carriers reaches 120 GHz. In a word, the larger the optical bandwidth is, the better the transmission performance of the stealth channel becomes.

When two non-adjacent ASE source are adopted as the carrier of the stealth user, the minimum optical bandwidth needed to realize error-free transmission is larger than that of a single ASE source, as shown in Fig. 6 and Fig. 9. The influence of the public channel on the stealth channel is just one reason. Another reason is the phase induced intensity noise (PIIN), which is introduced in the case of the multiple parts incoherent light source. Because the carrier of the stealth channel is non-adjacent, the beat noise of the multiple parts of the ASE source is large enough to affect the transmission performance of the stealth user.

We can conclude that the simulation results show the stealth user can realize error-free transmission with the enough optical bandwidth in the multi-user optical steganography transmission system, whether the ASE carrier of the stealth user is a continuum spectrum or divided into multiple parts.

B. SECURITY OF THE MULTI-USER OPTICAL STEGANOGRAPHY SYSTEM

The simulation results prove that the capacity of the stealth channel is improved in the multi-user optical steganography transmission system. However, for the optical steganography system, the security issue is still the problem. The stealth spectral-phase-encoded (SPE) OCDMA signal is transmitted through a public DPSK channel has been demonstrated [19]. The proposed steganography system is suits for the optical wireless communication, the secret data are extracted using correlation detection and balanced subtraction in the OCDMA decoder of the intended receiver [20]. The polarization-modulated-code-shift-keying modulation format, which is implemented with two super-structured fiber Bragg gratings OCDMA encoders, is proposed to enhance security of the optical steganography system [21].

The eavesdropper cannot find the existence of the stealth channel, when it is hidden under the public channel in the time and frequency domain. For intensity modulation multi-user optical steganography system, the eavesdropper may perform a blind attack on the system and guess which part of the spectrum between 1520 nm and 1560 nm carries the stealth channel. There will be two different situations. One is that the guessed spectrum is only a part of the spectrum of the stealth channel, the other is that the guessed spectrum is overlapped with the spectrum of the stealth channel. The two cases will be analyzed as follows, respectively.

In the proposed multi-user optical steganography transmission system, a single stealth user can realize the error-free transmission when the optical bandwidth of the continuum modulated ASE carrier is larger than 80 GHz. The ASE spectrum used by the stealth user can be randomly distributed between 1520 nm and 1560 nm, and its bandwidth can be

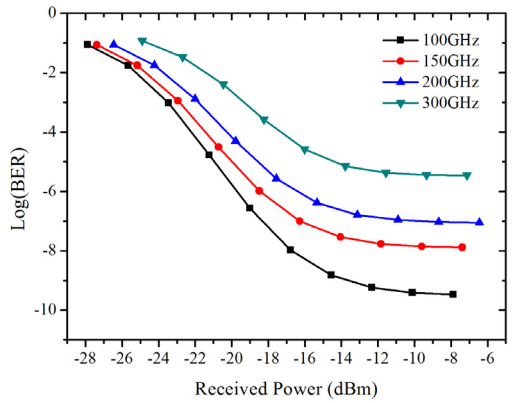


FIGURE 10. Simulated BER curves with different optical bandwidth in the eavesdropping receiver.

as small as 80 GHz. Since the stealth user can be hidden under the public channel in time and frequency domain, the eavesdropper needs to scan the optical spectrum little by little to find which part carries the stealth signal.

When a part of the ASE light source is used as the carrier of stealth channel, the optical bandwidth of the stealth user is 100 GHz. As shown in Fig. 6, when the spectrum of the stealth user is partially eavesdropped by the eavesdropper, i.e., the received bandwidth is less than the optical bandwidth of the stealth user, the BER performance of the eavesdropper is poor. When two non-adjacent ASE source is adopted as the carrier of the stealth user, the probability of the eavesdropper detecting part of the spectrum becomes smaller, and the error rate of the eavesdropper channel becomes worse, as shown in Figure 9.

For the second situation, the guessed spectrum is overlapped with the spectrum of the stealth user, which can be discussed in two cases. If the guessed spectrum is partially overlapped with the spectrum of the stealth channel, it also overlaps with the ASE noise. The BER performance of the eavesdropper is poor. And if the guessed spectrum overlapped with all spectrum of the stealth channel, the stealth signal may be detected depends on the optical bandwidth of the guessed spectrum.

In order to evaluate the security performance of the multi-user optical steganography transmission system, we realize the follow simulation. A part of ASE noise with an optical bandwidth of 100 GHz is used as the carrier of the stealth carrier in the transmitter. The eavesdropping signal is filtered by a WSS with different optical bandwidth, and the filtered optical signal includes not only the modulated ASE carrier of the stealth channel, but also the ASE noise as the interference source. Fig. 10 displays the corresponding BER curves with different optical bandwidth in the eavesdropping receiver.

When the filter with 100 GHz optical bandwidth is adopted in the eavesdropping receiver, the filtered optical spectrum only contains the modulated ASE carrier of the stealth channel, and the eavesdropping channel realizes the error-free transmission. The interference ASE noise is introduced with the optical bandwidth of the eavesdropping receiver increases, and the BER performance is decreased corresponding. In a summary, the bigger the optical bandwidth is, the worse the BER performance becomes. When the introduced ASE noise increases to a certain value, the eavesdropping receiver will not detect any useful information.

When the modulated ASE carrier of the stealth user is composed by two non-adjacent spectra, the optical bandwidth of the non-adjacent spectra is 120 GHz. The spectral position and bandwidth of the stealth carrier is numerous and uncertain. It is impossible for the eavesdropper to search each part of the spectrum exactly. When the eavesdropper scans the ASE spectrum little by little, the introduced ASE noise, which locates between two modulated ASE carriers, prevents any useful signal from being detected, i.e., the blind attack of the eavesdropper is useless in this situation. When multi-part non-adjacent spectra are adopted as the carrier of the stealth user, the spectral position and bandwidth are undetermined. The security performance of the stealth channel can be improved.

As a conclusion, when the ASE carrier of the stealth user is composed by multiple non-adjacent spectra, the spectra position and bandwidth of the stealth carrier is impossible to definite for the eavesdropper. The security issue that detected by the eavesdropper can be solved in the proposed multi-user optical steganography transmission system.

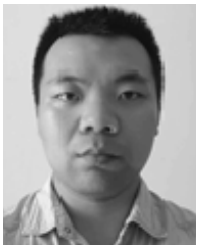
IV. CONCLUSION

In order to improve the user and the capacity of the optical stealth channel, we firstly propose a multi-user optical steganography transmission system based on filtered ASE noise. The SNR of the public channel and the stealth channel is studied based on the model of the proposed system. When the noise in the optical steganography system is dominated by the beat noise, we conclude that the power spectral density of the ASE noise and the optical bandwidth of the ASE noise have an impact on SNR of public channel and stealth channel, respectively. And the influence of the system parameters on the public and stealth channel is analyzed. The simulation results show that the minimum bandwidth of stealth channel is 80 GHz, which can realize the error-free transmission for the stealth channel and the public channel. As a result, the maximum user of the stealth channel is 62, and the capacity of the stealth channel can be improved to 155 Gb/s.

Security analysis of the multi-user optical steganography system is also discussed. We introduce the additional layer security of the stealth channel based on the filtered ASE noise. The eavesdropper must find 0.6 nm spectrum carried the stealth signal in a 40 nm range to find the existence of the stealth channel, when a span of ASE noise is used as stealth carrier. In addition, there is no hope for the eavesdropper to detect the stealth signal when the ASE spectrum of a single stealth user is a combination of multiple non-adjacent modulated ASE noise. We can conclude that the security of the stealth user can be guaranteed in the proposed system.

REFERENCES

[1] M. C. Soriano, P. Colet, and C. R. Mirasso, "Security implications of open- and closed-loop receivers in all-optical chaos-based communications," *IEEE Photon. Technol. Lett.*, vol. 21, no. 7, pp. 426–428, Apr. 1, 2009.
[2] Ü. Çavuşoğlu, A. Akgül, S. Kaçar, İ. Pehlĭvan, and A. Zengin, "A novel chaos-based encryption algorithm over TCP data packet for secure communication," *Secur. Commun. Netw.*, vol. 9, no. 11, pp. 1285–1296, Jan. 2016.
[3] D. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
[4] L. L. Yi, T. Zhang, Z. X. Li, Y. Zhang, Y. Dong, and W. S. Hu, "Power-penalty-free all-optical decryption using stimulated Brillouin scattering in optical fiber," *Laser Phys. Lett.*, vol. 10, no. 4, p. 045102, 2013.
[5] B. Wu, M. P. Fok, B. J. Shastri, Z. Wang, and P. R. Prucnal, "Analog noise protected optical encryption with two-dimensional key space," *Opt. Express*, vol. 22, no. 12, pp. 14568–14574, Jun. 2014.
[6] 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*, vol. 21, no. 2, pp. 2065–2071, Jan. 2013.
[7] Z. Huatao, R. Wang, T. Pu, Y. Chen, T. Fang, J. Zheng, and G. Su, "Complementary coding optical stealth transmission based on amplified spontaneous emission light source," *Opt. Express*, vol. 22, no. 23, pp. 28346–28352, Nov. 2014.
[8] B. Wu, A. N. Tait, M. P. Chang, and P. R. Prucnal, "WDM optical steganography based on amplified spontaneous emission noise," *Opt. Lett.*, vol. 39, no. 20, pp. 5925–5928, Oct. 2014.
[9] B. B. Wu and E. E. Narimanov, "Analysis of stealth communications over a public fiber-optical network," *Opt. Express*, vol. 15, no. 2, pp. 289–301, Jan. 2007.
[10] M. P. Fok and P. R. Prucnal, "Compact and low-latency scheme for optical steganography using chirped fibre Bragg gratings," *Electron. Lett.*, vol. 45, no. 3, pp. 179–180, Jan. 2009.
[11] H. Xuezhi, W. Dawei, X. Lei, and H. Sailing, "Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering," *Opt. Express*, vol. 18, no. 12, pp. 12415–12420, Jun. 2010.
[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*, vol. 18, no. 6, pp. 6079–6088, Mar. 2010.
[13] Z. Huatao, R. Wang, T. Pu, T. Fang, P. Xiang, J. Zheng, and D. Chen, "Optical stealth transmission based on super-continuum generation in highly nonlinear fiber over WDM network," *Opt. Lett.*, vol. 40, no. 11, pp. 2561–2563, Jun. 2015.
[14] B. Wu, B. J. Shastri, P. Mittal, A. N. Tait, and P. R. Prucnal, "Optical signal processing and stealth transmission for privacy," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1185–1194, Oct. 2015.
[15] P. R. Prucnal, M. P. Fok, K. Kravtsov, and Z. Wang, "Optical steganography for data hiding in optical networks," in *Proc. Int. Conf. Digit. Signal Process.*, 2009, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/5201086/
[16] B. Wu, B. J. Shastri, and P. R. Prucnal, "System performance measurement and analysis of optical steganography based on noise," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1920–1923, Oct. 1, 2014.
[17] R. C. Steele, G. R. Walker, and N. G. Walker, "Sensitivity of optically preamplified receivers with optical filtering," *IEEE Photon. Technol. Lett.*, vol. 3, no. 6, pp. 545–547, Jun. 1991.
[18] Z. Huatao, R. Wang, T. Pu, T. Fang, P. Xiang, J. Zheng, Y. Tang, and D. Chen, "Experimental demonstration of optical stealth transmission over wavelength-division multiplexing network," *Appl. Opt.*, vol. 55, no. 23, pp. 6394–6398, Aug. 2016.
[19] Z. Fei, P. Tao, W. Zhihu, F. Tao, C. Yinfang, Z. Jilin, and S. Dan, "Optical steganographic transmission of spectral-phase-encoded OCDMA signal over a public DPSK channel," in *Proc. 22nd Wireless Opt. Commun. Conf.*, 2013, pp. 552–554.
[20] C. Yen, J.-F. Huang, and W.-Z. Zhang, "Hiding stealth optical CDMA signals in public BPSK channels for optical wireless communication," *Appl. Sci.*, vol. 8, no. 10, p. 1731, 2018.
[21] C. Yanfang, R. Wang, T. Fang, T. Pu, P. Xiang, H. Zhu, and J. Zheng, "Stealth transmission of temporal phase en/decoded polarization-modulated-code-shift-keying optical-code-division multiple-access signal over synchronous digital hierarchy network with asynchronous detection," *Opt. Eng.*, vol. 53, no. 6, p. 066103, 2014.



GUORUI SU received the B.S. degree in communication engineering from the School of Information and Communication Engineering, Shandong University, Jinan, China, in 2013, and the M.S. degree in optical communication technology from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2016. He is currently pursuing the Ph.D. degree in optical communication technology with the College of Communications Engineering, Army Engineering University of PLA.

His current research interests include fiber-optic communication technology, optical code division multiple access systems, and coherent optical communication.

TAO PU received the B.S. degree in communication engineering and the M.S. and Ph.D. degrees in communications engineering and information systems from the PLA College of Communications Engineering, Nanjing, China, in 1996, 1999, and 2003, respectively. He is currently a Full Professor with the College of Communications Engineering, Army Engineering University of PLA.

His current research interests include optical communication technology, microwave photonics, signal processing, anti-interception communication, and fiber-optic sensing technology.

JILIN ZHENG received the B.S. and Ph.D. degrees in fiber-optic communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2005 and 2010, respectively. He is currently a Full Associate Professor with the College of Communications Engineering, Army Engineering University of PLA.

His current research interests include optical communication technology, microwave photonics, signal processing, and integrated laser.

YETENG TAN received the B.S. degree in physics from the School of Physics and Astronomy, Shanghai Jiao Tong University, Shanghai, China, in 2014, and the M.S. degree in optical communication technology from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2017. He is currently pursuing the Ph.D. degree in optical communication technology with the College of Communications Engineering, Army Engineering University of PLA.

His current research interests include fiber-optic communication technology, optical code division multiple access systems, quantum-noise randomized cipher system, and security estimation.