INTRODUCTION

1. INTRODUCTION

A GSM Jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled.

Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver.

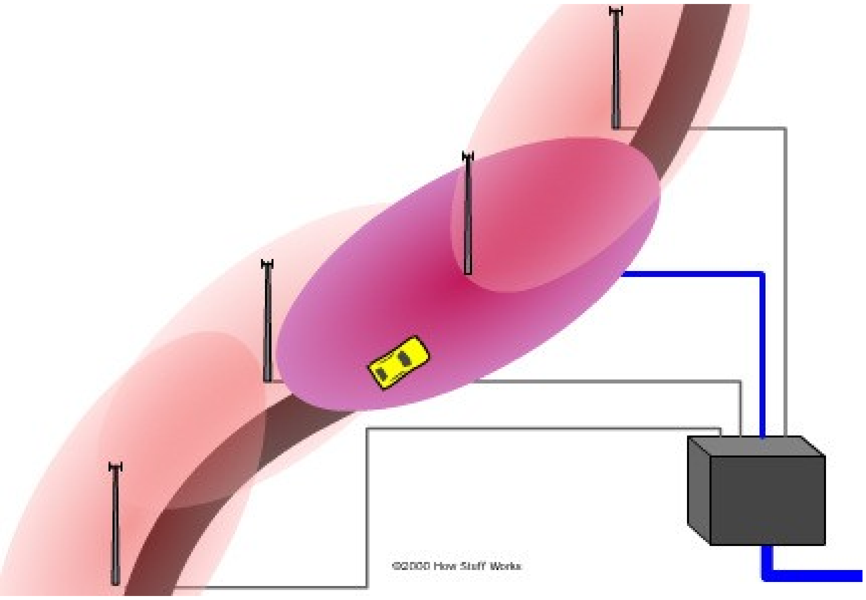
Nowadays the mobile jammer devices are becoming civilian products rather than electronic warfare devices, since with the increasing number of the mobile phone users the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated.

OPERATION

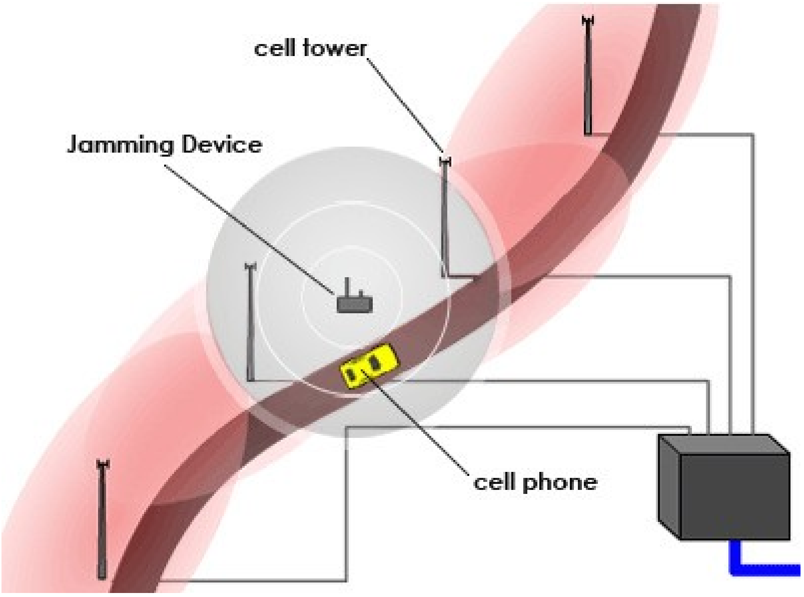
2. OPERATION

Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which mean 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, which 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. Some of the high-end devices block all frequencies at once and others can be tuned to specific frequencies.

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 AMPS, CDMA, TDMA, GSM, PCS, DCS, iDEN and Nextel systems. Old-fashioned analog cell phones and today's digital devices are equally susceptible to jamming. 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 town.



It's a called a **denial-of-service attack**. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems (AMPS, iDEN, GSM, etc) and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America.

The power of the jammer's effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of buildings and landscape, even temperature and humidity play a role. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. However, like cell phones, most of the devices in common use operate at low enough power output (<1W) to avoid causing any problems.

MOBILE JAMMING TECHNIQUES

3. MOBILE JAMMING TECHNIQUES

3.1 Type "A" Device: JAMMERS

In this device we overpower cell phone's signal with a stronger signal, This type of device comes equipped with several independent oscillators transmitting ‘jamming signals’ capable of blocking frequencies used by paging devices as well as those used by cellular/PCS systems’ control channels for call establishment. When active in a designated area, such devices will (by means of RF interference) prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. Technologist Jim Mahan said, “There are two types. One is called brute force jamming, which just blocks everything. The problem is, it’s like power-washing the airwaves and it bleeds over into the public broadcast area. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control.”

3.2 Type “B” Device: INTELLIGENT CELLULAR DISABLERS

Unlike jammers, Type “B” devices do not transmit an interfering signal on the control channels. The device, when located in a designated ‘quiet’ area, functions as a ‘detector’. It has a unique identification number for communicating with the cellular base station. When a Type “B” device detects the presence of a mobile phone in the quiet room; the ‘filtering’ (i.e. the prevention of authorization of call establishment) is done by the software at the base station.

When the base station sends the signaling transmission to a target user, the device after detecting simultaneously the presence of that signal and the presence of the target user, signals the base station that the target user is in a ‘quiet’ room; therefore, do not establish the communication. Messages can be routed to the user’s voice- mail box, if the user subscribes to a voice-mail service. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. For ‘emergency users’, the intelligent detector device makes provisions for designated users who have emergency status. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call are established for a specified maximum duration, say two minutes. The emergency users are also allowed to make out going calls. Similarly, the system is capable of recognizing and allowing all emergency calls routed to “911”.

It should be noted that the Type “B” detector device being an integral part of the cellular/PCS systems, would need to be provisioned by the cellular/PCS service providers or provisioned by a third-party working cooperatively with full support of the cellular/PCS service providers.

3.3 Type “C” Device: INTELLIGENT BEACON DISABLERS

Unlike jammers, Type “C” devices do not transmit an interfering signal on the control channels. The device, when located in a designated ‘quiet’ area, functions as a ‘beacon’ and any compatible terminal is instructed to disable its ringer or disable its operation, while within the coverage area of the beacon. Only terminals which have a compatible receiver would respond and this would typically be built on a separate technology from cellular/PCS, e.g., cordless wireless, paging, ISM, Bluetooth. On leaving the coverage area of the beacon, the handset must re-enable its normal function.

This technology does not cause interference and does not require any changes to existing PCS/cellular operators. The technology does require intelligent handsets with a separate receiver for the beacon system from the cellular/PCS receiver. It will not prevent normal operation for incompatible legacy terminals within a "quiet" coverage area, thus effective deployment will be problematic for many years.

While general uninformed users would lose functionality, pre-designated "emergency" users could be informed of a "bypass terminal key sequence" to inhibit response to the beacon. Assuming the beacon system uses a technology with its own license (or in the license exempt band), no change to the regulations are needed to deploy such a system. With this system, it would be extremely difficult to police misuse of the "bypass key sequence" by users.

3.4 Type "D" Device: DIRECT RECEIVE & TRANSMIT JAMMERS

This jammer behaves like a small, independent and portable base station, which can directly interact intelligently or unintelligently with the operation of the local mobile phone. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer.

This selective jamming technique uses a discriminating receiver to target the jamming transmitter. The benefit of such targeting selectivity is much less electromagnetic pollution in terms of raw power transmitted and frequency spectrum from the jammer, and therefore much less disruptive to passing traffic. The jam signal would only stay on as long as the mobile continues to make a link with the base station, otherwise there would be no jamming transmission – the technique forces the link to break or unhook and then it retreats to a passive receive mode again.

This technique could be implemented without cooperation from PCS/cellular providers, but Could negatively impact PCS/cellular system operation. This technique has an added advantage over Type B in that no added overhead time or effort is spent negotiating with the cellular network. As well as Type B, this device could discriminate 911 calls and allow for breakthroughs" during emergencies.

3.5 Type "E" Device: EMI SHIELD - PASSIVE JAMMING

This technique is using EMI suppression techniques to make a room into what is called a Faraday cage. Although labor intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage – or in this case a target room.

With current advances in EMI shielding techniques and commercially available products one could conceivably implement this into the architecture of newly designed buildings for so-called "quiet-conference" rooms. Emergency calls would be blocked unless there was a way to receive and decode the 911 transmissions, pass by coax outside the room and re-transmitted.

This passive configuration is currently legal in Canada for any commercial or residential location insofar as DOC Industry Canada is concerned, however municipal or provincial building code by- laws may or may not allow this type of construction.

GSM-MOBILE JAMMING REQUIREMENTS

4. GSM-MOBILE JAMMING REQUIREMENTS

Jamming objective is to inject an interference signal into the communications frequency so that the actual signal is completely submerged by the interference. It is important to notice that transmission can never be totally jammed - jamming hinders the reception at the other end. The problem here for the jammer is that only transmitters can be found using direction finding and the location of the target must be a specific location, usually where the jammer is located and this is because the jamming power is never infinite. Jamming is successful when the jamming signal denies the usability of the communications transmission. In digital communications, 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 power at the receiver. The effects of jamming depend 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.

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

P_j= jammer power P_t= 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 communications receiver

Lj= jammer signal 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 pr event jamming, the antenna gain toward 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 the jammer path loss is often different from the communications path loss; hence gives jammer an advantage over communication transmitters. In the GSM network, the Base Station Subsystem (BSS) takes care of the radio resources. In addition to Base Transceiver Station (BTS), the actual RF transceiver, BSS consists of three parts. These are the Base Station Controller (BSC), which is in charge of mobility management and signaling on the Air-interface between Mobile Station (MS), the BTS, and the Air-interface between BSS and Mobile Services Switching Center (MSC).

The GSM Air-interface uses two different multiplexing schemes: TDMA (Time Division Multiple Access) and FDMA (Frequency Division Multiple Access). The spectrum is divided into 200 kHz channels (FDMA) and each channel is divided into 8 timeslots (TDMA). Each 8 timeslot TDMA frame has duration of 4.6 ms (577 s/timeslot) [3]. The GSM transmission frequencies are presented in Table 1

	Uplink	Downlink
GSM 900	890-915 MHz	935-960 MHz

Table 1. GSM 900 Frequency Bands

Frequency Hopping in GSM is intended for the reduction of fast fading caused by movement of subscribers. The hopping sequence may use up to 64 different frequencies, which is a small number compared to military FH systems designed for avoiding jamming. Also, the speed of GSM hopping is approximately 200 hops /s; So GSM Frequency Hopping does not provide real protection against jamming attacks.

Although FH doesn’t help in protection against jamming, interleaving and forward error correction scheme GSM Systems can protect GSM against pulsed jamming. For GSM it was shown that as the specified system SNR is 9 dB, a jammer min requires a 5 dB S/J in order to successfully jam a GSM channel. The optimum GSM SNR is 12 dB, after this point the system starts to degrade.

GSM system is capable to withstand abrupt cuts in Traffic Channel (TCH) connections. These cuts are normally caused by propagation losses due to obstacles such as bridges. Usually another cell could be used to hold communication when the original BTS has disconnected. The GSM architecture provides two solutions for this: first handover when the connection is still available, second call reestablishment when the original connection is totally lost. Handover decisions are made based on transmission quality and reception level measurements carried out by the MS and the BTS. In jamming situations call re-establishment is probably the procedure the network will take in order to re-connect the jammed TCH.

It is obvious that downlink jamming (i.e. Jamming the mobile station 'handset'(receiver) is easier than uplink, as the base station antenna is usually located far a way from the MS on a tower or a high building. This makes it efficient for the jammer to overpower the signal fro m BS. But the Random Access Channel (RACH) control channels of all BTSs in the area need to be jammed in order to cut off transmission. To cut an existing connections, the jamming has to last at least until the call re-establishment timer at the MSC expires and the connection is released, which means that an existing call can be cut after a few seconds of effective jamming.

The GSM RACH random access scheme is very simple: when a request is not answered, the mobile station will repeat it after a random interval. The maximum number of repetitions and the time between them is broadcast regularly. After a MS has tried to request service on RACH and has been rejected, it may try to request service from another cell. Therefore, the cells in the area should be jammed. In most cases, the efficiency of a cellular jamming is very difficult to determine, since it depends on many factors, which leaves the jammer confused.

DESIGN AND IMPLEMENTATION OF GSM MOBILE JAMMER

5. DESIGN AND IMPLEMENTATION OF GSM MOBILE JAMMER

The Implementation of type "A" JAMMER is fairly simple, the block diagram for this type is shown in figure (2), it shows the main parts which are: RF-section, IF-section, and the power supply.

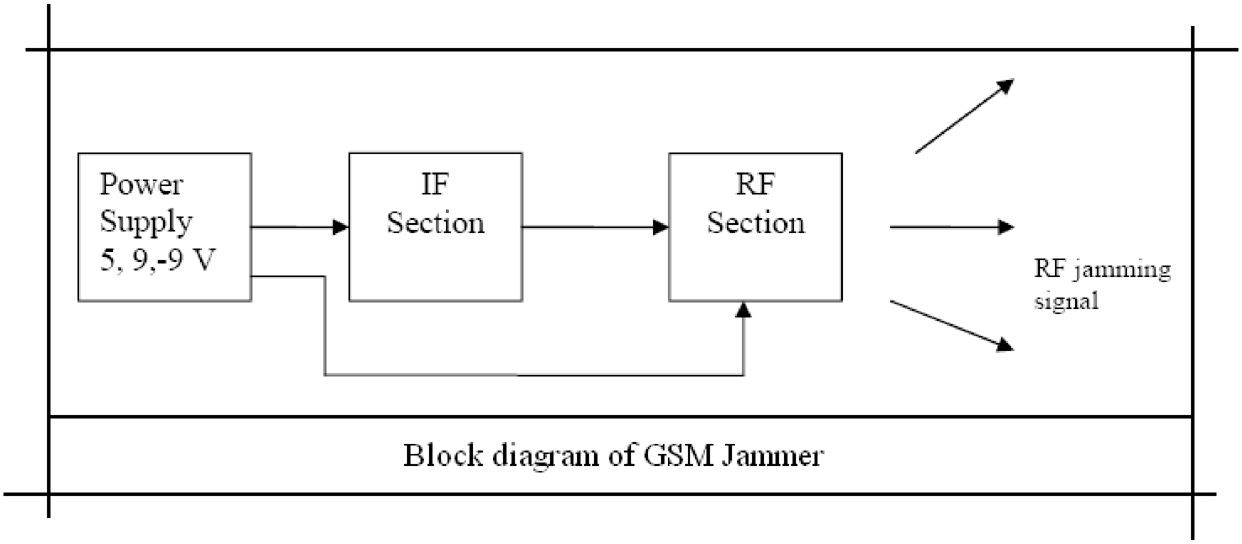


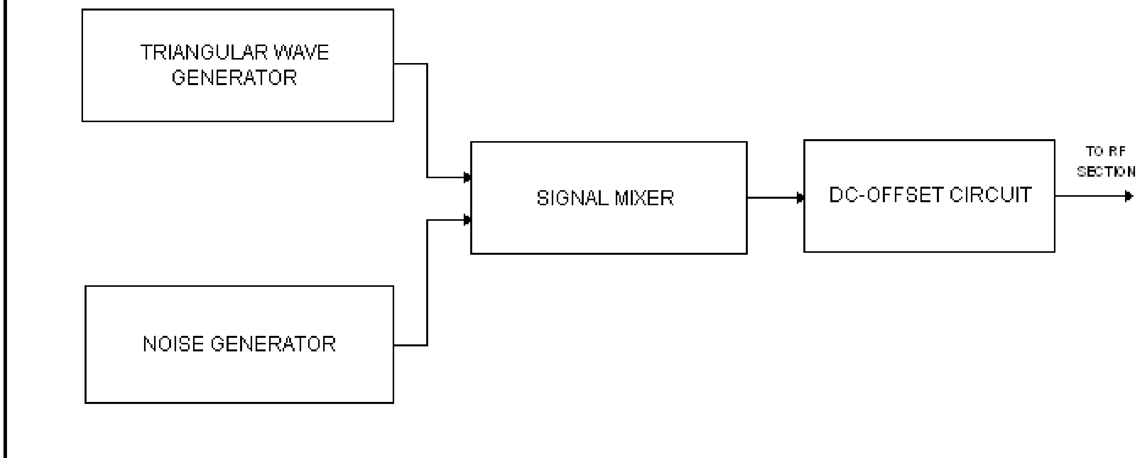
Figure (2). Block diagram of GSM Jammer

5.1 IF-SECTION

The function of the IF-section of the Mobile jammer is to generate the 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 (110 KHz) 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.

The components of the IF Section are as follows:

- 555 Timer IC (Triangular Wave Generator)
- Zener Diode (Noise Generator)
- Op-Amp in Summer Configuration (Signal Mixer)
- Diode–Clamper (Offset Circuit)



Block Diagram of IF Section

5.1.1 TRIANGULAR WAVE GENERATOR

Our requirement is to have a 110 KHz wave for which we have used a 555 timer IC. The 555 timer is used in the astable multivibrator mode. It basically consists of two comparators, a flip-flop, a discharge transistors and a resistive voltage divider to set the voltages at different comparator levels. The figure (2) shows the 555 timer connected to operate in the astable multivibrator mode as a non-sinusoidal oscillator.

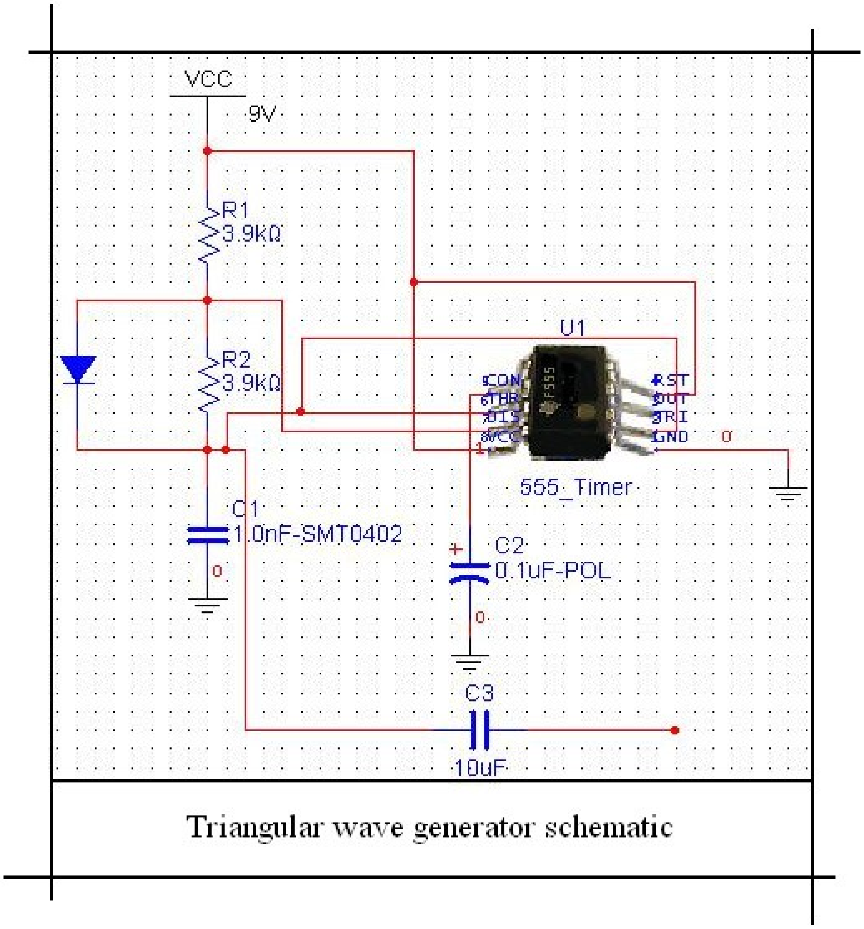


Figure (3) Timer connected as Oscillator

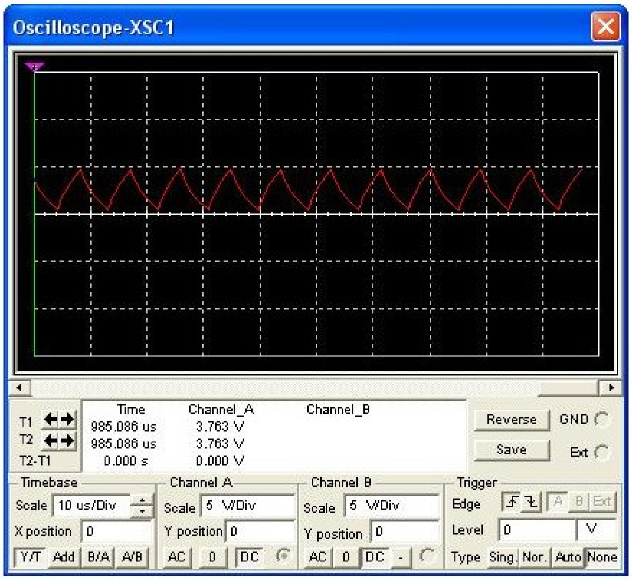
The 555 timer consists basically of two comparators, a flip-flop, a discharge transistor, and a resistive voltage divider. The resistive divider is used to set the voltage comparator levels all three comparator levels. A 555 timer connected to operate in the astable mode as a free-running nonsinusoidal oscillator (astable multivibrator).

The threshold input is connected to the trigger input. The external components R_1, R_2&C_{ex} Form the timing circuit that sets the frequency of oscillation. The 0.01uF 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 C_{ex} is uncharged and thus the trigger voltage (pin 2) is at 0 V. 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 Q, low and keeping the transistor off. Now, C_{ext} begins charging through R_1& R_2 (to obtain 50% duty cycle, one can connect a diode parallel with R_2 and choose R_1= R_2).

When the capacitor voltage reaches 1/3Vcc , the lower comparator switches to its low output state, and when the capacitor voltage reaches 2/3Vcc the upper comparator switches to its high output state. This resets the flip flop causes the base of Q_d to go high, and turns on the transistor. This sequence creates a charge path for the capacitor through R2 and the transistor, as indicated. The cap now begins to discharge, causing the upper comparator to go low. At the point whet capacitor discharges down to 1/3Vcc , the lower comparator switches high, setting the flip flop, which makes the base of Q_d low and turns off the transistor. Another charging cycles begins, and the entire process repeats. The result is a rectangular wave output whose duty cycle depends on the values of R1 and R2. The frequency of oscillation is given by the following formula

$$f = \frac{1.44}{(R1 + R2)C_{ext}}$$

Using the above equation for frequency equal 110 KHz, one can found the values of R_1(3.9K) , R_2(3.9K) , and C_{ext}(1nF). 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 (3).



	Time	Channel_A	Channel_B
T1	985.086 us	3.763 V	
T2	985.086 us	3.763 V	
T2-T1	0.000 s	0.000 V	

Timebase: Scale 10 us/Div, X position 0

Channel A: Scale 5 V/Div, Y position 0

Channel B: Scale 5 V/Div, Y position 0

Trigger: Level 0 V

Simulation of triangular wave by 555 timer

Figure 3: The output voltage on C_{ext}

To avoid loading the timing circuit and changing the operating frequency, the triangular wave on the terminal of the external capacitor was buffered using OP-Amp.

5.1.2 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.

The noise generator used in this design is based on the avalanche noise generated by a Zener breakdown phenomenon. It is created when a PN junction is operated in the reverse breakdown mode. The avalanche noise is very similar to shot noise, but much more intense and has a flat frequency spectrum (white).

The magnitude of the noise is difficult to predict due to its dependence on the materials. Basically the noise generator circuit consists of a standard 6.8 volt Zener diode with a small reverse current, a transistor buffer, and The National LM386 audio amplifier which acts as a natural band-pass filter and mall-signal amplifier. The output spectrum of the noise generator is shown in the figure (5).

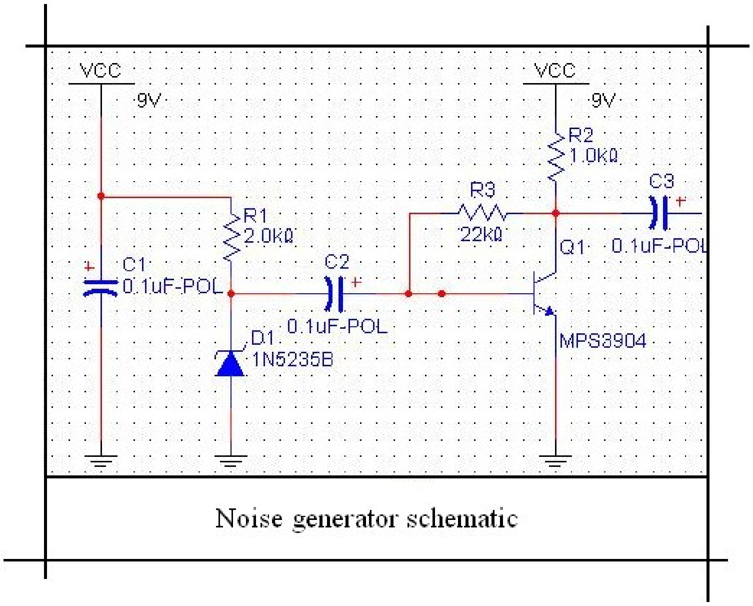


Figure (4): Noise Generator Schematic

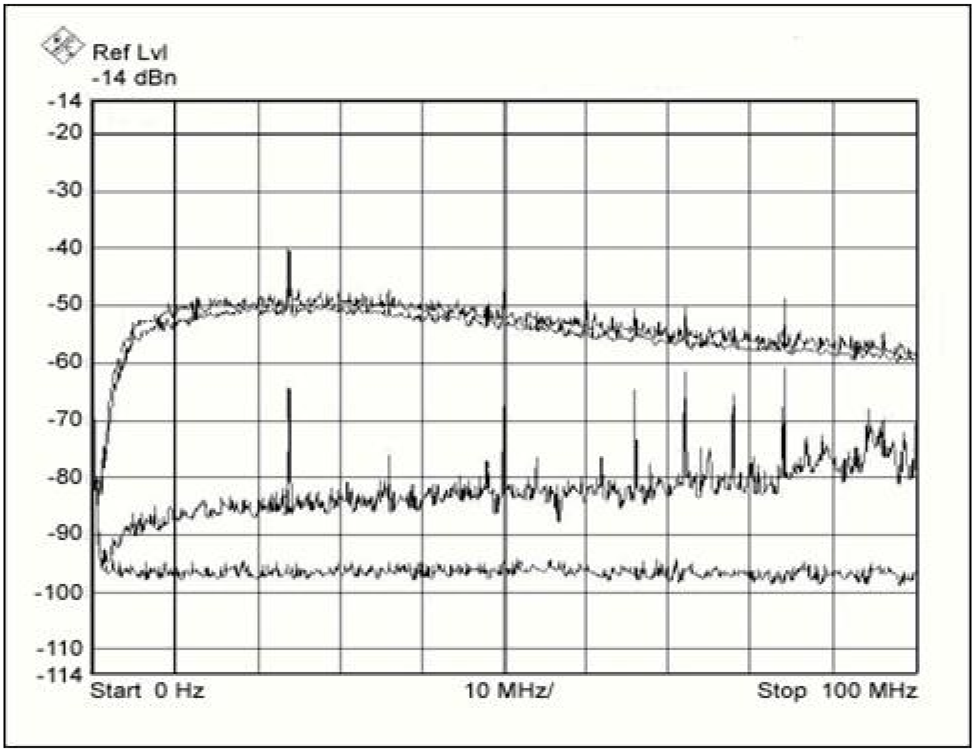


Figure (5): White-noise generator output spectrum

5.1.3 SIGNAL MIXER AND DC-OFFSET CIRCUITS:

The triangle wave and noise signals are mixed using Op-Amp configured as summer, see figure (6). Then a DC voltage is added to the resulted signal to obtain the required tuning voltage using Diode-Clamper circuit. Figure (7) shows a diode clamper circuit with Bias. 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.

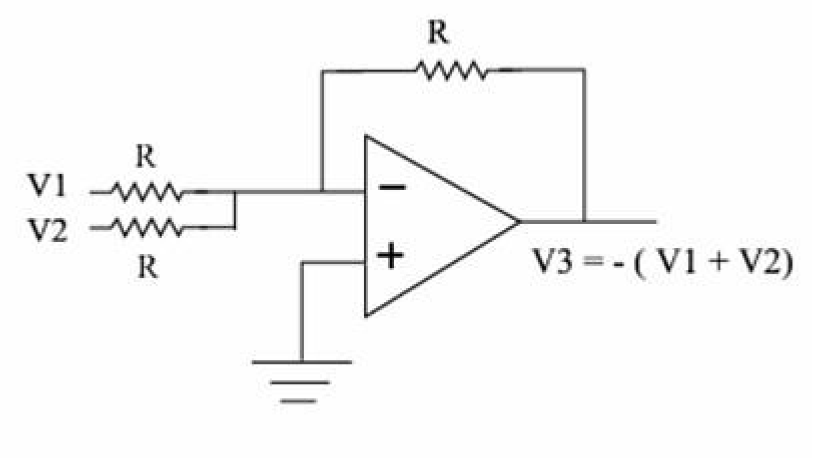


Figure (6): OP-Amp Summer Circuit

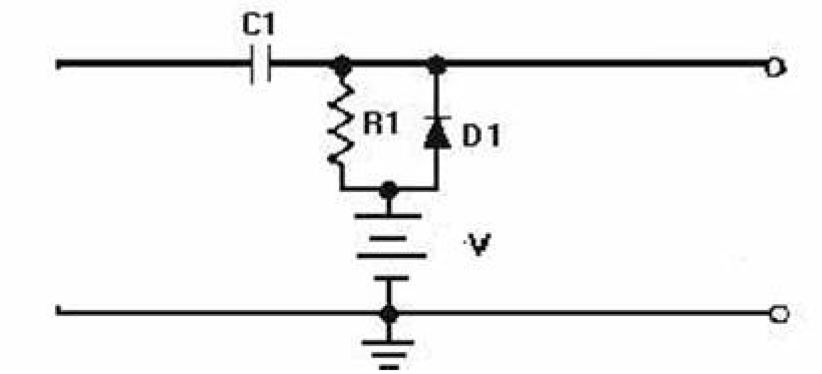
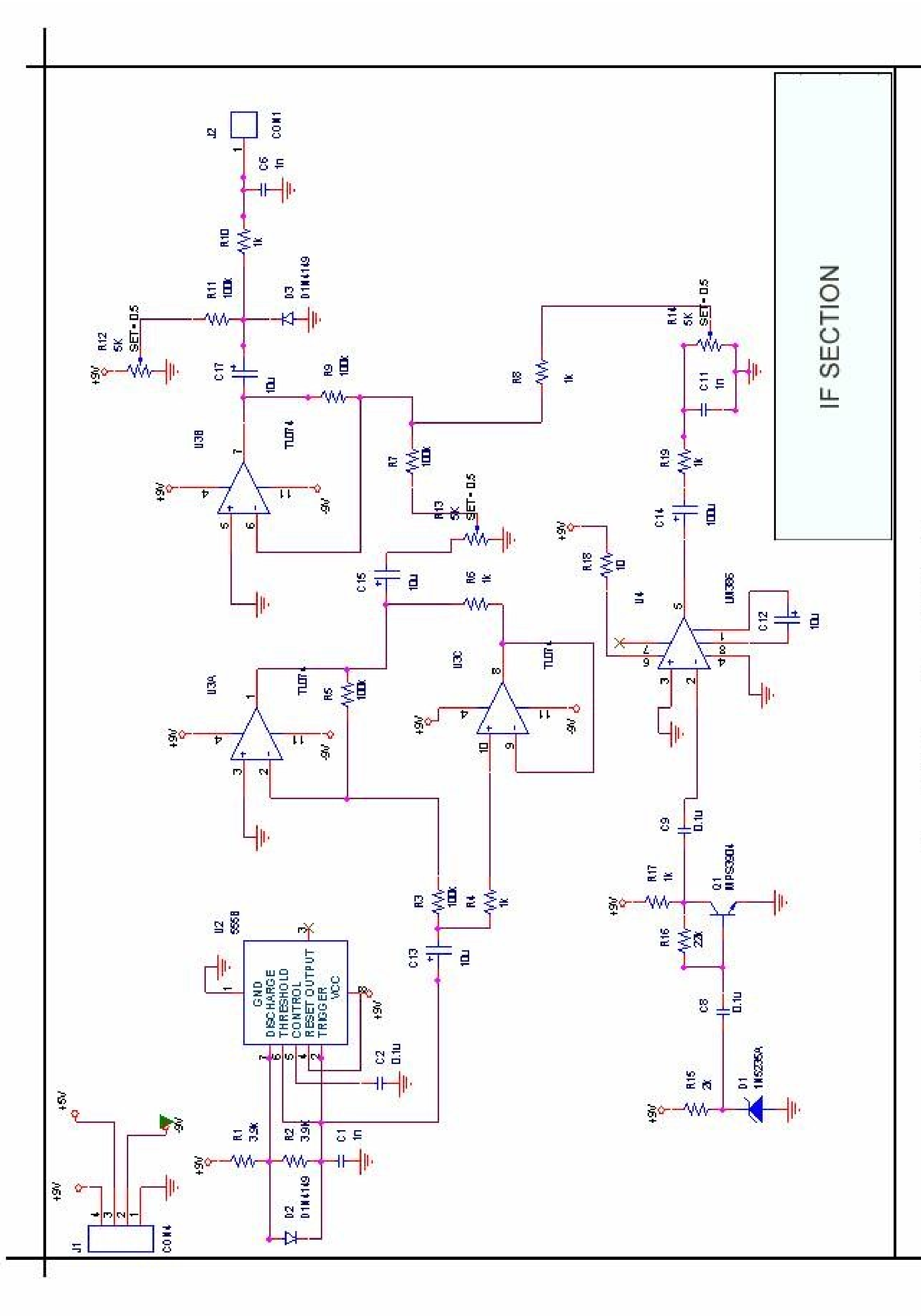


Figure (7): Positive Diode-Clamper with bias

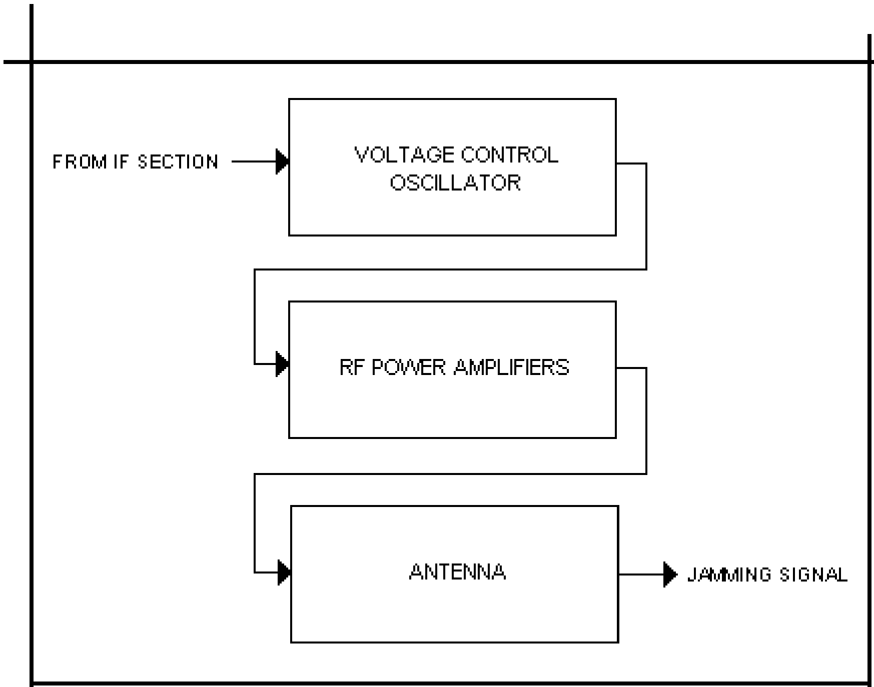


Circuit Schematic of IF Section

5.2 RF-SECTION

The RF-section is the most important part of the mobile jammer it consist of the

- Voltage Controlled Oscillator (VCO)
- RF Power amplifiers
- Antenna.



Block Diagram of RF Section

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. The width of the microstrip was calculated using the following Equations for w/h >1

$$Z_0 = \frac{120\pi}{\sqrt{\varepsilon_{eff}}} \bullet \frac{1}{\left(\frac{w}{h}+1.393+0.677 \bullet \ln\left(\frac{w}{h}+1.444\right)\right)}$$

$$\varepsilon_{eff} = \left[\frac{\varepsilon_r+1}{2}+\frac{\varepsilon_r-1}{2}\left[\frac{1}{\sqrt{1+\frac{12h}{w}}}\right]\right]$$

POWER REQUIREMENTS

To successfully jam a particular region, we need to consider a very important parameter – the signal to noise ratio, referred to as the SNR. Every device working on radio communication principles can only tolerate noise in a signal up to a particular level. This is called the SNR handling capability of the device. Most cellular devices have a SNR handling capability of around 12dB. A very good device might have a value of 9dB, although it is highly unlikely. To ensure jamming of these devices, we need to reduce the SNR of the carrier signal to below the 9dB level.

For this, we consider the worst-case scenario from a jammers point of view. This would mean maximum transmitted power Smax from the tower, along with the lowest value of the SNR handling capability of a mobile device. So, mathematically,

J = -24dBm

Since SNRmin = S/J

Where,J is the power of the jamming signal.

So we need to have jamming signal strength of -24dBm at the mobile device's reception to effectively jam it. However, our radiated signal will undergo some attenuation in being transmitted from the antenna of the jammer to the antenna of the mobile device. This path loss can be calculated using the simple *free space path loss* approximation:

$$L_p = 32.45 + 20\log_{10}(f.D)$$

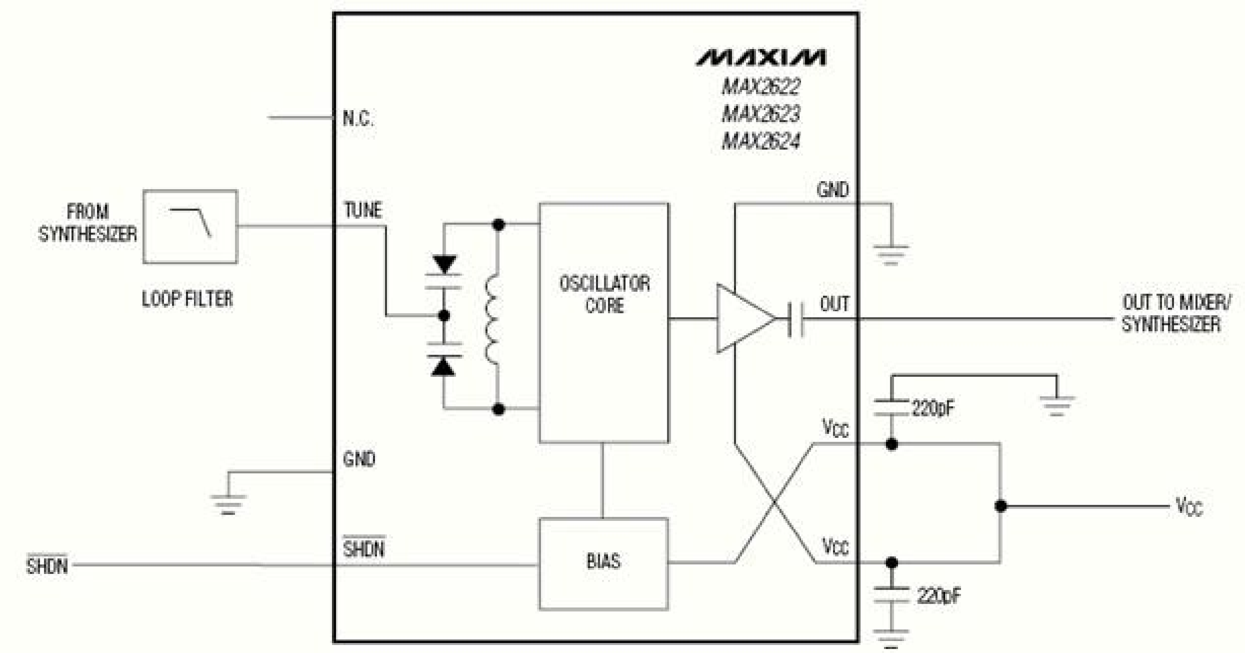
Here f is the frequency in MHz, and D the distance traveled in kilometers. Using the GSM downlink center frequency (947.5MHz) and a jamming radius of 20m, we get the value of path loss to be 58dBm. This ideal path loss is for free space only, and the path losses in air will me much greater. This means that the jamming radius will be less than the 20m used to calculate this value. So, including the power lost in path loss, we need to transmit a signal with strength of:

JT = 58 - 24 = 34dBm

Now, the power output of our VCO is -3dBm, which needs to be amplified by 37dBm to meet our requirements. For this, we used a two-stage amplification mechanism. The first stage is the MAR-4SM pre-amplifier, which provides a 8dBm power gain. This takes the power level to 5dBm. To match the power to the input recommendation of the second amplification stage (the PF08103B), we need to attenuate this by 4dB, for which a pi-attenuator is used. Now the power level is 1dB, which is amplified by a gain of 33dB by the PF08103B to an output power level of 34dBm.

5.2.1 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. Figure 3: Maxim2623 typical connection The MAX2623 VCO is implemented as an LC oscillator configuration, integrating all of the tank circuitry on-chip, this makes the VCO extremely easy-12 to-use, and the tuning input is internally connected to the varactor as shown in figure (8). 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.



Figure(9): Internal Block Diagram of MAX2623 IC

5.2.2 RF POWER AMPLIFIER

For the desired output to be achieved, gain stages were needed. The Hitachi PF08103B power amplifier module used in Nokia mobile phones sufficiently amplifies signals between 800 MHz and 1 GHz by 34 dB. But the recommended input in the datasheet is 1dBm. Due to this, another power amplifier was used between the VCO and PF08103B, the MAR4SM amplifier from Mini-Circuits. It has a gain of 8dB for frequencies from dc to 1 GHZ. This made the output 5 dBm. A typical biasing configuration for the MAR4SM is shown.

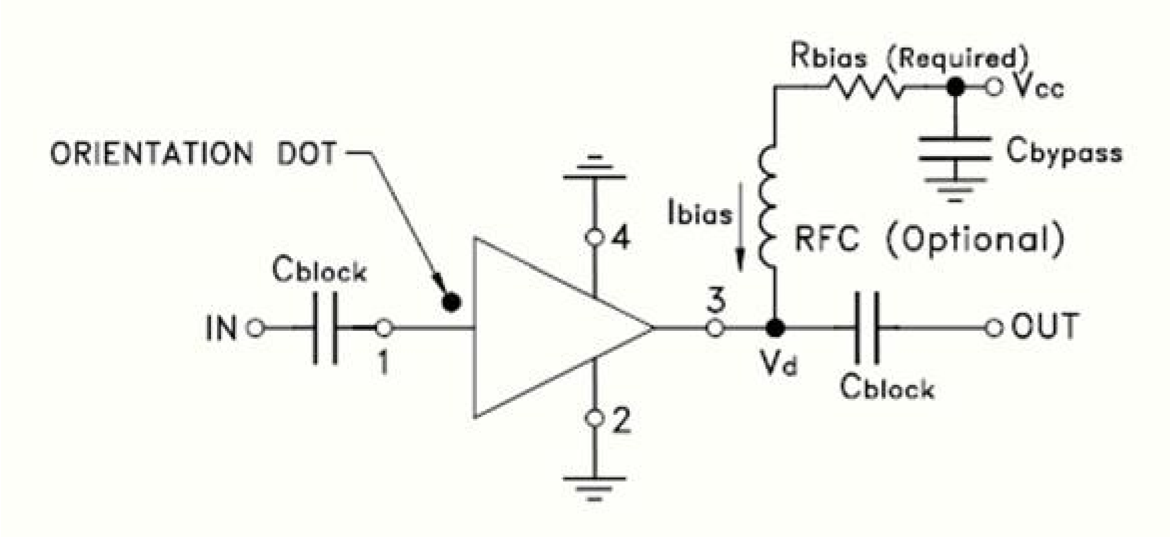
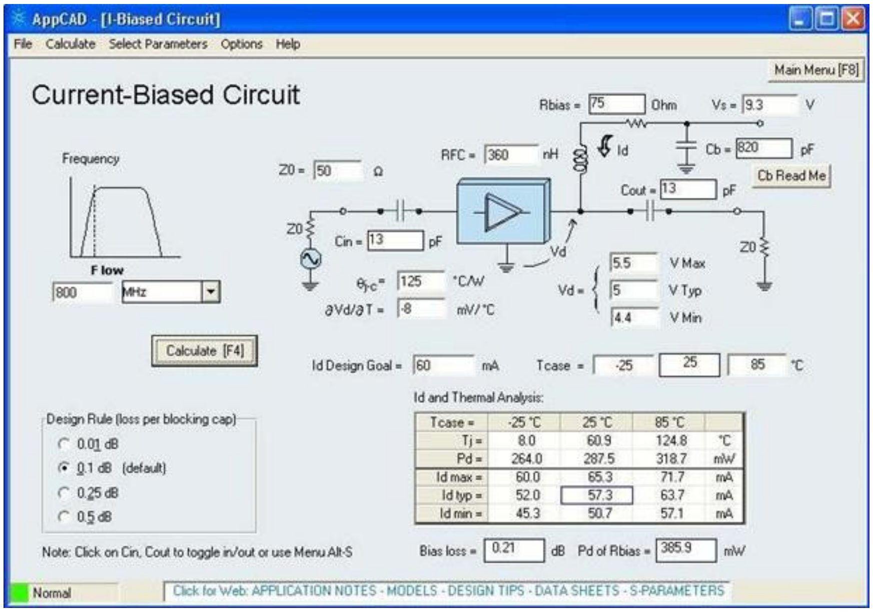


Figure (10): Typical biasing Configuration for the MAR-4SM

The bias current is delivered from a 9 V power supply through the resistor Rbias and the RF choke. The effect of the resistor is to reduce the effect of device voltage on the bias current by simulating a current source. Blocking capacitors are required at the input and output ports. A bypass capacitor is used at the connection to dc supply to prevent stray coupling to other signal processing components. The biasing current is given by the following equation:

$$I_{bias} = \frac{V_{cc} - V_d}{R_{bias}}$$

The design of MAR4SM was carried out on AppCAD. The results are shown below



Current-Biased Circuit

F low 800 MHz

Z0 = 50 Ω

RFC = 360 nH

Rbias = 75 Ohm   Vs = 9.3 V

Cb = 820 pF

Cout = 13 pF

Cin = 13 pF

θj-c = 125 °C/W

∂Vd/∂T = -8 mV/°C

Vd = 5.5 V Max, 5 V Typ, 4.4 V Min

Id Design Goal = 60 mA   Tcase = -25 25 85 °C

Design Rule (loss per blocking cap)

○ 0.01 dB
● 0.1 dB (default)
○ 0.25 dB
○ 0.5 dB

Id and Thermal Analysis:

Tcase =	-25 °C	25 °C	85 °C	
Tj =	8.0	60.9	124.8	°C
Pd =	264.0	287.5	318.7	mW
Id max =	60.0	65.3	71.7	mA
Id typ =	52.0	57.3	63.7	mA
Id min =	45.3	50.7	57.1	mA

Note: Click on Cin, Cout to toggle in/out or use Menu Alt-S

Bias loss = 0.21 dB   Pd of Rbias = 385.9 mW

Normal

Click for Web: APPLICATION NOTES - MODELS - DESIGN TIPS - DATA SHEETS - S-PARAMETERS

Figure (11): Design of MAR-4SM on AppCAD

Now the power before the Hitachi RF amplifier is 5dBm and since 1dBm is required; we used 4dB T-Network attenuator as shown in figure (12). The attenuator also designed to have 50 ohm characteristic impedance to easily match the whole circuits.

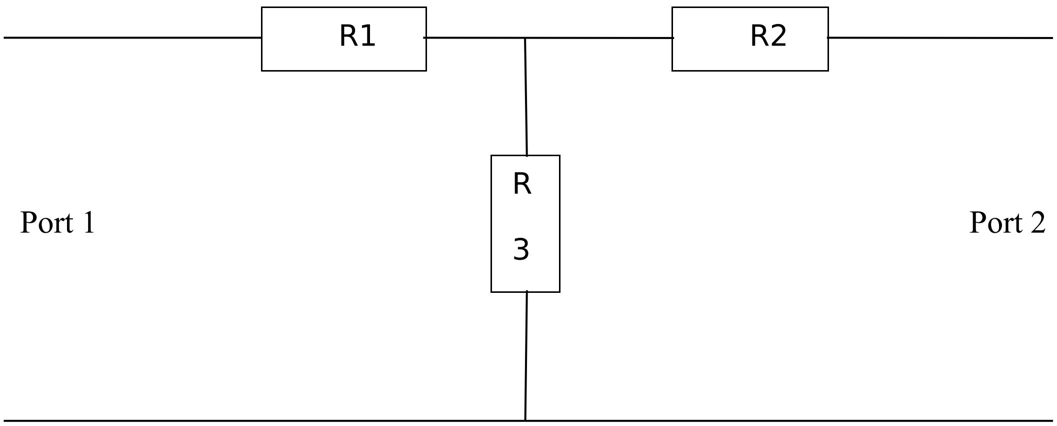


Figure (12): T-Network Attenuator

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

$$V_2 = 0.631V_1$$

And for 50 ohm characteristic impedance, the values of the resistors were found using the following equations:

$$50 = \frac{R2 + 50}{R3} + R1$$

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

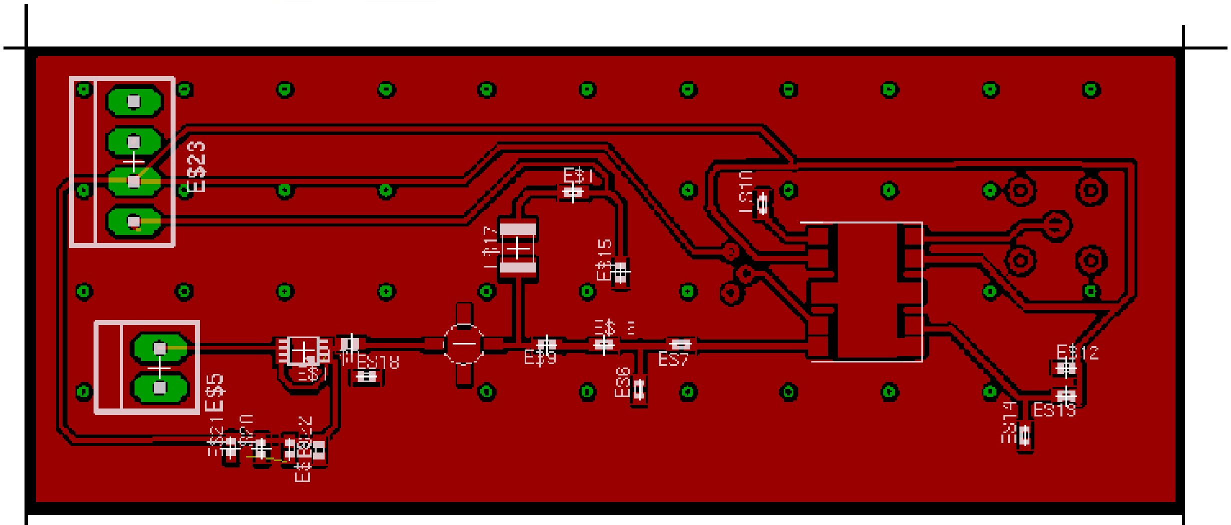
Where, $X = \frac{R2+50}{R3}$.

5.2.3 ANTENNA

At this point, we have a transmissible signal ready. Now we need to radiate it into our intended area to produce the desired jamming effect. Antenna designs are pattern and frequency specific. This means we needed to select the right antenna that matched:

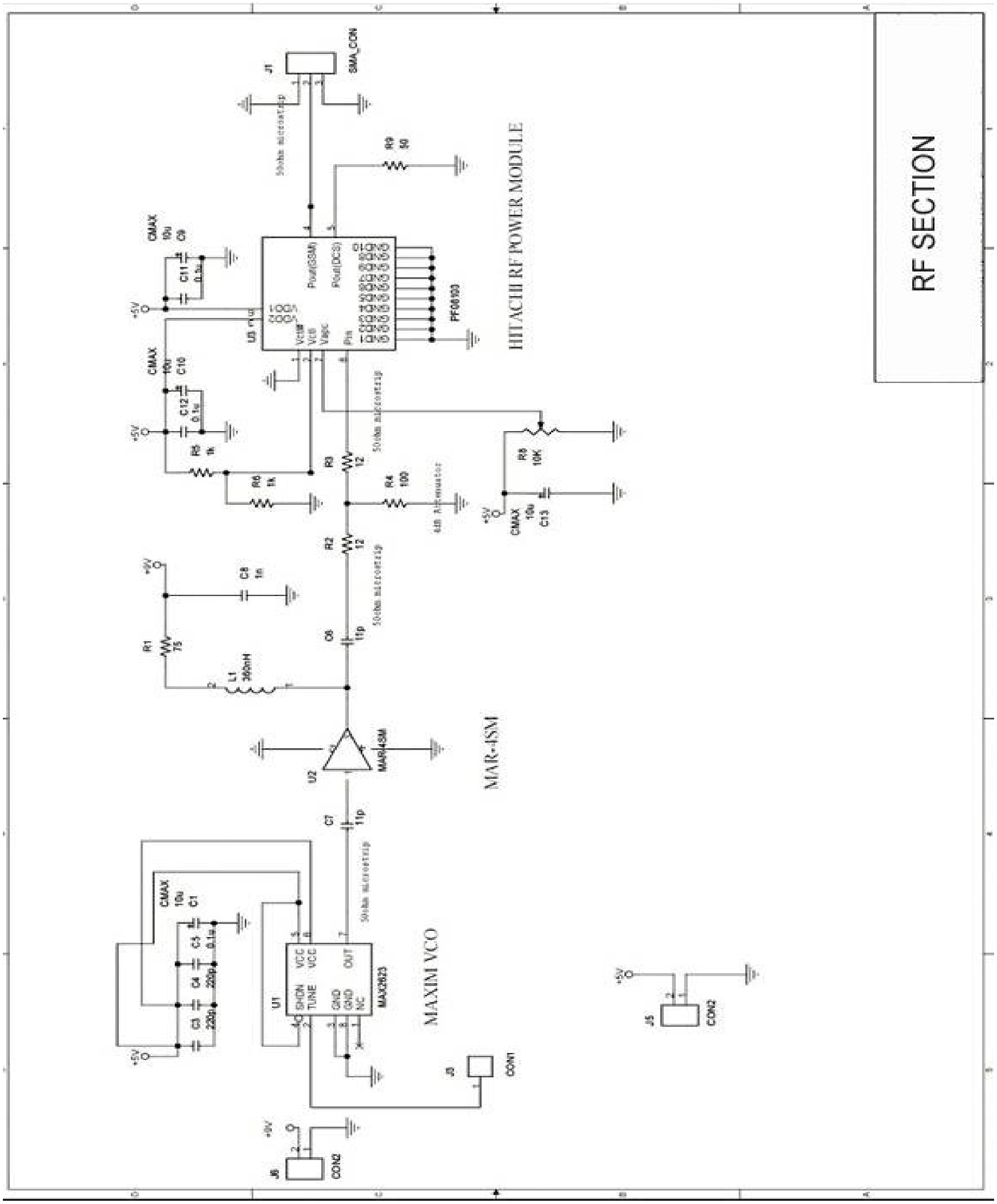
- The correct frequency range (935-960MHz)
- An Omni directional radiation pattern

From among the various antennas available in the market, the antenna used in the project was a Helical antenna, with a reflection coefficient of -17dB. It should be noted that the smaller the reflection coefficient, the better. And this value of -17dB is a very good value.



RF PCB Layout

It is important to note that the RF-Section was implemented on FR-4 printed circuit board (PCB) with thickness of 1/32 inches. Also RF layout issues such as good grounding, transmission lines, and vias was taken into consideration when designing the layout for the RF-Section.


RF SECTION
J1
SMA_CON
50ohm microstrip
R9
50
HITACHI RF POWER MODULE
U3
PF08103
Vctl
Vdd
Vapc
Pin
Pout(GSM)
Pout(DCS)
CMAX
10u
C9
C11
0.1u
+5V
CMAX
10u
C10
C12
0.1u
R5
1k
R6
1k
R3
12
R4
100
4dB Attenuator
R8
10K
CMAX
10u
C13
R2
12
C8
1n
R1
75
L1
390nH
C6
11p
U2
MAR-4SM
C7
11p
MAXIM VCO
U1
MAX2623
SHDN
TUNE
GND
GND
NC
VCC
VCC
OUT
CMAX
10u
C1
C5
0.1u
C4
220p
C3
220p
J3
CON1
J5
CON2
J6
CON2
+9V

6. CONCLUSION

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 restricted areas only.

Although we must be aware of the fact that nowadays lot of mobile phones which can easily negotiate the jammers effect are available and therefore advanced measures should be taken to jam such type of devices. These jammers includes the intelligent jammers which directly communicates with the GSM provider to block the services to the clients in the restricted areas,but we need the support from the providers for this purpose.

DATASHEETS