

# Experimental implementation of a cognitive Base Transceiver Station in GSM band using OpenBTS and spectrum sensing techniques

M. Tech. Dissertation

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

by

Swrangsar Basumatary

09d07040

Supervisor

Prof. S N Merchant



Department of Electrical Engineering  
**IIT Bombay**

May 29, 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 periodogram 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

<b>1</b>	<b>GSM</b>	<b>1</b>
1.1	Overview . . . . .	1
1.2	System Architecture . . . . .	1
1.2.1	Base Station Subsystem (BSS) . . . . .	2
1.2.2	Network and Switching Subsystem (NSS) . . . . .	3
1.2.3	The Operation Subsystem (OSS) . . . . .	3
1.3	Protocol Architecture . . . . .	4
1.3.1	Signalling Transmission . . . . .	5
<b>2</b>	<b>OpenBTS</b>	<b>9</b>
2.1	The OpenBTS Application Suite . . . . .	9
2.2	Key applications . . . . .	10
2.2.1	OpenBTS . . . . .	10
2.2.2	Transceiver . . . . .	10
2.2.3	SMQueue . . . . .	10
2.2.4	SIP router/PBX . . . . .	11
2.2.5	SIPAuthServe . . . . .	11
2.3	Network organization . . . . .	11
<b>3</b>	<b>Implementation of a cognitive Base Transceiver Station in GSM band using OpenBTS and spectrum sensing techniques</b>	<b>15</b>
3.1	The two-frequency system . . . . .	15
3.1.1	Experimental setup . . . . .	15
3.1.2	Testing . . . . .	16



# List of Figures

1.1	GSM PLMN architecture . . . . .	2
1.2	Network architecture for a single MSC Service Area . . . . .	2
1.3	GSM network components . . . . .	3
2.1	Simplest OpenBTS network . . . . .	12
2.2	OpenBTS network with two access points . . . . .	13





# Chapter 1

## GSM

### 1.1 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.

### 1.2 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

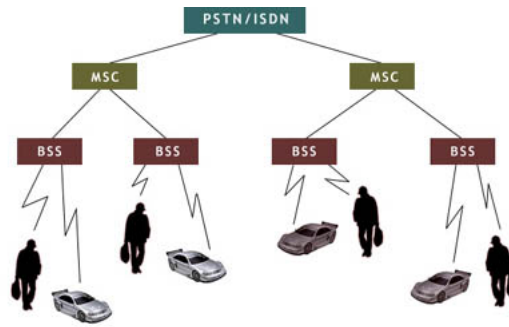


Figure 1.1: The architecture of a GSM Public Land Mobile Network (PLMN).  
Source: [http://wireless.arcada.fi/MOBWI/material/CN\\_1\\_2.html](http://wireless.arcada.fi/MOBWI/material/CN_1_2.html)

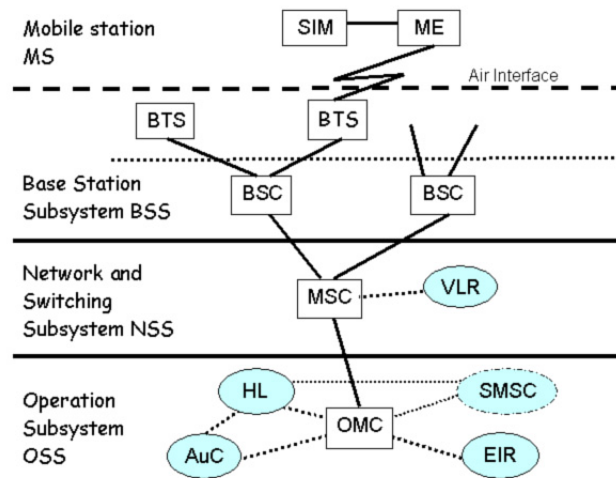


Figure 1.2: The GSM network architecture for a single MSC controlled Service Area.  
Source: [http://wireless.arcada.fi/MOBWI/material/CN\\_1\\_2.html](http://wireless.arcada.fi/MOBWI/material/CN_1_2.html)

## 1.2.1 Base Station Subsystem (BSS)

A base station subsystem consists of

- 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.

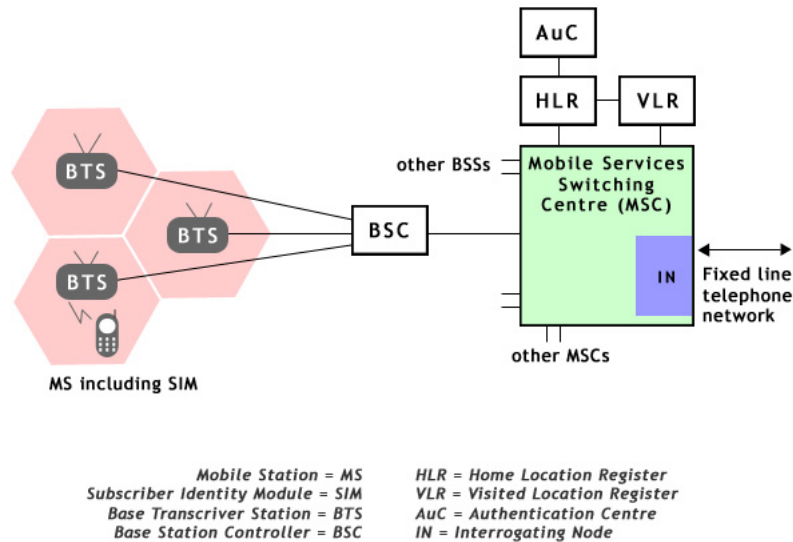


Figure 1.3: GSM network components.

Source: [http://wireless.arcada.fi/MOBWI/material/CN\\_1\\_2.html](http://wireless.arcada.fi/MOBWI/material/CN_1_2.html)

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.

### 1.2.2 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 additional 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.

### 1.2.3 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.

## 1.3 Protocol Architecture

The data communication protocols in a GSM network are implemented to work over the bearer<sup>1</sup> 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.

---

<sup>1</sup>A bearer data channel is a channel that carries call content i.e. one that does not carry signaling.

### 1.3.1 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 on 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 on 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<sup>2</sup>. 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).

---

<sup>2</sup>Operation Systems Interconnection model

## NETWORK LAYER (LAYER 3) PROTOCOLS

**Radio Resource Management (RR)** is a protocol that sets up, manages and terminates radio link channels. It is involved in measuring radio field strength, signal quality etc. It manages handover, modulation scheme, co-channel interference, etc. The goal is to utilize the limited spectral resources efficiently.

**Mobility Management (MM)** manages mobility of the mobile stations (MS). This protocol is used by the MS to communicate directly with the MSC bypassing the BSS. It works over an already established RR connection. It handles stuff like TMSI reallocation, authentication, IMSI attach/detach, roaming, location update procedure, etc.

**Call Management (CM)** protocol consists of the following parts:

- *Call Control (CC)* sets up, manages and ends calls. For each call a CC instance is created in the MS and another one in the MSC. CC instances communicate over already established MM and RR connections.
- *Short Message Service (SMS)* works over already established MM, RR and LAPDm connections.
- *Supplementary Services (SS)* provide upper layers the access to GSM supplementary services like call forwarding, call barring, etc.

**Signal Connection Control Part (SCCP)** is a SS7 protocol that provides routing, flow control, connection-orientation, error correction facilities etc. It works at the A-interface.

**Base Station System Application Part (BSSAP)** is a signaling protocol at the A interface supported by MTP and SCCP.

- *Direct Transfer Application Part (DTAP)* handles signaling between the MS and the MSC.
- *Base Station System Management Application Part (BSSMAP)* transfers management information from the BSC to the MSC.
- *Base Station System Operation and Management Application Part (BSSOMAP)* transports network management information from OMC to BSC.

**Mobile Application Part (MAP)** is an SS7 application-layer protocol for the various nodes in a GSM network. It provides facilities such as:

- roaming support via location update, IMSI attach/detach, authentication
- call handling

- subscriber tracing
- SMS
- supplementary services





# Chapter 2

## 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. 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 a much lower cost than existing technologies in many applications, especially rural cellular deployments and private cellular networks in remote areas.

### 2.1 The OpenBTS Application Suite

A complete OpenBTS installation consists of many 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.
- **SMQueue** – A store-and-forward server for text messaging.
- **Asterisk** – A VoIP PBX or “softswitch”.
- **SIPAuthServe** – An application managing the database of subscriber information.
- **Other Services** – Optional services supported through external servers, interfaced to OpenBTS through various protocols.

## 2.2 Key applications

### 2.2.1 OpenBTS

The OpenBTS application contains:

- L1 TDM functions (GSM 05.02)
- L1 FEC functions (GSM 05.03)
- L1 closed loop power and timing controls (GSM 05.08 and 05.10)
- L2 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 not to implement any function above L3 or L4, 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.

### 2.2.2 Transceiver

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

### 2.2.3 SMQueue

SMQueue is an RFC-3428 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.

## 2.2.4 SIP router/PBX

OpenBTS uses a SIP router or PBX to perform the call control functions that are normally performed by the MSC in a conventional GSM network, although in most network configurations this switching function is distributed over multiple switches. These switches also provide transcoding services.

The SIP router used in OpenBTS is Asterisk by default. Though there are other PBXs available in the market like Yate, FreeSwitch, etc.

## 2.2.5 SIPAuthServe

An application that implements Subscriber Registry, the database of subscriber information that replaces both the Asterisk SIP registry and the GSM Home Location Register (HLR) found in a conventional GSM network.

## 2.3 Network organization

In the simplest network, with just a single access point, all the applications run on the same embedded computer as shown in figure 2.1.

In larger network, with more than one access points, one of them can behave as a master and provide servers to the rest of them. Figure 2.2 shows a network with two access points where a master access points is providing servers to the 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, so they 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.

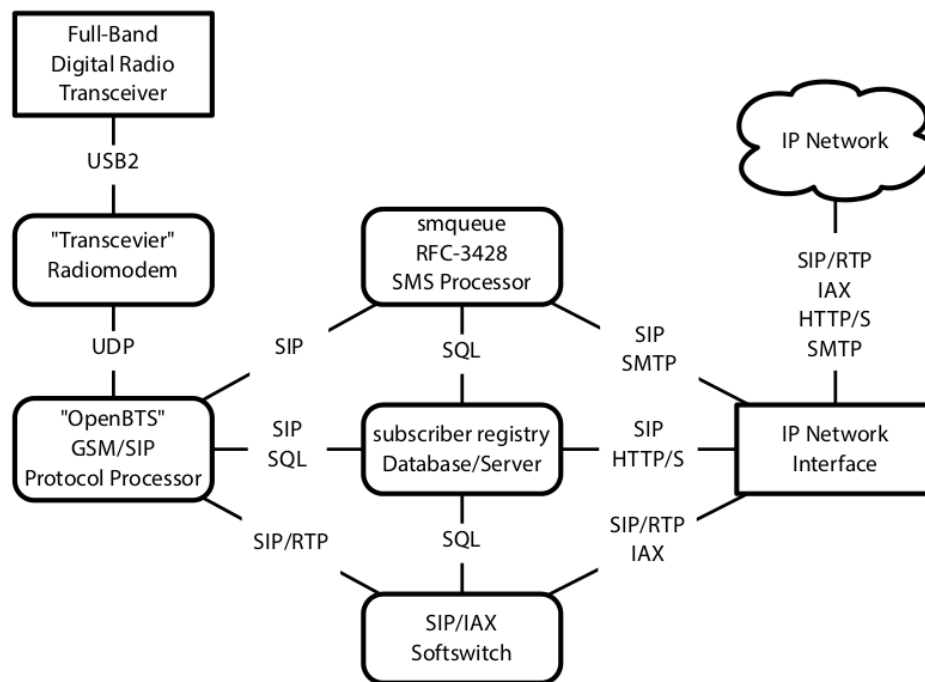


Figure 2.1: Components of the OpenBTS application suite and their communication channels as installed in each access point. Sharp-cornered boxes are hardware components. Round-cornered boxes are software components.

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

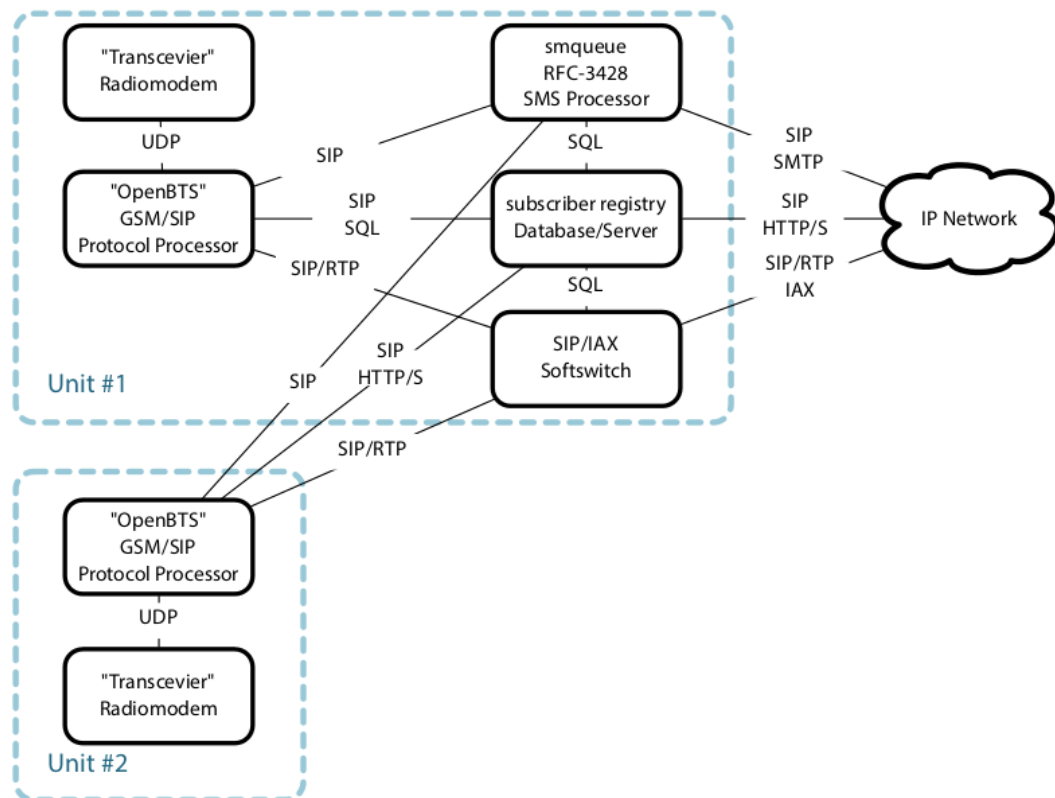


Figure 2.2: Two access points with unit #1 providing servers for both.

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



## Chapter 3

# Implementation of a cognitive Base Transceiver Station in GSM band using OpenBTS and spectrum sensing techniques

In this project we try to demonstrate a more efficient way of utilizing the spectral resources by having the secondary users make use of the spectrum holes. The spectrum holes are the frequency channels that have been licensed to the primary users but are not being used at that particular space and time. This allows secondary users to make use of already licensed frequency bands instead of having to allot them completely new frequency bands altogether.

In the first phase of the project, we implemented a two-frequency system where the secondary system had an option of switching into one of two frequency channels depending on which one was free. We expanded this to a four-frequency system with two primary systems in the second phase. The secondary would search for an unused frequency band among these four frequencies, two of which always remain used.

### 3.1 The two-frequency system

#### 3.1.1 Experimental setup

Experimental setup diagram:

The hardware and software components used in this experiment are the following

- **A primary BTS** – This is a Linux laptop running OpenBTS software with 1 USRP as the OpenBTS radio interface. The USRP hardware kit has a WBX 50-2200 MHz RX/TX daughterboard in it. Two mobile phones (primary users) are connected to the OpenBTS network running in this primary BTS system.
- **A secondary BTS** – This is an Ubuntu desktop running OpenBTS and GNURadio software. Two USRP kits are connected to this machine, one as the OpenBTS radio interface and the other as the GNURadio radio interface. The GNURadio software is used for the spectrum sensing. So, here the OpenBTS software with its radio interface acts as a Base Transceiver Station (BTS) while the GNURadio software alongwith its radio interface acts as a spectrum sensor. Each of the two USRP kits has a WBX 50-2200 MHz RX/TX daughterboard. Two other mobile phones (secondary users) are connected to the OpenBTS network running in this secondary BTS.

The secondary BTS system has cognitive capabilities. It was a challenge to make OpenBTS and GNURadio run simultaneously in the same computer and make them communicate with each other. GNURadio keeps sensing the spectrum used by the secondary users continuously in the background and takes decisions whether to switch the frequency band of the secondary BTS or not, depending upon the energy level in the frequency band in which it is running.

### 3.1.2 Testing

First we choose any two GSM frequency bands say 945 MHz ( $F_1$ ) and 950 MHz ( $F_2$ ). The primary users are made to occupy  $F_1$ . Then we let the secondary users come into  $F_1$ . This makes the energy level in  $F_1$  go high, which gets detected by the spectrum sensor of the secondary BTS. So, the secondary BTS moves out of  $F_1$  and switches its frequency to  $F_2$ . Similarly, now if the primary users are made to come into  $F_2$ , the secondary switches back to  $F_1$ .

In this experiment we don't have the situation where both  $F_1$  and  $F_2$  remain occupied because there is only one set of primary users. Therefore, the secondary also doesn't check the energy level in a channel before taking the decision to switch into that channel.



# Bibliography