



KADIR HAS UNIVERSITY
SCHOOL OF GRADUATE STUDIES
DEPARTMENT OF ELECTRONICS ENGINEERING

**PHYSICAL LAYER SECURITY AND CHANNEL
ESTIMATION IN OPTICAL GENERALIZED
INDEX-MODULATED OFDM SYSTEMS**

FURKAN BATUHAN OKUMUŐ

MASTER OF SCIENCE THESIS

İSTANBUL, JANUARY, 2022

Furkan Batuhan Okumuş

Master of Science Thesis

2022

PHYSICAL LAYER SECURITY AND CHANNEL ESTIMATION IN OPTICAL GENERALIZED INDEX-MODULATED OFDM SYSTEMS

FURKAN BATUHAN OKUMUŞ

A thesis submitted to
the School of Graduate Studies of Kadir Has University
in partial fulfilment of the requirements for the degree of
Master of Science in
Electronics Engineering

İSTANBUL, JANUARY, 2022

APPROVAL

This thesis titled PHYSICAL LAYER SECURITY AND CHANNEL ESTIMATION IN OPTICAL GENERALIZED INDEX-MODULATED OFDM SYSTEMS submitted by FURKAN BATUHAN OKUMUŞ, in partial fulfillment of the requirements for the degree of Master of Science in Electronics Engineering is approved by

Prof. Dr. Erdal Panayırıcı (Advisor)
Kadir Has University

Prof. Dr. Hakan Ali Çırpan
İstanbul Technical University

Prof. Dr. Serhat Erköçük
Kadir Has University

I confirm that the signatures above belong to the aforementioned faculty members.

.....
Prof. Dr. Mehmet Timur Aydemir
Dean of School of Graduate Studies
Date of Approval: 06.01.2022

DECLARATION ON RESEARCH ETHICS AND PUBLISHING METHODS

I, FURKAN BATUHAN OKUMUŞ; hereby declare

- that this Master of Science Thesis that I have submitted is entirely my own work and I have cited and referenced all material and results that are not my own in accordance with the rules;
- that this Master of Science Thesis does not contain any material from any research submitted or accepted to obtain a degree or diploma at another educational institution;
- and that I commit and undertake to follow the “Kadir Has University Academic Codes and Conduct” prepared in accordance with the “Higher Education Council Codes of Conduct”.

In addition, I acknowledge that any claim of irregularity that may arise in relation to this work will result in a disciplinary action in accordance with university legislation.

FURKAN BATUHAN OKUMUŞ

.....

06.01.2022



To My Dearest Family...

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my thesis supervisor, Dear Prof. Erdal Panayırıcı who has supported me throughout my graduate studies in every aspect, beside preparation of the thesis he has also supported me for the decisions I should have made. Without his guidance and knowledge I would not be able to complete my master's study. His endless energy and motivation be a lesson to us all.

I gratefully acknowledge the Kadir Has University, Department of Electrical - Electronics Engineering funding and Prof. Erdal Panayırıcı's research grant from the TUBITAK 1003 priority areas Research & Development projects support program, "Physical Layer Security In The Visible Light Communication Systems", Project No: 218E034 for providing me financial support throughout my graduate studies. I have served as a teaching assistant in the Department of Electrical - Electronics Engineering at Kadir Has University and a research assistant in Prof. Panayırıcı's project during my master's degree.

Last but not the least; I would like to express my thankfulness to my parents - Fikriye & Yavuz Selim Okumuş, my sister - Aybike Beyza Okumuş. Next, I thank my best friend Sümeyra Aldemir, who is always there when I need her and has a significant share to get me where I am today. Their unconditional support gave me the strength to carry out my thesis and finish it. Especially on these coronavirus days, I could not finish my graduate studies without the psychological support they provided.

PHYSICAL LAYER SECURITY AND CHANNEL ESTIMATION IN OPTICAL
GENERALIZED INDEX-MODULATED OFDM SYSTEMS

ABSTRACT

Visible light communication (VLC) is a promising and not completely discovered technology for next-generation wireless communication systems. In this thesis, generalized LED index modulation (GLIM-OFDM), which is a new modulation method for VLC systems based on multi-input multi-output (MIMO) orthogonal frequency division multiplexing (OFDM), is used. In the GLIM-OFDM system, the real and imaginary components of the complex time-domain OFDM signals are first separated from each other, and then the resulting bipolar signals are transmitted over a MIMO-VLC channel by encoding the signal information in light-emitting diode (LED) indices. Higher spectral efficiency and power efficiency are achieved by encoding the beacon information of complex signals to the position of the transmitter LEDs. As in RF systems, physical layer security (PLS) in VLC systems is an issue that must be taken into account to ensure the security of the system and prevent access to the transmitted information by unauthorized users. While examining PLS techniques for VLC systems, this thesis proposes a new and unique PLS algorithm and channel estimation method for GLIM-OFDM systems. We consider Bayesian(MMSE) estimation to handle the estimation problem, and then we propose a further enhancement of the PLS algorithm with secrecy key generation. From the curves we obtained, it is shown that the algorithm provides a high secrecy rate for the VLC system, i.e., when the legitimate user takes the transmitted information correctly, the eavesdropper cannot reach the correct information but a distorted one. Channel information also has an important place for proper transmission. In this study, the mean square error (MSE), bit error rate (BER), and Cramer-Rao (CR) sub-bound of the channel estimation algorithm were obtained analytically, and their performances according to the signal-to-noise ratio were analyzed with computer simulations. From the obtained MSE, BER, and CR curves, it is concluded that the

MSE performance of the proposed channel estimation algorithm is very high and the BER performance of the system obtained with the predicted channel information is very close to the BER performance when the channel is known perfectly.

Keywords: Visible light communication(VLC), Orthogonal frequency division multiplexing(OFDM), Physical layer security(PLS), Generalized LED index modulation OFDM(GLIM-OFDM), Bit error rate (BER), Mean square error (MSE), Signal to noise ratio (SNR), Channel estimation



OPTİK GENELLEŞTİRİLMİŞ İNDEKS MODÜLASYONLU OFDM SİSTEMLERİNDE FİZİKSEL KATMAN GÜVENLİĞİ VE KANAL KESTİRİMİ

ÖZET

Görünür ışıkla iletişim (Visible light communication, VLC), yeni nesil kablosuz iletişim sistemleri için umut verici ve tam anlamıyla keşfedilmemiş bir teknolojidir. Bu tezde, çok-girdili çok-çıkıtlı (multi-input multi-output, MIMO) dikgen frekans bölmeli çoğullama (orthogonal frequency division multiplexing, OFDM) tabanlı VLC sistemleri için yeni bir modülasyon yöntemi olan genelleştirilmiş LED indeks modülasyonu (Generalized LED Index Modulation, GLIM-OFDM) kullanılmıştır. GLIM-OFDM sisteminde, ilk önce karmaşık zaman bölgesi OFDM sinyallerinin gerçel ve sanal bileşenleri birbirinden ayrılır, ardından ortaya çıkan iki kutuplu sinyaller, işaret bilgileri LED indekslerinde kodlanarak bir MIMO-VLC kanalı üzerinden iletilir. Karmaşık sinyallerin işaret bilgilerinin verici LED'lerin konumuna kodlanmasıyla daha yüksek spektral verimlilik ve güç verimliliği elde edilir. RF sistemlerinde olduğu gibi, VLC sistemlerinde de fiziksel katman güvenliği sistemin güvenliğinin sağlanması ve yetkisiz kullanıcılar tarafından iletilen bilgiye ulaşılmaması için dikkate alınması gereken bir konudur. Bu tezde, VLC sistemleri için PLS teknikleri incelenirken aynı zamanda, GLIM-OFDM sistemleri için yeni ve özgün bir PLS algoritması ile kanal kestirim yöntemi önerilmektedir. Tahmin problemiyle baş edebilmek için Bayesian (MMSE) tahminini ele alıyoruz ve ardından gizlilik anahtarı oluşturma yöntemi ile PLS algoritmasının geliştirilmiş halini öneriyoruz. Elde ettiğimiz eğrilerden açıkça görülüyor ki, önerilen algoritma VLC sistemi için yüksek bir gizlilik oranı sağlıyor, yani meşru kullanıcı iletilen bilgiyi doğru bir şekilde alırken, kulak misafiri doğru bilgiye değil, çarpıtılmış bir bilgiye ulaşıyor. İletimin doğru bir şekilde gerçekleşmesi için kanal bilgisi önemli bir yer tutmaktadır. Bu tezde, kanal kestirim algoritmasının ortalama kare hatası (mean square error, MSE), bit hata oranı (bit error rate, BER) ve Cramer-Rao (CR) alt sınırları analitik olarak elde edilmiş ve sinyal-gürültü oranına (signal to noise ratio, SNR)

göre performansları bilgisayar simülasyonları ile analiz edilmiştir. Elde edilen MSE, BER ve CR eğrilerinden, önerilen kanal tahmin algoritmasının MSE performansının çok yüksek olduğu ve kestirilen kanal bilgisi ile elde edilen sistemin BER performansının kanal mükemmel bilinirkenki BER performansına çok yakın olduğu sonucuna varılmıştır. **Anahtar Sözcükler:** Görünür ışıkla haberleşme(VLC), dikgen frekans bölmeli çoğullama(OFDM), Fiziksel katman güvenliği(PLS) geliştirilmiş LED indeks modülasyonu(GLIM-OFDM), bit hata oranı (BER), ortalama karesel hata (MSE), sinyal-gürültü oranı (SNR), kanal kestirimi.



TABLE OF CONTENTS

ACKNOWLEDGEMENT	v
ABSTRACT	vi
ÖZET	viii
LIST OF FIGURES	xii
LIST OF TABLES	xiii
LIST OF ACRONYMS AND ABBREVIATIONS	xiv
1. INTRODUCTION	1
1.1 Optical Wireless Communication	1
1.2 Literature Review	2
1.3 Motivation	5
1.4 Contribution of the Thesis	6
1.5 Thesis Outline	7
2. VISIBLE LIGHT COMMUNICATION WORKING PRINCIPLES	8
2.1 Transmitter of VLC	9
2.2 Channel of VLC	9
2.3 Receiver of VLC	11
3. OPTICAL GLIM-OFDM IN THE PRESENCE OF FREQUENCY- FLAT MIMO CHANNELS	12
4. PHYSICAL LAYER SECURITY IN OPTICAL GENERALIZED INDEX-MODULATED OFDM SYSTEMS	16
4.1 Precoded(ZF) Transmitter Aided PLS in GLIM OFDM Systems	16
4.2 Normalization of Powers at Transmitter	17
4.3 Conditional Bayesian(MMSE) Estimation	19
4.4 Further Enhancement of the PLC algorithm with Secrecy Key Generation	23
4.5 Achievable Secrecy Rate of the GLIM-OFDM System	26
5. CHANNEL ESTIMATION IN OPTICAL GENERALIZED INDEX- MODULATED OFDM SYSTEMS	32

5.1	Cramer-Rao Lower Bound in Channel Estimation	33
6.	COMPUTER SIMULATIONS	35
6.1	Physical Layer Security Simulations	35
6.2	Channel Estimation Simulations	39
6.2.1	Simulation Examples	40
6.2.2	Computer Simulation Results of Channel Estimation	41
7.	CONCLUSIONS	45
	BIBLIOGRAPHY	46



LIST OF FIGURES

Figure 2.1	Basic Block Diagram of a VLC System	8
Figure 2.2	Geometry of an indoor VLC scenario	10
Figure 2.3	Receiver side of a VLC system	11
Figure 3.1	Block Diagram of the GLIM-OFDM for a 4x4 MIMO-VLC system	13
Figure 4.1	Comparison of the exact and Gaussian approximated mutual information	29
Figure 5.1	Block Diagram of the GLIM-OFDM with Precoder and Channel Estimation	34
Figure 6.1	Comparison of BER performances of Bob and Eve with and without secret key as a function of SNR for 1st scenario	36
Figure 6.2	Comparison of BER performances of Bob and Eve with and without secret key as a function of SNR for 2nd scenario	37
Figure 6.3	Mutual informations of Bob and Eve and achievable secrecy rate for Bob	38
Figure 6.4	Comparison of Bob's achievable secrecy rates obtained in the frequency and the time-domains	39
Figure 6.5	Contour plot of the BER values of Eve when Bob is at center and Eve is mobile in the room.	39
Figure 6.6	Simulation of the room for Example 1	40
Figure 6.7	Simulation of the room for Example 2	41
Figure 6.8	Channel Estimation MSE Performance and Cramer-Rao Lower Bound	43
Figure 6.9	GLIM OFDM BER Performance Under Channel Estimation Error	44

LIST OF TABLES

Table 6.1 Configuration Parameters 42



LIST OF ACRONYMS AND ABBREVIATIONS

ACO-OFDM	Asymmetrically Clipped Optical OFDM
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
Bob	Legitimate User
CR	Cramer-Rao
CRLB	Cramer-Rao Lower Bound
CRT	Chinese Remainder Theorem
CSIT	Channel State Information At The Transmitter
DC	Direct Current
DCO-OFDM	DC-Biased Optical OFDM
Eve	Eavesdropper
FFT	Fast Fourier Transform
Fov	Field Of View
GLIM-OFDM	Generalized Led Index Modulated Orthogonal Frequency Division Multiplexing
GSSK	Generalized Space Shift Keying
IFFT	Inverse Fast Fourier Transform
IM/DD	Intensity Modulation/Direct Detection
IOT	Internet Of Things
ISI	Inter-Symbol Interference
LED	Light Emitting Diode
LMMSE	Linear Minimum Mean Square Error
LoS	Line-Of-Sight
M-QAM	M-Level Quadrature Amplitude Modulation
MIMO	Multi-Input Multi-Output
MMSE	Minimum Mean Square Error
MSE	Minimum Square Error
NDC-OFDM	Non DC-Biased OFDM
OFDM	Orthogonal Frequency Division Multiplexing

OSI	Open System Interconnect
OWC	Optical Wireless Communication
P/S	Parallel To Serial
PD	Photodetector
PLS	Physical Layer Security
RF	Radio Frequency
RGB	Red-Green-Blue
Rx	Receiver
S/P	Serial To Parallel
SCD	Spatial Constellation Design
SM	Spatial Modulation
Tx	Transmitter
U-OFDM	Unipolar OFDM
VLC	Visible Light Communication
ZF	Zero-Forcing

1. INTRODUCTION

The main objective of this thesis is to investigate the PLS techniques in VLC and propose a new and novel PLS algorithm and channel estimation method in generalized optical index-modulated OFDM systems. To make these issues more precise, we now present the basic properties and components of the visible light communication systems as part of the optical wireless communications as well as the principles of PLS techniques employed in the optical domain.

1.1 Optical Wireless Communication

Optical wireless communication (OWC) is an attractive new technology with great potential for next-generation wireless communication systems. Artificial light is used in almost all areas of our lives, such as ceiling lights, mobile phone screens, vehicle headlights. It is known that there are billions of artificial light sources like these examples in the world. After the concept of the internet of things (IoT) came into our lives, not only computers and smartphones but also cars, lighting, watches, coffee machines, refrigerators, and washing machines became connected to the internet. Thanks to the capabilities of modern LEDs, a new communication form has been developed in which artificial light is used as a communication tool. VLC is a communication method in which visible light in the 400-800 THz frequency range is used as a means of communication. VLC is an ultra-fast data transmission technology that uses light to send and receive messages over a distance. Light travels 299,792 km per second, which means it is the fastest way of communication. VLC uses visible light between 375 and 780 nm, which is visible to the human eye. In VLC technology, data in the form of ones and zeros is transmitted by quickly turning the light on and off. Data transfer depends on how fast the light can be turned on and off. That's why LED lighting is well suited for VLC applications.

VLC requires a transmitter (LED) and a receiver (photodetector). The information received from the data source is transmitted by the LED via the driver. The LED flashes quickly to transmit the data to the photodetector. The signals are decoded by the receiving module and converted into the original information. Processes such as data packaging, hardware control, encoding and decoding, error handling, and synchronization are performed through software. VLC cannot pass through walls as it uses visible light to transfer data. So, it is safer than the other communication techniques for indoor communication. Also, it is known that VLC does not cause any harm to human health. VLC, which is the fastest way of data communication, is used in smart lighting, infrastructure and transportation technologies, the health sector, aviation, and many similar areas. VLC systems can be the most suitable solution for indoor mobile communication scenarios because of their frequency range. That is because the existing infrastructure of VLC systems is reusable and combines lighting and communication systems. It is evident that advantages such as license-free implementation, low cost of deployment, wide bandwidth, energy efficiency, and high security have made VLC one of the strongest candidates beyond 5G wireless communication standards. Besides these, although VLC appears to be secure compared to other communication methods, ensuring physical layer security is vital to ensure the complete safety of the system. Physical layer security aims to increase the security of the communication system used by using the randomness of the channels and interference to reduce the correct information rate received by eavesdroppers trying to access unauthorized information.

1.2 Literature Review

The OFDM and modified versions of the intensity modulation/direct detection (IM/DD) systems in VLC have drawn considerable attention [1], due to the frequency selective behavior of the VLC channels for medium and high data rates and the ability to efficiently perform bit and power loading. OFDM provides significant advantages in the presence of inter-symbol interference (ISI) caused by frequency selectivity. However, it is impossible to transmit OFDM signals without any modi-

fication in optical wireless communications since the transmitted optical signals are generally unipolar. Therefore, the addition of a direct current (DC) biasing and the power efficiency of optical OFDM form the primary motivation behind new, energy-efficient optical OFDM systems. The use of the IM/DD technique naturally requires light intensity levels to be real and positive-valued. These restrictions lead to many difficulties when the goal is to transmit IM/DD signals and maintain the same spectral and power efficiency that compatible transmission systems have. Many different methods have been proposed in the literature to overcome these difficulties. For example, real-time domain signals are directly obtained using the conjugate symmetry feature of the fast Fourier transform (FFT), known as Hermitian symmetry, but the main innovations of the proposed systems come from how they deal with the bipolar nature of the signals. One simple solution to generating positive-valued signals is to add a DC bias after the inverse FFT (IFFT) operation. The resulting system is called DC-biased optical OFDM (DCO OFDM)[2]. The FFT's anti-symmetric feature leads to the asymmetrically clipped optical OFDM (ACO OFDM) scheme, as described in [3], which is a clever way to solve the bipolarity problem in the OFDM transmission. In ACO-OFDM, DC bias is significantly reduced at the cost of sacrificing half of the spectral efficiency. In [4], a new unipolar transmission system called U-OFDM is proposed. Half power (3 dB) penalty caused by time-domain clipping in ACO-OFDM is resolved by transmitting positive and negative frames separately in U-OFDM; however, both systems only achieve half the spectrum efficiency compared to DCO-OFDM. The new method proposed in [5] and [6] offers time-domain superposition for both U-OFDM and ACO-OFDM to achieve the same spectral efficiency as DCO-OFDM. Recently, MIMO and index modulation transmission methods have begun to receive significant attention in the VLC literature for transmitting additional bits with reduced energy consumption. In [7], MIMO VLC-based systems are examined for the multi-user case. Index modulation techniques, in which indices of the building blocks of considered communication systems are used to transmit additional bits of information, are particularly promising for energy- and spectrum-efficient IM/DD applications. Transmission systems based on index modulation offer additional degrees of freedom to compensate for the loss of

phase size. In [8], spatial modulation (SM), the most common form of index modulation, is adopted for MIMO-VLC systems. The performance of SM and some variants of it are examined for VLC systems [9]. Also, a 2×2 optical SM-based structure is proposed in [10] to overcome DC bias loss by adding two LEDs to send negative and positive signals. Taking advantage of different wavelengths in the visible band is another promising solution to improve spectrum efficiency through multi-channel communication [11]-[15]. Eavesdropping is an issue to consider when considering wireless communication systems because the broadcast nature of electromagnetic waves includes optical band and dense small cell networks with decentralized structure [16]-[17]. Security in wireless networks is usually provided with passwords or secret key distribution, but these methods also have vulnerabilities in cases where the eavesdropper has high computational power[18]. Also, the secret key is difficult to manage and distribute over a densely deployed network[19]. Moreover, the physical layer has been used as a gate to connect the other six upper layers of open system interconnect (OSI) to the real world. Therefore, physical layer security has vital importance when we consider the security of the wireless communication system. It is shown that PLS relies on the secrecy capacity of the channel, making use of channel features to hide information from unauthorized users in [20]. MIMO systems have a big potential to combine high achievable data rates and physical layer security. As we see, physical layer security is the main problem to handle for indoor VLC systems because VLC is safer than the other communication systems in theory. Still, if there is an eavesdropper in the room or windows, it can turn unsafe; that is why physical layer security is one of the main stones for visible light communication systems. There are many pieces of research in the literature about PLS for VLC and its main concept. [21] gives a detailed survey and literature information of PLS in VLC. Some systems use a technique that combines the message signal in the transmitter with mixed sequences, preventing the eavesdropper from reaching the actual information and enabling the receiver to obtain the correct information using the known mixed pseudo-random code[22]-[24]. To achieve a good secrecy rate in an indoor VLC system, polar codes are proposed in [25]. In [26], a key generation mechanism is proposed that increases the robustness of the system. Unlike the

others, systems establishing a protective zone around the legitimate receiver have also been proposed. To enhance the system's secrecy performance, a disk-shaped protection zone is designed around the legitimate receiver in [27]. In [28]-[34], a method called friendly jamming, which means an artificial noise is produced and applied to eavesdropper to degrade its channels, is used. A system in which half of the LEDs are used for jamming and the others used for the information-bearing signal is proposed in [35]. In [36], to provide physical layer security for optical generalized space shift keying (GSSK), a novel spatial constellation design (SCD) technique is proposed. This study proposes precoded-PLS techniques, zero-forcing (ZF), minimum mean square error (MMSE), and secrecy key generation for precoding at the transmitter. It is aimed to eliminate the drawbacks by using advanced techniques for each step. On the other hand, there are very few studies, and publications in the literature on channel estimation related to VLC systems [37]-[38]. In this study, a channel estimation technique with low computational complexity and high MSE performance is proposed for a 4×4 MIMO-based optical OFDM system called generalized optical OFDM, proposed in [39], to work in the presence of flat-frequency and frequency-selective channels. In accordance with the MMSE criterion, the Cramer-Rao lower bound that the developed channel estimation algorithm can reach is also obtained analytically. Using computer simulations, the BER performance of the system is examined under various signal-to-noise ratios, and 4QAM, 8QAM, and 16QAM modulation types after channel information is estimated.

1.3 Motivation

Due to the rapid development of technology, speed and security in communication systems have become very important. Since radio frequency (RF) technology could not keep up with the rapid increase of communication devices, a search for new technology has arisen. As a result of the necessity, VLC emerged as a candidate. Light cannot pass walls or solids; therefore, VLC is safer than the other communication systems. However, this is no longer valid for common areas, such as libraries, offices, etc. In the environment where there is an eavesdropper who is not asked to access

the transmitted information, physical layer security is the case for the system, and channel information has an important place to ensure security. Since the devices in the room are mobile, channel information is required for each location where the devices can be found. Based on this idea, the channel estimation accuracy is crucial to ensure secure communication for indoor VLC scenarios. The studies in this thesis aim to ensure physical layer security and estimate channel information for an indoor VLC system, considering the realistic channels between OWC connections.

1.4 Contribution of the Thesis

In the studies carried out within the scope of this thesis, it will be assumed that VLC channels have a deterministic and sparse structure. In other words, VLC determines the channel impulse response with a component consisting of a line-of-sight (LOS) transmission and very few components caused by reflections. The main contributions of this thesis can be listed as follows:

1. Designing a new and novel physical layer security technique based on precoding at the transmitter side for the optical generalized index-modulated OFDM (GLIM-OFDM) transmission adopted in the indoor VLC systems.
2. Developing a conditional Bayesian(MMSE) estimation to solve the estimation problem analytically.
3. Giving further enhancement of the PLS algorithm with Secrecy Key Generation.
4. Determining the visible light channel models for indoor visible light communication scenarios and generating suitable visible light channel models depending on the geometry of the environment in the computer environment.
5. Developing a new and unique channel estimation algorithm for GLIM-OFDM system.
6. Obtaining the MSE performance of the developed channel estimation algorithm and examining the effects of these errors on the BER of the system.
7. Deriving the Cramer-Rao lower bounds (CRLB) analytically, which is a mea-

sure of the quality of the channel estimation algorithm and comparing the theoretical CRLB with the computer simulations.

1.5 Thesis Outline

In Chapter 1, the introduction of the thesis, the literature review, and the motivation of the thesis are presented. In Chapter 2, the working principle of VLC is introduced, including the transmitter and the receiver of VLC, which are LEDs and Photo-diodes, respectively. In Chapter 3, the OFDM technique used in the VLC system, which is named GLIM-OFDM, is detailed. In Chapter 4, the physical layer security of visible light communication is introduced. Three different transmitter precoding techniques are applied to see the difference between the change in secrecy capacity and an enhanced solution. In Chapter 5, a new channel estimation algorithm is proposed for GLIM-OFDM. In Chapter 6, computer simulations for PLS and channel estimation are given, and SNR and BER performance are shown in the presence of the channel estimation. Chapter 7 presents the conclusions of the thesis.

2. VISIBLE LIGHT COMMUNICATION WORKING PRINCIPLES

Light travels at a speed of 186,000 miles in a second, and VLC uses light to transmit data meanly; it is evident that VLC is the fastest way of communication. Every form of data can be changed into zeros and ones. In VLC, these data, which are represented by zeros and ones, can be symbolized using on-off keying. In other words, turning the light on and off, fastly, like blinking. LED has a fast switching property that is why LED lighting is suitable for this process. LEDs are used as transmitters and PDs which have a good response for visible light wavelength are used as receivers. The signal transmitted in VLC has to be positive and real characteristic. Air is taken as the communication medium. Figure 2.1 shows the basic block diagram of a VLC system which occurred of a receiver part, a transmitter part and a channel.

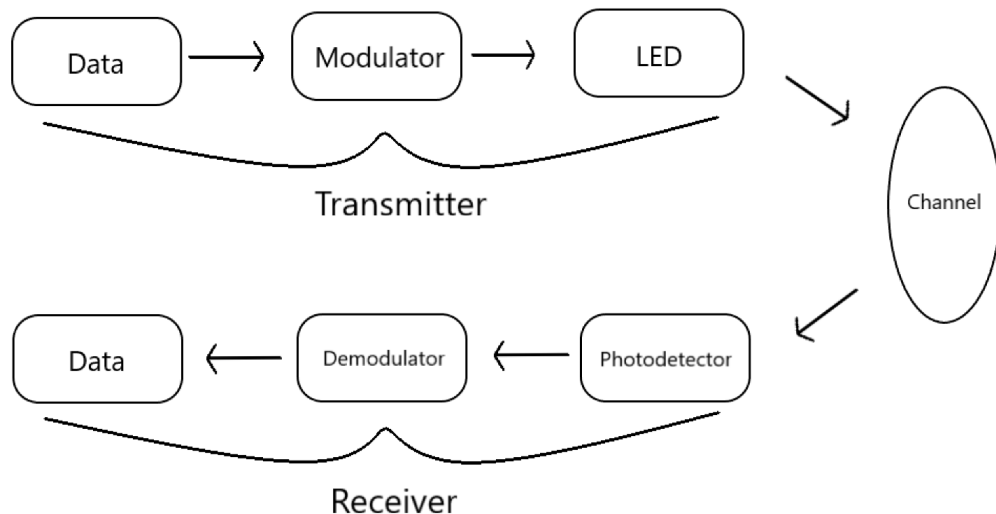


Figure 2.1 Basic Block Diagram of a VLC System

The received signal in a VLC system is shown below,

$$\mathbf{r}(\mathbf{t}) = \mathbf{H}\mathbf{s}(\mathbf{t}) + \omega(t) \quad (2.1)$$

where $\mathbf{r}(\mathbf{t})$ represents the received signal, \mathbf{H} represents the channel response, $\mathbf{s}(\mathbf{t})$ shows the signal and lastly $\omega(\mathbf{t})$ denotes the additive white Gaussian noise (AWGN) for the system.

2.1 Transmitter of VLC

In VLC systems, LEDs are used to transmit data as the transmitter. The development of LED technology has made it easier for optical communication to take precedence over other types of communication. The mission of LED is to convert the modulated electrical signal into an optical intensity value. LEDs are divided into two types as a single color and multi-color. Multi-color LEDs are known as RGB (Red-Green-Blue). LED colors can be assigned to antennas. LEDs blink too fast for the human eye to detect, and in this way, they transmit bits, i.e., zeros and ones, to the receiver.

2.2 Channel of VLC

The VLC channel model uses channels created using LoS elements between LEDs and photodetectors. While modeling the channel, the LoS channel matrix with dimensions $N_r \times N_t$ is created in the following order:

$$\mathbf{H} = \begin{bmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,N_t} \\ h_{2,1} & h_{2,2} & \dots & h_{2,N_t} \\ \vdots & \ddots & \ddots & \\ h_{N_r,1} & h_{N_r,2} & \dots & h_{N_r,N_t} \end{bmatrix} \in R^+$$

here, N_r represents the number of receivers and N_t represents the number of transmitters. $h_{r,t}$ shows the channel coefficient between the r-th receiving PD and the t-th emitting LED and is calculated as follows:

$$h_{r,t} = \frac{(m+1) A_{PD}}{2\pi d_{r,t}^2} \cos^m(\phi_{r,t}) \cos(\theta_{r,t}) 1_{\Psi_{1/2}}(\theta_{r,t})$$

Accordingly, the angles $\phi_{r,t}$ and $\theta_{r,t}$ represent the angle of emergence and angle of incidence between the r^{th} receive PD and the t^{th} transmit LED, respectively. The distance between the r^{th} PD and the t^{th} LED is denoted by $d_{r,t}$, and the parameter m is the Lambertian emission order of the light source. A_{PD} shows the domain of the un-imaged PD. $1_{\Psi_{1/2}}$ is the indicator function what decides whether the angle of incidence is in or not in the field of view (FoV) of the PD as follows:

$$1_{\Psi_{1/2}}(x) = \begin{cases} 1, & \text{if } |x| \leq \Phi_{1/2} \\ 0, & \text{otherwise} \end{cases}$$

where $\Phi_{1/2}$ is half angle of the PD's field of view.

Figure 2.2 shows the visual representation of the channel parameters:

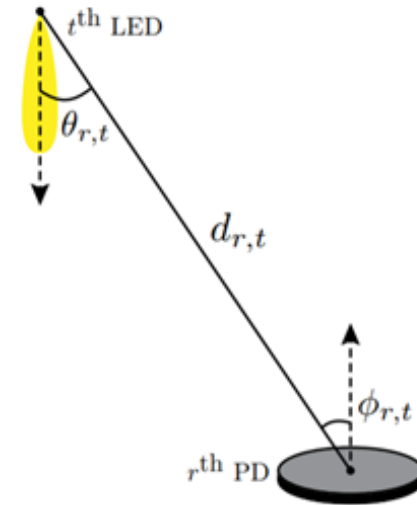


Figure 2.2 Geometry of an indoor VLC scenario

2.3 Receiver of VLC

After the channel response is applied to the optical signal, the resulting optical signal passes through the optical concentrator and optical filters and reaches the PD. The next step after PD is an amplifier to amplify the signal, and then the resulted signal gets in an equalizer. Lastly, an electrical filter is applied and the resulted signal reaches the user as an electrical signal. An illustration of the receiver part of a VLC system is shown in Figure 2.3.

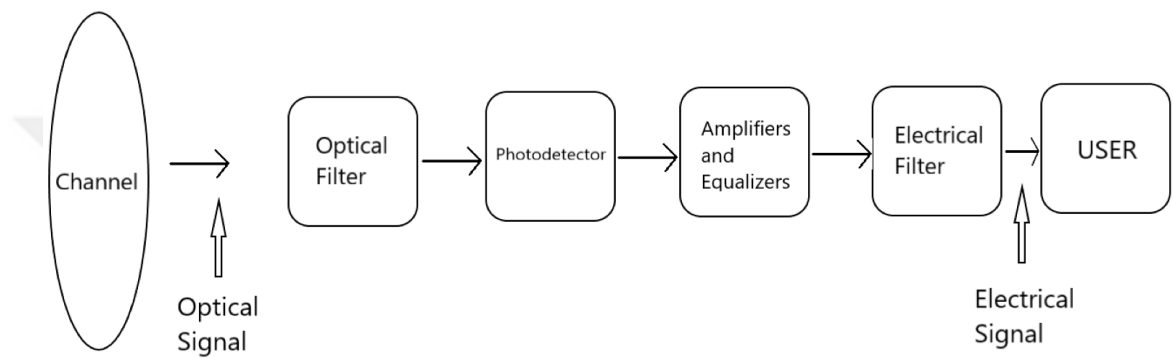


Figure 2.3 Receiver side of a VLC system

3. OPTICAL GLIM-OFDM IN THE PRESENCE OF FREQUENCY-FLAT MIMO CHANNELS

The GLIM-OFDM transceiver block diagram for frequency-flat MIMO channels is given in Figure 3.1. Information bits $N \log_2(M)$ carrying the vector \mathbf{u} are applied to the GLIM-OFDM transmitter for transmission of each OFDM block, where N is the number of OFDM subcarriers and M is the size of M -level quadrature amplitude modulation (M -QAM) signals used in transmission. The operation of DCO-OFDM, ACO-OFDM and non-DC-biased OFDM (NDC-OFDM) optical communication systems relies on Hermitian symmetry to generate real-time signals after the IFFT process. In the GLIM-OFDM, the OFDM modulator directly processes the complex frequency domain OFDM frame \mathbf{x}_F without requiring Hermitian symmetry. The resulting time-domain OFDM frame $\mathbf{x}_T=[x_1 \dots x_N]^T$ is composed of complex-valued and bipolar (positive and negative-valued) elements; therefore, it cannot be transmitted via a VLC channel. To solve this problem, a new LED index modulation-based MIMO transmission technique has been developed. After parallel to serial (P/S) conversion, using a technique similar to [39], for each time-domain OFDM signal x_k , where $k = 0, 1, \dots, N - 1$, first the real and imaginary parts of the complex signal x_k are separated where $x_k=x_{k,R} + jx_{k,I}$. The resulting real but bipolar signals $x_{k,R}$ and $x_{k,I}$ are then processed by positive-negative (+/-) separators to yield the following positive real-valued signals:

$$\begin{aligned}
 x_{k,R}^+ &= \begin{cases} x_{k,R}, & \text{if, } x_{k,R} > 0 \\ 0, & \text{if, } x_{k,R} < 0 \end{cases} & x_{k,R}^- &= \begin{cases} 0, & \text{if, } x_{k,R} > 0 \\ -x_{k,R}, & \text{if, } x_{k,R} < 0 \end{cases} \\
 x_{k,I}^+ &= \begin{cases} x_{k,I}, & \text{if, } x_{k,I} > 0 \\ 0, & \text{if, } x_{k,I} < 0 \end{cases} & x_{k,I}^- &= \begin{cases} 0, & \text{if, } x_{k,I} > 0 \\ -x_{k,I}, & \text{if, } x_{k,I} < 0 \end{cases}
 \end{aligned} \tag{3.1}$$

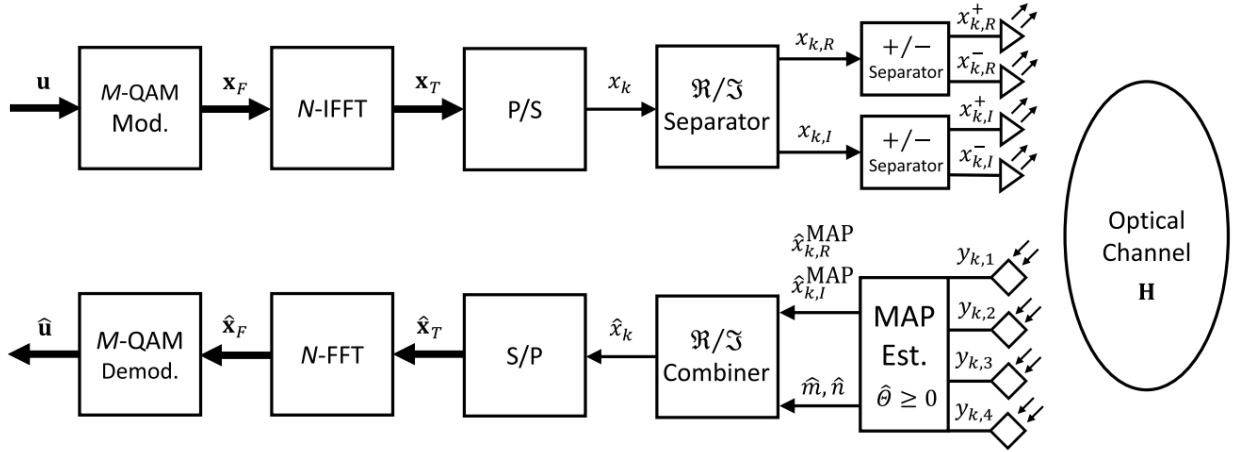


Figure 3.1 Block Diagram of the GLIM-OFDM for a 4x4 MIMO-VLC system

These signals are transmitted simultaneously from a $n_R \times n_T$ MIMO VLC system, where n_R and n_T indicate the number of the receiver (Rx) and transmitter (Tx) units, respectively. As can be seen from Figure 3.1, the LEDs transmit the absolute values of the $x_{k,R}$ and $x_{k,I}$ signals and are thus positive real numbers. Also, unlike other optical communication systems, GLIM-OFDM completely eliminates the Hermitian symmetry at the input of the IFFT and the loss of spectral efficiency caused by Hermitian symmetry. As a result, the spectral efficiency of the GLIM OFDM system is $\log_2(M)$ [bit/s/Hz], achieving a spectral efficiency up to twice that of conventional systems. Positive and real-valued OFDM time samples $x_{k,R}^+$, $x_{k,R}^-$, $x_{k,I}^+$ and $x_{k,I}^-$ where $k = 0, 1, \dots, N - 1$ are transmitted over a 4×4 optical MIMO channel which is represented by \mathbf{H} as,

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \quad (3.2)$$

where $\mathbf{y} = [y_{k,I} \dots y_{k,n_R}]^T \in R^{n_R \times 1}$ is the vector of received signals that contains the electrical signals obtained from PDs at the Rx units. In (3.1), $\mathbf{n} \in R^{n_R \times 1}$ is the vector of real-value AWGN that models shot and thermal noises. The elements have a probability distribution $N(0, \sigma_w^2)$ and are added to received signals in the electrical region. The transmitted signal vector $\mathbf{x} \in R^{4 \times 1}$ is generated for GLIM-OFDM as:

$$\mathbf{x} = [x_{k,R}^+ x_{k,R}^- x_{k,I}^+ x_{k,I}^-]^T. \quad (3.3)$$

Over a 4×4 optik MIMO channel which is shown as $\mathbf{H} = [h(r,t)]$, $h_{r,t}$ represents

the channel gain of the optical wireless channel formed between the t^{th} LED at the transmitter and the r^{th} PD at the receiver. In this study, the SNR is defined as the average SNR at the receiver:

$$SNR_{Rx} = \frac{P_{Rx}^{elec}}{\sigma_n^2} \quad (3.4)$$

where P_{Rx}^{elec} is the average electrical power reaching the receiver and σ_n^2 is the noise power at the receiver. The positive and real-valued OFDM time samples $x_{k,R}^+$, $x_{k,R}^-$, $x_{k,I}^+$ and $x_{k,I}^-$ can be transmitted simultaneously over an 4×4 MIMO VLC channel, represented by

$$\mathbf{H} = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} & h_{1,4} \\ h_{2,1} & h_{2,2} & h_{2,3} & h_{2,4} \\ h_{3,1} & h_{3,2} & h_{3,3} & h_{3,4} \\ h_{4,1} & h_{4,2} & h_{4,3} & h_{4,4} \end{bmatrix} \in \mathcal{R}^{4 \times 4}, \quad (3.5)$$

where $h_{r,t}$ denotes the channel gain of the optical wireless link between the Tx unit (LED) t and the Rx unit (PD) r . It should be noted that, n_T must be divisible by four for the proposed scheme where it is taken as $n_T = 4$ in this work. In real indoor VLC systems, given a number of LEDs placed on the ceiling with known geometry and some tilts, the channel coefficients can be determined between each of the LEDs and the points on a grid over the floor by either a ray-tracing method of Zemax© which is an optical and illumination software or by the formula given as

$$h_i = \frac{(m+1)A_{PD}}{2\pi D_i^2} \cos^m(\phi_i) \cos(\theta_i) \text{rect}\left(\frac{\theta_i}{\text{FOV}_{PD}}\right), \quad (3.6)$$

where the angles ϕ_i and θ_i represent the angle of incidence and angle of arrival between the receive PD and i^{th} transmit LED, respectively. The distance between the receive PD and i^{th} transmit LED is denoted by D_i . The parameter m is the Lambertian emission order of the light source and defined as $m = -1/\log_2(\cos(\Phi_{1/2}))$ where $\Phi_{1/2}$ is the semi-angle of the half-power of the transmit LED. FOV_{PD} and A_{PD} are indicating the semi-angle of the FoV and effective area of the non-imaging PD, respectively.

In the GLIM-OFDM scheme, LEDs transmit the absolute values of $x_{k,R}$ and $x_{k,I}$ signals and the index of the transmitting LED determines the sign of the correspond-

ing signals similar to the NDC-OFDM scheme. However, unlike the NDC-OFDM, GLIM-OFDM completely avoids the Hermitian symmetry at the input of IFFT as well as the accompanying loss in spectral efficiency. Consequently, the spectral efficiency of the proposed scheme becomes $\log_2(M)$ [bits/s/Hz], which is twice that of NDC-OFDM and DCO-OFDM schemes since Hermitian symmetry is no longer required to produce real-valued OFDM symbols. In this study, we consider $n_R = 4$ for ease of presentation, while a generalization is straightforward. We assume that the LEDs are operating within their dynamic range. Note that the operation in (3.1) is not subject to non-linear distortions.



4. PHYSICAL LAYER SECURITY IN OPTICAL GENERALIZED INDEX-MODULATED OFDM SYSTEMS

In visible light communication, channels are formed over the line-of-sight element and transmission occurs on these channels. Also, visible light cannot pass through opaque walls. For these reasons, VLC provides a more secure communication than RF in an indoor communication system. While physical layer security is an issue that is already considered in RF systems, it has become an essential issue on VLC with the emergence of VLC. Creating a protective field around the receiver, applying jamming signals to the eavesdropper, minimizing the correct information rate received by the eavesdropper by precoding at the transmitter are some of the methods used to ensure physical layer security. In this thesis, precoding is applied to the transmitter, while the authorized receiver reaches the correct information, the eavesdropper obtains the information with a terrible success rate, thus the system ensures physical layer security. As we will see in the following sections, while the information precoded in the transmitter is decoded and revealed correctly at the receiver, the signal that reaches the eavesdropper is in a corrupted state and the system's secrecy rate is high. In this study, three different precoding techniques are used which are zero-forcing, Bayesian estimation(MMSE) and secrecy key generation, respectively.

4.1 Precoded(ZF) Transmitter Aided PLS in GLIM OFDM Systems

With the aid of the legitimate user's (Bob) channel state information at the transmitter (CSIT), the BER performance of Bob is minimized over the provided co-channel interference-free and low complexity transmission between the source and Bob. On the other hand, the BER of the eavesdropper (Eve) is degraded significantly. To achieve the above objective, the precoding matrix \mathbf{P} has to ensure that no energy

leakage among the receiving PDs. For this purpose, the ZF precoding or the MMSE precoding may be used. We adopt the ZF precoding in this work whose precoding matrix \mathbf{P} is constructed from the pseudo-inverse of Bob's channel \mathbf{H}_B as

$$\mathbf{P} = \beta (\mathbf{H}_B^T \mathbf{H}_B)^{-1} \mathbf{H}_B^T \quad (4.1)$$

where $\beta = \sqrt{N_r / \text{trace}(\mathbf{P}^T \mathbf{P})}$ is a normalizing factor. It can eliminate the co-channel interference among the receiving PDs completely by preprocessing the source signal $\mathbf{x} = [x_{k,R}^+, x_{k,R}^-, x_{k,I}^+, x_{k,I}^-]^T \in R^{n_R \times 1}$ before its transmission. Consequently, a low-complexity signal stream estimation of \mathbf{x} becomes possible at the receiver of the legitimate user (Bob), independent of the channel parameters. However, since the channel \mathbf{H}_E between the source and an Eve is different from Bob's channel, the precoded source signal will be received by Eve with a jamming signal generated as a result of the precoding mismatch with Eve's channel.

After transmitting precoding, the time-domain, positive and real-valued OFDM sample vectors \mathbf{x} are converted into an optical signal \mathbf{u} transmitted from the activated LEDs, which can be written as

$$\mathbf{u} = \mathbf{P}\mathbf{x}. \quad (4.2)$$

where the signals emitted by the LEDs are indicated as the elements of \mathbf{u} . According to (1), for a given OFDM signal, only two out of four elements are non-zero, i.e., two LEDs remain inactive (turned off). In this way, the proposed scheme utilizes the index modulation concept for the active LED indices to transmit the complex OFDM signals.

4.2 Normalization of Powers at Transmitter

The signal components of \mathbf{u} , u_k 's in (4.2), arriving at each LED are real-valued variables taking values in $[-u_{\max}, u_{\max}]$, with substantial power fluctuations and a wide dynamic range. Hence, the positivity of the amplitudes, as well as the normalization of powers at the transmitter, should be ensured before transmission over the LEDs. For every channel realization, however, the normalized signal powers,

\bar{u}_k , $k = 1, 2, \dots, n_T$ ($n_T = 4$), driving each luminary, are subject to a power constraint $|\bar{u}_k - u_{dc}| \leq \alpha u_{dc}$, where u_{dc} is a dc(direct current) bias and $\alpha \in [0, 1]$ is a constant selected such that linearity is maintained over the LED operating range $[(1 - \alpha)u_{dc}, (1 + \alpha)u_{dc}]$. Consequently, the peak constrained signal driving k th LED can be determined as

$$\bar{u}_k = au_k + b, \quad (4.3)$$

where $a = \alpha u_{dc}/u_{\max}$ and $b = u_{dc}$. The term u_{\max} can be computed both at the transmit and Bob's receive unit as follows. Since the complete Bob's CSI, $\mathbf{H}_B \in \mathcal{R}^{N_r \times N_t}$, is known by the transmit unit and Bob's receiver, it can be seen from (4.2) that the norm of \mathbf{u} , for each LED combination for a given user location, can be upper bounded as

$$\begin{aligned} |\mathbf{u}| &= |\mathbf{P}\mathbf{x}| \\ &\preceq |\mathbf{P}| \mathbf{x} \\ &\preceq \rho_{\max} \det(\mathbf{P}) \mathbf{1}_{N_r} \equiv u_{\max} \mathbf{1}_{N_r} \end{aligned} \quad (4.4)$$

where, the symbol \preceq denotes component wise inequality between two vectors, and $|\cdot|$ around a matrix denotes component-wise absolute value and $\rho_{\max} \triangleq \rho \sqrt{E\{x_{\max}^2\}}$. Here, ρ is a constant and for a given dB level, it can be determined from $\text{dB} = 10 \log(1 + \rho^2)$. $x_{\max} \triangleq \max\{\bar{x}_{k,R}, \bar{x}_{k,I}\}$, where $\bar{x}_{k,R} = |x_{k,R}|$ and $\bar{x}_{k,I} = |x_{k,I}|$. It can be easily shown that $\bar{x}_{k,R}$ and $\bar{x}_{k,I}$ have folded Gaussian distribution having the following pdf

$$p_{\bar{x}_{k,R(I)}}(v) = \frac{2}{\sqrt{\pi}} e^{-v^2}, \quad v \geq 0. \quad (4.5)$$

It then follows easily that the pdf of x_{\max} is $p_{x_{\max}}(v) = 2\sqrt{2/\pi} \text{erf}(v/\sqrt{2}) \exp(-v^2/2)$ and $E\{x_{\max}^2\} = (0/5 - \frac{1}{\pi}) = 0.8183$.

Finally, the signal observed at the N_r PDs of Bob (B) and Eve (E) after propagation through their respective channels may be written as

$$\mathbf{y}_B = \mathbf{s}_B + b\mathbf{H}_B \mathbf{1}_{N_t} + \mathbf{n}_B \quad (4.6)$$

$$\mathbf{y}_E = \mathbf{s}_E + b\mathbf{H}_E \mathbf{1}_{N_t} + \mathbf{n}_E \quad (4.7)$$

where,

$$\mathbf{s}_B \triangleq \mathbf{H}_B \mathbf{P} \mathbf{x} = \beta \mathbf{x}$$

$$\mathbf{s}_E \triangleq \mathbf{H}_E \mathbf{P} \mathbf{x} = \beta \mathbf{H}_E (\mathbf{H}_B^T \mathbf{H}_B + \epsilon \mathbf{I}_{N_r})^{-1} \mathbf{H}_B^T \mathbf{x}$$

and, $\mathbf{y}_B, \mathbf{y}_E \in R^{n_R \times 1}$ are the vectors of received signals that contains the electrical signals obtained from PDs at the PDs Bob's and Eve's Rx units. In (4.6,4.7), $\mathbf{n}_B, \mathbf{n}_E \in R^{n_R \times 1}$ are the vectors of real-valued AWGN samples, that models the shot noise and thermal noise in the Bob's and Eve's chanel, with variances, σ_B^2 and σ_E^2 , respectively. Since, the dc-bias, u_{dc} , and the channel matrix, \mathbf{H}_B , between the source and Bob are known, u_{dc} can be suppressed before detection process. Consequently, the received signals (4.6) and (4.7) can be re-expressed as

$$\mathbf{y}_B = \beta \mathbf{x} + \mathbf{n}_B, \quad (4.8)$$

$$\mathbf{y}_E = \beta \mathbf{G} \mathbf{x} + \mathbf{n}_E, \quad (4.9)$$

where $\mathbf{G} \triangleq \mathbf{H}_E (\mathbf{H}_B^T \mathbf{H}_B + \epsilon \mathbf{I}_{N_r})^{-1} \mathbf{H}_B^T$.

4.3 Conditional Bayesian(MMSE) Estimation

A straightforward solution to the estimation problem formulated in (4.8) and (4.9) is the use of the ZF equalizer, which yields an estimate of \mathbf{x} simply as

$$\hat{\mathbf{z}}_{ZF} = \begin{cases} \frac{1}{\beta} \mathbf{y}_B, & \text{for BOB's transmisson} \\ \frac{1}{\beta} \mathbf{G}^{-1} \mathbf{y}_E & \text{for EVE's transmisson.} \end{cases} \quad (4.10)$$

After this operation, the receiver can determine the indices of the active LEDs and corresponding signals by selecting the higher magnitude signals from $\hat{\mathbf{x}}$ ZF [11]. Despite its simplicity, the ZF estimator can significantly enhance the noise power through the multiplication of \mathbf{n} with \mathbf{H}^{-1} ; furthermore, it does not consider the probability distribution of \mathbf{x} as a priori information and consequently, it may produce negative-valued estimates.

To overcome the aforementioned drawbacks of the ZF estimator, in this section, we propose a novel MMSE in a Bayesian setting by taking into account the prior information we have for the signal vector \mathbf{x} . The overall estimation scheme can be presented now as follows. Since the transmitting precoder is capable of perfectly separating the streams of $N_r(N_r = 4)$ parallel OFDM time samples at Bob's receiver, as seen from (4.8), a low complexity single stream estimation of these samples is facilitated at the receiver. Hence, given the indices of the active LEDs $i_1 \in \{1, 2\}$ and $i_2 \in \{3, 4\}$, (11) may be decomposed into

$$y_B(i_1) = \beta \bar{x}_{k,R} + n_B(i_1), \quad i_1 \in \{1, 2\} \quad (4.11)$$

$$y_B(i_2) = \beta \bar{x}_{k,I} + n_B(i_2), \quad i_2 \in \{3, 4\} \quad (4.12)$$

$$y_B(j) = n_B(j), \quad j \in \{1, 2, 3, 4\} \text{ and } j \neq \{i_1, i_2\}, \quad (4.13)$$

where $y_B(j)$ and $n_B(j)$ are the j , ($j = 1, 2, 3, 4$)th components of \mathbf{y}_B and \mathbf{n}_B , respectively. Consequently, for a given estimated LED indices pair (i_1, i_2) with $i_1 \in 1, 2$ and $i_2 \in 3, 4$, the conditional MMSE estimation of $\bar{x}_{k,R}$ and $\bar{x}_{k,I}$ can be estimated as

$$\hat{x}_{\text{MMSE}} = E\{x|y\}, \quad (4.14)$$

where, for the notational simplicity, we define $x \triangleq \bar{x}_{k,R(I)}^{((i_1, (i_2)))}$, $y \triangleq y_B(m)$ and $\hat{x}_{\text{MMSE}} \triangleq \hat{x}_{k,R(I)}^{(i_1, (i_1))}$,

The observation equation in (4.11) and (4.12) can be written with the simplified notation as

$$y = z + n \quad (4.15)$$

where $z = \beta x$.

The MMSE estimation of x is determined from (4.15) as,

$$\begin{aligned} \hat{x}_{\text{MMSE}} &= E\{x|y\} = \int_{-\infty}^{+\infty} v p_{x|y}(v, y) dv \\ &= \frac{1}{p_y(y)} \int_{-\infty}^{+\infty} v p_{y|x}(v, y) p_x(v) dv, \end{aligned} \quad (4.16)$$

where $p_x(v)$ and $p_y(y)$ are the pdfs of x and y , respectively; and $p_{y|x}(v, y)$ is the conditional pdf of y given x and pdf of x is a folded Gaussian and its pdf is given by (4.5). Hence, $p_z(v)$ can be expressed as

$$p_z(v) = \frac{1}{\sqrt{\pi}\beta^2} e^{-v^2/\beta^2}, \text{ for } t \geq 0. \quad (4.17)$$

The pdf of n can be written as

$$p_n(n) = \frac{1}{\sqrt{2\pi}\sigma_n^2} e^{-n^2/2\sigma_n^2}, \quad (4.18)$$

where σ_n^2 is the noise variance. Since we may assume that x is independent of n , y is the sum of two independent random variables and its pdf is

$$p_y(y) = \int_{-\infty}^{+\infty} p_z(\tau) p_n(y - \tau) d\tau \quad (4.19)$$

Substituting (4.35) and (4.18) into (4.19), we obtain

$$p_y(y) = \frac{2}{\sqrt{\pi}(2\sigma^2 + \beta^2)} \left(1 - Q \left(\frac{\beta y}{\sigma \sqrt{2\sigma^2 + \beta^2}} \right) \right) e^{-\frac{y^2}{2\sigma_n^2 + \beta^2}} \quad (4.20)$$

where $Q(x) = \frac{1}{\sqrt{\pi}\sigma_n^2} \int_x^{+\infty} e^{-t^2/2} dt$. From (4.15) and (4.18), it is easy to see that

$$p_{y|x}(v, y) = p_n(y - \beta v) = \frac{1}{\sqrt{\pi}\sigma_n^2} e^{-(y - \beta v)^2/2\sigma_n^2} \quad (4.21)$$

Finally, substituting (4.38) and (4.21) into (4.16), and after some algebra results in the following closed form expression of the MMSE estimator of x given y :

$$\hat{x}_{\text{MMSE}} = \frac{\sigma_n}{\sqrt{2\pi}(\beta^2 + 2\sigma_n^2)} \frac{e^{-\beta^2 y^2 (2\sigma_n^2 (\beta^2 + 2\sigma_n^2))}}{1 - Q(\beta y / (\sigma_n \sqrt{(\beta^2 + \sigma^2)}))} + \frac{\beta y}{\beta^2 + 2\sigma_n^2}. \quad (4.22)$$

The above expression shows that the MMSE estimator depends on the signal power $E\{x^2\} = 1/2$, the noise power σ_n^2 and the normalizing constant β . Now let the SNR is defined as $SNR = \beta^2 E\{x^2\} / \sigma_n^2$. We can then obtain \hat{x}_{MMSE} values from (4.22) at high SNR and low SNR regions as follows:

$$\hat{x}_{\text{MMSE}} = \begin{cases} \frac{1}{\beta} y, & \text{as } \sigma_n^2 \rightarrow 0 \\ E\{x\} = 1/\sqrt{\pi} & \text{as } \sigma_n^2 \rightarrow +\infty. \end{cases}$$

The MMSE estimates of $\bar{x}_{k,R}$ and $\bar{x}_{k,I}$, condition on (i_1, i_2) are determined from (4.22) as

$$\hat{x}_{k,R}^{(i_1)} = \left[\hat{x}_{\text{MMSE}}|_{y=y(i_1)} \right]^+, \quad \hat{x}_{k,I}^{(i_2)} = \left[\hat{x}_{\text{MMSE}}|_{y=y(i_2)} \right]^+ \quad (4.23)$$

where $[x]^+$ denotes $\max\{0, x\}$.

After finding the MMSE estimates of $\bar{x}_{k,R}$ and $\bar{x}_{k,I}$ for all $(i_1, i_2) \in \{(1, 3), (1, 4), (2, 3), (2, 4)\}$, the indices of the active LEDs are selected according to

$$\begin{aligned} \hat{i}_1 &= \arg \max_{i_1} |\mathbf{y}_B(i_1) - \beta \hat{x}_{k,R}^{(i_1)}|^2 \\ \hat{i}_2 &= \arg \max_{i_2} |\mathbf{y}_B(i_2) - \beta \hat{x}_{k,I}^{(i_2)}|^2. \end{aligned} \quad (4.24)$$

The \mathcal{R}/\mathcal{I} combiner then calculates the estimates the complex-valued time samples $x_k, k = 0, 1, \dots, N - 1$, as

$$\hat{x}_{k,R} = \begin{cases} \hat{x}_{k,R}^{(\hat{i}_1)} & \text{if } \hat{i}_1 = 1 \\ -\hat{x}_{k,R}^{(\hat{i}_2)} & \text{if } \hat{i}_1 = 2 \end{cases} \quad \hat{x}_{k,I} = \begin{cases} \hat{x}_{k,I}^{(\hat{i}_3)} & \text{if } \hat{i}_2 = 3 \\ -\hat{x}_{k,I}^{(\hat{i}_4)} & \text{if } \hat{i}_2 = 4 \end{cases} \quad (4.25)$$

After this point, classical OFDM processing steps such as serial-to-parallel (S/P) conversion, FFT, and M -ary demodulation are applied to obtain to detect the transmitted information.

On the other hand, exact analytical expressions for the optimal MMSE estimator of $\bar{\mathbf{x}}$ at Eve's receiver cannot be obtained analytically from the observation equation in (4.9), similar to the MMSE estimates obtained for Bob's receiver. However, note that condition on (i_1, i_2) , y_E in (4.9) can be expressed as

$$\mathbf{y}_E = \beta \mathbf{G}^{(i_1, i_2)} \bar{\mathbf{x}} + \mathbf{n}_E \quad (4.26)$$

where $\mathbf{G}^{(i_1, i_2)} = [\mathbf{g}_{i_1}, \mathbf{g}_{i_2}] \in \mathcal{R}^{n_R \times 2}$; \mathbf{g}_k for $k = 1, 2, 3, 4$, being the k th column of \mathbf{G} in (4.9) and $\bar{\mathbf{x}} = [\bar{x}_{k,R}, \bar{x}_{k,I}]^T$. As indicated earlier, $\bar{x}_{k,R}$ and $\bar{x}_{k,I}$ have folded Gaussian distribution having the pdf given by (4.5). Consequently, a linear MMSE

estimator (LMMSE)) $\hat{\bar{\mathbf{x}}}$ of $\bar{\mathbf{x}}$ can be found in closed form by means of the Bayesian Gauss-Markov theorem [40] as follows:

$$\hat{\bar{\mathbf{x}}}^{(i_1, i_2)} = \mathbf{C}_{\bar{\mathbf{x}}} \mathcal{G}^T (\mathcal{G} \mathbf{C}_{\bar{\mathbf{x}}}^{-1} \mathcal{G}^T + \sigma_n^2 \mathbf{I}_{n_R})^{-1} (\mathbf{x} - \mathcal{G} \mu_{\bar{\mathbf{x}}}) + \mu_{\bar{\mathbf{x}}}, \quad (4.27)$$

where $\mathcal{G} \triangleq \mathbf{G}^{(i_1, i_2)}$, and since the components of $\bar{\mathbf{x}}$ are independent folded Gauss random variables, $\mu_{\bar{\mathbf{x}}} = E\{\bar{\mathbf{x}}\} = [1/\sqrt{\pi}, 1/\sqrt{\pi}]^T$, $\mathbf{C}_{\bar{\mathbf{x}}} = E\{\bar{\mathbf{x}}\bar{\mathbf{x}}^T\} = [1, 0; 0, 1]$. Note that since \mathbf{y}_E and $\bar{\mathbf{x}}$ are not jointly Gaussian, the resulting LMMSE will not be optimal. But in practice, it is quite useful, being in a closed form and depending only on the means and co-variances. In addition, the covariance matrix and the mean vector of the LMMSE error vector $\epsilon = \mathbf{x} - \bar{\mathbf{x}}$, can also be obtained in closed form as

$$\begin{aligned} \mathbf{C}_\epsilon &= \left(\mathbf{C}_{\bar{\mathbf{x}}}^{-1} + \frac{\mathcal{G}^T \mathcal{G}}{\sigma_n^2} \right)^{-1}, \\ \mu_{\bar{\mathbf{x}}} &= \mathbf{0}. \end{aligned}$$

Finally, the indices of active LEDs and the corresponding estimate of $\hat{x}_{k,R}$ and $\hat{x}_{k,I}$ are obtained at Eve's site, similar to the previous steps as shown by (4.24), (4.25)

4.4 Further Enhancement of the PLC algorithm with Secrecy Key Generation

For further enhancement of the PLS capability of the previous technique based on transmitter preceding, we now consider a novel precoded-PLS technique with secret keying. Amplitude/phase modulated (APM) data symbols, $\mathbf{x}_F = [X_0, X_1, \dots, X_{N-1}]^T$, where $X_k = |X_k| \exp(j\theta_k)$, transmitted by the OFDM subcarriers in the frequency domain, are first encrypted with a random diagonal matrix $\Psi = \text{diag}(e^{j\psi_0}, e^{j\psi_1}, \dots, e^{j\psi_{N-1}})$, where $\{\psi_k\}$'s are called *cyclic shift encryption coefficients*. The resulted encrypted vector $\mathbf{c}_F = [C_0, C_1, \dots, C_{N-1}]^T$ can be generated in the frequency-domain by

$$\mathbf{c}_F = \Psi \mathbf{x}_F \quad (4.28)$$

where, the k th component of \mathbf{c}_F is

$$C_k = |X_k| e^{j(\theta_k + \psi_k)}.$$

$\{C_k\}'s$ provide strong physical layer security by changing the relationship between the physical waveform and the transmitted data bits. As explained shortly, ψ'_k 's are determined by means of a secret key sequence. Then, the encrypted OFDM message \mathbf{c}_F is decrypted first by the legitimate user at the receiver simply by the operation

$$\mathbf{x}_F = \Psi^H \mathbf{c}_F. \quad (4.29)$$

Then the data is demodulated by the classical OFDM receiver. However, at Eve's site, since the secret key information is not known, she will not be able to recover the original transmitted message \mathbf{x}_F in a reliable format. The main steps of the proposed encryption algorithm are now given as follows:

1. The most common way of realizing a point-to-point OWC link is utilizing visible light (VL) and infra-red (IR) LEDs in the downlink and uplink directions, respectively. During OFDM transmission, a Q -bit $\in \{64, 128, 256, \dots\}$ secret key sequence $b = (b_0 b_1, \dots, b_{Q-1})$ is generated at the receiver and send back to the transmitter via an IR uplink channel. Following the sharing of the secret key, the legitimate user receives encrypted data packets from the source while concurrently sharing the newly generated secret key through the IR channel for the next round of data transmission.

The issue of channel reciprocity does not create any problem in the VLC applications and inherently holds in Li-Fi systems even though the transceiver components (LED and PD) are distinct, unlike RF systems where a single antenna behaves either as a transmitter and receiver. It can be seen from the LoS channel expression given by the equation (3.6) that the channel coefficients solely depend on the geometrical parameters of the transmission environment and are independent of the transmitter's wavelength. It can be inferred that even under only LOS channel conditions, large-scale fading effects caused by the random orientation and mobility yields non-deterministic channel coefficients in practical OWC systems. Consequently, the reciprocity in OWC channels must hold in the LOS cases. Hence, there is no need for an additional data exchange to transmit the secret key information to the access point.

In addition, the critical issue as to how the transmitter and receiver can

retain the shared secret key while preventing the eavesdropper from acquiring it is directly related to the characteristics of the uplink IR channel. The directivity of the IR LEDs is intrinsically very high compared to VL LEDs due to their lack of illumination purpose [41]. Thus, the beam-width of the IR sources is significantly smaller as opposed to their VL counterparts. Furthermore, the upward direction of the IR LEDs, deployed on the legitimate user, obliges the eavesdropper to be located between the access point and the legitimate user. This requirement could become practically infeasible if the legitimate user is mobile hand-held equipment. Consequently, both the narrow-beam profile of the IR LEDs and the mobility of the user equipment will create inherent protection about the secret key information generated and sent to the source by the legitimate user.

2. For $L \in \{1, 2, \dots, 7\}$, the transmitter chooses randomly ν th secret key bit among the Q -bit secret key sequence, b , as the initial encryption bit and selects L bits sequentially $b_\nu = (b_\nu, b_{\nu+1}, \dots, b_{\nu+L-1})$, as the first encryption sequence, which is used to encrypt the first cyclic shift encryption coefficient ψ_0 . The value of the random number ν is updated every time the encryption of an OFDM symbols is completed before transmission to Bob. Note that, when the encryption bit subscript reaches to $Q - 1$, it is moved to the first position while shifting all others to the next position in a left circular cyclic shift. Subsequently, the cyclic shift encryption coefficients, $\psi_1, \psi_2, \dots, \psi_{N-1}$, are generated sequentially as described in the next item.
3. Given the encryption bit sequences $\{b_0, b_1, \dots, b_{N-1}\}$, generated initially with random bit position ν , the the cyclic shift encryption coefficients $\{\psi_k\}_{k=0}^{N-1}$ are determined by [42]

$$\psi_k = \alpha_k \bmod 2^\kappa + \frac{\alpha_k}{2^L} \quad (4.30)$$

where κ is a constant prime integer chosen as 3, 5, 7, ..., and α_k is the k th encryption value that is generated through binary-to-decimal conversion through b_k . Note that the first and second terms on the right-hand side of (4.30) represent the integer and the decimal parts of ψ_k , respectively, and L is related to

the resolution of the generated ψ_k 's. After generation of the Q -bit secret key sequence, the same ψ_k s, generated at the transmitter, encrypt the transmitted OFDM-APM symbols in frequency-domain according to (4.28) and decrypts them at the receiver according to (4.29). Hence, the security performance of the system is improved substantially against eavesdroppers on top of the physical layer security provided by the precoding.

4. To avoid the risk of randomly selected bit position being eavesdropped, during transmission from source to the legitimated receiver over the VLC channel, a technique based on the Chinese Remainder Theorem (CRT) is employed as described in [43]. We now explain this technique step-by-step with the following example:

(i) Two mutually prime integers m_1 and m_2 , that is when $m_1 \neq m_2$, $\gcd(m_1, m_2) = 1$, are shared with transmitter and the receiver.

(ii) At the transmitter, two integers r_1 and r_2 , are constructed by ν as $r_i = \nu \pmod{m_i}$, $i = 1, 2$, are transmitted to the receiver.

(iii) At the receiver, the congruence equations are constructed with the received integers as

$$\begin{aligned} \nu &\equiv r_1 \pmod{m_1} \\ \nu &\equiv r_2 \pmod{m_2} \end{aligned} \tag{4.31}$$

The CRT says that the unique $\nu \pmod{V}$ can be obtained for $V = m_1 * m_2$, as

$$\nu = c_1.V_1.y_1 \pmod{V} + r_2.V_2.y_2 \pmod{V} \tag{4.32}$$

where $V_i = V/m_i$ and $y_i = V_i^{-1} \pmod{m_i}$.

4.5 Achievable Secrecy Rate of the GLIM-OFDM System

We now consider the achievable secrecy rate of the MIMO wiretap channel of the GLIM-OFDM scheme, $R_{\text{GLIM-OFDM}}$, in the presence of an eavesdropper. Using the observation signals for Bob and Eve in 4.8 and 4.9, the achievable secrecy rate can

be expressed as

$$\begin{aligned}
R_{\text{GLIM-OFDM}} &= I(\mathbf{s}_B; \mathbf{y}_B) - I(\mathbf{s}_B; \mathbf{y}_E), \\
&= H(\mathbf{y}_B) - H(\mathbf{y}_B | \mathbf{s}_B) - \left(H(\mathbf{y}_E) - H(\mathbf{y}_E | \mathbf{s}_E) \right), \\
&= \frac{N_r}{2} \log_2 \left(\frac{\sigma_E^2}{\sigma_B^2} \right) - \left(H(\mathbf{y}_E) - H(\mathbf{y}_B) \right),
\end{aligned} \tag{4.33}$$

where $I(\cdot; \cdot)$, $H(\cdot)$ and $H(\cdot | \cdot)$ represent the mutual information, differential and conditional entropy, respectively, and

$$\begin{aligned}
H(\mathbf{y}_\times | \mathbf{s}_\times) &= \frac{N_r}{2} \log_2(2\pi e \sigma_\times^2) \\
H(\mathbf{y}_\times) &= - \int p(\mathbf{y}_\times) \log_2 p(\mathbf{y}_\times) \mathbf{d}\mathbf{y}_\times
\end{aligned} \tag{4.34}$$

where $p(\mathbf{y}_\times)$ is the probability density function (pdf) of \mathbf{y}_\times with $\times \in \{B, E\}$, [?].

As can be seen from (4.9), $p(\mathbf{y}_B)$ depends on the pdfs of the signal vector $\mathbf{x} = [x_{k,R}^+, x_{k,R}^-, x_{k,I}^+, x_{k,I}^-]^T \in R^{n_R \times 1}$ and the noise vector, \mathbf{n}_B , which has a Gaussian distribution with mean zero and covariance $\mathbf{C}_{n,B} = \sigma_B^2 I_{N_r}$. Assuming IFFT satisfies the normalization of $E\{\mathbf{x}_T^\dagger \mathbf{x}_T\} = N$, the elements of \mathbf{x}_T follow $\mathcal{CN}(0, 1)$ distribution for large N values. Hence, $x_{k,R}$ and $x_{k,I} \sim \mathcal{N}(0, 1/2)$ and consequently, all four components of \mathbf{x} are independent of each other and, due to the symmetry, have the following clipped Gaussian pdf.

$$p_{x_{k,R(I)}^\pm}(v) = \frac{1}{\sqrt{\pi\beta^2}} e^{-v^2/\beta^2} u(v) + \frac{1}{2} \delta(v), \tag{4.35}$$

where $u(v)$ and $\delta(v)$ represent the unit step and delta Dirac functions, respectively. The mean electrical power emitted from each LED of GLIM-OFDM scheme and the variance can be obtained as

$$I = E\{x_{k,R(I)}^\pm\} = \frac{1}{2\sqrt{\pi}}; \quad \sigma_{x_{k,R(I)}^\pm}^2 = \frac{1}{4} \left(1 - \frac{1}{\pi}\right). \tag{4.36}$$

Since all the components of \mathbf{x} and \mathbf{n}_B , as well as the random vectors \mathbf{x} and \mathbf{n}_B are independent of each other, the pdf of $\mathbf{y}_B = [y_1, y_2, y_3, y_4]^T$ can be expressed as

$$p(\mathbf{y}_B) = \prod_{i=1}^4 p_{y_i}(y), \tag{4.37}$$

where $y_i = \beta x_{k,R(I)} + n_i$ is the i th component of \mathbf{y}_B . Exact analytical expression for the pdf of y_i can be derived by the convolution theorem to calculate the sum of the independent random variables. After some algebra, for $i = 1, 2, 3, 4$, and $-\infty < y < +\infty$, it follows that

$$p_{y_i}(y) = 0.5 \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{y^2}{2\sigma_n^2}} + \frac{1}{\sqrt{\pi(2\sigma_n^2 + \beta^2)}} \left(1 - Q \left(\frac{\beta y}{\sigma_n \sqrt{2\sigma_n^2 + \beta^2}} \right) \right) e^{-\frac{y^2}{2\sigma_n^2 + \beta^2}}. \quad (4.38)$$

Consequently, using 4.37, the mutual information, in (4.33), between the source and Bob can be determined as

$$I(\mathbf{s}_B; \mathbf{y}_B) = - \sum_{i=1}^4 \int_{-\infty}^{\infty} p_{y_i}(y) \log_2(p_{y_i}(y)) dy - \frac{1}{2} \log_2(2\pi e \sigma_B^2). \quad (4.39)$$

Note that the exact evaluation of (4.39) is not feasible mathematically. However, this can be used to calculate the entropy for varying SNR values numerically. However, our extensive computer simulations showed that approximating the pdf $p_{y_i}(y)$ with a Gaussian distribution with the mean $\mu_{y_i} = \beta/(2\sqrt{\pi})$ and the variance $\sigma_{y_i}^2 = \frac{\beta^2}{4}(1 - \frac{1}{\pi}) + \sigma_n^2$, almost the same mutual information values are obtained for a wide range of SNRs. In the presence of Gaussian approximation, the mutual information formula becomes

$$I_{\text{approx}}(\mathbf{s}_B; \mathbf{y}_B) = 4 \frac{1}{2} \log_2 \left(1 + \frac{\frac{\beta^2}{4}(1 - \frac{1}{\pi})}{\sigma_{n_B}^2} \right). \quad (4.40)$$

As an example showing this approximation is valid, in Fig. 4.1, we compare the mutual information obtained numerically from (4.39) and approximately from (4.40) for the SNR range from -6 dB to 12 dB and show that these two curves almost coincide each other.

On the other hand, computation of the Eve's entropy, $H(\mathbf{y}_E)$ involves pdf of $\mathbf{y}_E = \beta \mathbf{G}\mathbf{x} + \mathbf{n}_E$, and becomes analytically infeasible. Hence to obtain the Eve's mutual information, we approximate the pdf of \mathbf{x} as a Gaussian distribution with mean vector $\mu_{\mathbf{x}} = \frac{1}{2\sqrt{\pi}} \beta \mathbf{G}\mathbf{1}$ and the covariance $C_{\mathbf{x}} = \frac{\beta^2}{4}(1 - \frac{1}{4\pi}) \mathbf{G}\mathbf{G}^T$. Consequently, the

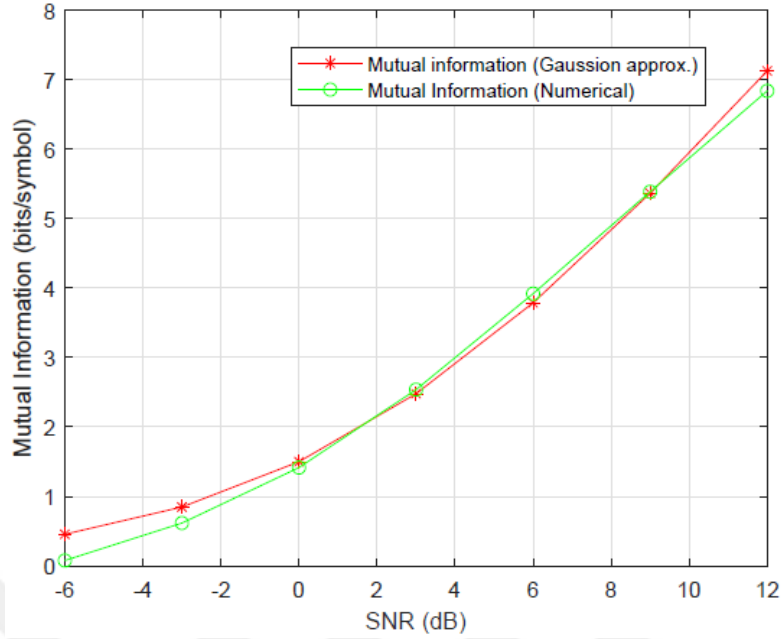


Figure 4.1 Comparison of the exact and Gaussian approximated mutual information

mutual information for Eve can be obtained as

$$I_{\text{approx}}(\mathbf{s}_E; \mathbf{y}_E) = \frac{1}{2} \log_2 \left(\det \left(I_4 + \frac{C_{\mathbf{x}}}{\sigma_{n_E}^2} \right) \right) \quad (4.41)$$

where $\mathbf{1} \triangleq [1, 1, \dots, 1]^T$, I_4 denotes a 4×4 diagonal matrix and G is defined in 4.8. Finally, the secrecy rate achievable for the GLIM-OFDM is obtained by substituting (4.41) and (4.40) in (4.33) as

$$R_{\text{GLIM-OFDM}} = I_{\text{approx}}(\mathbf{s}_B; \mathbf{y}_E) - I_{\text{approx}}(\mathbf{s}_E; \mathbf{y}_E). \quad (4.42)$$

Note that the achievable secrecy rate, determined from (4.42), based on the clipped Gaussian, is an upper bound. It does not yield the achievable secrecy rate because the OFDM time-domain signal samples are approximated as continuous random variables with the Gaussian distribution. Hence, the mutual information for continuous ensembles is not necessarily finite compared to the discrete ensembles whose entropies and mutual information take finite values and are limited by the alphabet size of the discrete source. Since the frequency-domain transmitted data symbols are discrete-valued random variables like M-PSK/M-QAM, the maximum achievable rate or the capacity of a GLIM-OFDM system is limited with $\log_2 M$ bits/symbol.

The capacity of such discrete-continuous memory-less channels of Bob and Eve, when the ML-based detection of data symbols is considered as in [44], can be expressed as

$$C_\chi = \log_2(M) - \frac{1}{M} \sum_{i=1}^M E_{\mathbf{n}_\times} \left\{ \log_2 \sum_{j=1}^M \exp \left(\Psi_\times(i, j) \right) \right\}, \quad \times \in \{\text{B}, \text{E}\} \quad (4.43)$$

where $\Psi_\times(i, j)$ is given by

$$\Psi_\times(i, j) = -\frac{\|x_F(i) - x_F(j) + n_\times\|^2 + \|n_\times\|^2}{\sigma_\times^2}.$$

and $x_F(i)$ is the i th alphabet value of MPSK/MQAM data symbols transmitted from one of the OFDM subcarriers. Consequently, the secrecy capacity of the optical GSSK can be determined as

$$C_{\text{GSSK}} = C_{\text{B}} - C_{\text{E}}. \quad (4.44)$$

Note that C_{GSSK} in (4.44) cannot be obtained analytically in a closed-form expression. However a reduced complexity information rate in bits per second between Alice-Bob and Alice-Eve can be computed based on the per bit mutual information $I_\times(b; \hat{b}_\times)$, $\times \in \{\text{B}, \text{E}\}$. The mutual information is measured for the proposed GLIM-OFDM system between the input bits $b \in \{0, 1\}$ and the corresponding demodulated output bits $\hat{b}_\times \in \{0, 1\}$. Hence, the resulting binary input-output channels between Alice-Bob, and Alice-Eve can be modeled as a BSC with crossover probabilities ϵ_{B} and ϵ_{E} , respectively. Both achieve equal input probabilities. That is $P(0) = P(1) = 1/2$. Consequently, both channels achieve the channel capacity exactly.

Computed with respect to this specific input distribution, the secrecy capacity of an optical GLIM-OFDM wiretap channel yields

$$\begin{aligned} C_{\text{GLIM-OFDM}} &= I_{\text{B}}(b; \hat{b}_{\text{B}}) - I_{\text{E}}(b; \hat{b}_{\text{E}}), \\ &= H_{\text{B}}(b) - H_{\text{B}}(b|\hat{b}_{\text{B}}) - H_{\text{E}}(b) + H_{\text{E}}(b|\hat{b}_{\text{E}}), \end{aligned} \quad (4.45)$$

where $H_\chi(b) = -\sum_{m=0}^1 P(m) \log_2 P(m)$ denotes the entropy of the input bits with respect to the input probabilities $P(m)$, $m = 1, 2$. On the other hand, $H_\chi(b|\hat{b}_\chi)$

represents conditional entropy and for a BSC it is given by

$$H_\chi(b|\hat{b}_\chi) = -\epsilon_\chi \log_2 \epsilon_\chi - (1 - \epsilon_\chi) \log_2(1 - \epsilon_\chi). \quad (4.46)$$

Hence, by substituting (4.46) into (4.45), and exploiting $H_\chi(b) = 1$, since the input bits are equally likely, the exact achievable secrecy capacity for L , the number of bits transmitted per APM symbol, becomes

$$C_{\text{GLIM-OFDM}} = L \left(\epsilon_B \log_2 \epsilon_B + (1 - \epsilon_B) \log_2(1 - \epsilon_B) - \epsilon_E \log_2 \epsilon_E - (1 - \epsilon_E) \log_2(1 - \epsilon_E) \right). \quad (4.47)$$

The crossover probabilities ϵ_χ in (4.47) correspond to the BER of the APM data symbols in the frequency-domain.



5. CHANNEL ESTIMATION IN OPTICAL GENERALIZED INDEX-MODULATED OFDM SYSTEMS

In the PLS section of the thesis, first, the PLS techniques for GLIM OFDM systems are presented. Then we concluded that one of the critical problems is to transmit channel state information from the receiver to the transmitter to implement precoding successfully. In Fig. 5.1, the block diagram of GLIM OFDM with precoder and channel estimation is given. As we can see from Fig. 5.1, at the first step, we need to estimate the channel at the receiver side and send it the channel state information (CSI) back to the precoder at the transmitter side of the system by a different uplink infrared channel. Therefore, the correctness of the estimation of the channels is vital for the correct operation of the system. In this thesis, we propose a channel estimation algorithm with a low computational complexity that ensures a BER for the system, almost the same as the scenario when the channel is already known. It also provides an MSE performance that has nearly reached the CRLB.

In GLIM OFDM, the positive and real-valued time-domain signal vector of the time-domain components arriving at the receiver's FFT input can be expressed as:

$$\mathbf{y}_k = \mathbf{H}\mathbf{x}_k + n_k \quad (5.1)$$

where the $\mathbf{x}_k \in \mathcal{R}^{4 \times 1}$ vector represents the time-domain sample vectors generated at the IFFT output at the transmitter side of the system for each $k = 0, 1, \dots, N - 1$, and $\mathbf{n}_k \in \mathcal{R}^{4 \times 1}$ represents the additive white Gaussian noise vector whose components are statistically independent. To estimate the channel matrix within each given time frame, the signal vectors $\mathbf{X} = [\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}]$ generated from the pilot symbols will be assumed to be known at the receiver. In this case, the receiver signal

can be expressed as:

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N}, \quad (5.2)$$

and, $\mathbf{Y} = [\mathbf{Y}_0, \mathbf{Y}_1, \dots, \mathbf{Y}_{N-1}] \in R^{4 \times N}$ and $\mathbf{N} = [\mathbf{n}_0, \mathbf{n}_1, \dots, \mathbf{n}_{N-1}] \in R^{4 \times N}$ Using classical matrix relations, the matrix \mathbf{Y} can be expressed as a $4N$ dimensional vector as follows:

$$\mathbf{y} = \mathbf{Q}\mathbf{h} + \mathbf{n} \quad (5.3)$$

where $\mathbf{y} = \text{vec}(\mathbf{Y})$, $\mathbf{n} = \text{vec}(\mathbf{N})$ and $\mathbf{Q} = \mathbf{X}^T \otimes \mathbf{I}_r$ and \otimes shows the Kronocker product. Using the linear observation equation in 5.3, the linear minimum mean-square estimation (LMMSE) for the unknown channel \mathbf{h} is obtained as follows:

$$\hat{\mathbf{h}}_{LMMSE} = \mathbf{Q}^T (\mathbf{Q}\mathbf{Q}^T + (1/\rho)\mathbf{I}_r) \mathbf{y} \quad (5.4)$$

and, where $\rho = I/\sigma_n^2$ ve $I = 1/\text{sqr}(2\pi)$ is equal to the square of the statistical mean of the sample values $|x_{k,R}|$ and $|x_{k,I}|$ with a folded-Gaussian probability distribution. If the error vector in the channel estimation calculated with this relationship is $\mathbf{e} = \hat{\mathbf{h}}_{LMMSE} - \mathbf{h}$, then MSE is defined as:

$$MSE = E \left\{ (\hat{\mathbf{h}}_{LMMSE} - \mathbf{h})^T (\hat{\mathbf{h}}_{LMMSE} - \mathbf{h}) \right\}.$$

Using this definition, the mean square error in the channel estimation considered is obtained as follows:

$$MSE = \frac{1}{\sqrt{2\pi}} \left(1 - \mathbf{Q}^T (\mathbf{Q}\mathbf{Q}^T + (1/\rho)\mathbf{I}) \mathbf{Q} \right).$$

5.1 Cramer-Rao Lower Bound in Channel Estimation

The lower limit of the mean error in the obtained channel estimation is determined by the CRLB and this limit is calculated as following:

$$MSE = E \{ (\hat{\mathbf{h}} - \mathbf{h})^T (\hat{\mathbf{h}} - \mathbf{h}) \geq \mathbf{I}(\mathbf{h})^{-1} \}. \quad (5.5)$$

where $\hat{\mathbf{h}} \triangleq \hat{\mathbf{h}}_{LMMSE}$ and $\mathbf{I}^{-1}(\mathbf{h})$ are named *Cramer-Rao* lower-bound. It is calculated as:

$$\mathbf{I}(\mathbf{h}) = E \left\{ \frac{\partial^2 \ln p(\mathbf{y}; \mathbf{h})}{\partial \mathbf{h}^2} \right\} \quad (5.6)$$

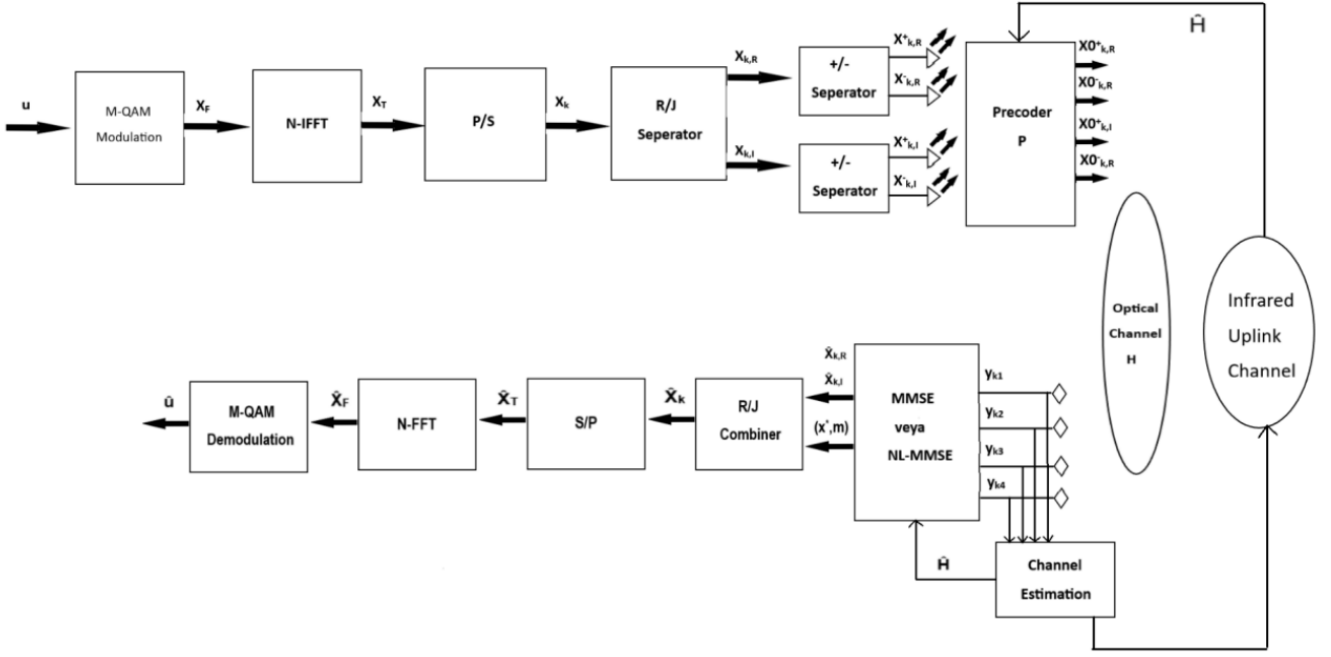


Figure 5.1 Block Diagram of the GLIM-OFDM with Precoder and Channel Estimation

In this relation, $p(\mathbf{y}; \mathbf{h})$ shows the probability density function of the signal arriving at the receiver modeled as $\mathbf{Qh} + \mathbf{w}$ and it can be expressed as:

$$p(\mathbf{y}; \mathbf{h}) \sim \exp \left\{ \frac{1}{\sigma_w^2} (\mathbf{y} - \mathbf{Qh})^T (\mathbf{y} - \mathbf{Qh}) \right\}$$

By taking the 2nd partial derivative of $p(\mathbf{y}; \mathbf{h})$ as in 5.6, the following expression is obtained for I:

$$\mathbf{I}(\mathbf{h}) = \frac{1}{\sigma_w^2} \mathbf{Q}^T \mathbf{Q}.$$

Finally, the Cramer-Rao lower bound for the channel estimation obtained with the help of this expression is found as follows:

$$MSE \geq \sigma_w^2 \text{trace}((\mathbf{Q}^T \mathbf{Q})^{-1}). \quad (5.7)$$

Figure 5.1 represents the new GLIM-OFDM scheme which has the precoder and channel estimation.

6. COMPUTER SIMULATIONS

6.1 Physical Layer Security Simulations

In this section, the simulation results for the PLS performance of the proposed GLIM OFDM-based indoor LiFi system are presented. The BER performance of the legitimate user and eavesdropper are investigated. We consider a $n_T = n_R = 4$, (4×4) MIMO-VLC system that is operating in a $3\text{m} \times 3\text{m} \times 3\text{m}$ typical room. We assume four luminaries on the ceiling whose coordinates are given by

$$\text{LED}_{\text{location}}(x, y) = \begin{bmatrix} 50 & -50 & 50 & -50 \\ 50 & 50 & -50 & -50 \end{bmatrix}^T \text{ cm.} \quad (6.1)$$

where x and y denote the horizontal axes. The FOV semi-angle and area of the PD are 70° and 1 cm^2 , respectively. The PDs are located at a height of 0.8 m , which is the standard height of a table. Luminaries and PDs are assumed to be facing vertically downward to the floor and upward to the ceiling, respectively. The half-power and half-angle of the LEDs and the areas of the PDs are assumed to be $\Phi_{1/2} = 2 = 60^\circ$; $\Psi_{1/2} = 70^\circ$; $A_{PD} = 1 \text{ cm}^2$. Then, the VLC channel coefficients between all the LEDs and PDs are found in accordance with (3.6). The BER vs. SNR performance curves are obtained for Bob and Eve in various VLC channel configurations and QPSK signal constellations, where the number of OFDM subcarriers are chosen as $N = 128$. The Bob and the Eve are located according to two configurations named as Config A (PDs of Bob are in the center of the table with an equidistant spacing of 0.4 m) and Config B (PDs of Bob are located at one of the corners of the room with an equidistant spacing of 0.4 m). PDs of Eve are positioned according to

$$\text{Config A : PDs of Bob}_{\text{location}}(x, y) = \begin{bmatrix} 20 & -20 & 20 & -20 \\ 20 & 20 & -20 & -20 \end{bmatrix}^T \text{ cm.}$$

$$\text{ConfigB : PDs of Bob}_{\text{location}}(x, y) = \begin{bmatrix} 150 & 150 & 110 & 110 \\ 150 & 110 & 150 & 110 \end{bmatrix}^T \text{ cm.}$$

For each configuration, we consider two critical positions for Eve's locations. Namely, in Config A, Eve is either located near the center of the room or at a point near the corner on the diagonal side of the room. Similarly, in Config B, the Eve's PDs are positioned on a table with different heights of 40 cm and 80 cm located close to the room's center. Due to the locations of Eve in Config A, Bob and Eve will have some spatially separated different channel gains. Whereas, in Config B, it can be expected that Eve's channel coefficients will have a spatial similarity for half of the LEDs that will affect the BER performance of the system.

In Fig 6.1, the BER performances of Bob and Eve are compared with and without a secret key as a function of SNR for Config A and Config B. The difference in the BER performance with a secret key and no secret key is highlighted in Fig 6.2.

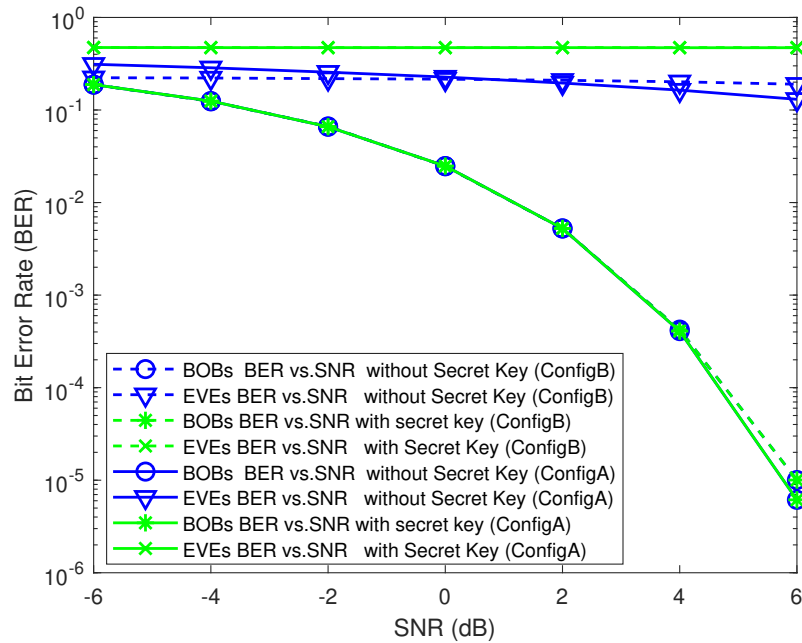


Figure 6.1 Comparison of BER performances of Bob and Eve with and without secret key as a function of SNR for 1st scenario

The mutual information of Bob and Eve and the actual achievable secrecy capacity

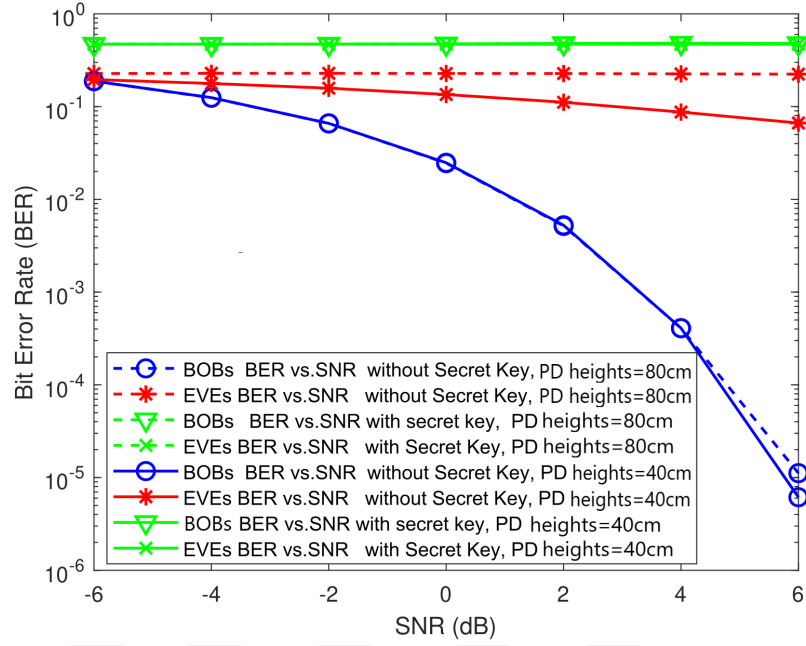


Figure 6.2 Comparison of BER performances of Bob and Eve with and without secret key as a function of SNR for 2nd scenario

of Bob is investigated in Fig 6.3 for a scenario for which the respective channels of Bob and Eve are chosen as

$$\mathbf{H}_B = 10^{-4} \times \begin{bmatrix} 0.6888 & 0.5559 & 0.5559 & 0 \\ 0.5559 & 0.6888 & 0 & 0.5559 \\ 0.5559 & 0 & 0.6888 & 0.5559 \\ 0 & 0.5559 & 0.5559 & 0.6888 \end{bmatrix}, \quad (6.2)$$

$$\mathbf{H}_E = 10^{-4} \times \begin{bmatrix} 0.9226 & 0.7964 & 0.7964 & 0.6888 \\ 0.7964 & 0.9226 & 0.6888 & 0.7964 \\ 0.7964 & 0.6888 & 0.9226 & 0.7964 \\ 0.6888 & 0.7964 & 0.7964 & 0.9226 \end{bmatrix}. \quad (6.3)$$

As can be seen from Fig. 6.3, while the mutual information of Bob reaches its ultimate information rate $I_B = \log_2 4 = 2$ bits/QPSK symbol at maximum 14 dB

SNR, the mutual information of Eve cannot exceed 0.2 bits/sec per QPSK symbol within this SNR range. Consequently, the achievable capacity of Bob reaches its actual capacity closed to 14 dB.

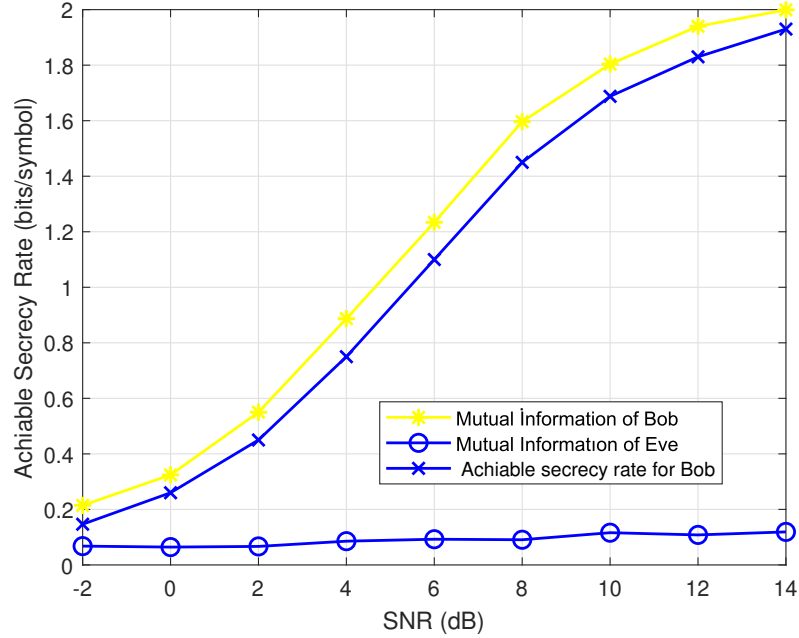


Figure 6.3 Mutual informations of Bob and Eve and achievable secrecy rate for Bob

We compare the achievable secrecy rates obtained by the observation in the time-domain samples and using clipped Gaussian distribution and the one obtained in the frequency-domain approach. Fig. 6.4 clearly shows that the time domain approach based on clipped Gaussian distribution gives an upper bound on the achievable capacity.

Finally, Figure 6.5 shows a 2D contour plot of the BER values of Eve for the scenario that when Bob is placed in the center of the room and Eve is navigating on the grid in the room. It is an output of the BER values obtained by using the channels created for every position of Eve. As we can see from Figure 6.5, there is a symmetry that is caused due to the symmetric structure of the channels produced in channel estimation. The simulations for this figure were created in a (3x3x3)m room when Bob's channel, HB, was fixed and Eve's channel was variable. In the simulations, most of the BER values of Eve are over 0.1, and Bob's BER values are over 10^{-5} .

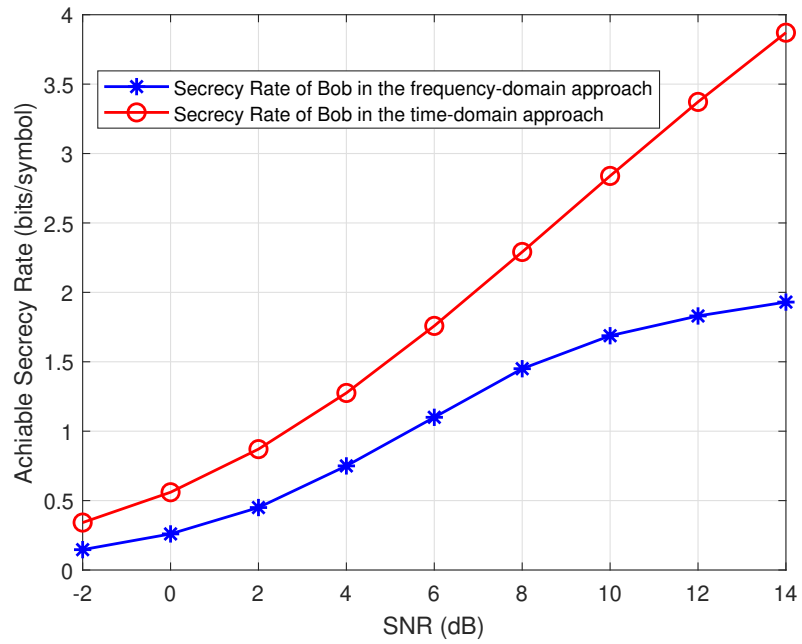


Figure 6.4 Comparison of Bob’s achievable secrecy rates obtained in the frequency and the time-domains

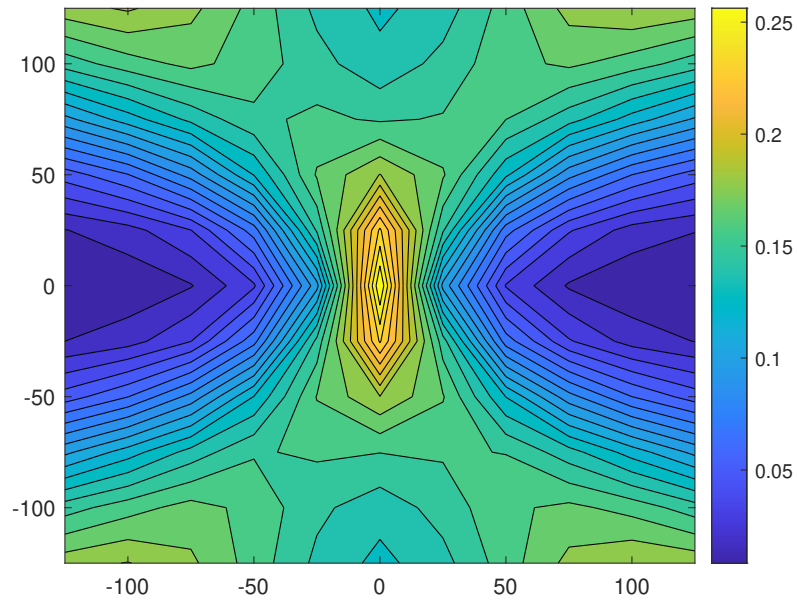


Figure 6.5 Contour plot of the BER values of Eve when Bob is at center and Eve is mobile in the room.

6.2 Channel Estimation Simulations

In this study, as VLC channel model, channels created by using line-of-sight element between the illuminators (LED) placed on the ceiling in a closed room which is in

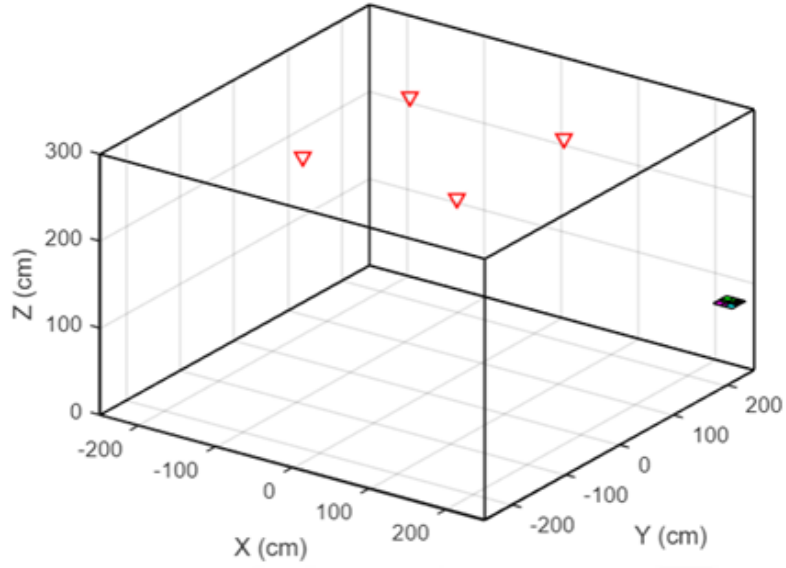


Figure 6.6 Simulation of the room for Example 1

the form of a square prism (5x5x3 m) and photodetectors (PD) placed at the corners of a table in the center of the room are used. As can be seen from Figure 6.6, in this scenario, the red inverted triangles represent the LEDs on the ceiling and the colored squares represent the PDs on a table (10x10x80 cm) on the floor.

6.2.1 Simulation Examples

Configuration parameters of the simulated room is shown in Table 6.1

Example 1:

LED coordinates: [130 70 300 ; 130 -130 300 ; -70 -130 300 ; -70 70 300]

PD coordinates: [-14 -24 80 ; -14 -14 80 ; -24 -24 80 ; -24 -14 80]

$$\mathbf{H}_{\text{LoS}} = 1.0e - 05 * \begin{bmatrix} 0.2185 & 0.0444 & 0.0213 & 0.0557 \\ 0.2026 & 0.0411 & 0.0202 & 0.0536 \\ 0.2294 & 0.0453 & 0.0223 & 0.0599 \\ 0.2124 & 0.0420 & 0.0211 & 0.0576 \end{bmatrix}$$

where \mathbf{H}_{LoS} is the LoS channel matrix. Figure 6.6 illustrates the simulated room for given values.

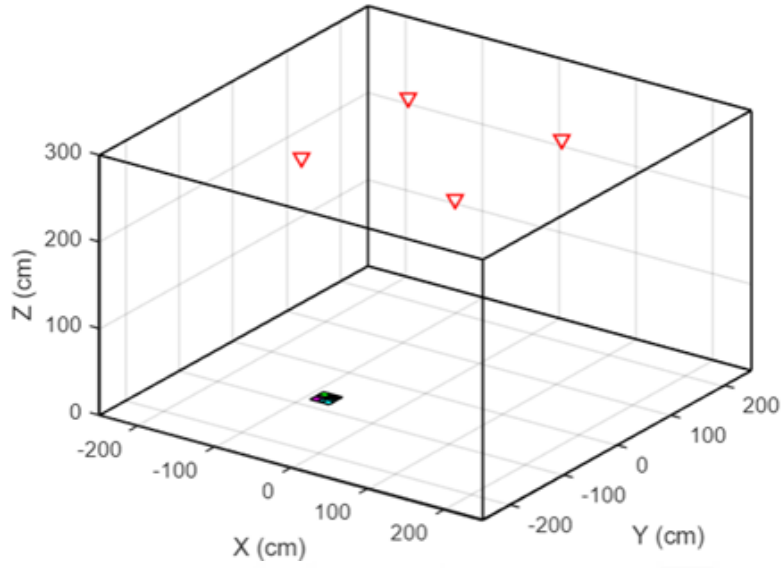


Figure 6.7 Simulation of the room for Example 2

Example 2:

LED coordinates: [130 70 300 ; 130 -130 300 ; -70 -130 300 ; -70 70 300]

PD coordinates: [-214 -484 80 ; -214 -474 80 ; -224 -484 80 ; -224 -474 80]

$$\mathbf{H}_{\text{LoS}} = 1.0e - 05 * \begin{bmatrix} 0.0688 & 0.3327 & 0.3104 & 0.0666 \\ 0.0746 & 0.3529 & 0.3286 & 0.0722 \\ 0.0670 & 0.3141 & 0.3290 & 0.0684 \\ 0.0726 & 0.3327 & 0.3489 & 0.0742 \end{bmatrix}$$

where \mathbf{H}_{LoS} is the LoS channel matrix. Figure 6.7 illustrates the simulated room for given values.

6.2.2 Computer Simulation Results of Channel Estimation

For channel estimation, it is necessary to add pilot symbols. For this purpose, different subcarriers in the frequency domain of OFDM are generally reserved for carrying pilot symbols. However, in the VLC-based OFDM system proposed in this paper, all sub-carriers of the first OFDM signal in a given OFDM time frame are allocated to pilot symbols. In a given frame, optical channels do not change much. By utilizing this property of optical channels, data transmission occurs from all sub-carriers of other OFDM signals in the frame. Depending on this configuration, the channel is

Parameters	Values
Room dimensions	5x5x3 m
Number of LEDs	4
Number of chips per LED	9
Model of chips	Cree Xlamp®MC-E
Power for each chip	5W
LED viewing angle	120°
PD viewing angle	85°
PD surface area	1 cm ²

Table 6.1 Configuration Parameters

estimated using the LMMSE-based estimation algorithm described in the previous section, and the data transmitted at the receiver in the frequency region using the estimated channel values are obtained with a certain error performance with the help of the data detection process within each OFDM frame.

In this subsection, both the MSE performance of the channel estimation algorithm realized at the receiver of the VLC system and the Cramer-Rao lower bound that this performance can reach, and also the data detection performance of the system in the transmission over the analytically obtained optical channel are examined. In Figure 6.8, the MSE error performances of the channel estimation realized in 4QAM, 8QAM and 16QAM modulated communication are obtained as functions of the signal-to-noise ratio in the system. The most important conclusions drawn from Fig. 6.8 are that the MSE performance of the proposed channel estimation algorithm is very suitable for real applications and is almost entirely independent of the different levels of modulation techniques used. It is also seen that the MSE performance has nearly reached the Cramer-Rao lower bound. From these calculations and the obtained results, it is concluded that the proposed channel estimation algorithm works very effectively and also the computational complexity is minimal for the algorithm.

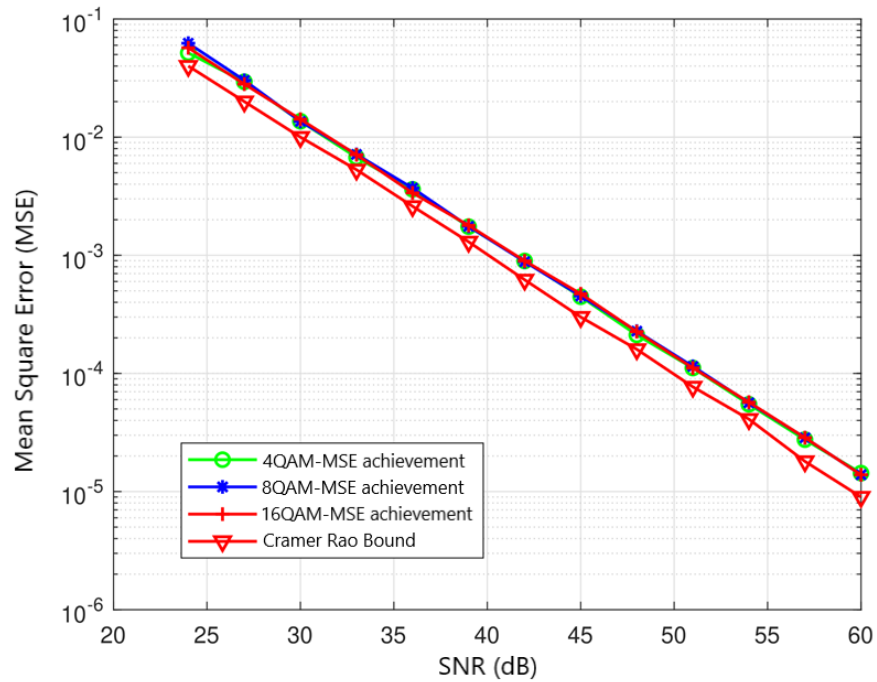


Figure 6.8 Channel Estimation MSE Performance and Cramer-Rao Lower Bound

In Figure 6.9, the BER performance of the data detection process performed at the receiver for the 4QAM, 8QAM and 16QAM modulations is examined as a function of the signal-to-noise ratio, using the predicted channel information. As can be clearly seen from this figure, the BER performance level of the system that can be reached under the presence of channel estimation errors is very high. In other words, it can be seen from Figure 6.9 that at each modulation level, the BER curves obtained for cases where the channel is perfectly known and channel estimation is used almost overlap.

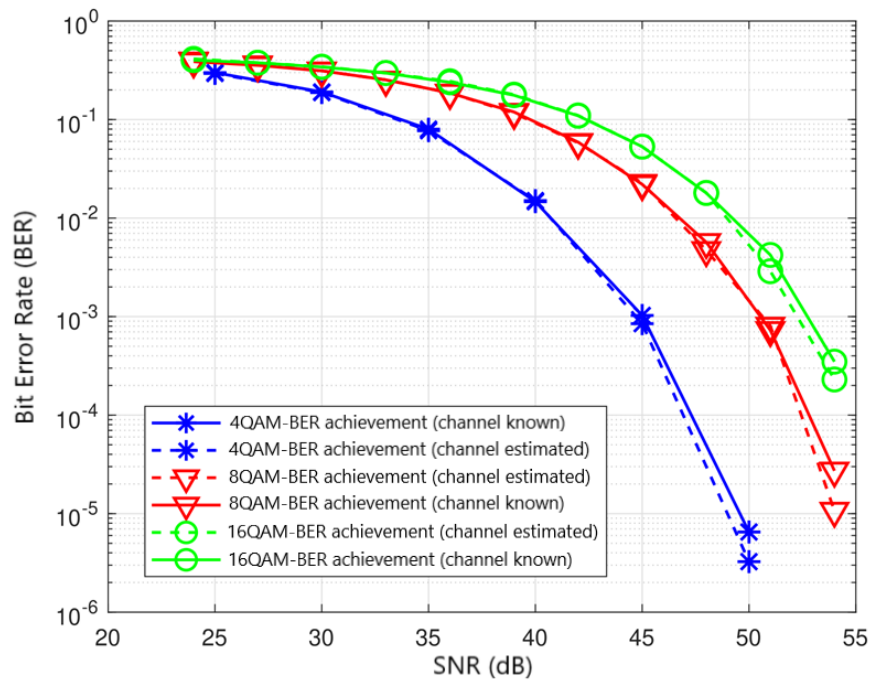


Figure 6.9 GLIM OFDM BER Performance Under Channel Estimation Error

7. CONCLUSIONS

This thesis proposes a new and novel PLS algorithm, and its achievable secrecy rate is improved through different techniques. The MMSE estimation method is adopted in the Bayesian setting to solve the OFDM sample estimation problem. Finally, a further enhancement using secrecy key generation is introduced in the last step. BER performances of Bob and Eve are compared for two configurations with and without the secret key, and it is shown that the BER performance of Eve is degraded further in the presence of a secret key. Also, the mutual information of Bob and Eve are compared and shown that when Bob reaches its ultimate information rate, at the same SNR range, Eve's mutual information stays very low. The achievable secrecy rates are compared for the frequency and time-domain approaches, and it is clearly shown that the time domain approach yields an upper bound on the achievable capacity. In the receivers of such wireless communication systems, the transmitted optical channel must be accurately estimated and monitored to detect the transmitted data accurately. Hence, within the scope of the thesis, a new pilot-based computationally efficient channel estimation technique is proposed for efficient estimation of the optical channel of a GLIM-OFDM system, operating under the effect of additive Gaussian noise. In addition, the Cramer-Rao lower bound, which is a measure of the estimation ability of the algorithm, is derived analytically. The computer simulation studies investigated the bit error rate and the mean-square error performances of the developed pilot-based channel estimation algorithm. It is concluded that the MSE performance of the proposed channel estimation algorithm is very suitable for real applications and is almost entirely independent of the different levels of modulation techniques used. When the outputs are examined, it is seen that the BER performance obtained as a result of the channel estimation is very close to the BER performance when the channel is known perfectly.

BIBLIOGRAPHY

- [1] F. Miramirkhani and M. Uysal, "Channel modeling and characterization for visible light communications," *IEEE Photon. J.*, vol. 7, no. 6, Dec. 2015.
- [2] Y. Tanaka, T. Komine, S. Haruyama, and M. Nakagawa, "Indoor visible communication utilizing plural white LEDs as lighting," in *Proc. 12th IEEE Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, vol. 2, Sep. 2001, pp. F-81–F-85.
- [3] J. Armstrong and A. J. Lowery, "Power efficient optical OFDM," *Electron. Lett.*, vol. 42, no. 6, pp. 370–372, Mar. 2006.
- [4] N. Fernando, Y. Hong, and E. Viterbo, "Flip-OFDM for optical wireless communications," in *Proc. IEEE Inf. Theory Workshop, Paraty, Brazil, Oct. 2011*, pp. 5–9.
- [5] D. Tsonev and H. Haas, "Avoiding spectral efficiency loss in unipolar OFDM for optical wireless communication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 3336–3341.
- [6] M. S. Islim, D. Tsonev, and H. Haas, "On the superposition modulation for OFDM-based optical wireless communication," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Orlando, FL, USA, Dec. 2015, pp. 1022–1026.
- [7] Q. Wang, Z. Wang, and L. Dai, "Multiuser MIMO-OFDM for visible light communications," *IEEE Photon. J.*, vol. 7, no. 6, pp. 1–11, Dec. 2015.
- [8] R. Mesleh, H. Elgala, and H. Haas, "Optical spatial modulation," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 3, no. 3, pp. 234–244, Mar. 2011.
- [9] C. He, T. Q. Wang, and J. Armstrong, "Performance comparison between spatial multiplexing and spatial modulation in indoor MIMO visible light communication systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
- [10] Y. Li, D. Tsonev, and H. Haas, "Non-DC-biased OFDM with optical spatial modulation," in *Proc. IEEE 24th Ann. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, London, U.K., Sep. 2013, pp. 486–490.
- [11] K. Abe, C.-J. Ahn, T. Omori, and K.-Y. Hashimoto, "Spatial performance of color clustered VLC-MIMO due to incompleteness of color filters," in *Proc. Int.*

- Symp. Intell. Signal Process. Commun. Syst. (ISPACS), Nusa Dua, Indonesia, Nov. 2015, pp. 417–421.
- [12] Y. Chen and M. Jiang, “Joint colour-and-spatial modulation aided visible light communication system,” in Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring), Nanjing, China, May 2016, pp. 1–5.
- [13] W. Xu, J. Wang, H. Shen, and H. Zhang, “Multi-colour LED specified bipolar colour shift keying scheme for visible light communications,” *Electron. Lett.*, vol. 52, no. 2, pp. 133–135, Jan. 2016.
- [14] P. Luo et al., “Experimental demonstration of RGB LED-based optical camera communications,” *IEEE Photon. J.*, vol. 7, no. 5, pp. 1–12, Oct. 2015.
- [15] A. H. Azhar, T. A. Tran, and D. O’Brien, “A gigabit/s indoor wireless transmission using MIMO-OFDM visible-light communications,” *IEEE Photon. Technol. Lett.*, vol. 25, no. 2, pp. 171–174, Jan. 15, 2013.
- [16] S. Cho, G. Chen, and J. P. Coon, “Physical layer security in visible light communication systems with randomly located colluding eavesdroppers,” *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 768–771, Oct. 2018.
- [17] A. Arafa, E. Panayirci, and H. V. Poor, “Relay-aided secure broadcasting for visible light communications,” *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 4227–4239, Jun. 2019.
- [18] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
- [19] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.
- [20] A. D. Wyner, “The wire-tap channel,” *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [21] M. A. Arfaoui et al., “Physical Layer Security for Visible Light Communication Systems: A Survey,” in *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1887–1908, thirdquarter 2020, doi: 10.1109/COMST.2020.2988615.
- [22] D. Li, L. Zhang and J. Qiu, “High security chaotic multiple access scheme for VLC systems”, Proc. ITNAC’16, pp. 133-135, Dec. 2016.

- [23] H. Lu, L. Zhang and X. Liu, "High-security colour shift keying modulation scheme with chaos-based constellation rotation for VLC system", Proc. ASID'16, pp. 20-24, Sept. 2016.
- [24] Y. M. Al-Moliki, M. T. Alresheedi and Y. Al-Harthi, "Physical-layer security against known/chosen plaintext attacks for OFDM-based VLC system", IEEE Commun. Lett., vol. 21, no. 12, pp. 2606-2609, Dec. 2017.
- [25] Z. Che, J. Fang, Z. L. Jiang, X. Yu, G. Xi and Z. Chen, "A physical-layer secure coding scheme for visible light communication based on polar codes", Proc. CLEO-PR'17, pp. 1-2, Aug. 2017
- [26] Y. M. Al-Moliki, M. T. Alresheedi and Y. Al-Harthi, "Robust key generation from optical OFDM signal in indoor VLC networks", IEEE Photon. Techn. Lett., vol. 28, no. 22, pp. 2629-2632, Nov. 2016.
- [27] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks", IEEE J. Sel. Areas Commun., vol. 36, no. 1, pp. 162-174, 2018.
- [28] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming", Proc. GC Wkshps'14, pp. 524-529, Dec. 2014.
- [29] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," IEEE Commun. Lett., vol. 19, no. 8, pp. 1351–1354, Aug. 2015.
- [30] Y. Wei, L. Wang, and T. Svensson, "Analysis of secrecy rate against eavesdroppers in MIMO modulation systems," in Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP), Oct. 2015, pp. 1–5.
- [31] C. Liu, L.-L. Yang, and W. Wang, "Secure spatial modulation with a full-duplex receiver," IEEE Wireless Commun. Lett., vol. 6, no. 6, pp. 838–841, Dec. 2017.
- [32] Z. Huang, Z. Gao, and L. Sun, "Anti-eavesdropping scheme based on quadrature spatial modulation," IEEE Commun. Lett., vol. 21, no. 3, pp. 532–535, Mar. 2017.
- [33] F. Wang et al., "Optical jamming enhances the secrecy performance of the generalized space-shift-keying-aided visible-light downlink," IEEE Trans. Commun., vol. 66, no. 9, pp. 4087–4102, Sep. 2018.
- [34] F. Wang, R. Li, J. Zhang, S. Shi, and C. Liu, "Enhancing the secrecy performance of the spatial modulation aided VLC systems with optical jamming,"

Signal Process., vol. 157, pp. 288–302, Apr. 2019.

- [35] D. Tian, W. Zhang, J. Sun and C. Wang, "Physical-Layer Security of Visible Light Communications with Jamming," 2019 IEEE/CIC International Conference on Communications in China (ICCC), 2019, pp. 512-517, doi: 10.1109/ICChina.2019.8855859.
- [36] E. Panayirci, A. Yesilkaya, T. Cogalan, H. V. Poor and H. Haas, "Physical-Layer Security With Optical Generalized Space Shift Keying," in IEEE Transactions on Communications, vol. 68, no. 5, pp. 3042-3056, May 2020, doi: 10.1109/TCOMM.2020.2969867.
- [37] E. Bektas and E. Panayirci, "Channel Estimation for DCO-OFDM Based VLC Systems in the Presence of Clipping Noise", IEEE 28th Signal Processing and Communications Applications Conference (SIU)", 5 - 7 Ekim 2020, Virtual.
- [38] E. Bektas and E. Panayirci, "Sparse Channel Estimation with Clipping Noise in DCO-OFDM Based VLC Systems", IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 26-29 May 2020, Virtual.
- [39] A. Yesilkaya, E. Basar, F. Miramirkhani, E. Panayirci, M. Uysal and H. Haas, "Optical MIMO-OFDM With Generalized LED Index Modulation," in IEEE Transactions on Communications, vol. 65, no. 8, pp. 3429-3441, Aug. 2017, doi: 10.1109/TCOMM.2017.2699964.
- [40] S. M. Kay, Fundamentals of Statistical Signal Processing: Estimation Theory, Prentice Hall PTR, ISBN 0-13-345711-7, 1993
- [41] Vishay TSUS4300 infrared emitting diode, 950 nm, GaAs, [Online]," <https://www.vishay.com/docs/81053/tsus4300.pdf>, accessed: 04-11-2019.
- [42] C. Zhang, J. Yue, L. Shi and S. Wang, "A novel physical encryption algorithm for LoRa", IEEE Commun. Lett., vol.25, no.8, pp. 2512 - 2516, May 2021.
- [43] K. H. Rosen, Elementary Number Theory and Its Applications (3rd ed.), Addison-Wesley, ISBN 978-0201-57889-8, 1993.
- [44] R. G. Gallager, Information Theory and Reliable Communications, John Wiley and Sons, ISBN W-471-29048-3, 1993.

CURRICULUM VITAE

Personal Information

Name and surname: Furkan Batuhan Okumuş

Academic Background

Bachelor's Degree Education: Kadir Has University (GPA: 3.01)

Post Graduate Education: Kadir Has University (GPA: 3.44)

Foreign Languages: English (C1)

French (A1)

Work Experience

NK Mühendislik Taahhüt ve Müşavirlik Tic. Ltd. Şti. 01.07.2017 – 31.08.2017

Kadir Has University, Alumni Relations Office Assistant 01.05.2018 – 30.09.2018

Kadir Has University, Assistant of Computer Lab. 01.06.2018 – 30.06.2019

Berrmak Makina Tekstil İnşaat Sanayi Ticaret Ltd. Şti. 01.07.2018 – 31.08.2018

Dione Local Development Centre 01.07.2019 – 30.09.2019

Tübitak, Project Assistant 01.01.2020 – 15.12.2021

Publications and Presentations Derived from the Thesis

29. IEEE SİNYAL İŞLEME ve İLETİŞİM UYGULAMALARI KURULTAYI 09-11
HAZİRAN 2021