Simulation of Light –Fidelity Technology for Secure Data Propagation in a Barricaded Hotspot

Peter Sungu Nyakomitta
School of Computing and IT, Jomo Kenyatta University of Agriculture and Technology, P O Box 62000-00200.

Cheruiyot Wilson. Kipruto
School of Computing and IT, Jomo Kenyatta University of Agriculture and Technology, P O Box 62000-00200.

Agnes Naliaka Mindila
School of Computing and IT, Jomo Kenyatta University of Agriculture and Technology, P O Box 62000-00200.

Abstract – Light Fidelity is a technology that has received attention in the recent years due to its ability to achieve high multiplexing by combining many data sources together and transmitting their data through wireless means. This networking technology permits the propagation of data through illumination by use of light emitting diodes, which is then received by the photo-detectors located at the destination devices. These diodes vary in light intensity faster than the human eye can trail. They are normally equipped with a circuit that modulates the light imperceptibly for optical data transmission. Li-Fi data is transmitted by the LEDs located at the transmitter and received by photoreceptors situated at the destination side. 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 bulbs flicker on and off to give different strings of 1s and 0s. Since the LED intensity is modulated so rapidly that human eye cannot recognize, it makes the output to appear invariable to an observer. In this paper, this technology was simulated to demonstrate how it can be utilized on a different perspective: to enhance network security in wireless hotspot.

Index Terms – Light fidelity, propagation, security, hotspot, Light Emitting Diode (LED).

1. INTRODUCTION

Light fidelity technology is a technology that has received interest in the current years due to its capability to achieve high multiplexing as a result of combining thousands of data sources (Jay, 2014). The Li-Fi communication system consists of a data input, transmitter and a receiver. The transmitter section is composed of the data input, Binary converter and high illumination light emitting diode. The data input is responsible for capturing the analogue data that is to be transmitted, which is then converted to digital/binary format before being fed to the light emitting diode driver. This circuit essentially transfers the electrical pulses to the LED which then couples this energy into the wireless medium. This forms the transmitted signal.

Figure 1 that follows shows the transmitter section of the Li-Fi communication system. On the other hand, the receiver section comprises of the photo-diode receiver (photo- sensor), double stage inverting amplifier, message converter and the output signal as shown in Figure 2.

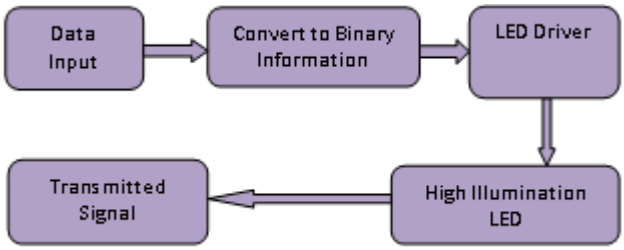

Figure 1: Li-Fi Transmitter Section

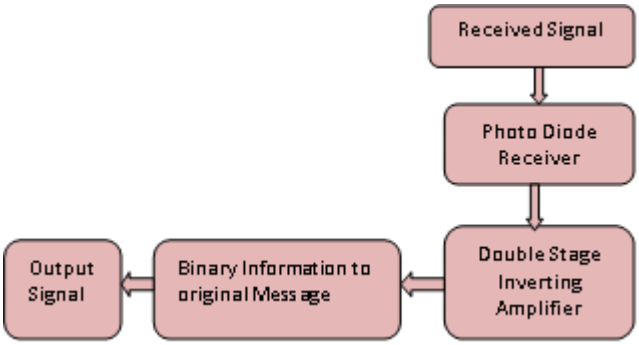

Figure 2: Li-Fi Receiver Section

It is clear from these two diagrams that it is very complex to practically implement Li-Fi communication Technology, many electrical circuitry and skills are required, which may not be readily available for actual construction of the circuit as used in this study. The study will therefore simulate this technology using Virtual components.

Therefore, a simulation approach was adopted for this study. Simulation is the replication of the operation of the actual

process or system. This requires that a model be first develop. The model represents the key characteristics of the actual process or system. It represents the system itself, whereas the simulation represents the operation of the system over time (Harrison and Andrew, 2011). Figure 3 describes the model that was utilized in this scenario.

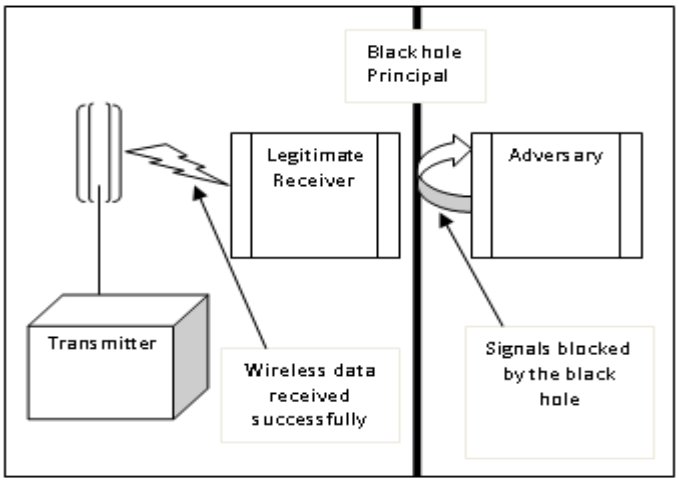

Figure 3: Li-Fi Conceptual Model

This figure shows that the conceptual model consisted of a wireless transmitter (which in this case was a light emitting diode). At the receiver side, both the legitimate terminal and the adversary are equipped with photo-sensors. In principle, the transmitted electrical pulses are to be received by the rightful users while the adversary does not get access to these electrical pulses. To achieve this, the concept of the black hole was employed, being represented by the thick dark line. The black hole principle emanates from the particle theory of light which argue that a body could be so massive that light could not escape from it. This line acts as a wall, effectively depriving an adversary access to the wireless transmitted data. This is represented by the arrow that bounces back to the adversary, indicating that his transmissions to the wireless transmitter were unsuccessful.

The operation of the model can be evaluated, and therefore, the characteristics concerning the behavior of the actual system or its subsystem can be inferred. In essence, simulation is a tool to evaluate the performance of a system, existing or proposed, under different configurations of interest and over long periods of real time. Simulation is employed for various reasons: to reduce the chances of failure to meet specifications; to eliminate unforeseen bottlenecks, to prevent under or over-utilization of resources and to optimize system performance (Leinonen, 2009).

In this paper, the operation of light fidelity data propagation was simulated using the National Instrument (NI) multi-simulation (Multi-Sim) software. The goal was to determine if this technology can be used instead of Wi-Fi in order to eliminate the security challenges posed by the latter.

2. WIRELESS NETWORKS SECURITY TECHNOLOGIES

Wireless networks are exposed to many attacks such as shared key decryption. Worse still, these attacks can be launched from a remote location, unlike in wired networks where one needs physical connections to the network of interest to compromise it. 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 (Karen et al, 2008).

According to Hassan and Challal, (2010), the main weaknesses of WEP are that: In maintaining a shared WEP key it has disabled a high percentage of wireless networks; since the shared key secret is held by another person, the private key becomes public key; The initialization vectors (IVs) that seeds the WEP algorithm is sent in the secret; and the WEP checksum is linear and predictable.

To overcome the drawbacks of WEP, WPA came into existence.WPA is the subset of the Institute of electrical and electronics engineers' (IEEE's) 802.11i wireless security specification. WPA uses an encryption method called Temporal Key Integrity protocol (TKIP). The setbacks of WEP addressed by TKIP include the mixing of functions, employing message integrity check, utilization of an extended initialization vector, and a re-keying mechanism. WPA depends upon central authentication, called the radius server, to authenticate each client (Habibi, 2009).

The chief challenge of WPA is that it utilizes Pre-shared Keys (PSKs). This is considered to be a substitute authentication device for small business and home client that do not need to use the individual authentication server and entire 802.1 x key architecture. Moreover, WPA makes use of handshake mechanism to interchange the data encryption keys for the wireless session between the access point and the end user (Habibi, 2009). This is disastrous because an intruder may not know the PSK being used, but can still employ intrusion techniques such as dictionary attack or brute force attack to guess it.

The latest version of WPA is the WPA 2. Its main demerits are that it is costly to implement for the already deployed networks. This is due to the fact that it requires a new encryption scheme, known as Counter-Mode/CBC-Mac Protocol (CCMP) and Advanced Encryption Standard (AES). These two protocols require that the overall hardware for the network is altered. Moreover, WPA 2 is fully depended on secrecy session keys; hence the network is prone to attacks (Pervaiz et al, 2011).

The main function of using the IEEE 802.1X standard is to provide the port based network access control. According to Abdul, (2010), the challenge of the 802.1x protocol is that it circumvents the single authentication procedure over a new process (Terry, 2012). Moreover, it requires a Remote Authentication Dial-In User Service (RADIUS) server which adds additional costs to its implementations.

3. LIGHT FIDELITY AND HOTSPOT SECURITY

Li-Fi is a wireless networking technology that allows the propagation of data through illumination by use of a light emitting diode (LED) bulb. These LEDs vary in intensity faster than the human eye can follow hence appearing invariable to a human observer. The bulbs are equipped with a circuit that modulates the light imperceptibly for optical data transmission. Li-Fi data is transmitted by the LED bulbs and received by photoreceptors. 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 then becomes possible to encode data in the light by varying the rate at which the light emitting diode bulbs flicker on and off to give different strings of 1s and 0s.

However, in this paper, the researcher sought to explore the security aspect of Li-Fi technology. To put this concept into context, simulation approach was adopted. The simulation set up comprised of a sender, LED source, legitimate receiver and an adversary as shown in Figure 2. It is important to note that the sender can receive the information from the receivers if it is equipped with a photo detector, which converted the light energy into electrical pulses. The diagram also includes an adversary, who was trying to access the hotspot resources. However, since light travels in a straight line and cannot penetrate through walls, the adversary was effectively isolated from the coverage area because he cannot receive the light signals. This is unlike a Wi-Fi setup which can penetrate through walls and hence can be detected by an adversary located outside the barricade hotspot so long he is equipped with a radio receiver.

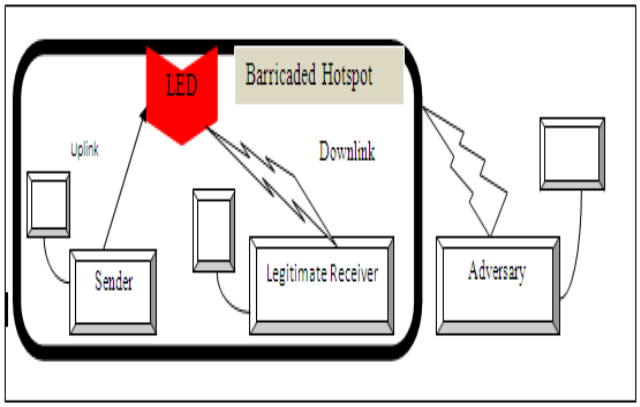

Figure 4: Simulation Design

As already noted, the NI Multi-Sim software was employed. The following steps were adopted in the development of this simulation: component identification to determine the ideal equipment or this technology; generation of a netlist of all the components; laying of the components on the design window; section optimization; and development of the final attuned set up. Figure 5 shows the layout of the components on the design window.

The function generator was employed to generate square waveforms, which were essentially digital signals. The opto-coupler was used to transfer electrical signals between two isolated circuits by using light signals. The two circuits were the transmitter section and the receiver section. The transmitter section was used to send a digital signal along the communication network. This digital signal could represent any data such as text, video and sound. The receiver section on the other hand was used to pick the signal from the communication media and feed it to the legitimate user. The receiver section on the other hand was used to pick the signal from the communication media and feed it to the legitimate user. The connection between the transmitter and the transmitter was wireless. The signal was transferred from the transmitter to the receiver via light as shown in Figure 5.

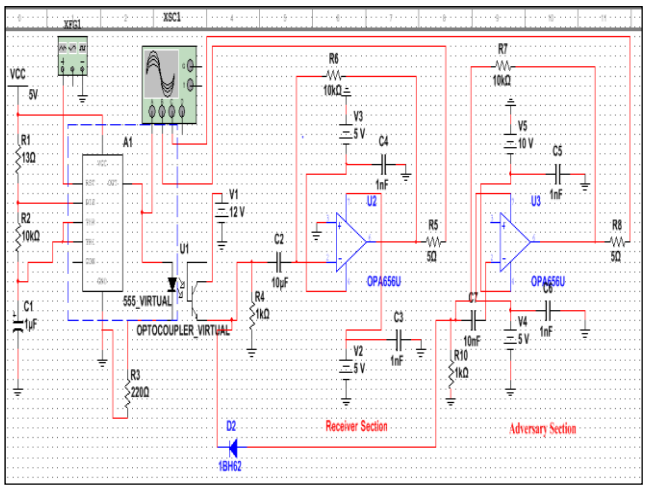

Figure 5: NI Multisim Simulation Set up with Legitimate Receiver

The inverting amplifier was used in the receiver section to produces a 180 degree phase shift in the transmitted signal from the 555 timer output, so as to make a mirror image of the original signal from the function generator.

The oscilloscope was used to display the output from the various sections of the experimental setup. To illustrate the fact that an intruder (a receiver that cannot get illuminated by the light signals) located outside the barricade hotspot cannot get access to the network data, a reverse-biased diode was used as a representation of the wall that ensured that light did not leak

to the outside of the hotspot. This setup was therefore modified as shown in Figure 5, under the section labeled 'Adversary'.

Finally, a reverse-biased diode was added in the setup which resembled that of the legitimate receiver. When a diode is reverse-biased, it does not conduct current, and therefore the components in the adversary's receiver were effectively barred from the light emitted by the opto-coupler, just the same way a wall would do to the receiver located outside the barricade hotspot.

The basis for the calibration of the components such as capacitors and resistors was done from the first principles of circuit theory. A close observation of the circuit in Figure 3.2 reveals that the components were connected in series. As an illustration, we consider the two resistors in the transmitter section. Electrical circuits normally consist of very complicated combinations of resistors. It then becomes valuable to have a set of rules for calculating the equivalent resistance of some general arrangement of resistors. In practical circuits, resistors can either be connected in series or in parallel. However since the resistors in our case are in series, only this type of connections is considered here.

As an illustration, the two resistors in the transmitter section can be interpreted as being connected as shown in Figure 6.

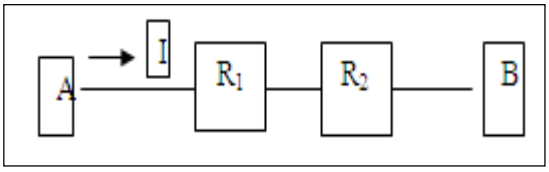

Figure 7: Resistors Connected In Series

In a series connection, the same current *I* flows through both resistors R_1 and R_2. Taking that the potential drop from point A to point B as V, this drop is the sum of the potential drops V1 and V_2 across the two resistors R_1 and R_2 respectively

Since V=IR, it is clear that voltage in a series connection increases with the increase in the individual resistances of the two resistors. The capacitors were introduced to store charge till it reaches a certain recommended level before it is fed to the 555 timer. This feature is called buffering and was employed to prevent circuit fluctuations.

4. RESULTS AND DISCUSSIONS

The study results were obtained by running the simulation setup. This was done by running the simulation from the menu as illustrated in Figure 4.

To view the waveforms from the four-channel oscilloscope, grapher view was selected from the view menu as shown in Figure 5. In the following sub-sectionals, the data obtained from the three channels is given and the discussions originating from this data is also provided.

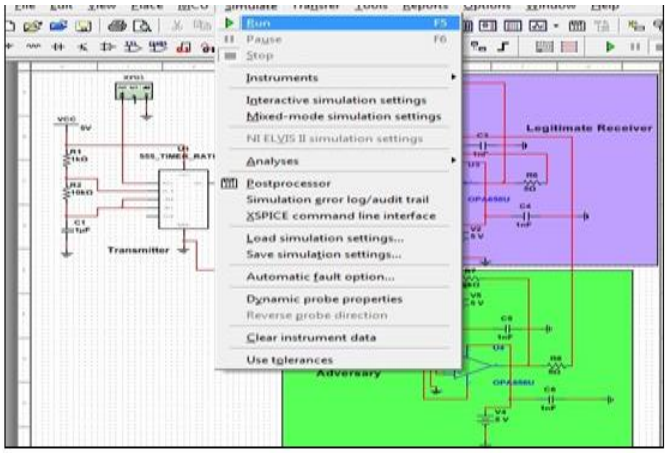

Figure 6: Running Simulation

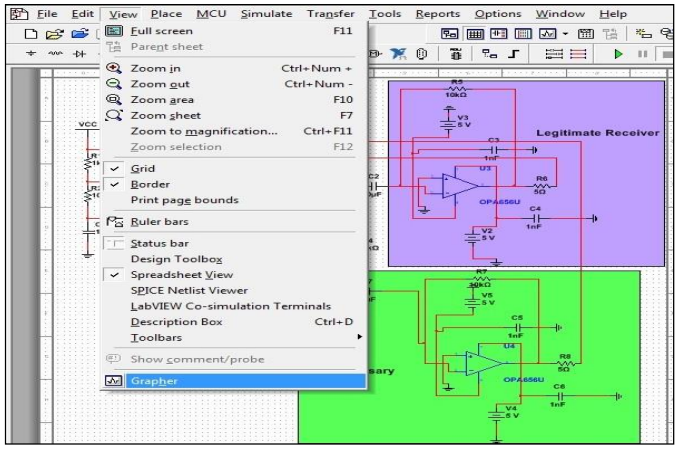

Figure 8: Grapher View Selection

4.1 Transmitter Output

To probe the transmitter data, the output of the 555 timer was used. The connection was established from the 'out' pin of the timer and fed to channel A of the oscilloscope. All the other channels were disconnected to yield the data shown in Figure 6. The 0.0 voltage level in channel A indicated logic level zero (0). On the other hand, the 5.0 voltage level in channel A indicated logic 1. It was observed that this signal moves from 0.0 to 5.0 and no any other location, confirming that this is an ideal digital signal. It was interesting to note that the LI-FI equipment took 22 milliseconds to respond to the trigger voltage as indicated by the lagging of the initial response of the transmitter. The lower left section indicates the channel currently under investigation, which is channel A for this case. This is due to the fact that the trigger voltage had to first power every LI-FI component before they could give their output. Afterwards, the signal took 10 milliseconds to make one complete oscillation (cycle).

4.2 Legitimate Receiver

To probe the output of the legitimate user, all other channels were disconnected remaining with only channel B. The output of the inverting amplifier was fed to channel B of the four-channel oscilloscope to yield the data shown in Figure 6.

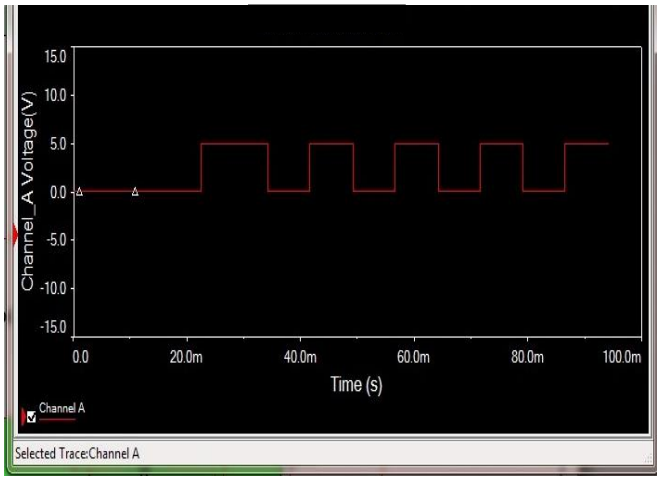

Figure 9: Transmitter Output

Once again, it took 22 milliseconds to power the LI-FI equipment before they could start giving an output. Unlike the firs scenario where logic zero was indicated by the 0.0 voltage level, logic zero at the legitimate receiver is indicated by -5.0 voltage level. Logic 1 on the other hand was indicated by the 5.0 voltage level. Moreover, the signal took 10 milliseconds to make one complete cycles, just like was the case for the transmitter output. The selected channel under investigation is B, as shown on the bottom left side section of Figure 7.

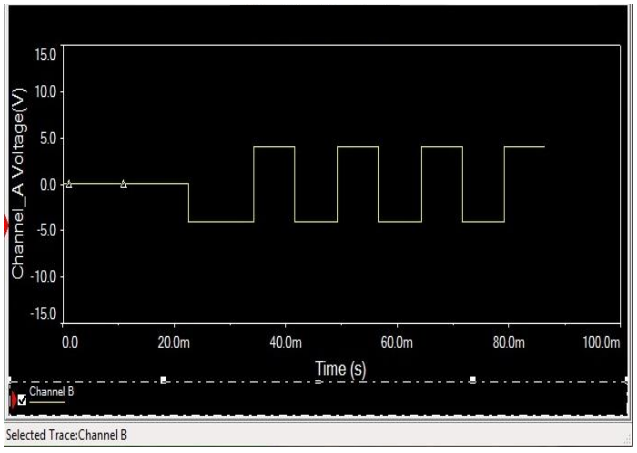

Figure 10: Legitimate Receiver Output

4.3 Adversary Output

As already stated, in a real network environment, an adversary is anybody who is located outside the barricaded hotspot area and therefore not eligible to get network data.

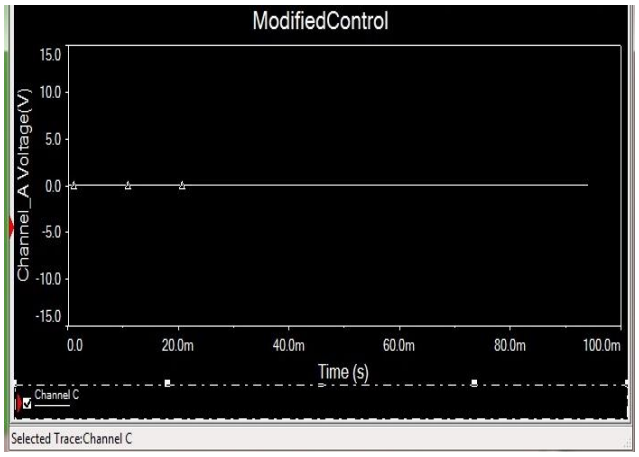

Figure 11: Adversary Output

Since light cannot pass through walls, this separation could be simulated by use of a wall between the adversary and the opto-coupler. The solution was to employ the diode which is reverse-biased, and hence cannot conduct current, between the opto-coupler and the adversary. To probe the output from the adversary, the output of the inverting amplifier was connected to channel C of the four-channel oscilloscope. The data obtained is shown in Figure 8. This was done by disconnecting all other devices, leaving alone channel C.

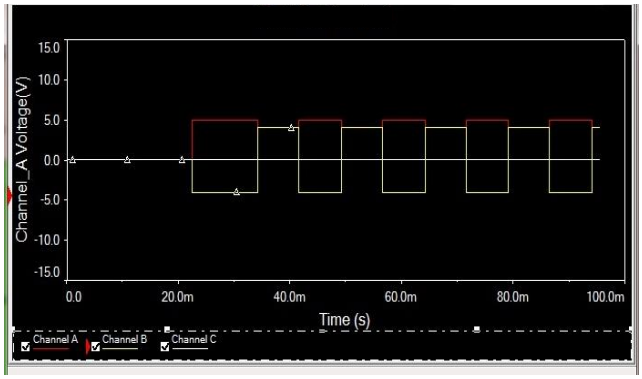

Figure 12: Legitimate users and Adversary Output

The figure demonstrates the fact that the adversary was effectively barred from the LI-FI communication network. This was evident from the persistence of the output at the 0.0 voltage level, which essentially indicated no signal output as confirmed in Figure 9.

5. CONCLUSIONS

In a Wi-Fi setup, authentication schemes are used to grant or deny wireless devices to the network. These schemes include Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Wi-Fi Protected Access version 2 (WPA2) is the later version of WPA. However, these protocols have been shown to be easily compromised. The ease with which these schemes can

be attacked depend on factors such as the initialization vectors (IV), the key generation function and the salting being employed. Weak IV, generation functions and salting renders the authentication scheme easy to guess and the key can be decrypted by learning these three features.

This study employed a different approach to wireless security by using light technology for signal transmission and reception. This study was important in addressing the security challenges that have been inherent in wireless environments such as brute forcing and dictionary attacks to get the authentication keys. The scope of this study was limited to wireless network security. A simulation research design was adopted as it encompassed the practical design and simulations of wireless communications using light technology. The persistence of the adversary at the logic zero level indicate that indeed the attacker was effectively network partitioned and therefore unable to access network data.

REFERENCES

[1] Jay H. (2014), "LI-FI Technology – A Visible Light Communication", International Journal Of Engineering Development And Research.
[2] Harrison and Andrew. (2011), "Throwing and catching movements exhibit post-activation potentiation effects following fatigue", Sports Biomechanics 10 (3): 185–196.
[3] Leinonen, H. (2009), "Simulation analyses and stress testing of payment networks", Bank of Finland Studies, Simulation publications.
[4] Karen, S. and Cyrus, T. (2008), "Guide to Security Legacy IEEE 802.11 Wireless Networks", NIST Special Publication 800-48 Revision 1.
[5] Hassan, H. And Challal, Y. (2010), "Enhanced WEP: An efficient solution to WEP threats".
[6] Habibi, A. (2009), ''Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)", International conference on Signal Processing Systems, Singapur.
[7] Pervaiz M., Cardei, M and Wu, J. (2011), "Security in wire-less local area networks", Department of Computer Sci-ence & Engine.
[8] Abdul, M. (2010), "WLAN Security", Technical report, IDE1013.
[9] Terry, C. (2012), "Confidentiality, Integrity, Availability: The three components of the CIA Triad", IT Security Stack Exchange.

Authors

Peter Sungu Nyakomitta

Pursuing M s c. in Information Technology from Jomo Kenyatta University of Agriculture & Msc in Information Technology Security and Audit from Jaramogi Oginga Odinga University Of Science And Technology School Of Informatics And Innovative System (JOOUST). Received B s c. Information Technology from JKUAT, Kenya. His research interest is on the Simulation LI-FI Technology communication to enhanced wireless data security. He is a career banker with bias in ebanking systems.

Dr. Cheruiyot Wilson Kipruto

Received Bsc. In Statistics & Computer Science from Jomo Kenyatta University of Agriculture & Technology(JKUAT),Kenya; Msc.inComputer Application Technology, CentralSouth University(CSU),P.R.China; PhD in Computer Science &Technology ,Central South University (CSU) ChangshaP.R.China. Serving as a senior lecturer in School of Computing & Information Technology at JKUAT Kenya. His Research interest includes but not limited to: Multimedia Data Retrieval, Internet of Things, Evolutionary Computation for Optimization, Digital Image Processing and ICT for Development.

Dr. Agnes Naliaka Mindila

Dr. Agnes N. Mindila is a lecturer in the department of Computing at the School of Computing and Information technology (SCIT) of Jomo Kenyatta University of Agriculture and Technology (JKUAT). She holds PHD Information Technology from JKUAT. Her research interest is Information system Management, Wireless Sensor Networks, ICT for economic development, system dynamics application, system dynamics and big data analytics. She holds a Bachelor of Science degree in Electronic and Electronics engineering from JKUAT and a Master of Science degree in Management of Information Technology (MIT) OF University of Sunderland, UK.