Department of Electrical Engineering

IIT Bombay

Dual Degree Project

Experimental implementation of a cognitive Base Transceiver Station using OpenBTS and spectrum sensing technique

Author:
Swrangsar Basumatary

Supervisor:
Prof. S N Merchant

May 24, 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 Background

The electromagnetic radio spectrum is a natural resource that remains underutilized [4]. It is licensed by governments for use by transmitters and receivers. With the explosive proliferation of cell phones and other wireless communication devices, we cannot afford to waste our spectral resources anymore.

In November 2002, the Spectrum Policy Task Force, a group under the Federal Communications Commission(FCC) in the United States, published a report 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 were to scan the radio spectrum even in metropolitan places where it's heavily used, we would find that [6]:

1. some frequency bands are unoccupied most of the time,
2. some are only partially occupied and
3. the rest are heavily used.

The underutilization of spectral resources leads us to think in terms of *spectrum holes*, which are defined as [3]:

> *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.*

The spectrum can be better utilized by enabling secondary users (users who are not licensed to use the services) to access spectrum holes unoccupied by primary users at the location and the time in question. *Cognitive Radio*, which includes software-defined radio, has been promoted as the means to make efficient use of the spectrum by exploiting the existence of spectrum holes [4][2][5].

1.2 Cognitive Radio

One of the definitions of Cognitive Radio is [4]:

> *Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind:*
>
> - *highly reliable communications whenever and wherever needed;*
> - *efficient utilization of the radio spectrum.*

Besides, a cognitive radio is also reconfigurable. This property of cognitive radio is provided by a platform known as *software-defined radio*. Software-defined Radio (SDR) is basically a combination of two key technologies: digital radio, and computer software.

1.3 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). Chapter 4 and 5 describe the literature survey done on the GNU Radio software package and OpenBTS software respectively. Chapter 6 covers a partial implementation of cognitive radio using GNU Radio and OpenBTS. It also describes the proposed future work along with a flowgraph describing the algorithm for the complete implementation of cognitive radio on the OpenBTS platform.

Chapter 2

GSM

2.1 Overview

GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile), is a very popular standard that describes protocols for second generation (2G) digital cellular networks used by mobile phones. GSM networks usually operate in the 900 MHz, 1800 MHz or 1900 MHz bands. It supports a full data rate of 9.6 kbits/sec or 14.4 kbits/sec using better codecs.

2.2 System Architecture

A GSM Public Land Mobile Network (PLMN) consists of at least one Service Area managed by a Mobile Switching Center (MSC) connected to the Public Switched Telephone Network (PSTN).

The network structure can be divided into the following discrete sections:

- Base Station Subsystem
- Network and Switching Subsystem
- Operation Subsystem

2.2.1 Base Station Subsystem (BSS)

A base station subsystem consists of

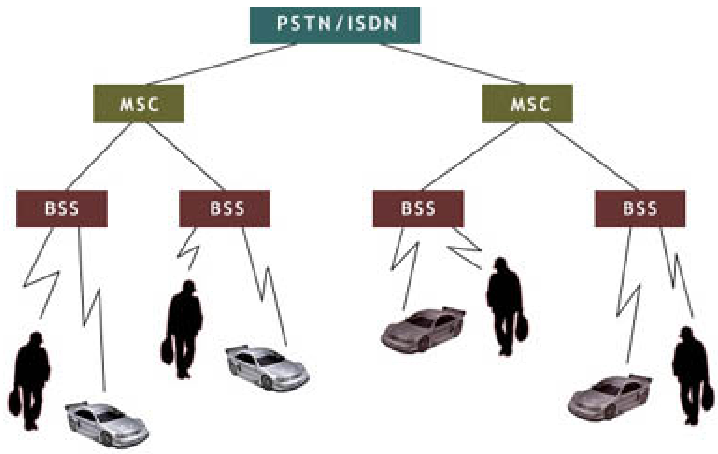

Figure 2.1: The architecture of a GSM Public Land Mobile Network (PLMN). *Source:* *http://wireless.arcada.fi/MOBWI/material/CN_1_2.html*

- a Base Station Controller (BSC) and
- at least one Base Transceiver Station (BTS) for Mobile Stations (MS). A mobile station can be a cell phone, or any electronic equipment such as a Personal Digital Assistant (PDA) with a phone interface.

The area served by a single BTS is considered a Network Cell. One or more BTSs are managed by a single BSC. A group of BSSs can be managed as a Location Area (Location Area) provided all those BSSs are being managed by the same MSC.

An MSC may also be connected via a Gateway MSC (GMSC) to other MSCs or the Public Switched Telephone Network (PSTN) with the Integrated Services Digital Network (ISDN) option. The Inter-Working Function (IWF) of a GMSC makes it possible to connect the circuit switched data paths of a GSM network with the PSTN/ISDN.

2.2.2 Network and Switching Subsystem (NSS)

The NSS is made up of an MSC and a Visitor Location Register (VLR). An MSC

- sets up, controls and shuts down connections
- handles call charges
- manages additionals services like call forwarding, call blocking, etc.

A VLR contains all the subscriber data of the phones being served by the accompanying MSC. It contains their location data too. The VLR also maintains data about the SIMs that do not belong to the network but have roamed into the network. The area served by an MSC is called a MSC/VLR service area.

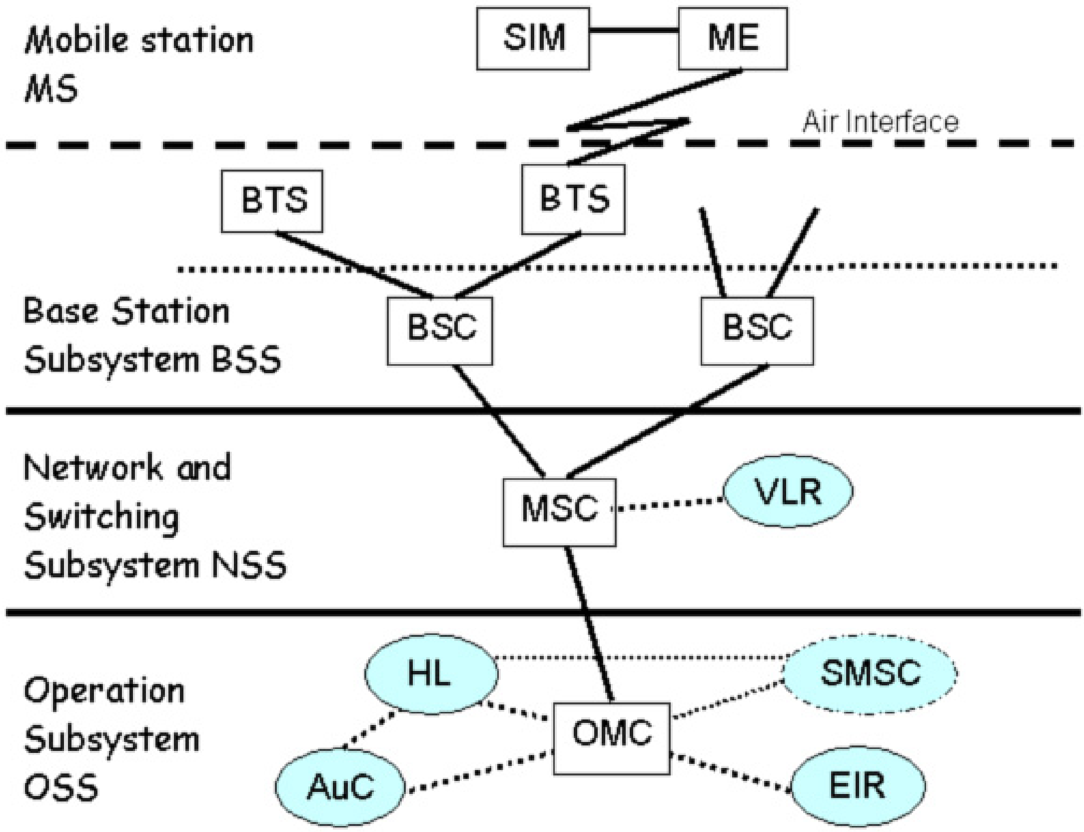

Figure 2.2: The GSM network architecture for a single MSC controlled Service Area. *Source:* *http://wireless.arcada.fi/MOBWI/material/CN_1_2.html*

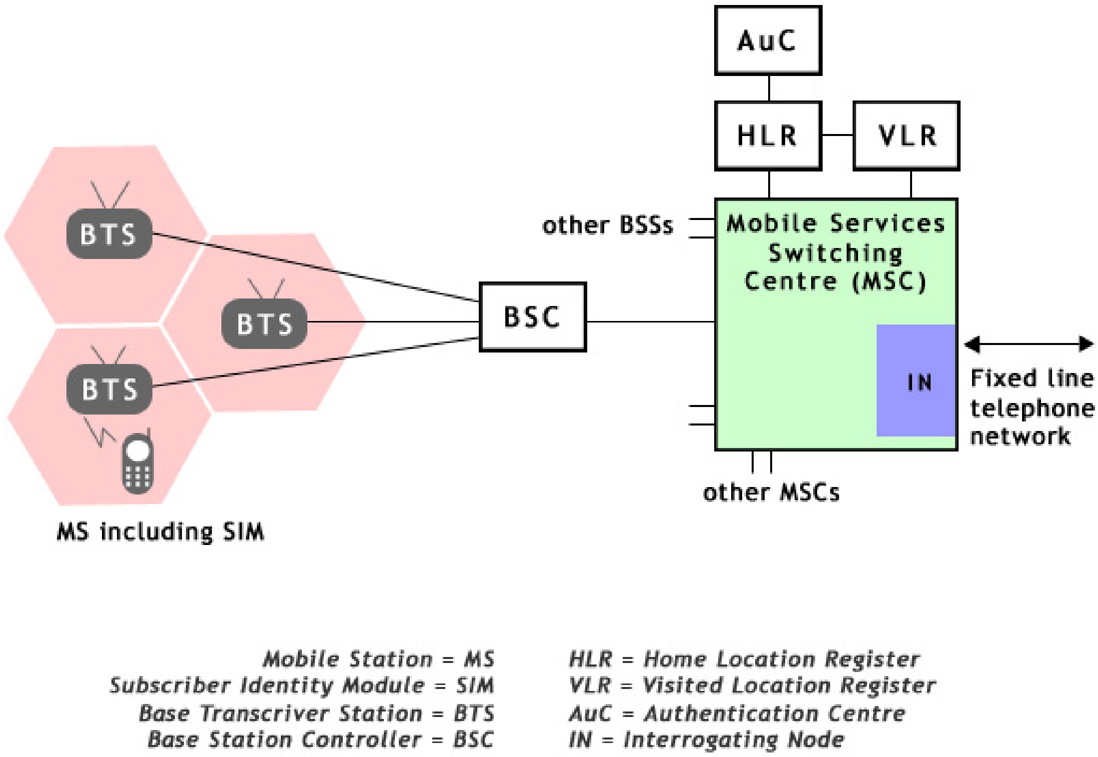

Figure 2.3: GSM network components. *Source:* *http://wireless.arcada.fi/MOBWI/material/CN_1_2.html*

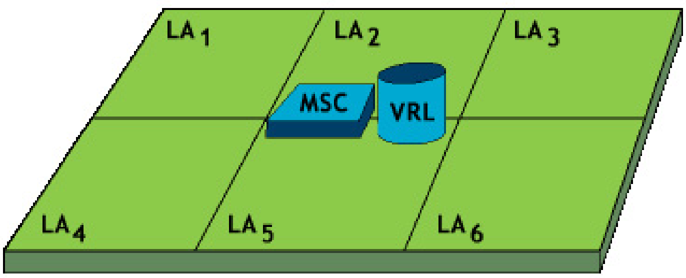

Figure 2.4: MSC/VLR Service Area. *Source:* *http://wireless.arcada.fi/MOBWI/material/CN_1_2.html*

2.2.3 The Operation Subsystem (OSS)

The OSS consists of :

- the Operation and Maintenance Center (OMC)
- the Authentication Center (AuC)
- the Home Location Register (HLR)
- the Equipment Identity Register (EIR)

The OSS is responsible for

- network management functions like service provisioning, network configuration, fault management, etc.
- billing calls
- administering subscribers

The AuC controls all the encryption algorithms used for verifying the SIMs. The EIR contains the serial numbers of all the MSs (mobile phones) being served. The HLR contains the subscriber data and location data of all the SIMs in different parts of the network.

2.2.4 GSM Network Areas

The area covered by a GSM operator is called a PLMN Service Area. A PLMN service area is made up of several MSC/VLR service areas. The hierarchy of service areas is as follows:

- PLMN service area,
- MSC/VLR service area,
- Location Area and
- Network Cell

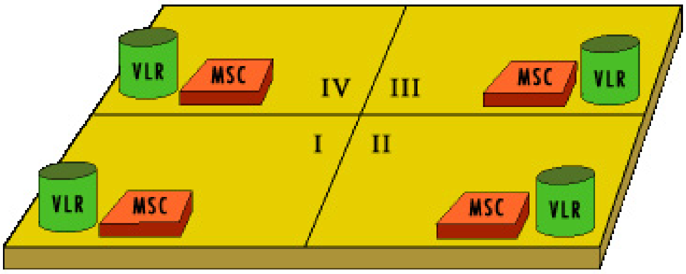

Figure 2.5: A PLMN Service Area for a GSM operator. *Source:* `http://wireless.arcada.fi/MOBWI/material/CN_1_2.html`

2.3 Protocol Architecture

The data communication protocols in a GSM network are implemented to work over the bearer[1] data channel. The GSM protocol architecture is structured into three independent planes:

- user plane
- control plane
- management plane

The user plane defines protocols for handling the voice and user data. At the Um interface, the traffic control channel (TCH) is used to carry the user data.

The control plane defines protocols for controlling connections by using signalling data. The signalling data are carried over logical channels called Dm-channels (wireless analog of the D-channels for wired interface). The spare capacities of the Dm-channels are used for carrying user data. Eventually all logical channels have to multiplexed onto the physical channel.

The management plane takes care of the coordination between different planes. It also manages functions related to the control and/or user planes. The management plane handles things like network configuration, network fault, etc.

[1] A bearer data channel is a channel that carries call content i.e. one that does not carry signaling.

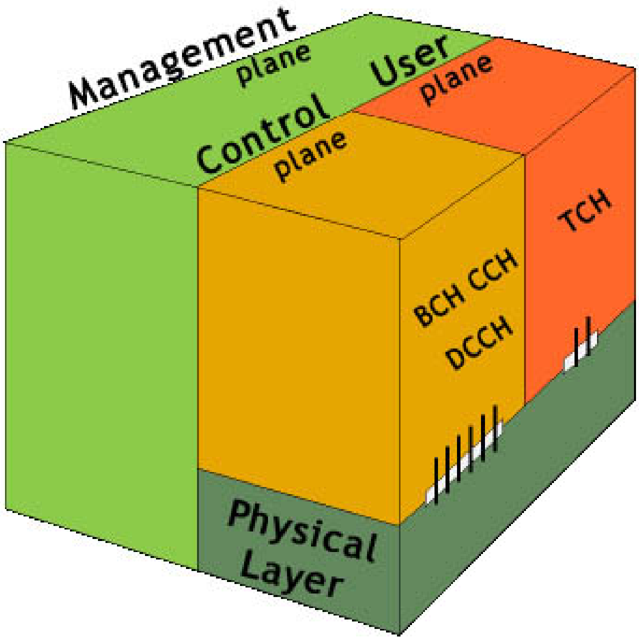

Figure 2.6: GSM protocol architecture planes. *Source:* *http://wireless.arcada.fi/MOBWI/material/CN_1_3.html*

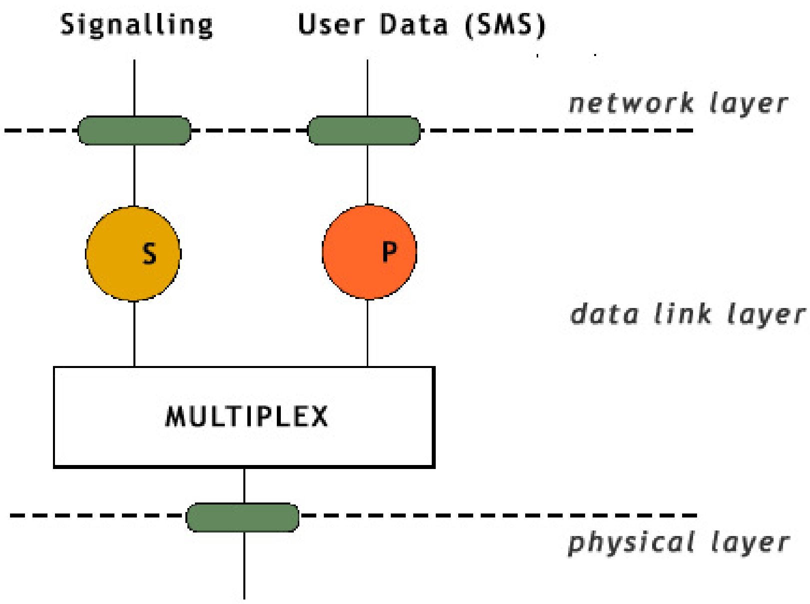

Figure 2.7: Logical channels for user plane data and control plane signalling. *Source:* *http://wireless.arcada.fi/MOBWI/material/CN_1_3.html*

2.3.1 Signalling Transmission

In GSM, the network nodes exchange signaling information with each other to establish, control and terminate connections. The various interfaces in a GSM network are:

- MS-BTS: Um
- BTS-BSC: Abis
- BSC-MSC: A
- MSC-VLR: B
- MSC-HLR: C
- VLR-HLR: D
- MSC-MSC: E
- MSC-EIR: F
- VLR-VLR: G

The Um interface is the only interface that uses the wireless physical medium for carrying signals. The rest of the interfaces all use wired and digital mediums.

DATA LINK LAYER (LAYER 2) PROTOCOLS

Link Access Protocol, Dm-channel (LAPDm) is a layer 2 protocol that provides safe, reliable connections to layer 3 protocols. It is a wireless-adapted version of the standard Link Access Protocol, D-channel (LAPD) of ISDN. It works in two modes: Unacknowledged and Acknowledged. In Unacknowledged mode it operates without acknowledgement, without error correction and without flow control. While in acknowledged mode, it asserts acknowledgement, error correction is done by resending and flow is controlled.

Message Transfer Part (MTP) is the standard ISDN message transport part of Signaling System 7 (SS7). The networking layers covered by MTP cannot be mapped one-to-one to the OSI model[2]. But it covers layer 1, layer 2 and parts of layer 3 from the OSI model. The parts of layer 3 not covered by MTP are covered by Signalling Connection Control Part (SCCP).

[2] Operation Systems Interconnection model

Bibliography

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

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

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

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

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

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