A Review of Security Methods in Light Fidelity Technology

Mohammed Majid Msallam[1,2,*], Refik Samet[2]

[1]Control and Systems Engineering Department, University of Technology, Baghdad, Iraq

[2]Computer Engineering Department, Ankara University, Ankara, Turkey

Received 06 March 2024; received in revised form 13 April 2024; accepted 14 April 2024

DOI: https://doi.org/10.46604/peti.2024.13149

Abstract

Light fidelity (Li-Fi) technology is a communication technology using visible light. Li-Fi technology solves the problem of radio frequency bandwidth shortage in wireless fidelity (Wi-Fi) and is more secure considering the wall is impenetrable to the light. However, an exception can be made if a vulnerability emerges when having indoor communication, and the wall leak may induce the hacker to attack the network. Thereby, the encryption data is needed in one or all layers of Li-Fi technology to secure data. This paper presents a review of security threats that need to secure data when using Li-Fi technology to transfer data, and the used methods to secure data in Li-Fi technology are elaborated. A descriptive analysis is also used for related work. As a result, the challenges in Li-Fi technology with encryption used in one of those layers of Li-Fi technology are identified.

Keywords: Li-Fi technology, visible light communication, security of Li-Fi technology, architecture of Li-Fi technology

1. Introduction

Visible light communication (VLC) emerged as a new technique for quick fully-networked wireless communication [1] and is a continuation of the trend toward using a higher electromagnetic spectrum. Meanwhile, Light fidelity (Li-Fi) technology is an extension of a VLC-based technology using light as a communication media to replace wire communication. German scientist Harald Haas, the founder of Li-Fi technology, first coined the term Li-Fi in 2011 [2]. Additionally, light-emitting diode (LED) bulbs used as transmitters in Li-Fi technology are similar to those currently found in many energy-conscious offices and homes [3], while a chip that modulates light for optical transmission of data is built into Li-Fi technology LEDs [4].

Recently, the shortage of radio frequency bandwidth can be attributed to the pervasive utilization of wireless fidelity (Wi-Fi) technology on various devices, while the radio frequency bandwidth used in Wi-Fi technology is barely seen [5]. Thus, Li-Fi technology using the light spectrum is regarded as the solution. Specifically, the features of the light spectrum are wide bandwidth and different wavelengths. Moreover, the light spectrum can be modulated to transfer data using the intensity, color, or flicker rate of the light spectrum.

The key difference between Li-Fi technology and Wi-Fi technology lies in the medium used to transmit data, where Li-Fi technology utilizes visible light to transmit data, while Wi-Fi technology utilizes radio waves within specific frequency bands to transmit data. In other words, using different mediums leads to several keys as bandwidth, range, maturity, and security. The bandwidth of the visible light spectrum used in Li-Fi technology is larger than the bandwidth of the radio frequency spectrum used in Wi-Fi technology, which means the possibility of larger data rates and more devices being supported without encountering congestion when using Li-Fi technology to transfer data [6]. Li-Fi technology, which cannot penetrate walls

[*] Corresponding author. E-mail address: mohammedarjeeli92@gmail.com

English language proofreader: Chih-Wei Chang

because of a limited range of light waves, compared to Wi-Fi technology that can pass through walls and provide a greater coverage area. Li-Fi technology is still in a nascent stage of development, unlike the well-established Wi-Fi technology. Therefore, to facilitate Li-Fi technology, infrastructure, commercial viability, and relevant applications, further development is required [7].

Li-Fi technology offers inherent security as the light signal cannot easily pass through walls and reach unauthorized, whereas encrypting data to increase the security of Li-Fi technology is required. Meanwhile, Wi-Fi technology requires robust encryption protocols to ensure data security as the signal can travel through walls and potentially be intercepted by unauthorized devices. However, technically, in the context of Li-Fi and Wi-Fi technology, the encryption and decryption techniques are comparatively similar, while both technologies rely on established cryptographic algorithms and protocols for securing data transmission [8]. To concretely distinguish, Table 1 summarizes the difference between Li-Fi technology and Wi-Fi technology.

Table 1 Comparison of Li-Fi technology with Wi-Fi technology

Parameters	Light fidelity	Wireless fidelity
Standard IEEE	802.15.7	802.11 a/b/g
Abbreviation	Li-Fi	Wi-Fi
Founder	Harald Haas	National Cash Register Company
Year	2011	1990
Speed transfer data	224 Gbps	150 Mbps
Communication medium	Light waves	Radio waves
Frequency	300 THz	2.4 GHz
Range	10 m	10 m to 100 m
Components	LED bulb, photograph detector, and Li-Fi access point	Router, modem, and passages
Power consumption	Low	Medium
Security	High	Less
Cost	Low	High
Compatibility	Low	High

Li-Fi technology is characterized as the option of transmitting and receiving data efficiently, compared to Wi-Fi technology, and therefore reconciles Wi-Fi technology and Bluetooth [9]. Moreover, Li-Fi technology features the impermeability of data. Consequently, data security can be ensured using Li-Fi technology. Concerning facilities requiring meticulous supervision such as hospitals and airlines, Li-Fi technology is preferably deployed due to having no interference in other electronic signals [10-11]. Specifically, Li-Fi technology can transfer data with a speed of up to 224 GB per second owing to its light media transmission [12]. The speed of transmission data in Li-Fi technology is superior to the speed of transmission data in optical fibers pervasively used nowadays [13].

Biologically, Li-Fi technology does not have any detrimental effect on humans [14]. Moreover, the variation in the intensity of light in LED lamps that transmit data does not impact the eyes due to imperceptibly expeditious emission. Furthermore, the frequency of the light spectrum is free, unrestricted, and 10,000 times higher than that of the radio waves [15]. Li-Fi technology is more cost-effective than radio technology, and energy efficient due to using LEDs, which are energy efficient [16]. Nevertheless, inevitably, several limitations of Li-Fi technology are noticeable in specific conditions. First, due to light-based communication, the presence of line of sight (LOS) is the requisite of Li-Fi technology for the connection between the transmitter and receiver [17]. Second, the intensity of light is inversely proportional to the distance, which constrains the application of Li-Fi technology when encountering excessively long distances [2].

Li-Fi technology is used in a wide range of applications and fields. First, Li-Fi technology can be used in transportation where vehicles can communicate with vehicles, persons, networks, or infrastructure using this technology to send and receive information [18]. Meanwhile, car headlights can also be used to transmit information. Second, given that Li-Fi technology is sound system communications, audio transmission using Li-Fi technology has been proposed as an alternative to Bluetooth and Wi-Fi technologies [19]. Third, location detection for users through the details of the position to create a map at the central server can also be achieved using Li-Fi technology [20].

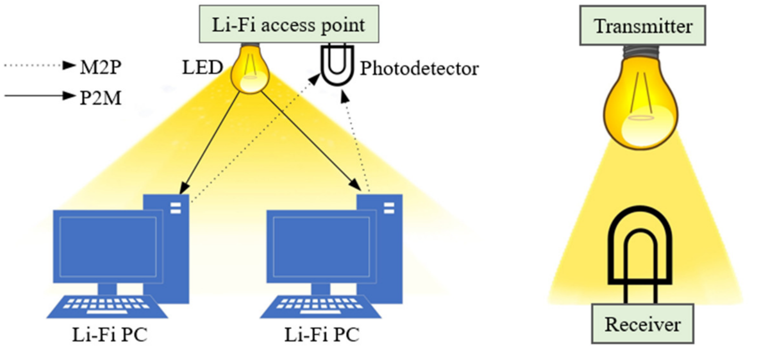
Furthermore, Li-Fi technology can be employed in educational systems due to the provision of faster internet connection [8]. In industrial areas, devices typically require a fast data transfer rate, and Li-Fi technology can consummately provide such a speed. Given its catholic applications, Li-Fi technology is superior to Wi-Fi technology, and the security in Li-Fi communication is better than in Wi-Fi communication. Concerning encryption and decryption, specifically, Li-Fi can implement both of them in one or all layers to ensure the security of encrypted data. Considering the encryption performance of Li-Fi technology, this study investigates the encryption process of Li-Fi technology and VLC in various layers since data is required to be encrypted before transmission. Additionally, this study has addressed the challenges that arise in each layer of Li-Fi technology when encrypted data is in one of those layers.

Regarding the content, this paper is organized as follows. Section 2 presents the basis of Li-Fi technology including structure, working principle, architecture, characteristics, security threats, and modulation techniques of Li-Fi technology. Section 3 reviews the used methods to secure data in Li-Fi technology including physical security, encryption methods, access control, medium access control (MAC) address filtering, light single tracking, optical orthogonal frequency division multiplexing (O-OFDM), quantum cryptography, and Li-Fi/Wi-Fi system. Section 4 mentions the challenges in Li-Fi technology when encryption is used in one of the Li-Fi technology layers. Finally, the conclusions and some future works about security issues requiring further investigations are mentioned.

2. Basics Li-Fi Technology

This section establishes the foundational principles of VLC and Li-Fi technology. First, the differentiation between Li-Fi technology and VLC technology is discussed. Second, the working principle section will elucidate the unique capability of Li-Fi to leverage LEDs for high-speed data transmission. The architecture section will further investigate the three-layered structure of Li-Fi systems, responsible for data transmission, management, and routing. Subsequently, the characteristics section will explore the advantages proffered by Li-Fi compared to traditional wireless technologies. The security threats section will address potential vulnerabilities associated with Li-Fi communication. Finally, the discussion will conclude by mentioning the modulation techniques employed in Li-Fi systems for data encoding.

2.1. Structure of Li-Fi technology



(a) Li-Fi communication (b) VLC communication

Fig. 1 Li-Fi and VLC communication

Technically, Li-Fi technology is an extension of VLC-based technology using light as a communication medium to replace wire communication. The goal of Li-Fi technology is to achieve secure and high-speed transfer of data from transmitter to receiver and to provide fully networked wireless communication [21]. Despite previously mentioning that Li-Fi is the extension of VLC, an obvious difference emerges between them. Specifically, the communication principle of Li-Fi technology is a complete wireless network system that contains a Li-Fi access point and devices. The Li-Fi network uses point-to-multipoint (P2M) and multipoint-to-point (M2P) and [22]. In P2M, a Li-Fi access point broadcasts data to multiple devices within its coverage area, while, in M2P, devices communicate individually with specific Li-Fi access points, as shown in Fig. 1(a) [23-24]. In contrast, VLC uses point-to-point (P2P) to communicate, as shown in Fig. 1(b).

A Li-Fi network is comprised of optical access points, which are known as attocells [25]. An attocell refers to a small, localized area covered by a single Li-Fi access point [26]. Fig. 2 shows Li-Fi access points that connect a different network with an ethernet cable. In comparison, the key difference between Li-Fi technology and Wi-Fi technology is that Wi-Fi technology uses radio waves to transmit data, whereas Li-Fi technology uses visible light. Therefore, Li-Fi technology can operate in places where the data would be vulnerable to electromagnetic waves at high speed to transfer data. Considering these aspects, Li-Fi technology will represent the fifth generation (5G) of wireless technology [27].

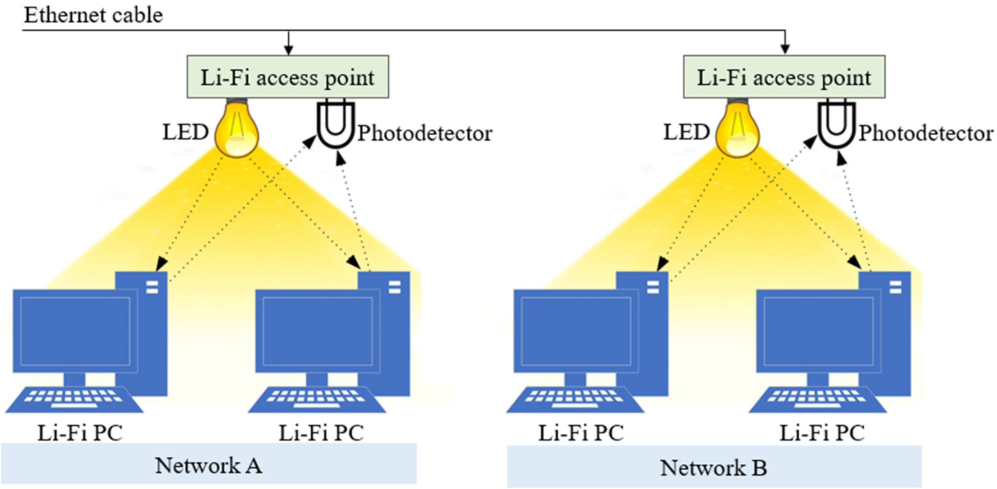


Fig. 2 The network of Li-Fi technology

2.2. Working principle of Li-Fi technology

Li-Fi technology uses an LED bulb as a transmitter with a photoreceptor as a receiver, as shown in Fig. 3. Meanwhile, the flicker rate of the LED is adjusted using an LED driver at the Li-Fi technology to modulate and transmit data. The transmitter transmits the digit of binary 1 when the LED is on and the digit of binary 0 when the LED is off. The delay of light in the free space optical (FSO) is rather low, which is 33.35 nanoseconds when light travels 10 meters. Therefore, understandably, the round trip time (RTT) is significantly short due to the high speed of the light [28], and the maximum data transmission speed is based on the alteration of the flicker of the LED.

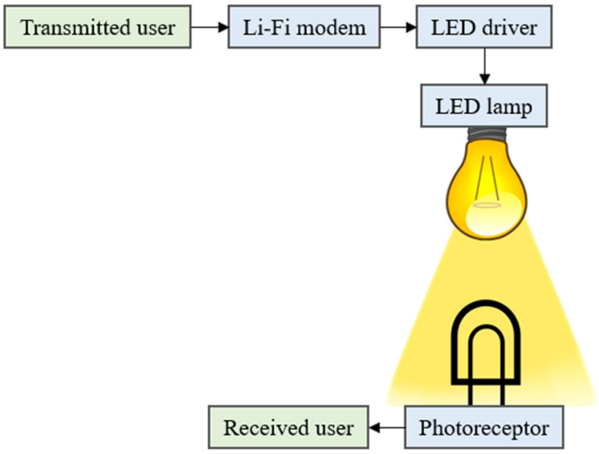


Fig. 3 Working principle of Li-Fi Technology

Fig. 4 shows a delay in receiving a binary signal when the data transmission speed is 1,000,000 bits per second, and the binary signal travels 10 meters using Li-Fi technology. Concerning the receiver, to receive data, it is habitually equipped with a photodetector. The receiver receives the digit of binary 1 when the photodetector detects light. In contrast, since the light is not detected, the digit of binary 0 would be received [29].

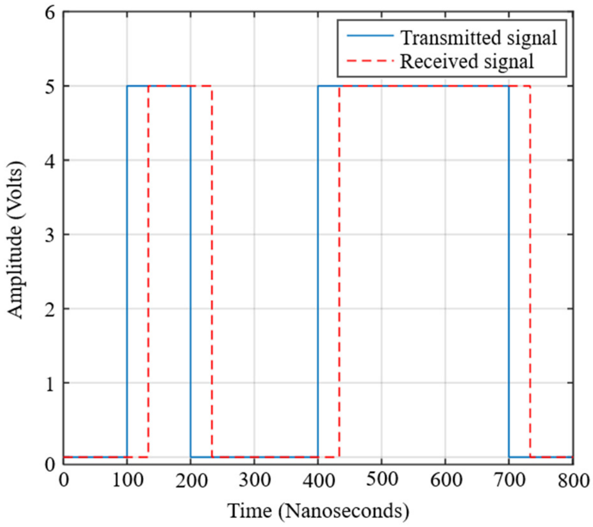


Fig. 4 The delay in receiving binary signal

2.3. Architecture of Li-Fi technology

The architecture of Li-Fi communication is built on three layers, namely the application layer, the MAC layer, and the physical layer [3]. The physical layer and the MAC layer are the only layers that the IEEE 802.15.7 protocol specifies [30]. Fig. 5 shows the layered architecture of Li-Fi technology.

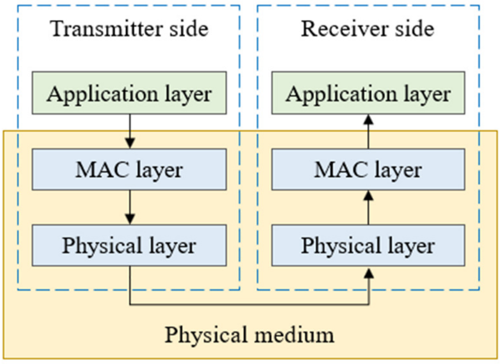


Fig. 5 Architecture of layers in Li-Fi technology

(1) Application layer

The application layer is constrainedly defined under the open systems interconnection (OSI) model. Specifically, the application layer is just the interface for interacting with host-based and user-facing programs, according to the OSI model [31]. In Li-Fi technology, the application layer defines the protocols and services, such as relay systems and various algorithms for routing as required by Li-Fi devices using the application layer in communication [29], providing network configuration, network manipulation, and message routing.

(2) MAC layer

The MAC layer controls the hardware responsible for interfacing with the optical wireless transmission medium. The MAC layer offers crucial functions such as synchronization, channel access, and addressing for Li-Fi devices [32]. Three topologies of a network that are defined in the MAC layer are peer-to-peer, star, and broadcast [33]. In peer-to-peer topology, it is communicated between two devices where one of them works as a coordinator. In star topology, it is communicated between multiple devices where one of them works as a coordinator and an infrastructure of illumination. In broadcast topology, the coordinator which is one of the devices in the network transmits data to multiple devices.

(3) Physical layer

The physical layer, also abbreviated as the physical layer, is processed data transmission and reception. The physical layer is responsible for deactivation, activation of optical transceivers, and the detection of the state of a transmission channel, whether it is busy or idle state [34]. In the Li-Fi system, the physical layers can be classified into three subordinate layers, i.e., physical I, physical II, and physical III [35]. Firstly, the physical I layer is used in outdoor applications, which has a data rate from 11.67 to 267.6 kilobits per second. Secondly, the physical II layer is used in indoor applications, which has a data rate from 1.25 to 96 megabits per second. Finally, the physical III layer is used in multiple optical transceiver applications, which has a data rate from 12 to 96 megabits per second [36].

2.4. Characteristics of Li-Fi technology

Li-Fi technology is considered superior to Wi-Fi technology due to several observable limitations emanating from Wi-Fi technology. However, a set of parameters that determine the efficiency of Li-Fi technology comparatively emerged. Details of the key parameters associated with Li-Fi technology are presented as follows.

(1) Capacity

The radio waves in Wi-Fi technology to transmit data are not cost-effective and performant as expected. Additionally, the amount of available radio spectrum is constantly depleted due to the irreconcilably elephantine usage of Wi-Fi technology [37]. In contrast, Li-Fi technology is expected to have the potential to offer higher capacity than Wi-Fi technology owing to a wider range of light spectrum. Numerically, the visible light spectrum is 10,000 times wider than the spectrum of radio waves and therefore emerges greater bandwidth in Li-Fi [38]. Furthermore, equipment of Li-Fi technology is already available for implementation due to the light sources naturally presented indoors and outdoors.

(2) Speed

Theoretically, Li-Fi technology can transfer data at far higher data rates than Wi-Fi technology [39]. Considering the transmission speed, such a postulation is understandably posed due to the superiority of light over radio waves. Data rates of Li-Fi technology can range from hundreds of megabits per second to terabytes per second [40], and the high data rates of Li-Fi technology depend on aspects such as modulation techniques and infrastructure in the system [41].

(3) Security

Radio waves used in Wi-Fi technology can penetrate through walls, which palpably provokes security concerns as radio waves can be easily intercepted and hack the Wi-Fi network. Consequently, Li-Fi technology is expected to be more secure than Wi-Fi technology given that the solid surface is impenetrable to light signals [42], on the other hand, hackers can barely invade Li-Fi networks. In addition, with the protection of LOS installed between the sender and receiver, it effectively scotches the possibility of hacking the Li-Fi network [43].

(4) Efficiency

Technically, Wi-Fi requires massive energy to send data [44], whereas Li-Fi technology consumes relatively less energy given that LED bulbs as the media of data transmission. Therefore, regarding energy consumption, Li-Fi functions more efficiently than Wi-Fi. Additionally, the light spectrum is less crowded than the radio spectrum. Thereby, Li-Fi does not suffer from the same level of congestion compared to Wi-Fi [45].

(5) Availability

Radio waves cannot be ubiquitously used, particularly in hospitals, airplanes, chemical and power plants, etc. [46], which hampers the flexibility of Wi-Fi applications. In contrast, Li-Fi technology is available in the condition of a sufficient and stable light source [47]. Hence, Li-Fi is convincingly possible to enable common users to use the internet everywhere.

(6) Coverage

Despite the security ensured by Li-Fi and direct LOS between the transmitter and receiver, the indoor range of Li-Fi is limited to 1-10 meters. To reconcile such a shortcoming reflected in Li-Fi coverage, the strategic deployment of additional LED transmitters within the desired area may required [48]. In other words, achieving blanket coverage using Li-Fi technology in large spaces might require a considerable amount of Li-Fi access points, which somewhat results in inefficiency.

2.5. Security threats in Li-Fi technology

In this section, possible security threats and various kinds of attacks when connecting Li-Fi are elaborated. Li-Fi technology has the property that light cannot pass through walls and thus ensures high security. However, the vulnerability emerges from the wall leak appearing spatially, and the hacker may be able to attack the network. The attacker may utilize the leakage to masquerade as the true data, which could pose a security threat [49], more concretely, attacks such as modification, snooping, or data jamming [50].

The modification, as noted above, is an attack on the integrity of data and occurs when an unauthorized party accesses data and tampers with the content [51]. The modification would be to alter the data packets being sent or launch a denial-of-service attack by flooding the network with erroneous data [52]. Modification attacks can be classified into insertion, deletion, and change [53]. In the insertion attack, the attacker inserts information previously absent in transmitted packets [54]. In the deletion attack, subsequently, the attacker removes existing information from transmitted packets [54]. In the change attack, the attacker changes existing information in transmitted packets that is already incorrect, and the change may intentionally target sensitive information or public information [55].

Another attack on the security of data is snooping, which is also called sniffing or eavesdropping [56-57]. Eavesdropping may occur when a user connects to an unprotected network and transfers sensitive data to a receiver. Meanwhile, in the context of using Li-Fi, the eavesdropper may lurk through a small gap under a door, windows, and keyholes [3]. To prevent data from eavesdropping, using encryption data in the sender and decryption at the receiver are strongly recommended. The jamming is regarded as a blockage to hamper the accessibility of data transmission despite the spatial presence of several light sources [58]. The jamming attack, whether deployed intentionally, could incur an attenuation in system performance and even the range of availability of the system. Reactive jamming is the derivation of jamming, which aims to interfere with the packet's synchronization at the receiver [59].

2.6. Modulation techniques of Li-Fi technology

Modulation is to carry and transmit specified data on the light, while modulation signals flicker an LED at different frequencies to transmit data. Moreover, according to the signal frequency, modulation can be subdivided into single-carrier modulation (SCM) and multiple-carrier modulation (MCM).

(1) Single-carrier modulation

SCM is a modulation technique where multiple signals can be received, whereas each signal is modulated separately at a different frequency. SCM is habitually used in applications with moderate to low data rates. To further subdivide based on different conditions of the pulse, pulse amplitude modulation (PAM), pulse-position modulation (PPM), and on-off keying

(OOK) are subcategories in SCM [60]. In PAM, the amplitude of a continuous sequence of signal pulses is used to encode certain data [61]. Meanwhile, PPM provides dimming and efficient support in variable PPM, where the position of signal pulses is used to encode certain data [38]. In OOK, the LED executes the activation or deactivation to transmit data using a visible light signal, where it transmits the digit of binary 1 when activating the LED and the digit of binary 0 when deactivating, respectively [62].

(2) Multiple-carrier modulation

MCM is a modulation technique segmenting the bandwidth into multiple subcarriers, while each one is used to transmit a portion of the data. OFDM and color shift keying (CSK) are the subcategories of MCM. OFDM is mainly used when plural devices are used as a transmitter to mitigate the shadowing effect [63]. CSK, also called Color Modulation, uses multiple colors of light with various wavelengths to send more bits of data simultaneously. Concerning the colors, red, blue, and green LEDs are utilized to transmit three bits of data simultaneously [64]. In this status, the receiver is designed to identify the different wavelengths of detected light and decode the transmitted data.

The second section summarizes the pros and cons of Li-Fi technology, and the fundament of Li-Fi data transmission is also introduced. Structurally, Li-Fi can be anatomized into the physical layer, MAC layer, and application layer. Regarding the security concerns, the possible threats of Li-Fi are analyzed above. By comprehensively and scrupulously analyzing the feasibility of Li-Fi, it has attested to the operative simplicity and convincing security.

3. Review the Used Methods to Secure Data in Li-Fi Technology

Given that visible light waves used in Li-Fi technology cannot pass through the wall, Li-Fi technology offers security advantages and employs various encryption methods to secure transferred data to increase security. This section will present a mini-review of the technique used to secure data in Li-Fi technology.

3.1. Physical security

Unlike Wi-Fi technology which uses radio waves, Li-Fi technology uses light waves that cannot penetrate walls or other opaque objects. This restriction within a room or designated area significantly prevents the network from the potential attack of eavesdropping while using Li-Fi technology to communicate [65]. Li-Fi technology relies on providing a direct LOS between the light source and receiver to transmit or receive data, yielding a hindrance to unauthorized access [66]. In this subsection, a portion of the signal light is used to encrypt the data matter, where the received past sample is used to generate the encryption key, as shown in Fig. 6. This encryption technique has been employed [67-69].

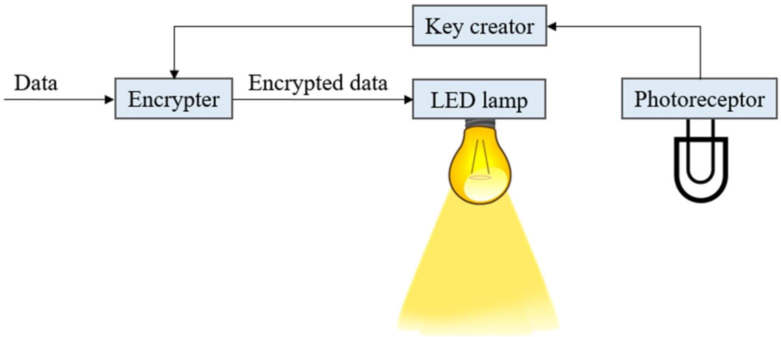


Fig. 6 Physical security in Li-Fi technology

3.2. Encryption methods

Li-Fi technology is still a new concept being developed, especially in the aspect of data security, as works emerged to encrypt transmitted data using this technology with different algorithms to yield robustness for this technology. Fig. 7

visualizes the process of encrypting data before sent while using Li-Fi. Methodologically, the algorithms used to encrypt transmitted data using Li-Fi technology were Advanced Encryption Standard (AES), Rivest Cipher 2 (RC2), Rivest Cipher 4 (RC4), Rivest Cipher 5(RC5), Rivest Cipher 6 (RC6), Blowfish, and Caesar Cipher Wheel [70-73].

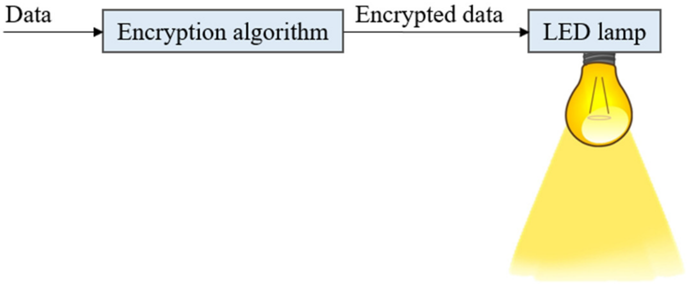


Fig. 7 Encryption in Li-Fi technology

3.3. Access control

Li-Fi technology relies on visible light to transmit and receive data, enabling precise control to access the Li-Fi network. The network can be protected by blocking the holes in the walls, windows, or doors, which enables light beams to be in contact with authorized devices and prevents unauthorized devices from accessing the Li-Fi network. Such protection is depicted in Fig. 8. This property facilitates a secure data transmission system in classrooms [74].

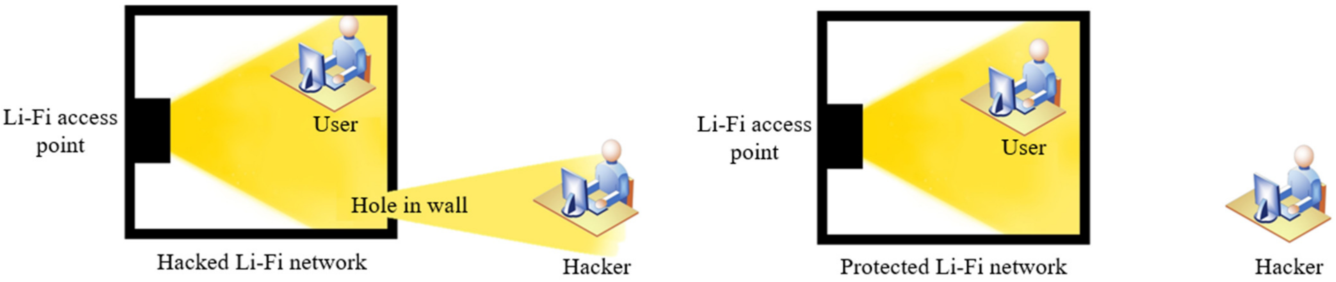


Fig. 8 Access control in Li-Fi technology

3.4. MAC address filtering

Li-Fi networks can filter devices in the network based on the MAC addresses and whitelist trustworthy devices to connect to the Li-Fi network [75]. MAC is a special number that is assigned to a network interface controller (NIC). MAC addresses of devices are saved in a table, where an algorithm in Fig. 9 filters authorized devices to enter and enable the devices to connect to the Li-Fi network. In home automation, the MAC address is assigned to the home device that is connected to the Li-Fi network [76]. These addresses are saved in the table to facilitate access to home devices quickly and with high security.

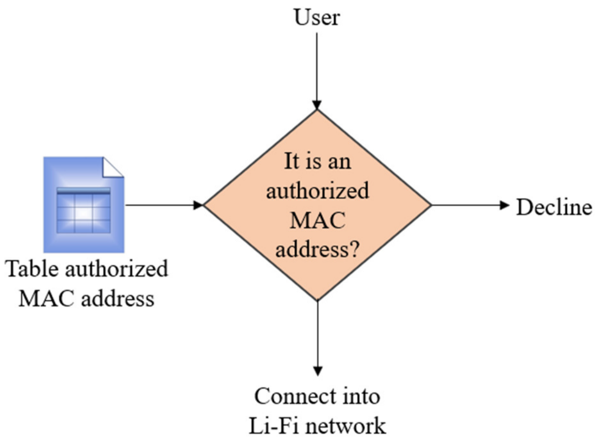

User
It is an authorized MAC address?
Decline
Table authorized MAC address
Connect into Li-Fi network

Fig. 9 MAC Address filtering in Li-Fi technology

3.5. *Light single tracking*

Li-Fi systems can track the location of a light signal to detect and blacklist unauthorized access attempts [77]. Such a process is found in advanced Li-Fi systems. The location of the signal is tracked by calculating the actual location of the user using triangulation algorithms [78]. Fig. 10 shows the technique used in Li-Fi technology since the tracker represents a real user. The values of the predicted position should be proximate to the real position. Otherwise, the entity will be marked as a fake user. This system is also used in the presence of multiple Li-Fi access points providing connectivity [79].

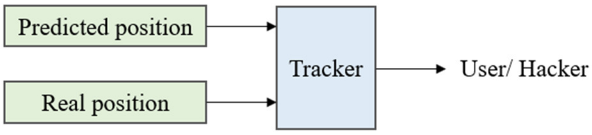


Fig. 10 Tracking system in Li-Fi technology

3.6. *Optical orthogonal frequency division multiplexing*

O-OFDM is a technique that segments transmitted data into multiple frequency bands and sends each partition of transmitted data to a specific frequency band [80]. This process includes passing data to obfuscate the eavesdropper, which yields greater security to the Li-Fi network and prevents data from interception [81]. Fig. 11 shows a transmitter and a receiver of the O-OFDM technique used in Li-Fi technology.

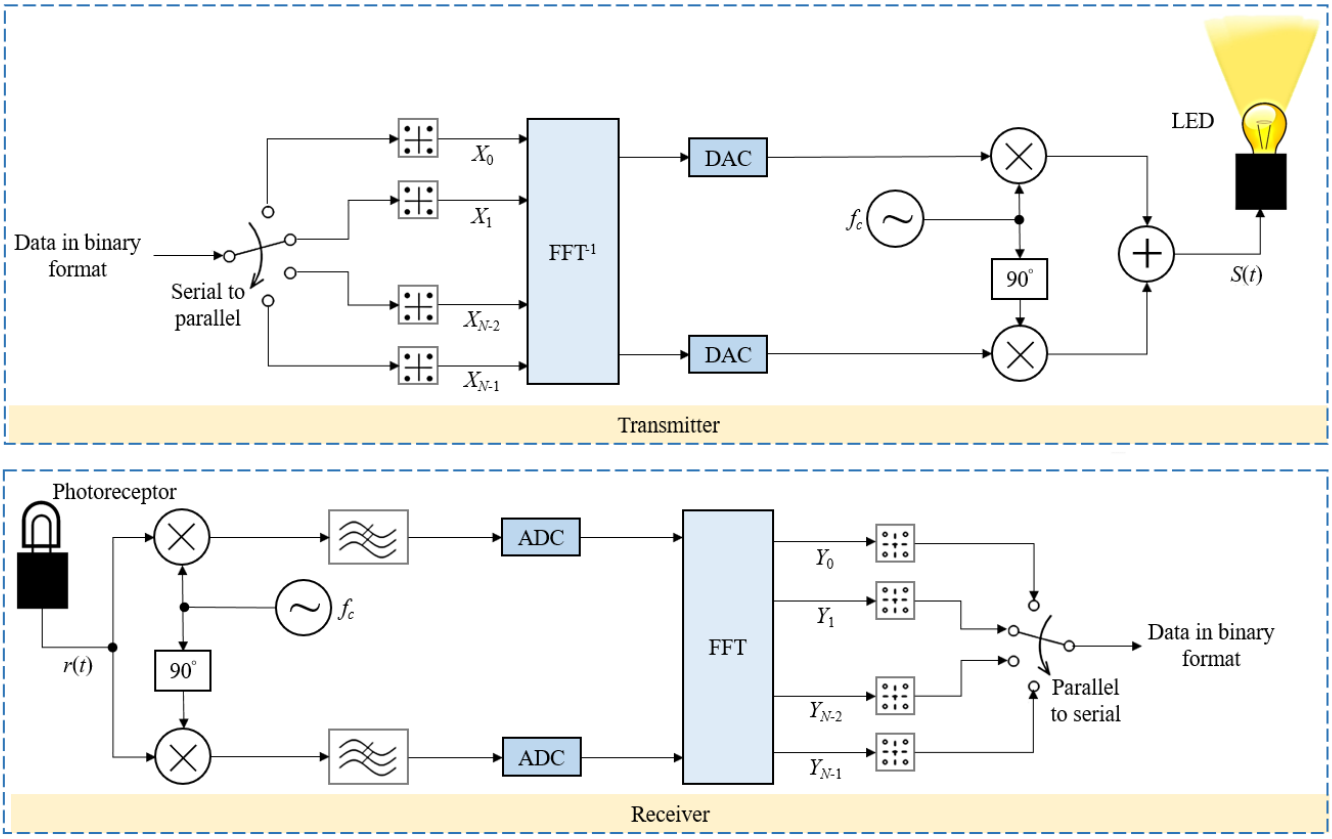


Fig. 11 O-OFDM technique in Li-Fi technology

3.7. *Color shift keying*

CSK modulates data by rapidly changing the colors emitted by LEDs and leverages the inherent color control of LEDs, potentially achieving higher data rates than traditional methods [82]. CSK segments transmitted data into multiple partitions. This process also includes passing data to obfuscate eavesdroppers due to each partition of transmitted data sent by LED with a certain color light, as shown in Fig. 12.

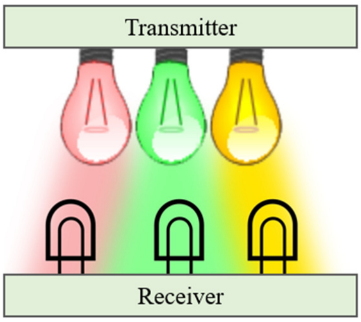


Fig. 12 Transmitter and receiver in CSK modulation

3.8. *Quantum cryptography*

The integration of quantum cryptography in Li-Fi technology is a representative improvement in the secure communication field, where quantum cryptography utilizes the strange properties of quantum mechanics to create unbreakable codes [83]. Quantum cryptography is also known as quantum key distribution [84]. It transmits messages using special particles in multiple states synchronously, hindering the possibility of eavesdropping without alerting the sender and receiver, ensuring ultimate security for highly sensitive information. The system comprising quantum cryptography and Li-Fi provides potentially infallible security [85]. Fig. 13 graphically presents Li-Fi technology using quantum cryptography as a method to secure transmitted data.

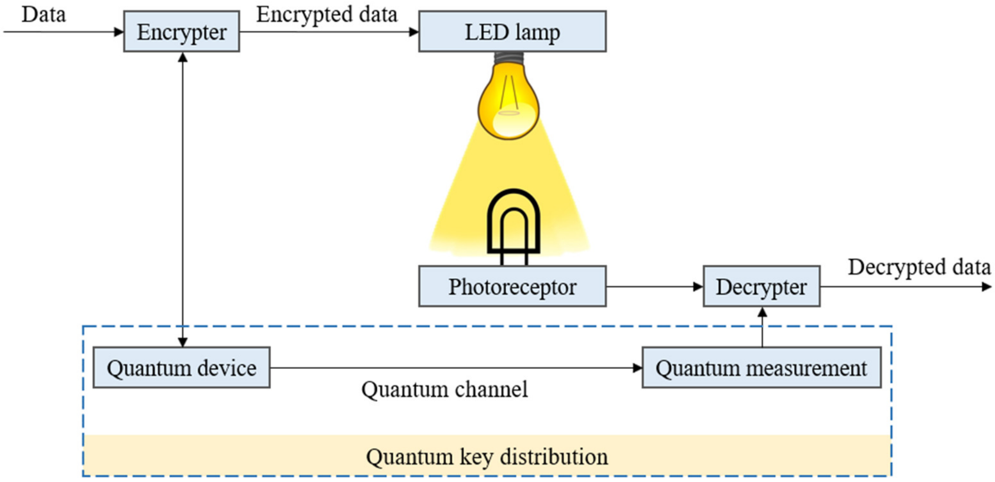


Fig. 13 Quantum cryptography in Li-Fi technology

3.9. *Li-Fi/Wi-Fi system*

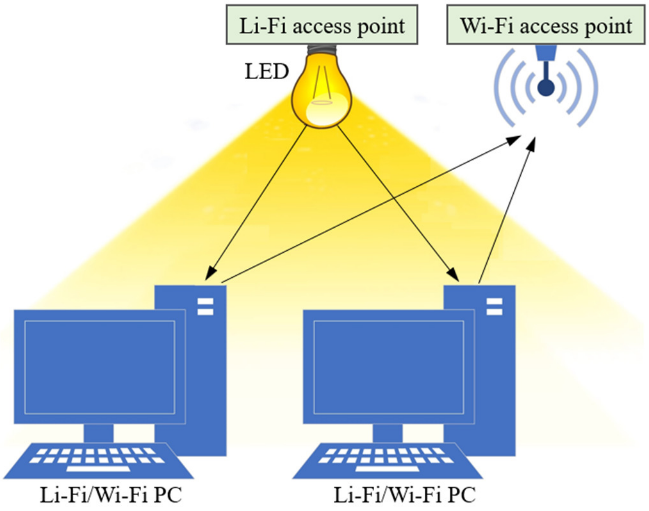


Fig. 14 Li-Fi/Wi-Fi system

Li-Fi/Wi-Fi system refers to the combination of Li-Fi technology and Wi-Fi technology in a system [83]. It is a hybrid system of orchestrating Li-Fi technology and Wi-Fi technology, where the downlink of Li-Fi technology is provided through Li-Fi technology, and the uplink is supported via Wi-Fi technology, as shown in Fig. 14 [75]. Li-Fi/Wi-Fi system is enhanced security due to the data transmission using two different technologies [85].

In this section, the problems of wall leakage of data that occur in Li-Fi technology and increasing security in Li-Fi technology are addressed by using the aforementioned methods. The method above improves the security of Li-Fi technology. For future work, high security can be achieved by implementing several methods previously introduced in one system. Encryption methods, quantum cryptography, access control, MAC address filtering, and O-OFDM or CSK can be used to obtain high security.

4. Secure Challenges of L-Fi Technology

Given that Li-Fi is still new, the criteria to encrypt transferred data has not been formulated yet. Each layer of Li-Fi technology has a format of specific data, where the encryption used in those layers has benefits and challenges. This section will present the benefits and challenges of encryption used in the application layer, MAC layer, and physical layer.

4.1. Application layer

Application layer encryption is a solution of data security that encrypts almost every type of data in an application. In this encryption, it uses the aforementioned methods and algorithms to encrypt data before sending it, and this process increases the protection of the sent data against many types of attackers. Flexibility, granular control, and compatibility are advantages when encryption is used in this layer. First, application layer encryption is flexible due to its adaptability to a variety of applications and data formats, which validates its strength for usage in a range collection of situations. Second, concerning the granular control, application layer encryption provides more precise control for transmitted data to offer protection, where it encrypts sensitive data only and leaves other data unencrypted [86]. Additionally, application layer encryption is compatible with current encryption algorithms and protocols, which enable seamless integration with current infrastructure and applications [87]. However, selecting specific algorithm encryption is required in the application layer of Li-Fi, and, when implementing encryption, some difficulties emerged are listed as follows:

(1) Performance attenuation: both encryption and decryption processes take time for data to transmit.

(2) Intricacy: encryption requires modifying the code of the application layer or using additional encryption libraries.

(3) Reliance: encryption used in the application layer depends on the security of the end devices, which may incur vulnerability if the devices are compromised.

4.2. MAC layer

When Encryption is used in the MAC layer of Li-Fi technology, it increases secure data transfer. Consequently, encrypting the data packets at the MAC layer before the packet moves into the physical layer of the Li-Fi technology is occasionally adopted [88]. Encryption in the MAC layer of Li-Fi technology offers several advantages, such as simplification, less performance impact, and standardization Concerning the complexity, encryption is suggested for implementing in the MAC layer of Li-Fi technology due to the independence of physical properties of the light. Since encryption in the MAC layer of Li-Fi technology does not affect data rate, it has less effect on the Li-Fi performance of systems. Moreover, several existing standards for encryption have been currently used in the MAC layer of Li-Fi technology, such as AES-CCM and WPA2 [87]. Notwithstanding the strengths stated above, still, several difficulties still emerge from the encryption implemented in the MAC layer of Li-Fi technology. The difficulties are introduced as follows:

(1) Longer delay: the data requires encryption or decryption before the packet can be transmitted or received.

(2) Less security: due to the independence of the physical properties of the light, the data is more susceptible to eavesdropping and decryption attacks.

(3) Physical limitations: given physical independence, physical protection is not supported while encrypting in the MAC layer of Li-Fi technology and is therefore prone to physical attacks, such as jamming and tampering in the Li-Fi transmitter or receiver.

4.3. Physical layer

Encryption in the physical layer of Li-Fi technology is currently under investigation. Various approaches are being used to secure transmitted data, whereas all these approaches converge into the same goal of using the physical characteristics of light signals to secure data during transfer [89]. Furthermore, when users encrypt data in the physical layer of Li-Fi, eavesdroppers can barely intercept and decrypt the data due to higher security. In addition to higher security, improved robustness and potential for new applications are also the benefits of encrypting in the physical layer. The encryption embedded in the physical layer of the Li-Fi technology is difficult to forge and increases security because it depends on the characteristics of the channel [69]. Li-Fi technology is more reliable when encryption is used in the physical layer due to shielding Li-Fi technology from interference and noise [90]. The physical layer encryption of Li-Fi technology could extend new applications, such as secure communication in sensitive environments [71]. However, still, various challenges still emerge when encryption is implemented in the physical layer of Li-Fi technology. The challenges are as follows:

(1) Performance attenuation: the attenuation of performance can be attributed to the possibility that the encryption will increase signal overhead and decrease data rate.

(2) Intricacy: the encryption in the physical layer of Li-Fi technology requires it be tailored to the specific physical characteristics of light signals.

(3) The absence of standardization: this might hinder the widespread adoption of Li-Fi technology.

In summary, every layer of Li-Fi technology when used for encryption has its pros and cons, while most of the shortcomings mentioned above remain unsolved currently and need further investigations to optimize Li-Fi technology.

5. Conclusion

Li-Fi technology is a wireless communication technology that uses visible light to transmit data, unlike Wi-Fi technology using radio waves. Historically, Li-Fi technology was invented by Harald Haas in 2011, which consists of an LED as the transmitter and a photodetector as the receiver. Functionally, Li-Fi technology features the capability to transmit data at a high data rate and high security. Moreover, structurally, Li-Fi technology consists of three layers, viz., application layer, MAC layer, and physical layer. Due to the leaking problem of the light from the locks or holes in the wall, Li-Fi technology as a communication media urgently requires reinforcement to secure data. Thus, this paper reviewed the security risks that should be considered while transferring data over Li-Fi technology and outlined the techniques that have been employed to improve data security. Furthermore, the difficulties in using encryption in one of those layers of Li-Fi technology have been noted in this research, and further research to solve data security concerns is needed.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] B. G. Guzman, M. S. Mir, D. F. Fonseca, A. Galisteo, Q. Wang, and D. Giustiniano, "Prototyping Visible Light Communication for the Internet of Things Using OpenVLC," IEEE Communications Magazine, vol. 61, no. 5, pp. 122-128, May 2023.

[2] O. Faruq, K. R. Shahriar Rahman, N. Jahan, S. Rokoni, and M. Rabeya, "Li-Fi Technology Based Long Range Free-Space Communication Data Transmit System Evaluation," International Review of Applied Sciences and Engineering, vol. 14, no. 3, pp. 413-425, December 2023.

[3] E. Ramadhani, "A Mini Review of LiFi Technology : Security Issue," International Journal of Computer and Information System, vol. 3, no. 3, pp. 90-93, July-September 2022.

[4] S. P. Cowsigan, S. Narendhran, B. Nithisree, and T. J. Jisshnu Kannan, "Vehicle to Vehicle Communication Using Li-Fi Technology," 8th International Conference on Advanced Computing and Communication Systems, pp. 1065-1068, March 2022.

[5] C. Singh, Modeling and Optimization of Optical Communication Networks, Hoboken: John Wiley & Sons, Inc., pp. 365-380, 2023.

[6] A. E. Ibhaze, P. E. Orukpe, and F. O. Edeko, "High Capacity Data Rate System: Review of Visible Light Communications Technology," Journal of Electronic Science and Technology, vol. 18, no. 3, article no. 100055, September 2020.

[7] O. D. Alao, J. V. Joshua, A. S. Franklyn, and O. Komolafe, "Light Fidelity (Li-Fi): An Emerging Technology for the Future," IOSR Journal of Mobile Computing & Application, vol. 3, no. 3, pp. 18-28, May-June 2016.

[8] Rabia, N. Ali, S. Ali, A. Sajid, and A. Zafar, "A Security Review Over Wi-Fi and Li-Fi," Information Management and Computer Science, vol. 3, no. 1, pp. 01-09, April 2020.

[9] L. I. Albraheem, L. H. Alhudaithy, A. A. Aljaser, M. R. Aldhafian, and G. M. Bahliwah, "Toward Designing a Li-Fi-Based Hierarchical IoT Architecture," IEEE Access, vol. 6, pp. 40811-40825, 2018.

[10] A. Neelopant, M. Yavagal, and R. Byahatti, "PC to PC Data Transfer Using Li-Fi," International Research Journal of Engineering and Technology, vol. 07, no. 08, pp. 2224-2227, August 2020.

[11] J. Sanusi, A. M. Aibinu, S. Adeshina, G. Koyunlu, and S. Idris, "Review of Handover in Li-Fi and Wi-Fi Networks," Second International Conference on Computer Networks and Communication Technologies, pp. 955-964, May 2019.

[12] V. Karthik, K. Balashanmugam, S. Abithsingh, S. Akash, and S. Arivumani, "High Speed Transmission of Data or Video Over Visible Light Using Li-Fi," International Conference on Advanced Computing Technologies and Applications, pp. 1-6, March 2022.

[13] R. Karthika and S. Balakrishnan, "Wireless Communication Using Li-Fi Technology," SSRG International Journal of Electronics and Communication Engineering, vol. 2, no. 3, pp. 6-14, March 2015.

[14] D. D. Diambeki, R. E. Mandiya, K. Kyamakya, and S. K. Kasereka, "Securing the Light Escaping in a Li-Fi Network Environment," Procedia Computer Science, vol. 201, pp. 684-689, 2022.

[15] A. Akbar Ali, R. Harish Kumar, R. Dheenathalayan, N. Prasanth, V. Parthasaradi, S. Senthilkumar, et al., "Audio Streaming Using Li-FI Communication," Irish Interdisciplinary Journal of Science & Research, vol. 7, no. 1, pp. 01-07, January-March 2023.

[16] S. Gupta, M. Sarkar, H. Kaur, M. Agrebi, and A. Roy, "An Efficient Data Transferring Through Li-Fi Technology: A Smart Home Appliance," Multimedia Technologies in the Internet of Things Environment, vol. 3, pp. 59-78, April 2022.

[17] F. Khair, I. W. Mustika, A. F. Isnawati, and N. Azizah, "Analysis of Bit Rate and Distance Variation on Multiplexing System of Indoor Li-Fi Technology Using Movable LED Panel," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 7, no. 2, pp. 246-253, April 2023.

[18] R. Badeel, S. K. Subramaniam, Z. M. Hanapi, and A. Muhammed, "A Review on LiFi Network Research: Open Issues, Applications and Future Directions," Applied Sciences, vol. 11, no. 23, article no. 11118, December 2021.

[19] S. Saranya, B. Ragavi, L. Pavithra, S. Susheel, M. Srivarsha, and V. Vishal, "Audio Transmission Using Visible Light Communication and Li-Fi Technology," 6th International Conference on Inventive Computation Technologies, pp. 19-24, January 2021.

[20] H. K. Yu and J. G. Kim, "Smart Navigation with AI Engine for Li-Fi Based Medical Indoor Environment," International Conference on Artificial Intelligence in Information and Communication, pp. 195-199, February 2019.

[21] Z. T. Aldarkazaly, M. F. Younus, and Z. S. Alwan, "Data Transmission Using Li-Fi Technique," International Journal of Advanced Science and Technology, vol. 29, no. 3, pp. 7367-7382, 2020.

[22] V. Meenakshi and S. M. Rafi, "A Survey on Light Fidelity Transmission Scheme Using VLC," International Journal of Management, Technology And Engineering, vol. 9, no. 6, pp. 422-427, June 2019.

[23] N. Saeed, A. Celik, T. Y. Al-Naffouri, and M. S. Alouini, "Underwater Optical Wireless Communications, Networking, and Localization: A Survey," Ad Hoc Networks, vol. 94, article no. 101935, November 2019.

[24] I. Al _Barazanchi, S. A. Sahy, Z. A. Jaaz, and H. R. Abdulshaheed, "Traffic Management with Deployment of Li-Fi Technology," Journal of Physics: Conference Series, vol. 1804, article no. 012141, 2021.

[25] A. E. Willner, Optical Fiber Telecommunications VII, United Kingdom: Academic Press, pp. 443-493, 2020.

[26] H. Haas, M. S. Islim, C. Chen, and H. Abumarshoud, An Introduction to Optical Wireless Mobile Communications, Norwood: Artech House, 2021.

[27] S. Alfattani, "Review of LiFi Technology and Its Future Applications," Journal of Optical Communications, vol. 42, no. 1, pp. 121-132, January 2021.

[28] E. Setiawan, T. Adiono, R. Mulyawan, N. Sutisna, I. Syafalni, and W. O. Popoola, "A Real-Time Baseband Processor for Li-Fi Internet Access," Wireless Communications and Mobile Computing, vol. 2022, article no. 6154495, 2022.

[29] M. A. S. Sejan and W. Y. Chung, "Secure VLC for Wide-Area Indoor IoT Connectivity," IEEE Internet of Things Journal, vol. 10, no. 1, pp. 180-193, January 2023.

[30] P. Shams, M. Erol-Kantarci, and M. Uysal, "MAC Layer Performance of the IEEE 802.15.7 Visible Light Communication Standard," Transactions on Emerging Telecommunications Technologies, vol. 27, no. 5, pp. 662-674, May 2016.

[31] A. Fraihat, "Computer Networking Layers Based on the OSI Model," Test Engineering & Management, vol. 83, pp. 6485-6495, July/August 2020.

[32] A. Km and S. Duttagupta, "HDL-Ready MAC Layer Implementation for Multi-Node Li-Fi Communications," International Journal of Information Technology, vol. 15, no. 4, pp. 2039-2051, April 2023.

[33] A. Arora, A. Rao, and M. Bhutani, "A Matlab Simulation Model for MAC Layer of Visible Light Communication," 7th International Conference on Signal Processing and Integrated Networks, pp. 941-945, February 2020.

[34] N. Elmangosh, I. Ighneiwa, and I. F. Elshami, "The Impact of Li-Fi Technology on Industrial Wireless Sensors Networks," International Conference on Engineering & MIS, pp. 1-7, July 2022.

[35] R. George, S. Vaidyanathan, A. S. Rajput, and K. Deepa, "LiFi for Vehicle to Vehicle Communication–A Review," Procedia Computer Science, vol. 165, pp. 25-31, 2019.

[36] K. D. Salman and E. K. Hamza, "Visible Light Fidelity Technology: Survey," Iraqi Journal of Computers, Communications, Control and Systems Engineering, vol. 21, no. 2, pp. 1-15, June 2021.

[37] T. D. Subha, T. D. Subash, N. Elezabeth Rani, and P. Janani, "Li-Fi: A Revolution in Wireless Networking," Materials Today: Proceedings, vol. 24, part 4, pp. 2403-2413, 2020.

[38] W. Lemstra, V. Hayes, and J. Groenewegen, The Innovation Journey of Wi-Fi: The Road to Global Success, Cambridge: Cambridge University Press, pp. 331-366, 2011.

[39] O. Faruq, K. R. Shahriar Rahman, N. Jahan, S. Rokoni, and M. Rabeya, "Li-Fi Technology-Based Long-Range FSO Data Transmit System Evaluation," Sustainable Engineering and Innovation, vol. 5, no. 1, pp. 85-98, February 2023.

[40] A. E. Ibhaze, P. E. Orukpe, and F. O. Edeko, "Li-Fi Prospect in Internet of Things Network," Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference, vol. 1, pp. 272-280, March 2020.

[41] W. Mongwewarona, S. M. Sheikh, and B. C. Molefhi, "Survey on Li-Fi Communication Networks and Deployment," African Journal of Engineering Research, vol. 8, no. 1, pp. 1-9, February 2020.

[42] A. A. Elngar, Handbook of Computational Sciences: A Multi and Interdisciplinary Approach, Hoboken: John Wiley & Sons, Inc., 2023.

[43] A. Ali, A. M. Chirawu, S. W. Zahra, M. Nadeem, Z. Hussain, K. S. A. H. Palli, et al., "A Visible Light-Based Indoor Navigation and Localization Solution for Visually Criticized Users," Journal of Telecommunication, Switching Systems and Networks, vol. 10, no. 2, pp. 22-34, 2023.

[44] C. W. D. Lumoindong, A. Muslim, B. M. Nasreddin, and M. Galina, "Performance and Environmental Impacts Review of Li-Fi and Wi-Fi Technologies," Journal of Environmental Engineering and Waste Management, vol. 3, no. 2, pp. 68-75, 2018.

[45] P. P. Rezayie, H. Shokrzadeh, M. D. T. Foladi, A. Rahmani, and S. M. Nasab, "Load Balancing in the Combined Technology of Li-Fi and Wi-Fi Based on Collaborative Game," International Journal of Distributed and Parallel Systems, vol. 14, no. 1/2/3/4/5/6, pp. 11-31, November 2023.

[46] P. Kuppusamy, S. Muthuraj, and S. Gopinath, "Survey and Challenges of Li-Fi with Comparison of Wi-Fi," International Conference on Wireless Communications, Signal Processing and Networking, pp. 896-899, March 2016.

[47] S. Dinesh and B. Chourasia, "Light Fidelity (Li-Fi) Technology: Will It Be an Eco-Friendly for Monitoring the Covid-19 Patients in Hospital," International Conference on Advance Computing and Innovative Technologies in Engineering, pp. 234-238, March 2021.

[48] P. Porkar Rezaeiye, A. Sharifi, A. M. Rahmani, and M. Dehghan, "Access Point Selection in the Network of Internet of Things (IoT) Considering the Strategic Behavior of the Things and Users," The Journal of Supercomputing, vol. 77, no. 12, pp. 14207-14229, December 2021.

[49] M. S. Bari, “LiFi Technology in Future Benefits in Several Sectors,” Journal of Science, Computing and Engineering Research, vol. 1, no. 3, pp. 67-72, July-August 2020.

[50] S. Riurean, M. Leba, and L. Crivoi, “Enhanced Security Level for Sensitive Medical Data Transmitted through Visible Light,” International Symposium on Networks, Computers and Communications, pp. 1-6, October-November 2021.

[51] S. Duggineni, “Impact of Controls on Data Integrity and Information Systems,” Science and Technology, vol. 13, no. 2, pp. 29-35, 2023.

[52] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, “Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat towards Smart Substation Pathways,” Sensors, vol. 21, no. 19, October 2021.

[53] K. A. E. Drandaly, W. Khedr, I. S. Mohamed, and A. M. Mostafa, “Digital Watermarking Scheme for Securing Textual Database Using Histogram Shifting Model,” Computers, Materials & Continua, vol. 71, no. 3, pp. 5253-5270, 2022.

[54] Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidehpour, and S. Shi, “A Simplified Co-Simulation Model for Investigating Impacts of Cyber-Contingency on Power System Operations,” IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4893-4905, September 2018.

[55] S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, “Security Issues in Mobile Ad Hoc Networks,” Procedia Computer Science, vol. 92, pp. 329-335, 2016.

[56] Y. S. Hussein and A. C. Annan, “Li-Fi Technology: High Data Transmission Securely,” Journal of Physics: Conference Series, vol. 1228, article no. 012069, 2019.

[57] M. Ozkan-Okay, O. Aslan, R. Eryigit, and R. Samet, “SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN,” IEEE Access, vol. 9, pp. 157639-157653, 2021.

[58] Y. Qi, J. Li, C. Wei, and B. Wu, “Free-Space Optical Stealth Communication Based on Wide-Band Spontaneous Emission,” Optics Continuum, vol. 1, no. 11, pp. 2298-2307, November 2022.

[59] H. Ruotsalainen, “Reactive Jamming Detection for LoRaWAN Based on Meta-Data Differencing,” Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1-8, August 2022.

[60] M. A. S. Sejan, R. P. Naik, B. G. Lee, and W. Y. Chung, “A Bandwidth Efficient Hybrid Multilevel Pulse Width Modulation for Visible Light Communication System: Experimental and Theoretical Evaluation,” IEEE Open Journal of the Communications Society, vol. 3, pp. 1991-2004, 2022.

[61] S. Salvi and V. Geetha, “From Light to Li-Fi: Research Challenges in Modulation, MIMO, Deployment Strategies and Handover,” International Conference on Data Science and Engineering, pp. 107-119, September 2019.

[62] B. Aydin and Ç. Duman, “Examination of OOK Modulation Schemes in Li-Fi Systems,” Optik, vol. 270, article no. 169996, November 2022.

[63] L. Sun, “Research on Construction and Simulation of Communication System Model Based on ODFM Technology,” IEEE International Conference on Sensors, Electronics and Computer Engineering, pp. 1361-1365, August 2023.

[64] R. Becerra, C. A. Azurdia-Meza, P. Palacios Jativa, I. Soto, J. Sandoval, M. Ijaz, et al., “A Wavelength-Dependent Visible Light Communication Channel Model for Underground Environments and Its Performance Using a Color-Shift Keying Modulation Scheme,” Electronics, vol. 12, no. 3, article no. 577, February 2023.

[65] X. Liu, W. Wang, G. Song, and T. Zhu, “LightThief: Your Optical Communication Information is Stolen behind the Wall,” Proceedings of the 32nd USENIX Conference on Security Symposium, pp. 5325-5340, August 2023.

[66] S. H. Alnajjar and H. M. Mahmoud, “Internet of Things Utilizing Light Fidelity Technology: A Review,” Al-Iraqia Journal for Scientific Engineering Research, vol. 2, no. 4, pp. 1-8, December 2023.

[67] I. Romdhane and H. Yuksel, “A Low-Complexity Security Technique in Physical Layer for Fixed LiFi Communication Systems,” Journal of Information Security and Applications, vol. 53, article no. 102514, August 2020.

[68] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, “Robust Key Generation from Optical OFDM Signal in Indoor VLC Networks,” IEEE Photonics Technology Letters, vol. 28, no. 22, pp. 2629-2632, November 2016.

[69] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, “Physical-Layer Security against Known/Chosen Plaintext Attacks for OFDM-Based VLC System,” IEEE Communications Letters, vol. 21, no. 12, pp. 2606-2609, December 2017.

[70] W. S. Aldolimi, A. A. Hnaif, and M. A. Alia, “Light Fidelity to Transfer Secure Data Using Advanced Encryption Standard Algorithm,” International Conference on Information Technology, pp. 963-967, July 2021.

[71] M. M. Msallam and R. Samet, “An Advanced Rivest Cipher 4 Algorithm to Transfer Fast and Secure Data Using Li-Fi Technology,” IEEE 13th International Conference on System Engineering and Technology, pp. 194-199, October 2023.

[72] S. Jeya Anusuya, S. Venket, V. Logesh Kumar, T. Manoj Gowtham, V. Goutham, and R. Gowtham, “Data Transmission by Ceaser Cipher Wheel Encryption Using LiFi,” International Journal of Advance Research, Ideas and Innovations in Technology, vol. 4, no. 2, pp. 512-517, March-April 2018.

[73] T. Koroglu and R. Samet, “Can There Be a Two Way Hash Function?” IEEE Access, vol. 12, pp. 18358-18386, 2024.

[74] S. Apoorv, S. K. Bhowmick, and E. Annadevi, “Implementation of Li-Fi Technology in Classrooms,” IOP Conference Series: Materials Science and Engineering, vol. 590, article no. 012044, 2019.

[75] S. Ullah, S. U. Rehman, and P. H. J. Chong, “A Comprehensive Open-Source Simulation Framework for LiFi Communication,” Sensors, vol. 21, no. 7, article no. 2485, April 2021.

[76] I. Siṃha, Z. Gao, and C. Massarelli, IoT Applications Computing, London: IntechOpen, article no. 98616, 2022.

[77] I. Madjarov, J. L. Damoiseaux, and R. Iguernaissi, “Towards Designing a Li-Fi-Based Indoor Positioning and Navigation System in an IoT Context,” Proceedings of the 2021 Future of Information and Communication Conference, vol. 1, pp. 266-277, April 2021.

[78] K. D. Salman and E. K. Hamza, “Indoor Positioning Systems Based on Li-Fi Technology Using RSS-Triangulation with Assisted by DNN,” International Journal of Intelligent Engineering and Systems, vol. 15, no. 2, pp. 213-231, April 2022.

[79] R. Kaur and H. Walia, “Review on Light Fidelity (Li-Fi) - An Advancement of Wireless Network,” International Journal of Wireless and Microwave Technologies, vol. 7, no. 3, pp. 25-35, May 2017.

[80] A. W. Azim, Y. Le Guennec, M. Chafii, and L. Ros, “Enhanced Optical-OFDM with Index and Dual-Mode Modulation for Optical Wireless Systems,” IEEE Access, vol. 8, pp. 128646-128664, 2020.

[81] A. Agarwal, C. Mohanta, and G. Misra, “Li-Fi Technology: Principle, Future Scope, Challenges and Applications,” American Journal of Electrical and Electronic Engineering, vol. 10, no. 1, pp. 1-5, 2022.

[82] O. O. Atiba, “Optical Wireless and Visible Light Communication Techniques,” Master’s thesis, Faculty of Information Technology and Communications Sciences, Tampere University, Tampere, Finland, 2023.

[83] X. Wu, M. Safari, and H. Haas, “Access Point Selection for Hybrid Li-Fi and Wi-Fi Networks,” IEEE Transactions on Communications, vol. 65, no. 12, pp. 5375-5385, December 2017.

[84] K. W. Hong, O. M. Foong, and T. J. Low, “Challenges in Quantum Key Distribution: A Review,” Proceedings of the 4th International Conference on Information and Network Security, pp. 29-33, December 2016.

[85] A. H. Hasanudin, I. H. Zainal, Z. Abdul-Mutalip, F. Jasman, and W. H. Wan-Hassan, “From WI-FI to LI-FI: A Comprehensive Review of Integration Strategies,” Przeglad Elektrotechniczny, vol. 2023, no. 9, pp. 171-174, September 2023. (In Polskim)

[86] V. Prakash and C. T. Manimegalai, “Data Security Using RTL Algorithm with Chaos Synchronization for VLC System,” Journal of Optics, vol. 51, no. 4, pp. 801-809, December 2022.

[87] M. S. R. Shimul, “Utilizing Li-Fi Transmission for IoT Devices to Strengthen Indoor Security,” Ph.D. dissertation, Department of Electronic and Telecommunication Engineering, International Islamic University Chittagong, July 2023.

[88] M. Bhutani, B. Lall, and M. Agrawal, “Optical Wireless Communications: Research Challenges for MAC Layer,” IEEE Access, vol. 10, pp. 126969-126989, 2022.

[89] Y. Xiao, L. Zhou, Z. Pan, Y. Cao, and W. Chen, “Physically-Secured High-Fidelity Free-Space Optical Data Transmission through Scattering Media Using Dynamic Scaling Factors,” Optics Express, vol. 30, no. 5, pp. 8186-8198, February 2022.

[90] S. Vappangi and V. V. Mani, “A Survey on the Integration of Visible Light Communication with Power Line Communication: Conception, Applications and Research Challenges,” Optik, vol. 266, article no. 169582, September 2022.