CELLPHONE JAMMER CIRCUIT

A thesis submitted in partial fulfilment of the requirements for the degree of
B.Sc. (HONS) in Electrical and Electronics Engineering
(ELECTRONICS AND COMPUTER ENGINEERING)

BY

MOHAMED OMER HASSAN SAEED

INDEX 124084

Supervisor
Prof. Sharief Fadul Babiker

TO

Department of Electrical and Electronics Engineering
Faculty of Engineering
University of Khartoum
October 2017
DECLARATION OF ORIGINALITY

I declare that this report entitled “Cellphone Jammer Circuit” is my own work except as cited in the references. This report had not been accepted for any degree and was not being submitted concurrently in candidature for any degree or another award.

Name: .................................................................................................
Signature: ..............................................................................................

Date: / / 2017
ACKNOWLEDGEMENTS

I would first like to thank my thesis advisor Prof. Sharief Fadul Babiker of the Faculty of Engineering – Department of Electrical and Electronic Engineering at University of Khartoum. The door to Prof. Babiker office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right the direction whenever he thought I needed it.

I would also like to thank the experts who were involved in the educational process for this research project: Prof. Sami Mohamed Shareef (Communication Engineering), Prof. Mustafa Omer Nawri (Control Engineering), Dr. Iman AbuAlMaali AbdalRahaman (Communication Engineering), Dr. Samah Omer Hashem (Electronics Engineering), Mr. Mohannad Ahmed AlHassan (Electronics Engineering) and Dr. Hiba Hassan Imam (Communication Engineering). Without their passionate participation and input, the thesis could not have been successfully conducted.

I would also like to acknowledge my Family as the first supporters of this thesis, and I am gratefully indebted to them, and without them this work wouldn’t be accomplished this neatly and clearly.
ABSTRACT

This paper presents the design, implementation, and testing of a dual-band mobile-phone jammer. This jammer works at GSM 900 and GSM 1800 simultaneously and thus jams the four well-known carriers’ frequency in Sudan (Zain, Sudani and MTN). This paper went through two stages: Stage one: studying the GSM-system to find the best jamming technique, establishing the system design and selecting suitable components. Stage two: buying all the needed components, drawing the overall schematics, assembling the devices, performing some measurements and finally testing the mobile jammer. The designing stage consists of voltage controlled oscillator, noise generator and Radio Frequency Amplification. MATLAB Simulink was used for the simulation of the frequency oscillator, On Running the simulation, and observing the output of the scope. We can see that the result must be a signal at frequency RF covers the whole downlink. The designed jammer as supposed to be successful in jamming the Sudanese carriers operating on 1G or 2G networks.
المستخلص

يعرض هذا المشروع تصميم وتنفيذ اختبار جهاز مزدوج التردد لتشغيل ترددات الijiتف المحمول. هذا التشويش يعمل على 900 و 1800 في GSM في وقت واحد، وبالتالي توقف عمل تردد ثلاثية نواقل معروفة في السودان (زين، سوداني، وMTN).

مر هذا المشروع من خلال مرحلتين: المرحلة الأولى: دراسة نظام GSM للعثور على أفضل تقنية التشويش، ووضع تصميم النظام واختيار العناصر المناسبة.

المرحلة الثانية: شراء جميع المكونات اللازمة، رسم الخطط الشاملة، وجمع الأجهزة، وأداء بعض القياسات وأخيراً اختبار جهاز تشويش المحمول. مرحلة التصميم: مذبذب مُتحكَّم بالجهد، مولدات الضجيج، ومضخات دوائر الترددات الراديوية. وقد استخدم لمحاكاة مذبذب التردد، في تشغيل المحاكاة، ومراقبة الخرج من النظام. يمكننا أن نرى أن النتيجة بفترض أن تكون إشارة على تردد يغطي دائرة التردد الهابطة كلها، ومن المفترض أن الجهاز نجح في التشويش على شركات الاتصالات السودانية العاملة على شبكات 1G أو 2G.
TABLE OF CONTENTS

DECLARATION OF ORIGINALITY ................................................ II
ACKNOWLEDGEMENTS ................................................................ III
ABSTRACT ................................................................................... IV
المستخلص ................................................................................. V
TABLE OF CONTENTS ................................................................. VI
TABLE OF FIGURES ................................................................. IX
LIST OF TABLES ..................................................................... XI
LIST OF SYMBOLS .................................................................. XII
LIST OF ACRONYMS ............................................................. XIV

Chapter One: Introduction .......................................................... 1
1.1 Overview ............................................................................. 1
1.2 Problem Statement ............................................................ 2
1.3 Background and Motivation ................................................. 3
1.4 Objectives of the Project .................................................... 4
1.5 Project Methodology .......................................................... 4
1.6 Thesis Layout ..................................................................... 5

Chapter Two: Literature Review About Cellphone Jammer Circuit ....... 7
2.1 Overview ............................................................................. 7
2.2 Introduction to GSM/DCS Systems ........................................ 8
2.3 Cellphone Jammer Circuit .................................................... 8
2.4 Jammer Architecture ........................................................... 9
  2.4.1 Voltage Controlled Oscillator ........................................... 9
  2.4.2 Tuning Circuit ................................................................. 9
  2.4.3 Mixer ............................................................................ 9
  2.4.4 Noise Generator ............................................................ 10
  2.4.5 RF Stage ...................................................................... 10
  2.4.6 Power Supply ............................................................... 10
  2.4.7 Antenna ..................................................................... 10

2.5 Jamming Techniques ............................................................ 10
  2.5.1 Strategies ................................................................... 10
  2.5.1.1 Noise Strategy ........................................................ 10
  2.5.1.2 Phase Strategy ........................................................ 10
  2.5.2 Techniques ................................................................. 11
  2.5.2.1 Spoofing ................................................................. 11
  2.5.2.2 Shielding Attacks ..................................................... 11
  2.5.2.3 Denial of Service ...................................................... 11
2.6 Types of Jammers ............................................................... 11
  2.6.1 Elementary Jammers ..................................................... 12
  2.6.1.1 Proactive Jammers ................................................... 12
  2.6.1.1.1 Constant Jammer ................................................ 12
3.1 Introduction .................................................................................................................. 17
3.2 Design Considerations .................................................................................................... 18
3.3 Project Scope .................................................................................................................. 18
3.4 Hardware Phase Design .................................................................................................. 19
  3.4.1 Design Parameters .................................................................................................... 19
  3.4.1.1 Jamming Distance ............................................................................................... 19
  3.4.1.2 Frequency Bands ............................................................................................... 19
  3.4.1.3 Jamming-to-Signal Ratio ................................................................................... 20
  3.4.1.4 Free Space Loss ................................................................................................. 20
  3.4.2 Sweep Generator (Timer Stage) ............................................................................... 21
  3.4.3 IF Stage ..................................................................................................................... 22
  3.4.3.1 Noise Generator ............................................................................................... 23
  3.4.3.2 Amplifier Stage ................................................................................................. 25
  3.4.4 Mixer ....................................................................................................................... 26
  3.4.5 RF Stage ................................................................................................................... 27
  3.4.5.1 Synthesizer (An Example) ............................................................................... 27
  3.4.5.2 RF Mixer ........................................................................................................... 28
  3.4.5.2.1 Power Amplifier ............................................................................................ 29
  3.4.5.2.2 Power Amplifier GSM-900 .......................................................................... 29
  3.4.5.2.3 Power Amplifier DCS-1800 ........................................................................ 30
  3.4.6 Voltage Controlled Oscillators ............................................................................... 30
  3.4.7 Power Supply .......................................................................................................... 31
  3.4.8 Antenna .................................................................................................................... 33
  3.4.8.1 Antenna Types ..................................................................................................... 35
  3.4.8.1.1 Wire Antenna ................................................................................................. 35
  3.4.8.1.2 PCB Antenna ................................................................................................. 36
  3.4.8.1.3 Chip Antenna ............................................................................................... 37
  3.4.8.2 Antenna Parameters ............................................................................................ 37
  3.4.8.2.1 Return Loss .................................................................................................... 37

2.7 Some Anti-Jamming Techniques ...................................................................................... 15
  2.7.1 Anti-Jamming Strategies in IEEE 802.11n Networks ................................................. 15
  2.7.2 Anti-Jamming in Wireless Mobile Networks ............................................................ 16
  2.7.3 Universal Anti-Jamming Technology ...................................................................... 16

Chapter Three: Design and Implementation of Cellphone Jammer Circuit ........ 17

VII
Chapter Five: Conclusions

Appendix E: RF Section Block Diagram

Appendix D: PCB Drilling Details (IF-SECTION)

References

Appendix A: Chips datasheets

Appendix B: Components List

Appendix C: Abbreviation Absolute Radio Frequency Channel Number (ARFCN)
TABLE OF FIGURES

Figure 2.1: Block Diagram of Cellphone Jamming Circuit ........................................... 9
Figure 2.2: Classification of jammers .................................................................................. 12

Figure 3.1: A 555-Timer in A-stable Mode ........................................................................ 22
Figure 3.2: Triangle Waveform the 555 Timer in A-Stable Mode ....................................... 22
Figure 3.3: White Noise Representatives .............................................................................. 23
Figure 3.4: Pink Noise Representatives ................................................................................. 24
Figure 3.5: Noise Spectrum .................................................................................................. 24
Figure 3.6: Noise Generator Circuit ..................................................................................... 24
Figure 3.7: Output Noise Waveform (EDA) ........................................................................... 25
Figure 3.8: Amplifier Stage Subcircuit ................................................................................. 25
Figure 3.9: Output Noise Waveform (Spectrum Analyzer) .................................................. 25
Figure 3.10: Mixer Circuit .................................................................................................. 26
Figure 3.11: The ADF4156 Synthesizer .............................................................................. 27
Figure 3.12: Synthesizer Circuit ......................................................................................... 27
Figure 3.13: The ADF4157 Frequency Synthesizer (Block Diagram) ..................................... 28
Figure 3.14: VCO Characteristics ........................................................................................ 31
Figure 3.15: Block Diagram of the Power Supply ................................................................. 32
Figure 3.16: The KBPC3510 Power Supply ......................................................................... 33
Figure 3.17: Center Tapped Transformer ............................................................................ 33
Figure 3.18: Dipole Antenna ................................................................................................ 34
Figure 3.19: Quarter Wave Antenna .................................................................................... 34
Figure 3.20: Antennas Used in Circuit ................................................................................ 35
Figure 3.21: Wire Antenna .................................................................................................. 36
Figure 3.22: PCB Antenna ................................................................................................. 36
Figure 3.23: Chip Antenna .................................................................................................. 36
Figure 3.24: Antenna Return Loss ...................................................................................... 37
Figure 3.25: Antenna Bandwidth vs. Frequency ................................................................. 39
Figure 3.26: Antenna Radiation Pattern Example ............................................................... 39
Figure 3.27: Surface Mount Chip Vs. Throw Hole Chips .................................................... 42
Figure 3.28: Footprint for Resistors ..................................................................................... 43
Figure 3.29: Footprint for Capacitors .................................................................................. 43
Figure 3.30: Footprint for Diodes ....................................................................................... 43
Figure 3.31: Footprint for BJT ............................................................................................ 43
Figure 3.32: Footprint for 555 timer ................................................................................... 44
Figure 3.33: Footprint for 8-pin amplifiers ........................................................................ 44
Figure 3.34: Top PCB Layer ............................................................................................. 44
Figure 3.35: Bottom PCB Layer ......................................................................................... 44
Figure 3.36: Physical Printed Board .................................................................................... 45
Figure 3.37: Overall Scheme ............................................................................................. 45

IX
Figure 4.1: Triangle Wave from the EDA ................................................................. 48
Figure 4.2: Triangle Wave (Spectrum analyzer) ......................................................... 48
Figure 4.3: Noise Output (EDA) ............................................................................... 49
Figure 4.4: Noise (Spectrum Analyzer) ...................................................................... 49
Figure 4.5: VCO ........................................................................................................ 51
Figure 4.6: GSM Channel Output ............................................................................... 51
Figure 4.7: DCS Channel Output ............................................................................... 52
Figure 4.8: Cellphone Signal when Jammer is (a) On (b) Off .................................. 53
LIST OF TABLES

Table 2.1: Classes of Jammers & their Attributes ......................................................... 15

Table 3.1: GSM Systems Frequencies ........................................................................ 19
Table 3.2: Return Loss and Power Reflected from Antenna ..................................... 38
# LIST OF SYMBOLS

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1G</td>
<td>First Generation</td>
</tr>
<tr>
<td>2G</td>
<td>Second Generation</td>
</tr>
<tr>
<td>Hz</td>
<td>Hertz</td>
</tr>
<tr>
<td>V</td>
<td>Volts</td>
</tr>
<tr>
<td>J/S</td>
<td>Jamming to Signal Ratio</td>
</tr>
<tr>
<td>d</td>
<td>Distance</td>
</tr>
<tr>
<td>dB</td>
<td>Decibels</td>
</tr>
<tr>
<td>P</td>
<td>Power</td>
</tr>
<tr>
<td>f</td>
<td>Frequency</td>
</tr>
<tr>
<td>C</td>
<td>Capacity</td>
</tr>
<tr>
<td>R</td>
<td>Resistance</td>
</tr>
<tr>
<td>L</td>
<td>Inductance</td>
</tr>
<tr>
<td>N</td>
<td>Noise</td>
</tr>
<tr>
<td>λ</td>
<td>Lambda (wavelength)</td>
</tr>
<tr>
<td>Ω</td>
<td>Ohms</td>
</tr>
<tr>
<td>π</td>
<td>Pi</td>
</tr>
<tr>
<td>K</td>
<td>Gain or Sensitivity</td>
</tr>
<tr>
<td>w</td>
<td>Omega</td>
</tr>
<tr>
<td>S</td>
<td>S-parameter</td>
</tr>
<tr>
<td>3D</td>
<td>Three Dimension</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>bps</td>
<td>Bits per Second</td>
</tr>
<tr>
<td>$f_{UL}$</td>
<td>Frequency of Up Link</td>
</tr>
<tr>
<td>$f_{DL}$</td>
<td>Frequency of Down Link</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>UofK</td>
<td>University of Khartoum</td>
</tr>
<tr>
<td>DEEE</td>
<td>Department of Electrical and Electronics Engineering</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineering</td>
</tr>
<tr>
<td>CJC</td>
<td>Cellphone Jammer Circuit</td>
</tr>
<tr>
<td>GSM</td>
<td>General System for Mobile-telecommunications</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>IF</td>
<td>Intermediate Frequency</td>
</tr>
<tr>
<td>1G, 2G, etc.</td>
<td>First Generation, Second Generation, etc.</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra-High Frequency</td>
</tr>
<tr>
<td>VHF</td>
<td>Very-High Frequency</td>
</tr>
<tr>
<td>WNJP</td>
<td>Wireless Network Jamming Problem</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WW1, WW2</td>
<td>World War I, World War II</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>AC</td>
<td>Alternate Current</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>BBC</td>
<td>British Broadcast Center</td>
</tr>
<tr>
<td>PCB</td>
<td>Printed Circuit Board</td>
</tr>
<tr>
<td>DCS</td>
<td>Digital Cellular System (GSM-1800)</td>
</tr>
<tr>
<td>AMPS</td>
<td>Advanced Mobile Phone Service</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>TACS</td>
<td>Total Access Communication System</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data Rates for Global Evolution</td>
</tr>
<tr>
<td>WCDMA</td>
<td>Wideband Code Division Multiple Access</td>
</tr>
<tr>
<td>IBD</td>
<td>Intelligent Beacon Disablers</td>
</tr>
<tr>
<td>EMF</td>
<td>ElectroMagnetic Field</td>
</tr>
<tr>
<td>TEMPEST</td>
<td>Transient ElectroMagnetic Pulse Emanation Standard</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal to Noise Ration</td>
</tr>
<tr>
<td>CSMA</td>
<td>Carrier Sense Media Access</td>
</tr>
<tr>
<td>RTS</td>
<td>Request to Send</td>
</tr>
<tr>
<td>CTS</td>
<td>Clear to Send</td>
</tr>
<tr>
<td>ACK</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>FDM</td>
<td>Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>ad-hoc</td>
<td>Advanced Developers Hands on Conference</td>
</tr>
<tr>
<td>ARFCN</td>
<td>Abbreviation absolute Radio Frequency Channel Number</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>FSPL</td>
<td>Free Space Path Loss</td>
</tr>
<tr>
<td>VCO</td>
<td>Voltage Controlled Oscillator</td>
</tr>
<tr>
<td>FET</td>
<td>Field Effect Transistor</td>
</tr>
<tr>
<td>FM</td>
<td>Frequency Modulation</td>
</tr>
<tr>
<td>SMPS</td>
<td>Switch Mode Power Supply</td>
</tr>
<tr>
<td>TL</td>
<td>Transmission Line</td>
</tr>
<tr>
<td>FR</td>
<td>Flame Retardant</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
</tr>
<tr>
<td>VSWR</td>
<td>Voltage Standing Wave Ratio</td>
</tr>
<tr>
<td>AWR</td>
<td>Automatic Workload Repository</td>
</tr>
<tr>
<td>EDA</td>
<td>Electronic Design Automation</td>
</tr>
<tr>
<td>ISBN</td>
<td>International Serial Book Number</td>
</tr>
<tr>
<td>PCS</td>
<td>Personal Communications Service</td>
</tr>
</tbody>
</table>
This page was left intentionally blank.
Chapter One: Introduction

1.1 Overview

Mobile jammers were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists to foil the use of certain remotely detonated explosives. The civilian applications were apparent with growing public resentment over usage of mobile phones in public areas on the rise & reckless invasion of privacy.

Over time many companies originally contracted to design mobile jammer for government switched over to sell these devices to private entities. As with other radio
jamming, mobile jammer blocks mobile phone use by sending out radio waves along the same frequencies that mobile phones use. This causes enough interference with the communication between mobile phones and communicating towers to render the phones unusable. Upon activating mobile jammer, all mobile phones will indicate "NO NETWORK". Incoming calls are blocked as if the mobile phones were off. When the Mobile jammers are turned off, all mobile phones will automatically reestablish communications and provide full service.

Mobile jammer’s effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of buildings and landscape, even temperature and humidity play a role. The choice of mobile jammers is based on the required range starting with the personal pocket mobile jammer that can be carried along with you to ensure undisrupted meeting with your client or a personal portable mobile jammer for your room or medium power mobile jammer or high power mobile jammer for your organization to very high power military jammers to jam large campuses.

1.2 Problem Statement

A cellphone jammer is an instrument used to prevent cellular phones from receiving signals from base stations. When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected.

Various Signal jamming devices may be used by different people or groups to block various frequencies, and hospitals are not an exception. Pacemakers can really interfere with jammers, but both jammers and pace-maker manufacturers are constantly make sure that such situation would be avoided any way.

The original pacemakers were developed to operate using short-range communication frequency (175 kHz), which no ordinary jammer is able to block. New pacemakers on the other hand, use UHF frequency range (402-405MHz).
The only jammer that blocks this spectrum is model of UHF/VHF jammers, and they block 140-180MHz and 450-480MHz frequencies, thus its jamming signal is near but not in the interfered frequency range.

Military strategists are constantly seeking ways to increase the effectiveness of their force while reducing the risk of casualties. In any adversarial environment, an important goal is always to neutralize the communication system of the enemy. In this work, we are interested in jamming a wireless communication network. Specifically, we introduce and study the problem of determining the optimal number and placement for a set of jamming devices in order to neutralize communication on the network. This is known as the Wireless Network Jamming Problem (WNJP). Despite the enormous amount of research on optimization in telecommunications, this important problem for military analysts has received little attention by the research community.

Possible electromagnetic interference to aircraft systems is the most common argument put forth for banning passenger electronic devices on planes. Theoretically, active radio transmitters such as mobile phones, small walkie–talkies, or radio remote–controlled toys may interfere with the aircraft or air traffic control devices. This may be especially true for older planes using sensitive instruments like older galvanometer based displays. The development of this experiment can present a one-time solution to these predicaments.

We also can see the availability to use the jammers to block cellphone signal from interfering with imam’s voice in Mosques and Islamic Centers.

1.3 Background and Motivation

Intentional communications jamming is usually aimed at radio signals to disrupt control of a battle. A transmitter, tuned to the same frequency as the opponents’ receiving equipment and with the same type of modulation, can, with enough power, override any signal at the receiver. Digital wireless jamming for signals such as Bluetooth and Wi-Fi is possible with very low power.
Chapter One

Introduction

During World War II, ground radio operators would attempt to mislead pilots by false instructions in their own language, in what was more precisely a spoofing attack than jamming. Radar jamming is also important to disrupt use of radar used to guide an enemy's missiles or aircraft. Modern secure communication techniques use such methods as spread spectrum modulation to resist the deleterious effects of jamming.

Jamming has also occasionally been used by the governments of Germany (during WW2), Israel, Cuba, Iraq, Iran (Iraq and Iran war, 1980–1988), China, North and South Korea and several Latin American countries, as well as by Ireland against pirate radio stations such as Radio Nova. The United Kingdom government used two coordinated, separately located transmitters to jam the offshore radio ship, Radio North Sea International off the coast of Britain in 1970, and without forgetting, the Nazis attempt to jam broadcasts to the continent from the BBC and other allied stations.

Legality Owning, manufacturing, marketing, offering for sale or operating a cell phone jammer is punishable by an $11,000 fine and up to a year in prison for each offense, which opposes a great deal to develop such a device as defensive weapon.

1.4 Objectives of the Project

The main objective of this project is to design a cellphone jammer circuit with hardware part with high flexibility and minimum cost for University of Khartoum, Educational ground station and making it available for use or modification by students, graduates and researchers.

1.5 Project Methodology

In order to implement a CJC in form of a PCB circuit hardware chip to make the sending (jamming) frequency tolerable and suiting the targeted device, a small set of requirements is considered and goes through each development phase for those set of requirements, design, implements is added in ever increasing until the application is ready for integration, installation and maintenance phase.
1.6 Thesis Layout

This report is organized as follows:

- **Chapter two (Literature Review about Cellphone Jammer Circuit):** In this chapter an overview to the GSM systems and cellphone jammer circuit is introduced with its definition, architecture and types followed by top-down classification of hence jammers followed by some Anti-Jamming Techniques.

- **Chapter three (Design and Implementation of the Cellphone Jammer Circuit):** This chapter includes all assumptions and considerations for the CJC project. It represents the scope of the project, requirements and presenting all the details of the design and implementations.

- **Chapter four (Results and Discussions):** This Chapter presents all results obtained from testing the stages of the project and overall project work, and discusses each one.

- **Chapter five (Conclusions):** By the end of this chapter project is reviewed, objectives achieved is mentioned, objectives not achieved is discussed and finally future work of the project.

- **Appendix A:** ChipsDatasheets
- **Appendix B:** List of components
- **Appendix C:** Abbreviation Absolute Radio Frequency Channel Number (ARFCN)
- **Appendix D:** PCB Drilling Details (IF-Section)
- **Appendix E:** RF-Section Block Diagram
This page was left intentionally blank.
Chapter Two: Literature Review About Cellphone Jammer Circuit

2.1 Overview

This chapter introduces a summarized introduction to the GSM/DCS systems, followed by a brief definition about cellphone jammer circuit definitions, architecture and types followed by top-down classification of hence jammers, followed by some Anti-Jamming techniques.
2.2 Introduction to GSM/DCS Systems

The key technologies used in cellular mobile radio include cellular frequency reuse, analog cellular (First Generation) include Advanced Mobile Phone Service (AMPS) was the original analog cellular system in the United States.

The frequency bands for the AMPS system are 824 MHz to 849 MHz (uplink) and 869 MHz to 894 MHz (downlink). After that, in First Generation the Total Access Communication System (TACS) was deployed with difference than AMPS in radio channel frequency bandwidth. Then, the Second Generation was implemented includes Global System for Mobile Communication (GSM) that will explain in details later in this chapter, also in the same generation the North American TDMA (IS-136 TDMA) and Code Division Multiple Access (CDMA) was deployed. The development in Second Generation was appearing in Packet based digital radio (2.5 generation) include General Packet Radio Service (GPRS) and Enhanced Data Rates for Global Evolution (EDGE). Finally, the CDMA2000 and Wideband Code Division Multiple Access (WCDMA) includes in Third Generation.

In Sudan, there are two types of (GSM), the GSM-900 and GSM-1800. This system also called digital cellular network system (DCS), so that this project is focusing only on GSM and DCS systems to design our intelligent jamming system.

2.3 Cellphone Jammer Circuit

Jamming in wireless networks is defined as the disruption of existing GSM communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering mobile signals. Hence, A CJC device is device that executes this duty.

The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen.
2.4 Jammer Architecture

Cell-phone jammers are very basic devices. The simplest just have an on/off switch and a light that indicates it’s on. More complex devices have switches to activate jamming at different frequencies. Components of a jammer include:

- Voltage Controlled Oscillator (VCO)
- Tuning circuit
- Mixer
- Noise Generator
- RF Stage
- Power Supply
- Antenna(s)

![Block Diagram of Cellphone Jamming Circuit](image)

Figure 2.1: Block Diagram of Cellphone Jamming Circuit

2.4.1 Voltage Controlled Oscillator

Generates the radio signal that will interfere with the cell phone signal.

2.4.2 Tuning Circuit

Controls the frequency at which the jammer broadcasts its signal by sending a particular voltage to the oscillator.

2.4.3 Mixer

Combines two signals in such a way to produce the sum and difference of the two input frequencies at the output.
Chapter Two  Literature Review about Cellphone Jammer Circuit

2.4.4 Noise Generator

Produces random electronic output in a specified frequency range to jam the cellphone network signal (part of the tuning circuit).

2.4.5 RF Stage

Boosts the power of the radio frequency output to high enough levels to jam a signal.

2.4.6 Power Supply

Battery operated or using a V-V transformer (small capacity), to provide the electrical power needed to operate the jammer.

2.4.7 Antenna

The broadcaster of jammer signal in desired map area.

2.5 Jamming Techniques

Here, a brief preview to methods of jamming a signal:

2.5.1 Strategies

2.5.1.1 Noise Strategy

The main idea here is to insert additional noise in receivers which prevent them from getting the correct information from the receiving signal. Almost all the techniques which will be discussed later depend on these strategies.

2.5.1.2 Phase Strategy

The main idea is to change the phase of signals to prevent the receivers which uses this phase to receive signal in correct phase.
Chapter Two  Literature Review about Cellphone Jammer Circuit

2.5.2 Techniques

2.5.2.1 Spoofing

In this kind of jamming, the device forces the mobile to turn off itself. This type is very difficult to be implemented since the jamming device first detects any mobile phone in a specific area, then the device sends the signal to disable the mobile phone. Some types of this technique can detect if a nearby mobile phone is there and sends a message to tell the user to switch the phone to the silent mode (Intelligent Beacon Disablers).

2.5.2.2 Shielding Attacks

This is known as TEMPEST or EMF shielding. This kind requires closing an area in a faraday cage so that any device inside this cage cannot transmit or receive RF signal from outside of the cage. This area can be as large as buildings, for example.

2.5.2.3 Denial of Service

This technique is referred to DOS. In this technique, the device transmits a noise signal at the same operating frequency of the mobile phone in order to decrease the signal-to-noise ratio (SNR) of the mobile under its minimum value. This kind of jamming technique is the simplest one since the device is always on. Our device is of this type.

2.6 Types of Jammers

Jammers are malicious wireless nodes planted by an attacker to cause intentional interference in a wireless network. Depending upon the attack strategy, a jammer can either have the same or different capabilities from legitimate nodes in the network which they are attacking. The jamming effect of a jammer depends on its radio transmitter power, location and influence on the network or the targeted node.

A jammer may jam a network in various ways to make the jamming as effective as possible. Basically, a jammer can be either elementary or advanced depending upon its functionality. For the elementary jammers, we divided them into two sub-groups: proactive and reactive. The advanced ones are also classified into two sub-types:
function-specific and smart-hybrid. The detailed classification of different jammers can be found in Figure 2.2.

![Figure 2.2: Classification of jammers.](image)

2.6.1 Elementary Jammers

2.6.1.1 Proactive Jammers

They transmit jamming interfering signals whether or not there is data communication in a network and send packets or random bits on the channel it is operating on, but do not switch channels and operates on only one channel until its energy is exhausted. The types of proactive jammers are: constant, deceptive and random.

2.6.1.1.1 Constant Jammer

Emits a continuous random bit switch out following the CSMA protocol and prevents legitimate nodes from communicating with each other by causing the media to be constantly busy.

2.6.1.1.2 Deceptive Jammer

Deceives other nodes to believe that a legitimate transmission is taking place so that they remain in receiving states until the jammer is turned off or dies.
2.6.1.3 Random Jammer

Intermittently, transmits either random bits or regular packets into networks. It saves energy by continuous switching between sleep and jamming states.

2.6.1.2 Reactive Jammers

Reactive jammer starts jamming only when it observes a network activity occurs on a certain channel, hence, targets on compromising the reception of a message. Reactive jammer is less energy efficient than random jammer. The following are two different ways to implement a reactive jammer:

2.6.1.2.1 RTS/CTS Jammer

Jams network when it senses a request-to-send (RTS) message is being transmitted from a sender. It starts jamming the channel as soon as the RTS is sent. Hence, receiver will not send back clear-to-send (CTS) reply because the RTS packet sent from a sender is distorted. Then, sender will not send data because it believes the receiver is busy with another on-going transmission.

2.6.1.2.2 DATA/ACK Jammer

Jams the network by corrupting the transmissions of data or acknowledgement (ACK) packets. It does not react until a data transmission starts at the transmitter end. This type of jammer can corrupt data packets, or it waits until the data packets reach the receiver and then corrupts the ACK packets.

2.6.2 Advanced Jammers

2.6.2.1 Function-Specific Jammers

Function-specific jamming is implemented by having a pre-determined function. In addition to being either proactive or reactive, they can either work on a single channel to conserve energy or jam multiple channel sand maximize the jamming throughput irrespective of the energy usage. Even when the jammer is jamming a single channel at a time, they are not fixed to that channel and can change their channels according to their specific functionality.
2.6.2.1 **Follow-On Jammer**

Hops over all available channels very frequently (thousand times per second) and jams each channel for a short period of time. It is particularly effective against some anti-jamming techniques, e.g. Frequency Hopping Spread Spectrum (FHSS) which uses a slow-hopping rate.

2.6.2.1.2 **Channel Hopping Jammer**

Hops between different channels proactively. It has direct access to channels by overriding the CSMA protocol algorithm provided by the MAC layer. Then, it starts performing attacks on different channels at different times according to a predetermined pseudo-random sequence.

2.6.2.1.3 **Pulsed Noise Jammer**

Can switch channels and jam on different bandwidths at different periods of time.

2.6.2.2 **Smart-Hybrid**

They are called smart because of their power efficient and effective jamming nature, and hybrid because they can be implemented as both proactive and reactive. Main aim of these jammers is to magnify their jamming effect in the network they intend to jam.

2.6.2.2.1 **Control Channel Jammer**

Work in multi-channel networks by targeting the control channel, or the channel used to coordinate network activity.

2.6.2.2.2 **Implicit Jammer**

Are those that in addition to disabling the functionality of the intended target, cause denial-of-service state at other nodes of the network too.

2.6.2.2.3 **Flow Jammer**

Involve multiple jammers throughout the network which jams packets to reduce traffic flow. These attacks are launched by using information from the network layer. If there is a centralized control, then the minimum power to jam a packet is computed and the jammer acts accordingly. In a non-centralized jammer model, each jammer shares information with neighbour jammers to maximize efficiency.
Chapter Two  Literature Review about Cellphone Jammer Circuit

At the end, table 2.1 shows the attributes of each jammer as a comparison between them.

<table>
<thead>
<tr>
<th>Jammer</th>
<th>Proactive</th>
<th>Reactive</th>
<th>Energy Efficient</th>
<th>Single Channel</th>
<th>Multiple Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>×</td>
<td></td>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Deceptive</td>
<td>×</td>
<td></td>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Random</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>RTS/CTS</td>
<td></td>
<td>×</td>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DATA/ACK</td>
<td></td>
<td>×</td>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Follow-on</td>
<td>×</td>
<td></td>
<td></td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Channel Hopping</td>
<td></td>
<td>×</td>
<td></td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Pulsed Noise</td>
<td>×</td>
<td></td>
<td></td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Control Channel</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Implicit</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Flow-Jammer</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

Table 2.1 :Classes of Jammers & their Attributes

2.7 Some Anti-Jamming Techniques

2.7.1 Anti-Jamming Strategies in IEEE 802.11n Networks

There is very few research work on jamming and anti-jamming techniques in IEEE 802.11n networks. Since the IEEE 802.11n is very different from its predecessor IEEE 802.11a/b/g, the results of applying existing jamming and anti-jamming techniques on IEEE 802.11n network could be very different. For example, XXXX shows that due to the channel bonding effect in IEEE 802.11n, proactive frequency hopping is not a suitable countermeasure for jamming. On the other hand, since the IEEE 802.11n
technology uses Orthogonal Frequency Division Multiplexing (OFDM), it will be easier to implement an effective reactive countermeasure.

2.7.2 Anti-Jamming in Wireless Mobile Networks

Most jamming detection and countermeasure are designed and evaluated in static networks. The anti-jamming problem becomes more challenging in a mobile network environment where jammers may move and cause the malfunction of jammer detection and localization algorithms. So far, spatial retreats seem to be the only strategy implemented on the mobile nodes. Having an effective approach for wireless mobile networks with acceptable overhead is still an open issue. The anti-jamming system for mobile networks should provide fast-detecting and fast-reacting mechanism which can identify and localize a jammer quickly.

Moreover, since the same jammer may move and cause jamming in other areas in the networks, how to prevent jamming based on historical jamming information will be very interesting.

2.7.3 Universal Anti-Jamming Technology

Finally, we want to pose the ultimate question: is it possible to have a single practical anti-jamming solution which can deal with all types of wireless networks (whether it is static or mobile, sensor or Wi-Fi, infrastructure-based or ad-hoc) and detect all kinds of jammers (e.g. constant, deceptive, random, reactive, follow-on, channel hopping, control channel, implicit, flow jammers)? In addition, since we have so many effective jamming techniques, beside preventing eavesdropper’s attack, can we use them for any useful purpose?
Chapter Three: Design and Implementation of Cellphone Jammer Circuit

3.1 Introduction

This chapter introduces the tools and methodology used to implement the project. First consideration that taken into account to design the project is introduced, then project scope and design options were defined, finally, the chosen design and the software design environment involved are discussed in details followed by conclusions that summarizes how the project works.
3.2 Design Considerations

- **Cost Effective:** The system is to be designed and implemented using available components with suitable cost.
- **Re-Configurability:** The system is to be easily reconfigurable and flexible so that it can be used to support any number of demodulations.
- **Extensibility:** The system must be designed such that new capabilities can be added to it without major changes to the underlying architecture.
- **Usability:** This system is to be designed with user interface such that it is convenient to be used by all users of all levels.
- **Compatibility:** The project target is to design a Cellphone Jammer Circuitry that can be implemented in any facility.
- **Simplicity:** The system design based on a simple approach to help future development.
- **Optimized:** The number of major problems fixed such as resonance and coverage of frequencies as discussed later in this chapter.

3.3 Project Scope

The scope of the project is to implement a design to the Cell-Phone Jamming Circuitry that works on the First and Second Generations mobile devices with a simple circuit (hand-made) and then on a Soft-Ware Designed PCB processed by a Personal Computer.

The system is designed to be an educational jammer targeting different users such as undergraduate and graduate students, researchers and different stakeholders such as manufacturers and marketers.
Chapter Three  Design and Implementation of Cellphone Jammer Circuit

3.4 Hardware Phase Design

as a reminder we’ll review our “jammer knowledge” by this definition:

**Signal Jamming:** denying the successful transport of information from the sender to the receiver, and vice-versa.

The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen.

3.4.1 Design Parameters

3.4.1.1 Jamming Distance

The output power of the device is related to the distance the device covers inverse proportionally.

\[ P_{OUT} \propto R_j \]

3.4.1.2 Frequency Bands

The following table contains the frequency bands for GSM and DCS systems. To avoid the fractions in frequency; the companies of mobile communication uses the abbreviation absolute radio frequency channel number (ARFCN) to define the uplink and downlink frequency at the same time, (see Appendix C).

<table>
<thead>
<tr>
<th>GSM System</th>
<th>Uplink Frequency Band</th>
<th>Downlink Frequency Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM 900</td>
<td>890 – 915 MHz</td>
<td>935 - 960 MHz</td>
</tr>
<tr>
<td>GSM 900 Extended Band</td>
<td>880 – 915 MHz</td>
<td>925 - 960 MHz</td>
</tr>
<tr>
<td>DCS 1800</td>
<td>1710 - 1785 MHz</td>
<td>1805 – 1880 MHz</td>
</tr>
</tbody>
</table>

Table 3. 1: GSM Systems Frequencies

Frequencies the device will cover:

**GSM 900: 935-960 MHz** and **GSM 1800: 1805-1880 MHz**
3.4.1.3 Jamming-to-Signal Ratio

- Jamming is successful when the jamming signal denies the usability of the communication transmission.
- Usability is denied when the error rate of the transmission cannot be compensated by error correction.
- J/S Ratio sets a measure to how powerful the jamming signal is, compared to the original signal.

General equation of the jamming-to-signal ratio is given as follows:

\[
\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j}
\]

where:

- \(P_j\): Power of jammer
- \(P_t\): Power of transmitter
- \(G_{jr}\): Antenna Gain from jammer to receiver
- \(G_{rj}\): Antenna Gain from receiver to jammer
- \(G_{tr}\): Antenna Gain from transmitter to receiver
- \(G_{rt}\): Antenna Gain from receiver to transmitter
- \(R_{tr}\): Range between transmitter and receiver
- \(R_{jr}\): Range between jammer and receiver
- \(L_r\): Power loss of receiver
- \(L_j\): Power loss of jammer
- \(B_r\): Bandwidth of receiver
- \(B_j\): Bandwidth of jammer

3.4.1.4 Free Space Loss

Free-Space Path loss (FSPL) is the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction. In our stand of view, we can calculate it as follows:

\[
\text{Path Loss (dB)} = 32.44 + 20 \log(d) \ (km) + 20 \log(f) \ (MHz)
\]
Chapter Three  Design and Implementation of Cellphone Jammer Circuit

where:

\( d \) : Jamming distance
\( f \) : Ranged Frequency

- Worst case (F) happens when the Maximum Frequency is used in the above equation.

Using 1880 MHz gives: \( P_{\text{max freq. (dB)}} = 32.44 + 20 \log (0.01) + 20 \log (1880) = 58 \text{ dB} \).

Now, let’s talk about the hardware:

3.4.2  **Sweep Generator (Timer Stage)**

The main use of the triangle wave is to sweep the VCO to the desired frequency ranges:

- 935-960 MHz for VCO66CL and 1805-1880MHz for VCO55BE
- we can use the 555 timer in the general A-stable mode to generate the sweeping signal.
- The output frequency depends on the charging and discharging of the capacitor, resistors values and the power supply for the IC.
- The Charging Time of the capacitor can be found as follows:
  \[
  T_C = 0.639(R_a + R_b)C
  \]
- The Discharging Time:
  \[
  T_D = 0.639R_b C
  \]
- And the Output Frequency can be calculated as follows:
  \[
  f_{\text{OUT}} = \frac{1.44}{(R_a + R_b)C}
  \]
- We need to get the charging and discharging time to equal so a %50 duty cycle appears. This can be done by equating the values of (\( R_a = R_b \)) (or \( R_1, R_2 \) respectively) and placing a diode across \( R_b \), and the output frequency can as hence previous equation. (see Figure 3.1 next page).
Figure 3. 1: A 555-Timer in A-stable Mode

the desired output will be a **triangle wave** showing that the circuit is working as shown in figure below:

Figure 3. 2: Triangle Waveform the 555 Timer in A-Stable Mode

### 3.4.3 IF Stage

We will be discussing two parts: the noise generator and the amplifier.
3.4.3.1 Noise Generator

In this project the jamming system needs a certain type of noise to cover a portion of spectrum, so the most applicable type of noise in this case is the white noise.

The Noise in general can be defined as: A random movement of charges or charge carriers in an electronic device generates current and voltage that vary randomly with time.

- **White Noise (Thermal Noise):**
  
  White noise is a random signal (or process) with a flat power spectral density. In other words, the signal's power spectral density has equal power in any band, at any center frequency, having a given bandwidth. White noise is considered analogous to white light which contains all frequencies.

![Diagram of noise generators](image)

**Figure 3.3: White Noise Representatives**

- **Pink Noise (Flicker Noise):**

  Pink noise is a signal or process with a frequency spectrum such that the power spectral density (energy or power per frequency interval) is inversely proportional to the frequency of the signal. In pink noise, each octave (halving/doubling in frequency) carries an equal amount of noise energy. The name arises from the pink appearance of visible light with this power spectrum. This is in contrast with white noise which has equal intensity per frequency interval.

\[ S(f) \propto \frac{1}{f^\alpha} \]

where: \( f \) is the frequency and \( 0 < \alpha < 2 \) (usually close to 1)
The proposed circuit to generate the noise is as shown below:
3.4.3.2 Amplifier Stage

Its use is to amplify the noise generated by the noise device former to it. Two stages are used as shown in Figure 3.7 which are: Low Power amplifier LM386 and operational amplifier (the summer) U741A. Capacitor C5 is used to block DC current, and the re resistor forms a none inverting amplifier and its gain is given by \(1 + \frac{R_1}{R_2}\). The noise wave form is shown in Figure 3.6 and Figure 3.8.
3.4.4 Mixer

Mixer is a nonlinear circuit that combines two signals in such a way to produce the sum and difference of the two input frequencies at the output.

- **Transistor Mixer**: In this project the mixer uses FET transistor; since it’s a low noise device and fast in response, so its efficient device in this case. The FET Circuit illustrates the technique of summing the two input signal at a single input terminal (both IN1 and IN2 are applied to the gate).

FETs can be used in mixers in both active and passive modes. There are different types of mixers and different techniques; in this project the mixer uses the simple summer circuit contains from just one dual LM 741. LM 741 OP-AMP is a high speed J-FET input dual operational amplifiers incorporating well matched, high voltage J–FET and bipolar transistors in a monolithic integrated circuit.

The devices features:

- High slew rates.
- Low input bias and offset current.
- Low offset voltage temperature coefficient.

![Mixer Circuit](image)

Figure 3. 10: Mixer Circuit
3.4.5 RF Stage

3.4.5.1 Synthesizer (An Example)

It’s a device which is used as a tunable oscillator. The ADF4156 is shown in Figure 3.10 is a 6 GHz Fractional-N frequency synthesizer that implements local oscillators in the up and down conversions sections of wireless receivers and transmitters.

![ADF4156 Synthesizer](image1)

![Synthesizer Circuit](image2)

Synthesizers use various methods to generate electronic signals (sounds). Among the most popular waveform synthesis techniques are subtractive synthesis, additive synthesis, wavetable synthesis, frequency modulation synthesis (our focus here), phase distortion synthesis, physical modeling synthesis and sample-based synthesis.

Next step, is to FM modulate. After, using a Zener diode in reverse mode which creates a lot of noise due to the emission it causes and the avalanche effect, hence creating a wide band noise.

Then, the noise will be amplified in two amplification stages: in the first stage, we use **NPN transistor** as common emitter (to amplify the whole signal), and in the second stage, using the **LM386** IC (Audio amplifier to make sure the signal is properly adjusted).
The following equation governs how the synthesizer should be programmed:

\[ RF_{OUT} = \left[ N + \frac{FRAC}{225} \right] \times F_{PFD} \]

where:

\( RF_{OUT} \): RF Frequency Output  
\( N \): Integer Division Factor  
\( FRAC \): The Fractionality  
\( F_{PFD} \): Phase/Frequency Detection Frequency

### 3.4.5.2 RF Mixer

The jamming signal must have the same frequency of the controller channel with bandwidth equal to (200KHz) provided from VCO in the IF stage, so you need to carry this baseband on a suitable carrier which have the frequency of controller channel; to do this its useful to use the RF Mixer.
3.4.5.2.1 Power Amplifier

As provided below; a calculation of the minimum blocking power is needed to complete the jamming of GSM-900 and GSM-1800 signals:

- For **GSM-900**:
  - The minimum Signal-to-Noise Ratio (SNR) is 9 dB.
  - The maximum signal power ($S_{MAX}$) is -15 dB.

\[
SNR = \frac{S}{N} = \frac{S}{J_r}
\]

where: $J_r$ (the jamming frequency range) in dBm = -15 - 9 = -24 dBm.

- Free-Space Power Loss (FSPL):

\[
FSPL = 20 \log\left(\frac{4\pi R}{\lambda}\right)
\]

where: $R$ and $\lambda$ in meter.

For **960 MHz**:

\[
\lambda = \frac{C}{F} = \frac{3 \times 10^8}{960 \times 10^6} = 0.3125 \text{ m}
\]

Substituting in FSPL equation gives:

\[
FSPL = 20 \log\left(\frac{4\pi \times 1}{0.3125}\right) = 58 \text{ dB}
\]

Then \[J_r = -24 + 58 = 34 \text{ dBm}.\]

- For **GSM-1800**:
  - The minimum Signal-to-Noise Ratio (SNR) is 9 dB.
  - The maximum signal power ($S_{MAX}$) is -23 dB.

Repeating the same calculation with $F = 1880 \text{ MHz}$ gives:

\[J_r = -32 + 63.9 = 31.9 \text{ dBm}\]

Which all what we need to operate the power amplifier.

3.4.5.2.2 Power Amplifier GSM-900

This power amplifier is suitable for GSM-900 downlink frequency (925-960MHz). This power amplifier can give 34dBm maximum power.
Chapter Three  Design and Implementation of Cellphone Jammer Circuit

In the PA08109B power amplifier there is no need to amplify the signal fed from synthesizer because it is sufficient to get the desired output power, it also works on both GSM-900 and GSM-1800 ranges.

Usually, the PA08109B chip is embedded with the voltage controlled oscillator, which we are discussing, as a one chip (See Appendix A).

3.4.5.2.3 Power Amplifier DCS-1800

It’s a power amplifier which can be used to give the sufficient power for jamming signal in range of DCS downlink frequency (1805 - 1880 MHz). This power amplifier can give 33dBm maximum power.

3.4.6 Voltage Controlled Oscillators

Voltage Controlled Oscillators (VCO’s) are oscillators whose frequencies could be varied electronically, and can be tuned over a certain frequency.

Figure 3.14 shows the desired behavior of a VCO. The output frequency varies from $\omega_1$ to $\omega_2$ (the required tuning range) as the control voltage, $V_{out}$, goes from $V_1$ to $V_2$. the slope of characteristics, $K_{VCO}$, is called the “gain” or “sensitivity” of the VCO and expressed in rad/Hz/V. The equation is:

$$\omega_{out} = K_{VCO} V_{cont} + \omega_0$$

where $\omega_0$ denotes the intercept point on the vertical axis. It is desirable that these characteristics be relatively linear, i.e., $K_{VCO}$ does not change significantly across the tuning range (See Appendix A).

The outputted signal from this stage should be carry out these properties:

- Same amplitude of the jammed signal.
- Different frequency in which when it sums the purposed signal they but cancel out each other.
we found the following VCO IC’s:-

- CVCO55CL; this is for GSM 900. The output frequency is 925-970 MHz and the output power is up to 8 dBm.
- CVCO55BE; this is for GSM 1800. The output frequency is 1785-1900 MHz and the output power is up to 5 dBm.

We chose these IC’s for the following reasons:-

- Surface mount, which reduces the size of product.
- Having large output power that reduces the number of amplification stages that we need.
- Having same value of power supply which is typically equal to 5 volt.
- Having same noise properties.

### 3.4.7 Power Supply

The main operator of the jamming system is the electrical power supplied by the power supply and feed through each stage in the system. Throughout this section, we are going to explain the relationship between the power supply and other stages in the system.

In general, the power supply consists of the following:

- Transformer.
- Rectifier.
Chapter Three  Design and Implementation of Cellphone Jammer Circuit

- Filter.
- Regulator.

Figure 3. 15: Block Diagram of the Power Supply

The power supply circuit works as follows:

1. The transformer is used to step down the input voltage from 220 Volts to the desired values.
2. The rectifier stage is used to convert the signal from AC to DC.
3. Filter is used to reduce the ripple of voltage that results from rectifier stage.
4. The regulator is used for safety and to ensure a fixed voltage across a certain load in the circuits in case the input values or the load are changed so it have the concept of the Zener diode principle.

- Using AC to DC power supply, which gives directly the wanted values, for example the power supply of the PC which has a complex arrangement of electrical components, including diodes, capacitors and transformers, this special power supply is called switched mode power supply (SMPS), the switching process is to convert the current frequency from 50 Hz to higher frequency; to reduce the ripple that inversely proportional to frequency. Their outputs are: 3.3, 5, 9, 12 and -5, -9, -12 Volts.
- Building a power supply from transformer, bridge rectifier, and regulators. In this method the center tap transformer stepdown from 220 to 30 is used, then
connects a bridge rectifier like KBPC3510 with two capacitors to get DC signal.

![KBPC3510 Power Supply](image)

Figure 3.16: The KBPC3510 Power Supply

![Center Tapped Transformer](image)

Figure 3.17: Center Tapped Transformer

### 3.4.8 Antenna

An antenna is basically a conductor exposed in space. If the length of the conductor is a certain ratio or multiple of the wavelength of the signal, it becomes an antenna. This condition is called “resonance”, as the electrical energy fed to antenna is radiated into free space.

In Figure 3.17, the conductor has a length $\lambda/2$, where $\lambda$ is the wave length of the electric signal. The signal generator feeds the antenna at its center point by a transmission
line known as “antenna feed”. At this length, the voltage and current standing waves are formed across the length of the conductor, as shown in Figure 3.17. The electrical energy input to the antenna is radiated in the form of electromagnetic radiation of that frequency to free space. The antenna is fed by an antenna feed that has an impedance of, say, 50 Ω, and transmits to the free space, which has an impedance of 377 Ω. Thus, the antenna geometry has two most important considerations:

1. Antenna length
2. Antenna feed

The $\lambda/2$-length antenna shown in Figure 3.18 is called a dipole antenna. However, most antennas in printed circuit boards achieve the same performance by having a $\lambda/4$-length conductor in a particular way. See Figure 3.18.

By having a ground at some distance below the conductor, an image is created of the same length ($\lambda/4$). When combined, these legs work like a dipole antenna. This type of antenna is called the quarter-wave ($\lambda/4$) monopole antenna.

Most antennas on the PCB are implemented as quarter-wave antennas on a copper ground plane. Note that the signal is now fed single-ended and that the ground plane acts as the return path.

Figure 3. 18: Dipole Antenna

Figure 3. 19: Quarter Wave Antenna
Figure 3.20: Antennas Used in Circuit

For a quarter-wave antenna that is used in most PCBs, the important considerations are:

1. Antenna length.
2. Antenna feed.
3. Shape and size of the ground plane and the return path.

3.4.8.1 Antenna Types

As described in the previous section, any conductor of length $\lambda/4$ exposed in free space, over a ground plane with a proper feed can be an effective antenna. Depending on the wavelength, the antenna can be as long as the FM antenna of a car or a tiny trace on a beacon. For 2.4-GHz applications, most PCB antennas fall into the following types:

3.4.8.1.1 Wire Antenna

A piece of wire extending over the PCB in free space with its length matched to $\lambda/4$ over a ground plane. This is generally fed by a 50-$\Omega$ transmission line. The wire antenna gives the best performance and RF range because of its dimensions and three-dimensional exposure. The wire can be a straight wire, helix or loop.
3.4.8.1.2 PCB Antenna

A trace drawn on the PCB. This can be a straight trace, inverted F-type trace, meandered trace, circular trace, or a curve with wiggles depending on the antenna type and space constraints.

There are guidelines that must be followed as the 3D antenna exposed in free space is brought to the PCB plane as a 2D PCB trace. A PCB antenna requires more PCB area, has a lower efficiency than the wire antenna, but is cheaper. It has easy manufacturability and has the wireless range acceptable for a BLE application.
3.4.8.1.3 Chip Antenna

An antenna in a small form-factor IC that has a conductor packed inside. This is useful when there is limited space to print a PCB antenna or support a 3D wire antenna. Refer to Figure 3.22 for a Bluetooth module containing a chip antenna. The size of the antenna and the module in comparison with a one cent coin is given above.

3.4.8.2 Antenna Parameters

The next couple pages contain some antenna performance key parameters:

3.4.8.2.1 Return Loss

Return Loss indicates how much of the incident power is reflected by the antenna due to mismatch. An ideal antenna when perfectly matched will radiate the entire energy without any reflection.

\[ \text{Return Loss (dB)} = 10 \log \left( \frac{P_{\text{incident}}}{P_{\text{reflected}}} \right) \]

The return loss of an antenna signifies how well the antenna is matched to the 50-Ω transmission line (TL), shown as a signal feed in Figure ##. The TL impedance is typically 50 Ω, although it could be a different value.
• If the return loss is infinite, the antenna is said to be perfectly matched to the TL, as shown in Figure 3.24. $S_{11}$ is the negative of return loss expressed in decibels.

• If the return loss $\geq 10$ dB (equivalently, $S_{11} \leq -10$ dB) is considered sufficient. Table 1 relates the return loss (dB) to the power reflected from the antenna (percent).

• A return loss of 10 dB signifies that the 90% of the incident power goes into the antenna for radiation.

The following table shows some extensive used values of signal powers and their return loss and radiated and reflected signals’ ratios calculated values:

<table>
<thead>
<tr>
<th>$S_{11}$ (dB)</th>
<th>Return Loss (dB)</th>
<th>$P_{\text{reflected}} / P_{\text{incident}}$</th>
<th>$P_{\text{radiated}} / P_{\text{incident}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-20</td>
<td>20</td>
<td>1 %</td>
<td>99 %</td>
</tr>
<tr>
<td>-10</td>
<td>10</td>
<td>10 %</td>
<td>90 %</td>
</tr>
<tr>
<td>-3</td>
<td>3</td>
<td>50 %</td>
<td>50 %</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>79 %</td>
<td>21 %</td>
</tr>
</tbody>
</table>

Table 3.2: Return Loss and Power Reflected from Antenna

### 3.4.8.2.2 Bandwidth

Bandwidth indicates the frequency response of an antenna and signifies how well the antenna is matched to the 50-$\Omega$ transmission line over the entire band of interest, that is, between:

• 890 MHz and 915 MHz (uplink) / 935 MHz and 960 MHz (downlink) for GSM-900.

• 1710 MHz and 1785 MHz (uplink) / 1805 MHz and 1880 MHz (downlink) for GSM-1800.

• Duplex spacing of 45, 95 MHz is used, respectively.
so the band width of interest is around 200 KHz

### 3.4.8.2.3 Radiation Efficiency

A portion of the non-reflected power (see Figure 3.24) gets dissipated as heat or as thermal loss in the antenna. Thermal loss is due to the dielectric loss in the FR4 substrate and the conductor loss in the copper trace. This information is characterized as radiation efficiency. A radiation efficiency of 100% indicates that all non-reflected power is radiated to free space. For a small-form-factor PCB, the heat loss is minimal.

### 3.4.8.2.4 Radiation Pattern

Radiation pattern indicates the directional property of radiation, that is, which directions have more radiation and which have less. This information helps to orient the antenna properly in an application.
• An isotropic dipol antenna radiates equally in all directions in the plane perpendicular to the antenna axis. However, most antennas deviate from this ideal behavior. See the radiation pattern of a PCB antenna shown in Figure # as an illustration. Each data point represents RF field strength, measured by the Received Signal Strength Indicator (RSSI) in the receiver. As expected, the contours are not exactly circle, as the antenna is not isotropic.

3.4.8.2.5 Gain

An indicator to the radiation in the direction of interest compared to the isotropic antenna, which radiates uniformly in all directions. This is expressed in terms of dBi how strong the radiation field is compared to an ideal isotropic antenna.

3.4.8.2.6 Voltage Standing Wave Ratio (VSWR)

Let us define some terms:

• Characteristic Impedance ($Z_o$): A parameter of transmission line that determines the behavior and response to a signal passing though (An antenna is a line not to forget). It is determined as follows:

$$Z_o = \sqrt{\frac{R + j\omega L}{G + j\omega C}}$$

• Reflection Coefficient ($\Gamma$): A ratio between the standing wave and the reflected wave, determined by the characteristic impedance and load impedance. Determined by following formula:

$$\Gamma = \frac{Z_L - Z_o}{Z_L + Z_o}$$

If $\Gamma = 0$; then we have “matching”.

If $Z_L = 0$; then $\Gamma = -1$ ($1 \angle 180^\circ$), Else $Z_L \rightarrow \infty$; then $\Gamma = 1$ ($1 \angle 0^\circ$).
Standing Wave: the wave opposing to the transmitted wave which could destroy it.

Voltage Standing Wave Ratio (VSWR): is the ratio between the incident and reflected wave.

assuming that $V_i$, $V_r$ are the incident and reflected waves amplitude respectively; the following formula defines the VSWR:

$$VSWR = \frac{V_i - V_r}{V_i + V_r}$$

ranging from 1 to $\infty$.

The purposed hypothesis here, is that we have matched transmission line (Antenna) each side (sending or receiving), so the all the sent signal will be totally disrupted (in best case), hopefully the better the reflection coefficient the better the jamming.

As for the Standing Wave Ratio; the closer the ratio to 1, the worse the jamming. Now, that we have basis knowledge about the VSWR, we can now talk about how to choose an antenna.

### 3.4.8.3 Choosing an Antenna

The selection of an antenna depends on the application, the available board size, cost, RF range, and directivity.

Bluetooth Low energy (BLE) applications such as a wireless mouse requires an RF range of only 10 feet and a data rate of a few kbps. However, for a remote control application with voice recognition, an antenna should have a range around 20 feet in an indoor setup and a data rate of 64 kbps.

For wireless audio applications or indoor positioning, antenna diversity is required. For antenna diversity, two antennas are placed orthogonally on the same PCB such that at least one of them is always receiving some radiation while the other may be
shadowed by reflection and multi-path-fading. This is required where real-time audio data is transmitted and a high throughput without packet loss is required.

As for our circuit we are utilizing a wire antenna that is connected to the PCB, and has these Specifications:

- Antenna 1 = GSM antenna (Frequency = 850MHz-1GHz, Input Impedance = 50Ω, VSWR<2)
- Antenna 2 = DCS antenna (Frequency = 1700MHz-1900MHz, Input Impedance = 50Ω, VSWR<2)

3.5 Software Phase Design

The term of software used here, refers to the group of computer aided design tools and programs involved in this project. These include the AWR environment plus the Spice Simulation tools plus the Altium Designer kit plus the Electronic Design Automation (EDA) tools plus Proteus environment.

3.5.1 PCB Layout

A printed circuit board (PCB) mechanically supports and electrically connects electronic components using conductive tracks, pads and other features etched from copper sheets laminated onto a non-conductive substrate. Components (e.g. capacitors, resistors or active devices) are generally soldered on the PCB.

According to the pins shape there are two sorts of chips; surface mount and through hole chips, the next couple of figure explain the difference.

Figure 3. 27: Surface Mount Chip Vs. Throw Hole Chips
Chapter Three        Design and Implementation of Cellphone Jammer Circuit

Some component like resistors, capacitors and inductors must be surface mounted. Each component has a certain footprint which meaning holes’ shapes which the component pin will be inserted in, also each foot print has certain dimensions.

CJC’s PCB has 37 components to be printed in the board, designed to be as two-layer board (top and bottom) to make the board area small as can be. Figures 3.29 - 3.34 shows number of footprints for som components (different components may have the same foot print).

Figure 3.28: Footprint for Resistors.

Figure 3.29: Footprint for Capacitors

Figure 3.30: Footprint for Diodes

Figure 3.31: Footprint for BJT
After each component got its footprint then all of them integrated in one PCB file. Each footprint will be placed in its suitable place, also mutual inductance effects taken in consideration. The placing of component will be manually. Figures 3.35, 3.36 respectively; show the layers of PCB layout in simulation, and Figure 3.37 shows the physical printed board.
3.5.1.1 PCB - RF Stage

The design given here was only printed but not tested.

3.5.1.2 Overall Scheme (IF-Stage)

The overall scheme conducted through Proteus Designer’s Suite:

![Overall Scheme Diagram](image)

Figure 3. 37: Overall Scheme
3.6 Conclusion

As a summary to the “Design and Implementation” Chapter, we can mention these points:

- The timer circuit produces a triangle wave that gets mixed with a noise signal coming from the noise generator, at the amplifier stage.
- The summed signal goes to the VCO and Power Amplifier combined stage to tolerate the frequency.
- The resulting signal, gets amplified to the desired frequency as required to jam a purposed signal.
- At the end, the attributed signal is broad casted to the antenna with predefined radius to jammed the semi-attribute signals inside this radius.
- The circuit, as shown, is tested part by part, and then implement as whole in one PCB Chip scheme.
Chapter Four: Results and Discussion

4.1 Introduction

This chapter aims to set the results of the various stages of the project and discuss each one of them, individually. First the Simulation and Results for each stage that isn’t a chip, then the integrated hardware stages simulated after that results from hardware stages.

4.2 Simulation Results

The stages simulated were Multi-vibrator, Noise Generator, Summer and Clamper circuits.
4.2.1 Multi-Vibrator (Triangle Wave Generator)

The output for Triangle Wave generator as in section 3.4.2 is a triangle wave that gets integrated into a train of pulses. Output is shown in figures below in Spectrum analyzer plus EDA.

Figure 4.1: Triangle Wave from the EDA

Figure 4.2: Triangle Wave (Spectrum analyzer)
4.2.2 Noise Circuit Results

The output of noise circuit is the mentioned requirement in section 3.4.3.1 that covers the required portion band of spectrum. Let’s not forget that it’s a white noise.

Figure 4.3: Noise Output (EDA)

Figure 4.4: Noise (Spectrum Analyzer)
4.2.3 Summer Circuit Results

The talk about the summed signal will be the same talk about clamped signal after enlarging the amplitude a little bit to fit the required voltage to enter the RF section.

4.2.4 Clamper’s Output

![Clamper’s Output Graph]

We are taking here about a semi train pulse signal with some modification to adjust it for our purpose which is to provide the frequency that could be tolerated by the VCO in next stage.
4.2.5 RF Stage Output

The signal came out of the VCO after the frequency was tolerated as mentioned in section 3.6.4 as in the next figures:

More specifically these two figures show discrete captures to signals’ power spectrums coming from the GSM and DCS channels respectively.

Figure 4. 5: VCO

Figure 4. 6: GSM Channel Output
These signals were obtained after the modifications mentioned in sections 3.4.5.2.2 and 3.4.5.2.3 had been adjusted in MATLAB Simulink. The output varies in 100 KHz around both 900 MHz, 1800 MHz.

### 4.2.6 Antenna

Last stage is the broadcasting; which is done by the antenna that was supplied from previous stages; presented in two parameters:

#### 4.2.6.1 Antenna Return Loss

Calculated value as in section 3.4.8.2.1 was:

\[
\text{Return Loss (dB)} = 10 \log \left( \frac{P_{\text{incident}}}{P_{\text{reflected}}} \right)
\]

\[
\text{Return Loss (dB)} = -\, 0.45939
\]

assuming that the reflected wave has 30 dB power and the 12 volts we entered will give 34.59 dB.
4.2.6.2 Antenna VSWR

The gain we were talking about in section 3.4.8.2.6 was calculated as follows:

- Reflection Coefficient could be calculated from Return Loss as follows:
  \[ \Gamma = e^{(\text{Return Loss} + 20)} = e^{(-.45939 + 20)} = 3.0646 \times 10^8 \sim \infty \]

- Means that VSWR \sim 1 which is less than 2 as desired

4.3 A Jammed Signal

![Image of cellphone signal with jammer on and off]

*Figure 4. 8: Cellphone Signal when Jammer is : (a) On (b) Off*
Chapter Four

Results and Discussion

This page was left intentionally blank.
Chapter Five: Conclusions

5.1 Project Preview

The objective of this project was to design a cellphone jammer circuit for the 1G and 2G operators, with hardware part with high flexibility and minimum cost for University of Khartoum, Educational ground station and making it available for use or modification by students, graduates and researchers.

The design of the project was done under certain considerations as to properly fit to the system requirements.

The current implementation although is not perfectly completed but the result obtained is very satisfactory and gives an indication that this Cellphone Jammer Circuit with a little more work in the integration phase, that couldn’t be done because of the time consideration, will match the objectives exactly.

Cellphone Jammer is a basic electronic application to the fundamentals of RF-IF laws, power amplifier and noise calculations, and a basic communications engineering application to the fundamentals of GSM design and Antenna design,
that makes a very interesting and curiosity indulgent experiment for Students of University of Khartoum.

5.2 Future Work

Cellphone Jammer Circuit still requires more researches and development in both sections (hardware and software). For the current implementation further work should be done so that to meet the requirements, by placing the hardware components on a ready PCB circuit and connect them together as the PCB design to a personal computer with a different voltage levels utility. Some features and capabilities that can be added to extend the functionality in the future are:

- Making 3G, 4G and 5G implementations for hence project.
- Adding more controllers for the frequencies, voltages and other signal attributes.
- Provide a better output shape and some encapsulation to whole package.
- Extend the Bandwidths for next generations.
- Trying to minimize the size of PCB circuit as possible.
References

- Introduction to Digital Cellular, Motorola, for training professional only. 2001
- Open Information User Descriptions about Frequency Hopping, Ericsson.
- Rick Hartley, RF / Microwave PC Board Design and Layout, Avionics Systems.
- John Scourias, Overview of the Global System for Mobile Communications, University of Waterloo.
- Siwiak, K., Radio-wave propagation and Antennas for personal communication.
- Pozar, D., Microwave Engineering, John Wiley and Sons, 2005.
- "Frequency Planning And Frequency Coordination For The Gsm 900, Gsm 1800, E-Gsm And Gsm-R Land Mobile SysteMS (Except direct mode operation (DMO) channels)" by Working Group Frequency Management" (WGFM).
- Tony Van Roon, 555 timer tutorial.
Appendix A: Chips datasheets

NE555P Timer / LM555C Timer

---

**DESCRIPTION**
The 555 monostable timing circuit is a highly stable controller capable of producing accurate time delays, or oscillation. In the time delay mode of operation, the time is precisely controlled by one external resistor and capacitor. For a stable operation as an oscillator, the free running frequency and the duty cycle are both accurately controlled with two external resistors and one capacitor. The circuit may be triggered and reset on falling waveforms, and the output structure can source or sink up to 200 mA.

**FEATURES**
- Turn-off time less than 2 μs
- Max. operating frequency greater than 500 kHz
- Timing from microseconds to hours
- Operates in both astable and monostable modes
- High output current
- Adjustable duty cycle
- TTL compatible
- Temperature stability of 0.005% per °C

**APPLICATIONS**
- Precision timing
- Pulse generation
- Sequential timing
- Time delay generation
- Pulse width modulation

---

**PIN CONFIGURATION**

---

**BLOCK DIAGRAM**

---

**ORDERING INFORMATION**

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>TEMPERATURE RANGE</th>
<th>ORDER CODE</th>
<th>DWG #</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-Pin Plastic Small Outline (SO) Package</td>
<td>0 to +70 °C</td>
<td>NE555D</td>
<td>SOT96-1</td>
</tr>
<tr>
<td>8-Pin Plastic Dual In-Line Package (DIP)</td>
<td>0 to +70 °C</td>
<td>NE555N</td>
<td>SOT97-1</td>
</tr>
<tr>
<td>8-Pin Plastic Small Outline (SO) Package</td>
<td>-40 °C to +85 °C</td>
<td>8A555D</td>
<td>SOT96-1</td>
</tr>
<tr>
<td>8-Pin Plastic Dual In-Line Package (DIP)</td>
<td>-40 °C to +85 °C</td>
<td>8A555N</td>
<td>SOT97-1</td>
</tr>
<tr>
<td>8-Pin Plastic Dual In-Line Package (DIP)</td>
<td>-55 °C to +125 °C</td>
<td>8E555CN</td>
<td>SOT97-1</td>
</tr>
<tr>
<td>8-Pin Plastic Dual In-Line Package (DIP)</td>
<td>-55 °C to +125 °C</td>
<td>8E555N</td>
<td>SOT97-1</td>
</tr>
</tbody>
</table>
Appendix A

Phileps Semiconductors

Timer

NE/SA/SE555/SE555C

EQUIVALENT SCHEMATIC

Figure 3. Equivalent schematic

ABSOLUTE MAXIMUM RATINGS

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>PARAMETER Description</th>
<th>RATING</th>
<th>UNIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCC</td>
<td>Supply voltage</td>
<td>+18</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>NE555, NE555C, EA555</td>
<td>-16</td>
<td>V</td>
</tr>
<tr>
<td>Pp</td>
<td>Maximum allowable power dissipation</td>
<td>600</td>
<td>mW</td>
</tr>
<tr>
<td>TAMB</td>
<td>Operating ambient temperature range</td>
<td>NE555</td>
<td>0 to +70</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EA555</td>
<td>-40 to +85</td>
</tr>
<tr>
<td></td>
<td></td>
<td>85555</td>
<td>-55 to +125</td>
</tr>
<tr>
<td>TSTG</td>
<td>Storage temperature range</td>
<td>NE555</td>
<td>-65 to +150</td>
</tr>
<tr>
<td>TCOL</td>
<td>Lead soldering temperature (10 sec max)</td>
<td></td>
<td>+260</td>
</tr>
</tbody>
</table>

NOTE:
1. The junction temperature must be kept below 125 °C for the D package and below 150 °C for the N package.
2. At ambient temperatures above 25 °C, the ambient temperature rating should be decreased by the following factors:
   - D package 180 °C/W
   - N package 100 °C/W

2003 Feb 14
UA741 Op Amp

LM741
Single Operational Amplifier

Features
- Short circuit protection
- Excellent temperature stability
- Internal frequency compensation
- High input voltage range
- Null of offset

Description
The LM741 series are general purpose operational amplifiers. It is intended for a wide range of analog applications. The high gain and wide range of operating voltages provide superior performance in integrator, summing amplifier, and general feedback applications.

Internal Block Diagram

Rev. 1.0.1

©2001 Fairchild Semiconductor Corporation
### Electrical Characteristics

\( \text{Vcc} = 15\text{V}, \text{Vee} = -15\text{V}, \text{TA} = 25\degree C, \text{unless otherwise specified} \)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Symbol</th>
<th>Conditions</th>
<th>LM741/LM7411</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Min.</td>
</tr>
<tr>
<td>Input Offset Voltage</td>
<td>( V_{IO} )</td>
<td>( R_{G} \leq 10k \Omega )</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( R_{G} \leq 50k \Omega )</td>
<td>-</td>
</tr>
<tr>
<td>Input Offset Voltage Adjustment</td>
<td>( V_{IO(R)} )</td>
<td>( \text{Vcc} = \pm 120\text{V} )</td>
<td>15</td>
</tr>
<tr>
<td>Range</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Input Offset Current</td>
<td>( I_{IO} )</td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>Input Bias Current</td>
<td>( I_{BIAS} )</td>
<td></td>
<td>80</td>
</tr>
<tr>
<td>Input Resistance (Note 1)</td>
<td>( R_{i} )</td>
<td>( \text{Vcc} = \pm 20\text{V} )</td>
<td>2.0</td>
</tr>
<tr>
<td>Input Voltage Range</td>
<td>( V_{IN(R)} )</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>Large Signal Voltage Gain</td>
<td>( G_{V} )</td>
<td>( R_{L} \geq 2k \Omega )</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{Vcc} = \pm 120\text{V}, \text{V}_{\text{O}} (\text{P-P}) = \pm 15\text{V} )</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{Vcc} = \pm 15\text{V}, \text{V}_{\text{O}} (\text{P-P}) = \pm 10\text{V} )</td>
<td>20</td>
</tr>
<tr>
<td>Output Short Circuit Current</td>
<td>( I_{SC} )</td>
<td></td>
<td>25</td>
</tr>
<tr>
<td>Output Voltage Swing</td>
<td>( V_{O(P-P)} )</td>
<td>( \text{Vcc} = \pm 120\text{V} )</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( R_{L} \geq 10k \Omega )</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( R_{L} \geq 2k \Omega )</td>
<td>-</td>
</tr>
<tr>
<td>Common Mode Rejection Ratio</td>
<td>( CMRR )</td>
<td>( \text{Vcc} = \pm 15\text{V} )</td>
<td>70</td>
</tr>
<tr>
<td>Power Supply Rejection Ratio</td>
<td>( PSRR )</td>
<td>( \text{R}_{S} \leq 10k \Omega, \text{VCM} = \pm 12\text{V} )</td>
<td>77</td>
</tr>
<tr>
<td>Transient Response</td>
<td>( T_{R} )</td>
<td>( \text{unity gain} )</td>
<td>0.3</td>
</tr>
<tr>
<td>Overshoot</td>
<td>( O_{S} )</td>
<td>( \text{unity gain} )</td>
<td>10</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>( B_{W} )</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Slew Rate</td>
<td>( S_{R} )</td>
<td>( \text{unity gain} )</td>
<td>0.5</td>
</tr>
<tr>
<td>Supply Current</td>
<td>( I_{CC} )</td>
<td>( \text{R}_{L} = \pm 1 \Omega )</td>
<td>1.5</td>
</tr>
<tr>
<td>Power Consumption</td>
<td>( P_{C} )</td>
<td>( \text{Vcc} = \pm 20\text{V} )</td>
<td>50</td>
</tr>
</tbody>
</table>

**Note:**
1. Guaranteed by design.
Appendix A

LM386N Low Power Amplifier

Absolute Maximum Ratings (Note 2)
If Military/Aerospace specified devices are required, please contact the National Semiconductor Sales Office/Distribution for availability and specifications.

- Supply Voltage (Vdd) 15V (LM386N-1, -3, LM386M-1)
- Supply Voltage (Vdd) 22V (LM386N-4)
- Package Dissipation (Note 3) (LM386N) 1.25W
- Package Dissipation (Note 3) (LM386M) 0.73W
- Package Dissipation (Note 3) (LM386MM-1) 0.595W
- Input Voltage ±5V
- Storage Temperature -65°C to +150°C
- Operating Temperature 0°C to +70°C
- Junction Temperature +150°C
- Soldering Information

Dual-In-Line Package
- Soldering (10 sec) -260°C
- Small Outline Package (SOIC and MSOP)
  - Vapor Phase (60 sec) -215°C
  - Infrared (15 sec) -220°C

See AN-460 “Surface Mounting Methods and Their Effect on Product Reliability” for other methods of soldering surface mount devices.

Thermal Resistance
- θJA (DIP) 37°C/W
- θJA (SO Package) 10°C/W
- θJE (MSOP) 21°C/W
- θJE (MSOP) 5°C/W

Electrical Characteristics (Notes 1, 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Conditions</th>
<th>Min</th>
<th>Typ</th>
<th>Max</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Supply Voltage (Vdd)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LM386N-1, -3, LM386M-1, LM386MM-1</td>
<td>4</td>
<td>12</td>
<td></td>
<td></td>
<td>V</td>
</tr>
<tr>
<td>LM386N-4</td>
<td>5</td>
<td>18</td>
<td></td>
<td></td>
<td>V</td>
</tr>
<tr>
<td>Quiescent Current (Iq)</td>
<td>Vd = 6V, Vdd = 0</td>
<td>4</td>
<td>8</td>
<td></td>
<td>mA</td>
</tr>
<tr>
<td>Output Power (POUT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LM386N-1, LM386M-1, LM386MM-1</td>
<td>250</td>
<td>325</td>
<td></td>
<td></td>
<td>mW</td>
</tr>
<tr>
<td>LM386N-3</td>
<td>590</td>
<td>700</td>
<td></td>
<td></td>
<td>mW</td>
</tr>
<tr>
<td>LM386N-4</td>
<td>700</td>
<td>1000</td>
<td></td>
<td></td>
<td>mW</td>
</tr>
<tr>
<td>Voltage Gain (AV)</td>
<td>Vd = 6V, f = 1 kHz</td>
<td>26</td>
<td></td>
<td></td>
<td>dB</td>
</tr>
<tr>
<td></td>
<td>10 µF from Pins 1 to 8</td>
<td>46</td>
<td></td>
<td></td>
<td>dB</td>
</tr>
<tr>
<td>Bandwidth (BW)</td>
<td>Vd = 6V, Pins 1 and 8 Open</td>
<td>300</td>
<td></td>
<td></td>
<td>kHz</td>
</tr>
<tr>
<td>Total Harmonic Distortion (THD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vd = 6V, R = 8Ω, POUT = 12mW</td>
<td>0.2</td>
<td></td>
<td></td>
<td>%</td>
</tr>
<tr>
<td></td>
<td>f = 1 kHz, Pins 1 and 8 Open</td>
<td></td>
<td></td>
<td></td>
<td>%</td>
</tr>
<tr>
<td>Power Supply Rejection Ratio (PSRR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dB</td>
</tr>
<tr>
<td></td>
<td>Vd = 6V, f = 1 kHz, CSHORT = 10 µF</td>
<td>50</td>
<td></td>
<td></td>
<td>dB</td>
</tr>
<tr>
<td></td>
<td>Pins 1 and 8 Open, Referred to Output</td>
<td></td>
<td></td>
<td></td>
<td>dB</td>
</tr>
<tr>
<td>Input Resistance (Ri)</td>
<td>Vd = 6V, Pins 2 and 3 Open</td>
<td>50</td>
<td></td>
<td></td>
<td>kΩ</td>
</tr>
<tr>
<td>Input Bias Current (IIBIAS)</td>
<td>Vd = 6V, Pins 2 and 3 Open</td>
<td>250</td>
<td></td>
<td></td>
<td>nA</td>
</tr>
</tbody>
</table>

Note 1: All voltages are measured with respect to the ground pin, unless otherwise specified.

Note 2: Absolute Maximum Ratings indicates limits beyond which damage to the device may occur. Operating Ratings indicate conditions for which the device is functional, but do not guarantee specific performance limits. Electrical Characteristics state DC and AC electrical specifications under particular test conditions which guarantee specific performance limits. The above assumes that the device is within the Operating Ratings. Specifications are not guaranteed for parameters where no limit is given; however, the typical value is a good indication of device performance.

Note 3: For operation in ambient temperatures above 25°C, the device must be derated based on a 150°C maximum junction temperature and 1) a thermal resistance of 107°C/W junction to ambient for the dual-in-line package and 2) a thermal resistance of 117°C/W for the small outline package.

www.national.com
Appendix A

CVCO55CL
# Appendix A

## Voltage Controlled Oscillator - VCO

### CVCO55CL-0800-0980

### Performance Specification

<table>
<thead>
<tr>
<th>Specification</th>
<th>MIN</th>
<th>TYP</th>
<th>MAX</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower Frequency</td>
<td>800</td>
<td>MHz</td>
<td>800</td>
<td>MHz</td>
</tr>
<tr>
<td>Upper Frequency</td>
<td>980</td>
<td>MHz</td>
<td>980</td>
<td>MHz</td>
</tr>
<tr>
<td>Tuning Voltage</td>
<td>0.6</td>
<td>VDC</td>
<td>0.6</td>
<td>VDC</td>
</tr>
<tr>
<td>Supply Voltage</td>
<td>4.75</td>
<td>VDC</td>
<td>5.0</td>
<td>VDC</td>
</tr>
<tr>
<td>Output Power</td>
<td>0</td>
<td>dBm</td>
<td>+6.0</td>
<td>dBm</td>
</tr>
<tr>
<td>Supply Current</td>
<td>25</td>
<td>mA</td>
<td>25</td>
<td>mA</td>
</tr>
<tr>
<td>Harmonic Suppression (2nd Harmonic)</td>
<td>-22</td>
<td>dBc</td>
<td>-22</td>
<td>dBc</td>
</tr>
<tr>
<td>Pushing</td>
<td>2.0</td>
<td>MHz</td>
<td>MHz</td>
<td>MHz</td>
</tr>
<tr>
<td>Pulling, all Phases</td>
<td>2.0</td>
<td>MHz</td>
<td>MHz</td>
<td>MHz</td>
</tr>
<tr>
<td>Tuning Sensitivity</td>
<td>75</td>
<td>MHz</td>
<td>MHz</td>
<td>MHz</td>
</tr>
<tr>
<td>Phase Noise @ 10kHz offset</td>
<td>-99</td>
<td>dBc/Hz</td>
<td>-99</td>
<td>dBc/Hz</td>
</tr>
<tr>
<td>Phase Noise @ 100kHz offset</td>
<td>-121</td>
<td>dBc/Hz</td>
<td>-121</td>
<td>dBc/Hz</td>
</tr>
<tr>
<td>Load Impedance</td>
<td>50</td>
<td>ohm</td>
<td>ohm</td>
<td>ohm</td>
</tr>
<tr>
<td>Input Capacitance</td>
<td>47</td>
<td>pF</td>
<td>47</td>
<td>pF</td>
</tr>
<tr>
<td>Operating Temperature Range</td>
<td>-40</td>
<td>°C</td>
<td>-40</td>
<td>°C</td>
</tr>
<tr>
<td>Storage Temperature Range</td>
<td>-45</td>
<td>°C</td>
<td>-45</td>
<td>°C</td>
</tr>
</tbody>
</table>

### Phase Noise (1 Hz BW, Typical)

![Phase Noise Graph]

### Tuning Curve (Typical)

![Tuning Curve Graph]
### Voltage Controlled Oscillator (VCO) CVCO55BE-1785-1900

<table>
<thead>
<tr>
<th>Performance Specification</th>
<th>Min</th>
<th>Typ</th>
<th>Max</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower Frequency</td>
<td></td>
<td></td>
<td>1785 MHz</td>
<td></td>
</tr>
<tr>
<td>Upper Frequency</td>
<td>1800 MHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuning Voltage</td>
<td>0.3 VDC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Voltage</td>
<td>4.75 VDC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output Power</td>
<td>0 dBm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Current</td>
<td>35 mA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harmonic Suppression (2nd Harmonic)</td>
<td>-16 dBC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pushing</td>
<td>2.0 MHz/√V</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pulling, all Phases</td>
<td>3.0 MHz pk-pk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuning Sensitivity</td>
<td>45 MHz/√V</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phase Noise @ 10kHz offset</td>
<td>-100 dBc/Hz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phase Noise @ 100kHz offset</td>
<td>-122 dBc/Hz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Impedance</td>
<td>50 Ohm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Capacitance</td>
<td>100 pF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Temperature Range</td>
<td>-40°C to 85°C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Temperature Range</td>
<td>-40°C to 90°C</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Phase Noise (1 Hz BW, Typical)**

**Tuning Curve (Typical)**
### Pin Arrangement

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N/C</td>
</tr>
<tr>
<td>2</td>
<td>N/C</td>
</tr>
<tr>
<td>3</td>
<td>Pout DCS</td>
</tr>
<tr>
<td>4</td>
<td>Vdd DCS</td>
</tr>
<tr>
<td>5</td>
<td>Vdd GSM</td>
</tr>
<tr>
<td>6</td>
<td>Pout GSM</td>
</tr>
<tr>
<td>7</td>
<td>N/C</td>
</tr>
<tr>
<td>8</td>
<td>Vbilo</td>
</tr>
<tr>
<td>9</td>
<td>Pin GSM</td>
</tr>
<tr>
<td>10</td>
<td>Vapc GSM</td>
</tr>
<tr>
<td>11</td>
<td>Vapc DCS</td>
</tr>
<tr>
<td>12</td>
<td>Pin DCS</td>
</tr>
<tr>
<td>G</td>
<td>GND</td>
</tr>
</tbody>
</table>

---

### PF08109B

**Absolute Maximum Ratings (Tc = 25°C)**

<table>
<thead>
<tr>
<th>Item</th>
<th>Symbol</th>
<th>Rating</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply voltage</td>
<td>Vdd</td>
<td>8</td>
<td>V</td>
</tr>
<tr>
<td>Supply current</td>
<td>Idd_{GSM}</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>Idd_{DCS}</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>Vbilo voltage</td>
<td>Vbilo</td>
<td>4</td>
<td>V</td>
</tr>
<tr>
<td>Vapc voltage</td>
<td>Vapc</td>
<td>4</td>
<td>V</td>
</tr>
<tr>
<td>Input power</td>
<td>Pin</td>
<td>10</td>
<td>dBm</td>
</tr>
<tr>
<td>Operating case temp</td>
<td>T_{op}</td>
<td>−30 to +100</td>
<td>°C</td>
</tr>
<tr>
<td>Storage temp</td>
<td>T_{stg}</td>
<td>−30 to +100</td>
<td>°C</td>
</tr>
<tr>
<td>Output power</td>
<td>Pout_{GSM}</td>
<td>5</td>
<td>W</td>
</tr>
<tr>
<td></td>
<td>Pout_{DCS}</td>
<td>3</td>
<td>W</td>
</tr>
</tbody>
</table>

**Note:** The maximum ratings shall be valid over both the E-GSM-band (880 MHz to 915 MHz), and the DCS1800-band (1710 MHz to 1785 MHz).
## Appendix B: Components List

<table>
<thead>
<tr>
<th>Comment</th>
<th>Designator</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>250Ω</td>
<td>R1</td>
<td>1</td>
</tr>
<tr>
<td>750Ω</td>
<td>R2</td>
<td>1</td>
</tr>
<tr>
<td>2KΩ</td>
<td>R3,R4,R6</td>
<td>3</td>
</tr>
<tr>
<td>100KΩ</td>
<td>R5</td>
<td>1</td>
</tr>
<tr>
<td>10KΩ</td>
<td>R7</td>
<td>1</td>
</tr>
<tr>
<td>1KΩ</td>
<td>R8,R9</td>
<td>2</td>
</tr>
<tr>
<td>2KΩ</td>
<td>R10</td>
<td>1</td>
</tr>
<tr>
<td>0.1μF</td>
<td>C1,C3,C4,C5,C6,C7,C9</td>
<td>7</td>
</tr>
<tr>
<td>1nF</td>
<td>C2,C15,C16</td>
<td>3</td>
</tr>
<tr>
<td>10μF</td>
<td>C8,C10</td>
<td>2</td>
</tr>
<tr>
<td>4.7μF</td>
<td>C11,C13</td>
<td>2</td>
</tr>
<tr>
<td>0.01μF</td>
<td>C12,C14</td>
<td>2</td>
</tr>
<tr>
<td>NE555P/LM555C</td>
<td>IC1</td>
<td>1</td>
</tr>
<tr>
<td>LM741/UA741C</td>
<td>IC2</td>
<td>1</td>
</tr>
<tr>
<td>LM386N</td>
<td>IC3</td>
<td>1</td>
</tr>
<tr>
<td>PF08190B</td>
<td>IC4,IC5</td>
<td>2</td>
</tr>
<tr>
<td>CVCO55BE</td>
<td>IC6</td>
<td>1</td>
</tr>
<tr>
<td>CVCO55CL</td>
<td>IC7</td>
<td>1</td>
</tr>
<tr>
<td>2N3904</td>
<td>T1</td>
<td>1</td>
</tr>
<tr>
<td>1N4148</td>
<td>D1,D2</td>
<td>2</td>
</tr>
<tr>
<td>6.8V</td>
<td>ZD1</td>
<td>1</td>
</tr>
<tr>
<td>850MHz-1GHz, 50 Ω, VSWR&lt;2</td>
<td>Antenna1</td>
<td>1</td>
</tr>
<tr>
<td>1700MHz-1900MHz, 50 Ω, VSWR&lt;2</td>
<td>Antenna2</td>
<td>1</td>
</tr>
</tbody>
</table>
Appendix C: Abbreviation Absolute Radio Frequency Channel Number (ARFCN)

(a code that specifies a pair of physical radio carriers used for transmission and reception in a land mobile radio system, one for the uplink signal and one for the downlink signal).

To calculate the ARFCN from frequency the following method is used:

$$\text{ARFCN} = \frac{f - f_b - f_o}{f_c}$$

Where:

- $f$ is the actual frequency [MHz]
- $f_b$ is the base frequency [MHz]
- $f_o$ is the offset frequency [MHz]
- $f_c$ is the channel spacing frequency [MHz]

**ARFCN Table for Common GSM Systems**

<table>
<thead>
<tr>
<th>Band</th>
<th>Designation</th>
<th>ARFCN</th>
<th>FUL</th>
<th>FDL</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM 500</td>
<td>GSM 450</td>
<td>259-293</td>
<td>450.6 + 0.2 (n-259)</td>
<td>FUL(n) + 10</td>
</tr>
<tr>
<td></td>
<td>GSM 480</td>
<td>306-430</td>
<td>419.0 + 0.2 (n-306)</td>
<td>FUL(n) + 10</td>
</tr>
<tr>
<td>GSM 700</td>
<td>GSM 750</td>
<td>438-511</td>
<td>747.2 + 0.2 (n-438)</td>
<td>FUL(n) + 30</td>
</tr>
<tr>
<td>GSM 850</td>
<td>GSM 850</td>
<td>128-251</td>
<td>824.2 + 0.2 (n-128)</td>
<td>FUL(n) + 45</td>
</tr>
<tr>
<td>GSM 900</td>
<td>P-GSM</td>
<td>1-124</td>
<td>890.0 + 0.2 n</td>
<td>FUL(n) + 45</td>
</tr>
<tr>
<td></td>
<td>E-GSM</td>
<td>0-124</td>
<td>890.0 + 0.2 n</td>
<td>FUL(n) + 45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>975-1023</td>
<td>890.0 + 0.2 (0-1024)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GSM-R</td>
<td>0-124</td>
<td>890.0 + 0.2 n</td>
<td>FUL(n) + 45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>955-1023</td>
<td>890.0 + 0.2 (n-1024)</td>
<td></td>
</tr>
<tr>
<td>GSM 1800</td>
<td>DCS 1800</td>
<td>512-885</td>
<td>1710.2 + 0.2 (n-512)</td>
<td>FUL(n) + 95</td>
</tr>
<tr>
<td>GSM 1900</td>
<td>PCS 1900</td>
<td>512-810</td>
<td>1850.2 + 0.2 (n-512)</td>
<td>FUL(n) + 80</td>
</tr>
</tbody>
</table>
Appendix D: PCB Drilling Details (IF-SECTION)

%FSDAX23Y23%
%MOIN%
%SFA1B1%

%IPPOS%
%ADD9500C,0.027559%
%ADD9501C,0.033465%
%ADD9502C,0.035433%

%LNpcb1-1%
%LPD%

G54D9500*
X01255Y01375D03*
X01945Y01170D03*
X02245D03*
X02510D03*
Y01470D03*
X02300Y01965D03*
X02095D03*
X01880D03*
Y02265D03*

X02485D03*
X02485D03*
Y02485D03*

X02265D03*
X02265D03*

X01965D03*
X01965D03*

Y01965D03*

X01515D03*
X01345D03*

X02300D03*
Y02265D03*
X01515D03* X02250Y02724D03*
X01430Y01605D03* Y02824D03*
X01425Y03275D03* Y02924D03*
X01240D03* Y03024D03*
Y03675D03* X02549D03*
X01425D03* Y02924D03*
Y03575D03* Y02824D03*
Y03975D03* Y02724D03*
X02010Y03735D03* X01180Y02165D03*
X02150Y03835D03* Y02065D03*
Y03435D03* Y01965D03*
X02010D03* X01240Y03895D03*
G54D9502* Y03995D03*
X01553Y01386D03* Y04095D03*
X01603D03* X01575Y03735D03*
X01653D03* Y03635D03*
X01949Y01420D03* Y03535D03*
X02049D03* Y03435D03*
X02149D03* X01875D03*
X02249D03* Y03535D03*
Y01719D03* Y03635D03*
X02149D03* Y03735D03*
X02049D03* M02*
X01949D03*
Appendix E: RF Section Block Diagram