Spectrum sensing based on specialized microcontroller based white space sensors

Measuring spectrum occupancy using a distributed sensor grid

JULIA ALBA TORMO PEIRÓ

KTH Information and
Communication Technology

Degree project in
Communication Systems
Second level, 30.0 HEC
Stockholm, Sweden

Spectrum sensing based on specialized microcontroller based white space sensors

Measuring spectrum occupancy using a distributed sensor grid

Julia Alba Tormo Peiró

10 July 2013

Supervisor and Examiner: Professor Gerald Q. Maguire Jr.

School of Information and Communication Technology

KTH Royal Institute of Technology

Stockholm, Sweden

Abstract

The continuing increase in the adoption and use of wireless technology aggravates the problem of spectrum scarcity due to the way we utilize the spectrum. The radio spectrum is a limited resource regulated by governmental agencies according to a fixed spectrum assignment policy. However, many studies show that this fixed radio frequency allocation leads to significant underutilization of the radio spectrum creating artificial scarcity, as most of the allocated spectrum is not used all of the time in every location. To meet services growing demands, efficient use of the spectrum is essential. Therefore, there is a need to estimate the radio spectrum utilization in several locations and during different periods of time in order to opportunistically exploit the existing wireless spectrum. Cognitive radio technology aims to search for those portions of the radio spectrum that are assigned to a specific service, but are unused during a specific time and at specific location in order to share these white spaces and thus to reduce the radio spectrum inefficiency.

In this thesis, we study spectrum utilization in the frequency range from 790MHz to 925MHz. The spectrum sensing has been realized using a number of specialized microcontroller based white space sensors which utilize energy detection, situated in different locations of a building in Kista, Sweden. The occupancy of the frequency bands in this chunk of the spectrum is quantified as the fraction of samples with a power level greater than a threshold. The results from these spectrum measurements show that a significant amount of spectrum in this scanned range around the building is inefficiently used all the time.

Sammanfattning

Den senaste tidens ökning av trådlös teknik förvärrar problemet med spektrumbrist på grund av hur vi använder den. Det radiospektrum är en begränsad resurs som regleras av statliga myndigheter enligt en fast spektrumtilldelningen politik. Men många studier visar att den fasta frekvensplan leder till betydande underutnyttjande av radiospektrum och skapar en konstgjord brist eftersom de flesta av de tilldelade spektrumet inte används hela tiden i varje platsen. För att uppfylla tjänster ökade krav, är viktigt en effektiv användning av spektrumet. Därför finns det ett behov av att uppskatta användningen av radiospektrum i flera platser och i olika tidsperioder för att kunna utnyttja den befintliga trådlösa spektrumet i opportunistiskt sätt. Kognitiv radio teknologi syftar till att söka efter dessa delar av radiospektrum som tilldelas till en konkret tjänst och är oanvända i en viss tid och på viss plats för att dela dessa vita ytor och därför lösa radio spektrum ineffektivitet problem.

I denna uppsats studerar vi spektrumanvändning i frekvensområdet från 790 MHz till 925 MHz. Spektrat avkänning har utförts med hjälp av ett antal specialiserade mikrokontroller blanktecken sensorer vilka utnyttjar energin upptäckt, som ligger på olika platser i en byggnad i Kista, Sverige. Uthyrningsgraden av frekvensbanden i denna del av spektrumet kvantifieras som antalet prover med en effektnivå överstiger en tröskel. Resultaten från spektrat mätningarna visar att en betydande del av spektrumet i denna scannade intervall ineffektivt används hela tiden.

Acknowledgements

I want to thank my supervisor Professor Gerald Q. Maguire Jr for all his help, his patience with me and my difficult with the language, and for giving me the opportunity to work and learn by his side. I also want to thank his colleague Professor Mark T. Smith for helping me always with a smile every time I needed him.

Next, I would like to thank Javier Lara Peinado for collaborating with me in my project and helping me as well as keeping me calm when I needed it most.

And finally, thanks to the most important people of my life, my mother Julia Peiró Martí, my father Ángel Tormo Cruañes, and my uncle Juan Rafael Peiró Martí, for giving me the best advice and supporting me in all my decisions.

Contents

List of Figures

List of Tables

Acronyms

AC	Alternating Current
AGC	Automatic Gain Control
BNC	Bayonet Neill-Concelman
CR	Cognitive Radio
CREW	Cognitive Radio Experimentation World
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DSA	Dynamic Spectrum Access
FC	Fusion Center
FCC	Federal Communications Commission
GSM	Global System for Mobile Communications
GSM-R	Global System for Mobile Communications - Railway
GUI	Graphical User Interface
HDF5	Hierarchical Data Format
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical
ITU	International Telecommunication Union
JTAG	Joint Test Action Group
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Medium Access Control
MCU	Microcontroller Unit
MPS	Maintain Power Signature
NTIA	National Telecommunication and Information Administration

PAMR	Public Access Mobile Radio
PD	Powered Device
PoE	Power over Ethernet
PSE	Power Sourcing Equipment
PTS	Swedish Post and Telecom Authority
RAM	Random Access Memory
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
SNMP	Simple Network Management Protocol
SMA	SubMiniature version A
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
SRD	Short Range Device
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TI	Texas Instruments
UDP	User Datagram Protocol
UPS	Uninterruptible Power System
USB	Universal Serial Bus
USRP	Universal Serial Radio Peripheral
VSN	Versatile Sensor Node

Chapter 1

Introduction

Radio spectrum is a term used to refer the frequency range from 3kHz to 300GHz within the electromagnetic spectrum. This range includes frequency bands that are used for television broadcasts, radio, mobile phones, Internet access, emergency services, military applications, and navigation, among others.

As an intangible asset and because of the multitude of services that can be provided via this radio spectrum, organizations and regulations have been created to avoid overlapping usage and interference between users as this would negatively affect the quality of radio transmissions. Therefore, the spectrum was administratively divided into frequency bands, each band having one primary service or several services that may be able to co-exist with each other. The process of assigning frequency bands to services is called *frequency allocation.* Once services are allocated to bands, they are frequently subdivided into a range of frequencies which are assigned for exclusive of a particular licensed user. Additionally, there are some bands where a user license is not required, such as the Industrial, Scientific, and Medical (ISM) frequency band. For these bands the equipment must meet the requirements of the regulations in terms of emitted energy, frequencies used, modulation, coding, etiquette, etc. Each service has either primary or secondary allocation status, and stations of a secondary service shall not cause harmful interference to stations of primary services, although stations of secondary services can be subject to interference from stations of primary services.

These bands are generally regulated, by governmental agencies, according to a fixed spectrum assignment policy, i.e., the allocation is often static in spatial (for large or small geographical regions) and temporal (for days or decades) dimensions. This management model is known as *command and control* [1], and dates from before the dramatic development of wireless communications and when the radio communication technologies only required interference free communication to provide suitable perceived quality.

As an example of allocation, we can see in Figure 1.1 the United States radio spectrum allocation chart, were the use of the radio spectrum is regulated by two different entities:

- National Telecommunications and Information Administration (NTIA) regulates federal government users of the radio spectrum [2].

- Federal Communications Commission (FCC) regulates all other users of the radio spectrum (private citizens, business, state, and local governments) [3].

Zooming in Figure 1.1 we see that the radio spectrum is all allocated except from 3kHz to 9kHz (the beginning of the radio spectrum), and from 275GHz to 300GHz (the end of the radio spectrum). Those unallocated portions of the spectrum are represented in white in the United States spectrum allocation chart, while other colors represent different systems. Several partitions (colors) in the same frequency band represent that this frequency band has been allocated to multiple services. Fortunately, the fact that almost all the spectrum is allocated, does not mean that is all used.

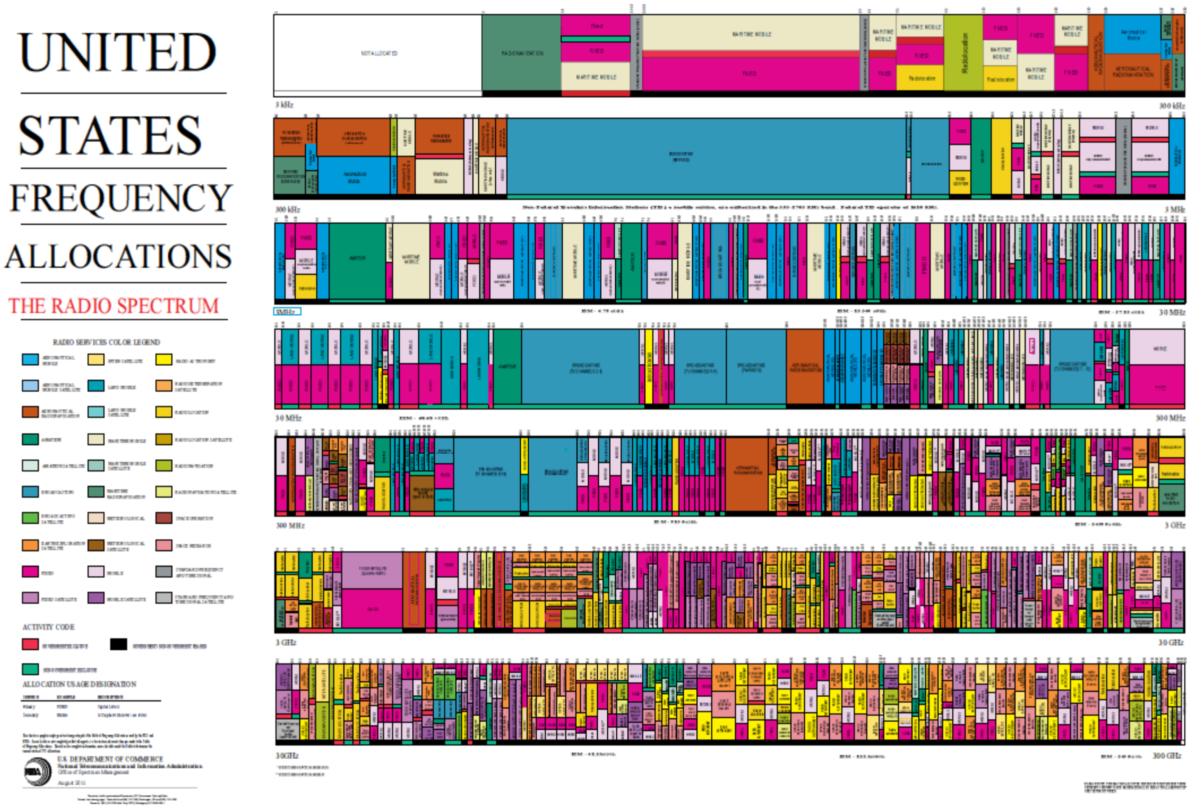


Figure 1.1 United States spectrum allocation chart, 2011 edition. [4]

1.1 Background summary

Nowadays, spectrum scarcity is primarily a problem due to the demand for more and more spectrum resources: The radio spectrum currently available for wireless communication services (unlicensed bands) is getting strained; access points and base stations are becoming overloaded; and prices for consumers are rising. However, the United States of America's Federal Communications Commission (FCC) responded with a report [5] showing that "*there is some evidence indicating that the shortage of spectrum is often a spectrum access problem. That is, the spectrum resource is available, but its use is compartmented by traditional policies based on traditional technologies. New radio technologies may enable new techniques for access of spectrum and sharing of the spectrum resources*". This means that theoretically everyone can be served with the limited spectrum available, but with the current spectrum management policy, some bands are very crowded while others such as the licensed bands and amateur radios are idle most of the time, leading to a waste of spectrum resources.

From January 2004 to August 2005, the US Shared Spectrum Company conducted measurements on the utilization of the spectrum in the range from 30 MHz to 3 GHz and their results showed that the average occupancy of these bands is only 5.2 % [6].

Other studies from 2008 to 2009 confirm this lack of efficiency, and conclude that spectrum utilization depends on time and the place [7, 8, 9].

Figure 1.2 shows one result of a survey of spectrum utilization made in a suburb of Brno, Czech Republic. In this figure we can see the notably different activity levels in different time periods even some of these frequencies show a total lack of activity.

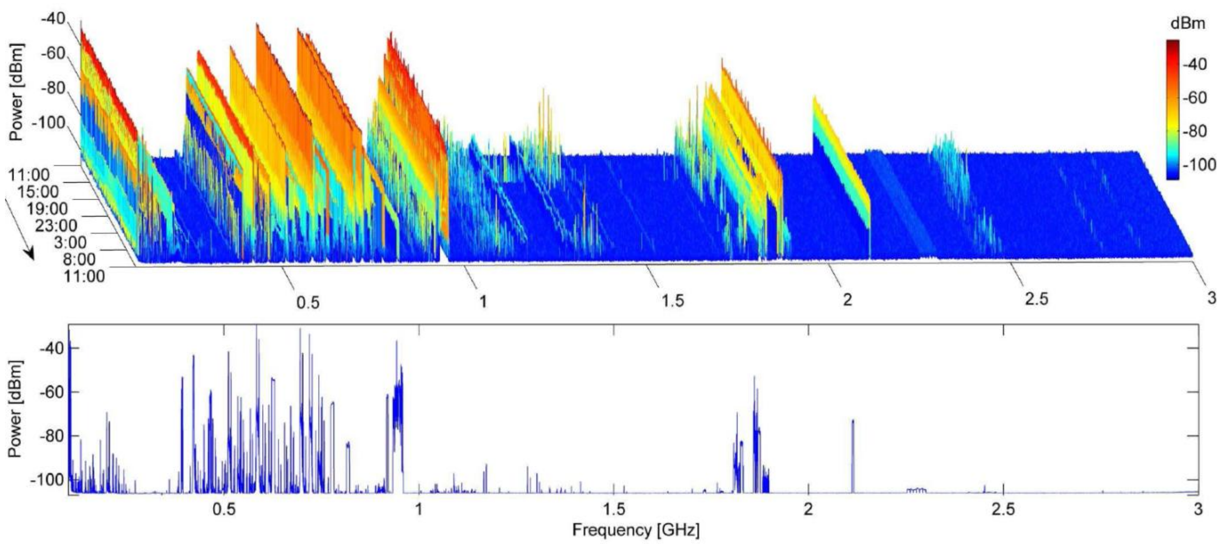


Figure 1.2 24-hour maximum spectrum usage measured over six days in Brno, Czech Republic. [9]

In the autumn of 2012 the European Commission put out a communication to promote the shared use of radio spectrum [10], and the FCC is also encouraging licensees to temporarily lease unused spectrum to third parties [5] with the obvious requirement that these secondary users (who can be licensees or non-licensees) do not interfere with the transmission of the primary user.

The idea of cognitive radio (CR) arose as the key technology to enable the use of spectrum in a dynamic manner, hence the spectrum could be used more efficiently. CR allows terminals to detect whether a part of the spectrum is being used or not and thus, the unused part can be shared. Initially, CR was to be realized using a software defined radio, where the software embedded in a wireless device automatically defines the communication parameters depending on the demands of the network and the user, and that these parameters change in real-time as the user moves from place to place. Next, the interest shifted to a newer version of CR which is designed to be sensitive to the changes in its surroundings. A CR aims to find those portions of the radio spectrum that are unused or used sporadically at a certain place and time. These unused portions of the radio spectrum are called *white space*. Consequently, instead of being stuck using one frequency band, CR devices would be able to dynamically pick the best frequencies with respect to the application's requirements and use one of these frequencies to communicate.

1.2 Goal

Many researchers in several different countries have done research concerning the inefficiency of the utilization of the spectrum leading to the problem of its scarcity. Many papers discuss how CR devices can take advantage of this inefficient use, and how CR devices should cooperate in order to accurately measure the spectrum usage at their location, and the different methods that can be used to detect the primary user.

In this thesis, the goal is to use a number of specialized microcontroller based low-cost white space sensors which utilize energy detection, to measure the spectrum occupancy in a specific range of frequencies, at a certain set of locations, and during a longer period of time. Due to the deployment of a number of sensor platforms, we aim to mitigate the negative effects of multipath, shadowing, and avoid the hidden listener problem. The sensors will deliver packets containing the frequency scanning data to a server which will collect this data and will permit us to evaluate the typical utilization in this chunk of spectrum, in order to find current and probable future white spaces. This approach could reduce the complexity of CR devices by requiring only a geospatial database of available spectrum that the CR device can query.

One of the main issues of this project is that the board should be connected only to an Ethernet cable, and with the prototype of the board this is not possible. Fixing this problem, this Ethernet cable will provide both power (using power over Ethernet) and communication (enabling the device to be programmed and to send data concerning its local environment to a server).

1.3 Thesis structure

This thesis is organized into 5 chapters, where chapter 1 puts the reader in a position to know the reason of this project; chapter 2 explains some knowledge needed to understand the rest of the thesis; chapter 3 presents the objectives fixed to achieve the goal of the thesis as well as the measurement equipment, measurement method, measurement parameters, and measurement location established to accomplish those objectives; chapter 4 reveals some obtained results and analyses them in order to reach conclusion based on the thesis's goal; and chapter 5 summarize conclusions and future plans.

Chapter 2

Background

This chapter presents and overviews the global context of this thesis project and focuses on specific background knowledge that is needed to understand the rest of this thesis.

2.1 Introduction to Cognitive Radio (CR)

Every year increases the range of frequencies that require a license, increases the wireless technology, increases the cellphone's required peak data-rate (which implies more spectrum bandwidth), … Since the FCC divided up the spectrum and sold licenses for frequency bands, it has been created artificial scarcity where none need exists due to the inefficiency of the allocation in finite radio spectrum resources.

2.1.1 White space

As it was explained in chapter 1, portions of the radio spectrum that are assigned to particular services but are not used at a specific location and time, are referred to as *white space* or *spectrum holes*.

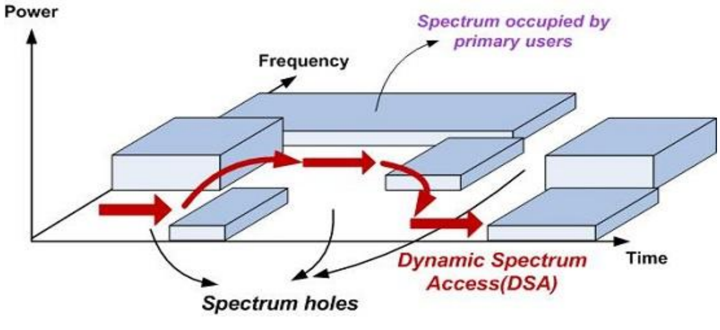


Figure 2.1 Radio frequency white space

2.1.2 CR technology

Cognitive radio (CR) technology is the key technology to share the available (limited) radio spectrum in a dynamic manner. This new communication paradigm is also known as dynamic spectrum access (DSA) or cognitive radio networks [11, 12], where licensed spectrum assigned to primary users (licensed users) can be used by secondary users (unlicensed users).

The idea of CR was officially presented for the first time in an article by Joseph Mitola III and Gerald Q. Maguire Jr., in August 1999 [13]. At that time, the CR was conceived as a wireless reconfigurable system defined by software. The software embedded in the multiband radio device would define the parameters under which the device should operate in real-time depending on the demands of the network and the user. The definitions of these parameters change as the user moves from place to place to more efficiently use the available spectrum.

Today, the majority of CR research is focused on the cognitive radio spectrum detector, which is designed to make decisions based on the state of the radio spectrum and a user's requirements (while considering the user's desired quality of service - QoS). This detector is generally envisioned as part of a CR built on a software radio platform and is aware of the changes in its surroundings, learning from them, and modifying its own communication parameters in order to adapt to changes in the environment [14].

2.1.3 CR architecture

The challenge of the physical architecture of a CR device is accurate detection of weak signals from licensed users (primary users) over a wide spectrum range. In order to address this sensing and to provide the QoS requested by the user, the CR must select an appropriate frequency band in which to transmit. Depending on CR's hardware design, it can be programmed to transmit and receive over different frequencies, and use different transmission access technologies. Figure 2.2 shows a generic architecture of a CR transceiver [12].

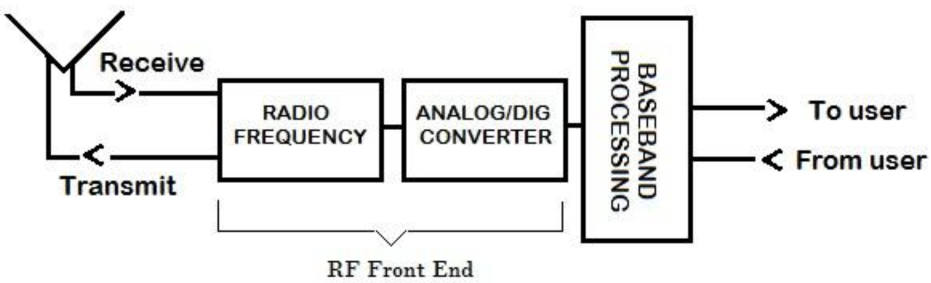


Figure 2.2 Generic architecture of the cognitive radio transceiver

2.1.4 Functions of a CR

The CR transceiver scans for unused bands, collects occupancy data, and depending on the user's requirement the CR device selects the most appropriate white space to utilize in this specific location, thus exploiting spectrum sharing. Therefore, a CR device must accomplish the following functions [12]:

- *Spectrum sensing*: Detecting white spaces. Also, maintaining an awareness of changes in the utilization the relevant spectrum.
- *Spectrum management*: Changes its own radio transmitter's parameters after selecting the best available channel that meets the user's communication requirements.
- *Spectrum sharing*: Coordinates access to the spectrum with other CR users (unlicensed users) to minimize the interferences between them [15].
- *Spectrum mobility*: Provides seamless communication during transmission. The secondary user's communication may be interrupted if the primary user uses the band, hence the CR device will need to perform spectrum handoff to enable continued data transmission.
- *Spectrum handoff*: In licensed bands, when a primary user is detected in the band occupied by a secondary user, the secondary user must vacate the current band as soon as possible and move to another available band. There are several handoff strategies that consider the latency of this handoff [16]. Interference avoidance with primary users is the most important issue, as otherwise the secondary users would usurp the rights of the primary user to use the band which they hold a license for.

2.1.5 How CR accomplish its functions

To accomplish its tasks, CR follows a *cognitive cycle* (illustrated in figure 2.3), where:

- First, captures information about its radio environment and detects the gaps (*spectrum sensing*);
- Second, studies the characteristics of the spectrum holes detected, in order to see if they can be shared without harming others with interference (*spectrum analysis*);
- Third, determines the data rate, the transmission mode, and the bandwidth of the transmission required by the user. Then an appropriate white space is chosen according to the characteristics studied in second step and the user's requirements (*spectrum decision*).

Given that most of the spectrum is licensed, and a large portion of it is unused or is unoccupied at specific locations and times, the challenge is to share the white spaces without causing interference. Additionally, if the band is to be used by a licensed user, the CR moves to another white space or remains in the band after changing its transmission power level or modulation scheme. Any environmental change during a transmission should provoke a real-time adjustment perhaps necessitating a handoff to switch from one white space to another as necessary (*spectrum mobility*).

Some unlicensed bands, such as the ISM bands and the mostly idle amateur radio bands have been very attractive for transmission and have led to the introduction of several novel wireless technologies (there are primary, secondary, and even tertiary users in several of the ISM bands), thus resulting in considerable coexistence problems. These bands can also benefit from spectrum sensing and in order to enable all users to have the same right to access the spectrum while avoiding triggering handoffs. However, there are some rules (often referred to as spectrum etiquette) these unlicensed users must follow to minimize mutual interferences (*spectrum sharing*) [17].

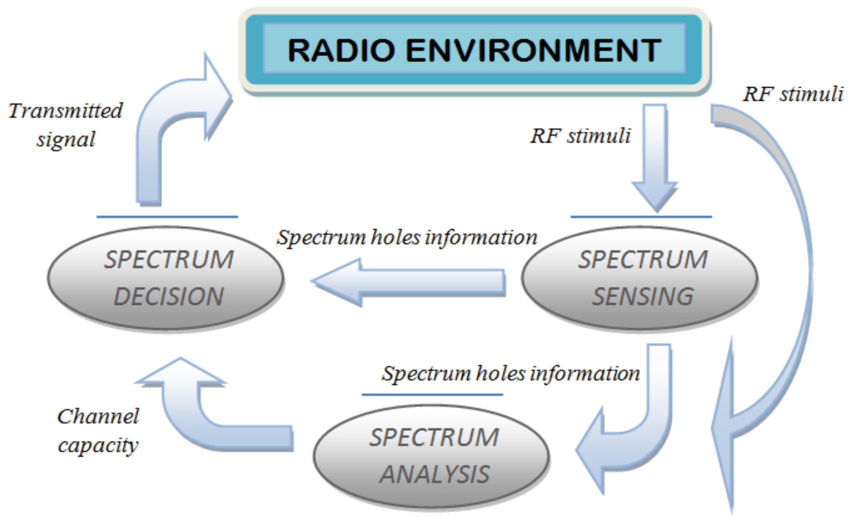


Figure 2.3 Cognitive cycle

2.1.6 Challenges of CR

Two of the most difficult challenges which CR has to deal with are the problem of hidden listeners and detecting spread spectrum primary users. Both of challenges may lead a CR to incorrectly decide that a frequency band is unoccupied and as a result CR may cause interference to the primary user.

2.1.6.1 Hidden listeners problem

In an ideal scenario CR devices are able to sense the local spectrum usage changes and adapt its own radio parameters accordingly. But, in reality in some cases a CR device which is scanning some regions of the spectrum for transmission might consider a frequency band free when it is not, due to the location of the CR device. As we can see in Figure 2.4 the secondary users can cause unwanted interference to the primary user (in this case for a receiver listening to a remote transmitter) as the primary transmitter's signal is not detected because of the CR device is located in a shadow with respect to this transmitter, because it is located too far from the transmitter, or some other reason that it cannot hear the transmitter - while the receiver which is listening to the primary transmitter can receive transmissions successfully [18]. This problem is known as the *hidden listeners* or *hidden primary user problem*.

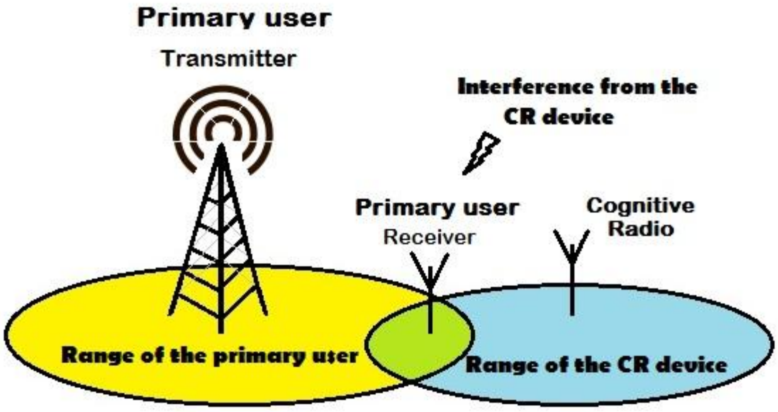


Figure 2.4 Hidden listener problem

As noted in the paragraph above, two of the dominant causes for the hidden listener problem are:

- *Multipath fading*: In any terrestrial radio communications system, the signal will reach the receiver not only via the direct path, but also as a result of reflections from objects such as buildings, hills, ground, water, etc.., that are adjacent to the main radio propagation path.
- *Shadowing*: A terminal cannot detect a signal because of objects such as mountains, houses, are in the middle of the path thus blocking the signal from propagating to the terminal (where in this case the relevant terminal is the CR device).

Figure 2.5 shows an example of multipath fading, shadowing, and hidden listener (called also receiver uncertainty) where:

- *CR1* (CR device) is located inside the transmission range of primary transmitter (PU Tx) and has a line-of-sight path to it.

- *CR2* is located inside the transmission range of PU Tx, but suffers *multipath fading* due to the multiple attenuated copies of the primary user transmitter (PU Tx). Also, there is a house that is blocking the direct signal from the PU Tx, thus CR2 also suffers from *shadowing*.

- *CR3* is located outside the transmission range of PU Tx hence it suffers from *receiver uncertainty* (*hidden listener problem*) because it does not detect the presence of the primary user receiver (PU Rx). As a result, CR3 may conclude that there is no primary user in the immediate vicinity and it may interfere with the reception at PU Rx.

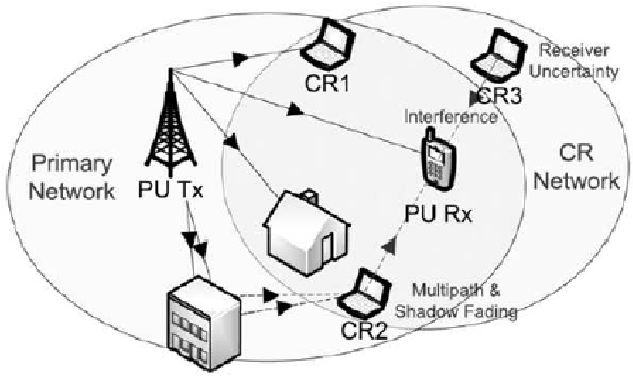


Figure 2.5 Example of hidden listener, shadowing, and multipath [12].

2.1.6.2 Spread spectrum primary users

Detecting *spread spectrum primary users* can be difficult, hence leading to a false identification of a white space. For commercially device there are two main types of technologies: fixed frequency (operates at a single frequency or *channel*) and spread spectrum (a modulation technique that uses a wide band to spread the signal's energy over). Primary users that use spread spectrum signaling are difficult to detect as the power of the primary user is distributed over a wide frequency range and this power level can even be lower than the channel's thermal noise or similar. This case is illustrated in Figure 2.6. Note that the case of a primary spread spectrum user is complex, since it may be possible for a narrow band interferer to successfully transmit without negatively affecting the primary spread spectrum transmissions if there is enough gain due to the coding of the spread spectrum signal. However, unless the CR knows about this spread spectrum transmission it will not be able to avoid mistaking the narrow band which is being sensed as white space.

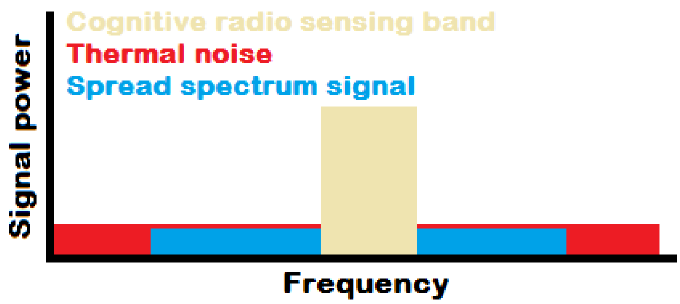


Figure 2.6 Spread spectrum signal

2.1.7 How CR detects spectrum holes (Spectrum sensing)

As it stated above, one of the functions of a CR is to detect spectrum holes and to be aware of changes in its surrounding radio environment. But, the fundamental issue is how to determine, in a specific location and at a specific moment, if any portion of the assigned spectrum is available for a secondary transmission. Consequently, there are number of spectrum sensing techniques which CR devices can use to detect the white spaces.

The most efficient way to know whether a frequency band is occupied or not, is to be told if there is a primary user, otherwise the CR must detect if there is a primary user emitting in that band. Theoretically, all the frequencies that the CR device does not detect a primary user must be a white space, but in reality is not that simple. For example, the CR may not always have a good line-of-sight channel to the primary transmitter. Additionally, the primary receiver might never transmit, hence it is a receiver only device and it is located in a different place than the CR device. Because these devices are located in different locations, the CR cannot determine what the receiver might be able to receive.

Many techniques have been developed to detect spectrum holes and these can be classified as [9, 19]:

- ***Transmitter detection*** (non-cooperative detection): The CR should have the capability to determine by itself (through its local observation) if a signal from primary transmitter is present in a certain range of spectrum. Unfortunately, this model cannot address 'hidden terminals', 'shadowing', and 'multipath fading'. The techniques proposed for transmitter detection are:

    - **Matched filter detection**: The CR has *a priori* knowledge of the primary users' signals based upon one or more databases (index by frequency). Given this knowledge the CR can correlate the received signal with the known signal or a template. Although this technique is the fastest and is the optimal, it requires maintain a lot of information about the different templates that need to be used at different frequencies and perhaps in different places.

    - **Energy detection**: When a receiver cannot gather information about the primary user's signal, an optimal detector is an energy detector. The energy detected from the primary signal is compared with a threshold value to decide whether a user is present or not. If the received energy exceeds this threshold, then the band is assumed to be occupied. This is the most common technique because of its low computational complexity; although, it is inefficient as there is no way to distinguish between noise, interference, and modulated signals.

    - **Cyclostationary feature detection**: Modulated signals are in general coupled with sine wave carriers, pulse trains, repeating spreading, hopping sequences, or cyclic prefixes, resulting in periodicity. This technique uses the spectral autocorrelation function, which correlates the signal with time-shifted signal versions of itself, hence it is useful for finding repeating patterns in a signal. The correlation enables the detector to distinguish between modulated signals (in which the autocorrelation exhibits periodicity) and noise signals (stationary signals with no correlation). However, it is computationally complex and needs a long observation time.

- ***Cooperative detection:*** Due to the fact that *transmitter detection* model cannot prevent the problems mentioned above, we can utilize sensing information from multiple CR terminals. The goals are to reduce the overall detection time and to mitigate false alarms by combining information from spatially distributed observations. In this approach a number of sensors located in different locations share their information. The cooperation can be [20]:

  - **Centralized**: By means of a base-station as a fusion center (FC) that gathers all the sensing information from the CR radios.

    1. The FC selects a channel or a frequency band of interest for sensing and instructs all cooperating CR devices to individually perform local sensing.

    2. Cooperating CR devices report their sensing results to the FC.

    3. The FC combines the received information, detects the presence of primary users and distributes the decision to the CR users.

  - **Distributed**: CRs exchanging observations among themselves and converging on a common decision as to whether there is a primary user or not.

  - **Relay-assisted**: When multiple hops are needed in distributed scheme to obtain sensing results, the intermediate hops relay information generated by the CRs.

  Only CRs with reliable information are allowed to report their decisions to the central unit. This reliability can be increase by using two threshold values instead of one, thus only those who detected a signal above those thresholds will be considered, hence some sensors will be ignored. This method does not eliminate the problems that degrade the performance of the primary user detecting mentioned in section 2.1.6, but rather they mitigate these problems. Although cooperative approaches provide more accurate sensing performance, they cause additional traffic to be sent between the cooperating CRs [21].

2.1.8 Using history for predictions

CR not only is based upon sensing, we can also monitor a certain frequency band of interest in order to learn that some frequencies are occupied only at some specific times, for example when somebody makes a phone call is unlikely that this call will last all day. Therefore, an essential feature of CR devices is the agility of the CR device to change from using one white space in the spectrum to using another white space. In order to understand these longer term temporal occupations of frequency bands, more sophisticated techniques are required in order to understand what portions of the spectrum are likely to be unused at a specific time and location, and to keep track of these variations in order to make predictions of the future profile of the usage of this portion of the spectrum in this location.

2.1.9 Hyperspace in CR

We have seen in section 2.1.7.1 different methods to detect the signal of a primary user in order to avoid interfering with it, but there are many challenges (such as not being able to detect the presence of spread spectrum signals) that are outside the scope of these methods, thus leading underestimating the usage of the spectrum.

There are some more advanced methods (such as waveform-based sensing or radio identification) that can make a deeper analysis of the signals present in a portion of the spectrum, rather than just measuring the amount of energy. These can give a more complete picture of the usage of the spectrum, but they have a higher computational complexity, thus requiring mid-range or high-end hardware for this computation. These methods can analyze the modulation, waveform, bandwidth, carrier frequency, and code dimension of a signal. These methods may create new opportunities for spectrum usage. For example, today with the use of multi-antenna technologies, multiple users can be multiplexed into the same channel, at the same time, and in the same geographical area, by exploiting different angles of arrival. In this hyperspace also called electrospace, white space is a *spectrum space hole*. In the case of cooperative distributed sensing, sharing information among CRs is a challenging task, as the individual CR's decision can be soft or hard and too conservative in decision process may lead to missed opportunities.

2.2 Introduction to Power over Ethernet (PoE)

Power over Ethernet (PoE) is a technology designed to deliver to the devices attached to a local area network (LAN) the power they need through the Ethernet cable. This eliminates the requirement to locate devices only near AC power outlets, eliminates low efficiency AC to DC adaptors, and there is no need to have an additional cable to power the device. PoE does not degrade the data communication of the network.

LAN cables are standardized with eight wires grouped into 4 pairs (the pairs are twisted together to cancel interference from external sources and avoid crosstalk between cables). Generally, only two pairs are used for data transmission, hence the other two pairs are available. This led to the idea of using this two pairs of twisted wire to provide power to attached devices.

Many different vendors introduced their own methods of providing power over these other pairs. This led to a need for standardization to provide guidance to manufacturers to develop interoperable devices. In 2003 PoE was standardized by an IEEE 802 working group as a standard called **IEEE 802.3af**. [22]. The original standard provides up to 15.4W of DC power (with a minimum 44 V DC and 350 mA) to each device, but only 12.95W (37V and 350mA) is assured at the powered device since some power is dissipated in the cable. In 2009 the standard was updated as **IEEE 802.3at.** [23], also known as **PoE+** or **PoE plus,** and provides up to 25.5W of power (at a minimum 42.5V and 600mA). Both versions of the standard define a process having three operational states (detection, classification, and operation) to safely power a powered device (PD) over the cable and to remove power if the PD is disconnected, while avoiding damaging devices that are not capable of PoE operation. This standard prohibits using all four pairs to provide power, but some manufacturers have announced products that claim to support the new 802.3at standard, but provide up to 51W of power through the same cable by using all the 4 pairs.

Category 5 (CAT5) and higher wiring can be used for PoE. PoE can even use category 3 (CAT3) wiring if less power is required. The maximum cable resistance for 100 meters of cable is 12.5Ω for CAT5 and above, and 20Ω for CAT3 [24]. Cables that use all four pairs to transmit data (as in the case of a 1000BASE-T LAN network) have two modalities to deliver the direct current (DC): **Mode A** uses pins 1-2 and 3-6 to power the device; **Mode B** uses pins 4-5 and 7-8 to power the device; thus two pairs of wires are going to transmit power and data at the same time [23].

Power is supplied via the LAN infrastructure through the RJ45 connector automatically when a compatible terminal is detected, while power is not supplied to devices that are not PoE capable. This technology supports a point-to-multipoint power distribution architecture (via a star topology), so all PoE devices can be connected to the same PoE switch. This PoE switch can be connected to a central uninterruptible power system (UPS) so that in case the electricity fails all PoE devices can continue to operate without problems. This is particularly a concern for voice over IP "telephony".

As PoE is an intelligent source of power, the devices can be turned off or rebooted remotely using a protocol like SNMP (for network management) [25]. Furthermore, PoE is designed to protect network equipment from overload, under powering, or incorrect installation.

2.2.1 PoE operation: PSE and PD

In terms of its operation, PoE devices can be classified into 2 groups:

- **PSE** (power sourcing equipment) → Feed power to PoE elements

  A PSE is a device which provides power over the Ethernet cable. If the device is a PoE switch, it is called "endspan" (typically a PoE capable switch or hub). Otherwise, if it is an intermediate device between a non-PoE Switch and PoE device the PSE is called "midspan" (for example using a PoE injector).

- **PD** (powered device) → Consume energy received by PoE

  A PD is a device that consumes energy and it is fed by a PSE. The PD input is typically an RJ-45 (8-pin) connector but, depending on its design it can also be powered by an auxiliary port (auxiliary ports are backup power in case a PoE PSE fails). Examples of PDs are IP cameras, wireless LAN access points, and VoIP phones.

2.2.2 Process for safely providing power over an Ethernet cable

The process for safely powering a PD over the cable and for removing power if a PD is disconnected, while preventing a PSE from injects electrical power to devices that do not support PoE the PSE follows these steps [26]:

1) **Detection**: Periodically the PSE must checks if there is a plugged-in device connected to it that supports PoE. This phase takes 500 milliseconds.

   To accomplish this, PSE sends different voltage levels (from 2.7V to 10.1V) and checks for any response. A PD device indicates that it compliances with the standard by having a ≈25kΩ resistor, and that it is awaiting power. If PSE detects too high or too low a resistance, i.e. the PSE does not receive an expected response, it means that the connected device does not support PoE.

2) **Classification**: Classification is an optional phase (otherwise, a PSE will supply 48V). To know how much power needed by the PD, the PSE increases the input voltage to between 14.5 V and 20.5 V and checks the amount of current flowing. The PD indicates its class by means of a fixed current set by a resistor (Rclass).

   This feature allows the PSE to measure the current flowing to the PD, indicating its "power class". Based upon this current the PSE determines which of the five available power classes this PD is signaling that it is. Changing the resistor (Rclass) will change the power requested by PD. The values of the Rclass for each power class change depend on the *controller* device each PD uses. Table 2.1 shows how much power is required for the default class and each of the optional power classes.

Table 2.1 Classification of PD in Power over Ethernet

CLASS	MODE OF USE	PD POWER (W)
0	Default	0.44-12.95
1	Optional	0.44-3.84
2	Optional	3.84-6.49
3	Optional	6.49-12.95
4	Reserved	-

3) **Operation**: The PSE monitors the PD and provides the required power. The PSE must itself against overload and avoid unwanted electrical power transmission. The maintain power signature (MPS) is presented by a powered PD to assure the PSE that it is still there.

The PD will operate based upon the configuration that the PSE imposes and this will depend upon the cable and the transmission mode used by the PSE. An example of a PoE capable switch connected to both PoE capable and not PoE devices is shown in Figure 2.7. In this figure the green color is used to illustrate the cables which carry power to the PDs.

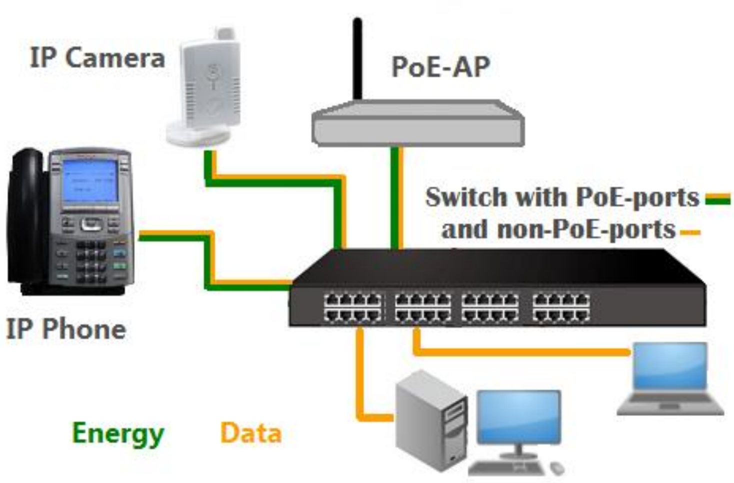


Figure 2.7 Example of a network with PoE

2.3 Related work

This section describes some other surveys and projects that are some way related to our project.

2.3.1 Cooperative spectrum sensing

There are many papers that discuss the benefits of cooperation in cognitive radio, but only limited number of testbeds are in operation. In [21] is shown that allowing the CRs operating in the same band to cooperate, the detection time is decreased and the agility of the CRs to detect a primary user and change from one white space to another increases. Also, in [19] conclude that *"individual sensing is not adequate for reliable detection of primary users due to shadowing and multipath effects"* being the cooperative decision the key to reduce the probability to interfere with the primary user. As we stated in section 2.1 we deployed a number of sensors platforms in order to mitigate the negative effects of multipath, shadowing and avoid hidden listener problem.

2.3.2 Protocol to Access White-Space (PAWS) Databases

The PAWS protocol [31] defines communications between the database and secondary devices, to allow a secondary device to access a database through the Internet in order to obtain spectrum availability information. The database contains current information about the available spectrum at a given location and time. Such a secondary device should provide its geolocation and perhaps other data to the database using a well-defined format to query the database. The server will answer with a list of available white-spaces frequencies for that specific geolocation. After this the device should send an acknowledgement to the database informing the database of the channel(s) that has selected along with other device operation parameters. If the device moves, changes operating parameters, loses connectivity, ..., it should query the database again. In our project, the sensor platforms deliver the frequency scanning data to the server, thus the idea could be that the server constructs databases with all the data collected, and CR devices just would have to query the database that contains information about the available spectrum at their location.

2.3.3 Spectrum sensing based on sensor node platforms

In October 2012, Zoltan Padrah presented his master's thesis Distributed Spectrum Sensing in Unlicensed Bands Using the VESNA Platform at Jozef Stefan Institute in Ljubljana, Slovenia [30]. This work is part of the Cognitive Radio Experimentation World (CREW) federation. They used a low-cost versatile sensor node platform (VSN) which can be powered by batteries, solar panel, or an external power supply. The radio module of this platform utilizes two radio interfaces based upon Texas Instruments CC1101 and CC2500. Both of these radios are connected to the processor module through the same serial peripheral interface (SPI interface). A graphical user interface (GUI) enables the user to specify control parameters for the radio and the resulting measurement can be shown using Matlab. This thesis names many applications for which this kind of sensor can be used, such as making a centralized grid to solve the problem of the hidden terminal or building a spatio-temporal spectrum occupancy map. The difference between the experiment for distributed spectrum sensing in this thesis and in our thesis is that they used the VSN based upon the CC2500 radio module to mimic a spectrum sharing scenario, where a terminal with CR capabilities is initially transmitting a continuous signal in a given frequency band, and has to change (in order to avoid interference) to another usable frequency band when it detects a second terminal (without CR capabilities) that starts transmitting in a frequency band that overlaps with the one used by the first terminal. In our experiment, we used a low-cost sensor platform powered by PoE that utilizes a radio based upon Texas Instruments CC1101 to scan, from a set of locations inside a building, the frequency range from 790MHz to 925MHZ to study the utilization in this portion of the spectrum, at those certain locations, and during a longer period of time.

In ISM Bands Spectrum Sensing based on Versatile Sensor Node Platform [32] shows spectrum sensing measurements results for the 868MHz ISM band using VSN to scan the ISM band frequencies. In their study, one VSN based on a C1101 transceiver has been used to demonstrate the RSSI based spectrum sensing in the 868MHz ISM band, performing a frequency sweep from 868MHz to 950MHz. In our experiment, we have scanned a larger frequency range to measure the spectrum occupancy.

2.3.4 Software for developing a distributed white space sensor grid for CR

Javier Lara Peinado [33] developed for use in his master's thesis project the software with which we are going to use to program our sensor nodes. This software includes:

- A network boot loader for a power over ethernet (PoE)-capable embedded platform.
- A UDP-based protocol to convey the scan options and data, allowing the boards to be fully configured via the network from a central server.
- A graphical interface for use with the server to allow the user to easily change the sensors nodes' settings and display information collected by the nodes.

Chapter 3

Methodology

This chapter presents how we achieve the thesis project's goal, including the equipment, the methods, and the tools that we have used to carry out our experiments.

3.1 Objectives

As it was stated in section 1.2, our goal is to use a number of specialized microcontroller based low-cost white space sensors to measure the spectrum occupancy using the energy detection principle, in a specific range of frequencies, at a certain location, and during a period of time, to evaluate the efficiency of radio channels use and to find current and probable future white spaces.

While CR devices can take advantage of spectrum white spaces, they need to perform many tasks and they can also exploit cooperative decision making based upon communication with other sensing devices in order to exploit multiple measurements so that they can make a more accurate assessment of the channel's occupancy. Therefore, in this project we are going to use a grid of specialized microcontroller platforms that are going to send frequency scanning data via an Ethernet cable to a server which will collect this data. With this data we will be able to compute the statistics of each channel of the specific range of frequencies that are being measured. In future work, with a greater number of white space sensors at different locations and a server with software that automatically extracts occupancy decisions the CR devices can reduce their complexity (and energy consumption) as they need only query a server a geospatial database of available spectrum that CRs can use in their location (see section 2.4.2).

An individual sensor device is not able by itself to make a reliable detection of primary users due to shadowing and multipath effects and cannot detect hidden receivers. Hence, a cooperative system is the key to reducing the probability of a false white space decision. In the experiments reported here our grid is formed by 4 sensors (as shown in Figure 3.1).

The measurements of spectrum occupancy not only can reveal spectrum utilization to help CRs to find white space, but can also provide information that could be used to modify current allocation policies or when making new allocations. For example, in some countries (such as Finland) licensed by unused spectrum is returned to the regulators.

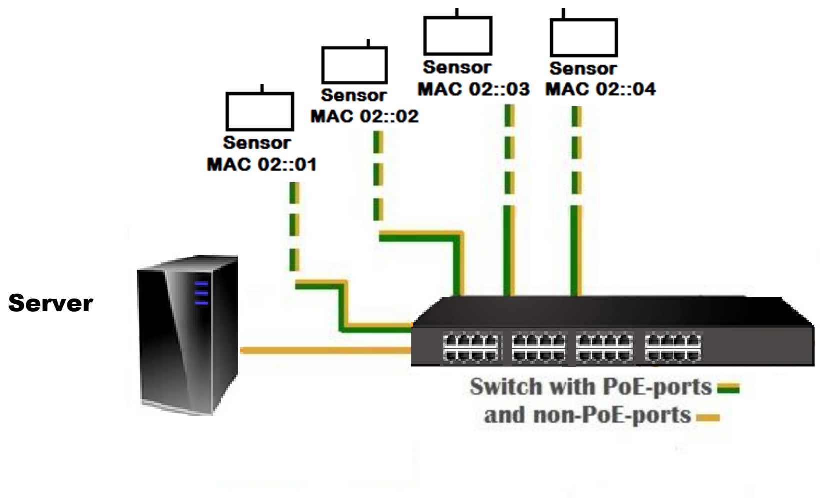


Figure 3.1 Grid of spectrum sensors

The objectives that need to be achieved to reach our goal are:

- We are going to use of a sensor platform developed in a previous degree project by Albert López and Francisco Javier Sánchez [34]. This platform was designed to be powered by a DC power supply or by PoE. However, their prototype has a problem with its PoE implementation, making that the platform can be powered only by a DC power supply. Since we want to use only the Ethernet cable to provide both power and communication, we needed to fix the PoE subsystem of the platform.

- Once we have the PoE part of the prototype working perfectly, we need to implement multiple platforms to realize a grid of sensors. In this case, we created three more instances of this platform, and assigned the four devices the following MAC addresses: 02:00:00:00:00:01; 02:00:00:00:00:02; 02:00:00:00:00:03; 02:00:00:00:00:04. Note that the leading byte of 02 means that these are locally administered MAC address and they are not guaranteed to be unique.

- We need to program the sensors to collect the information about the local radio environment and send it to the server. For this we are going to use the software developed in a previous master's thesis project by Javier Lara Peinado [33].

- Now that we are able to program and control these platforms we measure how much power the platforms need for sensing the environment and deliver their data.

- We will conduct a measurement campaign in order to do our experiment, and then we will analyze the results of these measurements.

3.2 Measurement scheme

Spectrum measurements require simple, practical, and efficient methods, and thus, it is necessary to devise a reasonable scheme for these measurements based on the objectives of the project. As part of this measurement scheme we have to consider the measurement equipment; the measurement methods and parameters; and measurement locations. We will describe each of these in turn in the following subsections.

3.2.1 Measurement equipment

The equipment and tools used in this project are: the platform of [34], the software of [33], a switch with PoE ports HP procurve 2626-pwr J8164A [35], a DELL OPTIPLEX GX620 computer, CAT5 Ethernet cables, a HP8922M GSM tester [36], and a HP8591A spectrum analyzer.

3.2.1.1 Hardware

The design of the platform used as spectrum sensor was developed as a gateway for sniffing wireless sensor traffic from existing sensors in the 868MHz band [34]. All the chips that have been used in the implementation of this platform are low-power chips. The platform is divided into a motherboard and a plug-in RF daughterboard, providing flexibility as another alternative daughterboard can be designed and constructed then connected to the serial interface to the microprocessor. The RF daughterboard could include several radio transceivers (or just receivers) enabling the device to both change the frequency range which it is going to scan and to increase the range of frequencies over which it can scan. Additionally, due to the simple serial connection, a motherboard can be designed to have multiple daughterboards connected, each one with a different radio transceiver (or receiver).

3.2.1.1.1 Motherboard

The motherboard (main board) incorporates the powering circuitry, the microcontroller unit (MCU), Ethernet controller, interface to the RF daughter card, and a simple user interface. Figure 3.2 illustrates the motherboard with its main components labeled. The most important features of these components are explained below.

- *Powering circuitry*

The motherboard can be powered via PoE since all of the chips that have been used are low-power chips. The energy required from the PSE is signaled by the Texas Instruments (TI) TPS2375 [37]. This is a controller chip which contains all the features needed to envelop an IEEE 802.3af [22] compliant PD (see section 2.2.2). The actual Rclass value of this motherboard is for a class 1 PD. The board can be also powered by a DC auxiliary port connected to an external DC power supply. The external DC supply can be any DC voltage greater than 3.3V and up to 60V. Typical AC to DC converters are 5V, 9V, or 12V. An external DC power supply can be used if a PSE is not available. The user can select between the two power options by changing the position of the two jumpers indicated in Figure 3.2 (a) as *Charger/PoE switch*.

The voltage regulator circuit has a TL2575HV step-down converter [38], a chip that converts the DC voltage supplied to the board to 3.3V.

- *Ethernet controller*

The Microchip ENC28J60 [39] was chosen because of its serial peripheral interface (SPI) which is used to communicate with the MCU. This chip is in charge of the actual transmission and reception of Ethernet frames and stores incoming frames from SPI and the Ethernet port in its 8kB transmit/receive buffer. ENC28J60 handles all the Ethernet layer functions and automatically encapsulates the IP packets received from the MCU via SPI into Ethernet frames. This chip lacks a factory-defined unique Medium Access Control (MAC) address hence, for our prototype we manually assigned local MAC address to each of the nodes (as described in section 3.1).

- *MCU*

A Texas Instruments MSP430 family microcontroller is the core of the platform. This microcontroller provides five low-power modes optimizing its energy consumption by activating only those modules required at each moment.

This chip has only 4kB of Static Random Access Memory (SRAM) but has 256kB of flash memory, which means that we are able to store a large amount of code but we must be very careful with this code's use of Random Access Memory (RAM). For this reason the 8kB buffer of the Microchip ENC28J60 is very useful.

For the platform are needed two independent SPI buses to connect: between the microcontroller and the radio transceiver; and between the microcontroller and the Ethernet controller. For this reason the MSP430F5437A [40] was chosen. Two programming interfaces are needed: Bootstrap Loader (BSL) and Joint Test Action Group (JTAG). However, only a JTAG connector was included on the board, hence the boot loader code is initially loaded via this JTAG connection as explained in [33].

The MCU together with the Microchip ENC28J60 implements a UDP/IP stack that provides the necessary networking function, and the processor will configure the radio chip(s) via the SPI based upon messages received via the network.

- *User interface*

For communication between the user and the hardware platform, there are two buttons and four light-emitting diodes (LEDs). One button is programmed to reset the MCU. Two of the LEDs are not user programmable, specifically a green LED turns on when the board is powered over the Ethernet and a red LED turns on when the board is powered by an external DC supply. The two LEDs (one yellow and one green) located between the two buttons are user programmable and they will blink when the networking module is working, i.e. when the board starts to deliver packets to the server with RSSI measurements.

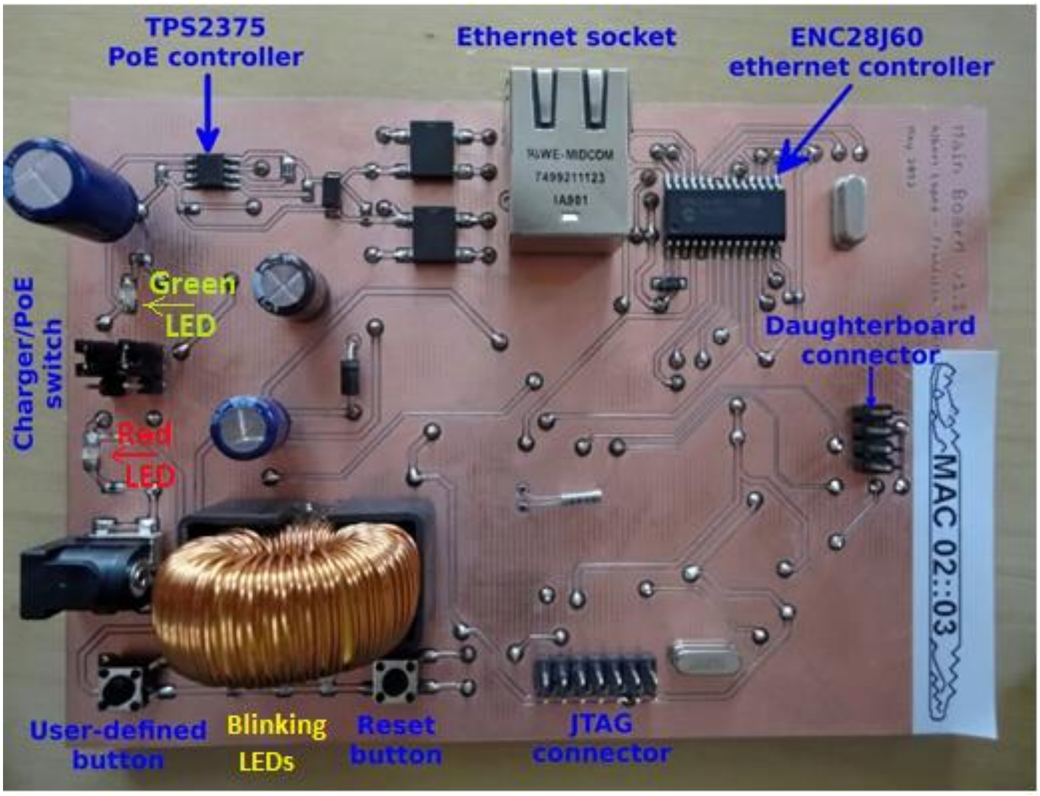


Figure 3.2 (a) Front of the motherboard

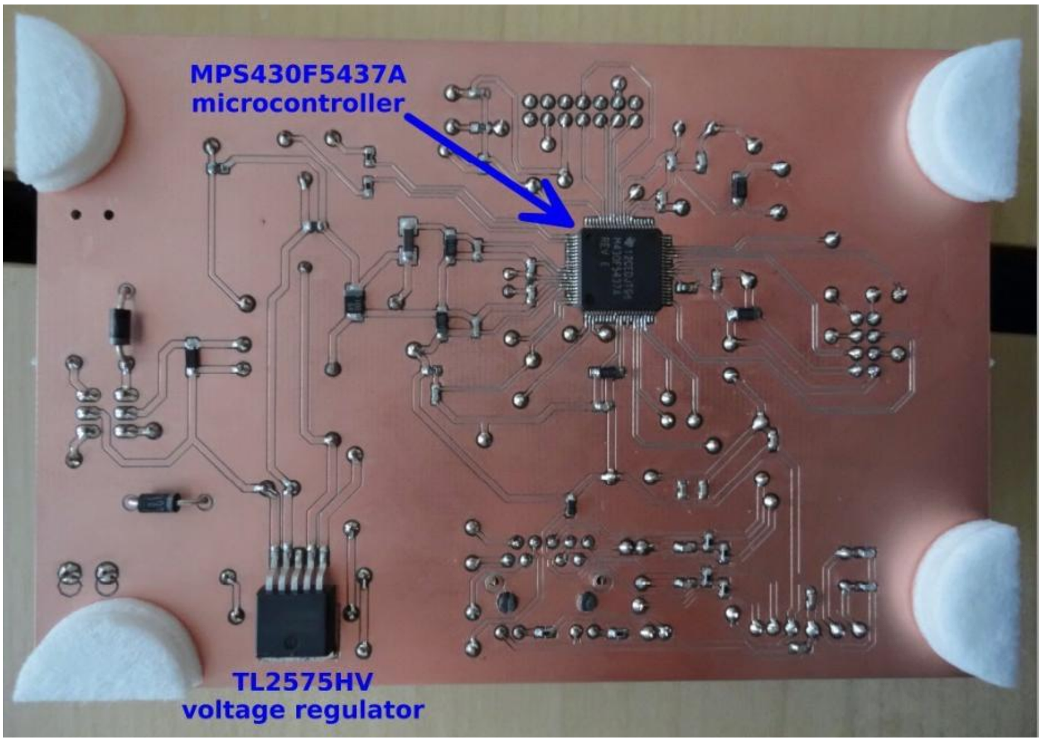


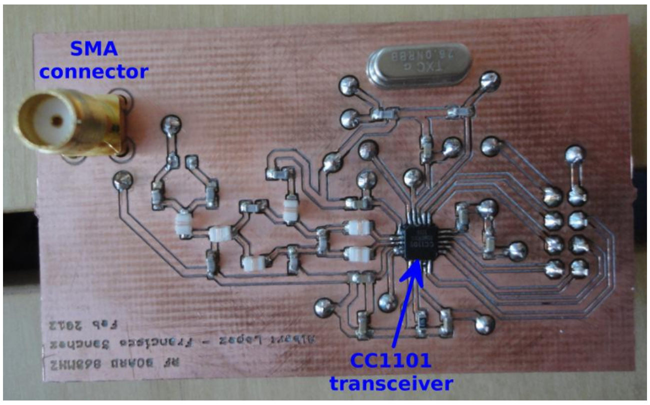
Figure 3.2 (b) Back of the motherboard

3.2.1.1.2 RF daughterboard

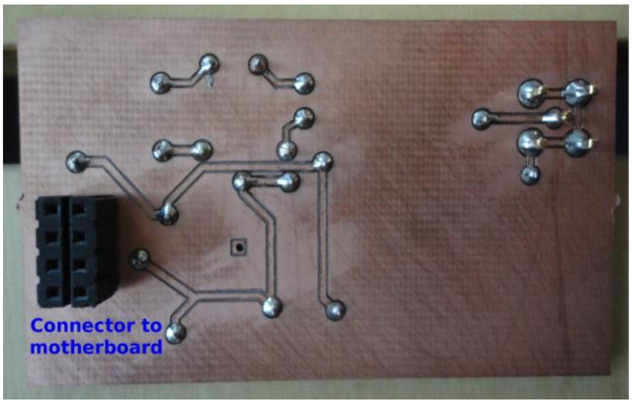
Figure 3.3 illustrates the daughterboard. This daughterboard contains all the radio related components: The transceiver (although in our case it is only used as a receiver), a passive LC filter, and a SubMiniature version A (SMA) socket for the antenna.

The transceiver of the daughterboard is the Texas Instrument C1101 [41]. This chip was selected because it has high receiver sensitivity, supports high data rates, and can work with several types of modulation. This chip can operate in the 300-348MHz, 387- 464MHz, and 779-928MHz frequency ranges, but the filter circuitry of the board is optimized for scanning frequencies in the 779-928MHz range.

As was said before, the daughterboard is connected with the motherboard through a standard SPI, and the connector for this is visible in the Figure 3.3 (b). Scanning a wider frequency range than channel width offered by this transceiver requires changing the radio channel. Due to the fact that we sequentially scan a number of frequency channels it is possible to miss short transmissions that are in a frequency range that is not currently being scanned. We average multiple RSSI values for each frequency channel to increase the accuracy of our measurements. As noted earlier we can change to another RF daughterboard in order to scan a different frequency range or we could utilize multiple daughterboard to different scan ranges at the same time.



(a) Front



(b) Back

Figure 3.3 RF daughterboard

3.2.1.1.3 Final look of the spectrum sensor

Figure 3.4 shows the final platform with an antenna.

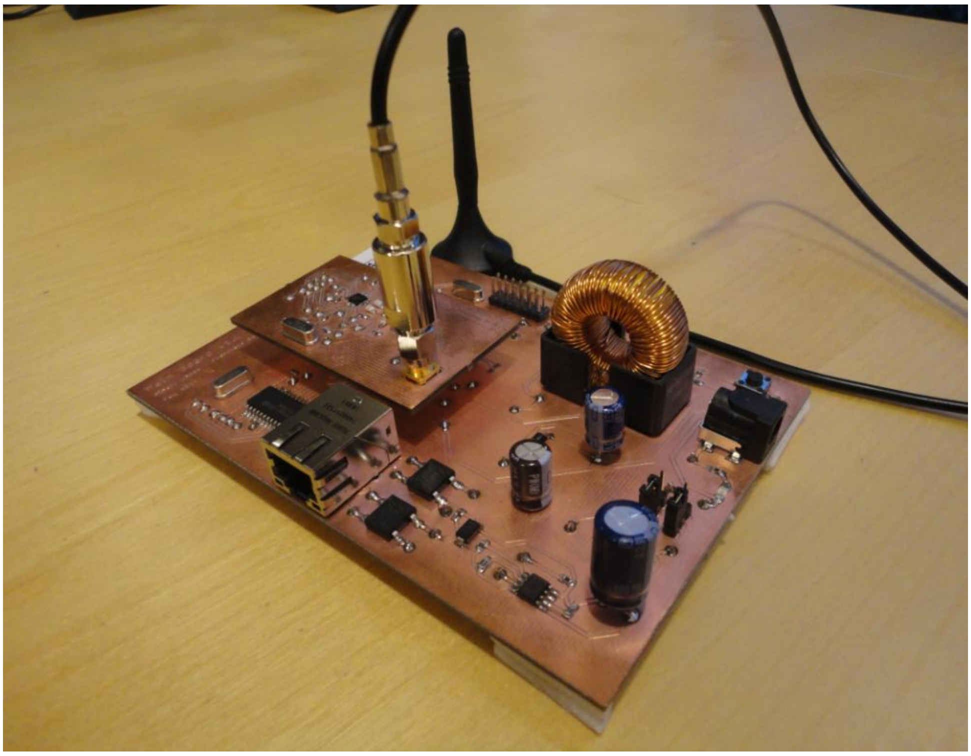


Figure 3.4 Platform with antenna

The antenna used for this project is Smarteq's Minimag 1140.30SMA model [42]. This antenna is designed to operate in 824-960 MHz and 1710-2170 MHz frequency ranges, suiting the first range of frequencies which we are going to scan with our transceiver. This antenna is connected to the RF daughterboard with a SMA connector.

3.2.1.1.4 Fixing the PoE power section of the board

As was mention in our objectives (in section 3.1), the prototype board worked properly with and external DC supply but the PoE subsystem had a problem that we needed to fix. When we first powered the platform by PoE, the green LED of the board and the LED of the PoE injector were on for several milliseconds and then the power supplied was cut off. This meant that the board was detected as a PD by the injector (the detection phase takes 500 ms) and maybe the PD was classified, but something was rejecting the power. In this section we are going to explain the process we followed until we found a solution to this problem, achieving that the platform obtains all the power it needs only through the Ethernet cable.

- The first test we conducted was to exclude the problem being caused by the voltage regulator (TL2575HV). Therefore, we injected power with the desired voltage with a laboratory power source directly at output side of the PoE section as Figure 3.5 shows. The result was that independent of the voltage we injected, at the output of the voltage regulator we had 3.3V.

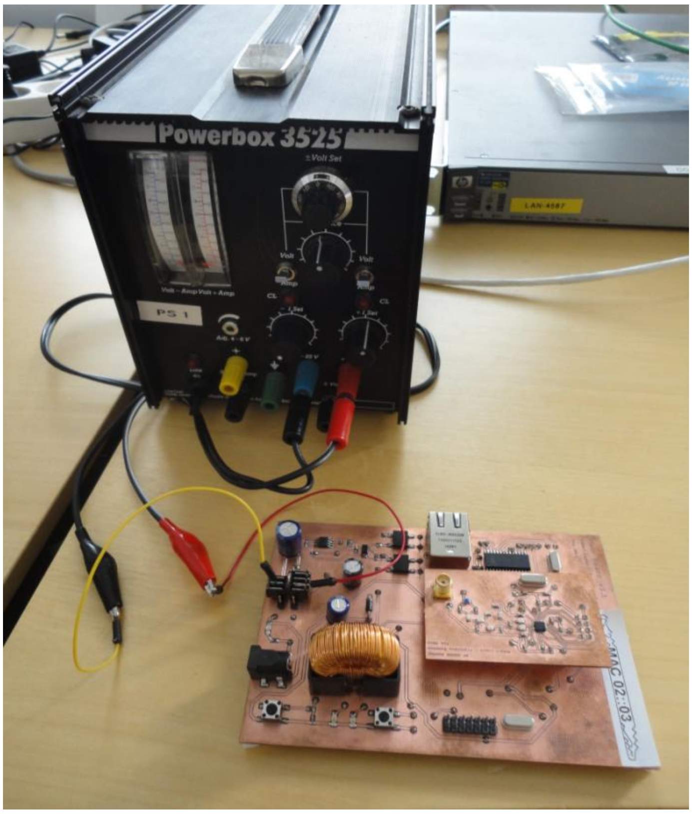


Figure 3.5 Testing the voltage regulator

○ After excluding the voltage regulator as the source of the problem, we decided to change the classification resistor (Rclass), whose functionality was explained in section 2.2.2. Table 3.1 shows the classification table of the TPS2375.

Table 3.1 Classification TPS2375

CLASS	PD POWER (W)	$R_{(CLASS)}$ (Ω)	802.3af LIMITS (mA)	NOTE
0	0.44 – 12.95	4420 ±1%	0 - 4	Default class
1	0.44 – 3.84	953 ±1%	9 - 12	
2	3.84 – 6.49	549 ±1%	17 - 20	
3	6.49 – 12.95	357 ±1%	26 - 30	
4	-	255 ±1%	36 - 44	Reserved for future use

The board had an R_{class} resistor with a value of 953Ω, i.e. class 1 (lowest maximum PD power), and we changed this to 4420Ω resistor, i.e. class 0, thus the power supplied by the switch would be greater. Nothing changed and we switch it again to 953Ω after realizing that the amount of power supplied was not the problem.

○ We thought that perhaps the reason for the problem was that the board was consuming very little energy and the PSE was interrupting the energy supplied. We decided to put a resistor between the GND ports of PoE as Figure 3.6 shows, and with the resistors of values of 680Ω, 750Ω, and 820Ω, the programmable LEDs (highlighted by the large blue arrow in the figure) were flashing and the board was working. In this figure one can also see the green LED indicating that the board is getting power via the Ethernet. (The extra wires connected to the board and from the black wire running across the board were in place to enable the board to be reprogrammed with the BSL interface to the MCU. Details of this are given in [33].)

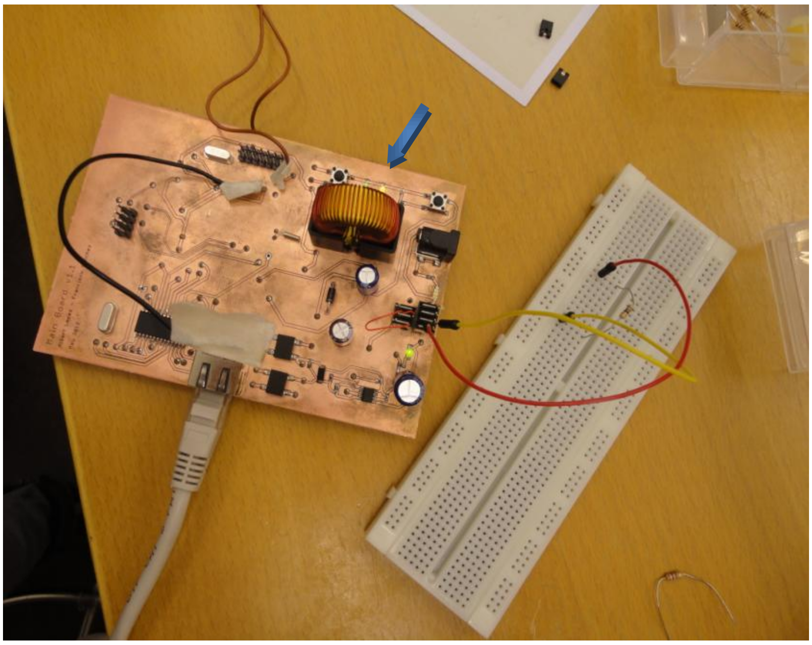


Figure 3.6 Adding a 680Ω resistor

We changed that resistor for a 680Ω resistor that could handle 10W, but the problem occurred again when we programmed the RF daughterboard with the software needed to scan frequencies, as explained in section 3.3. This program consumes more energy that previously consumed by the prototype and hence we needed more current.

- Finally we decided to change the $R_{(ILIM)}$ and this solved the problem.

The motherboard uses a TPS2375, an 8-pin integrated circuit, to realize a PD fulfilling the IEEE 802.3af standard as was explained in 2.2.2. Basically, the TPS2375 is a PD controller. This controller has an adjustable inrush limiting feature. Its data sheet [37] indicates that for setting the start-up inrush current limit, we need to connect a resistor from ILIM (pin 1) to VSS (pin 4). The value of the resistor is given by the equation $\{I_{(LIM)} = 25000 / R_{(ILIM)}\}$ where $I_{(LIM)}$ is the desired inrush current value (in Amps) and $R_{(ILIM)}$ is the value of the resistor (in Ohms).

As the board can also be powered by an auxiliary port we were able to measure with a digital multimeter the current required by the board when operating, and this value was under 200mA.

The problem was that the original board had a $R_{(ILIM)}$ with a value of 442kΩ resulting in a very small inrush current limit: $\{I_{(LIM)} = 25000 / 442k\Omega = 56.56\ mA\}$ and the board did not have enough current to operate in our scanning mode. Thereby, changing that resistor for another more appropriate valued resistor, the problem would be solved.

The TPS2375 datasheet says that the practical limits on $R_{(ILIM)}$ are 62.5kΩ to 500kΩ and as we wanted to increase the inrush current limitation, the new value for the $R_{(ILIM)}$ had to be smaller than the previous resistor. We changed the 442kΩ resistor for the most similar resistor to 62.5kΩ that was available in the laboratory, and the new resistor was 68kΩ. The board now has a higher current limit and works without problems: $\{ I_{(LIM)} = 25000 / 68k\Omega = 367\ mA \}$

Figure 3.7 indicates the part of the schematic where the $R_{(ILIM)}$ is (with the new resistor value) and Figure 3.8 shows where this resistor is located on the circuit board.

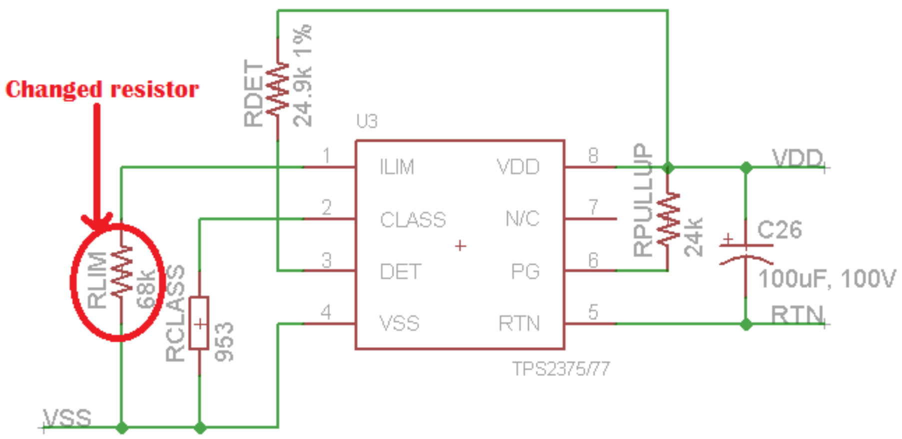


Figure 3.7 TPS2375 scheme part with the changed resistor

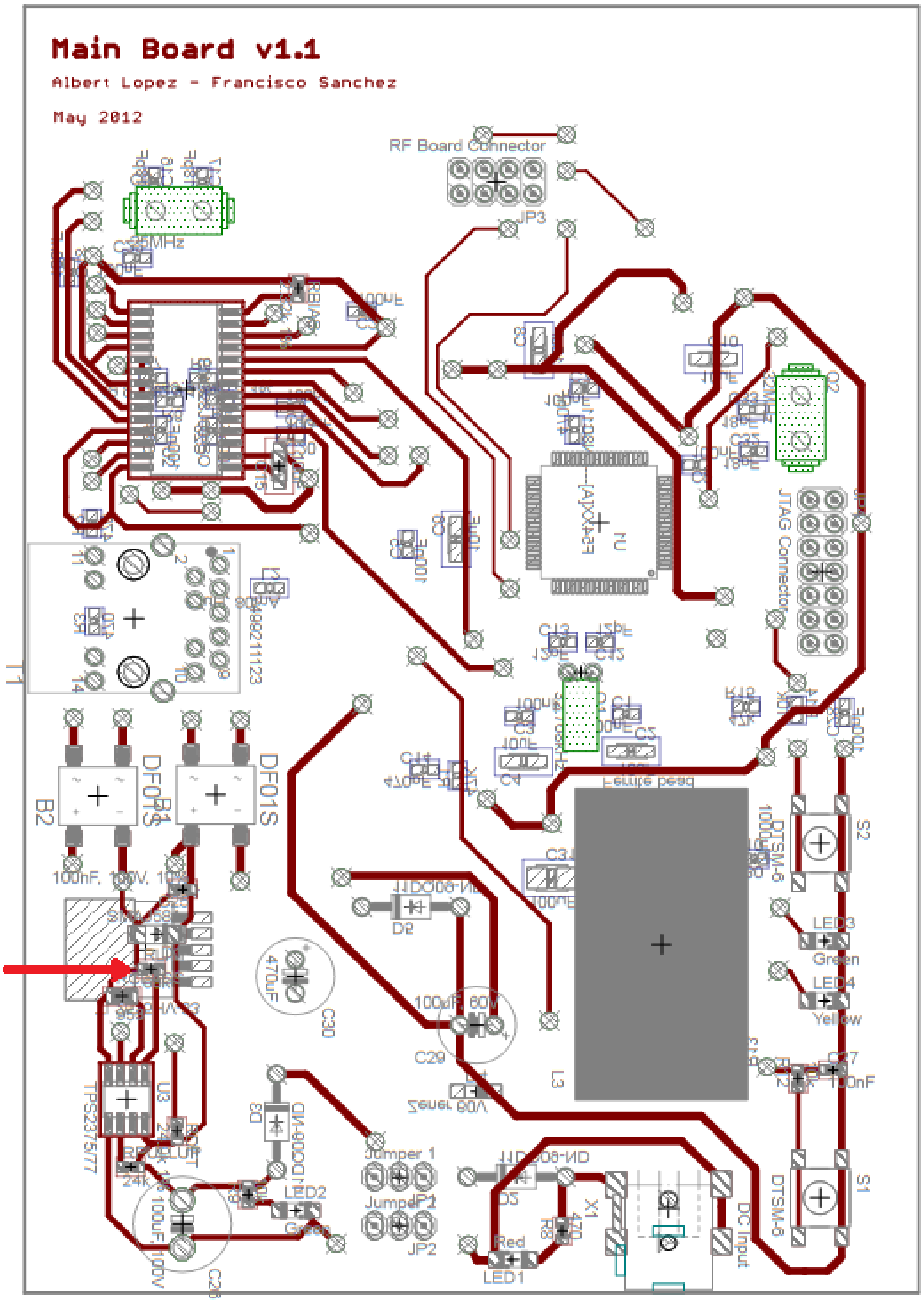


Figure 3.8 Changed resistor on the circuit board

3.2.1.1.5 Calibration of the RF daughterboard

In order to make accurate measurements, we calibrated the CC1101 radio used on the daughterboard for our spectrum sensing. For this purpose, we connected a 3 dB power divider to the output of the HP8922M GSM tester [36], where one side will be connected via a coaxial cable with Bayonet Neill-Concelman (BNC) connectors directly connected to a HP8591A spectrum analyzer, and the other side is connected with another coaxial cable (BNC-SMA) to the SMA connector of the daughterboard, as shown in Figure 3.9. The signals received by both devices (spectrum analyzer and board) should be the same signal, and should be the same signal generated by the GSM tester, but attenuated by 3dB due to the power divider. We compared both signals to see the offset in each frequency by displaying the signal received by the daughterboard using the GUI.

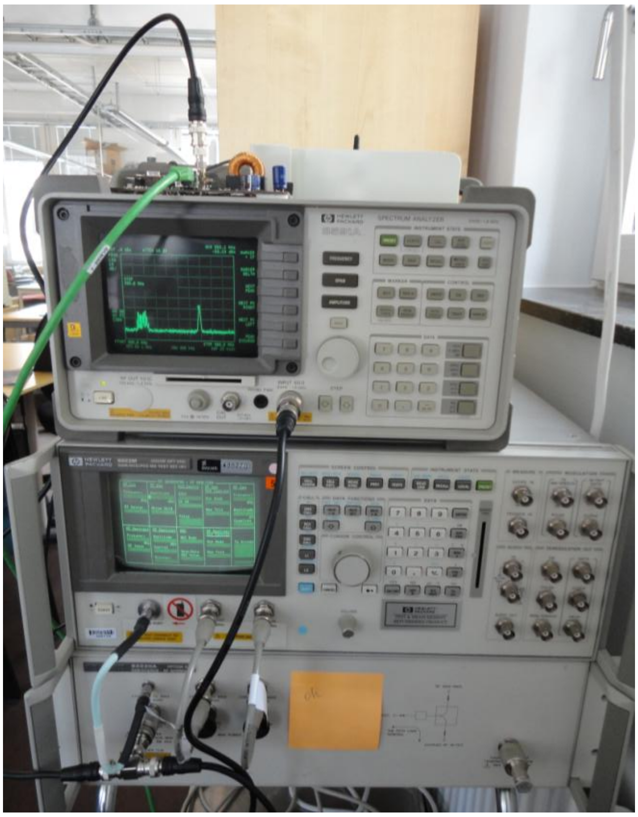


Figure 3.9 Equipment for calibration

Figure 3.10 shows the values output by the daughterboard when the input is a -50dBm signal (from the GSM tester). When making this measurement, we were generating a sine wave of a frequency from 779 MHz to 928 every 5 MHz. The results for the other 3 nodes were similar. We can take this set of measurements into account to adjust the offset in the RSSI when we want to know the actual power level (in dBm).

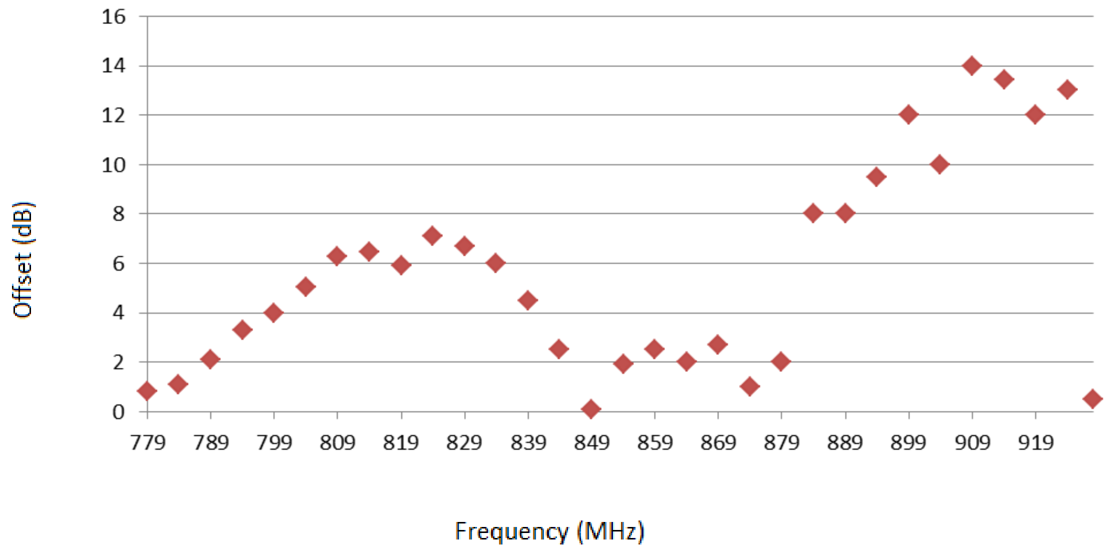


Figure 3.10 Results of the calibration measurements as seen by the daughterboard's RSSI values

3.2.1.1.6 Measurement of the energy consumed by the sensor

Once the platforms have been programmed, we wanted to measure how much power is needed by the sensor platform to perform all its functions. We assumed that the faster the scanning rate through the desired frequency band the greater the energy needed by the board, and the greater the number of packets that need to be sent to the server the greater the power needed by the board. In order to make this measurement we included in the path between the PoE controller and the input to the DC to DC converter a resistor of as low a value as we could get, as shown figure 3.11. In this case we used a 0.4Ω resistor which can support 10W and has a 5% tolerance. As we changed the scanning rate and other parameters via the GUI we were surprised that the sensor platform always needed the same low amount of energy to work, our measurements showed that the voltage drop across this resistor was between 8.8mV and 9mV, leading to an estimate of 22mA to 22.5mA of current was flowing. If the voltage at the input to this 0.4 Ohm resistor is 48V – thus the power consumption is ~ 1W.

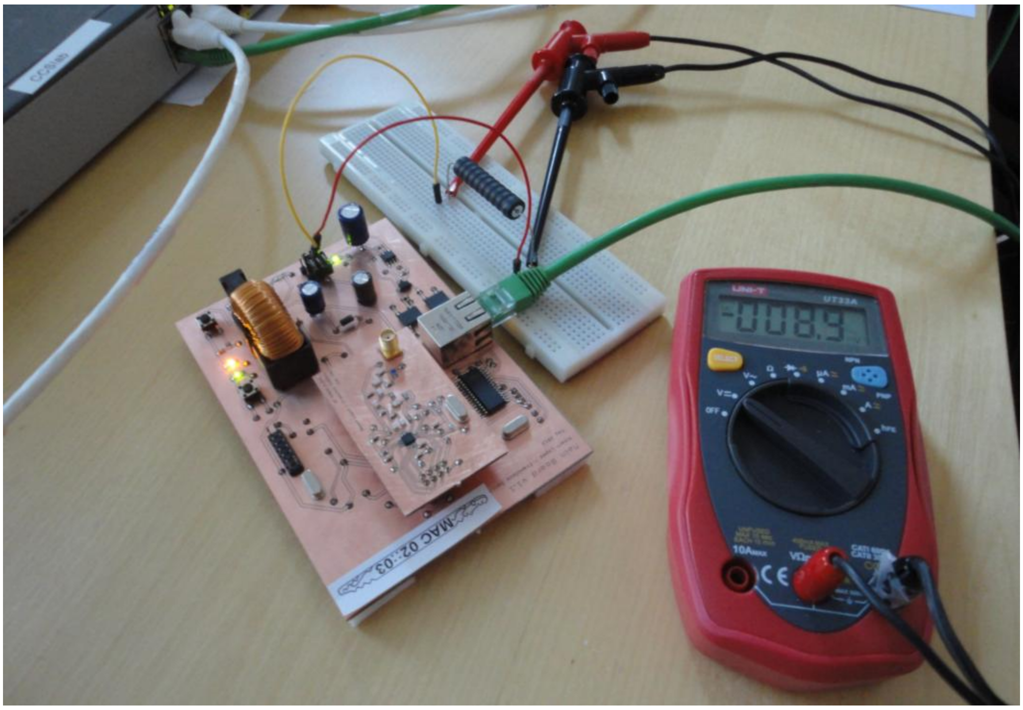


Figure 3.11 Measurement of the energy consumed by one sensor node

Whether we powered the board via a PSE (using a power injector), a PoE switch, or an external DC power supply the sensor platform took exactly the same amount of power.

3.2.1.2 Software

The software required for fulfilling the objectives of this thesis are described in detail in the master's thesis project of Javier Lara Peinado [33].

For the spectrum sensing grid experiment, we have changed the code in the backend server developed by Javier Lara Peinado to automatically save the data of each day into different HDF5 files.

To simplify the monitoring of the grid, we modified the GUI to allow the user to change the scanning options and to display the current scan data. This GUI shows the sensor nodes that are connected to the grid with their respective IP and MAC address, and whether they are active or inactive (as shown in Figure 3.12). The user can change the plot of the current scan data for the desired node just by clicking on the name of the node. The information displayed is extracted from the HDF5 file.

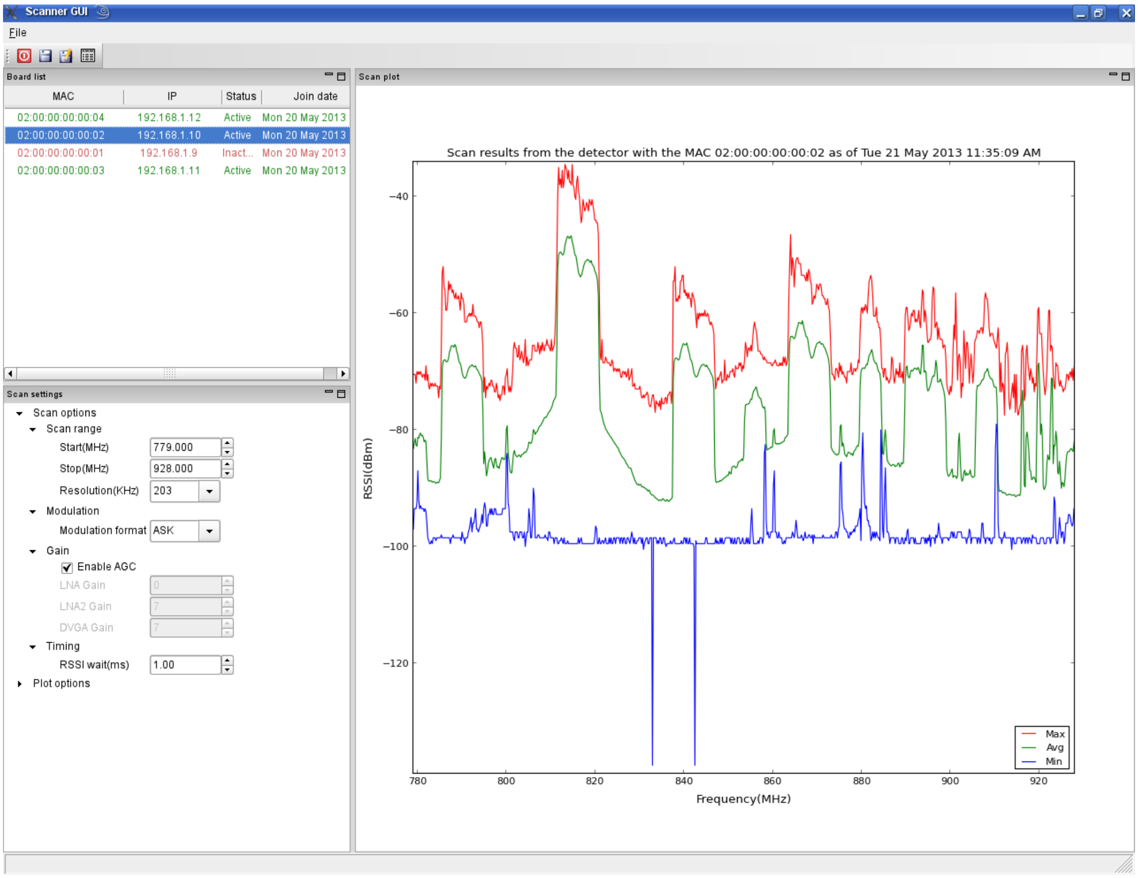


Figure 3.12 Capture of the grid GUI with four sensors connected

3.2.2 Measurement method

The spectrum sensing is based on energy detection of the transmitter, using cooperative detection in a centralized way. As we explained in section 2.1.7.1, energy detection is a simple and general sensing method based upon the received signal strength indicator (RSSI). In our case we measure this RSSI value using low-cost hardware. When the noise power is high compared with the signal power or has large fluctuations, this method does not yield a satisfactory measurement result. This means that we cannot easily detect signals below the noise floor or signals that rapidly appear above and then disappear below the noise floor.

By using a grid of sensors, we aim to avoid some problems due to shadowing, multipath fading, and hidden terminals. The multiple sensors operate in a cooperative detection scheme with a centralized database into which each of our sensors is going to deposit its data.

3.2.3 Measurement Parameters

The parameters chosen for our measurements are described below:

- *Frequency range of measurement*

Although the antenna we use is designed to operate in 824-960 MHz, the RF daughterboard is optimized to scan frequencies from 779 MHz to 928 MHz. The later frequency range is the range that we are going to scan, but for our measurements we are going to consider only the frequencies from 790 MHz to 925 MHz. We do not consider the frequencies from 779 MHz to 790 MHz and from 925 MHz to 928 MHz because both of these ranges are not an entire band according to the Swedish Post and Telecom Authority Spectrum Orientation Plan of 2012.

We did not calibrate the antenna, but we know from [33] section 4.6.2 that the propagation loss versus distance to the transmitter does not follow a logarithmic decrease, thus we assume that we have losses especially in the range from 790MHz to 824MHZ where the antenna is not efficient. This also means that the power measurements are the power detected at the receiver and not the power received at the antenna.

- *Bandwidth*

Table 3.2 shows the bandwidth of each band scanned as obtained from the Swedish Post and Telecom Authority (PTS) Spectrum Orientation Plan of 2012 [43]. This plan describes the current and planned use of these different frequency bands in Sweden, and includes the recent auction results [44]. *PTS is the government agency responsible for regulating the radio spectrum in Sweden.*

Table 3.2 Bandwidth of each band scanned as obtained from PTS

Spectrum band	Range (MHz)
Empty	790 – 791
800 MHz downlink	791 – 821
Empty	821 – 823
800 MHz center gap	823 – 832
800 MHz uplink	832 – 862
Empty	862 – 863
SRD-800	863 – 870
Licensed SRD	870 – 871
PAMR uplink	871 – 876
GSM-R uplink	876 – 880
GSM900 downlink	880 – 915
Empty	915 – 916
PAMR downlink	916 – 921
GSM-R downlink	921 – 925

❖ *Resolution Bandwidth*

We know from [32] that spectrum sweeps over large frequency ranges demand wide channel bandwidths, and in the case of the CC1101 transceiver these channel bandwidths are up to 420kHz. Possible resolutions that we can choose in our program are from 58kHz to 803kHz. The default resolution value in our program is 203kHz, thus samples are collected every 203kHz given that we think gives a reasonable solution. As a result each scan from 779MHz to 928MHz will contain 733 measurements.

❖ *Decision Threshold*

A threshold level is used to distinguish between noise and signal. This level should be set to filter out most noise. This threshold should be set as low as possible. Although a low threshold may mistake some noise for signals leading to some errors, it will capture even small signals coming from primary users. If the threshold is too high, then most channels will be declared as unoccupied most of the time, which would also be in error.

One of the International Telecommunication Union (ITU) recommendations [45] is to set the threshold 10 dB above the ambient noise. However, it is hard for us to know which this level is, thus we are going to follow the model of [9] and [6] by setting the threshold to 5-7 dB above the average noise (based on the observation of the average of the background noise), after depicting measurement results of each day corresponding to each white space sensor.

For this reason the software calculates the occupancy using the different thresholds we indicate it in different chunks of the spectrum within the range that is being scanned.

❖ *Timing*

The scanning timing of each 203kHz sample is 1ms (RSSI wait), i.e., every millisecond the sensor platform delivers information about the RSSI value at the current frequency to the server. This means that the scan of the whole frequency sweep, from 779MHz to 928MHz, with a resolution of 203kHz (733 measurements) takes less than 1 second.

❖ *Revisit Time*

When measuring the occupancies of the chosen frequency bands, enough samples should be collected to get accurate results, thus we scanned the same spectrum range with the sensors in the same location for a period of three consecutive weeks, averaging the samples of each hour of each day.

❖ *Occupancy*

The utilization of selected bands is described using a duty cycle parameter, which specifies the fraction of time the band is used, i.e. the number of samples with power levels greater than the threshold divided by the total number of samples.

3.2.4 Measurement location

We set up our sensor nodes indoors. The sensing nodes were placed for these three weeks, on the 4th floor of the Electrum building at Kista, in Stockholm. The area is surrounded by universities, many companies, a lot of shops, a commuter train station, and by base stations of many cellular operators. These base stations are mounted on this building and adjacent buildings.

Figure 3.13 shows the Electrum building and the red circle indicates the part of the building where the experiment took place. It should be noticed that the 4th floor is the 2nd floor above the ground (from the point of view of the figure).

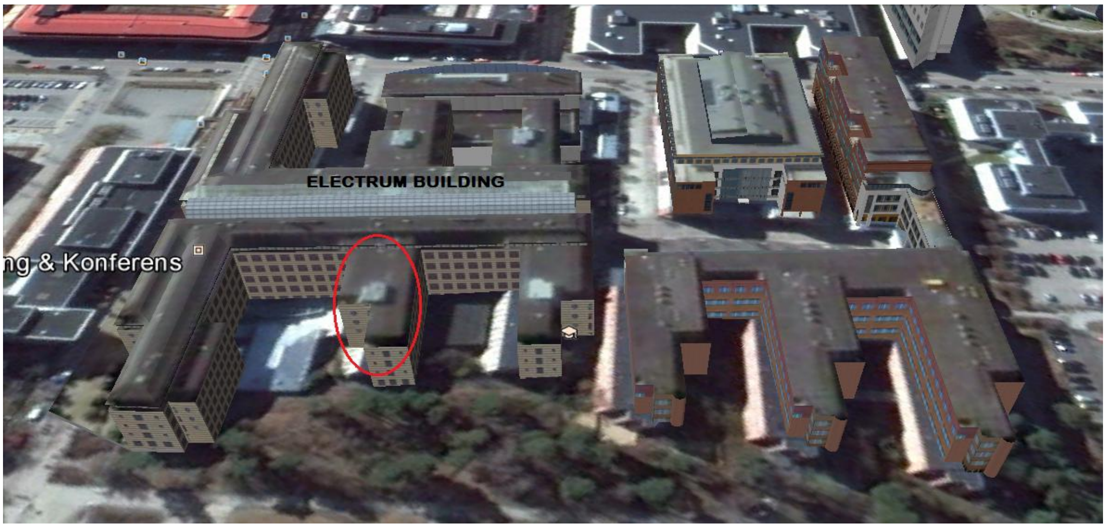


Figure 3.13 Electrum building in Google earth

Figure 3.14 shows part of the 4th floor and the squares indicate where the nodes were located.

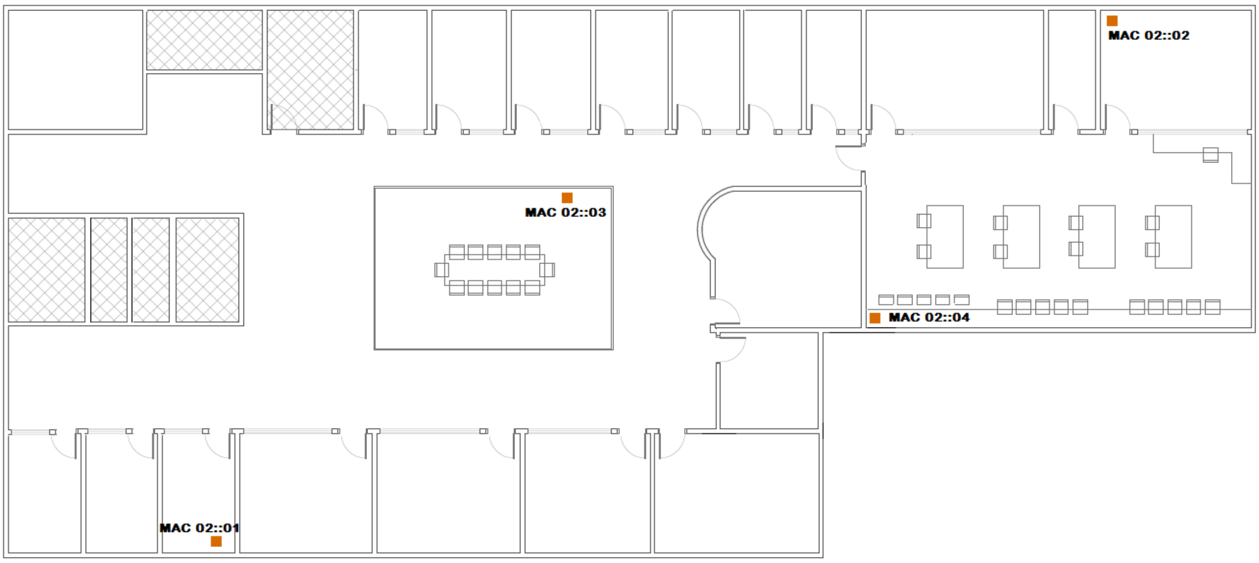


Figure 3.14 A floor plan of part of the 4th floor indicating where the sensor nodes were placed

Chapter 4

Measurement results and analysis

This chapter describes the results obtained after scanning the spectrum over the frequency range of 779MHz to 928MHz using a sensor grid with four nodes when using the energy detector method. As we stated in section 3.2.3 we are going to measure the occupancy in the frequency range of 790MHz to 925MHz. The chapter describes our analysis of this data and shows the occupancy of this spectrum at each hour of the day, on different days, and in the different locations where the nodes where situated. The result will be a cooperative assessment of the spectrum occupancy in different frequency bands as a function of the time of day and day of the week.

4.1 Measurements of one day with 4 nodes

Figure 4.1 depicts the power level (RSSI) of the measured bands (from 779MHz to 928MHz) that each node has sensed in each of four locations. This is the activity captured one Wednesday on the 4^{th} floor of Electrum building on Kista.

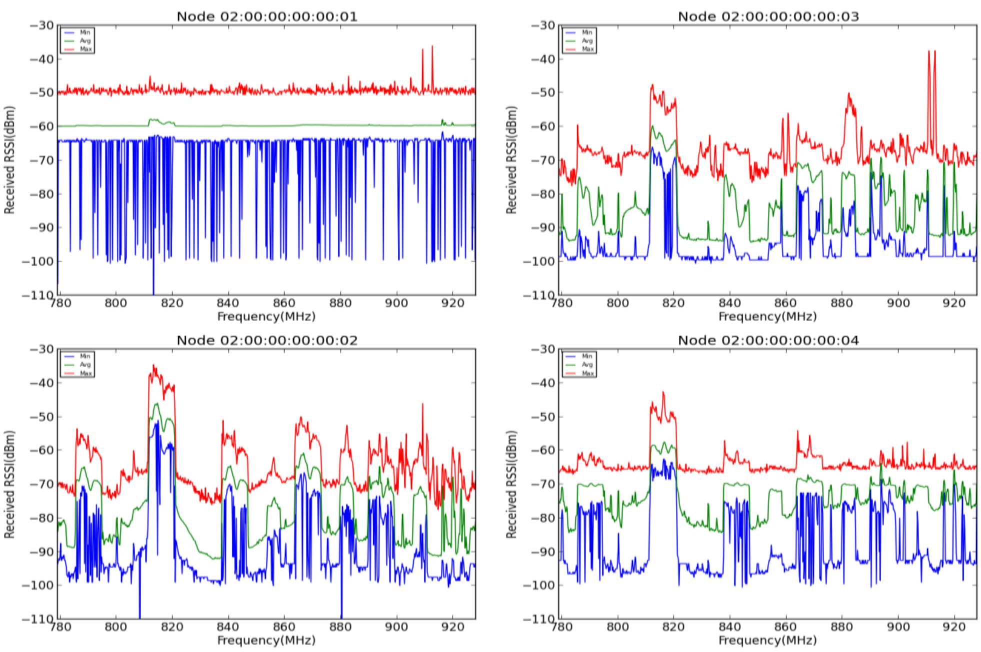


Figure 4.1 Spectrum measurements on one day with 4 nodes

After looking at this measurement data we decided that we needed to revise sensor node 02:00:00:00:00:01 as its measurements were not consistent with the other nodes. This platform was the original node (i.e., the oldest of the nodes and had the first RF daughterboard), but this node was located in a private office for which we did not have easy access. As a result we decided that we would simply ignore the measurements from this node.

Figure 4.2 depicts the same measurements of the same day as Figure 4.1, but showing the RSSI in each frequency as a function of time for 24-hours. On the right, is the color scale that has been used to indicate the RSSI values. In this scale, red indicates that the node is detecting a higher power level, while blue indicates that the node is not detecting anything. On the left of each plot we have the hours of the day (starting at midnight).

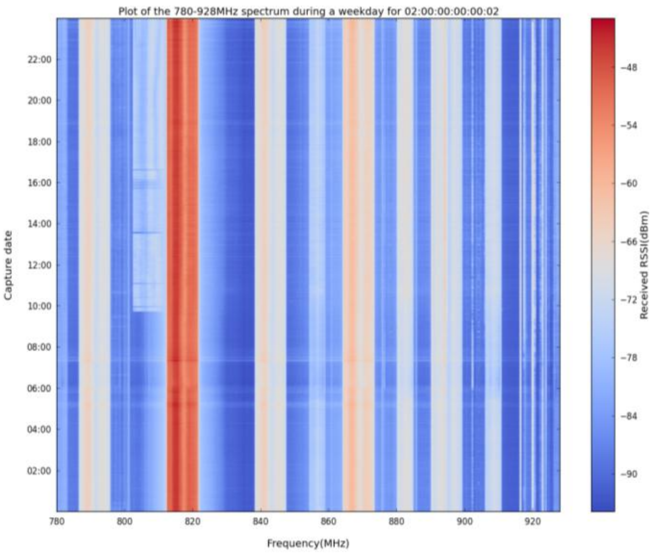


Figure 4.2 (a) Sensing spectrum with MAC 00::02

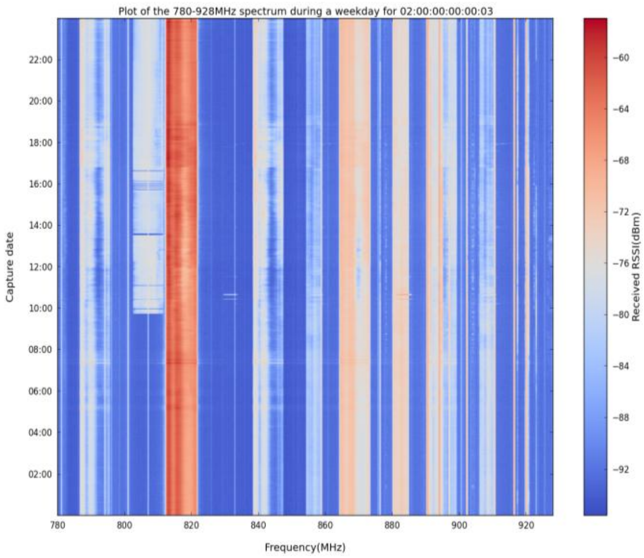


Figure 4.2 (b) Sensing spectrum with MAC 00::03

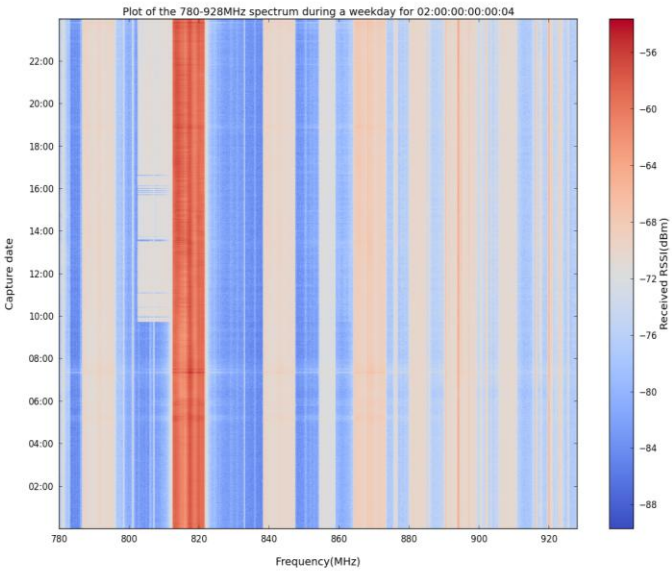


Figure 4.2 (c) Sensing spectrum with MAC 00::04

4.1.1 Spectrum occupancy in terms of situation

Observing the three measurements made by the nodes with MAC address 02::02, 02::03, and 02::04 (situated in the locations shown in Figure 3.14) we can compare the different power levels in the same frequency bands. We observe that in some cases one node captures power in some frequencies that the other node or other nodes do not. Figure 4.3 shows an example of those differences in the frequency range from 835MHz to 848MHz that belongs to the 800MHz uplink band. This is due to the *multipath fading* or *shadowing*.

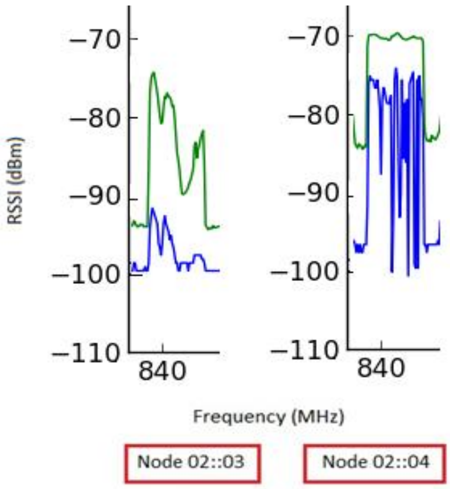


Figure 4.3 Example of different power levels detected in different frequencies based upon different locations (green is the average power level while blue is the minimum power level)

These results show that cooperative detection can give more accurate estimates of the real spectrum occupancy as if only the measurements at the location of a single node were used there are numerous cases where the decision regarding a band being unoccupied would have been in error. The problem of a *hidden listener* remains because, although each of these sensors is scanning the frequency bands at different locations, a primary receiver could be within the range of a primary transmitter while the primary transmitter is not heard by any of these sensors. This means that more complex methods are required to detect such a primary receiver. Additionally, we again note that since each node is using energy detection it cannot detect spread spectrum primary users even if we had hundreds of sensing nodes – although at some number and distribution of nodes we could detect an increase in the noise floor and identify the possible presence of spread spectrum transmitters if they were not operating continuously.

If a large number of sensors were deployed, then a server with the appropriate software to implement a database with spectrum availability information can reach more accurate conclusions based upon the different power levels in the same bands by correlating the data from different geospatial coordinates when secondary users query the server. The difference between the spectrum occupancy as sensed by node 02::02 and that sensed by node 02::04 clearly shows that if we had had sensed the spectrum with only node 02::02 we would have obtained many false positives with regard to saying that the frequency is unoccupied, i.e. we would think that many frequencies are unused when they really are used.

4.1.2 Spectrum occupancy in terms of time

In almost all bands, the power level is not constant throughout the day in the same frequency band. Zooming in on short periods of time some white spaces can be seen during certain slots of time. Since we already know that nodes 1, 2, and 3 have different spectrum sensing results, we will focus on only one sensor to examine the different utilization of the spectrum at each hour of the day. We note that node 02::04 is sensing more power than nodes 02::02 and 02::03, but there are still many chunks of blue, meaning that these bands are not being used at this time. Figure 4.4 shows the RSSI scanned with node 02::04.

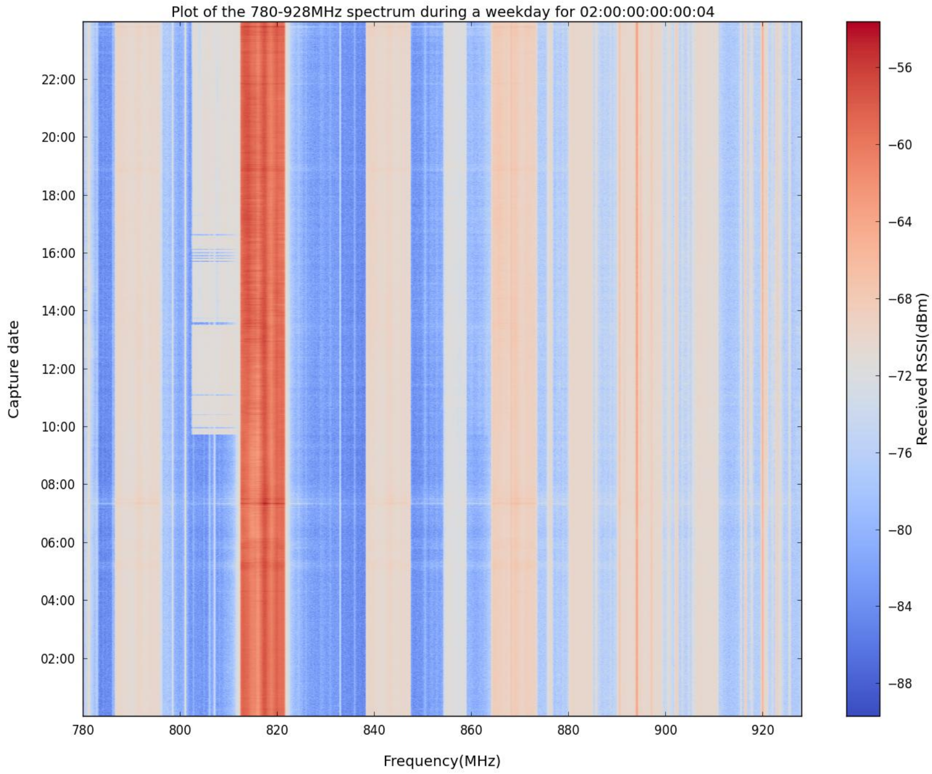


Figure 4.4 Relation between frequency and time over the course of one day as scanned by sensor node 02::04

The 800 MHz downlink band from 791MHz to 821MHz is dedicated to mobile communications. As we noted in Chapter 3, base stations for several operators are mounted on this building and adjacent buildings, hence it was expected to see a high RSSI in this frequency band. Even so, it is apparent that only the portion from 812MHz to 821MHz is efficiently used, while the rest of the frequencies in this band are not, especially the frequencies from 795MHz to 812MHz. This is a perfect example that white spaces depend not only on the location and the frequency, but also on the time of days, because from 10:00 a.m. to 00:00, the channel is more frequently occupied than from 00:00 to 10:00 a.m.

4.1.3 Spectrum occupancy in terms of frequency

Throughout this thesis we have discussed the inefficiency of the utilization of the spectrum, hence CR can take advantage of those frequencies that are unused. As can be observed in the plots of each frequency band's occupation, we see that many bands are underutilized. More specifically we make the following observations:

- As we stated in section 4.1.2, it is apparent that only the portion from 812MHz to 821MHz is efficiently used in the 800 MHz downlink band from 791MHz to 821MHZ.
- The 800 MHz center gap from 823 MHz to 832 MHz is licensed exempt, and is used for wireless microphones. In the plot we can see that nothing is sensed in this band, and it is known that no classes or conferences were given in the building during this period of time, hence it is unlikely that wireless microphones were in use. We believe that this observation of white space is accurate.
- The 800 MHz uplink band from 832 MHz to 862 MHz is reserved for communications from mobiles to the base station, and only the bands from 836 MHz to 846 MHz and from 854 MHz to 858 MHz have a higher RSSI than the value of the thresholds utilized for each node.
- The GSM900 band downlink from 880 MHz to 915 MHz is also dedicated to mobile communication. Is apparent that only the portion from 880 MHz to 885 MHz and from 890 MHz to 897.5 is efficiently used.

The easiest and the most common way to evaluate if a certain frequency band is efficiently used or not, is to calculate the duty cycle ratio. This ratio specifies the fraction of the number of samples with a power level greater than the threshold divided by the total number of samples scanned in this band. As node 02::03 observed less noise fluctuations than other nodes, we will present the channel occupancy as calculated based upon samples from this node using a threshold of -90dBm. This threshold has been chosen as the optimal value based on the observation of the average of the background noise. It should be noted that node 02::03 was the only node not surrounded by equipment as it was located in a conference room, were few meetings occurred during these three weeks. Table 4.1 shows how the entire frequency band associated with different services is used. In table 4.2 we show the calculated spectrum occupation for each portion of the band as assigned to a specific licensee.

It has to be noted that to calculate the duty cycle ratio with samples from nodes 02::04 and 02::02 there is a need to use different thresholds for different frequency bands, as the background noise level changes throughout the frequencies. To calculate the channel occupancy based upon samples from node 02::02, we set a threshold of -85dBm for all frequency bands except for the bands in the frequency range from 862MHz to 880MHz with a threshold of 80dBm. To calculate the channel occupancy based upon samples from node 02::04, we set a threshold of -75 dBm for all frequency bands except for 800 MHz band where we used a threshold of -80 dBm. It is difficult to accurately calculate the spectrum occupancy with this method in the two locations where node 02::02 and 02::04 were placed, as the background noise has many variations, and we might assume noise when in reality there is a signal or vice versa.

Table 4.1 Spectrum occupancy from 790 MHz to 925 MHz

Spectrum band	Range (MHz)	Occupancy (%)
Empty	790 – 791	52.12
800 MHz downlink	791 – 821	64.50
Empty	821 – 823	17.39
800 MHz center gap	823 – 832	4.07
800 MHz uplink	832 – 862	38.53
Empty	862 – 863	7.46
SRD-800	863 – 870	94.42
Licensed SRD	870 – 871	99.95
PAMR uplink	871 – 876	54.38
GSM-R uplink	876 – 880	18.92
GSM900 downlink	880 – 915	58.28
Empty	915 – 916	9.43
PAMR downlink	916 – 921	49.25
GSM-R downlink	921 – 925	15.49

Table 4.2 Spectrum occupancy in 800 MHz and GSM 900 bands with their associated licensee

800 MHz band	Range (MHz)	Occupancy (%)
FDD1 DL HI3G	791 – 796	55.95
FDD2 DL HI3G	796 – 801	19.38
FDD3 DL TeliaSonera	801 – 806	54.19
FDD4 DL TeliaSonera	806 – 811	62.41
FDD5 DL Net4Mobility	811 – 816	99.49
FDD6 DL Net4Mobility	816 – 821	99.99
Gap	821 – 832	6.35
FDD1 UL HI3G	832 – 837	5.95
FDD2 UL HI3G	837 – 842	86.80
FDD3 UL TeliaSonera	842 – 847	53.18
FDD4 UL TeliaSonera	847 – 852	3.17
FDD5 UL Net4Mobility	852 – 857	53.40
FDD6 UL Net4Mobility	857 – 862	31.92
GSM900 band	**Range (MHz)**	**Occupancy (%)**
DL HI3G	880 – 885	95.88
DL Swefour	885 – 890	16.18
DL Tele2	890 – 897.5	94.96
DL Telenor	897.5 – 905	43.65
DL TeliaSonera	905 – 915	45.23

We can conclude from the results of Table 4.1 that although lots of spectrum resources have been allocated only a small part of them are heavily used, other than the short range devices (SRD) bands. The SRD-800 band, from 863MHz to 870MHz, is license exempt and the spectrum occupancy of this band is about 94.42%, corroborating that unlicensed bands are getting strained while some other licensed bands are underutilized leading into room for secondary users. The Licensed SRD band is also efficiently utilized (99.95%) however, we have to notice that the range of this frequency band is the narrowest (from 870MHz to 871MHz) of the licensed bands here studied.

Table 4.2 shows the results calculated for each range of frequencies assigned to a specific licensee in the wider frequency bands. Most of the bands are occupied for only a limited period of time as we have seen before, but FDD1 uplink assigned to HI3G, and FDD4 uplink assigned to TeliaSonera are apparently unused almost all the time.

4.2 Scanning data of three weeks

We have studied the inefficiency of spectrum usage during one day, but what if we compare this Wednesday with the following Wednesdays? Figure 4.5 shows this data for three consecutive Wednesdays. There are clear patterns in almost all bands except for the bands assigned to FDD1 (791MHz-796MHz), FDD3 (801MHz-806MHz), and FDD4 (806MHz-811MHz) downlinks (where three of them show a spectrum occupancy of around 60% and 70% most of these three days). The RSSI values in the frequency bands assigned to FDD3 and FDD4 are strongly dependent each day on the time of the day. Table 4.3 shows the spectrum band occupancy in these three consecutive Wednesdays. Some of the results have been highlighted in yellow to emphasize the fact that each day most of the spectrum is available and underutilized, thus substantiating what we claimed in section 2.1, i.e., that the scarcity of radio spectrum does not exists in practice only administratively. For example, the 800MHz center gap is only utilized in a ~5% while the range of this frequency band is higher than the range of other frequency bands with higher level of occupancy. Table 4.4 shows the calculated spectrum occupancy for each channel assigned to a specific licensee. The red circles in Table 4.4 mark the different values obtained each Wednesday in the frequency bands assigned to FDD3 and FDD4, as the rest of the bands do not have big changes. After three weeks of scanning data, we can conclude that spectrum occupancy around Electrum building in kista is inefficiently used, and this means there is sharing opportunity which a CR can take advantage of.

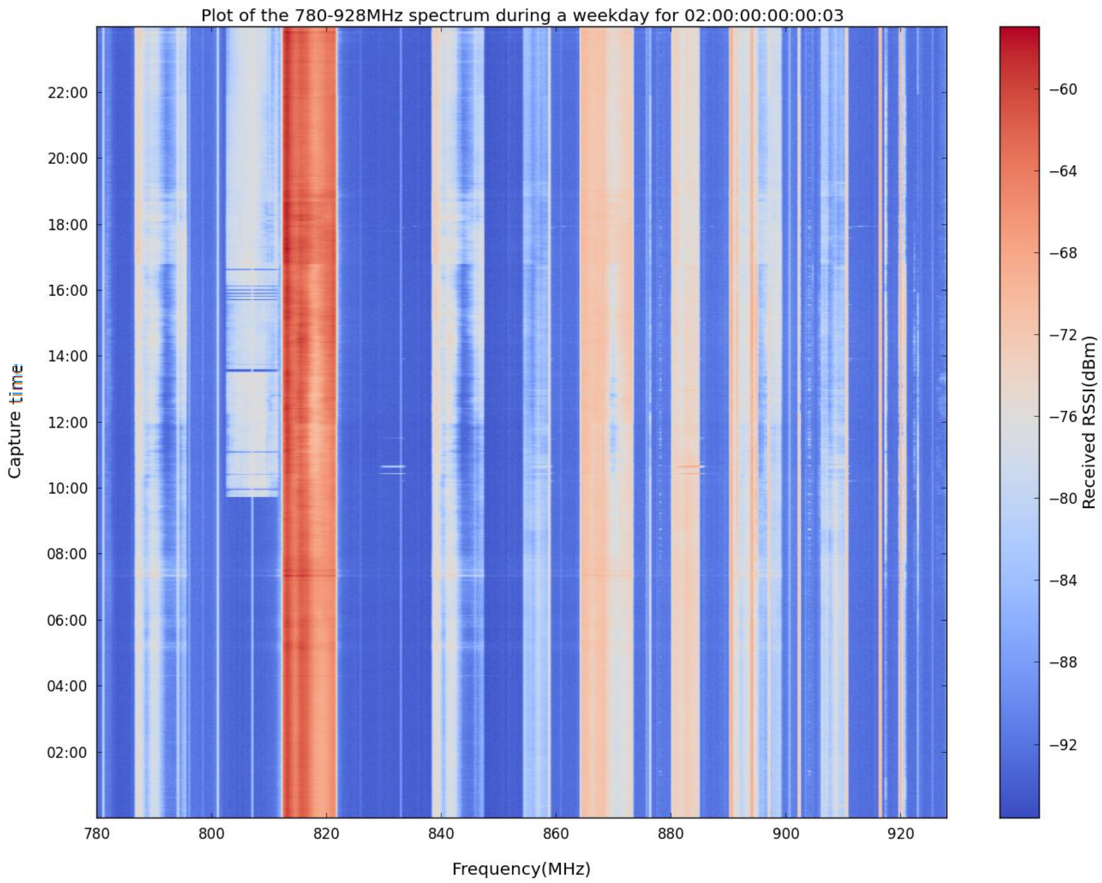


Figure 4.5 (a) Different spectrum occupancies in three weeks – first Wednesday

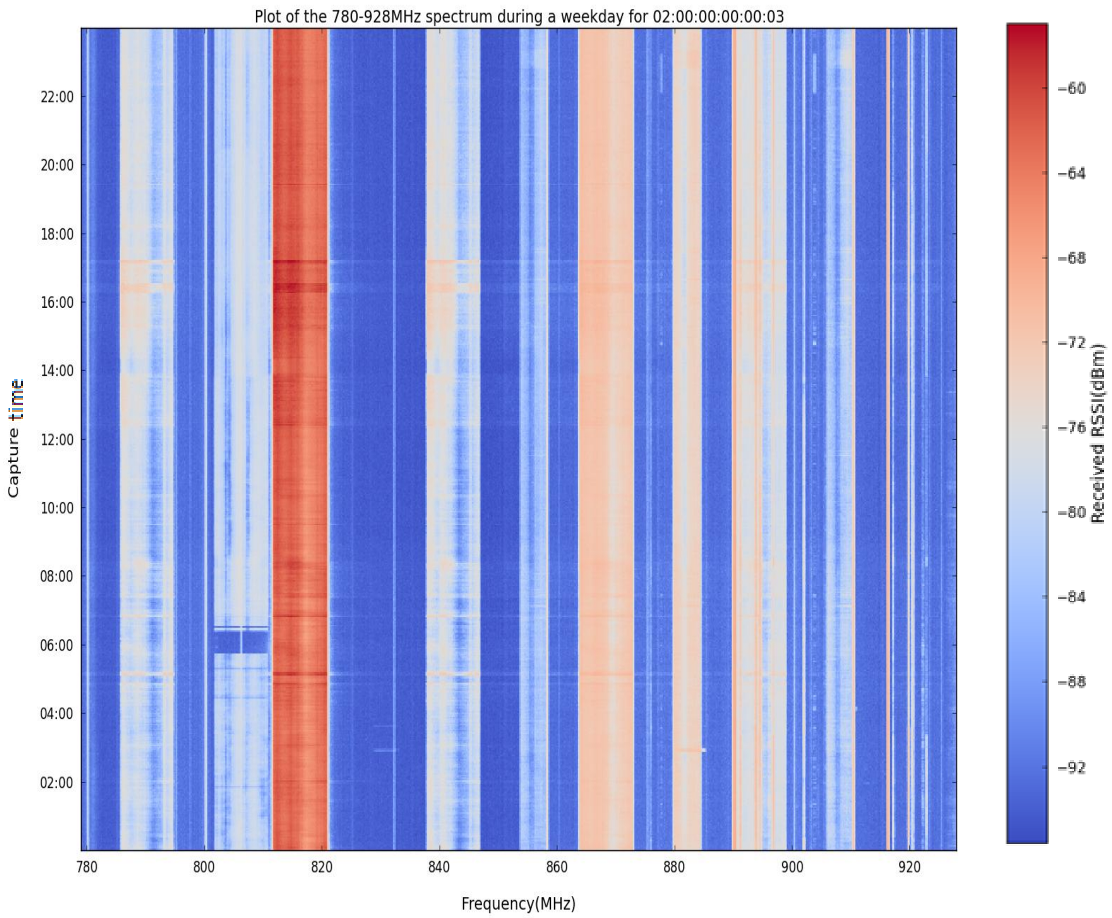


Figure 4.5 (b) Different spectrum occupancies in three weeks – second Wednesday

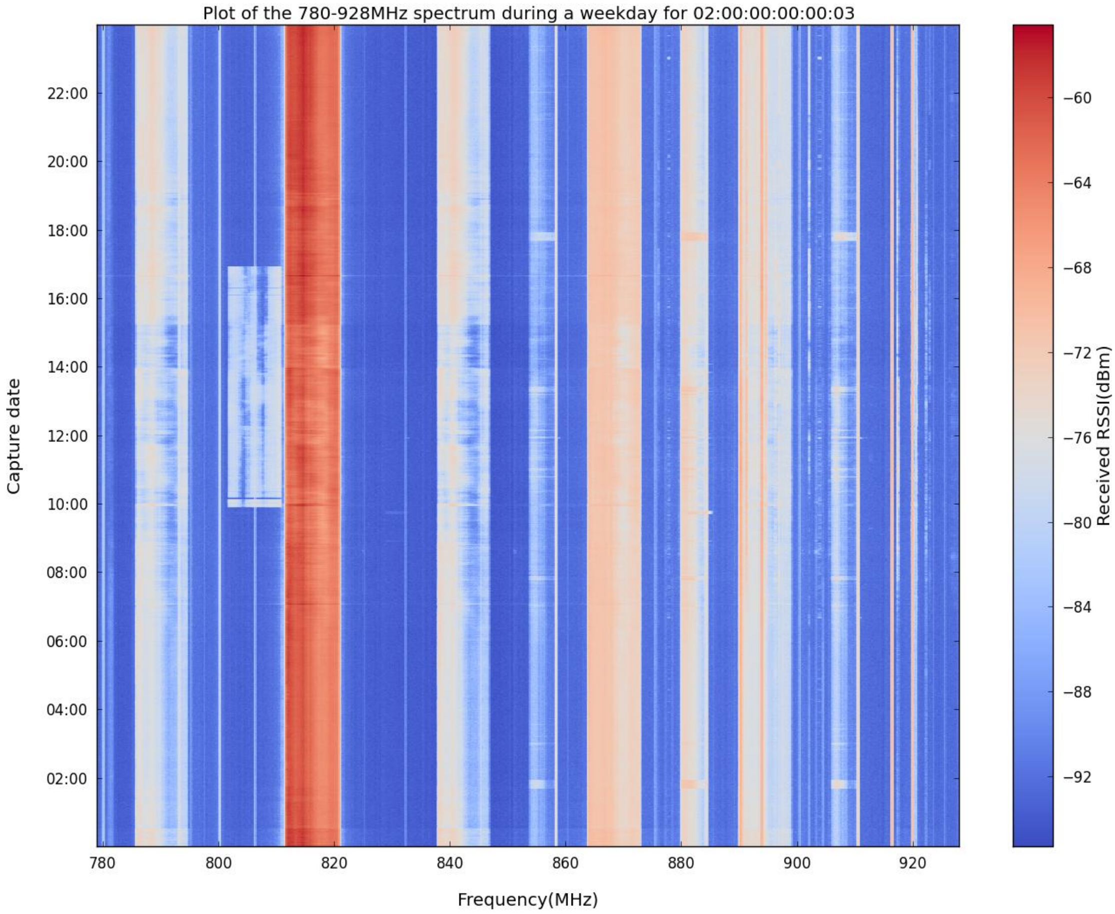


Figure 4.5 (c) Different spectrum occupancies in three weeks – third Wednesday

Table 4.3 Occupancies (%) in three weeks (yellow highlighting indicates particularly lower utilization on all three dates, specifically less than 22% utilization)

Spectrum band	Range (MHz)	Occupancy (%) 1º Wednesday	Occupancy (%) 2º Wednesday	Occupancy (%) 3º Wednesday
Empty	790 – 791	52.12	82.69	90.55
800 MHz downlink	791 – 821	64.50	77.70	58.91
Empty	821 – 823	17.39	28.57	20.20
800 MHz center gap	823 – 832	4.07	5.38	4.37
800 MHz uplink	832 – 862	38.53	44.34	40.91
Empty	862 – 863	7.46	10.81	8.63
SRD-800	863 – 870	94.42	94.70	94.62
Licensed SRD	870 – 871	99.95	100	99.99
PAMR uplink	871 – 876	54.38	55.09	52.39
GSM-R uplink	876 – 880	18.92	21.19	19.01
GSM900 downlink	880 – 915	58.28	59.17	55.81
Empty	915 – 916	9.43	10.71	9.52
PAMR downlink	916 – 921	49.25	45.91	47.50
GSM-R downlink	921 – 925	15.49	20.17	13.38

Table 4.4 Spectrum occupancy in three weeks in 800 MHz and GSM 900 bands with their associated licensee

800 MHz band	Range (MHz)	Occupancy (%) 1º Wednesday	Occupancy (%) 2º Wednesday	Occupancy (%) 3º Wednesday
FDD1 DL HI3G	791 – 796	55.95	73.56	73.42
FDD2 DL HI3G	796 – 801	19.38	20.97	18.69
FDD3 DL TeliaSonera	801 – 806	54.19	83.73	27.54
FDD4 DL TeliaSonera	806 – 811	62.41	94.51	38.77
FDD5 DL Net4Mobility	811 – 816	99.49	99.30	99.56
FDD6 DL Net4Mobility	816 – 821	99.99	100	100
Gap	821 – 832	6.35	9.38	7.09
FDD1 UL HI3G	832 – 837	5.95	6.80	5.30
FDD2 UL HI3G	837 – 842	86.80	87.92	88.79
FDD3 UL TeliaSonera	842 – 847	53.18	81.69	83.42
FDD4 UL TeliaSonera	847 – 852	3.17	4.26	3.43
FDD5 UL Net4Mobility	852 – 857	53.40	51.17	47.73
FDD6 UL Net4Mobility	857 – 862	31.92	37	21.89
GSM900 band	**Range (MHz)**	**Occupancy (%)**	**Occupancy (%)**	**Occupancy (%)**
DL HI3G	880 – 885	95.88	95.99	95.44
DL Swefour	885 – 890	16.18	17.55	15.98
DL Tele2	890 – 897.5	94.96	98.74	99.3
DL Telenor	897.5 – 905	43.65	43.71	39.62
DL TeliaSonera	905 – 915	45.23	44.80	36.70

Now we compare some consecutive working days at Electrum building. Figure 4.5 (b) above, depicts the measurements made on Wednesday of the second week, and we are going to compare that result with the results obtained on Tuesday and on Thursday of the same week. Figure 4.5 (b), Figure 4.6 (a), and Figure 4.6 (b) belong to the last week of May. By comparing the spectrum occupancy results calculated between this week and the other two weeks, this is the week that has greater occupancy in almost all bands.

Table 4.5 shows that occupancies from 790MHz to 925MHz do not change too much in consecutive days. However, in Table 4.6 we can see big difference in the usage of FDD3 downlink between one day and another as we stated before.

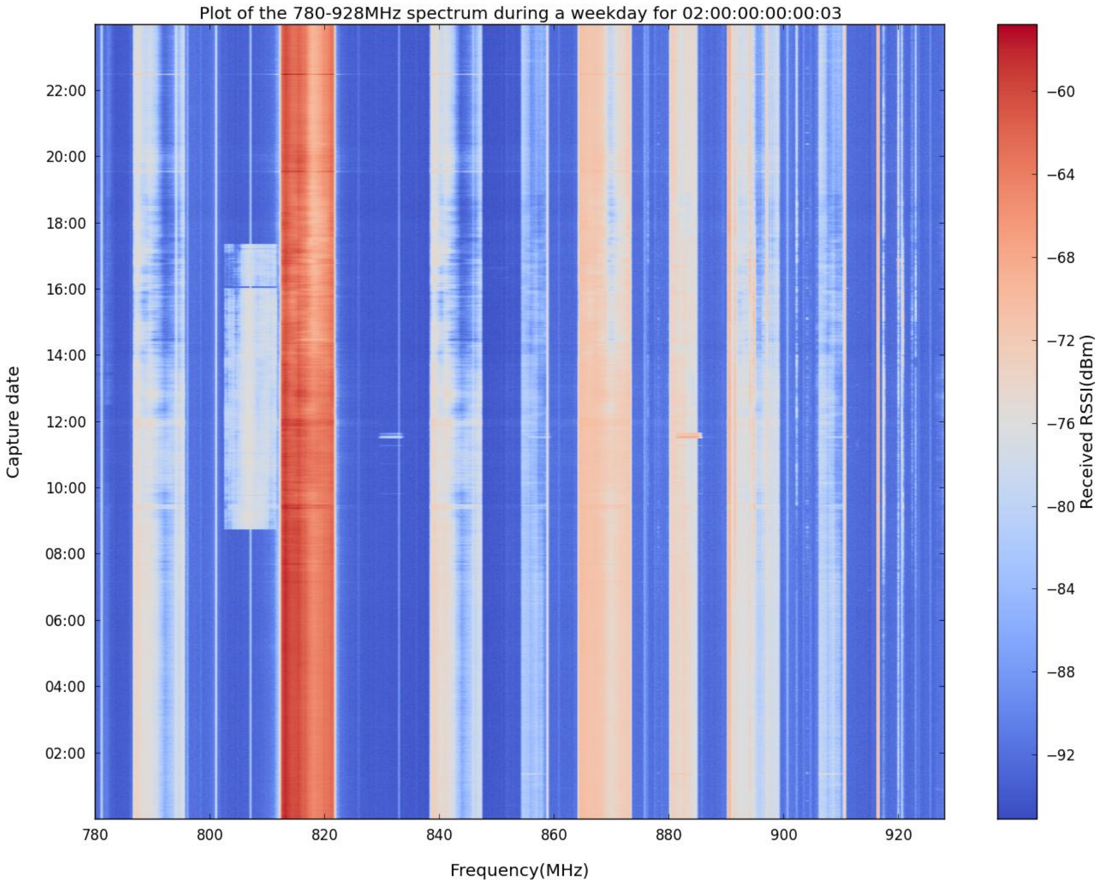


Figure 4.6 (a) Relation between frequency and time one Tuesday

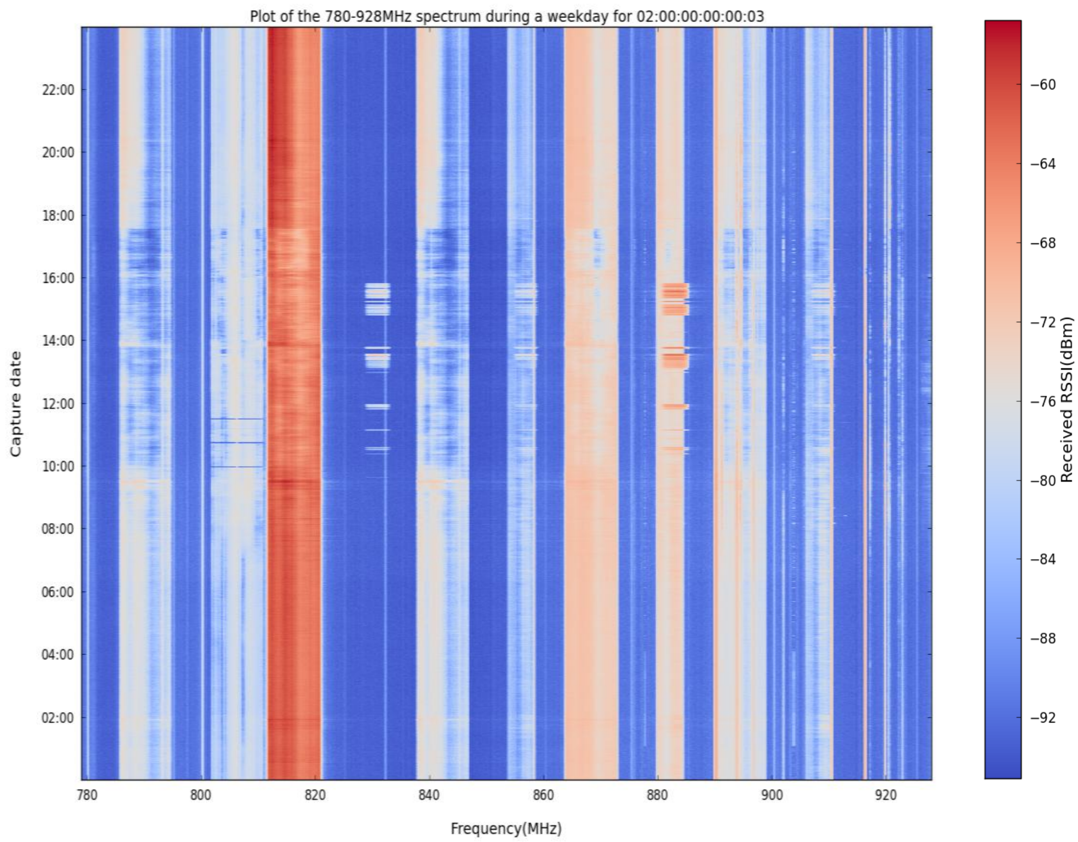


Figure 4.6 (b) Relation between frequency and time one Thursday

Table 4.5 Occupancies (%) from 790MHz to 925MHz in three consecutive working days

Spectrum band	Range (MHz)	Occupancy (%) Tuesday	Occupancy (%) Wednesday	Occupancy (%) Thursday
Empty	790 – 791	63.81	82.69	67.21
800 MHz downlink	791 – 821	60.25	77.70	77.06
Empty	821 – 823	23.32	28.57	20.61
800 MHz center gap	823 – 832	4.41	5.38	6.43
800 MHz uplink	832 – 862	40.95	44.34	41.23
Empty	862 – 863	8.20	10.81	8.68
SRD-800	863 – 870	94.44	94.70	94.3
Licensed SRD	870 – 871	99.8	100	99.91
PAMR uplink	871 – 876	52.66	55.09	52.43
GSM-R uplink	876 – 880	18.42	21.19	19.22
GSM900 downlink	880 – 915	56.57	59.17	57.48
Empty	915 – 916	9.06	10.71	9.39
PAMR downlink	916 – 921	40.57	45.91	40.40
GSM-R downlink	921 – 925	16.35	20.17	18.64

Table 4.6 Occupancies (%) in 800 MHz and GSM 900 bands with their associated licensee in three consecutive days

800 MHz band	Range (MHz)	Occupancy (%) Tuesday	Occupancy (%) Wednesday	Occupancy (%) Thursday
FDD1 DL HI3G	791 – 796	66.75	73.56	65.76
FDD2 DL HI3G	796 – 801	19.44	20.97	19.69
FDD3 DL TeliaSonera	801 – 806	32.65	83.73	87.02
FDD4 DL TeliaSonera	806 – 811	47.17	94.51	96.35
FDD5 DL Net4Mobility	811 – 816	99.6	99.30	99.18
FDD6 DL Net4Mobility	816 – 821	99.99	100	99.99
Gap	821 – 832	7.65	9.38	8.83
FDD1 UL HI3G	832 – 837	6.04	6.80	7.1
FDD2 UL HI3G	837 – 842	87.64	87.92	83.20
FDD3 UL TeliaSonera	842 – 847	68.91	81.69	68.37
FDD4 UL TeliaSonera	847 – 852	3.46	4.26	3.53
FDD5 UL Net4Mobility	852 – 857	55.44	51.17	54.18
FDD6 UL Net4Mobility	857 – 862	28.39	37	34.21
GSM900 band	**Range (MHz)**	**Occupancy (%)**	**Occupancy (%)**	**Occupancy (%)**
DL HI3G	880 – 885	95.83	95.99	96.19
DL Swefour	885 – 890	15.26	17.55	16.23
DL Tele2	890 – 897.5	95.26	98.74	96.12
DL Telenor	897.5 – 905	39.24	43.71	38.61
DL TeliaSonera	905 – 915	42.75	44.80	44.99

After observing the spectrum occupancy differences between working days, we are going to show some results obtained after scanning on weekends. Figure 4.7 depicts the RSSI scanned on Saturday, in the last week of May (the first week scanned). The RSSI scanned in the following Sunday, and the next weekend are practically the same as Figure 4.7. The only weekend that apparently changes is the second weekend of June (the third week scanned). Figure 4.8 shows the results of this third Saturday, being the results of scanned Sunday of the same weekend very similar. Finally Table 4.7 shows the difference between Saturdays, in which has been highlighted the big differences between third Saturday, and working days and the other two scanned Saturdays. SRD bands are apparently used most of the time, while the rest of the bands have lower occupancy values than the values calculated during working days.

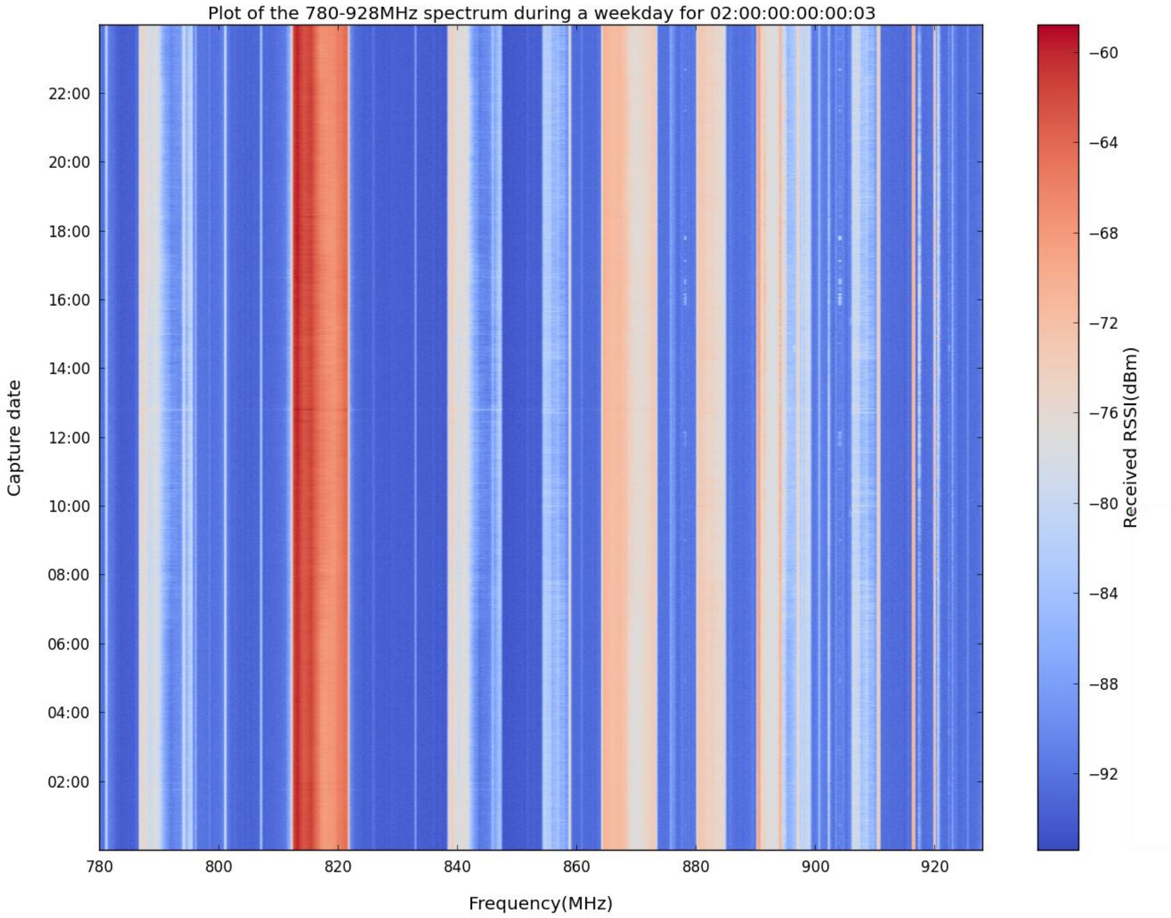


Figure 4.7 Relation between frequency and time first Saturday

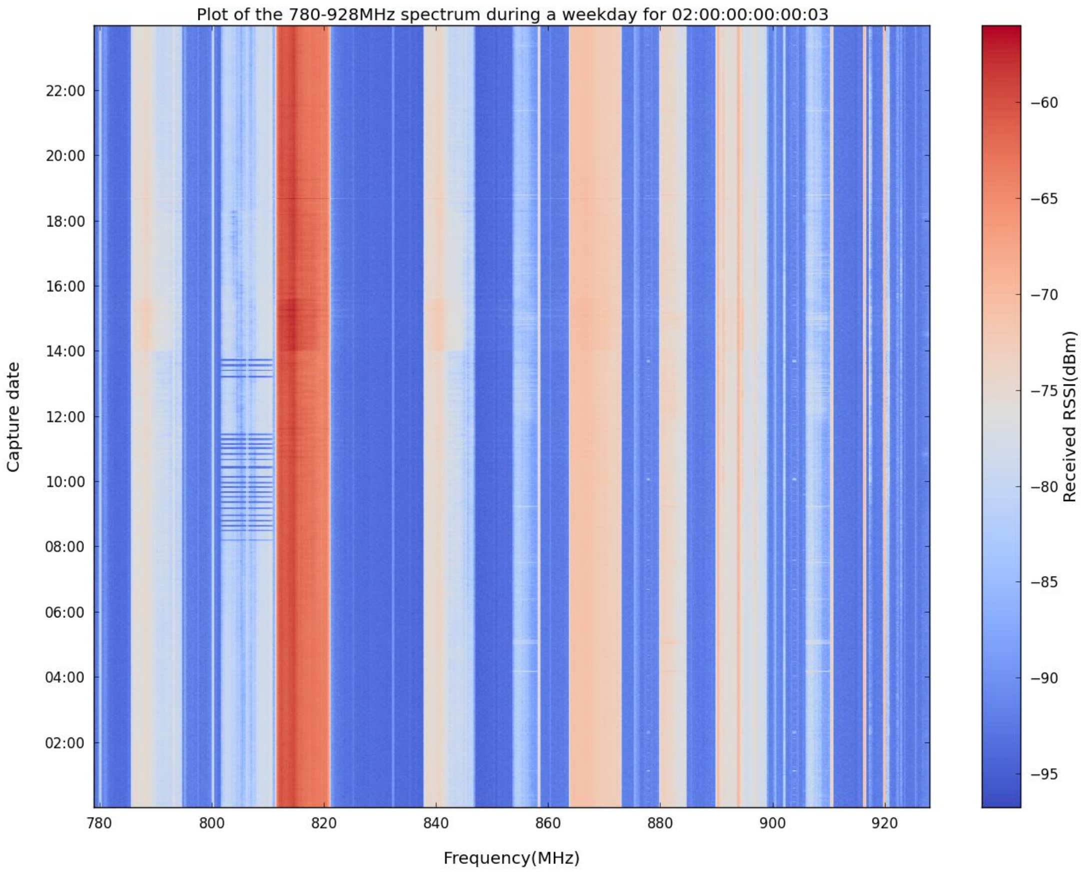


Figure 4.8 Relation between frequency and time third Saturday

Table 4.7 Occupancy (%) in different weekends highlighting the big differences

Spectrum band	Range (MHz)	Occupancy (%) 1º Saturday	Occupancy (%) Third Saturday
Empty	790 – 791	39.75	98.36
800 MHz downlink	791 – 821	47.87	77.22
Empty	821 – 823	13.84	17.82
800 MHz center gap	823 – 832	3.47	4.16
800 MHz uplink	832 – 862	35.13	44.57
Empty	862 – 863	6.20	8.63
SRD-800	863 – 870	94.48	94.64
Licensed SRD	870 – 871	99.99	100
PAMR uplink	871 – 876	51.18	51.93
GSM-R uplink	876 – 880	16.85	17.68
GSM900 downlink	880 – 915	55.16	56.68
Empty	915 – 916	8.39	8.70
PAMR downlink	916 – 921	40.31	45.81
GSM-R downlink	921 – 925	13.35	15.33

Chapter 5
Conclusions

This chapter presents the conclusions extracted from the analysis of the results obtained in the experiment, and compares the results with the goal of the thesis. It also suggests directions for future work following this area.

5.1 General conclusions

In this thesis we have studied the results obtained after scanning the frequency bands ranging from 779MHz to 928MHz around Electrum building at Kista, Sweden, with a number of specialized microcontroller based low-cost white space sensors which utilize energy detection. This detection of the environment has been carried out with a number of specialized microcontroller white space sensors, utilizing energy detector. These low-cost low-power sensors are powered by the same Ethernet cable by which they deliver RSSI data to a centralized server, which collects the data and allows the user to visualize the current scan data as well as change the scanning parameters. Our measurement results suggest that cooperating with the detection of primary signals in a centralized manner mitigates the effects of multipath fading and shadowing, as each node can detect different levels of RSSI for different frequencies in its location. However, we were not able to avoid the hidden listener problem or identify a spread spectrum primary user, hence more sophisticated methods are needed for this approach. It has also been observed that white spaces depend not only on the location and the frequency, but also on the time. In section 4.1.3 we have calculated the spectrum occupancy of the frequency range from 790MHz to 925MHz, while realizing that, although energy detector method is the most common used due to its low complexity, it is inefficient as we were not able to always distinguish between noise and primary signal. Our final conclusion is that some amount of radio spectrum in this range around Electrum building is being inefficiently used, hence CR could take advantage of this sharing opportunity. These long period observations enable us to identify patterns and potentially predict future white spaces. However, further occupancy studies with advanced sensing and decision making methods need to be performed to assess the feasibility of using alternative services, especially in those bands which were identify as less utilized, such as cellular uplink bands.

5.2 Future work

Since we conducted the experiment in a part of the 4th floor inside a building, the software could be enhanced to ease the installation in several personal computers to which local scanning data could be collected and then sent to a common server. This way a number of grids with sensor nodes in different locations separated by several kilometers perform coordinated white space detection. Also, the server needs additional software to automatically extract occupancy decisions, and to compute statistics about the successful prediction of possible future gaps, utilizing data collected for a longer period of time and at a greater number of locations. In addition, several different RF daughterboard could be realized in order to scan different frequency ranges with different boards, and the design of the platform could be improved by eliminating all the ground traces and put them directly in the copper on one side of the board that would have side which is largely connected to ground. While doing this kind of experiment, the situation of the base station concerning the frequency bands scanned should be taken into account in order to find several explanation for the results obtained with the different white sensor nodes.

Moreover, now a day the platforms send a packet to the server every millisecond with the RSSI detected in the current frequency, which occupy very few bits. It would be interesting send more than one RSSI value in one UDP packet to have less traffic through the Ethernet cables to the server, and gain in consumption.

Some other power alternatives for the board should be considered, such as solar panels if the experiment is going to be made at outdoor locations and during a season where the sun raises.

5.3 Required reflections

This thesis was motivated by the recent concern about the inefficient allocation of the radio spectrum. By developing a grid of white space sensors that can be aware of their environment, we hope to encourage the development of new technologies to effectively share the available spectrum and avoid the problem of artificial spectrum scarcity. In this sense, we consider this thesis project to have a positive social effect.

By deploying a sensor grid such as the one described in this project we might be able to offload tasks from CR devices to this grid, which would make CR devices cheaper and would reduce their energy consumption.

To reach the goal of this thesis, we have used the design of a low-cost low-power platform that considered both economic and environmental aspects. The circuit boards were mechanically milled out, meaning that no liquid chemical waste was produced. The solid waste from the milling contains copper, ground fiberglass, and resin. These could be recycled and the copper separated from the fiberglass and resin binder.

We have not encountered any significant ethical issues during the course of this Project. We have sense the radio spectrum to collect statistical information about the energy levels in different frequency bands, and we never transmitted on licensed bands and did not attempt to decode any signals. It should be noted that in Sweden listening to any frequency band is permitted, although you may not disclose received content to others.

Bibliography

[1] P. S. M. Tripathi, A. Chandra, A. Kumar, and K. Sridhara, “Dynamic spectrum access and cognitive radio,” in 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), Mar. 2011, pp. 1–5, DOI: 10.1109/WIRELESSVITAE.2011.5940911.

[2] Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook). NTIA. May 2012 Revision of the January 2008 Edition. Available: http://www.ntia.doc.gov/page/2011/manual-regulations-and-procedures-federal-radio-frequency-management-redbook

[3] Code of Federal Regulations. Title 47 – TELECOMMUNICATIONS. As of October 1, 2008. Available: http://www.gpo.gov/fdsys/pkg/CFR-2008-title47-vol1/pdf/CFR-2008-title47-vol1.pdf

[4] “US frequency allocation chart,” National Telecommunications and Information Administration, Oct. 2011. Available: http://www.ntia.doc.gov/page/2011/united-states-frequency-allocation-chart

[5] Federal Communications Commision, Spectrum Policy Task Force Report, ET Docket No. 02-155, Nov. 2002. Available: http://transition.fcc.gov/sptf/files/SEWGFinalReport_1.pdf

[6] M. A. Mchenry and D. Mccloskey. New York City spectrum occupancy measurements September 2004 [EB/OL]. Shared Spectrum Company.
Available: http://www.sharedspectrum.com

[7] M. H. Islam, et al., C. L. Koh, S. W. Oh, X. Qing, Y. Y. Lai, C.Wang, Y. C. Liang, B. E. Toh, F. Chin, G. L. Tan, and W. Toh, “Spectrum Survey in Singapore: Occupancy Measurements and Analyses”, In Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on, 2008, pp. 1-7, DOI:10.1109/CROWNCOM.2008.4562457.

[8] S. D’Iitri, and McHenry, “Dynamic spectrum access moves to the forefront” in Defence Electronics. April 2008.

[9] V. Valenta, R. Marsalek, G. Baudoin, M. Villegas, M. Suarez, and F. Robert, “Survey on spectrum utilization in Europe: Measurements, analyses and observations”, in 2010 Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks Communications (CROWNCOM), Cannes, France, June 2010. ISBN 978-1-4244-5885-1 pp.1–5.

[10] European Comission. Promoting the shared use of radio spectrum resources in the internal market. Brussels, 3.9.2012

[11] Q. Zhao and A. Swami “A Survey of Dynamic Spectrum Access: Signal Processing and Networking Perspectives”, in Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on, 2007, vol. 4, p. IV-1349-IV-1352, DOI:10.1109/ICASSP.2007.367328.

[12] I. F. Akyildiz, W. y. Lee, M. C. Vuran, and S. Mohanty, “Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey”, Computer Networks, vol. 50, no. 13, pp. 2127-2159, 2006, DOI: http://dx.doi.org/10.1016/j.comnet.2006.05.001. Available: http://www.sciencedirect.com/science/article/pii/S1389128606001009.

[13] J. Mitola and G.Q. Maguire Jr. “Cognitive radio: making software radios more personal”, IEEE Personal Communications, vol. 6, no. 4, pp. 13-18, August 1999,DOI:10.1109/98.788210. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=788210.

[14] J. Mitola, “Cognitive Radio”. Licentiate proposal, KTH, Stockholm, Sweden.

[15] J. M. Peha, “Sharing Spectrum Through Spectrum Policy Reform and Cognitive Radio”, Proceedings of the IEEE, vol. 97, no.4, pp. 708-719, 2009, DOI:10.1109/JPROC.2009.2013033. Available: http://morse.colorado.edu/~timxb/5520/ho/PehaSpectrum.pdf

[16] I. Christian, S. Moh, I. Chung, and J. Lee, “Spectrum mobility in cognitive radio networks”, Communications Magazine, IEEE, vol. 50, no. 6,pp.114-121,2012, DOI:10.1109/MCOM.2012.6211495.

[17] Pierre de Vries & Amber Hassan. “Spectrum Sharing Rules for New Unlicensed bands”. December 11, 2003.
Available:http://www.wi-fi.org/sites/default/files/kc_32_Spectrum%2550Sharing%2520Rules%2520for%2520New%2520Unlicensed%2520Brands.pdf

[18] T. Yucek and H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," Communications Surveys Tutorials, IEEE, vol. **11**, no. 1, pp. 116-130, 2009, DOI:10.1109/SURV.2009.090109.

[19] D. Cabric, S. Mishra, and R. Brodersen, “Implementation issues in spectrum sensing for cognitive radios,” in Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004, vol. 1, Nov. 2004. doi: 10.1109/ACSSC.2004.1399240 pp. 772 – 776 Vol.1.

[20] N. Dev Khaira, P. Bhadauria. “Cooperative spectrum sensing and Detection efficiency in cognitive radio network”. International Journal of Electronics and Computer Science Engineering. ISSN-2277-1956, vol. 1, no. 1, pp. 64-73. Available: www.ijecse.org/wp-content/uploads/2012/01/PP-64-73.pdf

[21] G. Ganesan and Y. Li, “Cooperative Spectrum Sensing in Cognitive Radio Networks”, in New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on, 2005, pp.137-143, DOI:10.1109/DYSPAN. 2005.1542628.

[22] IEEE Std. 802.3af-2003. Available: http://www.ieee802.org/3/af/index.html

[23] IEEE Std. 802.3at-2009. Available: http://standards.ieee.org/getieee802/download/802.3at-2009.pdf

[24] Calculating PoE Power loss due to Cable Resistance.
Available: http://www.comtrol.com/elements/uploads/fckeditor/file/Calc_PoE_PowerLoss.pdf

[25] D. Harrington, B. Wijnen, and R. Presuhn, “An Architecture for Describing Simple Network Management Protocol (SNMP) Management Networks”. March 09, 2012

Available: http://tools.ietf.org/html/rfc3411.

[26] PoE explained," Veracity UK Ltd, White Paper 002, Dec. 2008. Available: http://www.veracityglobal.com/media/27197/vwp-002%20poe%20explained.pdf

[27] R. Droms, "Dynamic Host Configuration Protocol", Internet Request for Comments, vol. RFC 2131 (Draft Standard), March 1997, Available: http://www.rfc-editor.org/rfc/rfc2131.txt

[28] K. Sollins, "The TFTP protocol (revision 2)," IETF, RFC 1350 (Standard), Jul. 1992. Available: http://www.ietf.org/rfc/rfc1350.txt

[29] J. Postel, "User Datagram Protocol", Internet Request for Comment, vol. RFC 768 (Standard), August 1980. Available: http://www.rfc-editor.org/rfc/rfc768.txt

[30] Protocol to Access White-Space (PAWS) Databases: Use Cases and Requirements. – Google. May 2013

[31] Z. Padrah, "Distributed Spectrum Sensing in Unlicensed Bands Using the VESNA Platform, MSc thesis, MPS, Ljubljana, Slovenia, December 2012. Available: http://sensorlab.ijs.si/en/publication/32/distributed-spectrum-sensing-in-unlicensed-bands-using-the-vesna-platform

[32] M. Smolnikar, M. Mihelin, G. Berke, G. Kandus and M. Mohorcic, "ISM Bands Spectrum Sensing based on Versatile Sensor Node Platform", in 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010, Rome, Italy, 2010, pp.1-5, DOI:10.1109/ISABEL.2010.5702937.

[33] J. Lara Peinado, "Minding the spectrum gaps: First steps toward developing a distributed White space sensor grid for cognitive radio". Degree project in Communication Systems, Royal Institute of Technology, School of Information and Communication Technology, Stockholm, Sweden. Junio 2013.
Available: http://kth.diva-portal.org/smash/get/diva2:627307/FULLTEXT01

[34] A. Lopez Garcia and F. J. Sanchez Galisteo, "Exploiting wireless sensors: A gateway for 868 MHz sensors," Masters's thesis, Royal Institute of Technology, School of Information and Communication Technology, Stockholm, Sweden, Jun. 2012, TRITA-ICT-EX; 2012:110. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-98209

[35] Switch HP procurve 2626-pwr J8164A.
Available: http://h10010.www1.hp.com/wwpc/ca/en/sm/WF06b/12136296-12136298-12136298-12136298-12136316-12136320-29584737.html?dnr=1

[36] "8922M/S GSM test set," Agilent Technologies, User's Guide 08922-90211, Jan. 1998. Available:
http://www.home.agilent.com/upload/cmc_upload/All/08922_90211.pdf?&cc=SE&lc=eng

[37] "TPS2375: IEEE 802.3af PoE Powered Device Controllers" Texas Instrument, Datasheet SLVS525B, April 2008. Available: http://www.ti.com/product/tps2375

[38] "TL2575HV step-down(buck) converter," Texas Instruments, Datasheet SLVS638B, January 2007. Available: http://www.ti.com/lit/gpn/tl2575hv-adj
[39] "ENC28J60 stand-alone ethernet controller with SPI interface," Microchip, Datasheet DS39662C, 2008. Available: http://ww1.microchip.com/downloads/en/DeviceDoc/39662c.pdf

[40] “Mixed signal microcontroller,” Texas Instruments, Datasheet SLAS655B, Oct. 2010. Available: http://www.ti.com/lit/ds/symlink/msp430f5437a.pdf

[41] “Low-Power Sub-1 GHz RF Transceiver”.
Available: http://www.ti.com/lit/ds/symlink/cc1101.pdf

[42] “MiniMag magnet mount antenna,” Smarteq, Product No. 1140.30SMA, May 2013. Available:http://www.smarteq.se/download/18.6018c17913483dc06428000159/MiniMag+1140.30SMA_550058E.pdf

[43] “Spectrum orientation plan,” Swedish Post and Telecom Agency, Rev. 2012-06-11, Oct. 2012. Available: http://www.pts.se/upload/Ovrigt/Radio/draft-orientation-plan-121011.pdf

[44] S. Ibrahim, “Decision about licences to use radio transmitters in the 791–821/832–862 MHz frequency band,” Swedish Post and Telecom Agency, Decision 10-10534, Mar. 2011. Available: http://www.pts.se/upload/Beslut/Radio/2011/10-10534-desicion-assignment-800mhz.pdf

[45] ITU-T Recommendations**.** Available:
http://www.itu.int/en/ITUT/publications/Pages/recs.aspx

TRITA-ICT-EX-2013:177