

ZIBELINE INTERNATIONAL
PUBLISHING

ISSN: 2616-5961 (Online)

CODEN: IMCSBZ

Information Management and Computer Science (IMCS)

DOI: <http://doi.org/10.26480/imcs.01.2020.10.13>

REVIEW ARTICLE

A REVIEW ON (Wi-Fi VS. Li-Fi) TECHNOLOGY

Moin Khan¹, Ahasham Sajid^{1*}, Aarsal Hanif¹, Muhammad Aqib¹, Afia Zafar²¹Department of Computer Science, Faculty of ICT, BUITEMS Quetta, Pakistan.²Department of Computer Science, NUTECH, University, Islamabad, Pakistan.*Corresponding Author Email: ahthasham.sajid@buitms.edu.pk, gullje2008@hotmail.com

This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article History:

Received 10 February 2020

Accepted 16 March 2020

Available online 27 March 2020

ABSTRACT

This paper is about the various limitations of the novel Li-Fi technology and perhaps those which have an adverse impact on its security and efficiency. Line of sight has been one of the major barriers for VLC based technology which causes eminent hindrance in the wider applicability of the technology. Li-Fi is a non-Line of Sight alternative which does not merely confine its limits or depreciates its efficiency; in fact, it makes it an ineffective option for the LoS based scenarios. This paper will discuss the hybrid approach to wireless solutions in an effort to address the said impediments. This paper also discusses the methods to minimize the lope holes which jeopardize the gains associated with the non Line of sight (NLoS) nature of the light propagation and explains ways to control eavesdropping.

KEYWORDS

Wi-Fi, Security, Electromagnetic spectrum, Line of Sight, Hybrid Model.

1. BACKGROUND

1.1 Mass Communication

Communication has been a primary element of every human civilization. It enjoys a vital and significant role in the survival and growth of a society. Since ages, people have used diverse means and mechanisms to convey information from one place to another. History has seen tremendous evolution in the techniques and tools of mass communication which rapidly accelerated human development and cultural advancement. Scientific developments in the early 1900s and onwards have not only been advantageous for making human lives more comfortable, but it has also spectacularly transformed prior approaches to mass communication. With advent of telephones and telegraphs, the amount of time for the message to travel was dramatically decreased. Then came mobile phones and televisions making the telecommunication even more efficient. Internet is the most modern source of communication in today's world. The worldwide web along the wonderful Smartphone technology is doing wonders in the field of communication with the world being stretched into a global village. Communication in today's digitalized environment is a matter of seconds from one part of the world to another at effective cost and security. One may wonder that the struggle of man in search of perfect communication is over, but that is just not the case. With every opportunity comes a risk, and it's the reason that today's communication demands are far more complex and greater than it used to be in the past. We need fast, efficient and secure channels to transfer data which governs the whole digital infrastructure in the modern society. Digital devices used to be joined through physical wires in order to connect them together. Wireless communication like WLAN, Bluetooth are a step forward in our journey for advancing communication methods which enabled two or more devices to communicate without any physical connection. OWC

(Optical Wireless Communication) is the latest technique of transmitting digital data through light pulses. In this paper, a novel approach for data communication through light (Li-Fi) will be discussed and we will also address some of the intrinsic disadvantages of the conventional wireless networks. At last, this paper will also mention a critical view at the various aspects of the OWC networks.

1.2 Wireless Networks

A wireless computer network uses radio communication to connect devices on the network. Wireless communication takes place on electromagnetic waves instead of using physical wires as a medium of data transmission. At the sender end, data being transmitted is modulated on the radio wave carriers such that it is extracted at the receiver's device. Radio waves allow a range of frequency variations to avoid interference and support more than a single data carriers in the same place. In order to receive the data, the receiver has to tune up to a given radio frequency in which the data has been modulated. Wireless communication networks has eliminated distances, by empowering people's capacity to interact more easily and expanded an enduring organizational network infrastructure. Portability of the system allows people to communicate and work while during their travel and daily routines (Anonymous, 2013).

1.3 Importance of Wireless Communication

The evolution of the wireless communication has triggered numerous fundamental shifts in the digital environment. Mass communication was never as easy as it is today, wireless communication has made internet accessibility easier for general population. People can access internet at coffee-shops, bus-stops and airports at anytime. Devices which operate with wireless technologies like Wi-Fi has experienced a sudden uptrend in the recent years. Demand for devices which operate on Wi-Fi and meet

Quick Response Code



Access this article online

Website:
www.theimcs.orgDOI:
[10.26480/imcs.01.2020.10.13](https://doi.org/10.26480/imcs.01.2020.10.13)

interoperability standards have dramatically expanded. Obvious convenience and portability factors involved in wireless communication has resulted in mass adoption of the technology. Organizations tend to move from ordinary wired communication infrastructure to an adaptable communication environment. Primary communication parameters like network coverage, portability and network security have improved due to organizational reliance on wireless networks. E-Banking, E-Marketing, Healthcare and education are some of those many areas evolved as a result of WLAN (Anonymous, 2013).

1.4 WLAN: The origin of Wi-Fi

Like a cell phone network, Wi-Fi is a wireless form of LAN which connects two or more devices without physically wired connection. Wi-Fi is an acronym for 'Wireless Fidelity'. It is the IEEE standard 802.11 which was initially approved in 1997. Managed and regulated by Wi-Fi Alliance, several extended versions of the Wi-Fi standard exist today with 802.11a, 802.11b, 802.11g and 802.11n being major of these revisions. 802.11a, 802.11b were the first among the bands which were promoted under the banner of Wi-Fi in 1999. Initial versions were limited in terms of bandwidth and other functionalities which were later replaced with latest 802.11g(2.4 GHz) and 802.11n(2.4 GHz or 5 GHz) releases stretching range and providing an increase in bandwidth of up to 250 Mbps.(Bensky et al., 2011).

Standard	Frequency	Data Rate ¹	Range	Type
802.11a	5 GHz	54 Mbps	120m	LAN
802.11b	2.4 GHz	11 Mbps	140m	LAN
802.11g	2.4 GHz	54 Mbps	140m	LAN
802.11n	2.4/5 GHz	248 Mbps ²	250m	LAN

Figure 1: 802.11 Versions

1.5 Pitfalls of Wi-Fi Networks:

Although Wi-Fi has offered much more to the digitalization of the society, there lie some critical disadvantages of the technology. Electromagnetic waves are utilized as the primary carrier of the communication which are highly vulnerable to interruptions and electromagnetic interference. Wi-Fi is not a communication solution in places where it poses threat to (more) important communication channels such as aircraft carrier signals (Soni et al., 2016).

Security is one of the looming concerns in the Wi-Fi networks. Networks operating on Wi-Fi are prone to various security attacks due to its open nature of radio propagation (Khandal et al., 2014). Moreover, it count on a more limited range of radio frequencies in the electromagnetic spectrum. Limited options of the medium, higher cost of carrier along with availability issues are some of the major drawbacks of the Wi-Fi communication networks (Soni et al., 2016).

2. INTRODUCTION

2.1 The birth of Light-Fidelity

After the widespread adoption of wireless communication networks, it has been greatly felt that Wi-Fi network cannot support the ever growing demands of higher data rates to the consumers. The origin of Li-Fi became public when Dr. Haas disclosed his research project along with his team in a ted talk to the audience where he played HD video from a gleaming LED (Light emitting diode). It was a phenomenal technology as it allowed data signals to be communicated through light beams originated from an illuminating source. Such type of data communication is defined under IEEE 802.15.7 standard known as Li-Fi. When an LED is glowing or ON, it means it communicates data or transmits 1. Off Light means no data transmission is taking place or that 0 is communicated. Transmission takes place when the source flickers at the frequency higher than human eyes can trace (Khandal et al., 2014).

2.2 Working of the Li-Fi

Li-Fi utilizes the optical portion of the electro spectrum for data communication. Major components of the Li-Fi based communication networks are the following:

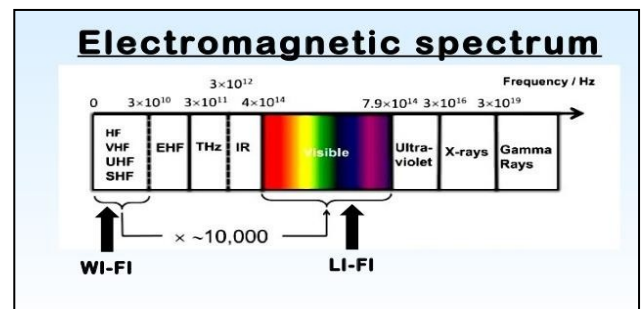


Figure 2: Electromagnetic Spectrum

- The Transmitter: Transmitter acts as a source of the light carriers. It can be a LED or an array of multiple LEDs. Binary data arrives in form of bytes which is transmitted in the form of On-Off patterns. Data conversion takes place at the transmitter where the data is encoded in light sequence for transmission.
- The Receiver: It has a photodiode receiver used to receive the optical signals sent from the receiver. Optical signals are decoded in the receiver and the encoded information is degenerated (Sarkar et al., 2015).

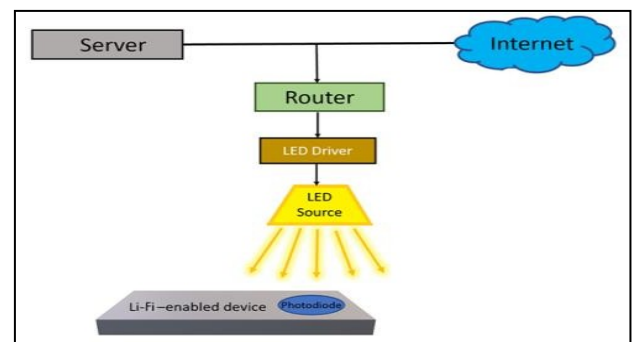


Figure 3: Components of Li-Fi Network

At the transmitter, a flickering bulb is used which makes light output by making optical variations depending upon the data. Glowing light means 1 and turning the light off transmits 0. The data pattern is thus mapped out of the continuous variations in the light status. Generally, LEDs used for the Li-Fi are also utilized for the illumination purposes. Data communication is possible through single LED point as well as through multiple sources. Multichromatic LEDs are also used for the purpose which combines the effect of Red, Green and Blue colors to transfer the data. Li-Fi combines the illumination with wireless communication while enabling every light as potential data transmitter (Khandal et al., 2014; Chatterjee et al., 2015).

2.3 Advantages over Wi-Fi

- Broad Spectrum: The major plus of Li-Fi over Wi-Fi is that it is not dependent upon the congested electromagnetic spectrum of radio frequency. Li-Fi is 10000 times broader than Wi-Fi in terms of its electromagnetic spectrum. (Sarkar et al., 2015).
- Increased Security: Due to the nature of the light, it cannot propagate through hard and concrete obstacles. Wi-Fi is prone to vulnerabilities due to its open nature of propagation.
- Increase Bandwidth: Due to the broader range of the electromagnetic spectrum, Li-Fi has higher bandwidth than Wi-Fi.
- Cost Effective: Optical based Li-Fi is cheaper than the conventional radio frequency based Wi-Fi.
- Power Safety: Radio waves propagation and broadcast consumes substantial amount of energy as compared to the Li-Fi. OWC is more power saving and hence more efficient (Soni et al., 2016).
- Green Technology: Due to its eco-friendly nature, Li-Fi is considered more environment friendly over Wi-Fi (Al-Alawi et al., 2006).

2.4 Applications of Li-Fi:

- **Indoor Communication:** VLC is making us all free from the dependence on the unlicensed radio spectrum. It provides best alternative for indoor communication requirements with reliable security attributes and faster data rates.
- **Smart Lights:** By integrating communication with illumination we can better utilize the technology in a more fashionable manner. Street lights can serve as potential communication access points providing connectivity to the pedestrians.
- **Medical Facilities:** Wi-Fi are not an appropriate option for medical usages due to its limitations. Wi-Fi based monitoring devices can cease to work if they are affected by the interference and other radio interruptions. Moreover, Wi-Fi radio waves can have adverse impact over the patients and can lead to health issues. Since Li-Fi is based on light communication, which makes it safe inside the hospitals and patient rooms.
- **Aviation and Airliners:** Wi-Fi signals can create huge disturbances inside the airplane. Due to its disruptive nature it can damage the internal communication channels. Through the proper use of Li-Fi, passenger will be able to connect to the internet without jeopardizing the safety of the jet.
- **Industrial Usage:** Some industrialized environments demand a safe connectivity without the electromagnetic interference. Li-Fi provides safe and secure communication as Wi-Fi is not a suitable option for such hazardous conditions.
- **Underwater Applications:** VLC based Li-Fi technology is a useful instrument for the marine operations and can help facilitate underwater exploration. Cable communication infrastructure used for ROVs can be substituted to allow freedom of movement and functionality. These features are never afforded by conventional radio waves which are bound to disruption. Optical wireless communication is the best solution for the underwater communication demands.
- **Educational Institutions:** Higher speed of the Li-Fi gives it a clear edge over the Wi-Fi. Demands for higher data transfer rate for educational purposes can lead widespread adoption of VLC in educational sphere.
- **Traffic Management:** Using LED based communication can lead to well informed driving and smart traffic management. Inter-vehicular communication through emplaced LEDs can dramatically reduce the traffic accidents (Khandal et al., 2014; Soni et al., 2016; Khan, 2017).

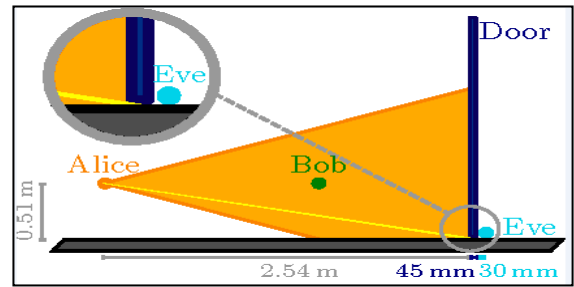


Figure 4: Eavesdropping Attack (Classen, 2015)

4. CRITICAL ANALYSIS

4.1. Hybridization

While as it is an obvious scenario that VLC is a non-Line of Sight technology, there still are avenues to utilize this limitation and still get what we achieved from the VLC. A model based on the hybrid approach containing channels of conventional RF and VLC can be a better option to consider. As far as indoor communication is concerned, Light communication is faster and efficient, but the dilemma to how users on such a network be made safe from being vulnerable to its NLoS design can be resolved by integrating both of these technologies. Since RF allows LoS propagation, it would not be a bad option to switch transmission from VLC to Radio channel in order to provide LoS communication. Doing so, we will be able to utilize the higher bandwidth capacity provided by the VLC for NLoS and eliminate the NLoS aspect of the hybrid network through using Radio channels (Saeed et al., 2019).

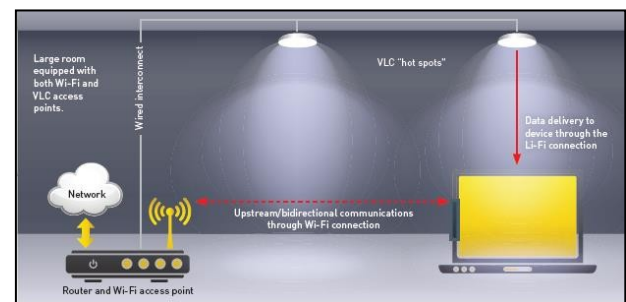


Figure 5: Hybrid Li-Fi/Wi-Fi Model

3. RELATED WORK

The most fundamental challenge faced by the Li-Fi is that it lacks Line of Sight feature. Light carriers are obstructed by the physical objects that come into its way. It could be a compound, building, vehicle, tree or even a human body. The intensity of the light dictates the data rate, which means the weakened and reflected beam of light could still be able to transmit data but at the lower pace due to intensity devaluation. Unavailability of the communication channel when the user enters into NLoS scenario poses a potential setback for the flexibility of the VLC.

Indoor VLC based networks are generally perceived to be comparative secure than its legacy radio based networks. It's because of the fact that light cannot pass through solid obstacles. But that does not make the model secure from the vulnerabilities that do exist in it. There are still potential weak spots which can be exploited by malicious attackers and eavesdroppers. Light reflections taking place out of floor surface, door gaps, door steps, window panels, keyholes, exhaust fans still provide sufficient bandwidth to the outsiders to get into the network.

The author in has described in detail the various means to prevent any outgoing light reflection from the premises (Classen, 2015). Floor material used affects the amount of light reflection going out of the premises and can help to avoid the eavesdropping if the material used is non-reflective. The color coating on the window panes does not necessarily stop the light going out of the room, even if it is hardly visible to look through it. All of these potential weaknesses still pose a major threat network security and user confidentiality (Classen, 2015).

4.2. Transmission Wall:

The actual NLoS feature of the VLC can perhaps prove favorable sometimes. It makes the technology comparatively secure than the RF communication by disallowing open propagation. Securing this factor as an advantage albeit takes into account some precautionary measures. Li-Fi communication can be vulnerable to eavesdropping as described by (Classen, 2015). However the issue can be drastically tackled by enabling the Light Sources to recognize the accessible premise of the compartment. If the system is allowed to initiate communication after recognizing and defining the valid or accessible region, it can considerably devalue the attacker's chances to eavesdrop. The system will only allow data transmission to the users who fall within that specified range and deny any accessibility to those found out of the transmission wall.

5. CONCLUSION

Although digital revolution brought comforts to our lives in countless ways, yet the race to secure our environment has never ceased to exist. In today's intertwined digital society, it puts us to an even greater risk of exposure to a variety of attacks than ever before. This article indicates some of the major dysfunctional aspects of the novel Light based communication systems and provide solutions to make the system secure from its potential vulnerabilities.

Li-Fi is a step forward in our journey to make communications faster and more efficient but, it all comes at a price. In light based Li-Fi, the security of the communication channel is subjected to a range of factors which, if not tackled appropriately, could lead to the network inefficiency, lack of

network security and major damages to human health. NLoS, a dominant feature of the novel communication technique, in particular, brings the Li-Fi technology under the scrutiny of the reliability and security. Overcoming these challenges is the key to better utilize a more efficient light based communication system.

6. FUTURE WORK

Comprehensive struggle is needed to provide a hybrid framework in order to integrate valuable features of both Light and radio waves based approaches. As far as the Light carriers can transmit the data, communication channel remains the Li-Fi. Once communication with user is obstructed due to NLoS, the primary channel of communication would switch to Wi-Fi. The next step will be to design a mechanism which makes possible the interaction between the Radio Network and Light Network in a hybrid approach. Resource allocation between those two domains will remain the major question to develop such a hybrid model. It is also important to figure out that how much is it efficient and workable to deploy a range based solution in LEDs to avoid eavesdropping and external threats. Adjustable LEDs which can alter the range of carrier light beams according to user input provided in order to provide flexibility and security for the indoor solutions.

REFERENCES

Al-Alawi, A. 2006. Wi-Fi Technology: Future Market Challenges and Opportunities. *Journal of Computer Science*.

Bensky, D., Bradley, T., Hurley, C., Rackley, S., Rittinghouse, P., Ransome, P., Stapko, T., Stefanek, G., Thornton, F. and Lanthem, C. 2011. *Wireless*

Security. Newnes.

Chatterjee, S., Agarwal, S. and Nath, A. 2015. Scope and Challenges in Light Fidelity (Li-Fi) Technology in Wireless Data Communication. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*.

Classen, J., Chen, J., Steinmetzer, D., Hollick, M. and Knightly, E. 2015. *The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications*. ACM.

Khan, L. 2017. Visible light communication: applications, architecture, standardization and research challenges. Department of Electrical Engineering, University of Engineering & Technology, Peshawar, Pakistan.

Khandaal, D. and Jain, S. 2014. Li-Fi (Light Fidelity): The Future Technology in Wireless Communication. *International Journal of Information & Computation Technology*, 4.

Saeed, R., Shakir Ullah, Peter Han C, Sira Y and Dan. 2019. *Visible Light Communication: A System Perspective –Overview and Challenges*.

Sarkar, A., Agarwa, S. and Nath, A. 2015. *Li-Fi Technology: Data Transmission through Visible Light*. ResearchGate.

Soni, N., Mohta, M. and Choudhury, T. 2016. The Looming Visible Light Communication Li-Fi: an edge over Wi-Fi. *IEEE*.

Wireless Networks. 2013. New Delhi: Excel Books Private Limited.

