Department of Electrical Engineering

IIT Bombay

Master of Technology Project

Experimental implementation of a cognitive radio using OpenBTS , GNU Radio and spectrum sensing techniques

---

Author:
Abrar Ahmad

Supervisor:
Prof. S N Merchant

May 28, 2014

Abstract

Our goal is to set up a software defined cognitive radio using OpenBTS, GNU Radio and USRP kits. We decide on a frequency channel, to run our cognitive OpenBTS system in, beforehand. First we sense the presence of ongoing calls made by the primary users in the predefined frequency channel. The sensing is done by calculating the energy in that channel using a technique of energy detection called peroidogram analysis. If the energy is above some predefined threshold then there are ongoing calls in that channel and hence we wait for the calls to end. As soon as the calls involving the primary users end the energy in that channel goes low. GNU Radio detects this change and it provides the ARFCN, corresponding to this channel, to the secondary BTS system and the secondary BTS starts using this ARFCN allowing secondary users to make calls and send SMSs.

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[7]. 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.[4]

Diagram of spectrum here

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.5,2,6 kranti. It uses one of the spectrum sensing techniques to identify the spectrum holes in the radio spectrum.

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 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 two frequency band cognitive system is developed where secondary users migrate to frequency f2 if frequency f1 is occupied an viceverca.
2. A two frequency system is extended to a four 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

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 a 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

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 problems in cognitive radio is detection of primary users in the licensed spectrum and enable secondary users to quit the frequency band as quickly as possible if the corresponding primary radio emerges to avoid interference to primary users. 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. cyclo stationarity detection

2.1 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:

Block diagram for energy detection technique from stage one report here:

As described in the energy detection block diagram, it is basically a hypothesis testing problem with two possible hypothesis H0 and H1. Hypothesis H1 concludes the presence of primary users in the band of interest and hypothesis H0 concludes their absence. And energy detection technique is basically about distinguishing between these two hypothesizes.[3 from stage one report]

$$x(t) = n(t); \qquad H0$$
$$x(t) = hs(t) + n(t); \qquad H1$$

where 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 Y and bandwidth W and comparing this statistics to a predetermined threshold. Energy detection is implemented using average periodogram analysis which is covered in later part of this report.

2.2 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:

X is the unknown signal an H is the impulse response of matched filter which is matched to reference signal for maximizing SNR.

Block diagram of matched filter is given in fig:

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. [4] kranti thesis

2.3 Cyclostationarity detection

This technique utilizes periodicity property of the received signal to detect presence of primary users. Periodicity property is generally exhibited by the communication signals due to sinusoidal carriers, pulse train, hopping sequences etc. Due to this underlying periodicity most of the communication signals can be modeled as cyclostationary processes[1from folder project on desktop]. This technique detects a random primary signal with a particular modulation type in a background of noise and other modulated signals.

Cyclostationary feature detection is robust to noise and is a better performer than energy based detection in low SNR regions. This technique also requires a priori knowledge of the primary signal. Also this technique is computationally highly complex and the sensing time is also quiete long. Due the these reasons it is less common than energy based detection Block diagram of cyclostationary detection is given in the figure:[14 from kranti thesis]

Diagram

The detection is done by finding a unique cyclic frequency of the spectral correlation function of the received signal [4kranti]. The spectral correlation function is the Fourier transform of the cyclic autocorrelation function the spectral correlation function is defined as:

$$S(f, \alpha) = \tag{2.1}$$

Where the cyclic autocorrelation function is defined by:

Here x(t) is the signal received an ? is the cyclic frequency. The spectral correlation function is also termed as cyclic spectrum. This is a two dimensional transform unlike power spectral density which is 1 dimensional. For successful detection under cyclo-stationary based spectrum sensing, we need a priori knowledge of the cyclo-stationary features of the received signal only. However matched filtering is the optimal solution when we completely know about received signal in advance. This technique doesn't work well when the underlying noise is stationary. More over channel fading destroys the property of cyclo stationarty of the received signal and is also susceptible to sampling clock offset.

Comparision of various spectrum detection techniques

Diagram from kranti's thesis

The figure 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 [2 from karanti thesis].

2.4 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.

2.4.1 Average periodogram anaylsis

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.[8 from krantis report]

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;Xr[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,

Ir[k] = k = 0,1.N-1 where Vr[k] is a N point DFT and U is normalization factor i.e. , Vr[k] = DFTW[n]*X[n] and U = (The PSD of X[n] sequence is then the time averaged periodogram estimate ,

I[k] =

2.5 Wide band spectrum analyzer

GNU radio packages provide a tool for wide band spectrum sensing called usrp_spectrum_sense.py. The program is provided in the appendix. 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 he 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 Fs to use N point complex FFT X(ω) 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 +Fs/2. The second half of the FFT (X[N/2] to X[N-1]) contains the negative baseband frequencies, i.e. from Fs/2 to centre frequency.

For our project purpose, we collected 1024 samples using a tuner centered at uplink frequency of our interest, say 900MHz. 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 10 MHz. The frequency resolution is therefore: 10 MHz / 1024 = 9.7656 MHz. 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 100MHz. Hence we chose sampling frequency to be 10 MHz which gives a decimation value of: 100 MHz / 10 MHz = 10.

Chapter 3

Implementation of cognitive radio using OpenBTS

In our project we are able to successfully demonstrate the coexistence of primary users and secondary users in the same frequency channel in the GSM band. In order to accomplish this, we have implemented a cognitive radio which detects the spectrum holes in the radio spectrum and enables secondary users to utilize these for communication. An experimental setup has been developed for this demonstration using OpenBTS and GNU radio software and USRP N210 as hardware.

Experimental setup diagram:

3.1 Description of setup

The figure above describes the experimental setup for a two-frequency system. The primary system has only one USRP as an RF front and it runs OpenBTS. The secondary system has two USRP kits connected to it and one of them runs OpenBTS and the other GNURadio. This secondary system has cognitive capabilities. To provide cognitive capabilities it was required that OpenBTS and GNU radio run together in the same system and talk to each other which was challenging. Secondary system continuously senses the frequency band of interest and does decision making 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. Also we made GNU radio and OpenBTS coordinate to behave in appropriate manner and take dynamic decisions as and when required to make over all system behave in a cognitive manner.

First a two-frequency cognitive system is developed. For this two GSM bands are used with centre frequency 945 MHz (F1) and 950 MHz (F2). Secondary users are made to occupy one of these two bands say F1. Then we make the primary users enter the same band. This

results in an increase in energy levels in this band which is sensed by the secondary system as it continuously scans this band. Immediately secondary users are shifted to other frequency band (F2) there by vacating F1 for primary users. Hence a two-frequency cognitive system demonstrating coexistence of a pair of primary and secondary users is accomplished.

The whole technique is described using a flow graph below:

Flow graph here :

Now this two frequency system is expanded to a four frequency system where we have F1 = 936 MHz, F2 = 943 MHz, F3 = 950 MHz, F4 = 957 MHz. The experimental setup is also expanded with two primary systems and one secondary system. Each primary system has an USRP kit running OpenBTS and the secondary system has two USRP kits connected to it, one for OpenBTS and the other one for GNURadio, as we had previously in the two-frequency system.

Figure for 4 frequency system here:

Here we make a pair of primary users occupy one of the four frequency channel say F2. We make secondary users use a frequency channel say F1. Now the other pair of primary users try to enter frequency F1 for communication. This is sensed by the secondary system and it tries to migrate secondary users to F2 which also happens to be occupied already. Our secondary system detects that F2 is occupied and therefore moves on to find a spectrum hole in the four-frequency spectrum. It finds that frequency F3 is unoccupied and thus allows secondary users to enter F3 and utilize it for communication. The difference between a four-frequency system and a two-frequency system is that the secondary system in a four-frequency system has to first check the presence of primary users before switching into a particular frequency channel. This was not the case in the two-frequency system. In the two-frequency system we assumed that the other band is always unoccupied at the time of switching as only a pair of primary users existed and thereby only a single band is always unoccupied.

The following flow graph describes the four frequency cognitive system:

Flow graph here

The spectrum sensing is done by energy detection technique and it was required that a proper threshold be set for decision making. A number of readings were taken to decide the noise level, energy level when only primary users were active and also energy levels when both primary users and secondary users were active 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 kit which is RF front for GNURadio. This distance dependency can be removed by setting the threshold quite lower than required so that even if the users move far away the decision making is not affected.

Bibliography

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