BACHELOR PAPER

Term paper submitted in partial fulfilment of the requirements for the degree of Bachelor of Science in Engineering at the University of Applied Sciences Technikum Wien - Degree Program Informations und Kommunikationssysteme

Mobile application able to analyse the Internet connections

By: Gonzalo Buil Bellido, Informations- und Kommunikationssysteme
Student Number: ic20x001

Supervisor 1: Mag. Franz Kopica, Informations- und Kommunikationssysteme

Wien, 23/05/2021

Declaration of Authenticity

“As author and creator of this work to hand, I confirm with my signature knowledge of the relevant copyright regulations governed by higher education acts (see Urheberrechtsgesetz/ Austrian copyright law as amended as well as the Statute on Studies Act Provisions / Examination Regulations of the UAS Technikum Wien as amended).

I hereby declare that I completed the present work independently and that any ideas, whether written by others or by myself, have been fully sourced and referenced. I am aware of any consequences I may face on the part of the degree program director if there should be evidence of missing autonomy and independence or evidence of any intent to fraudulently achieve a pass mark for this work (see Statute on Studies Act Provisions / Examination Regulations of the UAS Technikum Wien as amended).

I further declare that up to this date I have not published the work to hand nor have I presented it to another examination board in the same or similar form. I affirm that the version submitted matches the version in the upload tool.”

Vienna, 23.05.2021

Place, Date

Signature

Abstract

The wide use of wireless networks in every aspect of our life has risen new challenges and situations that affect the majority of the population around the globe. Issues such as interferences between each network, fading or security attacks have to be bearded in mind when a wireless network is set up or when a user wants to establish connection with one. Therefore the goal of this study is the use and development of a mobile application that is able to analyse the wireless networks that the device, a smartphone in this case. With the information obtained from the application the user should be able to find possible solution to the challenges that may arise and to improve the quality of the service that he or she is using in different environments with different characteristics. The testing of the application involved the obtainment of information in three different scenarios, the results of the three scenarios were satisfactory. In all three scenarios the environment could be analysed successfully and solutions could be given to improve the connectivity to each of the access points.

Keywords: Wireless Networks, Mobile Broadband, mobile application, security, access point, WLAN, internet connection.

Acknowledgements

First I would like to thank of my supervisor, Mag. Franz Kopica for the advice, support and patience during my Bachelor Thesis. His patience and continuous support helped me to finish my thesis and to achieve the desired results. I would also would like to thank all my professors from both FH Technikum Wien and from the Universidad de Zaragoza. Thanks to their support and kindness I have gained the necessary knowledge for my future professional life and to finish my thesis and therefore my bachelor. Finally I would like to thank my loved ones, without their continuous and unconditional support anything of this would have been possible.

Table of Contents

1 Introduction

WLAN networks are familiar to everyone nowadays with the accessibility of technology almost worldwide. Also with the progress of technology there are more technological devices in our homes making our home networks more saturated and sometimes do not work optimally.

For many years the power and the bandwidth of our home WLAN networks have become bigger and wider making them more powerful. At the begging the bandwidth of our networks was not a real issue because the amount of devices that we had and the information that was exchanged was very low. However this has changed in the last 2 decades especially with the introduction of smartphones and video streaming in our life. This has led to invest on having more powerful networks and also to design the networks in more optimal structures and topologies.

1.1 Problem definition

In our homes the access point of our Internet Provider is not in the most optimal point. Usually the Internet Provider gives the option to change the access point somewhere else in your house however this involves in more costs and investment. Also in other cases where you may need to choose to which network you connect your device between different available networks is useful to know the characteristics of that network in order to do a task more efficiently.

1.2 Aims and goals

The aim of this project is to create mobile application in this case an application for an Android device that is able to analyse the Internet connections that the telephone is able to detect (service that establishes the connection, duration, quantification, and characteristics of the traffic demanded, technology of the connection; if it is Wi-Fi, mobile or other type of Internet connection) making the information of the analysis available for the user on the phone.

The app must collect from the mobile of the user a series of variables and events to show them as statistics, making the user able to configure his preferences, have access to different services, make a tracing of the services that have been offered vs the requested and improve his own perception of the time that it is being invested to do each task and the quality of the services offered.

1.3 Motivation

There are different options in the market that are able to suit the need. However this applications are usually very basic and the information is displayed in a way that is usually not really intuitive for a basic customer that is not really familiar with characteristics of the Internet connections. So to enable to make this basic information that is useful for everyone, more accessible to more people and easier to understand we can create an application for our phones to spread it in a more visual and basic way.

1.4 Method

On the theoretical part of this project, we are going to learn about the different characteristics of both Wi-Fi and mobile networks and about how our devices make the connections to those networks in order to get access to the Internet.

In the practical part of the project, we are going to prepare a phone application in this case specifically an Android application that is able to check specific parameters of the phone and of the networks that the phone is capable of detect. After successful development of the application the parameters have to be shown in a visual way and to understand those parameters in order to reach a conclusion of the network characteristics.

2 Wireless Networks

2.1 Fundamentals

Wireless Networks are a computer network that use wireless data connection between the different nodes of one network. This type of networks are cheaper than non-wireless networks because they do not introduce cables or connections between various equipment locations which make the cost of the network increase drastically.

2.1.1 History

The first wireless communications that were created and used were every different form the ones we know today. This communications systems used visual signals in order to transmit information, examples of these signals are smoke signals, torch signals, mirrors, signal flares… However all of them had the same characteristic that they were communications systems based in the transmission of simple information over the line-of-sight. Therefore in order to send these messages the stations had to be in high places like hilltops and with high visibility such as places that were along roads. Obviously these kind of communications systems could not transmit complex messages. The ambition of the human being of being able to communicate through longer distances lead into the invention of the first telegraph network by Samuel Morse in 1838 and later the telephone in 1895 by an Italian engineer called Guillermo Marconi [1]. However it was not until 1971 with the invention of ALOHANET, that the first network based on packet radio was invented.

Nowadays this net is not used however one of the essential concepts of this net is the base for the Ethernet. Due to the transmission of this network was made by radio the channel was open and could be used anytime the user wanted, this was a problem when two or more systems in the same net sent information at the same time because there would be collisions. To avoid this there were 2 different methods one of them was to use one frequency for each node, what now we now as frequency multiplexing. However this method has an issue with scalability because you need a different frequency for each system and the bandwidth that we can use is limited. The other solution was to have timeslots for each system making like this to increase the maximum throughput. In order to a station to be able to transmit information it needs to wait until the beginning of a timeslot, making like this the number of collisions lower. Using this method the successful transmissions were a 36.8 % while using the first one were only an 18.4%. The network has a star topology with a computer that operates as the central hub of the whole network. Thanks to the development of these network other networks based on packet data and broadcast radio were created, for example the military of the United States of America and the Defence advanced Research Projects Agency (DARPA) put a significant amount of resources into developing networks that used the basics of ALOHANET [1].

Commercial applications started supporting wide-area wireless data service and therefore packet radio networks became more popular. They were first introduced at the beginning 1990's and data access at low speed (around 20 Kb/s) was enabled and supported. However these services almost disappeared in the 1990s, these services were replaced by cellular telephones and wireless local area networks (WLANs) [1].

In 1985 the commercial development of wireless LANs was permitted. This event happened thanks to the Federal Communications Commission (FCC) that authorized the public use of the Industrial, Scientific and Medical (ISM) frequency bands. The permission by the FCC to use these bands was very attractive for the wireless LAN vendors as they did not have to obtain a license from the FCC in order to operate or use those frequency bands. The first WLANs had a very poor performance and were very inefficient, the data rates and coverage were very poor due to the high interference from other uses that used also the ISM frequency bands [1].

Nowadays the WLANs that are being used are based on the IEEE 802.11 standards family. Wired Ethernet offers a higher data rate and this gap in the data rate being offer is likely to increase with the years, however the WLANs are becoming more popular and more preferred as the Internet access method in environments such as homes, offices and university campus, as they give more freedom [1]

2.1.2 Types of wireless links

Different wireless networks have different kind of transmitting the information and due to this different links to transmit the information. We can name the following wireless links [1]:

- **Terrestrial microwave**: this communication type uses terrestrial antennas in order to transmit information. This terrestrial antennas also called as terrestrial microwaves work in the low gigahertz range which limits all communications to line-of-sight. The stations and the repeaters are separated 48 km from each other in order to ensure a good communication.
- **Communications satellites**: this type of communication needs to use microwaves in order to avoid deflections by the atmosphere of the Earth. The satellites are stationed on space, typically in geosynchronous orbit 35.400 km above the equator. Some of the multiple uses of this systems are voice transmission and transmission of TV signals.
- **Cellular and PCS systems**: the main characteristic of this system is that it divides a territory into different areas called cells. Each of these cells have a low-power transmitter in order to communicate give coverage in that specific area.
- **Radio and spread spectrum technologies**: enables communications of devices in areas where there are limitations in terms security and interferences as these technologies are more resistant to noise and jamming.

- **Free-space optical communication**: use line-of-sight or non-line-of-sight communication. The most common one of these two it is line-of-sight communication however it limits the position and the mobility of the devices that are taking part of the communication process.

2.2 WWAN

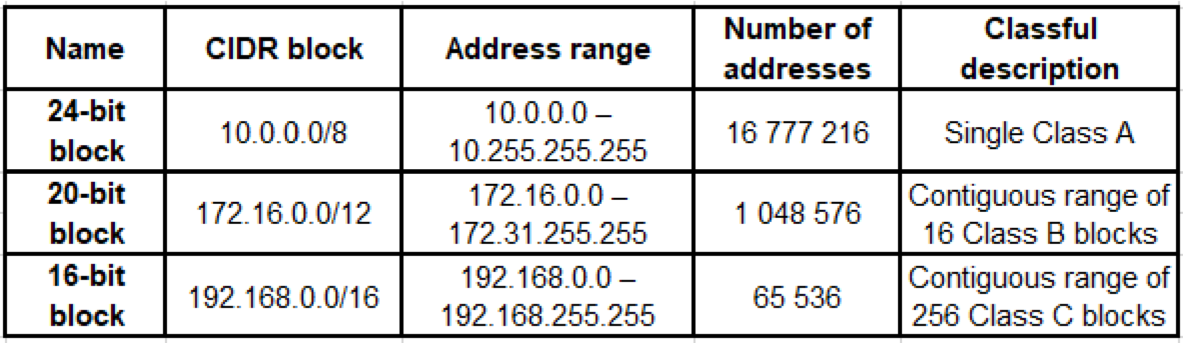
Wireless wide area networks (WWAN) are telecommunications networks that extend over a wide geographic area for the main purpose of exchanging data. This kinds of networks are usually used by businesses, schools and government entities in order to give an access to the data to staff, students, clients, customers or suppliers from various locations all over the globe. The Internet can be considered as a kind of WAN.

2.2.1 Architecture

The WWANs are different from other networks because they use the cellular network technology, which will be explained in chapter 3.2.1.1., examples of this kind of technology can be found in 2G, 3G, 4G LTE and 5G. Sometimes it is also known as Mobile Broadband. These technologies are offered by a wireless service provider and depending on the service that is being paid the coverage can be in a small region or even globally. A WWAN allow a user with a device and a WWAN card to surf the Internet from everywhere where there is coverage by the wireless service that has bought. Usually this kind of networks are used to interconnect smaller networks such as WLANs [31].

2.2.2 Private Networks

There are 2^{32} addresses defined in IPv4, that is approximately 4 billion addresses and 18 million out of that 4 billion addresses are private addresses. These private addresses are divided into 3 ranges and they are not accessible from public routers in order to communicate with a host that has a private IPv4 address a network address translation it is needed at the router gateway [31].



Name	CIDR block	Address range	Number of addresses	Classful description
24-bit block	10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 216	Single Class A
20-bit block	172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 576	Contiguous range of 16 Class B blocks
16-bit block	192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 536	Contiguous range of 256 Class C blocks

Table 1: Reserved private IPv4 network ranges [37].

So if there are two private networks, e.g. two networks from the same company but they are located in different geographical areas and they need to be connected, they cannot be interconnected using the Internet because as we have just explained the packets are not routable and are ignored by public routers. Therefore in order to interconnect both we need a WWAN (private WWAN). For these networks to be able to connect to the Internet is necessary to be bridge to the Internet via a virtual private network (VPN) or an IP tunnel, which encapsulates packets, so that the private address inside their headers is encapsulated with a header with a public address [31].

2.3 WMAN

Wireless Metropolitan Area Networks (WMAN) networks enable the users to establish wireless connections between several locations in the same metropolitan area, e.g. between several office building of one specific city o in a university campus, without the high cost of the installation of fibre optic or copper cables and the renting of the those lines.

WMAN use radio waves or infrared light to transmit the data. These networks have a lower action radius than the WWAN networks and a group of these networks form a WWAN. The radius is on the order of tens of kilometres, which is enough to cover a complete city. The main standard responsible of implementing WMANs is IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX). It used unlicensed and licensed bands to offer wireless connections for non-line-of-sight communication and data transfer, the data rate was up to 40 Mb/s per channel and a cell radius was up to 10 kilometres [40].

2.4 WLAN

2.4.1 History

Wireless Local Area Networks (WLAN) is the most popular technology for setting up wireless commuter networks, but this was not the situation always. At the beginning of the 1990s WLANs had almost no popularity nor success in selling to companies and campus environments that they were the replacement of wired LANs and the advantage of mobility that they had. The WLANs products of that day were inefficient and also cost inefficient compared to the wired LANs. Furthermore, mobile network connectivity was not as expanded as the technology was not as developed and the quality of service (QoS) was very poor compare to the wired based services [4].

In the middle of the 1990s four companies: Proxim, Symbol, Lucent (the former NCR WLAN division) and Aironet (which was still part of Telxon) formed and consolidated the WLAN industry and market [4]. However it was not until the late 1990s when the first important market opportunity appeared for the WLANs, as they were able to give the service of having a broadband internet connection in a home and to be able to have multiple devices connected to it. Thanks to this the WLAN products were chosen not by the enterprises but by the regular consumers, making the WLAN products more and more important, reaching to the level that we know today.

The group in charge of the standardization of the WLAN technology is IEEE 802.11, this group started to work in 1990 after having the approval of the IEEE 802 ExCOM, which is the committee in charge of the decision making inside IEEE 802. However until 1994 it was not possible to standardize the main parameters in the MAC and PHY layer [4][5]. The 802.11 working group was in charge of developing a standard similar to the already existing 802.3 standard for Ethernet but for wireless networks. However some challenges arose as there was a battle between the frequency hopping and direct sequence products which cause the division of the PHY layer into three specifications:

- Frequency hopping
- Direct Sequence
- Infrared

These three physical (PHY) layers are not capable of work with each other and also the direct sequence and frequency hopping PHYs both transmitting at 2.4 GHz caused interference between them if they are located one next to each other. These two PHY layer specifications support 1 Mb/s and 2 Mb/s data rates.

It was not until 1997 to the 802.11 standard to be formally considered as an IEEE standard. By this time the products were a success at the market and available at a lower cost and even in some cases higher performance to the 802.3 counterpart [4] [5].

The IEEE developed four main standards:

2.4.1.1 802.11a

At the beginning of 1997 the High Speed Study Group was created inside the 802.11 working group. This High Study Group decided in March of 1997 that two different groups should be created in order to create the standards, this lead to the creation of two Task Groups [4].

One of the first proposals was to elaborate a “Standard for Wireless Medium Access Method (MAC) and Physical Layer (PHY) Specifications – Supplement for High Speed Physical Layer (PHY) in the 5 GHz band” [4]. The final creation of the Task Group A (TGa) occurred thanks to a final refinement by the Study Group and the approbation of the IEEE 802 committee. TGa had the main task to develop the PHY layer standard, this standard was called 802.11a standard in mid-1997. The formation of TGb occurred using the other proposal and the main aim was to develop higher speed 2.4 GHz PHY layer, this standard was later called 802.11b [4].

The specific goals that were set by the 802.11a committee were to create a proposal to 802.11 to operate with a PHY data rate of 20 Mb/s or greater under the 5 GHz U-NII rules. At that time there were some individuals that believed that the TGa should adopt HIPERLAN and develop the standard with this embracement. This would mean the creation of a global standard for the wireless LANs, however this meant that some countries like Japan that have their own norms in terms of telecommunications and that are independent from the IEEE committee would also adopt this standard [4]. Finally this was not feasible as the HIPERLAN MAC layer had many differences from the 802.11 MAC layer and the TGa group did not had the authority and permissions by the IEEE committee to change it [5].

802.11a devices work at 5-6 GHz range and support even high data transfers rates up to 6, 12, 24 and 54 Mb/s. 802.11a devices work at a different frequency ranges than the 802.11b devices. This makes the interoperability of both the devices of different standards impossible making this one of the most important limitations of the standard [21].

The second drawback of the standard is the unavailability of free cost 5 GHz bands in some countries in the world and this is why IEEE called for planning to present the IEEE 802.11g standard [21].

2.4.1.2 802.11b

As it was mentioned in the last chapter, the formation Task Group B (TGb) was authorized by IEEE in 1997. The main task of TGb was to develop a high data rate PHY layer proposal. Other goals of the TGb were to achieve a data rate of 10 Mb/s in the 2.4 GHz band belonging to the ISM band and it should also have compatibility and interoperability with some of the already existing 802.11 PHYs [4].

In 1997 it was thought that it was a boundary at 4 Mb/s that could not be surpassed by either direct sequence or frequency hopping spectrum devices that already existed and that followed of the FCC 15.247 ISM band rules at 2.4 GHz. This was validated by the 802.11 PHY at the beginning and by the vendors of the products that were available at the market at the time [4].

Surpassing maximum limit of 4 Mb/s using frequency hopping and the channel bandwidth limit imposed by the FCC was really difficult to achieve. Even getting to both limits would require a very complex system and the WLANs of that time usually only reached maximum data rates of 1 or 2 Mb/s. In an attempt of surpassing this limit a WLAN company called Symbol Technology proposed to the FCC to change the maximum channel bandwidth from 1 MHz to 5 MHz. This would mean that the maximum possible data rate would increase to 10 Mb/s for this kind of WLANs that are based on frequency hopping. However the FCC did not accept this proposal, this fact made frequency hopping never a valid candidate for TGb [4][5].

In order to surpass the limit of 4 Mb/s data rate direct sequence spread spectrum (DSSS) should be used as the PHY layer method of the standard. The change from a 2 Mb/s DSSS 802.11 to an 11.2 Mb/s 802.11b systems was very easy because the modulation layout of both of them are really similar to each other. The coexistence of both DSSS systems was possible thanks to allowing a smooth transition to higher data rate technology, and performance to be greatly improved while maintaining the same protocol [21].

2.4.1.3 802.11g

The 802.11g standard was announced as the new standard that was going to replace 802.11a and improve 802.11b. The standard was created by 802.11g Task Group (TGg) and followed a similar process to the one that follower the TGa [4]. The new standards use the same OFDM based transmission scheme as 802.11a and works in the 2.4 GHz band as 802.11b. The maximum data rate at which the physical layer operates is 54 Mb/s, this data rate is exclusive of forward error correction if not the average data rate is of 22 Mb/s [21][24].

The 802.11g presented two different modulation techniques that support the different data rates:

- OFDM: offers a data rate of 54 Mb/s for its payload.
- Packet binary convolution code (PBCC): offers speed of data at a rate of 22 and 33 Mb/s for its payload.

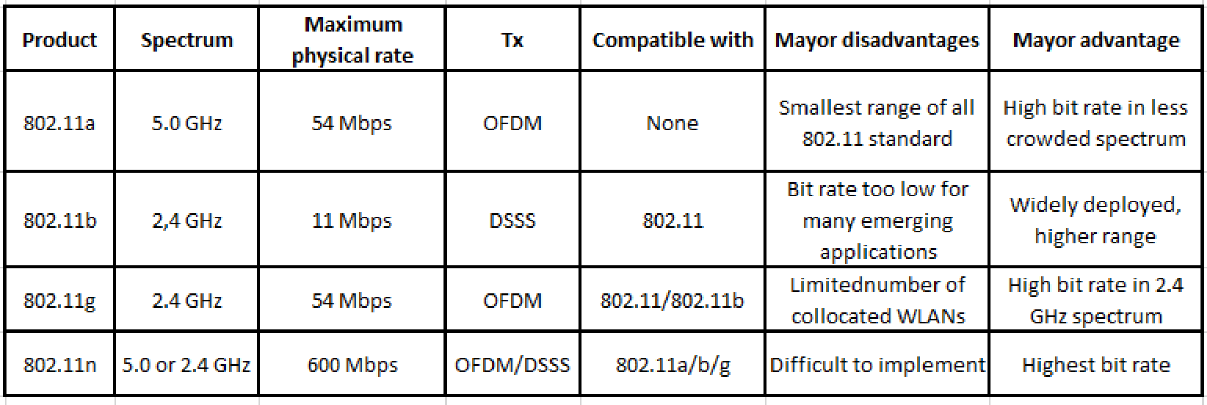
The most important advantage of this standard is that addressed and resolved the compatibility issue with 802.11b products in 802.11 products. IEEE finalized the 802.11g standard on 13 June 2003 [25].

2.4.1.4 802.11n

At the beginning of 2002 a ‘High Throughput Study Group’ was created and then in September 2003 this group transformed and was the base of the creation of Task Group N (TGn). The main objective was to create a new generation of PHY that would offer data rates of over 100 Mb/s in both the 2.4 GHz and 5.0 GHz band. The standardization process that followed the TGn was the same as TGg and TGa [4].

In October of 2009 the standard was published after being approved by the IEEE committee. Before the final approval by the IEEE, companies and enterprises were already changing their 802.11n networks that are based on the Wi-Fi Alliance’s certification to the networks based on the 802.11n standard [28].

The following table summarizes characteristics of previous standards and compares their advantages and disadvantages [21] [26].



Product	Spectrum	Maximum physical rate	Tx	Compatible with	Mayor disadvantages	Mayor advantage
802.11a	5.0 GHz	54 Mbps	OFDM	None	Smallest range of all 802.11 standard	High bit rate in less crowded spectrum
802.11b	2,4 GHz	11 Mbps	DSSS	802.11	Bit rate too low for many emerging applications	Widely deployed, higher range
802.11g	2.4 GHz	54 Mbps	OFDM	802.11/802.11b	Limitednumber of collocated WLANs	High bit rate in 2.4 GHz spectrum
802.11n	5.0 or 2.4 GHz	600 Mbps	OFDM/DSSS	802.11a/b/g	Difficult to implement	Highest bit rate

Table 2: Wireless LAN products on the Market [21] [27].

2.4.2 Architecture

A WLAN is formed mainly by two important elements:

- **Access Points (AP):** they are in charge of giving a service to the users. Each access point reaches an area of coverage which its form and dimensions depend on the power, type and orientation of the antenna, structure of the building, and obstacles in the path way of the electromagnetic waves… Each AP has its own Basic Service System Identifier (BSSID) (the MAC address of its wireless interface). The BSSID cannot be changed.
- **Stations (STAs):** they are the wireless interfaces of the systems of the user (personal computers, tablets, smartphones, e-books, etc.)

These basic two elements are the principle for the creation of a WLAN network, however there are several challenges that have to be taken into account in order set up and working with wireless local area networks [5] [6]:

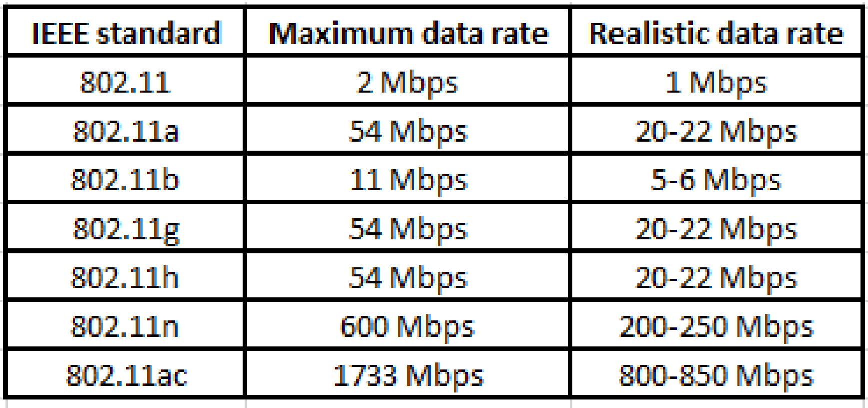
- **Interference with other sources:** as WLAN and Bluetooth both operate in the same frequency bands this may cause interference between different sources and therefore problems in the communication. Other devices such as motors or microwaves ovens that create electromagnetic noise also generate interferences.
- **Multipath propagation:** this challenge arises when the transmitted electromagnetic waves are reflected and take different paths in order to arrive to the receiver. These paths are from different length, affecting the signal power received and therefore make the signal that gets to the receiver more difficult to interpret. A similar scenario to this occurs when objects move through the direct path between transceiver and receiver during the communication process. In this situation the propagation paths will also

change as the objects will generate reflections. In order to avoid this problem one possible option is to use at reception two different antennas at a certain distance to each other and only use the strongest signal as the correct one in order to continue the manipulation of the information.

- **Hidden terminal:** (invisible or hidden terminal devices) obstacles in the middle of the path from the sender and the receiver may cause that some devices are not identifiable by others making the communication process impossible.
- **Fading:** (decreasing signal strength) obstacles cause reflections and attenuation of the electromagnetic waves, however they are not the only responsible of fading of these waves also the channel attenuates the electromagnetic waves. This issue can be solved by the implementation of repeaters in the middle of the communication path.

2.4.2.1 Data rate and power of WLAN

Each of the different WLAN standards offer different maximum data rates. All the devices and signal emitting stations share teh same bandwidth for both upload and download, however these were reduced depending on the media access method that each standard used. The total data rate takes into account the transmission of data that it is not part of the payload of the package, this means that there is also part of data that it is being transmitted that it is not part of the message that the user wants to transmit. This can be seen in Table 3 that the data rate of data at the payload is a bit more than half of the total data rate .



IEEE standard	Maximum data rate	Realistic data rate
802.11	2 Mbps	1 Mbps
802.11a	54 Mbps	20-22 Mbps
802.11b	11 Mbps	5-6 Mbps
802.11g	54 Mbps	20-22 Mbps
802.11h	54 Mbps	20-22 Mbps
802.11n	600 Mbps	200-250 Mbps
802.11ac	1733 Mbps	800-850 Mbps

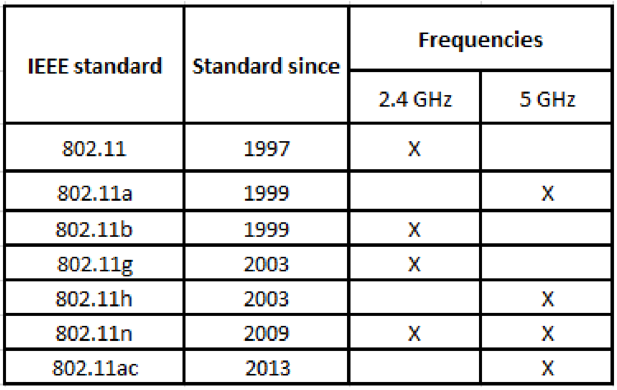
Table 3: Data Rates of the IEEE Standards for WLAN [5].

Due to the fact that WLAN was initially design to be used in homes and environments where the user is not very far away from the Access Point (AP), it uses low power in order to trasmit information (maximum signal level of 100 mW at 2.4 GHz and 1 W at 5 GHz), a level which is considered safe for the human health. If this transmission power is compared to the maximum transmission power permitted for GSM, it can be seen that for GSM the maximum transmission significally more, the maximum power is 2 W working at the 880-960 MHz frequency range.

Some WLAN devices operate at a power up to 1 W for the 2.4 GHz frequency band however they are banned in some countries suchs as Germany [5] [6].

2.4.2.2 Frequencies and modulations of WLAN

The majority of WLAN standards use the frequency blocks of 2.4 GHz or 5 GHz or even both of them. Each standard are different to each other as they use different data rates (Table 3), frequency blocks (Table 4) and modulation methods (Table 6).

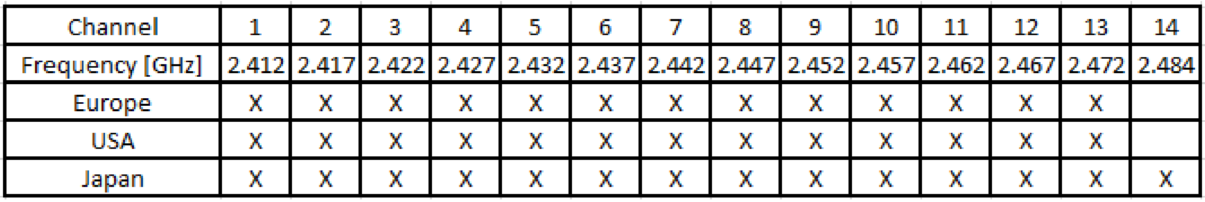


IEEE standard	Standard since	Frequencies	
		2.4 GHz	5 GHz
802.11	1997	X	
802.11a	1999		X
802.11b	1999	X	
802.11g	2003	X	
802.11h	2003		X
802.11n	2009	X	X
802.11ac	2013		X

Table 4: Frequencies of the IEEE Standards for WLAN [5].

WLAN is currently used all over the globe, however each country has its own rules in terms of the use of the standards, for example in Germany the frequency range from 5.15 to 5.35 GHz it can be only used inside buildings with a maximum power of 200 mW [6].

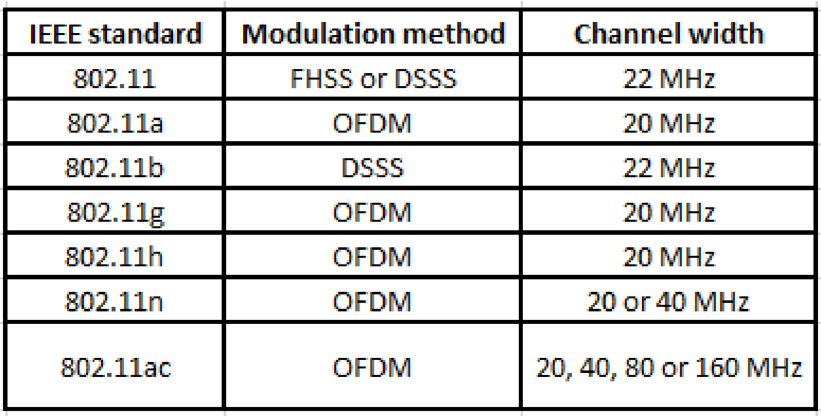
The two frequency blocks of WLAN are divided into channels as it happens with television and radio broadcasting. The frequency block of 2.4 GHz is divided into 13 different channels each with a bandwidth of 5 MHz. In Japan there is an extra channel which is located 12 MHz above the last channel and the only modulation method that can be used is DSSS (Table 5).



Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Frequency [GHz]	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484
Europe	X	X	X	X	X	X	X	X	X	X	X	X	X	
USA	X	X	X	X	X	X	X	X	X	X	X	X	X	
Japan	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 5: Permitted used of the WLAN Frequencies in the 2.4 GHz range [5].

Also the different standards for WLAN use different kind of modulation methods (Table 4). Depending on the modulation method used the bandwidth of the channels and the channel spacing will be different. For standards like 802.11b that use a DSSS as their modulation method the channel width is wider than in other standards that use OFDM as DSSS distributes the payload over a wider frequency range [7]. For 802.11b standard it can be seen in Table 6 that the channel width is 22 MHz and the spacing between channels is 5 MHz. For other standards that use OFDM as the modulation method, for example 802.11g and 802.11n the channel width is 20 MHz [5] [6]. Each channel is divided into 64 sub-carriers of 0.3125 MHz width, however only 52 out of the 64 subcarriers are used [8].



IEEE standard	Modulation method	Channel width
802.11	FHSS or DSSS	22 MHz
802.11a	OFDM	20 MHz
802.11b	DSSS	22 MHz
802.11g	OFDM	20 MHz
802.11h	OFDM	20 MHz
802.11n	OFDM	20 or 40 MHz
802.11ac	OFDM	20, 40, 80 or 160 MHz

Table 6: Modulation methods and Channel Widths of the IEEE Standards for WLAN [5].

The devices that use the 802.11a standard also use the modulation method OFMD and the channel width is 20 MHz, however in this particular case they operate at the 5 GHz frequency range. As it can be seen in Table 6 the 802.11n standard also allows the use of channels that have a width of 40 MHz for this case only two channels fit in the 2.4 GHz frequency block (channel 3 and channel 11). Instead of being divided into 64 sub-carriers they are divided into 128 sub-carriers of 0.3125 wide and 108 out of the 128 are used. This standard can also operate at the 5 GHz frequency block [5].

2.4.3 Types of wireless LAN

WLANs have two basic modes of communication ad-hoc mode and infrastructure via an access point:

2.4.3.1 Ad-hoc mode

In Ad-hoc mode (Figure 1) or also called Independent Basic Service Set (IBSS), the terminal devices form a meshed network (every node of the network is connected to all the nodes of the network). In this type of WLAN the terminals are directly connected to each other without using an Access Point (AP). Each terminal device can be connected to multiple devices. The network name (Service Set Identifier, SSI) and the encryption parameters have to be the same in all the terminals of the network in order to set up this type of network. In this kind of networks the STA which initiates the network chooses a BSSID random and the user must configure the Extended Service System Identifier (ESSID). This characteristics make this network easier to create and suitable for cases such as small organizations where there is no interest for one computer to see information from other computers, or even for rapidly setting up cases in a conference centre or a meeting room [21].

2.4.3.2 Infrastructure mode

In infrastructure mode, each terminal is connected an access point of a WLAN using their MAC address. The access point sends small packages to all the terminals inside its coverage area at adjustable time intervals. These packages contain information about the network and the access point, for example the network name (SSID), the list of the supported and maximum data rates as well as the encryption type and the security mechanisms. This modes can be divided into two topologies depending on its structure:

- Basic Service Set (BSS), Figure 2: exist a unique cell controlled by one AP [5]. The geographical area covered by a BSS is known as the Basic Service Area (BSA) [21].
- Extended Service Set (ESS), Figure 3: it is compound by several BSSs (each one with its own AP) connecting them through a distribution system (DS) which it is usually an Ethernet network. In this architecture, the stations can be mobile and travel to one cell to another and connect to another AP, this is called roaming and will be explained later [5] [21].

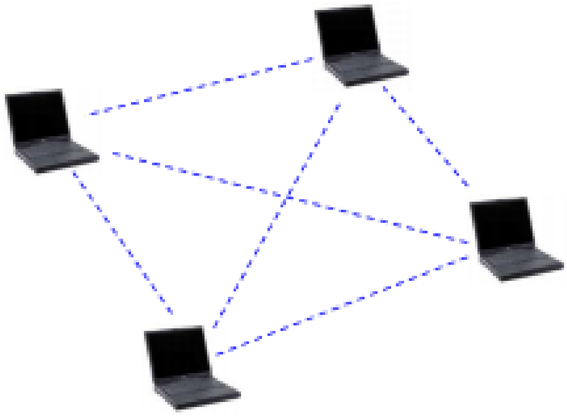


Figure 1: Example of an Ad-Hoc network.

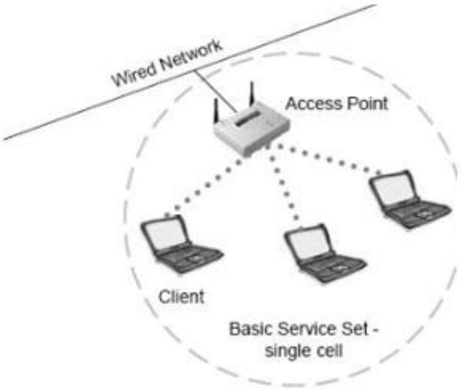


Figure 2: Example of a BSS

Each WLAN has its own SSID (Service Set Identifier) also sometimes called ESSID (Extended SSID). The SSID is a chain of 32 characters that can be configured by the user. If we only have an isolated AP (Basic Service Set, BSS) it will have both a SSID and a BSSID, if we have several APs forming an Extended Service Set (ESS) i.e. all connected at level 2 with a Distribution Service (DS), each AP has its own BSSID and all of them share the same SSID.

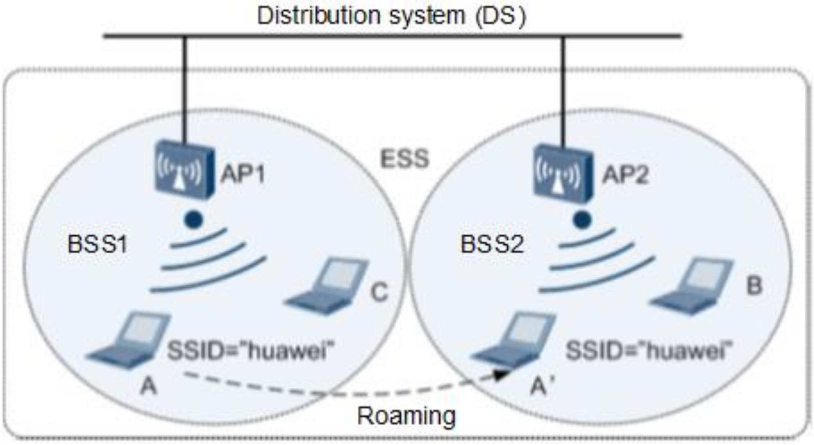


Figure 3: Example of an ESS network.

2.4.4 Roaming

Roaming is a crucial part in the WLAN technology as it delivers a global access to the Internet to all the users at any time without interruption. However this basic concept can create interruptions due to the authentication that must be carried out each time a roaming user visits another network. In order to avoid this interruptions and to make the roam from one network to another a handover authentication protocol is used [28]. Many other protocols were also possible candidates but they were not as efficient and secure as the handover authentication protocol.

For the roaming process three devices are needed: mobile nodes, access points and an authentication server in order to perform the authentication process. The first operation a mobile node does when a user wants to access the service of a WLAN through an AP is authenticate itself to the server, in this case an authentication server. After a correct authentication process and the approval of the authentication server the mobile device establish a connection to the AP and is able to use all the services offered by the WLAN. When this mobile node wants to move from the coverage area of the first AP to a coverage are of a second AP the authentication protocol has to be carried out again at the new AP. In order to avoid interruption in the service the new AP create session keys between the mobile and the new AP making the communication more secure, this process is dome using the handover authentication protocol [28].

2.4.4.1 Internal Roaming

Internal Roaming also known as L2 Roaming occurs when mobile station or mobile device roams from the coverage area of one AP to the coverage area of other AP that belong to the same network. This type of roaming happens in home environments, where the signal has low power. It is called L2 Roaming because it occurs in the data link layer as the user roams to an access point of the same network [29]. The process of internal roaming has the following phases [28]:

- The client makes the decision to roam.
- A new AP is chosen to establish connection with.
- The authentication process with the new AP is repeated.

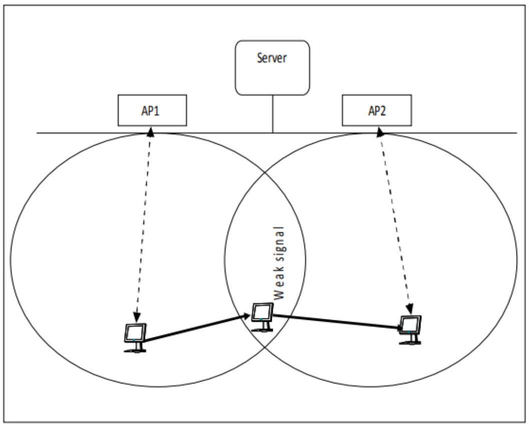


Figure 4: L2 Type Wireless LAN Roaming [28].

In the L2 roaming scenario the client that is roaming first has to disconnect all the connections with the AP to which is connected with and then establish the connections with the new AP. Therefore there is a time interval in which the client is not connected with any AP and due to that it cannot send or receive data. There is a huge list of protocols such as handover, authentication without key…, that make this interval almost zero and ensure security during the communication process [28].

2.4.4.2 External Roaming

External Roaming also known as L3 Roaming occurs when mobile station or mobile devices roams from an AP to another AP but in this case they do not belong to the same network. This type of roaming usually occurs when a client roams between WLANs of different Internet Service Providers (ISPs) [28].

In this situation each of the APs belong to different networks of different ISPs, therefore in the roaming process the roaming client would have to change its IP address when it roams to the new network. However this is not allowed, therefore another method had to be invented in order to enable external roaming. The method that was created consisted in keeping the address that the client device had at the old network and creating a tunnel from the old network to the new one, this method is described in the RFC5944 [30]. The packages that are sent are encapsulated into new IP packages and contain the address at the new network of the client as the destination address [29].

2.4.5 Security

The transmission channel of information for WLANs is open space, this, as it has already been explained, leads to some advantages such as mobility but also to some disadvantages like interferences and security issues. Usually the distances between the transceiver and the receiver are a couple of hundred of meters long, making all this travelled area unsecure and risky, as unauthorized individuals can access the information that is being sent. Because all of this security protocols and encryption protocols are necessary for the exchange of information at WLANs [20].

The security standard Wired Equivalent Privacy (WEP) is implemented in WLAN as it says the 802.11 standard. This security standard is based on the RC4 algorithm, as it is shown in Figure 5. The algorithm first does the calculation of the XOR of the payload bit stream and a pseudo-random bit stream that is generated by the algorithm. The length of the keys are 40 Bits or 104 Bits. This are static keys therefore they can be cracked easily using known-plain text attacks. The calculation of one of these keys can take a few minutes if the attacker has the correct knowledge and use the correct attacking methods. To do so the attacker would only need to record data and then with an application predict the WEP key [5]. WEP use two method of authentication [21]:

- **Open System Authentication:** The client is not required to provide its identity to the access point (AP), which means that any client can try to associate itself.
- **Shared Key Authentication:** the client is requested to have a WEP encryption key that can be used to access the network.

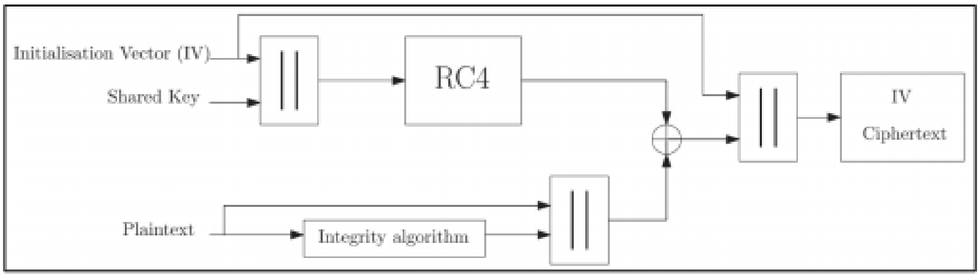


Figure 5: Encryption in WEP. [22]

Wi-Fi Protected Access (WPA) offers a better security than the WEP standard. As the WEP standard, WPA is also based on the RC4 algorithm but instead of using static keys it offers more security by using dynamic keys. It was created in 2003 with the objective of solving the problems and the security weaknesses of the WEP standards [21].

Each data package is encrypted with a different key thanks to the Temporal Key Integrity Protocol (TKIP) [5]. The TKIP sequence number, transmitters address, and an encryption key are entered to the key matrix algorithm to determine a 128 bit per-packet key. This process is done for each packet and this avoids the attacks that compromised WEP. Unlike in WEP, in WPA the per-packet key is used for generating new keys and not for encryption. In parallel, and to ensure data integrity and avoiding cross-site forgery attacks , a Message Integrity Code (MIC) is generated using 64 bit Michael key and plaintext packet MSDU. The MIC and the MSDU are entered to a fragment module along with the TKIP sequence number, the module divides the MSDU into smaller MPDU. Finally, MPDU packets with the per-packet WEP key are used as input to the WEP protocol that generates the cipher-text [21]. The WPA encryption process is shown in Figure 6 [23].

The WPA security protocol can also be cracked and attacked using the brute force or using dictionary attacks to the chosen password [5], especially in the PSK mode when we are using a weak password. The dictionary attacks can be performed if we are using a password that is less than 20 characters [21].

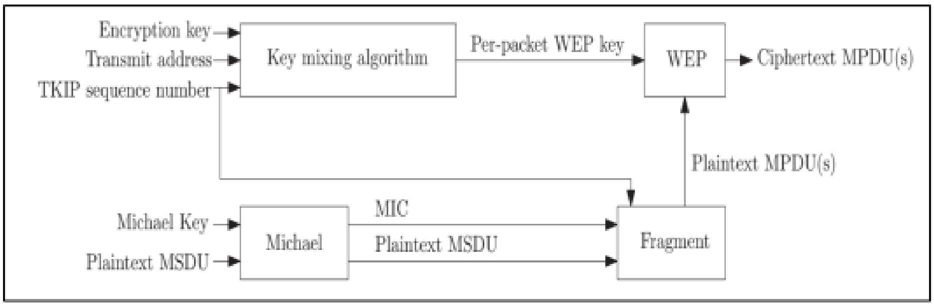


Figure 6: Encryption in WPA. [23]

The best current standard that is also the most popular one nowadays is Wi-Fi Protected Access 2 (WPA2). It was first released in 2004 by the Wi-Fi Alliance as a replacement of WPA and it one of the main objectives was to improve the security in the MAC layer [21]. WPA is based on the Advanced Encryption Standard (AES) and in order to ensure a better security than TKIP it includes Counter-Mode/CBC-MAC Protocol (CCMP). WLANs that use a long enough password and that use WPA2 encryption are considered as secure WLANs [5].

To generate the necessary keys in WPA2 a four-way handshake is required. The necessary keys are Pairwise Temporal Key (PTK) and the Group Temporal Key (GTK). In this four-way handshake protocol both client and the AP need to have PMK. The client first requests to associate itself to the AP and the AP acknowledge this request. Then it sends a random value, called ANonce, to determine if the client has specific information or not. After being tested, the client uses the ANonce to generate a new SNonce and sends it back to the AP to test it. The generation of the PTK requires the client to generate its own SNonce and append it to the ANonce. It is also necessary to have the PMK and the MAC address of both client and AP [21].

One of the main issues of WPA2 is the need of having a new hardware to deploy it since it includes AES and CCMP. Even though the majority of the devices that were released after 2006 support WPA2, it was expensive to older networks to replace older devices. Another security issue is that WPA2 allows the system information, which is also known as management frames, to be sent as plaintext packets, and this makes it easy for an attacker to spoof the packets to alter them in a way that makes them appear like they are coming from the target client [21].

These last 2 standards WPA and WPA2 are both recognized by the IEEE 802.11i standard which is an extension of the original 802.11 standard [28].

3 Mobile Broadband

3.1 Introduction

Mobile broadband in a marketing term in order to give a name for wireless access to the Internet through a portable modem or other device. In order to access the Internet a cellular based system is used, portable modems connect to the base stations that give coverage to each area. This technology is capable of supporting data, voice, and video information transmission at high speeds. Mobile broadband is the name that the market gave to the mobile Internet Access.

3.2 Generations

3.2.1 GSM

For the deployment of the mobile systems worldwide different standards were used and, therefore, while in the United States of America were using some specific standards, in Europe other standards were being used and in Asia and in the Pacific other were more popular. This diversity of different standards generate difficulties for the users to use the devices in other countries, as they were not compatible with other networks. This did not contribute to the diffusion of mobile systems, this and many other problems were the reason for the creation of GSM [9].

GSM (the name comes from the committee *Groupe Speciale Mobile* from the CEPT established in 1982) or Global System for Mobile communications is the European attempt to unify the different digital mobile systems and to substitute the more than 10 different analogue standards that were being used until then, which were all of them very costly. GSM was planned like a multioperator system and the standard was design with the possibility that several operators could share the radiofrequency spectrum. In each country it exists at least three operators of GSM in its territory, competing with each other [9].

The GSM network is the most used standard used at the beginning of the XXI century and in other parts of the world. It is called a standard of second generations because unlike to the first generation of mobile phones, the communication is produced completely digital.

This standard was ready to be commercialized in 1991 worldwide and it arrived in 1992 to Germany with T-Mobil and in 1994 to Austria with Mobilkom. It was defined to work in the range of 900 MHz and from the technical point of view it achieved the following [9]:

- It was a European standard that it become almost a worldwide standard. Out of Europe the standard was applied in many other countries like in the United States of America, where it was implemented in its version of 1900 MHz known as PCS (Personal Communication Systems)

- Had a better efficiency, thanks to the requirement of having a carrier-to-interference (CIR) of only 9dB, instead of the 18 dB that were needed for the analogue systems. Like this the efficiency could be multiplied by three or four in the radiofrequency spectrum and minimize the number of base stations per subscriber.
- Was a digital systems so the costs of the Base Stations and the commutation centres were less sensible than the ones for the analogue systems
- Was a system based in TDMA (Time Division Multiple Access), this made possible to share a transceiver of a base station for more than one device, with a smaller operational cost.
- There were internal interfaces to the system that enabled to the operators to select the manufacturers that offered the best partial solutions, without having to rely on a unique supplier.

Due to the fast growth of the popularity of cellular systems, as well as socioeconomic reasons (encourage the competitiveness), with the issue of the lack of frequencies in the 900 MHz bandwidth, boosted an adaptation of the digital system of GSM in the frequency band of 1800 MHz (it is called DCS or GSM 1800), and of 1900 MHz in the USA. With the use of the band of 1800 MHz the problem of the lack of spectrum for the planning in urban areas and for big density population groups was resolved (Figure 7).

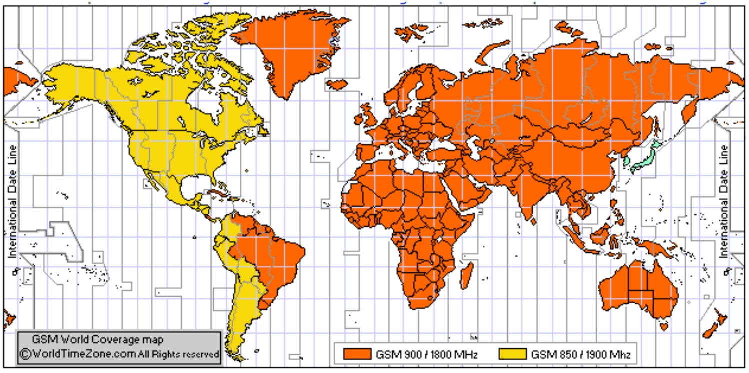


Figure 7: GSM World Coverage Map. [10]

3.2.1.1 Cellular system

GSM is based in the cellular system. The principal characteristics of a cellular systems are the following:

- Great capacity of users

- Efficiently use of the spectrum
- Wide coverage

Cellular systems are based in using a Base Station (BS) of small or medium power and give coverage to a more limited area than with other systems. The coverage area that the BS gives service is known as cell. In each cell it use a frequency subband, inside the whole frequency band that the operator has assigned. Like this in the cell only a part of the whole radio channels that the operator has available is being offered and to give coverage to a big territory a lot of cell are necessary. The issue can be if a cell cannot use the same radio channels that is using another cell and therefore nothing has improved because the number of radio channels are limited. If two cells use the same channels it may occur the known as co-channel interference, i.e. If a signal at a given frequency is interference by another signal at the same frequency or at the same channel, with a similar or bigger power the correct demodulation of the original signal is impossible to be carried out [9].

However in this system if the cells are far enough to each other they can use the same radio channel. This occurs because the interfering signal fades with the distance. If the power of the interfering signal is small enough, it could be considered as worthless noise and not give any issue to demodulate the original signal. The reutilization of the frequencies is therefore the base of the cellular system and of all the systems that have to do with the mobile networks such as GSM.

In GSM users in a single cell can transit simultaneously on:

- Different frequencies (FDMA, Frequency Division Multiple Access): a bandwidth is divided into channels of the same bandwidths and each user transmits their information at a specific frequency.
    - E.g. in GSM 900 there are 124 channels of a bandwidth of 200 kHz for uplink and 124 channels for downlink
    - Uplink and downlink separation is done via FDD (Frequency Division Duplex)
- Different timeslots on one frequency (TDMA, Time Division Multiple Access)
    - One carrier (frequency is divided into 8 timeslots, i.e. 8 users can use the same carrier concurrently, each timeslot a user can use the carrier to transmit information.

The size of these cell is different depending of several factors such as the density of population in a specific territory or number of channels available for that cell and obviously in the density of the traffic of information that is being exchanged, due to this we have bigger cells in the rural areas where they can reach dozens of kilometres and are known as macro cells while in urban centres where the number of users is higher the cells reach a size of 500 meters and are called microcells or picocells [9].

If in a cell there is more traffic that the one that is capable of process, due to a growth in the number of users it can be divided by adding a new BS and decrease the power of transmission of both BS in order to avoid co-channel interference. This is known as splitting

The shape of the cells in which is divided the territory depends on the antenna and the power that is being emitted from each base station. Usually two different types of antennas are used omnidirectional antennas and directive antennas. If the ones that are used are the omnidirectional antennas, the coverage area will have a circle form. However if we want to give coverage to a certain area using circles there will be overlapping between the coverage areas of the different stations [9]. This phenomenon leads to several issues from the spectrum point of view because in the overlapping area the traffic would use more frequencies than the ones it needs.

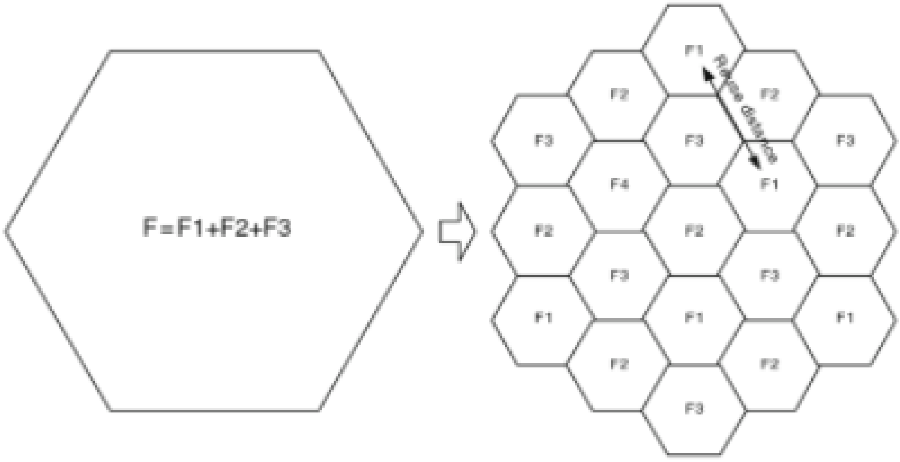


Figure 8: Cellular concept.

Due to this for the planning models, the coverages of the BS are taken as regular polygons that cover the area without overlapping. From these polygons the hexagon is the only one that has the property that for a radius of coverage R given (distance from the centre to the vertex), is the figure with the biggest surface and because of this it would be the one that lets cover the given area with the less number of BS. This phenomenon makes it the geometric form that is generally used to represent cells for the mobile cell system. Each of these hexagons are called sectors and have their own frequencies (Figure 8).

If instead of omnidirectional antennas directive antennas are used in environments where the coverage is difficult because they help to reduce the interference and obtain a bigger gain to favour the uplink, some example of these kind of environments are urban nature and the inside of buildings. In this case there are three antennas with the patterns of horizontal radiation that cover 120º each one, to cover 360º all of them [9].

Also another way to improve the data rates and to reduce the interference of neighbour cells is by using Adaptive Antenna Systmes (AAS). AAS is a type of multiantenna system based on the introduction of special processing systems thanks to the adaptively change of the radiation pattern of the antennas depending on the environment [11]. These kind of systems divide into two categories:

- **Switched-beam systems:** the antennas of this type of system use one beam at a time of all the prefixed beams. This beam changes as the mobile station moves through the coverage area of the antenna.
- **Adaptive array systems:** the antennas of this kind of systems employ an adaptive array technology known as SDMA. The main objective of this system is to track the mobile station and to locate it in order to avoid interferences with other stations offering like this the best possible service. However this technology implies a high complexity in term of architecture and signal processing techniques.

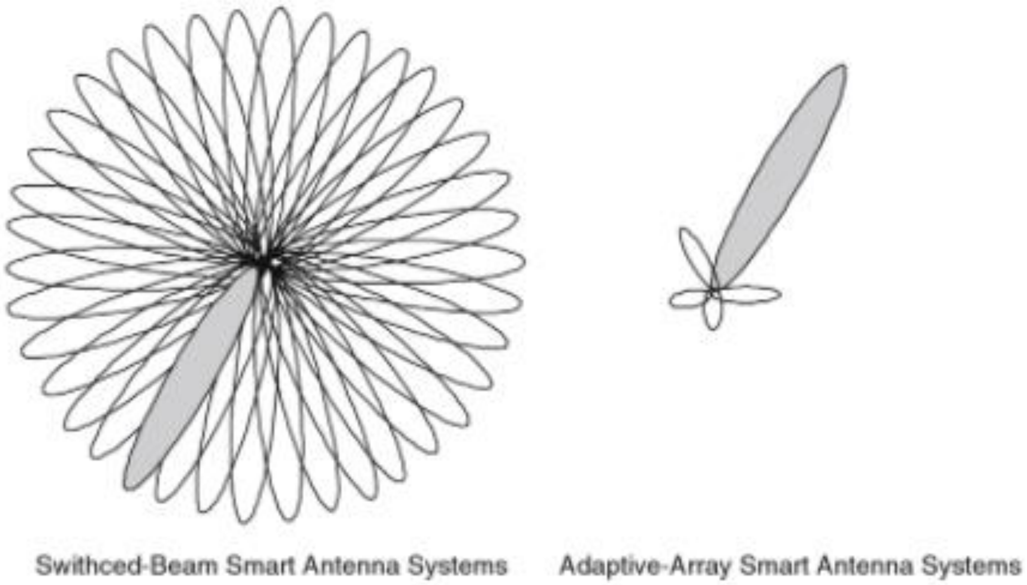

Swithced-Beam Smart Antenna Systems
Adaptive-Array Smart Antenna Systems

Figure 9: Adaptive antenna systems [11].

3.2.2 UMTS

The Universal Mobile Telecommunication System (UMTS) was created thanks to the great success not only in the European Union (by then European Economic Community) and it was created by a new standardization organization called 3GPP (Third Generation Partnership

Project), that was formed not only by the member of the EEC but also were members countries of other continents like it is shown in the Figure 10 [12]:

Figure 10: Members of the 3GPP [12].

UMTS is a system of third generation based in WCDMA or W-CDMA and it is one of the technologies selected by the ITU to form part of the IMT-2000. One of the principle characteristics of every radio system is the frequency band in which the devices and technology is going to work. In the case of UMTS, we can see in the Figure 11 the frequencies that are reserved for the systems IMT-2000 in each part of the world. In the WARC 92 (World Radiocommunications Conference) was defined a range of 230 MHz of the radio spectrum in the bands of 1.885-2.025 MHz and 2.110-2.200 MHz previously identified for the public terrestrial telecommunications systems, including the components based in satellites (MSS) [9] [14].

As a result of that decision, in Europe, Japan and other countries, those frequency ranges were assigned to the mobile services of third generation. However this did not happen in the USA that have a different criteria because the band around 2 GHz was assigned for PCS.

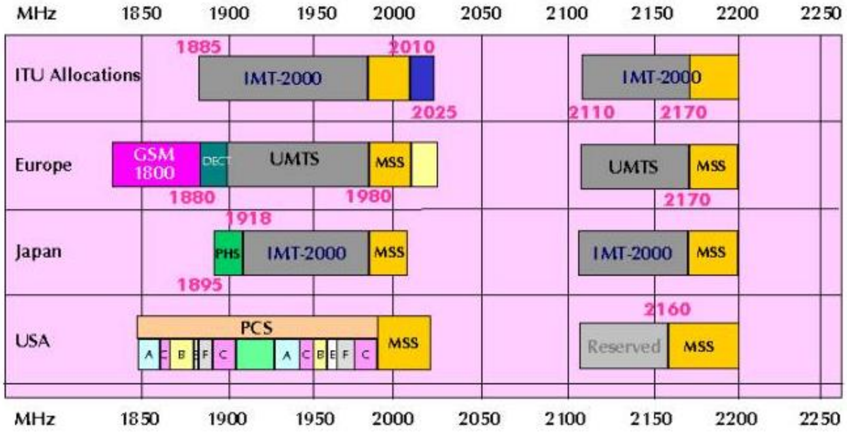


Figure 11: Worldwide frequency plans for IMT-2000 bands [13].

If we talk about the radio technology that was decided to be used, several options were taken into account: wideband CDMA (WCDMA), OFDMA, TDMA (WB-TDMA), TDMA with spreading (WB TDMA/CDMA) and ODMA (Opportunity-Driven Multiple Access). It was on the 29 of January of 1998 during the meeting ETSI SMG 24 bis, in Paris, when it was agreed to use two different technologies: W-CDMA and TD-CDMA. This enabled UMTS to work in two frequency modes, pared and unpaired, with FDD (Frequency Division Duplex) and TDD (Time Division Duplex) technologies [9] [15].

We can define the following components of a UMTS system:

- **The terminals or the user equipment (UE):** it is formed by the mobile phone and its identity module of the user/subscriber (USIM) that is the equivalent to the SIM card for the mobile phone. In the case of UMTS the security is improved in relationship to the GSM.
- **UMTS Terrestrial Radio Access Network (UTRAN):** provides the air-interface access method for the UE [15].
- **The core network (CN):** adds functionalities of transport and of intelligence. The first ones support the transportation of the traffic of information and of signalling, including commutation. Routing is located in the intelligence functionalities. Through the CN, UMTS connects to other telecommunications networks, in a way it is possible a communication not only between users of UMTS but also with the ones that are connected to other kind of networks (like fixed networks). The CN formed by:

  - **Circuit switching (CS):** used basically for the voice service.
  - **Packet switching (PS):** used for the data services.
  - **Core multimedia (IMS, IP Multimedia Subsystem):** defined later than the two mentioned above. It was connected to the PS to provide all the new multimedia services (like the RCS, Rich Communication Services) [9] [15].

In terms of security the UMTS defines the following characteristics for security:

- **Security in the network domain:** is a set of security characteristics that lets all the domain nodes of a provider to exchange signalling data in a secure way and protects against the attacks to the fixed network.

- **Security in the user domain:** is the set of characteristics that the security make safer the access to the BS.

- **Security in the application domain:** set of security characteristics that let the applications for the user domain and to the provider domain to exchange the messages in a safe way

- **Visibility and configuration of the security:** is the set of the characteristics that let the user inform if the security characteristics are working or not and if the use of the different services rely on the security characteristics.

The authentication parameters and the encryption in UMTS has the same bases as the ones used in GSM or GPRS. For the mutual authentication of the user and of the network to parameters were introduced to the three that already existed in GSM and GPRS. This additions were introduced in order to have the maximum compatibility with the GSM network that already existed. A sequence SQN is created by the authentication centre, as well as the unique user key (ki) and the random access number (RAND), which is used to check if the authentication process was done before or not [9] [15].

3.2.3 LTE

LTE (Long Term Evolution) is a technology defined by the 3GPP and it was developed to support packet-data transmission and not circuit-switched voice. Release 8 was the first version of LTE and it was deploy to the market at the end of 2009. The most important achievement of LTE was to be the first worldwide accepted single technology in the mobile broadband sector. This was a great achievement as it would mean that having only one technology would make the development of the upgrades faster and to reduce the cost for the clients [16].

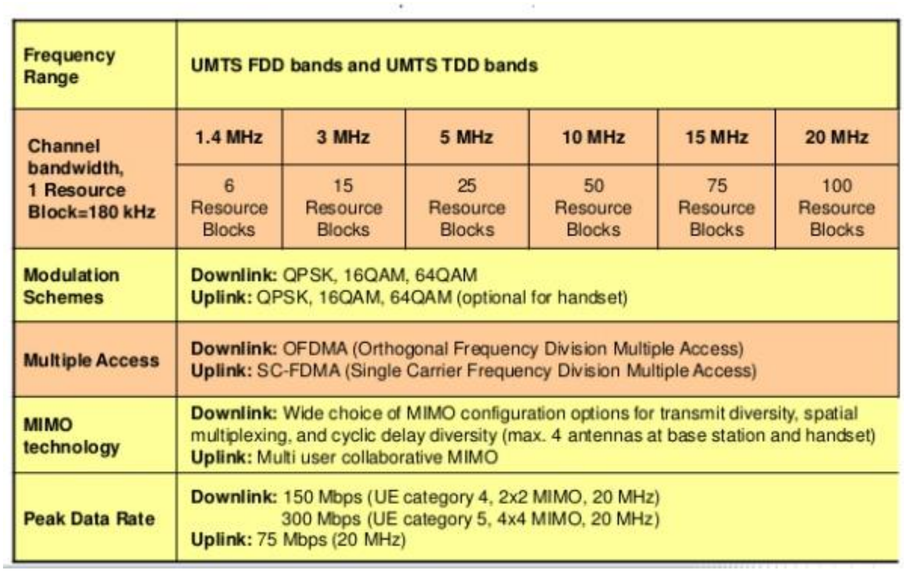
In LTE all architecture is based in IP (Internet Protocol), this generates challenges for real time services, such as voice, that until know was based in a fix circuit service. So to ensure a good quality of these systems some mechanisms were needed to be implemented. LTE enables also the use of bigger bandwidths, the generations before LTE, e.g. UMTS used a bandwidth of 5 MHz per signal, in LTE this bandwidth is widened to 20 MHz and the radio technology that uses which is based in OFDM makes the system more robust to the interferences [9].

For LTE it was selected an access method called OFDM (Orthogonal Frequency Division Multiplexing Access) for the uplink and SC-FDMA (Single Carrier – Frequency Division Multiplexing Access) for the downlink. For the modulation in case of the downlink it was defined that the types of modulation that can be used are BPSK, QPSK, 16 QAM and 64 QAM, while for the uplink the available ones are QPSK, 8 PSK and 16 QAM. However the broadcast channels can only use QPSK [9] [16].

The main characteristics of LTE of Rel-8 are the following (Table 7) [9]:

- **High Spectral efficiency:** as we have explained before OFDMA is used in the downlink. This technique of multiple access which is strong against multiple interferences and has high affinity to the modern techniques like the channel programming in the frequency domain and MIMO. SC-OFDMA is used for uplink and MIMO is used to support channels of multiple transmission in the antennas.

- **Very low latency:** shortening of the preparation and transmission time, short latency HO (handover) and interruption time. Reduction of the TTI (Transmission Time Interval). Simplification of the RRC status (Idle, connected).
- **Supports variable bandwidths:** 1.25-3-5-10-15 and 20 MHz.
- **Simple protocol architecture:** channels are shared and the information is sent via packages with VoIP (Video on IP) capacity.
- **Compatibility and interoperability with the older versions of 3GPP.**
- **Introduction of autoconfiguration and optimization functionalities.**



Frequency Range	**UMTS FDD bands and UMTS TDD bands**					
Channel bandwidth, 1 Resource Block=180 kHz	**1.4 MHz**	**3 MHz**	**5 MHz**	**10 MHz**	**15 MHz**	**20 MHz**
	6 Resource Blocks	15 Resource Blocks	25 Resource Blocks	50 Resource Blocks	75 Resource Blocks	100 Resource Blocks
Modulation Schemes	**Downlink:** QPSK, 16QAM, 64QAM **Uplink:** QPSK, 16QAM, 64QAM (optional for handset)					
Multiple Access	**Downlink:** OFDMA (Orthogonal Frequency Division Multiple Access) **Uplink:** SC-FDMA (Single Carrier Frequency Division Multiple Access)					
MIMO technology	**Downlink:** Wide choice of MIMO configuration options for transmit diversity, spatial multiplexing, and cyclic delay diversity (max. 4 antennas at base station and handset) **Uplink:** Multi user collaborative MIMO					
Peak Data Rate	**Downlink:** 150 Mbps (UE category 4, 2x2 MIMO, 20 MHz) 300 Mbps (UE category 5, 4x4 MIMO, 20 MHz) **Uplink:** 75 Mbps (20 MHz)					

Table 7: LTE Release 8 characteristics [17].

4 Development concept and application components

4.1 Initial situation

The initial situation that we find that we want to create or use an application that is gives the necessary information in order study and see how it is applied all the standards and the security of the theoretical part that has been explained before. Also with this application we should be able to draw some conclusions about the surrounding WLANs and it should be possible to give some recommendations in order to have a better and a more secure services in the cases were the QoS is poor.

The first step that was taken was to decide for what Operating System (OS) we would like to create the application. In these case as the application is going to be a mobile application we have two main OS for smartphones: Android and IOS. Each of these OS have disadvantages and advantages:

- **Android:**
  - *Advantages:* Android is the most used OS for mobile devices therefore the scope will be bigger than creating an application for IOS. Also a very important advantage is that the application development software for Android is completely free (Android Studio), therefore making an application is more accessible for Android than in IOS because for the application development software in IOS (Xcode) is also free but when deploy applications onto the IOS devices or distribute them in the App Store there is a fee of 99 $ a year that has to be paid. This factor is a real issue for this particular case as would be impossible to do the implementation in a real devices and the use of a simulator would be compulsory in order to test the application and to give the conclusions and the advices for the different scenarios.

  - *Disadvantages:* the main disadvantage of application development in Android is that you usually get 0 revenue of the work that you have done. There are studies that have found out that the Android users are less willing to pay for the applications than the IOS users. Also another important disadvantage is that competence because in Google Play there are more applications than in the Apple Store. By the end of 2016 there number of application in Google Play was higher than 2.4 million applications. So there are many applications that are practically the same or that at least give the same service making some applications practically forgotten and are usually little downloaded.

For this particular case as we do not want to neither commercialized the application these disadvantages are irrelevant, however the advantage that Android has in comparison to IOS when we are talking about testing an application in a real device is really important as one of the main parts of this BA-thesis is the study of real situations. Therefore the OS that was finally selected for the application was Android and the software development system used was Android Studio.

4.1.1 Integrated development environment (IDE)

Android Studio is the official integrated development environment (IDE) for Android operating system. It is available for download on Windows, Linux and macOS and it was created to replace Eclipse Android Development Tools as the main IDE for application development for Android. The principal programming language is Kotlin which replace Java as the preferred language for Android app development, however Java and C++ can still be used to develop application in Android Studio. One of the most power full features about Android Studio is its powerful integrated code editor and its construction system based on Gradle. Gradle enables to the developer to apply different configurations to the same code, creating in this way different versions of the same source code. This is especially useful if the developer wants to create to versions of the same application, i.e. a free version and a paid version. It is also very useful for the reuse of the code in other projects since the gradles can be exported to other projects and used on them. On top of that Android Studio has an editor tool which lets the user to previsualize the real layout of the application itself making the development and programming of the application simpler and more intuitive [38].

Android Studio is based on Kotlin that is a programming language created specifically for application development. It bring new features such as safety measures in terms of nullability and immutability. As Java Kotlin is statically typed however it is much stricter and therefore safe. It has to be told to the complier whether a variable can store a null value. It is also easy to debug as bugs can be detected easier and faster when the application is being developed, instead of having users reporting them and making the user's experience worse. One of its most important advantages is that it exists interoperability between Java and Kotlin as Kotlin was design to work side by side with Java. The existing Java libraries and frameworks work with Kotlin without any issues giving like this the possibility to the developer to capitalise on the advantages of both programming languages in order to make the code easier to optimize and modify [39].

Once the IDE was selected and it was all ready to start developing the application it was necessary to decide if an already made application was going to be used or if an application from scratch was going to be develop. Developing an application from scratch has advantages and disadvantages, for example some of the advantages are that it can be made as the developer wishes and implement the features that the developer wants however it is a very tedious work and nowadays every application developer uses a template in order to reduce the payload of programming an application. Therefore for this particular case it was decided to use an already made application that is called WiFiAnalyser. This is an open source application this means that it can be used freely and it can be changed and modify. For the main purpose of this thesis this application suited perfectly as it already implemented all the features that are necessary for wireless network analysis and changes could be made in order to display more information.

4.2 Requirements

4.2.1 Functional requirements

Functional requirements are often defined as what a system is supposed to do. As it was decided that the application was going to be created for Android it is obvious that in order to use this application a device with an Android OS is needed, if this is not possible a simulator of an Android device can also be used in order to use the application. Other functional requirements that are needed is that the application has to be able to access to the Wi-Fi information and the Location of the device in order to give the service. The application asks the user if he agrees to share this information with the application and the application lets the user know that this information is only going to be used with the purpose of getting the information of the wireless networks the user is surrounded by and not for commercial purposes.

4.2.2 Non-functional requirements

The non-functional requirements defined how a system is supposed to be. Therefore the application is required to be able to store and process at least the information of an access point at a time at least in order to display this information in the graphs. Also the information has to be display in a way so that it is clear for the user in order to make decisions and conclusion. So only the relevant information should be visible in the main screen for the user and if the user wants to know more information about a particular AP there must be an option that shows more detailed information about the particular AP that the user desires.

4.3 Restrictions

This application on the other side has some restrictions. As it has been explained before it is only able to analyse the signals of networks from the Wi-Fi frequency bands. Therefore if in the environment there are more wireless networks that use different frequencies for the transmission of the information it would be necessary to use another type of application or more professional measure equipment.

4.4 Application components

The android application has a large number of functionalities. The first display that is shown when the application is launched can be seen in the Figure 25 (Annex A). In this display there is a brief explanation of the Wi-Fi scanning for the different Android version as well as the Github repository from where it was obtained all the code of the application and where the changes were done.

Once the application is running the access points that the device is capable of detect are displayed. This display is shown in Figure 26 (Annex A). As it can be seen the access points are displayed in a list format and scrolling down the remaining access points can be seen. On the top part of the screen we can see two options [43]:

- **Filter option:** is a typical filter option that lets the user to filter the access point depending on the SSID, the Wi-Fi band, the signal strength and the type of security it is using. This option can be really useful in environments where there are a lot of different WLANs for example a city centre where public Wi-Fi can be found as well as the possible mobile broadband connections of the users that might have enable the sharing Wi-Fi option and making their phone to behave as an access point. The filtering is done by checking the SSID and to do it is not necessary to type the exactly characters of the SSID, by typing only characters that are contained in the SSID it is enough to do the filtering by SSID. The filtering can also be done depending on the security protocol of the wireless network, strength of the signal and the frequency band where the AP is transmitting the information. The filtering option is implemented in “Filter.kt” where all the code for the different kind of filters can be found.
- **Pause option:** when this option is turn on the application basically stops the scanner for the period of time it is on, this can be seen in “MainActivity.kt” where it can be found a Kotlin function called onPause() that pauses the scanner operation, stopping like this the obtainment of information. This option can be especially useful in order to take screenshots in places where there information of the WLANs is changing very fast. However the user has to keep in mind that the changes that happen to the network within the time that the pause option is turned on will not be stored and therefore will be impossible to analyse them. The pause option also has a resume option to continue the scanning of the network information this function is called onResume() and it is also in “MainActivity.kt”.

On the bottom of the screen we can see a different kind of features [43]:

- **Channel Rating:** this feature gives to the user a rating to the different channels Wi-Fi band that is being analysed in this case 2.5 GHz or 5 GHz. This rating as can be seen in the Figure 27 (Appendix A) is given in a visual way using stars. The rating system uses the strength of each signal that is being emitted in each channel and also the number of AP that are emitting in each channel. Like this does an estimation of the co-channel interference and depending on the possible existing interference the rating of each channel will be better or worse.

- **Channel Graph:** gives information about the power of the signal that is transmitted in each channel and the SSID of the access point that is using those channels. The intensity of the signal is given in dBm and it is a very visual way to see which access point is better and what channels are being used by which access points, how this power is calculated will be explained in chapter 5. An example of this can be seen in Figure 28 (Appendix A).
- **Time Graph:** this functionality gives information of the intensity of the signal received by each access point this information is refreshed every few seconds. Making this functionality very useful to see how the signals of each access points change through time. This can be used while moving and like this it can be seen to which access points the user is walking to or how obstacles affect the exchange of information. It is shown how it works in Figure 29 (Appendix A).

5 Implementation of functionalities and practical scenarios.

5.1 Mobile application

The components of the application that have been explained in the chapter 5.4 have different functions and have been implemented in different ways:

5.1.1.1 Obtainment of the information

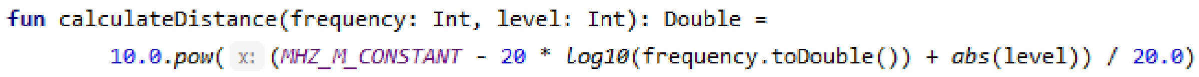
To obtain the information it has been used the android.net.wifi package that is already implemented in the packages for application development in Android Studio. From this package three principle classes were used:

- **WifiInfo**: gives information about the state of the Wi-Fi connection that are active and or that are being set up. In order to obtain this information it need a series of permission as the *WifiManager#getScanResults* function from the *WifiManager* class.
  If this access is not allowed, *getSSID()* will return *WifiManager#UNKNOWN_SSID* which as is obvious means that the Wi-Fi information could not be accessed. Also *getBSSID()* will return 02:00:00:00:00:00. This makes sense as if the access is not allowed it should not be able to retrieve the information of the Wi-Fi and therefore the information cannot be displayed.
- **WifiManager**: this class provides the primary Application Programming Interfaces (API). Thanks to this class several categories of items can be seen:
  - List of configured networks: can be updated and with several functions the attributes can be modified.
  - The current active Wi-Fi network to which the device is connected. With the functions that are implemented inside the class the developer can change the status of the connected WLAN by establishing the connection or turn it down and information about the state of the network and the AP can be retrieved.
  - Result of access point scans, contains important information about the available APs that the device is able to detect.
  - It defines the names of various Intent actions that are issued when the state of the network changes
- **ScanResult**: describes information about a detected access point. It also keeps track of the quality, noise and maxbitrate attributes, but does not report them to external clients in a current way.

How the information is queried can be seen in the class “WiFiManagerWrapper.kt” that have several methods that extract the network information.

It can be checked if the Wi-Fi is enabled or disabled to do so uses the function “wifiEnabled()”. This method returns a Boolean value depending if the Wi-Fi of the device is enabled (true) or not (false). There is also a method that disables the Wi-Fi of the device and also another one that enables it. In order to disable the Wi-Fi the method checks that it was enabled before the operation is carried out and the same happens to the enable method.

In this class is also used the mentioned “ScanResults()” that is previously used in the Scanner where the information is queried. With all the information obtained the application does an estimation of the distance to the access points. This estimation is done using the Free-Space path loss (FSPL) therefore this approximation will only be useful for the cases in which the conditions of FSPL are fulfilled. These conditions include not having any obstacle in the middle of the path between receiver and transceiver, therefore this approximation is useful only in very few cases because in real scenarios there will usually be at least an obstacle in the middle of the path that follows the electromagnetic waves that go from the transceiver to the receiver. For this particular the calculation is done in the “Strength.kt” class that uses one of the functions of “WiFiUtils.kt” in this particular case the function “calculateDistance()” that can be seen in Figure 12.



```
fun calculateDistance(frequency: Int, level: Int): Double =
        10.0.pow( x: (MHZ_M_CONSTANT - 20 * log10(frequency.toDouble()) + abs(level)) / 20.0)
```

Figure 12: Function used to calculate the distance

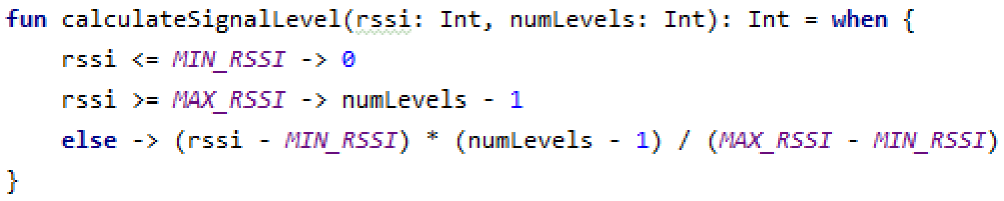
As it can it be seen in Figure 12 the “calculateDistance()” function is used to obtain the distance between the AP and the user’s device. As it has been explained above the estimation is done by using the FSPL. The formula for the FSPL is the following:

Formula for FSPL [42]:

$$\mathrm{FSPL(dB)} = 20\log_{10}(d) + 20\log_{10}(f) + 92.45 \qquad (1)$$

In this case it can the units for both the frequency (f) and the distance between the transceiver and the receiver (d) are GHz and km respectively. For our use case the constant value has to be -27.55 as in this case the application is going to analyse WLAN and the coverage area is not in the order of kilometres. Therefore in order to calculate the distance it was implemented the function shown in Figure 12. This function includes the Kotlin function “pow()” that raises a value in this case 10 to the power of x. As it has been explained before MHZ_M_CONSTANT is the constant value if the units used are MHz and M respectively and its value is -27.55. Then the estimation of the distance is shown at the APs screen (Annex A, Figure 26) [42].

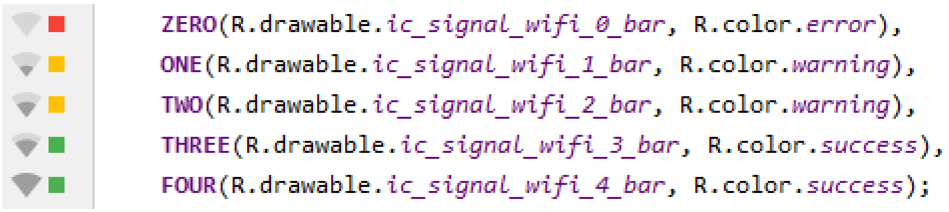
Another features that have been implemented in the application is the calculation of the signal power that it is received. In this case there is a function also in “WifiUtils.kt” called "calculateSignalLevel()". The code of this function can be seen in Figure 13 and it uses Received Signal Strength Indicator (RSSI) in order to put the signal receive into one level or another one. If the signal level is above the maximum value of RSSI that for the application has been selected -40 the application will show next to the AP a WiFi symbol coloured in green, as it can be seen in Annex A in Figure 26. The value of -55 was selected as it is considered to be between -40 and -60 the optimal range for a stable connexion. On the other side if the signal level is under -80 the application will show a WiFi symbol coloured red. The value of -80 for the minimum RSSI was selected because -80 is the minimum value of a signal to stablish an acceptable connexion. For the rest of the signal values that are inside the range, the application separates them into different levels thanks to a formula that it can be seen in the last line of the function code in Figure 13.



```
fun calculateSignalLevel(rssi: Int, numLevels: Int): Int = when {
    rssi <= MIN_RSSI -> 0
    rssi >= MAX_RSSI -> numLevels - 1
    else -> (rssi - MIN_RSSI) * (numLevels - 1) / (MAX_RSSI - MIN_RSSI)
}
```

Figure 13: Function used to divide the signal power into different levels

The function returns an integer that goes from 0 to the number of different levels that have been created minus 1. The application was develop with 5 different levels (Figure 14) therefore the range goes from 0 to 4. So depending on the value that it is obtained from "calculateSignalLevel()", that it is going to be always inside the range of 0 to 4, different symbols will be shown.



```
ZERO(R.drawable.ic_signal_wifi_0_bar, R.color.error),
ONE(R.drawable.ic_signal_wifi_1_bar, R.color.warning),
TWO(R.drawable.ic_signal_wifi_2_bar, R.color.warning),
THREE(R.drawable.ic_signal_wifi_3_bar, R.color.success),
FOUR(R.drawable.ic_signal_wifi_4_bar, R.color.success);
```

Figure 14: Levels to differentiate the signal power

The application also obtains information related to the APs, as it has been explained in chapter 2.4 each AP has its own BSSID and each wireless network has its own SSID. Therefore the application is capable of obtaining both the BSSID and the SSID. To do so, as it has been explained before the public class "WifiInfo" is used with the functions "getBSSID()" and "getSSID()". Both, the SSID and the BSSID are shown at the APs screen (Figure 26) and the SSID is always shown in every graph in order to differentiate each network. The application also gives information about the vendor of the APs, this feature might be interesting in order to do a comparison of different APs from different vendors.

5.1.1.2 Storage of the information

For the storage of the information a cache Kotlin class is used that was already implemented in the application. This cache stores the information that is scanned by using a List, the information of the list is stored for a period of time that depends on the Scanner. The period of time can be changed, the application gives the possibility to change it to 2, 5 or 10 seconds. Having a memory makes it is really useful to see the data for a period of time and to see how it changes depending on the situation the user is in. The scan speed can be changed in the setting screen that is available at the navigation panel.

5.1.1.3 Display of the information and graphics

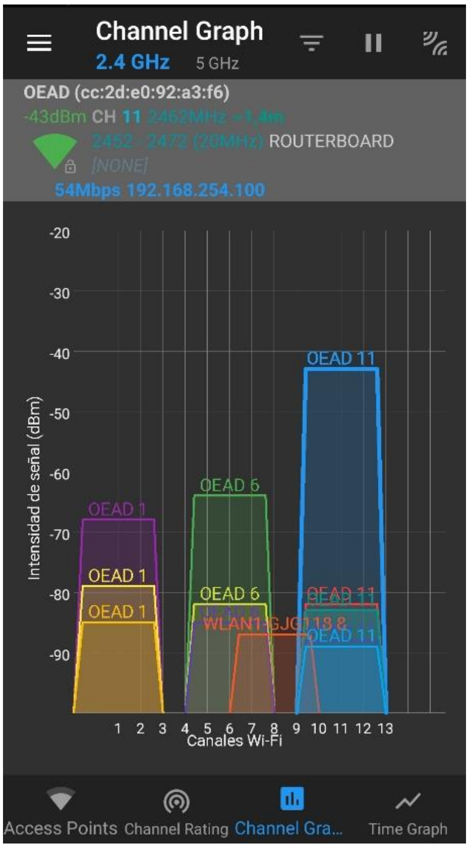
In this application the display of information is in a visual way in order to make it to the user easy to understand at least the basic concepts of the APs. In order to display the datea in the two graphs the application uses the cache memory in order to get access to the information that has been retreived. In the case of the channel graph apart from the power of the signal it are also relevant the channels where the APs are emiting the signal. Therefore in this graph for each AP the signal power, guard band, frequency where the bandwidth starts and ends it is stored. On the other side the time graph only show the power of each AP's signal through time therefore the values of guard band and frequency are not relevant in this case. In both cases the intensity of the signal is measured in dBm which is a unit of level used to indicate that the power level is expressed in decibels (dB) with reference to one milliwatt. This is a very common unit in the radio and telecommunications field [41].

5.2 Practical scenarios

5.2.1.1 Scenario 1 (WLAN with several AP)

The first scenario that we will study will be a WLAN that has several AP. This a type of network very common in for example a big office with several floors or in a student dorm. Usually these networks have a lot of APs in order to give service to all the users that work or live in the building. This is a very interesting case as we can see that different AP will use the same channels for transmission and it will not affect the service because they are usually located in different floors or rooms that are far away from each other and the signal of the other AP transmitting in the same channels will be considered as an unnoticeable interference (Figure 15). As it can be seen in Figure 16 in this case the OEAD network is an ESS as it is formed by several BSS each one with one AP. It can be seen that each AP of the OEAD network share the SSID of OEAD however they have different BSSID which it is obtained using the MAC address of each AP.

As we can see here there are a lot of AP and they depending on the AP they share the channels with other AP. This a really important factor that has to be beard in mind when the configuration of the network is done because if not it can happen that the signal of different AP will interference each other (co-channel interference). Also in Figure 15 we can see that the better channels in this particular case are channels from 9 to 13 that is where the AP OEAD 11 is transmitting its signal.



Channel Graph

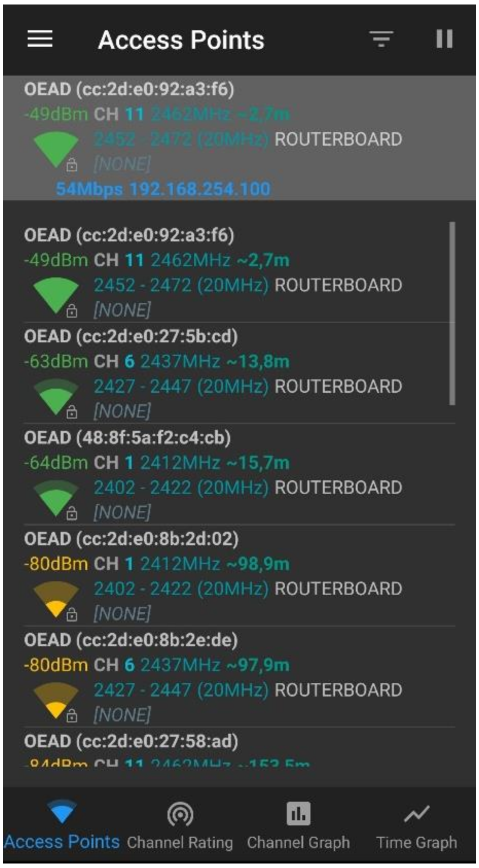
OEAD (cc:2d:e0:92:a3:f6)
-43dBm CH 11 2462MHz ~1,4m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]
54Mbps 192.168.254.100

Figure 15: Example of AP sharing channels.

In Figure 16 the access point detected can be seen. It can be seen that as it is common the access point that gives a better service is the one which is located closer to the user. We can see that also the APs do not have any kind of security and therefore it can be said that this network has security issues. In this kind of networks where there is not a security method it is really recommended to use an external security procedure and to not turn off the antivirus of the devices connected to the network.

A great way to improve the security in these cases is to use a VPN (Virtual Private Network), VPNs enable a secure extension of WLAN. It lets the devices to receive and transmit data over public or shared WLANs as it was a private WLAN, with all the functionalities, security and management policies of a private network.

A possible solution of this would be to use a web browser that implements a VPN for example Opera. Opera is a free web browser that has implemented its own VPN that will ensure extra security in this cases where the network has no configuration in terms of security. Usually this kind of networks do not have any kind of security because it is more comfortable to have an open WLAN without access key and like this there is not needed to configure the connection to each AP making the service less secure but more comfortable to the users. However if external security measures are not taken some task should be performed extremely careful as this networks are vulnerable against attacks and in this networks it is specially easy to extract information form the users when they are doing important tasks (bank transactions, messaging, emails, passwords, storage of private data…).



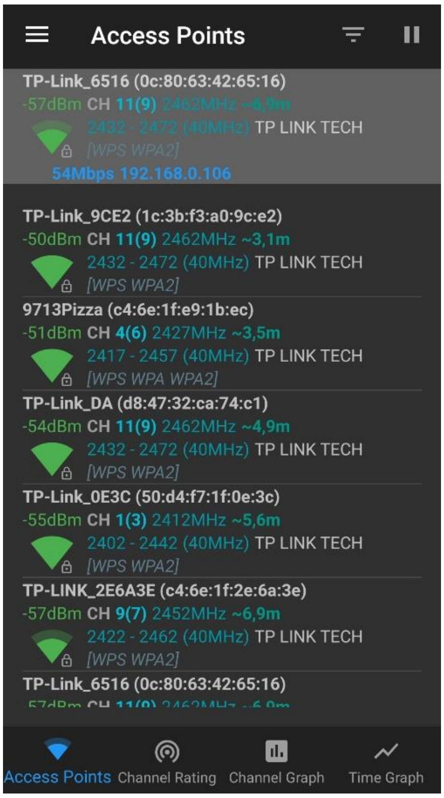
```
OEAD (cc:2d:e0:92:a3:f6)
-49dBm CH 11 2462MHz ~2,7m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]
54Mbps 192.168.254.100

OEAD (cc:2d:e0:92:a3:f6)
-49dBm CH 11 2462MHz ~2,7m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]
OEAD (cc:2d:e0:27:5b:cd)
-63dBm CH 6 2437MHz ~13,8m
2427 - 2447 (20MHz) ROUTERBOARD
[NONE]
OEAD (48:8f:5a:f2:c4:cb)
-64dBm CH 1 2412MHz ~15,7m
2402 - 2422 (20MHz) ROUTERBOARD
[NONE]
OEAD (cc:2d:e0:8b:2d:02)
-80dBm CH 1 2412MHz ~98,9m
2402 - 2422 (20MHz) ROUTERBOARD
[NONE]
OEAD (cc:2d:e0:8b:2e:de)
-80dBm CH 6 2437MHz ~97,9m
2427 - 2447 (20MHz) ROUTERBOARD
[NONE]
OEAD (cc:2d:e0:27:58:ad)
-84dBm CH 11 2462MHz ~153,5m
```

Figure 16: APs discovered by the application in the scenario 1.

5.2.1.2 Scenario 2 (Environment with several WLANs)

The second scenario of study will be an environment with several WLANs. This kind of environment would be really similar to the one that can be found in a block of flats where each house owner has its own AP and its own WLAN for personal use and from different ISP. In the Figures 22 and 23 we can that is this particular scenario the AP to which the user is connected is not the AP that transmits the signal at the highest power. However the user cannot connect to that AP because it is not his AP and therefore he does not have the password in order to connect to that WLAN and have a better QoS.

If the channel graph is studied we can see represented in Figure 19 that in this particular case the situation regarding co-channel interfering is worse than in scenario 1. As it can be seen easily the user is connected to an AP that use channels from 5 to 13 and there are a lot of AP that transfer information and the signal intensity is similar or even higher, e.g. TP-Link_9CE2 11(9). On the other side in this case WPA2 is the security protocol used therefore there should not be the security issues that were in the first scenario where there WLAN did not have a security protocol. Therefore in this scenario it can be said that there should be a reconfiguration of the location of the AP or in which channels it is working or even the power level at which it is emitting its signal.



Access Points

TP-Link_6516 (0c:80:63:42:65:16)
-57dBm CH 11(9) 2462MHz ~6,9m
2432 - 2472 (40MHz) TP LINK TECH
[WPS WPA2]
54Mbps 192.168.0.106

TP-Link_9CE2 (1c:3b:f3:a0:9c:e2)
-50dBm CH 11(9) 2462MHz ~3,1m
2432 - 2472 (40MHz) TP LINK TECH
[WPS WPA2]

9713Pizza (c4:6e:1f:e9:1b:ec)
-51dBm CH 4(6) 2427MHz ~3,5m
2417 - 2457 (40MHz) TP LINK TECH
[WPS WPA WPA2]

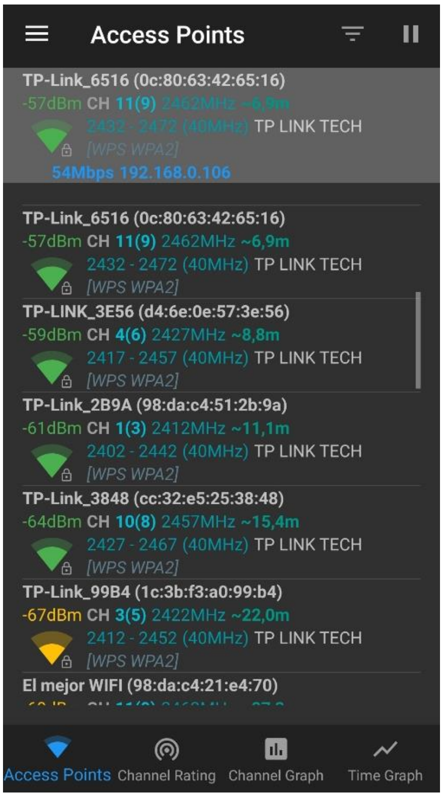
TP-Link_DA (d8:47:32:ca:74:c1)
-54dBm CH 11(9) 2462MHz ~4,9m
2432 - 2472 (40MHz) TP LINK TECH
[WPS WPA2]

TP-Link_0E3C (50:d4:f7:1f:0e:3c)
-55dBm CH 1(3) 2412MHz ~5,6m
2402 - 2442 (40MHz) TP LINK TECH
[WPS WPA2]

TP-LINK_2E6A3E (c4:6e:1f:2e:6a:3e)
-57dBm CH 9(7) 2452MHz ~6,9m
2422 - 2462 (40MHz) TP LINK TECH
[WPS WPA2]

TP-Link_6516 (0c:80:63:42:65:16)

Figure 17: APs discovered in the scenario 2 (1).



Access Points

TP-Link_6516 (0c:80:63:42:65:16)
-57dBm CH 11(9) 2462MHz ~6,9m
2432 - 2472 (40MHz) TP LINK TECH
[WPS WPA2]
54Mbps 192.168.0.106

TP-Link_6516 (0c:80:63:42:65:16)
-57dBm CH 11(9) 2462MHz ~6,9m
2432 - 2472 (40MHz) TP LINK TECH
[WPS WPA2]

TP-LINK_3E56 (d4:6e:0e:57:3e:56)
-59dBm CH 4(6) 2427MHz ~8,8m
2417 - 2457 (40MHz) TP LINK TECH
[WPS WPA2]

TP-Link_2B9A (98:da:c4:51:2b:9a)
-61dBm CH 1(3) 2412MHz ~11,1m
2402 - 2442 (40MHz) TP LINK TECH
[WPS WPA2]

TP-Link_3848 (cc:32:e5:25:38:48)
-64dBm CH 10(8) 2457MHz ~15,4m
2427 - 2467 (40MHz) TP LINK TECH
[WPS WPA2]

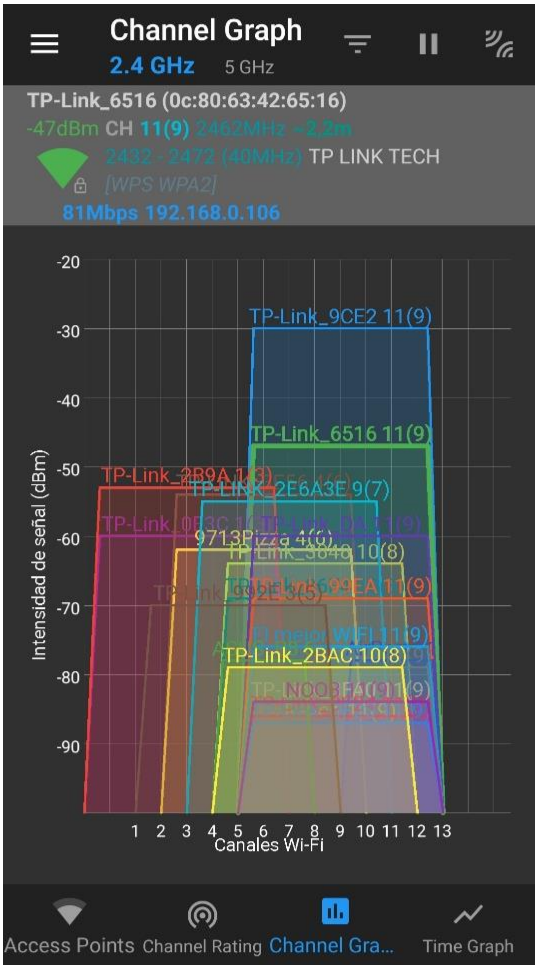
TP-Link_99B4 (1c:3b:f3:a0:99:b4)
-67dBm CH 3(5) 2422MHz ~22,0m
2412 - 2452 (40MHz) TP LINK TECH
[WPS WPA2]

El mejor WIFI (98:da:c4:21:e4:70)

Figure 18: APs discovered in the scenario 2 (2).

The first solution that can be taken into account would be changing the position of the AP. This solution is the easiest from a technical point of view because it does not require software nor really complex configuration. However this option may encounter issues, for example, impossibility of changing the position of the access point or the necessity of cables in order to change the AP's position. This last issue in some cases may be really important from a decoration point of view as some users may not want to have really long cables going through their home.

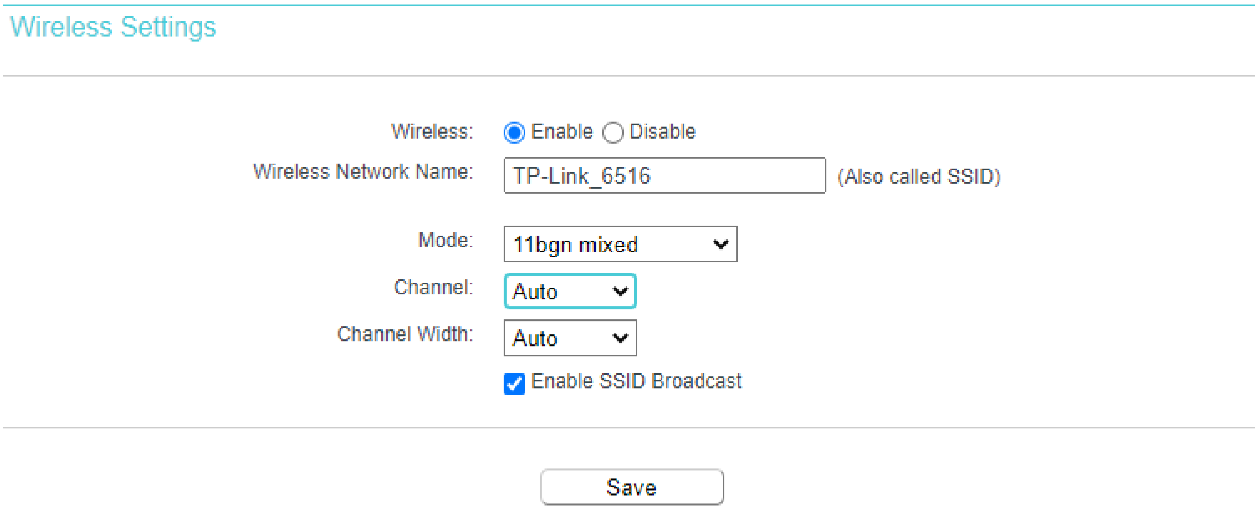
The second solution would be changing the frequency range of the signal that the AP is emitting. In this case the position of the AP would not have to be changed and therefore the issues of the last solution would disappear. However this solution is more difficult from a technical point of view as some research or previous knowledge of AP configuration is needed in order to not provoke any more issues that might appear due to a bad configuration. Also something that has to be beard in mind is if the current AP can emit at the desired frequency ranges as some AP can only emit at a really specific frequency ranges, meaning that a new AP would be needed in order to solve this problem. In this case the frequency ranges where the router is able to work is from 2.4-2.4835 GHz, i.e. the 2.4 GHz frequency band therefore the router can be configured. The ISP has a service that gives the option to the user to configure the AP. In this case this feature is really interesting as it gives the user the possibility to change the channels that the AP is using and therefore make the QoS better (Figure 20). In this case there should be avoided the channels were there are working a high number of AP in order to avoid the interferences.



TP-Link_6516 (0c:80:63:42:65:16)
-47dBm CH 11(9) 2462MHz ~2,2m
2432 - 2472 (40MHz) TP LINK TECH
[WPS WPA2]
81Mbps 192.168.0.106

Figure 19: Wireless Settings of the router to which the user is connected.

The third solution of making higher the signal level of the AP in this case is presents more inconveniences than the other two possible solutions as it would mean to change the antenna of the router and that would mean in more investment and in a more professional advice. This solution could also be change by changing the AP or the router but this would also mean in some extra investment.



Wireless Settings

Wireless: ● Enable ○ Disable

Wireless Network Name: TP-Link_6516 (Also called SSID)

Mode: 11bgn mixed

Channel: Auto

Channel Width: Auto

☑ Enable SSID Broadcast

Figure 20: Wireless Settings of the router to which the user is connected.

Therefore the best solutions are number 1 and 2. Solution 1 would be the easiest to implement in terms of knowledge as it would also mean to change the router to a better position where there is open space and there are not obstacles between the transceiver and receiver. On the other side the second option it would mean that the router can stay in the same position but some knowledge in router configuration is needed in order to not make the QoS even worse.

5.2.1.3 Scenario 3 (Urban environment)

In this third and last scenario it was studied the wireless networks and the access points that were detected in the centre of Vienna. In this particular case the measurement was done in Stephansplatz. For this particular case Vienna has a public WLAN, the AP are set up in fixed locations to create a wireless local area network (WLAN), which enables to have an access to the Internet without a personal registration throughout all the main parts of the city. The only necessary thing to do is to accept the terms of use. This terms of use include important information that is of relevance for the user connected to the public network, e.g. The City of Vienna does not warrant the availability of the service, therefore the availability of the network is not ensured also some internet services and contents are blacklisted through content filters to enhance user safety and to prevent abuse. Also it says that the users are obliged to fair use of internet access, this means avoid using multimedia services and obviously it says that any illegal actions carried out connected to this network will be punished and the users can be banned from connecting to the network [33]. Bandwidths and data volumes are limited in order to ensure a good quality of service to the maximum number of users. The connection duration time is also limited [32].

Every AP (Figure 21) has a range of about 100 metres, despite the different obstacles that can be found throughout the city and that prevent the transmission of radio waves. The data rate is between 1 and 54 Mb/s. The AP are integrated in existing infrastructure, therefore they are capable of giving service to a wide area without disturbing the appearance of the city [32]. These AP are usually situated in high position in this particular case on top of a streetlight (Figure 21).

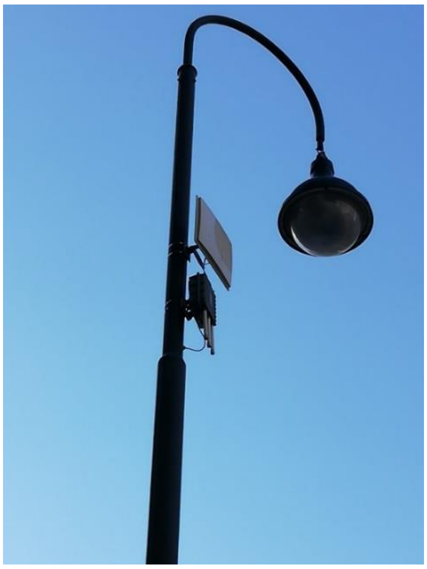


Figure 21: AP to the public WLAN. [Own image]

The exact position where the measurements were done can be seen in the Figure 22. It can be see that is was done in Stephansplatz and it was done between two access points of the public WLAN.

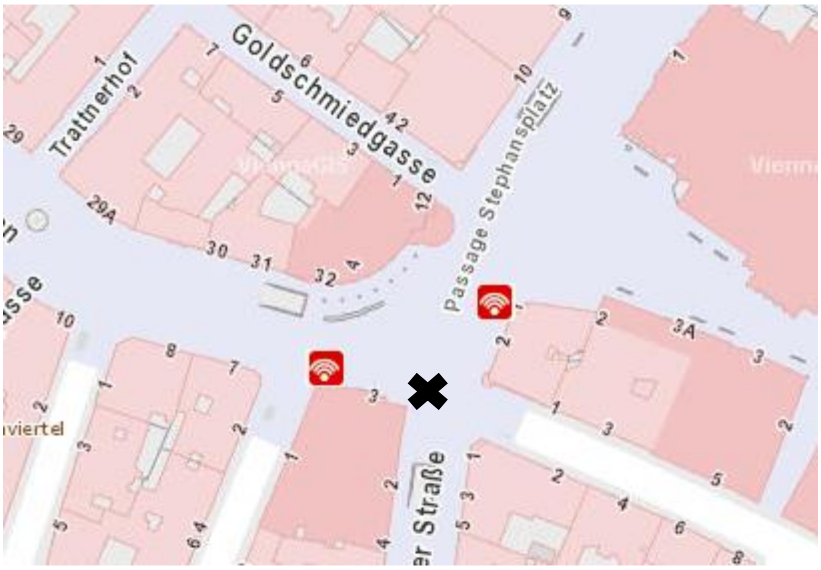
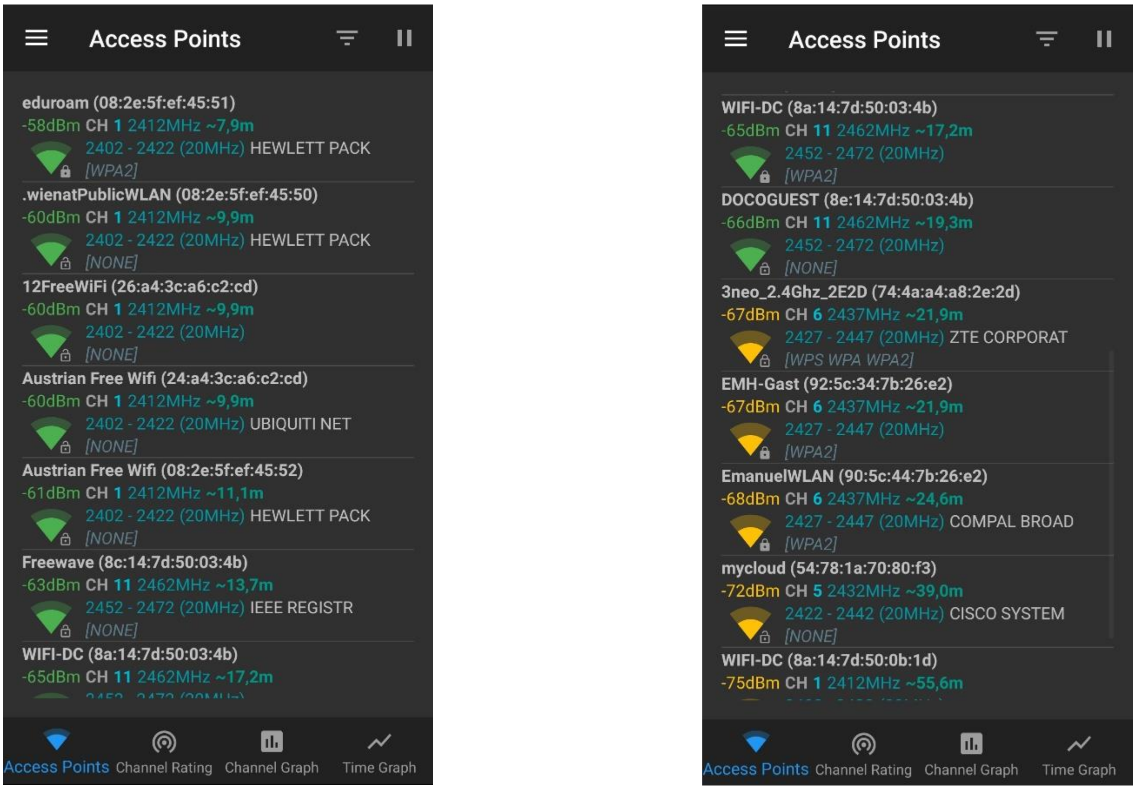


Figure 22: Map of the environment where the measurement was taken [34].

In this particular case it can be said that the network is not a WLAN and that it is a WMAN as it is a wireless network that gives service to a metropolitan area. Once the measurements with the application were done the APs that are visible in Figure 23 could be seen. As it can be seen the AP that sends the most power in this case is of eduroam, which stands for educational roaming and it is a wireless network developed by the academic community. On June of 2005 more than 350 institutions in 19 countries participated in eduroam, in this case for Vienna many universities are participating in the development of the network. The issue with this network is that you need to form part of one of these institution either as a student or as employee in order to be able to get Internet access. If you are part of the institution then you can use it with the username and password that you use in order to use the IT services of the institution [35] [36].

Then other wireless networks can be seen, one of these network is the public Wi-Fi of Vienna, which in this case is called Austrian Free Wifi and as it can be seen in the Figure 23 there are two access points to that wireless network.



eduroam (08:2e:5f:ef:45:51)
-58dBm CH 1 2412MHz ~7,9m
2402 - 2422 (20MHz) HEWLETT PACK
[WPA2]

.wienatPublicWLAN (08:2e:5f:ef:45:50)
-60dBm CH 1 2412MHz ~9,9m
2402 - 2422 (20MHz) HEWLETT PACK
[NONE]

12FreeWiFi (26:a4:3c:a6:c2:cd)
-60dBm CH 1 2412MHz ~9,9m
2402 - 2422 (20MHz)
[NONE]

Austrian Free Wifi (24:a4:3c:a6:c2:cd)
-60dBm CH 1 2412MHz ~9,9m
2402 - 2422 (20MHz) UBIQUITI NET
[NONE]

Austrian Free Wifi (08:2e:5f:ef:45:52)
-61dBm CH 1 2412MHz ~11,1m
2402 - 2422 (20MHz) HEWLETT PACK
[NONE]

Freewave (8c:14:7d:50:03:4b)
-63dBm CH 11 2462MHz ~13,7m
2452 - 2472 (20MHz) IEEE REGISTR
[NONE]

WIFI-DC (8a:14:7d:50:03:4b)
-65dBm CH 11 2462MHz ~17,2m

WIFI-DC (8a:14:7d:50:03:4b)
-65dBm CH 11 2462MHz ~17,2m
2452 - 2472 (20MHz)
[WPA2]

DOCOGUEST (8e:14:7d:50:03:4b)
-66dBm CH 11 2462MHz ~19,3m
2452 - 2472 (20MHz)
[NONE]

3neo_2.4Ghz_2E2D (74:4a:a4:a8:2e:2d)
-67dBm CH 6 2437MHz ~21,9m
2427 - 2447 (20MHz) ZTE CORPORAT
[WPS WPA WPA2]

EMH-Gast (92:5c:34:7b:26:e2)
-67dBm CH 6 2437MHz ~21,9m
2427 - 2447 (20MHz)
[WPA2]

EmanuelWLAN (90:5c:44:7b:26:e2)
-68dBm CH 6 2437MHz ~24,6m
2427 - 2447 (20MHz) COMPAL BROAD
[WPA2]

mycloud (54:78:1a:70:80:f3)
-72dBm CH 5 2432MHz ~39,0m
2422 - 2442 (20MHz) CISCO SYSTEM
[NONE]

WIFI-DC (8a:14:7d:50:0b:1d)
-75dBm CH 1 2412MHz ~55,6m

Figure 23: AP detected in scenario 3

As it can be seen in the figure in this case these networks do not have any kind of security in order to access to them which is a very common case in this kind of public networks. Therefore in this case it is extremely recommended to take actions in this aspect as all the task that are carried out using this network are in danger against possible attacks. To avoid this actions like in the first case can be carried out. In this case in terms of which access point of the network is better to be connected to there is not much difference and usually the devices connect to the AP that gives them the better QoS.

If the channels graph is looked (Figure 24) it can be seen that in this case there will be a lot of co-channel interference as the signals of the AP are a similar power level and they share the same channels. In this case unlike the scenario 2 the possibility of changing the channel where the AP is emitting is not possible as the network is a public network and the user does not have a direct access to the AP. In this case this makes sense as if every user could change the configuration of the access point it would generate security issues and even would make the configuration worse as every user would be able to change the configuration and would affect the QoS of the network.

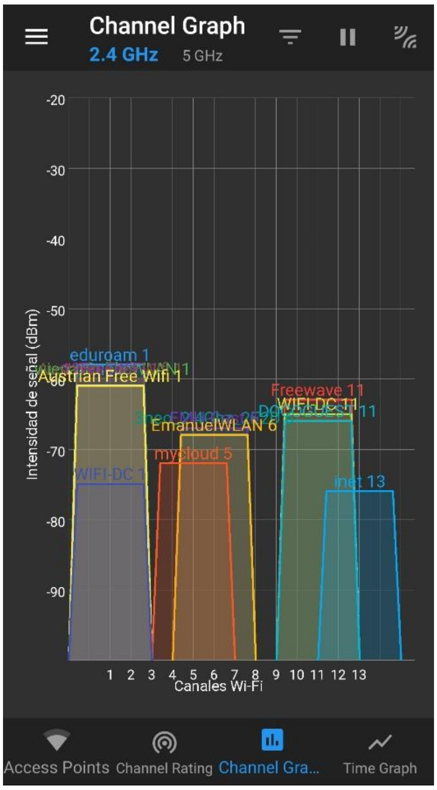


Figure 24: Channel graph for the APs

Therefore the best solution for this scenario is to use the mobile broadband connection in order to have a good Internet access. Also if the user uses the 4G connection there will be more security in all the tasks that the he carries out. Another possible solution is to use the eduroam wireless network if the user forms part of. With this network the issues of security disappear as in this case it uses the security protocol of WPA and therefore the tasks that carry out the user will be completely safe and without risks of attacks. Also an advantage that has this network is that there are not time, bandwidth and data rate limitations therefore the QoS will be better than the Austrian Free Wifi.

6 Conclusion and outlook

The wireless networks are here to stay in our lives and we have to be aware of the risks that have, how to solve the technical problems that might appear using them and how to optimize them in order to use them in an efficient way. Therefore the use of applications that analyse wireless networks should be a common thing in our daily life specially when we are in a new environment and we want to get access to the internet. The information that these applications give to us can be used in order to make decisions on to which access point does the user connects depending on the service that offers each network: security, speed, capacity…

The application displays the information in a very visual way in order to make the information easy to understand. Like this it will be easier for the user to decide which decisions have to be made in order to have the best experience when he connects to an AP to get Internet access. The application is really useful for every scenario, from a technical point of view or even from an informational point of view. It can be said that with the use of this application the user had improved the QoS of the Internet connexion and that the application gives valuable information to do so.

Some improvements could be done in order to make the application better. For example in order to make it easier for general public some recommendations could pop-up when the user is connected to a network, e.g. if the user is connected to a WLAN that does not have any security protocol the application could give information about the risks being connected to that network and also a list of some possible solutions could be given. Also in the case of the channels the application could calculate which channels are the ones with better QoS in order to configure the AP to emit in those channels. This kind of automatization could be implemented in order to improve the application and the main goals of it that are to improve both the QoS and to optimize the use that the users do of the WLANs.

Bibliography

[1] T. Seymour and A. Shaheen*, “History of Wireless Communication”,* RBIS, vol. 15, no. 2, pp. 37-42, Apr. 2011.

[2] Ahson, S. A., & Ilyas, M. (2007). WiMAX. Taylor & Francis.

[3] Nuaymi, L. (2007). *WiMAX: Technology for Broadband Wireless Access* (1st ed.). Wiley.

[4] Negus, K.J. and Petrick, A. (2009), "*History of wireless local area networks (WLANs) in the unlicensed bands*", info, Vol. 11 No. 5, pp. 36-56.

[5] Baun, C. (2019). *Computer Networks / Computernetze: Bilingual Edition: English – German / Zweisprachige Ausgabe: Englisch – Deutsch (German and English Edition)* (1. Aufl. 2019 ed.). Springer Vieweg. https://doi.org/10.1007/978-3-658-26356-0

[6] Kurose J, Ross K (2008) *Computernetzwerke.* Vieweg+Teubner, Wiesbaden

[7] Torrieri, Don (2018). *Principles of Spread-Spectrum Communication Systems*, 4th ed.

[8] Weinstein, S. B. (November 2009). "*The history of orthogonal frequency-division multiplexing*". IEEE Communications Magazine. IEEE Communications Magazine (Volume: 47, Issue: 11, November 2009). 47 (11): 26–35.

[9] Huidobro Moya, H. M. (2014). *Comunicaciones móviles: sistemas GSM, UMTS y LTE.*

[10] *GSM World Coverage Map- GSM Country List by frequency bands*. (2005). Accessed 21.April.2021. [Online]. Available at worldtimezone.com. https://www.worldtimezone.com/gsm.html

[11] Ergen, M. (2009b). *Mobile Broadband*. Springer Publishing.

[12] *Partners*. (2021). 3gpp.org. https://www.3gpp.org/about-3gpp/partners

[13] *IMT-2000 Spectrum*. (2000). Accessed 1.May.2021. [Online]. Available at Https://Www.Itu.Int/. https://www.itu.int/newsarchive/wrc2000/presskit/IMT-2000.html

[14] Resolution 212 (Rev.WRC-97). Implementation of International Mobile (1997, Geneva)

[15] Chen, H. (2007). *The Next Generation CDMA Technologies* (1st ed.). Wiley. pp 76-132.

[16] Dahlman, E., Parkvall, S., & Sköld, J. (2016). 4G*, LTE-advanced pro and the road to 5G* (Third edition.). Academic Press. pp 1-5

[17] Rohde & Schwarz North America. (2012, October 31*). LTE Evolution: From Release 8 to Release 10*. Accessed 5.May.2021. [Online]. Available at Https://Www.Slideshare.Net/.

https://www.slideshare.net/RohdeSchwarzNA/lte-eutran-rsanov2012day1

[18] Holma, H., & Toskala, A. (2009). *LTE for UMTS*. Wiley.

[19] Faruque, S. (2018). *Radio Frequency Multiple Access Techniques Made Easy* (SpringerBriefs in Electrical and Computer Engineering) (1st ed. 2019 ed.). Springer.

[20] Jaiaree, T. (2003). *The security aspects of wireless local area network* (WLAN).

[21] Faraj, K. E. (2019). *Security technologies for wireless access to local area networks*.

[22] J. R. Vacca. (2012). *Computer and information security handbook*. Newnes.

[23] S. Helling. (2015). *Home network security*. Technische Universiteit Eindhoven.

[24] R. Flickenger. (2007). *Wireless Networking in the Developing World: A practical guide to planning and building low-cost telecommunications infrastructure*. Hacker Friendly LLC, Seattle, WA, US.

[25] J.-H. Yeh, J.-C. Chen, and C.-C. Lee. (2003) *“Wlan standards,” IEEE Potentials*, vol. 22, no. 4, pp. 16–22.

[26] I. S. Association et al., (2011). “*Ieee 802.11 n-2009 amendment 5: Enhancements for higher throughput*,” Tech. Rep., Institute of Electrical and Electronics Engineers (IEEE), Tech. Rep.

[27] U. Varshney. (2003). "*The status and future of 802.11-based wlans*," Computer, vol. 36, no. 6, pp. 102–105.

[28] Kumar, A., Kumar, P., & Singh, M. P. (2013). A survey on wireless LAN internal roaming protocols. 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference On, 1–6. https://doi.org/10.1109/ICCCNT.2013.6726785

[29] Almási, B. (2012). A simple solution for wireless network layer roaming problems. *Carpathian Journal of Electronic and Computer Engineering*, 5, 5.

[30] C. Perkins. (2010). Ed. *IP Mobility Support for IPv4, Revised* RFC 5944. Accessed 6.May.2021. [Online]. Available at http://tools.ietf.org/html/rfc5944

[31] Khan, S., & Pathan, A. K. (2013). Wireless networks and security. Springer, 10, 978-3.

[32] *wien.at Public WLAN - free WiFi hotspots in Vienna*. (2014, 24 july).

Accessed 9.May.2021. [Online]. Available at Wien.Gv.At.

https://www.wien.gv.at/english/administration/ict/wlan/

[33] *GSM World Coverage Map- GSM Country List by frequency bands*. (2005).

Accessed 1.May.2021. [Online]. Available at

worldtimezone.com. https://www.worldtimezone.com/gsm.html

[34] Wierenga, K., & Florio, L. (2005). Eduroam: past, present and future. *Computational methods in science and technology*, *11*(2), 169-173.

[35] Florio, L., & Wierenga, K. (2005, June). Eduroam, providing mobility for roaming users. In *Proceedings of the EUNIS 2005 Conference, Manchester*.

[36] Rekhter, Y., Karrenberg, D., & Moskowitz, B. (1994). *Address allocation for private internets*.

[37] Hohensee, B. (2014). *Introducción a Android Studio. Incluye proyectos reales y el código fuente*. Babelcube Inc..

[38] Samuel, S., & Bocutiu, S. (2017). *Programming kotlin*. Packt Publishing Ltd.

[39] Sharma, K., & Dhir, N. (2014). *A study of wireless networks: WLANs, WPANs, WMANs, and WWANs with comparison*. International Journal of Computer Science and Information Technologies, 5(6), 7810-7813.

[40] Thompson, A., & Taylor, B. N. (2008). *Use of the international system of units (SI).*

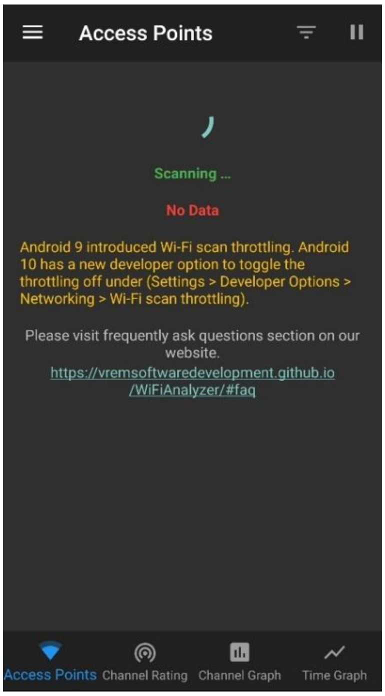
[41] Poole, I. (2017). *Free space path loss: details, formula, calculator. Adrio Communications Ltd,[Online].* Accessed 25.April.2021. [Online]. Available: *http://www. radio-electronics. com/info/propagation/path-loss/free-space-formula-equation. php.[Accessed 14 March 2017].*

[42] VREMSoftwareDevelopment, *WifiAnalyser* (23 December 2020), Accessed 15.April.2021. [Online]. Available at GitHub repository, https://github.com/VREMSoftwareDevelopment/WiFiAnalyzer

List of Figures

List of Tables

A: Figures that show the application screens and functionalities.



Access Points

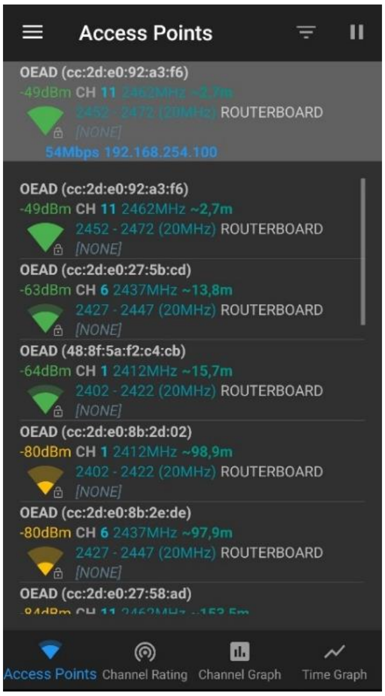
Scanning ...

No Data

Android 9 introduced Wi-Fi scan throttling. Android 10 has a new developer option to toggle the throttling off under (Settings > Developer Options > Networking > Wi-Fi scan throttling).

Please visit frequently ask questions section on our website.
https://vremsoftwaredevelopment.github.io/WiFiAnalyzer/#faq

Figure 25: Launching screen.



Access Points

OEAD (cc:2d:e0:92:a3:f6)
-49dBm CH 11 2462MHz ~2,7m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]
54Mbps 192.168.254.100

OEAD (cc:2d:e0:92:a3:f6)
-49dBm CH 11 2462MHz ~2,7m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]

OEAD (cc:2d:e0:27:5b:cd)
-63dBm CH 6 2437MHz ~13,8m
2427 - 2447 (20MHz) ROUTERBOARD
[NONE]

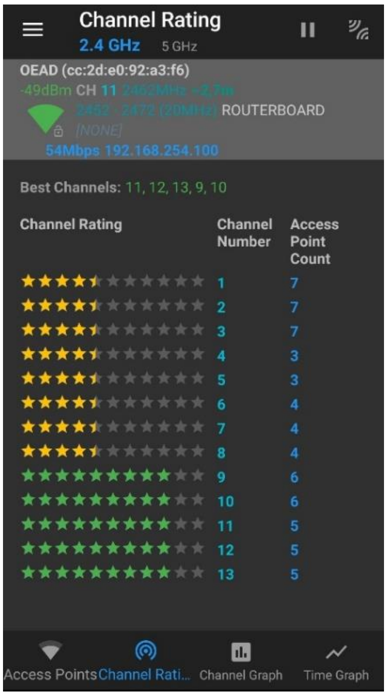
OEAD (48:8f:5a:f2:c4:cb)
-64dBm CH 1 2412MHz ~15,7m
2402 - 2422 (20MHz) ROUTERBOARD
[NONE]

OEAD (cc:2d:e0:8b:2d:02)
-80dBm CH 1 2412MHz ~98,9m
2402 - 2422 (20MHz) ROUTERBOARD
[NONE]

OEAD (cc:2d:e0:8b:2e:de)
-80dBm CH 6 2437MHz ~97,9m
2427 - 2447 (20MHz) ROUTERBOARD
[NONE]

OEAD (cc:2d:e0:27:58:ad)
-84dBm CH 11 2462MHz ~153,5m

Figure 26: Main screen of the application.



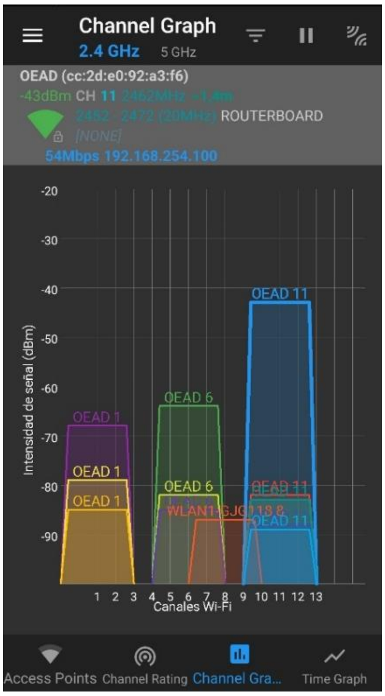
Channel Rating
2.4 GHz 5 GHz

OEAD (cc:2d:e0:92:a3:f6)
-49dBm CH 11 2462MHz ~2,7m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]
54Mbps 192.168.254.100

Best Channels: 11, 12, 13, 9, 10

Channel Rating	Channel Number	Access Point Count
★★★★½☆☆☆☆☆☆☆	1	7
★★★★½☆☆☆☆☆☆☆	2	7
★★★★½☆☆☆☆☆☆☆	3	7
★★★★½☆☆☆☆☆☆☆	4	3
★★★★½☆☆☆☆☆☆☆	5	3
★★★★½☆☆☆☆☆☆☆	6	4
★★★★½☆☆☆☆☆☆☆	7	4
★★★★½☆☆☆☆☆☆☆	8	4
★★★★★★★★★★☆☆	9	6
★★★★★★★★★★☆☆	10	6
★★★★★★★★★★☆☆	11	5
★★★★★★★★★★☆☆	12	5
★★★★★★★★★★☆☆	13	5

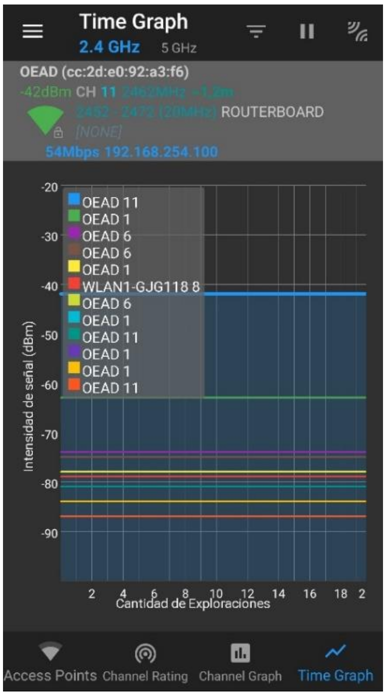
Figure 27: Channel rating screen.



Channel Graph
2.4 GHz 5 GHz

OEAD (cc:2d:e0:92:a3:f6)
-43dBm CH 11 2462MHz ~1,4m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]
54Mbps 192.168.254.100

Figure 28: Channel graph screen.



OEAD (cc:2d:e0:92:a3:f6)
-42dBm CH 11 2462MHz ~1.2m
2452 - 2472 (20MHz) ROUTERBOARD
[NONE]
54Mbps 192.168.254.100

Figure 29: Time graph screen