VIT®
BHOPAL
www.vitbhopal.ac.in

SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING

B.Tech Final Review Presentation

on

"Advance Military Defense Mechanism"

Date: 5th May, 2021

Guided by:-

Dr. Ribu Mathew
Assistant Professor, ECE

Presented By:-

Manas Goyan	19BEC10009
Shikha Saraswat	19BEC10012
Rishu	19BEC10018
Neha Rani	19BEC10021
Ashutosh Pathak	19BEC10022

Contents:-

INTRODUCTION:

- Advance military defense mechanism
- Aim-To improve current defense mechanism
- Brief overview: This mechanism is basically designed to tighten up the security at LOC via shutting down the communication of intruders in the LOC region.

According to Economic times survey Pakistan has violated the ceasefire more than?

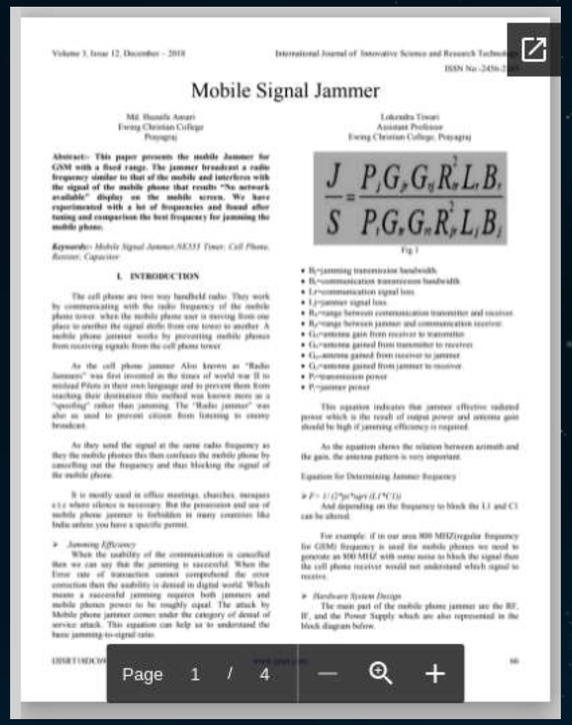
5100	36	24
CEASEFIRE	CIVILIAN LIFE CASUALTIES	SECURITY PERSONNEL DIED

- The main cause of the cease fire is to make militants cross the LOC while we are busy at the other place fighting the enemy.
- Also at remote locations which can't be easily reached by our military due to extreme conditions like Low visibility,extreme temperatures etc

A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network:

Suparna Biswas & Subhajit Adhikari– Gave solution to problem faced in the current apparatus are:

Literature Review:



Volume 3, Issue 12, December – 2018 International Journal of Innovative Science and Research Technol

ISSN No -2456-2

Mobile Signal Jammer

Md. Humila Ansari
Ewing Christian College
Prayagraj

Lokendra Tiwari
Assistant Professor
Ewing Christian College, Prayagraj

Abstract:- This paper presents the mobile Jammer for GSM with a fixed range. The jammer broadcast a radio frequency similar to that of the mobile and interferes with the signal of the mobile phone that results "No network available" display on the mobile screen. We have experimented with a lot of frequencies and found after tuning and comparison the best frequency for jamming the mobile phone.

Keywords:- Mobile Signal Jammer,NE555 Timer, Cell Phone, Resistor, Capacitor

I. INTRODUCTION

The cell phone are two way handheld radio. They work by communicating with the radio frequency of the mobile phone tower. when the mobile phone user is moving from one place to another the signal shifts from one tower to another. A mobile phone jammer works by preventing mobile phones from receiving signals from the cell phone tower.

As the cell phone jammer Also known as "Radio Jammers" was first invented in the times of world war II to mislead Pilots in their own language and to prevent them from reaching their destination this method was known more as a "spoofing" rather than jamming. The "Radio jammer" was also as used to prevent citizen from listening to enemy broadcast.

As they send the signal at the same radio frequency as they the mobile phones this then confuses the mobile phone by cancelling out the frequency and thus blocking the signal of the mobile phone.

It is mostly used in office meetings, churches, mosques etc where silence is necessary. But the possession and use of mobile phone jammer is forbidden in many countries like India unless you have a specific permit.

➢ *Jamming Efficiency*

When the usability of the communication is cancelled then we can say that the jamming is successful. When the Error rate of transaction cannot comprehend the error correction then the usability is denied in digital world. Which means a successful jamming requires both jammers and mobile phones power to be roughly equal. The attack by Mobile phone jammer comes under the category of denial of service attack. This equation can help us to understand the basic jamming-to-signal ratio.

$$\frac{J}{S} = \frac{P_j G_j G_t R_r^2 L_r B_r}{P_t G_t G_m R_j^2 L_j B_j}$$

Fig 1

- B_j=jamming transmission bandwidth
- B_r=communication transmission bandwidth
- L_r=communication signal loss
- L_j=jammer signal loss
- R_r=range between communication transmitter and receiver
- R_j=range between jammer and communication receiver.
- G_t=antenna gain from receiver to transmitter
- G_r=antenna gained from transmitter to receiver.
- G_m=antenna gained from receiver to jammer
- G_j=antenna gained from jammer to receiver.
- P_t=transmission power
- P_j=jammer power

This equation indicates that jammer effective radiated power which is the result of output power and antenna gain should be high if jamming efficiency is required.

As the equation shows the relation between azimuth and the gain, the antenna pattern is very important.

Equation for Determining Jammer frequency

➢ *F= 1/(2*pi*sqrt (L1*C1));*

And depending on the frequency to block the L1 and C1 can be altered.

For example: if in our area 800 MHZ(regular frequency for GSM) frequency is used for mobile phones we need to generate an 800 MHZ with some noise to block the signal then the cell phone receiver would not understand which signal to receive.

➢ *Hardware System Design*

The main part of the mobile phone jammer are the RF, IF, and the Power Supply which are also represented in the block diagram below.

ISSN:[illegible] www.ijisrt.com 66

Page 1 / 4

Link of website:

https://www.researchgate.net/publication/290977661_A_Survey_of_Security_Attacks_Defenses_and_Security_Mechanisms_in_Wireless_Sensor_Network

https://iopscience.iop.org/article/10.1088/1757-899X/322/5/052033/pdf

Traditional approach towards security apparatus using the methodology jamming of the communication system to prevent the security breach

The results given are like identification of different types of Security attacks, their effects and defense mechanisms in Wireless Sensor Network

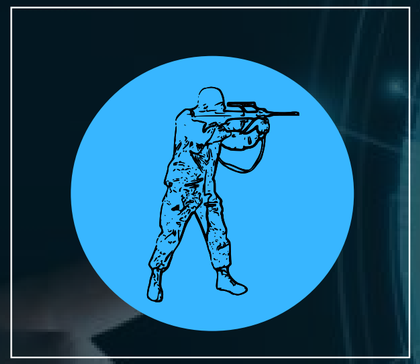
The advantage is that it stops security breach by cutting of the communication and disadvantage is that there are security attacks on sensor networks and they lack of central control.

The evaluation parameters used are based on the working of the sensors future work as suggested by author or concluded in this paper is the addition of machine learning will be very good.

Findings:-

Action Step 1

- The monitoring and eavesdropping on the packet exchange by unauthorized attackers, With the help of snooping to the data, the adversary could easily find the communication contents.



Action Step 2

- Attacks are being done on the availability of the network so we can cut off the communication in the region of intrusion by jamming.

Action Step 3

- Here we need an advance military defense mechanism in the modern warfare to restrict these activities so that the intrusion can be stopped.

Action Step 4

- Using this mechanism can help the soldiers in locating the intruders and restricting the communication among them.

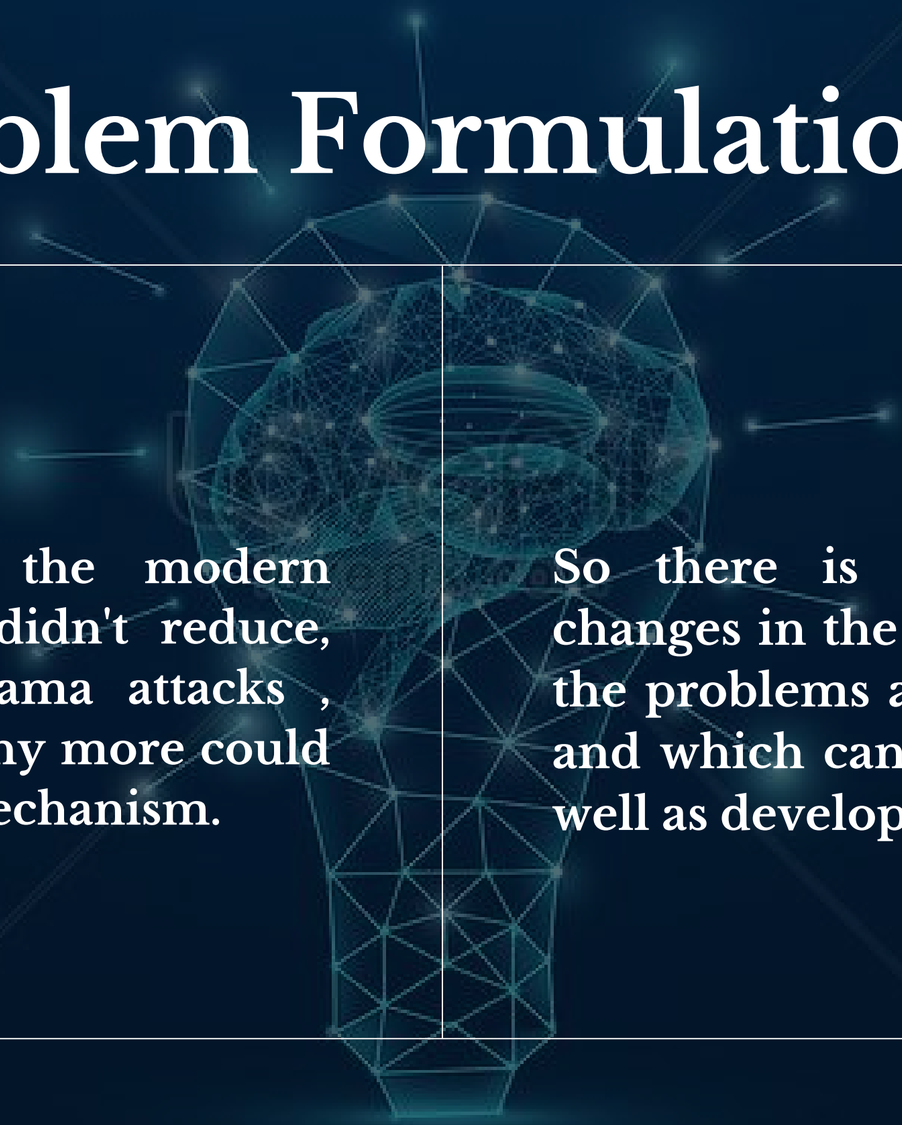
Objectives:

- To defend the soldiers from being attacked by the intruders
- To improve the present military defense mechanism
- Getting information of intruders while intrusion in the specific area.
- The information about them is to be communicated directly to the soldiers even in remote region.
- To cut off the communication between the intruders before they enter the LOC.

Work plan and gantt chart:

S.NO	Particulars	Duration	Outcome
1	Module 1 (Literature survey)	15-02-2021 to 23-02-2021	This literature survey helped us to get ideas about introducing different techniques like jammer and ultrasonic sensors etc. to reduce casualties.
2	Module 2 (Planning & Component finding)	24-02-2021 to 09-03-2021	It helped us in planning the prototype and make arrangements of the required components.
3	Module 3 (Designing & Assembling)	10-03-2021 to 29-03-2021	Designing of circuit on various software & Assembling of all the components like Arduino UNO, Ultrasonic sensor etc.
4	Module 4 (Implementation & Validation)	30-03-2021 to 14-03-2021 & 28-03-2021 to 01-04-2021	Helped us to visualize the components working and also to check whether we are encountering any problem in there working.
5	Module 5 (Report Preparation & Presentation)	01-04-2021 to 06-04-2021	The outcome of the report & presentation making is to provide important details about the project and can be used to develop future forecast about marketing plan, budget planning and improve decision making

Problem Formulation:



Despite the advancement in the modern defence system, the casualties didn't reduce, some of the attacks like Pulwama attacks , Mumbai attacks of 2006 and many more could have been resisted with proper mechanism.

So there is challenging need of making changes in the current military mechanism as the problems are in the roots of technicalities and which can be fulfilled with the proper as well as developed mechanism.

Methodology:

Sensing of any object in its radius

Alert through sound of Buzzer

Location on Radar

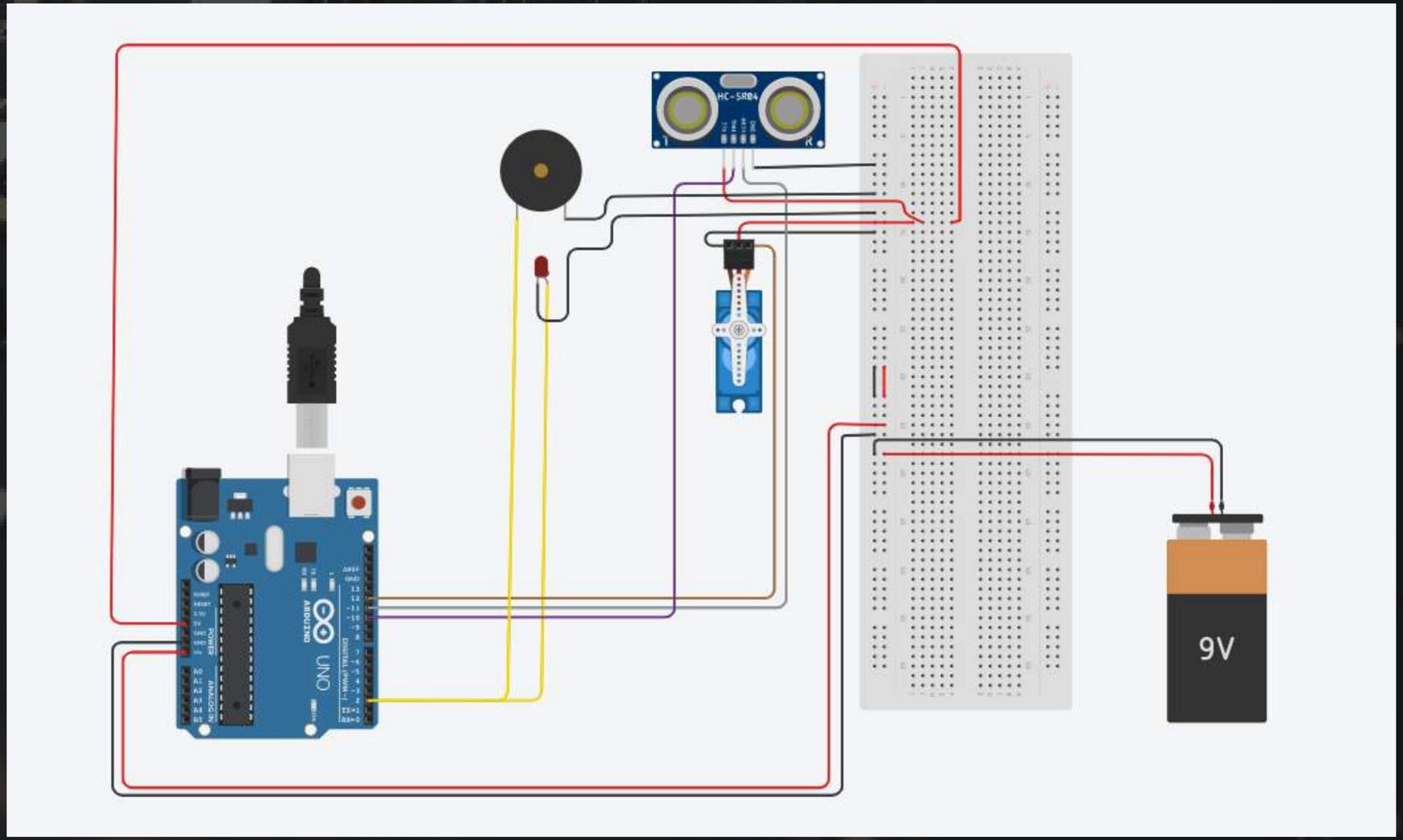
Jammer

LED Glow's

Circuit Diagram

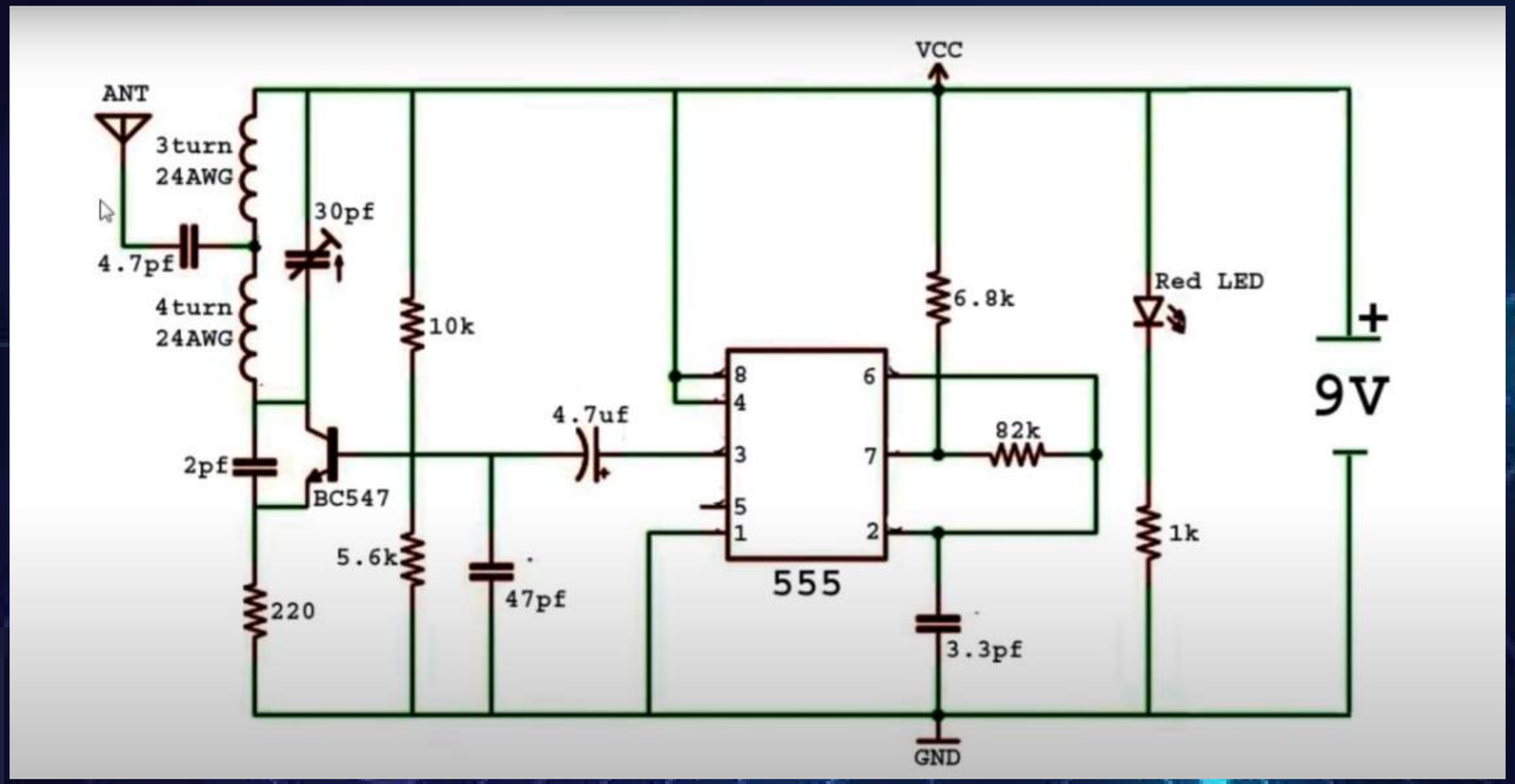
Ultrasonic sensor

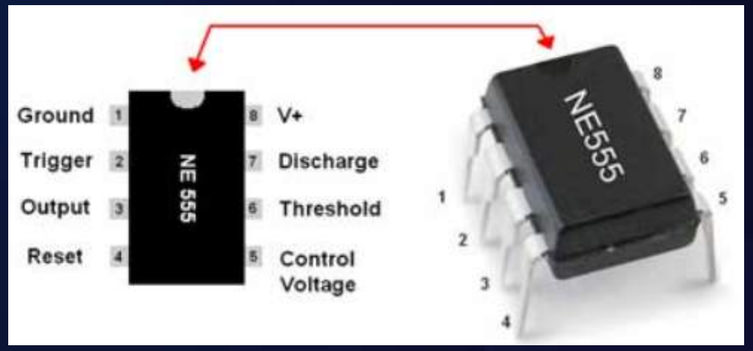
Servo Motor

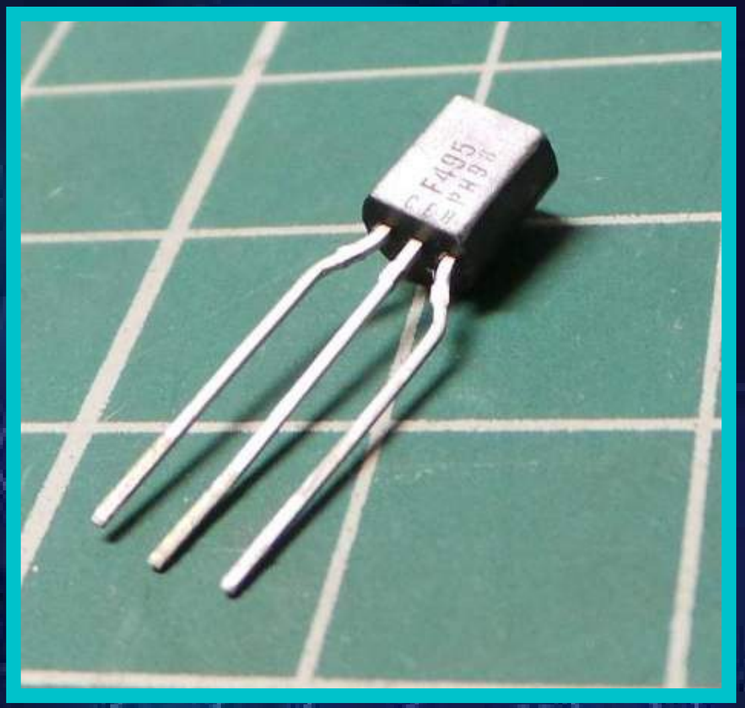


Circuit Diagram

Jammer







List Of Components

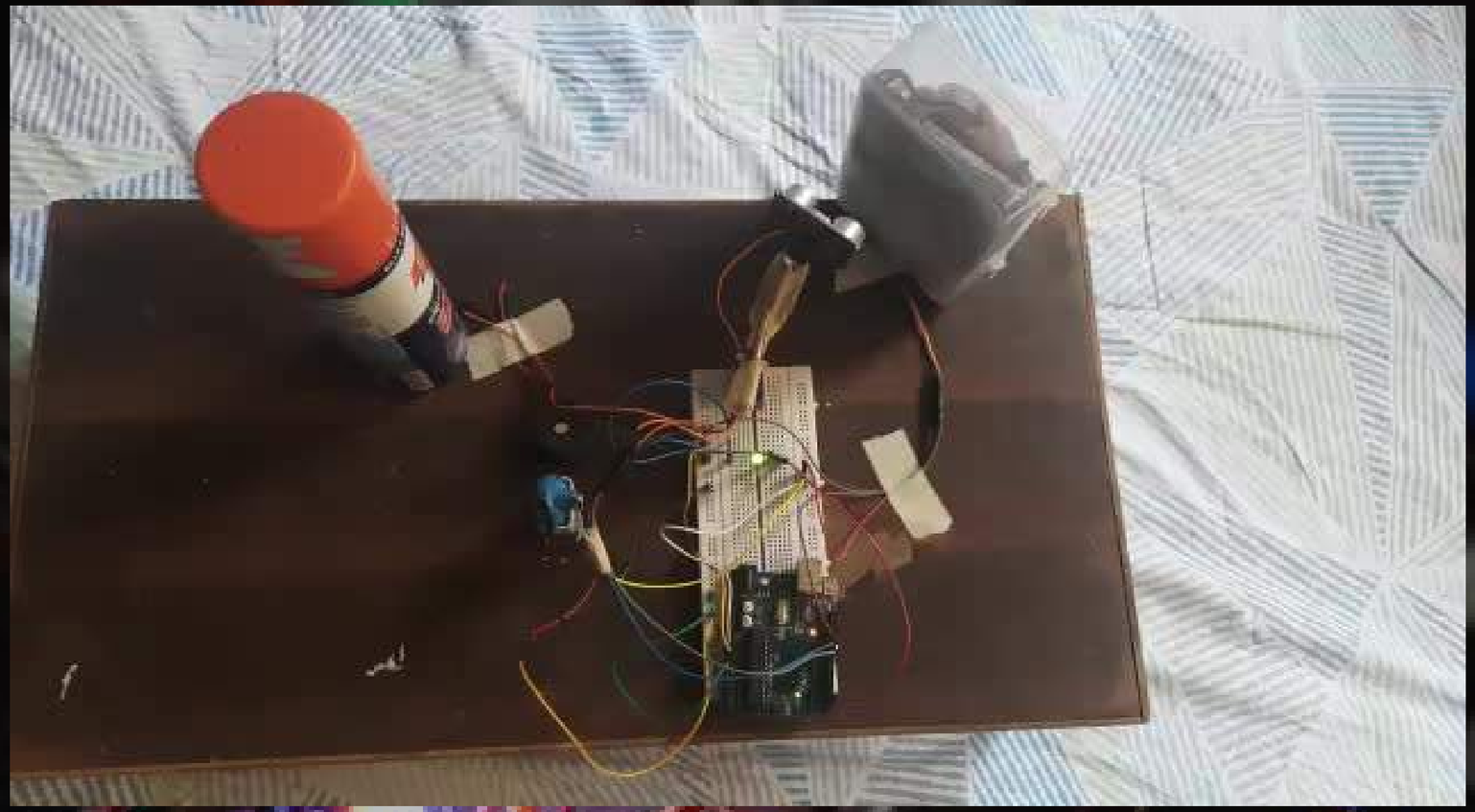
- PCB board
- Jumper wire
- Copper wire (0.5 mm wire of 24AWG)
- Capacitor (2.2µF,4.7µF,47 pF,3.3pF,30pF etc.)
- Resistance (8.8k Ω,82k Ω,220k Ω etc.)
- Transistor (BF495)
- IC(NE555)
- Led
- Buzzer
- Bread Board
- Arduino UNO
- Ultrasonic sensor/LIDAR Sensor
- Battery(9V Battery)
- Servo motor (mini)

Software Used:

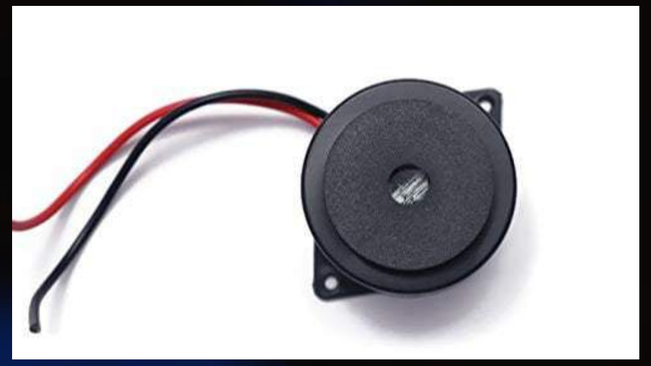
- Tinker Cad
- Proteus
- Arduino IDE
- Processing 3.5.4

Hardware Model

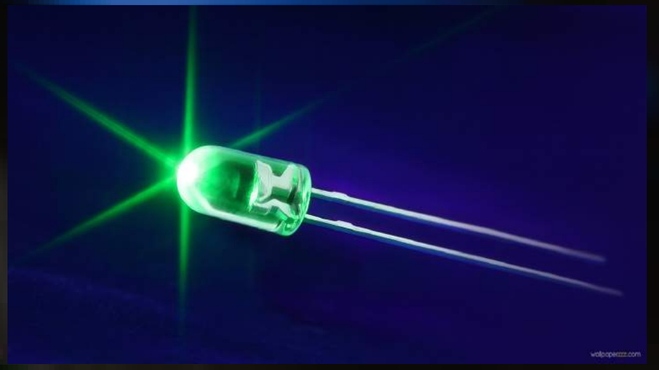
Sensing of any object in its radius



Alert through sound of Buzzer

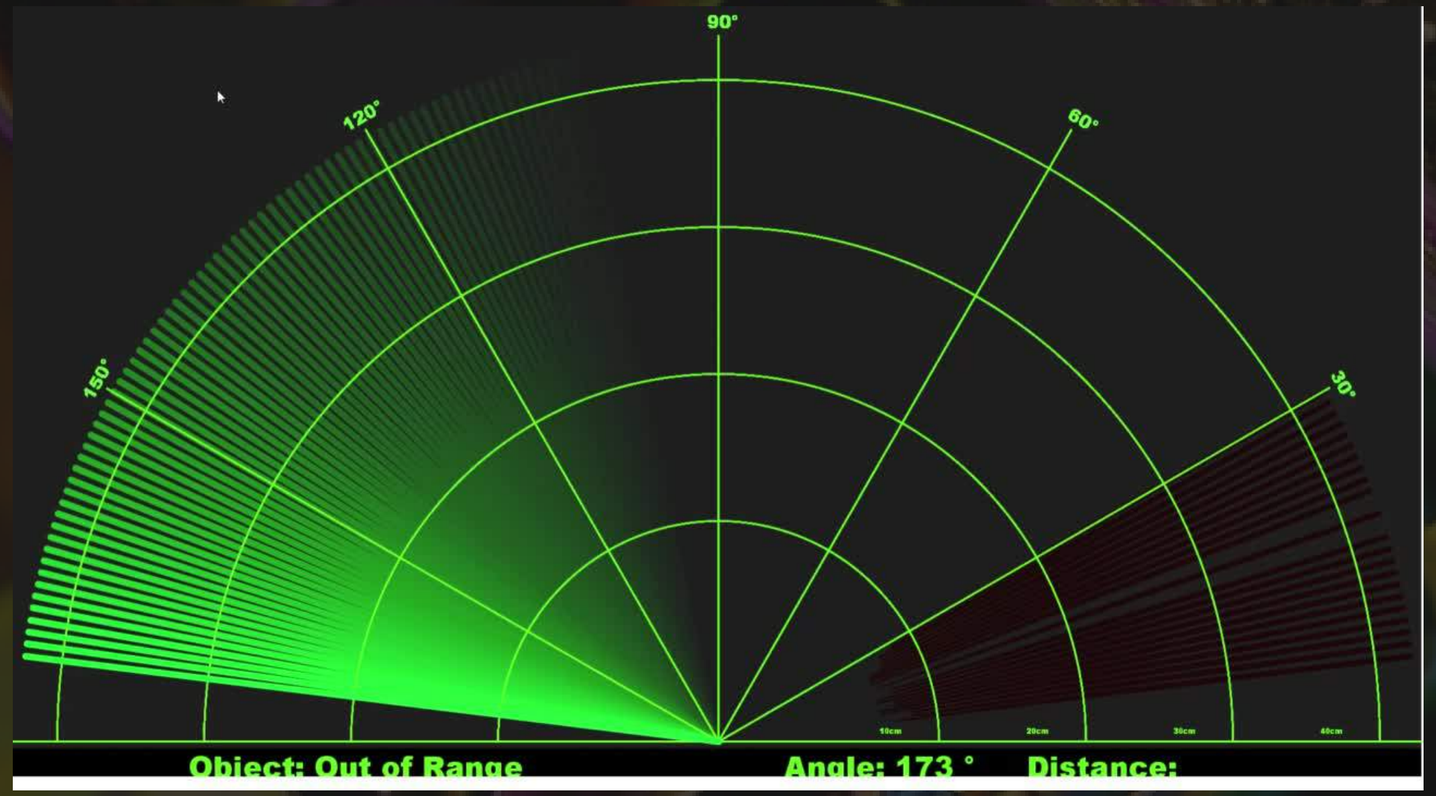


LED Glow's

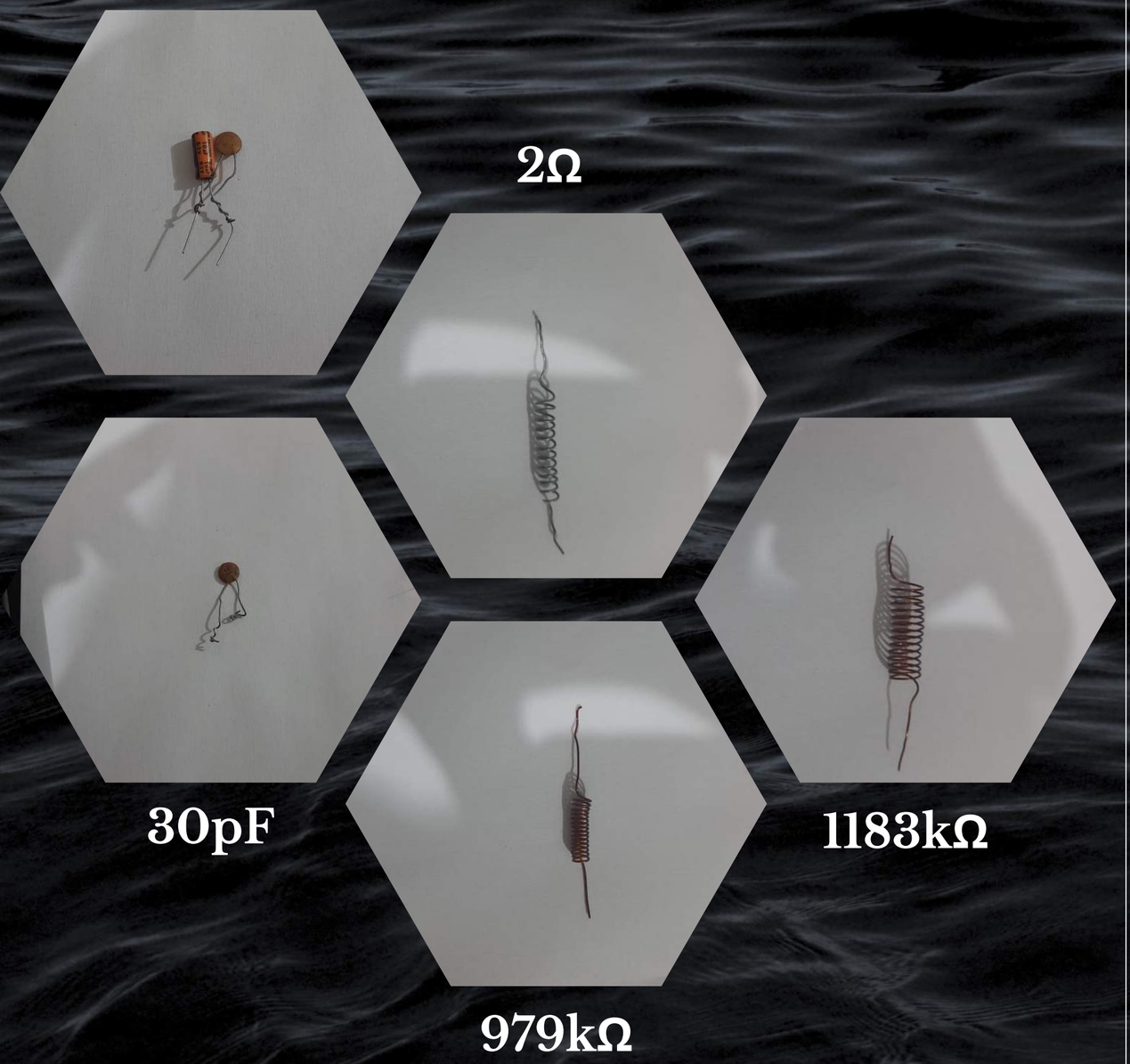


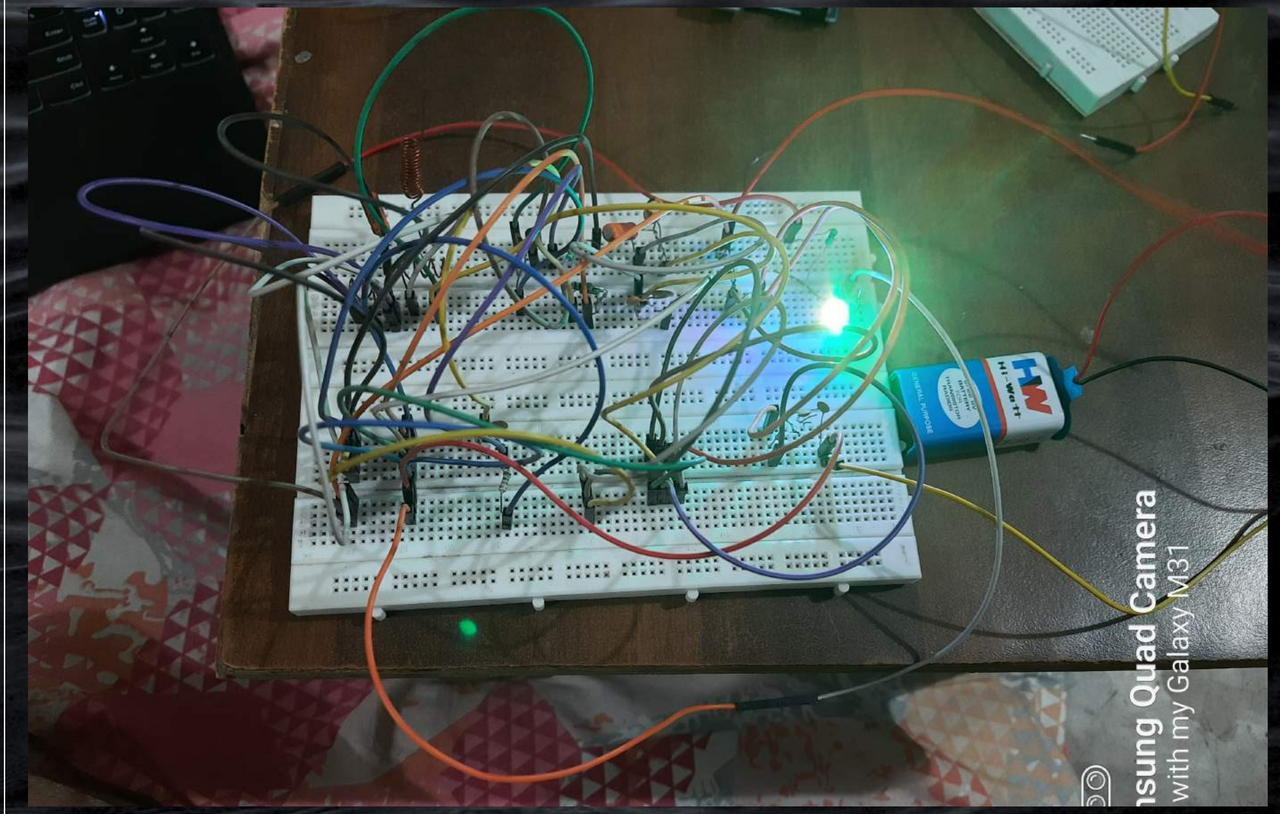
Working Model

Location on Radar



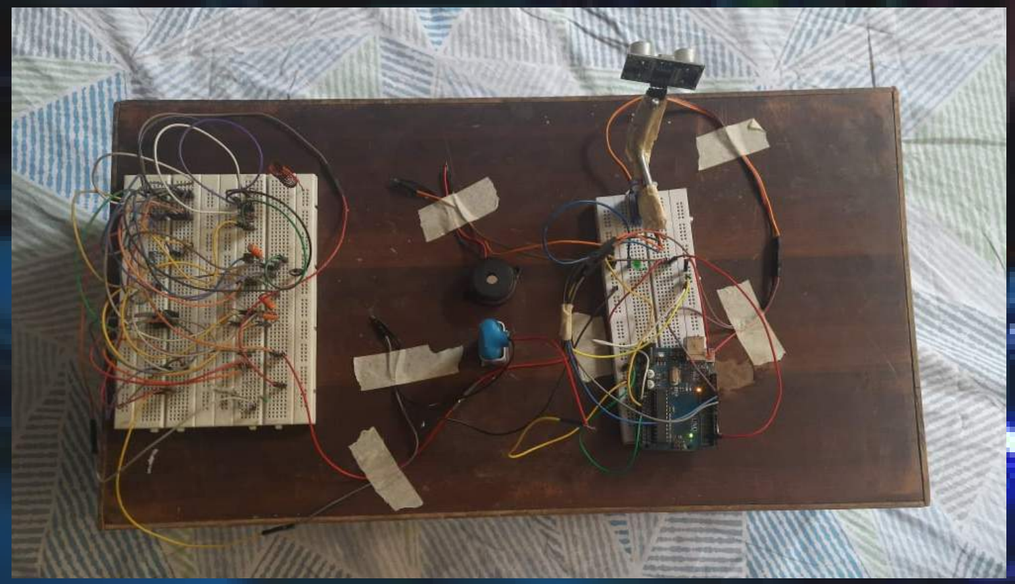
Hardware of jammer Circuit



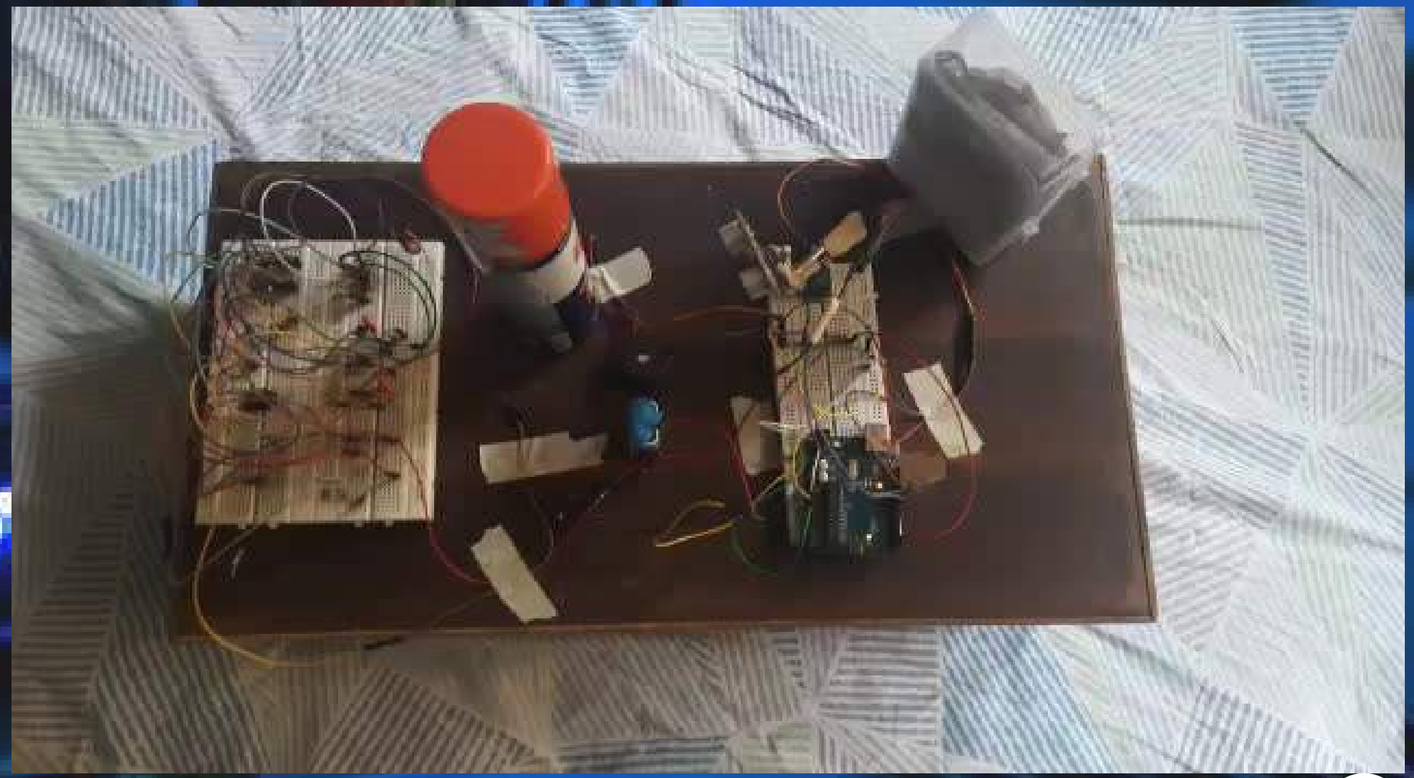


Full Hardware Model

Photo-



Working Video-



Results

The followings things are achieved.

- The radar model is working properly as it is showing location distance as well as angle on the radar.
- The ultrasonic sensor is sensing properly and whenever any object is detected, the buzzer starts buzzing and the LED starts glowing.
- For jammer we have applied the knowledge and about 99 percent work is completed for jammer , but due to some problems in antenna we are not able to complete it.
- We have used certain combination of antennas and collector capacitors for the proper functioning of the jammer as mentioned earlier.

We will be able to develop such mechanism for our military forces that will give them an opportunity to advance their mechanism and their power would be enhanced to reduce casualties.

Future Work

For the further advancement of the project we can

- Use the NIGHT VISION cameras for the proper identification of the enemy
- We can also use the enemy detection and auto firing system

- LIDAR can be implemented in this model. It uses the light technology to measure the distance between the object or in another way we can say that it is used in the range finding Applications(Range-1-200m)

The study of various defense mechanisms is very much important for future research study of several security attacks. The project deals with designing a simple and low cost System will be able to maintain itself i.e. if any problem occurs it will automatically notify the technician according to the Maintenance requirement, without the interference of the user thereby Enhancing Product Quality and Customer Service.

Individual Contribution

S. No.	Name	Reg. No.	Individual Contribution
1	Manas Goyan	19BEC10009	Planning, Designing and assembling of Circuit, Coding, Marinating records of Expenditure, Implementation on hardware(Practically) as well as software, Assisted other team members with the technical aspects of Project.
2	Shikha Saraswat	19BEC10012	Documentation making & Q/A
3	Rishu	19BEC10018	Findings on technical aspects, Presentation making, Report making
4	Neha Rani	19BEC10021	Findings on technical aspects, Presentation making, Report making
5	Ashutosh Pathak	19BEC10022	Planning, Findings in technical as well theoretical aspects , Coding, Implementation on software, Assisted other team members with the technical aspects of Project.

Note: Beside knowing the technial aspects by each member, it has been decided that all the members of team will be making there own model also.

References

[1] A Mohanty, Prabhudutta, et al., “SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY”, Journal of Theoretical & Applied Information Technology 13 ,2010.

[2] Li Xiaoping. Intrusion prevention system research and design. Microcomputer information, 22,2006.

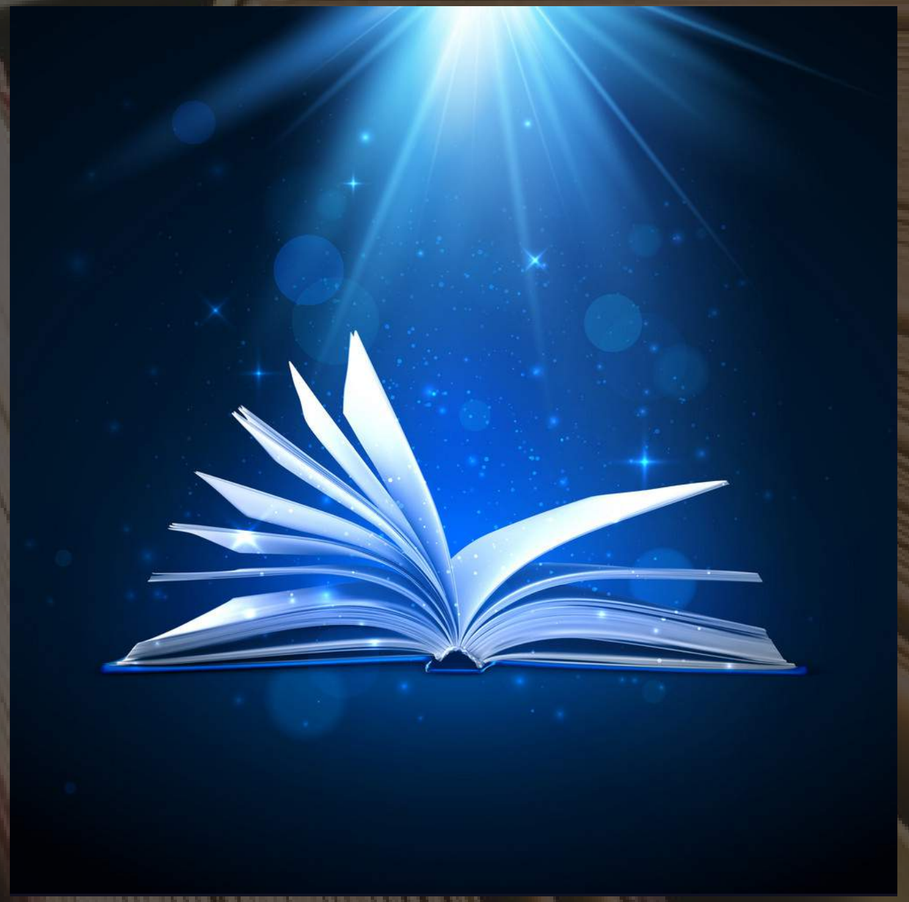
[3] Rawat, Danda B., ed. “Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications”, IGI Global, 2013.

[4]Anil M. Hingmire, “Enhancing Security of Wireless Sensor Network”, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

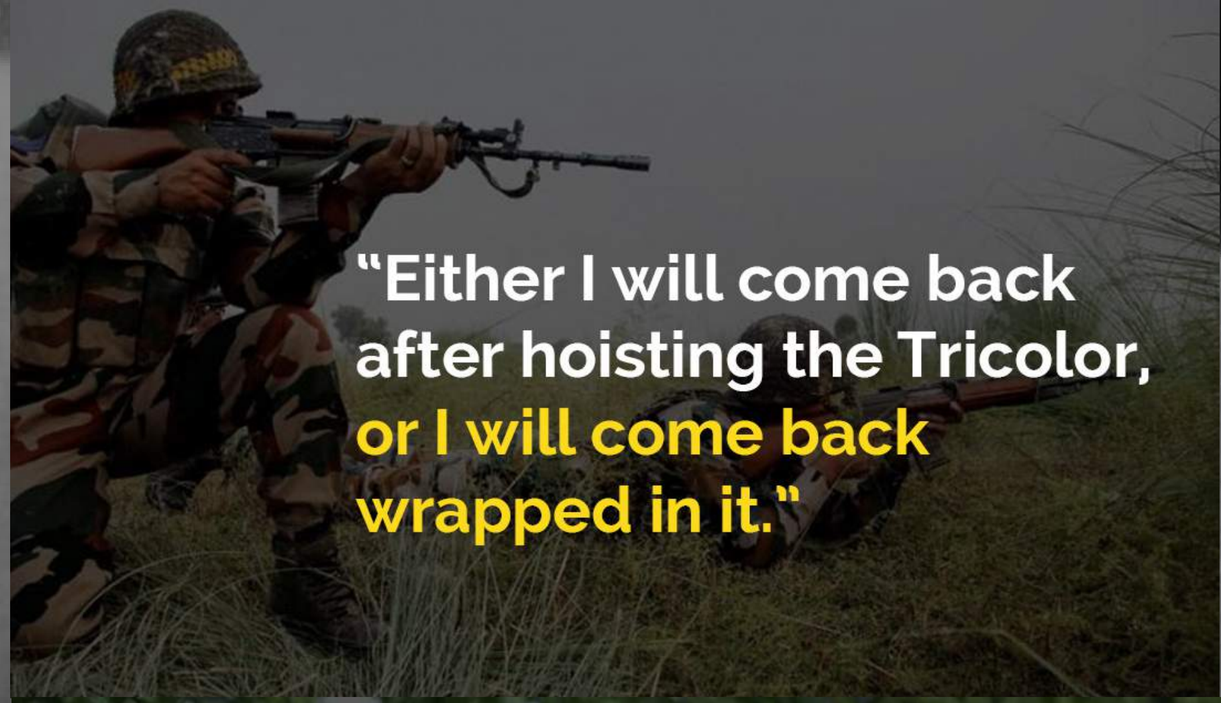
[5] Singh, Shio Kumar, M. P. Singh, and D. K. Singh, “A survey on network security and attack defense mechanism for wireless sensor networks”, International Journal of Computer Trends and Technology 1.2 ,2011.

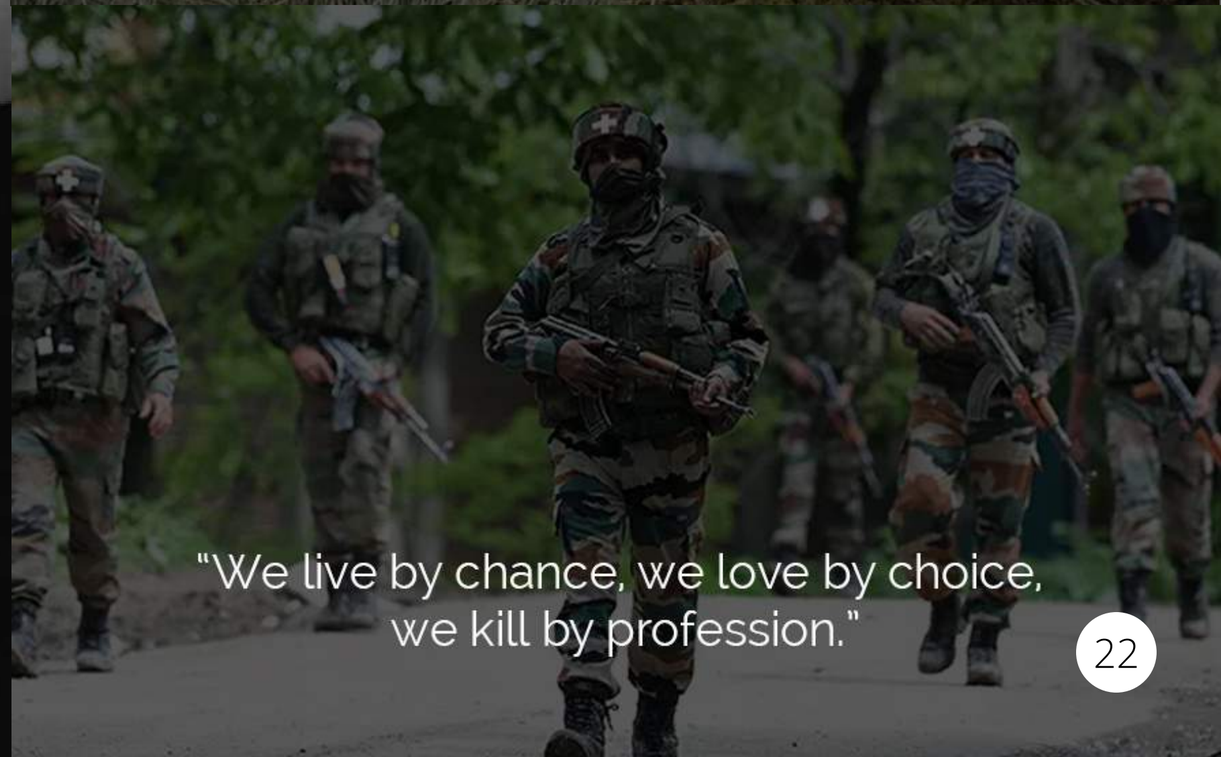
[6]Shafiei, Hosein, et al. “Detection and mitigation of sinkhole attacks in wireless sensor networks”, Journal of Computer and System Sciences, 80.3 ,2014.

[7] Butani, Bhavana, Piyush Kumar Shukla, and Sanjay Silakari, “An Exhaustive Survey on Physical Node Capture Attack in WSN”, International Journal of Computer Applications 95.3 ,2014.



Thank you


"Either I will come back
after hoisting the Tricolor,
or I will come back
wrapped in it."


"We live by chance, we love by choice,
we kill by profession."