Bangladesh University of Engineering and Technology

Department of Electrical and Electronics Engineering

EEE 310 Project Report

Title of the Report: Cell phone jammer circuit

Submitted by-

Group number: 06

Group members:

1. Md. Fahadul Islam - 1906054
2. Tasmin Khan - 1906055
3. Bokhtiar Foysol Himon - 1906056
4. Sayed Mommad Tawsif Arefin - 1906057

Submitted to-

1. Dr Mohammad Faisal

   Professor

   Department of Electrical and Electronics Engineering

   BUET

2. Mumtahina Islam Sukanya

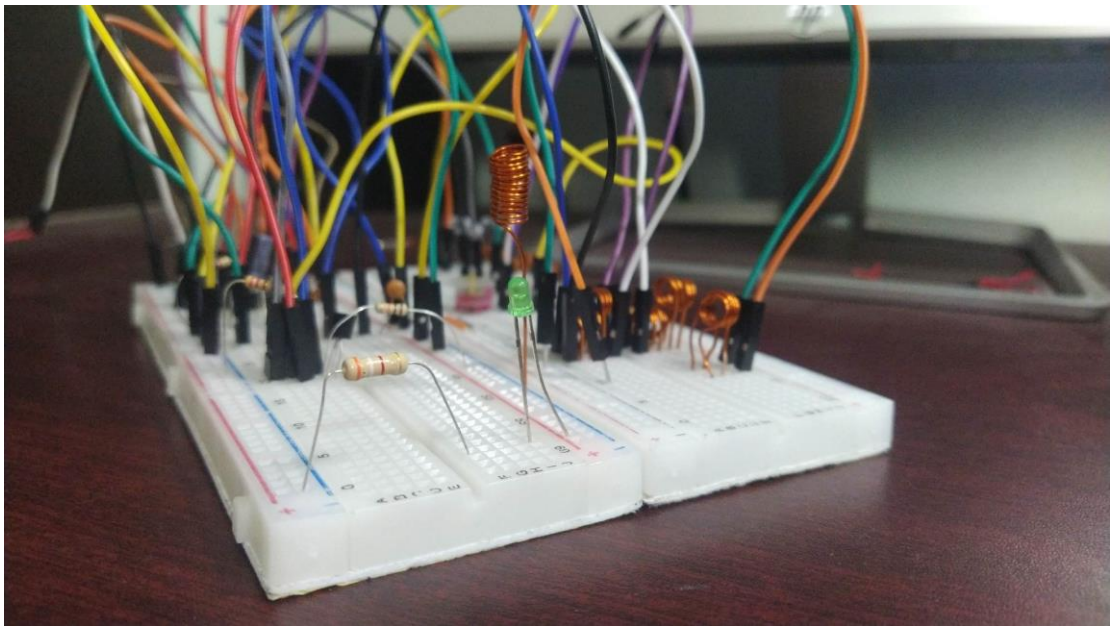
   Lecturer

   Department of Electrical and Electronics Engineering

   BUET

Date of Submission: 26/2/2023

Project: Cell phone jammer circuit



Introduction:

Cell phones use a portion of the radio frequency spectrum allocated to the mobile service, to receive and transmit the signals. Cellular frequencies are the frequency ranges included in UHF (Ultra high frequency) bands that are assigned for cellular phone use.

A **mobile phone jammer** or **blocker** is a device which deliberately transmits signals on the same radio frequencies as mobile phones, disrupting the communication between the phone and the cell-phone base station, effectively disabling mobile phones within the range of the jammer, preventing them from receiving signals and from transmitting them.

Jammers can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected, such as entertainment venues.

Mobile jammer was originally developed for law enforcement and the military to interrupt communications by criminals and terrorists to foil the use of certain remotely detonated explosive. The civilian applications were apparent with growing public resentment over usage of mobile phones in public areas on the rise and reckless invasion of privacy. Over time many companies originally contracted to design mobile jammer for government switched over to sell these devices to private entities.

Different Types of Mobile Jammers

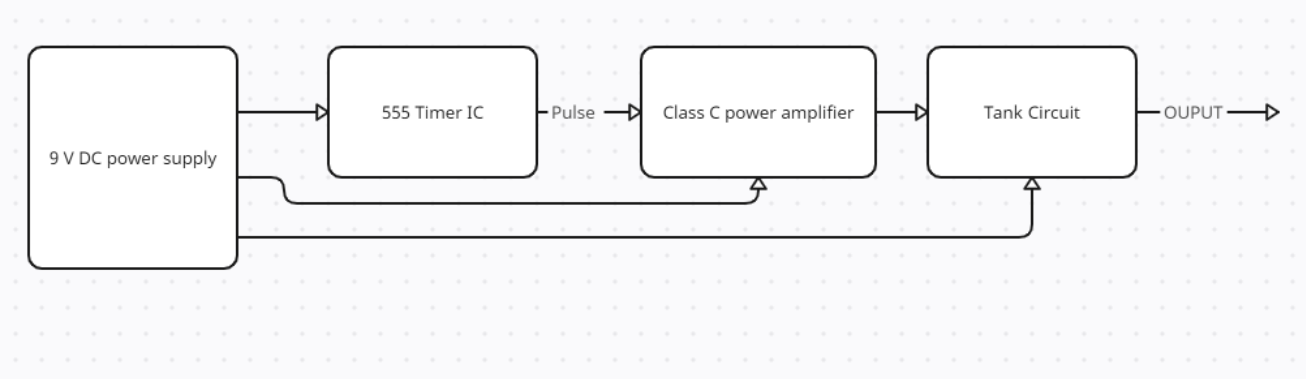
There are different types of mobile jammers which are given below:

- Remote Controlled Mobile jammer
- Adjustable Mobile Jammer
- School & Prison Mobile Jammer
- Explosion Proof Mobile jammer
- Police & Military Mobile Jammer

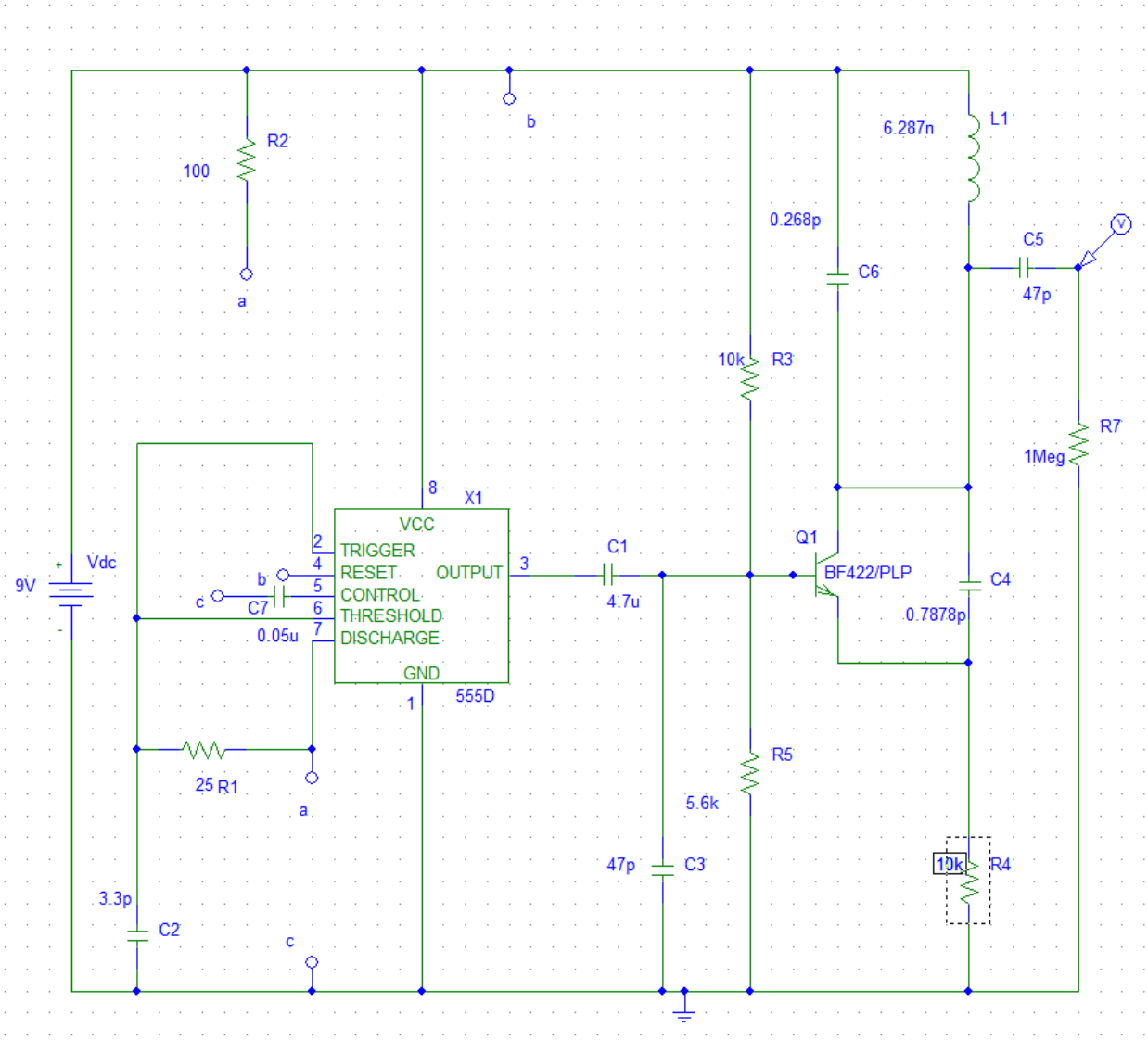
Apparatus:

1. LED light
2. Resistances – 5.6 kΩ, 25 Ω, 0.1 kΩ, 10kΩ etc
3. Switch
4. Voltage source
5. 24 AWG wire
6. NE555 IC
7. BF422 transistor
8. Capacitors 1uF, 3.3pF, 47 pF, 2pF, 30pF, 4.7 pF etc
9. Inductor – 0.6287 nH

Block diagram:



Circuit diagram:



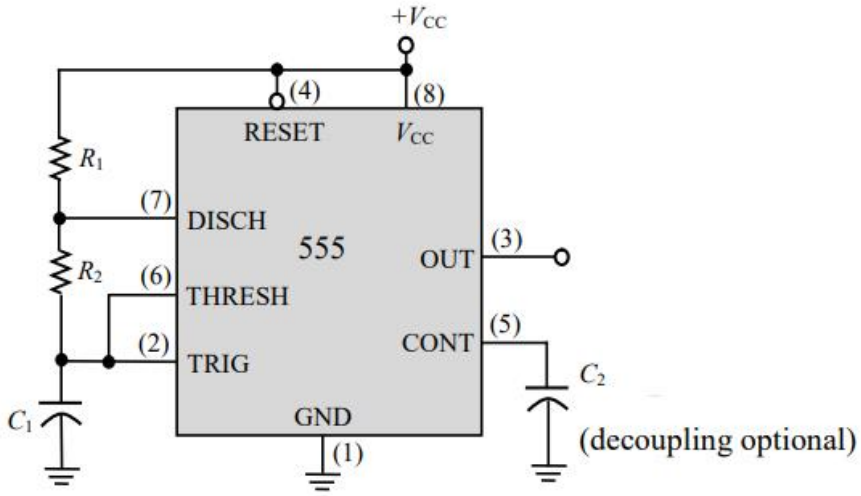
Working procedure:

We have used three main sections in the circuit:

1. Timer circuit to produce a pulse
2. Class C power amplifier to amplify output
3. Tank circuit to tune output frequency to the resonant frequency

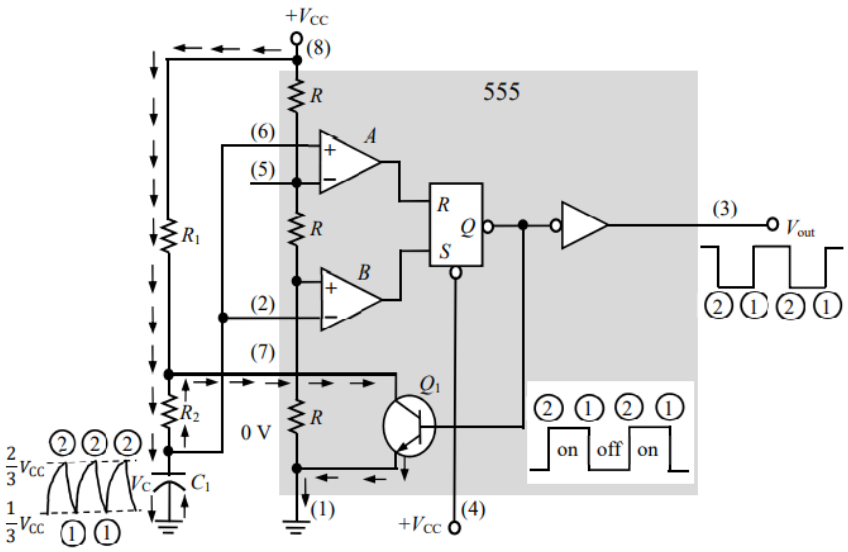
Part 1: Timer- implemented using a NE 555 IC

The 555 timer is a versatile and widely used device because it can be configured in two different modes as either a monostable multivibrator (one–shot) or as an astable multivibrator (oscillator). An astable multivibrator has no stable states and therefore changes back and forth (oscillates) between two unstable states without any external triggering.



A 555-timer connected to operate as an astable multivibrator, which is a free–running non–sinusoidal oscillator. As shown in the figure, the threshold input (THRESH) is connected to the trigger input (TRIG). The external components R1, R2, and C1 form the timing network that sets the frequency of oscillation. The capacitor C2 connected to the control (CONT) input is strictly for decoupling and has no effect on the operation.

Initially when the power is turned on capacitor C1 is uncharged and the trigger voltage at pin 2 is 0V. This keeps the transistor inside the IC off by keeping the base voltage low. As C1 begins charging through R1 and R2, the base of the transistor goes high when the capacitor voltage reaches to a voltage of 2Vcc/3. Thus, it turns the transistor on.



This sequence creates a discharge for the capacitor through R2 and the transistor. As the capacitor discharges and down to Vcc/3, the transistor is turned off again. And then the next charging cycle begins.

The duty cycle of the resultant wave's depends on the values of R1 and R2. The frequency of the oscillation is given by the equation as follows:

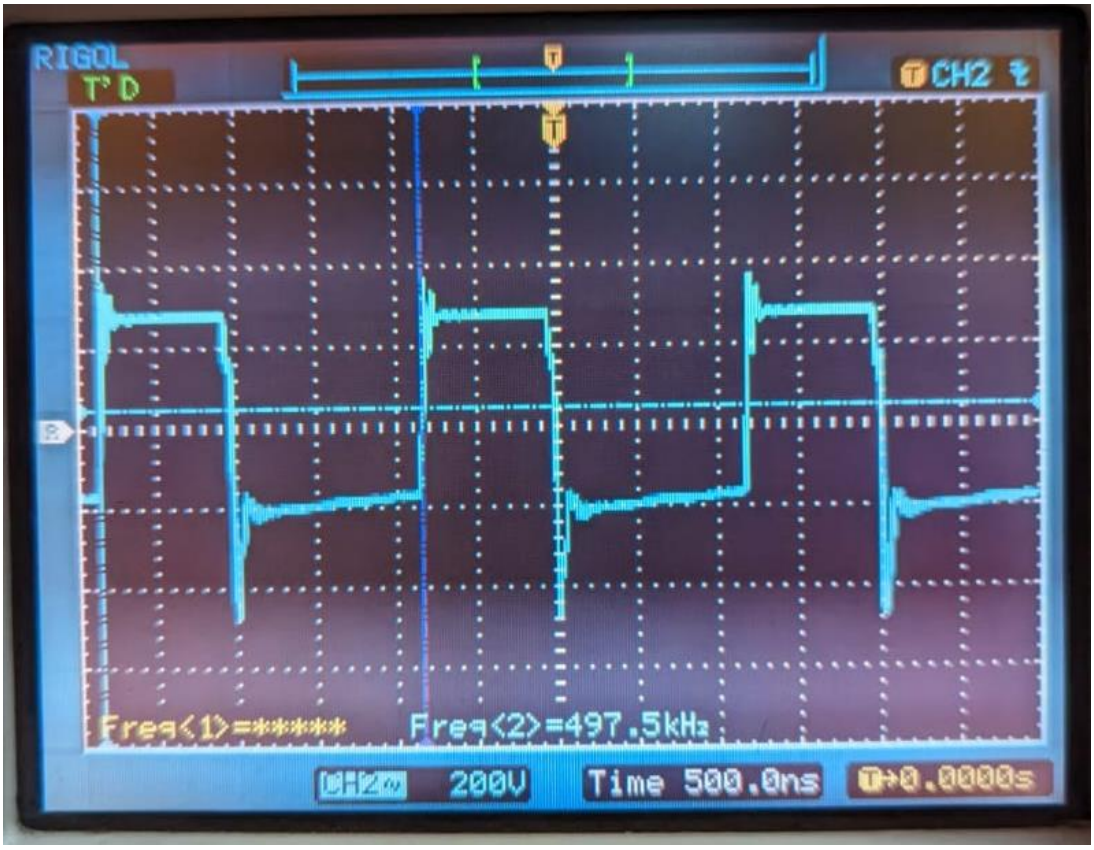
$$f = \frac{1.44}{(R1 + 2R2) * C1}$$

And the duty cycle can be determined as

$$Duty\ cycle = \frac{R1 + R2}{R1 + 2R2} * 100\%$$

The available IC for timer has a frequency limitation, It is only compatible for a frequency range of 2-3 MHz. We used the timer to produce a pulse of around 500 kHz from our DC power source supply. The pulse has high frequency components present as seen clearly from the plot in oscilloscope on the next page.

Timer output in oscilloscope channel 2:

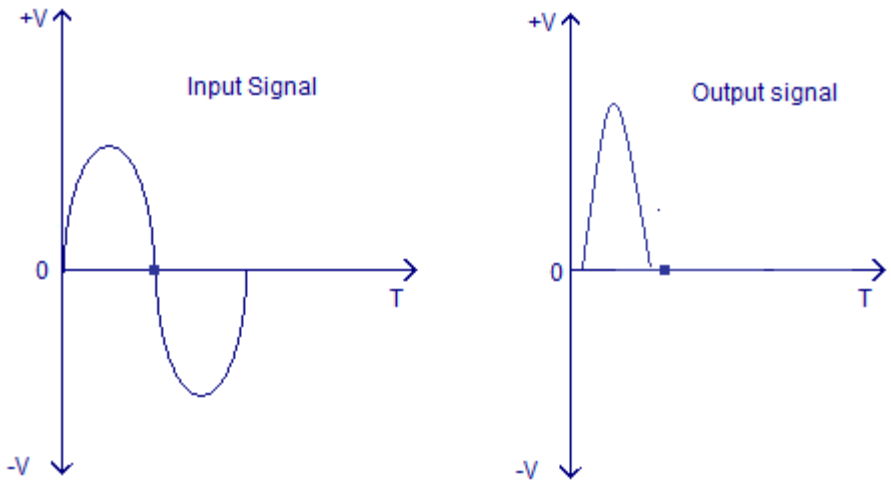


The output of this timer is then passed via a DC blocking capacitor C = 4.7µF to the next stage.

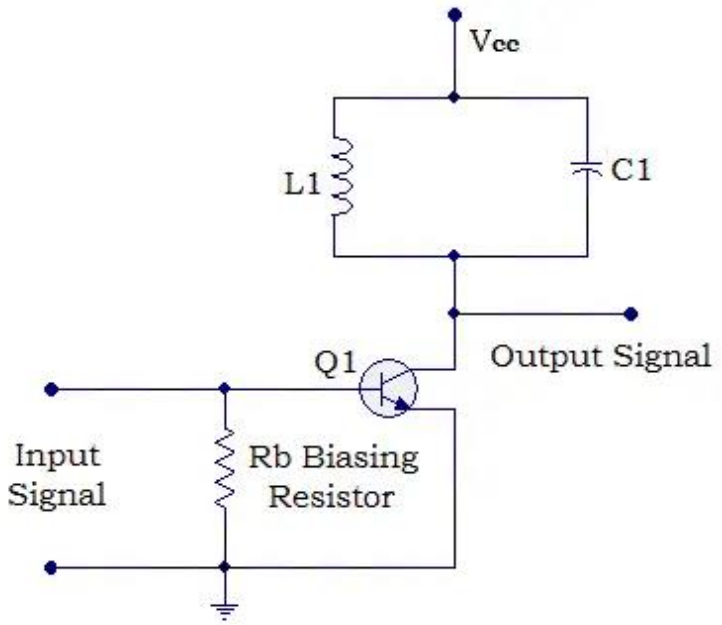
Part 2: Class C power amplifier implemented using BJT

Class C power amplifier is a type of amplifier where the active element (transistor) conduct for less than one half cycle of the input signal. Less than one half cycle means the conduction angle is less than 180° and its typical value is 80° to 120°. The reduced conduction angle improves the efficiency to a great extend but causes a lot of distortion. Theoretical maximum efficiency of a Class C amplifier is around 90%.

Due to the huge amounts of distortion, the Class C configurations are not used in audio applications. The most common application of the Class C amplifier is the RF (radio frequency) circuits like RF oscillator, RF amplifier etc where there are additional tuned circuits for retrieving the original input signal from the pulsed output of the Class C amplifier and so the distortion caused by the amplifier has little effect on the final output. Input and output waveforms of a typical Class C power amplifier is shown in the figure below:



The output from timer section is used as an input in the class C amplifier made with a npn BJT. A simpler figure is drawn below to explain the operation:



The circuit diagram of the class c power amplifier circuit is shown above. In the above circuit, the biasing resistor' Rb' is used to pull the base terminal of the Q1 transistor further downwards. The 'Q' point will be fixed to below the cutoff point in the DC load line.

As a result, the Q1 transistor will start conducting only after the i/p signal amplitude has increased above the base-emitter (BE) voltage plus the downward bias voltage caused by a biasing resistor. This is the reason why the main portion of the i/p signal is not present in the o/p signal.

Part 3: Tank circuit for frequency tuning

A tank circuit can be formed by using a capacitor ‘C1’ and an Inductor ‘L1’ which help in the removal of the necessary signal from the pulsed o/p of the transistor. Here, the main function of the transistor is to generate a current pulse in series according to the i/p and make it flow through the resonant circuit.

The values of the capacitor and inductor are selected so that the resonant circuit oscillates at the frequency of the i/p signal. Since the resonant circuit oscillates in the carrier frequency, then all other frequencies are attenuated & the values of L1 and C1 are so selected that the resonant circuit oscillates in the frequency of the input signal. Now as the resonant circuit oscillates in one frequency (generally the carrier frequency) all the necessary frequency can be pushed out using a duly tuned load. Harmonics in the o/p signal can be removed using an extra filter if necessary. In schematics, we used a capacitor in the output section to help with dc blocking and a resistor to visualize the output voltage.

In our experiment, we took the values for the components as

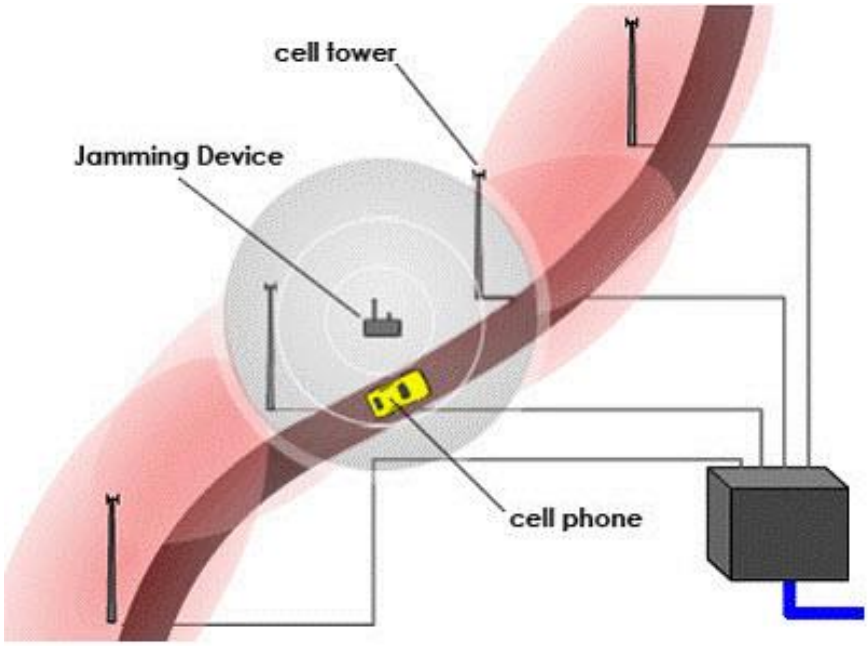
Rb = 5.6 kΩ

L1 = 6.287 nH

And C1 = 0.268 pF

By the components selected we tuned the voltage-controlled oscillator circuit to a frequency of $f = \frac{1}{2\pi\sqrt{LC}}$ = 3877.3 MHz

So, it is expected to produce an output in a frequency somewhere near this range. Thus the Mobile phone jammer devices transmit the similar radio frequency which is greater power than the cell phone. The communication between the cell phone and the base station of the phone tower is called as a denial-of-service attack.

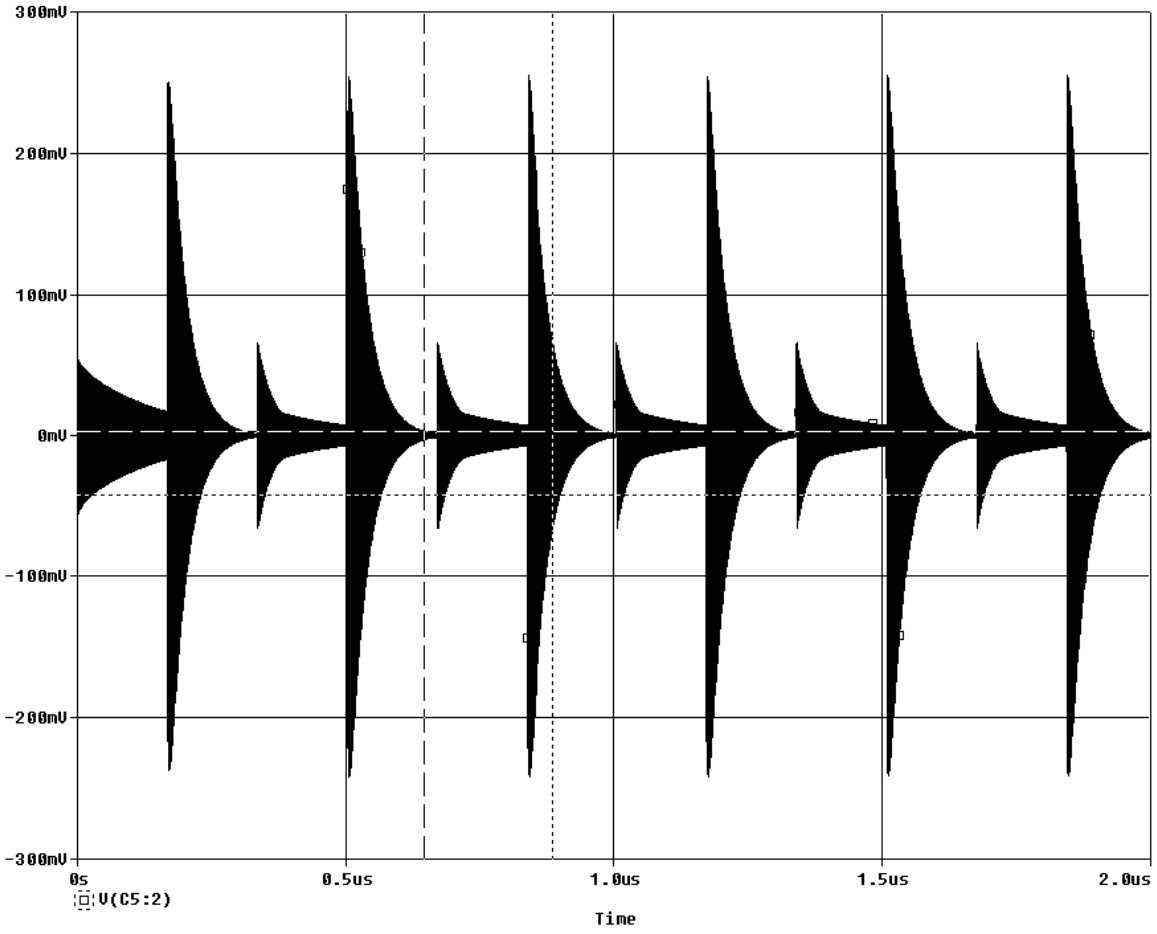


This causes the obstruction with the communication of cell phones and towers to make the cell phones not viable and there is no network visibility. Hence it works in both ways i.e. Cell phone to the tower frequency and the other one is tower to mobile frequency.

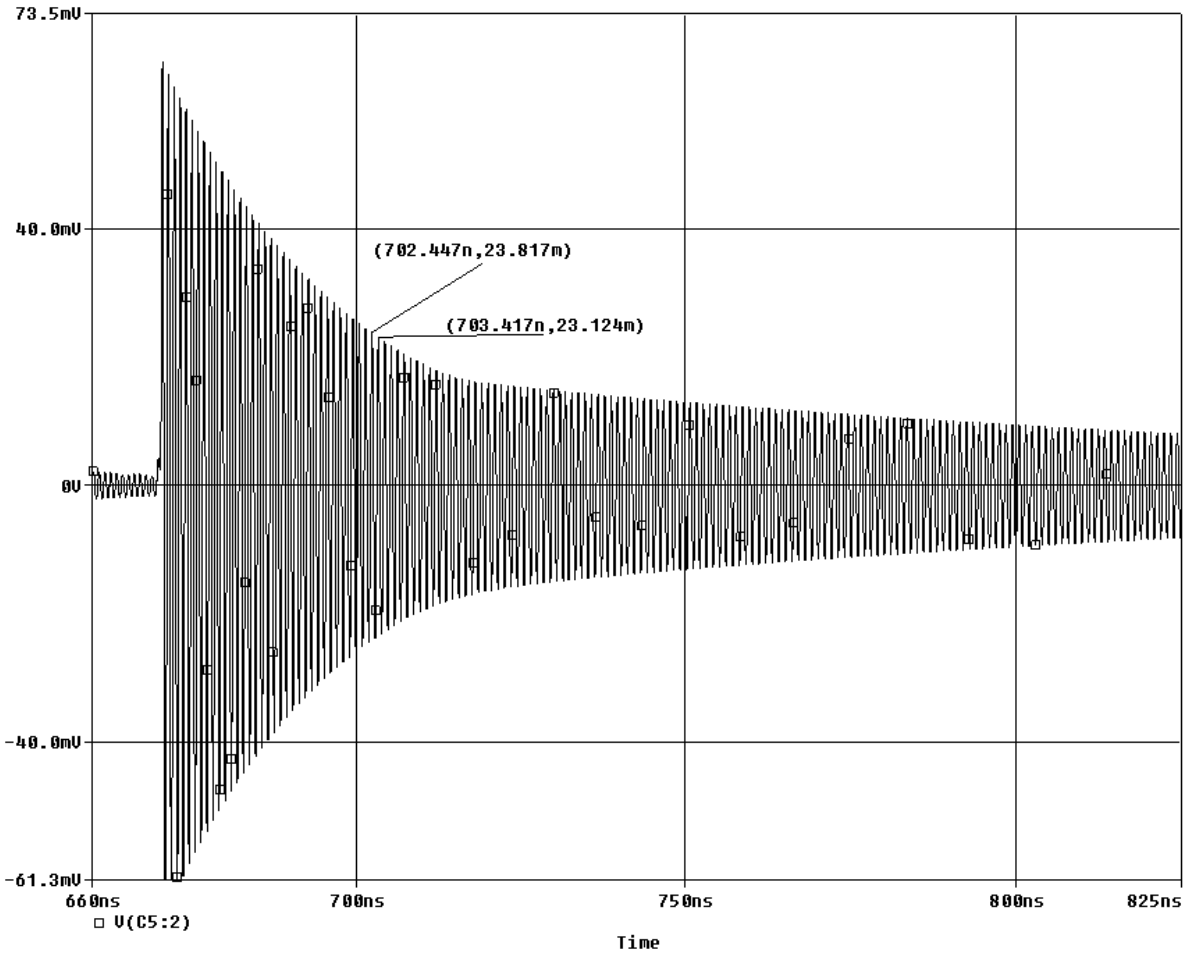
Simulation:

We first ran a simulation in PSPICE. But the model parameters in PSPICE library were out of our direct control. However we were able to produce periodic output of around 100 MHz. In the following picture the envelope for the high frequency signal is obvious. For better view into the high frequency output we also added a zoomed in version of the plot.

Output:

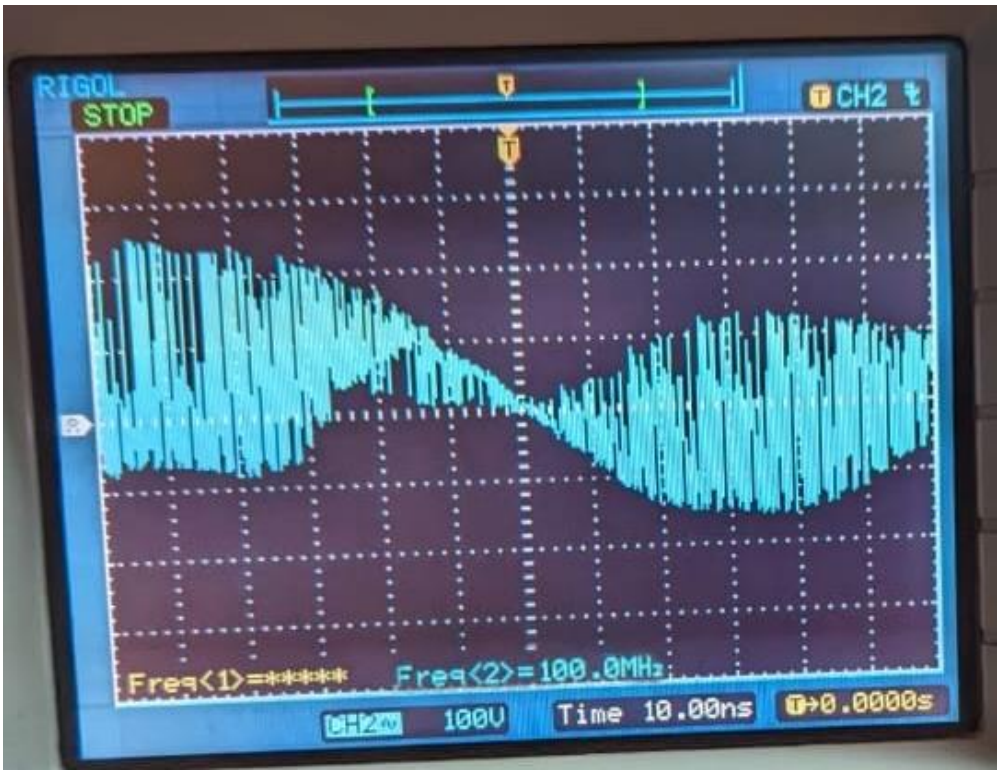


Zoomed In version:



Practical output:

For the BJT model of BF422 the operating frequency range is around 100 MHz. We were able to push the output to achieve this frequency as shown in the picture:



We then used this signal to jam the transmitting radio frequencies of around 100 Mhz. In mobile phone FM radio stations were jammed of the channel 104.0 MHz . We were also able to jam the signal for 106.0 Mhz channel. The radio station was hearable with clean sound when jammer circuit was off. But as we turned the jammer circuit on, the output was completely distorted, and no meaningful audio was present.

User interface in mobile phone for the mentioned channels:

So, we can say that we were successful in jamming the radio signal for specific frequency channels.

We used 24 AWG wire to make a coil to be used as the antenna. It allowed us to have a range of approximately 1 meter where the jamming worked precisely. As we increased the distance, the distortion due to jamming became less and less.

Limitation:

Among the limitations are that the timer can only produce a limited frequency due to the restrictions imposed upon it by physical structure. This frequency is passed to the input of the BJT. Based on the model of the BJT there is also a limitation applied on the maximum frequency that it can achieve in amplification. For our BJT model we were able to achieve a frequency of 100 MHz despite tuning the tank circuit for even higher frequency. This is a limitation imposed by the hardware available in the market.

Most of the cells operate in the range of the Radio frequency which ranges from 3kHz to 300GHz. RF usually refers to electrical rather than mechanical-oscillations, however, mechanical-RF-systems do exist.

Now a company only operates under the frequency band that is allocated to itself. In Bangladesh, according to ITU Radio Regulation and NFAP, 698 – 806 MHz, 2500 – 2690 MHz and 1920 -1980 / 2110-2170 MHz frequency bands are reserved for 3G/ 4G/ LTE services.

So we needed to produce output frequency in this range so that it interferes with the nearest cellular device signals and prevents it from having any feasible input or transmitting any meaningful output. Important thing to notice here that, cell phones are not barred from receiving or transmitting when operating in the zone of a signal jammer. But only the necessary signal is distorted with unwanted signal of the same frequency so that no one is able to use that frequency band as long as the jammer circuit is active and operating.

Due to our project hardware limitation, we were not able to produce required high frequency output necessary to jam the signals of today's cellphone. However, we were able to jam the signal for FM radio signal and the project was successful for frequency range at around 100 MHz.

If we could use different hardware, specially BJT which are manufactured for operating in very high frequencies like 900 MHz, then we would have been able to overcome this limitation. We could also increase our range of jamming with a better antenna configuration.

Drawbacks of RF jammer:

- RF jammer can only be used for military communications or government agencies or test and research applications etc.
- It is illegal to use in most of the countries. If it is used without obtaining permission from concerned authorities than fines will be levied.
- RF jammers can cause unintended interference to emergency communications, legitimate cellular communications, navigation systems such as GPS, wireless medical devices etc.
- RF jammers support limited coverage area as per its design specification and hence it can not jam target outside its coverage range.
- RF jammers can jam specific frequency range and wireless technologies for which they have been designed.
- For significant reasons RF jammers are illegal in many countries and can only be used for academic or research purpose.

Applications:

RF jamming devices were originally developed for law enforcement and the military to interrupt communications by criminals.

During a hostage situation, police can control when and where a captor can make a phone call. Police can block phone calls during a drug raid so suspects can't communicate outside the area.

Corporations use jammers to stop corporate espionage by blocking voice transmissions and photo transmissions from camera phones.

These days cell phone jammers are used in cinema halls, cricket stadium, temples or churches and even in office premises where business meetings are held. So, mobile cell phone jamming device works well when people forget to switch off their mobile phone and there would be no ringing of any mobiles and the meeting can continue peacefully.

Jammers are used in school, library and hospital as well to maintain silence when it is crucial for consistent operation.

Reference:

1. https://www.indiastudychannel.com/resources/112413-Mobile-Cell-Phone-Jammers-Applications-Use.aspx
2. https://en.wikipedia.org/wiki/Cellular_frequencies
3. https://www.vedantu.com/question-answer/cellular-mobiles-work-in-the-frequency-range-of-class-12-physics-cbse-5f8b45f84885cc7bcb3bc485
4. https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-RF-Jammer.html