

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

AUTO IDENTIFICATION OF MICRO-DRONES/UAV

Samyuktha Madhusudhan Thumala^{*1}, Geetha P², Pavithra J, R Uma³

^{*1,2&3}Department of Computer Science and Engineering, Sri Sai Ram Engineering College, Chennai, India

ABSTRACT

With the increase in utilization of micro-drones for a variety of commercial activities, the risks involved in its misuse have also increase. Drones/UAV's have been used in both military and civil environment, over the decade. However, the misuses of drones can cause serious damage. This calls for a method of identification wherein, an alien drone can be identified before its action is initiated. We propose a system that identifies the presence of an alien drone by regulating the interference produced by signal overlapping by initially appropriating the frequency of the signal within the given bandwidth.

Keywords: *Micro-Drone, UAV, Drone Detection, Frequency regulation.*

I. INTRODUCTION

Popularities of drones have caused the risks of the misuse of drones to grow parallely. [10] Many a times, privacy violations occur when drones used with legal permission, try to gain access of data in its controlling environment illegally. A very common use of drones is in the film industry. However, it also makes illegal filming easy with the ardent growth of micro drones and UAV's. Gone are the days when trespassing was done physically. With drones, one can enter unsecured areas and be unnoticed. Another common use of drones is in the oil and mineral industries, where it is used for the transportation of small items that are mined from one place to another. But this also allows room for smuggling of mined items. The most alarming misuse of drones are for terrorism, bombs are transported bombarded in remote areas. This calls for a counter action to prevent such security hazards.

II. RELATED REVIEWS

The existing system of identification focus on employing Radio Frequency detection and Object Recognition to detect drones.

Identification of drones from the controllers end through a Parrot AR. Drone. The position of target is determined using IMC position controller, using its on-board sensory equipment.

A drone detection was developed to assist airports in detecting and collecting information regarding drone flight around the vicinity of an airport to improve flight safety. It works by comparing the current drone location and altitude to a predefined position within the range of five miles. [1] The different techniques for object recognition and its suitable application areas were studied. It focuses on both single and multiple object detection. [2] For objects in flight, there is a necessity for sensors to be in communication with a controller to identify the object in the field of view. Pattern recognition algorithms were incorporated to provide better automatic detection, such as distinguishing from different flying objects.

An outline for the challenges in drone detection, identification and classification to preempt any possible malicious intent was discussed. [8] The deployment of drones in different war zones were presented. [3] The Radio-frequency interference (RFI) was addressed as a problem for microwave sensing. These statistics were useful in determining the methods of interference that produce new signals. [4] A survey of the radio-frequency interference (RFI) observed in the Aqua AMSR-E radio meter channel was carried out. Spectral difference method was used to determine the magnitude, which is applied to determine the plausible frequencies upon inward propagation, in our system. [9] Multiple frequency shift keying (MPSK) entails choosing one of N frequencies as the carrier or center frequency for each transmitted symbol. In a communication system, when frequency hopping is superimposed on

MFSK, resulting in an FH/MFSK system, the set of H possible frequencies changes with each hop. This helps identify the frequencies produced upon inward propagation.

III. EXISTING METHODS OF IDENTIFICATION

Current drone detection units employ a range of methods to identify the presence of drones in the vicinity of the area being monitored. The constituent methods/sensors of the detection system are:

A. Radio Frequency Scanners(Rf)

Radio frequency scanners are components that are used to track and identify any drone/UAV over a large area. They work on the basis of scanning the electromagnetic spectrum in order to achieve the frequency in which the drone in the area flies communicates with its controller. They can also in turn give command to the drone, however, this act is illegal.

B. Radar

Radar as in any other application, is used to find the distance of the micro-drone/UAV from the monitoring system. It works on the principle of signal reflection. It transmits a signal which bounces off the drone and is received by the radar. Through this, the position of the drone can be determined. However, since the speed of drones is not known, it needs constant action to determine the area the drone flies in.

C. Acoustic Sensors

Since there is no guarantee of radars and radio frequency sensors to accurately determine the position of drones, acoustic sensors provide an advanced detection technology to sense the micro-drones/UAV's. These sensors, listen for high pitch frequencies emitted in its vicinity. Along with this, the intensity of the receiving signal plays a role in determining its approximated location. These work well in Stealth conditions. It is majorly used for detection threats.

D. Cameras

Video camera are used to provide situational awareness, that is, when the area is completely monitored, there can still be times when a drone can go undetected. It is in such cases that video cameras with constant manual supervision along with video analytics provide a higher sense of monitoring.

The above-mentioned components are tied together in one unit as shown in Figure.1. These monitoring units are fixed in points in an area that are in need for high levels of security. The different signals are distinguished from one another using different lines. This system works best when the area under supervision is small and their radio frequencies can be captured easily.

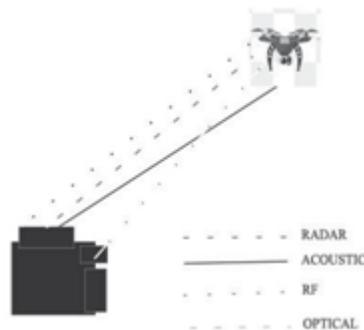
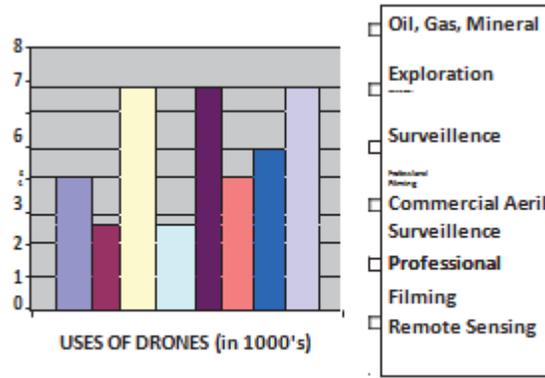


Figure 1. Existing Micro-Drone/UAV detection system

IV. MARKEY SURVEY

The following Figure 2 provides data on the increasing uses of drone in the year 2017 for the various purposes mentioned. The Figure 3. Presents the reported misuses of drones from the last 3 years in thousands.



SOURCES: The Economist, Technology Quarterly

Figure 2. Survey of Uses of Drones

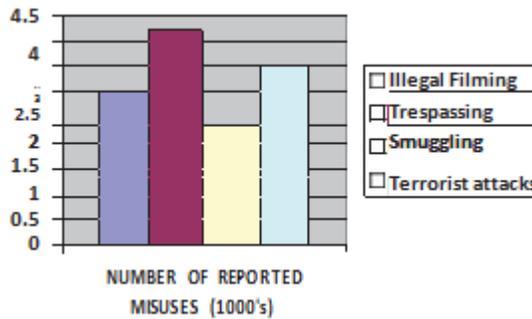


Figure 3. Survey on the misuse of drones

V. PROPOSED METHOD OF IDENTIFICATION

Issues in Existing System:

- The number of identification units increase exponentially with the increase in area being monitored.
- The area of coverage needs to be scalable.
- Using parrot drones for identification needs manual monitoring which is tedious.

For the above reasons, we propose a system wherein, the area being monitored is easily scalable. We employ frequency division method which helps in using low power consuming components which are particularly helpful in warzones. Manual monitoring is not necessary. The following are the steps for identification

We divide the given territory into hexagonal cells and install frequency emitters at every vertex. The frequencies emitted by the RF emitters will be within the bandwidth assigned. The frequencies as the propagate inwards, towards the center of the hexagon, will interfere with the neighboring signals. The initial RF's must be chosen such that the upon addition, subtraction and averaging any two signals, the resultant frequency lies in the assigned bandwidth itself. Thus, our drone (home drone) will be able to be operated through all frequencies without delay (Home Drones are designed to fly in that particular bandwidth). However, when an alien drone flies through the

region, there will be an unprecedented interference that results in a different frequency in that region which will be detected by an RF receiver. This enables us to identify an alien drone instantly.

A. Step 1

Six initial frequencies are to be chosen such that, the difference, sum and average between any two frequency lies between the designated bandwidth. The initial frequencies must be determined such that, when progressively averaged to an approximately close-range frequency, it produces a frequency within the same range. When the frequencies are progressively added or subtracted, they may go out of range. Therefore, two different lower range frequencies can be placed adjacently for addition to lie within the range. In case of subtracted signals, frequencies from extremes of the range must be chosen for the frequency to lie within the same range. Figure 4. Represents the placement of frequency emitters.

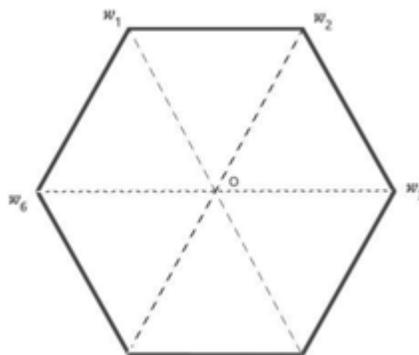


Figure 4. Placement of Frequency Emitters

B. Step 2

Given an area, we divide the area into hexagonal segments and install radio frequency emitters at each vertex. The frequency emitted is one of the frequencies in the given bandwidth for transmission to the military. Since, the radio frequencies propagate in all directions, filters can be installed at the periphery of the overall territory to avoid propagation outside the territory. The filters can ideally be installed at 5 meters in the opposing direction of inward propagation from the RF Emitter as in Figure 5.

C. Step 3

The adjacent signals will overlap at 6 points within the Hexagonal region wherein an amplifier will amplify the signals further inward. Each amplification point also contains an RF Detector. The interfered signals will have one of the following frequencies:

- $\omega_1 + \omega_2$
- $\omega_1 - \omega_2$
-

□2

Interference between two signals from different hexagons can be avoided by placing close range frequencies. The amplifier amplifies the frequency emitted further into the neighboring hexagonal cells as shown in Figure 6

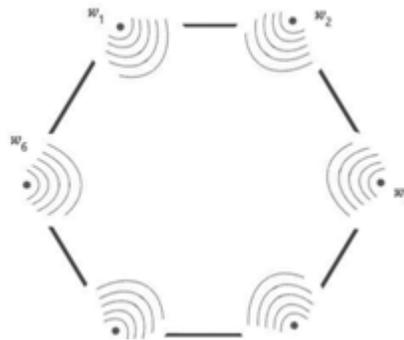


Figure 5. Frequencies (9) emitted by the Frequency Emitters

D. Step 4

The radio waves as they propagate inward, interfere progressively, in total providing $6 \times n$ signals in every hexagonal cell (n = number of interferences from the line of a vertex intersecting at the center of the hexagon) as shown in Figure 7

- When there is interference of six signals, it is assumed that the center of the hexagon is reached which contains a low range acoustic sensor.

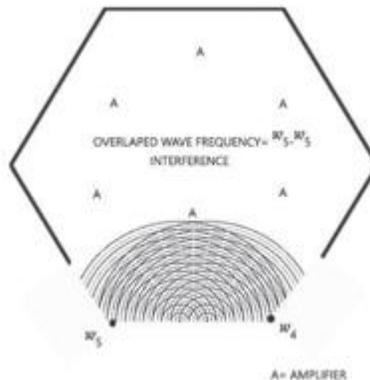


Figure 6. Frequency Interference between neighboring signals

- Drones that are permitted to fly within this territory are controlled using the designated bandwidth and hence, during its flight, it will be able to fly through all of the $6 \times n$ frequencies.
- All hexagonal units combined, we obtain a total of $6 \times m \times n$ signal frequencies, where m = number of hexagonal cell units. (Considering the slight deviation in frequency from cell to cell, we assume that a slightly variant $6 \times n$ signal frequency will be produced in the neighboring hexagonal units.
- However, when an alien drone from a predator is flown inside the region, it will cause unprecedented interference in one of the interference points, which can be detected by the RF Detector at every amplifier.
- An optical detection system can be installed outside the peripheral hexagon and a machine learning monitoring system can be employed. The system can use ‘Object detection by pattern recognition.’ [1]. It uses sensors to detect the presence of a far of object using pattern recognition followed by which the object is classified as a micro-drone or any other flying object.

VI. MAJOR COMPONENTS USED

A. RADIO FREQUENCY EMITTER

A RF transmitter is the prime component of the proposed system. It is used to generate the initial frequencies needed. It is a small PCB that transmits radio waves that can be modulated to carry data. They are regulated in order to provide a limit for transmitter output and band edge requirements. This regulation is done in the primary stage when the bandwidth is allocated to the military.

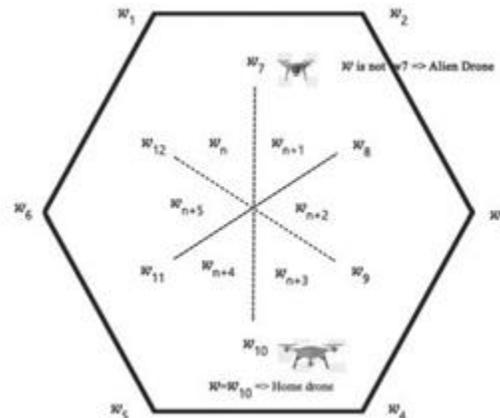


Figure 7. Propagation of signals

B. OPTICAL DETECTOR

The optical detector uses the object detection system which uses pattern recognition algorithms to identify the flying object. The objects are predefined to minimize false positives and eliminate background noises. Upon detection, it checks with the home controller if the drone is a home drone or an alien drone and accordingly initiates action.

C. AMPLIFIER

An amplifier is an electronic device that increases the power of the signal. It uses external power supply in order to increase the amplitude of the signals. The amount of amplification is measured by its gain.

D. ACOUSTIC SENSORS

Since there is no guarantee of radars and radio frequency sensors to accurately determine the position of drones, acoustic sensors provide an advanced detection technology to sense the micro-drones/UAV's. These sensors listen for high pitch frequencies emitted in its vicinity. Along with this, the intensity of the receiving signal plays a role in determining its approximated location. These work well in Stealth conditions. It is majorly used for detection threats. Figure .8 provides the overall layout of the system.

VII. EXAMPLE FREQUENCIES

Initial Frequencies: The initial frequencies are chosen based on close range values. Let the range provided for use be 200- 550MHz. In Table I., 'a' refers to added frequencies, 's' refers to subtracted frequencies and 'A' refers to the Averages frequencies

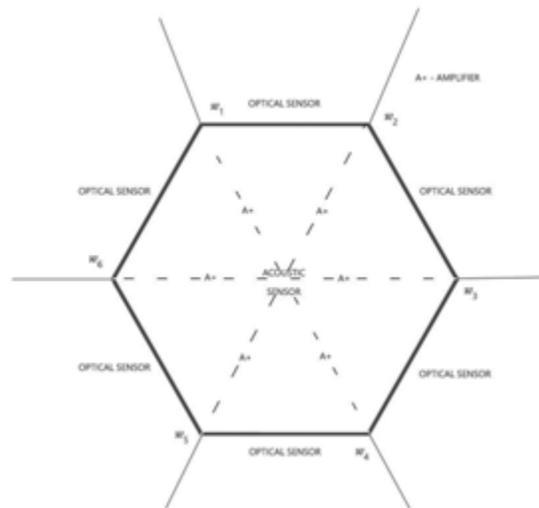


Figure 8. Overall System Layout

TABLE I.

S.no	INITIAL FREQUENCIES Vs RE			
	Frequency(M Hz)	Neighbor 1	Neighbor 2	Interference Operation (N1, N2)
1.	200	2	6	a, s
2.	250	1	3	a, a
3.	300	2	4	A, A
4.	350	3	5	A, A
5.	325	4	6	A, s
6.	530	1	5	s, s

VIII. CONCLUSION

The proposed method of drone identification employs frequency regulation to monitor interference levels in the area of concern. This method has an upper hand over the existing methods due to its scalability provided by the layout of components deployed. Moreover, it provides increase surveillance due to multiple levels of drone detection. The power consumed by the entire system is relatively minimal and hence can work in adverse conditions.

REFERENCES

1. *Techniques for Object Recognition in Images and Multi-Object Detection*, Khushboo Khurana, Reetu Awasthi, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 2, Issue 4, April 2013
2. *Object detection by pattern recognition US6154149A US Patent Grant*
3. E. G. Njoku, P. Ashcroft, T. K. Chan and Li Li, "Global survey and statistics of radio-frequency interference in AMSR-E land observations," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 43, no. 5, pp. 938-947, May 2005.
4. Li Li, E. G. Njoku, E. Im, P. S. Chang and K. S. Germain, "A preliminary survey of radio-frequency interference over the U.S. in Aqua AMSR-E data," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 42, no. 2, pp. 380-390, Feb. 2004.
5. A. Hernandez, C. Copot, R. De Keyser, T. Vlas and I. Nascu, "Identification and path following control of an AR.Drone quadrotor," 2013 17th International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, 2013, pp. 583-588.
6. Krista Brouwer, Thomas Cottam, Catherine LiVolsi, Stephen Pratt, "Eye in the Sky – Drone Detection & Tracking System", *Airport Cooperative*
7. *Research Program: University Design Competition for Addressing Airport Needs, 2014 – 2015*, University of Rhode Island.
8. M. Nijim and N. Mantrawadi, "Drone classification and identification system by phenome analysis using data mining techniques," 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2016, pp. 1-5.
9. Tyler Wall and Torin Monahan, "Surveillance and violence from afar: The politics of drones and liminal security-scapes", 2011, *Theoretical Criminology*, Vol 15, Issue 3, pp. 239-254
10. Torrieri, D. J., "Principles of military communication systems", Dedham, MA, Artech, 1981. 340 p., 1981
11. Hutter, M. Scurek, R., *Possibilities of misuse of unmanned aerial vehicles (UAVs) are terrorist targets*, *Scientific works of the Academy Jan Długosz in Częstochowa. Technology, , Information Technology, Security Engineering*, (2016), Vol. 4, pp. 195-202