SECURITY IN FREE SPACE OPTICAL COMMUNICATION SYSTEMS

ISHA CHAUHAN

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
OCTOBER 2024

SECURITY IN FREE SPACE OPTICAL COMMUNICATION SYSTEMS

by

ISHA CHAUHAN

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

OCTOBER 2024

To my loving Mummy and Papa

Certificate

This is to certify that the thesis entitled **"SECURITY IN FREE SPACE OPTICAL COMMUNICATION SYSTEMS"** being submitted by **Ms. Isha Chauhan** to the Department of Electrical Engineering, **Indian Institute of Technology Delhi**, for the award of the degree of **Doctor of Philosophy** is the record of the bona-fide research work carried out by her under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other university or institute for the award of any degree or diploma.

Date:

New Delhi

(Prof. Manav Bhatnagar)
Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi

Acknowledgements

My most profound appreciation and heartfelt gratitude go to my supervisor, Prof. Manav Bhatnagar, for his insightful auspices, valuable encouragement, and advises from the inception to the conclusion of my research. He has inspired me to become an independent researcher and has improved my critical thinking. It has been an absolute honor to work under him and to learn from him. I sincerely thank my committee members, Prof. Seshan Srirangarajan, Prof. Arpan Chattopadhyay, and Prof. Ananjan Basu, for their enriching comments and feedback during the research.

I am also obliged to my brilliant seniors, Dr. Pratiti Paul, Dr. Richa Priyadarshini, Dr. Ashish Shukla, Dr. Pranav Sharda, Dr. Muskan Ahuja for their kind care and promptness in lending a hand. I thank my lab mates and friends: Ms. Kshitija Dolas, Ms. Jinendra Sipani, Ms. Prerna Chaudhary, Dr. Upasana, Dr. Pialy Biswas, Mr. Ashutosh Balakrishnan, Ms. Srishti Sharma, and Ms. Soumita Hazra for their help.

I am grateful to the administrative staff for their support, and I appreciate the Ministry of Education for providing the necessary resources for my research.

Words cannot express my indebtedness to my Mummy and Papa for being the ground on which I flourished. Right from the beginning to every good and bad time and continuing, they are the source of light that I follow. My most enormous thank-you to Deeksha and Shekhar for emboldening, encouraging, and inspiring me whenever and wherever I needed and wanted it. I show my sincere gratefulness to my parents-in-law for their support and care. Finally, my loving thanks to my husband, Napendra, for being such an excellent companion, best friend, and fellow scholar who helps, encourages, pushes, and comforts me without any prompting or asking.

Isha Chauhan

Abstract

Free Space Optical (FSO) Communication has been enjoying the limelight in recent years owing to its many strengths, such as the capability to deliver very high data rates, provide low latency, and offer large bandwidth and capacity, making it a top applicant for prime, real-time services such as video conferencing and financial transactions.

As FSO communication gains ground in the field of data transmission, it is imperative to identify and address the security connotations associated with it. One challenge to the security of FSO communication is jamming: an unlawful transmitter sends optical signals and interferes with the legitimate receiver, thus, limits its ability to decode the information. Another threat lies from an eavesdropper (Eve), which can place a wicked receiver within the line-of-sight to capture a fraction of transmitted optical power, attaining unsanctioned ingress to the data. This dissertation endeavors to analyze the viable menaces to the security of FSO communication, develop their mathematical models, and present their resilient solutions, accompanied by the quantified attestations of their performance in securing communication for the ever-evolving landscape of wireless communication.

In the first work, the mettle of optical space shift keying (OSSK) is tested in abating the jamming in an FSO network. The jamming noise is modeled as a function of the atmospheric turbulence (AT) observed by the optical jamming signal, as opposed to its general representation following Normal distribution. The work proposes employing the OSSK in a multiple-input-single-output (MISO) system to retaliate the jammer. Specifically, a closed-form average bit error rate (ABER) of a 2×1 MISO system encountering saturated AT (modeled by negative exponential distribution) and confronting the jamming and Gaussian noise, concurrently, is derived. Building on it,

coding gain and diversity order are studied.

The subsequent work focuses on an $N \times 1$ MISO-FSO system under attack from an optical jammer with a saturated AT and varying pointing error (PE). The efficacy of the transmit aperture selection technique, where the transmitter experiencing the maximum channel gain is selected for communication, is investigated in circumventing the cordial attack of optical jamming and Gaussian noise. The considered approach is compared with other methods such as repetitive coding (RC) and OSSK.

The following study examines the repercussions of jamming on an unmanned aerial vehicle (UAV) engaged in FSO communication with a ground station. The optical link deteriorates due to concurrent Gaussian noise and jamming, while the channel fading is modeled by GG distribution with PE, considering the Angle-of-Arrival and field-of-view (FoV) of mobile UAV. The work defines the optimal conditions for UAV under attack from a non-Gaussian and optical jammer.

The subsequent study introduces a novel system model giving center stage to the exacerbation caused by an Eve on an FSO network. The work proposes different solutions to abate, quantifying the efficacy of each strategy by evaluating the discrete-input-continuous-output memory-less channel (DCMC) capacity for authentic and eavesdropping channels. The channel is characterized by generic $\alpha - \mu$ distribution, zero and non-zero boresight PE, and partial band or broadband jamming noise. The devised strategies, which included deploying a friendly jammer and employing channel fading, are assessed by formulating the closed-form average secrecy capacity in both scenarios.

In essence, this research sheds a spotlight on the potential security issues in the FSO communication and contrives their resolutions by presenting diverse and resilient propositions for ensuring that this innovative technology meets the evolving demands of modern communication networks.

सार

फ्री स्पेस ऑप्टिकल (FSO) संचार हाल के वर्षों में अपनी कई खूबियों के कारण सुर्खियों में रहा है, जैसे कि बहुत अधिक डेटा दर देने की क्षमता, कम विलंबता प्रदान करना, और बड़ी बैंडविड्थ और क्षमता प्रदान करना, जो इसे वीडियो कॉन्फ्रेंसिंग और वित्तीय लेनदेन जैसी प्राइम, रीयल-टाइम सेवाओं के लिए शीर्ष आवेदक बनाता है।

जैसे-जैसे FSO संचार डेटा ट्रांसमिशन के क्षेत्र में आगे बढ़ रहा है, इसके साथ जुड़े सुरक्षा अर्थों की पहचान करना और उनका समाधान करना अनिवार्य है। FSO संचार की सुरक्षा के लिए एक चुनौती जैमिंग है: एक गैरकानूनी ट्रांसमीटर ऑप्टिकल सिग्नल भेजता है और वैध रिसीवर के साथ हस्तक्षेप करता है, इस प्रकार, सूचना को डिकोड करने की इसकी क्षमता को सीमित करता है। एक और खतरा एक ईव्सड्रॉपर (ईव) से है, जो प्रेषित ऑप्टिकल पावर के एक अंश को कैप्चर करने के लिए एक अवैध रिसीवर को लाइन-ऑफ-विज़न के भीतर रख सकता है, जिससे डेटा तक अनधिकृत पहुंच प्राप्त होती है। यह शोध प्रबंध FSO संचार की सुरक्षा के लिए व्यवहार्य खतरों का विश्लेषण करने, उनके गणितीय मॉडल विकसित करने और उनके लचीले समाधान प्रस्तुत करने का प्रयास करता है, साथ ही वायरलेस संचार के निरंतर विकसित परिदृश्य के लिए संचार को सुरक्षित करने में उनके प्रदर्शन के मात्रात्मक प्रमाण भी प्रस्तुत करता है।

पहले काम में, FSO नेटवर्क में जैमिंग को कम करने में ऑप्टिकल स्पेस शिफ्ट कीइंग (OSSK) की क्षमता का परीक्षण किया गया है। जैमिंग शोर को ऑप्टिकल जैमिंग सिग्नल द्वारा देखे गए वायुमंडलीय अशांति (AT) के एक फ़ंक्शन के रूप में मॉडल किया गया है, जो सामान्य वितरण के बाद इसके सामान्य प्रतिनिधित्व के विपरीत है। काम में जैमर को जवाबी कार्रवाई करने के लिए एक मल्टीपल-इनपुट-सिंगल-आउटपुट (MISO) सिस्टम में OSSK को

नियोजित करने का प्रस्ताव है। विशेष रूप से, संतृप्त AT (नकारात्मक घातीय वितरण द्वारा मॉडल) का सामना करने वाले और जैमिंग और गॉसियन शोर का सामना करने वाले 2 × 1 MISO सिस्टम की एक बंद-फ़ॉर्म औसत बिट त्रुटि दर (ABER) प्राप्त की जाती है। इस पर निर्माण करते हुए, कोडिंग लाभ और विविधता क्रम का अध्ययन किया जाता है।

इसके बाद का कार्य संतृप्त AT और अलग-अलग पॉइंटिंग त्रुटि (PE) वाले ऑप्टिकल जैमर से हमले के तहत N × 1 MISO-FSO सिस्टम पर केंद्रित है। संचारण एपर्चर चयन तकनीक की प्रभावकारिता, जहाँ अधिकतम चैनल लाभ का अनुभव करने वाले ट्रांसमीटर को संचार के लिए चुना जाता है, ऑप्टिकल जैमिंग और गॉसियन शोर के सौहार्दपूर्ण हमले को दरकिनार करने में जाँच की जाती है। विचारित दृष्टिकोण की तुलना अन्य विधियों जैसे कि दोहरावदार कोडिंग (RC) और OSSK से की जाती है।

निम्नलिखित अध्ययन ग्राउंड स्टेशन के साथ FSO संचार में लगे एक मानव रहित हवाई वाहन (UAV) पर जैमिंग के नतीजों की जाँच करता है। समवर्ती गॉसियन शोर और जैमिंग के कारण ऑप्टिकल लिंक खराब हो जाता है, जबकि चैनल फ़ेडिंग को मोबाइल UAV के एंगल-ऑफ़-अराइवल और फ़ील्ड-ऑफ़-व्यू (FoV) पर विचार करते हुए PE के साथ GG वितरण द्वारा मॉडल किया जाता है। यह कार्य गैर-गॉसियन और ऑप्टिकल जैमर से हमले के तहत UAV के लिए इष्टतम स्थितियों को परिभाषित करता है।

इसके बाद के अध्ययन में एक नया सिस्टम मॉडल पेश किया गया है, जो एफएसओ नेटवर्क पर ईव के कारण होने वाली समस्या को केंद्र में रखता है। यह कार्य प्रामाणिक और ईव्सड्रॉपिंग चैनलों के लिए पृथक-इनपुट-सतत-आउटपुट मेमोरी-रहित चैनल (डीसीएमसी) क्षमता का मूल्यांकन करके प्रत्येक रणनीति की प्रभावकारिता को निर्धारित करते हुए, इसे कम करने के लिए विभिन्न समाधानों का प्रस्ताव करता है। चैनल की विशेषता सामान्य α - μ वितरण, शून्य और गैर-शून्य बोरसाइट पीई, और आंशिक बैंड या ब्रॉडबैंड जैमिंग है। तैयार की गई रणनीतियों, जिसमें एक अनुकूल जैमर को तैनात करना और

चैनल फ़ेडिंग को नियोजित करना शामिल है, का मूल्यांकन दोनों परिदृश्यों में बंद-फ़ॉर्म औसत गोपनीयता क्षमता तैयार करके किया जाता है।

संक्षेप में, यह शोध एफएसओ संचार में संभावित सुरक्षा मुद्दों पर प्रकाश डालता है और यह सुनिश्चित करने के लिए विविध और तन्यक प्रस्ताव प्रस्तुत करके उनके समाधान की योजना बनाता है कि यह अभिनव तकनीक आधुनिक संचार नेटवर्क की उभरती हुई मांगों को पूरा करती है।

Table of Contents

List of Figures

List of Tables

Abbreviations

ABER	Average bit error rate
AoA	Angle of Arrival
APD	Avalanche Photodiode
ASC	Average Secrecy Capacity
AT	Atmospheric Turbulence
AWGN	Additive white Gaussian noise
BER	Bit error rate
CCMC	Continuous-Input-Continuous-Output for Memoryless Channel
CDF	Cumulative Density Function
CSI	Channel State Information
DCMC	Discrete-Input-Continuous-Output for Memoryless Channel
EDRS	European Data Relay System
Eve	Eavesdropper
FoV	Field of view
FSO	Free Space Optical
GG	Gamma-Gamma
HAPS	High Altitude Platforms Systems
ICI	Inter Channel Interference
IEC	International Electrotechnical Commission
i.i.d.	Independent and identically distributed
ITS	Intelligent Transportation System
LASER	Light Amplification by Stimulated Emission of Radiation
LED	Light-Emitting Diode

LoS	Line of Sight
MIMO	Multiple-input-Multiple-output
MISO	Multiple-Input-Single-Output
mm-wave	millimetre wavelength
NE	Negative Exponential
NTNs	Non-Terrestrial Networks
OOK	On-Off Keying
OPALS	Optical PAyload for Lasercomm Science
OSSK	Optical Space Shift Keying
PAM	Pulse Amplitude Modulation
PAPR	Peak to Average-Power Ratio
PEP	Pair-wise Error Probability
PPM	Pulse Position Modulation
PAT	Pointing, Acquisition, and Tracking
PDF	Probability Density Function
PE	Pointing Error
RC	Repetitive Coding
RF	Radio Frequency
RV	Random variable
SC	Secrecy Capacity
SISO	Sultiple-Input-Single-Output
SJNR	Signal to Jamming-plus-Noise Ratio
SJR	Signal to Jamming Ratio
SNR	Signal to Noise Ratio
SSK	Space Shift Keying
UAV	Unmanned Aerial Vehicle
V2X	Vehicle-to-Everything

Notations

$\Re$	Real numbers
P_e	ABER
$\text{erfc}(\cdot)$	Complimentary error function
$\ln(\cdot)$	Natural logarithm
$\log_2(\cdot)$	Logarithmic base 2
N_0	Variance of additive Gaussian noise
λ	Optical wavelength
$\mathbf{x}$	Spatial Constellation vector for OSSK signaling
s	Transmitted OOK signaling
y	Received optical signal
th	Threshold for received optical signal
$\mathbf{e}_i$	i^{th} column of the 2×2 identity matrix
$\mathbf{I}_2$	2×2 Identity matrix
R	Responsivity of photodiode
P_x	Peak electrical transmitted power for OSSK signaling
P_s	Peak electrical transmitted power for OOK signaling
N_j	Net electrical transmitted power of jammer
P_j	Average jamming power
$\wp$	Probability with which a jammer becomes active
$P(\cdot)$	Probability function
J_s	State of jammer
$\mathbf{h}_x$	Channel gain vector for OSSK signaling
h_j	Channel gain between the jammer and receiver

h_{U_i}	Channel gain between the i-th user and receiver
h_m	Maximum channel gain between the i-transmitter and the receiver
N	Total number of transmitting apertures
η	Additive Gaussian noise
$P_{e_{\mathrm{J}_{\mathrm{idle}}}}$	ABER when the jammer is in an idle state
$P_{e_{\mathrm{J}_{\mathrm{active}}}}$	ABER when the jammer is in an active state
k', n	Number of transmit antenna
$PEP^{k' \to n}$	Pair-wise error probability (PEP) between the symbols $b_{k'}$ and b_n
d_H	Hamming distance between the transmitted and received symbol
e	Bit error events
κ	Arbitrary positive real number
G_c	Coding Gain
G_d	Diversity Order
γ	SJNR
$f_Z(z)$	PDF of RV z
$F_Z(z)$	CDF of RV z
$\Gamma(\cdot, \cdot)$	Incomplete Gamma function
$\Gamma(\cdot)$	Gamma function
$Q(\cdot)$	Q-function
ζ	Jitter parameter
$U(\cdot)$	Unit step function
$\delta(\cdot)$	Delta function
$K_n(.)$	Modified Bessel function of the second kind of order n
$\exp(.)$	Exponential function
${}_2F_1(., .; .; .)$	Gauss hypergeometric function
$E_n(\cdot)$	Generalized exponential integral of order n
${}_2F_2(., .; ., .; .)$	Generalized hypergeometric function
μ_0	Weather-dependent constant
L	Distance between transmitter and receiver
$G_{p,q}^{m,n}(.\vert.)$	Meijer-G function

$H_{p,q}^{m,n}[.\|.]$	Fox-H function
ϕ_{FoV}	FoV of receiver
σ_{ang}	Standard variation of UAV's orientation
α_G	Irradiance fluctuations of atmosphere due to large scale eddies
β_G	Irradiance fluctuations of atmosphere due to small scale eddies
α	Denotes non-linearity in channel
μ	Denotes clustering in channel
γ_r	SNR
$\hat{h}_{a,m,n}$	Root mean value of irradiance
$\mathbb{E}[\cdot]$	Expectation operator
σ_l^2	Log irradiance variance
C_n^2	Refractive index structure parameter
A_0	Fraction of power gathered at the center detector's center
w_{zeq}	Equivalent beam-width
σ_s	Standard deviation of displacement of legitimate beam
τ	Boresight displacement of the optical beam from the center of detector
k	Optical wave number
a	Radius of circular detector
θ	Divergence angle of the beam
$\sigma_{h_a}^2$	Scintillation index
$I_0(\cdot)$	Modified Bessel function of the first kind with zero order
$\mathcal{X}$	Finite input alphabet to DCMC system
M	Constellation size
$I(x;y)$	Mutual information
C_r	Average DCMC capacity of authentic channel
$C_r(h_{r,t})$	Instantaneous DCMC capacity of authentic channel
C_e	Average DCMC capacity of eavesdropping channel
$C_e(h_{e,j})$	Instantaneous DCMC capacity of eavesdropping channel
C_s	Average secrecy capacity
ϵ	Truncation Error

$C_{e_{NJ}}(\gamma_{e_{NJ}})$	DCMC capacity of eavesdropping channel when friendly jammer is not present
$C_{e_J}(\gamma_{e_J})$	DCMC capacity of eavesdropping channel when friendly jammer is present
C_{s_J}	Average Secrecy capacity of eavesdropping channel when friendly jammer is present