SECURITY ASPECTS OF LI-FI TECHNOLGY

BY

Md Altafur Rahman

ID: 161-15-7083

AND

Md Sabbir Hosan

ID: 161-15-7206

AND

Sabbir Ahmed Likhon

ID: 161-15-6931

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Mr. Narayan Ranjan Chakraborty

Assistant Professor

Department of CSE

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

DECEMBER 2019

APPROVAL

This Project/internship titled **"Security Aspects Of LiFi Technology"**, submitted by Altafur Rahman, ID No: 161-15-7083 and Sabbir Ahmed Likhon, ID No: 161-15-6931 and Sabbir Hosan, ID No: 161-15-7206 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 7 December 2019.

BOARD OF EXAMINERS

Dr. Syed Akhter Hossain — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Abdus Sattar — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

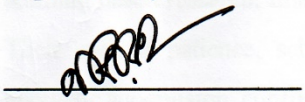
Shaon Bhatta Shuvo — **Internal Examiner**
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Md. Saddam Hossain — **External Examiner**
Assistant Professor
Department of Computer Science and Engineering
United International University

DECLARATION

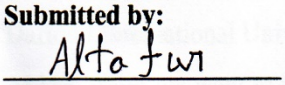
We hereby declare that, this project has been done by us under the supervision of **Mr. Narayan Ranjan Chakraborty, Assistant Professor, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

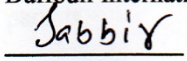


Mr. Narayan Ranjan Chakraborty
Assistant Professor
Department of CSE
Daffodil International University

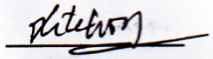
Submitted by:



Md Altafur Rahman
ID: 161-15-7083
Department of CSE
Daffodil International University



Md Sabbir Hosan
ID: 161-15-7206
Department of CSE
Daffodil International University



Sabbir Ahammad Likhon
ID: 161-15-6931
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

At First we would like to express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year thesis successfully.

We really grateful and wish our profound our indebtedness to **Mr. Narayan Ranjan Chakraborty**, Assistant Professor,Department of CSE, Faculty of Science and Information Technology, Daffodil International University, Dhaka. Their Deep Knowledge & keen interest with supportive instructions helped us in the field of deep learning based research, finally we completed our work on "Security Aspects of Li-Fi". Their endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Syed Akhter Hossain**, Professor and Head, Department of Computer Science and Engineering, Faculty of Science and Information Technology, DIU, for his valuable support and advice to finish our project and also heartiest thanks to other faculty member and the staff of department of CSE, Daffodil International University.

At last, again we want to thank all the good wishers, friends, family, seniors for all the help and inspirations. This research is a result of hard work and all those inspirations and assistance.

Finally, we must acknowledge with due respect the constant support and patience of our parents.

ABSTRACT

Nowadays all institutions as well as organizations are planning to shrink the size of hardware and are even trying to make it portable, olden days we had local area network wires to transmit data over devices then came in Wi-Fi which didn't have wires but was able to transmit data over devices but its sources are usually wired and sometimes not portable to every place and then now industries implement li-fi which uses a simple light to transmit data over devices. Users will just have to carry a small light source which will transmit the data over devices but what about the security measures to be taken that needs to be considered. This paper analysis defines measures for those security issues faced in Li-Fi technology.

CONTENTS PAGE

CHAPTER PAGE

LIST OF FIGURES

CHAPTER 1
Introduction

1.1 Introduction

LI-FI known as light fidelity is an upcoming technology which was first introduced by Harald Haas in 2011 in TED global Talk though it still didn't replace our existing WI-FI technology. But now at this current era of technology we are more concern about our security, stability and privacy. So before accepting this new wireless communication system as a concern citizen we are going to find and analysis every single security aspects of LIFI technology. After studying many papers related to life we have learned the modulation techniques and the advantages in security of this technology but we still don't know the actual upcoming threats that are coming through this. LI-FI uses global communication standard 802.11 bb. Using the pulse of 0 and 1 by changing the intensity of the LED ,any digital data can be transferred through LIFI .It is based on VLC. The fact is finding security flaws in light communication is comparatively complex than the radio wave communication. Because it is not a unidirectional communication system. So physical interference is the most legit way of gaining unauthorized access. In our day to day life how much security it will provide is the main matter of fact .

There are lots of question when it comes to security. Attacking any wireless access point is a common term in networking. Whether it is on the whole network or only the access point. We have tried different operation during our prototype testing. And we have find some really interesting things. Using some common property of light LIFI can also be compromised. But the fact is how much loss it will create in our privacy. Based on the use of this new tech in various platform the amount of destructions can be different. We already know that Wi-Fi has border range of connectivity but the speed and stability is very poor .On the other hand LIFI has lower range of connectivity but the advantage of creating multiple access point within a tiny space with a very high speed. APA management is one of important thing when it comes to wireless communication.

Where Wi-Fi has the limitation of using it in some sensitive place ,Life has the potential to use there without any problem. And when it comes to the point of security ,those sensitive places can be more vulnerable if the system in not so secure. In Life the main advantage is one access point can be devided into multiple point though it is also point possible in WI-FI using mesh but LI-FI use one connection and spread them into multiple LED. So we don't have to crave for bandwidth. The data density of LI-FI is much more higher than WI-FI.

We are not yet ready to accept this technology in our day to day life. In this paper we will search for the problems and the security flaws and some advantages also. We hope that after this research we will find more and more interesting facts about LI-FI. And we hope our research will help this new amazing technology to improve more than before. It will bring some necessary changes which will make LI-FI more effective. We are not against it we just want to know a bit more about it ,before we give it to the people because at this time people are more concern about their security and privacy more than before.

1.2 Motivation

First of all we wanted to do something that is connected to communication system or networking. We were searching ideas from different places. Our honorable supervisor was also trying his best to find interesting topics for us. Then we got the idea to do a research on a wireless communication system like LI-FI technology. But the fact was LI-FI is already introduced many times ago but still didn't grow rapidly. But day by day it's increasing. Experts think that it going to bring the 4^{th} industrial revolution in wireless communication system. Then we got an idea that we can analyze the security aspects of LI-FI technology, both the positive and most importantly the negative aspects of LI-FI in short vulnerability. On the other hand honestly our traditional WI-FI is going to obsolete soon or later. We have studied many online journal, articles and papers and find that there is really not much research on the security aspects of LI-FI. Most of them are telling about the benefits, advantages or just the basic modulation techniques. But everyone should know the precautions though if there is any. Because whenever we are going to use this technol

ogy in our daily life it can also create some major problems too. So we decided to hunt those causes, cautions about LIFI. We just didn't want to know the basic modulation technique rather than a bit more advance in the security portion. So our research is all about the aspects in security in LIFI.

1.3 Rational of the study

There is no doubt that people already know about this new communication technology. But what people don't know is the negative issues, disadvantages or the problems it's going to create in future. People don't know the comparative benefits of LI-FI instead of WI-FI. Someone still doesn't know the issues in our traditional WIFI which is really a fact. Our work is going to aware them from the common issues and even the upcoming issues of this latest technology. From our paper people will know that comparative study between LI-FI and WI-FI and mostly the security aspects of LI-FI technology. After studying our paper anyone will know the benefits and the issues of LIFI in term of security which matters the most right now. There are many possible that can happen on any communication system. Like jamming, snooping. Our research will help to know that all possible threats and it will help to improve this new communication system to overcome its limitations.

1.4 Research Questions

It was really hard for us to complete this research. There were many limitations. This is a new technology which is still not available in our local market. We know the modulation techniques, we know how it works But we didn't know how to measure the aspects or real life problems it can create. So we propose these following questions to express this feelings and outcomes this problem.

- Can we implement this in real life?
- Is it possible to face the real life obstacles by analyzing mathematically?
- Is there any outdoor light problems?

- How LIFI will be improved by this approach?
- Is it possible to avoid jamming?
- Is it possible to overcome down light problem?
- Is it possible to reduce the range issue?

1.5 Expected Output

In this section there are some points that were our minimum expectations. The main outcome of this research is to know how much secure LI-FI is in real life and analyzing the main security aspects of this technology that can make it vulnerable to unauthorized persons. Finding security flaws using some mathematical approach and the help of simulation tools will guide us to find the most accurate problems on this fact. Data redundancy, consistency, data loss or changing the pattern of data can be the main problem of our research. But the things that can be really benefit this new technology are given below,

- Range issue can be solved.
- Can analyze or measure the jamming issue.
- There is problem with outdoor light.
- Mac layer security can be compromised.
- Access point can be compromised in highbred network with WIFI.
- Caesar cipher encryption can make data transfer in LIFI more secure.

1.6 Layout of the Report

Chapter one have demonstrated an introduction to the project with objective, motivation, research questions, and expected outcome, this section describes the whole layout of this report. This chapter is all about the primary discussion, idea and planning for further work. Our expected outcome can be change during our research work.

CHAPTER 2

Background

2.1 Introduction

Visible light communication system is an alternative secured system against radio based wireless system. Alongside the features and speed of VLC, there are some major drawback of it. On that particular case, the radio wave has some advantages and the main thing is it has potentiality to travel long distance without losing the inbuilt data patterns in general sense. But when it comes to the point where security matters VLC is the best solution. Radio waves can be easily traced but the light wave is not so easy to manipulated. Because photons are a bit tricky to be distracted without any physical interference. Though still, we didn't reach at that level where we can analyze the data on that microscopic level. But stealing data or capturing the credentials of anyone is happening almost every communication system. Li-fi is not so different than that cause this the future of wireless communication which are going to be the next era of wireless communication. Lifi is a new addition in visible light communication System. Li-fi provides more security in visible light communication than RF signal Communication System. The signal of li-fi are not to able penetrate wall which add extra security in data transferring. Basically li-fi signal works without interruption but another light just like sun can affect the signal. In li-fi the shortage of bandwidth which occurred in RF signal can be short out. In this communication System, there are two back to back unidirectional system.As Li-fi use visible light communication which is not free from the risk of security. There are some issues just like data snoofing, modification , mac level security & also signal jamming. By using phosphor-containing paints there is a chance to change photon number distribution.

2.2 Literature Review

LiFi optical sign are not ready to infiltrate dividers, this being a favorable position in connection to security issues. A similar component can be abused to wipe out impedances between neighboring cells. During the most recent ten years, there have been ceaseless

reports of improved point-to-point interface information rates utilizing off-the-rack white LEDs under test lab conditions.

Light waves are works constantly with no interference. Assume different lights from sun, typical bulbs, can intrude on the transmission of light waves then the correspondence will be affected.Li-Fi tackle issues, for example, the lack of radio-recurrence transfer speed and furthermore permit web where customary radio based remote isn't permitted, for example, air ship or hospitals. The correspondence is on a very basic level unidirectional. Two unidirectional channels are utilized consecutive to make correspondences. Li-fi utilize the worldwide light correspondence guidelines 802.11 bb for correspondence through light. Light can be contained, and verified in a physical space. Li-Fi empowers extra control as Li-Fi offers exact localisation for resource following and client verification. RF is powerless against impedance from a wide scope of gadgets, for example, cordless telephones, microwaves and neighboring Wi-Fi systems. Li-Fi sign can be characterized by the territory of light, which means impedance is a lot easier to keep away from and even stop through and through. This likewise implies Li-Fi can be utilized in RF antagonistic zones, for example, medical clinics, control plants and planes.

2.3 Research Summary

Li-fi is the eventual fate of remote correspondence framework. The monstrous utilization of Li-Fi may illuminate the bottleneck of information Transmission in Wi-Fi innovation. Remote correspondence advancements dependent on radio recurrence and microwaves are progressively defenseless against listening stealthily, signal seizing or unapproved block attempt, savage power assaults and spontaneous organize associations.

2.4 Scope of the problem

The Li-Fi advancement can be used for various purposes, it has any kind of effect the data transmission through LEDs subsequently all of the screens which illuminate light can be filled in as a phase for data correspondence. The screen of the mobile phone, TV, bulbs can go about as a wellspring of light. On the other hand, the tolerant stage, the photodetector

can be displaced by a camera in the PDA for checking and recouping data. Its various applications are Li-fi for work regions, smartcard Li-fi, Li-fi for schools, medicinal facilities, Li-fi in urban territories, clever aides, recorded focuses, lodgings, jamboree, events indoor and LBS (Location-based Services), get the opportunity to control and conspicuous evidence crisis, strip malls, air terminal and hazardous conditions like warm power plants. It similarly has the advantage of being useful in electromagnetic sensitive regions, for instance, in carrier lodges, restorative facilities, and nuclear power plants without causing electromagnetic obstacle. Li-Fi can be used at the spot of Wi-Fi for a web relationship with all contraptions. It is similarly incredibly important for correspondence between two contraptions for data move and various sorts of affiliations. It gives an uncommonly fast speed to web access and spilling reason and moreover snappy and secure data move between the devices. So the Li-Fi Technology is useful for general use like at the spot of Wi-Fi and Other remote advancements for data transmission or web get to goal.

2.5 Challenges

Remote Internet controlled by radio waves is one of two predominant ways individuals logon to the Internet, where the other methodology is through wired Ethernet. All the more as of late, another methodology for the arrangement of the remote Internet through the encoding of data in light waves has developed. Known as Li-Fi, remote Internet is transmitted from light equipped for filling in as a switch, where data is encoded in light waves. Upon gathering by a USB thumb drive with a light sensor, light waves could be decoded into helpful data justifiable by the PC. Exhibited to be compelling in transmitting data at a speed of 42 Mbps, which is proportionate to the upper-speed utmost of the HSPA+ remote correspondence standard for the portable Internet, Li-Fi, in any case, faces serious difficulties to its handy execution. In particular, data must be dependably transmitted if there is a solid two-path correspondence between light switch and the USB transmitter. Along these lines, given that light goes in straight lines, Li-Fi must be employable if the client is legitimately beneath a light switch, where the uplink from the USB transmitter to the light switch is through immediate, straight-line correspondence connection fueled by light waves, and gathering could be through immediate or reflected light waves (e.g., from the dividers). Thus, Li-Fi is conceivably more prohibitive than wired Ethernet as far as

clients' development. Furthermore, interest for the rapid remote Internet would essentially prompt higher light power utilized for data transmission. In this manner, the probability exists where high-power light could bring about visual distress and warming impact to the clients as a generous measure of light vitality would be changed over to infrared warmth. On the whole, down to earth utilization of the new correspondence convention, Li-Fi is hampered by essential issues of diminished portability to clients just as a wellbeing concern, for example, to consider the methodology indefensible for a wide selection. Being a straight line specialized instrument between light switch and USB light sensor transmitter implied that the client is required to be under a light or light during the whole span of remote Internet get to, where he is probably going to encounter high-power light waves for giving more data transfer capacity and remote access speed that outcomes in a warming impact.

CHAPTER 3

Research Methodology

3.1 Introduction

In this Section we are going to discuss about the methodology. Here we will discuss the whole process, data that we have analyzed, data collection procedure, implementation requirement, statistical analysis. We are going to co-ordinate with our expected outcome and search for further more advance research. There is some key point like data collection, processing, proposed model also described with relevant equation, graph, table and description. Here we will use some MATLAB simulation data and results. The chapter is being closed by giving the explanation of our project's statistical theories and besides, giving the clear concept of the implementation requirements.

3.2 Research Subject and Instrumentation

Research subject can be called as research zone that was assessed and read for clearing ideas. For execution as well as for configuration model, gathering information, actualize or process information and preparing the model. On the other area is Instrumentation that is which innovation and strategy we utilized. We used windows platform, some MATLAB base simulation data and results and some data from different sources.

First of all we are going to describe the modulation of LIFI then we will analyze the data for various security purpose.

3.2.1 What is VLC?

Visible Light Communication (VLC) has amplified incredible enthusiasm for the most recent decade because of the fast improvements in Light Emitting Diodes (LEDs) manufacture. Effectiveness, strength and long life expectancy of LEDs make them promising private lighting hardware just as option modest and quick information move

gear. One of the thoughts laid forward for remote optical correspondence is the unmistakable light specialized strategy. The sign in the 380-780 nm wavelength interim of the electromagnetic range are the light flag that can be recognized by the human eye. It is conceivable to accomplish brightening and information move at the same time by methods for LEDs that is the conspicuous lighting gear of late. By along these lines, both interior lighting of a room and information move will be achieved without the need of an extra correspondence framework. This innovation is given the name of Visual Light Communication.

3.2.2 What is Li-Fi?

Li-Fi is a Visible Light Communications (VLC) framework. Like Wi-Fi it's a bidirectional remote correspondence innovation. In any case, where Wi-Fi uses radio waves to transmit information, Li-Fi utilizes obvious light from LED lights fitted with an uncommon chip. It's similar to Wi-Fi, yet has arrived at speeds multiple times quicker in testing, making it undeniably increasingly fit to the requests of things to come of information. Li-Fi and Wi-Fi are very comparative as both transmit information electromagnetically.

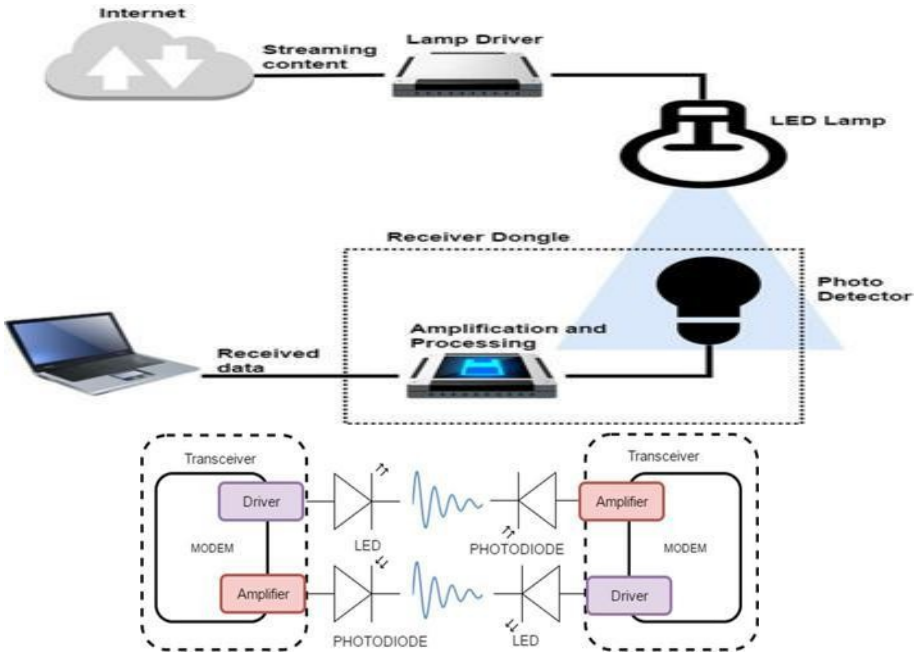


Figure 3.2.2.1: Simple LIFI Mechanism

In any case, Wi-Fi uses radio waves while Li-Fi runs on noticeable light. As we presently know, Li-Fi is a Visible Light Communications (VLC) framework. This implies it suits a photograph locator to get light flag and a sign handling component to change over the information into 'stream capable' content.

3.2.3 How Li-Fi work?

It is applied by utilizing a light at the downlink transmitter. Regularly the light gleams at a steady current inventory anyway quick and tricky varieties in current can be made to create the optical yields since it just uses the light, consequently can be effectively applied to any such zone where radio recurrence correspondence is frequently testing. The wellspring of light consistently shows up on the grounds that the LED can be turned ON and OFF rapidly and the sum is quickly balanced that human eye can't affixing despite the fact that it is gleaming. The LEDs action of ON-OFF which imperceptible and empowers the transmission of information utilizing the double codes for example 0s and 1s, for switch ON LED it is a coherent '1', and for switch OFF LED it is a consistent '0'. This strategy for utilizing fast beats of light to transmit data remotely is actually alluded to as unmistakable light correspondence (VLC).

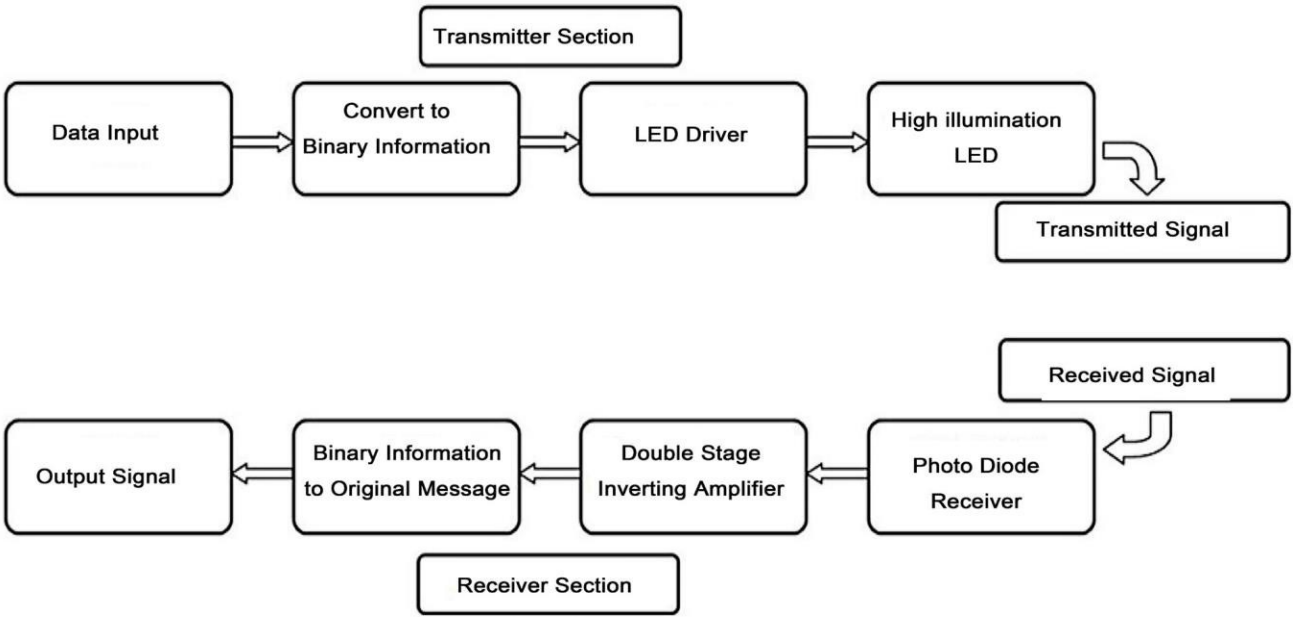


Figure 3.2.3.1: Li-Fi transmission Block Diagram

Transceiver a square that go about as a transmitter and collector simultaneously. This handset comprises of LED to transmit the light and photo diode to get the light. Intensifier is installed to quality the intensity of light got from the photo diode. The modem is utilized to adjust and demodulate the sign. The sign that originates from the photo diode is simple and it changes over into computerized in the modem. While the sign that prepared to transmit, the advanced sign proselyte into simple sign in the modem and sent by LED. The driver before the LED works to drive the ebb and flow of the LED so as to get the flashing. The gleaming is working the LED for information transmission, whenever LED is ON then it transmits computerized '1' and if OFF, it transmits advanced '0'.

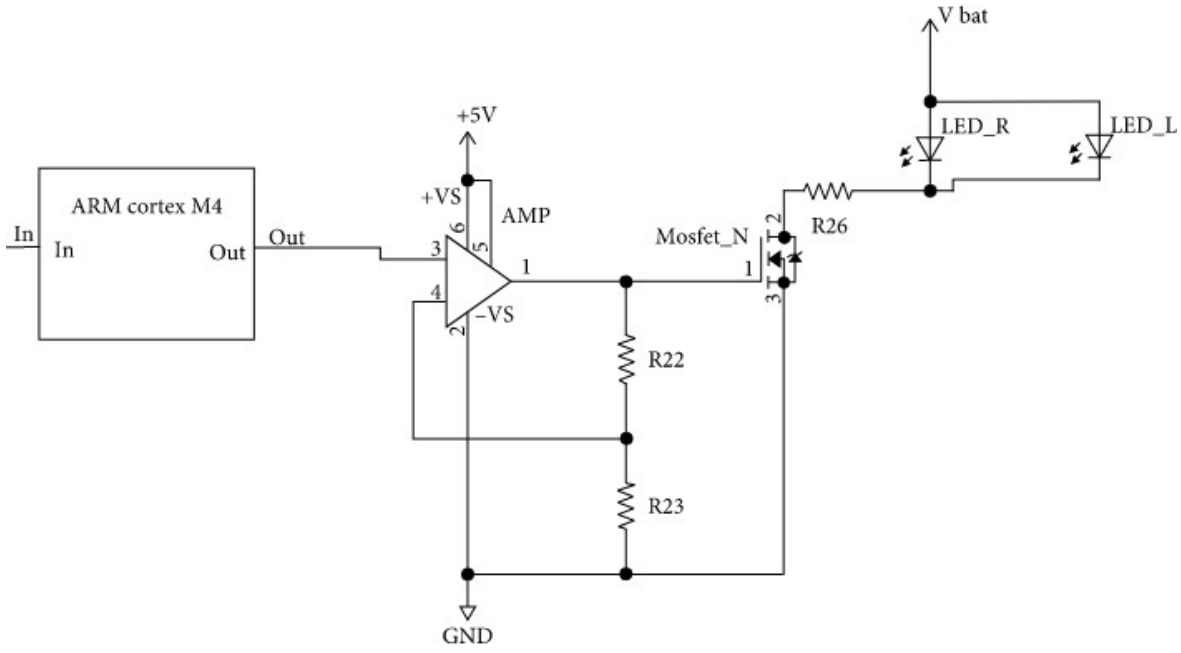


Figure 3.2.3.2: Transmission Circuit

The regulation sign is utilized to switch LED at wanted frequencies that contains data to be transmitted. As indicated by [6] there are a few method of balance in Li-Fi. Balance systems is required all together the correspondence is as yet accessible even the enlightenment isn't required. Hence, a tweak system may bolster a dimmable enlightenment. The variety in power of light relating to the data in the message signal. There are numerous run of the mill of balance in Li-Fi for example Single Carrier Modulation (SCM), Multiple Carrier Modulation (MCM), and Color Modulation.

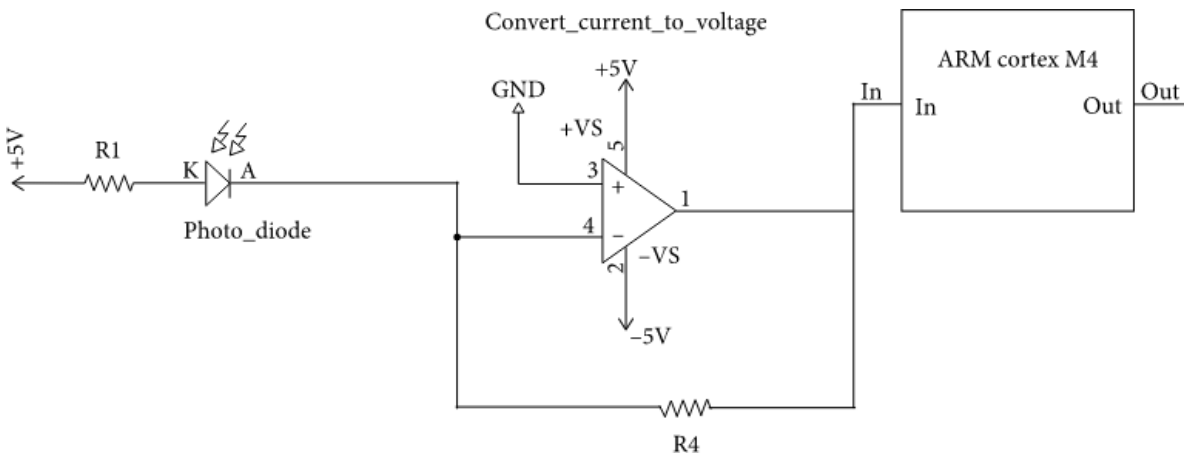


Figure 3.2.3.3: Reception Circuit

Productivity and security of the web are the ruling issues now. Li-fi was found in 2011 by Scientist Harold Haas from UK. The plan is to beaten the impediment of Wi-Fi. The speed of Wi-Fi is up to 1500mbps and it's not adequate to oblige an enormous client.

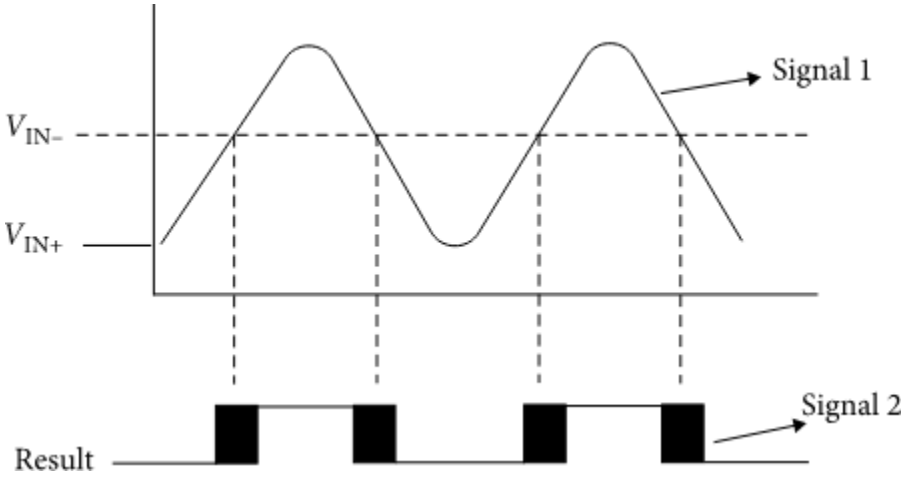


Fig3.2.3.4: Output Signal

Li-Fi empowering the framework utilizing completely arranged remote correspondence and could give a association that is multiple times quicker than Wi-Fi. It can arrive at velocities up to 3Gpbs by utilizing DMT adjustment. The other speed of Li-Fi with the diverse tweak additionally appeared in the table 5. M.D Renzo et all utilizing Spatial

Modulation for MIMO Wireless System in Li-Fi, the transmit speed is up to 10Gbps. The rate speed of Li-Fi can be higher than 3Gbps while the innovation is on research and creating. The rate speed of LiFi depends on the utilizing of the balance. Dr. P. Kuppusamy et.all doing a study of Li-fi and contrasting it and Wifi, there are a few attributes that utilized for looking at. The distinction of Li-Fi and Wi-Fi is appeared in table 6. For security, Li-Fi is more secure than a Wi-Fi. It is on the grounds that the inclusion territory of Li-Fi is just on their light up territory. The sign of Li-Fi can't experience the divider. While the sign of Wi-Fi can experience the divider, it can cause the vulnerabilities in information misfortune and information spillage. As indicated by security issues in VLC center around part of essential physical attributes of the correspondence channel. The paper likewise breaks down the danger of sign sticking, information snooping, change, and MAC-level security. The outcome is VLC framework is especially inclined to information security chance. As per one of the security issue in Li-Fi is spying, an assault occur by getting the sign that originate from the hole between the floor and entryway, break inside the ground surface or from somewhat protected windows.

3.2.4 List of some frequency and wavelength for different band

Gamma-ray <0.01 nm >30 EHz

X-ray 0.01-10 nm 30 PHz-30 EHz

Ultraviolet 10 nm-400 nm 790 THz-30 PHz

Visible (VLC) 400 nm-750 nm 405 THz-790 THz

Infrared 750 nm-1 mm 300 GHz-405 THz

Radio (RF) >1 mm 3 Hz- 300 GHz

3.3 Data Collection Procedure

Here we have used data from some papers related to LI-FI and analyzed them in MATLAB 2018ra version with proper circuit and input values. Then we have calculated the result

with some formulas based on the change in different situations and perspective. We have provided the necessary formulas and the data that we have worked with

- Collected data from different journal, article and thesis paper
- Designed necessary circuits in MATLAB
- Build formulas for analysis.
- Collected the changes in graph
- Compared them with previous graphs
- Finding the facts and describe them

3.4 Statistical Analysis

In VLC correspondences the transmitter is a LED driven with an exchanging transistor and a present limiting resistor. Basically the present experiencing LED is degree with the luminance of the light transmitted. For 1W Power LED for current of 350mA the luminance is 110 lx. Factorizing the intentional current with some relative enduring will give a deduced model for luminance yield of a LED.The beneficiary is extremely a photo discoverer. The photo locator is a photo transistor switch in which when light hits the base (portal for mosfet) of the transistor is turned on. The resistor yield models the TTL yield of the got twofold data.

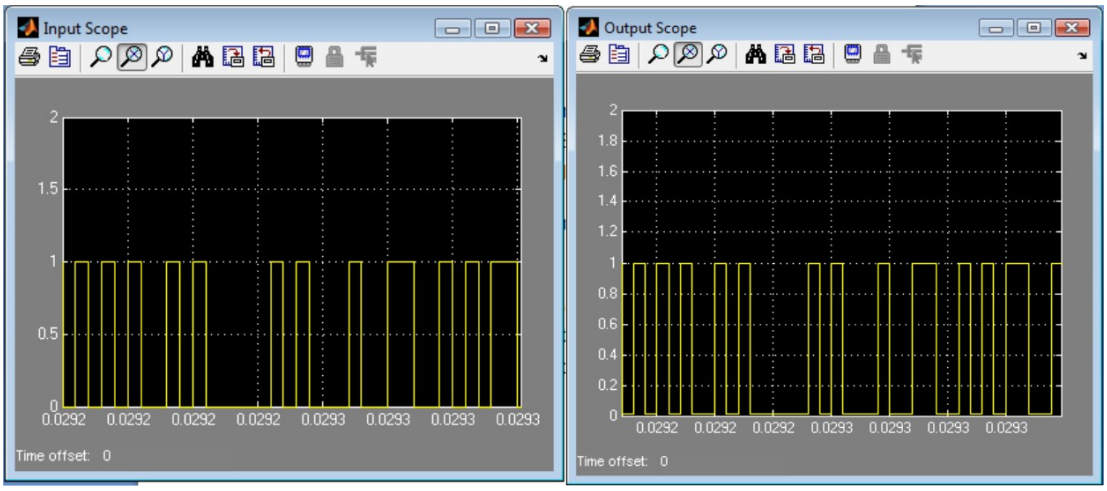


Figure 3.4.1: Input-output graph

• Path loss (Air)

The Path Loss square reenacts the decrease of luminance in air. As light adventures it misfortunes its quality relating to 1/Distance2. In the model it is acknowledged that the partition traveled is 4 meters.

• Noise from Path, Switching and Semiconductors:

A clamor source is added to show the commotion made by way, exchanging and semiconductors. A Gaussian commotion circulation capacity produces arbitrary clamor which is approximately the equivalent in genuine frameworks.

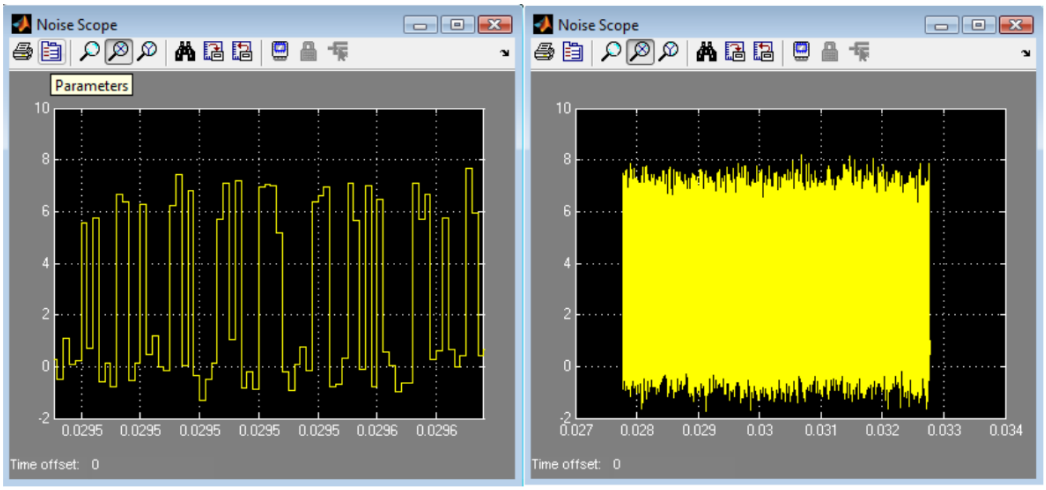


Figure 3.4.2: Input-output graph with noise

3.5 Implementation Requirements

After the correct investigation on all important factual or hypothetical ideas and strategies, a rundown of prerequisite has been produced that must be required for such a work of picture Classification. The plausible fundamental things are:

Equipment/Software Requirements

- OS(Windows 7 or above)
- Hard Disk (least 500 GB)
- Ram (Minimum 4 GB)
- MATLAB 2018ra
- Simulink
- NS2 simulator

Things that need to design in MATLAB

- Transmission Circuit
- Reception Circuit
- Modulation Formulas
- A2D & D2A converter
- Encoder & Decoder
- Some collected values to analysis

CHAPTER 4

Experimental result and discussion

4.1 Introduction

We will consider four fundamental parts of VLC correspondence security, to be specific: accessibility, privacy, genuineness, and trustworthiness as for framework, fixed and versatile classes of VLC gadgets. The dangers that we consider are the potential outcomes of: sticking, snooping and information change. Every danger ought to be considered independently for all correspondence plans, for example versatile to-portable, foundation to-versatile, versatile to-framework, and so on. Instinctively we realize that, for instance it is simpler to listen in on foundation to-portable correspondence than on versatile to-versatile, yet some kind of hazard appraisal related with every correspondence plan ought to furnish us with an answer about the regions of most noteworthy risk level. In this chapter we will discuss the results which will collected from different type of sources.

4.2 Experimental Results

We will use emotional threat characteristics: "low", "medium" and "high" in perspective on the correspondence plan's physical properties. Figure 4.2 shows abstract estimations of: vary, power and radiation plot for every correspondence arrange. On broaden, variable to-compact vary is taken into account "low" (~ ten cm), "medium" (up to one m) applies to fixed-to-fixed and fixed-to-convenient, and every one correspondences with system are thought-about to own "high" run (up to three m)[16]. Power is "low" for mobile phones, "medium" for fastened, and "high" once institution is that the sender. The radiation semi purpose is systematically thirty to sixty degrees for convenient and stuck contraptions; once structure encompassing lighting is employed we tend to settle for the sting to be "high" (Flimsy radiation edges which can be practiced with optical device connected with transmitter optics are wrong presently sure as shooting understood)[16].

I	3	3	-
F	2	2	3
M	1	2	3
R/S	M	F	I

Figure 4.2.1: Range (R)

I	1	2	-
F	1	2	3
M	1	2	3
	M	F	I

Figure 4.2.2: Power (P)

I	2	2	-
F	2	2	3
M	1	2	3
R/S	M	F	I

Figure 4.2.3: Radiation angle (A)

The risk of Jamming, Snooping & Data Modification is given below:

Jamming: $J = R / P$ (i)

Snooping: $S = P. A$ (ii)

Data modification: $M = J. S = R. A$ (iii)

Jamming (i) is clearly comparing to expand – the more drawn out the range, the easier to show a secured transmitting contraption, this component being conversely comparative

with the transmission control. Snooping (ii) is straightforwardly relative to transmission control and the radiation point – the more extensive and all the more dominant the transmission shaft, the simpler to regulate the correspondence. Data modification risk (iii) is evaluated as a result of the dangers of sticking and snooping. The determined dangers are appeared in figure

I	3	3/2	-
F	2	1	1
M	1	1	1
	M	F	I

Figure 4.2.4: Jamming (J)

I	2	4	-
F	2	4	9
M	2	4	9
R/S	M	F	I

Figure 4.2.5: Snooping(S)

I	6	6	-
F	4	4	9
M	2	4	9
R/S	M	F	I

Figure 4.2.6: Modification (M)

4.3 Descriptive Analysis

4.3.1 Physical and mac layer security

The risk estimation results are solid with our nature: the foremost real peril of harming VLC security develops once correspondence with system cares. We must always therefore

base totally on this piece of correspondence. The IEEE 802.15.7 customary communicates that "Because of detectable quality, if associate unapproved beneficiary is obstructing the correspondence signal, it'll normally be seen." Clearly, in any case, this isn't for every state of affairs legitimate: by virtue of the NLOS channel and LOS correspondence with the structure, associate unapproved authority could also be with success brought into nature while not being seen[16]. Snooping on VLC transmission is clearly duty-bound by physical factors, and is problematic than Wi-Fi snooping, anyway, there's no obvious inspiration driving why, it shouldn't be doable, particularly owing to correspondence with system. What are the potential styles for introducing a symptom staying or information dynamical device into the VLC structure channel? The assailant could use each composed and non-facilitated lightweight sources within the LOS or NLOS models, nonetheless because of force examinations a LOS model are most popular[16]. At the purpose once all is claimed in done, the aggressor's purpose is to realize the next lighting up at the beneficiary than that gave by the transmitter. One potential strategy for achieving this goal is also to use optical bar framing. Optical bar shaping in a very VLC structure was appeared soon with a solid state spacial lightweight modulator (Kim (2013)). The key rational issue from the attacker's viewpoint is to confirm that the sunshine gave by the dissident transmitter remains unobserved by the customers. During this method, the offender might use a considerably planned transmitter. VLC institution frameworks might contain completely different free transmitters to convey edible incorporation and purpose of confinement. Multi-transmitter "photocell" VLC frameworks are in like manner analyzed as Associate in Nursing enlargement to customary Wi-Fi and cell frameworks – see Cui, Quan and Xu (2013)[16]. In such circumstances the muse of a dissident transmitter might simply pass unobserved. Associate in Nursing succeeding likelihood is that giving birth hold of a section of the $64000 VLC institution by the ways for wired or remote channel; in a very stupendous foundation such vesicatory mediation might in like manner pass unobserved. Information amendment in VLC frameworks is also accomplished by responsive staying ways. As was displayed by Wilhelm (2011), progressing responsive staying is sufficiently in the reach of aggressors with employment of programming delineated radio (SDR) advancement. Within the recently documented work, ZigBee (IEEE 802. 15. 4) show devices were used

– it's vital the MAC-level comparable qualities of ZigBee and also the VLC 802.15.7 standard.

4.3.1.1 Security at the physical level

What are the security parts of VLC as far as the correspondence channel? An optical correspondence connection is demonstrated as a Poisson channel. The commitment to the Poisson channel is a non-negative waveform λ(t)[16]. The yield of the channel is an inhomogeneous Poisson process with force λ(t) + λ*0*. The subsequent term speaks to the added substance Poisson commotion of force λ*0*. From our point of view the multi-get to Poisson channel model presented by Lapidoth and Shamai (1998) is of intrigue. In the MAC model there are K autonomous sources of info and one yield. The channel yield is a superposition of the yields of K autonomous single-client Poisson channels.

Henceforth, for inputs $\lambda_1(t)$; $\lambda_2(t)$; ... $\lambda_k(t)$ the yield of the channel is an inhomogeneous Poisson process v(t), with power:

$$\lambda(t) = \sum_{i=1}^{K} \lambda_i(t) \qquad \text{(iv)}$$

In the general instance of K clients, it was appeared by Lapidoth and Shamai (1998) that the most extreme absolute throughput of the Poisson MAC monotonically increments with the quantity of clients and is limited from above. This is as opposed to the Gaussian MAC, where the most extreme complete throughput becomes unbounded as the log of the quantity of clients. The Poisson MAC has a limit accomplishing yield which is a Poisson procedure with a power L equivalent to the total of its K twofold data sources. A Poisson procedure of power λ has the entropy rate λ (1-log(λ)) bits/sec. – it doesn't monotonically increment with the info, and is inward with a top at input force 1/e. In this manner, adding more contributions to a Poisson MAC in the end soaks the entropy rate (and subsequently the data content) of the yield. The outcomes of the abovementioned, to the extent sign sticking and changing are concerned, are as per the following: given the channel limit constraint, a sign source with adequate transmitting force will have the option to soak the channel

clouding the information source; a similar outcome may likewise be acquired by a bigger number of maverick low-control transmitters.

4.3.1.2 Security at the MAC level

What is the current state of security of the regulated VLC show? IEEE standard 802.15.7 portrays the security instruments to be finished by the MAC sublayer when referenced by the higher show levels[16]. The huge assumption of the current IEEE standard is that data security and uprightness should be given by crypto graphical techniques, yet the use of these organizations should not be absurdly befuddled and should not eat up such countless computational resources. This supposition lines up with the PAN (singular zone frameworks) and BAN (body area frameworks) perspective inside which the enlisting resources may have through and through obliged capacities to the extent handling power, available accumulating, and power channel. Nevertheless, VLC frameworks are in like manner considered as a LAN development (or perhaps as a LAN expansion); from now on the directly proposed security instruments may show to be unreasonably weak. The cryptographic instrument of the IEEE 802.15.7 standard relies upon symmetric-key cryptography and usages keys that are given by higher layer structures[16]. Cryptographic layout security uses a key shared between two peer devices (interface key) or a key shared among a social occasion of devices (pack key), consequently allowing some flexibility and application-unequivocal trade off between key amassing and key bolster costs versus the cryptographic protection gave[16]. The standard describes 8 security levels:

"None" (no encryption and no trustworthiness), decency just gave by the MIC-32, MIC-64 and MIC-128 counts (three levels), encryption-just, and encryption notwithstanding MIC (the three recently referenced varieties)[16]. Encryption uses the CCM* figuring reliant on 128 piece AES in CBC-MAC mode. The optional key packaging counter framework forces key re-instatement and balances replay attacks. Packaging encryption is suited data, reference point payload and course payload. The standard itself doesn't describe increasingly critical level pieces of key age, recuperation and the officials these are unequivocally perceived as outside the standard's degree. This procedure passes on the going with perils: As security organizations gave by uprightness and encryption are

optional, there is a colossal risk that in practical applications security will be slaughtered as per usual or not executed using any and all means, a segment of the MAC header fields are not encoded, which may provoke attacks unquestionably known and portrayed for Wi-Fi (802.11) frameworks, the standard doesn't describe affirmation of the keying material or the spread of keys (as, 802.15.4 does), If a social affair key is used for dispersed correspondence, protection is given unmistakably against unapproachable devices and not against potential threatening contraptions in the key-sharing get-together.

4.4 Summary

Security elements of VLC have up to now force in very little thought. Continual pattern investigate during this field is for the foremost half centered arounds achieving higher transmission rates (novel modification plans, MIMO etc)[16]. Through our eyes, abundant identical because the case with numerous remote framework advancements, VLC is additionally not free from its own one in all a form security problems. VLC institution is especially disposed to information security threats. this IEEE commonplace 802.15.7 doesn't provide smart MAC-level protection from physical level risks[16]. Any analysis is relied upon to separate and improve stream VLC progresses the degree that channel-level security is bothered.

CHAPTER 5

Conclusion, recommendation and future works

5.1 Introduction

It have not to doubt that currently there are lots of research works on it. Security aspects of Li-Fi are one of the important domains in the Network world. In a variety of applications and its security and speeds, it has become one of the major important things of the running world. Nowadays there are many kinds of technology used but Li-Fi technology one of the most promising, secure and interesting things. So this approach will invent a new technology what is our main goal is to discover specialized more secure and speedy technology than Wi-Fi technology.

5.2 Conclusion

In this report, our main focus on provide security aspects of Li-Fi technology. Finally we stablished a new era of Li-Fi and the eventually the final result is really encouraging. Expectantly, this strategy will be pursued and elaborated in the future as section of further increases security aspect of Li-Fi technology. Expectantly, in the future, it will be changed networking and the internet era rapidly. In this report, we how out how the working methodology of Li-Fi and the regulation that it's utilized, the design, the presentation, and finally the difficulties. The motivation behind Li-Fi modification is to give active information communication appropriating a remarkable light area. Soon Li-Fi is on-going research, it has a possible bit of scope that can make an improvement RF communication and can be appropriated to improve remote system performance. Even though Li-Fi has a decent exhibition in the exchange rate, Li-Fi isn't adequate when conveying in an open-air

in daylight or other condition. Li-Fi will most likely not supplant Wi-Fi, these two advances can be utilized together to accomplish an increasingly productive and secure system. Li-Fi is an ongoing innovation that utilizations LED sheep for remote correspondences. It utilizes the noticeable light band rather than the radio range. In contrast to RF frameworks, where radio wires are utilized for transmission and recipients, Li-Fi frameworks use LED lights for transmission and photodetectors in the collectors. Notwithstanding the customary balance plans utilized in RF, Li-Fi has its interesting balance procedures, for example, CSK and MM. Since the noticeable light band is multiple times more extensive than the radio band, Li-Fi can give a very high information rate. Likewise, the noticeable light band is unlicensed and allowed to utilize. Other than these two benefits of Li-Fi technologies new era, it is a vitality productive framework reliant on the lighting, which is accessible all over. Additionally, it has a straightforward circuit with normally a security highlight, since light can't go through dividers. Moreover, in contrast to RF frameworks, Li-Fi doesn't experience the ill effects of multipath blurring issues. What's more, the Li-Fi frameworks are more secure and more financially savvy than RF frameworks.

5.3 Future Works

Li-Fi innovation is as yet obscure to many individuals and is past creative mind for some individuals. It has not been executed perfectly. When it is placed into down to earth use it can take care of various issues of systems strategy and can overcome numerous confinements of current remote correspondence structures. There are different fields where we can't utilize RF (radio recurrence) correspondence since they are destructive. For instance, in emergency clinics, radio waves are risky to the patients and can likewise influence readings of machines like X-ray machines and so forth. On the off chance that we accept Li-Fi that we can tackle the issue since it won't influence anything. Likewise in some military tasks, RF correspondence isn't permitted and to determine such concern Li-Fi could be appropriated to transmit information. Typical Wi-Fi innovation can't give protection of information or shroud the information however utilizing Li-Fi can give complete security of information which different organizations can use to conceal their significant subtleties. Water retains signal so RF correspondence submerged is

unimaginable and also the waves could influence marine life. Li-Fi would not make before-mentioned problems and can give a skillful answer for short-go transmission. In rush hour gridlock framework Li-Fi could be utilized into the road lights and it would pack in as Li-Fi hotspot as a whole [24]. After that, we can say won't just have fourteen billion lights, we may that we have fourteen billion Li-Fi posted universal for a greener and significantly increased encouraging time to come for racing information delivery. In this time, both light and radio waves can be used simultaneously to transfer information and warning. Various upgrades can be performed to the current variation, with the help of utilizing quick supplanting LEDs, information transmission flows may be additionally developed. The driving swiftness of the path may be improved by the help of using quick supplanting transistors. Light sources (particularly LED lightbulbs) are today wherever. In this case, it will help in unchanging data transmission (light is the tool of data transfer). Ingenious Hospitals: several medical types of equipment can be monitored and controlled using LiFi in healthcare policies. Aircraft and Aviation are can be part of the internet, which will display under in aircraft. Underwater Communications also can be part of this system. Where Wi-Fi does not work undersea areas because of high sound waves whereas Li-Fi will serve and can be served better performance. Dangerous/ Impatient Environments (Thermonuclear energy factories, tunnels and petrochemical factories that are responsive to electromagnetic collisions), Hazard control (storm, torrents), Education fields, Green information technology (there will no side effects on birds or animal), Radiotelephony reporting.

5.4 Limitation/Challenges of Light Fidelity (Li-Fi)

The test in Li-Fi depends on the point that has been examined in writing and the framework that effectively accessible. Counting the genuine clients of Li-Fi innovation is the means by which to reaction.

Modulation

The key of Li-Fi correspondence is the utilizing of regulation. An adjustment in Li-Fi is to convey double information by killing the LED on and rapidly. There are numerous viewpoints in Li-Fi identified with adjustment, enlightenment and the diminishing plan is the primary concern. Enlightenment is the expanse of the light that creates the LEDs that can be work as a factors in information communication. The test is how the weak is empowering the light of LEDs all together can send the information while the enlightenment is low. While the darkening procedure is to relative of LEDs brilliance. The test in darkening innovation is how the Li-Fi can satisfy the client fulfillment all together the diminishing of LEDs can remain alright for the client [13].

Interference

In optical enlightenment dependent on information correspondence, the critical step is to give the optical uplink administration. It is on the grounds that the uplink administration can meddle with the downlink signal. This issue is one of the difficulties in the obstruction sign issue. In Li-Fi, the transmitter ought to have the option to keep up a directional connection during the transmission [13].

Framework

The fundamental establishment in Li-Fi in indoors and outdoors. Kind of similar to the optical trademark, a Li-Fi moreover has an effect shadowing while it is transmission work. This shadowing sway, clearly, will give an effect during the time spent sending and getting the data. There is little research about the effect of shadowing in the Li-Fi correspondence [13].

Security

As maintained by a hazard like tuning in can happen in Li-Fi. It occurs when there is a gap between the floor and the door, the light may increase out between them. The break from within floor and secured windows also can be spillage [13].

Inclusion

Li-Fi is a development that has a nice introduction in an indoor system while it's not happening in the outdoors region. The incorporation in the outside zone for LiFi ought to be set up by and large the idea of the affiliation can give a not too bad introduction. As showed by [2], Li-Fi is joined with the Wi-Fi to get a nice display in outside or in the flexible establishment [13].

5.5 The solution of Light Fidelity (Li-Fi) based on its limitations

- Light can't undergo objects, so in case the recipient is unintentionally discouraged in any way, by then, the sign will immediately be evacuated.
- Collision from outside light sources like sunshine, common bulbs; and cloudy materials in transit of transmission will create a break in the correspondence.
- It perhaps works if there is a quickly visible pathway (LOS) among the transmitters and the recipient.
- Challenge with Li-Fi is the process by which the tolerant contraption will transmit to the transmitting device. One can't move the getting contraption if there ought to be an event of the indoor game-plan of the gadget as light can't invade through dividers and is adequately impeded by somebody just walks around the LED source.
- If the contraption is set up inside, one would not have the alternative to move the gatherer.
- If the mechanical gathering is set up outside, it would need to oversee changing atmospheric conditions.
- A person can't have a light that offers data to a quick-moving thing or to give data in a remote area where there are trees, dividers, and hindrances.
- Authenticity and framework consideration are noteworthy issues to be viewed by associations while giving VLC organizations.

- The huge base cost of the structures can be enhanced by colossal scale utilization of VLC through accepting this development will diminish further working costs like power charges, upkeep charges, etc.
- The use of very high frequencies (400-800THz) limits it to very short detachments and point-to-point correspondence as it might have been.
- We become subject to the light hotspot for the web gets to. In the case of the light source glitches, we lose access to the web.
- The sort of Light Source (Large LED, Smaller LED lights, Laser LEDs, etc. truly influences the momentum that can be practiced by Li-Fi plan.

5.6 Differentiation between Li-Fi and Wi-Fi

COMPARISION	LI-FI	WI-FI
Full Form	light fidelity	wireless fidelity
Invented/Coined	Prof. Harald Haas in 2011	NCR corporation on 1991
Operation	transmits data using light by the help of LED bulbs	transmits data using radio waves using wifi router
Technology	Present IrDA compliant devices	WLAN 802.11/b/g/n/ac/d standard compliant devices
Data Transfer Speed	About 1 Gbps	Ranges from 150Mbps to maximum of 2Gbps
Privacy	light is blocked by the walls hence provide more secure data transfer	walls cannot block radio waves so we need to employ more techniques to achieve secure data transfer
Frequency of operation	10, 000 times frequency spectrum of the radio	2.4Ghz, 4.9Ghz and 5Ghz
Coverage Distance	about 10 meters	about 32 meters(vary based on transmit power and antenna type)
Data density	work with high dense environment	work in less dense environment due to interference related issues
Bare minimum Components used	LED bulb, LED driver and photo detector	Routers, Modems and access points

Figure 5.6.1 : Basic difference between Li-Fi- and Wi-Fi

5.7 Misconceptions of Li-Fi technology

Li-Fi, otherwise called "Light Fidelity" is a remote optical systems administration innovation, which uses light-transmitting diodes (LEDs) to transmit information. In 2011, educator Harald Haas made a Li-Fi exhibition at the TED (Technology, Entertainment, Designs) Conference. Li-Fi is a rapid, bidirectional, and completely arranged remote correspondence of information utilizing light. Li-Fi is made of a few lights that structure a remote system. In straightforward words, Li-Fi is the web through Light. Watch the video underneath to perceive how Li-Fi functions. Here is some misconceptions of Li-Fi technology.

- **It conflicts with radiofrequency**

  Radio Frequency Technology like Wi-Fi can be upset by an assortment of gadgets, for example, cell phones, cordless telephones, microwaves, and other Wi-Fi systems. Li-Fi utilizes the obvious light range, which works at a higher recurrence than the Radio Waves range and subsequently doesn't meddle with Wi-Fi. Along these lines, Li-Fi can be utilized in medical clinics, planes and power plants without the dread of impedance from radiofrequency gadgets [25].

- **It provides less security than Bluetooth and Wireless Fidelity (Wi-Fi)**

  As opposed to Wi-Fi, light doesn't experience dividers and can without much of a stretch be contained in a physical space. This gives the chance of making secure specially appointed systems in meeting rooms which can enable members to share information without the danger of information spilling out. Some assigned rooms can be utilized as high-security territories with their Li-Fi systems, detaching them from different zones of the structure where there may be the association of defenseless Internet of Things (IoT) gadgets. Pure Li-Fi is as of now building up the security segments and innovations that will help security authorities and specialists convey progressively secure remote correspondences [25].

- **It will never be made moderate to the normal customer**

Once more, this is another misguided judgment. Even though the Li-Fi items can be extravagant going from £2500 to £5000, as far as cost, various organizations are progressing in the direction of the scaling down of Li-Fi items to make it reasonable for everybody and not simply organizations [25].

- **Just like Wi-Fi, Li-Fi will serve in our pockets**

  Indeed, except if your garments enable light to go through them, Li-Fi won't work if a Li-Fi empowered gadget is in your pocket. The Li-Fi beneficiary on the gadget must be presented to a Li-Fi prepared LED light [25].

- **Li-Fi is genuinely an unsettled innovation**

  Hang tight, let us first look into the meaning of problematic innovation". Troublesome innovation is characterized as an innovation uprooting a setup innovation shaking up a whole industry or notable item that makes a new industry. Instances of troublesome innovations are Peer-to-Peer ride-sharing stages like Uber and Lyft. Netflix, a membership-based spilling administration, can likewise be viewed as a troublesome innovation. Li-Fi will work related to existing Wi-Fi systems to give quicker and progressively secure web and information transmissions. Along these lines, Li-Fi ought not to be viewed as a troublesome innovation at this time [25].

- **Li-Fi won’t work in the dark and Obscurity**

  The facts demonstrate that any Li-Fi recipient would need turning on LED lights to get information transmission. This implies Li-Fi innovation can't be utilized in dull rooms. Nonetheless, a potential answer to tackle this issue is to diminish LEDs low enough so our eyes can't see them. A group of scientists, from Dartmouth College in the United States, areas of now chipping away at a task to encode information into ultra-short and indistinct light driving forces. The undertaking is designated "Dark-Light" [25].

- **There is currently only one organization that is commercializing Li-Fi**

  The facts confirm that pure Li-Fi was the principal organization that begat the term Li-Fi, where Professor Harald Haas played out a showing at the Global TED talk gathering

in July 2011. This brought about the development of various new Li-Fi organizations that are as of now moving in the direction of the commercialization of Li-Fi innovation. Oledcomm is a side project from the University of Versailles dependent on examining on Visible light correspondence that started in 2005. VLNComm is the main organization in Visible Light Communication (VLC) or supposed Li-Fi Technology, which is an elective information correspondence strategy for remote applications that utilizations optical vitality to give enlightenment and information transmission simultaneously [25].

- **Li-Fi can't work under daylight (Sunlight)**

  This isn't the circumstance. It is normally expected by various people that Li-Fi can't work under sunshine conditions. The usage of optical channels will engage Li-Fi to work outside without impedance from any ordinary or fake sources. These channels diminish recipient drenching. Basic and progressed isolating can similarly be used to confine the level of impediment. Pure Li-Fi communicated that Li-Fi relies upon recognizing the fast changes in light power and not on the aggregate or steadily fluctuating levels achieved by regular breaks in daylight or sunshine. Li-Fi Technology adjusts the light at high rates while the sunlight exhibitions like an unfaltering light source which can be filtered through at the recipient [25].

- **The LED lights used to transmit information (data) have a very short life expectancy**

  As opposed to glowing lights, LED lights have a general life expectancy of around 50,000 hours. At the end of the day, whenever utilized for 12 hours every day, the LED light will last in any event 11 years. Whenever utilized for 8 hours per day, the LED light can keep going for a long time. As should be obvious, LED lights can have an exceptionally long life expectancy [25].

- **You can't utilize Li-Fi in remote zones or in towns where living conditions are amazingly poor and restricted**

All things considered, that isn't the situation. In April 2017 out of a town situated close to Liberia, an organization called Li-Fi Led Côte d'Ivoire introduced sun oriented boards to give lasting lighting to its occupants. They additionally gave LED establishment to the whole town. Through these LED lights, the inhabitants approach the web and TV with no wire or Wi-Fi association on account of Li-Fi Technology. Li-Fi can work in remote regions with the correct gear [25].

- **Li-Fi isn't a bi-directional technology**

  As per the Merriam Webster word reference, bi-directional methods including, moving or occurring in two inverse bearings. For the most part, a Li-Fi framework is made of Trans-beneficiaries where one recipient is at the SOURCE and the other one is at the DESTINATION. At the point when the light flashes, the Trans-beneficiary detects the progressions at the Destination point through a photodiode that unscrambles the information. Pure Li-Fi characterizes Li-Fi as a bi-directional remote interchanges innovation that permits fast transmissions in both uplink and downlink all the while [25].

- **Li-Fi is strictly a line of sight technology**

  The observable pathway can be characterized as electromagnetic radiation or acoustic wave proliferation going immediately from a source to a beneficiary. In more straightforward terms, it is electromagnetic waves going in a straight line. Since light can ricochet off of a surface, Li-Fi can't be completely viewed as an observable pathway innovation. With an immediately viewable pathway, an extremely quick pace of correspondence can be accomplished yet when light skips off of a divider and different items, the pace of correspondence will be brought down. PureLiFi states that "Li-Fi is a phone correspondence framework and the information rate isn't reliant on the viewable pathway however on the sign quality at the gadget. Signal quality can be characterized by the proportion of the ideal information versus any meddling information and clamor." [25].

REFERENCES

[1] Farooq Aftab, Muhammad Nafees Ulfat khan, Shahzad Ali, "LIGHT FIDELITY (LI-FI) BASED I NDOOR COMMUNICATION SYSTEM,", International Journal of Computer Networks & Commun cations (IJCNC), Vol.8 No.3, pp. 21-29 May 2016

[2] Niraj.S.Dhangar, Prof.S.M.Patil, "LIGHT FIDELITY (LI-FI)-THE FUTURE TECHNOLOGY IN WIRELESS COMMUNICATION,", International Journal of Electrical and Electrical and Engineers, vol. 2, pp. 74-79, July-December 2015.

[3] Sheetal Singh and Arti Vaish, "Li-Fi: The Emerging Technology and the green avatar of Wi-Fi," International Journal of Recent Research Aspects, Vol. 5, pp. 111-114, March 2018.

[4] Pavas Goswami, Manoj Kumar Shukl, "Design of a Li-Fi Transceiver ," Wireless Engineering and Technology, Vol.8 No.4, pp. 71-86, October 2017.

[5] V.K.G.Kalaiselvi ,A.Sangavi, Dhivya, "Li-Fi technology in Traffic light," Second International Conference On Computing and Communications Technologies(ICCCT'17), pp. 404-407, 2017

[6] Ashmita Shetty, "A Comparative Study and Analysis on Li-Fi and Wi-Fi ," International Journal of Computer Applications (0975 – 8887), Vol. 150 No.6, pp. 43-48, September 2016 .

[7] Liang Yin, Mohamed Sufyan Islim, and Harald Haas, "LiFi: Transforming Fibre into Wireless," Broadband Access Communication Technologies XI, vol. 10128, pp. 1-9, 2017.

[8] D. Khandal and S. Jain, "Li-fi (light fidelity): The future technology in wireless communication," International Journal of Information & Computation Technology , vol. 4, no. 16, pp. 1687–1694, 2014.

[9] Xu Bao, Guanding Yu, Jisheng Dai, Xiaorong Zhu, "Li-fi: Light fidelity-a survey," Wireless Networks , vol. 21, no. 6, pp. 1879–1889, 2015.

[10] Harald Haas, Liang Yin, Yunlu Wang, Cheng Chen," What Is Li-Fi?," Journal of Lightwave Technology, vol. 34, pp. 1533-1544, December 2015.

[11] Emilie Bialic, Luc Maret, Dimitri Kténas, "Specific innovative semi-transparent solar cell for indoor and outdoor LiFi applications," Applied Optics. Vol. 54, pp. 8062-8069, September 2015.

[12] Polshetwar Poonam V. and Mr. Saad Siddiqui, "Li-Fi Technology," International Journal of Computer Science and Information Technologies, vol. 5, no. 6, pp. 8031-8032, 2014

[13] E Ramadhani and G P Mahardika, "The Technology of LiFi: A Brief Introduction," IOP Conference Series: Materials Science and Engineering, vol. 325, pp. 012013, 2018.

[14] M.D. Reddy and S. Sonali ,"Li-Fi Based Patient Monitoring System", International Journal of Scientific and Technology R esearch, vol. 04, no. 37, pp. 7972-7975, 2015.

[15] Monica Leba ; Simona Riurean ; Andreea Lonica, "LiFi — The path to a new way of communication,", 12th Iberian Conference on Information Systems and Technologies (CISTI), 2017

[16] Grzegorz Blinowski," Security issues in visible light communication systems," IFAC-PapersOnLine, vol. 48, pp.234-239,2015.

[17] Harald Haas, "LiFi is a paradigm-shifting 5G technology," Reviews in Physics, vol. 3, pp. 26-31, 2018

[18] Pradip Kumar Sharma, Jung Hyun Ryu, Kyung Yeob Park, Jin Ho Park, Jong Hyuk Park, "Li-Fi based on security cloud framework for future IT environment," Human-centric Computing and Information Sciences, vol. 8, 2018.

[19] Yaseein Soubhi Hussein, Amresh Chetty Annan, " Li-Fi Technology: High data transmission securely," Journal of Physics: Conference Series, vol. 1228, pp. 012069,2019.

[20] Vijey Thayananthan, Omar Abdulkader, Kamal Jambi, Alwi M. Bamahdi, "Analysis of Cybersecurity Based on Li-Fi in Green Data Storage Environments," IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017.

[21] Dr. Naveen Rathee, Shreyaa Nagpal, Abhinav Malik, Charvi Khandelwal, "An Efficient Intelligent System for Data Communication Using LIFI Technology," INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, vol.13, pp. 5044-5050.

[22] Prateek Gawande , Aditya Sharma , Prashant Kushwaha, "Various Modulation Techniques for LiFi," , International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, pp. 121-125, November 2016.

[23] R. Ponnulakshmi, R. Selvakumar, "LI-FI (LIGHT FIDELITY): WIRELESS COMMUNICATION USING LED," International Journal of Scientific Research and Modern Education (IJSRME),vol.1, pp. 474-479, 2016.

[24] Anwesha Chakraborty, Trina Dutta, Sushmita Mondal, Dr. Asoke Nath, "Latest advancement in Light Fidelity (Li-Fi) Technology," International Journal of Advance Research in Computer Science and Management Studies Volume 5, pg. 47-53, November 2017.

[25] Li-Fi Misconceptions, available at<< https://www.lifitn.com/blog/2018/8/5/li-fi-misconceptions>>, last accessed on 03-11-2019 at 1:45 PM.

Final Check

ORIGINALITY REPORT

28%	8%	16%	18%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Grzegorz Blinowski. "Security issues in visible light communication systems", IFAC-PapersOnLine, 2015 Publication	6%
2	E Ramadhani, G P Mahardika. "The Technology of LiFi: A Brief Introduction", IOP Conference Series: Materials Science and Engineering, 2018 Publication	5%
3	Grzegorz J. Blinowski. "Practical Aspects of Physical and MAC Layer Security in Visible Light Communication Systems", International Journal of Electronics and Telecommunications, 2016 Publication	3%
4	ijsrcseit.com Internet Source	2%
5	Submitted to Daffodil International University Student Paper	1%
	Submitted to Arab Open University	