System Performance Measurement and Analysis of Optical Steganography Based on Noise

Ben Wu, Bhavin J. Shastri, *Member, IEEE,* and Paul R. Prucnal, *Fellow, IEEE*

Abstract [illegible]

Index Terms [illegible]

I. INTRODUCTION

PITCAL steganography provides an effective way to hide a stealth channel in both the time domain and frequency domain of the public network [1]–[3]. Recently, an optical steganography method based on amplified spontaneous emission (ASE) noise has been proposed and experimentally demonstrated [4]–[7]. The stealth signal is carried by the ASE noise that comes from erbium doped fiber amplifiers (EDFAs) in the public optical network. The optical spectrum of the stealth data channel is exactly the same as the spectrum of the noise in the public channel. In the time domain, the stealth channel takes advantage of the short coherence length of the ASE noise. Since the stealth transmitter uses phase modulation, the delay length at receiver has to be exactly matched the delay length at the transmitter in order to recover the phase information and demodulate the data [4]. The requirement of the matching condition provides a large key space for the stealth channel, which makes it virtually impossible for an eavesdropper to detect the existence of the stealth channel [4], [5].

While optical steganography based on ASE noise can effectively hide the stealth channel, the system performance of the shows the spectrum in point A of the system diagram and the spectrum on the right shows the spectrum in point B. The peak in the spectrum is the public channel and the flat region the ASE noise. An optical filter can be used to separate the ASE noise from the public channel. After adding the stealth signal by modulating the ASE noise [6], [7], the stealth channel can be combined with the public channel and transmit through the public network. At the receiver, an optical filter can be used to separate the stealth channel and public channel.

B. SNR of the Stealth Channel

The SNR of the stealth channel is given by

$$SNR_{stealth} = \frac{\langle I \rangle^2}{\sigma_{thermal}^2 + \sigma_{shot}^2 + \sigma_{ASE-ASE}^2} \tag{1}$$

where $<I>$ is the average of receiver current, $\sigma_{thermal}^2$ is the thermal noise, σ_{shot}^2 is the shot noise, and $\sigma_{ASE-ASE}^2$ is the beat noise.

The thermal, shot and beat noise can be expressed as [8], [9]

$$\begin{aligned} \sigma_{thermal}^2 &= (4k_B T/R_L)F_n \Delta f \\ \sigma_{shot}^2 &= 2qR(2S_{sp}\Delta \nu_{opt})\Delta f \\ \sigma_{sp-sp}^2 &= 4R^2 S_{sp}^2 \Delta \nu_{opt} \Delta f \end{aligned} \tag{2}$$

where

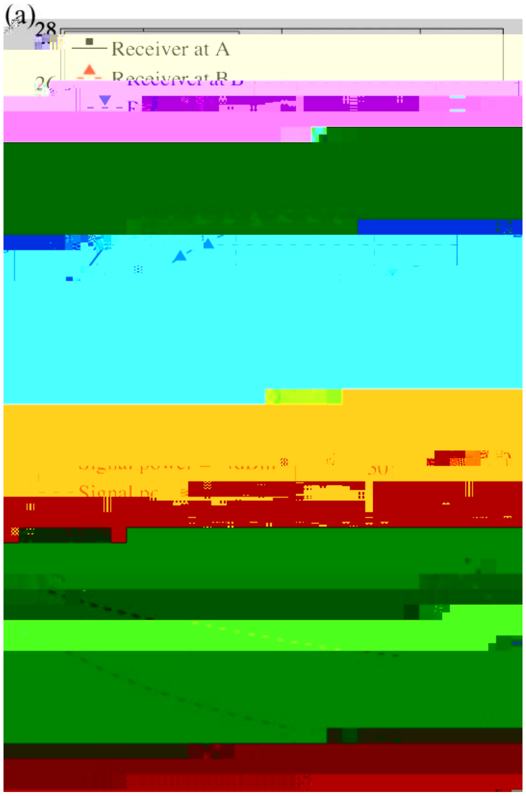

Fig. 5. (a) Dependence of SNR on the received power with different number of amplifiers. (b) Dependence of SNR on the transmission distance at different launch powers.

C. System Design and Analysis

The design of the stealth channel needs to find an optimum balance between the SNR and the required ASE power. Because the ASE power carrying stealth signal comes from the accumulation of noise from the public channel (Fig. 1), a lower ASE power level requires less noise in the public channel and thus provides more flexibility of applying the stealth channel in the public network. In the case of short distance communication without using amplifiers, the best operating point is when the SNR just saturates, which corresponds to -10dBm in Fig. 3(a). The SNR reaches a maximum value at -10dBm. The operating point depends on the amount of thermal noise of the receiver. In the case of long-haul transmission, where amplifiers are introduced, the initial ASE power needs to be increased further. Because the ratio of the initial ASE power and the newly generated ASE by the amplifier determines the degradation rate of SNR after the signal passes through other amplifiers, a larger initial power results in slower degradation of the SNR. The choice of