ANTI DRONE SYSTEM

SUBMITTED TO:

Mohd Alam

SUBMITTED BY:

Sushant Singh (20103122)

INDEX

INTRODUCTION

In the past several years, India has been seeing more use of drones—or small unmanned aerial vehicles (UAVs)—for various military and civilian purposes. These include reconnaissance, imaging, damage assessment, payload delivery and as seen recently amidst the COVID-19 pandemic, for contact-less delivery of medicines.

Nevertheless, the prevalent use of drones poses great threats to public security and personal privacy. For example, an attacker might strap explosives or other dangerous materials to a drone to carry out an attack; criminals can use drones to smuggle illicit materials across the border; an operator can control a drone carrying a high-fidelity camera to fly over walls and spy inhabitants' private information. The increasing frequency of incidents caused by drones makes it necessary to regulate drone air traffic. Analysts warn that as Unmanned Aerial Systems (UAS) become less expensive, easier to fly, and more adaptable for crime, terrorism or military purposes.

Therefore, it is of great significance to deploy an anti-drone system in a security-sensitive area. Such an anti-drone system is able to detect the drone at the time it flies into the sensitive area, and estimate its location for drone defence, e.g., jamming, hunting or control of the detected drone.

DRONE MONITORING EQUIPMENTS

Drone monitoring equipment can be passive (simply looking or listening) or active (sending a signal out and analysing what comes back) and can perform several functions, including:

1. **Detection:** Detection means the technology that is able to detect drones. Detection alone usually isn't enough though. Radar that detects drones may also detect birds, for example: That's why classification is useful.
2. **Classification and Identification:** Technology that classifies drones will usually be able to separate drones from other types of objects - like planes, trains, and automobiles, for example.
3. **Identification:** One step further is identification. Some equipment can identify a particular model of drone, or even identify the drone's or controller's digital fingerprint, like a MAC address for example. This level of identification can be handy for prosecution purposes.
4. **Alerting, Location and Tracking:** Being alerted that a drone is present somewhere in the vicinity is already useful. But your situational awareness and ability to deploy countermeasures is greatly enhanced if you know the drone's (and/or the controller's) exact location. Some equipment will even allow you to track the drone location in real-time.

TYPES OF DRONE MONITORING EQUIPMENTS:

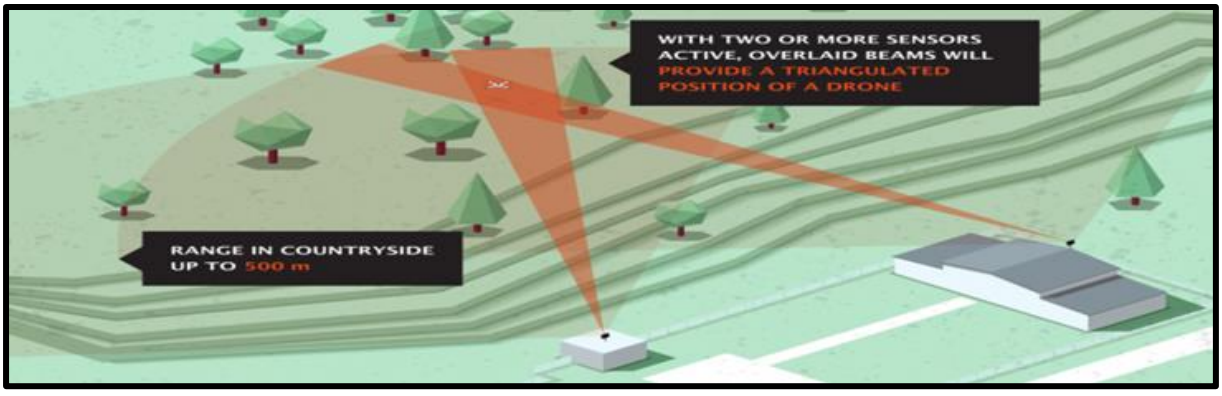
There are four main types of drone monitoring equipments:

1. Radio Frequency (RF) Analysers
2. Acoustic Sensors (Microphones)
3. Optical Sensors (Cameras)
4. Radar

1) Radio Frequency (RF) Analyzer

RF Analysers consist of one or more antennas to receive radio waves and a processor to analyse the RF spectrum. They're used to detect radio communication between a drone and its controller. Some systems are able to identify the more common drone makes and models, and some can even identify the MAC addresses of the drone and controller (if the drone uses Wi-Fi for communication). This is especially useful for prosecution purposes – proving that a particular drone and controller were active. Some high-end systems can also triangulate the drone and its controller when using multiple radio units spread far apart.

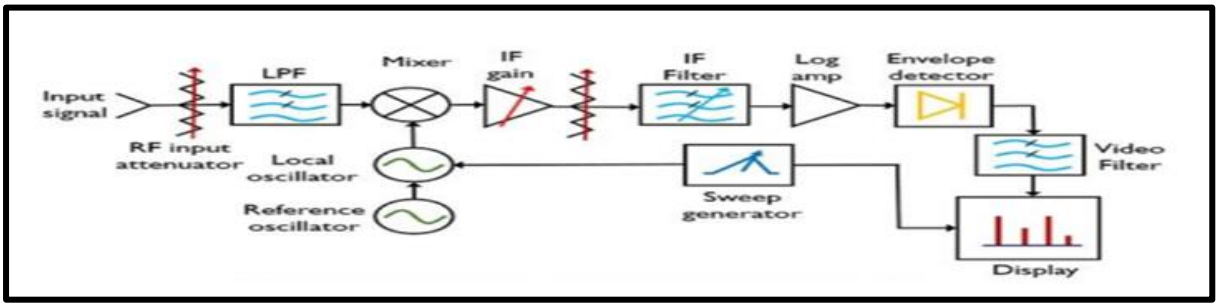
RF Analyzers



Aerial Triangulation of a drone

Components:

- **RF Input Attenuator:** This block serves as the first unit of the spectrum analyzer and is basically used to provide an optimum level signal as the input to the system. This is so because when high broadband signals are supplied to the system then there exist chances of overload, gain compression and distortion.
- **Low pass filter:** It blocks the high-frequency components of the signals and allows only low-frequency components to pass further. Thus by using LPF the out of band signals are not permitted to reach the successive units of the system. This restricts the system to give an unwanted response.
- **Mixer:** It basically acts as a frequency translator and converts one form of frequency into another. The applied input signal and the signal from the local oscillator are the two inputs of the mixer.
  The output frequencies of the mixer are the two applied input frequencies as well as the sum and difference frequencies of the two input frequencies.
- **IF gain:** It is the variable gain amplifier. It is present after the mixer and is used for the adjustment of the vertical position of the signal without altering the signal level of the mixer input.
- **IF filter**: It is basically a band pass filter that is centred at the intermediate frequency. Thus is designed to pass only the desired frequency component.
- **Detector**: Basically analyzer uses a detector so that the IF signal from the IF filter gets converted into baseband or video signal.
- **Video Filter:** This unit acts as an intermediary between the detector and the ADC and is basically a low pass filter. It is used to smoothen the traces that are to be displayed on the screen.
- **Local Oscillator**: This is used to tune the analyzer and is basically a voltage controlled oscillator.



Block diagram of an Analyzer

Pros: Low cost, detects (and sometimes identifies) multiple drones and controllers, no send signal needed - only requires passive sensors which could implicate a simple construction, some can triangulate drone and controller position.

Cons: Directed antennas on commercial drones make it virtually undetectable from the wrong direction, can't detect autonomous drones (without RF-emissions), less effective in crowded RF areas, typically short range.

(2) Acoustic Sensors (Microphones)

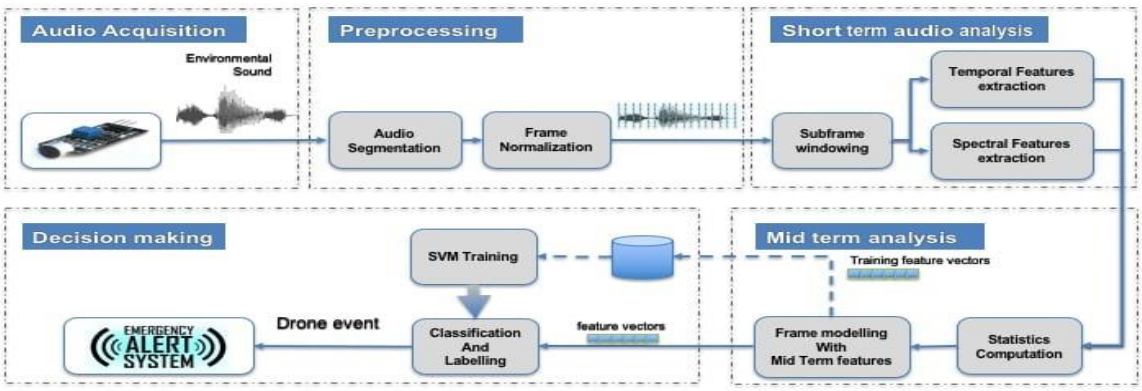
It is usually a microphone, or microphone array (lots of microphones), which detects the sound made by a drone and calculates a direction. More sets of microphone arrays can be used for rough triangulation.

Acoustic Sensor

Components and working:

The "Fast Fourier Transform" (FFT) is an important measurement method in the science of audio and acoustics measurement. It converts a signal into individual spectral components and thereby provides frequency information about the signal.

- **Audio acquisition:** The sounds produced by the surrounding environment are picked up by an audio sensor (microphone array) and converted into a digital format by a sound card.
- **Pre-processing:** Each digital sound segment recorded in a buffer memory is broken into consecutive frames of predetermined duration. This process is called **segmentation**. Then the frames are normalized in the range [-1, 1].
- **Short term analysis:** It aims to reduce the number of features in a dataset by creating new features from the existing ones (and then discarding the original features). These new reduced set of features should then be able to summarize most of the information contained in the original set of features.
- **Mid term analysis:** After analyzing the new set of features, the relative sequences of low level features are processed statistically. The goal is to obtain new salient mid term features with low sensitivity to the small variations of underlying audio signal.
- **Decision making:** UAS detection sensors compare the sound samples of the reduced dataset with the acoustic signatures from the built-in database. If the match is found, the drone acoustic detection system records identifying information and issues an automatic alert.



Block diagram for Acoustic Sensor

- Pros: Detects all drones within the near-field including those operating autonomously, detects drones in the ground clutter where other technologies can struggle, sound travel past some obstacles so great gap-filler in areas outside line-of-sight of other sensors, highly mobile and quickly deployable, completely passive.
- Cons: Doesn't work as well in noisy environments, very short range (max. 300-500m).

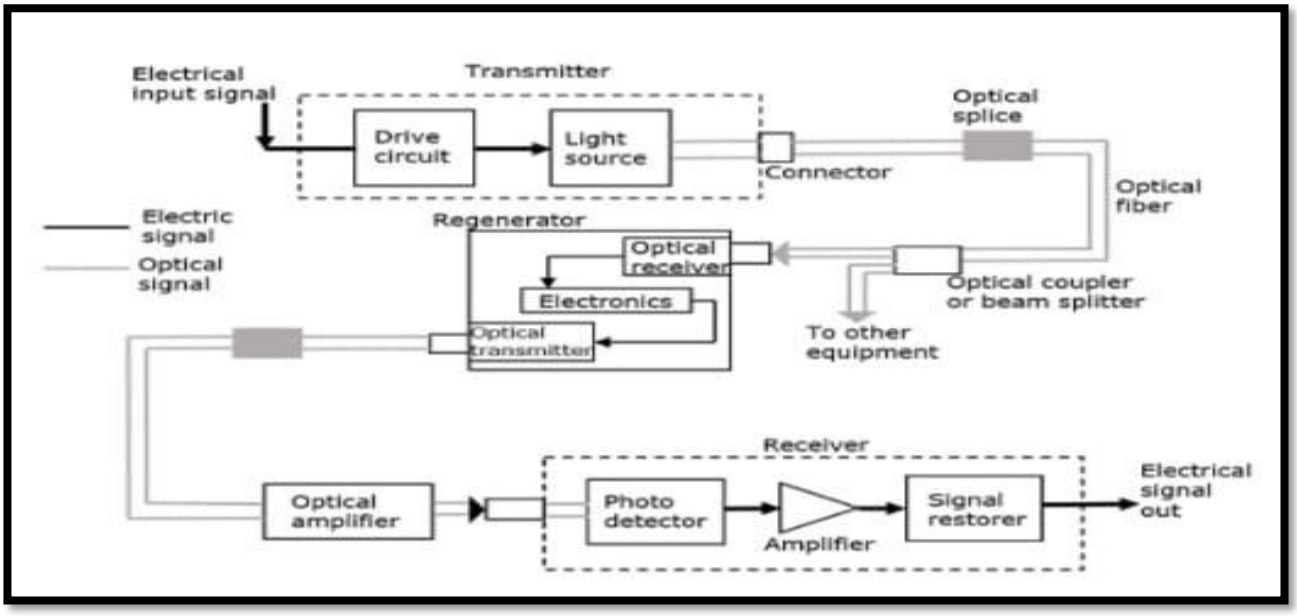
(3) Optical Sensors (Cameras)

Essentially a video camera as well as standard daylight cameras, optical sensors can be infrared or thermal imaging. With optical zoom, high resolution sensors and image stabilization the technology offers long range for detection and through recognition software also good basis for classification of targets.

Optical Drone detector System

Components

- **Optical Receiver:** Detects the incoming optical power and extract the signal from it.
- **Optical Fibre:** Used as a medium for long-distance communications.
- **Optical coupler:** A semiconductor device which is designed to transfer electrical signals by using light waves in order to provide coupling with electrical isolation between circuits or systems.
- **Beam-splitters:** Beam-splitters are optical components used to split incident light at a designated ratio into two separate beams. Additionally, beamsplitters can be used in reverse to combine two different beams into a single one.
- **Optical Transmitter:** Converts the electrical signal into optical form, and. launch the resulting optical signal into the optical fiber.
- **Optical Amplifier:** An optical amplifier amplifies light as it is without converting the optical signal to an electrical signal, and is an extremely important device that supports the long-distance optical communication networks.
- **Photo Detector:** Converts light signals into electrical signals.
- **Signal Restorer:** Used to minimise distortion in a signal and determine the true signal.



Block diagram for Optical Sensor

Working Principle

All optical sensors work in almost the same way, as they use a light source (transmitter) and a light detector (receiver) to sense the presence or absence of light. Typically, optical sensors use light-emitting diodes as a type of light source. The oscillating light is sensed by the light detector, and thus the detector captures all the surrounding light rays and searches for the oscillating light.

Optical Sensor

Pros: Provides visuals on the drone, can record images as forensic evidence for use in eventual prosecution.

Cons: Difficult to use for detection by itself, high false-alarm rates, mostly poor performance in dark, fog, etc.

(4) Radar

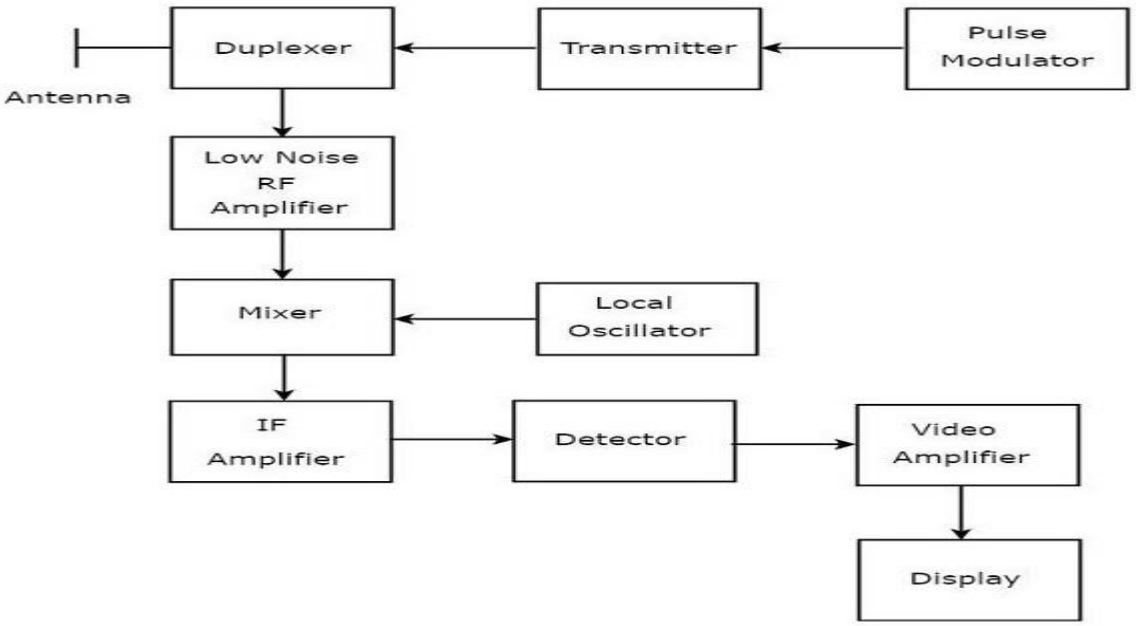
A device which uses radio energy to detect an object is known as Radar. Drone detection radar sends out a signal and receives the reflection, measuring direction and distance (position). Most radars send their radio signal as a burst, and then listen for the 'echo'. Almost all radars are designed to not pick up small targets. They are designed for large object tracking, like passenger aircraft.

Radar

Components

The essential parts of this system include the following:

- **A Transmitter:** It can be a power amplifier like a Klystron, Travelling Wave Tube, or a power Oscillator like a Magnetron. The signal is first generated using a waveform generator and then amplified in the power amplifier.
- **Waveguides:** The waveguides are transmission lines for transmission of the RADAR signals.
- **Antenna:** The antenna used can be a parabolic reflector, planar arrays, or electronically steered phased arrays.
- **Duplexer:** A duplexer allows the antenna to be used as a transmitter or a receiver. It can be a gaseous device that would produce a short circuit at the input to the receiver when the transmitter is working.
- **Receiver:** It can be a super heterodyne receiver or any other receiver which consists of a processor to process the signal and detect it.
- **Threshold Decision:** The output of the receiver is compared with a threshold to detect the presence of any object. If the output is below any threshold, the presence of noise is assumed



Block diagram for Radar

Working Principle

The **radar working principle** is very simple because it transmits electromagnetic power as well as examines the energy returned back to the target. If the returned signals are received again at the position of their source, then an obstacle is in the transmission way. This is the working principle of radar. To measure the range and location of moving objects, the Doppler Effect is used.

Pros: Long range, constant tracking, highly accurate localisation, can handle hundreds of targets simultaneously, can track all drones regardless of autonomous flight, independent of visual conditions (day, night, fog, etc.)

Cons: Detection range dependant on drone size, most do not distinguish birds from drones, requires transmission license and frequency check to prevent interference.

DRONE COUNTERMEASURE EQUIPMENTS

Countermeasures can be grouped as either:

- ✓ Physically destroying the drone
- ✓ Neutralising the drone
- ✓ Taking control of the drone

Types of Drone Countermeasure Equipments:

There are 4 major Drone Countermeasures Equipment:

1) RF Jammers
2) GPS Spoofers
3) High Power Microwave (HPM) devices
4) High Energy Lasers

(1) RF Jammers

As the name suggests, such a device will jam the radio transmissions between the source and the receiver.

RF Jammer Gun

How it works?

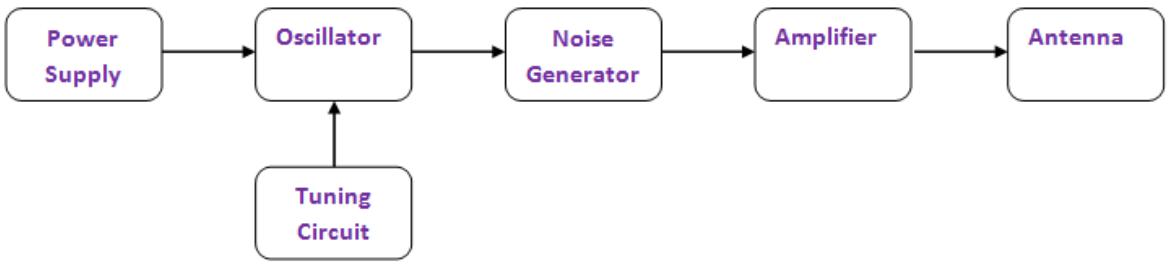
An RF Jammer is a static, mobile, or handheld device which transmits a large amount of RF energy towards the drone, masking the controller signal. This results in one of four scenarios, depending on the drone:

- Drone makes a controlled landing in its current position
- Drone returns to user-set home location (which could be set to a target position instead of home)
- Drone falls uncontrolled to the ground
- Drone flies off in a random uncontrolled direction.

Components

The basic devices present in a cell phone jammer are:

- **Power Supply:** Mobile jammers are battery operated devices.
- **Voltage Controlled Oscillator:** It is used to generate the RF signal.
- **Tuning Circuit:** Controls the frequency at which the jammer produces the RF signal.
- **Noise Generator:** RF signal is made to a specified frequency and made random.
- **RF Amplification:** It boosts the RF signal.
- **Antenna**: Mobile jammer uses an antenna to send the RF signal produced in the jammer.



Block diagram for RF Jammer

Pros: Medium cost, low power consumption, easy to implement, non-kinetic neutralisation (more focused on control of the opponent over outright damage).

Cons: Short range, can affect (and jam) other radio communications, can result in unpredictable drone behaviour, could unintentionally send the drone to its target.

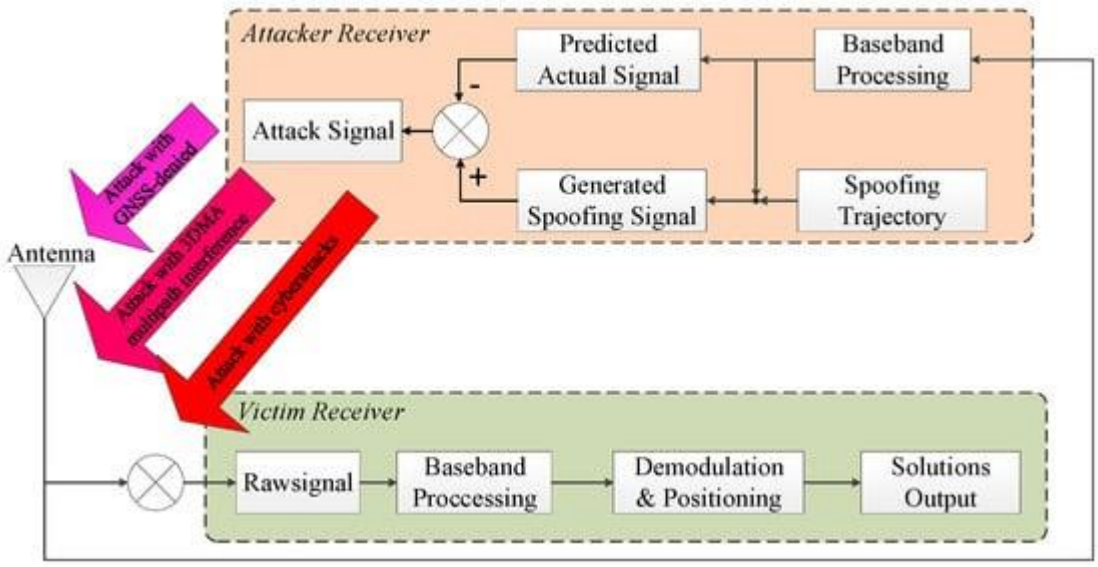
(2) GPS Spoofers

This device sends a new signal to the drone, replacing the communication with GPS satellites it uses for navigation. In this way, the drone is 'spoofed' (tricked) into thinking it's somewhere else. GPS signals are vulnerable to in-band interferences because of being extremely weak broadcasted signals over wireless channels. Therefore, even low-power interference can easily jam or spoof GPS receivers within a radius of several kilometres. By dynamically altering the GPS coordinates in real-time, the drone's position can be controlled by the spoofer. Once control is gained the drone can be directed to a safe zone.

GPS Spoofer

Components

- **Generator:** To detect the actual signal and modify the raw signals by cancelling the actual signal component and adding the spoofing signal component.
- **Radio Transmitter:** To send the spoofed signal to attack antenna.
- **Software Defined Ratio (SDR):** software or firmware, in order to carry out signal processing tasks. SDR only uses an ADC and DAC to do Analog to Digital and Digital to Analog signal conversion along with antennas, without needing many hardware components.
- **Attenuator:** An appropriately selected attenuator to ensure that the spoofed signals do not travel beyond the testing radius.



Block diagram for GPS Spoofer

Working

GPS Spoofing is accomplished by a system capable of mimicking the GPS signals associated with the drones. The GPS transmission power of the fake GPS signals are higher than the real signals, resulting in the receiver locking onto them in favour of the true GPS. A t this point the time shift of the fake signals can be manipulated to tamper with both the position and time reported by the receiver.

Firstly, the generator will track the actual signal synchronously to extract the ephemeris (position) of visible drone, their signal amplitude, and other parameters. Then, the generator will predict the actual signal and generate the cancellation component. At the same time, the spoofing trajectory will be converted to the corresponding spreading code frequency and carrier frequency to generate the spoofing signal component. Finally, the cancellation signal component and spoofing signal component will be combined as the attack signal. The proposed spoofing attack can be launched via a GPS-denied strategy.

Pros: Medium cost, non-kinetic neutralisation, widely available technology.

Cons: Short range, can affect (and jam) other radio communications, hostile drones could be built with robustness for false coordinates.

(3) High Power Microwave (HPM) Devices

How it works?

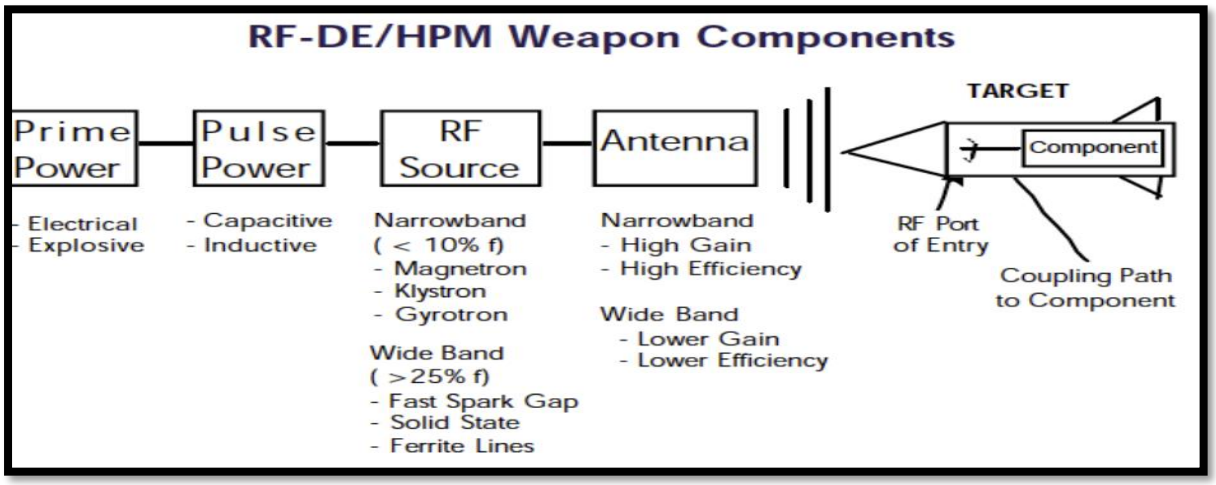
High Power Microwave (HPM) devices generate an Electromagnetic Pulse (EMP) capable of disrupting electronic devices. The EMP interferes with radio links and disrupts or even destroys the electronic circuitry in drones (plus any other electronic device within range) due to the damaging voltage and currents it creates. HPM devices may include an antenna to focus the EMP in a certain direction, reducing potential collateral damage.

High Power Microwave

Components

The HPM source is composed of:

- **HPM Source:** Impulsive sources and linear beam sources are used to generate microwave energy.
- **High voltage pulse generator:** It is used for generation of gigawatt microwave radiation pulses
- **Vacuum tube:** Used for amplification of microwave signals.
- **Wave guide:** Used to transfer radio frequency to the antenna.
- **Antenna:** Used for radiating microwave signal into space.



Block diagram for HPM

Pros: Appreciable range, the drone can be stopped effectively, non-kinetic.

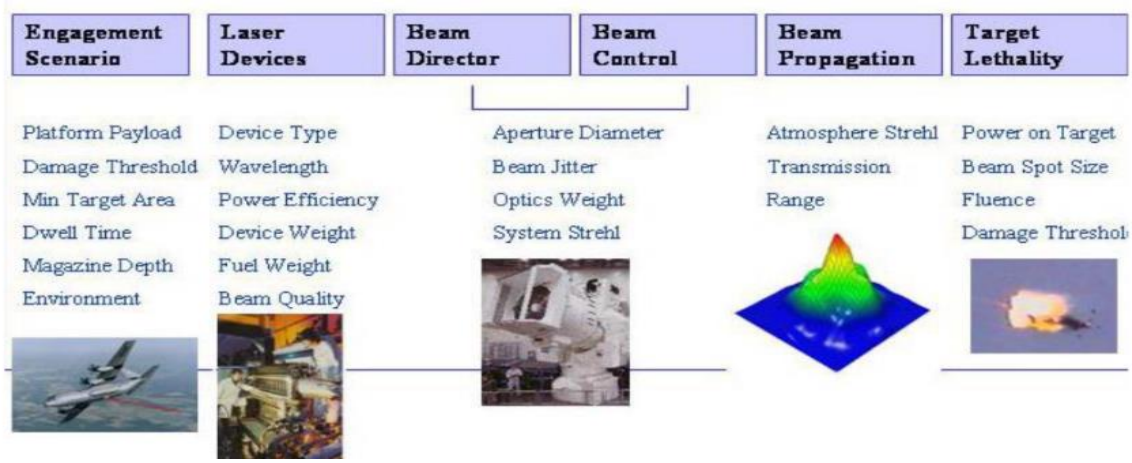
Cons: High cost, risk of unintentionally disrupting communications or destroying other electronic devices in the area, drone effectively switches off instantly falling uncontrolled to the ground.

(4) High-Energy Lasers

A highly-powered optical device which produces an extremely focused beam of light, or laser beam. The laser defeats the drone by destroying the structure and/or the electronics.

Components

- **High Energy Laser Device:** convert the electrical power into divergent beams of laser light.
- **Beam Control System:** Pointing the beam precisely at the chosen aim point on the target with sufficient intensity to neutralize it. It is also used to set beam aperture diameter, set phase corrections.
- **Thermal Systems:** Then there is the thermal subsystem. It removes the large amount of waste heat generated by the laser system and disposes of it in a way that doesn't degrade the performance of the laser.
- **Tracking System:** A monitor that displays the target and the aim.



Block diagram of HEL

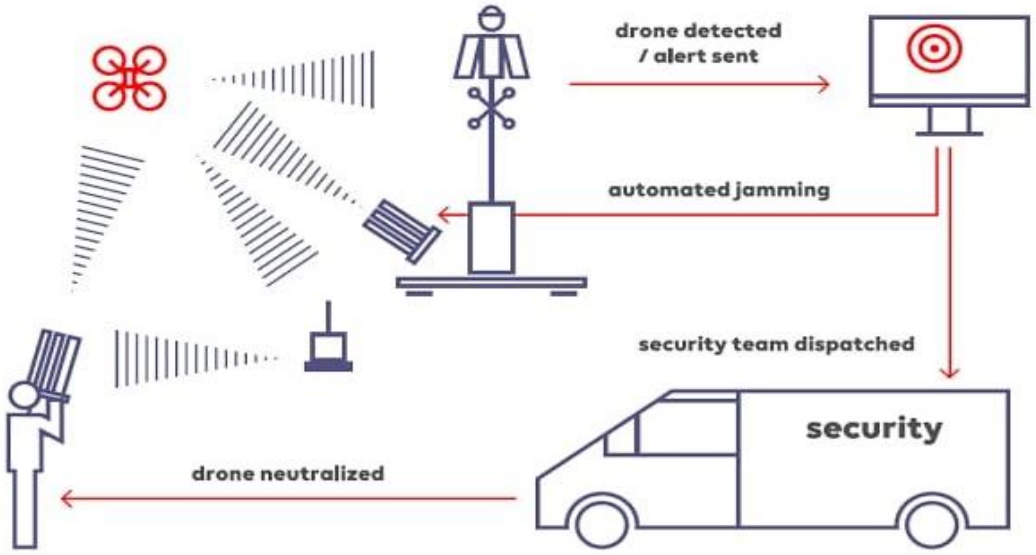
Working

It all starts with radar somewhere – typically on the platform itself or in an adjacent platform – that sends a message to say: 'there is something out there that might be a threat.' The laser system points in the direction of the threat. The decision-maker then determines whether the object is a threat that must be engaged. Once that decision is made, the beam control system engages sensors to ensure that the target is precisely tracked despite motion of both the platform and the target. Based on prior knowledge of the identified target, the most vulnerable point is selected via automation. The beam control system ensures that the high energy laser continues to hit the same point on the target with high precision until the target is neutralized.

Pros: Physically stops the drone.

Cons: High cost, risk of collateral damage, large system, mostly experimental technology.

Integration of Drone monitoring equipment and Drone Countermeasure Equipment gives rise to Anti Drone System



Model Diagram of Anti Drone System

FLOWCHARTS

There are three tasks in flowcharts:

1) Perceive: This section performs detection with high potential sensors. It also contains local processing based on the signal received. It is represented by **BLUE** colour.

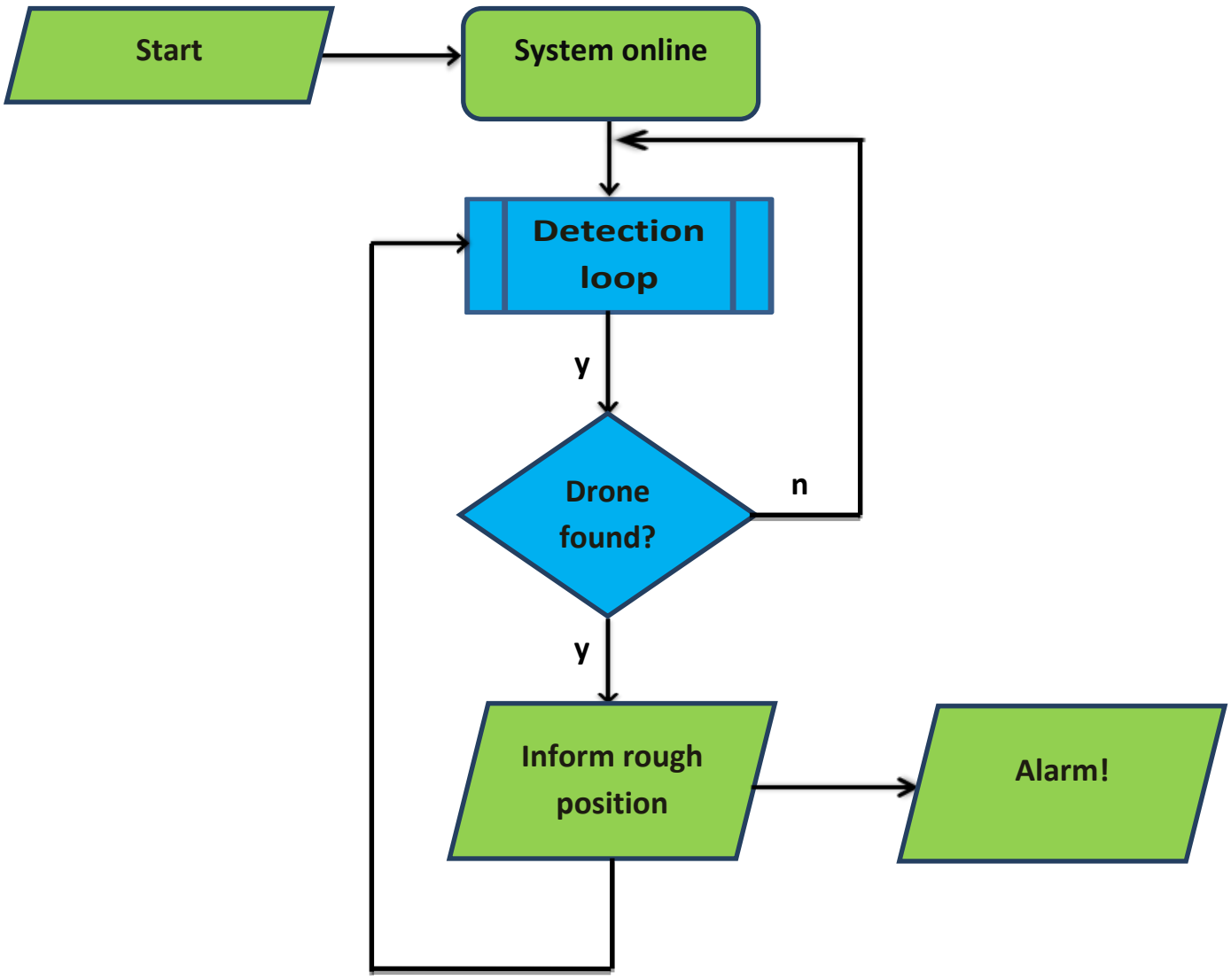
2) Operations: It receives the sensor's instructions, analyse the threat and based on it makes the decision. It is represented by **GREEN** colour.

3) Do: This section performs countermeasures against the drone. It is represented by **RED** colour.

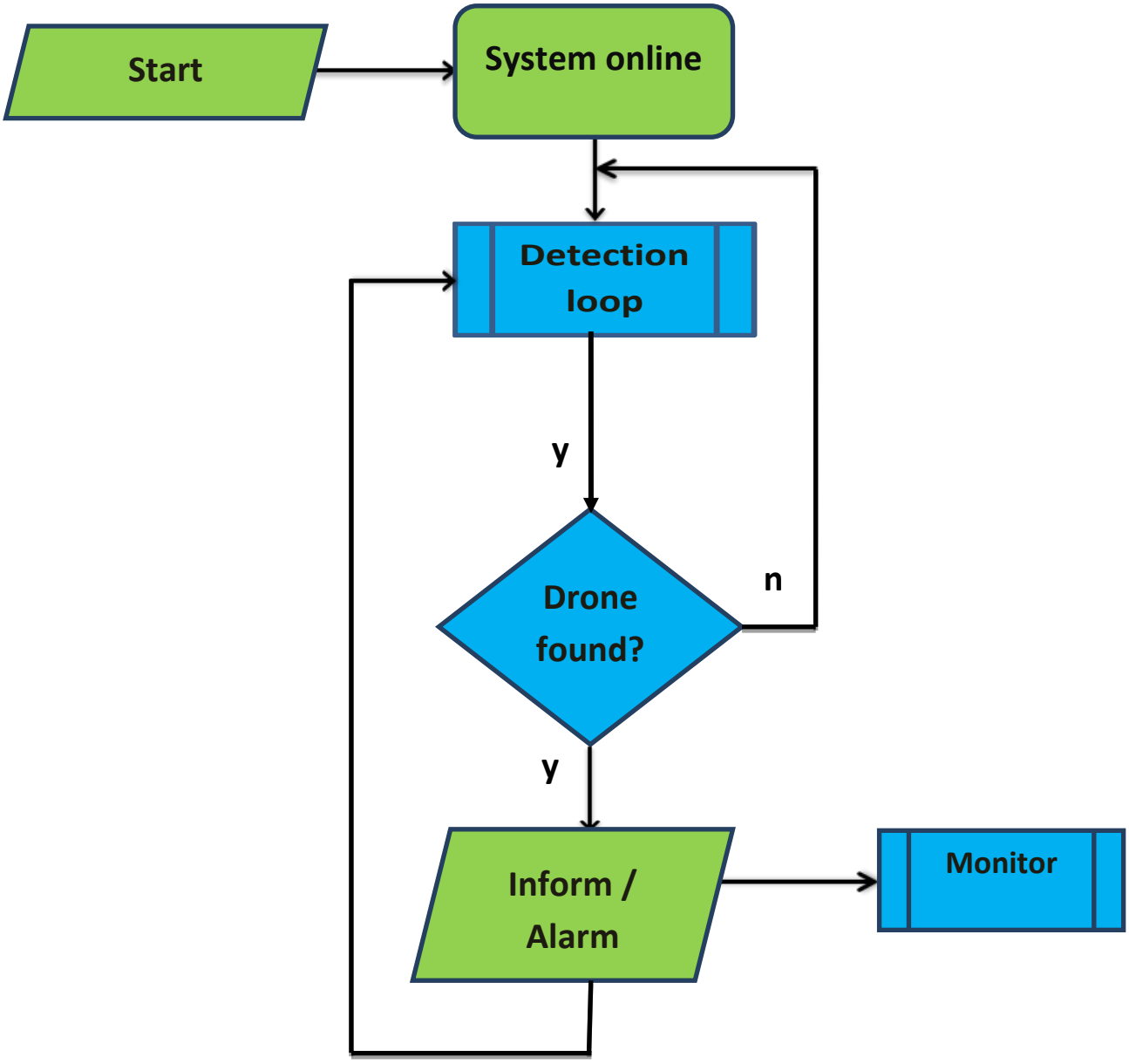
Four different scenarios:

1) Company office espionage
2) Airports
3) Military scenario
4) Prisons and Urban crowd scenario: Police & Stadiums

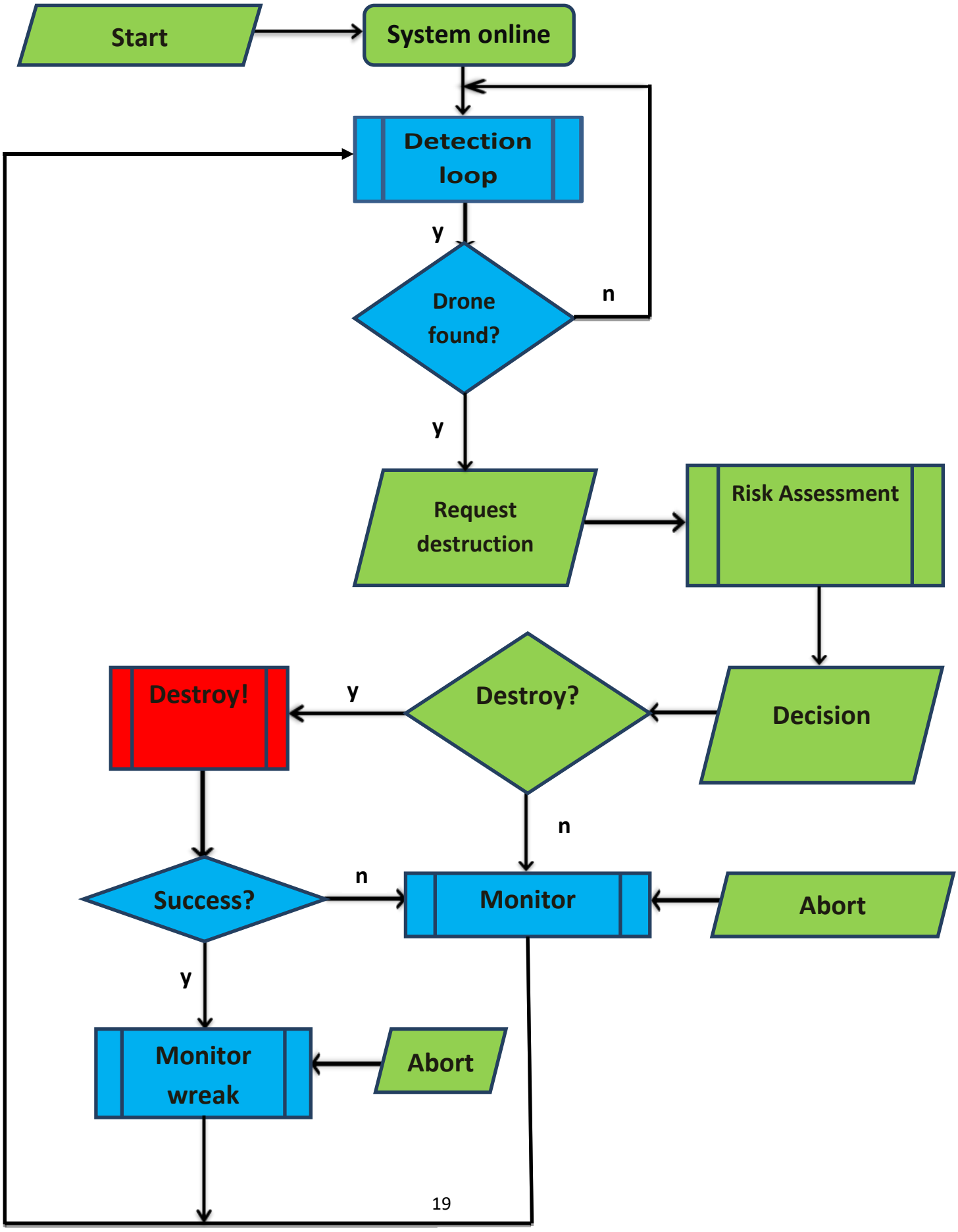
Company office espionage



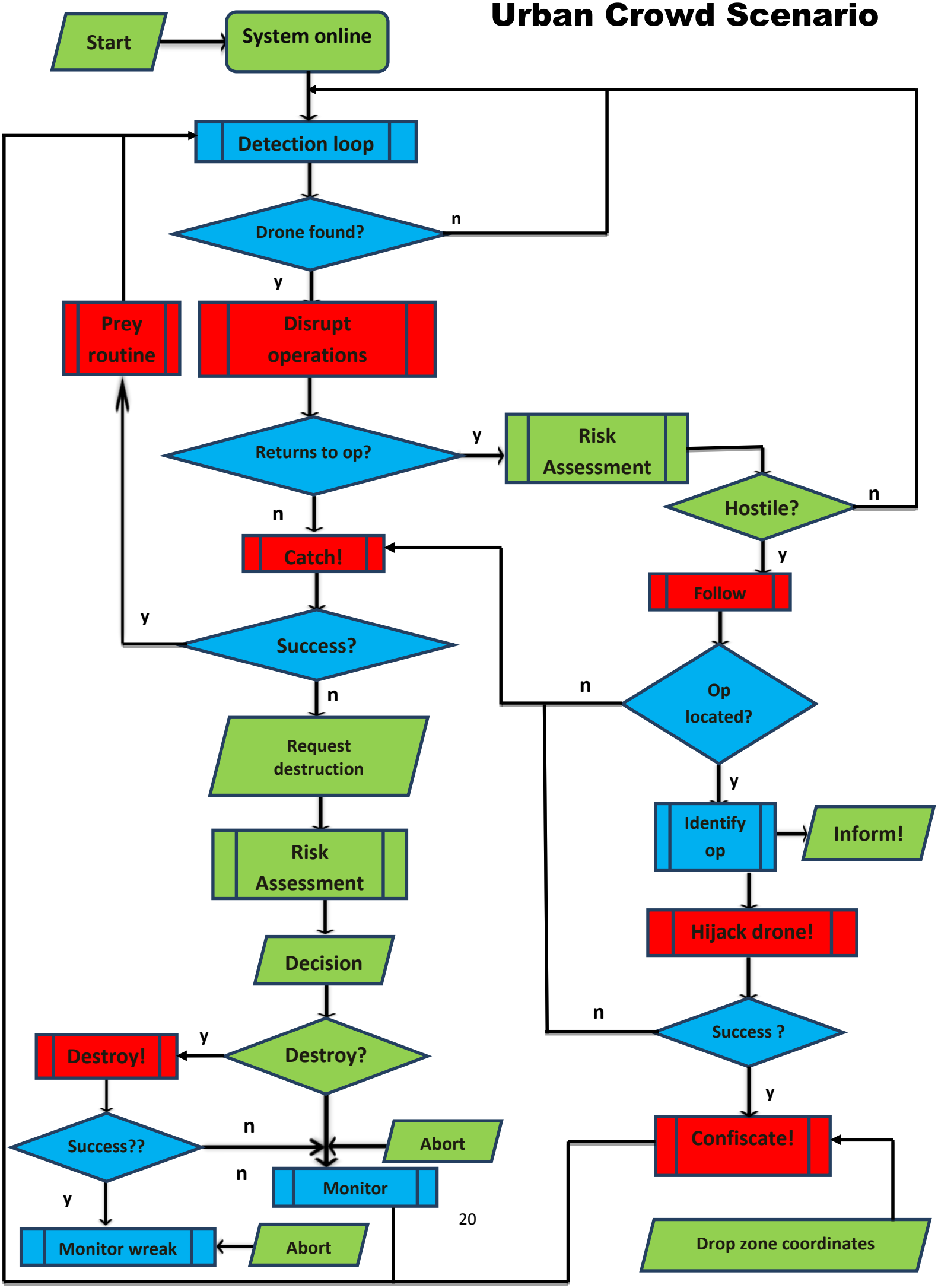
Airports


Start
System online
Detection loop
y
Drone found?
n
y
Inform / Alarm
Monitor

Military scenario



Urban Crowd Scenario



APPLICATIONS OF ANTI DRONE SYSTEM

- It has been used for airspace protection at airports, stadiums, prisons, corporations, and at major events such as the Super Bowl.
- It can be used at airforce stations or military bases to counter drone terrorism.
- It can be used in places where smuggling of drugs is done by drones.
- Many prisons have deployed a drone detection system to prevent smuggling prohibited items, such as drugs and mobile phones.
- India is considering deploying Anti Drone System near India-Pakistan border where drones are used for smuggling weapons by terrorists.

CHALLENGES

- Drone neutralization techniques causes interference with the useful information signal which is not desirable.
- Anti Drone Systems sometimes shoots down birds by accidently considering them as drones.
- Many new drones are being developed that are resistive to spoofing or interference.
- It is quite expensive as it is still under development.