ENGLISH TITLE

Month Year

Student name

Master of Science in Computer Science

HÁSKÓLINN Í REYKJAVÍK

REYKJAVIK UNIVERSITY

ENGLISH TITLE

Student name

Master of Science

Computer Science

Month Year

School of Computer Science

Reykjavík University

M.Sc. PROJECT REPORT

ISSN 1670-8539

English Title

by

Student name

Project report submitted to the School of Computer Science
at Reykjavík University in partial fulfillment of
the requirements for the degree of
Master of Science in **Computer Science**

Month Year

Project Report Committee:

Name, Supervisor
Title, Affiliation

Name
Title, Affiliation

Name
Title, Affiliation

The undersigned hereby certify that they recommend to the School of Computer Science at Reykjavík University for acceptance this project report entitled **English Title** submitted by **Student name** in partial fulfillment of the requirements for the degree of **Master of Science** in **Computer Science**.

Date

Name, Supervisor
Title, Affiliation

Name
Title, Affiliation

Name
Title, Affiliation

The undersigned hereby grants permission to the Reykjavík University Library to reproduce single copies of this project report entitled **English Title** and to lend or sell such copies for private, scholarly or scientific research purposes only.

The author reserves all other publication and other rights in association with the copyright in the project report, and except as herein before provided, neither the project report nor any substantial portion thereof may be printed or otherwise reproduced in any material form whatsoever without the author's prior written permission.

____
Date

____
Student name
Master of Science

English Title

Student name

Month Year

Abstract

English abstract.

Íslenskt heiti

Student name

Mánuður Ár

Útdráttur

Íslenskur útdráttur.

Dedication.

Acknowledgements

Thanks…

Publications

Part of the material in this thesis was published …

Contents

List of Figures

List of Tables

Chapter 1

Introduction

========== In recent years with the bloom of the field of solid state lighting leads to the replacement of florescent and tungsten lamps by Light Emitting Diodes (LEDs). LEDs are low cost, low power consumption and durable than other lamps. There for most houses, universities, government institute and public places used LEDs. LED are support fast switching capable than other lamps and its not cause to damage the lamp. Exponentiation growth of the LEDs and its fast switching capability may have caused opening up researches' eye towards exploring methods to use already

========== 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.

Chapter 2

Background

A. 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

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 throughputs (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.

B. 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 and 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. C. 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. D. 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. E. 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.

Chapter 3

Methods

Part I

Part Name

Chapter 4

Experiments

Chapter 5

Conclusions

School of Computer Science
Reykjavík University
Menntavegi 1
101 Reykjavík, Iceland
Tel. +354 599 6200
Fax +354 599 6201
www.reykjavikuniversity.is
ISSN 1670-8539