Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Counter-Unmanned Aerial Systems

To cite this article: D. Mototolea, A. Mîndroiu, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 192-195.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-026

Counter-Unmanned Aerial Systems

Dan Mototolea[1], Adelina Mîndroiu[1]
[1]"Ferdinand I" Military Technical Academy, Bucharest, Romania

E-mail: mototoleadan@gmail.com

Abstract. Counter-unmanned aerial systems (C-UAS), or counter-drone technology, refers to complex systems that are used to detect, locate, track and take over/down unmanned aerial vehicles. The proliferation of C-UAS technology accelerates due to the increasing number of incidents with commercially available drones that happen almost daily around the globe. This paper provides a background on how the technology works, when is applicable and what are the ups and downs.

1. Introduction

Low, small and slow (LSS) unmanned aerial systems (UAS) – commonly known as drones – are developing at an incredible speed. UASs are no longer associated only with the military. The use of drones offers opportunities for sectors like Agriculture, Disaster Relief, Security, Inspection, Mapping, Building and Journalism [1].

At the moment, more than 3 milion drones are sold per year through online shops around the world. It is expected that global drone-enabled services revenue will increase to $8.7 billion by 2025.

The explosion of these small cost and easily operated flying vehicles represents a new type of challenge for the protection of private and public spaces. Drones represent the traditional dual-use technology that, while providing considerable benefits, could also be adopted for hostile intents. Whether they are used by hobbyists or by terrorists, small drones represent a safety or security threat because they either can be misused or easily transformed into dangerous weapons. Drones are difficult to detect and are capable of carrying payloads up to a few kilograms. Not only that they represent a significant threat for civil entities, but for military as well. Several cases of drone attacks were reported in Syria and Ukraine.

C-UAS refers to systems used to detect, intercept and counter these types of threats. The growth of C-UAS market and development is proportional with the increase number of drones that are sold around the globe.

A variety of technologies were developed to detect and counter drones over the last few years. Each approach has its own limitations. It has been demonstrated over the years that there is no system which could offer 100% successful rate for detection and stopping the drone. A good C-UAS system contains more than one sensor for detection and also, employs more than one method for countering the drone.

Incidents with commercially available drones appear almost daily in the media [2]. In figure 1 we can see that there are drone related incidents (from smuggling of forbidden substances to spying and attacks) all around the world.

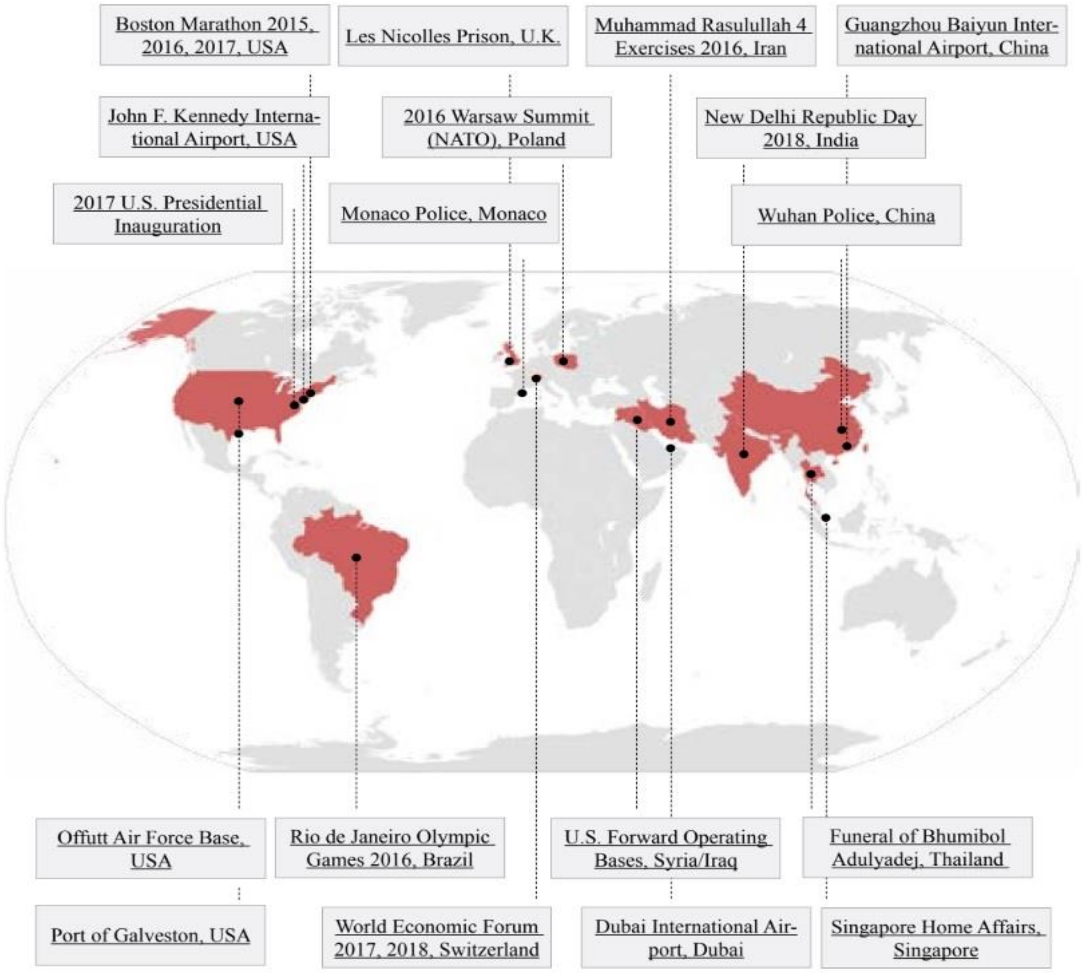
Boston Marathon 2015, 2016, 2017, USA
Les Nicolles Prison, U.K.
Muhammad Rasulullah 4 Exercises 2016, Iran
Guangzhou Baiyun International Airport, China
John F. Kennedy International Airport, USA
2016 Warsaw Summit (NATO), Poland
New Delhi Republic Day 2018, India
2017 U.S. Presidential Inauguration
Monaco Police, Monaco
Wuhan Police, China
Offutt Air Force Base, USA
Rio de Janeiro Olympic Games 2016, Brazil
U.S. Forward Operating Bases, Syria/Iraq
Funeral of Bhumibol Adulyadej, Thailand
Port of Galveston, USA
World Economic Forum 2017, 2018, Switzerland
Dubai International Airport, Dubai
Singapore Home Affairs, Singapore

Figure 1: Drone related incidents around the globe [3]

The most popular methods for countering the drone include shooting nets, the usage of lasers, spoofing GPS to confuse the drone's localization system, hijacking the software of drones by hacking into them, even training eagles to attack and disable drones.

The detection part includes the use of microphones, cameras or radars to sense the presence of drones. Each approach has its ups and downs.

This article provides a background on the technologies and methods used for detection, interception and countering LSS UASs.

2. Techniques used for detection and tracking

Different techniques have been studied, implemented and applied in C-UASs for detection and tracking. Most popular are: audio detection, video/ thermal detection, active and passive radar. In order to increase the rate of detection, different detection techniques need to be implemented simultaneously in the same system.

2.1 Audio detection

The noise from the propellers and from the motors can be used for detection. These are the main sources of acoustic waves in UASs. Using microphones, arrays of microphones and acoustic cameras can be a passive and at the same time relatively cheap solution for detection and tracking. Usually, the performances of an acoustic system can achieve a maximum of 300m. Modern techniques employ machine learning techniques in order to prevent false alarms. Audio techniques are mostly used combined with some other type of detection technique. Audio detection cannot be used to track target easily or accurately; it can only detect the presence of a drone in the vicinity of the system. The biggest drawback in using audio sensors is that it cannot be used in noisy environments (stadiums, concerts, etc).

Nonetheless, audio sensors for detecting small drones are already commercially available and integrated with other common detection approaches as multi-sensor drone trackers that can use optical, thermal, infrared and RF array of sensors.

2.2 Video detection

Video processing techniques provide also a relatively short-range detection. It does not work well in misty, foggy conditions and at night.

Because drones (especially quadcopters) fly at low speed, cameras have difficulty distinguishing between drones and birds, especially when the birds are gliding. This sometimes triggers an unacceptably high rate of false alarms. However, with the use of artificial intelligence algorithms the systems are able to differentiate drones from birds. The most advanced video processing techniques use frames of images and utilise algorithms of detection for interest points that are scale invariant (from the early Scale Invariant Feature Transform (SIFT) to the histogram of oriented gradients (HOG) and to the newest types of Convolutional neural networks (CNNs)).

2.3 Thermal detection

Thermal detection has a small range and is subjected to weather conditions. Small electrically powered multirotor UAVs can be detected with low-cost thermal sensor in some conditions. Main source of heat are batteries, not motors. Thermal shielding of the electric motors can degrade the effectiveness of thermal sensors. Most drones are built of plastic and carbon fibre materials; therefore, the detection is found to be problematic. Infrared cameras are more likely to pick up small birds due to their large thermal signatures, thus potentially causing a high rate of false alarm. Again, this type of detection must employ artificial intelligence algorithms in order to make the system reliable.

2.4 Radar detection

In order to be detected by the radar, the signals have to be strong enough in comparison to the noise. This is why the signal to noise-ration (SNR) is a key factor when talking about detecting drones. The SNR needs to be greater than 15dB in order to provide detection with acceptable false alarm rate.

Conventional radar systems for drone detection are available on the market. These systems can detect drones which have radar cross-section (RCS) the size of small birds (0.01 m2) at a range up to few kilometres. Usually, these are millimetric wave radars that use the frequency-modulated continuous-wave technique (FMCW).

The cost of this type of system, the radiation health concerns and the costs of operating and maintaining these types of sensors have to be taken in consideration when planning to purchase a radar - based counter drone system.

2.5 Passive RF detection

Another method of detection is to eavesdrop on the UAS communication. By measuring the propagation direction (measured as the Angle of Arrival (AOA) at the receiver), the propagation attenuation (measured as the Received Signal Strength (RSS)) or the propagation delay (measured as the Time of Arrival (TOA)) one can simply estimate the position of the drone. This type of detection is one of the most common one.

3. Techniques used for countering the drone

Just as there are multiple drone detection techniques, there are also multiple drone countermeasures.

Counter-drone measures can be divided into:

- Geo-fencing;
- Passive measures;
- Active measures;

3.1 Geo-fencing

Geo-fencing represents a virtual barrier which interdicts the flight of drones in certain areas. This is done either in software, using the GPS modules, or using RFID tags. Geo-fencing is useful to prevent drones from flying into fixed areas known a priori as sensitive. Not all drones have this capability.

3.2 Passive measures

Passive measures include spotting the drone and protecting the area of interest (closing the gates, moving sensible materials) by using only your own personnel (no equipment is used).

3.3 Active measures

Active Countermeasures include:

Jammers, Spoofers

Jamming or spoofing a drone’s radio connection or GPS signal is currently the most effective active countermeasure used. This will cause the drone to either return to its starting position, sheer away, land or crash.

The biggest drawback of this method is that it can affect other radio and GPS connections in the vicinity and it cannot be effective on pre programmed drones. The use of this type of countermeasure is subjected to approval by local authorities.

Firearms, electromagnetic pulse (EMP), laser

Drones can also be taken down using firearms, electromagnetic pulse (EMP) weapons, lasers. In this case, the drone is destroyed and crashes. These are military technologies and therefore not applicable for scenarios outside the warzone.

Net canon

The final active countermeasure, the use of nets, offers the benefit of stopping drones with minimum collateral damages. It involves shooting a net over the drone from the ground (with net cannon). This approach brings some disadvantages in that it is only effective at low range and has a low success rate.

4. Conclusions

The rapid growth of C-UAS technology accelerates due to the increasing number of incidents with commercially available drones that happen around the globe.

Every technique has its ups and downs. In order to increase the rate of detection, different techniques need to be implemented simultaneously in the same system. Artificial intelligence algorithms had become a necessity and they need to be implemented in every modern C-UAS.

The use of C-UAS is subjected to approvals from legal entities. The users have to take into account legalities associated with the airspace around them.

No single response is ideal for every threat, this is why the future users of C-UAS should address experts in this field prior of using such system.

References

[1] Gerton de Goeij, Eildert H. van Dijken, Frank Brouwer, “Research into the Radio Interference Risks of Drone”, Vianen, NL, May 2016.

[2] https://en.wikipedia.org/wiki/List_of_UAV-related_incidents

[3] Arthur Holland Michel, COUNTER-DRONE SYSTEMS, February 2018.