# Chapter 3: Methodology

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.

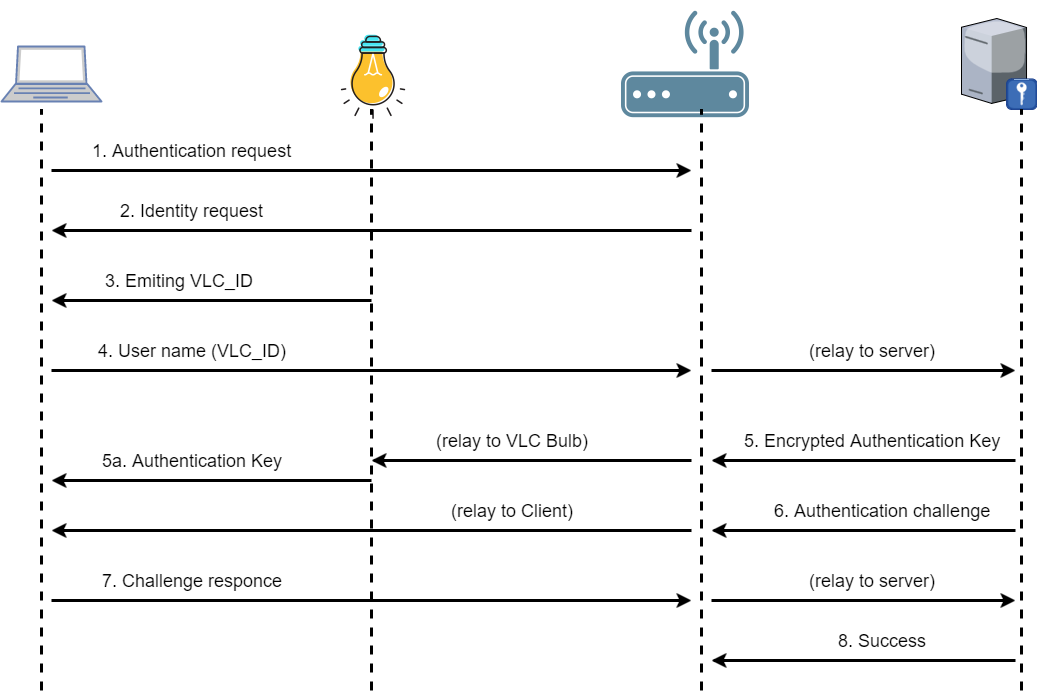


Fig.02: Communication process of the proposed protocol

*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.

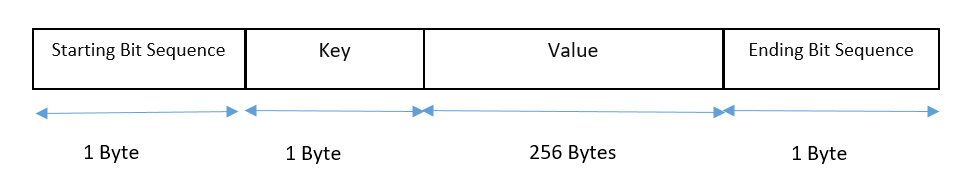


Fig 03: VLC message format

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.

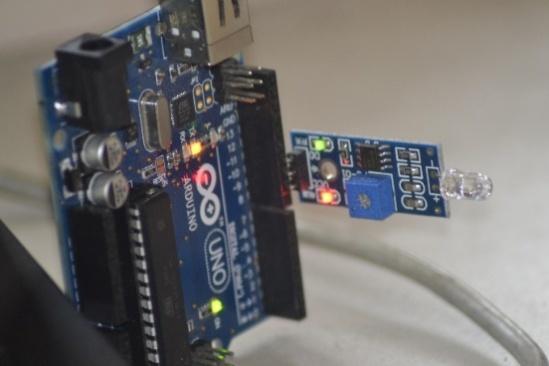


Fig 04: VLC Receiver (Photodiode Sensor)

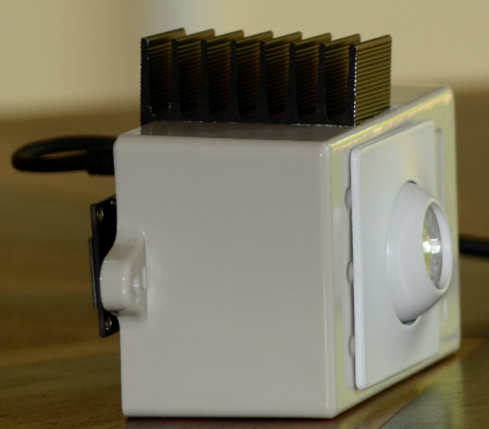


Fig 05.a: VLC Transmitter (Light Source with embedded Node MCU module)

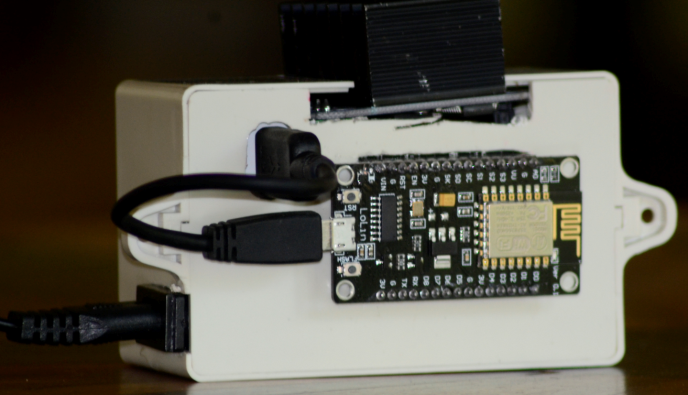


Fig. 5.b: Transmitter (Light Source with embedded Node MCU module)



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.

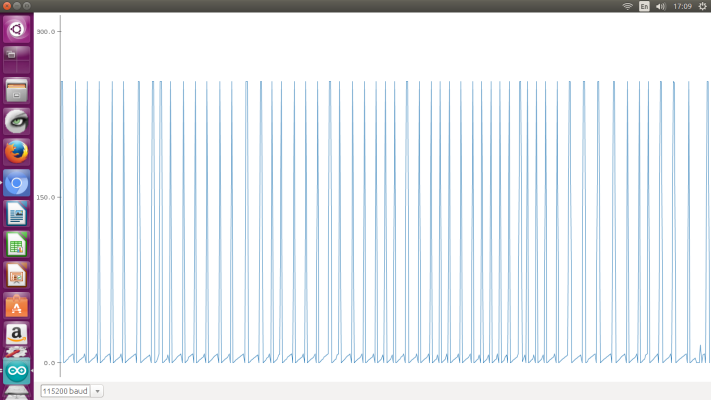


Fig. 07: Signals read by photodiode sensor

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'.

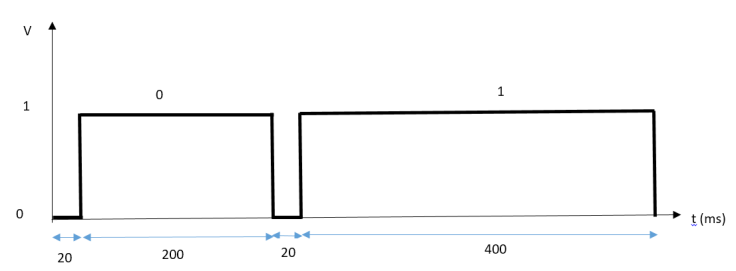


Fig. 08: Bit ‘1’ and ‘0’ definitions

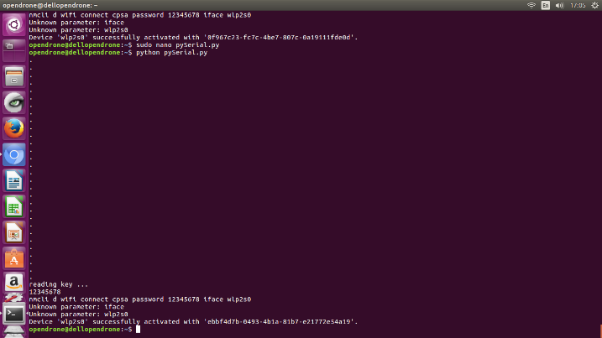


Fig. 09: Authentication success message gives at terminal

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).

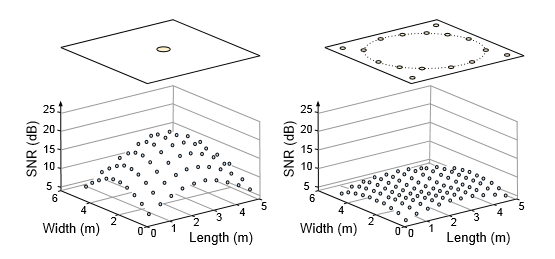


Fig 13: LED rearrangement design for equal data distribution.

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. 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.