Geo fencing for low flying objects

Mentor: Dr. Manish Kumar Bajpai || Co mentor: Dr. Trivesh Kumar

Team: **B. Chandra Haas || B. Rakesh || B. Sharath Naik || S. Sri Harsha || P. Rohith**

Note : All the sentences in red and italic are cited and hyperlinked.

Field study:

In today's rapidly changing world , low flying objects such as drones are a huge threat to security. During their early stage of development, drones were very expensive and were out of public reach. As technology evolved, they became dirt cheap and are available for public use very easily. This is a major security and privacy threat to the nation as well as the general public.In 2015, a recreational drone flew into one of the most secure places, the White house. One of the Defense personnel said "*The Defense Department typically scrambles fighter aircraft for aerial threats over Washington, but when it gets to a toy, that's not something the military typically addresses."* This has also raised serious questions of use of drone by unethical and terrorist orginizations in the nation border.

So we have realized that having a defensive shield against these drones is the need of the hour. Immobilizing commercial drones used for unethical purposes across the borders is the main motive of our project. We will be developing, testing and fine tuning a cost effective, accurate way to stop a drone into a predefined boundary. Essentially we will be creating a virtual fence around the objective area and we will be enforcing jamming signals to prevent drones and other small sized UAVs from entering a restricted area.

Data Analysis & Concept Generation::

After a good time and efforts into research, we have understood that most commercially available drones work in two frequency bands i.e, **2.4 GHz & 5.8 Ghz.** We will be designing a **jamming system** that will block and scramble the signals in one of these frequency bands so that the communication between the pilot and the drone is lost therefore immobilizing the drone.

We will be introducing noise to the **2.4 Ghz** frequency that will disrupt the communication link between the controller and the drone. To create a student grade prototype we will be using off-the shelf products. We will be using an **AV transmitter(2.4 GHz)** to send out **White noise** signals into the airspace. We would be using an **RF amplifier** and a **gain antenna** to increase our range of jamming and to increase the efficiency of our jammer. Our expected Range would be **20-25 meters** of omnidirectional blockage.

Also, before making this prototype , to test our theory , we would be making a small range jammer using **Arduino Uno** and **Nrf24l01 Rx/Tx** module. This would give us a greater idea on how our final prototype would work in the real world.

Now, the technical specifications of various drones collected is given below:

Brand	**Frequency**
DJI Phantom	2.4 GHz / 5.8 GHz
Futaba	2.4 GHz
Spektrum	2.4 GHz
JR	2.4 GHz
Hitec	2.4 GHz

Graupner	2.4 GHz
Yuneec	2.4 GHz
Parrot AR2	2.4 GHz
Immersion	433 MHz

Frequencies used by Popular Drone Brands

We can clearly observe that most drone brands use the 2.4 Ghz band to communicate. This is directe inference that our jammers efficiency would be greater if it jams in this band. However more advanced and pricey drones send a video feed to the controller that helps the controller to check out the environment in the drones airspace. This causes a greater threat as it would not only be used for illegal payload delivery , but also a recon and surveillance drone. So further research was done to know the video feed frequency of drones.

Brand	**Frequency**
DJI	2.4 GHz
Immersion	2.4 GHz
Yuneec	5.8 GHz
Connex	5.8 GHz
Boscam	5.8 GHz

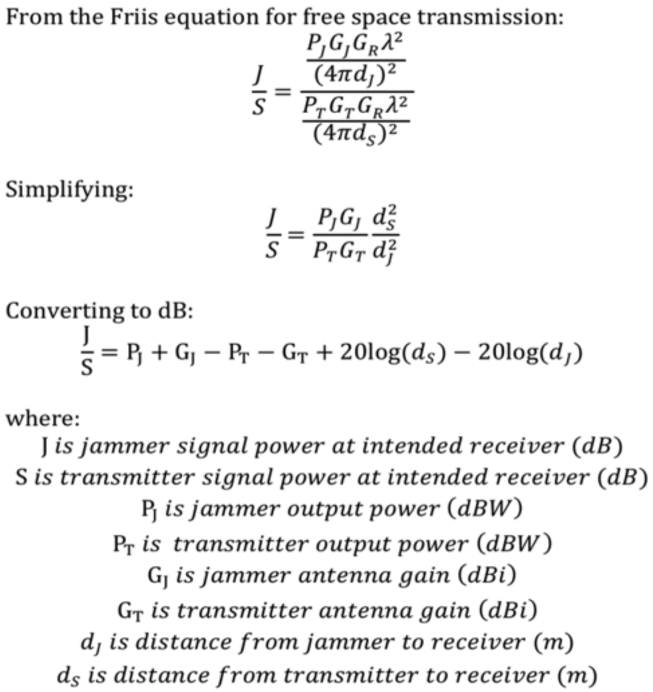
Frequencies used for Video by Common Drone Brands

So from the observations and a lot more research we have decided that 2.4 Ghz frequency is used in most cost effective drones that are used to transport drugs, aerial bombs and other illegal items across the border. So our target frequency will be **2.4 Ghz** frequency band. A drone uses this frequency band to communicate between itself and the transmitter (drone pilot remote)

We will be introducing noise to the **2.4 Ghz** frequency that will disrupt the communication link between the controller and the drone. To create a student grade prototype we will be using off-the shelf products. We will be using an **AV transmitter(2.4 GHz)** to send out **White noise** signals into the airspace. We would be using an **RF amplifier** and a **gain antenna** to increase our range of jamming and to increase the efficiency of our jammer.

Now, to make an efficient jammer , we must know the J/S ratio. J/S the ratio of jamming signal to transmitted signal. J/S is the inverse of S/N, with jamming noise J replacing more typical environmental noise N.most transceivers need S/N ratios of several dB to work tolerably, even a J to S of one (0 dB) can effectively disable the receiver's ability to decode the signal.

Equations that govern the J/S ratio are:



From the Friis equation for free space transmission:

$$\frac{J}{S} = \frac{\frac{P_J G_J G_R \lambda^2}{(4\pi d_J)^2}}{\frac{P_T G_T G_R \lambda^2}{(4\pi d_S)^2}}$$

Simplifying:

$$\frac{J}{S} = \frac{P_J G_J}{P_T G_T} \frac{d_S^2}{d_J^2}$$

Converting to dB:

$$\frac{\mathrm{J}}{\mathrm{S}} = \mathrm{P_J} + \mathrm{G_J} - \mathrm{P_T} - \mathrm{G_T} + 20\log(d_S) - 20\log(d_J)$$

where:

J *is jammer signal power at intended receiver* (dB)

S *is transmitter signal power at intended receiver* (dB)

$\mathrm{P_J}$ *is jammer output power* (dBW)

$\mathrm{P_T}$ *is transmitter output power* (dBW)

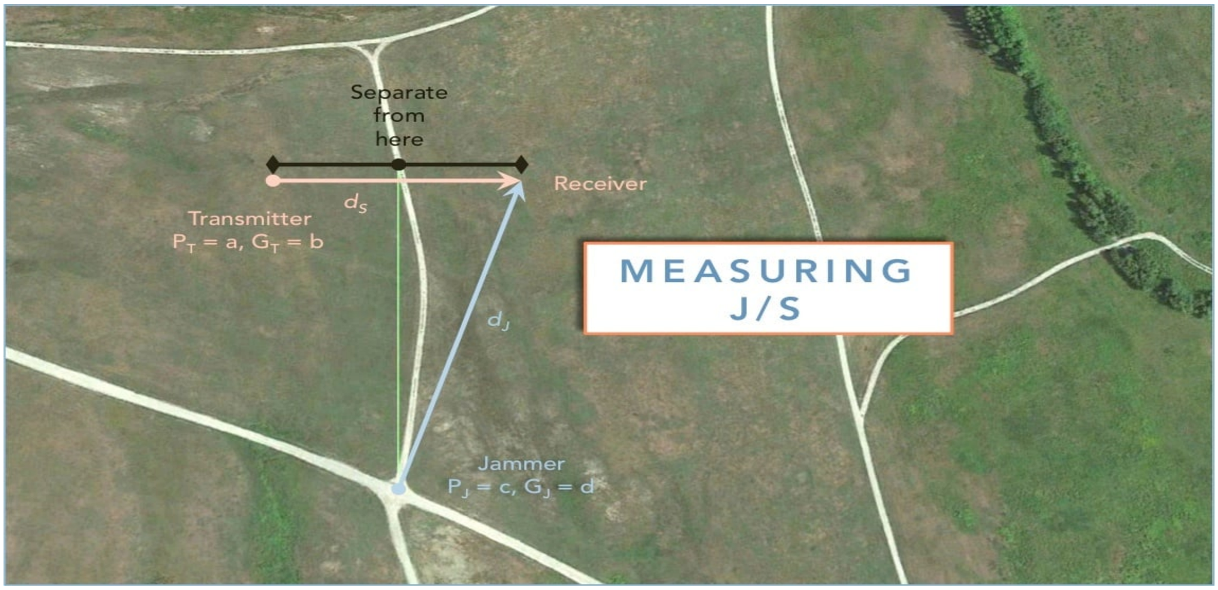
$\mathrm{G_J}$ *is jammer antenna gain* (dBi)

$\mathrm{G_T}$ *is transmitter antenna gain* (dBi)

d_J *is distance from jammer to receiver* (m)

d_S *is distance from transmitter to receiver* (m)

J/S equation



Visualization of J/S calculation

But in real world scenarios , 6dB J/S would have high efficiency to jam out the signal. We will be using a barrage jamming technique to block the signal.The simultaneous jamming of several frequencies or adjacent channels is barrage jamming. All the jammer's power is spread out over a larger portion of the frequency spectrum or band width.It is the simplest form of interference caused by a jammer that transmits noise-like energy throughout the portion of the spectrum occupied by the target. It essentially increases the noise level in the receiver, making it difficult to operate the communication system.

This equation gives us a clear idea of position vs J/S and possibility of jamming. To study about the power of transmitted signal at receiver i.e the drone, we will use the free path loss equation

i.e, $$FSPL\ (dB) = 20log(d) + 20log(f) + 20log(4\pi/c)$$

Where d is the distance from the receiver in Km , f is the frequency in GHz , c is the speed of light.

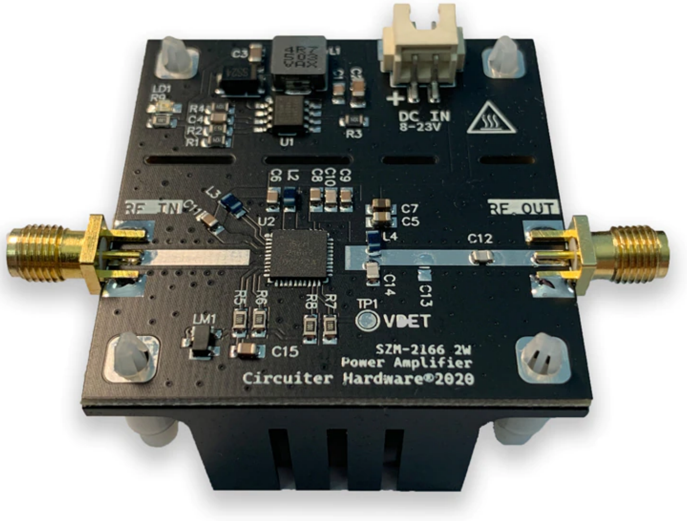
As we don't have a drone for testing yet , we have taken the data from the internet. The most common drone controller has a power of 20 dBm . The total power at that particular distance will be FSPL subtracted from the power of the drone controller.

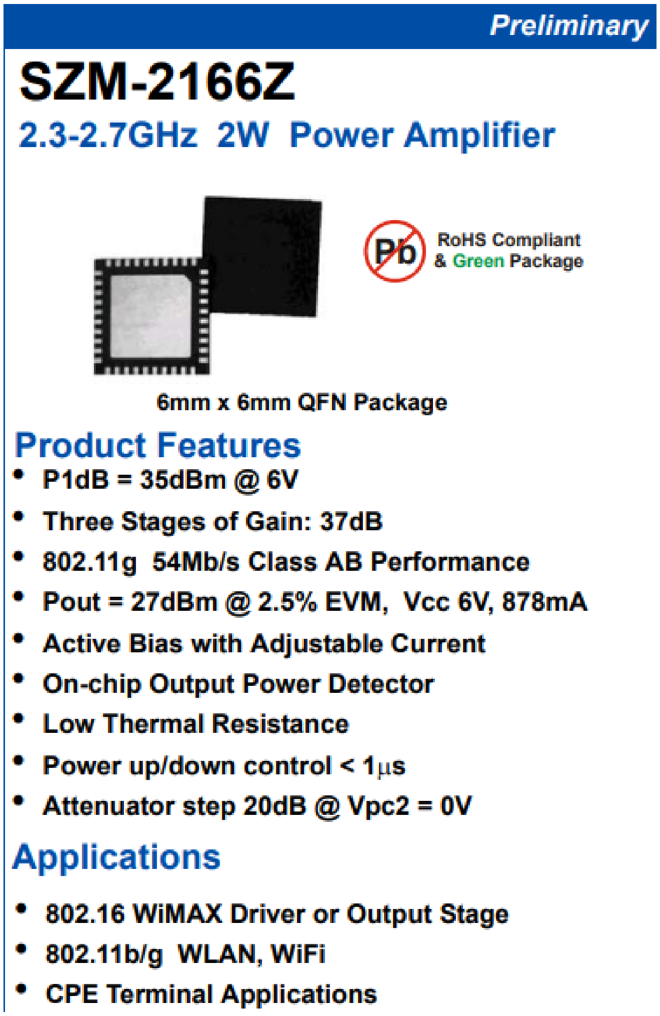
Distance	***Power in dBm***
10	-40.1

20	-46.1
50	-54
100	-60.1
250	-68

Power at various distances @ Drone controller

For an ideal approach we will use a 2W amplifier. The transmitter will transmit a 450mW signal. The gain will be **35 dBm** according to the product specifications. For the time being and for simplicity, we will be using a **15dbi** gain omni directional antenna. So power transmitted by the jammer according to the J/S equation, theoretically , will be **50 db**.





Preliminary

SZM-2166Z

2.3-2.7GHz 2W Power Amplifier

Pb
RoHS Compliant
& Green Package

6mm x 6mm QFN Package

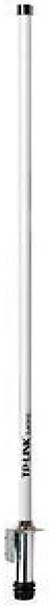
Product Features

- P1dB = 35dBm @ 6V
- Three Stages of Gain: 37dB
- 802.11g 54Mb/s Class AB Performance
- Pout = 27dBm @ 2.5% EVM, Vcc 6V, 878mA
- Active Bias with Adjustable Current
- On-chip Output Power Detector
- Low Thermal Resistance
- Power up/down control < 1µs
- Attenuator step 20dB @ Vpc2 = 0V

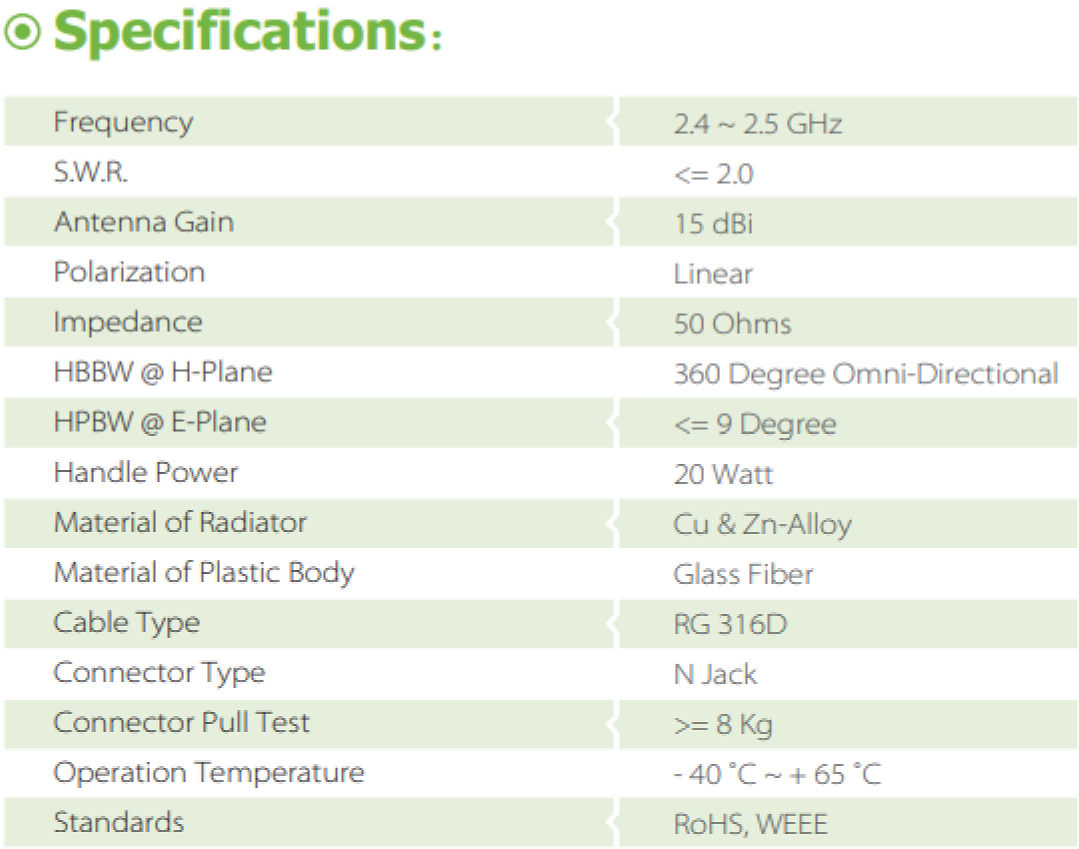
Applications

- 802.16 WiMAX Driver or Output Stage
- 802.11b/g WLAN, WiFi
- CPE Terminal Applications

Power amplifier and its specifications

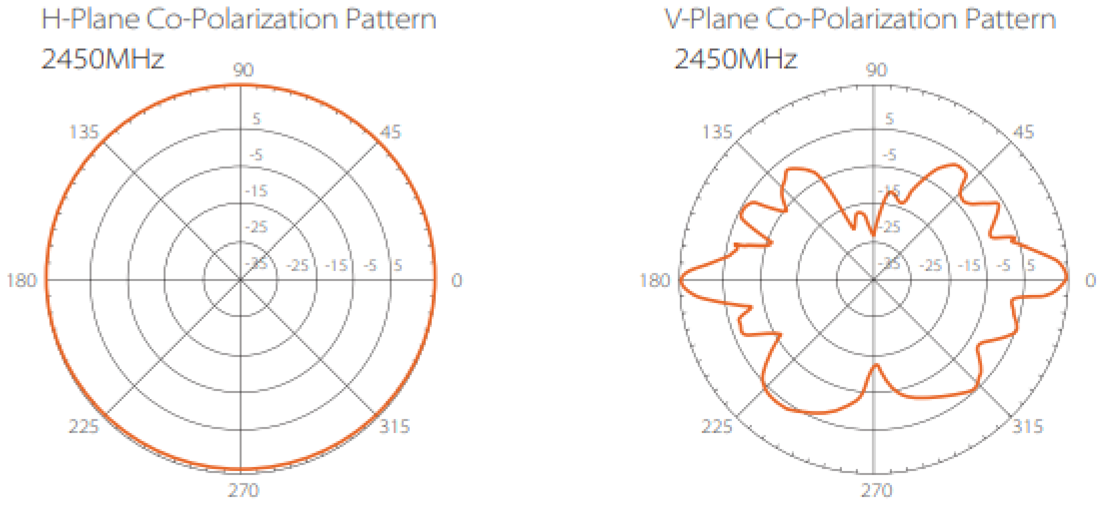


TL-ANT2415D Antenna and its specifications below

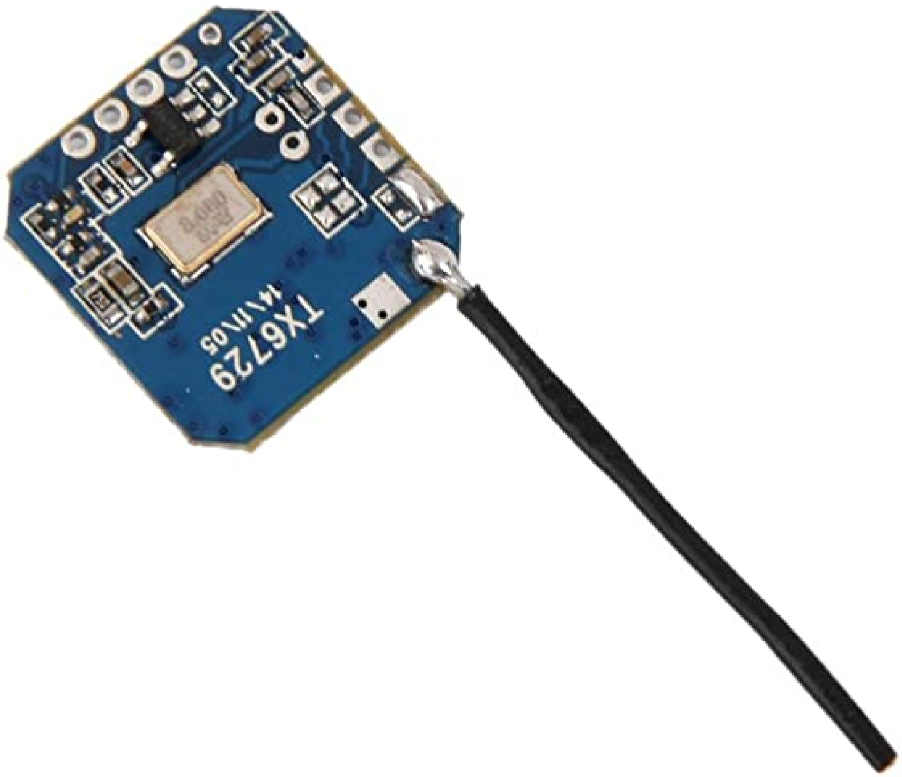


⊙ Specifications:

Frequency	2.4 ~ 2.5 GHz
S.W.R.	<= 2.0
Antenna Gain	15 dBi
Polarization	Linear
Impedance	50 Ohms
HBBW @ H-Plane	360 Degree Omni-Directional
HPBW @ E-Plane	<= 9 Degree
Handle Power	20 Watt
Material of Radiator	Cu & Zn-Alloy
Material of Plastic Body	Glass Fiber
Cable Type	RG 316D
Connector Type	N Jack
Connector Pull Test	>= 8 Kg
Operation Temperature	- 40 ˚C ~ + 65 ˚C
Standards	RoHS, WEEE



Polarization pattern of the antenna



A/V transmitting module

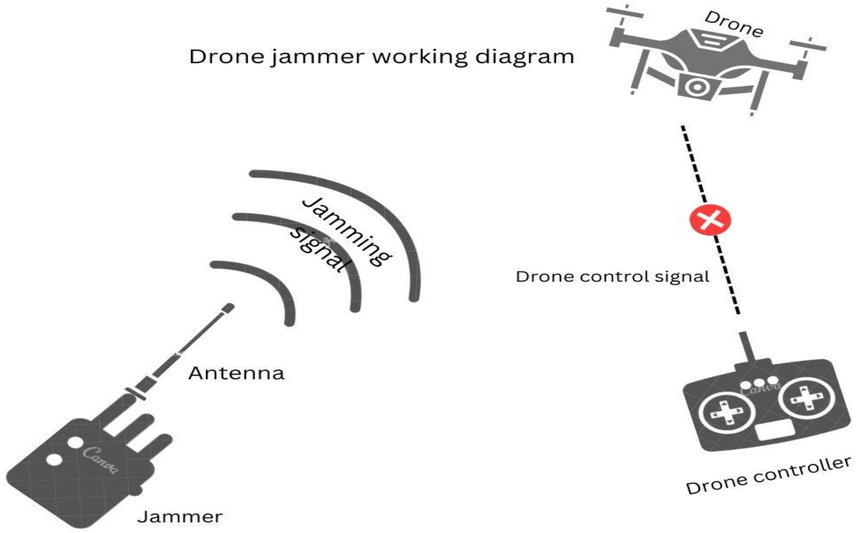
Now, the power vs distance table for the jammer will be:

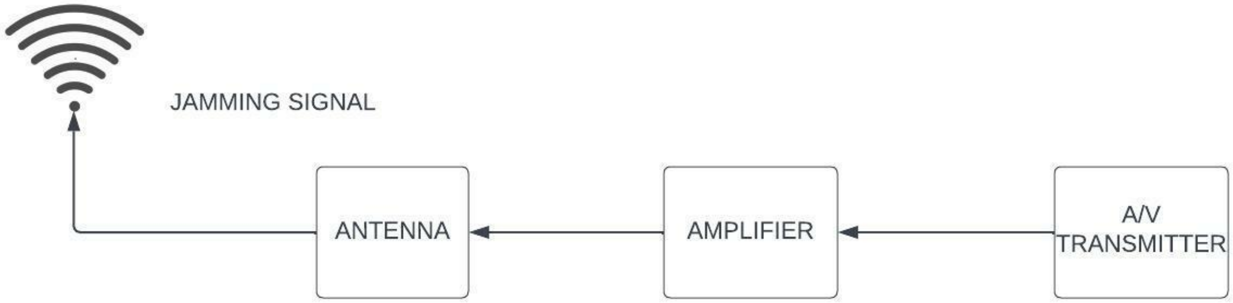
Distance	*Power @ Jammer in dBm*
10	-10.1
20	-16.1
50	-24
100	-30.1
250	-38

Power at various distances @ Jammer

Note that at all equal distances the difference between the jamming signal & drone controller transmitted signal is 30 dB. This is greater than our threshold value of 6dB. So theoretically our jammer would successfully block out signals transmitted from the drone controller very easily.

To increase our range furthermore , we can use highly directional antennas that give us higher gain as increasing the power from the amplifier would require costly equipment and a cleaner voltage source to power the amplifier.





Block Diagram of generation of jamming signal

Product Specifications:

For small range prototype:

- Arduino Uno
- Nrf24l01 Rx/Tx
- Gain antenna

For student grade prototype:

- **AV transmitter (**preferably XLT24017)
- **RF amplifier** (preferably that has output greater than 8 Watts and less than 10W, as anything above 10 W will be requiring a Ham Radio license)
- **Gain Antenna (**preferably a 15 dbi gain, omnidirectional)
- **SDR** (preferably HackRFOne , as its compatible with our target frequency)
- **Drone** for testing (works in 2.4 GHz frequency)

Progress:

- Have completed detailed analysis on the working of the drone communication system and the use of their 2.4 GHz band.
- After a lot of brainstorming and iteration rejection, we have decided to use Jamming using the Noise principle. We have also had thoughts of using EMP , using detection of drones using Computer Vision for greater accuracy and efficiency. But this would take monumental time and effort and this would hinder the timeline of the EDP project.
- Ready to make the testing prototype using Arduino Uno and Nrf24l01 Rx/Tx module. Will start this very shortly and would be getting a greater idea on our theory. Will help us to fine tune and make the changes required in our final prototype.
- Are currently working on using directional antennas such as horn antennas to give us more range. Understanding the radiation pattern and their decrease of gain with distance.
- Also working on the arrangement of antennas for optimal jamming of the signal in order to eliminate any kind of dead zones that may appear where the drone can pass through.