Wireless Network Authentication and Tracking Protocol based on Visible Light Communication

C.D.Palliyaguruge

2019

Wireless Network Authentication and Tracking Protocol based on Visible Light Communication

A dissertation submitted for the Degree of Master of Computer Science

C.D.Palliyaguruge
University of Colombo School of Computing

2019

Declaration

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student Name: C.D.Palliyaguruge

Registration Number: 2016/MCS/068

Index Number: 16440688

Signature: Date:

This is to certify that this thesis is based on the work of

Mr.C.D.Palliyaguruge

under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name:

Signature: Date:

ACKNOWLEDGEMENT

As a final year student of Masters in Computer Science, University of Colombo, Sri Lanka first I would like to express my gratitude to University of Colombo and University of Colombo School of Computing and also the people who helped me to through this project to complete this successfully.

I would like to make this an opportunity to thank my supervisor Dr.Kasun De Zoysa, Senior Lecturer, University of Colombo School of Computing who gave me the tremendous opportunity to do this wonderful project on the topic Wireless Network Authentication and Tracking Protocol based on Visible Light Communication, which also helped me in doing a lot of research, studies and hacking which gained me knowledge and exposed me to new technology stack.

Secondly I would also like to thank my co-supervisor Mr.Chathura Suduwella from Sustainable Computer Research (SCoRe) Lab, University of Colombo School of Computing who guided me throughout the project.

Finally I would like to thank my family members, friends and office colleagues from Cambio Software Engineering for supporting my projects work and giving support at it’s best for me to complete this project.

ABSTRACT

Wi-Fi has paved path to introduction of several wireless communication protocols and ecosystem of various kinds of wireless devices like IOT and BYOD which have many advantages as well as security vulnerabilities inherent to them which may expose organizations to threats. Since most of these technologies use Access Points to serve connectivity for their clients/users they can be accessed from several meters away from the Access Point which serves the connectivity and since these technologies are wireless they can be easily manipulated and misused.

Visible Light Communication (VLC) is a blooming research area which uses visible light spectrum as the communication channel. Exponential growth of Light Emitting Diode (LED) technology and deployment as a light source has encouraged to use them 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 the proposed location authentication protocol, VLC and Infrared(IR) technologies had been used for authentication purpose and Wi-Fi is used for data transfer once the device had 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 and IR.

In this proposed authentication protocol key distribution and authentication are done through VLC and IR. With this approach the network connectivity will be inherently restricted to the devices which are in the visible range of the Access Point(AP) VLC device (LED) which transmits the timely key and client devices can send responses to AP requests using IR with directed signaling.

The Visible Light and IR are incapable of penetrating through walls and that feature had been used here for providing location based access to the Wi-Fi network and tracking capabilities with secureness.

CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

Chapter 1. INTRODUCTION 1 - 8

Chapter 2. LITERATURE REVIEW 9 - 23

Chapter 3. METHODOLOGY 24 - 29

Chapter 4. PROPOSED SOLUTION DETAILS 30 - 36

Chapter 5. EVALUATION AND RESULTS 37 - 42

Chapter 6. CONCLUSIONS AND FUTURE WORKS 43

REFERENCES 44 - 45

LIST OF FIGURES

Figure 2.1 - Wireless Communication Standards 9
Figure 2.2 - Steps in Open Authentication 12
Figure 2.3 - Steps in Shared key 12
Figure 2.4 - Steps in EAP Authentication 13
Figure 2.5 - Steps in MAC based Authentication 13
Figure 2.6 - Electromagnetic Spectrum and Visible Light Frequency Range 19
Figure 2.7 - User authentication steps in existing protocol 21
Figure 3.1 - Message format of proposed protocol 27
Figure 4.1 - Client side setup 30
Figure 4.2 - Server side setup 31
Figure 4.3 - Effective luminaire placement design 35
Figure 4.4 - Photodiode sensor used for prototype development 35
Figure 4.5 - Few IR receivers tried for implementing prototype development 36
Figure 5.1 - Client Evaluation Flow Chart 38
Figure 5.2 - Access Point and Wi-Fi Server Evaluation Flow Chart 39

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
EAP	Extensible Authentication Protocol
IEEE	The Institute of Electrical and Electronic Engineers
IoT	Internet of Things
JSON	Java Script Object Notation
ms	milliseconds
PWM	Pulse Width Modulation
RADIUS	Remote Authentication Dial-In User Service
USB	Universal Serial Bus
VLC	Visible Light Communication
WEP	Wired Equivalent Privacy
Wi-Fi	IEEE 802.11 standards (Wi-Fi Technology)
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access Version2
WPA3	Wi-Fi Protected Access Version3

Chapter 1

INTRODUCTION

Wireless technologies have been started to adapt in to communication systems from decades ago replacing the wired technologies available for data communication network connectivity. Wi-Fi is one such 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 [1]. Wi-Fi is a 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 with or without a medium. 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. When establishing a Wi-Fi connection between an Access Point and a client there exists a 3 step process where authentication take place in. If the Wi-Fi network has not given an open access, client devices who are connecting need to provide unique username and password to authenticate. This need to take place at least once. The problem here is anyone within the range of the Wi-Fi can get reconnected if they have gain access previously and remember those login credentials. Also same RF is used to share the secret key in the existing Wi-Fi technology which make it possible for security vulnerabilities.

Through this research it is aimed to come up with an secure authentication protocol which work depending on Visible Light Communication(VLC) and Infrared(IR) Communication.

The term Visible Light Communication had been around for a long time. In 1880 Alexander Graham Bell invented the photophone, which transmitted speech on modulated sunlight over several hundred meters [1]. This pre-dates the transmission of speech by radio.

But the term again coined recently in 2003 when researchers started transmitting data using LEDs [1].

Visible Light Communication (VLC) is defined as communication of signals between two locations using the visible region of the electromagnetic spectrum. The process is been performed using a pair of visible light source and visible light detector as signal sender and signal receiver respectively. In practical applications fluorescent bulb or a bulb made of Light Emitting Diodes (LED), OLED displays can be used as transmitter or in other words as emitter. Photodiodes, LDR, Digital Cameras can be used as transmitter or in other words receiver.

In recent years with advancements of the field of solid state lighting leads to the replacement of fluorescent lamps and old Tungsten lamps by bulbs made of Light Emitting Diodes (LEDs) which further motivates the usage of VLC. It uses LED ability to switch into different intensity levels at a fast rate to transfer data. The characters of modern LED such as low cost, low power consumption, durability than other lamps and features like fast switching capability, Pulse Width Modulation (PWM) support on dimming capability (digital dimming without regulating voltage), direct control by digital circuit than other lamps, has made LED the best candidate for this. With the wide usage of LEDs for illumination purposes in public areas and the domestic, researchers have started to utilize this already available LED infrastructure for illumination as a communication medium for fast and efficient transfer of data by implementing VLC technology over it.

Therefore VLC is a novel communication method that most researchers have put faith on to become the communication technology of the next generation. LEDs and it's variants will be the future of modern lighting system as they provide many advantages over conventional lighting equipment, specially like it's efficiency as an illumination source and low power consumption capability.

Yet despite of advantages of using bulbs made out of LEDs for Visible Light Communication there exists some challenges as well as disadvantages of its' own.

The most important fact that should be considered when implementing VLC technology over an LED infrastructure is to eliminate the overlap of illumination process of LED light source with the process of signal communication. In literal terms, only the light should be visible to the human eye but not the data that is being transferred through it. The opportunity to send data usefully in this manner has largely arisen and under research because of the increasing use of LED light bulbs. It is possible to 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 Communication Technology. 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 transmitter and receiver of RF waves. Limited signal bandwidth is a major concern and has affected the data rates of RF based wireless communication. Also RFs can penetrate through barriers so that can not be limited for an area. This has become a major security issue and security threats and several attacks had taken place against RF based communication systems.

RF based data communication techniques have it’s own usability issues as well. There exists some scientific and medical equipment which are sensitive for RF signals and using RF based communication to connect with those devices might affect harmfully for those devices [4]. Also being exposed to RF signals for a long period of time has been identified as cause for some illnesses like cancers, etc. [3][5].

To overcome these issues scientists has proposed Visible Light based data communication methodologies. Having unused larger bandwidth of electromagnetic field based frequencies is the major reason for scientists to come up with Visible Light based data communication. Also Visible light cannot penetrate through physical barriers like walls and walls so that it can be easily limited for an area. Also it has feasible solutions for problems with mobility, power efficiency, cost, immunity to interference from electromagnetic sources and usability which other data communication methodologies fails to provide solutions for.

Several Visible Light Data Communication Standards do exist today. Li-Fi(Light Fidelity), IrDA(Infrared Data Association), RONJA(Reasonable Optical Near Joint Access) are some examples for currently available Visible Light based data communication standards. But adapting those standards in to industrial use has raised problems like need for more investments to upgrade existing RF based electronic devices to fully Visible light based communication devices, lack of security standards in Visible Light based data communication protocols.

Previous research carried out by researchers of University of Colombo School of Computing had introduced a novel authentication protocol for location dependent network connectivity protocol using VLC [2]. In that protocol researchers had used VLC only to create down link from Access Point to the Client. It still depends on Wi-Fi RF signals to create link from Client to AP which still has problems like usability issues, some security issues which inherent for Wi-Fi and compatibility with existing VLC protocols and compatibility issues with VLC data communication protocols.

In this thesis I am proposing a new protocol based on VLC and Infrared communication to authenticate a Client to an AP. With this new protocol I hope to give solutions for compatibility issues, security issue & usability issues which had with previous protocol.

1.1 Motivation

With increase of devices with Wi-Fi connectivity several security problems have aroused. To avoid these issues previous researchers have suggested VLC based authentication protocol with additional layer of security for network which still use RF signals in authentication process. But since still it uses RF signals as part of the protocol, proposed protocol has issue slike usability issues, security issues and compatibility issues.

The newly proposing protocol from thesis will eliminate those weaknesses of previously proposed protocol and will introduce some new features which will increase usability of the protocol.

1.2 Problem

With the introduction of Wi-Fi and it's variants of communication protocols, security of communication network has become more and more vulnerable for various types of attacks and misuse issues. Also its' capabilities and limitations have reduced usability of such protocols.

Since Wi-Fi and other wireless protocols depend on RF signals, networks built on top of those protocols can be accessed for an user even from several meters away from the AP (Basically around 20m from the Access Point [2]). This is a security flow of all wireless communication protocols as not having a physical connection between AP and client/user make it impossible to limit network connectivity for a certain geographical area. So an attacker who positions himself at reasonable amount of distance to an AP can listen to the network traffic and perform attacks on wireless network without alarming.

RF signals are generated using Radio Waves which are part of electromagnetic spectrum. RF bandwidth is already divided and assigned as operational frequencies for each protocol. So a protocol has a relatively limited bandwidth which limits data communication speed to a relatively low amount.

RF signals can be harmful for certain electronic devices such as medical and laboratory devices and operation of certain electronic devices can distort RF signals [3-5] which limits usability of RF based communication protocols.

With considering above problems researchers have come up with a VLC based authentication protocol. It uses VLC to create downward link between AP and a client yet still uses RF for client to AP communication. Using RF still limits the new protocol's usability & applications.

Several Visible Light Data Communication Standards do exist today. Li-Fi(Light Fidelity), IrDA(Infrared Data Association), RONJA(Reasonable Optical Near Joint Access) are some examples for currently available Visible Light based data communication standards. But adapting those standards in to industrial use has raised problems like, need for more investments to upgrade existing RF based electronic devices to fully Visible light based communication devices, lack of security standards in Visible Light based data communication protocols. Even in this situation the previously proposed protocol has a usability issue since it uses RF signals.

1.3 Aim

The aim of this research project is to come up with a protocol based on VLC and IR communication to authenticate wireless networks such as Wi-Fi. Users are provided with session password through the VLC enabled bulb. This VLC bulb will make sure that the users are within the light intensity range to receive the Wi-Fi authentication. That is to make sure, that the clients are within the building or in the visual range define by the organization. User will then use IR emitter which is connected to user device to response signals from AP which has IR receiver to retrieve signals from user.

The first part of this research will be to include a module to the Remote Authentication Dial-In User Service (RADIUS) server to enable VLC authentication. Then to change the password in timely manner through the RADIUS server. Thereafter to develop a module which can be coupled to an existing bulb to implement a low cost VLC enable bulb. Then a module will be included in client device to support VLC with the bulb (eg: through web camera, dongle). Then a IR emitter will be coupled with client device to send client responses to AP. Finally a receiver will be implemented and coupled with AP to retrieve IR responses from client in-order to complete the authentication process.

Also this protocol will be able to perform session management, client tracking and client data retrieval on demand.

1.4 Scope

Scope of this research will be to provide a reliable wireless network authentication protocol based on Visible Light Communication & Infrared Data Communication for existing wireless networks(In this case a Wi-Fi network). It will add another layer of security for network while being simple to maintain and cost effective. Also it will privilege network administrators to control user logins based on locations, track users. To achieve these, new protocol will guarantee the user connection while they are in pre-defined physical location.

1.5 Assumptions and Limitations of the Research Project

This project was carried out based on basic assumption of that client/network user can send data to the Access Point using Infrared data communication.

In this research it will cover network user authentication, session management and user location tracking only. Further data communication will be carried out by RF signals according to WiFi standard protocol. Data communication devices used in this research must be WiFi enabled devices.

Experiments will be carried out in an indoor environment and any disturbances in outdoor environments are not taken into account.

The new protocol can be used along with WiFi standards and later on can be adapted into fully Visible Light based communication systems.

1.6 Report Organization

CHAPTER 2 - LITERATURE REVIEW
Previous approaches will be critically evaluated under this chapter. Requirement gathering process and approaches are described under this chapter.

Chapter 3 - METHODOLOGY
This chapter describes the methodology which has been used for the suggested approach in details.

Chapter 4 - PROPOSED SOLUTION DETAILS
The chapter describes about the designing and software engineering techniques which have been used to design the system. Also describes the detailed design of the proposed system.

Chapter 5 - EVALUATION AND RESULTS
In order to assure quality of the functionality of the proposed approach, testing phase and evaluation process which were carried out describe in this chapter and the results are presented.

Chapter 6 - CONCLUSION AND FUTURE WORK
This chapter describes about the results of proposed approach and further modifications that can be done with this solution.

Chapter 2

Literature Review

In this chapter background of currently available wireless data communication technologies will be critically evaluated about the efforts those technologies have put to mitigate security issues of the wireless network and data transmitted inside the network.

First subsection of the chapter will provide overall introduction to available wireless data communication technologies highlighting their usage. Second section of this chapter will discuss about Wi-Fi technology, available Wi-Fi protocols, security flaws of the Wi-Fi technology in a critical manner and ways to mitigate those issues. Final section of this chapter will talk about advancement of non-radio wave based data communication technologies.

2.1 Wireless Communication Standards

Different methods and standards of wireless communication have developed across the world, based on various commercially driven requirements. These technologies can roughly be classified into four individual categories, based on their specific application and transmission range. These categories are summarised in the figure below.

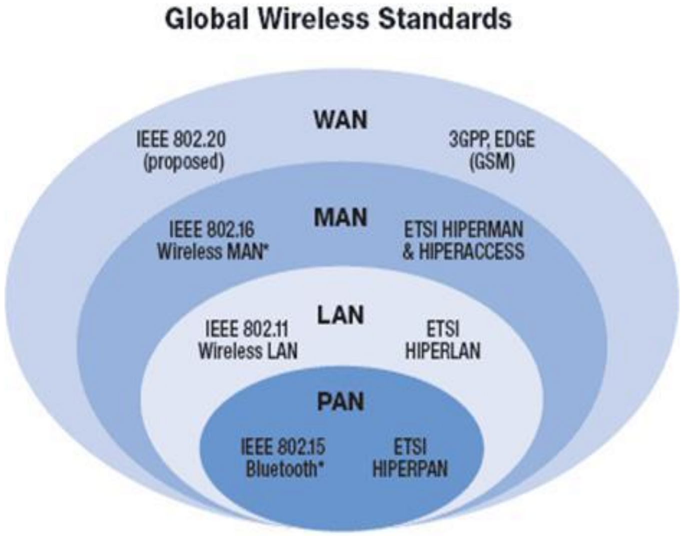


Figure 2.1 - Wireless Communication Standards

2.1.1 Personal Area Network (PAN):

A Personal Area Network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. The reach of a PAN is typically a few meters. PAN's can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet.

Personal area networks may be wired with computer buses such as USB and FireWire. However, a Wireless Personal Area Network (WPAN) is made possible with network technologies such as Infrared and Bluetooth.

2.1.2 Local Area Network (LAN):

A wireless LAN or WLAN is a wireless Local Area Network, which is the linking of two or more computers without using wires. It uses radio communication to accomplish the same functionality that a wired LAN has. WLAN utilizes spread-spectrum technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and still be connected to the network. Most common & popular example for LAN implementation is Wi-Fi networks.

2.1.3 Metropolitan Area Network (MAN):

Wireless Metropolitan Area Network (MAN) is the name trademarked by the IEEE 802.16 Working Group on Broadband Wireless Access Standards for its wireless metropolitan area network standard which is commercially known as WiMAX. This defines broadband Internet access from fixed or mobile devices via antennas. Subscriber stations communicate with base stations that are connected to a core network. This is a good alternative to fixed line networks and it is simple to build and relatively inexpensive.

2.1.4 Wide Area Network (WAN):

A Wide Area Network or WAN is a computer network covering a broad geographical area. Contrast with personal area networks (PAN's), local area networks (LAN's) or metropolitan area networks (MAN's) that are usually limited to a room, building or campus. The largest and most well known example of a WAN is the Internet. WAN's are used to connect local area networks (LAN's) together, so that users and computers in one location can communicate with users and computers in other locations. Many WAN's are built for one particular organisation and are private. Others, built by Internet service providers, provide connections from an organisation's LAN to the Internet. WAN's also refer to Mobile Data Communications, such as GSM, GPRS and 3G.

In this research project scope is focused on security concerns of Wi-Fi networks and possible solutions can be given using Visible Light Communication(VLC) methodologies.

2.2 Introduction to Wi-Fi

Wi-Fi is a technology for radio waves based wireless local area networking of devices based on IEEE 802.11 family standards[1], [6]. Devices that can use Wi-Fi technologies include desktops and laptops, video game consoles, smartphones and tablets, smart TVs, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points.

The term "hotspot" is used to define an area where WiFi access is available[7]. It can either be through a closed wireless network at home or in public places such as restaurants or airports. In order to access hotspots, users' computer/ device should include a wireless adapter.

Wi-Fi most commonly uses the 2.4 gigahertz (12 cm) UHF and 5.8 gigahertz (5 cm) SHF ISM radio bands[6], these bands are subdivided into multiple channels. Each channel can be time-shared by multiple networks. These wavelengths work best for line-of-sight. Many common materials absorb or reflect them, which further restricts range, but can tend to help minimise interference between different networks in crowded environments. At close range, some versions of Wi-Fi, running on suitable hardware can achieve speeds of over 1 Gbps[7].

In Wi-Fi protocol generally when connecting to a wireless network it is required to select the Access Point (AP) first using the Service Set Identifier (SSID). 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. During the discovery process, the client 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 client 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[8]. Open system authentication consists of two communications. First an authentication request is sent from the client 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 client device and the AP/router. 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 WiFi 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 client 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, client device will send an association request to AP. Once the association acceptance message is received only the client device can start transferring data. In the association process, AP and the client device get into certain agreements such as the network model, security parameters (WEP, WPA or WAP2), encryption method (TKIP, CCMP, AES) and channel frequency.

Authentication process for a Wi-Fi network can be implemented mainly in four(4) ways[9].

2.2.1 Open authentication

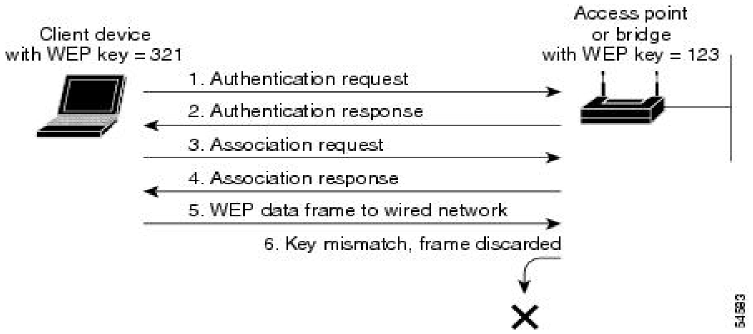


Figure 2.2 - Steps in Open Authentication

2.2.2 Shared key authentication

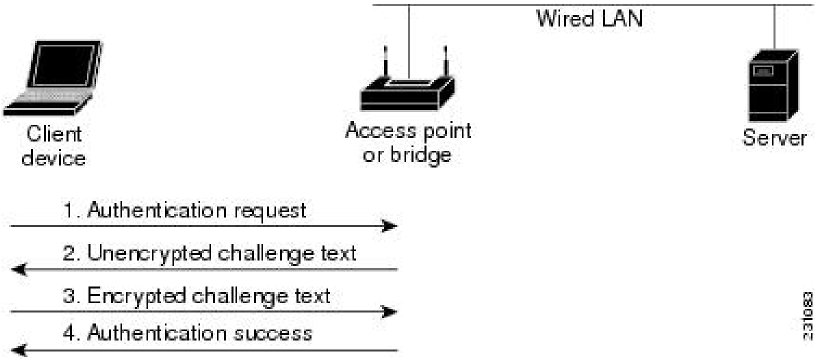

Wired LAN
Client
device
Access point
or bridge
Server
1. Authentication request
2. Unencrypted challenge text
3. Encrypted challenge text
4. Authentication success
231083

Figure 2.3 - Steps in Shared key

2.2.3 EAP(Extensible Authentication Protocol) Authentication

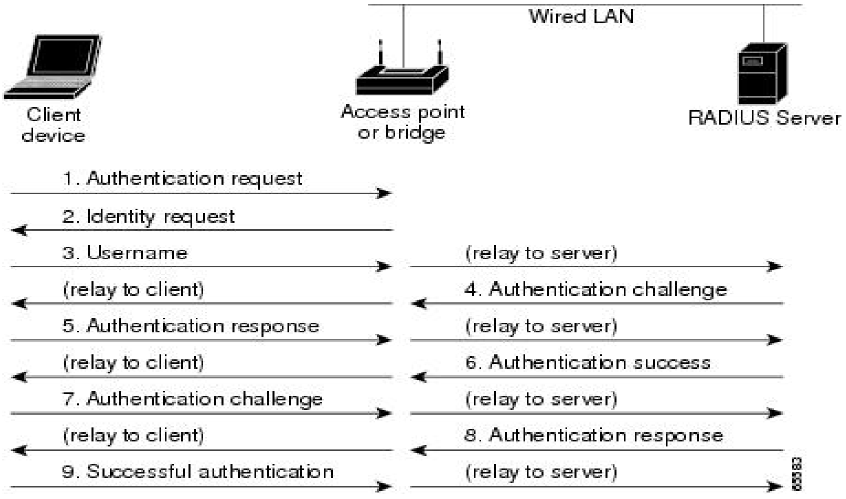


Figure 2.4 - Steps in EAP Authentication

2.2.4 MAC based Authentication

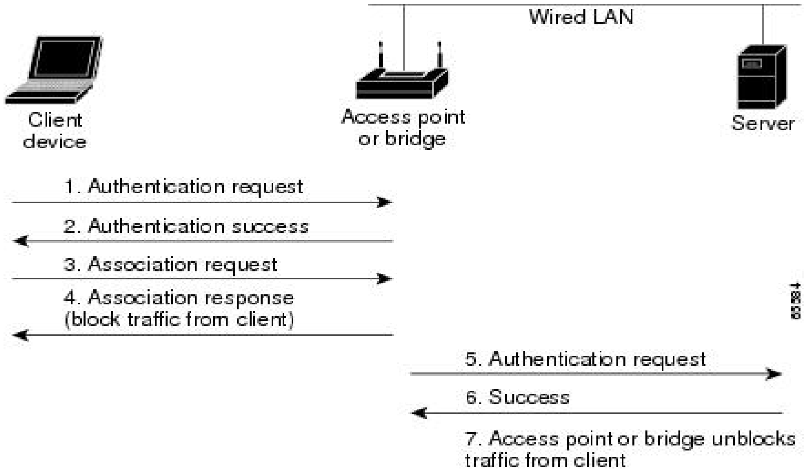

Wired LAN
Client device
Access point or bridge
Server
1. Authentication request
2. Authentication success
3. Association request
4. Association response (block traffic from client)
65584
5. Authentication request
6. Success
7. Access point or bridge unblocks traffic from client

Figure 2.5 - Steps in MAC based Authentication

There also exists a hybrid implementation using both MAC based & EAP based authentication protocols[9]. In that implementation first MAC based authentication will perform, if it succeeds device will be connected to network else will perform EAP based authentication.

2.3 Limitations and Vulnerabilities of WiFi Networks

As wireless signals travel through the atmosphere, they are sensitive to different types of impediments and interference as compared to wired network. Following are few limitations for WiFi technology.

2.3.1 Physical obstruction:

The number of walls the WiFi signal can pass through is determined by density of the materials used in a building's construction. Concrete and steel walls are difficult for a signal to pass through. These structures will weaken or at times completely prevent wireless signals.

2.3.2 Shared bandwidth:

The bandwidth of wireless network is shared among all the wireless users, so the more users you have, the slower the network becomes. Downloading torrents, for example, might cause other users to experience a slowdown in network speed. It is a good practice to protect your WiFi network with a strong WiFi password, to prevent unauthorized user from "stealing" the bandwidth.

2.3.3 Distance:

If you're sitting near a wireless router or access point, you will experience a faster network speed. But if another person is sitting far from the wireless router or access point, the network speed of both computers will drop drastically.

2.3.4 Speed of connected device:

The achievable download and upload speed of the device connected to the WiFi network is also dependent on the device itself. A mobile phone with better processor and more advanced antennas and radios design will promise higher download and upload speed.

2.3.5 Location:

Where an Access Point or wireless router is placed also makes the difference. Place the devices in higher ground to reduce the impact of physical objects.

Due to above reasons Wi-FI networks suffer from performance issues. Other than performance issues, security issues & concerns exists regarding Wi-Fi networks. Anyone within range with a wireless network interface controller can attempt to access a network; because of this, Wi-Fi is more vulnerable to attack (called eavesdropping) than wired networks. Wi-Fi Protected Access is a family of technologies created to protect information moving across Wi-Fi networks and includes solutions for personal and enterprise networks. Security features of Wi-Fi Protected Access have included stronger protections and new security practices as the security landscape has changed over time[1].

Few type of attacks on Wi-Fi networks can be explained as following.

2.3.6 Rogue Wireless Devices:

A rogue wireless device, or access point, is an unauthorised WiFi device added onto the network that isn't under the management of the network admins. They allow potential attackers a gateway into the network.

This sort of device can be maliciously installed if the attacker has direct access to the wired network, but more often than not they are added by users that are not aware of the implications.

2.3.7 Peer-to-peer Attacks:

Devices that are connected to the same access points can be vulnerable to attacks from other devices connected to that access point. Most Wi-Fi device providers provide for an option such as "Client Isolation" which ensures that clients connected to the access point cannot communicate with each other, preventing this issue.

2.3.8 Eavesdropping:

This is where wireless communications are monitored. There are two types of of eavesdropping.

The first, casual eavesdropping, or sometimes called WLAN discovery, is where a wireless client actively scans for wireless access points.

The second type, malicious eavesdropping, is the illegal kind. This is where someone tries to listen in on the data transferred between clients and the access point. Because of this, it is essential to encrypt Wi-Fi networks, as anything unencrypted can be listened in on.

2.3.9 Encryption Cracking:

This is where the attacker attempts to crack the encryption on the network. WEP networks are the most susceptible to this, being that they can be easily cracked in as little as 5 minutes.

It is important to ensure that you use the most secure encryption user can, and avoid using WEP where possible.

2.3.10 Authentication Attacks:

This is where the attacker scrapes a frame exchange between a client authenticating with the network, and then they simply run an offline dictionary attack.

With this sort of information, and depending on the strength of the password, it could be just a matter of time before they crack the password and gain access. Because of this it's important to keep user login credentials as secure as possible.

2.3.11 MAC Spoofing:

MAC spoofing is an extremely easy thing to do. Because of this, using MAC filtering to control which devices can connect to your network is not secure at all.

It can however be used in conjunction with other security measures to build up an overall more secure network architecture.

2.3.12 Management Interface Exploits:

This sort of attack can become an issue when user make use of some devices such as wireless controllers that allow user to control access points via things like web interfaces or console access. Default login credentials are widely available on the internet, so it's crucial to ensure that all devices are securely locked down to prevent unauthorised access.

2.3.13 Wireless Hijacking:

This occurs in situations where the attacker configures their laptop to broadcast as a wireless access point, using the same SSID as a public hotspot.

They then sit back and unsuspecting victims end up connecting to it, thinking it is the genuine public hotspot. This leaves them open to peer-to-peer attacks as well as monitor the victim's actions on the network.

2.3.13 Denial of Service:

This term covers a number of different things. DoS attacks can occur on different layers.

Layer 1 attacks are known as RF jamming attacks, and can be both intentional (attacker generating a signal to deliberately cause interference) and unintentional (devices such as microwaves or wireless phones causing interference. Layer 2 attacks can occur in a number of different ways. For example, an attacker can flood an AP with spoofed association and dissociation requests.

Other than security & performance issues there are some instances where Wi-Fi or any other radio signals can not be used for communication. Medical labs, physic & chemistry labs designed for special experiments are some examples for as such places[3-5].

2.4 Security Protocols in Wi-Fi Networks

To detect a wireless network all it is needed is a wireless compatible device. There is no way to selectively hide the presence of a wireless network from strangers, but prevention of unauthorized clients accessing the network 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.

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.5 Access Authentication in Wi-Fi Networks

2.5.1 How Wi-Fi authentication works

The architecture of Wi-Fi or in other words 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 client 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 client was accepted, the AP changes the virtual port with the client to an authorized state allowing full network access to that client. At log-off, the client virtual port is changed back to the unauthorized state.

2.6 Remote Authentication Dial-In User Service (RADIUS) Protocol

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 users 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 username 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 deauth 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-connecting 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 domestic 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 client is often guessable and can not be revoked for one client. 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 client to get the key through a VLC enabled LED placed at physical location.

2.7 Visible Light Communication

Visible Light Communication (VLC) is a newly invented communication technology which uses LEDs' ability to switch into different intensity levels at high frequency. It is a short range optical wireless communication using visible light spectrum from 380 to 750 nm [10]. 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 [10]. 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 [13-15]. 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 [10] 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.

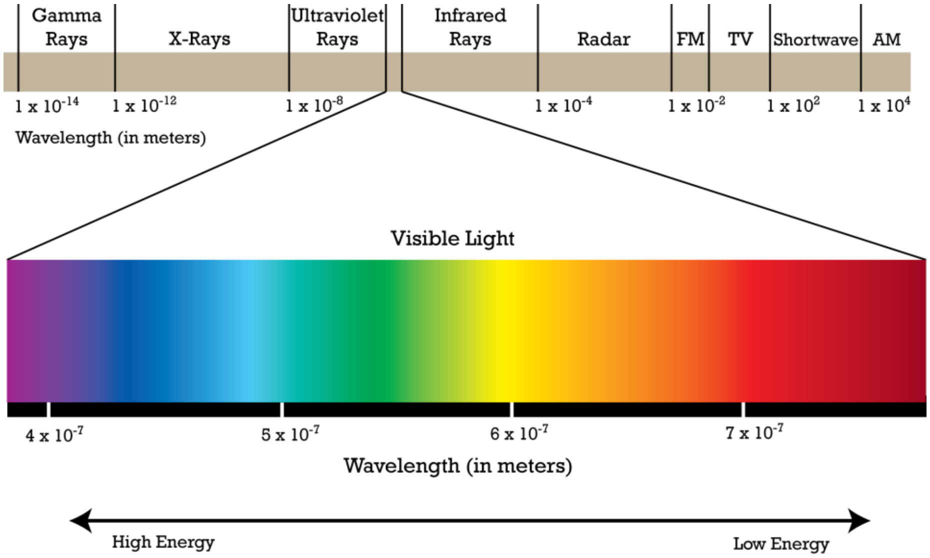


Figure 2.6 - ELectromagnetic Spectrum and Visible Light Frequency Frequency Range

It was shown in [11] 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 higher frequency than a human eye can detect. IEEE 802.15.7 standard [12] suggests that flickering should be faster than 200 Hz to avoid any harmful effect. That means high data rate will be provided by any VLC system.

Visible Light Communication(VLC)is important due to many reasons [10]. 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 intercell 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 or in other words a light source 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 [10]. 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, in this research a photodetector has been used 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.

2.8 Existing Solutions using VLC

Existing Wi-Fi standard(IEEE 802.1x standards) has several security issues[16], [17]. Authentication issues, user session management, limiting network users for a specific physical ground area and tracking network users are some major problems. Attacks like war driving, cracking, denial of service(DoS) and Karma do exists. Wifi can not be used in some places like aircrafts, medical labs and physics labs which uses highly sensitive equipment for Electromagnetic waves. In such cases users have to either use wired networks(Copper, Aluminium or Fiber Optics) which again reduce the mobility, increase cost and lower data rates.
There are few protocols based on Visible Light Data Communication. Li-Fi, RONJA, OWC, IrDA are some example for such protocols[18].

However existing VLC protocols lacks user authentication standards safe & efficient enough to use. A solution for this was given by a team of researchers using a combination of Wi-Fi & Visible Light Communication[2]. In their solution they have used EAP(Extensible Authentication Protocol) Authentication model in design for their protocol. In that protocol design, researchers use VLC to create a downlink between Access Point & user to authenticate user. Using VLC has increased security of protocol. A user must be in particular location to get authentication in this system since visible light cannot penetrate through obstacles. But still it uses Wi-Fi signals to create uplink for user authentication and it does not supports for user tracking.

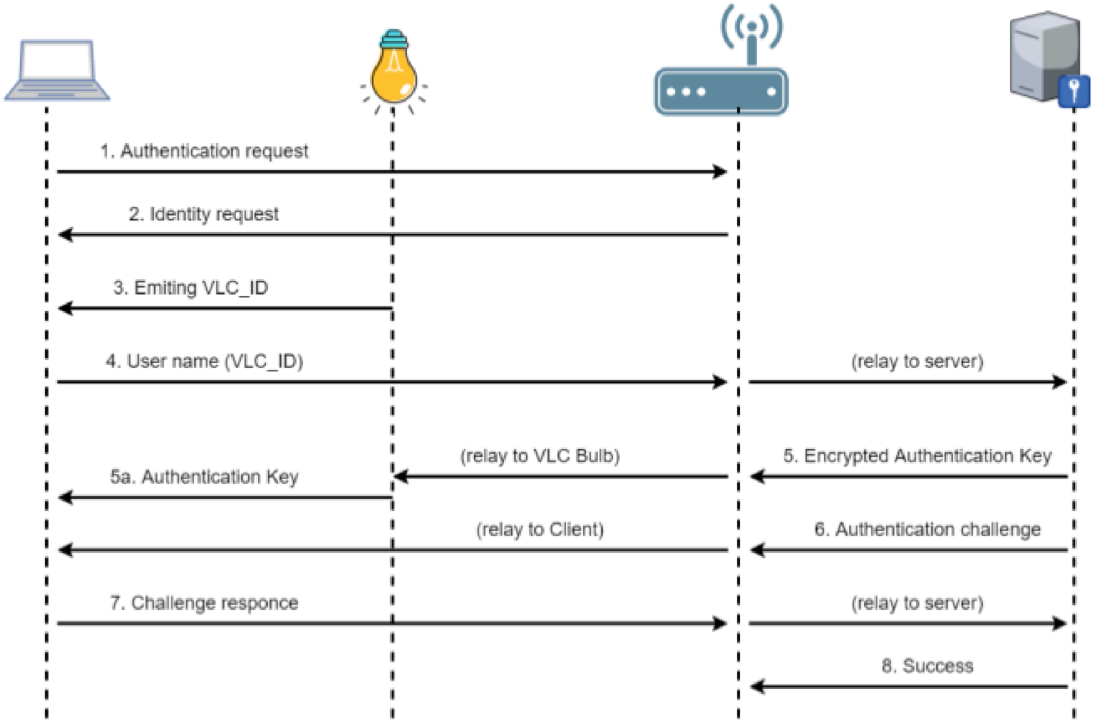


Figure 2.7 - User authentication steps in existing protocol.

2.9 Weaknesses of Existing Solution

Since the existing solution uses Wi-Fi signals, this protocol is still vulnerable for some attacks which can be performed on normal Wi-Fi data communication. Also as it uses RF signals, it can not be fully coupled with existing VLC data transmission protocols independently from Wi-Fi since it can not perform authentication process independently from Wi-Fi. Existing protocol use Wi-Fi to create uplink from user to Access Point. Since this it's usability drops as some places prohibits use of radio-frequency based communication[3-5].

2.10 Proposed Solution

Proposed protocol will use VLC to create both uplink & downlink between user & Access Point. Also it will provide facility to track user location and manage user sessions.

Proposed protocol will have following features.

1. Fully based on Visible Light data communication.
2. User authentication based on location.
3. User session management.
4. User's location tracking.
5. Can be coupled with existing VLC data communication standards for authentication purposes since it does not depend on Wi-Fi signals.

In this solution it is used a Directed Beam Radiation(DBR) to create uplink from client to AP device using IR.

Chapter 3

METHODOLOGY

This research project tries to check the possibility of using location based authentication mechanism for wireless network; in this case a Wi-Fi access point rather than using WPA/ WPA2 authentication protocols. Visible Light Communication and Infrared communication will be used to creates network links in between client and network Access Point. This chapter describes techniques related to the research methodology, design of the proposed system and steps that had been carried out to develop the proposed approach.

The main intention of the proposed protocol is to provide location based access to the wireless networks while tracking user activities. Already available solution to connect to a Wi-Fi network based on VLC uses VLC to create downlink from AP to client and the RF for create uplink from client to AP for successful authentication.

3.1 Proposing Architecture

The proposing solution architecture has five main components. Wi-Fi server component, Access Point(AP), AP VLC emitter and IR receiver, client VLC receiver and IR emitter and client device are those five components.

3.1.1 Wi-Fi Server Component

In this architecture Wi-Fi server component can have a RADIUS server running so that it can manage network users and APs.

Server component carries out following main tasks.

Authentication : who you are?
Authorization : what you are allowed to do?
Accounting : keeping records (Logging system)

3.1.2 Access Point

AP is the location which distribute network signals. This could be possible a wireless router. AP should support Wi-Fi protocols.

3.1.3 AP VLC Emitter and IR Receiver

To support this proposing solution, a VLC enabled light bulb is attached to AP. Also a IR receiver to retrieve client's IR responses is attached to AP. In this solution it is used a Directed Beam Radiation(DBR) to create uplink from client to AP device using IR.

The reason for using DBR is that it can assure the client is located in a permitted location to access the location. DBR ensure Line of Sight(LOS) between client and AP. If the client can not maintain LOS when authenticating, authentication will not success.

As VLC bulb it will be using a LED lamp which can be used for illumination purposes also. VLC signals from AP will be transmitted to client as Diffuse Radiation(DFR) signals since LED lamp is also used for illumination purposes.

3.1.4 Client VLC Receiver and IR Emitter

Client side VLC receiver detects VLC signals from AP VLC bulb and decode it so that client can understand messages from AP. IR emitter will encode client responses and send via IR emitter as DBR signals to AP IR sensor. Using DBF will ensure Line of Sight between client and AP which ensure client is at the given physical location when authenticating and connecting to network.

3.1.5 Client Device

Client device can be a mobile device such as mobile phone, a Wi-Fi enabled computer, etc. It should support existing Wi-Fi communication protocols.

3.2 Design of Protocol

Proposed communication protocol consists of steps which should be carried out by client and Access Point in given sequence in order to make a successful authentication and connection in between. If either of the component fails to success step in the below protocol, authentication will not happen and connection will not be created.

- Client emit VLC_ID and authentication request as IR signals.

- Access Point receiver read the client’s VLC_ID and authentication request and send to authentication server.

- Authentication server cross check client’s VLC_ID for permissions to access the network via the current Access Point/ from current physical location.

- If client is not permitted to access network, server will send signal to AP to emit VLC signal to let client know that it is not authorized to access.

- If client is authorized to access, server will look up for current ongoing sessions.

- If a current on going session found it will be checked for valid time period. If the session has exceeded the valid time period session will be deleted and new session will be created.

- If a current on going session is not invalid, it will be updated with current date and time as last login time.

- If an ongoing session is not found, a new session will be created and last login time will be updated by current session creation date and time.

- Authentication server will send request to Access Point to emit AP_ID and authentication key for client as VLC signals to login to Wi-Fi network.

- Client read AP_ID and authentication key sent by AP as VLC signals.

- Using received AP_ID and authentication key received, client log in to Wi-Fi network.

Protocol starts when client emit authentication and identification requests as IR signals. The most significant change of the proposing protocol is that it is not using radio signals for the whole verification and authentication process.

A session will be valid for a predefined time period. If the session exceeds the valid period of time, it will be automatically timed out and new session creation will be done.

A RADIUS server can be used to manage clients in server. In this protocol it is used a file based approach to manage client details and session details at server end.

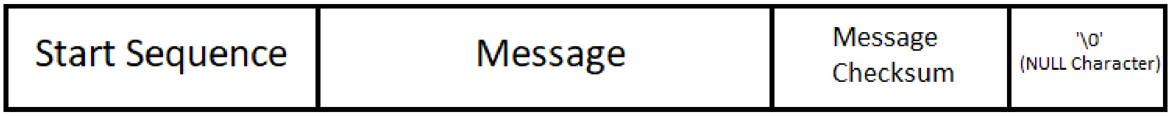
3.3 Messaging

Messaging of this proposed protocol is based on Voltage Variation Encoding since existing encoding mechanisms can not handle the flickering of the light source with the given hardware setup[2].

In this approach 10000 microseconds of voltage high state will mark start sequence of message. In message, each bit will start 10000 microseconds voltage high state. Depending on next bit value be transmitted is “0” or “1” voltage will be kept at low state for 500 or 1000 microseconds respectively.

At the end of the message checksum value of the original message will be appended and transmitted. Null character(‘\0’) will mark the end of the message.

The proposed protocol supports only for ASCII values.



Start Sequence	Message	Message Checksum	'\0' (NULL Character)

Figure 3.1 - Message format of proposed protocol

3.4 Operation Model

Proposed protocol will mainly operate in Physical Layer and Datalink Layer in OSI Network Reference model.

Electronic implementation will operate in Physical Layer and Driver software will operate in Datalink layer.

3.5 Communication Mediums

Proposed protocol uses Visible Light and Infrared as communication mediums. VLC uses visible light in between 400 and 800 Thz (780-375 nm) [18]. VLC uses existing infrastructure such as LED lamps, laser beams, ect which is used for illumination purposes. It is one of the advantages of using VLC since no separate infrastructure is needed to set up for data communication purpose.

In VLC photodiode sensors, LDRs, camera modules in electronic devices and Solar panels can be used as VLC receivers. Sensitivity of the receiver is highly affecting for VLC.

IR or infrared communication is a common, inexpensive and easy to use wireless communication technology. IR light is very similar to visible light, except that it has a slightly longer wavelength. IR is undetectable to the human eye which is perfect for wireless communication.

IR LED or array of IR LEDs can be used as IR emitters in IR communication where as IR receiver diode will be used as IR receiver.

Chapter 4

PROPOSED SOLUTION

4.1 Solution Overview

In order to prove usability and functionality of the proposed protocol, a prototype has been developed.

4.1.1 Client Implementation

An Arduino UNO board and an ESP 32 module are main components of client side implementation. Photodiode module is attached to arduino module to receive VLC signals from AP. An IR LED is attached to the arduino module to emit IR signals which is received by AP.

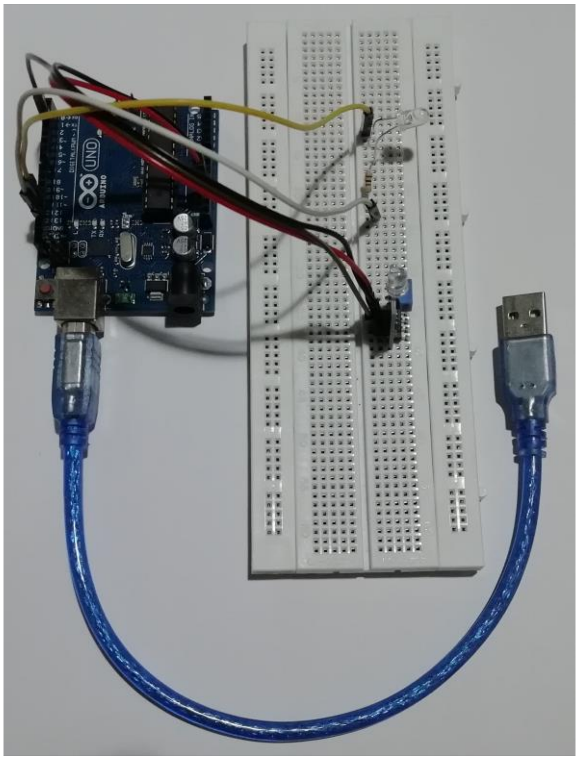


Figure 4.1 - Client side setup

After receiving Access Point's Wi-Fi ID and authentication keys as VLC signals, client implementation use those and authenticate and connect the ESP 32 module to the Wi-Fi network.

Other than hardware implementations, a python script is used to encode & decode messages and handle responses and messages sent from client. Both Arduino board and ESP 32 module is connected to a laptop.

4.1.2 Access Point and Authentication Server Implementation

An another Arduino Uno board is used to implement AP circuit. An LED bulb connected to a table lamp structure is used as AP VLC emitter. A IBT2 motor driver is used to switch the LED bulb in between high and low states. An IR detector is used to receive the IR signals emitted by client side.

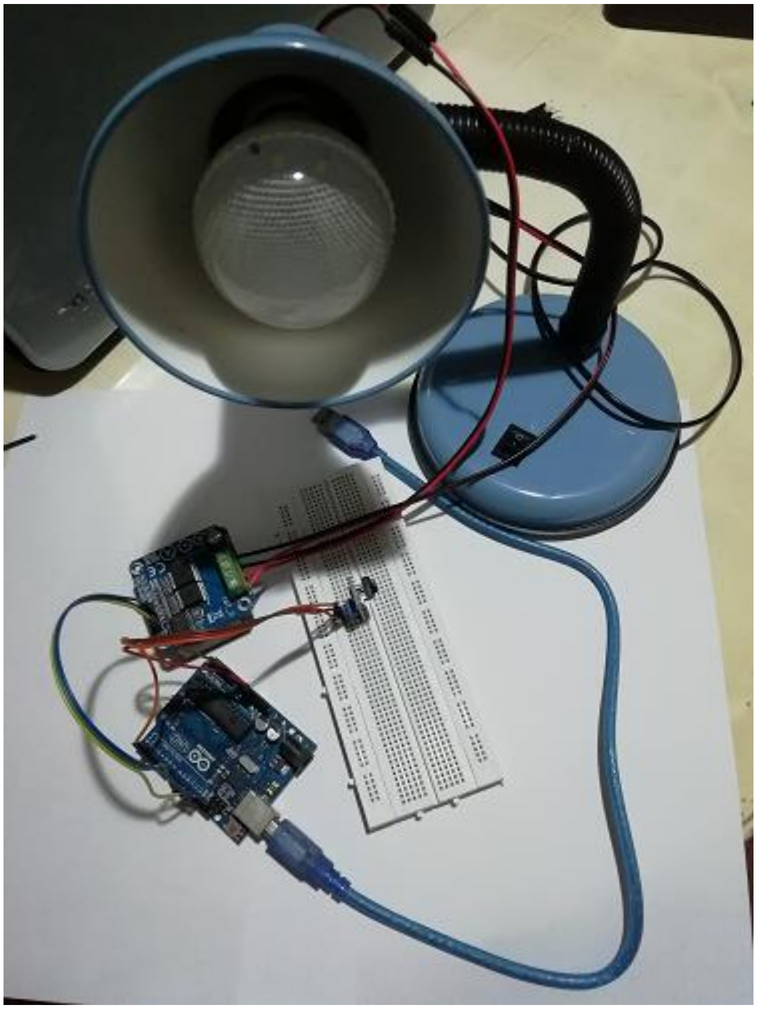


Figure 4.2 - Server side setup

To implement Wi-Fi server, a python program and a file based configuration and user data management system are used.

4.2 Authentication Process Prerequisites

Following requirements should be fulfilled before starting authentication process in between Client and AP.

1. AP should have a unique ID(VLC_ID) and an authentication key(VLC_KEY).
2. Client should have a unique ID(VLC_ID).
3. Client's VLC_ID should be registered as an allowed candidate to connect via the considered AP in Wi-Fi server.\
4. AP should emit ready to connect signal sequence periodically so that client can identify AP is ready to authenticate an another client.

4.3 Authentication Process

Authentication process steps can be listed down as following.

- Client emit VLC_ID and authentication request as IR signals.

- Access Point receiver read the client's VLC_ID and authentication request and send to authentication server.

- Authentication server cross check client's VLC_ID for permissions to access the network via the current Access Point/ from current physical location.

- If client is not permitted to access network, server will send signal to AP to emit VLC signal to let client know that it is not authorized to access.

- If client is authorized to access, server will look up for current ongoing sessions.

- If a current on going session found it will be checked for valid time period. If the session has exceeded the valid time period session will be deleted and new session will be created.

- If a current on going session is not invalid, it will be updated with current date and time as last login time.

- If an ongoing session is not found, a new session will be created and last login time will be updated by current session creation date and time.

- Authentication server will send request to Access Point to emit AP_ID and authentication key for client as VLC signals to login to Wi-Fi network.

- Client read AP_ID and authentication key sent by AP as VLC signals.

- Using received AP_ID and authentication key received, client log in to Wi-Fi network.

Each session created will be timed out when it exceeds predefined amount of time period. After that it will again has to follow same process defined above to authenticate to network.

4.4 Code Implementation

4.4.1 Client

Arduino UNO and ESP 32 modules are initialized with baud rate of 9600 at initial setup.

A photodiode module is attached to arduino board's digital pin 2 as an interrupt so that when VLC signals reaches, arduino board will automatically start listing to it and decode the signals. IR LED is attached to digital pin 13 of the arduino board to emit client responses as IR signals.

Both arduino board and ESP 32 module is attached to a PC so that python program running on that PC reads serial inputs from arduino board which are decoded VLC signals and send response to arduino board via serial link which will be encoded as IR signals and emitted and finally connects ESP 32 if the AP grant permission to connect.

4.4.2 Server

Main component of AP and Wi-Fi server implementation is based on an another Arduino UNO board. An IR receiver and an IBT2 motor driver is attached to Arduino board. This Arduino board is also initialized with baud rate of 9600 at initial setup.

Like in client setup, IR receiver is attached to arduino board's pin 2 as an interrupt when IR signal comes in, it will automatically receive and decode signals. IBT2 motor driver is attached to pin 13 of the Arduino board so that it will be switched according to VLC signal encoding so that Light Bulb attached to motor driver will also be switched.

A python program which runs on server computer will manage client sessions, authentications depending on the serial inputs from Arduino board which works as AP.

4.5 Challenges and Limitations

The main challenge faced while developing prototype for the proposed protocol was finding suitable set of sensors and illuminating sources.

Photodiode sensor module which capture VLC signals should fast enough to sense changes in VLC source so that it can capture and decode signal correctly. Also it had to be aligned in a way the photodiode exposed to VLC source directly so that it will be exposed to higher intensity of the VLC source.

Photodiode has very low Field Of View(FOV). To increase this, a matrix of photodiode can be used. This should be done when designing luminaire placement.

Two approaches can be given for placement of luminare.

1. Attocell - A single illumination source with multiple LEDs can be placed at center point of physical location so that multiple users can connect with it/
2. Zepto Cell - This is mostly for one device connectivity. Radius is limited fro 5 meters. A single illumination source is used as VLC transmitter.

A more effective luminare placement proposed by previous researchers can be shown as following[19,20].

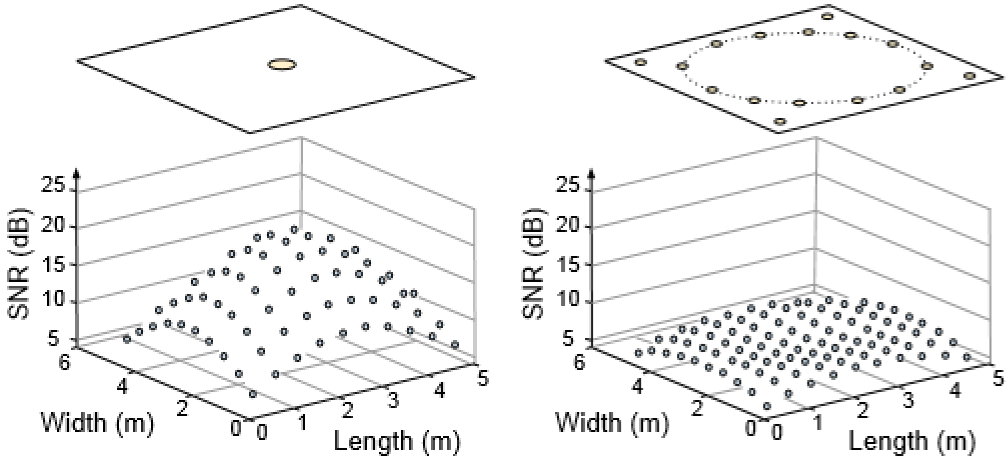


Figure 4.3 - Effective luminare placement design

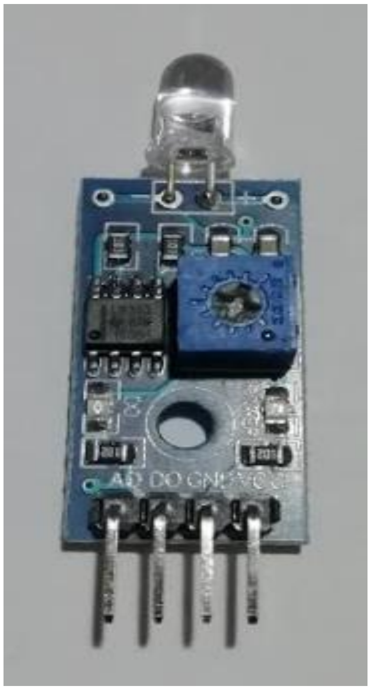


Figure 4.4 - Photodiode sensor used for prototype development

With Ambient light which causes signal distortions or noice, VLC detection can be difficult. This might cause decoding received signals.

IR communication link is set up using IR emitting LEDs and IR detectors. To maintain Line Of Sight(LOS), directed IR beam is used in IR link creation.

For IR emitter and IR LED is used. Several IR receivers were tried in prototype development. Some IR receivers only support few of existing source code libraries which support very small set of functionalities which limits usability of the IR receiver module.

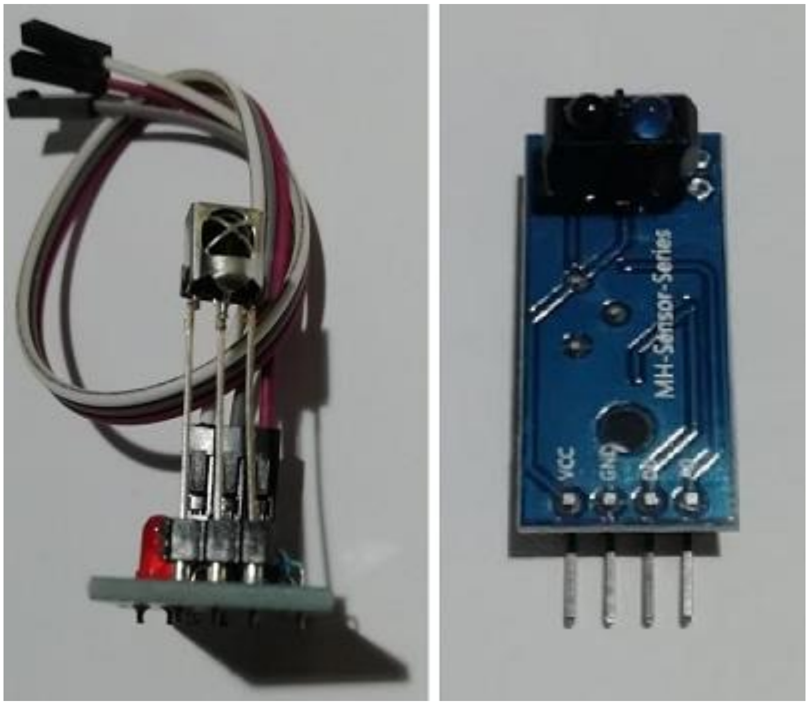


Figure 4.5 - Few IR receivers tried for implementing prototype development

Chapter 5

Evaluation and Results

Following are the flow charts to show how the prototype was evaluated.

5.1 Client Evaluation

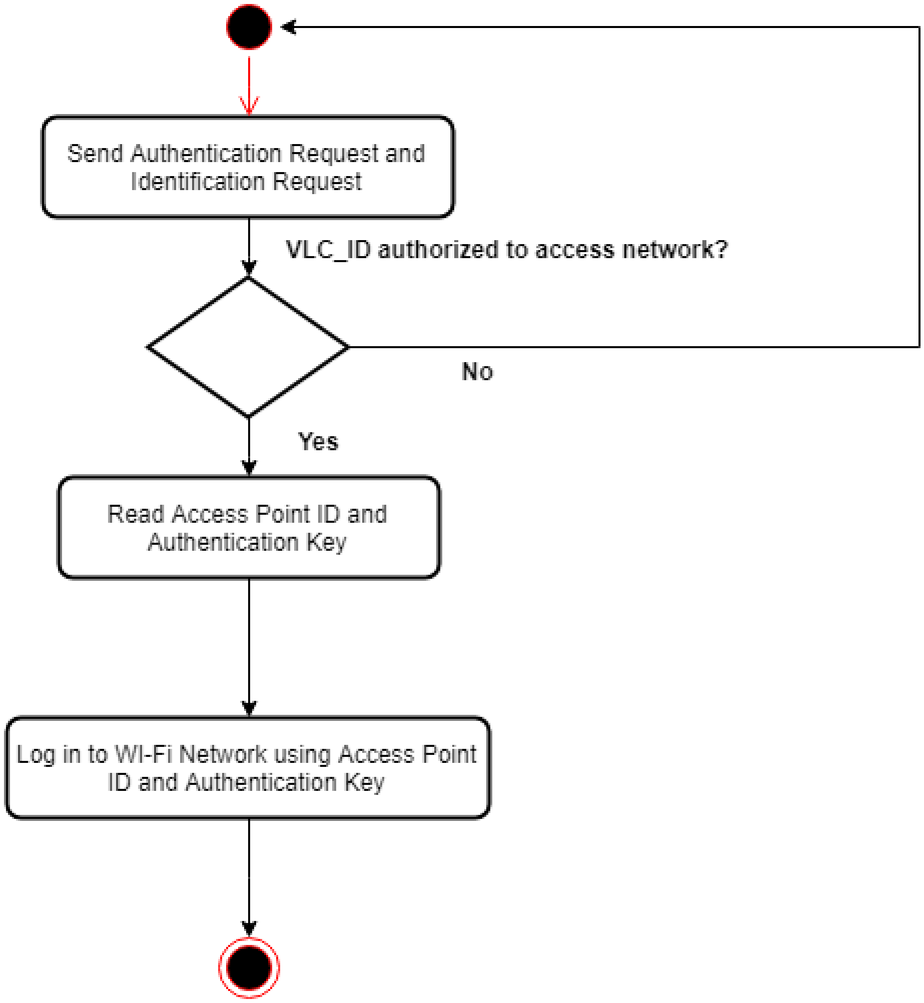

Send Authentication Request and Identification Request
VLC_ID authorized to access network?
No
Yes
Read Access Point ID and Authentication Key
Log in to WI-Fi Network using Access Point ID and Authentication Key

Figure 5.1 - Client Evaluation Flow Chart

5.2 Access Point and Wi-Fi Server Evaluation

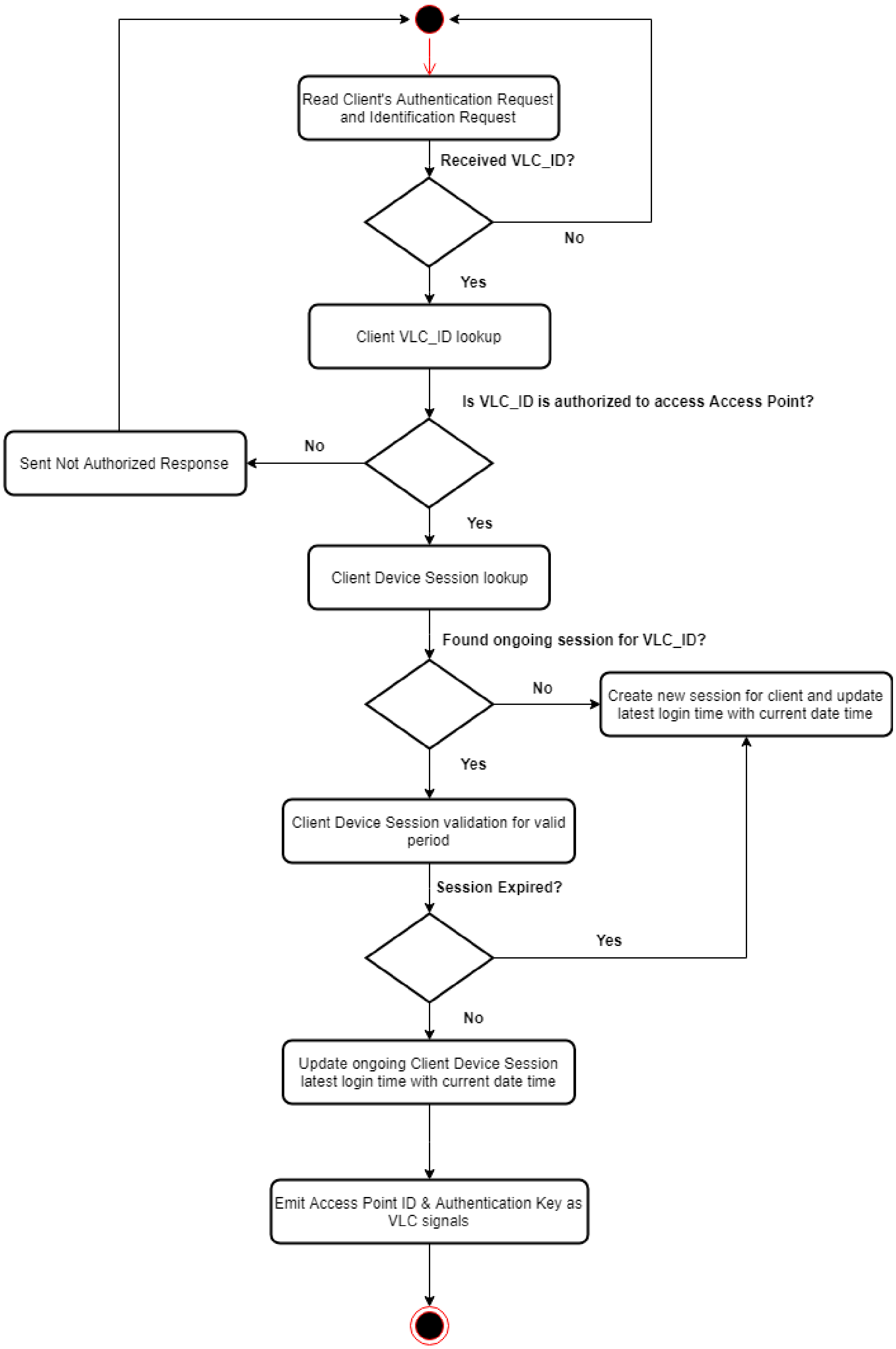

Read Client's Authentication Request and Identification Request
Received VLC_ID?
No
Yes
Client VLC_ID lookup
Is VLC_ID is authorized to access Access Point?
No
Sent Not Authorized Response
Yes
Client Device Session lookup
Found ongoing session for VLC_ID?
No
Create new session for client and update latest login time with current date time
Yes
Client Device Session validation for valid period
Session Expired?
Yes
No
Update ongoing Client Device Session latest login time with current date time
Emit Access Point ID & Authentication Key as VLC signals

Figure 5.2 - Access Point and Wi-Fi Server Evaluation Flow Chart

5.3 Preprocess requirements

Following requirements should be fulfilled before starting authentication process in between Client and AP.

5. AP should have a unique ID(VLC_ID) and an authentication key(VLC_KEY).
6. Client should have a unique ID(VLC_ID).
7. Client's VLC_ID should be registered as an allowed candidate to connect via the considered AP in Wi-Fi server.\
8. AP should emit ready to connect signal sequence periodically so that client can identify AP is ready to authenticate an another client.

5.4 Protocol Steps

Authentication process steps can be listed down as following.

- Client emit VLC_ID and authentication request as IR signals.

- Access Point receiver read the client's VLC_ID and authentication request and send to authentication server.

- Authentication server cross check client's VLC_ID for permissions to access the network via the current Access Point/ from current physical location.

- If client is not permitted to access network, server will send signal to AP to emit VLC signal to let client know that it is not authorized to access.

- If client is authorized to access, server will look up for current ongoing sessions.

- If a current on going session found it will be checked for valid time period. If the session has exceeded the valid time period session will be deleted and new session will be created.

- If a current on going session is not invalid, it will be updated with current date and time as last login time.

- If an ongoing session is not found, a new session will be created and last login time will be updated by current session creation date and time.

- Authentication server will send request to Access Point to emit AP_ID and authentication key for client as VLC signals to login to Wi-Fi network.

- Client read AP_ID and authentication key sent by AP as VLC signals.

- Using received AP_ID and authentication key received, client log in to Wi-Fi network.

Each session created will be timed out when it exceeds predefined amount of time period. After that it will again has to follow same process defined above to authenticate to network.

Chapter 6

CONCLUSION AND FUTURE WORK

The proposed protocol works with combination or VLC and IR communication. It uses special sensor devices which should be attached to existing Wi-Fi enabled device.

Since visible light and infrared can not penetrate through it is a perfect medium for location based messaging. If a person used radio waves, he/she can access network even actual location of that person is several meters away from the AP. Since this protocol depends on Line of Sight(LOS) the newly proposed protocol ensures person is actually located the permitted physical area to access the network.

Another advantage of the proposed protocol is it can be easily adapted with currently existing VLC protocols without any additional hardware changes.

As future work VLC receiver devices used to develop prototype could be replaced with camera modules, solar panels or more efficient and compact sensor modules.

This prototype works on full bright mode of the VLC source. Further researches and improvements could be done to make device operate in VLC source off state so that VLC can be performed and the environment can be kept in dark.

REFERENCES

[1] "Wi-Fi," *Wikipedia*, 09-Sep-2018. [Online]. Available:https://en.wikipedia.org/wiki/Wi-Fi. [Accessed: 13-Aug-2018].

[2] C. P. Suduwella, Y. S. Ranasinghe, and K. D. Zoysa, "Visible light communication based authentication protocol designed for location based network connectivity," 2017 Seventeenth International Conference on Advances in ICT for Emerging Regions (ICTer), 2017.

[3] "Radiofrequency (RF) Safety Manual," *Family and Medical Leave Act (FMLA) | Human Resources*. [Online]. Available:https://www.bu.edu/ehs/ehs-topics/radiation-safety/rf-safety/ radiofrequency-rf-safety-manual/. [Accessed: 15-Sep-2018].

[4] K. P. Dahal, "Mobile Communication and its Adverse Effects," *Himalayan Physics*, vol. 4, p. 51, 2013.

[5] D. S. M. Attalla, "Health Hazards of Mobile Information Communication Technologies," *Mobile Information Communication Technologies Adoption in Developing Countries*, pp. 237–251.

[6] V. Beal, "802.11 IEEE wireless LAN standards," Router vs Switch vs Hub: What's the Difference? Webopedia. [Online]. Available:https://www.webopedia.com/TERM/8/802_11.html. [Accessed: 13-Sep-2018].

[7] "What is WiFi and How Does it Work?," CCM. [Online]. Available:https://ccm.net/faq/298-what-is-wifi-and-how-does-it-work. [Accessed: 13-Sep-2018].

[8] "Rfc 5416 - control and provisioning of wireless access points (capwap) protocol binding for ieee 802.11," 2018. [Online]. Available: https://tools.ietf.org/html/rfc5416

[9] "Authentication Types for Wireless Devices," Cisco, 21-Mar-2015. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/ software/guide/SecurityAuthenticationTypes.html. [Accessed: 14-Sep-2018].

[10] "Visible light communication, networking, and sensing: A survey, potential and

challenges.” IEEE, 2015. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/7239528/

[11] “IEEE 802.15.7 visible light communication: modulation schemes and dimming support,” pp. 72 – 82, 2012. [Online]. Available: http://ieeexplore.ieee.org/document/6163585/

[12] “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,” pp. 1 – 309, 2011. [Online]. Available: http://ieeexplore.ieee.org/document/6016195/

[13] “Home access networks using optical wireless transmission.” IEEE, 2008, pp. 1 – 5. [Online]. Available: http://ieeexplore.ieee.org/document/4699864/

[14] “Sustainable energy-efficient wireless applications using light.” IEEE, 2010, pp. 66 –73. [Online]. Available: http://ieeexplore.ieee.org/document/5673074/

[15] “Fundamental analysis for visible-light communication system using led lights.” IEEE, 2010, pp. 100 – 107. [Online]. Available: http://ieeexplore.ieee.org/document/1277847/

[16] M. A. C. Aung and K. P. Thant, “Detection and mitigation of wireless link layer attacks,” 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), 2017.

[17] C. T. WiFi, “Types of Wireless Attacks – CT WiFi Blog,” CT WiFi Blog, 13-Jun-2017. [Online]. Available: https://blog.ct-networks.io/types-of-wireless-attacks-9b6ecc3317b9. [Accessed: 15-Sep-2018].

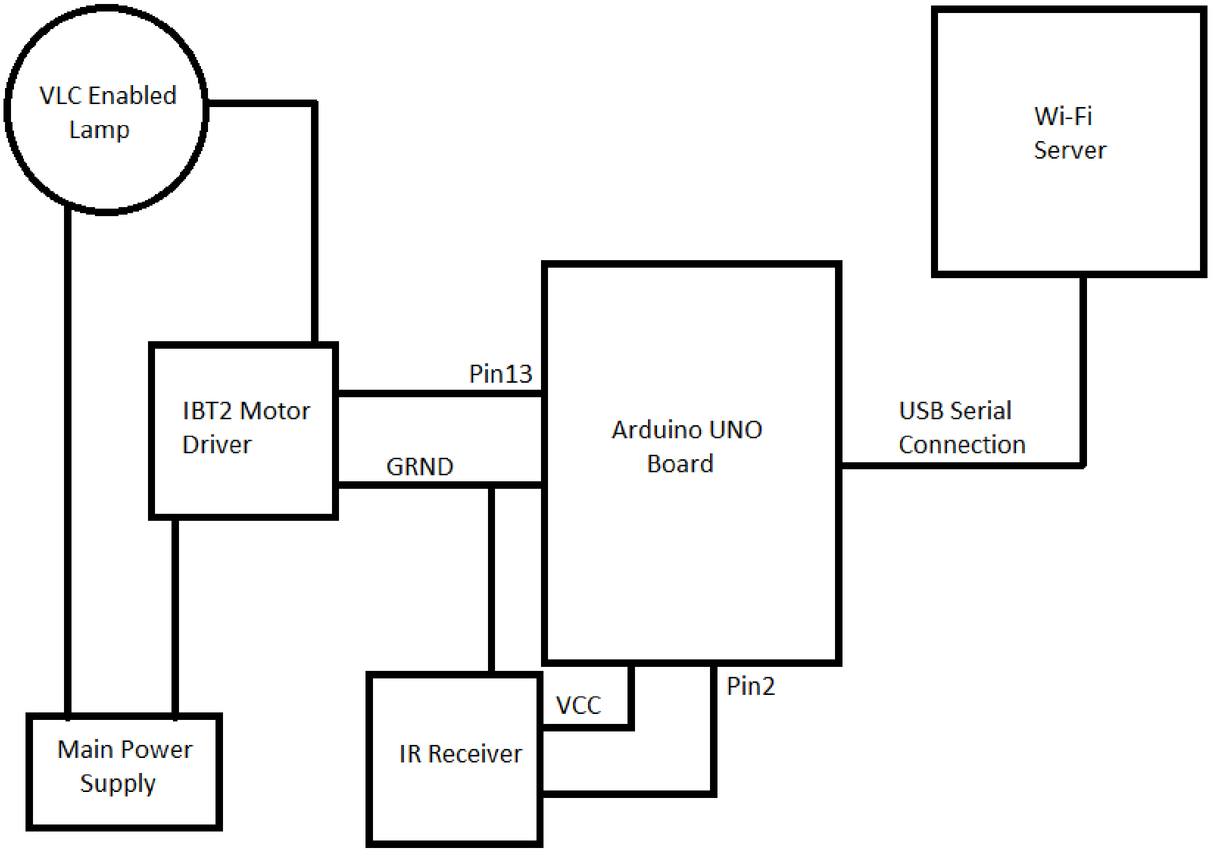
[18] “Visible light communication,” Wikipedia, 26-Jul-2018. [Online]. Available: https://en.wikipedia.org/wiki/Visible_light_communication. [Accessed: 15-Sep-2018].

[19] W.-D. Z. J. C. Z.Wang, C. Yu andW. Chen, “Performance of a novel led lamp arrangement to reduce snr uctuation for multi-user visible light communication systems,” 2012. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-20-4-4564

[20] C. Y. Z. Wang, W.-D. Zhong and J. Chen, “A novel led arrangement to reduce snr fluctuation for multi-user in visible light communication systems,” 2011. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-20-4-4564

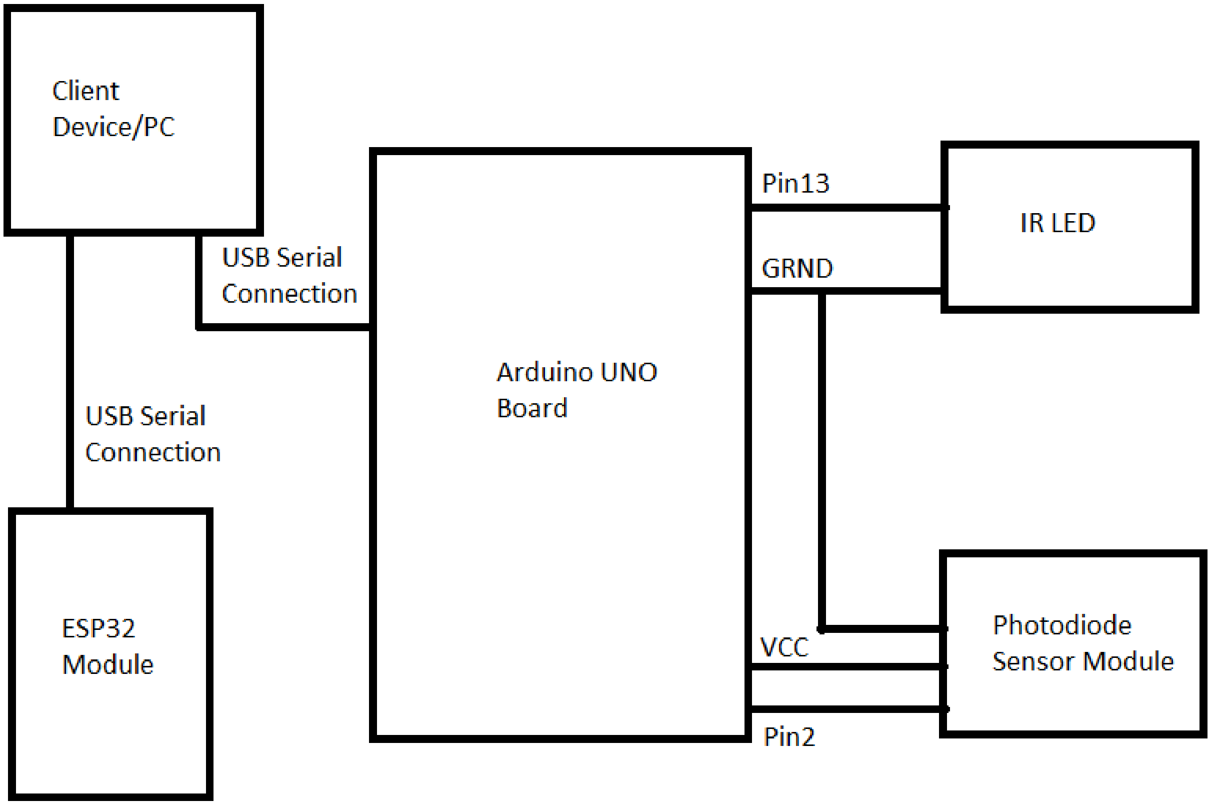
APPENDIX A

Access Point - Wi-Fi Server Circuit Setup



APPENDIX B

Client Circuit Setup


Client
Device/PC
USB Serial
Connection
USB Serial
Connection
ESP32
Module
Arduino UNO
Board
Pin13
GRND
IR LED
VCC
Pin2
Photodiode
Sensor Module