REVIEW ARTICLE

A SECURITY REVIEW OVER WI-FI AND LI-FI

Rabia, Naveed Ali, Shahzaib Ali, Ahthasham Sajid^{1*}, Afia Zafar²

¹Department of Computer Science, Faculty of ICT, BUITEMS Quetta, Pakistan.

²Department of Computer Science, NUTECH, Islamabad

*Corresponding Author Email: ahthasham.sajid@buitms.edu.pk, gullje2008@hotmail.com

This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article History:

Received 10 February 2020

Accepted 16 March 2020

Available online 06 April 2020

ABSTRACT

Wi-Fi and Li-Fi are two modern era technologies that are used for data communication. Wi-Fi stands for Wireless Fidelity and Li-Fi stands for Light Fidelity. Wi-Fi uses radio frequency (RF) waves to for transmission of data, on the other hand Li-Fi uses light signals or visible light for data communication. Li-Fi provides transmission of data through illumination by sending data through an LED light bulb. Wi-Fi and Li-Fi technology is used in the various applications of daily life. Both the technologies differ in their properties, architecture, and working. Li-Fi is based on the IEEE 802.11ad standard and uses VLC for data communication while Wi-Fi uses the IEEE standard 802.11 on different devices like routers to transmit data. The objective of this research work is to highlight security prospective of these both technologies; various attacks which can occur and their counter measure as well as misconceptions related to both Wi-Fi vs. Li-Fi is presented in this research paper. Wi-Fi is widely implemented in many major and minor fields of life and the capacity it is providing is accessed. Li-Fi, on the end hand, is a means of an opportunity to further develop the efficiency and use of data and to provide resources that are required for the future needs.

KEYWORDS

WI-FI (wireless fidelity), LI-FI (light fidelity), photodiode, VLC (visible light communication).

1. INTRODUCTION

Wi-Fi (wireless fidelity) and Li-Fi (light fidelity) are at two types of wireless technologies i.e. data is wirelessly transmitted in these technologies. The components of Wi-Fi include Routers, and it works on Radio Frequency (RF) waves to for communication, where Li-Fi uses LED bulbs and Visible Light Communication (VLC) light signals for communicating wirelessly (Shetty, 2016). The IEEE 802.11 standard and specifications forms the basis of Wi-Fi technology and IEEE 802.11ad is the standard for Li-Fi. Wi-Fi and Li-Fi are vital aspects of today's wireless technologies and Li-Fi being termed the future wireless technology. The importance of these technologies in everyday life cannot be stressed enough. A lot of advancements are yet to come to the technology of Wi-Fi whereas Li-Fi technology is yet to make its mark on the current technological world. Both the technologies have a lot of possibilities which can be further studied and explored. Micron sized LED with flicker rates 1000 times quicker than current large LEDs are being developed by the researchers. They offer better and faster data transfer in addition to consuming not a lot of space. The wireless communication can further enhance if Li-Fi technology is implemented on these LEDs. Li-Fi being more efficient and more advanced technology than Wi-Fi is set to replace the current applications of Wi-Fi and to make new innovations for the betterment and more luxury of human life.

There are three bands that are used interchangeably, and frequency change is also frequent in Wi-Fi. There are 12 channels that is used to split and compensate for the bandwidth usage (Kulkarni et al., 2016). Wi-Fi technologies is limited to these channels for communication of data. A

method of frequency hopping is used which provides interference free communication (Shetty, 2016). Data rates provided by Li-Fi can be up to 10 Gbps and more. The Micro LEDs can transmit more than 3 Gbps speed per LED (Julka et al., 2015). RF has 300 GHz frequency band whereas Li-Fi, which uses the visible light communication, has a frequency band of 300 THz meaning more space for data transmission (Kulkarni et al., 2016). HD movies can be downloaded in time as less than 30 seconds using Li-Fi based data connections (Kumar et al., 2017). This technology can also be used in sensitive areas and places like hospitals, power plants and aircrafts as visible light has no radiation problems like RF waves have (Kulkarni et al., 2016). The future of devices particularly handheld and mobile devices like laptops, mobile phones etc. are all predicted to be used with Li-Fi. The security measure of Li-Fi is also safer than that of Wi-Fi as data cannot go through walls and can only be accessed on the visible range of light (Monisha et al., 2017).

2. COMPARISON OF WI-FI AND LI-FI

Wi-Fi or wireless fidelity use multiple frequencies and bands to get high data rates in order to facilitate the people and devices connected to it (Leba et al., 2017). Wi-Fi can support multiple users at a given time, a single AP (Access Point) can connect and provide internet access to as many as 30 users and the range it can offer varies around 100-150 feet in indoor environments and around 300 feet in outdoor environments.

IEEE 802.11ad standards on the Wireless Local Area Network (WLAN) are being implemented to facilitate the local people and electronic devices, which are all based on Visible Light Communication (VLC) technology (Mosaif et al., 2017).

Quick Response Code

Access this article online

Website:
www.theimcs.org

DOI:
[10.26480/imcs.01.2020.01.09](http://doi.org/10.26480/imcs.01.2020.01.09)

The data communication done in Li-Fi based technologies are of dual nature with being dependent of the light intensity (Kulkarni et al., 2016). At present, both the technologies are used for connecting to the internet for wireless data communication. Both technologies have their advantages and drawbacks, and Li-Fi can be used to remove some of the drawbacks of Wi-Fi (Sebbar et al., 2016).

Li-Fi is like Wi-Fi with the difference of components used like LED bulbs and photograph detectors, and operates on visible light as compared to routers, modems, and radio waves (Sebbar et al., 2016). Wi-Fi and Li-Fi are compared in the given table below.

Table 1: Wi-Fi and Li-Fi Comparison		
Criteria	Li-Fi	W-Fi
Medium of data transfer	Visible light spectrum is used in Li-Fi	Radio Frequency spectrum is used in Wi-Fi
Technology	WLAN IEEE 802.11ad standard	WLAN IEEE 802.11 standard
Transfer Rate	Ranges about 10 Gbps and more	Ranges about 150 Mbps
Security	Signals cannot pass through walls meaning more security than Wi-Fi	Signals can pass through walls and data can be compromised by attackers meaning less than Li-Fi
Frequency	300 THz	2.4 GHz
Working Range	About 10 meters and LoS based	Ranges from 30 to 45 meters indoors and up to 90 meters outdoors
Network Topology	Point-to-point topology	Point-to-point topology
Components	LED bulb, light emitting diodes, photograph detector	Router, modem and passages
Cost	Cheaper than Wi-Fi as it uses light and components like LED bulbs	Costlier than Li-Fi and it uses Radio spectrum and components like routers

2.1 Advantages of Wi-Fi

Wi-Fi is easier to use and it can be used in places like at home, at office, at school, and other public areas. Internet and web can be accessed without the need to connect wires to the computer or other connecting device. Wi-Fi provide easy interacting with the world wide web and various and numerous contents and operations like songs, videos, send messages, have video talks, web based shopping, watch motion pictures, search for online information about studies or works. No extra wires or devices are needed when multiple users connect simultaneously. Administration access can also be provided easily through Wi-Fi than going the tedious procedure of setting connections through wires (Kuppusamy et al., 2016).

2.2 Limitations/Disadvantages of Wi-Fi

Wi-Fi radio waves which are used as a transmission medium has limited bandwidth and frequency bands are crowded resulting in poor connections and more cost of use. As the number of mobile and other technologies are increasing the capacity of Wi-Fi is not able to meet the increasing demands (Julka et al., 2015). There are around 1.4 million cellular radio stations worldwide that are used for Wi-Fi and telecommunications and these stations are not energy efficient meaning they are using more energy (Kumar et al., 2017). The cooling of base stations consumes most of the energy, rather than transmitting data signals. The factual figure of the efficiency of these stations is only at 5% (Swetha et al., 2018). A major issue is the availability of radio waves. For example, Wi-Fi cannot be used in places like airplanes and hospitals operation theatres. Radio waves and signals can pass through walls and

dividers making it possible for possible theft of data and information by unauthorized people.

2.3 Advantages of Li-Fi

Li-Fi uses LEDs and diodes to send and receive data by using the visible light spectrum which also gives fast communications. Li-Fi can be used to better work in the limitations of the Wi-Fi. It has 10 times more bandwidth than Wi-Fi resulting in more number of devices to be connected and also is available to Wi-Fi restricted places like aircrafts, hospitals and other areas like power plants (Swetha et al., 2018). The data rates and efficiency is also higher because Li-Fi uses illumination devices like LEDs to transmit data and they are highly energy efficient. Li-Fi is a more secured network as the signals cannot pass through walls making it safer for data and information (Mishra et al., 2018).

2.4 Limitations/Disadvantages of Li-Fi

The characteristic that light cannot pass through walls also generates a limitation of range. Establishing VLC systems are expensive for using Li-Fi (Monisha et al., 2017). Other sources of light like sunlight, bulbs other than LEDs and dark objects can cause the data transmitting light to get blocked. Li-Fi as a LoS technology can only work in the range of light.

3. ARCHITECTURE AND WORKING

The architecture of the technologies of Wi-Fi and Li-fi are not much different from one another. The working is also based on a general functioning of wireless technologies.

3.1 Architecture of Li-Fi

Li-Fi architecture is basically composed of some wireless devices like laptops, mobile, servers, internet and the main components are LED bulbs and lamps which are the source of communication and accessing of data in Li-Fi technology (Swetha et al., 2018).

- While executing Li-Fi we shall make sure that it has light availability
- line of sight
- Fluorescent light and LED
- A photo detector (Julka et al., 2015)

Figure 1: Basic architecture of Li-Fi system

Basic architecture of Li-Fi is being described in the diagram below where LED (light emitting diodes) bulbs and lamp are connected with server and internet and it is providing internet to laptops and other computers (Swetha et al., 2018).

The Li-Fi system is basically composed of four sub-assemblies (Shetty et al., 2016).

- Bulb
- RF Power Amplifier Circuit (PA)
- Printed Circuit Board (PCB)
- Enclosure

Figure 2: LI-FI sub-assembly

3.2 Working Principle of Li-Fi

LI-FI is basically a secure, cheap and fast source of communication, which can transmit data up to 10 meters and which works on the principle of transmitting data through light wave. It uses VLC and it uses optical spectrum of electromagnetic spectrum instead of radio waves ranging from 400THz and 800 THz for data carrier (Julka et al., 2015).

It transmits data by high speed ON and OFF of light signals which is not visible to human eyesight. VLC uses LED's to transmit data and it is too fast as one LED can transmit data faster than 3Gbps and uses photo diodes to receive those fast signals from LED's (Monisha et al., 2017).

Figure 3: Electromagnetic spectrum of light (Monisha et al., 2017)

3.3 Working of Li-Fi

LI-FI system is implemented using LED light at transmitter side which contains controller for converting the data signals to light signals and has a microchip which is typically used to detect the changes in ON and OFF of signals (Swetha et al., 2018).

LED (light emitting diodes) forms a message by a very high speed ON and OFF of signals at different ranges to produce different messages or uses LED's of different colours as blue, green and red which produces signals at different frequency for showing different messages and for transmission of parallel data range of 100 Mbps (Monisha et al., 2017).

Figure 4: Data Transmission (Swetha et al., 2018)

On receiving site, it has photo detector which is used to convert light signals to data again by detecting the signals. It detects 1 of binary when the LED light is ON and 0 of binary when the LED light is OFF (Swetha et al., 2018).

Basically the LED's are working as encoder and photo detector are working decoder.

Figure 5: LI-FI sub-system (Shetty, 2016)

3.4 Architecture of Wi-Fi

Wi-Fi architecture is basically composed of antenna, routers, laptops, mobiles, servers and PC's (Haas, 2016). It uses radio signals as mean of data transmission which ranges less than visible light spectrum. It can transfer data at speed of 150 Mbps (Shetty, 2016).

Figure 6: Wi-Fi system (Shetty, 2016)

It uses IEEE standard 802.11 for transmission of data and it has different types:

- 802.11
- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac

Standard	802.11b	802.11a	802.11g	802.11n	802.11ac
Theoretical Speed – Up to	11 Mbps	54 Mbps	54 Mbps	300 Mbps	1 Gbps
Frequency	2.4 GHz	5 GHz	2.4 GHz	2.4 and/or 5 Ghz	5 GHz
Range ft	100 – 150	25-75	100 - 150	~ 230	Not known

Figure 7: Comparison table for Wi-Fi standards

3.5 Working of Wi-Fi

WI-FI uses radio waves as mean of transmitting data, at transmitter side the computer has to have a wireless adapter which encodes data into radio signals to be transmitted through antenna to router which decodes the signals to data and passes it to internet through wired Ethernet connection.

It is double side communication because the data which also comes from the internet and goes to the router to get coded to radio signals and then it is passed to computer's wireless adapter (Kuppusamy et al., 2016).

Figure 8: Working of WI-FI

4. APPLICATIONS

Some of the applications of both Wi-Fi and Li-Fi that are researched and implemented on an experimental level are given below.

4.1 Human Identification System

In every home, office, shop, restaurant and other places in the city wireless devices like phones, laptops, tablets etc. can be found. Wi-Fi makes use of Radio Frequency (RF) signals and every wireless device is connected to Wi-Fi. When a person walks through the spaces created by these RF signals, they create a disturbance in this field. Basic human activities such as standing, sitting, walking and running can be observed by studying these disturbance (Zhang et al., 2016).

Wi-Fi signals can be used to make an identification of individual by using every individual's unique walking style. As these patterns (repetitive walking style) are unique they make unique disturbance in the Wi-Fi spectrum (Zhang et al., 2016).

A proposed system can be used to analyze the channel state information of Wi-Fi signals and extract the characteristics of an individual's unique walking style and thus resulting in the identification of that specific person (Zhang et al., 2016).

Figure 9: Operational scenario of the identification system

4.2 Indoor Wireless Visual Sensor Network

Wireless Visual Sensor Networks (WVSNs) are a network of visual nodes that can capture a large amount of image/video information. They are capable of collecting, processing and transmitting this information. The nodes are powered by batteries and are used in cameras (Mosaif et al., 2017).

Li-Fi technology can be used to further increase the efficiency of these WVSNs. Low energy consumption, high speed data transmission, high security, and higher quality of visuals can be achieved by the implementation of Li-Fi (Mosaif et al., 2017). Li-Fi can be used to more efficiently transmit and receive image/video data in an indoor wireless visual sensor network.

Figure 10: Li-Fi based WWSN

4.3 Navigation System

Radio waves (used by Wi-Fi) is over-crowded and overused as the number of people and devices has increased. Whereas on the other hand, Li-Fi uses light waves which has large frequency bandwidth and is largely unused as compared to the radio waves (Mishra et al., 2018).

Li-Fi technology can be used to aide in the navigation of roads in the city and towns to the overused navigation system using radio waves. Street lights integrated with the Li-Fi technology can be used to display a map of the area in the display screen of mobile phones or display screens of a vehicle (Mishra et al., 2018). The present day navigation system can improve significantly by the use of Li-Fi technology based navigation system.

Figure 11: Smart navigation system

4.3.1 Other applications of Li-Fi include:

Medical Technologies: Wi-Fi causes interference with the monitoring equipment of an operating room and due to the radiation the use of Wi-Fi is restricted. Using Wi-Fi in hospitals may have hazardous effects to the patient's health (Swetha et al., 2018). The operating rooms are illuminated with numerous lights and Li-Fi (being eco-friendly) can be implemented to solve these problems of radiation and accessing of internet and can also be used to make use of automated procedures (Shetty, 2016; Monisaha et al., 2017).

Figure 12: Lights inside an operating room

Underwater Communication: Underwater ROVs (Remotely Operated Vehicles) are attached with large cables to get power and receive signals from pilots above. Their limitation is the length of their tethers which restricts their movement (Shetty, 2016). Their wires could be replaced with light, for example from an underwater high water lamp, which would enable them to roam more freely, also communicate with one another and periodically sending data to the surface (Julka et al., 2015). Wi-Fi technologies fails completely underwater whereas Li-Fi has a lot of potential uses (Monisaha et al., 2017).

Figure 13: Underwater communication

Smarter Air Travel: Due to radio waves, Wi-Fi is prohibited in aircraft since the entire airways communication makes use of radio waves (Swetha et al., 2018). Every passenger can have access to fast internet using Li-Fi implemented on light sources like overhead reading bulbs since the entire airways communication makes use of radio waves and Wi-Fi cannot be used (Shetty, 2016).

Figure 14: Li-Fi potential in an airplane

Safer and Productive Power Plants: Radiation of any sort is hazardous to be used in power plants. Li-Fi can be used to provide communication access to fast inter-connected data systems to monitor things like grid integrity, demand, and core temperature with no drawback of radiation or electromagnetic interference (Shetty, 2016). Li-Fi can be used in petroleum and chemical plants as it does not use radio transmission and other frequencies which are hazardous to these plants (Monisaha et al., 2017).

Figure 15: Lights in a power plant

Smart Cities: Smart cities is an emerging trend in today's world. Li-Fi technology can be used to provide high speed data transmission in the street lights since LED is used (Kuppusamy et al., 2016).

Figure 16: Smart city

Home and Office Applications: Li-Fi technologies can be implemented to aide in commercial areas like a house like in TVs, secure systems, heating and cooling systems, clocks and other appliances to manage energy consumption more intelligently (Leba et al., 2017).

Figure 17: Home and office appliances

Bandwidth and Spectrum Relief: The bandwidth and spectrum of Wi-Fi is inadequate for the ever increasing number of smart devices. Li-Fi uses visible light for communication which means unlimited bandwidth and a wide spectrum (10,000 times the spectrum of Wi-Fi) (Shetty, 2016; Julka et al., 2015).

Figure 18: Bandwidth comparison

Mobile Connectivity: The interconnectivity of smart devices such as laptops, smart phones, and smart TVs can be made more productive and efficient using Li-Fi technology (Julka et al., 2015).

Figure 19: Interconnectivity of devices

Education System: Li-Fi technology can be used to provide educational institutions with access to fast internet (Swetha et al., 2018). These environments are over flooded with the use of Wi-Fi internet, resulting in different speeds to different people whereas Li-Fi can provide a stable and same speed to people in a particular area (Monisaha et al., 2017). Educational institutions and organizations can have features like video conference, digital tutorial downloads and online learning can be done with high speed internet connectivity using this technology (Kuppusamy et al., 2016).

Figure 10: Technology in education

Disaster Management: During a crisis or disaster situations like earthquake or tsunamis Li-Fi can be used more effectively to provide emergency communications to the people especially in dead-zone places like subway stations and tunnels (Monisaha et al., 2017). Li-Fi bulbs can be used to provide street light that can also provide cost-effective high speed internet access in every corner of the street (Kuppusamy et al., 2016). Disaster management can be more effective with the use of Li-Fi technology.

Figure 11: Types of Disasters

Traffic Management: Li-Fi can be used to be integrated as LED lights in the headlights and tail lights of vehicles and traffic lights. Communication can be established between the cars and accidents can be prevented by exchanging information (Kuppusamy et al., 2016). This will result in a more safety of roads and traffic control establishing a smart transport and traffic system (Leba et al., 2017).

Figure 12: Traffic lights

5. SECURITY AND THREATS

Security issues of both Wi-Fi and Li-Fi can have many different factors. Most of these factors depend upon the security measures taken by the system itself. An attacker can use the vulnerabilities of the system to their advantage, they can passively listen or capture packets or have a more

active part like manipulating packets. Wi-Fi technology is comparatively older than Li-Fi technology, and the amount of threats and vulnerabilities is also more and complex (Kuppusamy et al., 2016). Li-Fi does not have a complex architecture and yet is not accessible to the general public, thus making the security threats associated with it far less than that of Wi-Fi. The more detailed a system becomes, the harder it is for cybersecurity to cover all the flaws. Thus, creating more opportunities for attacks to hit their targets (Wen et al., 2018).

5.1 Li-Fi Security

Li-Fi is visible light communication meaning the signals cannot pass through walls (Leba et al., 2017). This feature is quite useful from a security perspective. Packets or data, like in Wi-Fi, is in no danger of being leaked outside the room, or buildings, or other public spaces. Some rooms could even be designated as high-security areas with their own Li-Fi networks, making them apart from other areas of the building and minimizing or terminating the possible harmful IoT devices (Julka et al., 2015).

In addition to that, the partition of access points can be made more precise and secure as the visible light from any Li-Fi device is limited (up to about 10m²) (Monisaha et al., 2017). Monitoring of activities performed by the legitimate users will be more effective with factors like assigning simple username/password and a physical space or location. An extra layer of security can also be supplemented by localizing every mobile device and continuously tracking the localized device between different access points (Leba et al., 2017). The users will be required to connect their respective area access point when they move from the previous AP.

5.2 Wi-Fi Security

Wi-Fi uses three main algorithms for its security: WEP, WPA, and WPA2. The initial standards of the IEEE 802.11 utilized an encryption algorithm which provided minimum security and was known as Wired Equivalent Privacy (WEP). WEP was the first security algorithm, deemed broken nowadays, was used in 802.11b standard in 1999. WPA and WPA2 were introduced in 2003 and 2004, respectively and they were used in 802.11i standard with higher and better security measures than that of WEP (Sebbar et al., 2016; Wen et al., 2018). Most modern devices use WPA2 as the default encryption algorithm. Today, both the WPA and WPA2 protocols, as advanced as they are, have some vulnerability, which can be exploited by attackers get authentication to the network, to sniff packets, and, in some cases, to insert packets into the bit stream or decrypt and manipulate traffic (Sagers et al., 2015). Advanced Encryption Standard (AES) encryption is used in WPA2 to secure the network from many of these attacks. Wi-Fi Protected Setup (WPS) is another type of encryption used in many newer devices for making the complex setup process of Wi-Fi easier though it can be cracked and hacked into extremely easily by using brute-force (Sagers et al., 2015). AES is more secure to be used as using WPS actually negates any security advantage given by the utilization of WPA2 (Wen et al., 2018).

According to a study conducted in the city of Rabat, Morocco: The comprehensive majority (77%) of the networks used WPA and WPA2 encryption algorithms (Sebbar et al., 2016). The level of security in the developed cities of the world like London (76%) and Dubai (64%) is not much different than that of Rabat. The remaining 23% of the networks were either using WEP or had no security measures at all. The open networks were 10% and the WEP based networks were 13%. To summarize the people associated with the networks in Rabat had good security knowledge and awareness as they used appropriate security measures.

Figure 13: Wi-Fi encryption use (Sebbar et al., 2016)

5.3 Threats

There are generally two kinds of attacks that are used against protected Wi-Fi networks: Traditional attacks and recent modern attacks.

5.3.1 Traditional Attacks

Traditional attacks are done only for sniffing and injecting packets to a protected network; manipulation of packets is not the purpose in attack type (Vanhoeft et al., 2018). Traditional attacks include: breaking Wired Equivalent Privacy (WEP) to sniff packets without any resistance, breaking Wi-Fi Protected Setup (WPA) is done by interacting with an Access Point (AP), and in case of WPA2 the 4-way handshake is captured passively to launch dictionary attacks (Sagers et al., 2015). Some common attacks are (i) Denial-of-Service (DoS), (ii) Buffer Overflow, and (iii) ARP Cache Poisoning.

5.3.1.1 Denial-of-Service Attack:

A Denial-of-Service (DoS) attack is a common attack with a purpose of shutting down a machine, server, or network, denying the users of the machine, server or network its services. The intended target is flooded with excess of data or traffic that makes the target to crash rendering it inaccessible (Hopper et al., 2016; Wen et al., 2018). In this way, the services promised by the machine or server is unable to be provided to the legitimate users.

Figure 14: Wi-Fi Denial of Service attack

DoS attacks can have major impacts on wireless networks of any organization. Wireless networks can be very vulnerable to DoS attacks and the results can be mild to catastrophic for an organization (Sombatruang et al., 2016; Wen et al., 2018). DoS attack can cause significant damage to a wireless network which can range from degradation of the wireless network to a complete loss of availability of the wireless network within the organization (Sagers et al., 2015).

DoS attacks are of two types: flooding services or crashing services. During Flood attacks excess amount of traffic sent to the system which the targeted is unable to buffer resulting in slowing down and eventually stopping of the system (Hopper et al., 2016). A popular flood attack is buffer overflow attack.

- Buffer Overflow Attacks – the most common DoS attack. In his attack, the network is flooded with data or traffic resulting the buffer to overflow as it is not programmed and meant to store large excess of traffic. The common consequence of this attack is a system or network crash, or in a worst case scenario it can lead to an entry point for a hacker or cyberattack (Hopper et al., 2016).

5.3.2 Modern Attacks:

Modern Attacks makes use of MitM position; MitM is a person between the user and AP. The purpose of these attacks is to actively manipulate data and traffic in addition to the common sniffing and injection of packets (Wen et al., 2018). These modern attacks use MitM to launch certain attacks against WPA-TKIP encryption algorithms and also against the 4-way handshake used in the security algorithms of WPA2 like most key reinstallation attacks (Vanhoeft et al., 2018).

5.3.2.1 Multi-Channel MitM Attacks:

Multi-channel MitM attack is done to reliably monitor as well as

manipulate traffic which is not an easy task in protected Wi-Fi networks particularly the ones using WPA and WPA2 encryption algorithms (Wen et al., 2018). To acquire the MitM position in order to launch key reinstallation attacks, a multichannel technique is used. This technique is successfully implemented when the attacker acts both as a legitimate AP and legitimate client/user and copies all frames of data sent by the real AP and real client (Vanhoeft et al., 2018). The manipulation of secured and encrypted traffic is easily done during this process by the attacker.

Figure 15: MitM attack

5.3.3 Public Wi-Fi Security:

Perhaps one of the most concerning areas of the use of Wi-Fi is the security and privacy of the public Wi-Fi networks. Many of these public Wi-Fi networks are open networks and are free to use, and do not require users to prove their authentication (Sombatruang et al., 2016). But a number of previous studies have shown how much unsecured and hazardous to user's privacy are these networks. Yet despite the security issues of these open networks the users connecting expose themselves – knowingly or unknowingly – to security and privacy risks (Wen et al., 2018). It stands to reason that the users may or may not have sufficient awareness of the risk they take when connecting and using these public networks.

According to a study, the people connecting to open public networks are in a false hope that their privacy is not at any risk of any danger (Sombatruang et al., 2016). Their decision making is based mostly upon the limited use they make of these networks like they argue that they only connect to check certain websites or check their social media for any messages etc. Or even if they are aware of the security and privacy issues they ignore them.

Apps like Instagram, Facebook leaked cookies according to the observed experiment (Sombatruang et al., 2016). These cookies included URL links to MP4 videos, links to the photos seen and history of the activities performed while connected to the open Wi-Fi network. Though there were no username or password leaks, others leaks associated with the cookies raises major concerns with the extent of the use of this type of unsecure public networks (Sombatruang et al., 2016).

Table 2: Top ten websites/applications observed (Sombatruang et al., 2016)

Web/App Category	Sessions	Web/App Category	Sessions
Google Search	34	Instagram	7
Facebook	20	Unknown	6
Apple iTunes	18	Google Mail	6
WhatsApp	13	Potential Malware	5
Snapchat	7	Apple FaceTime	5
Total	121		

6. CONCEPTIONS AND MISCONCEPTIONS

6.1 Wi-Fi and Li-Fi - A HetNet Concept

The increasing production of modern smart devices like smart phones, tablets, smart TVs, and other smart home and office appliances all contribute to the rise of the Internet of Things (IoT) and all these IoT innovations and technologies demand for mobility with wireless capacity being the upmost one (Haas, 2016). This demand requires the current state of networking and Internet infrastructures to evolve on order to

provide the adequate needs primarily for the future multimedia applications and also the current machines (Ayyash et al., 2016). The role and innovation of wireless Heterogeneous Networks (HetNets) is a vital one with the objective to provide high quality-of-service (QoS), especially in heavy data consumption environments i.e. an indoor area (Haas, 2016).

The radio frequency (RF) spectrum has been in use for in Wi-Fi and LTE technologies for years now providing the means for wireless connectivity (Ayyash et al., 2016). Though up till now the RF volume of 300 GHz has been in use for wireless communication with little drawbacks of speed and reliability, the exponential increase in data volumes mainly due to the rise of IoT in the next decade will not have enough RF resources. The visible light spectrum, on the other hand, has 1000 times the RF spectrum unused bandwidth with high frequencies (Haas, 2016). These resources can be fruitful when used for data communication (Ayyash et al., 2016). The fiber-optic communication can be taken as a successful example of the use of these visible light resources.

A concept has been proposed that discusses a combination of RF spectrum (Wi-Fi) and visible light spectrum (Li-Fi) making a HetNet for providing the necessary resources for the current and future data communication needs [16, 17]. The idea is to use the resources offered by the both technologies with such a method so that the communication can be more effective and reliable. According to the figure 18, both Wi-Fi and Li-Fi devices are set up to provide Access Points (APs) in an indoor environment alongside LTE so that the user can make use of the features of not only Li-Fi but also Wi-Fi technologies in the indoor area. Li-Fi adds an additional wireless networking layer that provides improvements in data density and physical layer security (Haas, 2016).

Figure 16: A Wi-Fi - Li-Fi HetNet (Wen et al., 2018)

6.2 Li-Fi Misconceptions

Figure 17: Common misconceptions of Li-Fi (Leba et al., 2017)

- Li-Fi is a Line-of-Sight (LoS) Technology: Li-Fi works beyond the general inaccurate idea that it is an exclusively LoS technology (Haas, 2016). There have been experiments carried out that proved wrong this misconception. The proofs were that light can be sensed beyond the LoS by photo detectors and data can be transmitted for video transmission (Leba et al., 2017).
- Li-Fi does not work in Sunlight: Sunlight interferes with the Li-Fi signals is wrong as Li-Fi operates at higher frequencies which are greater than 1 MHz (Haas, 2016). Thus, it simply filters the constant sunlight and the performance of Li-Fi is not affected by it.
- Lights cannot be Dimmed: Different experiments have proved that data communication in Li-Fi works even in low intensity and dimmed lights (Leba et al., 2017). High data rates is provided

whether the lights are at high output levels or low output levels (dimmed) (Haas, 2016).

- The Flickering of Lights is Disturbing: It is a fact that the Li-Fi lights bulbs flicker but they flicker at a rate (around 1 MHz) that is higher than the human eye can perceive which is below 120-150 Hz [4, 17]. Thus resulting in no caused disturbance or it being harmful for the human eye.
- Li-Fi is Unidirectional Downlink: Li-Fi can be used for both uplink and downlink. This conception arises from the fact that LED illumination is combined with Li-Fi network. This does not mean that Li-Fi cannot be used without the need of lightning, on the contrary it can be used very effectively as the infrared spectrum is perfect for the uplink (Haas, 2016).
- Replacement of Existing Lights: The infrastructure of existing lighting system does not have to be replaced for the use of Li-Fi. The Li-Fi equipment only has to be attached to the existing infrastructure (Leba et al., 2017).

7. CRITICAL ANALYSIS

Li-Fi is latest technology which is good for short range to provide internet to local area network by using visible light instead of radio waved which is more secure, fast and cheap. Li-Fi can easily be implemented by replacing all the lights with LED bulbs. More work can be done on Li-Fi technology as it is line of sight and is available if the user is under the light waves, if the user moves very fast or is behind some obstacles like tree or something the user is unable to access the net, so more research indeed needed in research community so that a light bulb that provides data to high speed moving objects. In Li-Fi technology light can get interfered with some others light so reliability and network coverage can become a great issue. More work is required to on Li-Fi technology to make it more reliable and to provide more coverage.

8. CONCLUSION FUTURE WORK

The growing demand of wireless connectivity every time, everywhere and at any place and with advent of internet of things people used multiple devices; thus making the Wi-Fi connectivity more congested and crowded. Li-Fi can ease this congested and problematic airways as Li-Fi has unused bandwidth and visible light spectrum. The difference in speed and reliability between Wi-Fi and Li-Fi even has a chance to propel the current Wi-Fi technology to advance and ground breaking researches. The security feature of both Wi-Fi and Li-Fi can have more research done on them and more improved security mechanism can be implemented. Particularly, the current WPA2 security protocol is being improved and is to be replaced by the new and more secure WPA3. This makes the use of these technologies more secure especially in his age where the data and information is as important is other material things like money etc. The current in used protocols can be further investigated and improved for better efficiency and working, more security features can also be added to improve security aspects of these two (Wi-Fi and Li-Fi) Technology.

9. FUTURE WORK

In the future these systems can be commercially released and made available to the general public or easily available to the intended clients. With the advancement of Wi-Fi and Li-Fi, the systems using these technologies will also be improved and, the better the functioning of the systems the better will be the feedback from the intended clients. Both technologies are here to stay and more advancements and researches are being made.

REFERENCES

- Ayyash M. et al. 2016. Coexistence of Wi-Fi and Li-Fi toward 5G: concepts, opportunities, and challenges. IEEE Communications Magazine, Available: 10.1109/mcom.2016.7402263. 54(2), 64-71.
- Haas H. 2016. Li-Fi: Conceptions, misconceptions and opportunities. IEEE Photonics Conference (IPC). Available: 10.1109/ipcon.2016.7831279. 680-681
- Hooper M. et al. 2016. Securing commercial Wi-Fi-based UAVs from common security attacks. MILCOM 2016 - 2016 IEEE Military Communications Conference. Available: 10.1109/milcom.2016.7795496

- Julka E. and Kumar D. 2015. A Review Paper on Li-Fi Technology. International Journal of Scientific & Engineering Research, Available: <https://www.ijser.org/researchpaper/A-Review-Paper-on-Li-Fi-Technology.pdf>. [Accessed 27 December 2019]. 6(2), 58-62.
- Kulkarni S., Darekar A. and Joshi P. 2016. A Survey on Li-Fi Technology. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). Available: 10.1109/wisnet.2016.7566413. 3(1), 7-12
- Kumar N., Srikanth A., Singha A. and Sam B. 2017. Comparison of Li-Fi and Wi-Fi and study of smart meter-survey. International Conference on Information Communication and Embedded Systems (ICICES). Available: 10.1109/icices.2017.8070715.
- Kuppusamy P., Muthuraj S. and Gopinath S. 2016. Survey and challenges of Li-Fi with comparison of Wi-Fi. International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). Available: 10.1109/wisnet.2016.7566262, 1-4.
- Leba M., Riurean S. and Lonica A. 2017. Li-Fi — The path to a new way of communication. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI). Available: 10.23919/cisti.2017.7975997
- Mishra N., Rai M., Mandal R. and Kaur H. 2018. Navigation System Using Light Fidelity. 2nd International Conference on Trends in Electronics and Informatics (ICOEI). Available: 10.1109/icoei.2018.8553760. 354-357
- Monisha M. and Sudheendra G. 2017. Li-Fi- Light Fidelity Technology. International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). Available: 10.1109/ctceec.2017.8455097. 818-821
- Mosaif A. and Rakrak S. 2017. An Indoor Wireless Visual Sensor Network Basing on Light-Fidelity Communication. International Conference on Wireless Networks and Mobile Communications (WINCOM). Available: 10.1109/wincom.2017.8238159
- Sagers G., Hosack B., Rowley R., Twitchell D. and Nagaraj R. 2015. Where's the Security in Wi-Fi? An Argument for Industry Awareness. 48th Hawaii International Conference on System Sciences. Available: 10.1109/hicss.2015.641. 5453-5461.
- Sebbar A., Boulahya S., Mezzour G. and Boulmalf M. 2016. An Empirical Study of Wi-Fi Security and Performance in Morocco - Wardriving in Rabat. International Conference on Electrical and Information Technologies (ICEIT). Available: 10.1109/eitech.2016.7519621
- Shetty A. 2016. A Comparative Study and Analysis on Li-Fi and Wi-Fi. International Journal of Computer Applications, Available: 10.5120/ijca2016911558, 150(6), 43-48.
- Sombatruang N., Sasse M. and Baddeley M. 2016. Why do people use unsecure public wi-fi?. Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust - STAST '16. Available: 10.1145/3046055.3046058
- Swetha V. and Annadevi E. 2018. Survey on Light-Fidelity. International Conference on Smart Systems and Inventive Technology (ICSSIT). Available: 10.1109/icssit.2018.8748272. 355-358
- Vanhoef M., Bhandaru N., Derham T., Ouzieli I. and Piessens F. 2018. Operating Channel Validation. Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '18. Available: 10.1145/3212480.3212493. 34-39.
- Wen Y. and Liu T. 2018. Wi-Fi Security Certification through Device Information. International Conference on Sensor Networks and Signal Processing (SNSP). Available: 10.1109/snsp.2018.00065. 302-305.
- Zhang J., Wei B., Hu W. and Kanhere S. 2016. Wi-Fi-ID: Human Identification Using Wi-Fi Signal. International Conference on Distributed Computing in Sensor Systems (DCOSS). Available: 10.1109/dcoss.2016.30. 75-82