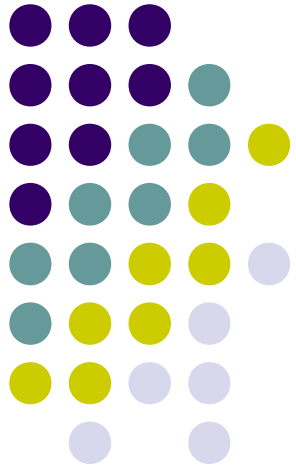
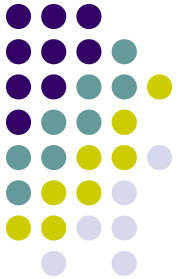
GSM-900 Mobile JAMMER

EE592:Graduation Project

Ahmad Jisrawi



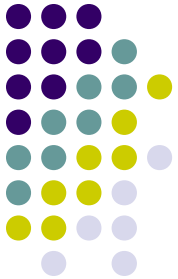
INTRODUCTION



- JAMMING is the act of intentionally directing electromagnetic energy at a communication system to disrupt or prevent signal transmission.

- The GSM Jammer is a device that transmit signal on the same frequency at witch the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located could’nt make or reciece call phones .

JAMMING Techniques 1



- Type “A”: JAMMERS
- Type ”B”: Intelligent Cellular Disablers
- Type “C”: Intelligent Beacon Disablers
- Type ”D”: Smart JAMMERS
- Type ”E”: Faraday Cage (EMI Suppression Techniques)

GSM JAMMING Requirement 1

- 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), and the modulation scheme.

GSM JAMMING Requirement 2

Jamming-to-Signal ratio is given by:

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

Where:
Pj = jammer power
Pt = transmitter power
Gjr = antenna gain (jammer to receiver)
Grj = antenna gain (receiver to Jammer)
Gtr = antenna gain (transmitter to receiver)
Grt = antenna gain (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

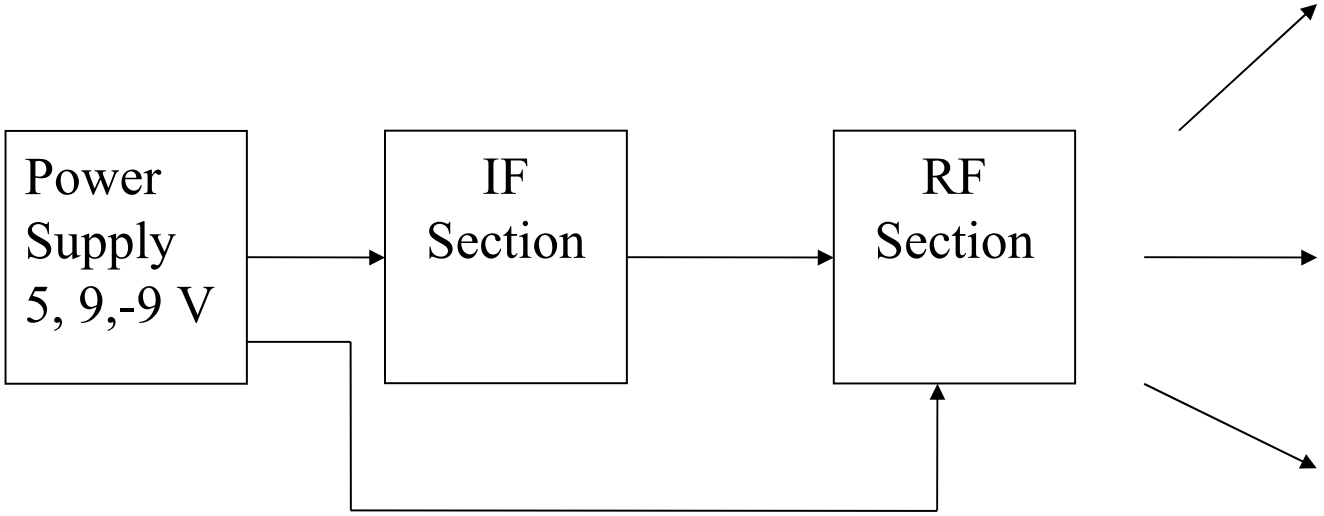
GSM JAMMING Requirement 3

- The frequency of the transmitted signal of the jammer must cover the GSM frequency range

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

- As the power received from the GSM Base Station is usually low, It is easier to jamm the downlink (i.e. Jamming the mobile station 'handset' receiver) than uplink, hence the jammer output frequency should cover the downlink frequency.

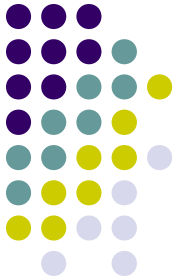
Design and Implementation GSM Mobile JAMMER



Block diagram of the mobile Jammer

GSM-900 Mobile Jammer

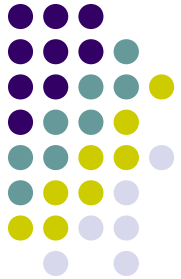
RF-Section 1



- The RF-section is responsible for generating and transmitting the RF-Jamming signal. The main parts are: VCO, Power Amplifier, and the Antenna.
- fortunately, all the parts used are internally matched to 50ohm load, and hence transmission lines used are microstrip lines designed to have 50ohm characteristic impedance
- The components used are all surface mount component

GSM-900 Mobile Jammer

RF-Section 2



- The output power of the jammer was designed so that it has a range of 20m, and was calculated as follow:
  - Jr (jammer power at mobile receiver) ≥ Smax – SNRmin

    SNRmin = 9 dB for mobile receiver and

    Smax = -15dBm (Mobile station signal power at mobile receiver)

    Jr ≥ -24 dBm
  - The jammer output power = Jr + F

    free space path loss equation:

    F = 32.45 + 20 log (f *D), f in MHZ and D in Km

    Output power = 58 – 24 = 34 dBm

GSM-900 Mobile Jammer

RF-Section 3
The VCO 1

- The MAX2623 VCO from MAXIM IC was used to generate the required signal

- The output frequency range for the VCO is:
  850 – 1000 MHz for a tune voltage from 0.4 – 2.6V.

- The input tune frequency best suited the VCO was 120KHz to sweep the desired frequency range.

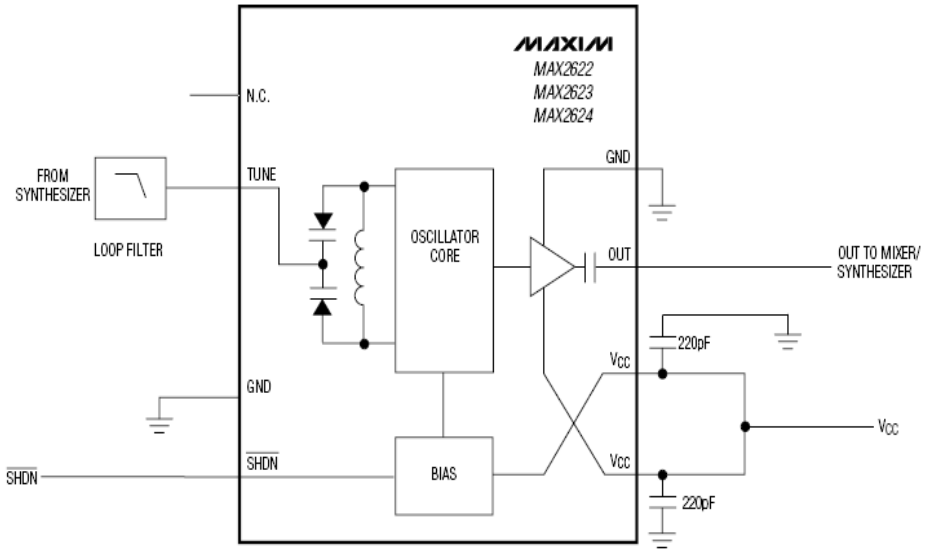
GSM-900 Mobile Jammer

RF-Section 4
The VCO 2

- The MAX2623 VCO is implemented as an LC oscillator configuration, integrating all of the tank circuitry on-chip.

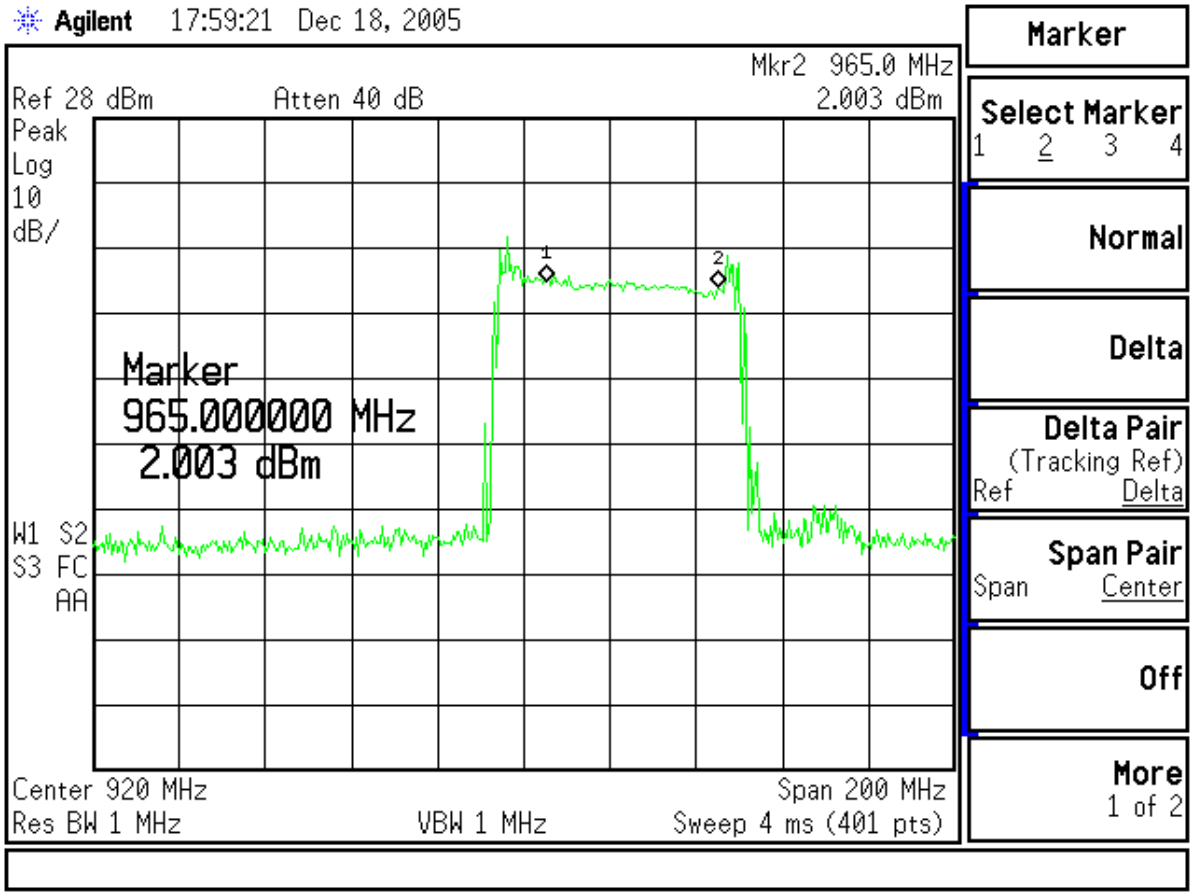
- The tuning input which control the output frequency is internally connected to the varactor.

- The output is internally matched to 50ohm, and output power of -3dBm.



GSM-900 Mobile Jammer

RF-Section 5
The VCO 3



The output of The VCO tuned to sweep from 625 – 960 MHz

GSM-900 Mobile Jammer

RF-Section 6
RF Power Amplifiers 1

- Two RF power amplifiers were used to achieve the required output power (i.e. 34dBm).
- The first stage power amplifier was the MAR-4SM from Mini-Circuits it has a gain of 8dB for frequency range from DC to 1000 MHz

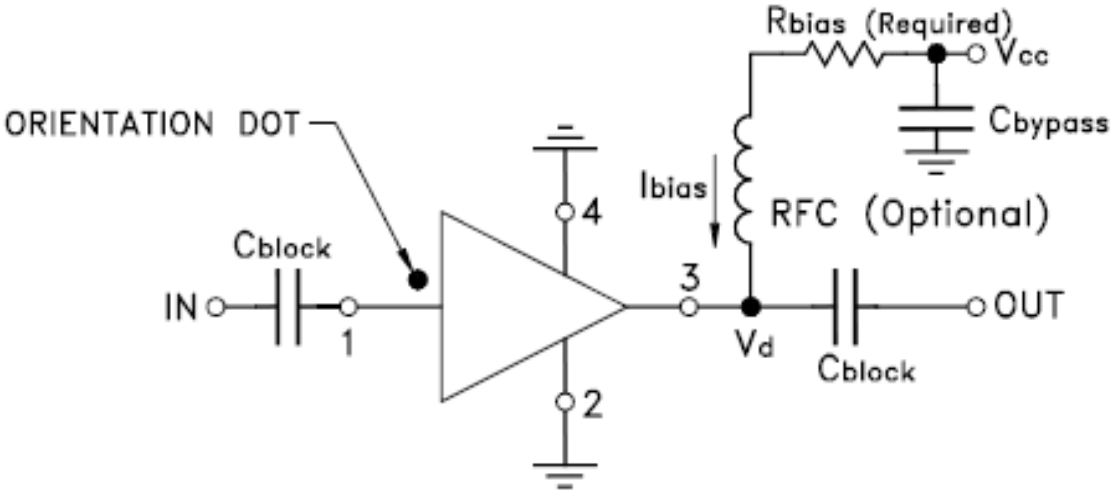
  so the output of this stage should be 5dBm

  for the -3dBm output of the VCO

MAR-SM

RF-Section 7
RF Power Amplifiers 2

- Input and output are matched to 50hom load
- The MAR-4SM is current biased power amplifier



Typical biasing Configuration for the MAR-4SM

GSM-900 Mobile Jammer

RF-Section 8
RF Power Amplifiers 3

- The second stage power amplifier is the Hitachi PF08103b dual power amplifier with efficiency at 48%.
- It can operate either on GSM-900 or DCS1800, so external circuitry was designed to configure it to operate in GSM mode
- The output of the power amplifier is 35dBm

  for 1dBm input

RF-Section 9
RF Power Amplifiers 4

- Symmetric T-Network with 4dB attenuation was used To obtain 1dBm at the input of the second power amplifier from the 5dBm output of the first power amplifier.

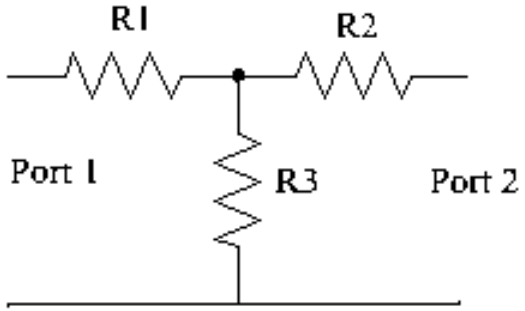
- For 4-dB attenuation, and matched to 50ohm transmission line, $V^-_2 = V_2 = 0.631 * V_1$

  (S12 = S21 = 0.631) the value of the resistors was found using the following equations

  $0.631 = (X / (X + R1))*(50 / (50 + R1)$

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

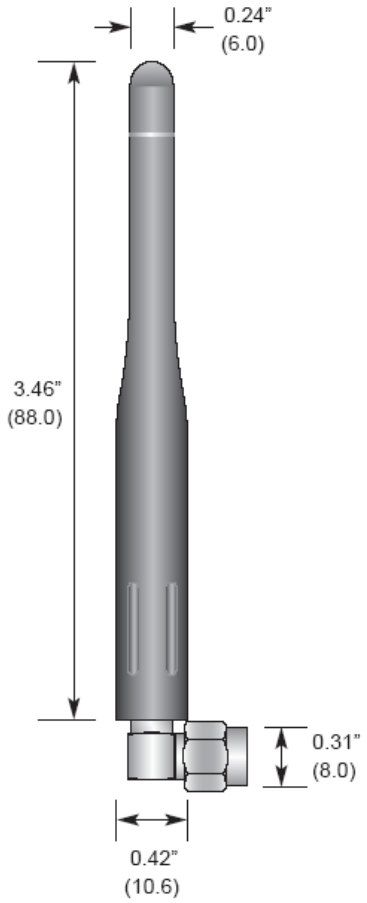
  where $X = (R2 + 50)//R3$.



GSM-900 Mobile Jammer

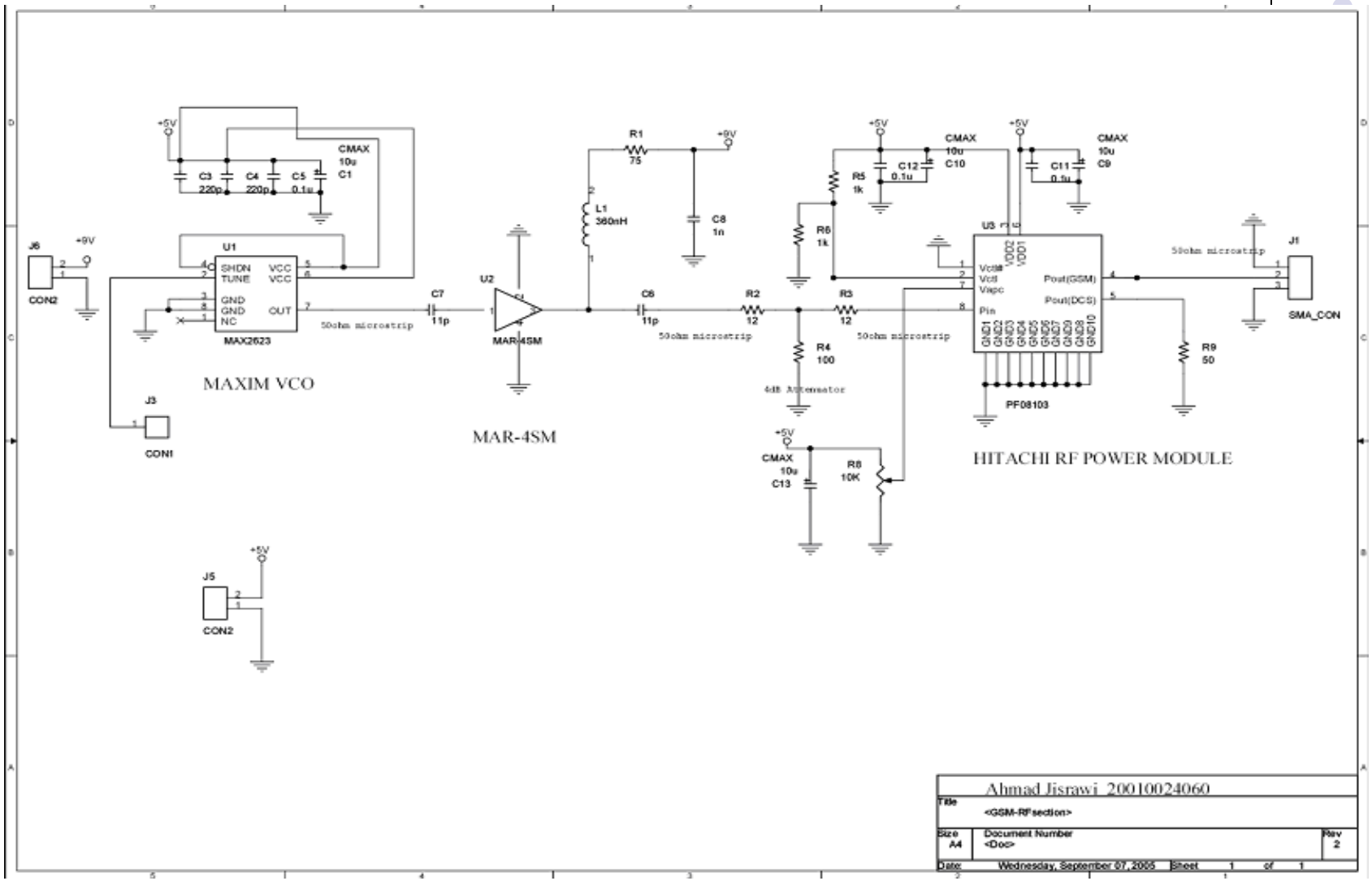
RF-Section 10
The Antenna

- 1/4 wave monopole antenna, with center frequency at 916Mhz and bandwidth of 150 MHz.
- 50 ohm impedance
- VSWR < 1.7
- Gain 2dBi
- Connected to the RF-Section using RP-SMA connector



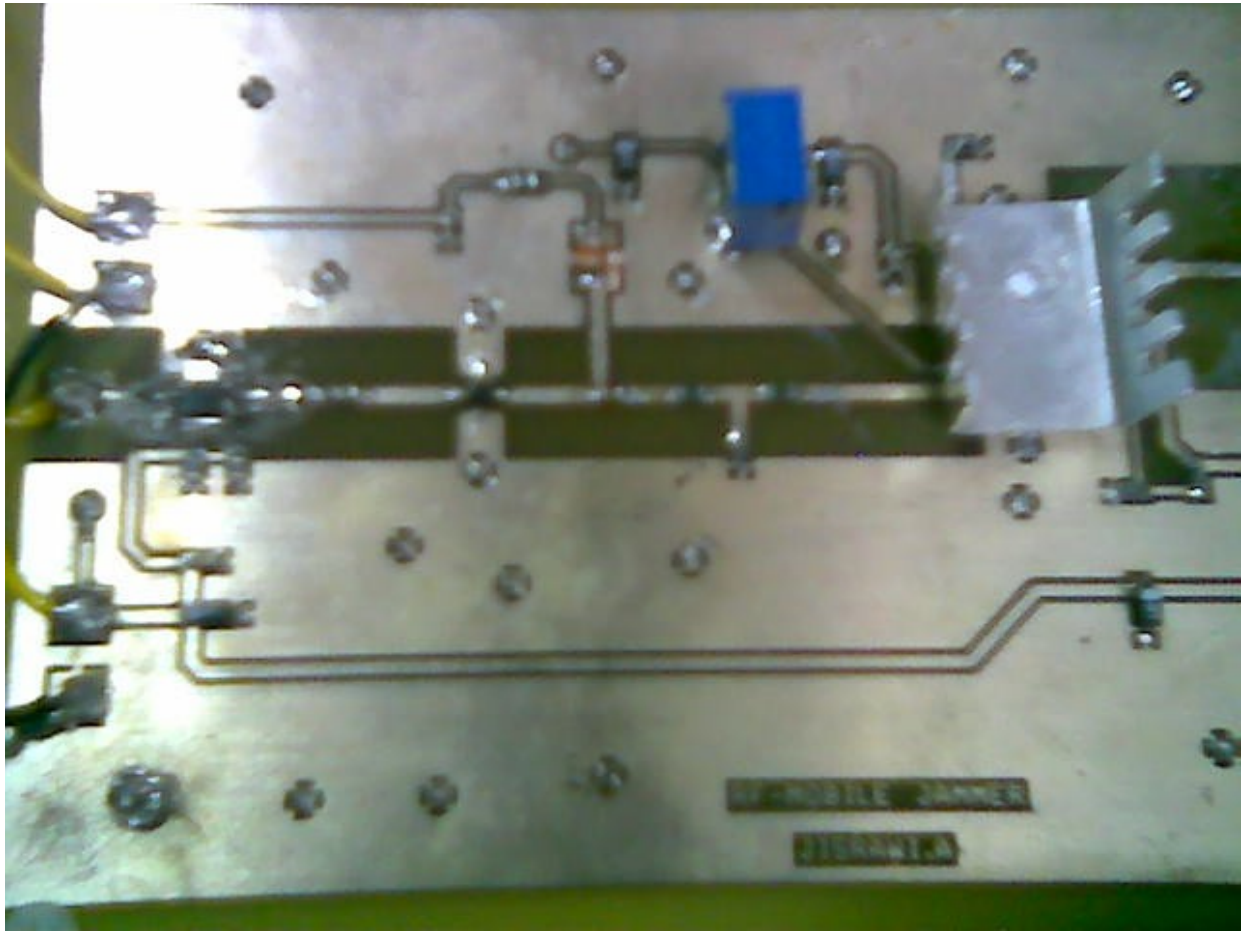
GSM-900 Mobile Jammer

RF-Section 11



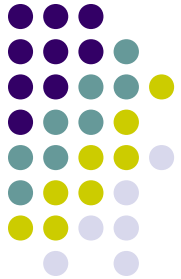
GSM-900 Mobile Jammer

RF-Section 12



GSM-900 Mobile Jammer

IF-Section 1



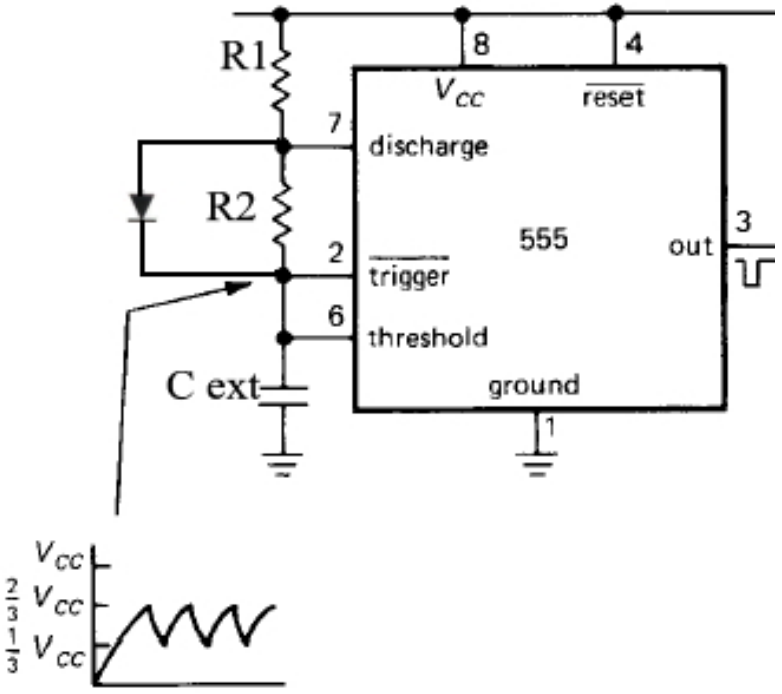
- The function of the IF-section of the Mobile jammer is to generate the tuning signal required by the VCO in the RF-Section
- The main parts of the IF-Section are:
  - Triangular Wave Generator
  - Noise Generator
  - Signal Mixer and DC offset

IF-Section 2
Triangular Wave Generator

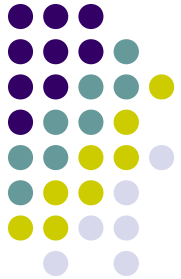
- The circuit used to generate the triangular wave is the 555-Timer as ASTABLE MULTIVIBRATOR
- The output frequency is given by the following equation:

$$f_r = \frac{1.44}{(R_1 + R_2)C_{ext}}$$

- Fr = 120 KHz



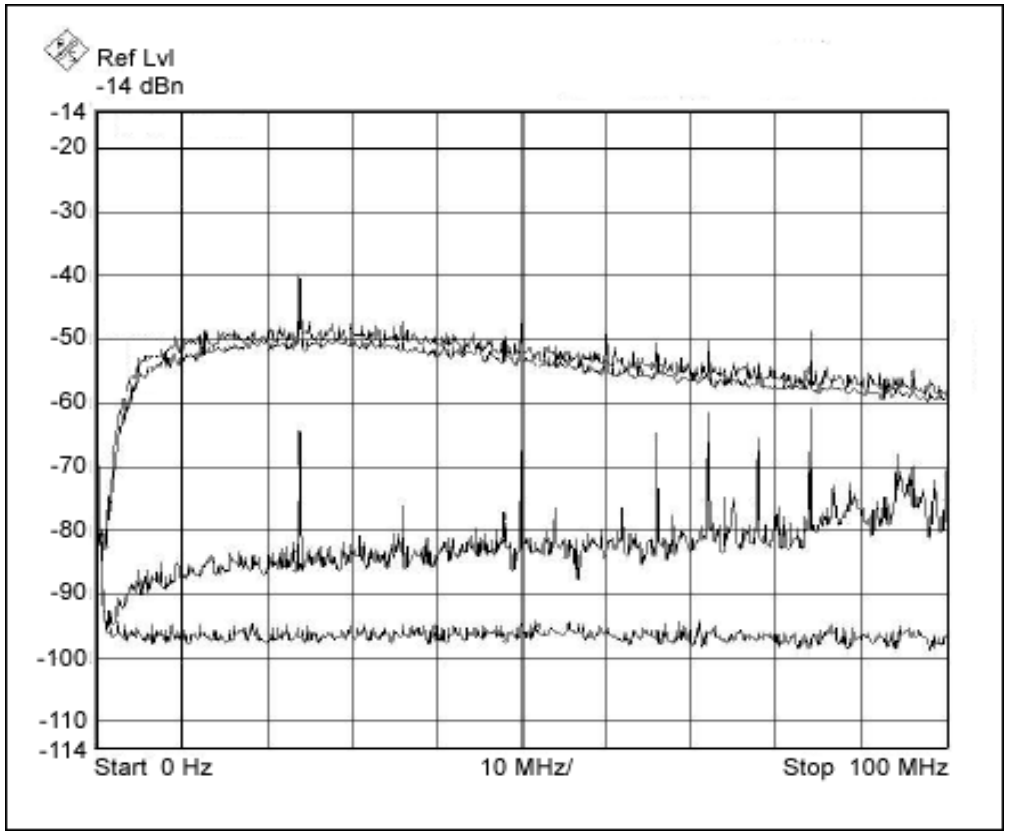
IF-Section 3
Noise Generator 1



- Noise will help in masking the jamming transmission, making it look like random "noise" to an outside observer.
- The noise generator used is based on the avalanche noise generated by a Zener breakdown phenomenon.
- The noise generator circuit consists of:
  - A standard 6.8 volt Zener diode with a small reverse current
  - Transistor buffer
  - National LM386 audio amplifier function as:
    - Small signal amplifier
    - Band pass filter

GSM-900 Mobile Jammer

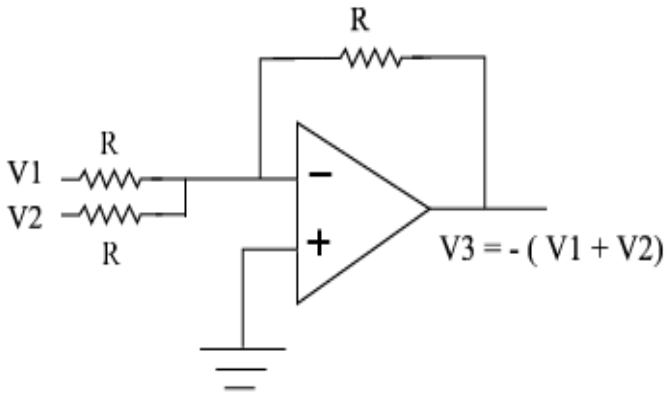
IF-Section 4
Noise Generator 2

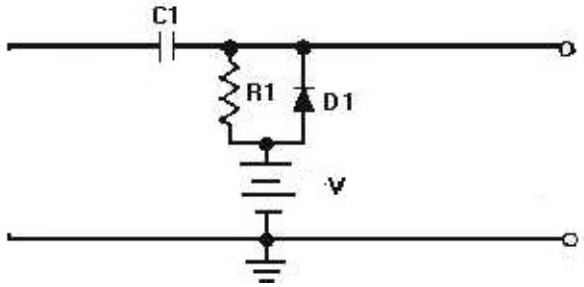


Noise generator output spectrum

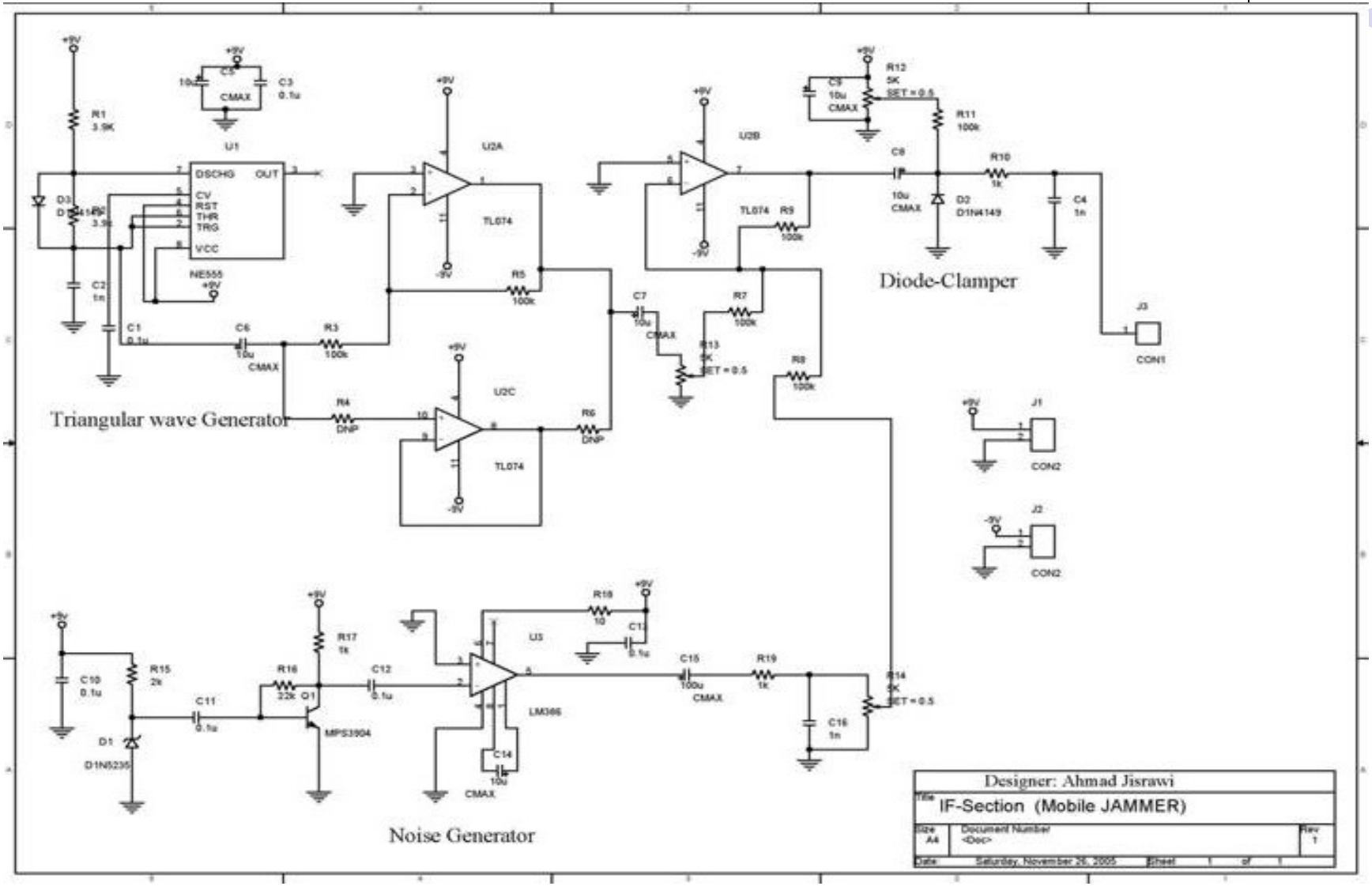
IF-Section 5
Signal Mixer and DC-Offset Circuits

- The triangle wave and noise signals are mixed using Op-Amp configured as summer.
- A DC voltage is added to the resulted signal to obtain the required tuning voltage using Diode-Clamper circuit.



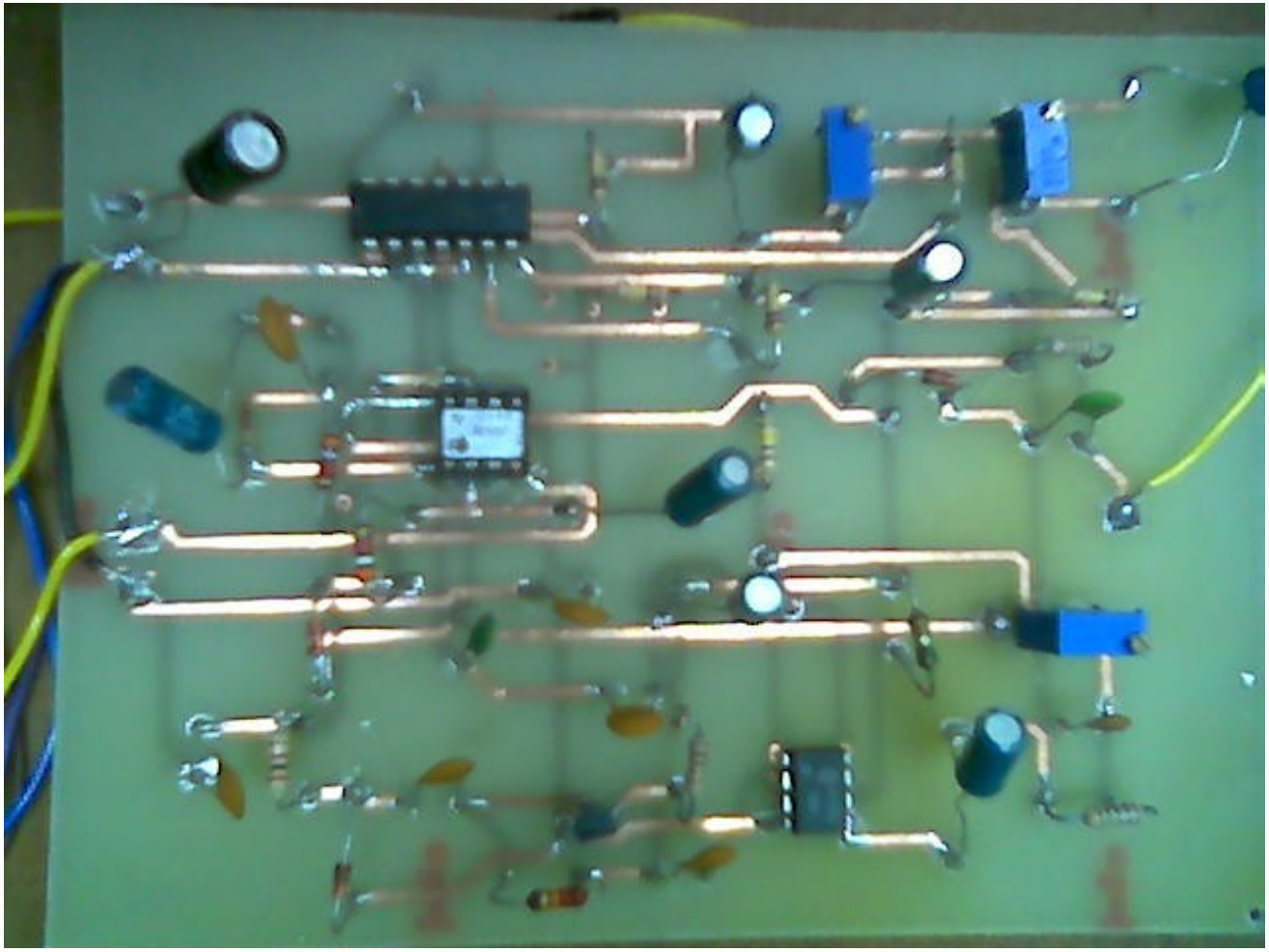


IF-Section 6 Schematics



GSM-900 Mobile Jammer

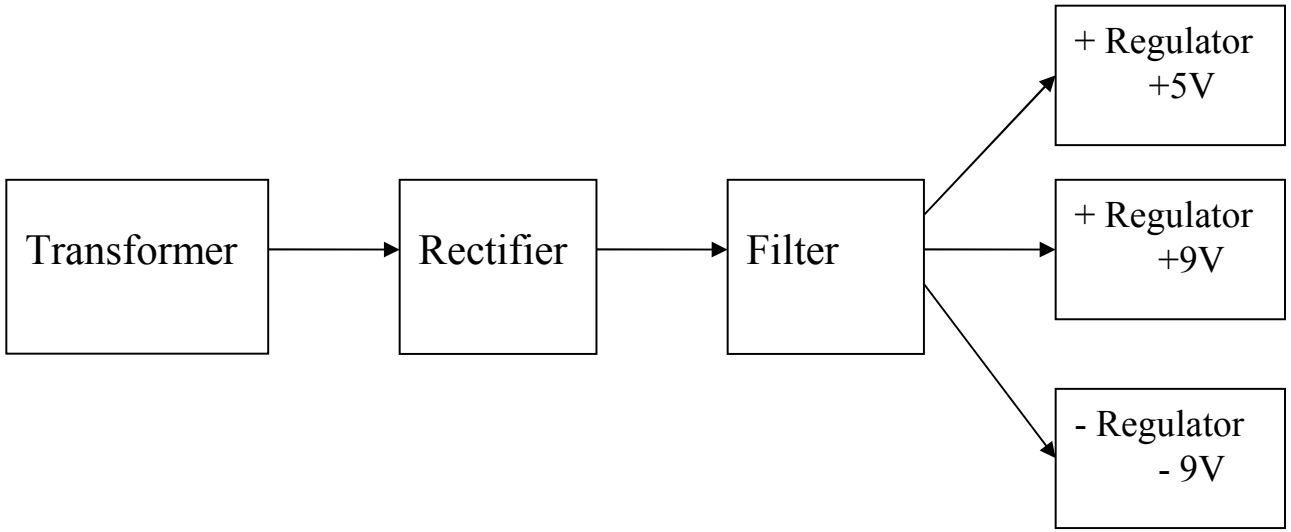
IF-Section 7
PCB



GSM-900 Mobile Jammer

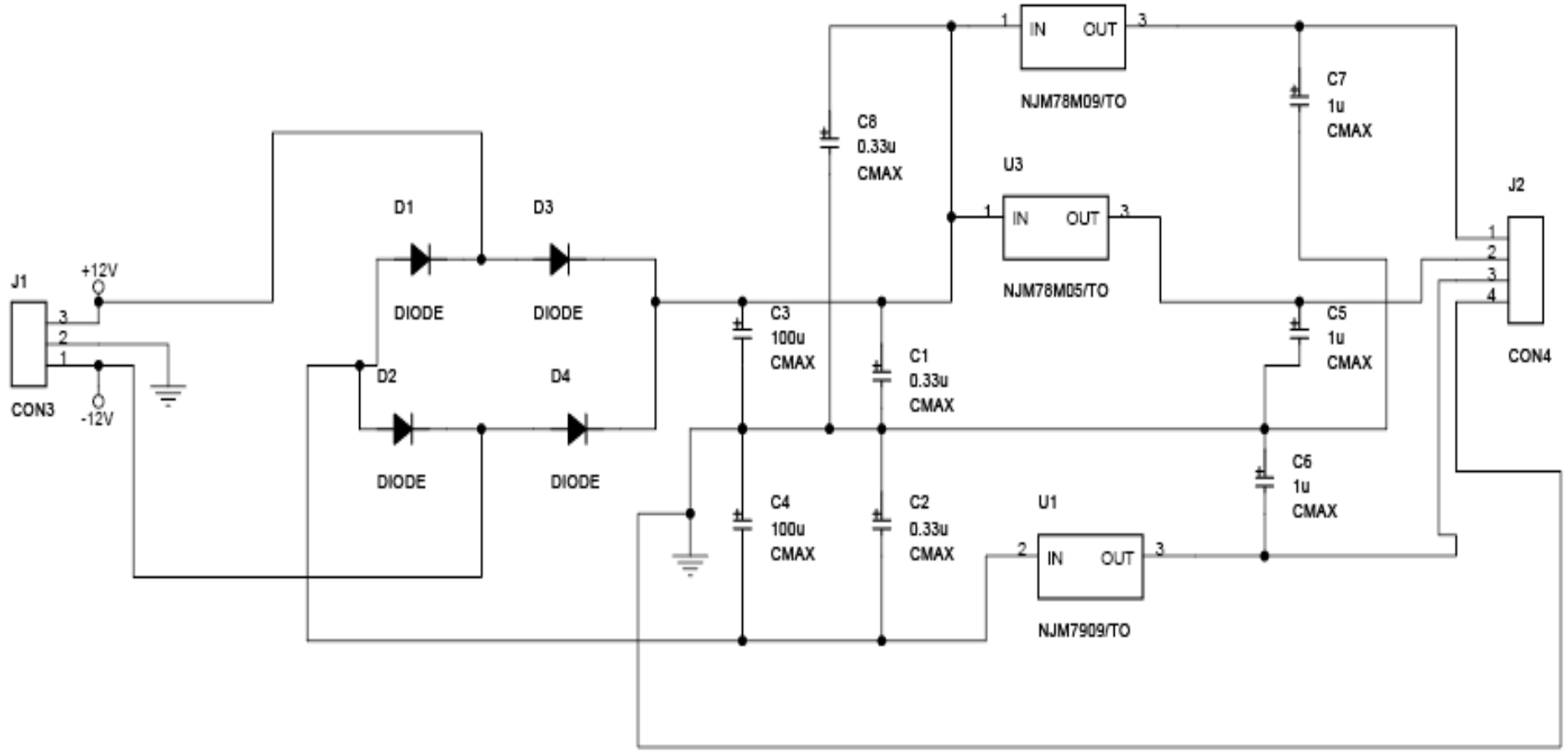
Power Supply 1

- The Jammer designed to take it's power from the regular 220V AC wall outlets.
- The IF & RF sections of the jammer require +5, +9, and -9 DC Voltages.



GSM-900 Mobile Jammer

Power Supply 2 Circuit Schematic



GSM-900 Mobile Jammer

Power Supply 3 PCB

Conclusions

- In this project a GSM-900 Mobile Jammer was designed and built.
- The project was tested against the two GSM-900 Networks in Jordan (i.e. Fastlink and Mobilecom) and has proven success.
- The effective jamming range was not as expected, due to the shortage in the current supplied to the power amplifier also a more stable power supply needed for a robust operation.

Questions?