LI-FI TECHNOLOGY AND THE NEW CONCEPT OF DATA TRANSFER SECURITY

Ramona DUMITRAȘCU *

Abstract

Li-Fi is a wireless technology that transmits high-speed data using visible light communication (VLC), it can achieve speeds of 224 gigabits per second in the lab. The potential Li-Fi technology can change a lot in virtual word considering it can provide transmission at 1 GB per second - that's 100 times faster than current average Wi-Fi speeds. By flickering the light from a single LED, Li-Fi technology can transmit far more data than a cellular tower, using Visible Light Communication (VLC) technology - a medium that uses visible light between 400 and 800 terahertz (THz). It works basically like an incredibly advanced form of Morse code - flicking an LED on and off at extreme speeds and can be used to write and transmit things in binary code. The benefit of Li-Fi over Wi-Fi, other than potentially much faster speeds, is that because light cannot pass through walls, it makes it a whole lot more secure.

Keywords: *internet, security, software, encryption*

1. Introduction

Demand for wireless data is increasing day by day which is escalating the congestion in radio spectrum. In present scenario the bandwidth capacity which is available is finite and not capable enough to sustain with the constantly increasing demand of wireless data. Wireless Fidelity dubbed as Wi-Fi has been in use from almost years to provide the internet services to all the required places right from home to humungous organizations. But it has limited bandwidth of about 54-100 megabits per second (Mbps). With High definition video & audios available for the viewers, it is becoming intricate to transfer them to the user flawlessly. The problem of speed & consistency even doubles when support is to be given to multiple devices because of splitting up of bandwidth between devices. The beauty of Wi-Fi is its easy and simple to set up network but threatening part is to provide security. To overcome technological boundaries of Wi-Fi, a new paradigm is in, which is Li-Fi[1].

Transfer of data from one place to another is one of the most important day-to-day activities. The current wireless networks that connect us to the internet are very slow when multiple devices are connected. As the number of devices that access the internet increases, the fixed bandwidth available makes it more and more difficult to enjoy high data transfer rates and connect to a secure network. But, radio waves are just a small part of the spectrum available for data transfer. A solution to this problem is by the use of Li-Fi. Li-Fi stands for ”Light- Fidelity”. Li-Fi is transmission of data through illumination by taking the fiber out of fiber optics by sending data through an LED light bulb that varies in intensity faster than the human eye can follow.

Li-Fi is the term some have used to label the fast and cheap wireless communication system, which is the optical version of Wi-Fi. Li-Fi uses visible light instead of Gigahertz radio waves for data transfer.

The idea of Li-Fi was introduced by a German physicist, Dr. Harald Hass, which he also referred to as data through illumination. The term Li-Fi was first used by a german scientist Dr. Harald Haas in his TED Global talk on Visible Light Communication[2].

According to Hass, the light which he referred to as D-Light, can be used to produce data rates higher than 10 Gigabits per second which is much faster than our average broadband connection.

Li-Fi can play a major role in relieving the heavy loads which the current wireless systems face since it adds a new and unutilized bandwidth of visible light to the currently available radio waves for data transfer. Thus it offers much larger frequency band (300 THz) compared to that available in RF communications (300 GHz). Also, more data coming through the visible spectrum could help alleviate concerns that the electromagnetic waves that come with Wi-Fi could adversely affect our health.

Li-Fi can be the technology for the future where data for laptops, smart phones, and tablets will be transmitted through the light in a room. Security would not be an issue because if you can‘t see the light, you can‘t access the data. As a result, it can be used in high security military areas where RF communication is prone to eavesdropping[3].

* PhD Candidate, Faculty of Law, "Nicolae Titulescu" University of Bucharest (email: **monadumitrascu@yahoo.com**).

[1] Vinod Saroha, Ritu Mehta, ”Network Security: Li-Fi: Data Onlight Instead of Online”, *International Journal Of Engineering And Computer Science* 3/1 (2014): 3681-3688.

[2] Anurag Sarkar, Shalabh Agarwal, Asoke Nath, ”Li-Fi Technology: Data Transmission through Visible light”, *International Journal of Advance Research in Computer Science and Management Studies*, 3/6 (2015): 1-12 (available online at: www. ijarcsms.com).

[3] A. Anvith Raj, Vamshi Krishna Sai Nagabandi, Santosh Kumar, *Li-Fi (Light-Fidelity) Technology. Transmission of data through light*.

Light waves do not penetrate through walls. So, they can't be intercept and misused[4].

2. Content

Light Fidelity, Li-Fi, is a relatively new form of wireless communication technology. It uses light signals to communicate data. The excitement surrounding Li-Fi is because it has proven to have higher speeds than Wi-Fi. In the lab, Li-Fi has reached speeds of 224 gigabits per second. The same lab field tested Li-Fi technology in a factory based in Estonia and achieved transmission rates at 1 gigabit per second.

Professor Harald Hass wanted to turn the world's light bulbs into wireless routers. "All we need to do is fit a small microchip to every potential illumination device and this would then combine two basic functionalities, illumination, and wireless data transmission. In the future we will not only have 14 billion light bulbs, we may have 14 billion Li-Fis deployed worldwide for a cleaner, greener, and even brighter future" (Harald Hass Ted Talk 2011).

Herald Hass has proved that data can be transmitted over the light spectrum - this makes Li-Fi a form of optical wireless communication. Li-Fi uses infra-red and ultra-violet (visible light) waves to communicate data. Infra-red and ultra-violet spectrums can carry more information than radio frequency waves. This is why Li-Fi can achieve greater speeds than Wi-Fi.In simple terms, Li-Fi can be thought of as a lightbased Wi-Fi. That is, it uses light instead of radio waves to transmit information. And instead of Wi- Fi modems, Li-Fi would use transceiver-fitted LED lamps that can light a room as well as transmit and receive information. Since simple light bulbs are used, there can technically be any number of access points[5].

Currently, Li-Fi technology is focused on using the light from light-emitting diodes (LEDS) to communicate data. LEDs have become very popular around the world for their efficiency, low environmental impact, and longevity. The LED lights in homes and offices can be turned into wireless routers. LED light bulbs are a semiconductor light source, therefore, the constant electricity supply to the bulb can be altered to make it brighter or dimmer. Using visible light communication (VLC) the current in the LED bulb is flicked on and off at very high rate, functioning like a complex Morse code involving 1s and 0s. The flicking will happen at a speed too fast for the human eye to notice, so humans and animals will not be impacted. Li-Fi will continue after you have switched the lights off because the LEDs will be lit and signaling at a low light level that cannot be recognized by the human eye. To access the Li-Fi network you simply need a device to detect the light signals, with a component to decipher the light signals.

Wi-Fi uses radio frequency waves, a technology which has limited space and is quickly reaching its capacity. The limited capacity is why the radio frequency spectrum is heavily regulated in the US a nd it also provoked many security liabilities.

One of the most endearing facets of Li-Fi is that it uses the visible light spectrum. The visible light spectrum is 10 000 times larger than the radio frequency spectrum and is unregulated. So you don't need a license to take advantage of the light spectrum.

Another upside to Li-Fi is that it uses light spectrum and not radio frequency. Therefore, it emits no electromagnetic interference. This makes it more suitable for highly sensitive areas. Electromagnetic interference can affect communication in areas like mines or disrupt sensitive equipment in places like hospitals.

Data is fed into an LED light bulb which is fitted with signal processing technology. The LED bulb pulses the data at a high non-visible rate to the photodetector. The pulses are interpreted by the receiver into an electrical signal, the electronic signal is then converted back to binary data which is the web content we consume. The LED lights will be networked, so multiple users can access data using a single LED light or move from one LED light to another without affecting their access.

Although Li-Fi has faster speeds than Wi-Fi, it has a very short range. The further away you are from the light source, the slower the speed. That being said, you don't necessarily need to be under the LED light to access Li-Fi because it can use light reflections on surfaces, including walls, to achieve speeds averaging 70 MB/s. Unlike Wi-Fi, Li-Fi cannot penetrate walls because it uses light spectrum. Although not being able to penetrate walls limits the range of Li-Fi, it also makes the technology much more secure. It ensures that users can limit the area of accessibility. The security aspect of Li-Fi has both technology and defence firms very interested.

Due to the speeds that Li-Fi can reach, and its spatial limits, the technology IS ESPECTED TO work well alongside cellular and Wi-Fi technology as an additional option for connectivity. Li-Fi can be used to syphon off heavy traffic from cellular and Wi-Fi networks. For example, Li-Fi can be made available in densely populated areas like a shopping mall or sports stadium, allowing users to consume content rich media like videos or live streaming. As the users will be on the Li-Fi network, this will free up cellular and Wi-Fi network capacity in that area. This is because the uplinks require little capacity - it is the downlinks that strain the networks. The Internet of Things (IoT) is a

[4] Gaurav Singh, Santoshkumar Yadav, Essakkimuthu Nadar, Kumari Gowda Archana Nanade, "Transmission of Data Using Li-Fi Technology", *International Journal of Computer Science Trends and Technology (IJCS T)* 4/2 (2016): 199-202 (available online at: www. ijcstjournal.org).

[5] Vinod Saroha, Ritu Mehta, "Network Security: Li-Fi: Data Onlight Instead of Online", *International Journal Of Engineering And Computer Science* 3/1 (2014): 3681-3688.

revolution that has a lot of experts asking, where will we find the capacity to handle all that data? Li-Fi has proven itself as a viable, efficient and secure solution. A home, office or factory could run its own high capacity network over Li-Fi without adversely affecting public capacity[6]. Moreover, there are areas where radio simply does not work, or is not permitted such as underwater and in aircraft cabins. The possibilities are nearly unlimited[7].

Security of the data transfer is currently one of the most important concerns. Visible light can be reflected but generally does not penetrate materials which can be a security advantage and perhaps a coverage disadvantage[8]. Wi-Fi communication is vulnerable to hackers as it penetrates easily through walls. Radio waves can penetrate through walls. This leads to many security concerns as they can be easily intercepted. Light of course does not penetrate through walls and thus data transmission using light waves is more secure Yet, one serious disadvantage of the. Li-Fi technology ist that it requires line of sight. If the intensity of an external source of illumination such as sun is greater than the intensity of the transmitting LED array then the data to be transmitted is washed out. The receiver cannot transmit back or provide feedback to the transmitter[9].

Arguably the most important criteria of choosing and using the transfer data through internet is the security of the transfer. As we all know, wireless signals delivered by radio waves can go through walls into the outside world, where hackers and other malicious entities might be waiting. Light, on the other hand, can't pass through walls, which means that it's more likely to stay secure than a wireless signal broadcast to the entire vicinity[10]. As long as transparent materials like windows are covered, access to a Li-Fi channel is limited to devices inside the room.

This raises the possibility of creating secure ad-hoc networks in meeting rooms for example – enabling participants to share data without risk of data leaking out. Communication only takes place where the light can be seen, therefore the light can be directed towards certain areas within the office. This creates possibilities in open plan offices to create network zones. Maybe one part of the office connects to a project network, alternatively if you walk to another area you are granted public Internet access**.** On the building infrastructure side, the sender (light bulb) and receiver (sensor) are not necessarily the same device, or even in the exact same spot.

The communication is fundamentally uni-directional. Two uni-directional channels are used back-to-back to create communications. While this in essence is an accident of the technology, it could be used creatively to build security enclaves as the solution effectively has data-diodes built in[11].

Li-fe is a free band and doesn't need license and it uses light[12]. Li-Fi is a visible light communication medium, which is not, required any kinds of spectrum license. It is we didn't pay any amount for communication and license[13].

It is a proven fact that Li-Fi is more secure as compared to traditional Wi-Fi. This is because Wi-Fi routers are generally used by attackers to enter a network and strong firewalls are also unable to safeguard your network from these attackers. One of the common reasons behind this is that the range of Wi-Fi routers is an important factor which enables these security breaches into your Wi-Fi network.

On the other hand, Li-Fi uses light which limits the range of the internet connection and it cannot be increased at any cost. Thus, not letting the bulb be lightened or dimmed manually. This peculiar feature of Li-Fi will protect your network from interference from your neighbours.

Along with those blazing speeds, Li-Fi offers security benefits beyond strong passwords and AES encryption. Because it uses visible light to transmit data, it can't pass through walls, making it practically as secure as sharing files with an external Thunderbolt drive. Furthermore, since light waves don't interfere with other radio signals like Wi-Fi does, it could even be used safely on planes, in hospitals, and in other areas where interference is an issue.

Li-Fi, could provide a substantially increased solution to enhance data security to businesses seeking to improve data protection, from government and defence organisations, to financial, public sector, pharmaceutical, or any 'high data risk' industries.By exploiting specific properties of light, the Li-Fi system prevents both sides of the communications link being intercepted. Professor Haas explains: "Let us consider what Li-Fi means for the security of public and corporate internet access. Wi-Fi signals propagate in all directions and pass through walls and all data within range can be recorded. Because Li-Fi signals travel in directional beams between an access point and a

[6] https://www.sitepoint.com/li-fi-lighting-the-future-of-wireless-networks/.

[7] http://www.securityinfowatch.com/article/12103850/light-enabled-wi-fi-may-be-the-future-of-secure-communications-technology.

[8] Sushilkumar E. Khaparde, Bhaskar Y. Kathane, "An emerging technology of data transfer through light waves (Li-Fi)", *International Journal of Recent Trends in Engineering & Research (IJRTER)* 2/2 (2016): 20-25.

[9] Nikhil Gujral, Sagar Dolas, Love Thakur, Samay Nikam, "Li-Fi (LED Based Data Transfer)", *International Journal on Recent and Innovation Trends in Computing and Communication* 4/3 (2016): 245-247.

[10] http://www.prosper-it.com/blog/game-changer-new-li-fi-technology-transmits-data-via-light.

[11] https://cybermatters.info/2017/01/10/li-fi-security/.

[12] Sinku U. Gupta, "Research on Li-Fi Technology& Comparison of Li-Fi/Wi-Fi", *International Journal of Advanced Research in Computer Science and Software Engineering* 5/6 (2015): 429-433 (available online at: www.ijarcsse.com).

[13] Manas Ranjan Mallick, "A Comparative Study Of Wireless Protocols With Li-Fi Technology: A Survey", *Proceedings of 43rd IRF International Conference, 29th May, 2016, Chennai, India*: 8-12.

terminal, and vice versa, a potential interceptor would need to be in the overlapping space of both light beams. Even an unencrypted Li-Fi access point provides better security than Wi-Fi". "Li-Fi removes the uncertainty of joining a network", he continues. "In a typical Li-Fi installation, ceiling lights which transmit and receive the data are part of the premises and this creates a chain of accountability for the security of the users' data. The inherent security advantages of Li-Fi and the accountability that it offers, provide a supplement to the emerging need for greater data security and responsibility"[14].

Having a global view on the new transfer data technology through by LI-FI one can easily conclude on it's major advantages such as: high speed transmission as high as 500 mbps or 30 GB per minute, Li- Fi uses light rather than radio frequency signals, VLC could be used safely in aircraft, Li-Fi can be integrated into medical devices and in hospitals as this technology does not deal with radio so it can easily be used in such places where Bluetooth, infrared, Wi-Fi and internet are banned. In this way, it will be most helpful transferring medium for us. Li-Fi is efficient under water in sea, where Wi-Fi does not work at. There are around 19 billion bulbs worldwide, they just need to be replaced with LED ones that transmit data. We reckon VLC is at a factor of ten, cheaper than Wi-Fi. Security is another benefit, since light does not penetrate through walls. By implanting the technology worldwide every street lamp would be a free access point. Li-Fi may solve issues such as the shortage of radio frequency bandwidth. Visible light spectrum has 10,000 time broad spectrum in comparison to radio frequency used in Wi-Fi[15].

The genial recognition of Haas to use led frequency as a replacement for wi-fi radio-frequency; enhancing the usable band with tremendously and at the same time making the message transmission more secure and less harmful (no magnetic field interference) has, however a possible disadvantage to be investigated: although led frequencies are not perceived by the human eye as such, it is uncertain weather the brain as such is not aware of the fluctuation of light- the essence of the message. Let it be understood that this issue gas been linked to the occurrence of epilepsy and other related symptoms. Although I am fully aware that this thesis has nothing to do with the essence and the purpose of this article, namely security issues in transfer of data and intellectual property issues I do have the opinion that ignoring the safety and well-being of humans supersede any other arguments.

3. Conclusions

Internet offers without a doubt unlimited possibilities in accessibility, for anyone and everyone to utilize which implies transparency and as consequence, total exposure which automatically will result in vulnerability. Until recently, enormous resources (people, money, research, security) have been allocated to protect and secure the data transfer. This resulted into a huge industry of software programs meant to protect the information, the intellectual property and the secret of communication. Until recently the solution of safety was always searched into software and only lately the revolution of the Li-Fi technology revealed that actually software-like solutions can be solved by changing the way of communicating online. Although many of the previous inventions still remain extremely useful, such us encryption and it variations, other might just not be useful anymore, such us firewalls.

References:

- Vinod Saroha, Ritu Mehta, "Network Security: Li-Fi: Data Onlight Instead of Online", International Journal Of Engineering And Computer Science 3/1 (2014): 3681-3688;
- Anurag Sarkar, Shalabh Agarwal, Asoke Nath, "Li-Fi Technology: Data Transmission through Visible light", International Journal of Advance Research in Computer Science and Management Studies, 3/6 (2015): 1-12 (available online at: www. ijarcsms.com);
- A. Anvith Raj, Vamshi Krishna Sai Nagabandi, Santosh Kumar. K, Li-Fi (Light-Fidelity) Technology. Transmission of data through light;
- Gaurav Singh, Santoshkumar Yadav, Essakkimuthu Nadar, Kumari Gowda Archana Nanade, "Transmission of Data Using Li-Fi Technology", International Journal of Computer Science Trends and Technology (IJCS T) 4/2 (2016): 199-202 (available online at: www. ijcstjournal.org);
- Sushilkumar E. Khaparde, Bhaskar Y. Kathane, "An emerging technology of data transfer through light waves (Li-Fi)", International Journal of Recent Trends in Engineering & Research (IJRTER) 2/2 (2016): 20-25;
- Nikhil Gujral, Sagar Dolas, Love Thakur, Samay Nikam, "Li-Fi (LED Based Data Transfer)", International Journal on Recent and Innovation Trends in Computing and Communication 4/3 (2016): 245-247;
- Sinku U. Gupta, "Research on Li-Fi Technology& Comparison of Li-Fi/Wi-Fi", International Journal of Advanced Research in Computer Science and Software Engineering 5/6 (2015): 429-433 (available online at: www.ijarcsse.com);

[14] http://purelifi.com/purelifi-technology-delivers-security-improvements-fight-against-cyber-crime/.

[15] Vinod Saroha, Ritu Mehta, "Network Security: Li-Fi: Data Onlight Instead of Online", *International Journal Of Engineering And Computer Science* 3/1 (2014): 3681-3688.

- Manas Ranjan Mallick, ”A Comparative Study Of Wireless Protocols With Li-Fi Technology: A Survey”, Proceedings of 43rd IRF International Conference, 29th May, 2016, Chennai, India: 8-12;
- https://www.sitepoint.com/li-fi-lighting-the-future-of-wireless-networks/;
- http://www.securityinfowatch.com/article/12103850/light-enabled-wi-fi-may-be-the-future-of-secure-communications-technology;
- http://www.prosper-it.com/blog/game-changer-new-li-fi-technology-transmits-data-via-light;
- https://cybermatters.info/2017/01/10/li-fi-security/.