Utilizing Li-fi as a More Secure Tool to Access the Internet

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Jaden Carroll

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Rosanne Vrugtman, Department of Computer Science

Utilizing Li-fi as a More Secure Tool to Access the Internet

CS4991 Capstone Report, 2023

Jaden Carroll
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
ujp6ra@virginia.edu

ABSTRACT

With the technological world becoming more and more dependent on the internet, the need for a connection safe from cyberattacks grows. Utilizing the light-based Li-Fi technology as an alternative to radio wave-based Wi-Fi can help to provide consumers with a more secure internet connection. Wi-Fi can be susceptible to outside attackers, so consumers can instead use Li-Fi to connect to the internet without fear of outside attackers stealing their information. However, the range of connection is limited with Li-Fi. There are also issues of outside interference because of outside light such as light that interferes with the Li-Fi's light waves. Although Li-Fi is not yet ready for large-scale implementations, there is great optimism for Li-Fi to soon serve as a more secure alternative to Wi-Fi. In the meantime, Li-Fi can support environments that are vulnerable to electromagnetic interference such as airplane cabins and hospitals.

1. INTRODUCTION

Wireless Fidelity or Wi-Fi has been around since 1997 when it was first made available to consumers. Over the years it has since been established as an integral part of the internet network giving users around the world the ability to connect to the internet. Every day, approximately half a million new users access the internet across the globe. In order to support the tremendous number of internet users, Wi-Fi uses radio frequencies (RF) to transmit data between our devices and wireless routers to grant access to the internet. Wi-Fi routers make use of these RF waves to provide consumers with a long range of connectivity to different networks.

The problem with Wi-Fi lies in these radio frequencies as radio waves can pass through walls which creates a security risk as attackers can easily intercept sensitive data from users. Cybercriminals often utilize man-in-the-middle attacks to target Wi-Fi users as they pose as an anonymous proxy that can eavesdrop and intercept information communicated between users and the internet.

One emerging solution to this security issue is the use of Light Fidelity or Li-Fi which utilizes visible light communication (VLC) to broadcast its signal. As Bao, et. al. (2015) described it: "VLC not only provides indoor illumination but also offers broadband connectivity by modulating information onto the intensity of the light." This works by having ordinary light-emitting diodes (LED) serve as signal transmitters where they send binary data to photo-diodes that act as signal receivers. The LED bulbs themselves serve as an access point for network-connected devices that are in the bulb's illuminated range.

This improves the overall security of the network as outsiders of a specified location cannot interfere with or intercept the data passed in the network, as VLC cannot pass through opaque walls. An emerging technology like Li-Fi and its applications offer great potential, as well as some possible drawbacks.

2. RELATED WORKS

Association attacks are a major vulnerability in modern network applications allowing hackers to trick users into connecting to a rogue Wi-Fi access point. Chatzisofroniou and Kotzanikolaou (2022) discuss this kind of attack in depth, describing how cyberattackers often target public vendors like a coffee shop or a library where free, public Wi-Fi is often provided. These vendors will often sacrifice the security of their network for usability for their customers, but this creates vulnerabilities to man-in-the-middle attacks like the association attack. The attacker needs to be within the signal of the network in order to set up their rogue one. This is not a big inconvenience, as Wi-Fi signals can pass through walls into nearby buildings. The attacker then broadcasts their seemingly identical yet stronger signal to trick users into using their malevolent access point.

When a client connects to a rogue access point, the attacker can monitor all the data sent and retrieved by these devices, which threatens the data security and privacy of the public. There are some existing solutions to such attacks such as the application of network data encryption. He, et al. (2021) explains the process of converting plaintext data into ciphertext, which is incredibly difficult for attackers to decrypt. They discuss types of encryption algorithms such as link encryption, node encryption, and end-to-end encryption which encrypt and decrypt information passed over networks like Wi-Fi to protect the data of internet users. The results of applying different encryption algorithms such as these improve by as much as 40% the cybersecurity index, which measures the risk a particular technology has to outside cyberattacks.

Although security measures such as these data encryption algorithms do help protect the customer, they are expensive to manage and maintain as the process of encrypting and decrypting can use a lot of unnecessary computing resources. This is why an emerging technology such as Li-Fi has so much potential, as it can prevent attackers outside a location from taking over a network. Data encryption is an important process but it can be costly, and Li-Fi can serve as an alternative internet access point for clients.

3. PROPOSED DESIGN

Wi-Fi or Wireless Fidelity has long been the standard technology used to connect billions of devices around the world. Wi-Fi uses radio waves to transfer information back and forth as these light waves easily traverse through the air without any threat to humans.

Li-Fi or Light fidelity is an optical alternative to Wi-Fi that utilizes other waves on the electromagnetic spectrum such as infrared, visible, or ultraviolet light. These waves have a much higher frequency than Wi-Fi’s radio waves which leads to much faster data transmission speeds. Another benefit is the security factor that light cannot travel through walls which prevent data leakage, a common issue of Wi-Fi applications.

Visible Light Communication or VLC is a system that utilizes an overhead light source used for the transmission of different signals. These signals are then detected by photodiodes known as the Li-Fi key, which recognizes the light emitted and converts this data into an electrical signal which can then be processed and converted into binary data which can be easily read by internet devices. Li-Fi makes use of this VLC system as it provides an ideal medium to communicate data between devices. VLC not unlike Wi-Fi allows for the transmission of any type of data whether it is text, audio, or videos.

With Li-Fi utilizing a very complex system such as VLC, it is essential that both the light source and the photodiodes perform their functions optimally. For the light source, VLC requires the source to be constantly turned on and off to represent binary data which is then detected by the Li-Fi key. LED bulbs are ideal for this as they are semiconductors which allows for the bulb to switch on and off at an extremely fast rate. When the bulb is off a 0 is sent to the photodiode, when the bulb is on a 1 is sent which allows for the transmission of binary data. The LED bulb flickering is controlled by a voltage controller and level shifter circuit which work together to alternate the bulb on and off. The constant flickering does not present an issue, as the "light can be traded on and off more rapidly than the human eye can recognize" (Sharma and Bansal, 2016). This allows for the LED light source to serve as both a viable source of illumination and a key mechanism of the VLC system. The LED bulb is usually equipped with a Li-Fi router which allows for the bulb to be connected to the local internet network via an Ethernet cable.

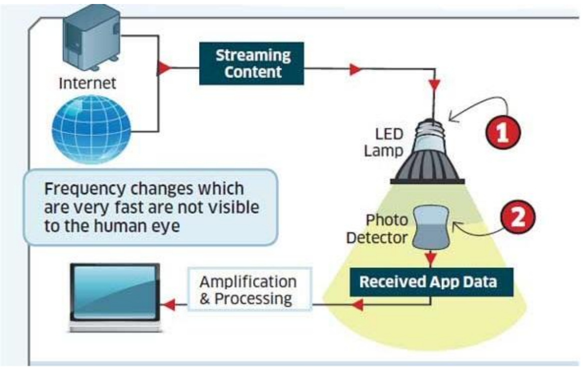
Internet
Streaming Content
LED Lamp
1
Frequency changes which are very fast are not visible to the human eye
Photo Detector
2
Received App Data
Amplification & Processing

Figure 1. Li-Fi Application Diagram
(Sharma and Bansal, 2016)

The above figure demonstrates Li-Fi in action as it utilizes the VLC system to transmit data between the user's device and the internet network. The amplification and processing portion of the diagram is incredibly important as the computer needs to understand and process the electrical signals being sent by the Li-Fi key so that the user can easily access and understand the transmitted data.

4. ANTICIPATED RESULTS

The implementation of a Li-Fi system at any location can bring numerous benefits whether it is increased data transmission speeds or better security. The ability to utilize LED visible light to communicate data between devices can bring data rates of around 1 Gbps. Currently Wi-Fi offers data rates in the range of 150Mbps to 2 Gbps (Panigrahi, n.d.). Li-Fi in a stage of infancy already performs extremely well when compared to the Wi-Fi speeds which shows the promise of the emerging technology. The enhanced security is an important feature of Li-Fi as light cannot penetrate through walls unlike radio waves. There are however certainly situations where this could cause an issue such as in a household with multiple rooms. This has been a huge setback in the development of Li-Fi as companies and families need these data signals to be able to penetrate through walls or dividers. This issue could be resolved with the implementation of multiple LED bulbs but this can be costly and Wi-Fi already solves this problem.

5. CONCLUSION

It is important to consider that the development of Li-Fi is still an ongoing process as these reliability issues need to be addressed before becoming a viable option. Today, Li-Fi can be applied in many locations because of its unique features. In environments prone to radio frequency interference such as airplanes, military bases, or even hospitals, Li-Fi can serve as a means to connect to the internet without obstructing any radiofrequency devices or communications. Underwater explorations are another interesting application for Li-Fi as radio waves do not travel well underwater so utilizing VLC can help companies or the military operating underwater. In all, Li-Fi does have its disadvantages but there are so many potential benefits of using this technology to connect to the internet. Li-Fi serves as a promising emerging technology that is continuing to develop to become a viable tool to connect to an internet network.

6. FUTURE WORK

Li-Fi has not yet been deployed on a large scale as it has its aforementioned reliability issues. However, in the near future this technology can be applied to many unique environments. Underwater communication is a notable application where Li-Fi is more reliable than Wi-Fi as radio waves are quickly absorbed by water. Li-Fi can very soon be designed to support environments that are vulnerable to electromagnetic interference such as airplanes and hospitals. These are just a few examples of the next steps in the development of the emerging Li-Fi technology. By implementing and testing Li-Fi in these smaller-scale environments, the technology will improve and become more reliable for future applications.

REFERENCES

Bao, X., Yu, G., Dai, J. & Zhu, X. (2015). Li-Fi: Light fidelity-a survey. Wireless Networks, 21(6), 1879–1889. https://doi.org/10.1007/s11276-015-0889-0

Chatzisofroniou, G., Kotzanikolaou, P., Grob, T. & Viganò, L. (2022). Exploiting WiFi usability features for association attacks in IEEE 802.11: Attack analysis and mitigation controls1. Journal of Computer Security, 30(3), 357–380. https://doi.org/10.3233/JCS-210036

Panigrahi, K. (n.d.). Difference between WiFi and LiFi. Retrieved March 17, 2023, from https://www.tutorialspoint.com/difference-between-wifi-and-lifi

He, Y., Ye, N. & Zhang, R. (2021). Analysis of Data Encryption Algorithms for Telecommunication Network-Computer Network Communication Security. Wireless Communications & Mobile Computing, 1–19. https://doi.org/10.1155/2021/2295130

Oledcomm.net. (2022, May 16). How does LiFI work? https://www.oledcomm.net/how-lifi-works-step-by-step/

Li-Fi is the light-based Wi-Fi alternative of the future | Mobile Fun Blog. (2015, October 13). https://www.mobilefun.co.uk/blog/2015/10/li-fi-is-the-light-based-wi-fi-alternative-of-the-future/

LiFi Speed. (n.d.). LiFi.Co. Retrieved March 16, 2023, from https://lifi.co/lifi-speed/

Nor, A. M. & Mohamed, E. M. (2019). Li-Fi Positioning for Efficient Millimeter Wave Beamforming Training in Indoor Environment. Mobile Networks and Applications, 24(2), 517–531. https://doi.org/10.1007/s11036-018-1154-4

Sharma, S. & Bansal, N. (2016). Li-Fi (Light Fidelity). The Future Technology In Wireless Communication. International Journal of Advanced Research in Computer Science, 7(6), 258–262.

Spamlaws.com. (n.d.) The Pros and Cons of Data Encryption. Retrieved February 24, 2023, from https://www.spamlaws.com/pros_cons_data_encryption.html