Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 201 (2022) 684–689

Procedia Computer Science

www.elsevier.com/locate/procedia

The 12th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2022)
March 22 - 25, 2022, Porto, Portugal

Securing the light escaping in a Li-Fi network environment

D.D. Diambeki[a], R.E. Mandiya[a,b], K. Kyamakya[c], S.K. Kasereka[a,b,*]

[a]*University of Kinshasa, Mathematics and Computer Science Department, Kinshasa, DR Congo*
[b]*Artificial intelligence, Big data and modeLing simulation research center (ABIL), Kinshasa, Democratic Republic of the Congo*
[c]*Alpen-Adria-Universitaet Klagenfurt, Institute of Smart Systems Technologies, Department of Mathematical Sciences, Klagenfurt, Austria*

Abstract

Nowadays, everyone knows Wi-Fi. The technology that ensures connection of computer equipment. It is now positioned as the easiest way to interconnect multiple end users because It allows user mobility in workspaces, avoids cable clutter within the network coverage, such as offices, homes and so on. Despite these advantages, several scientific studies have shown that this technology can raise security and safety issues and is dangerous to human health, and therefore not suitable for hospital networks. In an attempt to overcome these difficulties, Li-Fi technology based on visible light is beginning to interest researchers. This technology is considered more secure than Wi-Fi because the light can be contained in a physical space and waves can't pass through walls and other objects. Unfortunately, when the physical environment contains spaces that can escape light to the outdoors, this can be a security risk for Li-Fi because it uses light sources to transmit data. That why, in this paper, the main differences between Wi-Fi and Li-Fi technologies are explained, and a Li-Fi architecture provided with an authentification captive portal and a data transfer security mechanism between end users based on the AES algorithm is proposed. The developed prototype and the architecture proposed guarantee the security of the Li-Fi network even if the physical environment is provided with multiple light escape spaces.

Keywords: Li-Fi (Light-Fidelity), VLC (Visible Light Communication), LED (Light Emitting Diode), Photodetector, LDR (Light Dependent Resistor), Arduino, AES algorithm, Captive portal.

1. Introduction

A wired network uses Ethernet cables to connect different equipment in the network, it is characterized by its reliability, speed and security. However, this connection mode is also known for its lack of flexibility, especially in terms of moving around in workspaces, it does not allow users to be mobile during activities. Nowadays, the way of working is changing, users are more and more mobile. As a result, they now need to be able to access their usual work

* Corresponding author. Tel.: +243 82 18 28 964
E-mail address: selain.kasereka@unikin.ac.cd

1877-0509
10.1016/j.procs.2022.03.091

tools and company data anytime, anywhere. Hence, the appears to be the preferred technology for companies wireless connections (Wi-Fi), because this technology avoids cable clutter, allows users to move freely within the available radius without having to plug / unplug anything. Indeed, the Wi-Fi network is harmful to human health, hence its use in high-risk environments such as: hospitals, airplanes, nuclear industries, etc. needs to be reviewed. Wi-Fi equipment works with high frequency electromagnetic waves, the transmission frequency of which is approximately 2400 MHz. We know that it is this frequency that allows the water molecules agitation [11]. According to a study, the percentage of water in the constitution of the human body is around 60% in adults and 70% in infants [3], we can then ask ourselves the question about the impact of such waves in the human organism. Indeed, several studies in the literature point out that Wi-Fi is carcinogenic in the long term, that it could be a factor in sterility, hormonal system deregulation and that it could also be responsible for immune system disorders [2, 4, 10, 12, 8]. However, on Internet, the majority of information is exchanged over Wi-Fi technology. But due to its complexity and lack of security, this technology has certain limitations. Apart from the health problems posed by Wi-Fi, several authors have shown that this technology poses security problems and can be easily hacked because it can cover large areas.

In an attempt to overcome these difficulties, Li-Fi technology based on visible light is beginning to interest researchers. This technology is a wireless communication that uses light. Li-Fi is not harmful to human health, moreover from ancient times to the present day, no study has proven the harm of light on human health [6]. In truth, Li-Fi lamps comply with the Bee Law on Radiation Exposure, that is, they do not emit radiation that is harmful to health or interferes with the operation of medical equipment [10].

Only few researchers are interested in LiFi security issues [9, 13]. This is due to the fact that the literature affirms that this technology offers a better evolved security than the Wi-Fi by the fact that the radio waves are accessible from everywhere and can easily be intercepted while with the light waves this is not possible because they do not cannot cross obstacles. To have access to the Li-Fi connection, it is imperative to be under a light cone or light source. Thus, light cannot pass through obstacles (walls) is not a convincing argument for securing data, eavesdropping can occur in the Li-Fi network. This can happen when there is a gap between the floor and the door, light can spread between them and the grid becomes vulnerable. Based on the description of this problem, this paper aims to improve security on data exchanges by securing the light leak in the Li-Fi network by an asymmetric cryptographic algorithm of the AES type and by configuring a captive portal in order to authenticate each user in the network.

This paper is structured as follows: first we presented some key concepts and studied the main differences between Wi-Fi and Li-Fi technologies, then we presented the proposed solution by describing the adopted architectures and the configuration process, finally we concluded and presented some future works.

2. Key concepts

2.1. Li-Fi Technology

Li-Fi is a two-way, high-speed wireless communication technology that uses the visible part of the electromagnetic spectrum. Like Wi-Fi, Li-Fi, for example, allows a device to connect to the internet and therefore involves a transfer of data. The difference between these two technologies lies in the way of transmitting its data. Indeed, Wi-Fi connects computing devices within a network through radio waves, unlike Li-Fi, which, as said before, performs the same function using visible light: the data to be transmitted is encoded as an electrical signal and then transmitted as a light signal thanks to a circuit made up of one or more light sources (by light signal, we mean variations in the light intensity of the sources; in the case of Li-Fi, these variations are so rapid that they become imperceptible to the human eye). The variations in brightness can then be picked up by the devices concerned, will be transformed back into an electrical signal and decoded to recover the data, provided that these receiving devices are equipped with a light receiver. The term Li-Fi by analogy to Wi-Fi all derives its essence from the word Hi-Fi (High Fidelity) was proposed by Professor Harald Haas at the TED (Technology Entertainment and Design) conference [5]. The development of Li-Fi is strongly linked to the development of LEDs (Light Emitting Diodes), because they are the only light sources (apart from lasers) capable of having extremely fast switching (up to a million times per second) and a sufficient lifespan [7].

2.2. Architecture

The basic components of such a system are :

- Multiple LED lights for data transmission.
- A light sensor for receiving data.

As shown in Fig. 1, terminals can connect to the Internet through an LED lamp. The driver (lamp driver) controls the brightness of the LEDs according to the environment and the data received.

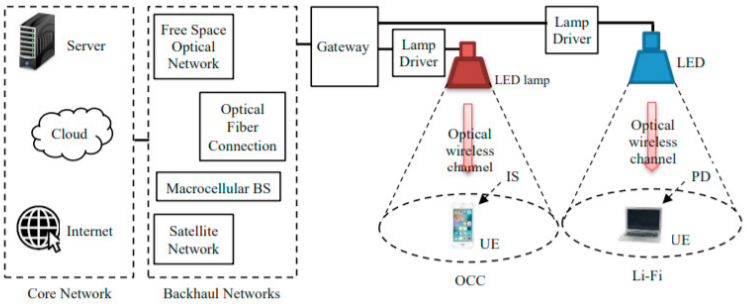

Fig. 1. Architecture of a Li-Fi system [1]

2.3. Working principle

The Li-Fi system consists of the many bulbs that form a wireless network, providing a user experience almost identical to that of Wi-Fi, but with the added benefit of using the visible spectrum. Each LED bulb gets data from an internet server and will store it in the LED. It will flash at a very high speed that will not be visible to the human eye. However, the Photodetector at the other end of the receiver will be able to read all scintillations and this data will be extracted after amplification and processing [7].

2.4. Advantage and Limitation of Li-Fi

1. Advantage
   The visible light spectrum has a wide frequency band of about 400 THz which is 10,000 times that of the radio band, it has a great advantage because of its health safety, Unlike Wi-Fi, which can not be used in some places, Li-Fi is more flexible because it does not present interference in those places, it has more advanced security than WI-Fi as the light that carries the data when a Li-Fi connection can not pass through the walls, and the transmitted data also can not be intercepted, compared to other wireless communication technologies, the cost of Li-Fi is among the cheapest , this is due to the lack of license. This technology differs from its competitors in that it does not waste a huge amount of energy because it uses the same lights. that we use daily for lighting.
2. Limitation
   Line of sight (LoS), Li-Fi is only accessible under a light cone, The transmission range of Li-Fi cannot compete with that of radio waves because it has a transmission range limited to 10 meters, another disadvantage of Li-Fi is its susceptibility to interference from other artificial light sources.

2.5. Li-Fi versus Wi-Fi

Li-Fi is a term used to describe visible light communication technology applied to high speed wireless communication. It acquired this name due to the similarity to Wi-Fi, using only light instead of radio waves as a transmission medium. Wi-Fi is ideal for general wireless coverage in buildings, while Li-Fi technology is ideal for high-density

wireless data coverage in confined areas and for reducing radio interference issues. The two technologies can therefore be considered as complementary. Li-Fi functionality includes the capacity, energy efficiency, security and safety benefits of a wireless system. They have a number of essential advantages over Wi-Fi, but by nature they are complementary technology. Table 1 represents a comparative study between these 2 technologies on different points.

Table 1. Li-Fi vs Wi-Fi

Full Name	Light Fidelity (*t*)	Wireless Fidelity (*t*)
Standard	802.15.7	802.11a
Year of creation	2011	1999
Coverage distance	10 meters	20-100 meters
Frequency range	430–770 THz	3 Hz to 3000 GHz
Communication	Based on communication by visible light	Based on communication by radio frequency
Debit	500 Mbps, up to 10 Gbps, 100 Gbps	11 Mbps
Environmental impact	Weak	Medium
Energy consumption	Weak	plenty
Interference	No interference	Interference with radio waves
Architecture	AttoCell	FemtoCell

3. Proposed solution and experimentation

3.1. Methodology

The schematic representation of our methodology is shown in Fig. 2

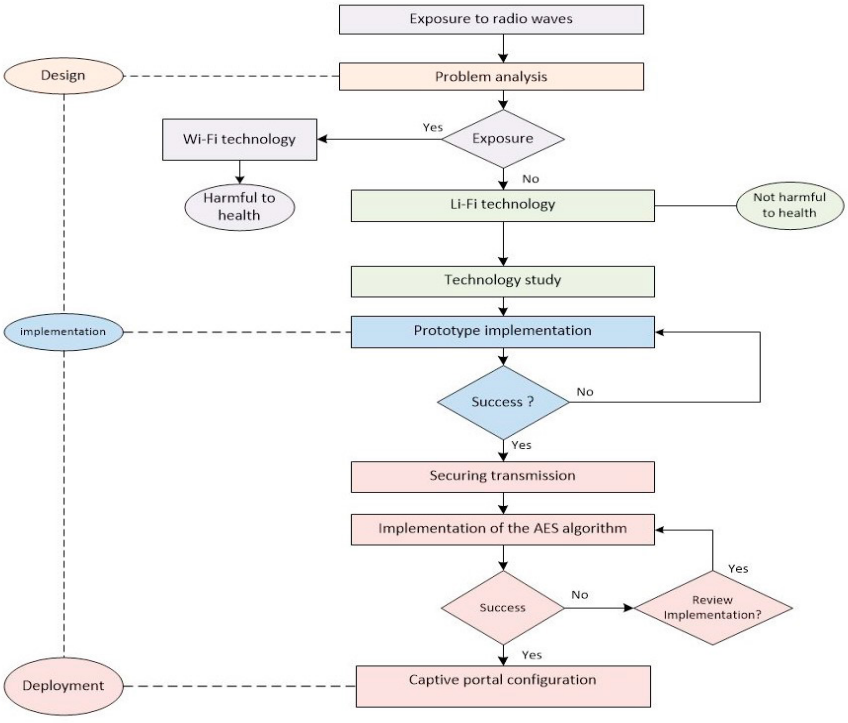

Fig. 2. Methodology flow diagram

3.2. Test architecture

To be able to do the test, we relied on an architecture shown in Fig. 3, which is called the test architecture. This architecture explains how it works, how we establish the connection links, or make the branching.

When we press button on the keyboard, the microcontroller converts the signal into electric light, the LED will light up. This light is considered as a transmission medium. On the receiver side, there is a device (photoresistor) capable of capturing light. In fact, it captures the light and converts it into a digital signal, which is then sent to the microcontroller, which in turn converts it to be read by humans thanks to the LCD (Liquid Crystal Display).

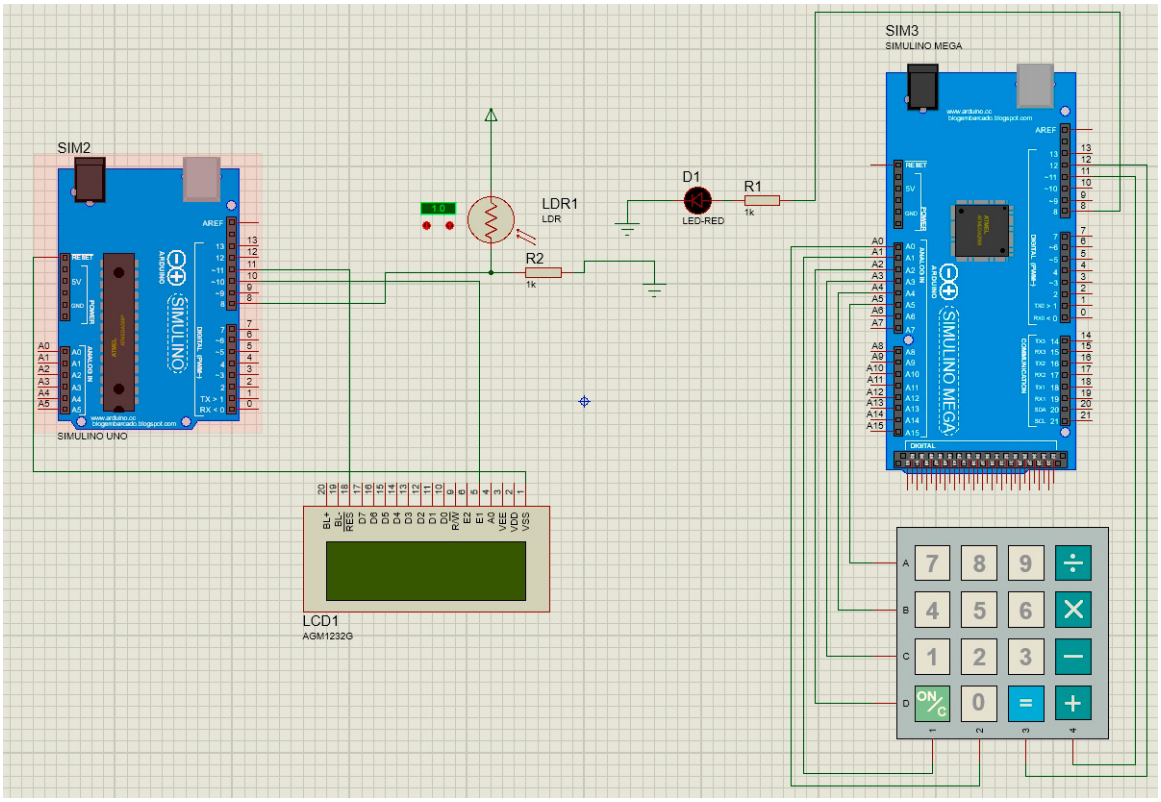

Fig. 3. Li-Fi test architecture

3.3. Transmission security in the Li-Fi network using AES algorithm

Li-Fi systems, or VLC systems in general, are often seen as a solution to spying problems, due to the fact that light cannot pass through walls. This property is a key point to prevent unauthorized people from accessing personal information, but it is not enough to fully protect against ”network sniffers”. Although the system broadcasts the data requested by a user mainly via a direct line of sight, the VLC channel has a broadcast nature, i.e. it will distribute the data to all users enlightened by the LEDs. This can cause a significant risk in public areas, where the light can be accessed by anyone, a threat such as eavesdropping can occur when there is a gap between the floor and the door, the light can spread between them. To ensure data security, according to [1], cryptographic protection (encryption, integrity and authentication) is undoubtedly an appropriate strategy to transmit data securely. It is one of the most widespread and popular techniques for securing information. This is basically done through the use of two essential processes: encryption and decryption. It renders a message unintelligible to anyone other than the rightful person. For our system, the cryptography algorithm chosen is the AES algorithm for ”Advanced Encryption Standard” because it is currently the most widely used and the safest.

3.4. Zeroshell captive portal in the Li-Fi network

To ensure user authentication on the Li-Fi network implemented, we developed a captive portal on the Li-Fi. This is a web page that appears to users newly connected to a wireless or wired network with a limited number of connections before they have full access to network resources. Details on the configuration and architecture are detailed in Section *Availability of materials*.

4. Conclusion

In this paper we proposed to secure the light of the Li-Fi network for possible security attacks. To achieve this, we have used the AES cryptographic algorithm to secure the data exchange between end users. Since our project should be implemented in the network of a hospital, the choice of Li-Fi was the best one compared to Wi-Fi because WiFi raises problem of human exposure to radio frequencies. Apart from the need for data transmission security, the aim was to limit the impact of the Wi-Fi waves on health, strengthen the safety of the Li-Fi system by implementing authentication mechanism. Based on the literature, we found that Li-Fi is renowned for a better rated security than Wi-Fi by the fact that light waves cannot pass through walls, but this does not guarantee us anything about data security, which is the reason for which we have built a system around the symmetric AES-type cryptographic algorithm in order to ensure data security. It should be noted that network management is a heavy task, we thought of setting up a captive portal authentication system through the Zeroshell software router.

Availability of materials

For any supplementary request, please find the details on the implementation of the prototype, the implementation of AES algorithm and the Li-Fi source code using Arduino technology by following the link https://github.com/Dib58/MyProject/tree/main/. A video of the implemented Li-Fi prototype is available on the following link https://tinyurl.com/59rsu33u.

Acknowledgements

The authors would like to thank the members of ABIL (www.abil.ac.cd) for material support. The authors express their deep thanks for the referee's valuable suggestions about the revision and improvement of the manuscript.

References

[1] Light fidelity (li-fi) : sécurité et secteur marchand. In *Actes de la 7e conférence internationale sur la photonique, l'optique et la technologie laser (PHOTOPTICS 2019)*, pages 154–62.
[2] Olivier Cachard. *La régulation des ondes électromagnétiques: droit et santé*. lexis-Nexis, 2020.
[3] Elena CIOBANU. L'eau–element essentiel de la vie humaine. *GUIDE DE BONNES PRATIQUES*, page 29, 2010.
[4] Kader Colnago. Scandale sanitaire des ondes électromagnétiques: pourquoi le npa devrait prendre position. 2015.
[5] Harald Haas. Wireless data from every light bulb, jul 2011. Accessed 2021-11-09.
[6] Harald Haas and Tezcan Cogalan. Lifi opportunities and challenges. In *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, pages 361–366. IEEE, 2019.
[7] Harald Haas, Liang Yin, Yunlu Wang, and Cheng Chen. What is lifi? *Journal of lightwave technology*, 34(6):1533–1544, 2016.
[8] Alain KALT. Tout savoir sur la téléphonie mobile et ses effets sur notre santé. 2010.
[9] Vinoth Kumar, VR Niveditha, V Muthukumaran, S Satheesh Kumar, Samyukta D Kumta, and R Murugesan. A quantum technology-based lifi security using quantum key distribution. In *Handbook of Research on Innovations and Applications of AI, IoT, and Cognitive Technologies*, pages 104–116. IGI Global, 2021.
[10] Isabelle Lagroye. Champs magnétiques, champs électromagnétiques et santé. *Environnement, Risques & Santé*, 1(1):24, 2016.
[11] Yonne Lautre. Agir contre la pollution électromagnétique en france, 2018. Accessed 2021-09-03.
[12] Yonne Lautre. Dangers sanitaires du wifi & autres sans-fil, 2018. Accessed 2021-11-09.
[13] Zhenyu Zhang, Anas Chaaban, and Lutz Lampe. Physical layer security in lifi systems. *Philosophical Transactions of the Royal Society A*, 2019.