DENIAL OF SERVICE TO A GSM NETWORK

By

NC Rabeea Imran

NC Noor Fatima

NC Usman Arshad

NC Muhammad Irfan

Submitted to the Faculty of Electrical Engineering Department
National University of Sciences and Technology, Islamabad, in partial fulfillment
for the requirements of a B.E Degree in Telecommunication Engineering
JUNE 2014

ABSTRACT

DENIAL OF SERVICE TO A GSM NETWORK

General state of Security situation in Pakistan has deteriorated after 9/11. Most of the terrorist attacks are planned using Improvised Explosive Devices (IEDs). Various wireless technologies are used to trigger these devices like Infrared Transmitters, Cordless Telephony, and GSM Phones etc. Recently, incidents of using GSM phones to trigger IEDs is on a rise and Government of Pakistan has resorted to shutdown all GSM services as a brute force measure against these terrorist activities. This creates unnecessary inconvenience to general public who use GSM services for running their day to day activities.

One measure to avoid IEDs is with the use of Jamming devices, but they have a drawback of very less effective range. In addition, high output power is required to generate the jamming signal. Instead of using brute force jammers, the idea of Denial of service (DOS) can be implemented in the area of interest where GSM services will be denied to the users.

The project aims to establish a USRP based prototype which could act as a Fake Base station and unknowingly provide service to the users of a particular target area. The users would assume to have GSM service available to them whereas they won't be able to generate calls/SMS or receive calls/SMS either. The Fake Base Station will continue to dump all user calls and will not allow the users to hook to the main base station. To avoid an IED being triggered through a GSM network DOS cloud in a sensitive area can be implemented without generating very high jamming signals.

CERTIFICATE OF CORRECTNESS AND APPROVAL

It is certified that the work contained in this thesis titled “Denial of service to a GSM network”, carried out by Rabeea Imran, Noor Fatima, Usman Arshad and Muhammad Irfan under the supervision of Assoc. Prof. Dr Imran Rashid in partial fulfillment of the Bachelors of Telecommunication Engineering, is correct and approved.

Approved by

_____

Asst. Prof. Dr Imran Rashid

Project Supervisor

Military College of Signals, NUST

Dedication

Almighty Allah for his countless blessings

Teachers and friends for their help

And our beloved Parents for their support and prayers

ACKNOWLEDGEMENT

All praise for Allah Almighty who enlighten us with the requisite knowledge on portion of this subject enabling us to accomplish this challenging task.

We would like to extend our gratitude toward our advisor Dr. Imran Rashid for his help, guidance and generous support throughout our final year project.

We would like to thank lab staff, our friends, our seniors and all those whoever has helped us either directly or indirectly in the completion of the project.

LIST OF ABBREVIATIONS

IED	Improvised Explosive Device
GSM	Global System for Mobile Communication
DOS	Denial of Service
BTS	Base Transceiver Station
MS	Mobile Station
SMS	Short Message Service
VIP	Very Important Person
USRP	Universal Software Radio Peripheral
SDR	Software Defined Radio
IMSI	International Mobile Subscriber Identity
SS7	Signaling System 7
TDMA	Time Division Multiple Access
2G	2nd Generation
VLR	Visitor Location Register
API	Application Programming Interface
TRX	Transceiver
USB	Universal Serial Bus
SIM	Subscriber identity Module
CLI	Command Line Interface
UHD	USRP Hardware Driver
SIM	Subscriber Identity Module
MCC	Mobile Country Code
MNC	Mobile Network Code
FAB	Frequency Allocation Board
ARFCN	Absolute Radio Frequency Channel Number

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

The thesis includes complete project description detailed in five chapters. The core of the project is GSM network. Chapter 1 will brief about the problem statement and the identification of the solution to that problem.

1.1 Background

Security has always been a major concern for the confidential institutions of our country. Latest advancement in technology has questioned security sate of our country many times. Nowadays, use of Infrared Explosive Devices (IEDs) is on a rise during terrorist activities. Various wireless technologies are used to trigger these devices like Infrared Transmitters, Cordless Telephony and GSM Phones etc. Recently, incidents of using GSM phones to trigger IEDs is brought into light and Government of Pakistan has resorted to shut down all GSM services as a measure against these terrorist activities.

1.2 Problem statement

Incidents of using GSM phones to trigger IEDs is on a rise and Government of Pakistan has resorted to shut down all GSM services as a brute force measure against these terrorist activities. This creates unnecessary inconvenience to general public who use GSM services for running their day to day activities.

Another measure to avoid IEDs is with use of Jamming devices, but they have a drawback of very less effective range. In addition, a high output power is required to generate the jamming signal. Instead of using brute force jammers, the idea of Denial of service (DOS) can be implemented in the area of interest. Instead of complete breakdown of communication, a DOS attack can be established where GSM services will be denied to the users. In this way, probability of terrorist activity might be minimized.

1.3 Project Description

1.3.1 Objective

The project aims at establishing a USRP based prototype which could act as a Fake Base station and unknowingly provide service to the users of a particular target area.

The users would assume to have GSM service available to them whereas they won't be able to generate calls/SMS or receive calls/SMS either. The Fake Base Station will continue to dump all user calls/SMS and will not allow the users to hook to the main base station. To avoid an IED being triggered through a GSM network; DOS cloud in a sensitive area can be implemented without generating very high jamming signals.

1.3.2 Academic Objectives

1. Practical Learning of handling GSM network subscribers
2. Handling of live GSM subscribers
3. Optimum use of output power to deny GSM service to subscribers
4. Practical handling of USRPs and associated coding

1.3.3 End Goal Objectives

The USRP based prototype will be tested on various scenarios of DOS attacks, an effort will be made to improve the performance of DOS attack and ensure denial of service to maximum number of subscribers. In addition, range of DOS will be increased several times than practical jammers that are commercially available in the market with reduced cost in the design.

We aim at understanding and evaluating DOS theoretically; by analyzing through simulations and experimentation on USRP under which real time low energy signal modifications can be successful. Initially only one service provider will be targeted and later efforts will be made to tackle all major GSM service providers in the country.

1.4 Scope of the project:

It's an Open source project comprising of compiling and configuring essential software and integrating it with USRP.

1) *Software Requirements*

a) Compiling GNUradio: Installation and configuration aspects of **GNU Radio**

b) Compiling OpenBTS

c) Compiling smqueue

2) Testing GNUradio
3) OpenBTS configuration
4) Asterisk Configuration: The Asterisk is used to interface the GSM calls between the cellular phones served by the OpenBTS network.
    a) Database for maintaining registration of IMSI
5) Hardware and software integration
6) Registering phones to the OpenBTS network

GNU Radio together with USRP hardware proved to be a valuable platform for implementing complex radio system prototypes in a short time.

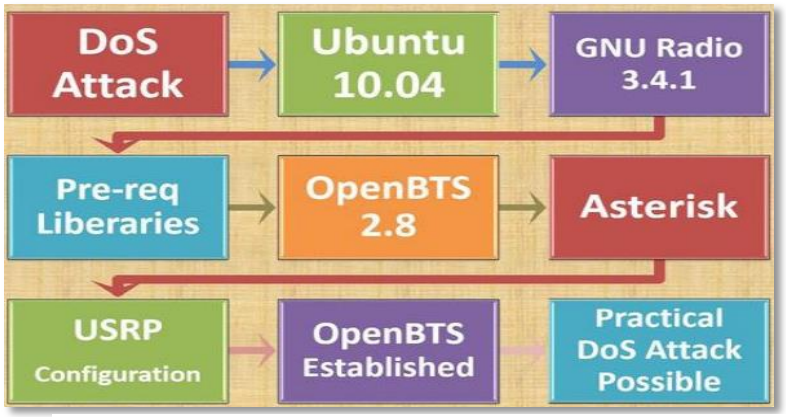

Figure 1-1: Approach

1.5 Applications

The prototype is designed for law enforcement agencies to implement in the regions marked as ‘red zones’ and the areas where the VIP movement is expected. The GSM users of the cell will get hooked to the device and their SMS and calls will be dumped unknowingly. Open registration feature of the design will enable the registration of users automatically to our network. Complete algorithm when implemented on a GSM BTS will assure greater range and efficient coverage just like the BTS of Telco of country.

1.6 System Model

In the figure1-2, system model diagram of the project has been shown. USRP mimics the functionality of BTS in GSM architecture, OpenBTS is the software implementation of GSM protocol stack; it will replicate the core network of GSM while the database functionality can be replicated through the Asterisk.

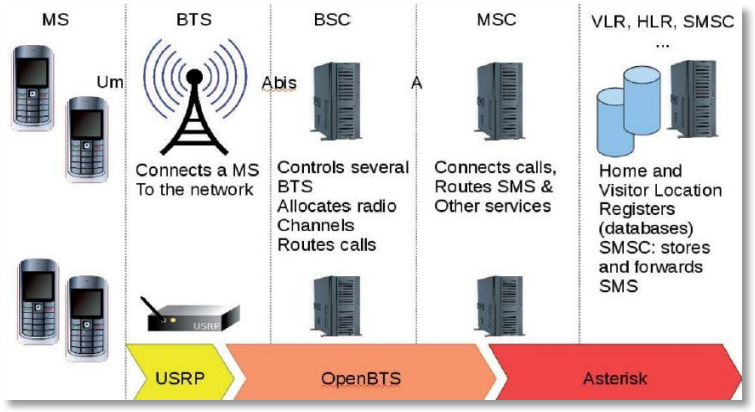

Figure 1-2: System model diagram

2 LITERATURE REVIEW

The core of the project is GSM network. This chapter covers the GSM architecture and important aspects which enabled the implementation of DOS attack.

2.1 GSM architecture

GSM stands for Group "Special Mobile", formed by the European Conference of Post and Telecommunications Administration (CEPT) in 1982, it was designed to replace the incompatible cellular systems in Europe, and this pan-European cellular system was called "GSM". When cellular service was set in, in 1991, the abbreviation of GSM was changed from "Group Special Mobile" to "Global System for Mobile Communications".

GSM is one of the most widely used standards worldwide, it is known as the second generation mobile telecommunications system "2G system". GSM network is the world's largest cellular network. Two billion people across 200 countries use GSM. Architecture of a GSM network is shown in figure 2-1.

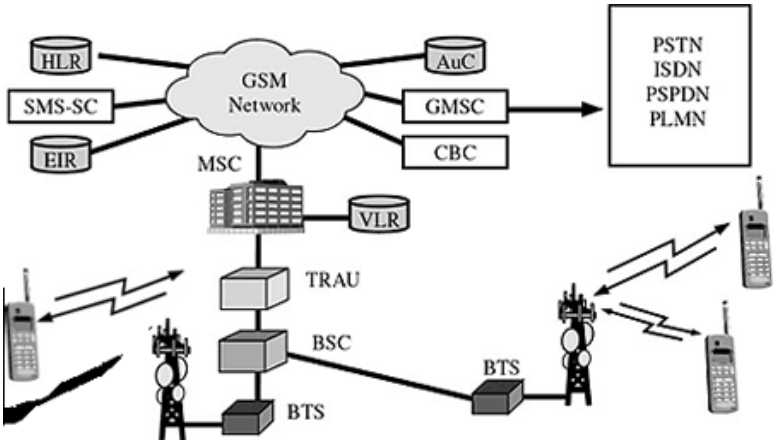

Figure 2-1: GSM architecture

A typical GSM network consists of terminal devices, Base Stations, Base Station Controller, databases namely HLR, VLR, EIR, switches and terminals. In the GSM network, information between signaling elements is transferred using many different signaling protocols including the SS7 protocol. The range of a GSM cell can exceed 35km.

2.1.1 Terminal equipment - Mobile Station (MS)

The MS consists of Mobile Equipment (ME) and a Subscriber Identity Module (SIM) card.

2.1.1.1 Mobile Equipment (ME)

The mobile station consists of digital signal processors, transceivers, and the subscriber identity card.

Mobile station provides the air interface in the GSM network to the users. Other services that are provided by the mobile station are

1. Voice Tele services
2. Data carrier services
3. And the supplementary services

The most common mobile equipment is the mobile phone. User inserts the SIM into the GSM cell phone so that the user can initiate and receive calls on the GSM cell phone, or can access other subscriber services in the GSM cell phone. If we remove the SIM from the mobile station then the mobile station can only be used to make emergency calls only and no other subscriber services can be accessed using that GSM cell phone or in other words the Mobile Station.

The Mobile Equipment uniquely identifies the International Mobile Equipment Identity (IMEI).

IMEI = TAC + FAC + SNR +spare

- TAC = Type Approval Code by central GSM body
- FAC = Final Assembly Code, identifies the manufacturer
- SNR = Serial Number, unique six digit number
- spare = spare for future use

2.1.1.2 Subscriber Identity Module (SIM)

The SIM provides the user the feature of mobility. It does not matter what is the location of the terminal or to which terminal is the specific user connected to, the user can have access to all the subscriber services because of the SIM card. In order to receive call and make calls and receive all the subscriber services, one has to insert the SIM card in the GSM cell phone.

When a subscriber registers to a network i.e. when a subscriber connects to a terminal, each user and each subscriber gets a unique subscriber IMSI identifier. A Mobile station can only work if a valid SIM card is inserted in it, and that valid SIM card should have a valid IMSI. The three parts of an IMSI number are:

IMSI = MCC + MNC + MSIN

- MCC = Mobile Country Code
- MNC = Mobile Network Code
- MSIN = Mobile Station Identification Number

Encryption is based on the subscriber identity IMSI.

The security features that come with a SIM are:

1. File access conditions
2. Authentication of the user ID to the cellular network
3. Data confidentiality

2.1.2 Access Network

2.1.2.1 Base Station Switching Subsystem (BSS)

The Base Station Subsystem consists of the following

1. Base Transceiver Station (BTS)
2. The Base Station Controller (BSC)

The radio coverage area of a BTS in called a cell. In a cell, BTS provides the user data traffic and the radio channels for signaling.

2.1.2.1.1 Base Transceiver Station (BTS)

In order to establish a contact with the Mobile Stations, a BTS, has equipment specific to the radio interfaces, the equipment includes transceivers and signaling equipment. Transcoder Rate Adapter Unit (TRAU) is an important part of the BTS. TRAU carries out speech encoding/decoding specific to GSM; TRAU also carries out rate adaptation in the process of data transmission. The BTS is responsible for handling the Radio Link Protocols with the Mobile Station and the BTS also has the radio transceivers that define a cell. Large number of BTSs is deployed in a large cosmopolitan area, large city or urban area.

.2.1.2.1.2 Base Station Controller (BSC)

A Base Station Transceiver is responsible for handling of the radio channel allocation. A BSC is also responsible for the handoff management for one or many BTS. A BSC handles the handovers, the radio channel setup and the frequency hopping. Other functions include establishing the connection between a mobile stations i.e. a GSM cell phone and the MSC. The standard voice channel used by the PSTN or ISDN is 64 kbps. The BCS translates the 13 kbps voice channel to 64 kbps.

2.1.3 Core Network

2.1.3.1 Network Switching Subsystem (NSS)

The Network Subsystem consists of the Mobile services Switching Center (MSC), the Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR) and Authentication Center (AuC). The NSS supports the switching functions, subscriber profiles and mobility management.

2.1.3.1.1 MSC

MSC is responsible for connecting the mobile to the landline side i.e. PSTN. GSM MSC is commonly designed as a regular ISDN switch with some added functionality for

mobility support. GSM Network can have more than one MSC. One of the MSC has an added functionality for communication with public network – Gateway MSC (GMSC). All calls from the "outside networks" are routed through GMSC

2.1.3.1.2 HLR

GSM provides two capabilities, call routing and roaming ability. HLR is responsible for these to features of a GSM network. All the administrative info and the location of the mobile station (current location of the GSM phone), in the particular GSM is contained in the HLR databases. There is one HLR in one GSM network. One HLR in one GSM network can be implemented as a distributed database. All the permanent data of the subscribers and all the relevant temporary data of the subscribers of a specific GSM network (that are the permanently registered users in the network) is stored in the one HLR of the one GSM network.

2.1.3.1.3 VLR

In the serving area of a GSM network, the necessary information for the call control and the provision of the subscriber services are contained in the VLR. This is the selective administrative information given by the HLR to the VLR. Majority of the manufacturers' of switching equipment implement only one VLR with one MSC, although it is a known fact that each entity can be implemented as one independent unit. So that one geographical area controlled by the VLR is actually a geographical area controlled by one MSC.

2.1.3.1.4 EIR

As it is known that each MS is known/ identified by its IMEI. A list of all the authorized/lawful ME on a network is contained in a database known as the "Equipment Identity Register (EIR)". The function of the EIR is the same as that of AuC, which is, authentication and security.

2.1.3.1.5 AUC

A secret key is stored in each and every subscriber/user's SIM card. A database contains all the copies of the secret keys of each and every subscriber registered on that particular network. This data base is called the "Authentication Center" or AuC. The secret key is

very important as it is used in the authentication and in the ciphering of the radio channels.

2.2 Operations and maintenance center (OMC)

The OMC is connected to all equipment responsible for switching and to the BSC. The implementation of OMC is called the operation and support system (OSS).

Here are some of the OMC functions:

1. Administration and commercial operation (subscription, end terminals, charging and statistics)
2. Security Management
3. Network configuration, Operation and Performance Management
4. Maintenance Tasks

2.3 Problem with GSM security

Wireless networks have become an important mean of transmitting important information. Hence users are likely to put significant and personal information over the wireless channels. Just like other media, security of wireless channel is also critical. It cannot be considered truly secure. Such security weaknesses may arise as a result of incompatible security scheme or design flaws in protocols. The greatest danger is that user may perceive wireless channel as truly secure and may convey important and confidential information using that channel. The wireless setting poses many security issues, such as privacy, authentication, integrity, authorization, non-repudiation and accessibility. The problems with GSM security are as follows:

- One way authentication: BTS authenticates the MS while MS doesn't authenticate the BTS
- Does not address active attacks
- Only as secure as the fixed networks to which they connect
- Terminal identity cannot be trusted

2.4 Conventional Jammers

A mobile phone jammer is an instrument used to prevent cellular phones from receiving signals from or transmitting signals to base stations. When used, the jammer renders cell phone capability of receiving and transmitting signals.

Principle of Jamming

Jammers work by sending out radio waves on the same frequencies that cellular phones use. This phenomena cause such high interference that disable the cell phones and leaves it unusable.

Drawbacks

On most phones, the network would simply appear out of range. Different bands are used to send and receive communications from towers. Thus jammers can work by either uplink or downlink communication. In addition high power interference signal is generated with lesser effective range. Jammers can have coverage of 300-500 meters within which their operation is effective and loses efficiency when the device goes out of range of jammers.

2.5 Active Attacks on a GSM network

2.5.1 Types of Attack

The attacks on GSM networks can be divided into four types:

The attacks on GSM networks can be divided into four types:

1. **Eavesdropping.** It is the type of an active attack in which user eavesdrop the signaling and data connectivity between the users.

2. **Impersonation of a user.** This is when intruder sends signaling and/or user data to the network in order to make the network believe that it has been generated by target user.

3. **Impersonation of the network.** The intruder sends signaling and/or user data to the target user, in an attempt to make the target user believe that data has been generated from a genuine network.

4. **Man-in-the-middle.** The intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signaling and user data messages exchanged between the two users.

2.6 Denial of Service (DOS)

Denial of Service may take different forms among which one form is to disable the network not to communicate messages; such that affecting it to an extent that it would not let any message to be transmitted to the legitimate users and another form may to affect the network in a way that it starts sending such messages which it should not be sending under normal operation. One apparent cause of DOS attack is affecting the initial communication during authentication process. The network cannot distinguish valid traffic from the fake one and there is not much that can be done as a preventive measure.

2.7 Man in the Middle and Impersonation of the network

Our UG project also focus two active attacks namely Impersonation of network and Man-in-the Middle. Equipment to set up a BTS environment is necessary. Such an environment would essentially be a fake one but users would have no idea of its existence. A fake BTS system is equipment located in a restricted area; functions and broadcast BTS signal over the air interface and enforce the mobile phones in this area to communicate with it. One-way authentication mechanism of 2G cellular communication just authenticates the identities of mobile users and do not validate the BTS to MS. Due to this feature the phone will not be able to distinguish the fake one from the legal one.

The first attack to be carried is IMSI catch attack followed by selective jamming attack. IMSI catch attack will get the mobile phone's IMSI. After getting the IMSI of the mobile

phone, it can be decided whether to dump the user's call/SMS or give access to the numbers registered and authorized in the database.

The attacker could also impersonate as a network by initiating the communication. As the base stations do not authenticate themselves to the MSs, attacker can operate in the vicinity of victim. The attacker needs to make sure that the BTS communicates on a beacon frequency of the victim's provider, and that the fake BTS transmits the MCC and MNC of the same provider.

3 DETAILED DESIGN AND DEVELOPMENT

3.1 Design summary

USRP based fake BTS operational in GSM 900 band was established with the installation and configuration of essential software packages including GNU Radio, Open BTS and Asterisk. Transmission of signal, reception was performed with USRP RF front end while the signal processing of the transmitted and received signal was performed with the USRP IF section. Waveform was fully generated with software algorithm.

In USRP, the processing power which is essential for signal processing is sourced out to a PC. The OpenBTS software uses the USRP hardware to receive and transmit the GSM signaling. This is done by using the GNU Radio framework. The Asterisk is used to interface the GSM calls between the cellular phones under the OpenBTS network.

3.2 Design Requirements and Technical Specifications

Following are the software and hardware requirements for the project.

3.2.1 Software

Software	Specification
Ubuntu	Version 10.04, 12.04
GNU Radio	Version 3.4.1, 3.4.2
OpenBTS	Version 2.8
Asterisk	Versions supported by OpenBTS
Libraries of GNU Radio and OpenBTS	Versions supported by OpenBTS

Table 3-1: Software used along with specifications

3.2.2 Hardware

For a BTS establishment the hardware requirements are:

1) Computer with operating system Ubuntu
2) USRP 1
3) RFX900/ RFX1800 daughterboard (as a Transceiver)

We are using RFX 900.

4) VERT900 antenna covering GSM frequencies
5) SIM card
6) GSM handset
7) 52MHz clock to be soldered with USRP hardware
8) 32 Mbps USB connection between USRP and computer

3.3 GNU Radio

GNU Radio is a free software toolkit licensed under the General Public License (GPL) for implementing Software Defined Radios. It provides signal processing blocks to be used with hardware. It works with several different types of RF hardware, but the most common is with integrating with USRP. GNU Radio is a library containing lots of standard signal processing functions. These functions are called blocks. These blocks are divided into:

- Source blocks
- Sink blocks
- Processing blocks

At low level the blocks of GNU radio are written in C++, while higher level blocks and GNU Radio graphs are written in Python. Actual computations are done in C++ and for higher level more user friendly language is used.

GNU Radio does not offer much of GSM sniffing capabilities, but it can be used to locate the beacon frequencies of GSM; However when used with OpenBTS; it performs the low level functions of GSM sniffing, reception and demodulation.

3.4 OpenBTS

OpenBTS is an open-source Unix application that uses a software defined radio (SDR) to present a GSM air interface to standard GSM handset and uses Asterisk to connect calls.
It is an innovative kind of technology that provides a cost effective solution offering compatibility with most of the handsets that are already in the market. This technology can also be implemented in private network applications at much lower cost and complexity than conventional GSM.
It can be deployed and operated at substantially at lower cost than existing technologies which includes rural cellular deployments and private cellular networks in remote areas.

OpenBTS is distributed in two forms:

1. **The commercial ("C") release:** The commercial release is installed in Range Networks products. Range Networks also offers a portal for commercial customers where source code is available for the GPL components of the OpenBTS installation. The "C" release is intended for

    - Cellular service in industrial, government or commercial applications
    - Intellectual property policies or business models which require commercial support, network monitoring or other professional services

2. **The public ("P") release:** The public release is a subset of the commercial release envisioned for experimentation, education, evaluation and proof-of-concept projects.

3.5 Software Defined Radios (SDRs)

Over the last decade as semiconductor technology has improved both in terms of performance, capability and cost, new radio technologies have emerged from military and research and development labs and captured the main stream of innovation. One of these technologies is software defined radio.

Software defined radio is: Radio in which the physical layer functions are software defined. SDR is a radio communication technology that is built on software defined wireless communication protocols instead of hardwired implementations. Instead of complete hardware replacement; Frequency band, air interface protocol and functionality can be upgraded with just software download and updates.

SDR Application

Through the last two decades of open source developing, the SDR has about several hundreds of applications such as Cognitive Radio, RF-ID and OpenBTS which is our project subject and will be discussed in detail.

3.6 USRP1

USRP does all of the waveform specific processing on the host CPU like Modulation and Demodulation. All of the high speed general purpose operations are done on the FPGA like

1. Digital Up Conversion (DUC)
2. Digital Down Conversion (DDC)
3. Decimation

Version	USRP1
Manufacturer	Ettus Research
ADC	64 MS/s 12-bit
DAC	128 MS/s 14-bit
Max. BW	16 MHz
PC connection	USB 2.0 (32 MB/s half duplex)
RF range	DC – 5.9 GHz, defined trough RF daughter boards
Daughter boards	RFX-900 and RFX-1800

Table 3-2: USRP specifications

The USRP is made up of the motherboard which has USB 2.0 interface for connection to the computer, power connector and, a FPGA section for high speed signal processing, and interchangeable daughter boards that cover different frequency ranges.

In addition to ADC, DAC and antennas; the motherboard provides the following subsystems:

1. FPGA
2. Host Processing interface
3. Power regulation, clock generation and synchronization

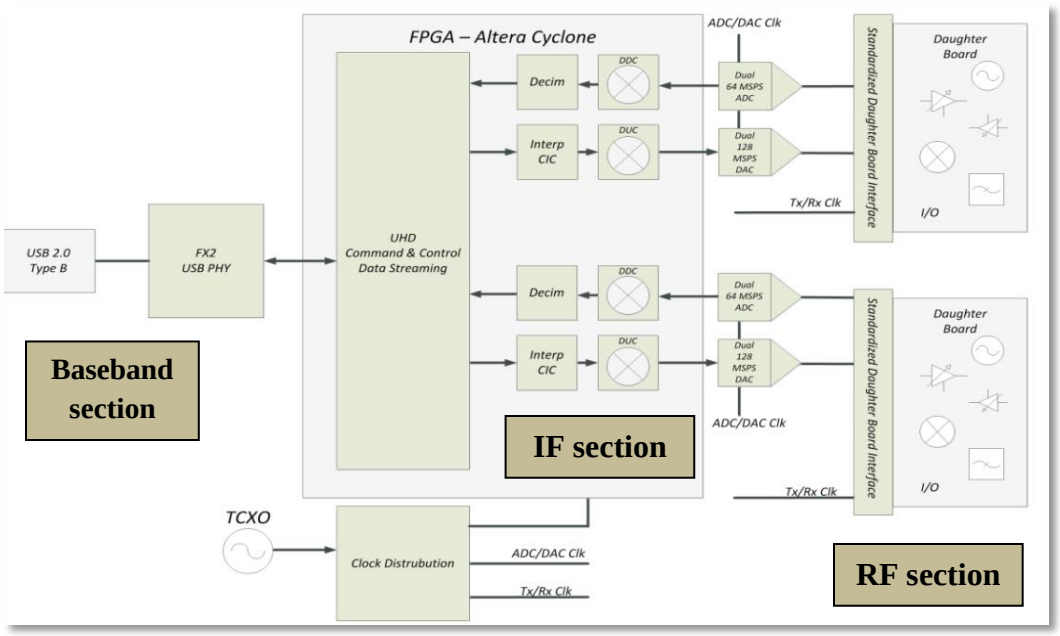

Figure 3-1: USRP schematics

3.6.1 VERT 900 antenna

Figure 3-2: VERT 900 antenna

Quad-band Cellular/PCS and ISM Band Vertical Antenna

Frequency of operation: 824-960 MHz, 1710-1990 MHz

Gain: 3dBi Gain

Height: 9 Inches

Ideal for RFX900 and RFX1800

3.6.2 RFX 900 daughter cards

For GSM 850/900

Frequency: 800-1000MHz Transceiver

Power output: 200 mW output

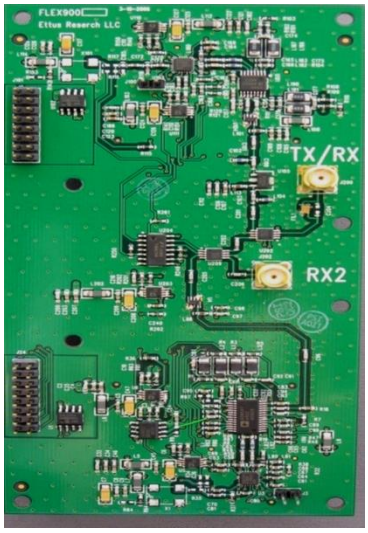

Figure 3-3: RFX 900 daughter cards

3.7 Project Development

Complete project development including software and hardware portions is described in this section.

3.7.1 Installation and compilation of GNU Radio

Installing GNU Radio on any recent Ubuntu is easy and requires the following steps:

1. Install the pre-requisites
2. Get the GNU Radio source code
3. Configure, compile and install GNU Radio
4. Configure USRP

Complete codes of installation of GNU Radio with results are described in Appendix A.

3.7.2 Open BTS Installation

3.7.2.1 Building OpenBTS

OpenBTS should be build and run on any Unix 64 bit operating system. However most of development is done on Ubuntu 10.04 or 12.04 LTS systems, so these are best-supported.

3.7.2.2 Ettus USRP1

The USRP1 has been deprecated by Ettus, making this install more difficult. To run OpenBTS using the USRP1, installation of GNU Radio is needed which has already been done. As per instructions installing something after 3.3.0 but before 3.5.0 is

recommended, so 3.4.1 was installed (where they removed USRP1 support). With that already installed. Single daughterboard configurations were set up. With the build resolved, linking of the transceiver appropriate for Ettus USRP 1 hardware was needed.

3.7.2.3 Database

OpenBTS.db is the database store for all OpenBTS configuration. It must be installed at /etc/OpenBTS, which does not preexist. Some other databases are also required to be built in same /etc/OpenBTS directory. These databases are Smqueue for sending, receiving messages and subscriber registry for providing authentication.

3.7.2.4 Running OpenBTS

In the above mentioned steps, we made all the databases and configurations of OpenBTS which were required to establish a fake base station to hook mobile phones.
Complete codes of installing OpenBTS are described in Appendix B.

3.8 Design Modifications

3.8.1 Transceiver Error

For OpenBTS configuration and proper working; transceiver cards of GSM(900MHz in our case) are required to operate. These transceiver cards work with OpenBTS configuration on 52MHz clock frequency for better synchronization with GSM. As the default clock embedded on USRP is synchronized with 64MHz frequency, we encountered following error in our setup:

```
ALERT 47613775102208 TRXManager.cpp:408:powerOn: POWERON failed
with

status -1

transceiver: no process killed

linux; GNU C++ version 4.1.2 20080704 (Red Hat 4.1.2-52);

Boost_104100;

UHD_003.
```

```
004.000-93a49d0



ALERT 47832442212256 UHDDevice.cpp:469:open: UHD make failed,
device

type=umtrx,

addr=192.168.1.10,name=UmTRX,serial=13

ALERT 47832442212256 runTransceiver.cpp:95:main: Transceiver

exiting...


EMERG 1104513344 OpenBTS.cpp:134:startTransceiver: Transceiver
quit

with status

Exiting.
```

Reason

Unfortunately, the internal clock of the USRP devices is too imprecise to allow reliable operation with cell phones. Additionally, operating the USRP at 64MHz for GSM isn't recommended; instead a multiple of the GSM bit symbol rate to make down-sampling more efficient is used. With the above error, mobile phones were not able to hook to fake BTS.

Discussed below are the two solutions. First solution didn't work while the second solution, which is universally, accepted works in all cases. Following is the modification performed with the hardware to enable successful completion.

3.8.2 Hardware Changes

The first solution was to down sample the rate and to perform code modification. This didn't provide desired result instead it crashed the system. The solution available was either to get OpenBTS development kit from Range Networks or to work with USRP B100 and WBX daughter cards. They both have built-in 52MHz clock with better stability but the cost was very high.

The alternate solution was to replace 64MHz clock of existing USRP1 with a 52MHz clock. For that purpose, 52MHz clock from China was imported with the help of our project supervisor. Complete specifications of imported clock are given below:

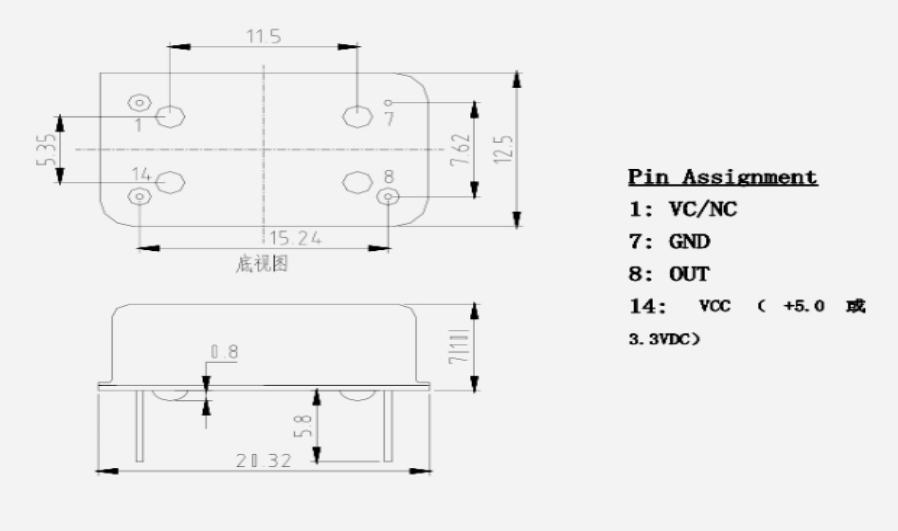

Figure 3-4: Pin configuration of 52MHz clock

Soldering requirements

1) Moved R2029 to R2030T. R2029/R2030 is a 0-ohmresistor.
2) Moved C925 to C926
3) Removed C924

The above steps disabled the on-board clock of USRP. After that new clock was installed with the following steps:

1) Glued the 52MHz Crystal Oscillator on the USRP main board.
2) Soldered the wire (Vcc) and connected it to the 3.3V power source.
3) Soldered the second wire (ground) and connected it to the ground point.
4) Soldered the third wire (52MHz) and connected it with the C927.

All the steps for soldering were done as per specifications provided in official group of OpenBTS from Range Networks.

The modified USRP with new clock is shown in figure below:

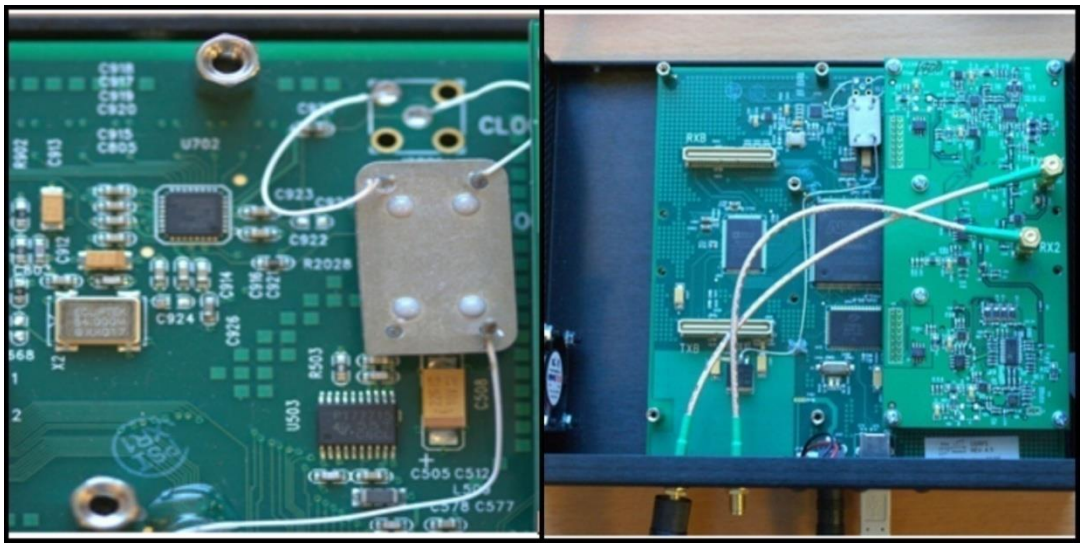

Figure 3-5: Hardware modification to USRP motherboard

3.8.3 Software Changes with new clock

After new clock soldered with USRP, software changes were required to enable and configure it with transceiver cards plus the rest of the USRP circuit .After software patch applied, GNU Radio was rebuild and OpenBTS transceiver paths were modified in configuration table.

With the above steps completed, there were no more errors in OpenBTS and mobile phone was able to receive signals from our OpenBTS. Codes are described in Appendix C.

3.9 Configuring OpenBTS variables

With OpenBTS working, OpenBTS Command Line interface (CLI) was configured according to the requirements. These variables were assigned value with the help of config command. Variables are listed below with their configuration value:

```
Control.LUR.OpenRegistration .*

Contro.LUR.OpenRegistration.ShortCode 101

GSM.Identity.MCC 101 (for Test Network)
```

```
GSM.Identity.MNC 01 (for test operator)

GSM.Identity.ShortName DOS

GSM.Radio.Band 900

GSM.Radio.C0 51
```

3.10 Enhanced feature in DOS

Completion of required DOS attack before time, some extra functionality was added to the project which aided to make the DOS selective in its attack.

The main objective of this denial of service is to deny all communication for common people and allow communication among pre authorized legitimate users. This feature adds a very unique functionality of selective jamming to the project. Asterisk and Smqueue databases are required to be built and configure with OpenBTS to add this functionality.

3.10.1 Asterisk Configurations

Asterisk is the standard PBX shipped with OpenBTS and is the most documented option for use with OpenBTS. Asterisk version used in our project is 1.8.4 that is most compatible with OpenBTS 2.8 version. For making calls enabled in two different mobile phones, their IMSIs are registered in Asterisk databases. For that purpose, two files of asterisk are required to be modified. These modifications are listed as follows:

Sip.Conf Modification

Sip.Conf is a file in asterisk that defines different parameters of GSM OpenBTS to allow calling between two different MS. After each IMSI entry, there is a list of variables that is defined.

Extensions.Conf Modification

Extensions.Conf defines all the parameters of GSM dial plan and other variables for OpenBTS configuration. It is also responsible for mapping between IMSI and the calling identity of the mobile phone.

Sip.Conf and Extensions.Conf codes modifications are described in Appendix D.

3.10.2 Smqueue Configurations

Smqueue is standard package of OpenBTS used to handle SMS services between mobile phones and among network and mobile phones.

To send SMS from network to mobile phone, IMSI is required that is readily available as a mobile phone gets registered to OpenBTS. But if SMS service between two different mobile phones that are registered to OpenBTS network needs to be enabled, then mobile number must be assigned to IMSI.

This is done by sending an SMS to OpenBTS default network number that is configured as 101. The message must contain the number that is demanded for communication and should not be out of range of Smqueue database, i.e. 4 – 14 digits long.

It is possible to use two different platforms for calling and SMS services as in established system, Asterisk is used to handle calls and Smqueue is used to handle SMS. These both work independently on different ports and do not create any problem for the mobile phone user.

4. ANALYSIS AND EVALUATION

After completing all the software configurations and hardware modifications, system testing required to be done. For that purpose, hardware was integrated with software and verification tests were performed. Results are discussed in detail in this chapter.

4.1 Benchmark Test

The test provides information about the data transfer rate between USRP and computer USB port. The maximum data rate is required to be 32MB/s.

```
Testing 2MB/sec... usb_throughput = 2M

ntotal    = 1000000

nright    = 998435

runlength = 998435

delta     = 1565

OK



Testing 4MB/sec... usb_throughput = 4M

ntotal    = 2000000

nright    = 1998041

runlength = 1998041

delta     = 1959

OK

Testing 8MB/sec... usb_throughput = 8M

ntotal    = 4000000
```

```
nright    = 3999272

runlength = 3999272

delta     = 728

OK



Testing 16MB/sec... usb_throughput = 16M

ntotal    = 8000000

nright    = 7992153

runlength = 7992153

delta     = 7847

OK



Testing 32MB/sec... usb_throughput = 32M

ntotal    = 16000000

nright    = 15986239

runlength = 15986239

delta     = 13761

OK

Max USB/USRP throughput = 32MB/sec
```

The result shows that required data rate was achieved.

4.2 GSM signal strength measuring

The test is to measure GSM signal strength with USRP. In this test USRP acts as a receiver of GSM signal or as small spectrum analyzer to measure the signal strength in desired area.

```
cd /usr/local/share/gnuradio/examples/usrp

./usrp_wfm_rcv_pll.py
```

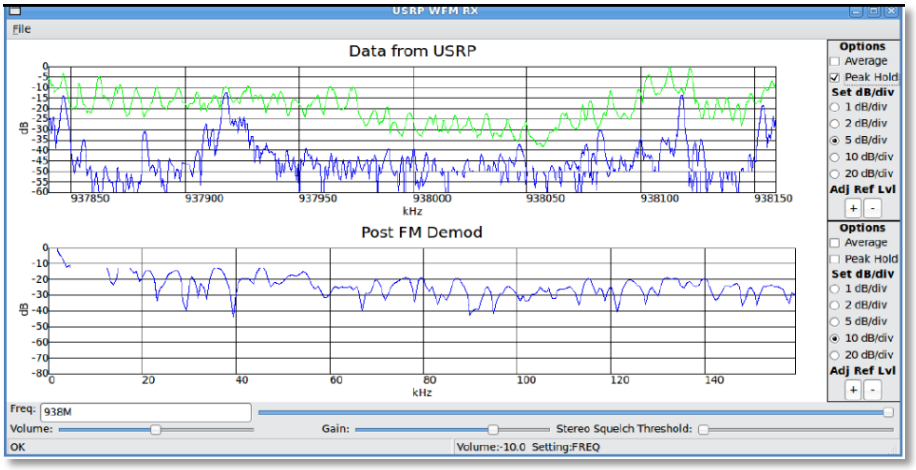

Figure4-1: GSM signal strength measure at 938MHz

4.3 OpenBTS Results

After soldering 52MHz clock with USRP and applying software modifications, variables of OpenBTS were configured. The setup was worked properly and this was the first time that mobile phones in the vicinity detected the established network.

Figure 4-2: Project setup

4.4 DOS to 'WARID' network

The configurations to hack operator are under this section. For hacking any operator, the first thing is to get MNC and MCC of operators. This list was available on Wikipedia and is shown below.

MCC	MNC	Brand	Operator	Status	Bands (MHz)
410	01	Mobilink	Mobilink-PMCL	Operational	GSM 900 / GSM 1800 /GSM 1900 / GSM 2100 /UMTS 2100
410	03	Ufone	Pakistan Telecommunication Mobile Ltd	Operational	GSM 900/ GSM 1800
410	04	Zong	China Mobile	Operational	GSM 900 / GSM 1800
410	06	Telenor	Telenor Pakistan	Operational	GSM 900 / GSM 1800
410	07	Warid	WaridTel	Operational	GSM 900 / GSM 1800

Table 4-1: MCC and MNC of cellular operators of Pakistan[1]

[1] *MNC & MCC allocated in Pakistan, Wikipedia, Internet:* http://en.wikipedia.org/wiki/Mobile_country_code

The next step was to assign channel numbers that lie in range of operators' band. For this purpose a list of operator's frequency allocation from FAB's website was taken and converted to ARFCNs. Due to legal restriction it cannot be mentioned here in detail.

With all the above data and configuration variables available DOS was established, results of successful DOS to Warid network are shown in figure 4-3.

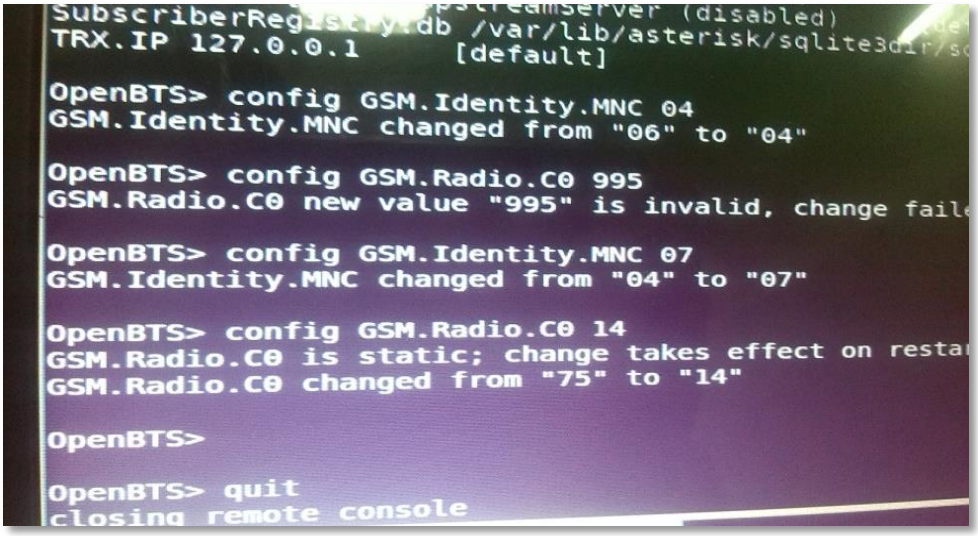

Figure 4-3: Configuration to hack WARID

After changing variables to new values, mobile phone with Warid SIM should automatically connect to fake BTS and BTS should be pretending to be a base station of Warid. Mobile phone connected to fake BTS of Warid was then under Denial of Service attack and the calls and SMS were denied by the BTS. Further mobile was then under control of BTS, any message can be sent to detect IMSI. As an example a message generated from BTS is shown in figure 4-4:

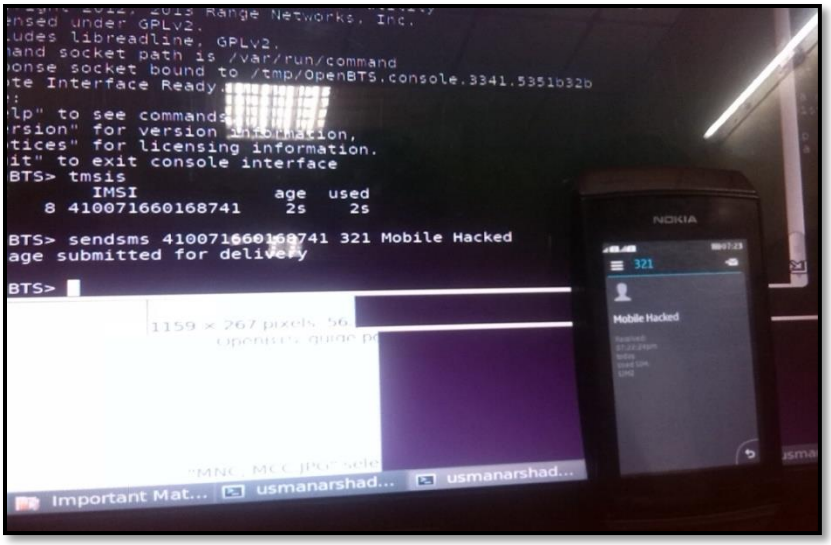

Figure 4-4: SMS sent by Fake BTS appears as originated from the actual operator

4.5 DOS TO 'Ufone' NETWORK

Same steps but with different configuration settings may be applied to attack on Ufone. The result of attack on Ufone are shown in the figures below

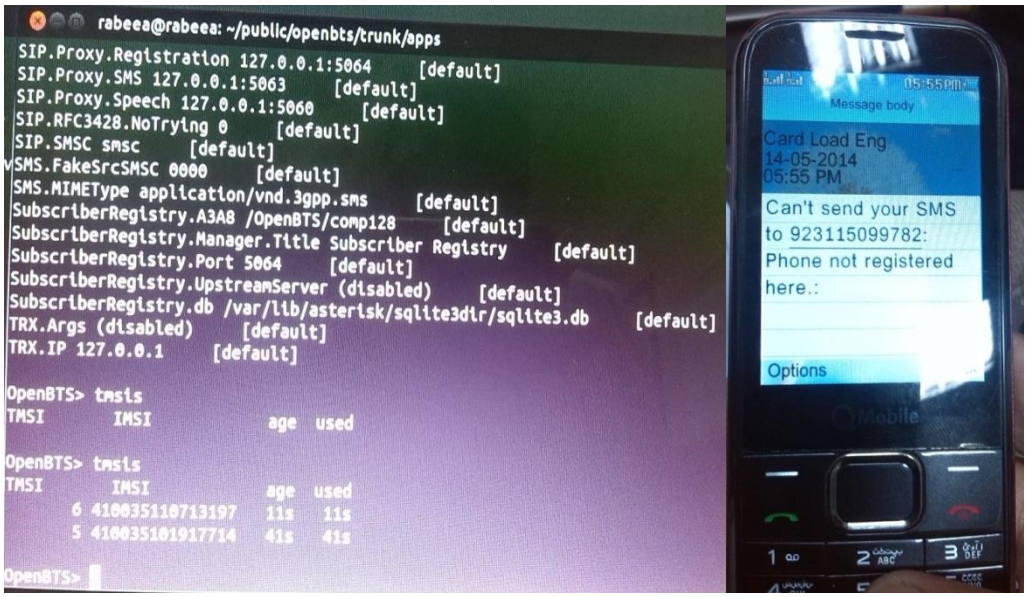

Figure 4-5: Configurations to jack UFONE

Similarly all operators can be attacked but due to the legal restriction, this cannot be performed repeatedly. It is recommended to establish a test network with following configuration parameters:

MCC	MNC	Brand	Operator	Status	Bands (MHz)	References and notes
001	01	TEST	Test Network	Operational	GSM 900 / GSM 1800	Used by GSM test equipment

Table 4-2: Configurations for Test network[2]

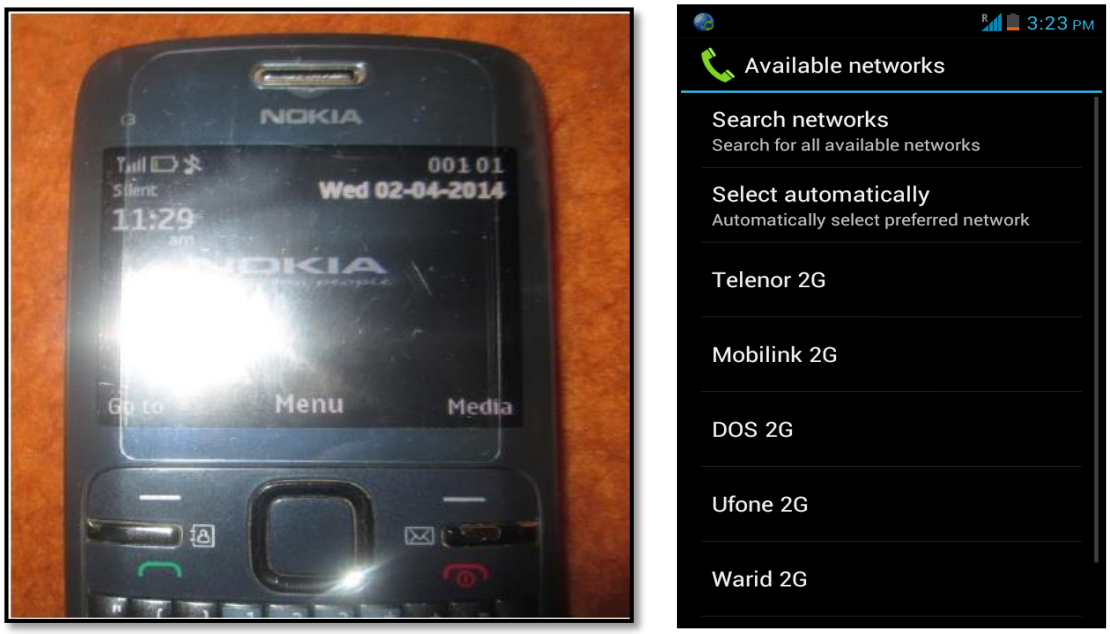

Figure 4-6: a) Mobile hooked to the test network b) phone showing DOS2G as a test network in the available networks

USRP based BTS can hook more than one user at a time. Figure below shows six users connected to Fake BTS but still more connections are possible as it has been tested with more than 40 users hooked to the BTS.

[2] *http://en.wikipedia.org/wiki/Mobile_country_code*

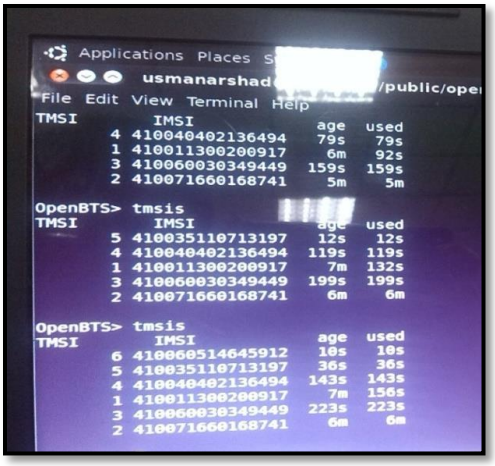

Figure 4-7 : Six phones hooked to Fake BTS

A message is generated by default by our fake BTS to welcome a subscriber to our network and tell him his/her IMSI number as shown in figure below. But if subscriber does not need to be informed whether he/she is connected to his fake BTS or not, it can be disabled.

As the mobile phone gets connected to BTS providing the IMSI number of SIM, those IMSIs can be registered in the database of fake BTS and any number (Caller ID) can be assigned. As a reference, shown in the figure4-8 a mobile phone is registered to fake BTS. The phone was assigned a caller ID as 12345.

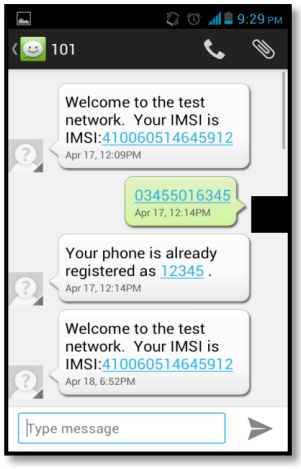

Figure 4-8 Welcome message by Fake BTS and mobile registered with ID 12345

Now as per the requirement of project, Denial of Service can be implemented to the subscriber that is hooked to the fake BTS. The need was to dump the calls and SMS of hooked subscribers. The idea implemented behind is to not allocate the channel to user for call or SMS. As the subscriber tries to generate calls or SMS, they were denied and a denial message is sent to the subscriber. This message can be disabled such that it won't let the subscriber know about the scenario. The figure4-9 below is showing practical denial of service possible on three different mobile phones.

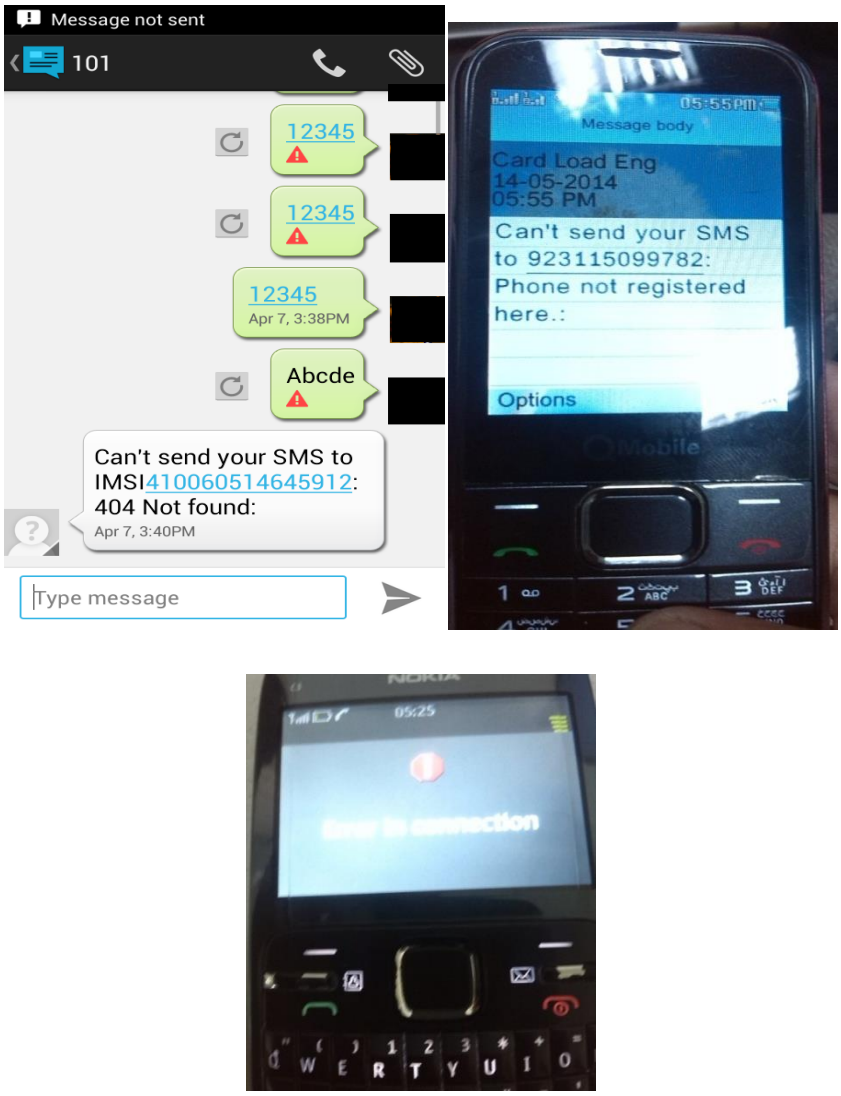

Figure 4-9: DOS to a network successfully accomplished

5. FUTURE WORK, SUMMARY AND CONCLUSION

We have carried out a practical DOS on a GSM network and only one service provider has been targeted at a time. There can be two perspectives of future work that can be done.

1. *Improvement Denial of Service (DOS) attack*
   a. Improvement in the practical Denial of service (DOS) attack to handle more than one operator at a time.

   The above denial of service attack may be made possible but only with intentions of improving security or betterment of the networks since it is a highly illegal task and hacking should be in within ethical limits.

   b. Improvement of DOS attack by increasing the range of prototype.

   This will enable people to test DOS attack on more number of users and handling of more traffic over a wider area. But again it should be done within ethical limits.

2. *An algorithm can be developed to prevent DOS attacks on GSM network.*

   As we've made practical denial of service attack possible on GSM network. It reveals many security flaws in GSM architecture. There can be a nice effort to improve security checks of GSM network to produce a more secure algorithm.

5.1 Project summary

A working USRP based prototype replicating the functionality of GSM BTS has been established which aims at denying service to the users of target area without dropping the signal strength.

BTS has been set to OPEN registration mode. Fake BTS operated in the Telco frequency band will be able to catch the IMSI of the terrorist as well as the users of the vicinity. With this fake BTS; the operator of the prototype can deceive the terrorist that he is able to receive the GSM service (Since the signal strength won't fade away) and that he might plan his activity. In an effort to trigger the IED, the call and SMS of the terrorist will be dumped. In this way, he won't be able to understand the situations and the killings can be avoided.

Objectives achieved

1. Software setup successfully accomplished
2. Hardware modification done

   52 MHz external clock has been soldered on the USRP motherhood
3. Working USRP BTS established

Successful DOS attack has been carried out on Pakistan's Telecom operator names "Warid". This was done configuring the OpenBTS parameters as under

Operator	Network code	ARFCN	Mobile code
Warid	07	14	0321

4. IMSI "**410071660168741**" caught up during the test run

   MCC: 410
   MNC: 07

Calls and SMS originated from the above mentioned IMSI were dumped. As a proof to check whether MS is hooked to fake BTS or not; SMS "Mobile hacked" was sent to following IMSI which was successfully received as originated from the actual operator.

Prototype range:approx 20 meters (when implemented on a GSM cell the range can increase to several kilometers roughly 30km)

Prototype power output: 200mW

5.1 Selective Jamming Feature

Allowing communication to the authorized subscriber and denying it to all others

One drawback of jammers is that all the communication of the targeted frequency falling in the range will be disabled. However with our prototype the law enforcement personnel will be able to communicate with each other. IMSI of trusted users will be registered in the database and allowed communication through our prototype. This feature will enable the law enforcement agencies to have a secure communication between each other while denying the services to the other unregistered user.

This is the enhanced feature implemented makes the device user friendly and more promising.

5.2 Limitations and Applications

Legal restrictions

Due to the legal restrictions, the above mentioned DOS attack cannot be performed openly so for test purpose we have established a test network and performed the DOS attack.

Applications

The project has a practical approach towards the security lapse occur during day to day activities. In military and paramilitary zones of the country, it is our top-most priority to make our networks inaccessible protecting the integrity and Confidentiality, while insuring complete and utmost access control.

- For VIP's protection in the national assembly and the provincial parliaments this device will prove to be very useful

- Threats of terrorist attacks will be minimized in the vicinity and operating range of our device and the GSM networks operating in our range will be monitored
- In highly sensitive governmental zones like the diplomatic enclave in Islamabad this device will be of utmost use
- For VIP's protection in the national assembly and the provincial parliaments this device will prove to be very useful
- In important gathering and meetings GSM networks will be monitored to safe people from internal and external threats
- All the IEDs will be disabled completely

BIBLIOGRAPHY

Previous work done:

Lt Col Dr Adnan Rashidi's syndicate made a fake BTS for monitoring the GSM calls in 2012 with a capability of intrusion as well. [3]

- *A National Instrument Company, "ETTUS RESEAR4CH official website", Internet:* http://home.ettus.com/about
- *Song, Yubo, "Fake BTS Attacks of GSM System on Software Radio Platform", School of Information Science and Engineering, Southeast University, Nanjing, China2, FEBRUARY 2012*
- *BOCAN, Valer , "Security and Denial of Service Threats in GSM Networks", Department of Computer Science and Engineering, Politehnica University of Timi7oara, 2004*
- *Fähnle, Matthias, "Software-Defined Radio with GNU Radio and USRP/2 Hardware Frontend: Setup and FM/GSM Applications", 2009-2010*

- *Mohammed, Hassan Ali, and Hussein Ali, Hussein Magdy and Mohammed, Mohammed Sabry Amin, Mohammed Mahmoud Abbas, "OpenBTS –Network Design & System Analysis", Faculty of Engineering, Cairo University, 2012*

- *Apvrille, Axelle, "OpenBTS for dummies", January 10, 2013*
- *MNC & MCC allocated in Pakistan, Wikipedia, Internet:* http://en.wikipedia.org/wiki/Mobile_country_code
- *Frequency Allocation Board of Pakistan, Internet:* http://www.fab.gov.pk/article/pakistan-table-of-frequency-allocation.html
- *GNU radio organization, "GNU radio official website",* http://gnuradio.org/redmine/projects/gnuradio/wiki/UbuntuInstall#Install-Dependencies

[3] *Khawaja, Ahtisham, "GSM interceptor", Military College of Signals, 2011-2012*

Appendix A

GNU Radio Installation

Installation of GNU Radio is described in step wise approach.

1. **Installing Pre requisite Libraries:**

```
sudo apt-get -y install git-core autoconfautomakelibtool g++ python-dev swig \ pkg-config libboost1.48-all-dev libfftw3-dev libcppunit-dev libgsl0-dev \ libusb-devsdcc libsdl1.2-dev python-wxgtk2.8 python-numpy \ python-cheetah python-lxmldoxygen python-qt4 python-qwt5-qt4 libxi-dev \ libqt4-opengl-dev libqwt5-qt4-dev libfontconfig1-dev libxrender-dev
```

2. **Building GNURadio:**

```
git clone http://gnuradio.org/git/gnuradio.git
```

```
cdgnuradio
mkdir build
cd build
cmake ../
make
make test
sudo make install
```

3. **Enabling USRP support with GNURadio:**

```
sudoaddgroupusrp

sudousermod -G usrp -a <YOUR_USERNAME>
```

```
echo 'ACTION=="add", BUS=="usb",
SYSFS{idVendor}=="fffe", SYSFS{idProduct}=="0002",
GROUP:="usrp", MODE:="0660"' >tmpfile

sudochownroot.roottmpfile

sudo mv tmpfile /etc/udev/rules.d/10-usrp.rules
```

```
sudoudevadm control --reload-rules

ls -lR /dev/bus/usb | grepusrp

cdgnuradio-examples/python/usrp

./usrp_benchmark_usb.py
```

```
cdusrp/host/apps

./test_usrp_standard_tx

./test_usrp_standard_rx
```

Appendix B

Installation of OpenBTS

```
sudo apt-get install autoconflibtool libosip2-dev
libortp-dev libusb-1.0-0-dev g++ sqlite3 libsqlite3-dev
erlang libreadline6-dev libncurses5-dev

cd a53/trunk

sudo make install

cdopenbts/trunk

autoreconf -i

./configure --with-usrp1

make

cdopenbts/trunk

autoreconf -i

./configure --with-usrp1 --with-singledb

make
```

```
#(from OpenBTS root)

cd apps

ln -s ../Transceiver52M/transceiver .


#and for the USRP1, install std_inband.rbf

sudomkdir -p /usr/local/share/usrp/rev4/

sudocp ../Transceiver52M/std_inband.rbf
/usr/local/share/usrp/rev4/

sudomkdir /etc/OpenBTS
```

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

sqlite3 /etc/OpenBTS/OpenBTS.db .dump

sudomkdir -p /var/lib/asterisk/sqlite3dir

(fromsvn root)

cdsubscriberRegistry/trunk

make

(fromsubscriberRegistry root)

sudo sqlite3 -initsubscriberRegistry.example.sql
/etc/OpenBTS/sipauthserve.db ".quit"

(fromsubscriberRegistry root)

sudo ./sipauthserve

autoreconf -i

./configure

make

(from the smqueue directory)

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

(from the smqueue directory)

cdsmqueue

sudo ./smqueue

smqueue/trunk/smqueue/smqueue

subscriberRegistry/trunk/sipauthserve

openbts/trunk/apps/OpenBTS

openbts/trunk/apps/OpenBTSCLI
```

Appendix C

Software modifications with External clock:

```
diff --git a/usrp/host/lib/usrp_basic.cc
b/usrp/host/lib/usrp_basic.cc

index 5b2f7ff..8f50ff2 100644

--- a/usrp/host/lib/usrp_basic.cc

+++ b/usrp/host/lib/usrp_basic.cc

@@ -107,7 +107,7 @@ usrp_basic::usrp_basic
(intwhich_board,

   : d_udh (0), d_ctx (0),

d_usb_data_rate (16000000),        // SWAG, see below

d_bytes_per_poll ((int) (POLLING_INTERVAL *
d_usb_data_rate)),

-    d_verbose (false),
d_fpga_master_clock_freq(64000000), d_db(2)

+    d_verbose (false),
d_fpga_master_clock_freq(52000000), d_db(2)

 {

   /*

    * SWAG: Scientific Wild Ass Guess.

modifyOpenBTS.config (or whatever config file you are
using) so that TRX.Path points to
"../Transceiver52M/transceiver".
```

Appendix D

1. Sip.Conf file modification

```
[IMSIXXXXXXXXXXXXXXX]

callerid=-------------

canreinvite=no

type=friend

allow=gsm

context=sip-external

host=dynamic

dtmfmode=info


[IMSIXXXXXXXXXXXXXXX]

Callerid=--------------

canreinvite=no

type=friend

allow=gsm

context=sip-external

host=dynamic

dtmfmode=info

[IMSIXXXXXXXXXXXXXXX]

Callerid=--------------

canreinvite=no

type=friend

allow=gsm

context=sip-external
```

```
host=dynamic

dtmfmode=info
```

2. Extensions.Conf file Modification

```
[macro-dialGSM]

exten => s,1,Dial(SIP/${ARG1},20)

exten => s,2,Goto(s-${DIALSTATUS},1)

exten => s-CANCEL,1,Hangup

exten => s-NOANSWER,1,Hangup

exten => s-BUSY,1,Busy(30)

exten => s-CONGESTION,1,Congestion(30)

exten => s-CHANUNAVAIL,1,playback(ss-noservice)

exten => s-CANCEL,1,Hangup



[sip-external]

exten => --------
,1,Macro(dialGSM,IMSIXXXXXXXXXXXXXXX@127.0.0.1:5062)

exten => --------
,1,Macro(dialGSM,IMSIXXXXXXXXXXXXXXX@127.0.0.1:5062)
```