Optical Encryption Based on Cancellation of Analog Noise

Ben Wu, Matthew P. Chang, Zhenxing Wang, Bhavin J. Shastri, and Paul R. Prucnal
Lightwave Communications Laboratory, Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA
benwu@princeton.edu

Abstract: We propose an optical encryption technique where the data is encrypted with wideband analog noise. Matching both the phase and amplitude of the noise is required, providing a large key space for the encryption process.
OCIS codes: (060.2330) Fiber optics communications; (060.4785) Optical security and encryption.

1. Introduction

Optical encryption provides an effective way to secure data transmission without compromising the bandwidth [1,2]. Different optical encryption methods have been studied, including optical XOR logic encryption [3] and optical chaotic encryption [4]. Although optical XOR logic can reach 20Gb/s [3], the encrypted data is a digital signal. Compared with analog noise, the digital signal leaves the original data undamaged, and once the eavesdropper knows the code for the encryption, he can still recover the original data from the encrypted digital signal. Optical chaotic encryption encrypts the data with noise-like analog signals; however, it requires the laser at the transmitter and receiver to be synchronized to recover the data. The synchronization parameters cannot be directly used as key distribution for encryption process. A high speed encryption method with both analog noise signal carrier and easily tunable parameters for large key space is required.

Optical interference cancellation techniques have been widely studied to remove self-interference in wireless communication systems [5,6]. The most challenging problem of optical interference cancellation is to satisfy the matching condition between the interference path and the cancellation path. The challenging problem in optical interference cancellation can be used as an advantage for the optical encryption, because the precise requirement of the matching condition provides a large key space to the encryption process.

In this paper, we propose and experimentally demonstrate an optical encryption method based on interference cancellation. The digital signals are combined with stronger analog interference noise. The signal can only be recovered by matching the interference noise and the cancellation noise. Both the phase and amplitude of the noise can be controlled and used as key distribution parameters between the transmitter and the receiver.

2. Experimental setup and principle

The noise encryption process includes two channels (Fig. 1). Each channel is carried by a different wavelength, λ_1 and λ_2. Channel 1 consists of both a signal and interference noise, and channel 2 carried the cancellation noise. The interference noise has a wide bandwidth and an amplitude stronger than the signal to protect the signal from being detected. At the receiver, a WDM filter is used to separate the two channels. The receiver can only cancel the interference noise by matching the noise signal between channel 1 and 2. To satisfy the matching condition, both the phase and amplitude of the noise signals have to be matched and these parameters can be the key of the encryption process. The phase can be controlled by a pair of optical delay lines at the transmitter and receiver. The amplitude can be controlled by both the modulation depth of the intensity modulator and the optical attenuator (Fig. 1).

In our experiment, the data rate of the transmitted data is 12Gb/s. The bandwidth for both the interference noise and cancellation noise covers from 4.5GHz to 5.5GHz. We design the frequency of the interference noise to be less than half of the signal data rate. This is to avoid enabling the eavesdropper to use a low pass radio frequency (RF) filter to remove the noise. Furthermore, the eavesdropper cannot use a band pass RF filter to remove the noise, because the noise spectrum overlaps with the zeroth-order lobe of the signal spectrum. If the eavesdropper removes the noise in the RF spectrum range of 4.5-5.5GHz, he also removes the signal information.

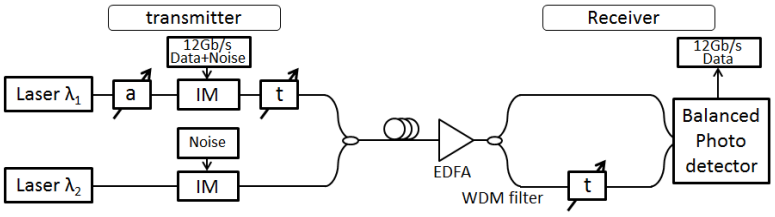

Fig. 1. Experimental setup (a: tunable optical attenuator; IM: intensity modulator; t: tunable optical delay; EDFA: erbium doped fiber amplifier; WDM: wavelength division multiplexer)

3. Experiment results and analysis

The RF spectrum response measurement shows that if the matching conditions are satisfied, the noise encryption system can cancel noise with bandwidth 1GHz at a central frequency of 5GHz by at least 25dB (Fig. 2). The noise cancelled spectrum is measured when signal is turn off and noise in the two channels satisfy the matching condition. The reference spectrum is the transmission spectrum of a single channel. Comparing the reference spectrum and noise cancelled spectrum, a minimum of 25dB cancellation is achieved in the 1GHz bandwidth.

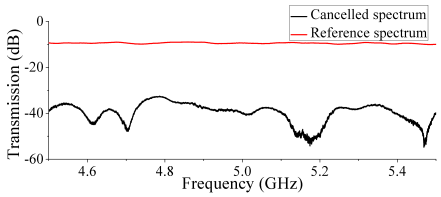

Fig. 2. Comparison of noise cancelled spectrum and reference spectrum

The eye diagram shows that a clear eye opening can only be obtained when the matching conditions are satisfied (Fig. 3(a)). If the optical delay length is not matched between the two channels, the noise in the channel 2 cannot cancel the interference noise in channel 1. The interference noise has a larger amplitude than the signal and leads to a signal-to-noise ratio of less than 1. The receiver can only receive completely noisy signals in this case (Fig. 3(b)). The bit error rate (BER) measurement shows that the BER reaches a minimum of 9×10^{-5} when the optical delay is matched. Forward error correction (FEC) with Reed-Solomon code can be used to reduce a BER of 9×10^{-5} to where it is error free. The matching range that can be corrected by FEC is only 4mm (Fig. 3(c)). The optical delay length difference between the two channels at the transmitter is designed to be in the order of 5m. Without information of optical delay, the eavesdropper needs to find the correct 4mm length in the range of 5m in order to decrypt the data. We design the system to be not error free by controlling the intensity of the RF noise, so after 25dB cancellation, there is still noise in the system (Fig. 3(a)). This design is intended to reduce the delay length range in which an observable eye diagram can be detected and increase difficulty for eavesdropper to find the right delay length.

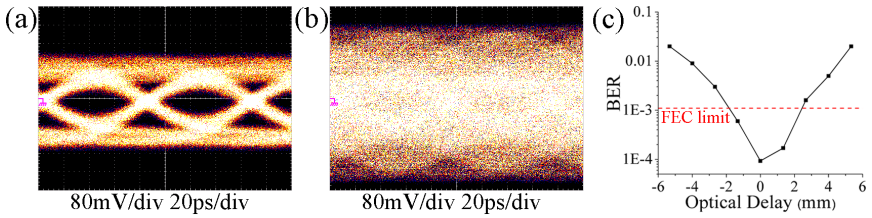

Fig. 3. (a) Eye diagram with the optical delay matched (b) Eye diagram with the optical delay unmatched (c) BER for optical delay changed from matched to unmatched (FEC: forward error correction)

4. Conclusion

We propose and experimentally demonstrate an optical encryption method based on analog noise. The signal in the encrypted channel is protected by the wideband noise with amplitude stronger then the signal. The interference noise can only be removed by matching both the phase and amplitude of the interference noise and the cancellation noise at the receiver. The precise requirement of matching conditions provides a large key space for the encryption. The cancellation process achieves 1GHz RF bandwidth and at least 25dB cancellation of the interference noise.

References

[1] M. P. Fok, et. al., "All-optical encryption based on interleaved waveband switching modulation for optical network security," Opt. Lett. 34 1315-1317 (2009).

[2] M. P. Fok, et. al., "Optical layer security in fiber-optic network," IEEE Trans. Inf. Forensics Security **6**, 725–736 (2011).

[3] A. Argyris, et. al., "Chaos-based communications at high bit rates using commercial fiber-optic links," Nature **438**, 343-346 (2006).

[4] K. Chan, et. al., "Demonstration of 20-Gb/s all-optical XOR gate by four-wave mixing in semiconductor optical amplifier with RZ-DPSK modulated inputs," IEEE Photon.Technol. Lett. **16**, 897–899 (2004).

[5] J. Suarez, et. al., "Instantaneous bandwidth of counter-phase optical interference cancellation for RF communications," IEEE Microw Wirel Co **21** 507-509 (2011).

[6] M. P. Chang, et. al., "Optical analog self-interference cancellation using electro-absorption modulators," IEEE Microw Wirel Co **23** 99-101 (2013).