NVEO
Natural Volatiles &
Essential Oils

Review on Anti-Drone Techniques

[1]P.D.Rathika, [2]Jaya Suriya B G, [3]Sivaranjani.A, [4]Aswadh Khumar G S

[1]Department of Robotics and Automation Engg
PSG College of Technology Coimbatore, India
pdr.rae@psgtech.ac.in

[2]Department of Robotics and Automation Engg.
PSG College of Technology
Coimbatore, India
balasuriya7699@gmail.com

[3]Department of Robotics and Automation Engg.
PSG College Of Technology Coimbatore, India
asr.rae@psgtech.ac.in

[4]Department of Robotics and Automation Engg
PSG College of Technology Coimbatore, India
aswadhkhumar15@gmail

Abstract

This circumstance has sparked a surge in demand for surveillance and defense systems that target drones in order to protect people, property, and national security from hostile drones. Drones can be used for a variety of purposes, including criminal and terrorist activities. It also infringes on a person's or company's privacy without their permission. This piques my curiosity in writing a review on anti-drone techniques. Some specific effective subjects, such as passive radar systems, spoofing, and other techniques, are exclusively explored in this review study. Advanced ways for preventing drone flight may be offered in the future.

Keywords— RADAR, Spoofing, Tracking.

I. Introduction

Unmanned aerial vehicles, also known as "drones," are unmanned aircraft that do not carry humans. Drones have become increasingly appealing for Internet of Things applications as their sensing and connectivity capabilities have improved, and their prices have decreased. Energy efficiency improves as the number of rotors is lowered. Drones have recently been utilized to detonate explosives at a variety of simulated targets. Drones that penetrate the airspace around airports can endanger traditional air travel by causing physical crashes or causing wireless interference.

The most important components for an IoT system to function. Sensors, connectivity, data processing, and a user interface are the four components. An autopilot is a gadget that can be used to integrate IoT and UAVs. It's a small avionics system that can be used to control unmanned aerial vehicles (UAVs). Though it was originally designed for complete drone autonomy, autopilot systems today include the sensors and processors needed to link the drone to the cloud.

Tactical applications are military surveillance applications such as border monitoring, accessing territories where a man cannot, mountain terrain monitoring, and so on. These applications necessitate drones that blend in with their environment, hence the drones employed are nano, micro, and mini in size and low in weight.

In the realm of anti-drone technology, surveillance is critical, and early warning systems are one approach to measure surveillance data promptly. Some military anti-drone technology is being developed.

The computerization of surveillance systems, as well as the huge volumes of data generated by such databases, along with the readily available computing power, give an incentive for the development of computer-assisted epidemic detection.

The Anti-Drone "Death Ray "Truck
The Drone Gun
Skyfence
QinetiQ (OBSINDIAN)
The Drone Killer IXI EW

Fig.1.Shows military anti-drone technology

II. TECHNIQUES USED FOR ANTI-DRONE

Warning Technique: From a mile away, detection systems such as ground cameras, sensors, and radars are used to provide early notice of the existence of any drone. The system can even locate the drone's location, providing crucial information that may be used to protect your site.

Spoofing Technique: Techniques of Spoofing Unmanned Aerial Vehicle (UAV) spoofing is typically accomplished via spoofing the UAV's GPS module. In comparison to the usage of three dissimilarity measures:

(1) Sum of Euclidian Distances among Corresponding Points (SEDCP),

(2) Attitude distance, and

(3) Taxicab distance, the Histogram of Oriented Displacements (HOD) of those sub-trajectories is used [8].

This method can identify the timing and function of UAV spoofing while also limiting the float inaccuracy of the VO. As a result of Sophisticated Receiver-Based (SRB) GPS spoofing, the results show that even this technology is efficient in finding UAV spoofing.

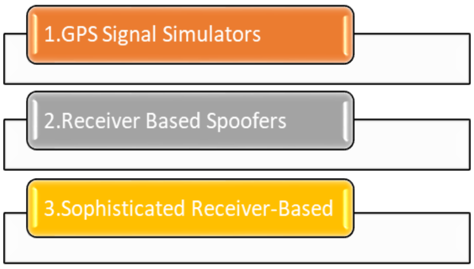

Fig.2.GPS Spoofing Methods

GNSS Receiver Stand-alone (GRS) and Hybrid Positioning Receiver (HPR) approaches are two types of anti-spoofing techniques. GPS signal detection is the main processing done in the GRS anti-spoofing approaches to detect and counter RFI attacks, and if intruders utilize more modern technology and sophisticated methodologies, this system fails badly.

To detect and prevent GPS spoofing, HPR algorithms use position data from alternative positioning systems, such as INS and LBS (Location-Based Service), or communication systems, such as cellular networks or Wi-Fi stations, as well as vision-based positioning systems.

The proposed vision-based UAV spoofing detection system is based on the UAV camera, which is a basic sensor that is unaffected by fraudulent GPS signals in terms of performance and pictures. A source of knowledge that may be obtained from Aerial imagery is the relative path of a UAV using VO..

Phases in the proposed vision-based spoofing detection technique for UAVs.[8]

1. The moving window size (k), the threshold of the employed dissimilarity measure (Th), and the threshold of UAV spoofing declaration (k/2) are all determined first. When determining false GPS coordinates, the threshold of dissimilarity measure is employed, and when declaring UAV spoofing, the threshold of UAV spoofing declaration is utilized. A sensitivity analysis is used to determine the SEDCP, HOD AD, and HOD TD dissimilarity measure threshold values. In addition, the UAV spoofing declaration threshold has been set to k/2.

2. Using a moving window of Wi, k photos from the UAV flight path are picked at each i-th UAV location, ranging from i-(k-1)/2 to i+(k-1)/2.

3. Two corresponding CTi and GTi sub-trajectories are computed using the selected images and their respective GPS coordinates within the window Wi.

4. The GTi coordinate system is converted into the CTi coordinate system.

5. CTi and TGTi's dissimilarity degree is calculated.

6. Within the window Wi, the computed dissimilarity measure between CTi and TGTi is compared to the threshold value, Th. The GPS position at the point I will be detected as a false position if the value of the dissimilarity metric exceeds Th.

7. The decision to declare UAV spoofing based on the stated threshold is determined based on the findings of the preceding phase.

In addition, UAV photos are frequently geotagged with GPS coordinates. In the event of a GPS malfunction. The sensitivity analysis process follows the iteration process of vision-based UAV detection. For the sensitivity assessment of the proposed technique to changes in UAV direction, one of the flight lines from the Golgir UAV photogrammetry project was first chosen as the true-traveled faked UAV route. Three dissimilarity metrics were proposed to compare these sub-trajectories: HOD AD, HOD TD, and SEDCP. To assess the recommended strategy, four scenarios were built using real photographs and GPS locations of the flight lines of the Golgir UAV photogrammetry project.

Jamming Technique: Drones having a maximum takeoff weight (MTOW) of less than 10% recently expanded their cargo capacity to 25%. This means that drones can carry and employ lethal weapons like guns and explosives. Only at heights of 150 meters or greater can control and monitor using the control radar be shown. Jamming, geofencing, and spoofing are all examples of soft death methods.

There are some radio jamming techniques. Jammers are available in some designs, which include the smooth constant jammer, which transmits a jamming signal continuously, the random jammer, which transmits nice intermittently, and extra complex jammers, which include the reactive jammer, which sends a signal nice while a purpose transmission is detected.

Mitigation Technique: Mitigation measures are divided into two categories: offensive and defensive. The mitigation strategy based on the Internet of Things is defensive, providing automatic responses. Drone detection systems can be combined with other security technologies, such as retractable roofs, window shades, closing doors, and enabling additional physical security measures, especially when protecting intellectual property or large groups of people.[1]

III. UAV Tracking and coordinate Detection

Anti-UAV defense system (AUDS) methods include spoofing attacks, tracking and early warning, detecting, defeating, and signal interference. Radar, satellites, and thermal imaging cameras are used to identify the trace of a drone from the ground and provide early warning and detection. Interfering with an invading drone's communications via electromagnetic interference techniques is successful, but it also impacts communications in the vicinity. As a result, the fault is readily apparent: communications systems in the immediate area are interrupted. The quality of life will also be impacted.

This paper proposes a dual-axis rotational tracing system that uses a thermal imaging camera and a full-color camera. Using an image recognition technique, this system tracks and locks a drone. When a drone is within visual detection range, the gadget employs dynamic coordinate tracing to track it. To accomplish the sensing and subsequently determine the drone's flying height, the proposed system employs a nine-axis attitude metre and laser rangers. Longitude and latitude data from the drone are collected using spherical coordinates..

A floor manipulate station arranges an attack drone to defeat the goal drone the use of an internet gun, laser gun, or different guns together with rifles through constantly locking the dynamic coordinates of the drone. At this point, real-time transmission of the dynamic coordinate to an attack drone is needed for a fast pursue.

To strengthen the drone's detecting capabilities, a mechanism frame within the dual-axis mechanism is fitted with a fine-tuning device, a nine-axis attitude meter, a thermal imaging camera, and a full-color camera for drone picture capture and position recognition.

Three laser rangers are used with the photographic lens, which is used as the center of the image frame's focus point and the focus distance of the drone to be acquired by the tracking device is found , so that the laser ranger on the drone's hitting spot overlaps with the center of the image's spot. Because of the requirement to avoid metal interference and signal-shelter in the thick casing of the tracking device, CPS and LoRa antennas are installed outside the tracking device.

Next to that, a Gaussian filter and a median filter are used to eliminate noise and smooth the image so that subsequent shots are not affected by the noise impact. The histogram of the picture reveals that there is indeed a largest value. Its value is the T value. After threshold processing, a binary image may be produced. Following threshold processing, the dilation in morphology technique may be used to separate independent UAV image components, emphasizing the UAV in the picture for improved system tracking.

It synchronizes the movement of anomalous things with that of the target and the camera. There will be a significant variation between future frames. Real-time tracing necessitates a little bit of rapid calculation to follow the drone steadily due to the fast drone flying speed. The advantage of the frame difference approach is that it nearly eliminates the background buildup problem.

This technique is tested under three different weather conditions: cloudy, sunny, and rainy. When opposed to wet conditions, the output of findings is better in bright and cloudy environments because there is a probability of missing the drone in those conditions (poor visibility and tracking). Although the efficacy of this method is not indicated, it is successful in both sunny and gloomy conditions.

Using the infrared camera to trace longitude and latitude coordinates at night.

Thermal detection is used in drones to detect the temperature of the batteries and motors.

IV. Position Tracking Using multiple Receivers

The anti-drone system's key technology is location tracking, which is used to detect and monitor the precise location of illegal drones. The positioning system has been continuously investigated as interest in location-based services has expanded due to improvements in IoT and mobile device technology. Refining strategies that include RSSI coefficient calibration, iterative trilateration, and a smoothing procedure to decrease dynamic signal variation were described to enhance the accuracy. A Kalman filter was employed to increase the precision of trilateration.[5]

Existing BLE-based location tracking approaches use the fingerprinting methodology referring to the received signal strength indication (RSSI) database and the trilateration method to track an object's position and also the RSSI-distance conversion formula using a propagation model. To boost performance, the authors proposed position tracking algorithms that integrate existing methods with diverse sensors. Radar is a common drone detection device that uses reflected radio signals to locate the position of illegal drones. Various methods were considered as a radar replacement technology to solve this problem, such as using the physical characteristics of an RF signal used for drone control to distinguish it from a mobile device, monitoring drones using camera images, and detecting an acoustic signal generated by a drone.

According to the method for determining the moving distance and angle, two tracking algorithms are used:

- The constant distance and quantized angle constant distance and quantized angle(CDQA)algorithm and
- The adaptive distance and continues angle (adaptive distance and continues angle (ADCA)) algorithm.

We leverage the memory process, which uses prior movement information, in the suggested algorithms to lessen the effect of the estimation mistake caused by RSSI inaccuracy.

Apply a memory process to the tracking algorithms, which saves the information from previous movement steps and minimizes the likelihood of moving in the wrong direction depending on the information saved.

nm is the number of movements required to follow the target, and it is constrained by nmax, the maximum number of movements. As a result, if nm > nmax, the tracking will fail[5]. Otherwise, in the case of nm nmax, the tracking is finished when the tracker arrives inside the threshold distance from the target.

Compare the recommended tracking algorithms to the existing trilateration-based algorithm and memory applied trilateration approach in terms of the number of movements, total moving distance, and success rate based on average tracking time. When compared to the existing M-Trilateration technique, the suggested M-ADCA method would achieve the best result.

As a result, all computations and methodologies are provided, along with a graphic representation of the method's efficacy. In the future, we will aim to progress in real-time, as this strategy produces positive and beneficial effects.

V. Anti-drone systems

The Anti-Drone system has three phases.

- Detection,
- Identification, and
- Neutralization of drones

Traditional zone security systems incorporate drone detection equipment like radars or cameras, but they lack the performance and awareness necessary to distinguish a variety of drone occurrences. In terms of weather resilience, identification availability, and cost, thermal detection outperforms radar-based systems. The genuine detection range (51 m) is, however, far less than most of the other approaches.

Signal intelligence and communication intelligence are the basic paradigms for RF-based drone detection. Drones that utilize unknown control protocols or distinct frequency bands are difficult to detect using an RF scanner that performs signal analysis. Frequency modulated continuous wave radar and coherent pulsed Doppler radar preserve and track broadcast and received signal phases to determine distance and velocity. The Ka, K, and Ku bands have relatively small wavelengths above 18 GHz. It was used for early airborne radar systems, aside from marine navigation radar systems.[6]

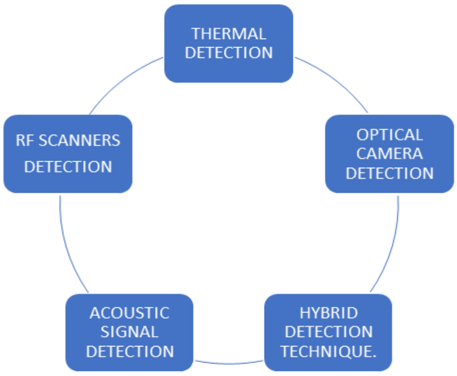

Fig.3. Anti-Drone Detection Techniques

The primary difference between 2D and 3D radar is just because 3D radar can forecast target object height, whereas 2D radar relies on auxiliary devices for limited Z-axis information. A drone detection system based on optical cameras has very few legal constraints, allowing for fine-grained tracking via dense deployment. Jamming limits, existing radar installations, and drone neutralization procedures are just a few of the constraints that non-military technologies must overcome..

An RF scanner is sufficient for identifying hobby drones flying in an unlawful manner over a large region. Meanwhile, drone-sensitive places such as airstrips and nuclear power plants must be provided with detecting components such as vision, radar, and hearing to ensure reliable monitoring of any flying objects. A drone detection blind zone is unavoidable when using a single detection technique. For done detection, radar and optical cameras function well together. By controlling image magnification, tilt, and focus, vision-based detection can easily monitor drones, but it lacks dynamic control over the target region. on the other hand, With low drone identification and scan frequency, radar detection allows for omnidirectional wide-area scanning.[3]

A detection range of 3–5 kilometers can be achieved using a variety of detecting technology combinations. In order to create a viable anti-drone system, you must first find an appropriate detection configuration for the target region.

Drone detection refers to the process of determining if a moving (or stationary) item is a drone, whereas drone identification is the process of determining whether the detected drone is unlawful and should be destroyed. Whether through classic image processing or machine learning, the bulk of systems rely on vision data to better drone tracking. Path estimation systems use neural networks or a variety of filters to recognize drone movement based on data collected. To detect and retrace tracking errors caused by fast positional changes, the authors developed a recursive filter.

RFID has become widely employed for identifying and real-time locating systems in recent decades. Attaching Ultra High Frequency RFID tags to UAVs and installing a number of passive tags over the target area, connected to the system proposed a differentiated method for indoor localization by attaching UHF RFID tags to UAVs and installing a number of passive tags over the target area, connected to the system proposed a differentiated method for indoor localization by attaching UHF RFID tags to UAVs and installing a number of passive tags over the target area, connected to the system

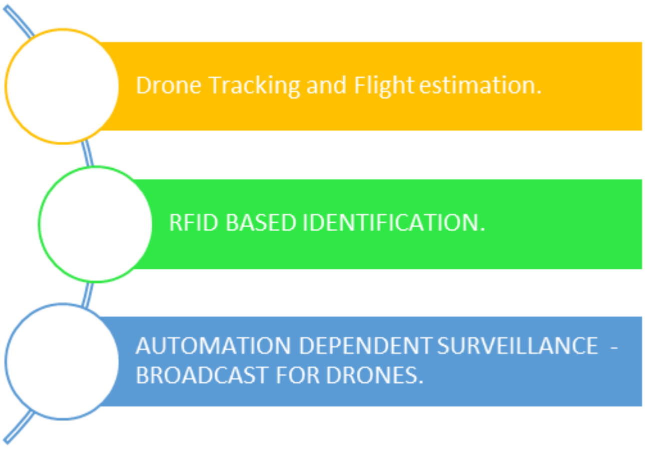
Drone Tracking and Flight estimation.
RFID BASED IDENTIFICATION.
AUTOMATION DEPENDENT SURVEILLANCE - BROADCAST FOR DRONES.

Fig.4.Drone Identification Techniques

Some activities stop the threats of stopping the drone movement are called as Drone neutralization.

Many countries now restrict the destruction of illegal drones, hence non-destructive methods are favored in various public establishments. The fundamental distinction between hijacking and spoofing is what happens after the attack. After a hijacking, the real controller loses control of the drone, whereas hijacking is done with the help of spoofing signals.

While geofencing effectively prevents hobby drones from accessing unauthorized regions, it is unable to safeguard a modified or renovated drone since it disables the drone controller's automated landing procedures. Because the system relies on the internal navigation logic of the drones, defective drones might allow trespassing into the restricted area. Hijacking, spoofing, and auto-landing are the top tier scheme categories [6].

Killer drones are authorized UAVs that follow and attempt to damage other drones. To differentiate it from drone capture, we reduce the scope of the killer drone to capabilities that physically attack invasion aircraft. Incoming drones need timely and efficient decision-making, along with exceptional physical toughness and agility.

Because airports are highly populated areas with a significant danger of injury in the case of a plane crash, national security authorities frequently implement military-grade defense systems. The hierarchical configuration, together with local anti-drone systems such as those found in airports and factories, will provide a global perspective of drone provocation and enable cooperative tracking and neutralization Minimal noise drones are seen as a larger hazard since noise can help humans detect and evacuate drones while also decreasing destruction.

VI . PASSIVE AND FMCW RADAR

The RCS of a metallic panel and a cylinder using the CAD CST was done for two reasons

- To be utilized as a reference target in the experimental set-up.
- To validate the suggested experimental technique. RCS values are higher for frequencies about 3.8 GHz and above 4.5 GHz.

For website standardization and validation, the canonical targets were positioned on a styrene column at a group distance of three meters from the antenna. The activity instrument at the antenna instrumentation was calibrated using a short-open-load technique. Throughout all measurements, the VNA was meant to brush the 1–4 Gc band with 1601 points and offer a supply strength of thirteen dBm.[4]

Calculating the reference RCS from the complex RCS of a cylindrical goal using CST software. The CST simulation is compared to the cylinder RCS observed with the double-ridged horn antenna at a distance of 3 m. This effectively verifies the semi-anechoic chamber's RCS measurements, making the IRIS drone's following RCS measurements more trustworthy. If the measurements' results are to be used in the creation of anti-drone radar, this is important. While the 3.8 Gigahertz range is restricted, the 2.4 GHz band is quite near to being one of the ISM bands and might be an acceptable alternative.

Frequency selection goes hand in hand with the selection of suitable sources of opportunity to be used as illuminators when utilizing illuminators of opportunity as illuminators in passive radar. The 2.3 GHz band, in particular, is particularly adapted to the use of widely accessible WIFI signals, and it has recently been demonstrated that it is capable of detecting vehicles such as cars and light planes, as well as human targets. According to the analysis, the use of passive radar based on Wifi networks of opportunity for the detection of commercial drones offers certain advantages..

Simulation of RAPID-SIM Contains

- Radar Model
- Drone Model and
- Parametric Analysis Tool.

There is presently just one FMCW model in the RAPID-SIM, but new types of radar models might be introduced in the future. The drone model is made up of kinematics, guidance law, and RCS features. The drone's fuselage and blades are said to include many reflectors. Every drone's positioning and velocity are computed using a numerical integration approach such as the Euler or Runge-Kutta methods.

Two micro-Doppler spectrograms are observed on a fixed-wing UAV and a quadcopter drone. Because the propeller rotates at 20Hz, the fixed-wing UAV's micro-Doppler signature shows a limited dispersion of blade reflector signal around the body reflector.[2]The quadcopter's micro-Doppler signature features a huge and powerful dispersion of blade reflectors' signal around the body reflector due to the rotor rotating at 100Hz and the number of reflectors on the blade being 8. The parameter analysis program may cover a wide variety of parametric studies, including performance and sensitivity analysis.

Range resolution Rres and velocity resolution VD, res are the two most important characteristics. Using these values, we may divide the full range-Doppler map into many cells. To mark a single target's position on a range-Doppler map, the CA-CFAR (Cell Average Constant False Alarm Rate) approach is widely utilized. One of the existing tracks is assigned to the most recent CA-CFAR result via the data association method. The following gates are calculated using motion estimations and maneuver model assumptions, which is a common aspect of all methods.

The proper collaboration of numerous radars necessitates the conversion of their readings to a common coordinate system azimuths must be measured in the same direction. The height of the object is also provided by three-dimensional radars[7]. This means that the precision of determining drone localization in a global coordinate system is determined not only by radar performance but also by the accuracy of radar coordinates and spatial orientation relative to the local horizon and north. Micro-Doppler signature analysis is the most often used classification approach.

The measurement of azimuths relative to the same direction is one of the main prerequisites for their efficient collaboration. Otherwise, inaccuracies in establishing the real position of will occur. Because all devices make the same constant error in azimuth measurements, the problem of azimuth misalignment does not occur. At a distance of 1000m, a 5Degree azimuth misalignment results in a drone coordinate inaccuracy of around 87.5m.[7]

A uniform distribution in the range of +/15 Degree will be used to construct the constant component of the azimuth measurement error. For each radar, the values will be created individually and will remain constant for one simulation. The difficulty with Azimuth in the actual world is misalignment of certain sensors, and this solution reduces the inaccuracy and accurately detects the item. The method's downside is that it requires a drone calibration flight along a predetermined path.

VII – CONCLUSION

In the relevant publications, we detailed the many tactics employed in this study, experimented with them, and provided the appropriate mathematical equations. With the fast growth of drone technology and the growing attention on anti-drone, a drone identification system should be able to determine if the observed aircraft should be neutralized or not. Aggressive and non-destructive methods must be examined separately and carefully selected in system design. Modern anti-drone systems have well-defined recognition, identification, and neutralization stages, but more precise and effective systems are needed to deal with high-speed, high-security, and three-dimensional threats.

REFERENCES

1. Guoru Ding, Qihui Wu, Linyuan Zhang, Yun Lin, Theodoros A. Tsiftsis, and Yu-Dong Yao, “An Amateur Drone Surveillance System Based on Cognitive Internet of Things,” November 2017.
2. Joongsup Yun,David Anderson and Franceso Fioraneli, “Parametric Investigation on Simulated Staring FMCW Radar for Anti-Drone Swarms”, September 2020.

3. Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi and Jiming Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," pp 1-22,April 2018.
4. Stefano Pisa, Emanuele Piuzzi, "Evaluating the Radar Cross Section of the Commercial IRIS Drone for Anti-Drone Passive Radar Source Selection," May 2018.
5. Jae-Min Shin 1, Yu-Sin Kim 1, Tae-Won Ban 1, Suna Choi 2, Kyu-Min Kang 2 and Jong-Yeol Ryu 1, "Position Tracking Techniques Using Multiple Receivers for Anti-Drone Systems," December 2020.
6. Seongjoon Park,"Survey on Anti-Drone Systems: Components, Designs, and Challenges," March 2021.
7. Aleksander Nowak, Krzysztof Naus and Dariusz Maksimiuk," A Method of Fast and Simultaneous Calibration of Many Mobile FMCW Radars Operating in a Network Anti-Drone System",pp 1-20,November 2019.
8. Masood Varshosaz, Alireza Afary, Barat Mojaradi," Spoofing Detection of Civilian UAVs Using Visual Odometry", pp 1-23 ,December 2019.