THE PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITYMOHAMED BOUDIAF - M'SILA

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
COMPUTER SCIENCE DEPARTMENT

N°: ……..

DOMAIN: MATHEMATICS AND COMPUTER SCIENCE
BRANCH: COMPUTER SCIENCE
SPECIALTY: NETWORKS AND INFORMATION AND COMMUNICATION TECHNOLOGY

Dissertation submitted in partial fulfilment of the requirements for the Degree of MASTER

By: Djaalab Amira

TOPIC:

Key management using visible light communication

Jury composed of:

Mr. Azedine Attir	**University of M'sila Supervisor**
……	**University of M'sila protractor**
……	**University of M'sila Examiner**

Academic Year: 2019 /2020

Dedication

I dedicate this to My parents

Acknowledgements

I would like to sincerely thank all the persons that helped me during this year, during the previous years and to those that will help me in the years to come!

I wish to express my sincere thanks and appreciation to my supervisors Attir Azedine for his patience, continuous assistance and his support to me with the necessary knowledge and guidance!

I thank the jury members who accepted the verdict for this letter!

Thanks my Brothers Abd Hakim and Salah eddine for your advice, support in pursuing a Master and for directing me to better!

I also would thank my mother for helping me in my worst moments!

I would like to deepest grateful to all my beautiful family and my friends for all their love and support, thank you so much my husband Hassan!

I thank also Dounia and Roumiassa for be close to me, for their many lessons and for all that you did for me!

Thank you for guiding me to become a better person!

I succeed thanks to you and I fail because of me!

Table of content

List of figures

List of tables

List of Terminology

VLC	Visible Light Communication
RF	Radio Frequency
MITM	Man In The Middle
LED	Lighting Emitting Diodes
IS	Image Sensor
PD	Photo Detector
PBKDF	Password Based Key Derivation Function
OOK	On-Off-Keying
VPPM	Variable Pulse Position Modulation
VLCC	Visible Light Communication Consortium
CSK	Color Shift Keying
MAC	Media Access Control
LOS	Line-Of-Sight
NLOS	Non Line-Of-Sight
PFKS	Phase-Frequency Shift Keying
LD	Laser Diode
PPM	Pulse Position Modulation
PWM	Pulse Width Modulation
LLR	Log Likelihood Ratio
IM	Intensity Modulation
DD	Direct Detection
OWC	Optical Wireless
FPGA	Field Programmable Gate Array
LIFI	Light-Fidelity
ITS	Intelligent Transport System
PER	Packet Error Rate
CMOS	Complementary Metal-Oxide-Semiconductor
LAN	Local Area Network
SAS	Serial-Attached SCSI
OOB	Out Of-Band
SIB	Seeing Is Believing
IR	Infra-Red
NFC	Near-Field Communication
QR	Quick Response Code
PBE	Password Based Encryption
DK	Derived Key

General Introduction

General introduction:

Due to the dramatic increase in high data rate services and in order to meet the demands of the fifth-generation (5G) networks [1], Visible light communication (VLC) has been proposed as an alternative standard to radio-based wireless networks. Because of its physical characteristics, and in line with the slogan "what you see is what you send", VLC is considered a secure communication method [2]. where it refers to wireless communications using a spectral range from 380 to 780 nm for the transmission of information This type of communication has several advantages respect to the RF wireless communications, such as free use of the visible spectrum, increased security in communication, the bandwidth 300THz and null electromagnetic interference.

In VLC, the receiver receives the signals, if it is opposite the transmitter face to face, or they cannot receive any information from the transmitters if they are in a different direction, this is what shows security immunity in wireless communication to the security issues. also we can use visible light for lighting and communication both. Due to the advantages of VLC, it can become a related wireless communication technology that meets all kinds of future applications like in GPS, transportation system (vehicle to vehicle V2V and infrastructure to vehicle I2V....), smart cities and smart homes, visible light ID system, hospitals, airports, and in smart phone etc.

This thesis is divided into three chapters, the first one introduces the visible light communication technology, all main standardizations of this type of communication, its system and thus its advantages are detailed. The different types of applications of this technology applied to the visible domain are also illustrated. The second chapter focuses on key management protocol for wireless devices, Device pairing methods and protocols in wireless communication are the points studied in this chapter, some were also shown devices pairing using visible light communication. The last chapter is devoted to putting the subject into practice. That is, the design of a visible light communication system using two wireless devices, used respectively for transmission and reception.

This thesis ends with a general conclusion on the work carried out, as well as on the various perspectives offered by all the results obtained.

Background and problem motivation:

Users often wish to configure two devices to communicate over a secret and authentic channel to exchange sensitive documents or personal messages. This is attainable via a dedicated physical connection such as a cable. However, today’s devices increasingly feature convenient, wireless communication interfaces (e.g., 802.11, Bluetooth, and WiMAX). Unfortunately, wireless communication is invisible to humans, rendering it vulnerable to Man-In-The-Middle (MITM) attacks. A MITM attack takes place when Alice and Bob believe they are communicating with each other, when in fact they are both communicating with Charlie, who is able to monitor,

General introduction

modify, inject, suppress, or otherwise tamper with Alice and Bob's intended communication without their knowledge. [3]

So the challenge lies in achieving the highest level of security in wireless communications, which has become an important aspect of daily life.

Overall aim:

This thesis concentrates on sharing a Secret key using visible light, where the LED use as transmitter and light sensor as receiver (photo detector), As an effort to achieve a required level of safety and the exploitation of light in communication, not just lighting.

An attempt is also made, in this thesis, to implement a small application mobile using visible Light.

Concrete and verifiable goals:

The goals of this thesis are listed as follows:

- ✓ generate a symmetric key by using Password-Based Key Derivation Function PBKDF
- ✓ Send key (bits) using LED-camera
- ✓ Detect key (bits) using the sensor of a smartphone.

Chapter 01:

Visible Light Communication and its applications

1.1 Introduction:

Now, the mobile data traffic is increasing drastically. This increase is due to the increase in number of devices accessing the mobile network.

Further, the online social service such as Facebook, WhatsApp and Twitter also increases the mobile data traffic. Beyond this, interference is another important issue in radio communication. According to Federal Aviation Administration (FAA), the use of mobile phones on aircraft causes interference with communication and navigational systems. The Federal Communication Commission (FCC) states that the mobile phones on aircraft will cause interference with ground system towers. One of the major need of any wireless communication system is that it should have very low latency. There is also a security issue in case of radio frequency communication techniques due to the penetration of waves through walls.

The increase in the transmission power of RF waves beyond a certain limit results in risks to human health. There is also power inefficiencies in case of RF communication due to the requirement of a separate setup for communication of the RF waves. [4]

Due the drawbacks of the RF communication systems, it was imperative to design new communication technology. Visible Light Communication (VLC) is a preferred communication technique because of its high bandwidth and immunity to interference from electromagnetic sources.

In this chapter, we introduce the VLC technology, standardization, system, and some of its applications.

1.2 Visible Light Communication(VLC):

The visible light communication (VLC) refers to the communication technology which uses the visible light source as a signal transmitter, the air is used as the transmission medium, and the appropriate photodiode as a signal-receiving component. Visible light should be considered as the medium for wireless transmission because it has few advantages over other standard wireless transmissions. LED's can be switched on and off faster, which helps for data transmission. To encode data in the light can be done by varying the rate at which the light flickers ON and OFF to give different strings of 1s and 0s. The intensity of the light is modulated so rapidly that human eye cannot detect, so the output appears to be constant. The photo detector at receiver side receives different strings of 1s and 0s and receiver decodes it in its original form. This data then can be saved to receiver device. In this way, data can be transferred from one computer to another computer. [5]

1.2.1 Visible light:

Visible light is the form in which electromagnetic radiation with wavelengths in a particular range is interpreted by the human brain:

- ✓ Visible light is comprised of visually perceivable electromagnetic waves.
- ✓ The visible spectrum covers wavelengths from 380 nm to 750 nm [6]

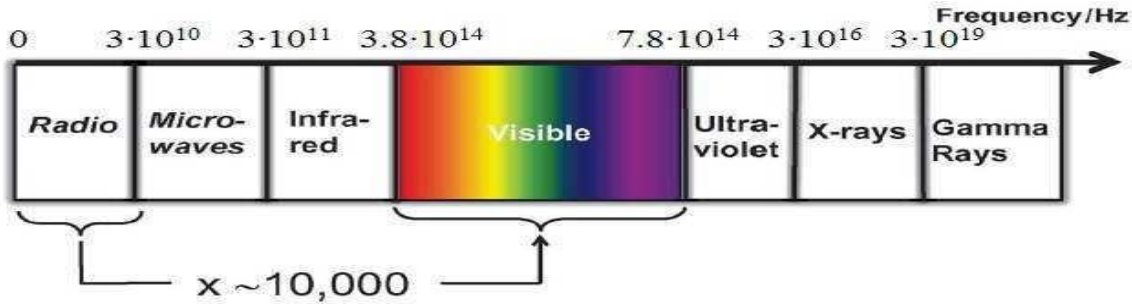

Figure 1.1. VLC Frequency Spectrum. [31]

1.3 Standardization of VLC:

To regulate transmission in VLC technology, the Institute of Electrical and Electronics Engineers (IEEE) working group IEEE 802.15.7, proposes schemes and techniques. The IEEE 802.15.7standard devises the physical layer (PHY) of VLC technology in three parts: PHY I, PHY II and PHY III specific modulation schemes and coding techniques are dedicated to each of these layers. PHY I operates from11.67 kb/s to 266.6 kb/s, PHY II operates from 1.25 Mb/s to 96 Mb/s, and PHY III operates from 12 Mb/s to 96 Mb/s. PHY III, dedicated to multiple optical sources using CSK. PHY I and PHY II use schemes such as OOK and VPPM. In Japan, VLCC proposes to use VPPM to implement communication systems in VLC technology. The VLCC member includes the following: Nippon Electric Company (NEC) Corporation, Panasonic, Toshiba Corporation, Samsung Electronics, Casio Computer, Nakagawa Laboratories, and Sharp Corporation. The activities of the VLCC consortium are to develop standards for VLC technology. In Europe, the Wireless World Research Forum (WWRF) also works on VLC technology. Its working group 5 is in charge of investigating the VLC environment. [7]

1.4 VLC system:

All VLC systems consists of two common parts namely the transmitter and the receiver. These two parts generally have three layers, namely physical layer, MAC layer and application layer. The layered architecture of VLC system is shown in figure1.2. In IEEE 802.15.7, only two layers (such as PHY and MAC) are defined for simplicity [4]:

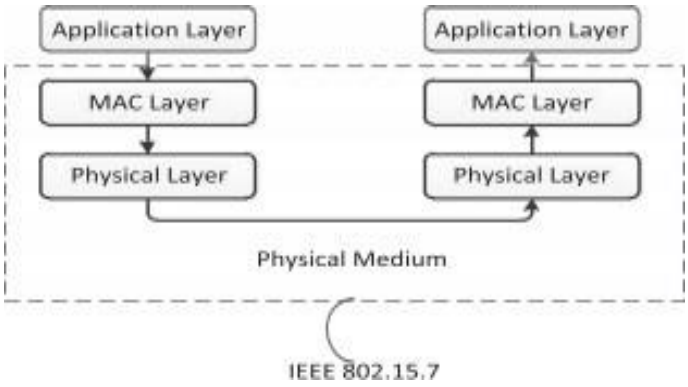

Figure 1.2. Layered architecture of VLC. [4]

1.4.1 Mac layer:

the tasks performed by Medium Access Control (MAC) layer include:

- ✓ Mobility support.
- ✓ Dimming support.
- ✓ Visibility support.
- ✓ Security support.
- ✓ Schemes for mitigation of flickering.
- ✓ Color function support.
- ✓ Network beacons generation if the device is a coordinator.
- ✓ VPAN disassociation and association support.
- ✓ Providing a reliable link between peer MAC entities.

The MAC layer support topologies like peer-to-peer, broadcast and star [4].

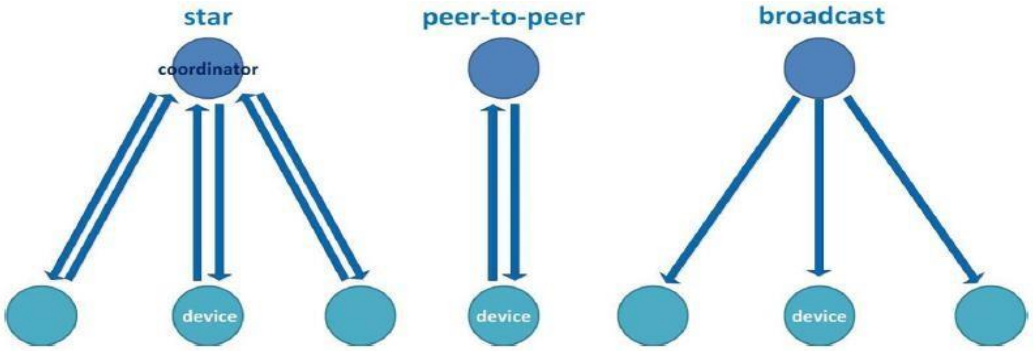

Figure 1.3. IEEE 802.15.7(VLC) topologies. [15]

1.4.2 Physical layer:

The main functions of physical layer include providing physical specification of the device and the relationship between the device and the medium. Figure 1.4 shows the typical physical layer system model of VLC.

First, the input bit stream is passed through a channel encoder. The most commonly used channel encoders are linear block codes, convolutional codes and turbo codes. The channel encoded bit stream is then passed through a line encoder to produce a line

encoded bit stream. Then it passes through a modulation module. The most commonly used modulation techniques include ON-OFF Keying, PPM and PWM. Finally, the data is fed to the LED or LD for transmission through the optical channel. The bidirectional transmission of VLC (using of one of RGB LED by transmitter and a color filter by receiver) system utilizes Wavelength Division Multiplexing (WDM) and Subcarriers Multiplexing (SCM). [4]

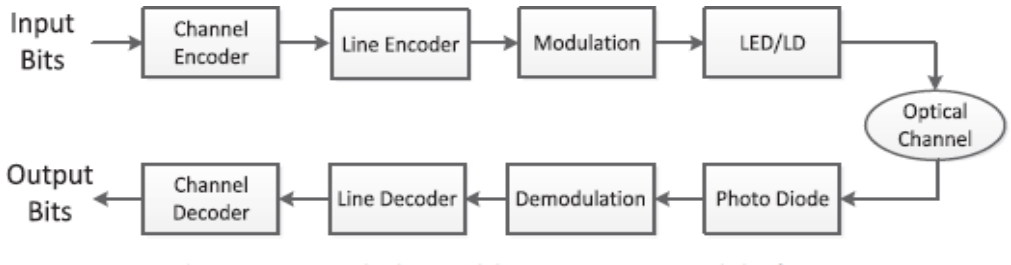

Figure 1.4. Typical physical layer system model of VLC. [15]

1.4.2.1 Coding and decoding Turbo Code:

Turbo codes are a class of concatenated and compound codes that use convolutional codes as their constituent codes. Specifically, a turbo codes consists of two Recursive Systematic Convolutional (RSC) codes with a (random) interleaver in between. The interleaver will re-shuffle the input symbols d_k to break up the low-weight error events from the first branch. the encoder of a typical turbo code is shown below:

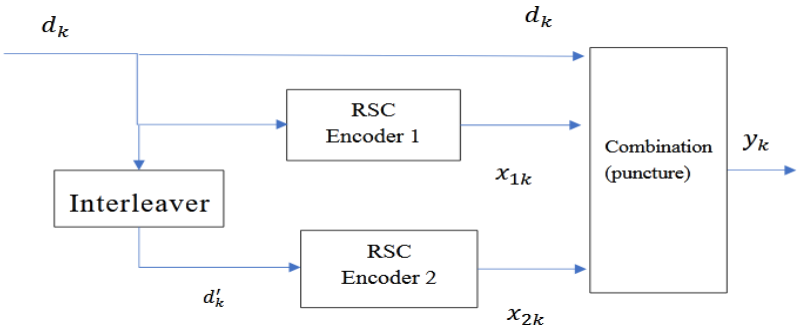

Figure 1.5. Turbo Code Encoder. [8]

The generator matrix for the two RSC encoders can be either the same or the different but is usually the same for simplicity purpose. In Figure 1.5. d_k represents the sequence of the input symbols, which comes in three replicas. The first replica stream goes directly to the output, i.e., it becomes the systematic part of the turbo code word. The second replica stream enter the first RSC encoder produces a coded sequence, denoted as X_{1k}. At the same time, the third replica stream will go into the interleaver and be re-shuffled to $d_{k'}$. The "interleaved" stream then goes to the second RSC encoder and generates coded sequence X_{2k}. The entire code word for the turbo code

consists of the systematic part and the outputs from both RSC codes and the three parts are usually multiplexed together. [8]

The key advantage for a turbo coding system is the decoding method. A turbo code uses an iterative algorithm and a soft-input-soft-output (SISO) decoding model. This soft-iterative paradigm has proven to be extremely effective. It provides near-optimal decoding capability with a manageable complexity. Since hard decoding presents only two-level quantized decision without supplying the reliability information, SISO sub-decoders are necessary in order for the iterative decoder to maximally extract the gains from both sub-decoders and to refine and improve the decoding result one iteration after another. Like any iterative system, we expect to see diminishing returns of the decoding gain after several decoding iterations. The basic decoding structure can be shown as following:

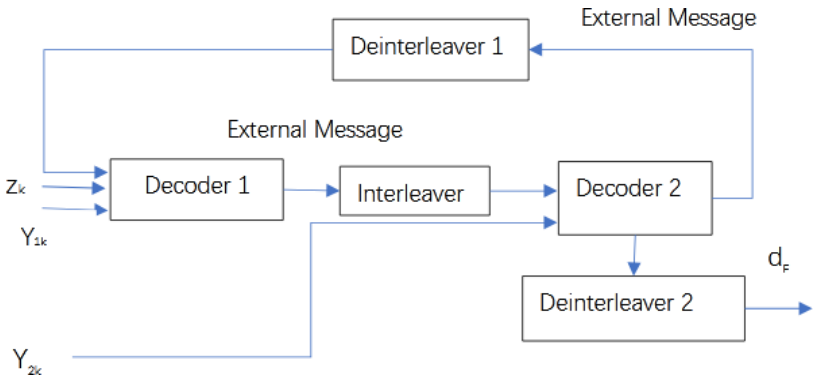

Figure 1.6. Turbo Code Decoder. [8]

The decoding system consists of 2 sub-decoders corresponding to the two component RSC codes, 2 de-interleavers and 1 interleaver. Z_k and Y_{1k} and Y_{2k}refer to the received sequence from the channel. Specifically, Z_k is the noise-corrupted version of the systematic subsequence. Y_{1k} and Y_{2k}correspond, respectively, to the noisy version of the parity subsequence from RSC1 and RSC2. Decoder 1 and 2 are the SISO sub-decoders corresponding respectively to RSC1 and RSC2.In each decoding iteration, each sub-decoder will output three parts of soft messages: system message, a priori message and extrinsic message. These soft messages take the form of log-likelihood ratio(LLR). Extrinsic message will be passed through the interleaver/de-interleaver 1, to the other sub-decoder as the priori message. If the system is well designed, then one expects to see noticeably improved perform through iterations. After a few iterations, usually 4 to 5titerations, the performance will reach the point of diminishing return, and this is where the turbo decode can stop. Please note that the total soft-output information (in the form of LLR) must combine the extrinsic information from both sub-decoders. [8]

1.4.2.2 Modulation techniques:

With comprehension of signal loss due to the distance range occurred is considered as path-loss, environmental noises, and signal to noise ratio (SNR). Various modulation schemes are used in VLC. The most prominent difference in VLC and RF technology is the VLC could not be encoded over phase and amplitude. It implies that phase and amplitude encoding cannot be employed in VLC. In VLC system, encoding is done through the intensity of light waves. The demodulation relies upon the direct detection of the data receiver. The intensity modulation is also known as direct detection modulation. [9]

Intensity Modulation (IM) is usually considered to be the most appropriate modulation technique for VLC. IM implies to modulate the desired waveform onto the instantaneous power of the carrier. The receiver extracts the data from the modulated light beam by using Direct Detection (DD). The photodetector generates a current proportional to the incident power. This current is thus transformed into a voltage by a trans impedance circuit and then the signal is processed through several filters and amplification stages until the data signal is reconstructed [10]. The modulation schemes VLC achieved higher data rates and convene the necessities of visible light to humans [9]. They are organized regarding the number of channels (carriers).

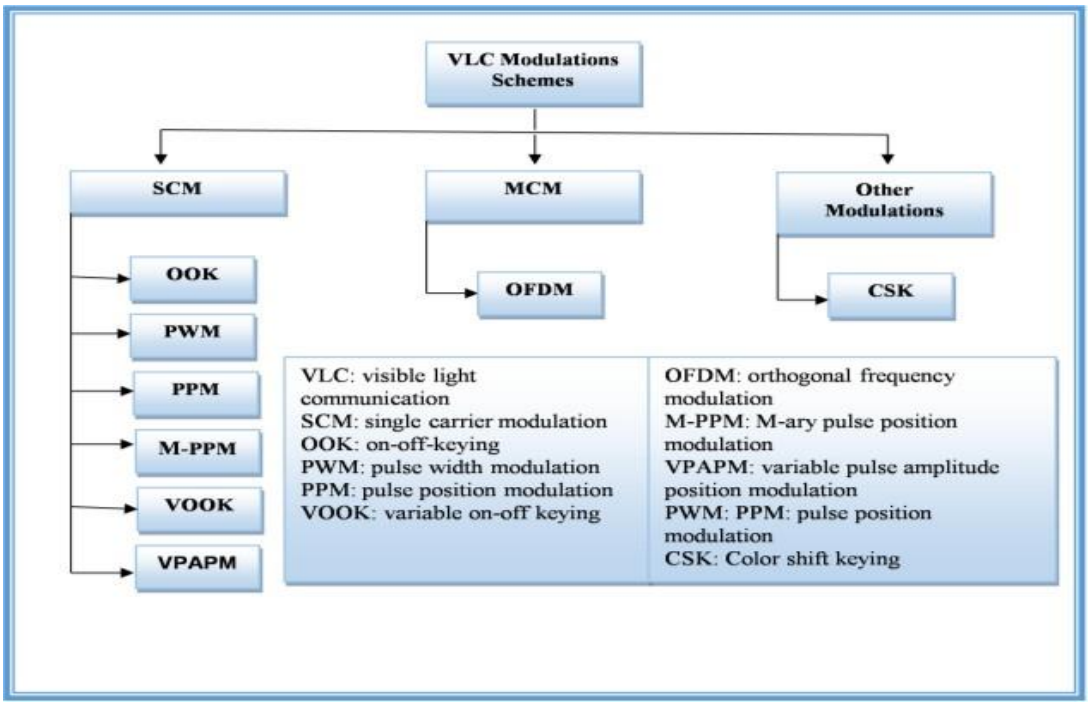

Figure 1.7. The modulation techniques VLC organized by the number of channels (carriers). [9]

a) The single carrier modulation:

✓ On Off Keying:

OOK is one of the well-known and simple modulation schemes, and it provides a good trade-off between system performance and implementation complexity. The 802.15.7 standard uses Manchester Coding to ensure the period of positive pulses is the same as the negative ones but this also doubles the bandwidth required for OOK transmission. Alternatively, for higher bit rates run length limited (RLL) coding is used which is more spectrally efficient. OOK dimming can be achieved by:

✓ Refining the ON/OFF levels:

Dimming through refining the ON/OFF levels of the LED can maintain the same data rate, however, the reliable communication range would decrease at low dimming levels.

✓ Applying symbol compensation:

dimming by symbol compensation can be achieved by inserting additional ON/OFF pulses, whose duration is determined by the desired dimming level.

On off keying (OOK) means the simplest form of amplitude-shift keying (ASK) modulation that represents digital data as the presence or absence of a carrier wave. The data is conveyed by turning the LED off and on (shown in Figure 1.8). In its simplest form a digital „1“ is represented by the light „on“ state and a digital „0“ is represented by the light “off“ state. The beauty of this method is that it is simple to generate and decode. As the maximum data rate is achieved with a 50% dimming level assuming equal number of 1sand 0s, increasing or decreasing the brightness of the LED would cause the data rate to decrease. [11]

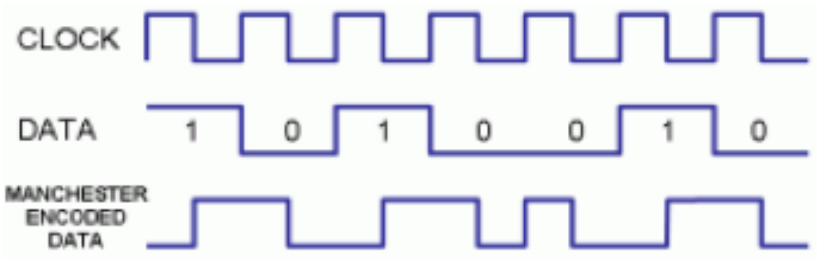

Figure 1.8. OOK modulation scheme using Manchester Coding. [11]

✓ PPM and VPPM:

L-PPM (in short PPM) as OOK is one of the simplest and intuitive form of modulation to transmit a signal in VLC.L-PPM, pulse position modulation is based on the position of the pulse inside the symbol. The symbol time Ts is divided in many time slots L. The position of the pulse is the value of the symbol. [12]

The duration of the period containing the pulse must be long enough to allow different positions to be identified, e.g. a "0" is represented by a positive pulse at the beginning of the period followed by a negative pulse, and a "1" is represented by a negative pulse at the beginning of the period followed by a positive pulse. When there is no requirement for lighting or indicating, SCPPM (Sub-Carrier PPM) is used in order to save energy. [11]

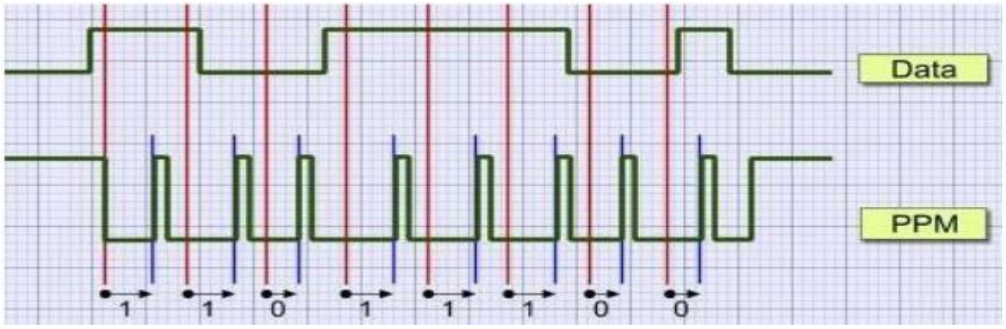

Figure 1.9.PPM example. [31]

The L-PPM is very simple to implement. It has very little susceptibility to LED non-linearity because it has only two amplitude levels. It has no flickering because every symbol is represented with the same power. In this way, the average intensity of the modulation is the same for each symbol. Moreover, the PPM dimming level can be adjusted simply by varying the duty cycle of the pulse, this variant is called variable pulse position (VPPM). [12]

Variable pulse position (VPPM) is a dimming variant of PPM. The idea is to change the time duration of the pulse according to the incoming signal intensity in order to deal with dimming: changing the time duration of the pulse means changing the duty cycle of the signal and consequently its average power and brightness. In this way, the user can change the illumination level of the room. This technique presents some problem of flickering. Changing the energy of the symbol can bring to large variations of the signal's intensity. [12]

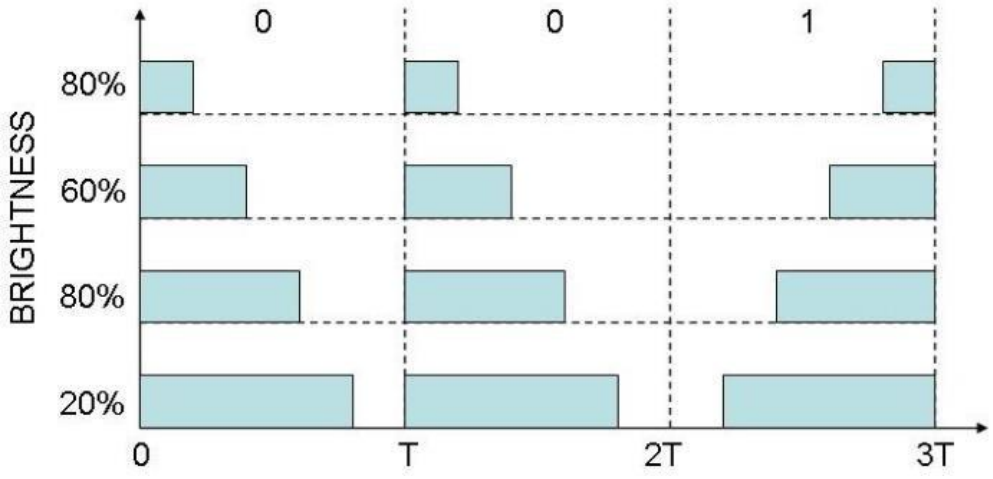

Figure 1.10. Variable Pulse Position Modulation to support dimming. [12]

b) The multi carrier modulation:

For high-speed optical wireless communication, efforts are drawn to multi-carrier modulation (MCM). Compared with SCM, MCM is more bandwidth-efficient but less energy-efficient. [11]

✓ OFDM (Orthogonal Frequency-Division Multiplexing):

OFDM is a method of encoding digital data on multiple carrier frequencies. This is a new approach to transmission in which an additional dimension is added to conventional 2D amplitude/phase modulation (APM) techniques such as quadrature amplitude modulation (QAM) and amplitude shift keying (ASK). Unlike the traditional OFDM technique, the Sub-Carrier Index Modulation Orthogonal frequency-division multiplexing technique splits the serial bit stream into two-bit sub-streams of the same length. The key idea is to use the sub-carrier index to convey information to the receiver.

As a result, the OFDM-generated signal is complex and bipolar by nature. In order to fit the IM/DD requirement imposed by commercially available LEDs, necessary modifications to the conventional OFDM techniques are required for Li-Fi.

Asymmetrically clipped optical OFDM (ACO-OFDM) is another type of optical OFDM scheme where, as well as imposing Hermitian symmetry, only the odd subcarriers are used for data transmission and the even subcarriers are set to zero. Therefore, the spectral efficiency of ACO-OFDM is further halved. Since only a small DC bias is required in ACO-OFDM, it is more energy-efficient than DCO-OFDM. To incorporate dimming support into optical OFDM, reverse polarity optical OFDM (RPO-OFDM) was proposed to combine the high rate OFDM signal with the slow rate PWM signal, both of which contribute to the overall illumination of the LED.As an alternative to ACO-OFDM, flip-OFDM and unipolar OFDM (U-OFDM) can achieve comparable bit error ratio (BER) performance and spectral efficiency. A novel modulation scheme, named enhanced unipolar OFDM (eU-OFDM), allows a unipolar signal generation without additional spectral efficiency loss as in ACO-OFDM, PAM-DMT, flip-OFDM and U-OFDM. Recently, an alternative to OFDM has been proposed, which uses the Hadamard matrix instead of the Fourier matrix as an orthogonal matrix to multiplex multiple data streams. [11]

c) Other modulation:

✓ Color shift keying (CSK):

CSK is an IM scheme outlined in IEEE 802.15.7, where signals are encoded into color intensities emitted by red, green and blue (RGB) LEDs.

In CSK, incoming bits are mapped on to the instantaneous chromaticity of the colored LEDs while maintaining constant average perceived color. By combining different colors of light, the output data can be carried by the color itself and hence

the intensity of the output can be near constant. Mixing of RGB primary sources produces different colors, which are coded as information bits. The x-y chromaticity diagram shows the color space and associated wavelengths in blue text (units are nm). The advantages of CSK over conventional IM schemes are twofold. Firstly, since a constant luminous flux is guaranteed, there would be no flicker effect over all frequencies.

Secondly, the constant luminous flux implies a nearly constant LED driving current, which reduces the possible inrush current at signal modulation, and thus improves LED reliability. Based on CSK, metameric modulation (MM) was developed and it can achieve higher energy efficiency and provide further control of the color quality, however, with the disadvantage of this system is the complexity of both the transmitter and the receiver. It requiring an additional and independently controlled green LED. [11]

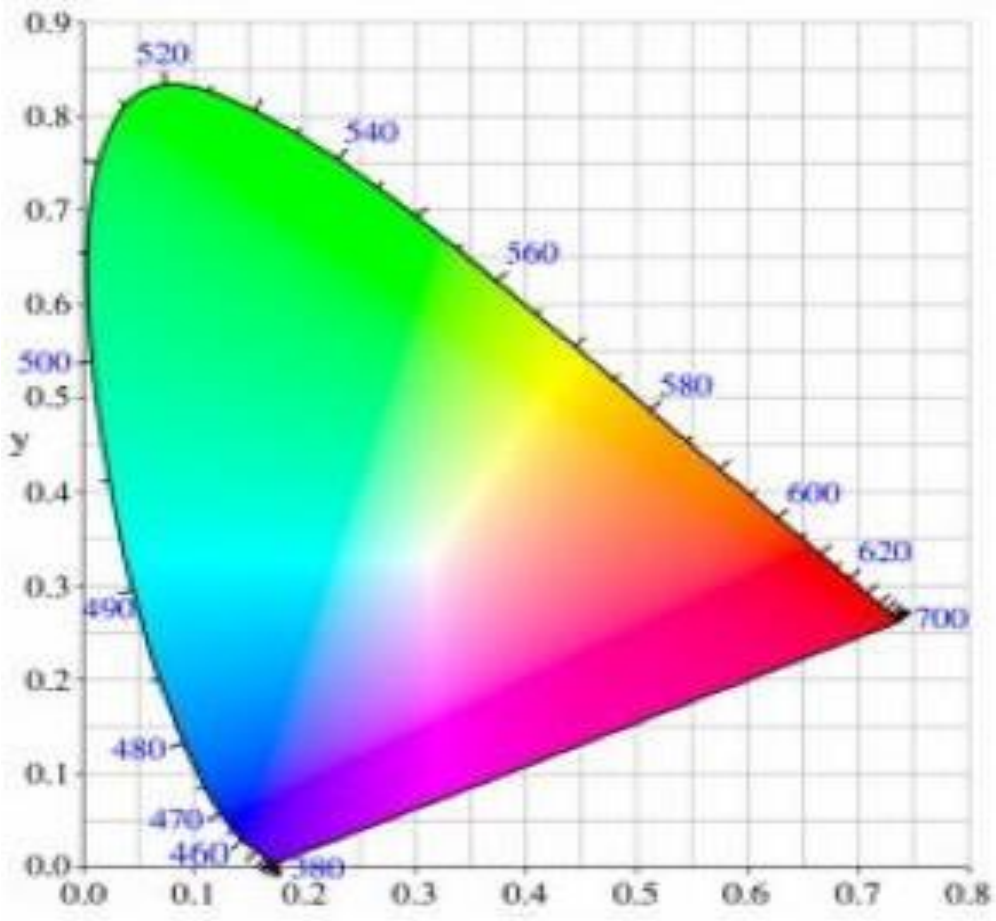

Figure 1.11. RGB LEDs that combines different wavelengths for CSK. [11]

The table 1.1 is summarized comparison between different modulation techniques.

Table 1.1. Comparison of different modulation techniques. [11]

PARAMETERS	OOK	PPM	OFDM	CSK
Bit rate, Rb	$1x10^6$	$1x10^6$	-	20mbps
Power Efficiency(Ep)	Low	High	Moderate	Low
No. of bits or bit resolution n(M)	10^3	M=3	256(Number of subcarriers)	-
Spectral Efficiency(Es)	High	Low	High	Moderate
Samples per symbols	10	250	128(Number of symbols)	number of samples (up to 25)
Bit duration, Tb	10^{-6}	10^{-6}	-	-
System Complexity	Low	Moderate	High	High
Eb/No	1:10	-10:5	[0:1:15]	-
Sampling time,Ts	10^{-7}	$0.375x10^{-6}$	-	oversampling rate of 25 samples per symbol

More than VLC technology is part of the set of optical wireless communications (OWC). Hence, the physical optical principles can apply to the VLC systems. In fact, the carrier in VLC is the visible rays used for illumination. VLC typically characterized by a non-negative and non-coherent signal transmission. It respects the communication principle in which three main parts are considered: a transmitter, a channel and a receiver. For a system corrupted by the additive white Gaussian noise (AWGN), the transmission is always governed by:

$$\mathbf{r}_i = \mathbf{H}s_i + \omega_i \qquad (1)$$

Where $\mathbf{r_i}$ and $\mathbf{s_i}$ are the received and the transmitted sets of symbols respectively, **H** is the channel response and $\boldsymbol{\omega_i}$ the channel noise. A suitable model for VLC communication systems is depicted in Figure 1.12. It shows two electrical domains and one optical domain. The modulated signal, added to a DC voltage is used to power the LED, this constitutes the transmitter. The LED in its operation produces the light and at the same time, convey the information through the channel. The receiver is made of the photo detector (PD) and the demodulator. The PD detects the light and produce an electrical signal composed of the message plus noise. Part of the noise here is produced by the channel even though in the model, we represent the total noise in the electrical domain. This is due to the fact that the PD converts both the message and the optical noise into an electrical current. [7]

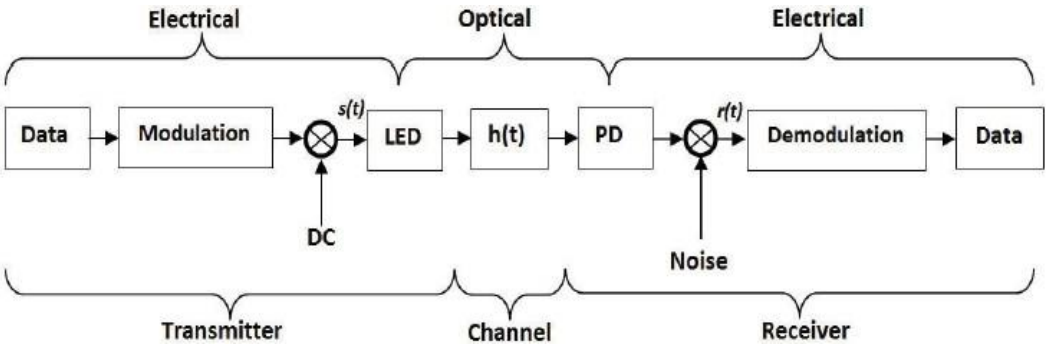

Figure 1.12. Model of VLC communication system. [7]

1.4.3 The VLC channel:

In communication, the channel represents the space between the transmitter and the receiver. It is characterized by its ability to transmit the carrier signal, and, it is influenced by many factors such as attenuation, interference and noise. In VLC technology, the channel is the space between the LED and the PD. It is mathematically represented by its transfer function H (see (1)). Two main types of channels are considered in VLC communication systems: the single VLC channel involving a single LED and a single PD, and the multichannel VLC systems in which the transmitter is made of multicolor LEDs. In this second case, the PD is made of more than one detector, each of them being sensitive to a color from the transmitter. [7]

1.4.3.1 A single VLC channel (single input-single output system (SISO)):

In single VLC channel, one LED and one PD are used to achieve transmission. The capacity C_{SISO} of the transmission link is given by:

$$C_{siso=} log_2(1 + \frac{g^2 P_t}{\sigma^2 B}) \qquad (2)$$

Where P_t, independent of the illumination, denotes the transmitter power, B the transmission bandwidth, σ^2 the variance of the total noise in an AWGN channel, and g the channel gain. The quantity g^2P_t/σ^2B represents the SNR characterizing the channel. The distribution link is organized in two different types [7]:

a) Line-Of-Sight (LOS direct and non-direct) link:

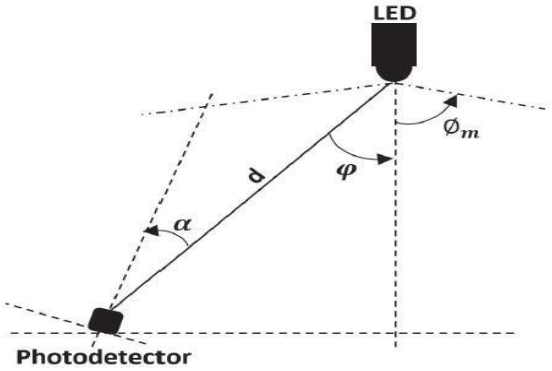

Figure1.13. Non-direct line-of-sight (ndLOS) distribution of a single ray. [7]

In LOS link, there is a straight link without obstacle between the LED and the PD (see Figure 1.13). We distinguish the direct LOS (dLOS) in which the LED is linked to the PD with 0o incidence ($\phi = 0$), and the non-direct LOS (ndLOS) in which the incidence is not null (ϕ 6= 0). dLOS and ndLOS links are similar in terms of model. In LOS VLC link, (1) becomes:

$$\mathbf{r}_i = \mathbf{H}_{LOS}\mathbf{s}_i + \omega_i, \tag{3}$$

Where HLOS is the LOS channel response. This model (3) was used to describe the VLC transmission system. The diffuse link model of a LOS VLC transmission is represented in Figure 1.13. The bandwidth in this situation can be determined by the summation of the LOS and diffuse component of the received signal. The transmission gains g(LOS) is given by:

$$g_{(LOS)} = [\frac{(\xi+1)A}{2\pi d^2}].cos^{\xi}(\varphi).T_f(\alpha).g(\alpha).cos(\alpha), \tag{4}$$

Where the incidence angle $\varphi$is given by $0 \leq \varphi \leq \phi_m$, $T_f(\varphi)$ is the transmission filter and $g(\alpha)$ the concentration gain. d represents the minimum distance between the LED and the PD. It is to be noted that g(LOS) is null for $\varphi > \phi_m$. The VLC channel is detailed with more distribution options and different situations is evaluated to characterize the transmission environment. [7]

b) Non-Line-Of-Sight (NLOS) link:

In NLOS VLC system, the light rays from the LED reach the PD after single or multiple reflections; this is due to an obstacle between the sender and the receiver. In a typical NLOS link between sender and receiver, the channel impulse response is seen as an infinite sum of light rays after many reflections, and can be expressed by:

$$\mathbf{H}_{NLOS} = \sum_{k=0}^{\infty} h^{(k)}, \tag{5}$$

Where $h^{(k)}$ is the impulse response of rays undergoing the $k^{(th)}$ path. However, this equation can be rearranged by subdividing the indoor environment into a finite number of portions. The transmission is characterized in this case by a transmission equation using the LOS transfer matrix multiplied by a coefficient ρ characterizing the NLOS link, for a NLOS link, (1) becomes [7]:

$$\mathbf{r}_i = \mathbf{H}_{NLOS}\mathbf{s}_i + \omega_i = \rho\mathbf{H}_{LOS}\mathbf{s}_i + \omega_i. \quad (6)$$

1.4.3.2 Multi-channel VLC systems:

Multi-carrier communication systems can be implemented over the VLC channel by using more than one color LED to inject the message signal to the channel. In this situation, we have finite numbers n and z of LEDs and PDs used as antenna and detectors respectively. n can be divided by the number m of groups of LEDs to obtain the number of LEDs per group. The transfer matrix in multi-carrier VLC systems is given by:

$$\mathbf{H}_{multi} = \begin{bmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,n} \\ h_{2,1} & h_{2,2} & \dots & h_{2,n} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ h_{z,1} & h_{z,2} & \dots & h_{z,n} \end{bmatrix},$$

Where the entries $\mathbf{h_{i,i}}$ represent the front-end gain between the $\mathbf{i^{th}}$ LED and the corresponding PD, and $\mathbf{h_{i,j}}$ represent the crosstalk gain between the $\mathbf{i^{th}}$ LED and the $\mathbf{j^{th}}$ PD. If there is no crosstalk, $\mathbf{H_{multi}}$ becomes a diagonal matrix with $h_{i,i}$ entries. The channel capacity $\mathbf{C_{multi}}$ in multi-carrier VLC is given by:

$$C_{multi} = \Gamma C_{siso} \quad (7)$$

Where Γ =min (n, z) and C_{SISO} is given in (2). [7]

1.4.4 The VLC transmitter:

A VLC emitter is a device that transforms data into messages that can be sent over the free space optical medium by using visible light. The purpose of the VLC emitter is to emit light and to transmit data at the same time. However, the data transmission must not affect in either way the primary goal of the appliance, which is illumination or signaling. From this concern, the VLC emitter must be able to adapt to the lighting requirements. It means that it is supposed to use the same optical power or if the application requires it, to allow for dimming. In addition, the VLC emitter must not induce any noticeable flickering.

The core component of the VLC emitter is the encoder which converts the data into a modulated message. The encoder commands the switching of the LEDs according to the binary data and to the imposed data rate. The binary data are thus converted into an amplitude modulated light beam [13]. in this context, we find two types of LEDs are used in VLC systems:

- The single-color LED.
- The multicolor LED groups in one package multiple single-color LEDs. The most used multicolor LED is the red-green-blue (RGB) LED. [4]

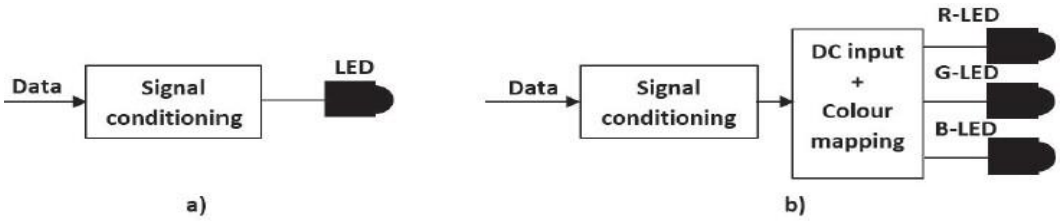

Figure 1.14. VLC transmitters: **a)** the single LED transmitter, **b)** A 3 channels VLC transmitter. [13]

1.4.5 The VLC receiver:

The VLC receiver is used to extract the data from the modulated light beam. It transforms the light into an electrical signal that will be demodulated and decoded by the embedded decoder module.

Depending on the required performances and the cost constraints, the decoder can be a microcontroller or a FPGA. The careful design of the VLC receiver represents a serious issue because in most applications, the VLC receiver's performances have the greatest influence on the performances of the VLC system, determining the communication range and the resilience against interferences.

Generally, the VLC receivers are based on photosensitive elements, which have high bandwidth and offer the possibility of high-speed communications. However, since the incident, light is not only due to the emitter but also from other light sources (artificial or natural); the receiver is subject to significant interferences. The performances of the VLC receiver can be enhanced using an optical filter that rejects the unwanted spectrum components, such as the IR component. [13]

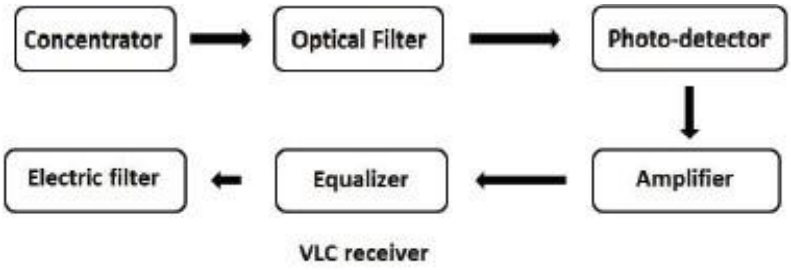

Figure 1.15. Architecture of a VLC receiver. [13]

1.5 Applications of Visible Light Communication:

VLC attractive for practical use because of its high bandwidth and low power consumption and non-licensed channels. Among applications that use VLC, we mention:

1.5.1 Light Fidelity (Li-Fi):

Light Fidelity (Li-Fi) is one of the future technology in wireless communication area. Li-Fi is similar to Wireless Fidelity (Wi-Fi). Li-Fi is bidirectional communication with very high speed and is a fully networked communication. In this technology, the information is transmitted by varying the intensity of the light. This variation is faster than human eye can capture. The data transmission in Li-Fi uses LED bulbs with transceiver and it is about 100 times faster than Wi-Fi. Li-Fi technology was proposed by the German scientist Harald Haas. [4]

Figure 1.16. Symbol of Li-Fi and Wi-Fi. [4]

Li-Fi uses the license free light spectrum and the communication is possible through use of LED bulbs. The visible light communication spectrum has no side effects. In this spectrum, 10,000 times more space is available. Li-Fi is the fast and cheap optical version of Wi-Fi. [4]

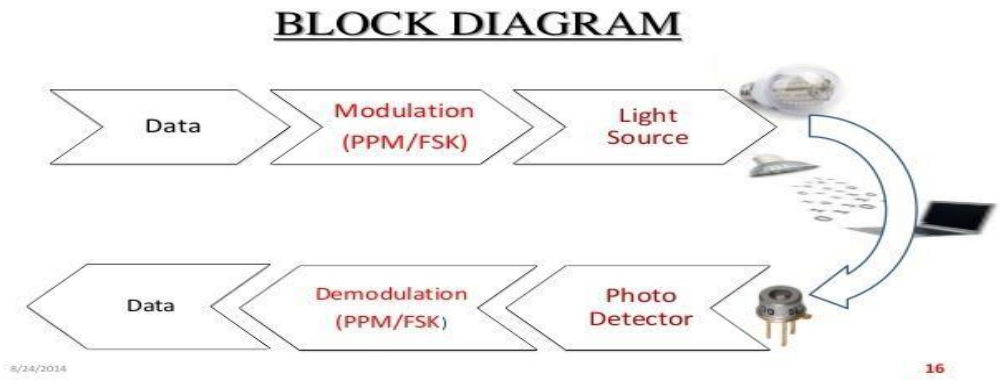

Figure1.17. Block diagram of Li-Fi Technology. [4]

The table 1.2 below shows the comparison between Li-Fi and Wi-Fi Technology:

Table 1.2. Comparison between Li-Fi and Wi-Fi. [4]

Parameters	Li-Fi [Light Fidelity]	Wi-Fi [Wireless Fidelity]
Range	10,000 times broader than that of RF	much lesser than the spectrum range of VL
Speed	High	High
Data density	High	Low
Security	High	Medium
Reliability	Medium	Medium
Power available	High	Low
Transmit/receive power	High	Medium
Ecological impact	Low	Medium
Device-to-device Connectivity	High	High
Obstacle interference	High	Low
Cost	Cheaper than Wi-Fi because it uses light	Costlier than Li-Fi because it uses radio spectrum
Market maturity	Low	High

1.5.1.1 Advantages of Li-Fi:

- ✓ It supports the user with more than sufficient communication speed for downloading movies, music, games and all in very less time.
- ✓ Capacity: Light has 10,000 times wider bandwidth than radio waves
- ✓ Efficiency: Since the LED, light consumes only very little energy, the Li-Fi technology is highly efficient.
- ✓ Availability: The transmitters and receivers for this communication is available locally.
- ✓ Security: Light waves are more secure than electric waves because they cannot penetrate through walls.
- ✓ Utilization: The use of Li-Fi technology is mainly concentrated in the areas where Wi-Fi cannot be used such as under water, aircraft cabins and nuclear power plant.
- ✓ Safety: Light communication methods like Li-Fi are safe as compared to radio means of communication because Li-Fi is not able to penetrate through the body. [4]

1.5.1.2 Limitations of Li-Fi:

- ✓ Interference from natural light sources present within the communication medium.

- ✓ The system works only if there is a line-of-sight between transmitter and receiver.
- ✓ Reliability issues.
- ✓ Coverage area. [4]

1.5.2 Indoor Positioning:

The advantage of using VLC over the traditionally existing indoor positioning technique is that, LED supported indoor localization techniques provide the advantages of high accuracy, no extra equipment for deployment, high security and short response. There are two methods for indoor location estimation using VLC: Trilateration, Angulation.

In trilateration approach, the target location is estimated by measuring the distances from multiple reference points with known coordinates. The distances can be estimated via different measurements like Received Signal Strength[RSS], Received Signal Strength Ratio(RSSR), Time Difference Of Arrival(TDOA) and distance based positioning.

The angulation method estimates the target location by measuring angles from multiple reference nodes. The most popular method for location estimation is to use RSS.

The wired BSs together with LED based illumination equipment provide wireless network access. Data broadcasting through a ceiling bulb realizes a point-to multipoint connection and a focused spotlight realizes a point-to-point connection. The Power over Ethernet(PoE) technology can be used to transport data traffic and supply the BSs as well as the lamps with the required power. The figure 1.18 shows a block diagram of indoor OW system. [4]

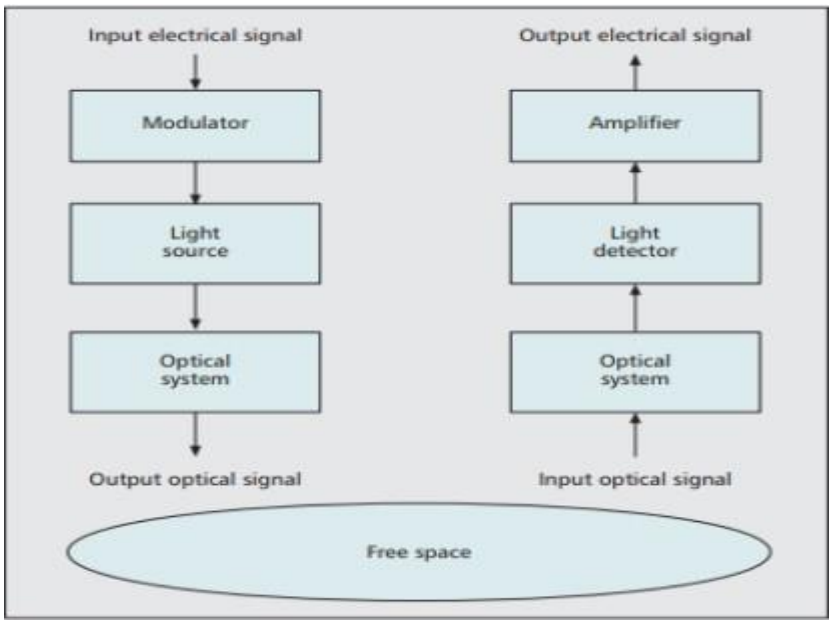

Figure 1.18. Block diagram of a typical indoor OW system. [4]

The basic OW system consists of a light source, free space as the propagation medium and a light detector. The analog or digital signals is given as the input to the electronic circuitry and that modulates the light source. The light source output is passes through an optical system and then in to free space. The received signal passes through the optical system. It may be an optical filter or a lens system or concentrator. The optical filter rejects the optical noise and the lens system or concentrator focuses light on the detector. The output of such an optical system forwarded to a light detector and the resulting photocurrent is amplified. The high data rate requirement of indoor OW systems can be achieved by Multiple Input Multiple Output(MIMO) techniques.

The visible light communication based positioning techniques are of two types. i.e. photodiodes(PD) and image sensor(IS) based system. Photodiodes are commonly used because they have high sensitivity to light and are also less expensive. The image sensors can spatially separate light sources. The performance metrics for indoor wireless location system includes accuracy, precision and complexity. Accuracy is the average Euclidean distance between the calculated location and the actual location. For a better system, the accuracy must be high. Precision is a measure of the toughness of the positioning process to give the difference in its performance after a number of chances. VLC communication link is designed for both data transmission and illumination. So the already existing LED lighting infrastructure reduces the implementation costs and allow the future expansion of the network. A Modified Monte Carlo based ray tracing algorithm(MMCA) is employed to evaluate the VLC channel impulse response for a typical office room as a function of the wavelength, the physical characteristics of the light sources and their layout in the room. [4]

1.5.3 Intelligent Transport System (ITS):

In ITS, vehicle to vehicle (V2V) and infrastructure to vehicle (I2V) communication ensures the safety of people, traffic flow and comfort of drivers as shown in Figure 1.19. ITS relies on reliable, robust and secure communication among vehicle and infrastructure (traffic lights, billboards). All vehicles are equipped with head and taillights that can be used for transmitting information. Traffic lights or billboards can also be used for sharing useful information about the road, traffic and weather conditions. These lighting sources can also be used for providing data connectivity to users and IoE (the internet of everything) entities. Cailean et al. have discussed challenges facing VLC in the context of vehicular communication (VC). VLC is proposed for ITS communication to complement or replace the existing crowded RF-based communication. Kunar and all have proposed to integrate LED-based Road Side Units (RSU) into the existing ITS infrastructure. The RSUs are used to broadcast information in infrastructure to vehicle (I2V) mode using VLC concepts. A robust modulation technique based on a Direct Sequence Spread Spectrum (DSSS) and Sequence Inverse Keying (SIK) is employed to minimize the effect of noise sources. The amount of data received by a car passing by RSU is considered as a performance metric. The experimental setup involves a movable receiver and a stationary emitter

both separated by a distance of 1.5 m. Results show that Packet Error Rate (PER) degrades linearly with distance during day light while at night the packet error varies due to the local nature of artificial light

The authors have considered VLC-based ITS for accident avoidance, particularly, when lorry fleet are moving through intersections. VLC has been used to send signals related to acceleration, reacceleration and braking to ITS infrastructure (e.g., RSUs) which can trigger appropriate signal. For example, to reduce the number of emergency brakes and lane change in a complex environment, a lorry fleet can send VLC signal to RSU which can set a green signal or express path. Yamazato and all have used VLC with imaging sensor-based receiver for automotive applications. Two scenarios I2V and V2V are considered. The first scenario consists of a transmitter designed from LED arrays (assumed to be RSUs) while the receiver is considered to be high frame rate CMOS imaging camera. In the second scenarios, a special CMOS sensor have been developed which can receive high-speed optical signals. In the field trials, a data rate of 32 kb/s and 10 Mb/s is achieved for I2V and V2V, respectively. [14]

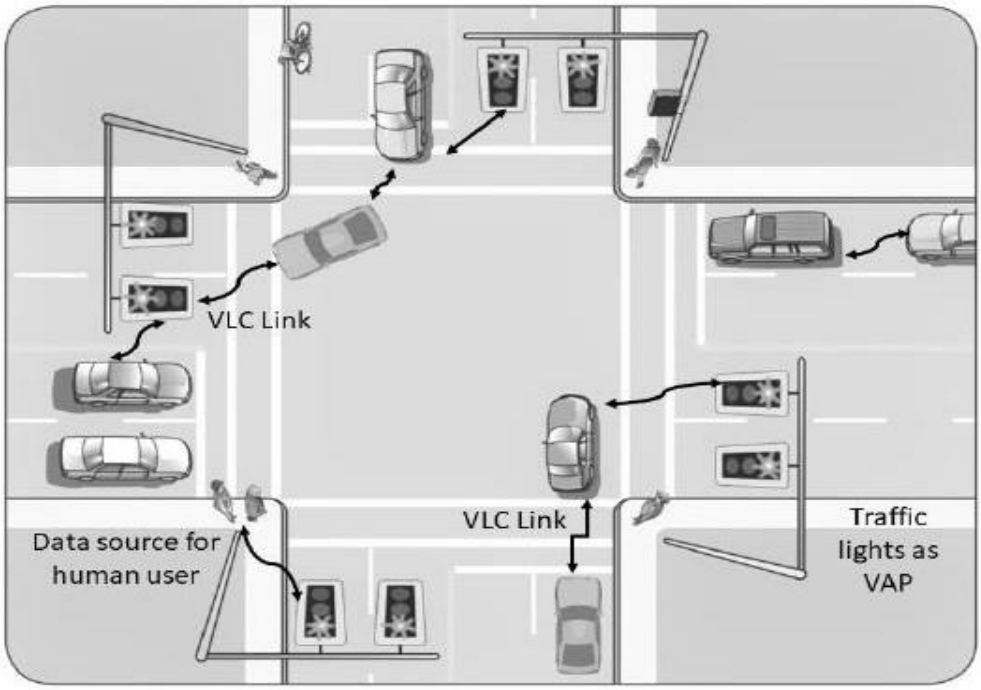

Figure 1.19. An intelligent transport system using visible light communication. [14]

1.5.4 Smart Cities and Smart Homes:

Smart cities are envisioned to provide seamless connectivity between people, government, infrastructure, economy and environment. Most of the functional entities of a smart city are already available around us. However, the reliable, sustainable and high data rate wireless connectivity is the bottleneck to connect all the enablers. The already available infrastructure of lightning (street lights, parking lights, billboards)

can be utilized to provide high-speed, low energy and sustainable network connectivity for some applications (e.g., utility services) in smart cities whereas freeing up the precious RF spectrum for other mobile applications. Streetlights or other lighting sources could be used as a hotspot to provide extremely high data rates to the user. A three-layer VLC based communication architecture is proposed to integrate different technologies in smart cities' applications seamlessly. Layer one uses VLC to allow user access and a sense of events. Layer two provides communication between different LEDs and sub gateways. The last layer provides communication between different sub gateways and the service gateway using optical communication. Based on this architecture several applications (such as intelligent communication, event surveillance, and object tracking) have been demonstrated. [14]

1.5.5 In hospitals:

In hospitals, electromagnetic wave sensitive areas (such as MRI scanners) are likely to switch to VLC because it will not interfere with radio waves of the other machines. A robot called HOSPI (shown in Figure1.20) was proposed that was used for transportation in hospitals. The control system enhancements in HOSPI were made using VLC installed in a building and navigational sensors of the robot. [15]

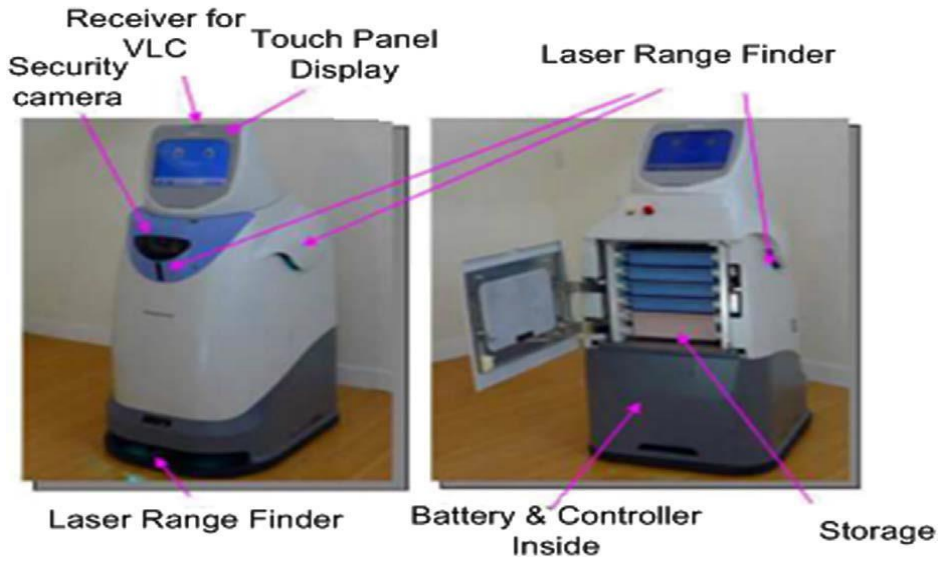

Figure 1.20. HOSPI Robot. [15]

1.5.6 Wireless local area networks (WLANs):

LED based visible light communication can be used in setting up LANs, an ultra-high speed full duplex; LAN based on star topology architecture using LED visible light communication is proposed to provide a speed of more than 10-Gb/s and tested for massive users. The schematic diagram of the high speed LAN is shown in Figure1.21. The reason for the design of the network using a star topology is to provide support for massive users. Fiber is used in connection with each lamp directly. [15]

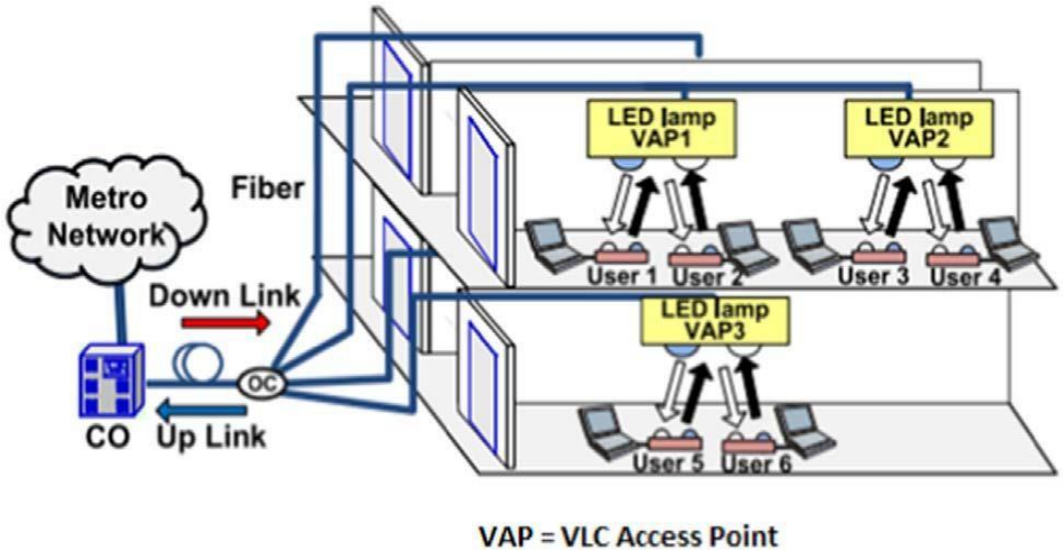

Figure 1.21. The VLC network schematic diagram. [15]

The hybrid access protocol is used in the proposed LAN such as time division multiplexing (TDM) for bidirectional VLC transmission and frequency division multiplexing (FDM) for uplink and downlink fiber transmission. The results of the proposed LAN revealed its potential power of offering high-speed access for massive users, a 10 Mbps VLC wireless LAN system was proposed using white LEDs. The lighting system was used for downlink and infrared light was used for up-link. The VLC wireless LAN has the potential to be used in office buildings and hospitals, which require a high level of safety. [15]

1.5.7 A Sound communication system:

Red, green and blue LEDs are used for the transmission of music signals as shown in figure 1.22. [15]

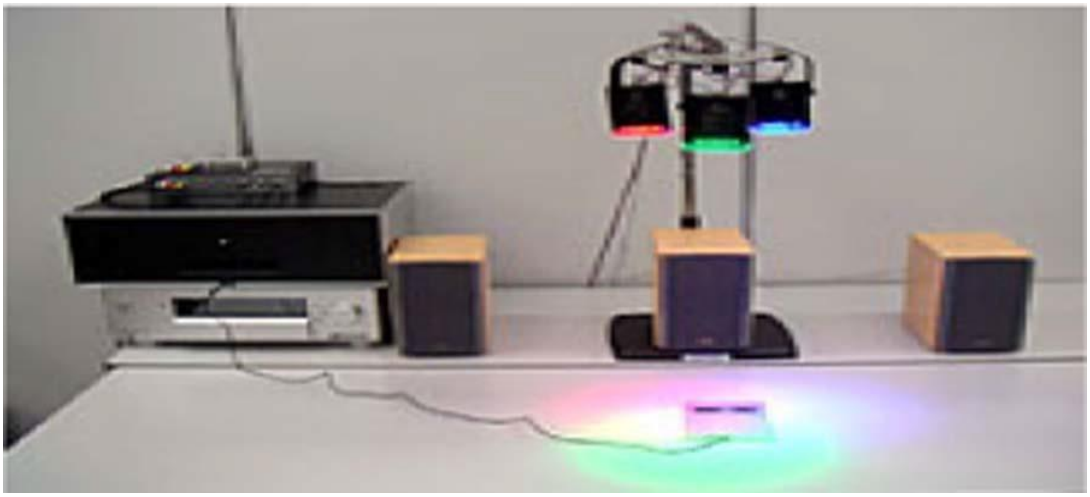

Figure1.22. VLC in a Musical System. [15]

1.5.8 Information displaying signboards:

Signboards are often made from an array of LEDs, which in turn are modulated to convey information in airports, bus stops and other places where the broadcasting of data is necessary. The signboard used for transmitting data was described. This type of signboard can be used for indications in various locations such as airports, museums and hospitals. [15]

1.6 VLC Advantages:

- ✓ High bandwidth: The RF communications come with an available spectrum of 300 GHz, where the VLC takes full advantage of the usage of the visible light spectrum which is between 380 and 780 THz.
- ✓ The usage of the visible light as a carrier for the data enables VLC to be completely safe for the human health.
- ✓ Unrestricted technology: RF communication can cause malfunctions of the high precision electronic equipment as the one found in hospitals or in aircrafts and for this reason, such places are RF restricted. On the other hand, besides being safe for the human body, VLC is safe also for the high precision electronic equipment, enabling its usage in such places.
- ✓ VLC provides high security by protect beam width the communication from eavesdropping.
- ✓ Low cost implementation: VLC uses the visible light for communication, which is in an unlicensed region of the electromagnetic spectrum. Since no cost for a license is implied, the implementation cost is significantly reduced. And second advantage that helps VLC reducing the implementation cost of such systems is its ubiquitous nature. VLC will rely on existing infrastructures that is already accepted and widespread across the world.
- ✓ Green wireless communication technology: for the earth firstly because it does not use additional power for the communication The same light which is used for illuminating or signaling is used for carrying the data. Another important advantage of VLC is the usage LEDs which provide substantial energy savings, reducing the CO2 emissions. [13]

1.7 Conclusion:

In this chapter, we offered an overview about the visible light communication as technology and them standardization between the various poles of the world; we mentioned also the architecture of VLC and its application in daily life. In the next chapter, we will introduce some works in pairing devices using visible light.

Chapter 02:

Key Management Protocol for wireless devices

2.1 Introduction

Wireless communication security is an important issue, which has been investigated by researchers for years. The most fundamental security problem in wireless communication is key management that covers the establishment, distribution, renewing and revocation of cryptographic keys. Several key management protocols were proposed in the literature.

In this chapter, we describe pairing methods and protocols wireless devices, as well we present devices pairing using visible light, such as internet using visible light communication, Secure Barcode-based Visible Light Communication for Smartphones, sending location Based keys using visible Light Communication, Visible Light Identification System for Smart Door Lock Application with Small Area Outdoor Interface.

2.2 Device pairing methods in wireless communication:

The goal of pairing methods is to establish a shared secret key that can be used to secure subsequent communication over the secure network. This section describes some secure pairing methods with detailed steps:

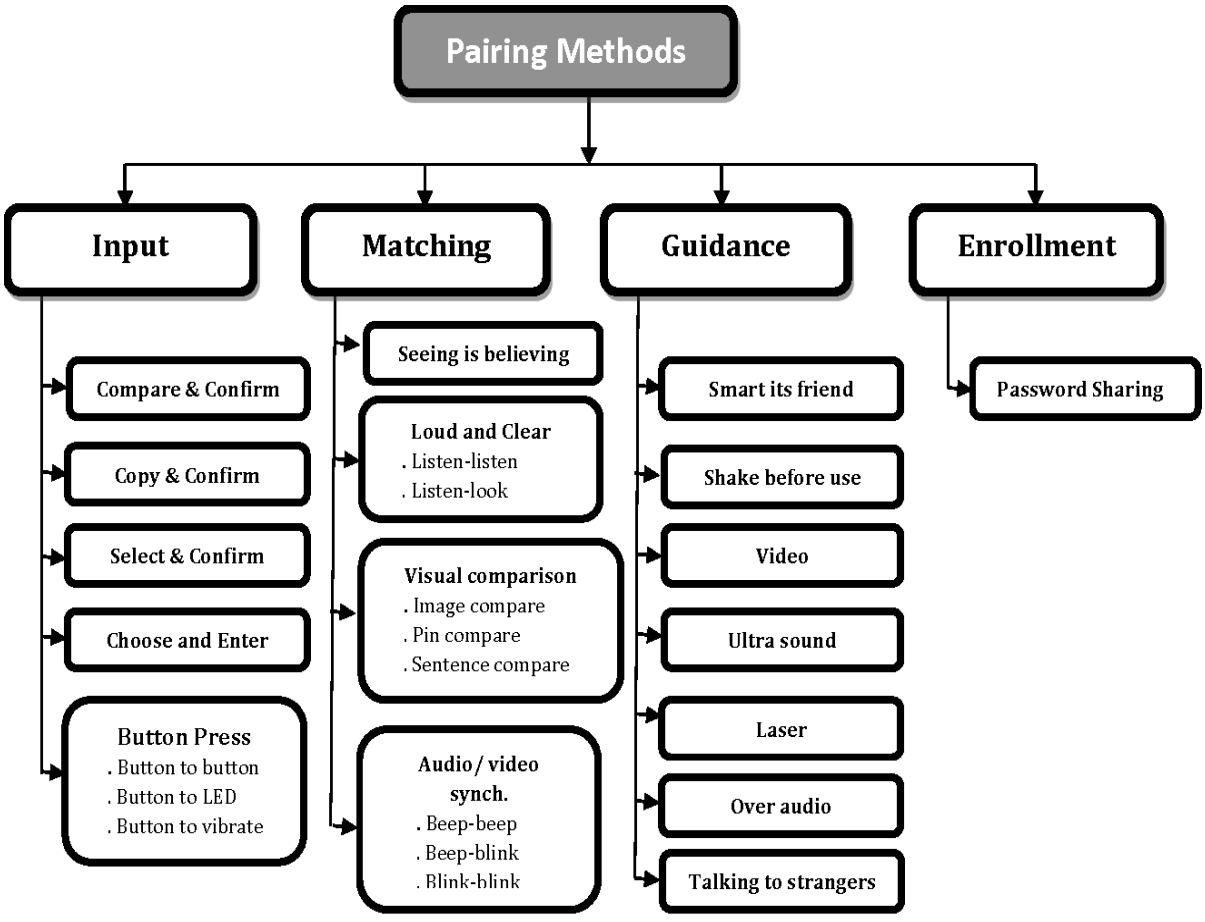

Fig. 5. Categories of pairing methods

Figure 2.1. Categories of pairing methods. [16]

2.2.1 Input:

The users generate information and enter on the user interfaces of their devices. For example, the Bluetooth pairing process requires its users to enter a passkey into the devices. It includes:

2.2.1.1 Compare and Confirm:

The user simply compares two 4-, 6- or 8-digit numbers displayed by devices. then decides to enter. This is quite inefficient and time taking and having high error rate, Abort and accept on sending device based on receiving device decision

2.2.1.2 Select and confirm:

In this approach, one device displays to the user a set of (4-, 6- or 8-digit) numbers, the user selects the one that matches the number displayed by the other device. The same disadvantages of compare and confirm method, and the receiving is the master of the decision.

2.2.1.3 Copy and confirm:

The device displays the number to the user for copy it in the other device, until in this method, the decision also is up to the receiving device.

2.2.1.4 Choose and enter:

Which asks the user to pick a ``random" 4- to 8-digit number and enter it into both devices. Its security is considerably weak due to user's choice. [17]

2.2.1.5 Button press: `

` Button-Enabled Device Authentication (BEDA)" suggests pairing devices with the help of user button presses, thus utilizing the tactile OOB channel.

a) Button to button:

As name shows, the user simultaneously presses buttons on both devices and random user-controlled inter-button-press delays are used as a means of establishing a common secret. 3 bits' secret key is generated in every time interval. this method is Successful unless synchronization error.

b) Button to LED:

Based on the SAS protocol variant, the sending device blinks its LED and the user presses a button on the receiving device. Each 3-bit block of string is encoded as the delay between consecutive blinks. As the sending device blinks, the user presses the button on the other device there by transmitting the SAS from one device to another. [17]

c) Button to vibrate:

This method also based on the SAS protocol variant, as the sending device vibrates, the user presses the button on the other device there by transmitting the SAS from one device to another. Each 3-bit block of string is encoded as the delay between consecutive vibrations. Acceptation and rejection on sending device is also based on output of receiving device. [17]

d) Button to Beep:

This is another approach that is suitable for the situation where LED or display facility is not available instead, a device has speaker only. Similarly, in previous method the device B selects a key convert it into appropriate coding format and transmit to other device A, that has a button, where user hears a beep and response through pressing button with random time interval. [16]

The input methods are simple, easy to use and to understand, but the user herself compares the OOB strings output by the devices and decides the pairing outcome. He can simply "accept" the pairing without having to take part in the decision process correctly, so these methods are vulnerable and them error rate is high.

2.2.2 Matching:

The users perform comparison of the output of devices in order to establish or reject a connection. It includes:

2.2.2.1 Seeing is believing:

In its simplest instantiation, SiB requires a unidirectional visual OOB channels: one device encodes OOB data into a two-dimensional barcode which it displays on its screen and the other device ``reads it'' using a photo camera, operated by the user. At a minimum, SiB requires one device to have a camera and the other a display. Thus, it is not suitable for low-end devices. [17]

2.2.2.2 Loud and clear:

The vocalized sentences and audio OOB channel are used in combination to exchange information on wireless channel. In this method Abort and accept on Depends both devices.

a) Listen-Listen:

Both devices "vocalize" a 3-word sentence and user tries to configure their resemblance, if they appear to be similar, the final response is added in two connecting devices separately. Two Speakers are required on both devices.

b) Listen-Look:

As name showed the listening occurs on one end and sighting on other. Device A show three-word sentence while at the other end three words sentence is spoken by device B and user inputs the decision after comparing both sentences. One speaker and a display is required on both devices. [16]

2.2.2.3 Visual Comparison based:

a) Image Compare: It encodes the OOB data into images and asks the user to compare them on two devices. Prominent examples include ``Snowflake'',

``Random Arts Visual Hash" and ``Colorful Flag". Such methods, however, require both devices to have displays with sufficiently high resolution. Applicability is therefore limited to high-end devices, such as: laptops, and certain cell phones. it based on SAS protocols

b) Pin Compare: In this method, the both devices display a 5-digit number, the user compares them, ultimate decision is from both devices (accept or reject).
c) Sentence Compare: Three word sentences are appeared on device A and B where user make comparison and enter the final decision (accept/reject) on both devices.

2.2.2.4 Audio/video synch:

In this technique, users compare simple audio and visual patterns for syncing:

a) Beep-beep: based on synchronized audio patterns, by forming two synchronized channels for transmitted beeps which comes out of the speakers as simultaneous streams, this method requires devices to have a speaker.
b) Beep-blink users comparing audiovisual patterns, transmitted as simultaneous streams, with forming two synchronized channels. It requires devices to have a LED and a basic speaker.
c) Blink-Blink: it works at the same principle of the other methods ``Beep-Beep" and ``Beep-Blink", the user comparing visual patterns, it requires devices to have a LED. [17]

2.2.3 Guidance:

The users perform a physical action (touch, point, proximate) on devices to direct them to discover each other. For example, the users are required to bring devices closer to each other as shown in Figure 2.2 to establish a connection in Android Beam. It includes the following:

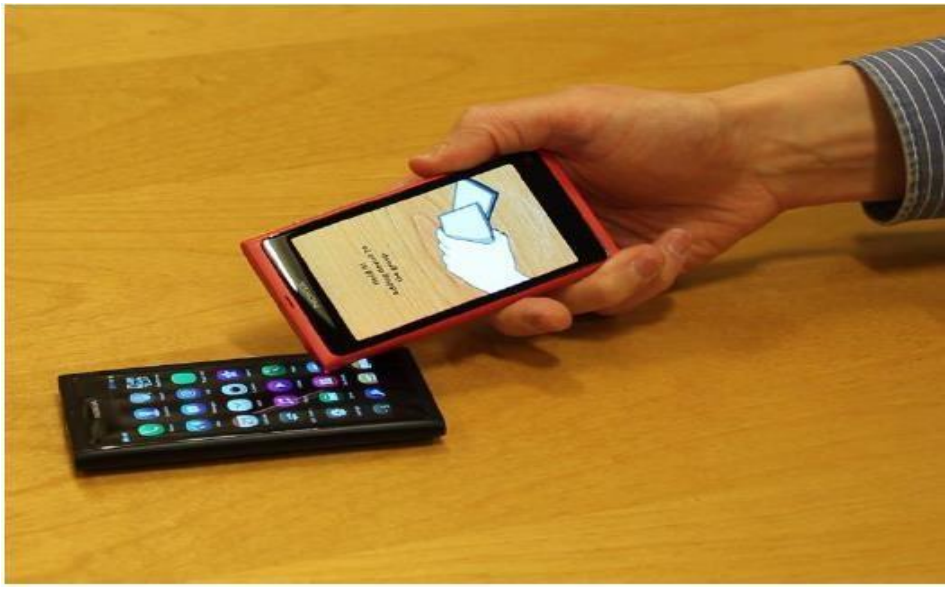

Figure 2.2. Touching device to add it to the group. [16]

2.2.3.1 Smart it's Friends:

The user input in one devices and shake both devices together that results in a secret pattern transmission between two devices, it requires to have 2-axis accelerometers on both.

2.2.3.2 Shake well before use:

The two-axis accelerometer is required on both devices and the devices are shaken to establish a pairing connection by user just like smart its friends 'method. But it's not usable for bulky or large fixed position devices.

2.2.3.3 Ultrasound:

Using ultrasound as the OOB channel, it requires each device to have a laser transceiver with 2-axis accelerometers.

2.2.3.4 Laser based:

Laser transceiver is required on both devices through which laser beam could be used for pairing process.

2.2.3.5 Video:

Device B displays a blinking pattern and the user capture a video of this pattern with device A then on the basis of A's output user accept or reject the offer on device B.

2.2.3.6 Over audio:

The devices that do not possess any common wireless channel preferably use this method. An audio protocol of cryptographic message is transmitted that is then closely monitored by user to avoid any third party interruption. Microphone and speaker should be present in both devices. [16]

2.2.3.7 Talking to stranger:

Which relies on infrared (IR) communication as the OOB channel and requires almost no user involvement, except for initial setup. However, this method is deceptively simple since IR is line-of-sight and, setting it up requires the user to find IR ports on both devices not a trivial task for many users and align them. Also, despite its line-of-sight property, IR is not completely immune to MiTM attacks.

the main drawback of IR is that is has been largely displaced by other wireless technologies (e.g., Bluetooth) and is available on very few modern devices. [17]

2.2.4 Enrollment:

The users set a password for the devices first which is then shared with the other devices that are intended to be connected.

2.2.4.1 Password sharing:

User enter the secret key on receiving device that was displayed on sender devices Abort and accept on sending device. This is used when users have to make Wi-Fi hotspot like a code is generated on the admin, which is shared with the devices which require connecting with the network. [16]

2.3 wireless device pairing protocols:

Many pairing protocols have already been developed, in particular for the pairing of devices over specific wireless networks. [18]

Device-pairing protocols extracts the shared secret key from data. If the created secret key has sufficient entropy to prevent offline brute-force attacks, it may be used directly as an encryption key. Most of the protocols described in the literature appear to be of this type. However, as the entropy of the fuzzy input typically is uncertain, it would be safer to use the extracted key as a transitory secret for authenticating a strong key exchange such as Diffie–Hellman. and there are only a few protocols of this type in the literature, all protocols of fist type can be easily converted to the safer second type. Using the potentially weak shared secret for authenticating a stronger one is also one of the design principles of protocol. [19]

For example, the current Bluetooth specifications include a pairing protocol that has evolved over several revisions towards better security and usability (BTLE Pairing). The Wi-Fi Alliance defined the Wi-Fi Protected Setup process to ease the setup of security-enabled Wi-Fi networks in home and small office environments (WPS). Other wireless standards have defined or are defining similar protocols, tailored to specific technologies. [18]

We limit the goal of the protocol to the establishment of a shared secret between two parties. Once that secret has been established, it can trivially be used to secure the exchange of other information, such as for example public keys and certificates. [18]

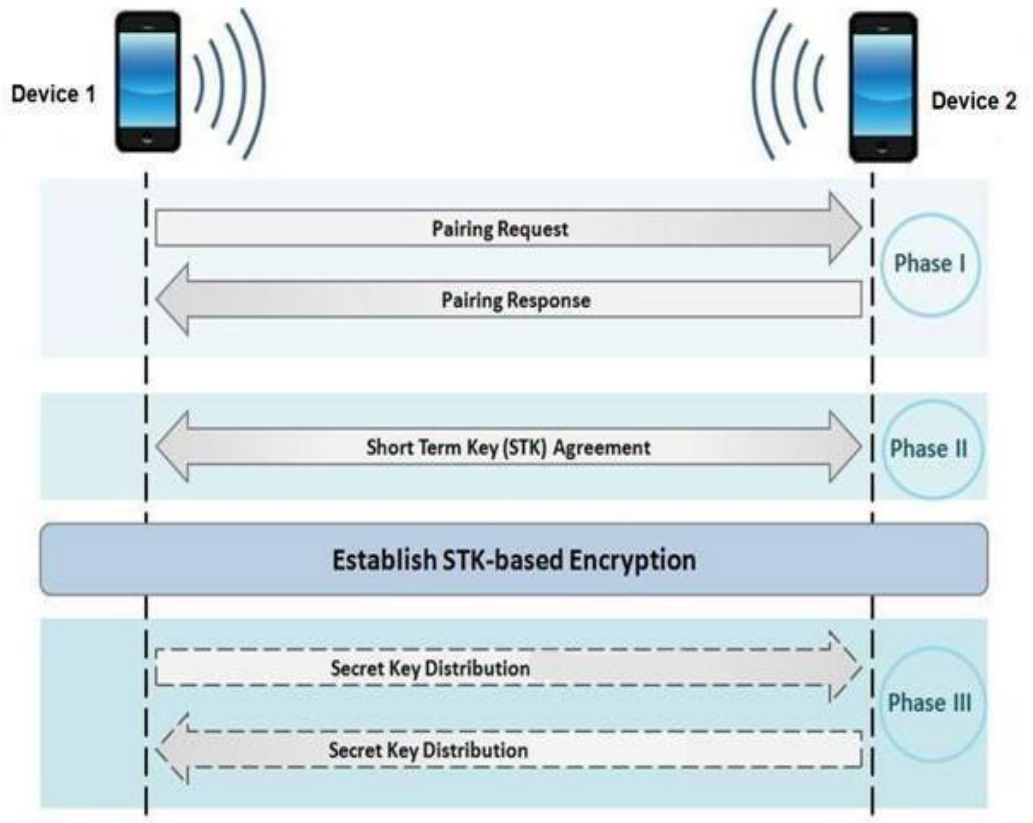

Figure 2.3. Simple device pairing protocol. [17]

2.4 Devices pairing using visible light communication

2.4.1 Internet using visible light communication:

In wired transmission, data is transferred through a physical medium or a link whereas no physical link is used in wireless transmission. Both mediums have its own characteristics and advantages. Wireless communication uses the RF source to modulate. But it takes some time. But, if we use a visible light instead of RF wave source, transmission speed can be increased. Light wave communications also should have larger bandwidth. The Li-Fi technology uses visible light for the data transmission as. the wireless medium. In Li-Fi technology, the data transmitted by illuminating LED or LASER that varies in intensity faster than the human eye can sense the light. The term Li-Fi is used to label the fast and cheap wireless-communication system, which is the optical version of Wi-Fi. Harald Haas[1] says, "They can be switched on and off faster, which helps for data transmission." To encode data in the light can be done by varying the rate at which the light flicker ON and OFF to give different strings of 1s and 0s. The intensity of the light is modulated so rapidly that human eye can't detect, so the output appears to be constant. [20]

LED send data rate up to 10 Gbps. But the previous wireless network will provide high data rates is nearly 100 Mbps in IEEE 802.15.7 standard but still it is not

[1] . **Dr. Harald Haas:** from the University of Edinburgh he coined the term "Li-Fi" during his appearance at TED Talk Global 2011. It was at this stage that he was able to highlight one of the newest pieces of technology that is able to transmit high volumes of data at high-speed capacity with only the use of overhead lighting.

sufficient for end of the user. Nowadays everywhere using the LEDs that's why the rapid increase in the usage of LEDs has provided a unique opportunity.

[21]

Sumit Jaykant Meshram, and Prof Avinash P Wadhe authors of 'Secure data transfer using visible light communication Technique [21] said that VLC provides the potential for multi-gigabit-per-second data rate communication at short distances with ~300 THz of available visible light spectrum at low power and cost, using simple LEDs and PDs. With the growing integration of LEDs in indoor and outdoor light sources, and advances in the design of low cost LEDs with fast sub nanosecond switching response times, the integration of lighting and communication provides significant potential for this technology. The two main challenges in communication in this spectrum are flicker mitigation and support for dimming.

They also said that Visible light communication is a creative approach to combine illumination, wireless communication, and novel play patterns for connected toys. Since it can be implemented at low cost with components that are available in many toys, VLC facilitates toy networking and, in addition, communication with phones via cameras and flashlights. This is possible without the need for extra hardware. In the future, free space optics (infrared or VLC) can play an interesting role complementing traditional radio communication in consumer electronics. [21]

2.4.2 Secure Barcode-based Visible Light Communication for Smartphones:

Compared with NFC, 2D barcodes have enjoyed a significantly higher usage rate in mobile applications. This is largely due to the extremely low barrier to adoption where almost every camera-enabled smartphone can read and process 2D barcodes. As an alternative to NFC, 2D barcodes have been increasingly used for security-sensitive applications including mobile payments and personal identification. for instance, PayPal recently rolled out a barcode-based payment service for retail customers. When a customer checks into a store with the PayPal app, the app will generate a QR code that acts as an individual signature. Merchants can scan the code with a scanner and the payment will go through.

On the other hand, the security of barcode-based communication in mobile applications has not been systematically studied. Due to the visual nature, 2D barcodes are subject to eavesdropping when they are displayed on the screens. The proliferation of smartphones puts a portable camera in everyone's pocket, making eavesdropping much easier. This is exacerbated by widely spread use of surveillance cameras in public areas like shopping malls. On the other hand, the fundamental design Principles of 2D barcodes make it difficult to add security features. First, a 2D barcode only contains a small amount of information and hence cannot simply adopt advanced encryption primitives. Moreover, most existing barcode applications are based on a single barcode exchange, which is insufficient for establishing a secure communication channel. For this a new method was followed are Secure Barcode-based Visible Light Communication.

SBVLC (Secure Barcode-based Visible Light Communication) a novel secure ad-hoc wireless communication system for smartphones. where the communication mode of him is ad-hoc in that the sender and the receiver are not expected to have a common shared secret knowledge such as secret key in priori to the communication. Similar to NFC setting, there is an air interface between the sender and the receiver, and the

typical reception distance is also a few inches. SBVLC supports secure data exchange for both smartphone and smartphone-terminal scenarios. SBVLC works on top of a fully duplex VLC channel, and thus the smartphones must be equipped with a color screen and a front-facing camera as the sender and the receiver are required to 'talk' to each other simultaneously. SBVLC works among various mobile platforms without specific requirement on the screen size and camera resolution, but a better specification usually leads to higher communication throughput. [22]

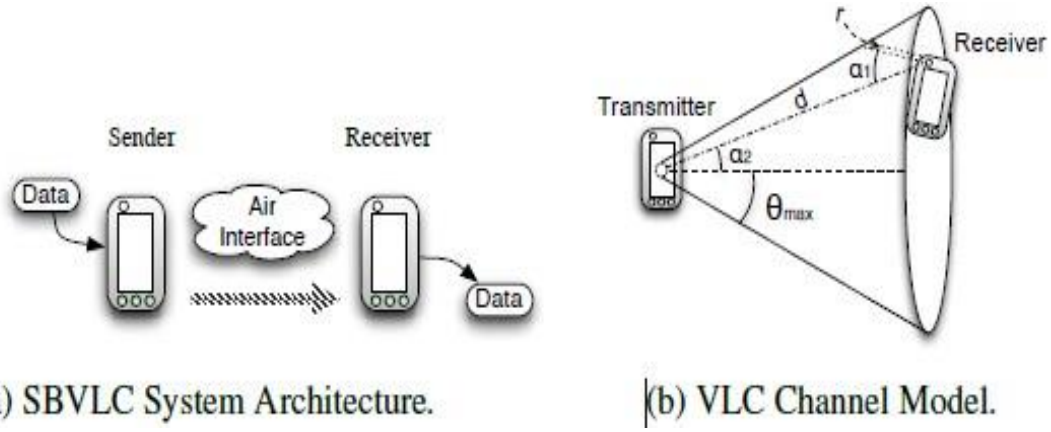

Figure2.4. SBVLC System Architecture. [22]

2.4.3 Sending Location-Based Keys Using Visible Light Communication:

Sharing keys securely is an important problem for many applications. The use of RF for sharing these keys is naturally prone to sniffing attacks especially in none-line-of-sight conditions. Obstacles that commonly cause NLOS conditions include buildings, trees, hills, mountains, and, in some cases, high voltage electric power lines. Some of these obstructions reflect certain radio frequencies, while some simply absorb or garble the signals; but, in either case, they limit the use of many types of radio transmissions. [23]

The authors of 'Poster Abstract: BouKey: Location-Based Key Sharing Using Visible Light Communication' describe a multiple light system for security applications. TmoteSky and UPWIS platforms are used to run the software with data rates of 32 bps and 128bps respectively. BFKS modulation with option of Manchester Encoding is used in order to allow transmission from multiple lights. The demodulation was carried out by applying the Groetzel algorithm to frequencies detected by a photodiode connected to a built in ADC in the microcontroller. Also, the Shamir Secret Sharing algorithm is used to encrypt the information by representing in a polynomial form. [24]

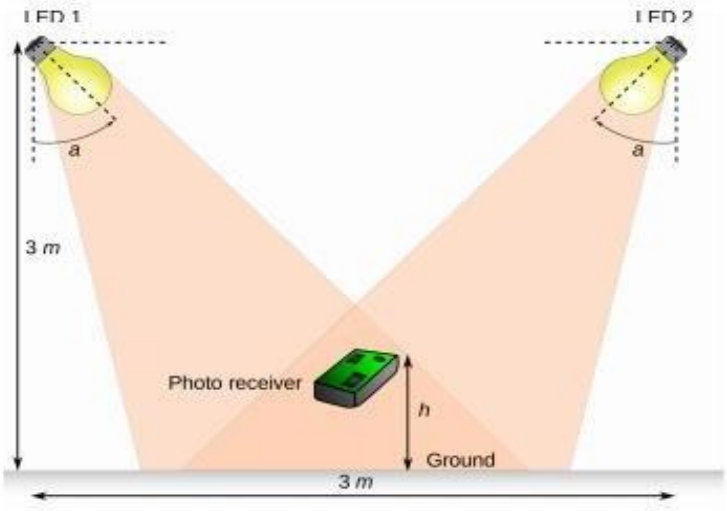

Figure2.5. BouKey Overview A secret key is split into several parts, and transmitted using multiple LEDs. The receiver equipped with a photodiode can receive this key only in specific areas which fall at the intersection of the reception area of all or the majority of the LEDs. [23]

2.4.4 Visible Light Identification System for Smart Door Lock Application with Small Area Outdoor Interface:

Visible light identification (VLID) is a user identification system for a door lock application using smartphone that adopts visible light communication (VLC) technology with the objective of high security, small form factor, and cost effectiveness. The user is verified by the identification application program of a smartphone via fingerprint recognition or password entry. If the authentication succeeds, the corresponding encoded visible light signals are transmitted by a light emitting diode (LED) camera flash. Then, only a small size and low cost photodiode as an outdoor interface converts the light signal to the digital data along with a comparator, and runs the authentication process, and releases the lock. VLID can utilize powerful state-of-the-art hardware and software of smartphones. Furthermore, the door lock system is allowed to be easily upgraded with advanced technologies without its modification and replacement. It can be upgraded by just update the software of smartphone application or replacing the smartphone with the latest one. Additionally, wireless connection between a smartphone and a smart home hub is established automatically via Bluetooth for updating the password and controlling the home devices.

As a first step, a user should register a smartphone to a VLID door lock system. Like conventional systems, a new phone can be registered only when a door is opened. After the indoor part of a door lock enters the registration mode by pressing a button, the new password randomly generated by a smart phone is transferred through an outdoor photodiode. In normal operation, a user places the back-side of a smartphone on a door lock to contact a camera flash to a photodiode. Consequently, a user can access the smartphone's VLID application program without any inconvenience during the door lock operation because the smartphone's screen turns toward the user.

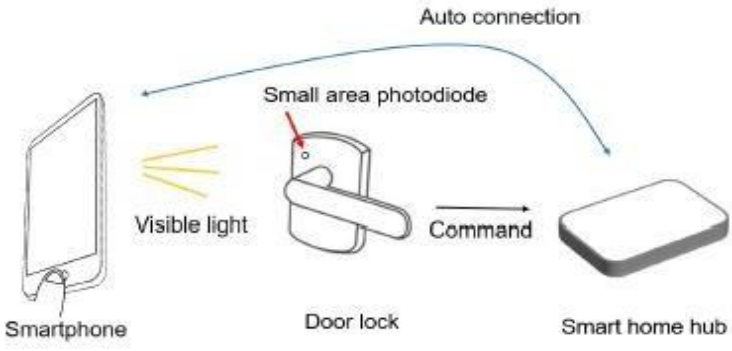

Figure2.6. Proposed VLID door lock system. [25]

The Figure2.7. shows a block diagram of the proposed VLID system. When a user enters a password or puts a finger on a fingerprint sensor of a smartphone, an internal powerful processor identifies the user and generates the corresponding binary passcode for visible light transmission.

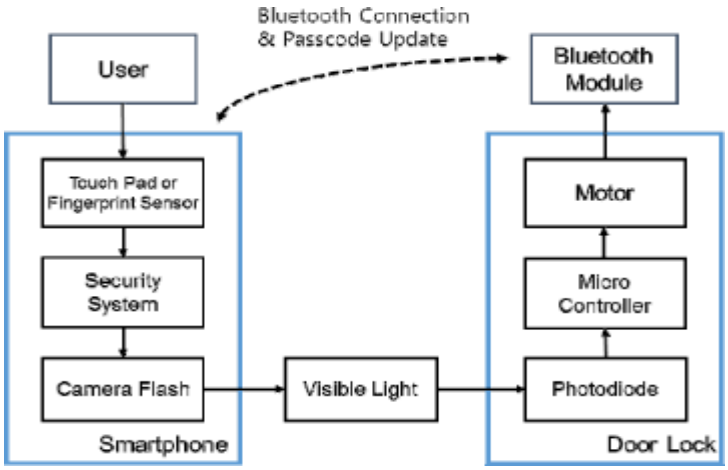

Figure 2.7. Block diagram of VLID door lock system. [25]

Then, the generated code is converted into visible light through a camera flash of a smartphone. The receiver of a VLID door lock senses the flash light sequence that is recovered into the binary stream. When the received binary data are equal to the binary passcode stored in advance, the processor of the door lock operates a servo motor and a Bluetooth module to open a door and to establish the connection with the smartphone, respectively. After the Bluetooth link is established, the new passcode randomly made up by a smartphone is updated at both smartphone and door lock system leading to strong security. Because the passcode is changed every VLID operation, anybody can not figure out the password by stealing a glance of a flickering LED.

A detailed process of the proposed VLID system is illustrated in Figure 2.8. After the smartphone identifies a user, it transmits the binary VLC signal consisted of a passcode and a user ID to a door lock receiver. And then, the door lock compares the received passcode with the passcode that is stored in advance and commands a Bluetooth module to send a connection request to the smartphone with the received user ID. The smartphone keeps monitoring a connection request and sends a

connection response to the door lock when the corresponding request is received. The connection is established by the smartphone and the door lock exchanging the connection confirm signal. Then, the smartphone generates the new random passcode that is shared with the door lock via Bluetooth. [25]

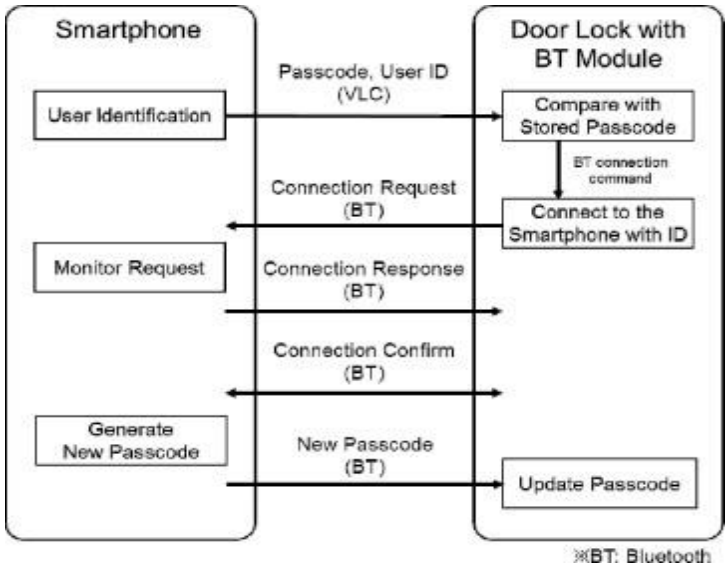

Figure 2.8. Procedure of VLID door lock. [25]

Despite the great impact of optical communication in various fields, there are many challenges that require a solution in order for VLC to be viable, the latter being reflected in:

- ✓ The mandatory LOS condition: a VLC transmission cannot be fulfilled unless the receiver can see the transmitter. it represents VLC's greatest disadvantage because an object interposed between emitter and received can block the communication, unless an alternate route is available. it possible to solves that by using multi-hop communications and retransmissions.
- ✓ Bandwidth: Limited to a few MHz, so it cannot compete with high-frequency wireless communication, multi-hop networks are a solution to optimize bandwidth in an orderly Gbps, with improvement in the transmitter and the receiver.
- ✓ susceptibility to interferences: VLC suffers from external interference (sunlight, artificial light ...) it produces low-frequency noise, but it can be eliminated by reducing the receiver FOV and using optical filters, even if the mentioned technique mitigates the effect of the interferences, noise still affect the communication performances.

On the other hand, we do not overlook its unique features that make it the next generation in wireless communication, the most important of which is VLC, safer than RF, data transmission is available in addition to the lighting function. Besides, VLC is a low-cost and easy-to-implement technology. This is what made it the focus of many researchers in their research, which is still under implementation, as it is still a modern technology.

2.5 Conclusion:

In this chapter, a general overview of wireless devices pairing methods and protocols was offered, we also introduce some related work of secure communication using visible light communication. In the next chapter, we design and implement a mobile application using LED and sensor light to share a key.

Chapter 03:

Proposition and Implementation

3.1 Introduction:

In this chapter, we describe concepts to our project as Password Based Encryption(PBE), salt and iteration count and Android Studio. Then we introduce our proposition and implementation.

3.2 Related concepts:

Data security is always associated with cryptography. Cryptography is the study of how to maintain the security of a message and maintain the confidentiality of messages from irresponsibility by encoding into an unreadable form (chipper text). Cryptography studies mathematical techniques related to information security aspects such as confidentiality, data integrity and authentication. So the authenticity of the data can be guaranteed. [26]

3.2.1 Password Based Encryption(PBE):

Password Based Encryption (PBE) is a symmetric cryptographic method that uses a password-like key to perform the encryption process and uses the same key to perform the decryption process so that it will generate the same data as the original plaintext data.

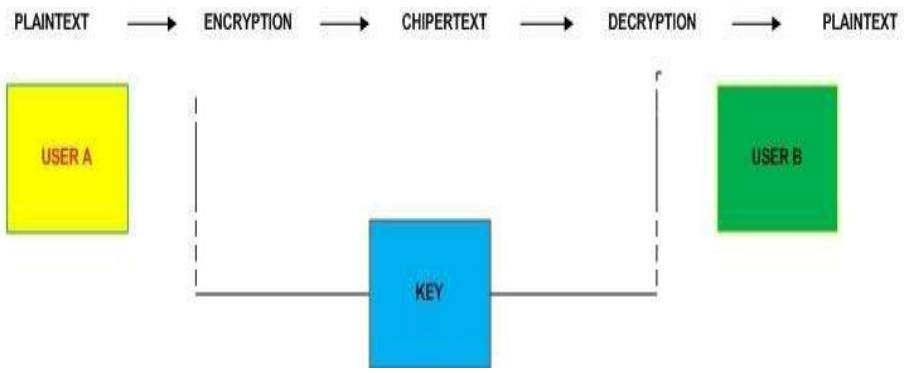

Figure3.1. Symmetric Algorithms Process. [26]

In general Approach, Morris and Thompson described password-based cryptography as combine a password with a salt to produce a key. The salt can be viewed as an index into a large set of keys derived from the password, and need not be kept secret. Although it may be possible for an opponent to construct a table of possible passwords (a so- called "dictionary attack"), constructing a table of possible keys will be difficult, since there will be many possible keys for each password. An opponent will thus be limited to searching through passwords separately for each salt.

Another approach to password-based cryptography is to construct key derivation techniques that are relatively expensive, thereby increasing the cost of exhaustive search. One way to do this is to include an iteration count in the key derivation technique, indicating how many times to iterate some underlying function by which keys are derived. A modest number of iterations,

say 1000, is not likely to be a burden for legitimate parties when computing a key, but will be a significant burden for opponents.

Salt and iteration count formed the basis for password-based encryption in PKCS #5 v1.5, that we adopted here as well for the various cryptographic operations. Thus,

password-based key derivation as defined here is a function of a password, a salt, and an iteration count, where the latter two quantities need not be kept secret. [27]

3.2.2 Salt and Iteration Count:

3.2.2.1 Salt:

A salt in password-based cryptography has traditionally served the purpose of producing a large set of keys corresponding to a given password, among which one is selected at random according to the salt. An individual key in the set is selected by applying a key derivation function KDF, as:

$$DK = KDF (P, S)$$

where DK is the derived key, P is the password, and S is the salt. This has two benefits:

- It is difficult for an opponent to precompute all the keys corresponding to a dictionary of passwords, or even the most likely keys. If the salt is 64 bits long, for instance, there will be as many as 2^64 keys for each password. An opponent is thus limited to searching for passwords after a password-based operation has been performed and the salt is known.

- It is unlikely that the same key will be selected twice. A gain, if the salt is 64 bits long, the chance of "collision" between keys does not become significant until about 2^32 keys have been produced, according to the Birthday Paradox. This addresses some of the concerns about interactions between multiple uses of the same key, which may apply for some encryption and authentication techniques.

3.2.2.2 Iteration Count:

An iteration count has traditionally served the purpose of increasing the cost of producing keys from a password, thereby also increasing the difficulty of attack. For the methods in this document, a minimum of 1000 iterations is recommended. This will increase the cost of exhaustive search for passwords significantly, without a noticeable impact in the cost of deriving individual keys. [27]

3.2.3 Key Derivation Function:

Dictionary attacks aim to recover passwords by trying the most-likely strings, such as the words in a dictionary. These attacks are less likely to succeed against passwords that include random combinations of upper/lowercase letters and numeric values. Such passwords can only be recovered using inefficient brute force attacks that try all possible passwords [28]. Among them we find the derived key which is calculated depending on key derivation function by using input public and secret data, its advantage is that if two parties share the same secret and mutually known parameters as inputs, they may, independent of each other, calculate identical derived keys by keeping track of the number of iterations. [29]

The main idea of a PBKDF (Password Based Key Derivation Function) is to slow dictionary or brute force attacks on the passwords by increasing the time needed to test each password. An attacker with a list of likely passwords can evaluate the PBKDF using the known iteration counter and the salt. Since an attacker has to spend

a significant amount of computing time for each try, it becomes harder to apply the dictionary or brute force attacks. [28]

A key derivation function produces a derived key from a base key and other parameters. In a password-based key derivation function, the base key is a password and the other parameters are a salt value and an iteration count. Two functions are specified: PBKDF1 and PBKDF2. PBKDF2 is recommended for new applications; PBKDF1 is included only for compatibility with existing applications, and is not recommended for new applications. A typical application of the key derivation functions defined here might include the following steps:

- ✓ Select a salt S and an iteration count c,
- ✓ Select a length in octets for the derived key, dkLen.
- ✓ Apply the key derivation function to the password, the salt, the iteration counts and the key length to produce a derived key.
- ✓ Output the derived key.

Any number of keys may be derived from a password by varying the salt.

3.2.3.1 PBKDF1 :

PBKDF1 applies a hash function, which shall be MD2, MD5 or SHA-1, to derive keys. The length of the derived key is bounded by the length of the hash function output, which is 16 octets for MD2 and MD5 and 20 octets for SHA-1. PBKDF1 is compatible with the key derivation process in PKCS #5 v1.5.

3.2.3.2 PBKDF2 :

PBKDF2 applies a pseudorandom function to derive keys. The length of the derived key is essentially unbounded. (However, the maximum effective search space for the derived key may be limited by the structure of the underlying pseudorandom function.) PBKDF2 is recommended for new applications.

DK = PBKDF2 (PRF, P, S, c, dkLen)

Options:	PRF	underlying pseudorandom function (hLen denotes the length in octets of the pseudo random function output)
Input:	P	password, an octet string
	S	salt, an octet string
	c	iteration count, a positive integer
	dkLen	intended length in octets of the derived key, a positive integer, at most (2^32 - 1) * hLen
Output:	DK	derived key, a dkLen-octet string. [27]

3.2.4 Android Studio:

To developed our application, we use android Studio because is the official Integrated Development Environment (IDE) for Android app development, based on IntelliJ IDEA. On top of IntelliJ's powerful code editor and developer tools, Android Studio offers even more features that enhance your productivity when building Android apps, such as:

- ✓ A flexible Gradle based build system

- ✓ A fast and feature-rich emulator
- ✓ A unified environment where you can develop for all Android devices
- ✓ Apply Changes to push code and resource changes to your running app without restarting your app
- ✓ Code templates and GitHub integration to help you build common app features and import sample code
- ✓ Extensive testing tools and frameworks
- ✓ Lint tools to catch performance, usability, version compatibility, and other problems
- ✓ C++ and NDK support

Built-in support for Google Cloud Platform, making it easy to integrate Google Cloud Messaging and App Engine. [30]

Figure3.2. Interface of Android Studio. [30]

3.3 Proposition:

In recent years, the security and protection of personal information has become an important in wireless communications, especially with the great increase in data demand and the large number of defects in RF in keeping pace with this increasing, which has led scientists from around the world to search for new technologies that can meet the increasing data rates at a lower cost. The best candidate was Visible light communication (VLC)technology, as the multiple advantages of this technology convinced many scientists to put their efforts to develop this technology in all its

fields, and it was the first research in the world in the Asian countries, where it added a great contribution to the progress of VLC.

3.4 Design and Implementation:

3.4.1 Methodology:

We designed a small application mobile of key management using visible Light communication in Android Studio 4.1 on windows System.

The principle working of this application is based on input a password Easy to remember to derive a Key from it using Password Based Key Derivation Function 2 algorithm. The light-emitting diodes (LEDs) are employed to transmit derived key. and light sensors are using to detect the light coming across line of sight to analysis it and extraction the data carries (the key).

3.4.1.1 The sender side:

A flash light was a suitable component because are semiconductors, they have the ability to turn off and turn on with times of the order of nanoseconds, his task is to convert digital data into visible light.

the data encode according to Manchester modulation. Where a '1' is represented by no light followed by a light pulse, and '0' is represented by a light pulse followed by no light. the encoded data is fed to the LED for transmission through the unidirectional optical channel

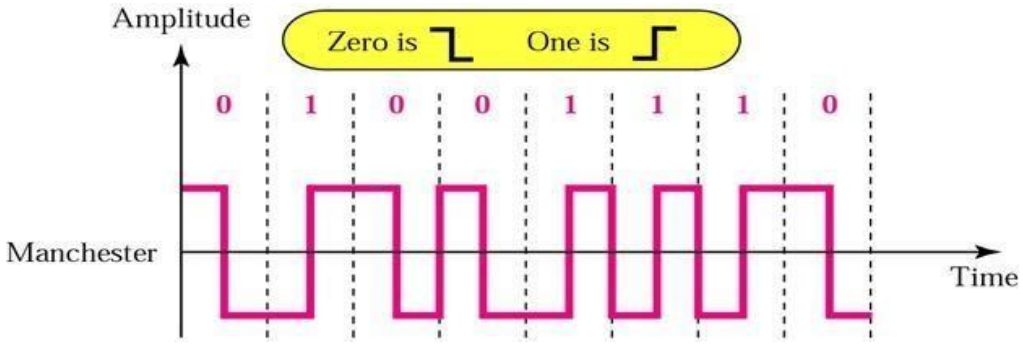

Figure 3.3. Manchester modulation. [32]

3.4.1.2 The receiver side:

We used as receiver light sensor, which is a semiconductor converting light into an electrical current.

When the transmitted light arrives across the line of sight between sender and receiver, demodulator recovers transmitted bits (key) and then by observing low to high '1' transition and high to low '0' transition Manchester decoding is implemented. Because the data transferred is a key, so to guarantee that the receiver has received the same key send by the transmitter I suggest Wi-Fi since the key is already sent.

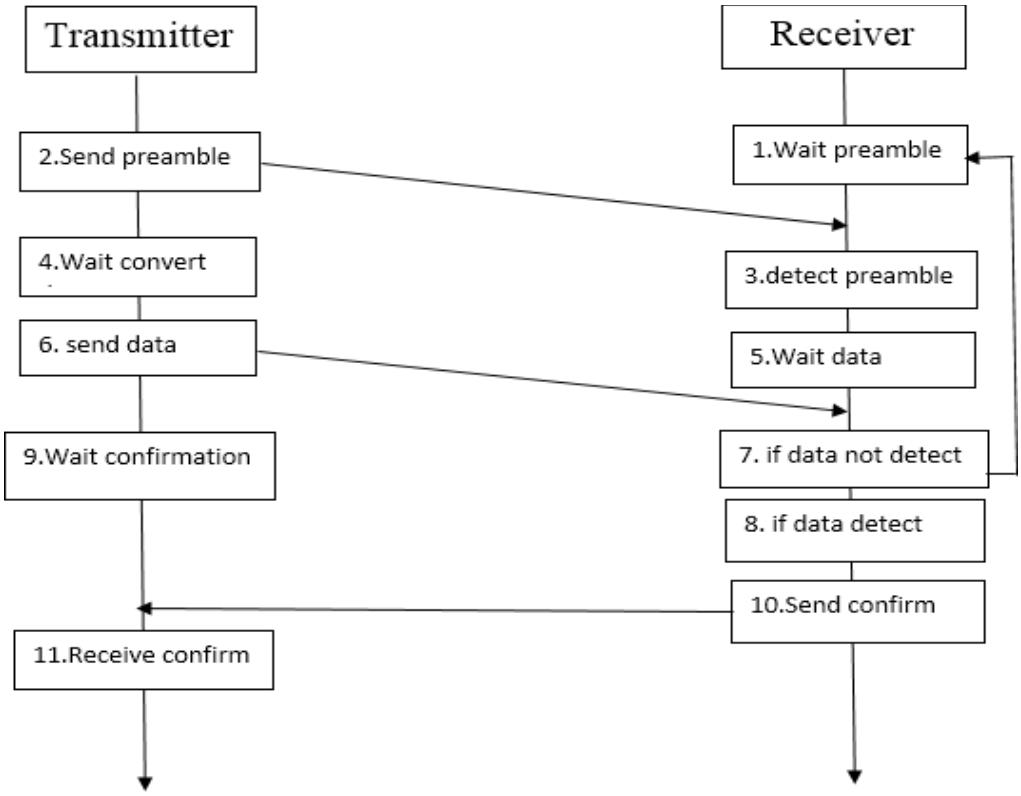

Figure 3.4. Protocol of VLC transmission

Line-of-sight and bandwidth are two important conditions in VLC communication, where the transmission cannot be establishing in the absence of line-of-sight between the transmitter and the receiver. Otherwise, the receiver is required to be the emitting range of the transmitter. In figure 3.4, we propose as a concept to adding this protocol for communication in VLC system.

The transmission starts when the transmitter send preamble empty (sequence of binary symbols non encoded 010101 modulate as light on and off) to wake up the receiver. Then waiting for data converted into binary symbols (1 and 0) which modulated by light to ON and OFF pulse Led using Manchester modulation.

After sending preamble. The transmitter sending data which is a key, then waiting for affirmation of sending from receiver.

In the other side, after waiting of preamble the receiver is detecting it, and is looking for receiving the data (key), then data incoming in the beam lighting across the line of sight, when the transmission is succeeding, the receiver send affirmation to sender which is ACK sending using Wi-Fi (our proposition). If it fails, the receiver will be waiting a new preamble.

3.5 Results:

3.5.1 Demonstration of devices pairing using VLC:

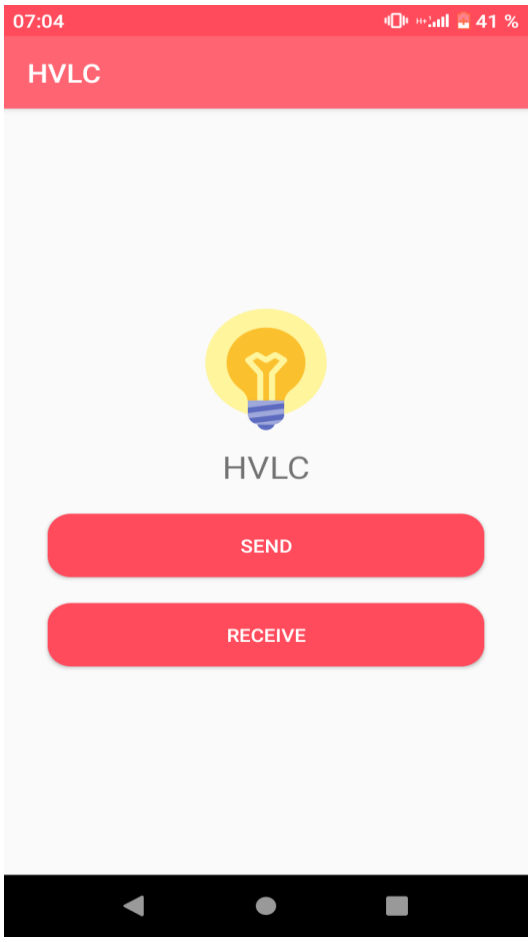

Figure 3.5. The main user interface.

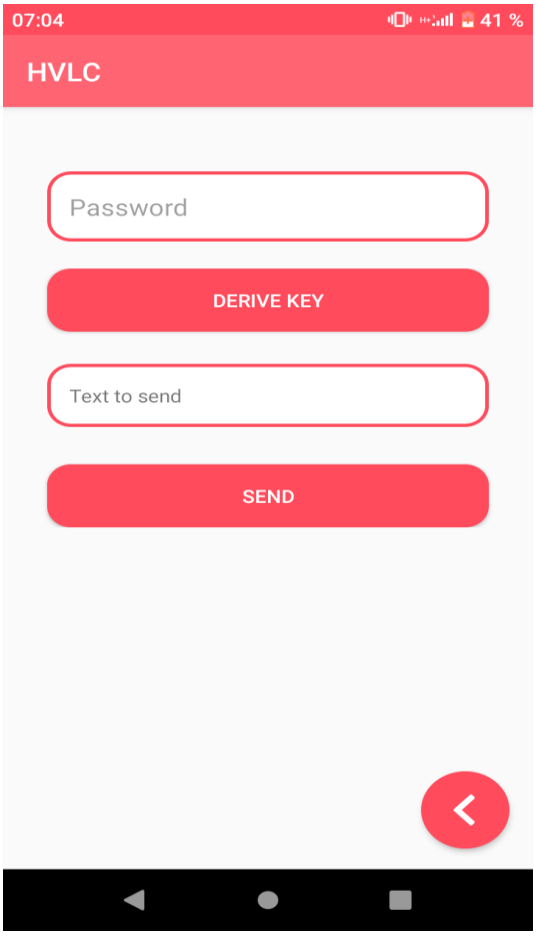

Figure 3.6. Sender interface

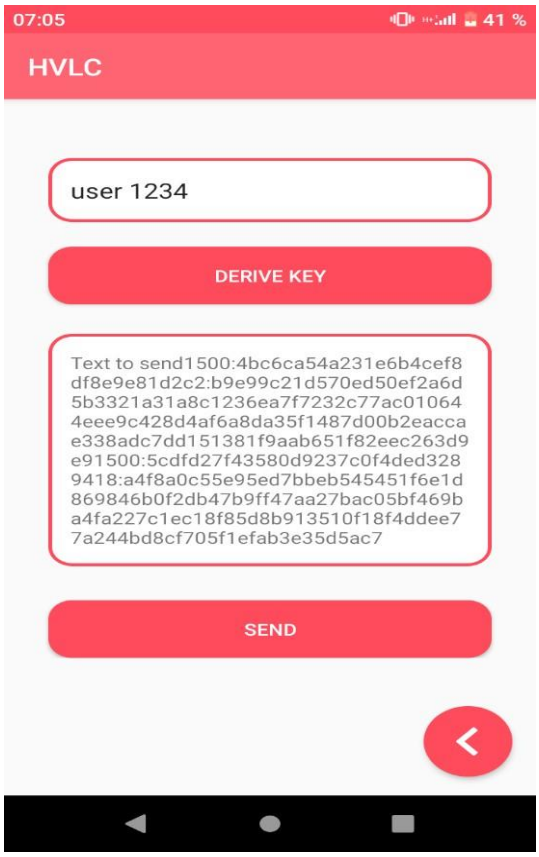

Figure 3.7. Sender procedures.

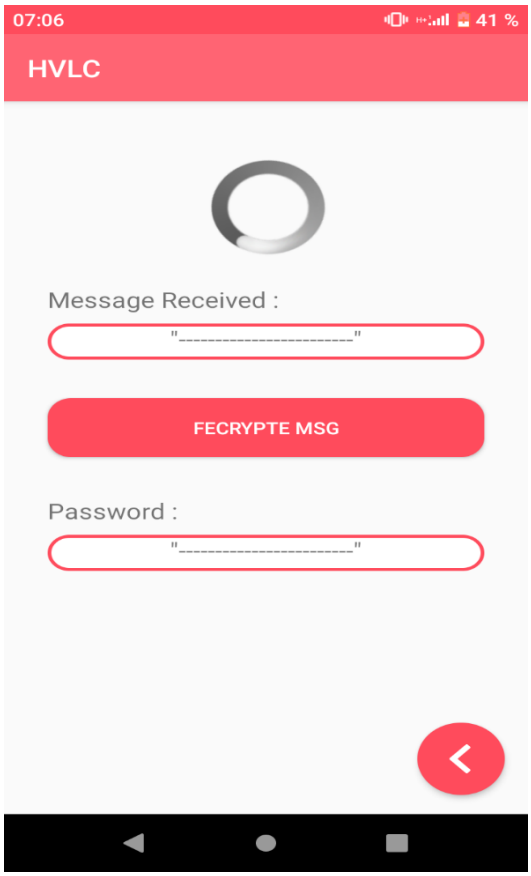

Figure 3.8. Receiver interface.

3.6 Conclusion:

In this chapter, some related concepts on key generation are introduced, we presented our proposition, the details implementation of application, and the overall result of this project.

Conclusion and future Work

The main goal of this effort was establishing a secure pairing communication using visible light, by sharing a secure key.

To achieve this goal, we derived a Key from password using Password Based Key Derivation function which depends mainly on the salt and the iteration count. We resort to this type of function to generate a strong key can thwart dictionary attacks or pre-computation attacks. then we shared it using visible light between tow devices where it requires to have on one a flash light for transmitted and in the other a photodiode to receive light beams carries the Key in binary data (1 and 0) form and process it to extract the key transmitted. Due to the conditions that we have gone through and the severe weakness of the Internet, we could not complete the work, we were only able to send a light message from the sender's side, and we hope to complete the receiver side in the near future, which we still working on it.

Bibliography

[1] Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb, Chadi Assi, Majid Safari, Harald Haas. (May 2019). Physical Layer Security for Visible Light Communication Systems: A Survey.

[2] Grzegorz Blinowski. (2015). Security issues in visible light communication systems

[3] Jonathan M. McCune, Adrian Perrig. (2009). Seeing-Is-Believing: using camera phones for human-verifiable authentication.

[4] Dr. Asha T S, Drisya K. (February 2019). Visible Light Communication [VLC] and its Applications.

[5] Mr. Yogesh Chavan, Mr. Ramchandra Gurav. (January 2017). Data Transfer using Visible Light Communication.

[6] รศ.ดร.ปิยะโควินท์ทวีวัฒน, ดร.วรรณรีย์วงศ์ไตรรัตน, รศ.ดร.อนันต์สืบสำราญ, ดร.กมลเขมะรังษ, รศ.ดร.ปรีชากอเจริญ. Visible Light Communication(VLC)and its Applications The reference found in: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjbtonEoOHxAhULmBQKHboRA-sQFnoECAcQAA&url=http%3A%2F%2Fdept.npru.ac.th%2Fvlc%2Fdata%2Ffiles%2F%25E0%25B9%2580%25E0%25B8%25AD%25E0%25B8%2581%25E0%25B8%25AA%25E0%25B8%25B2%25E0%25B8%25A3%25E0%25B8%25AD%25E0%25B8%259A%25E0%25B8%25A3%25E0%25B8%25A1%25201%2520-%2520Visible%2520Light%2520Communication%2520and%2520Its%2520Applications.pdf&usg=AOvVaw1SB8vM8oKfcMk7D33rL69i On: 5 April 2020.

[7] Alain Richard Ndjiongue, Hendrik. C. Ferreira, Telex M. N. Ngatched. (2006). Visible Light Communications (VLC) Technology.

[8] Yu Chen. (12-1-2019). A NEW RLL CODE FOR VISIBLE LIGHT COMMUNICATION SYSTEM.

[9] Faisal A. Dahri, Sajjad Ali, Muhammad Moazzam Jawaid. (February2018). A Review of Modulation Schemes for Visible Light Communication.

[10] Alin-Mihai Cailean, Barthélemy Cagneau, Luc Chassagne, Mihai Dimian, Valentin Popa. (May 2014). Miller Code Usage in Visible Light Communication sunder the PHY I Layer of the IEEE 802.15.7 Standard.

[11] Prateek Gawande, Aditya Sharma, Prashant Kushwaha. (November2016). Various Modulation Techniques for Li-Fi.

[12] Stefano Truzzi. (2015/2016). VISIBLE LIGHT COMMUNICATION

[13] Alin-Mihai CĂILEAN. (December 2014). Study, implementation and optimization of a visible light communications system. Application to automotive field.

[14] Saeed Ur Rehman, Shakir Ullah, Peter Han Joo Chong, Sira Yongchareon, Dan Komosny. (Published 7 March 2019). Visible Light Communication: A System Perspective—Overview and Challenges.

[15] Latif Ullah Khan. (Accepted 18 July 2016). Visible light communication: Applications, architecture, standardization and research challenges.

[16] Aatifah Noureen, Umar Shoaib, Muhammad Shahzad Sarfraz. (2017). Secure Device Pairing Methods: An Overview. Found in https://www.semanticscholar.org/paper/Secure-Device-Pairing-Methods%3A-An-Overview-Noureen-Shoaib/27e6726670cacecfcb78f1c9463757c2b8a4df7e On: 10 April 2020.

[17] Arun Kumar, Nitesh Saxena , Gene Tsudik , Ersin Uzun. (18 July 2009) A comparative study of secure device pairing methods.

[18] Khawla Bouchelghoum. (07/2019). Key management using visible light communication. Found in http://dspace.univ-msila.dz:8080/xmlui/handle/123456789/15936 On: 4 April 2020.

[19] Markku Antikainen, Mohit Sethi, Sinisa Matetic, Tuomas Aura. (January 2015). Commitment-based device-pairing protocol with synchronized drawings and comparison metric.

[20] Liju Sajan, Lince Mathew, Abraham Thomas, Sarun Sathyan, Bibin Baby. (2015). WIRELESS DATA TRANSFER USING VISIBLE LIGHT COMMUNICATION.

[21] Sumit Jaykant Meshram, Prof Avinash P Wadhe. (2016). Secure data transfer using visible light communication Technique.

[22] Bingsheng Zhang, Kui Ren, Guoliang Xing, Xinwen Fu, Cong Wang. (2014). SBVLC: Secure Barcode-based Visible Light Communication for Smartphones.

[23] Abdalah Hilmia, Kasun Hewage, Ambuj Varshney, Christian Rohner, Thiemo Voigt. (April 2016). Poster Abstract: BouKey: Location-Based Key Sharing Using Visible Light Communication.

[24] Estuardo Rene Garcia Velasquez. (June 2016). Sending Location-Based Keys Using Visible Light Communication

[25] Seok-Jeong Song, Hyoungsik Nam. (April 2017). Visible Light Identification System for Smart Door Lock Application with Small Area Outdoor Interface

[26] Hanna Willa Dhany, Fahmi Izhari, Hasanul Fahmi, Tulus, Sutarman. (2017). Encryption and Decryption using Password Based Encryption, MD5, and DES.
[27] B. Kaliski RSA Laboratories. (September 2000). PKCS #5: Password-Based Cryptography Specification Version 2.0.
[28] Meltem Sönmez Turan, Elaine Barker, William Burr, Lily Chen. (December 2010). Recommendation for Password-Based Key Derivation Part 1: Storage Applications.
[29] Marijke De Soete. Derived Key, found in: https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_284 On: 12 August 2020
[30] https://developer.android.com On: 20 August 2020
[31] Fadi Hani Khudur, Samer Majed Al-saady, Alaa Adnan Saleem. (October 2016). The Assessments and Challenges of LED Generated Data Traffic using Li-Fi Technology.
[32] Ajarn Preecha Pangsuban. Data Communications System.

Summary:

Over many years, researchers have been trying to secure a reliable wireless communication. The main challenge lies in the keys management that cover the creation of a shared secret between two wireless devices through which sensitive information can be exchanged.

Several pairing protocols have already been developed in wireless communication, but they do not meet the quest because they use the directly generated secret key as a potentially weak encryption key for authentication, and they are not sufficient to transfer large amounts of data at high speed. So other wireless standards define or define similar protocols, and are designed for specific technologies to solve these shortcomings. In this thesis, a new protocol describing the visible light communication specification is proposed as an alternative solution to existing radio-based protocols in wireless communication which is builded by LEDs to transmit data. This transmission prototype is there tested and analysed with a photodetector in the reception.

Keywords: VLC (Visible Light Communication), LED (Light Emitting Diode), photodetector, phototransistor, photodiode, secret key, key management.

Résumé :

Depuis de nombreuses années, les chercheurs tentent de sécuriser une communication sans fil fiable. Le principal défi réside dans la gestion des clés qui couvrent la création d'un secret partagé entre deux appareils sans fil à travers lesquels des informations sensibles peuvent être échangées.

Plusieurs protocoles d'appariement ont déjà été développés dans la communication sans fil, mais ils ne répondent pas à la quête car ils utilisent la clé secrète générée directement comme clé de cryptage potentiellement faible pour l'authentification, et ils ne sont pas suffisants pour transférer de grandes quantités de données à grande vitesse. Ainsi, d'autres normes sans fil définissent ou définissent des protocoles similaires et sont conçues pour des technologies spécifiques afin de résoudre ces lacunes. Dans cette thèse, un nouveau protocole décrivant la spécification de communication par la lumière visible est proposé comme solution alternative aux protocoles radio existants dans la communication sans fil qui est construit par des LED pour transmettre des données. Ce prototype de transmission est testé et analysé avec un photodétecteurs à la réception.

Mots clés : VLC (Visible Light Communication), LED (Light Emitting Diode), photodétecteur, phototransistor, photodiode, clef secrète, la gestion de clés.

ملخص:

عبر سنوات عديدة، يسعى الباحثون لتامين اتصال لاسلكي موثوق، يكمن التحدي الأساسي في إدارة المفاتيح التي تغطي انشاء سر مشترك بين جهازين لاسلكيين يمكن من خلاله تامين تبادل المعلومات الحساسة.

تم بالفعل تطوير العديد من بروتوكولات الاقتران في الاتصال اللاسلكي، لكنها لا تلبي المسعى كونها تستخدم المفتاح السري الذي تم إنشاؤه مباشرة كمفتاح تشفير الذي يحتمل أن يكون ضعيفًا للمصادقة، كما انها غير كافية لنقل سعة كبيرة من البيانات وبسرعة فائقة. لذلك حددت معايير لاسلكية أخرى بروتوكولات مماثلة أو تقوم بتعريفها، ومصممة لتقنيات معينة لحل هذه العيوب. في هذه الرسالة، تم اقتراح بروتوكول جديد يصف مواصفات الاتصال بالضوء المرئي كحل بديل للبروتوكولات الحالية القائمة على الراديو في الاتصالات اللاسلكية المبني على الصمام الثنائي الباعث للضوء لإرسال البيانات تختبر وتحلل من طرف الكاشف الضوئي.

الكلمات المفتاحية: VLC (اتصالات الضوء المرئي)، LED (الصمام الثنائي الباعث للضوء)، الترانزستور الضوئي، الثنائي الضوئي، المفتاح السري، إدارة المفاتيح.