USRP based Cognitive Radio Test-Bed using OpenBTS

M. Tech. Dissertation

Submitted in partial fulfilment of the requirements for the degree of
Master of Technology

by

Abrar Ahmad
113310017

Supervisor

Prof. S N Merchant

Department of Electrical Engineering
IIT Bombay

June 2014

Declaration of Academic Ethics

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Abrar Ahmad
(Roll 113310017)

Date: . . . . . .

Abstract

Wireless networks are currently regulated by fixed spectrum assignment policy which results in inefficient utilization of the spectrum. In the last few years there has been a drastic increase in the mobile services, which in turn has increased the demand for limited radio spectrum. Hence there is a need to change the conventional static spectrum assignment policy and make efficient utilization of spectrum. Cognitive Radio (CR) emerged as a new paradigm to address the spectrum underutilization problem. CR enables opportunistic use of the radio-frequency spectrum by allowing Secondary/Un-licensed users to utilize licensed bands under the condition that they should not cause the interference with the Primary/Licensed users. Secondary users utilize the detected free bands and leave them when the corresponding primary radio emerges.

A USRP based 2-frequency CR Test-Bed and a 4-frequency CR Test-Bed has been developed using GNURadio and OpenBTS to demonstrate these properties of cognitive radio. Primary and secondary users are made to coexist with no effect on the primary radio. Energy detection spectrum sensing technique is used to detect the free bands also known as the spectrum holes. We demonstrate that secondary users utilize these spectrum holes and vacate them whenever primary users want to use them.

Acknowledgement

This thesis wouldn't have been possible without the help of a few people who have contributed in one way or the other to the completion of this research. Firstly I would like to express my sincere gratitude to my guide Prof. S. N. Merchant for his persistent guidance, support, encouragement and vital suggestions during this research work. I thank him for introducing me to the world of wireless communication and cognitive radio. Apart from his technical input I thank him for his motivation in the project to make it an enjoyable learning experience. I would also like to thank Prof V. M. Gadre for his support and guidance.

I would like to thank my project partner Swrangsar Basumatary who helped me in resolving issues that came up in this research. I would also like to thank my parents for their immense support without which this wouldn't have been possible. I cannot thank enough, almighty God who provided me with the strength to make this possible. Also, I would like to mention SPANN lab members for giving their resources and time in enabling to complete my thesis.

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation

Due to the rapid increase of mobile phones and other wireless communication devices, there is a need for efficient utilization of the available radio spectrum. The Spectrum Policy Task Force, a group under the Federal Communications Commission (FCC) in the United States, published a report in 2002 saying [1]:

> "In many bands, spectrum access is a more significant problem than physical scarcity of spectrum, in large part due to legacy command-and-control regulation that limits the ability of potential spectrum users to obtain such access."

If we scan the spectrum in metropolitan cities which are heavily used regions, we find that some frequency bands are unoccupied most of the time[2]. These are referred to as spectrum holes. A spectrum hole is a band of frequencies assigned to a primary user, but, at a particular time and specific geographic location, the band is not being utilized by that user[3].

This problem of inefficient utilization of spectrum can be solved by allowing secondary users which are non licensed, to access these spectrum holes. Cognitive radio which includes software defined radio, is a means to accomplish this by utilizing these spectrum holes intelligently and efficiently[5][6][7]. It uses one of the spectrum sensing techniques to identify the spectrum holes in the radio spectrum.

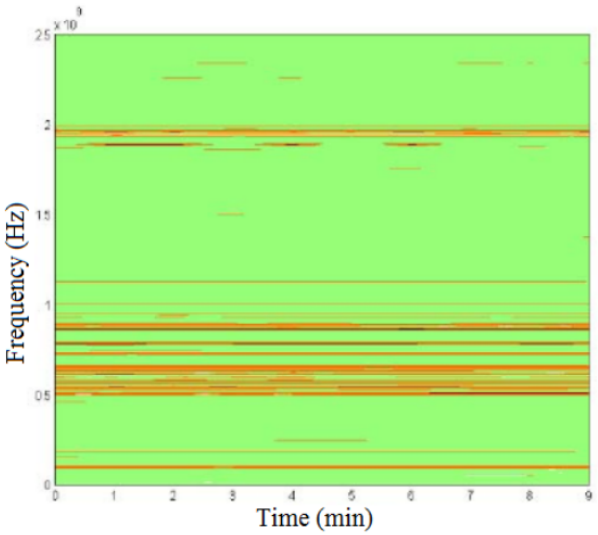

Figure 1.1: Frequency usage of Spectrum Band [4]

1.2 Cognitive Radio

A cognitive radio is an intelligent radio whose primary objective is efficient utilization of the radio spectrum. It can be programmed and configured dynamically. It works on the principle of understanding-by-building to learn from the surrounding environment and adapt to changes in the RF stimuli by making corresponding changes in operating parameters. The transceiver is designed to find an unoccupied channel in the vicinity and utilize it for transmission. It enables coexistence of primary licensed users and secondary unlicensed users. Whenever a primary user wants to occupy the channel which is currently in use by secondary users, it finds some other unoccupied channel in the vicinity and secondary users migrate seamlessly to this new channel thus vacating the previously used channel for primary users.

1.3 Contribution of this Thesis

An experimental setup is developed which demonstrates the presence of secondary users along with primary users in the existing GSM network and utilizing the already existing resources there by increasing the total mobiles in the network.

1. A 2-frequency band cognitive system is developed where secondary users migrate to frequency $f2$ if frequency $f1$ is occupied an viceverca.

2. A 2-frequency system is extended to a 4-frequency system where we demonstrate that primary users are occupying two bands out of these four and

secondary users occupy one out of the other two free bands.

3. We have used energy detection spectrum sensing technique and CUSUM peak detection technique to detect the presence of primary users. Band occupied by secondary users is continuously monitored to check if primary users are trying to occupy that band and as soon as the request from primary users is detected a new free band is found out in the vicinity and utilized by secondary users for transmission there by vacating the band for primary users .

1.4 Organization of this Thesis

The rest of this document is organized as follows. Chapter 2 briefly describes the GSM architecture and its Um interface. Chapter 3 gives a literature survey on Universal Software Radio Peripheral (USRP N210) the hardware used in this project. Literature survey done on the GNU Radio software package and OpenBTS software is described in Chapter 4 and 5 respectively. Chapter 6 covers spectrum sensing techniques to detect the presence of primary users in the channel. Chapter 7 covers an implementation of cognitive radio using GNU Radio and OpenBTS. It describes the experimental setup for our project in the beginning followed by detailed description of what we have achieved in this project along with a flow chart of our work. The final chapter of this thesis is the conclusion of our project followed by future work.

Chapter 2

Overview of traditional GSM networks

2.1 What is GSM?

GSM, or Global System for Mobile Communications, is a European standard for the Mobile telecommunications and it is considered as one of the most popular standard worldwide.There are thirteen different frequency bands defined in GSM. However, the 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz bands are the most commonly used. The frequency bands employed within each of the four ranges are similarly organized. They differ essentially only in the frequencies, such that various synergy effects can be taken advantage of; hence, here we give some details only for the usage in the 900 MHz band.

In the 900 MHz band, a total of 70 MHz bandwidth is allocated, two 25-MHz frequency bands for uplink and downlink and a 20 MHz unused guard band between them. The MS transmits in the 890 to 915 MHz range (uplink) and the BTS transmits in the 935 to 960 MHz (downlink) band. This corresponds to 124 duplex channels, where each channel within a BTS is referred to as an Absolute Radio Frequency Channel Number (ARFCN). This number describes a pair of frequencies, one uplink and one downlink, and is given a channel index between C0 and C123, with C0 designated as the beacon channel. An ARFCN could be used to calculate the exact frequency (in MHz) of the radio channel. In the GSM 900 band, this is computed by the following equations:

$$F_{uplink}(n) = 890 + 0.2 * n \qquad 1 \leq n \leq 124$$
$$F_{downlink}(n) = F_{uplink}(n) + 45 \qquad 1 \leq n \leq 124$$

Similar formulae are also defined for the other GSM frequency bands.

The principle component groups of a GSM network are as follows:

- The Mobile Station (MS)
- The Base Station System (BSS)
- The Network Switching System(NSS)

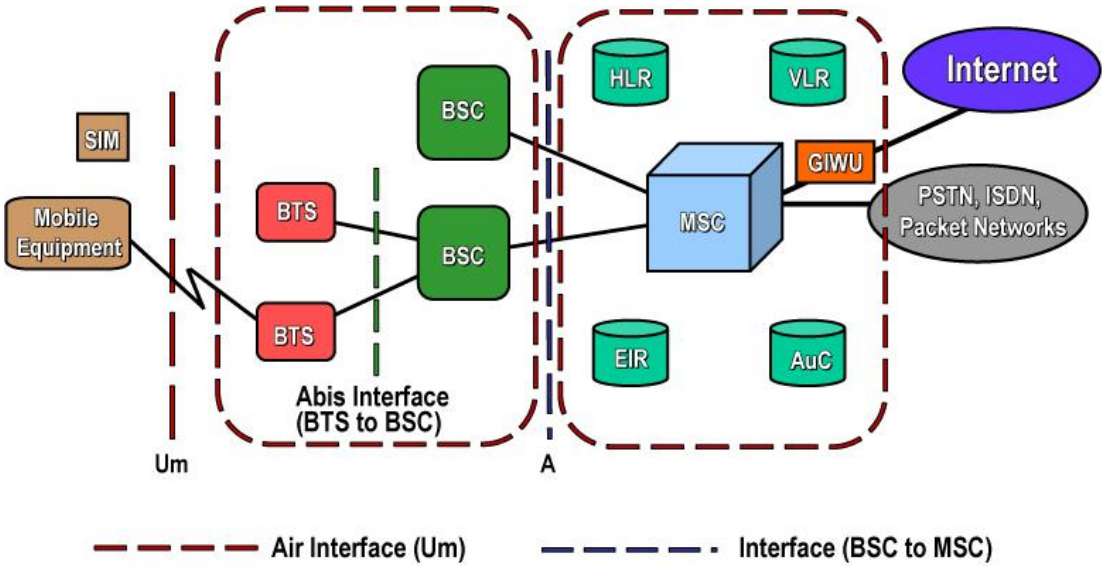

Figure 2.1: The conventional GSM architecture [8].

2.1.1 Mobile Station

The MS consists of two parts, the Mobile Equipment (ME) and Subscriber Identity module (SIM). The ME has an identity number called the International Mobile Equipment Identity (IMEI) associated with it, which is unique for that particular device and permanently stored in it.The SIM card consists the International Mobile Subscriber Identity(IMSI) number which is used to identify the subscriber to the system. The IMEI and the IMSI are independent of each other and hence allow personal mobility.

2.1.2 Base Station System

The GSM Base Station System is the equipment located at a cell site. It comprises of a combination of digital and RF equipment. The BSS provides the link between the MS and the Mobile Services Switching Centre (MSC). The BSS consists mainly of:

The Base Transceiver Station(BTS) The BTS contains the RF components that provide the air interface for a particular cell. This is the part of the GSM network which communicates with the MS. The antenna is included as part of the BTS.

The Base Station Controller(BSC) The BSC provides the control for the BSS. The BSC communicates directly with the MSC. The BSC may control single or multiple BTSs. Crucial functions like radio channel link establishment, frequency hopping, and handovers from one cell to another.

2.1.3 Network Switching Subsystem

The Network Switching Subsystem includes the main switching functions of the GSM network. It also contains the databases required for subscriber data and mobility management. Its main function is to manage communications between the GSM network and other telecommunications networks. The main components of the Network Switching System are:

Mobile Services Switching Centre(MSC)

The MSC does call-switching and its overall purpose is the same as that of any telephone exchange. When the MSC provides the interface between the PSTN and the BSSs in the GSM network it will be known as a Gateway MSC. In this position it will provide the switching required for all MS originated or terminated traffic. Each MSC provides service to MSs located within a defined geographic coverage area. One MSC is capable of supporting a regional capital with approximately one million inhabitants. The functions carried out by the MSC are: Call Processing, Operations and Maintenance Support, Internetwork Interworking and Billing

Home Location Register (HLR)

The HLR is a central database that contains the details of each mobile phone subscriber that is authorized to use the GSM core network. The IMSI of each SIM acts as a primary key to each HLR record. Each MSISDN is also a primary key to the HLR record. The HLR data is stored as long as a subscriber remains with the mobile phone operator. Data stored in the HLR against each IMSI are, GSM services that the subscriber has requested, GPRS settings to allow the subscriber to access packet services, current location of the subscriber, etc.

Visitor Location Register (VLR)

The VLR is a database of the subscribers who have roamed into the jurisdiction of the MSC which it serves. Each main base station in the network is served by exactly one VLR, hence a subscriber cannot be present in more than one VLR at a time.The data stored in the VLR has either been received from the HLR, or collected from the MS. Data stored includes: IMSI (the subscriber's identity number), authentication data, MSISDN, GSM services that the subscriber is allowed to access, the HLR address of the subscriber.

2.2 Um Interface

The Um interface is the air interface of the GSM mobile telephone standard. It is the interface between the MS and the BTS. It is called Um because it is the mobile analog to the U interface of ISDN. Um is defined in the GSM 04.xx and 05.xx series of specifications.

The layers of GSM are initially defined in GSM 04.01 Section 7 and roughly follow the OSI model. Um is defined in the lower three layers of the model.

2.2.1 Physical Layer (L1)

The Um physical layer is defined in the GSM 05.xx series of specifications, with the introduction and overview in GSM 05.01. For most channels, Um L1 transmits and receives 184-bit control frames or 260-bit vocoder frames over the radio interface in 148-bit bursts with one burst per timeslot. There are three sublayers:

Radiomodem

This is the actual radio transceiver. GSM uses 8PSK modulation with 1 bit per symbol which produces a 13/48 MHz (270.833 kHz or 270.833 K symbols/second) symbol rate and a channel spacing of 200 kHz. Since adjacent channels overlap, the standard does not allow adjacent channels to be used in the same cell. The standard defines several bands ranging from 400 MHz to 1990 MHz.GSM is frequency duplexed, meaning that the network and MS transmit on different frequencies, allowing the BTS to transmit and receive at the same time. Transmission from the network to the MS is called the "downlink" and that from the MS to the network is called the "uplink". The GSM uplink and downlink bands are separated by 45 or 50 MHz. Uplink/downlink channel pairs are identified by an index called the ARFCN. Within the BTS, these ARFCNs are given arbitrary carrier indexes C0..Cn-1, with C0 designated as a Beacon Channel and always operated at constant power. The radio channel is time-multiplexed into 8 timeslots, each with a duration of 156.25 symbol periods. These 8 timeslots form a frame of 1,250 symbol periods. The capacity associated with a single timeslot on a single ARFCN is called a physical channel (PCH) and referred to as "CnTm" where n is a carrier index and m is a timeslot index (0-7).Each timeslot is occupied by a radio burst with a guard interval, two payload fields, tail bits, and a midamble.

Multiplexing and Timing

GSM uses TDMA to subdivide each radio channel into as many as 16 traffic channels or as many as 64 control channels. The multiplexing patterns are defined in GSM 05.02.Each physical channel is time-multiplexed into multiple logical channels according to the rules of GSM 05.02. Traffic channel multiplexing follows a 26-frame (0.12 second) cycle called a "multiframe". Control channels follow a 51-frame multiframe cycle. The C0T0 physical channel carries the synchronization channel(SCH), which encodes the timing state of the BTS to facilitate synchronization to the TDMA pattern.

FEC Coding

The coding sublayer provides forward error correction. As a general rule, each GSM channel uses a block parity code (usually a Fire code), a rate-1/2, 4th-order convolutional code and a 4-burst or 8-burst interleaver.

2.2.2 Data Link Layer(L2)

The Um data link layer, LAPDm, is defined in GSM 04.05 and 04.06. LAPDm is the mobile analog to ISDN's LAPD.

2.2.3 Network layer(L3)

The Um network layer is defined in GSM 04.07 and 04.08 and has three sublayers. A subscriber terminal must establish a connection in each sublayer before accessing the next higher sublayer.

Radio Resource (RR) This sublayer manages the assignment and release of logical channels on the radio.

Mobility Management (MM) This sublayer authenticates users and tracks their movements from cell to cell. It is normally terminated in the VLR or HLR.

Call Control (CC) This sublayer connects telephone calls and is taken directly from ITU-T Q.931. GSM 04.08 Annex E provides a table of corresponding paragraphs in GSM 04.08 and ITU-T Q.931 along with a summary of differences between the two. The CC sublayer is terminated in the MSC.

The access order is RR, MM, CC. The release order is the reverse of that. Note that none of these sublayers terminate in the BTS itself. The standard GSM BTS operates only in layers 1 and 2.

Chapter 3

Software Defined Radio

Software defined radio also known as software radio or SDR is a radio in which some or all of the physical layer functions are software defined. Due to the exponential increase in the ways and means by which people need to communicate - data communications, voice communications, video communications, broadcast messaging, command and control communications, emergency response communications and etc, there is a constant need of modifying radio devices easily and cost efficiently. The traditional hardware radio system consist a variety of analogy elements such as mixers, filters, amplifers, converters, modulators and demodulators etc which are costly and are not flexible. Thus traditional hardware based radio devices limit cross-functionality and can only be modified only through physical intervention. This results in higher production costs and minimal flexibility. The solution to this is Software Defined Radio which is easily modifiable. Technologies such as Field Programmable Gate Array (FPGA), Digital Signal Processor (DSP) and General-Purpose Processor (GPP) are used to build the software radio elements.

The software defined radio (SDR) contains a number of basic functional blocks. The radio in genera can be divided into three basic sections, namely the front end,

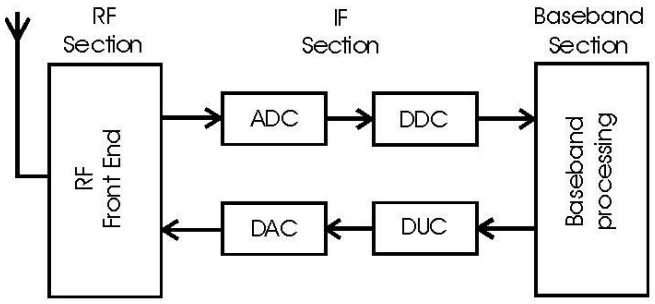

Figure 3.1: Block diagram of SDR [4].

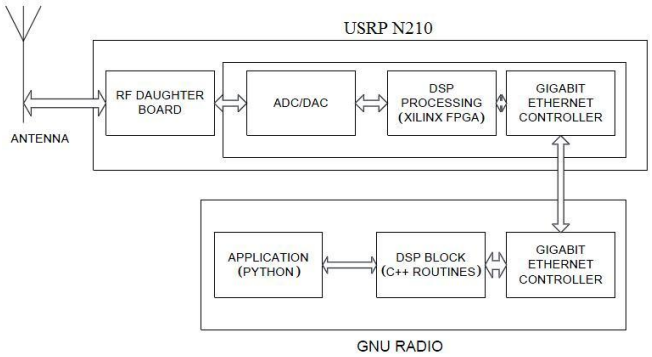

Figure 3.2: Block diagram for USRP operation with GNURadio [4].

the IF section and the base-band section as shown in Figure 3.1. The front end section uses analogue RF circuitry and it is responsible for receiving and transmitting the signal at the frequency of operation. IF section performs the digital to analog conversion and vice versa. It also contains the signal processing like Filtering, modulation and demodulation, Digital up conversion (DUC), Digital down conversion (DDC) etc. The last stage of the radio is the baseband processor. It is at this point that the digital data is processed [9][4]. We have used GNURadio and USRP N210 to confgure the SDR to implement the Cognitive Radio test-bed.

A block diagram of a USRP-based SDR transceiver built with a GNURadio flow graph is shown in Figure 3.2. USRP kit is used as a hardware while GNURadio package is used for the baseband signal processing tasks. The next sections describe USRP kits and GNURadio package.

3.1 USRP

The USRP (Universal Software Radio Peripheral) is intended to provide a low-cost, high quality hardware platform for software radio. It is designed and marketed by Ettus Research, LLC. It is commonly used by research labs, universities, and hobbyists. The USRP platform is designed for RF applications from DC to 6 GHz. USRPs connect to a host computer through a high-speed USB or Gigabit Ethernet link, which the host-based software uses to control the USRP hardware and transmit/receive data.

The USRP Hardware Driver (UHD) is the official driver for all Ettus Research products. The UHD supports Linux, Mac OS X and Windows.

In this project we are using a particular model of USRP product known as the

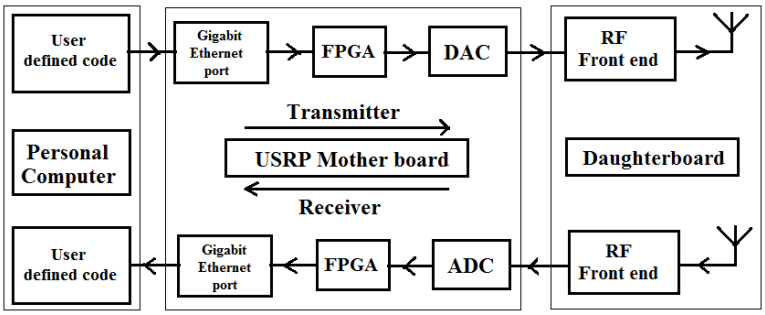

Figure 3.3: Block diagram of USRP [4].

USRP N210.

3.1.1 USRP N210

The USRP N200 and N210 are the highest performing class of hardware of the USRP family of products, which enables engineers to rapidly design and implement powerful, flexible software radio systems. The N200 and N210 hardware is ideally suited for applications requiring high RF performance and great bandwidth. Such applications include physical layer prototyping, dynamic spectrum access and cognitive radio, spectrum monitoring, record and playback, and even networked sensor deployment. The Networked Series products offers MIMO capability with high bandwidth and dynamic range. The Gigabit Ethernet interface serves as the connection between the N200/N210 and the host computer. This enables the user to realize 50 MS/s of real-time bandwidth in the receive and transmit directions, simultaneously (full duplex).

3.2 GNURadio package

GNURadio is an open source software toolkit for building software defined radios. GNURadio is build with the aim to bring the code as close to the antenna as possible and thereby turn hardware problems into software problems. GNURadio has software equivalents of real world radio system components like filters, demodulators, equalizers and other building blocks for signal processing, as well as a framework for data flow control between them. We can build a software defined radio by connecting these blocks together.

Basically GNURadio does all the signal processing. Functions provided by GNURadio includes Mathematical operations, Interleaving, delay blocks, Filters, FFT blocks, Automatic Gain Control (AGC) blocks, Modulation and demodulation

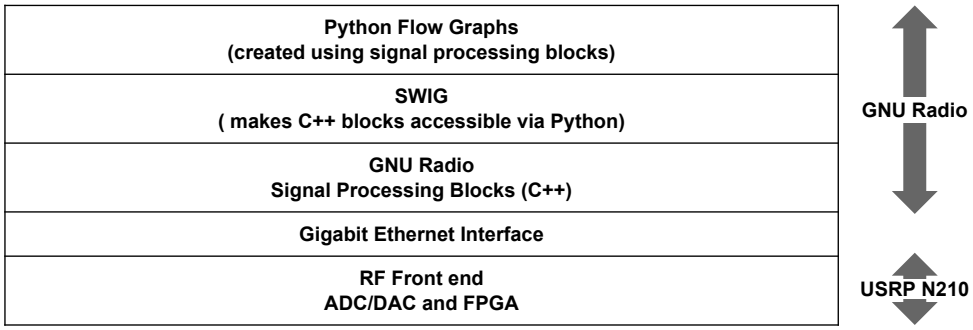

Figure 3.4: Architecture of GNU Radio

(FM, AM, PSK, QAM, GMSK, OFDM and etc), Interpolation and decimation. Apart from signal processing blocks, GNURadio also provides support for various signal sources and sinks, such as Signal generators, Noise generators, Pseudo random number generators, USRP source and sink, Graphical sinks, Audio source and sink, File source and sink and etc [10]. GNURadio applications are primarily written using thePython programming language.

USRP is the hardware used along with GNURadio for SDR and is either at the beginning of the flow graph (implementation of a receiver) or the end (transmitter).

Chapter 4

OpenBTS

4.1 What is OpenBTS?

OpenBTS is a Unix application that uses a software radio to present a GSM Um interface to handsets and uses a SIP softswitch or PBX to connect calls.(You might even say that OpenBTS is a simplified form of IMS that works with 2G feature-phone handsets). The combination of the global -standard GSM air interface with low cost VoIP backhaul forms the basis of a new type of cellular network that can be deployed and operated at substantially lower cost than existing technologies in many applications, especially rural cellular deployments and private cellular networks in remote areas.

4.2 The OpenBTS Application Suite

A complete OpenBTS P2.8 installation comprises several distinct applications:

OpenBTS The actual OpenBTS application, containing most of the GSM stack above the radio modem.

Transceiver The software radio modem and hardware control interface.

Asterisk The VoIP PBX in the standard public release configuration.

Smqueue The store-and-forward server for text messaging.

Subscriber Registry A database of subscriber information that replaces both the Asterisk SIP registry and the GSM Home Location Register (HLR).

Other Servers Other optional GSM services, beyond speech and text messaging, are supported through external servers.

The OpenBTS and Transceiver applications must run inside each GSM/SIP access point. The Asterisk and the subscriber registry applications are communicated through the filesystem and therefore must run on the same computer, but that computer can be remote from the access point. smqueue and the other servers can run anywhere and may have multiple instances.

4.2.1 OpenBTS

The OpenBTS application contains:

- L1 Time division multiplexing(TDM) functions (GSM 05.02)
- L1 Forward error correction(FEC) functions (GSM 05.03)
- L1 closed loop power and timing controls (GSM 05.08 and 05.10)
- L2 Link access protocol on Dm-channel (LAPDm) (GSM 04.06)
- L3 radio resource management functions (GSM 04.08)
- L3 GSM-SIP gateway for mobility management
- L3 GSM-SIP gateway for call control
- L4 GSM-SIP gateway for text messaging

The general design approach of OpenBTS is avoid implementing any function above L3, so at L3 or L4 every subprotocol of GSM is either terminated locally or translated through a gateway to some other protocol for handling by an external application. Similarly, OpenBTS itself does not contain any speech transcoding functions above the L1 FEC parts.

4.2.2 Transceiver

The transceiver application performs the radio modem functions of GSM 05.05 and manages the Gigabit Ethernet interface (USB2 interface, in case of USRP1 or older models) to the radio hardware.

4.2.3 Asterisk

OpenBTS uses a SIP switch or PBX to perform the call control functions that would normally be performed by the mobile switching center in a conventional GSM network, although in most network configurations this switching function is distributed over multiple switches. These switches also provide transcoding services. In OpenBTS P2.8 the standard SIP switch is Asterisk 1.8.

4.2.4 Subscriber Registry

OpenBTS uses a modified SIP registry as a substitute for the home location register found in a conventional GSM network. OpenBTS also relies on Asterisk for any transcoding functions.

4.2.5 Smqueue

Smqueue is a store-and-forward server that is used for text messaging in the OpenBTS system. Smqueue is required to send a text message from one MS to another, or to provide reliable delivery of text messages to an MS from any source.

4.2.6 Network Organization

In the simplest network, with a single access point, all of the applications in the suite run inside the access point on the same embedded computer. Figure 4.1 describes this.

The smqueue block handles SMSs. The subscriber registry database contains the details of all registered users and it maps the registered IMSIs to corresponding dialling numbers. The softswitch connects speech calls (e.g. Asterisk, FreeSwitch). The transceiver performs radio modem functions and manages the Gigabit Ethernet interface (USB2 interface, in case of USRP1 or older models) to the USRP device. The OpenBTS itself is the GSM implementation from the TDMA part of L1 up through L3 and the L3/L4 boundary. It has a SIP interface to communicate with the other blocks like smqueue, subscriber registry, etc.

In larger network, with more than one access points, one of the BTS can behave as a master and provide servers to the rest of them. Figure 4.2 describes a network with two access points where a master access points is providing servers to the

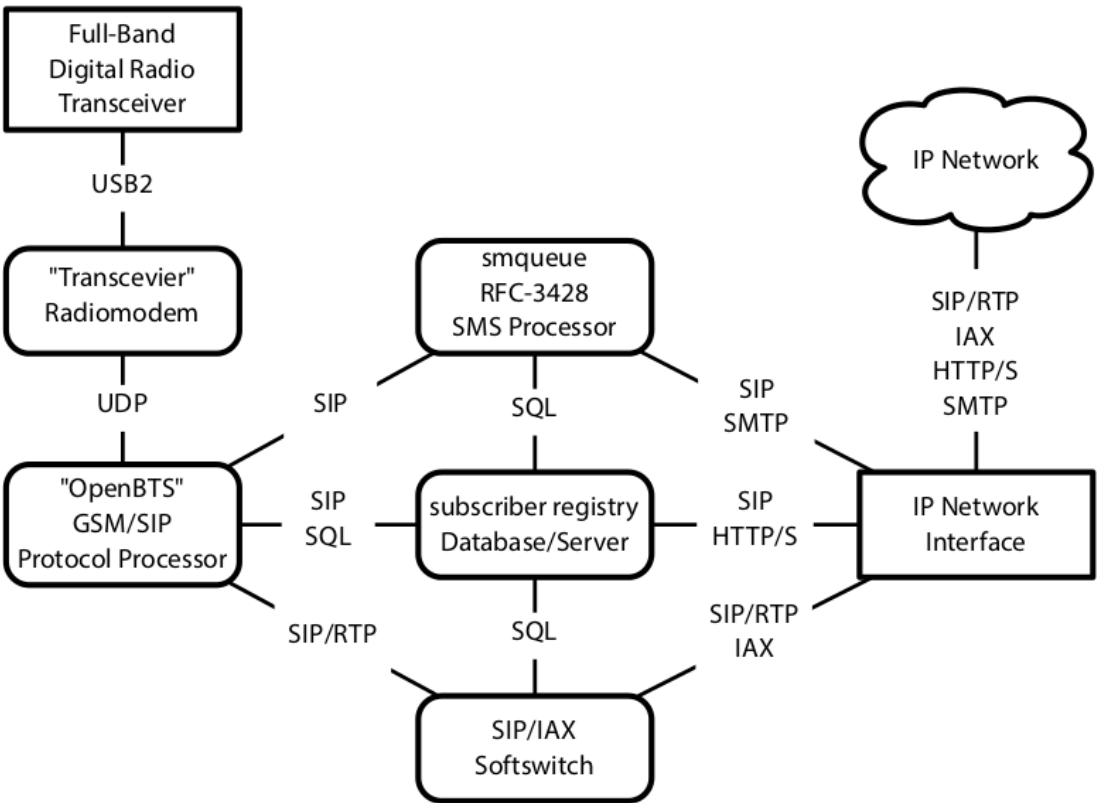

Figure 4.1: Network Organization of OpenBTS [11].

other one. The Transceiver applications and the OpenBTS must run in each GSM/SIP access point. The Asterisk and the Subscriber Registry applications (SIPAuthServe) communicate via the filesystem and hence must run in the same computer, but that computer can be remote to the access point. SMQueue and other servers can run in any access point and can have multiple instances.

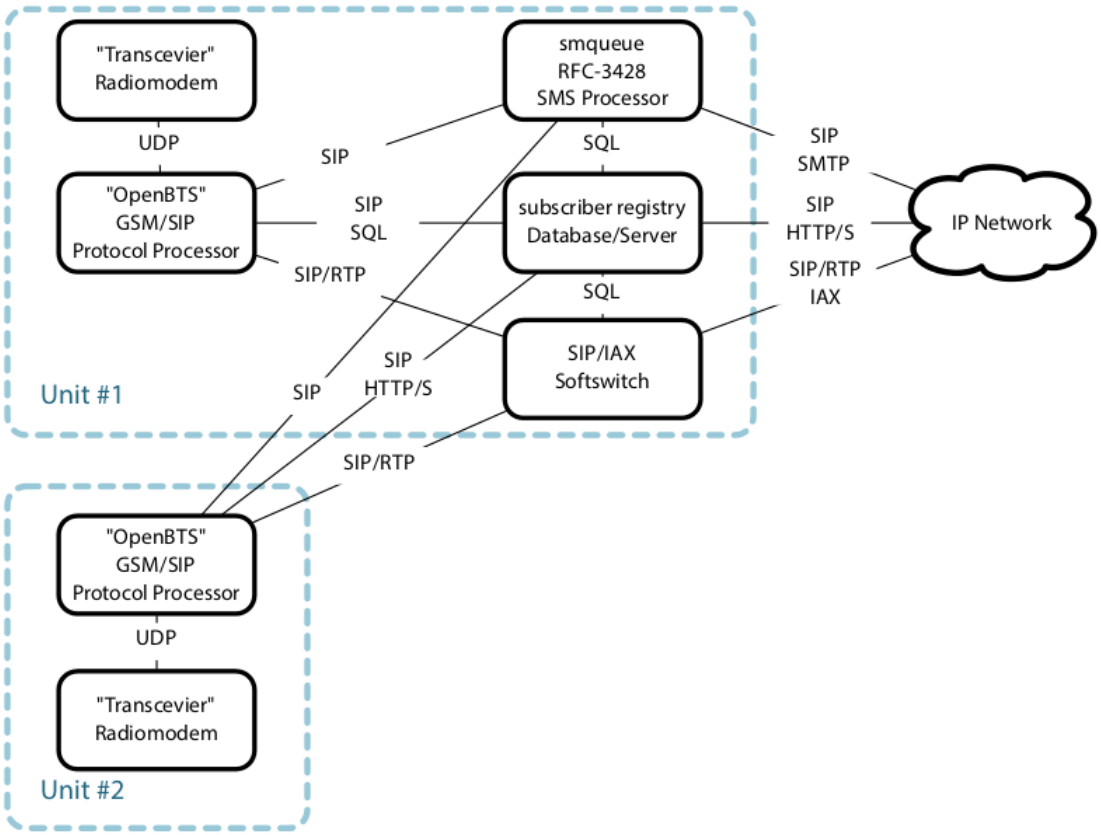

Figure 4.2: Two access points with unit #1 providing servers for both [11].

Chapter 5

SIM registration on OpenBTS network

The first task in our project is registration of the SIM in the local network that we have established using the OpenBTS software and USRP kits. In order to do this, we first establish the local network and then try to detect this network in the mobile by searching for all the available networks. We set the operator selection setting in the mobile network settings as manual instead of automatic. Then we select the local network as our choice of network for operation. Since the mobile is not registered in this network an SMS is been send by the base station indicating the IMSI of the mobile phone and asking for its registration. So the next we do is we do the entry of this IMSI number at three places : extension.conf, sip.conf and sqlite3.db..The following diagrams are the screen shots of these changes done by us for registration.

5.1 Sip.conf

Sip.conf is for user devices configuration. SIP is a session initiation protocol which is a protocol for call session handling. Sip.conf is a file in */etc/asterisk* used to configure SIP devices for communication with the asterisk system. We have sections for each SIP users also referred to as sip extensions, in this file. The first option of these sections is the name of the user device. We have named each user device using the IMSI of the SIM used by the device. The second option defines the caller ID that we have assigned to the user. The next option describes the type which we have set as friend. This tells that the match will happen first with the name and then the IP address. If it is set to peer the IP address will be

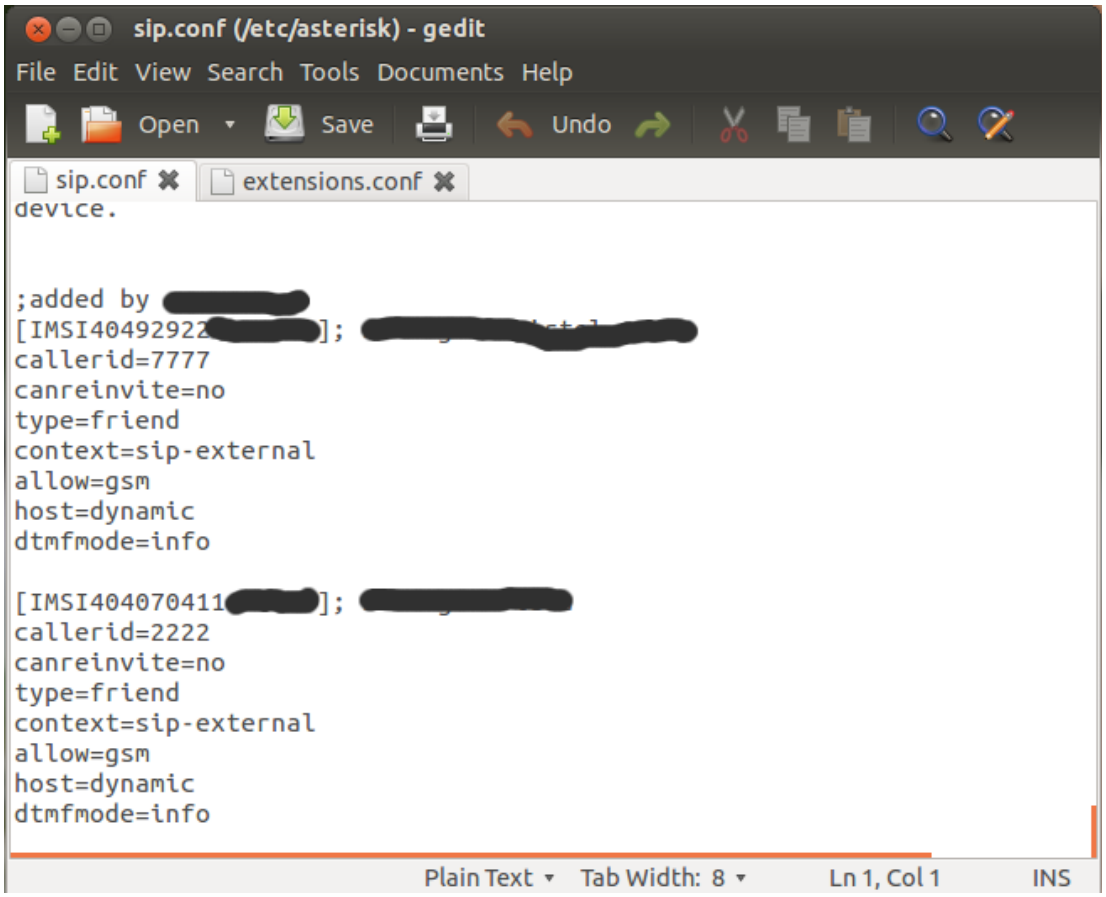

Figure 5.1: Screenshot of *sip.conf*.

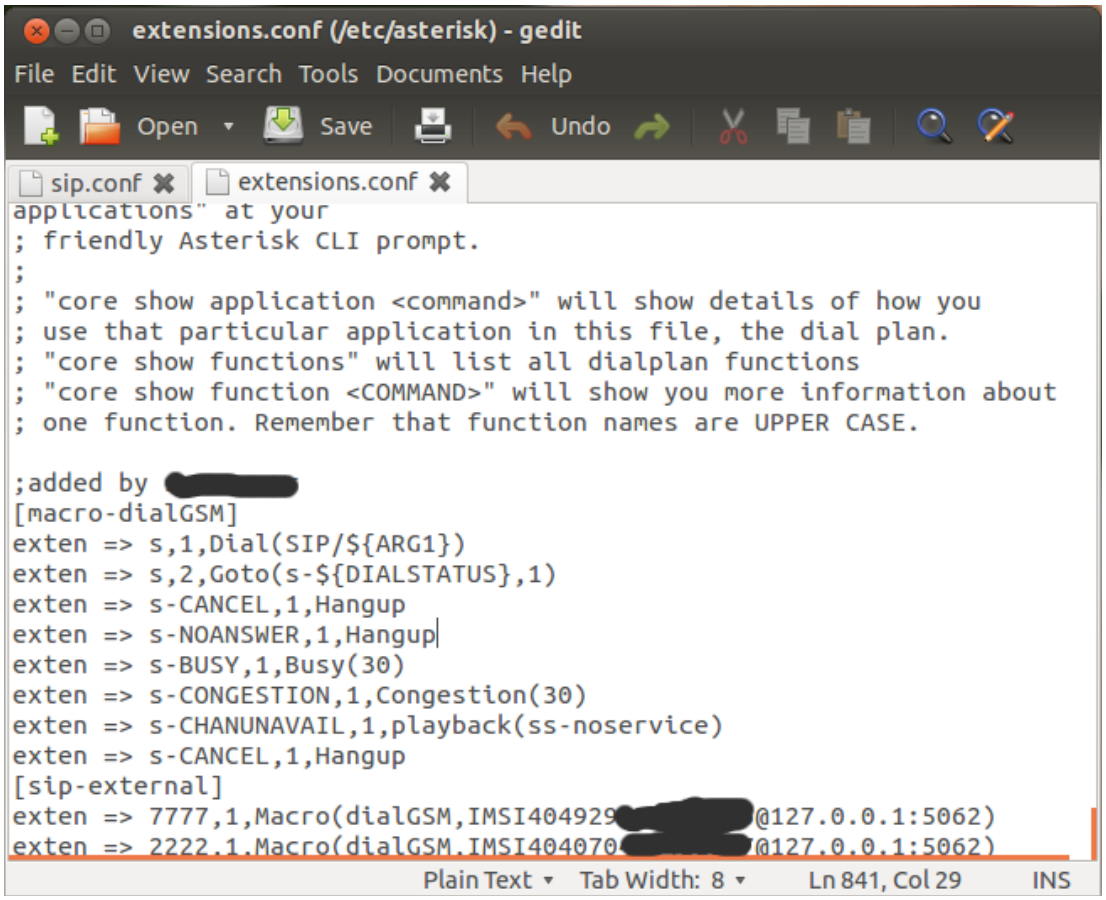

Figure 5.2: Screenshot of *extensions.conf*.

directly matched. If it is set user only the name will be matched directly. Next option is the context which defines which dial plan from the extension.conf file will be used. The next option is allow which refers to the audio codec that will be allowed for the call.

5.2 Extension.conf

This file is also in there inside etc/asterisk and it consists of the description of the dial plan. The dial plan defines how the calls flow into and out of the system, a form of scripting language , the dialplan contains instructions that asterisk follows in response to external triggers. Add following lines at end of the file extension.conf file. We should use macros to avoid repeating the same dial plan for every client as below.

```
[macro-dialGSM]
exten => s,1,Dial(SIP/${ARG1})
exten => s,2,Goto(s-${DIALSTATUS},1)
```

```
exten => s-CANCEL,1,Hangup
exten => s-NOANSWER,1,Hangup
exten => s-BUSY,1,Busy(30)
exten => s-CONGESTION,1,Congestion(30)
exten => s-CHANUNAVAIL,1,playback(s-noservice)
exten => s-CANCEL,1,Hangup
```

Now we define a new context which maps between Caller Id and the IMSI as shown below. This is needed because when you make a call, you don't dial a destination IMSI but you call its caller ID.

```
[sip-external]
exten => 200,1,Macro(dialGSM,IMSI404201378074 62@127.0.0.1:5062)
exten => 202,1,Macro(dialGSM,IMSI404201675035769@127.0.0.1:5062)
```

5.3 sqlite3.db

Figure 5.3 is the screenshot of the dialdatatable in the sqlite3.db file. Sqlite3.db is the database in sqlite format. It is part of the asterisk only. There are two tables in this database. One is dialdatatable and sip_buddies. Dialdatatable contains mapping from IMSI to the dialing number defined by us. Sip_buddies contain user device configuration similar to what we have it sip.conf. If we fill up only the dialdatatable and not sip_buddies during SMS the IMSI numbers will be shown instead of the SIP usernames (phone numbers) which is not very convenient.

After doing these specified changes we can call using the registered SIMs using the local network and also send SMS. More than one pair of users can be registered in the network. But if two calls happen simultaneously time division multiplexing is done as OpenBTS can operate only on one frequency at a time.

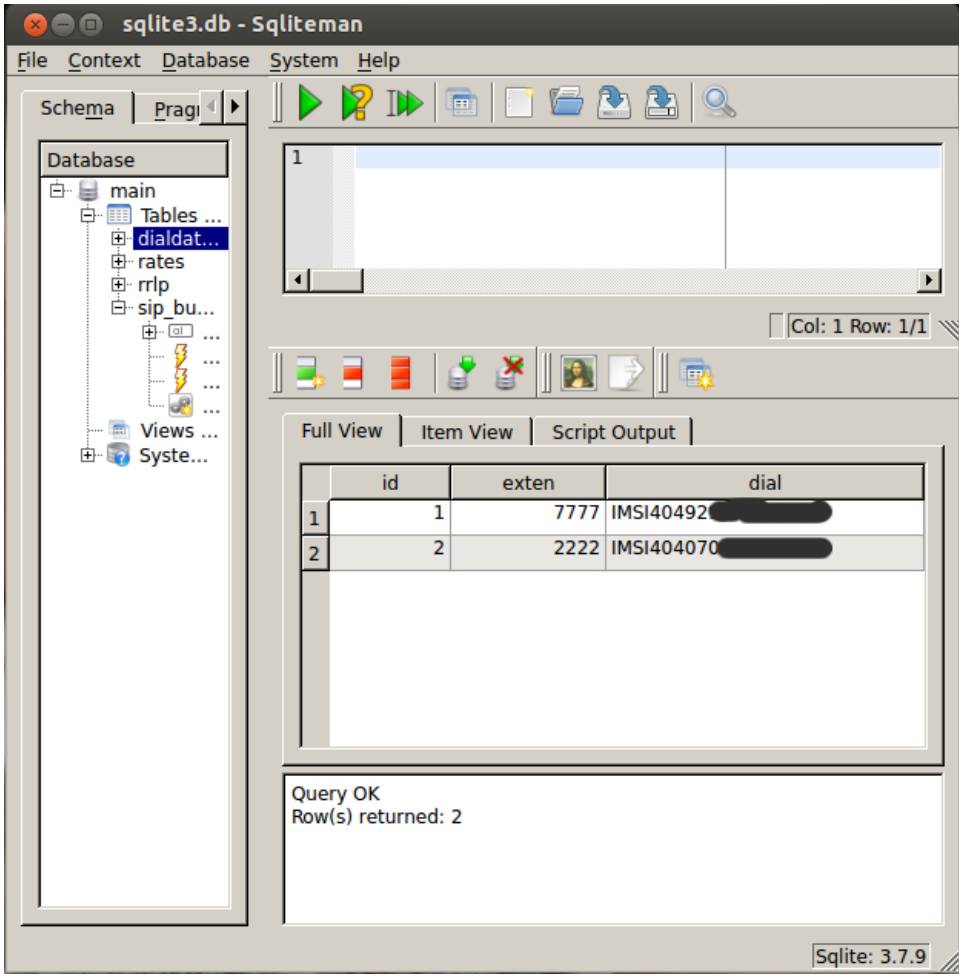

Figure 5.3: Screenshot of `dialdatatable`

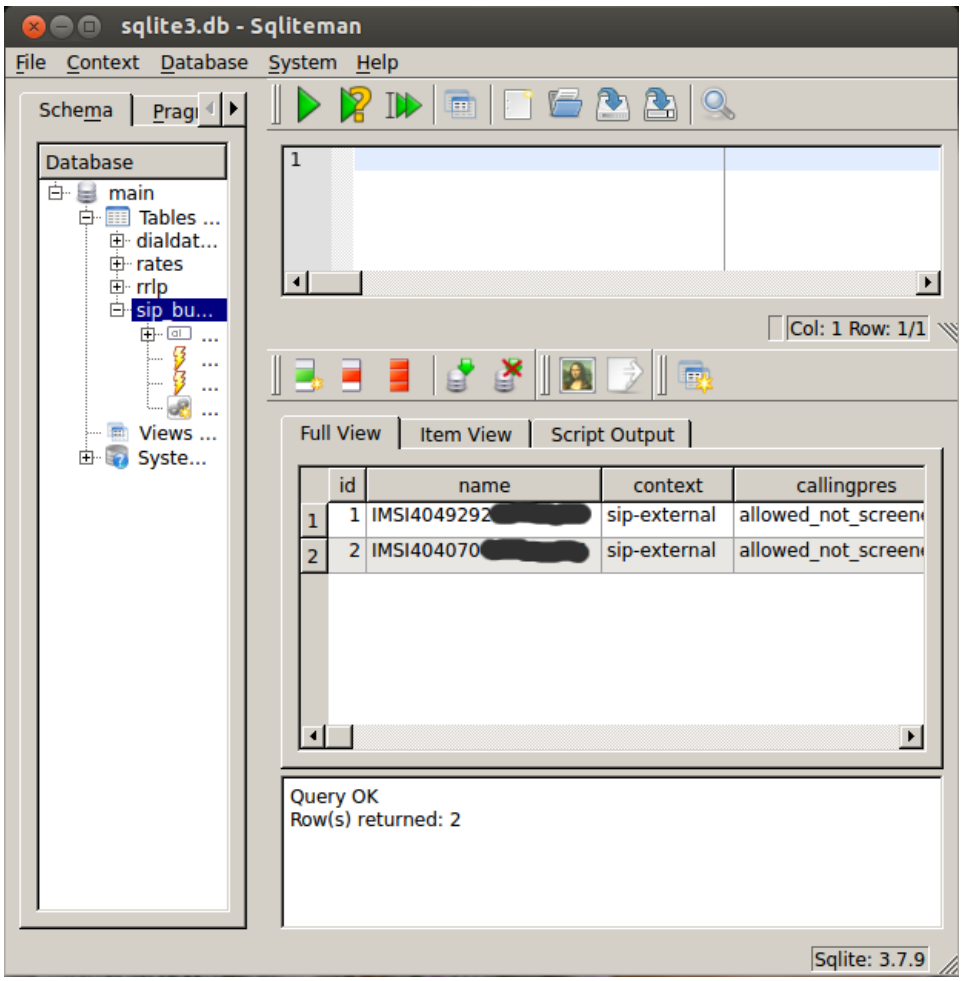

Figure 5.4: Screenshot of `sip_buddies`

Chapter 6

Spectrum Sensing

Due to limited availability of spectrum resource, there is a serious impact on the emerging mobile applications. Hence there is a need to efficiently utilize the available radio spectrum. The problem right now is not the physical scarcity of the radio spectrum rather the inefficient use of the spectrum. Solution to this is cognitive radio. The major problem in cognitive radio is to detect spectrum holes which can be utilized by secondary users for communication and to enable secondary users to quit the frequency band as soon as the corresponding primary radio emerges. This technique is called spectrum sensing. Spectrum sensing is the first step to implement cognitive radio system.

There are various methods for local spectrum sensing proposed by researchers.

The following section describes three important methods:

1. Energy detection
2. Matched filter detection
3. Cyclostationarity detection

6.1 Energy Detection

Measuring the energy of a particular band is one of the simplest techniques to detect the presence of primary users in that band. It is one of the most widely used technique to detect spectrum holes as it requires no a priori knowledge of the primary radio. Apart from this major advantage the technique is very cost efficient and less complex compared to other techniques. We calculate the energy of the received radio spectrum and this energy is compared with a predefined

energy detection threshold to conclude whether primary user is present or absent in the frequency of interest. This technique is an optimal one when we have absolutely no knowledge of the user occupying the channel in advance. The following block diagram describes energy detection technique:

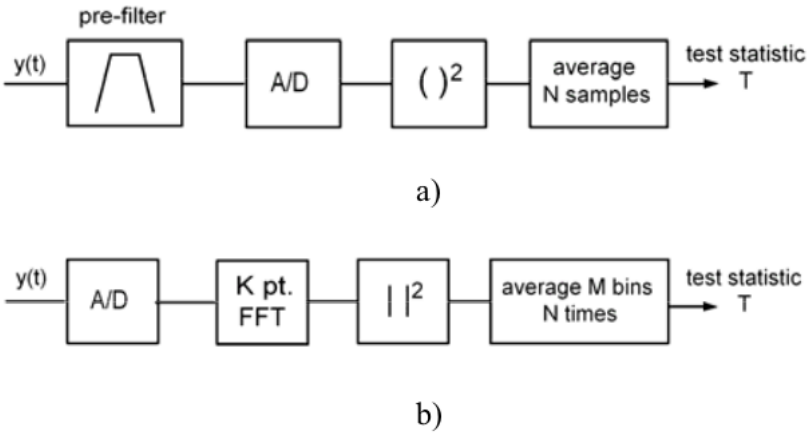

Figure 6.1: Block diagram of Energy Detection implementation[12].

As described in the energy detection block diagram, it is basically a hypothesis testing problem with two possible hypothesis H_0 and H_1. Hypothesis H_1 concludes the presence of primary users in the band of interest and hypothesis H_0 concludes their absence. And energy detection technique is basically about distinguishing between these two hypotheses[13].

$$\begin{aligned} H_0 : &\qquad x(t) = n(t); \\ H_1 : &\qquad x(t) = hs(t) + n(t); \end{aligned}$$

$x(t)$ is signal received by secondary user and $s(t)$ is primary radio signal, $n(t)$ is additive white Gaussian noise (AWGN) and h is the amplitude gain of the channel. $s(t)$ and $n(t)$ are assumed to be independent of each other. Signal detection is performed using an energy detector and compute decision statistics Y which corresponds to energy collected in observation time T and bandwidth W and comparing this statistics to a predetermined threshold γ. In our project energy detection is implemented using average periodogram analysis which is covered in later part of this chapter.

6.2 Matched filter detection

Matched filter is a linear filter used to match a particular transit waveform with the reference signal. The output is maximum when the match happens. When there is a priori knowledge of primary radio, matched filter technique is applied. Matched filter operation is equivalent to correlation operation in which the incoming signal is convolved with a filter whose impulse response is mirror and shifted version of reference signal. This output is then compared with the threshold for primary user detection. It is mathematically defined as:

$$Y[n] = \sum_{k=-\infty}^{\infty} x[k]h[n-k]$$

x is the unknown signal and h is the impulse response of matched filter which is matched to reference signal for maximizing SNR.

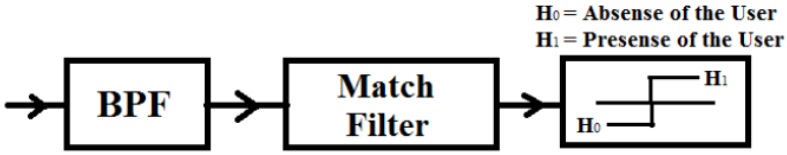

Figure 6.2: Block diagram of Matched Filter implementation [4].

There is a constraint on this technique. We need to have a prior information about the primary radio to perform matched filtering. However matched filter requires demodulation of primary signal which means it has information of primary radio both at the PHY layer and the MAC layer like operating frequency, modulation type, packet format bandwidth etc. But the cumbersome part is it has to achieve coherency with primary user by means of timing and carrier synchronization. This coherent detection is still achievable since primary signals have pilots, preambles etc to serve the purpose. The advantage of matched filter detection is when the information of the primary user signal is known, it is optimal detection in stationary Gaussian noise. But the performance of matched filter detection depends on the accuracy of the information of primary radio. This technique also requires cognitive radio to have dedicated receiver for every type of primary user which in turn results in complex hardware and large power consumption[14].

6.3 Comparision of various spectrum detection techniques

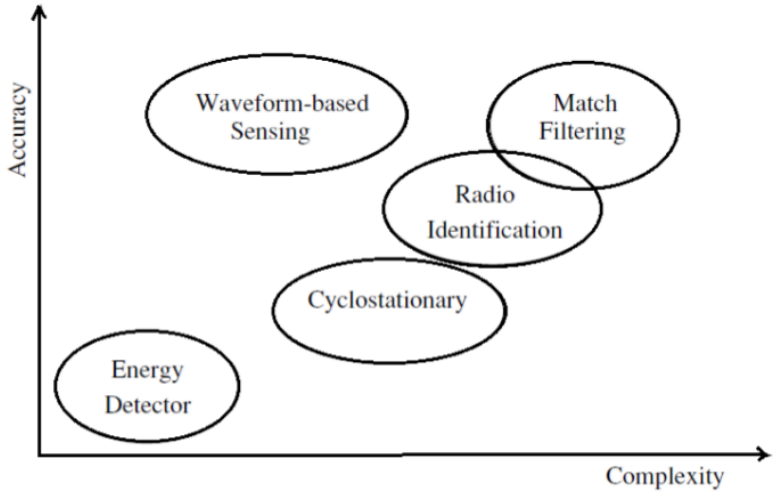

Figure 6.3: Comparison of sensing methods [4]

Figure 6.3 compares various spectrum sensing techniques on the basis of their accuracy and complexity. We can see that energy detection technique is the least accurate and least complex of all where as matched filtering is most complex and highly accurate. Other techniques lie in between with some having more accuracy and some less complex. There is no ideal detector that suits all occasions. Thus decisions, compromises and tradeoffs must be made depending on primary radio type, transmission and propagation characteristics, characteristics of secondary user receiver, and etc[15].

6.4 Implementaton of energy detection technique

We have used energy detection technique for spectrum sensing in our project for the detection of primary users in the band of interest. Average periodigram analysis is a method to implement energy detection technique of spectrum sensing. This section describes average periodogram analysis. Implementation of wide band spectrum analyzer using this technique is also described in this section.

6.4.1 Average periodogram analysis

Average Periodogram analysis estimates the power spectrum of the received signal and it is based on the Discrete Fourier Transform (DFT) of finite length

segments of signal. In this technique signal is sectioned into finite length segments and periodogram of each segment is calculated which are also referred to as modified periodograms. Then an average of all these modified periodogram is calculated[16].

Let $X[n]; n = 0, 1...L-1$ be the discrete time signal which is divided into M finite length segments of equal length, where N is the length of each segment i.e. $MN = L; X_r[n]; n = 0, 1...N-1$ is the rth segment and $W[n]; n = 0, 1...N-1$ is the window applied to each segment. The modified periodogram for the rth segment is,

$$I_r[k] = \frac{1}{NU} |V_r[k]|^2 \qquad k = 0, 1...N-1$$

where $V_r[k]$ is a N point DFT and U is normalization factor i.e. , $V_r[k] = DFT\{W[n] * X[n]\}$ and $U = \frac{1}{N}(\sum_{n-0}^{N-1}(W[n])^2)$. The PSD of $X[n]$ sequence is then the time averaged periodogram estimate ,

$$I[k] = \frac{1}{M} \left| \sum_{r=0}^{M-1} X_r[k] \right|$$

6.5 Wide band spectrum analyzer

GNU radio packages provide a tool for wide band spectrum sensing called usrp_spectrum_sense.py. It is used as a basic code for wide band spectrum analyzer implementation. The output of this code is the magnitude squared of the FFT. This means for each FFT bin[i] the output is $Y[i] = re[X[i]] * re[X[i]] + im[X[i]] * im[X[i]]$. We can calculate the power by taking square root of the output. We need N time samples of $x(t)$ sampled at a sampling frequency of F_s to use N point complex FFT $X(\omega)$ analysis. An appropriate window function is to be selected to reduce spectral leakage and applied to these time samples. The output of the complex FFT will represent the frequency spectrum content as follows: The first value of the FFT output ($bin0 == X[0]$) is the passband centre frequency The first half of FFT spectrum ($X[1]$ to $X[N/2-1]$) contains the positive baseband frequencies, which corresponds to the passband spectrum from centre frequency to $+F_s/2$. The second half of the FFT ($X[N/2]$ to $X[N-1]$) contains the negative baseband frequencies, i.e. from $-F_s/2$ to centre frequency.

For our project purpose, we collected 1024 samples using a tuner centered at uplink frequency of our interest, say 900 MHz. 1024 is choosen as the number of FFT points because the number of FFT points has to be a power of 2 for the fast execution of the FFT algorithm. Default sampling frequency is set as

1 MHz. The frequency resolution is therefore: 1 MHz / 1024 = 976.56 KHz. The decimation is defined as dsp rate divided by sample rate. The UHD driver requires the decimation value to be an even number. The dsp rate is the actual hardware-level sampling rate of the USRP kit. It is the rate at which the USRP device takes analog samples from the external world and converts them to digital form. The dsp rate of the USRP is 100 MHz. Hence we chose sampling frequency to be 1 MHz which gives a decimation value of: 100 MHz / 1 MHz = 100.

A GSM band is of 200 KHz. So, in order to calculate the energy in a particular frequency channel of interest, we need to find the average of all the bin values which lie in the 200 KHz band centered at that frequency.

Chapter 7

Two-frequency Cognitive Radio Test-Bed

The main aim of this project is to demonstrate the coexistence of primary users and secondary users in the GSM band. Also it has to be ensured that primary users is given a higher priority over the secondary users and there should be no mutual interference. Analysis of radio spectrum assigned to primary users conclude that it is most of the time underutilized. The spectrum bands which are assigned to primary user and are not utilized by them at certain time instants are called spectrum holes. So in order to accomplish coexistance of primary and secondary users, implementation of a cognitive radio which detects these spectrum holes in the radio spectrum and enables secondary users to utilize these for communication is needed. An experimental setup is developed for this demonstration using OpenBTS and GNU radio software and USRP N210 as hardware. First a 2-frequency system is developed which is then expanded to a 4-frequency system.

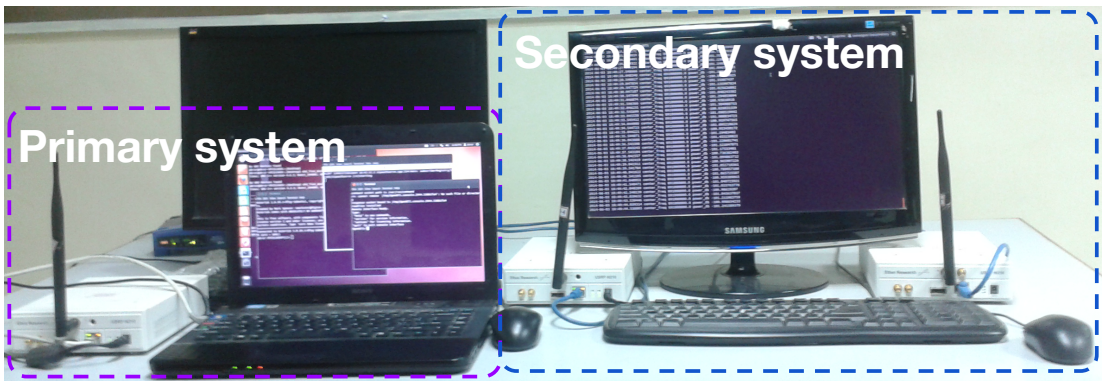

Figure 7.1: Experimental setup of the 2-frequency system

7.0.1 2-frequency system description

Figure 7.1 describes the experimental setup for 2-frequency system. It consist of one primary and one secondary subsystems. The primary subsystem has only OpenBTS software and one USRP for RF front. Where as secondary subsystem has OpenBTS along with GNU radio and two USRP kits for each of these softwares as hardware RF front. This secondary subsystem has cognitive capabilities. To provide cognitive capabilities it was necessary for OpenBTS and GNU radio to run together in the same computer and communicate with each other which was challenging. Secondary subsystem continuously senses the frequency band of interest and takes decision depending upon the analysis of the data collected and changes its parameters accordingly so that primary and secondary users coexist. The spectrum sensing is accomplished by using GNU radio. GNU radio and OpenBTS of the secondary subsystem were made to coordinate and behave in appropriate manner and take dynamic decisions as and when required to make over all system behave cognitively.

7.0.2 2-frequency system testing

For 2-frequency cognitive system, two GSM bands are used with centre frequency 945MHz (F_1) and 950MHz (F_2). Secondary users are made to occupy one of these two bands say F_1. Then we make primary users enter the same band. This results in an increase in energy levels in this band which is sensed by the secondary subsystem as it is continuously scanning this band. Immediately secondary users are shifted to other frequency band (F_2) thereby vacating F_1 for primary users. Periodogram analysis is used to calculate the energy levels in the band. Hence a 2-frequency cognitive system demonstrating coexistence of a pair of primary and secondary users is accomplished. The whole technique for this cognitive behavour of the secondary subsystemis described using a flow graph shown in figure 7.2:

As we can see in the flow graph, we begin with spectrum sensing where we choose optimal channel out of 945MHz and 950Mhz for secondary OpenBTS operation. Then secondary OpenBTS is made to operate on this channel which is utilized for communication by secondary users. This band of operation is continously scanned after every time interval 't' to check for the presence of primary radio. If energy is lower than predefined threshold we rescan the channel as it is seen in the flow graph. If at any time instant the energy is found to be higher than the predefined threshold, we conclude that primary radio has appeared and there is a need to vacate the channel. Hence OpenBTS of the secondary subsystem is

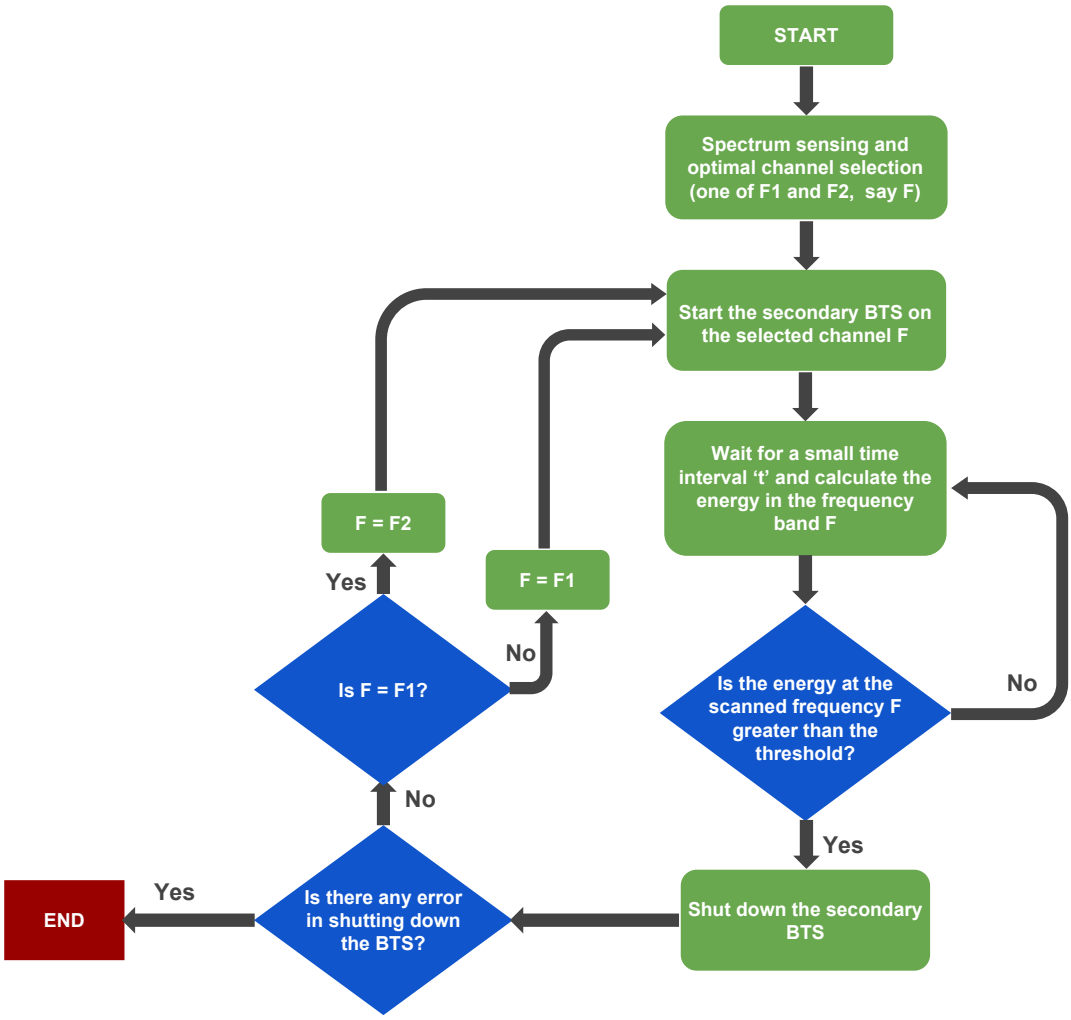

Figure 7.2: Flowchart for 2-frequency system

switched off and restarted with now frequency band of operation as F1 if it was F2 previously and viceversa. And next we go back to the second step in the flow graph that is contious spectrum scanning. If there are any issues in switching off of the OpenBTS the algorithm reaches end.

7.1 CUSUM

CUMSUM peak detection is also applied after energy detection to ensure that the detected high energy in the band of interest is not due to some irrelevant reasons like random fluctuations in noise power etc, but due to the presence of primary radio in that band. This ensures high accuracy in primary radio detection and correct decision making. CUSUM is basically a sequential analysis technique to detect change. It is a criterion for deciding when to take corrective action. As

the name implies CUSUM involves calculating cumulative sum. This makes it sequential. The samples from a process x_n are assigned weights ω_n and summed as followed,

$$S_0 = 0;$$
$$S_{n+1} = max(0, S_n + x_n - \omega_n)$$

When the value of S exceeds a certain threshold value a change in value has been found. This formula detects change only in positive direction. To detect change in negative direction we have to do min operation instead of max operation and the change is detected when value goes below the threshold.

Chapter 8

Four-frequency Cognitive Radio Test-Bed

The 2-frequency system is expanded to a 4-frequency system by adding another primary subsystem to the 2-frequency experimental setup. Here we assume radio spectrum to be made up of four freqencies instead of two. Secondray subsystem finds optimum channel out of these four frequencies for openBTS operation.

8.0.1 4-frequency system description

The experimental setup of the four freqency system has has two primary subsystems and one secondary subsystem as described in figure 8.1. Primary subsystem has OpenBTS and one USRP kit and secondary subsystem has OpenBTS and GNU radio software and two USRP kits as we had previously in 2-frequency system. Here we have four GSM bands with centre frequencies F_1=936MHz, F_2=943MHz, F_3=950MHz, F_4=957MHz as the radio spectrum.

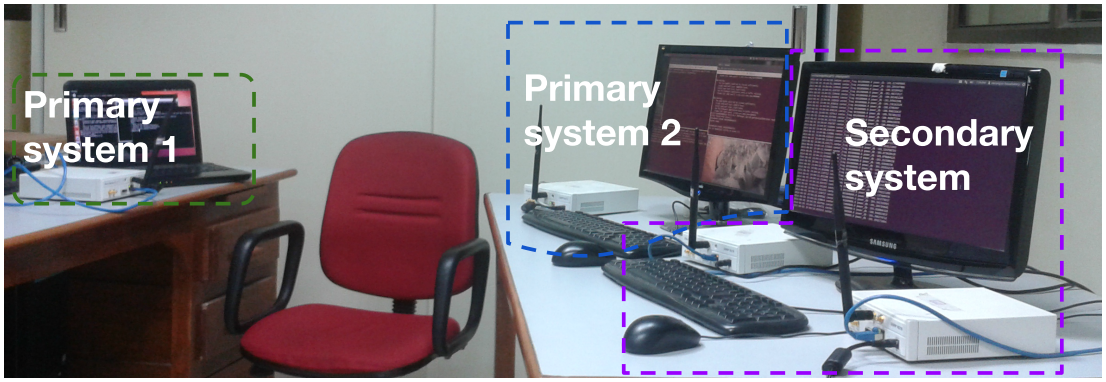

Figure 8.1: Experimental setup of the 4-frequency system

8.0.2 4-frequency system testing

Here we make one pair of primary users occupy one of the four frequencies say F_2. We make secondary users use one frequency say F_1. Now other pair of primary users are made to try and enter frequency F_1 for communication. This is sensed by the secondary system and it tries to migrate secondary users to F_2 which is also occupied. Our secondary system detects that F_2 is occupied and therefore continues to find a spectrum hole in a 4-frequency spectrum. It finds that frequency F_3 is unoccupied and thus allows secondary users to enter F_3 and utilize it for communication. The difference between a 4-frequency system and a 2-frequency system is that in a 4-frequency system the secondary subsystem has to first confirm absence of primary users in the band before making secondary users migrate to that band . This was not the case in 2-frequency system as it has only one pair of primary users. Hence the other band where secondary users will be made to migrate is always unoccupied at the time of switching secondary radio to that band. So there is no need to check for the peresence of primary users in that band.

The flow graph in figure 8.2 describes the algorithm for secondary subsystem of the 4-frequency cognitive system. We begin with optimal channel selection out of four frequencies 936MHz, 943MHz, 950MHz, 957MHz by using peridogram analysis . OpenBTS is started on this choosen frequency. Then we continously check for the presence of primary radio on this channel after every time interval 't'. If energy goes above predefined threshold OpenBTS of the secondary subsystem is switched off and restarted on a frequency which is seven more than previous frequency. If the previous frequency of operation was 957MHz than the new frequency is 936MHz. From here we go back to the second step of algorithm that is spectrum scanning. If there are issues in switching off of OpenBTS when algorithm reaches end.

The spectrum sensing is done by energy detection technique and it was required that a proper threshold is set for decision making. A number of readings were taken to decide the noise level, energy level when only primary users are occupying and also energy levels when both primary users and secondary users exist in the same band for a short duration of time. The threshold value depends on the power transmitted by the users and their distance from the USRP kits which is RF front for GNU radio. This distance dependency can be removed by setting the threshold much lower so that even if the users move far away, the decision making is not affected.

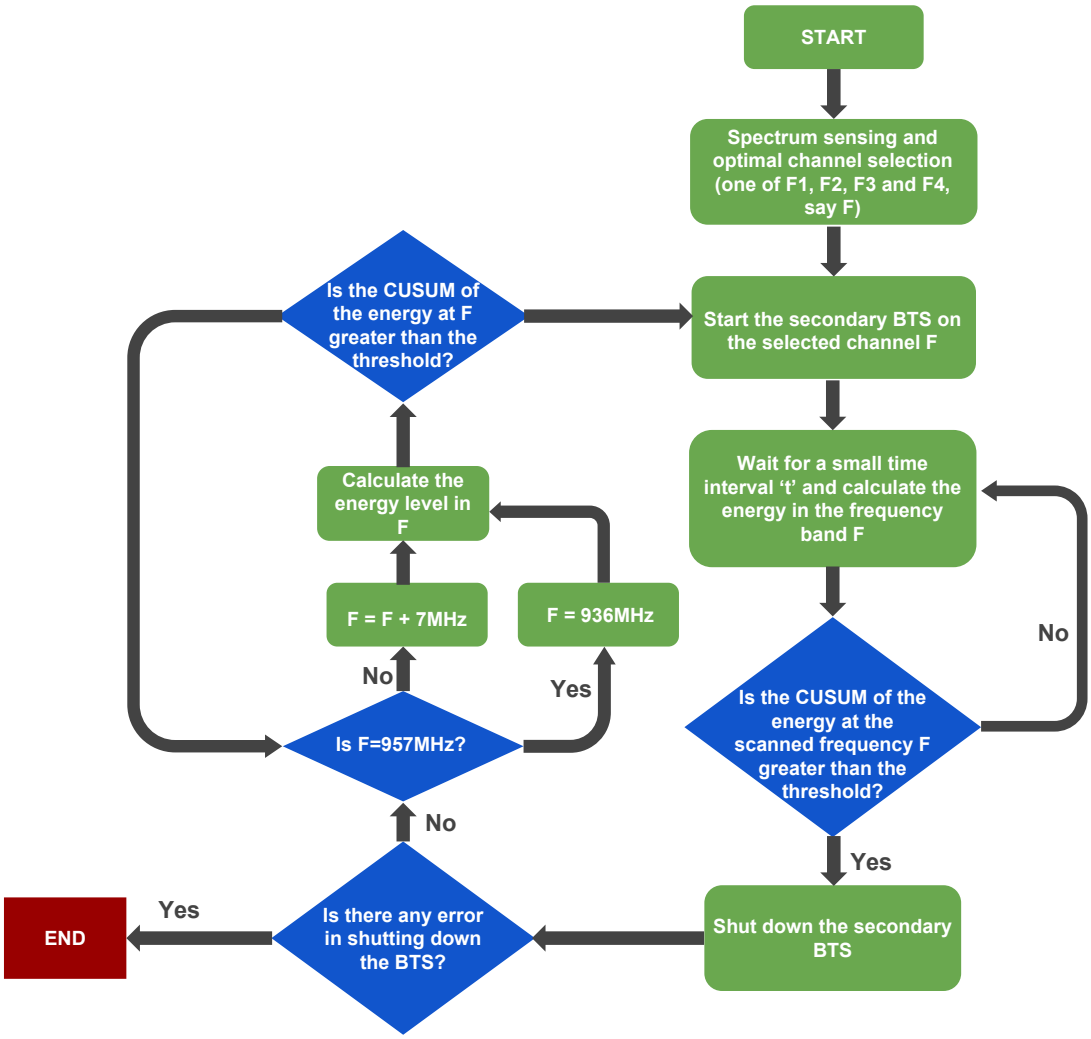

Figure 8.2: Flowchart for 4-frequency system

8.1 Wrap up

This section describes challenges we faced and tasks we accomplished while developing the 2-frequency and 4-frequency cognitive radio test-bed.

1. We began by exploring what cognitive radio is and how it can be used in the already existing radio. Ongoing work in the field of cognitive radio was surveyed.

2. An FM receiver was designed using GNURadio Companion to get ourselves familiarized with GNU software package.

3. GNURadio applications are primarily written in the Python programming language which we were required to extensively use for our work.

4. USRP N210 kit is used as hardware in our project. We carried out range testing of this kit to ensure distance is not a major factor in our decision making algorithm and can be neglected.

5. The next task was to understand the working of OpenBTS software. Starting with the installation of this software, we were able to register our GSM SIM cards in the local network established by OpenBTS and perform calling and sending SMS between our phones using this network. USRP kits are used as hardware end in the local network establishment.

6. Since spectrum sensing is major part of cognitive radio, spectrum sensing techniques were explored. We chose energy detection spectrum sensing method for our project and detailed study of a technique called Average Periodogram Analysis to implement this method was done. We also simulated this technique in Matlab using various windowing methods and understand results.

7. An algorithm and a flow graph to make secondary subsystem cognitive was developed. First challenging step to this was to run OpenBTS and GNURadio together in the same computer with two USRP kits connected one for each. This required the two USRP kits to have different IP addresses.

8. The next step was to build a 2-frequency cognitive system with a pair of primary and secondary users communicating in parallel and primary pair having higher priority when ever both try to use same radio band. Detailed description is in the previous sections of this chapter.

9. This 2-frequency system was expanded to 4-frequency system with two primary pair of users and one secondary pair of users coexisting. This demon-

strated that both primary and secondary users can exist in the same GSM Network without affecting the existing system.

Chapter 9

Conclusion and future work

9.1 Conclusion

Cognitive radio is the solution to current day problem of inefficient utilization of the radio spectrum. It identifies the spectrum holes and enables secondary users to utilize these holes for communication thereby increasing total number of mobile users. We have demonstrated these cognitive radio capabilities using a 2-frequency and a 4-frequency cognitive radio test-bed and successfully testing them. We demonstrated that the secondary users quit the frequency channel which they are utilizing for communication as soon as the corresponding primary radio emerges thereby giving higher priority to the primary users.

9.2 Future work

We used energy based spectrum sensing technique for the detection of free channels to be utilized by secondary users. The algorithm we have designed has dependency on the distance between the base station and mobile station as the energy varies with distance. This dependency can be removed by designing a better algorithm in future. Also we have made secondary users to vacate the channel as soon as they corresponding primary radio appears causing the ongoing secondary call to drop. An algorithm that can avoid this call drop and handle this scenario in a better way can be designed in future.

Appendix A

Codes

A.1 Code for the 2-frequency system

A.1.1 freq2secondaryBTS.py

This code was written to demonstrate the 2-frequency system. This code was written by modifying the already available program named usrp_spectrum_sense.py' that comes together with the GNURadio software package. We set the default UHD device address to 192.168.20.2 because that is the IP address of the USRP device we are using as a spectrum sensor. The default samping rate was set to 1e6 i.e. 1MHz. The default FFT size is given as sampling rate /channel bandwidth. We wanted an FFT size of 1024 so we set the bandwidth to 976.56 Hz since 1 MHz / 976.56 Hz $\approx$ 1024.

The class 'my_top_block' was modified by replacing the lines:

```
self.channel_bandwidth = options.channel_bandwidth
self.min_freq = eng_notation.str_to_num(args[0])
self.max_freq = eng_notation.str_to_num(args[1])
if self.min_freq > self.max_freq:
    # swap them
    self.min_freq, self.max_freq = self.max_freq,
        self.min_freq
```

with the lines

```
self.channel_bandwidth = options.channel_bandwidth
self.down_freq = eng_notation.str_to_num(args[0])
self.up_freq = (self.down_freq) - 45e6
```

The method set_next_freq of the class my_top_block was modified by replacing

```
target_freq = self.next_freq
self.next_freq = self.next_freq + self.freq_step
if self.next_freq >= self.max_center_freq:
    self.next_freq = self.min_center_freq
```

with

```
target_freq = self.up_freq
```

In the code listing that follows we have listed only the functions that we customized and the ones that we added.

```
def main_loop(tb):
    startOpenBTS(tb.down_freq,tb)

def sub_loop(tb):
    print 'fft_size', tb.fft_size
    N = tb.fft_size
    mid = N // 2
    cusum = 0
    counter = 0

    while 1:

        # Get the next message sent from the C++ code (
            blocking call).
        # It contains the center frequency and the mag
            squared of the fft
        m = parse_msg(tb.msgq.delete_head())

        # m.center_freq is the center frequency at the
            time of capture
        # m.data are the mag_squared of the fft output
        # m.raw_data is a string that contains the binary
            floats.
        # You could write this as binary to a file.

        center_freq = m.center_freq
        bins = 102
        power_data = 0
```

```
        noise_floor_db = 0 ## 10*math.log10(min(m.data)/tb
            .usrp_rate)

        for i in range(1, bins+1):
            power_data += m.data[mid-i] + m.data[mid+i]
        power_data += m.data[mid]
        power_data /= ((2*bins) + 1)

        power_db = 10*math.log10(power_data/tb.usrp_rate)
            - noise_floor_db
        power_threshold = -59.0
        print datetime.now(), "center_freq", center_freq,
            "power_db", power_db

        cusum = max(0, cusum + power_db - power_threshold)
        if (cusum > 0):
            counter += 1
            if (counter > 2):
                print "CUSUM is now positive!!!"
                down_freq = center_freq + 45e6
                quitOpenBTS(down_freq, tb)
                break


def startOpenBTS(downFrequency,tb):
    arfcn=int((downFrequency-935e6)/2e5)
    if (arfcn < 0):
        print "ARFCN must be -> 0 !!!"
        sys.exit(1)
    print 'ARFCN=', arfcn
    #DB modifications
    t=(arfcn,)
    conn=sqlite3.connect("/etc/OpenBTS/OpenBTS.db")
    cursor=conn.cursor()
    cursor.execute("update config set valuestring=? where
        keystring='GSM.Radio.C0'",t)
    conn.commit()

    #start the OpenBTS
```

```
    f=subprocess.Popen(os.path.expanduser('~/ddpOpenBTS/
        runOpenBTS.sh'))
    f.wait()
    tb.msgq.delete_head()
    time.sleep(0.25)
    sub_loop(tb)


def quitOpenBTS(downFreq, tb):
    f=subprocess.Popen(os.path.expanduser('~/ddpOpenBTS/
        quitOpenBTS.sh'))
    f.wait()
    if downFreq <= 945e6:
        newDownFreq = downFreq + 10e6
    else:
        newDownFreq = downFreq - 10e6

    tb.up_freq = newDownFreq - 45e6
    print "new tb.up_freq: ", tb.up_freq
    startOpenBTS(newDownFreq, tb)
```

A.2 Code for the 4-frequency system

A.2.1 secondaryBTS.py

Most of the code is similar to freq2secondaryBTS.py. The only modified functions are listed below:

```
def main_loop(tb):
    startOpenBTS(tb.down_freq,tb)


def sub_loop(tb):

    print 'fft_size', tb.fft_size
    N = tb.fft_size
    mid = N // 2
```

```
cusum = 0
counter = 0


while 1:
    m = parse_msg(tb.msgq.delete_head())

    center_freq = m.center_freq
    bins = 102
    power_data = 0
    noise_floor_db = 0        ##  10*math.log10(min(m.
       data)/tb.usrp_rate)

    for i in range(1, bins+1):
        power_data += m.data[mid-i] + m.data[mid+i]
    power_data += m.data[mid]
    power_data /= ((2*bins) + 1)

    power_db = 10*math.log10(power_data/tb.usrp_rate)
       - noise_floor_db
    power_threshold = -70.0

    print datetime.now(), "center_freq", center_freq,
       "power_db", power_db

    #cusum cusum cusum is here
    cusum = max(0, cusum + power_db - power_threshold)
    if (cusum > 0):
        counter += 1
        if (counter > 2):
            print "CUSUM is now positive!!!"
            down_freq = center_freq + 45e6
            quitOpenBTS(down_freq, tb)
            break
    else:
        counter = 0
```

```
def startOpenBTS(downFrequency,tb):
    arfcn=int((downFrequency-935e6)/2e5)
    if (arfcn < 0):
        print "ARFCN must be > 0 !!!"
        sys.exit(1)
    print 'ARFCN=', arfcn
    #DB modifications
    t=(arfcn,)
    conn=sqlite3.connect("/etc/OpenBTS/OpenBTS.db")
    cursor=conn.cursor()
    cursor.execute("update config set valuestring=? where
        keystring='GSM.Radio.C0'",t)
    conn.commit()

    #start the OpenBTS
    f=subprocess.Popen(os.path.expanduser('~/ddpOpenBTS/
        runOpenBTS.sh'))
    f.wait()
    tb.msgq.delete_head()
    time.sleep(0.25)
    sub_loop(tb)


def quitOpenBTS(downFreq, tb):
    f=subprocess.Popen(os.path.expanduser('~/ddpOpenBTS/
        quitOpenBTS.sh'))
    f.wait()
    newDownFreq = getNewChannel(downFreq, tb)
    startOpenBTS(newDownFreq, tb)



def getNewChannel(downFreq, tb):
    newDownFreq = downFreq + 7e6
    if newDownFreq > 960e6:
        newDownFreq = 936e6

    tb.up_freq = newDownFreq - 45e6
```

```
print "new tb.up_freq: ", tb.up_freq
tb.msgq.delete_head()
time.sleep(0.25)

print 'fft size', tb.fft_size
N = tb.fft_size
mid = N // 2
cusum = 0
counter = 0
loopcounter = 0


while loopcounter < 10:
    m = parse_msg(tb.msgq.delete_head())

    center_freq = m.center_freq
    bins = 102
    power_data = 0

    for i in range(1, bins+1):
        power_data += m.data[mid-i] + m.data[mid+i]
    power_data += m.data[mid]
    power_data /= ((2*bins) + 1)

    power_db = 10*math.log10(power_data/tb.usrp_rate)
    power_threshold = -70.0

    print datetime.now(), "center_freq", center_freq,
       "power_db", power_db
    print "precheck"

    cusum = max(0, cusum + power_db - power_threshold)
    loopcounter += 1
    if (cusum > 0):
        counter += 1
        if (counter > 2):
            print "CUSUM is now positive!!!"
            newDownFreq = getNewChannel(newDownFreq,
               tb)
```

```
                break
        else:
            counter = 0
    return newDownFreq
```

A.3 primaryBTS.py

```
#!/usr/bin/env python
import sys
import sqlite3
import os
import re

def main_loop():
    usage = "usage: %prog channel_freq"
    if len(sys.argv) != 2:
        print 'usage:', sys.argv[0], 'channel_freq'
        sys.exit(1)

    center_freq = int(re.match(r'\d+', sys.argv[1]).group
        ())*1e6
    startOpenBTS(center_freq)

def startOpenBTS(frequency):

    arfcn=int((frequency-935e6)/2e5)
    print 'ARFCN=', arfcn

    #DB modifications
    t=(arfcn,)
    conn=sqlite3.connect("/etc/OpenBTS/OpenBTS.db")
    cursor=conn.cursor()
    cursor.execute("update config set valuestring=? where
        keystring='GSM.Radio.C0'",t)
    conn.commit()

    #start the OpenBTS
    f=os.popen('~/ddpOpenBTS/runOpenBTS.sh')
```

```
    f.close()


if __name__ == '__main__':
    try:
        main_loop()

    except KeyboardInterrupt:
        pass
```

A.4 runOpenBTS.sh

```
#!/bin/bash

sudo echo "Hi, this script starts OpenBTS in Ubuntu 12.04!
   "
sudo service asterisk restart
sudo gnome-terminal -x sh -c "sudo asterisk -r" &

cd ~/OpenBTS/openbts/trunk/apps/
sudo gnome-terminal --tab -e "sudo ../../../smqueue/trunk/
   smqueue/smqueue" \
    --tab -e "sudo ../../../subscriberRegistry/trunk/
       sipauthserve" &
sudo gnome-terminal --tab -e "sudo ./OpenBTS" \
    --tab -e "sudo ./OpenBTSCLI" &
cd ~
```

A.5 quitOpenBTS.sh

```
#!/bin/bash

sudo echo "Hi, this script turns OpenBTS off in Ubuntu
   12.04!"
sudo killall transceiver smqueue sipauthserve OpenBTSCLI
   asterisk
```

Appendix B

Installation procedures

To install either GNURadio or OpenBTS, you first need to have the UHD (driver software for the USRP) installed. The installation procedures given in this chapter are for the Ubuntu Desktop Operating System (version 12.04 and greater) only. For other operating systems, please check the internet.

B.1 UHD

```
# Install the runtime dependencies:

sudo apt-get install python libboost-all-dev libusb-1.0-0-
    dev python-cheetah \
doxygen python-docutils git cmake

# Go to your home folder and git clone the UHD repository:

cd ~
git clone https://github.com/EttusResearch/uhd.git

# Generate Makefiles with CMake:

cd uhd/host
mkdir build
cd build
cmake ../
```

```
# Build and install:

make
make test
sudo make install
sudo ldconfig
```

B.2 OpenBTS

```
cd ~
sudo apt-get install subversion
mkdir OpenBTS
svn co http://wush.net/svn/range/software/public OpenBTS/

sudo apt-get install autoconf libtool libosip2-dev libortp
   -dev \
libusb-1.0-0-dev g++ sqlite3 libsqlite3-dev erlang
   libreadline6-dev \
libncurses5-dev asterisk

cd OpenBTS
cd a53/trunk
sudo make install


## for USRP N210 only, for other devices please check the
   internet <
cd openbts/trunk
autoreconf -i
./configure --with-uhd
make

#(from OpenBTS root)
cd apps
ln -s ../Transceiver52M/transceiver .

## for USRP N210 only, for other devices please check the
   internet >
```

```
sudo mkdir /etc/OpenBTS
sudo sqlite3 -init ./apps/OpenBTS.example.sql /etc/OpenBTS
   /OpenBTS.db ".quit"
sudo sqlite3 /etc/OpenBTS/OpenBTS.db .dump

sudo mkdir -p /var/lib/asterisk/sqlite3dir

cd ../..
cd subscriberRegistry/trunk
make

sudo sqlite3 -init subscriberRegistry.example.sql \
/etc/OpenBTS/sipauthserve.db ".quit"


cd ../..
cd smqueue/trunk
autoreconf -i
./configure
make

sudo sqlite3 -init smqueue/smqueue.example.sql /etc/
   OpenBTS/smqueue.db ".quit"
```

B.3 GNURadio

```
## for Ubuntu 12.04 only, for other versions
## of Ubuntu please check the internet <

sudo apt-get install libfontconfig1-dev libxrender-dev \
libpulse-dev swig g++ automake autoconf libtool python-dev
    \
libfftw3-dev libcppunit-dev libboost1.48-all-dev libusb-
   dev \
libusb-1.0-0-dev fort77 libsdl1.2-dev python-wxgtk2.8 git-
   core \
libqt4-dev python-numpy ccache python-opengl libgsl0-dev
   python-cheetah \
```

```
python-lxml doxygen qt4-dev-tools libusb-1.0-0-dev libqwt5
   -qt4-dev \
libqwtplot3d-qt4-dev pyqt4-dev-tools python-qwt5-qt4 cmake
    git-core wget \
libxi-dev python-docutils gtk2-engines-pixbuf r-base-dev
   python-tk \
liborc-0.4-0 liborc-0.4-dev libasound2-dev python-gtk2

## for Ubuntu 12.04 only, for other versions
## of Ubuntu please check the internet >
cd ~
git clone http://git.gnuradio.org/git/gnuradio.git
cd gnuradio
mkdir build
cd build
cmake ../
make && make test
sudo make install
sudo ldconfig
```

Bibliography

[1] Federal Communications Commission. Spectrum policy task force. *ET Docket No. 02-135*, November 2002.

[2] Gregory Staple and Kevin Werbach. The end of spectrum scarcity. *IEEE Spectrum*, 41(3):48–52, March 2004.

[3] Paul Kolodzy et al. Next generation communications: Kickoff meeting. In *Proc. DARPA*, October 2001.

[4] Kranthi Ananthula. Experimental setup of cognitive radio test-bed using software defined radio. Master's thesis, Department of Electrical Engineering, 2013.

[5] Simon Haykin. Cognitive radio: Brain-empowered wireless communications. *IEEE Journal on selected areas in communications*, 23(2), 2005.

[6] Joseph Mitola et al. Cognitive radio: Making software radios more personal. *IEEE Personal Communications*, 6(4):13–18, August 1999.

[7] Joseph Mitola. *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*. PhD thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2000.

[8] `http://www.hill2dot0.com/wiki/index.php?title=Image:G2407_GSM-Architecture.jpg`. [Accessed on Oct 22, 2013].

[9] Andreas Miller. *DAB Software Receiver Implementation*. PhD thesis, ETH, 2008.

[10] `http://gnuradio.org/redmine/projects/gnuradio/wiki`.

[11] `https://wush.net/trac/rangepublic/attachment/wiki/WikiStart/OpenBTS-4.0-Manual.pdf`. [Accessed on May 27, 2014].

[12] D Cabric, A Tkachenko, and R W Brodersen. Experimental study of spectrum sensing based on energy detection and network cooperation. In *TAPAS*

'06 Proceedings of the first international workshop on Technology and policy for accessing spectrum, August 2006.

[13] M. A. Sarijari et al. Energy detection sensing based on gnuradio and usrp: An analysis study. *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on*, December 2009.

[14] Mansi Subhedar and Gajanan Birajdar. Spectrum sensing techniques in cognitive radio networks: A survey. *International Journal of Next-Generation Networks*, 3(2), June 2011.

[15] Mehmet C. Vuran Ian F. Akyildiz, Won-Yeol Lee and Shantidev Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50, 2006.

[16] Peter D. Welch. The use of fast fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms. *Audio and Electroacoustics, IEEE Transactions on*, 15(2):70–73, June 1967.