Advances in Wireless Communications and Networks
2015; 1(4): 21-28
http://www.sciencepublishinggroup.com/j/awcn
doi: 10.11648/j.awcn.20150104.11

Survey Paper: State of the Art in Secure Wireless Propagation

Peter S. Nyakomitta, Wilson K. Cheruiyot, Agnes N. Mindila

Department of Computing, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Email address:
pnyakomitta@yahoo.com (P. S. Nyakomitta)

To cite this article:
Peter S. Nyakomitta, Wilson K. Cheruiyot, Agnes N. Mindila. Survey Paper: State of the Art in Secure Wireless Propagation. *Advances in Wireless Communications and Networks.* Vol. 1, No. 4, 2015, pp. 21-28. doi: 10.11648/j.awcn.20150104.11

Received: March 1, 2016; **Accepted:** March 24, 2016; **Published:** April 14, 2016

Abstract: Wireless networks provide an efficient means of connecting network devices. This is because they are fast, cost effective, flexible and easy to use. However, their usage is hindered by a number of challenges, owing to the fact that the physical connections between devices are replaced by logical associations. This means that anybody with a radio detector can receive these signals. Moreover, the data propagation in wireless environment is broadcast in nature and hence propagations can be overheard by anyone within a given range. To address these challenges, authentication protocols have been developed to deter any illicit access to these networks. They include Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). However, these protocols have been shown to be easily compromised, for example due to the utilization of weak initialization vector which leads to collision of the generated hashes. This necessitates the development of more secure mechanisms for protecting the information in transit. The latest effort in securing wireless data propagations involves the usage of the light-fidelity technology. In this paper, a survey of these security technologies given.

Keywords: Light-fidelity, wireless networks, data security

1. Introduction

In wireless propagation, signals are emitted uniformly in all directions and received in the same version by any device equipped with a radio detector. Wireless local area networks provide an expedient and low cost mechanism for connecting network devices such as mobile phones. They are convenient since they do not require physical connections [1]. In this point of view, they overcome the port limitations of the physical hardware in that any device that has radio receiver can detect these wireless signals. This is because a wireless router transmits the signals uniformly in all directions [2]. However, in this environment, masquerading can be a big challenge, where an adversary can illicitly disconnect a legitimate user and use his credentials to establish a connection to the network.

Wireless networks are exposed to many attacks such as shared key decryption. These attacks can be launched from a remote location, unlike in wired networks where one needs physical connections to the network of interest. To overcome this challenge, authentication protocols have been developed to deter any illicit access to wireless networks. These protocols include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and the IEEE 802.1X. Wi-Fi Protected Access version 2 (WPA2) is the later version of WP. However, these have been seen to be easily compromised [3].

In the light of this, light fidelity has been proposed as a solution to illegal wireless connections which lead to attacks such as shared key decryption, output validation by word comparison and port scanning.

2. Secure Wireless Data Propagation

The techniques that are currently used to protect wireless data propagation include wired equivalence privacy (WEP), Wi-Fi protected access (WPA) and the institute of electrical and electronics engineers 802.1x (IEEE 802.1X). The latest mechanism towards securing wireless data is the Li-Fi technology. The sub-sections below give a survey of each of these techniques.

2.1. Wired Equivalence Privacy

This authentication protocol works by encrypting the data that is to be transmitted over the network to keep it safe from eavesdropping [4]. The wireless device shares the key with the wireless access point. Each packet is encrypted with shared key together with the initialization vector (IV). Each packet also includes an integrity check. WEP security involves two phases, namely authentication and encryption stages. Authentication phase involves validating a device when it first joins the wireless network. This is meant to prevent devices joining the network unless they know the WEP secret key [5].

The wireless detector and the access point are not required to keep past states, hence this mechanism can fall prey of packet replay attacks. Moreover, the idea that the same key is shared between access point and wireless device means that if there are multiple devices using the same key, this can compromise WEP authentication process and increase the chances of initialization vector collision.

The shared key alteration at an access point necessitates that every user change their key accordingly. This makes key management difficult to administer manually. Therefore most of the users do not change access point keys frequently. They keep the same key for many months or years or forever [6]. This gives an attacker more time to analyze the traffic and identify the key-stream and initialization vector reuse.

2.2. WI-FI Protected Access (WPA)

This protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP [7]. It employs the Temporal Key Integration Protocol (TKIP) algorithm for encryption, which is a security protocol used in the IEEE 802.11 wireless networking standard as a solution to replace WEP without requiring the replacement of legacy hardware. This was necessary because the breaking of WEP had left Wi-Fi networks without viable link-layer security, and a solution was required for already deployed hardware [8].

Although the WPA protocol had increased wireless security to a great extent, it also has some challenges. Firstly, it has some weakness in passphrase choice in its interface. This weakness is inherent from the Pair Wise Master key (PMK) that is derived from the concatenation of the passphrase, Service Set Identifier (SSID), length of the SSID and nonces (a number or bit string used only once in each session).

Secondly, there is possibility of the brute force attack, which is a passive attack where the intruder generates every possible permutation in the key and tries to decrypt the encrypted message with each generated permutation [9]. From this, he can validate the output by means of cross comparison of words, file header and any other data. Moreover, there is placement of Message Integrity Check (MIC), which is considered a problem because it can be used by any hacker in validating the contents of the decrypted message combined with the brute force attack [10].

To address the problems in WPA, Wi-Fi Protected Access2 (WPA2) protocol was introduced. It utilizes a more robust encryption algorithm known as Advance Encryption Standard (AES). This standard brought in a new advanced encryption mechanism using the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).

This provides security against most of the attacks encountered due to weak encryption key [11]. However, WPA2 suffers from brute forcing attacks and placement of Message Integrity Check, just like the original WPA.

2.3. IEEE 802.1X

This is an IEEE Standard protocol for port-based Network Access Control (PNAC) that provides an authentication mechanism to devices desiring to attach to a network. IEEE 802.1X authentication enhances the security of wireless networks by thwarting unauthorized devices from achieving port-level access to protected networks through wired or wireless LAN connections.

It leverages an extensible architecture that supports a variety of authentication methods, including passwords, Rivest, Shamir and Adleman (RSA) keys, token cards, and certificates [12]. The 802.1x relies on an integrated system of components to manage the authentication process. The first component is the supplicant, which is a software or service running on a device that seeks access to a protected network.

The second component is the authenticator, which is a software or service running on a wireless access point or switch that manages the authentication process between the supplicant and authentication server. The authentication server provides authentication services to the authenticator. Using the credentials provided by the supplicant, the authentication server controls whether the supplicant is authorized to access the services provided on the authentication server's protected network or not [13].

Another constituent is the port, which is a service access point, typically on a router or switch, whose state is either unauthorized or authorized. An unauthenticated supplicant device initially connects to an unauthorized port on the public network. After successful authentication, the device is connected to an authorized port and able to access resources on the protected network.

The last component is the extensible authentication Protocol (EAP), which is a generic authentication framework that supports many different types of authentication methods with different options, including Kerberos, public-key encryption, and one-time passwords [14]. EAP data propagation between supplicants and authenticators is typically encapsulated using the EAP over LAN (EAPoL) protocol. EAP data propagation between authenticators and the authentication server is typically encapsulated using Remote Authentication Dial In User Service (RADIUS).

However, IEEE 802.1X requires integration with a 3rd party and every endpoint management. Therefore, all devices must be configured with 802.1 X and integrated with server authentication [15]. Moreover, this authentication method

requires 802.1X client software on the supplicant nodes.

2.4. Light -Fidelity Technology

Li-Fi is a wireless optical networking technology that allows the propagation of data through illumination by use of a light emitting diode (LED) that varies in intensity faster than the human eye can recognize [16]. The LEDs are outfitted with a chip that modulates the light imperceptibly for optical data transmission. Li-Fi data is transmitted by the LED and received by photoreceptors [17].

In this type of communication, when the LED is on, the data that is transmitted is a digital 1. On the other hand, when the LED is off, a digital '0' is transmitted.

It is possible to encode data in the light by varying the rate at which the light emitting diode flicker on and off to give different strings of 1s and 0s. The LED intensity is modulated so rapidly that human eye cannot recognize. This makes the output to appear invariable.

To utilize this technology, one requires some LEDs and a controller that codes data into the LEDs. These LEDs are located on the data transmitter. One needs to vary the rate at which the LED's flicker depending upon the data that is required to be encoded (Saproo and AshaBhagashra, 2013). Further enhancements can be made in this method, like using an array of LEDs for parallel data propagation, or using mixtures of red, green and blue LEDs to alter the light's frequency with each frequency encoding a different data channel.

Such advancements promise a theoretical speed of 10 Gbps – meaning one can download a full high-definition film in just 30 seconds [18]. On the receiver side, there are photo-detectors that act as transducers, converting the light energy into electrical signals, which can be digital or analogue. This signal is then fed to the data terminal equipment.

3. Li-Fi Technology and Wireless Security Enhancement

According to [19], wireless networks security can be evaluated using parameters such as data confidentiality, data integrity, data authentication and availability. While data confidentiality is concerned with the protection of data against disclosure to unauthorized parties, integrity deals with the protection of information from being modified by unauthorized parties.

On the other hand, availability of information refers to ensuring that authorized parties are able to access the information when needed [20]. Moreover, data authentication ensures that a receiver can verify that the data was sent by the claimed transmitter.

4. Procedure

A conventional LI-FI communication system consists of a transmitter and a receiver. The interface between the transmitter and the receiver is wireless, in that they are connected by light emitted from the transmitter and then detected by the photo-detector located in the receiver. Figure 1 gives an illustration of the operation of a LI-FI communication system.

The first component of the LI-FI communication system is the transmitter section. It comprises of the input, a timer circuit, and a light emitting diode (LED). The input refers to any type of data that is to be transmitted, such as voice, text, video or multimedia.

The timer circuit is used to provide the required time intervals between each bit that is to be transmitted. These bits are in the format of 1's and 0's and are transmitted in the form of flashes of the LED.

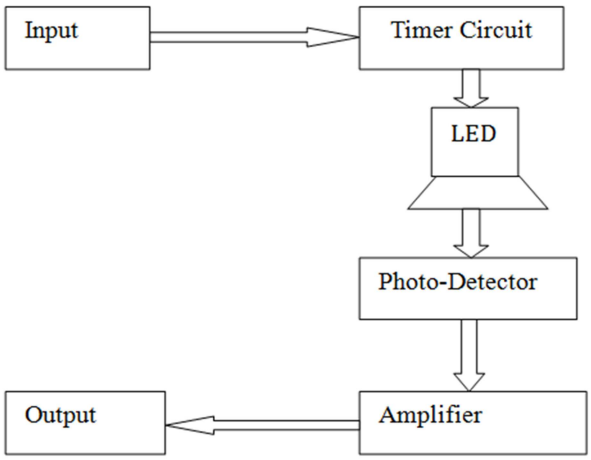

Figure 1. *Block Diagram of a LI-FI communication*

The light signals from the light emitting diode are received by the photodiode. The photodiode acts as a transducer, converting the light energy into electrical signals. Due to losses in the electronic devices due to medium resistance and noise, the transmitted signals are bound to be weak. They therefore need to be amplified before being fed to the output.

The output of choice was a four-channel oscilloscope. This is because the researcher needed to probe the output of the transmitter, the legitimate receiver and the adversary. The complete simulation design consisting of the legitimate users and the adversary is as shown in Figure 2.

Simulation is a mathematical way of emulating the behavior of a circuit to an extent of determining much of the circuit's performance without physically constructing the circuit or using actual test instruments. As indicated, there are three inputs to the four-channel oscilloscope: one from the transmitter, another from the legitimate user while the last one is from the adversary.

The components were laid out in NI Multisim software as shown in Figure 2 through identification which was mainly concerned with the calibration of the netlist items. The process of module optimization was used to tune the netlist items to their required values. It involved the connection of the section of interest to the oscilloscope and reading the output. The values of the individual components were then varied till the required output was available at the output, as

indicated by the oscilloscope probe.

The function generator is labeled XFGI, the oscilloscope is labeled XSCI while the operational amplifier is labeled OPA656U. The approach of this study was to completely prevent the adversary from receiving the communication signals instead of using authentication protocols, such as WEP, WPA or IEEE 802.1X.

The type of signal used in this simulation was a digital one with only two states: one and zero. Moreover, the persistence of the digital signal at level zero (0) indicates absence of the signal and hence lack of signal reception by that segment of the LI-FI communication network.

However, it was not possible to couple light signals from the LED to the photo-diode in the simulation software. Therefore, an opto-coupler was used instead of the LED and the photo-diode.

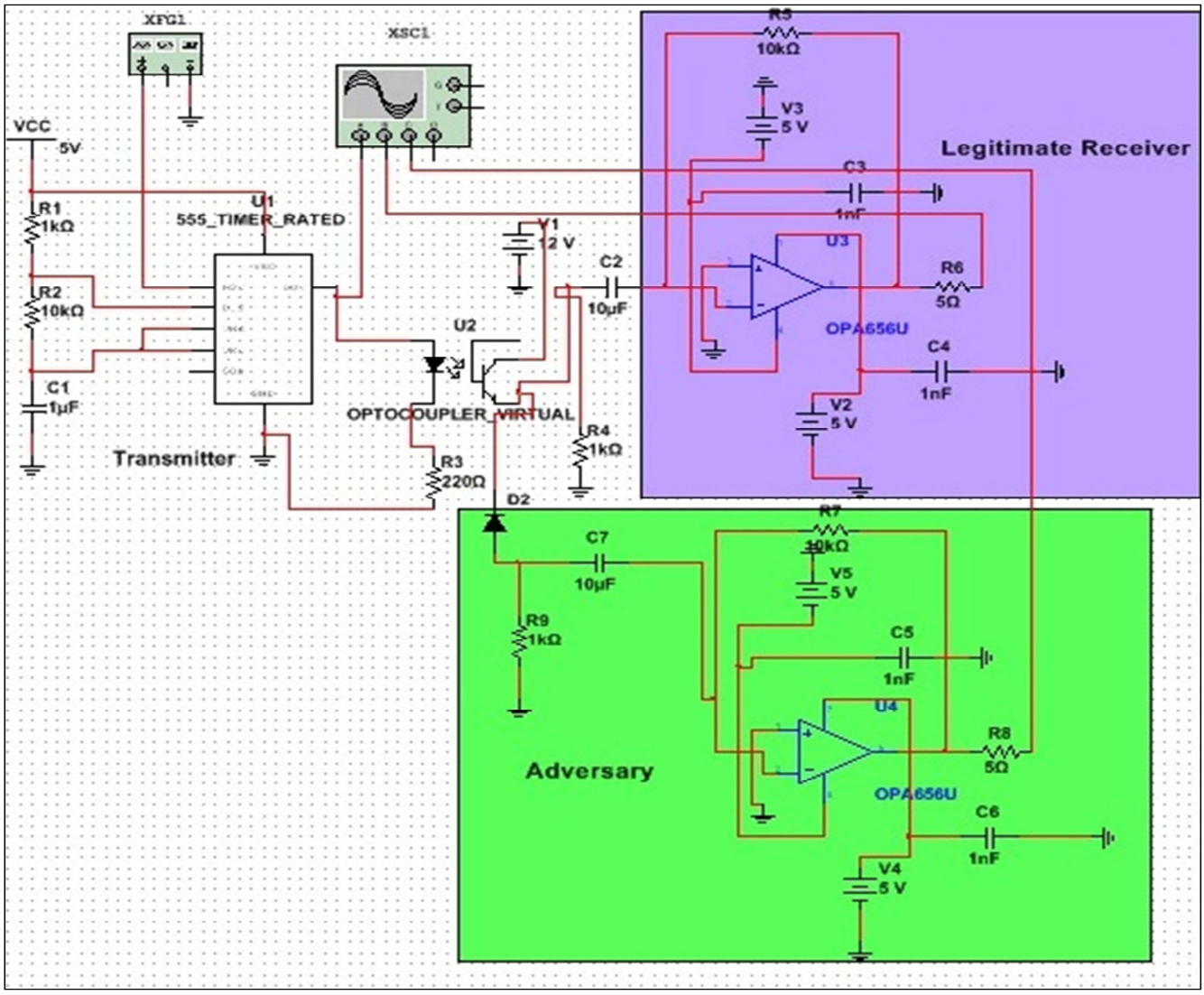

Figure 2. *NI Multisim Layout Consisting of Legitimate User and Adversary*

This device transfers electrical signals between two isolated circuits by using light. It is therefore a LED-photodiode combinational device as it incorporates the features of the LED (by emitting light signals) and the photo-diode (by transforming light energy into electrical pulses).

5. Security Assessment of Light-Fidelity Technology

The appraisal process for Li-Fi was carried out using four parameters identified above, namely confidentiality, integrity, availability and authentication.

5.1. Confidentiality and Integrity

To evaluate the Li-Fi technology against the principle of confidentiality and integrity, both the transmitter signals and the receiver signals were connected to the oscilloscope. Figure 3 shows the experimental setup for the transmitter on the left hand side while the right hand side shows the output obtained.

As this figure demonstrates on the left hand side, the transmitter was connected to the oscilloscope channel A. The right hand side contains the waveform that was observed.

Figure 4 that follows gives the experimental setup for the receiver on the left hand side while the right hand side shows the waveform examined.

Once again, Figure 4 demonstrates on the left hand side that the receiver was connectd to the oscilloscope channel B. The right hand side displays the waveform that was detected.

Comparing the output of the transmitter with that of the receiver, it was observed that the two waveforms are similar, with the difference being on the signal amplitude. While the transmitter amplitude was 5 volts, the receiver amplitude was 10 volts.

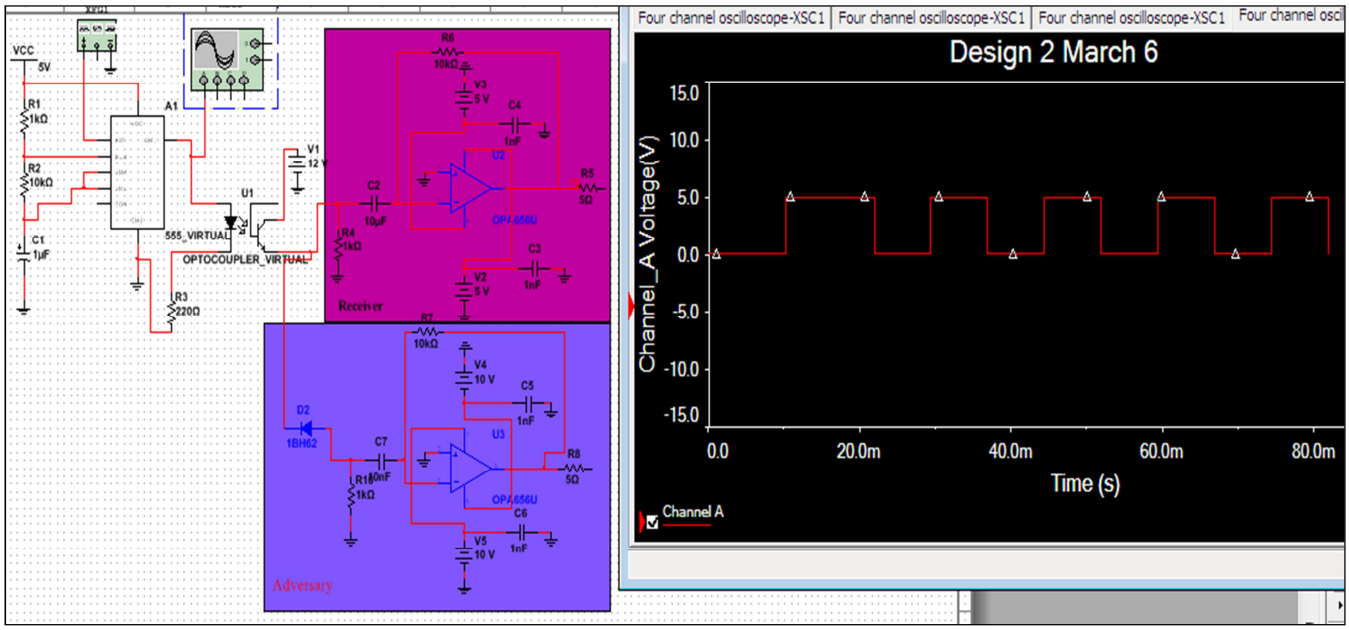

Figure 3. *Li-Fi Evalution Against Confidentiality – Transmitter Section*

This demonstrates that confidentiality, which guarantees that only the authenticated people can interpret the message / data content on transit and integrity, which holds to the concept that the content of the communicated data is assured to be the same as that in source document and has not been exposed to accidental or malicious alteration or destruction between the end points (sender and receiver) were upheld.

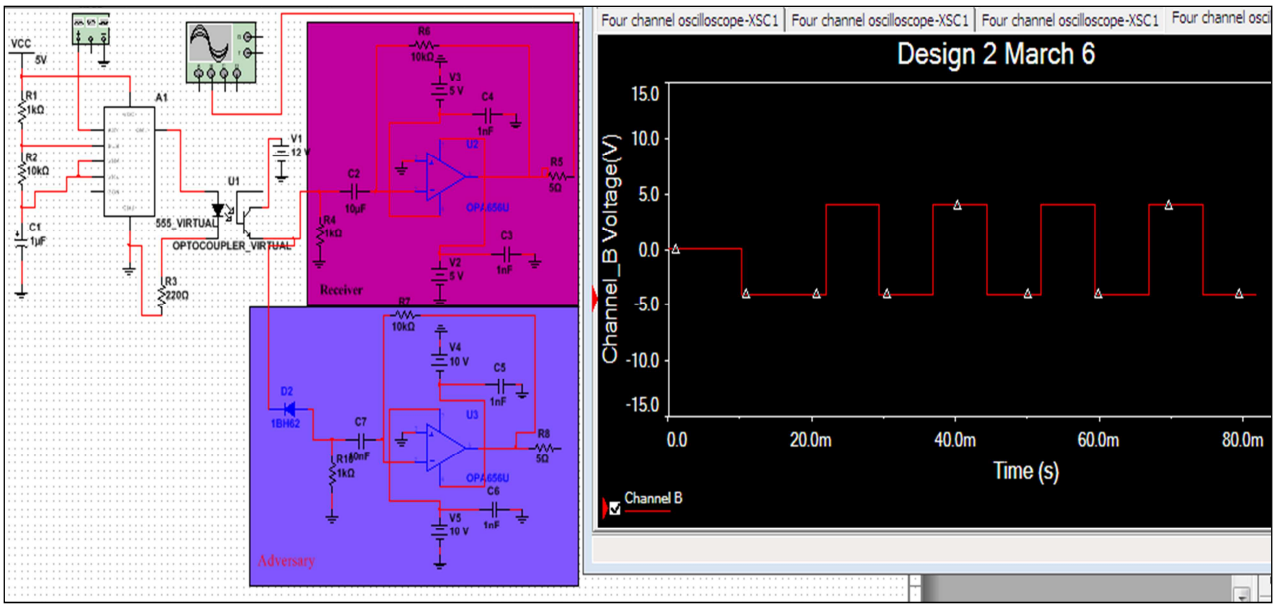

Figure 4. *Li-Fi Evalution Against Confidentiality – Receiver Section*

5.2. Availability

Availability is achieved when the transmitted data reaches the intended destinaton. To demonstrate that Li-Fi technology conforms to this principle, a signal was transmitted and its detection was done at the receiver section as shown in Figure 5. As the left hand side of Figure 5 shows, only the oscillosope's channel A was connected to the transmiter

section. The receiver section was effcetively disconnected from the oscilloscope channel B.

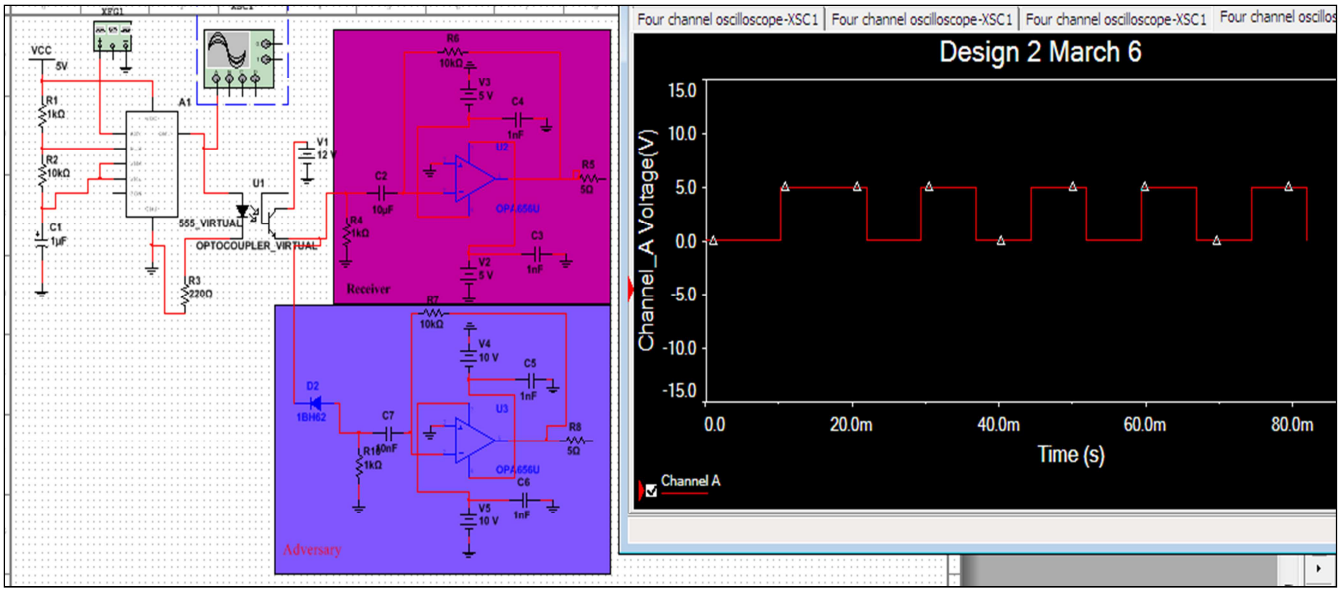

Figure 5. *Li-Fi Evalution Against Availability – Transmiter Section*

The output signal had an amplitude of 5 volts as demonstrated by the right hand side of Figure 5. It was necessary to observe whether this signal could be detected at the receiver section. Therefore, the receiver section was connected to the oscilloscope channel B as shown in Figure 6 that follows.

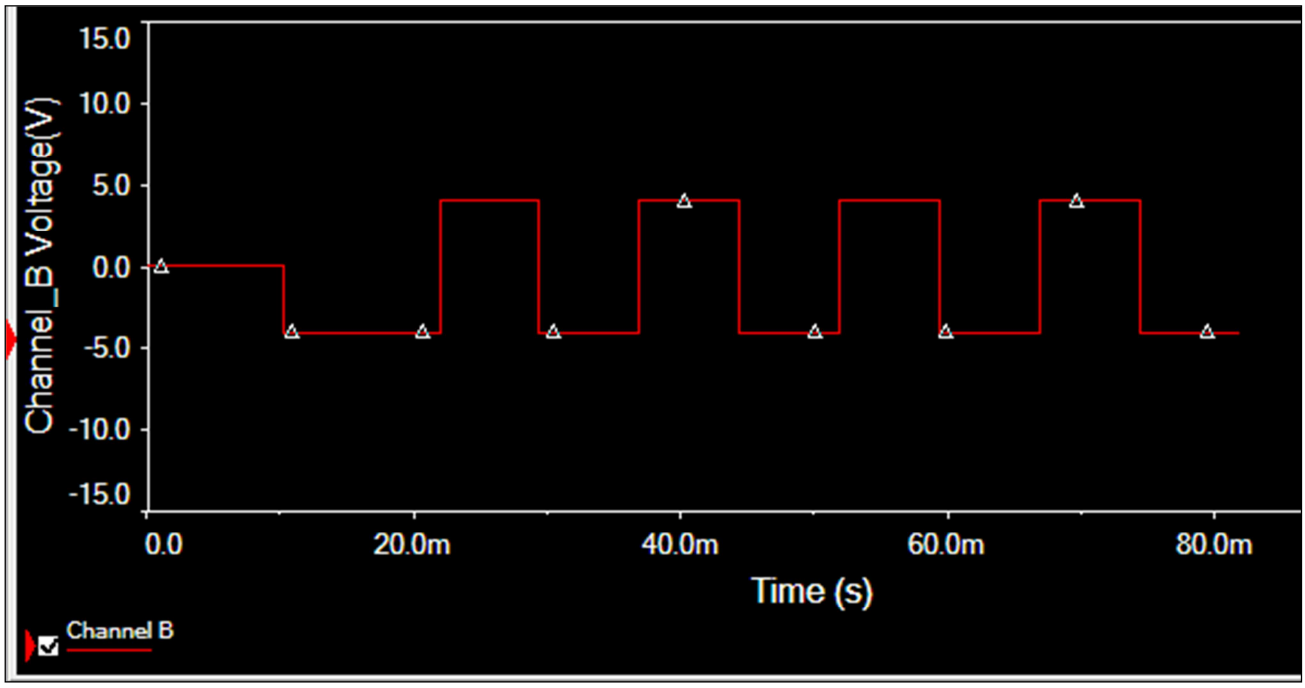

Figure 6. *Li-Fi Evalution Against Availability – Receiver Section*

Figure 6 shows that the received signal also had an amplitude of 5 volts, just like the transmitted signal. The availability aspect is a condition in which data, information, and communication system are accessible and usable on a timely basis and in the required manner without special skills as a prerequisite for use. All these conditions were sustained as evident from Figure 5 and Figure 6.

5.3. Aunthetication

To determine whether authentication was achieved, multiple transmitters and a single receiver were employed. The idea was to emit different signals and establish whether the receiver can distinguish the transmitted signals. Figure 7 shows the two signals that were transmitted by two different

transmitters.

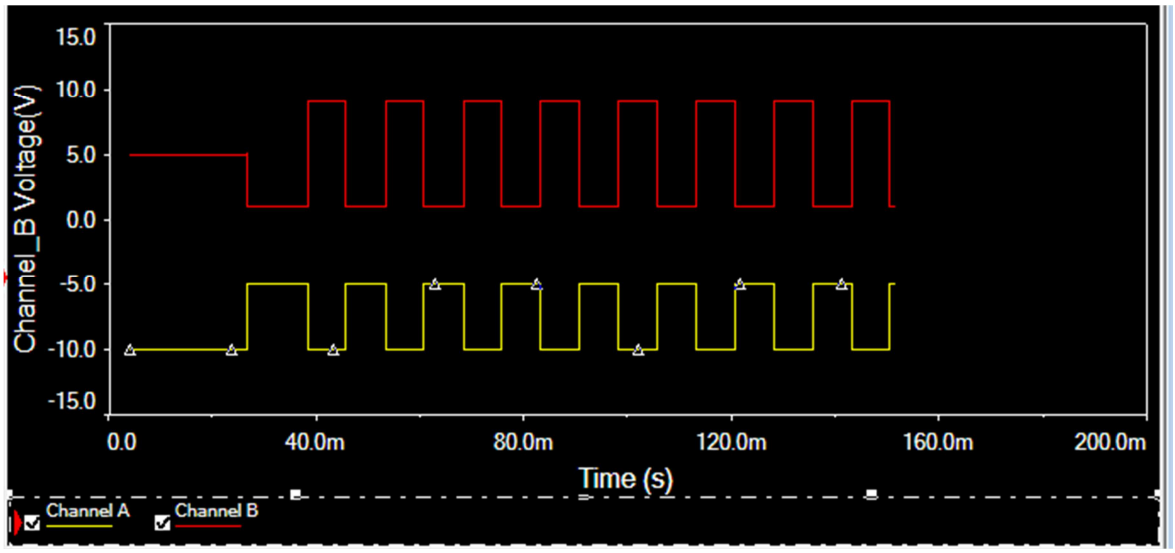

Figure 7. *Li-Fi Evalution Against Aunthenticity – Transmitters Section.*

As illustrated by Figre 7, the two signals were fairly similay, only that they were completely out of phase. This means that while channel A (from transmitter one) was at its peak, channel B (from transmitter two) was at its trough. Moreover, channel A had an amplitude of 10 volts while channel B had an amplitude of 5 volts.

The data in Figure 7 was then compared to the the reciever output shown in Figure 8 that follows.

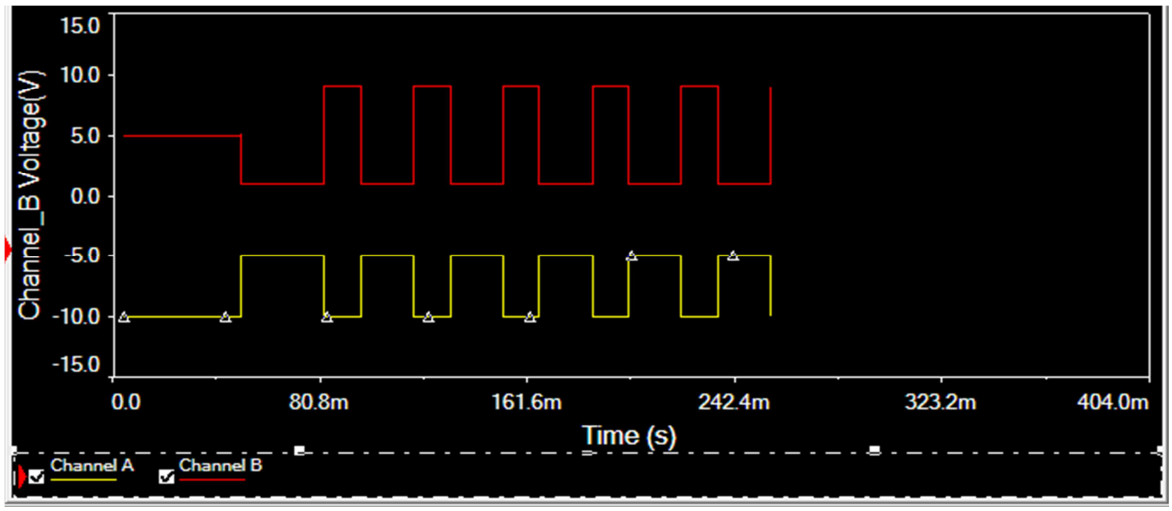

Figure 8. *Li-Fi Evalution Against Aunthenticity – Receiver Section.*

This figures demonstrates that at the receiver section, channel A maintained an amplitude of 10 volts while channel B also maintained an amplitude of 5 volts. The consequence of this is that the receiver distinguished the two transmitters with great precision.

In authentication, before sending and receiving data using the communication system, the receive and sender identity should be be verified and this was achieved as demostrated by the output in Figure 6 and Figure 7.

6. Conclusion and Recommendations

Wireless networks have found many applications, one of them being the establishment of hotspots. These hotspots have become popular in restaurants, vehicles, waiting bays and airports. However, the data being transmitted in these networks is not secured owing to the ease with which devices can establish connections to the wireless access points. This study sought to survey the current trends in wireless data propagation. This was meant to demonstrate how wireless network security can be compromised in the presence of authentication protocols. The protocols of interest were WEP, WPA and IEEE 802.X. the latest technology, which involves the usage of light signals for wireless data propagation was evaluated using four criteria: availability, integrity, confidentiality and authenticity. The results obtained demonstrated that Li-Fi is a better replacement of the authentication protocols from a security perspective. This is

inherent from its ability to assure that availability, integrity, confidentiality and authenticity of the wireless data transmissions is upheld.

References

[1] Abdul, M. (2010), "*WLAN Security",* Technical report, IDE1013.

[2] Zepnep,G., Halim, A and Ali, M. (2013), "*Security Mechanisms and Their Performance Impacts On wireless Local Area Networks"*.

[3] Karen, S. and Cyrus, T. (2008), "*Guide to Security Legacy IEEE 802.11 Wireless Networks*", NIST Special Publication 800-48 Revision 1.

[4] Rico, R. (2012), "*Wireless Security Wi-Fi Protected Access 2 (WPA2)*".

[5] Mustafa and Samani. (2010), "*WEP and WPA Improvement*", Wireless Sensor Network.

[6] Alexander, G. (2011), "*Wired Equivalent Privacy (WEP) Functionality, weak points, Attacks"*.

[7] Vanhoef, Mathy and Frank. (2013), "*Practical Verification of WPA-TKIP Vulnerabilities",* Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security.

[8] Stefan, V. (2011), "*Brute forcing Wi-Fi Protected Setup"*.

[9] Halvorsen and Finn. (2009), "*An Improved Attack on TKIP, 5838. pp. 120–132"*.

[10] Vanhoef, Mathy, Piessens and Frank. (2014), "*Advanced Wi-Fi Attacks Using Commodity Hardware",* Proceedings of the 30th Annual Computer Security Applications Conference.

[11] Van and Joris. (2010), "*WPA key calculation — From passphrase to hexadecimal key"*.

[12] Strand, L. (2014), "*802.1X Port−Based Authentication*".

[13] Kak, A. (2014), *"Computer and Network Security"*.

[14] Jason, B. (2011), *"Wireless Security"*.

[15] Jonsson, J. (2010), "*On the Security of CTR + CBC-MAC"*.

[16] Rani, J., Prerna, C and Tripathi, R. (2012), *"Li-Fi (Light Fidelity)-The future technology In Wireless communication"*, International Journal of Applied Engineering Research.

[17] Matthew H. (2013), *"Implementation of LiFi Technology"*.

[18] Rahaim, M and Vegni, B. (2011), "*A hybrid radio frequency and broadcast visible light data Propagation system*", In [IEEE Global Communications Conference (GLOBECOM 2011) Workshops].

[19] Suilivian, D. (2012),*"Criteria for network security Evaluation"*.

[20] Chia, T. (2012), *"Confidentiality, integrity, Availability: The three components of the CIAT Traid"*.