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

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

Domain :Mathematics and Computer Science

Branch : Computer Science

Specialty : networks and information and communication technology

By : Khawla Bouchelghoum

TOPIC

Key management using visible light communication

Publicly defended : / 07 /2019 before a Jury composed of:

Azeddine Attir	**University of M'sila Supervisor**
……	**University of M'sila protractor**
……	**University of M'sila Examiner**

Academic Year : 2018 /2019

First of all, I would like to express my sincere gratitude to my supervisor Azeddine Attir , thank you so mach for all knowledge you given to me And for this thesis and to provided me with a great deal of useful guidance and suggestions for this project.

I also would like to deepest grateful to my wonderful mother , all my beautiful family and my friends for all their love and support

Thank you Hamza to was always with me as friend more than you as a brother

Finally, I am deepest grateful to all my teachers specially ms.saoudi .

Table of Contents

CHAPTER 3 : PROPOSITION AND IMPLEMENTATION

List of figures

Terminology

Acronyms

VLC	Visible Light Communication
OOB	Out Of Band
IOT	Internet Of thing
RF	Radio Frequency
ITS	Intelligent Transport Systems
IR	InfraRed
NFC	Near_Field Communication
XML	eXtensible Markup Language
OWC	Opptical Wireless Communication
SSL	Solid State Lighting
MTBF	Prolonged Mean Time Failure
MIMO	Multiple Input Multiple Output
PBE	Password Based Encryption
PRNG	Pseudo Random Number Generator
ADT	Android Development Tools
UV	UltraViolet
PBKDF2	Password-Based Key Derivation Function 2

GENERAL INTRODUCTION

1.introduction:

As communications and information technology continue to evolve, short range wireless communication technology is becoming more mature. The general sense is that as long as the communication transceiver transmits information via radio waves, both sides and the transmission distance are limited to the shorter range (tens of meters) or less, that this can be called short-range wireless communications. Short-range wireless communications, for example IrDA, Bluetooth and 802.11(Wi-Fi), assist people to avoid physical connections, thus making people's lives more convenient.

Currently, more and more short-range wireless communication products are appearing in daily life, such as transmitting the data between two smart phones via Bluetooth and, additionally, the information being transmitted among the body sensors.

Since sensitive private information is collected or transmitted in these products, their security becomes issues of concern. [1]

we have focused on using VLC because the researchers proposed that attackers will be unable to intercept, modify or produce fake messages.

1.1.Visible light communications (VLC)

Is the name given to an optical wireless communication system that carries information by modulating light in the visible spectrum (400–700 nm) that is principally used for illumination . The communications signal is encoded on top of the illumination light. Interest in VLC has grown rapidly with the growth of high power light emitting diodes (LEDs) in the visible spectrum. The motivation to use the illumination light for communication is to save energy by exploiting the illumination to carry information and, at the same time, to use technology that is "green" in comparison to radio frequency (RF) technology, while using the existing infrastructure of the lighting system. The necessity to develop an additional wireless communication technology is the result of the almost exponential growth in the demand for high-speed wireless connectivity [2] Emerging applications that use VLC include:

a) communication wireless links for the internet of things (IOT) ;

b) communication systems as part of intelligent transport systems (ITS) ;

c) wireless communication systems in hospitals ;

d) toys and theme park entertainment ; and,

e) provision of dynamic advertising information through a smart phone camera .

1.2.Background and problem motivation

As the usage of mobile devices (cell-phones, PDA's, cameras and media players) is increasing, the need of spontaneous connection of two devices over a wireless connection has also become essential . The main advantage of using wireless technologies like Wi-Fi or Bluetooth is that ad hoc communication can take place without the infrastructure or any overhead charges to the users . There are many situations where devices interact with each other such as sharing files, photos and videos with the friends. It also includes editing the documents and reports cooperatively in a conference, and playing games with multiple players and exchanging of digital business cards. Sometimes, a single user controls both devices (e.g. communication between Alice's cell phone and her wireless headset or her PDA and a wireless printer) and sometimes two different users control their respective devices. (e.g. communication between A's and B's devices such as laptops/ PDAs or cell phones for professional or social reasons) .

But the heavy usage of these devices may carry many security risks. Sharing data with strangers and at public places (markets, parks and airports) may result in more concerns of security and privacy . As the wireless radio communication channels can easily be eavesdropped and manipulated, which raises many threats. Evil Twin attack as shown in Fig. 1 and Man-in-the-Middle which is shown in figure 1. 1 are the most common attacks . [3]

Figure 1. 1. Evil Twin attack.

figure 1. 2. Man-in-the-Middle attack.

1.3.Overallaim

This thesis concentrates on sharing a security key by using a LED and receive it by light sensor that areable to reduce the human burden in addition to achieving the desired level of security.

An attempt is also made, in this thesis, to implement a small application mobile using visible Light . In particular, their usability and security are evaluated.

1.4.Concrete and verifiable goals:

The goals of this thesis are listed as follows:

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

CHAPITER 1:

DEVICES PAIRING IN WIRELESS NETWORKS

1. devices pairing in wireless networks

1.1. introduction

In recent years, the advances in automation and a rapid growth of the consumer electronics market have resulted in a tremendous increase in the number of smart devices and personal gadgets. that's make devices pairing becoming more important, and there are a lot of methods to get pairing that use in technologies like bluetooth and wifi..

In this chapter, some Secure Devices Pairing Methods are introduced, including Protocol Independent Secure Pairing and devices pairing technologies.

1.2. Secure Devices Pairing Methods :

Figure 2. 1 is shows a categorization of some pairing methods along with the process details. The detailed steps involved in each steps are also explained.

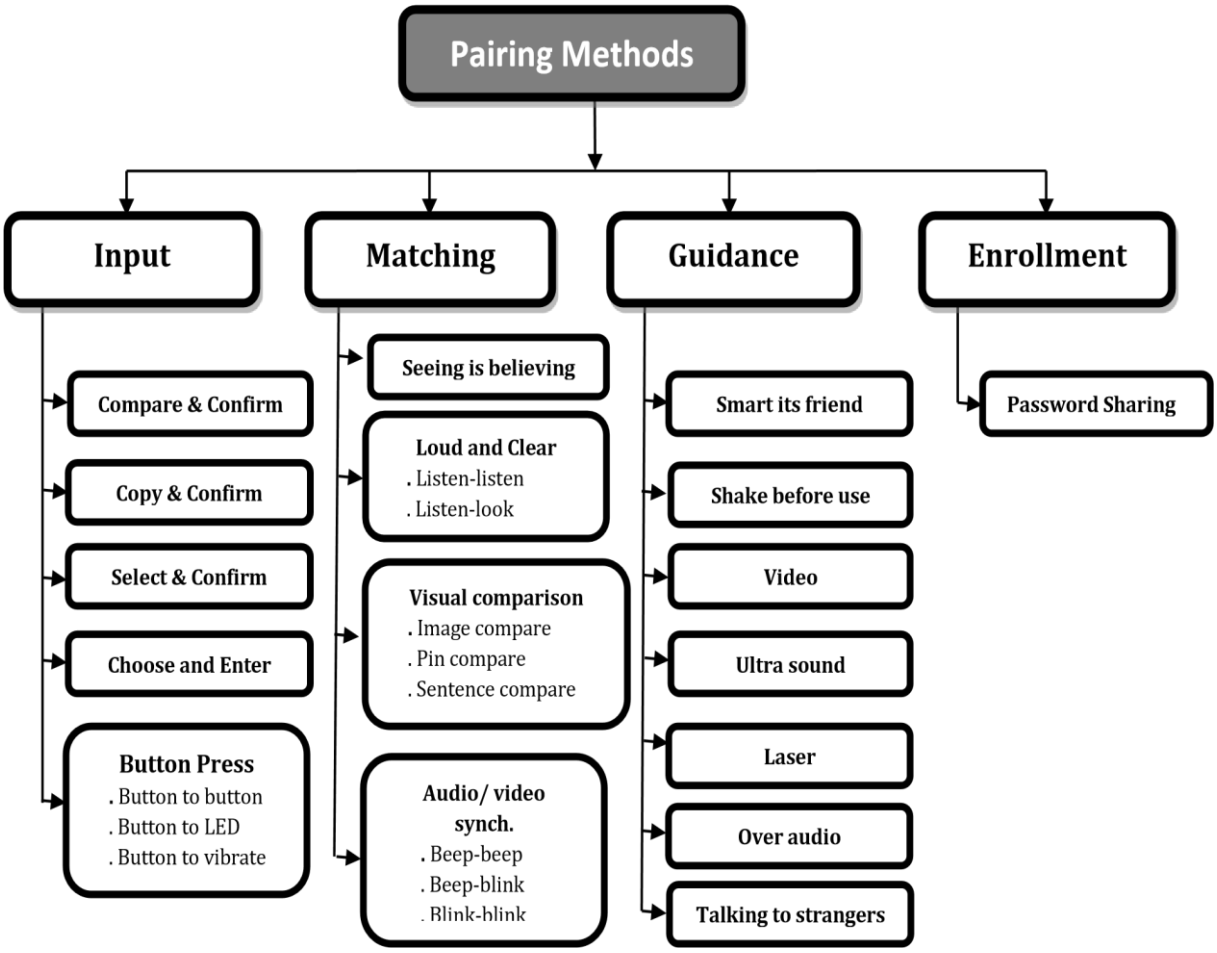

Figure 2. 1 Categories of pairing methods.

1.2.1. 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:

a. Compare and Confirm:The devices display a 4, 6 or 8-digit number and the user compares these and then decides to enter. This is quite inefficient and time taking and having high error rate .
b. Select and confirm:In this method a device shows one number and the other device show a series of numbers from which user selects the matching one to confirm the offer.
c. Copy and confirm:The number is copied by user from one device to another .
d. Choose and enter:In this four or eight-digit number is randomly chosen and then entered by user into each device. Its security is considerably weak due to user‘s choice.
e. Button press:

- Button to button: As name shows this method is based on pressing specific buttons to establish pairing connection. In random time interval user has to press the button simultaneously on both devices A and B. The devices are encoded with instructions to start timer when first button is pressed and then calculate secret key in the time interval between first button press on device A and second button press on another device B. 3 bits‘ secret key is generated in every time interval .

- Button to LED: In this approach a button is pressed on device A on the basis of display message generated by device B. The device B chooses a key, express it into a code and transfer it in form of display flashes on device A then user press a button in response and timer is started just like previous method in which sharing key bits are calculated by device.

- Button to vibrate: The users enter a button on device B when device A vibrates.Acceptation and rejection on device A is also based on output of device B .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 [3].

1.2.1.1.Pros of input methods:

These methods are simple, easy to use and easy to understand.

1.2.1.2.Cons of input method:

- Devices must have a keyboard/keypad
- Humans are not good random number/string generators
- High error rate
- Not highlysecure. [3].

1.2.2. Matching

The users perform comparison of the output of devices in order to establish or reject a connection. For example, many wireless sensors ask the users compare the numeric values which are displayed on the connecting devices in order to check whether these numbers are similar or not. It includes:

a. Seeing is believing: Device display a barcode and user have to take snap shot with device A then reject or accept the outcome on B on the basis of output appeared on A. It has limitations as all devices don‘t have big displays to show twodimensional bar codes. All devices don‘t have good quality cameras. Placing the devices sufficiently close and aligning the camera may not always be possible.

b. Loud and clear: The vocalized sentences and audio OOB channel are used in combination to exchange information on wireless channel :

- Listen-Listen: As three-word sentence is vocalized on both devices 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 bothdevices .
- 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 [3].

c. Visual Comparisonbased :

- Image Compare: A visual pattern is presented by both the devices then user is required to make a comparison. If both patterns accurately matched the decision is entered on both devices by user. Hash and colorful flag , snowflake, and random arts visual are

common example of this method. Its applicability requires high resolution devices on both ends such as PDAs, laptops and few specific cellphones .

- Pin Compare: A five-digit number appeared on two connecting devices, the user has to compare them and ultimate decision is entered by him/her at both ends .
- 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 . [3]

d. Audio/video synch

In this technique Beep-Beep, Beep-Blink and Blink-Blink methods are used. In this technique, users compare simple audio and visual patterns for syncing :

- Beep-beep: It requires devices to have a speaker.
- Beep-blink: It requires devices to have a LED and a basic speaker.
- Blink-blink: It requires devices to have a LED. [3]

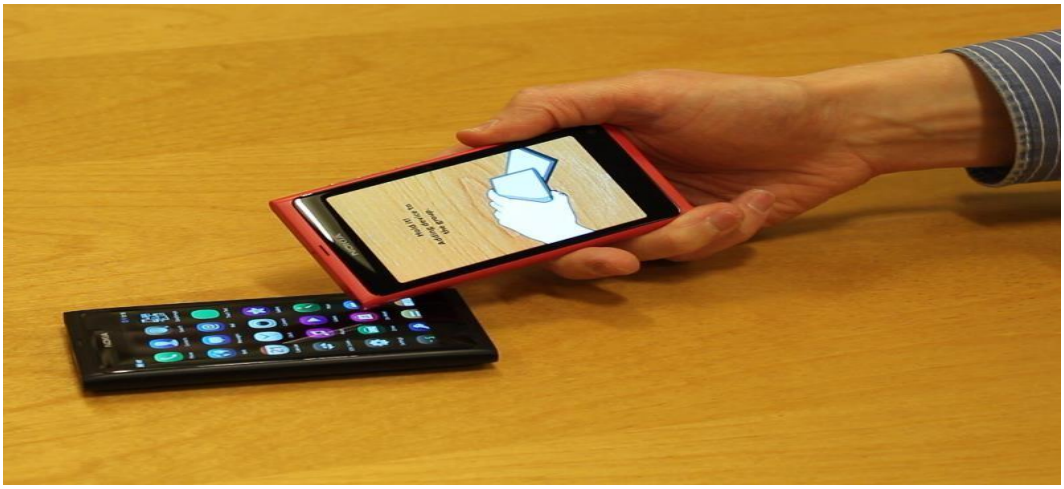

Figure 2. 2 Touching device to add it to the group.

1.2.3. 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 Fig. 2 to establish a connection in Android Beam. It includes the following:

a. Smart it's Friends: The user shake both devices together that results in a secret pattern transmission between two devices

b. Shake well before use: The two axis accelerometer is required on both devices and
c. 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 .
d. Ultrasound: Ultrasound is used as OOB channel but it is quite expensive and rarely used method.
e. Laser based: Laser transceiver is required on both devices through which laser beam could be used for pairing process.
f. 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.
g. Over audio: This method is preferably used by the devices that do not possess any common wireless channel. An audio protocol of cryptographic message is transmitted that is then closely monitored by user to avoid any third party interruption. Microphone and speaker shouldbepresent in bothdevices .
h. Talking to stranger: This method depends on infrared (IR) communication and doesn‘t require user involvement, except in initial setup, Problems in using talking to stranger: Finding and turning on IR ports, IR is invisible to humans; man in middle attack is still possible.

1.2.4. Enrollment

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

a. Password sharing: 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. [3]

1.3. Protocol Independent Secure Pairing

To engage in secure and privacy preserving communication, hosts need to differentiate between authorized peers, which must both know about the host's presence and be able to decrypt messages sent by the host, and other peers, which must not be able to decrypt the host's messages and ideally should not be aware of the host's presence. The necessary relationship between host and peer can be established by a centralized service, e.g. a certificate authority, by a web of trust, e.g. PGP, or -- without using global identities - by device pairing.

Many pairing protocols have already been developed, in particular for the pairing of devices over specific wireless networks. For example, the current Bluetooth specifications include a pairing protocol that has evolved over several revisions towards better security and usability [BTLEPairing]. 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 nvironments [WPS]. Other wireless standards have defined or are defining similar protocols, tailored to specific technologies. [3]

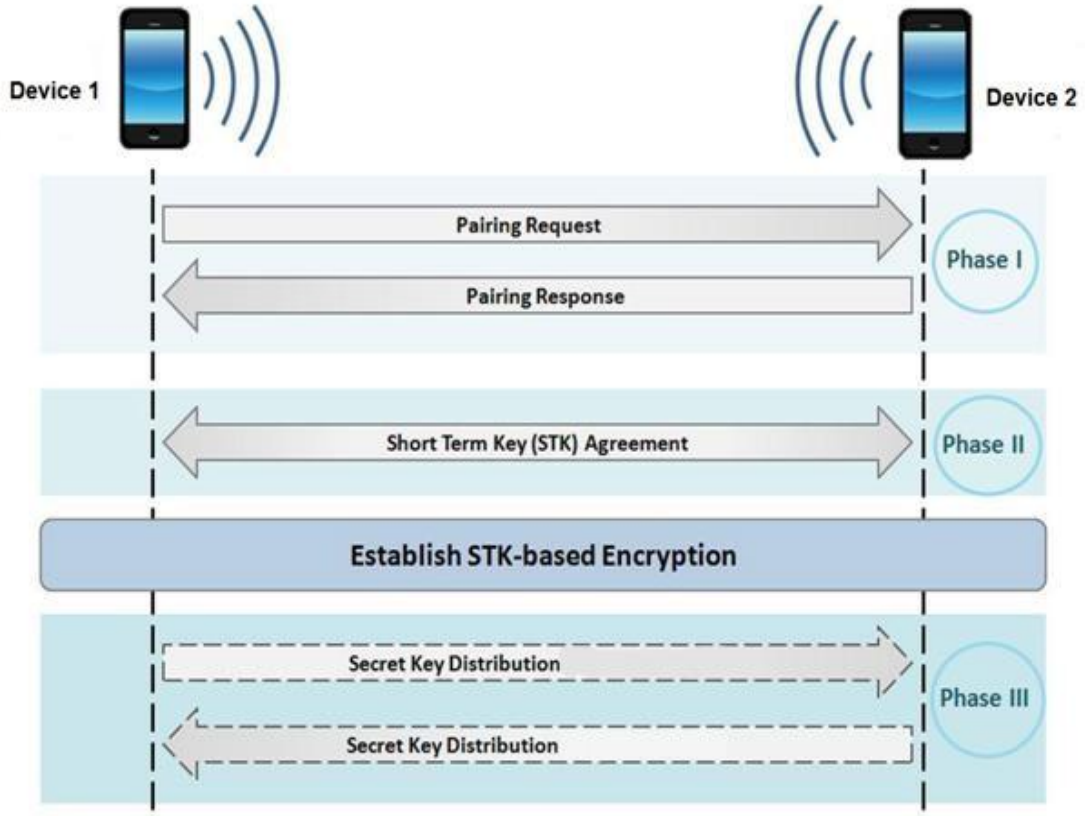

Figure 2. 3 Simple device pairing protocol.

1.4. devices pairing technologies

there is a lot of pairing devices technologies in our nowadays and some of it is so useful like bluetooth, NFC and wifi.some technologies in this project are introduced.

1.4.1. Bluetooth Technology

The Bluetooth is a wireless technology, used for transferring the data from one device to the other device. The distance between the two devices is very short from the fixed, mobile device and building personal area network. The Bluetooth technology is developed by the Bluetooth special interest group and its physical range is from 10m to 100m. The **Bluetooth**

device can connect up to seven devices and it is used in the industry like smartphones, personal computers, and gaming consoles, etc. The IEEE standardized Bluetooth as IEEE 802.15.1, but the standards are maintained for short periods. [4]

Figure 2. 4 Bluetooth Technology

1.4.2. NFC(near-field communication)

NFC stands for near-field communication and it allows phones, tablets, laptops, and other devices to easily share data with other NFC-equipped devices. The technology evolved from radio-frequency identification (RFID) tech. RFID is behind those security scan cards that get you into the office every day or bypass that tollbooth on your morning commute.

NFC is very much like RFID, but NFC is limited to communication within about four inches which is why you have to hold your phone so close to the contactless reader if you're using Apple Pay or Samsung Pay. Most people consider NFC's small radius a major security benefit, and it's one of the reasons that NFC has taken off as a secure alternative to credit cards. The technology can be used for more than buying coffee at Starbucks, however. NFC

can also transfer data like videos, contact information, and photos between two NFC-enabled devices.[5]

Figure 2. 5 NFC Technology.

1.4.3. ZigbeeTechnology

Zigbee communication is specially built for control and sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs), and it is the product from Zigbee alliance. This communication standard defines physical and Media Access Control (MAC) layers to handle many devices at low-data rates. These Zigbee's WPANs operate at 868 MHz, 902-928MHz and 2.4 GHz frequencies. The date rate of 250 kbps is best suited for periodic as well as intermediate two way transmission of data between sensors and controllers.[6]

Figure 2. 6 ZigbeeTechnology.

1.4.4. Wi-Fi Direct Technology

Wi-Fi CERTIFIED Wi-Fi Direct® is a certification mark for devices supporting a technology that enables Wi-Fi devices to connect directly, making it simple and convenient to do things like print, share, sync and display. Products bearing the Wi-Fi Direct certification mark can connect to one another without joining a traditional home, office or hotspot network.

Mobile phones, cameras, printers, PCs, and gaming devices connect to each other directly to transfer content and share applications quickly and easily. Devices can make a one-to-oneconnection, or a group of several devices can connect simultaneously. Connecting Wi-FiDirect-certified devices is easy and simple, with the push of a button, tapping two NFC-capable devices together, or entering a PIN. Moreover, all Wi-Fi Direct connections are protected by WPA2™, the latest Wi-Fi security technology. With Wi-Fi Direct, you do not need an access point or internet connection – your personal Wi-Fi network goes with you wherever you go. [7]

Figure 2. 7 Wi-Fi Direct Technology

1.5. conclusion

this chapter we introduce categorization of some pairing methods along with the process details and some fames technologies we use it every day to get pairing and we shows how work a Simple device pairing protocol and in the next chapter we will offers an overview of the related work aspects related to Secure devices pairing by using visible light.

CHAPTER 2:

SECURE DEVICES PAIRING USING VISIBLE LIGHT

2. Secure devices pairing using visible light

2.1. introduction

VLC has been recently proposed as an alternative security method because of its physical characteristics, VLC is considered a secure communication.

In this chapter, some related works about security using visible light communication in this project are introduced, including Secure Mobile Payment using Visible light communication with FSK modulation [8], Beam Scanning based Secure Communication using Visible Light [9], Secure data transfer using visible light communication Technique [10], and Shu using NSF grant to advance visible light communication security. [11]

2.2. Secure Mobile Payment using Visible light communication with FSK modulation

The authors of Secure Mobile Payment using Visible light communication with FSK modulation developed Wireless Cash Transactions using Visible Light Communication application, they based in VLC because Visible light communication systems provide an alternative to the current standards of wireless transfer of information, using light from LEDs as the communication medium. In these systems, light-emitting diodes blink at a rapid rate such that the human eye will not notice the change in light intensity, but a sensitive photodiode can detect the on-off behavior and decode the information embedded within it. The demonstrated version of this idea transmits an FSK at 1KHz and 5 KHz.

In the transmission and reception of their application they didn't use the conventionally path of FSK modulation that involves the use of sequence seperate frequencies to represent a 0 and a 1 that Conventionally it is implemented using multipliers and a frequency generator. They want to keep the transmitter as simple as possible so they opted a different path.

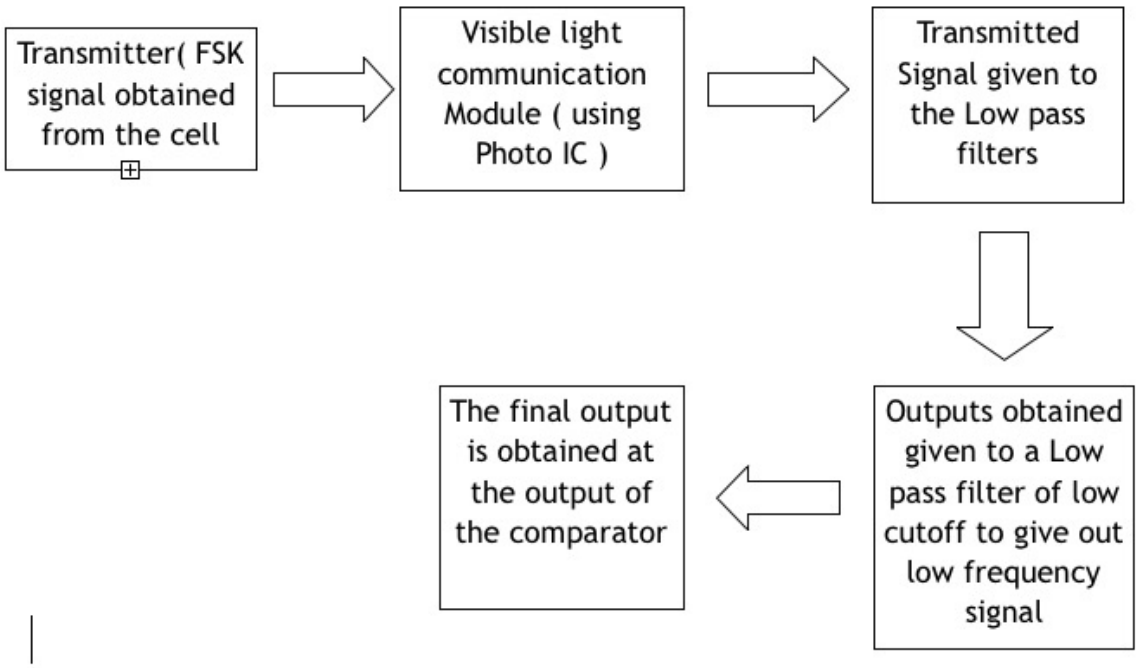

Figure 3. 1 Block diagram of the transceiver

They created an FSK signal using audacity converted it into a file with extension ".ogg" . This is essentially an audio clip of a very small duration. If we play this signal on a smartphone and observe the corresponding waveform on a DSO, they would see an FSK signal.

Afrah Mariyam and the other authors developed an android application used java as a primary programming language. All the back end functions and the functions, playing audio, programming is implemented in Java. The user interface ie front end is implemented using XML (Extensible Markup Language) and both the back end and front end are connected together in the Java program. they have used the Android Studio IDE (similar to eclipse IDE) to program the application.

The application consists of two buttons. One to send a test signal and another to send the required data. The user needs to type the required sequence of numbers in the text field. Each number in this sequence is mapped to the corresponding FSK signal (audio signal generated using audacity).

Through their project, they have demonstrated a proof of the concept that it is possible to transfer data from a smart phone to another device via the audio jack implementing FSK.

The transmitter is designed to be extremely compact and cost effective. Phone manufacturers could implement this technology to utilize the inbuilt flash light in

smartphones. [8]

2.3. Beam Scanning based Secure Communication using Visible Light

Muhammad Saadi and Ali Nasir propose a novel technique for secure data transmission at physical layer. Two transmitters are used for transmission the data instead of one. The receiver will only be able to reconstruct the transmitted data if it can receive data from both LEDs. For the reasons of Visible light communication (VLC) which is a part of optical wireless communication (OWC) is one of the promising technology which has the potential to fulfill the emerging needs of bandwidth and ensures environmental friendliness . With recent advancements in solid state lighting (SSL), VLC have provided a unique opportunity to realize low cost, hazard free, high speed, energy efficient and secure wireless communication in conjunction to lighting . LEDs offer many advantages over conventional and florescent lighting such as high tolerance to humidity, prolonged mean time before failure (MTBF), low power consumption, mercury free etc. Radio frequency (RF) communication spectrum is not only getting congested but also suffers from its open nature of RF propagation which give rise to significant security threat. However, as light cannot pass through the concrete structure so it gives an in-built security thus reducing the chances of eavesdropping, traffic analysis, resource consumption, message modification, masquerade attacks and hacking . An un-intercepted secure transmission of confidential information only to the intended user(s) is crucial in modern information and communication era. To maintain the data integrity, classical network cryptography techniques are being widely used at upper layers of wireless networks, however, in future, the wireless networks will be decentralized and massive in scale which can thus increase the computational complexity for cryptographic techniques. Furthermore, there is a probability that attackers can decrypt the encrypted confidential information.

Other than the cryptographic techniques, there exists physical layer secure approaches as well which can be classified into five categories namely, theoretical secure capacity, channel approaches, power approaches, code approaches and signal design approaches.

Using theoretical secure capacity approach, a system can be designed to achieve definite degree of secrecy but not the absolute one. Furthermore, this technique requires the knowledge of communication channel which might not be precisely available for all practical communication channels . The channel approaches for attaining security is capture and extract

electromagnetic wave features of the received signal with the help of multiple sensors or through transmitted code vectors. One popular method in channel approaches in randomization of multiple input multiple output (MIMO) transmission coefficients thus making the matrix undetectable to the intruder . The third physical layer approach for data protection is the power approach in which directional antennas are used . Other than that, artificial noise schemes can be introduced which makes intruder channel nosier than the intended receiver . The code approaches are primarily used for anti-jamming and to avoid eavesdropping by employing spread spectrum or error correction codes.

They proposed technique can be classified as a hybrid approach of theoretical secure capacity and power approach. In order to bring robustness to our system so that the probability of interception, probability of detection and probability of exploitation, the proposed technique consists of two transmitters and a receivers. These transmitters consists of stepper motor along with its driving circuit and LED along with its driving circuit. The receiver consists of not only the photodiode but also an Infrared (IR) LED array which is responsible for transmitting the feedback signal from the photodiode to the LED transmitters. Thus the proposed scheme is establishing a full duplex channel for secure communication. The proposed technique for secure communication consists of the following steps :

a. Beam Scanning and Position Locking
b. Data Splitting and Transmission
c. Data Reception and Noise Filtration
d. Data Recombination

They results show that a secure communication link can be achieved using the proposed approach with reduced probability of interception. Our secure communication approach can be classified as a hybrid approach of theoretical secure capacity and power approach as it employs space-time diversity as well as directionality. [9]

2.4. Secure data transfer using visible light communication Technique

Sumit Jaykant Meshram, Raisoni, and Prof. Avinash P. Wadhe2 authors of Secure data transfer using visible light communication Technique notice The incandescent bulb that has been widely used to lit our surroundings since its invention over a century ago but now we are using this LED everywhere, why? Because they consumed low power and low cost and very efficient to use.

Sumit Jaykant Meshram and his colleges believing in when we see the LEDs is glowing up that time it switching on and of very quickly, which is not recognize human eyes. This feature gives us nice opportunities for transmitting data. 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 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.

Visible light is not injurious to vision. In the first system we are using the white LEDs because it is the combination of all seven colors, menaces we got all seven channel. But after that we have to do control all the light colors. That whys here we used the blue color LED. Menace people used only one channel over here. The switching rate is fast enough to be imperceptible by a human eye. This functionality can be used for communication where the data is encoded in the emitting light in various ways. A photo detector or the matrix of photodiodes can received the modulation request signal and decode the data, Due to its high frequency, visible light cannot penetrate through most objects and walls.

In this Visible light communication system you see how to securely data is transmitted source to destination using visible light communication.

The LED-to-LED communication provides a unique opportunity to provide communication capabilities that is not noticed. From the simulation we can see that it is possible to transmit higher quality of data using visible light as a medium.

In this system we are transferring data vie one computer to another in a room using VLC system. The range of that transmitter spectrum to receiver is 2.5μm (760nm).

On the basis of transmission of data in high speed, not penetrating outside of wall, low cost of LED, no need to take permeation for used, etc. this lot of features of this technology can be used to replace the existing RF based Wi-Fi system to connect to the internet. [10]

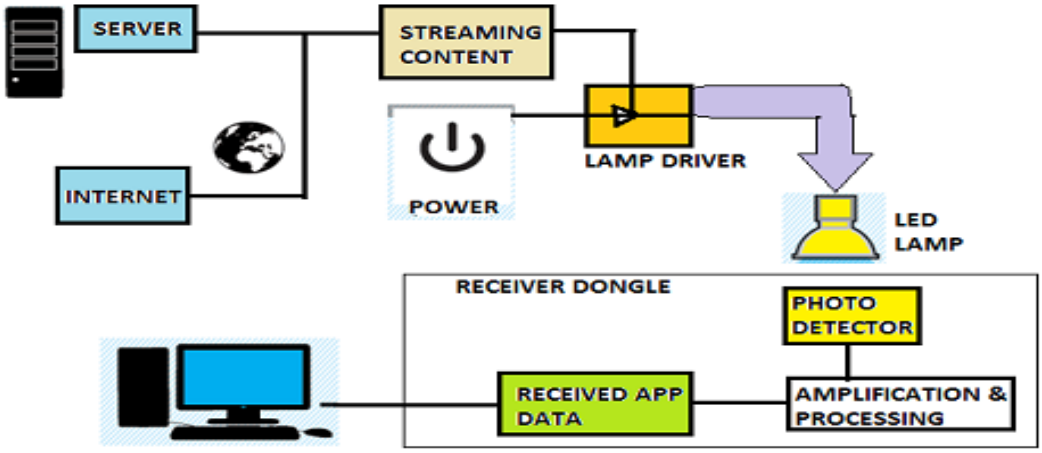

Figure 3. 2 Working of Li-Fi reproduced from

2.5. Shu using NSF grant to advance visible light communication security

And Shu using NSF grant to advance visible light communication security"Tao Shu, assistant professor of computer science and software engineering, has received a $120,000 grant from the National Science Foundation for his work in visible light communication, or VLC, security.

The NSF EArly-concept Grants for Exploratory Research, or EAGER, project will investigate the capability of visible light Multiple Input-Multiple Output, or MIMO, in combatting VLC-specific attacks. Shu and his team are researching the security vulnerabilities of VLC and exploring countermeasures to combat these vulnerabilities.

Due to its many features such as license-free spectrum, abundant bandwidth and Gigabits per second-level transmission rate, visible light communication has been considered to be a promising small-cell solution for alleviating the radio frequency spectrum scarcity problem in the 5G era," Shu said. "While research on VLC devices has made significant progress in recent years, the security aspect of VLC has not been well understood so far.

According to Shu, there initially was a common belief that VLC is intrinsically secure because the propagation of visible light is directive and can be confined within a closed space. However, recent studies have revealed that VLC is vulnerable to eavesdroppers outside of the direct beam of the light, or even outside the closed space, without direct line-of-sight to the light source.

The special optical nature of visible light propagation subjects VLC to other unique types of attacks, such as line-of-sight blocking and spoofing," Shu said. "These attacks will constitute serious threats to VLC systems when they are deployed in large scale in the near future.

Shu is proposing a jamming technique using MIMO technology to counter eavesdropping. [11]

2.6. Conclusion

This chapter offers an overview of the related work aspects to Secure devices pairing by using visible light we will describes in the next chapter how to implement the application with led and sensor light of devices mobile.

CHAPTER 3:

PROPOSITION AND IMPLEMENTATION

3. Proposition and Implementation

3.1.introduction

In this chapter, some knowledge to be used in this project will be introduced, which includes Password Based Encryption, Application Development Tool, proposition, Out-of Band Channels and implementation.

3.2.Password Based Encryption

Some users want to encrypt and decrypt their files with an easy to remember password (key) and at the same time be confident that their files are secure from prowling eyes. Public key

encryption requires the secure storage of the private key. The loss or compromise of the private key can be disastrous to the user. Password based encryption (PBE) was designed to solve problems of the kind described above.

A PBE algorithm generates a secret key based on a password, which will be provided by the end user. Currently there are two standards (PKCS #5 and #12) that define how a password can be used to generate a symmetric key. A good PBE algorithm will also mix in a random number called the salt along with the password to create the key. Without a salt, the hacker can perform a brute force search for the **key-space** with relative ease.

PBE is typically used in systems such as local file encryption tools, which are used to ensure data confidentiality. They are also used as a mechanism to protect the user's private key store (such as the PKCS #8 based protection of private keys). User prompted passwords are typically either a subset of ASCII or UTF-8 for purposes on inter-operability. It should be noted that UTF-8 is a superset of ASCII. [12]

3.2.1. Salt

The salt is a value that can thwart dictionary attacks or pre-computation attacks. An attacker can easily pre-compute the digests of thousands of possible passwords and create a "**dictionary**" of likely keys. Recall the fact that when you perform the digest, changing input data even a little changes the resulting digest. By digesting the password with a salt, the attacker's dictionary is rendered useless. The attacker will need to search through passwords for each value of the salt. Alternatively, the attacker has to wait until a password operation is performed and the salt used in that particular operation is captured. Because the salt is random

in nature, it is highly unlikely that the same salt will be used for the next encryption process thus limiting the attacker further.

The salt needs to be generated using a pseudo random number generator (PRNG). It is also strongly recommended not to reuse the same salt value for multiple instances of encryption. Note that the salt is not a secret value. So, it can be transmitted along with the cipher-text to the receiver or via out-of-band transmission methods. Ideally the length of the salt should be same as the output of the hash function being used. [12]

3.2.2. Iterations

Another important deterrent that can be used to thwart the advances of the attacker is to include an iteration count. This will complicate the key derivation function by performing a number of iterations. The iteration count increases the cost of exhaustive password search attacks by a significant amount. A minimum of 1000 iterations is recommended for minimum-security requirements. Just like the salt, the iteration count does not have to be kept a secret and can be transmitted in the clear along with the cipher-text if necessary. Usually the salt, the iteration count value and are sent to the receiver as a part of the **algorithm identifier** value. [12]

3.2.3. length of the keys

In order to generate stronger keys, we need to use standards such as PKCS#5 v2.0 or PKCS#12. The length of the keys that can be generated by these two standards is essentially unlimited. These two standards also go much beyond simple key generation and key derivation functions for password-based encryption. They also have support for password based message authentication schemes. Incidentally PKCS#5 v2.0 supersedes the PKCS#5 v1.5 standard, but includes compatible techniques too. [12]

3.3.Application Development Tool

To develop this application we use Eclipse with ADT for the reason of the Android Development Tools (ADT) is a plugin for the Eclipse IDE that is designed to give you a powerful, integrated environment in which to build Android applications.ADT extends the capabilities of Eclipse to let you quickly set up new Android projects, create an application UI, add components based on the Android Framework API, debug your applications using the Android SDK tools, and even export signed (or unsigned) .apk files in order to distribute your application.

Developing in Eclipse with ADT is highly recommended and is the fastest way to get started. With the guided project setup it provides, as well as tools integration, custom XML editors, and debug output pane, ADT gives you an incredible boost in developing Android applications. [13]

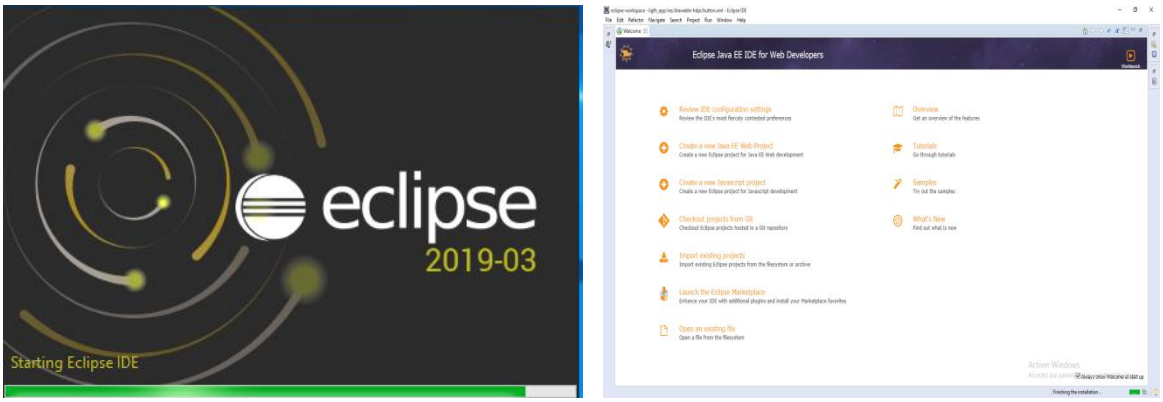

Figure 4. 1 eclipse interface.

3.4.Out-of Band Channels

Out-of-band channels are an important tool to establish security in general, and have been used in particular for authentication purpose. For example, receiving the same (or complementary) information through independent channels imply higher probabilities for message authentication. The potential ubiquity of VLC makes it an ideal candidate to complement a radio communication channel for security purposes, for instance to distribute public keys or a fingerprint thereof to check the authenticity of key material received over the primary communication channel. [18]

3.5.Proposition

Today, in an increasingly more connected world, wireless communication is beginning to play a greater role than the use of cable thanks to the advantages and conveniences it provides. but it had a negative impact on security posture, and if vulnerabilities exist they can be exploited by cybercriminals. Because of these security flaws, and the ease of exploiting them, wireless networks attacks are common.

Generally communication with wires is often too expensive, and creating networks by connecting devices wirelessly via radio wave links is becoming more difficult due to crowded

spectrums and signal interference, so visible light communication (VLC) technology was proposed as promising alternative for devices pairing

3.5.1. Comparison of Radio Frequency and Visible Light

Compared with the radio frequency communications, VLC has the following advantages :

- A visible light on the human body is relatively safe, thus causing no harm. VLC system is mainly used indoors with LED lights used to transmit data and with only a minor amount of radiation on the human body. [1]
- LEDs are used everywhere. Almost every place in life has lighting, so the lighting for communication can be installed anywhere and it can be more convenient for wireless data transmission [1].
- Transmit power can be high. Compared to the infrared communication, the infrared communication can cause greater damage to the human eye; it must suppress the transmission power to a low level and thus the system performance will be severely limited. For radio communications, the RF signal can cause relatively large damage to the human body, so it must also limit the power. VLC is the visible light transmission of information; therefore, the power can be relatively high. [1]
- Does not require certification of the radio spectrum. [1]
- No electromagnetic interference. This advantage allows visible light communication to be used in hospitals, aircraft, etc... [1]
- Figure 4. 2, below, shows that the wavelengths of visible light extend from 380 to 780 nm (nanometers; 1 nm =10-9 m). The color of visible light varies according to its wavelength: the longest visible wavelengths are seen as red light, and successively shorter wavelengths are seen as orange, yellow, yellow-green, green, blue and violet, in that order; i.e., the seven colors of the rainbow. Visible light wave communication (VLC) is point-to-point transmissions through the air and operates in the visible region of the spectrum generally unhampered by government restrictions. [14]
- As Figure 4. 3 indicates, non-visible EM radiation just outside that visible range is called infrared (IR) light for wavelengths too long to see (above 740nm), and ultraviolet (UV) light for wavelengths too short to see (below 380nm). Infrared

light is widely used in familiar devices such as TV remote controls because IR semiconductor lasers and light-emitting diodes (LEDs) are inexpensive and easy to work with. Ultraviolet light is not in general use, though, due to concerns that UV radiation might cause adverse health effects [14].

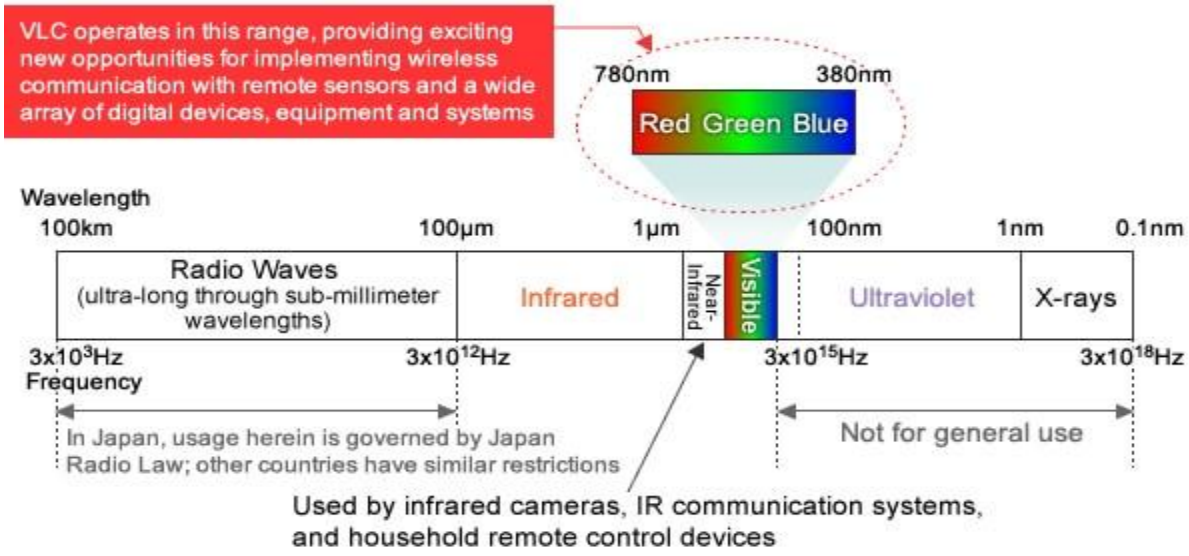

Figure 4. 2 The electromagnetic spectrum. The light our eyes can see goes from red to blue in the 780 to 380nm range of wavelengths. Infrared (IR) light has many uses today, and visible light communication (VLC) applications are now beginning to appear. VLC technology holds great promise for communicating information wirelessly over short distances using small, inexpensive transmitters and receivers built into next-generation lighting, display and computing products. [14]

3.5.2. Why secure by using visible light

a. VLC has been recently proposed as an alternative standard to radio-based wireless networks. because of its physical characteristics, and in line with the slogan" what we see is what you send", VLC is considered a secure communication. [15]

b. the object will transmit the information only when it knows that the smartphone is in its proximity**.**

c. Since light can't travel through solid objects, information transmitted via VLC can only be accessed if the receiver is in the same room. This has some very obvious security benefits. [16]

d. RF waves interfere with electronic devices and can infiltrate walls visible light cannot infiltrate walls and objects which permits to generate small cells of LED transmitters

with no inter-cell interference issues over the walls and parcels and feeds an inherent security for wireless data communications and can also increase the capacity of the available wireless channel. [16]

3.6.Implementation

3.5.1. Methodology

We have implemented our preliminary key management using visible Light communication application using Eclipse for Android Developers (Eclipse Jee 2019-03) on windows. In the current implementation, our decoding algorithm is given as input password to derive an encryption key from it. Passwords are easy for humans to remember whereas keys are needed in encryption schemes .so we use Password-Based Key Derivation Function 2 (PBKDF2) to deriving key that transmitted by flash light of smartphone. Light sensors sometimes use a component called a photodiode to measure illuminance. When beams of light strike a photodiode, they have a tendency to knock electrons loose, causing an electric current to flow. Photodiode of second smartphone use to receive key.

3.6.1.1. sending side

Data transfer using build in flashlight of a mobile device and we use Manchester modulation to encode the data being transmitted (see Figure 4). The sender turns the light-source (flash light) on and off repeatedly. The data is encoded in the time interval between each successive “on” or “off” event: a long pulse (80 ms) represents a ’1’ and a short pulse (40ms) represents a ’0’. Since the channel is unidirectional, the transmitter cannot know when the receiver starts reception. Therefore, the transmitter should start receiving in the same time until either the user approves the key agreement, or a timeout occurs.

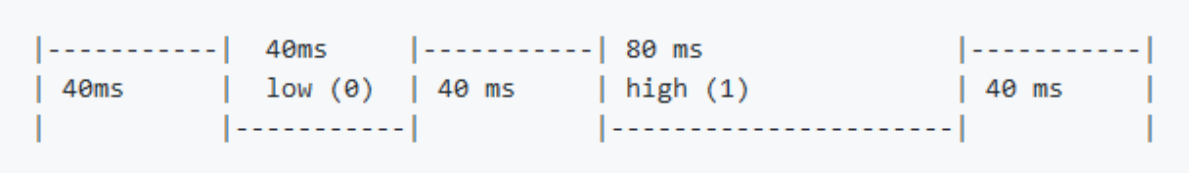

Figure 4.3 Data transmission via a single light-source

3.6.1.2. Receiving side

The receiver processing is analogous: we use senser light of mobile device to receive light alternating between positive and negative a transition in lighting is registered.The time between two consecutive changes indicates the transfer of either a ’1’ or a ’0

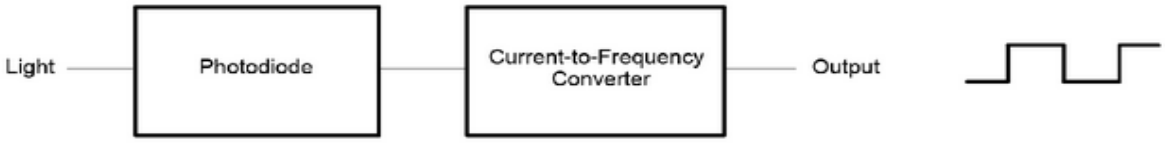

Figure 4.3 Light-to-Frequency

3.6.2. Results

3.6.2.1. Demonstration for devices pairing using VLC application

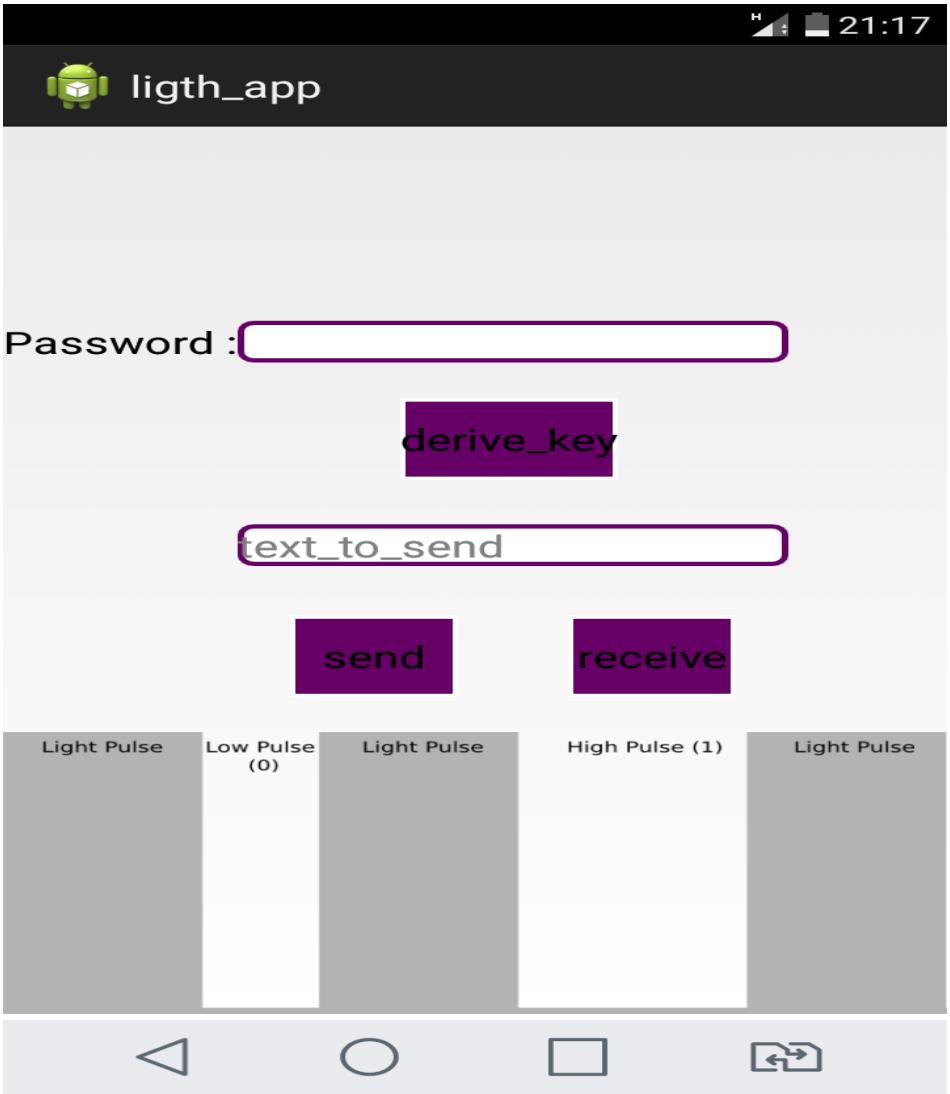

Figure 4. 4 Main user interface

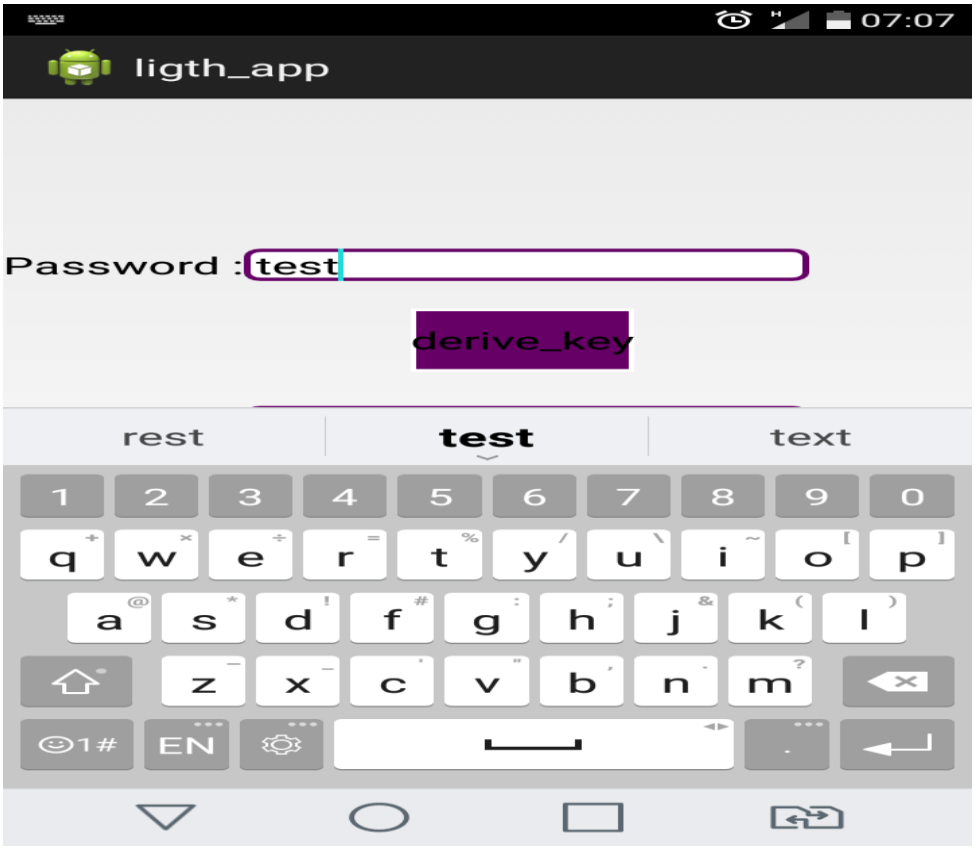

Figure 4. 5 password to create the key

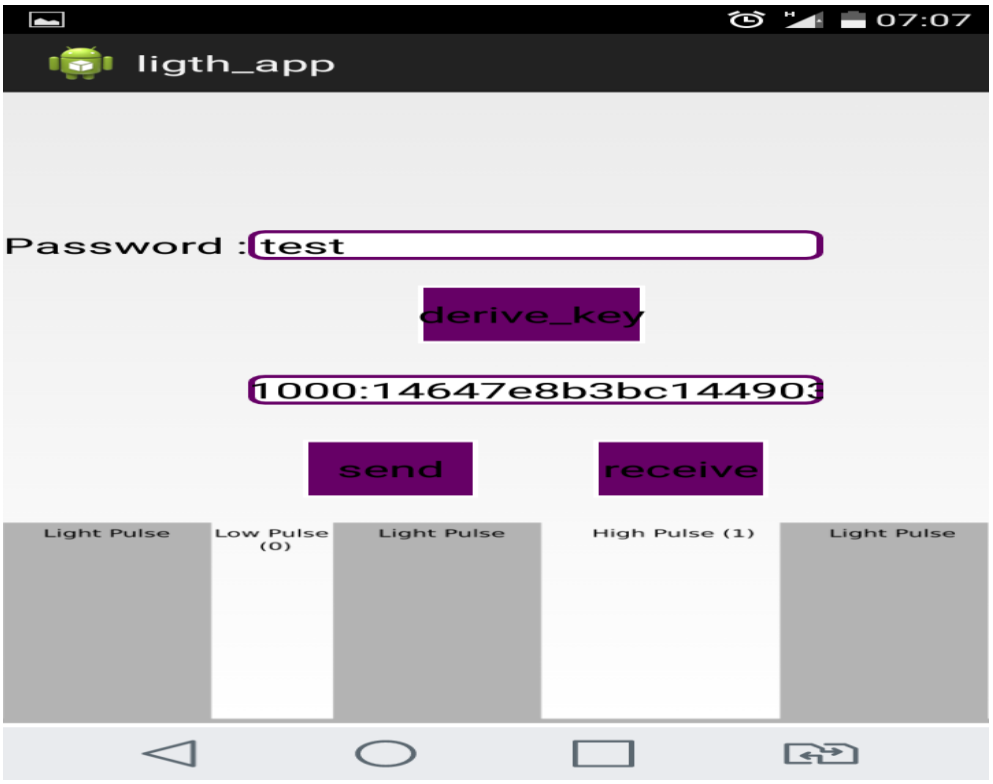

Figure 4. 6 derive symmetric key with PBKDF2

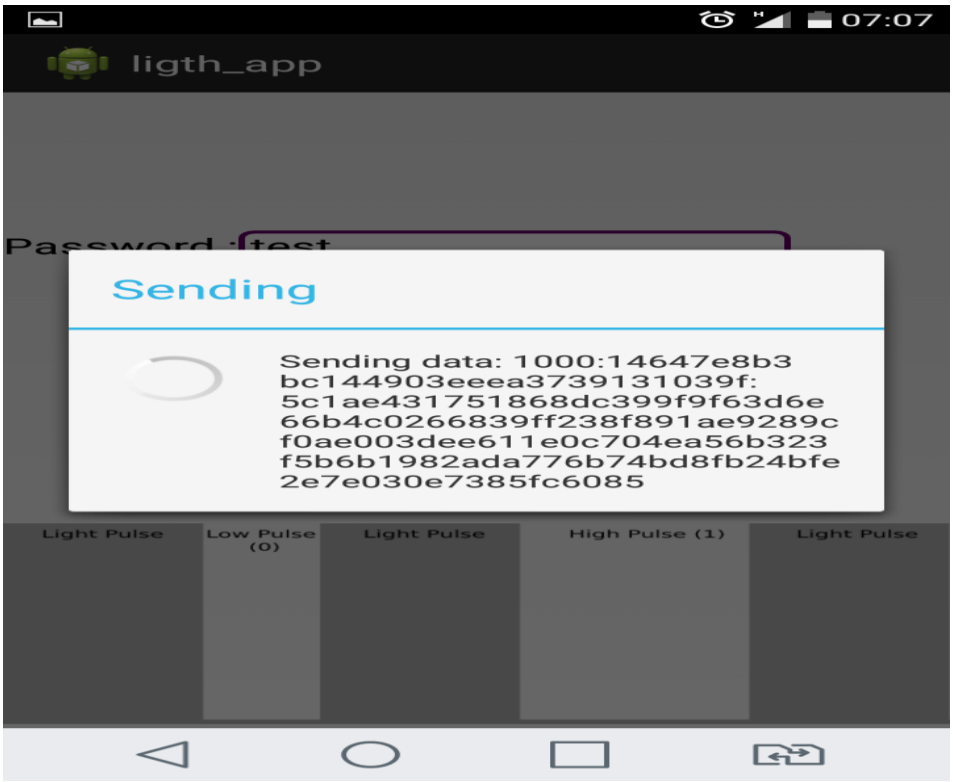

Figure 4. 7 sending key

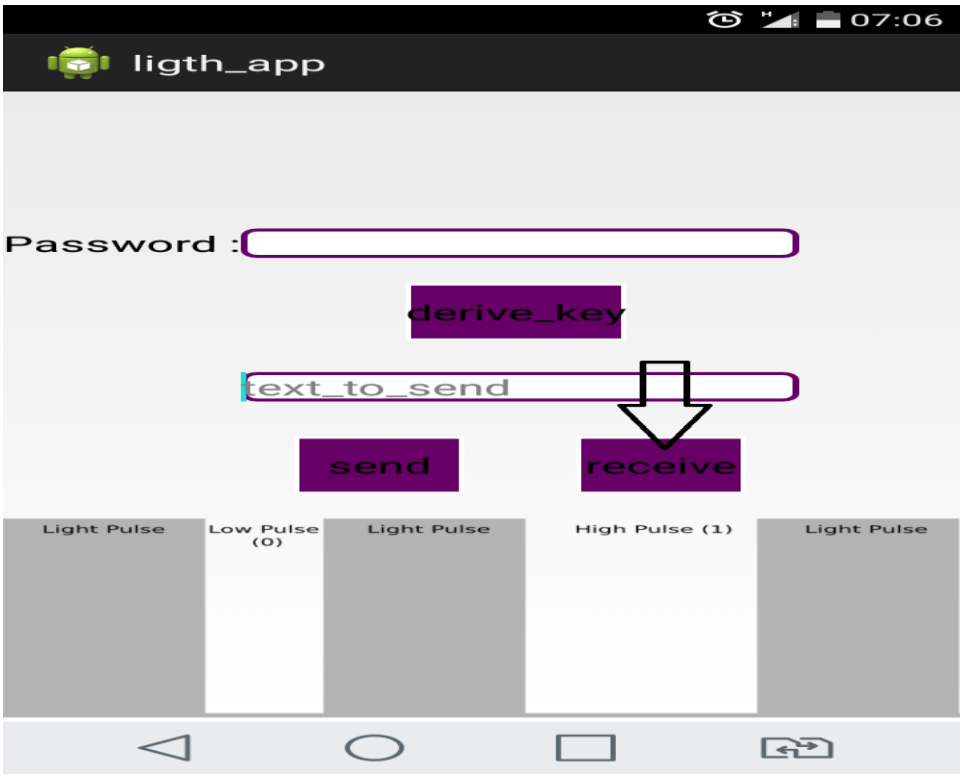

Figure 4. 8 presses the « receive » to Received the secret key

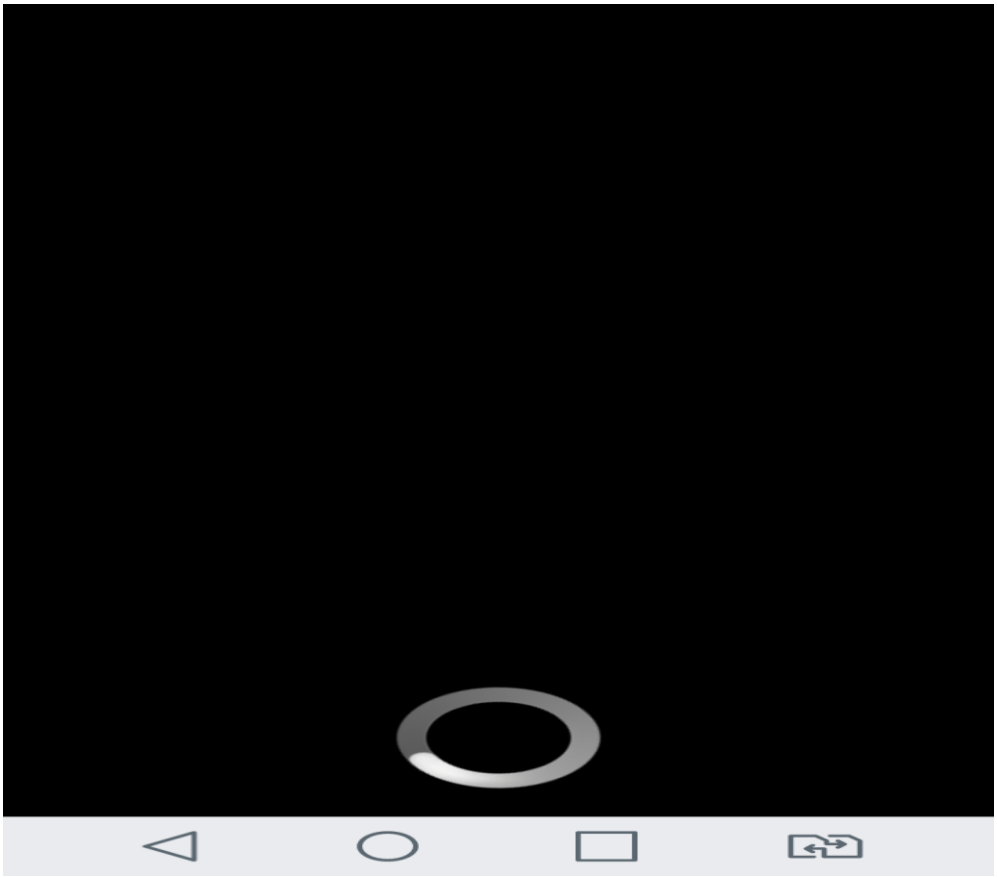

Figure 4. 10 click RECEIVE button, and wait for received the secret key

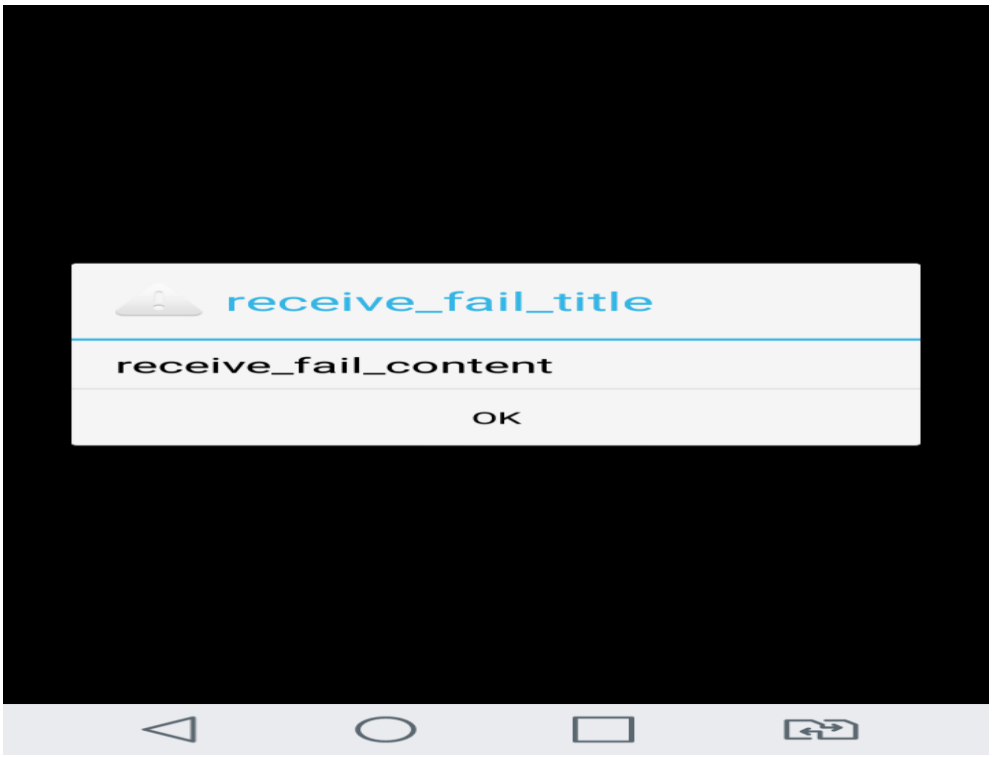

Figure 4. 10 the connection must done built in 5 seconds if not will failed

Conclusion and future work

The purpose of this work was to understand how and if it is possible to use visible light communication to ensure seurity in devices pairing .

First We generate a secret key based on a password which are used to ensure data confidentiality and we also mix in a random number called the salt along with the password to create the key that value can thwart dictionary attacks or pre-computation attacks.

Then we based in VLC to share this key between two mobile phone, as we know every smartphone have a flash light so we use it to built and send key with light . in the oposed side we try to receive this key that’s make a new challenge because of problem of the transmisson speed between both sides, the variance of light sensors and systems, these devices need photons of higher energies(thus higher frequencies) for their operations, and this directly implies that they can detect only a particular frequencies of light and even at this rates, android produces non consistent timing, thus creating errors in the dara stream.

we proposed an approach to detect key by using the sensor light of a mobile device but this solution stay just theoretical solution.

Finally we arrive to fully implement the sender side and as a future work, we try to implement the reception side.

[1] Guo, S. (2014-03-19). *Device Pairing Using Visible Light Communications.*

[2] ARNON, S. (First published 2015). *Visible light communication.*

[3] Aatifah Noureen, U. S. (2017). *Secure Device Pairing Methods: An Overview.*

[4] *Bluetooth Technology, Working and Its Applications.* Retrieved from EDGEFX.US: https://www.efxkits.us/different-types-bluetooth-technology-working-applications/

[5] Hill, S. (n.d.). *What is NFC? Here's everything you need to know* . Retrieved from digita ltrends: https://www.digitaltrends.com/mobile/what-is-nfc/

[6] Agarwal, T. (n.d.). *ZigBee Wireless Technology Architecture and Applications.* Retrieved from elprocus: https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/

[7] © 2019 Wi-Fi Alliance. (2015). *Wi-Fi Direct* . Retrieved from The worldwide network of companies: https://www.wi-fi.org/discover-wi-fi/wi-fi-direct

[8] Afrah Mariyam Iqbal, A. G. (2016). *Secure Mobile Payment using.*

[9] Muhammad Saadi, A. N. (2017). *Beam Scanning based Secure Communication using Visible Light.*

[10] Sumit Jaykant Meshram, A. P. (2016). *Secure data transfer using visible light* .

[11] Shu, T. (2017). *Shu using NSF grant to advance visible light communication security.* Retrieved from auburn.

[12] Atreya, M. (2006). *Password Based Encryption.*

[13] Android Developer Tools. *ADT Plugin.*

[14] Renesas. (2017). Visible Light Communication Technology Opens Up Intriguing New Ways to Network 'Smart Society' Applications. Retrieved from renesas: https://www.renesas.com/jp/en/about/edge-magazine/solution/10-visible-light-communication.html

[15] GrzegorzBlinowski. (2015). *Security issues in visible light communication systems.*

[16] Technavio. (2016). Three Reasons to Get Excited About Visible Light Communication. Retrieved from technavio.

[17] Pranav Kumar Jha, N. M. (2017). *Challenges and potentials for visible light communications: State of the art.*

[18] Christian ROHNER, D. P. (2015). *Security in Visible Light Communication: .*

Summary :

Recently several researchers and practitioners have begun to address the problem of secure device pairing or how to set up secure communication between two devices without the assistance of a trusted third party.

Nowadays, there are many interesting applications which communicate via the short-rang wireless communication channel (such as Bluetooth or WiFi). In the communication, a great deal of sensitive information is required to be transmitted. Therefore, device authentication is significant. In order to build a secure authentication mechanism. In this thesis, visible light communication is proposed as an alternative solution to radio-based wireless networks to ensure a secure communication.

Résumé :

Récemment, plusieurs chercheurs et praticiens ont commencé à s'attaquer au problème du couplage d'appareils sécurisés ou à la mise en place d'une communication sécurisée entre deux appareils sans l'aide d'un tiers de confiance.

De nos jours, de nombreuses applications intéressantes communiquent via le canal de communication sans fil à courte portée (tel que Bluetooth ou WiFi). Dans la communication, une grande quantité d'informations sensibles doit être transmise. Par conséquent, l'authentification du périphérique est importante. Afin de construire un mécanisme d'authentification sécurisé. Dans cette thèse, la communication en lumière visible est proposée comme solution alternative aux réseaux sans fil radio pour assurer une communication sécurisée.

ملخص:

في الآونة الأخيرة، بدأ العديد من الباحثين والممارسين في معالجة مشكلة الاقتران الآمن للأجهزة أو كيفية إعداد اتصال آمن بين جهازين دون مساعدة جهة خارجية موثوق بها .

في الوقت الحاضر، هناك العديد من التطبيقات المثيرة للاهتمام التي تتصل عبر قناة الاتصال اللاسلكي قصيرة المدى) مثل بلوتوث أو واي فاي .(في الاتصالات، يلزم إرسال قدر كبير من المعلومات الحساسة .لذلك، مصادقة الجهاز كبيرة .من أجل بناء آلية مصادقة آمنة .في هذه الرسالة، يُقترح الاتصال بالضوء المرئي كحل بديل للشبكات اللاسلكية القائمة على الراديو لضمان اتصال آمن