MOBILE PHONE SIGNAL JAMMER WITH PRESCHEDULED TIME DURATION

PROJECT REPORT

SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

BY

S. HEMA LATHA (06261A0448)

RUPA DEVI (07265A0402)

K.YASWANTHI (07265A0406)

Department of Electronics and Communication Engineering

MAHATMA GANDHI INSTITUTE OF TECHNOLOGY

(AFFILIATED TO JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, HYDERABAD, A.P)

Chaitanya Bharathi P.O., Gandipet, Hyderabad-500 075

2010

ABSTRACT

Mobile jammer is used to prevent mobile phones from receiving or transmitting signals with the base stations. Mobile jammers effectively disable mobile phones within the defined regulated zones without causing any interference to other communication means. Mobile jammers can be used in practically any location, but are used in places where a phone call would be particularly disruptive like Temples, Libraries, Hospitals, Cinema halls, schools & colleges etc.

As with other radio jamming, mobile jammers block 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 jammers, all mobile phones will indicate "NO NETWORK". Incoming calls are blocked as if the mobile phone were off. When the mobile jammers are turned off, all mobile phones will automatically re-establish communications and provide full service.

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 jammers for government switched over to sell these devices to private entities.

In this project, we are controlling this mobile jammer by means of a microcontroller. The activation and deactivation time schedules can be programmed with microcontroller. Real time clock chip DS1307 is used to set the schedule.

This project uses regulated 5V, 500mA power supply. Unregulated 12V DC is used for relay. 7805 three terminal voltage regulator is used for voltage regulation. Bridge type full wave rectifier is used to rectify the ac out put of secondary of 230/12V step down transformer.

ACKNOWLEDGEMENT

We express our earnest gratitude to Faculty Advisor/Liaison, **Mr.Ch.Raja**, Associate professor, Electronics and communication Engineering Department, MGIT.Who has given us all the necessary technical guidance in carrying out this project. We are grateful for his cooperation and his valuable suggestions.

We are grateful to **Dr.E Nagabhooshanam**, Head of the Department of Electronics and Communication Engineering, MGIT, for providing the facilities to complete the project successfully and project coordination for critically reviewing the progress of our project.

Finally, we thank all those who directly or indirectly helped us through the course of our project.

S. Hema Latha

Rupa Devi

K.Yaswanthi

.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

Cell phones are everywhere these days. It's great to be able to call anyone at anytime. Unfortunately, restaurants, movie theaters, concerts, shopping malls and churches all suffer from the spread of cell phones because not all cell-phone users know when to stop talking While most of us just grumble and move on, some people are actually going to extremes to retaliate.

Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell-phone user drives down the street, the signal is handed from tower to tower A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cell-phone base station in the tower Jamming devices overpower the cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide and cancel each other out.

Cell phones are full-duplex devices, which means they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, some has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal.

To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PCS-based systems, operates in the 900-MHz and 1800-MHz bands in Europe and Asia and in the 1900-MHz (sometimes

referred to as 1.9-GHz) band in the United States. Jammers can broadcast on any frequency and are effective against CDMA, GSM and DCS. Old-fashioned analog cell phones and today's digital devices are equally susceptible to jamming.

The actual range of the jammer depends on its power and the local environment, which may include hills or walls of a building that block the jamming signal. Low-powered jammers block calls in a range of about 16 feet (5 m). Higher-powered units create a cell-free zone as large as a football field. Units used by law enforcement can shut down service up to 1 mile (1.6 km) from the device.

1.1 AIM OF THE PROJECT:

Here our main intention is to block the signals of mobile phone using mobile phone signal jammer for prescheduled time duration using real time clock controlled by microcontroller. Switches are used to set the time for start and stop of jammer.

1.2 METHODOLOGY:

Hardware used in the project:

- Power supply board
- Switches board
- Microcontroller
- RTC
- Relay circuit
- Jammer

Software used in the project:

- Embedded ‘c’ programming
- Keil Uvision compiler
- Proload

Block Diagram

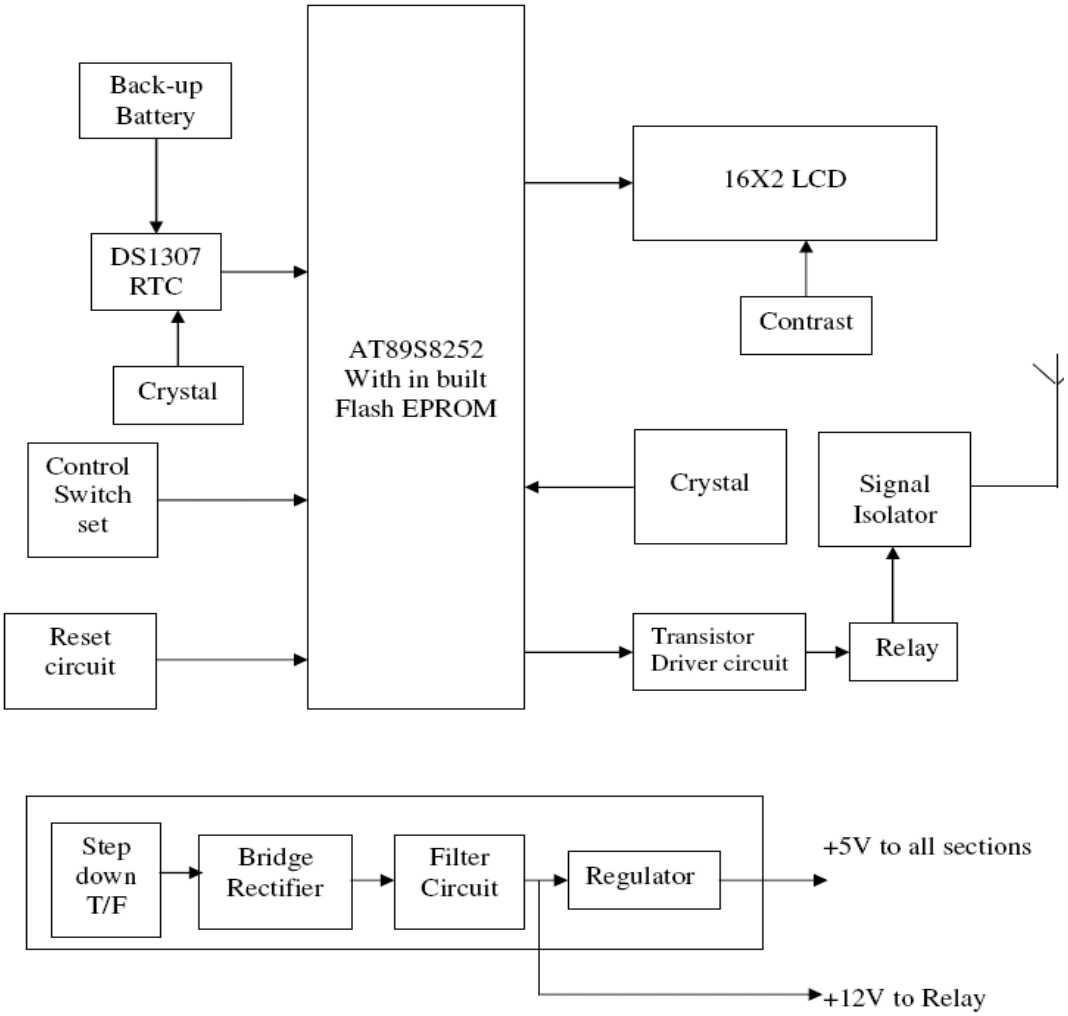


Fig: 2.1 Block Diagram

Explanation of Each Block

BLOCK DESCRIPTION

2.2 POWER SUPPLY:

The input to the circuit is applied from the regulated power supply. The a.c. input i.e., 230V from the mains supply is step down by the transformer to 12V and is fed to a rectifier. The output obtained from the rectifier is a pulsating d.c voltage. So in order to get a pure d.c voltage, the output voltage from the rectifier is fed to a filter to remove any a.c components present even after rectification. Now, this voltage is given to a voltage regulator to obtain a pure constant dc voltage.

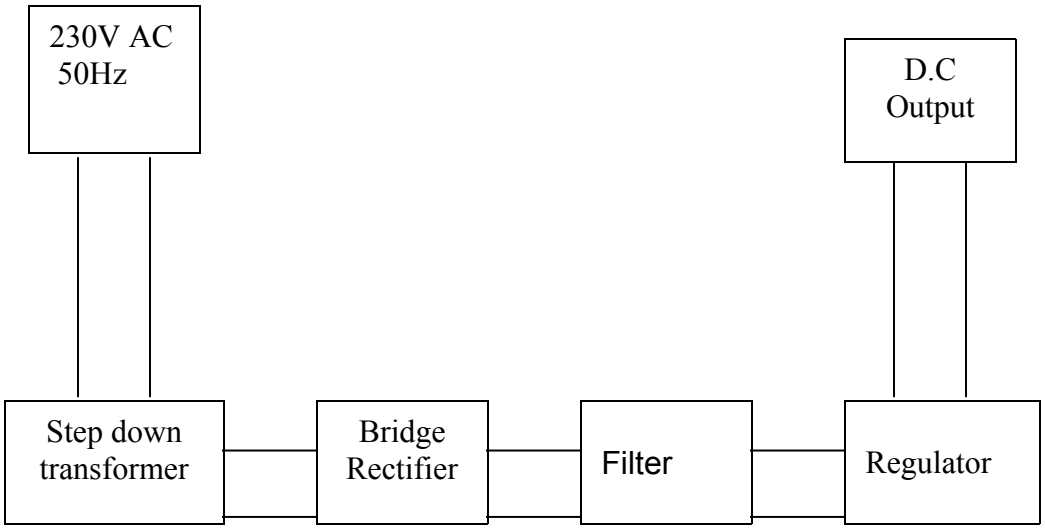


Fig: 2.2 Power supply

2.2.1 Transformer:

Usually, DC voltages are required to operate various electronic equipment and these voltages are 5V, 9V or 12V. But these voltages cannot be obtained directly. Thus the a.c input available at the mains supply i.e., 230V is to be brought down to the required voltage level. This is done by a transformer. Thus, a step down transformer is employed to decrease the voltage to a required level.

Fig: 2.3 Power Supply

2.2.2 Rectifier:

The output from the transformer is fed to the rectifier. It converts A.C. into pulsating D.C. The rectifier may be a half wave or a full wave rectifier. In this project, a bridge rectifier is used because of its merits like good stability and full wave rectification.

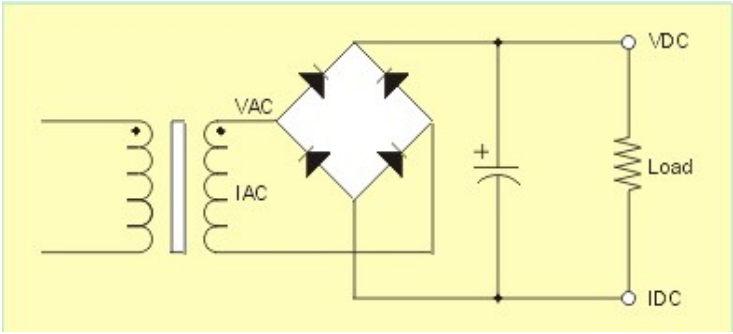
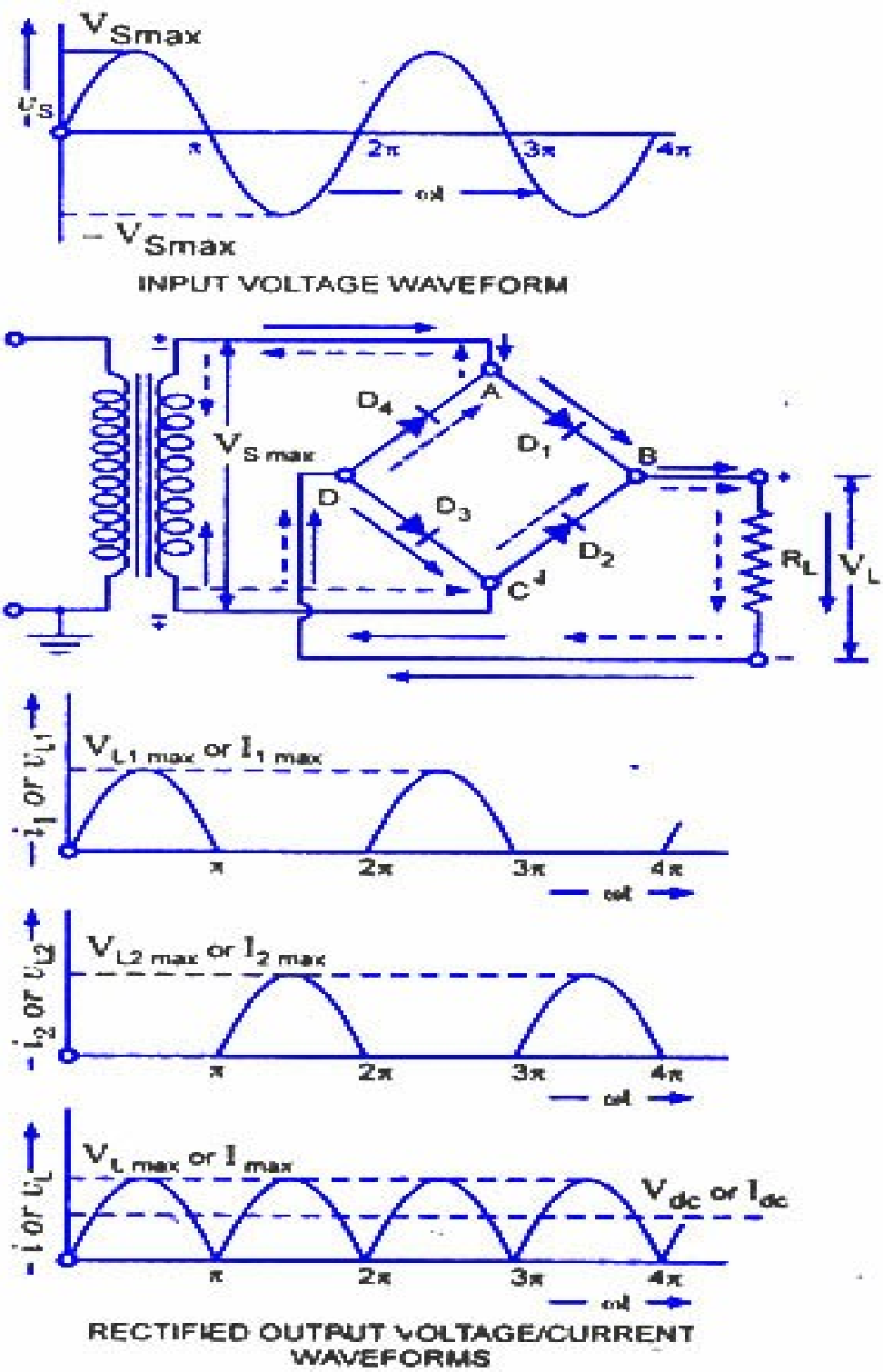


Fig: 2.4 Bridge Rectifier

The Bridge rectifier is a circuit, which converts an ac voltage to dc voltage using both half cycles of the input ac voltage. The Bridge rectifier circuit is shown in the figure. The circuit has four diodes connected to form a bridge. The ac input voltage is applied to the diagonally opposite ends of the bridge. The load resistance is connected between the other two ends of the bridge.

For the positive half cycle of the input ac voltage, diodes D1 and D3 conduct, whereas diodes D2 and D4 remain in the OFF state. The conducting diodes will be in series with the load resistance R_L and hence the load current flows through R_L.

For the negative half cycle of the input ac voltage, diodes D2 and D4 conduct whereas, D1 and D3 remain OFF. The conducting diodes D2 and D4 will be in series with the load resistance R_L and hence the current flows through R_L in the same direction as in the previous half cycle. Thus a bi-directional wave is converted into a unidirectional wave.



Bridge Rectifier

Fig: 2.4(a)

2.2.3 Filter:

Capacitive filter is used in this project. It removes the ripples from the output of rectifier and smoothens the D.C. Output received from this filter is constant until the mains voltage and load is maintained constant. However, if either of the two is varied, D.C. voltage received at this point changes. Therefore a regulator is applied at the output stage.

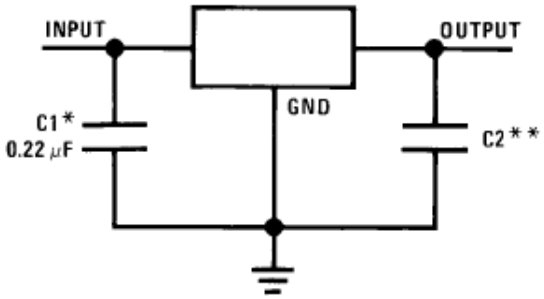


Fig: 2.5 Capacitive Filter

2.2.4 Voltage regulator:

As the name itself implies, it regulates the input applied to it. A voltage regulator is an electrical regulator designed to automatically maintain a constant voltage level. In this project, power supply of 5V and 12V are required. In order to obtain these voltage levels, 7805 and 7812 voltage regulators are to be used. The first number 78 represents positive supply and the numbers 05, 12 represent the required output voltage levels. The L78xx series of three-terminal positive regulators is available in TO-220, TO-220FP, TO-3, D2PAK and DPAK packages and several fixed output voltages, making it useful in a wide range of applications. These regulators can provide local on-card regulation, eliminating the distribution problems associated with single point regulation.

Fig: 2.6 Voltage Regulator

Each type employs internal current limiting, thermal shut-down and safe area protection, making it essentially indestructible. If adequate heat sinking is provided, they can deliver over 1 A output current. Although designed primarily as fixed voltage regulators, these devices can be used with external components to obtain adjustable voltage and currents.

AT89S52 Microcontroller

MICROCONTROLLER:

Microprocessors and microcontrollers are widely used in embedded systems products. *Microcontroller is a programmable device*. A microcontroller has a CPU in addition to a fixed amount of RAM, ROM, I/O ports and a timer embedded all on a single chip. The fixed amount of on-chip ROM, RAM and number of I/O ports in microcontrollers makes them ideal for many applications in which cost and space are critical.

The Intel 8051 is Harvard architecture, single chip microcontroller (µC) which was developed by Intel in 1980 for use in embedded systems. It was popular in the 1980s and early 1990s, but today it has largely been superseded by a vast range of enhanced devices with 8051-compatible processor cores that are manufactured by more than 20 independent manufacturers including Atmel, Infineon Technologies and Maxim Integrated Products.

8051 is an 8-bit processor, meaning that the CPU can work on only 8 bits of data at a time. Data larger than 8 bits has to be broken into 8-bit pieces to be processed by the CPU. 8051 is available in different memory types such as UV-EPROM, Flash and NV-RAM.

The present project is implemented on Keil Uvision. In order to program the device, proload tool has been used to burn the program onto the microcontroller.

The features, pin description of the microcontroller and the software tools used are discussed in the following section.

3.1 FEATURES OF AT89S52:

- 8K Bytes of Re-programmable Flash Memory.
- Internal RAM 256x8 bytes.
- 2.7V to 6V Operating Range.
- Fully Static Operation: 0 Hz to 24 MHz.
- Two-level Program Memory Lock.
- 32 Programmable I/O Lines.
- Three 16-bit Timer/Counters.

- Six Interrupt Sources.
- Programmable Serial UART Channel.
- Low-power Idle and Power-down Modes.

3.2 Description:

The AT89S52 is a low-voltage, high-performance CMOS 8-bit microcontroller with 8K bytes of Flash programmable memory. The device is manufactured using Atmel's high-density nonvolatile memory technology and is compatible with the industry-standard MCS-51 instruction set. By combining a versatile 8-bit CPU with Flash on a monolithic chip, the Atmel AT89S52 is a powerful microcomputer, which provides a highly flexible and cost-effective solution to many embedded control applications.

In addition, the AT89S52 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port and interrupt system to continue functioning. The power-down mode saves the RAM contents but freezes the oscillator disabling all other chip functions until the next hardware reset.

3.4 PIN DIAGRAM OF AT89S52:

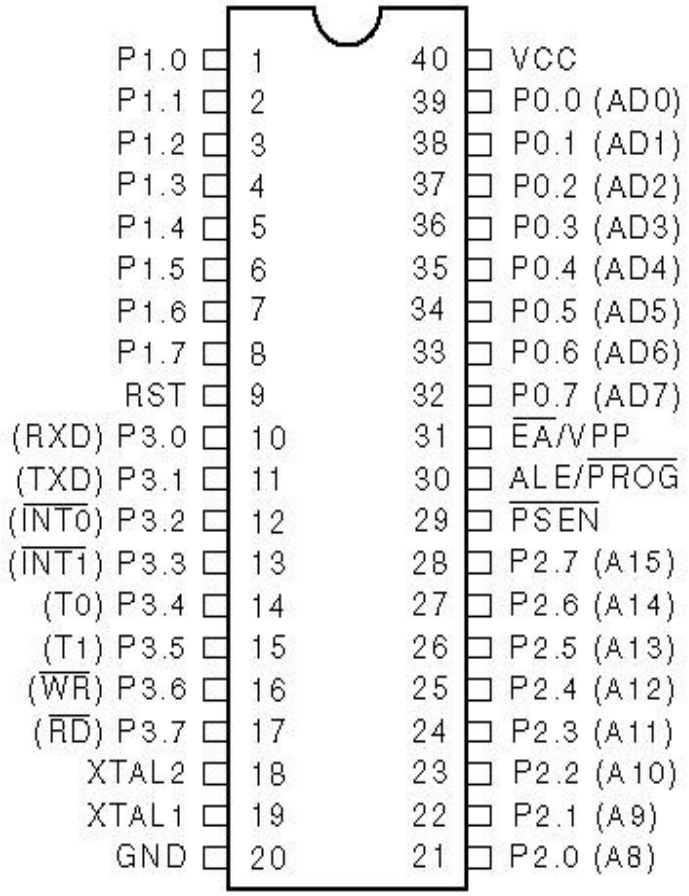


Fig: 3.1 Pin diagram

BLOCK DIAGRAM OF AT89S52:

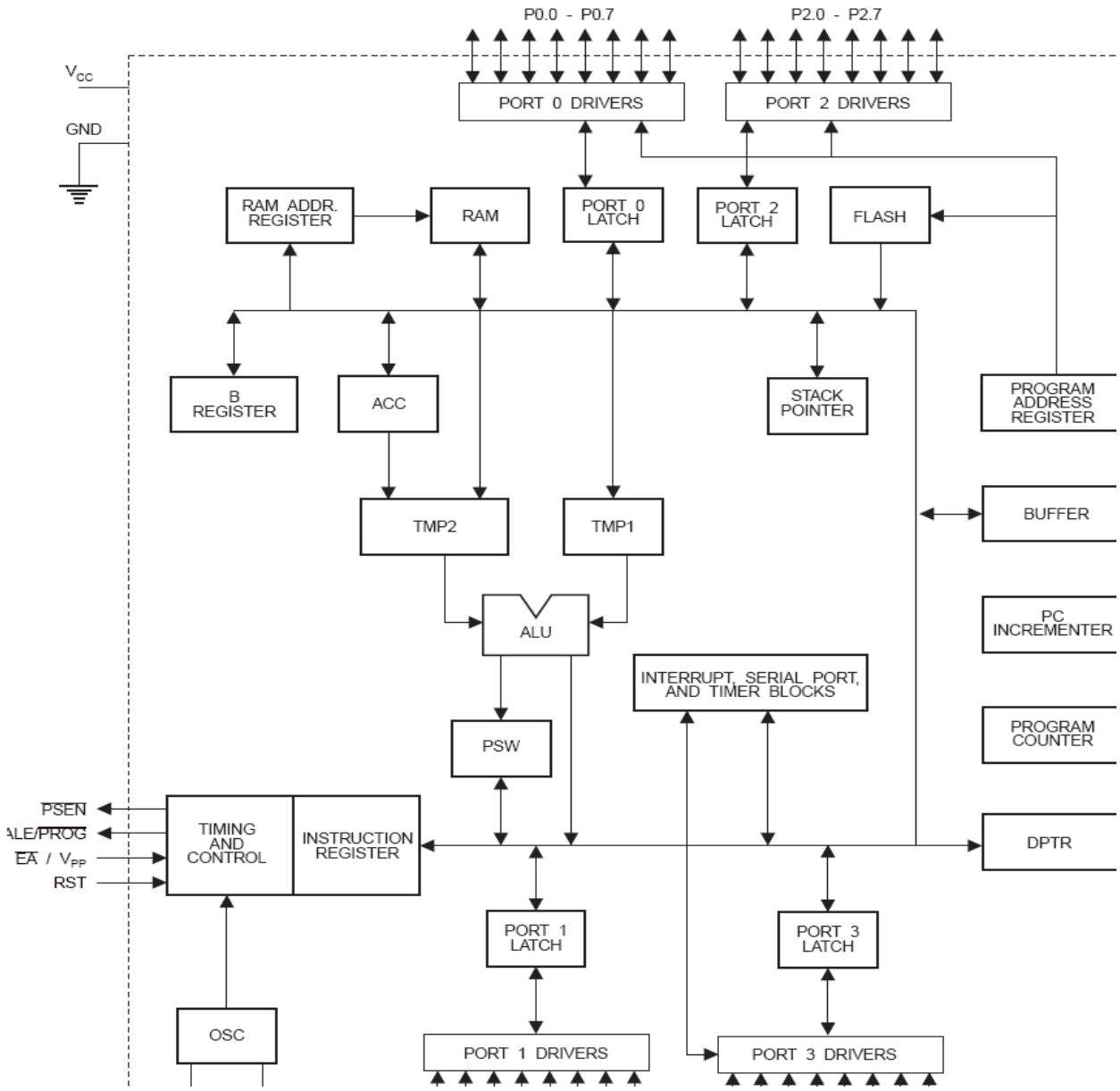


Fig: 3.2 Block diagram

PIN DESCRIPTION:

Vcc:

Pin 40 provides supply voltage to the chip. The voltage source is +5V.

GND:

Pin 20 is the ground.

XTAL1 and XTAL2:

XTAL1 and XTAL2 are the input and output, respectively, of an inverting amplifier that can be configured for use as an on-chip oscillator, as shown in Figure 11. Either a quartz crystal or ceramic resonator may be used. To drive the device from an external clock source, XTAL2 should be left unconnected while XTAL1 is driven, as shown in the below figure. There are no requirements on the duty cycle of the external clock signal, since the input to the internal clocking circuitry is through a divide-by-two flip-flop, but minimum and maximum voltage high and low time specifications must be observed.

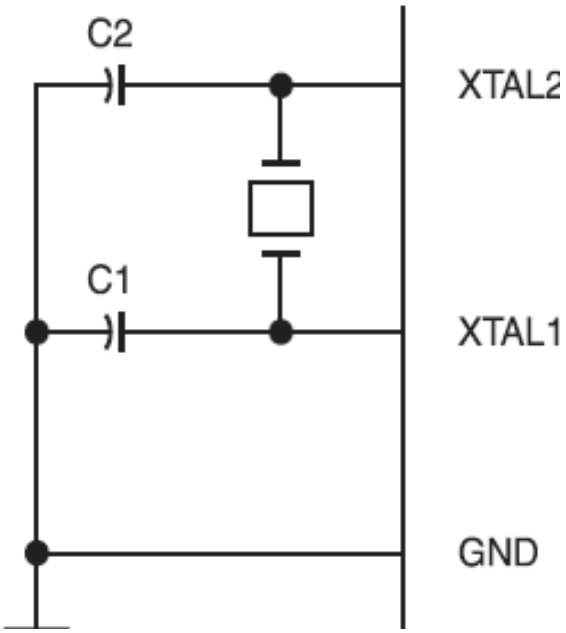


Fig: 3.3 Oscillator Connections

C1, C2 = 30 pF ± 10 pF for Crystals
= 40 pF ± 10 pF for Ceramic Resonators

RESET:

Pin9 is the reset pin. It is an input and is active high. Upon applying a high pulse to this pin, the microcontroller will reset and terminate all the activities. This is often referred to as a power-on reset.

Ports 0, 1, 2 and 3:

The four ports P0, P1, P2 and P3 each use 8 pins, making them 8-bit ports. All the ports upon RESET are configured as input, since P0-P3 have value FFH on them.

Port 0(P0):

Port 0 is also designated as AD0-AD7, allowing it to be used for both address and data. ALE indicates if P0 has address or data. When ALE=0, it provides data D0-D7, but when ALE=1, it has address A0-A7. Therefore, ALE is used for demultiplexing address and data with the help of an internal latch.

When there is no external memory connection, the pins of P0 must be connected to a 10K-ohm pull-up resistor. This is due to the fact that P0 is an open drain. With external pull-up resistors connected to P0, it can be used as a simple I/O, just like P1 and P2. But the ports P1, P2 and P3 do not need any pull-up resistors since they already have pull-up resistors internally. Upon reset, ports P1, P2 and P3 are configured as input ports.

Port 1 and Port 2:

With no external memory connection, both P1 and P2 are used as simple I/O. With external memory connections, port 2 must be used along with P0 to provide the 16-bit address for the external memory. Port 2 is designated as A8-A15 indicating its dual function. While P0 provides the lower 8 bits via A0-A7, it is the job of P2 to provide bits A8-A15 of the address.

Port 3:

Port 3 occupies a total of 8 pins, pins 10 through 17. It can be used as input or output. P3 does not need any pull-up resistors, the same as port 1 and port 2. Port 3 has an additional function of providing some extremely important signals such as interrupts.

Port Pin	Alternate Functions
P3.0	RXD (serial input port)
P3.1	TXD (serial output port)
P3.2	$\overline{\text{INT0}}$ (external interrupt 0)
P3.3	$\overline{\text{INT1}}$ (external interrupt 1)
P3.4	T0 (timer 0 external input)
P3.5	T1 (timer 1 external input)
P3.6	$\overline{\text{WR}}$ (external data memory write strobe)

Table: Port 3 Alternate Functions

Machine cycle for the 8051:

The CPU takes a certain number of clock cycles to execute an instruction. In the 8051 family, these clock cycles are referred to as machine cycles. The length of the machine cycle depends on the frequency of the crystal oscillator. The crystal oscillator, along with on-chip circuitry, provides the clock source for the 8051 CPU.

The frequency can vary from 4 MHz to 30 MHz, depending upon the chip rating and manufacturer. But the exact frequency of 11.0592 MHz crystal oscillator is used to make the 8051 based system compatible with the serial port of the IBM PC.

In the original version of 8051, one machine cycle lasts 12 oscillator periods. Therefore, to calculate the machine cycle for the 8051, the calculation is made as 1/12 of the crystal frequency and its inverse is taken.

The assembly language program is written and this program has to be dumped into the microcontroller for the hardware kit to function according to the software. The program dumped in the microcontroller is stored in the Flash memory in the microcontroller. Before that, this Flash memory has to be programmed and is discussed in the next section.

ALE/PROG:

Address Latch Enable is an output pulse for latching the low byte of the address during accesses to external memory. This pin is also the program pulse input (PROG) during Flash programming. In normal operation, ALE is emitted at a constant rate of 1/6 the oscillator frequency and may be used for external timing or clocking purposes. If desired, ALE operation can be disabled by setting bit 0 of SFR location 8EH. With the bit set, ALE is active only during a MOVX or MOVC instruction. Otherwise, the pin is weakly pulled high. Setting the ALE-disable bit has no effect if the microcontroller is in external execution mode.

PSEN (Program Store Enable) :

It is the read strobe to external program memory. When the AT89S8252 is executing code from external program memory, PSEN is acti-vated twice each machine cycle, except that two PSEN activations are skipped during each access to external data memory.

EA/VPP (External Access Enable):

Pin 31 is EA. It is an active low signal. It is an input pin and must be connected to either Vcc or GND but it cannot be left unconnected.

The 8051 family members all come with on-chip ROM to store programs. In such cases, the EA pin is connected to Vcc. If the code is stored on an external ROM, the EA pin must be connected to GND to indicate that the code is stored externally.

EA must be strapped to GND in order to enable the device to fetch code from external program memory locations starting at 0000H up to FFFFH. Note, however, that if lock bit 1 is programmed, EA will be internally latched on reset. EA should be strapped to VCC for internal

program executions. This pin also receives the 12-volt programming enable voltage (VPP) during Flash programming when 12-volt programming is selected.

EEPROM (Electrically Erasable Programmable Read only memory):

EEPROM has several advantages over other memory devices, such as the fact that its method of erasure is electrical and therefore instant. In addition, in EEPROM one can select which byte to be erased, in contrast to flash , in which the entire contents of ROM are erased. The main advantage of EEPROM is that one can program and erase its contents while it is in system board. It does not require physical removal of the memory chip from its socket. In general, the cost per bit for EEPROM is much higher when compared to other devices.

The EEPROM used in this project is 24C04 type.

Features of 24C04 EEPROM:

- 1 million erase/write cycles with 40 years data retention.
- Single supply voltage:
  3v to 5.5v for st24x04 versions.
  2.5v to 5.5v for st25x04 versions.
- Hardware write control versions:
  St24w04 and St25w04.
- Programmable write protection.
- Two wire serial interface, fully i2c bus compatible.
- Byte and multibyte write (up to 4 bytes).
- Page write (up to 8 bytes).
- Byte, random and sequential read modes
- Self timed programming cycle
- Automatic address incrementing
- Enhanced ESD/Latch up performances

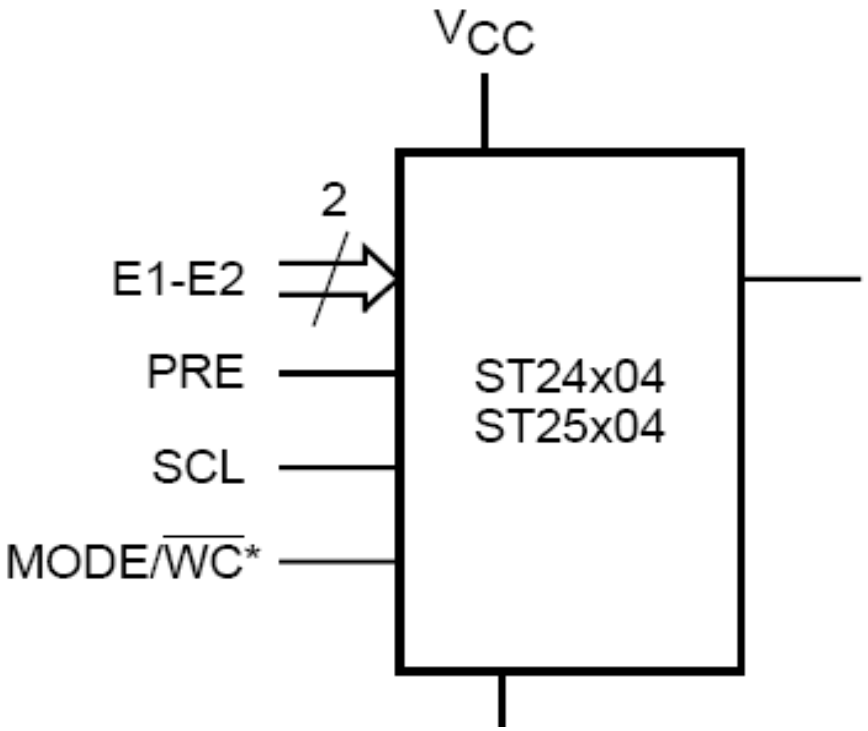


Fig: 4.1 Logic Diagram

4.2 DESCRIPTION:

The 24C04 is a 4Kbit electrically erasable programmable memory (EEPROM), organized as 2 blocks of 256 x8 bits. They are manufactured in ST Microelectronics' Hi-Endurance Advanced CMOS technology which guarantees an endurance of one million erase/write cycles with a data retention of 40 years. Both Plastic Dual-in-Line and Plastic Small Outline packages are available. The memories are compatible with the I2C standard, two wire serial interface which uses a bi-directional data bus and serial clock. The memories carry a built-in 4 bit, unique device identification code (1010) corresponding to the I2C bus definition. This is used together with 2 chip enable inputs (E2, E1) so that up to 4 x 4K devices may be attached to the I2C bus and selected individually. The memories behave as a slave device in the I2C protocol with all

memory operations synchronized by the serial clock. Read and write operations are initiated by a START condition generated by the bus master. The START condition is followed by a stream of 7 bits (identification code 1010), plus one read/write bit and terminated by an acknowledge bit.

	Device Code				Chip Enable		Block Select
Bit	b7	b6	b5	b4	b3	b2	b1
Device Select	1	0	1	0	E2	E1	A8

Table: Device Select Mode

Mode	$R\overline{W}$ bit	MODE	Bytes	Initial Sequence
Current Address Read	'1'	X	1	START, Device Select, $R\overline{W}$ = '1'
Random Address Read	'0'	X	1	START, Device Select, $R\overline{W}$ = '0',
	'1'			reSTART, Device Select, $R\overline{W}$ = '1
Sequential Read	'1'	X	1 to 512	Similar to Current or Random Mo
Byte Write	'0'	X	1	START, Device Select, $R\overline{W}$ = '0'
Multibyte Write (2)	'0'	V_{IH}	4	START, Device Select, $R\overline{W}$ = '0'
Page Write	'0'	V_{IL}	8	START, Device Select, $R\overline{W}$ = '0'

Table: Operating Modes

When writing data to the memory it responds to the 8 bits received by asserting an acknowledge bit during the 9th bit time. When data is read by the bus master, it acknowledges the receipt of the data bytes in the same way. Data transfers are terminated with a STOP condition

Power on Reset: VCC locks out write protect:

In order to prevent data corruption and inadvertent write operations during power up, a Power on Reset (POR) circuit is implemented. Until the VCC voltage has reached the POR threshold value, the internal reset is active, all operations are disabled and the device will not respond to any command. In the same way, when VCC drops down from the operating voltage to below the POR threshold value, all operations are disabled and the device will not respond to any command. A stable VCC must be applied before applying any logic signal.

SIGNAL DESCRIPTIONS:

Serial Clock (SCL):

The SCL input pin is used to synchronize all data in and out of the memory. A resistor can be connected from the SCL line to VCC to act as a pull up.

Serial Data (SDA):

The SDA pin is bi-directional and is used to transfer data in or out of the memory. It is an open drain output that may be wire-OR'ed with other open drain or open collector signals on the bus. A resistor must be connected from the SDA bus line to VCC to act as pull up.

Chip Enable (E1 - E2):

These chip enable inputs are used to set the 2 least significant bits (b2, b3) of the 7 bit device select code. These inputs may be driven dynamically or tied to VCC or VSS to establish the device select code.

Protect Enable (PRE):

The PRE input pin, in addition to the status of the Block Address Pointer bit (b2, location 1FFh as in below figure), sets the PRE write protection active.

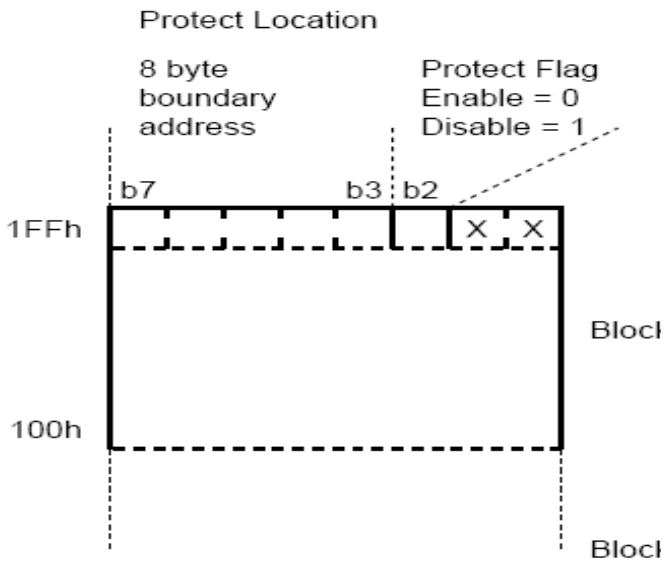


Fig: 4.2Memory Protection

Mode (MODE):

The MODE input is available on pin 7 and may be driven dynamically. It must be at VIL or VIH for the Byte Write mode, VIH for Multibyte Write mode or VIL for Page Write mode. When unconnected, the MODE input is internally read as VIH (Multibyte Write mode).

Write Control (WC):

An hardware Write Control feature (WC) is offered only for ST24W04 and ST25W04 versions on pin 7. This feature is useful to protect the contents of the memory from any erroneous erase/write cycle. The Write Control signal is used to enable (WC = VIH) or disable (WC =VIL) the internal write protection. When unconnected, the WC input is internally read as VIL and the memory area is not write protected.

5. RELAYS:

A relay is an electrically controllable switch widely used in industrial controls, automobiles and appliances.

The relay allows the isolation of two separate sections of a system with two different voltage sources i.e., a small amount of voltage/current on one side can handle a large amount of voltage/current on the other side but there is no chance that these two voltages mix up.

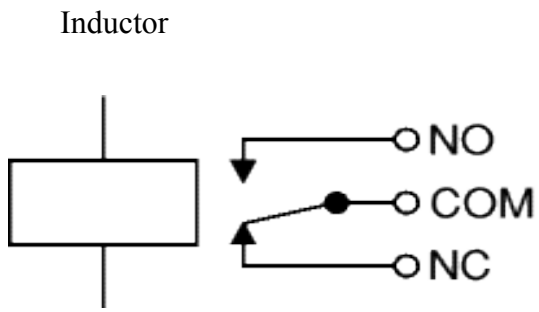


Fig: 5.1 Circuit symbol of a relay

5.1 Operation:

When a current flow through the coil, a magnetic field is created around the coil i.e., the coil is energized. This causes the armature to be attracted to the coil. The armature's contact acts like a switch and closes or opens the circuit. When the coil is not energized, a spring pulls the armature to its normal state of open or closed. There are all types of relays for all kinds of applications.

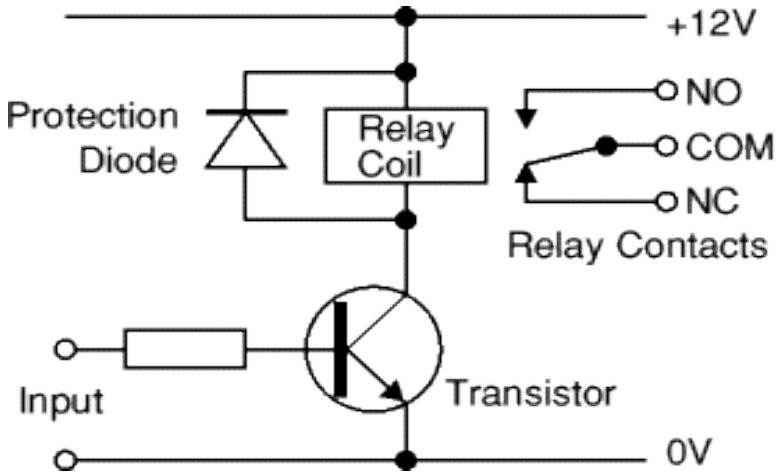


Fig: 5.2 Relay Operation and use of protection diodes

Transistors and ICs must be protected from the brief high voltage 'spike' produced when the relay coil is switched off. The above diagram shows how a signal diode (eg 1N4148) is connected across the relay coil to provide this protection. The diode is connected 'backwards' so that it will normally not conduct. Conduction occurs only when the relay coil is switched off, at this moment the current tries to flow continuously through the coil and it is safely diverted through the diode. Without the diode no current could flow and the coil would produce a damaging high voltage 'spike' in its attempt to keep the current flowing.

In choosing a relay, the following characteristics need to be considered:

1. The contacts can be normally open (NO) or normally closed (NC). In the NC type, the contacts are closed when the coil is not energized. In the NO type, the contacts are closed when the coil is energized.

2. There can be one or more contacts. i.e., different types like SPST (single pole single throw), SPDT (single pole double throw) and DPDT (double pole double throw) relays.

3. The voltage and current required to energize the coil. The voltage can vary from a few volts to 50 volts, while the current can be from a few milliamps to 20milliamps. The relay has a

minimum voltage, below which the coil will not be energized. This minimum voltage is called the “pull-in” voltage.

4. The minimum DC/AC voltage and current that can be handled by the contacts. This is in the range of a few volts to hundreds of volts, while the current can be from a few amps to 40A or more, depending on the relay.

5.2 Transistor Driver Circuit:

An SPDT relay consists of five pins, two for the magnetic coil, one as the common terminal and the last pins as normally connected pin and normally closed pin. When the current flows through this coil, the coil gets energized. Initially when the coil is not energized, there will be a connection between the common terminal and normally closed pin. But when the coil is energized, this connection breaks and a new connection between the common terminal and normally open pin will be established. Thus when there is an input from the microcontroller to the relay, the relay will be switched on. Thus when the relay is on, it can drive the loads connected between the common terminal and normally open pin. Therefore, the relay takes 5V from the microcontroller and drives the loads which consume high currents. Thus the relay acts as an isolation device.

Digital systems and microcontroller pins lack sufficient current to drive the relay. While the relay’s coil needs around 10milli amps to be energized, the microcontroller’s pin can provide a maximum of 1-2milli amps current. For this reason, a driver such as a power transistor is placed in between the microcontroller and the relay.

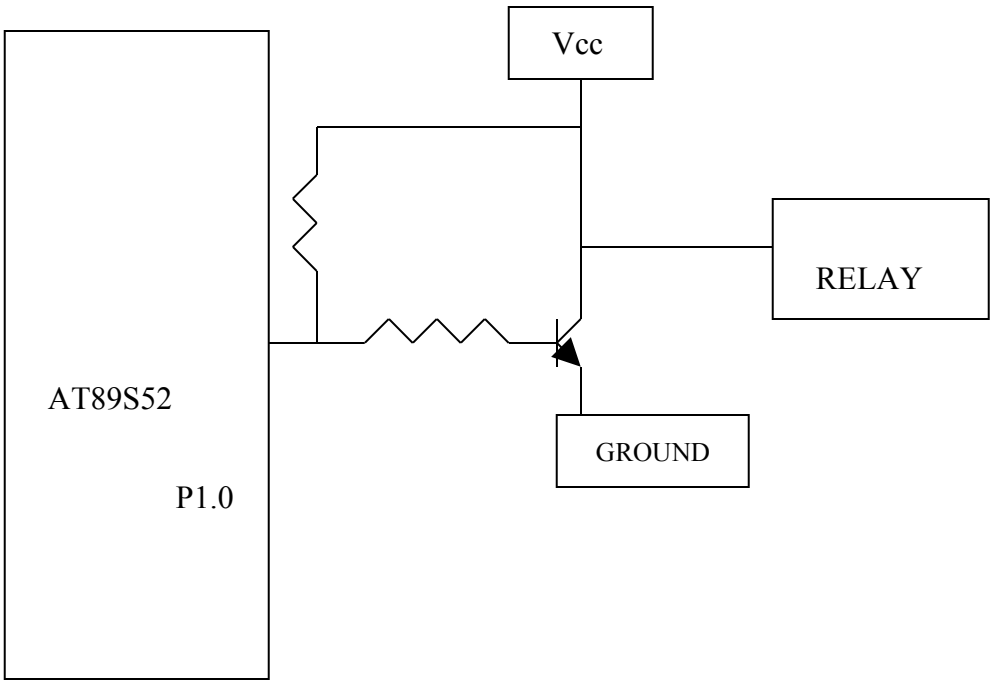


Fig: 5.3 Interfacing with Microcontroller

The operation of this circuit is as follows:

The input to the base of the transistor is applied from the microcontroller port pin P1.0. The transistor will be switched on when the base to emitter voltage is greater than 0.7V (cut-in voltage). Thus when the voltage applied to the pin P1.0 is high i.e., P1.0=1 (>0.7V), the transistor will be switched on and thus the relay will be ON and the load will be operated.

When the voltage at the pin P1.0 is low i.e., P1.0=0 (<0.7V) the transistor will be in off state and the relay will be OFF. Thus the transistor acts like a current driver to operate the relay accordingly.

RELAY INTERFACING WITH THE MICROCONTROLLER:

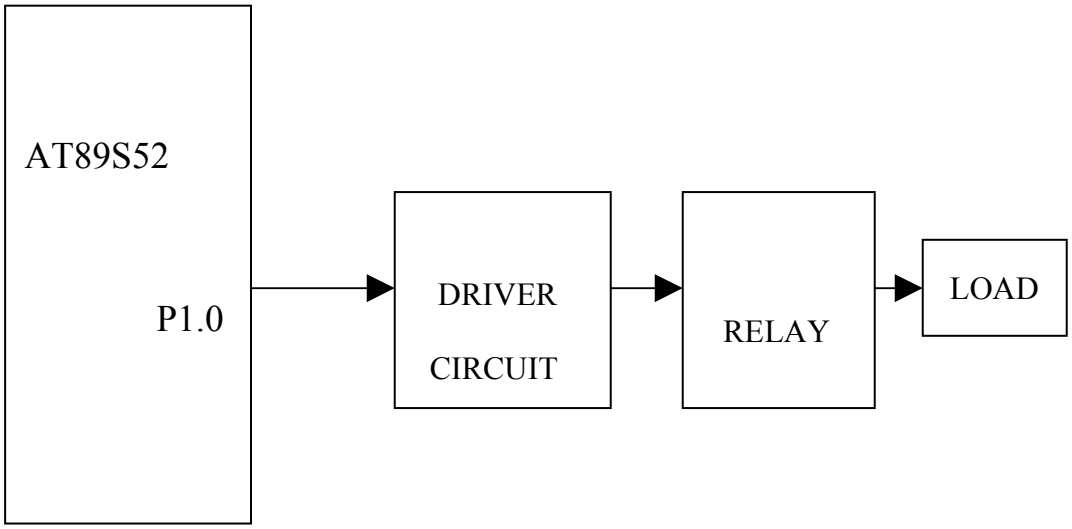
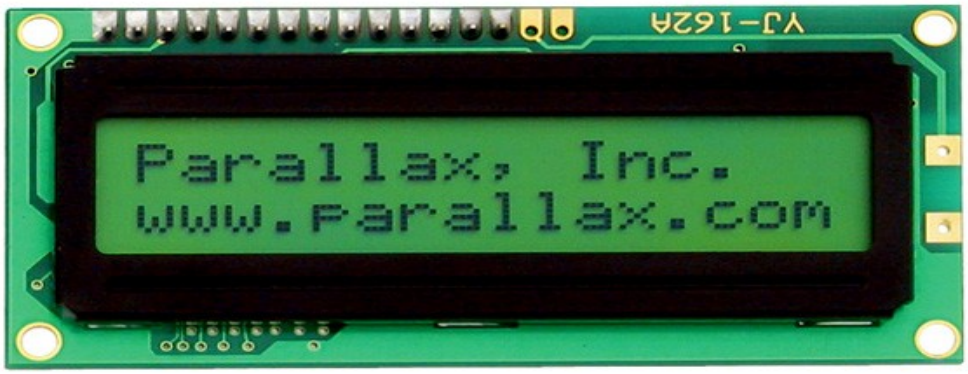


Fig: 5.4 Relay Interfacing With the Microcontroller



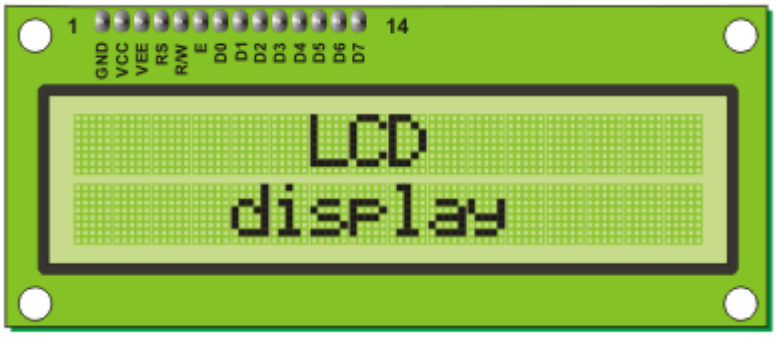
LCD INTERFACING

6.1 LIQUID CRYSTAL DISPLAY:

LCD stands for **L**iquid **C**rystal **D**isplay. LCD is finding wide spread use replacing LEDs (seven segment LEDs or other multi segment LEDs) because of the following reasons:

1. The declining prices of LCDs.
2. The ability to display numbers, characters and graphics. This is in contrast to LEDs, which are limited to numbers and a few characters.
3. Incorporation of a refreshing controller into the LCD, thereby relieving the CPU of the task of refreshing the LCD. In contrast, the LED must be refreshed by the CPU to keep displaying the data.
4. Ease of programming for characters and graphics.

These components are "specialized" for being used with the microcontrollers, which means that they cannot be activated by standard IC circuits. They are used for writing different messages on a miniature LCD.



A model described here can display messages in two lines with 16 characters each . It displays all the alphabets, Greek letters, punctuation marks, mathematical symbols etc. In addition, it is possible to display symbols that user makes up on its own. Automatic shifting message on display (shift left and right), appearance of the pointer, backlight etc. are considered as useful characteristics.

6.2 Pins Functions:

There are pins along one side of the small printed board used for connection to the microcontroller. There are total of 14 pins marked with numbers (16 in case the background light is built in). Their function is described in the table below:

Function	Pin Number	Name	Logic State	Description
Ground	1	Vss	-	0V
Power supply	2	Vdd	-	+5V
Contrast	3	Vee	-	0 – Vdd
Control of operating	4	RS	0 1	D0 – D7 are interpreted as commands D0 – D7 are interpreted as data
	5	R/W	0 1	Write data (from controller to LCD) Read data (from LCD to controller)
	6	E	0 1 From 1 to 0	Access to LCD disabled Normal operating Data/commands are transferred to LCD
Data / commands	7	D0	0/1	Bit 0 LSB
	8	D1	0/1	Bit 1
	9	D2	0/1	Bit 2
	10	D3	0/1	Bit 3
	11	D4	0/1	Bit 4
	12	D5	0/1	Bit 5
	13	D6	0/1	Bit 6
	14	D7	0/1	Bit 7 MSB

LCD screen:

LCD screen consists of two lines with 16 characters each. Each character consists of 5x7 dot matrix. Contrast on display depends on the power supply voltage and whether messages are displayed in one or two lines. For that reason, variable voltage 0-Vdd is applied on pin marked as Vee. Trimmer potentiometer is usually used for that purpose. Some versions of displays have built in backlight (blue or green diodes). When used during operating, a resistor for current limitation should be used (like with any LE diode).

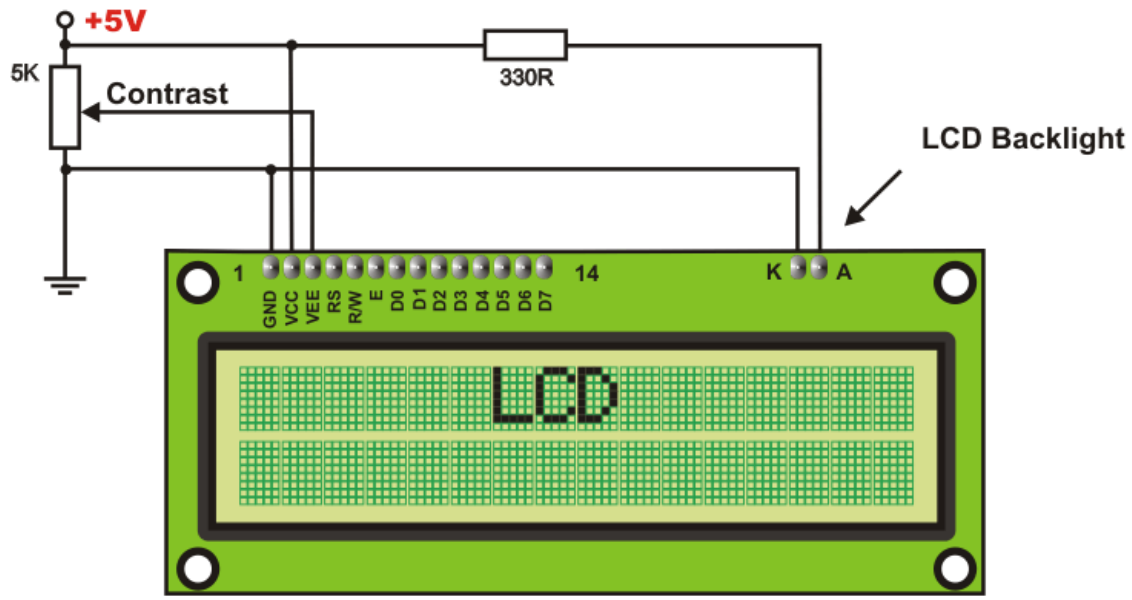


Fig: 6.1Pin Diagram of LCD

6.4 LCD Basic Commands

All data transferred to LCD through outputs D0-D7 will be interpreted as commands or as data, which depends on logic state on pin RS:

RS = 1 - Bits D0 - D7 are addresses of characters that should be displayed. Built in processor addresses built in “map of characters” and displays corresponding symbols. Displaying position is determined by DDRAM address. This address is either previously defined or the address of previously transferred character is automatically incremented.

RS = 0 - Bits D0 - D7 are commands which determine display mode. List of commands which LCD recognizes are given in the table below:

Command	RS	RW	D7	D6	D5	D4	D3	D2	D1	D0	Execution Time
Clear display	0	0	0	0	0	0	0	0	0	1	1.64mS
Cursor home	0	0	0	0	0	0	0	0	1	x	1.64mS
Entry mode set	0	0	0	0	0	0	0	1	I/D	S	40uS
Display on/off control	0	0	0	0	0	0	1	D	U	B	40uS
Cursor/Display Shift	0	0	0	0	0	1	D/C	R/L	x	x	40uS
Function set	0	0	0	0	1	DL	N	F	x	x	40uS
Set CGRAM address	0	0	0	1	CGRAM address						40uS
Set DDRAM address	0	0	1	DDRAM address							40uS
Read “BUSY” flag (BF)	0	1	BF	DDRAM address							-
Write to CGRAM or DDRAM	1	0	D7	D6	D5	D4	D3	D2	D1	D0	40uS
Read from CGRAM or DDRAM	1	1	D7	D6	D5	D4	D3	D2	D1	D0	40uS

I/D 1 = Increment (by 1)

0 = Decrement (by 1)

S 1 = Display shift on

0 = Display shift off

D 1 = Display on

0 = Display off

U 1 = Cursor on

0 = Cursor off

B 1 = Cursor blink on

0 = Cursor blink off

R/L 1 = Shift right

0 = Shift left

DL 1 = 8-bit interface

0 = 4-bit interface

N 1 = Display in two lines

0 = Display in one line

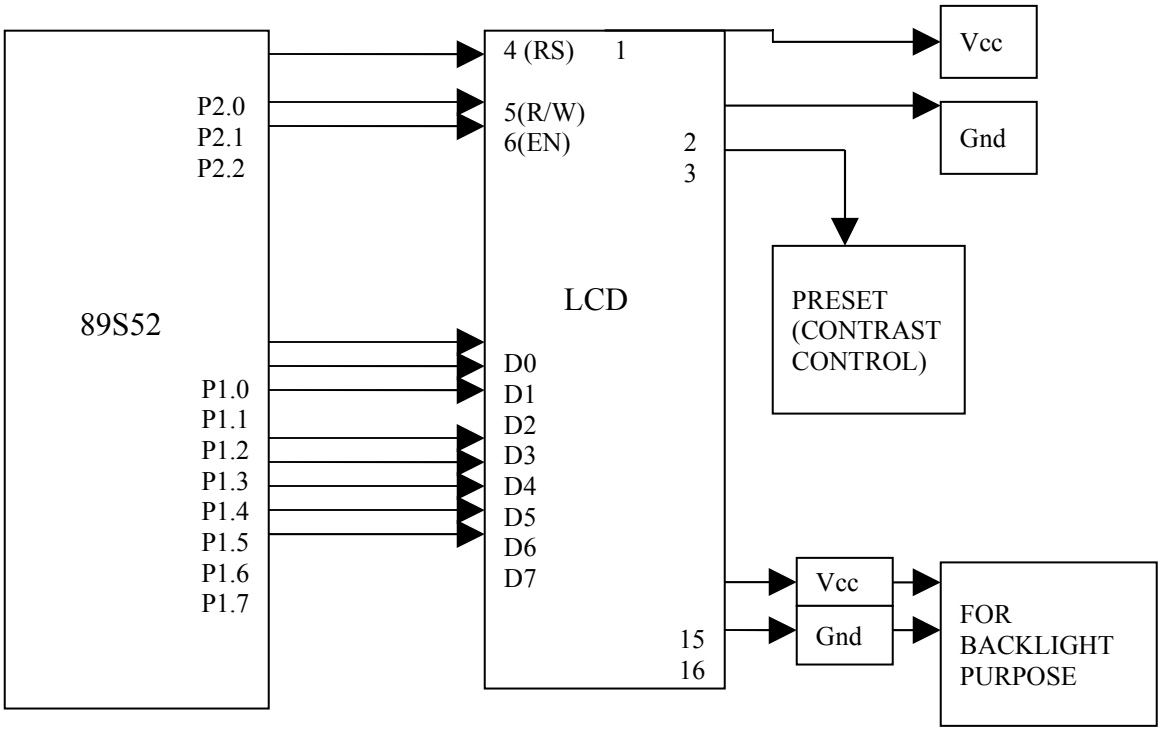
F 1 = Character format 5x10 dots

0 = Character format 5x7 dots

D/C 1 = Display shift

0 = Cursor shift

6.5 LCD INTERFACING WITH THE MICROCONTROLLER:



SWITCHES

7.1 SWITCH INTERFACING WITH THE MICROCONTROLLER:

Switches are the most widely used input/output devices of the 8051.

CPU accesses the switches through ports. Therefore these switches are connected to a microcontroller. This switch is connected between the supply and ground terminals. A single microcontroller (consisting of a microprocessor, RAM and EEPROM and several ports all on a single chip) takes care of hardware and software interfacing of the switch.

These switches are connected to an input port. When no switch is pressed, reading the input port will yield 1s since they are all connected to high (Vcc). But if any switch is pressed, one of the input port pins will have 0 since the switch pressed provides the path to ground. It is the function of the microcontroller to scan the switches continuously to detect and identify the switch pressed.

The switches that we are using in our project are 4 leg micro switches of momentary type.

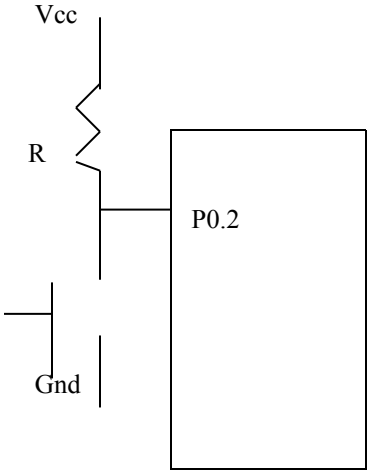


Fig: 7.1 Interfacing switch with the microcontroller

Thus now the two conditions are to be remembered:

1. When the switch is open, the total supply i.e., Vcc appears at the port pin P0.2

   P0.2 = 1

2. When the switch is closed i.e., when it is pressed, the total supply path is provided to ground. Thus the voltage value at the port pin P0.2 will be zero.

   P0.2 = 0

By reading the pin status, the microcontroller identifies whether the switch is pressed or not. When the switch is pressed, the corresponding related to this switch press written in the program will be executed.

8. REAL TIME CLOCK:

The real time clock (RTC) is a widely used device that provides accurate time and date for many applications. The RTC chip present in the PC provides time components of hour, minute and second in addition to the date/calendar components of year, month and day.The RTC chip uses an internal battery that keeps the time and date even when the power is off.One of the most widely used RTC chips is the DS1307 from Dallas semiconductor.

8.1 Description:

The DS1307 serial real-time clock (RTC) is a low power, full binary-coded decimal (BCD) clock/calendar plus 56 bytes of NV SRAM. Address and data are transferred serially through an I2C, bidirectional bus. The clock/calendar provides seconds, minutes, hours, day, date, month, and year information. The end of the month date is automatically adjusted for months with fewer than 31 days, including corrections for leap year. The clock operates in either the 24-hour or 12-hour format with AM/PM indicator.

The DS1307 has a built-in power-sense circuit that detects power failures and automatically switches to the backup supply. Timekeeping operation continues while the part operates from the backup supply.

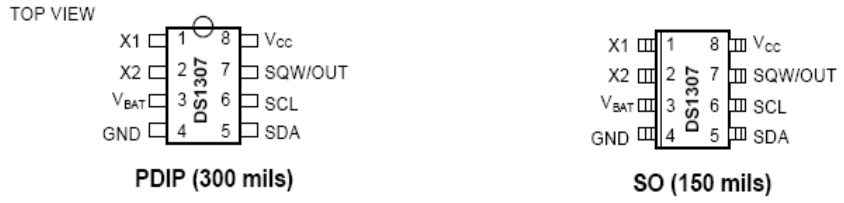


Fig: 8.1Pin configurations

8.2 FEATURES:

- Real-Time Clock (RTC) Counts seconds, minutes, hours, date of the month, month, day of the week, and year with Leap-Year Compensation valid up to 2100.
- 56-Byte, Battery-Backed, Nonvolatile (NV) RAM for Data Storage.
- I2C Serial Interface.
- Programmable Square-Wave Output Signal.
- Automatic Power-Fail Detect and Switch Circuitry.
- Consumes Less than 500nA in Battery-Backup Mode with Oscillator Running.
- Optional Industrial Temperature Range:-40°C to +85°C.
- Available in 8-Pin Plastic DIP or SO.

The DS1307 is a low-power clock/calendar with 56 bytes of battery-backed SRAM. The clock/calendar provides seconds, minutes, hours, day, date, month, and year information. The date at the end of the month is automatically adjusted for months with fewer than 31 days, including corrections for leap year.

The DS1307 operates as a slave device on the I2C bus. Access is obtained by implementing a START condition and providing a device identification code followed by a register address. Subsequent registers can be accessed sequentially until a STOP condition is executed. When VCC falls below 1.25 x VBAT, the device terminates an access in progress and resets the device address counter. Inputs to the device will not be recognized at this time to prevent erroneous data from being written to the device from an out-of tolerance system. When VCC falls below VBAT, the device switches into a low-current battery-backup mode. Upon power-up, the device switches from battery to VCC when VCC is greater than VBAT +0.2V and recognizes inputs when VCC is greater than 1.25 x VBAT.

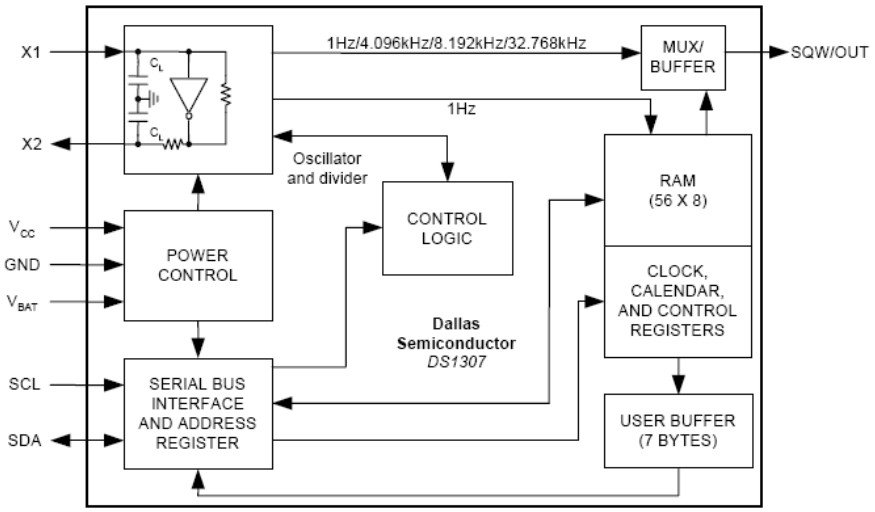


Fig: 8.2 Block diagram

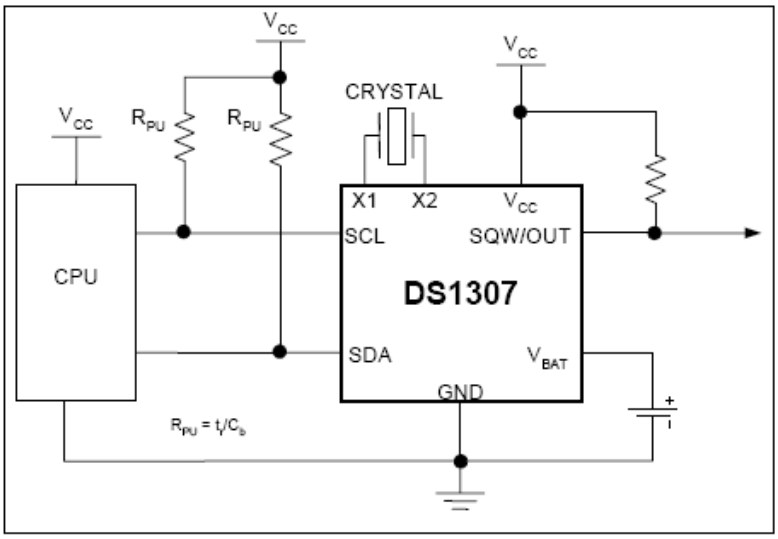
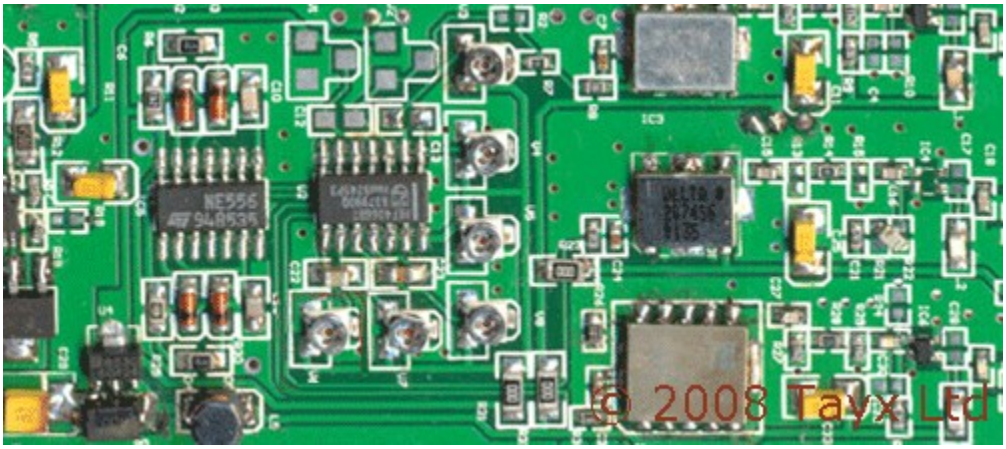


Fig: 8.3 Operating circuit

MOBILE JAMMER

A portable cell phone jammer featured by universal and handheld design, could blocking worldwide cell phone networks within 2-5 meters, including GSM900MHz, GSM1800MHz, GSM850MHz/CDMA800MHz and also 3G networks (UMTS / W-CDMA).



9.1 Operation:

As with other radio jamming, cell phone jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use. This causes enough interference with the communication between cell phones and towers to render the phones unusable. On most retail phones, the network would simply appear out of range. Most cell phones use different bands to send and receive communications from towers (called full duplexing). Jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies. Smaller handheld models block all bands from 800MHz to 1900MHz within a 16-feet range (5 meters). Small devices tend to use the former method, while larger more expensive models may interfere directly with the tower. The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units.

Actually it needs less energy to disrupt signal from tower to mobile phone, than the signal from mobile phone to the tower (also called base station), because base station is located at larger distance from the jammer than the mobile phone and that is why the signal from the tower is not so strong.

9.1.1 DESIGN AND IMPLEMENTATION OF MOBILE JAMMER:

The block diagram of mobile jammer consists of 4 main blocks. Those are

- Power supply
- IF section
- RF section
- Antennas

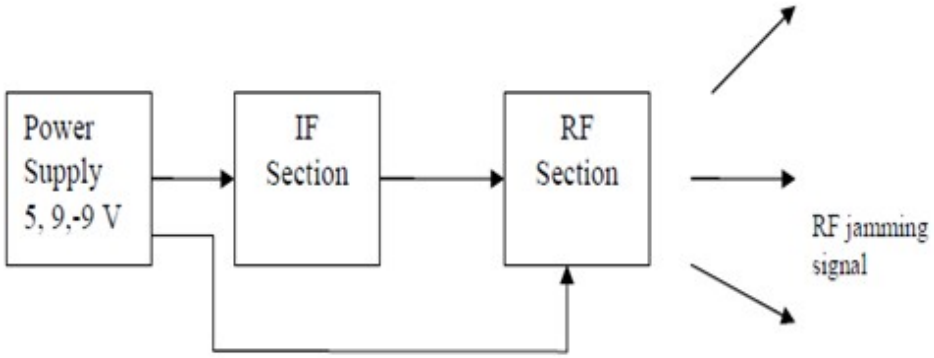


Fig: 9.1 Block Diagram of Mobile Jammer

Explanation of Each Block

9.2 Power Supply:

The mobile Jammer was designed for fixed use, and to take its power from the regular 220V AC wall outlets. The IF & RF sections of the jammer require +5V, +9Vand -9V dc.So a dc-dual polarity power supply should be designed.

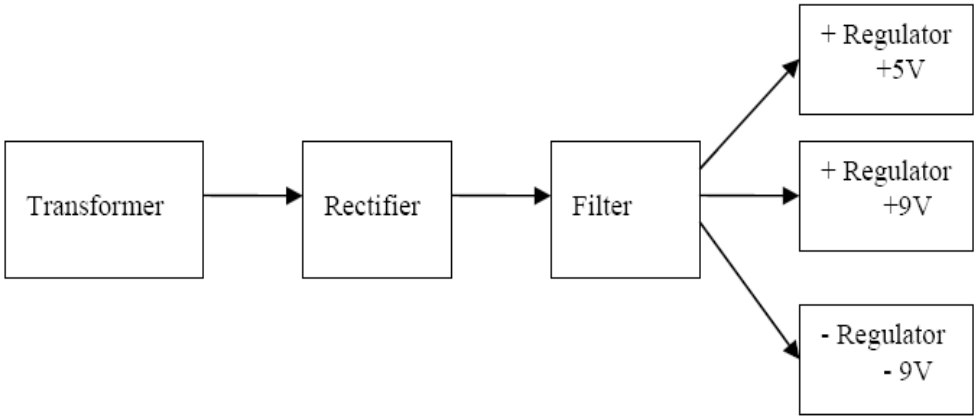


Fig: 9.2 Block Diagram of Dual polarity Power supply

The basic parts of power supply are rectifier, filter and regulator. The rectifier converts ac voltage to a pulsating dc voltage and can be either half wave rectifier and full wave rectifier, the one we use here is the full wave rectifier which has the advantage that it allows unidirectional current to the load during the entire cycle of the input voltage and the result of the full wave rectification is an output voltage with a frequency twice the input frequency that pulsated every half cycle of the input. The average value for a full wave rectifier for a sinusoidal input is given by

$$Vavg = 2 * Vp/\pi$$

The full wave rectifier used in the project is a full wave bridge rectifier, which uses four diodes the peak output is given by the

$$Vp = Vpsec - 1.4,$$

Where Vpsec is the output voltage across the secondary winigng of the transformer .In th project the transformer used is 220/12,1.5A rating ,So Vavg=11V and Vp=15.88V.

The second part of the power supply is the filter which eliminate the fluctuations in the output of the full wave rectifier so as to produce a constant dc voltage ,the filter is simply a capacitor and its chosen to be as large as possible to minimize voltage ripple in the output.

The final part of the power supply is the regulator and it is used to provide the desired constant dc output that is basically independent of the input voltage. Single chip regulators were used to give +5V, +9V and -9V dc voltages.

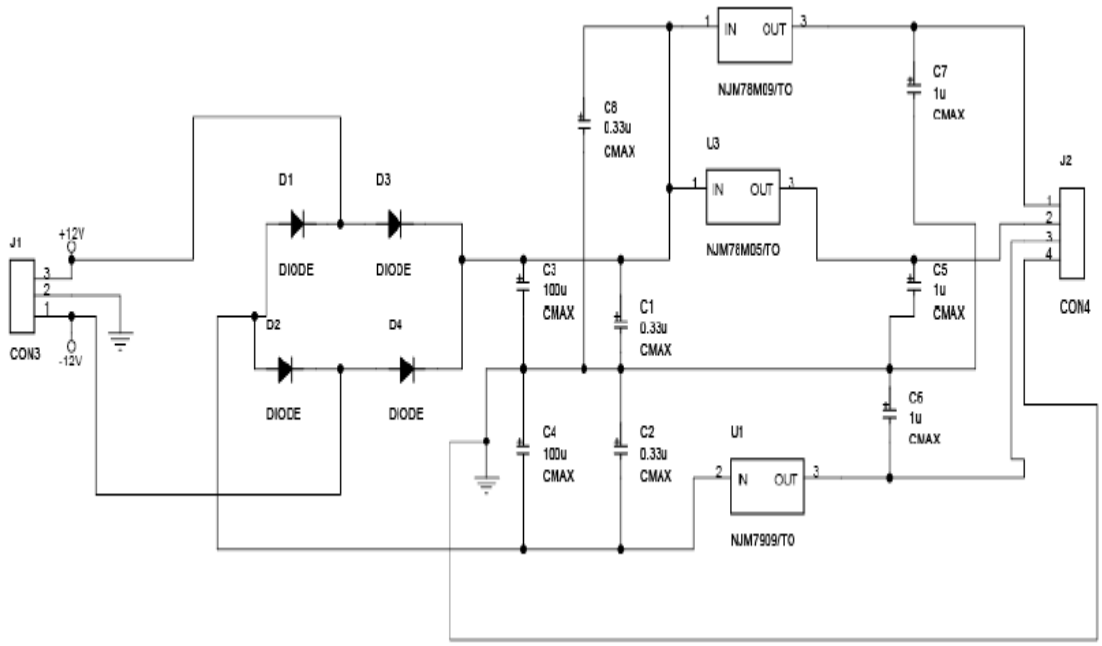


Fig: 9.3 Circuit Schematic of the power supply

9.3 IF SECTION:

The function of IF section of jammer is to generate tuning signal for the VCO in the RF section, which will sweep the VCO through the desired range of frequencies. This tuning signal is generated by a triangular wave generator along with noise generator, and then offset by proper amount so as to sweep the VCO output from the minimum desired frequency to a maximum.

9.3.1 TRIANGULAR WAVE GENERATOR:

To generator triangular wave we use 555 timer as a Astable Multivibrator

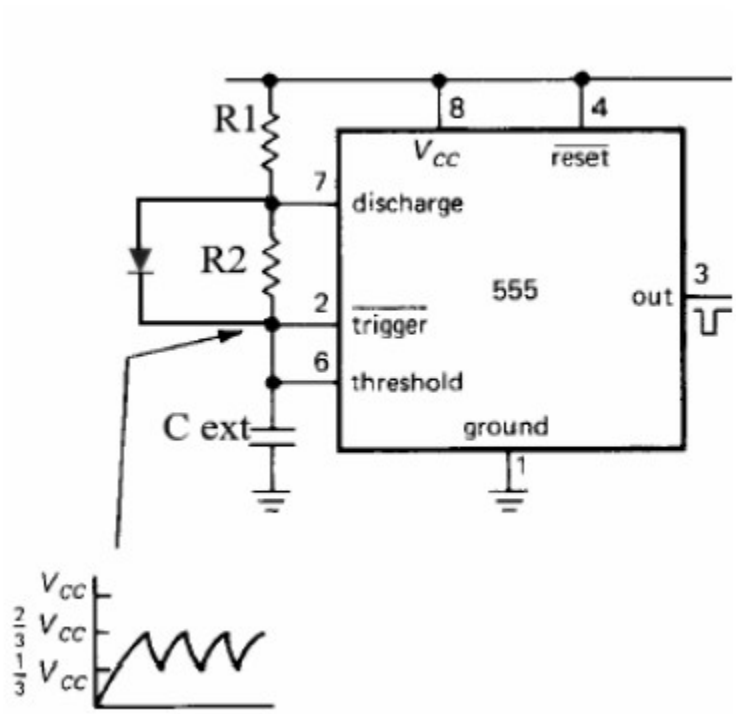


Fig: 9.4 IC **555**Timer connected as oscillator

The 555 timer consist basically of two comparators, a flip-flop, a discharge transistor, and a resistive voltage divider. The resistive divider is used to set the voltage comparator levels.

A 555 timer connected to operate in the astable mode as a free running non –sinusoidal oscillator, the threshold input is connected to the trigger input. The external components R1,R2 and Cex forms the timing circuit that sets the frequency of oscillation. The 0.01 uF capacitor connected to the control input is strictly for decoupling and has no effect on the operation, in some cases it can be left off. Initially when the power is turned on, the capacitor Cex is uncharged and thus the trigger voltage(pin2) is at 0V.This causes the output of the lower comparator to be high and the output of the upper comparator to be low, forcing the output of the flip-flop, and thus the base of Qd, low and keeping the transistor off. Now,Cex begin charging through R1 & R2 (to obtain 50% duty cycle, one can connect a diode parallel with R2 and choose R2=R1). When the capacitor voltage reaches 1/3Vcc,the lower comparator switcher to its low output state, and when the capacitor voltage reaches 2/3Vcc the upper comparator switches to its high output state. This reset the flipflop causes the base of Qd to go high, and turns on the transistor. This sequence creates a charge path for the capacitor through R2 and the transistor, as indicated. Yhe capacitor begins to discharge, causing the upper comparator to go low. At the point when capacitor discharge down to 1/3Vcc, the lower comparator switches high, setting the flipflop, which makes the base of Qd low and turns off the transistor. Another charging cycles begins and entire process repeats the result is a rectangular wave output whose duty cycle depends on the values of R1 and R2, The frequency of oscillator is given by the following formula:

$$fr = \frac{1.44}{(R1+R2)Cex}$$

Using the above equation for frequency equal 110KHz, one found the values of R1, R2, and Cex. Then the output was taken from the voltage on the external capacitor which has triangular wave form. A simulation was done to verify the operation of circuit and the output is shown in figure.

To avoid loading the timing circuit and changing the operation frequency, the triangular wave on the terminal of the external capacitor was buffered using op-amp

9.3.2 NOISE GENERATOR:

To achieve jamming a noise signal is mixed with the triangle wave signal to produce the tuning voltage for the VCO. The noise will help in masking the jamming transmission, making it look like random "noise" to an outside observer. Without the noise generator, the jamming signal is just a sweeping, unmodulated continuous wave RF carrier.

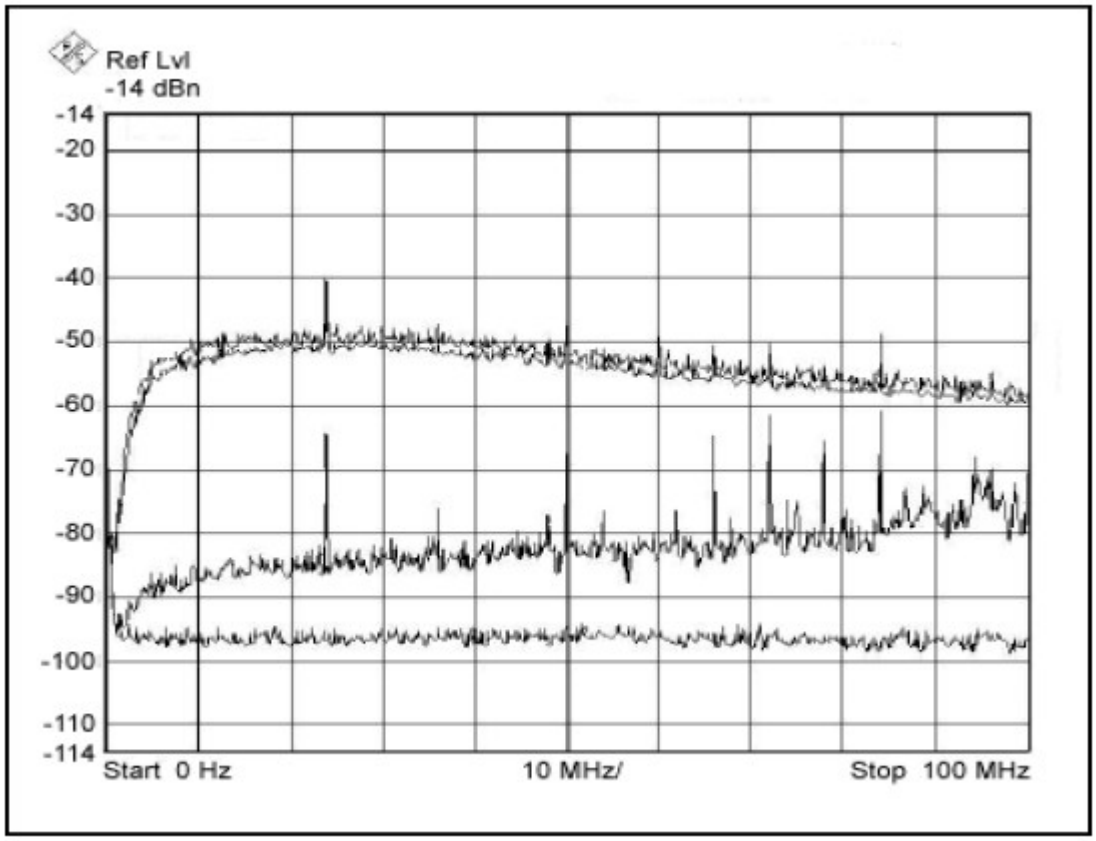


Fig: 9.5 White noise generator output spectrum

9.3.3Signal mixer and DC-Offset circuits:

The triangle wave and noise signals are mixed using OP-Amp configured as summer, then a dc voltage is added to the resulted signal to obtain the required tuning voltage using Diode-clamper circuit. To gain good clamping the RC time constant selected so that it's more than ten times the period of the input frequency, also a potentiometer was added to control the biasing voltage so as to get the desired tuning voltage.

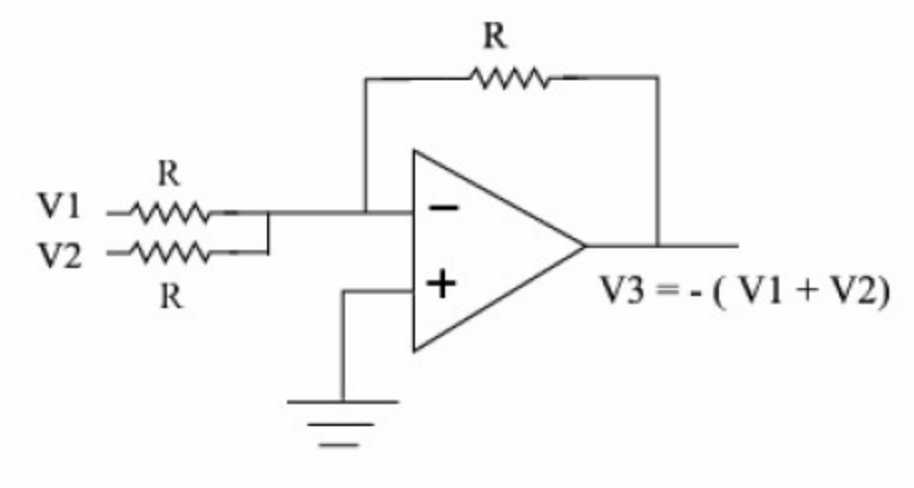


Fig: 9.6 Op-Amp Summer Circuit

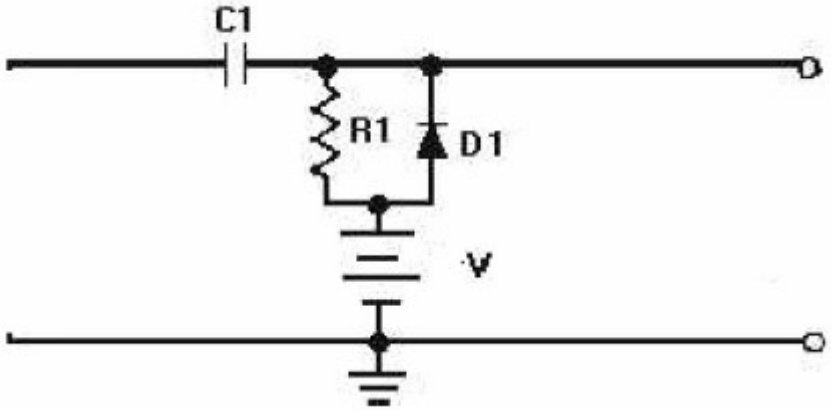


Fig: 9.7 Positive diode with Clamper bias

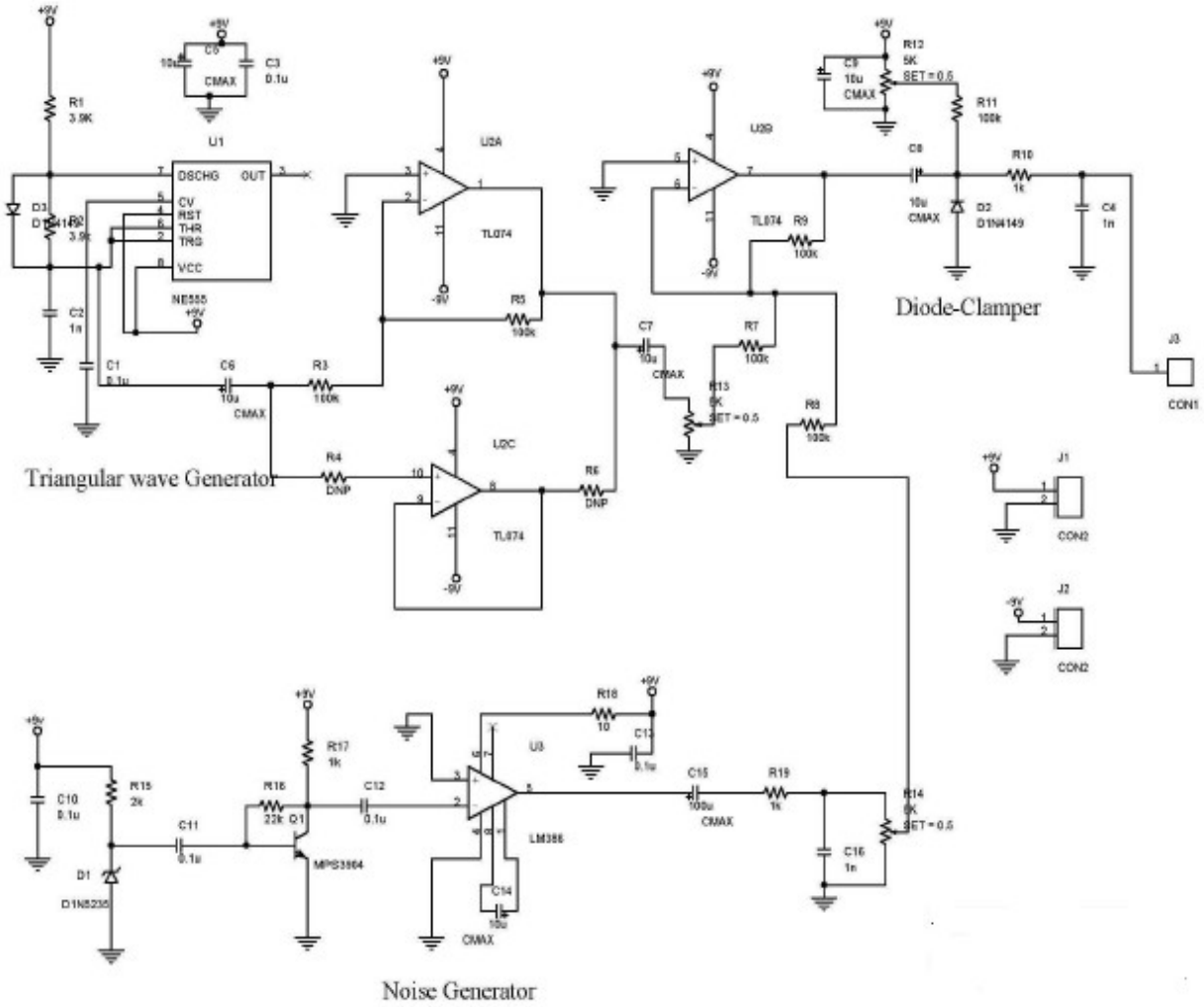


Fig: 9.8 Block Diagram of IF Section

9.4 RF SECTION:

The RF-section is the most important part of the mobile jammer it consist of the Voltage Controlled oscillator(VCO),RF Power amplifier ,and the antenna.These components were selected according to the desired specification of the jammer such as the frequency range and the coverage range .Its important to note that all the components used has 50 ohm input/output impedance, so 50 ohm microstrip was needed for matching between the components.

To obtain the desired output jamming power for coverage range of 20m first we found the jamming power required at the mobile receiver"Jr", knowing that SNRmin =9dB and Smax =-15dBm (i.e worst jamming case).[5] then from

SNRmin=S/J,where S=the signal power

Jr=-24dbm,then by invoking the free space path loss equation

F=32.45+20log(f*D),where "Ds" is distance in km and "f " is frequency in MHz for 20 m the loss equals 58dB hence the jammer should transmit a jamming signal with power equals : 58dBm-24dBm=34dBm,to sustain a 20m area

9.4.1 Voltage controlled oscillator:

The VCO is responsible for generating the RF signal which will over power the mobile downlink signal. The selection of the VCO was influenced by two main factors, the frequency of the GSM system, which will be jammed and the availability of the chip. For the first factor which implies that the VCO should cover the frequencies from 935 MHz to 960 MHz , The MAX2623 VCO from MAXIM IC was found to be a good choice , and fortunately the second factor was met sequentially since MAXIM IC was willing to send two of the MAX2623 for free.

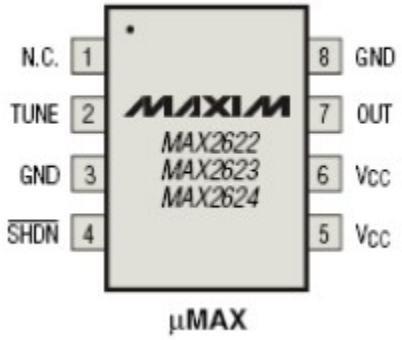


Fig: 9.9 Pin diagram of MAXIM

The MAX2623 VCO is implemented as an LS oscillator configuration, integrating all tank circuit of the tank circuit on-chip, this makes the VCO extremely easy-to-use , and the tuning input is internally connected to the varactor as shown in figure .The typical output power is -3dBm, and the output was best swept over the desired range when the input tuning voltage was around 120 KHz.

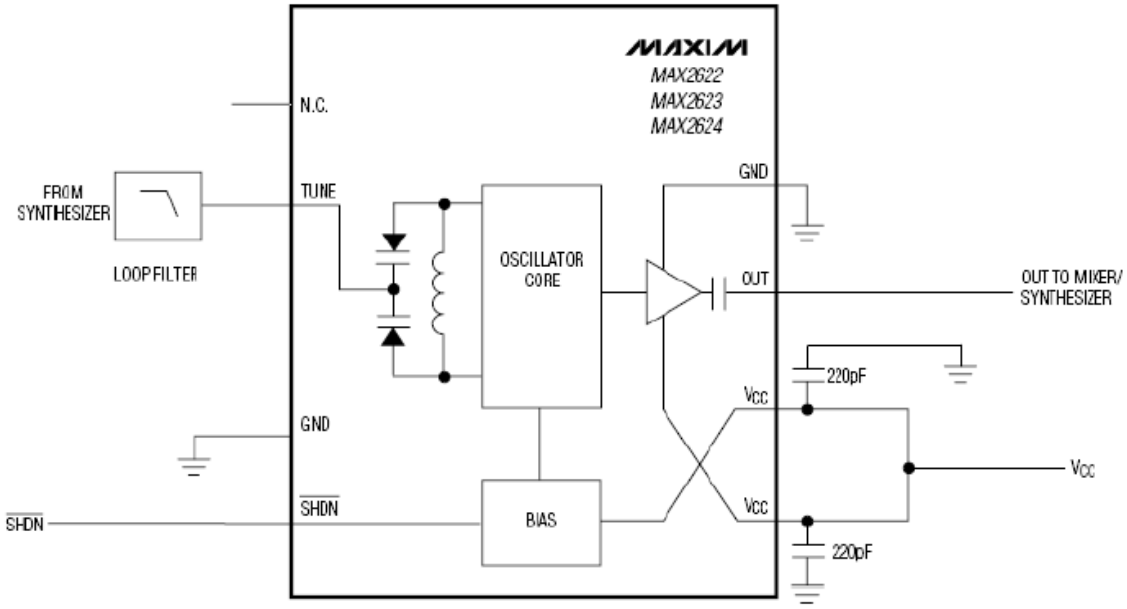


Fig: 9.10 MAXIM 2623 Pin connection

ABOUT VCO:

- Fully Monolithic
- Guaranteed Performance
- On-Chip 50Ω Output Match
- 885MHz to 950MHz (MAX2623)
- +2.7V to +3.3V Single-Supply Operation
- Low Current Shutdown Mode
- Smaller than Modules (8-pin µMAX package)

Pin description of VCO:

1- NC- No Connection. Not internally connected.

2-TUNE- Oscillator Frequency Tuning Voltage Input. High-impedance input with a voltage input range of 0.4V (low frequency) to 2.4V (high frequency) adjustment.

3-GND-Ground Connection for Oscillator and Biasing requires a low-inductance connection to the circuit board ground plane.

4- SHDN-Shutdown Logic Input. A high-impedance input logic level low disables the device and reduces supply current to 0.1μA. A logic level high enables the device

5- VCC-Output Buffer DC Supply Voltage Connection,bypass with a 220pF capacitor to GND for best high frequency performance

6 - VCC-Bias and Oscillator DC Supply Voltage Connection. Bypass with a 220pF capacitor to GND for low noise and low spurious content performance from the oscillator

7 -OUT Buffered Oscillator Output

8- GND-Ground Connection for Output Buffer. Requires a low-inductance connection to the circuit board ground plane.

9.4.2 RF Power Amplifier:

To achieve the desired output power a gain stage was needed, about searching for a suitable power amplifier it is cheaper to use power amplifier from an old Mobile phones.The PF08103b hitachi power amplifier module from nokia mobile phone is sufficient to amplify an input signal in the range 800MHz to 1 GHz by 34 dB.But in the data sheet input should be 1dBm.To meet this requirement we use another power amplifier stage after vco and before hitachi power amplifier .For this stage we use Mar-4SM power amplifier.The MAR-4Sm has a typical gain of 8-dB for the frequencies range from dc to 1GHz,so the output at this stage is around 5dBm.

A typical biasing configuration for MAR-4SM is shown in the figure

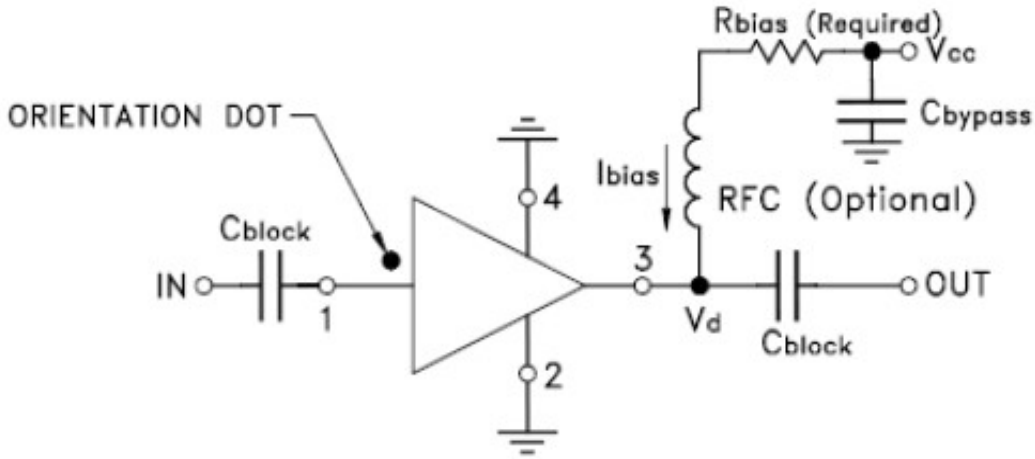


Fig: 9.11 Typical biasing configuration of MAR-4SM

Now the power before the Hitachi RF power amplifier is 5dBm and since 1dBm is required; so here we used 4dBm T-Network attenuator as shown in the figure.

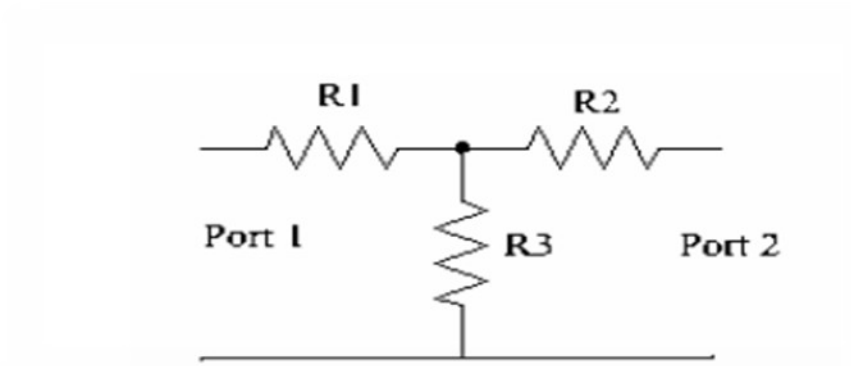


Fig: 9.12 T-Network attenuator

For a 4-dB attenuation and symmetric Network S12=S21=0.631

And for 50 ohms characteristic impedance we found the values of the resistor using the following equations

$50 = (R2 + 50)//(R3) + R1$

$$0.631 = \left(\frac{X}{X+R1}\right) * \left(\frac{50}{50+R1}\right),$$

Where X= (R2+50))//R3.

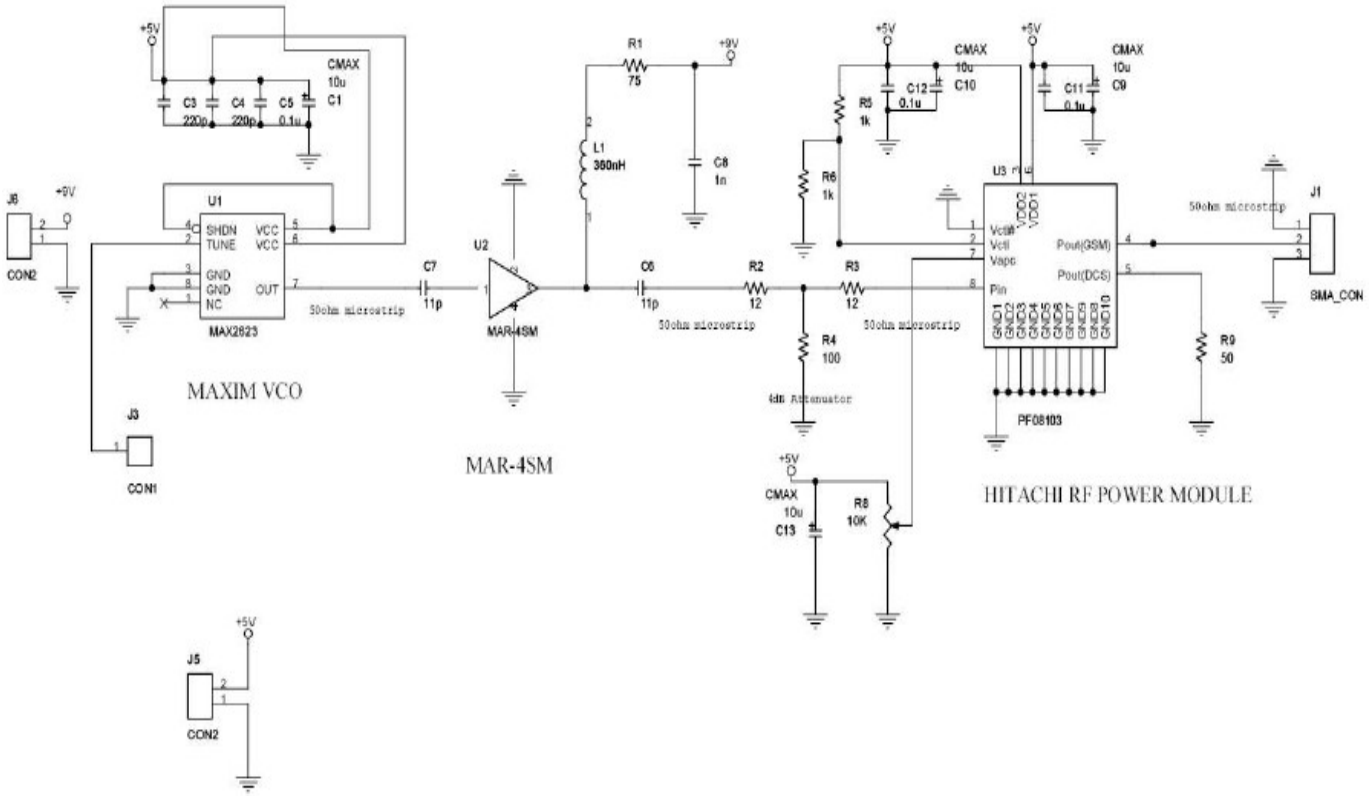


Fig: 9.13 Circuit diagram of RF section

9.5 Antenna:

The most important part of any transmitter is the antenna. So a suitable antenna should be selected .The antenna used in the project is λ/4 wave monopole antenna and it has 50 Ohm impedance so that the antenna is matched to the transmission system .Also this antenna has low VSWR less than 1.7,and a bandwidth of 150MHz around 916MHz center frequency which cover the mobile jammer frequency range .The antenna gain is 2dBi.

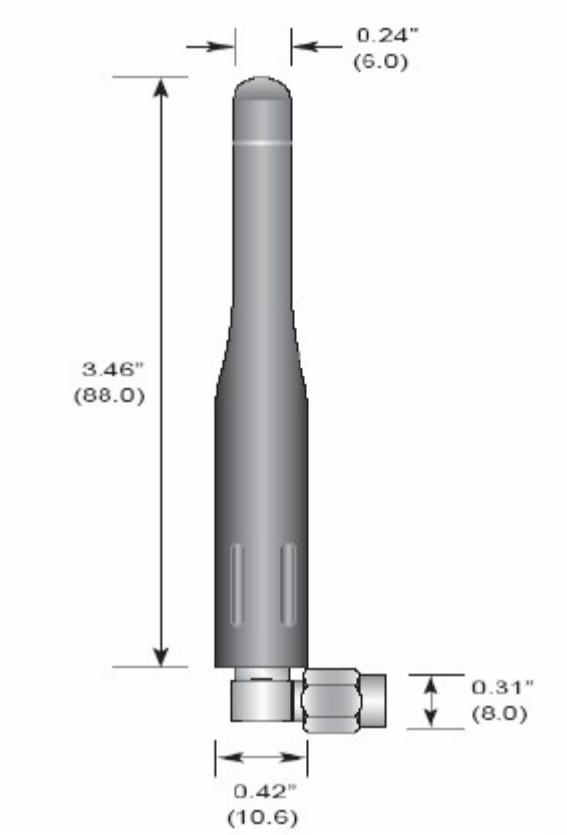


Fig: 9.14 λ/4 Monopole Antenna

The patterns for the antenna are shown below:

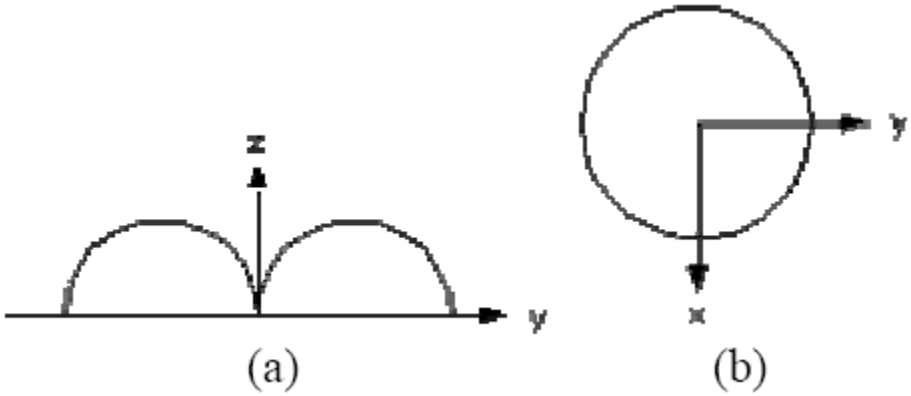


Fig: 9.15 (a) Monopole Principle E-plane pattern
(b) Monopole principle H-plane pattern

9.6 Mobile Jammer Requirement:

Jamming is successful when the jamming signal denies the usability of the communications transmission. In digital communication, the usability is denied when the error rate of the transmission cannot be compensated by error correction. Usually a successful jamming attack requires that the jammer power is roughly equal to signal at the receiver.

The effect of jamming depends on the jamming-to-signal ratio (J/S), modulation scheme, channel coding and interleaving of the target system.

Generally jamming-to-signal ratio can be measured according to the following Equation

$$\frac{J}{S} = \frac{PjGjrGrjR^2trLtrBr}{PtGtrGrtR^2jrLjBj}$$

Pj = jammer power

Pt = transmitter power

Gjr= antenna gain from jammer to receiver

Grj=antenna gain from receiver to jammer

Gtr=antenna gain from transmitter to receiver

Grt=antenna gain from receiver to transmitter

Br=communications receiver bandwidth

Bj=jamming transmitter bandwidth

Rtr=range between communications transmitter and receiver

Rjt=range between jammer and communication receiver

Lr= jammer signals loss (including polarization mismatch)

Lr= communication signal loss

The above equation indicates that the jammer Effective Radiated Power, which is the product of antenna gain and output power, should be high if jamming efficiency is required. On the other hand, in order to prevent jamming, the antenna gain towards the communication partner should be as high as possible while the gain towards the jammer should be as small as possible .As the equation shows, the antenna pattern, the relation between the azimuth and the gain, is a very important aspect in jamming

Also as we know from Microwave and shown in the equation distance has a strong influence on the signal loss. If the distance between jammer and receiver is doubled, the jammer has to quadruple its output in order for the jamming to have the same effect. It must also be noted here that jammer path loss is often different from the communication path loss. Hence gives jammer an advantage over communication transmitters.

SPECIFICATIONS :

Isolating Signal Bandwidth

GSM/CDMA: 850~960 MHz

GSM/CDMA1900 (DCS):1805~1990Mhz

3G: 2110~2170 MHz

Typical Coverage: 8 Meters

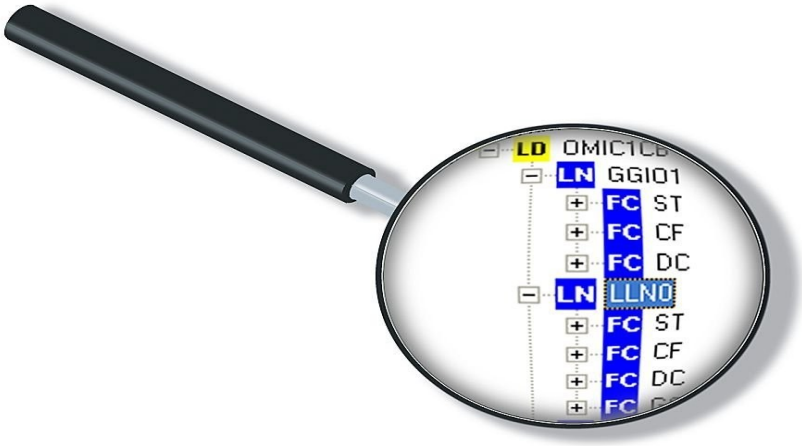
Average Output Power: 34 dBm

Typical Battery Life: 2 Hours

Power supply: Built in Rechargeable Li-ion battery

Dimension: Antennas off - 97mm x 45mm x 19mm (L x W x D)

Software Tools



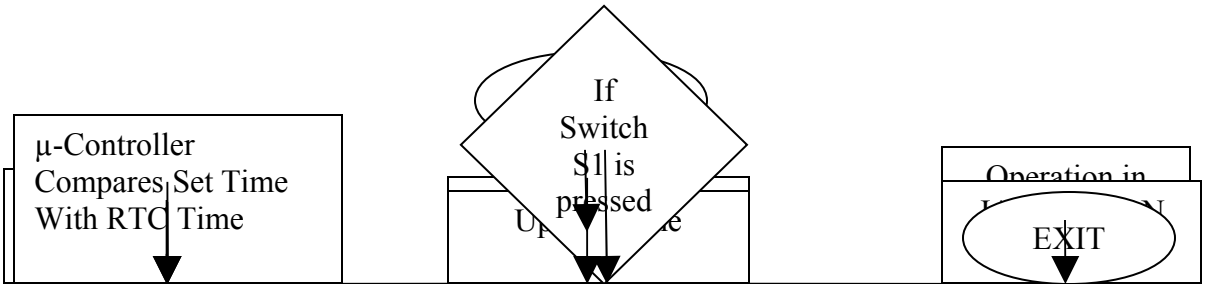
10.1 KEIL SOFTWARE:

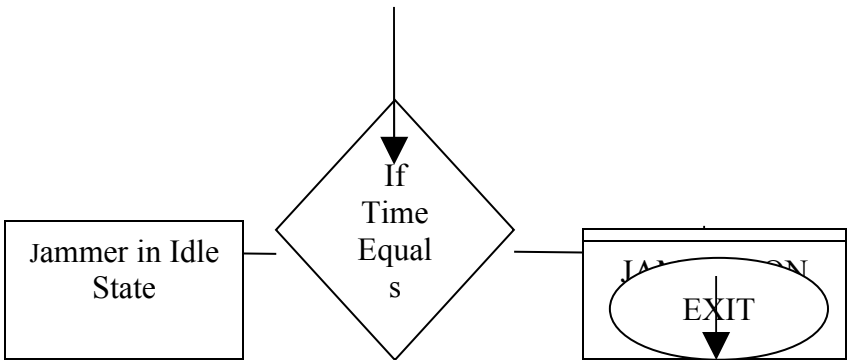
Keil compiler is a software used where the machine language code is written and compiled. After compilation, the machine source code is converted into hex code which is to be dumped into the microcontroller for further processing. Keil compiler also supports C language code.

10.2 PROLOAD:

Proload is a software which accepts only hex files. Once the machine code is converted into hex code, that hex code has to be dumped into the microcontroller placed in the programmer kit and this is done by the Proload. Programmer kit contains a microcontroller on it other than the one which is to be programmed. This microcontroller has a program in it written in such a way that it accepts the hex file from the keil compiler and dumps this hex file into the microcontroller which is to be programmed. As this programmer kit requires power supply to be operated, this power supply is given from the power supply circuit designed above. It should be noted that this programmer kit contains a power supply section in the board itself but in order to switch on that power supply, a source is required. Thus this is accomplished from the power supply board with an output of 12volts or from an adapter connected to 230 V AC.

11. Flow chart For Jammer Operation:




Jammer in Idle State
If Time Equal s
EXIT

ADVANTAGES

- Sophisticated Security.

- No loss of data due to back up battery.
- Works for both GSM and CDMA networks

APPLICATIONS

Main Locations:

Gas Stations, Oil and Gas Storage Facilities, Oil and Gas Fields, Hospitals, Theatres, Recording Studios, Banks, Contract Tendering Rooms, Churches, Conference Rooms, Classrooms, Testing Facilities, Security Services, Military Units, Secret Services, News Conference Rooms, Libraries, Museums, Prisons, Courts, Border Patrol and Drug Enforcement , Customs , Houses, Military Units, Police Units, Government Unit, Jail Unit.

1. Gas stations, the air entrainment station, the fuel depot and the flammable explosive chemical warehouse, the refinery, the petrified factory and so on need safely to protect place: May avoid changing suddenly the detonation which the signal radiative generation static electricity spark but causes, the fire. Posts the prohibition to dial the handset sign, does not have the initiative, this kind of accident all has the appearance in national many gas stations, in order to safeguard these important situations the security to be supposed to take the precautionary measure.

2. Governments, enterprise's each kind of conference room**:** May avoid the handset ting disturbs and answers when the telephone breaking the leader to speak but interrupts its person to hold a meeting.

3. Armies, public security department's important conference rooms**:** Might avoid the attending personnel divulging the military and the government using the handset is secret, at present the new spy science and technology, already used the handset interception, the monitor environment sound, therefore to important conference place, it is necessary to take effective also of security the initiative.

4. Hospitals**:** Might avoid the goon machine-hour but causing doctor to the hospital precision instrument equipment disturbance to misdiagnose, has delayed the rescue patient, as well as was surgery doctor to answer the handset telephone disturbance attention, underwent the surgery to doctor to the patient to be extremely disadvantageous.

5. Courts**:** May avoid the handset ting the disturbance, maintains the court conference site the dignity and the sacredness.

6. Libraries, New Bookstore**:** May avoid the handset ting and answer the telephone the noise, builds to study the study peaceful environment.

7. Theaters**:** As the upscale recreation area, eliminates the handset ting noise to be possible to maintain the audience to appreciate the program the interest.

8. Tests places, examination centre**:** May cease the examinee, monitor an exam the personnel to cheat using the modern communication facilities.

9. Schools classrooms and training organization classroom**:** May avoid the handset ting and answers when the handset telephone to attending class student's disturbance.

10. Instead fears the unit**:** Locking goal of tendency by handset telecontrolled bomb.

11. Coast defense unit**:** May prevent the seacoast smuggling member discloses secret information using the handset, effectively attacks smuggling criminal offender's smuggling.

12. The jail, detains the place**:** Prevented the criminal, the news media, the visit personnel, the prison tube does not collude with according to the stipulation inside and outside, forms conspires to get the story straight.

13. Church**:** May eliminate the handset signal noise, by maintains the religious place solemn and respectful.

CONCLUSION

In this project a GSM, CDMA, 3G Mobile jammer was designed and built. The project was tested against the networks and has proven success with average range of 5m.

Testing in different locations shows the dependent of the jamming range on the signal strength, for instance in low network coverage area of the base station the jamming range exceed 7m.In general the jamming attack was protected by network signal power, and having large power jamming device the Network will be jammed for sure, from this observation it can be concluded that the protection against jamming attack in the low coverage area was very weak and couldn't withstand the simplest jamming techniques.

The main disadvantage of the mobile jammer is that the transmission of the jamming signal which is prohibited by law in many countries, for instance the fines for this offense can range as high as 11,000$. Despite the legal issues the transmission of high power signal may affect the operation of some critical devices, such as hearing impairment hardware solution. These disadvantages will constrain the use of mobile jammer.

APPENDIX

SOURCE CODE:

```
#include<reg52.h>
#include<intrins.h>
sbit sda = P1^1;
sbit scl = P1^0;
sbit jammer_on = P1^3;
sbit update    = P1^4;
sbit inc       = P1^5;
sbit dec       = P1^6;
sbit alarm     = P1^7;

sbit  rs   =P3^0;
sbit  rw   =P3^1;
sbit  en   =P3^2;
void lcdcmd(unsigned char);
void lcddata(unsigned char);
void delay(unsigned int);
void displaymsg(unsigned char *p );
void convertion(unsigned char);
void send(unsigned int);
void start(void);
void stop(void);
unsigned int read(unsigned char,unsigned char );
void write(unsigned char ,unsigned  char,unsigned char );
unsigned char bcd2bin(unsigned char);
unsigned char bin2bcd(unsigned char );
//setalarm(unsigned char ,unsigned char  ,unsigned char,unsigned char );
setalarm(unsigned char,unsigned char,unsigned char,unsigned char);
unsigned int read(unsigned char,unsigned char );
void settime(unsigned char,unsigned char ,unsigned char,unsigned char,unsigned char);
```

```
unsigned char cmdarr[]={0x38,0x06,0x0e,0x01,0x0c,0x80};
code unsigned char msg11[]= "TIME            " ;

unsigned  char i,sec,k,j,z,r,hrs,min,ah1,am1,g,ah2,am2,ah3,am3,ah4,am4,check=0;
code unsigned char msg1[]= "TIME BASED      " ;
code unsigned char msg2[]= "MOBILE JAMMER";
code unsigned char msg3[]= "UPDATE THE TIME";
code unsigned char msg4[]= "00:00:00";
code unsigned char msg8[]= "SETALARM1        ";
code unsigned char msg9[]= "SETALARM2        ";
code unsigned char msg10[]= "JAMMER ON";

//code unsigned char msg10[ ]= "SETALARM3        ";
//code unsigned char msg12[ ]= "SETALARM4        ";

void main()
{
 P2=0x00;
  for(i=0;cmdarr[i]!='\0';i++)
 {
  lcdcmd(cmdarr[i]);
 }
 lcdcmd(0x80);
 displaymsg(msg1);
 lcdcmd(0xc0);
 displaymsg(msg2);

 delay(100);
  delay(100);
   delay(100);
```

```
   delay(100);
lcdcmd(0x01);
r =bcd2bin(read(0xd0, 0x00));

 {

}
 lcdcmd(0x80);
 displaymsg(msg11);
 delay(10);

 ah1=bcd2bin(read(0xd0,0x08));
 am1=bcd2bin(read(0xd0,0x0a));

 ah2=bcd2bin(read(0xd0,0x0b));

 //ah3=bcd2bin(read(0xd0,0x0d));
// am3=bcd2bin(read(0xd0,0x0e));

 //ah4=bcd2bin(read(0xd0,0x0f));
 //am4=bcd2bin(read(0xd0,0x10));

 while(1)
 {
  lcdcmd(0xc0);
  hrs=bcd2bin(read(0xd0, 0x02));
  convertion(hrs);
  lcdcmd(0xc2);
  lcddata(':');
  lcdcmd(0xc3);
  min=bcd2bin(read(0xd0, 0x01));
```

```
convertion(min);
lcddata(':');
sec=bcd2bin(read(0xd0, 0x00));
convertion(sec);
if (update==0)
{
 delay(10);
 while(update==0);
 lcdcmd(0x80);
 displaymsg(msg3);

 lcdcmd(0xc6);
 lcddata('0');
 lcddata('0');
 settime(0x02,23,0,0xc0,hrs );
 settime(0x01,59,0,0xc3,min);
 write(0xd0,0x00,0x00);

 lcdcmd(0x80);
 displaymsg(msg11);
 delay(200);
 }

 if(jammer_on==0)
 {
  delay(100);
        while(jammer_on==0);
        {
         P2=0xff;
         lcdcmd(0x01);
         displaymsg(msg10);
```

```
        lcdcmd(0xc0);
        displaymsg(msg11);
         while(1)
        {
        lcdcmd(0xc6);
        hrs=bcd2bin(read(0xd0, 0x02));
  convertion(hrs);
  lcdcmd(0xc8);
  lcddata(':');
  lcdcmd(0xc9);

  convertion(min);
  lcddata(':');
  sec=bcd2bin(read(0xd0, 0x00));
  convertion(sec);

         if(jammer_on==0)
         {
          while(jammer_on);
          P2=0x00;
          lcdcmd(0x01);
          displaymsg(msg11);
          //

          break;
         }
        }
       }
}
if(alarm==0)
{
```

```
    while(alarm==0);
            ah1=bcd2bin(read(0xd0,0x08));
    am1=bcd2bin(read(0xd0,0x0a));

            ah2=bcd2bin(read(0xd0,0x0b));
    am2=bcd2bin(read(0xd0,0x0c));

            //ah3=bcd2bin(read(0xd0,0x0d));
   // am3=bcd2bin(read(0xd0,0x0e));

//          ah4=bcd2bin(read(0xd0,0x0f));
   // am4=bcd2bin(read(0xd0,0x10));

/*******************instructions to setalarm1*********************/
            lcdcmd(0x80);
    displaymsg(msg8);

            lcdcmd(0xc0);
    convertion(ah1);
    lcdcmd(0xc2);
            lcddata(':');
            lcdcmd(0xc3);
    convertion(am1);

            settime(0x08,23,0,0xc0,ah1);
            ah1=bcd2bin(ah1);
    settime(0x0a,59,0,0xc3,am1);
            am1=bcd2bin(am1);

/*******************instructions to setalarm2*********************/
```

```
        lcdcmd(0x80);
    displaymsg(msg9);

        lcdcmd(0xc0);
    convertion(ah2);
    lcdcmd(0xc2);
        lcddata(':');
        lcdcmd(0xc3);
    convertion(am2);

    settime(0x0b,23,0,0xc0,ah2);
        ah1=bcd2bin(ah2);
    settime(0x0c,59,0,0xc3,am2);
        am1=bcd2bin(am2);

/*******************instructions to setalarm3**********************/
   /* lcdcmd(0x80);
    displaymsg(msg10);

        lcdcmd(0xc0);
    convertion(ah3);
    lcdcmd(0xc2);
        lcddata(':');
        lcdcmd(0xc3);
    convertion(am3);

    settime(0x0d,23,0,0xc0,ah3);
        ah1=bcd2bin(ah3);
    settime(0x0e,59,0,0xc3,am3);
        am1=bcd2bin(am3);*?
```

```
/******************instructions to setalarm4*********************/

/*      lcdcmd(0x80);
   displaymsg(msg12);

        lcdcmd(0xc0);
   convertion(ah4);
   lcdcmd(0xc2);
        lcddata(':');
        lcdcmd(0xc3);
   convertion(am4);

   settime(0x0f,23,0,0xc0,ah4);
        ah1=bcd2bin(ah3);
   settime(0x10,59,0,0xc3,am4);
        am1=bcd2bin(am3);   */

/******************end of alarms********************/

   lcdcmd(0x80);
   displaymsg(msg11);
   delay(200);

  }

 //  if(hrs==ah1&&min==am1)
  // {
//      lcdcmd(0x01);
//      displaymsg(msg10);
  //    P2=0x00;
  //}
```

```
  //else
 // if(hrs>=ah2&&min>=am2)
 //{
//        P2=0xff;
// }
 // else
 // if(hrs==ah3&&min==am3)
  //{
 //        P2=0x55;
//  }
// else

 // if(hrs>=ah4&&min>=am4)

 // {
 //        P2=0xff;
 // }

  if(hrs==ah1&&min==am1)
    {
            if(hrs==ah1&&min==am1&&sec==0)
            {
             lcdcmd(0x01);
             displaymsg(msg10);
             P2=0xff;
            }
            else
            P2=0xff;
    }
    else
    if(hrs>=ah2&&min>=am2)
```

```
    {
            if(hrs==ah2&&min==am2&&sec==0)
            {
              lcdcmd(0x01);
              displaymsg(msg11);
              P2=0x00;
            }
            else
            P2=0x00;
    }
  }
}

void write( unsigned char devadd,unsigned char loc,unsigned  char dat)
{
            start();
            send(devadd);                                //  fun to write to rtc
            send(loc);
            send(dat);
            stop();
}

void start(void)
{                                                        // fun to start
   scl=1;
   sda=1;
   _nop_();
   sda=0;
   scl=0;
}
void stop()                          //fun to stop
```

```
{

        sda=0;
        scl=1;
        _nop_();
        _nop_();
            sda=1;
            scl=0;
}
void send( unsigned int i)
 {                                                    // fun to send the data through 2 wire
communication//
   unsigned char c;
        k=i;
        for(j=0;j<8;j++)
        {

         if(c==0)
         sda = 0;
   else
         sda = 1;
         k=k>>1;
    scl=1;
         _nop_();
         scl=0;
   }

        _nop_();
        scl=1;
        _nop_();
        scl=0;
```

```
 }

unsigned int read( unsigned char devadd,unsigned char loc)
{
 unsigned char i,d=0;
 start();
 send(devadd); //device addr in write mode//
 send(loc);  //byte addr//

 _nop_();

 start();
 send(devadd+1);  //device addr in read mode//

 sda=1;
for(i=0;i<8;i++)
  {
        scl=0;
        _nop_();
        _nop_();
        scl=1;
        d=sda;
        k=d;
        z=z|k;
  }
   scl=0;
   stop();
return z;
}                                                    // fun to read the data from the
location using two wire communication//
```

```
void lcdcmd(unsigned char cmd)
{
 P0=cmd;
 rs=0;
 rw=0 ;
 en=1;
 delay(5);
 en=0;
}

void lcddata(unsigned char x)
{
 P0=x;
 rs=1;
 rw=0;
 en=1;
 delay(5);
 en=0;
}


void delay(unsigned int itime)
 {
   unsigned int k,l;                                    /*delay programming*/
          for(k=0;k<itime;k++)
            for(l=0;l<110;l++);
            }

void displaymsg(unsigned char *p)
{
```

```
            for(i=0;p[i]!='\0';i++)
        {
          lcddata(p[i]);
        }

    }

     unsigned char bcd2bin(unsigned char bcd)
    {
            return (((bcd & 0xf0)>>4)*10 )+ (bcd&0x0f);

    }
    void convertion(unsigned char data1)
    {
      unsigned v,w;
      v=data1/10;
      v=v+0x30;
      lcddata(v);
      w=data1%10;
      w+=0x30;
      lcddata(w);
      }

    void settime(unsigned char loc ,unsigned char max,unsigned char min,unsigned char
cur,unsigned char val )
    {
     while(1)
     {
      if(inc==0)
      {
      delay(5);
```

```
 while(inc==0);
 if(val>=max)
 {
  val=0;
 }
 else
  val++ ;
 lcdcmd(cur);
 convertion(val);
}

if(dec==0)
{
delay(5);
 while(dec==0);
 if(val<=min)
 {
   val=max;
 }
 else
  val--;
 lcdcmd(cur);
 convertion(val);
}

if(update==0)
{
delay(100);
 delay(100);
 while(update==0);
 write(0xd0,loc,bin2bcd(val));
```

```
  return;
 }

 lcdcmd(cur);
 convertion(val);
 delay(10);

}
}

unsigned char bin2bcd(unsigned char bin)
{
 return (((bin/10)<<4)|(bin%10));
}
```

REFERENCES

1. www. howstuffworks.com
2. EMBEDDED SYSTEM BY RAJ KAMAL
3. 8051 MICROCONTROLLER AND EMBEDDED SYSTEMS BY MAZZIDI
4. Magazines
5. Electronics for you
6. Electrikindia
7. www.google.com