International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 03, Issue 03, July 2022
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

A Mini Review of Lifi Technology: Security Issue

1st Erika Ramadhani
[1]Department of informatics Universitas Islam Indonesia
[1]Jl. Kaliurang No.Km. 14,5, Krawitan, Umbulmartani, Ngemplak, Sleman, Yogyakarta
[1]erika@uii.ac.id

Abstract— Visible Light Communication (VLC) is an extension of Light Fidelity (LiFi) that uses full duplex communication or fully networked wireless communication. LiFi is one of the top technologies for solving wireless fidelity (WiFi) issues. Communication over LiFi is one of its major advantages. However, no security system is infallible. The purpose of this paper is to conduct a mini review of LIFI technology in terms of security issues. As a new technology, Lifi is still not widely known for its security issues. Literature reviews are a necessary step to determining the issues related to Lifi technology. A descriptive qualitative approach is used in this paper to describe the data. As a result, several studies have documented security issues related to LiFi technology, including data modification, spoofing, and jamming.

Keywords : LiFi, security issue, attack taxonomy.

I. INTRODUCTION

LiFi is designed to use LED light bulbs similar to those currently used in many energy-conscious homes and offices. However, LiFi lamps are equipped with a chip that modulates the light for optical data transmission. LiFi data is transmitted by LED lights and received by photoreceptors as shown in Fig. 1. LiFi is the application of visible light communication (VLC). A VLC device is a front-end subsystem component that is a part of LiFi, which is developing the network and protocol, interference mitigation and security, MAC protocols, and link-level algorithms [1].

Li-Fi has only been introduced in the last few years. It rose quickly to fame when founder Harald Haas of the University of Edinburgh gave a TEDtalk. Chances are, Li-Fi will fill a gap that Wi-Fi and Bluetooth can't — for use on airplanes or for extra security. But Wi-Fi and Bluetooth are also constantly evolving (Bluetooth 5 and Mesh only came out in 2017), so we still need to continue to see the future of these three technologies, especially for IoT implementations.

One of the advantage of Li-Fi is that it is more secure because data cannot be intercepted without a clear line of sight (LOS conditions, line of sight). It also does not interfere with sensitive electronics, making it better for use in environments such as hospitals and airplanes.

Lifi technology is said to have a better system when compared to Wifi. However, no security system is infallible. In this paper we study about the issue in security that possible occur in the LiFi. This study according to the VLC technology that still relate to the LiFi technology[2]. Our research is a review of the existing threat and vulnerabilities. To collect the data of a security issue in LiFi, we search through the paper research with a focus on LiFi and VLC. A descriptive qualitative approach is used in this paper to describe the data.

According to paper [3], VLC has three type of attack that may exist in the indoor communication, i.e. data modification, spoofing, and jamming. We gain a comprehensive view to study the information about vulnerabilities that relate to VLC.

II. LIFI TECHNOLOGY

LiFi is the extend concept of visible light communication (VLC). The goal is to achieve high speed, secure, and bi-directional and fully networked wireless communication. The difference between LiFi and VLC is the principle of communication. LiFi can be describe as a complete wireless network system which communication in Lifi is point-to multipoint and multipoint to point communication. While VLC is a point-to point data communication. LiFi consisting multiple access point that act as a wireless network with using the small optical attocells that has a seamless handover[4][5]. The key different between LiFi and VLC is the method of modulation. This LiFi will be the next generation of wireless communication called 5G[6].

The architecture of LiFi is based on layers. It is consist of three layer i.e. (1) application layer, (2) MAC layer, and (3) Physical layer. According to IEEE 802.15.7, LiFi define in two layer: physical layer and

International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 03, Issue 03, July 2022
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

MAC layer[7][8].

In the optical wireless communication (OWC), the architecture of LiFi consist of block transmission, i.e. transmitter and receiver. The transmitter is a digital signal processing (DSP) block and a LED optic, while in the receiver is a filter, photodetector, and transimpedance amplifier (TIA)[9].

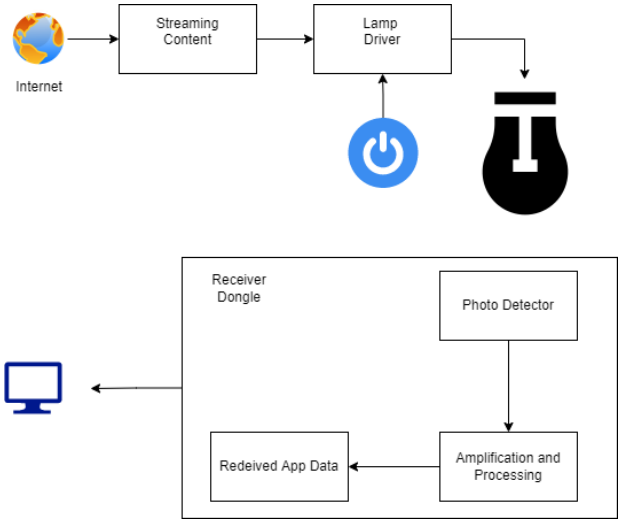

Figure 1. LiFi system[6]

Overall LiFi system is depicted in the figure 1. It is consist of Lamp driver and LED as a transmitter and photodetector as a receiver. The data will transmit through a LED lamp, and photo detector will detect the variations of LED light then convert to electrical signal. Computer will receive the data after it is processed, amplified, and converted back to its original format.

III. SECURITY ISSUE

In this stage, we determine several kind of attack in LiFi system. This section list the example of attack according to study literature obtained from previous research paper from journal and conference related to security and attack system. The attack of LiFi is according to OWC that relate to VLC system.

Paper [10] describe the feasibility of physical layer attacks in VLC system. The downlink communication infrastructure is the main aspect in the security that carefully provided. Data snooping, jamming, and modification is the form of attack that may occur in the VLC system. It is also examine that physical layer also has possible disruptions caused by rouge transmission scenario. This attack may occur in the office environment. The result of the paper is the attack is easy to disrupt, and there are some cases hijack legitimate transmission.

According to paper [11] another attack may occur in VLC system, i.e. eavesdropping. The simulation of the attack is by utilize null-steering and artificial noise to achieve positive secrecy rates when the eavesdropper's channel states information (CSI) is known and entirely unknown to the transmitter. This type of attack depicted in Fig. 2 which is Eve is an eavesdropper, Alice is the sender, and Bob is the receiver. Both Alice and Bob has one transmitter and one receiver. The jammer equipped with multiple light sources.

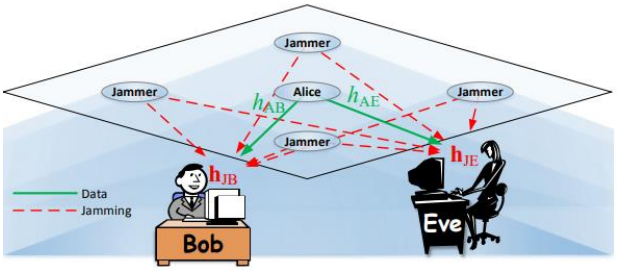

Figure 2. Attack in VLC communication[11][12]

The possibilities eavesdropping in LiFi system is experimented and analyze in paper [13]. The experiment by designing a testbed using software defines radios (SDRs) and evaluate different scenario. The finding is a small gap under a door, keyholes, and windows possible for an eavesdropper.

Friendly jamming is the type of attack in the VLC communication. The paper [14] said that friendly jamming has multiple light source but does not have the access to the data transmitted. The type of this jamming may cause degradation of the system performance. It can cause a new issue in the availability of the system. The example of another jamming type is reactive jamming, with its objective is to disturb the synchronization of the packet at the receiver[15].

Sniffing attack also possible become an attack in the VLC system, if it exploited more complex, the attack may occur as a spoofing and Man-in-the-Middle (MITM) attack[16]. Fig.3.a. is the attack scenario, consist of Alice as an emitter sending the data to a receiver (Bob). Any other receiver located under Alice area of illumination, Eve may receives the signal and sniff the messages. The scattering surfaces in an indoor communication is in Fig. 3.b. which is Eve or the attacker should be outside the area of communication, this condition also can make Eve sniff the information. Fig.3.c. the location of the attacker in the outside of covered by Alice's emission such as in a room corner or outside room. By this way, Eve may receive enough signal to sniff the information. According to the Fig.3,

International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 03, Issue 03, July 2022
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

it can be concluded that Eve is a passive device who receives the VLC transmission and does not interact with it. This type of scenario make a possibility that promiscuous devices not only sniff but interact with the VLC network.

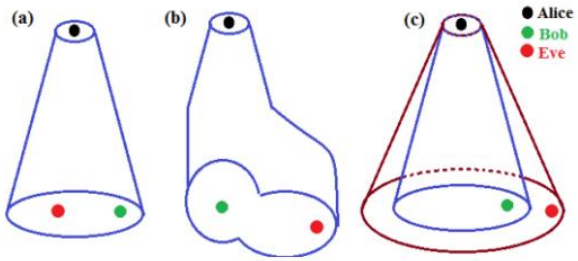

Figure 3. Sniffing attack scenario[16]

Sniffing over the VLC channel is viable attack by power gaining techniques. It is prove by using the cost-affordable devices suggests the sniffing techniques could be an actual threat. Another attack may exist in LiFi communication is data modification. Data modification attack is the result of the summary between risk of jamming and snooping[3] while snooping refers to listening to a conversation.

IV. TAXONOMY OF THE ATTACK

In this stage we present the taxonomy of attack that may occur in LiFi system. This objective is to organize all the possibilities of the attack. The model that we use is according to [17]. The attack classified by order and by phase. The order classification based on the type of the attack, while phase classification is in which part of the sequence of event that attack take place.

Table 1. Classification by order

Order	Attack Name
Physical Attacks	Rouge access point, jamming
Passive Attacks	Snooping, Sniffing, eavesdropping
Active Attacks	Man-in-the-Middle
DoS/DDoS Attacks	Authentication flood
Cracking Attacks	Pre-shared Key Cracking

Table 1 shows the classification of attack by in order physical, passive, active, DDoS, and cracking. The classification by phase can be seen in the Fig. 4. It describe the classification by the phase of the intrusion which the attack are reconnaissance, denial, and exploitation phase.

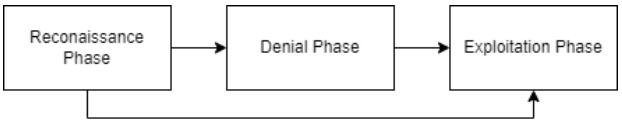

Figure 4. Attack classification by phase

In the reconnaissance phase, the objective of this work is to observes and examines the target network in order to find out the network's configuration and if an encryption scheme is used. This attack also called as the first tried. The case of this phase is eavesdropping and jamming.

Denial phase is to use the network to single or multiple user in order to gain access to such a network. The case of this stage is authentication flood. Last, the exploitation phase is the attacker exploits vulnerabilities of the system. The case in this stage is MITM attack. the summarize of the Fig.4 can be break down in the list of Table 2.

Table 2. Classification by phase

Intrusion Phase	Attack Name
Reconnaissance Attacks	Eavesdropping, snooping
Denial Attacks	Sniffing
Exploitation Attacks	Man-in-the-Middle

3.1 Attack relationship

In this section, we summarize the relationship of the attack. One attacks may create to another attack by associating the relationship. The relationship is according to the goal of the attack, such as data modification, DoS/DDoS, packet loss and synchronization fails. The relationship of the attack is depicted in Fig.5.

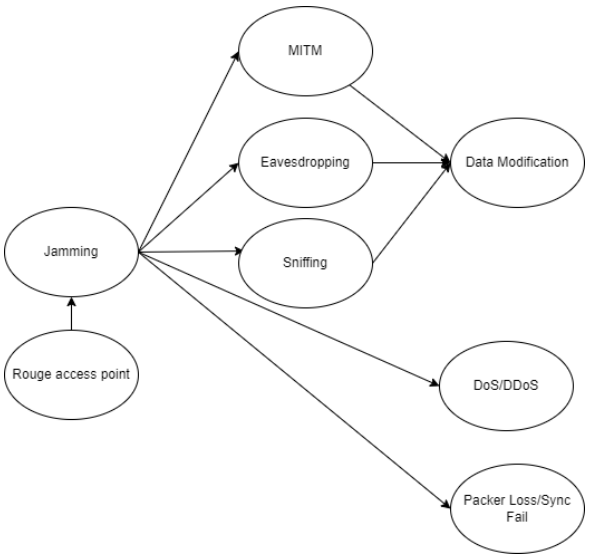

Figure 5. Attack relationship

V. CONCLUSION

The result of this paper is a taxonomy and the relationships between attacks. According to the literature review, the three issue that may exist in the LiFi communication are jamming, snooping, and data modification. Therefore, the three issue may cause another attack in LiFi communication that related, for example, data modification attack may occur from the leading attack of the snooping and jamming attack.

REFERENCES

[1] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?," *J. Light. Technol.*, vol. 34, pp. 1533–1544, 2016, doi: 10.1109/JLT.2015.2510021.

[2] D. Tsonev, S. Videv, and H. Haas, "Light Fidelity (Li-Fi): Towards All-Optical Networking", Accessed: Feb. 02, 2018. [Online]. Available: http://www.homepages.ed.ac.uk/hxh/Li-Fi_PAPERS/14_optical_attocells.pdf

[3] G. J. Blinowski, "Practical Aspects of Physical and MAC Layer Security in Visible Light Communication Systems," *Int. J. Electron. Telecommun.*, 2016, doi: 10.1515/eletel-2016-0001.

[4] H. Haas, "LiFi is a paradigm-shifting 5G technology," *Rev. Phys.*, vol. 3, pp. 26–31, Nov. 2018, doi: 10.1016/J.REVIP.2017.10.001.

[5] L. U. Khan, "Visible light communication: Applications, architecture, standardization and research challenges," *Digit. Commun. Networks*, vol. 3, no. 2, pp. 78–88, 2016, doi: 10.1016/j.dcan.2016.07.004.

[6] S. Alfattani, "Review of LiFi Technology and Its Future Applications," *J. Opt. Commun.*, vol. 42, Jun. 2018, doi: 10.1515/joc-2018-0025.

[7] Latif, U. Khan, V. Leds, L.-F. Ook, and P. P. Csk, "Visible light communication_ applications, architecture, standardization and research challenges," 2017, doi: 10.1016/j.dcan.2016.07.004.

[8] R. George, S. Vaidyanathan, A. S. Rajput, and K. Deepa, "LiFi for Vehicle to Vehicle Communication - A Review," *Procedia Comput. Sci.*, vol. 165, pp. 25–31, 2019, doi: 10.1016/J.PROCS.2020.01.066.

[9] S. Dimitrov and H. Haas, "Principles of LED Light Communications Towards Networked Li-Fi", Accessed: Feb. 12, 2018. [Online]. Available: http://aksitha.com/Future Technology/Principles of LED Light Communications Towards Networked Li-Fi - Svilen Dimitrov, Harald Haas - 2015.pdf

[10] G. Blinowski, "The feasibility of launching physical layer attacks in visible light communication networks", Accessed: Feb. 13, 2018. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1608/1608.07146.pdf

[11] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *2014 IEEE International Conference on Communications (ICC)*, Jun. 2014, pp. 3342–3347. doi: 10.1109/ICC.2014.6883837.

[12] J. Classen, D. Steinmetzer, and M. Hollick, "Opportunities and Pitfalls in Securing Visible Light Communication on the Physical Layer," in *Proceedings of the 3rd Workshop on Visible Light Communication Systems*, 2016, pp. 19–24. doi: 10.1145/2981548.2981551.

[13] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications", doi: 10.1145/2801073.2801075.

[14] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *2014 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 524–529. doi: 10.1109/GLOCOMW.2014.7063485.

[15] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, ACCEPTED FOR PUBLICATION Detection of Reactive Jamming in DSSS-based Wireless Communications", doi: 10.1109/TWC.2013.131037.

[16] V. Guerra, J. Rabadan, L. Palmas, and D. G. Canaria, "Data Sniffing Over an Open VLC Channel," pp. 1–6.

[17] S. L. Hansman, "A Taxonomy of Network and Computer Attack Methodologies," 2003. Accessed: May 01, 2022. [Online]. Available: https://ir.canterbury.ac.nz/handle/10092/11201