

BESSEL-GAUSSIAN BEAMS AND PHYSICAL-LAYER SECURITY IN A FREE-SPACE
OPTICAL CHANNEL

by

Tyan-Lin Wang

Copyright © Tyan-Lin Wang 2018

A Thesis Submitted to the Faculty of the

COLLEGE OF OPTICAL SCIENCES

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

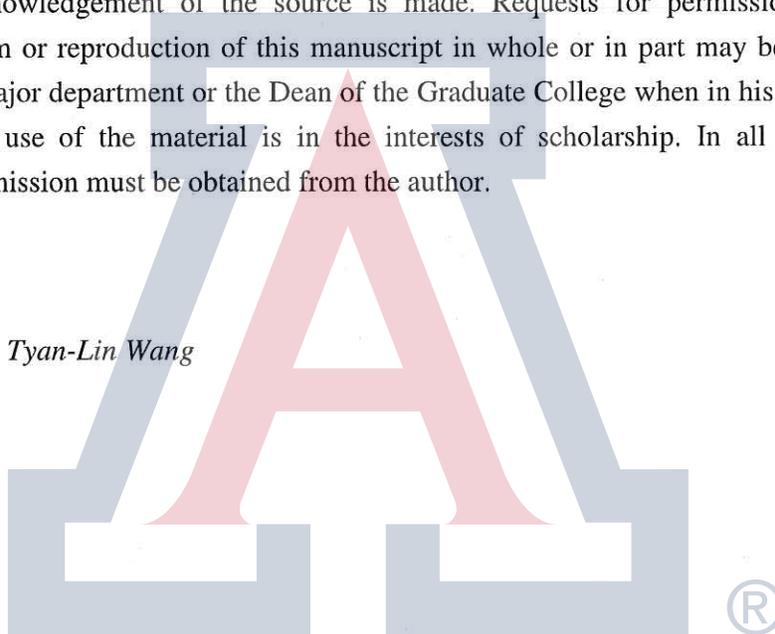
2018

STATEMENT BY AUTHOR

The thesis titled *Bessel-Gaussian Beams and Physical-Layer Security in a Free-Space Optical Channel* prepared by *Tyan-Lin Wang* has been submitted in partial fulfillment of requirements for a master's degree at the University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this thesis are allowable without special permission, provided that an accurate acknowledgement of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: *Tyan-Lin Wang*



APPROVAL BY THESIS DIRECTOR

This thesis has been approved on the date shown below:

Ivan B. Djordjevic

Dr. Ivan B. Djordjevic

Date

11/29/18

*Professor of Electrical and Computer Engineering
Professor of Optical Sciences*

ACKNOWLEDGEMENTS

I'd like to thank Prof. Ivan Djordjevic for accepting me into his research group and for his technical and financial support of this thesis project. I'm very grateful for the funding provided by the Office of Naval Research MURI program N00014-13-1-0627. I also want to thank my committee members Prof. Miroslav Kolesik, with whom I published a paper in Optics Letters, and Prof. Yuzuru Takashima, for advice regarding spatial light modulators in my experiments. I'd further like to acknowledge John Gariano and Mingwei Yang for their assistance with my experimental setup in the Optical Communications Systems Laboratory (OCSL) and Stefan Osten at Holoeye Photonics AG for providing technical support for the spatial light modulators. I want to recognize the staff in the Electrical and Computer Engineering department for providing assistance with purchase orders for equipment and providing IT support whenever I needed it.

I appreciate the College of Optical Sciences for giving me the opportunity to study in their program and Lindsay Loebig and Mark Rodriguez for their administrative help.

Finally, I wish to thank my parents for their understanding and encouragement when I made the decision to move to Arizona.

Table of Contents

List of figures	5
List of tables.....	8
Abstract.....	9
1 Introduction.....	10
2 Physical-Layer Security and the FSO Communications Channel	13
2.1 Physical-Layer Security in an Optical Wiretap Channel	13
2.2 Atmospheric Turbulence in the FSO Channel	15
2.3 Using Orbital Angular Momentum Modes for FSO	18
3 Employing Bessel-Gaussian Beams to Improve Physical-Layer Security in FSO.....	21
3.1 Definitions and Beam Propagation Simulations	21
3.1.1 Secrecy Capacity Formulas.....	21
3.1.2 Simulation Parameters	22
3.1.3 Simulation Results	23
3.2 Experiments With Spatial Light Modulators	25
3.2.1 Experimental Setup.....	25
3.2.2 Experimental Results	29
4 Physical-Layer Security of a Binary Data Sequence Transmitted with Bessel-Gaussian Beams.....	32
4.1 Laboratory Emulation of an Optical Wiretap Channel	32
4.2 Discussion of Operational Aspects	37
5 Conclusion	40
References.....	41

List of figures

Figure 2.1. Diagram of the Open System Interconnection model (source: Wikipedia).	13
Figure 2.2. (a) Schematic of an FSO link showing Eve performing an optical beam-splitting attack near Alice (top) near Bob (bottom). (b) Block diagram of the optical wiretap channel formulated in terms of Wyner's model. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE. .	13
Figure 2.3. Comparison of several PSD models used for atmospheric turbulence modeling.	17
Figure 2.4. Curve fitting to the gamma-gamma probability density function for a 1 km channel resulting in estimated values of $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), 5×10^{-14} (right) along with their corresponding Rytov variance. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.	17
Figure 2.5. (a) Depiction of Laguerre-Gaussian OAM modes from order -2 to order +2 (source: Wikipedia). (b) Top: Comparison of the formation of an ordinary Gaussian beam with a Bessel beam, highlighting the Bessel beam's longer depth of focus (source: [14]). Bottom: Simulated evolution of the zero order Bessel-Gaussian OAM mode undergoing refractive index distortions caused by turbulence of increasing strengths.....	19
Figure 2.6. Experimentally generated OAM modes from order 0 to order +5 after refractive index distortions caused by turbulence of strength $C_n^2 = 5 \times 10^{-14}$. The top row contains beam profiles for BS modes and the bottom row contains beam profiles for LG modes. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.	20
Figure 3.1. Simulated OAM modes from order 0 to order +5 after 1 km of propagation distance through $C_n^2 = 10^{-14}$ turbulence. The top row contains intensity profiles for BS modes and the bottom row contains intensity profiles for LG modes. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.....	24
Figure 3.2. Simulation crosstalk matrices for BS modes (top) and LG modes (bottom) for $C_n^2 = 10^{-17}$, 10^{-16} , 1.75×10^{-16} , and 1.75×10^{-15} (from left to right). Transmitted orders are labeled along the rows and the reference orders are labeled along the columns. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.	24
Figure 3.3. Plots of aggregate secrecy capacity calculated from crosstalk matrices over orders -15 to +15 as a function of turbulence strength. The shaded bands surrounding the data points represent error bars over the Monte Carlo runs. Reprinted with permission from T.-L. Wang, J. A.	

Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.....	25
Figure 3.4. OAM modes from order 0 to order +5. Top two rows: Phase pattern and beam profiles for finer resolution BS modes with a period of 64 pixels. Middle two rows: Phase pattern and beam profiles for coarser resolution BS modes with a period of 128 pixels. Bottom two rows: Phase pattern and beam profiles for LG modes. The transparent yellow circle overlaying each of the phase patterns represents the 5 mm diameter laser beam incident on the SLM chip. All the beam profile images were captured after 600 mm of tabletop propagation distance. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.	26
Figure 3.5. Diagram of the back-to-back experimental configuration. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.....	27
Figure 3.6. Conjugate mode detected spots for BS (left) and LG (right) modes from order -3 to order +3 in the back-to-back experiment. The thumbnails are not explicitly labeled but the transmitted orders are arranged along the rows and the reference orders along the columns following Figure 3.2. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE...	28
Figure 3.7. Diagram of the full experimental configuration including turbulence emulator. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.	28
Figure 3.8. Conjugate mode detected spots for BS modes from order -5 to order +5 for $C_n^2 = 5 \times 10^{-14}$ in the full experiment. The thumbnails are not explicitly labeled but the transmitted orders are arranged along the rows and the reference orders along the columns following Figure 3.2. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.	29
Figure 3.9. Conjugate mode detected spots for LG modes from order -5 to order +5 for $C_n^2 = 5 \times 10^{-14}$ in the full experiment. The thumbnails are not explicitly labeled but the transmitted orders are arranged along the rows and the reference orders along the columns following Figure 3.2. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.	30
Figure 3.10. Experimental crosstalk matrices of BS beams (top) and LG beams (bottom) for $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), and 5×10^{-14} (right). Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.....	31

- Figure 4.1. Diagram of the experimental setup emulating the optical wiretap channel (top). The noise loading stage consisting of ASE source, TBF, EDFA, and VOA is drawn on the top left corner of the diagram. The photograph on the bottom shows the free space portion of the setup. The red line traces the path of the laser beam through the FSO channel. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE..... 32
- Figure 4.2. Generated BS modes from order 0 to order +5 (from left to right) when no turbulence is applied. The top row shows beam profiles taken at checkpoint 1 and the middle row shows their evolved propagation at checkpoint 2. The bottom row shows beam profiles taken at checkpoint 3 when only SLM 3 contains the BS mode phase pattern and SLMs 1 and 2 do not. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE. 34
- Figure 4.3. Near-field conjugate mode-sorted beam footprints for transmitted BS modes of order 0 to order +5 (from left to right). Visual inspection showed that above order +2 the coupling of the data-carrying beam into the optical fiber would be inefficient. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE..... 35
- Figure 4.4. BER curves of $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), 5×10^{-14} (right). Bob's data points are shown in gray-filled circles and Eve's data points are shown in red-filled squares. Every set of data points is plotted with a dashed line curve fit to indicate the overall trend. In each plot a yellow triangular region upper bounded by 0.5 highlights Eve's BER curves to distinguish them from Bob's BER curves. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE..... 36
- Figure 4.5. Secrecy capacity values computed from the difference between the overlap regions of Bob's and Eve's measured BER curves for $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), 5×10^{-14} (right). Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE. 37

List of tables

Table 3.1. Beam Propagation Simulation Parameters. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.....	23
Table 3.2. Aggregate Secrecy Capacity Values From Experimental Crosstalk Matrices Over Orders -5 to +5. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.....	31

Abstract

Physical-layer security in free-space optical communications channels can be compromised when an eavesdropper performs optical beam-splitting attacks over an atmospheric channel. In this scenario the free-space optical communications channel is referred to as an optical wiretap channel, which is an extension of Wyner's wiretap channel model. For secure communications, Shannon's classical solution requires the transmitter and receiver to share a common secret key of length greater than or equal to the message length. This can become intractable as the message length grows in size. On the other hand the wiretap channel model proposed by Wyner is based on the premise that secrecy can be obtained even without a shared key if the noisy and degraded channel conditions experienced by the eavesdropper can be exploited. The primary metric to analyze physical-layer security is secrecy capacity, the highest data capacity at which the eavesdropper is unable to obtain information sent from the transmitter to the receiver. Positive secrecy capacity is possible when the main channel to the receiver is of better quality than the channel to the eavesdropper in the sense of signal-to-noise ratio.

In this thesis we study how transmitting data using orbital angular momentum modes such as Laguerre-Gaussian and Bessel-Gaussian beams can achieve higher secrecy capacities compared to that of ordinary Gaussian beams within the turbulent conditions of an optical channel. Using computer simulations and experiments with spatial light modulators we demonstrate that Bessel-Gaussian beams provide 10 to 30 bits/sec/Hz higher secrecy capacity over their corresponding Laguerre-Gaussian counterparts in the weak to medium turbulence regimes, indicating a better resilience to atmospheric turbulence effects. We follow this with another experiment exclusively conducted with Bessel-Gaussian beams onto which we encode a pseudo-random binary sequence to emulate data transmission over an optical wiretap channel. Bit-error rate curves for the intended receiver and the eavesdropper are calculated from which estimates of secrecy capacity are derived. We demonstrate that the bit-error rate curves for the eavesdropper are consistently worse than those of the intended receiver under several turbulence conditions and find further evidence of an error floor even when the eavesdropper uses an optical amplifier. While these results show promise for secure communications further research will be needed to optimize the quality of these beams to help realize a practical system.

1 Introduction

Free-space optical (FSO) communications over an atmospheric channel using information-carrying laser beams can provide high directionality and high data rate transmission between buildings or between moving platforms when the line of sight is maintained. This can be crucial in situations where an optical fiber infrastructure is either non-existent or hard to establish. Over relatively short distances the narrow divergence of a laser beam makes interception difficult and provides secure communications especially if the beam is initially collimated. However, over longer distance transmission, the beam divergence becomes an issue and atmospheric turbulence, scattering, and beam wander can allow an eavesdropper to capture a portion of the beam. Thus, the FSO system design must take into account both reliability and security issues of the transmitted message.

One of the aspects for secure communications at the physical layer, which arises from the classic solution developed by Shannon [1], is that it requires the transmitter (Alice) and receiver (Bob) to share a common secret key that is unknown to the eavesdropper (Eve). Alice uses a cipher to encrypt the message and sends it over the channel to Bob who then performs decryption on the received codeword. The simplest way to share a private key while providing unconditional security is the one-time pad. However, the information theory dictates that the length of the key must be at least as long as the message, must be securely distributed and stored in advance, and then discarded after use. Repeating this procedure every time a message is transmitted will become intractable as the length of the codeword grows in size. In addition, Shannon assumed a noiseless channel, which is not a realistic assumption. In 1975, A. D. Wyner developed the discrete memoryless wiretap channel model [2], which is based on the premise that secrecy can be obtained even when both parties do not share a key. The idea behind Wyner's model establishes secrecy by exploiting the noisy and imperfect channel itself, taking advantage of the fact that in a majority of scenarios the channel from Alice to Eve is degraded compared to that from Alice to Bob, which is typically true for FSO communications links. The mathematical formulation yielded a metric known as secrecy capacity in which communications are considered to be secure if the secrecy capacity stays positive. Intuitively the secrecy capacity is the highest data capacity at which Eve is unable to obtain information transmitted from Alice to Bob.

Research on physical-layer security (PLS) in the radio frequency (RF) domain has become a very popular topic this past decade and an overview of those developments are provided in [3]. Parallel research efforts pertaining to security in the FSO domain have also been ongoing and conceptual details along with information-theoretic secrecy capacity formulas for FSO are provided in [4]. Wyner's model can be extended to FSO channels which can then be referred to as the optical wiretap channel. In this context atmospheric turbulence induced refractive index changes serve as the main channel degradation mechanism and Eve attempts hypothetical optical beam-splitting attacks to covertly extract approximately 1% of the transmitted power without being noticed. Although atmospheric turbulence poses physical limitations on achieving power efficient and spectrally efficient data transmission, it can also be turned into an advantage in terms of achieving secrecy. In conjunction with this secrecy advantage, encoding the data onto laser beams which carry orbital angular momentum (OAM) can potentially increase the secrecy capacity to levels beyond what is achievable with a single Gaussian mode due to their intrinsic orthogonality property.

Beam propagation simulations through atmospheric turbulence using various orders of Laguerre-Gaussian (LG) beams were recently performed in [5] where aggregate secrecy capacities for PLS were calculated for several turbulence strengths to show improved performance over that of ordinary Gaussian beams. An older comprehensive study that numerically simulated the propagation of LG modes in an optical channel and quantified the OAM crosstalk versus turbulence strength [6] is also very relevant in the context of PLS. Using these results as background, we performed numerical simulations and experiments with spatial light modulators and showed that Bessel-Gaussian (BS) OAM beams can be used to further improve PLS secrecy capacities. The procedure involved comparing the propagation of several orders of BS and LG modes under various turbulence conditions, generating crosstalk matrices, and calculating the corresponding secrecy capacity values from the saved data. Since the crosstalk matrix measurements showed that BS modes could yield higher values of secrecy capacity than LG modes by 10 to 30 bits/sec/Hz, we devised a data transmission experiment which emulates an optical wiretap channel and measured the bit-error rate (BER) curves obtained at Bob's and Eve's receivers. The experiment was done exclusively with BS beams and under the same turbulence conditions and the results demonstrated once again that positive secrecy capacity can be achieved even in binary channels with direct detection.

This thesis is organized as follows. Chapter 2 discusses physical-layer security in the context of FSO, describes modeling atmospheric turbulence in the FSO channel, and motivates the use of orbital angular momentum modes for FSO communications. Chapter 3 summarizes the results from beam propagation simulations and the experiments with spatial light modulators to show that employing Bessel-Gaussian beams can improve physical-layer security in FSO. Chapter 4 summarizes the results from further experiments involving encoding and transmitting a binary data sequence using Bessel-Gaussian beams to achieve PLS over eavesdropping. Finally, Chapter 5 gives the conclusion.

The majority of the content contained in this thesis is taken from the author's publications:

T.-L. Wang, I. B. Djordjevic, "Physical-Layer Security of a Binary Data Sequence Transmitted with Bessel-Gaussian Beams Over An Optical Wiretap Channel," *IEEE Photonics Journal*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611.

T.-L. Wang, J. A. Gariano, I. B. Djordjevic, "Employing Bessel-Gaussian Beams to Improve Physical-Layer Security in Free-Space Optical Communications," *IEEE Photonics Journal*, vol. 10, no. 5, Sep. 2018, Art. no. 7907113.

Since the copyright has already been transferred to IEEE, the following message is required:

“In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of the University of Arizona's products or services. Internal or personal use of this material is permitted.

If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.”

2 Physical-Layer Security and the FSO Communications Channel

2.1 Physical-Layer Security in an Optical Wiretap Channel

Before considering security we describe what is meant by the physical layer. The Open Systems Interconnection (OSI) model is a protocol developed by the International Organization for Standardization which is used for communications between different networks. The lower levels are the media layers of which the physical layer is the bottom-most level as shown in Figure 2.1. It is here where digital data signals are transmitted between communications devices in the form of bits or voltages over a transmission medium. When considering security, the most important goal is to hide information from Eve at the physical layer. The higher layers such as data link and network layers group the bits into frames and packets respectively. Establishing security at these layers is insufficient to prevent Eve from learning something about the message.

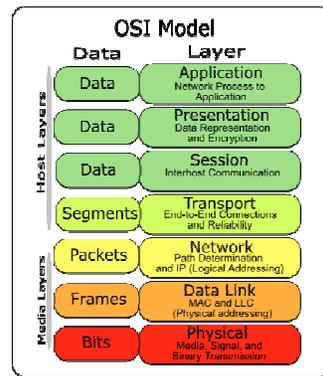


Figure 2.1. Diagram of the Open System Interconnection model (source: Wikipedia).

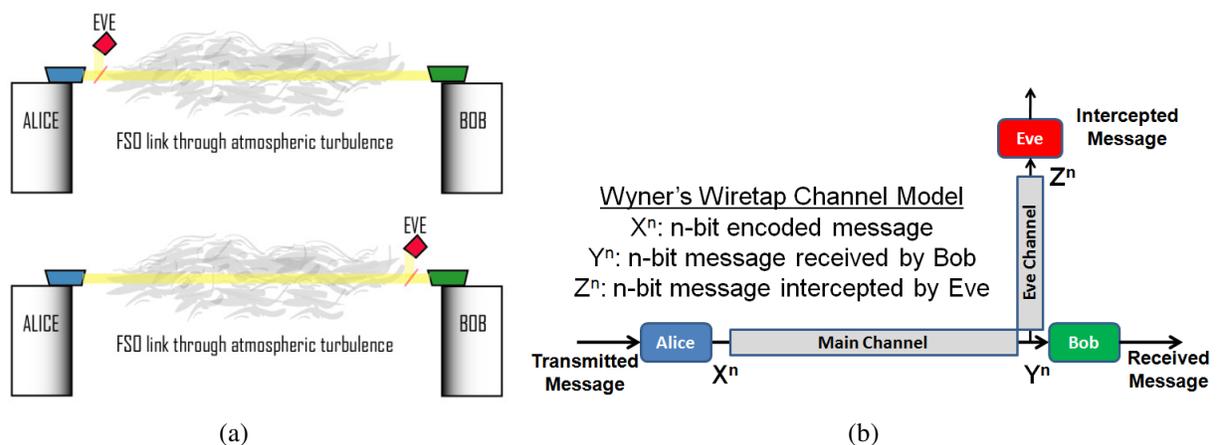


Figure 2.2. (a) Schematic of an FSO link showing Eve performing an optical beam-splitting attack near Alice (top) near Bob (bottom). (b) Block diagram of the optical wiretap channel formulated in terms of Wyner's model. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE.

Wyner's model extended to encompass the FSO communications channel is referred to as the optical wiretap channel and is illustrated in Figure 2.2. In addition to noise, the atmospheric turbulence induced refractive index fluctuations within the channel will impart intensity scintillations onto the information-carrying laser beam. Although in principle the eavesdropper can be located near the transmitter, this precludes the covertness of the attack. Thus the most practical PLS scenario has the transmitter and receiver being aligned to maximize the received power and the eavesdropper performing the attack near the receiver. While Eve can perform optical beam-splitting attacks in the channel to compromise PLS, it's possible to exploit the noisy and degraded channel conditions to obtain a certain level of secrecy even when Alice and Bob do not use a shared key for communications. This argument carries more weight if Eve is only allowed to intercept approximately 1% of the signal power. Going back to Figure 2.2, when Alice transmits a n -bit encoded message X^n , Bob receives Y^n over the main channel and Eve receives Z^n over another channel. The level of PLS in an FSO system is determined by the secrecy capacity where a positive value is possible only if the channel to Bob is of higher quality than the channel to Eve in terms of signal-to-noise ratio (SNR). Secrecy capacity C_S is defined as the difference between the mutual information of the Alice-Bob messages $I(X^n, Y^n)$ and the Alice-Eve messages $I(X^n, Z^n)$ where $I(X^n, Y^n) = H(X^n) - H(X^n|Y^n)$ and $I(X^n, Z^n) = H(X^n) - H(X^n|Z^n)$. The entropy $H(X^n)$ refers to the uncertainty in the original message during transmission while $H(X^n|Y^n)$ and $H(X^n|Z^n)$ refer to the uncertainty remaining in that message given Y^n and Z^n are received, respectively. From these definitions it is apparent that secrecy capacity is maximized when $I(X^n, Z^n) = 0$ i.e. Eve's uncertainty remaining in the received message equals its original uncertainty and thus Eve learns nothing from the intercepted message.

However, obtaining perfect secrecy requires unconditional statistical independence between X^n and Z^n which is not possible under realistic channel conditions so alternative criteria such as weak secrecy where $(1/n)I(X^n, Z^n) \rightarrow 0$ as $n \rightarrow \infty$ and strong secrecy where $I(X^n, Z^n) \rightarrow 0$ as $n \rightarrow \infty$ are employed. In particular, the strong secrecy condition necessitates that the amount of information learned by Eve approaches zero as the number of transmitted bits is increased and much research progress has been made to put this condition into mainstream use [3]. Returning to the definition of secrecy capacity of the discrete memoryless channel, because $I(X^n, Z^n)$ is always a nonzero quantity, Wyner formulated secrecy capacity based on considering X^n and Z^n as statistically independent given Y^n . The goal was then to maximize the difference between

$I(X^n, Y^n)$ and $I(X^n, Z^n)$ which can be accomplished by factoring in the non-ideal channel conditions. For secrecy capacity to be positive all that's needed is for the Alice-Bob channel to be less noisy and less degraded compared to the Alice-Eve channel at the level of the physical layer. In other words, the presence of turbulence in the channel provides the advantage that is needed to achieve security at the cost of some degree of reliability.

The definition has been adapted to the FSO channel [4] where the secrecy capacity from Alice to Bob is denoted as C_{AB} and the capacity from Alice to Eve is denoted as $C_{AE,Rx}$ (when Eve is near the receiver). The resulting expression $C_{S,Rx} = C_{AB} - C_{AE,Rx} = \log_2(1+\gamma_b) - \log_2(1+\gamma_{e,Rx})$ in units of bits/sec/Hz, where γ_b and $\gamma_{e,Rx}$ are Bob's SNR and Eve's SNR respectively, resembles the difference between the Shannon capacities of the Alice-Bob channel and the Alice-Eve channel due to the presence of SNR terms. As such, it is clear that as long as Bob's SNR is greater than Eve's SNR the communication will be secure. One should keep in mind that the above secrecy capacity formula only provides an information-theoretic upper bound but does not specify how that limit can be reached. Factors such as the strength of turbulence, the alignment accuracy of Eve's beam-splitter, the amount of extracted power, and the detection efficiency may influence the magnitude of $C_{S,Rx}$. More interestingly, transmitting binary data encoded onto BS beams may also impact the $C_{S,Rx}$ values.

2.2 Atmospheric Turbulence in the FSO Channel

Atmospheric turbulence occurs when differential heating and cooling of the Earth by sunlight leads to temperature variations that create wind. These convective motions accompanying the temperature changes will alter the refractive index of the air both spatially and temporally. This flow can transition from a laminar to a turbulent state, resulting in the formation of randomly distributed pockets of air or turbulent eddies. Since these eddies occur in various sizes the atmosphere consistently exhibits a random refractive-index profile, which affects both imaging and beam propagation.

The simplest approach to model atmospheric turbulence is to formulate it as a random process having an associated power spectral density (PSD). In computer simulations, arrays of random numbers are generated on a grid and filtered according to prescribed PSD models to become phase screens which approximate the statistical behavior of the turbulence over extended atmosphere. Information-carrying laser beams that propagate through turbulence will experience intensity scintillations that lead to beam distortion and beam wander. Commonly used PSD

models for phase screens are Kolmogorov, Tatarskii, Von Karman, and Modified Atmospheric which is also called the Andrews PSD [7]. The formula for each PSD as a function of spatial wavenumber κ is shown below in the order listed above. In these formulas the quantity C_n^2 is the refractive structure parameter which represents the strength of the turbulence and the factors $\kappa_l = 3.3/l_0$, $\kappa_m = 5.92/l_0$, and $\kappa_0 = 2\pi/L_0$, incorporate the quantities l_0 and L_0 which are the inner scale and outer scale of the turbulent eddies respectively. Changing the parameters in the functional form of the PSD formula causes the high and low spatial frequency features and the amount of root-mean-square wavefront displacement to change. One caveat is that these power law scaling models assume adequate time has passed for the turbulence to settle in, which is not always true in reality.

$$\begin{aligned}\Phi_n(\kappa) &= 0.033C_n^2\kappa^{-11/3} \\ \Phi_n(\kappa) &= 0.033C_n^2\kappa^{-11/3}e^{-\kappa^2/\kappa_m^2} \\ \Phi_n(\kappa) &= 0.033C_n^2\frac{e^{-\kappa^2/\kappa_m^2}}{(\kappa^2 + \kappa_0^2)^{11/6}} \\ \Phi_n(\kappa) &= 0.033C_n^2\left[1 + 1.802\left(\frac{\kappa}{\kappa_l}\right) - 0.254\left(\frac{\kappa}{\kappa_l}\right)^{7/6}\right]\frac{e^{-\kappa^2/\kappa_l^2}}{(\kappa^2 + \kappa_0^2)^{11/6}}\end{aligned}$$

Figure 2.3 shows a plot comparing the normalized PSD models. The shape of the curves indicates that turbulence generally behaves like white noise for small wavenumbers while viscosity damps out the turbulence effects at large wavenumbers. Kolmogorov is the simplest of all the PSDs and has no dependence on spatial scales. It agrees with the other PSDs in the inertial sub-range $1/L_0 \ll \kappa \ll 1/l_0$ where the turbulence can be considered as homogeneous and isotropic. Beyond the inertial sub-range, the Andrews PSD predicts deviation from a power law scaling due to energy accumulation in the inner scale. As shown in the inset of Figure 2.3 there is a subtle rise in its curve (red line) above the others which is referred to as the Hill bump [8]. This PSD most accurately reflects empirical measurements and is often used for modeling turbulence.

To synthesize the turbulence channel conditions for experiments in Chapter 3, 500 random phase screens based on the Andrews PSD were created and arranged into a continuously looping video at a frame rate of 60 Hz. The channel C_n^2 was characterized by capturing a series of camera images of a distorted Gaussian beam and doing a curve fit of the intensity values through its centroid to the gamma-gamma probability density function formula from the scintillation model of Al-Habash [9]. Three different C_n^2 conditions are characterized and plotted in Figure 2.4 along with another parameter called Rytov variance $\sigma_R^2 = 1.23C_n^2\kappa^{7/6}L^{11/6}$ which also measures the strength of turbulence while accounting for the actual beam propagation distance L .

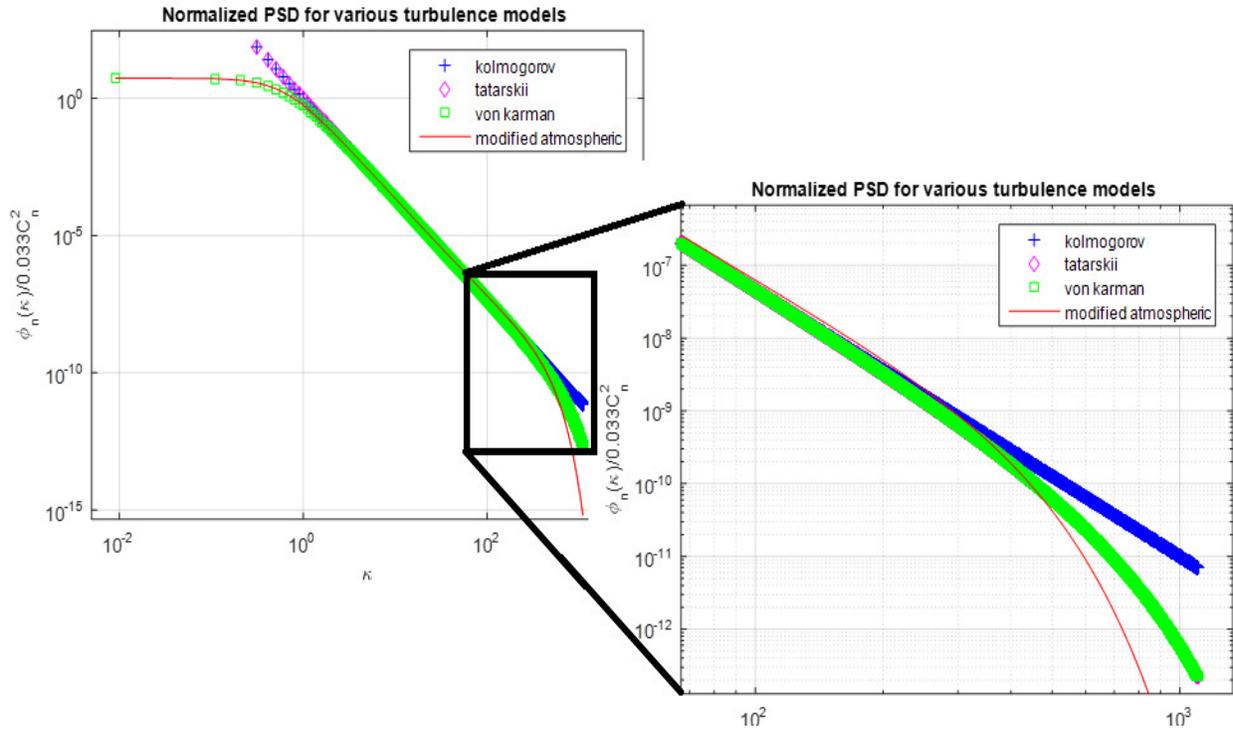


Figure 2.3. Comparison of several PSD models used for atmospheric turbulence modeling.

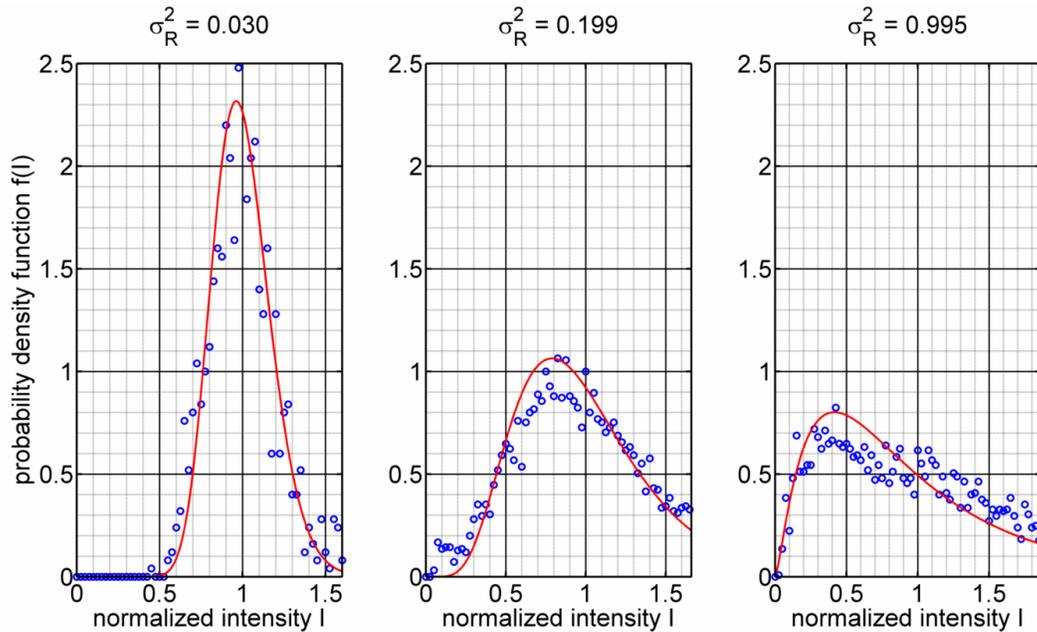


Figure 2.4. Curve fitting to the gamma-gamma probability density function for a 1 km channel resulting in estimated values of $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), 5×10^{-14} (right) along with their corresponding Rytov variance. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

2.3 Using Orbital Angular Momentum Modes for FSO

When laser light carries orbital angular momentum the phase front of each individual mode evolves in a helical-like manner as it propagates. For nonzero order modes, this in effect creates an on-axis singularity which manifests as an intensity null in the center of the beam. A classic paper by Allen et. al. [10] describes laser light with a Laguerre-Gaussian (LG) distribution as an example of modes having well-defined orbital angular momentum. The functional form of the complex electric field of a LG beam, which form solutions to the free-space Helmholtz equation, is expressed as:

$$u(r, \phi, z) = \sqrt{\frac{2p!}{\pi(p + |m|)!}} \frac{1}{w(z)} \left[\frac{r\sqrt{2}}{w(z)} \right]^{|m|} L_p^m \left[\frac{2r^2}{w^2(z)} \right] \exp \left[\frac{-r^2}{w^2(z)} \right] \exp \left[\frac{-ik_0 r^2 z}{2(z^2 + z_R^2)} \right] \exp \left[i(2p + |m| + 1) \tan^{-1} \left(\frac{z}{z_R} \right) \right] \exp(-im\phi)$$

where r is the radial coordinate, ϕ is the azimuthal angle, and z is the propagation distance. The function $L_p^m(\cdot)$ represents the Associated Laguerre polynomial with azimuthal order m and radial order p . Example modes are shown in Figure 2.5. The case of $p = m = 0$ corresponds to the zero-order Gaussian mode. Nonzero values of m represent higher order LG modes with $p = 0$ typically chosen to minimize the space-bandwidth product. The initial beam waist w_0 scales as the square root of the mode order and grows with the propagation distance as $w(z) = w_0 \sqrt{1 + (z/z_R)^2}$, where $z_R = \pi w_0^2 / \lambda$ is the Rayleigh range, λ is the wavelength, and k_0 is the laser wavenumber. The azimuthal phase term $\exp(-im\phi)$ is intrinsically tied to the order of the OAM mode.

Given the fact that mathematically the OAM modes form an infinite set of orthogonal basis functions, the possibility of leveraging that property for use in FSO communications has led to a wide variety of proposed applications in multidimensional spatial modulation and multiplexing [11], [12]. Ideally in a homogeneous medium the vorticity of OAM modes is preserved as they propagate and, as a result their wavefronts remain orthogonal even after undergoing diffraction. However in a FSO channel containing atmospheric turbulence, that orthogonality is no longer preserved because of fading and time-varying refractive index fluctuations that cause intensity scintillations in the beam profiles. This can lead to inter-modal crosstalk as the power inevitably gets transferred from one transmitted mode to its neighboring orders.

An intriguing possibility for FSO links that's been considered for quite some time has been to communicate using Bessel OAM modes through turbulence. Not only do Bessel beams form orthogonal solutions to the free-space Helmholtz equation but they also have the property of

being non-diffracting for extremely long distances and self-regenerating if partially blocked by obstructions along their propagation axis [13]. The functional form of the complex electric field of a Bessel beam is expressed as:

$$u(r, \phi, z) = J_m(k_0[\sin(\alpha)]r)\exp[ik_0[\cos(\alpha)]z]\exp(-im\phi)$$

where r is the radial coordinate, ϕ is the azimuthal angle, and z is the propagation distance. Once again the azimuthal phase term $\exp(-im\phi)$ is intrinsically tied to the order of the OAM mode. The function $J_m(\cdot)$ represents the Bessel function of the first kind of order m . A basic zero order Bessel beam can be generated by a refractive optical element called an axicon. The novelty in the electric field formula comes from the quantity α which is the cone angle of the axicon tip shown in Figure 2.5. Whereas the focusing of a Gaussian beam by an ordinary lens will yield a finite depth of focus given by the confocal parameter, the mechanism of focusing by an axicon involves the constructive interference of an entire angular spectrum of planar wavefronts arriving on-axis within the cone angle. This results in an on-axis beam profile consisting of a central main lobe surrounded by infinitely many rings [14]. As the beam propagates, energy from the rings continually flow towards the central lobe. Because of this effect, Bessel beams in theory can exhibit those special properties mentioned above.

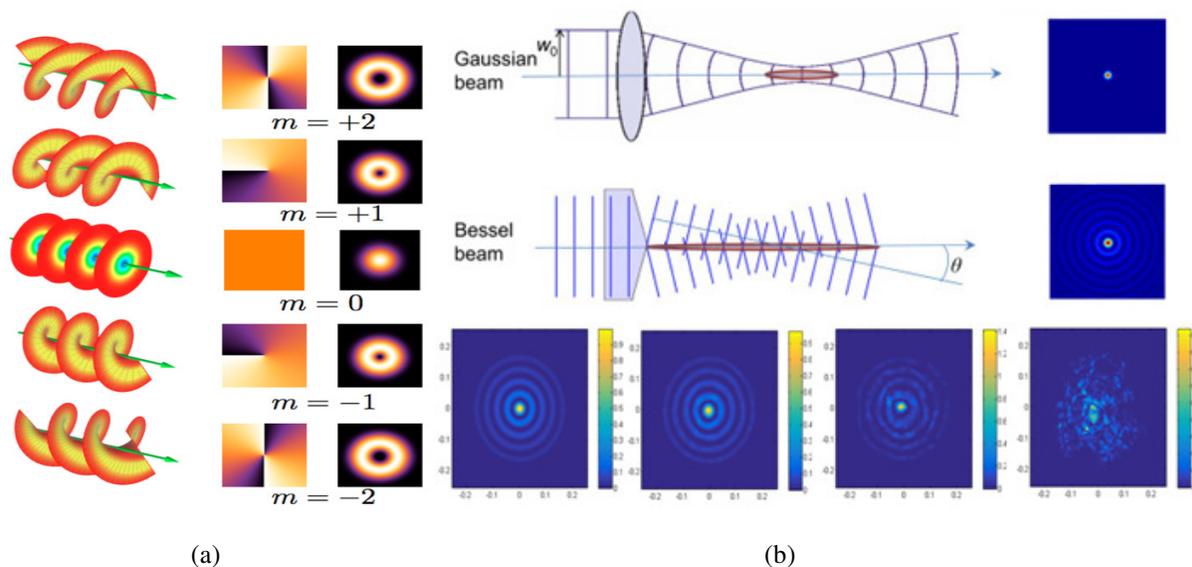


Figure 2.5. (a) Depiction of Laguerre-Gaussian OAM modes from order -2 to order +2 (source: Wikipedia). (b) Top: Comparison of the formation of an ordinary Gaussian beam with a Bessel beam, highlighting the Bessel beam's longer depth of focus (source: [14]). Bottom: Simulated evolution of the zero order Bessel-Gaussian OAM mode undergoing refractive index distortions caused by turbulence of increasing strengths.

However because theoretical Bessel beams contain an infinite number of nearly equal energy rings they have an infinite energy by definition. Thus the physically realizable analogue

to the Bessel beam is the Bessel-Gaussian (BS) beam which has minimal diffraction as it propagates over a finite, but still much longer, depth of focus distance compared to that of an ordinary Gaussian beam. Experimental demonstrations of this promising property being harnessed for use in transmitting data over an FSO channel were reported in [15], [16]. However the robustness of BS beams remains tenuous and very much depends on the nature of the obstructions that the beams encounter. While it's known that these beams can still regenerate when clipped by a discrete point object blocking a small section of their wavefront, simulation studies have indicated that they cannot overcome strong turbulence-induced phase changes that distort their entire profile [17]. This is apparent from the simulated propagation pictures in Figure 2.5. Nonetheless under certain scenarios such as a weak to medium turbulence FSO channel having distance on the order of 1 km, it's possible to create BS beams that can propagate intact. Figure 2.6 shows examples of experimentally generated BS and LG modes being distorted by emulated atmospheric turbulence. The laboratory setup which involves spatial light modulators will be discussed in Chapter 3.

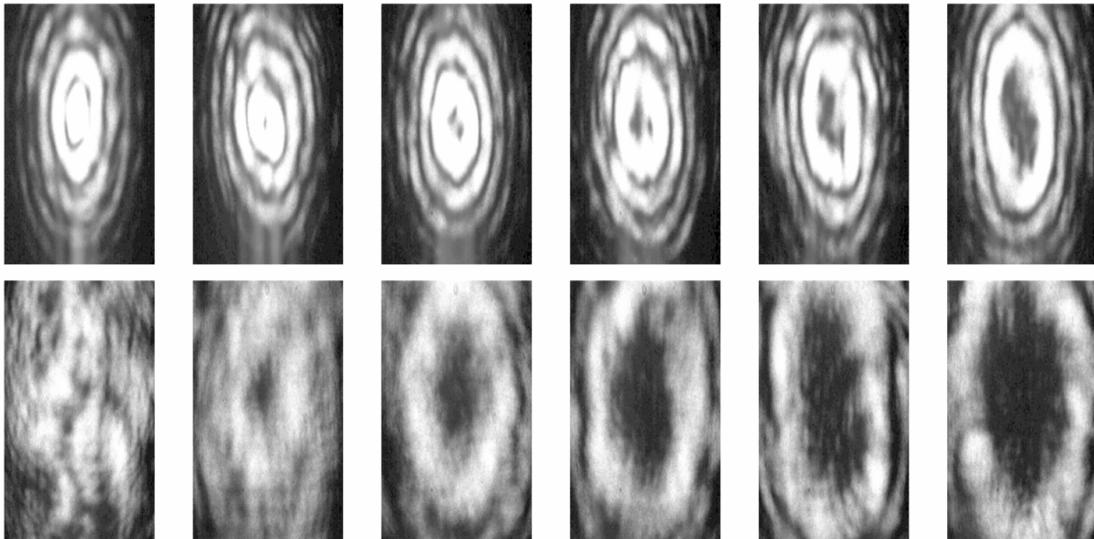


Figure 2.6. Experimentally generated OAM modes from order 0 to order +5 after refractive index distortions caused by turbulence of strength $C_n^2 = 5 \times 10^{-14}$. The top row contains beam profiles for BS modes and the bottom row contains beam profiles for LG modes. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

3 Employing Bessel-Gaussian Beams to Improve Physical-Layer Security in FSO

3.1 Definitions and Beam Propagation Simulations

3.1.1 Secrecy Capacity Formulas

Secrecy capacity is the highest data capacity at which Eve cannot obtain information transmitted from Alice to Bob. In the PLS scenario the quantities used to calculate secrecy capacity are the capacity from Alice to Bob (C_{AB}) and the capacity from Alice to Eve for the boundary cases of Eve being near the transmitter ($C_{AE,Tx}$) and near the receiver ($C_{AE,Rx}$). This in turn gives the two limits of secrecy capacity: transmitter capacity defined as $C_{S,Tx} = C_{AB} - C_{AE,Tx}$ (bits/sec/Hz) and receiver capacity defined as $C_{S,Rx} = C_{AB} - C_{AE,Rx}$ (bits/sec/Hz). Equations (1) through (4) outline the calculation of these limits from beam propagation of individual OAM modes through a turbulence channel. For simplicity it's assumed that Eve's beam-splitter can covertly extract a small fraction (1%) of the transmitted power and has adequately large diameter to collect that power over the entire area of the transmitted beam. The worst-case scenario of Eve having perfect detection efficiency is also assumed and thus the calculations using these formulas result in lower bound values. The notation is such that P_{Tx} is the power transmitted by Alice, P_b is the power received by Bob (γ_b being Bob's SNR), and P_e is the power received by Eve (γ_e being Eve's SNR and r_e being the fraction that's extracted). The total noise power (N) has contributions from both the crosstalk noise and the background noise (N_0). P_{Tx} is chosen to be 20 dB higher than N_0 . The complex electric field of an OAM mode in Cartesian coordinates is represented by $u_n(x,y,z)$ and η_{nm} denotes the channel efficiency values which populate the elements of the $n \times m$ channel crosstalk matrix.

Because the secrecy capacity formula for an individual mode increases only logarithmically it's common to calculate aggregate secrecy capacity tallied over an entire set of modes. This performance metric is used because a practical FSO system would have the capability to spatially multiplex multiple OAM modes for transmission. Following this convention the C_S values from individual beams propagating through the channel are summed to obtain the aggregate C_S . It's also important to note that channel capacity must be a non-negative quantity so C_S is reported only when γ_b is greater than γ_e and is set to 0 otherwise.

$$\eta_{nm} = \langle u_m(x, y, z), u_n(x, y, z) \rangle = \left[\iint u_n(x, y, z) u_m^*(x, y, z) dx dy \right] / P_{Tx}$$

$$P_{Tx} = \langle u_n(x, y, 0), u_n(x, y, 0) \rangle = \iint |u_n(x, y, 0)|^2 dx dy \quad (1)$$

$$N = (1 - r_e) \sum_{n \neq m} (\eta_{nm}^2 P_{Tx}) + N_0$$

$$r_e = \frac{P_e}{P_{Tx}} = .01$$

$$N_0 = \frac{P_{Tx}}{100} \quad (2)$$

$$\gamma_b = \frac{P_b}{N} = \frac{(1 - r_e) P_{Tx} \eta_{mm}^2}{(1 - r_e) \sum_{n \neq m} (\eta_{nm}^2 P_{Tx}) + P_{Tx}/100}$$

$$\gamma_{e,Tx} = \frac{P_e}{N_0} = \frac{r_e P_{Tx}}{P_{Tx}/100} = 100 r_e = 1$$

$$\gamma_{e,Rx} = \frac{P_e}{N} = \frac{r_e P_{Tx} \eta_{mm}^2}{(1 - r_e) \sum_{n \neq m} (\eta_{nm}^2 P_{Tx}) + P_{Tx}/100} \quad (3)$$

$$C_{AB} = \log_2(1 + \gamma_b)$$

$$C_{AE,Tx} = \log_2(1 + \gamma_{e,Tx})$$

$$C_{AE,Rx} = \log_2(1 + \gamma_{e,Rx}) \quad (4)$$

3.1.2 Simulation Parameters

In this paper the FFT split-step beam propagation method [18] is used for FSO simulations. Table 3.1 lists the main simulation parameters. For simulating OAM beam propagation, a square grid with a side length of 512 mm and 1024 pixels is specified. The total beam propagation distance is 1 km and is split into 10 equal steps of 100 m. The initial beam waist is nominally taken to be 50 mm which is a realistic choice for the output of a FSO expanding telescope. But more importantly, at a wavelength of 1550 nm, the resulting Rayleigh range for a Gaussian beam is approximately 5 km and this ensures that the beam stays collimated over the 1 km FSO link. Note that higher order modes for LG beams have diameters that scale in proportion to the square root of the OAM order and higher order modes for BS beams have inner ring diameters which also grow with the order. To model atmospheric turbulence, phase screens were created based on the Andrews modified atmospheric power spectral density with inner and outer scales of 1 mm and 20 m respectively. Their turbulence strength is characterized by the refractive index structure parameter (C_n^2) with values ranging from 10^{-17} to $10^{-13} \text{ m}^{-2/3}$.

Table 3.1. Beam Propagation Simulation Parameters. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

Simulation domain size : Domain length	1024x1024 pixels : 512x512 mm
Total propagation distance : Step Size	1000 m : 100 m
Beam waist : Wavelength	50 mm : 1550 nm
OAM mode : Range of orders	BS and LG : -15 to +15
Turbulence power spectral density	Andrews modified atmospheric
C_n^2 values : inner scale : outer scale	10^{-17} to 10^{-13} : 1 mm : 20 m

3.1.3 Simulation Results

The simulations propagated individual BS and LG orders from -15 to +15 one at a time over a 1 km turbulence channel of varying strengths. The equal channel power paradigm is assumed in which individual modes are launched at their own power levels rather than proportionally attenuated to satisfy a fixed system power constraint. Monte Carlo trials were done for C_n^2 values from the weak to strong turbulence regimes with each value specifically chosen to facilitate the plotting of the C_n^2 points on a semi-logarithmic horizontal scale. Figure 3.1 shows the simulated intensity profiles for several of the OAM modes after traveling through a strong turbulence channel. The complex electric field values at the final step were stored so that the channel crosstalk matrices could be generated by pair-wise computation of overlap integrals between the modal electric fields. Propagation of individual BS and LG orders through vacuum was also performed to serve as the conjugated reference beam for this overlap integral calculation.

Crosstalk matrices are arranged so that each row is designated to a particular transmitted order and every column element along that row contains the value from the overlap integral with the corresponding reference mode. An identity matrix would refer to the ideal case where no channel crosstalk occurs. In the presence of turbulence the wavefront is distorted leading to power leakage from the diagonal cells of the matrix to neighboring cells in the same row. Figure 3.2 contains crosstalk matrices ordered by increasing turbulence strength for several C_n^2 values. A visual inspection of these matrices revealed slightly more power leakage among the LG modes than among the BS modes for C_n^2 values below $10^{-15} \text{ m}^{-2/3}$. Above that value the matrices for both BS and LG modes are mostly dispersed with no obvious structure along the main diagonal. To quantify the modal crosstalk the aggregate secrecy capacity is calculated over the entire set of modes using the information-theoretic security formulas. The secrecy capacities when considering Eve to be near the transmitter and near the receiver are shown in Figure 3.3. Consistent with expectations the aggregate C_S values decrease with increasing turbulence strength. For reference, the maximum possible aggregate secrecy capacity is 175 bits/sec/Hz

when using consecutive orders from -15 to +15 in a perfect channel having no crosstalk regardless of whether Eve is on the transmit or receive sides.

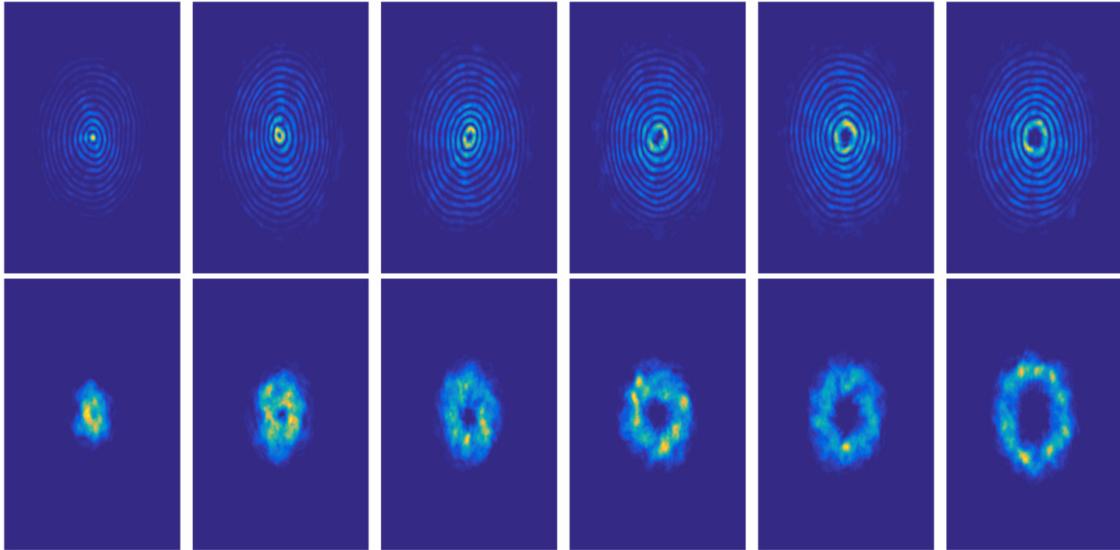


Figure 3.1. Simulated OAM modes from order 0 to order +5 after 1 km of propagation distance through $C_n^2 = 10^{-14}$ turbulence. The top row contains intensity profiles for BS modes and the bottom row contains intensity profiles for LG modes. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

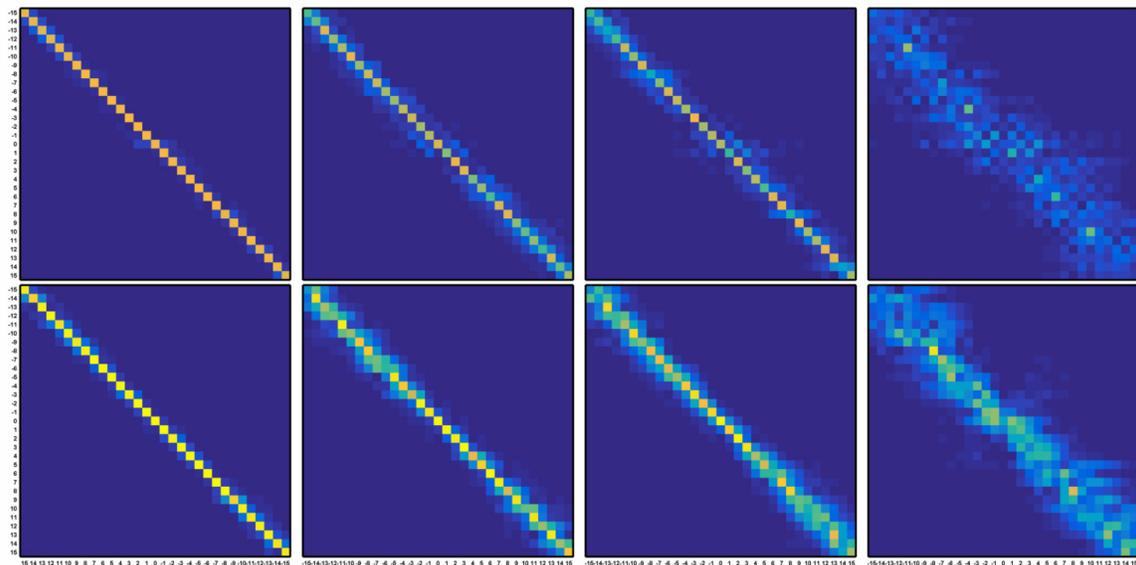


Figure 3.2. Simulation crosstalk matrices for BS modes (top) and LG modes (bottom) for $C_n^2 = 10^{-17}$, 10^{-16} , 1.75×10^{-16} , and 1.75×10^{-15} (from left to right). Transmitted orders are labeled along the rows and the reference orders are labeled along the columns. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

Comparing the data points in the BS and LG curves it's apparent that the C_S values are typically higher by 10 to 30 bits/sec/Hz when using BS beams. This indicates better PLS performance when using BS beams than when using LG beams. However this improvement is mostly negated in strong turbulence when the C_n^2 value is above $10^{-15} \text{ m}^{-2/3}$. Under these channel conditions the capacity already reaches 0 if Eve is located near the transmitter and rapidly approaches 0 bits/sec/Hz if Eve is located near the receiver.

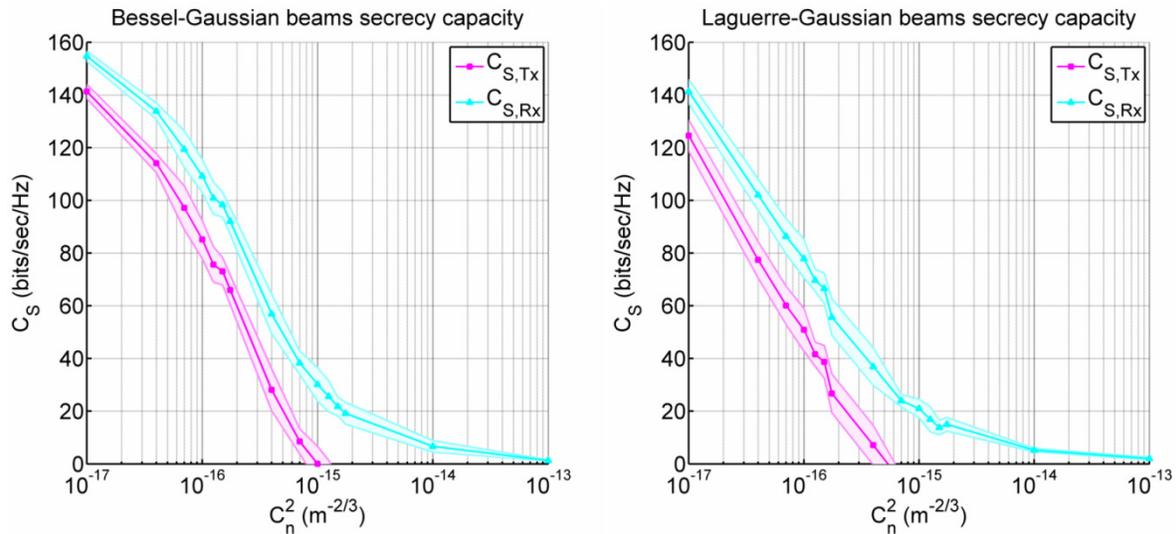


Figure 3.3. Plots of aggregate secrecy capacity calculated from crosstalk matrices over orders -15 to +15 as a function of turbulence strength. The shaded bands surrounding the data points represent error bars over the Monte Carlo runs. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

3.2 Experiments With Spatial Light Modulators

3.2.1 Experimental Setup

To corroborate the improved PLS provided by BS beams over LG beams and to compare their secrecy capacity performance in the laboratory, a tabletop experiment was designed using spatial light modulators (SLM) to generate and detect OAM modes and to emulate a turbulence channel. In order to be realizable on an optical table the diameter of the laser beam and the total propagation distance in the setup had to be at least an order of magnitude smaller than those of the simulations. Also the limited depth of focus over which BS beams could maintain minimal diffraction as well as the fact that LG beams would expand had to be taken into account in the experimental design.

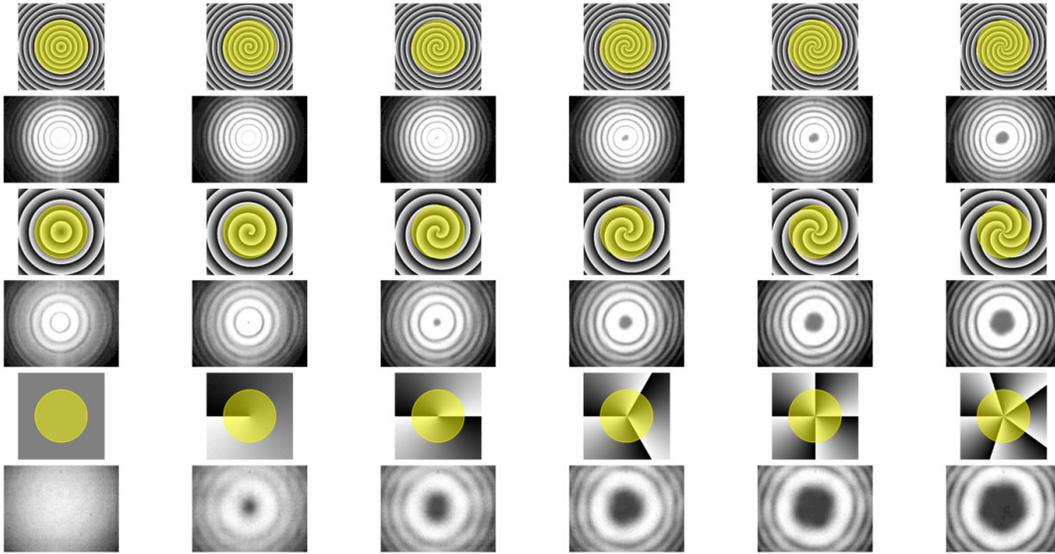


Figure 3.4. OAM modes from order 0 to order +5. Top two rows: Phase pattern and beam profiles for finer resolution BS modes with a period of 64 pixels. Middle two rows: Phase pattern and beam profiles for coarser resolution BS modes with a period of 128 pixels. Bottom two rows: Phase pattern and beam profiles for LG modes.

The transparent yellow circle overlaying each of the phase patterns represents the 5 mm diameter laser beam incident on the SLM chip. All the beam profile images were captured after 600 mm of tabletop propagation distance. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

The SLMs used in the experiment are the Holoeye PLUTO-TELCO-013 reflective phase-only SLMs with 1920 x 1080 pixels (15.36 mm x 8.64 mm active area) and 8 μm pixel pitch. The laser diode source is the AC Photonics LDLS-02 whose output is passed through a polarizer (POL) (Thorlabs LPNIR050-MP2) to establish a linear polarization state which can then be rotated by a half-wave plate (HWP) (Thorlabs WPH10M-1550) into alignment along the SLM display axis. Operating at a wavelength of 1550 nm the SLMs have >80% reflectivity and a maximum diffraction efficiency of 85%. Thus when creating phase patterns for the SLM to generate OAM beams it was unnecessary to make superposition for phase patterns since the undiffracted 0th order was not noticeable and the standard OAM phase patterns could be used directly. For BS modes the generated orders from -5 to +5 are considered and for LG modes, with the radial order set to 0, the generated azimuthal orders from -5 to +5 are considered. LG modes were created by loading a spiral phase pattern onto the SLM with the number of 0 to 2π phase crossings corresponding to the order of the mode. BS modes were created by loading the same spiral phase patterns superimposed with a blazed axicon phase pattern. Examples of the resulting OAM phase patterns are shown in Figure 3.4.

The experiment consisted of two configurations for testing with and without emulated turbulence. Figure 3.5 shows a back-to-back configuration without turbulence to verify the

generation and detection of OAM modes using the Gaussian beam output from the laser (approximately 2.5 mm in diameter). The HWP is used to adjust the polarization incident onto the transmit SLM to produce the best quality OAM mode. Referring to Figure 3.4 the higher order BS modes can be made to have finer or coarser resolution in terms of the size of their central dark spot and the width of their outer rings by changing the periodicity of the spiral phase pattern and adjusting the beam waist accordingly. For a given beam diameter the finer resolution modes will have a shorter depth of focus than their coarser counterparts. Because there is only 400 mm of tabletop propagation distance between transmit and receive SLMs the finer resolution was used. In order to detect OAM modes with the receive SLM the conjugate mode sorting technique [19] was used with a long shallow focusing lens of $f = 400$ mm focusing the light into a Point Grey CMLN-13S2M-CS phosphor-coated CCD camera in the far field. Because the beam reflects from steering mirrors prior to the receive SLM another HWP is needed to re-adjust the slightly degraded polarization. Thumbnails of the camera images arranged in an array resembling that of a crosstalk matrix are shown in Figure 3.6. When there are no turbulence-induced beam distortions the detection using the correct matching mode should result in a focused spot in the far field while the detection using incorrect modes should produce rings or other types of structures with fading intensity as the modes become more mismatched. This expected behavior is indeed shown in Figure 3.6.

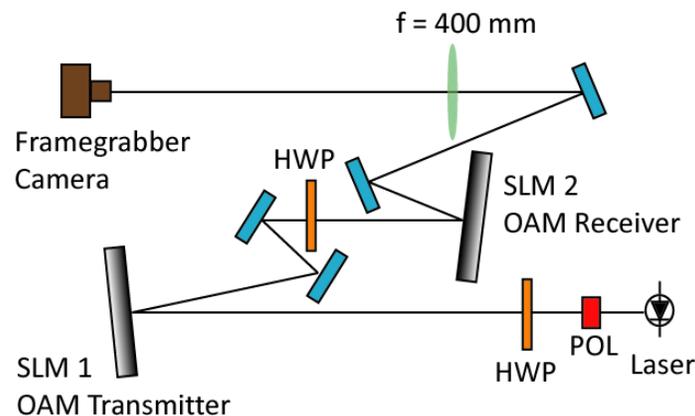


Figure 3.5. Diagram of the back-to-back experimental configuration. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

The diagram of the full experiment in Figure 3.7 shows the incorporation of one additional SLM to emulate a 1 km turbulence channel. Note there is no HWP in front of the turbulence SLM because it only imparts a random phase and is not used to generate structured OAM phase patterns. In order to impart the desired amount of turbulence onto the OAM beam the layout is designed for the beam from the transmit SLM to make a double pass reflection from the

turbulence SLM. Previous experiments have shown that a single reflection from a SLM containing turbulent phase does not produce adequate distortion to the beam and a minimum of two reflections are needed [20]. While this additional reflection from the surface of a SLM results in extra channel attenuation it ultimately does not impact the data analysis. To accommodate this geometry the tabletop distance between transmit and receive SLMs was lengthened to 1600 mm, which is four times longer than in the back-to-back setup. This necessitated the use of the coarser resolution BS modes and a longer depth of focus. The setup was modified so that the original Gaussian beam from the laser would pass through a beam expander to double its diameter to 5 mm. In addition a pinhole spatial filter was also installed to improve the wavefront quality before it reached the transmit SLM.

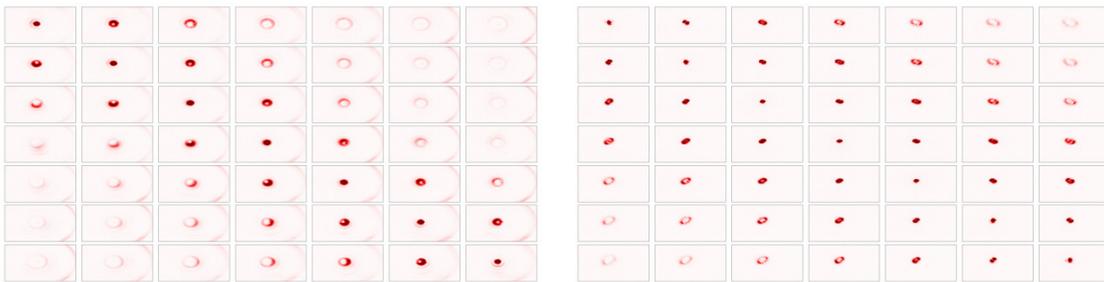


Figure 3.6. Conjugate mode detected spots for BS (left) and LG (right) modes from order -3 to order +3 in the back-to-back experiment. The thumbnails are not explicitly labeled but the transmitted orders are arranged along the rows and the reference orders along the columns following Figure 3.2. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

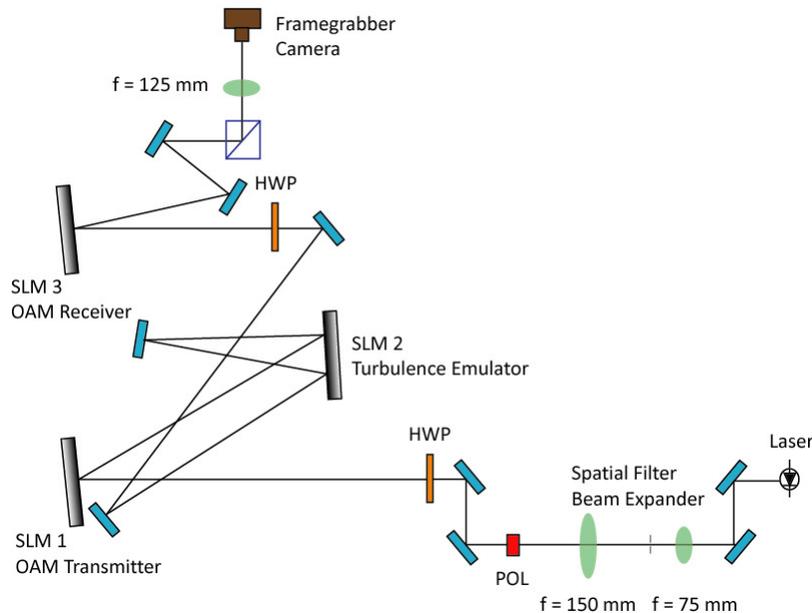


Figure 3.7. Diagram of the full experimental configuration including turbulence emulator. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

3.2.2 Experimental Results

Once again conjugate mode sorting was done albeit with a shorter $f = 125$ mm lens focusing the light into the camera. The results are compiled in Figure 3.8 for BS and Figure 3.9 for LG mode detection of orders -5 to +5 for $C_n^2 = 10^{-14} \text{ m}^{-2/3}$ turbulence. As the turbulence movies looped in real-time the far field footprints warped and flickered on the camera due to the beam intensity scintillation. Because of this the data acquisition had to involve collecting a 100 frame sequence of images for each entry of the crosstalk matrix and integrating the frames. A visual survey of the BS matrix showed that the beam footprints on the diagonal entries are more intense compared to their neighbors with the color fading significantly towards the far off-diagonals while those in the LG matrix are less intense compared to their neighbors and have less fading towards the far off-diagonals. In each of the thumbnails a blue circle is overlaid on the integrated far field footprint. The location of the circle is centered on the maximum pixel value of each diagonal thumbnail (which corresponds to the correct matching mode detection) and copies are then stamped across the rest of the row. Doing this is meant to mimic the aperture of a hypothetical fiber coupling stage which focuses the light into a single mode fiber. The flickering of the camera image would then be analogous to misalignment perturbations into the fiber coupling lens which causes fluctuations in the received power during data transmission over that particular spatial channel. Therefore summing over the pixel values within the blue circles leads to a qualitative estimate of the channel crosstalk based on power distribution.

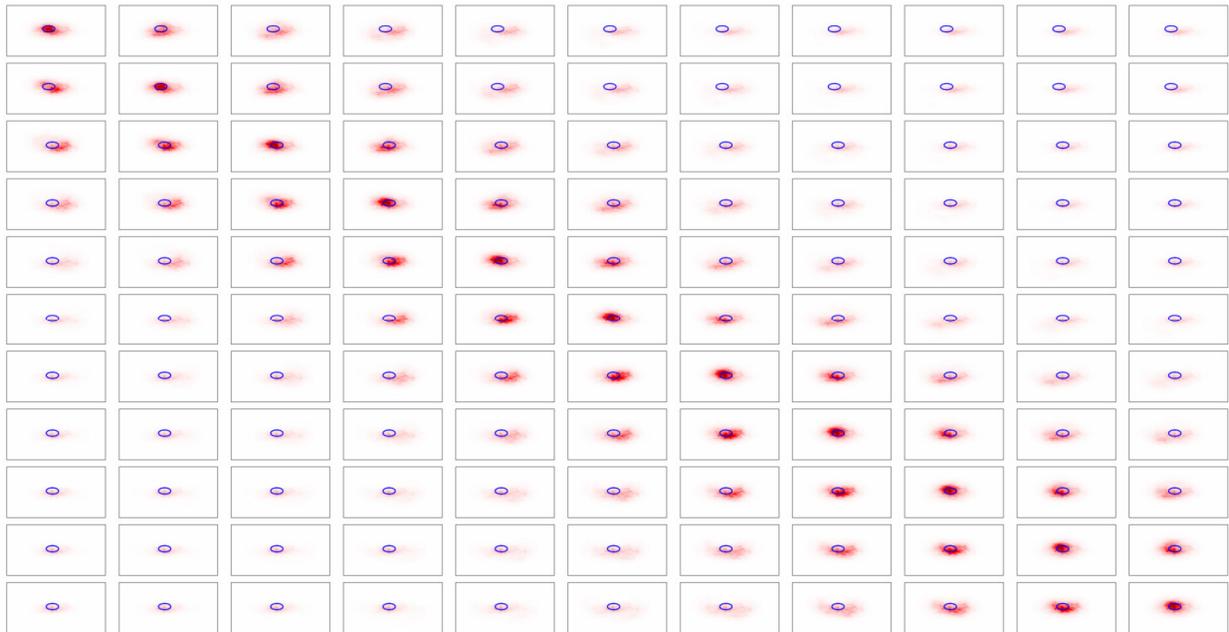


Figure 3.8. Conjugate mode detected spots for BS modes from order -5 to order +5 for $C_n^2 = 5 \times 10^{-14}$ in the full experiment. The thumbnails are not explicitly labeled but the transmitted orders are arranged along the rows and the

reference orders along the columns following Figure 3.2. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

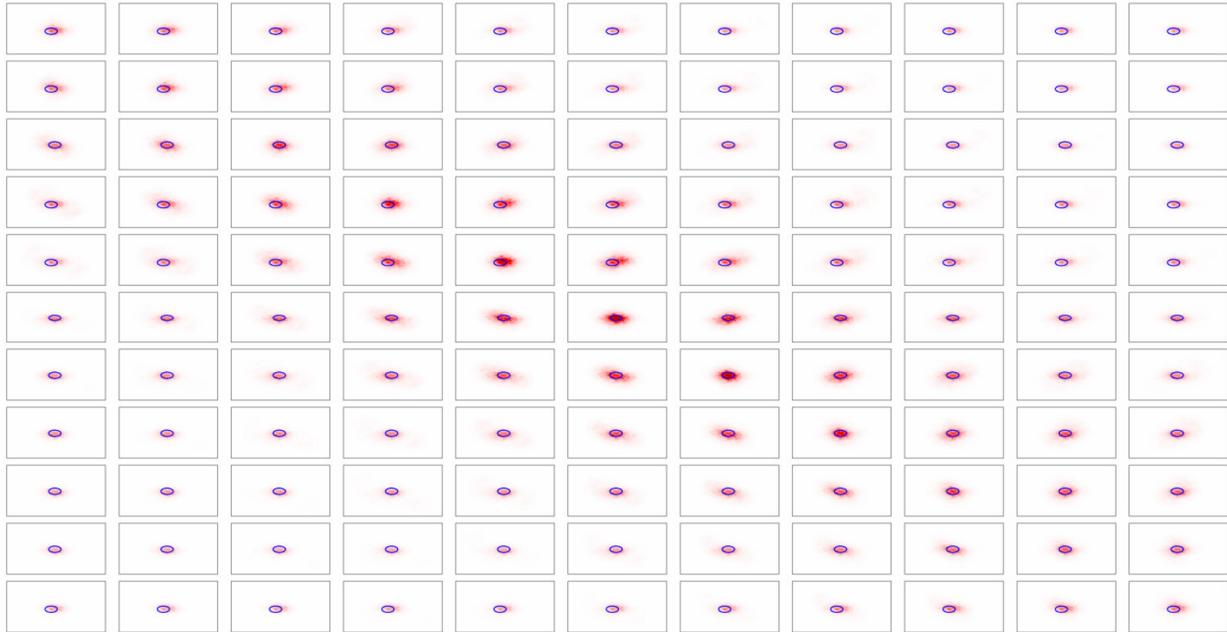


Figure 3.9. Conjugate mode detected spots for LG modes from order -5 to order +5 for $C_n^2 = 5 \times 10^{-14}$ in the full experiment. The thumbnails are not explicitly labeled but the transmitted orders are arranged along the rows and the reference orders along the columns following Figure 3.2. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

Table 3.2 shows the secrecy capacity values calculated from the crosstalk matrices in Figure 3.10 for the three turbulence conditions generated in the experiment. For reference, the maximum possible aggregate secrecy capacity is 62 bits/sec/Hz when using consecutive orders from -5 to +5 in a perfect channel having no crosstalk regardless of whether Eve is on the transmit or receive sides. The values in the table show that the BS modes consistently yielded a relative increase over their LG counterparts by roughly 10 bits/sec/Hz and thus the experimental results corroborate the conclusion from the simulations that using BS beams improves the PLS performance.

One caveat in regards to the turbulence strengths measured in the experiment is that it's challenging to accurately generate very weak turbulence conditions using the SLM due to its finite phase resolution. On the other hand, although the phase screens were nominally designed to produce strong turbulence, the fact that the tabletop propagation distance is at least an order of magnitude smaller than the 1 km channel has reduced the turbulence strength as well. In this case the secrecy capacity values reported in Table 3.2 most likely represent that of an effectively weaker turbulence channel which might explain why their values are higher than expected. Furthermore while it wasn't possible to generate a wider range of turbulence conditions with this

setup, there is evidence that the secrecy capacity values can extrapolate in a similar manner as the simulation results.

Table 3.2. Aggregate Secrecy Capacity Values From Experimental Crosstalk Matrices Over Orders -5 to +5. Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

Turbulence Strength ($m^{-2/3}$)	BS mode (bits/sec/Hz)	LG mode (bits/sec/Hz)
$C_n^2 = 1.5 \times 10^{-15}$	$C_{S,Tx} = 11.1$, $C_{S,Rx} = 21.6$	$C_{S,Tx} = 3.3$, $C_{S,Rx} = 14.0$
$C_n^2 = 10^{-14}$	$C_{S,Tx} = 6.2$, $C_{S,Rx} = 16.9$	$C_{S,Tx} = 0.0$, $C_{S,Rx} = 5.9$
$C_n^2 = 5 \times 10^{-14}$	$C_{S,Tx} = 2.7$, $C_{S,Rx} = 13.5$	$C_{S,Tx} = 0.0$, $C_{S,Rx} = 4.4$

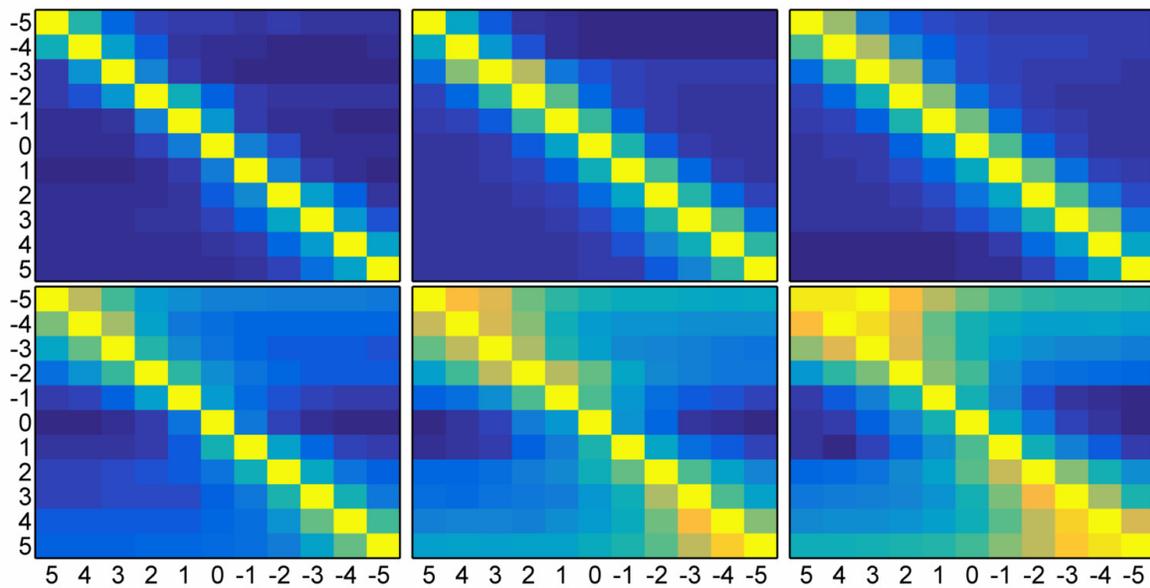


Figure 3.10. Experimental crosstalk matrices of BS beams (top) and LG beams (bottom) for $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), and 5×10^{-14} (right). Reprinted with permission from T.-L. Wang, J. A. Gariano, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 5, Sep. 2018, Art. no. 7907113. Copyright 2018 IEEE.

4 Physical-Layer Security of a Binary Data Sequence Transmitted with Bessel-Gaussian Beams

4.1 Laboratory Emulation of an Optical Wiretap Channel

To establish the experiment for transmitting data with BS beams the setup involving Holoeye PLUTO-TELCO-013 reflective phase-only spatial light modulators (SLM) used in Chapter 3 was moved and re-constructed in a different laboratory area to be in close proximity to the data transmitter and receiver hardware. The diagram of the new setup which emulates the optical wiretap channel on a tabletop is shown in Figure 4.1.

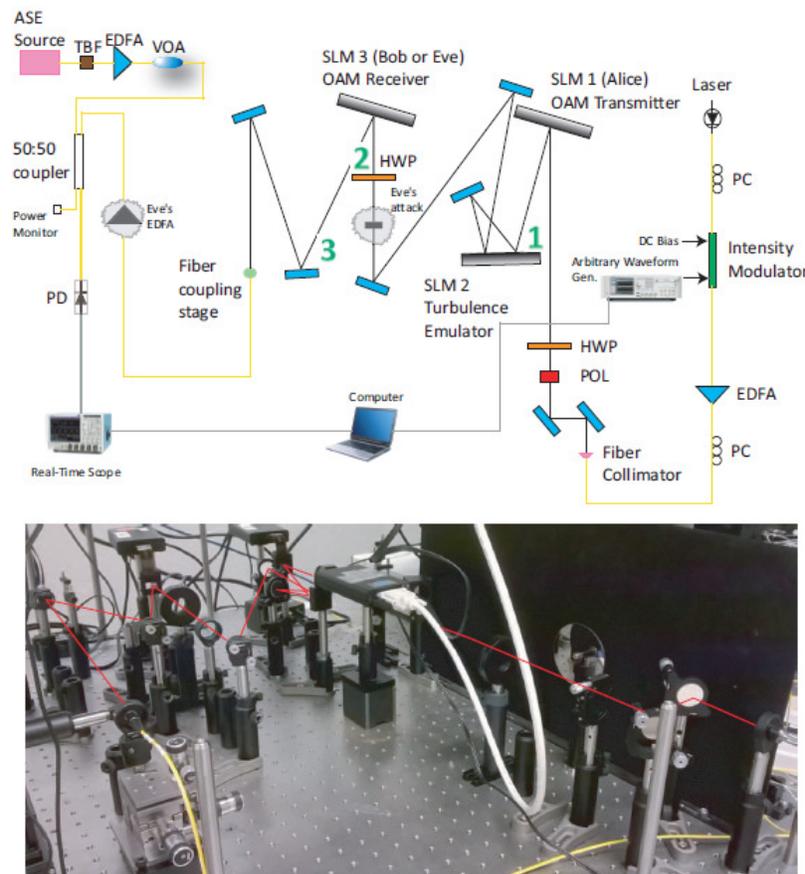


Figure 4.1. Diagram of the experimental setup emulating the optical wiretap channel (top). The noise loading stage consisting of ASE source, TBF, EDFA, and VOA is drawn on the top left corner of the diagram. The photograph on the bottom shows the free space portion of the setup. The red line traces the path of the laser beam through the FSO channel. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE.

The laser used for data transmission comes from a single channel of the Pure Photonics PPLA laser array and has center wavelength of 1550 nm with a narrow linewidth of 10 kHz. The output light is initially guided inside Corning SMF-28 optical fiber and enters a JDSU OC-192

intensity modulator that is DC biased at its quadrature point. A pseudo-random binary sequence (PRBS) is then loaded onto a Tektronix AWG70002A arbitrary waveform generator which drives the RF input port of the intensity modulator to impose the on-off-keying (OOK) format onto the laser beam. The modulated laser signal is then amplified by an erbium-doped fiber amplifier (EDFA) to approximately 32 mW average power. Polarization controllers (PC) are adjusted before and after to maximize the laser power. The light beam is then coupled out to free space as a 3 mm diameter beam by a fiber collimator. Due to table space limitations no spatial filtering or beam expansion was done. The FSO portion of the setup is almost identical to the setup in Chapter 3 except that information-carrying beams are now encoded onto OAM modes after reflecting from Alice's SLM. After the receive SLM performs conjugate mode sorting [19], the beam is aligned to a $f = 10$ mm focusing lens which couples it into another SMF-28 optical fiber. In order to create the BER curves, a range of optical signal-to-noise ratio (OSNR) levels had to be generated. This was achieved by fixing the signal power and using a noise loading stage consisting of a broadband amplified spontaneous emission (ASE) light source whose output is passed through a 1550 nm tunable bandpass filter (TBF) and finally amplified by an EDFA [21]. The variation in the noise level that's added to the signal is controlled by the JDSU HA9 variable optical attenuator (VOA). The VOA can progressively attenuate the noise power such that higher attenuation corresponds to a higher OSNR. The signal and noise beams are then combined inside a 2x2 50:50 fiber coupler with one output going to an Optilab PR-23-M photodetector (PD) and the other output being used for power monitoring. The PD is connected to a Tektronix DPO71604B real-time sampling oscilloscope having 16 GHz analog bandwidth and a sampling rate of 50 GS/s which is fast enough to acquire the detected signal for post-processing by a symbol recovery algorithm. Both the arbitrary waveform generator and real-time scope are connected to a computer running a Python script which coordinates a continuously repeating transmission of the OOK modulated codeword of length 38000 bits at a data rate of 12.5 Gbps. The Python script also calculates electrical SNR from the variance of the recovered symbol amplitudes and this quantity serves as a common reference when selecting the VOA noise attenuation to apply to Bob's and Eve's receivers.

With regards to emulating Eve's attack on the FSO channel we originally considered placing a commercially available 92:8 pellicle beam-splitter (Thorlabs BP108) in front of Bob's receive SLM so that 8% of the light could be re-directed to an additional Eve SLM. However, it was determined that attempting to go that route would cause complications in the alignment and increase the difficulty of the experiment, and needless to say that 8% is beyond Eve's extraction capability. Thus in lieu of a beam-splitter, an absorptive neutral density filter (Thorlabs NENIR20A-C) that causes 20 dB of attenuation was inserted directly into the beam path in front

of Bob's receive SLM. Doing this served the dual purpose of attenuating the laser down to 1% of its original power while in effect converting Bob's SLM into Eve's SLM. While the tradeoff came from having to perform each data collection twice, we could argue that this actually emulates the worst-case attack by Eve since 1% of entire beam footprint can be extracted without the need for further alignment.

Initially the average laser power is 32 mW but that value drops after the beam exits into free space and experiences losses due to the polarizer (POL), the half wave plates (HWP), the steering mirrors, and a total of four bounces from SLM surfaces each with 80% reflectivity. Using an integrating power meter to measure the power in the free space beam after the receive SLM gave readings between 1 mW to 4 mW. Therefore, Bob's received signal power is on the order of milliwatts whereas Eve's signal power is on the order of tens of microwatts. Furthermore, this power is coupled into the optical fiber with less than 100% coupling efficiency. Apparently, Eve's signal would be too weak to retain any part of the transmitted PRBS, even when no noise loading is done by the VOA, and as a result Eve's BER curve would simply be a horizontal line at 0.5. Thus, in order to create a meaningful BER curve it was necessary to equip Eve with a constant 20 dB gain EDFA to boost the captured signal. Note that Eve inevitably incurs further SNR degradation from the additional spontaneous emission noise created during the EDFA amplification process.

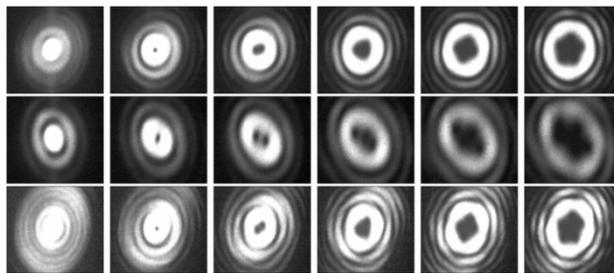


Figure 4.2. Generated BS modes from order 0 to order +5 (from left to right) when no turbulence is applied. The top row shows beam profiles taken at checkpoint 1 and the middle row shows their evolved propagation at checkpoint 2. The bottom row shows beam profiles taken at checkpoint 3 when only SLM 3 contains the BS mode phase pattern and SLMs 1 and 2 do not. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE.

BS modes of orders 0 to +5 were generated similar to those in Chapter 3 by loading spiral phase patterns superimposed on a blazed axicon pattern (with period of 160 pixels) onto the Alice SLM. Because the Bob or Eve SLM performs conjugate mode sorting to receive the OAM encoded data it was necessary to check the evolution the beam in the channel and inspect its structure before conducting the experiment. This was done by positioning an infrared camera to image the beam at three different checkpoints labeled 1, 2, and 3 in Figure 4.1. The captured beam profiles are shown in Figure 4.2, where checkpoint 1 images correspond to the beam made

from SLM 1 and checkpoint 2 images correspond to the propagated checkpoint 1 beams just before arriving at SLM 3. Note the rotation of the spiral phase can change direction depending on whether the beam reflects from an even or odd number of optical surfaces in the beam path. Checkpoint 3 images were taken as a sanity check to verify that a Gaussian beam passing by SLMs 1 and 2 (with no phase pattern loaded onto them) could produce BS modes from SLM 3 that are similar to the modes from SLM 1. This ensures that when conjugate mode sorting is done at SLM 3 using phase patterns of the opposite sign the beams associated with those patterns would be similar in size and structure to the arriving beam.

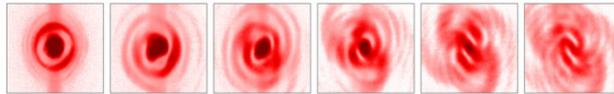


Figure 4.3. Near-field conjugate mode-sorted beam footprints for transmitted BS modes of order 0 to order +5 (from left to right). Visual inspection showed that above order +2 the coupling of the data-carrying beam into the optical fiber would be inefficient. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, *IEEE Phot. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE.

Because it was necessary to re-align the beam going to SLM 3 for each order that was transmitted, images of the near-field profiles after SLM 3 were collected to check the alignment accuracy. These are shown in Figure 4.3. For BS modes of order 0, +1, and +2 the near-field shows a prominent central lobe whereas for orders +3, +4, and +5 more of the power is distributed away from the central region. This indicates that focusing with a fiber coupling lens would be inefficient if portions of the beam are outside the acceptance angle of the fiber and the mismatch with the numerical aperture causes coupling loss and undesired spatial filtering of the signal. Our maximum achieved coupling efficiency was 74%, 66%, and 54% for orders 0, +1, and +2 respectively. Clearly the higher the order, the harder it is to generate BS modes of pristine quality for carrying data, not to mention the more stringent alignment requirements. Thus, the experiment only transmitted BS modes of order 0, +1, and +2 and a LG mode of order 0 (Gaussian) for comparison purposes.

Although only a few BS modes were transmitted in the experiment, we were able to generate a reasonable number of BER curves as shown in Figure 4.4 to demonstrate that Bob's receiver performance consistently surpasses that of Eve under the same refractive index structure parameter (C_n^2) conditions used in Chapter 3 and verify that Eve's channel degradations are indeed more severe than Bob's. Also, the received power measured by Bob and Eve fluctuate with the turbulence in the FSO channel and those fluctuations directly affect the calculated BER values. Because of this the data markers that are plotted represent an average over Monte Carlo runs. The higher the C_n^2 , the larger the magnitude of the power fluctuations which could be observed on the power monitor. For that reason, we also plot a dashed line curve fit along with

every set of data points to indicate the overall trend of each BER curve. Furthermore there is visual evidence that Eve's BER curve could possibly be trending towards an asymptotic error floor although Eve is equipped with an EDFA, which is promising for secure communications.

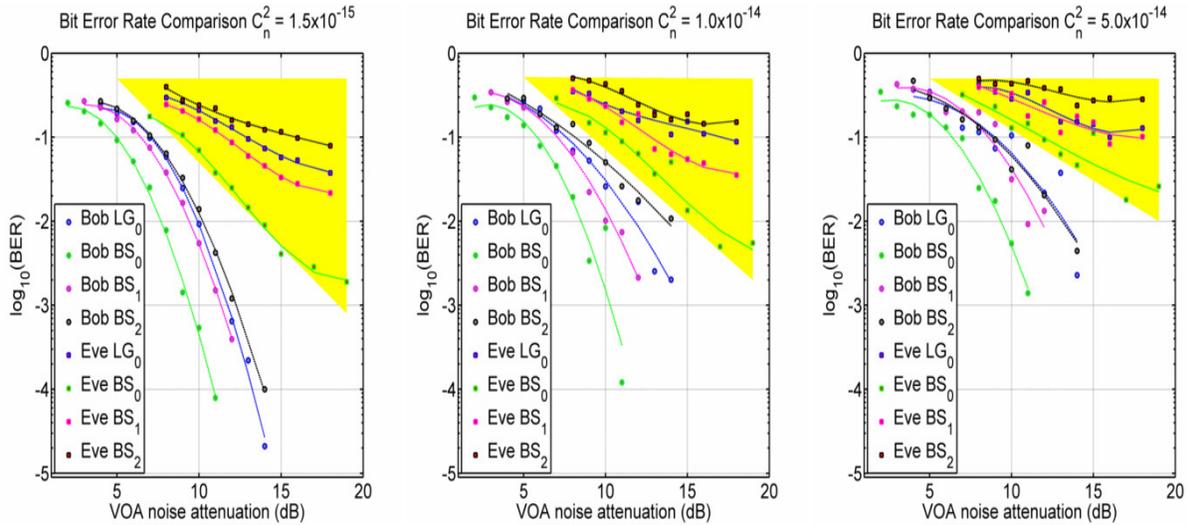


Figure 4.4. BER curves of $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), 5×10^{-14} (right). Bob's data points are shown in gray-filled circles and Eve's data points are shown in red-filled squares. Every set of data points is plotted with a dashed line curve fit to indicate the overall trend. In each plot a yellow triangular region upper bounded by 0.5 highlights Eve's BER curves to distinguish them from Bob's BER curves. Reprinted with permission from T.-L. Wang, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE.

To help quantify the positive secrecy capacity that Bob achieves over Eve, it was possible to compute the $C_{S,Rx}$ indirectly from the difference in performance between their BER curves. We did this by first obtaining estimates of Bob's and Eve's OSNR values using formulas in [22] that enabled a mapping between OSNR and BER. We inverted the formula for OOK bit error rate: $BER = \frac{1}{2} \operatorname{erfc}\left(\frac{Q}{\sqrt{2}}\right)$ to obtain the Q factor, which directly relates to OSNR. Then we

estimated the OSNR values by inverting the formula $Q \approx \sqrt{\frac{\text{OSNR} B_{op}}{2 \Delta f}}$ where an effective optical bandwidth B_{op} of 12.5 GHz at 1550 nm was used and the signal bandwidth Δf was taken to be 75% of the data rate. Finally the OSNR values were substituted into the $C_{S,Rx}$ formula listed in Chapter 2. The calculated $C_{S,Rx}$ values are visualized as bar charts in Figure 4.5. The individual bars are positioned only where there are common data points in between the two curves. Note that the charts just span the range of VOA attenuation levels over which Bob's and Eve's BER curves overlap, in this case between 7 dB and 14 dB of VOA noise attenuation. The calculations of $C_{S,Rx}$ yield values between 1 to 3 bits/sec/Hz for individual mode orders (LG₀, BS₀, BS₁, BS₂). We emphasize that focusing on the order of magnitude of the $C_{S,Rx}$ is more important than comparing the values among the modes since all of their values can fluctuate with the turbulence

strength. In addition, the secrecy capacity of individual BS modes can be aggregated by OAM multiplexing to obtain a total capacity, which exceeds that of the LG mode (which would remain constant on the order of 1 bits/sec/Hz). As reported in the previous experiment, which used crosstalk matrix calculations to compute secrecy capacity, aggregate $C_{S,Rx}$ values of 21.6, 16.9, and 13.5 bits/sec/Hz were reported after propagating BS modes through turbulence with C_n^2 of 1.5×10^{-15} , 10^{-14} , and $5 \times 10^{-14} \text{ m}^{-2/3}$ respectively. Since those aggregate values were obtained by summing over a total of eleven BS orders (from -5 to +5), simple division provides a rough per-order estimate of 1.2 to 2 bits/sec/Hz which is consistent with the measurements in this experiment.

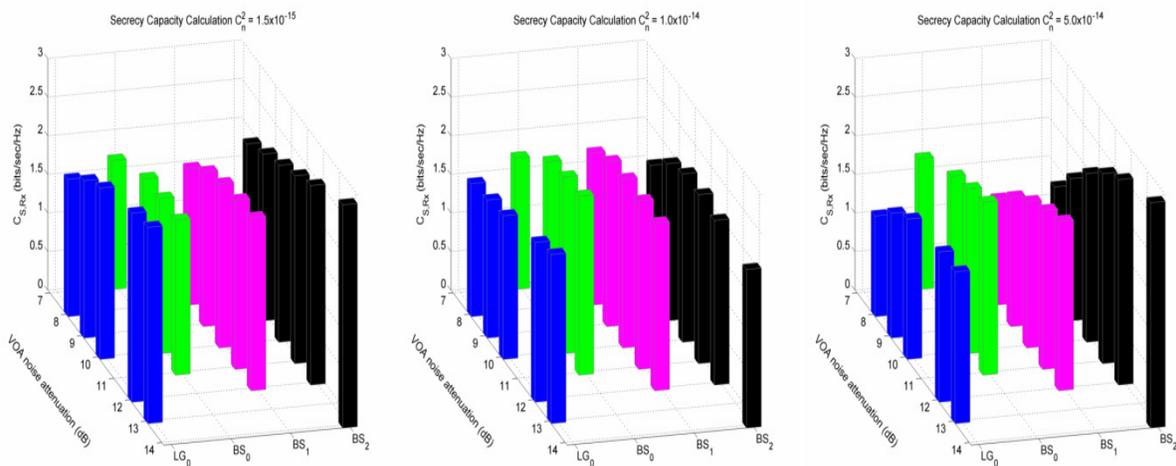


Figure 4.5. Secrecy capacity values computed from the difference between the overlap regions of Bob's and Eve's measured BER curves for $C_n^2 = 1.5 \times 10^{-15}$ (left), 10^{-14} (middle), 5×10^{-14} (right). Reprinted with permission from T.-L. Wang, I. B. Djordjevic, IEEE Phot. J., vol. 10, no. 6, Dec. 2018, Art. no. 7908611. Copyright 2018 IEEE.

4.2 Discussion of Operational Aspects

The results from this experimental demonstration of an optical wiretap channel scenario are fairly intuitive from the standpoint of PLS. Under the worst case scenario, when Eve's receive SLM has the exact same alignment accuracy as Bob's and Eve employs an EDFA to boost the signal level, the fact that Bob's BER performance is still superior to Eve's suggests that secure communication of messages is possible to a certain degree even though no secret key was used. However, all parties (Alice, Bob, and more so Eve) need to address the technical and operational difficulties that come with transmitting and receiving OAM encoded information. The security advantage of using OAM modes was studied in [23] in which physical factors pertaining to misalignment were emphasized. The most critical aspect is to ensure that the intended receiver is positioned on the direct line of sight to the transmitter without any obstructions present along the

beam path. Any lateral misalignment will effectively reduce the aperture size of the receiver and any angular misalignment will create additional background inter-modal crosstalk on top of the turbulence-induced crosstalk. Crosstalk leads to imperfect conjugate mode sorting, loss of information, and further degrades the reliability of the transmission. In this experiment, we dealt with these same alignment issues and this restricted us to transmitting only a few BS orders. Even if Eve's beam-splitter could intercept the beam perfectly on-axis, and were adequately large enough to split off power from the entire beam profile, the alignment issues mentioned in [23] would still be challenging to overcome and in conjunction with the degraded channel conditions would result in further data corruption.

SLMs in a laboratory setup are indeed useful for proof-of-principle demonstrations with OAM modes for FSO. However their sensitivity to misalignment, polarization mismatch, and finite pixel size will yield imperfect OAM phase patterns that are not precisely orthogonal to one another. Development of optical technology to optimize the BS beam quality to achieve better visibility and contrast will undoubtedly help to improve system performance. Precision fabrication of integrated diffractive optics such as phase plates [24] can provide a more practical alternative to SLMs. Techniques to create higher-order BS beams should also be leveraged. These include illuminating a refractive optic such as an axicon with Gaussian or LG beams [25] and illuminating a ring-slit aperture with a beam containing azimuthally varying phase to generate a superposition of higher order BS modes [26]. If the system is designed to transmit a superposition of modes, a spatial multiplexing configuration using non-consecutive modes can minimize the crosstalk and maintain the secrecy capacity advantage [5]. Finally, adaptive optics and algorithms can also be used to mitigate crosstalk by correcting the wavefront of OAM beams [27].

Another aspect is the ongoing debate regarding whether BS beams can be non-diffracting and resilient to turbulence over a finite distance [28] and whether or not they are the most optimal set of orthogonal OAM modes to use [29]. In this thesis we inferred that BS modes are more resilient to turbulence than LG modes based on the modest improvement in positive secrecy capacity that they provided and those results influenced the exclusive use of BS beams in this work. Nonetheless the insight provided by [28], [29] will have to be leveraged for any secure FSO system design considerations.

It's also worth mentioning that the secrecy capacity formula has an implicit relationship with the reliability of the data transmission. Referring to the BER curves measured by Bob's SLM the bit error rate performance can be further improved if forward error correction schemes are employed [30], [31]. Indeed, progress has been made on devising error correction techniques specifically for physical-layer security purposes [32]. Conversely, the BER curves measured by

Eve's SLM are beyond the regime in which forward error correction can be applied and therefore Eve's bit errors cannot be reduced.

Finally, the ultimate goal of any secure communication system is to have a secure key rate that approaches the channel capacity. Obviously if Eve's channel is degraded to the point where Eve only receives noise the secure key rate is limited only by the Shannon capacity itself. In this experiment, an uncoded OOK PRBS was used for a proof-of-concept demonstration but it's known that OOK modulation does not reach the Shannon capacity and cannot provide the maximum possible secure key rate. More sophisticated coherent modulation schemes involving an optimal signal constellation design [33] could in principle be used for future demonstrations.

5 Conclusion

In this thesis we studied how the transmission of Bessel-Gaussian beams can increase the positive secrecy capacity and be used to exploit the turbulent conditions of an optical channel to counter beam-splitting attacks by an eavesdropper. Using computer simulations and experiments with spatial light modulators, we demonstrated that BS beams can indeed provide higher secrecy capacities over corresponding LG counterparts in the weak to medium turbulence regimes because of their higher resiliency to turbulence effects. By propagating several orders of BS and LG modes through atmospheric turbulence and generating crosstalk matrices from those results, an increase in secrecy capacity of 10 to 30 bits/sec/Hz was calculated. Thus we agree that spatial multiplexing of OAM modes can conceivably achieve aggregate secrecy levels beyond that provided by a single Gaussian mode. Furthermore, both simulation and experimental results have shown that aggregate $C_{S,Rx}$ values are still positive even after $C_{S,Tx}$ values have reached zero in the strong turbulence regime. Whether or not a positive secrecy capacity can be maintained is an indicator of situations under which physical-layer security is either preserved or compromised.

We devised a data transmission experiment which emulated an optical wiretap channel to study how Wyner's wiretap channel concept could be extended to FSO channels. Again we found that it is possible to exploit the noisy and degraded channel conditions to achieve physical-layer security even when Alice and Bob do not use a shared key for communications. We also generated BER curves for Bob's and Eve's receivers to show the security advantage enjoyed by Bob even if Eve is equipped with an EDFA to boost the extracted signal and has access to a real-time sampling oscilloscope for post-processing. There's also indication that Eve's BER curves will approach an error floor which will limit Eve's ability to extract information at higher OSNR values. Further research on optimizing the quality of Bessel-Gaussian beams and addressing alignment issues can help to realize a practical system for more secure communications.

Finally it's necessary to point out that this approach to physical-layer security does not guarantee unconditional security and that in the long run a secret key agreement strategy may have a better chance of obtaining higher secure key rates. Specifically, the implementation of quantum key distribution protocols along with information reconciliation and privacy amplification steps can theoretically achieve unconditional security. However, that study is beyond the scope of this thesis.

References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949.
- [2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
- [3] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19-26, Jan. 2017.
- [4] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photonics Journal*, vol. 7, no. 2, Apr. 2015, Art. no. 7901014.
- [5] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7901110.
- [6] J. A. Anguita, M. A. Neifeld, and B. V. Vasic, "Turbulence-induced channel crosstalk in an orbital angular momentum-multiplexed free-space optical link," *Appl. Opt.*, vol. 47, no. 13, pp. 2414-2429, May 2008.
- [7] L. C. Andrews, *Field Guide to Atmospheric Optics*. Bellingham, WA, USA: SPIE Press, 2004.
- [8] L. C. Andrews, S. Vester, and C. E. Richardson, "Analytic Expressions for the Wave Structure Function Based on a Bump Spectral Model for Refractive Index Fluctuations," *J. Mod. Opt.*, vol. 40, no. 5, pp. 931-938, May 1993.
- [9] M. A. Al-Habash, L. C. Andrews, and R. L. Phillips, "Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media," *Opt. Eng.*, vol. 40, no. 8, pp. 1554-1562, Aug. 2001.
- [10] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, "Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes," *Phys. Rev. A.*, 45, 8185, Jun. 1992.
- [11] I. B. Djordjevic, "Oam-based hybrid free-space optical-terahertz multidimensional coded modulation and physical-layer security," *IEEE Photon. J.*, vol. 9, no. 4, Aug. 2017, Art. no. 7905812.
- [12] J. A. Anguita, J. Herreros, and I. B. Djordjevic, "Coherent multimode oam superpositions for multidimensional modulation," *IEEE Photon. J.*, vol. 6, no. 2, Apr. 2014, Art. no. 7900811.

- [13] D. McGloin and K. Dholakia, "Bessel beams: Diffraction in a new light," *Contemporary Phys.*, vol. 46, no. 1, pp. 15-28, Jan./Feb. 2005.
- [14] F. Courvoisier, R. Stoian, and A. Couairon, "Ultrafast laser micro- and nano-processing with nondiffracting and curved beams," *Optics & Laser Tech.*, vol. 80, pp. 125-137, Jun. 2016.
- [15] S. Chen et al., "Demonstration of 20-gbit/s high-speed bessel beam encoding/decoding link with adaptive turbulence compensation," *Opt. Lett.*, vol. 41, no. 20, pp. 4680-4683, Oct. 2016.
- [16] S. Li and J. Wang, "Adaptive free-space optical communications through turbulence using self-healing bessel beams," *Nature Sci. Rep.*, vol. 7, no. 43233, pp. 1-8, Feb. 2017.
- [17] W. Nelson, J. P. Palastro, C. C. Davis, and P. Sprangle, "Propagation of bessel and airy beams through atmospheric turbulence," *J. Opt. Soc. Amer. A*, vol. 31, no. 3, pp. 603-609, Mar. 2014.
- [18] J. D. Schmidt, *Numerical Simulation of Optical Wave Propagation*. Bellingham, WA, USA: SPIE Press, 2010.
- [19] T. Doster and A. T. Watnik, "Laguerre-gauss and bessel-gauss beams propagation through turbulence: Analysis of channel efficiency," *Appl. Opt.*, vol. 55, no. 36, pp. 10239-10245, Dec. 2016.
- [20] I. B. Djordjevic and Z. Qu, "Coded orbital-angular-momentum-based free-space optical transmission," *Wiley Encyclopedia of Electrical and Electronics Engineering*. Hoboken, NJ, USA: Wiley Online Library, 2016.
- [21] Z. Qu and I. B. Djordjevic, "500 gb/s free-space optical transmission over strong atmospheric turbulence channels," *Opt. Lett.*, vol. 41, no. 14, pp. 3285-3288, Jul. 2016.
- [22] M. Cvijetic and I. B. Djordjevic, *Advanced Optical Communication Systems and Networks*. Norwood, MA, USA: Artech House, 2013.
- [23] G. Gibson et al., "Free-space information transfer using light beams carrying orbital angular momentum," *Opt. Exp.*, vol. 12, no. 22, pp. 5448-5456, Nov. 2004.
- [24] K. S. Morgan, J. K. Miller, B. M. Cochenour, W. Li, Y. Li, R. J. Watkins, and E. G. Johnson, "Free space propagation of concentric vortices through underwater turbid environments," *J. Opt.*, vol. 18, no. 10, Sep. 2016, Art. no. 104004.
- [25] J. Arlt and K. Dholakia, "Generation of high-order bessel beams by use of an axicon," *Opt. Commun.*, vol. 177, no. 1-6, Apr. 2000, Art. no. 297301.

- [26] R. Vasilyeu, A. Dudley, N. Khilo, and A. Forbes, "Generating superpositions of higher-order Bessel beams," *Opt. Exp.*, vol. 17, no. 26, pp. 23389-23395, Dec. 2009.
- [27] Y. Ren et al., "Adaptive optics compensation of multiple orbital angular momentum beams propagating through emulated atmospheric turbulence," *Opt. Lett.*, vol. 39, no. 10, pp. 2845-2848, May 2014.
- [28] N. Mphuthi, R. Botha, and A. Forbes, "Are Bessel beams resilient to aberrations and turbulence?" *J. Opt. Soc. Amer. A*, vol. 35, no. 6, pp. 1021-1027, Jun. 2018.
- [29] J. Mendoza-Hernandez, M. L. Arroyo-Carrasco, M. D. Iturbe-Castillo, and S. Chavez-Cerda, "Laguerre-Gauss beams versus Bessel beams showdown: Peer comparison," *Opt. Lett.*, vol. 40, no. 16, pp. 3739-3742, Aug. 2015.
- [30] I. B. Djordjevic and M. Arabaci, "LDPC-coded orbital angular momentum (OAM) modulation for free-space optical communication," *Opt. Exp.*, vol. 18, no. 24, pp. 24722-24728, Nov. 2010.
- [31] I. B. Djordjevic, J. A. Anguita, and B. V. Vasic, "Error-correction coded orbital-angular-momentum modulation for FSO channels affected by turbulence," *J. Lightw. Technol.*, vol. 30, no. 17, pp. 2846-2852, Sep. 2012.
- [32] W. K. Harrison, J. Almeida, M. Bloch, S.W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41-50, Sep. 2013.
- [33] T. Liu and I. B. Djordjevic, "On the optimum signal constellation design for high-speed optical transport networks," *Opt. Exp.*, vol. 20, no. 18, pp. 20396-20406, Aug. 2012.