LOCALIZATION OF GSM DEVICES IN INTENDED AREA

By

NC Naila Amir

NC Saba Manzoor

NC Muhammad Hadi Raza

Project Supervisor

Maj (R) Imtiaz Ahmed Kokhar

Submitted to the Faculty of Electrical Engineering, Military College of Signals
National University of Sciences and Technology, Rawalpindi in partial fulfilment for the requirements of a B.E. Degree in Telecom Engineering

JUNE 2014

ABSTRACT

Security is of paramount importance in this world of terrorism. Terrorism has become a major nuisance for all and sundry. Newer and better methods are being explored every day to combat terrorism. The use of remote GSM devices to detonate explosives has been on the rise reason being the sheer mobility and versatility of GSM devices. In order to combat this threat, a system has been designed specifically as a countermeasure to this menace. Jammers have been and are being used for security sensitive locations. But, the problem with a jammer is that it also disrupts the useful communication between people. The project caters for such security sensitive locations without the barring of any kind of communication.

A 3D model fed with sensors will be deployed which will detect and locate any GSM device that enters into our intended area. After which, the GSM device will be hooked onto a local front of its service provider, providing complete access to communication of any GSM device within the prescribed domain. Through such a network, any device that lies in a suspicious area can be promptly dealt with eliminating the possibility of the use of a GSM device to trigger an explosive.

DEDICATION

In the name of Allah, the Most Merciful, the Most Beneficent.

To our parents, without whose constant support and unstinting cooperation and assistance a work of this magnitude would not have been possible.

ACKNOWLEDGEMENTS

All praises for Allah Almighty who gave us the strength to accomplish this mighty task despite numerous difficulties and hardships on our way.

We offer our utmost gratitude to our Supervisor, Maj (R) Imtiaz Ahmed Kokhar for his constant guidance and encouragement. He gave us hope and boosted up our confidence during the tough phases of our project. The project wouldn't have been possible without his expert advice, unfailing patience and invaluable efforts.

We are also grateful to our parents and family for their admirable support and last but not the least, our auspicious university for making us what we are today.

Table of Contents

LIST OF FIGURES

CHAPTER NO. 02

CHAPTER NO.03

CHAPTER NO.04

CHAPTER NO. 05

LIST OF TABLES

Table No. **Page No.**

LIST OF ABBREVIATIONS

GSM	Global System for Mobile Communication
SIM	Subscriber Identity Module
MS	Mobile Station
IMSI	International Mobile Subscriber Identity
Kc	Session Key
ME	Mobile Equipment
BSC	Base Station Controller
MSC	Mobile Switching Centre
GMSC	Gateway Mobile Switching Centre
HLR	Home Location Register
VLR	Visitor Location Register
AuC	Authentication Centre
EIR	Equipment Identity Register
USB	Universal Serial Bus

IMEI	International Mobile Equipment Identity
PUK	Personal Unblocking Key
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
TMSI	Temporary International Mobile Subscriber Identity
3D	3 Dimensional
RCIED	Remote Controlled Improvised Explosive Devices
CCTV	Closed Circuit Television
USRP	Universal Software Radio Peripheral
PC	Personal Computer
API	Application Programmer's Interface
BTS	Base Transceiver Station
RSSI	Received Signal Strength Indicator
RF	Radio Frequency
DC	Direct Current
GPS	Global Positioning System
ADS	Advanced Design Systems

CHAPTER 01

INTRODUCTION

1.1 Overview

As the title suggests, our project covers the determination of location of GSM devices indoors not in 2D, as is done traditionally, but in 3D. In a 3D model of the intended area, the precise location of GSM devices will be displayed. Furthermore, as soon as a GSM device enters into our domain, it will be hooked onto our GSM front end which will enable us to hack into the services of the GSM devices giving us access to actions like eavesdropping.

The project provides a complete GSM security network for an indoor environment which is very beneficial for security sensitive areas. The project particularly targets the prevention of use of RCIEDs. To put the threat of RCIEDs into perspective, consider some of the incidents of use of RCIEDs and their devastation. [1]There have been 15,222 RCIEDs events in Afghanistan in 2012 alone. The first nine months of 2011 saw an average of 608 attacks per month in 99 countries. United States has spent roughly $17 billion on various anti-IED gear over the last decade.

1.2 Problem Statement

Terrorism has been on a rise ever since the fateful 9/11 incident. The use of remote GSM devices by terrorists to trigger IED (Improvised Explosive Device) and other such explosive contraptions has seen a sharp rise. So much so that this has become mainstream practice of terrorists for detonation of bombs throughout the worlds. The advantage of such an attack is obvious the bomb can be triggered from virtually any part of the world. This scenario presents a lot of security issues. Anyone can come and place GSM triggered bomb in

backpack and leave it there, without anyone getting suspicious and then detonating the explosive for maximum effect. To design a system that acts as a countermeasure to the use of GSM devices in detonation of explosives in security sensitive areas without the barring of essential services.

1.3 Approach

While outdoor localization is almost exclusively performed using the Global Positioning System (GPS), indoor location systems have successfully employed a variety of technologies. One such method to meet our objectives are:

Make a very precise and accurate 3D model of our domain (indoors) through the use of existing open source softwares.

Establish a sensor network that deploys sensors for accurate 3D triangulation to determine the location of any GSM device within our domain.

Integrate the data from the sensor network into our 3D model thus revealing the precise location of any GSM device.

Staging a local front for GSM devices to hook on to through the use of OpenBTS software and USRP device(s) for complete access of communication.

1.4 Objective

Provide a complete GSM monitoring system which will provide detection, precise location and access to any GSM device within intended area to stop potential threats. Immensely valuable for security as it eliminates the possibility of use of GSM devices for any unwanted activity within our domain.

1.5 Organization of Thesis

In chapter 2 “Literature Review”, the basic GSM architecture is explained. Furthermore it includes the explanation of softwares and algorithms been implemented for the accomplishment of desired objectives.

In chapter 3 “Design and Development”, detailed design and development of the project is explained systematically.

In chapter 4 “Analysis and Evaluation”, results acquired during the implementation of the project modules are displayed .It leads to the project conclusion.

In chapter 5 “Future work”, future recommendations of the project are described.

In chapter 6 “Conclusion”, compiled results achieved at the end of project are briefly described.

CHAPTER 02

LITERATURE REVIEW

2.1 Background

This chapter contains a brief history of evolution of GSM network. The chapter will include basic components of GSM milieu, basic security and authentication procedures. Aim of the project is to give an idea to readers about the protocols being used in GSM environment without going into the details of each protocol. The chapter beings with a small historical ground of GSM network. Later it provides information about the basic GSM components. Then in the later part. The complete authentication and security operations are covered and how they are implemented to provide standard security aspects. The main aspiration of the thesis is to pin point the location of malicious device and then performing man in the middle attack. This attack in fact exploits the weaknesses of GSM architecture which is utilized to implement man in the middle attack.

2.2 Evolution of GSM System

[2]Global system for mobile communication (GSM) is one of the most significant technological advancements of recent times. It is the most widely used cellular structure presently in the world. In this part, let's have a bird eye view over the evolution of the GSM system. In early 1970s, in New York City, bell mobile systems could only support a maximum number of 12 simultaneous calls over 1000 square miles. Its main problems were limited spectrum allocation and demand for mobile phone services were increasing. First Generation (1G) systems were emerged in the late 1970s and lasted through the 1980s. These analog systems were the first true mobile phone systems, known at first as 'cellular mobile radio telephone'. In 1982 in United States (U.S.), 1G cellular took off with the deployment of

Advanced Mobile Phone Service (AMPS). Total Access Communication System (TACS) was introduction in United Kingdom (U.K.) in 1985. It was the European version of AMPS More than 25 countries availed TACS services.

Nordic Mobile Telephone (NMT) system was developed in the late 1980s by the telecommunications administrations of Sweden, Norway, Finland, and Denmark to create a compatible mobile telephone system in the Nordic countries. Second Generation (2G) was designed in the 1980s, based on digital technology rather than analog. A negative upshot of these hi-tech advances was a competitive sprint to plan, design and put into operation digital systems leading to a diversity of different and incompatible standards, mainly Global system for Mobile communication (GSM), Interim Standars-54(IS-54) Interim Standard -136 (IS-136) , Extended TDMA (E-TDMA), Personal Digital Cellular (PDC), Interim Standard -95 CDMA (IS-95CDMA).

Development of Global System for Mobile Communication (GSM) started in 1082 and mobile services based on GSM technology were first launched in Finland in 1991. Today, more than 690 mobile networks provide GSM services across 213 countries and GSM represents 82.4% of all global mobile connections. There are now more than 2 billion GSM mobile users worldwide. GSM World references China as “the largest single GSM market, with more than 370 million users, followed by Russia with 145 million, India with 83 million and the USA with 78 million users”

Although GSM initially stood for ‘Groupe Special Mobile’, named after the study group that created it, the acronym was later changed to refer to ‘Global System for Mobile Communications’ (GSM).

2.3 GSM Architecture

A GSM network is a combination of multiple components and interfaces. It is a collection of transceivers, switches and routers. In this section, all essential and basic components are introduced which are part and parcel of a GSM infrastructure. GSM infrastructure can be divided into three main groups Mobile station (MS), Base-station subsystem (BSS) and Network and Switching Subsystem (NSS).

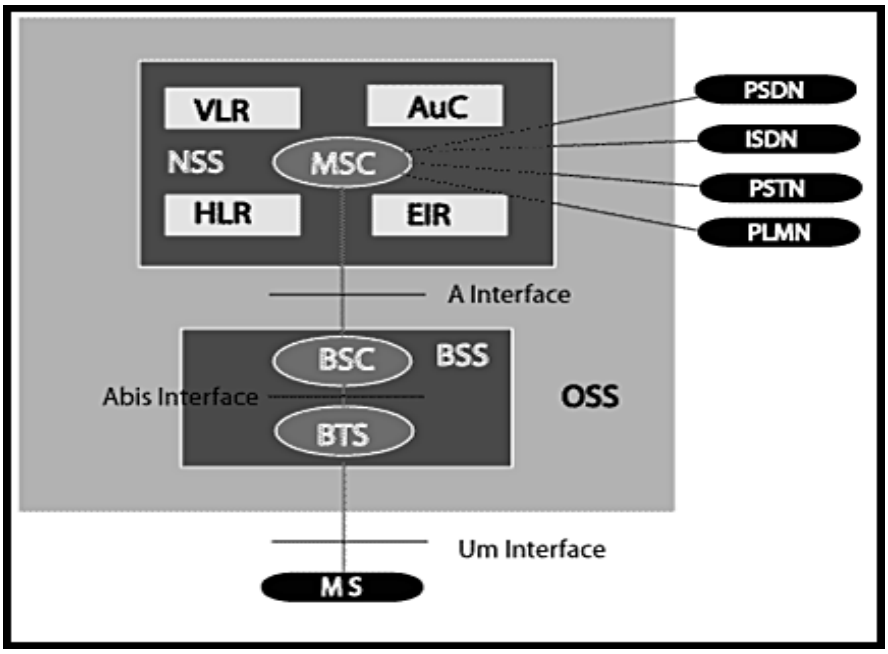


Figure 2. 1 GSM Architecture

2.4 Mobile Station (MS)

Mobile equipment (ME) and subscribers Identity Mobile (SIM) both combine to form Mobile station (MS). MS can be defined in terms of an equation

$$MS = ME + SIM$$

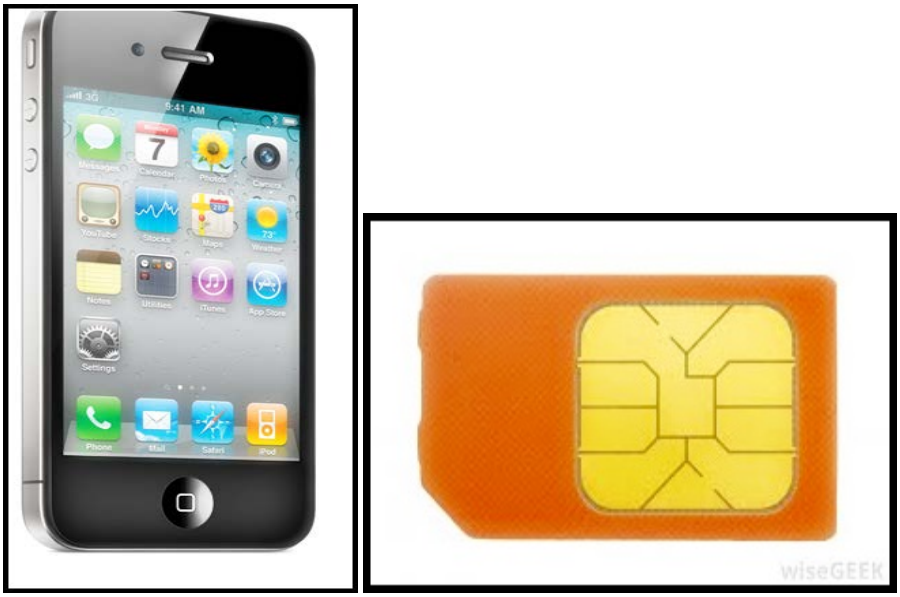


Figure 2. 2 GSM Mobile and SIM Card

2.5 Mobile Equipment (ME)

It is known as terminal equipment or commonly known as hand set. In fact ME is a physical phone itself. This is the hardware which actually communicates with GS, network. Its key essential elements are display, electronic circuit to transmit and receive signals, battery etc. Each ME has a unique number which is called as International Mobile Equipment Identity (IMEI). IMEI number is installed in the circuit board of the cell phone by the manufacturer company and a cell phone can be tracked by its IMEI number. ME are available in various styles and power classes.

2.6 Subscriber Identity Module (SIM)

Subscriber data is stocked up on a separate unit commonly known as SIM card. From the user's point of view, the SIM is indeed the best-known directory used in a GSM system. The SIM is a miniature memory gadget installed on a card and holds user-specific credentials.

Figure 2. 3 SIM

Here it is pertinent to mention that both SIM and ME combine together have almost same credentials and essentials as of a complete GSM network. GSM subscriber recognized by SIM instead of ME that is inserted into the cell phone before it can be used which in fact provides delicate mobility. The tools required for authentication and ciphering procedure are also stored din SIM.

Table No. 2.1 Data Hardcoded on SIM

PARAMETERS	REMARKS
SECURITY RELATED DATA	
Algorithm A3 and A8 (m/f)	Required for authentication and to determine Kc
Key Ki (m/f)	Individual values Known only on SIM and HLR
Key Kc (m/v)	Result of Ki, A8 and Rand
CKSN (m/v)	Ciphering key sequence number
Subscriber Data	
IMSI (m/f)	International Mobile Subscriber Identity
MSISDN (o/f)	Mobile Subscriber ISDN directory number of a subscriber
Access Control Class (m/f)	For control of network access
Roaming Data	
TMSI (m/v)	Temporary mobile subscriber identity
Value of T3212 (m/v)	For location updating
Location updating status	Is a location updating required?
LAI (m/v)	Location area information
Network color codes NCCs of restricted PLMNs (m/v)	Maximum of 4 PLMNs can entered on a SIM after successful location update Cause “PLMN not allowed.” Oldest entry is deleted when more than 4 restricted PLMNs are found
NCCs of preferred PLMNs(o/v)	What PLMN should the MS select, if there is more than one to choose from and the home PLMN is not available?
PLMN data	
NCC, mobile country codes (MCC) and mobile network codes of home PLMN (m/f)	Network Identifier
Absolute Radio frequency channel numbers (ARFCNs) of home PLMN (m/f)	Frequencies for which the home PLMN is licensed.

Legend m=mandatory; o=optional; f=fixed; v=changeable

Table No. 2.2 Administrative Data

PARAMETERS	REMARKS
Administrative Data	
PIN/PIN2(m/v)	Personal identification number, requested at every power up
PUK/PUK2 (m/f)	PIN unblocking key, required to unlock a SIM
SIM service table (m/f)	List if optional functionality of SIM
Last dialled number (o/v)	Redial
Charging meter (o/v)	Charges and time increments can be set
Language (m/v)	Determine the language for prompts by the mobile station

2.7 Base Station System (BSS)

The Base Station Subsystem is a subsystem of GSM network used for management and smooth running of the radio network, which is handled by Mobile Switching Center (MSC). Classically, several BSSs are manned by one MSC. One BSS itself may provide coverage to a significantly outsized area consisting of numerous cells. The BSS comprises the BSC itself and the connected BTSs. The BSS is subdivided into three major parts Base Station Controller (BSC) and Transcoding Rate and Adaptation Unit (TRAU).

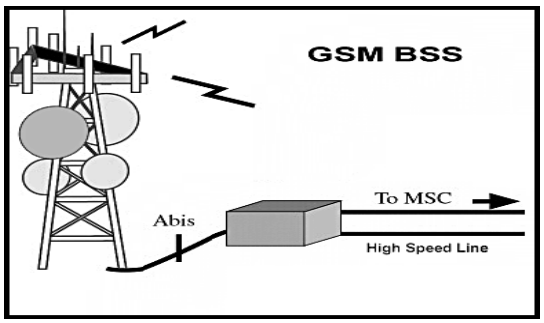


Figure 2. 4 Base Station System

2.8 Base Transceiver Station (BTS)

The BTS is the network element which allows MS to access the network. It manages the broadcasting interface to MS. The BTS is the broadcasting equipment that communicates to the transceivers where mast sections are used to feed every cell of the network. Broadcasting interface between the BTS and MS is recognized as the Um or Air Interface.

The BTS is the network element responsible for maintaining the air interface and minimizing the transmission problems (the air interface is very sensitive for disturbances). This task is accomplished with the help of some 120 parameters. These parameters define exactly what kind of BTS is in question and how MSs may see "see" the network when moving in this BTS area. The BTS parameters handle the following major items what kind of handovers (when and why), paging organization, radio power level control, and BTS identification.

A single BTS typically covers a 120 degree sector of a cell so a mobile phone tower with three BTSs will give coverage to the complete 360 degrees around the tower and entire area of a cell will be fed with communications. A cell can be further split up into one or more sectors which purely depend on number of users and topographical area. In case of superfluous sector coverage, a cell may be fed by a number of BTSs. A BTS is usually located in the middle of a cell. The size of a cell depends upon the transmitting power of BTS. Each BTS feeds a distinct one cell.

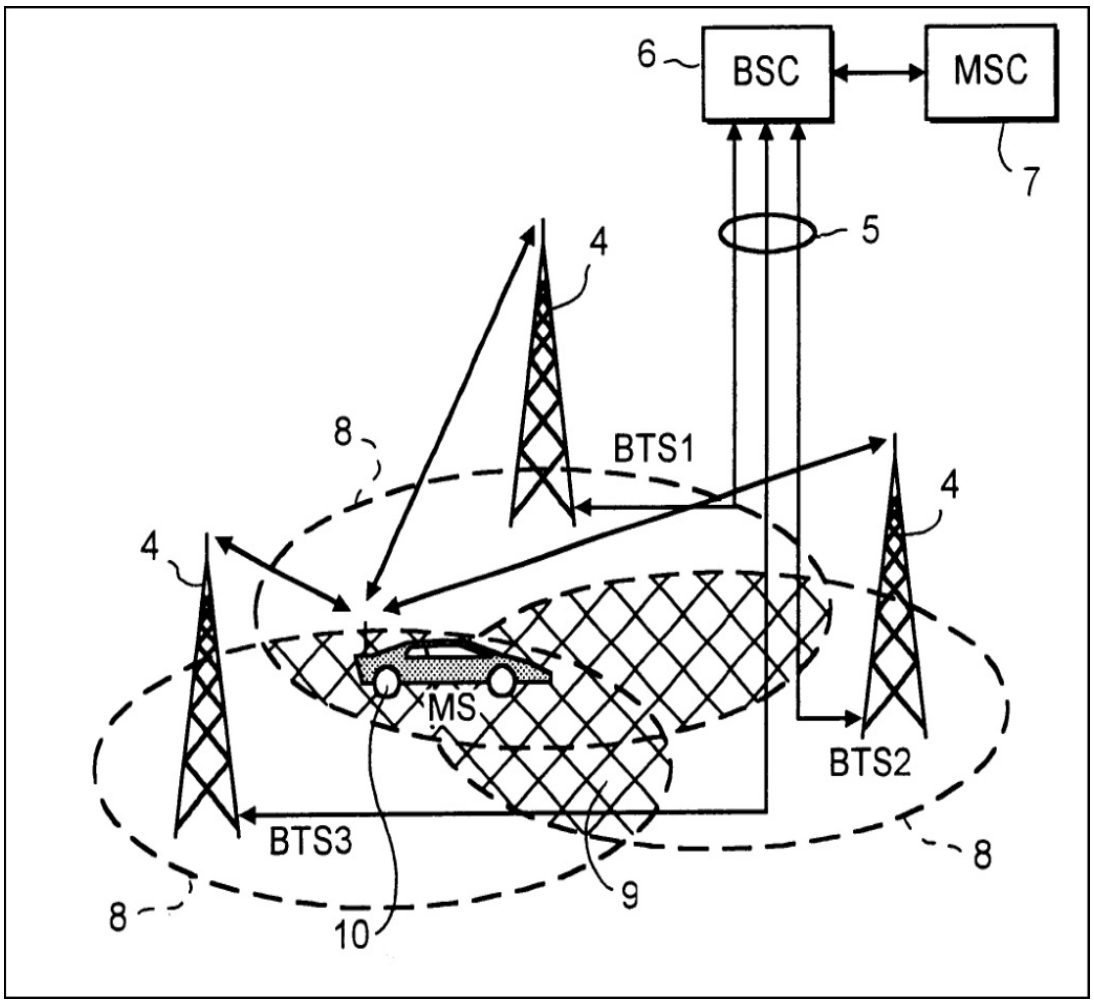


Figure 2. 5 Base Transceiver Station Sectorization

BTS functions can be defined as Encoding, encryption, multiplexing, modulation, and radio signal transmission, decoding, decryption, demultiplexing and demodulation of received radio signals, each BTS serves a single cell, support for full and half –rate speech codec, control of frequency hopping, random access detection, timing advance and uplink radio measurements.

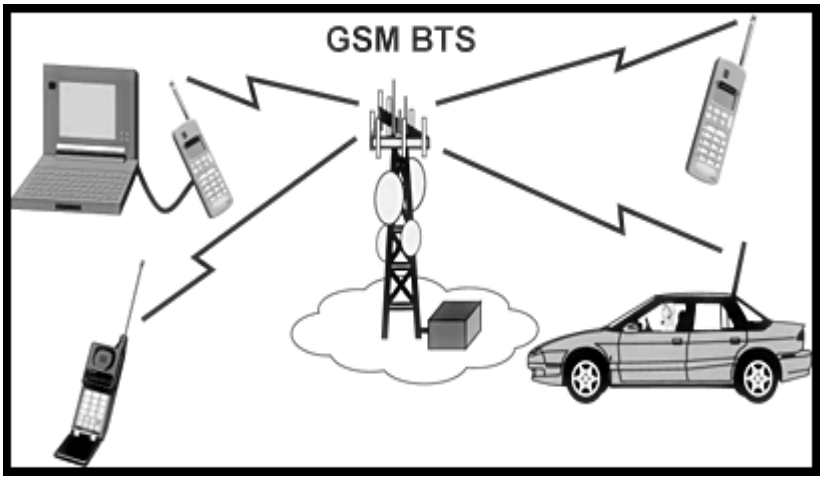


Figure 2. 6 BTS

2.9 Base Station Controller (BSC)

The BSC grants and manages the entire control functions and physical connection between the MSC and BTS. The BTS facilitates the GSM network with functions such as handover, cell configuration data and control of radio frequency (RF) power levels in BTSs. One or more BTSs are served by one BSC while numerous BSCs are managed by a single MSC. The interface used for communication between the BTSs and BSC is known as Abis Interface. Characteristically the BSC provide the brainpower to the BTSs and the most robust components of BSS.

BSC assigns and releases frequencies and time slots for the MS. The BSC also handles inter cell handover. It controls the power transmission of the BSS and MS in its area.

The function of the BSC is to allocate the necessary time slots between the BTS and the MSC. It is a switching device that handles the radio resources. Additional functions include control of frequency hopping, performing traffic concentration to reduce the number of lines from the MSC, providing an interface to the operations and maintenance synchronization, power management and time=delay measurements of received signals from the MS.

2.10 Transcoder and Rate Adaption Unit (TRAU)

TRAU is an important aspect of a mobile network which typically located between the BSC and the MSC. It compresses data over Air- interface to use the allocated bandwidth effectively and data compression is performed in both the MS and the TRAU. From the architecture perspective, the TRAU is part of the BSS and Graphical representation of the TRAU is a black box or, more symbolically, a clamp as it is used to compress or decompress speech between the MS and the TRAU.

The used method called regular pulse excitation-long term prediction (RPE-LTP). It compresses speech from 64 kbps to 16 kbps, in the case of a full rate channel and to 8 kbps in the case of a half rate channel, however in PSTN environment, the standard bit rate for speech is 64 kbits/s. TRAU is not used for data connections. Mostly the TRAU is installed at the site of the MSC to get the most benefit from the compression. When installed at the MSC side, a full rate speech channel uses only 16kbps over the link fron BSC to the MSC.

2.11 Network and Switching subsystem (NSS)

NSS plays a central part in every mobile network. It consists of a number of different essentials elements collectively known as core network of the GSM infrastructure. By using encryption, authentication and roaming various network elements of NSS perform functions of subscriber data handling, signaling, mobility management (MM), charging/billing, call control and set up call connections subsystems are interconnected directly or indirectly via SS7 network and NSS provides and manages all the interfaces among them, NSS has more flexible network topology than the hierarchical structure of the BSS.

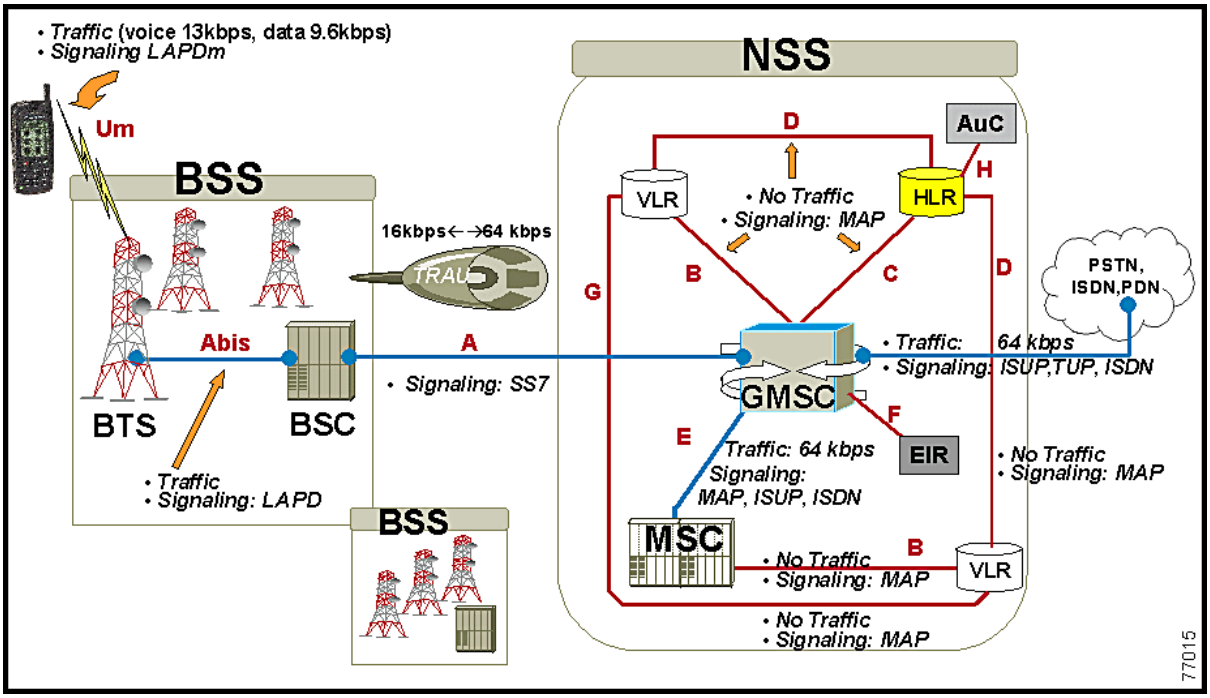


Figure 2. 7 Network Switching System

NSS is further sub divided into Mobile Switching center (MSC), gateway Mobile Switching (GMSC), Home location Register (HLR), Visitor location register (VLR, equipment identity register (EIR), authentication center (AuC), SMS gateway (SMS-G and chargeback center (CBC).

2.12 Mobile Switching Services Center (MSC)

Undoubtedly MSC is the brain of the GSM network so by the virtue of its tasking, it is the most important part of the GSM network. It handles a large number of BTSs, BSCs and even corresponds with different MSCs. Additional functions done by the MSC are call routing to a roaming subscriber, call setup, basic switching functions, handovers between BSCs and MSCs, registration, authentication and location updating.

It also provides an interface to the PSTN so that calls can be routed from the mobile network to a phone connected to a landline. Interfaces to other MSCs are provided to enable calls to

be made to mobiles on different networks. The interfaces between the BSC and the MSC is known as the “A interface”. The interface between two mobile switching centers (MSC) is called as the “E-interface”.

2.13 Gateway Mobile Switching Center (GMSC)

GMSC is just like a MSC which provides an interface to communication with other networks. Network operator may opt to equipment to facilitate all of their MSCs with gateway functionality. Any MSC not possessing gateway functionality routes calls to external networks via a gateway MSC. A mobile terminating call from PSTN enters PLMN via a gateway MSC which gathers required information from the HLR and then call is either re-routes by the GMSC to the specific MSC where the concerned cell phone user is positioned or call is transferred to the forward- to number with extension.

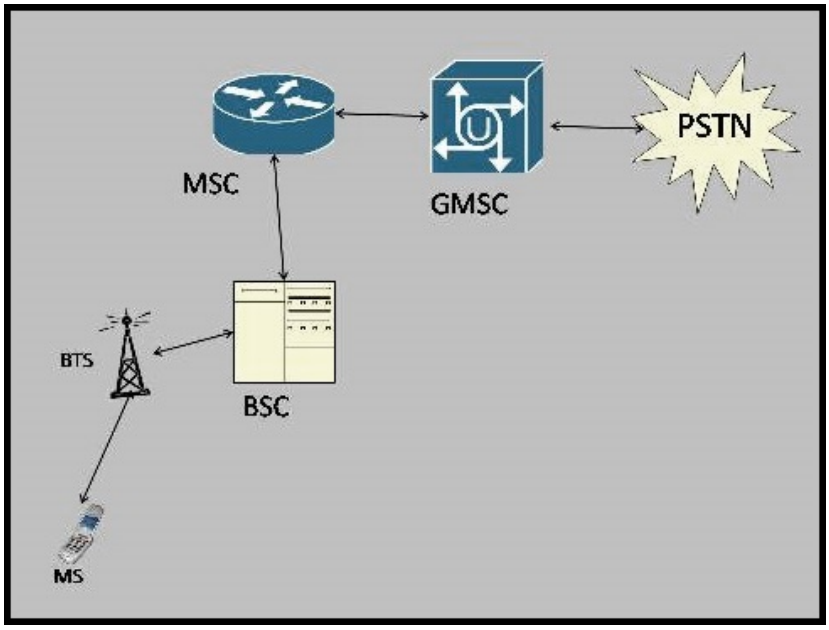


Figure 2. 8 MSC and GMSC

2.14 Home Location Register (HLR)

HLR is a data base containing all the details of the subscribers. Typically entire GSM network is handled by only a single HLR but keeping in view certain benefits more than one HLR are placed in the network. In the most of the GSM networks, both Equipment Identity Register (EIR) and Authentication Center (AuC) are part of HLR. HLR carries all the administrative information of every user listed in that specific network which includes phone numbers (Mobile subscriber Integrated Services Digital Network Number (MISISDN)), IMSIs, current locations of MSs, roaming data and Ki.

2.15 Visitor Location Register (VLR)

To trim down work load from HLR, the VLR was introduced. VLR is integrated with the MSC and it is a database that contains data about subscriber presently available in the area which are being served by the MSC/VLR. A VLR is a database just like a HLR, which momentarily holds data of the roaming consumers of the other mobile networks in the area served by the HLR. VLR data is based on the user information retrieved from HLR. MSC deals with roaming subscribers via VLR. Typically one VLR is dedicated for one MSC.

There is a VLR for every Location Area the Location Area(LA) is a set of data base stations that are grouped together to optimize the communication. The VLR reduces the overall number of queries to the HLR and thus reduces network traffic. The VLR is identified by LAC which is a sixteen digit number that identifies a particular LA within the GSM network.

2.16 Equipment identity Register (EIR)

EIR utilized for security purposes and it is help responsible for telling either IMEI number of the MS is valid or not. Each MS has a unique number and can be identified by that number which is known as International Mobile Equipment Identity (IMEI) number. The basic aim

behind EIR is to introduce a mechanism for MSs for identifying, tracking and to put them under surveillance.

EIR maintains of a database in the form of three lists “”white list” holds the record of all valid and security wise clear MSs. “black lists” holds the record of all the stolen, lost or tempered IMEI number MSs and “gray list” holds the record of all the MSs placed under observation. Now days, many GSM operators does not include EIR in their NSS because the prices os the cell phones have gone down drastically.

2.17 Authentication Center (AuC)

AuC is responsible for providing different security parameters such as Random Number (RAND), signed Response (SRES), session key (Kc) and Individual Subscriber Authentication Key (Ki), which enables the network to check SIM card is valid or not. The same security parameters are afterwards used in ciphering procedure.

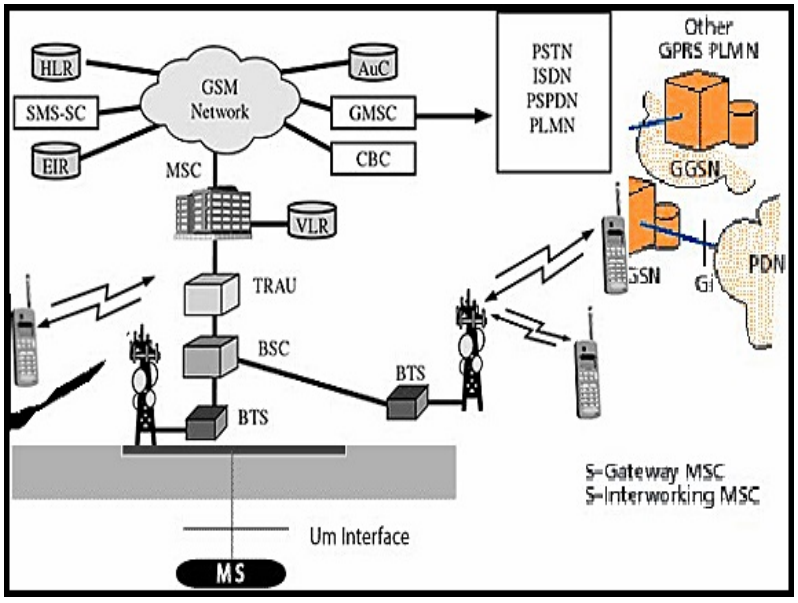


Figure 2. 9 GSM Database Registers

2.18 Softwares Implemented

2.18.1 OpenBTS

[3]OpenBTS is an open-source Unix application that uses a software defined radio (like USRP) to present GSM air interface to standard GSM handset and uses a software PBX (Asterisk) to connect calls. The combination of the ubiquitous GSM air interface with VoIP backhaul could form the basis of a new type of cellular network that could be deployed and operated at substantially lower cost than existing technologies in green fields in the developing world.

In plain language, we are working on a new kind of cellular network that can be installed and operated at about 1/10 cost of current technologies, but that will still be compatible with most of the handsets that are already in the market. This technology can also be used in private network applications (wireless PBX etc) at much lower cost and complexity than conventional GSM.

This figure gives an overview about the components used. The main hardware device is Ettus' Universal Software Radio Peripheral (USRP), connected via USB to a standard PC running the OpenBTS application and Asterisk.

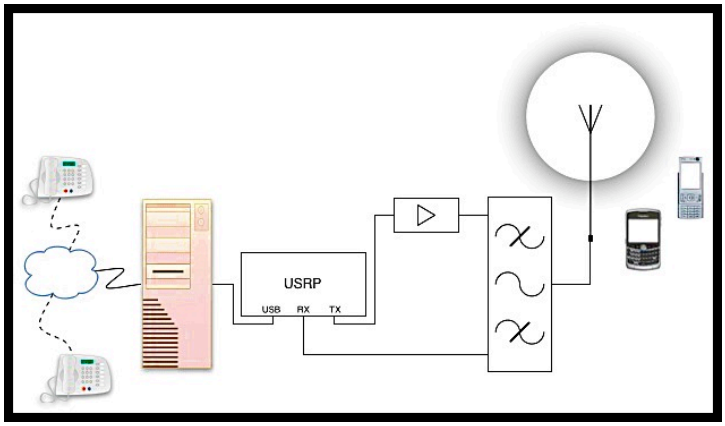


Figure 2. 10 OpenBTS

2.18.2 USRP

[4]The Universal Software Radio Peripheral (USRP) products are computer-hosted software radios. They are designed and sold by Ettus Research, LLC and its parent company, National Instruments. The USRP product family is intended to be a comparatively inexpensive hardware platform for software radio, and is commonly used by research labs and universities. 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. Some USRP models also integrate general functionality of host computer with an embedded processor that allows USRP Embedded Series to operate in standalone fashion. The USRP product family includes a variety of models that use a similar architecture. A motherboard provides the following subsystems clock generation and synchronization, FPGA, ADCs, DACs, host processor interface, and power regulation. These are the basic components that are required for baseband processing of signals. A modular front-end, called a daughterboard, is used for analogue operations such as up/down-conversion, filtering, and other signal conditioning. This modularity permits the USRP to serve applications that operate between DC and 6 GHz.

In stock configuration the FPGA performs several DSP operations, which ultimately provide translation from real signals in the analogue domain to lower-rate, complex, baseband signals in the digital domain. In most use-cases, these complex samples are transferred to/from applications running on a host processor, which perform DSP operations. The code for the FPGA is open-source and can be modified to allow high-speed, low-latency operations to occur in the FPGA.

A USRP equipped with two daughter boards.

Figure 2. 11 USRP

Softwares used for the implementation of OpenBTS system apart OpenBTS itself are:

Asterisk

GNU Radio

2.18.3 AsteriskS

[5]Asterisk is a software implementation of a telephone private branch exchange (PBX).Like any PBX, it allows attached telephones to make calls to one another, and to connect to other telephone services, such as the public switched telephone network (PSTN) and Voice over Internet Protocol (VoIP) services. Its name comes from the asterisk symbol, *.

Asterisk is released under a dual license model, using the GNU General Public License (GPL) as a free software license and a proprietary software license to permit licensees to distribute proprietary, unpublished system components. The Asterisk software includes many features available in proprietary PBX systems voice mail, conference calling, interactive voice response and automatic call distribution. The Inter-Asterisk exchange (IAX2) protocol, native to Asterisk, provides efficient trunking of calls among Asterisk PBXs, in addition to distributed configuration logic, and call completion to VoIP service providers who support it.

2.18.4 GNURadio

[6]GNU Radio is a free software toolkit for building software-defined radios. It can be used for signal processing from the physical layer with readily-available low-cost external RF hardware, or without hardware in a simulation-like environment. It's widely used for learning about, building, and deploying software radios, both in business and academic fields.

GNU Radio applications are primarily written using Python programming language, while the supplied performance-critical signal processing path is implemented in C++ using processor floating-point extensions, where available. Thus, the developer is able to implement real-time, high-throughput radio systems in a simple-to-use, application-development environment. GNU Radio supports development of signal processing algorithms using pre-recorded or generated data, avoiding the need for actual RF hardware.

GNU Radio is a signal processing package, which is distributed under the terms of the GNU General Public License (GPL). All of the code is copyright of the Free Software Foundation. The goal is to give ordinary software people the ability to 'hack' the electromagnetic spectrum, that is, to understand the radio spectrum and think of clever ways to use it.

The GNU Radio project utilizes the Universal Software Radio Peripheral (USRP) which is a computer-based transceiver containing four 64 mega sample-per-second (MS/s) 12-bit

analog-to-digital (A-D) converters, four 128 MS/s 14-bit digital-to-analog (D to A) converters, and support circuitry for the interface to the host computer. The USRP can process signals up to 25-MHz wide, depending on the model. Several transmitter and receiver plug-in daughter boards are available covering various bands between 0 and 5.9 GHz.

2.19 Triangulation

[7]In geometry, trilateration is the process of determining absolute or relative locations of points by measurement of distances, using the geometry of circles, spheres or triangles. In addition to its interest as a geometric problem, trilateration does have practical applications in surveying and navigation, including global positioning systems (GPS). In contrast to triangulation, it does not involve the measurement of angles.

In two-dimensional geometry, it is known that if a point lies on two circles, then the circle centres and the two radii provide sufficient information to narrow the possible locations down to two. Additional information may narrow the possibilities down to one unique location.

In three-dimensional geometry, when it is known that a point lies on the surfaces of three spheres, then the centres of the three spheres along with their radii provide sufficient information to narrow the possible locations down to no more than two (unless the centres lie on a straight line).

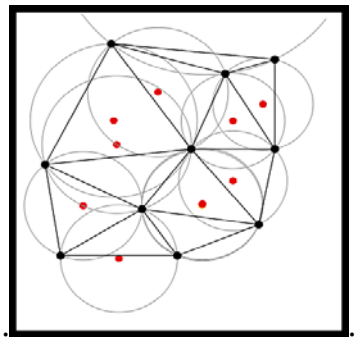


Figure 2. 12 3D Trilateration

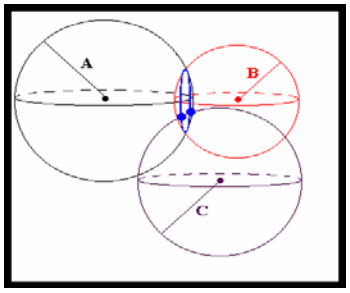


Figure 2. 13 3D Trilateration (1)

CHAPTER 03

DESIGN AND DEVELOPMENT

3.1 Detailed Design

Project has been divided into three modules

1. Development of 3D Model

2. Development of GSM Front End

3. Development of Sensor Network and Trilateration/Triangulation

3.2 Development of 3D model

The development of 3D model involves the following 3 steps

1. Accurate Measurements of the Intended Area

2. Development of 3D model in Google Sketchup

3. Conversion of 3D model from Google Sketchup to Blender

3.2.1 Accurate Measurements of the Intended Area

The very first device in this module involves that a precise measurement of all the permanent landscape of our domain. The permanent landscape includes

Walls

ACs

Doors

Or any other feature of the room that is not moved frequently.

3.2.2 Development of 3D model in Google Sketchup

The second step of this module is the development of the 3D model of our intended area according to measurements taken in the first step. We chose this software due to its simplicity and small learning curve.

3.2.3 Conversion of 3D model from Google Sketchup to Blender

Once the 3D model has been developed Google Sketchup, it needs to be exported into Blender. Blender is feature rich open source software that offers an API in Python. This fulfils our need as we require some customization of the software to display the location of the GSM device through conspicuous marker.

3.3 Development of GSM Frontend

To provide access to the GSM devices within our domain, a GSM front end will be established through the use of OpenBTS and USRP network. Any GSM device that enters into our domain will have its services hacked by the way of a middleman providing us with complete access to the communication in GSM-900 band as the USRP available provides us with this capability only in the GSM-900 band.

This module consists of following parts:

1. Acquiring a USRP kit
2. Installing Necessary Softwares
3. Interfacing the USRP Kit with a PC

3.3.1 Acquiring a USRP Kit

In order to establish a GSM front end we must acquire a USRP kit. The entire USRP kit consists of an antenna, a USRP device, a USB cable and adapter. This entire kit costs around $1000 but fortunately, these are available in the university.

3.3.2 Installing Necessary Softwares

The establishment of the GSM front for eavesdropping requires the use of following softwares:

1. GNU Radio

2. OpenBTS

3.3.3 Interfacing the USRP Kit with a PC

Once the aforementioned softwares have been installed, the USRP is connected with a PC. With some little adjustments, our USRP acts a GSM front end for the GSM devices in the intended area as shown in figure

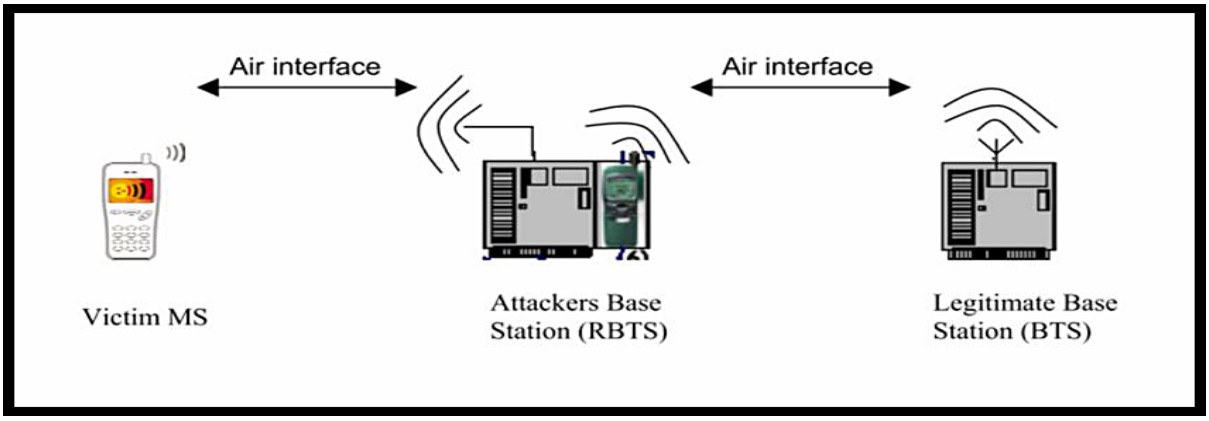


Figure 3. 1 Interfacing USRP with PC

3.4 Development of Sensor Network and Trilateration

This is the third and last module of our project. Multiple sensors will be deployed in different locations throughout our domain. These sensors will be responsible for the detection and location of the GSM devices within our domain. These sensors will be interfaced with Arduino microcontroller circuit. The data from the sensors will be processed and used in the triangulation. The choice of the triangulation algorithm depends upon the make and type of

sensors used which in turn is being decided according to our needs based on trials and tests. This module is further divided into the following devices

1. Selection of Suitable Sensors

2. Deployment of Sensors in the Intended Area and Collecting Their Data

3. Translating Data from Sensors into Distance

4. Feeding the Data into Trilateration/Triangulation Algorithm

5. Feeding the output from the Algorithm into our 3D model

3.4.1 Selection of Suitable Sensors

The first and perhaps the most critical and important part of this module is the selection of suitable sensors. Finding sensors for the localization of GSM devices is a very challenging prospect. At first, we were vying for the antenna circuitry used in GSM devices but they were of no use. Finally, the sensors of our requirement were diode based. Consider the circuit diagram shown in figure[8]:

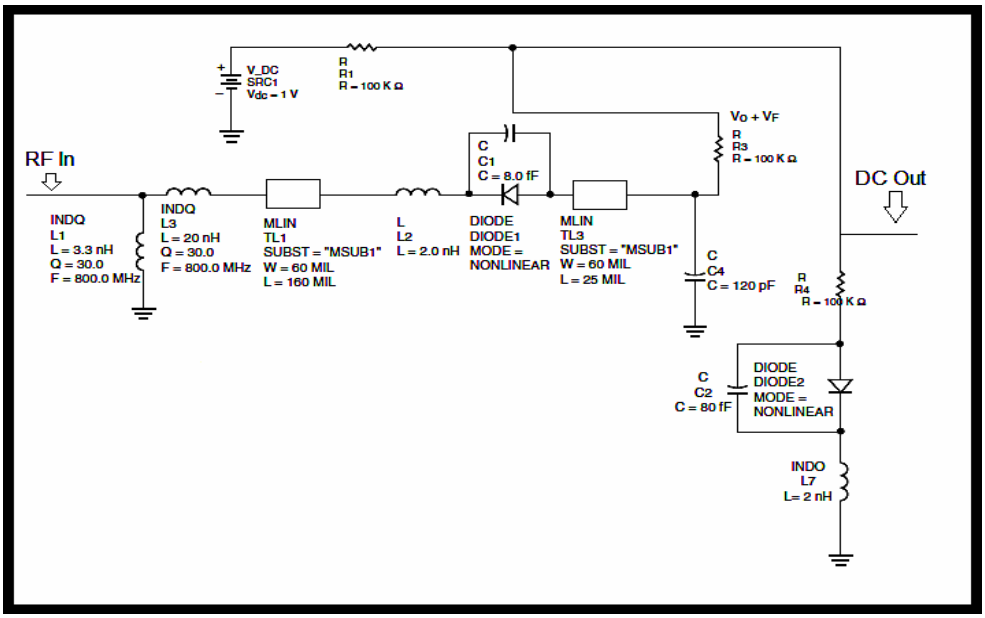


Figure 3. 2 Circuit Diagram of Sensors

This is the circuit diagram of the sensor we are using. It employs the HSMS-2820 Schottky Diode. This is basically a band pass circuit in which the matching circuitry will decide which band is to pass and which is to be barred.

3.4.2 Deployment of Sensors in the Intended Area and Collection of Data

Once the sensors have been selected, a minimum of 4 sensors will be deployed in arbitrary positions in the intended area. The sensors we are using will receive the RF power of any GSM device entering into our domain and based on that power will output DC voltage. This is called RSSI based localization. This voltage will be collected.

3.4.3 Translating Data from Sensors into Distance

The voltage thus collected carries no meaning unless it can be equated to distance. So, we will measure the output of our sensor corresponding to some distance of a GSM device from the sensor. In this way we can translate the voltage output from our sensor into distance.

3.4.4 Feeding the Data into Trilateration/Triangulation Algorithm

We have the distance of the GSM device that we calculated from the sensors. The DC voltage output will be interfaced with Arduino UNO microcontroller circuit, as shown in figure.

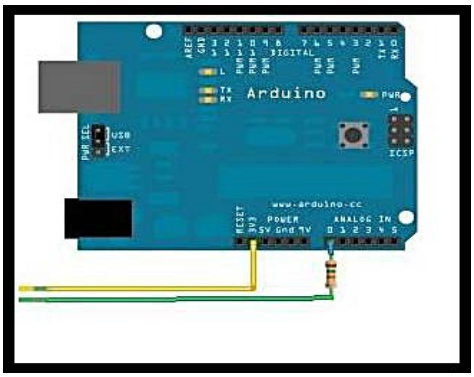
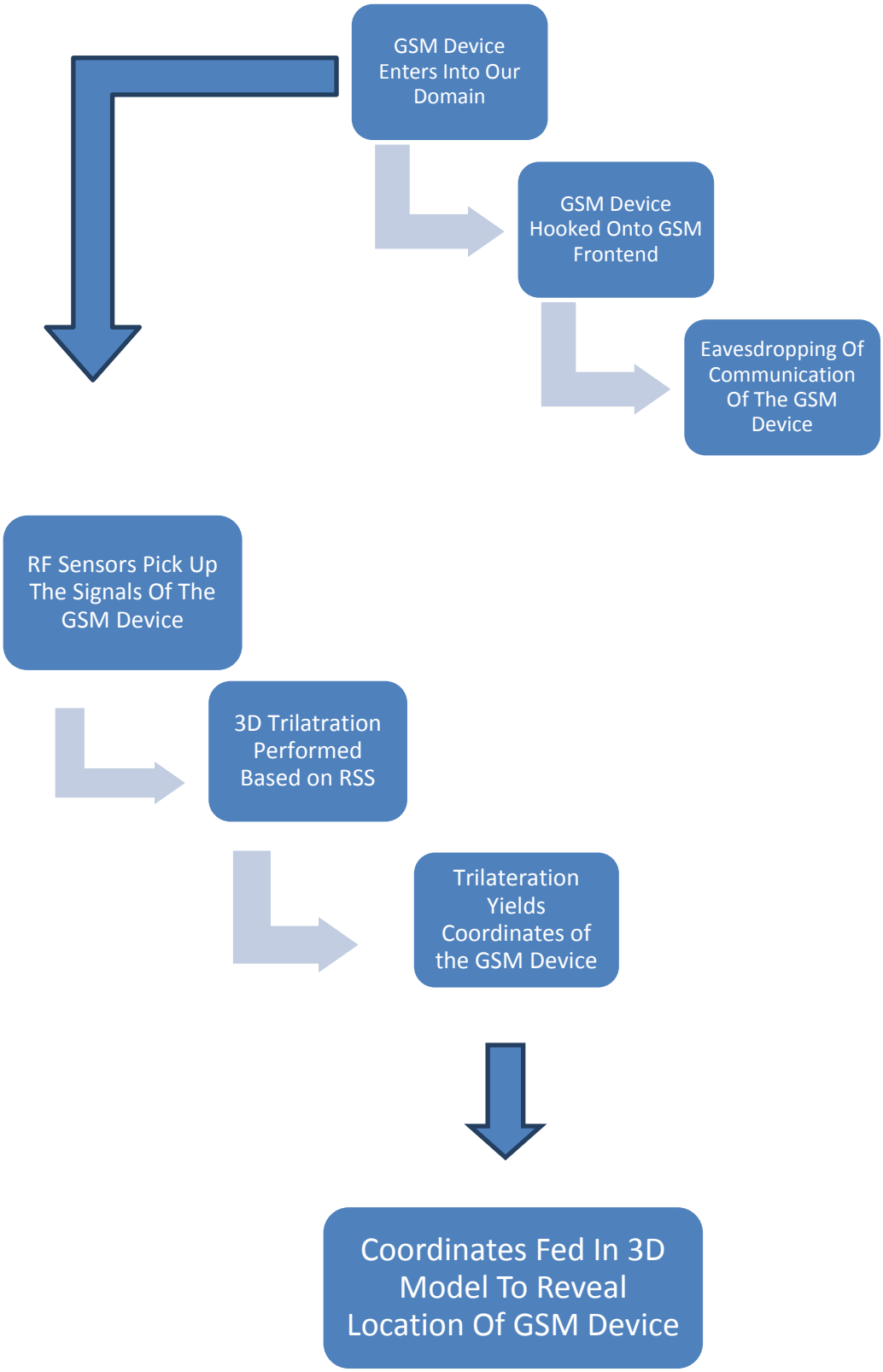


Figure 3. 3 Arduino UNO Microcontroller

3.4.5 Feeding the output from the Algorithm into our 3D model

The Arduino board will be interfaced with a PC via the serial port. The Arduino board will communicate to the PC the voltages collected from the sensors. The voltages will be translated into distance through trial and error method in MATLAB. Furthermore, the distances will be fed into the trilateration algorithm also developed in MATLAB, finally yielding coordinates of the GSM device. These coordinates will be imported into Blender thus revealing the precise location of the GSM device in our intended area.

Summary of Project Modules:



CHAPTER 04

ANALYSIS AND EVALUATION

4.1 Module No.1 Development of 3D Model of the Intended Area

Start off our results with the first module of this project-3D model. The measurements of the intended area which was decided to be the SDR Lab were taken according to which a 3D model was developed in Google Sketchup.

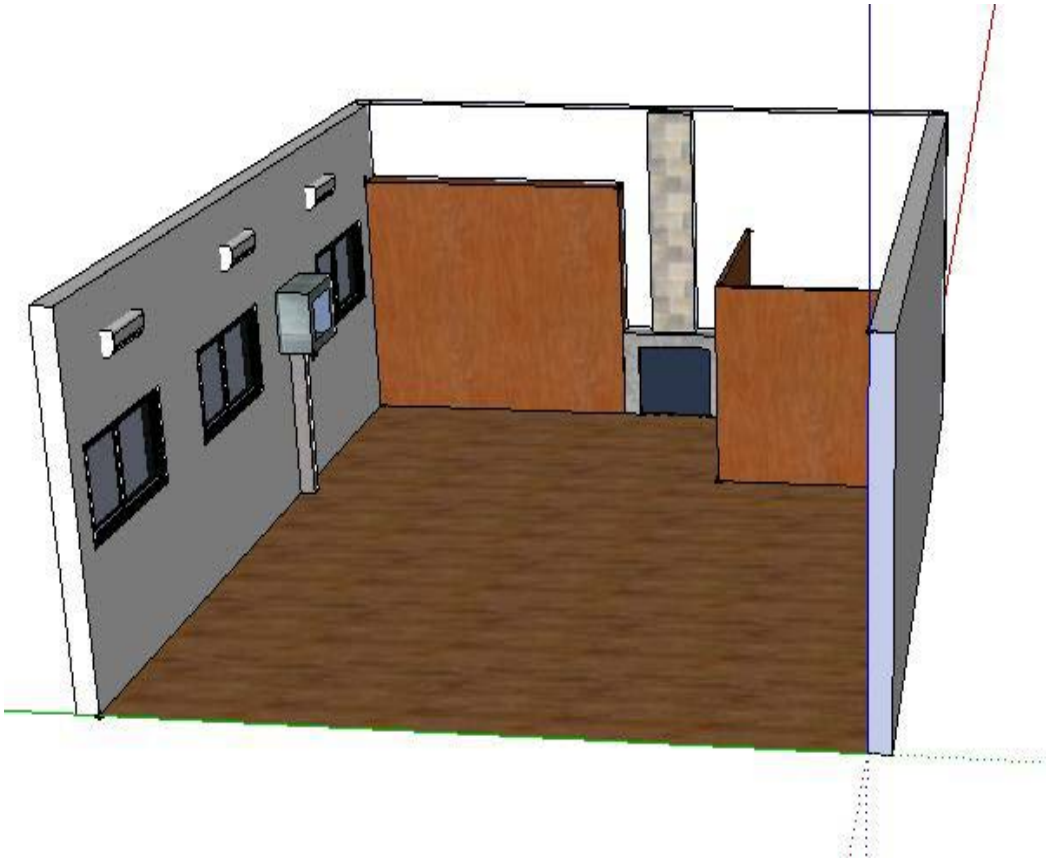


Figure 4. 1 3D Model Of Intended Area in Google Sketchup

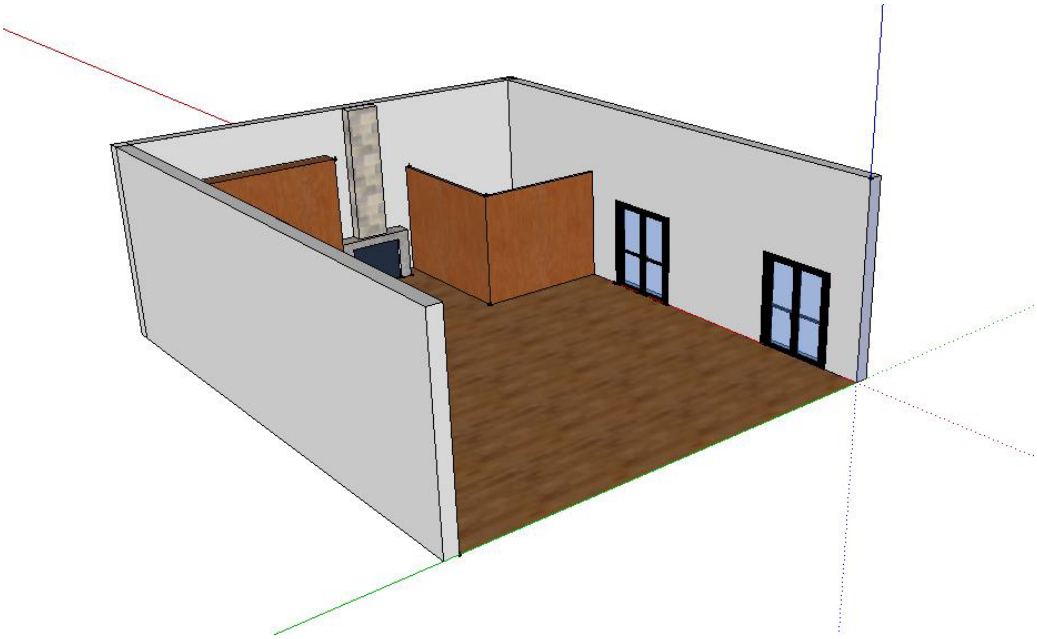


Figure 4. 2 3D Model of Intended Area in Google Sketchup

Once made in Google Sketchup, the 3D model was ready to be imported in Blender. The 3D model in Blender

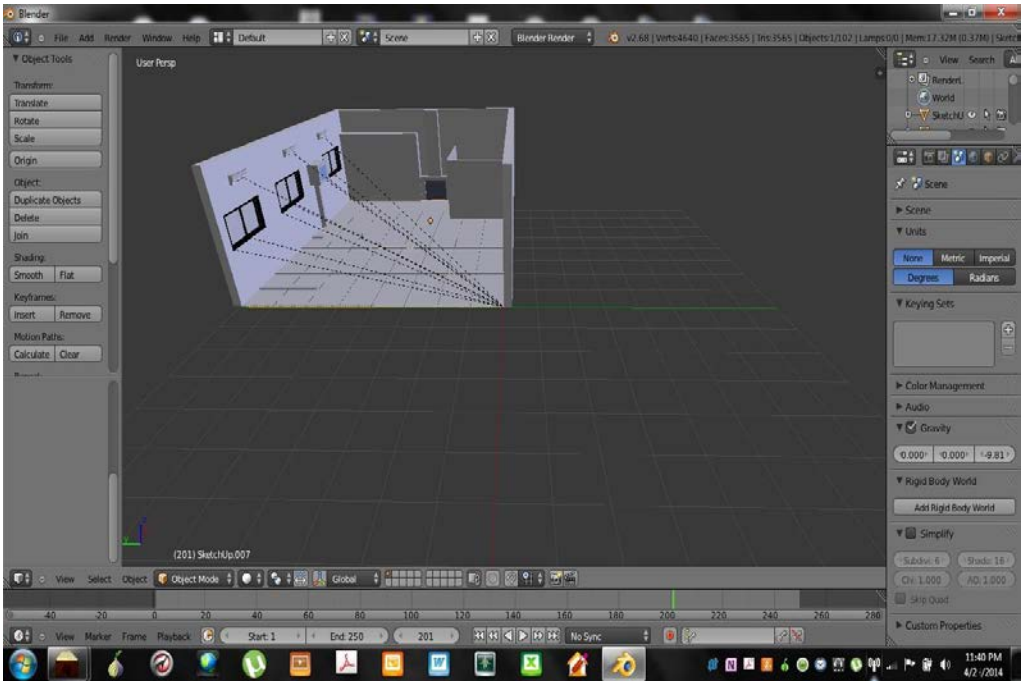


Figure 4. 3 3D Model in Blender

4.2 Module 2 Establishment of GSM Front End

As explained earlier, this module has 3 devices. First device was to acquire a USRP Kit. USRP Kit are available in SDR LAB. Second was to install certain softwares. These softwares are compatible with Linux operating system, for that we have installed Ubuntu 12.04 LTS. And then we continue with installation of these softwares i.e GNU radio 3.4.2, OpenBTS version 2.8. OpenBTS along with USRP kit makes fake BTS.

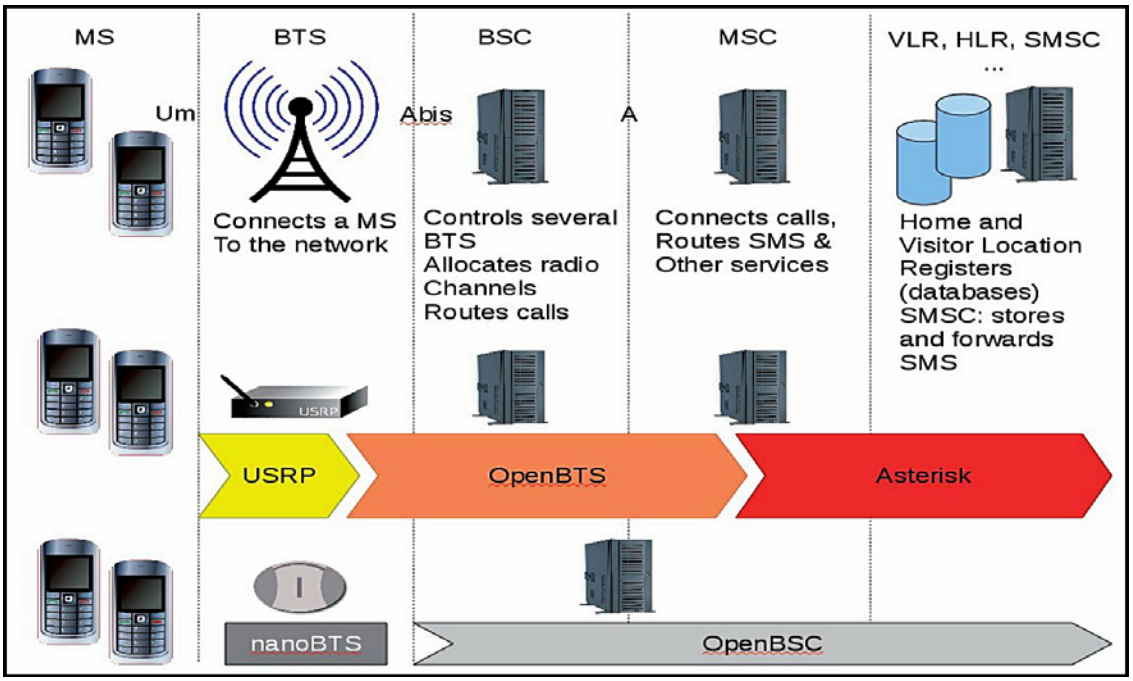


Figure 4. 4 GSM Front End

4.2.1 Installing Softwares

4.2.1.1 Installing GNU Radio

1) Building UHD (USRP hardware and software drive)

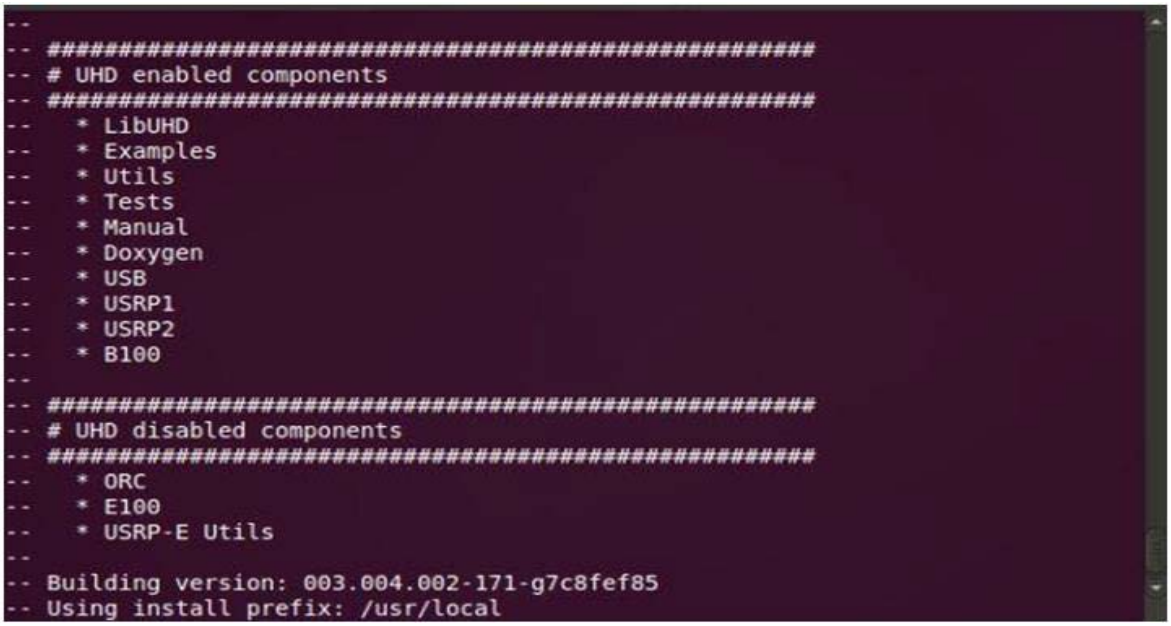


Figure 4. 5 Building UHD of GNU Radio

2) Installing GNU Radio

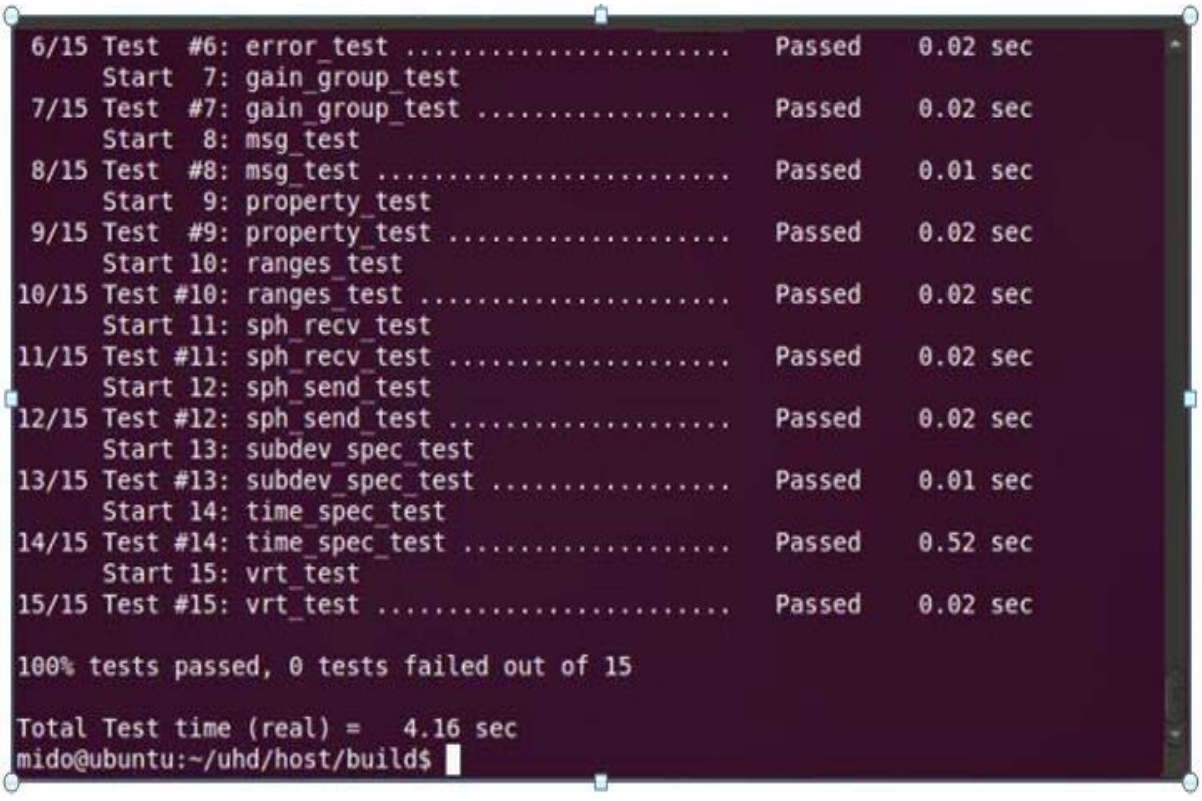


Figure 4. 6 Installing GNU Radio

4.2.1.2 Installing Open BTS

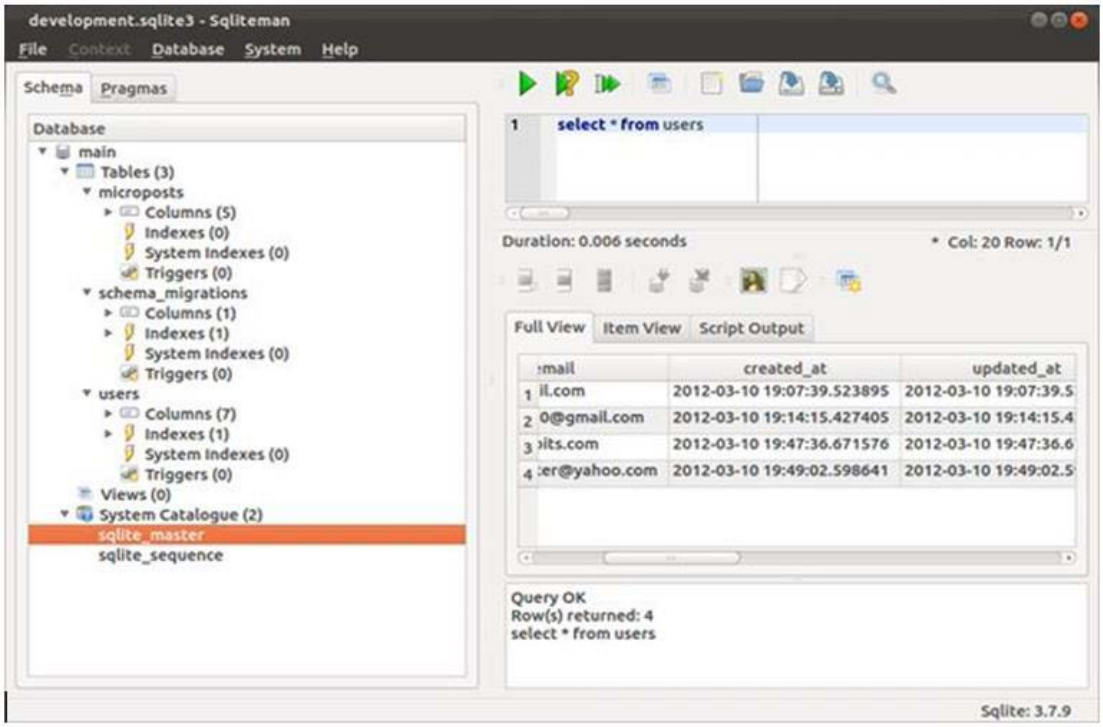


Figure 4. 7 OpenBTS Installation

Testing of USRP device by connecting it to the GNU Radio installed on Ubuntu 12.04

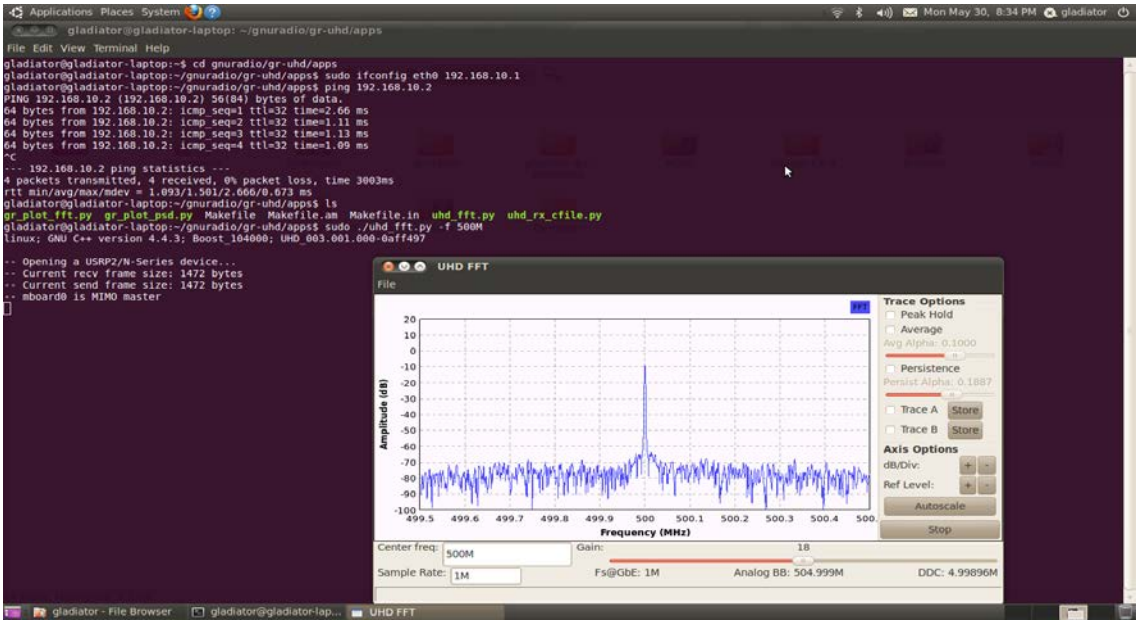


Figure 4. 8 Testing USRP

After installing OpenBTS successfully, For instance, a Global System for Mobile Communications (GSM) base station can be built by connecting the USRP to a computer that runs the open-source Unix software OpenBTS.

4.3 Clock Calibration

Kal is a tool to calibrate the clock. As we are using USRP 1 and the use of USRP1 require hardware modification. Because of onboard frequency reference, we must use an external reference for greater frequency accuracy. So must be modified to use an external 52MHz clock.

4.4 Link Establishment Process

For establishing link, we require a GSM modem. GSM modem will be a mobile phone (like Samsung mobile).We has the targeted mobile phone and will be connected to our FakeBTS using its credentials. Figure 25 shows screen shots taken while link establishment

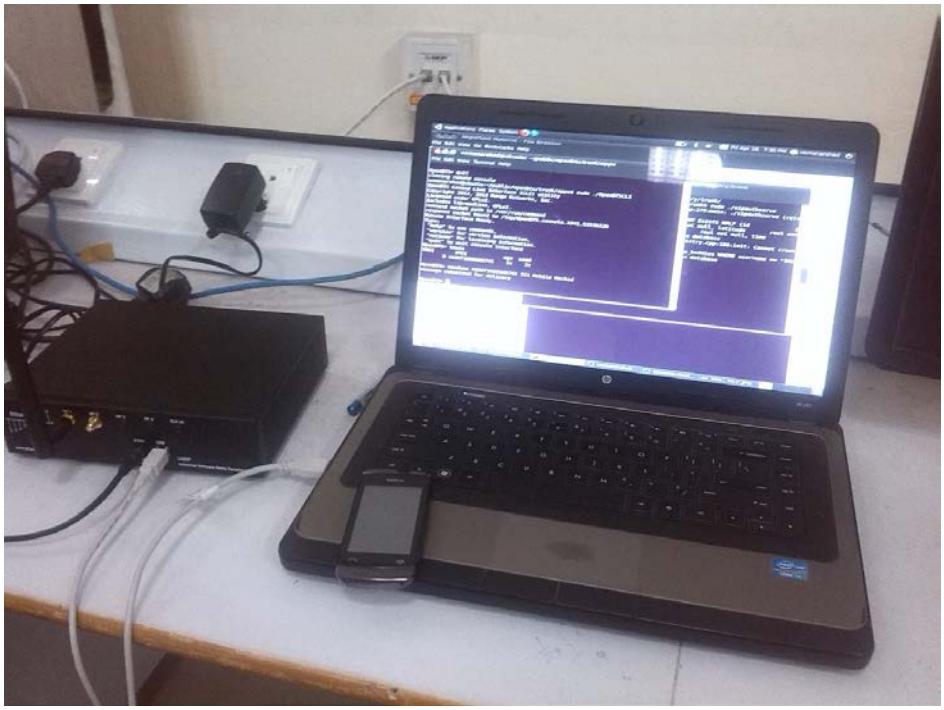


Figure 4. 9 Link Establishment Process

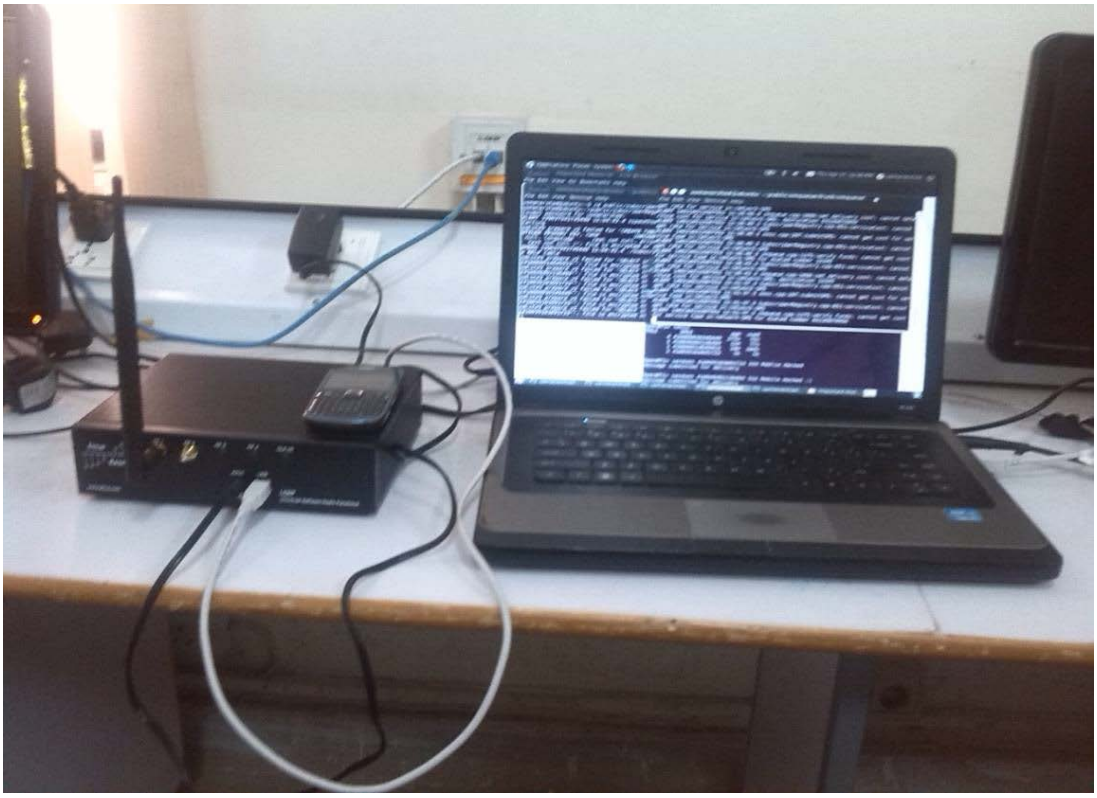


Figure 4. 10 Link Establishment Process (1)

4.5 Module No. 3 Development of Sensor Network and Trilateration

Progress in this module was halted for long due to the difficulty in finding and acquiring suitable sensors. Recently, we have found a suitable Schottky diode (HSMS-2820) based RF sensor that serves our need. [8]Following is the ADS simulation of the said sensor's circuit.As stated earlier, this is basically a band pass filter that allows a select band to pass. The first part the F_NTONE is for the generation of RF power at 850MHz. What follows are the two chip inductors L1 and L3, and Microstrip line MLIN. These components form the matching circuit. The rest of the components including the diode form the filter. The frequency response of the circuit displayed above is shown in figure:

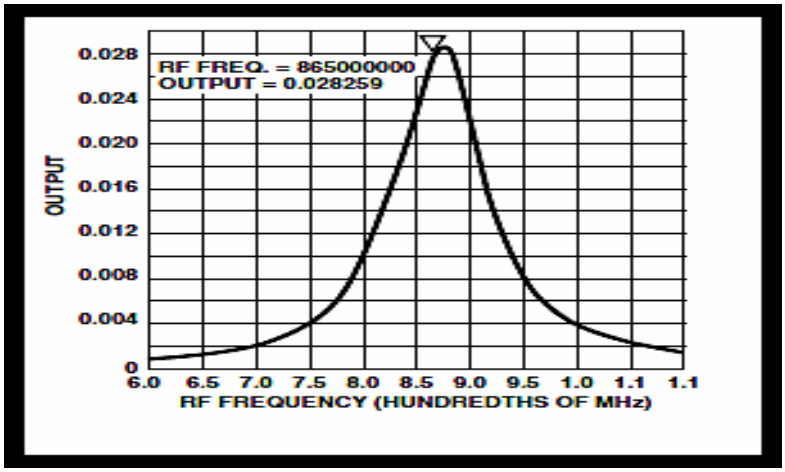


Figure 4. 11 Frequency Response Graph

It is visible, it has sufficient frequency response in the required band i.e. GSM 900. We are concerned mostly the uplink band 890-915 MHz

The magnitude of output DC voltage increases with increase in input RF power. Hence, with increase in distance, RF input decreases and DC output decreases as well which is our requirement. Consider this graph and table displayed in figure.

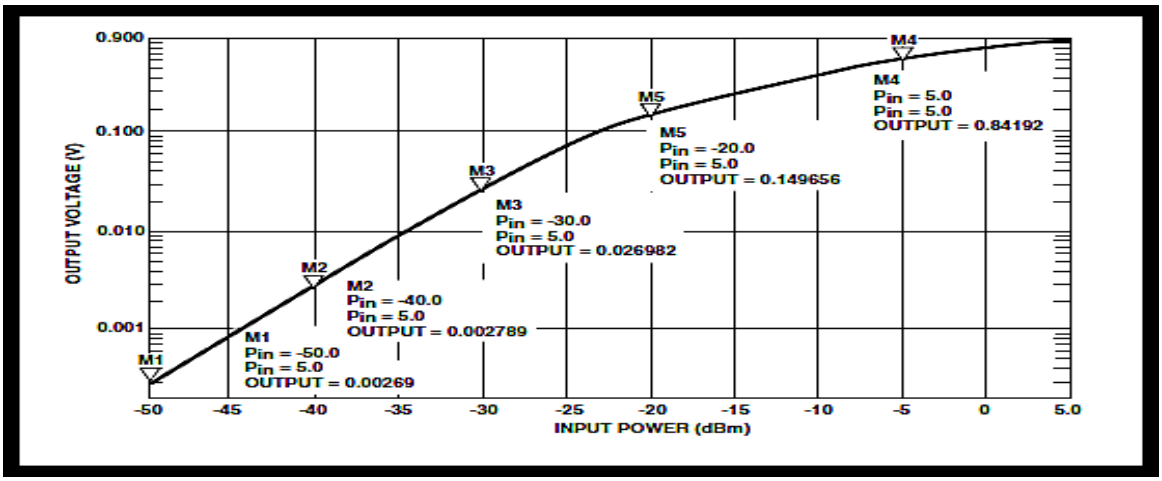


Figure 4. 12 Input power verses voltage graph

Table no 3 Voltage and corresponding power.

At 850 MHz Pin (dBm)	Simulated Vout
-40	0.00279
-35	0.00880
-30	0.02698
-25	0.07298
-20	0.14966
-15	0.24788
-10	0.37675
-5	0.55367
0	0.74701
5	0.84192

4.6 Trilateration Algorithm

We have designed the algorithm for trilateration in MATLAB. First off, we developed a function that calculates the location, based on the inputs of the location of sensors and the distance of the device from the sensor. The code of this function is given as APPENDIX A.

Once the function was developed, we made the main file that calls this function. With some dummy locations for sensors, we were able to test the algorithm.

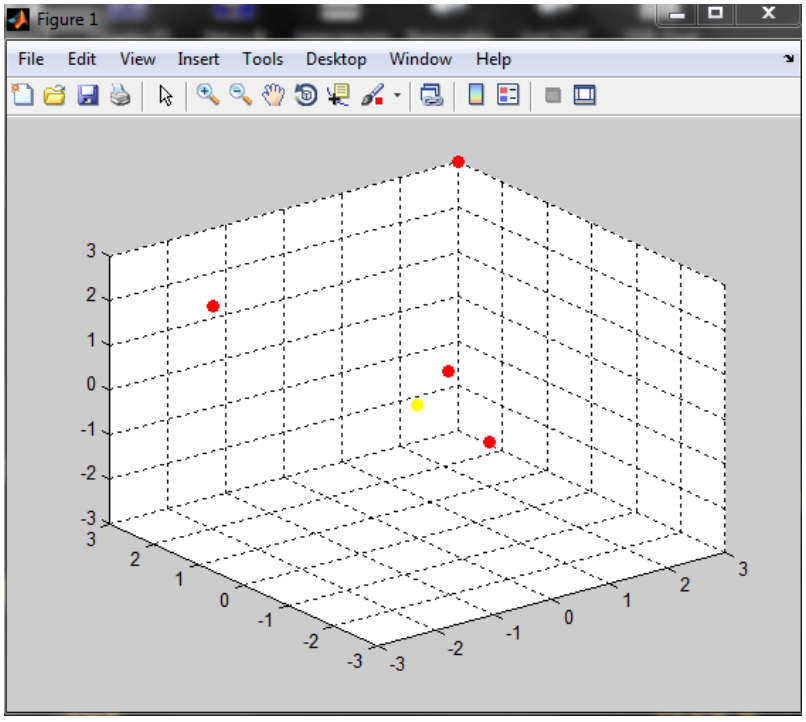


Figure 4. 13 Trilateration Algorithm Output

The red dots show the position of sensors while the yellow dot shows the position of the device.

At this instant, the coordinates of the device were written on to a text file for further use, employing the following code

4.7 Display in 3D Model

Once the coordinates have been calculated through the means of trilateration, the task of importing them and displaying them in the 3D model, remains. As mentioned earlier, the coordinates had been written on a text file. Employing the Python API of Blender, we were able to import those coordinates and create a 'MESH' on those coordinates. In this way, the task of locating and displaying our device in the 3D model was completed. Following figures shows the location of device, according to the coordinates to the results of the algorithm explained above

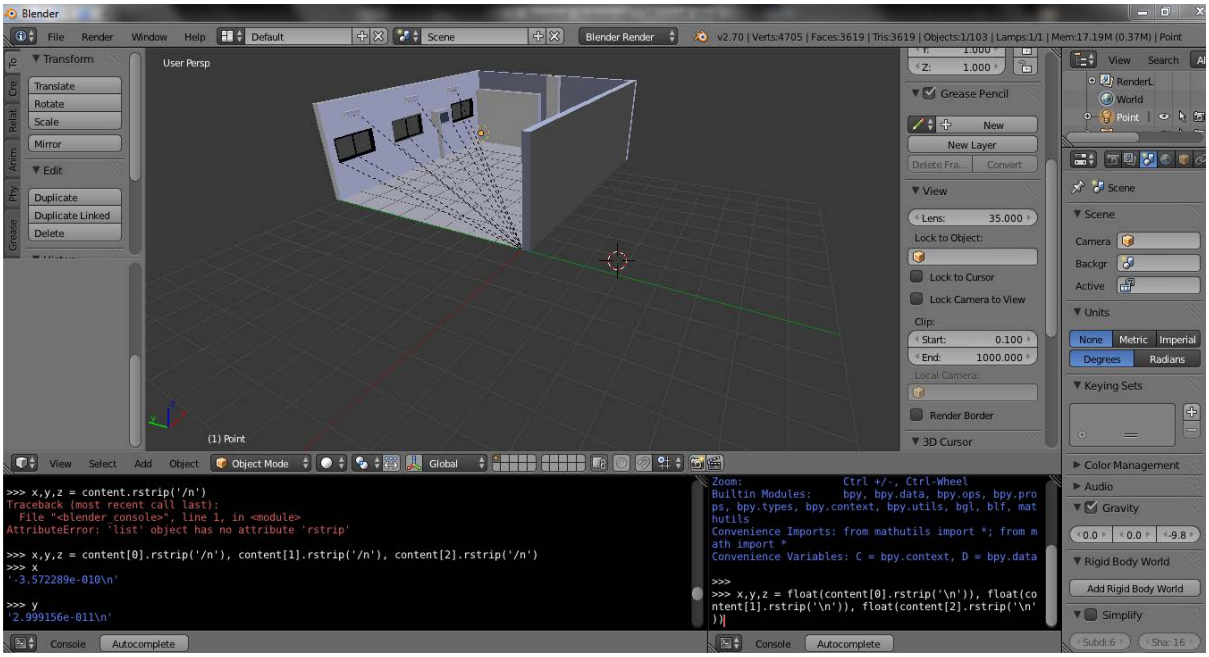


Figure 4. 14 3D model in blender

As is visible clearly, we can see the marker for location in bottom left corner of the domain thus, completing our objective of locating the GSM device in the intended area.

CHAPTER 05

FUTURE WORK

5.1 Recommendations for Future Work

The mechanism we have developed for the 3D localization of GSM devices can be extended to other wireless technologies like IR devices, Bluetooth and Wi-Fi. If such a system can be designed as to incorporate the localization of all such wireless technologies, that system would become a complete one of a kind monitoring system for wireless devices. Such a system would surely prove invaluable for security purposes.

Furthermore, with the advent of Smartphone another technology can be used for the purpose of localization – Beacons. Beacons are a very recent development. Beacons were actually developed to challenge NFC for transactions and information sharing. Beacons now days are finding use in commercial avenues. Following is a picture of a beacon:

Figure 5. 1 Beacons

Beacons use the Bluetooth 4.0 technology and operate on 2.4 GHz. As seen in the figure above they are small enough to fit inside the palm of a hand and are very power efficient with

a single battery lasting up to 2 years on end. They have range of about 200 ft. They work by constantly communicating with an app in the Smartphone, sending and receiving messages.

5.2 Conclusion

The GPS is an extremely accurate localization system but it fails when it is employed indoors due to various reasons. For these very reasons, we attempted to develop an indoor positioning system that could locate a GSM device within our intended area. Our project does what it states in its objective. As soon as a GSM device enters into our domain, it is detected and located immediately. Simultaneously, the GSM device is hooked onto a GSM front end giving us capabilities like eavesdropping.

APPENDICES

APPENDIX A

TRILATERATION CODE IN MATLAB

First of all a function was used to actually calculate trilateration based on the RSSI values and coordinates of sensors[9]:

```
function [x, y, z ] = three_tri( x1, y1, z1, d1, x2, y2, z2, d2, x3, y3,
z3, d3, x4, y4, z4, d4 )
%3-D trilateration. 4 anchor nodes
% x1 = x coordinate of reader 1
% y1 = y coordinate of reader 1
% z1 = z coordinate of reader 1
% d1 = distance from tag to reader 1
% Function signature is done this way to make the functions below easier
% to type and understand and debug. Harder to call the function but
% easier to edit/understand the equations below
%x_numerator elements
x_n11 = (d1^2-d2^2) - (x1^2-x2^2) - (y1^2-y2^2) - (z1^2-z2^2); %sigma
x_n21 = (d1^2-d3^2) - (x1^2-x3^2) - (y1^2-y3^2) - (z1^2-z3^2); %beta
x_n31 = (d1^2-d4^2) - (x1^2-x4^2) - (y1^2-y4^2) - (z1^2-z4^2); %phi
x_n12 = 2*(y2-y1);
x_n22 = 2*(y3-y1);
x_n32 = 2*(y4-y1);
x_n13 = 2*(z2-z1);
x_n23 = 2*(z3-z1);
x_n33 = 2*(z4-z1);
%all the individual elements in M(COLA ieee document)
d11 = 2*(x2-x1);
d21 = 2*(x3-x1);
d31 = 2*(x4-x1);
d12 = 2*(y2-y1);
d22 = 2*(y3-y1);
d32 = 2*(y4-y1);
d13 = 2*(z2-z1);
d23 = 2*(z3-z1);
d33 = 2*(z4-z1);
%bringing M together into [3, 3] matrix
d = [d11, d12, d13; d21, d22, d23; d31, d32, d33];
98
%bringing numerator together for x
x_n = [x_n11, x_n12, x_n13; x_n21, x_n22, x_n23; x_n31, x_n32, x_n33];
%finding x by dividing matrix operation and then determinant
x = x_n / d;
x = det(x);
%individual y elements
y_n11 = 2*(x2-x1);
y_n21 = 2*(x3-x1);
y_n31 = 2*(x4-x1);
y_n12 = x_n11; %sigma
y_n22 = x_n21; %beta
y_n32 = x_n31; %phi
y_n13 = 2*(z2-z1);
y_n23 = 2*(z3-z1);
y_n33 = 2*(z4-z1);
```

```
%bringing numerator together for y
y_n = [y_n11, y_n12, y_n13; y_n21, y_n22, y_n23; y_n31, y_n32, y_n33];
%finding y by dividing matrix operation and then determinant
y = y_n / d;
y = det(y);
%individual z elements
z_n11 = 2*(x2-x1);
z_n21 = 2*(x3-x1);
z_n31 = 2*(x4-x1);
z_n12 = 2*(y2-y1);
z_n22 = 2*(y3-y1);
z_n32 = 2*(y4-y1);
z_n13 = x_n11; %sigma
z_n23 = x_n21; %beta
z_n33 = x_n31; %phi
%bringing z numerator together
z_n = [z_n11, z_n12, z_n13; z_n21, z_n22, z_n23; z_n31, z_n32, z_n33];
%finding z by dividing matrix operation and then determinant
z = z_n / d;
z = det(z);
end
```

This function was called in the main file that displays the point of interest calculated from Trilateration, calibrated the coordinates of the room as to display the location of the GSM device calculated in Trilateration function, in the 3D model where the coordinates were imported[9]:

```
%while(1)
%prevents rounding when displaying fractions
format long
clear
pause(2)
%Reader 3-D Coordinates [x, y, z]
Reader = [4.96, 7.966, 1.87; 6.124, 7.966, 2.208; 9.749, 6.146, 2.711;
6.971, 0, 2.170];
%plot reader locations
scatter3(getcolumn(Reader(1:4,1:3),1),getcolumn(Reader(1:4,1:3),2),
getcolumn(Reader(1:4,1:3),3), 'MarkerEdgeColor', [1 0 0],
'MarkerFaceColor', [1 0 0]);figure(gcf)
%x = 0;0;0;
%y = 0;0;0;
%x = getcolumn(Reader(1:3,1:2),1)
%y = getcolumn(Reader(1:3,1:2),2)
%e = [1;1;1]
hold on
%errorbar(x,y, e, 'og', 'Marker', '+');
axis([0 9.749 0 7.966 0 3.558 0 1]) %set axis for 2-D graphs
set(gca, 'XTick', 0:1:9);
set(gca, 'YTick', 0:1:7);
set(gca, 'ZTick', 0:0.5:3.5);
grid on;
%distances to Tag from Reader(i)
%Distance = [2.82842715;2.236067977;2.236067977]; %(0, 0) tag
MobileLocation = [.38 .72 .32];
Distance = sqrt((MobileLocation(1) - Reader(:,1)).^2 + (MobileLocation(2) -
Reader(:,2)).^2 + (MobileLocation(3) - Reader(:,3)).^2); %(0, 0 , 0) tag
x=0;
y=0;
z=0;
```

```
[x, y, z] = three_tri(Reader(1, 1), Reader(1, 2), Reader(1, 3),
Distance(1), Reader(2, 1), Reader(2, 2), Reader(2, 3), Distance(2),
Reader(3, 1), Reader(3, 2), Reader(3, 3), Distance(3), Reader(4, 1),
Reader(4, 2), Reader(4, 3), Distance(4));
scatter3(x, y, z, 'MarkerEdgeColor', [1 1 0], 'MarkerFaceColor', [1 1
0]);figure(gcf)
x
y
z
fName = 'D:/FYP/io.data';          %# A file name
fid = fopen(fName,'w');             %# Open the file
if fid ~= -1
  fprintf(fid,'%s\r\n',x);
  fprintf(fid,'%s\r\n',y);
  fprintf(fid,'%s\r\n',z);
  fclose(fid);
end

break;
%end
```

The coordinates were exported to a text file, from where they were imported in Blender Python API:

```
import bpy
fname = 'D:/FYP/io.data'

with open(fname) as f:
    content = f.readlines()

x,y,z = float(content[0].rstrip('\n')), float(content[1].rstrip('\n')),
float(content[2].rstrip('\n'))

bpy.ops.object.lamp_add(type='POINT', view_align=False, location=(x, y, z))
import bpy
fname = 'D:/FYP/io.data'

with open(fname) as f:
    content = f.readlines()

x,y,z = float(content[0].rstrip('\n')), float(content[1].rstrip('\n')),
float(content[2].rstrip('\n'))

bpy.ops.object.lamp_add(type='POINT', view_align=False, location=(x, y, z))
```

APPENDIX B

BIBLIOGRAPHY AND REFERENCES

BIBLIOGRAPHY

- Global System for Mobile Communications (en.wikipedia.org/wiki/GSM)
- Global System for Mobile Communications (http://www.gsma.com/aboutus/gsm-technology/gsm)
- USRPDevices
- (http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral)
- Ettus Research USRP devices (https://www.ettus.com/product)
- NI USRP (http://sine.ni.com/nips/cds/view/p/lang/en/nid/209949)
- GNU Radio
    - http://en.wikipedia.org/wiki/GNU_Radio
    - http://code.ettus.com/redmine/ettus/projects/uhd/wiki/GNU_Radio_UHD
    - http://gnuradio.org/redmine/projects/gnuradio/wiki
- Asterisk
    - http://www.digium.com/en/products/telephony-solutions
    - http://en.wikipedia.org/wiki/Asterisk_(PBX)
    - http://www.digium.com/en/products/asterisk
- OpenBTS
    - http://en.wikipedia.org/wiki/OpenBTS

- https://wush.net/trac/rangepublic
- http://gnuradio.org/redmine/projects/gnuradio/wiki/OpenBTS
- http://www.rangenetworks.com/products/openbts

- Triangulation
  - http://en.wikipedia.org/wiki/Triangulation
  - Delaunay Triangulation (http://en.wikipedia.org/wiki/Delaunay_triangulation)
  - 3D Delaunay Triangulation(http://onlinelibrary.wiley.com/doi/10.1111/1467-8659.1230129/abstract)
- Eavesdropping on GSM state-of-affairs

  Fabian van den Broek

  Radboud University, Nijmegen

  Institute for Computing and Information Sciences (iCIS)

- GSM Sniffing by KarstenNohl and SylvianManaut(Security Research Lab)

  Osmocomm.com

- Location Leaks on the GSM Air Interface

  By Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim

  University of Minnesota

REFERNECES

[1] The Evolution of Improvised Explosive Devices (IEDs) (http://www.brookings.edu/research/articles/2012/02/improvised-explosive-devices-singer)

[2] Global System for Mobile Communications (en.wikipedia.org/wiki/GSM)

[3] OpenBTS (http://en.wikipedia.org/wiki/OpenBTS)

[4] USRP Device(http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral)

[5] Asterisk (http://en.wikipedia.org/wiki/Asterisk_(PBX)

[6] GNU Radio (http://en.wikipedia.org/wiki/GNU_Radio)

[7] Trilateration (http://en.wikipedia.org/wiki/Trilateration)

[8] Application Note 1187(Design of an Input Matching Network for a DC biased 850 MHz Small Signal Detector)

[9] Indoor Positioning System by Robert Jarvis, Arthur Mason, Kevin Thornhill, Bobby Zhang