January 2021

Visible Light Communication Cyber Security Vulnerabilities For Indoor And Outdoor Vehicle-To-Vehicle Communication

Rana Shaaban

VISIBLE LIGHT COMMUNICATION CYBER SECURITY VULNERABILITIES FOR INDOOR AND OUTDOOR VEHICLE-TO-VEHICLE COMMUNICATION

by

Rana Rageh Shaaban

Master of Science, University of North Dakota, 2017

A dissertation

Submitted to the Graduate Faculty

of the

University of North Dakota

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Grand Forks, North Dakota

August

2021

This dissertation, submitted by Rana Shaaban in partial fulfillment of the requirements for the Degree of Doctor of Philosophy from the University of North Dakota, has been read by the Faculty Advisory Committee under whom the work has been done and is hereby approved.

_____

Saleh Faruque

_____

Ryan Adams

_____

Naima Kaabouch

_____

William Semke

_____

Wen-Chen Hu

This dissertation is being submitted by the appointed advisory committee as having met all of the requirements of the School of Graduate Studies at the University of North Dakota and is hereby approved.

_____

Dean of the Graduate School

_____

Date

PERMISSION

Title Visible Light Communication Cyber Security Vulnerabilities for Indoor and Outdoor Vehicle-To-Vehicle Communication

Department Electrical Engineering

Degree Doctor of Philosophy

In presenting this dissertation in partial fulfillment of the requirements for a graduate degree from the University of North Dakota, I agree that the library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my dissertation work or, in his absence, by the chairperson of the department or the dean of the Graduate School. It is understood that any copying or publication or other use of this thesis or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of North Dakota in any scholarly use which may be made of any material in my dissertation.

Signature _____

Date _____

TABLE OF CONTENTS

TABLE OF CONTENTS ..... **v**

LIST OF FIGURE ..... **viii**

LIST OF TABLE ..... **xii**

ABSTRACT ..... **xv**

CHAPTER 1 ..... **1**

OVERVIEW **1**

1.1 Overview of the Thesis 1

1.2 Research Objectives and Goals 7

1.3 Publications and Contributions 8

1.4 Dissertation Organization 9

CHAPTER 2 ..... **11**

INTRODUCTION **11**

2.1 Challenges and Motivation 11

CHAPTER 3 ..... **19**

IEEE 802.15.7: VISIBLE LIGHT COMMUNICATION STANDARD **19**

3.1 Introduction 19

3.2 Overview of IEEE standard 802.15.7 20

3.3 MAC Layer 21

3.4 PHY Layer 23

3.5 Recent Activities in IEEE standardization 24

CHAPTER 4 ..... **29**

INDOOR VISIBLE LIGHT COMMUNICATION SECURITY **29**

4.1 Introduction 29

4.2 Indoor VLC System Model 31

A. Transmitter 32

B. Receiver 32

4.3 Simulation Results Discussion and Summary 34

A. Optical Power Distribution 34

B. Signal to Noise Ratio Analysis 35

4.4 Previous Work 37

CHAPTER 5 ..... **40**

INDOOR VLC PHYSICAL LAYER SECURITY **40**

5.1 Physical Layer Security Solutions 40

A. VLC beamforming: 40

B. VLC secure communication zones: 42

C. VLC friendly jamming: 43

5.2 VLC PLS Proposed System Model 43

A. Mathematical model 44

B. Differential Optical Receiver 44

5.3 Simulation Results Discussion and Summary 45

5.4 Previous Work 49

CHAPTER 6 ..... **54**

INTRAVEHICLE VISIBLE LIGHT COMMUNICATION **54**

6.1 Introduction 54

6.2 Vehicular System Model 55

6.3 Intra-Vehicle LEDs Locations Analysis 58

A. Two Sources of Power 58

B. Three Sources of Power 60

6.4 Simulation Results Discussion and Summary 60

CHAPTER 7 ..... **63**

OUTDOOR VEHICULAR VISIBLE LIGHT COMMUNICATION SECURITY **63**

7.1 Introduction 63

7.2 V2V VLC System Model 66

A. LOS Channel Analysis 66

B. Diffuse Channel Analysis 68

7.3 V2V Model Simulation Results 68

7.4 Vehicular VLC Security 71

7.5 Simulation Results Discussion and Summary 72

CHAPTER 8 ..... **76**

CONCLUSION **76**

REFERENCES **79**

LIST OF FIGURE

Figure 1. 5G Modern Applications.....2

Figure 2. Radio frequency (RF) spectrum, visible light spectrum, and infrared (IR) spectrum [18]. 4

Figure 3. Autonomous VANET communication Architecture [24].....7

Figure 4. Autonomous VANET communication Architecture [24].....11

Figure 5. Communication system block diagram. 12

Figure 6. Operation of a LiFi link under strict non-line-of-sight (LOS) conditions [50]....14

Figure 7. Communication Functional Block Diagram. 17

Figure 8. Representation of a room with four LEDs and their footprint.....31

Figure 9. Optical power distribution in received optical plane for a FWHM of (a) 35° with four APs, (b) 15°with six APs and (c) , (d) are top view for room 1 and room 2 respectively. 36

Figure 10. SNR or receiver for a FWHM of (a) 35° with four APs , (b) 15°with six APs .36

Figure 11. Spatial distribution of the SNR without beamforming (a), Secrecy rate achievable via zero-forcing beamforming (b). 37

Figure 12. Secrecy outage probability versus VLC AP density. 38

Figure 13. Footprint of a room with five LEDs. 43

Figure 14. Differential optical receiver, illustrating sunlight cancellation; Ip1 and Ip2 are photocurrents due to ambient light and optical signal, respectively [105]. 44

Figure 15. Received optical power distribution plane for a FWHM of (a) 35º with four APs (room 1) (b) 15º for 5th AP (user's AP in room 2), and (c) 15º for the four jamming APs in room 2. 46

Figure 16. SNR of receiver for a FWHM of (a) 35º with four APs (room 1) (b) 15º for 5th AP (user's AP in room 2), and (c) 15º for the four jamming APs in room 2. 48

Figure 17. Eve's SNR as function of Eve's location for the SISO case (a). Bob's SNR as a function of Eve's location for the MISO case with null-steering. (Bob is located at the room center) (b). 49

Figure 18. The distribution of (a) SNR and (b) secrecy capacity. 50

Figure 19. (a) the average SNR of EDs with beamforming and LED selection, (b) the average SNR of EDs with beamforming and repetition coding, (c) the ratio of the average SNRs of EDs generalized by beamforming. .....**Error! Bookmark not defined.**

Figure 20. Received signal power distributions. (a) 3D power distributions obtained by uniform beamformers. (b) 3D power distributions obtained by CSASPM. (c) 2D power distributions obtained by uniform beamformers. (d) 2D power distributions obtained by CSASPM. 52

Figure 21. Front-facing view of the deployment structure [110]. 56

Figure 22. Received power in μW for the rear passenger seats [110]. 56

Figure 23. Received power in μW for the front passenger seats [110]. 57

Figure 24. Optimized received power in mW for the rear and front passenger seats [106]. 58

Figure 25. Two LED received power in mW for the rear and front passenger seats. 58

Figure 26. SNR of the receiver. 60

Figure 27. Three LEDs received power in mW for the rear and front passenger seats. 61

Figure 28. The SNR of receiver for the rear and front passenger seats. 62

Figure 29. Demonstration of Intelligent transportation system. 63

Figure 30. V2V communication Architecture using two vehicles. 66

Figure 31. Received Optical power distribution of the headlights (projected on a vertical plane) for a FWHM of 20 º (a) traffic mode and (b) stop mode. 69

Figure 32. Received Optical power distribution of the headlights (projected on a vertical plane) for a FWHM of 10 º (a) traffic mode and (b) stop mode. 70

Figure 33. Hybrid Received Optical power distribution of the headlights (projected on a vertical plane) for a FWHM of 10 º (a) traffic mode and (b) stop mode.....71

Figure 34. Received Optical power distribution of the headlights in traffic mode when projected on a vertical plane for a FWHM of 7 º. 72

Figure 35. SNR and BER of the receiver (projected on a vertical plane) for a traffic mode with (a, d) a FWHM of 20 º, (b, e) a FWHM of 7 º and (c, f) for stop mode with a FWHM of 7 º.....74

LIST OF TABLE

Table 1. VLC Device Classification.....21

Table 2. VLC Device Classification.....25

Table 3. VLC Secrecy Enhancement Techniques.....30

Table 4. Indoor Simulation Parameters.....33

Table 5. VLC Physical Layer Security Techniques.....41

Table 6. PLS Indoor Simulation Parameters.....45

Table 7. Intra-Vehicle Simulation Parameters.....59

Table 8. V2V VLC Secrecy Enhancement Techniques.....64

Table 9. V2V VLV Simulation Parameters.....67

ACKNOWLEDGEMENTS

I would first like to thank my dissertation advisor Prof. Saleh Faruque at the University of North Dakota. The door to Prof. Faruque office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right the direction whenever he thought I needed it.

I would also like to acknowledge Prof. William Semke, Prof. Naima Kaabouch, Prof. Ryan Adams, and Dr. Wen-Chen Hu at the University of North Dakota as the second readers of this dissertation, and I am gratefully indebted to them for their very valuable comments on this dissertation.

I would also like to thank the Electrical Engineering Department at the University of North Dakota for giving me this opportunity and financial support to finish my dissertation.

Finally, I must express my very profound gratitude to my family for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this dissertation. This accomplishment would not have been possible without them. Thank you.

To my Kids,
The world’s greatest Kids!

ABSTRACT

Light fidelity (Li-Fi), developed from the approach of Visible Light Communication (VLC), is a great replacement or complement to existing radio frequency-based (RF) networks. Li-Fi is expected to be deployed in various environments were, due to Wi-Fi congestion and health limitations, RF should not be used. Moreover, VLC can provide the future fifth generation (5G) wireless technology with higher data rates for device connectivity which will alleviate the traffic demand.

5G is playing a vital role in encouraging the modern applications. In 2023, the deployment of all the cellular networks will reach more than 5 billion users globally. As a result, the security and privacy of 5G wireless networks is an essential problem as those modern applications are in people's life everywhere. VLC security is as one of the core physical-layer security (PLS) solutions for 5G networks. Due to the fact that light does not penetrate through solid objects or walls, VLC naturally has higher security and privacy for indoor wireless networks compared to RF networks. However, the broadcasting nature of VLC caused concerns, e.g., eavesdropping, have created serious attention as it is a crucial step to validate the success of VLC in wild.

The aim of this thesis is to properly address the security issues of VLC and further enhance the VLC nature security. We analyzed the secrecy performance of a VLC model by studying the characteristics of the transmitter, receiver and the visible light channel. Moreover, we mitigated the security threats in the VLC model for the legitimate user, by 1) implementing more

access points (APs) in a multiuser VLC network that are cooperated, 2) reducing the semi-angle of LED to help improve the directivity and secrecy and, 3) using the protected zone strategy around the AP where eavesdroppers are restricted. According to the model's parameters, the results showed that the secrecy performance in the proposed indoor VLC model and the vehicle-to-vehicle (V2V) VLC outdoor model using a combination of multiple PLS techniques as beamforming, secure communication zones, and friendly jamming is enhanced. The proposed model security performance was measured with respect to the signal to noise ratio (SNR), received optical power, and bit error rate (BER) Matlab simulation results.

CHAPTER 1

OVERVIEW

1.1 Overview of the Thesis

Visible light communication (VLC) is a promising candidate for future high speed broadband communications[1-3]. The VLC technology deploys the intensity modulation of white light emitting diodes (LEDs), which can be switched on and off at a very high rate, thus offering data communications, and illuminations[4]. VLC provides 10,000 times more bandwidth capacity than the radio frequency (RF) technology [5]. LEDs are already utilized widely in everyday infrastructures including schools, offices, homes, smartphones, streets and traffic lights. By occupying the current lighting infrastructure and changing the wireless communication frequency to the visible spectrum, VLC could mitigate the spectrum crunch in the present wireless systems using RF. In order to commercialize VLC in the near future, recent approaches have conducted the standardization of short-range wireless optical communication using VLC for local and urban area networks[6]. Moreover VLC is an interesting technique as it utilize the existing lighting systems and work on license free spectrum as a result lower implementation cost. Also it is considered safe for the electromagnetic sensitive areas, where RF is not allowed for safety issues. Additionally VLC can be applied along with current wireless networks since it receives zero interference.

The next-generation wireless communication is expected to acquire a vast amount of data, including full-motion video (FMV) and high-definition (HD) images. This mission-critical information will require a large transmission bandwidth as well as radiation safety, driving the need for efficient data transmission techniques, such as VLC. VLC is a branch of optical wireless (OW) communication technique that not only provides high bandwidth but also provides radiation

safety [7]. Typically, VLC system has been realized as a point-to-point wireless communication link between a data source (LED) to modulate and transmit the data to the receiver which can be any device that is sensitive to light (photodiode, image sensor, etc.), to demodulate the data for the end user.

Figure 1. 5G Modern Applications.

The new mobile-telecommunication system, fifth-generation 5G is playing a vital role in encouraging modern applications, such as internet-of-things (IoT), smart home, smart city, smart health care, internet-of-vehicles (IoVs), and industry 4.0 Fig. 1, where a massive number of smart devices are connected. Also, 5G will be used for communication in the new power grid system, smart grid (SG) as the advanced sensors and measurement systems will have a communication network backbone [8]. In 2024, the deployment of all the cellular networks will reach more than 7 billion users. Current cellular networks will not be sufficient to handle the enormous amount of increase in data traffic required [9]. 5G is characterized by 100% availability, up to 10 years increase in devices battery life, 90% reduction in network power consumption, and connectivity throughput up to 10 giga bit per second (Gbps) [10]. Moreover in [11], they explored the possibility of full-duplex 5G communications for monitoring systems in the sphere of ambient assisted living

(AAL) which simplifies and automates processes that do not require human interventions. As a result, the security and privacy of 5G wireless networks is an essential concern as those modern applications are in people's lives everywhere. To mitigate the aforementioned issues, an in-depth survey was presented in [12] of the proposals having 5G-enabled IoT as a backbone for blockchain-based industrial automation for those applications. Additionally, in another study they surveyed the state-of-the-art proposals having tactile internet as a backbone for delay mitigation by using 5G networks for future ultra-reliable low-latency applications [13].

For the last decade VLC has been applied in several scenarios, where it is difficult to utilize RF communication, and it was highlighted that OW may offer a consistent solution to the idea of intra-vehicle communications, which illuminate the interior of the vehicle with a light source to act as a communication link between anything from simple user-vehicular interface devices such as window or air conditioning controllers, to more advanced vehicular technologies such as audio-visual (AV) entertainment units or computer consoles [14].

Applying a VLC system within a vehicle or Vehicle Adhoc Network (VANET) combines multiple advantages like diminishing the highly common RF interference, decreasing the cost due to using an unregulated spectrum and not obligatory to design a system around other competing RF systems [15,16]. Moreover, energy efficient in terms of reduction in wired devices that are mostly copper cabled, and finally a possible improvement to manufacturing efficiency such cabling should be removed [17].

Light fidelity (Li-Fi) is developed from the approach of VLC. The Li-Fi protocol mainly depends on the intensity modulation of white LEDs, which at a very high rate switches on and off, thus providing illuminations and data communications [4]. It is important to note that the total capacity of the visible light and infrared (IR) spectrum is approximately 2600 times that of the full

RF spectrum of 300 GHz and is license-free (see Fig. 2). Due to the rise of machine type communication (MTC) and Internet-of-Things (IoT), the demand for the next 20 years will be 12,000 times the existing bandwidth with the exact similar spectrum efficiency. That will result in a 6 THz of bandwidth, which means a 20 times shortage bandwidth. In the RF spectrum as it is only 0.3 THz. On the other hand, just 0.8% of the total visible light and IR spectrum is the 6 THz of bandwidth.

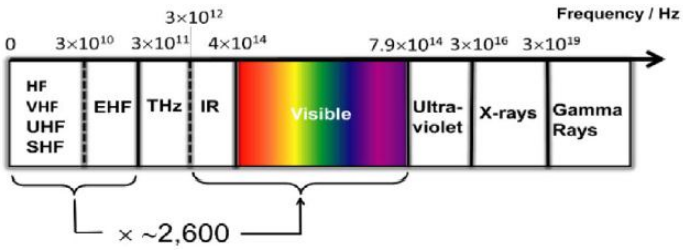


Figure 2. Radio frequency (RF) spectrum, visible light spectrum, and infrared (IR) spectrum [18].

The key advantage of VLC wireless networking is human safety. Since wireless routers, bluetooth and similar wireless systems radiate electromagnetic energy 24/7 and people absorb them continuously. The level of absorption is considered potentially dangerous to humans, especially children. The US and Int.cancer registries have proofs that link the increase of the number of people diagnosed with the type of brain tumor, glioblastoma multiforme (GBM), to cell phone use [19]. Furthermore, the author in [20] mentioned that the brain, renal, liver and thyroid cancers are spreading out among US children, and GBM (the brain cancer linked to radiation of cell phones) and central nervous system tumors are rising in Americans teenagers, in specifically the parts of the brain that absorb most of the microwave radiation emitted by phones. Also, a 2017 meta-analysis [21] of researches on parotid gland tumors discovered a relation between the risk of parotid gland tumors and mobile phone use. Although more evidence is required, the present

research result is showing that the use of mobile phones can modify salivary function, cause oxidative stress which could affect salivary gland tumor progress. However current evidence does not illustrate a relation between mobile phone use and tumor development. As to address such small risks, high-quality research with careful exposure assessment is essential [22]. In comparison to RF wireless communication, VLC is a safe wireless communication technology because it is harmless to the human body, and it avoids electromagnetic interference [16]. Thus it can be used in schools, offices, hospitals and in intrinsically safe environments such as oil platforms and petrochemical plants where RF is often restricted.

The lighting and digital modulation technology determine the achievable data rate that can reach up to 100 Gbps. The white light is either created by the most commercial phosphor-coated blue LED or by mixing the base colors in the red, green, blue (RGB) LEDs. The former LEDs consist of a high brightness blue LED with a phosphorous coating that changes blue light into yellow and the bandwidth is hardly 2 MHz. However the converting of the phosphor color slows down the frequency response, it is still possible to reach the region of 1 Gbps data rates by removing the slow yellow components using a blue filter. The later advanced RGB LEDs can achieve up to 5 Gbps since they do not use color converting chemical to produce white light. Also, [23] has recorded transmission speed with a single micro Gallium Nitride (GaN) LED of 8 Gbps, and [24] proved that 100 Gbps are attainable by laser-based lighting.

Though the worries about cyber security and privacy in the VLC wireless network because of the spreading behavior of VLC, VLC access points (APs) form a tiny cell, an optical attocell. In contrast to RF antennas with the omnidirectional signal transmission in all directions, a LED light source is normally designed to send optical power directionally. Therefore, the transmission of the visible light signals is typically concentrated within a limited zone, which normally provides

security and privacy. On the other hand, to achieve the same desire the RF mm-wave schemes need complicated and expensive antenna beamforming methods. Therefore VLC attocell networks qualify to enhance 5G cellular systems cost-effectively [25]. Nevertheless, VLC technology is vulnerable to multiple attacks including eavesdropping, hijacking, packet falsification, message manipulation, replay attack, and membership falsification, which have endorsed serious attention as it is an essential step to prove the success of VLC application in the wild [26]. In addition, VLC is considered to be an emerging technology for 5G, and security is an essential requirement for 5G. In [27] they covered VLC physical layer security (PLS) techniques that can improve the security to bring the deployment of the VLC system. In the VLC security research area, PLS is the most advanced approach and involves multiple techniques such as VLC beamforming, VLC secure communication zones, and VLC friendly jamming [21][22][22][23][24][24][25].

Although the light is blocked by the wall to sustain particular percentage of privacy, there are possible worries to network administrators and legitimate users concerning the privacy of information and confidentiality, especially in public, such as schools, airports, train stations, libraries, and offices, etc.[24]. The interferences in the VLC system is less than the case of the RF system due to line of sight (LOS) and directional communications. While interference from far-away concurrent transmissions affects RF, VLC suffers from other sources of interference, weather, sunlight, and artificial light. A camera-based VLC system can still avoid interferences [26] by spatially fliting out unwanted areas without transmitting light. The optical channel interference is reduced to LOS transmission only because it is completely blocked by opaque objects.

Moreover, VLC can play an important role in Intelligent Transportation Systems (ITS) and Vehicular Ad Hoc Networks (VANETs) as it can support car communication, Vehicle-to-

vehicle (V2V), to mitigate traffic fatalities as proposed in [27]. ITS are concerned about traffic safety because it is susceptible to all adversaries, as shown in Fig. 3. They work on scaling down traffic accidents by sustaining timely and accurate information about traffic jams, road conditions, and accidents. In [28] VANETs used dedicated short-range communications (DSRC) for V2V and vehicleto-infrastructure (V2I). Also soon, cars will drive through intersections without waiting for traffic signals to give them the green light to go. This free-for-all will take place at the union of three technologies: V2V technology; self-driving cars; and the IoT, which guarantees to connect 30 billion sensors and gadgets worldwide [29]. That will result in traffic flowing smoothly and safely without the use of any traffic lights. Also, a group of researchers has already implemented an algorithm that operates as a conductor to keep traffic humming along like a well-rehearsed orchestra [30].

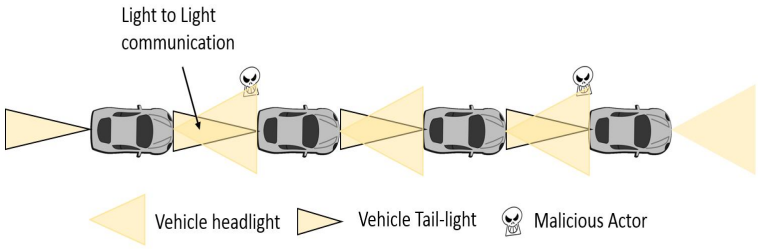


Figure 3. Autonomous VANET communication Architecture [24].

1.2 Research Objectives and Goals

In this dissertation, the aim is to analyze the secrecy performance of a VLC system model and further enhance its nature security by using additional security techniques. We studied the characteristics of the transmitter, receiver and the visible light channel properties using the light emitting diode (LED) Lambertian radiant intensity model. The proposed indoor VLC and outdoor V2V VLC model improved the system secrecy performance with higher levels for SNR and BER.

We applied combination of multiple PLS techniques as beamforming, secure communication zones, and friendly jamming. To mitigate the security threats in the VLC model for the legitimate user, we 1) implemented more access points (APs) in a multiuser VLC network that are cooperated, 2) reduced the semi-angle of LED to help improve the directivity and secrecy and, 3) used the protected zone strategy around the AP where eavesdroppers are restricted.

1.3 Publications and Contributions

Peer Reviewed Journal Papers

1. Shaaban R, Faruque S. An enhanced indoor visible light communication physical-layer security scheme for 5G networks: Survey, security challenges, and channel analysis secrecy performance. International Journal of Communication Systems. 2021 Jan: e4726.
2. Shaaban R, Faruque S. Cyber security vulnerabilities for outdoor vehicular visible light communication in secure platoon network: Review, power distribution, and signal to noise ratio analysis. Physical Communication. 2020 Apr 6:101094.

Peer Reviewed Conference Papers

1. Shaaban R, Faruque S. Optimized LEDs Positions for Channel Analysis Performance of an Intra-Vehicle Visible Light Communication System. In2020 IEEE Radio and Wireless Symposium (RWS) 2020 Jan 26 (pp. 302-305). IEEE.
2. Shaaban, R., Ranganathan, P., and Faruque, S., “Visible Light Communication Security Vulnerabilities in Multiuser Network: Power Distribution and Signal to Noise Ratio Analysis,” Springer FICC 2019, San Francisco, California, USA, 2019. (Published as a book chapter)
3. Shaaban, R. and Faruque, S., “Optimized optical wireless channel for indoor and intra-vehicle communications: power distribution and SNR analysis,” 2018 International Society for Optics and Photonics (SPIE OPTO 2018), San Francisco, California, USA, 2018.

4. Shaaban, R. and Faruque, S., “A survey of indoor visible light communication power distribution and color shift keying transmission,” 2017 IEEE International Conference on Electro/Information Technology (EIT 2017), Lincoln, Nebraska USA, 2017.

Contributions

1. Further enhanced the indoor VLC privacy and secrecy performance for the users by 1) implementing more access points (APs) in a multiuser VLC network that are cooperated, 2) reducing the semi-angle of LED to help improve the directivity and secrecy and, 3) using the protected zone strategy around the AP where eavesdroppers are restricted.
2. Applied a combination of multiple physical-layer security (PLS) techniques as beamforming, secure communication zones, and friendly jamming in the proposed indoor VLC model which enhanced the secrecy performance and mitigated the security threats in the VLC network.
3. Proved the effect of different number of LED's position on the received power within the designated area, which directly affects the system performance, the SNR, and probability of error.
4. Focused on vehicular VLC security; however, there are only a few security-related studies on vehicular VLC physical layer security. Improved the secrecy performance in an outdoor V2V VLC network using PLS techniques to achieve better SNR for the legitimate platoon member than the adversary, therefor ensure platoon stability and limit the detection of any adversary.

1.4 Dissertation Organization

This dissertation is organized as follows, chapter 3 shows the IEEE 802.15.7: visible light communication standard, and chapter 4 addresses the security issues of the indoor VLC model and proposes the secured indoor VLC model, channel transfer characteristics, transmitter, and receiver. Also the simulation results for the secured indoor VLC model are shown in chapter 4.

Several methods are studied and used to mitigate and improve the VLC physical-layer threats and solutions for the new 5G network in chapter 5. In addition, the proposed VLC PLS

system model and the simulation results are presented. Then, in chapter 6 the intravehicle VLC model is investigated with simulation results and discussion shown in the same chapter. Moreover, the secured model for the outdoor vehicular VLC system is proposed in chapter 7 for the vehicular communication in VANETs system. Finally, a suggestion of future work areas of research and conclusion are presented in chapter 8.

CHAPTER 2

INTRODUCTION

2.1 Challenges and Motivation

Due to the fact that visible light cannot penetrate through walls, it has high frequency reuse factor hence a high area spectral efficiency and naturally secured. However the broadcasting nature of VLC causes concerns in security and privacy in VLC, e.g., eavesdropping [19].As shown in Fig. 4, a VLC network includes one sender (Alice), one legitimate receiver (Bob), and one eavesdropper (Eve)[31].Communication protocol is susceptible to several attacks as shown in Fig. 5. The wall can block the light to provide certain degree of privacy but still there are potential concerns to legitimate users, particularly in public areas.

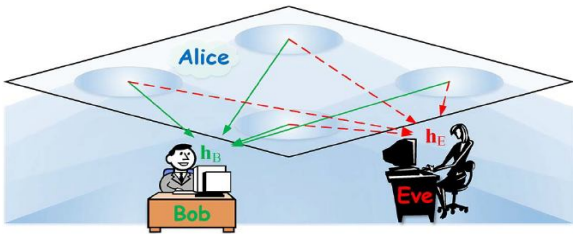


Figure 4. Autonomous VANET communication Architecture [24].

Also, Traffic safety is the major concern of Intelligent Transportation Systems (ITS) as it is highly vulnerable to all attackers, as shown in Fig. 3.The fundamental objective of ITS is to scale down traffic accidents by maintain timely and adequate data collection about events like road status ,traffic jam ,and accidents. Vehicular Ad Hoc Networks (VANETs) helps to alleviate traffic fatalities by vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [28] based on dedicated short range communications (DSRC) and VLC as proposed in [32].

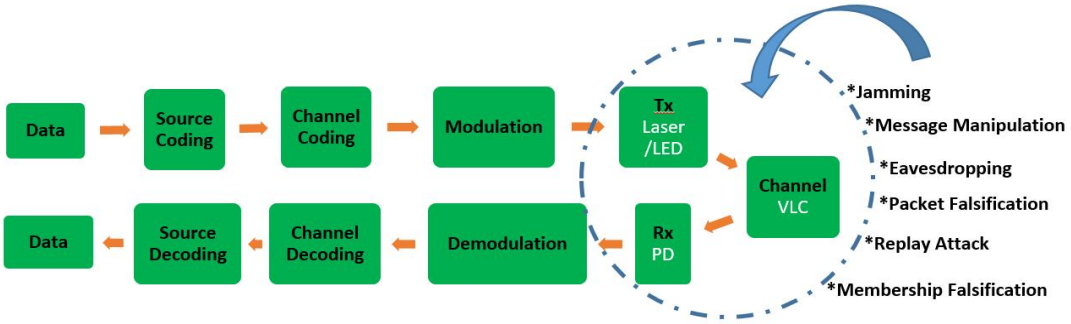


Figure 5. Communication system block diagram.

Information exchange is offered by (VANETs) using wireless communication between vehicles, which will mitigate traffic problems and support self- driving cars [33]. VANET applications transmit Cooperative Awareness Messages (CAM) frequently to maintain safe and efficient traffic flow, which includes information like timestamp, position, speed and heading. A critical privacy threat can result because this information is broadcast publicly [34], especially if CAMs are gathered and evaluated.

Wyner was a pioneer in proposing the wiretap channel [35], an information-theoretic point of the physical-layer security and a channel in which an eavesdropper perceives a corrupted version of the signal. Further Csiszár and Körner continued the degraded wiretap channel to the non-degraded broadcast channel [36]. Their crucial work showed that ideal secrecy can be achieved as long as the legitimate user has a less attenuated channel than the eavesdropper, and the secrecy capacity is the difference between the two user's information capacities. However the number of legitimate information detected by unauthorized eavesdroppers is limited because the physical-layer security use the randomness of the wireless communication channel noise [37][36]. Their work is all concentrated on RF based wireless networks. On the other hand, in VLC [38] proposed

the fuzzy timing passwords to differentiate between the legitimate user and the eavesdropper. Also in [39] screen view angles and leveraged user induced motions was used between smartphones in the secure barcode-based visible light communication (SBVLC). Furthermore to secure the physical layer, Mostafa et al. suggested the use of VLC-friendly jamming [40], VLC-artificial noise [41], and VLC beamforming [42].

Currently, many technological giants are working on VLC-enabled products [43][44], as a lot of research has been conducted to bring VLC to market. A research founder of VLC and PureLiFi Ltd. company, Harald Hass initiated a “LiFi-X station” and “LiFi- X Access Point” with a data rate of 43 Mbps. In France Oledcom, another indoor VLC company provides VLC modules and chips for communication. Also, Fraunhofer-Gesellschaft in Germany achieved 1 Gbps wireless local link using high-power LEDs. “WHAT YOU SEE IS WHAT YOU SEND” (WYSIWYS) [45], is an assumption for VLC security; due to the signal’s line-of-sight, directivity, and non-passing nature. However, there are still general security requirements for VLC networks to be secure against several threats and there are potential concerns to legitimate users, particularly in public areas.

During the past years, PLS has endorsed attention and renewed interest as part of multiple layer security. PLS depend on Wyner “wiretap channel” model in 1975 and then was developed for several channel models of wireless systems [46][47]. In the Gaussian MISO wiretap channel, zero-forcing the eavesdropper’s reception using beamforming is optimal at high SNR [48]. In the VLC security research area, PLS is the most advanced approach and involves techniques such as VLC beamforming, VLC secure communication zones, and VLC friendly jamming.

Several challenges lie ahead of the development of full wireless networks based on light from point to point links. Multiple access techniques are needed to serve multiple users within

each cell. Also, the portable devices will require low energy consumption thus the deployment of an uplink can have another scheme different from the downlink. The utilization of the IR spectrum is the most appropriate method for the uplink because the use of visible light sources can be distracting to users. Simultaneously, modulation schemes for a high-rate uplink have to be power efficient and spectrum efficient as achieved in two techniques, the enhanced unipolar orthogonal frequency division multiplexing (eU OFDM) [49], and the OFDM spectral and energy efficiency.

One of the greatest misunderstandings is that VLC is a LOS technology. Fig. 6 [50] shows a successful video transmission to a laptop where there is no direct LOS link and over a distance of about 3 m where the transmitter LED is not directed to the receiver but to the opposite white wall. Though a transmission with an error-free link cannot be achievable if the wall is dark and signal to noise ratio (SNR) drops below the -6 dB threshold; single-photon avalanche diodes can improve the receiver sensitivity in low-light conditions by at least an order of magnitude [51].

Figure 6. Operation of a LiFi link under strict non-line-of-sight (LOS) conditions [50].

Another misconception that VLC does not work in the daytime; the electrical filters can filter out the constant sunlight because VLC uses frequencies greater than 1 MHz. Moreover, the shot noise is another concern as it is hard to remove by optical filters. The author in [52] investigated the effect of shot noise qualitatively and discovered that the throughput is adjusted by

1.5% and 4.5%. By utilizing optical filters and automatic gain control algorithms, saturation can be eliminated.

The study in [50] achieved a data rate of 1.1 Gbps over a distance of 10 m with a 4.5 mW LED of optical output power. Current VLC systems data rates are proliferating quickly. Researchers have reported various high-speed data rates, and the OFDM VLC system achieves a throughput up to 11.1 Gbps [53]. Despite the application of high-speed VLC systems is limited due to offline processing instead of real-time. A real-time VLC system utilized 2ASK-OFDM coding and achieved a speed up to 76 Mbps [54]. [55] achieved a throughput of 200 Mbps by applying bidirectional rate adaptive OFDM transmission. Besides, the author in [56] realized a real-time VLC system with high-speed based on RGB-LEDs to meet the wireless indoor multimedia communication (WIMC) guidelines with a data rate beyond 500 Mbps and 100 Mbps under poor channel conditions.

The existence of LEDs in vehicular systems, VLC has been an attractive alternative to serve as vehicle-to-X Communications at a low cost [57][58][59][60][61]. The interesting double role of the LED light sources on vehicles leads to illumination and communication. Different from RF systems, VLC vehicular systems mostly depend on the undistracted LOS transmission due to the lack of reflecting fixed surfaces.

In [62] they found that the coherence time of VLC in all applicable areas is larger with an order of magnitude than the RF coherence time. Generally, the VLC link is more stable because the channel lasts steadily for a long time and needs less recurring channel estimation. Platooning and cooperative adaptive cruise control (CACC) (ETSI[63]) especially use it, as VLC is robust enough to provide constant and continuous V2V links; joined with the normal directional flow of cars in a platoon, and long coherence time. Also, VLC can serve as an alternative when the channel

is disturbed or congested in the RF link. Moreover, they showed that when vehicles are not in the same direction the duration for VLC link is less than RF. In other scenarios as long as cars are following the same direction, VLC sustained a long period of time link duration, which illustrates the use of V2V in platooning, emergency braking, overtaking, etc.[63].

In addition, VLC can improve accurate relative position vehicle estimation because of its stability to maintain relative positioning among cars [64]. Platooning, CACC [63], Vulnerable Road User (VRU) and Left-Turn Assist are case examples for such use. Satellite-based system (e.g., GPS) needs additional sensors for positioning due to the error that can be in meters in open space and tens of meters urban multipath scenarios [65]. Thus results in difficulty in most V2X lane-level accuracy and any use depending on relative position. However using radar/LIDAR systems or camera can make improvements, VLC offers an alternative positioning system that can be used in a cost-effective manner. For example, VLC can enhance the estimation and adjustment of intervehicle spacing in a platoon or help in car merging in case of CACC. Moreover, it can be used to determine the accurate trajectories of Vulnerable Road User (VRU) with respect to the car. The mobility between cars interrupts LOS links for VLC which likely cause limitation on the communication distance. Also, VLC does not work accurately for non-line of sight (NLOS) cases and both experimental [66] and theoretical [67] results show that stable communications take place only with a maximum of 50 meters distance.

Certainly, the major interest of platoon depends on the reduction of V2V spacing, which offers road capacity enhancement and fuel consumption reduction by limiting the air drag. Therefore, the latency in transmission must be controlled to stay as low as possible because it is crucial in platoon systems to reduce car response time and thus V2V spacing. The standard V2V gap on highways in the European Truck Platooning network is 0.3s, which is approximately

equivalent to 10 m at 130 km/h [68]. The latency in transmission must be below 20 ms, as reported by the United States Department of Transportation (USDOT), with around 400 bits packets transmission, even with other road members interfering the transmission [69]. Thus VLC has been considered as an alternative technology, and in [70] evaluated its compatibility with platooning. A simple system is tested with different indoor scenarios and evaluated the transmission latency at 4.2 ms with headlamps and taillights using commercial off-the-shelf (COTS) LED [71]. In addition, up to 30 m, the data rate was 100 Kbps deploying front or back lamps and bit error rate (BER) was below 10^{-6} [71].

Communication systems are designed to send information from a source to one or more destinations. The general communication system block diagram is shown in Fig. 7. The information generated by the source may be of the form of voice, a picture, video or plain text in some particular language, then converted into a sequence of binary digits by the source encoder. The channel encoder introduces, in a controlled manner, some redundancy in the binary information sequence which can be used at the receiver to overcome the effects of noise and interference in the transmission of the signal through the channel.

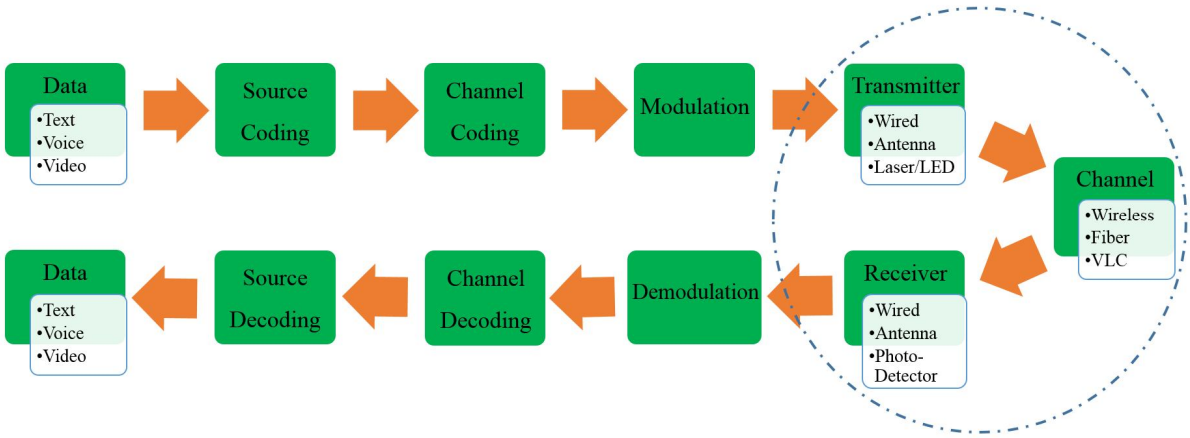


Figure 7. Communication Functional Block Diagram.

The output of the channel encoder is passed to the modulator then transmitted through the channel which can be wired or wireless medium; such as copper wire, coaxial cable, wave guide, fiber optic cable, antennas and laser or LED. Similarly for the receiver, it can be wired, antenna or photodetector, in case of optical transmission, which will recover the data that will be demodulated and decoded to construct the original data. Our research is focused on the circled part of the communication block diagram; considering visible light communication, LED for the transmitter, and photodetector for the receiver.

CHAPTER 3

IEEE 802.15.7: VISIBLE LIGHT COMMUNICATION STANDARD

3.1 Introduction

Visible light communications (VLC) use the visible spectrum wavelengths of 390–750 nm or frequency band of 400–790 THz and offer wireless communication using light-emitting diodes (LEDs).It is viable to transmit data using LEDs without an observable effect on the lighting output and the human eye, because the human eye notices only the average intensity when light changes fast enough. VLC can be used in a various range of short- and medium-range communication applications, which include wireless local, personal, and body area networks (WLAN, WPAN, and WBANs), vehicular networks, and machine-to-machine communication along with many others. In addition to energy efficiency, VLC provide multiple other inherent advantages over radio frequency (RF)-based counterparts, like immunity to electromagnetic interference, operation on unlicensed bands, additional physical security, and a high reuse factor resulting from a high degree of spatial confinement.

The academic interest in VLC is growing, resulting in a rich literature spanning from channel modeling to physical layer design and upper layer issues .Beside of academic interest, industrial attention to VLC has caused related standardization activities to avoid fragmentation of proprietary vendor solutions in this emerging market. In Japan, the Visible Light Communications Consortium (VLCC) (www.vlcc.net) boosted the standardization activities and offered two standards known as the visible light communication system standard and the visible light ID system standard, which were accepted by the Japan Electronics and Information Technology Industries Association (JEITA) in 2007 and became known as JEITA CP-1221 and JEITA CP-1222, respectively. Recently, in June 2013, they also proposed an enhanced version of the JEITA

CP-1222 named as JEITA CP-1223 visible light beacon system standard. Realizing the potential of this emerging technology, the Institute of Electrical and Electronics Engineers (IEEE) produced IEEE Standard 802.15.7, which was approved in June 2011 (IEEE, 2011). The standard describes a physical layer (PHY) and a medium access control (MAC) layer for VLC and guarantees data rates sufficient to accommodate audio and video multimedia services. In this chapter, we first provide an overview of this IEEE standard describing the main features of PHY and MAC layers. The last section is reserved for the most recent standardization activity, which will modify the IEEE Standard 802.15.7.

3.2 Overview of IEEE standard 802.15.7

As personal area network (PAN) is the connection of information technology devices within a short distance. IEEE Standard 802.15.7 presents visible light communication personal area network (VPAN) as its network form. In a VPAN, a coordinator is in charge for starting and maintaining a network, and assigning new devices to an existing VPAN. Also VPANs defined three different network topologies, peer-to-peer, star, and broadcast.

- **Peer-to-peer topology:** The peer-to-peer networking topology is described to support communication between two nodes that ordinarily can be used for both sending and receiving, and act as both a device and a coordinator.
- **Star topology:** For this topology, a coordinator controls the communication network and can connect with all the devices within the network.
- **Broadcast:** The coordinator sends data which will be received by every device in the network. This type of communication is unidirectional, as a result it doesn’t involve a destination address.

IEEE 802.15.7 standard examined three classes of VLC devices; infrastructure, mobile (portable), and vehicle. In Table 1, the main specifications of each class are shown.

Table 1. VLC Device Classification

	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

3.3 MAC Layer

The MAC layer offers two functions accessed through two service access points (SAPs). MAC management is accessed through the MAC link management entity SAP (MLME-SAP), while MAC data are accessed through the MAC common-part sublayer SAP (MCPS-SAP). The MAC layer executes 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 (i.e., a function that provides information, such as device status and channel quality to the human eye via color)
5. Supporting visibility to maintain illumination and mitigate flicker
6. Supporting dimming (i.e., reducing the radiant power of a transmitter while preserving the color of the transmitted light)
7. Supporting device security
8. Providing a reliable link between two peer MAC entities
9. Supporting mobility

The standard provides systems to start and maintain a VPAN. The device uses channel scanning to access the current state of a channel, locate all beacons within its operation environment, or detect a specific beacon with which it has lost synchronization. The networks need beacons for synchronization or support for low-latency devices. If the network does not require synchronization or support for low-latency devices, it can choose to turn off the beacon for ordinary transfers. However, network discovery still needs the beacon. Then a channel scan and selection of a proper VPAN identifier, which is not used by any other PAN in the same area, operation as a coordinator starts. The association/disassociation systems to permit the devices to join or leave a VPAN are further explained in the standard.

3.4 PHY Layer

The duties of the physical (PHY) layer are link foundation and termination of a connection to a communications medium. According to the IEEE 802.15.7 standard for VLC, the PHY layer is responsible for the following tasks:

- Activation and deactivation of the VLC transceiver
- Wavelength quality indication (WQI)
- Clear channel assessment
- Data transmission and reception
- Error correction
- Synchronization
- Supporting dimming

Based on the intended data rate and usage environment, the IEEE 802.15.7 standard includes a number of various PHY layer types:

- PHY I: In his type on–off keying (OOK) and variable pulse position modulation (VPPM) are used. It handles concatenated coding with Reed–Solomon (RS) and convolutional coding (CC). This PHY type is designed for outdoor low data-rate applications with rates in the tens to hundreds of Kbps.
- PHY II: Similar to PHY I, PHY II uses OOK and VPPM but with higher optical clock rates intending to achieve higher data rates in the tens of Mbps. But It only supports RS coding. This PHY type is for indoor operation with moderate data rate

applications. PHY I and PHY II also support a run-length limited (RLL) code to maintain DC balance, clock recovery, and flicker mitigation.

- PHY III: This type is designed for applications with multiple light sources and detectors. It operates using CSK and RS coding. The desire of this type is to achieve data rates in the order of the tens of Mbps.

All operating modes are listed in Table 2.Any IEEE 802.15.7-compliant device must assign at least one of the PHY I and PHY II types. For coexistence a device using the PHY III type should also implement PHY II mode. Also the PHY types may work in the existence of dimming. As OOK under dimming condition maintains constant range and variable data rate by embedding compensation time. However, VPPM under dimming maintains constant data rate and variable range by altering the pulse width. More specifications on the optical clock rates, data rates, and error correction codes for each PHY type are illustrated in Table 2. As shown in Table 2, multiple optical rates are presented for all PHY types in order to assist a broad class of LEDs for different applications. The MAC layer chooses the optical rate used for communication during device discovery.

3.5 Recent Activities in IEEE standardization

The IEEE 802.15 working group (WG) created a study group to determine if an amendment to the standard is needed. The group discussions and suggestions from industry and academia indicated a project authorization request which states:

This amendment explains a physical layer (PHY) using light frequencies over the spectral range of 10,000 nm (infrared [IR]) to 190 nm (near ultraviolet [UV]) and any MAC changes exactly required to aid this PHY.

Table 2. VLC Device Classification

				FEC		
	Modulation	RLL Code	Optical Clock r	Outer Code (rs)	Inner Code (cc)	Data Rate
PHY I	OOK	Manchester	200 KHz	(15,7)	1/4	11.67 Kbps
				(15,11)	1/3	24.44 Kbps
				(15,11)	2/3	48.89 Kbps
				(15,11)	None	73.3 Kbps
				None	None	100 Kbps
	VPPM	4B6B	400 KHz	(15,2)	None	3556 Kbps
				(15,4)	None	71.11 Kbps
				(15,7)	None	124.4 Kbps
				None	None	266.6 Kbps
PHY II	VPPM	4B6B	3.75MHz	(64,32)	None	1.25 Mbps
				(160,128)	None	2 Mbps
			7.5 MHz	(64,32)	None	2.5 Mbps
				(160,128)	None	4 Mbps
				None	None	5 Mbps
	OKK	8B10B	15 MHz	(64,32)	None	6 Mbps
				(160,128)	None	9.6 Mbps
			30 MHz	(64,32)	None	12 Mbps
				(160,128)	None	19.2 Mbps
			60 MHz	(64,32)	None	24 Mbps
				(160,128)	None	38.4 Mbps
			120 MHz	(64,32)	None	48 Mbps
				(160,128)	None	76.8 Mbps
				None	None	96 Mbps
PHY III	4-CSK		12 MHz	(64,32)	None	12 Mbps
	8-CSK			(64,32)	None	18 Mbps
	4-CSK		24 MHz	(64,32)	None	24 Mbps
	8-CSK			(64,32)	None	36 Mbps
	16-CSK			(64,32)	None	48 Mbps
	8-CSK			None	None	72 Mbps
	16-CSK			None	None	96 Mbps

Transmitting devices carry such sources as displays, commonly found on cameras and mobile devices, and other LED based sources such as flashes, flashlights, LED tags, and LED/laser sources. (IEEE P802.15.7r1, 2016)

As IEEE Standards Association accepted the project authorization request, the IEEE 802.15 WG are able to work on a new standard which is open to almost any type of VLC communication. For prospective standard proposals (Janget al, 2015), a technical requirements document has been prepared for guidance, which uses the term optical wireless communication (OWC) and classifies OWC into:

- Image sensor communications
- Low-rate photodiode communications
- High-rate photodiode communications

Considering the definition of low speed and high speed, the throughput threshold data rate is 1 Mbps as measured at the PHY layer output of the receiver. Any throughput less than 1 Mbps rate is considered low rate and higher than 1 Mbps is considered high rate. The group decided the feasible applications that can be served by each communication type. Image sensor communications enable OWCs using an image sensor as a receiver. Main applications of image sensor communications are listed as:

- Offline to online marketing/public information system/digital signage
- Internet of Things (device-to-device/Internet of light [IoL])
- Location-based services/indoor positioning
- Vehicular communication/vehicular positioning
- Underwater communication
- Point-to-(multi)point/relay communication

Low-speed photodiode receiver communications, which is a wireless light ID system using various LEDs with a low-speed photodiode receiver, can be used in the below applications:

- Underwater/seaside communication
- Point-to-(multi)point/communication
- Digital signage
- Internet of Things (device-to-device/Internet of light [IoL])
- LOS authentication
- Identification based services

The high-speed photodiode receiver communications is high-speed, bidirectional, networked, and mobile wireless communications using light with a high-speed photodiode receiver. Main applications for high-speed photodiode receiver communications are:

- Indoor office/home applications (conference rooms, general offices, shopping centers, airports, railways, hospitals, museums, aircraft cabins, libraries, etc.)
- Data center/industrial establishments, secure wireless (manufacturing cells, factories, hangers, etc.)
- Vehicular communications (vehicle-to-vehicle, vehicle-to-infrastructure)
- Wireless backhaul (small cell backhaul, surveillance backhaul, LAN bridging)

The group was assigned another task to determine if a channel model is necessary to compare different standard proposals. The group decided that all proposals which include the PHY algorithms for the high-rate PD communications must use the channel impulse responses provided

in TG7r1 Channel Model Document for High-rate PRD Communications (Jang et al. 2015) for the specific scenario that they intend to address in their proposal. The exact channel impulse responses are provided in TG7r1 CIRs Channel Model Document for High-rate PD Communications (Uysal et al. 2016).

CHAPTER 4

INDOOR VISIBLE LIGHT COMMUNICATION SECURITY

4.1 Introduction

Premier RF studies that define the secrecy performance in multiuser wireless networks from an information theoretic view depend on the secrecy graph model to study the node connectivity [72], [73] and the maximum secrecy rate [74]. Besides, the secrecy capacity scaling laws in a wireless network were indicated in [75] to study the secrecy rate per source-destination pair. Other than the network theory information, latter works used mathematical tools from stochastic geometry to study the secrecy performance in multiuser wireless networks [76],[77].

In contrast to RF communication, VLC uses intensity modulation and direct detection (IM/DD) due to the use of low-cost light-emitting diodes (LEDs) and photodiodes (PDs) as the optical transmitter and receiver, respectively. The signal in VLC is modulated using the LED intensity, but it must follow the dynamic range of typical LEDs and practical illumination guidelines [78][79][80][81]. The outcomes on the secrecy capacity achieved for RF networks cannot be directly used in VLC networks. As LEDs have a nonlinear electrical-to-optical transfer characteristic, this nonlinearity can be well restored by pre-distortion means [82]. It is important to attain the VLC channel information capacity with average, peak and non-negative constraints before figuring the secrecy capacity in VLC network, because the secrecy capacity is associated with the communication channel capacity information [36][37].

Even though still the definite information capacity of VLC channel is anonymous. Despite some bounds have been evaluated, still the information capacity is unknown for a simple case like SISO. As in [42] studied lower and upper bounds on the secrecy capacity of the amplitude-constrained Gaussian wiretap channel regarding one transmitter, one legitimate user and one

eavesdropper. Also [42], applied beamforming to enhance the secrecy capacity for the MISO VLC channel. Subsequently, the ideal beam former design issue subject to amplitude constraints was additionally examined in [83]. However, for the MISO case, the effect of the channel correlation on VLC security is totally ignored by previous work. The procedure of VLC system secrecy using one access point (AP) in a single cell was studied in [84]. However the arbitrary action of legitimate users and eavesdroppers, specifically the interaction between them, have not been exactly evaluated when considering the multiuser VLC network secrecy performance.

Table 3. VLC Secrecy Enhancement Techniques

Paper	Method
Mostafa [42]	Studied the secrecy capacity lower and upper bounds. Applied beamforming to enhance the secrecy capacity for the multiple-input single-output (MISO) VLC channel.
Wyner [37]	Showed that a non-negative secrecy rate can only be achieved when the legitimate user achieves a higher SNR than the strongest eavesdropper.
Araki [38]	Fuzzy timing passwords, which used different time delay to differentiate between the legitimate user and the eavesdropper.
Zhang [39]	Screen view angles and leveraged user induced motions was used between smartphones in the secure barcode-based visible light communication (SBVLC).
Mostafa [40][41]	To secure the physical layer VLC-friendly jamming, VLC-artificial noise, and VLC beamforming was used.
Liu [25][86]	Studied the effect of using more APs and their cooperation results in enhancing the secrecy performance of VLC networks. The effect of reflected paths and channel correlation on VLC security was modeled and analyzed.
Romero-Zurita [87]	Used a strategy named the “protected zone” to enhance the secrecy performance of legitimate user in VLC networks.

Moreover to the best of the author's knowledge the previous work neglected the light reflection which is not feasible in indoor model. Also it was proved that eavesdroppers can deduce legitimate information by using a small part of the reflected signal [85].

The work in [25] studied the performance of physical-layer secrecy in a three dimensional multiuser VLC network by using mathematical tools from stochastic geometry. The impact of reflected paths and channel correlation on VLC security was modeled and analyzed in [86]. Summary of different VLC network privacy enhancement methods are shown in Table 3.

4.2 Indoor VLC System Model

To simulate visible light indoor communication system model using LED lights, we define room 1 with the APs represented by four LEDs evenly distribution on the ceiling of the room as seen in Fig. 8, while room 2 used six APs with the locations shown in Table.4.Also, we consider a downlink VLC transmission scenario of a multiuser network with the existence of both legitimate user and eavesdroppers in a three dimensional space.

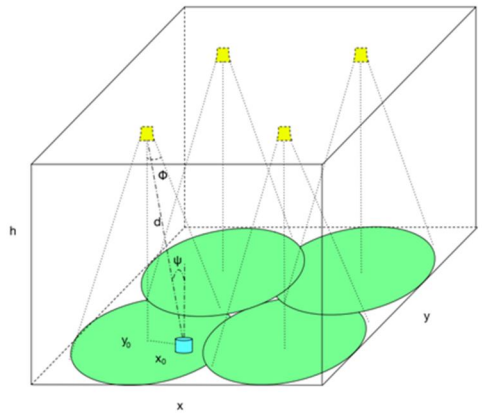


Figure 8. Representation of a room with four LEDs and their footprint.

In this chapter, the white LEDs emit high frequency light waves which has the modulated signals that are transmitted to the receiver through the air, lighting at the same time to complete

the wireless transmission of data. The VLC APs are attached to the room ceiling, and their positions are in Table.4. Similarly, mobile users are assumed to be at a fixed height.

A. Transmitter

The channel transfer function for white LED light source directly pointing in the direction of optical receiver is given by [88]:

$$H_{LOS} = \begin{cases} \frac{A_{rx}}{h^2} R(\emptyset) \cos(\varphi) & 0 \leq \varphi \leq \varphi_c \\ 0 & \varphi > \varphi_c \end{cases} \tag{3.1}$$

where A_{rx} denotes the effective detector area of the PD, h is the distance between the transmitter and the receiver, φ is the angle of incidence. The PD at each user is assumed to be facing vertically upwards with a field of view (FOV) of φ_c .The VLC Aps are assumed to have a Lambertian radiation profile R(∅) known as:

$$R(\emptyset) = \left[\frac{n+1}{2\pi}\right] cos^n(\emptyset) \tag{3.2}$$

$$n = -ln2/\ln(\cos \emptyset_{\frac{1}{2}}) \tag{3.3}$$

where n is Lambertian emission coefficient, associated with semi-angle at half power $\emptyset_{\frac{1}{2}}$ of the LED.

B. Receiver

The total received power for only LOS channel for only LOS channel expressed as:

$$P_{LOS} = \sum_{i=1}^{LED_{num}} P * H_{LOS} \tag{3.4}$$

The receiver is consisted of photodiode, concentrator and optical filter, as a consequence the received power for LOS channel is:

Table 4. Indoor Simulation Parameters

Parameters for a VLC downlink		
Room 1	Size	5×5×3 m^3
Source	Location (4 LEDs)	(1.25,1.25,3),(1.25,3.75,3), (3.75,1.25,3),(3.75,3.75,3)
	Semi angle at half power (FWHM)	35º
	Transmitted power (Per LED)	20mW
	Number of LEDs per array	60*60 (3600)
Room 2	Size	5×5×3 m^3
Source	Location (6 LEDs)	(1.6,1.25,3),(1.6,3.75,3), (2.5,1.25,3), (2.5,3.75,3) (4.1,1.25,3), (4.1,3.75,3)
	Semi angle at half power (FWHM)	15º
	Transmitted power (Per LED)	20mW
	Number of LEDs per array	60*60 (3600)
Receiver	Receive Plane above the floor	0.85 m
	Active area (A_{rx})	1 cm2
	FOV	60º
	Amplifier Bandwidth B_a	50 MHz
	Concentrator Gain g	6.0
	Photodiode responsivity r	0.4 A/W

	Amplifier noise density i_{am}	$5\ pA/\sqrt{Hz}$
	Ambient noise power P_n	19.272 μW
	Noise bandwidth factor I_1	0.562
	Optical filter's transmission coefficient T	1.0

$$P_{re} = P_{LOS} \times g \times T \tag{3.5}$$

where g is the concentrator gain, T is the optical filter's transmission coefficient.

4.3 Simulation Results Discussion and Summary

A. Optical Power Distribution

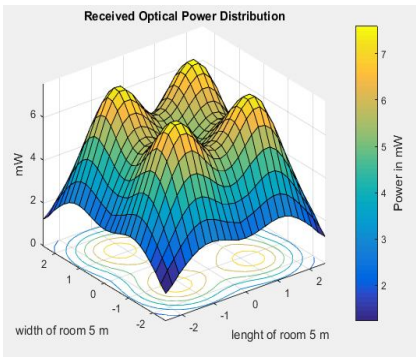
In this section, we used a MATLAB implementation to validate our proposed model. Two typical rooms are considered with a size of 5×5×3 m^3, the network parameters used for simulation setup are described in Table 4.

First we consider the scenario where the legitimate users are served by four APs, as depicted in Fig. 9(a).Therefore, malicious eavesdroppers can be as close as possible to the legitimate user, as shown in room 1 top view Fig. 9(c). It can be seen that, when the semi angle at half power is large, 35°; and using few APs, four in the first room can efficiently reduce the secrecy at the legitimate user. However, when reducing the semi angle to 15°, further increasing the APs within the second room to six, Fig. 9(b), the secrecy performance of the legitimate user obviously increased, as shown in room 2 top view Fig. 9 (d).As the received power is highly concentrated in the zone around the legitimate user, 1 m of diameter, and it decreases as long as you move away from the specified zone, so eavesdroppers cant reconstruct the signal with power levels lower the 4 mW.

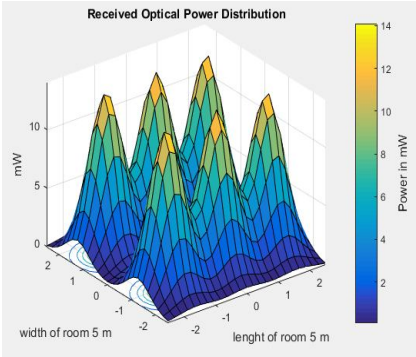
Therefore using both methods, reducing the semi angle at half power of the LED and applying more APs in the VLC indoor system, will automatically form a protected zone around the legitimate users to enhance the privacy and secrecy of the users in VLC networks. The AP will stop the communication and the AP will alert the legitimate user, if any eavesdropper get in the protected zone, as this action will be made aware to the AP. The operation of the protected zone in VLC networks can be utilized with motion sensors that are already built in current energy efficient lighting devices [87]. A secrecy protected zone is determined by its center, its associated AP position, and a security radius, which is the smallest horizontal distance between the AP and any undetected eavesdroppers.

B. Signal to Noise Ratio Analysis

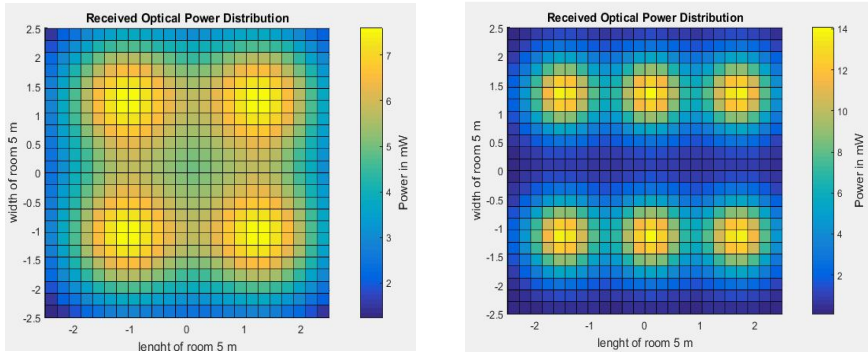
The authors of [25] proved that in order to have better secrecy performance it can be reached when the legitimate user has a higher SNR than the strongest eavesdropper. By analyzing the SNR and using the parameter in Table 4, the simulation results of the SNR for the two rooms is shown in Fig. 10.



(a) Room 1



(b) Room 2



(c) Room 1 (d) Room 2

Figure 9. Optical power distribution in received optical plane for a FWHM of (a) 35° with four APs, (b) 15°with six APs and (c) , (d) are top view for room 1 and room 2 respectively.

The photodetector will convert light signals to electrical signals and the SNR is indicated as:

$$SNR = \frac{i^2}{\sigma^2} \tag{3.6}$$

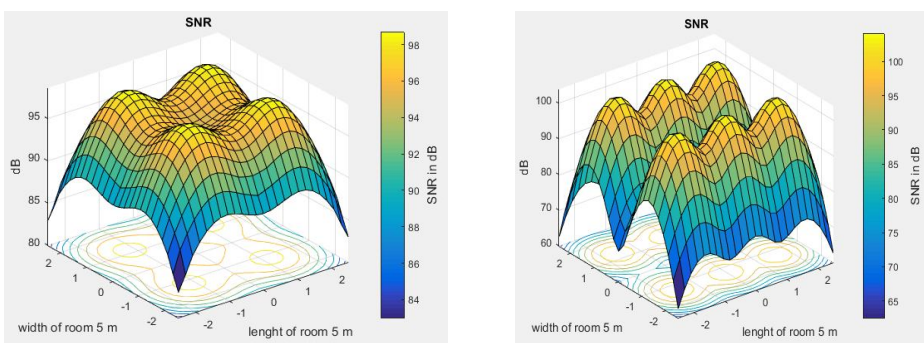
where σ^2 is the total noise variance and i is the photodiode's output current and are shown as :

$$\sigma^2 = \sigma_{sh}^2 + \sigma_{am}^2 \tag{3.7}$$

$$i = P_{re} \times r \tag{3.8}$$

$$\sigma_{sh}^2 = 2(P_{re} + P_n) \times q \times r \times B_n \tag{3.9}$$

.



(a) Room 1 (b) Room 2

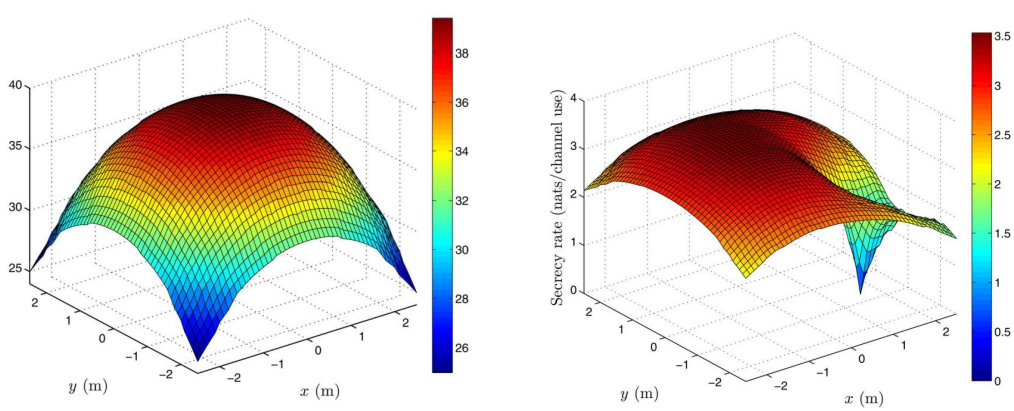
Figure 10. SNR or receiver for a FWHM of (a) 35° with four APs , (b) 15°with six APs .

$$B_n = I_1^2 R_b \tag{3.10}$$

$$\sigma_{am}^2 = i_{am}^2 B_a \tag{3.11}$$

where σ_{sh}^2 is the shot-noise variance, σ_{am}^2 is the amplifier noise variance, r is the photodiode response rate, P_n is the ambient light's noise power, B_n is the noise bandwidth, I_1 is noise bandwidth factor, R_b is data rate, i_{am}^2 and B_a are the amplifier noise density and the amplifier bandwidth, respectively. When the semi half angle is decreased from 35° to 15°and by using six APs rather than four APs, the SNR outside the circular protected zone at each AP dropped from 95 dB to 75 dB, as shown in Fig. 10 (a) and (b). This result is in agreement with what have been proved, increasing the density of APs can defiantly enhance the secrecy and privacy performance of the legitimate user in VLC networks. As it shows a significant decrement in SNR of the eavesdroppers located outside the protected zone and instead increasing the SNR of the legitimate user.

4.4 Previous Work



(a) (b)

Figure 11. Spatial distribution of the SNR without beamforming (a), Secrecy rate achievable via zero-forcing beamforming (b).

The authors in [42] derived closed-form lower and upper bounds on the secrecy capacity of the amplitude-constrained wiretap channel. Then, they utilized beamforming to obtain achievable secrecy rates for the MISO channel. They showed that zero-forcing is an appropriate strategy for secure transmission over MISO VLC channels. Although suboptimal, zero-forcing is preferable as it is an achievability strategy that eliminates the need to use secrecy codes which involve stochastic encoding. Fig. 11 (a) shows the spatial distribution of the SNR at the receiver's height without beamforming. As can be seen, the SNR reaches its maximum value, 39.40 dB, at the room center, and decays to 24.97 dB at the corners. In Fig. 11 (b), Bob's location is fixed and the secrecy rate is shown as a function of Eve's location within the entire room area. As expected, the secrecy rate significantly decreases when Eve is close to Bob. Once Eve is relatively far, e.g., more than about 2.5 m, the secrecy rate is almost independent of Eve's exact location.

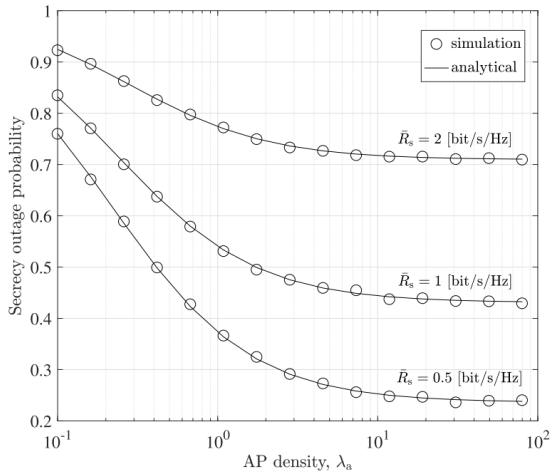


Figure 12. Secrecy outage probability versus VLC AP density.

The author in [25] fixed the density of eavesdroppers (λe = 0.2), the secrecy outage probability at the typical legitimate user is evaluated at different values of the AP density, as shown in Fig. 12. It can be seen that, when λa is small, increasing the density of VLC APs can

efficiently reduce the secrecy outage probability at the legitimate user. However, when λa is large, further increasing the density of VLC APs only slightly reduces the secrecy outage probability. When λa is increased from 1 to 10, the secrecy outage probability only drops by 0.1. Also, it is shown that a lower bound on the secrecy outage probability exists even if the density of VLC APs approaches infinity.

CHAPTER 5

INDOOR VLC PHYSICAL LAYER SECURITY

5.1 Physical Layer Security Solutions

During the past years, PLS has endorsed attention and renewed interest as part of multiple layer security. PLS depend on Wyner "wiretap channel" model in 1975 and then was developed for several channel models of wireless systems [46][47]. In the Gaussian MISO wiretap channel, zero-forcing the eavesdropper's reception using beamforming is optimal at high SNR [89] . In the VLC security research area, PLS is the most advanced approach and involves techniques such as VLC beamforming, VLC secure communication zones, and VLC friendly jamming.

A. VLC beamforming:

There is an obvious difference between the normally used beamforming methods in RF and those in VLC since in RF the exact data bit's energy is directed to a target zone to increase the signal gain. However, in VLC the illumination is kept at a uniform level and only the data signal is directed [99]. In [22], a VLC MIMO system maintains constant illumination and directs the data to the legitimate receiver to decrease the eavesdropping possibility by using hidden-channel methods and beamforming to allow security and channel access. Mostafa and Lampe [31] make an extended theoretical analysis of a robust beamforming technique, where Alice (transmitter) has unknown information about Bob's (legitimate receiver) and Eve's (eavesdropper) channels. In [41] they prove that secrecy rates can be enhanced by applying beamforming and null-steering if Eve's CSI is known or by using artificial noise to maintain secure transmission if Eve's CSI is unknown.

Table 5. VLC Physical Layer Security Techniques

Paper	Method
Yin [24]	Studied the achievable secrecy rate for the MISO VLC wiretap channel and showed that the truncated generalized normal distributions provide significant gains in secrecy rates under beamforming schemes compared to the normal distribution and Gaussian distributions.
Liang [47]	Proposed a random time reversal scheme for both SISO-VLC and MISO-VLC system which takes advantage of both the VLC's multi-path redundancy characteristics and time diversity to secure transmission. Automatically focusing the transmitted signal on the legitimate user while interfering with the eavesdropper's channel by time reversal and random choice techniques.
Khisti [90]	Showed that building an eavesdropper-free protected zone around the AP significantly improves the secrecy performance of legitimate users.
Yu [48]	The experimental results showed that by applying a physical-layer secure coding scheme based on polar codes for indoor VLC wiretap channels the secrecy capacity can be achieved for transmitting secret information with guaranteed security and reliability.
Al-Khori [91]	Achieved higher secrecy capacity in a hybrid RF/VLC network with multiple relays with jamming capabilities by using a novel joint relay-jammer selection scheme conditioned on the minimum outage and maximum SNR and beamforming vectors were applied in the formulation of the power minimization problem.
Soderi [92]	Proposed an innovative scheme in which red, green, blue (RGB) light-emitting-diodes (LEDs) and three color-tuned photo-diodes (PDs) are used to secure a VLC by using a jamming receiver in conjunction with the spread spectrum watermarking technique.
Wang [93]	Improved the security of VLC with simultaneous lightwave information and power transfer (SLIPT) and random terminals along with employing the protected zone.
Cho [94]	Studied beamforming schemes and a simpler LED selection scheme to enhance the secrecy performance in VLC systems.
Mostafa [83]	Designed both the optimal and robust secrecy beamformers for the indoor MISO visible light communication system for both cases of perfect eavesdropper channel state information (CSI) and imperfect eavesdroppers CSI.
Shen [95]	Maximized the SNR of the legitimate user by using both transmit beamforming and jamming techniques to enhance communication secrecy for a MISO VLC system.
Yesilkaya [96]	Enhanced PLS in a VLC system by two new PLS techniques based on generalized space shift keying (GSSK) modulation with spatial constellation design (SCD) and NOMA.

Arfaoui [97]	Proposed a low-complexity precoding scheme and a low-complexity design of the precoding matrix. Based on the generalized singular value decomposition (GSVDs) of the legitimate receiver channel matrices and the eavesdropper, which enhanced the secrecy performance of the system.
Liang [98]	Conducted a security zone in the room and proposed a PLS approach based on optical beamforming to achieve secure transmissions.

The work in [23] shows that the perfect secrecy rates of a MISO VLC Gaussian wiretap achieve the truncated generalized normal distribution by artificial noise and beamforming. The author in [23] designs a secure beamforming method optimal for scenarios lacking the CSI of the eavesdropper.

B. VLC secure communication zones:

The secure zone is defined by its center joined with the access point (AP) position and a security radius, the minimum horizontal distance to any potential eavesdroppers from the AP location. It uses the motion sensors which are already built into modern lighting equipment [24]. Only users located in the protected zone are allowed to decode the transmitted signals. Mostafa and Lampe are pioneers in the protected zone VLC work [31]. The secrecy is measured using the secrecy rates and capacities, which are the maximum rates of a secure link (source-destination), while the signal is totally unknown to the eavesdropper. The author also uses null-steering and artificial noise to conduct positive secrecy rates and numerically evaluates them. Liu et al.'s proposed model is able to have Bob reconstruct the message perfectly while Eve can't decode the legitimate message and Eve's bit error rate (BER) simulation results are greater than the threshold [100]. Also in [101], the author studies a 3D VLC model with multiple APs and eavesdroppers and shows that when neighbor APs are cooperating they can increase the secrecy rate around the AP in the secure zone.

C. VLC friendly jamming:

The purpose of friendly jamming is to increase Eve's (eavesdropper's) interference level by adding artificial noise (jamming signals) to the transmitted signal. Therefore Eve's ability to decode the legitimate data is limited and the secrecy rates are increased, especially when Eve's CSI is unknown to the transmitter [41]. In [102] a friendly jamming scenario is proposed with typical amplitude and LED nonlinearity constraints which achieve a positive secrecy rate. The scenario in [103] has a room with nine LEDs, Alice (transmitter) uses the center LED for legitimate data, while the rest are used to jam Eve which show the secrecy rates for Bob (legitimate user) and Eve.

5.2 VLC PLS Proposed System Model

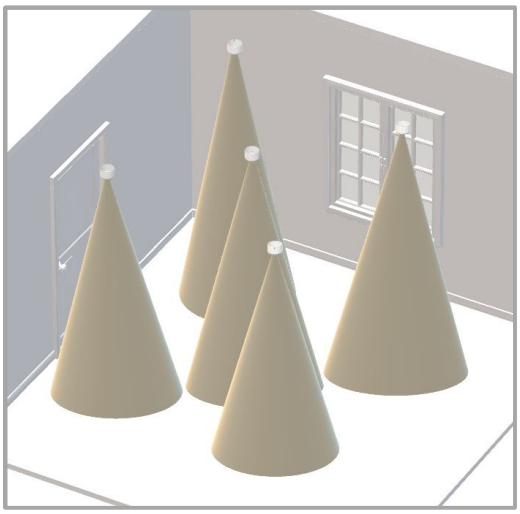


Figure 13. Footprint of a room with five LEDs.

We will study the indoor VLC model using LED lights, as shown in Fig. 13. Our work will focus on enhancing the secrecy rate by adding artificial noise to the channel, decreasing the semi angle of LED to create a secured zone around the legitimate user, and finally using a differential receiver to cancel any unwanted signals, such as jamming signals or ambient noise. The first

5×5×3 m3 room normally has four light fixtures attached to the ceiling and another room with five APs that use the Cartesian coordinate system to identify their locations and the center at (0,0). In the second room, the source at the center is used by Alice for data transmission, while the remaining 4 sources are used for jamming. To simulate a multiuser VLC system, we will consider both rooms with the downlink scenario in a 3-D space that has a legitimate channel in the existence of eavesdroppers. Since reflected signals are weaker compared to the line of sight (LOS) signal [104], a simplified model will consider the LOS component only, using the parameters in Table 6.

A. Mathematical model

The legitimate user has a better secrecy rate when they achieve higher SNR than any malicious attacker [101]. Therefore, the proposed model will depend on the SNR to reach the optimal secrecy performance. In order to calculate the SNR, the received optical power and the channel gain transfer function are shown in the mathematical model in chapter 3 using the new parameters in Table 6.

B. Differential Optical Receiver

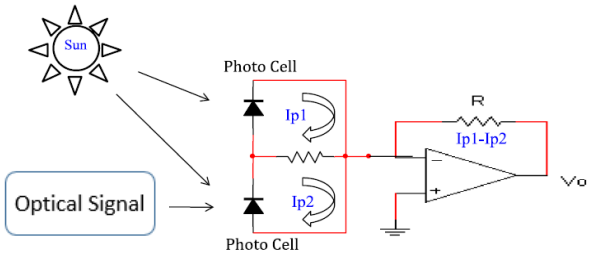


Figure 14. Differential optical receiver, illustrating sunlight cancellation; Ip1 and Ip2 are photocurrents due to ambient light and optical signal, respectively [105].

The differential optical receiver used by the legitimate user can cancel the ambient noise and any unwanted signals (jamming signals), two photodetectors are cross-coupled as shown in Fig. 14. The legitimate signal, sent to one receiver, becomes the dominant signal when all other

Table 6. PLS Indoor Simulation Parameters

Parameters for a VLC downlink		
Room 1	**Size**	**5×5×3 m^3**
Source	Location (4 LEDs)	(1.25,1.25,3),(1.25,3.75,3), (3.75,1.25,3), (3.75,3.75,3)
	Semi angle at half power (FWHM)	35º
	Transmitted power (Per LED)	20mW
	Number of LEDs per array	60*60 (3600)
Room 2	**Size**	**5×5×3 m^3**
Source	Location (5 LEDs)	(1.25,1.25,3), (1.25,3.75,3), (0,0,3), (3.75,1.25,3), (3.75,3.75,3)
	Semi angle at half power (FWHM)	15º
	Transmitted power (Per LED)	20mW
	Number of LEDs per array	60*60 (3600)
Receiver	Receive Plane above the floor	0.85 m
	Active area (A_{rx})	1 cm2
	FOV	60º
	Amplifier Bandwidth B_a	50 MHz
	Concentrator Gain g	6.0
	Photodiode responsivity r	0.4 A/W
	Amplifier noise density i_{am}	$5\ pA/\sqrt{Hz}$
	Ambient noise power P_n	19.272 µW
	Noise bandwidth factor I_1	0.562
	Optical filter's transmission coefficient T	1.0

signals are canceled out, then demodulated and decoded by means of code correlation [105]. As a result, the shot-noise will instead be expressed as:

$$\sigma_{sh}^2 = 2P_{re} \times q \times r \times B_n \tag{4.1}$$

5.3 Simulation Results Discussion and Summary

In this section, we produced our results using Matlab to simulate our proposed model with the parameters described in Table 6. Both rooms are typical in dimensions 5×5×3 m^3 and are deployed for the simulation setup. For the first room, Alice (transmitter) is supplied by four APs with 60×60 LEDs per array with 20 milliWatts (mW) optical power per LED, as depicted in Fig.15 (a) which was previously investigated in [24]. Bob (legitimate user) and Eve

(eavesdropper) are located 0.85 m above the floor. However, for the second room (proposed scheme), Alice will use a fifth AP added in the center of the room for data transmission, as shown in Fig.15 (b), while the four remaining sources are used for adding artificial noise (jamming) to the eavesdropper's channel, as shown in Fig.15 (c). The proposed footprint configuration is employed to enhance the secrecy performance of the legitimate user. Moreover, Bob's receiver will be equipped with a differential optical receiver to cancel the unwanted signal in the second room scenario.

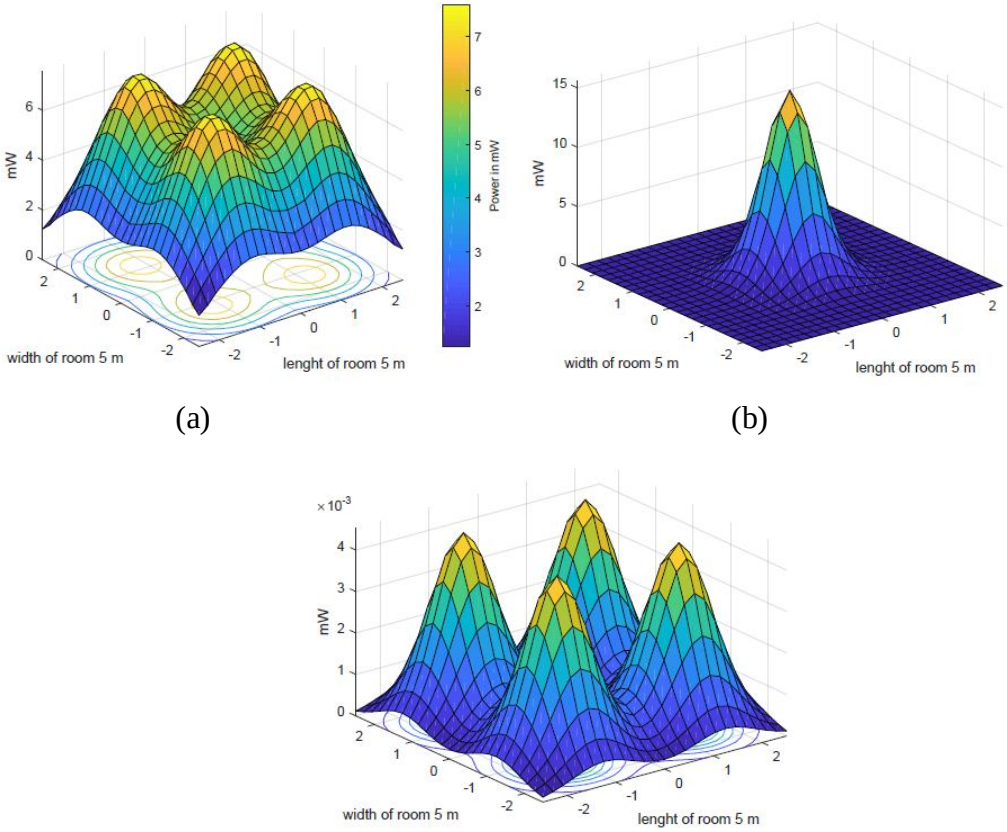


Figure 15. Received optical power distribution plane for a FWHM of (a) 35º with four APs (room 1) (b) 15º for 5th AP (user's AP in room 2), and (c) 15º for the four jamming APs in room 2.

It can be noticed that when using four APs for data transmission in room 1 with the semi angle at half power is large, 35º; the attacker can easily reconstruct the signal and decode the data with a power level around 6 mW as we previously studied in [24] Fig.15 (a).

However, in room 2, the semi angle is reduced to 15º to apply beamforming so the data is steered in the direction of Bob's receiver using the AP in the center, (Fig.15 (b)), and jamming the attacker's receiver by adding artificial noise using the other four APs (Fig.15 (c)). Therefore, compared to our previous studies in [24] a secure transmission is established by creating a protected communication zone around the user and reducing the chances for the attacker to decode the data stream as his interference level is increased. Moreover, the user's optical receiver employs a differential optical receiver which improves the dominant signal and cancels out the unwanted noise. In Fig.15 (b) the user's optical received power reached 15 mW, while the eavesdropper's received power barely reached 4 µW in Fig.15 (c).

The protected communication zone operation can be established by using the motion sensors that are currently built into energy-efficient lighting devices [87]. The AP will alert the legitimate user and stop the communication when it detects any attacker in the secured zone. Therefore, as the received power is directed in the secured zone, 1 m in diameter, the secrecy for the legitimate user is increased in the second room compared to the one in the first room. The power levels decrease as one moves away from the targeted zone so the eavesdropper can't reconstruct the data transmitted with power levels below 4 mW, as shown in Fig.15 (b).

In the SNR simulation results (Fig. 16) the spatial distribution of SNR in room 1 is shown in Fig.16 (a) when the 4 APs are used for data transmission. The SNR ranged from 85-98 dB with an average of 90 dB in most areas of room 1. However, for room 2 when a fifth AP is added and

is the only AP used for data transmission, the SNR at the corners is below 50 dB and the maximum SNR is located in the center (target zone) and exceeds 100 dB as can be seen in Fig.16 (b). Also for the eavesdropper located outside the protected zone, the artificial noise greatly affected the SNR levels, which barely reached 30 dB (Fig.16 (c)), thereby increasing the interference level of the eavesdropper. This scenario is promising since the SNR for the legitimate user is higher than that of the eavesdropper, which decreases the eavesdropper's ability to decode the legitimate data.

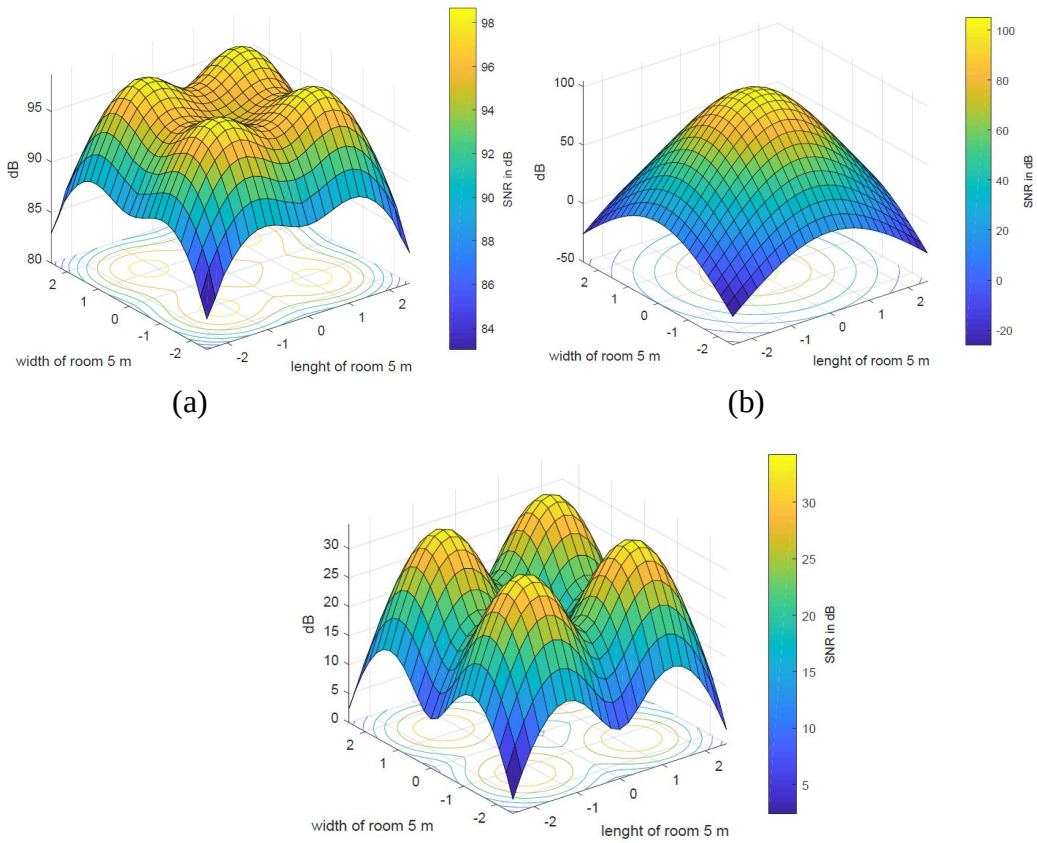
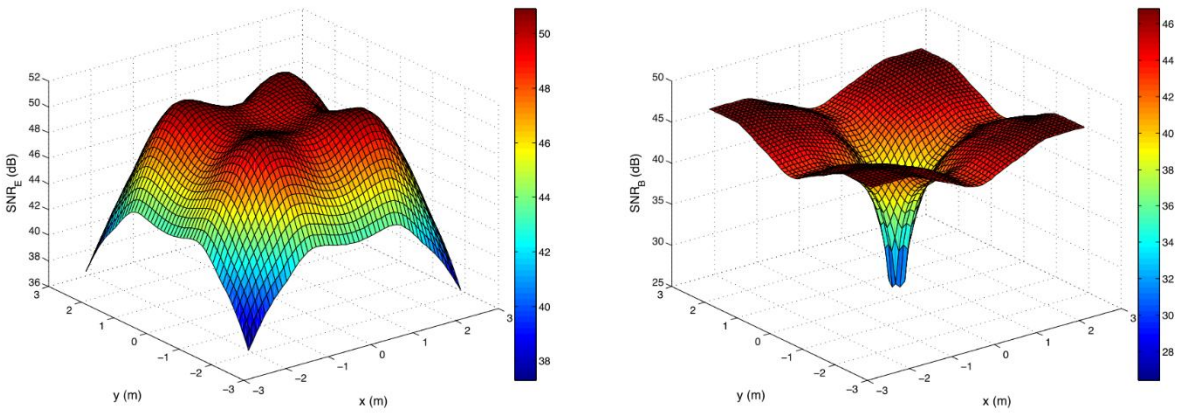


Figure 16. SNR of receiver for a FWHM of (a) 35º with four APs (room 1) (b) 15º for 5th AP (user's AP in room 2), and (c) 15º for the four jamming APs in room 2.

5.4 Previous Work

In [41], they proposed improving the confidentiality of VLC links via physical-layer security techniques. They numerically evaluated achievable secrecy rates for three typical VLC scenarios. For the SISO case, achievable secrecy rates are negligible. When beamforming is applicable at the transmitter, secrecy rates can be significantly improved via null-steering if the eavesdropper's CSI is available. With the lack of the eavesdropper's CSI, secure transmission is still possible via artificial noise transmission in the receiver's null space.



(a) (b)

Figure 17. Eve's SNR as function of Eve's location for the SISO case (a). Bob's SNR as a function of Eve's location for the MISO case with null-steering. (Bob is located at the room center) (b).

Fig. 17 (a) shows the spatial distribution of Eve's SNR within the room area when all the light fixtures are modulated by the same signal. As can be seen, Eve's SNR ranges between 37.30 dB at the room corners and 50.93 dB directly underneath any of the four fixtures with an average of 47.18 dB. Notice that Eve's SNR is higher than 43 dB in 91% of the room area. Such scenario is not promising from a security perspective since the probability that SNRE ≤ SNRB is low

making secure communication on a physical-layer basis not practical for the SISO case. Fig. 17 (b) shows Bob's SNR as a function of Eve's location when the zero-forcing beamformer is applied. It is obvious that utilizing Eve's CSI via null-steering significantly increases the achievable secrecy rate compared to the SISO case.

The work in [48] proposed a physical-layer secure coding scheme based on polar codes for indoor visible light communication wiretap channels. Results show that the secrecy capacity can be asymptotically achieved for transmitting secret information with guaranteed security and reliability. As can be seen in Fig. 18 (a), the distribution of secrecy capacity for Bob at position (0, 0) against Eve at random position is calculated as shown in Fig. 18 (b). The theoretical secrecy capacity increases versus the distance between Bob and Eve. The practical secrecy capacity achieved using the proposed coding scheme is demonstrated with several positions of Eve.

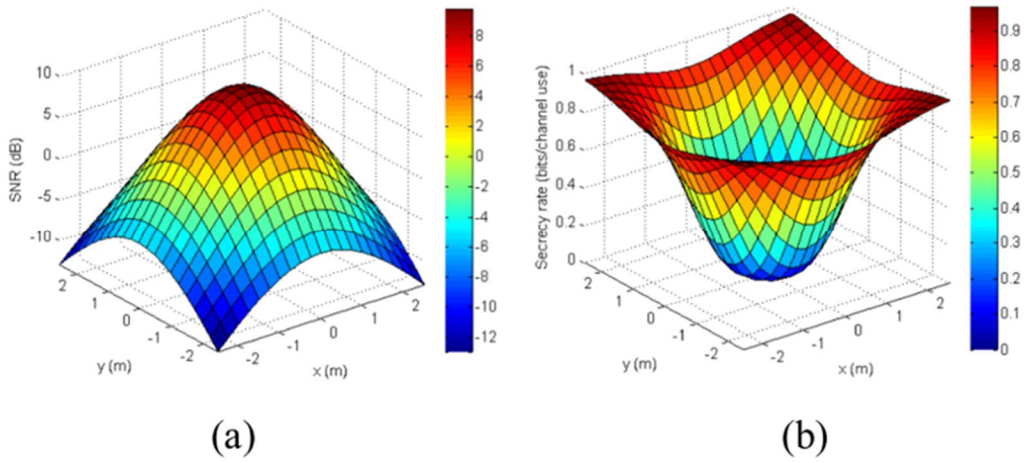


Figure 18. The distribution of (a) SNR and (b) secrecy capacity.

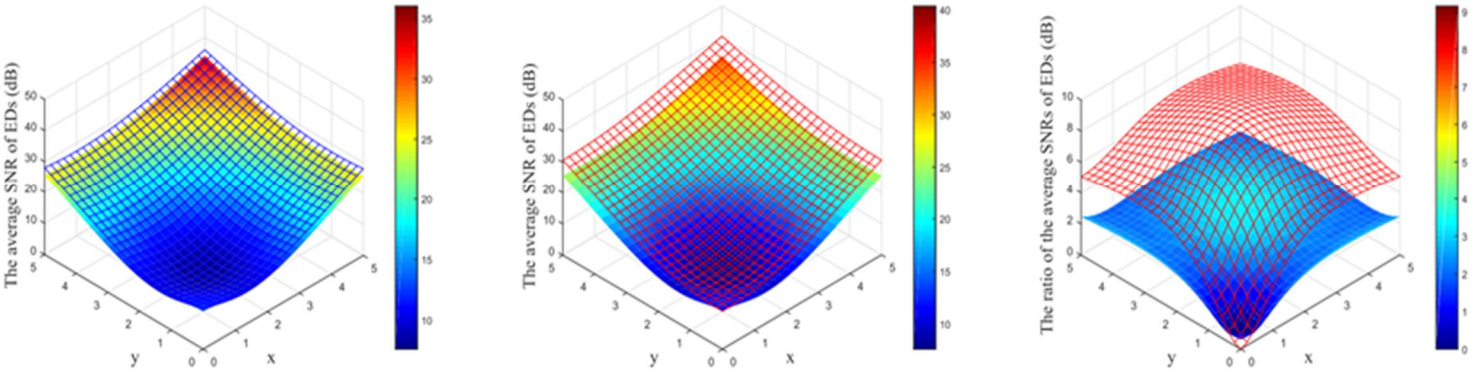


Figure 19. (a) the average SNR of EDs with beamforming and LED selection, (b) the average SNR of EDs with beamforming and repetition coding, (c) the ratio of the average SNRs of EDs generalized by beamforming.

The authors in [94] studied beamforming schemes and a simpler LED selection scheme to enhance the secrecy performance in VLC systems. Fig. 19 shows the average SNR of eavesdroppers (EDs) as a function of the User (UE) location. The bottom surfaces in (a) and (b) denote the results for the beamforming (identical). The top surfaces denote LED selection and repetition coding, respectively. In (c), the ratio of the average SNRs of EDs are given in which the top surface denotes the ratio of repetition coding and beamforming, and the bottom surface denotes the ratio of LED selection and beamforming, respectively. Four transmitters are located at (±1, ±1). By using the beamforming scheme, they can minimize the average SNR of EDs (or indeed the worst case SNR of EDs) and maximize the SNR of the UE with only statistical information about ED locations. The LED selection scheme is not superior to the beamformer in the respect of secrecy performance; however, when the UE is located near to one of the transmitters, LED selection provides a good practical solution to enhancing secrecy performance without high computational complexity.

In [98] the PLS scheme based on optical beamforming for the indoor VLC system is investigated. First, an optimization problem that maximizes the received signal power in the

security zone is formulated to make the eavesdroppers in the insecurity zone cannot receive the signal with enough power for decoding. Second, they proposed a cuckoo search with adaptive searching and population mutation (CSASPM) algorithm with two improved factors to solve the formulated optimization problem. Simulations results show that CSASPM effectively obtains the improvement of received signal power in the security zone. Fig. 20 (a) and 20 (b) show the 3D received signal power distributions obtained by the uniform beamforming weights and the proposed CSASPM, respectively.

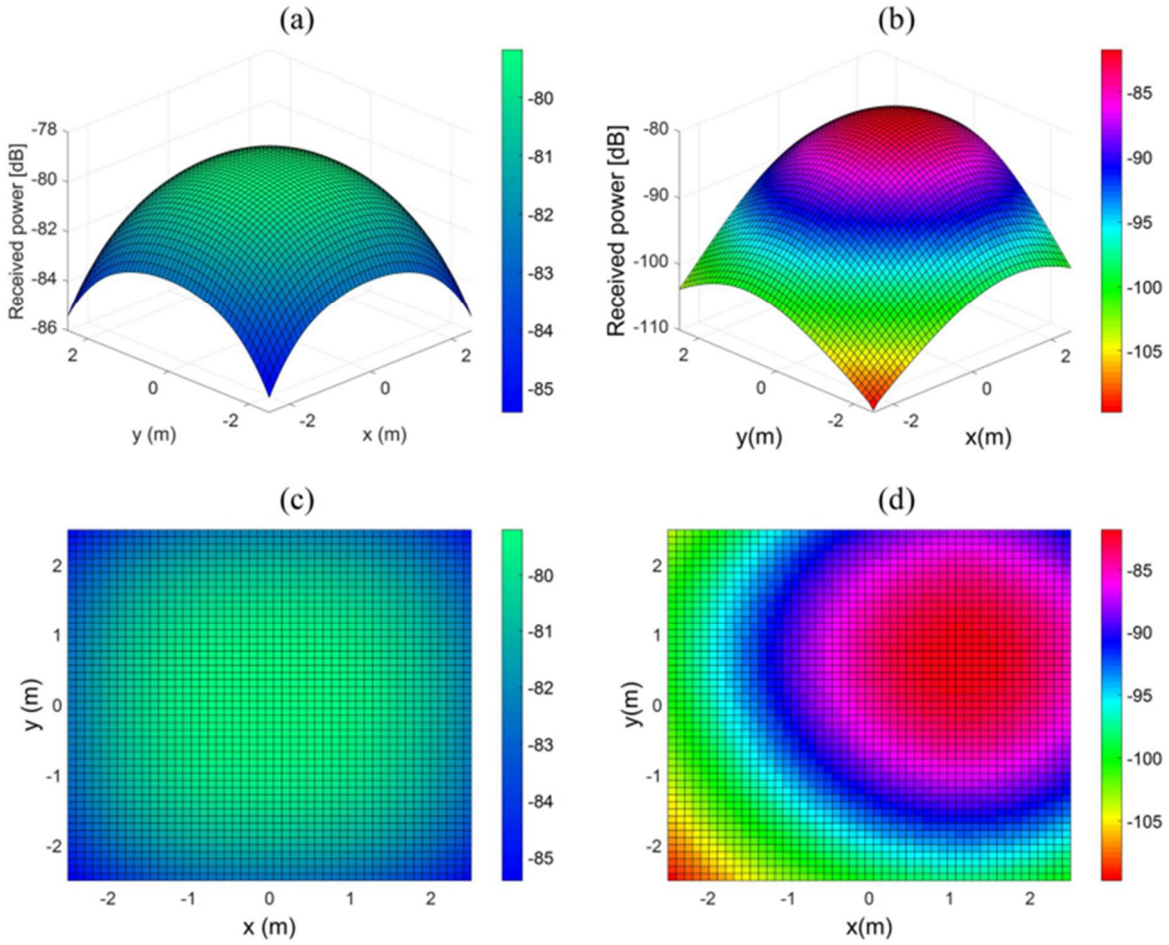


Figure 20. Received signal power distributions. (a) 3D power distributions obtained by uniform beamformers. (b) 3D power distributions obtained by CSASPM. (c) 2D power distributions obtained by uniform beamformers. (d) 2D power distributions obtained by CSASPM.

Moreover, the two dimensional (2D) forms of the received signal powers are shown in Fig. 20 (c) and 20 (d), respectively, for a more intuitive presentation. As can be seen, the received signals in the defined security zone obtained by CSASPM algorithm are much stronger than the signals in the insecurity zone, especially compared to the received signals with uniform beamformers.

CHAPTER 6

INTRAVEHICLE VISIBLE LIGHT COMMUNICATION

6.1 Introduction

Recently it was highlighted that optical wireless communication (OWC) may provide a compatible solution to the concept of intra-vehicular communications. For example irradiating the interior of the vehicle with infra-red (IR) radiation to serve as a communication link between anything from simple user-vehicular interface devices such as window or air conditioning controllers, to more advanced vehicular technologies such as audio-visual (AV) entertainment units or computer consoles [24]. The advantages to implementing an OWC system within a vehicle or Vehicle Ad-hoc Network (VANET) [106],[107] include mitigating against the highly prevalent radio frequency interference and a reduction in costs due to utilizing unregulated spectrum and not having to design a system around other competing RF systems. There is also a potential to save energy in terms of reduction in wired devices that are typically copper cabled and finally a potential to improve manufacturing efficiency should such cabling be removed.

Vehicular VLC provides lower complexity and therefore lower cost, primarily because LEDs are already installed in vehicles and street lights. Positioning technology based on VLC is more precise than RF-based ones, and the error in the order of tens centimeters. Moreover, DSRC is more exposed to longer delays, excessive packet collisions, and poor reception rate, particularly during rush hours [99]. To sustain safe and efficient traffic flow, VANET applications send Cooperative Awareness Messages (CAM) frequently. A CAM (aka Basic Safety Message (BSM) or beacon) consists of various data information like timestamp, position, speed, and heading. Since this information is broadcast publicly and these CAMs can be analyzed and collected, a serious privacy threat can happen [108].

In [27] they showed major security issues affecting VANETs which were classified into: application layer, system layer, and network layer. Also, they developed a ‘‘SecVLC’’ protocol using a hybrid communication simulation using DSRC and VLC, which reduced the effect of attacks on platoon stability. As SecVLC used to share a secret key between moving vehicles. In addition, when the platoon is attacked they suggested the utilization of adaptive cruise control (ACC) mode instead of CACC to prevent the possible collision. Since in CACC cars access each other’s information and make driving decisions autonomously.

6.2 Vehicular System Model

However, before any OWC based intra-vehicle communication system is prototyped or developed, it is typically customary for a designer to complete some form of channel analysis. Previously, researchers have designed the intra-vehicle communication channel analysis with an invisible light source, infra-red (IR), using the Phong reflection model. Furthermore, in our previous work, a visible LED, 1W of source power was used to enhance the received power and SNR [105]. It was the first kind of such an analysis to present the received power based upon a single IR LED source situated upon the ceiling of a Sports Utility Vehicle (SUV). It showed that several areas of the vehicle are illuminated with sufficient IR power, that intravehicular OWC is viable. The purpose of this study is to show how LED's allocation and positioning can improve intra-vehicle VLC performance.

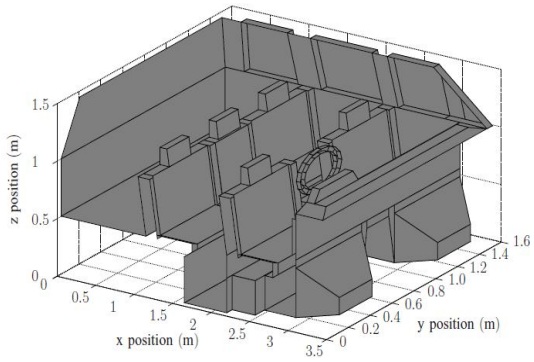


Figure 21. Front-facing view of the deployment structure [110].

For modeling, the VLC system is designed to be applied within a SUV with an internal dimension structure of 3.5×1.6×1.5 m^3 as shown in Fig. 21, with the driver side wall, windscreen and ceiling removed. Previously invisible IR LED was used in modelling of intravehicular OWC system, which resulted in the use of a strong specular IR reflection model, Phong reflection model [109]. The results showed that the rear passengers can, from the linearly scalable 1W source, achieve 49μW of received power as shown in Fig. 22 [109].

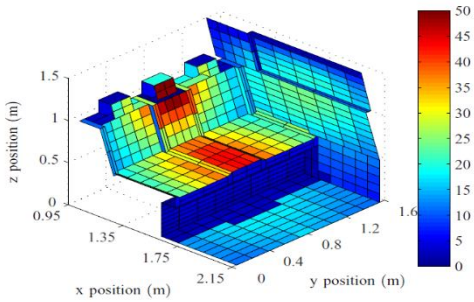


Figure 22. Received power in μW for the rear passenger seats [110].

In addition to a power up to 16μW can be received on the headrests of the front seats, where there might be audio visual (AV) entertainment units and computer consoles installed as shown in Fig. 23 [109].

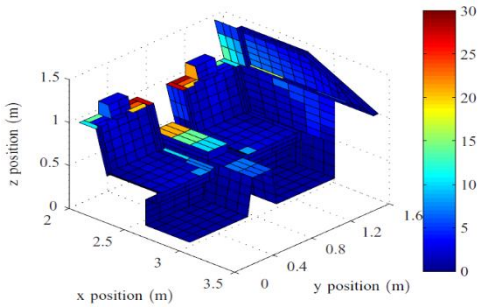


Figure 23. Received power in μW for the front passenger seats [110].

In our previous paper [105], the received power level and SNR are improved by changing the FWHM of a visible LED source by utilizing the Lambertian radiant intensity model. The position vector of the transmitter source is located centrally upon the vehicle ceiling [1.6, 0.8, 1.5].

The received optical power distribution and SNR simulation results developed based on the equations in chapter 3, prove that the proposed model power distribution received for the rear and front seats improved to 7 mW and 8 mW, respectively as shown in Fig. 24. The power level results validate that the use of visible source with the optimized characteristics is 100 times more than that of the IR LED. Using IR radiation before, the lower section of the back seat is exposed to a power ranging between 19μW and 43 μW rather than 4 mW to 7 mW. Users can comfortably exploit personal electronic devices such as mobile phones, laptops, hand-held computer consoles, etc. in these locations.

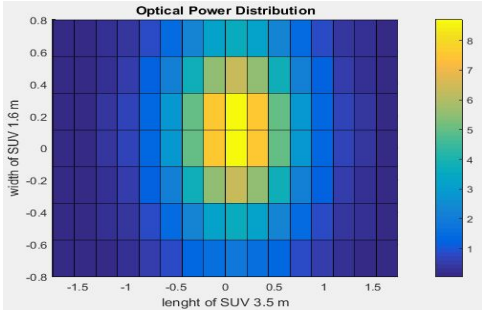


Figure 24. Optimized received power in mW for the rear and front passenger seats [106].

This work pursues our research goals in designing and modeling an efficient and practical intra-vehicle VLC system, where we have tested and analyzed the channel estimation for an intra-vehicle VLC system [105], studied and enhanced the secrecy performance in an indoor multiuser VLC network [105]. The aim of this study is to optimize the LED's positioning and allocation in an intra-vehicle VLC system and notice how they affect the system design and performance.

6.3 Intra-Vehicle LEDs Locations Analysis

In this section, we have used MATLAB to simulate and analyze the effect of different number of LED's position on the received power, which directly affects the system performance.

A. Two Sources of Power

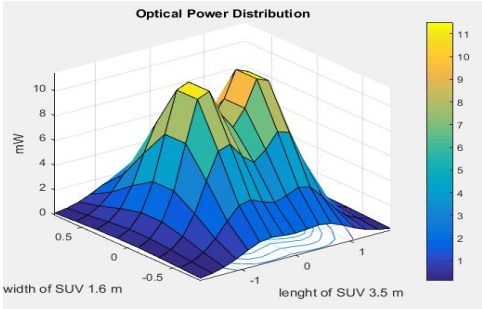


Figure 25. Two LED received power in mW for the rear and front passenger seats.

We have deployed two LED arrays with the number of LEDs per array = 50 to supply 2 W of source power. The received optical power distribution and SNR simulation results are formulated upon the parameters in Table 7 and the equations in chapter 3. Along with using the

SUV dimensions in section 5.2. As can be seen from Fig. 25, the power distribution received for the rear and front seats improved to 11 mW, compared to the 7 mW and 8 mW received respectively by applying one source of power. The power level results prove that the use of two visible sources with the optimized characteristics used in the previous model is enhanced more than that of the previous system. As the minimum power level around the passenger and driver seats is not less than 7 mW, unlike the 4 mW received in the previous model.

Table 7. Intra-Vehicle Simulation Parameters

System Parameters for a VLC Link		
Vehicle	Size	3.5×1.6×1.5 m^3
Source	Location (2 LEDs)	(1.25,0.8,1.5) (2.25,0.8,1.5)
	Semi angle at half power (FWHM)	30º
	Transmitted power (Per LED)	20mW
	Number of LEDs per array	50
	Center luminous intensity	300-910 lx
Receiver	Receive Plane above the floor	0.5 m
	Active area (A_{rx})	1 cm2
	FOV	70º
	Amplifier Bandwidth B_a	50 MHz
	Concentrator Gain g	6.0
	Photodiode responsivity r	0.4 A/W
	Optical filter's transmission coefficient T	1.0

The received power shown in Fig. 25 near the passenger's head throughout the rear passenger seats and front seats have high power which is suitable for wireless IR headphones or hands-free voice equipment and any portable devices. Also, the lower section of the back seat has 7 mW of power where mobile phones, laptops, or other personal electronic devices can comfortably be used in these locations. Simple vehicular-passenger interface panels; window,

air-conditioning, heating or AV controllers are easily applicable as the received power ranges from 3 mW to 5 mW. The SNR out got also enhanced by using two sources of power. A 67~ 97.2 dB is obtained, as shown in Fig. 26, validating the advantages of the VLC intra-vehicle proposed model. As the utilization of two sources enhanced the discovered results of SNR.

B. Three Sources of Power

The problem with the previous layout was that the maximum received power within the vehicle was concentrated around the center as a result of the combined power of the two LED sources.

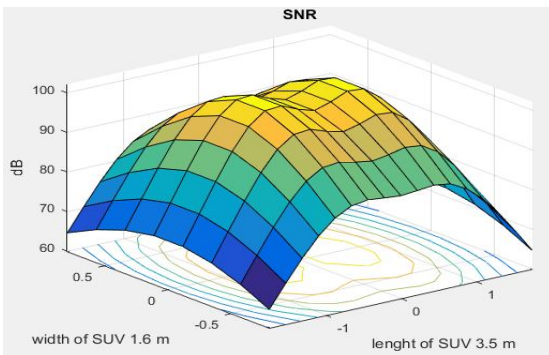


Figure 26. SNR of the receiver.

To improve this power gap, a three LED layout was used to move the previous two sources further away from the center while adding one source in the middle for the front seats. As for the rear passenger seats will be served by two separate sources of power. After applying different layouts for several simulations, the results showed that the optimal locations for the three sources are (2.75, 1, 1.5), (0.75, 1, 1.5) for the rear seats and (1.75, 0.6, 1.5) in the middle for the front seats.

6.4 Simulation Results Discussion and Summary

It is clear from Fig. 25 that the corners of the vehicle are the darkest areas. Even though the probability of having a receiver at the absolute corner is almost zero, the received power levels

of the system need to be at an acceptable level for the rear passengers and any simple vehicular-passenger interface application. As can be seen from Fig. 27, there is a minor increase in the maximum power compared to the two source layout 14mW instead of 11 mW, however, the minimum power levels at the sides and near the corners increased from 4 mW to 8 mW approximately. The received power throughout the rear passenger seats and front seats have high power which is suitable for any portable devices.

Also in Fig. 28, the minimum SNR level near the corner reached 80 dB instead of 70 dB in the previous layout while maintaining the same maximum level of 100 dB. Moreover, the SNR has a direct effect on the performance of the VLC system. Since the probability of error for an On-Off Keying modulation scheme is given by:

$$p(e) = Q(\sqrt{SNR}) \tag{5.1}$$

which shows that the layout design of LEDs is an important factor while designing a VLC system.

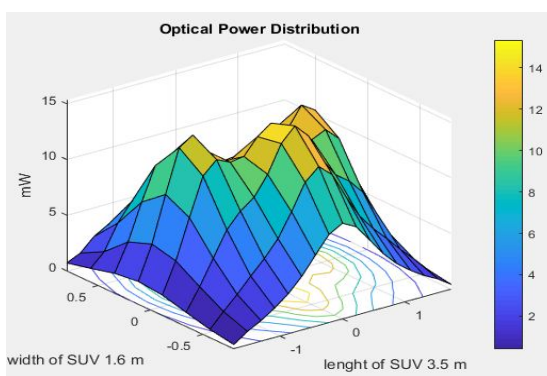


Figure 27. Three LEDs received power in mW for the rear and front passenger seats.

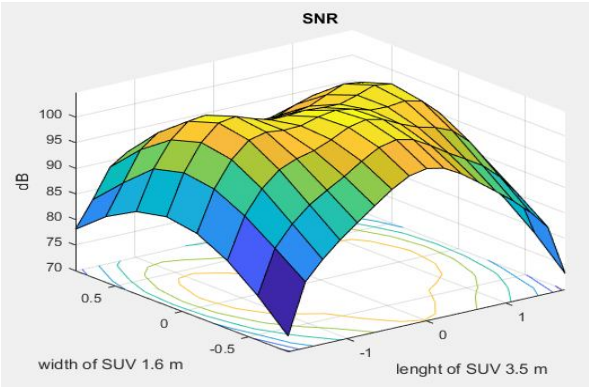


Figure 28. The SNR of receiver for the rear and front passenger seats.

The results show that choosing the LED's locations and numbers are necessary to determine the amount of the received power within the designated area, which directly affects the SNR and probability of error.

CHAPTER 7

OUTDOOR VEHICULAR VISIBLE LIGHT COMMUNICATION SECURITY

7.1 Introduction

Currently, V2V is an area of excessive research but for industry, security is not the prime focus of research [65].VANETs systems as seen in Fig. 29 are susceptible to different attacks such as replay attack and packet falsification. Firstly, the attacker in the replay attack pretends to be a legitimate user and eavesdrops and saves the packet's information that is previously transmitted by users. Afterward, it deceives the platoon users and retransmits the packets as if they are just created. This corrupts the system stability because those packets have out-of-date information. Secondly, in packet falsification, the intruder acts as a platoon leader and listens to the communication channel among vehicles constantly. As soon as a packet is received, it retransmits it while changing the information. Also, the adversary uses an automotive diagnostic tool to evaluate the data packet's information as shown in a modern automobile experimental security analysis [110]. For example, an attacker can alternate the speed of platoon which may cause an accident.

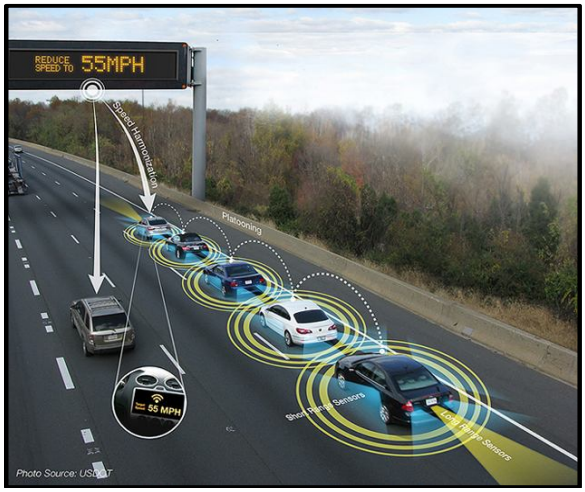


Figure 29. Demonstration of Intelligent transportation system.

Privacy schemes in VANET depend basically on changing pseudonyms frequently in a hidden mix-contexts to avoid likability of CAMs. Unobserved mix-contexts are performed by applying a silent period before a pseudonym change. Changing pseudonyms without using unobserved mix-contexts will not restrict vehicle tracking [111]. Summary of different privacy and safety schemes are shown in Table 8.

VLC can mitigate the threats by utilizing the impermeability and directivity of LEDs. On the other hand, applying VLC only in the platoon may disturb the stability of platoon because the surroundings affect VLC [112]. Seyhan Ucar in [112] proposed SP-VLC, an IEEE 802.11p

Table 8. V2V VLC Secrecy Enhancement Techniques

Paper	Method
Amoozadeh [113]	Used a physical layer secret key generation technique to exploit randomness of the road surface and the driving behavior, 128bits encryption key is generated based on real world vehicle trajectory big-data to prove the concept.
Freudiger [114]	Proposed the use of VLC for vehicle safety applications, creating a smart automotive lighting system. The system provides an all-in-one low-complexity and low-cost solution.
Blinowski [99]	Presented an implementation of secure V2V communication by using Blockchain as a V2V message transport, since it provides a secure, verifiable, shared, open and distributed ledger.
Yu [48]	Developed MixGroup to change pseudonym by efficiently using the sparse meeting chances among vehicles.
Lefèvre [115]	Proposed an intersection collision avoidance (ICA) system and studied a silent period method in terms of missed and avoided collisions and showed that the ICA system with silent periods can work in less than two seconds.
Agarwal [99][116]	Developed and proposed a hybrid communication V2V system using DSRC and VLC to reduce the effect of attacks and provide secure platoon maneuvers. The results proved a detection rate below 10%.

communication protocol, and VLC-based hybrid security system, intending to provide secure platoon maneuvers and stability and secure platoon maneuvers under different data packet attacks like channel overhearing, injection, jamming, and maneuver attacks. He also showed a maneuver attack based on different scenes identification where a malicious actor sends a fake packet. SP-VLC can switch to VLC only and secure platoon maneuvering by using the secret key establishment, jamming detection, message authentication, and data transmission. The results compared the eavesdroppers' decoding rate for packets transmitted via DSRC, VLC and SecVLC as a function of vehicle distance. The adversary using DSRC achieves a detection rate near 100% within 300 m of the transmitting vehicle. While using VLC the adversary receiver is limited by the direct link of VLC however, the eavesdropper still has a 70% detection rate when located within 6 m. The results provided that the detection rate is limited below 10% [65].

However, there are only a few security-related studies on vehicular VLC. Thus, this chapter focuses on the secrecy performance in an outdoor V2V VLC network using the Lambertian radiant intensity VLC channel analysis properties, by enhancing the received optical power in an outdoor V2V VLC network and analyzing the hybrid V2V VLC for LOS and diffused channel model. To achieve the optimal V2V VLC link for urban environments, the proposed platform will depend on the received optical power, SNR, and BER to improve the secrecy performance by achieving better SNR for the legitimate platoon member than the adversary, to ensure platoon stability and to limit the detection of any adversary. Also, we will improve the secrecy performance for legitimate platoon member by changing the LED semi-angle and implementing the protected zone strategy between the platoon members where intruders are banned to help improve the secrecy.

7.2 V2V VLC System Model

The Communication diagram for V2V VLC transmission model is shown in Fig. 30. Using non-return-to-zero (NRZ) on-off keying (OOK) to modulate the signal, which will be demodulated and decoded to recover the original data. To simulate VLC in practical driving scenarios, we designed 1.6 meters for the car width, a common car size, and the receiver is installed on the bumper of the front car 0.8 meters above the floor level with a field of view (FOV) of 55 º, as shown in Fig. 30. Also on the transmitter side, the following car has the LED headlamps fixed 0.8 meters above the floor with an inter-distance of 1.2 meters. Today most of the LEDs in the market are surface-emitting LEDs, which has the intensity directly proportional to the cosine of the angle from which it is received, as it follows Lambert's cosine law [66]. Therefore the horizontal plane of the received optical power distribution follows a Lambertian radiation pattern and the simulation parameters are shown in Table 9. The VLC link range for vehicular system depends on the adjacent vehicle's position and the half-power angle $\emptyset_{\frac{1}{2}}$ of the LED, which is the angle where the effective transmission power is half of the maximum power.

A. LOS Channel Analysis

The white LED light source directed to the optical receiver has a LOS channel transfer function as shown in chapter 3. The PD on each vehicle is facing the headlights with a FOV ofφ_c.

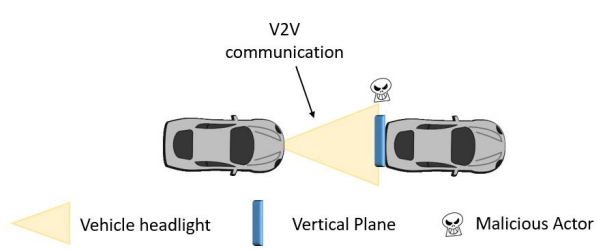


Figure 30. V2V communication Architecture using two vehicles.

Table 9. V2V VLV Simulation Parameters

System Parameters for a VLC Link		
Vehicle	Size	1.6×4.7×2 m^3
Source	Location (2 LEDs)	(0.25,0,0.8), (1.45,0,0.8)
	Number of LEDs per array	50*50 (2500)
	Transmitted power (Per LED)	20 mW
	Semi-angle at half power (FWHM)	10º
Receiver	FOV	55º
	Active area (A_{rx})	1 cm2
	Receive Plane above the floor	0.8 m
	Amplifier Bandwidth B_a	50 MHz
	Ambient noise power P_n	19.272 μW
	Photodiode responsivity r	0.4 A/W
	Amplifier noise density i_{am}	$5\ pA/\sqrt{Hz}$
	Concentrator Gain g	6.0
	Noise bandwidth factor I_1	0.562
	Optical filter's transmission coefficient T	1.0

We can drive the LOS total received power by (3.4). As a consequence the LOS received power is shown as in (3.5).

B. Diffuse Channel Analysis

The reflections resulting from the surrounding cars and road medium cause V2V VLC multipath propagation which don't observably impact the performance [117]. Therefore, in this study, we will investigate the diffuse reflection; in the Lambertian model, we can ignore the ground reflection and only consider the ambient noise and road reflections impacts. Modulating the signal with a chosen frequency allows us to filter out most ambient interferences as mentioned before to prevent saturating the PD.

For the diffused reflection, the Light reflection intensity [118],[116] is calculated in (6.1):

$$I = \frac{P_{LEDs}}{A} \rho \ , \tag{6.1}$$

where P_{LEDs} are LED's total power, A is the area of the reflecting surface, ρ is the reflectivity of surfaces. The received power of the diffused channel can be derived as:

$$P_{diff} = \mathrm{A} \times I \ , \tag{6.2}$$

In this case, the total received power in Eqn (3.5) is changed to:

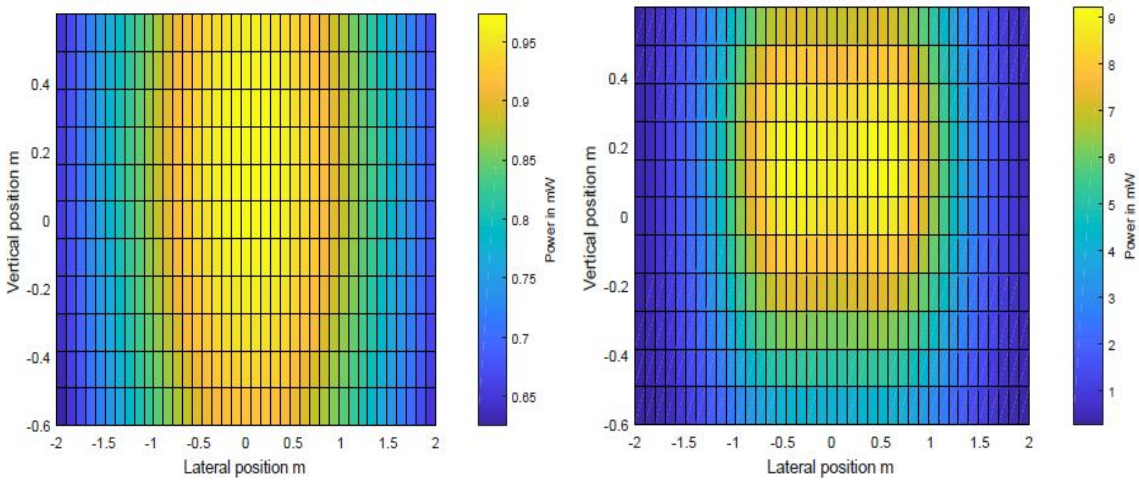
$$P_{re} = (P_{LOS} + P_{diff}) \times g \times T \ . \tag{6.3}$$

7.3 V2V Model Simulation Results

The simulation validated our proposed model by using MATLAB. Two normal vehicles are designed with a size of 1.6×4.7×2 m^3, the V2V VLC system parameters used for simulation setup are described in Table 9. Here, we consider the scenarios in two dominant conditions: traffic mode and stop mode. Based on USDOT reports, the minimal distance between two following

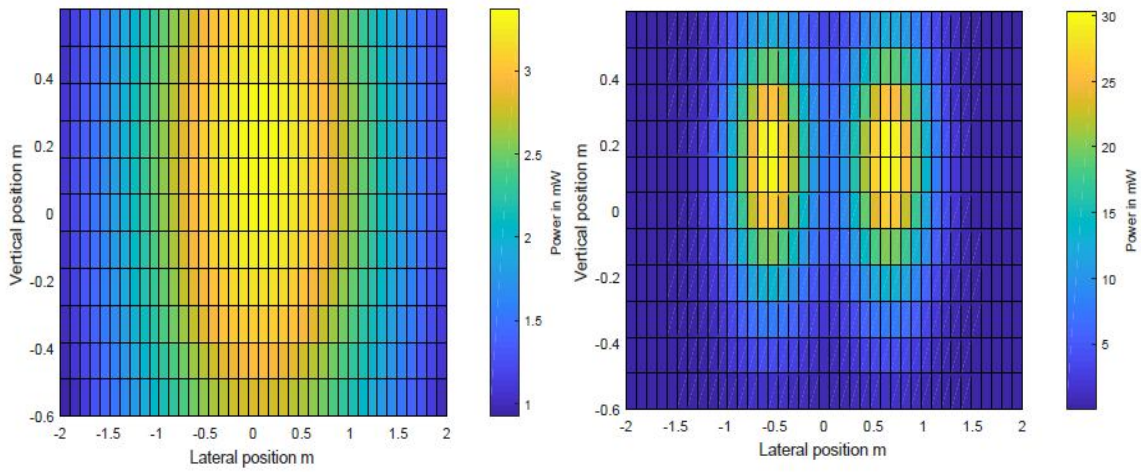
vehicles is 2 m and the average gap between vehicles in traffic mode is 8 m for urban environments at vehicle speeds less than 100Km/h [113]. Also, the simulation shows that the distance and the semi-angle at half power of LED are the two dominant factors affecting the received power. Since the LED bulbs in the headlights are used for communication and illumination, the LED luminance range should be moderate to meet the specific requirements outlined by the Federal Motor Vehicle Safety Standards (FMVSS) of US, 60 Watt maximum for low beam and 70 Watt maximum for high beam, to avoid disturbing the nearby drivers.

Therefore, the simulation results are shown at two different distances: 2 m, 8 m; and the semi angle at half power is adjusted to 10 º instead of 20 º for a slightly focused communication link for a low beam LED. When the semi angle at half power is increased to 20 º, with a gap distance of 8 m, the distribution of the received optical power at a vertical plane reached a maximum of 0.95 mW. However, when reducing the gap to 2 m, the received optical power exceeded 9 mW at the PD receiver's position, as shown in Fig. 31(a, b), respectively.



(a) (b)

Figure 31. Received Optical power distribution of the headlights (projected on a vertical plane) for a FWHM of 20 º (a) traffic mode and (b) stop mode.

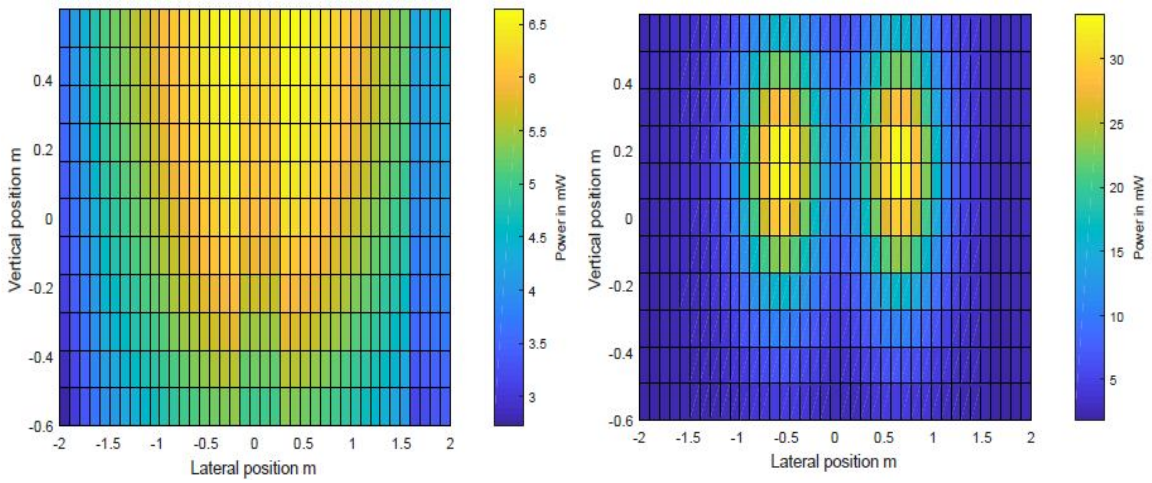


(a) (b)

Figure 32. Received Optical power distribution of the headlights (projected on a vertical plane) for a FWHM of 10 º (a) traffic mode and (b) stop mode.

The zone around the receiver's position has a highly concentrated received power which decreases in the areas away from the targeted zone. On the other hand, Fig. 32 (a,b) shows when the semi angle at half power is reduced to 10 º; with a gap of 8 m, the received optical power distribution achieved almost 3.5 mW of power at the vertical plane and 30 mW with a gap distance of 2 m, respectively.

As a result, adjusting the semi angle at half power of LED improved the V2V VLC system communication link and can enable a wider range of stable and robust V2V link. Fig. 33 (a,b) shows the hybrid received optical power simulation results for both the traffic mode and stop mode respectively, with considering LOS channel and diffused channel simultaneously. Therefore, the traffic mode received power is almost doubled and the received power in the stop/following mode almost achieved 40 mW, which assures the certainty of considering the diffused channel in the V2V VLC systems.



(a) (b)

Figure 33. Hybrid Received Optical power distribution of the headlights (projected on a vertical plane) for a FWHM of 10 º (a) traffic mode and (b) stop mode.

7.4 Vehicular VLC Security

In V2V VLC, a platoon has a leader that manages the system and platoon followers to follow the leader by controlling the speed. Platoon management protocols aim to keep the system stable and to platooning maneuvers such as entrance, merge, leave and split. Most of the previous studies assumed the presence of secure communication among vehicles while designing platoon management protocols. However, the absence of security protocol results in system instability. The goal in this section is to analyze the secrecy performance in a V2V VLC network to ensure stability and maneuvers security against maneuver attacks, data packet injection, eavesdropping, and jamming. In this security model, we will improve the secrecy performance for legitimate platoon member by changing the semi-angle of LED and by using the protected lane between vehicles.

The “protected zone” strategy [119] alerts the platoon leader and legitimate platoon members when a malicious actor is detected in the protected zone and temporarily stop the communication. A secrecy V2V VLC protected zone is efficiently utilized by built-in motion

sensors in vehicles and can be defined by the lateral range of the typical lane width, 3.6 meters [120]. To raise the secrecy performance, the legitimate platoon member has to achieve better SNR than the adversary [101]. By applying the parameters in Table 9, the simulation results for the SNR and BER analysis with a semi angle of 7°, for both scenarios, traffic mode and stop mode, are shown in Fig. 34 and 35. The SNR is derived in chapter 3. Moreover, the SNR has a direct effect on the performance of the VLC system, since the probability of error for an On-Off Keying modulation scheme is given by:

$$p(e) = Q(\sqrt{SNR}) \ . \tag{6.4}$$

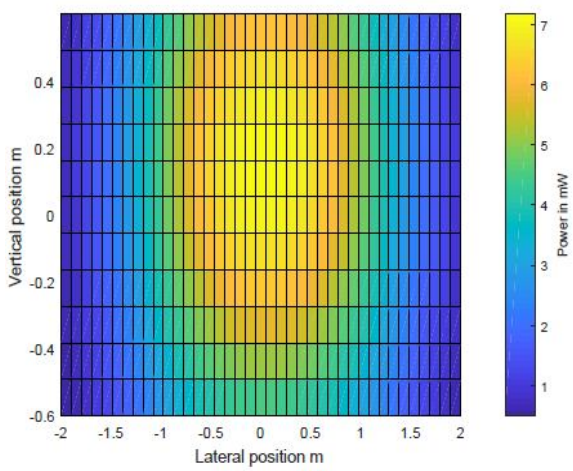


Figure 34. Received Optical power distribution of the headlights in traffic mode when projected on a vertical plane for a FWHM of 7 º.

7.5 Simulation Results Discussion and Summary

At first, when we examined the traffic mode for the legitimate platoon member following the platoon leader and the space gap is 8 m; we found that it is easier for the malicious actor to cause system instability. Therefore, it can damage membership by applying data packet injection, eavesdrop, and jam the communication link. As shown in the vertical plane view Fig. 31(a), when the semi angle at half power is large, 20°, the secrecy at the legitimate platoon member can

efficiently be reduced. As the received optical power reached a maximum of 1 mW which will result in poor SNR results. However, when the semi angle is reduced to 7°, it can be noticed that there is an obvious increase in the secrecy performance, as shown in the vertical plane view Fig. 34. As a received power of 7 mW is extremely centered and directed in the protected lane between the platoon members, and it decreases as long as you move away from the specified zone, so eavesdroppers can't reconstruct the signal with power levels lower the 4 mW. Therefore using both mechanisms, reducing the semi angle at half power of the LED and applying the protected zone strategy in the V2V VLC system, will result in platoon member privacy and secrecy improvement and will ensure secure platoon maneuvering in V2V VLC networks.

While when we consider the stop mode scenario, with a space gap of 2 m, the communication link is normally directed towards the leading vehicle. As a result, we can only apply the protected zone strategy to ensure privacy and secrecy.

Moreover, when the semi half-angle in the traffic mode is decreased from 20° to 7° and by applying the protected zone strategy; the SNR within the protected lane region increased from 80 dB to 96 dB while keeping the SNR below 78 dB outside the protected zone, as shown in Fig. 35 (a) and (b). Also in the stop mode with a semi half angle of 7°, the SNR for the legitimate platoon user exceeded 100 dB while the SNR for any malicious actor is below -60 dB. The results approve that the privacy and secrecy of the users in a V2V VLC network are defiantly improved when decreasing the semi half-angle. As it presents an obvious reduction in the attacker SNR levels outside the protected lane and rather rising the legitimate user SNR levels and therefore the BER will improve as shown in equation (6.4).

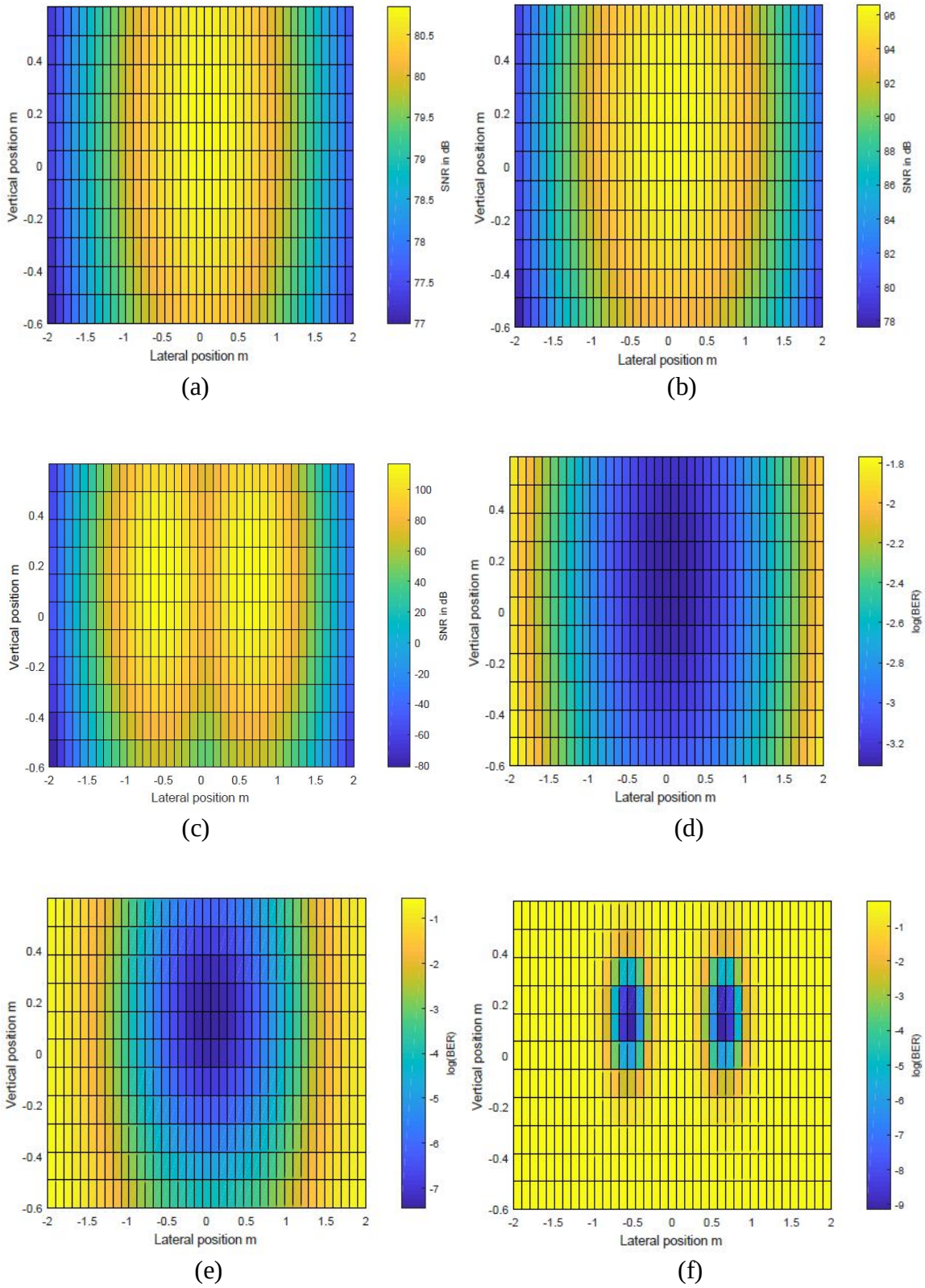


Figure 35. SNR and BER of the receiver (projected on a vertical plane) for a traffic mode with (a, d) a FWHM of 20 º, (b, e) a FWHM of 7 º and (c, f) for stop mode with a FWHM of 7 º.

Fig. 35 (d), (e), and (f) show the simulated bit error rate (BER) for V2V VLC communication based on the model described in section 6.2. Fig. 35 (d) shows BER < 10^{-2} in the protected zone while Fig. 35 (e) shows BER < 10^{-4} after decreasing the semi half-angle to 7°, leaving the BER > 10^{-1} outside the targeted zone as there is a weak signal reception. In case of the stop mode with a semi half-angle of 7°, the BER for the platoon member is below 10^{-5}.

CHAPTER 8

CONCLUSION

In this thesis, we have presented the key concepts, underlying principles of 5G physical-layer threats and solutions in the new 5G network. In particular, visible light communication as one of the main PLS solutions in 5G IoT networks and explored the VLC security threats for the indoor and vehicular applications. Several methods were used and studied to modify the SNR and power distribution levels for the legitimate user and weaken the malicious signals.

In chapter 4, a new VLC model was proposed for indoor environments that enhances the security in VLC technologies. We implemented six APs rather than four in a typical 5×5×3 m^3 multiuser VLC network (office) which are cooperated. Then we reduced the semi-angle of LED to 15° instead of 35° to further help improve the secrecy performance by directing the power in the specified zone for the legitimate user. Finally analyzed the SNR along with performing the protected zone around the AP where eavesdroppers are restricted to strengthen the legitimate user signal and weaken the other signals outside the protected zone. As the eavesdropper signal strength dropped from 95 dB to 75 dB, validating our work and improvement to the network secrecy performance

Chapter 5 provided a physical-layer secure model for indoor visible light communication systems. The proposal was based on VLC beamforming and generating artificial noise to enhance the secrecy performance in the VLC system with significant gains of SNR compared to the work in chapter 4. First, we steered the transmitted data to create a secure communication zone by decreasing the semi-half angle of the LED. Then we added artificial noise to the wiretap channel to jam the attacker. Finally, the legitimate user employed the differential receiver to cancel out any unwanted signal and strengthen the legitimate signal. The simulation results showed that the

secrecy performance significantly increased as the user's SNR exceeded 100 dB while the malicious user's SNR barely reached 30 dB outside the target zone, which increased his interference level. Also the legitimate user's optical received power reached 15 mW while the eavesdropper's received power barely reached 4 µW, therefore the eavesdropper can't reconstruct the data transmitted.

Chapter 6 studied the effect of LEDs position for an intravehicular scenario on the performance of a visible light communication system. The results showed that choosing the LED's locations and numbers are necessary to determine the amount of the received power within the designated area, which directly affects the SNR and probability of error.

In chapter 7, we presented an enhanced V2V VLC model for outdoor vehicular communication that improves the received power distribution and security in V2V VLC system. We have created a realistic driving scenario with two typical cars of size 1.6×4.7×2 m3 in a V2V VLC network. Then we changed the LED semi-angle to 10 degrees rather than 20 degrees to improve more the received power, and by targeting a specific area to direct the power for the legitimate platoon member and using a semi-angle of 7 degrees, the secrecy showed better performance. Moreover, applied the protected lane where attackers are banned and evaluated the SNR and the BER. The intruder signal strength dropped to 78 dB and -60 dB with BER > 10--1 while the signal strength for the legitimate vehicle reached 96 dB and 100 dB with BER< 10-4 and can reach 10-7 for both traffic mode and stop mode respectively.

In the future, VLC can work as a complementary technology to the RF 5.9 GHz DSRC technology in vehicular wireless communication as each of them is suitable for a scenario when the other is vulnerable. And human health is important and more studies on visible light effect using VLC on human safety are encouraged as done on RF technology. This thesis emphasizes that VLC is a promising way of communication. There are numerous approaches that can be used in real time applications which will renovate the present and future living styles.

To the best of our knowledge, light polarization and security are a new concern in VLC and there has been no work done yet in this area. However, the VLC system can use light polarization as an alternative method to transmit data, as data polarization has been used to encode data or hidden data. Polarization depends mainly on LOS communication rather than non-LOS, or reflected signal, which decreases the polarization factor. As a result, it is not easy to eavesdrop on polarized signals or apply any other attack to change or jam them. In the future, light polarization can play an important role in VLC physical layer security.

REFERENCES

[1] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 100–107, 2004, doi: 10.1109/TCE.2004.1277847.

[2] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?," *J. Light. Technol.*, vol. 34, no. 6, pp. 1533–1544, 2016, doi: 10.1109/JLT.2015.2510021.

[3] D. A. Basnayaka and H. Haas, "Hybrid RF and VLC systems: Improving user data rate performance of VLC systems," in *IEEE Vehicular Technology Conference*, 2015, vol. 2015, doi: 10.1109/VTCSpring.2015.7145863.

[4] R. Shaaban and S. Faruque, "A survey of indoor visible light communication power distribution and color shift keying transmission," in *IEEE International Conference on Electro Information Technology*, 2017, pp. 149–153, doi: 10.1109/EIT.2017.8053347.

[5] IEEE Computer Society, "IEEE Standard for Local and metropolitan area networks - Part 15.7: Short-Range Wireless Optical Communication Using Visible Light," *IEEE Std 802.15.7-2011*, vol. 1, no. September, pp. 1–286, 2011, doi: 10.1109/IEEESTD.2011.6016195.

[6] R. J. Green, H. Joshi, M. D. Higgins, and M. S. Leeson, "Recent developments in indoor optical wireless systems," *IET Commun.*, 2008, doi: 10.1049/iet-com:20060475.

[7] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, 2016, doi: 10.1016/j.phycom.2015.10.006.

[8] S. P. Bendale and J. Rajesh Prasad, "Security Threats and Challenges in Future Mobile Wireless Networks," 2019, doi: 10.1109/GCWCN.2018.8668635.

[9] S. Kaneriya, J. Vora, S. Tanwar, and S. Tyagi, "Standardising the use of duplex channels in 5G-WiFi networking for ambient assisted living," 2019, doi: 10.1109/ICCW.2019.8757145.

[10] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile internet and its applications in 5G era: A comprehensive review," *Int. J. Commun. Syst.*, 2019, doi: 10.1002/dac.3981.

[11] R. J. Green and S. Member, "Optical Wireless with Application in Automotives," in *ICTON*, 2010, pp. 1–4.

[12] L. Penubaku and K. Lakshmishree, "A survey on different techniques used for visible light communication," 2016, doi: 10.1109/ICATCCT.2015.7456988.

[13] J. M. Kahn, “Wireless infrared communications,” *Proc. IEEE*, vol. 85, no. 2, pp. 265–298, 1997, doi: 10.1109/5.554222.

[14] P. J. Winzer and D. T. Neilson, “From Scaling Disparities to Integrated Parallelism: A Decathlon for a Decade,” *J. Light. Technol.*, 2017, doi: 10.1109/JLT.2017.2662082.

[15] M. Yang *et al.*, “Mobile phone use and glioma risk: A systematic review and meta-analysis,” *PLoS One*, vol. 12, no. 5, p. e0175136, May 2017, doi: 10.1371/journal.pone.0175136.

[16] M. Röösli, S. Lagorio, M. J. Schoemaker, J. Schüz, and M. Feychting, “Brain and Salivary Gland Tumors and Mobile Phone Use: Evaluating the Evidence from Various Epidemiological Study Designs,” *Annu. Rev. Public Health*, 2019, doi: 10.1146/annurev-publhealth-040218-044037.

[17] D. Tsonev, S. Videv, and H. Haas, “Towards a 100 Gb/s visible light wireless access network,” *Opt. Express*, 2015, doi: 10.1364/OE.23.001627.

[18] M. Ayyash *et al.*, “Coexistence of WiFi and LiFi toward 5G: Concepts, opportunities, and challenges,” *IEEE Commun. Mag.*, 2016, doi: 10.1109/MCOM.2016.7402263.

[19] A. Mostafa and L. Lampe, “Enhancing the security of VLC links: Physical-layer approaches,” in *2015 IEEE Summer Topicals Meeting Series, SUM 2015*, 2015, pp. 39–40, doi: 10.1109/PHOSST.2015.7248182.

[20] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey,” *IEEE Commun. Surv. Tutorials*, 2019, doi: 10.1109/COMST.2018.2878035.

[21] E. Udvary, “Visible light communication survey,” *Infocommunications J.*, 2019, doi: 10.1201/9781315151724-8.

[22] H. Le Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, “Secured communications-zone multiple input multiple output visible light communications,” 2014, doi: 10.1109/GLOCOMW.2014.7063482.

[23] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, “On the secrecy capacity of MISO visible light communication channels,” 2016, doi: 10.1109/GLOCOM.2016.7842062.

[24] R. Shaaban, P. Ranganathan, and S. Faruque, “Visible light communication security vulnerabilities in multiuser network: power distribution and signal to noise ratio analysis,” in *Lecture Notes in Networks and Systems*, 2020.

[25] L. Yin and H. Haas, “Physical-Layer Security in Multiuser Visible Light Communication Networks,” *IEEE J. Sel. Areas Commun.*, 2018, doi: 10.1109/JSAC.2017.2774429.

[26] T. Yamazato *et al.*, “Image-sensor-based visible light communication for automotive applications,” *IEEE Commun. Mag.*, 2014, doi: 10.1109/MCOM.2014.6852088.

[27] S. Ucar, S. C. Ergen, and O. Ozkasap, “Security vulnerabilities of IEEE 802.11p and visible light communication based platoon,” *2016 IEEE Veh. Netw. Conf.*, pp. 1–4, 2016, doi: 10.1109/VNC.2016.7835972.

[28] S. Ucar, S. C. Ergen, and O. Ozkasap, “Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination,” *IEEE Trans. Veh. Technol.*, 2016, doi: 10.1109/TVT.2015.2421277.

[29] S. Arnon, *Visible light communication*. 2015.

[30] O. Tonguz, “How Vehicle-to-Vehicle Communication Could Replace Traffic Lights and Shorten Commutes,” *Red Light Green Light. Light.*, 2018.

[31] A. Mostafa and L. Lampe, “Physical-Layer Security for MISO Visible Light Communication Channels,” *IEEE J. Sel. Areas Commun.*, 2015, doi: 10.1109/JSAC.2015.2432513.

[32] S. Ucar, S. C. Ergen, and O. Ozkasap, “Security vulnerabilities of IEEE 802.11p and visible light communication based platoon,” 2016, doi: 10.1109/VNC.2016.7835972.

[33] K. Emara, “Safety-aware location privacy in VANET: Evaluation and comparison,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10718–10731, 2017, doi: 10.1109/TVT.2017.2736885.

[34] ETSI EN 302 637-3, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service,” *Etsi*, 2019.

[35] A. D. Wyner, “The Wire-Tap Channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[36] I. Csiszár and J. Körner, “Broadcast Channels with Confidential Messages,” *IEEE Trans. Inf. Theory*, 1978, doi: 10.1109/TIT.1978.1055892.

[37] A. D. Wyner, “The Wire-Tap Channel,” *Bell Syst. Tech. J.*, 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[38] T. Araki and T. Suzuki, “Fuzzy timing passwords for providing easy user authentication to

disable persons and their application to visible light communication," 2012.

[39] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: Secure barcode-based visible light communication for smartphones," *IEEE Trans. Mob. Comput.*, vol. 15, no. 2, pp. 432–446, 2016, doi: 10.1109/TMC.2015.2413791.

[40] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *2014 IEEE Globecom Workshops, GC Wkshps 2014*, 2014, pp. 524–529, doi: 10.1109/GLOCOMW.2014.7063485.

[41] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," 2014, doi: 10.1109/ICC.2014.6883837.

[42] A. Mostafa and L. Lampe, "Physical-Layer Security for MISO Visible Light Communication Channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, 2015, doi: 10.1109/JSAC.2015.2432513.

[43] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible Light Communication, Networking, and Sensing: A Survey, Potential and Challenges," *IEEE Communications Surveys and Tutorials*. 2015, doi: 10.1109/COMST.2015.2476474.

[44] L. W. M. Saadi, "Samsung Electronics, ETRI, VLCC, University of Oxford. 2008. Visible Light Communication: Tutorial," *2017*. http://dx.doi.org/10.1515/joc-2017-0107.

[45] "J.P. Conti, What you see is what you send, Eng. Technol. 2008 (2008) 66–67."

[46] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, 2008, doi: 10.1109/TIT.2008.921908.

[47] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends Commun. Inf. Theory*, 2008, doi: 10.1561/0100000036.

[48] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 1, pp. 93–105, 2016, doi: 10.1109/TDSC.2015.2399291.

[49] D. Tsonev, S. Videv, and H. Haas, "Unlocking Spectral Efficiency in Intensity Modulation and Direct Detection Systems," 2015, doi: 10.1109/JSAC.2015.2432530.

[50] H. Haas, "LiFi is a paradigm-shifting 5G technology," *Reviews in Physics*. 2018, doi: 10.1016/j.revip.2017.10.001.

[51] Y. Li, M. Safari, R. Henderson, and H. Haas, "Optical OFDM With Single-Photon

Avalanche Diode," *IEEE Photonics Technol. Lett.*, 2015, doi: 10.1109/LPT.2015.2402151.

[52] M. S. Islim, M. Safari, S. Videv, and H. Haas, "A Proof-of-Concept of Outdoor Visible Light Communications in the presence of Sunlight," 2016.

[53] I. C. Lu, C. H. Yeh, D. Z. Hsu, and C. W. Chow, "Utilization of 1-GHz VCSEL for 11.1-Gbps OFDM VLC Wireless Communication," *IEEE Photonics J.*, 2016, doi: 10.1109/JPHOT.2016.2553839.

[54] Y. Xue, Y. Hou, S. Xiao, Y. Zhang, and L. Zhang, "Real-time visible light communication system based on 2ASK-OFDM coding," 2016.

[55] L. Grobe *et al.*, "High-speed visible light communication systems," *IEEE Commun. Mag.*, 2013, doi: 10.1109/MCOM.2013.6685758.

[56] Z. Li, C. Zhang, D. Sun, H. Yang, and J. Song, "A real-time high-speed visible light communication system based on RGB-LEDs," 2017, doi: 10.1109/BMSB.2017.7986189.

[57] C. Liu, B. Sadeghi, and E. W. Knightly, "Enabling vehicular Visible Light Communication (V2LC) networks," 2011, doi: 10.1145/2030698.2030705.

[58] S. H. Yu, O. Shih, H. M. Tsai, and R. D. Roberts, "Smart automotive lighting for vehicle safety," *IEEE Commun. Mag.*, 2013, doi: 10.1109/MCOM.2013.6685757.

[59] I. Takai, T. Harada, M. Andoh, K. Yasutomi, K. Kagawa, and S. Kawahito, "Optical vehicle-to-vehicle communication system using LED transmitter and camera receiver," *IEEE Photonics J.*, 2014, doi: 10.1109/JPHOT.2014.2352620.

[60] A. Bazzi, B. M. Masini, A. Zanella, and A. Calisti, "Visible light communications as a complementary technology for the internet of vehicles," *Comput. Commun.*, 2016, doi: 10.1016/j.comcom.2016.07.004.

[61] A. M. Cailean and M. Dimian, "Current Challenges for Visible Light Communications Usage in Vehicle Applications: A Survey," *IEEE Communications Surveys and Tutorials*. 2017, doi: 10.1109/COMST.2017.2706940.

[62] L. Cheng, W. Viriyasitavat, M. Boban, and H. M. Tsai, "Comparison of Radio Frequency and Visible Light Propagation Channels for Vehicular Communications," *IEEE Access*, 2017, doi: 10.1109/ACCESS.2017.2784620.

[63] A. Vinel, L. Lan, and N. Lyamin, "Vehicle-to-vehicle communication in C-ACC/platooning scenarios," *IEEE Commun. Mag.*, 2015, doi: 10.1109/MCOM.2015.7180527.

[64] R. Roberts, P. Gopalakrishnan, and S. Rathi, "Visible light positioning: Automotive use

case," 2010, doi: 10.1109/VNC.2010.5698229.

[65] J. I. Meguro, T. Murata, J. I. Takiguchi, Y. Amano, and T. Hashizume, "GPS multipath mitigation for urban area using omnidirectional infrared camera," *IEEE Trans. Intell. Transp. Syst.*, 2009, doi: 10.1109/TITS.2008.2011688.

[66] S. H. Yu, O. Shih, H. M. Tsai, and R. D. Roberts, "Smart automotive lighting for vehicle safety," *IEEE Commun. Mag.*, 2013, doi: 10.1109/MCOM.2013.6685757.

[67] P. Luo, Z. Ghassemlooy, H. Le Minh, E. Bentley, A. Burton, and X. Tang, "Performance analysis of a car-to-car visible light communication system," *Appl. Opt.*, 2015, doi: 10.1364/ao.54.001696.

[68] "Vision truck platooning 2025," *European Truck Platooning Network*, 2016. https://www.tno.nl/en/abouttno/%0Anews/2016/4/vision-truck-platooning-2025/.

[69] M. Y. Abualhoul, M. Marouf, O. Shagdar, and F. Nashashibi, "Platooning control using visible light communications: A feasibility study," 2013, doi: 10.1109/ITSC.2013.6728448.

[70] B. Bechadergue, L. Chassagne, and H. Guan, "Suitability of visible light communication for platooning applications: An experimental study," 2018, doi: 10.23919/GLC.2018.8319093.

[71] L. Cheng, W. Viriyasitavat, M. Boban, and H. M. Tsai, "Comparison of Radio Frequency and Visible Light Propagation Channels for Vehicular Communications," *IEEE Access*, 2017, doi: 10.1109/ACCESS.2017.2784620.

[72] M. Haenggi, "The secrecy graph and some of its properties," 2008, doi: 10.1109/ISIT.2008.4595044.

[73] P. C. Pinto, J. Barros, and M. Z. Win, "Secure Communication in Stochastic Wireless Networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 125–138, 2012, doi: 10.1109/TIFS.2011.2165946.

[74] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks - Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Secur.*, 2012, doi: 10.1109/TIFS.2011.2165947.

[75] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," in *IEEE Transactions on Information Theory*, 2012, vol. 58, no. 5, pp. 3000–3015, doi: 10.1109/TIT.2012.2184692.

[76] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of

physical layer security in decentralized wireless networks," *IEEE Trans. Wirel. Commun.*, 2011, doi: 10.1109/TWC.2011.061511.102257.

[77] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 6, pp. 2776–2787, 2013, doi: 10.1109/TWC.2013.041713.120865.

[78] H. Ma, L. Lampe, and S. Hranilovic, "Coordinated broadcasting for multiuser indoor visible light communication systems," in *IEEE Transactions on Communications*, 2015, vol. 63, no. 9, pp. 3313–3324, doi: 10.1109/TCOMM.2015.2452254.

[79] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Trans. Inf. Theory*, 2009, doi: 10.1109/TIT.2009.2027522.

[80] J. B. Wang, Q. S. Hu, J. Wang, M. Chen, and J. Y. Wang, "Tight bounds on channel capacity for dimmable visible light communications," *J. Light. Technol.*, 2013, doi: 10.1109/JLT.2013.2286088.

[81] A. Chaaban, J. M. Morvan, and M. S. Alouini, "Free-Space Optical Communications: Capacity Bounds, Approximations, and a New Sphere-Packing Perspective," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1176–1191, 2016, doi: 10.1109/TCOMM.2016.2524569.

[82] S. Dimitrov and H. Haas, "Information rate of OFDM-based optical wireless communication systems with nonlinear distortion," *J. Light. Technol.*, 2013, doi: 10.1109/JLT.2012.2236642.

[83] A. Mostafa and L. Lampe, "Optimal and Robust Beamforming for Secure Transmission in MISO Visible-Light Communication Links," 2016, doi: 10.1109/TSP.2016.2603964.

[84] G. Pan, J. Ye, and Z. Ding, "On Secure VLC Systems with Spatially Random Terminals," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, 2017, doi: 10.1109/LCOMM.2016.2643632.

[85] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications," in *2nd International Workshop on Visible Light Communications Systems - VLCS '15*, 2015, pp. 9–14, doi: 10.1145/2801073.2801075.

[86] X. Liu, X. Wei, L. Guo, Y. Liu, and Y. Zhou, "A new eavesdropping-resilient framework for indoor visible light communication," 2016, doi: 10.1109/GLOCOM.2016.7841521.

[87] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based

on protected zone and artificial noise," *IEEE Signal Process. Lett.*, 2013, doi: 10.1109/LSP.2013.2252898.

[88] H. Lu, Z. Su, and B. Yuan, "SNR and Optical Power Distribution in an Indoor Visible Light Communication System," pp. 1063–1067, 2014.

[89] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, 2010, doi: 10.1109/TIT.2010.2068852.

[90] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, 2010, doi: 10.1109/TIT.2010.2048445.

[91] M. Al-Khori, J., Nauryzbayev, G., Abdallah, M.M. and Hamdi, "Joint beamforming design and power minimization for friendly jamming relaying hybrid RF/VLC systems," *IEEE Photonics J.*, vol. 2, no. 11, pp. 1–18, 2019.

[92] S. Soderi, "Enhancing security in 6G visible light communications," 2020, doi: 10.1109/6GSUMMIT49458.2020.9083740.

[93] J. Y. Wang, Y. Qiu, S. H. Lin, J. B. Wang, Q. Wang, and B. Zhang, "Performance Analysis and Improvement for Secure VLC with SLIPT and Random Terminals," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2988470.

[94] S. Cho, G. Chen, and J. P. Coon, "Securing Visible Light Communication Systems by Beamforming in the Presence of Randomly Distributed Eavesdroppers," *IEEE Trans. Wirel. Commun.*, 2018, doi: 10.1109/TWC.2018.2804390.

[95] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-Oriented Transmitter Optimization for Visible Light Communication Systems," *IEEE Photonics J.*, 2016, doi: 10.1109/JPHOT.2016.2598684.

[96] A. Yesilkaya *et al.*, "Physical-layer security in visible light communications," 2020, doi: 10.1109/6GSUMMIT49458.2020.9083799.

[97] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy Performance of the MIMO VLC Wiretap Channel with Randomly Located Eavesdropper," *IEEE Trans. Wirel. Commun.*, 2020, doi: 10.1109/TWC.2019.2944144.

[98] J. Liang, S., Fang, Z., Sun, G. and Zhang, "A physical layer security approach based on optical beamforming for indoor visible light communication," 2020.

[99] G. Blinowski, "Security of Visible Light Communication systems—A survey," *Phys.*

Commun., 2019, doi: 10.1016/j.phycom.2019.04.003.

[100] X. Liu, X. Wei, L. Guo, Y. Liu, and Y. Zhou, "A new eavesdropping-resilient framework for indoor visible light communication," *2016 IEEE Glob. Commun. Conf. GLOBECOM 2016 - Proc.*, 2016, doi: 10.1109/GLOCOM.2016.7841521.

[101] L. Yin and H. Haas, "Physical-Layer Security in Multiuser Visible Light Communication Networks," *IEEE Journal on Selected Areas in Communications*, 2018. .

[102] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," 2014, doi: 10.1109/GLOCOMW.2014.7063485.

[103] A. Mostafa and L. Lampe, "Pattern synthesis of massive LED arrays for secure visible light communication links," 2015, doi: 10.1109/ICCW.2015.7247366.

[104] Z. Che *et al.*, "A Physical-Layer Secure Coding Scheme for Indoor Visible Light Communication Based on Polar Codes," *IEEE Photonics J.*, 2018, doi: 10.1109/JPHOT.2018.2869931.

[105] R. Shaaban and S. Faruque, "Optimized optical wireless channel for indoor and intra-vehicle communications: power distribution and SNR analysis," 2018, doi: 10.1117/12.2292151.

[106] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless communication technologies for ITS applications [Topics in Automotive Networking]," *IEEE Commun. Mag.*, vol. 48, no. May, pp. 156–162, 2010, doi: 10.1109/MCOM.2010.5458377.

[107] F. Bai and B. Krishnamachari, "Exploiting the wisdom of the crowd: Localized, distributed information-centric VANETs," *IEEE Commun. Mag.*, vol. 48, no. 5, pp. 138–146, 2010, doi: 10.1109/MCOM.2010.5458375.

[108] ETSI, "ETSI EN 302 637-3 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," *Etsi*, vol. 1, pp. 1–73, 2014.

[109] M. D. Higgins, R. J. Green, and M. S. Leeson, "Optical wireless for intravehicle communications: A channel viability analysis," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 123–129, 2012, doi: 10.1109/TVT.2011.2176764.

[110] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," 2010, doi: 10.1109/SP.2010.34.

[111] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular

networks: Why simple pseudonym change is not enough," in *WONS 2010 - 7th International Conference on Wireless On-demand Network Systems and Services*, 2010, pp. 176–183, doi: 10.1109/WONS.2010.5437115.

[112] S. Ucar, S. C. Ergen, and O. Ozkasap, "IEEE 802.11p and visible light hybrid communication based secure autonomous platoon," *IEEE Trans. Veh. Technol.*, 2018, doi: 10.1109/TVT.2018.2840846.

[113] M. Amoozadeh, H. Deng, C. N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Veh. Commun.*, 2015, doi: 10.1016/j.vehcom.2015.03.004.

[114] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," 2007.

[115] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on Intersection Collision Avoidance systems," in *IEEE Vehicular Networking Conference, VNC*, 2013, pp. 71–78, doi: 10.1109/VNC.2013.6737592.

[116] A. Agarwal and G. Saini, "SNR Analysis for Visible Light Communication Systems," *Int. J. Eng. Res. Technol.*, 2014.

[117] W. H. Shen and H. M. Tsai, "Testing vehicle-to-vehicle visible light communications in real-world driving scenarios," 2018, doi: 10.1109/VNC.2017.8275596.

[118] V. Jungnickel, V. Pohl, S. Nönnig, and C. Von Helmolt, "A physical model of the wireless infrared communication channel," *IEEE J. Sel. Areas Commun.*, 2002, doi: 10.1109/49.995522.

[119] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, 2013, doi: 10.1109/LSP.2013.2252898.

[120] "American Association of State Highway and Transportation Officials." .