Secure Free-Space Optical Communication via Amplified Spontaneous Emission (ASE)

Hanzi Huang[1,2], Jian Chen[1], Haoshuo Chen[2], Yetian Huang[1,2], Yingchun Li[1], Yingxiong Song[1], Nicolas K. Fontaine[2], Roland Ryf[2], and Min Wang[1]

[1] *Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai Institute for Advanced Communication and Data Science, Shanghai University, 200444 Shanghai, China*
[2] *Nokia Bell Labs, 791 Holmdel Rd., Holmdel, NJ 07733, USA*
chenjian@shu.edu.cn

Abstract: We propose a secure free-space optical (FSO) communication scheme employing the internal randomness of amplified spontaneous emission. 60-Gbit/s FSO transmission is demonstrated with temporal and spectral encryption.

OCIS codes: (060.2605) Free-space optical communication; (060.4785) Optical security and encryption.

1. Introduction

Free-space optical (FSO) communication has been proposed in several applications such as satellite communications, intra-datacenter interconnections, metropolitan area network (MAN) extension and military applications [1]. Meanwhile, FSO communication is considered as a backup or complementary technology for the radio frequency (RF) communication in 5G transport network to enhance the robustness of the link [2]. Its major advantages are ease of deployment like RF communication and a wide optical bandwidth allowing much higher data rates than using typical RF wireless devices. In recent years, a lot of efforts have been made in alleviating the effects from the atmospheric turbulence-induced fading and scattering [3]. But, little attention has drawn to the network security. Traditional FSO links employ intensity modulation and direct detection (IM/DD) and are lack of considering the physical-layer methods to enhance security [4]. Although the good directionalty of lasers makes it more secure than RF technology, there is still a risk that optical signals in free-space being detected by malicious eavesdroppers. For example, an eavesdropping attack can be performed by detecting a small portion of the light beam while not inducing a significant insertion loss. It is prone to happen at the free space range away from the beam waist where the beam size is large.

In this paper, we propose a secure FSO communication system based on low temporal coherence of the amplified spontaneous emission (ASE). ASE noise can be generated easily from erbium dope fiber amplifier (EDFA), which gives the scheme an advantage over conventional coherent optical communication systems using lasers in terms of cost. The applicability of ASE in crosstalk mitigation is proven in [5, 6]. The phase across the ASE bandwidth experiences rapid changes due to the internal randomness of ASE noise, making it unable to track or reproduce. At the receiver side, coherent detection with optical delay matched between the signal and the local oscillator (LO) needs to be applied to recover the signal modulated on the ASE light, which acts like the 1^{st} encryption key. The eavesdropper may find it impossible to recover the signal even if both signal and LO are intercepted in the free-space channel because the optical delay between them is no longer matched. And the device with both a wide dynamic range and fine precision to search for the matched delay is not commercially available yet. Another innovation of our scheme is the 2^{nd} encryption by applying the spectral phase coding to the signal, which transforms the signal deliberately before launching it into free-space. The receiver needs to transform the LO in the same way which the signal experiences. Otherwise, they will not appear coherence even if the time delay is matched. We used chromatic dispersion as our 2^{nd} encryption key in our experiment and it has the potential to expand to other spectral phase coding methods like random phase offset for different slices of the ASE bandwidth.

2. 1^{st} Encryption Based on Low-coherence Property of ASE

A low-coherence source (LCS) is easy to obtain by using an EDFA, a polarizer and a spectral filter. The coherence length is dependent on its spectral width $\mathbf{B_{ase}}$ controlled by the filter. According to [5], a wider $\mathbf{B_{ase}}$ will have a shorter coherence length, which puts a stricter temporal matching requirement at the receiver.

The setup to characterize the performance of the secure FSO transmission system is shown in Fig. 1(a). At the transmitter (Tx), a 20-Gbaud QPSK or 8-PSK signal was generated through a single-polarization Inphase and Quadrature (IQ) Mach-Zehnder modulator (MZM) from the LCS module. After that, the signal was amplified

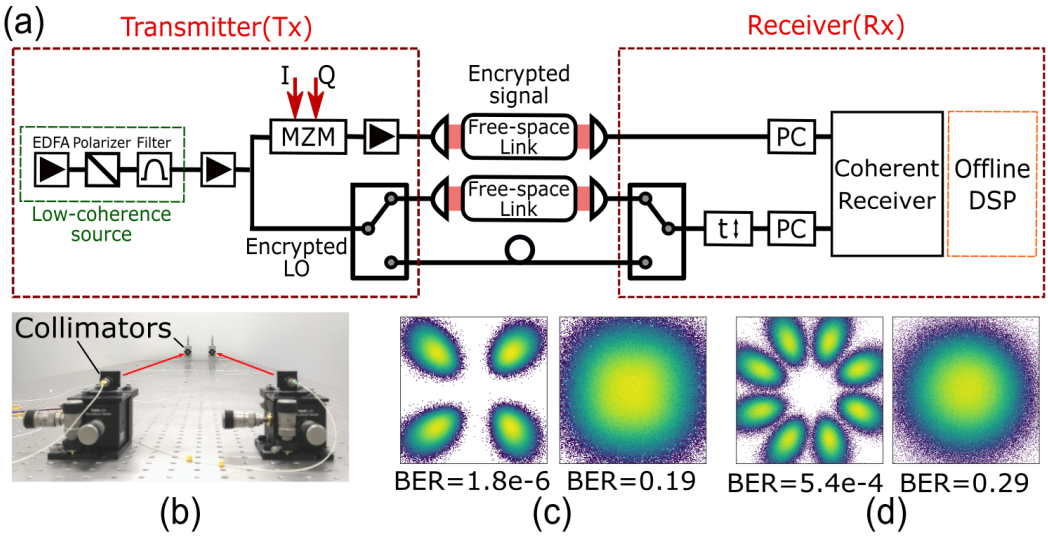

Fig. 1: (a) Setup for the secure FSO transmission system based on low-coherence matched detection, (b) photograph of the free-space link, recovered constellations of (c) QPSK and (d) 8-PSK using a ASE source with delay-matched condition on the left and its delay-unmatched counterpart on the right.

by an EDFA and then to the free-space link. One copy of the unmodulated ASE source was used as the LO for the coherent detection at the receiver, either through a free-space link or a single-mode fiber (SMF), controlled by a pair of optical switches on both sides of the channel. Each of the two FSO links consisted of a collimator made of a 18.40-mm focal length lens and a fiber holder with a multi-axis stage at the transmitter side, and a commercial collimator with 18.36-mm focal length at the receiver side, as shown in Fig. 1(b). A 4-m free space transmission distance is used for the proof-of-concept demonstration. At the receiver (Rx) side, a tunable delay line was used to set the delay between the signal and LO and two polarization controllers (PCs) are applied to align the polarization states between them. After the coherent receiver, an offline digital signal processing (DSP) chain including downsampling, timing synchronization, frequency offset compensation, frequency domain equalization, optical carrier recovery and BER calculation was applied to characterize the link performance.

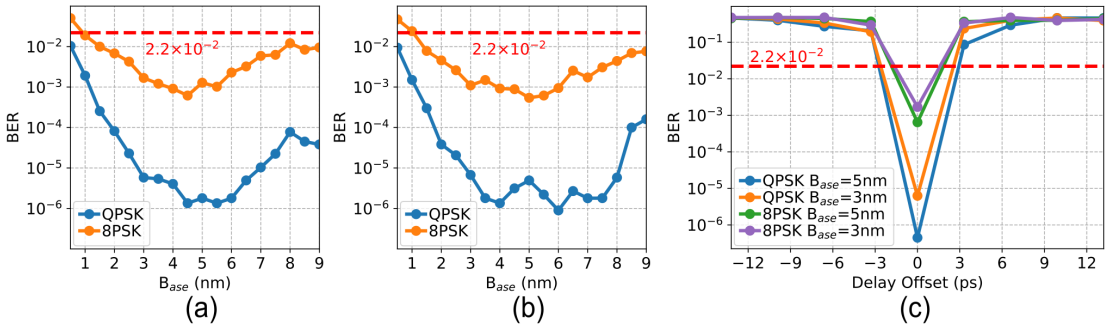

Fig. 2: The measured BER curves versus $\mathbf{B_{ase}}$ of QPSK and 8-PSK under delay-matched condition when the LO is transmitted through (a) a SMF and (b) a 4-m free-space, (c) the measure BER curves under delay-offset condition by tuning the fiber delay line manually when $\mathbf{B_{ase}}$ is fixed.

After the FSO transmission, the recovered constellations with delay matched and unmatched condition are present in Fig. 1(c) and (d), respectively. The delay-unmatched condition corresponds to the signal and LO being eavesdropped. Only when the delay is matched, the constellation will appear a fixed pattern radiating outward from the center, which is caused by the amplitude fluctuation of the ASE source. And achieving a low BER capable of communication is feasible in this condition. The BER cureves versus $\mathbf{B_{ase}}$ of QPSK and 8-PSK under delay-matched condition with two different ways to transmit the LO is showed in Fig. 2(a) and (b) respectively. Both two cases have preferable results, making a BER lower than 2.2×10^{-2} forward error correction (FEC) threshold. When a free-space LO is applied, the similarity between the two FSO channels makes the curves in Fig. 2(b) slightly better than those in Fig. 2(a). Figure 2(c) shows the measured BER curves with delay offset between the signal and LO by tuning the fiber delay line manually. Even a 3-ps delay offset will cause a huge increase in BER, making it higher than FEC threshold to realize error-free transmission. A 3-ps delay corresponds to roughly 1 mm for light propagating in free-space, which makes it difficult to eavesdrop when not knowing the delay between the signal and LO. So the delay can act like a key here, which is shared between the transmitter and receiver in advance. They can also dynamically change the delay key by adding extra fiber in their system or adjusting the light path, only need to make sure the delay is matched between the signal and LO.

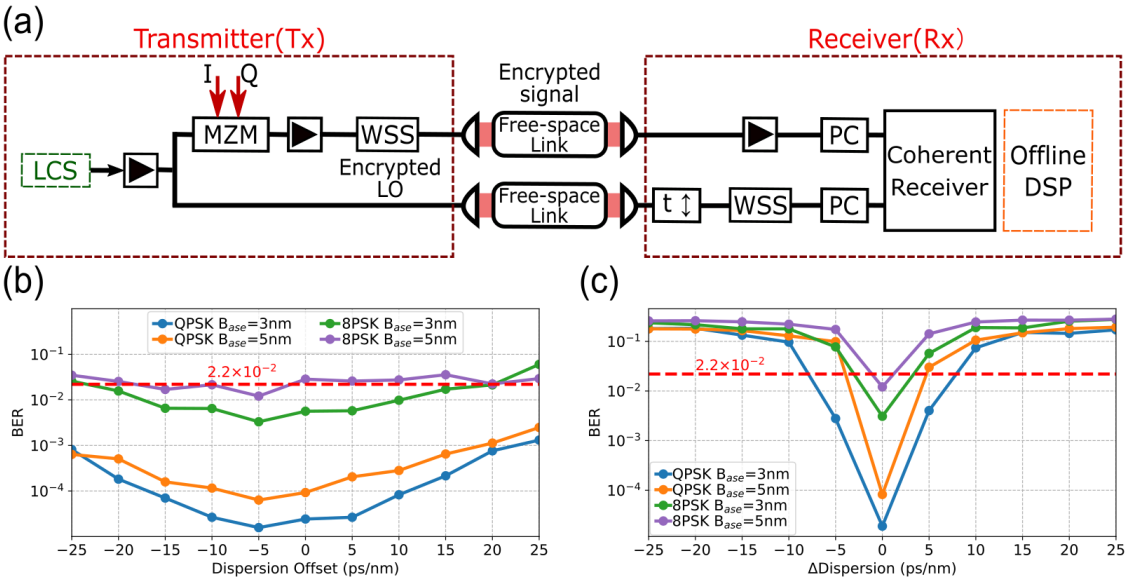

Fig. 3: (a) Setup for two-level optical encryption employing spectral phase coding, (b) the measured BER curves when the delay and dispersion value at both the transmitter and receiver are matched, (c) the measured BER curves when the delay is matched but dispersion values at the transmitter and receiver are different.

3. 2nd Encryption Based on Spectral Phase Coding

After the 1st encryption, the 2nd encryption using spectral phase coding is applied to prevent being eavesdropped by searching all the possible delay values mechanically. We used two programmable wavelength selective switches (WSSs) to achieve broadband and frequency-dependent phase modulation. A phase mask applying dispersion in each WSS was modulated to the signal before launching it into free-space, which blocked the correlation between the signal and LO even if they are matched in time domain. The setup employing spectral phase coding is shown in Fig. 3(a). One WSS was placed at the transmitter to employing the phase coding to the signal, and the other in the receiver to employing the same phase coding to the LO to recover the correct constellation. To compensate the insertion loss of WSS, an additional EDFA was put before the PC at the receiver. The measured BER curves with the same and different dispersion values of two WSSs are plotted in Fig. 3(b) and (c) respectively. In Fig. 3(c), the dispersion value in the Tx side is fixed to -5 ps/nm, and the dispersion value in the Rx WSS keeps scanning from -30 ps/nm to 20 ps/nm. The difference between them is defined as ΔDispersion. If the phase coding masks are the same at both sides, the curves show minor penalty compared to one-level encryption method, mainly because of the insertion loss of the devices. When the phase coding masks are different, the BER performances deteriorate rapidly with the difference of the applied dispersion values at both sides, thus the eavesdropper not only need to align the delay, but also need to find the correct phase coding pattern.

4. Conclusion

We proposed and experimentally demonstrated a secure FSO communication scheme based on the internal randomness of the ASE light source and realized a 20-Gbaud QPSK and 8-PSK transmission. The low coherence property and spectral phase coding between the signal and carrier prevents data from being eavesdropped, which can effectively enhance the security of future wireless network.

This work was supported in part by the National Natural Science Foundation of China (Project No. 61420106011, 61635006, 61601277, 61601279) and the Science and Technology Commission of Shanghai Municipality (Project No. 17010500400, 18511103400).

References

1. M. A. Khalighi, et.al., "Survey on Free Space Optical Communication: A Communication Theory Perspective," in *IEEE Communication Surveys and Tutorials* **16**, pp. 2231-2258 (2014).
2. J. M. Estarán, et.al., "FSO SpaceComm Links and Its Integration with Ground 5G Networks," in *Optical Fiber Communication Conference (OFC)*, 2019, p. M4F.1.
3. K. P. Peppas, et.al., "Free-Space Optical Communication With Spatial Modulation and Coherent Detection Over H-K Atmospheric Turbulence Channels," in *J. of Lightwave Technol.* **33**, pp. 4221-4232 (2015).
4. Hiroyuki Endo, et.al., "Free-space optical channel estimation for physical layer security," in *Opt. Express* **24**, pp. 8940-8955 (2016).
5. H. Chen, et.al., "Optical Crosstalk Reduction using Amplified Spontaneous Emission (ASE)," in *Optical Fiber Communication Conference (OFC)*, 2018, p. M4G.5.
6. Y. Huang, et,al., "Mode-Multiplexed Transmission with Crosstalk Mitigation Using Amplified Spontaneous Emission (ASE)," in *Conference on Lasers and Electro-Optics*, 2019, paper SM1G.2.