High Speed Data Security Enabled by Stimulated Brillouin Scattering in Optical Fiber

Tao Zhang, Lilin Yi*, Zhengxuan Li, Yi Dong and Weisheng Hu
State Key Lab of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Department of Electronic Engineering, Shanghai 200240, China.
*E-mail: lilinyi@sjtu.edu.cn

Abstract: We propose to use SBS effect to enable high speed data security. A 10.86-Gb/s NRZ-OOK data is encrypted by a SBS loss and decrypted by a corresponding SBS gain with 1-dB power penalty.

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

1. Introduction
Physical-layer security which performs data encryption using optical approaches has attracted a lot of interest due to its inherent properties of high speed and difficulty in eavesdropping. Chaos communication [1-2] and optical code-division multiplexing (OCDM) [3-4] are two mainly physical-layer encryption methods. Chaos encryption needs to generate a chaotic carrier from the transmitter and synchronize the chaotic carrier at the receiver; while OCDM requires a pico-second pulse laser as the source. Therefore both the encryption methods require special transmitters and receivers. From the practical viewpoint, it is desired to directly encrypt/decrypt the signal based on the traditional transmitter and receiver using an encryption/decryption module, therefore compatible with the existing fiber-optic communication systems. We have proposed to use a 200-MHz wide Gaussian-shape stimulated Brillouin scattering (SBS) gain in optical fiber to encrypt a 10-Gb/s non-return-to-zero-on-off-keying (NRZ-OOK) data, and decrypt it using a corresponding SBS loss [5]. But the power penalty of the decrypted signal is as high as 5 dB due to the strong noise from the current-dithered Brillouin pump and its strong Rayleigh backscattering.

In this letter, we use continuous-wave (CW) Brillouin pumps to encrypt and decrypt a 10.86-Gb/s NRZ-OOK signal to solve the noise problem and achieved much better encryption and decryption results than in [5]. The carrier and low frequency components of the signal will be amplitude- and phase-distorted by a SBS gain/loss to implement encryption and then completely recovered by using a corresponding SBS loss/gain. After encryption, the eye diagram of the signal is totally distorted and the bit-error-rate (BER) cannot be measured. The power penalty of the decrypted signal is only 1 dB compared with the original signal without encryption/decryption.

2. Operation Principle

In the stimulated Brillouin scattering (SBS) process, the Brillouin pump with a frequency of \( v_0 \) generates a SBS gain/loss resonance at lower/higher frequency. The frequency difference between the Brillouin pump and the SBS gain/loss resonance is \( v_B \), called as Brillouin frequency shift. Based on Kramers-Kronig relationship, the spectral resonance induces phase index variation of the medium, corresponding to a phase variation. The process is shown as Fig. 1 (a). If two lasers with the frequency of \( v_0 - v_B \) and \( v_0 + v_B \) are used as Brillouin pumps, the SBS amplification and absorption will happen at the same frequency of \( v_0 \). By controlling the power of two Brillouin pumps, the SBS gain can completely compensate the SBS loss and the corresponding phase variation is also counterbalanced as shown in Fig. 1 (b). If a broadband OOK is amplified/absorbed by a SBS gain/loss, both the amplitude and phase of the carrier and the low-frequency components of the signal will be changed, resulting in a distorted eye diagram. The signal can be recovered by using a corresponding SBS loss/gain to compensate the amplitude and phase variation. The eye diagram distortion and recovery process can be treated as encryption and decryption process respectively. The simulated eye diagrams of the original signal, the SBS-loss encrypted signal and the SBS-gain decrypted signal are shown in Fig. 1 (c).
3. Experimental setup

We make an experiment to evaluate the performance of the proposed SBS encryption/decryption method. The experimental setup is shown as Fig. 2. A distributed feedback laser-diode (DFB-LD) operating at 1550 nm serves as both the Brillouin pump and signal source for easy pump and signal frequency matching. The power of the laser is boosted to 16 dBm by an erbium-doped fiber amplifier (EDFA1) then divided into two parts by a 3-dB coupler. In the lower path, the light is modulated by a Mach-Zehnder modulator (MZM1) with a 10.86-Gb/s pseudo-random bit sequence (PRBS) data with a word length of $2^{29}-1$ from a pulse pattern generator (PPG). The broadband signal is launched into a 25-km single-mode fiber (SMF) with a Brillouin frequency of 10.86 GHz through an optical isolator (ISO). In the upper path, the light is modulated by MZM2 at the Brillouin frequency of the SMF using the optical carrier-suppressing double sidebands technique. The modulated light is divided by a 3-dB coupler and two tunable filters (TFs) are employed to separate the left and right sidebands for serving as two Brillouin pumps. EDFA2 and EDFA3 are used to control the Brillouin pump powers. The amplified Brillouin pumps are combined by another 3-dB optical coupler and then sent into the SMF through an optical circulator (OC). Polarization controllers (PC) are used to control the polarization state of the light. The broadband signal is exported from port 3 of OC2. Turning off both EDFA2 and EDFA3, the original signal is observed. SBS amplification is achieved by turning on EDFA2. The signal is simultaneously amplified and absorbed by SBS gain and loss through turning on both EDFA2 and EDFA3. Insets (a) to (e) show the optical spectra at the corresponding points in Fig. 2. Insets (f) to (h) represent the optical spectra of the signal experiencing SBS loss, SBS gain and both SBS gain and loss respectively.

![Fig.2 The experimental setup and the measured optical spectra at the marked points.](image)

4. Experimental results

Fig. 3 shows the electrical spectra of the original 10.86-Gb/s NRZ signal, the distorted signal by a SBS loss and the recovered signal by a corresponding SBS gain. Fig. 3 (b) shows the change of the frequency power distribution caused by both the amplitude and phase variation of the signal carrier and low frequency components, manifesting as the distortion of the eye diagram in time domain. The electrical spectrum of the signal experiencing SBS gain is quite similar with Fig. 3 (b). By using a corresponding SBS gain/loss to compensate both the amplitude and phase variation, the frequency power distribution can be recovered to the original case but with some low frequency SBS noise as shown in Fig. 3 (c).

Fig. 4 and Fig. 5 show eye diagrams and BER measurements of the original signal, the encrypted and decrypted signal in different gain/loss amplitude cases. With a 6-dB SBS gain, even though the eye is distorted, the BER is still detectable therefore the encryption is not ideal. With a 9-dB SBS gain, the eye is severely distorted and the BER cannot be measured due to data out of synchronization, realizing a complete encryption. But the sensitivity of the corresponding decrypted signal becomes worse due to higher SBS amplification noise. For the SBS-loss encryption case, once the SBS loss is higher than 5 dB, the signal eye is totally distorted and the BER is undetectable therefore not shown in Fig 5. The eavesdropper cannot achieve any useful information by directly...
detecting the distorted signal as shown in Fig. 4(d1) and (e1). For the encryption with a higher SBS loss, the sensitivity of the decrypted signal also becomes worse due to higher noise. Note that the decryption performance using SBS-loss encryption is better than that of gain encryption case. This is because the signal always works at gain/loss saturation region for the gain encryption case resulting in higher amplification/absorption noise. As shown in (d1) and (d2), a 10-dB SBS loss can totally distort the signal and after a corresponding 10-dB SBS gain, the eyes are fully recovered with a power penalty of only 1 dB compared with the original signal, demonstrating a perfect encryption and decryption performance.

Fig. 4 The original, encrypted and decrypted eye diagrams of the 10.86-Gb/s OOK data.

Fig. 5 BER measurement results of the original, encrypted and decrypted signals.

To enhance the security level, one can vary the Brillouin pump power using a slowly-varied waveform (such as in ~ms level) therefore the eavesdroppers can only see the average effect. A synchronized slowly-varied waveform has to be used for decryption. Here the slowly-varied waveform can be called as an enhanced encryption key. The security will be significantly improved since the eavesdroppers cannot recognize the encryption key from both the frequency-domain and time-domain due to the average effect of the slow modulation, and only the legal users who know the encryption keys and the enhanced encryption key can decrypt the signal.

5. Summary

We have experimentally demonstrated the encryption and decryption performance of a 10.86-Gb/s NRZ-OOK data using SBS gain and loss as encryption keys respectively. For a 10-dB SBS loss encryption, the power penalty of the decrypted signal is only 1 dB compared with the original signal. The security level could be enhanced by varying the Brillouin pump power using a slowly-varied waveform and synchronization at the receiver is required for the decryption. The proposed SBS encryption/decryption proposal is completely compatible with the existing fiber-optic communication systems.

Acknowledgement: This work was supported by 973 Program (2012CB315602 and 2010CB328204-5), Nature Science Foundation China (61007041, 61090393, 61132004 and 60825103), 863 Program, Program of Shanghai Subject Chief Scientist (09XD1402200), Program of Shanghai Chen Guang Scholar (11CG11) and Program of Excellent PhD in China (201155).

6. References