



Görünür Işıkla Haberleşmede Fiziksel Katman Güvenliği

Program Kodu:1003

Proje No:218E034

Proje Yürütücüsü:

Prof. Dr. ERDAL PANAYIRCI

Araştırmacı(lar)

Prof. Dr. GÜNEŞ ZEYNEP KARABULUT KURT

Prof. Dr. MUTLU KOCA

Danışman(lar)

HARALD HAAS

Bursiyer(ler)

NUĞMAN SU

EKİN BAŞAK BEKTAŞ

FURKAN BATUHAN OKUMUŞ

MEHMET CAN ERDEM

OĞUZ GÜRCÜOĞLU

ŞUBAT 2022

ANKARA



**Görünür Işıkla Haberleşmede Fiziksel Katman Güvenliği
(Physical Layer Security in Visible Light Communications)**

Program Kodu:1003

Proje No:218E034

Proje Yürütücüsü:

Prof. Dr. ERDAL PANAYIRCI

Araştırmacı(lar)

Prof. Dr. GÜNEŞ ZEYNEP KARABULUT KURT

Prof. Dr. MUTLU KOCA

Yurtdışı Danışman

Prof. Dr. HARALD HAAS

Bursiyer(ler)

NUĞMAN SU

EKİN BAŞAK BEKTAŞ

FURKAN BATUHAN OKUMUŞ

MEHMET CAN ERDEM

OĞUZ GÜRCÜOĞLU

ŞUBAT 2022

ANKARA

ÖNSÖZ

Bu çalışma, Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) tarafından 1003-Öncelikli Alanlar Ar-Ge Projeleri Destekleme Programı No. 218E034 kapsamında desteklenmiştir. Öncelikle, TÜBİTAK'a sağladığı bu değerli destek nedeniyle teşekkür ederim.

Bu projede,

Prof. Dr. Erdal Panayırıcı (Kadir Has Üniversitesi) Yürütücü olarak,

Prof. Dr. Mutlu Koca (Boğaziçi Üniversitesi) ve Prof. Dr. Güneş Kurt (İstanbul Teknik Üniversitesi) Araştırmacı olarak,

Nuğman Su (Boğaziçi Üniversitesi), Ekin Bektaş Başak ve Furkan Batuhan Okumuş (Kadir Has Üniversitesi), Oğuz Gürcüoğlu ve Mehmet Can Erdem (İstanbul Teknik Üniversitesi) Bursiyer olarak,

Prof. Harald Haas (Edinburgh Üniversitesi ve daha sonra Strathclyde Üniversitesi, Birleşik Krallık) Proje Yurtdışı Danışman olarak görev almışlardır.

Ayrıca İTÜ'den Doç Dr. Onur Ferhanoğlu, ve yine Edinburgh Üniversitesinden (UK) değerli öğrencilerim Dr. Anıl Yeşilkaya ve Dr. Tezcan Çoğalan, ve Princeton Üniversitesinden, (Amerika Birleşik Devletleri) Prof. H. Vincent Poor projeye önemli katkılarda bulunmuştur.

Proje süresince bana destek olan tüm değerli proje ekibine, özellikle teknik desteğini esirgemiyen Doç. Dr. Ferhanoğlu'na, ve bu araştırmayla ilgili kritik geri bildirimlerini sağlayan Prof. Haas ve Prof. Poor'a en içten teşekkürlerimi sunarım.

Son olarak, bu projeyi değerlendiren değerli Hakem'e ve Kadir Has Üniversitesi, Proje Yönetim Yetkin Uzmanı sayın Selçuk Tuncer'e proje sürecince gösterdiği yakın ilgi ve yardımlarından dolayı teşekkürlerimi sunarım.

E. Panayırıcı

15/02/2022

ACKNOWLEDGEMENTS

This project was supported by the Scientific and Technical Research Council of Turkey (TUBITAK) under 1003-Priority Areas R&D Projects Support Program No. 218E034. First of all, I would like to thank TÜBİTAK for this valuable support.

In this project,

Prof. Erdal Panayırıcı (Kadir Has University) served as the Project Leader,

Prof. Mutlu Koca (Bogazici University) and Prof. Güneş Kurt (Istanbul Technical University (ITU)) served as the Project Researchers,

Nuğman Su (Boğaziçi University), Ekin Bektaş Başak and Furkan Batuhan Okumuş (Kadir Has University), Oğuz Gürcüoğlu and Mehmet Can Erdem (ITU) worked as the funded graduate students,

Prof. Harald Haas (The University of Edinburgh and later The University of Strathclyde, the United Kingdom (UK)) acted as an International Project Consultant.

In addition, Associate Professor Onur Ferhanoğlu from ITU , and my former students Dr. Anıl Yeşilkaya and Dr. Tezcan Çoğalan from The University of Edinburgh,UK, and Prof. H. Vincent Poor, from the Princeton University, the USA, have contributed significantly to the project.

I would like to thank all the project team who supported me, especially Dr. Ferhanoğlu who provided critical feedback on this research. My deepest gratitude to Prof. Haas and Prof. Poor for continuous collaboration and interactions during this work.

Finally, I would like to thank the anonymous Reviewer of the project and Mr. Selçuk Tuncer, Kadir Has University, Project Management Specialist, for his close attention and assistance concerning the financial issues.

E. Panayırıcı
15/02/2022

ÖZET

Optik Kablosuz Haberleşme ve bunun olası uygulaması olan Görünür Işıklı Haberleşme (Visible Light Communications (VLC)), sahip olduğu çok yüksek bant genişliği, bilgi iletim kapasitesi, elektromanyetik girişimlere karşı yüksek bağıışıklığı, uzaysal ortamlarda yüksek oranda güvenli kapsama özelliği ve çalışma frekans spektrumunun belli regülasyonlarla düzenlenmemiş olması nedeniyle, geniş bir uygulama alanı içinde, çok önemli teknik ve operasyonel üstünlükler sağlamakta ve radyo tabanlı kablosuz haberleşme sistemlerine bir seçenek olarak veya onların tamamlayıcı niteliğinde karşımıza çıkmaktadır. Son bir kaç yıl içinde, varolan şifreleme tekniklerini güçlendirmek için ve onlara tamamlayıcı bir ek olarak, fiziksel katman güvenliği (physical layer security) diye adlandırılan umut verici yeni bir araştırma ve ilgi alanı ortaya çıkmıştır. Fiziksel katman güvenliği, haberleşme ortamındaki yetkili olmayan kişilerden bilginin saklanması amacıyla, her türlü üst katman şifrelemeden bağımsız olarak, tamamen iletişim kanal ortamının özelliklerini kullanarak, geliştirilen teknik ve yöntemlerdir. Projede, genişbant ağlarda VLC fiziksel katman düzeyi güvenliği sağlamak amacıyla, geleneksel yaklaşımların ötesinde hızlı ve güvenilir çözümler için, etkin kuramsal çalışmalardan başlayarak laboratuvar düzeyine kadar geniş bir spektrumda özgün ve yenilikçi algoritmaların tasarımı önerilmektedir. Bu bakımdan, proje, "1003-BIT-GNBT 2018-1 Genişbant Haberleşme Ağları için Veri İşleme Teknolojileri" Çağrı Metnindeki (a) ve (b) amaçları ile büyük bir uyum içinde, araştırma bileşeni yüksek, yenilikçi ve özgün bir proje niteliğindedir. Projede, geleneksel sistemlere göre getirilen yenilikler ve sağlanan üstünlükleri şu şekilde sıralanabilir:

(1) Projede, fiziksel katman güvenliğine sahip VLC sisteminin gerçekleşmesinde, Indis modülasyonu ve bunun bir takım varyasyonları olan uzamsal modülasyon, uzay kaydırmalı anahtarlama ve OFDM-indis modülasyonu gibi yeni modülasyon teknikleri ve çok-girişli-çok çıkışlı LED (light emitting diode) yapıları ile, dikgen olmayan çoklu erişimin birlikte çalışan MIMO-NOMA tekniği önerilmektedir. Elde edilecek yeni ve özgün algoritmalar geleneksel sistemlere göre hesaplama karmaşıklığı düşük, güç randımanı yüksek ve çok kullanıcı senaryolar için de çalışabilme yeteneğine sahip olacaktır. Özellikle, sadece bu modülasyon tekniklerine özgü, yapay karıştırma (artificial jamming) sinyal üretme özelliği, bu tekniklerin fiziksel güvenliğin sağlanmasında geleneksel yaklaşımlara kıyasla en önemli üstünlüğünü oluşturmaktadır. Ayrıca, geliştirilecek algoritmalara ilişkin 'erişilebilecek maksimum gizlilik kapasitesi' ve 'gizlilik oranları'nın analitik yollardan belirlenmesi için izlenecek kuramsal yaklaşımlar, sistem mimarilerinin farklı olmasından dolayı, geleneksel sistemlerde izlenen yollardan çok daha farklı olacaktır.

(2) LED'lerin ve ışığın neden olduğu kısıtlar sonucu, RF kabosuz haberleşmedeki geleneksel kanal kestirim tekniklerinin uygulanamaması nedeniyle, Masif MIMO yapıdaki

görünür ışık kanallarının optimal ve hızlı kestiriminde yeni kanal kestirim algoritmalarının tasarımı önerilmektedir. Ayrıca, kestirim hataları ve kanal bilgilerin vericiye iletilmesindeki gecikmelerin, sistemin bit hata başarımına etkilerinin kuramsal ve bilgisayar benzetimleriyle incelenmesi hedeflenmektedir.

(3) Projede son olarak, fizisel katman güvenliğine sahip VLC sistemlerin laboratuvar ortamında donanımsal olarak gerçekleştirilmesi ve gerçek-zamanda çalışmasının test edilmesi önerilmektedir. Literatürde bir karıştırma sinyali üreterek gizliliği sağlayan geleneksel sistemlerle, algoritmanın gerek hesaplama karmaşıklığı ve hızı, gerekse hata başarımı ve erişilebilecek enbüyük gizlilik oranları farklı sinyal-gürültü düzeylerinde karşılaştırılarak üstünlüğü kanıtlanacaktır.

Anahtar Kelimeler: Optik Kablosuz Haberleşme, Görünür Işık Haberleşmesi, Fiziksel Katman Güvenliği, Dik Frekans Bölmeli Çoğullama, Uzamsal Modülasyon

SUMMARY

Optical Wireless Communications and one of its potential applications, Visible Light Communications (VLC), with attractive features such as high bandwidth capacity, robustness to electromagnetic interference, high degree of spatial confinement, inherent security and unregulated spectrum, offer powerful alternatives and/or complementary technologies to the existing radio frequency (RF) based wireless systems for a wide range of applications. During the past few years, physical-layer security in VLC networks has emerged as a promising approach to complement conventional encryption techniques and provide a first line of defense against eavesdropping attacks. To provide security at VLC physical layer level in broadband networks, in this project, design of original and innovative algorithms is proposed starting from effective theoretical studies to laboratory level for fast and reliable solutions beyond traditional approaches. In this respect, the project proposal is planned to contribute fully to the goals of the call "1003-BIT-GNBT-2018-1 Data Processing Technologies for Broadband Communication Networks" as well as in the goals and objectives specified in the call text "a" and "b, and has a potential to increase competitiveness of our country at the international level. In the project, the innovations and advantages as compared to the state-of-art systems can be listed as follows:

(1) New and novel algorithms for physical layer security in multiuser and broadband VLC systems applying new modulation schemes such as index modulations (IM) and its variations like spatial modulation (SM), space shift keying (SSK), OFDM-index modulation techniques (OFDM-IM), as well as optical multiple-input-multiple output (MIMO) with non-orthogonal multiple excess (NOMA) system are developed. The algorithms to be design will have low complexity, high power efficiency and have the capability to work with multi-user scenarios. In particular, the artificial jamming signal generation property of these modulation techniques is the most important advantage in providing physical security compared to the traditional approaches. Moreover, the theoretical methods, to develop the maximum achievable secrecy capacity and secrecy rate of the physical layer security algorithms will be much different than the approaches adopted by the by traditional systems because of the different system architectures employed.

(2) Due to some physical constraints imposed by the LEDs and light, it is not possible to employ conventional channel estimation techniques in RF communications. Hence, design of new optimal and computationally efficient estimation algorithms for massive MIMO structured optical channels will be proposed. In addition, the effects of channel estimation errors and the delays in the transmission of channel state information to the transmitter on the bit error performance will be investigated theoretically and by computer simulations.

(3) Finally, the proposed system will be implemented in a laboratory environment and its BER performance will be tested and compared with the state-of-art systems, employing conventional jamming signals.

Keywords: Optical Wireless Communications, Visible Light Communications, Optical Multiple-Input-Multiple-Output (MIMO) channels, OFDM Index Modulation, Spatial Modulation, Spatial Shift Keying, Non-orthogonal Multiple Access (NOMA)

İÇİNDEKİLER

ÖNSÖZ	i
ÖZET	iii
ŞEKİL LİSTESİ	ix
TABLO LİSTESİ	xiv
1. GİRİŞ	1
2. LİTERATÜR ÖZETİ	6
3. GEREÇ VE YÖNTEM	12
3.1. Görünür Işıklı Haberleşmede MIMO SSK Tabanlı Bir Fiziksel Katman Güvenlik Algoritması Geliştirilmesi	12
3.1.1. PLS'nin İyileştirmesi için Uzaysal Takım Tasarımı	16
3.1.1.1. Işık Şiddeti Normalizasyonu	19
3.1.2. VLC'de MIMO SSK Tekniğine Dayanan PLS Algoritmasına İlişkin Gizlilik Oranlarının (Secrecy Rates) Belirlenmesi	21
3.2. Görünür Işıklı Haberleşmede bir NOMA Tabanlı PLS Algoritması Geliştirilmesi	24
3.2.1. Önerilen PLS Sağlayıcı NOMA Önkodlayıcı Tasarımı	27
3.2.2. DC Noktası ve γ Tasarımı	29
3.2.3. Görünür Işıklı Haberleşmede (VLC) Önerilen NOMA Tabanlı Fiziksel Katman Güvenlik Algoritmasının Gizlilik Analizi	31
3.2.3.1. Ulaşılabilir Gizlilik Oranlarının Limitleri	32
3.3. Genelleştirilmiş LED İndeks Modülasyonu ile Optik MIMO-OFDM (GLIM-OFDM) için Fiziksel Katman Güvenliği	37
3.3.1. Optik GLIM OFDM Mimarisi	37
3.3.2. GLIM OFDM'de Vericide Önkodlayıcı Destekli PLS	39
3.3.3. Vericide Güç Normalizasyonu	40
3.3.4. Koşullu Minimum Karesel Ortalama (Bayes) Kestirimi	42
3.3.5. Gizlilik Anahtarı ile PLS algoritmasının daha da geliştirilmesi	47
3.3.6. GLIM-OFDM Sistemlerinde Erişilebilir Gizlilik Oranı	49
4. PLS-VLC SİSTEMLERDE KANAL KESTİRİMİ	54
4.1. Önkodlamasız GLIM-OFDM Sistemlerde Kanal Kestirimi	54
4.2. Kanal Kestiriminde Cramer-Rao Alt Sınırı	57
4.3. Önkodlamasız GLIM-OFDM Sisteminin BER Başarımı	58
4.4. Önkodlamalı Durumda NL-MMLS Algoritması geliştirilmesi ve MIMO Kanal Kestirimi Etkisi Altında Sistemin BER Başarımı	59
5. BULGULAR	64
5.1. Geliştirilen PLS Yetenekli ve MIMO SSK Tabanlı VLC Sistemin Bilgisayar Benzetimleri	64
5.1.1. <i>İdeal CSI ile MU-GSSK-SCD altında BER başarımı</i>	67

5.1.2.	<i>MU-GSSK-SCD sistem tasarımı üzerine değerlendirmeler</i>	67
5.1.3.	<i>İdeal olmayan CSI ile MU-GSSK-SCD BER başarımı</i>	69
5.1.3.1.	ρ 'nun ML kestirimi	72
5.1.4.	<i>MU-GSSK-SCD'nin Literatürle Kıyaslanması</i>	76
5.2.	VLC'de MIMO SSK Tekniğine Dayanan PLS Algoritmasının Gizlilik Oranlarının (Secrecy Rates) Belirlenmesi	77
5.2.1.	<i>Bilgisayar Benzetim Sonuçları</i>	77
5.3.	Geliştirilen PLS Yetenekli ve MIMO-NOMA Tabanlı VLC Sistemin Bilgisayar Benzetimleri	79
5.4.	VLC-NOMA Tabanlı PLS Tekniğinin Gizlilik Analizi	81
5.5.	Geliştirilen PLS Yetenekli GLIM-OFDM Tabanlı VLC Sistemin Bilgisayar Benzetim Sonuçları	83
6.	FİZİKSEL KATMAN GÜVENLİKLİ VLC SİSTEMİNİN DONANIMSAL TASARIMI	87
6.1.	Başlangıç PLS-VLC düzeneği	87
6.2.	Son PLS-VLC donanım yapısı	95
6.3.	3B-baskı tabanlı lens eyleyiciler kullanılarak PLS'nin artırılması	104
6.4.	Deney Sonuçları	108
7.	TARTIŞMA	111
7.1.	VLC'de MIMO SSK Tabanlı bir PLS Algoritması Geliştirilmesi	111
7.1.1.	İdeal CSI'ye sahip MU-GSSK-SCD Sisteminin BER Başarımının Değerlendirilmesi	111
7.1.2.	İdeal Olmayan CSI'ye sahip MU-GSSK-SCD'nun BER Başarımının Değerlendirilmesi	111
7.1.3.	MU-GSSK-SCD'nin Literatürle Kıyaslanması	112
7.1.4.	Karmaşıklık Analizi Değerlendirmesi	112
7.2.	VLC'de MIMO SSK Tekniğine Dayanan PLS Algoritmasına İlişkin Gizlilik Oranlarının (Secrecy Rates) Değerlendirilmesi	113
7.3.	VLC NOMA Tabanlı PLS Algoritmasının Değerlendirilmesi	113
7.3.1.	VLC-NOMA Tabanlı PLS Algoritmasının Gizlilik Analizi Değerlendirmesi	114
7.4.	GLIM OFDM tabanlı PLS Algoritmasının Değerlendirilmesi	114
7.5.	PLS-VLC Sistemlerde Kanal Kestirim Algoritmasının Değerlendirilmesi	115
7.6.	Laboratuvar ortamında PLS-VLC Sistemin Donanımsal Tasarımıyla ilgili Değerlendirmeler	116
8.	SONUÇ VE ÖNERİLER	117
	REFERANSLAR	119

ŞEKİL LİSTESİ

Şekil 3.1.	SCD ile donatılmış çok kullanıcılı MIMO-GSSK-VLC sistem modeli. . . .	13
Şekil 3.2.	Önerilen PLS Önkodlama tasarımı için verici tasarımı.	25
Şekil 3.3.	Önerilen önkodlayıcı için Kullanıcı 1'deki alıcı tasarımı.	27
Şekil 3.4.	Önerilen önkodlayıcı için Kullanıcı 2'deki alıcı tasarımı.	28
Şekil 3.5.	Bir fiziksel katman güvenli ve kanal kestimli VLC GLIM-OFDM sistemin verici ve alıcı blokları	38
Şekil 3.6.	Ortak bilginin (mutual information) yaklaşık ve kesin Gauss olasılık dağılımları kullanılarak hesaplanması durumunda karşılaştırılması	51
Şekil 4.1.	OFDM verici ve alıcı sistemin blok şeması	56
Şekil 4.2.	Kanal kestirimi MSE başarımları ve Cramer-Rao alt sınırı	60
Şekil 4.3.	Kanal kestirim hatası etkisinde GLIM OFDM BER Başarımları	61
Şekil 4.4.	Önkodlamalı GLIM-OFDM sistemin blok şeması	62
Şekil 4.5.	Tam ve kısıtlı CSI altında, 4QAM için önkodlamalı GLIM-OFDM BER başarımları	63
Şekil 5.1.	Ele alınan MIMO-VLC kullanıcı konfigürasyonlarından Senaryo 1.	65
Şekil 5.2.	Ele alınan MIMO-VLC kullanıcı konfigürasyonlarından Senaryo 2.	65
Şekil 5.3.	MIMO-VLC kullanıcı konfigürasyonlarından Senaryo 3.	66
Şekil 5.4.	Senaryo 1'de elde edilen BER eğrileri. Eve'in lokasyonu, [-1, 1, 0.85] olarak seçilmiştir.	66
Şekil 5.5.	Senaryo 1'de elde edilen BER eğrileri. Eve'in lokasyonu, [0, 0, 0.85] olarak seçilmiştir.	67

Şekil 5.6.	Senaryo 1’de elde edilen BER eğrileri. Eve’in lokasyonu, [1, -1, 0.85] olarak seçilmiştir.	68
Şekil 5.7.	Senaryo 2’de elde edilen BER eğrileri. Eve’in lokasyonu [-1.5, -0.375, 0.85] olarak seçilmiştir.	68
Şekil 5.8.	Senaryo 2’de elde edilen BER eğrileri. Eve’in lokasyonu, [-0.5, -0.25, 0.85] olarak seçilmiştir.	69
Şekil 5.9.	Senaryo 2’de elde edilen BER eğrileri. Eve’in lokasyonu, [0.5, -0.125, 0.85] olarak seçilmiştir.	70
Şekil 5.10.	Senaryo 3’te elde edilen BER eğrileri. Eve’in lokasyonu, [1.125, -1, 0.85].	70
Şekil 5.11.	Senaryo 3’te elde edilen BER eğrileri. Eve’in lokasyonu, [1.25, -1, 0.85] olarak seçilmiştir.	71
Şekil 5.12.	Senaryo 3’te elde edilen BER eğrileri. Eve’in lokasyonu, [1.375, -1, 0.85] olarak seçilmiştir.	72
Şekil 5.13.	Eve içmekanda yer değiştirirken ve Kullanıcı 1’i dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.9, -1] koordinatlarındadır. Tüm birimler metredir.	73
Şekil 5.14.	Eve içmekanda yer değiştirirken ve Kullanıcı 2’yi dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.9, -1] koordinatlarındadır. Tüm birimler metredir.	73
Şekil 5.15.	Eve içmekanda yer değiştirirken ve Kullanıcı 1’i dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.1, -1] koordinatlarındadır. Tüm birimler metredir.	74
Şekil 5.16.	Eve içmekanda yer değiştirirken ve Kullanıcı 2’yi dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.1, -1] koordinatlarındadır. Tüm birimler metredir.	74
Şekil 5.17.	Senaryo 1’de kullanıcılarda kusurlu CSI varken, kestirim hatası olan $ \rho - \hat{\rho} $ ifadesinin RMSE değerleri.	75
Şekil 5.18.	Senaryo 1’de kullanıcılarda kusurlu CSI varken elde edilen, değişen SNR’a göre BER eğrileri.	76

Şekil 5.19.	8-PAM ve MU-GSSK-SCD için Eve'in BER vs. SNR eğrileri. Tüm eğrilerde, spektral verimlilik kullanıcı başına 3 bit/s/Hz olarak seçilmiştir.	77
Şekil 5.20.	8-PAM ve MU-GSSK-SCD için Bob ve Eve'in BER vs. SNR eğrileri. Tüm eğrilerde, spektral verimlilik kullanıcı başına 3 bit/s/Hz olarak seçilmiştir.	78
Şekil 5.21.	Kullanıcılar arasındaki mesafe 30 cm iken elde edilen gizlilik oranı bölgeleri.	78
Şekil 5.22.	Kullanıcılar arasındaki mesafe 90 cm iken elde edilen gizlilik oranı bölgeleri.	79
Şekil 5.23.	Eve Kullanıcı 1'den Kullanıcı 2'ye doğru hareket ederken, elde edilen gizlilik oranı bölgeleri. Tüm eğrilerde SNR, 0 dB alınmıştır.	80
Şekil 5.24.	MU-GSSK-SCD stratejisiyle elde edilen gizlilik oranı bölgeleri. Verici ve aktive edilen anten sayısı sırayla $N_t = 16$, $N_a = 8$ olup N_r çeşitlendirilmiştir.	80
Şekil 5.25.	Senaryo 1 için, önerilen PLS önkodlayıcısıyla elde edilen BER başarımlarının grafikleri.	82
Şekil 5.26.	Senaryo 2 için, önerilen PLS önkodlayıcısıyla elde edilen BER başarımlarının grafikleri.	82
Şekil 5.27.	Önerilen PLS önkodlayıcı ile Senaryo 3 için elde edilmiş olan BER başarımlarının grafiği.	83
Şekil 5.28.	Önerilen PLS önkodlayıcı ile artan N_r için elde edilmiş olan BER başarımlarının grafiği (Senaryo 1).	84
Şekil 5.29.	Önerilen PLS önkodlama stratejisiyle elde edilmiş ulaşılabilir gizlilik oranı eğrileri ile alt ve üst limitleri.	85
Şekil 5.30.	Önerilen PLS önkodlama stratejisiyle, Eve iki farklı noktada iken elde edilmiş ulaşılabilir gizlilik oranı eğrileri.	85
Şekil 5.31.	Gizli anahtar kullanan ve kullanmayan durumlarda 1. senaryo için Bob ve Eve'in BER başarımlarının karşılaştırılması	86
Şekil 5.32.	Gizli anahtar kullanan ve kullanmayan durumlarda 2. senaryo için Bob ve Eve'in BER başarımlarının karşılaştırılması	86

Şekil 6.1.	Gizlilik problemini görselleştiren, bir yasal alıcı bir yasal olmayan alıcıdan ouşan VLC sisteminin şeması	88
Şekil 6.2.	Geleneksel bir kapalı ortam MISO-VLC sisteminin şeması. (a) sağ üstteki LED veriyi ileten verici olarak ayarlanabilir. Etraftaki diğer kaynaklar ise yapay gürültü oluşturmak için kullanılabilir. (b),(c) bir LED vericinin önüne yerleştirilen mercek ile bilginin odada belirli bir noktaya aktarılması sağlanmıştır.	91
Şekil 6.3.	Uygulamada kullanılan komple deney düzeneği	92
Şekil 6.4.	(a) Mercek altındaki alanda bulunan Bob'a erişen sinyal, (b) Doğrudan LES ışınımı dışındaki bir noktada alınan sinyal. (c) Merceksiz LED altındaki noktada alınan sinyal	93
Şekil 6.5.	Test ortamını fotoğrafı	94
Şekil 6.6.	LED'leri sürmek için kullanılan <i>bias-tee</i> devreleri ve LED üniteleri	95
Şekil 6.7.	Deney düzeneğine entegre edilen LED sürücü birimleri	95
Şekil 6.8.	4 LED, 2 PD ünitesinden oluşmuş test ortamının farklı açılarda görünümü	97
Şekil 6.9.	Test ortamında Bob ve Eve'in yerleştirilmesi	100
Şekil 6.10.	Bob'un alıcısına gelen sinyallerin genliği	101
Şekil 6.11.	Eve'in alıcısına gelen sinyallerin genliği	101
Şekil 6.12.	Uzaysal modülasyon kullanıldığında Bob tarafında algılana sinyal genlikleri	102
Şekil 6.13.	Uzaysal modülasyon kullanıldığında Eve tarafında algılana sinyal genlikleri	103
Şekil 6.14.	Uzaysal modülasyon kullanıldığında Eve tarafında algılana sinyal genlikleri	105
Şekil 6.15.	(a)VLC için lens elektromanyetik eyleyici tasarımı ve (b) gerçekleşmesi	106
Şekil 6.16.	Statik hareket analizi ve FEM ortamında3 farklı yön için yay sabitlerinin belirlenmesi	107

Şekil 6.17.	Statik hareket analizi ve FEM ortamında 3 farklı yön için yay sabitlerinin belirlenmesi	108
Şekil 6.18.	Işın tarama genişliğinin voltaja göre değişimi	109
Şekil 6.19.	Işın tarama deneyinde Bob ve Eve'in algıladığı ışık yoğunlukları	109
Şekil 6.20.	Hedef üzerinde ışın yönlendirme deneyine ilişkin düzenek. Hedef 1 cm kaydırıldığında, eyleyiciye uygulanan 9 Volt luk bir gerilim, ışının hedef ile birlikte kaymasını sağlamıştır.	110

TABLO LİSTESİ

Tablo 3.1.	Örnek: 2–Kullanıcılı GSSK-VLC için eniyilenmiş SCD ($N_t = 6, N_a = 3, N_r = 3$)	18
Tablo 5.1.	Kullanıcı yerleşimleri	81
Tablo 6.1.	Donanım ve Yazılım Listesi	89
Tablo 6.2.	Bob ve Eve için hesaplanan P değerleri	100
Tablo 6.3.	LED'lerin sürücü gerilimleri (SM öncesi ve sonrası)	100
Tablo 6.4.	LED'lerin sürücü gerilimleri (SM öncesi ve sonrası)	103
Tablo 6.5.	Önkodlama öncesi ve sonrası sistemin eriştiği gizlilik kapasitesi	103
Tablo 6.6.	Lens eyleyicisine ait ebatlar	107

1. GİRİŞ

Optik Kablosuz Haberleşme ve bunun olası uygulaması olan Görünür Işıklı Haberleşme (Visible Light Communications (VLC)), sahip olduğu çok yüksek bant genişliği, bilgi iletim kapasitesi, elektromanyetik girişimlere karşı yüksek bağışıklığı, uzaysal ortamlarda yüksek oranda güvenli kapsama özelliği ve çalışma frekans spektrumunu Optik Kablosuz Haberleşme sistemleri (Optical Wireless Communications (OWC)) ve bunun olası bir uygulaması olan Görünür Işıklı Haberleşme , sahip olduğu çok yüksek frekans bant genişliği, bilgi iletim kapasitesi, elektromanyetik girişimlere karşı yüksek bağışıklığı, uzamsal ortamlarda yüksek oranda güvenli kapanma özelliği ve kapsadığı frekans spektrumunun belli regülasyonlarla düzenlenmemiş olması nedeniyle, geniş bir uygulama alanı içinde, çok önemli teknik ve operasyonel üstünlükler sağlamakta ve özellikle 5G ve ötesi radyo tabanlı kablosuz haberleşme sistemlerine bir seçenek olarak veya onların tamamlayıcı niteliğinde kesinlikle yaygın kullanıma ve standartlara girecek yeni bir teknoloji olarak karşımıza çıkmaktadır. VLC sistemleri ışık yayan diyotların (LED'ler) kullanımına dayanır ve halen yeni ve gelecek nesil genişbant teknolojileri arasında üzerinde en fazla araştırma yapılan ve en çok ilgi çekenlerden biridir. 400- 800 THz (780–375 nm) gibi çok geniş bir frekans bandında çalışan ve bu band içinde 100 Gigabit/saniye (Gbps) hızlara erişebilen VLC, 5G ötesi sistemlerin uygulanmasını kolaylaştıracak ve bu yönde büyük katkılar sağlayacaktır. n belli regülasyonlarla düzenlenmemiş olması nedeniyle, geniş bir uygulama alanı içinde, çok önemli teknik ve operasyonel üstünlükler sağlamakta ve radyo tabanlı kablosuz haberleşme sistemlerine bir seçenek olarak veya onların tamamlayıcı niteliğinde karşımıza çıkmaktadır.

Diğer taraftan, son bir kaç yıl içinde, varolan şifreleme tekniklerini güçlendirmek için ve onlara tamamlayıcı bir ek olarak, fiziksel katman güvenliği (physical layer security) diye adlandırılan umut verici yeni bir araştırma ve ilgi alanı ortaya çıkmıştır. Fiziksel katman güvenliği, haberleşme ortamındaki yetkili olmayan kişilerden bilginin saklanması amacıyla, her türlü üst katman şifrelemeden bağımsız olarak, tamamen iletişim kanal ortamının özelliklerini kullanarak, geliştirilen teknik ve yöntemlerdir. Projede, genişbant ağlarda VLC fiziksel katman düzeyinde güvenliği sağlamak amacıyla, geleneksel yaklaşımların ötesinde hızlı ve güvenilir çözümler için, etkin kuramsal çalışmalardan başlayarak laboratuvar düzeyine kadar geniş bir spektrumda özgün ve yenilikçi algoritmaların tasarlanmış olup, geleneksel sistemlere göre getirilen yenilikler ve sağlanan üstünlükleri ortaya çıkarılmıştır. Genel olarak bir güvenlik yazılım ve donanım platformu olarak gerçekleşen projenin hedefleri ve her bir hedefte elde edilen somut çıktılar aşağıda belirtilmiştir.

I) Tek ve çok kullanıcı ve geniş bantlı VLC ağları için üst katmanlara ek olarak, fiziksel katman düzeyinde güvenliğini (physical layer security) sağlamaya yönelik, kısıtlı hesaplama gücüne sahip yeni ve özgün tekniklerinin tasarımı ve geliştirilen güvenlik algoritmalarının

başarılarının bir ölçütü olan 'erişilebilen maksimum gizlilik kapasitesi' (secrecy capacity) ve 'gizlilik oranlarının' (secrecy rate) analitik yollardan belirlenebilmesi için kuramsal çalışmaların yapılması hedeflenmiştir. Projede, fiziksel katman güvenliğine sahip VLC sisteminin gerçekleştirilmesinde, Indis modülasyonu ve bunun bir takım varyasyonları olan uzamsal modülasyon, uzay kaydırmalı anahtarlama ve OFDM-indis modülasyonu gibi yeni modülasyon teknikleri ve çok-girişli-çok çıkışlı LED (light emitting diode) yapıları ile, dikgen olmayan çoklu erişimin birlikte çalışan MIMO-NOMA tekniği önerilmektedir. Bu yolda elde edilen yeni ve özgün algoritmaların geleneksel sistemlere göre hesaplama karmaşıklığı düşük, güç randımanı yüksek ve çok kullanıcı senaryolar için de çalışabilme yeteneğine sahip olduğu görülmektedir. Özellikle, sadece bu modülasyon tekniklerine özgü, yapay karıştırma (artificial jamming) sinyal üretme özelliği, bu tekniklerin fiziksel güvenliğin sağlanmasında geleneksel yaklaşımlara kıyasla en önemli üstünlüğünü oluşturmaktadır. Ayrıca, geliştirilen algoritmalara ilişkin 'erişilebilecek maksimum gizlilik kapasitesi' ve 'gizlilik oranları'nın analitik yollardan belirlenmesinde izlenen kuramsal yaklaşımlar, sistem mimarilerinin farklı olmasından dolayı, geleneksel sistemlerde izlenen yollardan çok daha farklı olduğu görülmektedir. Aşağıdaki paragraflarda, bu hedefler doğrultusunda, projede VLC sistemlerde fiziksel katman güvenliğini sağlamaya yönelik geliştirilen yeni ve özgün algoritmalar (mimariler) özetlenmektedir.

- ***Görünür Işıklı Haberleşmede MIMO SSK Tabanlı Bir Fiziksel Katman Güvenlik algoritması Geliştirilmesi***

Bu projede öncelikle görünür ışık (visible light) frekans bandı içinde çalışan, çok-girişli-çok-çıkışlı (multiple-input-multiple-output (MIMO)) yapıdaki uzamsal anahtar kaydırmalı (spatial shift keying (SSK)) ve uzamsal modülasyon (spatial modülasyon (SM)) tekniklerine dayalı VLC sistemleri üzerinde çalışmalar yapılmış ve bu tekniklerin fiziksel katman güvenliğine (physical layer security (PLS)) uygulanabilirliği araştırılmıştır. Literatürden bilindiği gibi, MIMO temelli SSK ve SM teknikleri, verici taraftaki anten veya LED'lerden birini rastlantısal olarak seçip bu anten veya LED üzerinden, SM de bilgi bir taraftan M-QAM veya M-PSK simgeleriyle taşınırken aynı zamanda seçilen anten veya LED'in indisıyla de taşınmakta ve böylece sistemin bant genişlik verimi (bits/sec/Hz) artırılmış olmaktadır. Diğer taraftan, SSK da ise, bilgi sadece anten veya LED indisleriyle taşınmaktadır. Yaptığımız çalışmalarda literatüre yeni girmiş ve özellikle 5G ve ötesi için büyük potansiyel olacak bu tekniklerin PLS'nin tasarımı için çok önemli bir özelliği sahip olduğunu belirledik. Bilindiği gibi, PLS de etkili bir yöntem olarak, verici tarafından yetkili olmayan kişiye güvenliğin sızması için yönlendirilmiş bir karıştırma (jamming) sinyali gönderilmektedir. Bu jamming sinyal yetkili kullanıcının sıfır uzayına düşecek biçimde tasarlandığı için kullanıcıya iletilen bilginin doğru alınmasına hiç etkisi olmayacaktır. Ancak bu tekniğin uygulamada şu türden sakıncaları bulunmaktadır: **i)** Alıcıda oluşturulan jamming sinyalinin üretimi, bilgi taşımak için kullanılan sinyal gücünün bir bölümünü kullanarak gerçekleştiği için sistemin toplam güç veriminin önemli ölçüde düşmesine neden olacaktır. **ii)** Bu amaçla

kullanılacak jamming sinyalin tasarımında vericinin yetkili olmayan kişiyle arasındaki iletişim kanalını bilmesi gerekmektedir. Bu da vericinin yetkili olmayan kullanıcının yerini kesin bilmesi sonucunu doğurur ki bu durum gerçek uygulamalarda pek olası değildir. **iii)** Vericinin oluşturduğu jamming sinyal, ortamda yalnız bir yetkili kullanıcı olduğu zaman uygulanabilir. Birden fazla yetkili kullanıcılar için bu tasarım gerçekleştirilemez matematiksel bakımdan mümkün değildir. Diğer taraftan, MIMO-SSK ve SM tabanlı sistemlerde bilginin tamamı ya da bir kısmı anten veya LED'ler den birinin rastlantısal olarak seçilerek onun indis bilgisi ile iletilmektedir. Bu ise her sinyalleşme aralığında seçilen antenler arasında, "dost karıştırma sinyali" (friendly jamming signal) diye tabir ettiğimiz rastlantısal bir anahtarlama gürültüsünün (random switching noise) oluşmasına neden olur. Yaptığımız çalışmalarda, bu, SSK veya SM tekniğine has üretilen karıştırma gürültüsünün PLS için çok etkili olarak kullanılabileceğini göstermiştir. Bu tekniğe dayalı PLS sisteminin klasik jamming sinyal üretimine dayalı tekniğine göre yukarıda belirtilen üç problemin çözümünde de çok etkili olduğu anlaşılmaktadır. Diğer bir deyişle, MIMO-SSK veya SM e dayanan PLS sistemlerinde, **i)** vericide oluşturulan jamming sinyal, anten veya LED'lerin rastlantısal anahtarlama sürecinde doğal olarak üretildiği için ek bir güç harcanmasına gerek olmayacaktır ve dolayısıyla sistemin güç verimliliği klasik PLS sistemlere göre çok daha yüksek olacaktır **ii)** bu amaçla kullanılacak jamming sinyalin tasarımında vericinin yetkili olmayan kişiyle arasındaki iletişim kanalını bilmesine gerek yoktur. Çünkü, verici tarafından üretilen jamming signal omni-direksiyonel biçimde yayılmakta ve yetkili olmayan kullanıcılar nerede olursa olsun etkilenmektedir. Ancak aşağıda daha ayrıntılı olarak görüleceği gibi, proje kapsamında geliştirilen özgün MIMO-SSK tabanlı PLS algoritması, oluşan bu anahtarlama gürültüsünün yetkili kullanıcılara hiç bir bozucu etkisinin olmamasını sağlamaktadır, **iii)** vericinin oluşturduğu jamming sinyalin, ortamda birden fazla yetkili ve yetkili olmayan kullanıcıların olması durumunda da çok etkili olarak çalıştığı görülmektedir.

- ***Görünür Işıklı Haberleşmede (VLC) NOMA Tabanlı Bir Fiziksel Katman Güvenlik algoritması Geliştirilmesi***

Kablosuz veri iletimine yönelik artan talep artık makine tipi iletişimlere doğru genişlediğinden, gelişen teknolojilerin birden fazla kullanıcıya güvenli iletişim sunmasını da gerektirmektedir. Bu bağlamda, dik olmayan çoklu erişim (non-orthogonal multiple access (NOMA)), aynı kaynak bloğunu (zaman, frekans, kod vb.) kullanarak birden fazla kullanıcıya bilgi iletimi sağlayarak, diğer çoklu erişim yöntemlerine göre artırılmış spektral verimlilik sunar. Ancak, NOMA'nın VLC sistemlerine tam olarak entegre edilebilmesi için iletilen bilginin güvenliğini de tam olarak sağlamak gerekmektedir. LED'lerin kapsama alanı ışığın yerel olarak sınırlandırılması nedeniyle çok daha küçük olduğundan, VLC sistemleri, RF tabanlı sistemlere kıyasla doğası gereği daha güvenlidir. Ancak iletişimin fiziksel katman güvenliği, yetkili olmayan kullanıcılardan (eavesdropper (Eve)) gelen çeşitli bilgi güvenliği saldırılarıyla tehdit altındadır. Eve'in yetkisiz müdahalelerini bozmak amacıyla, iletilen sinyalleri alıcıların kanal durum bilgisi (channel state information

(CSI)) ile şekillendirmeye dayanan PLS teknikleri ile gizlilik sağlanabilir. 4. Bölümde, MIMO-NOMA-VLC sistemlerine PLS sağlamak amacıyla, yeni bir iletim ön kodlama stratejisi önerilmektedir. Önerilen PLS algoritması, dışbükey olmayan optimizasyon problemlerini çözmek gibi hesaplama açısından karmaşık teknikleri içermemektedir. Bunun yerine, yasal kullanıcılara (Bob) iletilen NOMA sembollerin, diğer yasal kullanıcılardan gelen girişimden arındırılarak, sezildiği ve yetkisiz kullanıcıda da önemli ölçüde bozulmuş bir sinyal olarak alındığı yeni ve özgün bir önkodlayıcı önerilmektedir. Tasarlanan önkodlayıcı yalnızca Bob'ların kanal durum bilgilerine (CSI) ve onlara iletilen veri bilgilerine gereksinim duymaktadır. Buna ek olarak, önerilen sistemde, Bob'larda kodçözme için gerekli olmayan, ancak yetkisiz kullanıcıda alınan sinyaldeki gizlemeyi artıran bir takım sembol kodlama matrisi de kullanılmaktadır. Önerilen önkodlayıcı tasarımı, pratik bir iç mekan VLC ortamında çeşitli kullanıcı yerleşimleri kullanılarak bilgisayar benzetim çalışmaları yapılmıştır. Hem simetrik hem de asimetrik kanal koşulları altında yapılan benzetimlerde, Eve'in BER başarımının önemli ölçüde kötüleştiği, Bob'ların ise kaynaktan iletilen gizli bilgileri başarıyla çözebildiği ve PLS'nin önerilen bu önkodlama tekniği ile sağlandığı gözlemlenmiştir. Benzetim sonuçları ayrıca, önerilen önkodlayıcılı PLS sistemde alıcıdaki PD'lerin sayısı artırıldığında Eve'deki BER başarımı 0.5 düzeyi olan en kötü durumda kalırken, Bob'ların BER başarımlarının daha da iyileştiğini göstermektedir.

- **Genelleştirilmiş LED indis modülasyonu ile VLC MIMO-OFDM (GLIM-OFDM) için fiziksel katman güvenliği**

Bu raporun 5. Bölümünde, son olarak, MIMO-OFDM tabanlı VLC sistemlerde PLS problemi incelenmekte ve araştırma gurubunca daha önce geliştirilen ve literatürde çok sayıda atıf alan "Genelleştirilmiş LED indis modülasyonu OFDM (GLIM-OFDM)" sistemleri için yeni bir PLS algoritması önerilmektedir. GLIM-OFDM, VLC'de OFDM zaman-bölgesi sinyallerin pozitif ve gerçek değerli olma kısıtlamasını ortadan kaldıran MIMO temelli özgün bir mimaridir. Bölüm 5'de ayrıntılı olarak açıklandığı gibi, bu özellikten yararlanarak, GLIM-OFDM'de bir fiziksel katman güvenliği algoritması tasarlanmış ve yapılan yoğun bilgisayar benzetimlerde geliştirilen PLS algoritmasının yasal olmayan kullanıcılara karşı fiziksel katmanda çok güçlü bir bilgi güvenliği sağladığı gösterilmiştir.

II) LED'lerin ve ışığın neden olduğu kısıtlar sonucu, RF kabosuz haberleşmedeki geleneksel kanal kestirim tekniklerinin uygulanamaması nedeniyle, Masif MIMO yapıdaki görünür ışık kanalların optimal ve hızlı kestiriminde yeni kanal kestirim algoritmalarının tasarımı önerilmektedir. Ayrıca, kestirim hataları ve kanal bilgilerin vericiye iletilmesindeki gecikmelerin, sistemin bit hata başarımına etkilerinin kuramsal ve bilgisayar benzetimleriyle incelenmesi hedeflenmektedir.

III) Projede son olarak, fiziksel katman güvenliğine sahip VLC sistemlerin laboratu-

var ortamında donanımsal olarak geekleřtirilmesi ve gerek-zamanda alıřmasının test edilmesi nerilmektedir. Literatürde bir karıřtırma sinyali üreterek gizlilięi saęlayan geleneksel sistemlerle, algoritmanın gerek hesaplama karmařıklıęı ve hızı, gerekse hata başarımı ve eriřilebilecek enbüyük gizlilik oranları farklı sinyal-gürültü düzeylerinde karřılařtırılarak üstünlüęü kanıtlanacaktır.

2. LİTERATÜR ÖZETİ

Kapalı bir ortamda aydınlatma altyapısını kullanarak ve haberleşme frekansını görünür ışık frekans bandına kaydırarak gerçekleştirilen VLC [75]- [3], gelecek kuşak yüksek hızlı ve geniş bantlı haberleşme için umut verici bir aday olarak karşımıza çıkmakta ve RF tabanlı kablosuz haberleşme sistemlerdeki spektrum tıkanıklığı sorununu çözmeye etkili bir çözüm olarak görülmektedir. Bu konudaki son gelişmeler özellikle yerel ve kırsal alanlarda VLC'yi kullanan kısa mesafeli kablosuz optik haberleşme sistemlerinin standardartlaşmasına olanak sağlamıştır [4]. Örneğin 2011 de oluşturulan IEEE802.15.7 standardı VLC ağların ticaretleşmesi ve yaygın olarak kurulmasını öngörmektedir [4]. VLC'nin potansiyel uygulama alanları: **(a)** kablosuz yerel ağlar (WLAN), **(b)** hava meydanları, tren istasyonları ve diğer halka açık kritik noktalar **(c)** uçaklar ve hızlı trenler **(d)** hastaneler, müzeler ve sanat galerileri, **(e)** araç içinde ve araç ile altyapısı oluşturulmuş haberleşme ağlarıdır. Araştırma sonuçlarına göre, ayrıca, optik kablosuz haberleşme teknolojisinin kullanıldığı diğer alanlarda da VLC yararlı olacaktır.

Genellikle, çok kullanıcıli VLC ağların tasarımlarında VLC'nin yayın (broadcasting) özelliği yaygın olarak kullanılmaktadır [5]- [7]. Haberleşme trafiğinde son yıllardaki akıl almaz artışlar nedeniyle, bu özellik, tren istasyonları, kütüphaneler, hastaneler, müzeler ve sanat galeriler gibi ortak kullanım alanlarında üretilen kişisel bilgilerin gizliliğiyle ilgili, gerek yetkili kullanıcılara ve gerekse ağ yöneticilerine büyük sorunlar çıkarmaktadır. RF tabanlı sistemlerde bu konuyla ilgili güvenlik mekanizması haberleşme sisteminin üst katmanlarında bir takım erişim teknikleri, "password" korumaları ve noktadan-noktaya şifreleme teknikleriyle sağlanmaya çalışılmaktadır. Ancak, bu çözümler bilgiye erişmeye çalışan yetkili olmayan kullanıcıların hesaplama güçlerinin ve bilgi depolama kapasitelerinin belli sınırlar içinde kalması koşuluyla sağlanabilmektedir. Diğer taraftan son bir kaç yıl içinde, varolan şifreleme tekniklerini güçlendirmek için ve onlara tamamlayıcı bir ek olarak, fiziksel katman güvenliği diye adlandırılan yeni bir araştırma ve ilgi alanı ortaya çıkmıştır.

Bilgi kuramı dalında fiziksel katman güvenliği ile ilgili ilk çalışmalar, Wyner'in bu amaçla 'wire-tap' diye adlandırdığı bir kanal modelini ortaya atmasıyla başlamıştır [8]. Bu kanal modelinde, vericiden iletilen sinyalin yetkili olmayan kullanıcıya bozulmuş (degraded) bir versiyonunun eriştiği varsayılmaktadır. Bozuk dinleme kanalı modeli daha sonra Csiszár ve Körner tarafından genişletilerek haberleşmenin bozulmadan gerçekleştiği yeni bir yayın kanal modeli de ortaya atılmıştır [9]. Bu kapsamda yaptıkları çalışmalarda, yetkili kullanıcıya iletilen sinyalin daha az bozulmuş olduğu varsayımı altında, mükemmel gizliliğin sağlanabileceği ve sistemin gizlilik kapasitesinin yetkili ve yetkili ve olmayan kullanıcıların bilgi kapasitelerinin farkı alınarak hesaplanabileceği gösterilmiştir.

Fiziksel katman güvenliği, haberleşme ortamındaki yetkili olmayan kişilerden bilginin saklanması amacıyla, her türlü üst katman şifrelemeden bağımsız olarak, tamamen iletişim kanal ortamının ve bu kanallardaki gürültülerin raslantısal değişim özelliğini kullanarak sağlanmaktadır [8], [9]. Ortalamın güç kısıtı (constraint) ve Gauss gürültüsü etkisi altında çalışan klasik RF haberleşmesinden farklı olarak, VLC, genel olarak bilgiyi LED'lerin yaydığı ışık şiddetinin (light intensity) oluşturduğu optik sinyallerle alıcıya iletir. Alıcıda ise foto-detektörler yardımıyla bu sinyallerden doğru bilginin yeniden çıkarılması sağlanır. VLC'de iletilen optik sinyaller, yayılan ışığın şiddetiyle modüle edildiği için gerçel ve pozitif değerlidir. Ayrıca, bu amaçla kullanılan LED'lerin doğrusal bölgede çalışma karakteristiklerinin sınırlı olması ve ortamın aydınlatmasını yeterli biçimde sağlaması gerekliliği, iletilen optik sinyallerin ortalama ya da tepe genliklerinin sınırlı olması kısıtlamasını getirmektedir [6], [10]- [12]. Genellikle, her ne kadar tipik LED'ler doğrusal olmayan elektrik-optik (E/O) transfer karakteristiğine sahipse de, bu doğrusal olmama sorunu uygun bir ön-bozulma (pre-distortion) tekniği ile kolayca çözülebilmektedir [13]. Diğer taraftan, görünür ışık dalga boyunun alıcı taraftaki tipik bir foto-detektörün algılama yüzeyine kıyasla çok çok küçük olmasından dolayı, RF dalgaların yayılımı sonucu oluşan çok yönlü sönümlenme etkisi VLC'de yoktur ve genellikle alıcı ile verici arasındaki iletişimin direkt görüş (line of sight) yayılımı ile sağlandığı varsayılır. Bu temel farklılıklar nedeniyle, RF ağları için elde edilen gizlilik kapasitesi sonuçları VLC ağlarına doğrudan uygulanamaz.

Bir VLC sistemine ilişkin gizlilik kapasitesi, o sistemdeki haberleşme kanalının bilgi kapasitesi (channel capacity) ilintili olduğu için [8], [9], öncelikle optik kanal kapasitesinin, ortalama, tepe ve gerçek değerli, pozitif genlik kısıtları altında doğru ve tam olarak hesaplanması gerekir. Ancak, VLC'de, çok basit tek-girişli-tek-çıkışlı (single-input-single output (SISO) kanallar için bile, bu kısıtlar altında kanal kapasitesinin kesin ve tam olarak hesaplanmasıyla ilgili halen analitik bir formülasyon bulunamamıştır. Bunu yerine, kanal kapasitesi için analitik bir takım alt ve üst sınırlar çıkarılmıştır [10]- [12]. Örneğin, [14]'de, bir verici, tek yetkili ve yetkili olmayan kullanıcılardan oluşan VLC sistemlere ilişkin gizlilik kapasitesinin hesabı için, [10]'da elde edilen alt ve üst sınırlardan yararlanarak bir takım kuramsal çalışmalar yapılmıştır. [15]'de sıfır zorlamalı çok-girişli-tek-çıkışlı (MISO) hüzme yönlendirme sistemi ele alınmış, sistemde elde edilebilecek veri iletim hızı artışı benzetim çalışmaları ile incelenmiştir. MISO sistemlerin gizli iletim kapasitesi ile ilgili yapılmış ender çalışmalardan olan [16]'de ise MISO sistem yapısı sayesinde elde edilebilecek gizli iletim kapasitesi incelenmiş, VLC sistemlerinin gizli iletime uygunluğu gözlenmiştir. Ayrıca NOMA VLC sistemlerin gizli iletim kapasitesi artışına olabilecek etkileri de [17] çalışmasında ele alınmıştır. Bu çalışmalarda, önerilen projede uygulanacak, yenilikçi modülasyon teknikleri kapsamamış olup proje hedefleri henüz literatürdeki açık noktaları adreslemeyi hedeflemektedir.

Diğer taraftan, tipik bir aydınlatma uygulamasında, LED'lerden oluşan diziler kullanılarak

istenilen aydınlatma seviyesine ulaşılır. Dolayısıyla, çok-girişli çok-çıkışlı (MIMO) haberleşme teknikleri, VLC sistemlerinin veri hızlarını arttırmak için ve aşağıda açıklanacağı gibi, fiziksel katman güvenliğini sağlamak için uygun bir yöntem olarak karşımıza çıkmaktadır [18]- [20]. Uzamsal çoğullama kullanan bir MIMO VLC sistemde [21], her bir LED eş zamanlı olarak bağımsız bir veri dizisini ileterek veri hızı, iletim elemanlarına sayısına göre (iletim elemanlarının sayısının alıcı elemanlarının sayısından büyük ya da eşit olduğu kabul varsayımı altında), verimli bir şekilde arttırılabilir ve uzamsal çoğullamanın katkıları tam ranklı MIMO kanal matrisleri için kesin biçimde elde edilebilir. Bunun dışında, İndis Modülasyonu(IM), yüksek frekans bant ve enerji randımanına sahip, MIMO ya da “çok taşıyıcı” (Multicarrier) yapıda, fiziksel katmanda geliştirilen yeni bir haberleşme tekniğidir. Uygulamada IM'nun iki farklı biçimi geniş uygulama alanı bulmuştur. Bunlar, **(a)** Uzamsal Modülasyon (Spatial Modulation, (SM)) [22]- [24] ve Uzay Kaydırmalı Anahtarlama (Space-Shift Keying (SSK)) [25]: Bu tekniklerde bilgi, MIMO sistemin verici antenlerinin indisleriyle taşınmaktadır. **(b)** İndis Modülasyonlu Dik frekans Bölmeli Çoğullama (Orthogonal frequency division multiplexing with IM (OFDM-IM)) [26]: Bu teknikte bilgi OFDM alt taşıyıcıların indisleriyle iletilmektedir.

Gerek SM ve SSK, gerekse OFDM-IM yüksek hızlı VLC sistemler için güçlü bir fiziksel katman tekniği olarak görülmektedir [26]- [29]. VLC frekans spektrumunun, şu anda 5G için düşünülen RF bandından çok daha yüksek olması, VLC'de anten elemanı olarak kullanılan LED'lerin hem çok sayıda ve hem de fiziksel olarak birbirine çok yakın olarak yerleştirilmelerine olanak sağlamaktadır. Bu şekilde kullanılacak LED'lerle hem kapalı ortamın aydınlanması sağlanırken bir taraftan da LED'ler ve alıcı optik detektörler arasında oluşan çok sayıda kanallar üzerinden yüksek veri kapasiteli haberleşme gerçekleştirilmektedir. Bu konuda yapılan çalışmalar, özellikle IM tekniğinin fiziksel katman güvenliği için de çok uygun bir uygulama alanı olduğunu göstermektedir [30], [31]. Örneğin, yetkili ve yetkili olmayan kullanıcıların kanal bilgilerinin kaynak tarafından doğru olarak bilinmesi varsayımı altında, vericide LED'lerden oluşan MIMO düzeniyle üretilen bir karıştırma (jamming) sinyalinin yetkili olmayan alıcı yönde oluşturacağı güçlü bir karışım (enterferans) etkisi, iletilen bilginin bu alıcıya doğru olarak erişmesini önlerken, karışım sinyalinin yetkili kullanıcı kanalına ilişkin sıfır uzayı içine düşecek biçimde tasarlanması nedeniyle, alıcı tarafta hiç girişim etkisi yaratılmadan bilginin tam ve doğru olarak alınması sağlanabilmektedir [32], [33]. Diğer taraftan, sadece yetkili kullanıcının vericiyle arasındaki kanalın bilinmesi durumunda ise, bilginin, yine MIMO yapısındaki LED'lerle yetkili kullanıcı doğrultusunda oluşturulacak dar bir hüzmeye (beam forming) iletilmesi, gerekli fiziksel gizliliği sağlamaktadır. Bu sonuçlardan yararlanarak, [15]'de genlik kısıtlaması altında eniyi hüzmeye tasarımı problemi üzerine bir takım çalışmalar yapılmıştır. [16]'da sadece tek erişim noktasına (access point) sahip tek hücreli bir VLC sisteminin gizlilik başarımıyla ilgili bir takım yeni sonuçlar elde edilmiştir. Optik SSK tekniğini kullanarak geliştirilen yeni bir VLC tabanlı fiziksel katman güvenlik sisteminde ise, kaynak tarafında tasarlanan uygun önkodlayıcı ve ön denkleştiriciler yardımıyla,

yetkili alıcıya iletilen bilginin çok büyük bir doğrulukla alınmasına karşın, aynı bilginin yetkili olmayan alıcı tarafında sezilmesinde yapılan bit hata olasılığının (BER) yüzde yüze yakın olduğu gösterilmiştir [31]. Bunların dışında, kapalı ortamlarda çok sayıda yetkili kullanıcıların bulunması durumunda dik olmayan çoklu erişim (non-orthogonal multiple access, (NOMA) sisteminin fiziksel katman güvenliği için uygun bir çözüm olduğu görülmektedir [34], [35].

Projenin izleyen bölümünde, VLC kanalların kestirilmesi ve kanal kestirim hatalarının tasarlanan PLS algoritmalarının başarımlarının nasıl etkilediği araştırılmaktadır. Gerçekleştirilecek fiziksel katman güvenlik algoritmaları, verici ile yetkili ve yetkili olmaya kullanıcılar arasındaki optik kanalların birbirinden farklılığına büyük ölçüde bağlı olduğu için, görünür ışık kanallarının doğru olarak modellenmesi, kestirilmesi ve kestirilen kanal durum bilgilerinin (channel state information (CSI)) farklı bir geri beslem kanalıyla vericideki kaynağa iletilmesi büyük önem taşımaktadır. Görünür ışık kanallarının kestirimi ve denkleştirme ve veri sezimleme süreçleri, VLC'de tasarlanacak PLS algoritmalarının yüksek başarımla çalışabilmeleri için en kritik fonksiyonları oluşturur. Diğer bir deyişle, bu süreçleri gerçekleştiren algoritmalar, alıcıların olmazsa olmaz alt üniteleridir ve bunların kalitesi sistem başarımlarını en önemli ölçüde etkileyen bir faktördür. Bu amaçla [36]- [40]'de bu konuyla ilgili bazı çalışma sonuçları verilmiştir. Bu projede, MIMO-OFDM, MIMO-SM ve OFDM-IM tabanlı fiziksel katman güvenliğine sahip görünür ışıkla haberleşme sistemlerinde bir takım yeni özgün, hesaplama karmaşıklığı çok düşük ve hızlı kanal kestirim/denkleştirme ve veri sezimi algoritmaları tasarlanmış ve donanımsal olarak gerçekleştirilmiştir.

Gerek SM ve SSK, gerekse OFDM-IM yüksek hızlı VLC sistemler için güçlü bir fiziksel katman tekniği olarak görülmektedir [26]- [29]. VLC frekans spektrumunun, şu anda 5G için düşünülen RF bandından çok daha yüksek olması, VLC'de anten elemanı olarak kullanılan LED'lerin hem çok sayıda ve hem de fiziksel olarak birbirine çok yakın olarak yerleştirilmelerine olanak sağlamaktadır. Bu şekilde kullanılacak LED'lerle hem kapalı ortamın aydınlanması sağlanırken bir taraftan da LED'ler ve alıcı optik detektörler arasında oluşan çok sayıda kanallar üzerinden yüksek veri kapasiteli haberleşme gerçekleştirilmektedir. Bu konuda yapılan çalışmalar, özellikle IM tekniğinin fiziksel katman güvenliği için de çok uygun bir uygulama alanı olduğunu göstermektedir [30], [31]. Örneğin, yetkili ve yetkili olmayan kullanıcıların kanal bilgilerinin kaynak tarafından doğru olarak bilinmesi varsayımı altında, vericide LED'lerden oluşan MIMO düzeniyle üretilen bir karıştırma (jamming) sinyalinin yetkili olmayan alıcı yönde oluşturacağı güçlü bir karışım (interferans) etkisi, iletilen bilginin bu alıcıya doğru olarak erişmesini önlerken, karışım sinyalinin yetkili kullanıcı kanalına ilişkin sıfır uzayı içine düşecek biçimde tasarlanması nedeniyle, alıcı tarafta hiç girişim etkisi yaratılmadan bilginin tam ve doğru olarak alınması sağlanabilmektedir [32], [33]. Diğer taraftan, sadece yetkili kullanıcının vericiyle arasındaki kanalın bilinmesi durumunda ise, bilginin, yine MIMO yapısındaki LED'lerle yetkili kullanıcı doğrultusunda oluşturulacak dar bir

hüzme (beam forming) ile iletilmesi, gerekli fiziksel gizliliği sağlamaktadır. Bu sonuçlardan yararlanarak, [15]'de genlik kısıtlaması altında eniyi hüzme tasarımı problemi üzerine bir takım çalışmalar yapılmıştır. [16]'da sadece tek erişim noktasına (access point) sahip tek-hücreli bir VLC sisteminin gizlilik başarımıyla ilgili bir takım yeni sonuçlar elde edilmiştir. Optik SSK tekniğini kullanarak geliştirilen yeni bir VLC tabanlı fiziksel katman güvenlik sisteminde ise, kaynak tarafında tasarlanan uygun önkodlayıcı ve ön denkleştiriciler yardımıyla, yetkili alıcıya iletilen bilginin çok büyük bir doğrulukla alınmasına karşın, aynı bilginin yetkili olmayan alıcı tarafında sezilmesinde yapılan bit hata olasılığının (BER) yüzde yüze yakın olduğu gösterilmiştir [31]. Bunların dışında, kapalı ortamlarda çok sayıda yetkili kullanıcıların bulunması durumunda dik olmayan çoklu erişim (non-orthogonal multiple access, (NOMA) sisteminin fiziksel katman güvenliği için uygun bir çözüm olduğu görülmektedir [34], [35]. Projenin ikinci aşamasında, VLC kanallarının kestirilmesi ve kanal kestirim hatalarının tasarlanan fiziksel katman güvenlik algoritmalarının başarımlarının nasıl etkilendiği araştırılmaktadır. Gerçekleştirilen PLS algoritmaları, verici ile yetkili ve yetkili olmaya kullanıcılar arasındaki optik kanalların birbirinden farklılığına büyük ölçüde bağlı olduğu için, görünür ışık kanallarının doğru olarak modellenmesi, kestirilmesi ve kestirilen kanal durum bilgilerinin (channel state information (CSI)) farklı bir geri beslem kanalıyla vericideki kaynağa iletilmesi büyük önem taşımaktadır. Görünür ışık kanallarının kestirimi ve denkleştirme ve veri sezimleme süreçleri, VLC'de tasarlanacak PLS algoritmalarının yüksek başarımla çalışabilmeleri için en kritik fonksiyonları oluşturur. Diğer bir deyişle, bu süreçleri gerçekleştiren algoritmalar, alıcıların olmazsa olmaz alt üniteleridir ve bunların kalitesi sistem başarımını en önemli ölçüde etkileyen bir faktördür. Bu amaçla [36]- [40]'de bu konuyla ilgili bazı çalışma sonuçları verilmiştir.

Diğer taraftan, fiziksel katman güvenli VLC sistemin donanımsal gerçekleşmesi üzerine literatürde bugüne kadar çok az çalışmaya raslanmıştır. Bir PLS-VLC mimarisinde, verici, alıcı ve PLS algoritması dahil çeşitli bileşenlerden oluşur. Verici modül, modülasyon ve verinin analogdan sayısala çevrim işlemini ve PLS algoritmasının çalışmasını yürütür. Vericiden gönderilen veriler, LED'e uygulanmak amacıyla bir sürücü devreye aktarılır. Sürücü devre aynı zamanda LED parlaklığını ayarlayan bir doğru akım kaynağına bağlı olup, ortamda istenen parlaklığı sağlamak ve analog veriyi LED kontrol sinyali ile birleştirmekle görevlidir. LED'le yayımlanan görünür ışık alıcıda bir fotodiyot ile algılanır. Alıcı modül algılanan analog sinyali sayısala çevirerek demodüle eder. Projede önerilen sistem mimarisinde, ışık kaynağı herhangi bir renk veya renk kombinezonunda ışık yayabilmektedir. Diğer ışık kaynaklarından (yani güneş, sokak lambaları, araç lambaları vb. gibi dış ortamdaki) gelen etkiler grubumuz tarafından başka bir çalışmada araştırılmıştır [44]. VLC ön-uçlarının ve farklı alıcıların kalitesini değerlendirmek amacıyla odak düzlemi dizilerine dayalı VLC sistemlerini test etmek için literatürde çok sayıda test yatağı (testbed) tasarımı kullanılmıştır [41], [42]. Test yataklarının sağladığı üstünlükler arasında göreceli basitlik, düşük maliyet ve güvenlik gibi özellikler sıralanabilir. Boş alan tezgah üstü test yatakları

üzerinde, bir dizi ışık yayan diyot (LED)'lar [43], iç mekan izleme, [45] ve optik frekans tanımlama (OFID [46]) gibi olanaklarla OFDM temelli VLC, Hibrit VLC – RF iletişim [47] ve çift yönlü VLC sistemlerini donanımsal olarak gerçeklemek çok kolay ve uygun olmaktadır [48]. Daha önce, iyileştirilmiş PLS'den yararlanmanın bir yolu olarak, seçilen LED'in önünde bir lensin kullanılmasından yararlanmıştır [49]. Ancak bu yaklaşıma dayanan minyatür test yatakları, farklı oda, pencere ve kapı tasarımları ve entegre opto-mekanik bileşenler yapma esnekliği ve kolaylığından yoksundur [50]. Bunun yanında, ayrıca, VLC odaklı deneysel çalışmalarda genellikle mikroişlemciler, tek kartlı bilgisayarlar [51], WARP [52], USRP [53] gibi çeşitli bileşenler kapsayan deney sistemlerinden yararlanılmaktadır. Tek kartlı bilgisayarların hızı analog-sayısal çevirici hızı ile sınırlanırken, USRP gibi yazılım temelli, radyolar ile daha yüksek hızda işlem yapılabilir. Bu projede, VLC alanında deneyler yapmak için 4 LED'li düşük maliyetli 70 cm × 40 cm × 40 cm minyatür oda modelinin test yatağı benimsenmiştir. Test yatağı, geleneksel bir odanın 10:1 küçültülmüş bir kopyasıdır ve sürücü ve opto-elektronik algılayıcı bileşenleri hariç, toplam fiyatı 10\$'ın altında olan basit ofis malzemeleriyle oluşturulabilir. Bu çalışmada literatürde ilk kez kuramsal yoldan geliştirilene türlü PLS algoritmalarıyla çalışan ve yasal alıcı ve gizli dinleyici arasında sağlam ve güvenli iletişim sağlayan bir PLS-VLC sisteminin donanımsal tasarımının gerçekleştirilmiş ve erişilebilir gizlilik kapasitesinde başarılı sonuçlar verdiği saptanmıştır

3. GEREÇ VE YÖNTEM

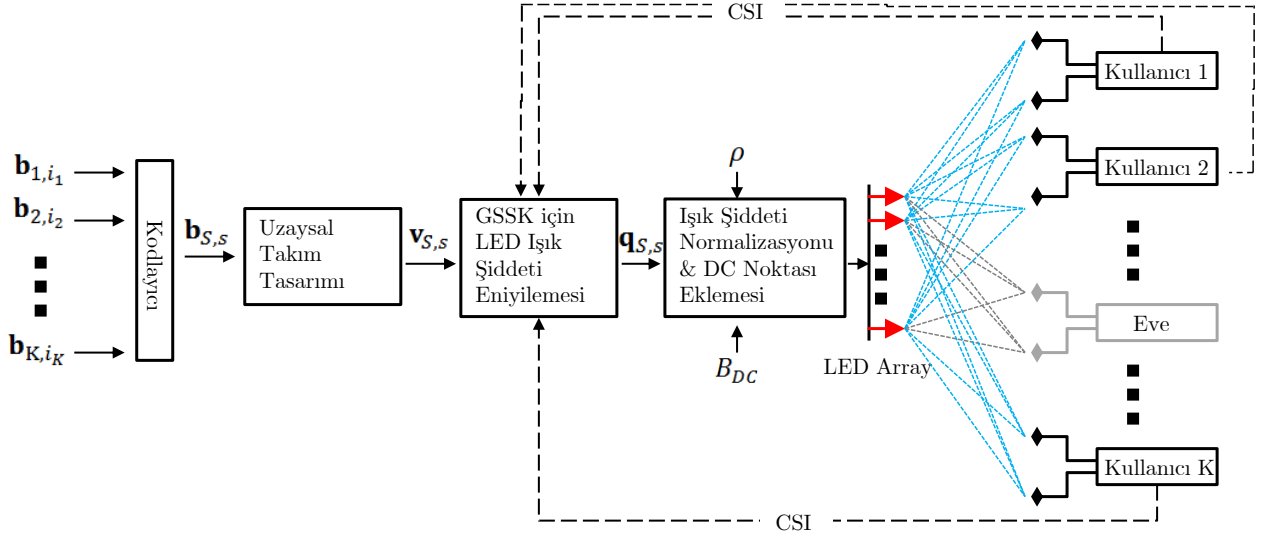
3.1. Görünür Işıklı Haberleşmede MIMO SSK Tabanlı Bir Fiziksel Katman Güvenlik Algoritması Geliştirilmesi

Bu kısımda, erişim noktası (access point (AP)) olan Alice'in N_t ışık yayan diyot (light-emitting diode (LED)) ile, K yetkili kullanıcı ve Eve'in N_r fotodetektör (photodetector (PD)) ile donatıldığı bir içmekan görünür ışıkla haberleşme (visible light communication - VLC) sistemi ele alınmaktadır. Kullanıma hazır optik komponentlerle VLC sistemi tasarlamak için en basit yaklaşım yoğunluk-modülasyonu-doğrudan-veri-sezim (intensity-modulation-direct-detection (IM/DD)) tekniğidir.. Buna göre bilgi, verici (transmitter (TX)) tarafında anlık ışık şiddetindeki değişikliklere uyarak kodlanır. Işık şiddetinin değişim hızı MHz mertebesinde olduğundan, bu değişiklikler insan gözüyle algılanamaz. Bununla birlikte, anlık ışık şiddetindeki ufak değişiklikler alıcıdaki PD'ler tarafından sezilerek taşınan bilgi alıcıda (receiver (RX)) yeniden elde edilir.

Geleneksel radyo haberleşme (radio frequency (RF)) sistemlerinden farklı olarak, IM/DD sistemlerinde küçük ölçekli sönümlenme etkileri yok denecek kadar azdır. Bunun nedeni, PD'lerin yüzey alanının, haberleşmenin yapıldığı dalga boyuna (nm) kıyasla önemli ölçüde büyük olmasıdır. Bunun sonucunda, faz değerleri $[-\pi, \pi]$ arasında düzgün dağılmış yayılan ışık dalgalarının toplam fazı, PD'nin geniş alanı üzerinde üst üste binmesinin sonucunda ortalama değeri sıfır olur. Ayrıca, [54] ve [55]'de, VLC kullanıcılarının çoğunun, odanın köşelerinden uzak oldukları sürece, bir doğrudan görüş hattı (line-of-sight (LoS)) kanal ile modellenebileceği bildirilmiştir. Dolayısıyla, MIMO - VLC uygulamalarında çok yollu kanal bileşenlerinin minimum olduğu sonucuna varabiliriz. Başka bir deyişle, bu tür kanallarda sadece LoS bileşeninin etkin olduğu varsayılabilir. Bu nedenle bu projede karşılaşılan optik kanallar, yalnız LoS kanal katsayıları ile tanımlanmaktadır. Alice'in t 'inci vericisi ile k 'inci kullanıcının r 'inci alıcısı arasındaki kanalın LoS katsayılarını, [56] referansında da verildiği gibi, şu şekilde tanımlanır:

$$h_k^{r,t} = \frac{(\beta + 1)A_{PD}}{2\pi(d_k^{r,t})^2} \cos^\beta(\phi_k^{r,t}) \cos(\theta_k^{r,t}) \mathbb{1}_{\Psi_{1/2}}(\theta_k^{r,t}). \quad (3.1)$$

Burada, $\beta = -1/\log_2(\cos(\Phi_{1/2}))$ ışık kaynağının Lambertian emisyon derecesini simgelemektedir. $\Phi_{1/2}$ değişkeni yayın yapan LED'in gücünün yarıya düştüğü açının yarısını göstermektedir. A_{PD} , görüntülemeyen PD'nin etkin alanını belirtir. $d_k^{r,t}$, $\phi_k^{r,t}$ ve $\theta_k^{r,t}$ parametreleri, sırayla t 'inci verici ve r 'inci alıcı arasındaki uzaklığı, ışığın çıkış açısını ve geliş açısını belirtir. Geliş açısının PD'nin görüş alanı (field-of-view (FoV)) içinde olup olmadığı şu fonksiyonla



Şekil 3.1. SCD ile donatılmış çok kullanıcılı MIMO-GSSK-VLC sistem modeli.

belirtilir.

$$\mathbb{1}_{\Psi_{1/2}}(\theta_k^{r,t}) = \begin{cases} 1, & \|\theta_k^{r,t}\| \leq \Psi_{1/2} \text{ ise} \\ 0, & \|\theta_k^{r,t}\| > \Psi_{1/2} \text{ ise} \end{cases}. \quad (3.2)$$

$\Psi_{1/2}$ parametresi PD'nin FOV alanının yarı açısıdır. Alice ve k 'inci kullanıcı arasındaki kanal matrisi ise aşağıdaki şekilde tanımlanmıştır.

$$\mathbf{H}_k = \begin{bmatrix} h_k^{1,1} & h_k^{1,2} & \dots & h_k^{1,N_t} \\ h_k^{2,1} & h_k^{2,2} & \dots & h_k^{2,N_t} \\ \vdots & \vdots & \ddots & \vdots \\ h_k^{N_r,1} & h_k^{N_r,2} & \dots & h_k^{N_r,N_t} \end{bmatrix}. \quad (3.3)$$

Bu kısımda önerdiğimiz çok kullanıcılı (multi user (MU)) MIMO genelleştirilmiş uzay kaydırmalı anahtarlamalı (generalized space shift keying (GSSK)) VLC (MIMO-GSSK-VLC) sistemi Şekil 3.1 ile gösterilmiştir. Bu sistem, geleneksel MU-MIMO-GSSK sisteminden, burada önerilen uzamsal sinyal kümesi tasarımı (spatial constellation design (SCD)) ve bunun içerdiği güç eniyilemesi tekniğiyle ayrılmaktadır. Bu teknik, bir sonraki bölümde detaylıca incelenecektir. Ele aldığımız sistemde, bilginin yayılan ışığın şiddetiyle kodlandığı IM/DD tekniği kullanılmaktadır. Bu teknikte, [57] çalışmasında da belirtildiği gibi, LED'lere uygulanan elektrik akımının bir doğru akım (direct-current (DC)) noktası (B_{DC}) etrafında çeşitlendirilmesiyle, iki kutuplu sinyallerin tek kutuplu ışık şiddetine kodlanabilmesine olanak sağlanmaktadır. Bu teknik, GSSK ile birleştirilip, kanala her erişimde N_t adet LED'den N_a

tanisi aktive edilerek (ışık şiddeti modüle edilerek), bilgi iletimi gerçekleştirilir. Diğer LED'lere ise bir modülasyon işlemi uygulanmaz ve DC noktasında çalıştırılarak yalnızca aydınlanma sağlar. Aktive edilen LED'ler, tüm kullanıcılara ait bilgileri taşıyan bir ortak bit dizisini yaparak MU-GSSK iletimi gerçekleştirilir. Bu sistemde, Alice tarafından bir kanal erişiminde yayılabilecek toplam bit oranı

$$N_B = \left\lfloor \log_2 \left(\frac{N_t}{N_a} \right) \right\rfloor \quad (3.4)$$

ifadesiyle bulunur. Her iletim, her kullanıcıya yalnızca kendi bilgisini aktaracak şekilde tasarlanmaktadır. Bu nedenle,

$$N_B = \sum_{k=1}^K N_B^{(k)} \quad (3.5)$$

olur. Burada, $N_B^{(k)}$, kullanıcı başına düşen bilgi miktarını bit cinsinden ifade eder. Her kanal kullanımında, k 'inci kullanıcının sembol alfabesinden (\mathcal{C}_k) bir bilgi sembolü oluşturulur. Bu sembol alfabesi,

$$\mathcal{C}_k = \{\mathbf{b}_{k,1}, \mathbf{b}_{k,2}, \dots, \mathbf{b}_{k,i_k}, \dots, \mathbf{b}_{k,M_k}\}, \quad (3.6)$$

şeklinde tanımlanmıştır. Burada, $M_k = 2^{N_B^{(k)}}$ değişkeni, \mathcal{C}_k 'daki toplam sembol sayısını, $i_k \in \{1, 2, \dots, M_k\}$ ise sembol indisini ifade eder. \mathbf{b}_{k,i_k} değişkeni, i_k 'inci bilgi sembolüne ait olan bit dizisidir, ve

$$\mathbf{b}_{k,i_k} = [b_{k,i_k}^{(1)}, b_{k,i_k}^{(2)}, \dots, b_{k,i_k}^{(\ell)}, \dots, b_{k,i_k}^{(N_B^{(k)})}], \quad (3.7)$$

şeklinde tanımlanmıştır. Burada, ℓ bit indisini simgeler. Her kanal kullanımında, $k = 1, 2, \dots, K$ kullanıcıları için üretilen \mathbf{b}_{k,i_k} bit dizileri sıralanarak bir ortak bit dizisi oluşturulur. Bu ortak bit dizisi de ortak sembol alfabesi olan \mathcal{C}_S 'ye aittir. Ortak sembol alfabesi,

$$\mathcal{C}_S = \mathcal{C}_1 \times \mathcal{C}_2 \times \dots \times \mathcal{C}_k \times \dots \times \mathcal{C}_K = \{\mathbf{b}_{S,1}, \mathbf{b}_{S,2}, \dots, \mathbf{b}_{S,s}, \dots, \mathbf{b}_{S,M_S}\}, \quad (3.8)$$

şeklinde tanımlanmıştır. Burada, \times Kartezyen çarpımı işlemi simgeler ve $M_S = \prod_k M_k$ şeklinde bulunur. $\mathbf{b}_{S,s}$ bit dizisi, s 'inci ortak sembolü ifade eder ve

$$\mathbf{b}_{S,s} = [\mathbf{b}_{1,i_1}, \mathbf{b}_{2,i_2}, \dots, \mathbf{b}_{k,i_k}, \dots, \mathbf{b}_{K,i_K}], \quad (3.9)$$

şeklinde tanımlanmıştır. Yukarıda da anlatıldığı gibi, \mathbf{b}_{k,i_k} , k 'inci kullanıcının (3.6) denkleminde verilen sembol alfabesinden seçilmiş i_k^{th} 'inci bilgi sembolüne ait olan bit dizisidir. Sembol indisi olan s ,

$$s = \sum_{k=1}^{K-1} \left((i_k - 1) \prod_{j=k+1}^K M_j \right) + i_K, \quad (3.10)$$

ifadesiyle bulunabilir. Bu yüzden, $\mathbf{b}_{S,s}$ ortak bit dizisi, sırayla $k = 1, 2, \dots, K$ 'inci kullanıcılara ait olan $\{i_1, i_2, \dots, i_K\}$ 'inci bilgi sembollerine ait olan bilgileri taşır, ve MU-GSSK-VLC kanalına verilir. Bu iletim esnasında N_t adet LED'den N_a tanesi rastgele seçilir ve

$$\mathbf{I}_{S,s} = [I_{S,s}^{(1)}, I_{S,s}^{(2)}, \dots, I_{S,s}^{(\ell)}, \dots, I_{S,s}^{(N_a)}]^T, \quad (3.11)$$

vektöründe saklanır. Burada, aktif LED indislerini simgeleyen $I_{S,s}^{(\ell)}$ ve $I_{S,s}^{(\ell')}$ değişkenleri, $\ell \neq \ell'$ ve $\ell, \ell' = 1, \dots, N_a$ olacak şekilde $[1, N_t]$ aralığındaki tam sayılardan rastgele seçilir.

Tüm LED'ler tarafından iletilen ışığın şiddeti, B_{DC} değeriyle ve bu noktanın etrafında $\mathbf{b}_{S,s}$ vektörüne ait bilgiyi taşıyan ışık şiddeti değişimlerine göre belirlenir. Her LED'in ışık şiddetinin B_{DC} noktası etrafında ne kadar değiştirileceği $\mathbf{q}_{S,s} \in \mathcal{R}^{N_t \times 1}$ vektörü tarafından belirlenmektedir. $\mathbf{q}_{S,s}$ vektörü ve B_{DC} değeri bir sonraki bölümde önerilen MU-GSSK-SCD sistemine göre tasarlanır. Sonuç olarak, k 'inci kullanıcı ve Eve tarafından alınan sinyaller

$$\mathbf{y}_k = \mathbf{H}_k \left(\mathbf{q}_{S,s} + [(B_{DC})_{\times N_t}]^T \right) + \mathbf{n}_k, \quad (3.12a)$$

$$\mathbf{y}_e = \mathbf{H}_e \left(\mathbf{q}_{S,s} + [(B_{DC})_{\times N_t}]^T \right) + \mathbf{n}_e, \quad (3.12b)$$

olarak bulunur. Burada, $[(B_{DC})_{N_t \times 1}]^T$ vektörü, LED'lerin DC noktasını simgelerken, tüm LED'lerden yayılan ışık şiddeti, $\left(\mathbf{q}_{S,s} + [(B_{DC})_{N_t \times 1}]^T \right)$ vektörüyle ifade edilmiştir. Eve ile k 'inci yetkili kullanıcının kanal durum bilgisi (channel state information (CSI)) sırayla \mathbf{H}_e , $\mathbf{H}_k \in \mathcal{R}^{N_r \times N_t}$ ile gösterilmiştir. Bu kanal matrisleri, (3.3) denkleminde elde edilir Alice'te kullanılmaya hazır durumdadır. $\mathbf{y}_k, \mathbf{y}_e \in \mathcal{R}^{N_r \times 1}$ değişkenleri, sırayla k 'inci kullanıcının ve Eve'in aldığı sinyal vektörleridir. Gürültü vektörleri olan $\mathbf{n}_k, \mathbf{n}_e \in \mathcal{R}^{N_r \times 1}$ ise sırayla $\sigma_k^2 \mathbf{I}_{N_r}$ ve $\sigma_e^2 \mathbf{I}_{N_r}$ kovaryansa sahip, sıfır ortalamalı rastgele Gauss vektörleridir. Burada, \mathbf{I}_{N_r} , boyutları $N_r \times N_r$ olan birim matristir.

Önerilen MU-GSSK-SCD sisteminde, tüm yetkili kullanıcılara ait bilgi sembolleri, tüm aktif LED'ler kullanılarak, $\mathbf{q}_{S,s}$ vektörüyle aynı anda yollar. Bu, [58], [59], [60] gibi çalışmalarda ele alınan, LED kümeleme yönteminden farklı bir yaklaşımdır. Bu kümeleme yönteminde,

her bir ya da birkaç kullanıcı için farklı bir LED kümesi atanır, bizim önerdiğimiz yaklaşımda ise böyle bir kümelemeye gerek yoktur.

Her kanal kullanımında, (3.11) denkleminde uygun olarak, N_a LED aktive edildiğinden, $\mathbf{q}_{S,s}$ vektörünün yalnızca aktive edilen LED indislerine karşılık gelen elemanları sıfırdan büyük olur. Bu nedenle, $\mathbf{q}_{S,s}$ vektörünün sıfıra eşit olan elemanlarının çarptığı \mathbf{H}_k kanal matrisinin sütunlarının, \mathbf{y}_k vektörüne hiçbir katkısı yoktur. Ayrıca, her kullanıcı kendi kanal bilgisine de sahip olduğundan, alıcılarda \mathbf{y}_k vektöründen DC noktası da çıkarılabilir. Böylece, alınan sinyaller,

$$\begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_K \end{bmatrix} = \rho \begin{bmatrix} \tilde{\mathbf{H}}_1 \\ \tilde{\mathbf{H}}_2 \\ \vdots \\ \tilde{\mathbf{H}}_K \end{bmatrix} \tilde{\mathbf{q}}_{S,s} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \\ \vdots \\ \mathbf{n}_K \end{bmatrix}, \quad (3.13)$$

şeklinde yeniden yazılabilir. Burada, $\tilde{\mathbf{H}}_1, \tilde{\mathbf{H}}_2, \dots, \tilde{\mathbf{H}}_K \in \mathcal{R}^{N_r \times N_a}$ matrisleri, $1, 2, \dots, K$ kullanıcılarının katkı sağlayan kanal durum matrisleridir. Bu matrisler, \mathbf{H}_k matrislerinin N_a adet katkı sağlayan sütununu içermektedir. Bunlar da (3.11) denkleminde yer alan $\mathbf{I}_{S,s}$ vektörünün gösterdiği sütunlardır. $\tilde{\mathbf{q}}_{S,s} \in \mathcal{R}^{N_a \times 1}$ vektörü, aktive edilmiş olan N_a adet LED'in yaydığı ışık şiddetinin DC noktası eklenmemiş halini göstermektedir. Yayılan ışık şiddetinin ayrıca ρ parametresiyle normalize edilmesi gerekmektedir ki bu da sıradaki bölümde detaylıca ele alınmıştır.

3.1.1. PLS'nin İyileştirmesi için Uzaysal Takım Tasarımı

Geleneksel GSSK aşağı yöne iletimde (downlink), iletilen sinyalin oluşturduğu uzaysal takım(constellation) noktaları, farklı aktif verici kümeleriyle belirlenir. Bu haberleşmede hedef alıcılar, AP'nin yolladığı her takım noktası için, antenlerin kanal çıktılarının süperpozisyonunu elde ederler. Dolayısıyla, her aktif verici kümesinin alıcıda oluşturduğu sinyal, bir alınmış sinyal takımı oluşturur. Hedef alıcı da, bilgiyi, her elemanı kanal katsayılarına bağlı olan bu alınmış sinyal takımını kullanarak sezimler. Kanal katsayıları, (3.1) denkleminde verilmiştir. Dolayısıyla, VLC için geleneksel GSSK uygulandığında, fiziksel katman güvenliği (physical layer security (PLS)) ağırlıklı olarak sistem konfigürasyonuna, yani alıcı ve vericilerin yer ve yönlerine bağlı olur. Ancak, kullanıcıların alınmış sinyal takımlarını, bahsettiğimiz kanal bağımlılığından kurtararak kullanıcıların bit hata oranını (bit error ratio (BER)) enküçültmek mümkündür. [61] referansında tek kullanıcılı bir MIMO-GSSK-VLC sisteminin BER'i, kullanıcılardaki alınmış sinyal takımlarını akıllıca tasarlayarak enküçültülmüştür. Bu bölümde, MU-MIMO-GSSK-VLC sisteminin yetkili kullanıcılardaki BER'i enküçültlen bir uzaysal sinyal takımı eniyilemesi önerilmekte ve bu sisteme MU-GSSK-SCD adı verilmek-

tedir. MU-GSSK-SCD'ye göre, (3.13) denklemindeki alınmış sinyaller, aşağıda verildiği gibi olacak şekilde, $\tilde{\mathbf{q}}_{S,s}$ vektörünü tasarlanır.

$$\mathbf{y}_k = \rho \mathbf{v}_{k,i_k} + \mathbf{n}_k, \quad 1 \leq k \leq K. \quad (3.14)$$

Burada, ρ normalizasyon katsayısını ve \mathbf{v}_{k,i_k} vektörü de k 'inci kullanıcının i_k indisi bilgi sembolüne karşılık gelen alınmış sinyali simgelemektedir. Alınmış sinyal vektörü \mathbf{v}_{k,i_k} , aşağıda verilen tasarlanan uzaysal sinyal takımına aittir.

$$\mathcal{V}_k : \left\{ \mathbf{v}_{k,i_k} = [v_{k,i_k}^{(1)}, v_{k,i_k}^{(2)}, \dots, v_{k,i_k}^{(N_r)}]^T, 1 \leq i_k \leq M_k \right\}. \quad (3.15)$$

\mathcal{V}_k kümesinin her bir öğesinin seçimi kritiktir çünkü bu kümenin elemanları, k 'inci kullanıcının ve Eve'in BER performanslarını doğrudan etkilemektedir. [62] çalışmasında da belirtildiği gibi, SCD yaklaşımı, bir optik uzaysal modülasyon (optical spatial modulation (OSM)) sistemindeki tek alıcı antenli bir kullanıcının BER'ini enküçültmektedir. Bu enküçültmeyi de, kullanıcının alınmış sinyal takımlarının en küçük ikili Öklit uzaklıklarını, sinyallerin ortalama enerjileri sabitken enbüyüterek sağlamaktadır. [61] çalışması, SCD yaklaşımını MIMO sistemine uygular ve çift kutuplu sinyal takımının N_r uzayında optimal olduğunu gösterir. Bizim çalışmamızda, SCD yaklaşımı çok-kullanıcıli sisteme uygulandığından, \mathcal{V}_k , alınmış uzaysal takımları, N_r boyutlu uzayda ve her k için, optimal olarak M 'li sinyal takımları olarak seçilmiştir. Işık şiddeti vektörü olan $\tilde{\mathbf{q}}_{S,s}$,

$$\tilde{\mathbf{H}}_k \tilde{\mathbf{q}}_{S,s} = \mathbf{v}_{k,i_k}, \quad 1 \leq k \leq K, \quad (3.16)$$

sağlanacak şekilde tasarlanır. Bu sayede (3.14) denklemini de sağlanmış olur. Tüm kullanıcılar tarafından ortak sağlanması gereken (3.16) denklemindeki koşul nedeniyle, (3.16) denklemini

$$\begin{bmatrix} \tilde{\mathbf{H}}_1 \\ \tilde{\mathbf{H}}_2 \\ \vdots \\ \tilde{\mathbf{H}}_K \end{bmatrix} \tilde{\mathbf{q}}_{S,s} = \begin{bmatrix} \mathbf{v}_{1,i_1} \\ \mathbf{v}_{2,i_2} \\ \vdots \\ \mathbf{v}_{K,i_K} \end{bmatrix} \rightarrow \tilde{\mathbf{H}} \tilde{\mathbf{q}}_{S,s} = \mathbf{v}_{S,s}, \quad (3.17)$$

şeklinde yeniden yazılır. Burada, $\tilde{\mathbf{H}}$ matrisi genel kanal matrisini ve $\mathbf{v}_{S,s}$ vektörü de ortak alınmış sinyal vektörünü ifade eder. $\mathbf{v}_{S,s}$ vektörü, (3.8) ifadesindeki \mathcal{C}_S ortak sembol alfabetinin s 'inci öğesine, \mathbf{v}_{k,i_k} vektörü de (3.6) ifadesinden \mathcal{C}_k sembol alfabetinin i_k 'inci öğesine karşılık gelmektedir.

Tablo 3.1’de, 2 kullanıcılı bir GSSK-SCD sistemine optimal bir örnek yer almaktadır. Bu örnekte, $N_t = 6$, $N_a = 3$, $N_r = 3$ ve $K = 2$ alınmış, ve (3.4) denklemini sağlayacak şekilde, kanal kullanımı başına $N_B^{(1)} = N_B^{(2)} = 2$ bit yollanmıştır. Bu nedenle, her iki kullanıcının \mathcal{C}_k sembol alfabeti, (3.6) denklemini sağlayacak şekilde $M_k = 2^{N_B^{(k)}} = 4$ sembol içermektedir. $N_r = 3$ boyutlu bir uzayda, birim enerjili 4 nokta eğer bir düzgün dörtyüzlünün köşelerinde yer alırlarsa, bu noktaların ikili Öklit uzaklıkları enbüyütmüş olur. Bu nedenle, eniyi uzaysal takım noktaları $k = 1, 2$ numaralı kullanıcılar için aşağıdaki gibi bulunur.

$$\begin{aligned} \mathbf{v}_{k,1} &= \left[\sqrt{\frac{8}{9}}, 0, -\frac{1}{3} \right], & \mathbf{v}_{k,2} &= \left[-\sqrt{\frac{2}{9}}, \sqrt{\frac{2}{3}}, -\frac{1}{3} \right], \\ \mathbf{v}_{k,3} &= \left[-\sqrt{\frac{2}{9}}, -\sqrt{\frac{2}{3}}, -\frac{1}{3} \right], & \mathbf{v}_{k,4} &= [0, 0, 1]. \end{aligned}$$

Tablo 3.1. Örnek: 2–Kullanıcılı GSSK-VLC için eniyilenmiş SCD ($N_t = 6$, $N_a = 3$, $N_r = 3$)

i_1	i_2	s	$\mathbf{b}_{S,s}$ (3.9)	$\mathbf{I}_{S,s}$ (3.11)	$\mathbf{v}_{S,s}$ (3.15)
1	1	1	[[0, 0], [0, 0]]	[1, 2, 3]	$[\mathbf{v}_{1,1}, \mathbf{v}_{2,1}]$
1	2	2	[[0, 0], [0, 1]]	[1, 2, 4]	$[\mathbf{v}_{1,1}, \mathbf{v}_{2,2}]$
1	3	3	[[0, 0], [1, 0]]	[1, 2, 5]	$[\mathbf{v}_{1,1}, \mathbf{v}_{2,3}]$
1	4	4	[[0, 0], [1, 1]]	[1, 2, 6]	$[\mathbf{v}_{1,1}, \mathbf{v}_{2,4}]$
2	1	5	[[0, 1], [0, 0]]	[1, 3, 4]	$[\mathbf{v}_{1,2}, \mathbf{v}_{2,1}]$
2	2	6	[[0, 1], [0, 1]]	[1, 3, 5]	$[\mathbf{v}_{1,2}, \mathbf{v}_{2,2}]$
2	3	7	[[0, 1], [1, 0]]	[1, 3, 6]	$[\mathbf{v}_{1,2}, \mathbf{v}_{2,3}]$
2	4	8	[[0, 1], [1, 1]]	[1, 4, 5]	$[\mathbf{v}_{1,2}, \mathbf{v}_{2,4}]$
3	1	9	[[1, 0], [0, 0]]	[1, 4, 6]	$[\mathbf{v}_{1,3}, \mathbf{v}_{2,1}]$
3	2	10	[[1, 0], [0, 1]]	[1, 5, 6]	$[\mathbf{v}_{1,3}, \mathbf{v}_{2,2}]$
3	3	11	[[1, 0], [1, 0]]	[2, 3, 4]	$[\mathbf{v}_{1,3}, \mathbf{v}_{2,3}]$
3	4	12	[[1, 0], [1, 1]]	[2, 3, 5]	$[\mathbf{v}_{1,3}, \mathbf{v}_{2,4}]$
4	1	13	[[1, 1], [0, 0]]	[2, 3, 6]	$[\mathbf{v}_{1,4}, \mathbf{v}_{2,1}]$
4	2	14	[[1, 1], [0, 1]]	[2, 4, 5]	$[\mathbf{v}_{1,4}, \mathbf{v}_{2,2}]$
4	3	15	[[1, 1], [1, 0]]	[2, 4, 6]	$[\mathbf{v}_{1,4}, \mathbf{v}_{2,3}]$
4	4	16	[[1, 1], [1, 1]]	[2, 5, 6]	$[\mathbf{v}_{1,4}, \mathbf{v}_{2,4}]$

(3.17) denklemindeki eniyi alınmış sinyali veren LED ışık şiddeti vektörü, aşağıda ver-

ildiği gibi bir sifıra zorlayan önkodlayıcı ile bulunabilir.

$$\tilde{\mathbf{q}}_{\mathcal{S},s} = \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} \right)^{-1} \tilde{\mathbf{H}}^T \mathbf{v}_{\mathcal{S},s}. \quad (3.18)$$

(3.18) denklemini (3.13) denkleminde yerine koyduğumuzda, yetkili kullanıcılardaki alınmış sinyaller aşağıdaki gibi bulunur.

$$\begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_K \end{bmatrix} = \rho \begin{bmatrix} \mathbf{v}_{1,i_1} \\ \mathbf{v}_{2,i_2} \\ \vdots \\ \mathbf{v}_{K,i_K} \end{bmatrix} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \\ \vdots \\ \mathbf{n}_K \end{bmatrix}. \quad (3.19)$$

(3.19) denklemindeki ifadenin doğruluğu şu şekilde gösterilebilir. $N \leq M$ olacak şekilde, $\mathbf{A} \in \mathcal{R}^{N \times N}$ ve $\mathbf{B} \in \mathcal{R}^{N \times M}$ matrisleri için $\mathbf{A} = \mathbf{B} (\mathbf{B}^T \mathbf{B})^{-1} \mathbf{B}^T = \mathbf{I}_N$ doğrudur. Bunun doğruluğu, \mathbf{A} matrisini \mathbf{B}^T matrisiyle soldan çarptıktan sonra $\mathbf{B}^T \mathbf{A} \equiv \mathbf{B}^T$ ifadesinin sadece $\mathbf{A} = \mathbf{I}_N$ için sağlandığını gözlemleyerek tespit edilebilir. Ayrıca, OWC'de kanal katsayıları, (3.1) ifadesinde verildiği gibi alıcı ve vericilerin yerlerine ve yönlerine bağlı olduğundan, farklı LED-PD çiftleri arasındaki kanallar, kullanıcı yerlerine bağlı olarak birbirlerine çok benzer olabilir. Bu durum, [63] çalışmasında da değinildiği gibi, bazen $\tilde{\mathbf{H}}$ matrisinde doğrusal bağımlı satır ya da sütunlara yol açabilir. Bu durumda, $\mathbf{B} = \tilde{\mathbf{H}}^T \tilde{\mathbf{H}}$ matrisi kötü şartlandırılmış olur. Bunu düzeltmek için, aşağıda gösterildiği gibi, matrisi tam rütbeli yapmak için ϵ gibi küçük değerli bir *düzenleme parametresi* eklenir.

$$\tilde{\mathbf{q}}_{\mathcal{S},s} = \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} + \epsilon \mathbf{I}_{N_a} \right)^{-1} \tilde{\mathbf{H}}^T \mathbf{v}_{\mathcal{S},s}. \quad (3.20)$$

Burada, $\mathbf{I}_{N_a} \in \mathcal{R}^{N_a \times N_a}$ birim matrisi göstermektedir. LED ışık şiddeti vektörü, (3.20), her kullanıcıda eniyi alınmış sinyali oluştururken, (3.19) denkleminde de gösterildiği gibi sıfır kullanıcı girişimini garantiler. Ayrıca, sistemde yalnızca $K = 1$ kullanıcı olduğu zaman (3.17) ifadesinden ötürü $\tilde{\mathbf{H}}$ genel kanal matrisi $\tilde{\mathbf{H}}_1$ 'e, ve $\mathbf{v}_{\mathcal{S},s}$ vektörü de \mathbf{v}_1 'e indirgenir. Bu durumda, tek kullanıcıya gelen sinyalin yine (3.19) ifadesinin $K = 1$ durumunda verildiği gibi olduğunu görebiliriz. Bu çözüm, [61] çalışmasının (13) numaralı denklemindeki çözümle aynıdır. Böylece, önerdiğimiz MU-GSSK-SCD stratejisinin, [61] çalışmasında yer alan tek kullanıcı sistem için de çalıştığını göstermiş bulunmaktayız.

3.1.1.1. Işık Şiddeti Normalizasyonu. Bu bölümde, DC noktası olan B_{DC} ve LED ışık şiddeti normalizasyon katsayısı olan ρ tasarlanmaktadır. [64] çalışmasında belirtildiği gibi, LED'lerde fazla ısınmayı ve elektrooptik verimliliğin düşmesini önlemek için, LED'leri süren akımın belli bir eşığın altında kalması gerekmektedir. Ayrıca, [65] çalışmasında da belirtildiği

gibi LED'lerden haberleşme yaparken aynı zamanda ortama sabit bir aydınlanma vermesi de beklendiğinden, LED'leri süren akımın bir $[I_{\min}, I_{\max}]$ aralığında kalması gerekmektedir. Bu nedenle, $\tilde{\mathbf{q}}_{S,s}$ vektöründeki elemanlar aşağıda verilen aralıkta olmalıdır.

$$I_{\min} < \tilde{q}_{S,s}^{(\ell)} < I_{\max}, \quad \ell = 1, \dots, N_a. \quad (3.21)$$

(3.20) denkleminin bir sonucu olarak, $k = 1, 2, \dots, K$ numaralı kullanıcıların hepsine eniyi olan \mathcal{V}_k kümeleri için $E\{\tilde{\mathbf{q}}_{S,s}\} = 0$ bulunur. Bu yüzden, $B_{DC} = (I_{\min} + I_{\max})/2$ olarak seçmekteyiz. [64] çalışmasında belirttiği gibi, hazır beyaz LED'ler ortalama olarak $I_{\max} = 100$ mA akımının altında çalışmaktadır. Eğer, haberleşme ortamında tercih edilen aydınlatma seviyesi örneğin $B_{DC} = 75$ mA noktasını gerektiriyorsa, $I_{\min} = 50$ mA olarak seçilir. LED ışık şiddeti normalizasyon katsayısı, $\rho = (I_{\max} - I_{\min}) / \max\{\|\tilde{\mathbf{q}}_{S,s}\|\}$ ile hesaplanır. Burada $\max\{\|\tilde{\mathbf{q}}_{S,s}\|\}$, LED ışık şiddeti vektörünün normunun herhangi bir i_k sembolü için alacağı enbüyük değerdir. Bu terimi üstten limitleyecek ifade ise

$$\max\{\|\tilde{\mathbf{q}}_{S,s}\|\} = \max \left\{ \left\| \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} \right)^{-1} \tilde{\mathbf{H}}^T \mathbf{v}_{S,s} \right\| \right\} \prec \max \left\{ \left\| \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} \right)^{-1} \tilde{\mathbf{H}}^T \right\| \right\} \max\{\|\mathbf{v}_{S,s}\|\}, \quad (3.22)$$

olarak bulunur. Sonuçta, k 'inci yetkili kullanıcının aldığı sinyal

$$\mathbf{y}_k = \mathbf{s}_k + \mathbf{n}_k, \quad (3.23)$$

şeklinde ifade edilir. Burada, \mathbf{s}_k vektörü, k 'inci kullanıcı tarafından gözlemlenen yollanan sinyaldir ve

$$\mathbf{s}_k = \rho \tilde{\mathbf{H}}_k \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} + \epsilon \mathbf{I}_{N_a} \right)^{-1} \tilde{\mathbf{H}}^T \mathbf{v}_{S,s} + B_{DC} \tilde{\mathbf{H}}_k, \quad (3.24a)$$

$$= \rho \mathbf{v}_{k,i_k} + B_{DC} \tilde{\mathbf{H}}_k, \quad (3.24b)$$

şeklinde ifade edilebilir. Bu sinyalin DC değeri, alıcının kendi kanal bilgisini kullanmasıyla çıkarılabilir. Eve ise, yollanmış sinyali

$$\mathbf{y}_e = \rho \mathbf{H}_e \mathbf{q}_{S,s} + \mathbf{n}_e \quad (3.25)$$

$$= \rho \mathbf{H}_e \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} + \epsilon \mathbf{I}_{N_a} \right)^{-1} \tilde{\mathbf{H}}^T \mathbf{v}_{S,s} + \mathbf{n}_e, \quad (3.26)$$

şeklinde alır. Eve'in aldığı \mathbf{y}_e sinyali,

$$\mathbf{y}_e = \mathbf{s}_k + \mathbf{J}_k + \mathbf{n}_e, \quad (3.27)$$

şeklinde de ifade edilebilir. Burada, k 'inci kullanıcıyı dinleyen Eve'i etkileyen karıştırma sinyali \mathbf{J}_k ile gösterilir ve

$$\mathbf{J}_k = \rho (\mathbf{H}_e - \mathbf{H}_k) \mathbf{q}_{S,S}, \quad (3.28)$$

olarak ifade edilir. Bu karıştırma sinyali sayesinde \mathbf{v}_{k,i_k} vektörü, Eve tarafında hiçbir k için tam olarak sezimlenemez. Yetkili kullanıcılarda ve Eve'de alınmış olan GSSK sinyali, enbüyük olasılıklı (maximum-likelihood (ML)) sezimlemeyle çözülür. Bu kural,

$$\hat{\mathbf{v}}_k = \arg \min_{\mathbf{v}_{k,i_k}} \{ \|\mathbf{y}_k - \rho \mathbf{v}_{k,i_k}\| \}, \quad (3.29a)$$

$$\hat{\mathbf{v}}_{e,k} = \arg \min_{\mathbf{v}_{k,i_k}} \{ \|\mathbf{y}_e - \rho \mathbf{v}_{k,i_k}\| \}, \quad (3.29b)$$

ile verilmiştir. Burada, $\hat{\mathbf{v}}_k$ ve $\hat{\mathbf{v}}_{e,k}$ ifadeleri sırayla k 'inci kullanıcıda ve k 'inci kullanıcıyı dinleyen Eve'de çözülen bilgi sembolleridir.

3.1.2. VLC'de MIMO SSK Tekniğine Dayanan PLS Algoritmasına İlişkin Gizlilik Oranlarının (Secrecy Rates) Belirlenmesi

Önerilen MU-GSSK-SCD sisteminde, k 'inci kullanıcının gizlilik kapasitesi, [66] çalışmasında belirtildiği gibi, (3.23) ve (3.27) denklemlerinden yola çıkarak aşağıdaki gibi tanımlanır.

$$\begin{aligned} C_{\text{GSSK}}^{(k)} &= \mathbb{I}(\mathbf{s}_k; \mathbf{y}_k) - \mathbb{I}(\mathbf{s}_k; \mathbf{y}_e), \\ &= \mathbb{H}(\mathbf{y}_k) - \mathbb{H}(\mathbf{y}_k | \mathbf{s}_k) - (\mathbb{H}(\mathbf{y}_e) - \mathbb{H}(\mathbf{y}_e | \mathbf{s}_k)). \end{aligned} \quad (3.30)$$

Burada, entropi, koşullu entropi ve ortak bilgi sırayla $\mathbb{H}(\cdot)$, $\mathbb{H}(\cdot|\cdot)$ ve $\mathbb{I}(\cdot;\cdot)$ ile gösterilmiştir. $\mathbb{H}(\mathbf{y}_k | \mathbf{s}_k)$ entropi ifadesi, (3.23) denkleminde yola çıkarak aşağıdaki gibi Gauss entropisi olarak bulunur.

$$\mathbb{H}(\mathbf{y}_k | \mathbf{s}_k) = \frac{N_r}{2} \log_2(2\pi e \sigma_k^2). \quad (3.31)$$

(3.28) denkleminde verilen karıştırıcı sinyali, yaklaşık olarak sıfır ortalamalı $\mathbf{C}_{\mathbf{J}_k}$ kovaryanslı bir Gauss vektörü ile ifade edilebilir. Bu durumda, (3.27) denkleminde gösterilen Eve'in almış olduğu sinyaldeki toplam gürültü, $\mathbf{w}_k = \mathbf{J}_k + \mathbf{n}_e$ şeklinde ifade edilebilir ve sıfır ortalamalı bir Gauss vektörü olur. Bu raslantısal vektörün kovaryans matrisi

$$\mathbf{C}_{\mathbf{w}_k} = \mathbf{C}_{\mathbf{J}_k} + \sigma_e^2 \mathbf{I}_{N_r}, \quad (3.32)$$

şeklinde bulunur. Bu nedenle,

$$\mathbb{H}(\mathbf{y}_e | \mathbf{s}_k) = \frac{1}{2} \log_2(2\pi e |\mathbf{C}_{\mathbf{w}_k}|). \quad (3.33)$$

Bu sayede (3.30) denklemindeki gizlilik kapasitesi,

$$\mathbb{C}_{\text{GSSK}}^{(k)} = \frac{N_r}{2} \log_2 \left(\frac{|\mathbf{C}_{\mathbf{w}_k}|^{1/N_r}}{\sigma_k^2} \right) - (\mathbb{H}(\mathbf{y}_e) - \mathbb{H}(\mathbf{y}_k)), \quad (3.34)$$

olarak bulunur. k' inci kullanıcıya gelen sinyalin, \mathbf{y}_k , ista tistiksel olarak M adet Gauss vektörünün karışımı olması sebebiyle, bu sinyale ait entropi

$$\begin{aligned} \mathbb{H}(\mathbf{y}_k) &\leq \log_2(M) + \frac{N_r}{2} \log_2(2\pi e \sigma_k^2) \\ &= \frac{N_r}{2} \log_2 \left(2\pi e \sigma_k^2 M^{2/N_r} \right), \end{aligned} \quad (3.35)$$

ifadesiyle üstten limitlidir. Eve'in aldığı sinyalin entropisi, $\mathbb{H}(\mathbf{y}_e)$, de $\mathbf{y}_e = \mathbf{y}_k + \hat{\mathbf{n}}_k$ denkleminde, [67] çalışmasında verilen, entropi-güç eşitsizliği (EPI) uygulanarak alttan limitlenir. Bu ilişkide, $\hat{\mathbf{n}}_k = \mathbf{w}_k - \mathbf{n}_k$ daha büyük güce sahip olan gürültü terimidir. EPI kuralına göre,

$$\begin{aligned} \mathbb{H}(\mathbf{y}_e) &= \mathbb{H}(\mathbf{y}_k + \hat{\mathbf{n}}_k) \\ &\geq \frac{N_r}{2} \log_2 \left(2^{(2/N_r)} \mathbb{H}(\hat{\mathbf{n}}_k) + 2^{(2/N_r)} \mathbb{H}(\mathbf{y}_k) \right) \\ &= \frac{N_r}{2} \log_2 \left(2\pi e |\mathbf{C}_{\hat{\mathbf{n}}_k}|^{(1/N_r)} + 2^{(2/N_r)} \mathbb{H}(\mathbf{y}_k) \right), \end{aligned} \quad (3.36)$$

bulunur. Burada, $\hat{\mathbf{n}}_k$ raslantısal vektörünün kovaryans matrisi $\mathbf{C}_{\hat{\mathbf{n}}_k} = \mathbf{C}_{\mathbf{w}_k} - \sigma_k^2 \mathbf{I}_{N_r}$ ile gösterilmiştir. Şimdi, (3.34) denkleminde (3.35) ve (3.36) ifadelerinin uygulanmasıyla

$$\mathbb{C}_{\text{GSSK}}^{(k)} \leq \frac{N_r}{2} \log_2 \left(\frac{|\mathbf{C}_{\mathbf{w}_k}|^{(1/N_r)} M^{(2/N_r)}}{\sigma_k^2 M^{(2/N_r)} + |\mathbf{C}_{\mathbf{n}_k}|^{(1/N_r)}} \right), \quad (3.37)$$

elde edilir. Ulaşılabilir gizlilik oranı bölgesi, $(R^{(1)}, R^{(2)}, \dots, R^{(K)})$, [68] çalışmasında ve aşağıda verilen ortak üst limiti sağlayan kullanıcı gizlilik oranlarının tamamının oluşturduğu bölgedir.

$$\sum_{k=1}^K 2^{R^{(k)}} \leq \sum_{k=1}^K 2^{\mathbb{C}_{\text{GSSK}}^{(k)}}. \quad (3.38)$$

Burada, $\mathbb{C}_{\text{GSSK}}^{(k)}$ ifadesi, $k = 1, 2, \dots, K$ için (3.37) denklemini sağlamaktadır. Sıradaki bölümde, önerdiğimiz MU-GSSK-SCD tekniğinin gizlilik oranı bölgeleri incelenecektir.

3.2. Görünür Işıkla Haberleşmede bir NOMA Tabanlı PLS Algoritması Geliştirilmesi

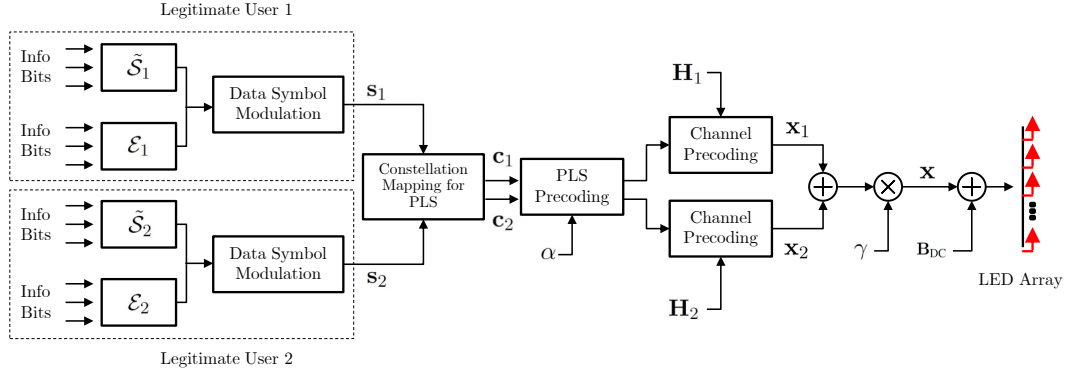
Bu kısımda, erişim noktası olan Alice'in 2 hareketsiz yasal kullanıcı (Bob) grubuyla iletişim kurduğu bir iç mekan MIMO-NOMA-VLC sistemini ele alıyoruz. Bu sistemde, Alice her iletimde yasal kullanıcılar için ayrı ayrı bilgi sembolü üretir ve onların süperpozisyonunu oluşturarak NOMA bilgi sembolünü elde eder. Bu NOMA sembolü, daha sonra LED dizisiyle yasal kullanıcılara görünür ışık kanalı üzerinden yollar. Bu sırada yetkisiz kullanıcı olan Eve bu iletimi kendi kanalı üzerinden dinler. Önerilen PLS ön kodlama şeması, Eve'in aldığı NOMA sembolünü başarılı bir şekilde çözmesini önlemek amacıyla tasarlanmıştır.

Alice, iletim birimi olarak N_t adet LED ile donatılmıştır. Boblar ve Eve ise alıcı birimleri olarak her biri N_r adet fotodetektörden (photodetector (PD)) oluşan alıcı birimini kullanır. Bilginin, LED'lerden yayılan ışık şiddetini kiplediği, doğru akım (direct current (DC))-noktalı yoğunluk-modülasyonlu/doğrudan sezimleme (intensity modulation / direct detection (IM/DD)) tekniği kullanılır. Alıcı birimlerdeki PD'ler, alınan ışığı kod çözme işlemi gerçekleştirmek için kullanılan elektrik akımına dönüştürür. Bu senaryoda tüm kullanıcılar ve Alice sabit olduğundan, iç mekan VLC kanalı zamanla değişmez olarak kabul edilebilir. Ayrıca, VLC sistemlerindeki kanalın sönmüleme etkileri, RF iletişim sistemlerindeki çok daha küçüktür. Bunun nedeni, [54] referansında belirtildiği gibi, kullanılan PD'lerin alanının, bilginin taşındığı görünür ışığın dalga boyuna kıyasla çok büyük olmasıdır. Ayrıca, [74] referansında belirtildiği gibi, kullanıcılar kenarlardan ve duvarlardan uzakta olduklarında, yansıyan ışık dalgalarının sönmüleme etkisi oldukça küçüktür. Bu nedenle, iç mekan VLC kanalı, yalnızca görüş hattı bileşeni kullanılarak tanımlanabilir. LED'lerden yayılan ışık yoğunluğunu $\mathbf{x} \in \mathfrak{R}^{N_t \times 1}$ vektörü ile gösterilirse, k 'inci kullanıcıda alınan sinyal

$$\mathbf{y}_k = \mathbf{H}_k(\mathbf{x} + \mathbf{B}_{DC}) + \mathbf{n}_k, \quad (3.39)$$

biçiminde ifade edilebilir. Burada, \mathbf{H}_k , Alice ile k 'inci yasal kullanıcı arasındaki (3.1) de verilen kanal matrisini, $\mathbf{n}_k \in \mathfrak{R}^{N_r \times 1}$, PD'lerdeki ısı gürültüden kaynaklanan bozulmayı modelleyen sıfır ortalamalı toplamsal beyaz Gauss gürültü (additive white Gaussian noise (AWGN)) vektörünü göstermektedir. \mathbf{n}_k 'nin kovaryans matrisi $(\sigma_n^2/N_r)\mathbf{I}_{N_r}$ olarak tanımlanmıştır. \mathbf{I}_{N_r} ise birim matrisi göstermektedir. DC noktasını ifade eden $\mathbf{B}_{DC} \in \mathfrak{R}^{N_t \times 1}$ vektörü, hem Alice hem de tüm alıcılar tarafından bilinmekte olup, LED ışık şiddeti vektörünün negatif değerler almamasını ve böylece iletilen sinyalin LED çalışma özellikleri nedeniyle kırılmamasını sağlar. LED ışık şiddetini gösteren \mathbf{x} vektörü,

$$\mathbf{x} = \gamma(\sqrt{\alpha}\mathbf{s}_1 + \sqrt{1-\alpha}\mathbf{s}_2), \quad (3.40)$$



Şekil 3.2. Önerilen PLS Önkodlama tasarımı için verici tasarımı.

ile verildiği üzere yasal kullanıcılara yollanan bilgi sembollerinin üst üste toplanmasıyla bulunur. Burada, s_k , k 'inci kullanıcıya ait birim ortalama enerjili bilgi sembolü vektörüdür. Birinci yasal kullanıcının sinyal gücünün toplam sinyal gücündeki oranı α ile, toplam sinyal genliği ise γ ile gösterilmektedir. Toplam sinyal genliği olan γ , iletilen ışık şiddetinin LED'lerin sınırlı dinamik aralığında olacak şekilde tasarlanmıştır. Bu durumda, iletilen NOMA sembolü, yasal kullanıcılar tarafından (3.39) ile verilen ifadeye göre alınır. Standart NOMA sistemlerinde, kanal katsayısı daha düşük olan (zayıf) kullanıcıya oransal olarak daha yüksek bir sinyal gücü atanır ve bu kullanıcı, bilgisini doğrudan enyüksek olabirlikli (maximum likelihood (ML)) sezimleme ile çözer. Güçlü kullanıcılara ise oransal olarak daha düşük bir sinyal gücü atanır ve bu kullanıcılar öncelikle zayıf kullanıcı bilgilerini ardışık girişim iptali (successive interference cancellation (SIC)) ile yok ettikten sonra ML sezimleme uygular.

İletilen NOMA-VLC sinyali, Alice'den kullanıcılara aktarılan γ, α, B_{DC} parametrelerini elde edebilen bir yasal olmayan kullanıcı tarafından gelen pasif gizli dinleme saldırılarına açıktır. Bu tarz tehditlere karşı koymak için, Şekil 3.2'de görselleştirilen rassal takımsembol eşlemesi ile güçlendirilmiş bir PLS ön kodlayıcı tasarlıyoruz. Önerilen ön kodlayıcı ile iletilen sinyal, hedef kullanıcıda yalnızca 1 PD'yi etkinleştirmektedir. Benimsenen PD seçim stratejisi, takımsembol kümesini genişleterek iletim başına yollanabilecek bit miktarını artırır. PD seçimi için, M elemanlı takımsembol kümesi ve k 'inci kullanıcı için uzamsal takımsembol kümesi sırasıyla

$$\tilde{\mathcal{S}}_k = \{s_k^1, s_k^2, \dots, s_k^M\}, \quad (3.41)$$

$$\mathcal{E}_k = \{e_1, e_2, \dots, e_{N_r}\}, \quad k = 1, 2, \quad (3.42)$$

şeklinde tanımlanır. Tanımlanan \mathcal{E}_k kümesinden seçilen e_j vektörü, k 'inci yasal kullanıcının hangi PD'sinin aktive edileceğini göstermektedir. Burada e_j $j = 1, \dots, N_r$ için, $\{N_r \times N_r\}$ birim matrisinin j 'inci sütununu ifade etmektedir. Alınan takımsembolü kümesi, k 'inci kul-

lanıcı için s_k^i ve e_j çarpılmasıyla

$$\mathcal{S}_k = \{s_k^1 \mathbf{e}_1, s_k^2 \mathbf{e}_1, \dots, s_k^i \mathbf{e}_j, \dots, s_k^M \mathbf{e}_{N_r}\}, \quad (3.43)$$

şeklinde elde edilir. Burada $s_k^i \mathbf{e}_j$ vektörü, j 'inci elemanı s_k^i olan N_r uzunluğunda bir vektördür. Buradan itibaren, \mathcal{S}_k kümesinden seçilen sembolü, s_k ile ifade edeceğiz. Bilgi sembolü olan s_k , $m^{(k)} = \log_2(MN_r)$ bitlik bilgi taşımaktadır. Görüldüğü gibi, \mathcal{E}_k uzaysal takımsembolünün kullanılmasıyla, $\tilde{\mathcal{S}}_k$ kümesi daha büyük bir takımsembol olan \mathcal{S}_k kümesine genişletilmiş ve sembol başına aktarılan bit miktarı artırılmıştır. Önerilen algoritmada, PLS iki bileşenle sağlanmaktadır. İlk bileşen, Alice'de oluşturulan $\mathbf{C} \in \mathbb{R}^{N_r \times N_r}$ rastgele takımsembol matrisidir. Üretilen s_k sembolü, \mathbf{C} matrisiyle çarpılarak

$$\mathbf{c}_k = \mathbf{C} s_k, \quad (3.44)$$

kod sembol vektörü elde edilir. İkinci bileşen, k 'inci kullanıcıya özel \mathbf{Q}_k Önkodlama matrisidir. Bu matris

$$\mathbf{Q}_k = \begin{bmatrix} q_k(1) & 0 & \dots & 0 \\ 0 & q_k(2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & q_k(N_r) \end{bmatrix}_{(N_r \times N_r)}, \quad (3.45)$$

olarak tanımlanmış olup bir köşegen matristir. Önkodlama matrisi olan \mathbf{Q}_k 'in tasarımı, bir sonraki bölümde detaylı olarak ele alınacaktır. Tüm bu bileşenleri içeren bilgi sinyali, k 'inci kullanıcı için

$$\mathbf{x}_k = \beta_k \mathbf{P}_k \mathbf{Q}_k \mathbf{C} s_k, \quad (3.46)$$

şeklinde tanımlanır. Burada, $\mathbf{P}_k \in \mathbb{R}^{N_t \times N_r}$, yasal kullanıcılarda gözlemlenen kanal etkilerini ortadan kaldırmak için

$$\mathbf{P}_k = (\mathbf{H}_k^T \mathbf{H}_k)^{-1} \mathbf{H}_k^T, \quad (3.47)$$

şeklinde tanımlanmıştır. Yukarıda (3.46) ile verilen ifadedeki β_k katsayısı, k 'inci kullanıcının

kanal katsayılarına bağlı olup

$$\beta_k = \sqrt{N_r / \text{tr}(\mathbf{H}_k^T \mathbf{H}_k)}, \quad (3.48)$$

şeklinde hesaplanır. Burada, $\text{tr}(\cdot)$, matrisin ilköşegen toplamını göstermektedir. Sonra, Alice \mathbf{x}_1 ve \mathbf{x}_2 vektörlerini

$$\mathbf{x} = \gamma(\mathbf{x}_1 + \mathbf{x}_2). \quad (3.49)$$

şeklinde üst üste toplayarak iletilecek olan NOMA sembolünü elde eder. NOMA güç oranı, $\alpha = \beta_1^2 / (\beta_1^2 + \beta_2^2)$ ifadesi üzerinden β_k 'ye bağlıdır. Burada, kanal kazancı daha yüksek olan kullanıcıya, (3.48) içindeki β_k tasarımından dolayı (3.49) ile verilen ifadede daha düşük iletim gücü atanır. NOMA sembolü, DC noktası ilavesinin ardından iletilir ve k 'inci kullanıcı tarafından

$$\mathbf{y}_k = \mathbf{H}_k(\mathbf{x} + \mathbf{B}_{DC}) + \mathbf{n}_k, \quad k = 1, 2, \quad (3.50)$$

şeklinde alınır.

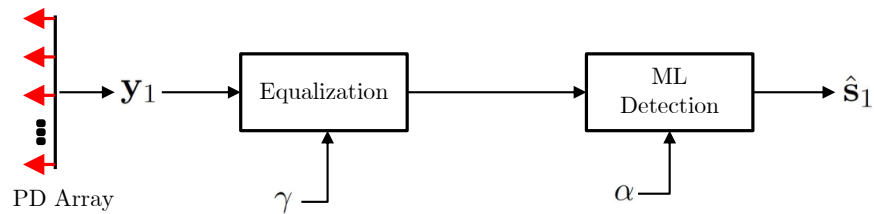
3.2.1. Önerilen PLS Sağlayıcı NOMA Önkodlayıcı Tasarımı

Bir önceki bölümde (3.50) ifadesindeki alıcıya gelen NOMA sinyali

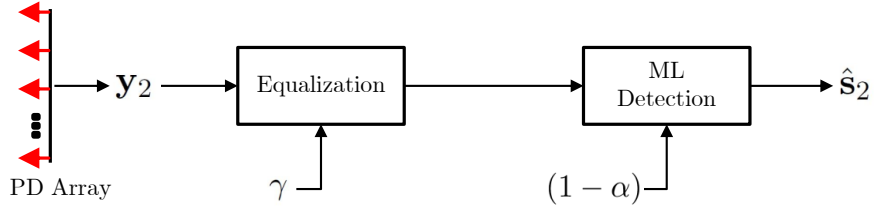
$$\mathbf{y}_1 = \beta_1 \mathbf{H}_1 \mathbf{P}_1 \mathbf{Q}_1 \mathbf{c}_1 + \beta_2 \mathbf{H}_1 \mathbf{P}_2 \mathbf{Q}_2 \mathbf{c}_2 + \mathbf{n}_1, \quad (3.51a)$$

$$\mathbf{y}_2 = \beta_1 \mathbf{H}_2 \mathbf{P}_1 \mathbf{Q}_1 \mathbf{c}_1 + \beta_2 \mathbf{H}_2 \mathbf{P}_2 \mathbf{Q}_2 \mathbf{c}_2 + \mathbf{n}_2, \quad (3.51b)$$

biçiminde yazılabilir.



Şekil 3.3. Önerilen önkodlayıcı için Kullanıcı 1'deki alıcı tasarımı.



Şekil 3.4. Önerilen önkodlayıcı için Kullanıcı 2'deki alıcı tasarımı.

Kanal ters çevirme matrisi, (3.47) ifadesinde verildiği gibi tasarlandığından,

$$\mathbf{H}_k(\mathbf{H}_k^T \mathbf{H}_k)^{-1} \mathbf{H}_k^T = \mathbf{I}_{N_r}, \quad (3.52)$$

ifadesi sağlanır ve yasal kullanıcılardaki kanal etkileri sıfırlanır. Ek olarak, PLS önkodlayıcı olan \mathbf{Q}_k matrisi de bir köşegen matrisi olduğundan,

$$\mathbf{Q}_k \mathbf{c}_k = \text{diag}(\mathbf{c}_k) \mathbf{q}_k, \quad (3.53)$$

ifadesiyle yeniden yazılabilir. Burada $\text{diag}(\cdot)$ operatörü, argümanı olan $N \times 1$ boyutundaki vektörün elemanlarını kullanarak $N \times N$ boyutlarında bir köşegen matris üretir. Benzer olarak, $\mathbf{q}_k \in \mathbb{R}^{N_r \times 1}$ vektörü de \mathbf{Q}_k matrisinin ilkköşegenindeki elemanları içermekte olup

$$\mathbf{q}_k = \text{diag}(\mathbf{Q}_k) = [q_k(1), q_k(2), \dots, q_k(N_r)]^T, \quad (3.54)$$

olarak tanımlanmıştır. Yukarıda (3.51) ile verilen ifadedeki alınan sinyaller, (3.52), (3.53) ve (3.54) ile verilen ifadeleri kullanarak

$$\begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} = \mathbf{V} \mathbf{q} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \end{bmatrix}, \quad (3.55)$$

şeklinde matris-vektör çarpımı cinsinden yazılabilir. Burada,

$$\mathbf{V} = \begin{bmatrix} \beta_1 \text{diag}(\mathbf{c}_1) & \beta_2 \mathbf{H}_1 \mathbf{P}_2 \text{diag}(\mathbf{c}_2) \\ \beta_1 \mathbf{H}_2 \mathbf{P}_1 \text{diag}(\mathbf{c}_1) & \beta_2 \text{diag}(\mathbf{c}_2) \end{bmatrix}, \mathbf{q} = \begin{bmatrix} \mathbf{q}_1 \\ \mathbf{q}_2 \end{bmatrix} \quad (3.56)$$

sağlanır. Alınan sinyaller, (3.56)'da gösterildiği gibi hem kullanıcı bilgisinden hem de kullanıcılar arası girişimden oluşur. Bu noktada, hem \mathbf{y}_k 'daki girişimi kaldırmayı hem de Eve'de

alınan sinyali bozmayı amaçlıyoruz. Bu nedenle \mathbf{q}_k vektörü,

$$\mathbf{q} = \begin{bmatrix} \mathbf{q}_1 \\ \mathbf{q}_2 \end{bmatrix} = \mathbf{V}^{-1} \begin{bmatrix} \sqrt{\alpha} \mathbf{s}_1 \\ \sqrt{(1-\alpha)} \mathbf{s}_2 \end{bmatrix}, \quad (3.57)$$

şeklinde tasarlanır. Burada sinyal güçleri kullanıcılar arasında

$$\alpha = \beta_1^2 / (\beta_1^2 + \beta_2^2), \quad (3.58)$$

katsayısıyla paylaşılır. Önkodlama matrisleri de \mathbf{q}_k vektörleri kullanılarak

$$\mathbf{Q}_k = \text{diag}(\mathbf{q}_k), \quad (3.59)$$

ile bulunur. Sonunda, \mathbf{x}_k vektörü önceki bölümdeki (3.46) ifadesine uygun olarak bulunup LED'lerin ışık şiddeti kiplenir.

3.2.2. DC Noktası ve γ Tasarımı

Yukarıda, (3.49)'deki ifadede verilen NOMA sembolünün başarılı bir şekilde iletilebilmesi için, LED'ler her zaman kendi dinamik aralıklarında çalışmalıdır. Aksi takdirde, VLC sinyalleri LED'lerin ışık şiddeti kiplenirken kırılabilir. Ayrıca, LED'ler aşırı ısınabilir ve sürüş akımları maksimum eşiği aşarsa [70] referansında belirtildiği gibi optoelektronik verimlilikleri düşebilir. Bu nedenle, \mathbf{x} vektörü elemanları,

$$I_{\min} < \mathbf{x}^{(t)} < I_{\max}, \quad t = 1, \dots, N_t, \quad (3.60)$$

aralığında kalmaya zorlanır. Burada, $\mathbf{x}^{(t)}$, \mathbf{x} ögesinin t 'inci elemanını belirtir. İnsan gözünün ışık şiddetine olan hassasiyeti için iletişim sırasında LED'ye gelen ortalama akımın, [69] referansında belirtildiği gibi, sabit bir seviyeyi koruması gerekir. Bu nedenle, LED'lere gelen akım, iç ortamın aydınlatma gereksinimleri tarafından belirlenen $\mathbf{B}_{\text{DC}} = (I_{\min} + I_{\max})/2$ noktasına kutuplanır. Örnek olarak, aydınlatma tercihlerinin $B_{\text{DC}} = 75$ mA gerektirdiğini varsayalım. Kullanıma hazır LED'ler [73]'de belirtildiği gibi genellikle ortalama olarak $I_{\max} = 100$ mA altında çalıştığından, I_{\min} değeri 50 mA olarak ayarlanır.

Ardından, iletilen sinyal genliği, $\gamma = (I_{\max} - I_{\min}) / \max\{\|\mathbf{x}_1 + \mathbf{x}_2\|\}$ ile hesaplanır. Burada, $\max\{\|\mathbf{x}_1 + \mathbf{x}_2\|\}$, herhangi bir \mathbf{c}_k vektörü için, LED ışık şiddeti vektörünün olabilecek

enbüyük normunu verir. $\max\{\|\mathbf{x}_1 + \mathbf{x}_2\|\}$ ifadesi için bir üst sınır,

$$\max\{\|\mathbf{x}_1 + \mathbf{x}_2\|\} \prec \sum_{\forall k} \beta_k \mathbf{P}_k \max\{\|\mathbf{Q}_k\|\} \max\{\|\mathbf{c}_k\|\},$$

ifadesinden bulunabilir. Sonuç olarak, LED ışık şiddeti vektörü,

$$\mathbf{x} = \gamma(\beta_1 \mathbf{P}_1 \mathbf{Q}_1 \mathbf{c}_1 + \beta_2 \mathbf{P}_2 \mathbf{Q}_2 \mathbf{c}_2) + \mathbf{B}_{DC}, \quad (3.61)$$

olarak ifade edilir. Yasal kullanıcılar, (3.61) denkleminde gösterilen iletim sinyalini, (3.50)'deki ifadeye uygun olarak alırlar. Alınan sinyaldeki DC noktası kaldırılır ve

$$\begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} = \gamma \begin{bmatrix} \sqrt{\alpha} \mathbf{s}_1 \\ \sqrt{(1-\alpha)} \mathbf{s}_2 \end{bmatrix} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \end{bmatrix}, \quad (3.62)$$

elde edilir. Burada \mathbf{Q} matrisinin (3.57)'deki ifadeyi sağlaması kullanılmıştır. Sonra, k 'inci yasal kullanıcı, kendi bilgisini ML sezimlemesi ile Şekil 3.3 ve 3.4'de gösterildiği gibi çözer. Buna göre

$$\hat{\mathbf{s}}_1 = \arg \min_{\mathbf{s}_1 \in \mathcal{S}_1} \{\|\mathbf{y}'_1 - \sqrt{\alpha} \mathbf{s}_1\|\}, \quad (3.63)$$

$$\hat{\mathbf{s}}_2 = \arg \min_{\mathbf{s}_2 \in \mathcal{S}_2} \{\|\mathbf{y}'_2 - \sqrt{(1-\alpha)} \mathbf{s}_2\|\} \quad (3.64)$$

ifadeleri sezimlenmiş sembolleri belirtir. Burada, $\mathbf{y}'_k = \mathbf{y}_k/\gamma$ ve $\mathbf{n}'_k = \mathbf{n}_k/\gamma$ olarak tanımlanmıştır. Önerilen PLS önkodlayıcı sayesinde yasal kullanıcılar kendi bilgilerini, kanal etkileri ve diğer kullanıcılardan gelen girişimler olmaksızın bilinen γ katsayısıyla orantılı olarak elde ederler. Öte yandan, Eve'in aldığı sinyal olan \mathbf{y}_e , \mathbf{H}_e Alice'te tanımlanmamış bir kanal olduğu için, oldukça bozulmuştur. Bu bozulmayı,

$$\mathbf{y}_e = \gamma \sqrt{\alpha} \mathbf{s}_1 + \mathbf{J}_1 + \mathbf{n}_e, \quad (3.65a)$$

$$= \gamma \sqrt{(1-\alpha)} \mathbf{s}_2 + \mathbf{J}_2 + \mathbf{n}_e, \quad (3.65b)$$

şeklinde ifade edilen Eve'in aldığı sinyalde de görebiliriz. Burada, \mathbf{J}_k , Eve k 'inci kullanıcıyı dinlerken aldığı sinyale karışan jamming sinyali olup \mathbf{Q}_k kaynaklıdır. Bu sinyal,

$$\mathbf{J}_k = (\mathbf{H}_e - \mathbf{H}_k) \mathbf{x}, \quad (3.66)$$

şeklinde ifade edilir. Eve yine de s_k sinyalini

$$\hat{s}_e^{(1)} = \arg \min_{s_1 \in \mathcal{S}_1} \{ \|\mathbf{y}_e - \gamma \sqrt{\alpha} \mathbf{s}_1\| \}, \quad (3.67a)$$

$$\hat{s}_e^{(2)} = \arg \min_{s_2 \in \mathcal{S}_2} \{ \|\mathbf{y}_e - \gamma \sqrt{(1-\alpha)} \mathbf{s}_2\| \}, \quad (3.67b)$$

ile ML sezimlemesi kullanarak çözmeye çalışabilir. Yukarıdaki ifadede, γ ve α Eve tarafından bilinmektedir.

3.2.3. Görünür Işıqla Haberleşmede (VLC) Önerilen NOMA Tabanlı Fiziksel Katman Güvenlik Algoritmasının Gizlilik Analizi

Bu iş paketinde, önerilen MIMO-NOMA-VLC sisteminin gizlilik oranları alt ve üst limitleriyle birlikte türetilmiştir. Önerilen MIMO-NOMA-VLC sisteminin gizlilik kapasitesi, [80]

$$\mathbb{C}_s^{(k)} = \mathbb{C}_k - \mathbb{C}_e^{(k)}, \quad k = 1, 2, \quad (3.68)$$

ifadesiyle bulunabilir. Burada \mathbb{C}_k ve $\mathbb{C}_e^{(k)}$ sırasıyla k 'inci kullanıcının ve Eve'in kanal kapasitelerini ifade etmektedir. Önerilen önkodlanmış MIMO-NOMA sisteminde, bilgi \mathcal{S}_1 ve \mathcal{S}_2 semboltakımlarıyla iletilmekte, k 'inci kullanıcıda ve Eve'de

$$\begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} = \gamma \begin{bmatrix} \sqrt{\alpha} \mathbf{s}_1 \\ \sqrt{(1-\alpha)} \mathbf{s}_2 \end{bmatrix} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \end{bmatrix}, \quad (3.69)$$

$$\mathbf{y}_e = \gamma \sqrt{\alpha} \mathbf{s}_1 + \mathbf{J}_1 + \mathbf{n}_e, \quad (3.70)$$

$$= \gamma \sqrt{(1-\alpha)} \mathbf{s}_2 + \mathbf{J}_2 + \mathbf{n}_e, \quad (3.71)$$

ifadelerine göre alınmaktadır. Bu nedenle, bu VLC sistemi, çok kullanıcılı ayırık sürekli belleksiz kanal (discrete continuous memoryless channel (DCMC)) olarak tanımlanabilir. Buna göre, k 'inci kullanıcının DCMC kapasitesi, [72] referansında belirtildiği gibi

$$\mathbb{C}_k = \max_{\mathcal{P}} \sum_{i=1}^{MN_r} \int_{-\infty}^{\infty} p(\mathbf{y}_k, \mathbf{s}_k^{(i)}) \log_2 \left(\frac{p(\mathbf{y}_k, \mathbf{s}_k^{(i)})}{\sum_{j=1}^{MN_r} p(\mathbf{y}_k, \mathbf{s}_k^{(j)})} \right) d\mathbf{y}_k, \quad (3.72)$$

for $\mathcal{P} = \{p(\mathbf{s}_k^1), \dots, p(\mathbf{s}_k^{MN_r})\}$,

olarak bulunur. Burada, $p(\cdot)$, olasılığı, $\mathbf{s}_k^{(\cdot)}$ ise \mathcal{S}_k 'dan seçilen bilgi sembolünü belirtir. Ayırık semboltakımları için, (3.72)'teki ifade $i = 1, \dots, MN_r$ için $p(\mathbf{s}_k^i) = 1/(MN_r)$ ile enyükseltir.

$p(\mathbf{y}_k, \mathbf{s}_k^{(\cdot)})$ ögesinin bir Gauss dağılımını tanımladığı göz önüne alındığında, integraller [72]'daki gibi hesaplanabilir ve DCMC kapasitesi,

$$\mathbb{C}_k = \log_2(MN_r) - \frac{1}{MN_r} \sum_{i=1}^{MN_r} \mathbb{E} \left[\log_2 \left(\sum_{j=1}^{MN_r} \exp(\Omega_k^{ij}) \right) \right],$$

$$\text{for } \Omega_k^{ij} = \frac{-\|\rho_k(\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)}) + \mathbf{n}_k\|^2 + \|\mathbf{n}_k\|^2}{\sigma_n^2}, \quad (3.73)$$

olarak bulunur. Burada, $\mathbb{E}[\cdot]$ istatistiksel ortalama operasyonunu ifade ederken sinyal katsayıları

$$\rho_1 = \gamma\sqrt{\alpha}, \quad (3.74)$$

$$\rho_2 = \gamma\sqrt{1-\alpha}, \quad (3.75)$$

olarak tanımlanmıştır. Eve'nin alınan sinyalinde önkodlama kaynaklı ortaya çıkan jamming sinyali, bir rastgele vektördür ve yaklaşık olarak sıfır ortalamalı Gauss dağılımından geldiği varsayılabilir. Dolayısı ile, jamming sinyalini kullanarak $\mathbf{w}_e^{(k)} \triangleq \mathbf{J}_k + \mathbf{n}_e$ şeklinde başka bir rastgele Gauss vektörü tanımlayabiliriz. Bu vektörün kovaryans matrisi

$$\text{Cov}(\mathbf{w}_e^{(k)}) = \mathbb{E} [\mathbf{J}_k \mathbf{J}_k^T] + \sigma_n^2, \quad (3.76)$$

ifadesiyle bulunur. Yukarıdaki ifade, gürültü ve jamming sinyallerinin birbirlerinden bağımsız süreçlerden geldiği için doğrudur. Sonra, Eve'in kanal kapasitesi olan $\mathbb{C}_e^{(k)}$, (3.72) ifadesine uygun olarak

$$\Omega_{e,k}^{ij} = \frac{-\|\rho_k(\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)}) + \mathbf{w}_e^{(k)}\|^2 + \|\mathbf{w}_e^{(k)}\|^2}{\det(\text{Cov}(\mathbf{w}_e^{(k)}))^{(1/N_r)}}, \quad (3.77)$$

şeklinde bulunabilir. Burada, $\det(\cdot)$ determinant işlemini ifade eder. Son olarak, k 'inci kullanıcının kanal kapasitesi de (3.73) ifadesiyle bulunur.

3.2.3.1. Ulaşılabilir Gizlilik Oranlarının Limitleri. Bu bölümde, önerilen NOMA iletim Önkodlama stratejisiyle ulaşılabilecek gizlilik oranları için üst ve alt limitler türetiyoruz. Öncelikle,

(3.73) ifadesi,

$$\mathbb{C}_s^{(k)} = \mathbb{I}(\mathbf{y}_k; \mathbf{s}_k) - \mathbb{I}(\mathbf{y}_e^{(k)}; \mathbf{s}_k), \quad (3.78)$$

$$= \mathbb{h}(\mathbf{y}_k) - \mathbb{h}(\mathbf{y}_k | \mathbf{s}_k) - \mathbb{h}(\mathbf{y}_e^{(k)}) + \mathbb{h}(\mathbf{y}_e^{(k)} | \mathbf{s}_k), \quad (3.79)$$

şeklinde ortak bilgiler (mutual information) cinsinden yeniden yazılır. Burada, $\mathbb{I}(\cdot; \cdot)$ karşılıklı bilgiyi, $\mathbb{h}(\cdot)$, $\mathbb{h}(\cdot | \cdot)$ ise sırasıyla ayrımsal entropiyi (differential entropy) ve koşullu ayrımsal entropiyi (conditional differential entropy) göstermektedir. Kanala erişim sayısının çok yüksek olduğu durumda, $\mathbf{J}_k + \mathbf{n}_e$ vektörünün aldığı değerler Gauss dağılımına yakınsar. Bu nedenle, koşullu ayrımsal entropi

$$\mathbb{h}(\mathbf{y}_k | \mathbf{s}_k) = \mathbb{h}(\mathbf{n}_k) = \frac{1}{2} \log_2(\det(2\pi \exp(1) \boldsymbol{\Sigma}_k)) \quad (3.80)$$

$$= \frac{N_r}{2} \log_2(2\pi \exp(1) \sigma_k^2) \quad (3.81)$$

$$\mathbb{h}(\mathbf{y}_e^{(k)} | \mathbf{s}_k) = \mathbb{h}(\mathbf{J}_k + \mathbf{n}_e) = \frac{1}{2} \log_2(\det(2\pi \exp(1) \boldsymbol{\Sigma}_e^k)) \quad (3.82)$$

$$= \frac{N_r}{2} \log_2 \left((2\pi \exp(1))^{N_r} \sqrt{\det(\boldsymbol{\Sigma}_e^k)} \right), \quad (3.83)$$

şeklinde hesaplanır. Burada, $\boldsymbol{\Sigma}_k$ k 'inci kullanıcının AWGN kovaryans matrisini, $\boldsymbol{\Sigma}_e^k$ ifadesi de k 'inci kullanıcıyı izinsiz dinleyen Eve'deki jamming ve AWGN terimlerinin toplamının kovaryans matrisini göstermektedir. AWGN ve önkodlama kaynaklı jamming vektörleri birbirlerinden bağımsız oldukları için

$$\boldsymbol{\Sigma}_k = \sigma_k^2 \mathbf{I}_{N_r}, \quad (3.84)$$

$$\boldsymbol{\Sigma}_e^k = \mathbb{E}[\mathbf{J}_k \mathbf{J}_k^T] + \sigma_e^2 \mathbf{I}_{N_r} \quad (3.85)$$

şeklinde bulunur. Bu yüzden, k 'inci kullanıcının gizlilik oranı aşağı verilen formülasyon göre bulunur:

$$\mathbb{h}_{lb}(\mathbf{y}_k) = \log_2(MN_r) + \frac{N_r}{2} \log_2(4\pi\sigma_k^2) - \log_2 \left(1 + \frac{1}{MN_r} \sum_{i=1}^{MN_r} \sum_{\substack{j=1 \\ j \neq i}}^{MN_r} \exp \left(\frac{-\rho_k^2 |\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)}|^2}{4\sigma_k^2} \right) \right), \quad (3.86)$$

$$\begin{aligned} \mathbb{h}_{lb}(\mathbf{y}_e^k) &= \log_2(MN_r) + \frac{N_r}{2} \log_2 \left(4\pi \sqrt[{}^{N_r}]{\det(\boldsymbol{\Sigma}_e^{(k)})} \right) - \\ &\quad - \log_2 \left(1 + \frac{1}{MN_r} \sum_{i=1}^{MN_r} \sum_{\substack{j=1 \\ j \neq i}}^{MN_r} \exp \left(\frac{-\rho_k^2 (\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)})^T (\boldsymbol{\Sigma}_e^{(k)})^{-1} (\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)})}{2} \right) \right), \end{aligned}$$

$$\begin{aligned} \mathbb{C}_{s,ub}^{(k)} &= \frac{N_r}{2} \log_2 \left(\frac{\exp(1)(\rho_k^2 + \sigma_k^2)}{2\sigma_k^2 \sqrt[{}^{N_r}]{M^2 N_r^2}} \right) + \\ &\quad + \log_2 \left(1 + \frac{1}{MN_r} \sum_{i=1}^{MN_r} \sum_{\substack{j=1 \\ j \neq i}}^{MN_r} \exp \left(\frac{\rho_k^2 (\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)})^T (\boldsymbol{\Sigma}_e^{(k)})^{-1} (\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)})}{2} \right) \right), \quad (3.87) \end{aligned}$$

$$\begin{aligned} \mathbb{C}_{s,lb}^{(k)} &= \frac{N_r}{2} \log_2 \left(\frac{2}{\exp(1)} \sqrt[{}^{N_r}]{\frac{M^2 N_r^2 \det(\boldsymbol{\Sigma}_e^{(k)})}{\det(\rho_k^2 \mathbf{I}_{N_r} + \boldsymbol{\Sigma}_e^{(k)})}} \right) - \\ &\quad - \log_2 \left(1 + \frac{1}{MN_r} \sum_{i=1}^{MN_r} \sum_{\substack{j=1 \\ j \neq i}}^{MN_r} \exp \left(\frac{-\rho_k^2 |\mathbf{s}_k^{(i)} - \mathbf{s}_k^{(j)}|^2}{4\sigma_k^2} \right) \right). \quad (3.88) \end{aligned}$$

$$\mathbb{C}_s^{(k)} = \frac{N_r}{2} \log_2 \left(\frac{\sqrt[{}^{N_r}]{\det(\boldsymbol{\Sigma}_e^{(k)})}}{\sigma_k^2} \right) + \mathbb{h}(\mathbf{y}_k) - \mathbb{h}(\mathbf{y}_e^{(k)}) \quad (3.89)$$

$\mathbb{C}_s^{(k)}$ ifadesinin üst ve alt limitleri, $\mathbb{h}(\mathbf{y}_k)$ ve $\mathbb{h}(\mathbf{y}_e^{(k)})$ entropileriyle ilişkili limitler kullanılarak

$$\mathbb{C}_{s,lb}^{(k)} \leq \mathbb{C}_s^{(k)} \leq \mathbb{C}_{s,ub}^{(k)}, \quad (3.90)$$

$$\mathbb{C}_{s,ub}^{(k)} = \frac{N_r}{2} \log_2 \left(\frac{\sqrt{N_r} \sqrt{\det(\boldsymbol{\Sigma}_e^k)}}{\sigma_k^2} \right) + \mathbb{h}_{ub}(\mathbf{y}_k) - \mathbb{h}_{lb}(\mathbf{y}_e^{(k)}), \quad (3.91)$$

$$\mathbb{C}_{s,lb}^{(k)} = \frac{N_r}{2} \log_2 \left(\frac{\sqrt{N_r} \sqrt{\det(\boldsymbol{\Sigma}_e^k)}}{\sigma_k^2} \right) + \mathbb{h}_{lb}(\mathbf{y}_k) - \mathbb{h}_{ub}(\mathbf{y}_e^{(k)}). \quad (3.92)$$

olarak bulunur. Eve'de alınan \mathbf{y}_k ve $\mathbf{y}_e^{(k)}$ sinyalleri, farklı Gauss dağılımlarının toplamıdır (karışımli Gauss rassal değişkenleri). Herhangi bir rassal değişkenin entropisi, aynı kovaryanslı Gauss rassal değişkeninin entropisini aşamayacağından, $\mathbb{h}(\mathbf{y}_k)$ ve $\mathbb{h}(\mathbf{y}_e^{(k)})$ entropilerine ait üst limitler,

$$\mathbb{h}(\mathbf{y}_k) \leq \mathbb{h}(\mathbf{N}_k), \quad (3.93)$$

$$\mathbb{h}(\mathbf{y}_e^{(k)}) \leq \mathbb{h}(\mathbf{N}_e^{(k)}) \quad (3.94)$$

şeklinde bulunur. Burada \mathbf{N}_k ve $\mathbf{N}_e^{(k)}$, sırayla $N(\mathbf{0}, \mathbb{E}[\mathbf{y}_k \mathbf{y}_k^T])$ ve $N(\mathbf{0}, \mathbb{E}[(\mathbf{y}_e^{(k)})(\mathbf{y}_e^{(k)})^T])$ çoklu Gauss rassal değişkenleridir. İlgili kovaryans matrisleri,

$$\mathbb{E}[\mathbf{y}_k \mathbf{y}_k^T] = \rho_k^2 \mathbb{E}[\mathbf{s}_k \mathbf{s}_k^T] + \sigma_k^2 \mathbf{I}_{N_r} = (\rho_k^2 + \sigma_k^2) \mathbf{I}_{N_r} \quad (3.95)$$

$$= \rho_k^2 \mathbf{I}_{N_r} + \boldsymbol{\Sigma}_k, \quad (3.96)$$

$$\mathbb{E}[(\mathbf{y}_e^{(k)})(\mathbf{y}_e^{(k)})^T] = \rho_k^2 \mathbb{E}[\mathbf{s}_k \mathbf{s}_k^T] + \mathbb{E}[\mathbf{J}_k \mathbf{J}_k^T] + \sigma_k^2 \mathbf{I}_{N_r} \quad (3.97)$$

$$= \rho_k^2 \mathbf{I}_{N_r} + \boldsymbol{\Sigma}_e^k \quad (3.98)$$

olarak hesaplanır. Bu ifadeler kullanarak, entropi üst limitleri,

$$\mathbb{h}_{ub}(\mathbf{y}_k) = \mathbb{h}(\mathbf{N}_k) \quad (3.99)$$

$$= \frac{N_r}{2} \log_2 (2\pi \exp(1)(\rho_k^2 + \sigma_k^2)), \quad (3.100)$$

$$\mathbb{h}_{ub}(\mathbf{y}_e^{(k)}) = \mathbb{h}(\mathbf{N}_e^{(k)}) \quad (3.101)$$

$$= \frac{N_r}{2} \log_2 \left(2\pi \exp(1) \sqrt{N_r} \sqrt{\det(\rho_k^2 \mathbf{I}_{N_r} + \boldsymbol{\Sigma}_e^k)} \right) \quad (3.102)$$

olarak bulunur.

İçbükey olan entropi fonksiyonunun alt limitleri, Jensen eşitsizliğini kullanarak,

$$\mathbb{h}(\mathbf{y}_k) = \mathbb{E} [-\log_2(f(\mathbf{y}_k))] \geq -\log_2(\mathbb{E}[f(\mathbf{y}_k)]) \quad (3.103)$$

$$= -\log_2 \int f^2(\mathbf{y}_k) d\mathbf{y}_k = \mathbb{h}_{lb}(\mathbf{y}_k). \quad (3.104)$$

şeklinde bulunur. Bu nedenle, entropi alt limitleri, olasılık dağılım fonksiyonlarının (probability distribution function (pdf)) karesinin integralini hesaplayarak bulunabilir. Yasal kullanıcılarda ve Eve'de alınmış olan sinyaller,

$$f(\mathbf{y}_k) = \sum_{i=1}^{MN_r} f(\mathbf{y}_k|I=i)Pr(I=i) \quad (3.105)$$

$$= \frac{1}{MN_r} \sum_{i=1}^{MN_r} (2\pi\sigma_k^2)^{-N_r/2} \exp\left(-\frac{|\mathbf{y}_k - \rho_k \mathbf{s}_k^{(i)}|^2}{2\sigma_k^2}\right) \quad (3.106)$$

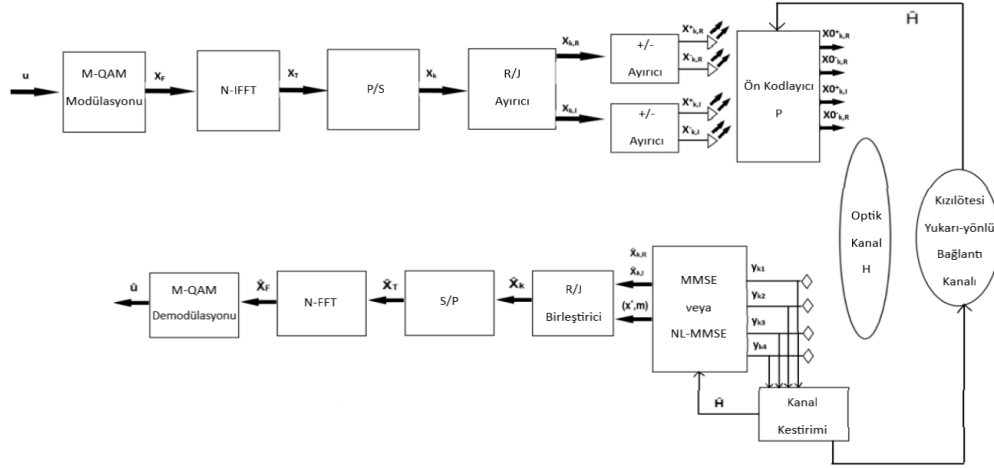
pdf'leriyle verilen karışımli Gauss rassal deęişkenleridir. Bu pdf'leri (3.103) denkleminde yerine koyup integralleri çözürek (3.86) denkleminde verilen entropi alt limitleri bulunur. Bulunan entropi üst ve alt limitleri (3.90) ifadesinde yerine konarak (3.87) ifadesinde verilen gizlilik oranı limitleri bulunur.

3.3. Genelleştirilmiş LED İndeks Modülasyonu ile Optik MIMO-OFDM (GLIM-OFDM) için Fiziksel Katman Güvenliği

3.3.1. Optik GLIM OFDM Mimarisi

Geçen dönem görünür ışıkla haberleşme (VLC) için geliştirilen GLIM-OFDM sistemi için bir takım hesaplama karmaşıklığı düşük ve hızlı kanal kestirim algoritmalar geliştirilmiştir. Bu sistem üzerinde yapılan bilgisayar benzetimleri, önerilen kanal kestirim algoritmasının gerek ortalama kestirim hatası ve gerekse kestirim hatalarının sistem bit hata olasılığına etkileri yönünden çok başarılı sonuçlar verdiği görülmüştür. Bu iş paketiyle ilgili son dönemdeki gelişmeler ise geçen dönemde yapılan çalışmaların bir devamı niteliğinde olup iç mekan (VLC) GLIM-OFDM sistemleri için yeni ve özgün bir fiziksel güvenlik tekniği geliştirilmiştir. Teknik, sistemin verici-alıcı (Alice-Bob) arasındaki optik kanal matrisinin kaynak tarafından bilinmesi varsayımı altında tasarlanan bir önkodlayıcıya (precoder) dayanmaktadır. Bu nedenle geçen dönem geliştirilen kanal kestirim algoritması, GLIM-OFDM PLS tekniğinde potansiyel bir uygulama alanı bulacaktır.

Fiziksel katman güvenliğine sahip bir GLIM OFDM optik kablosuz iletişim sisteminin alıcı ve vericisinin blok şeması Şekil 1'de verilmiştir. Bu şekilde u vektörü tarafından taşınan $N \log_2(M)$ bilgi bitleri, her OFDM bloğunun iletimi için GLIM-OFDM vericisinden iletilmektedir. Burada N , OFDM alt taşıyıcılarının sayısını, M 'de M -ary karesel genlik modülasyonlu (M-QAM) sinyal kümesinin boyutunu göstermektedir. DCO-OFDM, ACO-OFDM ve DC öngerilimi olmayan OFDM (NDC-OFDM) yapıları, ters Fourier dönüşüm (IFFT) işleminden sonra gerçek zamanlı sinyal örneklerini üretmek için Hermisyen simetrisini kullanmaktadır. Önerilen yapıda ise, OFDM modülatörü, Hermisyen simetrisi gerektirmeden x_F karmaşık- değerli zaman- bölge-sinde OFDM çerçevesini doğrudan işler. Ortaya çıkan zaman bölgesi OFDM çerçevesi, $x_T = [x_1, x_2, \dots, x_N]^T$, karmaşık değerli ve iki kutuplu (pozitif ve negatif değerli) olması nedeniyle optik bir kanal aracılığıyla iletilemez. Bu sorunu çözmek için LED indeks modülasyonu tabanlı yeni bir MIMO iletişim tekniği geliştirilmiştir. Paralelden seriye (P/S) dönüştürmeden sonra, [75]'dekine benzer bir teknik kullanılarak, OFDM zaman-bölgesi sinyal örnekleri, x_k , $k = 0, 1, \dots, N - 1$, ilk olarak, $x_k = x_{k,R} + jx_{k,I}$ k gerçel ve sanal kısımlarına ayrılmaktadır. Ardından, elde edilen gerçel, ancak iki kutuplu $x_{k,R}$ ve $x_{k,I}$ sinyaller, aşağıdaki gibi, pozitif ve gerçel değerli sinyalleri elde etmek için



Şekil 3.5. Bir fiziksel katman güvenli ve kanal kestimli VLC GLIM-OFDM sistemin verici ve alıcı blokları

pozitif-negatif (+/-) ayırıcılar tarafından işlenir:

$$\begin{aligned}
 x_{k,R}^+ &= \begin{cases} x_{k,R}, & \text{if } x_{k,R} > 0 \\ 0, & \text{if } x_{k,R} < 0 \end{cases} & x_{k,R}^- &= \begin{cases} 0, & \text{if } x_{k,R} > 0 \\ -x_{k,R}, & \text{if } x_{k,R} < 0 \end{cases} \\
 x_{k,I}^+ &= \begin{cases} x_{k,I}, & \text{if } x_{k,I} > 0 \\ 0, & \text{if } x_{k,I} < 0 \end{cases} & x_{k,I}^- &= \begin{cases} 0, & \text{if } x_{k,I} > 0 \\ -x_{k,I}, & \text{if } x_{k,I} < 0 \end{cases}
 \end{aligned} \tag{3.107}$$

Daha sonra, pozitif ve gerçekteğerli OFDM zaman-bölgesi örnekleri, aşağıdaki gibi, $x_{k,R}^+$, $x_{k,R}^-$, $x_{k,I}^+$ ve $x_{k,I}^-$ ile temsil edilen, bir 4×4 MIMO VLC kanalı üzerinden eş zamanlı olarak iletilirler:

$$\mathbf{H} = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} & h_{1,4} \\ h_{2,1} & h_{2,2} & h_{2,3} & h_{2,4} \\ h_{3,1} & h_{3,2} & h_{3,3} & h_{3,4} \\ h_{4,1} & h_{4,2} & h_{4,3} & h_{4,4} \end{bmatrix} \in \mathcal{R}^{4 \times 4}, \tag{3.108}$$

burada $h_{r,t}$ kablosuz optik linkin vericisi (TX) (t) ile alıcısı (RX) (r) arasındaki kanal kazancını göstermektedir. Bu çalışmada $n_T = 4$ olarak alındığı varsayılan yapı için n_T 'in dörde bölünebil-

mesi gerektiğine dikkat edilmelidir. Gerçek iç mekan VLC sistemlerinde, bilinen geometri ve bazı eğimlerle tavana yerleştirilmiş bir dizi LED'ler verildiğinde, Zemax'ın ışın izleme yöntemiyle, LED'lerin her biri ile zemin üzerindeki her nokta arasındaki kanal kazançları (katsayıları) ya bir optik ve aydınlatma yazılımı olan © ile yada aşağıdaki formüle göre belirlenir.

$$h_i = \frac{(m+1)A_{PD}}{2\pi D_i^2} \cos^m(\phi_i) \cos(\theta_i) \text{rect}\left(\frac{\theta_i}{\text{FoV}_{PD}}\right), \quad (3.109)$$

burada ϕ_i ve θ_i açıları, sırasıyla alıcıda konumlanan photo-detector (PD) ile i^{th} verici LED arasındaki geliş açısını ve varış açısını temsil etmektedir. Ayrıca, alıcıdaki PD ile i^{th} iletim LED'i arasındaki mesafe D_i ile gösterilmekte, $m = -1/\log_2(\cos(\Phi_{1/2}))$ parametresi, ışık kaynağının Lambert emisyon düzeyini tanımlamaktadır. Bu formülde $\Phi_{1/2}$ vericinin gücünün yarıya düştüğü açıyı, LED. FoV_{PD} ve A_{PD} , sırasıyla görüş alanının (FoV) yarı açısını ve görüntüleme dışı PD'nin etki alanını gösterir.

GLIM-OFDM iletişim tekniğinde, LED'ler $x_{k,R}$ ve $x_{k,I}$ sinyallerinin mutlak değerlerini iletmekte ve ileten LED'in indeksi, NDC-OFDM'e karşılık gelen sinyallerin işaretini belirlemektedir. Bununla birlikte, NDC-OFDM'den farklı olarak, GLIM-OFDM, IFFT girişindeki Hermisyen simetrisini göz önüne almadan spektral verimlilikteki kaybı tamamen önler. Dolayısıyla Hermisyen simetrisine artık gerek olmaması nedeniyle, önerilen yapının spektral verimliliği $\log_2(M)$ [bit/s/Hz] olup, bu NDC-OFDM ve DCO-OFDM tekniklerinde erişilenlerin iki katıdır, ve zaman-bölgesinde optik iletişime uygun gerçek-değerli OFDM sembolleri üretilir. Bu çalışmada, sunum kolaylığı için $n_R = 4$ alınmakta ve, LED'lerin kendi dinamik aralıklarında çalıştığı varsayılmaktadır. Sonuç olarak, (1)'deki işlem doğrusal olmayan bozulmalardan etkilenmeyecektir.

3.3.2. GLIM OFDM'de Vericide Önkodlayıcı Destekli PLS

Vericideki yasal kullanıcının (Bob) kanal durum bilgisi (CSIT) yardımıyla, Bob'un bit hata başarıımı (BER), kaynak ve Bob arasında sağlanan ortak-kanal-girişiminden (co-channel interference) etkilenmeyen bir iletişimle enaza indirilir. Öte yandan, yasal olmayan kullanıcının (Eve) BER'i ise önemli ölçüde bozulur. Yukarıdaki amaca ulaşmak için, \mathbf{P} ön kodlama matrisi yardımıyla alıcı PD'ler arasında hiçbir enerji sızıntısının olmaması sağlanmalıdır. Bu amaçla, sıfır zorlamalı (ZF) ön kodlama veya minimum ortalama karesel hatalı (MMSE) ön kodlama tekniği kullanılabilir. Bu çalışmada, \mathbf{P} ön kodlama matrisinin Bob'un \mathbf{H}_B kanalının sözde tersinden (pseudo-inverse) oluşan sıfıra zorlayıcı (ZF) türden bir ön kodlama tekniği

benimsenmiştir.

$$\mathbf{P} = \beta (\mathbf{H}_B^T \mathbf{H}_B)^{-1} \mathbf{H}_B^T \quad (3.110)$$

burada $\beta = \sqrt{N_r / \text{trace}(\mathbf{P}^T \mathbf{P})}$ bir güç normalizasyon katsayısıdır. İletim öncesinde $\mathbf{x} = [x_{k,R}^+, x_{k,R}^-, x_{k,I}^+, x_{k,I}^-]^T \in \mathbb{R}^{n_R \times 1}$, kaynak sinyalini işleyerek alıcı PD'ler arasındaki ortak kanal girişimini tamamen ortadan kaldırabilir. Sonuç olarak, kanal parametrelerinden bağımsız olarak, yasal kullanıcının (Bob) alıcısında \mathbf{x} 'in düşük hesaplama karmaşıklığıyla kestiriminin gerçekleşmesi mümkün olur. Ancak, kaynak ve Eve arasındaki \mathbf{H}_E kanalı Bob'un kanalından farklı olduğundan, ön-kodlanmış kaynak sinyali Eve tarafından, tamamen bir gürültü (Jamming) sinyali olarak algılanacaktır. Önkodlama işleminden sonra, zaman-bölgesinde üretilen pozitif ve gerçek değerli OFDM örnek vektörleri \mathbf{x} aktif LED'lerden iletilen bir optik sinyale \mathbf{u} dönüştürülür ve şu şekilde yazılabilir:

$$\mathbf{u} = \mathbf{P}\mathbf{x}. \quad (3.111)$$

burada LED'ler tarafından yayılan sinyaller \mathbf{u} 'nun bileşenleri olarak gösterilir. (1)'e göre, belirli bir OFDM sinyali için dört bilşenden sadece ikisi sıfırdan farklıdır, yani iki LED devre dışı kalmaktadır (kapalı). Bu şekilde önerilen iletişim yapısı, karmaşık OFDM sinyallerini iletmek için aktif LED indeksleri için indeks modülasyon konseptini kullanmaktadır.

3.3.3. Vericide Güç Normalizasyonu

\mathbf{u} , u_k 'in (3.111), her bir LED'e ulaşan sinyal bileşenleri, $[-u_{\max}, u_{\max}]$, önemli güç dalgalanmaları ve geniş bir dinamik aralığında değer alabilen gerçek değerli değişkenlerdir. Bu nedenle LED'ler üzerinden iletim yapılmadan önce hem sinyal genliklerinin pozitifliği hem de vericideki güçlerin normalizasyonu sağlanmalıdır. Bununla birlikte, her kanal durumu için, normleştirilmiş sinyal, \bar{u}_k , $k = 1, 2, \dots, n_T$ ($n_T = 4$)'a güç vererek her bir LED'i çalıştırırken şöyle bir kısıtlamaya tabidir; $|\bar{u}_k - u_{dc}| \leq \alpha u_{dc}$, burada u_{dc} dc(doğru akım) öngerilimi ve $\alpha \in [0, 1]$, doğrusallık LED çalışma aralığı $[(1-\alpha), (1+\alpha)]$ boyunca korunacak şekilde seçilen bir sabittir. Sonuç olarak, k . LED'i süren tepe genliği kısıtlı sinyal şu şekilde belirlenir:

$$\bar{u}_k = a u_k + b, \quad (3.112)$$

burada $a = \alpha u_{dc} / u_{\max}$ ve $b = u_{dc}$. u_{\max} terimleri Bob'un hem verici hem de alıcı biriminde aşağıdaki gibi hesaplanabilir. Bob'un kanal durum bilgisi (CSI) $\mathbf{H}_B \in \mathcal{R}^{N_r \times N_t}$ Bob'un verici ve alıcısı tarafından tamamen bilindiğinden, belirli bir kullanıcı konumunda her LED kombi-

nasyonu için \mathbf{u} normu şu şekilde üstten sınırlanabilir (3.111):

$$\begin{aligned} |\mathbf{u}| &= |\mathbf{P}\mathbf{x}| \\ &\preceq |\mathbf{P}| \mathbf{x} \\ &\preceq \rho_{\max} \det(\mathbf{P}) \mathbf{1}_{N_r} \equiv u_{\max} \mathbf{1}_{N_r} \end{aligned} \quad (3.113)$$

burada, \preceq sembolü, iki vektör arasındaki bileşen bazında eşitsizliği ve bir matris etrafındaki $|\cdot|$, ise bileşen bazında mutlak değeri gösterir ve $\rho_{\max} \triangleq \rho \sqrt{E\{x_{\max}^2\}}$. Burada, ρ bir sabit olup verilen bir dB düzeyi için, şu şekilde belirlenir: $\text{dB} = 10 \log(1+\rho^2)$. $x_{\max} \triangleq \max\{\bar{x}_{k,R}, \bar{x}_{k,I}\}$, burada $\bar{x}_{k,R} = |x_{k,R}|$ and $\bar{x}_{k,I} = |x_{k,I}|$ dir. $\bar{x}_{k,R}$ ve $\bar{x}_{k,I}$ 'un katlanmış Gauss (folded Gaussain) olasılık dağılımına (pdf) sahip olduğu kolaylıkla gösterilebilir.

$$p_{\bar{x}_{k,R(I)}}(v) = \frac{2}{\sqrt{\pi}} e^{-v^2}, \quad v \geq 0. \quad (3.114)$$

x_{\max} 'in pdf'nin $p_{x_{\max}}(v) = 2\sqrt{2/\pi} \text{erf}(v/\sqrt{2}) \exp(-v^2/2)$ olduğu kolaylıkla gösterilebilir ve $E\{x_{\max}^2\} = (0/5 - \frac{1}{\pi}) = 0.8183$.

Son olarak, Bob (B) ve Eve'in (E) N_r sayıdaki PD'lerinde gözlemlenen sinyal, ilgili kanalları aracılığıyla iletdikten sonra şu şekilde ifade edilebilir:

$$\mathbf{y}_B = \mathbf{s}_B + b\mathbf{H}_B\mathbf{1}_{N_t} + \mathbf{n}_B \quad (3.115)$$

$$\mathbf{y}_E = \mathbf{s}_E + b\mathbf{H}_E\mathbf{1}_{N_t} + \mathbf{n}_E \quad (3.116)$$

where,

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

ve $\mathbf{y}_B, \mathbf{y}_E \in \mathbb{R}^{n_R \times 1}$, alıcıya ulaşan elektriksel sinyal vektörleridir. Ayrıca, (3.115,3.116)'daki $\mathbf{n}_B, \mathbf{n}_E \in \mathbb{R}^{n_R \times 1}$ 'da sırasıyla Bob'un ve Eve'in kanallarındaki impuls gürültüsünü ve ısı gürültüyü σ_B^2, σ_E^2 modelleyen gerçek değerli toplamsal beyaz Gauss gürültüsü (AWGN) örneklerinin vektörleridir. Kaynak ve Bob arasındaki dc-öngerilimi, u_{dc} ve kanal matrisi, \mathbf{H}_B bilindiğinden, u_{dc} , sezme (detection) işleminden önce bastırılabilir. Sonuç olarak, alınan

sinyaller (3.115) ve (3.116) şu şekilde yeniden ifade edilebilir:

$$\mathbf{y}_B = \beta \mathbf{x} + \mathbf{n}_B, \quad (3.117)$$

$$\mathbf{y}_E = \beta \mathbf{G} \mathbf{x} + \mathbf{n}_E, \quad (3.118)$$

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

3.3.4. Koşullu Minimum Karesel Ortalama (Bayes) Kestirimi

(3.117) ve (3.118)'de formüle edilen kestirim problemine basit bir çözüm, bir sıfır zorlamalı (ZF) kestirimci kullanarak \mathbf{x} 'in kestirilmişini elde etmektir.

$$\hat{\mathbf{z}}_{ZF} = \begin{cases} \frac{1}{\beta} \mathbf{y}_B, & \text{for BOB's transmisson} \\ \frac{1}{\beta} \mathbf{G}^{-1} \mathbf{y}_E & \text{for EVE's transmisson.} \end{cases} \quad (3.119)$$

Bu işlemden sonra, alıcı aktif LED'lerin indekslerini ve bunlara karşılık gelen sinyal örneklerinden genliği en büyük olanını $\hat{\mathbf{x}}$ 'dan seçerek ZF [11] algoritmasıyla belirler. Basitliğine rağmen, ZF kestirimcisi, \mathbf{n} ile \mathbf{H}^{-1} çarparak sistemi etkileyen Gauss gürültüsünün önemli ölçüde güçlenmesine neden olur. Ayrıca, \mathbf{x} 'in olasılık dağılımının ön bilgi kullanma yeteneği yoktur ve sonuçta negatif değerli kestirimler de üretebilir.

Yukarıda belirtilen ZF kestirimcisiyle ilgili sakıncaların üstesinden gelmek için, bu bölümde, \mathbf{x} sinyal vektörü için sahip olduğumuz ön-bilgileri (a priori) de göz önüne alan Bayes ortamında yeni bir minimum ortalama kare kestirimcisi (MMSE) önerilmektedir. Genel olarak MMSE kestiriminin ayrıntıları aşağıdaki gibi sunulabilir: Vericideki ön kodlayıcı yardımıyla, Bob'un alıcısında N_r ($N_r = 4$) paralel OFDM zaman-örnekleri tam bir şekilde ayrıştırılabildiğinden, alıcıda bu örneklerin düşük karmaşıklıkta tek boyuta indirgenmiş kestirimlerinde büyük kolaylık sağlanmış olur. Bu nedenle, $i_1 \in \{1, 2\}$ ve $i_2 \in \{3, 4\}$, aktif LED'lerin indislerin bilinmesi koşulu altında, (11) aşağıdaki biçime dönüşür:

$$y_B(i_1) = \beta \bar{x}_{k,R} + n_B(i_1), \quad i_1 \in \{1, 2\} \quad (3.120)$$

$$y_B(i_2) = \beta \bar{x}_{k,I} + n_B(i_2), \quad i_2 \in \{3, 4\} \quad (3.121)$$

$$y_B(j) = n_B(j), \quad j \in \{1, 2, 3, 4\} \text{ and } j \neq \{i_1, i_2\}, \quad (3.122)$$

olup, $y_B(j)$ ve $n_B(j)$ sırasıyla \mathbf{y}_B ve \mathbf{n}_B 'nin, j , ($j = 1, 2, 3, 4$)th bileşenleridir. Sonuç olarak, verilen belirli bir çift LED indisleri için (i_1, i_2) , ($i_1 \in 1, 2$ ve $i_2 \in 3, 4$), $\bar{x}_{k,R}$ ve $\bar{x}_{k,I}$ 'nin koşullu

MMSE kestirimi şu şekilde elde edilir:

$$\hat{x}_{\text{MMSE}} = E\{x|y\}, \quad (3.123)$$

Bundan sonraki derivasyonlarda kullanılan notasyonda bir kolaylık sağlamak için şu tanımlar kullanılacaktır: $x \triangleq \hat{x}_{k,R(I)}^{(i_1, (i_2))}$, $y \triangleq y_B(m)$ ve $\hat{x}_{\text{MMSE}} \triangleq \hat{x}_{k,R(I)}^{(i_1, (i_1))}$. (3.120) ve (3.121) de verilen gözlem denklemleri de bu basitleştirilmiş notasyonlarla aşağıdaki gibi ifade edilebilir.

$$y = z + n \quad (3.124)$$

ve $z = \beta x$ dir. Bu durumda \hat{x} 'in MMSE kestirimi (3.124) dekleminde şu şekilde elde edilir.

$$\begin{aligned} \hat{x}_{\text{MMSE}} &= E\{x|y\} = \int_{-\infty}^{+\infty} v p_{x|y}(v, y) dv \\ &= \frac{1}{p_y(y)} \int_{-\infty}^{+\infty} v p_{y|x}(v, y) p_x(v) dv, \end{aligned} \quad (3.125)$$

olup, $p_x(v)$ ve $p_y(y)$ sırasıyla x ve y 'in pdf'i ve $p_{y|x}(v, y)$, verilen x için y 'in koşullu pdf'dir. Ayrıca, x 'in pdf'i katlanmış Gauss olasılık dağılımına sahip olup, pdf'i (3.114) ile verilir. Dolayısıyla $p_z(v)$ şu şekilde ifade edilebilir:

$$p_z(v) = \frac{1}{\sqrt{\pi\beta^2}} e^{-v^2/\beta^2}, \text{ for } t \geq 0. \quad (3.126)$$

n 'nin pdf'i şu şekilde ifade edilebilir:

$$p_n(n) = \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-n^2/2\sigma_n^2}, \quad (3.127)$$

burada σ_n^2 gürültünün varyansıdır. x 'in n 'dan bağımsız olduğunu varsaydığımız için, y iki bağımsız raslantısal değişkenin toplamıdır ve pdf'i şu şekilde hesaplanır:

$$p_y(y) = \int_{-\infty}^{+\infty} p_z(\alpha) p_{y|z}(y | \alpha) d\alpha \quad (3.128)$$

$$p_z(\alpha) = \frac{2}{\pi\beta} e^{-\frac{\alpha^2}{\beta}}, \alpha \geq 0 \quad (3.129)$$

$$p_{y|z}(y | \alpha) = p_n(y - \alpha) = \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{1}{2\sigma_n^2}(y-\alpha)^2} \quad (3.130)$$

(3.130) ve (3.129)'u (3.128)'de yerine konduğunda aşağıdaki ilişki elde edilir:

$$p_y(y) = \int_0^{+\infty} \left(e^{-\frac{\alpha^2}{\beta}} e^{-\frac{1}{2\sigma_n^2}(y-\alpha)^2} d\alpha \right) \frac{1}{\sqrt{2\pi\sigma_m^2}} \frac{2}{\sqrt{\pi\beta^2}}. \quad (3.131)$$

Bu integralde parantez içindeki ifade için aşağıdaki cebirsel işlemler yapılırsa,

$$\begin{aligned} \frac{\alpha^2}{\beta^2} + \frac{(y-\alpha)^2}{2\sigma_n^2} &= \frac{2\sigma_n^2\alpha^2 + \beta^2(y-\alpha)^2}{2\beta^2\sigma_n^2} \\ &= \frac{2\sigma_n^2\alpha^2 + \beta^2(y^2 - 2y\alpha + \alpha^2)}{2\beta^2\sigma_n^2} \\ &= \frac{\alpha^2(\beta^2 + 2\sigma_n^2) - 2\alpha y\beta^2 + \beta^2 y^2}{2\beta^2\sigma_n^2} \\ &= \frac{(\beta^2 + 2\sigma_n^2) \left(\alpha^2 - 2\alpha \frac{y\beta^2}{\beta^2 + 2\sigma_n^2} + \frac{\beta^2 y^2}{\beta^2 + 2\sigma_n^2} \right)}{2\beta^2\sigma_n^2} \\ &= \frac{\alpha^2 - 2\alpha \frac{y\beta^2}{\beta^2 + 2\sigma_n^2} + \frac{\beta^2 y^2}{\beta^2 + 2\sigma_n^2}}{\frac{2\beta^2\sigma_n^2}{\beta^2 + 2\sigma_n^2}} \\ &= \frac{\alpha^2 * 2\alpha y P + P y^2}{2P\sigma_n^2} \end{aligned}$$

elde edilir. Burada, $P = \beta^2/(\beta^2 + 2\sigma_n^2)$ dir. Bu eşitliğe $y^2 P$ ekleyip çıkarılıp çözümlendiğinde aşağıdaki ilişki elde edilir:

$$= \frac{(\alpha - yp)^2 + P y^2 (1 - P)}{2P\sigma_n^2}.$$

Bunu kullanarak ve $s^2 = P\sigma_n^2$ alarak, (3.31)'deki integral kolayca aşağıdaki gibi alınabilir.

$$p_y(y) = \frac{2}{\sqrt{\pi\beta^2}} \frac{1}{\sqrt{2\pi\sigma_n^2}} \sqrt{2\pi s^2} \left(1 - Q\left(\frac{yP}{s}\right) \right) e^{-\frac{y^2(1-p)}{2\sigma_n^2}}. \quad (3.132)$$

Daha sonra, $s^2 = P\sigma_n^2$ ve $P = \beta^2/(\beta^2 + 2\sigma_n^2)$ değerleri (3.132) de yerine konarak $p_y(y)$ analitik olarak aşağıdaki gibi bulunur.

$$p_y(y) = \frac{2}{\sqrt{\pi(2\sigma^2 + \beta^2)}} \left(1 - Q\left(\frac{\beta y}{\sigma\sqrt{2\sigma^2 + \beta^2}}\right) \right) e^{-\frac{y^2}{2\sigma_n^2 + \beta^2}}. \quad (3.133)$$

Burada, $Q(x) = \frac{1}{\sqrt{\pi\sigma_n^2}} \int_x^{+\infty} e^{-t^2/2} dt$ dir. (3.124) ve (3.127) denklemlerinden kolayca aşağıdaki

ilişki elde edilebilir.

$$p_{y|x}(v, y) = p_n(y - \beta v) = \frac{1}{\sqrt{\pi\sigma_n^2}} e^{-(y-\beta v)^2/2\sigma_n^2}. \quad (3.134)$$

Son olarak, (3.129), (3.132) ve (3.131) denklemleri (3.125)'de yerine konarak ve bir takım cebirsel işlemlerden sonra, verilen y için x 'in MMSE kestirimi aşağıdaki gibi kapalı bir biçimde ifade edilebilir

$$\hat{x}_{\text{MMSE}} = \frac{\sigma_n}{\sqrt{2\pi(\beta^2 + 2\sigma_n^2)}} \frac{e^{-\beta^2 y^2 (2\sigma_n^2 (\beta^2 + 2\sigma_n^2))}}{1 - Q(\beta y / (\sigma_n \sqrt{(\beta^2 + \sigma_n^2)}))} + \frac{\beta y}{\beta^2 + 2\sigma_n^2}. \quad (3.135)$$

Yukarıdaki ifade, MMSE kestirimcisinin $E\{x^2\} = 1/2$ sinyal gücüne, σ_n^2 gürültü gücüne ve β normalizasyon sabitine bağlı olduğunu gösterir. Eğer, sinyal-gürültü oranı (SNR) $SNR = \beta^2 E\{x^2\} / \sigma_n^2$ biçiminde tanımlanırsa, yüksek ve düşük SNR bölgelerindeki (3.135) \hat{x}_{MMSE} değerleri aşağıdaki gibi elde edebilir:

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

$(i_1, (i_2))$ 'nin bilinmesi durumunda, (3.135) $\bar{x}_{k,R}$ ve $\bar{x}_{k,I}$ için MMSE kestirimleri şu şekilde belirlenir:

$$\hat{x}_{k,R}^{(i_1)} = \left[\hat{x}_{\text{MMSE}}|_{y=y(i_1)} \right]^+, \quad \hat{x}_{k,I}^{(i_2)} = \left[\hat{x}_{\text{MMSE}}|_{y=y(i_2)} \right]^+ \quad (3.136)$$

burada $[x]^+ = \max\{0, x\}$ 'u simgelemektedir.

$\bar{x}_{k,R}$ 'in MMSE kestirimi bulunduktan sonra, tüm $(i_1, i_2) \in \{(1, 3), (1, 4), (2, 3), (2, 4)\}$ için aktif LED'lerin indeksleri aşağıdaki gibi seçilir.

$$\begin{aligned} \hat{i}_1 &= \arg \max_{i_1} |y_B(i_1) - \beta \hat{x}_{k,R}^{(i_1)}|^2 \\ \hat{i}_2 &= \arg \max_{i_2} |y_B(i_2) - \beta \hat{x}_{k,I}^{(i_2)}|^2. \end{aligned} \quad (3.137)$$

\mathcal{R}/\mathcal{I} birleştirici daha sonra karmaşık değerli zaman örnekleri $x_k, k = 0, 1, \dots, N - 1$ 'lerin kestirimlerini şu şekilde hesaplar:

$$\hat{x}_{k,R} = \begin{cases} \hat{x}_{k,R}^{(i_1)} & \text{if } \hat{i}_1 = 1 \\ -\hat{x}_{k,R}^{(i_2)} & \text{if } \hat{i}_1 = 2 \end{cases} \quad \hat{x}_{k,I} = \begin{cases} \hat{x}_{k,I}^{(i_3)} & \text{if } \hat{i}_2 = 3 \\ -\hat{x}_{k,I}^{(i_4)} & \text{if } \hat{i}_2 = 4 \end{cases} \quad (3.138)$$

Bu noktadan sonra, iletilen bilgiyi saptamak için seriden paralele (S/P) dönüştürme, FFT ve M -ary demodülasyonu gibi klasik OFDM işlem adımları uygulanır. Öte yandan, Eve'in alıcısındaki \bar{x} 'in optimal MMSE kestirimcisi için tam analitik ifadeler, Bob'un alıcısı için elde edilmiş olan MMSE kestirimine benzer şekilde (3.118)'deki gözlem denkleminin analitik olarak elde edilemez. Ancak (i_1, i_2) 'nin bilinmesi koşulu altında, y_E 'nin şu aşağıdaki gibi ifade edilebileceği unutulmamalıdır.

$$\mathbf{y}_E = \beta \mathbf{G}^{(i_1, i_2)} \bar{\mathbf{x}} + \mathbf{n}_E \quad (3.139)$$

burada $\mathbf{G}^{(i_1, i_2)} = [\mathbf{g}_{i_1}, \mathbf{g}_{i_2}] \in \mathcal{R}^{n_R \times 2}$; $k = 1, 2, 3, 4$, için, \mathbf{g}_k , \mathbf{G} 'nin k . satırını göstermektedir (3.118) ve $\bar{\mathbf{x}} = [\bar{x}_{k,R}, \bar{x}_{k,I}]^T$. Önceden gösterildiği gibi, $\bar{x}_{k,R}$ ve $\bar{x}_{k,I}$ katlanmış Gauss dağılımına sahiptir ve olasılık yoğunluk fonksiyonu (3.114) da verilmektedir. Sonuç olarak, $\hat{\bar{\mathbf{x}}}$ $\bar{\mathbf{x}}$ doğrusal bir MMSE kestirimi (LMMSE)), Bayes Gauss-Markov teoremiyle [76] kapalı formda aşağıdaki gibi bulunabilir.

$$\hat{\bar{\mathbf{x}}}^{(i_1, i_2)} = \mathbf{C}_{\bar{\mathbf{x}}} \mathcal{G}^T (\mathcal{G} \mathbf{C}_{\bar{\mathbf{x}}}^{-1} \mathcal{G}^T + \sigma_n^2 \mathbf{I}_{n_R})^{-1} (\mathbf{x} - \mathcal{G} \mu_{\bar{\mathbf{x}}}) + \mu_{\bar{\mathbf{x}}}, \quad (3.140)$$

burada $\mathcal{G} \triangleq \mathbf{G}^{(i_1, i_2)}$ olup $\bar{\mathbf{x}}$ vektörünün bileşenlerinin bağımsız katlanmış Gauss rastgele değişkenleri olduğundan, $\mu_{\bar{\mathbf{x}}} = E\{\bar{\mathbf{x}}\} = [1/\sqrt{\pi}, 1/\sqrt{\pi}]^T$, $\mathbf{C}_{\bar{\mathbf{x}}} = E\{\bar{\mathbf{x}}\bar{\mathbf{x}}^T\} = [1, 0; 0, 1]$ dir. Ayrıca, y_E ve $\bar{\mathbf{x}}$ ortak Gauss dağılımlı olmadıklarından, sonuçta ortaya çıkan LMMSE kestiriminin optimal olmayacağını görülür. Ancak bu kestirimin kapalı bir formda olması ve sadece ortalama ve kovaryansa bağlı olması gerçek uygulama alanlarında oldukça yararlı ve tercih edilen bir yöntemdir. Ayrıca, $\epsilon = \mathbf{x} - \bar{\mathbf{x}}$, LMMSE hata vektörünün kovaryans matrisi ve ortalama vektörü de kapalı biçimde şu şekilde elde edilebilir:

$$\mathbf{C}_\epsilon = \left(\mathbf{C}_{\bar{\mathbf{x}}}^{-1} + \frac{\mathcal{G}^T \mathcal{G}}{\sigma_n^2} \right)^{-1},$$

$$\mu_{\bar{\mathbf{x}}} = \mathbf{0}.$$

Son olarak, aktif LED'lerin indeksleri ve buna karşılık gelen $\hat{x}_{k,R}$ ve $\hat{x}_{k,I}$ 'in kestirimi, öncekine benzer şekilde Eve tarafında da (3.137), (3.138) gösterildiği gibi elde edilebilir.

3.3.5. Gizlilik Anahtarı ile PLS algoritmasının daha da geliştirilmesi

Önceki bölümde açıklanan vericiÖnkodlamasına dayalı PLS sisteminin yeteneğinin daha da geliştirilmesi için, bu bölümde, gizli anahtarlamalı yeni bir önceden-kodlanmış PLS tekniği önerilmektedir. Genlik/faz modülasyonlu (APM) veri sembolleri, $\mathbf{x}_F = [X_0, X_1, \dots, X_{N-1}]^T$, frekans bölgesindeki OFDM alt taşıyıcıları tarafından $X_k = |X_k| \exp(j\theta_k)$ biçiminde iletilmeden önce rastgele bir köşegen matrisi $\Psi = \text{diag}(e^{j\psi_0}, e^{j\psi_1}, \dots, e^{j\psi_{N-1}})$, ile şifrelenmektedir. Burada $\{\psi_k\}$ 'lere *döngüsel kaydırma şifreleme katsayıları* denir. Elde edilen şifreli vektör $\mathbf{c}_F = [C_0, C_1, \dots, C_{N-1}]^T$ frekans-bölgesinde şu şekilde oluşturulabilir:

$$\mathbf{c}_F = \Psi \mathbf{x}_F \quad (3.141)$$

burada, \mathbf{c}_F 'in k . bileşeni

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

$\{C_k\}$ 'lar, fiziksel dalga biçimi ve iletilen veri bitleri arasındaki ilişkiyi değiştirerek güçlü bir fiziksel katman güvenliği sağlar. Aşağıda kısaca açıklandığı gibi, ψ_k katsayıları, bir gizli anahtar dizisi aracılığıyla belirlenir. Daha sonra, şifrelenmiş OFDM mesajı \mathbf{c}_F ilk önce alıcıdaki yasal kullanıcı tarafından basit bir işlemle şifresi çözülür.

$$\mathbf{x}_F = \Psi^H \mathbf{c}_F. \quad (3.142)$$

Daha sonra veriler klasik OFDM alıcısı tarafından demodüle edilir. Ancak Eve'in pozisyonunda, gizli anahtar bilgisi bilinmediğinden, iletilen orijinal iletiyi \mathbf{x}_F güvenilir bir biçimde elde edemez. Önerilen şifreleme algoritmasının ana adımları şimdi şu şekilde açıklanmaktadır:

- (i) Bir noktadan diğer bir noktaya kablosuz optik bağlantıyı (OWC) gerçekleştirmenin en yaygın yolu, sırasıyla aşağı bağlantı (downlink) ve yukarı bağlantı (uplink) yönlerinde görünür ışık (VL) ve kızılötesi (IR) LED'ler kullanmaktır. OFDM iletimi sırasında, bir Q -bit uzunluğunda $\in \{64, 128, 256, \dots\}$ gizli anahtar dizisi $\mathbf{b} = (b_0, b_1, \dots, b_{Q-1})$ alıcıda oluşturulur ve bir IR yukarı bağlantı kanalı aracılığıyla vericiye geri gönderilir. Gizli anahtarın paylaşılmasının ardından, yasal kullanıcı kaynaktan şifrelenmiş veri paket-

leri alırken aynı zamanda yeni oluşturulan gizli anahtarı bir sonraki veri iletim aşaması için IR kanalı aracılığıyla paylaşır.

Kanal karşılıklık (channel reciprocity) sorunu, VLC uygulamalarında herhangi bir sorun yaratmaz ve tek bir antenin hem verici hem de alıcı olarak davrandığı RF sistemlerinden farklı olarak, alıcı-verici bileşenleri (LED ve PD) farklı olsa bile, Li-Fi sistemlerinde bu özellik doğal olarak bulunur. (3.109) denklemiyle verilen LoS kanal ifadesinden, kanal katsayılarının yalnızca iletim ortamının geometrik parametrelerine bağlı olduğu ve vericinin dalga boyundan bağımsız olduğu görülebilir. Sadece LoS kanal koşullarında bile, pratik OWC sistemlerinde rastgele yönelim ve hareketliliğin neden olduğu büyük ölçekli sönümlenme etkilerinin belirgin (deterministik) olmayan kanal katsayıları verdiği sonucuna varılabilir. Sonuç olarak, OWC kanallarındaki karşılıklık LoS durumlarında da geçerli olmaktadır. Bu nedenle, gizli anahtar bilgisini erişim noktasına iletmek için ek bir veri alışverişine gerek yoktur. Bunlara ek olarak verici ve alıcının paylaşılan gizli anahtar yardımıyla gizlice dinleme engellenirken bunu nasıl sürdürülebileceğiyle ilgili kritik konu, doğrudan yukarı bağlantıyı sağlayan IR kanalının özellikleri ile ilgilidir. Aydınlatma amaçlı [77] olmamasından dolayı IR LED'lerin yönlülüğü, VL tabanlı LED'lere kıyasla özünde çok yüksektir. Dolayısıyla, IR kaynaklarının ışın genişliği, VL eşdeğerlerine kıyasla önemli ölçüde daha küçüktür. Ayrıca, yasal kullanıcı üzerine yerleştirilen IR-LED'lerin yukarı yönü, dinleyicinin erişim noktası ile yasal kullanıcı arasında bulunmasını zorunlu kılar. Yasal kullanıcının elde tutulan mobil ekipmanı ise, bu gerekliliği pratik olarak olanaksız hale getirebilir. Sonuç olarak, hem IR-LED'lerin dar huzme profili hem de kullanıcı ekipmanının hareketliliği, yasal kullanıcı tarafından üretilen ve kaynağa gönderilen gizli anahtar bilgileri hakkında doğal koruma oluşturacaktır.

- (ii) $L \in \{1, 2, \dots, 7\}$ için verici, Q -bit gizli anahtar dizisi arasından rastgele ν th gizli anahtar bitini ilk şifreleme biti olarak seçer, b_ν . Daha sonra, sırayla L bitlik $b_\nu = (b_\nu, b_{\nu+1}, \dots, b_{\nu+L-1})$, diziyi seçerek ilk şifreleme dizisini oluşturur. ν rastgele sayısının değeri, OFDM sembollerinin şifrelenmesi tamamlandığında güncellenir. Şifreleme biti alt indisi $Q - 1$ 'a ulaştığında, ilk pozisyona taşınırken diğerlerini bir sonraki pozisyona sol dairesel bir çevrimsel kaydırma ile kaydırır. Ardından, döngüsel kaydırma şifreleme katsayıları, $\psi_1, \psi_2, \dots, \psi_{N-1}$, bunu izleyen şıkta açıklandığı gibi oluşturulur.
- (iii) Şifrelenmiş bit dizileri bilimesi durumunda, $\{b_0, b_1, \dots, b_{N-1}\}$, başlangıçta rastgele oluşturulan $\{b_0, b_1, \dots, b_{N-1}\}$ şifreleme bit dizilerinden yararlanarak bit konumu ν , döngüsel kaydırma şifreleme katsayıları $\{\psi_k\}_{k=0}^{N-1}$ tarafından belirlenir, [78].

$$\psi_k = \alpha_k \bmod 2^\kappa + \frac{\alpha_k}{2L} \quad (3.143)$$

burada κ sabit bir asal tamsayı olup 3, 5, 7, ..., arasından seçilir. α_k ise b_k aracılığıyla ikili tabandan ondalık tabana dönüştürme yoluyla oluşturulan k . şifreleme değeridir. (3.143)'nin sağ tarafındaki birinci ve ikinci terimlerin sırasıyla ψ_k tamsayısını ve ondalık

kısımlarını temsil etmekte ve L 'yi oluşturulan ψ_k ise çözünürlükle ilgilidir. Q -bit gizli anahtar dizisinin tasarımından sonra, vericide oluşturulan aynı ψ_k 'lar, iletilen OFDM-APM sembollerini (3.141)'ye göre frekans-bölgesinde şifreler ve bunların şifresini çözer. Bu nedenle, sistemin güvenlik başarımı, ön kodlama tarafından sağlanan fiziksel katman güvenliğinin yanı sıra, gizlice dinlemelere karşı önemli ölçüde iyileştirilmiş olmaktadır.

(iv) Rastgele seçilen bit konumunun gizlice dinlenmesi riskini önlemek için, kaynaktan yasal alıcıya optik kanalı üzerinden aktarım sırasında, [79]'da açıklandığı gibi, Çin bölme Teoremine (Chinese remainder theorem(CRT)) dayalı bir teknik kullanılır. Bu teknik aşağıdaki örneklerle adım adım açıklanmaktadır :

(i) İki karşılıklı asal tam sayı m_1 ve m_2 , diğer bir deyişle, $m_1 \neq m_2$, $\gcd(m_1, m_2) = 1$, verici ve alıcı ile paylaşılır.

(ii) Vericide, iki tamsayı r_1 ve r_2 , ν tarafından $r_i = \nu \pmod{m_i}$, $i = 1, 2$, alıcıya iletilir.

(iii) Alıcıda, uygunluk denklemleri alınan tamsayılarla şu şekilde oluşturulur:

$$\begin{aligned}\nu &\equiv r_1 \pmod{m_1} \\ \nu &\equiv r_2 \pmod{m_2}\end{aligned}\tag{3.144}$$

CRT, $\nu \pmod{V}$ ' nun $V = m_1 * m_2$ için aşağıdaki şekilde tek olarak elde edilebileceğini söylemektedir:

$$\nu = c_1.V_1.y_1 \pmod{V} + r_2.V_2.y_2 \pmod{V}\tag{3.145}$$

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

3.3.6. GLIM-OFDM Sistemlerinde Erişilebilir Gizlilik Oranı

Şimdi, GLIM-OFDM yapısına ilişkin MIMO telefon dinleme kanalının (wiretap channel) ulaşılabilir gizlilik oranı, $\mathbb{R}_{\text{GLIM-OFDM}}$, bir dinleyicinin varlığında incelenmektedir. (11) ve (12)'deki Bob ve Eve için gözlem sinyalleri kullanılarak, ulaşılabilir gizlilik oranı şu şekilde ifade edilebilir:

$$\begin{aligned}R_{\text{GLIM-OFDM}} &= \mathbb{I}(\mathbf{s}_B; \mathbf{y}_B) - \mathbb{I}(\mathbf{s}_B; \mathbf{y}_E), \\ &= \mathbb{H}(\mathbf{y}_B) - \mathbb{H}(\mathbf{y}_B | \mathbf{s}_B) - \left(\mathbb{H}(\mathbf{y}_E) - \mathbb{H}(\mathbf{y}_E | \mathbf{s}_E) \right), \\ &= \frac{N_r}{2} \log_2 \left(\frac{\sigma_E^2}{\sigma_B^2} \right) - \left(\mathbb{H}(\mathbf{y}_E) - \mathbb{H}(\mathbf{y}_B) \right),\end{aligned}\tag{3.146}$$

Burada $\mathbb{I}(\cdot; \cdot)$, $\mathbb{H}(\cdot)$ ve $\mathbb{H}(\cdot|\cdot)$ sırasıyla ortak bilgi, fark (differential) bilgi ve koşullu bilgileri göstermekte olup şu şekilde tanımlanmaktadır:

$$\begin{aligned}\mathbb{H}(\mathbf{y}_\times|\mathbf{s}_\times) &= \frac{N_r}{2} \log_2(2\pi e\sigma_\times^2) \\ \mathbb{H}(\mathbf{y}_\times) &= - \int p(\mathbf{y}_\times) \log_2 p(\mathbf{y}_\times) d\mathbf{y}_\times\end{aligned}\quad (3.147)$$

ve $\mathbf{y}_\times, p(\mathbf{y}_\times)$, $\times \in \{B, E\}$ için \mathbf{y}_\times 'in olasılık yoğunluk fonksiyonunu göstermektedir, [80].

(3.118)'den görülebileceği gibi, $p(\mathbf{y}_B)$, sinyal vektörü $\mathbf{x} = [x_{k,R}^+, x_{k,R}^-, x_{k,I}^+]$ 'ün pdf'ine bağlıdır ve gürültü vektörü, \mathbf{n}_B , ortalaması sıfır ve $\mathbf{C}_{n,B} = \sigma_B^2 \mathbb{I}_{N_r}$ ile gösterilen kovaryansa sahip bir Gauss dağılımlı rastlantı değişkenidir. IFFT'nin $E\{\mathbf{x}_T^\dagger \mathbf{x}_T\} = N$ ile normalize edildiği varsayılarak, \mathbf{x}_T vektörün bileşenlerin her biri, büyük N değerleri için, $\mathcal{CN}(0, 1)$ dağılımına sahip olur. Bu nedenle, $x_{k,R}$ ve $x_{k,I} \sim \mathcal{N}(0, 1/2)$ ve sonuç olarak, \mathbf{x}_T 'in dört bileşeninin tümü birbirinden bağımsızdır ve simetri nedeniyle aşağıda verilen kırılmış Gauss olasılık yoğunluk fonksiyonuna uygun şekilde dağılır.

$$p_{x_{k,R(I)}^\pm}(v) = \frac{1}{\sqrt{\pi\beta^2}} e^{-v^2/\beta^2} u(v) + \frac{1}{2} \delta(v), \quad (3.148)$$

burada $u(v)$ ve $\delta(v)$ sırasıyla birim adım (unit-step) ve delta-Dirac fonksiyonlarını temsil eder. GLIM-OFDM'in her bir LED'inden yayılan ortalama elektrik gücü ve varyans şu şekilde elde edilebilir:

$$I = E\{x_{k,R(I)}^\pm\} = \frac{1}{2\sqrt{\pi}}; \quad \sigma_{x_{k,R(I)}^\pm}^2 = \frac{1}{4} \left(1 - \frac{1}{\pi}\right). \quad (3.149)$$

\mathbf{x} ve \mathbf{n}_B 'in tüm bileşenleri ve ayrıca \mathbf{x} ve \mathbf{n}_B rasgele vektörleri birbirinden bağımsız olduklarından, $\mathbf{y}_B = [y_1, y_2, y_3, y_4]^T$ 'in pdf'si şu şekilde ifade edilebilir:

$$p(\mathbf{y}_B) = \prod_{i=1}^4 p_{y_i}(y), \quad (3.150)$$

burada $y_i = \beta x_{k,R(I)} + n_i$ \mathbf{y}_B 'in i bileşenidir. y_i 'nin pdf'si için tam analitik ifade, bağımsız rastgele değişkenlerin toplamını hesaplamak için konvolüsyon teoremi ile türetilir. $i = 1, 2, 3, 4$, ve $-\infty < y < +\infty$ için bir takım cebirsel işlemlerden sonra, şunlar elde edilir:

$$p_{y_i}(y) = 0.5 \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{y^2}{2\sigma_n^2}} + \frac{1}{\sqrt{\pi(2\sigma_n^2 + \beta^2)}} \left(1 - Q\left(\frac{\beta y}{\sigma_n \sqrt{2\sigma_n^2 + \beta^2}}\right)\right) e^{-\frac{y^2}{2\sigma_n^2 + \beta^2}}. \quad (3.151)$$

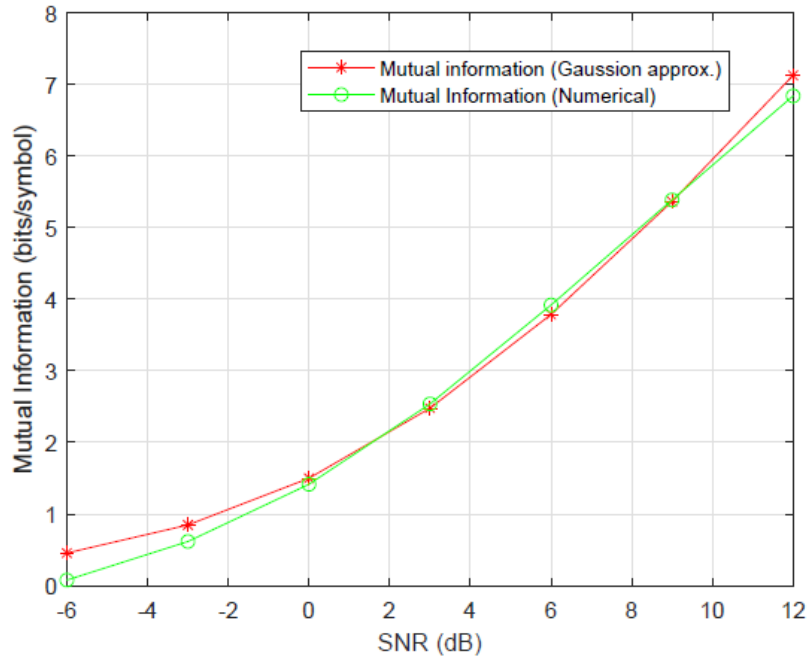
Sonuçta, (40) kullanılarak, (3.146) içindeki kaynak ve Bob arasındaki karşılıklı bilgi şu şekilde belirlenebilir:

$$\mathbb{I}(\mathbf{s}_B; \mathbf{y}_B) = - \sum_{i=1}^4 \int_{-\infty}^{\infty} p_{y_i}(y) \log_2(p_{y_i}(y)) dy - \frac{1}{2} \log_2(2\pi e \sigma_B^2). \quad (3.152)$$

(3.152)'nin analitik yoldan kesin olarak bulunması matematiksel olarak mümkün değildir. Ancak bu sonuç, değişken SNR değerleri için entropiyi sayısal olarak hesaplamak için kullanılabilir. Bununla birlikte, yapmış olduğumuz kapsamlı bilgisayar benzetimleri, $p_{y_i}(y)$, olasılık yoğunluk fonksiyonunun, ortalaması $\mu_{y_i} = \beta/(2\sqrt{\pi})$ ve varyansı $\sigma_{y_i}^2 = \frac{\beta^2}{4}(1 - \frac{1}{\pi}) + \sigma_n^2$ olan bir Gauss dağılımına yaklaştığı görülmektedir. Bu yaklaşıklık altında ortak bilgi (mutual information) ifadesi aşağıdaki gibi doğruya çok yakın biçimde hesaplanabilir.

$$\mathbb{I}_{\text{approx}}(\mathbf{s}_B; \mathbf{y}_B) = 4 \frac{1}{2} \log_2 \left(1 + \frac{\beta^2}{4} \frac{(1 - \frac{1}{\pi})}{\sigma_{n_B}^2} \right). \quad (3.153)$$

Bu yaklaşımın geçerli olduğunu gösteren bir örnek olarak, Şekil 3.6'de, belli bir SNR aralığı için (3.152) ve (3.153)'den sayısal olarak yaklaşık elde edilen ortak bilgiler karşılaştırılmakta ve -6 dB ile 12 dB arasında bu iki eğrinin neredeyse birbiriyle tamamen örtüştüğü gösterilmektedir.



Şekil 3.6. Ortak bilginin (mutual information) yaklaşık ve kesin Gauss olasılık dağılımları kullanılarak hesaplanması durumunda karşılaştırılması

Öte yandan, Eve'in entropisinin, $\mathbb{H}(\mathbf{y}_E)$, hesaplanması, $\mathbf{y}_E = \beta \mathbf{G}\mathbf{x} + \mathbf{n}_E$ 'nin pdf'inin hesaplanmasını gerektirdiği için bu analitik olarak olanaksız hale gelir. Bu nedenle, Eve'e ilişkin ortak bilgiyi elde etmek için, \mathbf{x} 'in pdf'inin ortalama vektörü $\mu_{\mathbf{x}} = \frac{1}{2\sqrt{\pi}}\beta \mathbf{G}\mathbf{1}$ ve kovaryans matrisi $\mathbb{C}_{\mathbf{x}} = \frac{\beta^2}{4}(1 - \frac{1}{4\pi})\mathbf{G}\mathbf{G}^T$ sahip Gauss dağılımlı bir raslantı değişkenini olduğu varsayılmaktadır. Sonuç olarak, Eve için ortak bilgi şu şekilde elde edilebilir:

$$\mathbb{I}_{\text{approx}}(\mathbf{s}_E; \mathbf{y}_E) = \frac{1}{2} \log_2 \left(\det \left(\mathbb{I}_4 + \frac{\mathbb{C}_{\mathbf{x}}}{\sigma_{n_E}^2} \right) \right) \quad (3.154)$$

burada $\mathbf{1} \triangleq [1, 1, \dots, 1]^T$, \mathbb{I}_4 bir 4×4 köşegen matrisi göstermekte ve \mathbf{G} (12) de tanımlanmıştır. Son olarak, GLIM-OFDM için ulaşılabilen gizlilik oranı, (3.154) ve (3.153) ifadelerini (3.146)'de yerine koyarak elde edilir.

$$R_{\text{GLIM-OFDM}} = \mathbb{I}_{\text{approx}}(\mathbf{s}_B; \mathbf{y}_E) - \mathbb{I}_{\text{approx}}(\mathbf{s}_E; \mathbf{y}_E). \quad (3.155)$$

(3.155)'den belirlenen ulaşılabılır gizlilik oranı ifadesinin, kırılmış Gauss varsayımı altında elde edilmiş bir üst sınır olduğuna dikkat edilmelidir. OFDM zaman-bölgesi sinyal örnekleri, sürekli-değerli Gauss dağılımı yaklaşıklığı altında çıkarıldıkları için erişilebilir gizlilik oranını sağlamazlar. Bu nedenle, sürekli-değerli sinyaller için hesaplanan ortak bilgi genellikle sonsuz değer alabilir. Dolayısıyla, bu sonuçların, entropileri ve ortak bilgileri sonlu değerler alan ve ayrık kaynağın alfabe boyutu ile sınırlı olan ayrık değerli sinyallerle karşılaştırılmaması gerekir. Bu gözlemin bir sonucu olarak, göz önüne aldığımız GLIM-OFDM sisteminde, frekans-bölgesinde iletilen veri sembolleri, M-PSK/M-QAM gibi ayrık değerli raslantısal değişkenler olduğundan, ulaşılabilecek en büyük hız veya kapasite $\log_2 M$ bit/sembol ile sınırlıdır. Veri sembollerinin ML tabanlı sezimi (detection) [80]'da olduğu gibi düşünüldüğünde, Bob ve Eve'in bu tür ayrık-sürekli belleksiz kanallarının kapasitesi şu şekilde ifade edilebilir:

$$\mathbb{C}_X = \log_2(M) - \frac{1}{M} \sum_{i=1}^M \mathbb{E}_{\mathbf{n}_X} \left\{ \log_2 \sum_{j=1}^M \exp \left(\Psi_X(i, j) \right) \right\}, \quad X \in \{B, E\} \quad (3.156)$$

dir ve $\Psi_X(i, j)$

$$\Psi_X(i, j) = - \frac{\|x_F(i) - x_F(j) + n_X\|^2 + \|n_X\|^2}{\sigma_X^2}.$$

ilişkisinden elde edilir. $x_F(i)$, OFDM alt taşıyıcılarından birinden iletilen MPSK/MQAM veri sembollerinin i 'nci alfabe değeridir. Sonuç olarak, optik GSSK'nın gizlilik kapasitesi şu

şekilde belirlenebilir:

$$C_{GSSK} = C_B - C_E. \quad (3.157)$$

(3.157) içindeki C_{GSSK} 'in kapalı biçimde bir ifadeyle analitik olarak elde edilemeyeceği unutulmamalıdır. Bununla birlikte, Alice-Bob ve Alice-Eve arasında saniyede bit cinsinden azaltılmış karmaşıklık bilgi hızı, bit başına karşılıklı bilgi temelinde hesaplanabilir $\mathbb{I}_X(b; \hat{b}_{kez})$, $X \in \{B, E\}$. Ortak bilgi, önerilen GLIM-OFDM sistemi için $b \in \{0, 1\}$ giriş bitleri ile buna karşılık gelen demodüle edilmiş çıkış bitleri $\hat{b}_X \in \{0, 1\}$ arasında ölçülür. Bu nedenle, Alice-Bob ve Alice-Eve arasındaki sonuçtaki ikili giriş-çıkış kanalları, ϵ_B ve ϵ_E çapraz olasılıkları olan bir ikili simerik kanak (binary symmetric channel (BSC)) olarak modellenenebilir ve kanalın entropisi giriş olasılıklarının eşit olması, yani $P(0) = P(1) = 1/2$, durumunda enbüyük değeri olan 1 bit'e ulaşır. Sonuç olarak, her iki kanal da kanal kapasitesini tam olarak elde eder.

$$\begin{aligned} C_{GLIM-OFDM} &= \mathbb{I}_B(b; \hat{b}_B) - \mathbb{I}_E(b; \hat{b}_E), \\ &= \mathbb{H}_B(b) - \mathbb{H}_B(b|\hat{b}_B) - \mathbb{H}_E(b) + \mathbb{H}_E(b|\hat{b}_E), \end{aligned} \quad (3.158)$$

burada $\mathbb{H}_X(b) = -\sum_{m=0}^1 P(m) \log_2 P(m)$, $P(m)$, $m = 1, 2$, giriş olasılıklarına bağlı olarak giriş bitlerinin entropisini göstermektedir. Diğer taraftan, $\mathbb{H}_X(b|\hat{b}_X)$ koşullu entropiyi temsil etmekte ve BSC kanal için bu entropi şu şekilde hesaplanmaktadır:

$$\mathbb{H}_X(b|\hat{b}_X) = -\epsilon_X \log_2 \epsilon_X - (1 - \epsilon_X) \log_2 (1 - \epsilon_X). \quad (3.159)$$

Bu nedenle, (3.159)'yi (3.158) ile değiştirerek ve $H_X(b) = 1$ 'dan yararlanarak ve giriş bitlerinin olasılığı eşit olduğundan, L için tam olarak ulaşılabilir gizlilik kapasitesi, yani genlik-faz modülasyonlu (anplitude-phase modulatın (APM)) sembol başına iletilen bit sayısı, aşağıdaki gibi hesaplanır.

$$C_{GLIM-OFDM} = L \left(\epsilon_B \log_2 \epsilon_B + (1 - \epsilon_B) \log_2 (1 - \epsilon_B) - \epsilon_E \log_2 \epsilon_E - (1 - \epsilon_E) \log_2 (1 - \epsilon_E) \right). \quad (3.160)$$

(3.160)'da ϵ_X ile gösterilen olasılık değerleri APM veri sinyallerinin frekans-bölgesindeki bit hata olasılığını (BER) vermektedir.

4. PLS-VLC SİSTEMLERDE KANAL KESTİRİMİ

4.1. Önkodlamasız GLIM-OFDM Sistemlerde Kanal Kestirimi

Fiziksel katman güvenliği (PLS) yeteneği olmayan GLIM-OFDM sistemi Panayırıcı ve araştırma gurubu tarafından geliştirilmiş [75] ve literatürde çok sayıda atıf olarak dikkat çekmiştir. Düz-frekans MIMO kanalları için önerilen GLIM OFDM alıcı-verici blok diyagramı Şekil 4.1'de verilmiştir. \mathbf{u} vektörünü taşıyan $N \log_2(M)$ bilgi bitler bir GLIM-OFDM sisteminin vericisine uygulanır. Burada N , OFDM alt taşıyıcılarının sayısını, M de, iletimde kullanılan M -düzeyli dik genlik modülasyonu (M -QAM) simgelerin düzeyini göstermektedir. DCO-OFDM, ACO-OFDM ve DC öngerilimli olmayan OFDM (NDC-OFDM) optik iletişim sistemlerin çalışması, ters hızlı Fourier dönüşümü (Inverse Fast Fourier Transform, IFFT) işleminden sonra gerçel zamanlı sinyalleri üretmek için Hermisyen simetrisine dayanır. Önerilen teknikte ise, OFDM modülatörü karmaşık frekans bölgesi OFDM çerçevesi \mathbf{x}_F 'i, Hermisyen simetrisi gerektirmeden doğrudan işler. Elde edilen zaman-bölgesi (time-domain) OFDM çerçevesi $\mathbf{x}_T = [x_1, x_2, \dots, x_N]^T$, karmaşık değerli ve iki kutuplu (pozitif ve negatif değerli) öğelerinden dolayı bir VLC kanalı aracılığıyla iletilemez. Bu problemi çözmek için yeni bir LED indis modülasyonu tabanlı MIMO iletişim tekniği geliştirilmiştir. Paralelden seriye (P/S) dönüşümden sonra her bir zaman bölgesi OFDM örneği, x_k , $k = 0, 1, \dots, N-1$, önce $x_{k,R}$ ve $x_{k,I}$ ile gösterilen gerçel ve sanal kısımlarına ayrılır. Bu şekilde elde edilen iki kutuplu örnekler, $x_{k,R}$ ve $x_{k,I}$ ile gösterilen pozitif gerçel değerli örneklere, pozitif-negatif (+/-) ayırıcılar tarafından (1) ilişkisindeki gibi işlenerek dönüştürülür:

$$x_{k,R}^+ = \begin{cases} x_{k,R} & \text{if, } x_{k,R} > 0 \\ 0 & \text{if, } x_{k,R} < 0 \end{cases}, \quad x_{k,R}^- = \begin{cases} 0 & \text{if, } x_{k,R} > 0 \\ -x_{k,R} & \text{if, } x_{k,R} < 0 \end{cases} \quad (4.1)$$

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

Burada, n_R ve n_T , sırasıyla alıcı (Rx) ve verici (Tx) birimlerinin sayısını göstermektedir.

Şekil 4.1'den görüleceği gibi, LED'ler $x_{k,R}$ ve $x_{k,I}$ sinyallerinin mutlak değerlerini iletmektedir ve dolayısıyla pozitif değerli gerçel sayılardır. Ayrıca, diğer optik iletişim sistemlerinden farklı olarak GLIM-OFDM, IFFT'nin girişindeki Hermisyen simetrisini ve buna bağlı spektral verimlilik kaybını tamamen ortadan kaldırır. Sonuç olarak, GLIM OFDM sisteminin spektral verimliliği $\log_2(M)$ [bit/s/Hz] olup, klasik sistemlere oranla iki katına varan bir spek-

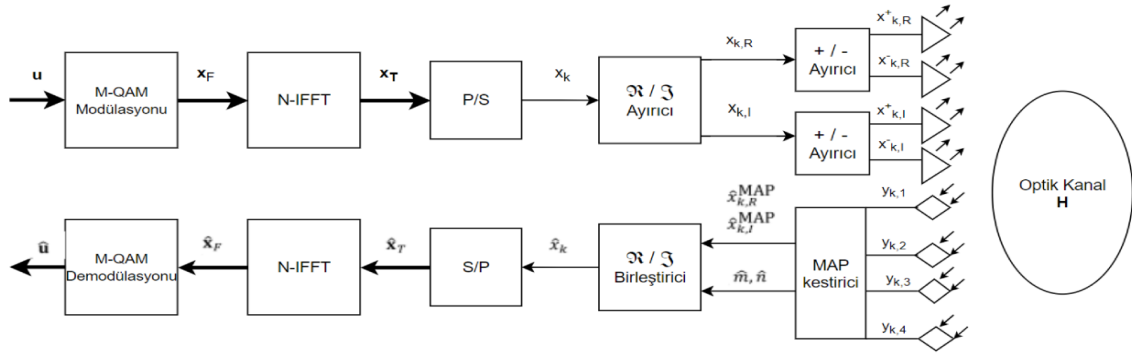
tral verime ulaşır. Pozitif ve gerçel değerli OFDM zaman-bölgesi örnekleri, $x_{k,R}^+$, $x_{k,R}^-$, $x_{k,I}^+$ ve $x_{k,I}^-$ $k = 0, 1, \dots, N - 1$, \mathbf{H} ile gösterilen bir optik 4×4 MIMO kanalı üzerinde (4.2)'deki gibi alıcıda FFT girişine ulaşır:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}. \quad (4.2)$$

Yukarıda 4.2'de verilen iletim modeli, klasik tek taşıyıcılı MIMO-SM sistemlerine benzer; ancak, bu modellerden iki ana nedenden dolayı farklılık gösterir: Birincisi, alıcıya gelen sinyal, 4.2, gerçel değerli değerlidir ve ikincisi, iletilen veri vektörü \mathbf{x} , kırpılmış bir Gauss dağılımına sahiptir. Ayrıca, alınan sinyal vektörü \mathbf{y} 'nin OFDM demodülatörüne doğrudan iletilmesi mümkün değildir. Çünkü, frekans-bölgesindeki \mathbf{x}_F , sinyal vektörünün sezimi için, daha önce zaman-bölgesinde karmaşık değerli OFDM örneklerinin bir şekilde kestirilerek oluşturulması gerekir. Buna basit bir çözüm olarak sıfıra-zorlanmış bir denkleştiricinin (zero-forcing equalizer) kullanılmasıdır. Bu işlemden sonra, alıcı \mathbf{x}_{ZF} vektörünün enbüyük mutlak değerli genliklerini seçerek, LED indislerini belirlemektedir. Ancak, basit gerçekleştirme yapısına karşın ZF-denkleştiricinin, sistemde oluşan gürültüyü çok büyük oranda güçlendirdiği bilinmektedir. Buna karşın yine literatürde yaygın olarak kullanılan doğrusal minimum karesel ortalama kestirim tekniği (Linear Minimum-Mean Square Estimation (LMMSE)) tekniği ZF-denkleştiricisinde ortaya çıkan problemi kısmen çözmekte ise de yine de optimal kestirimin sağladığı başarımdan uzaktır. Bu iş paketinde, sözkonusu MIMO kanalın kestiriminden sonra, aşağıdaki bölümde ayrıntıları verileceği gibi, \mathbf{x} , zaman-bölgesi örneklerinin olasılık dağılımı bir ön-bilgi olarak (a-priori) kullanılarak optimal yapıda doğrusal olmayan yeni bir minimum-karesel-ortalama kestirim tekniği (NL-MMSE) 3. bölümde geliştirilmiştir

Şimdi gözönüne alınan GLIM-OFDM sisteminde öncelikle önkodlama kullanmadan bir kanal kestirim algoritması geliştirilecektir. Belli sayıda OFDM sembollerinden oluşan bir çerçevede ilk OFDM sembolünün tüm taşıyıcılarından bilinen pilot simgeler iletilerek MIMO kanal, geliştirilen kanal kestirim algoritmasıyla kestirilecektir. Son olarak kestirilen kanal katsayıları kullanılarak, OFDM çerçevesinde diğer OFDM semboller tarafında taşınan veri simgeleri alıcıda enbüyük olabilirlik (Maximum Likelihood (ML)) tekniğiyle sezim (Detection) işlemi gerçekleştirilecektir. Çalışmanın ikinci aşamasında ise, bir önkodlama kullanılarak alıcıdaki indirgenmiş sinyal modelinden yararlanarak OFDM zaman-bölgesi örneklerinin (time-domain samples) doğrusal ve doğrusal olmayan enküçük karesel ortalama kestirimleri (LMMSE, NL-MMSE) elde edilecek ve yeni sistemin BER başarımı incelenecektir.

GLIM OFDM'de, alıcının FFT girişine ulaşan, bileşenleri pozitif ve gerçel değerli,



Şekil 4.1. OFDM verici ve alıcı sistemin blok şeması

zaman-bölgesi sinyal vektörü şu şekilde ifade edilebilir:

$$\mathbf{y}_k = \mathbf{H}\mathbf{x}_k + n_k \quad (4.3)$$

burada $\mathbf{x}_k \in \mathcal{R}^{4 \times 1}$, her $k = 0, 1, \dots, N - 1$ için sistemin verici tarafında IFFT çıkışında üretilen zaman-bölgesi örnek vektörlerini ve $\mathbf{n}_k \in \mathcal{R}^{4 \times 1}$, bileşenleri istatistiksel bağımsız toplamsal beyaz Gauss gürültü vektörünü göstermektedir. Bu çalışmada ele alınan VLC GLIM-OFDM sisteminde belli bir OFDM zaman çerçevesi içindeki ilk OFDM sinyalinin tüm alttaşıyıcıları pilot simgelere ayrılmıştır. Verilen bir çerçeve içinde optik kanalın fazla değişme özelliğinden yararlanarak, çerçevedeki bunu izleyen diğer OFDM sembollerinin tüm alttaşıyıcılarından veri iletimi gerçekleştirilmektedir. Bu durumda verilen her zaman çerçevesi içinde kanal matrisini kestirmek için pilot simgelerden üretilmiş $\mathbf{X} = [\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}]$ sinyal vektörlerinin alıcıda bilindiği varsayılarak alıcı sinyali şu şekilde ifade edilebilir:

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N}. \quad (4.4)$$

$\mathbf{Y} = [\mathbf{Y}_0, \mathbf{Y}_1, \dots, \mathbf{Y}_{N-1}] \in R^{4 \times N}$ ve $\mathbf{N} = [\mathbf{n}_0, \mathbf{n}_1, \dots, \mathbf{n}_{N-1}] \in R^{4 \times N}$ dir. Matris ilişkilerinden yararlanarak \mathbf{Y} matrisi $4N$ boyutlu bir vektör olarak şöyle ifade edilebilir:

$$\mathbf{y} = \mathbf{Q}\mathbf{h} + \mathbf{n}. \quad (4.5)$$

Burada $\mathbf{y} = \text{vec}(\mathbf{Y})$, $\mathbf{n} = \text{vec}(\mathbf{N})$ ve $\mathbf{Q} = \mathbf{X}^T \otimes \mathbf{I}_r$ olup \otimes Kronocker çarpımını göstermektedir. (4.5)'teki doğrusal gözlem denkleminde yararlanarak, bilinmeyen \mathbf{h} kanalı için Doğrusal Minimum Karesel Ortalama kestirimi (linear minimum mean square estimation (LMMSE)) ilişikteki gibi elde edilir:

$$\hat{\mathbf{h}}_{LMMSE} = \mathbf{Q}^T (\mathbf{Q}\mathbf{Q}^T + (1/\rho)\mathbf{I}_r)^{-1} \mathbf{y} \quad (4.6)$$

olup, burada $\rho = I/\sigma_n^2$ ve $I = 1/\sqrt{2\pi}$, katlanmış-Gauss (folded-Gaussian) olasılık dağılımına sahip $|x_{k,R}|$ ve $|x_{k,I}|$ örnek değerlerin istatistiksel ortalamasının karesine eşittir. Bu ilişkiyle hesaplanan kanal kestiriminde yapılan hata vektörü $\mathbf{e} = \hat{\mathbf{h}}_{LMMSE} - \mathbf{h}$ ise, ortalama karesel hata (mean-square error, MSE), şu şekilde tanımlanır:

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

Bu tanımdan yararlanarak göz önüne alınan kanal kestiriminde yapılan ortalama karesel hata şu şekilde elde edilir:

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

4.2. Kanal Kestiriminde Cramer-Rao Alt Sınırı

Elde edilen kanal kestiriminde yapılan ortalama hatanın alt sınırı Cramer-Rao (CR) alt sınırı ile belirlenir ve bu sınır ilişikteki gibi hesaplanır:

$$MSE = E \{ (\hat{\mathbf{h}} - \mathbf{h})^T (\hat{\mathbf{h}} - \mathbf{h}) \geq \mathbf{I}(\mathbf{h})^{-1} \}. \quad (4.7)$$

Burada $\hat{\mathbf{h}} \triangleq \hat{\mathbf{h}}_{LMMSE}$ ve $\mathbf{I}^{-1}(\mathbf{h})$ 'ye *Cramer-Rao* alt sınırı adı verilir. $\mathbf{I}(\mathbf{h})$ aşağıdaki gibi hesaplanır:

$$\mathbf{I}(\mathbf{h}) = E \left\{ \frac{\partial^2 \ln p(\mathbf{y}; \mathbf{h})}{\partial \mathbf{h}^2} \right\} \quad (4.8)$$

Bu ilişkide, $p(\mathbf{y}; \mathbf{h})$, $\mathbf{Q}\mathbf{h} + \mathbf{w}$ biçimde modellenmiş alıcıya ulaşan sinyalin olasılık yoğunluk fonksiyonunu göstermekte olup

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

biçiminde ifade edilir. $p(\mathbf{y}; \mathbf{h})$ 'nin (7)'deki gibi 2. kısmi türevi alınarak \mathbf{I} için aşağıdaki ifade elde edilir:

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

Son olarak bu ifade yardımıyla elde edilen kanal kestirimi için Cramer-Rao alt sınırı aşağıdaki gibi bulunur:

$$MSE \geq \sigma_w^2 \text{trace} \left((\mathbf{Q}^T \mathbf{Q})^{-1} \right). \quad (4.9)$$

4.3. Önkodlamsız GLIM-OFDM Sisteminin BER Başarımı

Optik kanal matrisi \mathbf{H} , sütun vektörleri açısından şu şekilde tanımlanır: $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \mathbf{h}_4]$ ve bu durumda (2)'de verilen gözlem sinyali şu şekilde ifade edilebilir:

$$\mathbf{y} = \mathbf{h}_m \bar{x}_{k,R} + \mathbf{h}_n \bar{x}_{k,I} + \mathbf{n}, \quad (4.10)$$

burada $\bar{x}_{k,R} = |x_{k,R}|$, $\bar{x}_{k,I} = |x_{k,I}|$, $m \in \{1, 2\}$ and $n \in \{3, 4\}$. $|\bar{x}_{k,R}|$ ve $|\bar{x}_{k,I}|$ değişkenlerinin aşağıdaki gibi katlanmış Gauss (folded Gaussian) dağılımına sahip olduğu kolayca gösterilebilir.

$$p_{\bar{x}_{k,R(I)}}(v) = \frac{2}{\sqrt{\pi}} e^{-v^2} u(v). \quad (4.11)$$

Bir önceki altbölümde açıklandığı gibi, kestirilen kanal yardımıyla alıcıda önce bir ZF-denkleştirici kullanılarak, aşağıdaki gibi \mathbf{x} 'in bir kestirimi elde edilir,

$$\mathbf{x}_{ZF} = \hat{\mathbf{H}}^{-1} \mathbf{y}.$$

Bundan sonra, alıcı iletimdeki aktif LED'lerin indislerini ve bu indislerde taşınan veri simgelerini, \mathbf{x}_{ZF} vektörünün enyüksek mutlak-değerli genliklerini seçerek belirler. Son olarak, GLIM-OFDM, klasik uygulamada olduğu gibi, alıcıda FFT alarak frekans bölgesine geçip son veri sezimi işlemi enbüyük olabilirlik (maximum likelihood (ML)) tekniği ile gerçekleştirir. Aşağıdaki paragraflarda GLIM-OFDM'in bit hata başarımı (BER) bilgisayar simülasyonlarıyla incelenmektedir.

Kanal kestirimi için, pilot simgelerin eklenmesi gereklidir. Bu amaçla, genel olarak OFDM'nin frekans bölgesindeki farklı altaşıyıcılar pilot simgelerin taşınması için ayrılmıştır. Ancak bu çalışmada kullanılan VLC tabanlı OFDM sisteminde belli bir OFDM zaman çerçevesi içindeki ilk OFDM sinyalinin tüm altaşıyıcıları pilot simgelere ayrılmıştır. Verilen bir çerçeve içinde optik kanalın fazla değişmeme özelliğinden yararlanarak, çerçevedeki diğer OFDM

sinyallerinin tüm alt taşıyıcılarından veri iletimi gerçekleşir. Bu konfigürasyona bağlı olarak, her OFDM çerçevesi içinde, önceki bölümde açıklanan kanal kestirim algoritması kullanılarak kanal kestirilmekte ve kestirilen kanal değerlerini kullanarak alıcıda frekans bölgesinde iletilen veriler, veri sezim işlemi yardımıyla, belli bir hata başarıımı ile elde edilmekte ve gerek analitik olarak elde edilen kanal kestirim algoritmasının ortalama karesel hata (mean square error, MSE) başarıımı ve bu başarıımın ulaşabileceği Cramer-Rao alt sınırı ve gerekse sistemin veri sezim başarıımı incelenmektedir. Şekil 4.2'de, 4QAM, 8QAM ve 16QAM modülasyonlu iletişimde gerçekleşen kanal kestiriminin karesel ortalama (MSE) hata başarıımları, sistemdeki sinyal-gürültü oranının (SNR) fonksiyonları olarak elde edilmiştir. Şekil 4.2'den çıkarılan en önemli sonuçlar, teklif edilen kanal kestirim algoritmasının MSE başarıımının gerçek uygulamalar için çok uygun olduğu ve kullanılan farklı düzeylerdeki modülasyon tekniklerinden neredeyse tamamen bağımsız olduğudur. Ayrıca MSE başarıımının neredeyse Cramer-Rao altsınırına ulaştığı görülmektedir. Bu hesaplamalar ve elde edilen sonuçlardan, teklif edilen kanal kestirim algoritmasının çok etkin bir şekilde çalıştığı ve ayrıca hesaplama karmaşıklığının çok küçük olduğu sonucuna varılmaktadır

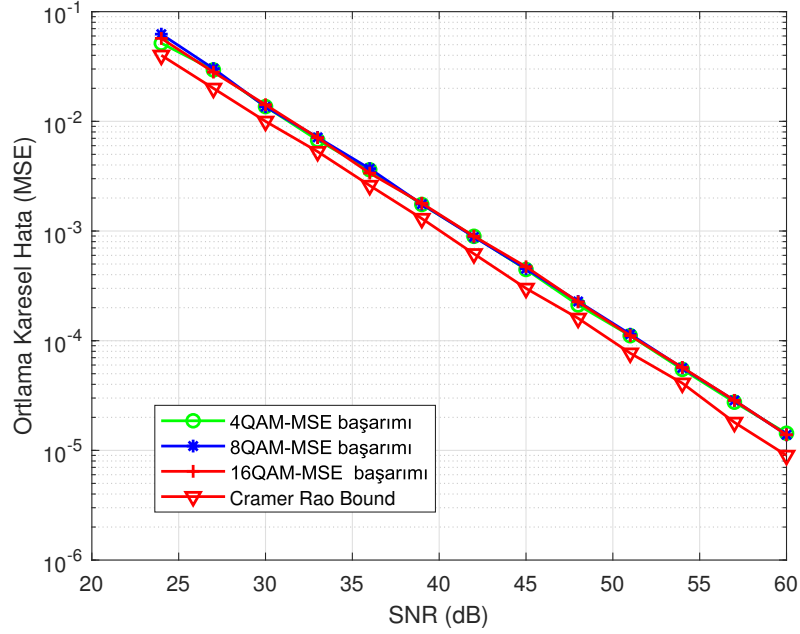
Şekil 4.3'de, kestirilen kanal bilgilerini kullanarak, 4QAM, 8QAM ve 16QAM modülasyonları için alıcıda gerçekleştirilen veri sezim işleminin BER başarıımı sinyal-gürültü oranının fonksiyonu olarak incelenmektedir. Bu şekilden açık olarak görüleceği gibi, kanal kestirim hatalarının varlığı altında ulaşılabilen sistemin BER başarıım düzeyi çok yüksektir. Diğer bir deyişle, Şekil 4.3'den, her modülasyon düzeyinde, kanalın mükemmel bilindiği ve kanal kestiriminin kullanıldığı durumlar için elde edilen BER eğrilerinin neredeyse üst üste geldiği görülmektedir. Sonuç olarak, ulaşılan çıktılara bakıldığında, kanal kestirimi sonucunda ulaşılan BER başarıımının kanalın mükemmel bilinmesi durumundaki BER başarıımına çok yakın olduğu görülmektedir.

4.4. Önkodlamalı Durumda NL-MMLS Algoritması geliştirilmesi ve MIMO

Kanal Kestirimi Etkisi Altında Sistemin BER Başarıımı

Bu kısımda, bir GLIM-OFDM yapısındaki VLC sistemin zaman-bölgesindeki giriş sinyal örneklerine bir önkodlama(pre-coding) uygulandığı durumda, alıcıda NL-MMSE tabanlı optimal bir denkleştirici tasarlanmakta ve daha sonra, kestirilen kanalın etkisi altında, alıcıda bu denkleştiriciyi kullanılarak, sistemin BER başarıımı incelenmektedir. Önkodlamalı GLIM-OFDM sisteminin blok şeması Şekil(4.4) 'de verilmektedir.

Öncelikle bundan önceki bölümde açıklandığı gibi, verici kısmında sinyal örneklerinin positif ve negatif kısımlarına ayırıp benzer şekilde önkodlamayla elde edilen güncellenmiş



Şekil 4.2. Kanal kestirimi MSE başarıımı ve Cramer-Rao alt sınırı

$\mathbf{X}_0 \in \mathcal{R}^{4 \times N}$ sinyali aşağıda açıklanan adımlarla elde edilmektedir:

$$\mathbf{P} = (\mathbf{H}^T \mathbf{H})^{-1} \mathbf{H}^T, \quad \text{Ön-kodlama gerçekleme}$$

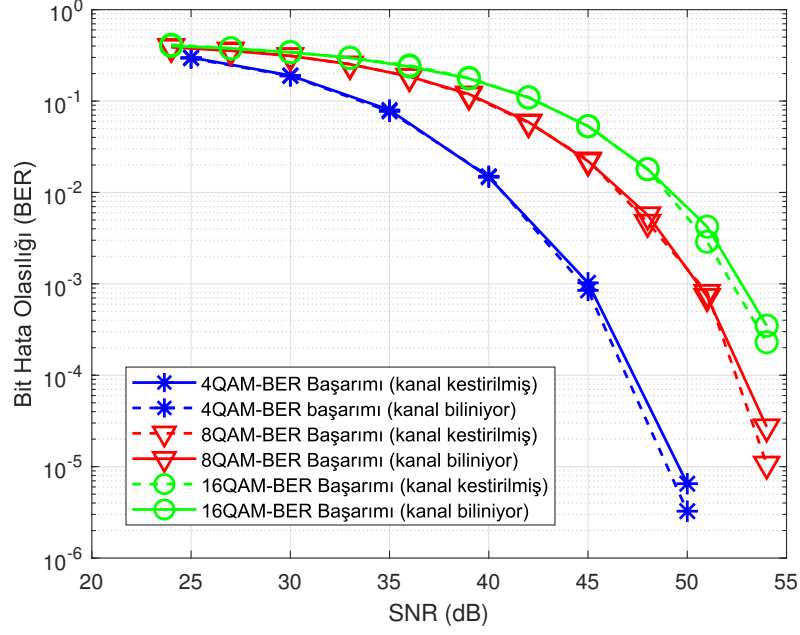
$$\beta = \sqrt{n_R / \text{trace}(\mathbf{P} \mathbf{P}^T)}, \quad \text{Vericide normalizasyon}$$

$$\mathbf{X}_0 = \beta \mathbf{P} \mathbf{X}, \quad \text{kanala LED'lerden iletilen sinyal}$$

Burada \mathbf{X}_0 , önkodlama uygulanmış giriş sinyalini, n_R , alıcı sayısını, \mathbf{H} 'da kestirilmiş kanal matrisini göstermektedir. Bu durumda alıcıya ulaşan alıcı sinyal vektörünün her bileşeni şu şekilde ifade edilebilir:

$$y = \beta \bar{x} + n \quad (4.12)$$

ve, $\bar{x} \sim P_{\bar{x}}(\alpha) = \frac{2}{\sqrt{\pi}} e^{-\alpha^2}, \alpha \geq 0$ ve $n \sim P_n(\alpha) = \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{\alpha^2}{2\sigma_n^2}}$ dir. $z = \beta \bar{x}$ biçiminde tanımlayarak (4.12) denklemi $y = z + n$ ve $z \sim P_z(\alpha) = \frac{2}{\sqrt{\pi\beta^2}} e^{-\frac{\alpha^2}{\beta^2}}, \alpha \geq 0$ olarak yazılabilir. Bu temel deklemleri verdikten sonra, $\bar{x} = z/\beta$ 'nin doğrusal olmayan minimum ortalama



Şekil 4.3. Kanal kestirim hatası etkisinde GLIM OFDM BER Başarımı

karesel kestirimi (NL-MMSE) aşağıdaki ilişkiden hesaplanabilir:

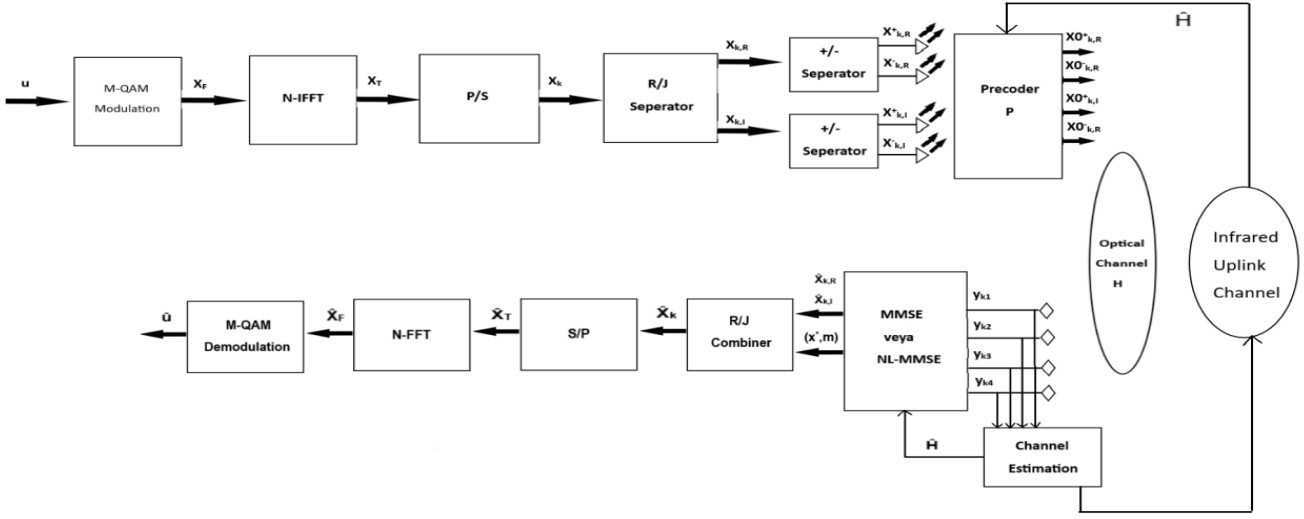
$$\hat{x}_{NL-MMSE} = \frac{1}{\beta} E\{z | y\} = \frac{1}{P_y(y)} \int_{-\infty}^{+\infty} \alpha P_{z|y}(\alpha | y) P_z(\alpha) d\alpha. \quad (4.13)$$

(4.13) denkleminin sağ tarafı geçen bölümde hesaplanmış ve (3.154) ilişkisi elde edilmiştir. Bu ilişkiyi (4.13) de yerine koyarak $\hat{x}_{NL-MMSE}$ aşağıdaki gibi tamamen analitik olarak aşağıdaki gibi elde edilir:

$$\hat{x}_{NL-MMSE} = \frac{1}{\beta} \left(\frac{se^{-\frac{y^2 P^2}{2s^2}}}{\sqrt{2\pi}(1 - Q(\frac{yP}{s}))} + yP \right). \quad (4.14)$$

GLIM-OFDM sistemine bir fiziksel katman güvenlik yeteneği kazandırmak için, tasarlanan kestirim algoritmasıyla kestirilen kanal bir infrared geribesleme linkinden vericiye iletilerek, kaynak tarafından bilgi yetkili kullanıcılara iletilmeden önce, bir önkodlayıcıdan geçirilir. Diğer bir deyişle önkodlama çıkışında kaynaktan yetkili kullanıcılara iletilen sinyal

$$\mathbf{x}_0 = \mathbf{P}\mathbf{x}$$



Şekil 4.4. Önkodlamalı GLIM-OFDM sistemin blok şeması

gibi olup, $\mathbf{P} = (\mathbf{H}^T \mathbf{H})^{-1} \mathbf{H}^T$ önkodlama matrisini göstermektedir. Bu durumda yetkili alıcılara kanalları üzerinden ulaşan sinyal genel olarak

$$\mathbf{y} = \mathbf{x} + \mathbf{n}$$

biçimine dönüşür. Kanal Kestirimi $\mathbf{x} = \beta s_q^i$ olup, s_q^i , i 'inci LED'den iletilen M-QAM simgesinin b_q 'uncu düzeyini ve β 'da vericide önkodlayıcı üzerinde yapılan bir güç normalizasyon katsayısını göstermektedir. Bu ilişkiden de görüleceği gibi, vericide kullanılan bir önkodlayıcı, farklı LED indisleri üzerinden iletilen bilgilerin alıcıda birbirlerine karışmayacak şekilde ayrışmasına ve dolayısıyla alıcının veri sezim işlem yükünün büyük oranda düşmesine neden olmaktadır. Sonuç olarak, alıcıdaki sinyal şu şekilde indirgenir.

$$y_i = \beta b_j + n_i \quad (4.15)$$

$$y_k = n_k, \quad \text{for all } k \neq i.$$

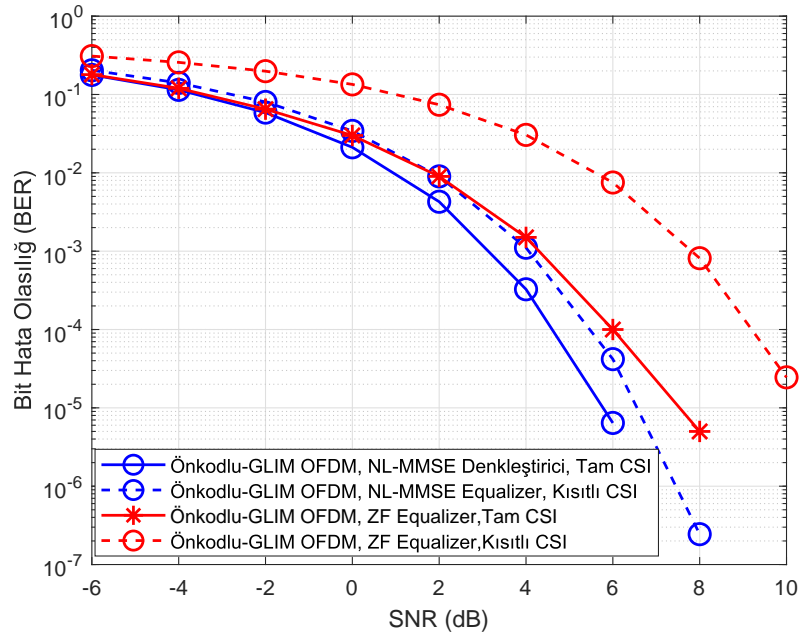
Yukarıda (4.15) ilişkisinde verilen gözlem sinyali önce optimal yapıda tasarlanmış olan NL-MMSE denkleştiricisinden geçirilerek aşağıdaki gibi \mathbf{x} 'in bir kestirimi elde edilir.

$$\mathbf{x}_{NL-MMSE} = \hat{\mathbf{H}}^{-1} \mathbf{y}.$$

Bundan sonra, alıcı iletimdeki aktif LED'lerin indislerini ve bu indislerde taşınan veri simgelerini, $\mathbf{x}_{NL-MMSE}$ vektörünün enyüksek mutlak-değerli genliklerini seçerek belirler. Son olarak, GLIM-OFDM, klasik uygulamada olduğu gibi, alıcısında bir FFT işlemiyle frekans bölgesine

geçip veri sezimini enbüyük olabilirlik (maximum likelihood (ML)) tekniği ile gerçekleştirir. Bunu izleyen paragrafta önkodlamalı GLIM-OFDM'in bit hata başarıımı (BER), alıcıda optimal NL-MMSE denkleştirici kullanılması durumunda bilgisayar incelenmekte ve sonuçlar ZF-denkleştirici kullanılması durumula karşılaştırılmaktadır.

Şekil(4.5)'de önkodlamalı GLIM OFDM'in BER başarıımı, 4-QAM veri simgelerinin üretilmesi durumunda ve alıcıda kanalın tam (perfect channel state information (CSI)) yada kısmi (imperfect channel state information (CSI)) bilinmesi ve alıcısında NL-MMSE yada ZF-denkleştirici kullanılması durumunda incelenmiştir. Şekil(4.5)'den kanalın tam olarak bilinmesi durumunda, NL-MMSE denkleştiricisi altında çalışan sistemin ZF denkleştiriciye oranla özellikle yüksek SNR değerlerinde 10 dB e varan iyileşmeler sağladığı görülmektedir. Diğer taraftan kanalın kanal kestirim hatalarından dolayı kısmı bilinmesi durumunda NL-MMSE denkleştirilici sistemin kestirim hataların çok daha az etkilendiği sonucuna varılmaktadır



Şekil 4.5. Tam ve kısıtlı CSI altında, 4QAM için önkodlamalı GLIM-OFDM BER başarıımı

5. BULGULAR

5.1. Geliştirilen PLS Yetenekli ve MIMO SSK Tabanlı VLC Sistemin Bilgisayar Benzetimleri

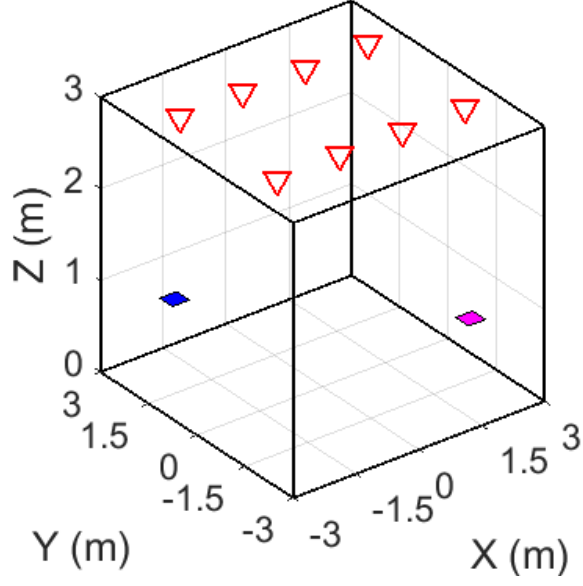
Bu bölümde, önerilen farklı PLS-VLC senaryoları için bilgisayar benzetimleriyle yasal kullanıcıların ve Eve'in bit hata(BER) başarımları incelenmektedir. Yapılan benzetimler için VLC'in 6 m ×6 m ×3 m boyutlarında bir içmekanda gerçekleştiği varsayılmaktadır ve erişim noktası(access point), bu içmekanın tavanında yerleştirilen toplam $N_t = 8$ LED'den oluşmaktadır. Bu LEDler,

$$\text{LED}_{\text{koor}}(x, y) = \begin{bmatrix} -2.25, -0.75, 0.75, 2.25, -2.25, -0.75, 0.75, 2.25 \\ 1.5, 1.5, 1.5, 1.5, -1.5, -1.5, -1.5, -1.5 \end{bmatrix}^T \text{ m},$$

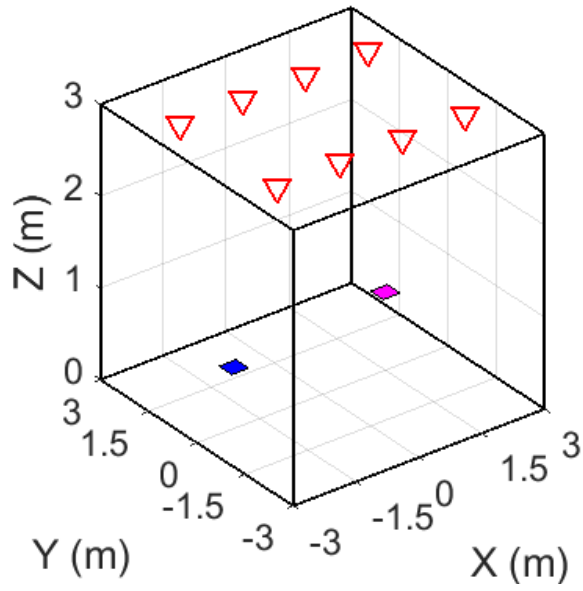
iki-boyutlu koordinat matrisine göre dizilmiş olup, koordinatlar metre cinsinden verilmiştir. Gözönüne alınan her senaryoda yasal kullanıcıların ve Eve'in koordinatları farklı olup, kanal durum katsayıları, aşağıdaki parametreler kullanılarak (3.1) ilişkilerien göre hesaplanmıştır.

$$\Phi_{1/2} = 60^\circ, \quad \Psi_{1/2} = 70^\circ, \quad A_{\text{PD}} = 1 \text{ cm}^2. \quad (5.1)$$

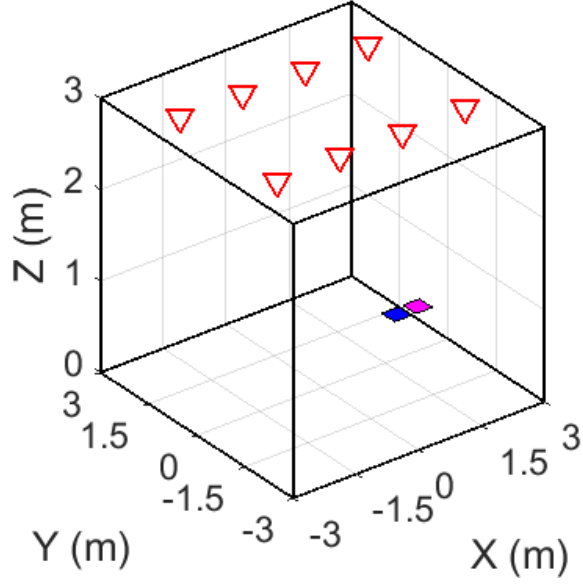
Diğer kanal parametreleri olan $\beta, d_k^{r,t}, \phi_k^{r,t}, \theta_k^{r,t}$ ise LED'lerin, kullanıcıların ve Eve'in yer ve yön bilgileri kullanılarak bulunmuştur. Ayrıca, bir LED'in emisyon gücü 1 W olarak belirlenmiştir. Benzetimlerde, kanal kullanımı başına $N_a = 4$ LED aktive edilmekte ve $K = 2$ yetkili kullanıcıyla haberleşme yapılmaktadır. Tüm alıcılarda $N_r = 2$ adet PD kullanılmaktadır. Kanal kullanımı başına yollanabilen bit miktarı, (3.4) denklemine göre $N_B = 6$ bit olarak bulunur. Bu toplam bit sayısı, yetkili kullanıcılar arasında eşit olarak bölünmüş ve kullanıcıların alfabesindeki sembol sayısı $M = 2^{N_B/2} = 8$ olarak bulunmuştur. Böylece, \mathcal{C}_1 ve \mathcal{C}_2 kümelerinin eleman sayısı $M = 8$ olup her eleman $N_B/2 = 3$ bit uzunluğunda bir bit vektörü olur. Ortak sembol alfabeti, $\mathcal{C}_S, \mathcal{C}_1$ ve \mathcal{C}_2 kümelerin Kartezyen çarpımı olduğundan, \mathcal{C}_S alfabeti, $N_B = 6$ bit uzunluğunda $n^2 = 64$ adet vektörden oluşur. $N_r = 2$ and $M = 8$ olduğundan, \mathcal{V}_1 ve \mathcal{V}_2 alınmış uzaysal sinyal kümesi, 8-QAM sembollerden seçilmiştir. Her kanal kullanımında, \mathbf{b}_{1,i_1} ve \mathbf{b}_{2,i_2} vektörleri \mathcal{C}_1 ve \mathcal{C}_2 kümelerinden raslantısal biçimde seçilir ve onların ortak bit vektörü olan $\mathbf{b}_{S,s}$ \mathcal{C}_S kümesinden bulunur. Sonrasında, sinyal genliği ρ için eniyi ışık şiddeti vektörü $\tilde{\mathbf{q}}_{S,s}$, (3.20) denklemine göre hesaplanır. En sonunda, oluşturulan GSSK sinyali, tüm kullanıcılar tarafından (3.12) denklemine göre algılanır.



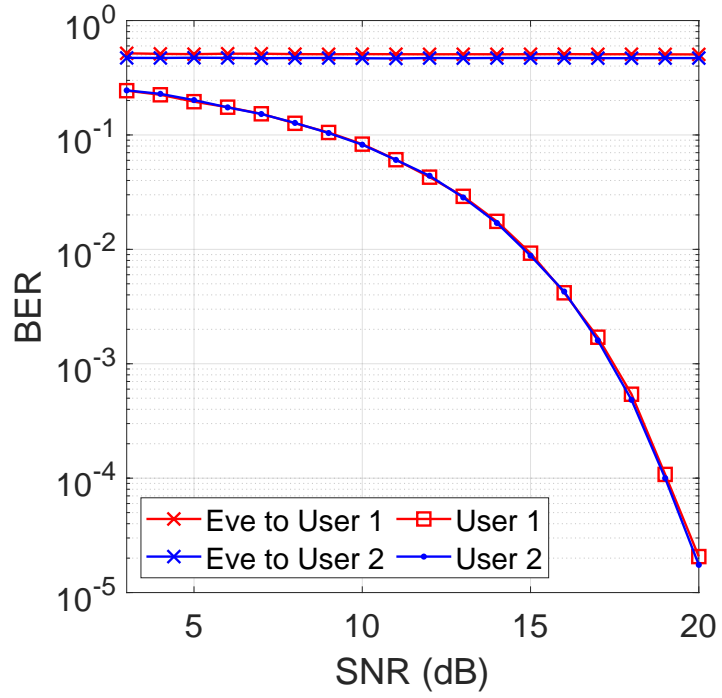
Şekil 5.1. Ele alınan MIMO-VLC kullanıcı konfigürasyonlarından Senaryo 1.



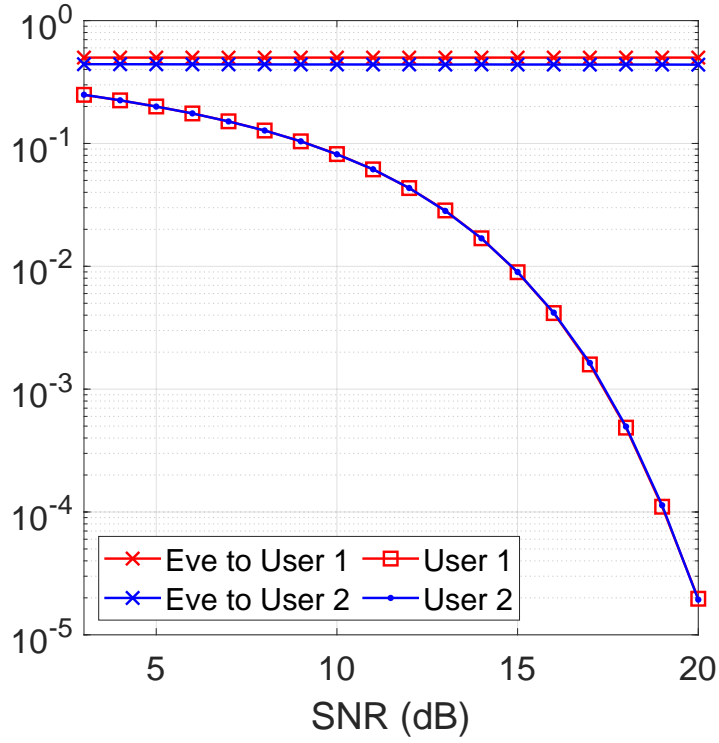
Şekil 5.2. Ele alınan MIMO-VLC kullanıcı konfigürasyonlarından Senaryo 2.



Şekil 5.3. MIMO-VLC kullanıcı konfigürasyonlarından Senaryo 3.



Şekil 5.4. Senaryo 1'de elde edilen BER eğrileri. Eve'in lokasyonu, [-1, 1, 0.85] olarak seçilmiştir.



Şekil 5.5. Senaryo 1'de elde edilen BER eğrileri. Eve'in lokasyonu, $[0, 0, 0.85]$ olarak seçilmiştir.

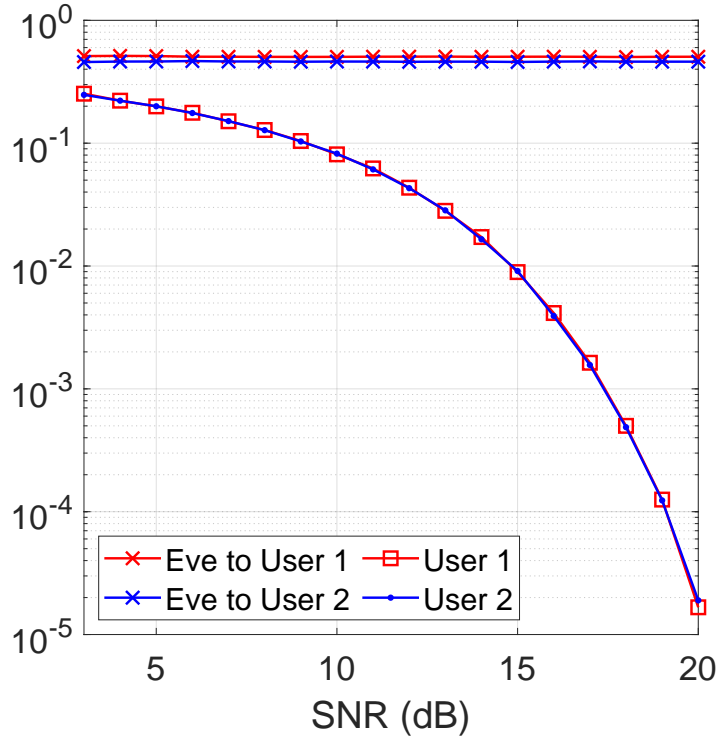
5.1.1. *İdeal CSI ile MU-GSSK-SCD altında BER başarımı*

Şekil 5.1'da verilen ilk senaryoda, kullanıcılar içmekanın zıt köşelerinde, tam olarak $[-2, 2, 0.85]$ ve $[2, -2, 0.85]$ koordinatlarında yer almaktadır. Bu senaryoda Eve üç farklı noktaya yerleştirilmiştir, bunlar *a)* Kullanıcı 1'e daha yakın, *b)* iki kullanıcının tam ortasında, *c)* Kullanıcı 2'ye daha yakın, olarak seçilmiştir. Her üç durum için üretilen BER eğrileri Şekil 5.4, 5.5, 5.6'de sırayla gösterilmiştir. Tüm BER grafiklerinde, dört eğri üretilmiştir. Bunlardan ikisi, Kullanıcı 1 ve 2'ye aittir. Eve'in başarımı ise Kullanıcı 1'i ve Kullanıcı 2'yi ayrı ayrı dinlediği varsayılarak iki farklı eğriyle gösterilmiştir.

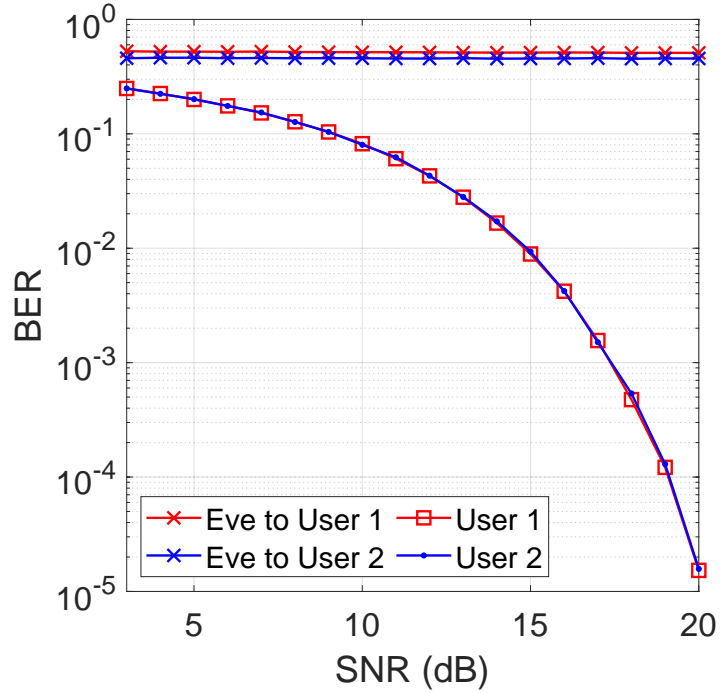
Şekil 5.7, 5.8, 5.9, 5.10, 5.11, 5.12'te sırayla Senaryo 2 ve Senaryo 3'te üretilen BER başarımları gösterilmiştir. Senaryo 2'de, yetkili kullanıcılar x eksenine paralel yerleştirilmiş, Senaryo 3'te ise birbirlerine çok yakın konumlandırılmışlardır.

5.1.2. *MU-GSSK-SCD sistem tasarımı üzerine değerlendirmeler*

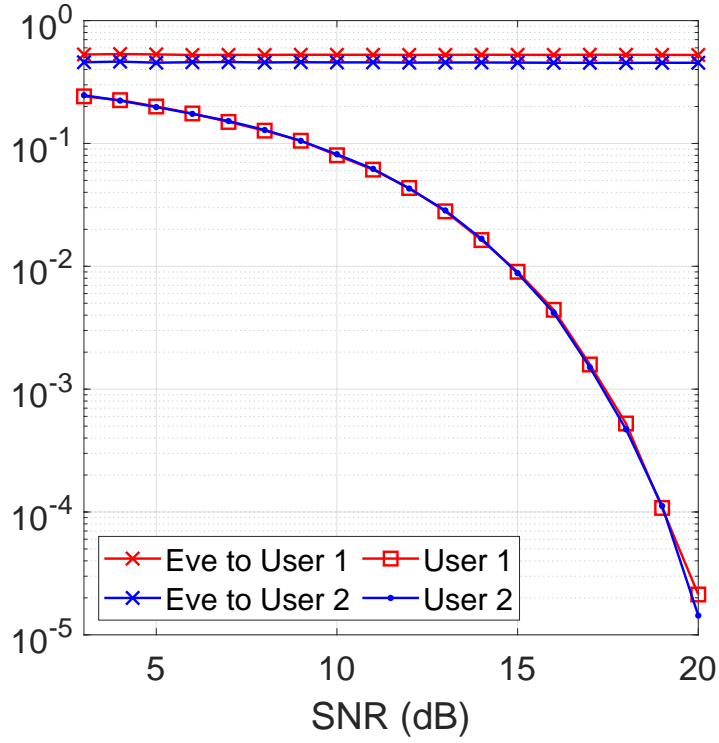
Bu bölümde, önerdiğimiz sistemin tasarımıyla ilgili bir öngörü oluşturmak için, kullanıcıların alıcı anten sayısı ve Eve'in içmekanda bulunduğu noktayı daha da fazla çeşitlendirerek,



Şekil 5.6. Senaryo 1'de elde edilen BER eğrileri. Eve'in lokasyonu, $[1, -1, 0.85]$ olarak seçilmiştir.



Şekil 5.7. Senaryo 2'de elde edilen BER eğrileri. Eve'in lokasyonu $[-1.5, -0.375, 0.85]$ olarak seçilmiştir.



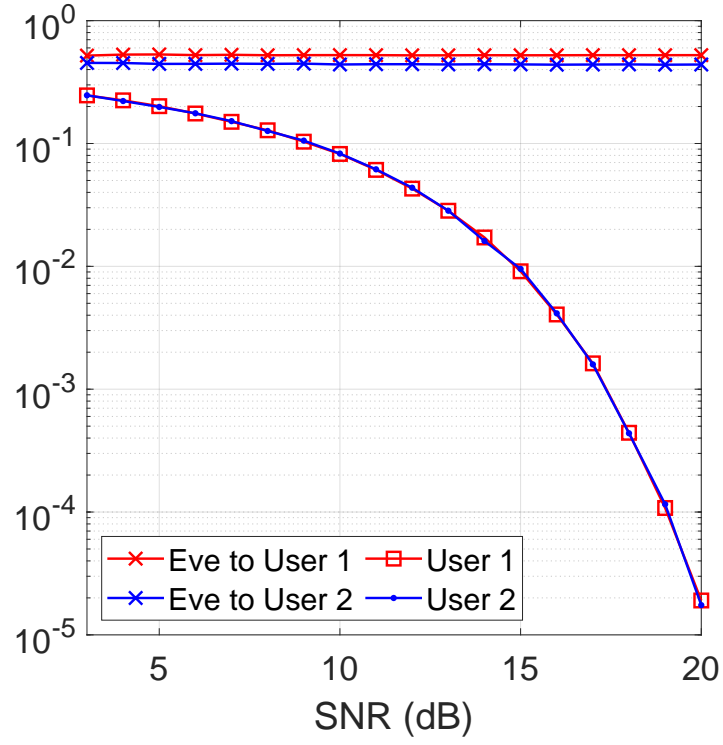
Şekil 5.8. Senaryo 2'de elde edilen BER eğrileri. Eve'in lokasyonu, [-0.5, -0.25, 0.85] olarak seçilmiştir.

BER başarımlarına etkilerini inceleyeceğiz. Bu amaçla, Şekil 5.13, 5.14, 5.15 ve 5.16'de gösterilen BER başarımlarını üretilmiştir. Bu sonuçlar, Eve içmekandaki Kartezyen koordinatı üzerinde hareket ederken Monte Carlo benzetimleriyle üretilmiştir. Şekil 5.13 ve 5.14, sırayla Eve'in Kullanıcı 1 ve Kullanıcı 2'yi dinlerken elde ettiği BER başarımlarını göstermektedir. Bu iki şekilde, kırmızı kareciklerle gösterilen yetkili kullanıcılar birbirlerine görece uzak olacak şekilde konumlandırılmışlardır. Eve'in BER seviyesi renge eşlenmiştir ve bu eşleme şekillerin yanındaki renk barıyla gösterilmiştir.

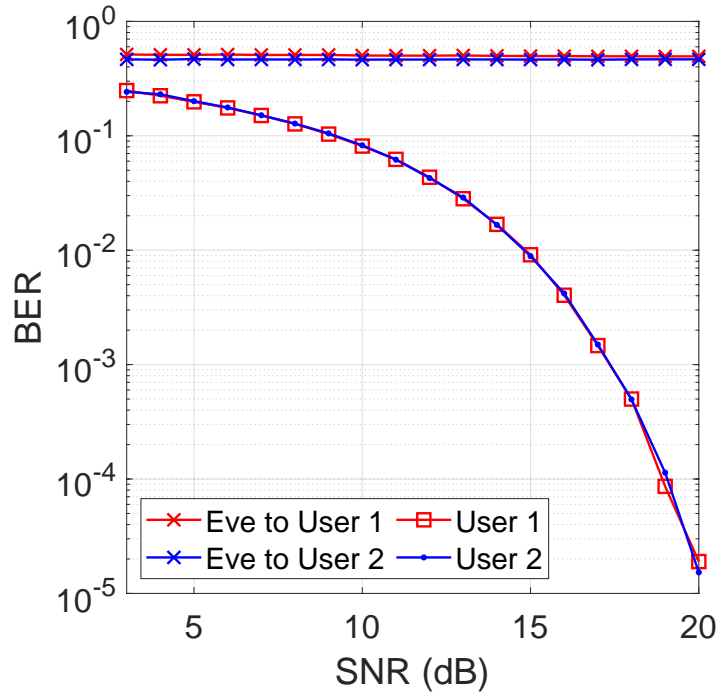
5.1.3. İdeal olmayan CSI ile MU-GSSK-SCD BER başarımları

Bir önceki bölümde, vericinin doğru olarak CSI bilgisine sahip olması durumunda, MU-GSSK-SCD'in içmekan VLC sistemindeki yetkili kullanıcılara çok iyi BER başarımları sağladığını gözlemledik. Ancak, gerçek uygulamalarda kanal durum katsayıları her zaman tam ve doğru olarak bilinmiyebilir. Bu nedenle, önerilen PLS çözümünün kanal kestirim hatalarına karşı duyarlılığının da analiz edilmesi gerekir. Yasal kullanıcılar tarafından alınmış olan sinyaller, (3.13) ilişkisinden hareketle

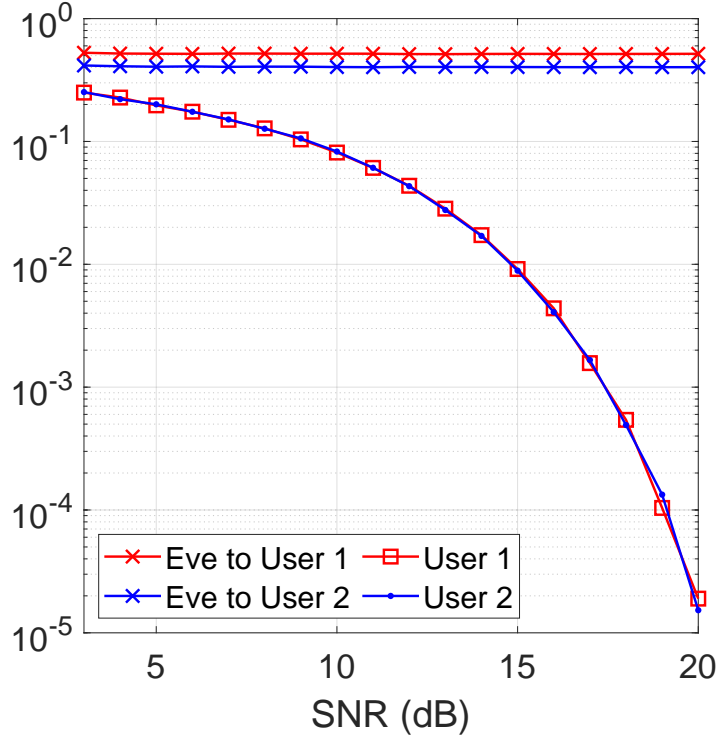
$$\mathbf{y}_k = \rho \mathbf{G} \mathbf{v}_{k,i_k} + \mathbf{n}_k, \quad k = 1, 2, \dots, K, \quad (5.2)$$



Şekil 5.9. Senaryo 2’de elde edilen BER eğrileri. Eve’in lokasyonu, $[0.5, -0.125, 0.85]$ olarak seçilmiştir.



Şekil 5.10. Senaryo 3’te elde edilen BER eğrileri. Eve’in lokasyonu, $[1.125, -1, 0.85]$.



Şekil 5.11. Senaryo 3'te elde edilen BER eğrileri. Eve'in lokasyonu, $[1.25, -1, 0.85]$ olarak seçilmiştir.

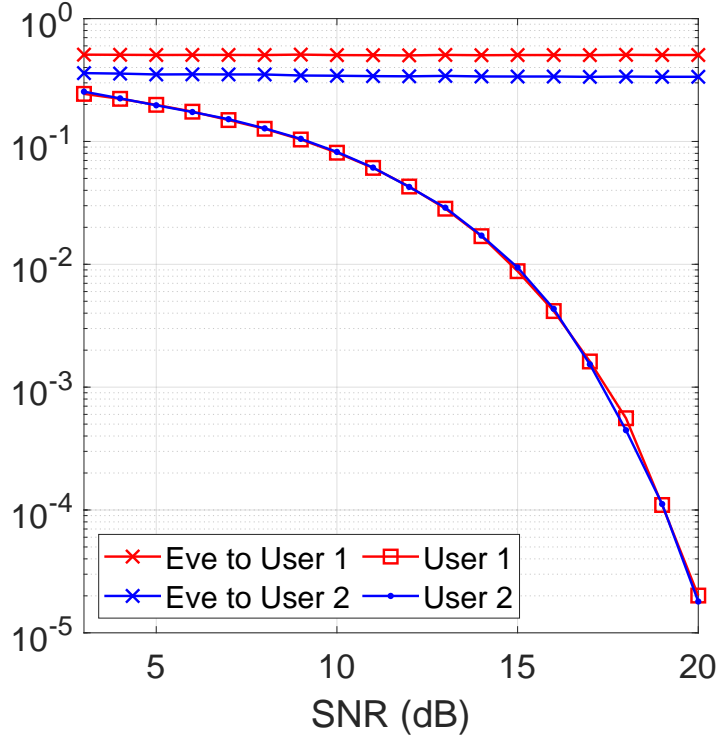
şeklinde ifade edilebilir. Kanal Kestirimi $\mathbf{G} \in \mathcal{R}^{KN_r \times KN_r}$, $\mathbf{G} = \tilde{\mathbf{H}} \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} \right)^{-1} \tilde{\mathbf{H}}^T$ şeklinde tanımlanmıştır. Bir önceki bölümde açıklandığı gibi, ρ parametresi, kanal durum katsayılarına doğrusal olmayan bir şekilde bağlıdır ve alıcı tarafında tam doğru kestirilmesi için kullanıcılarındaki CSI bilgisi tam doğru olmalıdır. Ayrıca, Bölüm 3.1.1'de anlatıldığı gibi, vericide tam doğru CSI olması durumunda, \mathbf{G} bir birim matris olur. Aşağıda, CSI'nin kullanıcılarda tam doğru olarak bilinmemesi durumunda bile, alıcıdaki optimum bilgi sezimlemesinin bu ideal olmayan durumdan etkilenmediğini gösterilmektedir:

Kanal durum matrisi \mathbf{H} 'nin alıcıda bir hata matrisi \mathbf{E} farkıyla kestirildiğini varsayalım. Bu durumda, kestirilen kanal dmatrisi $\hat{\mathbf{H}}$, hatasız kanal matrisi \mathbf{H} cinsinden Burada ifade edilebilir.

$$\mathbf{H} = \hat{\mathbf{H}} + \mathbf{E}.$$

Bu ifadeyi, \mathbf{G} ifadesinde yerine konursa,

$$\hat{\mathbf{G}} = (\hat{\mathbf{H}} + \mathbf{E}) \left((\hat{\mathbf{H}} + \mathbf{E})^T (\hat{\mathbf{H}} + \mathbf{E}) \right)^{-1} (\hat{\mathbf{H}} + \mathbf{E})^T = \mathbf{I}_{2N_r}, \quad (5.3)$$



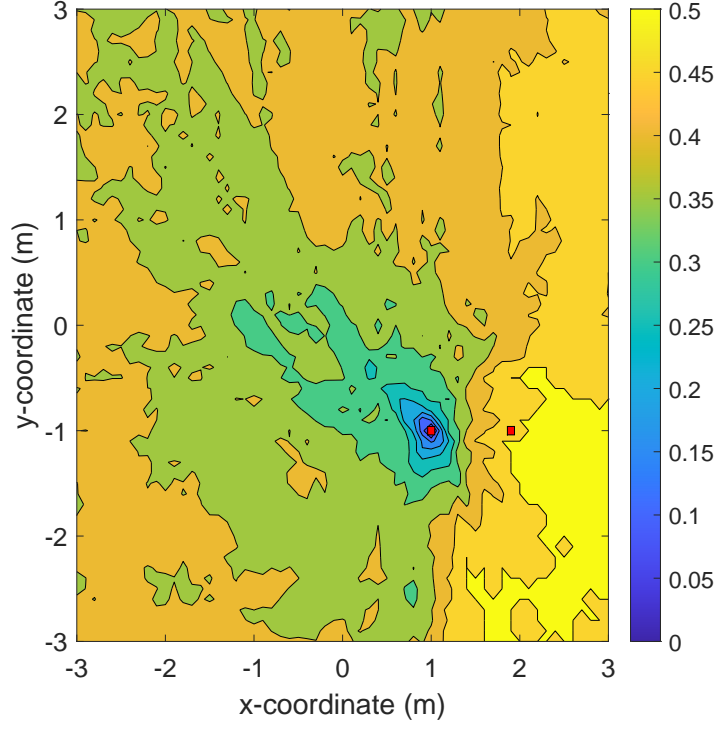
Şekil 5.12. Senaryo 3'te elde edilen BER eğrileri. Eve'in lokasyonu, [1.375, -1, 0.85] olarak seçilmiştir.

elde edilir. Sonuçta, yollanan \mathbf{v}_{k,i_k} sinyali, alınmış olan $\mathbf{y}_k = \rho \mathbf{v}_{k,i} + \mathbf{n}_k$ sinyaline ML sezimlemesi uygulanmasıyla optimum şekilde çıkartılabilir. Ancak, ρ 'nun gerçek değeri, k 'inci kullanıcıda tam olarak bilinmeyebilir, bu yüzden alınmış sinyal \mathbf{y}_k kullanılarak olabildiğince doğru kestirilmesi gerekir. Bu kestirme işlemi için, verici tarafından belli sayıda GSSK pilot sembolünden yararlanılabilir. Bunu izleyen bölümde, ρ 'nun ML kuralıyla kestirilmesi açıklanmaktadır.

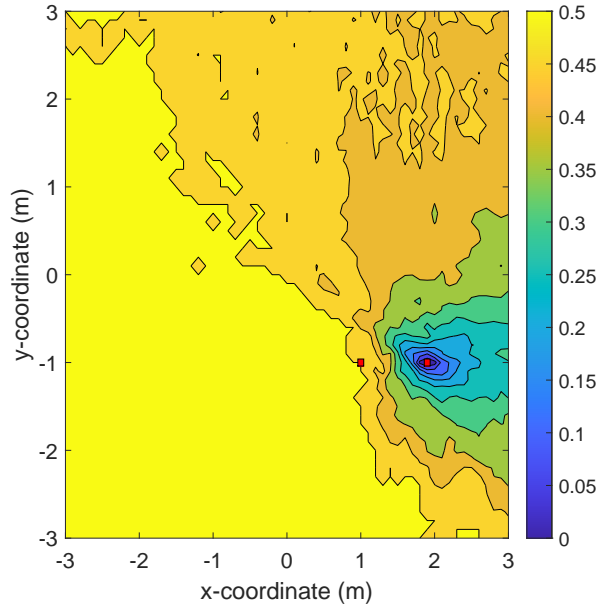
5.1.3.1. ρ 'nun ML kestirimi. Işık şiddeti normalizasyon katsayısı ρ , ortak sembol alfabeti \mathcal{C}_S 'ten seçilmiş pilot semboller, $\mathbf{s}_p = [\mathbf{s}_{p,1}^T, \mathbf{s}_{p,2}^T, \dots, \mathbf{s}_{p,K}^T]^T$, aracılığıyla, k 'inci kullanıcıda kestirilebilir. ρ parametresi için olasılık fonksiyonu, pilot sembollerin birbirinden bağımsız ve eş dağılmış olması nedeniyle

$$\hat{\ell}(\rho; \mathbf{y}_k) = \frac{1}{N_p} \sum_{\ell=1}^{N_p} \ln f(\mathbf{y}_{k,\ell} | \rho), \quad (5.4)$$

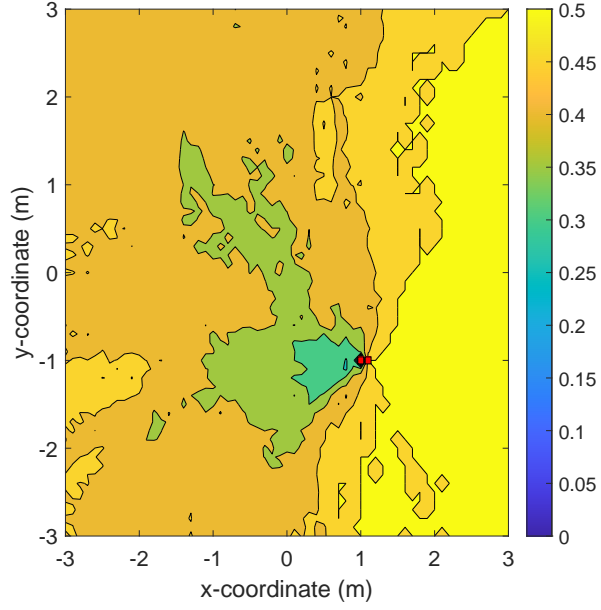
şeklinde ifade edilebilir. Kanal Kestirimi, $\mathbf{y}_{k,\ell}$ sinyali, k 'inci kullanıcının aldığı pilot sembollerden ℓ 'inci olanı göstermektedir. Tüm $\ell = 1, 2, \dots, N_p$ değerleri için $\mathbf{y}_{k,\ell}$ sinyalinin, ρ 'ya



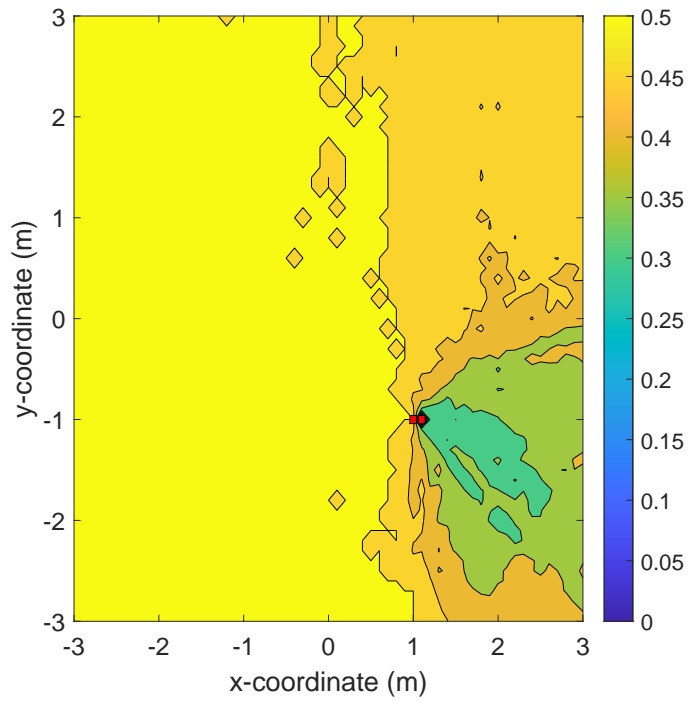
Şekil 5.13. Eve içmekanda yer değiştirirken ve Kullanıcı 1'i dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.9, -1] koordinatlarındadır. Tüm birimler metredir.



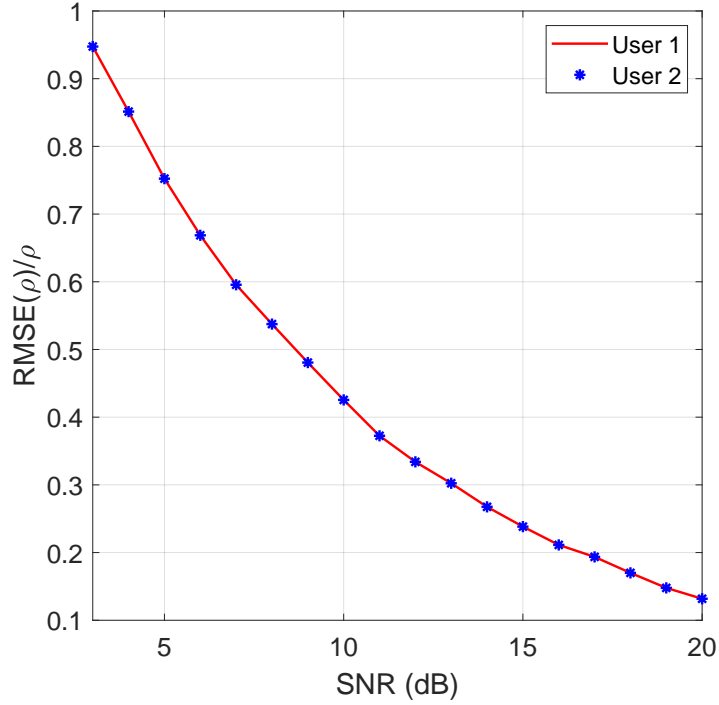
Şekil 5.14. Eve içmekanda yer değiştirirken ve Kullanıcı 2'yi dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.9, -1] koordinatlarındadır. Tüm birimler metredir.



Şekil 5.15. Eve içmekanda yer değiştirirken ve Kullanıcı 1'i dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.1, -1] koordinatlarındadır. Tüm birimler metredir.



Şekil 5.16. Eve içmekanda yer değiştirirken ve Kullanıcı 2'yi dinlerken elde edilen BER başarımı. Kullanıcı 1 lokasyonu [1, -1]. Kullanıcı 2 ise [1.1, -1] koordinatlarındadır. Tüm birimler metredir.



Şekil 5.17. Senaryo 1’de kullanıcılarda kusurlu CSI varken, kestirim hatası olan $\|\rho - \hat{\rho}\|$ ifadesinin RMSE değerleri.

koşullu olasılık yoğunluğu fonksiyonu (pdf) $f(\mathbf{y}_{k,\ell}|\rho)$, (3.19) denklemi kullanılarak

$$\ln f(\mathbf{y}_{k,\ell}|\rho) = \ln \left(\frac{(2\pi)^{N_r/2}}{|\mathbf{C}_{\mathbf{n}_k}|^{1/2}} \right) - \frac{\|\mathbf{y}_{k,\ell} - \rho \mathbf{s}_p\|^2}{2},$$

şeklinde bulunur. Eniyi ρ katsayısı, (5.4) ifadesini enbüyükleme sonucunda aşağıda verildiği gibi ρ 'nun ML kestirimi olarak bulunur.

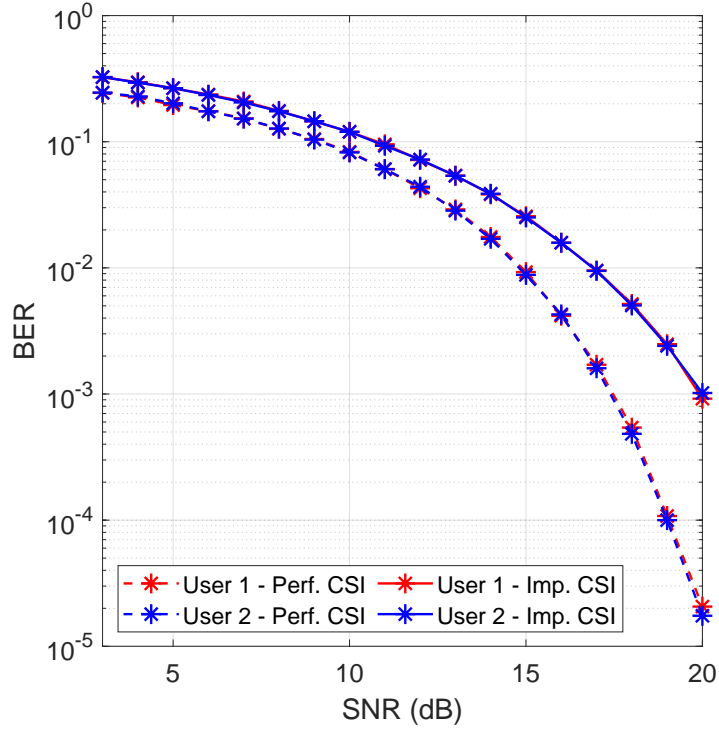
$$\hat{\rho} = \arg \max_{\rho} \{\hat{\ell}(\rho; \mathbf{y}_k)\} = \frac{1}{N_p} \sum_{\ell=1}^{N_p} \frac{\mathbf{y}_{k,\ell}^T \mathbf{s}_p}{\mathbf{s}_p^T \mathbf{s}_p}, \quad (5.5)$$

Kestirim doğruluğu,

$$\text{RMSE}(\hat{\rho}) = \frac{1}{N_p} \sum_{\ell=1}^{N_p} \|\rho - \hat{\rho}\|^2, \quad (5.6)$$

şeklinde ifade edilen $\rho - \hat{\rho}$ hatasının ortalama karekökü (RMSE) ile ölçülür.

Aşağıda, MU-GSSK-SCD tekniği, ideal olmayan CSI bilgisi altında, Şekil 5.1’deki Senaryo 1 ile gösterilen 2 kullanıcıli bir sisteme uygulanmaktadır. Her SNR değeri için,

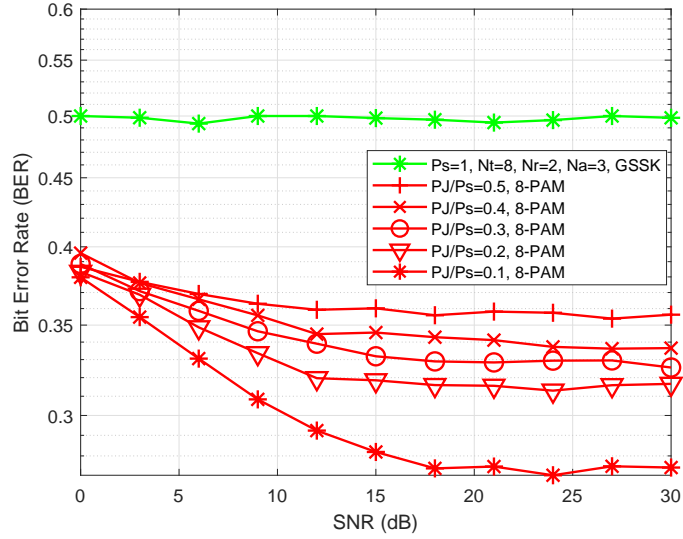


Şekil 5.18. Senaryo 1’de kullanıcılarda kusurlu CSI varken elde edilen, değişen SNR’a göre BER eğrileri.

kullanıcılar erişim noktasından iletilen $N_p = 1000$ pilot sembolü yardımıyla (5.5) denkleme göre ρ 'yu kestirmektedir. Şekil 5.17’de, $\hat{\rho}$ için elde edilen RMSE değerleri normalize edilerek sunulmuştur. Önerilen sistemin BER başarımı, kestirilen ρ değerleriyle bulunmuş ve Şekil 5.18’de sunulmuştur. Bu şekilde, kullanıcıların tam doğru CSI’a sahip olduğu durumda elde edilen BER başarımları kesik eğrilerle gösterilmiştir. Bu durumda ρ , kullanıcı tarafında tam doğru olarak kestirilebilmiş ve RMSE sıfır olmuştur.

5.1.4. MU-GSSK-SCD’nin Literatürle Kıyaslanması

Bu bölümde, önerilen MU-GSSK-SCD stratejisini, üzerinde oldukça yoğun araştıma yapılan, dost karıştırıcı (friendly jamming) yöntemiyle kıyaslanmaktadır. Kıyas için kullanılan dost karıştırıcı yöntemi için DC öngerilim verilmiş, 8 seviyeli darbe genlik modülasyonu (8-PAM) kullanılmıştır. Bilgi, alıcıda DC öngeriliminin çıkarılması sonrası klasik ML sezimlemesiyle elde edilmiştir. Karışıma sinyali, yine verici tarafından birden fazla LED kullanılarak, yollanan bilgi kullanılmadan üretilmiştir. Vericide Eve’e ait olan kanal durum bilgisinin tam doğru olarak bilindiği varsayımıyla, yalnızca Eve’in aldığı sinyali bozacak bir karıştırma sinyali tasarlanmıştır. Bu sayede Eve’in BER başarımı kötü etkilenmektedir. Diğer yandan, karıştırıcı sinyali vericinin enerji bütçesinden harcanmaktadır. Bu 8-PAM’lu dost karıştırıcıya dayalı PLS sisteminde, kıyaslanan yöntemler arasında eşitlik sağlanması amacıyla, gönderilen sinyalin gücü 1’e ayarlanmıştır.



Şekil 5.19. 8-PAM ve MU-GSSK-SCD için Eve'in BER vs. SNR eğrileri. Tüm eğrilerde, spektral verimlilik kullanıcı başına 3 bit/s/Hz olarak seçilmiştir.

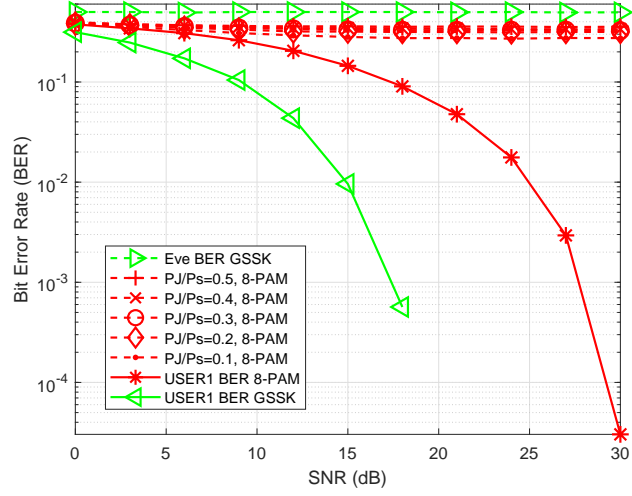
Şekil 5.19'de, bu strateji, bizim önerdiğimiz MU-GSSK-SCD yöntemiyle, aynı haberleşme kanalı ve parametreleri kullanılarak, BER başarımları açısından kıyaslanmıştır. Her iki VLC sistemi, verici tarafında $N_t = 8$ LED ile donatılıp, 3 bit/s/Hz spektral verimlilik ile çalıştırılmıştır. Her iki sistemde gönderilen sinyal enerjisi 1 olacak şekilde ayarlanmıştır. Şekil 5.19'de gösterilen 8-PAM dost-karıştırcılı sistemine ait olan her BER eğrisi için, gönderilen sinyal gücünün belirtilen oranı kadar olan kısmı, Eve'e karıştırma sinyali yollamak için kullanılmıştır. Şekil 5.20 ise yetkili kullanıcıların her iki sistem altında elde ettiği BER başarımlarını kıyaslamaktadır.

5.2. VLC'de MIMO SSK Tekniğine Dayanan PLS Algoritmasının Gizlilik Oranlarının (Secrecy Rates) Belirlenmesi

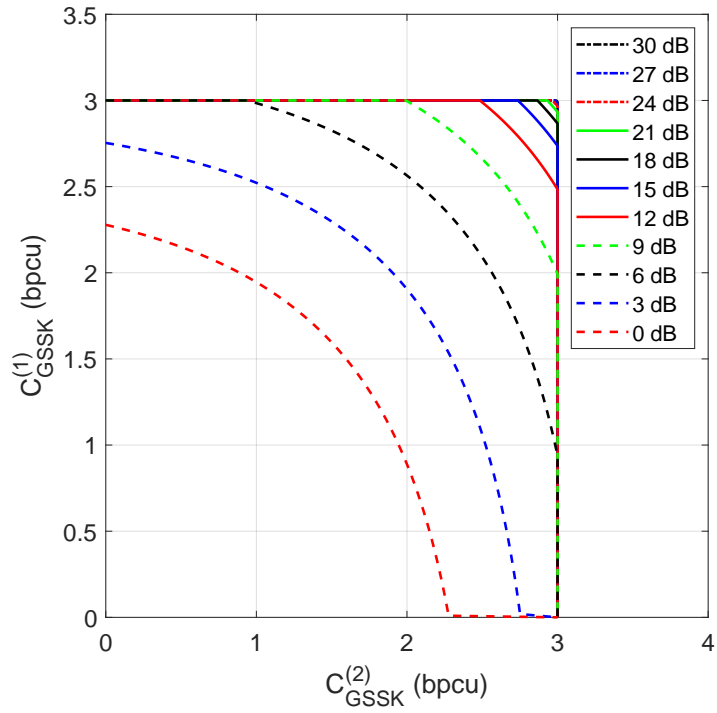
5.2.1. Bilgisayar Benzetim Sonuçları

Bu bölümde, önerilen MU-GSSK-SCD için (3.37) ve (3.38) denklemlerinde tanımlanan gizlilik oranı bölgeleri, kullanıcıların farklı konumları için bulunmuştur.

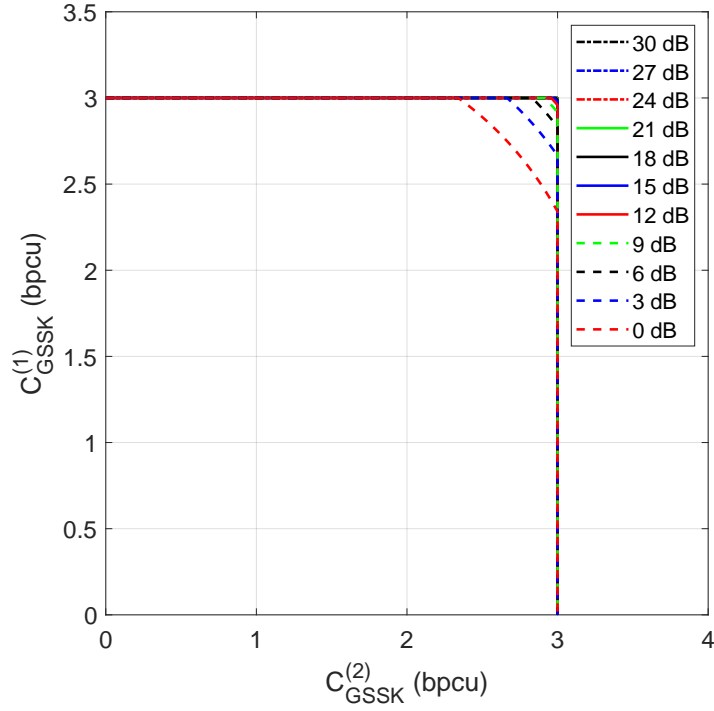
İlk olarak, iki kullanıcı 30 cm aralıklı olacak şekilde $[1, -1, 0.85]$ ve $[1.3, -1, 0.85]$ pozisyonlarında, Eve ise kullanıcıların tam ortasına konumlandırılmıştır. Bu konfigürasyona ait gizlilik oranı bölgeleri Şekil 5.21 ile sunulmuştur. Başka bir konfigürasyonda ise kullanıcılar $[1, -1, 0.85]$ ve $[1.9, -1, 0.85]$ koordinatlarında, Eve ise kullanıcılardan birine daha yakın olacak şekilde $[1.15, -1, 0.85]$ koordinatında konumlandırılmıştır. Bu konfigürasyon için bulunan



Şekil 5.20. 8-PAM ve MU-GSSK-SCD için Bob ve Eve'in BER vs. SNR eğrileri. Tüm eğrilerde, spektral verimlilik kullanıcı başına 3 bit/s/Hz olarak seçilmiştir.



Şekil 5.21. Kullanıcılar arasındaki mesafe 30 cm iken elde edilen gizlilik oranı bölgeleri.



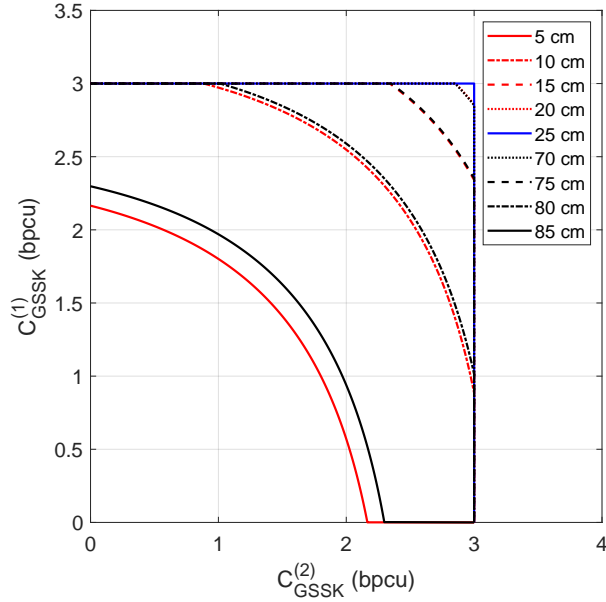
Şekil 5.22. Kullanıcılar arasındaki mesafe 90 cm iken elde edilen gizlilik oranı bölgeleri.

gizlilik oranı bölgeleri, Şekil 5.22 ile sunulmuştur. Şekil 5.23'de, MU-GSSK-SCD tekniğiyle elde edilen gizlilik başarımı, Şekil 5.22'deki konfigürasyon için 0 dB SNR seviyesinde tekrar sunulmuştur. Bu şekilde, Eve Kullanıcı 1'den Kullanıcı 2'ye doğru hareket etmekte ve belirli uzaklıklarda gizlilik oranı bölgeleri bulunmaktadır. Bu senaryo için, Eve'in herhangi bir kullanıcıya minimum uzaklığı, x değişkeni Eve'in Kullanıcı 1'e olan uzaklığını göstermek üzere, $\min\{x, 90 - x\}$ cm olarak bulunur.

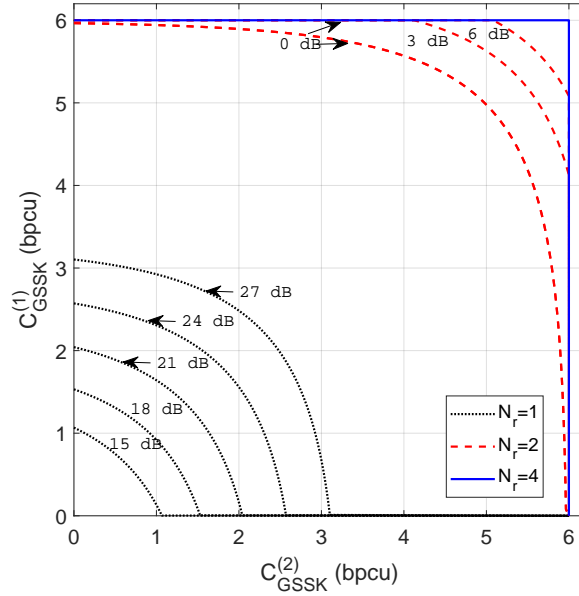
Son olarak, Şekil 5.24'de, yetkili kullanıcılarda ve Eve'de $N_r \in \{1, 2, 4\}$ adet alıcı PD kullanıldığında ve önerilen MU-GSSK-SCD stratejisi benimsendiğinde, ulaşılan gizlilik oranı bölgelerini sunulmaktadır. Bu sistemde $N_t = 16$ ve $N_a = 8$ alınmış ve her kanal kullanımında her kullanıcıya 6 bit yollanabilmesine olanak sağlanmıştır.

5.3. Geliştirilen PLS Yetenekli ve MIMO-NOMA Tabanlı VLC Sistemin Bilgisayar Benzetimleri

Bu bölümde, MIMO-NOMA-VLC için geliştirdiğimiz PLS algoritması altında, yetkili kullanıcılarda ve Eve'de gerçekleşen bit hata oranı (bit error rate (BER)) oranlarını sunuyoruz. BER benzetimleri için haberleşmenin $6 \text{ m} \times 6 \text{ m} \times 3 \text{ m}$ boyutlarında bir iç mekanda gerçekleştiği varsayılmaktadır. Bu mekanın tavanında, $N_t = 8$ adet verici LED konumlandırılmıştır.



Şekil 5.23. Eve Kullanıcı 1'den Kullanıcı 2'ye doğru hareket ederken, elde edilen gizlilik oranı bölgeleri. Tüm eğrilerde SNR, 0 dB alınmıştır.



Şekil 5.24. MU-GSSK-SCD stratejisiyle elde edilen gizlilik oranı bölgeleri. Verici ve aktive edilen anten sayısı sırayla $N_t = 16$, $N_a = 8$ olup N_r çeşitlendirilmiştir.

LED koordinatları,

$$\text{LED}_{\text{coord}}(x, y, z) = \begin{bmatrix} -2.25, -0.75, 0.75, 2.25, -2.25, -0.75, 0.75, 2.25 \\ 1.5, 1.5, 1.5, 1.5, -1.5, -1.5, -1.5, -1.5 \\ 3, 3, 3, 3, 3, 3, 3, 3 \end{bmatrix}^T \text{ m,}$$

Tablo 5.1. Kullanıcı yerleşimleri

	Kullanıcı 1	Kullanıcı 2	Eve	α
Senaryo 1	[-1, 1, 0.85]	[1, -1, 0.85]	[0, 0, 0.85]	0.49
Senaryo 2	[-1.5, 1, 0.85]	[0, 1, 0.85]	[1, -1, 0.85]	0.51
Senaryo 3	[0, 0, 2]	[3.1, 3.1, 0.3]	[1.55, 1.55, 1.15]	0.21

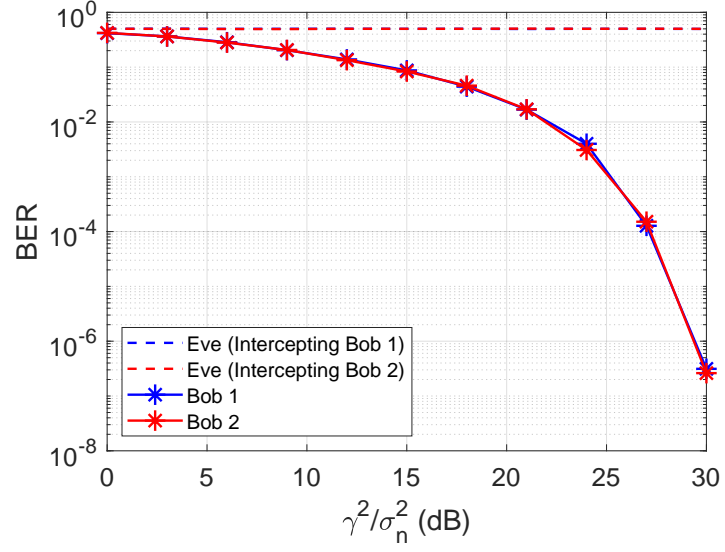
olarak esas alınmıştır. Kanal Kestirimi, x ve y yatay eksenleri, z ise dikey eksenini simgelemektedir. Yasal kullanıcılar, Tablo 5.1'de gösterildiği gibi 3 farklı senaryoya göre konumlandırılmıştır. Eve dahil tüm kullanıcıların alıcı birimleri birbirinden 3 santimetre uzaklıkta bulunan $N_r = 4$ adet PD ile donatılmıştır. LED'lerin yarı gücü ve yarı açısı ile PD'lerin alanlarının

$$\Phi_{1/2} = 60^\circ, \quad \Psi_{1/2} = 70^\circ, \quad A_{PD} = 1 \text{ cm}^2, \quad (5.7)$$

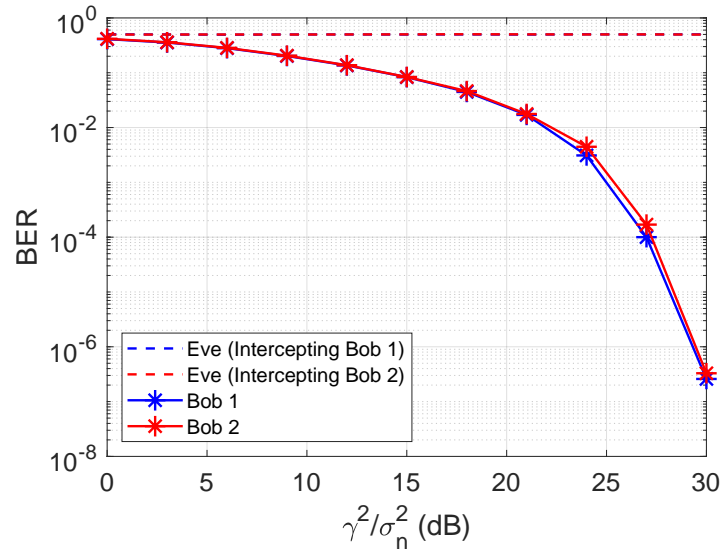
Kanal parametrelerinin geri kalanı, PD'lerin ve LED'lerin konumları ve yönelimleri kullanılarak bulunur. Daha sonra, tüm LED'ler ve PD'ler arasındaki VLC kanal katsayıları (3.1)'e göre bulunur ve her kullanıcı yerleşimi için (3.58)'a göre α oranı bulunur. MIMO-NOMA-VLC sistemi, yukarıda verilen ayrıntılara göre bilgisayar ortamında oluşturulmuş, ve önerilen PLS önkodlayıcı uygulanmıştır. Ayrıca, \tilde{S}_1 ve \tilde{S}_2 için 8-PAM sinyal takımsembol kullanılmıştır. Senaryo 1 ve 2 için BER başarımları sonuçları, sırasıyla Şekil 5.25 ve 5.26'de sunulmaktadır. Bu iki senaryoda, yasal kullanıcıların Alice'e benzer mesafeler ve açılarla konumlandırıldığından ve ortalama kanal kazançları benzer olmuştur. Bu nedenle, β_1 ve β_2 katsayıları da (3.48)'ya göre benzerdir ve dolayısıyla Tablo 5.1'da gösterildiği gibi $\alpha \approx 0,5$ elde edilmiştir. Ardından, Senaryo 3 için BER başarımları Şekil 5.27'de sunulmaktadır. Senaryo 3'te, Bob 1'in Bob 2'ye göre Alice'e çok daha yakın konumlanmıştır. Bu nedenle, Bob 1'in ortalama VLC kanal kazancı Bob 2'ninkinden daha büyüktür. Bu da $\alpha < 0,5$ 'a yol açar. Bundan dolayı, Bob 1'e, (3.62)'e göre sinyal gücünün daha küçük bir kısmı tahsis edilir. İlgili sonuçlar Şekil 5.27'de gösterilmiştir. PD sayısının BER başarımları üzerindeki etkisi, Şekil 5.28'da sunulmuştur. Bu BER eğrileri, Bob 1 için Senaryo 1'de elde edilmiştir. Kanal Kestirimi her iki kullanıcının iletişim başarımının Şekil 5.25'da görüldüğü gibi benzer olduğu gözlemlenmiştir. Şekil 5.28'de, Eve'in BER başarımları da $N_r = 2$ için dahil edilmiştir.

5.4. VLC-NOMA Tabanlı PLS Tekniğinin Gizlilik Analizi

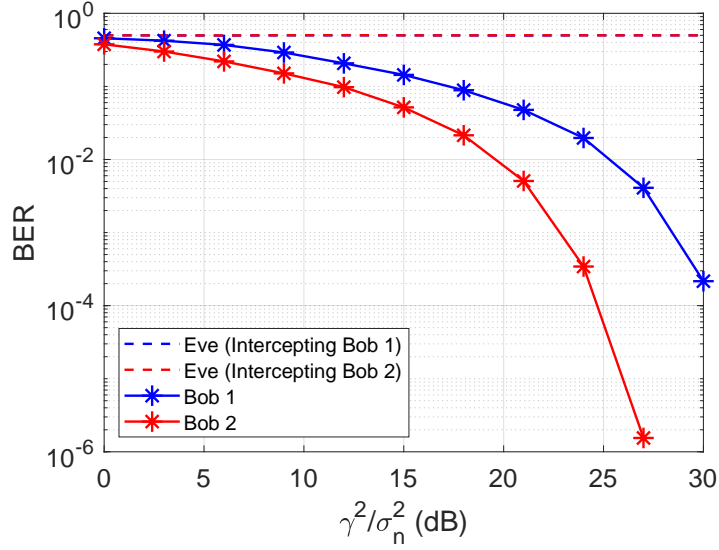
Şekil 5.29 ve 5.30'de, kullanıcılar, $[-1, 0, 0.85]$ ve $[1, 0, 0.85]$ noktalarında konumlandırıldığından elde edilen gizlilik başarımları grafikleri gösterilmiştir. Bu grafiklerde, önerilen ön kodlama stratejili MIMO-NOMA-VLC sisteminin gizlilik oranları, (3.72) ifadesine göre DCMC kapasiteleri olarak elde edilmiş ve $\{\text{sec}\}$ alt simgesiyle gösterilmiştir. Gizlilik oranlarının analitik alt ve üst sınırları, (3.87) ifadesine göre hesaplanmış olup $\{\text{lb}\}$ ve $\{\text{ub}\}$ ile gösterilmektedir.



Şekil 5.25. Senaryo 1 için, önerilen PLS önkodlayıcısıyla elde edilen BER başarımları grafikleri.



Şekil 5.26. Senaryo 2 için, önerilen PLS önkodlayıcısıyla elde edilen BER başarımları grafikleri.



Şekil 5.27. Önerilen PLS önkodlayıcı ile Senaryo 3 için elde edilmiş olan BER başarımlar grafiği.

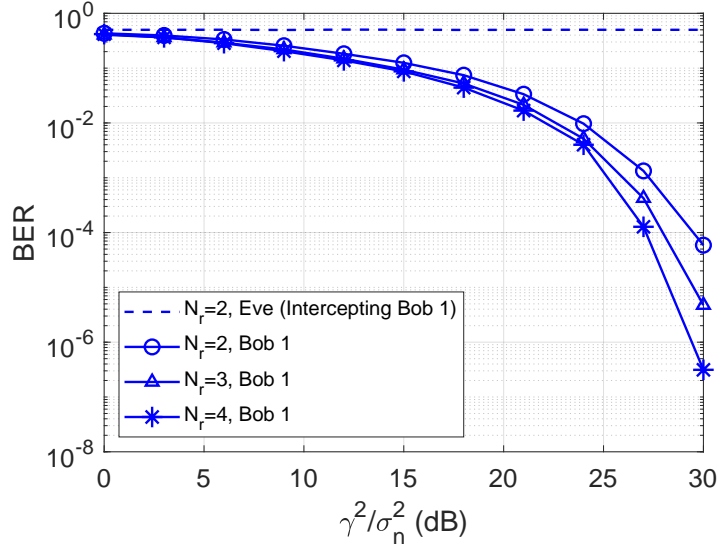
Şekil 5.30'de Eve'in 2 farklı noktada bulunduğu durumlar için elde edilen ulaşılabilir gizlilik oranları gösterilmektedir. Eve, $[0, 0, 0.85]$ noktasında iken elde edilen gizlilik oranları, Eve $[-0.75, 0, 0.85]$ noktasında iken yani kullanıcılardan birine daha yakınken elde edilen gizlilik oranlarından daha yüksektir. Bununla beraber, 20 db SNR'da 3.5 bpcu seviyesinde bir gizlilik oranı görece daha kötü olan pozisyonlamada bile elde edilebilmektedir. Bu sonuçların gösterdiğine göre, önerilen PLS önkodlama tekniğiyle yeterli gizlilik oranına ulaşılabilmektedir.

5.5. Geliştirilen PLS Yetenekli GLIM-OFDM Tabanlı VLC Sistemin Bilgisayar Benzetim Sonuçları

Bu bölümde, önerilen GLIM OFDM tabanlı iç mekan LiFi sisteminin PLS başarımlarıyla ilgili bilgisayar benzetim sonuçları sunulmaktadır. Yasal ve yasal olmayan kullanıcıların BER başarımları araştırılmaktadır. Bu amaçla, $3m \times 3m \times 3m$ ' boyutlarında tipik bir kapalı ortamda çalışan bir $n_T = n_R = 4$, (4×4) MIMO-VLC sistemi gözöne alınmakta ve tavanda belli koordinatları verilen dört aydınlatma LED'inin bulunduğu varsayılmaktadır:

$$\text{LED}_{\text{location}}(x, y) = \begin{bmatrix} 50 & -50 & 50 & -50 \\ 50 & 50 & -50 & -50 \end{bmatrix}^T \text{ cm.} \quad (5.8)$$

Kanal Kestirimi x ve y yatay eksenleri belirtir. PD'nin FoV yarı açısı ve alanı sırasıyla 70° ve 1 cm^2 'dir. PD'ler, bir masanın standart yüksekliği olan 0,8 m yüksekliğe yerleştirilmiş olup aydınlatmaların ve PD'lerin sırasıyla zemine dikey olarak aşağıya ve tavana yukarıya dönük olduğu varsayılmaktadır. LED'lerin yarı gücü ve yarı açısı ile PD'lerin alanlarının



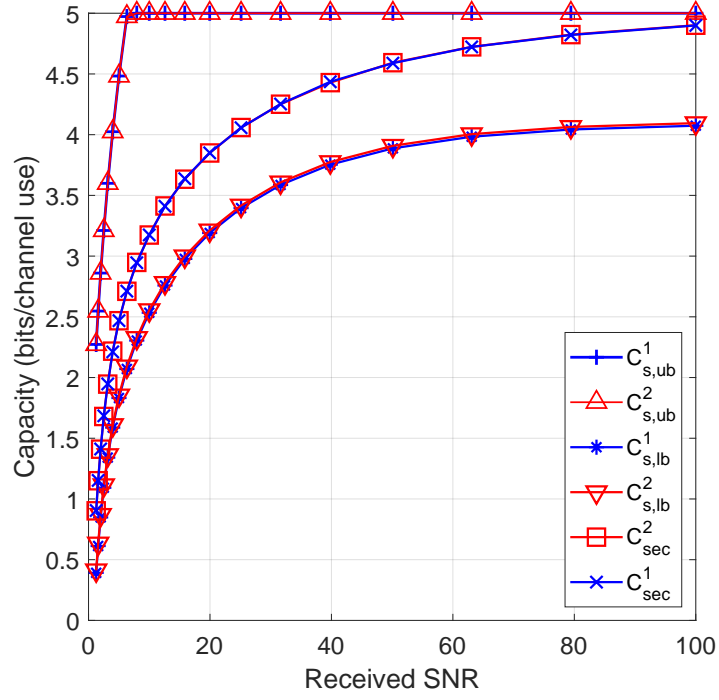
Şekil 5.28. Önerilen PLS önkodlayıcı ile artan N_r için elde edilmiş olan BER başarımları grafiği (Senaryo 1).

$\Phi_{1/2} = 2 = 60^\circ$; $\Psi_{1/2} = 70^\circ$; $A_{PD} = 1 \text{ cm}^2$ dir. Bu durumda, tüm LED'ler ve PD'ler arasındaki VLC kanal katsayıları (3.109) ile uyumlu olarak görülmektedir. BER ve SNR başarımları, Bob ve Eve için, OFDM alt taşıyıcılarının sayısının $N = 128$ olarak seçildiği, çeşitli VLC kanal konfigürasyonlarında ve QPSK sinyal kümelerinden elde edilir. Bob ve Eve, Config A (Bob'un PD'leri, 0,4 m'lik eşit aralıkla tablonun ortasındadır) ve Config B (Bob'un PD'leri, 0,4 m'lik eşit aralıkla ekranın köşelerinden birinde bulunur) olarak adlandırılan iki konfigürasyona göre yerleştirilmektedir.

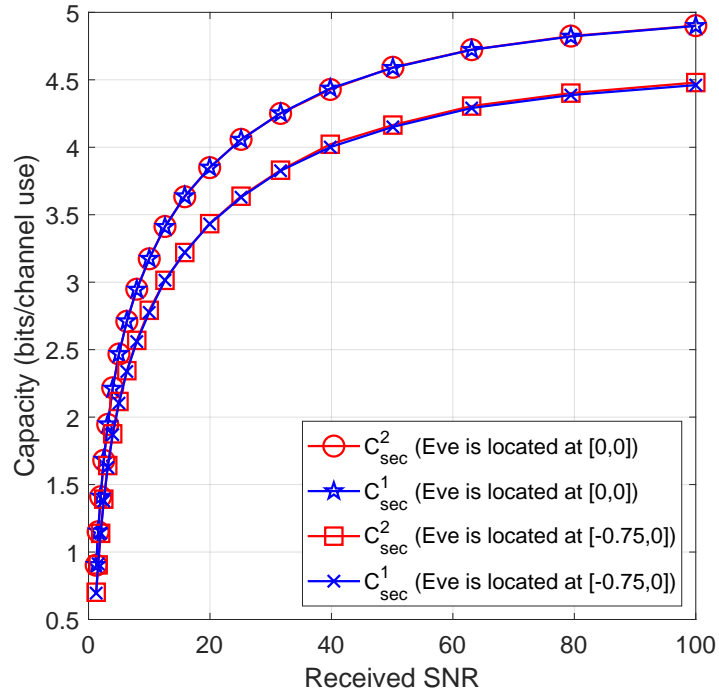
$$\text{ConfigA : PDs of Bob}_{\text{location}}(x, y) = \begin{bmatrix} 20 & -20 & 20 & -20 \\ 20 & 20 & -20 & -20 \end{bmatrix}^T \text{ cm.}$$

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

Her konfigürasyon için, Eve için iki kritik konumu ele alınmaktadır. Yani, Config A'da Eve ya odanın merkezine yakın bir yerde ya da odanın köşegen tarafında köşeye yakın bir noktada olacak şekilde seçilmiştir. Benzer şekilde, Config B'de Eve'nin PD'leri, odanın merkezine yakın bir yerde bulunan 40 cm ve 80 cm'lik farklı yüksekliklerde bir masa üzerine yerleştirilmiştir. Eve'nin Config A'daki konumları nedeniyle, Bob ve Eve uzamsal olarak ayrılmış farklı kanal kazançlarına sahip olacaktır. Oysa Config B'de, Eve'in kanal katsayılarının, sistemin BER başarımlarını etkileyecek LED'lerin yarısı için uzamsal bir benzerliğe sahip olması beklenebilir.

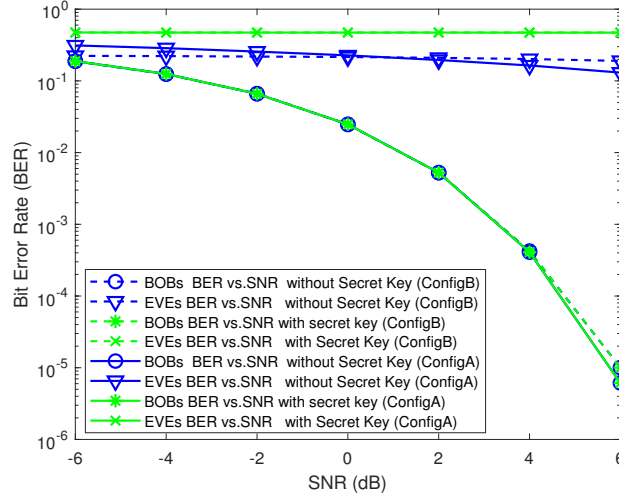


Şekil 5.29. Önerilen PLS önkodlama stratejisiyle elde edilmiş ulaşılabilir gizlilik oranı eğrileri ile alt ve üst limitleri.

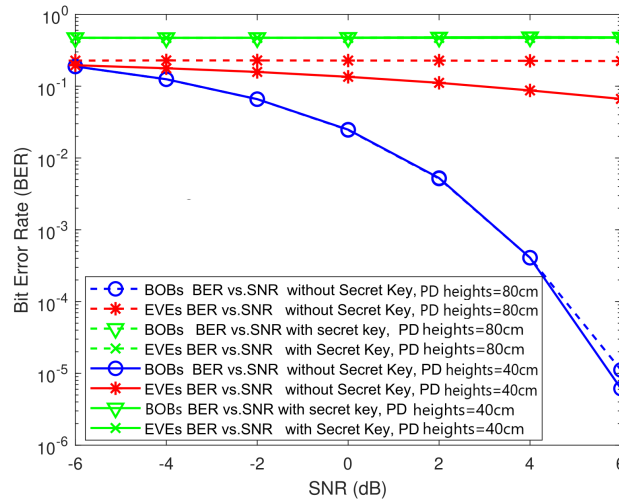


Şekil 5.30. Önerilen PLS önkodlama stratejisiyle, Eve iki farklı noktada iken elde edilmiş ulaşılabilir gizlilik oranı eğrileri.

Şekil 5.31’de Bob ve Eve’in BER başarımları, Config A ve Config B için SNR’nin bir işlevi olarak gizli anahtarla ve gizli anahtar olmadan karşılaştırılmaktadır. Gizli anahtarla ve gizli anahtar olmadan BER başarımlarındaki fark, Şekil 5.32’de vurgulanmıştır.



Şekil 5.31. Gizli anahtar kullanan ve kullanmayan durumlarda 1. senaryo için Bob ve Eve'in BER başarımlarının karşılaştırılması



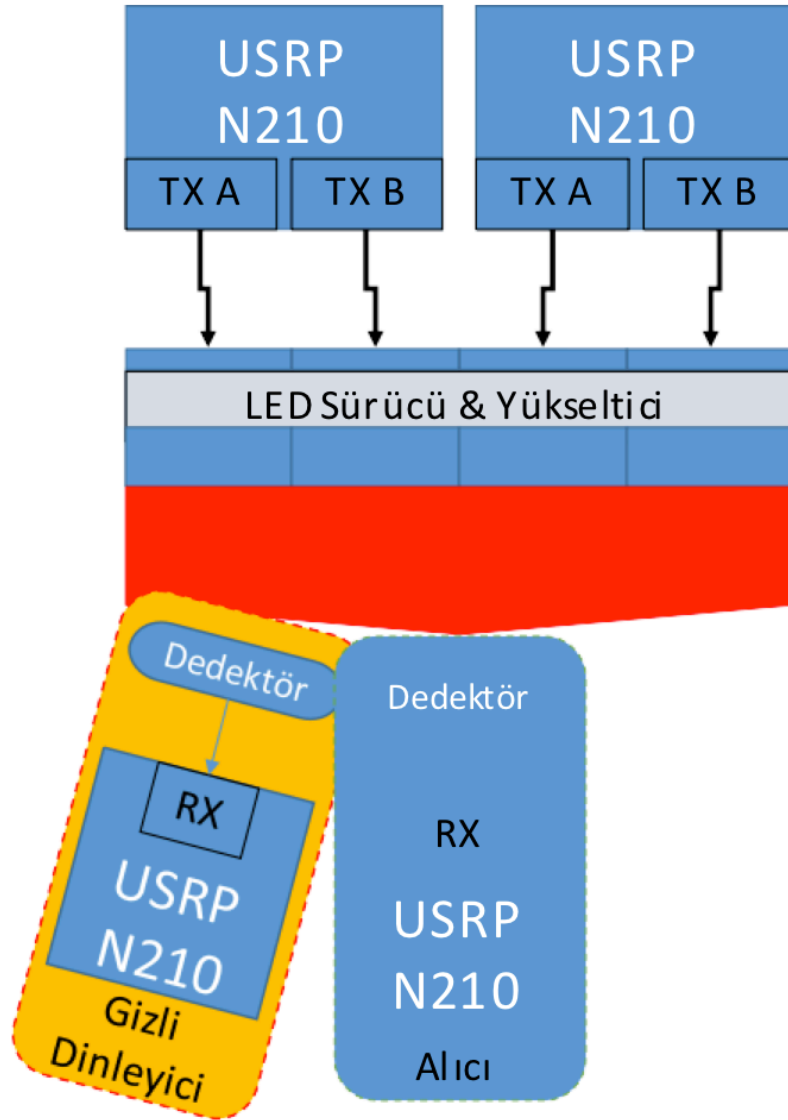
Şekil 5.32. Gizli anahtar kullanan ve kullanmayan durumlarda 2. senaryo için Bob ve Eve'in BER başarımlarının karşılaştırılması

Bob ve Eve'nin ortak bilgileri (mutual information) ve Bob'un gerçek erişilebilir gizlilik kapasitesi, Bob ve Eve'in ilgili kanallarının aşağıdaki gibi seçildiği bir senaryo için Şekil ??'de incelenmiştir:

6. FİZİKSEL KATMAN GÜVENLİKLİ VLC SİSTEMİNİN DONANIMSAL TASARIMI

6.1. Başlangıç PLS-VLC düzeneği

Kablosuz haberleşmede, belirlenen verici ile alıcı arasında iletilen sinyaller sistemin çevresinde bulunan başka alıcılar tarafından bu algılanabilmekte ve bu durum, bu tür sistemlerde Şekil6.1'deki gibi bir güvenlik açığına neden olmaktadır. Bu sorunu çözmek adına yapılan araştırmalarda, güvenlik açığına karşı geliştirilen ve geçen bölümlerde kuramsal olarak ayırtılabilir biçimde incelenen fiziksel katman güvenliği (PLS)'nin başarımını ölçmek için "gizlilik kapasitesi" kavramı ortaya konmuştur. Kablosuz haberleşmenin fiziksel katmanında bu güvenlik açığının ortadan kaldırmak için, haberleşmeyi sağlayan sistemin fiziksel özellikleri değiştirilerek verici ile alıcı arasındaki sinyal iletimi sağlanmakta ve bu sinyalin, çevrede bulunan başka alıcılar tarafından algılanması engellenmektedir. Dolayısıyla, güvenlik açığının haberleşmenin fiziksel katman düzeyinde ortadan kaldırılması, ya daha üst katmanlardaki güvenlik önlemlerine büyük katkı sağlanmakta ya da bazı durumlara bir önlem alınmasına gerek kalmamaktadır. Bu projende geliştirilen ve ayrıntıları önceki bölümlerde açıklanan önkodlama temelli PLS algoritmasının donanımsal olarak gerçekleştirilmesi için yapılan ön çalışmalarda gizlilik düzeyinin artırılması için VLC sisteminin vericisinin önünde optik merceklerin kullanılması önerilmiştir. Bu amaçla yürütülen deneysel çalışmalarda kullanılan donanım ve yazılım listesi Tablo 6.1'de verilmiştir. Bu kapsamda, kapalı ortam içinde çalışan tek-girişli-çok çıkışlı (multiple-input single-output (MISO)) bir VLC iletişim senaryosu PLS çerçevesi içinde incelenmektedir. Senaryoda alıcının sabit konumda olduğu varsayılmaktadır. Geleneksel bir MISO-VLC sisteminin yapısı Şekil6.2(a)'da gösterilmektedir. Önerilen toplayıcı mercek, Şekil6.2(b)'de gösterildiği gibi, bilgi kaynağından üretilen sinyalin genliğini sınırlandırmakta olup, yayımlanan ışınların ilerlediği yön de Şekil6.2(c)'de gösterilmektedir. Bu aşamada yapılan ilk çalışmalar ve sonunda elde edilen katkılar, merceği bulunmayan diğer LED'lerden gelen karıştırıcı sinyallerin deneysel olarak incelenmesinden oluşmaktadır. Bilgi taşıyan ve karıştırıcı sinyallerin güç seviyelerinin ayarlanması, gizli dinleyicinin odanın herhangi bir konumunda olması durumunda elde edilebilecek ortalama gizlilik seviyesine bağlı olarak gerçekleştirilmektedir. LED ışıklarının oldukça geniş bir alana yayılması nedeniyle, iletişim kanalları gizli dinleyiciye açık konumda kalacaktır. Önerilen katkılardan ikincisi ise, gizli dinleyicinin kanal bilgisinin bilgi üreten kaynak tarafından bilinmemesi durumunda bile, veri ileten LED'in önüne yerleştirilen merceğin fiziksel katmanda belli bir güvenlik sağladığının gösterilmiş olmasıdır. Kullanılan mercek sayesinde bilgi aktarımı bir bölge içerisinde sınırlandırılarak sadece bu güvenli alan içerisindeki alıcıların veri iletimine dahil olması sağlanmaktadır. Şekil6.2'de gösterilen bir deneysel test düzeni kurularak önerilen yaklaşımın verimliliği ölçüm sonuçları incelenmiştir.



Şekil 6.1. Gizlilik problemini görselleştiren, bir yasal alıcı bir yasal olmayan alıcıdan oluşan VLC sisteminin şeması

2x N210 USRP
LFTX Daughter Board (Frequency Range: 0 - 30 MHz, Bandwith: 30 MHz/Channel)
LFRX Daughter Board (Frequency Range: 0 - 30 MHz, Bandwith: 30 MHz/Channel)
LabView kurulu, GB ethernet arayüzlü, bilgisayar
LED
2n7000 entegre ile oluşturulan LED sürücü
Osiloskop
Sinyal Kaynağı
Thorlabs Fotodiyot –PDA36A
DC güç kaynağı

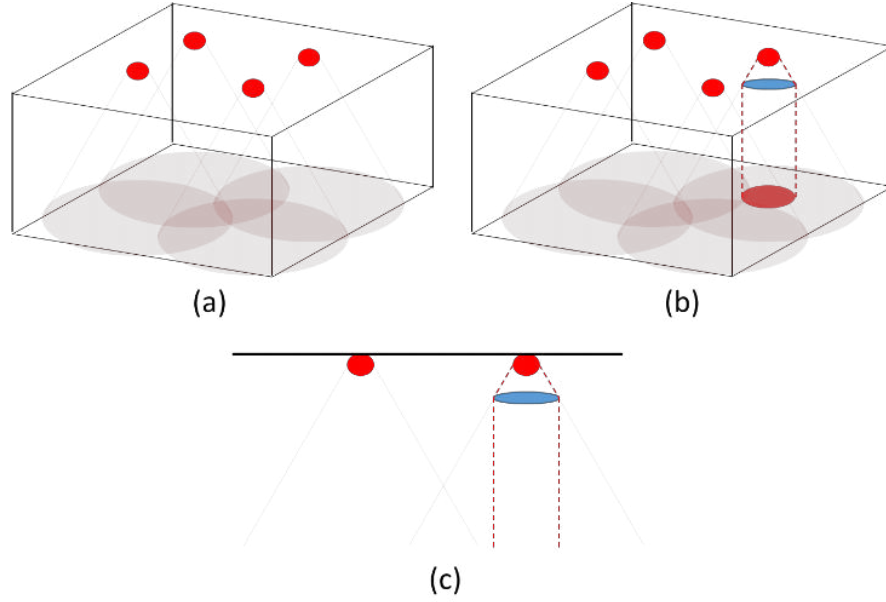
Tablo 6.1. Donanım ve Yazılım Listesi

Donanım çalışmalarında ele alınan VLC sistem modeli belirli bir kapalı alan içerisinde bulunan dört LED ve iki fotodedektörden(PD) oluşan bir MISO - VLC haberleşme sisteminden oluşmaktadır. Şekil6.2'(a)'daki sistemde LEDler, kırmızı daireler biçiminde gösterilmiş ve belirtilen kapalı alan üzerine ışık yaymaktadır. Bu sistemin sinyal ileticisi olarak görev yapan LED, alanın belirli bir köşesinde konumlandırılmıştır. Belirtilen LED tarafından iletilen sinyal, alıcı tarafta bir fotodedektör ile optikten elektriğe dönüştürülmekte ve alıcıdaki veri sezimi ve denkleştirici gibi işlemler elektriksel domende gerçekleşmektedir. Bu konfigürasyonda görülmeyen ikinci bir fotodedektör ise bir eavesdropper (kulak misafiri) görevi yaparak iletilen sinyal hakkında bilgiyi yasal olmayan yoldan almaya çalışmaktadır. Belirtilen noktanın etrafında dizilmiş diğer LED'ler ise iletilen bilgiye erişmeye çalışan fotodedektöre karşı gürültü sinyalleri yaymaktadır. Şekilde gösterilen MISO-VLC modeli, bir kriptografi senaryosu ile de açıklanabilir. Bu sistemi oluşturan alt birimler literatürde şöyle adlandırılmaktadır sinyal iletiminin vericisi, Alice, alıcısı, Bob, yasal olmayan yoldan Bob'a iletilen bilgiyi dinlemeye çalışan alıcı'da Eve. Ayrıca sistemde yapay olarak gürültü sinyalleri üreten kaynak da Jack olarak isimlendirilmiştir. Bu senaryoda hedef, Alice ile Bob arasındaki sinyal iletiminin, Jack'in yardımı ile Eve tarafından algılanmasının enaza indirilmesi ya da mani olunmasıdır. VLC'de optik iletişim, asenkron biçimde faz bilgisini kullanmadan sinyal şiddetine dayana bir modülasyon tekniği ile gerçekleştirir. Bu nedenle, temel bant sinyali sadece gerçek ve negatif olmayan değerler alır. Sinyal modülasyonundaki kısıtlamaya ek olarak verici LEDler konumsal ve zamansal olarak uyumsuzdur. Hüzmeleme (beam forming) gibi uyumlu ışık kaynaklarına gereksinim duyan yöntemler gerçek sistemlerde uygun gözükmemektedir. Bu kısıtlamalar ışığında, göz önüne alınan çalışmada, uyumsuz ışık yayan LED'ler için,

karıştırıcı sinyal yayın LED'lerin yanında bir sinyal üreten verici LED'in olduğu donanım ele alınmaktadır. Bu donanımda fiziksel güvenliği artıran yapay gürültü ile ve bilgi sinyali arasındaki güç paylaşımı temel alınmaktadır. Önerilen sistemin gizliliği için kullanılacak gizlilik oranı, ulaşılabilecek en büyük gizlilik kapasitesi ile sınırlıdır. Bu senaryoya bağlı olarak gizlilik kapasitesi, sinyal iletimi esnasında verileri algılayan Bob ile verileri yasal olmayan yoldan elde etmeye çalışan Eve'in kanal kapasitelerinin farkı olarak tanımlanabilir. Hesaplanan gizlilik kapasitesinin değerinin ne kadar büyük olduğu da, VLC sistemindeki bit hata oranı (BER) başarımının ne kadar iyi olduğu ile doğru orantılıdır. Gizlilik kapasitesi, ayrıca verici ile alıcının, buldukları kapalı ortam içindeki konumlarına da bağlıdır. Bu durum, Bob ile Eve'in kanal kazançlarının hesaplanabilmesi amacıyla üç boyutlu vektörel birimlerin kullanılmasından kaynaklanmaktadır.

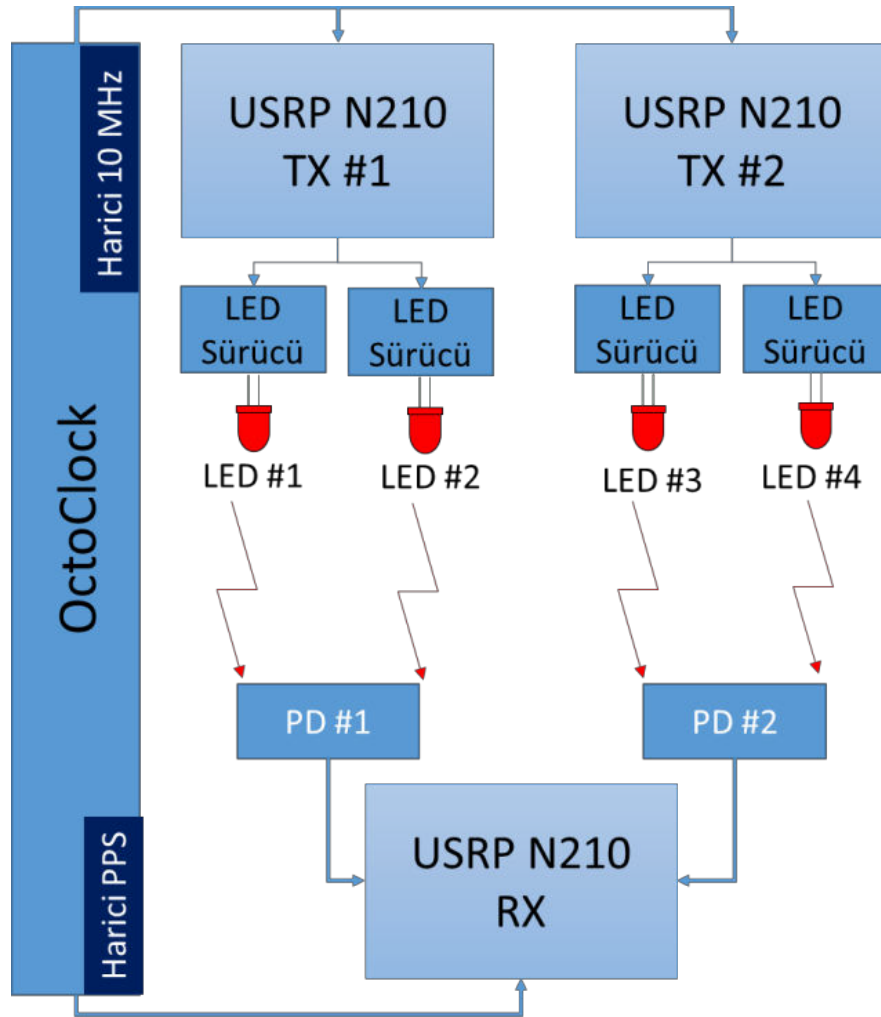
Deneyler sırasında Şekil6.3'de gösterilen düzeneğe alıcı ve verici birimleri olarak *Ettus Research USRP N210* yazılımsal radyo birimleri seçilmiştir. Deney düzeneğine eklenen 3 USRP'den bir tanesi LFRX kartı ile donatılmış ve alıcı rolünü üstlenmiş, diğer ikisi ise LFTX kartı ile donatılmış ve verici rolünü üstlenmiştir. Kullanılan radyoların senkronizasyonu için *National Instruments CDA-2990* modülü kullanılmış ve harici olarak 10 MHz ve PPS sinyali sağlanmıştır. Verici olarak 4 adet standart kırmızı LED kullanılmıştır. USRP çıkışı LED'lerin çalışması için gerekli akım beslemesini sağlayamadığından LED'lerin sürülmesi ve sürekli ışığa yapmaları için MOSFET kullanılarak bir yükseltici devre tasarlanmıştır. Bu sayede doğru akım (DC) ve radyo frekanslı (RF) sinyaller toplanarak söz konusu LED'ler sürülmektedir. Alıcı olarak *Thorlabs PDA36A* fotodetektörler kullanılmıştır.

Gözönüne alınan sistem modeli, bir MISO-VLC kurulumuna dayanmakta olup, belirli bir kapalı alan içinde konumlandırılmış dört LED ve iki fotodetektörden (PD) oluşan bir MISO - VLC haberleşme sisteminden oluşmaktadır. Şekil6.4'de gösterilen sistemde kapalı alan içindeki LED'ler, kırmızı daireler biçiminde görülmektedir ve belirtilen alanlar üzerine ışık yaymaktadır. Bu sistemin sinyal ileticisi LED, alanın belirli köşesinde konumlandırılmıştır. Belirtilen LED tarafından iletilen sinyal, alıcıda bir PD tarafından elektriksel sinyale dönüşür. Bu şekilde görülmeyen bir noktada konumlanmış ikinci bir PD ise bir eavesdropper (kulak misafiri) olarak iletilen sinyal hakkında bilgi alabilmek için hazırda beklemektedir. Belirtilen noktanın etrafında dizilmiş diğer LEDler ise iletilen bilgiye erişmeye çalışan PD'ye karşı gürültü sinyalleri yaymaktadır. Şekilde gösterilen MISO-VLC modeli, bir kriptografi senaryosu ile de açıklanabilir. Bu sistemin birimleri; sinyal iletiminin vericisi Alice, alıcısı Bob, belirlenen sinyal alıcısı dışında çevreden sinyali ayrıca algılayan Eve ve yapay olarak gürültü sinyalleri üreten Jack olarak tanımlanabilir. Bu senaryoda hedef, Alice ile Bob arasında sağlanan sinyal iletiminin Jack'in yardımı ile Eve tarafından algılanmasını önlemektir. Yukarıda belirtildiği gibi, VLC'de sinyallerin faz bilgisi kullanılmadığı için, iletilen temel bant sinyali sadece gerçek ve negatif olmayan değerler alır. Sinyal modülasyonundaki kısıtlamaya ek olarak verici LED'ler konumsal ve zamansal olarak uyumsuzdur. Bu kısıtlamalar

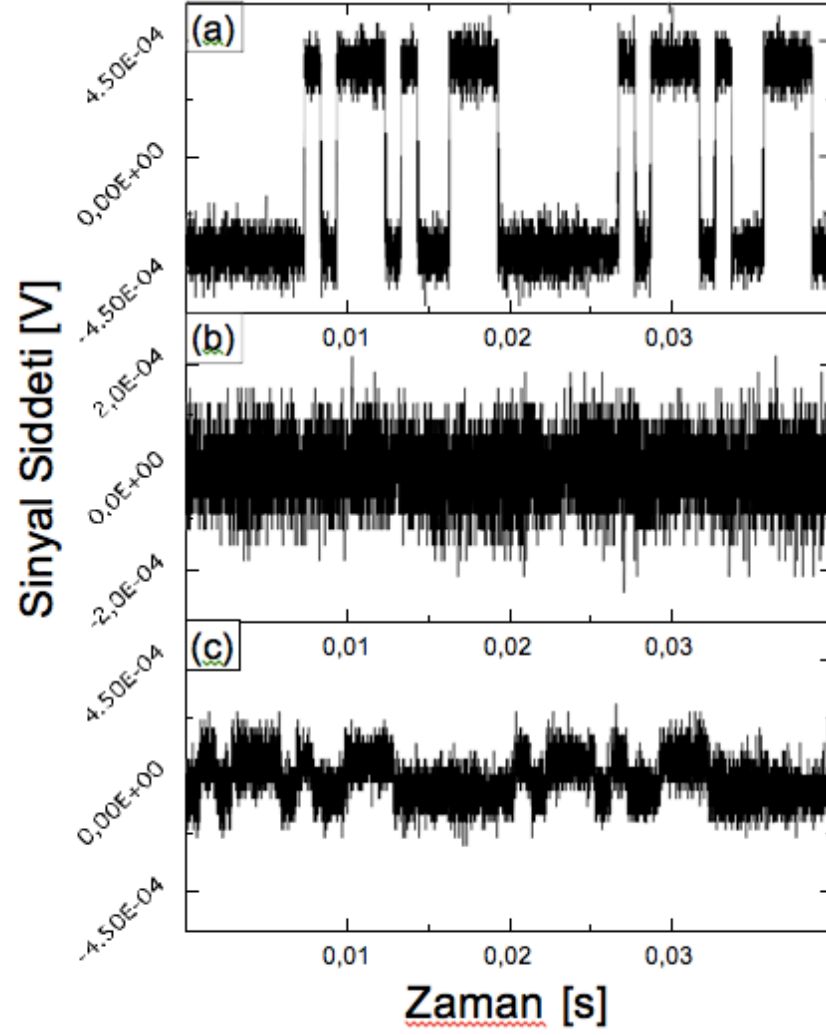


Şekil 6.2. Geleneksel bir kapalı ortam MISO-VLC sisteminin şeması. (a) sağ üstteki LED veriyi ileten verici olarak ayarlanabilir. Etraftaki diğer kaynaklar ise yapay gürültü oluşturmak için kullanılabilir. (b),(c) bir LED vericinin önüne yerleştirilen mercek ile bilginin odada belirli bir noktaya aktarılması sağlanmıştır.

ışığında, uyumsuz ışık yayan LED ler için karıştırıcı sinyal yayan LEDlerin yanında bir sinyal verici LED in olduğu donanım ele alınmaktadır. Bu donanımda güvenlik artırımı oluşturulan yapay gürültü ve sinyal arasındaki güç dağıtımını temel almaktadır. Oluşturulan test donanımına ilişkin yapı, Şekil6.4'de gösterildiği gibi, bir kapalı ortam içerisinde kurulmuş olup, USRP aracılığı ile sinyal iletmek için *LabVIEW* yazılımı kullanılmıştır. Oluşturulan sistem ile kurulan minyatür oda içerisinde LED'ler aracılığı ile Bob'a sinyal aktarımı ve bu sırada oda içerisinde bulunabilecek Eve'e gelen sinyal değerleri gözlemlenmiştir. Yayınlanan sinyal için LabView kullanılarak rastgele bir veri dizisi oluşturulmuş ve bu diziyeye göre OOK (on-off-keying) türünden bir sayısal modülasyon kullanılarak modüle edilen sinyal oda içerisine yayınlanmıştır. Uygulama sırasında mercek altındaki ve merceğin alt hizasının dışındaki fotodetektörden USRP ile alınan sinyal genel olarak Şekil6.4'de gösterilmektedir. Bob tarafından mercek altında alınan sinyal Şekil6.4(a)'da görülmektedir. Şekil6.4(b)'de ise verilen sinyalin kapalı ortamdaki rastgele bir konumda bulunan Eve tarafından alınmış hali görülmektedir. LED'lerden uzak bir konumda iken Eve'in aldığı sinyalin iletilen gerçek sinyale oranla büyük bozulmaya maruz kaldığı görülmektedir. Şekil6.4(c)'de ise mercek kullanılmadan yayın yapan bir LED'in altındaki alıcıya ulaşan sinyal görülmektedir. Mercek ile yayın yapan bir LED'e göre daha geniş bir alana yayın yapan LED'in sinyalinin şiddeti yaklaşık olarak kullanılan PD'nin aktif alanı ile sınırlanmış olduğu görülmektedir.



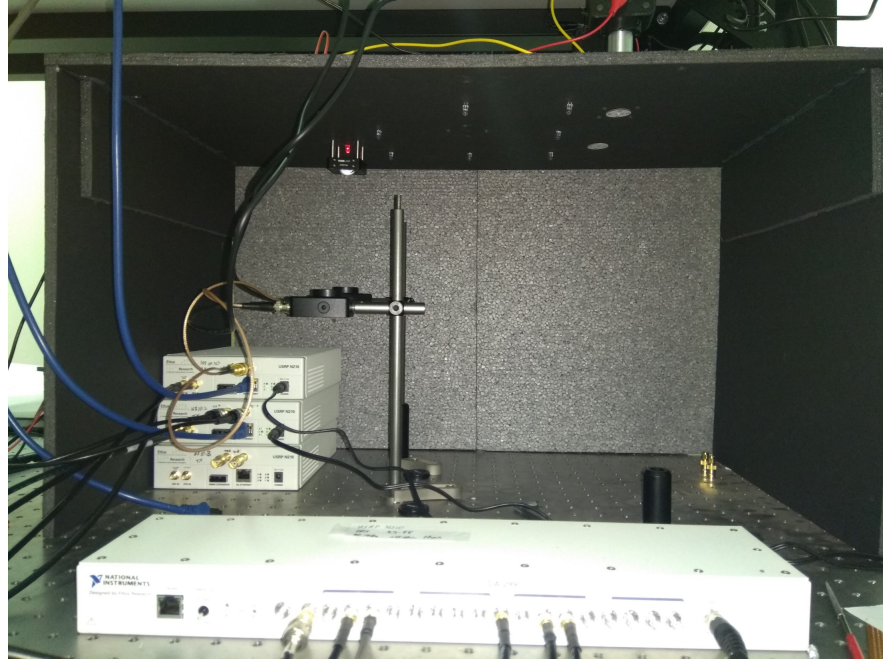
Şekil 6.3. Uygulamada kullanılan komple deney düzeneği



Şekil 6.4. (a) Mercek altındaki alanda bulunan Bob'a erişen sinyal, (b) Doğrudan LES ışınımı dışındaki bir noktada alınan sinyal. (c) Merceksiz LED altındaki noktada alınan sinyal

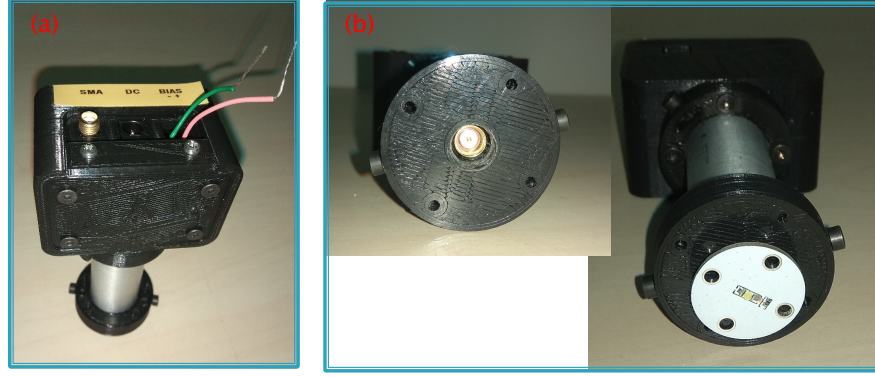
verici üzerinde yapılacak ufak deęişiklikle bir mercek eklenmesi durumunda, iletiřimin fiziksel düzeyde güvenlięinin iyileřtięi grlmektedir. Bu basit donanım uygulamasında sadece bir vericiye eklenen mercek ile hem basitlik ve dřk maliyet saęlanmakta ve geri kalan LED ışık kaynakları ise aydınlatma amalı kullanılabilir. Bu bakımdan PLS'yi arttırılırken nerilen mercek sistemi aydınlatma ihtiyalarına da bir engel teřkil etmemektedir. Benzer bir sistem verici LED'in stne yerleřtirilen bir kresel ukur ayna ile de saęlanabilir. Allice nnde bir mercek konumlandırılması, sinyalin alınacaęı konumu sınırlandırarak PLS'yi nemli miktarda arttırırken, LED ve mercek arasındaki mesafe ile oynanarak sınırlı blgenin geniřlięi ayarlanabilir.

Yukarıdaki paragraflarda aıklanan test ortamı Őekil6.5'de gsterilmiřtir. Kırmızı ile gsterilen kısımda ise yeni donanımda kullanılacak LED'ler grlmektedir. Bu LED'ler yukarıda bulunan *bias tee* ile baęlantılıdır. Sol kısımda ise yeřil halka ierisinde mevcut donanımda kullanılan MOSFET ile srlen LED ve mercek grlmektedir.



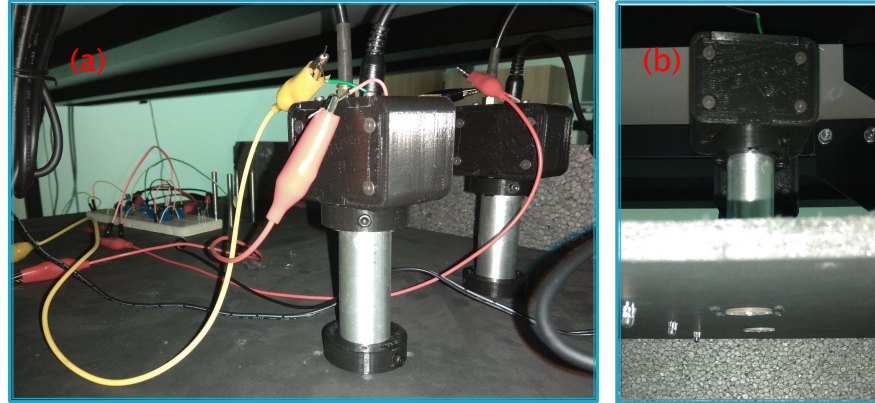
Őekil 6.5. Test ortamını fotoęrafı

Kurulan ikinci deney dzeneęinde LED'leri srmek iin kullanılan *bias tee* ve LED niteleri Őekil6.6'de gsterilmiřtir. Őekil6.6(a)'da src kısmında RF sinyal giriři iin bir adet SMA baęlantısı, LED'in srekli aık kalması iin bir akım beslemesi ve src sistem birimlerinin alıřması iin DC g giriři bulunmaktadır. Őekil6.6(b)'de ise LED birimleri src birimin altında bulunan SMA soket ile sisteme baęlanmaktadır. Deney dzeneęine entegre edilen LED src birimleri Őekil6.7'de gsterilmiřtir. Őeklin sol tarafındaki grsel



Şekil 6.6. LED'leri sürmek için kullanılan *bias-tee* devreleri ve LED üniteleri

uzak kısmında bulunan MOSFET LED sürücü birimini ve yeni düzenekte kullanılacak LED sürücü birimleri (yakındakiler) göstermektedir. Şeklin sağ tarafındaki görsel ise Bias tee ve LED'lerin mevcut deneysel düzeneğe monte edilmiş durumları göstermektedir.



Şekil 6.7. Deney düzeneğine entegre edilen LED sürücü birimleri

6.2. Son PLS-VLC donanım yapısı

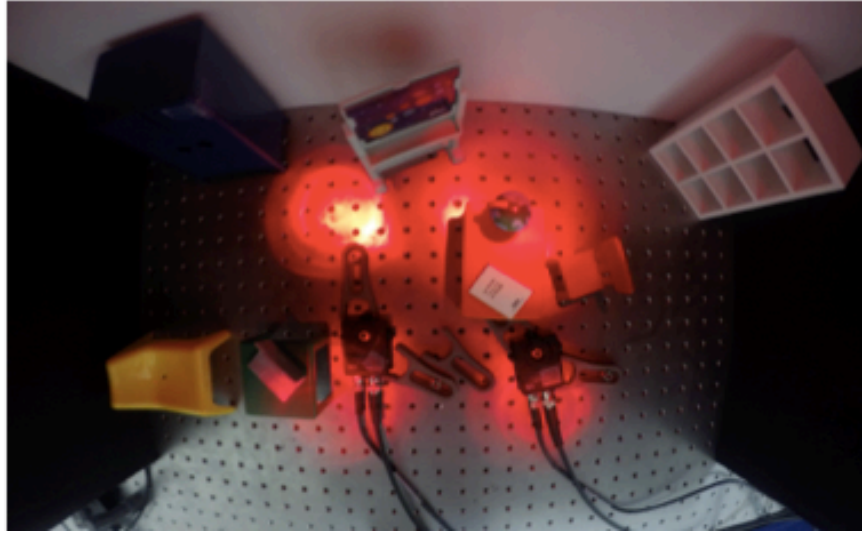
Bu kısımda, Şekil6.8'de görüldüğü gibi, VLC alanında deneyler yapabilmek için 4 LED'li düşük maliyetli 70 cm × 40 cm × 40 cm bir minyatür oda modelinin test yatağı sunulmaktadır. Test yatağı, geleneksel bir odanın 10:1 küçültülmüş bir kopyasıdır ve sürücü ve opto-elektronik algılayıcı bileşenleri hariç, toplam fiyatı 10\$'ın altında olan basit ofis malzemeleriyle oluşturulabilmektedir. Test yatağı uygun maliyetli olmasının ötesinde, (i) optik bileşenlerin entegrasyonuna, (ii) istenilen pencere ve kapı desenlerinin farklı karton renk tonlarında oyularak, ışığın farklı renkli duvarlardan yansımaların ve dış ışık kaynaklarının etkisinin gözlemlenmesine de olanak tanımaktadır. Yerleşik kurulumda, bundan

önceki bölümde tasarlanan uzamsal (spatial modulation (SM)) ve ön kodlamaya dayalı bir PLS algoritmasının donanımsal geliştirilmesi gözönüne alınmaktadır. Literatürde ilk kez, bu çalışmada, ileten LED'ler ile yasal alıcı ve yasal olmayan dinleyici arasında sağlam ve güvenli bir iletişimin sağlandığı deneysel olarak gösterilmektedir. Ölçüm sonuçları, elde edilen erişilebilir gizlilik oranındaki büyük oranda iyileşmeleri doğrulamaktadır.

Bilindiği gibi, VLC, geleneksel radyo frekansı (RF) iletişimine alternatif ya da RF'i tamamlayıcı olarak gelişmekte olan bir teknolojidir [81]. VLC ön uçlarının ve farklı alıcıların kalitesini değerlendirmek için odak düzlemi dizilerine dayalı VLC sistemlerini test etmek için literatürde çok sayıda test yatağı tasarımı kullanılmıştır [82]- [83]. Boş alan tezgah üstü test yatakları, bir dizi ışık yayan diyot (LED) [84], iç mekan izleme [85] ve optik frekans tanımlama (OFID [86]) üzerinde Dik-Frekans Bölmeli çoğullamayı (OFDM) sergilemek için geliştirilmiştir. . Hibrit VLC – RF iletişimi [87] ve çift yönlü VLC de tezgah üstü kurulumlarda [88] gösterilmiştir. Bu çalışmada, Aşağıdaki şekilde gösterildiği gibi ofis malzemelerine (70 cm × 40 cm × 40 cm boşluklu kartonlar) ve basit LED'lere (4 × Thorlabs LED630E) dayalı düşük maliyetli minyatür (10:1) bir VLC test yatağı sunulmaktadır. Işığın algılanması , değişken kazançlı trans-empedans güçlendiricileri -TIA ($2 \times Thorlabs PDA36A$) ile bağlantılı olarak PD'ler aracılığıyla gerçekleştirilmektedir. LED'lerin ayakları doğrudan üst kartona yerleştirilmiş olup, bağlantıları tavanın üzerine kurulan sinyal üreteçleri aracılığıyla beslenmektedir. Üretilen akımı sınırlamak için sinyal üreticinin çıkış uçları arasına, (50Ω)'luk seri direnç bağlanmıştır. PD'lerin sisteme sağlam biçimde bağlanabilmeleri için, bunlar iki opto-mekanik çatal aracılığıyla doğrudan alt yüzeye (optik masa üzerinde) iliştilmiştir. PD'lerle osiloskop arasındaki bağlantı bir koaksiyal (BNC) hatla kurulmuş ve her iki PD'den alınan sinyaller eş zamanlı olarak osiloskop ekranından kaydedilmiştir.

Maliyetin yanı sıra, VLC demoları için karton duvarlı oda tasarımlarının kullanılması, kapı ve pencere özelliklerinin istenildiği gibi uygun şekilde şekillendirilmesine ve oyulmasına olanak tanır. Ayrıca, renk paletlerinin ve kartonların dokularının varlığı, farklı yüzeylerden çoklu yansıma etkilerini test etmeyi sağlar. 10:1 minyatürleştirme ayrıca mobilya yerleşiminin ve VLC sistemi üzerindeki etkilerinin uygun şekilde izlenmesine olanak sağlar. Sunulan kurulum ayrıca ek opto-mekanik kafes bileşenlerinin (yani lens tutucular, lensler, çeviri aşamaları) entegre edilmesine de açıktır. Bu konuda ilk çalışmalarımız, LED'in önünde bir lensin kullanılması temeline dayanmaktaydı [89]. Bu çalışmanın aksine, daha önce sunulan minyatür test yatakları, farklı oda, pencere ve kapı tasarımları ve entegre opto-mekanik bileşenler yapma esnekliği ve kolaylığından yoksundur [90]. Sonuçta, bu geleneksel haberleşme (Alice-Bob-Eve) modelinde önkodlamalı uzaysal modülasyon temeline dayanan güvenli bir iletişim bağlantısı donanımsal olarak sağlanmaktadır.

Bu çalışmada, VLC'de fiziksel katman güvenliğini sağlamak için yeni bir yaklaşım olan uzamsal modülasyonun ve verici tarafta bir ön kodlama işleminin gerçekleştirildiği yeni ve özgün



Şekil 6.8. 4 LED, 2 PD ünitesinden oluşmuş test ortamının farklı açılarda görünümü

bir teknik ele almaktadır. Bilginin sadece veri sembolleri ile değil, LED'lerin indisleriyle de iletilmesini sağlayan uzamsal modülasyon ve VLC kanal modellerinin nispeten statik doğası olmasının nedeniyle literatürde iyi bilinmektedir [91]. Uzamsal modülasyon, çoklu antenli vericilerin varlığında, spektral verimliliği artıran çok etkili bir araçtır [92]. Ayrıca, uzaysal modülasyonun kullanımı, aşağıda ayrıntılı olarak açıklandığı gibi VCL sistemlerinin [93]- [95] gizlilik düzeylerinin iyileştirilmesinde bir derece serbestlik sağlar.

Deney düzeneğinde, yoğunluk modülasyonu ve doğrudan algılama teknolojisinin kombinasyonu düşünülmüştür. $m \in \{A, -A\}$ ile temsil edilen ikili veriler iletilir. n_T ile kaynaktaki (Alice) LED ünitelerinin sayısını ifade eden bu veriler, bir ön kodlama işleminden sonra meşru kullanıcıya (Bob) iletilir. Alıcı fotodetektörlerin (PD'ler) (n_R) sayısının deneysel kurulumumuzda olduğu gibi 1'e eşit olduğunu varsayarak, kaynak tarafında n_T sayıda LED'lerden iletilen ayrık-zamanlı sinyal vektörü aşağıdaki gibi ifade edilebilir:

$$\mathbf{u} = \beta \mathbf{P}m + dc \mathbf{1}_{n_T}. \quad (6.1)$$

Burada dc parametres, verilen bir uygun aydınlanma için ön kodlayıcı çıktısının her zaman pozitif olmasını sağlamak için uygun DC bileşenini temsil eder. Ön- işleme (prerocessing) sırasında büyük güç dalgalanmalarını önlemede, güç kısıtlamasını korumak için tasarlanmış bir β ölçeklendirme faktörü sunulmaktadır. Burada, geleneksel $\mathbf{u}^T \mathbf{u} = 1$. biçiminde formüle edilen doğrusal Kanal Ters Çevirme (CI) tabanlı ön kodlama tekniği kullanılacaktır.

$$\mathbf{P} = \mathbf{H}^T (\mathbf{H} \mathbf{H}^T)^{-1} \quad (6.2)$$

olup, $\mathbf{H} \in \mathcal{R}^{n_R \times n_T}$, VLC sisteminde verici ve alıcı arasındaki optik kanal matrisini ve ön işlemden sonra çıkış gücünün güç normalizasyon katsayısı aşağıdaki ilişikten hesaplanır:

$$\beta = \sqrt{\frac{1}{\text{trace}(\mathbf{H}^T (\mathbf{H} \mathbf{H}^T)^{-1})}}. \quad (6.3)$$

Son olarak, önerilen donanımda olduğu gibi, Bob'un ve Eve'in tek PD'lerinde gözlemlenen sinyal, ilgili kanalları aracılığıyla yayıldıktan sonra şu şekilde edilir:

$$y_B = s_B + (dc) \times \mathbf{H}_B \mathbf{1}_{n_T} + n_B, \quad (6.4)$$

$$y_E = s_E + (dc) \times \mathbf{H}_E \mathbf{1}_{n_T} + n_E \quad (6.5)$$

Burada,

$$s_B \triangleq \mathbf{H}_B \mathbf{P} m = \beta m$$

$$s_E \triangleq \mathbf{H}_E \mathbf{P} m = \beta \mathbf{H}_E \mathbf{H}_B^T (\mathbf{H}_B \mathbf{H}_B^T)^{-1} m$$

olup, \mathbf{H}_B ve \mathbf{H}_E sırasıyla Alice ve Bob ve Alice ve Eve arasındaki optik kablosuz kanal (OWC) matrislerini temsil eder. w_B ve w_E , ortalamaları sıfır, varyansları σ_B^2 ve σ_E^2 olan toplamsal beyaz Gauss gürültüsünü belirtir. Son olarak, y_B, y_E Bob ve Eve'in alıcıları tarafından alınan temel-bant elektrik sinyallerini gösterir. Daha sonra doğrudan algılama kullanılarak m 'le gösterilen veri sezimi şu şekilde gerçekleştirilir: $\mathbf{H}_B \mathbf{P} = \mathbf{I}_{n_T}$ gerçeğini dikkate alarak ve algılamadan önce alıcıdaki dc bileşenini bastırarak, Bob'un ve Eve'in alıcı antenlerinde gözlemlenen (4) ve (5) nolu sinyaller yeniden şöyle ifade edilebilir.

$$y_B = \beta m + w_B, \quad (6.6)$$

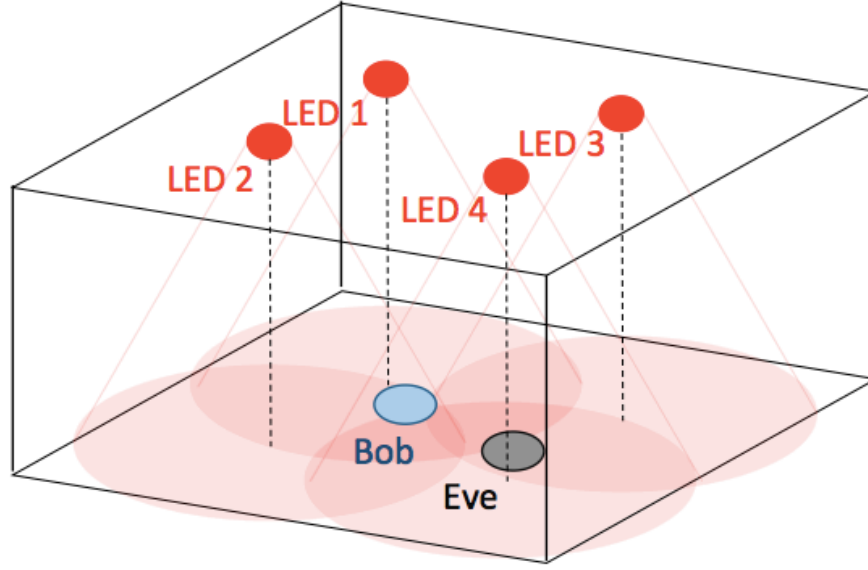
$$y_E = \beta m + J_E + w_E, \quad (6.7)$$

burada $J_E = s_E - s_B = \beta(\mathbf{H}_E - \mathbf{H}_B) \mathbf{P} m$ dir. (7)'deki J_E terimi, bir karıştırma (jamming) sinyalini göstermekte olup, (9)'da gösterildiği gibi tamamen Bob ve Eve arasındaki kanal farkları tarafından oluşturulur. Bu sinyale yaklaşık olarak sıfır ortalamalı ve varyansı $\sigma_{J_E}^2$ olan bir Gauss rastgele değişken olarak modellenebilir. Karıştırma sinyali, J_E , Eve'in maruz kaldığı girişimi arttırmada çok etkilidir ve onun bit hata oranını (BER) önemli ölçüde düşürür. İletilen indis bilgisi ve veri simgeleriyle taşınan bilgiler, ($I = (m, ind)$), alıcıda enbüyük olabilirlik(maximum likelihood) sezim kriterine uygun olarak sezilirler. Böylece sistem üzerinden $\log_2 n_T$ bit fazladan bilgi taşınmış olur.

$$\hat{I}_B = \arg \max_I \{ ||y_B - s_B||^2 \} \quad (6.8)$$

$$\hat{I}_E = \arg \max_I \{ ||y_E - s_E||^2 \}.$$

Şekil6.9, Bob ve Eve olarak adlandırılan iki PD'nin yerleşimini göstermektedir. Bob ve Eve, LED1 ve LED4 arasındaki diyagonal boyunca yerleştirilmiştir; Bob, LED 1'e (tabandaki izdüşümüne) 2 cm mesafeye, Eve ise LED 4'e (tabandaki izdüşümüne) 3 cm yakınlıkta yakın yerleştirilmiştir. LED'ler, genellik kaybı olmaksızın 2 Hz'lik sinyal üreteçleri ile sürülmüş olup, sürücü gerilim ofseti (VDC) ve tepeden tepeye (Vpp) değerleri, LED 1 için (2,6 VDC, 200 mVpp), LED 2 için (2,8 VDC, 240 mVpp), LED 3 için (3,2 VDC) ve LED 4 için (2,7 VDC, 210 mVpp), aynı çıkış optik gücüne sahip olacak şekilde ayarlanmıştır.



Şekil 6.9. Test ortamında Bob ve Eve'in yerleştirilmesi

	LED 1	LED 2	LED 3	LED 4
Bob	0.0714	0.0107	0.0059	0.0075
Eve	0.0127	0.0124	0.0075	0.0121

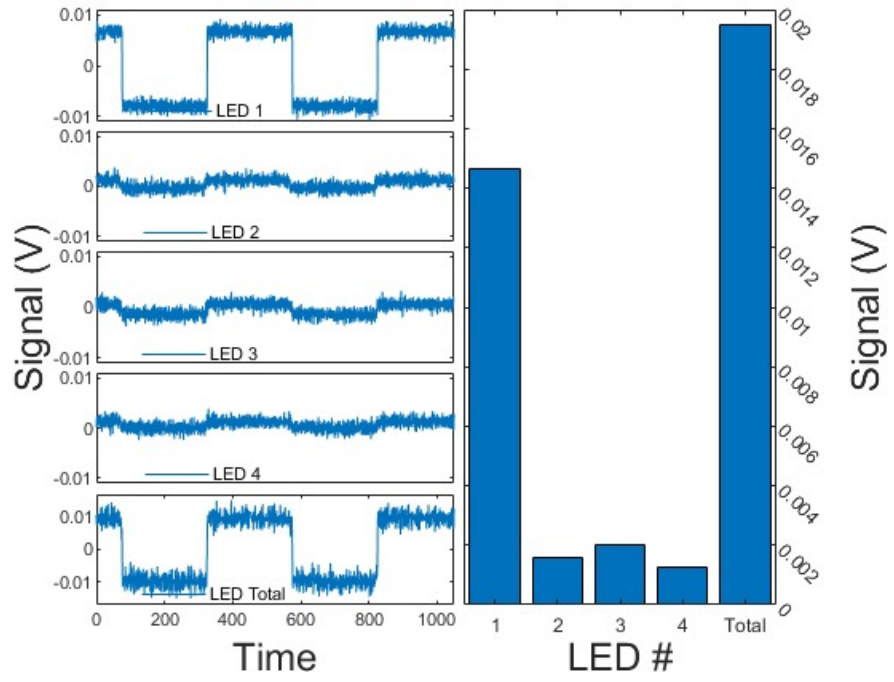
Tablo 6.2. Bob ve Eve için hesaplanan P değerleri

Bob ve Eve tarafından kaydedilen sinyaller (75 kV/A kazanç karşılık gelen 40 dB'ye ayarlanmış TIA kazanç ayarı ile) bir çubuk grafikte birlikte aşağıdaki Şekil6.10 ve Şekil6.11 de gösterilmektedir (tüm LED'lerden alınan kanal ölçümleri belirli bir periyodun gerilimine işaret eden zaman dilimleri). Genel olarak, Bob tarafından alınan ilk toplam optik güç (19 mV TIA çıkışı, $0,25 \mu W$ optik güce ve $0,02 W/n^2$ yoğunluğa karşılık gelir) ve Eve ($0,17 \mu W$ optik güce karşılık gelen 13 mV TIA çıkışı ve $0,014 W/n^2$ yoğunluğu) birbiriyle karşılaştırılabilir. Aşağıdaki Tablo 6.2 ve Tablo 6.3 daha önce matematiksel işlemler doğrultusunda hesaplanan P önkodlama matrisinin eleman değerlerini ve sürücü gerilimlerini göstermektedir.

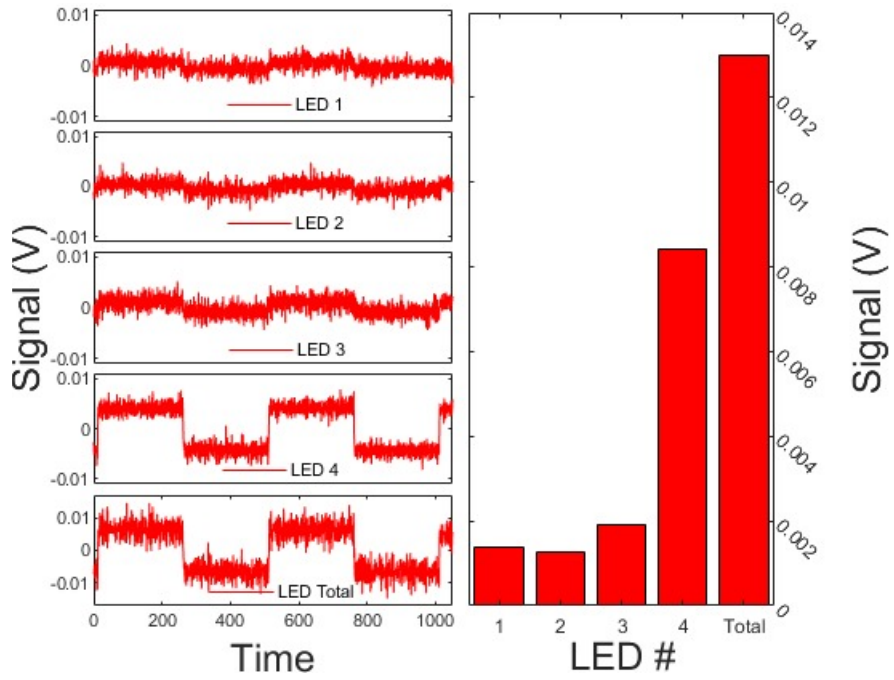
Uzaysal modülasyonu takiben Bob ve Eve'in her LED'e karşılık gözlemlediği sinyaller aşağıdaki Şekil6.12 ve Şekil6.13'de gösterilmektedir. Bu şekillerden ve Tablo 6.4, Tablo 6.5'den, uzaysal modülasyonun bir sonucu olarak, Bob tarafından elde edilen en yüksek

	LED 1	LED 2	LED 3	LED 4
Vpp	0.200	0.240	0.300	0.210
Vpp'	0.198	0.022	0.027	0.017

Tablo 6.3. LED'lerin sürücü gerilimleri (SM öncesi ve sonrası)

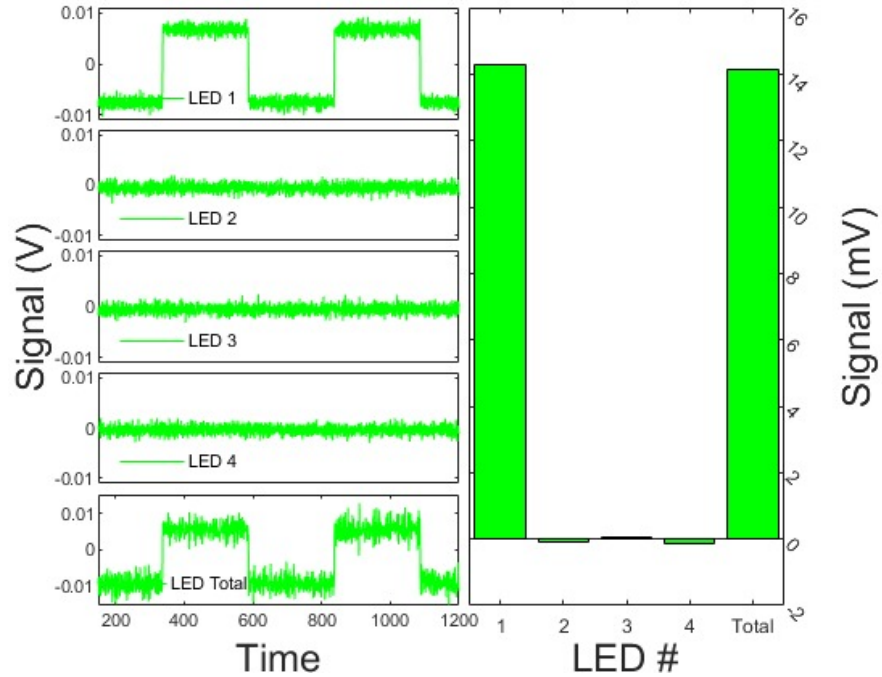


Şekil 6.10. Bob'un alıcısına gelen sinyallerin genliği

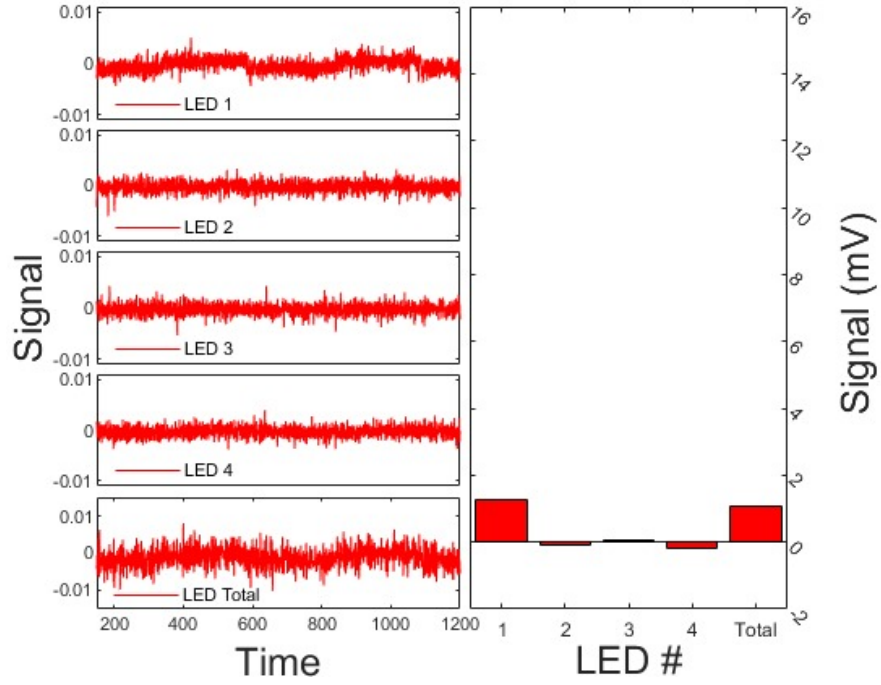


Şekil 6.11. Eve'in alıcısına gelen sinyallerin genliği

sinyalle sonuçlanan ilk LED'in sürücü voltajın neredeyse değişmediği, diğer tüm LED ışınlarının ise önemli ölçüde karartılmış olduğu görülmektedir. Ayrıca, Bob tarafından alınan toplam optik gücün, ($0,18\mu W$ optik güce ve $0,015W/n^2$ yoğunluğa karşılık gelen 14 mV TIA çıkışı), Eve tarafından algılanan optik güce oranla ($1,25\text{ mV}$ TIA çıkışı, 17 nW optik güce karşılık gelen), indeks modülasyonunun bir sonucu olarak, önemli ölçüde büyük olduğu görülmektedir. LED 2 ve 4 için uzaysal indis modülasyonundan sonra negatif ve küçük çıkış voltajları gözlemlenmiştir. Bunun TIA ve osiloskopun ofset gürültüsünden kaynaklandığı anlaşılmaktadır. Genel olarak, ön kodlamadan sonra, hem Bob hem de Eve için LED1 genliğinin (Bob'a en yakın olan LED) diğer LED'lere baskın olduğunu gözlemlenmektedir. Yürütülen deney için, tüm LED'lerin aktif olması durumunda, LED1 ile arasındaki farkın nispeten küçük olduğu görülmektedir. Bunun başlıca nedeni kanal eşleşmelerinin hatasız bir şekilde elde edilememesindedir. Doğal olarak, Bob ve Eve kanallarının ideal olmayan kestirimleri de başarımda düşüşe neden olmaktadır. Dikkate almamız gereken bir diğer nokta da, önerilen önkodlanmış SM yaklaşımının daha fazla sayıda LED'e ve değişen çevresel koşullara karşı esnek olmasıdır. Dolayısıyla önerilen yaklaşımın genel esnekliği ve ölçeklenebilirliği, iletimler için tek veya daha az LED kullanmaktan basitçe daha yüksektir. Son olarak, SNR, elde edilen sinyalin tepeden tepeye genlik değerinin (tüm LED'ler için) üzerindeki düz bölgenin (bir tepe veya bir düşüş) efektif(karesel ortalama değer)(rms) değerine bölünmesiyle elde edilmiştir. Gözlenen kare dalga SNR değerleri, [99]'da verilen formülasyona dayalı olarak gizlilik kapasitelerine (bit/sn/Hz) eşdeğerine bir değere dönüştürülmüş ve sonuçta önkodlama durumunda 2.5 katlık bir gelişme elde edilmiştir.



Şekil 6.12. Uzaysal modülasyon kullanıldığında Bob tarafında algılanan sinyal genlikleri



Şekil 6.13. Uzamsal modülasyon kullanıldığında Eve tarafında algılanan sinyal genlikleri

	LED 1	LED 2	LED 3	LED 4
Uzamsal Modülasyon Öncesi				
Bob	0.014667	0.001595	0.002009	0.001246
Eve	0.001382	0.001252	0.001926	0.008426
Uzamsal Modülasyon Sonrası				
Bob	0.014304	-0.00010	0.0004	-0.00012
Eve	0.001257	-0.0008	0.0007	-0.00019

Tablo 6.4. LED'lerin sürücü gerilimleri (SM öncesi ve sonrası)

	Hedef	SNR*	Secrecy Capacity (bit/sec/Hz) [99]
Ön kodlama öncesi	Bob	9.85	0.98
	Eve	4.49	
Ön kodlama sonrası	Bob	7.41	2.33
	Eve	0.67	

Tablo 6.5. Önkodlama öncesi ve sonrası sistemin eriştiği gizlilik kapasitesi

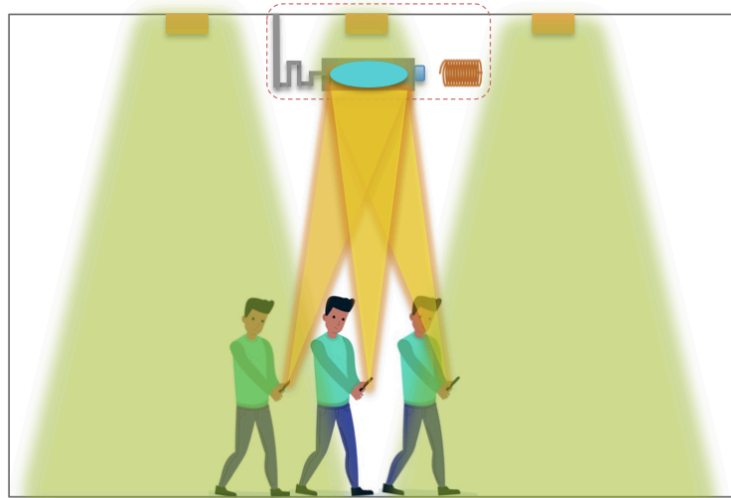
Özetle, projde literatürde ilk kez, VLC test yatağı olarak birden fazla LED’li ve dedektörlü düşük maliyetli minyatür bir oda modeli sunulmuştur. Test yatağı, istenen pencere ve kapı konfigürasyonları mukavva duvarlarından rahatlıkla oyulabildiğinden özellikle çekicidir. Ayrıca optik bileşenlerle (ışık kaynakları, dedektörler, lensler vb.) donatılmış opto-mekanik ray sistemleri, seçilen duvarlara yerleştirilebilmekte ve bu bir VLC sistemine entegre edilebilecek çeşitli optik bileşenlerin rolünü test etmeye olanak sağlamaktadır. Minyatürleştirilmiş test yatağımız, mobilya yerleşiminin etkisini izleme yeteneğine sahip olsa da, asıl odak noktası, mekansal indis modülasyonu yoluyla geliştirilmiş güvenliğin uygulanması olmuştur. VLC için geleneksel olarak beyaz LED’ler kullanılır. Ancak deneylerde kırmızı LED’ler kullanılmıştır. Kullanılan foto-dedektör üniteleri renge duyarsızdır, bu nedenle ışık kaynağı renk seçimi laboratuvarımızdaki mevcut LEDlerle yapılmıştır. Burada sunulanlar herhangi bir renkteki kaynak (veya renk kombinasyonu) için geçerlidir. Diğer ışık kaynaklarından (yani güneş, sokak lambaları, araç lambaları vb. gibi dış ortamdaki) gelen etkiler araştırma gurubumuz tarafından başka bir yayında gözönüne alınmıştır [101] ve dış etkilerin daha düşük ışık modülasyon frekansına sahip olduğu ve modüle edilmiş sinyal üzerinde bir doğru akım eklenmesi etkisi yaptığı sonucuna varılmıştır. Uzaysal indis modülasyonu, modülasyon sinyalinin genliğinin kalibre edilmesine dayanır, bu nedenle bu tür dış etkilere toleranslıdır. Son olarak, literatürde ilk kez yerleşik kurulum üzerinde uzay indis modülasyonu ile güvenli bir VLC iletişiminin başarıyla çalıştığını ve yasal olmayan kullanıcı tarafından alınan sinyalin de tamamen gürültü biçimine dönüştüğü görülmüştür. Donanımsal olarak tasarlanan test yatağındaki uzaysal modülasyon, laboratuvar olanakları çerçevesinde, düşük bir frekansta gerçekleştirildi. Ancak, gerçek uygulamalarda 100 MHz’e kadar modülasyonu destekleyen hazır kaynaklar ve fotodedektörler bulunmaktadır. [24,25] Test yatağı, veri toplama için bir otomasyon rutini ve gerçek zamanlı sinyal izleme için LED dalışı uygulanarak daha da geliştirilebilir. Gelecekteki bir çalışma olarak, alıcıda alıcıda (Bob) ışın yönlendirmesi için lens eyleyicilerini(actuator) entegre ederek test yatağının sağladığı üstünlüklerden daha fazla yararlanması planlanmaktadır.

6.3. 3B-baskı tabanlı lens eyleyiciler kullanılarak PLS’nin artırılması

Bu bölümde, görünür ışık iletişim uygulamalarında kullanılmak üzere 3B Baskılı lens tarayıcı tabanlı ışın yönlendirmesine ilişkin projede gerçekleşen tasarım, üretim ve uygulama çalışmaları sunulmaktadır. 5×5 cm boyutlarındaki bir tarayıcı , Poliaktik asit kullanılarak kaynaşmış biriktirme modellemesi (FDM) ile düşük maliyetli 3D baskı için tasarlanmıştır. Tarama, geleneksel bir 25 mm lensi taşıyan lens çerçevesinin, dikey iki yönden elektromanyetik olarak eyleyilmesi ile sağlanmaktadır. Mercek çerçevesini dış çerçeveye bağlayan serpantin yay, çalıştırma yönlerinde benzer yay sabitleri ve merceğin kütlesi nedeniyle minimum (< 1.5 mm) sarkma sağlayacak şekilde tasarlanmıştır. Üretilen eyleyici, minyatür bir VLC test yatağına ($70 \text{ cm} \times 40 \text{ cm} \times 40 \text{ cm}$) entegre edilmiş ve test ortamını kullanarak, yanal düzlemde eyleyicinin uygulanan gerilime karşı yer değiştirme ve

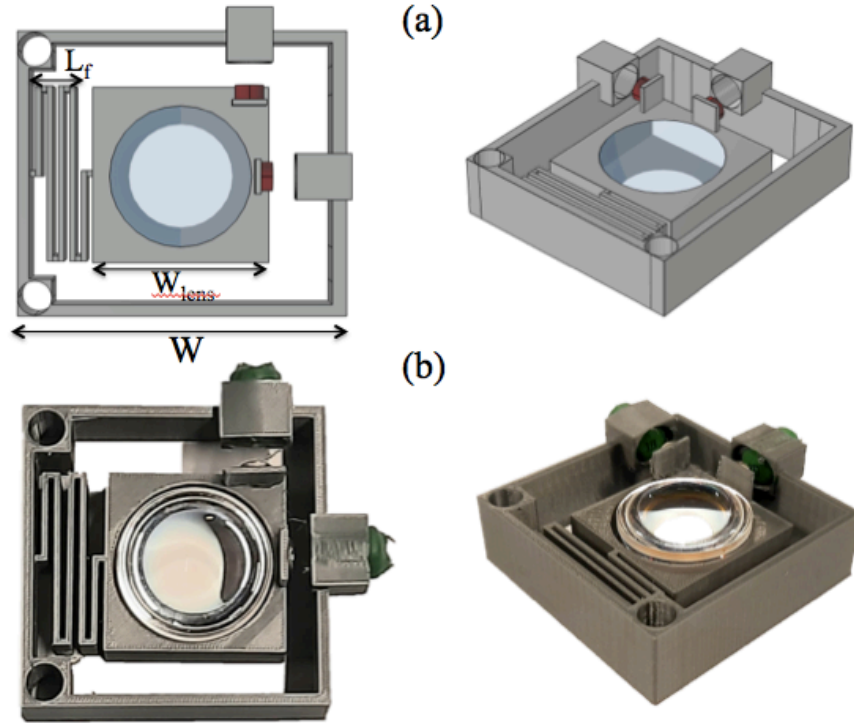
ışın tarama davranışı test etmenin yanında, yüz tanıma geri bildirimini ile hareketli bir hedef üzerinde ışın yönlendirmesi gösterilmiştir. Önerilen donanım, yasal alıcıyı izleyerek (yüz tanıma yoluyla) görünür ışık iletişimde gelişmiş bir güvenlik önlemi sunmayı ve odaklanmış ışığı hedeflenen cihaza yönlendirmek için geri bildirimini kullanmayı hedeflemektedir. Odaklama ve yönlendirme özelliklerinin ortak kullanımı, yasal alıcının odaklanmış ışık nedeniyle artırılmış gizliliğin üstünlüklerine sahip olurken bir taraftan da oda içinde dolaşmasına izin vermektedir. Sunulan eyleyici daha büyük oda boyutlarıyla kullanılabilir, ancak daha büyük aydınlatma ünitelerine (düşük ışıklı lambalar) yükseltme, daha hacimli lensleri taşımak ve daha büyük açı taramaları ele almak için 3D baskılı eyleyicilerle birlikte motorların kullanılmasını gerektirebilir.

Görünür ışıkla İletişim, hem iç hem de dış ortamda görünür ışık modülasyonu yoluyla kısa menzilli optik iletişim sağlar [106]. Geniş bir bant aralığı sunan, halen var olan aydınlatma amaçlı tüketici elektroniği ürünleriyle etkileşime neden olmayan VLC, radyo frekansı (RF) iletişiminin gelecek vaat eden bir tamamlayıcısı olarak kabul edilir [107]. Işığın uzamsal dağılımının güvenli bir bölge ile sınırlı olduğu çok girişli tek çıkışlı (MISO) bir VLC sisteminde VLC bağlantı gizliliğini geliştirmek için seçilen bir vericinin önünde optik lenslerin kullanımını [108]'da incelenmiştir. Hızlı ve düşük maliyetli üretim kabiliyeti (hem ekipman hem de filament maliyeti) ve düşük fiyatı sayesinde 3D baskı, mikrosistem üretimi için alternatif bir teknik olarak ortaya çıkmıştır [115]. Bu çalışmada, VLC'de odaklanmış ışık yayıcıları kullanma konusundaki önceki çalışmalarımızdan yararlanmak amacıyla, odaklanmış ışığı yasal alıcıya yönlendirmek için elektromanyetik olarak çalıştırılan bir 3D baskılı lens tarayıcısı tasarlanmaktadır. Şekil6.14'de, önerilen fiziksel katman güvenlik şeması görülmekte ve bunu izleyen paragraflarda yüz tanıma geri bildirimine dayalı ışık yönlendirmesine ilişkin testlerin sonucu verilmektedir.



Şekil 6.14. Uzaysal modülasyon kullanıldığında Eve tarafında algılanan sinyal genlikleri

Şekil 6.15'de, 25 mm çapındaki ($f = 25$ mm) bir plano-dışbükey lens çerçevesine bağlı ve serpantin bükülmeden (yaydan) oluşan bir lens tarayıcının tasarımı görülmektedir. Dış çerçeve boyutu, LED'lerin minyatür VLC test yatağına yerleştirildiği periyodun yarısı olan 5 cm x 5 cm'ye ayarlanmıştır. Elektromanyetik eyleme işlevini kolaylaştırmak için uzak kenara ve uzak köşeye iki Neodymyum mıknatıs (3 mm çap, 1 mm kalınlık) yerleştirilmiştir. Bobin yuvaları, iki farklı yönde elektromanyetik kuvvet oluşturmak için mıknatıslar hizasında dış çerçeve üzerinde tanımlanmıştır. Tarayıcının test yatağı ile entegrasyonu için opto-mekanik kafes çubukları kullanılmıştır. Tasarlanan tarayıcının boyutları aşağıdaki tabloda verilmiştir.



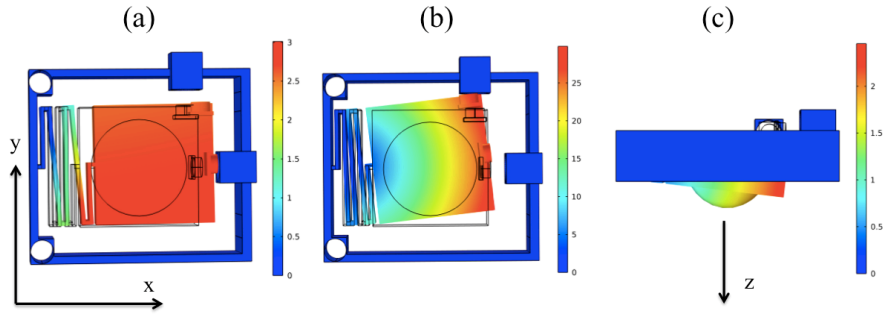
Şekil 6.15. (a)VLC için lens elektromanyetik eyleyici tasarımı ve (b) gerçekleştirilmesi

Yay genişliği, uzunluğu ve serpantin periyotlarının sayısı, ve çalıştırma yönlerinde benzer yay sabitleri elde edilerek bunlar merceğin kütesinden dolayı minimum sarkmayı sağlayacak şekilde ayarlanmıştır. Eyleyicilerin sonlu elemanlar analiz (COMSOL) sonuçları Şekil 6.16, burada yanal yönlerde (x ve y), 1 N ve z (dik) yönünde 0, 15 N'luk bir statik kuvvet, çerçevenin ağırlığını (toplam) temsil etmektedir. Merceğin merkezinden bakıldığında yay sabitlerini $k_x = 369$ N/m, $k_y = 65$ N/m olarak elde ettik. Ayrıca, $k_z = 110$ N/m'lik dikey sertlik, eyleyici lens ile yüklendiğinde mıknatıslar ve bobinler arasında minimum yanlış hizalama sağlayarak lens merkezinde < 1.5 mm'lik bir sarkma ortaya çıkarmaktadır. Tasarım, Poliaktik asit (PLA) üzerinde FDM (Ender Creality Pro 3.0 ile) kullanılarak basılmıştır. Benzetimlerde PLA üreticisinin spesifikasyonlarına uygun mekanik özellikler kullanılmıştır ($EE =$

	Sembol	Ebat
Çerçeve genişliği, uzunluğu	W	50 mm
Lens taşıyıcı genişliği	W_{lens}	30 mm
Yay uzunluğu	L_f	14 mm
Çerçeve yüksekliği	h	15 mm
Lens tutucu yüksekliği	h_{lens}	10 mm
Yay yüksekliği	h_f	10 mm
Yay genişliği	W_f	1 mm
Lens çapı	D	25 mm

Tablo 6.6. Lens eyleycisine ait ebatlar

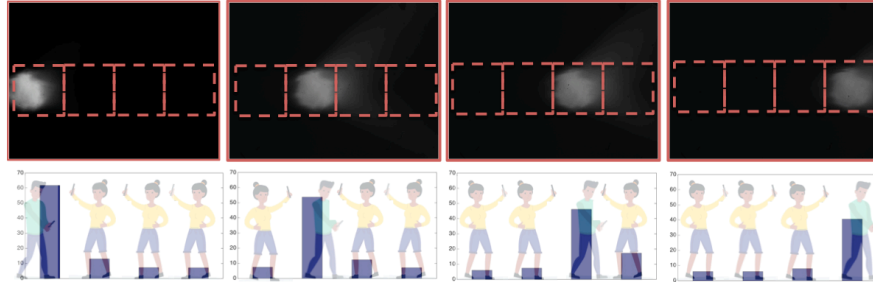
3.5 GPa, yoğunluk : $d = 1240 kg/m^3$).



Şekil 6.16. Statik hareket analizi ve FEM ortamında 3 farklı yön için yay sabitlerinin belirlenmesi

Eyleyicinin FDM ile üretimi, 25 mm odak uzunluklu lensin ve iki adet 100 mH indüktör bobininin presle oturtularak yerleştirilmesiyle gerçekleştirilmiştir. Neodimiyum mıknatıslar, standart epoksi kullanılarak lens çerçevesi kenarında ve köşesinde tanımlanan dikdörtgen prizma şeklindeki yapılara yerleştirilmiştir. Bobin-mıknatıs mesafesi, yay sabitlerindeki farkı gidermek ve ortamda hareketi neden olduğu voltajdaki değişimleri daha duyarlı biçimde elde edebilmek için x yönü, y yönünden daha yakın tutulmuştur. Üretilen eyleyici, minyatür VLC test yatağındaki tavana bağlanmıştır. 70 cm x 40 cm x 40 cm boyutlarındaki kapalı ortamın, tavanına 20 cm arayla Kartezyen tarzda yerleştirilmiş 4 LED'li düzeneğe 6 mm çapında iki kafes çubuk ile aktüatörün dış çerçevesi iliştilmiştir. Tabanda bir odaklanmayı elde etmek için lens merkezi LED'den 27 mm uzakta olacak şekilde ayarlanmıştır. Işın yönlendirmesi, bir CMOS kamera ile bobinlere uygulanan gerilime (veya akıma) göre odaklanmış ışının kaymasının gözlemlenmesiyle, ve/veya kamera yerleştirilirken test yatağı zeminindeki bir

grafik kağıdında odaklanılan noktanın gözlemlenmesiyle, karakterize edilmiştir, (Şekil6.17). Son olarak, OpenCV ve Python'un yüz tanıma kütüphaneleri kullanılarak bir yüz tanıma rutini uygulanmıştır. Kod, yasal bir alıcıyı (Albert Einstein'ın basılı fotoğrafı) şu şekilde kullanmaktadır: giriş veri kümesi kod, giriş veri kümesinde bulunan yüz özelliklerini, farklı hedeflerin görüntülerine dayalı Haar benzeri özellikler içeren bir örnek veri kümesiyle karşılaştırır. Hedefin yüz koordinatlarının belirlenmesinden sonra eyleyici için bu koordinatlar geri besleme olarak kullanılan doğrusal bir işlemle bobinlerin sürülmesinde kullanılacak gerilim değerlerine dönüştürülür.

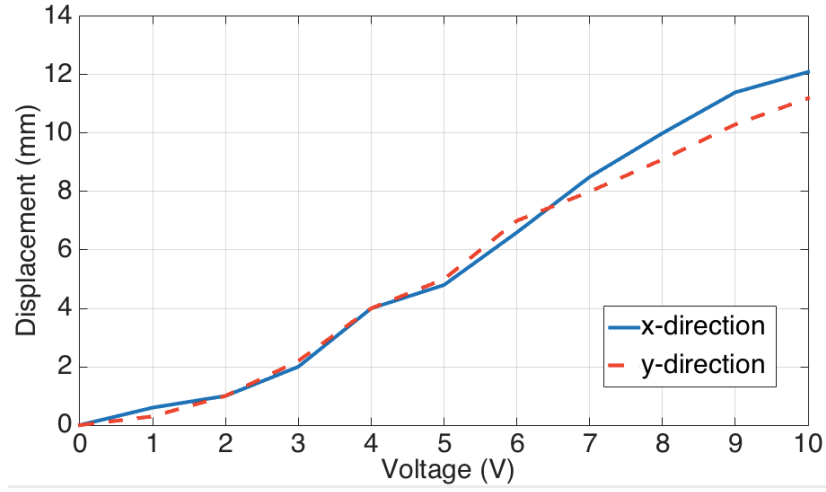


Şekil 6.17. Statik hareket analizi ve FEM ortamında 3 farklı yön için yay sabitlerinin belirlenmesi

6.4. Deney Sonuçları

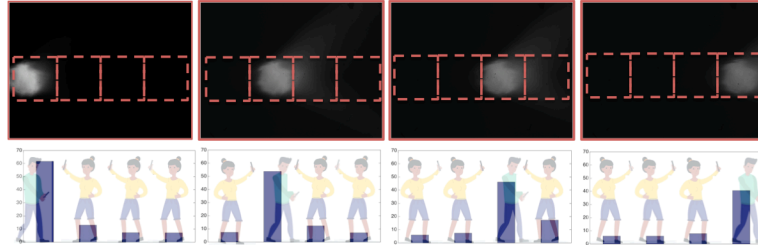
Yukarıda ana mimarisi verilen donanım kullanılarak, ilk olarak, Şekil6.18'de gösterildiği gibi, test yatağı tabanında oluşan odaklanılan noktanın, voltajın bir fonksiyonu olarak değişimi gözlemlenmiştir. Her iki eksen için 10V uygulanan voltaj (70 mA akım) ile 12 mm'lik bir yer değiştirme olduğu görülmektedir. Sistemin optik büyütmesine göre (1:13.5), eyleyicinin her iki yönde yaklaşık $900\mu m$ yer değiştirmesine karşılık geldiği saptanmıştır. Çok daha büyük bir optik büyütme elde etmek için, minyatür ve daha yüksek bir NA (numerik apertür) lensin kullanılmasıyla, tarama uzunluğunun doğrudan iyileştirilebileceği sonucuna varılmaktadır. Hareket ve tarama aralığı, daha yüksek güç tüketimi pahasına daha yüksek sürüş voltajları kullanılarak daha da geliştirilebilir.

Şekil6.19, bir eyleyiciyi yardımıyla tabana odaklanmış ışın demetinin, CMOS kamera (Thorlabs 1501M) ile dört bitişik konum için gözlemlerini göstermektedir. Söz konusu şekilde de gösterildiği gibi, yasal olmayan alıcılar kapalı ortamdaki diğer konumlarda bulunurken, yasal alıcının sırası ile soldan sağa hareket ettiği varsayılan bir senaryo test edilmiştir. Şekil6.19, yasal ve yasal olmayan alıcılara ulaşan ortalama parlaklık seviyelerini (kare yuvalar üzerinden ortalama) göstermekte olup, yasal olmayan alıcının, yasal alıcıdan önemli ölçüde düşük ışık yoğunluğuna (parlaklığa) sahip olduğu görülmektedir. Ayrıca, LED ve aktüatör arasındaki yanıl kaymanın (yönlendirme sırasında) Bob tarafından alınan yoğunluk



Şekil 6.18. Işın tarama genişliğinin voltaja göre değişimi

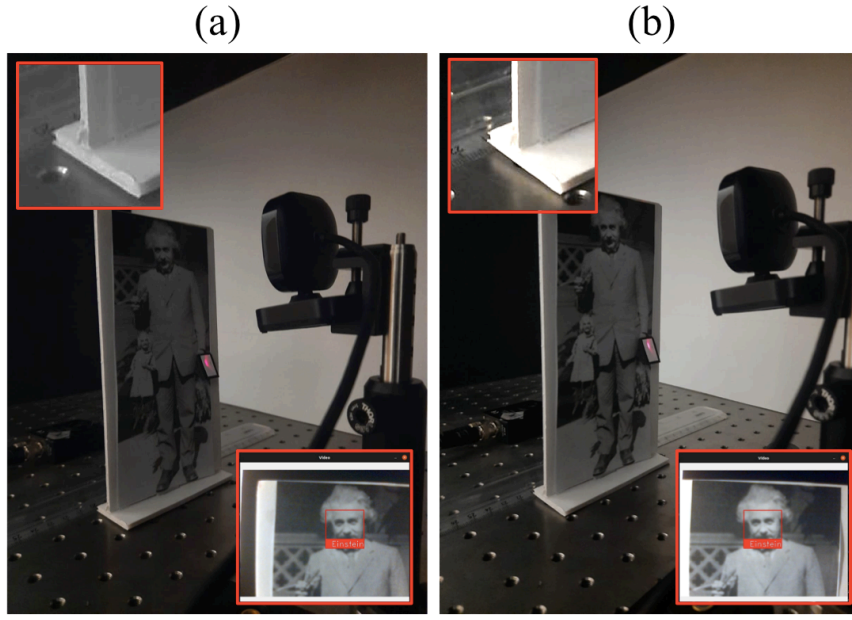
seviyesinde hafif bir değişikliğe neden olduğu sonucuna varılmıştır.



Şekil 6.19. Işın tarama deneyinde Bob ve Eve'in algıladığı ışık yoğunlukları

Tasarlanan donanımla ilgili ele alınan son deney, yüz tanıma geri bildirimine dayalı olarak Einstein hedefinin izlenmesinin gösterilmesini içermektedir Daha önce de belirtildiği gibi, kare merkezin (veya köşenin) piksel konumu, doğrusal bir ilişki yoluyla bobinin sürücü voltajına dönüştürülür. Hedefi 1 cm hareket ettirmek, algılanan yüzün 80 piksel kaymasıyla sonuçlanmıştır. Bu nedenle, Şekil6.20'den görüleceği gibi, belirlenen yüz koordinatının 0.11 V/pix kaymasının uygulanması (1 cm hareket için toplam 9 V), sunulan deneysel koşulların ve eyleyici için yönlendirmenin başarıyla başarıyla gerçekleştiği görülmektedir. Eyleyici gerilim ve akım değerleri, herhangi bir lens tarayıcı cihazında her iki eksen için ayrı ayrı önceden kalibre edilmesinin gerektiği anlaşılmaktadır.

Özetle, bu altbölümde, fiziksel katmada güvenli bir görünür ışıkla iletişim için 3B Baskı ile üretilmiş bir lens tarayıcı sunulmuştur. Tarayıcı, FDM tekniği ve PLA malzemesi kullanılarak üretilmiş ve bir yönlendirme sağlanabilmiştir. 10:1 minyatür (70 cm x 40 cm x 40 cm) VLC test yatağında 10 V sürücü voltajı ile 12 mm ışın yönlendirme gözlemlenmiştir.



Şekil 6.20. Hedef üzerinde ışın yönlendirme deneyine ilişkin düzenek. Hedef 1 cm kaydırıldığında, eyleyiciye uygulanan 9 Volt luk bir gerilim, ışının hedef ile birlikte kaymasını sağlamıştır.

Lens tarayıcı, yüz tanıma geri bildirim

7. TARTIŞMA

7.1. VLC’de MIMO SSK Tabanlı bir PLS Algoritması Geliştirilmesi

7.1.1. İdeal CSI’ye sahip MU-GSSK-SCD Sisteminin BER Başarımının Değerlendirilmesi

Şekil 5.1’da verilen ilk senaryoya göre elde edilen ve Şekil 5.4, 5.5, 5.6’de gösterilen benzetim sonuçlarında, Eve’in haberleşmesinin yüksek BER değerleriyle fazlaca bozulduğunu göstermektedir. Eve’in elde ettiği BER değerleri, hangi kullanıcıyı dinlediği fark etmesizin 0.5 seviyesindedir. Gözlemlediğimiz bir diğer sonuç ise Eve’in bulunduğu yerin BER’i üzerinde çok fazla bir etkisi olmadığıdır. Şekil 5.7, 5.8, 5.9, 5.10, 5.11, 5.12’te gösterilen Senaryo 2 ve Senaryo 3 için üretilmiş BER başarımlarına göre, denenmiş tüm senaryolar için yasal kullanıcılarda MU-GSSK-SCD ile elde edilen BER başarımları birbirine oldukça yakındır. Önerdiğimiz stratejinin, kullanıcıların nerde olduğuna fazla bağlı olmadan, yetkili kullanıcılara Eve’e kıyasla epey düşük BER sağladığı görülmüştür. Ayrıca, kullanılan iletişim tekniğinin Eve’in BER başarımını oldukça bozduğu gözlemlenmiştir. Şekil 5.13 ve 5.14’deki sonuçların gösterdiğine göre, Eve’in BER başarımı içmekanının neredeyse her noktasında 0.3’e eşit ya da daha fazladır. Bununla beraber, Eve dinlediği kullanıcıya yaklaştıkça BER’i 0.1 seviyelerine çıkabilmektedir. Kullanıcılar, Şekil 5.15 ve 5.16’de gösterildiği gibi birbirlerine yaklaştırıldıkça, Eve’in BER başarımının içmekanının büyük bir kısmında 0.5 seviyesinde olduğu görülmektedir. Ayrıca yine bu durumda, Eve’in düşük BER elde ettiği bölgenin bir önceki konfigürasyona göre epey küçüldüğü de gözlenmiştir. Bu sonuçlara göre, önerilen MU-GSSK-SCD stratejisi, özellikle kullanıcılar birbirine yakınsa, Eve’de oldukça kötü BER başarımıyla sonuçlanmaktadır.

7.1.2. İdeal Olmayan CSI’ye sahip MU-GSSK-SCD’nun BER Başarımının Değerlendirilmesi

Şekil 5.17’de gösterilen sonuçlara göre, elde edilen ML kestiriminin 3 dB SNR’da, 0.95ρ değerinde bir RMSE’ye ulaştığı ve RMSE’nin de 20 dB SNR’a kadar üstel biçimde 0.12ρ ’ya kadar düştüğü görülmektedir. Şekil 5.18’de gösterilen sonuçlara göre ise kullanıcılardaki kestirim hatası sonucunda, SNR’da 2–3 dB’lik bir kayıp gerçekleşmiştir. Bununla beraber, yüksek SNR bandında, içmekan VLC uygulamaları için yeterli olan 10^{-3} seviyelerinde bir hata oranı elde edilmiştir. Böylece, önerilen MU-GSSK-SCD sisteminin BER başarımının alıcısındaki CSI’in doğruluk oranına hassasiyetinin düşük olduğu söylenebilir.

7.1.3. MU-GSSK-SCD'nin Literatürle Kıyaslanması

Şekil 5.19'de gösterilen eğrilerden anlaşıldığı üzere, 8-PAM dost karıştırıcı sistemi, MU-GSSK-SCD sistemine göre her SNR değerinde daha düşük BER seviyesi ile çalışmıştır. Şekil 5.20'deki sonuçlara göre, MU-GSSK-SCD sistemi, örneğin 10^{-3} BER seviyesinde SNR'da 15 dB kazandırarak, yetkili kullanıcılara daha düşük BER sağlamıştır. Bu iki şekilde sunulan sonuçlardan hareketle, MU-GSSK-SCD sisteminin Eve'e daha yüksek, yetkili kullanıcılara da daha düşük BER sağlayarak, 8-PAM dost-karıştırıcı sistemine göre daha verimli ve efektif bir sistem olduğunu söyleyebiliriz. Kıyaslama sonuçlarına ek olarak, 8-PAM dost karıştırıcılı sisteminin çalışması için gerekli olan Eve'in CSI bilgisinin vericide tam doğru olarak hazır bulunduğu varsayımı pratik haberleşme sistemlerinde garanti yeceğini de belirtelim. Çünkü, Eve kendi kanal bilgisini vericiyle gönüllü olarak paylaşmayacaktır. Bu yüzden, Şekil 5.19'de gösterilen BER eğrileri, gerçek haberleşme uygulamalarında dost karıştırıcılı sistemi için bir üst sınır olabilir. Önerdiğimiz MU-GSSK-SCD sistemi ise Eve'in kanal durum bilgisine ihtiyaç duymadığından daha gerçekçi bir varsayıma dayanmaktadır.

7.1.4. Karmaşıklık Analizi Değerlendirmesi

Önerilen MU-GSSK-SCD'nin hesaplama yükü, erişim noktasında ön kodlama sırasında ve kullanıcı tarafında sezimleme yapılırken en yüksektir. Önceki kısımlarda anlatıldığı gibi, erişim noktası yetkili kullanıcılara, onların kanal durum bilgilerini kullanarak doğrusal bir sifıra zorlayan ön kodlayıcı aracılığıyla iletim yapmaktadır. Bu ön kodlayıcı, (3.24) denkleminde hareketle

$$\mathbf{P}_k = \rho \tilde{\mathbf{H}}_k \left(\tilde{\mathbf{H}}^T \tilde{\mathbf{H}} + \epsilon \mathbf{I}_{N_a} \right)^{-1} \tilde{\mathbf{H}}^T \mathbf{v}_{S,s}, \quad (7.1)$$

şeklinde tanımlıdır. Burada, k 'inci kullanıcı ile erişim noktası arasındaki kanal matrisi $\tilde{\mathbf{H}} \in \mathbb{R}^{N_r \times N_a}$ ile ve ışık şiddeti normalizasyon katsayısı ρ ile gösterilmiştir. ϵ ise düzenleme parametresidir. Yukarıdaki ifadede, matris çarpımı yaklaşık $\mathcal{O}(N_r N_a^2)$, matrisi tersine alma işlemi de yaklaşık $\mathcal{O}(N_a^3)$ adet operasyon gerektirmektedir. Alıcılar tarafında ise tek akışla gelen bilgi, düşük karmaşıklıkla sezimlenmektedir. k 'inci kullanıcı tarafından alınmış sinyal olan

$$\mathbf{y}_k = \mathbf{s}_k + \mathbf{n}_k, \quad k = 1, 2, \dots, K, \quad (7.2)$$

ifadesine göre sezimlemeden gelen hesaplama karmaşıklığı K sayısı ile doğrusal olarak artmaktadır. Bu ifadede, \mathbf{s}_k , (3.24) denkleminde de belirtildiği gibi k 'inci kullanıcı tarafından gözlenen yollanmış sinyaldir. Bu nedenle, kullanıcılarda sinyallerin sezimlenmesinin hesaplama

karmaşıklığı, M_k , k 'inci kullanıcının aldığı sinyal olmak üzere, $\mathcal{O}(KM_kN_a)$ ile bulunur. Özetle, bu kısımda önerilen MU-GSSK-SCD tekniğinin karmaşıklığı yaklaşık $\mathcal{O}(N_rN_a^2+N_a^3+KM_kN_a)$ olur.

7.2. VLC'de MIMO SSK Tekniğine Dayanan PLS Algoritmasına İlişkin Gizlilik Oranlarının (Secrecy Rates) Değerlendirilmesi

Fig 5.21da gösterilen sonuçlara göre, kullanıcıların gizlilik oranları 0 – 3 dB SNR seviyelerinde 2 – 2.5 bpcu iken SNR'daki 1 dB'lik artışa karşılık yaklaşık 0.16 bpcu artmaktadır. SNR 6 dB seviyelerindeyken, kullanıcıların gizlilik oranları 8-QAM haberleşmesi için en yüksek değer olan 3 bpcu'ya çok yaklaşmıştır. Şekil 5.24deki sonuçlara göre, kullanıcılar tek PD ile donatıldığında, en yüksek gizlilik oranı, 27 dB gibi yüksek sinyal-gürültü oranı (signal-to-noise ratio (SNR)) değerinde bile, her kanal kullanımında kullanıcı başına 3 biti çok az aşabilmiştir. Kullanıcılardaki alıcı sayısı bir artırılarak $N_r = 2$ PD kullanıldığında, ulaşılabilen en yüksek gizlilik oranı, 0 dB gibi düşük SNR değerinde bile, her kanal kullanımında kullanıcı başına 6 bite çok yaklaşmıştır. Bu değer gizlilik oranının alabileceği en yüksek değerdir. Ayrıca, kullanıcılar, 4 PD ile haberleşme yaptığında, gizlilik oranı bölgesi şekilde görüldüğü gibi, her kanal kullanımında kullanıcı başına 6 bit üst sınırıyla çakışmaktadır. Bu sonuçlara göre, alıcı devrelerindeki PD sayısının, haberleşmenin gizlilik oranına etkisinin çok fazla olduğu sonucuna varılmaktadır.

7.3. VLC NOMA Tabanlı PLS Algoritmasının Değerlendirilmesi

Şekil 5.25 ve 5.26'de gösterilen sonuçlara göre, Eve'in BER değerleri tüm SNR seviyeleri için önemli ölçüde büyükken, yasal kullanıcılar 20 – 25 dB SNR bandında 10^{-5} BER seviyesine düşebilmektedir. Eve'in BER başarımının, hangi kullanıcının izinsiz olarak dinlendiğinden bağımsız olduğu gözlemlenmiştir. BER başarımı, tüm SNR değerlerinde 0,5 seviyesinde olduğu için, Eve'in tarafında çözülen bilgi, anlamlandırılabilir olmaktan uzaktır. BER başarım sonuçları her iki senaryo için de benzerdir, bu da önerilen PLS önkodlayıcının neden olduğu jamming sinyalinin, (3.65), PLS'i etkin bir şekilde sağladığını gösterir. Şekil 5.27'de gösterilen sonuçlara göre diğer değişkenler sabitken Bob 1'e atanan SNR Bob 2'ye atanandan daha küçük olduğundan, Bob 1 BER değerleri, Bob 2'nin BER değerlerinden daha yüksek elde edilmiştir. Yine de Bob 1, 30 dB'de 10^{-4} BER seviyesinde haberleşme yapabilmektedir. Bu senaryoda da Eve'in iletişiminin yüksek BER değerleri nedeniyle oldukça bozulduğu gözlemlenmiştir. Bu sonuçlar, Şekil 5.25 ve 5.26'deki sonuçlarla birleştiğinde, önerilen PLS ön kodlama algoritmasının, yasal kullanıcıların Alice'e göre simetrik ya da asimetric olarak konumlanmasından bağımsız olarak, güvenli iletişim sağladığını göstermektedir.

Şekil 5.25'da gösterildiği üzere her iki kullanıcının iletişim başarımının benzer olduğu gözlemlenmiştir. Bu sonuçlar, PD sayısının artırılmasının, önerilen MIMO-NOMA-VLC sisteminin BER'lerini iyileştirdiğini göstermektedir, ki bu durum artan çeşitleme kazancı nedeniyle beklenmektedir. Şekil 5.28'de, Eve'in BER başarımı da $N_r = 2$ için dahil edilmiştir. Görüldüğü üzere, bu BER başarımı önemli ölçüde bozulmuştur. Bu sonuçlar, önerilen PLS ön kodlama algoritmasının, PD sayısı düşük olduğunda bile yasal kullanıcılar için yeterli BER seviyelerini korurken PLS'yi de sağladığını göstermektedir.

7.3.1. VLC-NOMA Tabanlı PLS Algoritmasının Gizlilik Analizi Değerlendirmesi

Şekil 5.29'da gösterilen sonuçlara göre, analitik olarak türettiğimiz gizlilik alt limitlerinin denenmiş tüm SNR değerleri için, elde edilen DCMC kapasitesine oldukça yakın olduğunu belirtelim. Türetilen üst limitler de düşük SNR seviyeleri için faydalı olabilecek sonuçlar vermektedir. İkinci olarak da, ele alınan senaryoda, 3 ve 4 bpcu seviyelerindeki gizlilik oranları, sırasıyla 13 ve 22 SNR seviyelerinde ulaşılabilir olmaktadır. Ayrıca alt limit eğrisinin gösterdiğine göre, önerilen PLS önkodlama stratejisi kullanıldığında, 3 bpcu değerinde bir gizlilik oranı en az 20 dB SNR'da hali hazırda ulaşılabilir olmaktadır. Bu senaryoda iletim hızının sembol başına 5 bit olduğu da göz önüne alındığında, elde edilen başarımların önerilen NOMA tabanlı PLS önkodlama stratejisinin çok kullanıcılı VLC sistemine yeterli PLS sağladığını göstermektedir.

7.4. GLIM OFDM tabanlı PLS Algoritmasının Değerlendirilmesi

Bölüm de GLIM-OFDM için geliştirilen, kanal önkodlama ve kaynakla yasal alıcı arasında gizli anahtar değişimine dayanan yeni özgün PLS algoritmasının fiziksel katmanda son derece etkili bir güvenlik ve gizlilik sağladığı gösterilmektedir. Farklı yaklaşımlar kullanılarak analitik yoldan bulunan algoritmanın ulaşılacağı en büyük gizlilik oranları da bu sonucu doğrulamaktadır. Ayrıca, en küçük-karesel-ortalama (minimum-mean-square estimation (MMSE)) kestirim yöntemi ile GLIM-OFDM'de ortaya çıkan MIMO yapıdaki kanallar için önerilen yeni kanal kestirim tekniğinin de çok etkili bir biçimde çalıştığı bilgisayar benzetimleriyle gösterilmiştir. Son olarak, sistemin sağladığı fiziksel katman güvenliğini daha da güçlendirmek için, gizli anahtar değişimi (secret key exchange)'ye dayanan yeni bir güvenlik algoritması sistem dahil edilmiştir. Bob ve Eve'nin BER başarımları, gizli anahtarlı ve gizli anahtarsız iki konfigürasyon için karşılaştırılmış ve Eve'nin BER başarımının bir gizli anahtarın varlığında en düşük düzeyi olan 0.5'e yaklaştığı bilgisayar benzetimleriyle gösterilmiştir. Ayrıca, Bob ve Eve'nin erişebilecekleri gizlilik oranları analitik olarak elde edilmiş ve Bob'un aynı SNR aralığında gerekli spektral hızına ulaşırken, Eve'in bu spektral hıza ulaşmaktan çok uzak kaldığı sonucuna varılmıştır. Buna ek olarak, ulaşılabilir gizlilik oranları, frekans ve zaman bölgelerinde karşılaştırılmıştır ve zaman bölgesi yaklaşımının ulaşılabilir kapasite üzerinde

bir üst sınır sağladığı açıkça gösterilmiştir.

7.5. PLS-VLC Sistemlerde Kanal Kestirim Algoritmasının Değerlendirilmesi

Projede tasarlanan PLS-VLC sistemlerin iletişim yaptığı görünür ışık kanallarının kestirimiyle ilgili hızlı, hesaplama karmaşıklığı ve kestirim hataları düşük yeni bir kanal kestirim algoritması geliştirilmiştir. Algoritma özellikle OFDM tabanlı PLS-VLC sistemlerinde yetkili ve yetkili olmayan kullanıcılarla kaynak (verici) arasında oluşan çok sayıda kapalı ortam kızılötesi/görünür-ışık kanallarının, fiziksel özelliklerinin de göz önüne alarak, alıcılarda en iyi biçimde kestirilmesinde çok etkili çalıştığı yapılan yoğun bilgisayar benzetimleri sonucunda görülmektedir. Ayrıca, kanal kestirim hatalarının ve alıcıda kestirilen kanal bilgilerinin kaynağa iletimindeki gecikmelerin tasarlanan sistemin bit hata başarımına (BER) etkileri analitik yollardan ve bilgisayar benzetimleriyle araştırılmıştır. Özellikle projede gözönüne alınan GLIM-OFDM sistemlerde kanal kestirim algoritmalarının geliştirilmesiyle ilgili literatürde çok az sayıda olduğu görülmüştür. Bunun temel nedenleri şöyle açıklanabilir; (i) VLC'de iletilen sinyallerin gerçel ve pozitif değerli olma kısıtlılığı (ii) ışığın kapalı ortam (indoor) içinde yayılımında, kapalı ortamın geometrik yapısı ve bu ortamı içindeki materyallere (mobilyaların, duvar kaplamasının türü ve konumu vs.) göre yayılım karakteristiği değişebilmesi, ve dolayısıyla ışığın radyo dalgalarından farklı biçimde yayılıma sahip olması nedeniyle optik kanal modellerinin geleneksel radyo frekanslı kablosuz haberleşme kanal modellerinden farklı olması. (iii) VLC'ye ilişkin optik kanal modellerin ve özellikle mobil VLC kanallarının standartları daha yeni oluşmaya başlamış ve VLC'de yapılan çalışmaların hemen hepsinde sabit bir kapalı ortam için optik kanalın deterministik ve noktadan-noktaya görüş çizgisi doğrultusunda (line-of-sight) yayıldığı varsayılmış olması. Ancak, çok yüksek veri iletim hızlarına çıkıldıkça ve kullanıcıların üzerlerinde taşıdıkları alıcılardaki fotodetektörlerin yönlerinin ve konumlarının kullanıcının hareketine bağlı sürekli değişmesi nedeniyle, bu varsayım günümüz VLC kanalları için geçerliliğini yitirmektedir. Bu nedenle, sabit bir kapalı ortamda aynı alıcı algoritmasını kullanan ve rastlantısal (random) konuma sahip kullanıcıların olduğu varsayıldığında her bir kullanıcının haberleşmesini etkileyen kanalların bir rastlantısal optik kanal modeline uyacağı kesindir. Dolayısıyla, VLC sistemlerine ilişkin optik kanalların istatistiksel modellerini ortaya koymadıkça, kanal kestirimi için literatürde var olan kanal kestirim yöntem ve tekniklerin VLC sistemlerine doğrudan uygulaması mümkün olamayacaktır.

Bu projede PLS yetenekli GLIM-OFDM'de kanal kestirimiyle ilgili yürütülen çalışmalarda VLC kanallarının kestirimi, GLIM-OFDM'in zaman bölgesinde oluşan 4×4 MIMO kanallarının kestirimi problemine indirgenmektedir. Bu kapsamda hem normal ve hem de PLS yeteneğe sahip GLIM-OFDM için yeni bir kanal kestirim algoritması teklif edilmektedir. Ayrıca, bu amaç için gerekli MIMO kanal çıkışıdaki zaman-bölgesi OFM örneklerinin belirlenmesi için

yeni bir Bayes temelli enküçük-karesel –ortalama (Bayesian minimum-meansquare (MMSE)) kestirimcisi tasarlanmaktadır. Yapılan bilgisayar benzetimler, önerilen kanal kestirim algoritmasının çok etkili olduğu ve sistemin kestirimde yapılan hatalara çok dayanıklı olduğunu göstermiştir.

7.6. Laboratuvar ortamında PLS-VLC Sistemin Donanımsal Tasarımıyla ilgili Değerlendirmeler

Projenin ilk aşamasında, VLC'de fiziksel katman güvenliğini gerçekleştirecek bir sistem laboratuvar ortamında yazılım tabanlı radyo birimleri ve LED kaynak fotodetektör hedefler kullanılarak gerçekleştirilmektedir. 4 LED'li bir bilgi kaynağı, 1 yetkili kullanıcı ve 1 yetkili olmayan kullanıcının oluşturduğu kapalı ortam VLC sisteminde, vericide yetkili olmayan kullanıcı doğrultusunda bir karıştırma (jamming) sinyal oluşturarak, bu kişinin mesajı doğru olarak almasını önlemeye yönelik donanım çalışmaları yapılmıştır. Ayrıca güvenlik açığının ortadan kaldırılması için haberleşmeyi sağlayan sistemin fiziksel özelliklerini değiştirerek verici ile yasal alıcı arasındaki sinyal iletimi sağlanmış ve bu sinyalin, çevrede bulunan yasal olmayan alıcılar tarafından algılanması engellenmiştir. Bu güvenlik açığının, haberleşmenin fiziksel katman kısmında ortadan kaldırılmış olması nedeniyle haberleşmenin daha üst katmanlarında herhangi ek bir önlem alınmasına da gerek kalmamaktadır.

Projenin son aşamasında ise, projede geliştirilen uzamsal modülasyon ile önkodlamaya dayanan özgün ve yeni PLS algoritması, literatürde ilk kez, donanımsal olarak gerçekleştirilmiştir. Bu mimariyle tasarlanan PLC-VLC sistem donanımı ile, kaynaktan LED'lerle iletilen bilginin yasal alıcı ve gizli dinleyici arasında sağlam ve güvenli iletişim sağladığı deneysel olarak gösterilmekte ve ölçüm sonuçları, elde edilen gizlilik iyileştirmesini doğrulamaktadır. Donanımsal çalışmada, 4 LED'li düşük maliyetli 70 cm × 40 cm × 40 cm minyatür oda modelinin test yatağı sunulmaktadır. Test yatağı, geleneksel bir odanın 10:1 küçültülmüş bir kopyasıdır ve sürücü ve opto-elektronik algılayıcı bileşenleri hariç, toplam fiyatı 10\$'ın altında olan basit ofis malzemeleriyle oluşturulabilir. Test yatağı uygun maliyetli olmakla birlikte, i) optik bileşenlerin entegrasyonuna, ii) istenilen pencere ve kapı desenlerinin farklı karton renk tonlarında oyularak farklı renkli duvarlardan yansımaların ve dış ışık kaynaklarının etkisinin gözlemlenmesine de olanak tanımaktadır .

8. SONUÇ VE ÖNERİLER

Bu projede temel olarak türlü mimarilere sahip VLC sistemler için bir takım yeni ve özgün fiziksel katman güvenlik ve kanal kestirim algoritmaları geliştirilmiş ve bunlar donanımsal olarak gerçekleştirilmiştir. VLC-MIMO-SSK, VLC-NOMA, VLC-GLIM OFDM sistemleri için vericide kanal önkodlamasına dayanan bu PLS algoritmalarının mükemmel biçimde gizliliği sağladığı sonucuna varılmıştır. Diğer bir deyişle, yasal kullanıcılara bilgi iletiminde ulaşılan BER başarımı özellikle BER çalışma aralığı olan 25-35 dB aralığında 10^{-6} gibi çok yüksek bir başarımla düzeyine erişirken, yasal olmaya kullanıcıların her SNR düzeyindeki BER başarımlarının 0.5 gibi en düşük düzeyde kaldığı görülmüştür. Geliştirilen PLS algoritmalarının tümü, yalnızca yasal olmayan kullanıcıya bilginin bozularak gitmesini sağlayan fakat yasal kullanıcılara bilgi iletiminde hatalara neden olmayan bir dost jamming (friendly jamming) gürültünün üretilmesine dayanmaktadır. Literatürde önerilen diğer jamming sinyal ile PLS'yi gerçekleyen ve sistemin güç randımanında (power efficiency) önemli ölçülerde düşüşlere neden olan tekniklerden farklı olarak, sözkonusu çalışmada önerilen tüm PLS algoritmaları jamming sinyal üretimi için ayrıca güç harcamadığı için, sistemin güç randımanı geleneksel PLS algoritmalarına oranla ço daha yüksek olmaktadır. Ek olarak, önerilen güvenlik algoritmaları ile çalışan sistemlerde, türetilen ulaşılabilir gizlilik bölgeleri (achievable secrecy regions), bilgiyi birden fazla yasal kullanıcıya etkili ve güvenli bir şekilde ilettiğini ve elde edilen BER başarımlarına göre de aynı bilgiyi Eve'in çözmesinin engellendiği kanıtlanmaktadır. Ayrıca, kaynaktan ideal olmayan CSI ile yapılan iletimde, kullanıcıların BER başarımlarının parametre kestirim hatalarına pek duyarlı olmadığı sonucuna varılmış ve aynı SNR seviyesi için yasal kullanıcılar arasındaki mesafe arttıkça gizlilik bölgesinin genişlediği ve kullanıcı ayırımı 90 cm'ye ulaştığında 0 dB SNR'de tam gizliliğin ulaşılabilir olduğu görülmüştür. Diğer taraftan, projede çok kullanıcılı VLC sistemleri için NOMA tabanlı bir PLS Önkodlama stratejisi önerilmiştir. Önerilen önkodlayıcı, Eve oldukça bozulmuş bir VLC sinyali alırken, yasal kullanıcıların, kullanıcılar arası girişimden arındırılmış bir sinyal alması sağlanacak şekilde tasarlanmıştır. Önerilen sistemle ulaşılabilir gizlilik oranları ve ilgili alt-üst limitleri de analitik olarak kapalı formda türetilmiştir. Bu oranlar, bilgisayar benzetim sonuçlarıyla doğrulanmıştır. PLS başarımları, elde edilen BER grafikleri ve gizlilik sonuçlarıyla ortaya konmuştur. Benzetim sonuçlarında, hem oldukça yüksek gizlilik oranı elde edildiği hem de Eve'in birçok kullanıcı konumlaması için 0.5 seviyelerinde BER elde edebildiği görüldüğünden, önerilen önkodlayıcının VLC sisteminde PLS sağladığı gösterilmiştir.

Son olarak projede, literatürde ilk kez VLC'de kanal önkodlamaya (channel precoding) dayanan PLS algoritmalarını donanımsal olarak gerçeklemek için, odak düzlemi dizilerine dayalı minyatür (10:1) bir test yatağı düzeneği tasarlanmıştır. Bu düzenek yardımıyla 4 LED ve 2 PD'den oluşan bir uzamsal (spatial) modülasyonlu iletişim sisteminde PLS algoritması tasarlanmıştır. Yapılan deneysel çalışmalar, PLS algoritmasının kuramsal sonuçlarda

varılan BER başarımına yaklaştığını gösterilmiştir.

Projede, ileriye dönük kuramsal çalışmalar ve donanımsal gerçekleştirme kapsamında, **(i)** 6G haberleşmede kablosuz optik iletişim sistemlerinin ve projede önerilen PLS algoritmalarının uygulanabilmesi ve standartlarının oluşturulması, ve **(ii)** şu anda laboratuvar ortamında gerçekleştirilen PLS-VLC sisteminin daha gelişmiş bir prototipinin hazırlanarak bir ürüne dönüştürülmesi ile ilgili çalışmaların yapılması planlanmaktadır.

REFERANSLAR

1. T. Komine and M. Nakagawa, "Fundamental analysis for visiblelight communication system using LED lights," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 100–107, Feb. 2004.
2. S. Dimitrov and H. Haas, *Principles of LED Light Communications: Towards Networked Li-Fi*. Cambridge, U.K.: Cambridge Univ. Press, 2015.
3. H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 15, 2016.
4. IEEE Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Wireless Optical Communication Using Visible Light, IEEE Computer Society, IEEE Standard 802.15.7-2011, 2011.
5. X. Li, F. Jin, R. Zhang, J. Wang, Z. Xu, and L. Hanzo, "Users first: User-centric cluster formation for interference-mitigation in visible-light networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 39–53, Jan. 2016.
6. H. Ma, L. Lampe, and S. Hranilovic, "Coordinated broadcasting for multiuser indoor visible light communication systems," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3313–3324, Sep. 2015.
7. L. Yin, W. O. Popoola, X. Wu, and H. Haas, "Performance evaluation of non-orthogonal multiple access in visible light communication," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5162–5175, Dec. 2016.
8. A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
9. I. Csiszär and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
10. A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4449–4461, Oct. 2009.
11. J.-B. Wang, Q.-S. Hu, J. Wang, M. Chen, and J.-Y. Wang, "Tight bounds on channel capacity for dimmable visible light communications," *J. Lightw. Technol.*, vol. 31, no. 23, pp. 3771–3779, Dec. 1, 2013.

12. A. Chaaban, J. M. Morvan, and M. S. Alouini, "Free-space optical communications: Capacity bounds, approximations, and a new sphere-packing perspective," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1176–1191, Mar. 2016.
13. S. Dimitrov and H. Haas, "Information rate of OFDM-based optical wireless communication systems with nonlinear distortion," *J. Lightw. Technol.*, vol. 31, no. 6, pp. 918–929, Mar. 15, 2013.
14. A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.
15. A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Signal Process.*, vol. 64, no. 24, pp. 6501–6516, Dec. 2016.
16. G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, Mar. 2016.
17. Zeng L., O'brien D., Minh H., Faulkner G., Lee K., Jung D., Oh Y., Won E., High Data Rate Multiple Input Multiple Output (MIMO) Optical Wireless Communications Using White LED Lighting, *IEEE J. Sel. Areas Commun.*, 27, 9, 1654–62, (2009).
18. Dambul K., O'brien D., Faulkner G., Indoor Optical Wireless MIMO System With An Imaging Receiver, *IEEE Photonics Tech. Lett.*, 23, 2, 97–99, (2011).
19. R. Mesleh, R. Mehmood, H. Elgala, H. Haas, "Indoor MIMO Optical Wireless Communication Using Spatial Modulation", *IEEE Int. Conf. Commun.(ICC)*, Cape Town-South Africa, (2010).
20. K. Park, Y. Ko, M. Alouini, "On the power and offset allocation for rate adaptation of spatial multiplexing in optical wireless MIMO channels", *Int.Wireless Commun. and Mobile Computing Conf. (IWCMC)*, Istanbul-Turkey, (2011), pp. 141–146.
21. R. Mesleh, H. Haas H., S. Sinanovic S., C. Ahn, S. Yun, "Spatial Modulation", *IEEE Tran. on Veh.Tech.*, 57, 4, pp. 2228–41, (2008).
22. E. Basar, U. Aygolu, E. Panayirci and H.V. Poor, "Space-time block coded spatial modulation", *IEEE Trans. Communications*, vol.59, no.3, pp. 823-832, Mar. 2011.
23. E. Basar, U. Aygolu, E. Panayirci and H.V. Poor, "New Trellis Code Design for Spatial Modulation",

IEEE Trans. Wireless Communications, vol. 10, no. 8, Aug. 2011.

24. E. Basar, U. Aygolu, E. Panayirci and H.V. Poor, "Super-orthogonal trellis coded spatial modulation", IET Communications, vol. 6, no. 17, pp. 2922-2932, Nov. 2012.
25. J. Jeganathan, S. Ghayeb, L. Zczecinski, A. Ceron, "Space-Shift Keying Modulation For MIMO Channels", IEEE Trans. Wireless Commun., 8, 7, 3692-3703, (2009).
26. A. Yesilkaya, E. Basar, F. Miramirkhani, E. Panayirci, M. Uysal, H. Haas, "Optical MIMO-OFDM with generalized LED index modulation", IEEE Trans. Commun., vol.65, no. 8, pp. 3429-3441, May 2017.
27. R. Mesleh, H. Elgala, H. Haas, "Optical Spatial Modulation", J. Opt. Commun. Netw., 3, 3, 234-44 (2011).
28. A. Yesilkaya, T. Cogalan, E. Panayirci, H. Haas and H. V. Poor, (Best paper award), "Achieving Minimum Error in PAM Based MISO Optical Spatial Modulation Systems", IEEE Int. Conf. Commun. (ICC2018), Kansas City, USA, 2018.
29. A. Yesilkaya, F. Miramirkhani, E. Basar, E. Panayirci and M. Uysal, "Performance of MIMO enhanced unipolar OFDM with realistic indoor visible light channel models", IEEE Workshop on Optical Wireless Communication (co-located with IEEE-WCNC'16), Doha, Qatar, April 2016.
30. O. Hassan, E. Panayirci, H. V. Poor, and H. Haas, "Physical-Layer Security for Indoor Visible Light Communications with Space Shift Keying Modulation", IEEE Globecom 2018, 9-13 Dec. 2018, Abu Dhabi, UAE.
31. F. Wu, L-L. Yang, W. Wang and Z. Kong, "Secret precoding-aided spatial modulation", IEEE Com. Letters, vol. 19, no. 9, pp. 1544-1547, Sept. 2015.
32. A. Mostafa and L. Lampe, "Physical-layer security for visible light communications," IEEE ICC 2014, Optical Networks and System Workshop, pp. 3342–3347, Sydney, Australia, 10-14 June 2014.
33. A. Mostafa and L. Lampe, "Securing Visible Light Communications via Friendly Jamming," IEEE Globecom2014, Optical Wireless Communications Workshop, pp. 524–529, Sydney, Australia, 10-14 June 2014.

34. N. Horiike, E. Okamoto and T. Yamamoto, "A downlink non-orthogonal multiple access scheme having physical layer security", *EURASIP J. Wireless Commun. and Networking*, 2018: <https://doi.org/10.1186/s13638-018-1156-8>, 2018.
35. A. Arafa, E. Panayirci, and H. V. Poor, "Relay-Aided Secure Broadcasting for VLC", *GlobalSIP 2018*, Nov. 26–28, 2018, Anaheim, California, USA
36. F. Miramirkhani, M. Uysal, and E. Panayirci, "Novel channel models for visible light communications", *Invited Paper, SPIE Photonics West*, San Francisco, CA, USA, Feb. 2015.
37. A. Yesilkaya, F. Miramirkhani, E. Basar, E. Panayirci, M. Uysal, "Performance of MIMO Enhanced Unipolar OFDM with Realistic Indoor Visible Light Channel Models", *IEEE WCNC2016 Workshop on Optical Wireless Communications*, Doha, Qatar, Apr. 3-6, 2016.
38. M. Uysal, F. Miramirkhani, O. Narmanlioglu, T. Baykas, E. Panayirci, "IEEE 802.15.7r1 Reference channel models for visible light communications", *IEEE Comm. Magazine*, vol. PP, no. 99, pp. 1, Jan. 2017.
39. F. Miramirkhani, O. Narmanlioglu, M. Uysal and E. Panayirci, "A Mobile Channel Model for VLC and Application to Adaptive System Design", *IEEE Communications Letters*, vol. 21, no. 5, pp. 1089-1038, Jan. 2017.
40. E. Başar, Ü. Aygölü, E. Panayirci, H. V. Poor, "Performance of Spatial Modulation In The Presence of Channel Estimation Errors", *IEEE Commun. Letters*, 16, 2, 176-79, (2012).
41. Jovicic A, Li J and Richardson T. 2013 Visible light communication: Opportunities, challenges and the path to market *IEEE Commun. Mag.* 51 26–32.
42. Haas H, Yin L, Wang Y and Chen C. 2016 What is LiFi? *J. Light. Technol.* 34 1533–44.
43. Benzetimler A, Panayirci E and Vincent Poor H. 2019 Relay-Aided Secure Broadcasting for Visible Light Communications *IEEE Transactions on Communications* vol 67pp 4227–39.
44. Büyükçorak S, Topal O A, Ferhanog O and Karabulut Kurt G. 2020 Mixture model and its experimental validation for visible light communications *Electron. Lett.* 56 559–62
45. Huang Z, Gao Z and Sun L. 2017 Anti-Eavesdropping Scheme Based on Quadrature Spatial Modulation *IEEE Commun. Lett.* 21 532–5

46. Wang F, Li R, Zhang J, Shi S and Liu C 2019 Enhancing the secrecy performance of the spatial modulation aided VLC systems with optical jamming *Signal Processing* 157 288–302.
47. Yin L and Haas H. 2018 Physical-Layer Security in Multiuser Visible Light Communication Networks *IEEE J. Sel. Areas Commun.* 36 162–74.
48. Cogalan T, Haas H and Panayirci E 2020. Optical spatial modulation design *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* 378.
49. Yesilkaya A, Basar E, Miramirkhani F, Panayirci E, Uysal M and Haas H. 2017 Optical MIMO-OFDM with Generalized LED Index Modulation *IEEE Transactions on Communications* vol 65pp 3429–41.
50. Panayirci E, Yesilkaya A, Cogalan T, Poor H V and Haas H. 2020 Physical-Layer Security with Optical Generalized Space Shift Keying *IEEE Trans. Commun.* 68 3042–56.
51. H. Wu, Q. Wang, J. Xiong, M. Zuniga, SmartVLC, 2020, “Co-Designing Smart Lighting and Communication for Visible Light Networks”, *IEEE Trans. Mob. Comput.* 19, 1956–1970. <https://doi.org/10.1109/TMC.2019.2915220>.
52. P. Dhulipalla, M. Kang, T. Kim, N. Tan, S. Govindasamy, M.B. Raunications System, 2019 Int. Conf. Comput. Inf. Telecommun. Syst. 1–6haim, 2019, An Integrated Visible-Light and Radio Frequency Comm.
53. O.R.B. Sayco, A.C. Gordillo, 2029, “Design and Implementation for a USRP - Based Visible Light Communications Transceiver”, *Proc. - 2019 UNSA Int. Symp. Commun. UNSA ISCOMM 2019.* (2019). <https://doi.org/10.1109/UNSAISC.2019.8712826>.
54. Chen et al., 2016. Chen, C., Basnayaka, D. A., and Haas, H. (2016). “Downlink performance of optical attocell networks” . *J. Lightw. Technol.*, 34(1):137–156.
55. Al-Kinani, A., Wang, C., Zhou, L., and Zhang, W. (2018). Optical wireless communication channel measurements and models. *IEEE Commun.Surv. Tutor.*, 20(3):1939–1962.
56. Kahn and Barry, 1997. Kahn, J. M. and Barry, J. R. (1997). “Wireless infrared communications”. *Proc. IEEE*, 85(2):265–298.
57. Burchardt et al., 2014. Burchardt, H., Serafimovski, N., Tsonev, D., Videv, S., and Haas, H.

- (2014). VLC: Beyond point-to-point communication. *IEEE Commun. Mag.*, 52(7):98–105.
58. Shi et al., 2019. Shi, J., He, J., Wu, K., and Ma, J. (2019). “Enhanced performance of asynchronous multi-cell VLC system using OQAM/OFDM-NOMA”. *J. Lightw. Technol.*, 37(20):5212–5220.
59. Yang et al., 2018. Yang, H., Chen, C., and Zhong, W. (2018). “Cognitive multi-cell visible light communication with hybrid underlay/overlay resource allocation”. *IEEE Photon. Technol. Lett.*, 30(12):1135–1138.
60. Tran et al., 2019. Tran, C., Hoang, T., and Nguyen, N. (2019). “Coordinated multichannel transmission scheme for indoor multiple access points VLC networks”. In 19th ISCIT, pages 611–615.
61. Panayirci et al., 2020b. Panayirci, E., Yesilkaya, A., Cogalan, T., Poor, H. V., and Haas, H. (2020b). “Physical-layer security with optical generalized space shift keying.” *IEEE Trans. Commun.*, 68(5):3042–3056. 92
62. Yesilkaya et al., 2018. Yesilkaya, A., Cogalan, T., Panayirci, E., Haas, H., and Poor H. V. (2018). “Achieving minimum error in MISO optical spatial modulation”. In Proc., IEEE ICC, pages 1–6.
63. Purwita et al., 2019. Purwita, A. A., Yesilkaya, A., Tavakkolnia, I., Safari, M., and Haas, H. (2019). “Effects of irregular photodiode configurations for indoor MIMO VLC with mobile users”. In Proc. IEEE PIMRC, pages 1–7.
64. Khalid et al., 2012. Khalid, A. M., Cossu, G., Corsini, R., Choudhury, P., and Ciaramella, E. (2012). “1-Gb/s transmission over a phosphorescent white LED by using rate-adaptive discrete multitone modulation”. *IEEE Photon. J.*, 4(5):1465–1473.
65. Tsiatmas et al., 2014. Tsiatmas, A., Baggen, C. P. M. J., Willems, F. M. J., Linnartz, J. M. G., and Bergmans, J. W. M. (2014). “An illumination perspective on visible light communications”, *IEEE Commun. Mag.*, 52(7):64–71.
66. Leung-Yan-Cheong and Hellman, 1978. Leung-Yan-Cheong, S. and Hellman, M. (1978). “The Gaussian wire-tap channel.” *IEEE Trans. Inf. Theory*, 24(4):451–456.
67. Cover and Thomas, 2006. Cover, T. M. and Thomas, J. A. (2006). *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley Interscience, USA.

68. Cheng, 1994. Cheng, R. S. (1994). "Multirate achievability in memoryless multiaccess Channel". In Proc. IEEE ISIT, pages 58–60.
69. Haas et al., 2016. Haas, H., Yin, L., Wang, Y., and Chen, C. (2016). "What is LiFi?" J. Lightw. Technol., 34(6):1533–1544.
70. Bloch and Barros, 2011. Bloch, M. and Barros, J. (2011). Secrecy capacity, page 49–111. Cambridge University Press. Burchardt et al., 2014.
71. Gallager, 1968. Gallager, R. (1968). *Information Theory and Reliable Communication*. Wiley-New York, NY.
72. Zhang et al., 2015. Zhang, R., Yang, L.-L., and Hanzo, L. (2015). "Error probability and capacity analysis of generalised pre-coding aided spatial modulation". IEEE Trans. Wireless Commun., 14(1):364–375.
73. A. M. Khalid and G. Cossu and R. Corsini and P. Choudhury and E. Ciaramella, 2012 "1-Gb/s Transmission Over a Phosphorescent White LED by Using Rate-Adaptive Discrete Multitone Modulation", IEEE Photon. J., vol. 4, no. 5, pp. 1465-1473.
74. A. Al-Kinani and C. Wang and L. Zhou and W. Zhang, 2018, "Optical Wireless Communication Channel Measurements and Models", IEEE Commun. Surv. Tutor., vol. 20, no. 3, pp. 1939-1962.
75. A. Yesilkaya, E. Basar, F. Miramirkhani, E. Panayirci, M. Uysal, H. Haas, 2017, "Optical MIMO-OFDM with generalized LED index modulation", IEEE Trans. Commun., vol. 65, no. 8, pp. 3429-3444.
76. S. M. Kay, 1993, *Fundamentals of Statistical Signal Processing: Estimation Theory*, Prentice Hall PTR, ISBN 0-13-345711-7.
77. Vishay, 2019, TSUS4300 infrared emitting diode, 950 nm, GaAs, [Online],
<https://www.vishay.com/docs/81053/tsus4300.pdf>.
78. C. Zhang, J. Yue, L. Shi and S. Wang, 2021, "A novel physical encryption algorithm for LoRa", IEEE Commun. Lett., vol. 25, no. 8, pp. 2512 - 2516.
79. K. H. Rosen, 1993, *Elementary Number Theory and Its Applications (3rd ed.)*, Addison-Wesley, ISBN 978-0201-57889-8.

80. R. G. Gallager, 1993, *Information Theory and Reliable Communications*, John Wiley and Sons, ISBN W-471-29048-3.
81. Su N, Panayirci E, Koca M, Yesilkaya A, Poor H V and Haas H 2021 Physical layer security for multi-user MIMO visible light communication systems with generalized space shift keying *IEEE Trans. Commun.* 69 2585–98
82. Jovicic A, Li J and Richardson T 2013 Visible light communication: Opportunities, challenges and the path to market *IEEE Commun. Mag.* 51 26–32.
83. Haas H, Yin L, Wang Y and Chen C 2016 What is LiFi? *J. Light. Technol.* 34 1533–44
84. Benzetimler A, Panayirci E and Vincent Poor H 2019 Relay-Aided Secure Broadcasting for Visible Light Communications *IEEE Transactions on Communications* vol 67pp 4227–39.
85. Huang Z, Gao Z and Sun L 2017 Anti-Eavesdropping Scheme Based on Quadrature Spatial Modulation *IEEE Commun. Lett.* 21 532–5
86. Wang F, Li R, Zhang J, Shi S and Liu C 2019 Enhancing the secrecy performance of the spatial modulation aided VLC systems with optical jamming *Signal Processing* 157 288–302.
87. Yin L and Haas H 2018 Physical-Layer Security in Multiuser Visible Light Communication Networks *IEEE J. Sel. Areas Commun.* 36 162–74
88. Cogalan T, Haas H and Panayirci E 2020 Optical spatial modulation design *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* 378
89. A, Basar E, Miramirkhani F, Panayirci E, Uysal M and Haas H 2017 Optical MIMO-OFDM with Generalized LED Index Modulation *IEEE Transactions on Communications* vol 65pp 3429–41
90. Panayirci E, Yesilkaya A, Cogalan T, Poor H V and Haas H 2020 Physical-Layer Security with Optical Generalized Space Shift Keying *IEEE Trans. Commun.* 68 3042–56.
91. Aghdam S R and Duman T M 2016 Physical Layer Security for Space Shift Keying Transmission with Precoding *IEEE Wirel. Commun. Lett.* 5 180–3.
92. Saud M S, Wirtanen M, Chowdhury H, Hänninen T, Häkkinen J and Katz M 2016 FPGA-based test-bed for visible light communication physical layer study *European Wireless Conference 2016*,

EW 2016 pp 383–8.

93. Setiawan E, Adiono T, Osahon I N O and Popoola W O 2019 Experimental Demonstration of Visible Light Communication using White LED, Blue Filter and SoC based Test-Bed Proceeding - 2019 International Symposium on Electronics and Smart Devices, ISESD 2019
94. Mirvakili A, Koomson V J, Rahaim M, Elgala H and Little T D C 2015 Wireless access test-bed through visible light and dimming compatible OFDM 2015 IEEE Wireless Communications and Networking Conference, WCNC 2015 pp 2268–72.
95. Li S, Wang Z, Shi L and Zhang X 2019 Experimental indoor tracking testbed based on Visible Light Communication 2019 26th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2019 pp 129–30.
96. Denton S L 2020 Optical Communications Testbed for the Exploitation of Luminescence Emission of Solar Cells for Optical Frequency Identification (OFID) (Purdue University)
97. Gawlowicz P, Jarchlo E A and Anatolij Zubow 2020 Wov: WiFi-based VLC testbed arXiv:2001.08489v1
98. Kamsula P Design and Implementation of A Bi-Directional Visible Light Communication Testbed (University of Oulu)
99. Çirkinoğlu H O, Ferhanoğlu O and Karabulut Kurt G 2021 Improved physical layer security of visible light communications with focused light emitters Opt. Commun. 485.
100. Fortes M and González O 2021 Testbed for experimental characterization of indoor visible light communication channels Electron. 10.
101. Büyükçorak S, Topal O A, Ferhanog O and Karabulut Kurt G 2020 Mixture model and its experimental validation for visible light communications Electron. Lett. 56 559–62.
102. Sun H, Zhang Y, Wang F, Zhang J and Shi S 2021 SVM Aided Signal Detection in Generalized Spatial Modulation VLC System IEEE Access 9 80360–72.
103. Panayirci E 2021 Optical Index-Coded Space Shift Keying (IC/SSK) IEEE Commun. Lett. 25 2654–8

104. Kisacik R, Yalcinkaya A D, Pusane A E, Baykas T and Uysal M 2021 Characterization of LEDs for visible-light communications *Opt. Eng.* 60.
105. Kisacik R, Yagan M Y, Uysal M, Pusane A E and Yalcinkaya A D 2021 A New LED Response Model and its Application to Pre-Equalization in VLC Systems *IEEE Photonics Technol. Lett.* 33 955–8.
106. S. Arnon, *Visible Light Communication* (2015).
107. F. Wang, Z. Wang, C. Qian, L. Dai, and Z. Yang, "Efficient vertical handover scheme for heterogeneous VLC-RF systems," *J. Opt. Commun. Netw.* 7, 1172–1180 (2015).
108. C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.* 28, 656–715 (1949).
109. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.* 58, 1875–1888 (2010).
110. M. Eghbal and J. Abouei, "Security enhancement in free-space optics using acousto-optic deflectors," *J. Opt. Commun. Netw.* 6, 684–694 (2014).
111. S. Cho, G. Chen, and J. P. Coon, "Securing Visible Light Communication Systems by Beamforming in the Presence of Randomly Distributed Eavesdroppers," *IEEE Trans. Wirel. Commun.* 17, 2918–2931 (2018).
112. A. Mostafa and L. Lampe, "Physical-Layer Security for MISO Visible Light Communication Channels," *IEEE J. Sel. Areas Commun.* 33, 1806–1818 (2015).
113. A. Mostafa and L. Lampe, "Optimal and Robust Beamforming for Secure Transmission in MISO Visible-Light Communication Links," in *IEEE Transactions on Signal Processing* (2016), Vol. 64, pp. 6501–6516.
114. H. O. Çirkinoğlu, O. Ferhanoğlu, and G. Karabulut Kurt, "Improved physical layer security of visible light communications with focused light emitters," *Opt. Commun.* 485, (2021).
115. O. Gürcüoğlu, I. Deniz Derman, M. Altınsoy, R. Khayatzadeh, F. Çivitci, A. C. Erten, and O. Ferhanoğlu, "A 3D-printed 3D actuator for miniaturized laser scanning probes," *Sensors Actuators, A Phys.* 317, (2021).

116. S. Bargiel, L. Nieradko, M. Józwik, C. Gorecki, and J. A. Dziuban, "New generation of fully integrated optical microscopes on-chip: application to confocal microscope," in MEMS, MOEMS, and Micromachining II (2006), Vol. 6186, p. 618602.
117. T. Liu, M. Rajadhyaksha, and D. L. Dickensheets, "MEMS-in-the-lens architecture for a miniature high-NA laser scanning microscope," Light Sci. Appl. 8, (2019).

TÜBİTAK
PROJE ÖZET BİLGİ FORMU

Proje Yürütücüsü:	Prof. Dr. ERDAL PANAYIRCI
Proje No:	218E034
Proje Başlığı:	Görünür Işıklı Haberleşmede Fiziksel Katman Güvenliği
Proje Türü:	1003 - Öncelikli Alanlar (2. Aşama)
Proje Süresi:	24
Araştırmacılar:	GÜNEŞ ZEYNEP KARABULUT KURT, MUTLU KOCA
Danışmanlar:	HARALD HAAS (Yurt Dışı)
Projenin Yürütüldüğü Kuruluş ve Adresi:	KADİR HAS Ü. MÜHENDİSLİK VE DOĞA BİLİMLERİ F. ELEKTRONİK MÜHENDİSLİĞİ B.
Projenin Başlangıç ve Bitiş Tarihleri:	15/11/2019 - 15/12/2021
Onaylanan Bütçe:	662630.68
Harcanan Bütçe:	456464.67

TÜBİTAK

Öz:

Proje Özeti

Optik Kablosuz Haberleşme ve bunun olası bir uygulaması olan Görünür Işıklı Haberleşme (Visible Light Communications (VLC)), sahip olduğu çok yüksek bant genişliği, bilgi iletim kapasitesi, elektromanyetik girişimlere karşı yüksek bağımsızlığı, uzaysal ortamlarda yüksek oranda güvenli kapsama özelliği ve çalışma frekans spektrumunun belli regülasyonlarla düzenlenmemiş olması nedeniyle, geniş bir uygulama alanı içinde, çok önemli teknik ve operasyonel üstünlükler sağlamakta ve radyo tabanlı kablosuz haberleşme sistemlerine bir seçenek olarak veya onların tamamlayıcı niteliğinde karşımıza çıkmaktadır. Son bir kaç yıl içinde, varolan şifreleme tekniklerini güçlendirmek için ve onlara tamamlayıcı bir ek olarak, fiziksel katman güvenliği (physical layer security) diye adlandırılan umut verici yeni bir araştırma ve ilgi alanı ortaya çıkmıştır. Fiziksel katman güvenliği, haberleşme ortamındaki yetkili olmayan kişilerden bilginin saklanması amacıyla, her türlü üst katman şifrelemeden bağımsız olarak, tamamen iletişim kanal ortamının özelliklerini kullanarak, geliştirilen teknik ve yöntemlerdir. Projede, genişbant ağlarda VLC fiziksel katman düzeyinde güvenliği sağlamak amacıyla, geleneksel yaklaşımların ötesinde hızlı ve güvenilir çözümler için, etkin kuramsal çalışmalardan başlayarak laboratuvar düzeyine kadar geniş bir spektrumda özgün ve yenilikçi algoritmaların tasarımı önerilmektedir. Bu bakımdan, proje, 1003-BIT-GNBT 2018-1 Genişbant Haberleşme Ağları için Veri İşleme Teknolojileri Çağrı Metnindeki (a) ve (b) amaçları ile büyük bir uyum içinde, araştırma bileşeni yüksek, yenilikçi ve özgün bir proje niteliğindedir. Projede, geleneksel sistemlere göre getirilen yenilikler ve sağlanan üstünlükleri şu şekilde sıralanabilir:

1.Projede, fiziksel katman güvenliğine sahip VLC sisteminin gerçekleştirilmesinde, Indis modülasyonu ve bunun bir takım varyasyonları olan uzamsal modülasyon, uzay kaydırmalı anahtarlama ve OFDM-indis modülasyonu gibi yeni modülasyon teknikleri ve çok-girişli-çok çıkışlı LED (light emitting diode) yapıları ile, dikgen olmayan çoklu erişimin birlikte çalışan MIMO-NOMA tekniği önerilmektedir. Elde edilecek yeni ve özgün algoritmalar geleneksel sistemlere göre hesaplama karmaşıklığı düşük, güç randımanı yüksek ve çok kullanıcı senaryolar için de çalışabilme yeteneğine sahip olacaktır. Özellikle, sadece bu modülasyon tekniklerine özgü, yapay karıştırma (artificial jammig) sinyal üretme özelliği, bu tekniklerin fiziksel güvenliğin sağlanmasında geleneksel yaklaşımlara kıyasla en önemli üstünlüğünü oluşturmaktadır. Ayrıca, geliştirilecek algoritmalara ilişkin ?erişilebilecek maksimum gizlilik kapasitesi? ve ?gizlilik oranları?nın analitik yollardan belirlenmesi için izlenecek kuramsal yaklaşımlar, sistem mimarilerinin farklı olmasından dolayı, geleneksel sistemlerde izlenen yollardan çok daha farklı olacaktır.

2.LED?lerin ve ışığın neden olduğu kısıtlar sonucu, radyo frekanslı kabosuz haberleşmedeki geleneksel kanal kestirim tekniklerinin uygulanamaması nedeniyle, Masif MIMO yapıdaki görünür ışık kanallarının optimal ve hızlı kestiriminde yeni kanal kestirim algoritmalarının tasarımı önerilmektedir. Ayrıca, kestirim hataları ve kanal bilgilerin vericiye iletilmesindeki gecikmelerin, sistemin bit hata başarımına etkilerinin kuramsal ve bilgisayar benzetimleriyle incelenmesi hedeflenmektedir.

3.Projede son olarak, fizisel katman güvenliğine sahip VLC sistemlerin laboratuvar ortamında donanımsal olarak gerçekleştirilmesi ve gerçek-zamanda çalışmasının test edilmesi önerilmektedir. Literatürde bir karıştırma sinyali üreterek gizliliği sağlayan geleneksel sistemlerle, algoritmanın gerek hesaplama karmaşıklığı ve hızı, gerekse hata başarımı ve erişilebilecek enbüyük gizlilik oranları farklı sinyal-gürültü düzeylerinde karşılaştırılarak üstünlüğü kanıtlanacaktır.

Abstract:	<p>ABSTRACT</p> <p>Optical Wireless Communications and one of its potential applications, Visible Light Communications (VLC), with attractive features such as high bandwidth capacity, robustness to electromagnetic interference, high degree of spatial confinement, inherent security and unregulated spectrum, offer powerful alternatives and/or complementary technologies to the existing radio frequency (RF) based wireless systems for a wide range of applications. During the past few years, physical-layer security in VLC networks has emerged as a promising approach to complement conventional encryption techniques and provide a first line of defense against eavesdropping attacks. To provide security at VLC physical layer level in broadband networks, in this project, design of original and innovative algorithms is proposed starting from effective theoretical studies to laboratory level for fast and reliable solutions beyond traditional approaches. In this respect, the project proposal is planned to contribute fully to the goals of the call 1003-BIT-GNBT-2018-1 Data Processing Technologies for Broadband Communication Networks as well as in the goals and objectives specified in the call text (a) and (b), and has a potential to increase competitiveness of our country at the international level. In the project, the innovations and advantages as compared to the state-of-art systems can be listed as follows:</p> <p>1.New and novel algorithms for physical layer security in multiuser and broadband VLC systems applying new modulation schemes such as index modulations (IM) and its variations like spatial modulation (SM), space shift keying (SSK), OFDM-index modulation techniques (OFDM-IM), as well as optical multiple-input-multiple output (MIMO) with non-orthogonal multiple excess (NOMA) system are developed. The algorithms to be design will have low complexity, high power efficiency and have the capability to work with multi-user scenarios. In particular, the artificial jamming signal generation property of these modulation techniques is the most important advantage in providing physical security compared to the traditional approaches. Moreover, the theoretical methods, to develop the maximum achievable secrecy capacity and secrecy rate of the physical layer security algorithms will be much different than the approaches adopted by the by traditional systems because of the different system architectures employed.</p> <p>2.Due to some physical constraints imposed by the LEDs and light, it is not possible to employ conventional channel estimation techniques in RF communications. Hence, design of new optimal and computationally efficient estimation algorithms for massive MIMO structured optical channels will be proposed. In addition, the effects of channel estimation errors and the delays in the transmission of channel state information to the transmitter on the bit error performance will be investigated theoretically and by computer simulations.</p> <p>3.Finally, the proposed system will be implemented in a laboratory environment and its BER performnce will be tested and compared with the state-of-art systems, employing conventional jamming signals.</p>
Anahtar Kelimeler:	Anahtar Kelimeler: VLC, PLS, OFDM indis modülasyonu, MIMO, SM, çoklu erişim.
Fikri Ürün Bildirim Formu Sunuldu Mu?:	Evet

Proje Yapılan Yayınlar:	<ol style="list-style-type: none">1- Physical Layer Security for Multi-User MIMO Visible Light Communication Systems With Generalized Space Shift Keying (Makale - Diğer Hakemli Makale),2- Physical-Layer Security in 6G Networks (Makale - Diğer Hakemli Makale),3- Optical spatial modulation design (Makale - İndeksli Makale),4- Spatial Constellation Design Based Generalized Space Shift Keying for Physical Layer Security of Multi-User MIMO Communication Systems (Makale - İndeksli Makale),5- Optical Index-Coded Space Shift Keying (IC/SSK) (Makale - İndeksli Makale),6- Physical Layer Security for Multi-User MIMO Visible Light Communication Systems With Generalized Space Shift Keying (Makale - İndeksli Makale),7- Physical-Layer Security With Optical Generalized Space Shift Keying (Makale - İndeksli Makale),8- Flexible LED Index Modulation for MIMO Optical Wireless Communications (Bildiri - Uluslararası Bildiri - Sözlü Sunum),9- Sparse Channel Estimation with Clipping Noise in DCO-OFDM Based VLC Systems (Bildiri - Uluslararası Bildiri - Sözlü Sunum),10- Physical-Layer Security in Visible Light Communications (Bildiri - Uluslararası Bildiri - Sözlü Sunum),11- DCO-OFDM Tabanlı VLC Sistemlerde Kırpma Gürültüsü Etkisinde Kanal Kestirimi Channel Estimation for DCO-OFDM Based VLC Systems in the Presence of Clipping Noise (Bildiri - Ulusal Bildiri - Sözlü Sunum),12- DCO-OFDM Tabanlı VLC Sistemlerde Kırpma Gürültüsü Etkisinde Kanal Kestirimi Channel Estimation for DCO-OFDM Based VLC Systems in the Presence of Clipping Noise (Bildiri - Ulusal Bildiri - Sözlü Sunum),13- PHYSICAL LAYER SECURITY IN THE VISIBLE LIGHT COMMUNICATIONS SYSTEMS (Tez (Araştırmacı Yetiştirilmesi) - Yüksek Lisans Tezi),14- Physical Layer Security and Channel Estimation in Optical Generalized Index-Modulated OFDM Systems (Tez (Araştırmacı Yetiştirilmesi) - Yüksek Lisans Tezi),15- PHYSICAL LAYER SECURITY IN THE VISIBLE LIGHT COMMUNICATIONS SYSTEMS (Tez (Araştırmacı Yetiştirilmesi) - Yüksek Lisans Tezi),16- Advanced Techniques for Cooperation and Physical Layer Security In Visible Light Communications (Tez (Araştırmacı Yetiştirilmesi) - Doktora Tezi),
-------------------------	--