Physical Layer Approach to Secure Visible Light Communication and Sensing

by

Jian Chen

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
May 7, 2022

Keywords: Physical layer security, Visible light security, VLC and VLS

Approved by

Tao Shu, Chair, Associate Professor of Computer Science and Software Engineering
Dean Hendrix, Associate Professor of Computer Science and Software Engineering
Alvin Lim, Professor of Computer Science and Software Engineering
David Umphress, Professor of Computer Science and Software Engineering

Abstract

Visible Light (VL) is a wireless technology that uses visible light (400 $\sim$ 790 THz) as the medium to transmit information (i.e., visible light communication or VLC) or sense user's activities (i.e., visible light sensing or VLS) and it has now become a very active research topic in the area of wireless communication. While VL is expected to have a wide range of applications in the near future and there has been significant progress on the research, the security vulnerabilities of this technology have not been well understood so far. This situation may lead to the dangerous "zero-day attacks" issue when the technology is deployed in the near future. Thus, it's urgent to study the security vulnerabilities of VL and develop rigid countermeasures to these vulnerabilities.

In particular, due to the extremely short wavelength of visible light, the VL channel presents several unique characteristics than its radio frequency counterparts, which imposes new features on the VL security. Taking a physical-layer security perspective, the first proposed research of this exploratory dissertation attempts to investigate the intrinsic confidentiality of VLC communication as induced by its special channel characteristics. By exploiting the intrinsic linear superposition properties of VL, the second proposed research of this exploratory dissertation aims to design a signal-level always-on spoofing detection framework VL-Watchdog to secure the VL system from spoofing attack. The results reveal that due to the different types of reflections (specular and diffusive), the VL system becomes more vulnerable at specific locations where strong reflections exist, and the proposed VL-Watchdog was numerically evaluated under different factors and it was proved to be effective for VL spoofing attack detection.

Acknowledgments

I would like to take this chance to sincerely thank my adviser, Dr. Tao Shu, whose motivation, encouragement, guidance of this dissertation made its completion possible. My gratitude also goes to my other committee members Dr. David Umphress, Dr. Alvin Lim, and Dr. Dean Hendrix. Thank you all for your support and insightful comments to my dissertation research. I would also like to thank my dissertation University Reader, Dr. Xiaowen Gong, for his willingness and supportive comments.

Moreover, my gratitude also extends to the rest of the faculty members, staff, and graduate students in the Department of Computer Science and Software Engineering at Auburn University, who provided the necessary support and assistance. I'm also thankful for many other people, especially for Dr. Lorraine Wolf and Dr. Xiao Qin, who helped me at various times throughout my arduous PhD journey.

Last but not least, I would like to send out all of the love and appreciation that I could for my family members, especially for my dear wife, Rongting Xu, as well as my lovely daughter, Christina Chen. The support they have shown me throughout my life will never be eclipsed, and my gratitude is endless.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background and Motivation

The blooming of Internet of Things (IoT) network that involves pervasive communication and sensing among large amount of smart devices makes the current radio frequency (RF) spectrum over crowded [1, 2, 3, 4]. In search of new spectrum resources, visible light (VL) technology has received a lot of interest for both communication and sensing applications since the release of IEEE 802.15.7 standard in 2011 [5]. VL is a wireless technology that uses visible light (400 $\sim$ 790 THz) as the medium (Figure 1.1) to transmit information (i.e., visible light communication or VLC) or sense user's activities (i.e., visible light sensing or VLS) and it has now become a very active research topic in the area of wireless communication. Compared with regular RF based communication and sensing, VLC and VLS enjoy several unique benefits. Firstly, the VL spectrum is at a much higher frequency band and provides much wider bandwidth (more than 10,000X) than the RF spectrum. As a result, a VLC link can easily achieve Gbps-level transmission rate in short range ($\sim$ 10 meters), and VLS can achieve higher spatial resolution than RF sensing. Secondly, VL is more accessible than its RF counterparts. The VL spectrum is license free while most of the RF bands are not. More importantly, VLC and VLS enjoy the widely available lighting infrastructure that has already been installed in almost all indoor and many outdoor environments. By piggybacking their communication/sensing signals on today's low-power solid-state LED illumination, VLC and VLS have higher energy efficiency than their RF counterparts. Furthermore, because VL wave cannot penetrate walls and obstacles, visible light communication and sensing signals can be well confined within an enclosed area and cause little inter-cell interference. This allows dense spatial reuse of the VL spectrum.

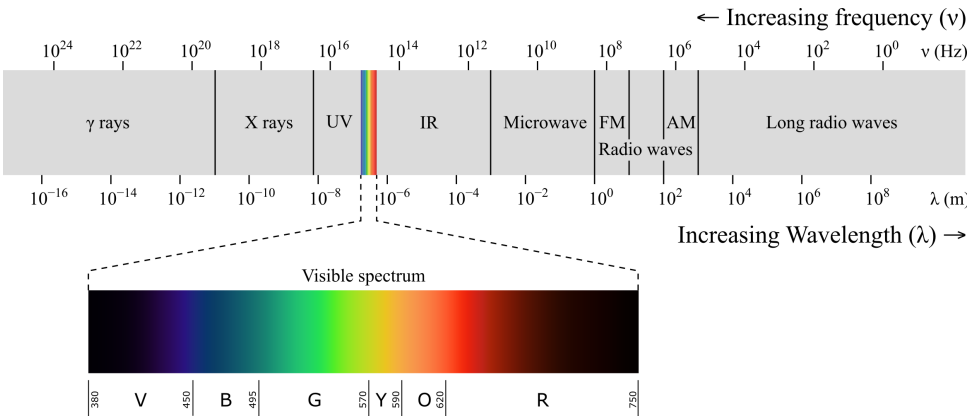

Figure 1.1: Electromagnetic spectrum

Because of these nice features, VL has been considered to be a promising and urgently-needed small-cell solution for offloading the crowded RF bands in 5G systems and beyond.

While VLC and VLS are expected to have a wide range of applications in the near future, the security vulnerabilities of this technology have not been well understood so far. In typical VL systems, data is transmitted by modulating the output intensity of the emitters, and the data signal is captured using photo-diodes as receivers. Contrary to the initial belief that VL is intrinsically secure because the propagation of visible light is directive and can be confined within a closed space, recent studies have revealed that this is not necessarily true, especially in public areas [6, 7]. Without any sort of wave-guiding transmission media, the light illumination that a VL link piggybacks on is diffusive in most real-world applications, which makes VL links inherently susceptible to eavesdropping by an unintended receiver in the same room. For example, the diffusive visible light illumination can be easily picked up and recorded by an eavesdropper using a VL receiver at many locations in the space, and may be analyzed afterwards to reveal the information embedded in the light. Such a unique "what-you-see-is-what-you-get" feature of visible light [8] makes eavesdropping a highly realistic threat to VLC, as its light can be seen at many locations due to its diffusiveness. This threat applies to most public indoor environments, such as libraries, meeting rooms, shopping centers, or aircrafts. Even worse, eavesdropping from outside of the space is possible when there are windows on the wall [6, 9, 10].

Meanwhile, due to the extremely short wavelength of visible light (380 $\sim$ 700 nm), the VL channel presents several unique features than its RF counterparts. For example, a VLC

channel is a mix of both specular reflection and diffusive reflection, which allows a VLC signal to be overheard (or seen) at much more locations than a RF signal whose reflection is dominantly specular, even when an eavesdropper is outside the main-lobe of the intended VL communication and sensing. As a result, in contrast to the conventional multi-path RF channel, a VL channel is no longer a discrete sequence of a small number of signal paths, but rather a continuous combination/clusters of signal paths reflected by the entire environment – a direct consequence of the diffusive reflection of visible light. Such a drastic change on channel characteristics imposes new security features on VLC communication, and requires a different method to investigate than its well-studied RF counterparts.

As more and more VLC/VLS systems are mounted on today's light fixtures, how to guarantee the authenticity of the VL signal in these systems becomes an urgent issue. This is due to the fact that almost all of today's light fixtures are unprotected and can be openly accessed by almost anyone, and hence are subject to tampering and substitution attacks. An attacker can easily replace an authentic LED by a rogue LED under his control to inject spoofed VL signal into user's receiver. Unfortunately, most of today's VLS applications do not have a reliable built-in signal authentication mechanism to detect these spoofed signals and hence will mistakenly accept them as authentic sensing inputs, leading to compromised sensing outcome. Similar situation also arises in VLC. For example, the attacker may first block the line of sight (LOS) of the authentic VLC link, and then subsequently point a rogue LED transmitter to the user's receiver (typically a photo-diode) to inject spoofed data to the user [9].

In consideration of both the computationally demanding and complexity of the upper-layer cryptographic techniques and severe hardware and energy constraints in IoT, we resort to physical layer approach to address the aforementioned security challenges in VLC/VLS. Physical layer security has been identified as one of the promising secrecy scheme to secure transmission in a wireless network. The underlying idea behind it is to sacrifice a portion of the communication rate, which otherwise would be used for secret data transmission via carefully-designed signaling and coding schemes. It exploits dissimilarities among the physical communication channels of different receivers in order to hide information from unauthorized receivers, without relying on upper-layer encryption techniques. So, it can serve as an alternative to the

computationally demanding and complex cryptographic algorithms and techniques. Moreover, it also has the potential to provide lightweight standalone secrecy solutions in communication systems functioning under limited hardware, low-complexity, and energy constraints such as machine-type communication devices in the IoT [1].

The overarching goal of this exploratory dissertation is to obtain a comprehensive understanding on the security vulnerabilities of VLC and VLS, and to develop a solid mathematical framework that can be used to investigate and develop rigid and provably-secure countermeasures to these vulnerabilities. Taking a physical-layer security perspective, the first proposed research of this exploratory dissertation attempts to investigate the intrinsic confidentiality of VLC communication as induced by its special channel characteristics. By exploiting the intrinsic linear superposition properties of VL, the second proposed research of this exploratory dissertation aims to design a signal-level always-on spoofing detection framework VL-Watchdog to secure the VL system from spoofing attack.

1.2 Major Contributions

1. **Statistical modelling and analysis on the confidentiality of VL systems**

   Our study in this work aims to exploit the unique characteristics of VLC channel in calculating its secrecy capacity. To the best of our knowledge, this is the first work that comprehensively considers the impact of both the specular and the diffusive reflections on secrecy capacity of indoor VLC and also investigates the spatial characteristics/distribution of the secrecy capacity over the indoor communication space. More specifically, the main contributions of our study are as follows:

   - A modified Monte Carlo ray tracing method is proposed to account for both the specular and diffusive reflections in calculating VLC channel impulse response at a given location.
   - A deep neural network (DNN) regression model is proposed to efficiently estimate the VLC channel impulse response as a function of the VLC link location in the

communication space based on the training data set of a limited number of channel response samples calculated according to the ray tracing model.

- Based on these models, the upper bound and the lower bound of the VLC secrecy capacity are calculated considering multiple reflections under specific conditions.
- Leveraging the secrecy capacity bounds, we depict the spatial characteristics/distribution of the VLC secrecy capacity over given indoor communication space.
- We also study how the multiple types of reflections affect VLC secrecy capacity against a comprehensive set of factors, including the locations of the VLC transmitter, receiver, and eavesdropper, the VLC channel bandwidth, the ratio between the specular and the diffusive reflections, and the reflection coefficient.

The content of this contribution will be presented in Chapter 3 and they have been published in the following papers [11, 12]:

- J. Chen and T. Shu, "Impact of multiple reflections on secrecy capacity of indoor VLC system," in *Proceedings of 21st International Conference on Information and Communications Security (ICICS'19)*, J. Zhou, X. Luo, Q. Shen, and Z. Xu, Eds. Cham: Springer International Publishing, 2019, pp. 105–123.
- J. Chen and T. Shu, "Statistical modeling and analysis on the confidentiality of indoor vlc systems," in *IEEE Transactions on Wireless Communications*, 2020, vol. 19, no. 7, pp. 4744–4757.

2. **Spoofing detection with redundant orthogonal coding for VL systems**

In this work, we present VL-Watchdog, a novel signal-level always-on spoofing detection framework for VLC and VLS systems. VL-Watchdog can be implemented as a small hardware (receiver) add-on to an existing VL system. Once deployed, the watchdog will persistently monitor the light signals in the field to ensure they are sent only from authentic (legitimate) sources. VL-Watchdog supports large-scale VL systems, i.e., one with many smart LEDs, and does not assume any physical or optical difference in the LED hardware. Instead, VL-Watchdog is based on coding. It uses orthogonal codes

to encode the illumination of each legitimate LED, so that the transmitted light of a legitimate LED is identifiable by detecting the unique signal structure possessed by the received light. To the best of our knowledge, this work serves as the first signal-level always-on counter-spoofing mechanism applicable to both VLC and VLS systems. Our main contributions are summarized as follows:

- An orthogonal coding based signal-level always-on VL spoofing detection framework VL-Watchdog is proposed. Its optimal detection threshold is also derived by analysis.
- A false-warning filter is proposed to improve VL-Watchdog's detection accuracy by accounting for random light perturbations caused by human activities and environmental changes in realistic application scenarios.
- A proof-of-concept testbed is developed to verify the feasibility of VL-Watchdog.
- The performance of VL-Watchdog is evaluated based on extensive numerical simulations by taking into account a comprehensive set of parameters, including the number of orthogonal coding basis, the spoofing power to noise ratio, spoofing detection window size, the spoofer's strategies in fabricating its spoofing signals, and random perturbations from the application environment.

The content of this contribution will be presented in Chapter 4 and they have been published in the following papers [13, 14]:

- J. Chen and T. Shu, "Spoofing detection for indoor visible light systems with redundant orthogonal encoding," in *Proceedings of 2021 IEEE International Conference on Communications (ICC'21)*, Montreal, Canada, 2021, pp. 1-6.
- J. Chen and T. Shu, "VL-Watchdog: Visible Light Spoofing Detection with Redundant Orthogonal Coding," in *IEEE Internet of Things Journal*, 2022, accepted.

1.3 Organization

The structure of the dissertation reflects the list of contributions in the previous section, and is presented as follows:

In Chapter 2, Literature review including the most recent VLC standardization survey and related work is presented.

In Chapter 3, Statistical modelling and analysis on the confidentiality of VL systems.

In Chapter 4, Spoofing detection with redundant orthogonal coding for VL systems.

Finally, in Chapter 5, Conclusions and future work.

Chapter 2

Literature review

2.1 VLC standardization survey

2.1.1 Introduction

Since the first introduction of Light Fidelity (Li-Fi) terminology in 2011 at a TED Global conference by Harald Haas [15], Visible Light Communication (VLC) has regained a lot of interest, and its standardization and commercialization have been accelerating. Li-Fi is a high speed bi-directional fully connected VLC system and is analogous to Wi-Fi, which uses radio frequency (RF) for communication. VLC is a wireless communication technology that uses visible light spectrum (wavelengths of 390–750 nm or frequency band of 400–790 THz) as the medium to provide wireless networking access. Compared with the RF wireless communications, VLC enjoys several nice features, and its main characteristics are listed in Table 2.1. Because of these nice features, VLC and the applicable Li-Fi technology have been considered to be a promising solution for offloading the crowded RF traffic in 5G systems and beyond.

Feature	VLC	RF
Bandwidth	High	Low
Installation	Easy	Medium
Power Consumption	Low	High
Coverage distance	Short	Medium
Security	High	Low
EM Interference	None	High
Health Concern	None	Medium

Table 2.1: VLC vs. RF characteristics

As we are stepping into the era of Internet of Things (IoT), more and more smart devices make the current Wi-Fi solution run into limitations, such as bandwidth, data rate, electromagnetic (EM) interference, and security. Crowded spectrum is creating real problems in the deployment of Wi-Fi and Li-Fi is believed to be able to alleviate some of those problems. The features of high transmission rate, wide bandwidth, free of interference in electromagnetic sensitive areas and non-hazardous to health have made Li-Fi an attractive technique for future communication. Although Li-Fi is still in an exploratory phase at present, the standardization of VLC facilitates to accelerate the development of Li-Fi technology and eventually deliver real world deployments.

Recently, VLC is growing rapidly because of the rapid development of the solid-state lighting that uses semiconductor light-emitting diodes (LEDs) as the light source. As VLC embeds communication into lighting, it can reuse the widely available lighting infrastructure that has already been installed in almost all indoor and many outdoor environments. Simultaneous use of LEDs for both lighting and communications purposes is a sustainable and energy-efficient approach that has the potential to revolutionize wireless applications. VLC standards are crucial to VLC applications, especially in the coming era of IoT, a landscape composed of a very diverse set of smart devices. VLC standards are really the only way for these heterogeneous devices to talk with one another and collaborate successfully in creating a large-scale VLC ecosystem.

In this chapter, we will briefly overview the recent progress on VLC standardization and present the mainstream VLC standards published by different standardization organizations.

2.1.2 Brief history of VLC standardization

Along with the growing academic interest in VLC [16, 17, 18, 19, 20, 21], industrial attention to VLC has triggered standardization activities in this emerging market [22, 23, 24]. In Japan, the Visible Light Communications Consortium (VLCC) (www.vlcc.net) was leading the VLC standardization activities and proposed two VLC standards. These two standards were accepted by the Japan Electronics and Information Technology Industries Association (JEITA) in 2007 and became known as JEITA CP-1221 (visible light communication system standard) and

JEITA CP-1222 (visible light ID system standard), respectively. Additionally, in June 2013, the JEITA CP-1223 visible light beacon system standard was approved as an improved version of the JEITA CP-1222 [18, 19].

At the same time, the Institute of Electrical and Electronics Engineers (IEEE) also recognized the potential of this emerging technology and created IEEE Standard 802.15.7, which was approved in June 2011 (IEEE Std 802.15.7-2011). A few years later, a new revision was approved in December 2018 (IEEE Std 802.15.7-2018) [25]. This standard defines a physical (PHY) layer and a medium access control (MAC) sublayer for VLC and promises data rates sufficient to support audio and video multimedia services.

More recently, the International Telecommunication Union (ITU) organization released the ITU-T G.9991 standard in March 2019 [26]. This standard is the derivative of ITU-T G.9960 standard that was developed for next generation home network technology. This standard mainly defines the VLC system architecture, physical (PHY) layer and data link layer (DLL) for high-speed indoor optical wireless communication transceiver using visible light.

2.1.3 IEEE 802.15.7 Standard

The IEEE 802.15.7 (IEEE VLC hereafter) standard [25] describes the use of visible light for the standard network type VLC Personal Area Network (VPAN) and defines PHY layer and MAC sublayer protocols. It covers issues such as network topologies, addressing, collision avoidance, acknowledgment, performance quality indication, dimming support, visibility support, colored status indication, and color stabilization.

IEEE VLC network topologies and architecture

In this standard, three classes of VLC devices are considered, including infrastructure, mobile, and vehicle. The main features of each class are summarized in Table 2.2.

Depending on different application scenarios, a VPAN can be classified into one of three different network topologies, namely peer-to-peer, star, and broadcast, as shown in Figure 2.1. In each class, there is always a device (D) serving as coordinator (C), which is responsible for

	Infrastructure	Mobile	Vehicle
Fixed coordinator	Yes	No	No
Power supply	Ample	Limited	Moderate
Form factor	Unconstrained	Constrained	Unconstrained
Light source	Intense	Weak	Intense
Physical mobility	No	Yes	Yes
Range	Short/long	Short	Long
Data rates	High/low	High	Low

Table 2.2: IEEE VLC device classification

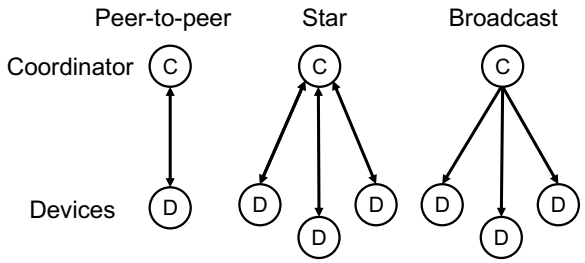

Figure 2.1: IEEE VLC network topologies

starting and maintaining a network and assigning new devices to an existing VPAN. In the peer-to-peer and star topology, the destination address is required for bidirectional communication, which is in contrast to the unidirectional communication in the broadcast topology.

The overall VLC network architecture is defined by a number of layers as illustrated in Figure 2.2. Each of the layers is responsible for one part of the standard and offers services to its upper layer. The upper layers include network layer (providing network configuration, manipulation, and message routing) and application layer (providing the intended function of the device), which are vendor specific so that they are not defined in the standard. The logical link control (LLC) layer provides access between the upper layers and the MAC sublayer through the service-specific convergence sublayer (SSCS). The MAC data and MAC management information are accessed through the MAC common-part sublayer (MCPS) and the MAC layer management entity (MLME), respectively. The PHY data and PHY management information are accessed through the PHY layer Data (PD) and the PHY layer management entity (PLME), respectively. The PHY switch serves as an interface to the optical service access point (Optical-SAP) and connects to the optical cells. The device management entity (DME) communicates with the dimmer to interface with upper layers and provide dimming information to the MAC

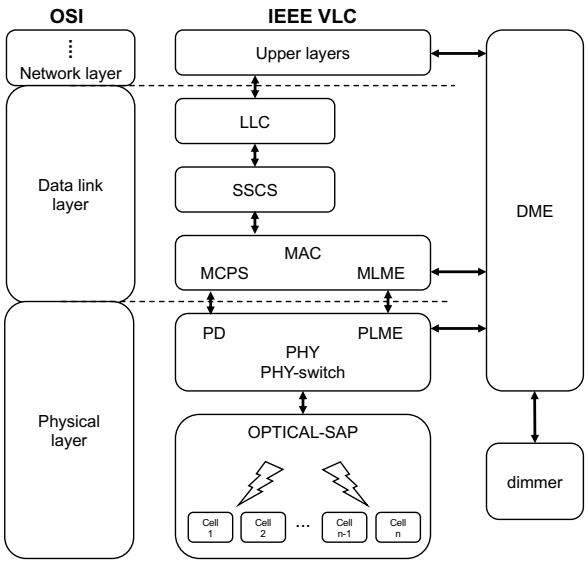

Figure 2.2: IEEE VLC network architecture

and PHY layers. The DME also controls the PHY switch through PLME for selection of the optical transceivers to accommodate different size and position of a specific cell.

IEEE VLC PHY layer

The PHY layer provides the physical specification of the device and the relationship between the device and the medium. The PHY layer mainly serves to establish and terminate a communication link, and it is responsible for the following tasks: 1) Activation and deactivation of the VLC transceiver; 2) Wavelength quality indication (WQI) for received frames; 3) Channel selection; 4) Data transmission and reception; 5) Error correction; 6) Synchronization.

General system model: Figure 2.3 shows the block diagram of the general physical layer implementation of the VLC system. The input bit stream is first passed through the channel encoder. Then, the channel encoded bit stream is passed through the line encoder to generate the encoded bit stream. After line encoding, modulation is performed and finally, the data is fed to the LED for transmission through the optical channel. At the receiver side, the photodiode receiver receives the optical signal. After demodulation and line decoding, the bit stream passed through the channel decoder to generate the output bit stream.

PHY layer types: Depending on the usage environment and transmission data rate, physical implementations of VLC are divided into 6 different types as listed in Table 2.3.

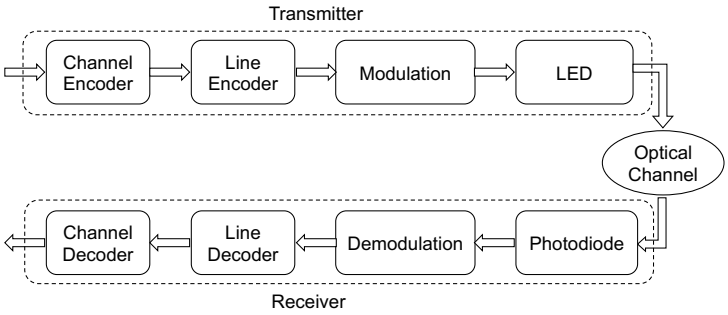

Figure 2.3: General physical layer system model of IEEE VLC

PHY types	Usage environment	Data rate
PHY I	Outdoor	Tens to hundreds of kb/s
PHY II	Indoor	Tens of Mb/s
PHY III	Applications with multiple transceivers	Tens of Mb/s
PHY IV	Discrete light sources	Up to 22 kb/s
PHY V	Diffused surface light sources	Up to 5.71 kb/s
PHY VI	Video displays	Up to 512 kb/s

Table 2.3: PHY layer types classification

Operating mode: The common PHY I, II, III and their settings of operating modes on the modulation, optical clock rates, error correction codes, and data rates are summarized in Table 2.4. In this table, multiple optical rates are provided for all PHY types to support different classes of LEDs for various applications. For a given VPAN, its compliant PHY is defined as one or multiple combinations of those types and implements at least one of the corresponding operating modes listed in Table 2.4, and the upper MAC sublayer will choose an appropriate optical rate during device discovery.

Modulation: There are three common modulation schemes for VLC, including On-Off Keying (OOK), Variable Pulse Position Modulation (VPPM), and Color-Shift Keying (CSK). OOK modulation is the simplest modulation scheme for VLC, where the LEDs are turned on or off (the intensity of the light may simply be reduced so that it can be distinguished) depending on data bits being 1 or 0. VPPM changes the duty cycle of each optical symbol to encode bits. CSK modulation encodes the bit patterns into color (wavelength) combinations.

RRL line coding: Run length limited (RLL) line codes are used to avoid long runs of 1s and 0s that could potentially cause flicker. RLL line codes take in random data symbols at input and guarantee DC balance with equal 1s and 0s at the output for every symbol. Various RLL

	Modulation	RLL code	Optical clock rate (Hz)	FEC (RS) [CC]	Data rate (bps)
PHY I	OOK	Manchester	200k	(15,7) 1/4	11.67k
				(15,11) 1/3	24.44k
				(15,11) 2/3	48.89k
				(15,11)	73.3k
				None	100k
	VPPM	4B6B	400k	(15,2)	35.56k
				(15,4)	71.11k
				(15,7)	124.4k
				None	266.6k
PHY II	VPPM	4B6B	3.75M	(64,32)	1.25M
				(160,128)	2M
			7.5M	(64,32)	2.5M
				(160,128)	4M
				None	5M
	OOK	8B10B	15M	(64,32)	6M
				(160,128)	9.6M
			30M	(64,32)	12M
				(160,128)	19.2M
			60M	(64,32)	24M
				(160,128)	38.4M
			120M	(64,32)	48M
				(160,128)	76.8M
				None	96M
PHY III	4-CSK	None	12M	(64,32)	12M
	8-CSK			(64,32)	18M
	4-CSK		24M	(64,32)	24M
	8-CSK			(64,32)	36M
	16-CSK			(64,32)	48M
	8-CSK			None	72M
	16-CSK			None	96M

Table 2.4: PHY I, II, III and their operating modes

MAC frame type	Functionality
BEACON frame	transmit beacons by a coordinator in any topology
DATA frame	transmit all data
ACK frame	verify successful reception of a frame
MAC command frame	manage and transmit all MAC control signal transfer
CVD frame	use visibility and dimming support providing side information

Table 2.5: MAC frame types

line codes such as Manchester, 4B6B, and 8B10B are defined in the standard and provide DC balance, clock recovery, and flicker mitigation.

FEC coding: IEEE VLC standard supports various forward error-correcting (FEC) schemes, which support both long and short data frames for low data rate outdoor and high data rate indoor applications. For outdoor applications, stronger codes using concatenated Reed-Solomon (RS) and convolutional coding (CC) are developed to overcome the additional path loss due to longer distances and potential interference introduced by optical noise. For indoor applications, only RS codes are used for FEC since they are better suited to high data rate implementations.

IEEE VLC MAC sublayer

The MAC sublayer mainly supports data and management services. It handles all access to the physical layer and is responsible for the following tasks: 1) Generating network beacons if the device is a coordinator; 2) Synchronizing to network beacons; 3) Supporting device association and disassociation; 4) Supporting color function; 5) Supporting visibility to maintain illumination and mitigate flicker; 6) Supporting dimming; 7) Flicker-mitigation scheme; 8) Supporting visual indication of device status and channel quality; 9) Supporting device security; 10) Providing a reliable link between two peer MAC entities; 11) Supporting mobility.

MAC frame: The MAC frame comprises three basic components: the MAC header (MHR), the MAC payload (MACP), and the MAC footer (MFR). The MHR contains the frame control field, the sequence number field, the address information field, and the security-related information field. An MACP part comprises specific information based on the selected frame type (except ACK frame). An MFR, which contains a frame check sequence (FCS), is an error correction–related footer and located at the end part of a MAC frame. According to its functionality, the MAC frames can be classified into five types (Table 2.5).

Network management: The device uses channel scanning to assess the current state of a channel, locate all beacons within its operation environment, or locate a particular beacon with which it has lost synchronization. The device can perform either active or passive scanning to discover an operating network and the results of the channel scanning are used to choose a suitable VPAN. Following a channel scan and selection of a suitable VPAN identifier, operation as a coordinator starts. The association/disassociation mechanisms that allow devices to join or leave a VPAN are further defined in the standard.

Random access mechanism: Depending on the network configurations, the standard provides four random access mechanism: slotted and unslotted random access with/without carrier sense multiple access with collision avoidance (CSMA/CA). Except for DATA and ACK frames, all other frame types use slotted random access mechanism with/without CSMA/CA to access the channel. If the devices are using the same spectrum and within the coverage of each other, CSMA/CA can be optionally implemented. Otherwise, each device should ensure that the channel is not used by another device to avoid collision by performing a channel clear assessment, which is requested by MAC and performed by PHY. Using the CSMA/CA algorithm, each device can sense the transmission channel before transmitting a frame.

Flicker mitigation and dimming support: Flicker refers to the modulation of the brightness of light at frequencies higher than the critical fusion frequency that can cause noticeable and negative/harmful physiological impacts on humans. To avoid flicker, the brightness changing period must fall within the maximum flickering time period (MFTP). The MFTP is defined as the maximum time period over which the light intensity can change without the human eye perceiving it. Therefore, the modulation process in VLC must avoid either intraframe flicker or interframe flicker. Dimming support is another important consideration for VLC for power savings and energy efficiency. It is desirable to maintain communication while a user arbitrarily dims the light source. It is a cross layer function between PHY and MAC and the standard describe three major dimming methods: adding compensation symbols, controlling pulse width, and controlling the amplitude of the signal [5].

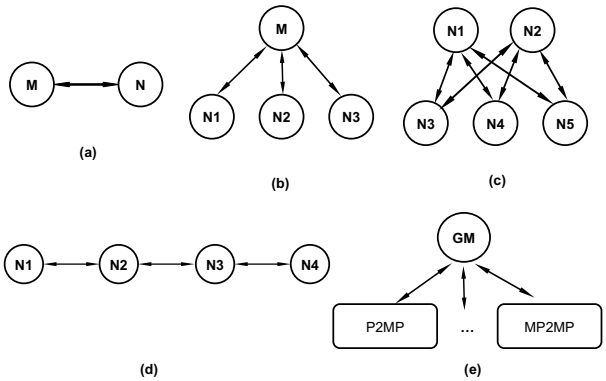

Figure 2.4: ITU VLC network topologies: (a) point-to-point (b) point-to-multipoint (P2MP) (c) multipoint-to-multipoint (MP2MP) (d) relayed mode (e) centralized

2.1.4 ITU-T G.9991 Standard

The ITU-T G.9991 (ITU VLC hereafter) standard [26] details the VLC network architecture, physical layer (PHY), and data link layer (DLL) specifications for high-speed indoor VLC access points.

ITU VLC network topologies and architecture

In this standard, a VLC system consists of one or more domains. Inside each domain, there are only one domain master (M) and one or more nodes (N) registered with it. The domain master is responsible for assigning and coordinating resources (bandwidth and priorities) of all nodes in its domain. The global master (GM) interacts with domain masters and coordinates resources such as bandwidth reservations, inter-domain handover and operational characteristics between domains. There are 5 legal topologies inside a domain, as illustrated in Figure 2.4.

The network architecture is presented in Figure 2.5. In particular, two PHY layers are defined to adapt to different scenarios, in which PHY I is adapted from [ITU-T G.9960] and PHY II is specifically designed for VLC, and a common DLL is laid upon them. The network architecture includes three main reference points: application interface (A-interface), physical medium-independent interface (PMI), and medium-dependent interface (MDI). The A-interface is described in terms of primitives exchanged between the AE and the DLL. The PMI interface, which is both medium independent and application independent, is responsible for function flows and logical signals. The MDI is a physical interface defined in terms of the

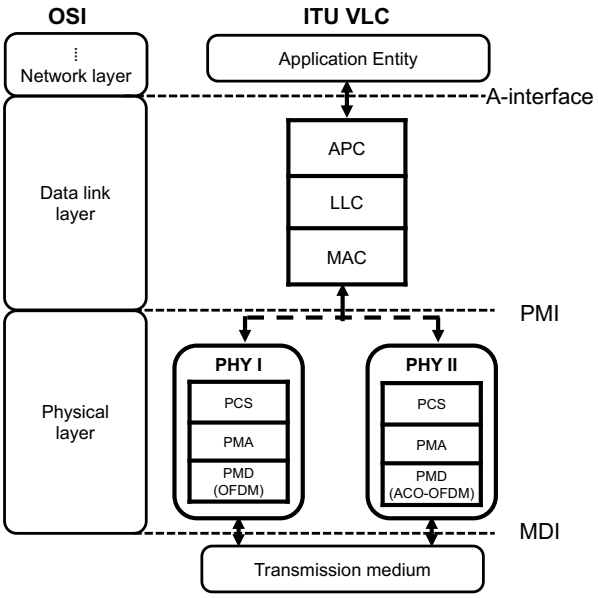

Figure 2.5: ITU VLC network architecture

physical signals transmitted over a specific medium and mechanical connection to the medium.

ITU VLC PHY layer

The standard supports two physical layers, in which PHY I describes the adaptation of an [ITU-T G.9960] PHY layer based on orthogonal frequency-division multiplexing (OFDM) approach, while PHY II describes a PHY layer based on an asymmetrically clipped optical (ACO-OFDM) approach. Both PHY I and PHY II include three sublayers: Physical Coding sublayer (PCS), Physical media attachment (PMA) sublayer and Physical medium dependent (PMD) sublayer. Functional model: The functional model of PHY layer is shown in Figure 2.6. In the transmit (Tx) direction, data is transformed to MAC protocol data units (MPDUs) by PMI first. Then the MPDU is mapped into a PHY frame in the PCS, scrambled and encoded in the PMA, modulated in the PMD and transmitted over the medium using OFDM (PHY I) or ACO-OFDM (PHY II). In the receive (Rx) direction, frames incoming from the medium via the MDI are demodulated and decoded all the way up to PCS, where they will be recovered to MPDUs and forwarded to the MAC via the PMI.

PHY frame: The PHY frame consists of a preamble, a header, an additional channel estimation (ACE) symbols and a payload. The preamble is intended to assist the receiver with

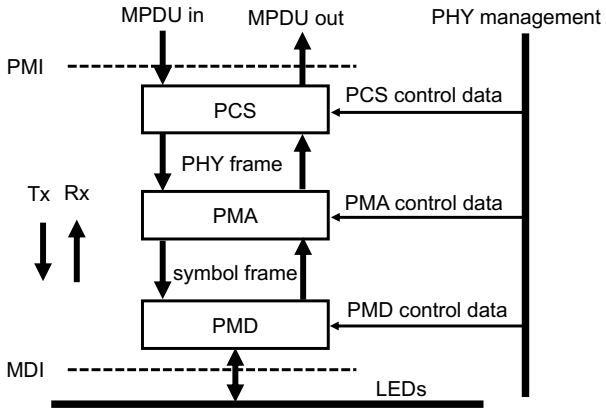

Figure 2.6: Physical layer functional model

Frame Type	Description
MAP/RMAP	MAP/RMAP frame
MSG	Data and management frame
ACK	Acknowledgement control frame
RTS	A request-to-send control frame
CTS	A clear-to-send control frame
CTMG	Short control frame
PROBE	Probe frame
ACKRQ	ACK retransmission request
BMSG	Bi-directional MSG frame
BACK	Bi-directional ACK frame
ACTMG	ACK for CTMG
FTE	Frame type extension

Table 2.6: PHY frame types

detecting and synchronizing to the frame boundaries, and acquiring the physical layer parameters such as channel estimation and OFDM symbol alignment. The header identifies the frame type and carries frame information, such as domain ID, source / destination ID, etc. PHY frame types are presented in Table 2.6.

ITU VLC data link layer

The DLL within the standard defines three sublayers: Application Protocol Convergence (APC), Logical Link Control (LLC) and Medium Access Control (MAC).

Functional model: The DLL functional model is shown in Figure 2.7. In the transmit direction, the application data primitive (ADP) enters the DLL from AE. Each incoming ADP set is converted by APC into an APC protocol data unit (APDU). Next, the LLC receives the

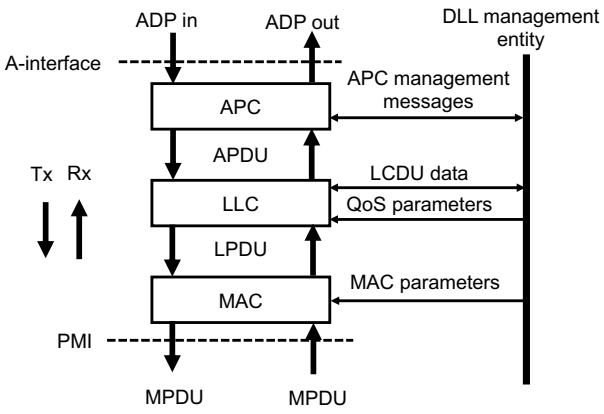

Figure 2.7: Data link layer functional model

APDU as well as the link control data units (LCDUs) from the DLL management entity and converts them into LLC protocol data units (LPDUs). LPDUs are then passed to MAC, which is responsible for concatenating LPDU into MAC protocol data units (MPDUs). In the receive direction, incoming MPDUs enter MAC via PMI and disassembled into LPDUs. Then, they are recovered into the original APDUs and LCDUs by LLC and sent to the APC and LLC management entity, respectively. ADPs are generated in the APC and conveyed to the AE via A-interface.

Medium access: The MAC cycle includes one or more transmission opportunities (TXOPs), in which two types of TXOPs are described in the standard: shared TXOP (STXOP) and full duplex shared TXOP (FDSTXOP). A STXOP may consist of one or more time slots (TSs), which can be a contention-free TS (CBTS) or a contention-based TS (CFTS). Each CFTS could be assigned to a data connection, a single source node, a single destination node and a minimum user priority, while a CBTS is assigned to a group of nodes and a minimum user priority. When a STXOP only contains CBTS, it is denoted as CBTXOP. Medium access in CBTXOP is illustrated in Figure 2.8. Each TS in CBTXOP includes one access channel, one or zero transmission channel, and the channel for ACK and IND frame. Inside the access channel, a node shall randomly choose one contention slot to send the access request (AR) to the domain master before transmitting, and then it will be allowed to transmit depending on whether an access channel exists revealed from the ACK. Medium access in FDSTXOP involves a central node, a primary receiver node and a group of secondary transmitter nodes. The central node is fixed and allowed to transmit to the primary receiver and receive from a secondary transmitter node

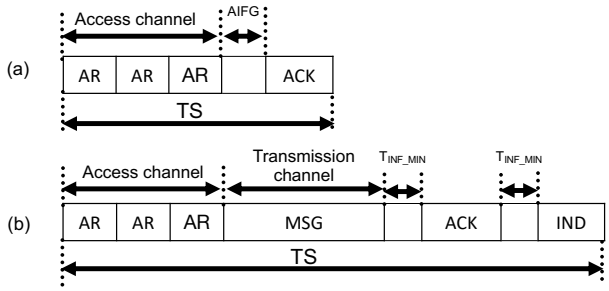

Figure 2.8: Medium access in CBTXOP: (a) no access channel exists (b) access channel exists

simultaneously. In the transmit direction, the central node transmits in a contention-free manner, whereas in the receive direction, the TXOP is shared by a group of secondary transmitter nodes to transmit to the central node.

2.1.5 Conclusions

In this chapter, we briefly present two mainstream VLC standards published by IEEE and ITU. These standards detail the specifications on VLC network standardization, such as network architecture and network layer configuration, which are crucial for the development and deployments of VLC. They also pave the road for the rapid growth of the VLC market. With the promising development of VLC standard, we would expect more and more real-world Li-Fi deployments in the near future, e.g., the outdoor streetlights can be used as access points for smart city applications, and the indoor ceiling lights can supply high throughput for smart home appliances.

2.2 Related work

2.2.1 VL channel modelling and analysis

While the research on VLC has achieved significant development in many fields, such as channel modelling [27, 28, 29, 30], modulation [31], channel estimation [32, 33, 34], and channel capacity analysis [35, 36], the security aspect of VLC has not been well understood so far. Existing research on VLC security is preliminary, as evidenced by the limited number of related works and the narrow scope of problems addressed in the literature. In [7], the authors discussed different scenarios of VLC sniffing, and the results of the experiment suggested that

VLC channels should not be considered intrinsically secure. Yin and Haas also confirmed the vulnerabilities of multiuser VLC networks by providing an analytical framework to characterize the secrecy performance [37]. Actually due to the broadcast feature of VLC, an unintended receiver within the same communication room may receive the information without being noticed, and this kind of threat could even apply to a scenario that the unintended receiver from outside of the room could eavesdrop merely through the windows or door gaps. The feasibility of such an attack was verified in [10], where an attacker outside a room was able to accurately figure out the program being played on a TV set in the room just by observing the change of light intensity illuminated by the TV through the window. Eavesdropping outside the direct beam of the light was also verified by testbed in [6].

For most cases of securing VLC system, conventional cryptographic methods can be implemented at specific layers of the protocol stack to provide data confidentiality, integrity, and authenticity for VLC applications. The secret keys required by these cryptographic methods can be generated by taking advantage of the physical layer characteristics of the VLC channels, e.g., [38, 39, 40]. But it is facing great challenges with the elevated capability of computation. As a promising complement to it, physical layer security, mainly represented by non-cryptographic methods, exploits the noise and the structure of the VLC channel to limit the amount of information that can be overheard by unauthorized eavesdroppers [41, 42, 43].

From an information-theoretic point of view, the physical-layer security was first introduced by Wyner as a wiretap channel model [44]: an eavesdropper sniffs a degraded signal from the main channel. The secrecy capacity is derived as the difference between the information capacity for the two channels. Different with RF communication, which is typically modeled as a Gaussian broadcast channel with an average power constraint at the transmitter side, the signal in VLC is typically modulated onto the intensity of the emitted light, it must satisfy average, peak as well as non-negative amplitude constraints, imposed by practical illumination requirements [35, 36, 45]. Due to the fundamental differences, results on the secrecy capacity obtained for RF networks can not be directly applied to VLC networks.

By considering one transmitter, one legitimate user and one eavesdropper in a VLC system, lower and upper bounds on the secrecy capacity of the amplitude-constrained Gaussian

wiretap channel was recently studied in [46, 47, 48], with the use of the derived capacity lower and upper bounds in [49]. Mostafa, et al. analyzed the achievable secrecy rate for single-input single-output (SISO) and multiple-input single-output (MISO) scenarios, and proposed various beamforming and jamming schemes to enhance the confidentiality of VLC links [42]. In addition, Arfaoui, et al. derived in closed-form the achievable secrecy rate as a function of the discrete input distribution for wiretap channel under the amplitude constraints of the input signal [50, 51]. To address the issue of priori knowledge of locations or channel state information of eavesdropper, in [52, 53], Cho, et al. investigated the secrecy connectivity in VLC in the presence of randomly located eavesdroppers, and they also study how the multipath reflections affect the secrecy outage probability. However, when considering the multipath reflections, they only deal with the impact of main channel without considering of the inter-symbol interference from multipath reflections.

2.2.2 Spoofing detection related to VL systems

Existing research on VLC security is preliminary, as evidenced by the limited number of related works and the narrow scope of problems addressed in the literature. Among the limited efforts, most of which are focused on studying the secrecy capacity limit of VLC link by modeling it as a wiretap channel [49, 54, 55]. These works take an information-theoretical approach, and thus can only give the limit of the capacity but cannot answer how the limit can be achieved in a realistic setting. Except the secrecy capacity, other issue unique to VLC, such as blocking and spoofing [56, 9, 55], have been rarely investigated in the literature. Recently, there has been comparable works, which could be exploited to investigate the spoofing issue, in other research field, e.g., VLC indoor localization. Zhang et al. in [57] utilized the distinctive fluorescent light, discriminating by unique inherent characteristic frequency, as location landmark to achieve a simple and robust localization. Wei et al. in [58] exploited the intensity of polarized light from optical anchor to extract the relative orientation of indoor object. Both of these physical approaches could be exploited to light transmitter discrimination, but they require either specific light fixture or extra facility to polarize transmitted light under the current multi-link VLC network infrastructure.

Meanwhile, to tackle the spoofing issues, different solutions were provided for WIFI networks in the literature [59, 60]. In particular, the related works can be roughly classified into crypotographic and non-cryptographic methods. The crypotographic methods focus on the data at higher layers and exploit crypotographic primitives to achieve authenticity. Traditionally researchers have applied cryptographic authentication and encryption techniques to tackle spoofing attacks [61, 62]. As most secure encryption techniques are usually highly resourced intensive and complex, the crypotographic computation in these methods introduces long delay in relative to the high-speed transmission at the physical layer, which significantly downgrades the effective throughput perceived at higher layers. The non-cryptographic methods address spoofing vulnerabilities under bottom layers, e.g., data link layer and physical layer. Sequence number field from the MAC header of data link layer was firstly used for detecting identity spoofing. In [63], Guo and Chiueh proposed sequence number gap based spoofing detection algorithm in the link-layer header of IEEE 802.11 frames. Similarly, in [64] Li and Trappe suggested the use of the sequence number gap and the distribution of inter-arrival times between packets sequence numbers at data link layer frames to classify MAC address spoofing. However, in consideration of a packet crafting tool that can manipulate the desired fields in packets, the sequence number based methods will lose their functionality. Down to the physical layer, the studies of RSS have shown promise in identifying and detecting identity-based attacks. Faria et al. in their work [65] used RSS based signalprint to detect of a large class of identity-based masquerading and resource depletion attacks in an indoor environment. Chen et al. in [66] formulated the attack detection as a statistical significance test and proposed RSS-based k-means clustering to detect spoofing attack for IEEE 802.11 in indoor environments. Sheng et al. in [67] showed that the RSS distribution function tends to a multi-Gaussian model due to antenna diversity in their IEEE 802.11 testbed and built RSS profiles for spoofing detection by modelling the RSS readings using Gaussian Mixture Models.

Chapter 3

Statistical modelling and analysis on the confidentiality of VL systems

3.1 Introduction

Visible light communication (VLC), which integrates communication and illumination, has now become a very active research topic in the area of wireless communication. Compared with its radio frequency (RF) counterparts, VLC enjoys many nice features, such as license free, interference free, reusable spectrum, wider bandwidth, higher transmission rate, higher energy efficiency and so on. Because of these nice features, VLC has been considered to be a promising and urgently-needed solution for offloading the crowded RF traffic in fifth generation (5G) networks.

While VLC is expected to have a wide range of applications in the near future, the security vulnerabilities of this technology have not been well understood so far. In typical VLC systems, data is transmitted by modulating the output intensity of the emitters, and the data signal is captured using photo-diodes as receivers. Contrary to the initial belief that VLC is intrinsically secure because the propagation of visible light is directive and can be confined within a closed space, recent studies have revealed that this is not necessarily true, especially in public areas [6, 7]. Without any sort of wave-guiding transmission media, the light illumination that a VLC link piggybacks on is diffusive in most real-world applications, which makes VLC links inherently susceptible to eavesdropping by an unintended receiver in the same room. For example, the diffusive visible light illumination can be easily picked up and recorded by an eavesdropper using a VLC receiver at many locations in the space, and may be analyzed afterwards to reveal the information embedded in the light. Such a unique "what-you-see-is-what-you-get" feature of visible light [8] makes eavesdropping a highly realistic threat to VLC,

as its light can be seen at many locations due to its diffusiveness. This threat applies to most public indoor environments, such as libraries, meeting rooms, shopping centers, or aircrafts. Even worse, eavesdropping from outside of the space is possible when there are windows on the wall [6, 9, 10].

In particular, due to the extremely short wavelength of visible light ($0.38 \sim 0.69$ μm), the VLC channel presents several unique features than its RF counterparts. For example, a VLC channel is a mix of both specular reflection and diffusive reflection, which allows a VLC signal to be overheard (or seen) at much more locations than a RF signal whose reflection is dominantly specular, even when an eavesdropper is outside the main-lobe of the intended VLC communication. As a result, in contrast to the conventional multi-path RF channel, a VLC channel is no longer a discrete sequence of a small number of signal paths, but rather a continuous combination/clusters of signal paths reflected by the entire environment – a direct consequence of the diffusive reflection of visible light. Such a drastic change on channel characteristics imposes new security features on VLC communication, and requires a different method to investigate than its well-studied RF counterparts.

With that in mind, in this work we attempt to investigate the intrinsic confidentiality of VLC communication as induced by its special channel characteristics. We consider the issue of communication confidentiality, because eavesdropping has been foreseen as the most common threats faced by VLC communications once they are deployed [7, 9, 68]. In contrast to many existing confidentiality studies that take measures at upper layers of the network protocol stack, such as access control, password protection, and end-to-end encryption, our investigation takes a physical-layer security perspective and targets at the fundamental issue of VLC channel's secrecy capacity, by characterizing how easily a VLC signal would be overheard when it is transmitted over the channel. Note that our study aims at understanding the intrinsic security limits faced by the VLC signal itself, which is independent from any cryptographic measures that could be added on the upper layers. Our work is also distinguishable from other VLC security papers [69, 70, 71, 72] that aim at exploiting physical layer features to provide encryption in the sense that our focus is on the intrinsic information-theoretic secrecy limits of the channel, while their studies are from the operational/implementation perspectives of VLC systems. In

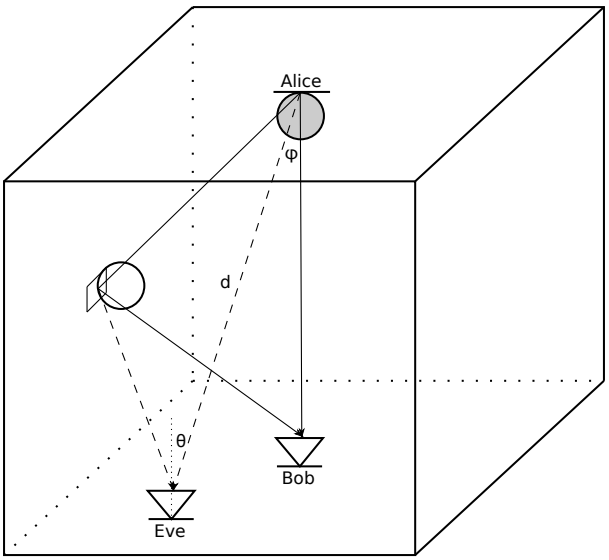

Figure 3.1: A typical indoor VLC network system with Alice, Bob and Eve considering reflections.

practice, our study may lead to a better design of VLC transceivers that possess certain built-in eaversdropping-proofness, and may be used in orthogonal with upper-layer cryptographic methods to further enhance the security of VLC systems.

3.2 VLC channel modelling

In a typical indoor VLC system (Figure 3.1), data signal is transmitted by modulating the output intensity of the emitter (Alice), and then it is captured using simple photo-diodes as receivers (Bob or Eve). As the indoor optical wireless channel is significantly different from the RF channel, statistical propagation models developed for the RF, which characterize the multipath fading, can't be directly applied to VLC. Accounting for the multiple types of reflections in the indoor VLC system requires a distinct channel modeling that is able to capture the unique characteristics of a VLC channel. In particular, a VLC channel response could be decomposed into the line of sight (LOS) path component and the non-line of sight (NLOS) path component, which are described respectively as follows.

According to [30], the emitter source is modeled as a generalized Lambertian radiation pattern

$$P(m, \phi) = \frac{m+1}{2\pi} \cos^m(\phi) \tag{3.1}$$

where m is the Lambertian order defining the radiation lobe, which specifies the directivity of the source, ϕ is the angle between the initial direction of ray and the direction of maximum power, which specifies the emitting angle. The coefficient $(m+1)/2\pi$ ensures that integrating radiation intensity pattern over the surface of a hemisphere can obtain the source power. $m = 1$ corresponds to a traditional Lambertian source.

So, the LOS path gain can be calculated as

$$h_{LOS} = P(m, \phi) A_D \cos(\theta) \frac{1}{d^2} \delta(t - \frac{d}{c}) \tag{3.2}$$

where A_D is the detecting surface area of the receiver, θ is the incident angle between incident light and the receiver normal direction, product of both gives the effective collection area of the receiver. d is the LOS distance between the emitter and receiver, which depicts the geometric attenuation. c is the speed of light and Dirac delta function gives the time delay.

Multipath channel gain due to the reflections by the walls was studied in [27]. The proposed deterministic model calculated the reflection channel gain by partitioning a wall into many elementary reflectors and summing up the impulse response contributions from different reflectors as secondary sources until reaching the time limit. However, there is a problem with this model, in that they only take into account diffusive reflection and can't simulate specular reflection when light reaches a wall. In reality, for grazing incidence there is strong specular reflection with quite different behavior. If there are polished surface, such as windows or mirrors, the specular reflection is dominant over diffusive reflection. In order to consider the high specular reflection of smooth surfaces, here we use the Phong's model to approximate the reflection patterns (Figure 3.2), considered as the sum of the diffusive component and the specular component [33, 73]. In this model, the surface characteristics are defined by two parameters: the percentage of incident signal that is reflected diffusely r_d and the directivity of the specular component of the reflection m''. Due to the high attenuation, in this paper, we consider only the first reflection since the channel gain of the higher order reflections is small enough to be neglected [33].

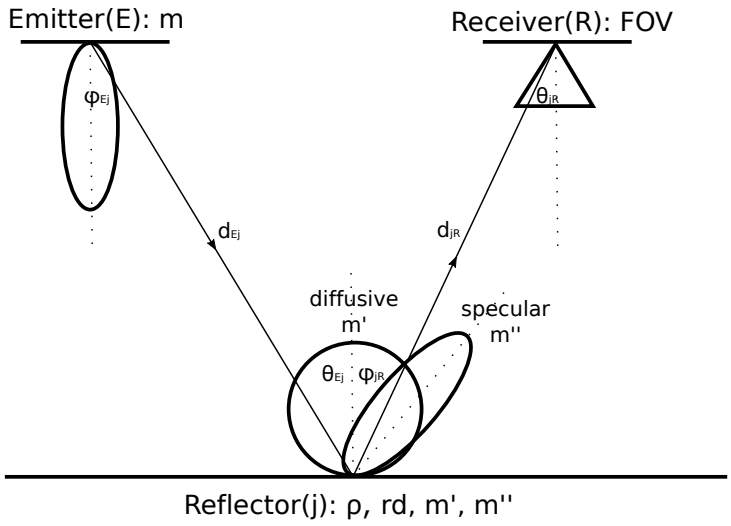

Figure 3.2: Reflection pattern is described by Phong's model.

So, the NLOS path gain can be described as

$$h_{NLOS} = \sum_{j=1}^{n} P(m, \phi_{Ej}) \Delta A \cos(\theta_{Ej}) \frac{1}{d_{Ej}^2} \rho_j \left[r_{dj} P(m', \phi_{jR}) + (1 - r_{dj}) P(m'', \phi_{jR} - \theta_{Ej}) \right] A_D \cos(\theta_{jR}) \frac{1}{d_{jR}^2} \delta \left(t - \frac{d_{Ej} + d_{jR}}{c} \right) \tag{3.3}$$

where the wall is divided into n grid reflectors, each of which has an area of ΔA, ρ is the surface reflection coefficient, m' gives the directivity of the diffusive reflection component and m'' gives the directivity of the specular reflection component, ϕ and θ represent emitting angle and incident angle, respectively. Such a model is general enough to accommodate various reflection settings of the wall. For example, for a wall of homogeneous material, ρ_j and r_{dj} are identical for all the grids, so the subscript j can be dropped in the notation, resulting in a common setting of ρ and r_d in the channel model. For a wall of heterogeneous materials, e.g., a glass window embedded in the wall, different ρ_j and r_{dj} should be used for different areas of the wall, reflecting the heterogeneous reflection behavior of the different parts of the wall.

Therefore, the channel gain considering both the LOS and NLOS can be described as

$$H = h_{LOS} + h_{NLOS}. \tag{3.4}$$

Table 3.1: Main notations

Notation	Explanation	Notation	Explanation
m, m', m''	Lambertian directivity order	I_{LOS}	LOS intensity
ϕ	Emitter radiation angle	I_{NLOS}	NLOS intensity
θ	Receiver incident angle	Δt	Time delay between NLOS and LOS
d	Transmission distance	α, β	Gamma fitting parameters
ρ	Reflection coefficient	H_B, H_E	Channel gain
r_d	Diffusive percentage	σ_B^2, σ_E^2	Variance of noise
ΔA	Reflector effective area	$I(X;Y)$	Mutual information between X and Y
A_D	Receiver effective area	ξ	Dimming target
c	Speed of light	A	Maximum optical intensity

We use a modified Monte Carlo ray-tracing statistical approach to numerically calculate the channel impulse response, as explained later in the experimental section. In case that the consideration of higher order reflections is desirable, it can be recursively calculated by a nested ray tracing model. For example, the second-order reflection can be considered by treating the first-order reflected light at each grid as a secondary light illumination source. For each secondary light source, the proposed Monte Carlo ray tracing model (Equations (2) and (3)) can be applied to compute its contribution to the second-order reflection. The actual second-order reflection is just the summation of the contribution from all secondary light sources.

To improve the readability of our paper, we summarized the main notation in Table 3.1.

3.3 Channel Impulse Response fitting and synthesizing

Although the channel impulse response with multiple reflections could be numerically calculated using different approaches, there is lacking an analytical expression for it in current literature. The main drawback of the numerical methods is their excessive computational time complexity. Due to the additional NLOS reflections, numerical computation of the impulse response of a single VLC channel turns out to be very time consuming, and it becomes even more prohibitive when one needs to calculate the channel response as a function of the VLC link location over the entire communication space, e.g., to characterize the spatial distribution of the VLC channel secrecy capacity. Therefore, for the very first time, we propose a fast analytical approach to synthesize channel impulse response using gamma probability distribution function fitting and Deep Neural Network regression.

3.3.1 Channel Impulse Response Fitting As A Gamma Probability Distribution

When analyzing the numerically calculated channel impulse response (Figure 3(a)), we notice that it could be divided into two distinct components, LOS and NLOS. The LOS component is a scalar channel gain related to the propagation attenuation of the VLC signal over the distance between the transmitter and the receiver, and can be easily calculated according to the channel model and system geometry. On the other hand, however, the NLOS component is much more complicated, as it presents some time-series structure, as shown in Figure 3(b), where the NLOS impulse response has been normalized by the total NLOS light intensity. Based on the fact that the integral of the normalized NLOS time series equals to one, we hypothesize that this time series can be fitted analytically by some probabilistic distribution function. Physically, this hypothesis reflects the insight that the NLOS channel response is actually the distribution of the reflected light power over different time delays[74]. To verify our hypothesis, we have tested a number of probabilistic distribution functions, among which the gamma distribution turns out to be the most promising one for the fitting.

A gamma distribution can be parameterized in terms of a shape parameter α and a rate parameter β. The corresponding probability density function (PDF) in the shape-rate parametrization is

$$f(x;\alpha,\beta) = \frac{\beta^{\alpha}x^{\alpha-1}e^{-\beta x}}{\Gamma(\alpha)};\ x>0;\alpha,\beta>0 \tag{3.5}$$

where $\Gamma(\alpha)$ is the gamma function. Given a numerically computed NLOS channel response, its fitted gamma distribution expression (i.e., the fitted parameters (α,β)) can be obtained by nonlinear regression. For instance, Figure 3(c) plots the fitted gamma distribution function for the numerically calculated and normalized NLOS channel impulse response in Figure 3(b). The fitting in this case turns out to be very accurate according to the normalized mean square error (normalized $mse < 0.002$). To graphically assess how well the numerical calculation matches with the fitted gamma distribution, a scatter quantile-quantile (Q-Q) plot is shown in Figure 3(d), where the calculated set (X) and fitted set (Y) of quantiles are plotted against each other. The cross points (+) are referred to as percentiles, below which a certain proportion of the data fall. Ideally, if X and Y quantiles come from the same distribution, then all + marks

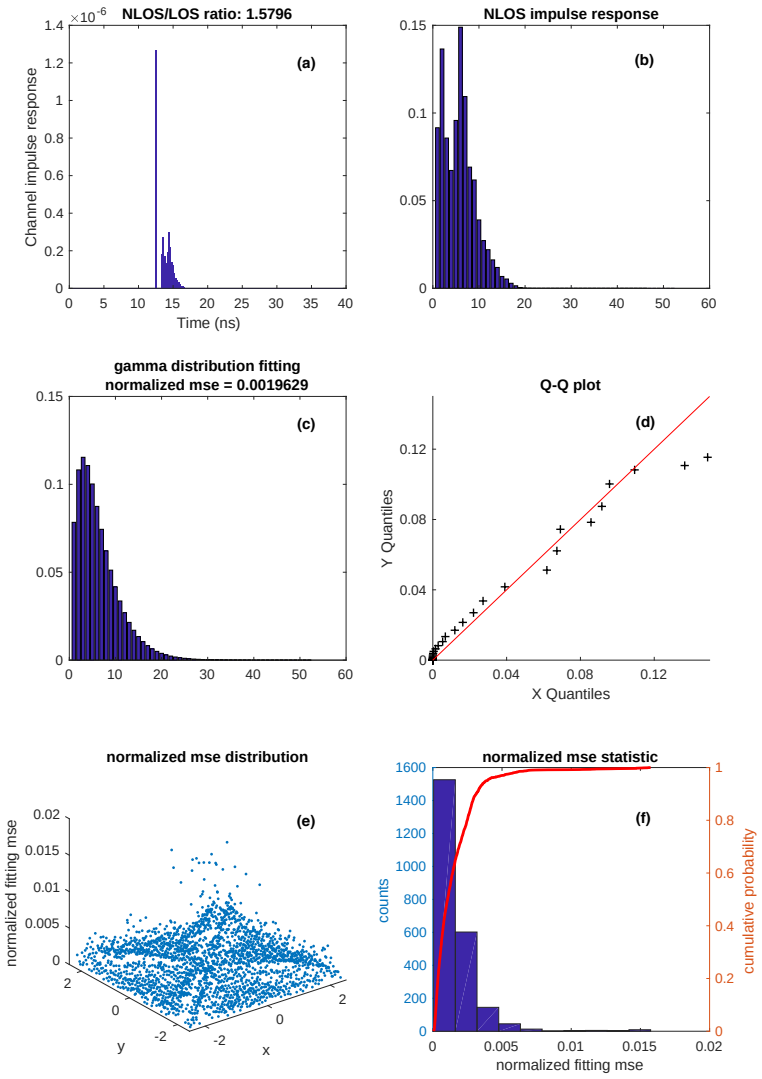

Figure 3.3: A typical example of channel impulse response fitting. (a) a numerically calculated channel impulse response with LOS and NLOS; (b) the NLOS impulse response normalized with total NLOS intensity; (c) the fitted NLOS impulse response; (d) Q-Q plot to evaluate the fitting result; (e) normalized fitting mse spatial distribution over the experimental area; (f) normalized fitting mse statistic from e.

should be aligned along the diagonal line (the red line in the figure). Indeed, it can be observed in Figure 3(d) that most of the + marks are aligned well with the diagonal line, except a couple exceptions, which are just a little off the diagonal line. This observation confirms that the fitted gamma distribution matches reasonably well with the numerical calculations.

In order to statistically verify the accuracy of gamma fitting for more general cases, we compared the calculated NLOS channel response against their gamma fitting outcomes in Figures 3(e) and 3(f) for 2401 VLC channels, which are taken over a 49-by-49-grid area with a distance interval of 0.1 m per grid, in an indoor VLC communication environment. According to the spatial distribution of the normalized mse in Figure 3(e) and the normalized mse histogram and cumulative density function (CDF) in Figure 3(f), it can be observed that more than 2200 (i.e., over 90% of the tested VLC channels) channel impulse responses fitting achieve normalized mse less than 0.005. This exemplifies the accuracy and reliability of the proposed gamma distribution fitting in general cases.

3.3.2 Channel Impulse Response Synthesizing with Deep Neural Network Regression

Now we can analytically express the channel impulse response as a LOS scalar plus a NLOS gamma distribution, for which the key parameters include LOS intensity I_{LOS}, NLOS intensity I_{NLOS}, the time delay Δt between NLOS and LOS, α, and β. Although we can get those key parameters for some sample locations using numeric calculations, it becomes prohibitive when calculating the channel impulse response at an arbitrary location. Being aware of those key parameters are following nonlinear distribution over locations from the numeric samples, we develop a Deep Neural Network (DNN) regressor to model the key parameters of channel impulse response at an arbitrary location. In order to keep the DNN regressor as simple but effective as possible and avoid over-fitting, we defined a 4-layer deep neural network model with 3 hidden layers of 64 neurons through empirical experiments as shown in Figure 3.4. To simplify our analysis, but without loss of generality, we assume that the location of the VLC transmitter is fixed in the middle of the ceiling, and are interested in obtaining the channel impulse response as a function of the receiver's location. Accordingly, the proposed DNN has two inputs, the x and y coordinates of the receiver's location, and five outputs, I_{LOS}, I_{NLOS}, Δt,

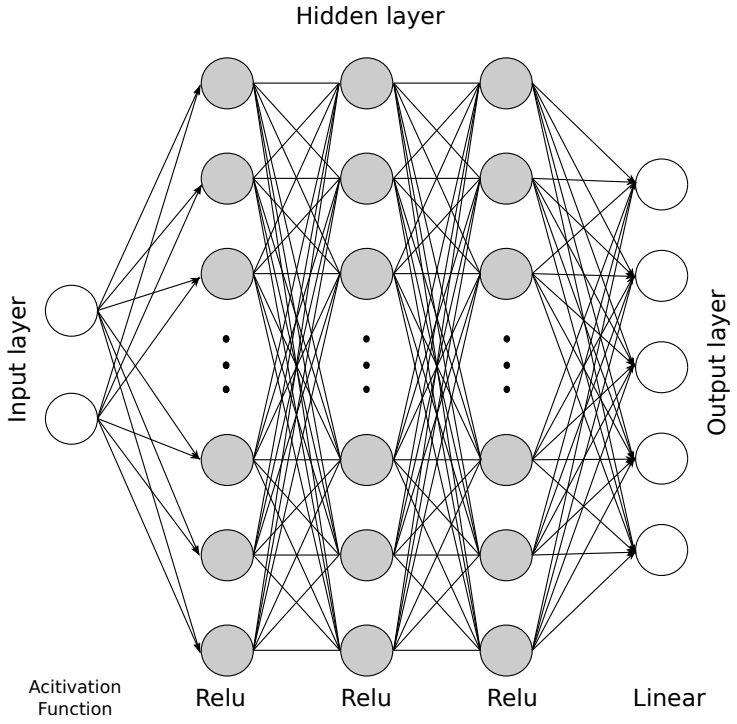

Figure 3.4: Framework of the DNN regression model. Input layer includes the x and y coordinates of receiver, output layer includes the fitted parameters for synthesizing impulse response, each of the three hidden layers includes 64 neurons. The DNN is fully connected between each adjacent layers. The activation function for each layer is listed at the bottom.

α, and β. Each of the three hidden layers includes 64 neurons with their own sets of parameters. The DNN model is set as a sequential model with loss function specified as mean square error and optimizer specified as Adam, and each layer inside this model is fully connected between its adjacent layers. As the DNN model is used as a nonlinear regression model, the activation function of the last layer is specified as linear function and the activation function for three hidden layers is set as rectified linear unit (ReLU), which is nonlinear.

The DNN regression model needs to be trained and tested before it can be used for channel response prediction at an arbitrary receiver location. The detailed procedure for DNN training and testing is presented in Section VI. Based on the predicted channel response parameters, the channel impulse response at a given receiver location can be represented analytically as

$$H = I_{LOS}\delta(t - \frac{d}{c}) + I_{NLOS}f(t - \frac{d}{c} - \Delta t; \alpha, \beta) \tag{3.6}$$

where $\frac{d}{c}$ is the light propagation delay between the transmitter and the receiver by following the LOS path, and f is the Gamma distribution function. The proposed DNN regression allows us

to efficiently obtain the channel impulse response at an arbitrary location based on an analytic function, rather than time-consuming numerical calculations.

3.4 Secrecy capacity analysis

Consider an indoor VLC system consisting of a transmitter Alice, an intended receiver Bob, and an eavesdropper Eve, as shown in Figure 3.1. Due to the diffusive and specular reflections of light, the signal transmitted from Alice to Bob may also be overheard by Eve. The received signals at Bob and Even can be represented respectively by

$$\begin{cases} Y_B = H_B X + Z_B, Z_B \sim N(0, \sigma_B^2) \\ Y_E = H_E X + Z_E, Z_E \sim N(0, \sigma_E^2) \end{cases} \tag{3.7}$$

where X denotes the transmitted light intensity from Alice, H_B and H_E denote the main channel gain, defined between Alice and Bob, and the wiretap channel gain, defined between Alice and Eve, respectively. Z_B and Z_E are zero-mean additive white Gaussian noise (AWGN) at Bob and Eve, respectively, which are assumed to be independent from each other. The variance of noise $\sigma_k^2(k = B, E)$ is given by [75]

$$\begin{cases} \sigma_k^2 = \sigma^2 + W_{ISI} \\ \sigma^2 = \sigma_{thermal}^2 + \sigma_{shot}^2 \end{cases} \tag{3.8}$$

where $\sigma_{thermal}^2$ and σ_{shot}^2 denote variances of the thermal noise in the receiver electronic circuits and the shot noise caused by ambient illumination from other light sources, respectively. These two noises are well modeled by an additive white Gaussian process. W_{ISI} denotes the inter-symbol interference (ISI) caused by the multiple reflections in a VLC channel, which may become significant under high symbol transmission rate. This is illustrated in Figure 3.5, where the ISI for symbol 4 (S4) accounts for the accumulated power from all previous symbols (S1, S2, S3) over S4's reception window $[4t, 5t]$, where $t = 1/B$ is the reception time duration of a symbol at the receiver and B is simply the symbol rate of the VLC channel (binary intensity modulation is assumed). From this figure, it is clear that the received signal power and the ISI

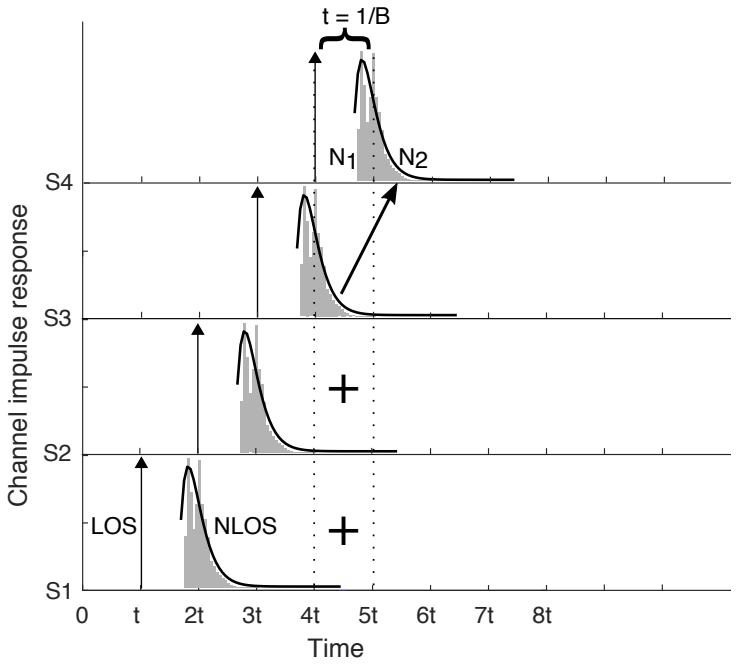

Figure 3.5: Impact of ISI on system model caused by reflection. S stands for Symbol, t stands for inter symbol time interval.

of a symbol (light pulse) can be calculated by partitioning the channel impulse response into two parts according to the symbol's reception window: The first part, denoted by N_1 in the figure, accounts for the first t seconds of the channel response inside the reception window, as measured beginning from the LOS component. The integral of N_1 contributes to the received signal power of the symbol. On the other hand, the second part, denoted by N_2 in the figure, includes all the remainder outside the reception window, whose integral amounts to the ISI (W_{ISI}) to the received symbol. So, H_k and σ_k^2 can be represented by

$$\begin{cases} H_k = N_1^{(k)} \\ \sigma_k^2 = \sigma^2 + N_2^{(k)} \end{cases} \qquad k = B, E. \tag{3.9}$$

where $N_1^{(k)}$ and $N_2^{(k)}$ are the integral of N_1 and N_2 defined w.r.t. the channel response at receiver k, respectively.

The secrecy capacity of a channel is a notion in the information-theoretic security and it represents the maximum transmission rate at which the eavesdropper is unable to decode any information while the intended receiver is able to receive all information error-free. It has been shown that under the additive white Gaussian noise (AWGN) main channel and wiretap

channel model, the secrecy capacity amounts to the difference between the main channel capacity and the wiretap channel capacity. Based on (7), if $H_B \leq H_E$, which means the main channel is stochastically degraded by the wiretap channel, the secrecy capacity C is essentially zero. Alternatively, if $H_B > H_E$, the secrecy capacity C in the same VLC network can be mathematically expressed as [46, 47, 49]

$$\begin{aligned} C = & \max_{f_X(x)} [I(X;Y_B) - I(X;Y_E)] \\ & s.t. \begin{cases} \int_0^A f_X(x)dx = 1; & 0 \leq X \leq A \\ E(X) = \int_0^A x f_X(x)dx = \xi A; & \xi \in (0,1] \end{cases} \end{aligned} \tag{3.10}$$

where $f_X(x)$ denotes the PDF of X, $I(X;Y)$ denotes the mutual information between two variables X and Y. A denotes the maximum peak optical intensity of the transmitter, ξ is the dimming target. For a practical system, the maximum optical intensity will be constrained by A and the dimmable average optical intensity will be constrained by ξ to satisfy the consistent illumination requirements.

Since the secrecy capacity is related to the information capacity of the communication channel, before determining the secrecy capacity in VLC networks it is essential to obtain the information capacity of the VLC channel with average, peak and non-negative constraints. However, to the best of our knowledge, the exact information capacity of the VLC channel with such constraints still remains unknown, even for the simplest SISO case, except that some lower and upper bounds have been derived [35, 46, 49]. In this paper, as we aim to study the impact of multiple reflections on secrecy capacity, our analysis will be based on the lower and upper bounds of the secrecy capacity. In particular, accounting for the new structure of the received signal and ISI (3.9) as induced by the multiple types of reflections in the VLC channel, and by following a similar derivation process in [46, 47, 49], we obtain a new set of lower bound and upper bound on the VLC channel secrecy capacity when the diffusive reflection and the specular reflection in the channel are considered.

Proposition 1: a lower bound for (3.10) is given by

$$C \geq \frac{1}{2} ln \left[\frac{3(\sigma^2 + N_2^{(E)})(N_1^{(B)2} A^2 + 2\pi e N_2^{(B)} + 2\pi e \sigma^2)}{2\pi e(\sigma^2 + N_2^{(B)})(N_1^{(E)2} \xi^2 A^2 + 3N_2^{(E)} + 3\sigma^2)} \right]. \tag{3.11}$$

Proof: The proposition can be proved by following the framework in [46, 47, 49]. For simplicity, we choose the average-to-peak optical intensity ratio $\xi = 0.5$ and rewrite the objective function in (3.10) in entropy as

$$C = \max_{f_X(x)} [\mathcal{H}(Y_B) - \mathcal{H}(Y_E)] - \mathcal{H}(Y_B|X) + \mathcal{H}(Y_E|X) \tag{3.12}$$

then using the entropy power inequality in [76] and given $\mathcal{H}(Y_B|X) = \frac{1}{2} ln(2\pi e(\sigma^2 + N_2^{(B)}))$, $\mathcal{H}(Y_E|X) = \frac{1}{2} ln(2\pi e(\sigma^2 + N_2^{(E)}))$,

$$C \geq \max_{f_X(x)} \left[\frac{1}{2} ln(e^{2\mathcal{H}(N_1^{(B)} X)} + e^{2\mathcal{H}(Z_B)}) - \frac{1}{2} ln(2\pi e \mathbf{var}(Y_E)) \right] + \frac{1}{2} ln(\frac{\sigma^2 + N_2^{(E)}}{\sigma^2 + N_2^{(B)}}) \tag{3.13}$$

moreover, we have $\mathcal{H}(N_1^{(B)} X) = \mathcal{H}(X) + ln(N_1^{(B)})$ and $\mathcal{H}(Z_B) = ln(\sqrt{2\pi e(\sigma^2 + N_2^{(B)})})$, so

$$C \geq \max_{f_X(x)} \left[\frac{1}{2} ln(e^{2(\mathcal{H}(X) + ln(N_1^{(B)}))} + 2\pi e \sigma^2 + 2\pi e N_2^{(B)}) - \frac{1}{2} ln(2\pi e \mathbf{var}(Y_E)) \right] + \frac{1}{2} ln(\frac{\sigma^2 + N_2^{(E)}}{\sigma^2 + N_2^{(B)}}) \tag{3.14}$$

by choosing an arbitrary input PDF $f_X(x)$ under the given constraints in (3.10), we can solve the functional optimization problem using the variational method, then $\mathcal{H}(X)$ and $\mathbf{var}(Y_E)$ can be written as

$$\mathcal{H}(X) = ln(A); \mathbf{var}(Y_E) = N_1^{(E)2} \frac{\xi^2 A^2}{3} + \sigma^2 + N_2^{(E)} \tag{3.15}$$

therefore, substituting (15) into (14), the lower bound on secrecy capacity for $\xi = 0.5$ can be derived.

Proposition 2: an upper bound for (3.10) is given by

$$C \leq \frac{1}{2} ln \left[\frac{\left((1 + \frac{N_1^{(E)2}}{N_1^{(B)2}}) \sigma^2 + \frac{N_1^{(E)2}}{N_1^{(B)2}} N_2^{(B)} + N_2^{(E)} \right) (N_1^{(B)2} A^2 \xi + N_2^{(B)} + \sigma^2)}{(\sigma^2 + N_2^{(B)}) \left(N_1^{(E)2} A^2 \xi + 2\frac{N_1^{(E)2}}{N_1^{(B)2}} N_2^{(B)} + N_2^{(E)} + (1 + 2\frac{N_1^{(E)2}}{N_1^{(B)2}}) \sigma^2 \right) \left(1 + \frac{N_1^{(E)2}(\sigma^2 + N_2^{(B)})}{N_1^{(B)2}(\sigma^2 + N_2^{(E)})} \right)} \right]. \tag{3.16}$$

Proof: The proposition can be proved by following the framework in [46, 47, 49]. The dual expression of the secrecy capacity is employed when deriving the upper bound as in [49]. Given an arbitrary conditional PDF $g_{Y_B|Y_E}(y_B|y_E)$, we have the relative entropy equation

$$\begin{aligned} &I(X;Y_B|Y_E) + E_{XY_E}\{D(f_{Y_B|Y_E}(y_B|Y_E)||g_{Y_B|Y_E}(y_B|Y_E))\} \\ &= E_{XY_E}\{D(f_{Y_B|XY_E}(y_B|X,Y_E)||g_{Y_B|Y_E}(y_B|Y_E))\} \end{aligned} \tag{3.17}$$

according to the non-negative property of the relative entropy, we have

$$I(X;Y_B|Y_E) \leq E_{XY_E}\{D(f_{Y_B|XY_E}(y_B|X,Y_E)||g_{Y_B|Y_E}(y_B|Y_E))\} \tag{3.18}$$

considering the constrains in (3.10), we can find an unique PDF $f_{X'}(x)$ that maximizes $I(X;Y_B|Y_E)$, which will lead to the secrecy capacity

$$\begin{aligned} C &\leq E_{X'Y_E}\{D(f_{Y_B|XY_E}(y_B|X,Y_E)||g_{Y_B|Y_E}(y_B|Y_E))\} \\ &= E_{X'}\left\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{Y_BY_E|X}(y_B,y_E|X) ln\left[\frac{f_{Y_B|XY_E}(y_B|X,y_E)}{g_{Y_B|Y_E}(y_B|y_E)}\right] dy_B dy_E\right\} \\ &= E_{X'}\left\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{Y_BY_E|X}(y_B,y_E|X) ln[f_{Y_B|XY_E}(y_B|X,y_E)] dy_B dy_E\right\} \\ &- E_{X'}\left\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{Y_BY_E|X}(y_B,y_E|X) ln[g_{Y_B|Y_E}(y_B|y_E)] dy_B dy_E\right\} \end{aligned} \tag{3.19}$$

each parts in (19) can be rewritten as

$$\begin{aligned} &E_{X'}\left\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{Y_BY_E|X}(y_B,y_E|X) ln[f_{Y_B|XY_E}(y_B|X,y_E)] dy_B dy_E\right\} \\ &= -[\mathcal{H}(Y_B|X') + \mathcal{H}(Y_E|X',Y_B) - \mathcal{H}(Y_E|X')] \\ &= -\frac{1}{2} ln\left[2\pi e(\sigma^2 + N_2^{(B)})(1 + \frac{N_1^{(E)2}(\sigma^2 + N_2^{(B)})}{N_1^{(B)2}(\sigma^2 + N_2^{(E)})})\right] \end{aligned} \tag{3.20}$$

and

$$
\begin{aligned}
&E_{X'}\left\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{Y_B Y_E|X}(y_B, y_E|X) ln[g_{Y_B|Y_E}(y_B|y_E)]dy_B dy_E\right\} \\
&= -\frac{1}{2}ln(2\pi s^2) - E_{X'}\left\{\frac{(1-\mu\frac{N_1^{(E)}}{N_1^{(B)}})^2(N_1^{(B)2}X^2+\sigma^2+N_2^{(B)}) + \mu^2((1+\frac{N_1^{(E)2}}{N_1^{(B)2}})\sigma^2 + \frac{N_1^{(E)2}}{N_1^{(B)2}}N_2^{(B)} + N_2^{(E)})}{2s^2}\right\} \\
&\geq -\frac{1}{2}ln\left[2\pi e\frac{\left((1+\frac{N_1^{(E)2}}{N_1^{(B)2}})\sigma^2 + \frac{N_1^{(E)2}}{N_1^{(B)2}}N_2^{(B)} + N_2^{(E)}\right)(N_1^{(B)2}A^2\xi + N_2^{(B)} + \sigma^2)}{N_1^{(E)2}A^2\xi + 2\frac{N_1^{(E)2}}{N_1^{(B)2}}N_2^{(B)} + N_2^{(E)} + (1+2\frac{N_1^{(E)2}}{N_1^{(B)2}})\sigma^2}\right]
\end{aligned}
\tag{3.21}
$$

therefore, substituting (20) and (21) into (19), the upper bound on secrecy capacity can be derived.

3.5 Experimental Design

Without loss of generality, we design an indoor VLC environment with 5 m in length, 5 m in width, and 3 m in height. Similar to Figure 3.1, the emitter is fixed at the center of ceiling and the receiver is placed on the receiver plane with a height of 0.85 m that is close to the height of a regular desk. We partition the receiver plane into small grid area with length of 0.1 m, resulting in 49-by-49-grid points taken as potential receiver location. Additional parameters assumed in the calculation are listed in table 3.2. The default parameter value will be taken from the table hereafter if not specified.

We use a modified Monte Carlo ray tracing model from [33] and [77] for numerical calculation of the channel impulse response. Our calculation is implemented using Matlab R2017a. Firstly, a large number of rays are randomly generated according to the radiation pattern from the emitter. When a ray impinges on a wall, the reflection point is converted into a new optical source, so a new ray is generated with a similar distribution as the reflection pattern of that wall. In order to consider both the specular and diffusive reflections, when a ray arrives at the wall, a random number in the range (0, 1) is generated. If the generated number is smaller than the diffusive percentage r_d, the reflection for this ray is determined to be purely diffusive; otherwise, it becomes a specular reflection. This treatment ensures that among all the rays reflected by

Table 3.2: Numerical Calculation Parameters

	Parameter	Value
Room	Room size	$5 \times 5 \times 3\, m^2$
	Reflection Coefficient (ρ)	0.8
	Diffusive Percentage (r_d)	75%
Emitter	Emitter height	3 m
	Emitted Optical Power	1 W
	Number of Rays	68000
	Modulation Bandwidth	500 MHz
	Lambertian Order (m, m', m'')	(1, 1, 250)
Receiver	Receiver height except B'_1, E'_2, E'_3	0.85 m
	Receiver height for B'_1, E'_2, E'_3	1.45, 0.25, 0.25 m
	Receiver Effective Area	$10^{-4}\, m^2$
	Receiver FOV	60°
	Resolution (Δt)	0.2 ns

any small contiguous area of the wall, we can expect that r_d fraction of them represent the diffusive reflection and $(1 - r_d)$ fraction of them represent specular reflection, which is consistent with our model in (3). After each reflection the power of the ray is reduced by the reflection coefficient of the wall. Since this model implements both diffusive and specular reflections, so it can represent real world scenarios more plausibly.

Then for each of the calculated 2401 channel impulse responses from 49-by-49-grid receivers, we use the nonlinear regression model in Matlab to fit the NLOS part of channel impulse response as gamma probability distribution. So far, we can get the seven key parameter sets, including receiver location coordinates, LOS intensity, NLOS intensity, the time delay Δt between NLOS and LOS, α, and β, which will be used as training dataset for the DNN regression model. Before feeding the training dataset into the DNN regression model, it has been preprocessed. Min-Max normalization is applied to the training dataset to guarantee stable convergence. For the sake of enabling fast and easy experimentation, the DNN regression model is implemented on Keras [78], which is a high-level neural networks Python library for deep learning and running on top of TensorFlow. The training dataset are split into two parts, of which 90% are used to fit the model and the left 10% are used to evaluate the fitting result. The two evaluation metrics mean square error and mean absolute value are shown in Figure 3.6. The overlapped curves of training and testing show the comparable error level, which indicates the DNN regression model is neither over-fitted nor under-fitted. Since mean square error gives a

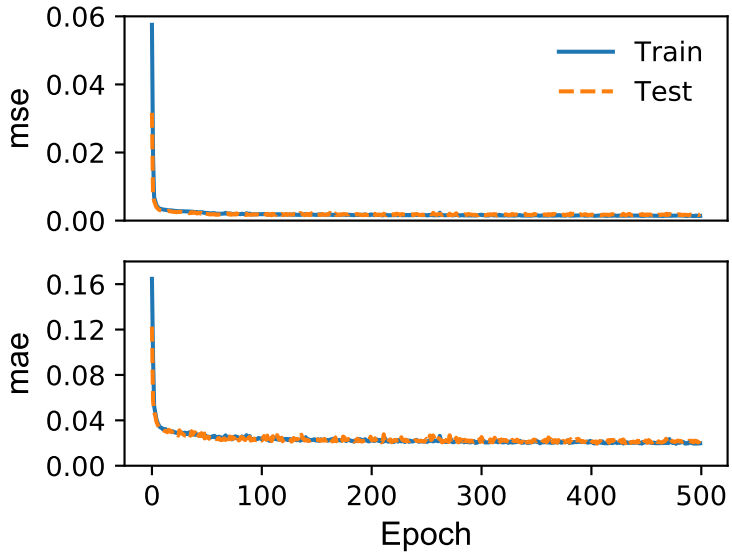

Figure 3.6: Loss function plot that shows the fitting residuals, MSE - mean square error and MAE - mean absolute error. An epoch refers to a training iteration with a random portion of training dataset.

relatively high weight to large errors, mean absolute error is used to show average deviation of fitted parameters. Both of the two metrics rapidly converge to a relative low error level, which confirms the efficacy and veracity of the training process. To give a more intuitive evaluation of the trained DNN regression model, we predicate the key parameters at the same locations of calculated training dataset. Comparison between the calculated and fitted parameters is shown in Figure 3.7. The calculated and fitted parameters for Δt, I_{LOS}, and I_{NLOS}, match well with each other. For α and β, we can also observe a reasonably good match on most of the grids except for a few mismatch over the diagonal line. In terms of the relative low fitting error level, the overall accuracy should be taken as valid.

Once the DNN regression model finishes training and testing, it can be used to predict the key parameters for synthesizing channel impulse response at any possible location inside the indoor VLC system. Finally, the synthesized channel impulse response could be substituted into equations (3.11) and (3.16) to calculate the corresponding secrecy capacity lower and upper bound. In order to quantitatively present the secrecy capacity bounds, we set the dimming target ξ as 0.5 during calculation.

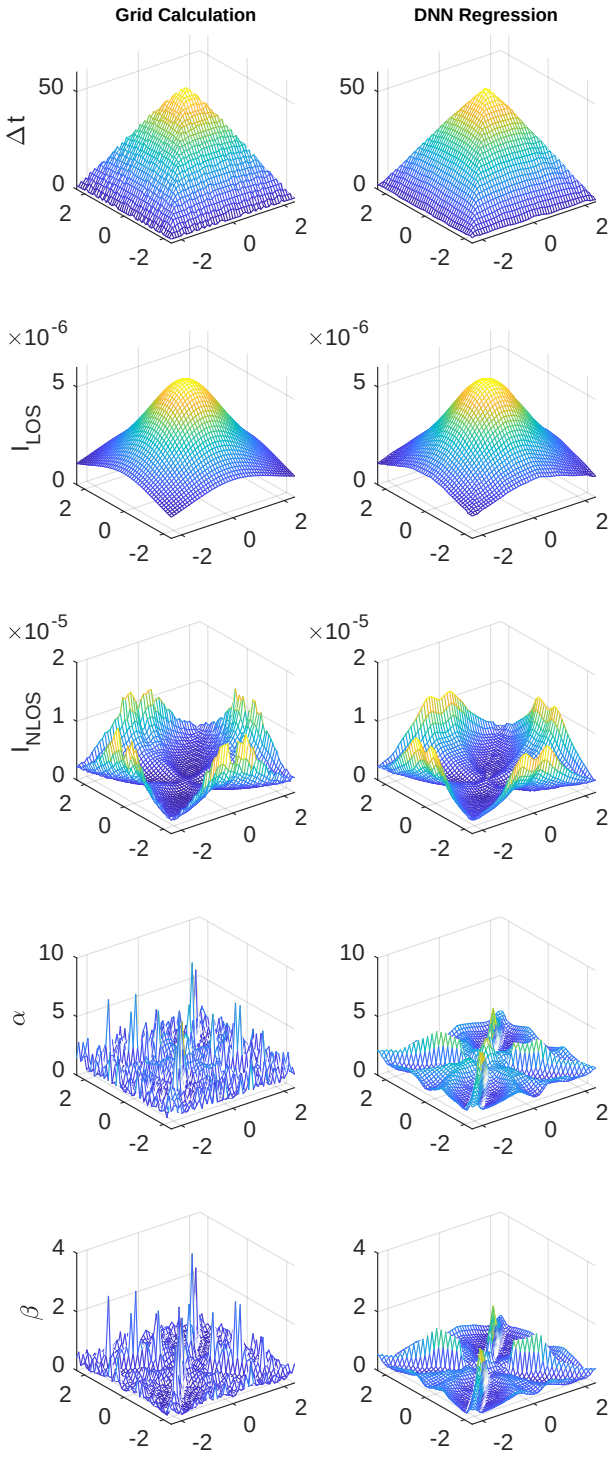

Figure 3.7: Calculated and fitted parameters comparison for Δt, LOS intensity, NLOS intensity, α, β. Left and right columns refer to the calculated and fitted results, respectively.

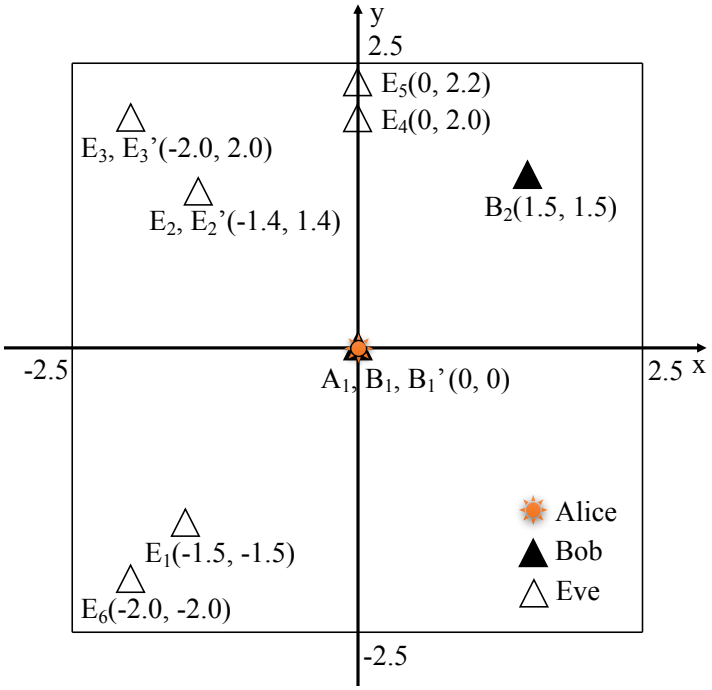

Figure 3.8: Planimetric locations of Alice, Bob, and Eve for different experimental scenarios. A_x refers to Alice, B_x refers to Bob, and E_x, E'_x refers to Eve at different height.

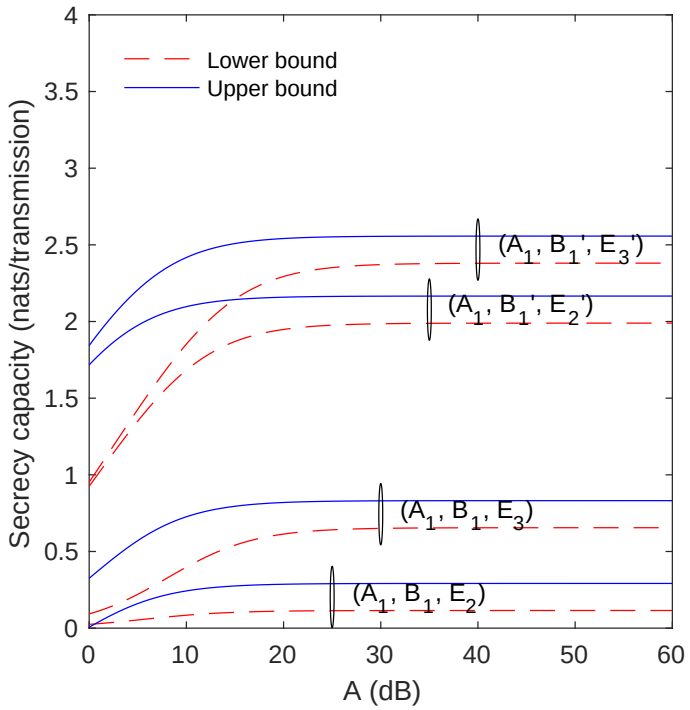

Figure 3.9: Secrecy capacity bounds versus the optimal peak intensity A when Alice locates at A_1, Bob locates at B_1 and B'_1, Eve locates at E_2, E_3, E'_2, and E'_3.

3.6 Evaluations and Discussions

In order to test the key factors that impact the secrecy capacity, we create different scenarios by changing the locations of Bob and Eve, shown as in Figure 3.8. It shows the planimetric position of Alice (yellow illuminant), Bob (black triangle), and Eve (empty triangle), with Alice locates on the ceiling, Bob and Eve locates on the receiver plane. As shown in Figure 3.9, when fixing Alice at A_1, Bob at B_1, the secrecy capacity changes with the optimal peak intensity A when Eve locates at E_2 and E_3, respectively. It is worth noting that our derivations of the upper and lower bounds are valid only when $A \geq 0$ dB, otherwise the secrecy capacity would be 0 (for $A < 0$ dB). As the increase of A, the secrecy capacity also increases accordingly until it saturates, which is consistent with previous study [46]. Moreover, if we move Eve from E_2 to E_3, the secrecy capacity increases as a result of degradation of communication channel, which indicates that the system security performance depends on the relative strength of the main channel compared to the wiretap channel. As we discussed before, for a practical VLC system, the maximum optical intensity will be constrained by A to satisfy the consistent illumination requirements. Considering maximizing the secrecy capacity and energy efficiency, we can refer to Figure 3.9 to find the minimum A that saturates the secrecy capacity as the maximum optical intensity. It can also be observed from Figure 3.9 that, while our upper and lower bounds are reasonably tight in the high secrecy capacity regime (i.e., for the cases of (A_1, B_1', E_2') and (A_1, B_1', E_3')), they are relatively loose in the low secrecy capacity regime (the cases of (A_1, B_1, E_2) and (A_1, B_1, E_3)). In particular, let the tightness of the bounds be defined as the ratio of the gap between the upper bound and the lower bound to the value of the lower bound. It can be observed from this figure that, when $A \geq 20$ dB, the tightness of the bounds is smaller than 8% for the case of (A_1, B_1', E_3'), and is smaller than 10% for the case of (A_1, B_1', E_2'). Such a tightness should be reasonably sufficient from an engineering's point of view. How to improve the bounds in the low secrecy capacity regime is out of the scope of this paper, and will be pursued in our future study.

In the following subsections, some additional numerical results are provided to show the security performance of the indoor VLC system with multiple reflections considered. We start

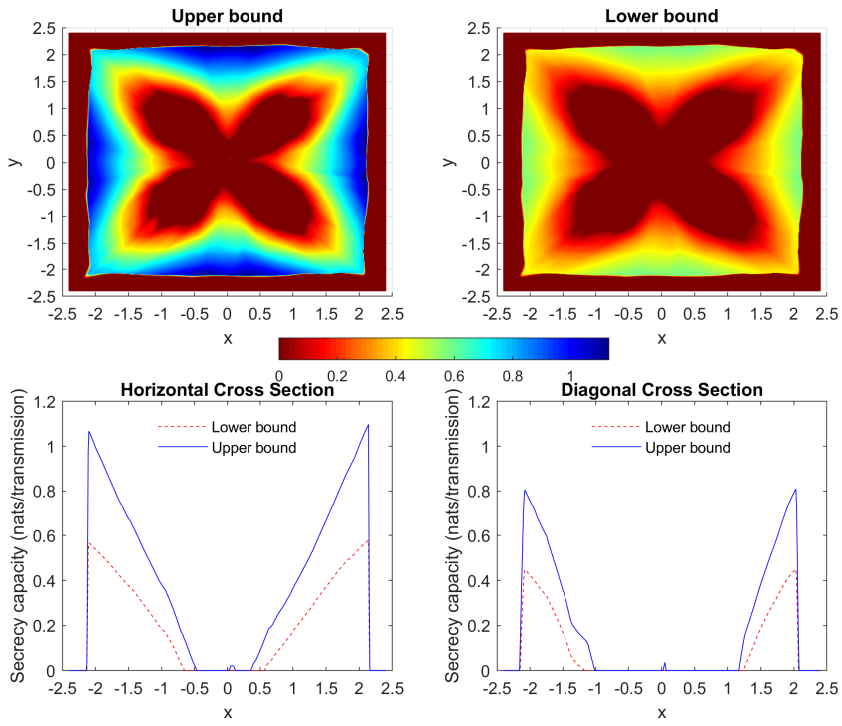

Figure 3.10: Spatial characteristics of secrecy capacity bounds when Alice locates at A_1, Bob locates at B_1, and Eve locates at any place.

from the spatial characteristics of the secrecy capacity, and then discuss the other factors that impact secrecy capacity at a specific location.

3.6.1 Spatial Characteristics of Secrecy Capacity

Since the channel impulse response could be synthesized at any possible location in the indoor VLC system, the spatial character of secrecy capacity can be calculated accordingly. Figure 3.10 shows the spatial characteristics of secrecy capacity bounds calculated for Eve locating at each grid point with an spatial interval of 0.01 m, when Alice locates at A_1 and Bob locates at B_1. The upper two panels depict the spatial pattern of the upper bound and lower bound, both of which present similar spatial characteristics. Those red regions show the vulnerable area of the VLC system, where the secrecy capacity approaches zero. They are mostly either following the diagonal line of the experimental plane or nearby the walls. The strong reflections from two adjacent walls might account for this quincunx pattern of the vulnerable zone. When receiver is approaching the walls, the intensity of NLOS part increases significantly, and it could become as strong as, or even stronger than, the intensity of LOS part. It would partially explain those vulnerable areas nearby the walls. The bottom two panels show the horizontal and diagonal

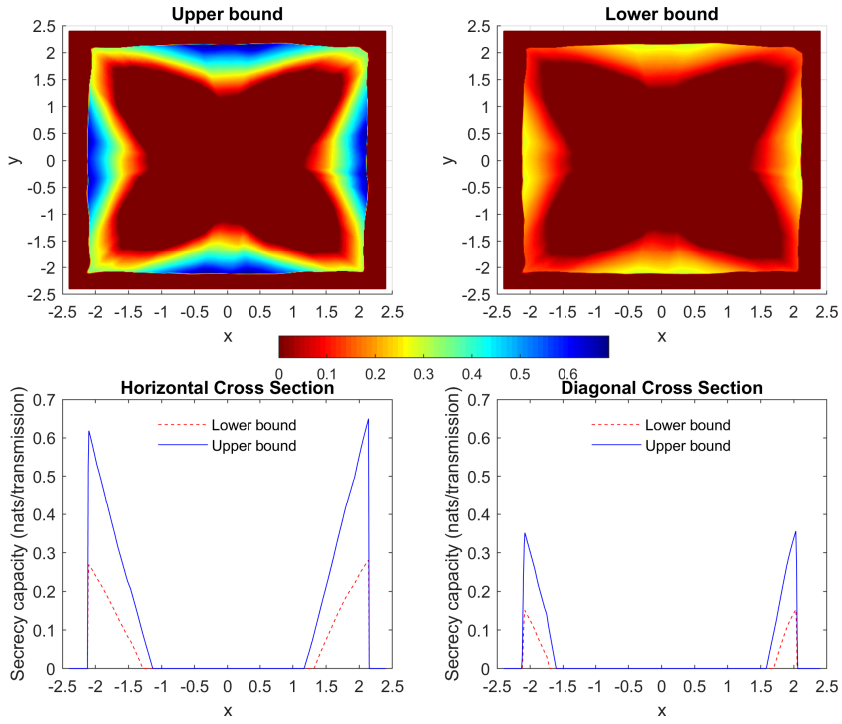

Figure 3.11: Spatial characteristics of secrecy capacity bounds when Alice locates at A_1, Bob locates at B_2, and Eve locates at any place.

cross section of the spatial secrecy capacity bounds. The relative quantity of secrecy capacity bounds is increasing from center to edge as Eve is getting far away from Bob. It's worthwhile to point out that there is a secrecy capacity cutoff on both sides, and it turns out to be result of the fixed modulation bandwidth as approaching the walls, which will be discussed in the next subsection. We can conclude that areas with secrecy capacity approaching zero fall into three cases: 1. when Eve is located nearby Bob; 2. when Eve is located around the diagonal line; 3. when Eve is located nearby the walls.

If Bob is moved from B_1 to B_2, the corresponding spatial characteristics are shown in Figure 3.11. A similar vulnerability pattern can be observed from the upper two panels, but there is more vulnerable area inside the indoor VLC system. Since moving Bob from B_1 to B_2 will degrade the main communication channel, there is an increase of vulnerable area towards outside. Compared with Figure 3.10, we also notice a decrease of the relative quantity of secrecy capacity bounds, which is consistent with the degradation of the main communication channel. In real world application, it's also consistent with our real life experience as we always want the intended receiver placed at location with the best communication channel. When

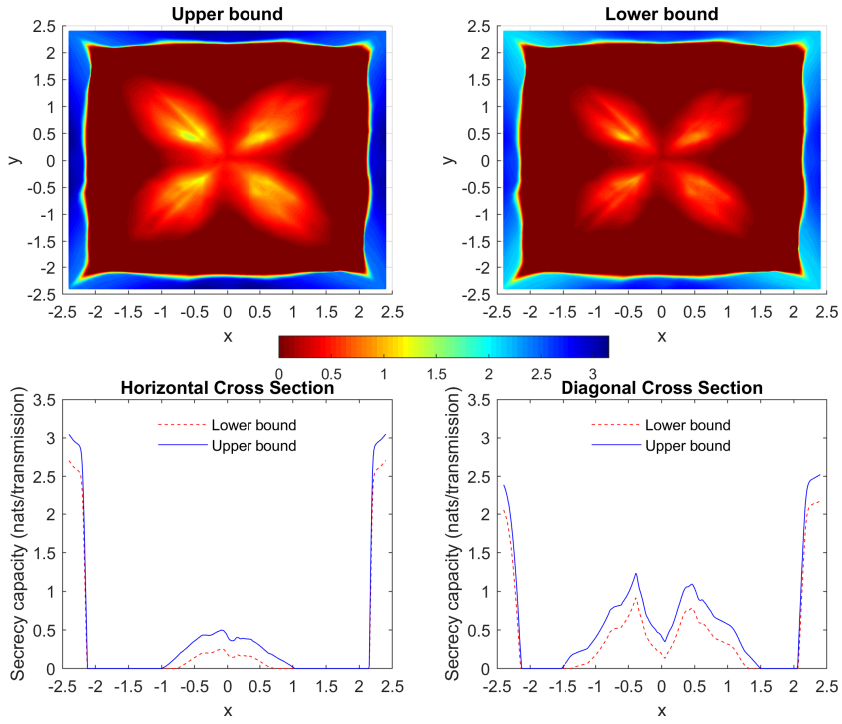

Figure 3.12: Spatial characteristics of secrecy capacity bounds when Alice locates at A_1, Eve locates at E_1, and Bob locates at any place.

we have the main communication channel set up, the spatial characteristics would be used to identify the possible vulnerable area where eavesdropping likely takes place, which could be exploited to counter data sniffing. Based on the limited vulnerable area, additional detection mechanism could be instrumented to tell when an eavesdropping attack is under way.

On the contrary, if we fix Alice and Eve at A_1 and E_1 respectively, we can get the spatial characteristics of secrecy capacity bounds when moving Bob around, which is shown in Figure 3.12. The upper two panels show the spatial pattern of the upper bound and lower bound, both of which present similar spatial characteristics, which could be used to identify the best location for Bob. Those yellow regions show the possible locations for Bob, where the VLC system secrecy capacity achieves a high value in excess of zero. The bottom two panels show the horizontal and diagonal cross section of the spatial secrecy capacity bounds. Similar with the secrecy capacity cutoff in previous scenario, there is also a secrecy capacity uplifting nearby the walls due to the strong reflections and fixed modulation bandwidth. In such a scenario, when the location of eavesdropper is known, we need to figure out the location for the intended receiver to achieve the secrecy capacity as high as possible. In reality, although an

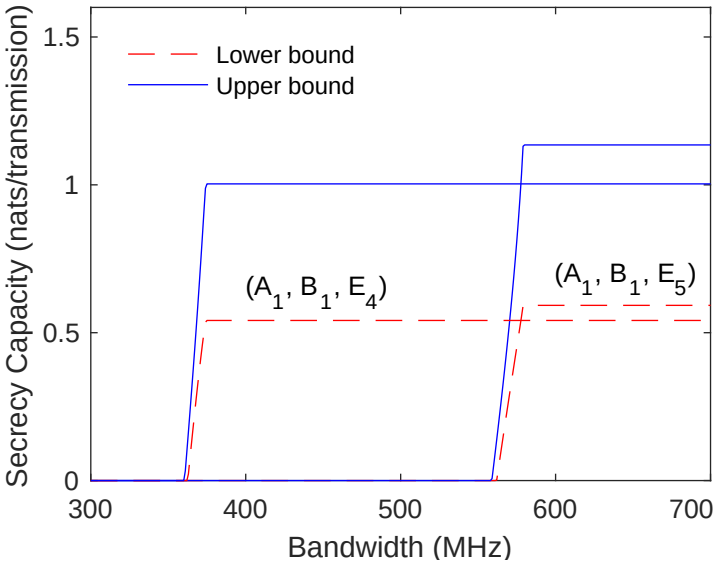

Figure 3.13: Secrecy capacity bounds changes with modulation bandwidth when Alice locates at A_1, Bob locates at B_1, and Eve locates at E_4 and E_5.

eavesdropper will always hide from the main communication channel in an unconscious place, in a typical indoor VLC system we can still assume the possible locations of eavesdropper (e.g., close to the door, around the corner), then the spatial characteristics could be used to identify the best location for the intended receiver.

3.6.2 Secrecy Capacity vs. Modulation Bandwidth

When considering the impact of multiple reflections on secrecy capacity, inter-symbol time interval (i.e., reception time duration of a symbol) is another significant factor for calculating ISI on secrecy capacity. It is determined by the reciprocal of symbol rate, as stated in section V. For simplicity, the binary intensity modulation is assumed during calculation, so the symbol rate is equivalent to modulation bandwidth if neglecting roll off factor. As long as the modulation bandwidth is determined, the inter-symbol time interval for each receiver at different location will be fixed as the same. However, the time delay from LOS to NLOS for channel impulse response of each receiver at different location will be different because of the different reflection path. So, given a location of receiver, if we change the modulation bandwidth, the impact on secrecy capacity will be identified once the inter-symbol time interval becomes comparable to the time delay from LOS to NLOS for channel impulse response. Figure 3.13 shows the change

of secrecy capacity bounds with the bandwidth when Alice locates at A_1, Bob locates at B_1, and Eve locates at E_4 and E_5, respectively.

As we move Eve from E_4 to E_5, the wiretap channel is degraded, so there is an increase of secrecy capacity as expected. From both scenarios, we see a step function shaped change of secrecy capacity when increasing the modulation bandwidth. This is because for a given location of Eve, the time delay from LOS to NLOS for channel impulse response is determined, there is an increase of secrecy capacity as increase of bandwidth when the inter-symbol time interval is approaching the time delay. Once the inter-symbol time interval gets less than the time delay, the secrecy capacity will get saturated. It acts like a cutoff frequency of secrecy capacity due to the impact of reflections. This cutoff frequency varies for each location of Eve, and it increases as Eve getting far away from the center. It could partially explain the drastic drop or rise of secrecy capacity nearby the walls as we discussed in previous subsection (Figure 3.10, 3.11, and 3.12), because we used 500 MHz fixed modulation bandwidth for those scenarios. So, when we deploy a VLC system, we will have to consider not only the quality of the communication channel, but also the modulation bandwidth, as a higher modulation bandwidth would eliminate the feasibility of eavesdropping nearby the reflector, even though it could be far away from the main communication channel.

3.6.3 Secrecy Capacity vs. Diffusive Percentage

As discussed before, each reflection is supposed to be comprised of specular and diffusive reflections depending on the roughness of the wall. Intuitively, the more rough the wall is, the more diffusive part the reflection will contain. As the increase of the diffusive percentage, we would expect to see the corresponding increase of secrecy capacity, which is verified in Figure 3.14 when Alice locates at A_1, Bob locates at B_1, and Eve locates at E_6. Since the numerically calculated channel impulse response using statistic approach for a given location varies from time to time, We calculate secrecy capacity bounds ten times for each diffusive percentage, and get the 95% confidence interval. There is a distinct increasing trend with larger uncertainty as the increase of diffusive percentage. Obviously, it would be difficult for eavesdropper to sniff effective data when most of the emitted energy are diffusely reflected. As

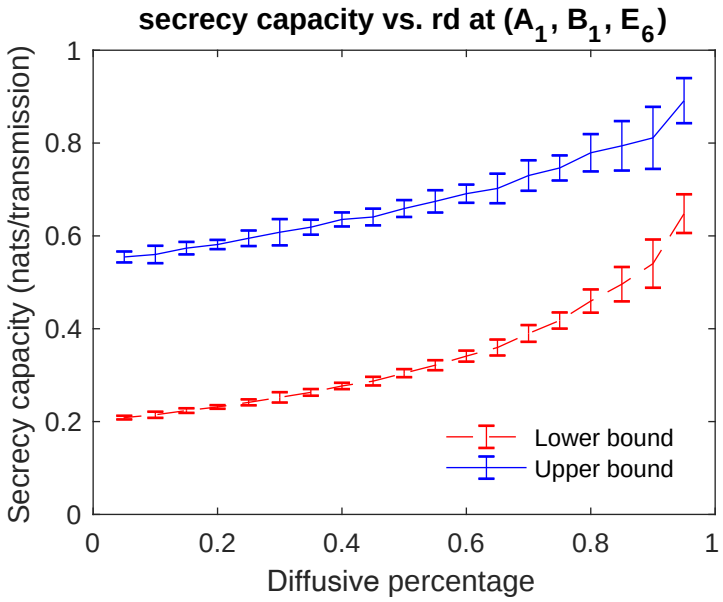

Figure 3.14: Secrecy capacity bounds change with the percentage of diffusive reflection when Alice locates at A_1, Bob locates at B_1, and Eve locates at E_6. Error bar represent 95% confidence interval.

a testbed exemplification in [6], different flooring materials (e.g., acrylic glass, vinyl plank, glazed tile, carpet, and laminate flooring) result in variable decoding bit error rate for eavesdropper, which imposes potential eavesdropping vulnerability. Thus, for indoor VLC system implementation, the construction material and design should be taken into consideration in case of security vulnerability.

3.6.4 Secrecy Capacity vs. Reflection Coefficient

On the other hand, when considering the property of the wall, the reflection coefficient is another significant factor that could impact the intensity of reflection. As for each reflection, the total emitted energy would be reduced by the reflection coefficient. Figure 3.15 shows the change of secrecy capacity with the reflection coefficient when Alice locates at A_1, Bob locates at B_1, and Eve locates at E_6. We can see a decreasing trend of the secrecy capacity with the increase of reflection coefficient, which is consistent with our intuition that high reflection coefficient would generate strong reflection and result in secrecy vulnerability. Considering the feasibility of vulnerability due to the high reflection coefficient, it would suggest to choose materials with low reflection coefficient to reduce the impact of reflections on secrecy capacity when designing an indoor VLC system. But in the real world application, according to [73],

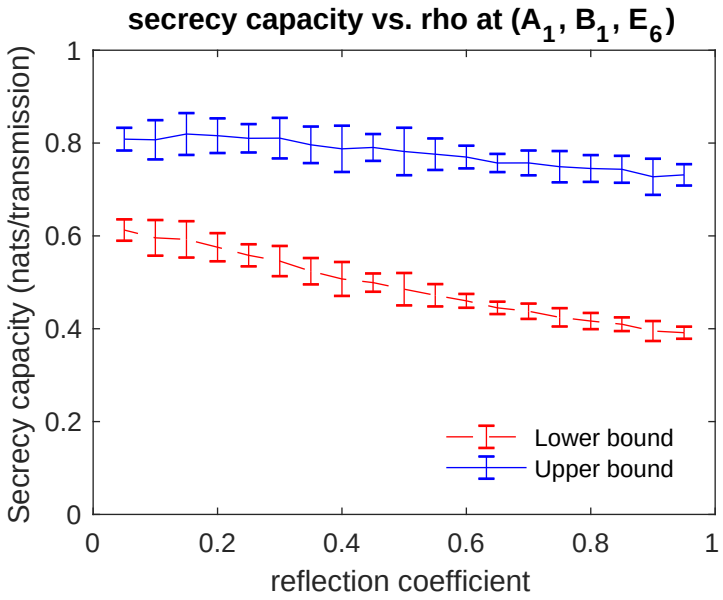

Figure 3.15: Secrecy capacity bounds change with the reflection coefficient when Alice locates at A_1, Bob locates at B_1, and Eve locates at E_6. Error bar represent 95% confidence interval.

since the VLC uses a wide spectrum in 380 $\sim$ 750 nm, spectral reflectance of indoor reflector (e.g., ceiling, floor, plaster wall, plastic wall) varies a lot, which will make the design of indoor VLC system more complicated by inducing spectrum information.

3.7 Conclusions

In this paper, the impact of multiple reflections on secrecy capacity of indoor VLC system is investigated. Base on the established indoor VLC system model with three entities, the system security performance is evaluated against a comprehensive set of factors, including the locations of the transmitter, receiver, and eavesdropper, the VLC channel bandwidth, the ratio between the specular and diffusive reflections, and the reflection coefficient, according to the calculated lower and upper secrecy capacity bounds. Both the specular reflection and diffusive reflection are considered in the system model, as the increase of the specular reflection part, the VLC system becomes more vulnerable. The spatial characteristics of secrecy capacity are also discussed, which could be used to identify possible vulnerable areas. Due to the addition of LOS and NLOS components, we have found areas with strong reflections, which makes feasible that if an eavesdropper located on those areas, he could sniff data at least partially due

to reflection. The possible sniffing attack could also be used as an exploit on insidious attacks such as blocking and spoofing in future complex systems.

Chapter 4

Spoofing detection with redundant orthogonal coding for VL systems

4.1 Introduction

The blooming of Internet of Things (IoT) network that involves pervasive communication and sensing among large amount of smart devices makes the current radio frequency (RF) spectrum over crowded [2, 3, 4]. Emerging IoT applications such as VR/AR with high-throughput, low latency and reliability requirements make the case even worse [79]. In search of new spectrum resources, visible light (VL) technology has received a lot of interest for both communication and sensing applications since the release of IEEE 802.15.7 standard in 2011 [5]. VL is a wireless technology that uses visible light ($430 \sim 790$ THz) as the medium to transmit information (i.e., visible light communication or VLC) or sense user's activities (i.e., visible light sensing or VLS). Compared with regular RF based communication and sensing, VLC and VLS enjoy several unique benefits. Firstly, the VL spectrum is at a much higher frequency band and provides much wider bandwidth (more than 10,000X) than the RF spectrum. As a result, VLS and VLC can accommodate the ubiquitous sensing and device-to-device communication demand for IoT applications with higher throughput and lower latency than their RF counterparts. More importantly, the VL spectrum is license free and the widely available lighting infrastructure has already been installed in almost all indoor and many outdoor environments, which makes the IoT applications enjoy free spectrum and easy deployment. By piggybacking their communication/sensing signals on today's low-power solid-state LED illumination, IoT applications utilizing VLC and VLS also have higher energy efficiency than those of RF. Furthermore, because VL wave cannot penetrate walls and obstacles, visible light communication and sensing signals can be well confined within an enclosed area and cause little inter-cell interference.

This allows dense spatial reuse of the VL spectrum and help enhancing privacy and security of IoT applications where data exchange can be easily restricted through obstacles like doors, walls, and window blinds. Because of these nice features, VLC/VLS has been considered to be a promising and urgently-needed small-cell solution for offloading the crowded RF bands in 5G systems and beyond for IoT.

As more and more VLC/VLS systems are mounted on today's light fixtures, how to guarantee the authenticity of the VL signal in these systems becomes an urgent issue. This is due to the fact that almost all of today's light fixtures are unprotected and can be openly accessed by almost anyone, and hence are subject to tampering and substitution attacks. As will be clear shortly in Section 4.2.2, an attacker can easily replace an authentic LED by a rogue LED under his control to inject spoofed VL signal into user's receiver. Unfortunately, most of today's VLS applications do not have a reliable built-in signal authentication mechanism to detect these spoofed signals and hence will mistakenly accept them as authentic sensing inputs, leading to compromised sensing outcome. Similar situation also arises in VLC. For example, the attacker may first block the line of sight (LOS) of the authentic VLC link, and then subsequently point a rogue LED transmitter to the user's receiver (typically a photo-diode) to inject spoofed data to the user [9].

Ensuring the received signals are coming from the legitimate transmitters (LEDs) is the key to address the above problem. Conventionally, this is achieved either at the physical layer – by authenticating the LED hardware, or at the link layer – by authenticating the received data from the LEDs based on cryptographic algorithms. Both methods have their own limitations. In particular, a physical layer authentication method is able to tell from which LEDs a received VL signal is coming by identifying certain physical features pertinent to the LED hardware, such as the light temperature color [80], or the polarization angle [81]. For example, due to the subtle differences in the material and manufacturing conditions, LEDs of the same nominal color temperature actually illuminate light of slightly different wavelengths (i.e., different colors), which could be used as a fingerprint to identify different LEDs. The physical layer methods provide always-on authentication at the signal level, but require each LED to present sufficient and measurable differences in its hardware, which is not scalable in practice [57]. On

the other hand, a link-layer data authentication typically relies on cryptography and involves extensive computation (e.g., encryption/decryption) over the transmitted data [61, 82, 83]. While these cryptographic methods are applicable to VLC applications, as will be clear shortly in Section 4.2.2, they are often irrelevant to VLS, because typically sensing happens at the signal level, and no data (i.e., sequence of 0's and 1's) is transmitted in a VLS application.

In this paper, we present VL-Watchdog, a novel signal-level always-on spoofing detection framework for VLC and VLS systems. VL-Watchdog can be implemented as a small hardware (receiver) add-on to an existing VL system. Once deployed, the watchdog will persistently monitor the light signals in the field to ensure they are sent only from authentic (legitimate) sources. VL-Watchdog supports large-scale VL systems, i.e., one with many smart LEDs, and does not assume any physical or optical difference in the LED hardware. Instead, VL-Watchdog is based on coding. It uses orthogonal codes to encode the illumination of each legitimate LED, so that the transmitted light of a legitimate LED is identifiable by detecting the unique signal structure possessed by the received light.

Meanwhile, we need to point out that this is not the first time that orthogonal coding is used for anti-spoofing attack. In particular, there are extensive studies trying to use orthogonal coding to secure communication in RF, e.g., pilot authentication [84] and global position system counter-spoofing [85]. However, applying orthogonal coding in VL faces unique challenge because of the excessive noises introduced by the significant bandwidth gap between the photo-diode's light spectrum response bandwidth (this corresponds to the range of light wavelengths to which the photo-diode will generate an electric current) and the VL signal's bandwidth. More specifically, in RF communication, a fine-tuned band-pass filter can be conveniently used to filter out all out-band noises and extract a clean copy of the desired signal. However, in VL the light spectrum response bandwidth of nearly every type of commercially available photo-diode is much greater than VL signal's bandwidth. For example, a silicon-based photo-diode has responsive wavelengths ranging from 190 to 1100 nm, which is much wider than any VL signals ($380 \sim 700$ nm). Therefore, any light signal that is outside of the bandwidth of the desired VL signal but inside the photo-diode's light spectrum response bandwidth (e.g., ultraviolet and infrared) can also generate electric current via the photo-diode (a light-to-current conversion

device). Because this conversion is mainly based on the light intensity, these electric current cannot be separated from those converted from the true/desired VL signal, hence introducing excessive noises to the electronic signals after the photo-diode. If nothing is done, these noises can easily break the orthogonality of the encoded signal, making the orthogonal-coding based spoofing detection fail. This will be reflected by the high detection error probabilities (i.e., false-alarm and miss-detection rates) presented by the detection scheme when being used in realistic environment, where the ambient light (e.g. the sunlight) forms a good source of noises.

A naive solution to the above challenge is to use optical filter, a glass-based optical device. However, this hardware-based solution has several limitations: (1) high cost: a good-quality optical filter can easily cost hundreds of dollars, and therefore they are typically used in high-end medical and imaging devices, and rarely intended for lower-end consumer-level uses; (2) the pass band of the optical filter must match with the bandwidth of the VL signal. Practically this is difficult to achieve because, unlike those RF filters whose pass band can be fine-tuned by carefully deciding the parameters of the elements in the circuit, the pass band of the optical filter is pre-set when the device is manufactured and can not be tuned during the use phase. So it is difficult to use such a pre-set pass band to match with the various light spectrum distributions of different types of LED bulbs used in practice.

In this paper, we propose a software based solution to the above challenge. Instead of trying to suppress the out-of-band light noise in the front end (this is what the optical-filter solution attempts to do), our solution tries to use carefully designed signal processing algorithm to minimize detection error probabilities when the noises present. Such a software based solution enjoys the benefits of low cost, wide applicability and flexibility to accommodate all types of LED bulbs used in practice. To the best of our knowledge, except for our preliminary conference paper [13], this work serves as the first signal-level always-on counter-spoofing mechanism applicable to both VLC and VLS systems.

4.2 Indoor VL System Model and Spoofing Attack Model

In this section, we briefly introduce the indoor Multi-link VL system model and the spoofing attack model.

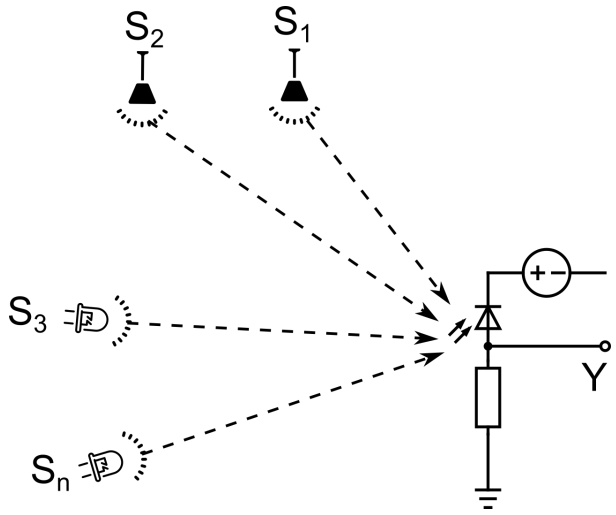

Figure 4.1: Indoor Multi-link VL channel.

4.2.1 Indoor Multi-link VL System Model

We consider a typical multi-link VL channel as shown in Figure 4.1, which is a general multi-link VL conceptual system that could be used to represent many different applications, such as visible light communication, visible light localization, and visible light sensing. A photo-diode is used to pick up the light and convert it into proportional current, which will be demodulated to a received data Y. So, the Multi-link VL channel in Figure 4.1 can be modelled as

$$Y = \sum_{i=1}^{n} h_i S_i + \omega, \tag{4.1}$$

where h is VL LOS channel gain that is calculated from geometric attenuation when the light source is assumed to follow a Lambertian radiation pattern [30], S is transmitted signal, $\omega \sim N(0, \sigma^2)$ is the noise processes that are well-modelled as signal-independent, zero-mean, additive, white Gaussian noise (AWGN). The channel gain in this multi-link VL channel model considers only LOS component and ignores reflected components from nearby reflectors. It is valid for most indoor scenarios, because regular building materials (e.g., plaster, wood, and plastic) of walls are diffusive reflectors for light, a unique characteristic of VL channel presents that the LOS component is much stronger than the non-LOS components, leading to a neglectable multipath effect [75, 86].

4.2.2 VL Spoofing Attack Model

Illuminating through an open space, the open nature of VL makes its channel inherently susceptible to spoofing attacks. This threat is especially true when it comes to most public indoor spaces, such as meeting rooms, libraries, shopping malls, and commercial airliners, where VL devices are expected to be widely deployed for sensing and communication applications in the near future. To make our presentation more concrete, in the following we describe the VL spoofing attack model based on two important example visible light sensing applications: visible light localization [87] and visible light posture sensing for human-computer interaction (HCI) [88].

Visible Light Localization (VLL)

VLL utilizes LEDs as localization anchors to compute the location of a light receiver (i.e., the user). More specifically, using a fixed light intensity P_T, each LED periodically broadcasts beacon packets that carry its location information. The beacon signals from LED i are modulated using, e.g., binary frequency shift keying (BFSK) [87], at a carrier frequency f_i. The f_i's are sufficiently separated apart from each other so that the modulated beacon signals sent by different LEDs do not overlap with each other in the frequency domain. By tuning to each carrier frequency f_i, the light receiver will be able to receive the beacon of LED i, and hence obtaining knowledge of the LED's location. Meanwhile, based on the received intensity of the beacon, say $P_R^{(i)}$, the receiver is also able to calculate the propagation path loss from LED i to the receiver as $h_i = \frac{P_R^{(i)}}{P_T}$. Based on h_i, and by applying the Lambertian channel model [30], the receiver can estimate the distance between itself and LED i (i.e., the length of the LOS propagation path). Multilateration can subsequently be used to estimate the receiver's location based on the LEDs' location and ranging information.

A rogue LED can easily impersonate a legitimate LED i in VLL by (1) blocking LED i's beacon broadcast from the receiver (this could be done, e.g., by tampering the hardware of the LED, as typically the light fixture is unprotected), and (2) switching to carrier frequency f_i and replaying beacons of LED i on that frequency. Note that in this case encrypting or digitally signing the beacons of LED i does not prevent the rogue LED from replaying these beacons, so

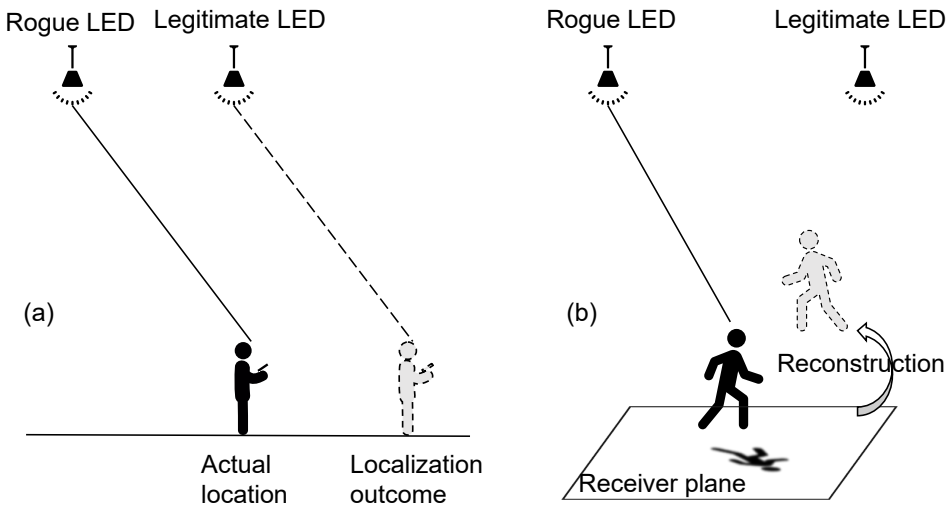

Figure 4.2: Spoofing attack scenarios: (a) VLL, (b) VLHPS.

cryptographic methods adopted at higher layers cannot stop such impersonation. Consequently, as illustrated in Figure 4.2(a), the distance between the rogue LED and the user will be misidentified by the localization algorithm as the distance between LED i and the user, leading to false localization outcome.

Visible Light Human Posture Sensing (VLHPS)

VLHPS is realized by analyzing complex shadow pattern generated by human body from different light fixtures in the environment. In particular, through optics reverse engineering, VLHPS maps the shape of a user's shadow to a posture of the user that most likely generates such a shape in the shadow [88]. To improve the accuracy of posture sensing outcome, typically multiple LEDs mounted at different locations are used to shed light on the user from different directions, resulting in a complex shadow pattern that is essentially the superimposition of the shadow components generated by each LED individually. As such, a key step in the optics reverse engineering is to separate these shadow components, including identifying the shadow component generated by each LED and extracting it from the composite shadow pattern. To make the shadow components separable, a LED i flashes its illumination at a high frequency f_i (KHz level), resulting in the shadow component generated by this LED being amplitude-modulated by the frequency f_i. The f_i's are separated sufficiently apart from each other, so that different shadow components do not overlap with each other in the frequency domain. The

component generated by LED i can then be extracted from the composite shadow pattern by using a band-pass filter of central frequency f_i.

A rogue LED can easily impersonate a legitimate LED i in the above VLHPS by (1) blocking LED i's illumination from the user, and (2) flashing its illumination at frequency f_i. Consequently, the shadow generated by the rogue LED will be mis-used by the reverse engineering algorithm as a component generated by LED i, leading to false posture sensing outcomes. For example, consider the VLHPS spoofing attack scenario illustrated in Figure 4.2(b), where for simplicity only one legitimate LED is shown. Suppose that the true posture of the user is "moving to the right", and hence the shadow generated by the rogue LED becomes longer and longer with time. However, because this shadow is mis-identified by the reverse engineering algorithm as one generated by the legitimate LED, it will be mis-mapped to a false posture sensing outcome of "moving to the left", because, based on the relative position of the user and the legitimate LED, moving to the left is the only possible posture under which a shadow generated by the legitimate LED can become longer and longer with time. Note that in this case cryptography-based counter measures are irrelevant, because the attack happens at the signal level (i.e., the shadow) and no logical data is involved in the process.

Remarks: From the above two case studies, it is clear that the major reason that such spoofing attacks can happen is because there lacks an effective method to authenticate, at the very basic signal level and on an always-on basis, that the received light signals are indeed sent from legitimate devices. Cryptographic authentication methods are either not relevant (because no data is transmitted in the application) or not effective. For example, a cryptographic authentication method may authenticate the identity of the legitimate LEDs at the beginning of the application, but it cannot prevent the application's sensing signal from being hijacked later by a rogue LED. Considering the wide applications envisioned for VL in the near future and the fact that most existing light fixtures are un-protected, spoofing attack is a highly practical and urgent issue to be addressed for VL systems.

4.3 Proposed Spoofing Detection Framework: VL-Watchdog

In this section, we present VL-Watchdog, a novel signal-level always-on spoofing detection framework for VLS and VLC systems. In the case of VLS, VL-Watchdog does not require a re-design of the existing sensing algorithm. Instead, VL-Watchdog augments over the underlying system as a small hardware (receiver) add-on. In the case of VLC, the receiver can implement the proposed framework with a small overhead to fulfill the role of VL-Watchdog for its communication link. In the following, we first introduce the intuition behind VL-Watchdog and then present its orthogonal-coding based design. Then we formulate the spoofing detection problem as a classical statistical hypothesis test, and determine the test statistic and its optimal threshold by analyzing optimal spoofing detection strategy of the watchdog under ambient light noise.

4.3.1 Overview

In the proposed VL-Watchdog framework, signals illuminated from legitimate LEDs are made orthogonal between each other. VL-Watchdog determines the authenticity of received signals by checking whether the expected orthogonality still holds in the received signals. More specifically, consider a VL system that has n legitimate LEDs $T_1, \ldots, T_n$ and a m-dimensional signal space spanned by m base vectors $A_1, \ldots, A_m$, where $m > n$, and A_i is orthogonal with A_j for any $1 \leq i, j \leq m$ and $i \neq j$. From a geometric perspective, a m-axis Cartesian coordinate system is used to represent the space, where an axis i corresponds to the base vector A_i, for $1 \leq i \leq m$. Let the whole set of all axes be denoted by $\mathbf{A} \stackrel{\text{def}}{=} (A_1, \ldots, A_m)$.

At time t, a subset of n axes are selected from the whole set $\mathbf{A}$ and are used to modulate the data bits sent by the n legitimate LEDs, one for each LED. In the case of VLC, these bits are the data to be communicated. In the case of VLS, however, these are just arbitrary bits generated by the transmitter and superimposed on the regular sensing signal after modulation. These bits can be open (i.e., it can be known as a pre-knowledge by the spoofer), and the transmitter does not need to coordinate with the receiver in generating these bits. It will be clear shortly that the value of these bits does not affect the proposed spoofing detection. We assume that the duration of each of these bits is much shorter than that of the regular sensing signal, so the

regular sensing signal can be simply viewed as a DC bias from the perspective of these bits. We also assume that the amplitude of these bits are much smaller than that of the regular sensing signal, so the superposition of these bits with the sensing signal will not affect the normal operation of the sensing algorithm. Denote the n axes that are selected at time t by the set $\mathbf{R}(t) \stackrel{\text{def}}{=} (r_1(t), \ldots, r_n(t))$, and $\mathbf{R}(t) \subset \mathbf{A}$. Without loss of generality, let us suppose that axis $r_i(t)$ is used to modulate the data of T_i, so a bit $S_i(t) \in (-1, +1)$ to be sent by T_i at time t will be modulated as $S_i(t)A_{r_i(t)}$, for $1 \leq i \leq n$. The signal $S_i(t)A_{r_i(t)}$ will be transmitted by T_i over VL channel using intensity modulation (IM), for which the intensity of the modulated signal is much weaker than that of the visible light carrier (i.e., the DC bias), so in the case of VLS the transmission of the modulated signal does not affect the normal operation of the original sensing algorithm. $\mathbf{R}(t)$ is referred to as the transmission mode of the VL system at time t. $\mathbf{R}(t)$ changes with time t according to some pseudo random schedule that is a shared secret between the transmitter of the VL system and the receiver of VL-Watchdog. After authenticating each other's identity based on any cryptographic entity authentication mechanism, such a shared secret transmission mode schedule can be established, for example, by a synchronized random number generator at the two parties, whereby the synchronization is achieved by VL transmitter sending an encrypted seed to VL-Watchdog ahead of each session.

Given the absence of any illegitimate transmissions, the received signal at the VL-Watchdog at time t, say $Y(t)$, is simply a linear combination of $S_i(t)A_{r_i(t)}$'s, for all $1 \leq i \leq n$. Such a received signal resides in the sub-space spanned by vectors $A_{r_i(t)}$'s, where $1 \leq i \leq n$, and therefore should be orthogonal to any axis j that is not in $\mathbf{R}(t)$, i.e., $\forall j \in \mathbf{A} - \mathbf{R}(t)$, which is defined as spare basis. Such an orthogonality condition can be efficiently checked by VL-Watchdog by projecting $Y(t)$ to each of the m axes and verifying that

$$\begin{cases} Y(t) \bullet A_i \neq 0 & \text{if } i \in \mathbf{R}(t) \\ Y(t) \bullet A_i = 0 & \text{if } i \in \mathbf{A} - \mathbf{R}(t) \end{cases} \tag{4.2}$$

where the operator $\bullet$ denotes inner product between two vectors.

Clearly, when an illegitimate LED presents, $Y(t)$ will include a component contributed by the spoofing signal. The only way for the orthogonality condition in (4.2) to continue to hold

(so the attack can elude from being detected), is for the spoofer to generate its signal at time t only in the sub-space spanned by vectors $A_{r_i(t)}$'s. This requires the spoofer to follow every orthogonal axis that is selected for modulation at every moment of time. But this is difficult to achieve, as $\mathbf{R}(t)$ appears to be a random process from the spoofer's viewpoint, especially when m is sufficiently greater than n. Consequently, the presence of illegitimate LED transmission will cause frequent violations of (4.2), rendering the spoofing attack detectable. Note that even though the attacker may be able to resolve $\mathbf{R}(t)$ by projecting $Y(t)$ to each axis in $\mathbf{A}$, such a projection can be performed only after $Y(t)$ is received, and therefore it does not help the attacker to generate the spoofing signal in $Y(t)$.

4.3.2 Orthogonal Coding Based VL-Watchdog Design

VL-Watchdog implements the aforementioned Cartesian coordinate system by using orthogonal coding. In particular, Walsh-Hadamard codes are used due to their simplicity and great popularity in real-world applications [89].

Walsh-Hadamard codes can be efficiently generated because they correspond to rows of the Hadamard matrix. In particular, given a Hadamard matrix $\mathbf{H}$ with size of m ($2^k, k = 1, 2, 3...$), up to m orthogonal codes, say $\mathbf{C}_1, \ldots, \mathbf{C}_m$ can be generated as follows:

$$\begin{bmatrix} \mathbf{C}_1 \\ \vdots \\ \mathbf{C}_m \end{bmatrix} = \mathbf{H}_m = \begin{bmatrix} \mathbf{H}_{m/2} & \mathbf{H}_{m/2} \\ \mathbf{H}_{m/2} & -\mathbf{H}_{m/2} \end{bmatrix} \text{ where } \mathbf{H}_1 = [\mathbf{1}]. \tag{4.3}$$

From a geometric perspective, if the Hadamard matrix expands to be a m dimensional space, each pair of orthogonal codes represents two perpendicular vectors in it, so the m orthogonal codes constitute the m orthogonal basis in such a space.

In VL-Watchdog, the aforementioned base vector set $\mathbf{A}$ is implemented as the set of orthogonal codes $(\mathbf{C}_1, \ldots, \mathbf{C}_m)$, so an axis i in the Cartesian coordinate system is represented by code $\mathbf{C}_i$, for $1 \leq i \leq m$. The modulation process is simply implemented by convolving each transmitted signal with the assigned orthogonal code, which will expand the transmitted signal

into a much higher frequency band (e.g., at 100 KHz level). The same orthogonal code is used by VL-Watchdog to perform the signal projection defined in (4.2).

For a VL system of n legitimate LEDs, the received signal at VL-Watchdog at time t can be modelled as

$$Y_j(t) = \sum_{i=1}^{n} h_i S_i(t) C_{(r_i(t),j)} + \omega_j \text{ for } 1 \leq j \leq m \tag{4.4}$$

where h is the VL LOS channel gain, $S(t)$ is the signal bit to be sent by each legitimate LED, C_{ij} is the orthogonal code chips from $\mathbf{C}_i$ and $r_i(t)$ is the selected orthogonal code index from $\mathbf{R}(t)$ at time t, ω is the ambient light noise and interference that could be well-modelled as AWGN. The projection process mathematically constitutes a correlation of the received signal with all the orthogonal codes. So, the detected signal at VL-Watchdog at time t can be mathematically calculated as

$$\begin{aligned} S_i(t)' &= \frac{1}{m} h_i^{-1} \sum_{j=1}^{m} Y_j(t) C_{ij} \\ &= \begin{cases} S_i(t) + \frac{1}{m} h_i^{-1} \sum_{j=1}^{m} \omega_j C_{ij} & \text{if } i \in \mathbf{R(t)} \\ \frac{1}{m} h_i^{-1} \sum_{j=1}^{m} \omega_j C_{ij} & \text{if } i \in \mathbf{A} - \mathbf{R(t)} \end{cases} \end{aligned} \tag{4.5}$$

Since there are non-zero projections on the complementary subset of $\mathbf{R}(t)$ caused by AWGN interference in (5), a certain threshold τ is essential to reduce the probability of false detection.

As an example shown in Figure 4.3, there are 2 legitimate transmitters, S_1 and S_2. Each of them transmits a random binary signal, which is represented by a high (1) or low (-1) signal in order to be distinguished from light-off signal (0). Then the input signal are encoded into transmitted chips with the assigned orthogonal code $r_i(t)$ from the transmission mode $\mathbf{R}(t)$ at t moment. For simplicity, here we choose the least 4-chip Walsh-Hadamard codes for illustration purpose, which will supply at most 4 orthogonal codes to expand as 4 dimensional space and it will leave 2 redundant codes as spare basis for spoofing detection. The transmitted chips will be amplitude modulated as 2 levels of LED intensity and they will be accumulated and quantized to multi-level intensity signal and represented by received chips (S_t) on the receiver side. As a result, the received chips will be projected onto all the orthogonal basis as detected

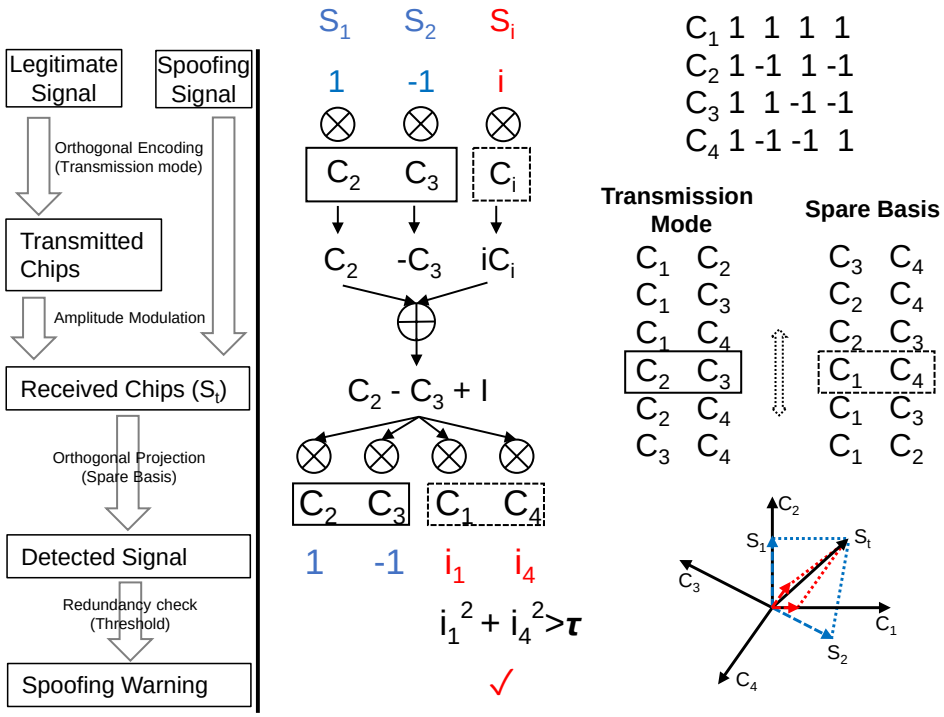

Figure 4.3: Simple example of spoofing detection framework using orthogonal coding.

signal. From the geometric perspective, the encoding and projection process performs like vector composition and decomposition in the 4 dimensional space spanned by orthogonal codes (Figure 4.3). If the same orthogonal codes from $\mathbf{R}(t)$ are used in the projection process, it will exactly reconstruct the legitimate signal S_1 and S_2 at the receiving end. If the corresponding orthogonal codes within spare basis are used, it is supposed to output zero signal when there is no spoofing attack, otherwise any significant non-zero signal detection on the spare basis would indicate a potential spoofing attack once the total accumulated power exceeds the predefined threshold τ.

It is worth noting that the received signal intensity is accumulated from different transmitters in the multi-link VL system, so the proposed orthogonal coding based VL-Watchdog piggybacks on the unique linear superposition characteristics of VL due to its high frequency, which is invalid in the low frequency RF system. Since there are few experiments in the literature that validate the communication effectiveness of the multi-link VL system with orthogonal coding, a proof-of-concept testbed is developed shortly in Section 4.4 to verify the feasibility of the proposed VL-Watchdog with orthogonal coding.

4.3.3 Spoofing Detection under Noise

For a given indoor multi-link VL system, the proposed VL-Watchdog aims to determine whether there is a spoofing attack or not in a reasonable amount of time. Under the proposed VL-Watchdog framework, any non-zero projection detected on the spare basis could be only due to noise or spoofing. In order to differentiate the spoofing attack from noise, we propose a statistical hypothesis test based on the average signal power projected on all spare basis during a given time window T that consists of s time slots, say $t_1, \ldots, t_s$, each with its randomly assigned transmission mode $\mathbf{R}(t)$. More specifically, the null hypothesis is given as

$$\mathcal{H}_0 : \text{no spoofing (i.e., noise induced non-zero projection),}$$

and the alternate hypothesis is given as

$$\mathcal{H}_1 : \text{ presence of spoofing (i.e., spoofing induced non-zero projection).}$$

In this significance testing, the test statistic P is defined as the average total signal power projected on all spare basis in each time slot $t_j (j = 1, 2, \ldots, s)$. So, the observed test statistic P_{obs} can be mathematically expressed as

$$P_{obs} = \frac{1}{s} \sum_{j=1}^{s} \sum_{i} |S_i(t)'|^2, \forall i \in \mathbf{A} - \mathbf{R}(t). \tag{4.6}$$

For a given hypothesis test threshold τ, the presence of spoofing attack is declared under the condition:

$$P_{obs} > \tau. \tag{4.7}$$

The threshold τ plays an important role in the proposed spoofing detection framework, and an optimal threshold τ would maximize the spoofing detection accuracy of the VL-Watchdog. According to the maximum a posteriori (MAP) criteria, the optimal threshold τ is decided by the test statistic distribution under the null hypothesis $\mathcal{H}_0$ and alternative hypothesis $\mathcal{H}_1$, respectively, which can be analyzed as follows.

To calculate the test statistic distribution under the null hypothesis $\mathcal{H}_0$, we model the noise as AWGN shown in (4), whose amplitude projection on each spare basis i in $\mathbf{A}-\mathbf{R}(t)$ is i.i.d. and follows normal distribution, i.e.,

$$S_i(t)' \sim N(0, \frac{\sigma^2}{m}), \tag{4.8}$$

where σ^2 is the average power of the AWGN. So the total detected power P_1^j on all spare basis given the presence of only noise in time slot t_j can be calculated as

$$P_1^j = \sum_{i \in \mathbf{A}-\mathbf{R}(t)} |S_i(t)'|^2. \tag{4.9}$$

Therefore the random variable $P_1^j \frac{m}{\sigma^2}$ follows chi-square distribution with $m-n$ degrees of freedom, i.e.,

$$P_1^j \frac{m}{\sigma^2} = \sum_i \left(S_i(t)' \frac{\sqrt{m}}{\sigma} \right)^2 \sim \chi^2(m-n) \tag{4.10}$$

Therefore P_1^j follows Gamma distribution with a shape parameter of $\frac{m-n}{2}$ and a scale parameter of $\frac{2\sigma^2}{m}$, i.e., $P_1^j \sim$ Gamma$(\frac{m-n}{2}, \frac{2\sigma^2}{m})$. Over the time window T, the average total detected power on all spare basis given the presence of only noise, denoted by P_1, can be calculated as

$$P_1 = \frac{1}{s} \sum_{j=1}^{s} P_1^j. \tag{4.11}$$

So the random variable P_1 follows Gamma distribution with a shape parameter of $\frac{s(m-n)}{2}$ and a scale parameter of $\frac{2\sigma^2}{sm}$, i.e., $P_1 \sim$ Gamma$(\frac{s(m-n)}{2}, \frac{2\sigma^2}{sm})$, and its probability density function is given by

$$f_{P_1}(x) = \frac{\sigma^2}{sm} \frac{x^{\frac{s(m-n)}{2}-1} e^{-\frac{x}{2}}}{2^{\frac{s(m-n)}{2}} \Gamma(\frac{s(m-n)}{2})} \tag{4.12}$$

where $\Gamma(\bullet)$ denotes the gamma function. So, the detected test statistic distribution for given $\mathcal{H}_0$ will be calculated as

$$f_{P|\mathcal{H}_0}(x|P_1) = f_{P_1}(x). \tag{4.13}$$

To calculate the test statistic distribution under the alternative hypothesis $\mathcal{H}_1$, we consider a blind-guess spoofing strategy, in which the attacker randomly chooses $k(1 \leq k \leq m)$ orthogonal codes from the whole base vector set $\mathbf{A}$ in each time slot to generate its spoofing signal. Among the k chosen orthogonal codes, let ξ denote the number of those that happen to be in the spare basis set $\mathbf{A} - \mathbf{R}(t)$ and $k - \xi$ denote the rest of the chosen codes that are in the transmission mode set $\mathbf{R}(t)$. Clearly, ξ is a random variable that takes value from the set $0 \leq \xi \leq k$. The attacker then equally allocates its transmission power P_s onto the k chosen orthogonal codes to generate the spoofing signal. In our following analysis, we first consider the basic case that k is a deterministic number known to the hypothesis test. Based on the result of this basic case, we will then extend our analysis subsequently to the more general case that k is a random variable.

The Case of Deterministic k

In this case, the probability mass function of ξ in each time slot can be calculated as

$$\text{Prob}(\xi = k_s) = \begin{cases} \frac{C_{m-n}^{k_s} C_n^{k-k_s}}{C_m^k}, & k_s = \begin{cases} 0, \ldots, k; & 1 \leq k \leq n \\ k-n, \ldots, k; & n < k < m-n \\ k-n, \ldots, m-n-1; & m-n \leq k \leq m \end{cases} \\ \sum_{k'=m-n}^{k} \frac{C_n^{k'-m+n}}{C_m^{k'}}, & k_s = m-n; \quad m-n \leq k \leq m \end{cases} \tag{4.14}$$

where $C_i^j = \frac{i!}{(i-j)!j!}$ is the binomial coefficient of i choose j. Its expectation and variance can be calculated as

$$E(\xi) = \sum_{\xi=0}^{m-n} \xi \text{Prob}(\xi) = \begin{cases} \sum_{\xi=0}^{k} \xi \frac{C_{m-n}^{\xi} C_n^{k-\xi}}{C_m^k}; & 1 \leq k \leq n \\ \sum_{\xi=k-n}^{k} \xi \frac{C_{m-n}^{\xi} C_n^{k-\xi}}{C_m^k}; & n < k < m-n \\ \sum_{\xi=k-n}^{m-n-1} \xi \frac{C_{m-n}^{\xi} C_n^{k-\xi}}{C_m^k} + & \\ (m-n) \sum_{k'=m-n}^{k} \frac{C_n^{k'-m+n}}{C_m^{k'}}; & m-n \leq k \leq m \end{cases} \tag{4.15}$$

$$
\begin{aligned}
Var(\xi) &= \frac{1}{m-n+1}\sum_{\xi=0}^{m-n}[\xi - E(\xi)]^2 \\
&= \begin{cases}
\frac{1}{k+1}\sum_{\xi=0}^{k}\left[\xi - \sum_{\xi=0}^{k}\xi\frac{C_{m-n}^{\xi}C_n^{k-\xi}}{C_m^k}\right]^2; & 1 \le k \le n \\
\frac{1}{n+1}\sum_{\xi=k-n}^{k}\left[\xi - \sum_{\xi=k-n}^{k}\xi\frac{C_{m-n}^{\xi}C_n^{k-\xi}}{C_m^k}\right]^2; & n < k < m-n \\
\frac{1}{m-k+1}\sum_{\xi=k-n}^{m-n}\left[\xi - \sum_{\xi=k-n}^{m-n-1}\xi\frac{C_{m-n}^{\xi}C_n^{k-\xi}}{C_m^k}\right. & \\
\left.-(m-n)\sum_{k'=m-n}^{k}\frac{C_n^{k'-m+n}}{C_m^{k'}}\right]^2; & m-n \le k \le m
\end{cases}
\end{aligned} \tag{4.16}
$$

As the attacker is randomly selecting k orthogonal codes in each time slot, ξ's in time slots $t_j(j = 1, 2, \ldots, s)$ are i.i.d. Given a sufficiently large number of slots in the time window T (e.g., greater than 10 slots in T), according to the central limit theorem, the average number of orthogonal codes that are chosen by the attacker in a time slot but are not in the underlying transmission mode set of that slot should approximately follow a normal distribution, i.e.,

$$
\overline{\xi} \sim N(E(\xi), \frac{1}{s}Var(\xi)). \tag{4.17}
$$

Thus, the average total detected power on all spare basis given the presence of spoofing in an arbitrary slot is given by $P_2 = \frac{P_s}{k}\overline{\xi}$. Clearly, P_2 also follows a normal distribution:

$$
P_2 \sim N(\frac{P_s}{k}E(\xi), \frac{P_s^2}{sk^2}Var(\xi)) \tag{4.18}
$$

and its probability density function is

$$
f_{P_2}(x) = \frac{1}{\sqrt{\frac{2\pi P_s^2}{sk^2}Var(\xi)}}e^{-\frac{1}{2}\frac{sk^2(x-\frac{P_s}{k}E(\xi))^2}{P_s^2 Var(\xi)}}. \tag{4.19}
$$

So, the test statistic distribution given $\mathcal{H}_1$ can be calculated as

$$
f_{P|\mathcal{H}_1}(x|P_1 + P_2) = f_{P_1+P_2}(x) \approx f_{P_2}(x). \tag{4.20}
$$

Here the approximation is due to the fact that the power of spoofing signal is usually much stronger than that of the AWGN (i.e., $\frac{P_s}{\sigma^2} \gg 1$), so noise power can be safely neglected from the test statistic.

Given an equally-probable a priori distribution between $\mathcal{H}_0$ and $\mathcal{H}_1$, i.e., $\text{Prob}(\mathcal{H}_0) = \text{Prob}(\mathcal{H}_1) = 0.5$, the MAP criteria downgrades to the maximum likelihood (ML) criteria. Therefore the optimal detection threshold τ^o can be determined by solving the following equation

$$\frac{f_{P|\mathcal{H}_1}(\tau^o|P_1+P_2)}{f_{P|\mathcal{H}_0}(\tau^o|P_1)} = 1. \tag{4.21}$$

In practice, because $P_s \gg \sigma^2$, the solution to the above equation always exists and is unique.

The Case of Random k

In this case, let p_k denote the probability by which the attacker selects k orthogonal codes in a time slot, where $1 \leq k \leq m$ and $\sum_{k=1}^{m} p_k = 1$. The probability mass function of ξ in a time slot can be calculated as

$$\text{Prob}(\xi = k_s) = \sum_{k=1}^{m} p_k \text{Prob}(\xi = k_s|k) = \begin{cases} \sum_{k=1}^{n} p_k \frac{C_n^k}{C_m^k}, & k_s = 0 \\ \sum_{k=k_s}^{k_s+n} p_k \frac{C_{m-n}^{k_s} C_n^{k-k_s}}{C_m^k}, & 0 < k_s < m-n \\ \sum_{k=m-n}^{m} p_k \sum_{k'=m-n}^{k} \frac{C_n^{k'-m+n}}{C_m^{k'}}, & k_s = m-n \end{cases} \tag{4.22}$$

Its expectation and variance can be calculated by substituting (4.22) into (4.15) and (4.16). By following a similar derivation in the previous deterministic case, we can calculate the test statistic distribution given $\mathcal{H}_1$ from (4.19) with the updated expectation and variance in this random case. Therefore the optimal detection threshold τ^o can be determined by solving (4.21) in this case.

4.4 Proof-of-Concept Testbed for feasibility verification

As stated in Section 4.3.1, signals illuminated from legitimate LEDs are made orthogonal between each other with orthogonal coding in the proposed VL-Watchdog framework. VL-Watchdog determines the authenticity of received signals by checking the orthogonality condition in (4.2) to continue to hold in the received signals. It's clear that the presence of illegitimate LED transmission will cause frequent violations of (4.2), rendering the spoofing attack detectable, unless the spoofer could generate its signal at time t if and only if within the transmission mode sub-space. Thus, it's more crucial for us to demonstrate the feasibility of orthogonal coding on VL signals, and hence verify the feasibility of VL-Watchdog, we have developed a proof-of-concept VL orthogonal encoding and decoding testbed for a multi-link VLC system. This is described as follows.

4.4.1 Testbed Settings

Figure 4.4(a) shows a picture of our testbed. In particular, we use four commercial off the shelf (COTS) LEDs [90] from DigiKey on the transmitter side and one COTS photo-diode on the receiver side to compose a 4-channel multi-link VLC system. The LED transmitter and photo-diode receiver are placed about 10 cm apart and are controlled by an Arduino UNO R3 [91] control board, which is connected to a desktop computer (as a host) via USB. On the desktop computer, MATLAB is used to control the Arduino board via the Matlab API supplied by Arduino and also to implement orthogonal encoding and decoding.

The left part of Figure 4.4(b) shows a diagram of the transmitter circuit. In particular, the transmission is based on pulse-amplitude modulation (PAM) [30], with the DC bias at the transmitter ensuring the non-negativity of the total current driving the LEDs. On the transmitter side, a high speed serial bit stream input (S) is parallelized into 4 sub bit streams (S_1, S_2, S_3, S_4). A fixed bias current I_{DC} is superimposed with S_i ($i = 1, 2, 3, 4$) and the resulting modulated current $I_{DC} + S_i$ drives the illumination of each of the LEDs. In order to maintain linear current-light conversion and avoid clipping distortion [92, 49], a unique requirement to VLC is that the total current must be constrained within some range $I_{DC}+\alpha I_{DC}$, where $\alpha \in [0, 1]$ is the modulation index. Thus S_i is amplitude-constrained by $|S_i| < \alpha I_{DC}$, which is different from

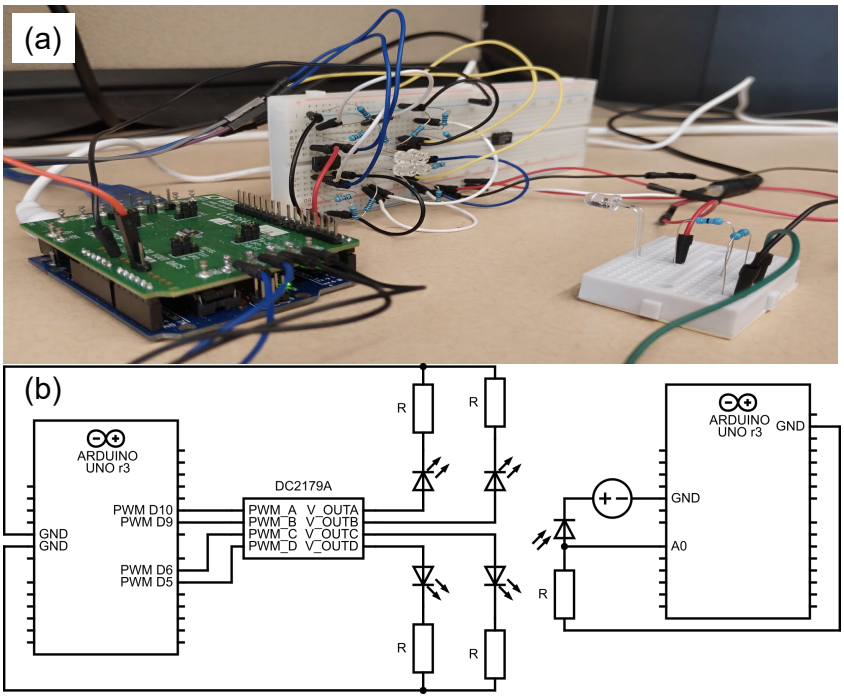

Figure 4.4: (a) Multi-link VL system prototype and (b) Transmitter and receiver circuits schematic diagram.

the common mean-power constraint in RF communication. To this end, each LED is cascaded with a current limiting resistor R of 100 Ω. The intensity-modulated signals are generated by supplying a 2-level (high or low) driving voltage to each LED. In order to generate these driving voltages, we use a COTS Analog Devices DC2179A [93] demo board that integrates with itself a LTC2645 PWM-DAC. To transmit a bit, Matlab instructs the Arduino control board to send DC2179A the digital PWM signal corresponding to the bit. This PWM signal will then be converted by DC2179A into the required voltage to drive the LEDs.

The right part of Figure 4.4(b) shows the diagram of the receiver circuit. In particular, the photo-diode works in photoconductive mode to measure the received light intensity and is driven by a 12 V DC and cascaded with a 510 Ω resistor. The received optical power is linearly proportional to the output voltage of the resistor as well as the light driven current inside the circuit. We connect the output voltage of the resistor back to Analog-In pins of Arduino control board. The recorded voltage data are quantified and processed in MATLAB to recover the transmitted signal.

All computation required in the orthogonal encoding and decoding processes are implemented using Matlab. The transmitter is responsible for converting the generated codes into VL

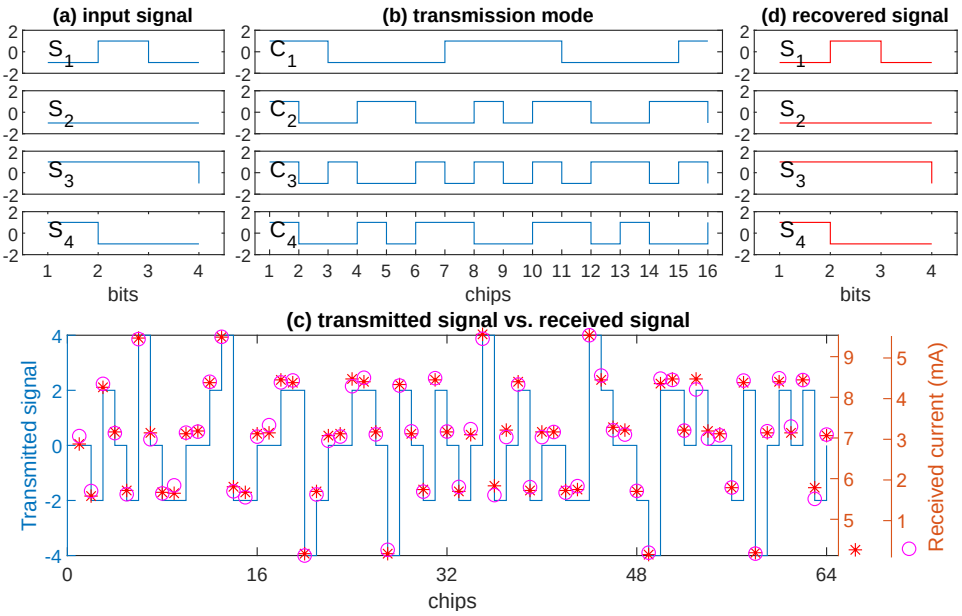

Figure 4.5: Verification of multi-link VL communication based on orthogonal coding.

signals, and the receiver is responsible for converting the received VL signals into codes based on which the transmitted bits can be decoded. To simplify our implementation but without loss of generality, the driving voltages for the 4 LED transmitters are calibrated so that the received light intensity from each of them are equalized for the same transmitted chip.

4.4.2 Feasibility of Orthogonal Coding over VL

We verify the feasibility of orthogonal coding over VL by actually transmitting and receiving coded bit stream over our testbed. Figure 4.5 shows the Matlab measurements of a representative snapshot in our experiment. In particular, Figure 4.5(a) shows a measurement of the input signals (S_1, S_2, S_3, S_4) for the 4 LED transmitters, respectively. Each input signal consists of 4 bits binary data and is encoded by a 16-bit Walsh-Hadamard code (C_1, C_2, C_3, C_4), randomly selected from the 16-chips Hadamard matrix. So the length of transmitted signal at each LED would be 64 chips. Figure 4.5(b) shows the randomly selected Walsh-Hadamard codes C_1, C_2, C_3, C_4 for each of the 4 LED transmitters, which forms the transmission mode at this moment. The sum of the transmitted signals (in blue) and the strength of the received signal as represented by the current in the receiver circuit (in read) are depicted in Figure 4.5(c). It can be observed that the multi-level pattern of the received current is fully consistent with that of the transmitted signals. After the quantization and projection process at the receiver, the received

bits in the four coding channels (C_1 through C_4) are shown in Figure 4.5(d), which verifies the successful communication of data based on orthogonal coding of the VL signals.

In order to demonstrate the feasibility over large transmission distance, we increase the distance between the LED transmitter and photo-diode to about 20 cm and replicate the testbed experiment with the same input signals and transmission mode. The strength of the received signal as represented by the multi-level pattern of current in the receiver circuit (shown as magenta circle in Figure 4.5(c)) still presents consistency with that of the transmitted signals, and further can be recovered and decoded into the transmitted bits in Figure 4.5(d) after the corresponding quantization and projection process. Thus, it verifies the the successful communication of data based on orthogonal coding of the VL signals over large transmission distance.

4.5 Numerical Evaluation

To evaluate the performance of VL-Watchdog, we resort to simulations, which allow us to measure how the proposed spoofing detector performs against a set of attack parameters.

4.5.1 Performance Metrics

We use the following spoofing detection rate PD, miss detection rate MD, and false warning rate FW to characterize the accuracy of the proposed VL-Watchdog detector:

$$\begin{aligned} PD &= \int_{\tau^o}^{\infty} f_{P|\mathcal{H}_1}(x|P_1+P_2)dx, \\ MD &= \int_{-\infty}^{\tau^o} f_{P|\mathcal{H}_1}(x|P_1+P_2)dx, \\ FW &= \int_{\tau^o}^{\infty} f_{P|\mathcal{H}_0}(x|P_1)dx. \end{aligned} \tag{4.23}$$

where τ^o is the optimal detection threshold as defined in (4.21). Based on these quantities, the precision and sensitivity measures of the detector are defined as follows:

$$Precision = \frac{PD}{PD+FW}, Sensitivity = \frac{PD}{PD+MD}. \tag{4.24}$$

The overall performance is measured by the F_1 score [94], which is defined as

$$F_1 = 2\frac{Precision \times Sensitivity}{Precision + Sensitivity} = \frac{2PD}{2PD + FW + MD}. \tag{4.25}$$

F_1 score is calculated as harmonic mean between precision and sensitivity and it represents the overall accuracy of the detector.

4.5.2 Simulation Results

We simulate a multi-link VLC system with 8 legitimate LED transmitters ($n = 8$). In each time window T, we assume that a spoofer will present randomly with a 0.5 probability. We are interested in evaluating how the VL-Watchdog will perform against a set of parameters, including the number of base vectors m, the spoofing power to noise ratio $\frac{P_s}{\sigma^2}$, the number of time slots s within the given time window, and the number of orthogonal codes k that the spoofer chooses in fabricating its spoofing signal. In each simulation we vary the value of one of the above parameters while keeping the others constant. To this end, we assume the following default value for the parameters in our simulation: $m = 16, \frac{P_s}{\sigma^2} = 5, s = 5,$ and $k = 8$. The simulation results are shown in Figure 4.6.

Impact of the Number of Base Vectors

Figure 4.6(a) shows the impact of the number of base vectors m on the spoofing detection performance. We can see that there is an optimal number of base vectors ($m = 32$), which is about four times of the number of transmitters and it maximizes the overall spoofing detection performance (F_1 score). It could be used to determine the optimal number of base vectors that should be used for a given number of transmitters in a multi-link VLC system. Additionally, there is a slight increase of overall performance before the optimal m, which could be explained by the fact that adequate increase of spare basis would benefit the overall performance. After the optimal m, we can see that with the increase of m, F_1 score decreases rapidly and the $Sensitivity$ measurement drops off while the $Precision$ measurement maintains at approximately same level. It turns out that the decline of the $Sensitivity$ measurement is mainly induced by the rapid decrease of PD, which leaves FW almost unchanged. It is not surprising because as the

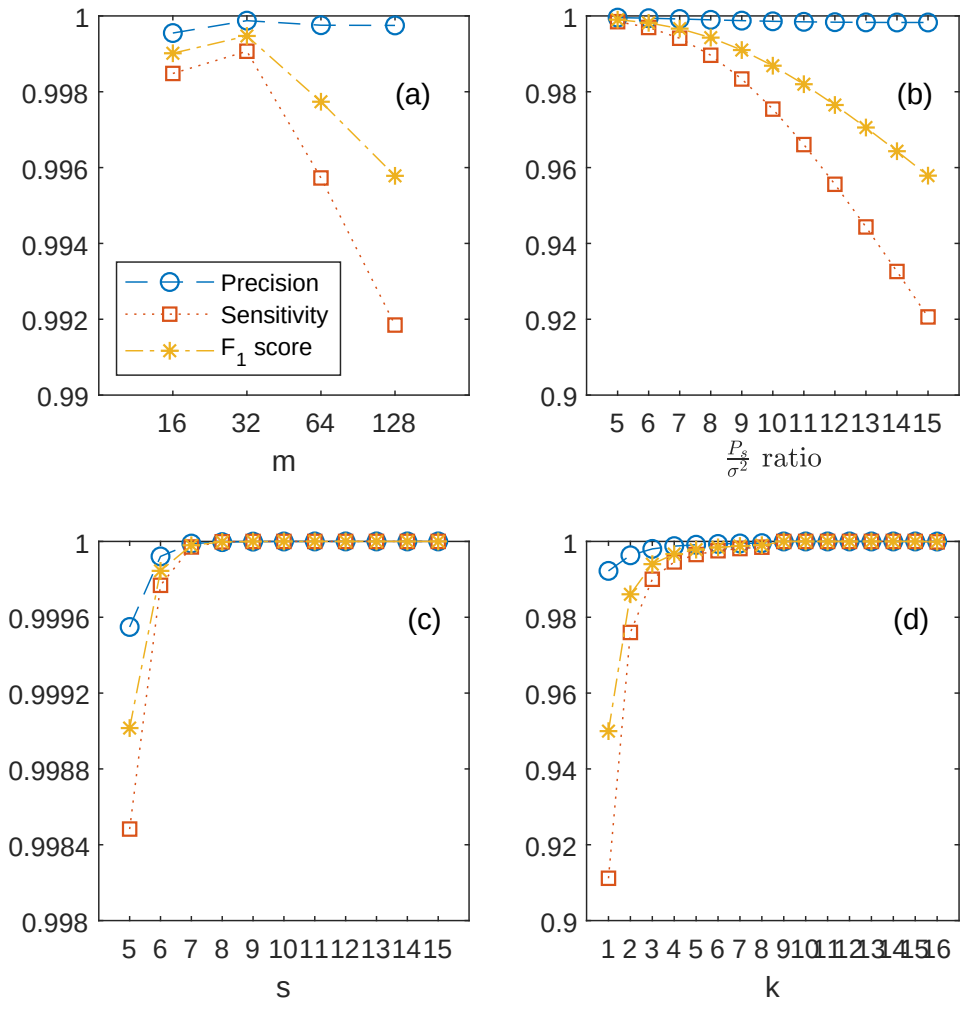

Figure 4.6: Performance evaluation for spoofing detection under varying factors.

increase of m, the average power assigned to each base vectors from spoofing will decrease rapidly, which will make the spoofing signal behaves much more similar with the background noise.

Impact of Spoofing Power

Figure 4.6(b) shows the impact of the spoofing power to noise ratio $\frac{P_s}{\sigma^2}$ on the spoofing detection performance. As for the numerical simulation, we fix the noise power $\sigma^2 = 1$, so the spoofing power P_s changes accordingly with the $\frac{P_s}{\sigma^2}$ ratio. We can see from the figure that with the increase of the $\frac{P_s}{\sigma^2}$ ratio, the overall spoofing detection performance degrades gradually, i.e., the F_1 score decreases gradually. We can also observe that the $Precision$ measurement remains almost unchanged while the $Sensitivity$ measurement decreases rapidly. It might be a little surprising at first sight, but it would be still in line with our intuition if we take a thorough consideration on (18). Although the mean of the detected average spoofing power on spare basis increases with P_s, the variance increases quadratically, so the enlarged variance would eventually induce the decrease of PD, which is represented as $Sensitivity$ measurement in the figure.

Impact of the Number of Time Slots

Figure 4.6(c) shows the impact of the number of time slots s within a given time window on the spoofing detection performance. We can see the increase of the overall spoofing detection performance from F_1 score with the increase of s, but it has a very limited impact which is about 0.1%. In practice, as the power of spoofing signal differs significantly from that of the background noise, we can always expect using a large s would differentiate a spoofing attack from noise with less randomness. It is worth noting that once s exceeds a certain number, e.g., $s \geq 8$ in this case, it won't impact the spoofing detection performance anymore. This could be utilized to explore an minimum s as we always prefer to detect a potential spoofer in an efficient way, given the condition that the received power projection process in VL-Watchdog is performed in each time slot.

Impact of the Number of Random Selections

In order to simplify the calculation, we only simulate the deterministic selection case, in which k is a random number but it's deterministic to be the same for all the s time slots. Figure 4.6(d) shows the impact of the number of orthogonal codes k that the spoofer chooses in fabricating its spoofing signal on the spoofing detection performance. We can see an improvement of the overall spoofing detection performance from F_1 score as the increase of k. It can be also observed that there is a significant improvement of overall performance when k is relative small and then the overall performance saturates once k exceeds the number of transmitters ($k > 8$), which is in line with the intuition that for a fixed m and n, with the increase of k, there could be much more proportions of the average spoofing power projected onto the spare basis to be detected since it's assumed that the spoofing power is equally assigned to k orthogonal basis.

In consideration of the computational complexity and transmission efficiency when introducing VL-Watchdog into existing VL systems, we only consider the major impact of the number of base vectors m and the number of time slots s for calculation simplicity but without loss of generality. The computational complexity increases with the product of these two major factors and can be written as $\mathbf{O}(m*s)$. It would be utilized as a qualitative control for determining the optimal factors, because we would always pursue an add-on spoofing mechanism with minimum computational overhead. As the secrecy is achieved with additional coding from sacrificing a portion of the transmission rate, the transmission efficiency decreases proportionally with the increase of m when the symbol transmission rate is fixed. It also indicates that a small m is always preferred as long as the overall performance is maximized, which is in line with the observation in Figure 4.6(a).

4.6 Improvements by Accounting for the Application Environment

Because indoor VLC and VLS systems typically use intensity modulation, their performance are subject to not only background light noise, but also the random light perturbation from activities happening in the environment. For example, opening a door that connects to a lighted hallway may abruptly increase the background light intensity for a VL system working in a

(relatively) dark room. Similarly, a moving user whose trajectory cuts through the line of sight (LOS) between the LED and the photo-diode may first trigger a sudden bright-to-dark transition when it blocks the LOS, and then a dark-to-bright transition when it leaves the LOS. It is easy to see that such an environment-induced perturbation, when it takes place, will break the orthogonality of the in-transmission VL signal, and hence may trigger VL-Watchdog to issue a (false) spoofing warning, while actually there is no spoofer present. Since in a realistic working environment the above activity-induced perturbation happens frequently, if nothing is done, a high false alarm rate should be expected for the baseline VL-Watchdog spoofing detector presented in the previous sections.

4.6.1 False Warning Filter

To tackle this problem and hence significantly improve the accuracy of VL-Watchdog in a realistic environment, we propose a false-warning filtering mechanism, which attempts to identify and filter out those (false) spoof warnings that are caused by the environment changes from those caused by the real spoofing signals. The key insight in our filtering mechanism is the observation that environment-induced false warnings are typically related to the mechanical movements of some objects in the environment, and therefore they should happen at a lower rate than those caused by the real spoofer, which has to persistently generate spoofing signals for a prolonged period of time in order to make its attack meaningful. The proposed filtering mechanism exploits this key difference in the statistical behavior of the two sources (i.e., the environment changes and the real spoofing signals) to reach its goal.

In particular, our filter maintains a counter that counts the total number of warnings, denoted by K_{obs}, generated by the VL-Watchdog over a predefined number, say n_t, of time windows, where $n_t \gg 1$ in order to make the filtering accurate. The filter considers the filtering as a hypothesis test problem that differentiates between the following two hypothesis,

$\mathcal{I}_0$: no spoofing (i.e., warnings are caused by activities in the environment),

$\mathcal{I}_1$: presence of spoofing.

Accordingly, an optimal threshold κ^o can be decided based on the distribution of the number of warnings associated with $\mathcal{I}_0$ and $\mathcal{I}_1$ according to the MAP criteria (or the ML criteria when the two hypothesis are equally probable), so that a spoofing alarm is announced only if

$$K_{obs} \geq \kappa^o. \tag{4.26}$$

The distribution of the number of warnings in a period of n_t time windows under $\mathcal{I}_0$ and $\mathcal{I}_1$ can be derived as follows.

Spoof Warnings Generated by Change of Environment

The change of environment can be modeled as a Poisson process with rate λ_e, where the value of λ_e could be decided in the system calibration phase by measuring the average number of warnings generated by VL-Watchdog per unit of time when there is no spoofer. Accordingly, the probability that n environment-change-induced warnings will be generated during a given period of n_t i.i.d time windows when there is no spoofer can be calculated as

$$\text{Prob}\{N(n_t) = n|\mathcal{I}_0\} = \frac{(\lambda_e n_t)^n}{n!} e^{-\lambda_e n_t}. \tag{4.27}$$

Spoof Warnings Generated by Spoofing Signals

Given a spoofer presents, in each time window, the VL-Watchdog generates a spoof warning with probability PD (see (4.23)), and does not generate spoof warning with probability $1-PD$. Therefore, over a period of n_t i.i.d. time windows, the number of spoof warnings generated by VL-Watchdog follows Binomial distribution and its probability mass function can be calculated as

$$\text{Prob}\{N(n_t) = n|\mathcal{I}_1\} = C_{n_t}^n PD^n (1 - PD)^{n_t - n}, \tag{4.28}$$

where $C_{n_t}^n = \frac{n_t!}{n!(n_t-n)!}$ is the binomial coefficient.

Given an equally-probable a priori distribution between $\mathcal{I}_0$ and $\mathcal{I}_1$, i.e., Prob$(\mathcal{I}_0) =$ Prob$(\mathcal{I}_1) = 0.5$, the MAP criteria downgrades to the maximum likelihood (ML) criteria. Therefore the optimal detection threshold κ^o can be determined by the following

$$\underset{\kappa^o \in [0,1,\ldots,n_t]}{\arg\min} |\text{Prob}\{N(n_t) = \kappa^o | \mathcal{I}_1\} - \text{Prob}\{N(n_t) = \kappa^o | \mathcal{I}_0\}|. \tag{4.29}$$

4.6.2 Numerical Evaluation for the Filter

Taking the induced spoofing warnings from random changes of environment into consideration by modelling it as Poisson process, we can numerically evaluate the effectiveness of the proposed false-warning filtering mechanism and the performance of it under different settings, respectively. To simplify the calculation, here we only consider those random changes of environment that are significant enough to trigger a false warning by VL-Watchdog, otherwise they will be taken as background noise. As in real-world applications we always expect to determine whether a VL system is under spoofing attack or not in a reasonable amount of time, we define the time period as the number of time windows n_t used to make such a decision. In order to evaluate the performance of the proposed filter, we conduct numerical simulations without and with the false-warning filter by taking two critical factors of the filter into account, including the rate of environment changes λ_e and the number of time windows n_t.

Simulation Settings and Performance Metrics

In each simulation we vary the value of one of the above parameters while keeping the other constant and assume the following default value in our simulation: $\lambda_e = 5$ and $n_t = 10$. The rest of the parameters are set as the same default values as in the previous simulations in Section 4.5.2. We use the F_1 score defined in (25) and false alarm rate FA to characterize the performance of VL-Watchdog with and without the filter. In order to make those two cases (i.e., with and without the filter) fairly comparable with each other, FA will be calculated within n_t time windows for both the without-filter case and the with-filter case. For the without-filter case, FA is calculated as the probability of either the background noise or the change of

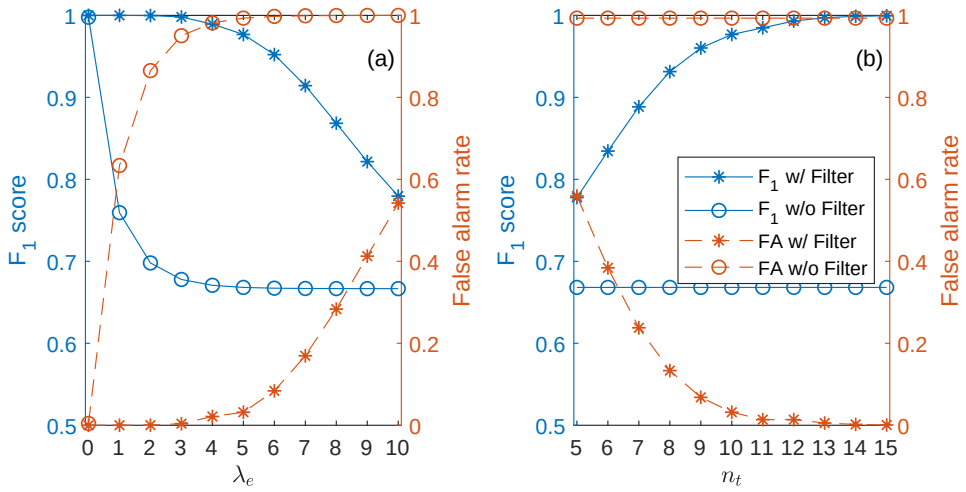

Figure 4.7: Performance evaluation under practical environment perturbation for false-warning filtering.

environment triggers a false warning:

$$FA^{(w/o)} = 1 - (1 - FW)^{n_t} \text{Prob}\{N(n_t) = 0 | \mathcal{I}_0\}, \tag{4.30}$$

For the with-filter case, FA is calculated according to the following equation based on the optimal detection threshold κ^o given in (4.29):

$$FA^{(w/)} = \sum_{n=\kappa^o}^{n_t} \text{Prob}\{N(n_t) = n | \mathcal{I}_0\}. \tag{4.31}$$

Some representative results from our simulation are shown in Figure 4.7.

Performance vs. the Rate of Environment Changes

Figure 4.7(a) shows the performance of the VL-Watchdog under the impact of λ_e with and without false-warning filter, respectively. Our first observation is that VL-Watchdog achieves significantly higher F_1 score and significantly lower false alarm rate under the filter than without the filter in all simulated cases, indicating that the filter does reduce the chances of false alarm and increase the overall accuracy of the watchdog as expected in its design. Furthermore, we can see that the overall performance indicated by F_1 score decreases with the increase of λ_e regardless of using the filter or not. It is not surprising because as the increase of λ_e the number

of spoofing warnings triggered by the changes of environment will approach those caused by the spoofer, making it more and more difficult to distinguish between the two. However, if we take a close look at the small λ_e part, we can see the rapid decrease of F_1 score without filter while the F_1 score with filter maintains at a high level, which demonstrate the effectiveness of the proposed false-warning filter on the overall performance. Moreover, it can be observed that with the increase of λ_e, the FA increases accordingly for both cases, which cause the decrease of the overall performance after we consider practical environment perturbation. In real-world applications, if we use the VL-Watchdog in a crowded indoor environment without the proposed filter, it will lose its functionality by keeping sending false alarms. This observation justifies the necessity of the proposed false-warning filtering mechanism in a realistic application environment.

Performance vs. the Number of Time Windows

Figure 4.7(b) demonstrates the performance of the VL-Watchdog under the impact of n_t with and without filter, respectively. From the figure, we can see that with the increase of n_t, the overall performance represented by F_1 score is improved gradually while the FA decreases correspondingly for the with-filter case. This is in line with our intuition that the increase of n_t would lead to the decrease of the average λ_e within each time window, so the overall performance would be improved as a result. However, as for the without-filter case, we can see that the performance of VL-Watchdog would stay at a very poor level once n_t exceeds a certain number (e.g., 5 in our simulation), as indicated by the low F_1 score and the high false alarm rate. Physically, this means at this point VL-Watchdog will keep giving false alarms when n_t is large, and hence demonstrates the necessity of turning on the proposed false-warning filter.

4.7 Conclusions

In conclusion, to secure the indoor multi-link VL system from spoofing attack, we proposed a signal-level always-on spoofing detection framework VL-Watchdog in this paper, which piggybacks on the redundant orthogonal coding. By exploiting the intrinsic linear superposition properties of VL, the transmission mode consisting of periodically changed orthogonal codes

was used to identify encoded data transmitted by multiple LED transmitters in case of rogue LED transmitters. A proof-of-concept testbed was built to validate the identification feasibility of multi-link VL system under the framework. The proposed VL-Watchdog was numerically evaluated under different factors and it was proved to be effective. In addition, we proposed a false-warning filter to improve VL-Watchdog by accounting for the environment perturbation. Its performance was also numerically evaluated accordingly. In terms of implementation, the proposed VL-Watchdog can be easily integrated into the current VL system with a small hardware add-on of minimum overhead under existing infrastructure.

Chapter 5

Conclusions and future work

5.1 Conclusions

Taking a physical-layer security perspective, the first proposed research of this exploratory dissertation aimed to investigate the intrinsic confidentiality of VLC communication as induced by its special channel characteristics. This work exploited the unique characteristics of VLC channel in calculating its secrecy capacity, and it comprehensively considered the impact of both the specular and the diffusive reflections on secrecy capacity of indoor VLC and also investigated the spatial characteristics/distribution of the secrecy capacity over the indoor communication space. Base on the established indoor VLC system model with three entities, the system security performance was evaluated against a comprehensive set of factors, including the locations of the transmitter, receiver, and eavesdropper, the VLC channel bandwidth, the ratio between the specular and diffusive reflections, and the reflection coefficient, according to the calculated lower and upper secrecy capacity bounds. Due to the addition of LOS and NLOS components, we have found areas with strong reflections, which makes feasible that if an eavesdropper located on those areas, he could sniff data at least partially due to reflection. The possible sniffing attack could also be used as an exploit on insidious attacks such as blocking and spoofing in future complex systems.

By exploiting the intrinsic linear superposition properties of VL, the second proposed research of this exploratory dissertation aimed to design a signal-level always-on spoofing detection framework to secure the VL system from spoofing attack. This work proposed such

a framework named VL-Watchdog, which is applicable to both VLC and VLS systems. VL-Watchdog piggybacks on the redundant orthogonal coding, and it uses orthogonal codes to encode the illumination of each legitimate LED, so that the transmitted light of a legitimate LED is identifiable by detecting the unique signal structure possessed by the received light. A proof-of-concept testbed was built to validate the identification feasibility of multi-link VL system under the framework. The proposed VL-Watchdog was numerically evaluated under different factors and it was proved to be effective. In addition, a false-warning filter was proposed to improve VL-Watchdog by accounting for the environment perturbation. Its performance was also numerically evaluated accordingly. In terms of implementation, the proposed VL-Watchdog can be easily integrated into the current VL system with a small hardware add-on of minimum overhead under existing infrastructure. Once deployed, the watchdog will persistently monitor the light signals in the field to ensure they are sent only from authentic (legitimate) sources.

5.2 Future work

Our work is also subject to some limitations. In particular, while the upper and lower bounds derived in the first proposed research are reasonably tight in the high secrecy capacity regime, they are relatively loose in the low secrecy capacity regime. Further study on how to improve these bounds in the low secrecy capacity regime needs to be done in the future work. Meanwhile, in the second proposed research, a real-world simulation testbed is better to accommodate a more complicated real-world scenario and take more practical factors into consideration. While the refinement on the proposed research is ongoing, we consider this exploratory dissertation as an exploration of physical layer approach to secure both VLC and VLS systems and expect it can inspire more research on the same direction.

References

[1] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[2] X. Liu, X. Wei, and L. Guo, "Dimloc: Enabling high-precision visible light localization under dimmable leds in smart buildings," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3912–3924, 2019.

[3] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5g wireless networks for iot: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[4] S. Ma, Q. Liu, and P. C.-Y. Sheu, "Foglight: Visible light-enabled indoor localization system for low-power iot devices," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 175–185, 2018.

[5] S. Rajagopal, R. D. Roberts, and S. Lim, "IEEE 802.15.7 visible light communication: modulation schemes and dimming support," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 72–82, Mar. 2012.

[6] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications," in *Proceedings of the 2Nd International Workshop on Visible Light Communications Systems*, ser. VLCS '15. New York, NY, USA: ACM, 2015, pp. 9–14. [Online]. Available: http://doi.acm.org/10.1145/2801073.2801075

[7] I. Marin-Garcia, A. M. Ramirez-Aguilera, V. Guerra, J. Rabadan, and R. Perez-Jimenez, "Data sniffing over an open VLC channel," in *2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, Jul. 2016, pp. 1–6.

[8] S. Wu, H. Wang, and C. Youn, "Visible light communications for 5g wireless networking systems: from fixed to mobile communications," *IEEE Network*, vol. 28, no. 6, pp. 41–45, 2014.

[9] G. J. Blinowski, "The Feasibility of Launching Rogue Transmitter Attacks in Indoor Visible Light Communication Networks," *Wireless Personal Communications*, pp. 1–19, Aug. 2017. [Online]. Available: https://link.springer.com/article/10.1007/s11277-017-4781-3

[10] Y. Xu, J.-M. Frahm, and F. Monrose, "Watching the Watchers: Automatically Inferring TV Content From Outdoor Light Effusions," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 418–428. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660358

[11] J. Chen and T. Shu, "Impact of multiple reflections on secrecy capacity of indoor vlc system," in *Proceedings of 21st International Conference on Information and Communications Security (ICICS'19)*, J. Zhou, X. Luo, Q. Shen, and Z. Xu, Eds. Cham: Springer International Publishing, 2019, pp. 105–123.

[12] ——, "Statistical modeling and analysis on the confidentiality of indoor vlc systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 7, pp. 4744–4757, 2020.

[13] ——, "Spoofing detection for indoor visible light systems with redundant orthogonal encoding," in *Proceedings of 2021 IEEE International Conference on Communications (ICC'21)*. IEEE, 2021, pp. 1–6.

[14] ——, "Vl-watchdog: Visible light spoofing detection with redundant orthogonal coding," *IEEE Internet of Things Journal*, pp. 1–1, 2022.

[15] H. Haas, "Wireless data from every light bulb," 2011. [Online]. Available: https://www.ted.com/talks/harald_haas_wireless_data_from_every_light_bulb

[16] D. C. O'Brien, G. Faulkner, Hoa Le Minh, O. Bouchet, M. E. Tabach, M. Wolf, J. W. Walewski, S. Randel, S. Nerreter, M. Franke, K. Langer, J. Grubor, and T. Kamalakis, "Home access networks using optical wireless transmission," in *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep. 2008, pp. 1–5, iSSN: 2166-9589.

[17] S. Arnon, Ed., *Visible Light Communication*. Cambridge: Cambridge University Press, 2015. [Online]. Available: https://www.cambridge.org/core/books/visible-light-communication/34CAFB565027F65A82C6E5E6E7A2989D

[18] Z. Ghassemlooy, L. N. Alves, S. Zvanovec, and M.-A. Khalighi, *Visible Light Communications: Theory and Applications*. CRC Press, Jun. 2017.

[19] L. U. Khan, "Visible light communication: Applications, architecture, standardization and research challenges," *Digital Communications and Networks*, vol. 3, no. 2, pp. 78–88, May 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864816300335

[20] S. Al-Ahmadi, O. Maraqa, M. Uysal, and S. M. Sait, "Multi-User Visible Light Communications: State-of-the-Art and Future Directions," *IEEE Access*, vol. 6, pp. 70 555–70 571, 2018, conference Name: IEEE Access.

[21] H. Chun, A. Gomez, C. Quintana, W. Zhang, G. Faulkner, and D. O'Brien, "A Wide-Area Coverage 35 Gb/s Visible Light Communications Link for Indoor Wireless Applications," *Scientific Reports*, vol. 9, no. 1, p. 4952, Mar. 2019, number: 1 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41598-019-41397-6

[22] S. Hranilovic, L. Lampe, and S. Hosur, "Visible light communications: the road to standardization and commercialization (Part 1) [Guest Editorial]," *IEEE Communications*

Magazine, vol. 51, no. 12, pp. 24–25, Dec. 2013, conference Name: IEEE Communications Magazine.

[23] S. Hranilovic, L. Lampe, S. Hosur, and R. D. Roberts, "Visible light communications: the road to standardization and commercialization (Part 2) [Guest Editorial]," *IEEE Communications Magazine*, vol. 52, no. 7, pp. 62–63, Jul. 2014, conference Name: IEEE Communications Magazine.

[24] A. Cailean and M. Dimian, "Impact of IEEE 802.15.7 Standard on Visible Light Communications Usage in Automotive Applications," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 169–175, Apr. 2017, number: 4 Conference Name: IEEE Communications Magazine.

[25] IEEE, "IEEE Standard for Local and metropolitan area networks–Part 15.7: Short-Range Optical Wireless Communications," *IEEE Std 802.15.7-2018 (Revision of IEEE Std 802.15.7-2011)*, pp. 1–407, Apr. 2019.

[26] ITU, "VLC High Speed Indoor Visible Light Communication Transceiver—System Architecture, Physical Layer and Data Link Layer Specification," *ITU-T G.9991*, pp. 1–88, Mar. 2019.

[27] J. R. Barry, J. M. Kahn, W. J. Krause, E. A. Lee, and D. G. Messerschmitt, "Simulation of multipath impulse response for indoor wireless optical channels," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 3, pp. 367–379, Apr. 1993.

[28] J. B. Carruthers and S. M. Carroll, "Statistical impulse response models for indoor optical wireless channels," *International Journal of Communication Systems*, vol. 18, no. 3, pp. 267–284, Apr. 2005. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/dac.703/abstract

[29] M. I. S. Chowdhury, W. Zhang, and M. Kavehrad, "Combined Deterministic and Modified Monte Carlo Method for Calculating Impulse Responses of Indoor Optical Wireless Channels," *Journal of Lightwave Technology*, vol. 32, no. 18, pp. 3132–3148, Sep. 2014.

[30] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling with MATLAB*. CRC Press, Aug. 2012.

[31] D. Zhang and S. Hranilovic, "Bandlimited Optical Intensity Modulation Under Average and Peak Power Constraints," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3820–3830, Sep. 2016.

[32] X. Chen and M. Jiang, "Adaptive Statistical Bayesian MMSE Channel Estimation for Visible Light Communication," *IEEE Transactions on Signal Processing*, vol. 65, no. 5, pp. 1287–1299, Mar. 2017.

[33] S. Rodríguez Pérez, R. Pérez Jiménez, F. López Hernández, O. González Hernández, and A. Ayala Alfonso, "Reflection model for calculation of the impulse response on IR-wireless indoor channels using ray-tracing algorithm," *Microwave and Optical Technology Letters*, vol. 32, no. 4, pp. 296–300, Feb. 2002. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/mop.10159/abstract

[34] D. Wu, Z. Ghassemlooy, H. Le-Minh, S. Rajbhandari, and L. Chao, "Channel characteristics analysis of diffuse indoor cellular optical wireless communication systems," in *2011 Asia Communications and Photonics Conference and Exhibition (ACP)*, Nov. 2011, pp. 1–6.

[35] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the Capacity of Free-Space Optical Intensity Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4449–4461, Oct. 2009.

[36] J. Wang, Q. Hu, J. Wang, M. Chen, and J. Wang, "Tight Bounds on Channel Capacity for Dimmable Visible Light Communications," *Journal of Lightwave Technology*, vol. 31, no. 23, pp. 3771–3779, Dec. 2013.

[37] L. Yin and H. Haas, "Physical-Layer Security in Multiuser Visible Light Communication Networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 1, pp. 162–174, Jan. 2018.

[38] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Robust Key Generation From Optical OFDM Signal in Indoor VLC Networks," *IEEE Photonics Technology Letters*, vol. 28, no. 22, pp. 2629–2632, Nov. 2016.

[39] ——, "Secret Key Generation Protocol for Optical OFDM Systems in Indoor VLC Networks," *IEEE Photonics Journal*, vol. 9, no. 2, pp. 1–15, Apr. 2017.

[40] A. Mukherjee, "Secret-Key Agreement for Security in Multi-Emitter Visible Light Communication Systems," *IEEE Communications Letters*, vol. 20, no. 7, pp. 1361–1364, Jul. 2016.

[41] X. Liu, X. Wei, L. Guo, Y. Liu, and Y. Zhou, "A New Eavesdropping-Resilient Framework for Indoor Visible Light Communication," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2016, pp. 1–6.

[42] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *2014 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 524–529.

[43] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini, "Improved achievable secrecy rate of visible light communication with cooperative jamming," in *2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Dec. 2015, pp. 1165–1169.

[44] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1975.tb02040.x

[45] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian Wiretap Channel With Amplitude and Variance Constraints," *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5553–5563, Oct. 2015.

[46] J. Wang, S. Lin, C. Liu, J. Wang, B. Zhu, and Y. Jiang, "Secrecy Capacity of Indoor Visible Light Communication Channels," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[47] J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6423–6436, 2018.

[48] J.-Y. Wang, S.-H. Lin, Y. Qiu, N. Huang, and J.-B. Wang, "Tradeoff between secrecy capacity and harvested energy for secure visible light communications with swipt," *IEEE Access*, vol. 7, pp. 29 543–29 552, 2019.

[49] A. Mostafa and L. Lampe, "Physical-Layer Security for MISO Visible Light Communication Channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[50] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "On the achievable secrecy rate of the MIMO VLC Gaussian wiretap channel," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct. 2017, pp. 1–5.

[51] ——, "Secrecy Rate Closed-Form Expressions for the SISO VLC Wiretap Channel With Discrete Input Signaling," *IEEE Communications Letters*, vol. 22, no. 7, pp. 1382–1385, Jul. 2018.

[52] S. Cho, G. Chen, and J. P. Coon, "Secrecy analysis in visible light communication systems with randomly located eavesdroppers," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2017, pp. 475–480.

[53] S. Cho, G. Chen, H. Chun, J. P. Coon, and D. O'Brien, "Impact of multipath reflections on secrecy in VLC systems with randomly located eavesdroppers," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2018, pp. 1–6.

[54] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the Secrecy Capacity of MISO Visible Light Communication Channels," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2016, pp. 1–7.

[55] G. Blinowski, "Security of Visible Light Communication systems—A survey," *Physical Communication*, vol. 34, pp. 246–260, Jun. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874490718304786

[56] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," *12th USENIX Security Symposium Washington, D.C., USA*, pp. 15–27, Aug. 2003.

[57] C. Zhang and X. Zhang, "LiTell: Robust Indoor Localization Using Unmodified Light Fixtures," in *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '16. New York, NY, USA: ACM, 2016, pp. 230–242. [Online]. Available: http://doi.acm.org/10.1145/2973750.2973767

[58] Y. L. Wei, H. I. Wu, H. C. Wang, H. M. Tsai, K. C. J. Lin, R. Boubezari, H. L. Minh, and Z. Ghassemlooy, "LiCompass: Extracting orientation from polarized light," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, May 2017, pp. 1–9.

[59] M. H. Yılmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*. IEEE, 2015, pp. 812–817.

[60] A. RazaCheema, M. Alsmadi, and S. Ikki, "Survey of identity-based attacks detection techniques in wireless networks using received signal strength," in *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*. IEEE, 2018, pp. 1–6.

[61] A. Bittau, M. Handley, and J. Lackey, "The final nail in WEP's coffin," in *2006 IEEE Symposium on Security and Privacy (S P'06)*, May 2006, pp. 15 pp.–400.

[62] F. I. K. Mousa, N. A. Maadeed, K. Busawon, A. Bouridane, and R. Binns, "Secure MIMO Visible Light Communication System Based on User's Location and Encryption," *Journal of Lightwave Technology*, vol. 35, no. 24, pp. 5324–5334, Dec. 2017.

[63] F. Guo and T.-c. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," in *Recent Advances in Intrusion Detection*, ser. Lecture Notes in Computer Science, A. Valdes and D. Zamboni, Eds. Springer Berlin Heidelberg, 2006, pp. 309–329.

[64] Q. Li and W. Trappe, "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 793–808, Dec. 2007.

[65] D. B. Faria and D. R. Cheriton, "Detecting Identity-based Attacks in Wireless Networks Using Signalprints," in *Proceedings of the 5th ACM Workshop on Wireless Security*, ser. WiSe '06. New York, NY, USA: ACM, 2006, pp. 43–52. [Online]. Available: http://doi.acm.org/10.1145/1161289.1161298

[66] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Jun. 2007, pp. 193–202.

[67] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, Apr. 2008, pp. 1768–1776.

[68] J. Classen, D. Steinmetzer, and M. Hollick, "Opportunities and Pitfalls in Securing Visible Light Communication on the Physical Layer," in *Proceedings of the 3rd Workshop on Visible Light Communication Systems*, ser. VLCS '16. New York, NY, USA: ACM, 2016, pp. 19–24. [Online]. Available: http://doi.acm.org/10.1145/2981548.2981551

[69] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Physical-layer security against known/chosen plaintext attacks for ofdm-based vlc system," *IEEE Communications Letters*, vol. 21, no. 12, pp. 2606–2609, 2017.

[70] Y. Al-Moliki, M. Alresheedi, and Y. Al-Harthi, "Randomness evaluation of key generation based on optical ofdm system in visible light communication networks," *Electronics Letters*, vol. 53, no. 24, pp. 1594–1596, 2017.

[71] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Chaos-based physical-layer encryption for ofdm-based vlc schemes with robustness against known/chosen plaintext attacks," *IET Optoelectronics*, vol. 13, no. 3, pp. 124–133, 2018.

[72] R. Melki, H. N. Noura, and A. Chehab, "Efficient & secure physical layer cipher scheme for vlc systems," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–6.

[73] K. Lee, H. Park, and J. R. Barry, "Indoor Channel Characteristics for Visible Light Communications," *IEEE Communications Letters*, vol. 15, no. 2, pp. 217–219, Feb. 2011.

[74] R. Perez-Jimenez, J. Berges, and M. J. Betancor, "Statistical model for the impulse response on infrared indoor diffuse channels," *Electronics Letters*, vol. 33, no. 15, pp. 1298–1300, Jul. 1997.

[75] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 100–107, Feb. 2004.

[76] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[77] F. Lopez-Hernandez, R. Perez-Jimenez, and A. Santamaria, "Ray-tracing algorithms for fast calculation of the channel impulse response on diffuse IR wireless indoor channels," *Optical Engineering*, vol. 39, no. 10, pp. 2775–2780, 2000.

[78] F. Chollet *et al.*, "Keras," https://keras.io, 2015.

[79] M. Haus, A. Y. Ding, Q. Wang, J. Toivonen, L. Tonetto, S. Tarkoma, and J. Ott, "Enhancing indoor iot communication with visible light and ultrasound," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.

[80] A. T. L. Lee, H. Chen, S.-C. Tan, and S. Y. Hui, "Precise dimming and color control of LED systems based on color mixing," *IEEE Transactions on Power Electronics*, vol. 31, no. 1, pp. 65–80, Jan. 2016.

[81] Y. Wang, C. Yang, Y. Wang, and N. Chi, "Gigabit polarization division multiplexing in visible light communication," *Optics Letters*, vol. 39, no. 7, p. 1823, 2014.

[82] K. Bhargavan, A. D. Lavaud, C. Fournet, A. Pironti, and P. Y. Strub, "Triple handshakes and cookie cutters: Breaking and fixing authentication over tls," in *2014 IEEE Symposium on Security and Privacy*. IEEE, 2014, pp. 98–113.

[83] C. Meyer, J. Somorovsky, E. Weiss, J. Schwenk, S. Schinzel, and E. Tews, "Revisiting ssl/tls implementations: New bleichenbacher side channels and attacks," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 733–748.

[84] D. Xu, P. Ren, J. A. Ritcey, and Y. Wang, "Code-frequency block group coding for anti-spoofing pilot authentication in multi-antenna ofdm systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1778–1793, 2018.

[85] Q. Zeng, H. Li, and L. Qian, "Gps spoofing attack on time synchronization in wireless networks and detection scheme design," in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, 2012, pp. 1–5.

[86] J. M. Kahn, W. J. Krause, and J. B. Carruthers, "Experimental characterization of non-directed indoor infrared channels," *IEEE Transactions on Communications*, vol. 43, no. 2/3/4, pp. 1613–1623, Feb. 1995.

[87] L. Li, P. Hu, C. Peng, G. Shen, and F. Zhao, "Epsilon: A visible light based positioning system," in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*. Seattle, WA: USENIX Association, Apr. 2014, pp. 331–343. [Online]. Available: https://www.usenix.org/conference/nsdi14/technical-sessions/presentation/li

[88] T. Li, C. An, Z. Tian, A. T. Campbell, and X. Zhou, "Human sensing using visible light communication," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 331–344. [Online]. Available: https://doi.org/10.1145/2789168.2790110

[89] M. Noshad and M. Brandt-Pearce, "Hadamard-Coded Modulation for Visible Light Communications," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1167–1175, Mar. 2016.

[90] DigiKey, Visible Red Emitter, https://www.digikey.com/product-detail/ en/marktech-optoelectronics/MTE6066N3-UR/1125-1242-ND/4746370. Accessed: 2020-07-21.

[91] ——, Arduino UNO R3, https://www.digikey.com/product-detail/en/arduino/A000066/1050-1024-ND/2784006, Accessed: 2020-07-21.

[92] S. Hranilovic and F. R. Kschischang, "Optical intensity-modulated direct detection channels: signal space and lattice codes," *IEEE Transactions on Information Theory*, vol. 49, no. 6, pp. 1385–1399, Jun. 2003.

[93] DigiKey, DC2197A, https://www.digikey.com/products/en/development-boards-kits-programmers/evaluation-boards-digital-to-analog-converters-dacs/793?k=LTC2645. Accessed: 2020-07-21.

[94] D. M. Powers, "Evaluation: from precision, recall and f-measure to roc, informedness, markedness and correlation," *arXiv preprint arXiv:2010.16061*, 2020.