GSM JAMMER

Project Report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology in

Electronics and Communication Engineering

under the Supervision of

PROF. D.C. KULSHRESHTHA

By

ABHISHEK MANOHAR CHELLANI (091057)

SAIYAM TAKKAR (091110)

YASHASVI NIJHAWAN (091123)

Jaypee University of Information and Technology

Waknaghat, Solan – 173234, Himachal Pradesh

CERTIFICATE

This is to certify that project report entitled " JAMMER ", submitted by Abhishek Manohar Chelani , Saiyam Takkar and Yashasvi Nijhawan in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communication Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

12th May,2013

PROF. D.C. KULSHRESHTHA

PROFESSOR

ACKNOWLEDGEMENT

Working on this project has been a great learning experience for us as it provided a brisk and viable experience to us. Our experience while working in this project ranges from the moment of anxiety, when we could not solve for several days, to moments of ecstasy when after struggling for several days we were ultimately able to find solution to our problems. It would not have been possible for us to work on this project without the help of many people. We would like to express our gratitude to all of them but some omissions are inevitable.

It is said that behind the accomplishment of any effort there are some dedicated individuals who put in their best to get the job done. Firstly, we would like to express our appreciation and gratitude to our esteemed project guide **Professor D.C. KULSHRESHTHA** for the endless hours of help, suggestions, ideas and advice during the development of this project. Their technical know-how in this subject is only surpassed by their experience. Secondly, we would like to thank **Mr. BHASKER GUPTA** for the practical knowledge he gave us.

We are also grateful to all the faculty members for their sincere remarks and suggestions about our project and grateful for their time to time useful and productive suggestions. We are also expressing our gratitude towards the laboratory technician **Mr. Manoj Pandey** for his valuable efforts in the laboratory that has provided our project to get on to a platform.

Abhishek Manohar Chellani (091057)

Saiyam Takkar (091110)

Yashasvi Nijhawan (091123)

TABLE OF CONTENTS

Contents

LIST OF FIGURES AND TABLES

ABSTRACT

Cell Phone Jammer is an instrument to prevent cellular phone from receiving and transmitting the mobile signals to the base station. Unfortunately, in all places such as church, mosque, library, movie theatres and meeting room because not all cell-phone users know that they should not use their cell-phones. Hence here arises the need of a cell phone jammer

Cell phone jamming devices were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists. The cell phone Jammers are now a necessity for accomplishing a more cultured society because there is a growing demand for silence at places like hospital, libraries and movie theatres. Nowadays, there is a wide range of cell phone jammers starting from a pocket sized to as big as to jam an entire sport area.

Working of Cellular and How to Jam it

In order to explain how cellular jammers work we need to understand first how mobile phones work. A cellular phone keeps communicating with cellular base stations every several minutes by transmitting "alive" signal with ID code. This notifies cellular network that our cellular phone is ON and in coverage area.

Now imagine that the PAN ID of the tower is changed and tower is not able to receive the “alive” signal. The communication between base station and cellular phone cuts-off and the cellular phone will be totally blocked. Therefore the receiver in cellular phone "thinks" that cellular phone is not in coverage area. After 20-60 seconds mobile's phone display will show "NO SERVICE" or "Searching for network". From this point of time the cellular phone will not be able to receive incoming call or dial outgoing call. However, cellular phone will be able to communicate again after switch off the cellular jammer.

CHAPTER 1

GSM

1.1 INTRODUCTION

GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile), is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones. It became the de facto global standard for mobile communications with over 80% market share.

The GSM standard was developed as a replacement for first generation (1G) analog cellular networks, and originally described a digital, circuit switched network optimized for full duplex voice telephony. This was expanded over time to include data communications, first by circuit switched transport, then packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution or EGPRS).

Further improvements were made when the 3GPP developed third generation (3G) UMTS standards followed by fourth generation (4G) LTE Advanced standards.

"GSM" is a trademark owned by the GSM Association.

1.2 HISTORY

Early European analog cellular networks consisted of a mix of technologies and protocols that varied from country to country, meaning that phones did not necessarily work on different networks. In addition, manufacturers had to produce different equipment to meet various standards across the markets.

In 1982, work began to develop a European standard for digital cellular voice telephony when the European Conference of Postal and Telecommunications Administrations (CEPT) created the Groupe Spécial Mobile committee and later provided a permanent group of technical support personnel, based in Paris. Five years later in 1987, 15 representatives from 13 European countries signed a memorandum of understanding in Copenhagen to develop and deploy a common cellular telephone system across Europe, and European Union rules were passed to make GSM a mandatory standard.[1] The decision to develop a continental standard eventually resulted in a unified, open, standard-based network which was larger than that in the United States. In 1989, the Groupe Spécial Mobile committee was transferred from CEPT to the European Telecommunications Standards Institute(ETSI).

In 1987 Europe produced the very first agreed GSM Technical Specification (February). Ministers from the 4 big EU countries cemented their political support for GSM with the Bonn Minister's Declaration (May) and the GSM MoU was tabled for signature (September). The MoU drew-in mobile operators from across Europe to pledge to invest in new GSM networks to an ambitious common date. It got GSM up and running fast.

In this short 37 week period the whole of Europe (countries and industries) had been brought behind GSM in a rare unity and speed guided by four public officials Armin Silberhorn (Germany), Stephen Temple (UK), Philippe Dupuis (France) and Renzo

Failli (Italy). In 1989, the Groupe Spécial Mobile committee was transferred from CEPT to the European Telecommunications Standards Institute (ETSI).

In parallel, France and Germany signed a joint development agreement in 1984 and were joined by Italy and the UK in 1986. In 1986 the European Commission proposed reserving the 900 MHz spectrum band for GSM.

Phase I of the GSM specifications were published in 1990. The world's first GSM call was made by the former Finnish prime minister Harri Holkeri to Kaarina Suonio (mayor in city of Tampere) on 1 July 1991 on a network built by Telenokia and Siemens and operated by Radiolinja. The following year in 1992, the first short messaging service (SMS or "text message") message was sent and Vodafone UK and Telecom Finland signed the first international roaming agreement.

Work began in 1991 to expand the GSM standard to the 1800 MHz frequency band and the first 1800 MHz network became operational in the UK by 1993. Also that year, Telecom Australia became the first network operator to deploy a GSM network outside Europe and the first practical hand-held GSM mobile phone became available.

In 1995, fax, data and SMS messaging services were launched commercially, the first 1900 MHz GSM network became operational in the United States and GSM subscribers worldwide exceeded 10 million. Also this year, the GSM Association was formed. Pre-paid GSM SIM cards were launched in 1996 and worldwide GSM subscribers passed 100 million in 1998.

In 2000, the first commercial GPRS services were launched and the first GPRS compatible handsets became available for sale. In 2001 the first UMTS (W-CDMA) network was launched and worldwide GSM subscribers exceeded 500 million. In 2002 the first multimedia messaging services (MMS) were introduced and the first GSM network in the 800 MHz frequency band became operational. EDGE services first became operational in a network in 2003 and the number of worldwide GSM subscribers exceeded.1 billion in 2004.

By 2005, GSM networks accounted for more than 75% of the worldwide cellular network market, serving 1.5 billion subscribers. In 2005, the first HSDPA capable network also became operational. The first HSUPA network was launched in 2007 and worldwide GSM subscribers exceeded two billion in 2008.

The GSM Association estimates that technologies defined in the GSM standard serve 80% of the global mobile market, encompassing more than 5 billion people across more than 212 countries and territories, making GSM the most ubiquitous of the many standards for cellular networks.

Macau planned to phase out their GSM networks on June 4, 2015, making it the first region to decommission a GSM network.

1.3 NETWORK STRUCTURE

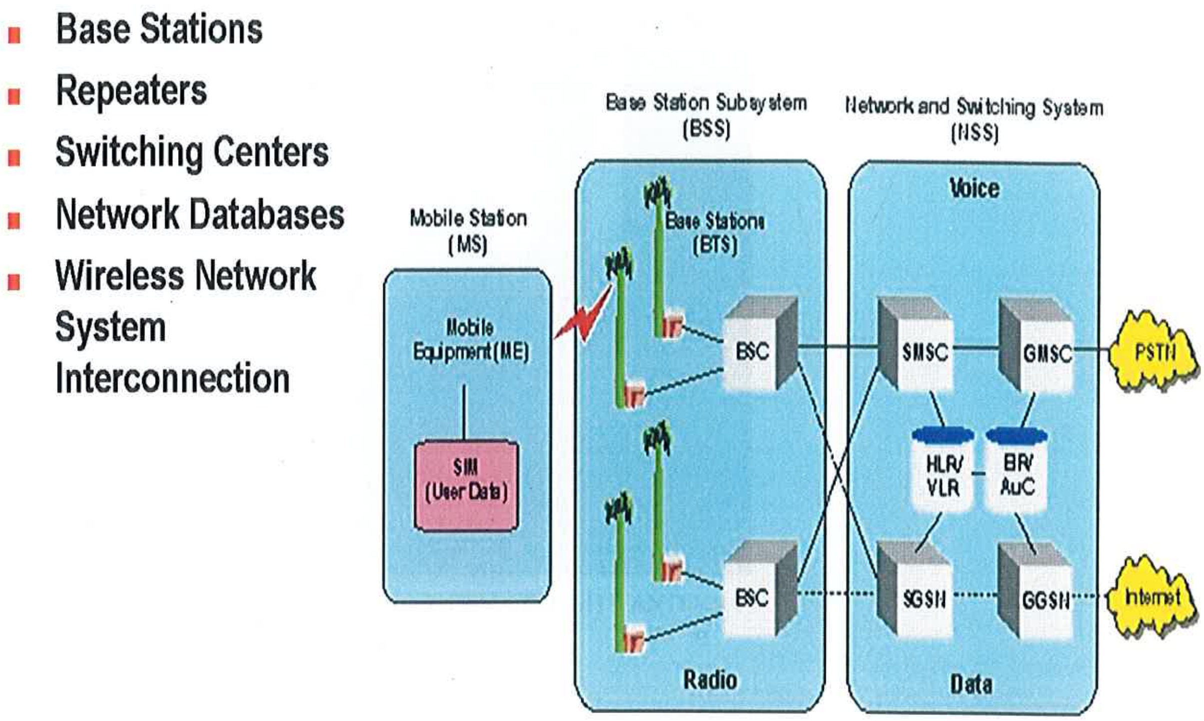

FIGURE 1.1: NETWORK STRUCTURE

The structure of a GSM network

The network is structured into a number of discrete sections:

- The Base Station Subsystem (the base stations and their controllers).
- The Network and Switching Subsystem (the part of the network most similar to a fixed network). This is sometimes also just called the core network.
- The GPRS Core Network (the optional part which allows packet based Internet connections).
- The Operations support system (OSS) for maintenance of the network.

1.4 Base Station subsystem

FIGURE 1.2: GSM CELL SITE ANTENNA

GSM cell site antennas in the Deutsches Museum, Munich, Germany

GSM is a cellular network, which means that cell phones connect to it by searching for cells in the immediate vicinity. There are five different cell sizes in a GSM network—macro, micro, pico, femto and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average roof top level. Micro cells are cells whose antenna height is under average roof top level; they are typically used in urban areas. Picocells are small cells whose coverage diameter is a few dozen metres; they are mainly used indoors. Femtocells are cells designed for use in residential or small business environments and connect to the service provider's network via a broadband internet connection. Umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.

Cell horizontal radius varies depending on antenna height, antenna gain and propagation conditions.from a couple of hundred meters to several tens of kilometers. The longest distance the GSM specification supports in practical use is 35 kilometers (22 mi). There are also several implementations of the concept of an extended cell, where the cell radius could be double or even more, depending on the antenna system, the type of terrain and the timing advance.

Indoor coverage is also supported by GSM and may be achieved by using an indoor Pico cell base station, or an indoor repeater with distributed indoor antennas fed through power splitters, to deliver the radio signals from an antenna outdoors to the separate indoor distributed antenna system. These are typically deployed when a lot of call capacity is needed indoors; for example, in shopping centers or airports. However, this is not a prerequisite, since indoor coverage is also provided by in-building penetration of the radio signals from any nearby cell.

1.5 GSM carrier frequencies

GSM networks operate in a number of different carrier frequency ranges (separated into GSM frequency ranges for 2G and UMTS frequency bands for 3G), with most 2G GSM networks operating in the 900 MHz or 1800 MHz bands. Where these bands were already allocated, the 850 MHz and 1900 MHz bands were used instead (for example in Canada and the United States). In rare cases the 400 and 450 MHz frequency bands are assigned in some countries because they were previously used for first-generation systems.

Most 3G networks in Europe operate in the 2100 MHz frequency band. For more information on worldwide GSM frequency usage, see GSM frequency bands.

Regardless of the frequency selected by an operator, it is divided into timeslots for individual phones to use. This allows eight full-rate or sixteen half-rate speech channels per radio frequency. These eight radio timeslots (or eight burst periods) are grouped into a TDMA frame. Half rate channels use alternate frames in the same timeslot. The channel data rate for all 8 channels is 270.833 Kbit/s, and the frame duration is 4.615 ms.

The transmission power in the handset is limited to a maximum of 2 watts in GSM 850/900 and 1 watt in GSM 1800/1900.

1.6 Subscriber Identity Module (SIM)

One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM card. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the user to retain his or her information after switching handsets. Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as SIM locking.

1.7 Phone locking

Sometimes mobile network operators restrict handsets that they sell for use with their own network. This is called locking and is implemented by a software feature of the phone. A subscriber may usually contact the provider to remove the lock for a fee, utilize private services to remove the lock, or make use of free or fee-based software and websites to unlock the handset themselves. Unlocking a phone without an operator's consent is illegal in many countries and may carry severe penalties.

In some countries

(e.g., Bangladesh, Brazil, Chile, HongKong, India, Lebanon, Malaysia, Pakistan, Sing apore) all phones are sold unlocked. In others (e.g., Singapore) it is unlawful for operators to offer any form of subsidy on a phone's price.

1.8 GSM service security

GSM was designed with a moderate level of service security. The system was designed to authenticate the subscriber using a pre-shared key and challenge-response. Communications between the subscriber and the base station can be encrypted. The development of UMTS introduces an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user – whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation.

GSM uses several cryptographic algorithms for security.
The A5/1, A5/2 and A5/3 stream ciphers are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in other countries. Serious weaknesses have been found in both algorithms: it is possible to break A5/2 in real-time with a cipher text-only attack, and in January 2007, The Hacker's Choice started the A5/1 cracking project with plans to use FPGAs that allow A5/1 to be broken with a rainbow table attack. The system supports multiple algorithms so operators may replace that cipher with a stronger one.

On 28 December 2009 German computer engineer Karsten Nohl announced that he had cracked the A5/1 cipher. According to Nohl, he developed a number of rainbow tables (static values which reduce the time needed to carry out an attack) and have found new sources for known plaintext attacks. He also said that it is possible to build "a full GSM interceptor ... from open source components" but that they had not done so because of legal concerns. Nohl claimed that he was able to intercept voice and text conversations by impersonating another user to listen to their voice mails, make calls or send text messages using a seven-year-old Motorola cell phone and decryption software available free off the Internet.

New attacks have been observed that take advantage of poor security implementations, architecture and development for smart phone applications. Some wiretapping and eavesdropping techniques hijack the audio input and output providing an opportunity for a 3rd party to listen in to the conversation.

GSM uses General Packet Radio Service (GPRS) for data transmissions like browsing the web. The most commonly deployed GPRS ciphers were publicly broken in 2011.

The researchers revealed flaws in the commonly used GEA/1 and GEA/2 ciphers and published the open source "gprs decode" software for sniffing GPRS networks. They also noted that some carriers don't encrypt the data at all (i.e. using GEA/0) in order to detect the use of traffic or protocols they don't like, e.g. Skype, leaving their customers unprotected. GEA/3 seems to remain relatively hard to break and is said to be in use on some more modern networks. If used with USIM to prevent connections to fake base stations and downgrade attacks, users will be protected in the medium term, though migration to 128-bit GEA/4 is still recommended.

CHAPTER 2

DEVELOPMENT BOARD

2.1 INTRODUCTION

Development Board Features are:

- 40 Pin Atmel ATmega16 microcontroller with internal system clock upto 8 MHz and externally upto 16 MHz
- 16 kb Flash RAM memory for programs
- One 16 Pin header to connect 16*2 alphanumeric LCD
- Dual 7805 Voltage regulator
- Dual power input options (Through molex connector or through DC Jack)
- Two programmable micro-switches
- Two programmable LEDs

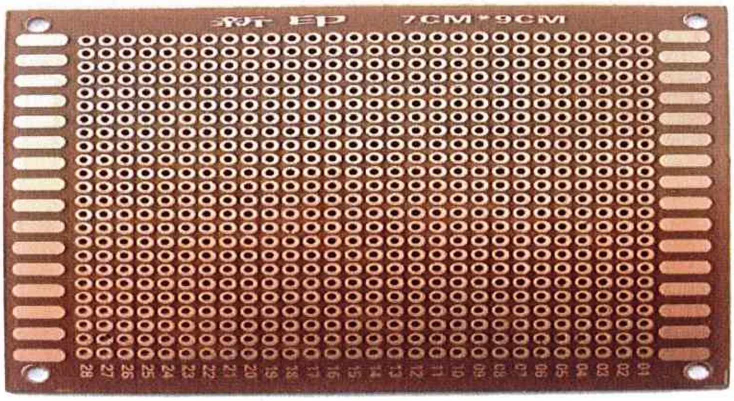

FIGURE 2.1: DEVELOPMENT BOARD

2.2 DEVELOPMENT BOARD PRINTING

- Printed circuit board has been developed using the EAGLE (**E**asily **A**pplicable **G**raphical **L**ayout **E**ditor) software.

- After designing the circuit on the EAGLE we took a print out of it on a glossy paper.

- We dipped the circuit into a solution of $fecl_3$.

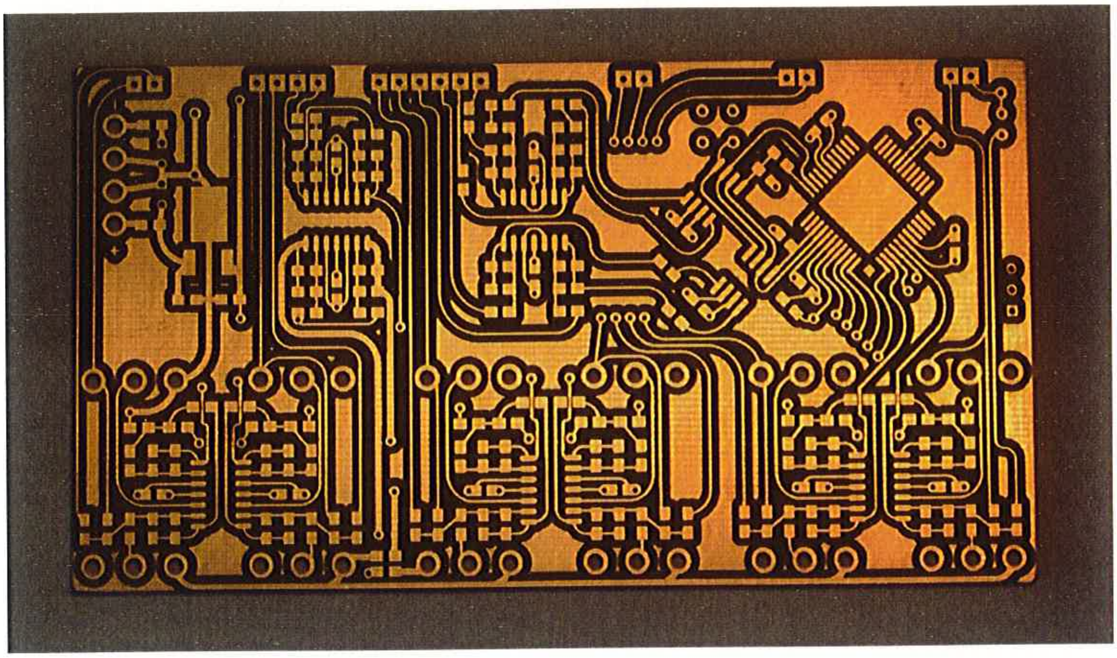

FIGURE 2.2: PRINTED CIRCUIT BOARD

2.3 CIRCUIT DIAGRAM

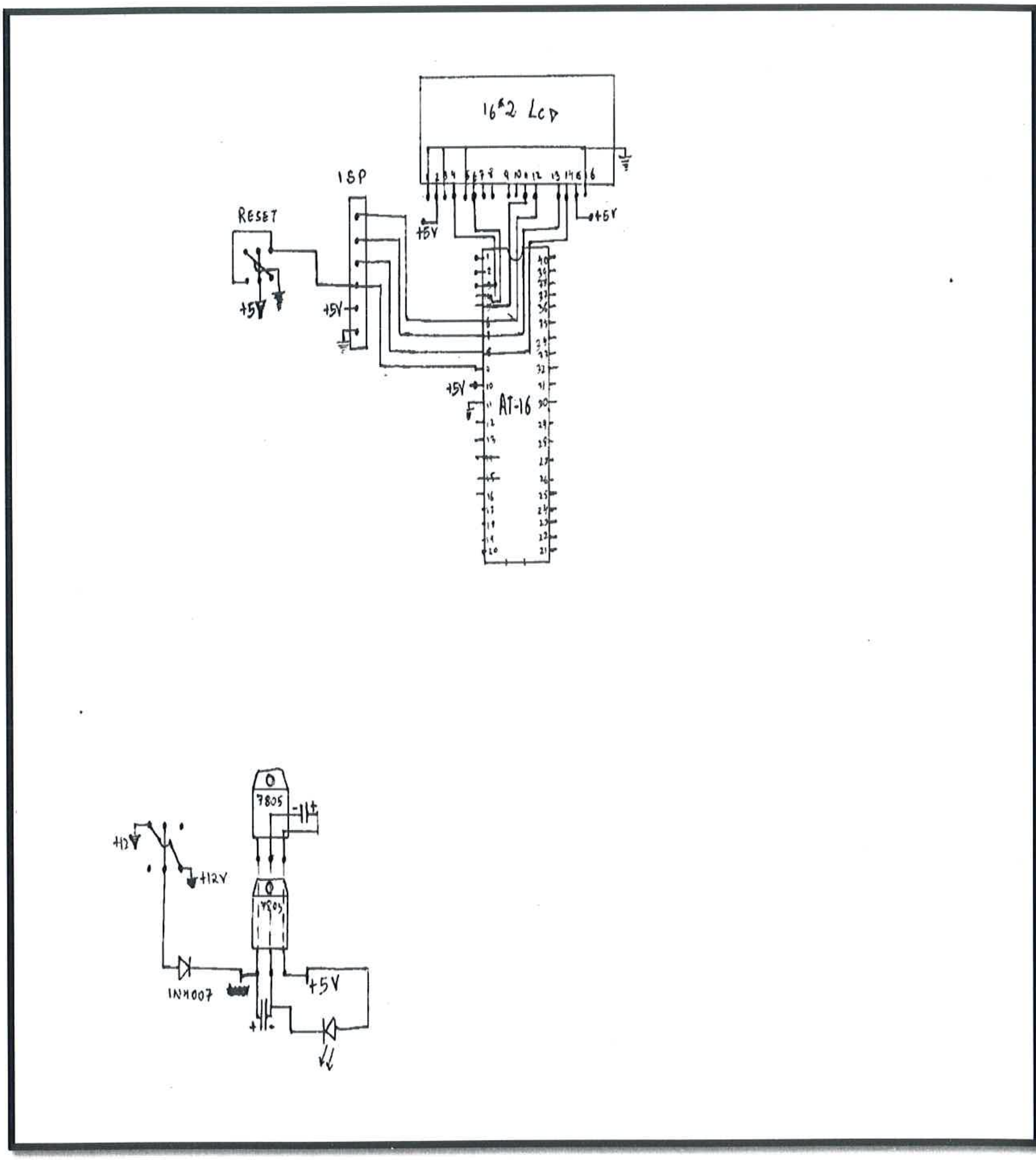

FIGURE 2.3: CIRCUIT DIAGRAM

2.4 MICROCONTROLLER BOARD

2.4.1 Supply Section:

The Microcontroller has Voltage Regulator IC7805 which converts the 12 volts supply to 5 volts.

2.4.2 Power Supply Section Designing

- The power section consists of Regulator 7805.
- The adaptor is connected to 220 volts AC household supply, and this supply is converted to 12 volts DC supply.

The 12-V (DC) is fed to a diode, so that there is no backflow of current. Further the supply is fed to a 0.33 μF capacitor, to avoid voltage spike. This supply is then connected to the first pin of Voltage Regulator 7805.

- 7805 converts this supply into 5 V (DC)
- The 5 V supply is obtained from the 3rd pin of 7805
- Again the 5 V supply is fed to 0.33μF capacitor

An LED is connected to check whether the supply is available or not.

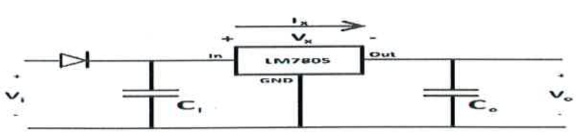

FIGURE 2.4: POWER SUPPLY

CHAPTER 3

MICROCONTROLLER

3.1 INTRODUCTION

A microcontroller (sometimes abbreviated µC, uC or MCU) is a small computer on a single integrated circuit containing a processor core, memory, and programmable input/output peripherals. Program memory in the form of NOR flash or OTP ROM and a typically small amount of RAM is also often included on chip.

Microcontrollers are designed for embedded applications, in contrast to the microprocessors used in personal computers or other general purpose applications. Microcontrollers are used in automatically controlled products and devices, such as automobile engine control systems, implantable medical devices, remote controls, office machines, appliances, power tools, toys and other embedded systems. By reducing the size and cost compared to a design that uses a separate microprocessor, memory, and input/output devices, microcontrollers make it economical to digitally control even more devices and processes. Mixed signal microcontrollers are common, integrating analog components needed to control non-digital electronic systems.

3.2 AVR FAMILY

The AVR is a modified Harvard architecture 8-bit RISC single chip microcontroller which was developed by Atmel in 1996. The AVR was one of the first microcontroller families to use on chip flash memory for program storage, as opposed to one-time programmable ROM, EPROM, or EEPROM used by other microcontrollers at the time.

3.2.1 Atmega16

ATmega16 is an 8-bit high performance microcontroller of Atmel's Mega AVR family with low power consumption. Atmega16 is based on enhanced RISC (Reduced Instruction Set Computing) architecture with 131 powerful instructions. Most of the instructions execute in one machine cycle. Atmega16 can work on a maximum frequency of 16 MHz

ATmega16 has 16 kb programmable flash memory, static RAM of 1 kb and EEPROM of 512 bytes. The endurance cycle of flash memory and EEPROM is 10,000 and 100,000, respectively. ATmega16 is a 40-pin microcontroller. There are 32 I/O (input/output) lines which are divided into four 8-bit ports designated as PORTA, PORTB, PORTC and PORTD.

ATmega16 has various in-built peripherals like USART, ADC, Analog Comparator, SPI, JTAG, etc. Each I/O pin has an alternative task related to in-built Peripherals. The following table shows the pin description of ATmega16.

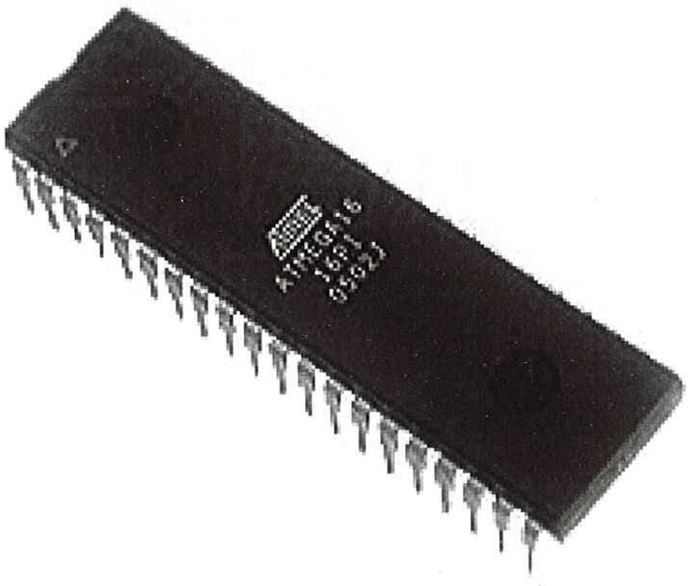

FIGURE 3.1: ATMEGA16 MICROCONTROLLER

3.2.1.1 Pin Diagram of Atmega16

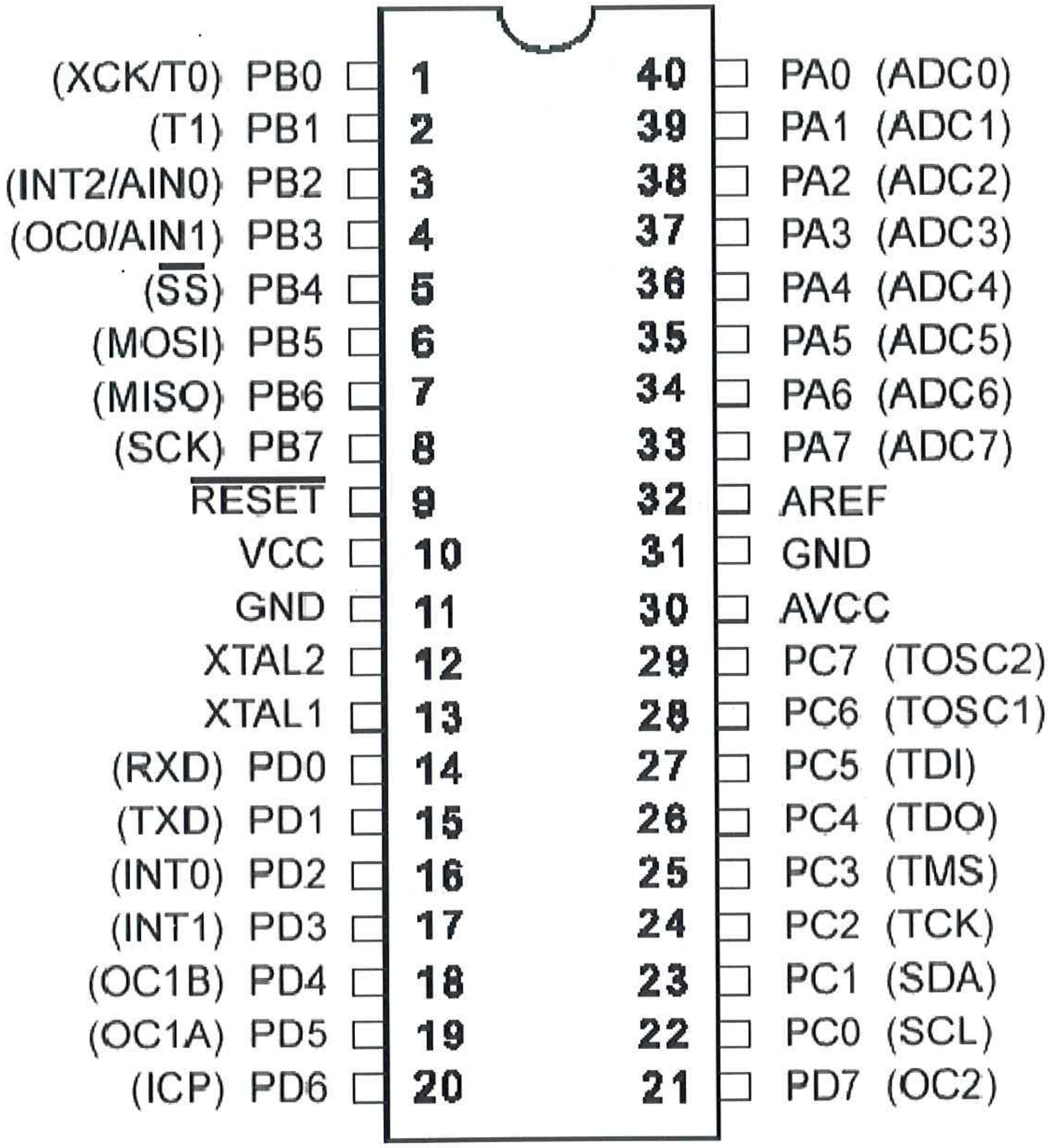

FIGURE 3.1b : PIN DIAGRAM OF ATMEGA16

3.2.1.2 Pin Description of Atmega16

S.No.	Pin Name	Description	Function
1	(XCK/T0) PB0	I/O PORTB, Pin 0	T0: Timer0 External Counter Input. XCK : USART External Clock I/O
2	(T1) PB1	I/O PORTB, Pin 1	T1:Timer1 External Counter Input
3	(INT2/AIN0) PB2	I/O PORTB, Pin 2	AIN0: Analog Comparator Positive I/P INT2: External Interrupt 2 Input
4	(OC0/AIN1) PB3	I/O PORTB, Pin 3	AIN1: Analog Comparator Negative I/P OC0 : Timer0 Output Compare Match Output
5	(SS) PB4	I/O PORTB, Pin 4	In System Programmer (ISP) Serial Peripheral Interface (SPI)
6	(MOSI) PB5	I/O PORTB, Pin 5	
7	(MISO) PB6	I/O PORTB, Pin 6	
8	(SCK) PB7	I/O PORTB, Pin 7	
9	RESET	Reset Pin, Active Low Reset	
10	V_{cc}	V_{cc} = +5 V	
11	GND	GROUND	
12	XTAL2	Output to Inverting Oscillator Amplifier	
13	XTAL1	Input to Inverting Oscillator Amplifier	
14	(RXD) PD0	I/O PORTD, Pin 0	USART Serial Communication Interface
15	(TXD) PD1	I/O PORTD, Pin 1	

16	(INT0) PD2	I/O PORTD, Pin 2	External Interrupt INT0
17	(INT1) PD3	I/O PORTD, Pin 3	External Interrupt INT1
18	(OC1B) PD4	I/O PORTD, Pin 4	PWM Channel Outputs
19	(OC1A) PD5	I/O PORTD, Pin 5	
20	(ICP) PD6	I/O PORTD, Pin 6	Timer/Counter1 Input Capture Pin
21	PD7 (OC2)	I/O PORTD, Pin 7	Timer/Counter2 Output Compare Match Output
22	PC0 (SCL)	I/O PORTC, Pin 0	TWI Interface
23	PC1 (SDA)	I/O PORTC, Pin 1	
24	PC2 (TCK)	I/O PORTC, Pin 2	JTAG Interface
25	PC3 (TMS)	I/O PORTC, Pin 3	
26	PC4 (TDO)	I/O PORTC, Pin 4	
27	PC5 (TDI)	I/O PORTC, Pin 5	
28	PC6 (TOSC1)	I/O PORTC, Pin 6	Timer Oscillator Pin 1
29	PC7 (TOSC2)	I/O PORTC, Pin 7	Timer Oscillator Pin 2
30	AV_{cc}	Voltage Supply = V_{cc} for ADC	
31	GND	GROUND	
32	AREF	Analog Reference Pin for ADC	
33	PA7 (ADC7)	I/O PORTA, Pin 7	ADC Channel 7
34	PA6 (ADC6)	I/O PORTA, Pin 6	ADC Channel 6

35	PA5 (ADC5)	I/O PORTA, Pin 5	ADC Channel 5
36	PA4 (ADC4)	I/O PORTA, Pin 4	ADC Channel 4
37	PA3 (ADC3)	I/O PORTA, Pin 3	ADC Channel 3
38	PA2 (ADC2)	I/O PORTA, Pin 2	ADC Channel 2
39	PA1 (ADC1)	I/O PORTA, Pin 1	ADC Channel 1
40	PA0 (ADC0)	I/O PORTA, Pin 0	ADC Channel 0

TABLE 3.1 : MICROCONTROLLER PIN DESCRIPTION

CHAPTER 4

Liquid Crystal Display

4.1 INTRODUCTION

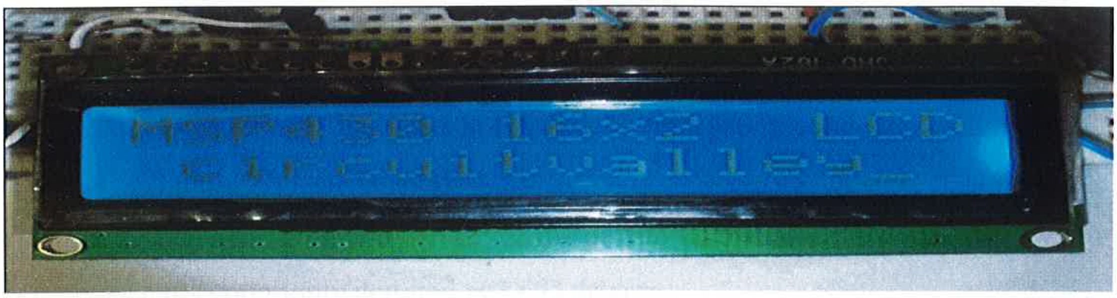

FIGURE 4.1: LCD

LCD (Liquid Crystal Display) that uses the light modulating properties of liquid crystals. LCD displays utilize two sheets of polarizing material with a liquid crystal solution between them. An electric current passed through the liquid causes the crystals to align so that light cannot pass through them. Each crystal, therefore, is like a shutter, either allowing light to pass through or blocking the light.

An LCD monitor consists of five layers: a backlight, a sheet of polarized glass, a "mask" of pixels, a layer of liquid crystal solution responsive to a wired grid of x, y coordinates, and a second polarized sheet of glass. By manipulating the orientations of crystals through precise electrical charges of varying degrees and voltages, the crystals act like tiny shutters, opening or closing in response to the stimulus, thereby allowing degrees of light that have passed through specific colored pixels to illuminate the screen, creating a picture.

Each pixel of an LCD typically consists of a layer of molecules aligned between two transparent electrodes, and two polarizing filters, the axes of transmission of which are (in most of the cases) perpendicular to each other. With no actual liquid crystal between the polarizing filters, light passing through the first filter would be blocked by the second (crossed) polarizer.

The surface of the electrodes that are in contact with the liquid crystal material are treated so as to align the liquid crystal molecules in a particular direction. This treatment typically consists of a thin polymer layer that is unidirectional rubbed using, for example, a cloth. The direction of the liquid crystal alignment is then defined by the direction of rubbing. Electrodes are made of a transparent conductor called Indium (ITO). The Liquid Crystal Display is intrinsically a "passive" device; it is a simple light valve. The managing and control of the data to be displayed is performed by one or more circuits commonly denoted as LCD drivers.

Before applying an electric field, the orientation of the liquid crystal molecules is determined by the alignment at the surfaces of electrodes. In a twisted nematic device (still the most common liquid crystal device), the surface alignment directions at the two electrodes are perpendicular to each other, and so the molecules arrange themselves in a helical structure, or twist. This reduces the rotation of the polarization of the incident light, and the device appears grey. If the applied voltage is large enough, the liquid crystal molecules in the center of the layer are almost completely untwisted and the polarization of the incident light is not rotated as it passes through the liquid crystal layer. This light will then be mainly polarized perpendicular to the second filter, and thus be blocked and the pixel will appear black. By controlling the voltage applied across the liquid crystal layer in each pixel, light can be allowed to pass through in varying amounts thus constituting different levels of gray.

The optical effect of a twisted nematic device in the voltage-on state is far less dependent on variations in the device thickness than that in the voltage-off state. Because of this, these devices are usually operated between crossed polarizer's such that they appear bright with no voltage (the eye is much more sensitive to variations in the dark state than the bright state).

Both the liquid crystal material and the alignment layer material contain ionic compounds. If an electric field of one particular polarity is applied for a long period of time, this ionic material is attracted to the surfaces and degrades the device performance. This is avoided either by applying an alternating current or by reversing the polarity of the electric field as the device is addressed (the response of the liquid crystal layer is identical, regardless of the polarity of the applied field)

4.1.1 Types of LCDs:

There are mainly two types of LCD

- Passive display
- Active display

Passive Display: Passive displays are widely used with segmented digits and characters for small readouts in devices such as calculators, fax machines and remote controls, Most of these display are monochrome or have only a few colors.

Active Display: Used in all LCD TVs and desktop computer monitors and 99.9% of all laptops, Active displays are essentially "active matrix" displays and almost always color. The reason why all laptops do not use active LCD displays is that a new a new display device OLED (organic light-emitting diode) is emerging

4.2 CHARACTERISTICS OF LCD:

Here by 16*2 we mean that there are 16 characters can be displayed in one line and 2 means there are 2 lines in our display.

4.2.1 Features of 16*2 character LCD

• 5 x 8 dots with cursor

• Built-in controller (KS0066 or Equivalent)

• +5 V power supply (Also available for +3 V)

• 1/16 duty cycle

• B/L to be driven by pin 1, pin 2 or pin 15, pin 16 or AK (LED)

• NV optional for +3 V power supply

4.3 CONNECTIONS OF LCD

- Pin 1 of LCD to ground.
- Pin 2 of LCD to V_{CC} (5 V).
- Pin 3 of LCD to ground.
- Pin 4 of LCD to PortB.2 (2nd pin of port B).
- Pin 5 of LCD to ground.
- Pin 6 of LCD to PortB.3.
- Pin 7-10 are left floating (open).
- Pin 11 of LCD to PortB.4.
- Pin 12 of LCD to PortB.5.
- Pin 13 of LCD to PortB.6.
- Pin 14 of LCD to PortB.7.
- Pin 15 of LCD to V_{cc} (5 V).
- Pin 16 of LCD to ground.

4.4 SYNTAX FOR CONFIGURING LCD

CONFIG LCD = LCD_type

CONFIG LCDPIN = PIN, DB4= PN,DB5=PN, DB6=PN, DB7=PN, E=PN, RS=PN

LCD_type – It is the type of LCD you want to configure. It can be: 40 * 4, 16 * 1, 16 * 2, 16 * 4,

16 * 4, 20 * 2 or 20 * 4 or 16 * 1a or 20*4A.

Config Lcdpin - Override the LCD-PIN select options.

Now to configure our 16*2 alphanumeric LCD we use the following command:-

Config LCD = 16*2

Config Lcdpin = Pin, Db4 = PortB.4, Db5 = PortB.5, Db6 = PortB.6, Db7 = PortB.7, E= PortB.3 , Rs = PortB.2

4.5 LED

A light-emitting diode (LED) is a semiconductor light source. When a light switched on, electrons are able to recombine with holes within the device, releasing energy in the form of photons.

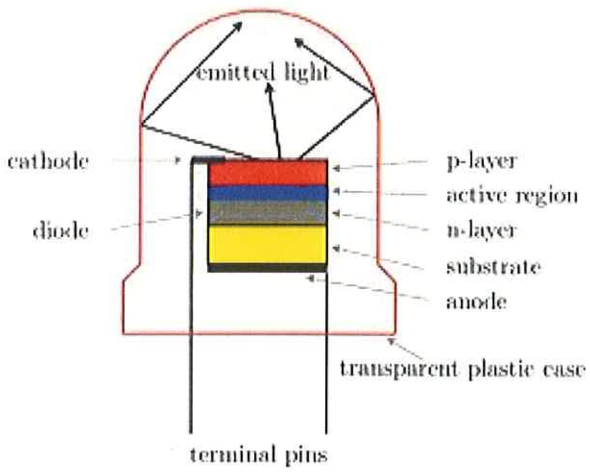

FIGURE 4.2: LIGHT EMITTING DIODE

CHAPTER 5

BASCOM

5.1 PROGRAMMING IN BASCOM

$regfile = "m16def.dat"

(It refers to the name of register file. The register files are stored in the BASCOM-AVR application directory with .DAT extension. The register file holds information about the chip such as the internal registers and interrupts addresses. Since we are using Atmega16 microcontroller, we will define $regfile= "m16def.dat")

$crystal = 1000000

(1000000 indicate 1 MHz frequency that a user can set freely for the microcontroller. It defines the clock speed at which you want to run your microcontroller.)

Config ADC = Single, Prescaler = Auto, Reference = AVcc

(ADC – It defines the running mode. Its value is SINGLE.

PRESCALER - A numeric constant for the clock divider. Use AUTO to let the compiler generate the best value depending on the XTAL.

REFERENCE - Some chips like the M163 have additional reference options. Its value may be OFF, AVCC or INTERNAL.

Single means instructing the ADC to fetch the value only when its asked to."Auto" means that the ADC can automatically set its frequency in regard with the microcontroller frequency in the program.

Reference is set as AVcc because Aref voltage is referred from the voltage supply to the ADC's i.e. AVcc.)

Start ADC

(StartAdc id=s the command given to initialize the ADCs.)

Config Timer1 = Pwm, Pwm = 8, Prescale = 1, Compare A Pwm = Clear Down,

Compare B

Pwm = Clear Down

(We use PWM to control the motor speed which is of 8 bit that is why we set PWM= 8, PWM works on the same frequency as microcontroller, and the Channels A & B are set as clear down to vary the speeds from 0 to 255 in increasing order.)

StartTimer1

(StartTimer1 is used to start the PWM channels.)

5.1.1 Defining Variables

SYNTAX:

DIM (var) as type Var- Name of Variable

Type - Bit, Byte, Word, Integer, Long, Single, Double or String

5.1.2 Start and Clear Commands

Start Command: This command is used to start the specified device.

Syntax

START device

Device - TIMER0, TIMER1, COUNTER0 or COUNTER1, WATCHDOG, AC (Analog comparator power) or ADC (A/D converter power)

Example – Start ADC

CLS Command: Clear the LCD display and set the cursor to home.

Syntax/ Example – Cls

5.1.3 Loops

If – Else statement, Loops and Select – case statement

BASCOM allows using all types of loops in the program like do, while and for. Concept of using these loops is same as using them in other languages like C. Given below are syntaxes of all loops you can use in BASCOM

5.1.3.1 Do Loop

```
Do
    <Statements>
Loop
```

5.1.3.2 If – else statement

```
If (condition) then
        <Statements>
Else
        <statements>
Endif
```

5.1.4 GETADC Command

This command is used to take input from the analog sensor connected to the development board. This command retrieves the analog value from channel 0-7 of port A. The range of analog value is from 0 to 1023.

5.1.5 WAITMS & PWMXX Command

Waitms command: Suspends program execution for a given time in mS.

Syntax

WAITMS Ms

Ms- The number of milliseconds to wait. (1-65535)

Example: Waitms 200

PWMXX command: It is used to set the speed of motor

5.2 MAIN SYNTAX

```
$regfile = "m16def.dat"
$crystal = 2000000
$baud = 9600
Config Lcd = 16*2
Config Lcdpin = Pin, Db4 = Portb.4, Db5 = Portb.5, Db6 = Portb.6 , Db7 = Portb.7 ,
E = Portb.3 , Rs = Portb.2
Config Adc = Single, Prescaler = Auto , Reference = Avcc
Start Adc
Config Timer1 = Pwm, Pwm = 8, Prescale = 1, Compare A Pwm = Clear Down,
Compare B Pwm = Clear Down
Start Timer1
Config Portc.1 = Output
Config Portc.2 = Output
Dim A as String*1
Do
   A = Wait key ()
   Cls
   Lcd A
   Print A
   Loop
End
```

CHAPTER 6

ZIGBEE

6.1 INTRODUCTION

ZigBee is an open global standard built on the IEEE 802.15.4 MAC/PHY. ZigBee defines a network layer above the 802.15.4 layers to support advanced mesh routing capabilities. The ZigBee specification is developed by a growing consortium of companies that make up the ZigBee Alliance. The Alliance is made up of over 300 members, including semiconductor, module, stack, and software developers.

In modern wireless protocols, such as Wi-Fi (IEEE 802.11) and Bluetooth (IEEE 802.15.1), the protocol helps ensure data arrives at the correct destination without errors as discussed. The protocol greatly reduces the work of the programmer in ensuring data delivery. Some key features of protocols in ensuring data delivery and integrity include:

- Media Access: A means to ensure two network nodes do not transmit at the same time causing data collisions and errors in transmission.
- Addressing: A means to ensure only the intended node uses the received data, allowing data to be sent from one point to another point. Or, point to multi-point by sending a broadcast meant for all nodes on the network.
- Error Detection: A means to verify data received at the node correctly.
- Acknowledgements & Retries: A means to inform the transmitting node that the data was delivered successfully. Lacking this, several retries may be performed in an effort to deliver the data.

The zigbee utilizes the IEEE 802.15.4 protocol which implements all of the above features. This protocol is known as a Low-Rate, Wireless Personal Area Network (LR-WPAN). It provides up to 250 kbps of data throughput between nodes on a CSMA/CA network. While not intended for large volumes of data, such as image

files, it provides a means of moving data quickly between nodes for use in monitoring and control systems commonly referred to as a Wireless Sensor Network (WSN).
In comparison to Bluetooth (IEEE 802.15.1), the LR-WPAN is designed as a much simpler protocol with lower data transfer rates (250 kbps compared to 1 Mbps). Bluetooth was designed as a replacement for peripheral cables and is used in communications between handheld devices, such as phones, requiring access security and high rates of data transfer.

The zigbee, using the IEEE 802.15.4 protocol, incorporates the following for communications and control on the WSN (wireless sensor network).

- Clear Channel Assessment (CCA): Before transmitting, a zigbee node listens to see if the selected frequency is busy.
- Addressing: The zigbee has two addressing options: a fixed 64-bit serial number (MAC address) which cannot be changed, and a 16-bit assignable address (which we will use) that allows over 64,000 addresses on a network.
- Error Checking and Acknowledgements: The zigbee uses a checksum to help ensure received data contains no errors. Acknowledgements are sent to the transmitting node to indicate proper reception. Up to 3 retries are performed by default if acknowledgements are not received.

6.2 ZIGBEE STACK LAYERS

The ZigBee stack consists of several layers including the PHY, MAC, Network, Application Support Sub layer (APS), and ZigBee Device Objects (ZDO) layers. Technically, an Application Framework (AF) layer also exists, but will be grouped with the APS layer in remaining discussions. The ZigBee layers are shown in the figure below. A description of each layer appears in the following table:

ZigBee Layer	Description
PHY	Defines the physical operation of the ZigBee device including receive sensitivity, channel rejection, output power, number of channels, chip modulation, and transmission rate specifications. Most ZigBee applications operate on the 2.4 GHz ISM band at a 250kbps data rate. See the IEEE 802.15.4 specification for details.
MAC	Manages RF data transactions between neighboring devices (point to point). The MAC includes services such as transmission retry and acknowledgment management, and collision avoidance techniques (CSMA-CA).
Network	Adds routing capabilities that allows RF data packets to traverse multiple devices (multiple "hops") to route data from source to destination (peer to peer).
APS (AF)	Application layer that defines various addressing objects including profiles, clusters, and endpoints.
ZDO	Application layer that provides device and service discovery features and advanced network management capabilities

TABLE 6.1:Zigbee layers

6.3 NETWORKING CONCEPTS

Device Type

ZigBee defines three different device types: coordinator, router, and end device. Node Types / Sample of a Basic ZigBee Network Topology

A **coordinator** has the following characteristics:

- Selects a channel and PAN ID (both 64-bit and 16-bit) to start the network
- Can allow routers and end devices to join the network
- Can assist in routing data Cannot sleep--should be mains powered •Can buffer RF data packets for sleeping end device children

A **router** has the following characteristics:

- Must join a ZigBee PAN before it can transmit, receive, or route data
- After joining, can allow routers and end devices to join the network
- After joining, can assist in routing data •Cannot sleep--should be mains powered.
- Can buffer RF data packets for sleeping end device children.

An **end device** has the following characteristics:

- Must join a ZigBee PAN before it can transmit or receive data
- Cannot allow devices to join the network
- Must always transmit and receive RF data through its parent. Cannot route data.
- Can enter low power modes to conserve power and can be battery-powered..

6.4 PIN SIGNAL

S.No.	Pin Name	Direction	Description
1	V_{cc}	-	Power supply
2	DOUT	Output	UART Data Out
3	DIN/CONFIG	Input	UART Data In
4	DIO8	Either	Digital I/O 8
5	RESET	Input	Module Reset(Reset pulse may be at 200ns)
6	PWM0/RSSI/DIO10	Output	PWM Output 0/RX Signal Strength Indicator/Digital IO
7	PWM/DIO11	Either	Digital I/O 11
8	[RESERVED]	-	Do not connect
9	DTR/SLEEP_RQ/DI8	Input	Pin sleep control line/Digital input 8
10	GND	-	Ground
11	DIO4	Either	Digital I/O 4
12	CTS/DIO7	Either	Clear to send flow control/Digital I/O 7
13	ON/SLEEP	Output	Module status indicator
14	[RESERVED]	-	Do not connect
15	Associate/DIO5	Either	Associated Indicator/Digital I/O 5
16	RTS/DIO6	Either	Request to send flow control/Digital I/O 6
17	AD3/DIO3	Either	Analog input 3/Digital I/O 3
18	AD2/DIO2	Either	Analog input

			2/Digital I/O 2
19	**AD1/DIO1**	**Either**	**Analog input 1/Digital I/O 1**
20	**AD0/DIO0**	**Either**	**Analog input 0/Digital I/O 0**

TABLE 6.2: PIN SIGNAL

Design Notes

• Minimum connections: VCC, GND, DOUT & DIN

• Minimum connections to support firmware upgrades: VCC, GND, DIN, DOUT, RTS & DTR

• Signal Direction is specified with respect to the module

• Module includes a 30k Ohm resistor attached to **RESET**

• Several of the input pull-ups can be configured using the PR command • Unused pins should be left disconnected

6.5 DATA TRANSMISSION AND ROUTING

All data packets are addressed using both device and application layer addressing fields. Data can be sent as a broadcast, multicast, or unicast transmission.

- **Broadcast Transmissions** Broadcast transmissions within the ZigBee protocol are intended to be propagated throughout the entire network such that all nodes receive the transmission. To accomplish this, all devices that receive a broadcast transmission will retransmit the packet 3 times. Each node that transmits the broadcast will also create an entry in a local broadcast transmission table. This entry is used to keep track of each received broadcast packet to ensure the packets are not endlessly transmitted. Each entry persists for 8 seconds. The broadcast transmission table holds 8 entries. Since broadcast transmissions are retransmitted by each device in the network, broadcast messages should be used sparingly.

- **Multicast Transmissions** Multicast transmissions operate similar to broadcast transmissions. Data packets are broadcast throughout the network in a similar fashion. However, only devices that are part of the multicast group will receive the data packets.

- **Unicast Transmissions** Unicast ZigBee transmissions are always addressed to the 16-bit address of the destination device. However, only the 64-bit address of a device is permanent; the 16-bit address can change. Therefore, ZigBee devices may employ network address discovery to identify the current 16-bit address that corresponds to a known 64-bit address. Once the 16-bit address is known, a route to the destination device must be discovered. ZigBee employs mesh routing using the Ad-hoc On-demand Distance Vector routing (AODV) protocol to establish a route between the source device and the destination.

- **Network Address Discovery** Data transmissions are always sent to the 16-bit network address of the destination device. However, since the 64-bit address is unique to each device and is generally known, ZigBee devices must discover the network address that was assigned to a particular device when it joined the PAN before they can transmit data. To do this, the device initiating a transmission sends a broadcast network address discovery transmission throughout the network. This packet contains the 64-bit address of the device the initiator needs to send data to. Devices that receive this broadcast transmission check to see if their 64-bit address matches the 64-bit address contained in the broadcast transmission. If the addresses match, the device sends a response packet back to the initiator, providing the network address of the device with the matching 64-bit address. When this response is received, the initiator can then transmit data.

- **Mesh Routing** Mesh routing allows data packets to traverse multiple nodes (hops) in a network to route data from a source to a destination. The route a packet can take in a mesh network is independent of the parent/child relationships established during joining. Before transmitting a data packet from source to destination nodes, a route must be established. Route discovery is based on the AODV (Ad-hoc On-demand Distance Vector routing) protocol.

- **AODV (Ad-hoc On-demand Distance Vector) Routing Algorithm** Routing under the AODV protocol is accomplished using tables in each node that store in the next hop (intermediary node between source and destination nodes) for a destination node. If a next hop is not known, route discovery must take place in order to find a path. Since only a limited number of routes can be stored on a Router, route discovery will take place more often on a large network with communication between many different nodes. When a source node must discover a route to a destination node, it sends a broadcast route request command. The route request command contains the source Network Address, the destination Network Address and a Path Cost field (a metric for measuring route quality). As the route request command is propagated through the network (refer to the Broadcast Transmission), each node that re-broadcasts the message updates the Path Cost field and creates a temporary entry in its route discovery table. When the destination node receives a route request, it compares the 'path cost' field against previously received route request commands. If the path cost stored in the route request is better than any previously received, the destination node will transmit a route reply packet to the node that originated the route request. Intermediate nodes receive and forward the route reply packet to the Source Node (the node that originated route request).

- **Retries and Acknowledgments** ZigBee includes acknowledgment packets at both the Mac and Application Support (APS) layers. When data is transmitted to remote device, it may traverse multiple hops to reach the destination. As data is transmitted from one node to its neighbor, an acknowledgment packet (Ack) is transmitted in the opposite direction to indicate that the transmission was successfully received. If the Ack is not received, the transmitting device will retransmit the data, up to 4 times. This Ack is called the Mac layer acknowledgment. In addition, the device that originated the transmission expects to receive an acknowledgment packet (Ack) from the destination device. This Ack will traverse the same path that the data traversed, but in the opposite direction. If the originator fails to receive this Ack, it will retransmit the data, up to 2 times until an Ack is received. This Ack is called the ZigBee APS layer acknowledgment.

6.5.1 Starting a Co-ordinator

When a coordinator first comes up, it performs an energy scan on mulitple channels (frequencies) to select an unused channel to start the PAN. After removing channels with high detected energy levels, the coordinator issues an 802.15.4 beacon request command on the remaining, low energy level channels. Any routers or coordinators respond to the beacon request frame with a small beacon transmission that indicates the PAN identifier (PAN ID) that they are operating on, and whether or not they are allowing joining.The coordinator will attempt to start on an unused PAN ID and channel. After starting, the coordinator may allow other devices to join its PAN.

6.5.2 Joining a Router

When a router first comes up, it must locate and join a ZigBee PAN. To do this, it issues an 802.15.4 beacon request command on multiple channels to locate nearby PANs. Nearby routers and coordinators respond to the beacon request frame with a small beacon transmission, indicating which channel and PAN ID they are operating on. The router listens on each channel for these beacon frames, and determines which device it should join. If a valid PAN is found from one of the received beacons, the router issues a join request to the device that sent the beacon. If joining succeeds, the router will then receive a join confirmation from the device, indicating the join was successful. Once the router joins the PAN, it can communicate with other devices on the PAN and allow new devices to join to it.

6.5.3 Joining an End Device

When an end device first comes up, it must also locate and join a PAN. End devices follow the same process as a router to join a PAN. Once the end device has successfully joined a PAN, it can communicate with other devices on the PAN. However, since end devices cannot route data, it must always communicate directly with its parent and allow the parent to route data in its behalf.

6.6 Multi–Node Network Issues

- Many wireless modules for microcontrollers simply send data and receive data on the provided frequency.
- It is up the end user and his (or her) application code to deal with issues such as media access rules, data delivery verification, error checking, and, in multi-node networks, which node will accept and use the data.
- Devices using a networking protocol can ease the work of the programmer by handling these tasks.

RESULT

This section describes the output of the implemented system. Several testing has been performed to ensure it's executed and produce the intended result. The device will be able to jam the cell phone carriers. The effective jamming range will be the whole area using the tower with same **PAN ID** (Personal Area Network Id). This is more than what a normal jammer is designed for.

This project is mainly intended to prevent the usage of mobile phones in places inside its coverage without interfering with the communication channels outside its range, thus providing a cheap and reliable method for blocking mobile communication in the required areas only. This prototype can be used by the government at the time of emergency. So that the communication made by the people causing trouble cannot communicate with each other.

REFERENCES

1. http://www.howstuffworks.com/lcd.htm
2. http://www.webopedia.com/TERM/L/LCD.html
3. http://en.wikipedia.org/wiki/Liquid_crystal_display
4. http://en.wikipedia.org/wiki/Light-emitting_diode
5. http://en.wikipedia.org/wiki/Microcontroller