

**Li-Fi Technology: High data transmission securely**

Yaseein Soubhi Hussein and Amresh Chetty Annan

Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia

dr.yaseein@staffemail.apu.edu.my, amre78@gmail.com

**Abstract.** Visible light communication (VLC) is an optical wireless communication method which transmits data through the medium of light within the visible light spectrum. The bidirectional communication through the light is called light fidelity Li-Fi. The infrastructure of such technology is already available where the light can be used for illumination and communication simultaneously. In the paper, we discuss the usage of VLC applied as Li-Fi as a secure method to transmit data wirelessly in a more secure method compared to the traditional Wi-Fi architecture. In addition, we investigate the bit-error rate (BER) performance in the VLC network based on the modulation format of Orthogonal Frequency-Division Multiplexing (OFDM) for high data transmission.

**Index Terms**— Least Square method (LS), Light Fidelity (Li-Fi), Minimum Mean Square Error method (MMSE), Orthogonal Frequency-Division Multiplexing (OFDM), Secure Li-Fi network, Visible Light Communication (VLC)

1. **Introduction**

Li-Fi communications system was coined by Harald Haas in 2011, based on the idea of transmitting data via the imperceptible flickering of LED light. Morse code as an on-off series that happening so fast, its invisible to the human eye. The VLC technology also known light fidelity Li-Fi and it is highly expected to be the Wi-Fi replacement for indoor communication. The current download is 40 gigabits per second (Gbps) in early testing, 2017 [1]. Comparing to the best Wi-Fi systems available max data rate at around 300 Mbps (around 100 times slower). In addition, the expected download data rate for Li-Fi to be 100 Gbps.

Integrating and implementing a new method of wireless data transmission into an existing environment in which hardware and software have already been installed is a difficult task. Especially when that environment has been around for many years and has the confidence of most end users. It is because most users are unaware of the disadvantages in the current architecture. Currently, all environments that have electronic communication and data transfer involve the usage of the standard 802.11 wireless fidelity (Wi-Fi). Despite Wi-Fi being readily available and immensely scalable, the benefits, is what causes the disadvantage. This is because Wi-Fi uses radio waves to transmit data from one point to another. This radio wave spectrum has multiple limitations.

With the Internet of Things (IoT) technology, there is a huge number of devices expected to be connected to internet. This makes another issue for the current Wi-Fi networks and might be fully saturated and unable to accommodate such number of users.
In this paper, we discuss the security level of Li-Fi has over Wi-Fi and the various other benefits as to why Li-Fi could prove to be the future of secure wireless transmission. We also investigate the usage of channel estimation and its methods with OFDM based VLC network. A comparison between two methods, least square (LS) and Minimum Mean Square Error method (MMSE), is done and evaluated with a discussion of the results to cement the necessity of a robust and excellent channel estimation method for high data rate.

2. Literature Review

The Li-Fi technology has been rather hot these past few years after Professor Harald Haas coined the term back in 2011. Lots of research has been done to make it a reality to be the major substitute to Wi-Fi. Minor analysis has been done to get knowledge about the know-how and system specification of the Li-Fi system and how to emulate it in a controlled environment, via a simulation. Thus, this review of previous work will be carried out to gain more insight into Li-Fi and possibly help us improve on the limitations of older research and solve problems.

After an increase and continuous demand for quicker and more reliable internet connection since the radio spectrum has become insufficient, some researchers sought to increase the frequency of transmissions from below 10GHz to above 10GHz [2]. This might seem good on paper, but it poses serious problems such health concerns and lack of ability to pass through obstruction thus needing more hardware. As for health concerns, an increase in radio frequency may impact human health. With the current frequencies used, such at the 2.4GHz and 5GHz bands, human health is in no immediate danger but, with performance and speed concerns at stake, an increase in frequency will pose issues as the human body is not meant to take high radio frequency environments. A research done in 2018 highlights the many health risks documented by various other reports by other researchers to link the dangers of regular Wi-Fi signals [3]. With that information, we will definitely bear in mind the consequences of high frequencies as opposed to using Li-Fi which uses light as a medium in which high amounts of light does not have any adverse health risks. To add to this, the radio frequency is also limited as compared to the visible light frequency and that can be seen in the figure below.

![Comparison of VLC and RF frequencies](image)

With basic knowledge on Li-Fi, a comparison must be made to see the differences between the current architecture Wi-Fi and Li-Fi to see if it actually is an important change. According to [4] in 2016, it was found that there were a few major differences that can give us a deeper understanding into the impact of implementing Li-Fi. It can be seen that Li-Fi is built with a stronger and more futureproof base compared to Wi-Fi since the visible light spectrum has 10,000 times broader spectrum compared to radio frequency [5]. This is shown in the figure above. The speed of Li-Fi also proves to be nearly 100 times faster in addition to being health conscious as visible light frequency has no harm on human and animals. Li-Fi has many attractive features, such as an unlicensed spectrum, worldwide availability of unused
bandwidth, non-interference with radio frequency (RF) bands, very high data rates and secure communication [6], [7].

In addition to weaknesses posed by Wi-Fi, the security risks are needed to pay close attention to as it is discussed in this paper. As seen in many researches [8], [9]. Wi-Fi seems to pose many security issues that can easily be exploited. Small/ large offices, homes and organisations all use wireless networks to transmit data and if it is compromised, lots of information may be leaked. Exploits such as sniffing/eavesdropping, distributed denial-of-service (DDoS) and man-in-the-middle (MITM) attacks are some of the few that are commonly seen and are successful at getting information they want [8]. By pumping up security, these attacks will be on the low ‘for a while’ as attackers think of new and more devastating attacks. Thus, based on research [9], [10] a new method should be in place to avoid these risks posed to organisations especially ones that deal with sensitive information.

Furthermore, the advantages of Li-Fi often seems to outweigh the ones of Wi-Fi especially in terms of security and moving forward in the technological age. It can be seen in research done in 2014 [11] that Li-Fi is secure as it does not penetrate walls, allowing visible users, tremendous data transmission rates and safe light waves which allows for more applications in the real world if developed and implemented. This study is highlighting the potential of applications that can grow immensely especially in the medical industry as Wi-Fi can harm the human body and underwater communications as radio waves are absorbed by the currents and waves of water [12]. Thus, showing the large margin of benefits displayed by Li-Fi.

On the other hand, Li-Fi has one drawback compared to Wi-Fi that is the dependence on line of sight (LOS) connections between the transmitter and receiver. If the LOS is lost, connection is ceased, leaving issues with placement of the LEDs. To combat this, solutions need to be in place and based on a 2014 study [13], it is said that by pumping up the signal strength and placing Li-Fi in smaller rooms in the beginning as it is a new technology will provide a good stepping stone to rid of those problems. This issue may be solved by considering the reflected light as a replacement of LOS connection. Therefore, this eco-friendly data transmission method will be part of future wireless networks such as 5G.

3. Literature Review

Channel estimation is the essential technique that is used to detect the signal (visible light) coherently, with a low bit-error rate (BER) and try to remove as much distortion and noise [14], [15]. There are multiple benefits that can be acquired from the usage of channel estimation, namely, a very low BER which allows near full data transmission wirelessly. Aside from that, it also lowers and potentially avoids inter-channel interference that can affect the quality of transmission [16]. Despite this, there are some challenges involved which is that by using some channel estimation algorithms, which include difficulty in implementation. This is caused by the complexity of the algorithm itself such as the MMSE method which has a very low BER but has a high complexity rate [17], [18]. Thus, making it difficult to use despite the good results which forces some designers to opt for a simple algorithm that may not get as good results.

4. Proposed Method

As of now, the common methods being used for Li-Fi channel estimation are either LS or MMSE [17]. At the case of channel estimation absence, this could potentially hinder the accuracy and performance of recovering the original transmitted data due to certain reasons such as noise, interference and signal
fluctuation. These reasons being, for implementing LS or MMSE channel estimation, it is very important on receiver sides for OFDM systems to achieve lower BER and consequence high data rate.

Figure 2 shows the general indoor Li-Fi architecture of the proposed method. It is comprised of a transmitter and receiver that are located on the ceiling and end-user device respectively. As seen in the figure, the transmitter LED will be considered as a base station while the end-user device can be any device equipped with a photodiode. The environment shows that the indoor communication takes place for short-range data transmission. 

4.1 Simulation

For the proposed method design, we have implemented an existing channel estimation method to investigate the BER for Li-Fi network. These two methods, LS and MMSE are evaluated based on a software simulation in MATLAB. The simulation parameters are presented in Table 1.
Table 1: Example of a table of simulation

| Parameter                                      | Value                                      |
|-----------------------------------------------|--------------------------------------------|
| Transmitted optical power by individual LED (P_t) | 20 mW                                      |
| Room Size                                     | (5 × 5 × 3) m³                            |
| Location for 4 LEDs                           | (1.25, 1.25, 3), (1.25, 3.75, 3), (3.75, 1.25, 3), (3.75, 3.75, 3) |
| Semi-angle at half power (Φ1/2)               | 30, 70 degrees                             |
| Filter gain Ts(Φ)                             | 1                                         |
| Number of LEDs per array                      | 60 × 69                                    |
| Active area (A)                               | 1 cm²                                      |
| Concentrator gain g(Φ)                        | 2.5                                        |

[19]

We create a new Li-Fi environment in which we set up the transmitter, LED, and receiver, photodiode, and this connection can be placed up to a distance of maximum 5 meters. At the transmitting side, the signal is set and is modulated to be sent across an optical channel, light, to the receiver side. The signal is then received by the photodiode (PD) and is demodulated. This is because the bits sent will contain lots of noise and will potentially have a high BitError Rate (BER) which will cause loss of original bits. We then set up the demodulation of the signal at the receiving end to reduce the BER to almost nil. This allows nearly hundred-percent of the packets to be received successfully. Thus, giving chance to properly determine if there are any issues with the current architecture and whether or not any changes or modifications need to be made to further improve the system [20].
5. Results and Discussions

Li-Fi uses the light waves to transmit data wirelessly compared to the radio signals used by Wi-Fi. Thus, it works efficiently within the light source and the environment within the allowed radius which prevents any unwanted users sniffing the traffic and packets that are being transmitted [21]. Whereas for Wi-Fi, the long-distance capabilities hinder the security as people who are far away can easily monitor packets and potentially carry out a man-in-the-middle attack that severely compromises integrity and confidentiality of data.

Li-Fi also is a directed beam of light in which it is based off light waves that can only be transmitted in a straight line. This allows corporations to create highly secure networked zones that use VLC to increase privacy within the area [21]. For example, the IT department network is using Li-Fi technology which significantly secures the private company data being transmitted. Moreover, Li-Fi networks cannot pass through opaque objects, such as walls due to the nature of the light waves. These security advantages stem from the result of Li-Fi being a highly focused technology that requires precision of light to receiver to ensure effective transmission [22].

Li-Fi also have already been proven to have significantly faster transmission speeds as compared to Wi-Fi. This can be seen via lab tests that were carried out in which the theoretical speed of Wi-Fi is a mere 1 Gbps whereas its Li-Fi counterpart can hit up to 224 Gbps. In addition to this, the average internet connection in the United States during the first quarter of 2017 was recorded to be only 18.7 Mbps while Li-Fi transmission methods have already hit 1 Gbps in lab testing [23].

Thus, with a higher speed output, comes the capability of a higher bandwidth usability. Since the visible light frequency is 10,000 times larger than the radio frequency used by Wi-Fi (Wi-Fi uses the 2.4GHz and 5GHz bands while Li-Fi uses between 4 and 8THz), Li-Fi allows users an improved and higher browsing speed for regular internet access while allowing companies to provide a larger bandwidth for security systems implementations [24]. This was previously less, since heavy Wi-Fi bandwidth usage led to immense network issues such as lag and slow data rates and transmissions. Furthermore, the Li-Fi frequencies that it uses is not subject to external interferences that can affect the performance of the network or the external device unlike radio frequencies that often have interference issues. Thus, making Li-Fi highly functional and beneficial in secure and equipment-heavy environments.

Despite the obvious benefits for security purposes and significant improvements in terms of speed and performance, Li-Fi comes with its own set of disadvantages that clearly stem from the fact that it is still a largely prototyped-based technology that is not ready for mainstream usage yet. Thus, more robust and advanced research and tests must be done to ensure that it is consumer ready and a decent alternative to the current Wi-Fi architecture to coax users to invest in this new technology.

By not penetrating walls and having a highly focused network comes the disadvantage of its limitation in the transmission area [22]. For example, a home user needs to be exactly within the light area to allow for data to be detected which can become a demotivating factor.

In addition, despite the fact that Li-Fi technology is significantly more secure than Wi-Fi and extremely difficult to carry out attacks to potentially sniff and obtain data, it still is not impossible to do so. Thus, due to the fact that the difficulty levels of attacking Li-Fi networks are very high. However, according to [25] there is some possibility to disrupt or even hijack legitimate network transmission sessions within certain Li-Fi networks using VLC.
Finally, it provides a strong and nearly impenetrable network which cannot penetrate walls and be sniffed, allowing secure and private information to be transferred without any worries about data leakage and other attacks [26]. To summarize Li-Fi security in one sentence, “what you see is what you send” [25].

The analysis of the data that was carried out after the research methods were stated and explained in detail have garnered enough results that we can now display the results from the simulation software. With these results, analysis can now be done and discussed to further cement the progress so far of this paper in terms of system workability and performance.

Figure 3 shows the result of BER performance for Li-Fi networks. The figure shows the Signal-to-Noise (SNR) ratio against the Bit-Error Rate (BER) to showcase the performance levels and outcome of the simulation using the methods stated in the proposed method which is the least square method (LS) and the minimum mean square error (MMSE) method against the proposed hybrid solution which combines the two methods.

Based on the Figure 3, it can be seen that the two methods were started off by having the exact same BER, as well as the benchmarking where no channel estimation is implemented. It is obvious that, from the figure, to achieve a BER of $10^{-1}$, the MMSE channel estimation requires 15 dB of SNR whereas the LS method requires 2 more dB of SNR to achieve similar results. For no channel estimation, it is impossible to achieve such BER even with very high SNR value of more than 30 dB.

According to the Figure 3, it's seen clearly that the BER decreases gradually as the SNR increases for all the methods. It also can be seen that the MMSE method performs better in terms of having a lower BER compared to the LS method. This is because the MMSE involves a more complex computational process and a matrix inversion, which highly increases complexity of the channel estimation implementation compared to LS. While it does help with lowering the BER, it also increases complications during coding and implementation.

While it is shown that the LS method has a higher BER than MMSE but still better than no channel estimation. LS is known to have a less complicated and more convenient method to implement. But, along with the easy implementation comes the disadvantage that the LS method is very much more sensitive to channel noise that can affect the BER because it may interfere and cause the packets received by the photodiode to not be accurate and complete due to excessive noise.
6. Conclusion

In conclusion, by carrying out data transmission via VLC as Li-Fi technology, it is also known based on the research carried out that it is far more secure and reliable compared to traditional Wi-Fi architecture. Thus, we evaluated the security level of Li-Fi compared to Wi-Fi. Wi-Fi is subject to security risks such as data leakage and session hijacking while Li-Fi is highly secure due to the light propagation property that does not allow the light waves to penetrate opaque objects.

We have demonstrated that, within the simulation, Li-Fi has a high data rate with less BER. In addition, Li-Fi uses an unlicensed spectrum of light waves and nearly unlimited bandwidth. These make the Li-Fi technology to accommodate huge number of devices with very high data rate. Finally, we can summarize these Li-Fi security features as simply “shutting the door”.

For future works, to address the major issue of LOS dependence, this issue may be solved by considering reflected light as a replacement of full LOS connection.

References

[1] F. Macdonald, "A new type of light-based WiFi is 100 times faster than the best WiFi we have now," Business Insider, 21 March 2017. [Online]. Available: https://www.businessinsider.com/new-infrared-lifi-is-100-times-faster-than-the-best-wifi-we-have-now-2017-3?IR=T. [Accessed 30 September 2018].
[2] H. Haas and C. Chen, "What is LiFi?," Journal of Lightwave Technology, vol. 34, no. 6, pp. 1533-1544, 2016.
[3] M. L. Pall, "Wi-Fi is an important threat to human health," Environmental Research, vol. 164, pp. 405-416, 2018.
[4] S. Modi, "Lighting up data - Visible Light Communications," 5 September 2018. [Online]. Available: http://blog.echelon.com/echelon_blog/2016/06/lighting-up-data-visible-lightcommunications-vlc-by-sohrab-modi.html
[5] A. Shetty, "A Comparative Study and Analysis on Li-Fi and Wi-Fi," International Journal of Computer Applications, vol. 150, no. 6, pp. 43-48, 2016.
[6] S. &. B. R. Singh, "163m/10Gbps 4QAM-OFDM visible light communication," International Journal of Engineering & Technical Research, vol. 2, no. 2, pp. 225-228, 2014.
[7] H. S. N. T. D. V. S. &. H. H. Burchardt, "VLC: Beyond point-to-point communication," Communications Magazine, IEEE, vol. 52, no. 7, pp. 98-105, 2014.
[8] T. Mekhaznia and A. Zidani, "Wi-Fi Security Analysis," The International Conference on Advanced Wireless, Information, and Communication Technologies, vol. 73, pp. 172-178, 2015.
[9] G. Blinowski, "Security issues in visible light communication systems," in IFAC, Warszawa, Poland, 2015.
[10] S. R. Remya Remesh, "LI-FI in Defense and Security," International journal of current engineering and scientific research, vol. 4, no. 10, pp. 25-31, 2017.
[11] D. Passi, B. Aggarwal and B. S. Rawat, "LI-FI: A New Era Of Wireless Communication Data Sharing," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 3, no. 10, pp. 118-119, 2014.
[12] P. Verma, D. J. Shekhar, P. and D. A. Asthana, "Light-Fidelity (Li-Fi): Transmission of Data through Light of Future Technology," *International Journal of Computer Science and Mobile Computing, vol. 4, no. 9*, pp. 113-124, 2015.

[13] S. Vicky, "LI-FI THE BEST ALTERNATIVE TO OVERCOME THE EXISTING TECHNOLOGIES," *International Journal of Computer Science and Information Technology Research, vol. 2, no. 2*, pp. 208-212, 2014.

[14] M. Y. A. A. A. N. O. Yaseein Soubhi Hussein, "Expectation-maximization-based channel estimation algorithm for OFDM visible light communication systems," *International Journal of Engineering & Technology, vol. 7, no. 4*, pp. 2638-2645, 2018.

[15] ShareTechnote, "Communication - Channel Estimation," 2014. [Online]. Available: http://www.sharetechnote.com/html/Communication_ChannelEstimation.html. [Accessed 10 October 2018].

[16] V. K. Batav and B. Chourasiya, "Channel Estimation in OFDM Mobile Wireless Channel Using Pilot Sequences," *International Journal of Engineering Trends and Technology, vol. 4, no. 3*, pp. 489-492, 2013.

[17] M. Y. A. A. A. Yaseein Soubhi Hussein, "On Performance Analysis of LS and MMSE for Channel Estimation in VLC Systems," in *IEEE 12th International Colloquium on Signal Processing & its Applications*, Melaka, Malaysia, 2016.

[18] M. Zamanighomi, Z. Wang, K. Slavakis and G. B. Giannakis, "Linear minimum mean-square error estimation based on high-dimensional data with missing values," in *48th Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, USA, 2014.

[19] Y. S. Hussein, M. Y. Alias and A. A. Abdulkafi, "On Performance Analysis of LS and MMSE for Channel Estimation in VLC Systems," Melaka, 2016.

[20] A. A. Abdulkafi, M. Y. Alias, Y. S. Hussein, N. Omar and M. K. B. Salleh, "PAPR Reduction of DC Biased Optical OFDM using Combined Clipping and PTS Techniques," Johor Bahru, 2017.

[21] C. Robbins, "Li-Fi Security," CYBER MATTERS, 10 January 2017. [Online]. Available: https://cybermatters.info/2017/01/10/li-fi-security/. [Accessed 24 October 2018].

[22] Private Tunnel, "Benefits And Future Security Concerns Of Li-Fi Networks," OpenVPN, 15 November 2016. [Online]. Available: https://www.privatetunnel.com/news/lowfinetworks/. [Accessed 24 October 2018].

[23] T. Scargill, "Is LiFi the Future of Secure Networks?," Secure World, 11 September 2017. [Online]. Available: https://www.secureworldexpo.com/industry-news/is-lifi-the-future-of-secure-networks. [Accessed 24 October 2018].

[24] A. Shetty, "A Comparative Study and Analysis on Li-Fi and Wi-Fi," *International Journal of Computer Applications, vol. 150, no. 6*, pp. 43-48, 2016.

[25] G. Blinowski, "The feasibility of launching physical layer attacks in visible light communication networks," Institute of Computer Science, Warsaw University of Technology, Warszawa, Poland, 2016.

[26] R. R. Sharma, R. and A. Sanganal, "Li-Fi Technology Transmission of data through light," *International Journal of Computer Technology & Applications, vol. 5, no. 1*, pp. 150-154, 2014.

[27] F. Aftab, "Potentials and Challenges of Light Fidelity Based Indoor Communication System," *International Journal of New Computer Architectures and their Applications, vol. 6, no. 3*, pp. 92-102, 2016.
