Commercial drones and radio-controlled aircraft are of increasing concern, with commercial airlines afraid of collision and property owners worrying that their privacy is being invaded.

The main problems faced are-

1. Signal interference-

The distortions in the propagation of radio waves are due to various factors like noise of other waves.

1. Signal strength weakening-

The obstacles, unwanted climatic conditions and range have a drastic effect on the strength of the signal strength.

3. Obstacles met at the time of returning of UAV.

4. Hijacking and Hacking for illegal activities.

**An overview of the problems faced by drones is listed as follows :-**

**Hijacking** – Wi-Fi hijacking has been proved successful through the use of de-authentication attacks which break to communications between the UAV and controller and establishes a new connection with the attacker.

**Spoofing** – RF or GPS spoofing techniques can be used to relay false information to a UAV.

Another risk is the possibility of hijacking or jamming a drone in flight. In recent years several security researchers have made public vulnerabilities for these flying machines. In some cases even providing full source code or tools to play their attacks.

We have implemented a dual circuit system in the drone.

The solution of ours include-

1. The drone will return home if the signal is lost or in case if it is hacked or hijacked.
2. There two circuits in the drone- Primary and Secondary.
   1. The Primary Circuit consists of a GPS module used for navigation, Opamp to be used as a comparator for desired and the actual signal, Amplifier used for signal strengthening.
   2. Secondary circuit consisting of a Radio Wave Transmitter and Receiver and Motion Sensors.
3. The signal for the drone will have a predefined range. It will be amplified if it falls below a certain value. If there is a further decrease in its strength, in that case, drone will return back home.
4. The data in the drone will have end to end encryption (cryptography) to avoid the possibilities of hacking.
5. The drone distinguishes whether it has lost the signal or it has been landed by the user by checking the status of the throttle when the transmitter shuts down. The secondary circuit will come into play when the transmitter has shut down but the throttle is not zero.
6. If the signal is hacked or hijacked, such that its IP address gets changed due to change in the controlling server, then the primary circuit will be deactivated and the control will be done by the secondary circuit only.
7. If the drone is hijacked by some external means such that it's controlling server remains same, then the on-board motion sensors will detect the deviation of drone from the desired path and primary circuit will cut off.
8. The radio wave transmitter in the secondary circuit will generate the R.F. pulse to be reflected by the nearby base stations, the drone will head towards the base station having the smallest return time.
9. The frequency of generation of this pulse would be inversely proportional to the distance from the base station, which can be estimated by noting the return time of the previous pulse, i.e., the pulses will be generated more rapidly as the drone approaches the base station.

This distance dependency of the pulse generation serves a triple point purpose of randomising the pulse receiving operation thus eliminating the possibility of external interference, increasing the battery life of the drone and also increasing the precision by which the base station is located.

1. To avoid obstacle during the return, the on-board motion sensors (ultrasonic) will be used as Inertial Navigation System.