

GSM Sensor

Passive detection of mobile phone users

BACHELOR'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science

in

Telecommunication Technologies

by

Marc Pàmies

Registration Number 1635857

to the Faculty of Informatics

at the TU Wien

Advisor: Ao.Univ.Prof.Dr. Wolfgang Kastner

Assistance: Dipl.-Ing. Philipp Raich

Vienna, 24th February, 2017

Marc Pàmies

Wolfgang Kastner

Erklärung zur Verfassung der Arbeit

Marc Pàmies
Schäffergasse 2, 1040 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 24. Februar 2017

Marc Pàmies

Acknowledgements

First of all, I would like to express my sincere gratitude to my advisor Dr. Wolfgang Kastner for giving me the opportunity to work on this Bachelor's thesis at the Automation Systems Group of the Institute of Computer Aided Automation from Technische Universität Wien.

Moreover, I am especially grateful to my co-advisor Philipp Raich for his unconditional support throughout all the thesis. I really appreciate all the counsel given in our weekly meetings, as well as his predisposition to help in any aspect related to the project.

Furthermore, I want to thank my friends and family for their mental support throughout all my studies, especially in these last months that I have spent away from home.

Abstract

In the recent years a wide range of sensors has been developed in the field of human presence detection for user-centered applications. Some of them are not focused on detecting people themselves but the electronic gadgets that they use to carry, which are basically mobile phones. On this basis, and taking into account that almost everyone owns a cellular phone nowadays, the overall goal of this thesis is to explore a new way to passively detect persons by means of their mobile phone emissions.

Modern phones make use of several technologies, most of them valid for the realization of sensors. However, this thesis will be exclusively focused on the Global System for Mobile Communications (GSM) that has been used for cellular telephony from the early nineties to the present day. The work relies on the literature as a starting point for a complete understanding of the intricacies of the second-generation digital cellular networks.

A method for detecting nearby mobile phones that are not currently being used is proposed. The method is implemented as a proof of concept using a Software Defined Radio (SDR) peripheral together with the proper open-source software to test the feasibility of the whole idea.

While the detection of inactive mobile phones could not be shown using the proposed method, the reliable detection of actively used phones has proven to be possible. As the initial approach could not be implemented successfully, the aforementioned sensor will be limited to the detection of active mobile phone users.

Contents

Abstract	iv
Contents	v
1 Introduction	1
1.1 Motivation	1
1.2 Problem Statement and Methodological Approach	2
1.3 Structure of the Work	2
2 Theoretical Background of GSM	3
2.1 Overview	3
2.2 Network Architecture	3
2.2.1 Mobile Station	5
2.2.2 Base Station Subsystem	5
2.3 Carrier Frequencies	6
2.4 Channel Access Methods	7
2.4.1 FDMA	8
2.4.2 TDMA	8
2.5 Modulation	10
2.5.1 Modulator	11
2.5.2 Demodulator	12
2.6 Frequency Hopping	12
2.7 Power Control	13
2.8 Radio Interface	14
2.8.1 Traffic Channels	15
2.8.2 Control Channels	15
2.9 Mobility Management	17
2.9.1 Location Area	17
2.9.2 Handover	18
2.9.3 Roaming	19
3 Suggested Solution	20
3.1 Related work	20

3.2	Concept for passive GSM detection	24
3.3	Hardware and Software tools	26
3.3.1	Software Defined Radio	26
3.3.2	HackRF One	27
3.3.3	Low Noise Amplifier	29
3.3.4	GNU Radio	30
3.3.5	Operating System	32
4	Implementation	33
4.1	Acquiring Network Information	33
4.2	Detection in idle mode	35
4.2.1	Overview	35
4.2.2	Parameters	36
4.2.3	Methodology	39
4.2.4	Results	41
4.3	Detection in dedicated mode	44
4.3.1	Overview	44
4.3.2	Parameters	46
4.3.3	Methodology	47
4.3.4	Results	47
5	Conclusion and Outlook	49
5.1	Summary and Critical Reflection	49
5.2	Future Work	49
	Annex I: HackRF One	51
	Glossary	52
	Acronyms	53
	Bibliography	56

Introduction

1.1 Motivation

Human presence detection has become an important research topic since automation systems came to light, especially for user-centred applications. Some examples of where this technology could be applied are smart homes, street lights' control, surveillance or customer analytics among others.

A large number of sensors have already been used for this purpose, such as radars, thermographic cameras, pressure-sensitive floors, acoustic sensors or motion detection techniques. All these technologies offer different ways of detecting the presence of a human body in a specific area without the participation of the detected person. However, it is believed that alternative ways allow for better results.

The main idea of this project is to take advantage of the fact that nowadays almost everyone owns a mobile phone, a device that is constantly exchanging information with the cellular network via Radio Frequency (RF) signals. Those signals are sent over the air interface, so it should be possible to detect them using the right tools. In other words, given the high probability of a person carrying a mobile phone, it would be of great interest to prove if human sensing could be achieved by passively detecting mobile phone users. Thereby it would be possible to discern between human beings and other moving objects, such as animals or cars.

The thesis follows the approach presented in other projects where WiFi or Bluetooth signals are used in order to detect pedestrians, but going one step further opting for a different technology: Global System for Mobile Communications (GSM). The reason is that GSM probe request signals are sent more frequently than WiFi's requests and they are not as easy to hide as Bluetooth signals, so this alternative technology could be used to supplement the aforementioned solutions for overall improved accuracy giving rise to a more reliable sensor.

1.2 Problem Statement and Methodological Approach

The aim of this thesis is the development of sensor capable of identifying the presence of a any nearby cellular system that makes use of the GSM technology. Such a sensor should preferably be able to detect mobile phones that are not currently being used, as these devices allegedly maintain contact with the network at all times. If this proves to be unworkable, the sensor should at least be able to detect active phones which are either calling or sending a message via Short Message Service (SMS).

The first step to achieve this should be to do a preliminary research of relevant literature in the field of mobile phone users' detection. Based on this research, an analysis of the possible solutions should be performed from a theoretical point of view.

In order to determine which is the hardware that better suits our interests, a market survey should be done to evaluate all feasible options. Finally, a prototype should be built as proof-of-concept and be evaluated in different real life scenarios. The obtained results will give us the insight to conclude if the chosen approach is worth to be put into practice.

1.3 Structure of the Work

Some theoretical background about GSM is presented in chapter 2. This chapter will be focused on those aspects of the GSM standard that are necessary to fully understand the explanations from future sections, leaving aside most of the concepts that do not serve for that purpose.

Afterwards, in chapter 3 a solution to the problem is approached by discussing the possible alternatives. It starts with a general review about what has already been carried out by third parties in the field of human presence detection, always within the context of mobile telephony. Then, a suggested solution is widely explained and the basic requirements that should be achieved are exposed as well.

Subsequently, chapter 4 presents a reference implementation of the chosen concept that serves as a proof-of-concept. A detailed explanation of how to use the different hardware and software tools is included, as well as an overview of the results obtained from tests carried out in different scenarios.

The thesis is concluded by a summary and an outlook for possible future work in chapter 5.

Theoretical Background of GSM

2.1 Overview

The Global System for Mobile Communications (GSM) is a telecommunications standard that was originally developed in 1984 by the European Telecommunications Standards Institute (ETSI). The respective standard describes the protocols for the second-generation digital cellular networks (2G), which replaced the first-generation analog cellular networks (1G) in the early nineties. The main services offered by GSM are full duplex voice telephony and Short Message Service (SMS). However, over time newer versions of the protocol have introduced data communications to cell phone systems (General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE)). Since GSM was first deployed in 1991, newer generations of mobile communication networks have come to light, but still at the present time GSM is widely used around the world, having over 90% of market share. For this reason, and taking into account that almost everyone owns a telephone nowadays, the option of using GSM signals to detect pedestrians is promising.

In this introductory section the necessary theoretical background behind the world's most popular mobile phone system is presented in order to ensure that the reader has the required knowledge to fully understand the upcoming sections.

2.2 Network Architecture

Despite the development of new telecommunication systems, the initial GSM system architecture has remained intact since it was first launched more than twenty years ago. The main difference with its predecessors is that it has to handle users' mobility and radio resource management. In addition, it has to deal with the disposal of a limited spectrum and also with propagation losses that can be critical in urban environments.

This is why this technology requires a network that divides the coverage territory into different areas (cells), each of them with its own access point (base station). This system allows having a wide coverage area and to offer service to a large number of subscribers by doing frequency reuse. The only condition is that, to ensure that interferences between users remain below a harmful level, adjacent cells cannot use the same frequencies.

A visual example of this can be found in figure 2.1.

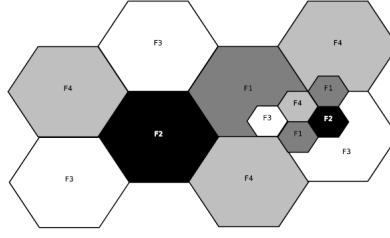


Figure 2.1: Frequency reuse in a geographical area. Source: [1]

The frequency-reuse factor will largely determine the final cost of the infrastructure since it has a direct impact on the number of cells that will be needed to cover a given area and a given traffic with a limited radio spectrum. There are several techniques to improve spectral efficiency, but for now this initial section shall be limited to describe the different parts involved in a GSM cellular network. The network's architecture as defined in the GSM specifications can be broadly divided into:

- Mobile Station (MS)
- Base Station Subsystem (BSS)
- Network Switching Subsystem (NSS)
- Operation and Support Subsystem (OSS)

Each layer is composed of different elements that interact with each other, as can be appreciated in the figure below.

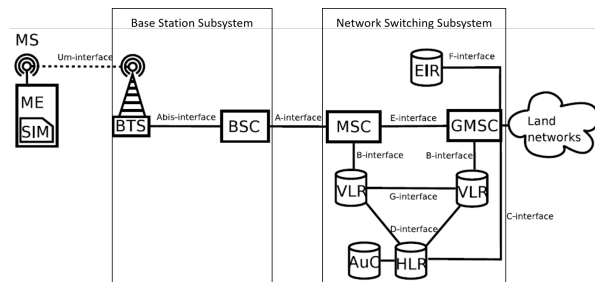


Figure 2.2: GSM Network Architecture. Source: [1]

As our interest remains in the air interface (commonly called Um interface), in this section only the elements who participate in that communication link will be explained. It means that the NSS (responsible for the switching of calls) and the OSS (used to control and monitor the overall network and the traffic load) will be omitted to avoid diverting the reader from the main topic.

2.2.1 Mobile Station

The MS is the main hardware from the user's point of view: a Mobile Equipment (ME) with a Subscriber Identity Module (SIM) card inside. All subscribers need a MS to access the mobile network as it incorporates all the generic radio and processing functions required to operate in the air interface.

The ME is a transceiver that allows the user to make and receive calls. It is identified by a unique 15-digits code called International Mobile (Station) Equipment Identity (IMEI), a serial number that is burned into the phone by the manufacturer.

The second element, the SIM card, is an integrated circuit used by all GSM terminals to provide the user's identity to the network. This smart card contains all the subscriber-related information and a secret key for authentication. The network provider identifies each SIM by a unique number called International Mobile Subscriber Identity (IMSI), which specifies the Mobile Country Code, the Mobile Network Code as well as the Mobile Subscriber Identification Number. Inserting a SIM card to any GSM phone subscribers can have access to the subscribed services, irrespective of a specific terminal.

2.2.2 Base Station Subsystem

The BSS can be defined as a group of transceivers that serve as access points for the MSs to the whole network. So, this part of the network is in charge of establishing communication with as many MSs as possible. Any BSS consists of a Base Station Controller (BSC) connected to multiple Base Transceiver Stations (BTSs). These two elements communicate across a standardized interface regardless of whether they were made by different suppliers or not.

BTSs are radio transceivers capable of establishing direct communication with MSs. Such communication takes place over the air interface with all the handsets that are located within their coverage area. Each BTS covers a specific cellular area, whose radius may vary between 100 m and 35 km depending on the hardware and the environment (geography, buildings, weather and population density). Network providers should consider all these factors to determine the minimum number of BTSs required to cover the entire area. For example, in large urban areas the number of BTSs will be potentially higher than in semi-urban or rural locations due to a much higher population density.

From now on we will refer to these antennas as "cell tower", "cell site", "base station" or simply BTS. The next hierarchy in the network structure is known as the BSC, which controls the radio resource management of several BTSs. Mainly it handles the allocation and release of radio channels as well as session handovers between adjacent cells, but it is also responsible of controlling frequency hopping, choosing the encryption algorithm or making signal power adjustments among other things (all these concepts will be explained in detail later). A BSC is usually co-located with one of its associated BTSs.

The BSC is the link between the mobile station and the NSS. However, as it was previously said in this section, this part of the network is out of the scope of the project.

2.3 Carrier Frequencies

GSM implements a Frequency-Division Duplexing (FDD) technique to make full duplex telephony possible, which means that the transmitter and the receiver operate at different carrier frequencies. All messages from MSs to BTSs are sent using an uplink frequency while messages from BTSs to MSs are sent using a downlink frequency. The distance between those two frequencies is known as “duplex distance” or “duplex spacing” and its value depends on the frequency band that is being used, always ensuring that this offset is enough to guarantee that there are no interferences between the up and down links.

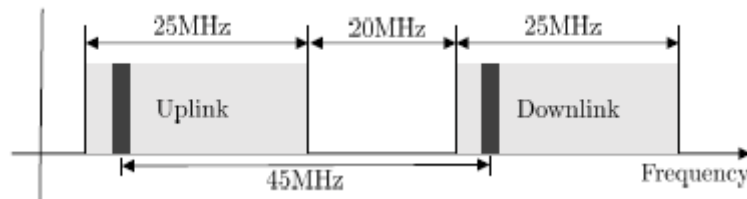


Figure 2.3: Duplex distance in GSM-900. Source: [2]

In section 2.4 it will be explained that network operators divide the total band available in consecutive radio channels of 200 KHz each. In the case of GSM-900 (which has a bandwidth of 25 MHz for each link) this results in 125 bidirectional channels, as it can be seen in figure 2.3. An important characteristic to take into account is that the duplex spacing is maintained regardless of the used channel. Thus, if the third channel of the GSM-900 band is used for the uplink (890.4 MHz – 890.6 MHz) then the frequencies used for the downlink would also be the ones of the third downlink channel (935.4 MHz – 935.6 MHz).

According to this, it can be deduced from the picture above that in GSM-900 the duplex distance between the uplink and downlink channels is exactly 45 MHz, a value that would be completely different if we were talking about GSM-1800 or GSM-1900.

To compute the uplink and downlink frequencies a code called Absolute Radio Frequency Channel Number (ARFCN) is required. Higher ARFCN values result in higher uplink and downlink channel frequencies, but there is no specific formula as the way of computing those frequencies is different from one GSM band to another. In any event, it can be said that each pair of frequencies of a GSM channel has a unique ARFCN number assigned.

All this concepts are summarised in the the table from figure 2.4.

It is well known that GSM uses several frequency bands, which vary depending on the country. In the case of Austria, where this project is taking place, the bands used are

Band	Name	ARFCN Range	Uplink Frequency (MHz)	Downlink Frequency (MHz)
GSM400	GSM450	$259 \leq n \leq 293$	$450.6 + 0.2 \times (n-259)$	$f_{up}(n) + 10$
	GSM480	$306 \leq n \leq 340$	$479.0 + 0.2 \times (n-306)$	$f_{up}(n) + 10$
GSM700	GSM750	$438 \leq n \leq 511$	$747.2 + 0.2 \times (n-438)$	$f_{up}(n) + 30$
GSM850	GSM850	$128 \leq n \leq 251$	$824.2 + 0.2 \times (n-128)$	$f_{up}(n) + 45$
GSM900	Primary GSM	$1 \leq n \leq 124$	$890 + 0.2 \times n$	$f_{up}(n) + 45$
	Extended GSM	$0 \leq n \leq 124$	$890 + 0.2 \times n$	$f_{up}(n) + 45$
		$975 \leq n \leq 1023$	$890 + 0.2 \times (n-1024)$	
	GSM Rail	$0 \leq n \leq 124$ $955 \leq n \leq 1023$	$890 + 0.2 \times n$ $890 + 0.2 \times (n-1024)$	$f_{up}(n) + 45$
GSM1800	GSM1800 (DCS1800)	$512 \leq n \leq 885$	$1710.2 + 0.2 \times (n-512)$	$f_{up}(n) + 95$
GSM1900	GSM1900 (PCS1900)	$512 \leq n \leq 810$	$1850.2 + 0.2 \times (n-512)$	$f_{up}(n) + 80$

Figure 2.4: Uplink/Downlink formulas for each band. Source: [3]

GSM-900, EGSM-900 and GSM-1800. Those bands are also used in Africa, Asia, Oceania, Middle East and the rest of Europe, while in other parts of the world GSM-450, GSM-850 and GSM-1900 bands are used instead. Nowadays it is no longer a problem for travellers as modern phones support multiple bands to facilitate roaming.

Notice that EGSM-900 is just an extension of GSM-900 that has a bandwidth 20 MHz larger allowing the accommodation of 50 extra pairs of channels. It was introduced to increase the available spectrum and, with this, provide service to more subscribers.

To conclude this section we must remark that different bands have different characteristics. As a matter of fact, GSM-900 offers a higher coverage area than GSM-1800 because it uses lower frequencies. For the same reason, the higher wavelengths of GSM-900 provide a better indoor coverage as the waves of 900 MHz can cross walls more easily than 1800 MHz waves. But on the other hand GSM-1800 is supposed to be better suited for high populated areas since this newer version has a wider band than GSM-900 and can handle a bigger network load.

2.4 Channel Access Methods

GSM uses two channel access methods on the air link: Time-Division Multiple Access (TDMA) and Frequency-Division Multiple Access (FDMA). This means that the physical channel is defined by selecting a certain radio carrier and a certain time slot, as explained below.

2.4.1 FDMA

This technique consists in dividing the available spectrum into individual channels of 200 kHz bandwidth each. This allows multiple subscribers to use a shared bandwidth without interfering with each other. Actually, the spectrum of the GSM signals is extended outside the fairly narrow band assigned to a radio channel so that adjacent channels interfere with each other. Anyhow it does not pose a serious problem because GSM is an interference-limited system (its performance depends on the signal-to-interference ratio rather than the signal-to-noise ratio) in which orthogonal narrowband channels are assigned to users within a cell. This entails a complex process of network planning where operators try to reuse the available frequencies in a smart way.

This effort to reduce as much interference as possible between users involves an inefficient use of the total bandwidth because users in adjacent cells cannot be assigned the same channel.

2.4.2 TDMA

Apart from the division in the frequency domain, each sub-frequency band is divided into eight time slots using a TDMA scheme. The same slot is used for both transmission and reception, but obviously at different frequencies (section 2.3). This allows having up to eight different conversations being handled simultaneously by the same carrier frequency.

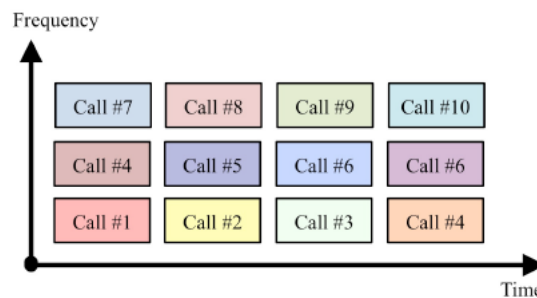


Figure 2.5: Channel allocation in GSM. Source: [3]

Each MS can only use the single time slot that has been assigned to him, but transmitting and receiving on the same time slot does not mean that it is done at the same time: there is a three-bursts offset present between the downlink and uplink (see figure 2.6). The reason is just that the transmission time depends on the distance between the receiver and the transmitter (which is different for each MS), so bursts transmitted from long distances could easily move out of their time slots. To control this the BSS computes a timing advance for all the phones connected to their BTSs and informs them so that they can know the exact moment in which they are supposed to transmit.

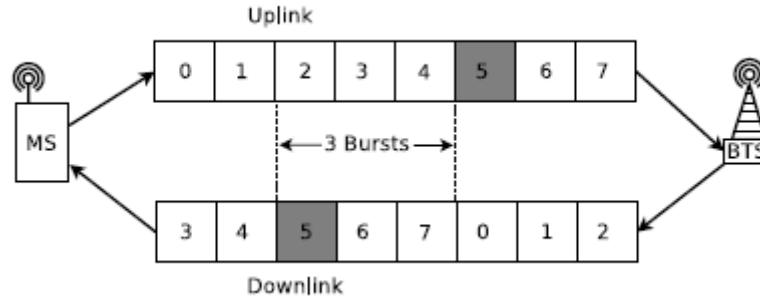


Figure 2.6: Offset between uplink and downlink. Source: [1]

When a MS broadcasts for the first time there is a high probability of receiving the message outside of its burst period since the device does not know its timing advance yet. This first message is always an “access burst” sent over the Random Access Channel (RACH), and as can be seen in figure 2.7 this type of bursts have a much longer guard period and more starting tail bits precisely to prevent interference from other MSs transmitting on the RACH. MSs send this message to access the network following the ALOHA protocol. Apart from the access burst, which are the only ones that are sent over the uplink channel, there are four other types of bursts (normal burst, frequency correction burst, dummy burst and synchronization burst) but they will not be described in detail as it is out of the scope of this project. We will only pay attention to the structure of each type, which can be seen in the following scheme:

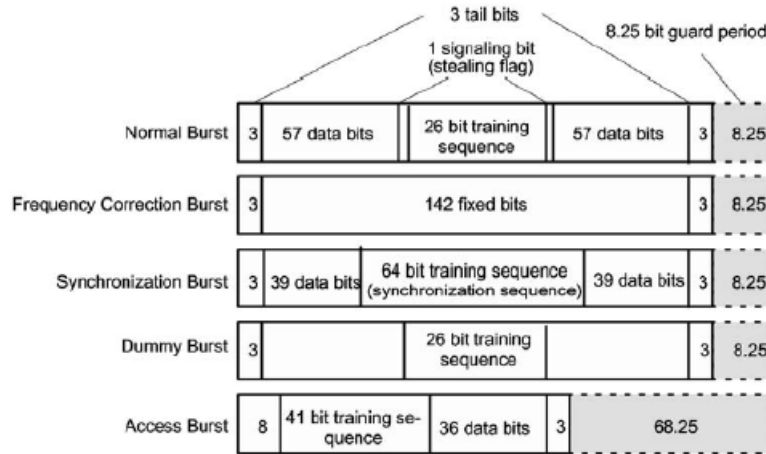


Figure 2.7: Types of GSM bursts. Source: [4]

2.5 Modulation

In telecommunications, modulation is the process of conveying either binary data or an analog signal inside a propagating electromagnetic field. In the case of GSM the information is carried in the phase of this electromagnetic field that will be transmitted over the air.

In consequence GSM uses a continuous-phase frequency-shift keying modulation scheme called Gaussian Minimum-Shift Keying (GMSK), in which the phase of the carrier is instantaneously varied by the modulating signal. It is a derivative from the Minimum-Shift Keying (MSK) modulation scheme, which uses a sine wave whose frequency varies according to the logical value to be modulated. The main difference between these modulation schemes is that in GMSK the signal is previously filtered with a Gaussian Filter of an appropriate bandwidth, which has the following consequences:

- Less out-of-band radiation due to a reduction of the side-band power. Hence the interferences between signal carriers in adjacent frequency channels are reduced.
- Inter-symbol interference: each data bit influences the signal during a period exceeding the bit duration (the receiver may require an adaptive equalizer because of this).

The problem of MSK is that it does not satisfy the requirements with respect to out-of-band radiation for single-channel-per-carrier mobile radio. It is the Gaussian filter used by GMSK what solves the problem by making the output power spectrum more compact. This modulation was chosen as a compromise between a fairly high spectrum efficiency and a reasonable demodulation complexity.

Section 2.4 addressed the subject of time slots, which become important now to understand how mobile telephony signals are modulated. In figure 2.8 we can see the internal structure of all types of GSM frames.

In the image we can see that the duration of a TDMA frame is of 4.616 ms, which means that the slots' duration is 576.9 μ s (because one frame is formed by eight slots). Then, considering that GMSK provides a modulation rate of 227.833 Kb/s, the duration of a single time slot allows the transmission of 156.25 bits.

At the bottom of the image we can see that a normal burst has 114 bits intended for data. Dividing this value by the duration of one slot we can deduce the theoretical bit rate of a single time slot: 197.6079 Kb/s. Thus, the bit rate of a TDMA frame would be eight times smaller (24.7 Kb/s).

As a consequence of the particular GMSK scheme used in GSM, the spectrum has a bandwidth much wider than the channel separation of 200 KHz, which implies a non-negligible overlap between the spectrum of adjacent frequency slots. The only way to

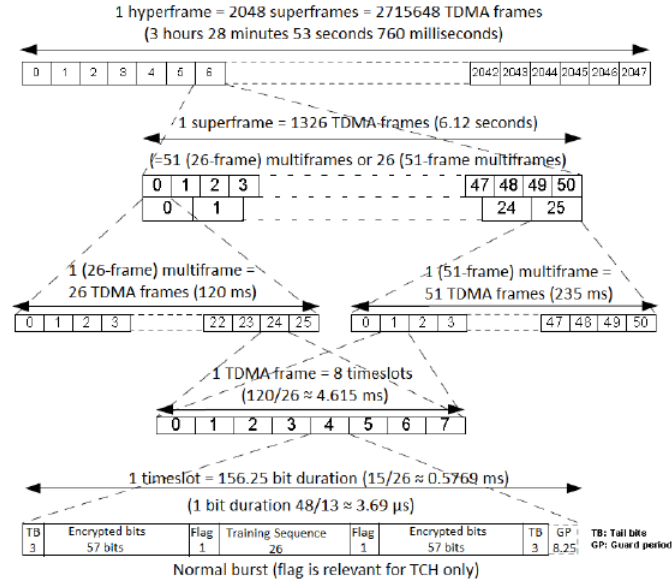


Figure 2.8: Frame structure in GSM. Source: [4]

control this source of interference consists in not using close frequencies in the same geographical area.

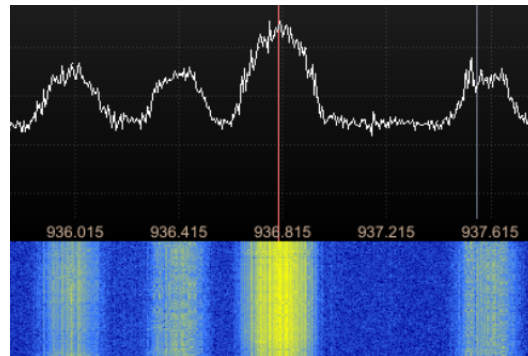


Figure 2.9: Typical pattern of GSM spectrum captured with GQRX.

2.5.1 Modulator

The typical implementation includes a first stage where a low frequency signal is created, and a second stage where this signal is transposed to the correct burst frequency after adjusting its power to the desired level. The phase of the signal must remain intact along all of the process as it contains the information to be transmitted.

2.5.2 Demodulator

As expected in the field of telecommunications, the received signal will differ from the emitted one due to multiple effects: the free space loss, shadowing, reflections, diffractions and a long list of possible noises and interferences.

So the demodulator must deal with these problems and estimate the most probable sequence of modulating data according to the distorted signal that has been received. The receiver estimates the distortion of the signal due to multipath using a known training sequence that is included in a portion of each burst.

Simple demodulation techniques are not able to cope with the inter-symbol interference characteristic of GSM, for this reason it was said before that an equalisation is required in the reception site. The demodulation technique accepted for GSM is based on the so called Viterbi algorithm. It is a maximum likelihood technique used to find the most probable emitted sequence.

2.6 Frequency Hopping

A method called Slow Frequency Hopping (SFH) is used in GSM to compensate the differences in signal quality between carriers, mainly produced by multipath, interferences and atmospheric noise. These effects do not generate the same distortion at each carrier channel, so “hopping” from one carrier to another is a good method to reduce the subscriber’s risk of suffering co-channel interferences. It improves the channel capacity and the frequency reuse ratio, which is very important as the frequency spectrum is a scarce resource.

It basically consists of changing the uplink and downlink frequencies during transmission at regular intervals (see figure 2.10). Above all, this technique is necessary for cancelling the Rayleigh fading effect, which occurs when the reflected signals received by the MS cancel each other because of their unfavourable phases. It mainly affects stationary or quasi-stationary mobiles, because the signal’s phase depends on the relative position between the receiver and the transmitter. So one possibility to correct this effect would be to slightly move the receiver or the transmitter, but BTSs are fixed on the ground and subscribers should have a good service whether they are moving or not. Then, the only alternative is to change the transmitter frequency taking advantage of the fact that radio signal’s phases are also frequency-dependent.

So, as position correction is not an option to improve the receiving conditions, network operators randomly change the transmitting frequency between consecutive TDMA frames to introduce diversity on the transmission link. This significantly increases the Quality of Service (QoS) because the transmission errors are randomly distributed instead of having long bursts of errors, and at the same time is an added difficulty for eavesdroppers because the pseudorandom sequence of ARFCN numbers to be used is generated by the

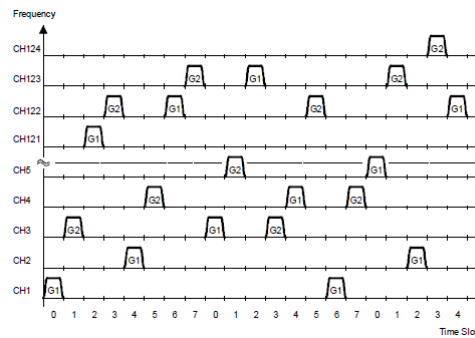


Figure 2.10: Frequency hopping scheme. Source: [5]

BTS and transmitted encrypted to the MS over the air interface. The BTS is the one that always initiates the hopping process by sending the following required parameters:

- Mobile Allocation (MA): Set of frequencies the mobile is allowed to hop over.
- Hopping Sequence Number (HSN): Determines the hopping order used in the cell.
- Mobile Allocation Index Offset (MAIO): Determines which frequency of the HSN should be first used to transmit.

With this information the MS can apply an algorithm to compute which ARFCN is going to be used for the actual burst.

If SFH is enabled, signals hop every 4.615 ms (more than 200 hops per second). There are faster hopping algorithms such as Fast Frequency Hopping (FFH) where the carrier frequency is allowed to change more than once during a bit duration, but it is not implemented in GSM because it would greatly increase the costs of mobile equipment. Instead, in SFH all the bits in a burst are transmitted in the same frequency.

2.7 Power Control

Power control consists of modifying the transmitter output power in a communication system for optimal performance. In GSM, both the BTS and the MS can reduce the transmission power with three main goals: reduce interferences between nearby cells, extend the battery life of mobile phones and improve spectral efficiency (a high transmitting power translates into a lower frequency reuse).

If one side of the link is receiving more power than necessary, the other peer end should be warned to reduce the transmission power thus keeping a similar quality level on both sides. Broadly speaking, if the quality is good enough the transmission power should be

automatically decreased in order to reduce co-channel and adjacent channel interference as well as power consumption.

Uplink and downlink power control are independently controlled and depend on the hardware manufacturers. The control in both directions is managed by BSSs. In the uplink it computes the optimum transmission power according to the received signal strength level measured by BTSs. It also has to consider the maximum output power of the MS, but not the minimum power level as it is typically the same for all mobile phone classes. On the contrary, the optimum BTS transmission power for the downlink is computed considering the measurement reports that are regularly sent by GSM phones to BTSs.

When a connection is established on the air interface for the first time, the initial transmission power is also determined by the BSC but only taking into account the reception level of a single access burst. Afterwards the power levels will be adjusted as the phone moves closer or further away from the cell tower. When the distance changes significantly the base station sends a command to the cell phone to change the output power level without degrading the Signal-to-Noise Ratio (SNR). In this case the transmission level of the BTS could also be adjusted, but it is not so common.

2.8 Radio Interface

The radio interface between MSs and BTSs is also known as air interface or Um interface, and it is probably the most important of the entire mobile radio system architecture. As it has been seen in previous sections, on the air interface traffic and signalling information is transmitted using separate frequencies for the uplink and downlink channels. In order to reuse frequencies a TDMA scheme is also used, so physical channels are divided through both time and frequency.

Before being transmitted over the air, the MS has to convert the speech data into a digital signal of 104 kbps which is later compressed and encrypted with a specific session key. Then the packets are modulated with a GMSK modulation to be transmitted as radio waves, and when the signal reaches the other peer end the reverse process must be carried out in order to recover the original signal. Notice that it is necessary to encrypt the information transmitted in this interface as wireless communications are prone to eavesdropping. Consequently, to ensure the privacy of users and avoid unauthorized access to the network, SIM cards incorporate algorithms to generate the ciphering keys and mechanisms to perform subscriber's authentication.

The Um interface is not only used to transmit calls and SMSs but also to send technical information concerning the overall operation of the system. While physical channels are determined by time slots, there is another type of channels known as logical channels, which are determined by the information carried within the physical channel. These logical channels use physical channels not only to transfer users' data but also to send signalling information. Broadly speaking there are two classes of logical channels:

2.8.1 Traffic Channels

This first category of logical channels is exclusively used to transmit either digitalized speech or user data. Considering the issue of multiple access, we must differentiate between TCH/F and TCH/H standing for full-rate and half-rate respectively. The only difference is that a full-rate traffic channel (TCH/F) dedicates one slot per frame for a communication channel, while when operating at half-rate (TCH/H) the data will always be in a same time slot but at alternate frames.

Now that traffic channels have been defined, it is possible to differentiate the two possible operating states of GSM handsets. When a MS has a Traffic Control Channel (TCH) at its disposal (it is not possible to own a TCH at all times, only when necessary) , it is then described as being in “dedicated mode”, and otherwise it would be in “idle mode”. While being in dedicated mode, bi-directional transmission is possible through the TCH. Although even when the mobile is in idle mode it is constantly listening to the broadcast messages sent by cell towers, waiting for paging messages to be able to detect incoming calls and monitoring the radio environment to choose the BTS that offers a higher QoS.

2.8.2 Control Channels

The second and last category are a group of signalling channels that are critical for maintenance, such as network management and channel maintenance. They are used to establish and release calls, but also for information exchange between the MS and the BTS. Depending on their usage, this channels can be divided into the following categories:

- Dedicated Control Channels:
 - Slow Associated Control Channel (SACCH)
 - Fast Associated Control Channel (FACCH)
 - Standalone Dedicated Control Channel (SDCCH)
- Broadcast Control Channels:
 - Broadcast Control Channel (BCCH)
 - Frequency Correction Channel (FCCH)
 - Synchronization Channel (SCH)
 - Cell Broadcast Channel (CBCH)
- Common Control Channels:
 - Paging Channel (PCH)
 - Access Grant Channel (AGCH)
 - Random Access Channel (RACH)

All of them are important for system operation, but for efficiency issues control channels have to share time slots at different instants of time. By doing this, network operators can use the remaining time slots for traffic messages.

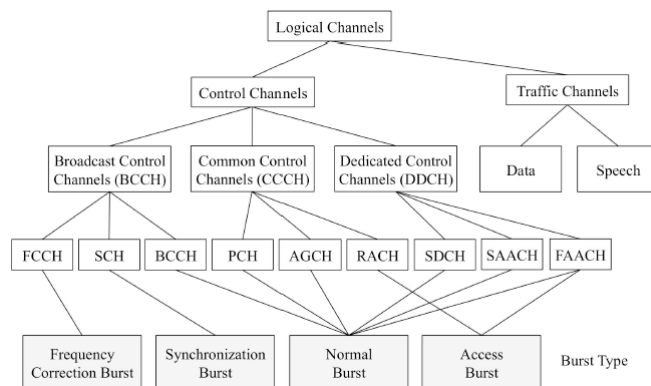


Figure 2.11: GSM logical channels. Source: [3]

Each GSM traffic channel comes with an associated bi-directional low rate channel called SACCH, which transmits two signalling messages per second in each direction. In the downlink, it is used to indicate the appropriate power level to the MS and also to provide timing advance information. On the other hand, it is also used in the uplink to carry the received signal strength, TCH quality information and measurement reports from neighbouring cells (really useful to make handover related decisions). In full-rate operation (TCH/F) a SACCH appears once in a multiframe, always using the same physical channel: the first time slot of the first frequency band. The SACCH can also be associated to SDCCH and FACCH, which will be explained in brief.

Messages to indicate the call establishment progress or to carry out subscriber authentication use the TCH instead. To be more precise, they use a special control channel (FACCH) that replaces speech data from a TCH by its own signalling information. To avoid confusing the receiver, two bits are reserved to differentiate data TCH messages from signalling TCH messages, which is the same as FACCH. This logical channel is used to send urgent signalling control messages such as handover commands, call setup and call disconnection.

Even when there are no incoming or outgoing calls, there is a need to stay in contact with the GSM infrastructure for call forwarding management or location updating. For this reason an additional channel called SDCCH is used to transmit bidirectional messages for a really short portion of time. This channel is one eighth of a TCH/F, meaning that it has the same characteristics as a TCHs but a much lower rate. This point-to-point signalling channel is also used both for the uplink and the downlink.

The next category, Broadcast Control Channels, comprehends all those logical channels that transmit data in the first time slot of various GSM frames, always in the downlink direction. All MSs must monitor the information carried on these channels every 30

seconds for proper performance. As time and frequency synchronization is crucial in a GSM network, two broadcast control channels are used by all base stations for this purpose: SCH and FCCH. Besides this, every two seconds an 80 octet message is sent in the downlink to idle mobiles using a special channel called CBCH, and BCCH is used to broadcast information related to the cell, a list of the channels that are currently being used within the cell and a list of neighbouring cells. This information is really important as MSs need to monitor surrounding cells to determine which are the most suitable ones.

Finally we have the Common Control Channels, which must be also frequently monitored by mobile phones. They are required for call origination and call paging procedures, in which the network finds out the mobile phone location before establishing a call. The channel used for paging is called PCH. It sends paging messages to all phones within a cell and warns them if they have an incoming call (the IMSI number is part of the message so that the addressee of the call can know that it is addressed to him).

Another important channel is the RACH. Unlike those mentioned so far, this unidirectional channel is the only one exclusively used for uplink communication. It is used to issue a request to BSS, so this messages are only sent when there is an interest to access the system, either because the user wants to originate a call or the device just needs to answer to a paging request from PCH. MSs choose their emission time on this shared channel in a random manner following the ALOHA access scheme, which results in collisions between phones that try to access the network at the same time.

This channel together with the AGCH (its analogue in the downlink channel) form the medium access mechanism to the air interface. The AGCH is used by base stations to answer channel requests sent by subscribers' handsets via the RACH. After listening to this channel, a MS will move to a particular physical channel with a particular dedicated control channel, and there it will be able to carry out different procedures: call setup, location area update or paging response. Apart from allocating a channel to the user, the base station also assigns a SDCCH for signalling during a call.

2.9 Mobility Management

2.9.1 Location Area

In a network where subscribers are in constant movement, it is a must to track their physical location for whenever it is necessary to reach them. It has been already explained that the GSM geographical area is divided into small cells (each of them covered by a single BTS) to provide good coverage and frequency re-use, so users are constantly moving from one cell to another without even realizing it.

To track subscribers efficiently, it was necessary to introduce the concept of "Location Area". A location area is formed by several base stations that are close to each other, all of them sharing a same Location Area Code (LAC). With the introduction of this

new concept, it is only relevant if a MS goes from one cell to another that belongs to a different location area. Every time a MS in idle mode, constantly listening to the broadcast channels, notices that the actual LAC has changed with respect to the previous update, it has to notify the cellular network via a location update procedure. Thereby, every time that there is an incoming call, the paging message will be only sent to those cells that are within the location area where the target MS is supposed to be according to its last location update request.

This entails a great improvement in terms of efficiency. If mobile reports were to be made every time that there is a change of serving cell, the battery life of the device would be shortened. The only advantage in that scenario is that the network would know which is the exact serving cell, so the paging messages for incoming calls would go directly to that BTS, without having to do a broadcast to the neighbouring cells within the same location area. The opposite method would consist in not sending any position report at all from MSs towards BTSs, but then the incoming call alerts must be sent to absolutely all the network cells. In the first case there would be too much location updates carried out, while in the second case an excess of messages addressed to the wrong cells would saturate the network. In conclusion, the intermediate solution used by GSM balances the amount signalling messages in both directions.

A particular case in which MSs have to do a location update is during IMSI attach or IMSI detach procedures, situations that occur when the MS is switched on or off respectively. In addition, MSs are forced to periodically report their location regardless of whether they are moving or not. The time between two periodic location updates is specified by a timer that is sent by the network through the BCCH, the default value of which is usually 60 minutes. The periodic updates happen infrequently in order to reduce battery consumption and the communication overhead.

2.9.2 Handover

The process of automatically transferring an ongoing call from one cell to another is commonly called handover. It is carried out to maintain the continuity of a call when a MS in dedicated mode leaves the radio coverage area of the cell in charge, i.e. when the signal strength is below the minimum required by the system. It is also executed in situations where the error rate is too large because of interferences or when the capacity of the serving cell is overwhelmed by a high number of connected subscribers. This process must be carried out without interrupting or deteriorating the service.

The main parameters to be taken into account during the decision process are the real-time measurements performed by the BTS in the uplink channel and the MS in the downlinks. Apart from that, it is also important to consider the traffic load, cell capacity and the maximum transmission power of all possible participants. Based on these parameters the network might trigger a handover to improve the service quality. For example, if a MS is switched to a cell with a lower path loss, it will contribute less

to the overall interference level by transmitting at lower power and the network would benefit. Another example is based on what happens when a big agglomeration of MSs congests a cell. In this situation the network forces some of them to change the cell, leaving room to other subscribers, even if it implies altering the frequency planning and increasing the interferences in the surrounding area.

As described in figure 2.12, there are two main types of handover processes:

- Inter-cell handover: The MS moves from one cell to another, whose BTSs can be controlled by a same BSC or not.
- Intra-cell handover: The MS remains in the same cell, but it is switched to a different channel less prone to interferences.

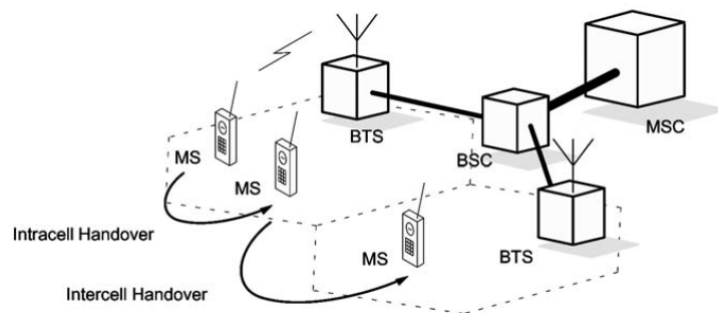


Figure 2.12: Inter-cell and intra-cell handover. Source: [6]

In any case, the handover decision is made by the BSC, who owns a list of candidate cells. The execution of a handover starts with the BSC sending a simple command to the MS right after deciding the future communication path. Next, the MS releases the old path in order to access the new assigned channel. Notice that a change of cell implies a change of frequency channel since frequencies cannot be reused in adjacent cells to avoid generating interference.

2.9.3 Roaming

Finally, the procedure of roaming is basic to enable mobile services to users that are outside the geographical area covered by their network operator. In other words, thanks to roaming, subscribers can benefit from GSM services while travelling as long as their mobile phones can operate on the frequency bands of the visited country.

To make roaming possible, it was necessary to standardize the air interface and the co-operation between network operators, who made international agreements to extend the coverage area of their clients worldwide.

Suggested Solution

3.1 Related work

The first reference for detection of mobile phone emissions dates back to the nineties, when a particular accessory for cellular phones became very popular. It was a simple pendant that emitted light every time that the telephone was receiving a call, alerting its owner visually. These devices were able to perceive incoming calls by detecting strong Radio Frequency (RF)-activity in the reserved uplink band of the GSM technology, taking advantage of the fact that MSs have to send signalling messages towards the base station during call establishment. This process starts right after receiving the first paging message from the network, which is why the pendant always brightened even before hearing the ring tone. The existence and former prevalence of these devices are an indication that detection of MSs is possible under certain circumstances, by simple means of using power detector circuits or equivalents.

Over time new possibilities to detect mobile phone emissions emerged as these devices were progressively making use of more telecommunication standards. However, using GSM signals for human detection is not really common, as other technologies such as WiFi or Bluetooth are usually the topic of research. For example, [7] proposes a method to sense pedestrian flocks by measuring the Radio Signal Strength (RSS) of WiFi packets emitted by their telephones. Applying clustering techniques in an indoor environment they are able to detect groups of people moving together. In [8] the authors choose to locate and track users with a RAdio Detection And Ranging (RADAR) system based on WiFi signals, but it requires a previous data-collection step to record information about the RSS measurements as a function of the user's location in the room.

With regard to Bluetooth, there are also projects where it is used for indoor positioning [9] but it is not the most appropriate technology to detect pedestrians as modern phones are able to hide themselves even while they are paired with another Bluetooth device. Furthermore, in [10] a pedestrian flow estimation system is made using both wireless communications systems (WiFi and Bluetooth) and the authors concluded that Bluetooth estimations were not accurate enough in comparison to the ones provided by WiFi packets. Because of this we cannot uniquely rely on this technology to build a sensor.

A sensor based exclusively on these telecommunication standards has certain drawbacks.

A big inconvenience would be that users can have this technologies disabled on their phones making them undetectable to this type of sensors, but also that both technologies are prone to interference as they operate in the globally unlicensed Industrial, Scientific and Medical (ISM) band. This implies that not the totality of signals in these bands are for telecommunication purposes, and thus not all the detected signals might imply the presence of a mobile phone user.

Other technologies such as Universal Mobile Telecommunications System (UMTS) or Long Term Evolution (LTE) do have frequency bands reserved for the exclusive use of cellular communications, but they are not present in all mobile phones and their use depend on whether the user has data to consume. They could be added features too, although working with standards that operate at such different frequency bands entails a considerable increase in hardware cost.

Nonetheless, it could be worth to combine various wireless technologies in order to take advantage of their different characteristics. A good example of this could be [11], where an hybrid system is made combining WiFi and GSM to improve the accuracy of an indoor location system. As the goal of that project is not to detect but to locate each MS, only those GSM messages that carry identity information are useful, hence they additionally use WiFi because they expect to have a rather low number of GSM measurements. In our case this will not be a problem because to determine if there is any GSM handset nearby we only need to see the corresponding activity in the RF spectrum, so all GSM messages being sent from the MS to the BTS can be exploited.

These two types of short-range signals and others like ultrasound or infrared are mainly used for projects that deal with indoor positioning, where the Global Positioning System (GPS) presents certain weaknesses that are not present in outdoor environments. Users can be located by triangulation using the RSS measurements provided by cheap hardware located in different known places of the room [8]. Although this can be a good solution to locate home inhabitants, it leaves much to be desired as a presence detector because of the drawbacks exposed in the previous paragraphs.

In the same line, the authors of [12] make use of wide signal-strength fingerprints to demonstrate that GSM is also a suitable solution for indoor positioning, obtaining accuracies comparable to WiFi-based location systems. In this case it is necessary to previously perform a training phase to measure the RSSs in all possible positions and additionally install certain software on the GSM handsets. Once the measurements are completed, the user's location can be computed by comparing the actual RSSs received by the phone with the signal strengths already measured in the training stage. However, the proposed approach excludes requiring active user collaboration.

In other cases, such as [13], the cooperation does not come from the user but from the network operator. In that particular example the goal was to locate mobile callers requesting emergency assistance, something that can only be done if you have access to the real infrastructure of base stations (which is assumed to be not possible in our case). Furthermore, the aim of our project is not only to detect those mobile phones that are

making a call or sending a SMS but also to find out if it is possible to detect those which are currently not being used.

Since apart from mobile operators no one has access to the network, some researchers try to detect mobile phone users simulating a BTS so that nearby devices would get connected to it instead of real base stations. Unlike years ago, nowadays it is possible to build such a system at a low price using a Software Defined Radio (SDR) peripheral and the appropriate open source software. One of the most widely used software for this purpose is called OpenBTS¹, a software-based GSM access point that allows radio amateurs to run their own GSM network, as it replaces the operator core network infrastructure from layer 3 upwards.

With the release of this software tools, researchers were encouraged to go one step further trying to reveal the information that is being transmitted over the air interface. According to [14], those devices that get connected to a fake cell-site can be forced to transmit unencrypted data, leaving the user's private information uncovered. However, an important drawback exposed in that project is that the MS has to be forced to operate in 2G because otherwise it would try to transmit data over faster networks, so it is necessary to jam both 3G and 4G frequencies to perceive relevant information. Nevertheless, this and related methods are not considered because of legal uncertainty, as jamming and telephone eavesdropping is strictly forbidden by law in most countries. Furthermore, it is not within the scope of this project to decrypt private user data as we are only interested in determining whether there is someone near the sensor or not.

Another well-known air interface analysis tool is the so called Airprobe². It is used in many GSM-sniffing projects that try to demonstrate how insecure the current standard is, although it has not been designed to analyse uplink traffic. Most of the times this tool, as well as OpenBTS, are used together with Wireshark in order to analyse the detected packets afterwards.

A project where all this resources are put into practice is [15], which is very similar to the proposed approach as it is focused in the uplink channel instead of the downlink, and additionally it does not require the cooperation of end-users or network operators (passive receiver). Besides this, it is only focused on the unencrypted messages so no illegal practices are carried out. In this project a passive wideband receiver captures, processes and analyses the GSM radio signals coming out from a MS while being in synchronization with the end-users in the time and frequency domains. An active system running at any end of the link would have access to the Frequency Correction Bursts (FBs) and Synchronization Bursts (SBs) that the BTS periodically sends to stay synchronized with the MS, but the challenge of building a passive receiver able to capture and parse GSM signals consists in being synchronized without having access to these messages. Achieving this is one of the main goals of that project, but again it is not relevant in our case, as we do not intend to reconstruct the messages from the captured radio signals. In our

¹<http://openbts.org/>

²<https://svn.berlin.ccc.de/projects/airprobe/>

case, the main goal will be finding a way to detect the almost undetectable GSM signals that are transmitted by cellphones, which always operate at the lowest possible power level to avoid interfering other subscribers. It would be much easier to look for the strong RF-activity that emerges during a call establishment, but a sensor only able to detect calls would have many less practical applications.

Finally, another line of research is the feasibility of using GSM-based passive RADARs, which have some advantages over active RADARs like being smaller, cheaper and undetectable. This approach considers the possibility of detecting and tracking moving objects with a multi-static GSM-based passive RADAR. Previous studies proved that non-cooperative signals such as commercial radio or TV broadcast could be used as RADAR signals, which is why in [16] the possibility of using GSM as illuminator of opportunity is studied. The idea of those projects is to use one antenna to receive the downlink signal emitted by a known BTS and a second identical antenna to detect the echo coming from the target's position. This type of systems are mostly used to detect ground-moving vehicles such as cars, but in [17] they are able to do human motion measurements. It must be said that these systems are designed for very specific situations, e.g. a very long straight road, so the set up cannot be done anywhere. Despite that this is not the optimal solution to our problem, as we intend to make a GSM sensor that detects both standing and moving pedestrians in different environments, there is a relation with those projects as both consist of detecting moving targets by looking at the GSM spectrum, which is similar to the proposed approach.

Considering that every MS has to be always in contact with at least one base station, it should be possible to detect mobile phones in idle state. However, this preliminary research has shown that the methodological contributions to this particular topic are very scarce. Keeping in mind that the thesis' approach is to build a passive GSM receiver for the uplink channel within the framework of legality, none of the methods found in literature meets all these characteristics; in most of the cases either antennas listen to the downlink channels, users participation is required or illegal practices are carried out.

3.2 Concept for passive GSM detection

The aim of this section is to depict a first approach to the problem posed by this thesis and expose the main difficulties that it entails. At any case, unexpected problems that may arise during the implementation process will be reflected in chapter 4, where the preliminary idea will be put into practice.

Broadband scanner

Passive detection is intended to be achieved in this project, so physical interaction with the GSM handsets or users' collaboration are not an option. Being a mere spectator entails a lack of knowledge of the exact frequencies where transmissions are going to take place, since the ARFCN values to be used are decided by the network and sent over the air interface towards MSs via encrypted signalling messages. This is a big inconvenience for signal detection, since it is not possible to look at a whole GSM band at once because of hardware limitations: the actual bandwidth depends on the number of samples per second that our equipment is able to provide. As it is stated by the Nyquist-Shannon theorem, the sampling rate must be at least twice the bandwidth to avoid the irreparable effect of aliasing. Then, taking as example the Austrian GSM uplink spectrum, a total bandwidth of 100 MHz has to be analysed. This is rather impossible to do at once with nowadays' medium-priced receivers, so alternative ways must be conceived to overcome this first impediment.

ARFCNs prediction

One way of minimizing the problem would be to estimate the possible ARFCNs that could be used by nearby phones. As two characteristics of the GSM technology are that MSs get connected to the BTS that offers a better service and that the frequency distance between the uplink and downlink carrier frequencies is fixed (see section 2.3), the uplink frequencies that are being used to transmit by nearby phones should be associated to the strongest downlink channels seen by our GSM sensor. Hence, uplink channels can be computed just by subtracting the duplex distance to the most powerful downlink channels while ARFCNs can be calculated applying a simple band-dependant formula.

It could be said that it is a way to reduce the possible ARFCNs that might be used by nearby phones. With this knowledge, the potential frequencies to be used as uplink channels are greatly reduced, and as a consequence the sensor can perform a more precise narrow-frequency analysis in the bands of interest without having to sweep the whole band.

Then, a previous step to uplink detection must be the scanning of the whole downlink band looking for the strongest broadcast channels. The activity in such band has little to do with what can be discerned on the uplink; In the first case the occupancy is much

higher and stable as base stations are constantly broadcasting control messages over the Broadcast Control Channels, which are easier to detect than the short-lived messages emitted by cell phones.

Discrete step scanning

However, to scan the GSM downlink band from beginning to end there is a need to sweep the whole bandwidth in different stages, retuning the receiver to a new frequency at each step. The lower the sample rate the more spectrally narrow steps are required. This implies a considerable loss of samples as there is an interval of time during tuning in which samples have to be discarded due to the synchronization issues (during the transition time it is not possible to discern samples obtained from the old and new frequencies). Apart from that, it is important to use a rather high sample rate as the signalling messages sent by MSs to cell towers are not constant but intermittent. It means that an uplink signal would remain unnoticed if the receiver is not tuned at the appropriate frequency at the exact instant of time. But using a high sample rate is not enough to reduce the probability of missing the presence of such signals, as it has a lot to do with how fast the whole band is scanned and this is directly related to the processing time.

Resolution

To perform analysis in the frequency domain it is necessary to apply a Discrete Fourier Transform (DFT) to the input data, or alternatively a Fast Fourier Transform (FFT) for greater efficiency. The frequency resolution of the transformed signal is the result of dividing the sampling rate by the FFT size. According to this, just increasing the sampling rate implies a loss of resolution, which could be very detrimental for weak signal detection. This resolution, expressed in Hertz/bin, could be improved by increasing the number of bins, but this would entail a greater computational load and consequently a longer processing time. So there is trade-off between these two parameters, considering that the hardware used will have a lower and upper limits in terms of sampling frequency.

There are obviously more technical considerations which cannot be overlooked, but these will be addressed in chapter 4.

3.3 Hardware and Software tools

To conclude this chapter, this final section intends to describe the different hardware and software tools that will be used for the implementation process. It basically includes a radio receiver and a popular open-source software to interact with it.

3.3.1 Software Defined Radio

Software Defined Radio (SDR) is a wireless communication system in which all radio components are implemented by means of software instead of traditional hardware. The official definition provided by the SDR Forum and the IEEE P1900.1 Working Group is as follows:

"Radio in which some or all of the physical layer functions are software defined"

In other words, it solves the problem that researchers had three decades ago, when they would have to spend large amounts of money in hardware (filters, mixers, amplifiers, modulators...) and a lot of time putting all these components together, without mentioning the high technical skills that it required. Since the introduction of SDR, all these components can be implemented in software, so modifications do not require physical intervention anymore.

All in all, SDR offers an easy and cost-effective way to work with radio receivers, which makes it a perfect tool for product developers. This efficient and inexpensive solution enables rapid prototyping in communication projects because just by reconfiguring the software it is possible to use a same hardware for multiple applications.

In particular, SDR was suitable for this project because it allows multi-band operation. Before SDR you had to choose a specific band and resort to specialized hardware, but now with a generic hardware you can do frequency selection and filter using different bandwidths. So nowadays it is possible to tune a SDR peripheral into different frequencies instead of using a fixed narrow frequency band as it was done in the old days of radio communications. This versatility is especially important for a project based on GSM because this technology uses several frequency bands.

And last but not least, another important asset of SDR is multi-functionality. Wireless systems employ different protocols, for this reason a device as common as a mobile phone has to use a number of special-purpose chips to deal with different radio standards. This is not the case of SDR peripherals because they work with raw electromagnetic signals, and just by launching the right software they can address a wide range of uses simultaneously. This could also be important for the presented project as presence detection can be achieved making use of different wireless technologies, and SDR provides the required flexibility to support multiple waveform standards.

3.3.2 HackRF One

Once one opts for SDR the next step is to decide which is the most appropriate hardware to use. Despite the fact that software has the main role when dealing with software defined radios, the hardware is still important in the overall design because it will impose the limits of what can be done with the software.

The design of SDR peripherals is not simple, since the controlled functions need to be as close as possible to the antenna in order to provide more software control. The user should be able to tune the device at any frequency band, select a desired bandwidth and modulate or demodulate different types of signals without even touching the device itself. To enable this, a generic hardware should present the following scheme:

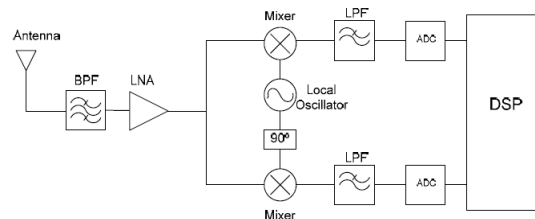


Figure 3.1: Block diagram of a Software Defined Radio receiver. Source: [18]

First of all, the input signal goes through a wideband preselect filter that provides most of the out-of-band rejection. In the next stage a Low Noise Amplifier (LNA) increases the amplitude of weak signals, slightly increasing the signal power without degrading the SNR. Then a mixer translates the RF signal to Intermediate Frequencies (IFs), using a local oscillator to tune the device at the desired frequency. Despite not appearing in the picture, before the mixer there is often a narrowband filter that suppresses nearby out-of-band interferences at the mixer image locations that would fall into the IF passband. Next an IF amplifier could be used to enhance the dynamic range, together with an anti-aliasing filter that limits the noise and distortion contributions from the IF amplifier and filters the Analog-to-Digital Converter (ADC)'s alias bands. In the last stage there is an ADC, which is probably the most important component of the circuit because it samples the input analog signal and turns it into digital bits. Those bits are sent to the Digital Signal Processor (DSP) unit, where the information is processed using the algorithms implemented by software. An alternative accepted option is to send the RF signal directly to the ADC after amplification, without tuning it to an intermediate frequency.

Notice that in this way a generic hardware can be used for a wide range of projects, since its behaviour entirely depends on the instructions received from the processing unit. That is why in the previous section the idea of flexibility was mentioned: unlike conventional radio systems, if the modulation scheme changes there is no need to modify the hardware as it is enough to load a new software to the DSP module.

There are several SDR peripherals available in the market with prices ranging from tens to thousands of euros, so choosing one is not a decision to be taken lightly. The main

features that one should take into account to make the right decision are listed below:

- Capability to transmit. Some devices are able to do it apart from receiving.
- Frequency range: Range of frequencies that can be tuned.
- Bandwidth: High bandwidths implies analysing a bigger part of the spectrum at once and more software decimation (better SNR), but it requires more Central Processing Unit (CPU) power.
- Sensitivity: The greater the sensitivity the grater the ability to hear weak stations and produce high SNR values.
- ADC resolution: The higher the bit size of the ADC, the more accurate it can be when sampling. It is directly proportional to the dynamic range and sensitivity. In addition, a high resolution implies a better ability to discern weak signals, less signal imaging and a lower noise floor.
- Dynamic range: Ability to receive weak signals when strong signals are nearby. It is strongly related with the ADC resolution and the DSP software processing. When the dynamic range is not high enough, a strong signal can saturate the ADC, generating signal images and significantly reducing the receiver's sensitivity. This situation is known as "overloading" and it leaves no space for weak signals to be measured.
- System design: The number of lossy components that are part of the RF path affect the receiver performance.
- Noise and Interferences: The circuit board of the device should not generate interfering signals because those would be impossible to remove.
- Preselectors: Analog filters on the frontend that reduce out of band interferences and imaging. The device can switch between different preselectors depending on the tuned frequency.

Taking all this into consideration, together with the price and available software, the hardware chosen for this project was the HackRF One. Some of the main advantages of this device are its incredibly wide bandwidth (offers a maximum sample rate of 20 MS/s) and a frequency range that covers almost all currently prevalent digital radio systems (from 1 MHz to 6 GHz). Another important characteristic that makes a difference with other similar-price devices is its transmitting capabilities. In any case, this is not an important feature for us because our prototype will be only focused on reception, but it could be a plus for other projects in the field of radio communications.

On the other hand, there are concerns about its rather low resolution. The ADC works with 8-bit data width while there are competing products with 12-bit ADCs. The main

consequence of this, as discussed earlier in this section, is a loss of accuracy to discern weak signals and a reduction of the dynamic range (48 dB). To increase this value and thus reduce the possibility of overloading some type of RF filtering should be applied.

Probably the other drawback that we could highlight is that, in order to operate in such a wide range of frequencies, the RF chain has some extra diode switches. The small losses introduced by these electronic components can reduce the device's sensitivity, but at the same time the presence of switches at the critical junction points gives to the HackRF a high flexibility to choose the signal path.

It is true that there are a couple of SDR peripherals in the same price range as the HackRF (i.e. AirSpy and SDRplay) that use 12-bit ADCs, but their sample rates are much lower and their frequency range is noticeably narrower. This could be a problem considering that an improved version of the sensor could make use of other technologies from higher frequency bands (i.e. WiFi or Bluetooth). So maybe the HackRF does not have the best reception specifications, but it means that if we are able to make a sensor that works using a 8-bit ADC device it should also work in any other peripheral that uses a more accurate converter.

For further information about the HackRF's specifications, please refer to Annex I (5.2).

3.3.3 Low Noise Amplifier

A Low Noise Amplifier (LNA) is an electronic amplifier typically used in communications systems to strengthen the input signals without significantly degrading the SNR. These components provide voltage gain to subsequent stages without adding too much compromising noise, as they are designed to minimize their own additional noise to avoid masking the real signal. It is intended to improve the detection range of the sensor by increasing the SNR of the signals entering the HackRF.

This low-powered component is a critical interface between any antenna and electronic circuit, but the HackRF already has an internal LNA so one could think that there is no need for an additional one. However, it all has to do with properly placing the LNA so that it can be really effective. According to Frii's formula [19] the first stages of the front end are critical to determine the overall Noise Figure of the receiver, and many studies show that an LNA next to the antenna is much more effective than anywhere else. The reason is that in this case the signal levels are higher since the beginning (before being attenuated along the signal path) and as a consequence they are degraded to a lesser extent.

Usually by placing a preamplifier next to the antenna the noise floor is reduced without compromising the linearity of the system. However, with LNA equipped receivers (like the HackRF) linearity can be degraded so that even moderate interferences can desensitize the receiver. So, the advantages and disadvantages of using such hardware together with the HackRF remain to be analysed.

The model chosen for this project is called LNA4ALL (see figure 3.2), a cheap preamplifier valid for many applications from 28 MHz to 2500 MHz. This 20€ gadget should lower the Noise Figure of the HackRF and improve its sensibility.

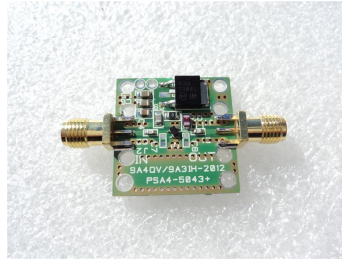


Figure 3.2: LNA4ALL printed circuit board. Source: [20]

According to the manufacturer’s website [20], a couple of hardware modifications must be made to use the HackRF phantom power. The LNA performance could be slightly altered, reducing its linearity while the noise factor is improved. Apart from that, the website also warns about a high risk of damaging the device with static electricity, so it is important to use it very carefully as it can endanger the whole system by releasing too high currents.

3.3.4 GNU Radio

In the realm of SDR the software represents the signal processing engine while the hardware provides the RF front end. In our case, the software that will provide the necessary drivers to allow interaction between the HackRF One and the host system is called GNU Radio.

GNU Radio is a free software development toolkit widely used in the field of software defined radios. First published in 2001 as a fork of a MIT-originating framework called PSpectra, GNU Radio is by far the most popular SDR development toolset at the moment. This signal-processing package is copyrighted by the Free Software Foundation and is part of the GNU project, which means that it is distributed under the terms of the GNU general public license.

The GNU Radio framework enables users to design real-world radio systems in a very intuitive way using general purpose computers. It comes with an extensive library of processing blocks which implement standard algorithms and functions (such as encoding, modulating, mixing, filtering, equalizing or packet handling), and just by properly combining them the user can create what is commonly known as a ‘flowgraph’ (series of connected signal processing blocks). Figure 3.3 shows the appearance of a typical flowgraph displayed in GNU Radio’s Graphical User Interface (GUI).

The flow of data through the flowgraph is managed by the program, so the user only has to worry about setting the right parameters at each block. Notice that it is not mandatory

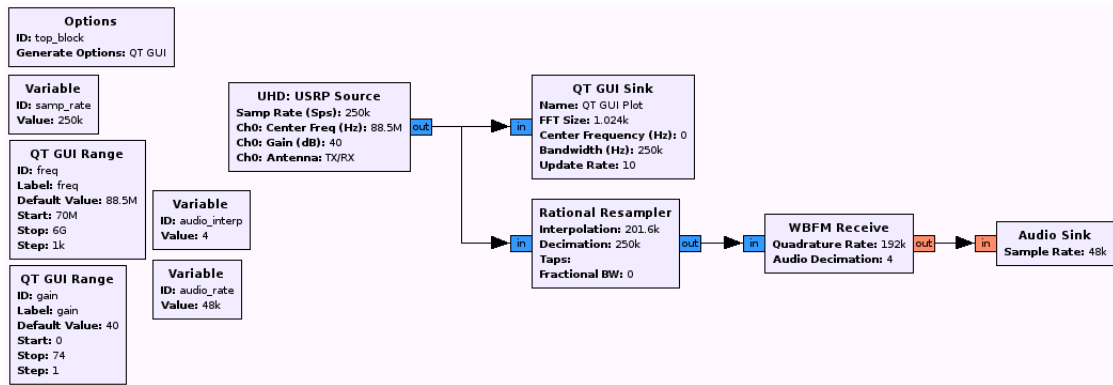


Figure 3.3: Flowgraph of an FM receiver. Source: [21]

to connect a SDR peripheral on the host computer; GNU Radio can be executed in a simulation mode as some of these easy-to-use blocks are signal generators. There are also blocks that allow plotting and data visualization, such as FFT displays or constellation diagrams. This allows the creation of a user-interface for the final application which can facilitate the user's understanding of the results.

This GUI used to develop GNU Radio applications is called GNU Radio Companion (GRC), which in fact is a Python code-generation tool. It generates a Python code for each flowgraph in which all the required blocks are defined as well as the connections between them. The main advantage of GRC generating those project files is that they can be modified by users to do things that cannot be done by simply interconnecting GNU Radio's blocks. For instance, a simple "if-then-else" statement can be written in code but not represented in a flowgraph. Apart from giving a lot of freedom to the programmer, working with Python also provides access to lots of standard libraries with built-in modules that can be of great utility.

However not the entire GNU Radio code is written in Python. In fact, all the infrastructure of signal processing blocks is written in C++ while many of the user tools are written in Python. The reason is that to achieve real-time processing it is preferred to use an efficient precompiled language like C++, which gets compiled directly into the processor instructions leaving the minimum work to be done during run time. So it could be said that the most heavy and performance-critical signal processing tasks are implemented in C++ while the creation of flowgraphs is done with Python, which is a much simpler and user-friendly development environment.

If the signal processing blocks provided by GNU Radio are not enough, the user is free to create his own blocks programming either in Python or C++. There are no compatibility issues between these two programming languages because the C++ blocks can be easily used in Python code. Therefore, when implementing the suggested solution, we will quickly change the GNU Radio environment by Python, as the second option gives much more freedom to perform tasks.

3.3.5 Operating System

All the tests are performed on a Pentoo Linux virtual machine running on a 64-bit computer. This Linux distribution not only presents a great compatibility with the chosen hardware but also includes many SDR tools by default, making it the first choice for many SDR researchers. Although it is possible to install GNU Radio in a Windows environment, this combination was not considered as it is extremely prone to issues and not supported by the GNU Radio community.

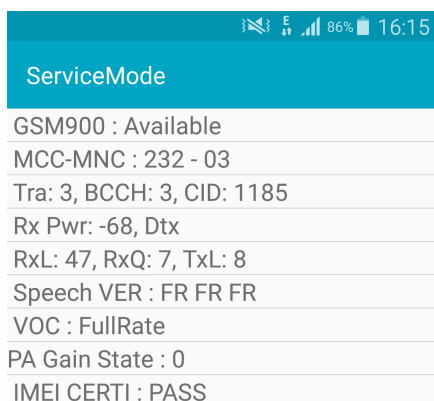
A switch to a more energy-efficient platform is possible (i.e. Raspberry Pi), once the intended functionality of the software has been shown.

Implementation

4.1 Acquiring Network Information

In order to perform tests it is necessary to dispose of a mobile phone able to provide network information, otherwise it would be difficult to discern if the software is detecting the test equipment or other GSM handsets that are nearby. To know if the test MS is being detected, it is necessary to know its frequency channel. So, for this project it is especially important to obtain the ARFCN value assigned to the testing device at each instant of time. Without knowledge of this number, results would be almost meaningless, being impossible to discern if the detections are due to the tested MS or because of other subscribers' activity.

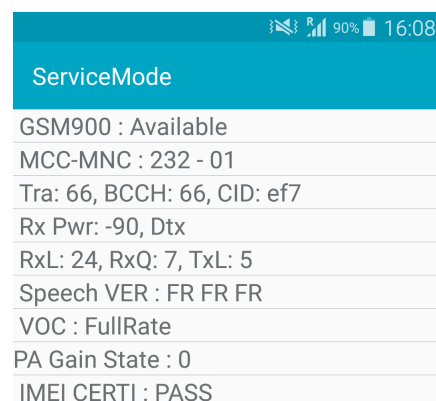
Two phones have been used for testing purposes: a Samsung Galaxy S4 and a OnePlus 2. In the first device it is possible to obtain network information just by entering the sequence `"*#0011#"` on the dial-pad, a Samsung-code that enables the Service Mode menu where ARFCNs can be found among other values. But the vast majority of phones do not have a default code to provide such information, as it is the case of the second device.



The screenshot shows the Service Mode menu for a Samsung device connected to T-Mobile. The status bar at the top indicates 86% battery and the time 16:15. The menu items are as follows:

ServiceMode
GSM900 : Available
MCC-MNC : 232 - 03
Tra: 3, BCCH: 3, CID: 1185
Rx Pwr: -68, Dtx
RxL: 47, RxQ: 7, TxL: 8
Speech VER : FR FR FR
VOC : FullRate
PA Gain State : 0
IMEI CERTI : PASS

(a) Serving cell from T-Mobile



The screenshot shows the Service Mode menu for a Samsung device connected to A1 Telekom. The status bar at the top indicates 90% battery and the time 16:08. The menu items are as follows:

ServiceMode
GSM900 : Available
MCC-MNC : 232 - 01
Tra: 66, BCCH: 66, CID: ef7
Rx Pwr: -90, Dtx
RxL: 24, RxQ: 7, TxL: 5
Speech VER : FR FR FR
VOC : FullRate
PA Gain State : 0
IMEI CERTI : PASS

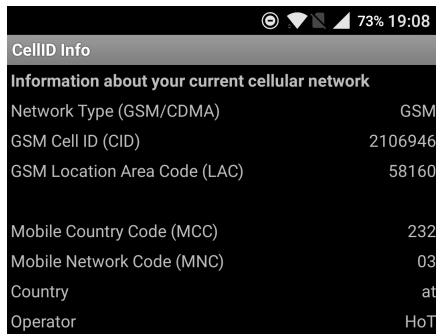
(b) Serving cell from A1 Telekom

Figure 4.1: Samsung's Service Mode menu

Figure 4.1 shows an example of the Service Mode menu, where the most important information is concentrated in the very first lines. The top line indicates which GSM band is currently being used, while the second one displays the Mobile Country Code and the Mobile Network Code. The country code is 232 in both cases as the device was within the boundaries of Austria all the time, but the network code varies because the screenshots were made using SIM cards from different network operators: In the first case the device was connected to a BTS from T-Mobile (figure 4.1a) while in the other case it was using a A1 Telekom tower (figure 4.1b). But the most relevant information is visible in the third line, where under the name of BCCH the actual ARFCN value is displayed. With this information, it is possible to obtain the uplink and downlink frequencies with a simple calculation. For example, the frequencies associated to the ARFCN from figure 4.1a can be calculated as follows:

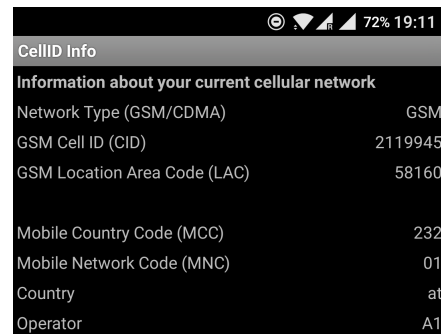
$$\begin{aligned}\text{Uplink Frequency (MHz)} &= 0.2 * \text{ARFCN} + 890 = 0.2 * 3 + 890 = 890.6 \text{ MHz} \\ \text{Downlink Frequency (MHz)} &= \text{Uplink Frequency} + 45 = 890.6 + 45 = 935.6 \text{ MHz}^1\end{aligned}$$

In MSs unable to access this menu, an external application can be installed to obtain information about the serving cell, but not the ARFCN value. The screenshots from figures 4.2a and 4.2b show the information displayed in this case.



CellID Info	
Information about your current cellular network	
Network Type (GSM/CDMA)	GSM
GSM Cell ID (CID)	2106946
GSM Location Area Code (LAC)	58160
Mobile Country Code (MCC)	232
Mobile Network Code (MNC)	03
Country	at
Operator	HoT

(a) Serving cell from T-Mobile



CellID Info	
Information about your current cellular network	
Network Type (GSM/CDMA)	GSM
GSM Cell ID (CID)	2119945
GSM Location Area Code (LAC)	58160
Mobile Country Code (MCC)	232
Mobile Network Code (MNC)	01
Country	at
Operator	A1

(b) Serving cell from A1 Telekom

Figure 4.2: Cell information provided by CellID Info application

As this information includes the LAC (set of BTSs grouped together to optimize signalling), it is possible to locate the serving cell towers consulting public information available on the internet. Figure 4.3 shows the distance between the MS and its two favourite BTSs in the location where the tests take place. It does not mean that it is all along connected to these BTSs; in some occasions it may switch to others depending on the network's state.

¹The formulas would be different if the MS is connected to another GSM band (i.e. GSM-1800).

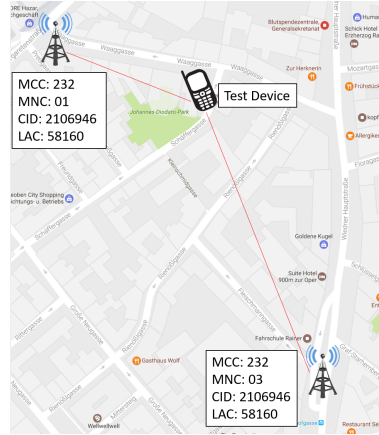


Figure 4.3: Map showing the positions of the serving BTSs, obtained from [22]

4.2 Detection in idle mode

4.2.1 Overview

The large amount of information broadcasted by base stations make the downlink channels extremely active. The reason is that all four Broadcast Control Channels are required to transmit continuously at full power so that MSs can be in synchronization with the network. This is why mobile phones listen to the broadcast channels in a matter of seconds. The waterfall of figure 4.4, placed under the plot where some GSM-900 downlink frequencies are displayed, illustrates that the downlink channels are always in use with a high level of transmission power in comparison to the noise level.

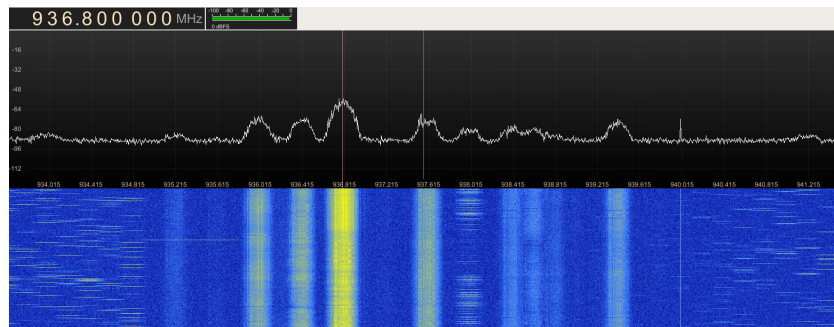


Figure 4.4: GSM-900 downlink channels, captured with GQRX

The graph makes it clear that it should be possible to detect these channels with the right software running on a SDR peripheral. Taking the example from the picture, the software should return the frequency of the strongest channel (936.8 MHz) and others of interest like 936.4 MHz or 936.0 MHz. It is true that if the HackRF was a MS it would definitely chose the carrier frequency of 936.8 MHz, but it is important to remark that such frequency belongs to a specific network provider, so a cell phone with a SIM card from another company would not be able to use that carrier frequency. Then, in order to detect any phone regardless of its network provider, it is a must to select the frequencies of various channels that can potentially be used in the area.

The Python script named `downscan.py`² that implements this logic is based on the open-source code `usrp_spectrum_sense.py`³.

The second step to detect idle MSs would be to make use of Python packages and libraries to perform a more accurate analysis in the bands of interest. Once the possible uplink channels are known, it should be possible to perform a FFT of higher resolution and statistically analyse the output samples to detect even the weakest and short-lasting signals. However, this second part of code has not been implemented for being infeasible as will be explained later in this section.

4.2.2 Parameters

The command `"downscan -h"` prints all the information regarding the input parameter on the Terminal. The output of the help command shows all the configurable options of the implemented script. For proper operation it is essential to choose appropriate input parameters, so the aim of this section is to explain the decision process behind the selected values.

Sample rate

This value should be between the limits imposed by the HackRF, which are a minimum sample rate of 2 MHz and a maximum of 20 MHz. Besides this, the maximum rate that can be handled by the host computer has to be considered too. This value can be discovered by running the command

```
hackrf_transfer -r /dev/null -s SAMPLE_RATE
```

on a Terminal while the HackRF is attached via USB port. This will display the real speed of the data transmission once per second, so if the printed values are below the chosen sample rate, it is because there is a hardware limitation. The command must be

²<https://gitlab.auto.tuwien.ac.at/ptraich/sdr-gsm-detector>

³http://gnuradio.org/redmine/projects/gnuradio/repository/revisions/9880e7bb383054aa43681b52ebd33c8fd4cb8fcb/entry/gnuradio-examples/python/usrp_usrp_spectrum_sense.py

executed as many times as necessary until the real maximum sample rate of the computer is found based on trial and error. The computer used for testing purposes has shown to perform well at 20 MHz, so in this case the limitation comes from the radio receiver.

Once the upper and lower limits are known, to choose a specific value some technical things must be considered. First of all, the Nyquist-Shannon theorem is applied in a particular way in complex sampling receivers like the HackRF. Unlike real sampling receivers, where the bandwidth is half the sample rate, for the HackRF both values are equal. So, choosing a sampling rate of 10 million samples per second implies being able to display 10 MHz of spectrum at once.

Bandwidth

This parameter should be set to 200 kHz as this is the bandwidth of a GSM channel. As this is the default value, there is no need to specify it from the command line.

FFT size

This value must be a power of two as it is a requirement of the Fast Fourier Transform (FFT) algorithm. It should be as large as possible to have a good resolution in the frequency domain without compromising performance due to the increases of the processing time. Values like 1024, 2048 or 4096 are considered correct for the case under study.

Tune delay

This parameter is important in terms of synchronization with the radio receiver. Every time that the script sends a command to the HackRF's daughterboard ordering it to change its center frequency, it is necessary to wait until the right samples arrive at the FFT engine. Not waiting would suppose using samples from the last center frequency, because there are many delays along the digitization path that prevent the tuning from being immediate.

To overcome this problem, some data has to be discarded during a period of time specified by the "tune delay" parameter. After that time the samples entering the FFT block should belong to the requested center frequency. In fact, while tuning, there are some transients generated by oscillator energy leaking into the receiver that make data useless for a short period of time.

Despite it is a configurable input parameter, it was decided to use the default value (0.25 seconds) as the results obtained with it were quite accurate.

Number of downlink channels

This variable is used to determine how many frequencies the user wants to have stored by the end of execution. To decide the right value, the number of network providers that operate in the area must be considered (in the case of Austria there is T-Mobile, A1 Telekom and Hutchinson Drei Austria). If there are many network providers, this parameter should be higher, as the possibility of having a MS not connected to the downlink channels with strongest signal is increased.

Considering that a MS in idle mode is constantly monitoring the activity of the six strongest BTSs to know which is the most adequate at all times, the number of downlink channels to be found should be not more than six times the amount of network providers in the area. However, as the base stations from the test location are not overloaded by a high number of subscribers, the GSM handsets rarely get connected to the last cells of their lists. Hence, there is no need to store so many frequencies.

Gains

There are three different configurable gains when using a HackRF One in receiver mode:

- IF Gain: From 0 dB to 40 dB in steps of 8 dB.
- Baseband Variable-Gain Amplifier: From 0 dB to 62 dB in steps of 2 dB.
- RF amplifier: It can be turned ON (14 dB) or OFF (0 dB).

Those are probably the most important parameters to detect radio channels. If they are not set correctly, even the strongest channels can be undetectable. In addition, they can be the source of many interferences such as intermodulation products. To find out the best combination, experiments with GQRX were performed. This software allows the user to play with the different gain settings while seeing how the changes affect at the perceived spectrum. After trying multiple combinations, it was decided that the best option was to leave the RF amplifier disabled (it was the source of spurious emissions) and the baseband gain to 20 dB (for higher values the signal and the noise were equally increased). As for the IF gain, it was concluded that for downlink detection it should be set to its maximum value (40 dB) while for uplink detection it was better to keep it to a minimum (0 dB).

Execution example

With everything explained so far, it is possible to execute the program with certain criteria. An example of execution is displayed below:

```
downscan -a hackrf -s 10000000 -b 200000 -F 1024 -N 5 935000000 960000000  
> output_down
```

In the example above, a sample rate of 10 MHz and an FFT size of 1024 bins is being used aiming to find the five strongest downlink channels (and uplink by association) present between 935 MHz and 960MHz. Notice that the default values will be used for all those parameters that are not specified by the user (i.e. the bandwidth, the tune delay and the three configurable gains).

The first argument is used to indicate which receiver is attached to the host computer (HackRF), while the last numbers indicate the initial and final frequencies to be scanned. The frequency range entered covers only the GSM-900 downlink band (from 935 MHz to 960 MHz), leaving aside GSM-1800. Tests will be focused in GSM-900 as the procedure would be the exactly the same to scan the GSM-1800 band.

The results of the script can be found in the text file that is automatically generated in the working directory, called “output_down” in this case.

4.2.3 Methodology

The Python script basically tunes the HackRF’s frontend in suitable steps in order to examine a larger part of the spectrum, since it is impossible for the SDR periperhal to examine the whole GSM bandwidth at once. So, the code works as a frequency scanner that recursively performs FFTs of portions of the spectrum. After each transformation, the resulting FFT frame is analysed looking for the strongest GSM downlink channels.

After importing the required libraries and saving the input parameters into local variables, a handful of instructions are used to define the GNU Radio flowgraph. The required blocks are created, configured according to the input parameters and interconnected for proper operation. The main blocks used are a signal source from the osmoSDR⁴ project that allows interaction with the HackRF (the block’s output is the data sent by the receiver via USB connection) and another block that computes the FFT of the sequence provided by the aforementioned block. Finally, a special block to control the tuning of the HackRF and record frequency domain statistics is used, as well as other auxiliary blocks responsible for carrying out data type conversions. Information regarding GNU Radio blocks can be found at [23].

⁴<https://osmocom.org/projects/sdr/wiki/GrOsmoSDR>

Something to emphasize is that, before moving to the frequency domain, there is a need to apply a temporal window to the signal. It is done because the FFT mistakenly assumes that the input signal is periodic and of infinite duration, and this causes discontinuities in the time domain between the last sample of a period and the first repeated sample of the next one, which is translated in artefacts in the frequency domain. This effect is known as “frequency leakage”, and it can be reduced using the overlapping technique; a method that consists in overlapping the last data points of a FFT frame with the first ones of the next frame, as displayed in figure 4.5.

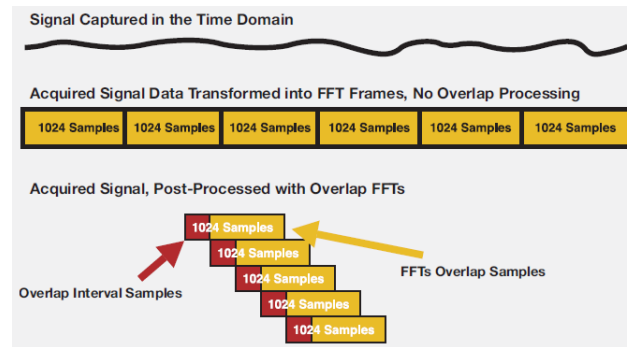


Figure 4.5: Overlap FFT processing. Source: [24]

The code uses a Blackman-Harris window and an overlapping of 25%, meaning that 12.5% of the samples are discarded at both sides of the FFT frames. This is equivalent to see less spectrum at every step, as if the sample rate was smaller than it really is. For example, if the selected sample rate is 10 MHz, the frequency steps used by the program would be of 7.5 MHz instead of 10 MHz and, consequently, the number of steps required to scan the whole GSM band will be slightly higher.

At each “step” the receiver is tuned at a different frequency and the FFT block provides a number of samples (commonly known as bins) that depends on one of the input parameters: the FFT size. The greater this value, more bins will be obtained as a result. Furthermore, the FFT size determines the spectral resolution of the transformed signal, which is computed dividing the sample rate by this value. It means that, for a given sample rate, narrower bins are obtained by increasing the FFT size.

Assuming that a FFT size of 1024 bins is being used, and that each transform is being made on 10 MHz of the spectrum with a 25% overlap as said in the previous paragraph, the first and last 128 bins are discarded. So, only 768 bins are left representing a spectrum of 7.5 MHz (25% of the total bandwidth). As the GSM standard uses channels of 200 kHz, the total 768 bins have to be divided into groups of 200 kHz each. The number of bins that comprise a GSM channel can be easily found dividing its bandwidth (200 kHz) by the bins resolution ($10\text{M}/1024 = 9765.625 \text{ Hz/bin}$). With the values of the given example, the total FFT output would be divided in groups of 21 bins that would have to be analysed separately.

After performing all these calculations, the script defines two arrays where the power and frequencies of the downlink channels will be stored. For each group of 21 consecutive bins the total power is computed as the sum of each bin's spectral power. This result is then compared against the array of powers, and replaces any entry which has a lower value. Its associated frequency is stored in the same position of the second array. This way of computation was chosen, instead of simply looking for parts of the spectrum that are above a certain threshold, because there are spurious emissions due to hardware imperfections that would be detected as false positives. These interferences are extremely narrow, so comparing the power of 200 kHz bands is equivalent to neglecting them.

This process is repeated for each group of 21 bins of all FFT frames. After every step there are two possibilities: the actual power is discarded for being below the minimum value that the vector contains, or otherwise it replaces the minimum value stored for the moment. That way, at the end of the execution, the array of powers should have stored the total power of the GSM channels that would offer a better service. At that point, the frequencies stored in the second vector are printed.

4.2.4 Results

Listing 4.1 shows the output generated after running the script to inspect the GSM-900 downlink band sampling at 10 MHz. The MS used for testing was connected to the A1 Telekom network using ARFCN 80 most of the time and occasionally switching to ARFCN 66, whose downlink frequencies are 951 MHz and 948.2 MHz respectively. This company shares the available spectrum in Austria with T-Mobile and 3, owning only the frequencies from 945 MHz to 959.1 MHz of the downlink GSM-900. This is consistent with the ARFCN values used by the phone and is important to understand the results obtained after running the script.

Listing 4.1: Example of results obtained with the *downscan* script

```
downlink freq.: [938400000, 948200000, 935600000, 955200000, 951000000]
power at those freq.: [675.842, 476.446, 681.287, 451.675, 483.306]
sorted downlink freq.: [935600000, 938400000, 948200000, 951000000, 955200000]
sorted uplink freq.: [890600000, 893400000, 903200000, 906000000, 910200000]
```

The results are satisfactory as both frequencies are present in the first printed line, where the final array of frequencies is displayed. Notice that the two preferred channels for the phone (ARFCN 80 and 66) are not the strongest ones according to the script results. There are two frequencies (935.6 MHz and 938.4 MHz) with a greater associated power, but the cell phone cannot get connected to these channels as they are owned by T-Mobile. So it is normal to see more powerful channels with the SDR peripheral that are not being used by the phone.

However, after performing multiple tests running GQRX on Linux to visually analyse the GSM spectrum, it was concluded that the periodicity of the uplink signals sent by a MS in idle mode is not high enough to build a sensor based on it. In fact, a static mobile

phone in stand-by sends signalling messages very rarely. Figure 4.6 shows a screenshot that was taken after 30 minutes of inactivity. A MS whose carrier frequency was 906 MHz (ARFCN=80) was placed near the sensor during that period of time without receiving nor sending any call or SMS.

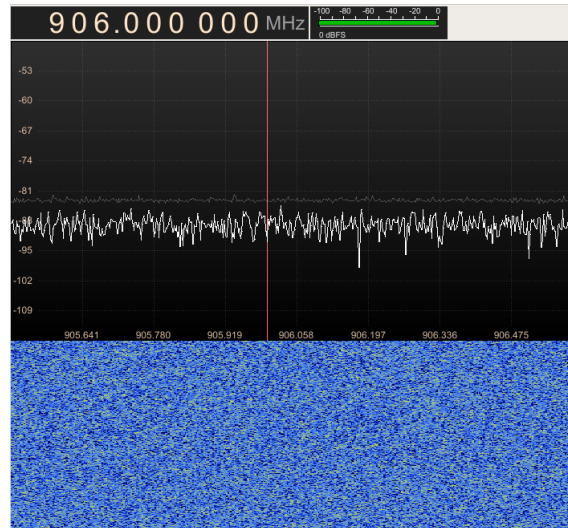


Figure 4.6: MS in idle mode for half an hour, captured with GQRX

Just above the spectrum there is a thin line which marks the maximum power value reached until the moment of capture. With this tool it is easy to see that throughout all the observation time there has not been any type of RF-activity in the frequency of interest (indicated by a red vertical line). The horizontal line is completely stable from start to finish, despite zooming in to see it with a highest level of detail.

If a SMS is sent to the device, a short-lived peak is formed at the time of receipt. Technically speaking, the peak appears right after receiving the SMS, as it is caused by an ACKnowledgement (ACK) message that the MS sends to the network indicating the success of reception. The shape and magnitude of the peaks are indicated by the thin line from above the spectrum in figure 4.7, and the duration of peaks can be seen on the waterfall below, where multiple lines of more vivid colours are displayed. Such lines reveal that four messages were sent from another GSM phone in short intervals.

Something similar happens when the MS sends a SMS instead of receiving it, but in this case the signalling message that can be seen in the uplink carrier frequency is not an ACK but an SMS-submission report. On the other hand, when a call is made or received the spectrum changes more significantly while it is in progress, but these specific cases will be treated in section 4.3.

Comparable RF-activity can be discerned when a mobile is turned on (IMSI attach) or off (IMSI detach), but these are very particular cases that do not happen very often.

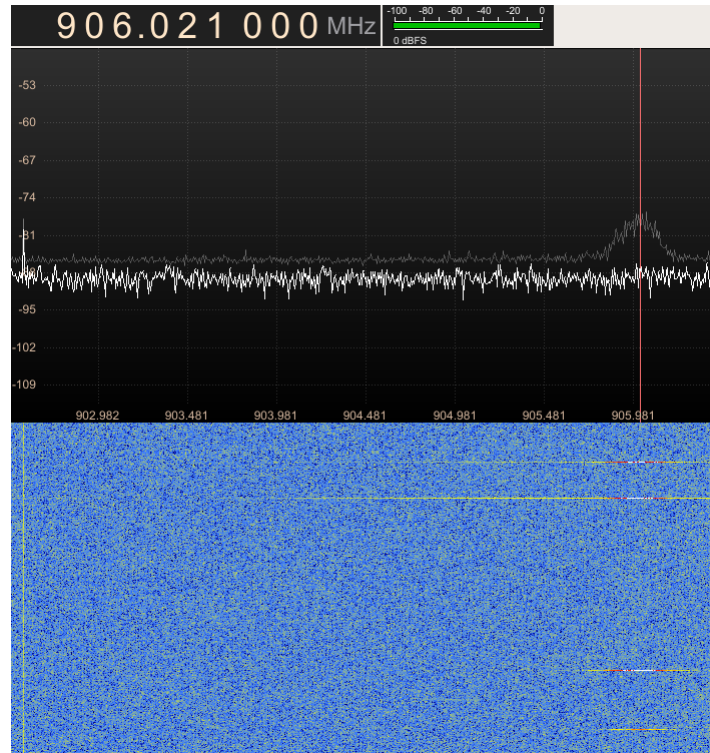
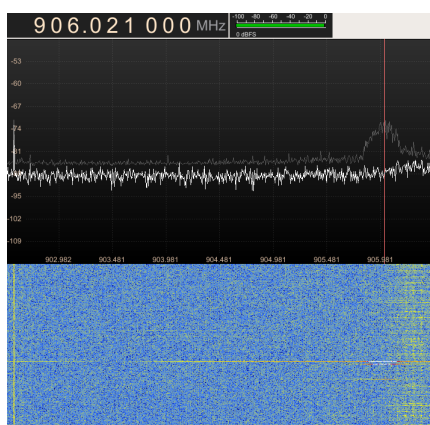


Figure 4.7: Reception of consecutive SMSs captured with GQRX

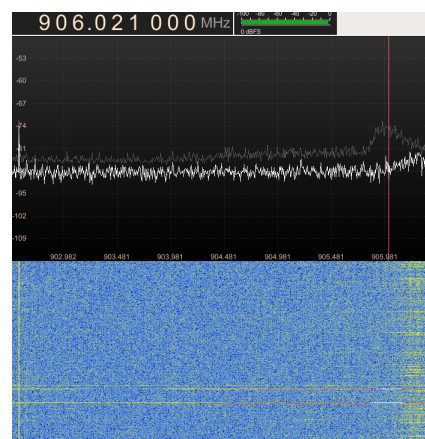
Figures 4.8a and 4.8b show the RF-activity generated by the IMSI attach and detach procedures respectively.

Although it has not been shown in practice, according to the GSM specifications an idle mobile that is moving (i.e. inside a moving car) should send signalling messages more often than while being static. For instance, it would notify the network every time it enters a new location area. To know if its location area has changed, the MS listens to the Broadcast Control Channels once every 30 seconds to find out the actual LAC, but this is done on the downlink carrier frequency (951 MHz in the examples above) while nothing happens in the uplink.

In conclusion, it is not worth building a sensor to detect phones in idle mode as they do not emit signals the vast majority of time. Despite the results obtained after running the *downscan* script demonstrate that it is feasible to find uplink channels by detecting the associated downlinks, it was not worthwhile to continue on this line of research as there is basically nothing to detect. The situation is completely different when the devices are being used for calling, a process that significantly increases the abundance of uplink messages as will be seen in the next section.



(a) IMSI attach captured with GQRX



(b) IMSI detach captured with GQRX

Figure 4.8: IMSI attach and detach procedures

4.3 Detection in dedicated mode

4.3.1 Overview

The first attempt to detect mobile phone users did not meet the initial expectations. However, applying a few modifications to the software it should be possible to, at least, detect MSs in dedicated mode. When a mobile enters dedicated mode by making or receiving a call, it becomes highly active. There are three possible scenarios:

Outgoing call

When a user dials the telephone number of another subscriber, his MS requests the allocation of a dedicated signalling channel by sending a “channel request” to the BSS over the RACH. After some protocol steps are carried out in upper levels of the network, the MS receives a message on the AGCH indicating which SDCCH has been assigned to its call. Then, the device uses this logical channel to send a call establishment request and waits for a response in the same channel. Afterwards it sends a setup message with the target number, and a traffic channel will be assigned to that call. The phone finds out the frequency that will be used during the call by listening at the FCCH, and sends an uplink ACK message before starting to use the TCH. To sum up, a lot of information is exchanged between a MS and the networks during call establishment. This can be discerned by listening to the air interface with a HackRF while a call is being made. Figure 4.9 shows the spectrum in such a situation.

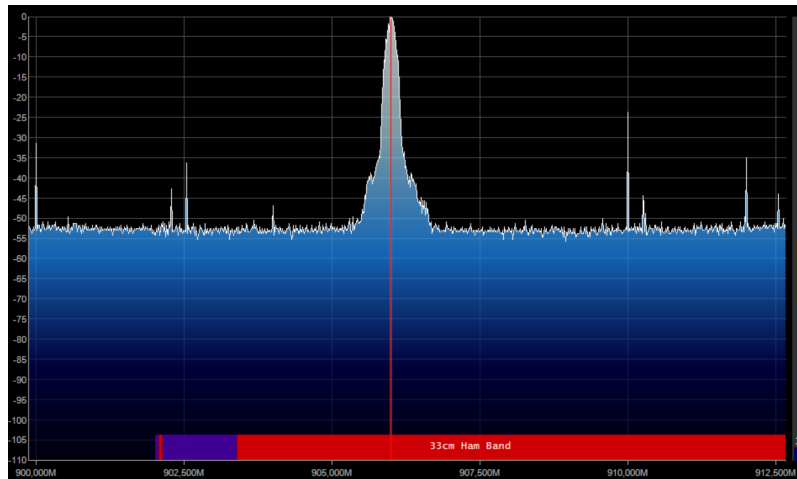


Figure 4.9: Outgoing call on ARFCN 80 captured with SDRsharp

Incoming call

In the opposite case, the MS receives a paging message on the PCH. Then it generates a channel request on RACH which is immediately answered over its homologous AGCH. Now that the MS owns a SDCCH for signalling, it uses such channel to answer the paging message that triggered the process. After exchanging multiple messages over the SDCCH, the network assigns a TCH to be used for the call and, right after that, receives an ACK message from the MS. Finally, alert messages are sent by the network towards the FACCH until the user answers the call and the communication switches to the TCH. So, again, a lot of signalling messages are sent in both directions when a call is being received. This is displayed in figure 4.10.

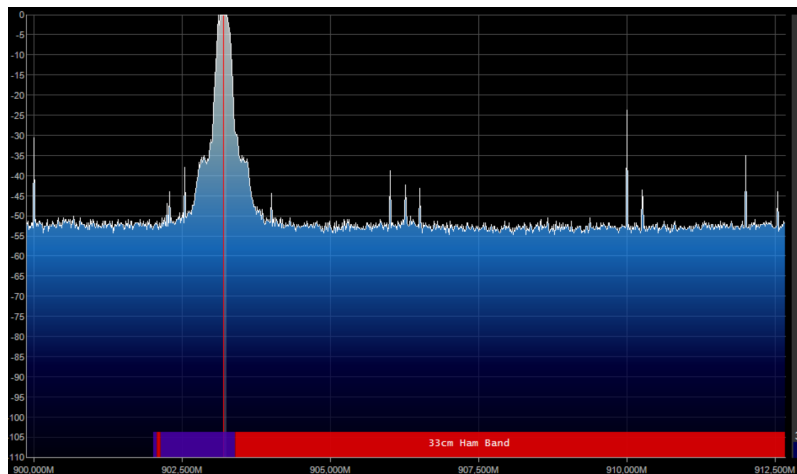


Figure 4.10: Incoming call on ARFCN 66 captured with SDRsharp

Ongoing call

When the subscriber answers a call, both phones switch to their respective TCHs where speech data is exchanged. However, the signalling messages are still ongoing over the control channels. In fact, each TCH has an associated SACCH where uplink measurement reports are sent every second. These uplink messages are essential to perform timing and power control, and they are not hard to detect because of their high periodicity. A screenshot from the spectrum in this case would look exactly the same as the ones from figure 4.9 or figure 4.10. However, it is a bit different over time as the GSM carrier is not continuously active. In fact, there is a technique called “silence suppression” that is used in telephony to reduce the bandwidth usage. It consists in not transmitting information in the uplink channel if the subscriber is not currently speaking. This is done to avoid sending background noise from one peer-end to the other, given that in a typical conversation when one person speaks the other one listens. In GSM this concept is known as “discontinuous transmission”, and consists of not sending uplink messages if there is no voice input, mainly for efficiency reasons and to preserve the phone’s battery. This could make it difficult to detect a conversational partner who stops speaking for a while, but the presence of signalling messages from the SACCH facilitate detection.

The basics of the already implemented code should work for this case too, considering the stability of the spectrum during a call. The Python script named `upscan.py`⁵ implements this logic.

4.3.2 Parameters

The settings for the *upscan* script are almost the same as the ones described in section 4.2.2. The only difference is the lack of parameter *N* (number of downlink channels to be detected) and the presence of a new input called “threshold”. This value will be used to determine if there is an ongoing call in the GSM channel under study or not.

The triage of this value depends on how far away phone calls should be detected. There is not a specific value as it depends a lot on the environment: it is known that in empty space the power of radio waves decreases with the inverse of the squared distance, but the presence of interferences and multipath in urban environments cause the received power to be typically proportional to the inverse of the distance to the fourth.

However, the distance is not the single most relevant variable considering that the network operator controls and adjusts the transmitting power of the connected MSs. As explained in chapter 2, this is done by sending downlink commands to the MS, based on measurements sent by the MS itself. The range of possible transmitting powers goes from 0 dBm to 39 dBm, but some devices have a maximum output power that is below 39 dBm (the most widely used class of GSM transmits at a maximum level of 33 dBm). According to [25], output powers above 30 dBm are used most of the time.

⁵<https://gitlab.auto.tuwien.ac.at/prairich/sdr-gsm-detector>

4.3.3 Methodology

The *upscan.py* script uses a largely similar method to the script described in section 4.2.3. The major difference is that instead of scanning the GSM downlink band once, it does it repeatedly in the uplink band. Regardless of whether a call has been found or not, after scanning the whole band, the receiver will be tuned again to the first frequencies to start a new scanning iteration. During execution, the program simply prints if a call has been detected or not.

It is enough to check if the cumulative power of a GSM channel is above a certain threshold. In such a case, it can be assumed that a call is in progress in the carrier frequency where an RF-activity above the threshold has been detected.

4.3.4 Results

The test results show that it is possible to detect phone calls with a high level of precision. All calls performed near the receiver (same room) were detected without false positives. Even if the call was initiated from a different room or floor, it was detected. The range of detection in the indoor environment of the building where tests were performed was of approximately 25 meters, with walls in between.

It must be said that it is difficult to fully guarantee that the detected call is produced by the test equipment; it could be from any other nearby subscriber. During the test period it was considered that a call is detected if its ARFCN value (displayed on the printed messages) matches the ARFCN that the test device was using just before receiving or making the call. However, because of the TDMA technique used in GSM, a MS transmits on the carrier frequency only one eighth of the time (duration of a single slot). The other seven slots can be used by other MSs operating at the exact same frequency. So, an unfortunate situation in which the test call is not detected but another subscriber's call using the same ARFCN is detected would cause a false positive.

The frequency found by the program corresponds to the ARFCN that was being used by the test equipment all along. The other MS used for testing purposes was not able to provide the ARFCN in use, but it is known from previous tests that its SIM card gets preferably connected to two ARFCN carriers at the place where tests are carried out: one from the GSM-900 band and another one from GSM-1800. Sometimes, during a call, only one peak was detected in the spectrum. This might be because the second phone is using the carrier frequency from GSM-1800, a band that is not being analysed during testing. In other occasions, two calls are detected at different frequencies allegedly because both MSs are operating in the GSM-900 band.

If the LNA presented in chapter 3 (LNA4ALL) is attached to the antenna, then the SNR of the received signals is increased, increasing with this the sensor's range of detection.

The SNR improvement was seen comparing the spectrum displayed in GQRX with and without LNA. However, it was also seen that the system is more prone to interferences;

if the gain parameters are not properly adapted to the new hardware, a large number of spurious emissions appear throughout the spectral band. In addition, if the gains are not adequate, replicas of the signal are also generated. To control this, it is recommended to have an IF gain below 16 dB and a maximum baseband gain of 20 dB.

To supply power to the LNA, the antenna bias voltage has to be set to "receive mode" by software, activating a phantom power of 3.3 V and 50 mA on the transceiver antenna port. Once the modification is done, the HackRF will only work in receiver mode, which is not an inconvenience since transmission is not required for this project.

Conclusion and Outlook

5.1 Summary and Critical Reflection

This thesis began with a simple question: Is it possible to detect mobile phone users that are not currently using their GSM handsets? After doing a preliminary research about the GSM technology, a first approach to the problem was performed. It was intended to scan a whole GSM uplink band using the general-purpose radio receiver HackRF together with the open-source software GNU Radio in order to detect any type of RF-activity that could be present in such band.

A first method was carried out to passively recognize inactive MSs just by detecting the uplink control messages that these devices periodically report to the network. However, the method did not work as expected, because the aforementioned periodicity turned out to be too low to achieve reliable detection. A second method focused on detection of MSs that are currently being used for calling as evaluated. In this case the results were more promising, as all calls were detected within an acceptable range. This more effective approach is not comparable to the initial goal in terms of ambition, since the possible applications are greatly reduced by the scarcity of situations in which a user would be detected. Hence the sensor would not be reliable enough to compete with typical presence detection sensors (i.e. proximity, image or motion sensors), yet it could serve as an additional information source in certain scenarios, e.g. where information about discerning humans from animals or other interferences is beneficial.

As a final reflection on this thesis, the main conclusion would be that the GSM technology cannot be used for detection of passive mobile phones with the proposed method. The exposed results demonstrate that a sensor based on this technology is not comparable to other same-purpose sensors. In any case, the performed work has served to eliminate the initial doubt about whether the idea was feasible or not.

5.2 Future Work

Now that the research has concluded, there are enough arguments to assert that the initial approach was too ambitious. Nonetheless, it should not be considered a dead end.

Despite the final implementation is limited to call detection, it offers a basis for further development.

First of all, an attempt could be made to reduce the cost of the overall system. For instance, the software could be run on a single-board computer (i.e. Raspberry Pi) instead of a regular computer. Despite the fact that this hardware is supposed to be compatible with the HackRF, it remains to be seen if it fulfils the requirements imposed by the receiver during operation. For testing purposes the cost was not as important as proving the validity of the idea, but if a sensor of this characteristics is to be used, it would be worthwhile to migrate the whole software to a cheaper hardware.

The implementation using cheaper and/or smaller components is also worth investigating. It should be previously studied how the limitations of a low-cost receiver would affect the performance of the whole system. If the results are still acceptable, the sensor would gain in portability. The use of a battery could be considered to give autonomy to the whole system taking advantage of the fact that it would be composed of low-powered devices. However, the battery life of such a system is unknown at this moment.

Another line of research could be the inclusion of other telecommunication technologies such as Bluetooth, WiFi, LTE or UMTS, as the detection of any of them implies the presence of a person nearby. A hardware update might be necessary to operate in a broader spectral band, and the software should be also adapted to work properly with different telecommunication standards. So, a previous research would be necessary to fully understand the particularities of the different signals to be detected and, consequently, determine if it is worth implementing it.

A part from that, the sensor could also be used in a wider range of areas to differentiate subscribers from different network providers. Since the way in which network operators distribute the available spectrum is known, just by looking at the carrier frequency where calls are detected, it is possible to know the network provider of the involved SIM cards.

It is also thinkable to evaluate the first method, focused on the location of idle cell phones that remain undetectable most of the time, for very specific situations in which MSs send report messages. For example, a situation in which a MS becomes detectable is during a handover process. In such a situation the device accesses the target cell with its maximum transmitting power, becoming detectable for a moment. Thus, the idea could be tested in places with large agglomerations of people or between two adjacent location areas with a extremely small overlap. Both situations engender a high number of handovers, generating detectable activity in the uplink channels, thereby increasing the reliability of the sensor.

Finally, it would be also possible to go one step further, migrating both method's code from Python to C++. The efficiency of this programming language could result in a better performance for possible real-time applications of the sensor. In this thesis Python was used for testing purposes as run-time efficiency was traded in for the speed up development that is offered by using this language.

Annex I: HackRF One

Technical Specifications	
Type of SDR Peripheral	Half-Duplex Transceiver
Dimensions	12.2 x 7.6 x 1.7 cm
Weight	100 g
Maximum Bandwidth	20 MHz
Frequency Range	From 1 MHz to 6 GHz
ADC Resolution	8-bit quadrature samples (8-bit I and 8-bit Q)
Dynamic Range	48 dB
Frontend Filters	Preselection filters (2.3 GHz LPF, 2.7 GHz HPF)
Frontend Chips	MAX5864, RFFC5071
Antenna Port Power	50 mA at 3.3 V
Antenna Connector	SMA female
Additional Connectors	SMA female CLKIN/CLKOUT for synchronization
Clock Precision	30 PPM XO
Hi-Speed	USB 2.0
Power Supply	micro USB
Open Source	Yes
Compatible Software	GNUradio, GQRX, SDR-Radio
Price	280 EURO

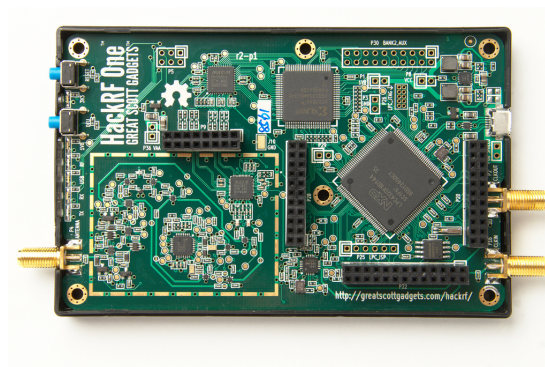


Figure 1: HackRF One's daughterboard

Glossary

GQRX Open source SDR receiver powered by GNU Radio that can work either on Linux or Mac. Allows the control of many SDR hardware devices..

Noise Figure Noise Factor converted to decibel notation.

SDRsharp Also known as SDR#, it is the Windows version of GQRX.

Acronyms

ACK ACKnowledgement.

ADC Analog-to-Digital Converter.

AGCH Access Grant Channel.

ARFCN Absolute Radio Frequency Channel Number.

BCCH Broadcast Control Channel.

BSC Base Station Controller.

BSS Base Station Subsystem.

BTS Base Transceiver Station.

CBCH Cell Broadcast Channel.

CPU Central Processing Unit.

DFT Discrete Fourier Transform.

DSP Digital Signal Processor.

EDGE Enhanced Data Rates for GSM Evolution.

ETSI European Telecommunications Standards Institute.

FACCH Fast Associated Control Channel.

FB Frequency Correction Burst.

FCCH Frequency Correction Channel.

FDD Frequency-Division Duplexing.

FDMA Frequency-Division Multiple Access.

FFH Fast Frequency Hopping.

FFT Fast Fourier Transform.

GMSK Gaussian Minimum-Shift Keying.

GPRS General Packet Radio Service.

GPS Global Positioning System.

GRC GNU Radio Companion.

GSM Global System for Mobile Communications.

GUI Graphical User Interface.

IF Intermediate Frequency.

IMEI International Mobile (Station) Equipment Identity.

IMSI International Mobile Subscriber Identity.

LAC Location Area Code.

LNA Low Noise Amplifier.

LTE Long Term Evolution.

ME Mobile Equipment.

MS Mobile Station.

MSK Minimum-Shift Keying.

NSS Network Switching Subsystem.

OS Operative System.

OSS Operation and Support Subsystem.

PCH Paging Channel.

QoS Quality of Service.

RACH Random Access Channel.

RADAR RAdio Detection And Ranging.

RF Radio Frequency.

RSS Radio Signal Strength.

SACCH Slow Associated Control Channel.

SB Synchronization Burst.

SCH Synchronization Channel.

SDCCH Standalone Dedicated Control Channel.

SDR Software Defined Radio.

SFH Slow Frequency Hopping.

SIM Subscriber Identity Module.

SMS Short Message Service.

SNR Signal-to-Noise Ratio.

TCH Traffic Control Channel.

TDMA Time-Division Multiple Access.

UMTS Universal Mobile Telecommunications System.

Bibliography

- [1] F. Van Den Broek, B. Jacobs, and E. Poll, “Catching and understanding gsm-signals,” *Master’s thesis, Radboud University Nijmegen*, 2010.
- [2] I. F. A. Alyafawi and T. Braun, *Real-time localization using software defined radio*. PhD thesis, Universität Bern, 2015.
- [3] R. Academy, “Introduction to gsm device testing,” *National Instruments*, 2009.
- [4] M. Glendrange, K. Hove, and E. Hvideberg, *Decoding GSM*. Institutt for Telematikk Uppsala Universität, 2010. Master Thesis.
- [5] R. . Schwarz, “Frequency hopping for gsm base station tests with signal generators sme,” *Note, Application*, 1995.
- [6] J. Eberspächer, H.-J. Vögel, C. Bettstetter, and C. Hartmann, *GSM-architecture, protocols and services*. John Wiley & Sons, 2008.
- [7] M. B. Kjærgaard, M. Wirz, D. Roggen, and G. Tröster, “Mobile sensing of pedestrian flocks in indoor environments using wifi signals,” in *Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on*, pp. 95–102, IEEE, 2012.
- [8] P. Bahl and V. N. Padmanabhan, “Radar: An in-building rf-based user location and tracking system,” in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, pp. 775–784, Ieee, 2000.
- [9] Y. Wang, X. Yang, Y. Zhao, Y. Liu, and L. Cuthbert, “Bluetooth positioning using rssi and triangulation methods,” in *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, pp. 837–842, IEEE, 2013.
- [10] L. Schauer, M. Werner, and P. Marcus, “Estimating crowd densities and pedestrian flows using wi-fi and bluetooth,” in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 171–177, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ACM Digital Library, 2014.

- [11] I. Alyafawi, S. Kiener, and T. Braun, “Hybrid indoor localization using multiple radio interfaces,” *To be submitted*, 2015.
- [12] V. Otsason, A. Varshavsky, A. LaMarca, and E. De Lara, “Accurate gsm indoor localization,” in *International conference on ubiquitous computing*, pp. 141–158, Springer, 2005.
- [13] C. Drane, M. Macnaughtan, and C. Scott, “Positioning gsm telephones,” *IEEE Communications magazine*, vol. 36, no. 4, pp. 46–54, 1998.
- [14] K. van Rijsbergen, “The effectiveness of a homemade imsi catcher build with yatebts and a bladerf,” *University of Amsterdam*, 2016. Report.
- [15] I. Alyafawi, D. C. Dimitrova, and T. Braun, “Real-time passive capturing of the gsm radio,” in *2014 IEEE International Conference on Communications (ICC)*, pp. 4401–4406, IEEE, 2014.
- [16] P. Samczynski, K. Kulpa, M. Malanowski, P. Krysik, *et al.*, “A concept of gsm-based passive radar for vehicle traffic monitoring,” in *Microwaves, Radar and Remote Sensing Symposium (MRRS), 2011*, pp. 271–274, IEEE, 2011.
- [17] D. K. Tan, H. Sun, Y. Lu, M. Lesturgie, and H. L. Chan, “Passive radar using global system for mobile communication signal: theory, implementation and measurements,” *IEE Proceedings-Radar, Sonar and Navigation*, vol. 152, no. 3, pp. 116–123, 2005.
- [18] P. Cruz, H. Gomes, and N. Carvalho, *Receiver front-end architectures-Analysis and evaluation*. INTECH Open Access Publisher, 2010.
- [19] H. T. Friis, “Noise figures of radio receivers,” *Proceedings of the IRE*, vol. 32, no. 7, pp. 419–422, 1944.
- [20] A. Adam, “LNA FOR ALL.” <http://lna4all.blogspot.co.at/>, 2015. Visited on 2017-01-03.
- [21] M. Braun, M. Müller, and T. Rondeau, “Guided GNU Radio Tutorials.” http://gnuradio.org/redmine/projects/gnuradio/wiki/Guided_Tutorials, 2013. Visited on 2016-10-19.
- [22] “CellID Finder.” <http://cellidfinder.com/>, 2013. Visited on 2017-01-22.
- [23] “GNU Radio Manual and C++ API Reference.” <http://gnuradio.org/doc/doxygen/>, 2016. Visited on 2016-11-12.
- [24] R. G. Lyons, *Understanding Digital Signal Processing*. Pearson Education India, 2004.

- [25] S. Lönn, U. Forssen, P. Vecchia, A. Ahlbom, and M. Feychting, “Output power levels from mobile phones in different geographical areas; implications for exposure assessment,” *Occupational and Environmental Medicine*, vol. 61, no. 9, pp. 769–772, 2004.