International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Li-Fi Security Issues and its Measures

Jason John D'souza[1], **Seeza Franklin**[2]
[1]Student, [2]Professor
[1,2]Bharati Vidyapeeth Institute of Management & Information Technology,
Navi Mumbai, Maharashtra, India

ABSTRACT

As we see in today's world, all institutes as well as organizations are planning to shrink the size hardware and are even trying to make it portable, olden days we had local area network wires to transmit data over devices then came in Wi-Fi which didn't have wires but was able to transmit data over devices but its sources are usually wired an sometimes not portable to every place and then now industries are planning to implement li-fi which uses a simple light to transmit data over devices users will just have to carry a small light source which will transmit the data over devices but what about the security measures to be taken that needs to be considered. This paper analysis and defines measures for those security issues faced in Li-fi technology. [1]

Keywords: *LI-FI, network, data, security*

I. INTRODUCTION

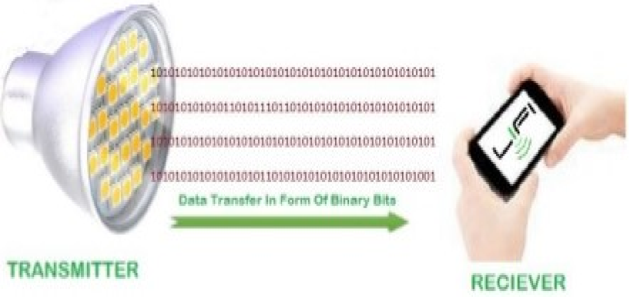
Wireless communication technology such as WI-FI is very widely used for wireless communication services and ubiquitous computing systems. These technologies have evolved drastically which is the main reason for our motivation. In Early days the internet was made available to the user using a wired Modem that used to modulate and de-modulate the signals coming from a wired transmission system, After that came up the wireless technology termed as Wi-Fi which uses Radio Frequency to transmit data wirelessly, This technology uses a device known as router which creates a hotspot area which means the router becomes a informal data access point for internet in the form of an invisible cloud. But Wi-Fi generally suffers interference from Bluetooth devices, microwave oven radiations, cordless telephones etc. In spite of several advantages and plus points Due to disadvantages like the limit in the radio frequency spectrum and the interference by various things A new technology based on data transmission using the light as a source and medium emerged. This technology is Li-fi. In this paper we are going to talk about this emerging technology called as light-fidelity (Li-fi) which is based of Visible Light Communication (VLC) with its enhanced features. In this paper we thoroughly go through the concepts, security issues, all possible future opportunities of Li-fi technology and measures for the security of this technology. [5]

II. OBSERVATION

1. The main objective of this paper is to aware about issues arriving in Li-Fi.
2. Prevention measures taken by user or consumers.
3. Prevention measures taken by developers and application developers.
4. Prevention measures taken by mobile hardware companies.

III. CONCEPTS

Li-fi is a technology that is based on wireless optical networking and it uses the LED's (Light Emitting Diodes) for transmitting data in the form of light. The Design of Li-fi has been developed particularly to use the low power led blub so that its design becomes very similar to trending energy - conscious homes and offices. But it works a bit differently. The LED used in this technology is fitted to a controller chip which is responsible to modulate the light and make it suitable for data transmission in optical format. The transmitting work is done by the led and on the other hand information is received and captured by photoreceptors. Light Fidelity is a system including VLC (visual light communication) that runs wire-free communications that to at a great speed. The speed can go up to 224GB (Gigabits) per second. This Fascinating idea to transfer data using simple led was first introduced by Harald Haas who was a professor at University Edinburg in 2011. It is a Bi-Directional technology and is Like Wi-Fi. It not only uses the visible light sources but this technology can also make use of the invisible but existing Ultraviolet and infrared radiations. Fig 1 shows the abstract view of how the data is first converted into bits and then transferred in the form of zeros and ones.



Li-Fi operating range is 380nm to 780 nm Li-Fi technology has the capacity to transfer data with the speed which is 10000 times that of the traditional radio spectrum; this is all achieved due to the use of visible light spectrum. Li-Fi is just another form of OWC (Optical Wireless Communication) that uses only light as a carrier medium in order to provide very high speed, networked and mobile communication which sounds very similar to Wi-Fi. This technology turns the led on to indicate signal 0(Zero) and turns the led on to indicate the signal 1 (One), Hence the information is totally converted into binary and transmitted to the receiver by switching the led on and off at such a high speed that human eyes cannot recognize it. As we know the led blubs should be kept on all the time to transmit data but we can suppress this by making the light so dim that they are below the human visibility range. [2]

IV. BENEFITS AND ADVANTAGES

Li-Fi will be used in sensitive electromagnetic areas like hospitals, airplanes cabins and also the nuclear plants that do not require any electromagnetic interference. Li-Fi will also be able to transmit the data using ultraviolet and infrared which makes it unique. Li-Fi is limitless when it comes to capacity whereas Wi-Fi has a limitation of capacity due to the spectrum crisis. Li-Fi has 10000 times higher data transfer rate then whole radio frequency band. The maximum speed achieved by Li-Fi is about 224 Gb\s. Also in terms of cost Li-Fi is 10 times cheaper than that of the existing Wi-Fi. As all of us use lights in our daily life, Li-Fi can make use of this light to transfer data, making it very efficient. Light bulbs are available everywhere so availability of light bulbs makes the availability of Li-Fi. One of the most beautiful advantages of Li-fi is that light cannot pass through walls and things which are opaque. So anyone outside the room cannot try to breach the security. This makes it very secure to limited areas which will be an internal network. Li-Fi devices require low power to operate and so they can be used in vast IOT applications but those IOT must also consider some security features. As Li-fi uses light it is not harmful like the radio frequency spectrum. So there is no issue regarding the health safety concerns in the systems based on Li-Fi. As less energy is consumed the amount of heating of devices has been greatly reduced. These technologies are very easy to install. Also the maintenance cost is very low as compared to the Wi-Fi technology. Innumerable number of streetlights can be converted to Li-Fi threatening hotspot, also it does not require any license. It also allows the multi user communication feature. This technology has a very long service life (10 years to 15 years). Data Density is very high in Li-Fi. [3][4]

V. PROBLEMS FACED IN LI-FI

As Wi-Fi security is essential to deny access to the unauthorized user which doesn't allow access to them. In the same way even Li-Fi requires security measures to be taken care of so that unauthorized users don't get access to the data that is being transformed. As we know that there are various types of securities in Wi-Fi like WEP, WPA2, etc. Even Li-Fi has to take care of many issues that can occur during data transfer.

Below are some issues that can be faced during transfer of Li-Fi with measures to overcome those issues. [6][7]

➢ Point To Point Transfer

As we know Led bulbs used for transmission of data emits more amount of light and has a wider range compared to other bulbs, hence can be accessible to many users in that range even to those who doesn't require it Hence for such scenario Li-Fi process can use such led bulbs that has straight focus (not a wide angle range where the transmitter bulbs will be in point to point focus to the receiver. As the range is reduced, an only user who wants to receive it will be able to receive it and rest available device won’t be able to access it

- **Login Password credentials**

The most commonly used security measure of Wi-Fi i.e. Authentication, where an individual user gets username and password where only authorized users get to access the data. In the same way use such kind of security for Li-Fi too where a user gets a username and password to access data from Li-Fi device and rest who are not authorized doesn't get to access it.

- **Specific Light** (that differs from other Led Bulbs)

Li-Fi uses the standard led bulb to transfer its data to other devices where it keeps on changing the frequencies of the light according to signals that it wants to send to other devices (the frequencies keeps or varying by the source behind the bulb from where the data is being transmitted). The receiver device on the other end receives the light which it converts into signals. Here the problem that might occur for receiver is that suppose there are two led bulbs that are present, the receiver device might flicker with other bulb signals which will result to disrupted data that is being received.

Hence we should take care that there should be a proper distance between two Led bulbs the one that is transmitting and the other normal led bulb which isn't, by these the receiver will be able to receiver light from one specific led only and will not be deflected by other bulb.

- **Transfer Within Room**

Li-Fi cannot transmit within walls the way Wi-Fi does, this disadvantage of Li-Fi can also be used as an security measure where transmission will only be done inside a particular space and the devices which are not present inside the space will not be able to access it.

- **Encrypting and Decrypting Signals**

Encryption and decryption of the data and then transferring it over the light will be most feasible as other device will not be able to interpret the data that is being transferred. Only the device that has the key to encrypt and decrypt it will be able to interpret it.

VI. Conclusion

Li-fi security is not that easy to achieve, some people are still trying its implementation and applications into different field but are not considering security issues into it. As we know Li-fi security would be more difficult than Wireless network security. We all know that Li-fi is coming into existence hence no protocols have been declared which will keep on varying until its final application therefore we hope that these flaws to be considered while creating your Li-fi device and also its measures.

VII. REFERENCE

1. **Whatis**
   https://whatis.techtarget.com/definition/LiFi
2. **Techworld**
   https://www.techworld.com/data/what-is-li-fi-everything-you-need-know-3632764/
3. **Techopedia**
   https://www.techopedia.com/7/31772/technology-trends/what-are-the-advantages-and-disadvantages-of-li-fi-technology
4. **PureLifi**
   https://purelifi.com/faq/how-is-lifi-more-secure-than-other-wireless-technologies/
5. **Wikipedia**
   https://en.wikipedia.org/wiki/Li-Fi
6. **Cybermatters**
   https://cybermatters.info/2017/01/10/li-fi-security/
7. **Quora**
   https://www.quora.com/What-are-some-current-problems-with-Li-Fi-technology-that-need-to-be-overcome-in-order-for-the-tech-to-become-more-widespread