Slepian-FBGs-based Optical Covert Communications

Ivan B. Djordjevic

University of Arizona, Department of Electrical and Computer Eng., 1230 E. Speedway Blvd., Tucson, AZ 85721, USA
E-mail: ivan@email.arizona.edu

Abstract— Various optical encryption/physical-layer security schemes are able to protect the content of the message, but are not able to protect user's privacy by preventing the detection of transmission attempt. To solve for this problem, we propose a Slepian-FBGs-based scheme enabling positive rate optical covert communications.

I. INTRODUCTION

Significant effort has been made to satisfy never-ending demands for higher data rates and to deal with the incoming bandwidth capacity crunch [1]. On the hand, by tapping out the portion of DWDM signal, the huge amount of data can be compromised [2]-[4]. Therefore, the security of future optical networks is becoming one of the key issues to be addressed sooner rather than later. To solve for this problem we recently proposed several physical-layer security (PLS) schemes suitable for optical communications [1]-[4]. Various optical PLS schemes, proposed so far, are able to protect the content of the message, but are not able to protect the users' privacy from detecting the very existence of the message [5]-[9].

To solve for this problem, in this paper we propose to use the Slepian sequences based FBGs (Slepian-FBGs) described in [1] in different context, having the orthogonal impulse responses, to enable future positive-rate covert optical communications. In covert communications [5]-[9], also known as stealth or low probability of detection (LPD) [6] communications, the encrypted channel is hidden within the public channel. So the covert optical communications will be able not only to protect the message, but also to protect user's privacy by preventing the detection of transmission attempt. Conventional covert communications are governed by the square root law, indicating that $\mathcal{O}(\sqrt{n})$ bits can be reliably

transmitted in n channel uses without being detected by adversary. With the proposed Slepian-FBGs, we can achieve the positive-rate covert optical communication in which $\mathcal{O}(n)$ covert symbols can be transmitted in n channel uses, therefore, dramatically increasing the covert communication rate.

II. SLEPIAN-FBGs-BASED COVERT COMMUNICATIONS

For conventional covert optical communication, we have to transmit $\mathcal{O}(\sqrt{n})$ covert bits in n channel uses, with mean photon number of $\mathcal{O}(1/\sqrt{n})$, in the presence of amplified spontaneous emission (ASE) noise. Alice and Bob also pre-share the $\mathcal{O}(\sqrt{n} \log n)$ bits specifying the locations where to place/take the covert bits and one-

time pad of size $\mathcal{O}(\sqrt{n})$ to avoid the adversary exploiting the FEC side information. The problem with this conventional approach is the zero cover rate for large n , given that [5]-[9] $\mathcal{O}(\sqrt{n})/n \rightarrow 0$ as $n \rightarrow \infty$. To solve for this

problem and enable positive rate covert optical communication, here we proposed to use Slepian-FBGs.

The encoder scheme for Slepian-FBGs-based optical covert communication, shown in Fig. 1(top), is composed of two stages: *encryption stage*, the upper section of the encoder, and the *masking stage*, the lower section of the encoder, serving the role of a friendly jammer in wireless communications. The pulse laser is used in encryption stage, while the ASE noise source, such as EDFA together with variable optical attenuator (VOA), is used in the masking stage. The data sequence is by means of an electro-optical modulator (E/O MOD) such as Mach-Zehnder modulator (MZM), phase modulator, or optical I/Q modulator converted into optical domain. The 1:K optical switch is used to randomly select one out of K available Slepian-FBGs to be used as an encryption device. On the other hand, an arbitrary sequence, synchronized with data sequence generator, is used in masking stage to ensure that signal sequence and noise sequence are synchronized. The optical input to E/O MOD in masking stage is an additive white Gaussian noise signal generated by the ASE noise source. One of L available Slepian-FBGs is selected at random by control input of the 1:L optical switch. On such a way the colored Gaussian noise is orthogonal to encrypted data sequence. Both Slepian-FBGs of encryption and masking sections are derived from the same class of Slepian sequences of cardinality $\geq L+K$. On the receiver side, as shown in Fig. 1(bottom), the matched conjugate Slepian-FBG has been used to decipher the transmitted sequence. When the transmitter and receiver use complementary Slepian-FBGs strong autocorrelation peak get generated at every signaling interval, while zero autocorrelation is obtained after non-matched Slepian-FBGs. Since the masking sequence has been generated by randomly selected Slepian-FBG, generated from the same set of Slepian sequences as for the encryption stage of the transmitter, there is no need to use de-masking at the receiver side. Therefore, the masking is used only to hide any data structure to the adversary in both time- and spectral-domains. At the same time, the signal level is kept below the ASE noise level. To enable positive rate covert optical communication, we have to operate the scheme shown in Fig. 1 as follows. Namely, from [8],[9] we learned that positive rate covert communication is possible when adversary is either ignorant of the

probabilistic structure of the noise channel or does not have complete knowledge of the noise model. For instance, it has been shown in [9] that AWGN variance fluctuations yield to positive rate covert communication. The key idea of our proposal is in addition to Alice-Bob covert communication model shown in Fig. 1(top), to employ also the masking stage shown in Fig. 1(bottom), to add the Slepian-FBGs colored Gaussian noise of variable average noise power, whose level is changed by VOA. Given that the seed for selection of Slepian-FBGs is secretly pre-shared between Alice and Bob, adversary will neither know which randomly selected-FBG is used in masking stage nor what is the average noise power, and given his ignorance of the probabilistic structure of the noise source, the positive rate covert optical communication will be possible. Also, given the ignorance of adversary's noise model, the positive rate covert optical communication is achievable.

The proposed scheme is applicable to any optical communication system: (i) SMF-based, (ii) free-space optical (FSO) channel-based, (iii) few-mode fiber (FMF)-based, (iv) few-core fiber (FCF)-based; to mention few. In the rest of this paper, we focus on Slepian-FBGs-based FSO covert communications.

Fig. 1 Encoder/decoder configurations for Slepian-FBGs-based optical covert communications: (a) encryption scheme, (b) decryption scheme.

III. FBGS-BASED FSO COVERT COMMUNICATIONS

The encryption and decryption schemes for covert FSO communications are already provided in Fig. 1. The output of the encryption stage is with the help of an expanding telescope transmitted towards the Bob's receiver. After compressing telescope, the decryption takes place as illustrated in Fig. 1(bottom). During FSO propagation, the signal experiences the atmospheric turbulence and Mie scattering effects.

To model turbulence effects we employ the gamma-gamma distribution of irradiance, which is valid in all turbulence regimes. The Rytov variance is used as a figure of merit to characterize the turbulence strength, since it takes refractive structure parameter C_n^2 , FSO link length L , and wavelength λ into account; and it is defined

as $\sigma_R^2 = 1.23 C_n^2 (2\pi / \lambda)^{7/6} L^{11/6}$. For $\sigma_R^2 < 1$ the system is affected with weak turbulence, while for $\sigma_R^2 > 1$ with strong turbulence. To demonstrate high potential of proposed Slepian-FBGs-based FSO covert communications, we performed Monte Carlo simulations, with results being summarized in Fig. 2, in which we compare the covert capacity per single dimension (spatial mode) against secrecy capacity/dimension of the PLS scheme proposed in [3]. For the PLS scheme, the ratio in average SNRs for main (Alice-Bob) and adversary channels, defined as $\rho = \bar{\gamma}_m / \bar{\gamma}_a$, is used as a parameter.

Clearly, the proposed Slepian-FBGs-based covert communication scheme provides positive covert capacity for all SNR values in main channel, and significantly outperforms the corresponding PLS scheme. While PLS scheme benefits from atmospheric turbulence effects, the covert communication scheme is affected by turbulence effects, but still significantly outperforms the PLS scheme in strong turbulence regime.

Fig. 2 Covert capacity (per dimension) of proposed scheme against secrecy capacities of corresponding PLS scheme over FSO links for weak (top) and strong (bottom) turbulence regimes.

REFERENCES

- [1] I. Djordjevic, *et al.*, *Opt. Express*, vol. 22, pp. 10882-10897, 2014.
- [2] X. Sun, I. Djordjevic, *IEEE Photonics J.*, vol. 8, p. 011110, 2016.
- [3] I. B. Djordjevic, *et al.*, *IPC 2017*, Paper ThH1.3, 2017, FL, USA.
- [4] I. Djordjevic, *IEEE Photonics J.*, vol. 9, no. 4, p. 7905712, 2017.
- [5] B. A. Bash, *et al.*, *Nature Communications*, vol. 6, p. 8626, 2015.
- [6] M. Bloch, *IEEE Trans. Inform. Th.*, vol. 62, pp. 2334-2354, 2016.
- [7] B. Bash, *et al.*, *IEEE J. Sel. Areas Comm.*, vol. 31, p. 1921, 2013.
- [8] S. Craver, *IS&T Electronic Imaging*, vol. 7541, p. 754 103, 2010.
- [9] S. Lee, *et al.*, *IEEE J. Sel. Top. Signal Proc.*, vol. 9, p. 1195, 2015.