Ελληνικό Μεσογειακό Πανεπιστήμιο

(ΕΛΜΕΠΑ)



Τμήμα Ηλεκτρονικών Μηχανικών

Πρόγραμμα Μεταπτυχιακών Σπουδών "Ηλεκτρονικά Συστήματα Τηλεπικοινωνιών & Αυτοματισμών" (ΗΣΤΑ)

Μεταπτυχιακή Διατριβή

Μέθοδοι Αντιμετώπισης Μη Επανδρωμένων Αεροσκαφών

Γεώργιος Μεσαρχάκης

ΑΜ: MT123

Επιβλέπων Καθηγητής: Ευάγγελος Κόκκινος

Χανιά, Απρίλιος 2024

Hellenic Mediterranean University

(HMU)



Department of Electronic Engineering

MSc in Telecommunication & Automation Systems (TeleAutoS)

Master Thesis

Methods of countering Unmanned Aircraft Vehicles

Georgios Mesarchakis

MT123

Thesis Supervisor: Evangelos Kokkinos

Chania, April 2024

Copyright © Γεώργιος Μεσαρχάκης, 2024.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Ιδρύματος.

Ευχαριστίες

Στο σημείο αυτό, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου Δρ. Ευάγγελο Κόκκινο, τόσο για την ανάθεση της εκπόνησης της συγκεκριμένης διπλωματικής εργασίας όσο και για την αμέριστη κατανόηση που επέδειξε καθ' όλη τη διάρκεια αυτής αλλά και για τον πολύτιμο χρόνο του που αφιέρωσε προκειμένου να διορθώσει την εργασία.

Θα ήθελα επίσης να ευχαριστήσω όλους τους καθηγητές μου για την εμπειρία και τις γνώσεις που μου χάρισαν κατά τη διάρκεια των σπουδών μου στο Μεταπτυχιακό Πρόγραμμα.

Τέλος , ευχαριστώ την σύζυγό μου Χριστίνα για την κατανόηση και την υπομονή που επέδειξε κατά τη διάρκεια των σπουδών μου.

ΣΥΝΟΨΗ

Τα τελευταία χρόνια, τα drones έχουν γνωρίσει τεράστια ανάπτυξη. Λόγω της χαμηλής τιμής και της ευκολίας στην χρήσης τους, χρησιμοποιούνται ευρέως σε πολλές εφαρμογές, ωστόσο η χρήση τους για κακόβουλες ενέργειες έχει αυξηθεί σημαντικά τα τελευταία χρόνια. Για τον μετριασμό αυτών των απειλών είναι απαραίτητο να αναπτυχθούν σε ευαίσθητες περιοχές συστήματα anti-drone ή αλλιώς C-UAS (Counter Unmanned Aerial System). Η παρούσα διπλωματική εργασία παρουσιάζει μεθόδους για τον εντοπισμό των drones, δίνοντας έμφαση στα χαρακτηριστικά των περισσότερων μεθόδων εντοπισμού, όπως ο εντοπισμός με την χρήση ραντάρ, ραδιοσυχνοτήτων, ο ηχητικός εντοπισμός, ο εντοπισμός με την χρήση καμερών καθώς και με την χρήση αλγορίθμων [35]. Στόχος της ανάλυσης που πραγματοποιείται είναι η διαμόρφωση κατευθυντήριων γραμμών για την επιλογή των κατάλληλων μεθόδων που θα χρησιμοποιηθούν κατά περίπτωση για τον εντοπισμό των drones. Επιπρόσθετα, η εργασία παραθέτει συστήματα anti-drone για την αντιμετώπιση και την καταστολή των πιθανών απειλών πέραν του εντοπισμού τους. [34]

Λέξεις κλειδιά: Μη Επανδρωμένο Αεροσκάφος, drone, UAV, anti-drone, C-UAS, μέθοδοι αντιμετώπισης, παρεμβολές, GPS spoofing

ΠΕΡΙΛΗΨΗ

Η χρήση των Μη Επανδρωμένων Αεροσκαφών, γνωστών και ως drones, αναπτύσσεται με ταχύτατους ρυθμούς τα τελευταία χρόνια, εξυπηρετώντας μια μεγάλη γκάμα μη στρατιωτικών εφαρμογών. Ωστόσο, η χρήση των drones, για κατασκοπεία, τρομοκρατία ή άλλες κακόβουλες ενέργειες, έχει οδηγήσει σε ραγδαία ανάπτυξη τον τομέα της έρευνας για τον εντοπισμό και την αντιμετώπιση μια απειλής από drones.

Ο σκοπός της διπλωματικής εργασίας είναι η παρουσίαση των κατάλληλων μεθόδων που θα χρησιμοποιηθούν τόσο για τον εντοπισμό των drones όσο και για την αντιμετώπιση των πιθανών απειλών.

Το 1ο κεφάλαιο αποτελεί ένα εισαγωγικό κομμάτι στα drones μέσω της παρουσίασης των όρων που χρησιμοποιούνται στον τομέα αυτόν, της ιστορίας των drones, των πεδίων εφαρμογής τους, και του ισχύοντος κανονιστικού πλαισίου σχετικά με τη χρήση τους.

Το 2ο κεφάλαιο παρουσιάζει τις κατηγορίες των μη επανδρωμένων αεροσκαφών και των συστημάτων τους καθώς και τα είδη των εμπορικών drones και του εξοπλισμού που αυτά χρησιμοποιούν.

Το 3ο κεφάλαιο αφιερώνεται στους κινδύνους που έχουν προκύψει από την ευρεία χρήση των drones καθώς και των μελλοντικών προκλήσεων από την αυξανόμενη παραγωγή και βελτίωσή τους.

Στο 4ο κεφάλαιο παρουσιάζονται οι μέθοδοι εντοπισμού και αντιμετώπισης μιας ενδεχόμενης απειλής από drone καθώς και οι εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα συστήματα αυτά.

Τέλος, στο 5ο κεφάλαιο παρουσιάζονται συμπεράσματα που προέκυψαν από την εργασία και γίνονται προτάσεις για μελλοντική διερεύνηση.

ABSTRACT

In recent years, drones have experienced tremendous growth. Due to their low price and ease of use, they are widely used in many applications, however their use for malicious activities has increased significantly lately. To mitigate these threats it is necessary to deploy anti-drone systems or C-UAS (Counter Unmanned Aerial System) in sensitive areas. This thesis presents methods for the detection of drones, emphasizing the characteristics of most detection methods, such as detection using radar, RF detection, acoustic detection, optical and thermal detection using cameras as well as detection using algorithms. The aim of the analysis is to formulate guidelines for the selection of appropriate methods to be used on a case-by-case basis for the tracking of drones. In addition, the paper lists anti-drone systems to counter and suppress potential threats beyond their detection.

Keywords: Unmanned Aerial Vehicle, drone, UAV, anti-drone, C-UAS, countermeasures, jamming, GPS spoofing

SUMMARY

The use of Unmanned Aerial Vehicles, also known as drones, has been growing rapidly in recent years, serving a wide range of civilian applications. However, the use of drones, for espionage, terrorism or other malicious activities, has led to rapid growth in the field of research to detect and counter a threat from drones.

The purpose of this thesis is to present the appropriate methods to be used for both the detection of drones and the countering of potential threats.

Chapter 1 is an introduction to drones through the presentation of the terms used in this field, the history of drones, their fields of application, and the current regulatory framework regarding their use.

Chapter 2 presents the categories of drones and their systems as well as the types of commercial drones and the equipment they use.

Chapter 3 is devoted to the risks that have arisen from the widespread use of drones and the future challenges arising from their increasing production and improvement.

Chapter 4 presents the methods of detecting and countering a potential drone threat as well as the applications in which these systems can be used.

Finally, Chapter 5 presents the conclusions drawn from the thesis and makes recommendations for future investigation.

Πίνακας Περιεχομένων

1. ΕΙΣΑΓΩΓΗ ΣΤΑ DRONES 29

1.1 Όροι – Ορισμοι 29
1.1.1 Μη Επανδρωμένο Αεροσκάφος (Unmanned Aerial Vehicle) 29
1.1.2 Σύστημα Μη Επανδρωμένου Αεροσκάφους (Unmanned Aircraft System) 29
1.2 Συντομη ιστορικη αναδρομη 30
1.2.3 Το πρώτο ξεκίνημα 31
1.2.4 Η γέννηση των μη επανδρωμένων αεροσκαφών 36
1.2.5 Η εμπορευματοποίηση στα τέλη του 20ου αιώνα 40
1.2.6 Η έλευση των τετρακοπτέρων και των πολυκόπτερων 41
1.3 Πεδια εφαρμογης 43
1.3.1 Στρατιωτική χρήση των UAS 43
1.3.2 Χρήση των UAS στο αστικό περιβάλλον 45
1.3.2.1 Κατηγορίες εφαρμογών 46
1.4 Νομοθεσια περι πολιτικης χρησης των drones 48

2. ΚΑΤΗΓΟΡΙΕΣ ΚΑΙ ΕΞΟΠΛΙΣΜΟΣ 50

2.1 Κατηγοριες μη επανδρωμενων αεροσκαφων 50
2.2 Συνθεση συστηματος μη επανδρωμενου αεροσκαφους (UAS) 52
2.2.1 Χαρακτηριστικά των υποσυστημάτων 53
2.3 Εμπορικα drones και εξοπλισμος 54
2.3.1 Πολυκόπτερα 54
2.3.1.1 Γρήγορο nano-quadcopter 55
2.3.1.2 Γρήγορο micro-drone με κάμερα υψηλών επιδόσεων 55
2.3.1.3 Micro-drone με κάμερα και οπτικό ζουμ 56
2.3.1.4 Μικρό επαγγελματικό drone πολλαπλών χρήσεων 56
2.3.1.5 Μικρό γεωργικό drone 57
2.3.2 Άτρακτος / Σκελετός 57
2.3.3 Ελεγκτής πτήσης (flight controller) 58
2.3.4 Κινητήρες 59
2.3.5 Ηλεκτρονικός ελεγκτής ταχύτητας (Electronic Speed Controller - ESC) 60
2.3.6 Τηλεχειρισμός (πομπός και δέκτης) 61
2.3.7 Μπαταρία 62
2.3.8 Gimbal 63
2.4 Αισθητηρες εμπορικων drones 64
2.4.1 Μονάδα αδρανειακής μέτρησης (IMU) 64
2.4.2 Αισθητήρας υψομέτρου 65
2.4.2.1 Υπέρυθρες 66
2.4.2.2 Βαρομετρικός αισθητήρας 66
2.4.2.3 GPS 66
2.4.3 Κάμερα 67
2.4.4 Εικονοληπτικοί αισθητήρες 68
2.4.5 Radar 69
2.4.6 LiDAR 70
2.4.7 Σόναρ 71

3. ΚΙΝΔΥΝΟΙ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ 73

3.1 Ατυχηματα 73
3.2 Ηθικη και δεοντολογια 74
3.3 Προστασια προσωπικων δεδομενων 75
3.4 Εθνικη ασφαλεια 76
3.4.1 Τρομοκρατικές ενέργειες 76
3.4.2 Αεροδρόμια 77
3.5 Μελλοντικες προκλησεις 77
3.5.1 Μεγαλύτερη εμβέλεια 77
3.5.2 Ρομποτικά πτηνά 78
3.5.3 Μικροσκοπικά drones 78
3.5.4 Σμήνη από drones 79

4. ΑΝΤΙΜΕΤΩΠΙΣΗ ΑΠΕΙΛΩΝ 80

4.1 Μεθοδοι εντοπισμου drone 80
4.1.5 Εντοπισμός με ραντάρ 81
4.1.5.1 Παλμικό ραντάρ 82
4.1.5.2 Ραντάρ συνεχούς κύματος με διαμόρφωση συχνότητας (Frequency Modulated Continuous Wave Radar - FMCW) 83
4.1.5.3 Ραντάρ FMCW υψηλής συχνότητας 84
4.1.5.4 Doppler ραντάρ 84
4.1.5.5 Παθητικό ραντάρ 86
4.1.6 Εντοπισμός ραδιοσυχνοτήτων 88
4.1.7 Ηχητικός εντοπισμός 90
4.1.7.1 Ανάλυση σήματος ήχου 91
4.1.8 Εντοπισμός με κάμερες 92
4.1.9 Εντοπισμός με θερμικές κάμερες 94
4.1.10 Εντοπισμός με την χρήση αλγορίθμων 95
4.1.11 Συνδυασμός μεθόδων 95
4.2 Μεθοδοι αντιμετωπισης 95
4.2.1 Παρεμβολή σήματος (Jamming) 96
4.2.1.1 Παρεμβολή σήματος RF 97
4.2.1.2 Παρεμβολή σήματος GPS 98
4.2.1.3 Τεχνικές παρεμβολής 102
4.2.2 GPS Spoofing 106
4.2.2.1 Απλή επίθεση 108
4.2.2.2 Μεσαίας κλίμακας επίθεση 109
4.2.2.3 Σύνθετη επίθεση 109
4.2.2.4 Χαρακτηριστικά των εμπορικών συστημάτων παρεμβολής 109
4.2.3 Άλλες μέθοδοι 110
4.2.3.1 Κατάρριψη του drone 110
4.2.3.2 Καταστροφή του drone 110
4.3 Εφαρμογες 111
4.3.1 Αεροδρόμια 111
4.3.2 Φυλακές 112
4.3.3 Στάδια 113
4.3.4 Αστυνομία 113
4.3.5 Ένοπλες δυνάμεις 113
4.3.6 Βιομηχανική κατασκοπεία 114

5. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ 115

5.1 Συμπερασμα 115

5.2 ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ 116

Κατάλογος Εικόνων

Εικόνα 1.1 Το γυροσκόπιο του Λεονάρντο Ντα Βίντσι 32
Εικόνα 1.2 Navicella Volante του Λεονάρντο Ντα Βίντσι. 33
Εικόνα 1.3 Το αερόστατο των αδερφών Μοντγκολφιέ. 33
Εικόνα 1.4 Ο βομβαρδισμός της Βενετίας.....34
Εικόνα 1.5 Το ελικόπτερο του Ενρίκο Φορλανίνι 35
Εικόνα 1.6 Το αεροπλάνο των αδερφών Ράιτ.....36
Εικόνα 1.7 Το πρώτο ηλεκτρονικό τηλεχειριστήριο 37
Εικόνα 1.8 Hewitt-Sperry Automatic Airplane 38
Εικόνα 1.9 Radioplane OQ-2.....38
Εικόνα 1.10 Ryan 147B πάνω σε DC-130A.....39
Εικόνα 1.11 MQ-1 Predator.....40
Εικόνα 1.12 Parrot AR.Drone.....42
Εικόνα 1.13 DJI Phantom 1 43
Εικόνα 1.14 Μελλοντικός ρόλος των UAVs στο θέατρο επιχειρήσεων 45
Εικόνα 1.15 Κατηγορίες αδειών χειριστών 48
Εικόνα 2.1 Δομή ενός UAS 52
Εικόνα 2.2 Εναλλακτική δομή ενός UAS.....53
Εικόνα 2.3 Επικοινωνίες ενός UAS.....54
Εικόνα 2.4 Draco drone 55
Εικόνα 2.5 DJI Phantom 4 pro.....56
Εικόνα 2.6 Walkera Voyager 5.....56
Εικόνα 2.7 ProDrone PD6B-AW.....57
Εικόνα 2.8 DJI Agras MG-1 57
Εικόνα 2.9 Άτρακτος ενός VTOL drone.....58
Εικόνα 2.10 Ελεγκτής πτήσης DJI A2.....59
Εικόνα 2.11 Brushless DC motor 60
Εικόνα 2.12 Drone motor.....60
Εικόνα 2.13 Ρύθμιση ταχύτητας για την επίτευξη της επιθυμητής κίνησης 61
Εικόνα 2.14 Πομπός και δέκτης 62
Εικόνα 2.15 DJI Mavic Pro - 3830 mAh LiPo Battery.....63
Εικόνα 2.16 Gimbal.....64
Εικόνα 2.17 IMU 65
Εικόνα 2.18 Αισθητήρας υψομέτρου.....65
Εικόνα 2.19 GPS.....67
Εικόνα 2.20 Κάμερα 68
Εικόνα 2.21 Synthetic Aperture Radar 70
Εικόνα 2.22 LiDAR.....71
Εικόνα 2.23 Σόναρ.....72
Εικόνα 4.1. Σύγκριση μεθόδων εντοπισμού [35].....81
Εικόνα 4.2 Λήψη ενός Doppler ραντάρ.....85

Εικόνα 4.3 Επεξεργασία σήματος παθητικού ραντάρ [39].....86
Εικόνα 4.4 Παρεμβολή ενός drone με φορητό παρεμβολέα.....96
Εικόνα 4.5 Η επίδραση διαφόρων παρεμβολέων σε δέκτες GPS.....100
Εικόνα 4.6 Κατηγοριοποίηση παρεμβολέων 102
Εικόνα 4.7 Barrage jamming 103
Εικόνα 4.8 Tone jamming.....104
Εικόνα 4.9 Sweep jamming 105
Εικόνα 4.10 Protocol-Aware jamming 106
Εικόνα 4.11 Παρεμβολή ενός drone με την μέθοδο του GPS Spoofing.....107

Κατάλογος Πινάκων

Πίνακας 4.1 Χαρακτηριστικά των drones και μέθοδοι εντοπισμού.....80

Συντομογραφίες

ΞΕΝΕΣ ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

AGL (Above Ground Level)

AWGN (Additive White Gaussian Noise)

BLOS (Beyond Line of Sight)

C/A (Coarse/Acquisition)

CCTV (Closed-Circuit Television)

CPU (Central Processing Unit)

CS (Control Station)

CTR (Control Zone)

C-UAS (Counter Unmanned Aerial System)

CW (Continuous Wave)

DAGR (Drone Aware – GR)

DC (Direct Current)

DoD (Department of Defense)

EASA (European Aviation Safety Agency)

EMP (Electromagnetic Pulse)

ESC (Electronic Speed Controller)

FAA (Federal Aviation Administration)

FIR (Flight Information Region)

FMCW (Frequency Modulated Continuous Wave)

FRSS (Flight Regulation Support System)

GCS (Ground Control Station)

GDT (Ground Data Terminal)

GLONASS (Global Navigation Satellite System)

GPS (Global Positioning System)

GSM (Global System for Mobile communication)

HALE (High Altitude Long Endurance)

HAPs (High Altitude Platforms)

HD (High Definition)

ICAO (International Civil Aviation Organization)

IEEE (Institute of Electrical and Electronics Engineers)

IMU (Inertial Measurement Unit)

IR (InfraRed)

LAPs (Low Altitude Platforms)

LED (Light Emitting Diode)

LiDAR (Light Detection and Ranging)

LiPo (Lithium-Polymer)

LOS (Line of Sight)

LPC (Linear Predictive Coding)

LRS (Launch and Recovery System)

MAC (Media Access Control)

MALE (Medium Altitude Long Endurance)

MAV (Micro UAV)

MOSFET (Metal Oxide Semiconductor Field Effect Transistor)

MSL (Mean Sea Level)

MUAV (Mini UAV)

NAV (Nano Air Vehicles)

RADAR (Radio Detection And Ranging)

RCS (Radar Cross Section)

RF (Radio Frequency)

ROA (Remotely Operated Aircraft)

RPH (Remotely Piloted Helicopter)

RPV (Remotely Piloted Vehicle)

SDR (Software Defined Radio)

SMR (Surface Movement Radar)

SNR (Signal to Noise Ratio)

TDOA (Time Difference of Arrival)

TMA (Terminal Maneuvering Area)

TUAV (Tactical UAV)

UAS (Unmanned Aircraft System)

UAV (Unmanned Air Vehicle)

UCAR (Unmanned Combat Rotorcraft)

UCAV (Unmanned Combat Air Vehicle)

UMTS (Universal Mobile Telecommunications System)

VLOS (Visual Line of Sight)

VPS (Vision Positioning System)

VTUAV (Vertical Take-off UAV)

Wi-Fi (Wireless Fidelity)

WLAN (Wireless Local Area Network)

ΕΛΛΗΝΙΚΕΣ ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΕΕ (Ευρωπαϊκή Ένωση)

ΕΣΣΔ (Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών)

ΗΠΑ (Ηνωμένες Πολιτείες της Αμερικής)

ΣμηΕΑ (Συστήματα μη Επανδρωμένων Αεροσκαφών)

ΦΕΚ (Φύλλα Εφημερίδας της Κυβέρνησης)

1. ΕΙΣΑΓΩΓΗ ΣΤΑ DRONES

1.1 Όροι – Ορισμοί

1.1.1 Μη Επανδρωμένο Αεροσκάφος (Unmanned Aerial Vehicle)

Ως «Μη Επανδρωμένο Αεροσκάφος» νοείται κάθε αεροσκάφος που λειτουργεί ή έχει σχεδιαστεί για να λειτουργεί αυτόνομα ή να οδηγείται εξ αποστάσεως, χωρίς χειριστή επί του σκάφους. [1]

Το μη επανδρωμένο αεροσκάφος (UAV) είναι επίσης γνωστό και ως drone. Όρος που αναφέρεται σε μια ιπτάμενη μηχανή χωρίς ανθρώπινο πιλότο ή επιβάτες. Ως εκ τούτου, ο όρος «μη επανδρωμένο» υποδηλώνει την πλήρη απουσία ανθρώπου που κατευθύνει και πιλοτάρει ενεργά το αεροσκάφος. Οι λειτουργίες ελέγχου για τα μη επανδρωμένα αεροσκάφη μπορεί να είναι είτε επί του σκάφους είτε εκτός του σκάφους (τηλεχειρισμός). Για το λόγο αυτό χρησιμοποιούνται ευρέως και οι όροι τηλεχειριζόμενο αεροσκάφος (ROA) και τηλεχειριζόμενο όχημα (RPV). Ωστόσο, ο όρος UAV χρησιμοποιείται εδώ και αρκετά χρόνια για να περιγράψει αυτού του είδους τα μη επανδρωμένα εναέρια συστήματα. [2]

1.1.2 Σύστημα Μη Επανδρωμένου Αεροσκάφους (Unmanned Aircraft System)

Οι Κανονισμοί χρησιμοποιούν τον όρο UAS (Unmanned Aircraft System ή Σύστημα Μη Επανδρωμένου Αεροσκάφους) και αναφέρονται σε ένα σύστημα που αποτελείται από το μη επανδρωμένο αεροσκάφος και τον εξοπλισμό που χρησιμοποιείται για τον έλεγχο και τη λειτουργία του (π.χ. επίγειο σταθμό ελέγχου, πιθανό καταπέλτη για την εκτόξευσή του κ.α.). [1]

Οι πλέον καταξιωμένοι διεθνείς οργανισμοί, όπως ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (ICAO), το EUROCONTROL, ο Ευρωπαϊκός Οργανισμός Ασφάλειας της Αεροπορίας (EASA), η Ομοσπονδιακή Υπηρεσία Πολιτικής

Αεροπορίας (FAA), καθώς και το αμερικανικό Υπουργείο Άμυνας (DoD), υιοθέτησαν τον όρο UAS (Unmanned Aircraft System, Σύστημα Μη Επανδρωμένου Αεροσκάφους) ως τον ορθό και επίσημο όρο. Το ακρωνύμιο που υιοθετήθηκε οφείλεται στα ακόλουθα: [2]

- Ο όρος «μη επανδρωμένο» του UAS αναφέρεται στην απουσία πιλότου από το ιπτάμενο τμήμα του συστήματος.

- Ο όρος «αεροσκάφος» υποδηλώνει ότι το UAS είναι αεροσκάφος και ως εκ τούτου θα πρέπει να αποδεικνύεται η αξιοπλοΐμότητά του.

- Τέλος, ο όρος «σύστημα» εισήχθη λόγω του γεγονότος ότι το UAS δεν είναι απλώς ένα τηλεκατευθυνόμενο αεροσκάφος αλλά ένα σύστημα που αποτελείται από επίγειους σταθμούς ελέγχου, ασύρματες ζεύξεις επικοινωνίας και συστήματα εκτόξευσης και ανάκτησης.

1.2 Σύντομη ιστορική αναδρομή

Τα drones έχουν διανύσει πολύ δρόμο από την δημιουργία τους, εξελισσόμενα από όπλα που για τον πόλεμο σε μηχανές πολλαπλών χρήσεων που χρησιμοποιούμε τώρα για εξερεύνηση, φωτογραφία, ακόμη και για παράδοση δεμάτων, έχοντας επεκταθεί σε διάφορες βιομηχανίες και βρίσκοντας πολλαπλές εφαρμογές με την πάροδο του χρόνου.

Το ταξίδι των drones, όπως τα ξέρουμε σήμερα, ξεκίνησε στις αρχές του 20ου αιώνα με την ανάπτυξη του πρώτου αεροσκάφους χωρίς πιλότους. Ο Πρώτος Παγκόσμιος Πόλεμος πυροδότησε την ανάγκη για τεχνολογικές εξελίξεις στον πόλεμο, και αυτό οδήγησε στη δημιουργία του Kettering Bug , το οποίο ήταν ένα από τα πρώτα UAV που κατασκευάστηκαν ποτέ. Ωστόσο, μόνο μετά τον Δεύτερο Παγκόσμιο Πόλεμο τα drones χρησιμοποιήθηκαν ευρύτερα, ιδιαίτερα σε επιχειρήσεις επιτήρησης και αναγνώρισης. Καθώς η τεχνολογία των drones συνέχισε να εξελίσσεται μετά τους πολέμους, άρχισαν να κερδίζουν έδαφος και σε μη στρατιωτικούς τομείς. [3]

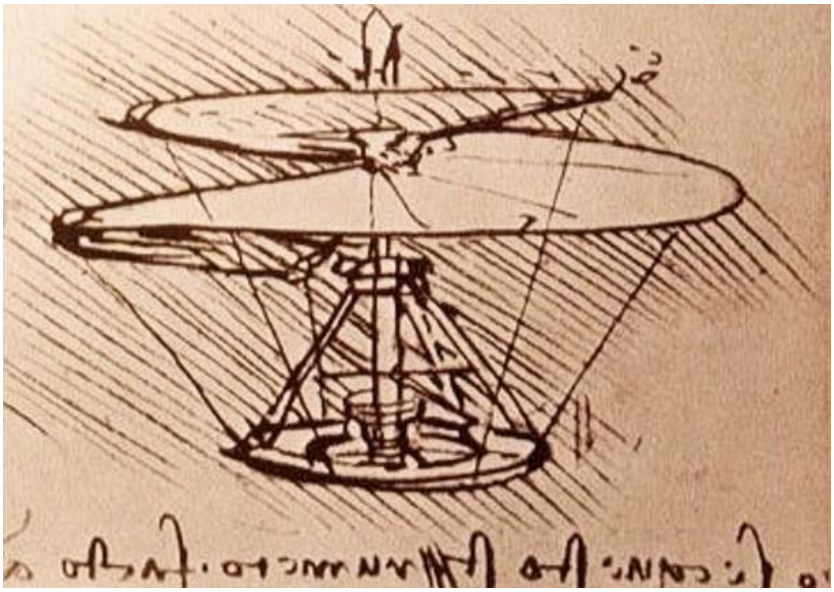
1.2.3 Το πρώτο ξεκίνημα

Η αρχή των πρώτων ιπτάμενων μηχανών έγινε 2500 χρόνια πριν στην Ελλάδα και στην Κίνα. Η δημιουργία της πρώτης αυτόνομης ιπτάμενης μηχανής της ανθρωπότητας αποδίδεται στον πυθαγόρειο φιλόσοφο και μαθηματικό Αρχύτα, από τον Τάραντα, ο οποίος ήταν ο πρώτος που εφάρμοσε μαθηματικές αρχές στη μηχανική και ο πρώτος που χρησιμοποίησε την αρχή της δράσης αντίδρασης πάνω στην οποία στηρίζεται η λειτουργία των πυραύλων και των αεριωθούμενων αεροπλάνων. [3]

Ο Αρχύτας το 425 π.Χ. ήταν αυτός που κατασκεύασε ένα μηχανικό, αεριοπροωθούμενο πουλί που το ονόμασε «περιστέρι». Ήταν μία μικρή ξύλινη συσκευή σε σχήμα αεροπλάνου και είχε στο εσωτερικό της μία κύστη ζώου σαν μπαλόνι, η οποία κατέληγε στο άκρο της συσκευής όπου συνδεόταν με αεραντλία. Κάθε φορά που η πίεση του αέρα περνούσε από αυτό το άνοιγμα, εκτοξευόταν λόγω του πεπιεσμένου αέρα που έβγαινε από πίσω με ορμή, λειτουργώντας σαν αεριωθούμενο αεροπλάνο βάσει της αρχής δράσης - αντίδρασης. Το «περιστέρι» πέταξε για πρώτη φορά γύρω στα 200 μέτρα. [4]

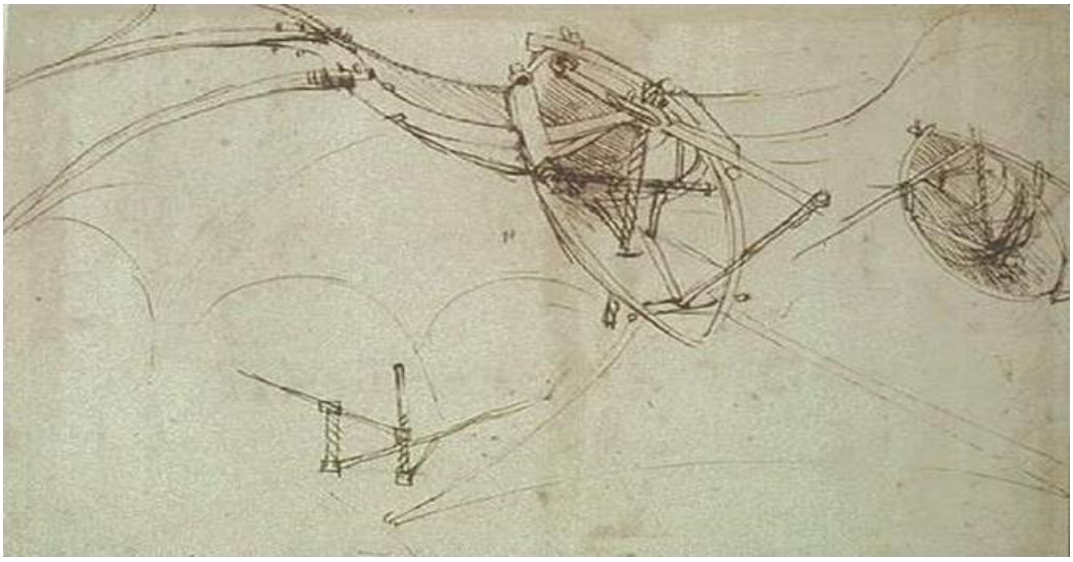
Την ίδια χρονική περίοδο, στην Κίνα, χαρταετοί και μπαλόνια πετούσαν με τη χρήση ζεστού αέρα. Αν και δημιουργήθηκαν κυρίως για ψυχαγωγία, εικάζεται πως χρησιμοποιήθηκαν και για στρατιωτικούς σκοπούς.

Το 1843, ο Λεονάρντο Ντα Βίντσι, βασιζόμενος στην βίδα (κοχλία) νερού που είχε κατασκευάσει ο Αρχιμήδης, δημιούργησε μια μηχανή ικανή να υπερίπταται, την αερική βίδα ή γυροσκόπιο, που θεωρείται κατά πολλούς ο πρόγονος του σημερινού ελικοπτέρου. Αποτελούνταν από μια ελικοειδή επιφάνεια διαμέτρου 5 μέτρων, κατασκευασμένη από σιδερένιο σύρμα και λινό η οποία στροβιλίζεται για να προκαλέσει ανύψωση. Ωστόσο, αν και στηρίζονταν σε ορθές αρχές της αεροδυναμικής, στερούνταν της κατάλληλης πηγής ενέργειας προκειμένου να ανυψωθεί. [4]



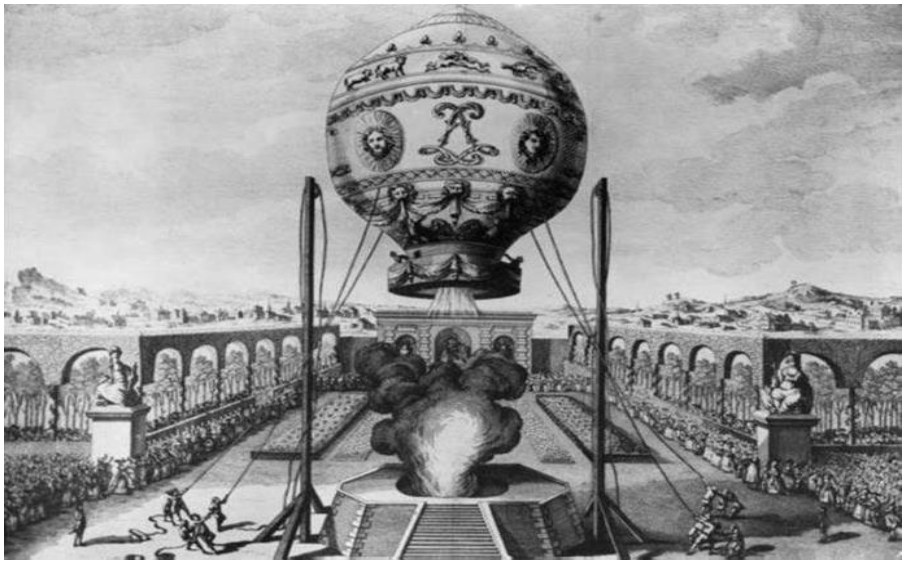
Εικόνα 1.1 *Το γυροσκόπιο του Λεονάρντο Ντα Βίντσι*

Ο Ντα Βίντσι αντιγράφοντας τα φτερά των νυχτερίδων και των μεγάλων πουλιών, σχεδίασε μηχανικά φτερά, τα οποία διαθέτουν αρθρωτή, αεροδυναμική δομή. Τα φτερά αυτά προσαρμόζονται πάνω στο ανθρώπινο σώμα, αποτελώντας προέκταση και κομμάτι αυτού. Η μυϊκή ανθρώπινη δύναμη παράγει την απαιτούμενη ενέργεια για να επιτευχθεί η κίνηση αυτών. Το πιο διάσημο ίσως σχέδιό του αποτελεί η περίφημη Navicella Volante, μία κατασκευή από ξύλο και ύφασμα, με άτρακτο ωοειδούς σχήματος, μέσα στην οποία βρίσκεται η θέση του «πιλότου», καθώς και οι μηχανισμοί πλοήγησης που ρυθμίζουν την κίνηση των δύο φτερών, όμοιων με φτερά νυχτερίδας. [4]



Εικόνα 1.2 *Navicella Volante του Λεονάρντο Ντα Βίντσι.*

Το 1783 αποτελεί χρονιά ορόσημο για την κατάκτηση των αιθέρων καθώς έχουμε την πρώτη γνωστή επανδρωμένη πτήση με το αερόστατο που κατασκεύασαν οι αδερφοί Μοντγκολφιέ. Στην πρώτη αυτή επανδρωμένη αποστολή μετέφεραν ένα νεαρό γιατρό και ένα αξιωματικό του στρατού.



Εικόνα 1.3 *Το αερόστατο των αδερφών Μοντγκολφιέ.*

Τα drones, όπως και πολλές άλλες σημαντικές τεχνολογικές καινοτομίες, εφευρέθηκαν προς εξυπηρέτηση στρατιωτικών επιχειρήσεων. Η πρώτη καταγεγραμμένη ιστορικά χρήση ιπτάμενων μέσων που θεωρείται ως λειτουργία

drone συνέβη το 1849 όταν οι Αυστριακοί εκτόξευσαν 200 μη επανδρωμένα αερόστατα εξοπλισμένα με βόμβες για να πλήξουν τη Βενετία. [5]



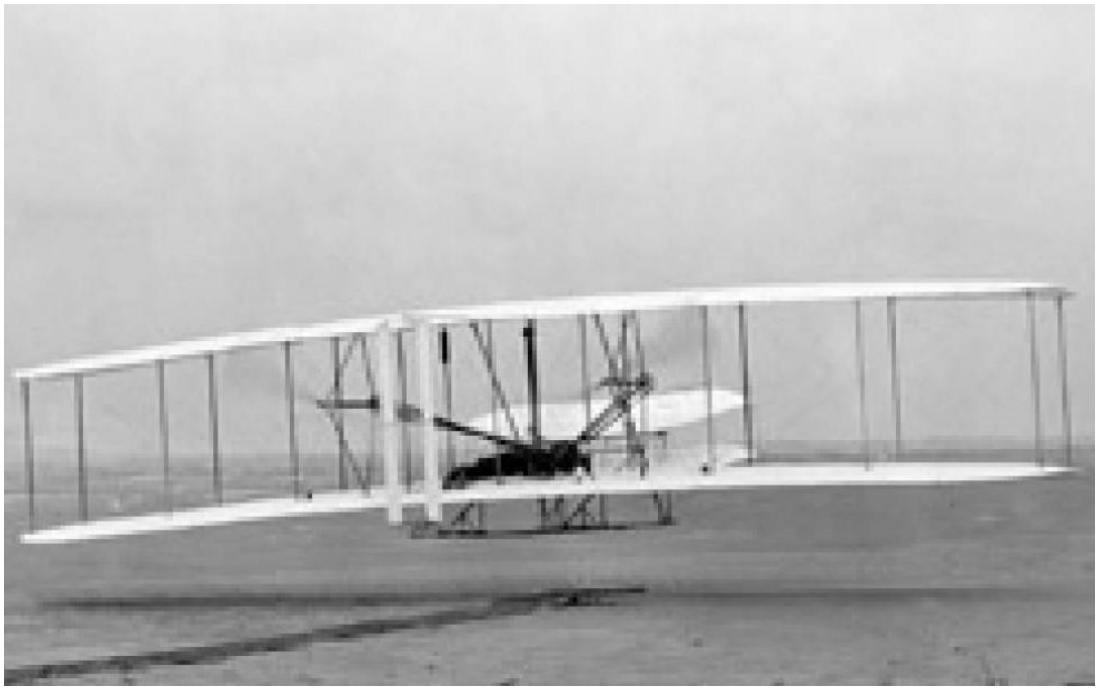
Εικόνα 1.4 *Ο βομβαρδισμός της Βενετίας*

Το πρώτο μη επανδρωμένο όχημα που χρησιμοποιήθηκε για μη στρατιωτικούς σκοπούς ήταν η κατασκευή του Ενρίκο Φορλανίνι το 1877. Πρόκειται για ένα πρώιμο μοντέλο ελικοπτέρου το οποίο τροφοδοτούνταν από μια ατμομηχανή. Έφτασε σε ύψος 13 μέτρων, όπου παρέμεινε για περίπου 20 δευτερόλεπτα, μετά από κατακόρυφη απογείωση από πάρκο του Μιλάνο. Ωστόσο δεν είχε ευστάθεια και δεν υπήρχε η δυνατότητα να πηδαλιουχηθεί.



Εικόνα 1.5 *Το ελικόπτερο του Ενρίκο Φορλανίνι*

Στις 17 Δεκεμβρίου του 1903, πραγματοποιείται η πρώτη ελεγχόμενη, μηχανικά προωθούμενη και με διάρκεια, βαρύτερη από τον αέρα, ανθρώπινη πτήση. Οι Όρβιλ και Γουίλμπορ Ράιτ κατασκεύασαν το πρώτο αεροπλάνο στον κόσμο, το διπλάνο Flyer, με το οποίο κατάφεραν να πραγματοποιήσουν την πρώτη ελεγχόμενη, μηχανικά προωθούμενη και βαρύτερη από τον αέρα πτήση. Με το διπλάνο τους Flyer 1, κατάφεραν να πραγματοποιήσουν τέσσερις συνολικά πτήσεις διάρκειας 12, 13, 15 και 59 δευτερολέπτων. Στην τελευταία πτήση διένυσαν απόσταση 260 μέτρων. Μέσα στα επόμενα δύο χρόνια, το αεροπλάνο των αδερφών Ράιτ εξελίσσεται στο πρώτο αεροσκάφος σταθερής πτέρυγας, το οποίο θα μπορούσε να κατευθυνθεί με επιτυχία.

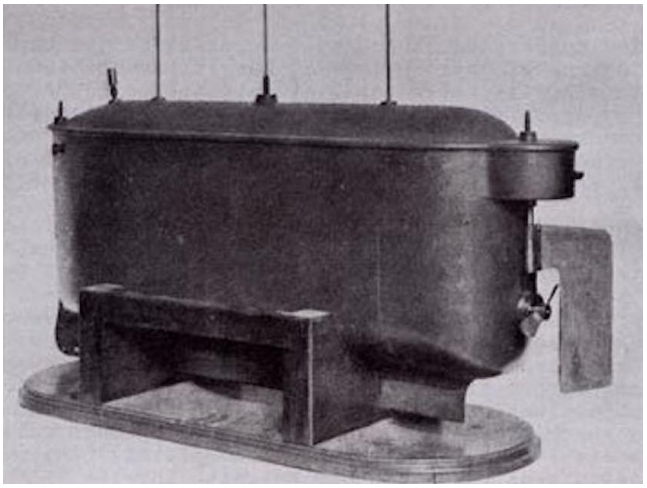


Εικόνα 1.6 *Το αεροπλάνο των αδερφών Ράιτ.*

1.2.4 Η γέννηση των μη επανδρωμένων αεροσκαφών

Μετά και την ανακάλυψη των αδερφών Ράιτ, το ενδιαφέρον στράφηκε στην κατασκευή επανδρωμένων αεροσκαφών ενώ τα μη επανδρωμένα αεροσκάφη είχαν να αντιμετωπίσουν πολλές τεχνολογικές προκλήσεις. Κυριότερες από αυτές, ήταν ο απομακρυσμένος έλεγχος του αεροσκάφους.

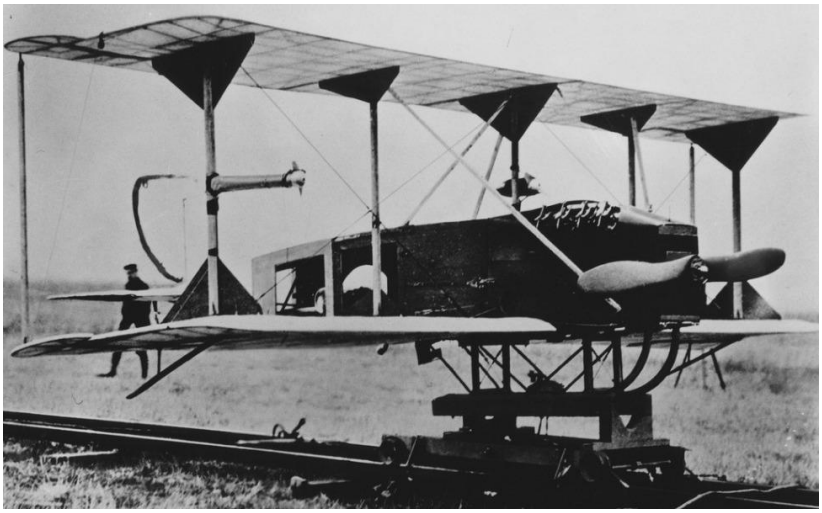
Απάντηση σε αυτή την πρόκληση δόθηκε από το Nikola Tesla, ο οποίος αρχικά επέτυχε την ασύρματη επικοινωνία (1893), ενώ το 1898 σε έκθεση στην πλατεία Madison Square Garden της Νέας Υόρκης παρουσίασε το πρώτο τηλεκατευθυνόμενο εναέριο όχημα το οποίο κινούταν μέσω ραδιοκυμάτων. Αργότερα, το ίδιο έτος, κατέθεσε δίπλωμα ευρεσιτεχνίας που περιγράφει λεπτομερώς τη νέα του συσκευή για τον έλεγχο της κίνησης ενός οχήματος με ραδιοσυχνότητες. Αυτή η συσκευή του Τέσλα αποτελεί και το πρώτο ηλεκτρονικό τηλεχειριστήριο. [6]



Εικόνα 1.7 *Το πρώτο ηλεκτρονικό τηλεχειριστήριο*

Το έργο του Tesla έθεσε τις βάσεις για τη ανάπτυξη των στρατιωτικών μη επανδρωμένων αεροσκαφών από βρετανικές αλλά και αμερικανικές ομάδες. Το 1916, ο Βρετανός λοχαγός Archibald Low δημιούργησε ένα ξύλινο μη επανδρωμένο αεροσκάφος εξοπλισμένο με εκρηκτικές κεφαλές που ήταν γνωστό ως «ιπτάμενος στόχος» και το οποίο εξελίχθηκε και χρησιμοποιήθηκε για να επιφέρει πλήγματα εναντίον των Ζέπελιν. [7]

Την ίδια εποχή, ένα άλλο δημιούργημα που άνοιξε το δρόμο ήταν το Hewitt-Sperry Automatic Airplane, γνωστό και ως "Flying Bomb" ή "Aerial Torpedo", καθώς μπορούσε να διανύσει μια απόσταση 50 μιλίων μεταφέροντας μια βόμβα 300 λιβρών χωρίς χειριστή επί του σκάφους. Το αξιοσημείωτο στη λειτουργία του, ήταν ότι χρησιμοποίησε την «γυροσκοπική πυξίδα», μία εφεύρεση του Sperry με σκοπό τη σταθεροποίηση της τροχιάς του μη επανδρωμένου αεροσκάφους [8]. Το αεροσκάφος αυτό θεωρείται ως ο πρόγονος του πυραύλου cruise. [7]



Εικόνα 1.8 *Hewitt-Sperry Automatic Airplane*

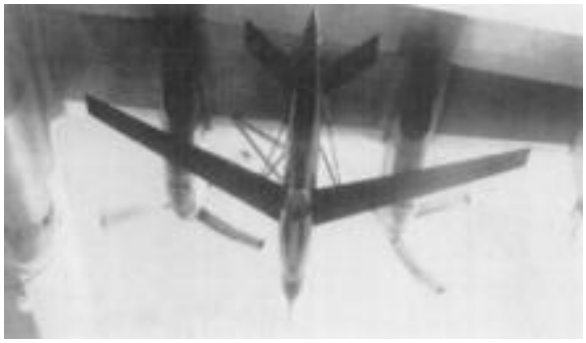
Την σκυτάλη στην εξέλιξη της τεχνολογίας των drones την πήρε κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου, ο Reginald Denny ο οποίος καταλαβαίνοντας ότι υπήρχε ζήτηση για αεροσκάφη χαμηλού κόστους με δυνατότητα ελέγχου μέσω ραδιοσυχνοτήτων, που θα μπορούσαν να χρησιμοποιηθούν ως στόχοι εκπαίδευσης των αντιαεροπορικών όπλων, πούλησε 15.000 αεροσκάφη Radioplane OQ-2 στο στρατό κατά τη διάρκεια του πολέμου και χιλιάδες περισσότερα τα επόμενα χρόνια. [8]



Εικόνα 1.9 *Radioplane OQ-2*

Η κατάρριψη του αμερικανού πιλότου Francis Gary Powers κατά τη διάρκεια αναγνωριστικής πτήσης ενός U-2 αεροσκάφους στον εναέριο χώρο της ΕΣΣΔ, το

1960 πυροδότησε μια σειρά από εξελίξεις στον τομέα των drones. Το περιστατικό οδήγησε τις ΗΠΑ στην επένδυση μεγάλων χρηματικών ποσών στην κατασκευή αεροσκαφών ικανών να συλλέγουν αυτόνομα πληροφορίες. Πιο συγκεκριμένα, η πολεμική αεροπορία των ΗΠΑ χορήγησε 200.000$ στην εταιρεία Ryan Aeronautical Company, με σκοπό την κατασκευή ενός drone αναγνώρισης. Το drone αναγνώρισης που δημιουργήθηκε πήρε την ονομασία “Red Wagon” ή “Ryan 136”. Ακολούθησαν μεταγενέστερα μοντέλα, τα οποία εκτοξεύονταν από τα αεροσκάφη DC-130 Hercules, είχαν εκ των προτέρων προγραμματισμένα σχέδια πτήσης και ελέγχονταν από πιλότους επί του αεροσκάφους. Χρησιμοποιήθηκαν πολύ στο Βιετνάμ και τη νότια Κίνα από την πολεμική αεροπορία των ΗΠΑ, αποκλειστικά για αναγνωριστικούς σκοπούς. [9]



Εικόνα 1.10 *Ryan 147B πάνω σε DC-130A*

Ενώ οι στρατιωτικές και αναγνωριστικές αποστολές κυριαρχούσαν στην χρήση των drones, το Gnat 750 της δεκαετίας του 1990, ήταν αυτό που έκανε το βήμα και οδήγησε στο γνωστό MQ-1 Predator, το οποίο επαναπροσδιόρισε τις στρατιωτικές επιχειρήσεις τον 21ο αιώνα. Το MQ-1 Predator της General Atomics, αποτέλεσε το πρώτο ευρέως χρησιμοποιούμενο drone για στρατιωτικούς σκοπούς επιτρέποντας την πραγματοποίηση επιθέσεων ακριβείας, χωρίς να διακινδυνεύεται η ζωή των στρατιωτών. Μπορεί να λειτουργήσει σε αποστάσεις έως και 460 μίλια από τον σταθμό εκτόξευσης και να ίπταται για 14 ώρες συνεχόμενα. Τα Predators αποτελούν μια σχετικά φθηνή και ασφαλή εναλλακτική λύση των επίγειων επιχειρήσεων ή των αεροπορικών επιθέσεων με επανδρωμένα αεροσκάφη. [10]



Εικόνα 1.11 *MQ-1 Predator*

1.2.5 Η εμπορευματοποίηση στα τέλη του 20ου αιώνα

Η περίοδος αυτή υπήρξε καθοριστική λόγω της σημαντικής προόδου στην τεχνολογία των drones με την χρήση του να επεκτείνεται και σε άλλους τομείς. Το Aerosonde ήταν το πρώτο drone που σχεδιάστηκε ειδικά για μετεωρολογική και περιβαλλοντική παρακολούθηση. Αναπτύχθηκε τη δεκαετία του 1990, σηματοδοτώντας την αρχή για εμπορική τους χρήση.

Ακολουθούν ορισμένες βασικές αλλαγές που έλαβαν χώρα στα τέλη του 20ου αιώνα και που οδήγησαν στο άνοιγμα των drones προς το καταναλωτικό κοινό:

- Πρόοδος στην τεχνολογία υπολογιστών: Καθώς οι υπολογιστές έγιναν πιο ισχυροί, επέτρεψε στους προγραμματιστές drone να βελτιώσουν τη σταθερότητα, τον έλεγχο και τις δυνατότητές τους. Αυτή η πρόοδος επέτρεψε τη δημιουργία πιο εξελιγμένων drones και κατάλληλων για εμπορική χρήση.

- Μείωση του κόστους κατασκευής: Καθώς η τεχνολογία προχωρούσε, το κόστος κατασκευής τους μειώθηκε σημαντικά, καθιστώντας τα πιο οικονομικά και κατ' επέκταση πιο οικονομικά.

- Μείωση μεγέθους των εξαρτημάτων: Στα τέλη του 20ου αιώνα πολλά βασικά εξαρτήματα έγιναν μικρότερα, όπως οι κάμερες, οι αισθητήρες και οι κινητήρες. Το μικρότερο μέγεθος αυτών των εξαρτημάτων κατέστησε δυνατή την ανάπτυξη ελαφρύτερων drones με βελτιωμένες δυνατότητες και μεγαλύτερους χρόνους πτήσης.

Κατά τη διάρκεια αυτής της περιόδου, εφαρμογές όπως η αεροφωτογραφία και η εξ' αποστάσεως συλλογή δεδομένων, έγιναν εφικτές χάρη στις τεχνολογικές εξελίξεις. Το ίδιο συνέβη για την χρήση τους πλέον στην γεωργία, στην παρακολούθηση της πανίδας και την μαγνητοσκόπηση. Την περίοδο αυτή διαμορφώθηκε το σκηνικό για την ευρεία υιοθέτησή τους στην αγορά.

Συνοψίζοντας, τα τέλη του 20ου αιώνα έφεραν κρίσιμες εξελίξεις στην τεχνολογία των drones, μετατρέποντάς τα από στρατιωτικά εργαλεία σε καταναλωτικά προϊόντα.

1.2.6 Η έλευση των τετρακοπτέρων και των πολυκόπτερων

Πότε λοιπόν τα drones έγιναν δημοφιλή στο ευρύ κοινό; Η απάντηση βρίσκεται στις αρχές της δεκαετίας του 2010 με την κυκλοφορία του Parrot AR.Drone, το οποίο κυκλοφόρησε για ψυχαγωγική χρήση. Έκτοτε τα drones βρίσκουν χρήση σε μια πληθώρα εφαρμογών. Τον 21ο αιώνα, η αγορά των drones άλλαξε με την εμφάνιση των τετρακόπτερων και των πολυκόπτερων.

Τα τετρακόπτερα και τα πολυκόπτερα είναι τύποι drones με πολλαπλούς έλικες, που τους βοηθούν να αιωρούνται και να παραμένουν σταθεροί κατά την πτήση. Άσκησαν μεγάλη επιρροή στους φίλους των drones, λόγω των μοναδικών σχεδίων και των πολλαπλών χρήσεων τους. Αυτού του είδους τα drones έγιναν πολύ δημοφιλή το 2006, όταν το Paparazzi Project ανέπτυξε ένα σύστημα αυτόματου πιλότου ανοιχτού κώδικα για μη επανδρωμένα αεροσκάφη, γεγονός που αποτέλεσε κομβικό σημείο στην εξέλιξή τους. [11]

Τα οφέλη των πολυκόπτερων περιλαμβάνουν:

- Καλύτερη σταθερότητα
- Ικανότητα πολλαπλών ελιγμών
- Μεγαλύτερη χωρητικότητα ωφέλιμου φορτίου
- Χρήση σε πολλαπλές εφαρμογές

Το Parrot AR.Drone, μπορούσε να συνδεθεί με smartphone μέσω Wi-Fi και ήταν εξοπλισμένο με δύο κάμερες που μπορούσαν να προβάλλουν την εικόνα τους με φωτογραφίες και βίντεο χαμηλής ποιότητας [12]. Χάρη στους αισθητήρες του και την μεγάλη σταθερότητά του εξαιτίας ενός αλγόριθμου ελέγχου, η αεροφωτογραφία, έγινε πιο εύκολη για όλους.



Εικόνα 1.12 *Parrot AR.Drone*

Ο σημερινός ηγέτης της αγοράς των drones όμως είναι η κινεζική εταιρεία DJI, η οποία ιδρύθηκε από τον Frank Wang το 2006, με πρωταρχικό στόχο το σχεδιασμό του λογισμικού ελέγχου πτήσης. Τον Ιανουάριο του 2013, η DJI παρουσίασε το Phantom 1, εφοδιασμένο με μια υψηλής ποιότητας φωτογραφική μηχανή GoPro προσαρτημένη σε βάση στήριξης gimbal, που να ελεγχόταν από έναν radio controller και αναμετάδιδε εικόνες ζωντανής ροής στον χρήστη μέσω εφαρμογής smartphone. Το Phantom 1 παρουσίασε σημαντικές βελτιώσεις στην σταθερότητα, το μέγιστο υψόμετρο και τον χρόνο πτήσης σε σύγκριση με το Parrot AR.Drone. Η εύκολη και αξιόπιστη χρήση του, σε συνδυασμό με τη λήψη εικόνων υψηλής ποιότητας, έδωσε το έναυσμα στην καταναλωτική μανία των drones. [13]



Εικόνα 1.13 *DJI Phantom 1*

Όλα τα παραπάνω έθεσαν τα θεμέλια για έναν κόσμο με τα drones όπως τα γνωρίζουμε σήμερα. Από τα μπαλόνια και τους χαρταετούς μέχρι τα τηλεκατευθυνόμενα και τα αυτόνομα αεροσκάφη, η ιστορία των drones είναι πραγματικά ένα συναρπαστικό ταξίδι.

1.3 Πεδία εφαρμογής

1.3.1 Στρατιωτική χρήση των UAS

Η ευρεία χρήση των UAS και η ενσωμάτωσή τους στις στρατιωτικές επιχειρήσεις άρχισε ουσιαστικά μετά τον Πόλεμο του Κόλπου το 1991, καθώς αποδείχθηκε στη μάχη η ικανότητά τους να διεξάγουν επιχειρήσεις με ελάχιστο κόστος σε ανθρώπινες ζωές. Η χρήση των συστημάτων αυτών στις πρόσφατες συγκρούσεις πάνω από το Ιράκ, τη Σερβία και το Αφγανιστάν, απέδειξε ότι τα UAS αποτελούν ανεκτίμητο πλεονέκτημα για όποιον τα έχει στην κατοχή του. [2]

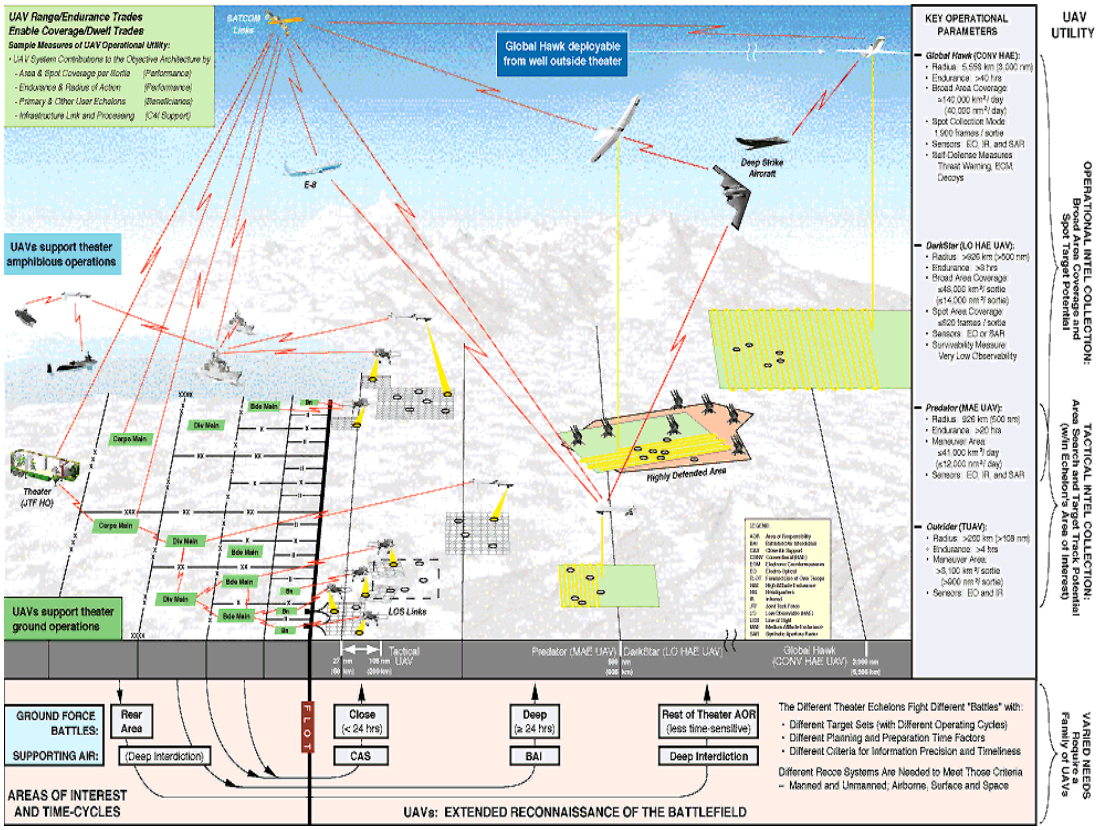
Τα περισσότερα στρατιωτικά μη επανδρωμένα συστήματα αεροσκαφών χρησιμοποιούνται για αναγνώριση και πλήγματα εχθρικών στόχων. Χρησιμοποιούνται επί των πλείστων από τις ένοπλες δυνάμεις των ΗΠΑ, και του Ισραήλ. Ωστόσο, πολλές χώρες, συμπεριλαμβανομένης της Ελλάδας, έχουν

πραγματοποιήσει προσπάθειες ανάπτυξης ενός συστήματος UAS και περισσότερες έχουν ήδη ενσωματώσει τουλάχιστον ένα σύστημα UAS στις στρατιωτικές τους δυνάμεις.

Τα κύρια χαρακτηριστικά των σύγχρονων στρατιωτικών UAS συνοψίζονται παρακάτω: [2]

- Διαφορετικό μέγεθος και εμβέλεια ανάλογα με τις αποστολές για τις οποίες προορίζονται.
- Αυξημένα ποσοστά ευπάθειας και φθοράς λόγω της χαμηλού κόστους κατασκευής τους και της απουσίας χειριστή επί του αεροσκάφους.
- Ένας τουλάχιστον χειριστής ανά αεροσκάφος.
- Περιορισμένη αυτονομία.
- Άμεσος έλεγχος του UAV από τον χειριστή και εξάρτηση από τις ζεύξεις επικοινωνίας.
- Τα συστήματα ελέγχου βασίζονται σε τεχνικές γραμμικού ελέγχου.
- Σχεδιασμός διαδρομής βάσει σημείων πορείας (waypoints).
- Χαμηλού κόστους αδρανειακές μονάδες και αισθητήρες αυξάνουν την εξάρτηση από τα συστήματα GPS για πλοήγηση και έλεγχο.
- Ελάχιστη έμφαση στην επιχειρησιακή ασφάλεια, με αποτέλεσμα τον εντοπισμό ηχητικών, θερμικών, οπτικών και ηλεκτρομαγνητικών αποτυπωμάτων.
- Ωφέλιμο φορτίο σχεδιασμένο για μία πλατφόρμα.

Μελλοντικά τα UAS θα εκτελούν πιο σύνθετες αποστολές, όπως αερομαχίες, εντοπισμό στόχων, αναγνώριση και καταστροφή, καταστολή εχθρικής αεράμυνας, ηλεκτρονικό πόλεμο, αναμετάδοση επικοινωνιών, αερομεταφορές και εναέριο εφοδιασμό, πόλεμο κατά πλοίων επιφανείας και ανθυποβρυχιακό πόλεμο. Επηρεαζόμενες από την οικονομική κρίση και τις συνεχείς πιέσεις για μείωση των ανθρώπινων απωλειών, οι ένοπλες δυνάμεις αναμένεται να επικεντρωθούν στην ανάπτυξη των UAS.



Εικόνα 1.14 *Μελλοντικός ρόλος των UAVs στο θέατρο επιχειρήσεων*

1.3.2 Χρήση των UAS στο αστικό περιβάλλον

Εκτός από τις στρατιωτικές εφαρμογές, έχει αποδειχτεί η χρησιμότητα των drones σε διάφορους τομείς μη στρατιωτικών εφαρμογών και ιδιαίτερα στο αστικό περιβάλλον. Εκτιμάται ότι η αγορά των drones, υπερβαίνει τα 127 δισεκατομμύρια $, με το κομμάτι των επιθεώρησης υποδομών να αντιστοιχεί σε 45.2 δισεκατομμύρια $ και της γεωργίας στα 32.4 δισεκατομμύρια $, ακολουθούμενες από τον τομέα των μεταφορών και της ασφάλειας. [14]

Μέχρι το 2025 εκτιμάται ότι θα έχουν προκύψει περισσότερες από 100.000 νέες θέσεις εργασίας, ενώ για να γίνει κάποιος χειριστής drone, θα πρέπει να παρακολουθήσει τα αντίστοιχα προγράμματα σπουδών σε πανεπιστήμια ή ειδικά εκπαιδευτικά κέντρα. Το κόστος του εξοπλισμού που θα φέρουν τα drones (κάμερες, αισθητήρες, συσκευές επικοινωνίας) εκτιμάται ότι μέχρι το 2027 θα προσεγγίσει τα 3 δισεκατομμύρια $, με το μεγαλύτερο ποσοστό αυτού του ποσού να αφορά τις

συσκευές ανίχνευσης και επικοινωνίας (περίπου 80%), ενώ το 11% να σχετίζεται με αισθητήρες και κάμερες. [14]

Τα drones παρουσιάζουν σημαντικά πλεονεκτήματα σε σύγκριση με τις συμβατικές τεχνολογίες, που μπορούν να χρησιμοποιηθούν για τον ίδιο σκοπό. Τα πλεονεκτήματά τους οφείλονται στη λιγότερη κατανάλωση ενέργειας, στην εξάλειψη των κινδύνων απώλειας της ανθρώπινης ζωής και στην ευκολία συλλογής δεδομένων, καθιστώντας τα ιδιανικά για χρήση σε πληθώρα εφαρμογών. [15]

1.3.2.1 Κατηγορίες εφαρμογών

Σήμερα και μετά από πολλά χρόνια ανάπτυξης, τα UAS φτάνουν στο κρίσιμο σημείο στο οποίο θα μπορούσαν να βρουν εφαρμογή στην αγορά. Οι πιθανές εφαρμογές μπορούν να κατηγοριοποιηθούν σε πέντε ομάδες: [2]

- Περιβαλλοντικές εφαρμογές: Παρακολούθηση της ατμόσφαιρας και μέτρηση της ρύπανσης, πρόγνωση του καιρού, γεωλογικές έρευνες.

- Εφαρμογές έκτακτης ανάγκης: Σε αυτές περιλαμβάνονται η πυρόσβεση, η έρευνα και διάσωση, η παρακολούθηση τσουνάμι/πλημμυρών, η παρακολούθηση πυρηνικής ακτινοβολίας, ειδοποίηση σε περίπτωση καταστροφών και η παροχή ανθρωπιστικής βοήθειας.

- Εφαρμογές επικοινωνιών: Υπηρεσίες αναμετάδοσης επικοινωνιών κινητής τηλεφωνίας και ευρυζωνικών επικοινωνιών.

- Εφαρμογές επιτήρησης: Χρήσεις που αφορούν την ασφάλεια (χερσαία και θαλάσσια περιπολία συνόρων, παράκτια παρακολούθηση, αστυνόμευση), παρακολούθηση καλλιεργειών και συγκομιδής, ανίχνευση πυρκαγιών, παρακολούθηση υποδομών (αγωγοί πετρελαίου/αερίου, δίκτυο υψηλής τάσης) και χαρτογράφηση εδάφους (χαρτογράφηση δασών, παρακολούθηση κυκλοφορίας αστικών περιοχών).

- Εμπορικές εφαρμογές: Αυτές περιλαμβάνουν αεροφωτογραφίες, γεωργία ακριβείας, χημικούς ψεκασμούς, μεταφορά εμπορευμάτων και παράδοση αγαθών.

Το σημαντικότερο εμπόδιο για την επέκταση των UAS εντοπίζεται στον περιορισμό της λειτουργίας τους σε ένα συγκεκριμένο τμήμα του εναέριου χώρου. Σχεδόν όλες οι εφαρμογές που συζητήθηκαν απαιτούν πρόσβαση είτε στον εθνικό εναέριο χώρο μιας χώρας είτε σε ξένο εναέριο χώρο σε κάποιο σημείο του σχεδίου πτήσης, ιδίως για χρήσεις που προορίζονται για απομακρυσμένες περιοχές. Ωστόσο, απαιτείται να λειτουργούν κοντά στο αστικό περιβάλλον και να είναι πλήρως ενσωματωμένα στο σύστημα εναέριας κυκλοφορίας. Αυτό προϋποθέτει τόσο την ανάπτυξη προτύπων και κανονισμών όσο και τη βελτίωση του σχεδιασμού των UAS που πρέπει να βασίζεται σε απαιτήσεις αξιοπλοΐας παρόμοιες με εκείνες της πολιτικής αεροπορίας. [16]

- Καθιέρωση ασφαλών και αξιόπιστων επικοινωνιών μεταξύ των drones και του σταθμού ελέγχου ή/και του σταθμού ελέγχου του UAS και του πύργου εναέριας κυκλοφορίας, για την παρακολούθηση των εν εξελίξει πτήσεων.
- Βελτίωση της αξιοπιστίας για να την κάλυψη των απαιτήσεων αξιοπλοΐας, αλλά και για την εκτέλεση μεγαλύτερης διάρκειας αποστολών.
- Επίτευξη μεγαλύτερης αυτονομίας στη διαχείρισης της αποστολής, ώστε να αξιοποιηθεί το πλεονέκτημα της χρήσης πλατφόρμας UAS για την υποστήριξη των αποστολών. Λιγότερη ανθρώπινη αλληλεπίδραση κατά την πτήση επιτρέπει σε λιγότερο προσωπικό στο σταθμό, λιγότερες υποδομές υποστήριξης και σε έναν χειριστή που παρακολουθεί πολλά οχήματα την δεδομένη στιγμή. Όλα αυτά δεδομένου ότι ο χειριστής και το drone ανταποκρίνονται εγκαίρως στις οδηγίες του ελέγχου εναέριας κυκλοφορίας.
- Ακριβώς όπως και τα στρατιωτικά UAS, η χρήση σμηνών UAV θα είναι απαραίτητη για μια οικονομικά αποδοτική εφαρμογή των UAS σε πολλές πολιτικές εφαρμογές.
- Η μεγαλύτερη διάρκεια ζωής και η αντοχή στις καιρικές συνθήκες και τις αναταράξεις είναι επίσης απαραίτητη ανάλογα με την εφαρμογή χρήσης.

1.4 Νομοθεσία περί πολιτικής χρήσης των drones

Όσον αφορά την πολιτική χρήσης των drones, ανάλογα με τα τεχνικά χαρακτηριστικά τους καθώς και την γεωγραφική περιοχή στην οποία χρησιμοποιούνται, μπορούν να ανήκουν στις εξής κατηγορίες: «ανοικτή», «ειδική» και «πιστοποιημένη». [17]

Ο χειριστής του drone χρειάζεται να έχει στην κατοχή του Άδεια Χειριστή ΣμηΕΑ, ενώ για την επαγγελματική χρήση των drones απαιτείται η χορήγηση της Άδειας Εκμετάλλευσης ΣμηΕΑ. Οι άδειες των χειριστών ΣμηΕΑ εκδίδονται για τις παρακάτω κατηγορίες και ανάλογα το μέγιστο βάρος απογείωσης (Maximum Take Off Mass) του drone, ως εξής: [17]

ΜΤΟΜ ΣμηΕΑ	Κατηγορία
Μέχρι 1 kg (<1)	UAS Pilot A
Από 1 kg (=/>1kg) μέχρι 4 kgs (<4)	UAS Pilot B
Από 4kgs (=/>4kgs) μέχρι 25 kgs (<25)	UAS Pilot C
Από 25 kgs (=/>25kgs) μέχρι 150 kgs (< 150)	UAS Pilot D
Από 150 kgs (=/>150) και άνω (Κανονισμός EASA)	UAS Pilot E

Εικόνα 1.15 *Κατηγορίες αδειών χειριστών*

Σχετικά με τις απαραίτητες προετοιμασίες για την πτήση του drone, ο εκάστοτε χρήστης πρέπει να εγκαταστήσει το διαδικτυακό σύστημα UAS-FRSS το οποίο έχει ως στόχο την συνεργασία των διαφόρων επαγγελματικών και μη, φορέων. Μέσω αυτού του συστήματος μειώνονται οι πιθανότητες ατυχημάτων μεταξύ των ιπτάμενων οχημάτων, καθώς και των παραβιάσεων αποκλεισμένων περιοχών από την Ελληνική Κυβέρνηση. Τα δύο μέρη του UAS – FRSS είναι τα ΥΕΔ και DAGR (Drone Aware – GR). Στο πρώτο πεδίο ολοκληρώνεται η εγγραφή των πολιτών καθώς και η εξυπηρέτησή τους, ενώ στο δεύτερο αναφέρονται οι γεωγραφικοί περιορισμοί καθώς και οι πορείες όλων των drones. Ο χρήστης θα πρέπει να γνωρίζει μονάδες μέτρησης που χρησιμοποιούνται στην αεροπλοΐα, όπως ναυτικά μίλια και πόδια, καθώς και την σημασία ορισμένων όρων, όπως MSL, AGL, FIR, TMA και CTR. [18]

Σύμφωνα με το ΦΕΚ (Απόφαση Διοικητή Υπηρεσίας Πολιτικής Αεροπορίας, 2016) ένα UAV θα πρέπει να ίπταται έως τα 400 πόδια σε υψόμετρο από την επιφάνεια του εδάφους (AGL) ή την στάθμη της θάλασσας (MSL). Επίσης τα χρονικά περιθώρια για την πραγματοποίηση της πτήσης έχουν καθοριστεί ως μισή ώρα πριν την ανατολή και μισή ώρα μετά την δύση του ηλίου. Για την έγκριση χρήσης ενός drone για επαγγελματικούς σκοπούς είναι αναγκαία η χορήγηση άδειας από τη Διεύθυνση Αεροπορικής Εκμετάλλευσης της Υπηρεσίας Πολιτικής Αεροπορίας. [17]

2. ΚΑΤΗΓΟΡΙΕΣ ΚΑΙ ΕΞΟΠΛΙΣΜΟΣ

2.1 Κατηγορίες μη επανδρωμένων αεροσκαφών

Τα συστήματα των UAV κατηγοριοποιούνται σύμφωνα με τον Austin βάσει την επιχειρησιακή ικανότητα ή το μέγεθος του αεροσκάφους που χρησιμοποιείται σε μια αποστολή. Οι ορισμοί που χρησιμοποιούνται για τον προσδιορισμό τους συνεχώς τροποποιούνται, εξαιτίας των τεχνολογικών εξελίξεων. Αυτό έχει ως αποτέλεσμα, τα όρια που προσδιορίζουν τα συστήματα να μεταβάλλονται και γι' αυτόν το λόγο οι ορισμοί μπορεί να αλλάξουν. Οι κατηγορίες των συστημάτων βάσει τον τύπο των αεροσκαφών είναι οι εξής: [19]

HALE (High Altitude Long Endurance): UAV με επιχειρησιακή οροφή πάνω από 15.000μ. και αυτονομία πάνω από 24 ώρες. Στόχος τους είναι η αναγνώριση και παρακολούθηση σε πολύ μεγάλη εμβέλεια, φέροντας οπλισμό. Χρησιμοποιούνται από Πολεμικές Αεροπορίες πολλών χωρών.

MALE (Medium Altitude Long Endurance): UAV με επιχειρησιακή οροφή από 5.000 έως 15.000μ. και αυτονομία 24 ώρες. Έχουν αποστολές όμοιες των HALE, με μικρότερη όμως εμβέλεια αλλά πάνω από 500χλμ.

TUAV (Medium Range or Tactical UAV): UAV με εμβέλεια μεταξύ 100 και 300 χλμ. Είναι μικρότερα σε μέγεθος, απλούστερα από τα συστήματα HALE και MALE και χρησιμοποιούνται από χερσαίες και ναυτικές δυνάμεις.

Close Range UAV: Ίσως ο πιο κοινός τύπος UAV που επιχειρεί συνήθως σε απόσταση έως 100χλμ και χρησιμοποιείται για στρατιωτικές και μη αποστολές. Μερικές από αυτές είναι η αναγνώριση, η κατάδειξη στόχου, η παρακολούθηση, η ασφάλεια αεροδρομίων, οι ψεκασμοί σε καλλιέργειες, η επιθεώρηση γραμμών ηλεκτροδότησης, και η παρακολούθηση της κυκλοφορίας.

MUAV (Mini UAV): UAV που ζυγίζουν συνήθως κάτω από 20 κιλά αλλά δεν είναι πιο μικρά από τα MAV. Η εμβέλεια τους ανέρχεται μέχρι τα 30χλμ και μπορούν να εκτοξευθούν με το χέρι. Συνήθως χρησιμοποιούνται από κινητές ομάδες μάχης αλλά και για μη στρατιωτικούς σκοπούς.

MAV (Micro UAV): UAV που έχουν εκπέτασμα πτερύγων μικρότερο των 150mm. Χρησιμοποιούνται σε αστικό περιβάλλον και κυρίως για χρήση σε εσωτερικό κτιρίων. Χαρακτηριστικό τους είναι η πολύ μικρή ταχύτητα, η δυνατότητα αιώρησης, ενώ έχουν πρόβλημα σε συνθήκες βροχόπτωσης.

NAV (Nano Air Vehicles): Έχουν πολύ μικρό μέγεθος και χρησιμοποιούνται σε σμήνη για παρεμβολές σε ραντάρ ή, ενδεχομένως, για επιτήρηση εξαιρετικά μικρής περιοχής.

Ορισμένες από τις ανωτέρω κατηγορίες συναντώνται με περιστρεφόμενες πτέρυγες, συνήθως μέχρι το μέγεθος των TUAV και συχνά αναφέρονται με τον όρο remotely piloted helicopter (RPH).

RPH, τηλεχειριζόμενο ελικόπτερο ή VTUAV: Είναι UAV κάθετης απογείωσης και προσγείωσης. Θετικό χαρακτηριστικό είναι η δυνατότητα αιώρησής του κατά τη διάρκεια μιας αποστολής. Επίσης είναι λιγότερο επιρρεπή στις αναταράξεις του αέρα σε σύγκριση με τα αεροσκάφη σταθερής πτέρυγας.

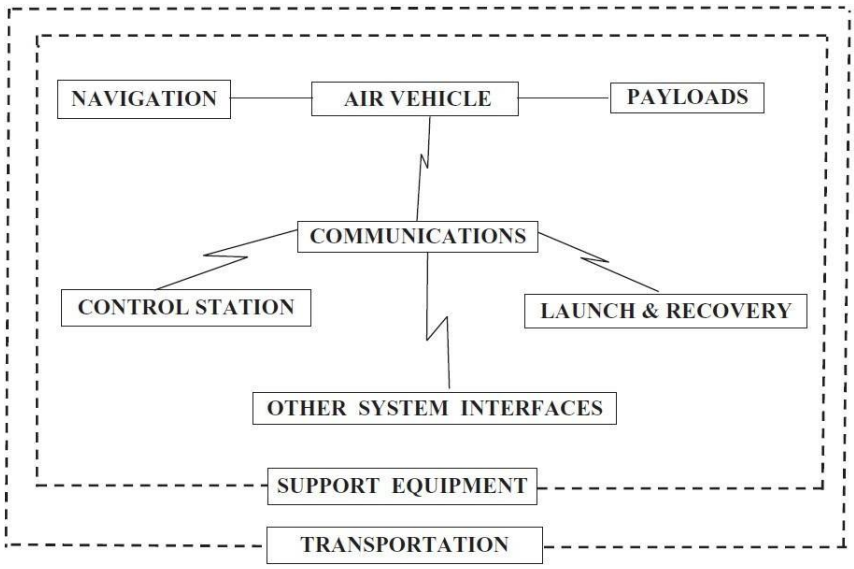
UCAV (Unmanned Combat Air Vehicle) και UCAR (Unmanned Combat Rotorcraft): Είναι UAV που φέρουν οπλισμό ή ακόμη που μπορούν να συμμετέχουν σε μάχη αέρος-αέρος.

Σύμφωνα με τους Mozaffari et al. (2019), τα drones κατηγοριοποιούνται με βάση την επιχειρησιακή τους οροφή, σε υψηλού υψομέτρου (HAPs - High Altitude Platforms) και χαμηλού υψομέτρου (LAPs - Low Altitude Platforms). Τα HAPs έχουν υψόμετρο άνω των 17χλμ ενώ τα LAPs, από την άλλη πλευρά, μπορούν να πετάξουν σε υψόμετρο από μερικές δεκάδες μέτρα έως μερικά χιλιόμετρα, με όμως μεγαλύτερη ταχύτητα. Επιπλέον τα UAV μπορούν επίσης να κατηγοριοποιηθούν, με βάση τον

τύπο τους, σε UAV σταθερής πτέρυγας (fixed-wing) και σε UAV περιστρεφόμενων πτερυγίων (rotary-wing).

2.2 Σύνθεση συστήματος μη επανδρωμένου αεροσκάφους (UAS)

Ένα σύστημα μη επανδρωμένου αεροσκάφους αποτελείται από υποσυστήματα, εκ των οποίων το drone είναι μόνο ένα. Τα υποσυστήματα ενός UAS είναι τα εξής: ο σταθμός ελέγχου (Control Station - CS), το ωφέλιμο φορτίο (payload), το drone, το σύστημα πλοήγησης (Navigation system), ο εξοπλισμός εκτόξευσης, και περισυλλογής (Launch, recovery and retrieval equipment), οι επικοινωνίες (Communications), οι διεπαφές (Interfaces), ο εξοπλισμός υποστήριξης (Support Equipment) και η μεταφορά (Transportation). [19]

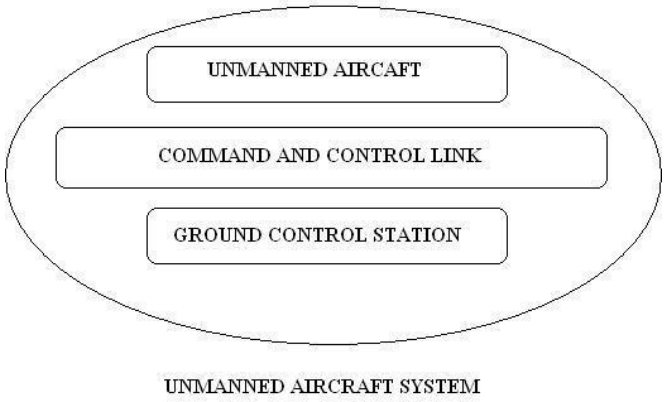


Εικόνα 2.1 *Δομή ενός UAS*

Επισημαίνεται ότι, κάθε υποσύστημα του UAS θεωρείται αναπόσπαστο μέρος του συστήματος αυτού. Κανένα υποσύστημα δεν είναι πιο σημαντικό από ένα άλλο, αν και ορισμένα και συνήθως το ίδιο το drone, έχουν μεγαλύτερη επίδραση στο σχεδιασμό των άλλων υποσυστημάτων του συστήματος από ό,τι άλλα. Ανάλογα με τον τύπο του UAS, τα υποσυστήματα αυτά θα πρέπει να μπορούν να λειτουργούν ταυτόχρονα, γεγονός που αυξάνει τη σημαντικότητα των διεπαφών τους. Τέλος, μεγάλη σημασία έχει και η αλληλεπίδραση του UAS με το περιβάλλον καθώς

εξαρτάται σε μεγάλο βαθμό από τις καιρικές και τις γεωμορφολογικές συνθήκες της εκάστοτε περιοχής που χρησιμοποιείται.

Τα υποσυστήματα αυτά δύναται να θεωρηθούν και ως τρία (3) μεγαλύτερα υποσυστήματα, τα οποία μπορεί να είναι: το drone, ο επίγειος σταθμός ελέγχου (GCS - Ground Control Station) και η ζεύξη επικοινωνιών εντολών και ελέγχου του σταθμού με το drone. [21]



Εικόνα 2.2 *Εναλλακτική δομή ενός UAS*

2.2.1 Χαρακτηριστικά των υποσυστημάτων

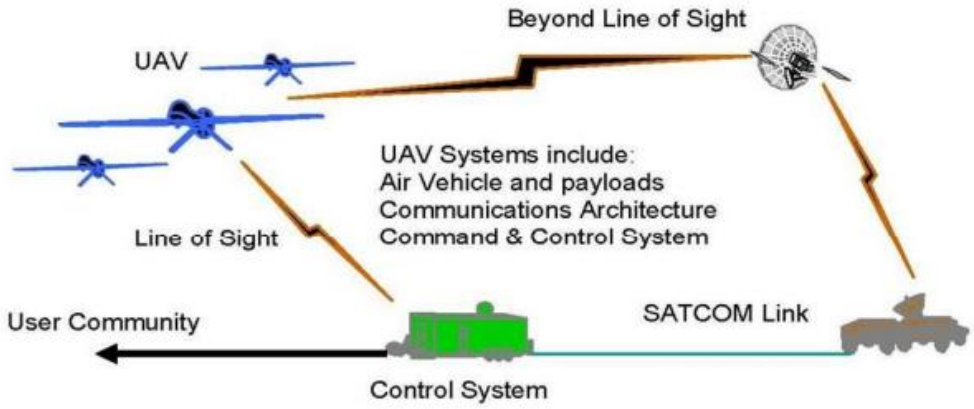
Όπως αναφέρθηκε ένα UAS μπορεί να θεωρηθεί ότι απαρτίζεται από τρία κύρια υποσυστήματα: [2]

Μη Επανδρωμένο Αεροσκάφος: Το υποσύστημα αυτό περιλαμβάνει ένα ή και περισσότερα μη επανδρωμένα αεροσκάφη μαζί με τα ωφέλιμα φορτία τους. Κάθε ένα από τα περιλαμβάνει την άτρακτο του αεροσκάφους, τα ηλεκτρονικά του συστήματα (avionics) και το σύστημα κίνησης. Το ωφέλιμο φορτίο αποτελείται από συστήματα που υποστηρίζουν την διεκπεραίωση μια επιτυχημένης πτήσης και αποστολής, όπως κάμερες, αισθητήρες, κεραίες κ.λπ.

Τμήμα Επίγειου Εξοπλισμού : Αποτελείται από διάφορα μέρη, τον επίγειο σταθμό ελέγχου (GCS), το σταθμό ελέγχου ωφέλιμου φορτίου / τερματικό σταθμό δεδομένων εδάφους (GDT - Ground Data Terminal) και, εάν απαιτείται, από το σύστημα

εκτόξευσης και περισυλλογής (LRS - Launch and Recovery System). Σε αυτό το τμήμα το GCS είναι το σημαντικότερο. Περιλαμβάνει όλο τον απαιτούμενο εξοπλισμό για τον χειριστή, για το σχεδιασμό της πτήσης και την παρακολούθησή της. Επίσης, μεταφράζει τις εντολές του πιλότου στις κατάλληλες κινήσεις και τις μεταδίδει μέσω της ζεύξη επικοινωνιών στο αεροσκάφος.

Τμήμα Επικοινωνιών: Αποτελείται από τη ζεύξη επικοινωνιών εντολών και ελέγχου, στη ζεύξη δεδομένων ωφέλιμου φορτίου και τις εξωτερικές επικοινωνίες. Οι κύριες κατηγορίες επικοινωνιών ορίζονται ανάλογα με την απόσταση στην οποία λειτουργεί το UAS: οπτικού πεδίου (VLOS), ορίζοντα (LOS) και πέραν του ορίζοντα (BLOS).



Εικόνα 2.3 *Επικοινωνίες ενός UAS*

2.3 Εμπορικά drones και εξοπλισμός

2.3.1 Πολυκόπτερα

Στην κατηγορία αυτή των drones που είναι διαθέσιμα στην αγορά και απευθύνονται στο καταναλωτικό κοινό με μεγάλη απήχηση τα τελευταία χρόνια, νοούνται τα τετρακόπτερα, εξακόπτερα ή και οκτακόπτερα, ήτοι drones χωρίς περιορισμό στον αριθμό των ελίκων. Ο αριθμός τους συνδέεται με το μέγεθος του drone, το οποίο μπορεί να κατηγοριοποιηθεί σε κατηγορίες μεγέθους, επηρεάζοντας έτσι την ευκολία εντοπισμού του, το ωφέλιμο φορτίου που δύναται να φέρει αλλά και το μέγεθος της ζημιάς που προκαλεί σε ενδεχόμενη σύγκρουση. [22]

Οι δυνατότητες και τα χαρακτηριστικά των εμπορικών πολυκόπτερων ποικίλουν. Ως εκ τούτου, παρατίθενται πέντε κατηγορίες εμπορικών πολυκόπτερων, ως ένδειξη των διαφόρων κατηγοριών UAS στα οποία ανήκουν. [22]

2.3.1.1 Γρήγορο nano-quadcopter

Κατηγορία αγωνιστικών τετρακόπτερων με υψηλές ταχύτητες, παρόμοια με αυτήν των τηλεκατευθυνόμενων αυτοκινήτων και αεροπλάνων.



Εικόνα 2.4 *Draco drone*

2.3.1.2 Γρήγορο micro-drone με κάμερα υψηλών επιδόσεων

Ένα παράδειγμα drone αυτής της κατηγορίας είναι η σειρά DJI Phantom. Τα drone αυτά χρησιμοποιούνται τόσο από χομπίστες όσο και από επαγγελματίες και κυκλοφορούν σε διάφορες εκδόσεις. Οι ακριβότερες εκδόσεις προσφέρουν καλύτερα χαρακτηριστικά, ιδίως όσον αφορά την κάμερα. Το τελευταίο μοντέλο περιορίζεται στα 500 μέτρα σε υψόμετρο από το λογισμικό, αλλά τα προηγούμενα μοντέλα δεν έχουν αυτόν τον περιορισμό. Χρησιμοποιούν πολλαπλούς αισθητήρες που προσφέρουν προηγμένες και αποτελεσματικές λειτουργίες αποφυγής εμποδίων.



Εικόνα 2.5 *DJI Phantom 4 pro*

2.3.1.3 Micro-drone με κάμερα και οπτικό ζουμ

Αυτός ο τύπος drone χρησιμοποιεί το μεγάλης εμβέλειας οπτικό ζουμ του για επιθεώρηση βιομηχανικών εγκαταστάσεων, όπως για παράδειγμα τα πτερύγια ανεμογεννητριών, τα οποία είναι δύσκολο να επιθεωρηθούν οπτικά με άλλο τρόπο, αλλά και από αστυνομικές υπηρεσίες.



Εικόνα 2.6 *Walkera Voyager 5*

2.3.1.4 Μικρό επαγγελματικό drone πολλαπλών χρήσεων

Αυτός ο τύπος drone είναι αρκετά μεγάλος ώστε να μπορεί να μεταφέρει διάφορα ωφέλιμα φορτία, τα οποία χρησιμοποιούνται για πολλαπλούς ρόλους.



Εικόνα 2.7 *ProDrone PD6B-AW*

2.3.1.5 Μικρό γεωργικό drone

Εξειδικευμένο drone, όπου μπορεί να προγραμματιστεί για να εκτελεί ψεκασμούς καλλιεργειών.



Εικόνα 2.8 *DJI Agras MG-1*

2.3.2 Άτρακτος / Σκελετός

Το μέγεθος και το σχήμα ενός drone εξαρτώνται από το σχεδιασμό της ατράκτου, τη διαμόρφωση του ωφέλιμου φορτίου και των μπαταριών του. Αυτά επηρεάζουν το συντελεστή ανάκλασης, την κατανάλωση ενέργειας, την αυτονομία και την

επιβιωσιμότητά του. Για να επιτευχθεί μεγάλη ανθεκτικότητα, τα drones κατασκευάζονται ή επικαλύπτονται από αυτοθεραπευόμενα υλικά (self-healing coating materials), ήτοι υλικά που μπορούν να θεραπεύσουν μικρορωγμές, όπως βιοπολυμερή και ισομερή, βελτιώνοντας έτσι σημαντικά τη διάρκεια ζωής τους. [23]



Εικόνα 2.9 *Άτρακτος ενός VTOL drone*

2.3.3 Ελεγκτής πτήσης (flight controller)

Πρόκειται για τον προγραμματιζόμενο εγκέφαλο του drone, την κεντρική μονάδα ή αλλιώς ελεγκτή πτήσης που μέσω του οποίου πραγματοποιούνται όλοι οι αναγκαίοι υπολογισμοί για την επίτευξη της πτήσης. Είναι άμεσα συνδεδεμένος με την απόδοση των κινητήρων και καθορίζει τον χρόνο πτήσης και το ποσοστό χρήσης της μπαταρίας.

Ειδικότερα, πρόκειται για μια πλακέτα τυπωμένου κυκλώματος με έναν επεξεργαστή Intel ή ARM ως CPU. Λαμβάνει πληροφορίες από τους αισθητήρες και ανταποκρίνεται στις εντολές του χειριστή ή του εγκατεστημένου λογισμικού. Οι εντολές αυτές μπορεί να περιλαμβάνουν απλές διεργασίες όπως η αναφορά της κατάστασης των εξαρτημάτων του drone, έως πιο σύνθετες αλγοριθμικές διεργασίες

όπως ο έλεγχος του ESC (Electronic Speed Controller) για τη σταθεροποίηση του drone έναντι του ανέμου με βάση τα δεδομένα από τους αισθητήρες. [12]

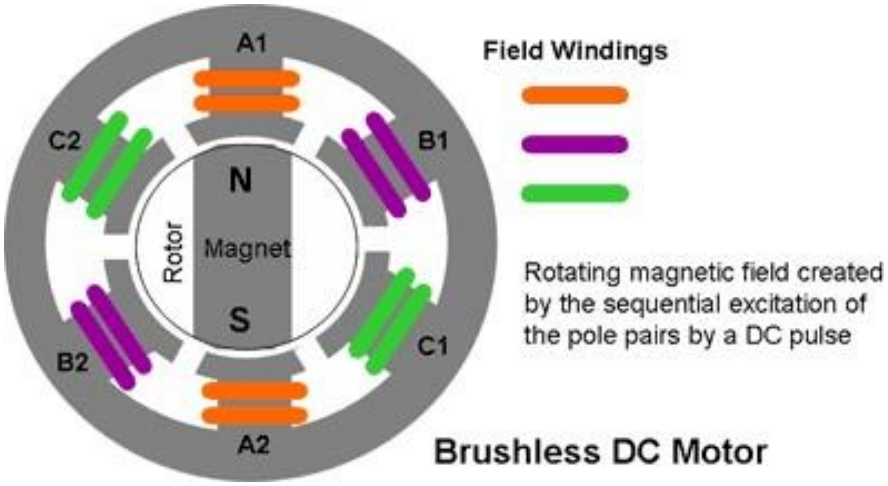


Εικόνα 2.10 *Ελεγκτής πτήσης DJI A2*

2.3.4 Κινητήρες

Πρόκειται για ένα από τα κύρια εξαρτήματα που καθορίζουν την ισχύς του drone. Ο καθορισμός των κατάλληλων κινητήρων εξαρτάται από το συνολικό βάρος του drone που υπολογίζεται από το άθροισμα του βάρους όλων των εξαρτημάτων από τα οποία απαρτίζεται.

Επικεντρώνοντας την προσοχή μας στα τετρακόπτερα και τα πολυκόπτερα, παρατηρείται η χρήση άψυκτων κινητήρων συνεχούς ρεύματος (brushless DC motors) για την περιστροφή των ελίκων δεξιόστροφα είτε αριστερόστροφα για την ανοδικής ώθησης. Οι κινητήρες περιέχουν μια κυκλική διαμόρφωση πηνίων με κατεύθυνση προς το κέντρο και έναν ισχυρό μαγνήτη (συνήθως νεοδυμίου) στο κέντρο. Οι κινητήρες λειτουργούν παρέχοντας παλμούς συνεχούς ρεύματος στα πηνία για τη δημιουργία ενός περιστρεφόμενου ηλεκτρομαγνητικού πεδίου στον μαγνήτη. Ο μαγνήτης περιστρέφεται συνεχώς για να ευθυγραμμιστεί εκ νέου με τα μαγνητικά πεδία, περιστρέφοντας έτσι και τον έλικα. Η ισχύς που παρέχεται στα πηνία επηρεάζει άμεσα την κατεύθυνση, την ταχύτητα και την ώθηση που παράγεται. [13]



Εικόνα 2.11 *Brushless DC motor*

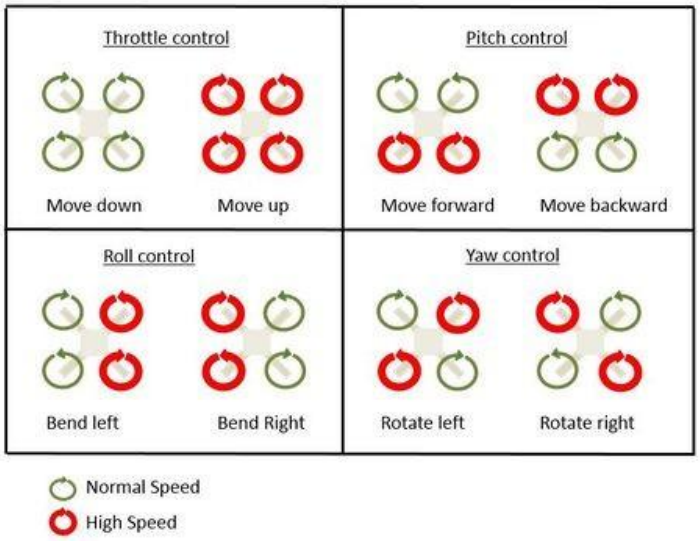


Εικόνα 2.12 *Drone motor*

2.3.5 Ηλεκτρονικός ελεγκτής ταχύτητας (Electronic Speed Controller - ESC)

Η ρύθμιση της κλίσης του drone και της ταχύτητας απαιτούν συντονισμό της ταχύτητας των ελίκων οι οποίοι επιτυγχάνονται αλγοριθμικά από ηλεκτρονικούς ελεγκτές ταχύτητας (ESC). Κάθε κινητήρας έχει το δικό του ESC για να του παρέχει τα απαραίτητα επίπεδα ρεύματος ώστε να περιστρέφεται με την επιθυμητή ταχύτητα. Ένας ενσωματωμένος μικροελεγκτής MOSFET λειτουργεί εντός του ESC, για να δίνει παλμούς ρεύματος εκατοντάδες φορές ανά δευτερόλεπτο, σε ακολουθίες που θα περιστρέφουν τον έλικα. Ο ελεγκτής πτήσης επιτυγχάνει την επιθυμητή δυναμική

πτήσης συντονίζοντας την περιστροφή των ελίκων μέσω των ESC. Για παράδειγμα, η δεξιόστροφη περιστροφή απαιτεί ο μπροστινός δεξιός και ο πίσω αριστερός έλικας να περιστρέφονται γρηγορότερα από τους άλλους για να επιτευχθεί η περιστροφή.



Εικόνα 2.13 *Ρύθμιση ταχύτητας για την επίτευξη της επιθυμητής κίνησης*

2.3.6 Τηλεχειρισμός (πομπός και δέκτης)

Η πλοήγηση του drone επιτυγχάνεται μέσω της συνεχής επικοινωνίας του πομπού (τηλεχειριστήριο) και του δέκτη που είναι τοποθετημένος επί του drone. Αυτή η επικοινωνία πραγματοποιείται μέσω συχνοτήτων που μεταδίδουν τις εντολές του χειριστή από τον πομπό στον δέκτη.



Εικόνα 2.14 *Πομπός και δέκτης*

2.3.7 Μπαταρία

Η μπαταρία είναι ένα από τα σημαντικότερα εξαρτήματα καθώς αποτελεί πηγή ενέργειας όλων των ηλεκτρονικών συστημάτων τους, όπως οι αισθητήρες ή τα συστήματα ώθησης. Σήμερα, η διάρκεια πτήσης των drones είναι σχετικά περιορισμένη λόγω των περιορισμών που παρουσιάζουν οι σύγχρονες τεχνολογίες ενέργειας. Αυτό σημαίνει, ότι ένας από τους σημαντικότερους παράγοντες ώστε να υπάρξει ευρεία διάδοση των drones, είναι η τεχνολογία των μπαταριών, που θα πρέπει να εξελιχθεί ώστε να προσφέρει προϊόντα που να συνδυάζουν μικρό βάρος και κόστος και μεγάλη αυτονομία. Η χρήση μπαταριών Lithium-Polymer (LiPo) έφεραν την επανάσταση στην σχεδίαση των drones, καθώς συνδυάζουν μικρό μέγεθος και βάρος με καλή απόδοση [24]

Κάποια από τα σημαντικά της χαρακτηριστικά είναι η χωρητικότητα, το βάρος, η μέγιστη ένταση ρεύματος, η ταχύτητα φόρτισης και οι κύκλοι ζωής.



Εικόνα 2.15 *DJI Mavic Pro - 3830 mAh LiPo Battery*

2.3.8 Gimbal

Το gimbal είναι ένα εξάρτημα που συνοδεύει μια κάμερα ή έναν άλλο αισθητήρα και σταθεροποιεί τον προσανατολισμό και την περιστροφή του στους τρεις άξονες. Χρησιμοποιώντας γυροσκόπιο, το gimbal επιτρέπει στην κάμερα ή τον αισθητήρα να προσανατολίζεται και να σταθεροποιείται ανεξάρτητα από το drone. Χρησιμοποιείται κυρίως για την καταγραφή σταθερής και ομαλής ροής βίντεο . Χωρίς gimbal, το χρησιμοποιούμενο εξάρτημα θα είναι επιρρεπές σε θόρυβο από κραδασμούς όταν το όχημα επιταχύνει ή αλλάζει στάση. [13]



Εικόνα 2.16 *Gimbal*

2.4 Αισθητήρες εμπορικών drones

Τα εξαρτήματα και οι αισθητήρες του drone ποικίλλουν ανάλογα με τις αποστολές για τις οποίες έχει σχεδιαστεί, επιτρέποντάς του να συλλέγει δεδομένα που αφορούν την κατάσταση λειτουργίας του και το περιβάλλον του. Σε ορισμένες περιπτώσεις, εάν ο σχεδιασμός το επιτρέπει, το drone μπορεί να είναι εξοπλισμένο με επιπλέον εξαρτήματα και αισθητήρες πέραν των ενσωματωμένων και διαφορετικού μεγέθους και δυνατοτήτων για διαφορετικούς τύπους drone. Για παράδειγμα, οι προδιαγραφές των αισθητήρων και των εξαρτημάτων για ένα HALE UAV θα είναι αρκετά διαφορετικές από τις αυτές για ένα MAV. [23]

2.4.1 Μονάδα αδρανειακής μέτρησης (IMU)

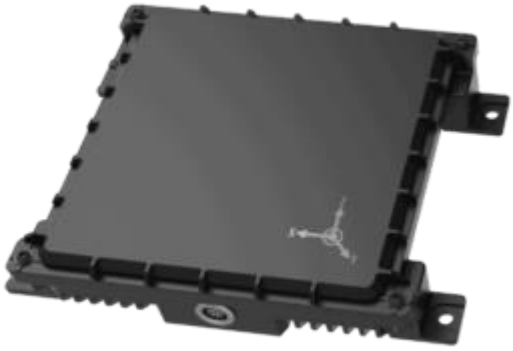
Η IMU είναι ο πιο κρίσιμος αισθητήρας για τον προσδιορισμό της κατάστασης ενός drone. Η IMU χρησιμοποιεί έναν συνδυασμό επιταχυνσιόμετρων και γυροσκοπίων για τον προσδιορισμό της ταχύτητας, του προσανατολισμού και της βαρυτικής έλξης. Η ερμηνεία των εξόδων της, μας επιτρέπει να αναπαραστήσουμε το drone στον τρισδιάστατο χώρο, χρησιμοποιώντας τόσο την τρισδιάστατη θέση του κέντρου μάζας όσο και τις 3 δυναμικές γωνίες πτήσης (yaw, pitch, roll). Γενικά, τα drones φέρουν ελαφριές και μικρού μεγέθους IMU.



Εικόνα 2.17 *IMU*

2.4.2 Αισθητήρας υψομέτρου

Μετρά το υψόμετρο του αεροσκάφους. Μερικές φορές είναι ενσωματωμένος στην IMU. Ένας παράγοντας που περιπλέκει το θέμα είναι ότι τα υψόμετρα των drones μπορούν να λειτουργούν με διαφορετικούς μηχανισμούς. Σε ορισμένες περιπτώσεις, μπορεί να διαθέτουν περισσότερα από ένα συστήματα μέτρησης του υψομέτρου και να εναλλάσσονται μεταξύ τους υπό ορισμένες συνθήκες.



Εικόνα 2.18 *Αισθητήρας υψομέτρου*

2.4.2.1 Υπέρυθρες

Τα περισσότερα διαθέτουν αισθητήρες που είναι στραμμένοι προς τα κάτω και χρησιμοποιούν υπέρυθρες ακτίνες. Αυτοί ονομάζονται συνήθως VPS (Vision Positioning System). Είναι ακριβές, δεδομένου ότι το drone δεν πετάει πάνω από ανακλαστική επιφάνεια, όπως το νερό και είναι μέσα στα όρια ύψους.

Ο κύριος περιορισμός του VPS που βασίζεται στις υπέρυθρες είναι ότι λειτουργεί μόνο σε ένα μικρό εύρος υψομέτρων. Στα περισσότερα μη επανδρωμένα αεροσκάφη, το όριο αυτό είναι περίπου στα 8 μέτρα AGL (Above Ground Level). Πέρα από αυτό, το υπέρυθρο σήμα γίνεται πολύ αδύναμο λόγω της φυσικής εξασθένησης.

2.4.2.2 Βαρομετρικός αισθητήρας

Ο κυρίαρχος μηχανισμός μέτρησης του υψομέτρου στα drones είναι με βαρομετρικό αισθητήτα. Αυτός μετρά το υψόμετρο ως συνάρτηση της πίεσης του αέρα. Καθώς το μη επανδρωμένο αεροσκάφος κερδίζει ύψος, η ένδειξη της πίεσης του αέρα μειώνεται σταθερά. Μπορεί να μετρήσει το υψόμετρο στα μέγιστα επίπεδα που μπορεί να φτάσει ένα drone και να μετρήσει τόσο το σχετικό όσο και το απόλυτο υψόμετρο. Αυτό σημαίνει ότι καταγράφει ταυτόχρονα το υψόμετρο σε μονάδες MSL και AGL. Οποιαδήποτε ή και οι δύο αυτές ενδείξεις μπορεί να είναι σημαντικές ανάλογα με την περίπτωση. Ωστόσο, εντός της πτήσης, οι μετρήσεις του υψομέτρου μπορεί να κυμαίνονται λόγω τυχόν σημαντικών αλλαγών στην πίεση του αέρα ή στη θερμοκρασία.

2.4.2.3 GPS

Οι ενσωματωμένοι δέκτες GPS καθορίζουν τη θέση του χρησιμοποιώντας δεδομένα από διάφορους δορυφόρους. Χρησιμοποιείται κυρίως για τον προσδιορισμό της οριζόντιας θέσης ενός drone. Τα δεδομένα GPS μπορεί επίσης να χρησιμοποιηθούν και για τον προσδιορισμό του ύψους πτήσης ενός drone, ωστόσο θεωρείται λιγότερο ακριβής και μάλιστα πιο επιρρεπής σε αποκλίσεις σε σύγκριση με

το βαρομετρικό. Τα περισσότερα drones μπορούν να καταγράφουν τόσο το βαρομετρικό όσο και το GPS υψόμετρο.

Η ακρίβεια των δεδομένων θέσης GPS μπορεί να διαφέρει ανάλογα με την ισχύ του σήματος GPS. Μπορεί να επηρεαστεί από παρεμβολές, από άλλες πηγές ηλεκτρομαγνητικών σημάτων είτε από τυχόν μεγάλες κατασκευές κοντά που εμποδίζουν το σήμα GPS.



Εικόνα 2.19 *GPS*

2.4.3 Κάμερα

Η κάμερα, είναι πολύ σημαντική καθώς θα είναι το βασικό κομμάτι επικοινωνίας μεταξύ του τι «βλέπουν» το όχημα και ο χειριστής. Συνήθως είναι μικρού μεγέθους και υψηλής ευκρίνειας (HD, 2K, 4K) [4]



Εικόνα 2.20 *Κάμερα*

2.4.4 Εικονοληπτικοί αισθητήρες

Αξίζει να αναλυθούν περαιτέρω στην κατηγορία των καμερών καθώς αποτελούν ένα βασικό κομμάτι των drones. Η διάκριση των αισθητήρων τους είναι η εξής: [25]

Αισθητήρες ορατού φάσματος: Λειτουργούν στα μήκη κύματος 0,4-0,7μm και μετατρέπουν την εικόνα σε ραδιοφωνική συχνότητα και την μεταφέρουν στον πομπό.

Πολυφασματικές κάμερες: Λειτουργούν στα μήκη κύματος 350-1000nm και εντοπίζουν την ανωμαλία του εδάφους. Για εφαρμογές στη γεωργία, η πολυφασματική απεικόνιση ανιχνεύει πράσινο, κόκκινο, κόκκινο εγγύς του υπέρυθρου και εγγύς υπέρυθρο φως για να συλλέξει πληροφορίες για τις καλλιέργειες και τα χωράφια που το ανθρώπινο μάτι δεν μπορεί να δει. Πέρα από τις παραπάνω χρήσεις που καλύπτονται και από την απλή RGB κάμερα, η πολυφασματική είναι πολύ χρήσιμη για τον προσδιορισμό δεικτών βλάστησης. [26]

Υπερφασματικές κάμερες: Λειτουργούν στα μήκη κύματος 350-2500nm. Αρχικά αναπτύχθηκε για στρατιωτική και διαστημική χρήση, όμως η υπερφασματική απεικόνιση εφαρμόζεται τώρα μεταξύ άλλων και σε άλλους κλάδους. Παρέχει δεδομένα σε πολύ περισσότερα μήκη κύματος (bands) σε ολόκληρο το συνεχές ηλεκτρομαγνητικό φάσμα του χρώματος και του φωτό, σε αντίθεση με μια πολύφασματικη κάμερα. Τα δεδομένα μιας υπερφασματικής είναι πιο ογκώδη και

περίπλοκα καθώς και με πολύ μεγαλύτερο κόστος. Ο τεράστιος όγκος δεδομένων σε συνδυασμό με το ακριβό υλικό και την πολυπλοκότητα της λειτουργίας και της επεξεργασίας δεδομένων αποτελούν συνήθως σημαντικές προκλήσεις για τον χειρισμό και την ανάλυση υπερφασματικών δεδομένων.

Κάμερα θερμικής απεικόνισης: Η θερμική ακτινοβολία αποτελείται από μήκη κύματος των 0,7-1000 μm ενώ οι κάμερες θερμικής απεικόνισης εστιάζουν σε δύο τμήματα αυτής, των 3-5μm και 7-15μm. Αυτά τα τμήματα είναι μικρού και μεγάλου μήκους κυμάτων IR (InfraRed) αντίστοιχα. Όσο υψηλότερη είναι η θερμοκρασία ενός αντικειμένου, τόσο υψηλότερη είναι η εκπεμπόμενη θερμική ακτινοβολία. Οι περιβαλλοντικές συνθήκες μπορούν να επηρεάσουν τις θερμικές μετρήσεις, οι οποίες πρέπει να λαμβάνονται υπόψιν για τις εφαρμογές θερμικών καμερών. Αυτό περιλαμβάνει τις αλλαγές της ταχύτητας του ανέμου, της ηλιακής ακτινοβολίας και της θερμοκρασίας του αέρα κατά τη διάρκεια μιας πτήσης.

2.4.5 Radar

Μέσω μιας κεραίας τοποθετημένης στο drone, κάθετα στην κατεύθυνση της πτήσης, χρησιμοποιώντας την έννοια της μέτρησης των χρόνων άφιξης των παλμών, στέλνει ηλεκτρομαγνητικά κύματα για να χαρτογραφήσει το περιβάλλον. Οι διαφορές στο χρόνο άφιξης του ανακλώμενου σήματος ραντάρ δημιουργούν διακυμάνσεις στα κύματα, οι οποίες, όταν συνδυάζονται, μπορούν να δημιουργήσουν μια εικόνα των αντικειμένων. [13]



Εικόνα 2.21 *Synthetic Aperture Radar*

2.4.6 LiDAR

Χρησιμοποιώντας τη σταθερή ταχύτητα του φωτός, οι αισθητήρες αυτοί εκτοξεύουν παλμούς λέιζερ σε επιφάνειες και μετρούν το χρόνο που χρειάζεται κάθε παλμός για να επιστρέψει. Χρησιμοποιώντας το χρόνο επιστροφής, ο αισθητήρας μπορεί να υπολογίσει την απόσταση μεταξύ του ίδιου και της επιφάνειας. Το LiDAR (Light Detection and Ranging) δεν επηρεάζεται από το φως του ήλιου (ενώ οι κάμερες επηρεάζονται πολύ) και είναι ταχύτερος στη μέτρηση της απόστασης από επιφάνειες από όλους τους αισθητήρες που παρουσιάζονται. Αυτοί οι αισθητήρες είναι ιδιαίτερα χρήσιμοι καθώς η ποσότητα του φωτός στο περιβάλλον δεν επηρεάζει τις μετρήσεις, οπότε μπορούν να χρησιμοποιηθούν τόσο την ημέρα όσο και τη νύχτα. Ωστόσο, προς το παρόν είναι πολύ ακριβοί και δύσχρηστοι. [13]



Εικόνα 2.22 *LiDAR*

2.4.7 Σόναρ

Χρησιμοποιώντας παρόμοια θεωρία με το LiDAR, οι αισθητήρες σόναρ στέλνουν παλμούς ήχου με γνωστές ταχύτητες, που ονομάζονται "pings", σε μια επιφάνεια. Μετρώντας το χρόνο που χρειάζεται ο παλμός για να επιστρέψει στον αισθητήρα, προσδιορίζεται η απόστασή του από την επιφάνεια. Επειδή τα ηχητικά κύματα είναι σχετικά αργά, το σόναρ χρησιμοποιείται κυρίως σε εσωτερικούς χώρους ή σε προσγειώσεις όπου το UAV βρίσκεται πολύ κοντά στις επιφάνειες που προσπαθεί να ανιχνεύσει. Επιπλέον, οι αισθητήρες αυτοί είναι ιδιαίτερα ευαίσθητοι στις παρεμβολές. Για παράδειγμα, εάν πολλά drones που χρησιμοποιούν αισθητήρες σόναρ λειτουργούν σε κοντινή απόσταση, θα "ακούσουν" ο ένας τους παλμούς του άλλου, με αποτέλεσμα να προκύψουν ανακριβείς μετρήσεις. Αυτοί οι αισθητήρες είναι σχετικά φθηνοί και ελαφροί, οπότε και προτιμώνται κυρίως στα εμπορικά drones. [13]



Εικόνα 2.23 *Σόναρ*

3. ΚΙΝΔΥΝΟΙ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ

Ενώ υπάρχουν πολλά οφέλη από την ανάπτυξη και την χρήση των drones σε μη στρατιωτικές εφαρμογές, ορισμένοι ακαδημαϊκοί, οργανώσεις και δημοσιογράφοι εκφράζουν σημαντικές ανησυχίες για τα drones. Θέματα προς συζήτηση αποτελούν η ασφάλεια της ανθρώπινης ζωής, το ενδεχόμενο ηθικών πρακτικών και πρακτικών που παραβιάζουν την ιδιωτική ζωή και αποτελούν σαφή απειλή για τις πολιτικές ελευθερίες. [27]

Για την ανάπτυξη ενός συστήματος που αντιμετωπίζει απειλές που προέρχονται από drones, θα πρέπει να ληφθεί υπόψη ότι η τεχνολογία των drones δεν έχει φτάσει στο απόγειό της, καθώς ένα σύστημα πρέπει να επιλύει μια μελλοντική ανάγκη και όχι μόνο την τρέχουσα. Το πρόβλημα εικάζεται ότι θα μεγαλώνει με τον χρόνο, δεδομένου ότι θα αυξηθεί η παραγωγή τους, οι δυνατότητές τους αλλά και η χρήση τους για παραβατικούς σκοπούς.

3.1 Ατυχήματα

Η ασφάλεια αποτελεί ένα από τα κύριους προβληματισμούς των ατόμων που επικρίνουν την χρήση ευρείας κλίμακας των drones, λόγω ελλιπής συντήρησης, σφάλματος του χειριστή και πιθανής χρήσης τους ως όπλα. Επειδή πρόκειται μη επανδρωμένα οχήματα, μπορεί να συντηρούνται λιγότερο καλά και κατά συνέπεια, να είναι λιγότερο αξιόπιστα από τα αεροσκάφη που μεταφέρουν προσωπικό. Το σημερινό ποσοστό ατυχημάτων με drones είναι 100 φορές μεγαλύτερο από εκείνο των επανδρωμένων αεροσκαφών. Το Electronic Privacy Information Center υποστηρίζει ότι αυτά τα στατιστικά αυξάνουν τους κινδύνους για τα συμβατικά αεροσκάφη και τους πολίτες που παρακολουθούνται. [27]

Το 2007, το Εθνικό Συμβούλιο Ασφάλειας Μεταφορών των ΗΠΑ ανέφερε ότι η αιτία της συντριβής του Predator τον Απρίλιο του 2006 ήταν το λάθος του χειριστή, καθώς η ομάδα που χειριζόταν το UAV έσβησε κατά λάθος τον κινητήρα. Τα δυστυχήματα με drones έχουν οδηγήσει σε περιορισμούς στην χρήση τους σε ορισμένα αθλήματα, όπου κινδυνεύουν να πέσουν πάνω σε πλήθος κόσμου. Ο σκιέρ

σλάλομ κατάβασης Marcel Hirscher απείχε κλάσματα του δευτερολέπτου από το να χτυπηθεί από ένα βαρύ drone με κάμερα σε αγώνα το 2015. Η σωστή χρήση και η βελτίωση των υλικών θα ελαχιστοποιήσουν πιθανότατα τον κίνδυνο που ενέχουν τα drones. Η αυτοματοποίηση και ενδεχομένως ο εξοπλισμός τους με αλεξίπτωτα θα μπορούσαν να μειώσουν τον κίνδυνο ατυχήματος.

Τον Οκτώβριο του 2017 το CNN ήταν η πρώτη αμερικανική ειδησεογραφική εταιρεία που πήρε άδεια να πετάξει πάνω από πλήθος κόσμου. Για να γίνει αυτό, χρησιμοποιήθηκε ένα ειδικό ελαφρύ drone με καλυμμένους έλικες και ασφαλή σχεδιασμό για την περίπτωση συντριβής. [28]

3.2 Ηθική και δεοντολογία

Εκτός από τις ανησυχίες σχετικά με την ασφάλεια, υπάρχουν πολλοί προβληματισμοί σχετικά με τη χρήση των drones σε μη στρατιωτικές εφαρμογές. Επίσης υπάρχει συζήτηση σχετικά με τη δεοντολογία της χρήσης UAVs σε στρατιωτικές επιχειρήσεις, καθώς ευθύνονται για σημαντικές απώλειες ζωών στο πεδίο της μάχης. Αναφορικά με τις μη στρατιωτικές εφαρμογές τους, ο Hayes, από το Big Brother Watch, δηλώνει ότι τόσο τα drones όσο και άλλα ρομποτικά οχήματα θα αυξήσουν τους κινδύνους υιοθέτησης μιας συμπεριφοράς τύπου Playstation στα σύνορα της Ευρώπης, όπου τα ανθρώπινα σώματα μετατρέπονται σε αντικείμενα που πρέπει να παρακολουθούνται, να ελέγχονται, να εκτιμώνται και να εξουδετερώνονται. [29]

Ωστόσο, υπάρχει διαφωνία σχετικά με τον τρόπο με τον οποίο τα drones αντιμετωπίζουν τους στόχους μέσω της διακριτικής παρακολούθησης. Αρκετοί υποστηρίζουν ότι τα drones εγείρουν ανησυχίες για τις πολιτικές ελευθερίες επειδή ο καθένας παρακολουθείται, φωτογραφίζεται και στοχοποιείται, ενώ η δυνατότητα των drones να φέρουν όπλα εγείρει πιο πολλές ανησυχίες για την ασφάλεια και την ανθρώπινη ζωή. [27]

3.3 Προστασία προσωπικών δεδομένων

Η προστασία της ιδιωτικής ζωής αποτελεί βασικό ζήτημα των ατομικών ελευθεριών αναφορικά με την χρήση των drones. Οι υπηρεσίες επιβολής του νόμου έχουν προσπαθήσει να μετριάσουν τις φωνές σχετικά με την προστασία των προσωπικών δεδομένων, υποστηρίζοντας ότι τα drones δεν διαφέρουν από μια σειρά υφιστάμενων συστημάτων επιτήρησης, όπως οι κάμερες κλειστού κυκλώματος παρακολούθησης ή τα ελικόπτερα. Αν και αυτό μπορεί να είναι σε γενικές γραμμές αληθές, το επιχείρημα αυτό δεν εξετάζει την τρέχουσα πολυμορφία των συστημάτων UAS, τα οποία μπορεί να χρησιμοποιούνται όπως οι σταθερές κάμερες CCTV σε ορισμένες περιπτώσεις ή όπως τα ελικόπτερα σε άλλες περιπτώσεις, ούτε αντιμετωπίζει τις πιθανές μελλοντικές εξελίξεις στις δυνατότητες ή τα ωφέλιμα φορτία τους. [27]

Οι Finn και Wright αναφέρουν ότι η βιομηχανία των drones, λόγω των εμπορικών εφαρμογών τους που ελέγχονται από ιδιωτικούς φορείς, θέτει σε κίνδυνο την προστασία της ιδιωτικότητας, των προσωπικών δεδομένων και της δεοντολογίας. Οι προκλήσεις αυτές οφείλονται στην έλλειψη γνώσης και στην «αδιαφορία» ως προς το σχετικό κανονιστικό πλαίσιο της ΕΕ [27]. Επιπλέον σημειώνουν ότι η ιδιωτικότητα συχνά συνδέεται με την τοποθεσία, τη συμπεριφορά και τα χαρακτηριστικά του σώματος και επηρεάζεται και από τη συμπεριφορά των χειριστών των drones. Σημειώνουν ότι με ένα drone, οι χειριστές μπορούν να αντλήσουν μεγάλο πλήθος πληροφοριών σχετικά με τη θέση κάποιου, τις συνήθειές του και την εξωτερική του εμφάνιση, αντλώντας έτσι τις περισσότερες φορές ακόμα και ακούσια, προσωπικές πληροφορίες και δεδομένα, θέτοντας σε κίνδυνο θεμελιώδη δικαιώματα όπως η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, όπως αυτά ορίζονται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. [30]

Η εισβολή των drones στην κοινωνική ζωή μπορεί να έχει σωματικές, ψυχολογικές και κοινωνικές επιπτώσεις. Τα συμβατικά αεροσκάφη επιτήρησης, όπως τα ελικόπτερα σε αντίθεση με τα drones, παρέχουν ακουστική ειδοποίηση ότι πλησιάζουν και επιτρέπουν σε ένα άτομο να λάβει μέτρα για να κρατήσει ιδιωτικές

τις δραστηριότητες που δεν επιθυμεί να εκθέσει σε δημόσια θέα. Η μαζική χρήση των drones τα οποία δεν γίνονται αντιληπτά από το έδαφος θα μπορούσε να οδηγήσει σε ένα περιβάλλον όπου οι πολίτες θα πιστεύουν ότι ένα drone τα παρακολουθεί ακόμη και όταν δεν υπάρχουν. Η φοβία αυτή ενδέχεται να οδηγήσει σε μια συμπεριφορά ενσυνείδητης πειθαρχίας, όπως περιγράφηκε για πρώτη φορά από τον Bentham και τον Foucault, όπου τα άτομα προσαρμόζουν τη συμπεριφορά τους σαν να παρακολουθούνται ανά πάσα στιγμή. [31]

Επομένως, θα πρέπει τα δεδομένα που συλλέγονται με τη χρήση των drones να μην δημιουργούν προβλήματα σε θέματα προστασίας των προσωπικών δεδομένων. Αναφορικά με τη συλλογή προσωπικών δεδομένων μέσω καμερών ή άλλου τύπου αισθητήρων που είναι εγκατεστημένοι στο drone και με βάση την ισχύουσα νομοθεσία προστασίας δεδομένων, αν δεν έχει προηγηθεί συναίνεση, δεν έχουν παρθεί τα απαραίτητα μέτρα ασφαλείας ή δεν υπάρχει απόκρυψη προσωπικών στοιχείων, αυτή θεωρείται παράνομη. Φυσικά οι χειριστές των drones, τις περισσότερες φορές δεν είναι εύκολο να έχουν τη συναίνεση του κόσμου σχετικά με τη συλλογή των προσωπικών τους δεδομένων. Επομένως, η όποια συλλογή δεδομένων εκμεταλλεύεται τα κενά της νομοθεσίας σχετικά με την τεχνολογία των drones. Οι χειριστές δεν υποχρεούνται να ενημερώσουν αλλά ούτε και να ειδοποιήσουν κανένα σχετικά με τη χρήση drone σε κάποια εφαρμογή. Κάτι τέτοιο αποτελεί έλλειψη ελέγχου σε θέματα που αφορούν την προστασία της ιδιωτικότητας και της συλλογής προσωπικών δεδομένων.

3.4 Εθνική ασφάλεια

Τα drones επιτρέπουν στην εξ’ αποστάσεως παρακολούθηση και επίθεση σε επιλεγμένους στόχους που βρίσκονται χιλιάδες χιλιόμετρα μακριά. Από νωρίς διαπιστώθηκε ότι η τεχνολογία αυτή είναι πολύ εύκολο να χρησιμοποιηθεί για εγκληματικές και τρομοκρατικές ενέργειες. [32]

3.4.1 Τρομοκρατικές ενέργειες

Η εύκολη πρόσβαση σε φθηνά drones με προδιαγραφές που φτάνουν ακόμα και αυτές στρατιωτικού υλικού, δίνει την ευκαιρία σε τρομοκρατικές οργανώσεις να εξοπλιστούν με drones, αυξάνοντας τις επιχειρησιακές τους δυνατότητες. Τα drones του εμπορίου, η τιμή των οποίων κυμαίνεται σε εκατοντάδες ευρώ, δεν μπορούν να συγκριθούν τεχνολογικά με τα στρατιωτικά UAVs πολλαπλών χρήσεων τύπου Predator ή Global Hawk, τα οποία κοστίζουν εκατομμύρια δολάρια, αλλά παρ' όλα αυτά δίνουν στους επίδοξους τρομοκράτες ή ένοπλες δυνάμεις έτερης χώρας έναν εύκολο τρόπο εισβολής στον εναέριο χώρο μιας χώρας-στόχου. [32]

3.4.2 Αεροδρόμια

Όπως και τα πτηνά, έτσι και τα drones αποτελούν σημαντικό κίνδυνο για τα μεγάλα επιβατικά αεροσκάφη. Ακόμη και το πιο μικρό drone μπορεί να προκαλέσει βλάβη σε κινητήρα τζετ με την απορρόφηση από την τουρμπίνα όταν λειτουργεί σε κοντινή απόσταση. Αν και πολλοί από τους κατασκευαστές drones έχουν περιορίσει τις πτήσεις κοντά σε αεροδρόμια, αυτά που πετούν σε μεγάλο ύψος σε οποιαδήποτε περιοχή μπορούν να αποτελέσουν απειλή για τα αεροσκάφη. Έχουν παρατηρηθεί πολλά περιστατικά σε αεροδρόμια, τα οποίο έχουν μεγάλο αντίκτυπο στην οικονομία και στο αίσθημα ασφάλειας. Το γεγονός ότι τα drones μπορούν να προκαλέσουν τεράστια οικονομική ζημία στα αεροδρόμια, αποτελεί έναν σημαντικό λόγο για τον οποίο σχεδόν όλα τα αεροδρόμια αποκτούν ή σχεδιάζουν να αποκτήσουν συστήματα C-UAS (Counter Unmanned Aerial System).

Το πιο σοβαρό περιστατικό συνέβη στο αεροδρόμιο Gatwick, όταν οι ζημιές που προκλήθηκαν από τη διακοπή της λειτουργίας του αεροδρομίου για 33 ώρες υπολογίστηκαν σε 50 εκατομμύρια λίρες [33]. Ακόμα και σήμερα, τα κράτη δεν είναι ακόμη σε θέση να αναπτύξουν αποτελεσματικά μέτρα κατά των drones ώστε να αποτρέπονται εκ των προτέρων πιθανές επιθέσεις.

3.5 Μελλοντικές προκλήσεις

3.5.1 Μεγαλύτερη εμβέλεια

Τα περισσότερα drones χρησιμοποιούν σήματα RF, πράγμα που προκαλεί περιορισμούς στην εμβέλεια και προβλήματα με τυχόν εμπόδια που εμποδίζουν το σήμα αυτό. Υπάρχει ωστόσο δυνατότητα χειρισμού του drone μέσω του διαδικτύου και του 5G που συνδυάζει υψηλό εύρος ζώνης με χαμηλούς χρόνους απόκρισης, γεγονός που εξαλείφει εντελώς αυτό το εμπόδιο. Επίσης, οι βελτιωμένες λειτουργίες αποφυγής εμποδίων θα βελτιώσουν την επιβιωσιμότητα του drone όταν το σήμα χάνεται. [22]

3.5.2 Ρομποτικά πτηνά

Μικρά ρομπότ που μοιάζουν με ζώα έχουν αναπτυχθεί εδώ και χρόνια που μιμούνται τις κινήσεις τους, όπως ρομποτικά πουλιά και εντόμα. Ρομποτικά αρπακτικά πουλιά πωλούνται ήδη σε αεροδρόμια για να τρομάζουν τα πτηνά ώστε να μειωθούν οι συγκρούσεις πουλιών με αεροσκάφη.

Ένα ρομποτικό πτηνό μπορεί να κάνει το έργο ενός συστήματος αντιμετώπισης drones πιο πολύπλοκο. Οι αισθητήρες που ανιχνεύουν τον ήχο των πολυκόπτερων δεν θα έχουν πλέον εφαρμογή, ενώ ο αλγόριθμος ανάλυσης συμπεριφοράς που χρησιμοποιείται για να ξεχωρίσει τα drones από τα πουλιά σε μια περιοχή που καλύπτεται από ραντάρ θα έχει μια νέα πρόκληση αν το μοτίβο κίνησής τους είναι όμοιο με αυτό των πτηνών.

3.5.3 Μικροσκοπικά drones

Η μείωση του μεγέθους των drones, σε αυτό της τάξης ενός εντόμου μπορεί να φαντάζει ελκυστικό για διάφορες εφαρμογές του μέλλοντος. Με την βελτίωση της αυτοματοποίησης και της συμπεριφοράς εντός ενός δικτύου ή σμήνους από drones, είναι πιθανό να επέλθει μείωση των εναέριων απειλών. Το μικρότερο μέγεθος θα επιφέρει μείωση της εμβέλειας και του μεγέθους του ωφέλιμου φορτίου. Ωστόσο, θα διευκολυνθεί η παρακολούθηση, η κατασκοπία και πιθανότατα τρομοκρατικές ενέργειες καθώς μικρές εκρηκτικές συσκευές θα μπορούσαν να απειλήσουν την εθνική ασφάλεια.

3.5.4 Σμήνη από drones

Τα στρατιωτικά σμήνη μη επανδρωμένων αεροσκαφών έχουν αποδείξει την αποτελεσματικότητά τους καθώς με το μικρό τους μέγεθος είναι δύσκολο να εντοπιστούν και να εξουδετερωθούν. Επίσης, οι αλγόριθμοι του λογισμικού ενός σμήνους θα βελτιώσουν τον χειρισμό τους και την αποφυγή της συντριβής.

Μελλοντικά, τα σμήνη από drones ενδεχομένως να συμβάλλουν σε εργασίες κατασκευών, ενώ ήδη η Disney και η Intel είναι δύο από τις εταιρείες που χρησιμοποιούν σμήνη σε επιδείξεις με φωτισμό LED, με περίπου 500 drones.

4. ΑΝΤΙΜΕΤΩΠΙΣΗ ΑΠΕΙΛΩΝ

Η αντιμετώπιση των εχθρικών drones μπορεί να διακριθεί σε δύο φάσεις: στην φάση του εντοπισμού και στην φάση των παρεμβολών. Η επιλογή της κατάλληλης μεθόδου εντοπισμού και αντιμετώπισης θα εξεταστεί σε αυτήν την ενότητα.

4.1 Μέθοδοι εντοπισμού drone

Ο εντοπισμός ενός drone είναι δύσκολη υπόθεση. Η μέθοδος εντοπισμού εξαρτάται από τον τύπο του drone και τις παραμέτρους του. Τα μικρά σε μέγεθος drones είναι πιο δύσκολο να εντοπιστούν από τα μεγάλα στρατιωτικά UAVs, για τα οποία χρησιμοποιείται συνήθως κάποιο σύστημα ραντάρ. Τα μικρά εμπορικά drones, λόγω του μεγέθους τους, δεν διαθέτουν μεγάλες ανακλαστικές επιφάνειες και επομένως η ανίχνευση με ραντάρ είναι πολύ δύσκολη έως αδύνατη. Επομένως, είναι απαραίτητη η χρήση άλλων σύγχρονων μεθόδων εντοπισμού, όπως τα ευφυή ψηφιακά μέσα (intelligent video analysis) ή η ακουστική ανίχνευση. Οι περισσότερες μέθοδοι, επομένως, χρησιμοποιούν κάποιο χαρακτηριστικό του drone ή ένα συνδυασμό τους. Ακολουθεί ενδεικτικά μία αντιστοιχία των μεθόδων εντοπισμού με βάση χαρακτηριστικά του drone: [32]

Χαρακτηριστικό του drone	**Μέθοδος εντοπισμού**
Αντανάκλαση ραδιοκυμάτων	Ανίχνευση με ενεργό ραντάρ
Θερμική ακτινοβολία	Θερμογραφική ανίχνευση
Εκπομπή ραδιοφωνικού σήματος	Ανίχνευση με παθητικό ραντάρ
Ακουστικά κύματα	Ακουστική ανίχνευση
Οπτική ορατότητα	Ανάλυση βίντεο

Πίνακας 4.1 *Χαρακτηριστικά των drones και μέθοδοι εντοπισμού*

Καθεμία από αυτές έχει τα υπέρ και τα κατά της, δηλαδή τις περιπτώσεις που είναι κατάλληλη για εφαρμογή και τις περιπτώσεις που τα αποτελέσματά της στον εντοπισμό δεν είναι ικανοποιητικά. Γι' αυτό συνήθως εφαρμόζονται πολλές διαφορετικές τεχνικές μαζί. [34]

Surveillance technology	Drone signature	Localization/tracking method	Detection range	Challenges
Radar	Micro Doppler	Doppler-based tracking delay-based localization	≤3000 m	Low radar cross section Low speed and altitude
Audio	Time-frequency feature	DOA-based localization	40–300 m	High ambient noise
Video	Appearance feature Motion feature	Motion-based tracking	100–1000 m	Occlusion Indistingushable small objects
RF	Communication channel	RSS/DOA-based localization	≤1000 m	Ambient RF noise Multipath Non-line of sight

Εικόνα 4.1. *Σύγκριση μεθόδων εντοπισμού [35]*

Το περιβάλλον στο οποίο επιδιώκεται ο εντοπισμός είναι επίσης καθοριστικό για την επιλογή της μεθόδου. Ο εντοπισμός ενός drone στον εναέριο χώρο ενός αεροδρομίου αφορά εντοπισμό σε ανοιχτό πεδίο, ενώ ο εντοπισμός σε περιοχή με κτίρια αφορά την περιοχή πλησίον των υποδομών του αεροδρομίου, περιοχή που δεν μπορεί να προσεγγιστεί από drone μετά από έναν πετυχημένο εντοπισμό σε ανοιχτό πεδίο.

Παρακάτω παρουσιάζονται οι μέθοδοι εντοπισμού και περιγράφονται οι αντίστοιχες αρχές λειτουργίας τους, τα πλεονεκτήματα καθώς και τα μειονεκτήματά τους.

4.1.5 Εντοπισμός με ραντάρ

Τα συστήματα ραντάρ χρησιμοποιούνται ευρέως τόσο στην καθημερινή ζωή όσο και σε στρατιωτικές εφαρμογές. Τα συμβατικά συστήματα ραντάρ είναι προσαρμοσμένα για την ανίχνευση σχετικά μεγάλων αντικειμένων και δεν είναι κατάλληλα για την ανίχνευση μικρών drones, ιδίως όταν η ταχύτητά τους είναι μικρή, όταν πετούν σε χαμηλό ύψος ή όταν αιωρούνται. Η δυνατότητα εκτέλεσης ελιγμών με μεγάλη ευκολία είναι επίσης περιοριστικός παράγοντας στην ανίχνευσή τους καθώς οι διαστάσεις των drones και ο τρόπος με τον οποίο κινούνται έχουν ως αποτέλεσμα ίχνος ανίχνευσης στο ραντάρ παρόμοιο με των πτηνών [36]. Αποτέλεσμα των ανωτέρω διαπιστώσεων είναι ότι, ο εντοπισμός drone με ραντάρ δεν αξιόπιστος. Μερικά από αυτά τα συστήματα που έχουν υλοποιηθεί παρουσιάζονται στο [37].

Πλεονεκτήματα

1. Εντοπισμός σε μεγάλη απόσταση, όταν δεν υπάρχουν εμπόδια.
2. Εντοπισμός αυτόνομων drones, τα οποία δεν έχουν επικοινωνία με χειριστή και δεν εκπέμπουν σήμα.
3. Εντοπισμός drones σε κακές καιρικές συνθήκες και σε συνθήκες χαμηλού φωτισμού.
4. Είναι δυνατός (αν και όχι εύκολος) ο διαχωρισμός των drones από τα πτηνά.

Μειονεκτήματα

1. Δεν αντανακλούν όλα τα υλικά με τον ίδιο τρόπο τα σήματα ραντάρ, με ορισμένα από αυτά να μην τα αντανακλούν καθόλου.
2. Δεν είναι δυνατός ο εντοπισμός πίσω από εμπόδια, γεγονός που συμβάλλει ιδιαίτερα στην υποβάθμιση των δυνατοτήτων τους σε αστικές περιοχές-
3. Βλαβερά υψηλή ακτινοβολία εκπομπής, γεγονός που σημαίνει ότι δεν είναι επιτρεπτή η εφαρμογή ενός ραντάρ σε πολυσύχναστες περιοχές. [35]
4. Η διαφορά μεταξύ ενός και δέκα χιλιομέτρων απόστασης από τον ίδιο στόχο μεταφράζεται θεωρητικά σε ανάγκη εκπομπής 10.000 φορές ισχυρότερου σήματος για να επιτευχθεί το ίδιο αποτέλεσμα. Η απλοποιημένη εξίσωση του ραντάρ δείχνει ότι, με το διπλασιασμό της εμβέλειας R για να επιτευχθεί το ίδιο λαμβανόμενο αποτέλεσμα Pe πρέπει να πολλαπλασιαστεί το αποτέλεσμα εκπομπής P_S με συντελεστή 16:

$$P_e = \frac{P_S \cdot G^2 \lambda^2 \cdot \sigma}{(4\pi)^3 \cdot R^4}$$

Ο εντοπισμός ενός drone με την μέθοδο του ραντάρ είναι εφικτός μέσω διάφορων εφαρμογών.

4.1.5.1 Παλμικό ραντάρ

Παλμικό ραντάρ που χρησιμοποιεί την ίδια κεραία τόσο για εκπομπή όσο και για λήψη. Στέλνει έναν ισχυρό παλμό και στη συνέχεια μεταβαίνει σε λειτουργία λήψης. Τα πλεονεκτήματα αυτού του τύπου ραντάρ είναι ότι ο δέκτης δεν δέχεται παρεμβολή

από τον πομπό, καθώς δεν λειτουργούν ταυτόχρονα και δεν χρησιμοποιούνται από κοινού εξαρτήματα για την αποστολή και τη λήψη. [22]

Το μειονέκτημα της εναλλαγής μεταξύ εκπομπής και λήψης είναι ότι θα υπάρχει ένα εσωτερικό τυφλό σημείο. Εάν ένας παλμός έχει για παράδειγμα διάρκεια 1μs, ο παλμός διανύει 300 μέτρα σε αυτό το διάστημα. Στόχος σε απόσταση 140 μέτρων σημαίνει 280 μέτρα για να φτάσει στον στόχο και να επιστρέψει. Στην περίπτωση παλμού διάρκειας 1ms, το ραντάρ εξακολουθεί να εκπέμπει και δεν θα λάβει την επιστροφή του σήματος από τον στόχο. Ωστόσο, η χρονική διάρκεια της εναλλαγής μεταξύ εκπομπής και λήψης, περιορίζει αυτήν την απόσταση στην οποία το ραντάρ δεν εντοπίζει τον στόχο. [22]

Πλεονεκτήματα

- Μεγάλη εμβέλεια, καθώς ο δέκτης δεν δέχεται παρεμβολές από τον πομπό.

Μειονεκτήματα

- Τυφλό σημείο.

4.1.5.2 Ραντάρ συνεχούς κύματος με διαμόρφωση συχνότητας (Frequency Modulated Continuous Wave Radar - FMCW)

Αυτός ο τύπος ραντάρ εκπέμπει και λαμβάνει ταυτόχρονα, με αποτέλεσμα να μην έχει το τυφλό σημείο του παλμικού ραντάρ. Η συχνότητα εκπομπής μπορεί να αλλάξει ώστε να διακρίνει καλύτερα τον στόχο, καθώς διαφορετικές συχνότητες παράγουν διαφορετικές επιστροφές. [22]

Πλεονεκτήματα

- Δεν υπάρχει τυφλό σημείο.
- Μικρή μέγιστη ισχύς λόγω συνεχούς εκπομπής.

Μειονεκτήματα

- Οι παρεμβολές από την ταυτόχρονη εκπομπή και λήψη οδηγούν σε μείωση της εμβέλειας.

4.1.5.3 Ραντάρ FMCW υψηλής συχνότητας

Τύπος ραντάρ που λειτουργεί σε υψηλή συχνότητα με μεγάλη διακριτική ικανότητα στόχου. Η υψηλή συχνότητα έχει ως αποτέλεσμα μεγαλύτερη ατμοσφαιρική εξασθένηση, και κατ' επέκταση μικρότερη εμβέλεια. [22]

Πλεονεκτήματα

- Ομοίως με το FMCW.
- Καλύτερη διακριτική ικανότητα και λεπτομέρεια στον εντοπισμό.

Μειονεκτήματα

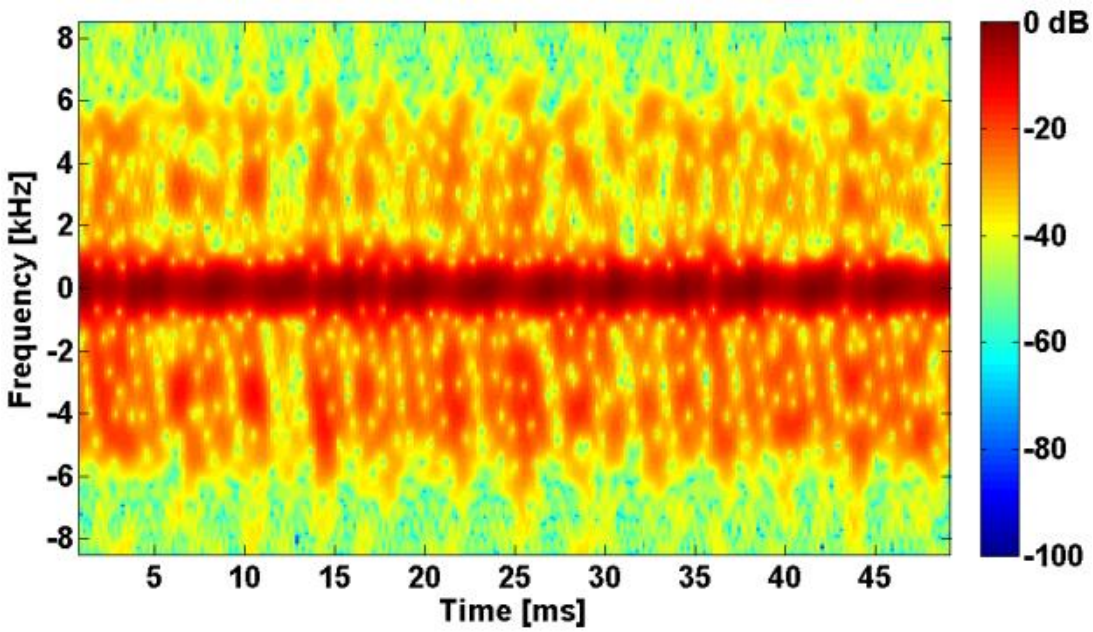
- Ομοίως με το FMCW.
- Μεγαλύτερη ατμοσφαιρική εξασθένηση σε σχέση με ραντάρ μικρότερων συχνοτήτων, που σημαίνει μικρότερη εμβέλεια.
- Μεγάλο κόστος εξαρτημάτων.

4.1.5.4 Doppler ραντάρ

Αυτή η μέθοδος αφορά τον τρόπο ανάλυσης των δεδομένων που λαμβάνονται και μπορεί να εφαρμοστεί σε διάφορες μεθόδους με ραντάρ. Χρησιμοποιείται για την ανίχνευση αντικειμένων με μικρή ραδιοδιατομή (Radar Cross Section – RCS). Τα ραντάρ υψηλής απόδοσης έχουν την ικανότητα να ανιχνεύουν micro UAV, με χαρακτηριστικό παράδειγμα στο [38], αλλά με δύο σημαντικά μειονεκτήματα. Το πρώτο είναι ότι παράγει μεγάλες ποσότητες δεδομένων και το δεύτερο είναι ότι, επειδή με το Doppler ανιχνεύονται οι ταχύτητες ενός αντικειμένου και λόγω του ότι ένα τετρακόπτερο μπορεί να αιωρείται και να ταξιδεύει με αργές ταχύτητες έως και 40 m/s, αυτό μπορεί να σημαίνει ότι το ραντάρ δεν θα μπορεί να διακρίνει αντικείμενα που αιωρούνται ή που κινούνται αργά. Μια λύση σε αυτό είναι να εξεταστεί το micro-Doppler αποτύπωμα που προκύπτει από τα πτερύγια του έλικα και παράγει ταχύτητες εύρους από 0 (στο μέσο του πτερυγίου) έως την ταχύτητα της άκρης του πτερυγίου που είναι στο πεδίο της συχνότητας. Αυτό σημαίνει ότι όχι μόνο εντοπίζεται ένας μικρός στόχος με ραντάρ, αλλά και διακρίνεται από άλλα αντικείμενα με παρόμοιες

ιδιότητες και δίνεται η δυνατότητα κατηγοριοποίησής του. Η Εικόνα 4.2 απεικονίζει την λήψη ενός Doppler ραντάρ για ένα τετρακόπτερο και συγκεκριμένα την συχνότητα λήψης στον άξονα του χρόνου. Ο κυματοειδής μορφή του σήματος προέρχεται από την ταχύτητα του κάθε πτερυγίου του έλικα, για κάθε μία από τις παρακάτω περιπτώσεις όπου και έχουμε μεγάλες ταχύτητες Doppler. [22]

1. Περιστρέφεται προς το ραντάρ (περίπου 135 m/s στην άκρη για ένα DJI phantom 4).
2. Επιβραδύνει και στιγμιαία μένει ακίνητο από την οπτική γωνία του ραντάρ, καθώς η άκρη κινείται πλευρικά και δεν παράγεται μεγάλο αποτύπωμα Doppler.
3. Απομακρύνεται από το ραντάρ, δημιουργώντας έτσι μια αρνητική συχνότητα στην εικόνα.
4. Επιβραδύνει και μένει ακίνητο στιγμιαία στην άλλη πλευρά.



Εικόνα 4.2 *Λήψη ενός Doppler ραντάρ*

<u>Πλεονεκτήματα</u>

- Δυνατότητα κατηγοριοποίησης ανάλογα με το αποτύπωμα κάθε drone.
- Δυνατότητα διαχωρισμού των drones από τα πτηνά.

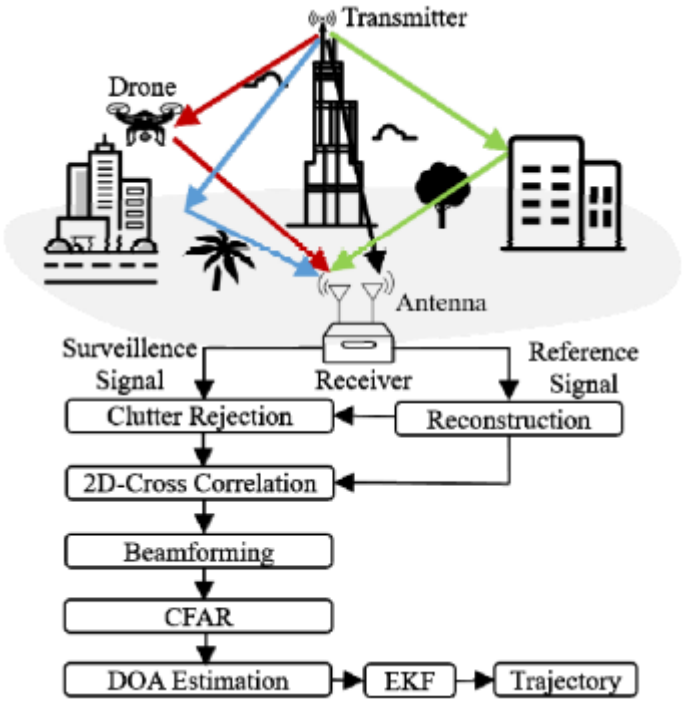
<u>Μειονεκτήματα</u>

- Εντοπισμός πτηνών και άλλων αντικείμενων από το ραντάρ.

- Κίνδυνος δημιουργίας μεγάλης ποσότητας δεδομένων προς επεξεργασία κατά την αναζήτηση.

4.1.5.5 Παθητικό ραντάρ

Τύπος ραντάρ στον οποίο ο μηχανισμός εκπομπής και ο μηχανισμός λήψης είναι ξεχωριστοί. Το παθητικό ραντάρ πηγαίνει αυτό το διαχωρισμό ένα βήμα παραπέρα και χρησιμοποιώντας τα υπάρχοντα σήματα που βρίσκονται στον αέρα ως εκπομπή, προσφέροντας οφέλη σε ορισμένα σημεία αλλά και σε σημαντικά μειονεκτήματα σε άλλα. [22]



Εικόνα 4.3 *Επεξεργασία σήματος παθητικού ραντάρ [39]*

Πλεονεκτήματα

- Μικρή κατανάλωση ενέργειας και ελαφρύτερη κατασκευή από το ενεργό ραντάρ.
- Σήματα όπως τα ψηφιακά τηλεοπτικά σήματα μεταδίδονται ευρέως και όλο το εικοσιτετράωρο.

Μειονεκτήματα

- Δεν υπάρχει αρκετή τεχνογνωσία.
- Τα αποτελέσματα εξαρτώνται από τις θέσεις των πομπών.
- Τα αποτελέσματα εξαρτώνται από τη συχνότητα του πομπού, η οποία μπορεί να δυσχεράνει την ανάλυση των πληροφοριών από τα δεδομένα που λαμβάνονται.

Όπως παρατηρήθηκε καθεμιά από τις μεθόδους που παρουσιάστηκαν έχει συγκεκριμένα πλεονεκτήματα και μειονεκτήματα. Η προστασία μιας περιοχής, όπως ένα αεροδρόμιο, μπορεί να πραγματοποιηθεί με ένα ραντάρ κινήσεων επιφανείας (Surface Movement Radar – SMR) ή με πολλά μικρότερα ραντάρ με χαμηλότερες δυνατότητες. Με την εφαρμογή της δεύτερης λύσης καλύπτονται και περιοχές που βρίσκονται πίσω από αντικείμενα και τα οποία δεν έχουν οπτική επαφή (LOS) με το ραντάρ. [40]

Ένα Doppler ραντάρ δύναται να εντοπίσει drones (τύπου τετρακόπτερου ή πολυκόπτερου) διαχωρίζοντάς τα από τα πτηνά [41]. Ο διαχωρισμός αυτός βασίζεται στο micro-Doppler αποτύπωμα της περιστροφής της έλικας του drone, καθώς το λαμβανόμενο φάσμα micro-Doppler έχει συγκεκριμένο και επαναλαμβανόμενο μοτίβο όταν το drone αντανακλά το σήμα του ραντάρ, ενώ αυτά τα χαρακτηριστικά δεν παρατηρούνται όταν πρόκειται για πτηνά που εντοπίζονται από το ραντάρ.

Η ραδιοτομή (RCS) ενός drone μπορεί επίσης να αποτελέσει βασική παράμετρο για τον εντοπισμό διάφορων τύπων drone, των οποίων οι έλικες δεν περιστρέφονται είτε περιστρέφονται πολύ αργά [42]. Γνωρίζοντας την τιμή RCS, η μέγιστη απόσταση Rmax μεταξύ του drone και του ραντάρ μπορεί να προσδιοριστεί από τη γνωστή εξίσωση.

$$R_{max} = \sqrt[4]{\frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 P_{min}}}$$ [1]

[1] R_{max} = απόσταση του drone
P_t = ισχύς εκπομπής
G = κέρδος κεραίας
A_e = άνοιγμα κεραίας
σ = ραδιοτομή του στόχου (dBsm)
P_{min} = ελάχιστο ανιχνεύσιμο σήμα δέκτη

Τέλος, στον τομέα των ραντάρ, θα μπορούσε να αξιοποιηθεί η τεχνολογία των LiDAR στην οποία αναφερθήκαμε προηγουμένως και έχει γίνει ένας από τους βασικούς αισθητήρες στη ρομποτική εξαιτίας της υψηλής ακρίβειάς του στον προσδιορισμό της θέσης. [43], [44]. Παρόλο που τα LiDAR εξακολουθούν να κοστίζουν αρκετά, τα πλεονεκτήματα της υλοποίησης αυτής είναι τα εξής:

- Εύκολος διαχωρισμός του αντικειμένου από το περιβάλλον.
- Εντοπισμός που δεν επηρεάζεται από τις καιρικές συνθήκες.
- Η ακριβής θέση του αντικειμένου προσδιορίζεται εύκολα μετά την ανίχνευσή του.

4.1.6 Εντοπισμός ραδιοσυχνοτήτων

Στα περισσότερα συστήματα των εμπορικών drones, υπάρχει αμφίδρομη μετάδοση δεδομένων μεταξύ του drone και ενός χειριστή στο έδαφος, στην ζώνη συχνοτήτων 2,4 ή 5GHz. Υπάρχει η δυνατότητα ανίχνευσης του σήματος που εκπέμπει το drone, ωστόσο πρόκειται για μια ζώνη συχνοτήτων που χρησιμοποιείται από τα περισσότερα ασύρματα routers (Wi-Fi) και από άλλα δίκτυα ασύρματης επικοινωνίας (WLAN). [22]

Το χαρακτηριστικό της διάδοσης RF σήματος, σε αστικές περιοχές, είναι η εξασθένησή του, η οποία είναι μεγαλύτερη από ό,τι στον ελεύθερο χώρο. Η εξασθένηση αυτή προσομοιώνεται με τον συντελεστή διάδοσης γ. Στον ελεύθερο χώρο το γ=2 ενώ σε άλλες περιπτώσεις η τιμή του γ κυμαίνεται από 1,6 (εντός κτιρίων ή σε περιοχές που βρίσκονται ανάμεσα από βουνά) έως 6 (εντός κτιρίων με πολλά εμπόδια) [45]. Στις αστικές περιοχές οι τιμές του γ κυμαίνονται μεταξύ 3 και 5 και λόγω της απόσβεσης κατά τη μετάδοση του σήματος από το drone στον χειριστή. Ως αποτέλεσμα των υψηλότερων τιμών του γ, είναι η μείωση της επιχειρησιακής εμβέλειας των drones γεγονός που σημαίνει μικρότερη ακτίνα εξάπλωσης RF σημάτων, μειώνοντας τις πιθανότητες εντοπισμού τους και την δυνατότητα παρεμβολής της επικοινωνίας [46]. Ως εκ τούτου, είναι απαραίτητη η υλοποίηση ενός πυκνότερου δικτύου αισθητήρων RF, εάν στόχος είναι η προστασία μιας αστικής περιοχής

Πλεονεκτήματα

1. Δεν απαιτείται εκπομπή σήματος αλλά μόνο παθητικός αισθητήρας σήματος RF.
2. Υπάρχει δυνατότητα εντοπισμού του χειριστή.
3. Τα περισσότερα εμπορικά drones στέλνουν δεδομένα στον χειριστή.
4. Προσπάθεια εντοπισμού μπορεί να γίνει χωρίς περιορισμούς και σε μη αστικές περιοχές, επειδή δεν υπάρχει ακτινοβολία.
5. Ως αποτέλεσμα της μη ανάγκης ύπαρξης πομπού, ο εξοπλισμός είναι απλούστερος από ό,τι στην περίπτωση του εντοπισμού με ραντάρ.

Μειονεκτήματα

1. Δεν είναι δυνατός ο εντοπισμός drones που δεν επικοινωνούν με τον χειριστή.
2. Η αυξημένη ασύρματη κυκλοφορία στο διαδίκτυο και σε δίκτυα WLAN στις συχνότητες που χρησιμοποιούνται για τις επικοινωνίες των drones αποτελεί σημαντική πηγή θορύβου.
3. Τα drones χρησιμοποιούν συχνά κατευθυντικές κεραίες, οπότε είναι δύσκολος ή ακόμη και μερικές φορές αδύνατος ο εντοπισμός των επικοινωνιών τους, εάν δεν γίνεται κοντά στον λοβό της κεραίας.

Η αξιοπιστία της ανίχνευσης RF σημάτων μπορεί να βελτιωθεί με την τοποθέτηση περισσότερων διάσπαρτων αισθητήρων και με την εφαρμογή ανάλυσης χρόνου εκτός από ανάλυση συχνότητας. Η χρονική διαφορά άφιξης (TDOA) προσδιορίζεται μεταξύ των στιγμών ανίχνευσης του σήματος RF του drone στους χωρικά διάσπαρτους αισθητήρες, και απαιτείται ο εντοπισμός του σήματος από τουλάχιστον 3 αισθητήρες για τον προσδιορισμό της θέσης του χειριστή [47]. Όσο περισσότεροι αισθητήρες υπάρχουν τόσο εξαλείφεται το πρόβλημα της μεγάλης εξασθένησης του σήματος σε αστικές περιοχές και κατ’ επέκταση της αδυναμίας εντοπισμού του λόγω των πολλών εκπομπών στις ίδιες ζώνες συχνοτήτων.

Επίσης δύναται να ανιχνευτεί ένα drone, εντοπίζοντας συγκεκριμένο αποτύπωμα στην RF επικοινωνία, που οφείλεται στις δονήσεις της ατράκτου του drone και στην ολίσθηση λόγω περιστροφής των ελίκων, τα οποία προκαλούν χαρακτηριστικές αλλαγές στο εκπεμπόμενο σήμα που μεταδίδεται από το drone στον χειριστή. Το λαμβανόμενο σήμα αναλύεται και διακρίνεται μεταξύ άλλων εκπομπών ίδιων

συχνοτήτων που παράγονται από άλλες πηγές, με την βοήθεια της εφαρμογής «ραδιοεπικοινωνίας μέσω λογισμικού» (Software Defined Radio - SDR). [48]. Επιπρόσθετα, ένας άλλος αξιόπιστος τρόπος εντοπισμού επιτυγχάνεται καταγράφοντας το φάσμα RF κατά τη διάρκεια της πτήσης ενός drone και στη συνέχεια τροφοδοτώντας τα ακατέργαστα δεδομένα σε ένα μοντέλο μηχανικής μάθησης. [49]

Ιδιαίτερο ενδιαφέρον παρουσιάζει η λύση που προτείνει τον εντοπισμό των αποτυπωμάτων που αφήνουν τα drone και συγκεκριμένα την διεύθυνση Media Access Control (MAC), καθώς αυτά λειτουργούν χρησιμοποιώντας ένα συνηθισμένο πρωτόκολλο Wi-Fi (802.11) για να συνδεθούν με μια συσκευή που εκτελεί ένα διαθέσιμο στην αγορά λογισμικό. Με αυτήν την μέθοδο είναι δυνατή η καταγραφή της κίνησης των πακέτων επικοινωνίας μεταξύ των συζευγμένων συσκευών, κάνοντας δυνατή την απόκτηση ελέγχου του drone. [50]

Πλεονεκτήματα

- Δεν εξαρτάται από το μέγεθος και το υλικό του drone.
- Δεν είναι απαραίτητο να υπάρχει οπτική επαφή μεταξύ του drone και του αισθητήρα.

Μειονεκτήματα

- Είναι δυνατή η ανίχνευση μόνο της διεύθυνσης MAC.
- Είναι δύσκολο να δημιουργηθεί και να ενημερωθεί βάση δεδομένων με όλες τις διευθύνσεις MAC των νέων drones.
- Η διεύθυνση MAC του drone μπορεί να παραποιηθεί προκειμένου να αποφευχθεί η ανίχνευση του. [35]

4.1.7 Ηχητικός εντοπισμός

Μπορούν να χρησιμοποιηθούν ειδικά μικρόφωνα για τον εντοπισμό των drones. Όπως και στην εντοπισμό με ραντάρ ή ραδιοσυχνότητες, κάθε τύπος drone έχει ένα ηχητικό αποτύπωμα που παράγεται από τους έλικες. Επειδή η ταχύτητα του ήχου στον αέρα είναι χαμηλή, είναι δυνατόν να εντοπιστεί ένα drone βάσει της διαφοράς του

χρόνου άφιξης του ήχου σε διάφορους ηχητικούς αισθητήρες. Μια εφαρμογή της μεθόδου αυτής είναι η χρήσης ενός συμπλέγματος από πολλά μικρόφωνα υπερήχων τοποθετημένα αρκετά κοντά το ένα στο άλλο, έτσι ώστε η ίδια περίοδος του ημιτονοειδές σήματος ήχου να φτάνει ταυτόχρονα σε όλα τα μικρόφωνα. Η σύγκριση του χρόνου άφιξης του ηχητικού κύματος χρησιμοποιείται για τον υπολογισμό της κατεύθυνσης της πηγής. [22]

4.1.7.1 Ανάλυση σήματος ήχου

Πολλοί αλγόριθμοι που εφαρμόζονται στην ανάλυση ομιλίας μπορούν επίσης να χρησιμοποιηθούν για τον εντοπισμό drone, επειδή αυτά τα δύο έχουν ομοιότητες. Τα αποτελέσματα μεθόδου ανάλυσης που χρησιμοποιεί αλγορίθμους γραμμικής προγνωστικής κωδικοποίησης (Linear Predictive Coding - LPC) και κλίσης του φάσματος συχνοτήτων (slope of the frequency spectrum), καταλήγουν σε ικανοποιητικό αποτέλεσμα εντοπισμού. [50]

Όμοια μέθοδος αλλά με την χρήση διαφορετικού αλγορίθμου που επικεντρώνεται σε διαφορετικά χαρακτηριστικά του λαμβανόμενου σήματος ήχου, παρουσιάζεται στο [51]. Τόσο με την πρώτη όσο και με την δεύτερη μέθοδο με την χρήση αλγορίθμου, είναι απαραίτητο να συγκριθούν τα αποτελέσματα που προκύπτουν με το ηχητικό αποτύπωμα του drone.

Αναφορικά με την τοποθέτηση των μικρόφωνων υπάρχουν τρεις τεχνικές με τις οποίες είναι δυνατός ο εντοπισμός της κατεύθυνσης του ήχου: [52]

1. Ένα μονοκατευθυντικό μικρόφωνο, το οποίο κινείται αργά πάνω σε ημικυκλική επιφάνεια, με την βοήθεια δύο σερβοκινητήρων, με τον ένα να το περιστρέφει στο οριζόντιο επίπεδο και τον άλλο να αλλάζει τη γωνία στο κατακόρυφο επίπεδο.
2. Οκτώ σταθερά μονοκατευθυντικά μικρόφωνα τοποθετημένα σε ένα επίπεδο στις κορυφές ενός οκταγώνου και με μικρή απόσταση μεταξύ τους (μικρότερη από 10 cm). Η κατεύθυνση του ήχου προσδιορίζεται από το χρόνο στον οποίο ανιχνεύεται το ηχητικό σήμα.
3. Οκτώ μικρόφωνα τοποθετημένα όπως στην προηγούμενη περίπτωση και ένα επιπλέον μικρόφωνο βρίσκεται σε δεύτερο επίπεδο, παράλληλα και πάνω από το

πρώτο. Αυτό το τελευταίο μικρόφωνο ανιχνεύει τη γωνία ανύψωσης του drone, ενώ τα προηγούμενα οκτώ ανιχνεύουν την κατεύθυνσή του στο οριζόντιο επίπεδο.

Συνοψίζοντας, τα πλεονεκτήματα και τα μειονεκτήματα της μεθόδου του ηχητικού εντοπισμού είναι τα εξής: [34]

Πλεονεκτήματα

1. Εντοπισμός ακόμα και όταν δεν υπάρχει οπτική επαφή, καθώς ο ήχος μπορεί να παρακάμψει ορισμένα εμπόδια.
2. Εντοπισμός αυτόνομων drones, τα οποία δεν έχουν επικοινωνία με χειριστή και δεν εκπέμπουν σήμα.
3. Δυνατότητα ανάπτυξης εφαρμογής χαμηλού κόστους με περιορισμένες δυνατότητες και επιδόσεις.

Μειονεκτήματα

1. Η εμβέλεια εντοπισμού είναι περιορισμένη.
2. Είναι πιθανό το drone να διανύσει αρκετά μεγάλη απόσταση, καθώς ο ήχος φτάνει σε έναν απομακρυσμένο ηχητικό αισθητήρα, επειδή η ταχύτητα του ήχου είναι χαμηλή. Ενδεικτικά, στα 500 μέτρα, υπάρχει καθυστέρηση περίπου 1,5 δευτερόλεπτο, επιτρέποντας σε ένα DJI phantom 4 να διανύσει περίπου 30 μέτρα πριν τα ηχητικά κύματα φτάσουν στους αισθητήρες.
3. Ευαίσθητοι αισθητήρες στη βροχή και κυρίως στον άνεμο.
4. Υψηλά επίπεδα θορύβου στο αστικό περιβάλλον κάτω από τα 20 KHz, δυσχεραίνοντας τον εντοπισμό.
5. Οι υπέρηχοι που παράγουν τα drones, εκτός των άλλων συχνοτήτων, είναι ιδιαίτερα εκτεθειμένοι σε ατμοσφαιρικές απώλειες.
6. Η αγορά στρέφεται προς την ανάπτυξη όλο και πιο αθόρυβων μοντέλων.
7. Κοστίζει ακριβά, ιδίως όταν πρόκειται για εφαρμογή πολλών μικροφώνων.
8. Δεν μπορεί να ανιχνεύσει ταχύτητα ή απόσταση εκτός αν εφαρμοστεί τριγωνισμός.

4.1.8 Εντοπισμός με κάμερες

Οι ψηφιακές κάμερες, οι κάμερες παρακολούθησης και η αναγνώριση προσώπου είναι τεχνολογία που χρησιμοποιείται σε πολλές εφαρμογές. Το οπτικό ζουμ, οι αισθητήρες υψηλής ανάλυσης και η σταθεροποίηση εικόνας προσφέρουν μεγάλη εμβέλεια για τις ανάγκες του εντοπισμού, ενώ το λογισμικό αναγνώρισης εξυπηρετεί την κατηγοριοποίηση των στόχων. [22]

Συγκεντρωτικά, τα πλεονεκτήματα και τα μειονεκτήματα της μεθόδου του εντοπισμού με την χρήση καμερών, είναι τα εξής: [34]

Πλεονεκτήματα

1. Χρήση καμερών του εμπορίου.
2. Μεγάλη εμβέλεια εντοπισμού χάρη στο υψηλής ποιότητας οπτικό ζουμ των καμερών.
3. Εντοπισμός και κατηγοριοποίηση στόχων με τη χρήση λογισμικού.
4. Εντοπισμός την νύχτα με την χρήση καμερών υπερύθρων (IR).

Μειονεκτήματα

1. Δυσκολία εντοπισμού σε κακές καιρικές συνθήκες.
2. Ανάλυση πολλών εικονοστοιχείων (pixels) σε σύντομο χρονικό διάστημα για την κάλυψη του χώρου σε οριζόντιο και κατακόρυφο επίπεδο.
3. Χρήζει συντήρησης και καθαρισμού καθώς ο φακός πρέπει να διατηρείται καθαρός.
4. Μη αξιόπιστη λειτουργία στην περίπτωση που δεν χρησιμοποιείται κάμερα IR σε συνθήκες χαμηλού φωτισμού.
5. Πρέπει να έχει ικανοποιητική σταθεροποίηση εικόνας για να υποστηρίζει μεγάλη εμβέλεια.
6. Δυσκολία στην εκτίμηση της ταχύτητας και της απόστασης του drone, εάν κινείται προς την κάμερα.

Μια ολοκληρωμένη πρόταση για τον εντοπισμό ενός drone που βασίζεται εξολοκλήρου σε κάμερες, αφορά την εφαρμογή 30 καμερών συνδεδεμένων σε τοπικό δίκτυο και τοποθετημένων σε ομόκεντρους δίσκους σε πολλαπλά επίπεδα, έτσι ώστε να καλύπτεται πλήρως το πεδίο, χωρίς κενά διαστήματα. [53]

4.1.9 Εντοπισμός με θερμικές κάμερες

Οι θερμικές (υπέρυθρες) κάμερες διαφέρουν από τις συμβατικές κάμερες ως προς το χαρακτηριστικό ότι μπορούν να απεικονίσουν εικόνες κατά τη διάρκεια της νύχτας. Αυτό είναι και το κύριο πλεονέκτημά τους στον εντοπισμό των drones έναντι του εντοπισμού με κάμερες υψηλής ανάλυσης. [34]

Πλεονεκτήματα

1. Οι θερμικές κάμερες είναι μικρές, εύκολες στον χειρισμό και οικονομικές.
2. Δεν απαιτείται καμία ή και ελάχιστη συντήρηση,
3. Είναι αποτελεσματικές και αντέχουν σε όλες τις καιρικές συνθήκες.

Μειονεκτήματα

1. Ο εντοπισμός ενός drone εξαρτάται σε μεγάλο βαθμό από την ύπαρξη ανιχνεύσιμης θερμότητας (πολλά drones είναι κατασκευασμένα από πλαστικό με ηλεκτρικούς κινητήρες, οπότε σε τέτοιες περιπτώσεις είναι πιο πιθανό να εντοπιστεί ένα πτηνό αντί ενός drone).
2. Η ανάλυση της θερμικής κάμερας είναι συνήθως περιορισμένη, οπότε μικρά drones σε σχετικά μεγάλες αποστάσεις ενδέχεται να μην εντοπιστούν. [53]

Αναφορικά με το δεύτερο μειονέκτημα που αναφέρθηκε έχει αποδειχτεί ότι, με την χρήση χαμηλού κόστους αισθητήρα θερμικής κάμερας, ο μικρός αριθμός εικονοστοιχείων (pixels) της εικόνας έχει ως αποτέλεσμα σε απόσταση περίπου 100 μέτρων ή και λιγότερο, το drone να αποτυπώνεται σε ένα μόνο εικονοστοιχείο (pixel) στην κάμερα, γεγονός που σημαίνει ότι ο εντοπισμός δεν είναι αξιόπιστος. Η μέγιστη απόσταση εντοπισμού μειώνεται περαιτέρω όταν το drone δεν κινείται υπό γωνία 90^o σε σχέση με τον άξονα της κάμερας αλλά και επειδή δεν είναι ολόκληρο το drone πηγή της θερμικής ακτινοβολίας αλλά κυρίως οι μπαταρίες του. [54]

Για την βελτίωση της απόστασης εντοπισμού, είναι απαραίτητη η χρήση ακριβότερων καμερών με μεγαλύτερη ανάλυση και οι οποίες επιτρέπουν την ταυτόχρονη παρακολούθηση περισσότερων στόχων σε αποστάσεις αρκετών χιλιομέτρων [55].

4.1.10 Εντοπισμός με την χρήση αλγορίθμων

Ένας αλγόριθμος μπορεί να χρησιμοποιηθεί για τον προσδιορισμό του μοτίβου κίνησης ενός κινούμενου στόχου στο ραντάρ, ώστε να διαχωρίζει το drone από ένα πτηνό ή άλλα αντικείμενα, μέσω ενός δεντροδιαγράμματος αποφάσεων. Αυτό βασίζεται στην ιδέα ότι το μοτίβο κίνησης ενός πτηνού και ενός drone διαφέρουν. Ωστόσο ένα πρόβλημα είναι ότι, διαφορετικά πτηνά έχουν διαφορετικά μοτίβα κίνησης και αρκετές φορές δεν διαφέρουν από αυτά ενός drone. [22]

Πλεονεκτήματα

1. Πρόκειται για λογισμικό και επομένως μπορεί να αναβαθμιστεί.
2. Μπορεί να χρησιμοποιηθεί με πολλές μεθόδους εντοπισμού.

Μειονεκτήματα

1. Χρειάζεται μεγάλη υπολογιστική ισχύς.
2. Ομοιότητες μεταξύ του μοτίβου κίνησης ορισμένων πτηνών και των drones.

4.1.11 Συνδυασμός μεθόδων

Το συμπέρασμα σε αυτήν την ενότητα είναι ότι δεν υπάρχει προτιμώμενη μέθοδος εντοπισμού. Η αξιοπιστία της μεθόδου που θα χρησιμοποιηθεί εξαρτάται από πολλούς παράγοντες, όπως για παράδειγμα τα χαρακτηριστικά του εκάστοτε drone, οι καιρικές συνθήκες, η απόσταση κ.α. Αυτός είναι ο λόγος που ενδείκνυται συνδυασμός δύο ή περισσότερων μεθόδων, όπως και εφαρμόζεται για παράδειγμα στο [35] που συνδυάζεται ο ηχητικός εντοπισμός, κάμερες και ανίχνευση ραδιοσυχνοτήτων, στο [56], που συνδυάζεται εντοπισμός με ραντάρ, ηχητικός, RF και κάμερες, στο [58], χρησιμοποιείται εντοπισμός με ραντάρ, αισθητήρες RF και θερμικές κάμερες, ενώ το [53] συνδυάζει μόνο κάμερες και ηχητικούς αισθητήρες.

4.2 Μέθοδοι αντιμετώπισης

Μετά τον επιτυχή εντοπισμό των drones ακολουθεί η φάση της αντιμετώπισής τους. Ο συνεχόμενος αριθμός των περιστατικών που αφορούν στην ανεπιθύμητη

παρουσία των drones, έχει οδηγήσει στην ανάπτυξη διάφορων αντιμέτρων για αυτόν τον σκοπό. Η χρήση συμβατικών όπλων για την καταπολέμησή τους αποδείχθηκε αρκετά δύσκολη, καθώς το μεγάλο βελησνεκές και το μικρό μέγεθος του στόχου απαιτούν μεγάλη ακρίβεια στην χρήση τους. Εξετάζοντας τις μεθόδους αντιμετώπισης που ήδη χρησιμοποιούνται, η πιο συνηθισμένη είναι η παρεμβολή καθώς και διάφοροι μέθοδοι καταστροφής τους.

4.2.1 Παρεμβολή σήματος (Jamming)

Υπάρχουν μια σειρά από συστήματα και συσκευές που προορίζονται για την παρεμβολή των drones [58], [59]. Η μορφή της συσκευής μπορεί να διαφέρει έχοντας αυτή του όπλου, να είναι φορητή σαν βαλίτσα, σαν επιτραπέζια συσκευή, είτε εγκατεστημένη σε οχήματα κ.ο.κ. Δεδομένου ότι, οι συχνότητες λειτουργίας του drone είναι γνωστές, η υλοποίηση ενός παρεμβολέα είναι πιο απλή. Οι συχνότητες που χρησιμοποιούνται για τις επικοινωνίες των drone και για τις ζεύξεις βίντεο και τηλεμετρίας είναι οι 433MHz, 868MHz, 915MHz, 1,2GHz, 2.4GHz, 5.8GHz, καθώς και οι 1176MHz, 1227MHz και 1.57-1.62GHz για τα συστήματα GPS ή GLONASS [35], [60], [61], [62]. Τα παλαιότερα τηλεκατευθυνόμενα drone χρησιμοποιούν τις συχνότητες 27MHz, 35MHz, 49MHz, 72MHz ή 75MHz. [49]



Εικόνα 4.4 *Παρεμβολή ενός drone με φορητό παρεμβολέα*

Πλεονεκτήματα

1. Αποτελεί ένα ήπιο αντίμετρο.
2. Δεν προκαλείται ζημιά στον εξοπλισμό του drone, εκτός από την περίπτωση που η διακοπή των επικοινωνιών οδηγήσει σε συντριβή του drone, εάν αυτό δεν διαθέτει τις κατάλληλες λειτουργίες αυτοματισμού.
3. Εύκολο να παρατηρηθεί το αποτέλεσμα της ενέργειας, εάν το drone επιστρέφει στο σημείο αφετηρίας.
4. Τα εμπορικά drones σπάνια διαθέτουν λειτουργίες αυτόματου πιλότου στην περίπτωση διακοπής της ζεύξης. Αντίθετα, μπορούν να επιστρέψουν στο σημείο αφετηρίας ή να προσγειωθούν άμεσα.
5. Ευρεία χρήση των παρεμβολών σε άλλες εφαρμογές.
6. Διατίθεται εξοπλισμός και συσκευές σε χαμηλή τιμή.
7. Χαμηλή κατανάλωση ενέργειας.
8. Εύκολη εφαρμογή.

Μειονεκτήματα

1. Δεν λειτουργεί ενάντια σε αυτόνομα drones, τα οποία δεν έχουν επικοινωνία με χειριστή και δεν εκπέμπουν σήμα, εκτός εάν γίνει παρεμβολή τους σήματος GPS.
2. Υψηλός κίνδυνος διακοπής έτερων επικοινωνιών, όπως το Wi-Fi και το τηλέφωνο.
3. Δυσχέρεια στην παρεμβολή μίας συγκεκριμένης συχνότητας.
4. Οι νόμοι και οι ρυθμιστικά πλαίσια περιορίζουν τη χρήση των παρεμβολέων.

4.2.1.1 Παρεμβολή σήματος RF

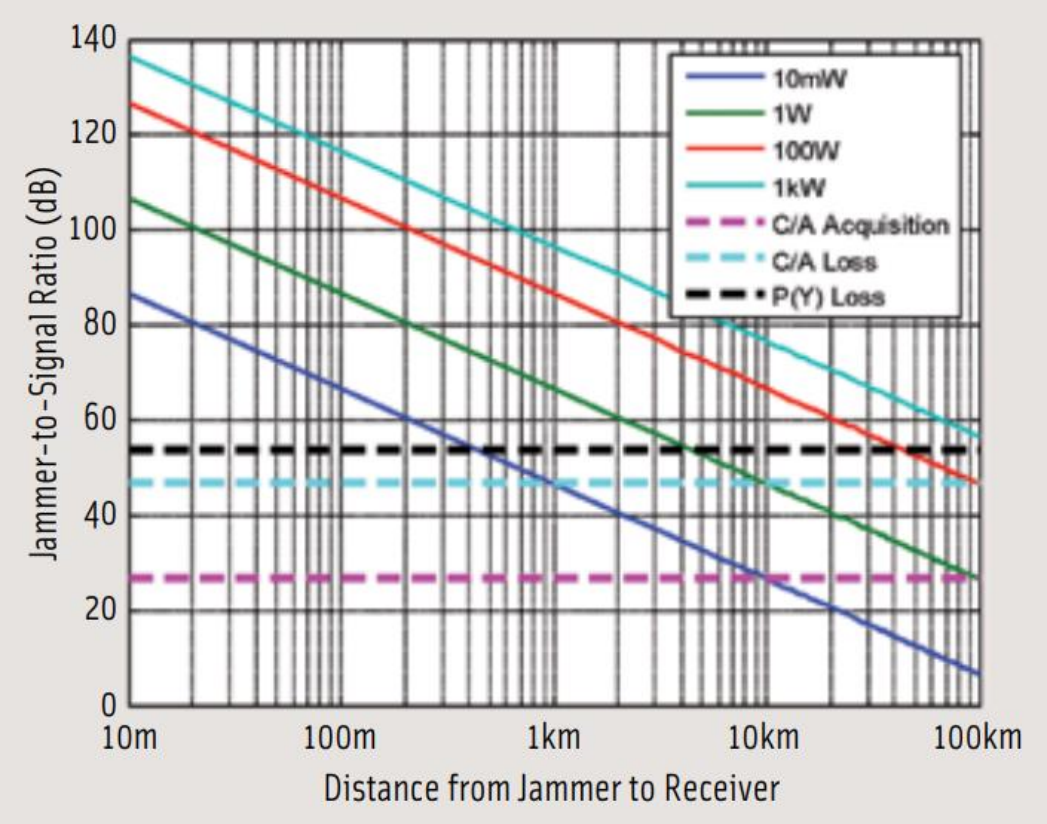
Τα μη επανδρωμένα αεροσκάφη ελέγχονται εξ αποστάσεως χρησιμοποιώντας σήματα RF, γεγονός που τα καθιστά επιρρεπή σε πιθανές επιθέσεις. Οι παρεμβολείς κυκλοφορούν σε διάφορους τύπους, από τον παρεμβολέα συνεχόμενης παρεμβολής που εκπέμπει συνεχώς ένα σήμα, τον παρεμβολέα τυχαίας παρεμβολής ο οποίος εκπέμπει μόνο κατά διαστήματα [63], έως πιο σύνθετους, όπως ο ενεργός παρεμβολέας όπου γίνεται παρεμβολή μόνο όταν ανιχνεύεται εκπομπή [63], [64], [65], και άλλους ευφυείς παρεμβολείς. [66]

Παρεμβολή του σήματος επιτυγχάνεται με διαταραχή της επικοινωνίας, μέσω της εκπομπής ισχυρότερου σήματος στην ίδια συχνότητα. Όμοιες παρεμβολές μπορεί να χρησιμοποιηθούν για την διαταραχή γενικότερα ασύρματων επικοινωνιών, όπως για παράδειγμα ραδιόφωνο, Wi-Fi, τηλέφωνα και ραντάρ. Υπάρχουν εγκαταστάσεις που εκπέμπουν σήμα παρεμβολής για την απενεργοποίηση κινητών τηλεφώνων, ενώ ερασιτεχνικός εξοπλισμός παρεμβολής είναι διαθέσιμος στο διαδίκτυο και χρησιμοποιείται για ένα ευρύ φάσμα συχνοτήτων με ποικίλες εφαρμογές. Ωστόσο, η παρεμβολή είναι μια καταστροφική ενέργεια και συχνά είναι παράνομη η εφαρμογή της ανάλογα με τη συχνότητα και την ισχύ του σήματος. [22]

Η παρεμβολή του σήματος επικοινωνίας του drone δεν είναι η μοναδική, αλλά είναι ίσως η πιο αποτελεσματική μέθοδος αντιμετώπισης. Ειδικότερα, μπορεί να εφαρμοστεί RF παρεμβολή κατευθυντική ή προς όλες τις κατευθύνσεις. Όταν εφαρμόζεται κατευθυντική παρεμβολή, η εμβέλεια παρεμβολής είναι μεγαλύτερη απ' ό,τι αν εφαρμοστεί προς όλες τις κατευθύνσεις. Από την άλλη πλευρά, η εκπομπή σήματος παρεμβολής προς όλες τις κατευθύνσεις είναι πιο αξιόπιστη, επειδή δεν εξαρτάται από τον εντοπισμό του drone [58]. Το μειονέκτημα όμως εντοπίζεται εκτός από τη χαμηλότερη εμβέλεια και στην ενδεχόμενη δυσλειτουργία άλλων συσκευών που βρίσκονται κοντά, οι οποίες λειτουργούν στη συχνότητα εκπομπής της παρεμβολής. Στόχος της παρεμβολής είναι η παραμόρφωση του σήματος σε τέτοιο σημείο κατά το οποίο ο δέκτης αδυνατεί πλήρως να το ανιχνεύσει ή να καταστήσει ορισμένα τμήματα του συστήματος πρακτικά άχρηστα, με αποτέλεσμα την ολική ή μερική αδυναμία παροχής υπηρεσιών [66]. Στις περισσότερες περιπτώσεις, το drone χρησιμοποιεί ζεύξη με το τηλεχειριστήριο, για τη λήψη εντολών από τον χειριστή, ζεύξη τηλεμετρίας για την αποστολή δεδομένων πτήσης και της κατάστασής του σε αυτό, ζεύξη βίντεο για την αποστολή εικόνων και συστήματα εντοπισμού θέσης (GPS και GLONASS). Η παρεμβολή του GPS του drone είναι ο πιο αποτελεσματικός τρόπος ακινητοποίησής του, καθώς πιθανότατα θα συντριβεί. Αντίθετα, εάν παρεμβληθούν άλλες συχνότητες σημαντικές για τη λειτουργία του drone και όχι το GPS, αυτό θα προσγειωθεί μόνο του ή θα κινηθεί προς το σημείο εκκίνησής του. [67]

4.2.1.2 Παρεμβολή σήματος GPS

Σημειώνεται ότι, η παρεμβολή μπορεί να πραγματοποιηθεί σε διαφορετικές συχνότητες από τις ονομαστικές αλλά η στάθμη της πρέπει να είναι υψηλότερη από ό,τι στις ονομαστικές συχνότητες. Ο λόγος είναι ότι τα σήματα GPS έχουν πολύ χαμηλή στάθμη στο χώρο του δέκτη GPS (συνήθως χαμηλότερη από -120dBm). Γι' αυτό το λόγο, κατάλληλη στάθμη σήματος μπορεί να επιτευχθεί και από σήμα εκτός ζώνης, πλευρικούς λοβούς ή από αρμονικές του σήματος ως αποτέλεσμα ενδοδιαμόρφωσης [68]. Σύμφωνα με τα αποτελέσματα των δοκιμών για διάφορους τύπους δεκτών GPS που παρουσιάζονται στο [69], ο λόγος ισχύος παρεμβολής προς ισχύ σήματος J/S=25dB προκαλεί μέγιστο σφάλμα θέσης μεταξύ 129m (ο χειρότερος δέκτης) και 16m (ο καλύτερος δέκτης), ενώ κατά τη διάρκεια της παρατήρησης η θέση ήταν αμετάβλητη μεταξύ 16% του χρόνου και 100% του χρόνου, αντίστοιχα. Τα αποτελέσματα στο [70] φανερώνουν ότι, ισχύς σήματος παρεμβολής 13dBm (20mW) παρεμβάλει όλους τους δέκτες GPS σε απόσταση μέχρι και 2km. Επιπλέον, το γράφημα της Εικόνας 4.5 από το [71], επιτρέπει στον προσδιορισμό με μεγαλύτερη ακρίβεια του κατάλληλου επιπέδου σήματος παρεμβολής ανάλογα με την απόσταση και το βαθμό απώλειας εντοπισμού. Στοιχείο πολύ σημαντικό όχι μόνο για την μείωση της κατανάλωσης ισχύος, αλλά και για να επιτευχθεί όσο το δυνατόν μικρότερη διαταραχή σε άλλους δέκτες GPS στην προστατευόμενη περιοχή.



Εικόνα 4.5 *Η επίδραση διαφόρων παρεμβολέων σε δέκτες GPS*

Κατά την παρεμβολή ενός drone, δύο είναι τα πιθανά αποτελέσματα. Πρώτο, το επίπεδο σήματος παρεμβολής είναι σχετικά υψηλό και δεν είναι δυνατός ο εντοπισμός σήματος GPS. Η διαταραχή αυτή προκαλείται σε μια ευρύτερη περιοχή, υποβαθμίζοντας επίσης τη λειτουργία πολλών άλλων συσκευών στην προστατευόμενη περιοχή εκτός από τα drones. Το δεύτερο πιθανό αποτέλεσμα είναι όταν το σήμα παρεμβολής είναι χαμηλότερο. Στην περίπτωση αυτή ο εντοπισμός GPS είναι δυνατός, αλλά η προσδιοριζόμενη θέση που προκύπτει είναι λανθασμένη. [72]

4.2.1.2.1 Συσκευές παρεμβολής GPS

Τα σήματα παρεμβολής που διαταράσσουν τις επικοινωνίες GPS εκπέμπονται από μια μεγάλη ποικιλία συσκευών που έχουν διάφορα χαρακτηριστικά και ιδιότητες. Οι συσκευές αυτές μπορούν να ταξινομηθούν με βάση τα χαρακτηριστικά τους σε τρεις ομάδες. [73]

Ομάδα 1: Παρεμβολείς αναπτήρα τσιγάρων. Αυτές οι συσκευές έχουν σχεδιαστεί για να συνδέονται στον αναπτήρα του αυτοκινήτου με τροφοδοσία 12V.

Ομάδα 2: Παρεμβολείς που τροφοδοτούνται με μπαταρία και συνδέονται με εξωτερική κεραία μέσω υποδοχής SMA.

Ομάδα 3: Παρεμβολείς μπαταρίας χωρίς υποδοχή SMA. Αυτές οι συσκευές τροφοδοτούνται από μπαταρία και χρησιμοποιούν ενσωματωμένη κεραία για τη εκπομπή των σημάτων.

Παρόλο που οι δύο προηγούμενες κατηγορίες αποτύπωσαν τα περισσότερα χαρακτηριστικά των παρεμβολέων, πρέπει να λαμβάνονται υπόψη και οι ακόλουθες ιδιότητες των συσκευών παρεμβολής. [72]

α. Παρεμβολείς μίας συχνότητας έναντι παρεμβολέων πολλαπλών συχνοτήτων: Οι παρεμβολείς πολλαπλών συχνοτήτων μπορούν να επηρεάσουν πολλές ζώνες σήματος GPS ταυτόχρονα.

β. Παρεμβολείς μίας κεραίας έναντι παρεμβολέων πολλαπλών κεραιών: Ορισμένες συσκευές παρεμβολής είναι εξοπλισμένες με πολλές κεραίες, εκπέμποντας σήματα σε διαφορετικές ζώνες συχνοτήτων.

γ. Παρεμβολείς ενός συστήματος έναντι παρεμβολέων πολλαπλών συστημάτων: Ορισμένες συσκευές παρεμβολής μπορούν να επηρεάσουν ταυτόχρονα τόσο τις επικοινωνίες GPS όσο και άλλα συστήματα επικοινωνιών, όπως για παράδειγμα τα συστήματα τηλεπικοινωνιών UMTS και GSM.

4.2.1.2.2 Σήματα παρεμβολής

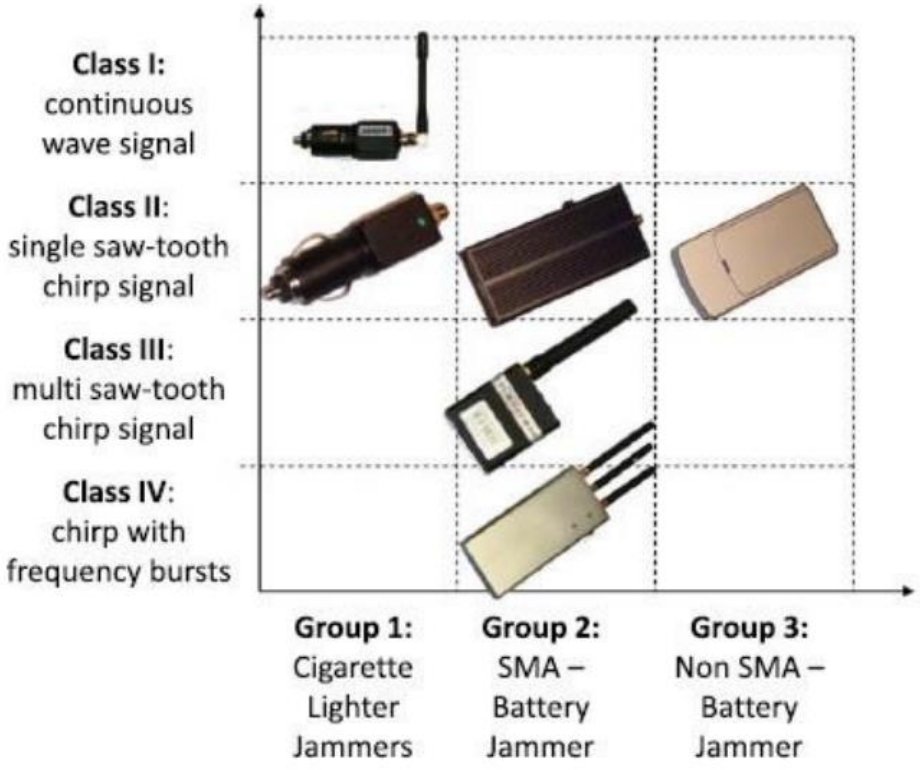
Σύμφωνα με το [73] τα σήματα παρεμβολής διαχωρίζονται στις εξής κατηγορίες:

Κατηγορία Ι: Παρεμβολείς που εκπέμπουν σήμα συνεχούς κύματος (CW).

Κατηγορία II: Παρεμβολείς που εκπέμπουν ένα διαμορφωμένο κατά συχνότητα πριονωτό σήμα (chirp) σήμα.

Κατηγορία III: Παρεμβολείς που εκπέμπουν πολλαπλά διαμορφωμένα κατά συχνότητα πριονωτά σήματα. Ωστόσο η αλλαγή της συχνότητας με τον χρόνο είναι ακόμη πιο πολύπλοκη και καθορίζεται από το συνδυασμό πολλών πριονωτών σημάτων.

Κατηγορία IV: Παρεμβολείς που παράγουν chirp σήματα με ριπές συχνότητων, οι οποίες διευρύνουν τη ζώνη συχνοτήτων που επηρεάζεται από το σήμα παρεμβολής.



Εικόνα 4.6 *Κατηγοριοποίηση παρεμβολέων*

4.2.1.3 Τεχνικές παρεμβολής

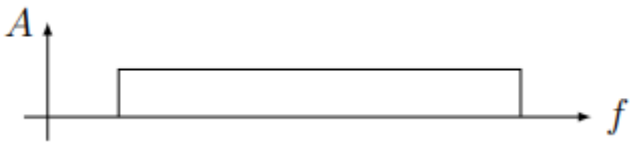
Οι τεχνικές που εφαρμόζονται για παρεμβολές σε drones είναι οι ίδιες με αυτές που εφαρμόζονται για παρεμβολές άλλων συστημάτων και διακρίνονται ως εξής: [74]

4.2.1.3.1 Barrage Jamming

Η παρεμβολή αυτή είναι η απλούστερη μορφή παρεμβολής και συνήθως αφορά έναν παρεμβολέα ο οποίος εκπέμπει συνεχώς σήμα που μοιάζει με θόρυβο σε ολόκληρο το τμήμα του φάσματος που καταλαμβάνει ο στόχος. Ουσιαστικά αυξάνει το επίπεδο θορύβου στο δέκτη, δυσχεραίνοντας τη λειτουργία του συστήματος επικοινωνίας, επηρεάζοντας άμεσα έτσι τη χωρητικότητα καναλιού ενός συστήματος επικοινωνίας. Η χωρητικότητα του καναλιού μελετήθηκε για πρώτη φορά από τον Shannon το 1948 όσον σε σχέση με τον Γκαουσιανό θόρυβο [75]. Ο Shannon υπολόγισε το μέγιστο απαιτούμενο ρυθμό δεδομένων για ένα κανάλι, ώστε το σφάλμα να είναι απειροελάχιστο. Εάν για το δεδομένο κανάλι χρησιμοποιείται υψηλότερος ρυθμός δεδομένων τότε είναι βέβαιο ότι θα υπάρχουν σφάλματα στο λαμβανόμενο σήμα. Η χωρητικότητα ενός καναλιού που υπόκειται σε προσθετικό λευκό γκαουσιανό θόρυβο (AWGN) δίνεται από τη σχέση:

$$C = B * log_2\left(1 + \frac{S}{N}\right)$$

όπου B είναι το εύρος ζώνης του καναλιού, S είναι η μέση ισχύς του σήματος και N είναι ο συνολικός μέσος όρος του θορύβου που υπάρχει στο σύστημα. Επομένως, όταν το επίπεδο του θορύβου αυξάνεται σκόπιμα στο κανάλι, το SNR μειώνεται μαζί με τη χωρητικότητα του καναλιού. [74]



Εικόνα 4.7 *Barrage jamming*

Η παρεμβολή αυτή έχει αποδειχθεί ότι είναι η καλύτερη τεχνική ενός παρεμβολέα δεδομένου ότι δεν γνωρίζουμε την παρουσία του σήματος-στόχου, με την δημιουργία ενός συνεχούς θορύβου με επαρκή ισχύ ώστε να εφαρμοστεί πλήρης παρεμβολή των ασύρματων δικτύων. Από την άλλη πλευρά, αυτή η προσέγγιση έχει υψηλές απαιτήσεις ενέργειας, υψηλή πιθανότητα εντοπισμού του παρεμβολέα και δεν υπάρχει τρόπος επιλογής των σημάτων που θα παρεμβληθούν στη χρησιμοποιούμενη

ζώνη RF. Ωστόσο είναι εφικτή η αντιμετώπιση της παρεμβολής με τεχνικές spread spectrum, έναντι των οποίων η μέθοδος αυτή είναι αναποτελεσματική.

4.2.1.3.2 Tone Jamming

Στην τεχνική αυτή χρησιμοποιούνται μία ή περισσότερες συχνότητες που υπόκεινται σε παρεμβολή. Οι συχνότητες αλλά και ο αριθμός τους επηρεάζουν την απόδοση του παρεμβολέα.



Εικόνα 4.8 *Tone jamming*

Στην παρεμβολή πολλών συχνοτήτων, η ισχύς του παρεμβολέα κατανέμεται μεταξύ αυτών, ενώ το σήμα παρεμβολής δίνεται από τη σχέση

$$J(t) = \sqrt{\frac{2P_J}{N_J}} \sum_{i=1}^{N_j} \cos(2\pi f_i t + \phi_i)$$

όπου P_J είναι η ισχύς παρεμβολής, N_J είναι ο αριθμός των συχνοτήτων παρεμβολής, f_i είναι η i συχνότητα παρεμβολής, φ_i είναι η διαφορά φάσης μεταξύ της i συχνότητας παρεμβολής και του φέροντος. [74]

Ωστόσο, και εδώ έναντι τεχνικών spread spectrum η μέθοδος αυτή είναι αναποτελεσματική Αυτό ισχύει διότι τα drones, έχουν εφεδρικότητα με την έννοια ότι η κατάσταση του τηλεχειριστηρίου μεταδίδεται συνεχώς σε διαφορετικά κανάλια. Επομένως, εάν ένα μόνο από αυτά τα κανάλια δεν είναι διαθέσιμο, τότε η λειτουργία του drone δεν θα υποβαθμιστεί αισθητά. Συνοψίζοντας, η τεχνική αυτή παρουσιάζει παρόμοια μειονεκτήματα με αυτή του barrage jamming εναντίων spread spectrum συστημάτων.

4.2.1.3.3 Sweep Jamming

Η τεχνική του sweep jamming είναι ένας συνδυασμός barrage και tone jamming. Με αυτήν, ένα σχετικά στενού εύρους σήμα σαρώνεται χρονικά σε μία ζώνη συχνοτήτων (Εικόνα 4.8). Ομοίως με το tone jamming, μόνο ένα τμήμα του φάσματος παρεμβάλλεται σε κάθε χρονική στιγμή. Ωστόσο, δεδομένου ότι το σήμα σαρώνεται, μπορεί να παρεμβληθεί ένα ευρύ φάσμα συχνοτήτων σε μια χρονική περίοδο.



Εικόνα 4.9 *Sweep jamming*

Το σήμα chirp που χρησιμοποιείται για παρεμβολές σάρωσης δίνεται από τη σχέση:

$$J(t) = P_J \cos(2\pi f(t)t + \phi)$$
$$f(t) = f_0 + kt,\ k = \frac{f_1 - f_0}{T_{sweep}}$$

όπου P_J είναι η ισχύς παρεμβολής, f(t) είναι η στιγμιαία συχνότητα, f_0 είναι η αρχική συχνότητα του σήματος, f_1 είναι η τελική συχνότητα, T_{sweep} είναι η χρονική περίοδος με την οποία καλύπτεται το εύρος συχνοτήτων.

Το αποτέλεσμα μιας τέτοιας τεχνικής παρεμβολής σε μια δεδομένη χρονική περίοδο είναι παρόμοιο με αυτό του barrage jamming. Είναι επίσης δυνατό να γίνει διαχωρισμός της παρεμβολής και να αποφευχθεί η παρεμβολή ορισμένων ζωνών συχνότητας.

Τα αποτελέσματα που παρουσιάζονται στο [76] και αφορά συσκευές ασύρματου τοπικού δικτύου που βασίζονται στο IEEE 802.11 και δοκιμάστηκαν υπό διάφορα σήματα παρεμβολής καταλήγουν ότι η τεχνική παρεμβολής sweep jamming σε ορισμένους ρυθμούς σάρωσης είναι αρκετά αποτελεσματική.

4.2.1.3.4 Protocol-Aware Jamming

Η τελευταία τεχνική παρεμβολής που παρουσιάζεται είναι η παρεμβολή με έχοντας γνωστό το πρωτόκολλο επικοινωνίας (Protocol-Aware Jamming), με την οποία λαμβάνονται υπόψη οι παράμετροι του σήματος-στόχου κατά την κατασκευή του σήματος παρεμβολής (Εικόνα 4.9).

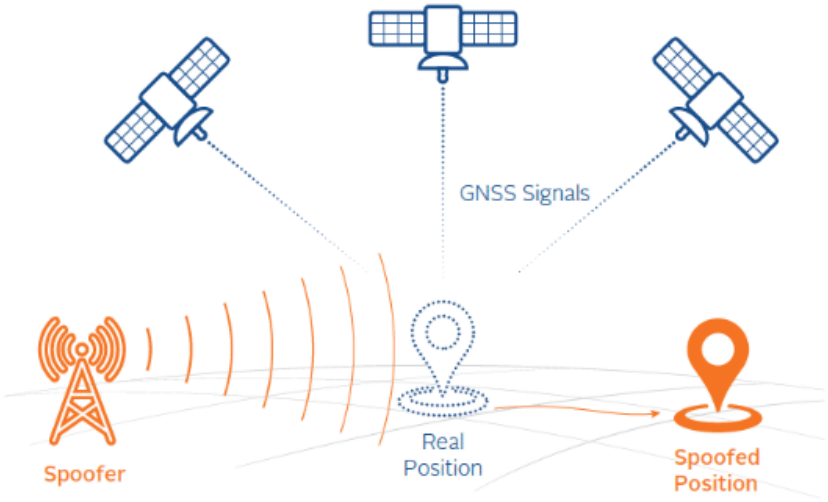


Εικόνα 4.10 *Protocol-Aware jamming*

Η αποτελεσματικότητα της τεχνικής αυτής έχει μέχρι στιγμής μελετηθεί κυρίως στο IEEE 802.11 και έχει διαπιστωθεί ότι μπορεί να επιτύχει αποτελεσματική παρεμβολή με πολύ χαμηλές ενεργειακές απαιτήσεις και χαμηλή πιθανότητα ανίχνευσης του σήματος παρεμβολής. Η παρεμβολή αυτή δεν παρεμβάλλει άλλα συστημάτα επικοινωνίας που λειτουργούν στην ίδια ζώνη RF, επειδή το σήμα παρεμβολής πλήττει μόνο στα τμήματα της ζώνης που χρησιμοποιούνται από το σήμα-στόχο. [74]

4.2.2 GPS Spoofing

Τα περισσότερα drones (εκτός από αυτά της κατηγορίας των τηλεκατευθυνόμενων παιχνιδιών) χρησιμοποιούν GPS για πλοήγηση. Ορισμένα χρησιμοποιούν επίσης άλλα συστήματα πλοήγησης, ενώ υπάρχει επίσης η δυνατότητα χρήσης πολλαπλών συστημάτων για εφεδρικότητα. Η αποστολή ψεύτικων συντεταγμένων μέσω ενός ισχυρότερου σήματος, δίνει τη δυνατότητα της παραπλάνησης του drone με έναν ψεύτικο χάρτη που το κάνει να ακολουθήσει μια διαφορετική διαδρομή. Αυτό απεικονίζεται στην Εικόνα 4.10, όπου σε ένα drone δίνονται ψευδείς ενδείξεις για το πού βρίσκεται. [22]



Εικόνα 4.11 *Παρεμβολή ενός drone με την μέθοδο του GPS Spoofing*

Το spoofing ορίζεται στο [77] ως μια τεχνική που χρησιμοποιείται εδώ και πολύ καιρό για την παραπλάνηση της λειτουργίας εντοπισμού στόχου ενός ραντάρ. Σκοπός της μεθόδου αυτής είναι να οδηγήσει έναν δέκτη GPS στον λήψη ψευδών σημάτων. Παρόλο που ο κώδικας P(Y) του GPS (κώδικας περιορισμένης χρήσης που χρησιμοποιείται συνήθως σε στρατιωτικές εφαρμογές όπου είναι σημαντικό το αδιάβλητο της ακρίβειας) είναι κρυπτογραφημένος και συνεπώς δύσκολα παραποιήσιμος, η δομή του σήματος, οι κώδικες και η διαμόρφωση του κώδικα C/A (δημόσιος κώδικας για μη στρατιωτικές εφαρμογές) είναι ανοικτές στο κοινό, καθιστώντας ευκολότερη την παραποίηση.

<u>Πλεονεκτήματα</u>

1. Αποτελεί ένα ήπιο αντίμετρο.
2. Δεν προκαλείται ζημιά στον εξοπλισμό του drone, εκτός από την περίπτωση που η διακοπή των επικοινωνιών οδηγήσει σε συντριβή του drone, εάν αυτό δεν διαθέτει τις κατάλληλες λειτουργίες αυτοματισμού.
3. Εύκολο να παρατηρηθεί το αποτέλεσμα της ενέργειας, εάν το drone επιστρέφει στο σημείο αφετηρίας.
4. Τα εμπορικά drones σπάνια διαθέτουν λειτουργίες αυτόματου πιλότου στην περίπτωση διακοπής της ζεύξης. Αντίθετα, μπορούν να επιστρέψουν στο σημείο αφετηρίας ή να προσγειωθούν άμεσα.

5. Οι γνωστές συχνότητες λειτουργίας των δορυφόρων καθιστούν εύκολη την εφαρμογή αυτής της μεθόδου.
6. Διατίθεται εξοπλισμός και τεχνογνωσία.

Μειονεκτήματα

1. Δεν λειτουργεί για drones που καθοδηγούνται μέσω χειροκίνητης πλοήγησης ή άλλων αισθητήρων.
2. Δυνατότητα σχεδίασης drone με ανθεκτικότητα σε όμοια παρεμβολή.
3. Χρειάζεται εκ των προτέρων ενημέρωση ή εικασία σχετικά με το πού σχεδιάζει να κατευθυνθεί ένα εχθρικό drone, έτσι ώστε η μέθοδος του GPS Spoofing να το καθοδηγήσει σε ασφαλής τοποθεσία.

Σύμφωνα με το [78], μια επίθεση GPS Spoofing διακρίνεται σε απλή, μεσαία και σύνθετη επίθεση.

4.2.2.1 Απλή επίθεση

Στην απλή επίθεση, δεν χρειάζεται να είναι γνωστή η αρχική θέση, η ταχύτητα και ο χρόνος του στόχου, καθώς ο προσομοιωτής εκπέμπει σήματα GNSS της παραποιημένης θέσης στον δέκτη GNSS που δέχεται την επίθεση. Απλώς τοποθετείται ένας ενισχυτής ισχύος και μια κεραία με έναν προσομοιωτή σήματος GPS και εκπέμπεται σήμα RF προς τον δέκτη-στόχο.

Παρά την ευκολία που υπάρχει στην πραγματοποίηση μιας επίθεσης με έναν προσομοιωτή σήματος GPS, υπάρχουν ορισμένα μειονεκτήματα. Το ένα είναι το κόστος καθώς η τιμή των προσομοιωτών μπορεί να φτάσει τα $400.000. Ένα άλλο μειονέκτημα είναι το μέγεθος καθώς είναι βαριοί και δύσχρηστοι. Επιπλέον, πρόκειται για μία τεχνική που μπορεί εύκολα να γίνει αντιληπτή λόγω της δυσκολίας συγχρονισμού του σήματος του προσομοιωτή με τα πραγματικά σήματα GPS στην περιοχή και ως εκ τούτου του κινδύνου για απώλεια κλειδώματος του δέκτη-στόχου στο ψευδές σήμα. Στην περίπτωση αυτή είναι που γίνεται αντιληπτή η προσπάθεια παραπλάνησης με την μέθοδο αυτή.

4.2.2.2 Μεσαίας κλίμακας επίθεση

Στην μεσαία, ο παρεμβολέας (spoofer) αποκτά πληροφορίες για την αρχική θέση, την ταχύτητα και τον χρόνο του στόχου, εκπέμποντας σήμα GPS ενώ κινείται προς αυτόν. Ο δέκτης θα λάβει και θα κλειδώσει τελικά στην υψηλότερη ισχύ του παραποιημένου σήματος χωρίς να το αντιληφθεί.

Η πρόκληση στην τεχνική αυτή είναι η ακριβής γνώση της θέσης και της ταχύτητας της κεραίας του δέκτη-στόχου. Αυτή η γνώση απαιτείται για την ακριβή παραγωγή των ψευδών σημάτων όμοιων με τα γνήσια σήματα στην κεραία του στόχου. Χωρίς αυτό, μια επίθεση GPS Spoofing εντοπίζεται σχετικά εύκολα.

4.2.2.3 Σύνθετη επίθεση

Η ίδια διαδικασία με πριν συμβαίνει και στην σύνθετη επίθεση, με την διαφορά ότι εδώ χρησιμοποιούνται αρκετοί παρεμβολείς (spoofers) σε μία προσπάθεια να μιμηθούν την κατανομή του σήματος στον χώρο, γεγονός που απαιτεί πολλές κεραίες εκπομπής για να εκτελεστεί με επιτυχία. Με την τεχνική αυτή είναι πολύ δύσκολο να γίνει αντιληπτός ο παρεμβολέας (spoofer) από έναν συμβατικό δέκτη με μία κεραία. [79]

4.2.2.4 Χαρακτηριστικά των εμπορικών συστημάτων παρεμβολής

Οι περισσότερες εμπορικές συσκευές που διατίθενται για GPS Spoofing, δεν επιτίθενται στο ίδιο το σήμα GPS, αλλά εισάγουν τις παραποιημένες πληροφορίες απευθείας στην έξοδο του δέκτη, γεγονός που απαιτεί φυσική πρόσβαση ή πρόσβαση στο λογισμικό του δέκτη του στόχου. Τέτοιοι εμπορικοί spoofers χρησιμοποιούνται για παράδειγμα για παράνομη αλιεία σε ύδατα όπου αυτή απαγορεύεται. Οι συσκευές GPS Spoofing σήματος RF είναι πολύ λιγότερο διαδεδομένες και οι εμπορικές συσκευές κοστίζουν πολύ. Παρόλο που δεν είναι σε θέση να εκτελέσουν μια ενδιάμεση επίθεση μπορούν να διαταράξουν σημαντικά έναν τυπικό δέκτη GPS. Το λογισμικό SimSAFE μαζί με τη συσκευή GPS Spoofing σήματος RF είναι πιθανώς ο πρώτος εμπορικός spoofer GNSS [80] που υποστηρίζει επιθέσεις στις ζώνες GPS L1 και Galileo E1, όπου ένας εμπορικός δέκτης GPS παρακολουθεί τα υπάρχοντα

σήματα από τον δορυφόρο και χρησιμοποιεί αυτές τις πληροφορίες για να παράγει το ψευδές σήμα με τον προσομοιωτή GPS. [70]

4.2.3 Άλλες μέθοδοι

Εκτός από τις μεθόδους που αναφέρθηκαν υπάρχουν και άλλοι για να αντιμετωπιστεί ένα drone. [22]

4.2.3.1 Κατάρριψη του drone

Υπάρχουν πιο δραστικές και αμφιλεγόμενες πρακτικές για την αντιμετώπιση ενός drone και ενδεχομένως να μην οδηγήσουν σε επιτυχές αποτέλεσμα.

Όπλο με δίχτυ: Πρόκειται για όπλο που εκτοξεύει δίχτυ που πιάνει το drone στον αέρα, ενδεχομένως με την χρήση αλεξίπτωτου για να αποφευχθεί η συντριβή του.

Εκπαιδευμένος αετός: Οι εκπαιδευμένοι αετοί έχει αποδειχθεί ότι μπορούν να απομακρύνουν με επιτυχία μικρά drone κατόπιν εντολής. Έχουν χρησιμοποιηθεί κατά καιρούς τόσο από τον γαλλικό στρατό όσο και από την ολλανδική αστυνομία.

Αερομεταφερόμενα δίχτυα: Πρόκειται για δίχτυα τα οποία φέρονται από drone και αιχμαλωτίζουν το drone-στόχο στον αέρα, με αποτέλεσμα να κρέμεται ακινητοποιείται στο δίχτυ.

4.2.3.2 Καταστροφή του drone

Πρακτική που εγκυμονεί κινδύνους λόγω της πτώσης του drone από τον ουρανό. Από την άλλη πλευρά, περιλαμβάνει περισσότερες επιλογές και διευρύνει τις δυνατότητες αποτελεσματικής αντιμετώπισης της απειλής.

Όπλα: Αυτή η μέθοδος έχει χρησιμοποιηθεί από την αστυνομία ελλείψει άλλων μεθόδων, όταν ένα drone πρέπει να απομακρυνθεί. Η χρήση οπλισμού σε αστικό περιβάλλον δεν μπορεί να θεωρηθεί ασφαλής και αποτελεσματική.

Σφαίρες διχτυών: Οι σφαίρες διχτυών για κυνηγετικά όπλα που πιάνουν drone πωλούνται ήδη στις ΗΠΑ. Ωστόσο, η λύση αυτή είναι εξαιρετικά περιορισμένη σε εμβέλεια, χρηστικότητα και ποσοστό επιτυχίας. Στις περιπτώσεις που πετυχαίνει τον στόχο λειτουργεί περισσότερο σαν πυρομαχικό, διαλύοντας τμήματα του drone σε κομμάτια αντί να το πιάσει.

Πυρομαχικά διασποράς: Αυτά τα πυρομαχικά ρυθμίζονται ώστε να εκρήγνυνται κοντά στο στόχο αυξάνοντας έτσι την περιοχή που πλήττουν και μειώνοντας την ανάγκη για ακρίβεια ή επέκταση της εμβέλειας. Το όπλο χρησιμοποιεί στόχο λέιζερ για τον προσδιορισμό της απόστασης από τον στόχο και προγραμματίζει τα πυρομαχικά να εκραγούν την κατάλληλη στιγμή.

Όπλο λέιζερ: Πρόκειται για λέιζερ υψηλής ισχύος που μπορεί να στείλει μια ακτίνα λέιζερ αρκετά ισχυρή ώστε να βάλει φωτιά σε ένα μικρό drone.

Drone καμικάζι: Το drone αυτό μπορεί να στοχεύσει και να καταστρέψει τον στόχο πέφτοντας πάνω του ή ως εκραγέν πυρομαχικό.

Χειροβομβίδα EMP: Μια χειροβομβίδα ηλεκτρομαγνητικού παλμού (EMP) απενεργοποιεί τα ηλεκτρονικά συστήματα στέλνοντας έναν σύντομο παλμό υψηλής ισχύος.

4.3 Εφαρμογές

Έχοντας παρουσιάσει τις μεθόδου εντοπισμού και αντιμετώπισης των ανεπιθύμητων drones, αξίζει η αναφορά στους τομείς που μπορούν να βρουν εφαρμογή, ανάλογα με τις εκάστοτε ανάγκες του καθενός.

4.3.1 Αεροδρόμια

Τα drones αποτελούν μεγάλο πρόβλημα για τα περισσότερα αεροδρόμια, καθώς πετούν στον εναέριο χώρο των αεροδρομίων και έστω κατά λάθος τα αναγκάζουν να αναστείλουν όλη την κυκλοφορία για 30 λεπτά ή και περισσότερο. Έτσι τα αεροδρόμια χρειάζονται μια λύση για να διασφαλίζεται η αδιάλειπτη λειτουργία τους. Μία λύση με την οποία θα εμποδίζεται η είσοδος των drones και δεν θα χρειάζεται να κλείσει προσωρινά το αεροδρόμιο και να δαπανήσει χρόνο για τον εντοπισμό των drones και των χειριστών τους.

Υπάρχουν προτάσεις για τη χρήση αναμεταδοτών σε όλα τα drones, ώστε να μπορούν να επικοινωνούν μαζί τους, αποτρέποντας έτσι τις ακούσεις διελεύσεις από τους χώρους των αεροδρομίων. Το 2017, η κατασκευάστρια εταιρία drone DJI ενημέρωσε πολλά από τα προϊόντα της ώστε να απαιτούν σύνδεση στο διαδίκτυο πριν από την απογείωση, έτσι αν βρίσκονται εντός προστατευόμενων περιοχών της βάσης δεδομένων τους, να μην εκκινούν.

Η ύπαρξη αξιόπιστων πληροφοριών σχετικά με το τι κινείται γύρω από τα αεροδρόμια επιτρέπει τον αποτελεσματικό έλεγχο της κυκλοφορίας. Το πρόβλημα αφορά κυρίως οικονομικό αντίκτυπο, καθώς το κλείσιμο ενός μεγάλου αεροδρομίου φέρει οικονομικές επιπτώσεις. Ένα πλήρως αυτοματοποιημένο σύστημα με πλήρη κάλυψη του χώρου θα ήταν ιδανικό για τα αεροδρόμια.

4.3.2 Φυλακές

Το πρόβλημα σε μία φυλακή είναι η μεταφορά λαθραίων εμπορευμάτων από drones. Η φύλαξη του εναέριου χώρου προς όλες τις κατευθύνσεις με προσωπικό ασφάλειας είναι δαπανηρή και δύσκολη. Τα drones έχουν χρησιμοποιηθεί κατά καιρούς ως αναμεταδότες σήματος κινητής τηλεφωνίας για τους κρατούμενους που έχουν λαθραία τηλέφωνα, παρακάμπτοντας τον αποκλεισμό του σήματος στη φυλακή.

Μία λύση θα μπορούσε να περιλαμβάνει συναγερμούς για την είσοδο των drones, ενώ το πρόβλημα αντιμετωπίζεται με τον εντοπισμό των χειριστών των drones που επιδίδονται σε λαθρεμπόριο, ώστε να αποφευχθούν μελλοντικές εισβολές.

4.3.3 Στάδια

Στα στάδια λαμβάνουν χώρα πολυπληθείς εκδηλώσεις με δεκάδες χιλιάδες θεατές ταυτόχρονα. Συχνά είναι ανοικτά χωρίς οροφή, αφήνοντας όλο ή μέρος του πλήθους απροστάτευτο από drones. Όταν ένα drone πετάει και κατά την διάρκεια μιας συναυλίας ή ενός αθλητικού αγώνα, ελάχιστα μπορεί να κάνει κάποιος γι' αυτό.

Μια προσωρινή επίλυση του προβλήματος για τα drones στα γήπεδα θα ήταν η τροποποίηση της νομοθεσίας με την απαγόρευση της πτήσης ορισμένων ή όλων των drones πάνω από πλήθη κατά τη διάρκεια εκδηλώσεων. Ωστόσο θα ήταν ιδανική η χρήση ενός συστήματος εντοπισμού των χειριστών που παρανομούν από την αστυνομία. Η απαγόρευση πτήσης σε προστατευόμενες περιοχές της DJI περιλαμβάνει επίσης και γήπεδα.

4.3.4 Αστυνομία

Η αστυνομία είναι αρμόδια για την αντιμετώπιση των drones που παραβιάζουν τους νόμους και τους κανονισμούς. Σε κάποιο βαθμό, ένα φορητό όπλο μπορεί να λύσει ορισμένες από τις ανάγκες της αστυνομίας, ενώ ο μεγαλύτερος περιορισμός σε αυτό είναι η εξαιρετικά περιορισμένη εμβέλεια λειτουργίας.

Η κατάρριψή τους με ένα κανονικό όπλο είναι πολύ δύσκολη καθώς η χρήση όπλου είναι επικίνδυνη, όπως μπορεί να γίνει κατανοητό. Η κατάρριψη του drone προσφέρει προσφέρει μία προσωρινή λύση καθώς το πραγματικό πρόβλημα η σύλληψη του δράστη που είναι ο χειριστής του drone.

4.3.5 Ένοπλες δυνάμεις

Η αποτροπή εισόδου των drones στρατιωτικές εγκαταστάσεις αποτελεί πρόβλημα προς επίλυση για τις ένοπλες δυνάμεις των χωρών, καθώς μπορεί να χρησιμοποιηθούν για κατασκοπεία ή για εμπρησμό.

Ο καθοριστικός παράγοντας σε αυτή την περίπτωση είναι η μεγάλη εμβέλεια ανίχνευσης, ενώ τα υφιστάμενα στρατιωτικά ραντάρ εδάφους μεγάλης εμβέλειας, αποτελούν υπερβολή για απειλή τέτοιου μεγέθους. Επίσης, η αντιμετώπισή τους με τα υφιστάμενα όπλα θεωρείται ακριβή και επικίνδυνη, καθιστώντας έτσι καταλληλότερες τις μεθόδους κατάρριψης και όχι καταστροφής τους.

4.3.6 Βιομηχανική κατασκοπεία

Μία από τις χρήσεις τους αποτελεί η βιομηχανική κατασκοπεία με την είσοδο τους σε εταιρικούς χώρους ή την λήψη τους εταιρικού ασύρματου δικτύου.

Τα κτίρια των γραφείων θα μπορούσαν να χρησιμοποιήσουν μια εγκατάσταση που προειδοποιεί για την εισβολή, δίνοντας στο προσωπικό του γραφείου χρόνο να προετοιμαστεί για την απειλή. Στην περίπτωση αυτή η ανάγκη εμβέλειας είναι χαμηλή, ενώ ανάλογα με την κατάσταση, η κάλυψη μπορεί να είναι σημαντικός παράγοντας εάν άλλα κτίρια και δέντρα εμποδίζουν την οπτική επαφή.

5. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

5.1 Συμπέρασμα

Από τα παραπάνω προκύπτει ότι τα drones αντιπροσωπεύουν ένα νέο και πολλά υποσχόμενο κεφάλαιο των σύγχρονων τεχνολογιών. Η χρήση των συστημάτων αυτών εξαπλώνεται όλο και περισσότερο χάρη στην ευκολία χρήσης τους σε διάφορες εφαρμογές, τόσο προς όφελος της καθημερινότητάς μας όσο όμως και για την εξυπηρέτηση κακόβουλων σκοπιμοτήτων.

Τα drones αναπτύσσονται ραγδαία εξοπλίζοντας τα εμπορικά συστήματα με νέες δυνατότητες. Όσο οφέλη όμως και αν προσφέρουν, οι κίνδυνοι και οι απειλές που εμφανίζονται με την ευρεία χρήση τους χρήζουν ιδιαίτερης προσοχής και μνείας για την αντιμετώπισή τους. Έτσι, ενώ υπάρχουν διασωστικές ομάδες που μπορούν ήδη να στείλουν ένα drone σε τραυματίες με ζωτικής σημασίας υλικό για την επιβίωσή τους, κάποιος άλλος μπορεί εξίσου εύκολα να στείλει με μια βόμβα σε ευαίσθητη περιοχή. Ομοίως, τα drones μπορούν να το χρησιμοποιηθούν για να την επίβλεψη πληγείσας περιοχής, αλλά μπορεί επίσης να χρησιμοποιηθούν καταχρηστικά για κατασκοπεία ή τον εντοπισμό ευάλωτων σημείων για μια τρομοκρατική επίθεση.

Η παρούσα εργασία παρουσίασε τις τεχνικές που μπορούν να χρησιμοποιηθούν για τον εντοπισμό των drones, δίνοντας έμφαση στα σημεία που ξεχωρίζει η καθεμία. Επιπλέον, μέσω της μεταξύ τους σύγκρισης και παράθεσης των πλεονεκτημάτων και μειονεκτημάτων κάθε τεχνικής συμπεραίνεται ότι, δεν υπάρχει κάποια που να ξεχωρίζει και να εφαρμόζεται για όλες τις περιπτώσεις. Για να την αντιμετώπιση τυχόν προβλημάτων που προκύπτουν, η λύση εντοπίζεται στον συνδυασμό διαφορετικών τεχνικών. Αναφορικά με τις τεχνικές παρεμβολής, οι τεχνικές που εφαρμόζονται αντιστοιχούν σε κοινές τεχνικές παρεμβολής, ενώ αυτή που ξεχωρίζει για την αποτελεσματικότητά της είναι η παρεμβολή του σήματος GPS του drone.

Από την παρούσα μελέτη προκύπτει ότι ο τομέας της ασφάλειας εναντίων των κινδύνων που ελλοχεύει η ευρεία χρήση των drones θα συνεχίζει να απασχολεί την κοινωνία. Είναι, επομένως, απαραίτητη να εκτός από την εφαρμογή αυστηρών

μέτρων τόσο σε αεροδρόμια όσο και σε οποιαδήποτε άλλη δομή που χρήζει προστασίας, η ανάπτυξη και εγκατάσταση συστημάτων αντιμετώπισης των drones. Η εγκατάσταση βασικής προστασίας παραμένει καθήκον όλων καθώς ενδεχόμενες οικονομικές συνέπειες των καταστροφών, όπως δείχνει η ιστορία, μπορούν να καλυφθούν, αλλά το κόστος της απώλειας ανθρώπινης ζωής είναι ανυπολόγιστο.

5.2 Μελλοντικές επεκτάσεις

Εύκολα συμπεραίνεται ότι, είναι θέμα χρόνου μέχρι τα αεροδρόμια να αντιμετωπίσουν την απειλή όχι μόνο ενός ιπτάμενου drone και μιας σύγκρουσης με αυτό, αλλά και των drones που μεταφέρουν καταστροφικά όπλα ή ουσίες που θα ενεργοποιούνται με την κατάρριψή τους. Προς αυτή την κατεύθυνση, θα πρέπει να ενισχυθεί εκ των προτέρων η έρευνα των αμυντικών συστημάτων. Ωστόσο, καθώς το μέγεθος των εμπορικών drones συνεχίζει να μειώνεται και ο εντοπισμός τους γίνεται ολοένα και δυσκολότερος επιτρέποντας την αθόρυβη εισβολή σε προστατευόμενες περιοχές, η τεχνολογία πρέπει να εστιάσει αντίστοιχα στην βελτίωση των τεχνικών εντοπισμού τους και στην αποτελεσματικότερη λήψη αντιμέτρων.

Τέλος, η ανάλυση της παρούσας εργασίας θα μπορούσε να χρησιμοποιηθεί μελλοντικά, τόσο για την επιλογή των κατάλληλων για την εκάστοτε περίπτωση τεχνικών για την αντιμετώπιση των drones όσο και για την βελτίωση των ίδιων των συστημάτων drone.

Βιβλιογραφία

[1] Υ.Π.Α. - ΣμηΕΑ -. (2020). Hcaa.gr. https://uas.hcaa.gr/Faq#anchor3

[2] Limnaios, G. (2014). Current usage of unmanned aircraft systems (UAS) and future challenges: a mission oriented simulator for UAS as a tool for design and performance evaluation.

[3] Complete Evolution & History of Drones: From 1800s to 2021. https://www.propelrc.com/history-of-drones/

[4] Μαρκάτης, K. (2017). Drone technology & data in research journalism. Διπλωματική Εργασία.

[5] Keane, J. F., & Carr, S. S. (2013). A brief history of early unmanned aircraft. Johns Hopkins APL Technical Digest.

[6] Civric, Z. (2011). Elements of the Concept of Sustainability in the Works of Nikola Tesla In Proceedings ECOS Conference, Novi Sad.

[7] Nikola Budanovic. (2017, January 15). The Early Days Of Drones - Unmanned Aircraft From World War One And World War Two. WAR HISTORY ONLINE. https://www.warhistoryonline.com/military-vehicle-news/short-history-drones-part-1.html

[8] Whitmore, B. A. (2016). Evolution of unmanned aerial warfare: a historical look at remote airpower-a case study in innovation. US Army Command and General Staff College Fort Leavenworth United States.

[9] Maslen, S., Weizmann, N., Homayounnejad, M., & Stauffer, H. (2018). Drones and Other Unmanned Weapons Systems Under International Law. Brill.

[10] Whittle, R. (2014). Predator: the secret origins of the drone revolution. Macmillan.

[11] Hattenberger, Gautier & Bronz, Murat & Gorraz, Michel. (2014). Using the Paparazzi UAV System for Scientific Research.

[12] Piskorski, S., Brulez, N., Eline, P., & D'Haeyer, F. (2012). Ar. drone developer guide. Parrot.

[13] Theilmann, C. A. (2015). Integrating autonomous drones into the national aerospace system. Master of Science, University of Pennsylvania.

[14] Shakhatreh, H., et al. Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges.

[15] Singhal, G., Bansod, B., & Mathew, L. (2018). Unmanned Aerial Vehicle Classification, Applications and Challenges: A Review.

[16] Konstantinos Dalamagkidis, Valavanis, K. P., & Piegl, L. A. (2008). On Integrating Unmanned Aircraft Systems into the National Airspace System. Springer Science & Business Media.

[17] ΦΕΚ Τεύχος Β' 3152/30.09.2016

[18] Καραμούτας Σ. (2021). Εναέρια Εποπτικά Μέσα (Drones) Σε Θερμοκηπιακές Μονάδες. Πτυχιακή Εργασία.

[19] Austin, R. (2010). Unmanned air vehicles: UAV design, development, and deployment. Wiley.

[20] Mozaffari, M., Saad, W., Bennis, M., Nam, Y. H., & Debbah, M. (2019). A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. IEEE Communications Surveys & Tutorials.

[21] Gupta, S. G., Ghonge, M. M., & Jawandhiya, P. M. (2013). Review of unmanned aircraft system (UAS). International journal of advanced research in computer engineering & technology (IJARCET).

[22] Eriksson, N. (2018). Conceptual study of a future drone detection system Countering a threat posed by a disruptive technology. Master thesis in Product Development, Chalmers University of Technology.

[23] Demir, K. A., Cicibas, H., & Arica, N. (2015). Unmanned aerial vehicle domain: areas of research. Defence Science Journal.

[24] Kardasz, P., Doskocz, J., Hejduk, M., Wiejkut, P., & Zarzycki, H. (2016). Drones and Possibilities of their Using. Journal of Civil Environmental Engineering.

[25] Νίκη, Κ., (2018). Εναέρια μη επανδρωμένα συστήματα λήψης εικόνων και τα προγράμματα φωτογραμμετρικής παραγωγής τους. Ερευνητική Εργασία. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

[26] Οι αισθητήρες στα drones της γεωργίας. Agroclica. https://www.agroclica.gr/blog/207/aisthitires-drones-georgias

[27] Finn, R. L., & Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. Computer Law & Security Review.

[28] Loyd, L. (2017, Οκτώβριος 18). CNN gets permission to fly drones over crowds to gather news. Https://Www.inquirer.com. https://www.inquirer.com/philly/business/cnn-gets-permission-to-fly-drones-over-crowds-to-gather-news-20171018.html

[29] Hayes, Ben. (2006). Arming big brother: the EU's security research programme. Transnational Institute.

[30] Kindt, E. J. (2016). Privacy and data protection issues of biometric applications (Vol. 1). Springer.

[31] Foucault, M. (1977). Discipline and punish: The birth of the prison. Penguin Books.

[32] Kotkova, B. (2022). Airport defense systems against drones attacks. 26th International Conference on Circuits, Systems, Communications and Computers (CSCC). Tomas Bata University

[33] Gatwick drone disruption over Christmas cost £50m. (2019, Ιανουάριος 22). The Independent. https://www.independent.co.uk/travel/news-and-

advice/gatwick-drone-airport-cost-easyjet-runway-security-passenger-cancellation-a8739841.html

[34] Matic, Vladimir. Kosjer, Vladimir. Lebl, Aleksandar. Pavic, Branislav. Radivojevic, Jovan. (2020). Methods for Drone Detection and Jamming.

[35] Shi, X. Yang, C. Liang, C. Shi, Z. Chen, J. (2018). Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges.

[36] Hoffmann, F. Ritchie, M. Fioranelli, F. Charlish, A. Griffiths, H. (2016). Micro-Doppler Based Detection and Tracking of UAVs with Multistatic Radar.

[37] Systems, R. R. Drone Detection Radar | IRIS® | Robin Radar. Www.robinradar.com. https://www.robinradar.com/iris-datasheet

[38] Jahangir, M. Baker, C. (2016). Robust Detection of Micro-UAS Drones with L-Band 3-D Holographic Radar.

[39] Liu, Y. Wan, X. Tang, H. Yi, J. Cheng, Y. Zhang, X. (2017). Digital television based passive bistatic radar system for drone detection.

[40] Sturdivant, R. L. Chong, E. K. P. (2017). Systems Engineering Baseline Concept of a Multispectral Drone Detection Solution for Airports.

[41] Karlsson, B. (2017). Modeling multicopter radar return, A study in discrimination of multicopter UAVs from birds using the micro-Doppler effect. Master thesis in Applied Physics, Chalmers University of Technology.

[42] Li, C. J. Ling, H. (2017). An Investigation on the Radar Signatures of Small Consumer Drones“, IEEE Antennas and Wireless Propagation Letters.

[43] Salhi, M. Boudriga, N. (2020). Multi-Array Spherical LIDAR System for Drone Detection. 22nd International Conference on Transparent Optical Networks (ICTON). Bari, Italy.

[44] Sier, H. Yu, X. Catalano, I. Queralta, J. P. Zou, Z. Westerlund, T. (2023). UAV Tracking with Lidar as a Camera Sensor in GNSS-Denied Environments.

International Conference on Localization and GNSS (ICL-GNSS). Castellón, Spain.

[45] Mileusnić, M. Popović, M. Lebl, A. Mitić, D. Markov, Ž. (2014). Influence of Users' Density on the Mean Base Station Output Power.

[46] Willy L. (2003). Effects of RadioWave Propagation in Urbanized Areas on UAV-GCS Command and control. Master of science thesis in electrical engineeringNaval Postgraduate School, Montery, California.

[47] Teh, B.-P. (2017). RF techniques for detection, classification and location of commercial drone controllers. Keysight technologies.

[48] Nguyen, P. Truong, H. Ravindranathan, M. Nguyen, A. Han, R. Vu, T. Matthan. (2017). Drone Presence Detection by Identifying Physical Signatures in the Drone's RF Communication.

[49] Scheller, W. D. (2017). Detecting drones using machine learning. Thesis for master of science. Iowa State University.

[50] Peacock, M. Johnstone, M. N. (2013). Towards Detection and Control of Civilian Unmanned Aerial Vehicles. 14th Australian Info. Warfare and Security Conference, Edith Cowan Univ., Perth, Western Australia.

[51] Bernardini, A. Mangistordi, F. Pallotti, E. Capodiferro L. (2017). Drone detection by acoustic signature identification. IS&T International Symposium on Electronic Imaging. San Francisco, United States.

[52] Chua, Z. Haroush, G. Leung, C. Malhotra, A. Olexa, P. Wilson, A. Zhao, Y. (2016). Detection of Civil Unmanned Aerial Vehicles by Sound Processing. Imperial College London.

[53] Liu, H. Qu, F. Liu, Y. Zhao, W. Chen, Y. (2018). A drone detection with aircraft classification based on a camera array. Conference Series: Materials Science and Engineering.

[54] Andraši, P. Radišić, T. Muštra, M. Ivošević, J. (2017). Night-time Detection of UAVs using Thermal Infrared Camera. International Conference on Air Transport.

[55] CASE STUDY SPYNEL IR Camera: A Proven Solution for Drone Swarms /Small UAVs Detection & Tracking OVERVIEW. https://hgh-infrared.com/wp-content/uploads/2020/11/HGH_CaseStudy_Spynel_DroneUAVDetection.pdf

[56] Comprehensive anti-drone system.. APS. https://apsystems.tech/en/products/comprehensive-anti-drone-system

[57] SmartHub - Countermeasure. AI-Enabled Multi-Mission Solutions. https://www.droneshield.com/products/smarthub

[58] OPTIX Anti-Drone system. Www.optixco.com. https://www.optixco.com/en/security-and-monitoring-systemss-166/optix-anti-drone-system-196/optix-anti-drone-system-111

[59] Drone Jammer UAV Blocker Anti-Drone Radio Frequencys Signal for Sale. Www.perfectjammer.com. https://www.perfectjammer.com/drone-signal-jammers.html

[60] Drone Jammers. Jammers4u.com. http://jammers4u.com/drones-jammer

[61] Drone Killer 6 - Powerful UAV (GPS WIFI 5GHz) jammer - 120Watt. Jammer-Store.com. https://www.jammer-store.com/drone-killer-6.html

[62] Pokrajac, I. Kozić, N. Čančarević, A. Brusin, R. (2018). Jamming of GNSS Signals.

[63] Grover, K. Lim, A. Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: A survey.

[64] Xu, W. Ma, K. Trappe, W. Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies.

[65] Bayraktaroglu, E. King, C. Liu, X. Noubir, G. Rajaraman, R. Thapa, B. (2013). Performance of ieee 802.11 under jamming.

[66] Mead, J. Bobda, C. Whitaker, T. JL. (2016). Defeating Drone Jamming with Hardware Sandboxing. Asian Hardware-Oriented Security and Trust (AsianHOST) Conference. Yilan, Taiwan.

[67] Drone jammer for hostile environments: DroneDefender. Www.dedrone.com. https://www.dedrone.com/solutions/drone-defender

[68] Borio, D. (2008). A Statistical Theory for GNSS Signal Acquisition. Tesi di Dottorato in Elettronica e delle Communicazioni. Politecnico di Torino.

[69] Kuusniemi, H. Airos, E. Bhuiyan, M. Kröger, T. (2017). Effects of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. NNF Workshop on GNSS Interference and Jamming. Oslo, Norway.

[70] Da Silva, D. A. M. (2017). GPS Jamming and Spoofing using Software Defined Radio. A Dissertation for the Degree of Master in Telecommunications and Computer Engineering. University Institute of Lisbon.

[71] Jones, M. (2011). The Civilian Battlefield: Protecting GNSS Receivers from Interference and Jamming.

[72] Farid, M. A. Ahmad, M. Ahmed, S. Rahim, S. S. (2018). Impact and Detection of GPS Jammers and Countermeasures against Jamming. International Journal of Scientific & Engineering Research.

[73] Borio, Daniele. Dovis, Fabio. Kuusniemi, Heidi Lo Presti, Letizia. (2016). Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers.

[74] Pärlin, K. (2017) Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems. Master's Thesis. Tallinn University of Technology.

[75] Shannon, Claude E. (1948). A mathematical theory of communication. The Bell System Technical Journal.

[76] Harjula, Ilkka. Pinola, Jarno. Prokkola, Jarmo. (2011). Performance of IEEE 802.11 based WLAN devices under various jamming signals. Military Communications Conference.

[77] Volpe, J. (2001). Vulnerability assessment of the transportation infrastructure relying on the global positioning system. National Transportation Systems Center.

[78] Humphreys, T. Ledvina, B. Piaski, M. O'Hanlon, B. Kintner, P. (2008). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer.

[79] Psiaki, M. Powell, S. O'Hanlon, B. (2013). GNSS Spoofing Detection Using HighFrequency Antenna Motion and Carrier-Phase Data.

[80] Von Hunerbein, K. Lange, W. (2014). A New Solution of Generation of Spoofing Signals for GNSS Receivers. International Symposium on Certification of Gnss Systems and Services (CERGAL).