Visible Light Communication based Authentication Protocol Designed for Location based Network Connectivity

Chathura P. Suduwella#1, Yohani S. Ranasinghe#2, Kasun de Zoysa#3

#University of Colombo School of Computing, No.35, Reid Avenue, Colombo 07, Sri Lanka

1cps@ucsc.cmb.ac.lk

2ysr@ucsc.cmb.ac.lk2

3kasun@ucsc.lk

***Abstract-* Visible Light Communication (VLC) is a blooming research area which uses visible light spectrum as the communication channel. Exponential growth of Light Emitting Diodes (LEDs) deployment as a light source is encouraged to use for communication purposes as well. With the introduction of VLC, LED can be used for communication while providing the primary function of illumination. Since location-based network access protocols have not been implemented for Wi-Fi devices, this research has been conducted with the intention of using VLC to perform location-based authentication. In our location authentication protocol, VLC technology is used for authentication purpose and Wi-Fi is used for data transfer once the device has been authenticated. The proposed protocol provides location-based connectivity to Wi-Fi devices with minimum changes to Remote Authentication Dial-In User Service (RADIUS) and Wi-Fi Protected Access 2 (WPA2) protocol by using VLC.**

***Keywords*- VLC, Location Based Connectivity, Wi-Fi Authentication Protocol**

1. INTRODUCTION

In recent years with the bloom of the field of solid state, lighting leads to the replacement of florescent lamps by Light Emitting Diodes (LEDs) which further motivates the usage of Visible Light for communication (VLC). Exponential growth in LED usage which has been experienced, may have caused opening up researchers' eye towards exploring methods to use already existing, widely available LED infrastructure to use as the communication medium which finally resulted in using the visual light spectrum for data transfer[1]. Visible Light Communication or VLC is a novel communication method that most researches have put faith on to become the communication technology of the next generation. It uses Light Emitting Diodes’ (LED) ability to switch into different intensity levels at a fast rate to transfer data[1-2]. LEDs will be the future of modern lighting system as they enjoy many advantages over conventional lighting devices. LED is known to be an efficient illumination source. The VLC technology in addition to illumination is also used to send information using the same light signal. In literal terms, any information that can be sent using a light signal that can be visible to the human eye is considered to be VLC but most importantly light should be visible to humans but not the data we transfer through it.

The opportunity to send data usefully in this manner has largely arisen and under research because of the widespread use of LED light bulbs. We can switch LEDs at very high speed that was not possible with older light sources such as fluorescent and incandescent lamps. The adaptation of LED light bulbs during the last few years has created a massive opportunity for VLC. The problem of congestion of the radio spectrum utilized by Wi-Fi is also helping to the improvement of VLC. The Radio Frequency (RF) communication suffers from high latency and interference issues and also it requires a separate setup for transmission and reception of RF waves. Overcoming the above mentioned issues VLC can be used as a preferred communication technique because of its high bandwidth and immunity to interference from electromagnetic sources.

The world has moved to use wireless technology decades ago replacing the wired technologies available for Internet connectivity. Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections with devices based on the IEEE 802.11 standards [3]. Wi-Fi is the widely used wireless technology to connect with the global Internet. In Wi-Fi when an RF current is supplied to an antenna, an electromagnetic field is created that is able to propagate through space. The main component of a wireless network is a device known as an Access Point (AP). The primary job of an access point is to broadcast a wireless signal that can be detected by computers and "tune" into. That is the main problem that we have identified in the available Wi-Fi technology. When establishing a Wi-Fi connection there is a 3 step process to get connect to an AP or wireless router where authentication happens. Same RF is used to share the secret key in the existing Wi-Fi technology. Thus, if the Wi-Fi has not given an open access, users, who are connecting need to provide user name and password to authenticate at least once. The problem here is anyone within the range of the Wi-Fi can get access once they have authenticated and if not forget.

Through this paper, we are proposing a novel protocol for location dependent Internet connectivity using VLC. This authentication protocol mainly depends on VLC to share the secret key for user authentication and once authenticated, available Wi-Fi technology can be used for data transfer. Our main target is to provide location-based Internet access which will ultimately result in more restricted access to Wi-Fi where more sensitive and confidential data transfer is required. The available Wi-Fi access points use password authentication but anyone within the range of the access point who has the password can get access. However using this novel protocol we can restrict the access to a single indoor location or a room. The proposed protocol uses the existing infrastructure to achieve its objective.

1. TECHNICAL BACKGROUND
   1. *Visible Light Communication*

Visible Light Communication acronym as VLC is a novel communication method which uses LEDs’ ability to switch into different intensity levels at a fast rate. It is a short range optical wireless communication using visible light spectrum (Fig 01) from 380 to 750 nm [4]. VLC uses LED luminaries for high speed data transfer. LED adaptation has continuously increased and it is expected 75% of total usage by 2030 and this rapid increase in LED usage provides a unique opportunity for communication [4]. LED’s ability to switch into different intensity levels at a very fast rate can be used to transfer data at a high speed without being detected by the human eye [5]–[7]. The idea is to encode the data and send through emitting light and using a photo detector detect at the other end as modulated signals and decode them. Therefore LED is dual purpose, one way as a light source and in the other way as a data communication method. In other terms, it can be used for illumination as well as communication. According to [4] recent research on VLC has shown a very high data rates up to 100Mbps in IEEE 802.15.7 standard and several Gbps in research.

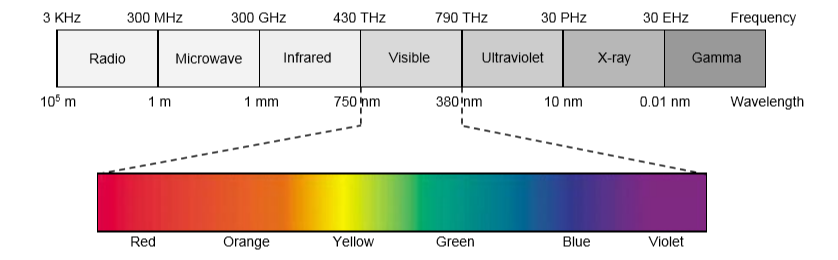


Fig.1: Visible Light Spectrum

It was shown in [8] that ﬂickering can cause serious detrimental physiological changes in humans. For this reason, it is necessary to have changes in the light intensity at a rate faster than a human eye can perceive. IEEE 802.15.7 standard [9] suggests that ﬂickering (or change in light intensity) should be faster than 200 Hz to avoid any harmful effect. That means high data rate will be provided by any VLC system.

Communication through visible light is important due to many reasons [4]. Firstly, mobile data traffic has increased exponentially in the last two decades and it has proved the fact that RF spectrum is scared to meet ever increasing demand. Compared to that the visible light spectrum is completely untapped for communication and it includes terahertz of unused free bandwidth. Secondly, due to its high frequency, it cannot penetrate through most of the objects and walls. This characteristic allows one to create small cells of LED transmitters with no inter-cell interference issues beyond the walls and partitions. The inability of signals to penetrate through the walls provides an inherent wireless communication security. Thirdly it allows us to use the existing lighting infrastructure for communication as well. Therefore VLC systems can be deployed with less cost and effort. The above reasons motivate us to use VLC for building location-based wireless communication protocol.

In any VLC system, there are two main parts involved, one is the transmitter and the other one is the receiver. LED luminaire is the transmitter of any VLC system. The most important design aspect of a VLC system is that it should not affect the illumination, which is the primary purpose of the luminaire, due to the communication usage. There are two types of receivers; photodetector and image sensor [4]. The image sensor can allow any mobile device with a camera to receive visible light communication. However, this can provide very limited throughput (few Kbps) due to its low sampling rate. However, stand-alone photodetectors have a signiﬁcantly higher throughput (hundreds of Mbps). In this research, we have used the receiver to be the photodetector in the initial prototype design and the target in future is to replace it with an image sensor, in other words by the camera of the laptop or the mobile device.

1. *Wireless Communication and Connection Establishment*

Wireless communication is widespread due to its advantages over wired connections [10]. When connecting to a wireless network it is required to select the Access Point (AP) first using the Service Set Identifier (SSID) and if it is secured, a dialog prompts for authentication. Connecting to an AP is a 3 step process. Three steps involved are Discovery, Authentication & Association [11].

During the discovery process, the device needs to be connected to the AP listen for beacon frames broadcasted in regular intervals by the AP. When a user tries to connect to the AP, the device sends an authentication request to the AP.

The Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.11 standard defines two link-level types of authentication: Open System and Shared Key[12]. Open system authentication consists of two communications. First, an authentication request is sent from the device. Then, an authentication response from the AP/router with a success or failure message will receive. With shared key authentication, a shared key or passphrase is manually set on both the mobile device and the AP/router. Several types of shared key authentication such as WEP, WPA, and WPA2 are available. Only those wireless clients who have the shared key can connect. If there are no passwords set for AP it will be automatically connected same as open Wi-Fi connectivity. But for a password protected Wi-Fi, the AP replies to the authentication request with a challenge in form of text to the device. At this point, we need to provide the password. Then the device encrypts the challenge text sent by the AP with the password and sends back to AP. If the correct password has entered, then the decrypted response will match the initial challenge sent to your device by the AP earlier and then the association stage is initiated with the AP telling the machine that the authentication was successful.

Once authenticated machine will send an association request to AP and once the association acceptance message is received only the device can start transferring data. In the association process, AP and the device get into certain agreements such as the network model, security parameters (either WEP, WPA or WAP2), encryption method (TKIP, CCMP, AES) and channel frequency.

1. *Data Security in Wireless Networks*

To detect a wireless network all we need is a wireless-equipped device. There is no way to selectively hide the presence of a wireless network from strangers, but prevention of unauthorized people from connecting can be done, and thus can protect the data traveling across the network. Scrambling the data and controlling access to the network can be done by turning on a wireless network's encryption feature. Mentioned below are the most widely used security protocols in wireless networks to provide security and privacy.

*1) Wired Equivalent Privacy (WEP)*

WEP is not recommended for a secure WLAN. Static client keys for access control made WEP cryptographically weak. The main security risk is the hackers capturing the encrypted form of an authentication response frame, using widely available software applications and using the information to crack WEP encryption.

*2) Wi-Fi Protected Access (WPA)*

WPA complies with the wireless security standard and strongly increases the level of data protection and access control (authentication) for a wireless network. WPA enforces IEEE 802.1X authentication and key-exchange and only works with dynamic encryption keys. A common pre-shared key (PSK) must be manually configured on both the client and AP/router.

*3) Wi-Fi Protected Access 2 (WPA2)*

WPA2 is a security enhancement to WPA. Users must ensure the fact that the mobile device and AP/router are configured using the same WPA version and pre-shared key (PSK).

Key distribution is an important issue in wireless networks. To secure communication between two nodes, a shared cryptographic key between the two nodes must be established. Random key pre-distribution systems provide an efficient approach to the key establishment in such networks that guarantee security against passive attackers.

1. *How 802.1x authentication works*

The architecture of 802.1x protocol has three main components known as supplicant, access point and authentication server such as Remote Authentication Dial-In User Service (RADIUS). The authentication process begins when the end user attempts to connect to the WLAN. The authenticator or the AP acts as a proxy for the end user passing authentication information to and from the authentication server. The client may send an Extensible Authentication Protocol (EAP) start message. The access point sends an EAP-request identity message. The client's EAP-response packet with the client's identity is "proxied" to the authentication server by the authenticator. The authentication server challenges the client to prove themselves and may send its credentials to prove itself to the client. The client checks the server's credentials and then sends its credentials to the server to prove itself. The authentication server accepts or rejects the client's request for a connection. If the end user was accepted, the AP changes the virtual port with the end user to an authorized state allowing full network access to that end user. At log-off, the client virtual port is changed back to the unauthorized state.

1. *Remote Authentication Dial-In User Service (RADIUS) Protocol*

Remote authentication dial-in user service or RADIUS is an authentication system that has been used to secure networks. A wireless RADIUS server uses a protocol called 802.1X, which governs the sequence of authentication-related messages that go between the user’s device, the wireless access point (AP), and the RADIUS server. When a user wants to connect to a Wi-Fi network with RADIUS authentication, the device establishes a communication with the AP, and requests access to the network. The AP passes the request to the RADIUS server, which returns a credential request back to the user via the AP. The user provides the proper user name and password, which the RADIUS server checks against the authentication directory. If the credentials are correct, the RADIUS server informs the AP to allow the user access to the network.

When a user authenticates an SSID using 802.1X, that individual session is encrypted uniquely between the user and the access point. This means that another user connected to the same SSID cannot sniff the traffic and acquire information because they will have a different encryption key for their connection. With a Pre-Shared Key (PSK) network, every device connected to the access point is on a "shared encryption". If you need to de-auth a particular user or device, having RADIUS makes this much easier because you disconnect a single user or device without having to change the key for everyone or allow that potential security risk of that user re-joining the network with the known access key. This special feature has used in the proposed VLC based authentication protocol where keys are dynamically expiring and issuing new keys to ensure the location-based connectivity.

Common home-use Wi-Fi networks may not need a RADIUS server because they "secure" the network with one single network key, the "WPA/WPA2 Pre-Shared Key" (PSK). That key which is same for every user, is often guessable, and can't be revoked for one user. When a network is sniffed, an attacker can perform offline attacks to guess the key. To provide location constraints, it is mandatory to refresh the key which is assigned to a particular location time to time and allows the user to get the key through a VLC enabled LED placed inside the room.

1. PROTOCOL DESIGN

The main intention of the proposed protocol is to provide location based access to the wireless networks. Already available method to connect to a Wi-Fi network uses the same RF for both authentication and data transfer after successful authentication. The architecture of the RADIUS based authentication protocol contains three major components; Access Point, RADIUS Server, and the client, communicating with each other before connection establishment.

The architecture of the proposed protocol has four major components. RADIUS Server VLC Module which is a Li-Fi authentication enabled module in RADIUS Server, VLC enabled LED, Access Point, and the client. The proposed protocol uses VLC for key distribution. The authentication process of the proposed protocol is given step by step in Fig 02.

E:\UCSC\ResearchWork\VLC\Untitled Diagram (1).png

Fig.02: Communication process of the proposed protocol

*A. Prerequisites for Authentication*

* VLC authentication enabled RADIUS module
* VLC enabled bulb with a unique ID ( VLC\_ID) and a key (VLC\_KEY)
* VLC bulb should be registered on RADIUS server VLC module with VLC\_ID, VLC\_KEY (attached with the LED).
* AUTH\_KEY is generated by the RADIUS server VLC module. This is a timely key.
  + AUTH\_KEY should be updated periodically.
* VLC enabled LED should emit VLC\_ID periodically.
* VLC enabled LED should emit AUTH\_KEY upon request periodically.

*B. Communication Protocol*

1. Client/ the device requests Wi-Fi access from the Access Point (AP)

2. AP will send an Identity request to the client.

3. The device detects the VLC\_ID emitting periodically by the LED and reads it using the receiver in the device.

4. Then it is sent as the user name (VLC\_ID) with the reply message to the AP which will relay to RADIUS server.

5. Once the reply reached to the RADIUS server, it gets the AUTH\_KEY and VLC\_KEY relevant to VLC\_ID and AES encrypt AUTH\_KEY using VLC\_KEY, and then send to VLC bulb via Wi-Fi.

a. VLC bulb: decrypt AUTH\_KEY using the VLC\_KEY and emitting plain AUTH\_KEY via VLC.

6. At the same time RADIUS server sends Authentication challenge to the client via AP.

7. The client reads VLC emitting AUTH\_KEY and response to challenge using AUTH\_KEY to RADIUS server via AP.

8. RADIUS server matches the AUTH\_KEY in the server database with the AUTH\_KEY in the reply message.

9. RADIUS server sends authentication success to AP.

10. AP will grant connectivity to the Wi-Fi network.

Connecting device should be within the same room where key sharing VLC enabled LED is available. Since the visible light is not propagating through walls, clients outside the room cannot read KEY\_ID or AUTH\_KEY.

Each VLC enabled LED comes with a unique ID for the bulb and a random key. The key and the ID should be registered on the Li-Fi Authentication enabled module embedded to RADIUS server. These VLC\_ID and VLC\_KEY can be changed if necessary.

Communication starts when a device needs to connect to the Wi-Fi network and sends a connection request. This communication uses normal RF channels.

Once the authentication is completed, access to the Wi-Fi connection is granted and from that onwards already available Wi-Fi infrastructure and RF are used to transfer data and to connect to the Internet.

Proposed protocol has session timeouts to ensure that the above mentioned cycle will repeatedly happen within predefined time intervals. AUTH\_KEY is also a timely key which times out. Then the device that wants to get access needs to be near the VLC device to have a continuous connectivity, otherwise, the device will remain connected only until time out. Thus this proposed protocol ensures the location-based connectivity to Wi-Fi networks.

*C. Message Format*

A simple message format has been designed to share VLC\_ID and the AUTH\_KEY. The message format for VLC communication is given in Fig. 3.

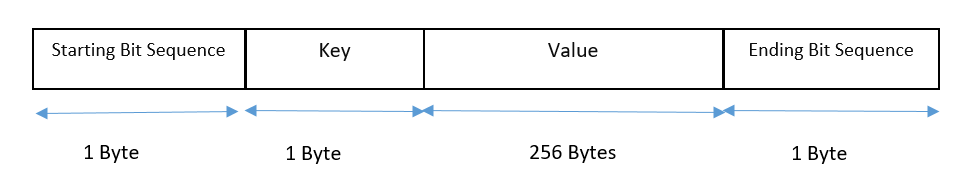


Fig 03: VLC message format

1. PROOF OF CONCEPT DEVELOPMENT

Proof of concept authentication platform has been developed using the proposed protocol.

Photodiode sensor module has been attached to Arduino Uno and it is used as the VLC key reader. It is connected to the laptop computer (Fig. 04). Wi-Fi enabled LED light source is given in Fig.05.a and Fig.05.b. FreeRADIUS has been used as the Li-Fi Authentication server. Proposed protocol uses VLC for key exchange only for the authentication purposes. The Key exchange system including the photodiode sensor and LED light source is given in Fig. 06. At this initial stage in order to make the communication happen, the sender and the receiver should be placed in line of sight.

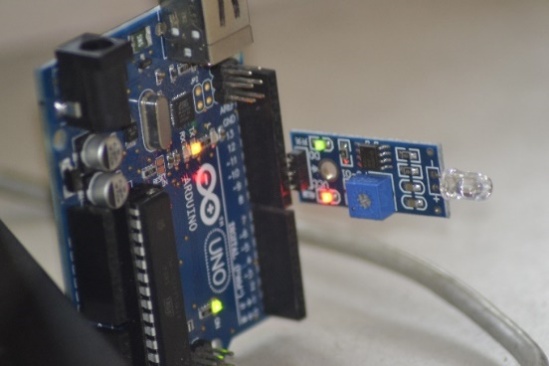


Fig 04: VLC Receiver (Photodiode Sensor)

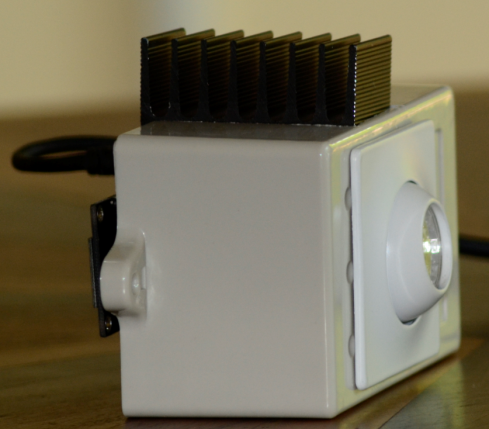


Fig 05.a: VLC Transmitter (Light Source with embedded Node MCU module)

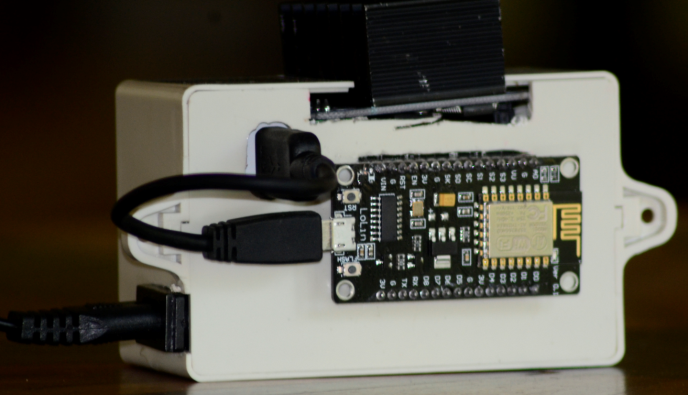


Fig. 5.b: Transmitter (Light Source with embedded Node MCU module)



Fig 06: Key Exchange System

*A. Prerequisites for Authentication*

* FreeRADIUS server.
* VLC enabled bulb with a unique ID (VLC\_ID) and a key (VLC\_KEY)
* VLC bulb should be registered on RADIUS server VLC module with VLC\_ID, VLC\_KEY and the IP address (attached with the VLC module). This ID and the KEY are stored in the database in Radius server.
* AUTH\_KEY is generated by a random key generator written in the RADIUS server VLC module.
* VLC enabled LED should emit VLC\_ID periodically.

*B. Authentication Process*

1. Client machine which needs to be connected to an available Wi-Fi network will send a connection request.

2. AP will send an Identity request to the client.

3. The device detects the VLC\_ID emitting periodically by the LED and reads it using the photodiode sensor attached to the device.

4. Then send it as the user name with the reply message to the AP which will relay to RADIUS server.

5. Once the reply reached to the RADIUS server, AES encrypt AUTH\_KEY using VLC\_KEY, and then send to VLC transmitter (LED).

a. VLC transmitter decrypts AUTH\_KEY using the VLC\_KEY and starts emitting AUTH\_KEY to the device.

6. At the same time RADIUS server sends Authentication challenge to the device via AP.

7. The device reads VLC emitting AUTH\_KEY using the VLC receiver (photodiode) and response to challenge using AUTH\_KEY.

8. RADIUS server matches the authentication response in the reply message.

9. RADIUS server sends authentication success/fail message.

10. AP will grant connectivity to the Wi-Fi network.

11. Each session will timeout after time t which can be assigned to the RADIUS server and step 1 to 10 will happen repeatedly.

Fig. 07 shows the signals detected by the photodiode sensor and Fig 09 shows the authentication success message given at the terminal.

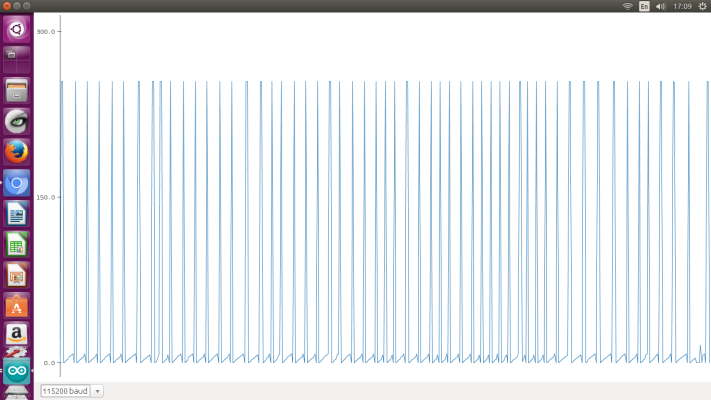


Fig. 07: Signals read by photodiode sensor

The developed prototype uses the following definition to identify bit ‘0' and bit '1'. (Fig.08). After 20 milliseconds in turn-off state (0), the transition from turn off (0) to turn on (1) is the starting point of a bit. If the turn-on state remains 200ms it is identified as a bit ‘0' and if it lasts for 400ms it is identified as bit ‘1'.

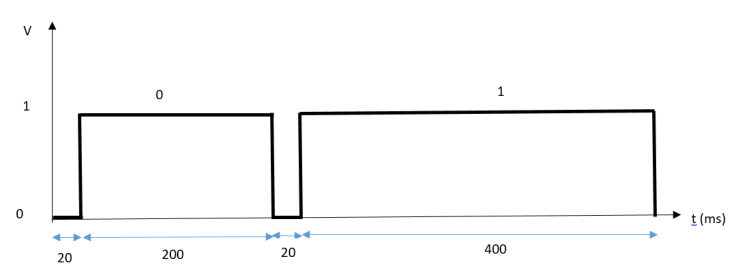


Fig. 08: Bit ‘1’ and ‘0’ definitions

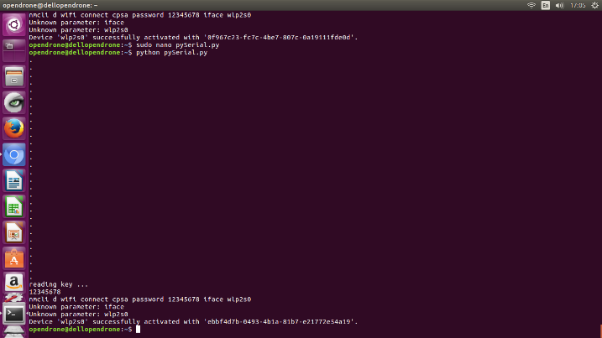


Fig. 09: Authentication success message gives at terminal

1. LIMITATIONS AND CHALLENGES

In the proposed system, we have used photodiode as the receiver, advantage in that is a very high gain can be achieved due to narrow Field Of View (FOV) of each photodiode. The disadvantage, however, is that such a receiver requires careful alignment with the transmitter, VLC enabled LED light source in the proposed system, because of the narrow FOV. For future development, we hope to replace it with a web camera or an image sensor which contains a projection lens and a large matrix of photodiodes. The projection lens ensures a large FOV which nearly eliminates the alignment requirement.

For the moment FOV of LED is limited to the direction of the LED’s central axis. This limits the coverage to a single direction. This should be overcome by designing cell layout efficiently. Designing the LED front end with multiple LEDs is not practical because we are trying to use the existing LED infrastructure for the system.

Design should be considered in advanced for luminaire placements. The size of a cell which can be varied depending on the size of the illumination is provided. One possible method is, one multi-LED luminaire on the ceiling provides illumination to an entire room. Multiple users with multiple devices can obtain data using this single luminaire. This type of cell is introduced as an attocell in [13]. The other method is, providing illumination mostly for personal usage. Table lamps used for brightening small area is one such example. This type of cell is referred as a zeptocell [13]. The radius of a zeptocell is no more than 5 meters. Further investigation is needed to determine optimal cell topology which can maximize the throughput while meeting the illumination requirements because one of the main purposes of this research is to develop the protocol to use the existing LED bulbs and implement it with low cost.

Providing similar connectivity to all can be achieved by arranging the cells in a novel LED arrangement design proposed by, [14] and [15] (Fig. 13).

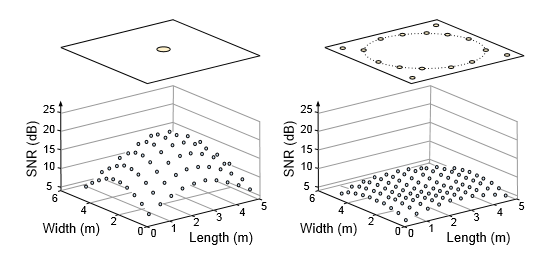


Fig 13: LED rearrangement design for equal data distribution.

Ambient light is a source of noise which changes the luminance of the received pixels. This can cause errors in the information encoded in the pixels, resulting in information loss at the receiver.

Uplink transmission which is difficult with LED can be used only as the transmitter. Therefore protocol is designed only with downlink. Two-way communication using VLC is a limitation at the stage of developing this prototype.

1. CONCLUSION

Existing Wi-Fi connectivity is available for everyone who is within the range and has the passwords. Available Wi-Fi networks use RF for data transmission and due to its ability to penetrate through walls and objects it is impossible to implement location-based restrictions using RF as the communication technology. Using the emerging Visible Light-based communication technology, we have proposed authentication protocol where key distribution is done through VLC thus automatically the network connectivity will be restricted to the people in the location where VLC device (LED) transmits the timely key. The Visible Light is incapable of penetrating through walls and that feature has been used here for providing location based access to the Wi-Fi network. Proposed protocol is implemented using existing LED technologies. The design has been made carefully to avoid extra cost. The minimum changes have to be made to the RADIUS server to obtain the above mentioned location based access advantage.

1. FUTURE WORK

As future enhancements several improvements that need to be added to the protocol design have been identified. Proof of concept has been designed using photo diode as the receiver and it should be attached to the computer separately. The protocol would be more useful if the receiving end of the VLC can be replaced with existing web camera of the Wi-Fi device. This can improve the reliability of the protocol. When considering the transmitters, careful design should be made for the existing LED bulbs and cell layout of the indoor location to make sure equal quality of VLC is available for all within the room, without exceeding the cost of using LED for illumination purposes.

REFERENCES

[1] D. Tsonev, S. Videv, and H. Haas, “Light fidelity (Li-Fi): towards all-optical networking,” 2013, vol. 9007, pp. 900702-900702–10.

[2] L. U. Khan, “Visible light communication: Applications, architecture, standardization and research challenges,” *Digit. Commun. Netw.*

[3] “Wi-Fi,” *Wikipedia*. 21-Mar-2017.

[4] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, “Visible Light Communication, Networking, and Sensing: A Survey, Potential and Challenges,” *IEEE Commun. Surv. Tutor.*, vol. 17, no. 4, pp. 2047–2077, Fourthquarter 2015.

[5] D. C. O’Brien *et al.*, “Home access networks using optical wireless transmission,” in *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2008, pp. 1–5.

[6] M. Kavehrad, “Sustainable energy-efficient wireless applications using light,” *IEEE Commun. Mag.*, vol. 48, no. 12, pp. 66–73, Dec. 2010.

[7] T. Komine and M. Nakagawa, “Fundamental analysis for visible-light communication system using LED lights,” *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 100–107, Feb. 2004.

[8] S. Rajagopal, R. D. Roberts, and S. K. Lim, “IEEE 802.15.7 visible light communication: modulation schemes and dimming support,” *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 72–82, Mar. 2012.

[9] “IEEE SA - 802.15.7-2011 - IEEE Standard for Local and Metropolitan Area Networks--Part 15.7: Short-Range Wireless Optical Communication Using Visible Light.” [Online]. Available: https://standards.ieee.org/findstds/standard/802.15.7-2011.html. [Accessed: 19-Mar-2017].

[10] “Comparisons of Wired and Wireless Networks: A Review,” *TechRepublic*. [Online]. Available: http://www.techrepublic.com/resource-library/whitepapers/comparisons-of-wired-and-wireless-networks-a-review/. [Accessed: 16-Mar-2017].

[11] “How do Wireless Networks Work? - Webopedia.com.” [Online]. Available: http://www.webopedia.com/DidYouKnow/Computer\_Science/wireless\_networks\_explained.asp. [Accessed: 16-Mar-2017].

[12] D. Stanley, P. Calhoun, and M. Montemurro, “Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11.” [Online]. Available: https://tools.ietf.org/html/rfc5416. [Accessed: 23-Mar-2017].

[13] H. Haas, PureLiFi Attocell, www.pureliﬁ.com. [Accessed: 22-Mar-2017].

[14] Z. Wang, C. Yu, W.-D. Zhong, J. Chen, and W. Chen, "Performance of a novel LED lamp arrangement to reduce SNR ﬂuctuation for multi-user visible light communication systems," Opt. Express, vol. 20, no. 4, pp. 4564–4573, Feb 2012. [Online]. Available: http://www.opticsexpress.org/ abstract.cfm?URI=oe-20-4-4564 [Accessed: 26-Mar-2017].

[15] Z. Wang, W.-D. Zhong, C. Yu, and J. Chen, “A novel LED arrangement to reduce SNR ﬂuctuation for multi-user in visible light communication systems,” in Information, Communications and Signal Processing (ICICS) 2011 8th International Conference on, Dec 2011, pp. 1–4.