ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
Τμ. ΜΗΧΑΝΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ
Π.Μ.Σ. «ΜΗ ΕΠΑΝΔΡΩΜΕΝΑ ΑΥΤΟΝΟΜΑ ΚΑΙ ΤΗΛΕΚΑΤΕΥΘΥΝΟΜΕΝΑ ΣΥΣΤΗΜΑΤΑ»

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΜΗ ΕΠΑΝΔΡΩΜΕΝΑ ΑΥΤΟΝΟΜΑ ΚΑΙ ΤΗΛΕΚΑΤΕΥΘΥΝΟΜΕΝΑ ΣΥΣΤΗΜΑΤΑ»

ΤΙΤΛΟΣ

ΜΕΛΕΤΗ ΚΑΙ ΑΠΟΤΙΜΗΣΗ ANTI-DRONE ΤΕΧΝΟΛΟΓΙΩΝ

ΤΙΤΛΟΣ ΑΓΓΛΙΚΑ:

STUDY AND EVALUATION OF ANTI-DRONE TECHNOLOGIES

Ονοματεπώνυμο Φοιτητή:

Πολυχρόνης Ρεκατσίνας

Ονοματεπώνυμο Υπεύθυνου Καθηγητή:

Δρ. Χρήστος Δρόσος

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΑΡΤΙΟΣ 2024

Μέλη Εξεταστικής Επιτροπής

Δρόσος Χρήστος

Digitally signed by CHRISTOS DROSOS
Date: 2024.04.26 09:09:46 +03'00'

Παπουτσιδάκης Μιχαήλ

Digitally signed by Michail Papoutsidakis
Date: 2024.04.26 13:54:22 +03'00'

Χατζόπουλος Μάκης

Digitally signed by AVRAAM CHATZOPOULOS
Date: 2024.04.28 21:15:37 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Πολυχρόνης Ρεκατσίνας του Ιωάννη, με αριθμό μητρώου 8096618 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «Μη Επανδρωμένα Αυτόνομα και Τηλεκατευθυνόμενα Συστήματα» του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής της Σχολής Μηχανικών Πανεπιστημίου Δυτικής Αττικής, δηλώνω υπεύθυνα ότι: «Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου».

Ο δηλών

Ημερομηνία

03/2024

ΤΙΤΛΟΣ

ΜΕΛΕΤΗ ΚΑΙ ΑΠΟΤΙΜΗΣΗ ANTI-DRONE ΤΕΧΝΟΛΟΓΙΩΝ

ΟΝΟΜΑ ΦΟΙΤΗΤΗ

Πολυχρόνης Ρεκατσίνας

Μεταπτυχιακή Διπλωματική Εργασία που υποβάλλεται στο καθηγητικό σώμα για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του μεταπτυχιακού τίτλου του Προγράμματος Μεταπτυχιακών Σπουδών «Μη Επανδρωμένα Αυτόνομα και Τηλεκατευθυνόμενα Συστήματα» του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής του Πανεπιστημίου Δυτικής Αττικής.

Περίληψη

Αυτή η μεταπτυχιακή διατριβή παρουσιάζει μια εκτενή έρευνα σχετικά με τα συστήματα αντί-Drone. Μετά την εμφάνιση των εναέριων Drone για στρατιωτικές χρήσεις άρχισαν να κάνουν την εμφάνισή τους και οι εμπορικές εφαρμογές τους . Πλέον τα εμπορικά UAV είναι εντυπωσιακά drone και οικονομικά προσβάσιμα στον απλό πολίτη .Πέρα από τις εφαρμογές τους σε πάρα πολλές εργασίες, συγχρόνως άρχισαν να εμφανίζονται και οι κακόβουλες χρήσεις τους δημιουργώντας προβλήματα και απειλές για την ζωή και τις κτιριακές εγκαταστάσεις και τα κρούσματα αυτά άρχισαν να αυξάνονται σταδιακά. Ωστόσο, είναι αδύνατο σήμερα να είναι διαθέσιμο από ένα υπερσύγχρονο αντί-Drone σύστημα στρατιωτικού επιπέδου για κάθε δημόσια εγκατάσταση ή κοινωνική συνάθροιση για προστασία από τρομοκρατικά χτυπήματα με χρήση εναέριων drone λόγω του κόστους εγκατάστασης και της πολύπλοκης λειτουργίας τους. Σε αυτή την μελέτη επικεντρώνομαι στην ανάλυση συστημάτων και τεχνολογιών αντί-Drone που δεν αποτελούν μεγάλες εγκαταστάσεις συστημάτων που αποτελούν στρατιωτικά όπλα άμυνας, ερευνώντας μια ευρεία γκάμα διαθέσιμων τεχνολογιών που μπορούν να χρησιμοποιηθούν σε αντί-Drone συστήματα και προτείνοντας κατάλληλα μοντέλα συστημάτων και τεχνολογίες για αξιόπιστη προστασία από Drone που χρησιμοποιούνται με κακόβουλη χρήση. Αρχικά γίνεται ταξινόμηση στις τεχνολογίες αντί-Drone στην ανίχνευση, ταυτοποίηση και εξουδετέρωση και γίνετε έρευνα και ανάλυση για καθεμία από αυτές καθώς και για τον τρόπο λειτουργίας και τα πρωτόκολλα που χρησιμοποιούνται από αυτά τα συστήματα. Στη συνέχεια παρουσιάζονται πολύπλοκες επαγγελματικές ή στρατιωτικές λύσεις που υπάρχουν σήμερα και στο τέλος προτείνεται ένα υποθετικό σύστημα αντί-Drone με υπάρχουσες και διαθέσιμες τεχνολογίες ανοιχτού κώδικα και αναλύεται ο τρόπος κατασκευής και λειτουργίας του για χρήση σε εμπορικά Drone ως μια προσιτή λύση σε σχέση με τα ακριβά και πολύπλοκα στρατιωτικά συστήματα που είναι διαθέσιμα ως τεχνολογία . Επιπλέον, παρουσιάζονται τεχνολογίες ασφάλειας που υπάρχουν στα Drone και μπορούν να ακυρώσουν τις τρέχουσες μεθόδους αντί-Drone και τέλος προτείνω βελτιώσεις και μελλοντικές λύσεις για την αντιμετώπιση αυτών των προκλήσεων.

Λέξεις Κλειδιά:

RF ,anti-drone ,UAV ,Drone , Drone Protocols, Doppler, PESA, AESA, Stealth mode, RFID,RSSI,ADS-B ,GPS,Παρεμβολή ,Ανίχνευση ,Hijacking , spoofing, Jamming, spot jamming ,sweep jamming, barrage jamming, PX4,ArduPilot ,Killer Drones ,Swarm drones, RCS ,EMP ,Passive RF UCAV, Στερεοσκοπική Σάρωση Lidar, GPS, GLONASS, Galileo, Laser Dazzlers, Laser Guns, shooting nets, Drone hunter-killer, DroidPlanner, Tower, MAVLink, Mission Planner,Flying ad-hoc network -FANETs Protocols, AODV,OLSR,DSR,MANET,DSDV,RRP,DSR,TSODR ,HRP,ZRP,TORA,DAG,IEEE 802.1X ,WiMAX,LTE,LoRa,LoRaWAN,LPWAN,OTAA,ABP,5G,6G,LECast-blockchain,ELPC,SATCOM,Ku,Ka-Band,Clock glitching, malware, CUS, LAP, HAP, Data Fusion, SAR, Pulse-Doppler, MIMO, HPEM,HPM,EMP , Ddos ,Hack RF ,mcu8266

Abstract

This master's thesis presents an extensive study on anti-Drone systems. Following the emergence of unmanned aerial vehicles (UAVs) for military purposes, their commercial applications have also expanded. Commercial UAVs are now impressively advanced and economically accessible to the general public. Beyond their various applications, concerns arise regarding potential malicious uses, posing threats to both safety and infrastructure. This study focuses on the analysis of anti-Drone systems and technologies that are not large installations of systems that constitute military defence weapons, surveying a wide range of available technologies that can be used in anti-Drone systems and recommending suitable system models and technologies for reliable protection from Drones being used maliciously. The study begins with a classification of anti-Drone technologies in detection, identification, and neutralization, conducting research and analysis on each, including their operational methods and protocols. Subsequently, complex professional or military solutions currently available are presented, followed by a hypothetical anti-Drone system utilizing existing open-source technologies, analyzing its construction and operation for use against commercial drones as a cost-effective alternative to expensive and intricate military-grade systems. Additionally, security technologies existing within drones that can counter current anti-Drone methods are discussed, and finally, improvements and future solutions for addressing these challenges are proposed.

Keywords:

Galileo, Laser Dazzlers, Laser Guns ,shooting nets, Drone hunter-killer, DroidPlanner, Tower, MAVLink, Mission Planner ,Flying ad-hoc network -FANETs Protocols, AODV,OLSR,DSR,MANET,DSDV,RRP,DSR,TSODR ,HRP,ZRP,TORA,DAG,IEEE 802.1X ,WiMAX,LTE,LoRa,LoRaWAN,LPWAN,OTAA,ABP,5G,6G,LECast-blockchain,ELPC,SATCOM,Ku,Ka-Band,Clock glitching, malware, CUS, LAP, HAP, Data Fusion, SAR, Pulse-Doppler, MIMO, HPEM,HPM,EMP , Ddos ,Hack RF ,mcu8266

Περιγραφή

Στη παρούσα διπλωματική θα μελετηθούν εκτεταμένα τα πρωτόκολλα ,επικοινωνίας που χρησιμοποιούνται για την επικοινωνία των drone με το σταθμό ελέγχου αλλά και μεταξύ τους. Θα υπάρξει έρευνα για υπάρχουσες τεχνολογίες πάνω στο πεδίο αυτό θα πραγματοποιηθεί αποτίμηση αυτών και στο τέλος θα υπάρξουν προτάσεις για τη βελτίωση αυτών ή και τη δημιουργία καινούργιας.

SkyWiper

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσους με βοήθησαν να επιτύχω αυτό το ερευνητικό έργο. Πρώτα από όλους θα ήθελα να ευχαριστήσω το επιβλέποντα αξιότιμο καθηγητή μου Δρ. Δρόσο Χρήστο καθηγητή του Πανεπιστημίου Δυτικής Αττικής του τμήματος Βιομηχανικής Σχεδίασης και Παραγωγής – Σχολής Μηχανικών για την άψογη συνεργασία στη διπλωματική μου και την διαθέσιμη πηγή γνώσης που κατέχει. Ευχαριστώ επίσης τον καθηγητή και διευθυντή κέντρου ερευνητικών προγραμμάτων του πολεμικού ναυτικού Τσάκωνα Κωνσταντίνο για την πρόσβαση σε επιστημονική γνώση που μου παρείχε. Θα ήθελα να εκφράσω επίσης την ικανοποίηση και χαρά μου που υπήρξα μεταπτυχιακός φοιτητής στο Πανεπιστήμιο Δυτικής Αττικής (UNIWA) στο μεταπτυχιακό πρόγραμμα ‘MSc-Unmanned Autonomous and Remote Controlled Systems ‘ με διευθυντή προγράμματος τον Δρ. Παπουτσιδάκη Μηχαήλ , στο οποίο διαθέτει υψηλού επιπέδου κατάρτισης καθηγητές και προγράμματα σπουδών στην αιχμή της τεχνολογίας.

chronisrr@gmail.com

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ /ΕΙΚΟΝΩΝ

1. Εισαγωγή

Τα μη επανδρωμένα εναέρια οχήματα, γνωστά και ως drones, έχουν προκαλέσει σημαντική πρόοδο σε διάφορους βιομηχανικούς τομείς, από τη γεωργία έως την άμυνα [1]. Ωστόσο, η επιταχυνόμενη ανάπτυξη στη βιομηχανία των drones έχει ξεπεράσει κατά πολύ τα όρια των κανονισμών ασφάλειας όπου αυτοί υπάρχουν για την ασφαλή και εύλογη χρήση τους, καθιστώντας τα πρόκληση για κατάχρηση και στην χρήση για εγκληματικούς σκοπούς [1]. Αυτή η ανησυχία και η πιθανότητα τέτοιου κινδύνου έχει οδηγήσει στην ανάπτυξη της τεχνολογίας αντί-drone και στα στρατιωτικά συστήματα CUS (ή Counter UAV Systems), που αποσκοπεί στον έλεγχο των drones ,τον περιορισμό των απειλών και των επιπτώσεων που συνδέονται με την κακή χρήση των drones. Τα συστήματα αντι-drone στις μέρες μας σχεδιάζονται τεχνολογικά για την αντιμετώπιση παράνομων δραστηριοτήτων ή τρομοκρατικών επιθέσεων που πραγματοποιούνται με τη χρήση UAV, και πρέπει να συνεχίσουν να εξελίσσονται για να είναι ικανά να αντιμετωπίσουν και τις μελλοντικές ραγδαία αναπτυσσόμενες τεχνολογίες πτήσης των drones.

Αυτή τη στιγμή, τα περισσότερα επαγγελματικά συστήματα αντι-drone είναι στρατιωτικά ή βασίζονται σε στρατιωτικές τεχνολογίες για την ανίχνευση και αντιμετώπιση των drones. Οι κύριες μέθοδοι αντιμετώπισης περιλαμβάνουν τον εντοπισμό των drones μέσω ραντάρ, αισθητήρων θερμότητας, οπτικών καμερών και ανιχνευτών σήματος, καθώς και τη χρήση επεμβατικών μεθόδων για την αποτροπή ή την απομάκρυνση των drones. Οι στρατιωτικές επεμβατικές μέθοδοι περιλαμβάνουν την κατάρριψη των drones μέσω ρουκετών, τη χρήση εμποδίων ή αντιαεροπορικών πυραύλων, και τη χρήση τεχνολογίας παρεμβολών διαφόρων τύπου RF (Radio Frequency) με στόχο την ανάληψη του έλεγχου του εχθρικού drone. [2]

Ωστόσο, οι συνεχώς εξελισσόμενες τεχνολογίες πτήσης των drones, καθώς και η αύξηση της χρήσης τους σε πυκνοκατοικημένες περιοχές ,έχουν οδηγήσει στην ανάγκη για πιο ασφαλείς μεθόδους ρίψης για τον περιβάλλοντα χώρο και γενικότερα πιο αποτελεσματικές μεθόδους αντιμετώπισης τους. Μια από τις προσεγγίσεις που έχουν εξεταστεί είναι η χρήση τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) για τον εντοπισμό και την απόκτηση ελέγχου των drones που χρησιμοποιούνται με εγκληματική χρήση.

Η τεχνητή νοημοσύνη και η μηχανική μάθηση μπορούν να βοηθήσουν στον εντοπισμό των drones μέσω ανάλυσης εικόνων και δεδομένων σήματος. Επίσης, η αυτοματοποίηση και η αυτόνομη λήψη αποφάσεων μπορούν να χρησιμοποιηθούν για την ανίχνευση και τον εντοπισμό των drones, καθώς και για τη λήψη αποτελεσματικών μέτρων αντιμετώπισης, όπως η ρίψη του drone ή η ανάληψη του ελέγχου του.

Παράλληλα, είναι σε εξέλιξη ερευνητικές προσπάθειες για την ανάπτυξη τεχνολογιών αντι-drone που βασίζονται σε ανεξάρτητους αισθητήρες, όπως οι ειδικοί αισθητήρες ήχου και lidar και οι θερμικές κάμερες και υπερύθρων, που θα είναι σε θέση να εντοπίζουν και να αναγνωρίζουν τα drones ανεξαρτήτως του τύπου τους ή της τεχνολογίας που χρησιμοποιούν.

Συνολικά, η ανάπτυξη τεχνολογιών αντιμετώπισης drones βρίσκεται σε συνεχή εξέλιξη, με τη συμβολή της τεχνητής νοημοσύνης και της μηχανικής μάθησης να ανοίγει νέες δυνατότητες για την αντιμετώπιση του αυξανόμενου προβλήματος των drones σε διάφορους τομείς. Παράλληλα, είναι σημαντικό να λαμβάνονται υπόψη οι ηθικές, νομικές και ασφαλείας πτυχές κατά την ανάπτυξη και χρήση αυτών των τεχνολογιών, προκειμένου να εξασφαλίζεται πάντα η ασφάλεια και η ιδιωτικότητα των ανθρώπων.

2. Περιστατικά κακόβουλης χρήσης UAV drone:

-Αύξηση της Παράνομης Χρήσης και η Απειλή της Τρομοκρατίας.Οι περιπτώσεις παράνομης χρήσης drone και οι ενδεχόμενες συνέπειες τους ,έχουν γνωρίσει πρόσφατα ανησυχητική αύξηση. Μέσα από την ανάλυση πολλών σημαντικών περιστατικών, μπορούμε να αναδείξουμε τους αναγκαίους στόχους των αντι- drone συστημάτων.

-Παράνομες Πτήσεις σε Αεροδρόμια Το δεύτερο μεγαλύτερο αεροδρόμιο του Ηνωμένου Βασιλείου, το Gatwick, σταμάτησε τη λειτουργία των πτήσεων τον Δεκέμβριο του 2018, [2] καθώς ένα παράνομο drone παραβίασε τον εναέριο χώρο του αεροδιαδρόμου [13]. Σε αυτή την περίπτωση, drones χωρίς άδεια εμφανίστηκαν περισσότερες από 50 φορές κοντά στο αεροδρόμιο, δημιουργώντας αναστάτωση για σχεδόν 15 ώρες. Αυτά τα drones ήταν εξαιρετικά μεγάλα και ανήκαν στην κατηγορία των βιομηχανικών μοντέλων, υπερβαίνοντας δραστικά τα εμπορικά drones. Παρόμοια περιστατικά παρατηρήθηκαν και στο αεροδρόμιο της Φρανκφούρτης, στη Γερμανία, τον Μάιο του 2019, όπου παράνομα drones παρέμειναν κοντά στην περιοχή προσγείωσης για περίπου μία ώρα [14]. Και στις δύο περιπτώσεις, τα drones κατάφεραν να πλησιάσουν κρίσιμα σημεία όπως ο διάδρομος προσγείωσης ή ο κρίσιμος εναέριος χώρος, χωρίς να εντοπιστούν από τα συστήματα ασφαλείας των αεροδρομίων. Τέτοια περιστατικά οδήγησαν σε σημαντικές οικονομικές απώλειες λόγω της δυσκολίας εντοπισμού, έλλειψης ακρίβειας και συτημάτων αντιμετώπισης έναντι ανεξέλεγκτης κυκλοφορίας μη εξουσιοδοτημένων ή παράνομων drones.

-Επιθέσεις σε Δημόσια Ιδρύματα Τον Σεπτέμβριο του 2011. [2] Ένα μη επανδρωμένο αεροσκάφος φορτωμένο με βόμβα C-4 προσπάθησε να επιτεθεί στο Υπουργείο Άμυνας των ΗΠΑ και στο Καπιτώλιο [15]. Ευτυχώς, ο χειριστής συνελήφθη από το FBI πριν από την εκτέλεση της επίθεσης. Αυτό το περιστατικό αποτέλεσε την πρώτη γνωστή περίπτωση τρομοκρατίας που χρησιμοποιούσε drones και ήταν ένα παράδειγμα πρόληψης επιθέσεων από το FBI μέσω ανίχνευσης και προληπτικής αποτροπής. Αυτή η υπόθεση υπογραμμίζει τη σημασία της ανάπτυξης ενός συστήματος αντιμετώπισης των drones, το οποίο απαιτεί συνεργασία με εθνικούς οργανισμούς, όπως η αστυνομία και ο στρατός.

-Ο ρωσικός στρατός απέτρεψε την πρώτη επίθεση κατά του στόλου του από μη επανδρωμένα αεροσκάφη τον Ιανουάριο του 2018 [2] .Δεκατρία οπλισμένα μη επανδρωμένα αεροσκάφη σταθερής πτέρυγας προσπάθησαν να εισβάλλουν στην

εγκατάσταση του στόλου, αλλά απωθήθηκαν από τα αντι-αεροπορικά συστήματα που τα εντόπισαν και κατέστησαν ανίκανα τα drones. Και αυτό το περιστατικό αποτέλεσε σημαντικό παράδειγμα για την ανάγκη ανάπτυξης και εφαρμογής αποτελεσματικών συστημάτων ανίχνευσης και αποκλεισμού των UAVs.

Τα παραπάνω περιστατικά αποτελούν μόνο μερικά παραδείγματα της παράνομης χρήσης drones και της απειλής της τρομοκρατίας που μπορούν να συνεπάγονται. Για να αντιμετωπιστεί αυτή η πρόκληση, είναι απαραίτητο να αναπτυχθούν αποτελεσματικά συστήματα ανίχνευσης, παρακολούθησης και αποτροπής για την αντιμετώπιση της παράνομης χρήσης των drones και την προστασία των κρίσιμων υποδομών και του κοινού.

-Σε ένα άλλο περιστατικό ένα αεροσκάφος που είχε αναπτυχθεί για να επιτεθεί στη βάση της Πολεμικής Αεροπορίας Khmeimim και στη ναυτική εγκατάσταση Tartus [2] απωθήθηκε από τη ρωσική στρατιωτική τεχνολογία ηλεκτρονικού ραδιοπολέμου. Συγκεκριμένα, δέκα drones καταρρίφθηκαν από πυραύλους, ενώ τα άλλα τρία μπλοκαρίστηκαν από τη ρωσική τεχνολογία αεροπειρατείας. Πολλές στρατιωτικές βάσεις διέθεταν υψηλού επιπέδου αντιαεροπορικά συστήματα, αλλά οι αντιαεροπορικοί πύραυλοι δεν μπορούν να χρησιμοποιηθούν σε μη στρατιωτικές εγκαταστάσεις και κατοικημένες περιοχές. Γι' αυτό, τα συστήματα αντι-drone θα πρέπει να επικεντρωθούν στην ανάπτυξη τεχνολογιών εξουδετέρωσης που δεν απαιτούν όπλα, όπως η ανάληψη ελέγχου και η σύλληψη του κακόβουλου drone.

-Ένα άλλο παράδειγμα παράνομης χρήσης drones συνέβη στην Aramco, την εθνική εταιρεία πετρελαίου της Σαουδικής Αραβίας, τον Σεπτέμβριο του 2019. Σε αυτή την επίθεση, δέκα drones επιτέθηκαν στις μεγαλύτερες εγκαταστάσεις διύλισης πετρελαίου, μεταφέροντας εκρηκτικά. Το περιστατικό προκάλεσε σημαντική ζημιά στην παραγωγή αργού πετρελαίου της Σαουδικής Αραβίας και επηρέασε την παγκόσμια τιμή του αργού πετρελαίου. Η επίθεση αυτή πραγματοποιήθηκε λόγω έλλειψης συστημάτων ταυτόχρονης ανίχνευσης και άμυνας κατά πολλαπλών drones. Η εγκατάσταση εξοπλισμού εξουδετέρωσης drone σε τόσο μεγάλο αριθμό εγκαταστάσεων και επιχειρήσεων είναι σχεδόν αδύνατη. Ως εκ τούτου, είναι αναγκαίο να δοθεί προτεραιότητα και να επικεντρωθούν οι προσπάθειες καταπολέμησης των drones σε κρίσιμες εγκαταστάσεις.

-Επιθέσεις σε συγκεκριμένα άτομα:Τον Απρίλιο του 2015, ένα μικρό drone που περιείχε ραδιενεργά υλικά έπεσε στην οροφή της κατοικίας του Ιάπωνα πρωθυπουργού [18]. Το drone όχι μόνο κατάφερε να πετάξει πάνω από την κατοικία του πρωθυπουργού, αλλά παρέμεινε ανεπτυγμένο και ανενόχλητο για περίπου δύο εβδομάδες. Είναι προφανές ότι υπήρχε έλλειψη ή ανεπαρκές σύστημα ανίχνευσης για drones. Ωστόσο, η εγκατάσταση εξειδικευμένου εξοπλισμού ανίχνευσης θα μπορούσε να αποδειχθεί δύσκολη λόγω των συνθηκών της τοποθεσίας, ειδικά λόγω του ζητήματος της ιδιωτικής ζωής. Συνεπώς, είναι αναγκαίο να διασφαλιστούν διάφορες μέθοδοι ανίχνευσης που να προσαρμόζονται στις απαιτήσεις της κάθε περίπτωσης.

-Η ισλαμική μαχητική ομάδα Ισλαμικό Κράτος (ΙΚ) [2] χρησιμοποιεί μικρά μη επανδρωμένα αεροσκάφη για να εκτελέσει επιθέσεις με ρίψη χειροβομβίδων από το 2016. Το Ισλαμικό Κράτος σκότωσε δύο Ιρακινούς στρατιωτικούς το 2016 χρησιμοποιώντας ένα αυτοσχέδιο 'αυτοκτονικο' drone , φορτωμένο με εκρηκτικά, το οποίο εκτοξεύθηκε από απόσταση [19]. Αυτή η επίθεση αποτελεί παράδειγμα του πώς οι τρομοκρατικές οργανώσεις εκμεταλλεύονται την τεχνολογία των drones για να προβούν σε επιθέσεις σε συγκεκριμένα άτομα ή στρατηγικούς στόχους.

Είναι σημαντικό να σημειωθεί ότι οι περιπτώσεις επιθέσεων με drones είναι σχετικά σπάνιες και έχουν συμβεί σε συγκεκριμένες περιοχές και συγκεκριμένες περιστάσεις. Ωστόσο, η αυξανόμενη δημοτικότητα και προσιτότητα των drones έχει αυξήσει την ανησυχία για πιθανές επιθέσεις στο μέλλον. Οι αρχές και οι ειδικοί αναπτύσσουν μέτρα ασφαλείας και τεχνολογίες για τον εντοπισμό και την αντιμετώπιση απειλών από drones, προκειμένου να διασφαλίσουν την ασφάλεια του κοινού.

-Δύο μη επανδρωμένα ελικοφόρα εναέρια οχήματα, εφοδιασμένα με βόμβες, προσπάθησαν να σκοτώσουν τον πρόεδρο της Βενεζουέλας, Νικολάς Μαδούρο, κατά τη διάρκεια μιας εθνικής υπαίθριας εκδήλωσης τον Αύγουστο του 2018, αλλά απέτυχαν [20]. Αυτό το περιστατικό υπογραμμίζει την ανάγκη για συστήματα αντιμετώπισης των drones σε περιπτώσεις σημαντικών μεγάλων εκδηλώσεων. Για να αντιμετωπιστούν τέτοιες καταστάσεις έκτακτης ανάγκης, οι προσωρινοί μηχανισμοί αντιμετώπισης των drones απαιτούν γρήγορη εγκατάσταση και ανάπτυξη του εξοπλισμού τους. [2]

Είναι δύσκολο να ανιχνευθούν διάφορα περιστατικά με μικρά drones, ανεξαρτήτως του είδους των τοποθεσιών, είτε αυτές είναι σε στρατιωτικές εγκαταστάσεις, και σχετίζονται με τρομοκρατικές επιθέσεις ή στρέφονται κατά συγκεκριμένων ατόμων σε κατοικημένες περιοχές. Πέρα από αυτά τα περιστατικά, υπάρχουν πολλές περιπτώσεις μικροατυχημάτων, όπως εισβολή σε απαγορευμένες περιοχές από μη εξουσιοδοτημένα ή παράνομα drones. Οι απαιτήσεις για συστήματα αντιμετώπισης των drones για την αντιμετώπιση τέτοιων περιστατικών αυξάνονται διαρκώς.

3. Απαιτήσεις Συστήματος Αντί-Drone

Οι ακόλουθες είναι οι βασικές απαιτήσεις λειτουργίας για ένα σύστημα αντί-Drone[3] :

1)Ικανότητα ανίχνευσης drone: Τα υπάρχοντα συστήματα ανίχνευσης drone, όπως τα ραντάρ και οι κάμερες, δεν είναι επαρκή για την αναγνώριση διάφορων επικίνδυνων περιστατικών με drones. Το σύστημα αντι-Drone πρέπει να εξοπλιστεί με εξειδικευμένο εξοπλισμό που θα του επιτρέπει να ανιχνεύει και μικρά drones σε επαρκή απόσταση για την ανάπτυξη αποτελεσματικών μέτρων άμυνας.

2)Ικανότητα αντιμετώπισης σμήνους από drones: Υπάρχει η πιθανότητα επίθεσης από έναν ή περισσότερα drones, όπως έχει συμβεί σε προηγούμενα περιστατικά. Επομένως, το σύστημα αντι-Drone πρέπει να είναι σε θέση να ανιχνεύει και να αντιμετωπίζει παράλληλα πολλαπλές απειλές από drones.

3)Φορητότητα του συστήματος: Η αντιμετώπιση μη εξουσιοδοτημένων ή παράνομων drones ποικίλλει ανάλογα με τον χώρο και τον χρόνο. Το σύστημα αντι-Drone πρέπει να είναι φορητό ή αυτοκινούμενο για να μπορεί να μετακινείται ανάλογα με τις απαιτήσεις του περιβάλλοντος, χρησιμοποιώντας σύγχρονους πομπούς, αισθητήρες και ασύρματα δίκτυα.

Αυτές οι απαιτήσεις αποτελούν τη βάση για τον σχεδιασμό αποτελεσματικών συστημάτων αντι-Drone που θα ανταποκρίνονται στις αυξανόμενες ανάγκες ασφαλείας .Είναι γεγονός ότι [3]ο τομέας της έρευνας και ανάπτυξης αντι-drone συστημάτων παραμένει σε αρχικό στάδιο σε αντίθεση με τις τεχνολογικές εξελίξεις των drones [3] .Αν και οι συνήθεις λύσεις, όπως οι παρεμβολές ή τα αντιαεροπορικά όπλα, παρέχουν αποδεκτά αποτελέσματα για την αντιμετώπιση των drones, η χρήση αυτών των λύσεων έρχεται σε αντίθεση πολλές φορές με τη νομοθεσία,αλλά και η λειτουργία τους απαιτεί υψηλό κόστος. Για τον λόγο αυτό, η μελέτη αυτή επικεντρώνεται σε προσεγγίσεις που μπορούν να αναπτυχθούν για μη στρατιωτικές εφαρμογές και θα μπορούν να παρέχουν ασφάλεια σε εγκαταστάσεις, όπως πολιτικά αεροδρόμια, αθλητικά στάδια, χώρους συνεδριάσεων σε εξωτερικό ή εσωτερικό χώρο, κ.λπ. Αυτές οι προσεγγίσεις έχουν ως στόχο την κατασκευή αποτελεσματικών συστημάτων κατά των drones.

4. Σύστημα Αντι-drone Ανίχνευσης UAV

Η ανίχνευση drone εκμεταλλεύεται διάφορα χαρακτηριστικά λειτουργίας των εναέριων drone. Τα drones εκπέμπουν συνήθως θερμότητα, ήχο και σήματα ραδιοσυχνοτήτων για να επικοινωνούν με τον απομακρυσμένο χειριστή ή μεταξύ ενός σμήνους UAV. Το σύστημα ανίχνευσης συλλέγει δεδομένα αισθητήρων για να επιβεβαιώσει την παρουσία drones σε κοντινές περιοχές. Ανάλογα με τα δεδομένα των μετρήσεων, μπορεί να καθορίσει τις αναμενόμενες θέσεις και αποστάσεις των drones.

4.1. Θερμική Ανίχνευση

Τα εξαρτήματα-μέρη των drones, όπως οι κινητήρες, οι μπαταρίες και το εσωτερικό υλικό, εκπέμπουν σημαντική ποσότητα θερμότητας, η οποία μπορεί να ανιχνευθεί με θερμικές κάμερες . Πολλές μελέτες έχουν προτείνει την ανίχνευση των drones με βάση τις θερμικές υπογραφές τους. Ο Andrasi [4] και συνεργάτες του πρότειναν ένα σύστημα ανίχνευσης

drone που εκμεταλλεύεται τη θερμική ενέργεια που εκπέμπεται από τα drones κατά τη διάρκεια της πτήσης τους. Οι Wang και συνεργάτες χρησιμοποίησαν ένα συνελικτικό νευρωνικό δίκτυο για να βελτιώσουν την απόδοση του συστήματος και να ανιχνεύσουν με ακρίβεια τους στόχους-drones από θερμικές εικόνες. Το προϊόν Spynel της εταιρείας HGH Infrared Systems ανιχνεύει υπέρυθρες ακτίνες που εκπέμπονται από το ίδιο το αντικείμενο, επιτρέποντας παρακολούθηση σε 360°.

Σχήμα 1. Σύστημα Αναζήτησης & Παρακολούθησης Υπέρυθρων με την υψηλότερη ευκρίνεια στην αγορά - Spynel-X

Η θερμική ανίχνευση έχει ορισμένα πλεονεκτήματα, όπως την ανθεκτικότητα σε καιρικές συνθήκες, τη δυνατότητα αναγνώρισης και το χαμηλότερο κόστος σε σύγκριση με τα συστήματα βασιζόμενα σε ραντάρ. Ωστόσο, η πρακτική απόσταση ανίχνευσης (51 μέτρα [5]) είναι σημαντικά μικρότερη από τις περισσότερες άλλες προσεγγίσεις, επομένως η ενίσχυση της ευαισθησίας του συστήματος ανίχνευσης ή η βελτίωση της ανάλυσης της θερμικής κάμερας αποτελούν σημαντικές προκλήσεις.

4.2. RF Scanner

Τα drones που ελέγχονται συνήθως από έναν χειριστή ανταλλάσσουν με το χειριστήριο ή την βάση συγκεκριμένα μηνύματα που μεταφέρονται ως σήμα ραδιοσυχνοτήτων που

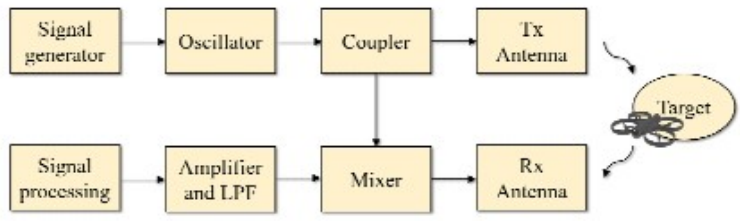
περιέχει πληροφορίες αισθητήρων, εντολές πτήσης κ.λπ. Τα αντι-drone συστήματα διαθέτουν τεχνολογίες σαρωτών ραδιοσυχνοτήτων και καταγράφουν ασύρματα τα σήματα αυτά και προσδιορίζουν την ύπαρξη drones στην περιοχή και το είδος τους.

Η ανίχνευση drone με βάση τις ραδιοσυχνότητες βασίζεται σε ευφυή μοντέλα αναγνώρισης σήματος (SIGINT) και μοντέλα επικοινωνίας (COMINT). Παραδείγματα ερευνητικών εργασιών περιλαμβάνουν αλγόριθμους εκμάθησης και ανίχνευσης σήματος ραδιοσυχνοτήτων drone όπου χρησιμοποιειούν ένα βαθύ νευρωνικό δίκτυο για την κατηγοριοποίηση των τύπων και των τρόπων πτήσης των drones. Ένα παρόμοιο αντι-drone σύστημα έχει κυκλοφορίσει η εταιρεία Da-Jing Innovations (DJI) ,το Aeroscope, ένα σύστημα ανίχνευσης που συλλέγει δεδομένα ελέγχου από drones DJI στο περιβάλλον.

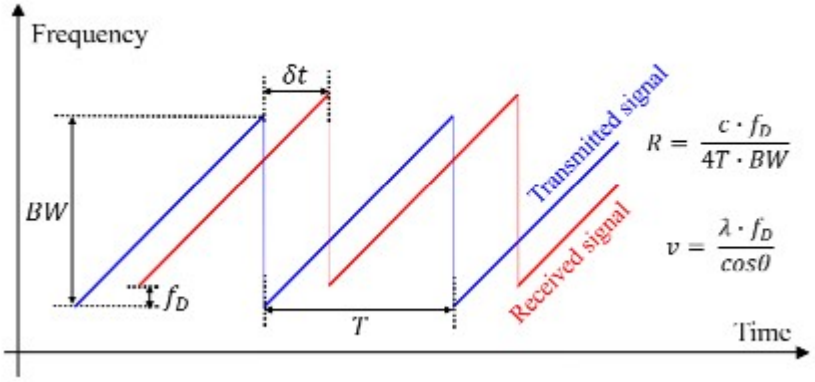
Ένα κύριο μειονέκτημα της ανίχνευσης βασιζόμενης σε ραδιοσυχνότητες είναι ότι δεν μπορεί να ανιχνεύσει drones που δεν ανταλλάσσουν συνεχώς σήματα RF, όπως αυτά που χρησιμοποιούν αυτόνομη πλοήγηση. Επιπλέον, η ανίχνευση των drones μέσω σαρωτή συγκεκριμένων ραδιοσυχνοτήτων που βασίζεται στην ανάλυση του σήματος, είναι δύσκολο να ανιχνευθούν τα drones που χρησιμοποιούν άγνωστα πρωτόκολλα ελέγχου ή διαφορετικές ζώνες συχνοτήτων. Παρ' όλα αυτά, πολλά συστήματα ανίχνευσης drone χρησιμοποιούν σαρωτές ραδιοσυχνοτήτων λόγω της μεγάλης εμβέλειας και του χαμηλού κόστους τους, συνδυάζοντάς τους με άλλες μεθόδους.

Feature	Sensing devices	Advantages	Disadvantages	Detection range
Heat	Infrared camera	• Less affected by weather • Long range	• Low accuracy	1–15 km
RF signal	RF receiver	• Obstacle-free • Detect the drone operator	• Unable to detect • Autonomous flight	3–50 km
Physical object	Radar	• Less affected by weather • Long range	• High expense • Regulations on RF license • Vulnerable to obstacles	1–20 km
Visibility	Optical camera	• Low expense • Miniaturized • Identification	• Highly affected by the weather • Vulnerable to obstacles	0.5–3 km
Acoustic signal	Acoustic receiver	• Compatible with RF based sensors • Miniaturized	• Extremely low detection range • Low accuracy • High signal detection complexity	< 0.2 km

Σχήμα 2. Drone Detection Technologies [6]



Σχήμα 3. Frequency modulated continuous wave (FMCW) mechanism. [6]



Σχήμα 4. Προσδιορισμός απόστασης και ταχύτητας – FMCW Radar (Frequency Modulated Continuous Wave) [2]

4.3. Ανίχνευση με Ραντάρ

Η ανίχνευση με βάση το ραντάρ λειτουργεί ανιχνεύοντας φυσικά αντικείμενα και παρέχοντας πληροφορίες για το σχήμα, την απόσταση, την ταχύτητα και την κατεύθυνσή τους μέσω της ανίχνευσης ανακλώμενων ραδιοσημάτων. Σε αντίθεση με τον σαρωτή ραδιοσυχνοτήτων, το ραντάρ μετρά τον χρόνο μετάδοσης του ανακλώμενου σήματος που εκπέμπει, ενώ ο σαρωτής ραδιοσυχνοτήτων αποδιαμορφώνει το λαμβανόμενο σήμα. Το ραντάρ συνεχούς κυμάτων (FMCW) και το ραντάρ παλμικού Doppler χρησιμοποιούνται για την ανίχνευση και την παρακολούθηση UAV, υπολογίζοντας την απόσταση και την ταχύτητα μέσω της μέτρησης των φάσεων του μεταδιδόμενου και λαμβανόμενου σήματος. Το ραντάρ FMCW υπολογίζει την απόσταση R από το Drone , με βάση την ταχύτητα του φωτός c, τον χρόνο μέτρησης δt, τη μετατόπιση της συχνότητας Doppler f_D και το εύρος ζώνης BW. Στη συνέχεια, η ταχύτητα του αντικειμένου μπορεί να υπολογιστεί από το c, το μήκος κύματος λ και τη γωνιακή απόκλιση θ . Τα συστήματα επιτήρησης και η παρακολούθησης με ραντάρ χρησιμοποιούν διάφορες ζώνες συχνοτήτων, οι οποίες συνοψίζονται παρακάτω.

-Ζώνες Ka, K και Ku, άνω των 18 GHz, πολύ μικρού μήκους κύματος. Χρησιμοποιούνται σε ραντάρ για ανίχνευση ιπτάμενων μέσων. Σήμερα συνηθίζονται να χρησιμοποιούνται περισσότερο από τα συστήματα ραντάρ θαλάσσιας πλοήγησης.

-Ζώνη X, 8–12 GHz. Χρησιμοποιείται εκτενώς για ανίχνευση AUV σε στρατιωτικά ραντάρ.

-Ζώνη C, 4–8 GHz. Ζώνη που χρησιμοποιείται σε πολλά αερομεταφερόμενα ερευνητικά συστήματα (π.χ. CCRS Convair-580 και NASA Air-SAR) και διαστημικά συστήματα (π.χ. ERS-1 και 2 και RADARSAT).

-Ζώνη S, 2–4 GHz. Χρησιμοποιείται σε ρωσικούς δορυφόρους ALMAZ και ραντάρ καιρού. -Ζώνη L, 1–2 GHz. Χρησιμοποιείται σε δορυφόρους US SEASAT και ιαπωνικούς δορυφόρους JERS-1 και αερομεταφερόμενα συστήματα της NASA.

-P-band, 300 kHz έως 1 GHz. Η ζώνη με τα μεγαλύτερα μήκη κύματος σε ραντάρ και χρησιμοποιούνται σε πειραματικά ερευνητικά συστήματα από τη NASA.

Το ραντάρ ταξινομείται επίσης σε 2D και 3D ανάλογα με τον τύπο της κεραίας και της φάσης σήματος. Τα δισδιάστατα ραντάρ υιοθετούν κεραίες ηλεκτρονικά σαρωμένης παθητικής συστοιχίας (PESA- Passive Electronically Scanned Array), οι οποίες ελέγχουν τη διεύθυνση της δέσμης με τη φάση ηλεκτρικού πεδίου που εφαρμόζεται σε κάθε στοιχείο συστοιχίας, παρέχοντας σχετικά μεγάλη εμβέλεια ανίχνευσης ενώ η χρήση ευρείας ζώνης δεν είναι δυνατή. Το τρισδιάστατο ραντάρ χρησιμοποιεί συνήθως κεραίες ηλεκτρονικά σαρωμένης ενεργούς συστοιχίας (AESA- Active Electronically Scanned Array), οι οποίες ελέγχουν τη διεύθυνση και το σχήμα της δέσμης από το κέρδος ηλεκτρικού πεδίου και τη φάση κάθε στοιχείου. Αν και τα AESA έχουν σχετικά μικρό εύρος ανίχνευσης, μπορούν να διορθώσουν μόνα τους σφάλματα και να υποστηρίξουν ανίχνευση ευρείας ζώνης. Σε πολλά συστήματα εφαρμόζονται τρισδιάστατα ραντάρ. Η κύρια διαφορά μεταξύ 2D και 3D ραντάρ είναι ότι το 3D ραντάρ μπορεί να εκτιμήσει το υψόμετρο των αντικειμένων-στόχων, ενώ το 2D ραντάρ αποκτά περιορισμένες πληροφορίες του άξονα z μέσω βοηθητικών συστημάτων. Το 3D ραντάρ είναι επιθυμητό για συστήματα anti-drone, όπως και το 2D ραντάρ σε συνδυασμό με άλλες μεθόδους μπορεί να είναι ακόμα και μια καλύτερη λύση από την άποψη της μεγάλης κλίμακας παρακολούθησης και της οικονομικής αποδοτικότητας.

Παρά το γεγονός ότι τα ραντάρ έχουν ευρεία χρήση σε συστήματα στρατιωτικής και πολιτικής επιτήρησης , η χρήση τους για την έγκαιρη ανίχνευση των drones είναι αμφιλεγόμενη λόγω του εξαιρετικά χαμηλού RCS (Radar Cross Section) των drones . Γενικά προτείνεται η χρήση παθητικού διστακτικού ραντάρ πολλαπλών καναλιών (PBR) για τη βελτίωση της ευαισθησίας της ανίχνευσης μέσω ραντάρ, με τη χρήση εκτεταμένων φίλτρων Kalman (EKF) και την προσέγγιση του κοντινότερου γειτονικού (GNN) για τον προσδιορισμό της θέσης του drone. Πολλές μελέτες ανίχνευσης των drones έχουν προτείνει τη χρήση ραντάρ FMCW υψηλής ανάλυσης με διάφορες βελτιώσεις, που περιλαμβάνουν διάφορες ζώνες.

Η ανίχνευση των drones μέσω ραντάρ προσφέρει μεγαλύτερη εμβέλεια και σταθερή ανίχνευση σε σύγκριση με τον σαρωτή ραδιοσυχνοτήτων, αλλά υπάρχουν περιορισμοί στη διαθεσιμότητα ανίχνευσης και νομικοί-ρυθμιστικοί περιορισμοί. Το ραντάρ δεν μπορεί να διακρίνει ένα drone κοντά σε εμπόδια, εάν το drone παραμένει σε μία θέση ή πετά με χαμηλή ταχύτητα. Επομένως, συνιστάται ο συνδυασμός ραντάρ με άλλες τεχνολογίες, όπως κάμερες, σαρωτές ραδιοσυχνοτήτων κ.λπ. Επιπλέον, τα συστήματα ραντάρ εκπέμπουν συνεχώς σήματα ραδιοσυχνοτήτων υψηλής ισχύος, και απαιτείται άδεια από το κράτος για τις ζώνες συχνοτήτων και τις τοποθεσίες εγκατάστασης. Ειδικότερα, οι ήδη

υπάρχον εγκαταστάσεις ραντάρ που λειτουργούν, όπως σε αεροδρόμια , μπορεί να αντιμετωπίσουν δυσκολίες στην εγκατάσταση ραντάρ σε κοντινές αποστάσεις λόγω προβλημάτων παρεμβολών στις ραδιοσυχνότητες. Η μερική φασματική επικάλυψη μεταξύ ραντάρ και δημοσίων δικτύων ραδιοπρόσβασης μπορεί να προκαλέσει παρεμβολές στο σήμα και μη ικανοποιητική απόδοση τόσο για το ραντάρ όσο και για το δίκτυο. Πολλές μελέτες έχουν εξετάσει την αμοιβαία παρεμβολή μεταξύ των ραντάρ από στρατιωτικούς ή άλλους κρατικούς/ιδιωτικούς οργανισμούς και των δικτύων ραδιοπρόσβασης, όπως το 5G, προκειμένου να εξασφαλιστεί η συνύπαρξη [7] . Κατά την εγκατάσταση ενός συστήματος ανίχνευσης drone, ο διαχειριστής πρέπει να λαμβάνει υπόψη αυτούς τους παράγοντες σχετικά με τις ραδιοσυχνότητες.

4.4. Ανίχνευση με Οπτική Κάμερα

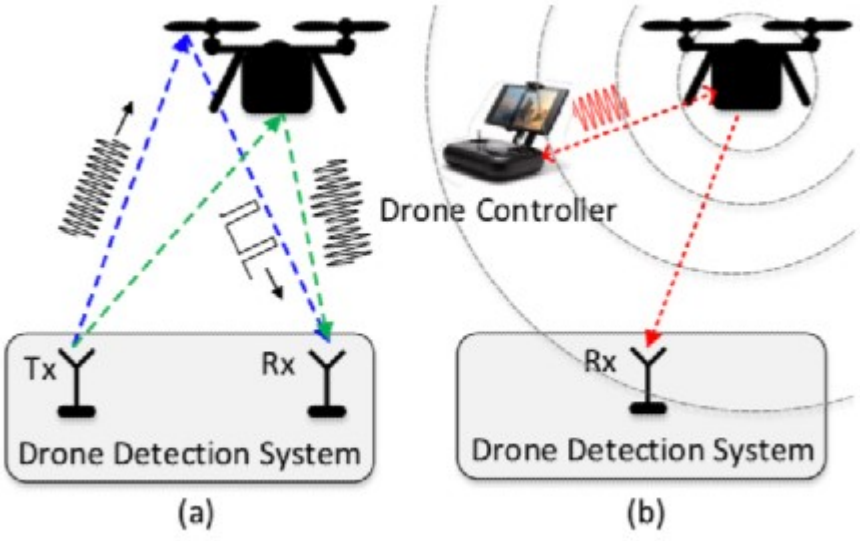
Όμοια με την ανίχνευση θερμικής κάμερας, οι οπτικές κάμερες χρησιμοποιούνται ευρέως για την ανίχνευση drones. Έχουν προταθεί διάφορες μέθοδοι για την ανίχνευση drones με χρήση οπτικών καμερών. Ένας από αυτούς είναι το ιστόγραμμα των χαρακτηριστικών προσανατολισμένων κλίσεων για την ανίχνευση drones από εικόνες, ενώ ένα άλλο είναι ένα σύστημα παρακολούθησης drones με βάση το βίντεο για την παρακολούθηση μεγάλων τρισδιάστατων χώρων σε πραγματικό χρόνο [8].

Ο εξοπλισμός ανίχνευσης drones που βασίζεται σε οπτικές κάμερες διακρίνεται για το χαμηλότερο κόστος και λιγότερους ρυθμιστικούς περιορισμούς σε σχέση με άλλες μεθόδους που αναφέρθηκαν προηγουμένως. Ωστόσο, η ανίχνευση με οπτικές κάμερες έχει μειονεκτήματα, όπως περιορισμένη εμβέλεια, ευαισθησία στις καιρικές συνθήκες και δυσκολία αντιμετώπισης εμποδίων. Για να αντιμετωπιστούν αυτά τα προβλήματα, έχει γίνει προσπάθεια συνδυασμού οπτικών καμερών με άλλους αισθητήρες. Για παράδειγμα, τα ευρέως χρησιμοποιούμενα στρατιωτικά ηλεκτροοπτικά/υπερύθρων συστήματα (EO/IR) συνδυάζουν οπτικές κάμερες με υπέρυθρους αισθητήρες για την ανίχνευση drones. Άλλοι μέθοδοι χρησιμοποιούν την χρήση μηχανικής μάθησης για την αναγνώριση εικόνας και την εύρεση πλησιέστερων στόχων, επιτυγχάνοντας ακρίβεια περίπου 83%. Παρόλο που η ανίχνευση με οπτικές κάμερες έχει περιορισμούς όσον αφορά την εμβέλεια και την παρακολούθηση της κατεύθυνσης του drone, παραμένει μια αποτελεσματική επιλογή σε συνδυασμό με άλλες μεθόδους ανίχνευσης.

Συνοψίζοντας τα μη στρατιωτικά συστήματα πρέπει να ανταποκριθούν σε ένα ευρύ φάσμα απαιτήσεων, λαμβάνοντας υπόψη τους περιορισμούς σχετικά με την παρεμβολή συχνοτήτων , τα υφιστάμενα ραντάρ και τις τεχνικές απενεργοποίησης των drones.

Κάθε μέθοδος μόνη της δεν μπορεί να ικανοποιήσει πλήρως τις τρέχουσες απαιτήσεις πληροφορίας του αντι- drone συστήματος. Για το λόγο αυτό το σύστημα ανίχνευσης drone θα πρέπει να σχεδιαστεί να χρησιμοποιεί συνεργατικές μεθόδους , συνδυάζοντας τα

στοιχεία από πολλούς αισθητήρες. Για να επιτευχθεί αυτό, όχι μόνο η κάθε μέθοδος πρέπει να βελτιωθεί για να αυξηθεί η περιοχή κάλυψης αλλά πρέπει επίσης να συνδυαστούν διάφοροι μηχανισμοί σε ένα υβριδικό σύστημα, λαμβάνοντας υπόψη τις απαιτήσεις ασφαλείας της προστατευόμενης περιοχής. Για παράδειγμα, ο σαρωτής RF παρουσιάζει σημαντικά πλεονεκτήματα σε εμβέλεια και λειτουργικότητα, εκτός από το γεγονός ότι περιορίζεται στη χρήση μόνο για εμπορικά drones που δεν φέρουν αντίμετρα και πολύπλοκα συστήματα ασφαλείας. Έτσι, ο σαρωτής ραδιοσυχνοτήτων είναι αποδεκτός σε μεγάλη κλίμακα για την ανίχνευση παράνομων ερασιτεχνικών UAV drones. Παράλληλα, οι περιοχές που είναι ευαίσθητες στα drones, όπως αεροδρόμια ή πυρηνικές εγκαταστάσεις, πρέπει να εξοπλιστούν με στοιχεία ανίχνευσης όρασης, ραντάρ και ακουστικούς αισθητήρες για την ακριβή παρακολούθηση οποιουδήποτε εναέριου drone. Προκειμένου να αντιμετωπιστούν τα μη ανιχνεύσιμα UAV με ραδιοσυχνότητα, όπως τα ειδικά κατασκευασμένα drones που χρησιμοποιούνται σε μια τρομοκρατική απειλή, η περιοχή υψηλής ασφάλειας πρέπει να αναπτύξει ευέλικτες μεθόδους ανίχνευσης για την αντιμετώπιση της τεχνολογίας απόκρυψης της πτήσης(Stealth mode) των drones .



Σχήμα 5. Ταξινόμηση μεθόδων ανίχνευσης σε σχέση με τη λειτουργικότητα και το εύρος. [9]

4.5. Υβριδικό Σύστημα Ανίχνευσης

Η χρήση μιας ενιαίας μεθόδου ανίχνευσης οδηγεί αναπόφευκτα σε τυφλό σημείο ανίχνευσης drone, καθιστώντας δύσκολη την επιτυχή εξουδετέρωση των παράνομων drones. Πολλοί κατασκευαστές υιοθετούν υβριδικά συστήματα ανίχνευσης drone, στα οποία συνδυάζουν τεχνολογία συνδυασμού αισθητήρων . Υπάρχουν μερικά χαρακτηριστικά υβριδικών συστημάτων:

Ραντάρ + όραση: Η συνδυασμένη χρήση ραντάρ και οπτικών (ή θερμικών) καμερών παρέχει συμπληρωματική ανίχνευση drone. Η ανίχνευση βασιζόμενη στην όραση μπορεί να παρακολουθεί τα drones με τον έλεγχο του ζουμ, της κλίσης και της εστίασης της εικόνας, αλλά μπορεί να αντιμετωπίσει δυσκολίες στον δυναμικό έλεγχο της περιοχής στόχου. Από την άλλη πλευρά, η ανίχνευση με ραντάρ παρέχει ευρεία περιοχή σάρωσης με χαμηλή αναγνώριση drone και χαμηλή συχνότητα σάρωσης. Έτσι, το σύστημα ραντάρ σαρώνει την περιοχή στόχου ενώ το σύστημα όρασης ελέγχει τις εξωτερικές και εσωτερικές παραμέτρους της κάμερας για ακριβή αναγνώριση ύποπτων σημείων. Αυτός ο συνδυασμός αντισταθμίζει δυναμικά τα μειονεκτήματα του ενός με του άλλου και, ως εκ τούτου, πολλοί επιλέγουν αυτήν τη δομή.

Πολλαπλοί σαρωτές RF: Οι σαρωτές ραδιοσυχνοτήτων μπορούν να ανιχνεύσουν drones και να λάβουν πρόσθετες πληροφορίες (όπως τύπος, εντολές ελέγχου κ.λπ.), αλλά δεν μπορούν πάντα να παράσχουν την ακριβή θέση τους. Εάν τα drones ελέγχονται μόνο μέσω μηνυμάτων διαμόρφωσης θέσης παλμού (PPM) ή διαμόρφωσης πλάτους παλμού (PWM), ενδέχεται να μην εκπέμπουν πληροφορίες τοποθεσίας σε κανάλι RF. Υπάρχουν πολλαπλοί σαρωτές ραδιοσυχνοτήτων που λαμβάνουν μηνύματα RF και υπολογίζουν τις θέσεις των drones χρησιμοποιώντας παραδοσιακά σχήματα εντοπισμού ραδιοσυχνοτήτων. Αυτή η προσέγγιση είναι οικονομικά πιο αποδοτική από τη χρήση κάλυψης με ισοδύναμα συστήματα ραντάρ, και γι' αυτόν το λόγο, αποτελεί μια πολύ καλή λύση η χρήση πολλαπλών σαρωτών ραδιοσυχνοτήτων αντί για ραντάρ.

Συνδυασμός οπτικών συστημάτων και ακουστικής-ήχου: Ο συνδυασμός οπτικών και ακουστικών αισθητήρων αποτελεί μια παραδοσιακή τεχνική συνδυασμού αισθητήρων που βελτιώνει την ακρίβεια της ανίχνευσης . Η ανίχνευση με βάση οπτικούς αισθητήρες δυσκολεύεται να διακρίνει άγνωστα σχήματα drone, ενώ η ανίχνευση με βάση τον ήχο επιδεικνύει χαμηλή απόδοση σε θορυβώδη περιβάλλοντα. Ο συμπληρωματικός σχεδιασμός αισθητήρων είναι αποτελεσματικός ως προς την ανθεκτικότητα στις καιρικές συνθήκες, την ανθεκτικότητα σε περιβαλλοντικές συνθήκες και την ακρίβεια της ανίχνευσης.

Διατίθενται διάφοροι συνδυασμοί τεχνολογίας ανίχνευσης που επιτυγχάνουν παρόμοια εμβέλεια ανίχνευσης στα 3-5 χιλιόμετρα. Μπορούν να εγκατασταθούν πολλαπλά συστήματα με αξιόπιστα και χαμηλής καθυστέρησης δίκτυα. Έτσι, η εύρεση μιας αποτελεσματικής διαμόρφωσης ανίχνευσης για την περιοχή του στόχου αποτελεί ένα ουσιαστικό βήμα για την κατασκευή ενός ισχυρού συστήματος αντι-drone.

Vender	Model	Radar	RF scanner	Camera (Infrared, optic)	Acoustic	Detection range (indicated)
ELTA	Drone guard	✓	✓	✓		4.5 km
Aaronia AG	AARTOS DDS	✓		✓		5 km
Advanced Protection Systems	Ctrl+Sky	✓	✓	✓	✓	3 km
CerbAir	CerbAir Fixed, Mobile		✓	✓		3 km
Rodhe and Schwarz	ARDRONIS		✓			3 km
Drone Shield	DroneSentinel	✓	✓	✓	✓	3.5 km

Σχήμα 6. Υβριδικά συστήματα ανίχνευσης -Εμβέλεια. [2]

5. Αναγνώριση Drone

Η ανίχνευση drone αναφέρεται σε συστήματα που εντοπίζουν ένα ιπτάμενο (ή ακίνητο) αντικείμενο και καθορίζουν εάν αυτό το αντικείμενο είναι ένα drone και το είδος του. Επίσης η αναγνώριση drone αναφέρεται και στον προσδιορισμό εάν το ανιχνευμένο drone κινείται παράνομα ή χρησιμοποιείται κακόβουλα και χρήζει αντιμετώπισης. Ένα απλό σύστημα ραντάρ μπορεί να επιτύχει μόνο ανίχνευση drone, αλλά δεν μπορεί να ξεχωρίσει μεταξύ drones και παρόμοιου μεγέθους πτηνών χωρίς πρόσθετο σύστημα ή επιπλέον εξοπλισμό, όπως κάμερες όρασης. Η αναγνώριση πρέπει να εκτελείται με ακρίβεια, αξιοπιστία και εγκαίρως, ιδίως όταν η περιοχή ενδιαφέροντος επιτρέπει τη νόμιμη χρήση drones για αναψυχή ή χρησιμοποιείται νόμιμα από drones. Το σύστημα αναγνώρισης πρέπει να συνεργάζεται με το σύστημα ανίχνευσης για την προστασία της περιοχής, αποφεύγοντας ψευδείς ενεργοποιήσεις αντιμέτρων.

Ιδανικά, η αναγνώριση drone θα πρέπει να πραγματοποιείται παθητικά, αναγνωρίζοντας τη νομιμότητα των drones μέσω ετικετών αναγνώρισης που προσαρτώνται σε αυτά και που περιοδικά μεταδίδουν τις πληροφορίες τους, όπως ετικέτες RFID. Ωστόσο, η πλήρης εφαρμογή της ετικέτας αναγνώρισης για να λειτουργήσει με επιτυχία θα πρέπει να υλοποιηθεί σε εθνικό ή διεθνές επίπεδο και αυτήν τη στιγμή είναι ακόμη υπό συζήτηση. Κάθε σύστημα αντι-Drone πρέπει να περιλαμβάνει ενεργές λύσεις αναγνώρισης για την αξιολόγηση του επιπέδου κινδύνου των ανιχνευμένων drones, παρακολουθώντας και αξιολογώντας τις πτήσεις συλλέγοντας συγκεκριμένες πληροφορίες, όπως το μοντέλο του drone και αναλυτικά χαρακτηριστικά που παραβιάζουν τους κανόνες ασφάλειας.

6. Παρακολούθηση(Tracking) και Εκτίμηση Πτήσης Drone

Για την παρακολούθηση της θέσης και εκτίμηση της πτήσης των drones, υπάρχουν διάφορες μέθοδοι ανίχνευσης που εστιάζουν σε θεωρητικά και συστηματικά σχήματα εκτίμησης θέσης. Οι περισσότερες μέθοδοι βασίζονται στη χρήση πληροφοριών όρασης, είτε μέσω συμβατικής επεξεργασίας εικόνας είτε μέσω μηχανικής μάθησης (όπως νευρωνικά δίκτυα, ασαφή λογική).

Τα συστήματα εκτίμησης διαδρομής χρησιμοποιούν νευρωνικά δίκτυα ή διάφορα φίλτρα για την ανάλυση των αποτελεσμάτων παρακολούθησης και την καθορισμό των κινήσεων του drone. Ένας αλγόριθμος φίλτρου Kalman μπορεί να βελτιώσει την ακρίβεια της εκτίμησης θέσης του drone βασιζόμενος σε μετρήσεις αζιμούθιου, υψομέτρου και απόστασης από τον εξοπλισμό ανίχνευσης. Επιπλέον, μέθοδοι παρακολούθησης που βασίζονται στην οπτική ροή εικόνων μπορούν να χρησιμοποιηθούν για την παρακολούθηση γρήγορων και μικρών drones, με τη χρήση αναδρομικών φίλτρων για την ανίχνευση αστοχιών παρακολούθησης που προκαλούνται από γρήγορες αλλαγές θέσης.

Επιπλέον, προτάσεις όπως ένα πολυεπίπεδο νευρωνικό δίκτυο μπορούν να χρησιμοποιηθούν για την εκτίμηση της διαδρομής του drone, λαμβάνοντας υπόψη μη γραμμικές κινήσεις και παραμέτρους δικτύου. Η παρακολούθηση και η εκτίμηση θέσης του drone είναι σε κάποιες περιπτώσεις ανεπαρκές για να κριθεί η νομιμότητά του, αλλά είναι σημαντικό επίσης να εκτιμηθεί η επικινδυνότητα της κίνησής του και ο βαθμός απειλής που μπορεί να αποτελέσει για την περιοχή άμυνας.

7. Αναγνώριση Βάσει RFID

Η τεχνολογία αναγνώρισης ραδιοσυχνοτήτων (RFID) έχει ευρύτατη χρήση στα συστήματα αναγνώρισης και εντοπισμού θέσης σε πραγματικό χρόνο (RTLS) τις τελευταίες δεκαετίες. Μια προσέγγιση αυτού του είδους είναι το σύστημα Active RFID, το οποίο χαρακτηρίζεται από χαμηλό κόστος και ελαφρύ σχεδιασμό. Προτείνεται ένα τέτοιο σύστημα για την αναγνώριση drones σε μεγάλες περιοχές, με σκοπό τον διαχωρισμό αδειοδοτημένων και μη αδειοδοτημένων UAV drones. Η κύρια πρόκληση είναι η επέκταση της εμβέλειας και οι ανησυχίες σχετικά με την ασφάλεια. Τα μη επανδρωμένα αεροσκάφη υψηλής ταχύτητας μπορεί να μην παρέχουν αρκετό χρόνο για την αναγνώρισή τους από ένα σύστημα RFID μικρής εμβέλειας. Επιπλέον, η πλαστογράφηση του σήματος RFID μπορεί να εξαπατήσει το σύστημα και να επιτρέψει σε κακόβουλα drones να παραβιάσουν την προστατευόμενη περιοχή. Επομένως, απαιτείται περαιτέρω μελέτη των μέτρων ασφαλείας για συστήματα αναγνώρισης drone με RFID και της ενεργής επικοινωνίας RFID μεγάλης εμβέλειας .

Πέρα από την αναγνώριση, έχει εκτενώς μελετηθεί η ανίχνευση της ακριβής θέσης των drones με τη χρήση ετικετών RFID για την παρακολούθησή τους. Προτείνεται μια

προηγμένη μέθοδος εντοπισμού σε εσωτερικούς χώρους, όπου εφαρμόζονται ετικέτες RFID Ultra High Frequency (UHF) στα UAV και τοποθετούνται παθητικές ετικέτες στην περιοχή ενδιαφέροντος, οι οποίες συνδέονταν με το σύστημα. Αυτή η λύση βασίζεται στις παρεμβολές μεταξύ των UAV και των ετικετών εδάφους, οι οποίες μπορούν να ανιχνευθούν μέσω της μέτρησης του δείκτη ισχύος του ληφθέντος σήματος (RSSI- Residual Signal-Strength Indicator). Το σύστημα πρώτα μετρά τις διακυμάνσεις του RSSI της ετικέτας και στη συνέχεια εκτιμά δυναμικά τη μελλοντική θέση του drone εντοπίζοντας το σημείο με τις μεγαλύτερες παρεμβολές σε σχέση με τις προμετρημένες διακυμάνσεις. Ο εντοπισμός παθητικών ετικετών σε μεγάλες περιοχές μπορεί να είναι δαπανηρός, αλλά η εκτίμηση της θέσης σε μια πυκνή κατανομή ετικετών εδάφους μπορεί να επεκτείνει επαρκώς την κάλυψη της διαθέσιμης περιοχής.

8. Αυτόματη Εκπομπή Εξαρτημένης Επιτήρησης Drone (ADS-B)

Το σύστημα ADS-B (Automatic Dependent Surveillance-Broadcast) έχει υιοθετηθεί για τον έλεγχο της εναέριας κυκλοφορίας (ATC-Air Traffic Control) των αεροσκαφών . Μέσω του ADS-B, τα αεροσκάφη εκπέμπουν περιοδικά πληροφορίες πλοήγησης μέσω ραδιοσυχνοτήτων μεγάλης εμβέλειας. Οι χρήστες εδάφους και όπως και άλλα αεροσκάφη μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να αναγνωρίσουν την κατάσταση των αεροσκαφών και να διαχωρίσουν την κίνησή τους. Το περιεχόμενο των μηνυμάτων ADS-B περιλαμβάνει τυποποιημένες πληροφορίες αναγνώρισης και πλοήγησης του αεροσκάφους, όπως υψόμετρο, GPS, αριθμός αναγνώρισης αεροσκάφους κ.λπ.

Πρόσφατα, το ADS-B έχει εφαρμοστεί και σε drones για την καταγραφή πληροφοριών πτήσης εντός μιας περιοχής στόχου. Ωστόσο, τα συμβατικά συστήματα ADS-B είναι υπερβολικά μεγάλα για μικρότερα drones, οπότε απαιτούνται μικρότερες μονάδες ADS-B. Η σειρά συστημάτων Ping2020 της uAvionix είναι ένα προϊόν που παρέχει ADS-B για drones και μπορεί να συνδεθεί με τον έλεγχο πτήσης του drone (π.χ. Pixhawk) για τη μετάδοση πληροφοριών πτήσης μέσω ραδιοκαναλιού. Ωστόσο, το Ping2020 έχει αυξημένο κόστος συγκριτικά με το αναμενόμενο (2000 δολάρια ΗΠΑ ανά Ping2020i), πράγμα που εμποδίζει την υιοθέτηση σε μεγάλη κλίμακα.

Για να δημιουργηθεί ένα ευρύτερο σύστημα αναγνώρισης drones και να υιοθετηθεί, απαιτείται ευελιξία στη φάση αναγνώρισης, από τον έλεγχο ταυτότητας του drone έως την ανάλυση των απειλών. Ένα τέτοιο αντι-drone σύστημα θα πρέπει να καθορίζει τη λογική και τη διαδικασία για αναγνώριση της πορείας εισβολής των drones. Αυτή η διαδικασία πρέπει να βασίζεται σε σταθερά κριτήρια, όπως τα αποτελέσματα ανίχνευσης, εθνικούς ή διεθνείς κανονισμούς και εργαλεία αναγνώρισης. Στη συνέχεια, ανάλογα με την καθορισμένη διαδικασία, το σύστημα αντι-drone πρέπει να παρέχει ασφαλή και προσαρμοσμένη ασφαλή λύση για την κάθε απειλή που αντιμετωπίζεται σε συγκεκριμένες συνθήκες.

Με αυτόν τον τρόπο, μπορεί να αναπτυχθεί ένα ευρύτερο σύστημα αναγνώρισης drones που θα παρέχει συνεχή και αποτελεσματική ανίχνευση. Τα χαμηλού κόστους δηλαδή μοντέλα και οι εθνικές υποδομές καταγραφής drone μπορούν να συνδυαστούν για τη δημιουργία ενός ευρέος δικτύου αναγνώρισης drone που θα είναι αποτελεσματικό και αξιόπιστο σε πολλές περιοχές.

9. Εξουδετέρωση Drone Κακόβουλης χρήσης

Ο όρος "εξουδετέρωση drone" χρησιμοποιείται για να αναφερθεί στις δράσεις που αποσκοπούν στην αντιμετώπιση απειλητικών κινήσεων από χειριστές drone, ως μέρος ενός αντι-drone συστήματος . Οι μέθοδοι εξουδετέρωσης χωρίζονται σε καταστροφικές και μη-καταστροφικές και διακρίνονται τόσο από τεχνικές παραμέτρους όσο και από τη συμμόρφωση προς τους αστικούς κανονισμούς. Σε πολλές χώρες, η καταστροφή παράνομων drones απαγορεύεται, και γι' αυτό προτιμώνται μη-καταστροφικές μέθοδοι, ειδικά σε δημόσια-αστικά περιβάλλοντα. Τα μη στρατιωτικά συστήματα επικεντρώνονται περισσότερο στις μη-καταστροφικές μεθόδους, και πρωταρχικός στόχος είναι να επιτευχθεί υψηλή αποτελεσματικότητα των συστημάτων αντι-drone ακόμη και σε αντίξοες συνθήκες.

Συγκεκριμένα, προτιμώνται μέθοδοι, όπως η προσωρινή εμπλοκή επικοινωνίας, που αποτρέπει την πρόκληση δευτερογενών κρίσεων (π.χ. προσγείωση, σύγκρουση ή/και αποτυχία λειτουργίας). Η εμπλοκή είναι αναγνωριστική και μη-καταστροφική και προκαλεί προσωρινή απώλεια επικοινωνίας σε όλη την περιοχή στόχο.

9.1. Drone Hijacking

Ο όρος "αεροπειρατεία (hijacking) " χρησιμοποιείται συχνά στον τομέα των drones.. Η μέθοδος hijacking ενός drone αναφέρεται στην περίπτωση όπου ένας επιτιθέμενος χειριστής αναλαμβάνει τον έλεγχο ενός άλλου drone στόχου, ανεξάρτητα από τη μεθοδολογία. Από την άλλη, η πλαστογράφηση(spoofing) σε ένα drone στόχο σημαίνει ότι ο χειριστής παράγει ένα ψεύτικο σήμα για να εμποδίσει το drone να ακολουθήσει τις εντολές του αρχικού απομακρυσμένου χειριστή.

Η κύρια διαφορά μεταξύ αεροπειρατείας και πλαστογράφησης έγκειται στη συμπεριφορά μετά την επίθεση. Μετά την αεροπειρατεία, ο αρχικός ελεγκτής δεν μπορεί να ανακτήσει τον έλεγχο του drone, ενώ στην πλαστογράφηση, μπορούν να χρησιμοποιηθούν ψεύτικα σήματα για να αποπροσανατολιστεί η επικοινωνία αλλά θα συνεχίσει πιθανά ημιτελώς την παράνομη δράση το drone. Η μέθοδος spoofing επικεντρώνεται κυρίως στην ανάγκη για στέρηση ελέγχου. Ένας αμυνόμενος μπορεί να παρεμβάλει ή να χακεύσει την επικοινωνία του drone με τη βάση του πριν το αντι-hijacking σύστημα του drone αποκτήσει τον

πραγματικό έλεγχο και ολοκληρώσει την επίθεσή του. Η αεροπειρατεία ενός επιθετικού-απειλητικού drone είναι τεχνικά και νομικά αμφισβητήσιμη, αλλά είναι πιο αποτελεσματική από την πλαστογράφηση. Σε κάθε περίπτωση, και οι δύο μορφές επίθεσης πρέπει να διερευνηθούν και να ληφθούν μέτρα για την προστασία και σωστή χρήση σε περιπτώσεις μόνο πραγματική απειλής.

Τα περισσότεροι drones διατηρούν στενή σύνδεση με τον χειριστή, και η αεροπειρατεία επικεντρώνεται στο να διακόψει αυτήν τη σύνδεση. Γενικά προτείνεται ένα σύστημα να διακόπτει τη σύνδεση χρησιμοποιώντας ένα σήμα εμπλοκής και να επαναφέρει αμέσως τον έλεγχο στον χειριστή του εισβολέα. Η αεροπειρατεία με drones είναι μια ιδανική προσέγγιση για την ασφαλή απόκτηση ελέγχου ή αναγκαστική προσγείωση και επιτρέπει περαιτέρω έρευνα. Πρόκληση για έρευνα αποτελεί η κάλυψης σε όλες τις περιπτώσεις πτήσεων, όπως η αυτόνομη πτήση και τα πολλά διαφορετικά πρωτόκολλα επικοινωνίας που χρησιμοποιούν τα drones.

9.2. Drone Spoofing

Η πλαστογράφηση (Spoofing)του σήματος των drones μπορεί να χρησιμοποιηθεί επίσης στην διαδικασία την αεροπειρατεία τους ή για τη σύγχυση των διαδρομών πτήσης τους. Τα drones συνήθως ελέγχονται χρησιμοποιώντας το σήμα RF από τον χειριστή, αλλά εξάγουν επίσης πληροφορίες από αισθητήρες για την παρακολούθηση της τρέχουσας κατάστασης. Τα σήματα GPS είναι κρίσιμα για τον προσδιορισμό της θέσης του drone κατά τη χειροκίνητη ή αυτόνομη πτήση. Προκαλείται με ένα σύστημα που παράγει πλαστά σήματα RF ή GPS για να παραπλανήσει τον δέκτη του drone και να τον καθοδηγήσει προς λανθασμένη θέση. Ο σκοπός είναι να επιτευχθεί η αεροπειρατεία με ασφάλεια, επηρεάζοντας για παράδειγμα τη λειτουργία GPS του εσωτερικού συστήματος του drone και να κατευθυνθεί αθόρυβα προς μια συγκεκριμένη τοποθεσία. Οι τεχνικές πλαστογράφησης μπορούν να επηρεάσουν τους διάφορους τύπους αισθητήρων των drones, οι οποίες μπορούν να συνδυαστούν και με άλλες μεθόδους για να επιτευχθεί η παραπλάνηση . Η παραπλάνηση των αισθητήρων των drones μπορεί να γίνει με ποικίλες προσεγγίσεις ανεξάρτητα από το πρωτόκολλο επικοινωνίας, αλλά η έλλειψη αντίστοιχων μέτρων ασφαλείας όπως σε πυκνοκατοικημένες περιοχές μπορεί να οδηγήσει σε ατυχήματα, όπως η απρόβλεπτη προσγείωση του drone λόγω διακοπής ελέγχου από τον χειριστή.

9.3. Αποκλεισμός Περιοχής (Geofencing)

Το σύστημα Geofence αποκλείει μια περιοχή και εμποδίζει τα drones να εισέρθουν πέρα από μια κλειστή περίμετρο ή εικονικό φράγμα ή ένα συγκεκριμένο σημείο. Λειτουργεί στη

λογική αντιμετώπισης ότι το ίδιο το drone αποφασίζει εάν πρέπει να προσγειωθεί ή όχι, με βάση την τρέχουσα θέση του . Η τεχνολογία Geofence για τα drones κατατάσσεται σε δύο τύπους .

Το δυναμικό Geofence μεταδίδει πληροφορίες σχετικά με τις περιοχές πτήσης που απαγορεύονται, ενώ το στατικό Geofence χρησιμοποιεί ένα αποθηκευτικό χώρο αδειών πτήσης που μπορεί να προσεγγιστεί από κάθε drone.

Τα περισσότερα εμπορικά drones με δημοφιλείς στοίβες ελέγχου πτήσης (πιλότους- flight controllers με πλακέτες ελεγκτών ηλεκτρικών κινητήρων) με τα αντίστοιχα λογισμικά (firmwares), όπως τα ανοιχτού κώδικα PX4 και το ArduPilot , διαθέτουν δυνατότητα για ενσωματωμένες μονάδες αυτόματης προσγείωσης για την αύξηση της ασφάλειας. Αυτή η μέθοδος αποτρέπει αποτελεσματικά τα παράνομα drones από την εισβολή σε περιοχές χωρίς άδεια, αλλά δεν μπορεί να αντιμετωπίσει ένα τροποποιημένο ή αναδιαμορφωμένο drone που απενεργοποιεί ή δεν λαμβάνει υπόψιν τα ενσωματωμένα αυτόματα συστήματα προσγείωσης. Λόγω της δυνατότητας προσαρμοσμένου προγραμματιστικά λογισμικού του drone, τα εμπορικά(όσα διαθέτουν σύστημα συμμόρφωσης) drones μπορεί να επιτρέψουν την παραβίαση της ασφαλούς περιοχής. Απαιτούνται περαιτέρω μελέτες για την αντιμετώπιση των περιπτώσεων γεωγραφικής περίφραξης, οι οποίες μπορεί να αγνοηθούν με μεθόδους και τεχνικές πλαστογράφησης.

Destructive	Name	Advantages	Disadvantages
Non-destructive	Hijacking	• Enable safe landing	• Only available for drones using known protocols
	Spoofing	• Wide availability • Includes autonomous and manual flight	• Difficult to control • Possibly nullified by manual control
	Geofencing	• Simultaneous response • Easily extended	• Only available for communicable drones • Modified or disabled by drone operators
	RF jamming	• Simple, instant procedure • Effective for drones using unknown protocols	• Can affect nearby facilities • Not effective for autonomous drones
	Capture	• Available for follow-up investigation • Ground and aerial solutions available	• Difficult to target and hit • Possible damage during landing/crush
Destructive	Laser	• Long range • Confirmatory destruction	• High maintenance and operation cost • Generally unsuitable or unavailable for non-military facilities
	Killer drone	• Low maintenance and operation cost • Possible simultaneous response to multiple drones	• Hard to target and hit • Deregulation for public drone flight required
	Anti-aircraft weapons	• Confirmatory destruction • Long range neutralization	• High maintenance and operation cost • Generally unsuitable or unavailable for non-military facilities

Σχήμα 7. Τεχνολογίες αντι – Drone .Μειονεκτήματα-Πλεονεκτήματα κάθε μεθόδου.

9.4. Drone Jamming

Η παρεμβολή των drones στοχεύει στην ‘παράλυση’ της ραδιοεπικοινωνίας μεταξύ του στόχου drone και του ελεγκτή του, μέσω της εκπομπής έντονων σημάτων ραδιοσυχνοτήτων και επικάλυψης του αρχικού σήματος. Αυτά τα σήματα μπορούν να είναι οποιουδήποτε είδους, συμπεριλαμβανομένων κενών πακέτων, εντός μιας συγκεκριμένης περιοχής συχνοτήτων. Ο γενικός στόχος είναι να προκαλέσει την αναταραχή του στόχου και να το αναγκάσει σε μια ανεξέλεγκτη κατάσταση, όπου δεν μπορεί να επικοινωνήσει με τον απομακρυσμένο χειριστή-κέντρο εκπομπής εξωτερικών σημάτων . Η τεχνολογία παρεμβολής drones μπορεί να ταξινομηθεί σε διάφορους τύπους ανάλογα με τους στόχους και τις καλύψεις που επιδιώκονται. Ορισμένα αντιπροσωπευτικά κριτήρια ταξινόμησης περιλαμβάνουν τα εξής:

Κατευθυντική παρεμβολή : Το σύστημα παρεμβολής επικεντρώνεται σε μια συγκεκριμένη κατεύθυνση.

Πανκατευθυντική παρεμβολή : Το σύστημα παρεμβολής μπορεί να επηρεάσει όλες τις κατευθύνσεις.

Σταθερή παρεμβολή: Το σύστημα παρεμβολής είναι εγκατεστημένο σε μια σταθερή τοποθεσία, όπως μια στρατηγική θέση ή ένας σταθμός βάσης.

Κινητή παρεμβολή: Το σύστημα παρεμβολής λειτουργεί από φορητές συσκευές, όπως φορητούς υπολογιστές ή συσκευές που τοποθετούνται σε οχήματα .

Στενή παρεμβολή: Ο συγκεκριμένος όρος αναφέρεται σε ένα σύστημα παρεμβολής που επηρεάζει μια στενή ζώνη συχνοτήτων.

Μεγάλη παρεμβολή: Ο συγκεκριμένος όρος αναφέρεται σε ένα σύστημα παρεμβολής που καλύπτει ένα ευρύ φάσμα συχνοτήτων .

Το jamming μπορεί επίσης να επιτευχθεί ακόμα και μειώνοντας την ποιότητα της επικοινωνίας του στόχου. Η προσέγγιση του jamming αποτελεί μια απλή, ισχυρή και ευρείας εμβέλειας λύση με χαμηλό κίνδυνο σφάλματος, και για αυτό τον λόγο πολλά αντι-drone συστήματα υιοθετούν την παρεμβολή ως την κύρια μέθοδο απενεργοποίησης ενός εχθρικού Drone. Ωστόσο, δεδομένου ότι οι τεχνικές παρεμβολής βασίζονται κυρίως στην εκπομπή ηλεκτρομαγνητικών σημάτων, μπορεί να έχουν ανεπιθύμητες επιπτώσεις, όπως παρεμπόδιση των τηλεοπτικών εκπομπών, επηρεασμό των τηλεπικοινωνιών ή ακόμα και παρεμβολή του συστήματος εναέριας κυκλοφορίας. Για το λόγο αυτό, πολλές χώρες έχουν αυστηρούς κανονισμούς περί παρεμβολών και απαγορεύουν αυστηρά την χρήση τέτοιων τεχνολογιών στο κοινό. Για παράδειγμα, η Ομοσπονδιακή Επιτροπή Επικοινωνιών των

Ηνωμένων Πολιτειών απαγορεύει αυστηρά τη χρήση οποιουδήποτε συστήματος παρεμβολών σημάτων RF από πολίτες , ενώ το Γραφείο Επικοινωνίας του Ηνωμένου Βασιλείου περιορίζει επίσης τις παρεμβολές που εμποδίζουν τις ραδιοεπικοινωνίες . Πολλές χώρες παρέχουν κατευθυντήριες οδηγίες για τη χρήση παρεμβολών, αλλά υπάρχουν αυστηροί νομικοί περιορισμοί. Έτσι, σχεδόν καμία πρακτική τεχνολογία παρεμβολών δεν είναι διαθέσιμη για μη στρατιωτική χρήση.

9.5. Αμυντικά Drone -Killer Drones

Ο όρος "killer drone" αναφέρεται σε νόμιμα UAV drones που ανιχνεύουν και προσπαθούν να προκαλέσουν ζημιές σε στόχους drones . Τα "killer drones" απαιτούν γρήγορη και πραγματικού χρόνου λήψη αποφάσεων σχετικά με τα εισερχόμενα drones, ακριβή εκτίμηση της πορείας πτήσης των drones και εξαιρετική φυσική ανθεκτικότητα και κινητικότητα . Η χρήση drones για την πρόκληση ζημιών σε παράνομα drones αποτελεί τεχνολογία που βρίσκεται σε πολύ πρώιμο στάδιο και απαιτεί ακόμα χρόνο για να υιοθετηθεί σε μη στρατιωτικά συστήματα αντι-drone. Η ομαδοποίηση των "killer drones" με τεχνιτή νοημοσύνη και ακριβή συστήματα παρακολούθησης μπορεί να αποτελέσει μια ελπιδοφόρα λύση για πολύπλευρες επιθέσεις από σμήνη (Swarm) drones. Όπως και με το jamming και τα ραντάρ, η χρήση "killer drones" υπόκειται σε κανονιστικούς περριορισμούς .

9.6. Drone με εκτοξευτές διχτυών (Drone Net Capture)

Οι προσεγγίσεις κατάσχεσης κακόβουλης χρήσης drone συνδέονται φυσικά με τον στόχο drone με διάφορα εργαλεία, συνήθως με δίχτυ ή παρόμοια μη στρατιωτικά εργαλεία ως όπλα. Τα συστήματα κατάσχεσης drones διακρίνονται σε δύο ομάδες, ανάλογα με τον μηχανισμό κατάσχεσης.

Στα συστήματα κατάσχεσης επίγειας διάταξης που χειρίζονται από ανθρώπους ή τοποθετούνται σε οχήματα και είναι διαθέσιμα σε μεγάλη ποικιλία μεγεθών διχτυών και αριθμού βολών.

Στα εναέρια συστήματα κατάσχεσης που είναι εγκατεστημένα σε αμυντικά drones, με περιορισμούς στον αριθμό και το μέγεθος των ριπτόμενων διχτυών.Τα συστήματα αυτά μπορεί να συνοδεύοντα και με σύστημα ανοίγματος μικρού αλεξιπτώτου για την μη απότομη πτώση του συλληφθέντος drone. Η κατάσχεση από αέρος παρέχει πολύ μεγαλύτερη ακρίβεια και ταχύτητα από την επίγεια κατάσχεση λόγω της κινητικότητας των drones, αλλά οι υψηλές απαιτήσεις για ακρίβεια και ταχύτητα παρακολούθησης αυξάνουν ταυτόχρονα και τον κίνδυνο αποτυχίας της αποτροπής.

Τα συστήματα επίγειας κατάσχεσης πρέπει να λάβουν υπόψη την κάλυψη κάθε διαφορετικής κατηγορίας drone και τα βέλτιστα σημεία για ασφαλή κατάσχεση και πτώσης. Επιπλέον, η στρατηγική βελτίωσης είναι να αυξηθεί η αποτελεσματική εμβέλεια των συστημάτων αυτών, η οποία έχει μια καλύτερη ισορροπία μεταξύ του κόστους και της απόδοσης από την περίπτωση της uav drone κατάσχεσης. Από την άλλη πλευρά, οι συσκευές εναέριων κατάσχεσης έχουν μεγαλύτερη αντιστάθμιση μεταξύ του βάρους και της απόδοσης λόγω του περιορισμένου φορτίου των drones. Επιπλέον, το εναέριο σύστημα κατάσχεσης λαμβάνει κυρίως υπόψη την ιχνηλασιμότητα του ίδιου του drone την πτητική απόδοση και τη στρατηγική σχηματισμού σε περίπτωση σμήνους από drones.

Καθώς ο μηχανισμός ανίχνευσης των εχθρικών drones βασίζεται στα χαρακτηριστικά της λειτουργίας τους, η αποτροπή των drones εκμεταλλεύεται επίσης αυτά τα χαρακτηριστικά και προσπαθεί να διακόψει τη λειτουργία τους. Είναι προτιμότερο να προετοιμάζονται πολλές μορφές αποτροπής ως ένα πακέτο και να αυξάνεται το ποσοστό επιτυχίας. Επιπλέον, το σύστημα αντι-drone πρέπει να είναι σε θέση να επιλέγει την σωστή μέθοδο αποτροπής, λαμβάνοντας υπόψη την εμβέλεια του συστήματος και την εκτιμώμενη διαδρομή πτήσης και σημείου πτώσης μετά την κατάριψη.

10. Ζητήματα Αντιμετώπισης Τεχνολογιών Ακύρωσης Αντί-Drone Μέτρων

Οι προσεγγίσεις των παράνομων drones για την αποφυγή ανίχνευσης από τα αντι-drone συστήματα περιλαμβάνουν την παραπλάνηση των αισθητήρων ανίχνευσης μέσω την ελαχιστοποίηση των χαρακτηριστικών του πλαισίου τους(ίχνους στο ραντάρ). Αυτές οι προσεγγίσεις αναφέρονται επίσης ως τεχνικές stealth-mode (απόκρυψης) των drones . Οι περισσότερες τεχνικές stealth επικεντρώνονται στη μείωση της ανιχνευσιμότητας RCS (Radar Cross Section) του πλαισίου. Ήδη, ορισμένα μικρο-UAV είναι σχεδόν μη ανιχνεύσιμα σε επαρκή απόσταση, επιτρέποντας την υποκλοπή πληρφοριών ή την κατασκοπεία απόρρητων στρατιωτικών εγκαταστάσεων. Εάν το drone είναι εξοπλισμένο με μονάδες κρυπτογράφησης, οι σαρωτές ραδιοσυχνοτήτων μπορεί να μην ανιχνεύουν το είδος του κινδύνου ή ακόμα και την προσέγγισή του. Ένας σμήνος drones μπορεί να δημιουργήσει ένα υψηλής ασφάλειας δίκτυο χρησιμοποιώντας προηγμένους μικροϋπολογιστές (τύπου raspberry pi) και έξυπνα συστήματα ασφαλείας , τα οποία είναι αδύνατο να εντοπιστούν σύντομα με αποτέλεσμα να ολοκληρωθεί η εισβολή και το πιθανό χτύπημα των drones. Οι σαρωτές ραδιοσυχνοτήτων μπορεί να είναι παλαιότερης τεχνολογίας και να μην είναι ικανοί να αντιμετωπίσουν τα συστήματα κρυπτογράφησης ή να απαιτούνται συσκευές κβαντικής υπολογιστικής. Τα αθόρυβα σχεδιασμένα drones είναι ικανά για αποφυγή της ακουστικής ανίχνευσης, όπου συγκεκριμένοι σχηματισμοί των drones μπορούν σημαντικά να μειώσουν την ακρίβεια ανίχνευσης από κάμερες, καθώς τα συστήματα όρασης βασίζονται στο σχήμα για την αναγνώριση των drones. Η τεχνολογία ανίχνευσης των απειλητικών drones αντιμετωπίζει την πρόκληση της γρήγορης εξέλιξης των drones σε ό,τι αφορά το μέγεθος, την ταχύτητα, το σχήμα και τον θόρυβο.

Οι υφιστάμενες λύσεις ανίχνευσης παρουσιάζουν περιορισμένη αποτελεσματικότητα στην αντιμετώπιση της εισβολής των drones. Αντίθετα, ο συνδυασμός με πυκνά και εκτεταμένα δίκτυα αναγνώρισης των drones μπορεί να αποτελέσει μια καλύτερη προσέγγιση για τον προσδιορισμό εάν το uav είναι απειλητικό ή όχι. Αυτό σημαίνει ότι στα σύστημα ανίχνευσης πρέπει να παρακολουθείται ιδιαίτερα οι μεγάλες κατηγορίες uav, ανεξάρτητα από τα χαρακτηριστικά τους, και να επιτρέπει στο σύστημα αναγνώρισης να αποφασίσει εάν πρέπει να αντιμετωπιστούν.

11. Αποφυγή Εξουδετέρωσης Drone

Υπάρχουν πολλές τεχνικές για την αντιμετώπιση των αντι-drone συστημάτων , με αποτέλεσμα να υπάρχει και μεγάλη ποικιλία στις λύσεις. Η αντιμετώπιση των παρεμβολών είναι μια συμπληρωματική λύση για τα συστήματα από τα εχθρικά drones. Πολλά drones μπορούν να λειτουργήσουν αυτόνομα, και η μη ανάγκη συνεχής επικοινωνίας και της σύνδεσης μεταξύ του εισβολέα drone και του χειριστή του μπορεί να αποτρέψει πολλές από τις μεθόδους των αντι-drone τεχνολογιών και τις προσπάθειες τους για απόκτηση εμπιστευτικών πληροφοριών. Επίσης η αποφυγή των περιορισμών μέσω αδειοδοτημένων ζωνών των drones μπορεί να είναι αναποτελεσματική με ιδιοκατασκευές drones που χρησιμοποιούν τροποποιημένο λογισμικό . Οι μη καταστροφικές αντι-drone μέθοδοι προϋποθέτουν συνήθως γνώση του τρόπου λειτουργίας των ανιχνευμένων drones, όπως τα πρωτόκολλα που χρησιμοποιούνται και γνώση για το εάν ένα drone λειτουργεί σε αυτόνομη πτήση.

Το hijacking λειτουργεί μόνο για χειροκίνητα ελεγχόμενα drones και είναι αναποτελεσματική έναντι των αυτόνομων drones. Επίσης, ενώ η πλαστογράφηση(spoofing) μπορεί να παραπλανήσει ή να μπερδέψει τα drones, η πλοήγηση με βάση την όραση , μπορεί να αποφύγει την πλαστογράφηση του GPS του. Οι καταστροφικές μέθοδοι, όπως η επίθεση σε εχθρικά drones ή η κατάσχεση με χρήση αμυντικών drones, έχουν μεγάλη δυνατότητα να εξουδετερώσουν τα εχθρικά drones, αλλά μπορεί να αντιμετωπίσουν προκλήσεις όταν πρέπει να λειτουργήσουν σε υψηλή ταχύτητα .

Συνεπώς, τα συστήματα καταπολέμησης των μη επανδρωμένων drone πρέπει να αναπτύσσουν ολοκληρωμένες, αποτελεσματικές και ακριβείς στρατηγικές απόκρισης έναντι των επιθετικών drones

Επίσης ο τεχνολογικός ανταγωνισμός μεταξύ των βιομηχανιών drone και αντί-drone συστημάτων προκαλεί ταχεία ανάπτυξη νέων προϊόντων νικώντας την αντίθετη πλευρά των συστημάτων αυτών. Έτσι, τα αποτελεσματικά συστήματα anti-drone πρέπει να είναι ικανά για συνεχείς ενημερώσεις (updates και upgrades), πράγμα που σημαίνει ότι τα εξαρτήματα τους πρέπει να αντικαθίστανται εύκολα και να είναι συμβατά και με κοινή αρχιτεκτονική. Η τυποποίηση εξαρτημάτων του συστήματος anti-drone είναι απαραίτητη, όπως μια μορφή

αρχιτεκτονικής υψηλού επιπέδου , για να επιτρέψει στους προηγμένους σχεδιασμούς εξαρτημάτων να αξιολογηθούν γρήγορα και να υιοθετηθούν στο πραγματικό περιβάλλον.

12. Ασφαλές Κανάλι Παρεμβολών (Safe Channel in Jamming)

Λόγω των τεχνικών δυσκολιών που αντιμετωπίζουν άλλες μέθοδοι εξουδετέρωσης, η παρεμβολή σήματος παραμένει η τελευταία αμυντική γραμμή κατά των εχθρικών drones. Προκειμένου να μειωθεί ο κίνδυνος της απειλής ,και να διασφαλιστεί η λειτουργία ενός αντι-drone συστήματος ,καθώς και να αυξηθεί ασφάλεια των προστατευόμενων εγκαταστάσεων, απαιτείται η διαθεσιμότητα ενός ασφαλούς καναλιού επικοινωνίας για τις αμυνόμενες πλευρές, γνωστού ως "Ασφαλές κανάλι" (Safe channel). Το ασφαλές κανάλι μπορεί να δημιουργηθεί μέσω της εκμετάλλευσης της χαμηλής ζώνης του ελεγχόμενου φάσματος ή με τη χρήση άλλων μέσων, όπως το ορατό φως ή το ακουστικό σήμα .

Συνοψίζοντας σχετικά με την ανίχνευση των drones ,οι σύγχρονες λύσεις ανίχνευσης εξασφαλίζουν ένα συγκεκριμένο επίπεδο ακρίβειας στην ανίχνευση των drones, συνδυάζοντας πολλαπλά συστήματα ανίχνευσης. Κάθε μέθοδος έχει περιορισμούς απόδοσης όσον αφορά την εμβέλεια ανίχνευσης, τη λειτουργικότητα, την επίδραση των καιρικών συνθηκών κ.λπ. Συνεπώς, η βιομηχανία αντι-drone συστημάτων τάσσεται προς την ανάπτυξη υβριδικών συστημάτων ανίχνευσης. Οι κατασκευαστές αναλύουν την περιοχή άμυνας για να σχεδιάσουν βέλτιστα συστήματα ανίχνευσης και να βελτιώσουν την αποτελεσματικότητα της ανίχνευσης των drones. Το σύστημα ανίχνευσης πρέπει να συνδέεται στενά με δίκτυα αναγνώρισης των drones προσφέροντας μια αποτελεσματική λύση για την παρακολούθηση και εξουδετέρωση των drones.

Επίσης, λαμβάνοντας υπόψη τις τρέχουσες επιδόσεις στην τεχνολογία ανίχνευσης και τις ικανότητες των drones, κάθε μηχανισμός πρέπει να βελτιωθεί σε εμβέλεια και ακρίβεια για την παρακολούθηση των drones με προηγμένες δυνατότητες stealth-mode πτήσης. Επιπλέον, η τεχνολογία συνδυασμού αισθητήρων πρέπει να αντισταθμίζει τα ελαττώματα κάθε μεθόδου, με την αποδοτικότητα σε σχέση με το κόστος .Η συνύπαρξη σχεδιαστών hardware και προγραμματιστών software μπορεί να οδηγήσει στην τεχνολογική πρόοδο στα συστήματα ανίχνευσης drone.

13. Επιχειρησιακή αξιοποίηση Αντί-Drone Συστημάτων-Μέθοδοι Λειτουργίας

Η επιχειρησιακή αξιοποίηση αντι-Drone (UAV) συστημάτων αναφέρεται στη χρήση τέτοιων μεθόδων για να ανιχνεύσουν, παρακολουθήσουν, αποτρέψουν ή εξουδετερώσουν ανεπιθύμητες δραστηριότητες με drones. Αυτά τα συστήματα σχεδιάζονται για να αντιμετωπίσουν τις απειλές που μπορεί να προκαλέσουν drones, όπως παραβίαση

αεροδρομίων, κρίσιμων υποδομών, προσωπικής ιδιωτικότητας ή ακόμη και ανθρώπινης ασφάλειας.

Τα αντί-drone συστήματα αποτελούνται όπως αναφέρθηκε συνήθως από ποικίλα εξειδικευμένα εργαλεία και τεχνολογίες που συνδυάζουν την ανίχνευση, την αναγνώριση και την αντίδραση σε ανεπιθύμητες δραστηριότητες με drones. Αυτές οι τεχνολογίες μπορεί να περιλαμβάνουν ραντάρ, οπτικές κάμερες, θερμικές κάμερες, αισθητήρες λέιζερ, συστήματα αναγνώρισης ήχου, κεραίες επέκτασης και ειδικό λογισμικό επεξεργασίας δεδομένων. Με την χρήση αυτών των συστημάτων, οι φορείς ασφαλείας και οι οργανισμοί μπορούν να ανιχνεύουν την παρουσία drones, να παρακολουθούν την κίνησή τους και να λαμβάνουν μέτρα για την αποτροπή των απειλών που μπορεί να προκαλέσουν.

Η επιχειρησιακή αξιοποίηση αντι- drone συστημάτων είναι κρίσιμη για πολλούς τομείς, όπως οι στρατιωτικές εγκαταστάσεις, τα αεροδρόμια, οι επιχειρήσεις ασφαλείας, οι κρατικοί θεσμοί και οι εκδηλώσεις μαζικής συγκέντρωσης. Με την αύξηση της χρήσης των drones και την εμφάνιση νέων απειλών, η ανάπτυξη και η βελτίωση των αντι- drone συστημάτων αποτελούν σημαντική προτεραιότητα για την ασφάλεια και την προστασία. Ακολουθούν αναλυτικότερα οι τεχνικές αυτές και ο τρόπος λειτουργίας τους.

13.1. Διακοπή μετάδοσης πληροφορίας drone (από/προς Controller βάσης του ή τηλεχειριστηρίου)

Η διακοπή της μετάδοσης πληροφορίας από ή προς τον ελεγκτή (controller) ενός drone μπορεί να επιτευχθεί με διάφορους τρόπους, ανάλογα με τις δυνατότητες του συστήματος και της επιθυμητές αποτελεσματικότητας και του επιλεγμένου επιπέδου επέμβασης. Ορισμένοι τρόποι που χρησιμοποιούνται για τη διακοπή της μετάδοσης περιλαμβάνουν:

1)Αναίρεση του σήματος: Μια επιλογή είναι να αναιρεθεί ή να παρεμποδιστεί το σήμα επικοινωνίας μεταξύ του ελεγκτή και του drone. Αυτό μπορεί να γίνει μέσω της χρήσης διαφορετικών τεχνολογιών κεραιών , με συστήματα απομόνωσης σήματος ή με χρήση ηλεκτρομαγνητικών παρεμβολών.

2)Κατάργηση της επικοινωνίας: Μια άλλη προσέγγιση είναι να διακοπεί η επικοινωνία μεταξύ του ελεγκτή και του drone, ώστε να αποτραπεί η μετάδοση των εντολών και των δεδομένων. Αυτό μπορεί να γίνει μέσω της ανάμειξης στο σήμα επικοινωνίας ή της επιβολής εμποδίων στη μετάδοση των σημάτων.

3)Ανάλυση πληροφοριών: Μια άλλη προσέγγιση είναι να αναλύονται οι πληροφορίες που μεταδίδονται μεταξύ του ελεγκτή και του drone και να αναγνωρίζονται τα συγκεκριμένα μοτίβα ή εντολές που αφορούν τη λειτουργία του drone και στη συνέχεια, να

παρεμποδίζονται, να παρεμβάλλονται ή να αντικαθίσταται αυτές οι πληροφορίες για να αλλοιωθεί η επικοινωνία και η λειτουργία του drone.

13.2. Αδρανοποίηση / χειραγώγηση UAV

Η αδρανοποίηση ή χειραγώγηση ενός drone αναφέρεται στη διαδικασία απενεργοποίησης ή έλεγχος των λειτουργιών ενός drone από απόσταση. Υπάρχουν διάφοροι τρόποι για να αδρανοποιηθεί ή να χειραγωγηθεί ένα UAV, και αυτοί εξαρτώνται από την τεχνολογία και τα μέσα που χρησιμοποιούνται. Ορισμένες από τις κύριες μεθόδους περιλαμβάνουν:

1)Επιλογή συχνότητας: Τα περισσότερα drones λειτουργούν σε συγκεκριμένες συχνότητες επικοινωνίας για τη μετάδοση εντολών και λήψη δεδομένων. Μια μέθοδος αδρανοποίησης είναι η χρήση συστημάτων αποκοπής σήματος για να εμποδίσουν την επικοινωνία μεταξύ του ελεγκτή και του drone, αποτρέποντας έτσι τη λειτουργία του.

2)Ανάμειξη σήματος: Μια άλλη μέθοδος αδρανοποίησης είναι η ανάμειξη ή η παρεμβολή στο σήμα επικοινωνίας του drone, προκαλώντας παρεμβολές και διαταραχές που επηρεάζουν την επικοινωνία και τη λειτουργία του.

3)Κατάργηση ενέργειας: Μια πιο άμεση μέθοδος αδρανοποίησης είναι η κατάργηση της παροχής ενέργειας προς το drone. Αυτό μπορεί να επιτευχθεί με τη χρήση τεχνικών όπως η εκτόξευση εμποδίων που απενεργοποιούν το drone ή η χρήση EMP για την απενεργοποίηση των ηλεκτρονικών συστημάτων του.Ο ηλεκτρομαγνητικος παλμός (Electromagnetic Pulse -EMP) είναι ηλεκτρομαγνητικές παλμικές εκρήξεις που παράγονται από πυρηνικά ή υψηλής ισχύος ηλεκτρονικά συστήματα. Αυτές οι εκρήξεις απελευθερώνουν μια μεγάλη ποσότητα ηλεκτρομαγνητικής ενέργειας σε μια πολύ μικρή χρονική διάρκεια.

Ο EMP είναι ικανός να προκαλέσει σοβαρές διαταραχές σε ηλεκτρονικές συσκευές και συστήματα που βρίσκονται εντός της περιοχής επίδρασης του. Η ηλεκτρομαγνητική ακτινοβολία του EMP μπορεί να προκαλέσει ανεπανόρθωτες ζημιές ή απώλεια λειτουργικότητας σε ηλεκτρονικά στοιχεία, κυκλώματα και συστήματα, καθιστώντας τα ανίκανα να λειτουργήσουν σωστά.
Ο EMP μπορεί να προκληθεί από πυρηνικές εκρήξεις, υψηλής ισχύος ραδιοσυχνοτήτων (HPEM) και άλλες πηγές που παράγουν έντονα ηλεκτρομαγνητικά πεδία. Η χρήση EMP για την αδρανοποίηση drone είναι μέθοδος απενεργοποίησης των ηλεκτρονικών συστημάτων του drone, με αποτέλεσμα την απώλεια ελέγχου του και την αδυναμία μετάδοσης πληροφοριών από/προς τον χειριστή του.

13.3. Παραπλάνηση drone και Controller:

Η παραπλάνηση drone και controller αναφέρεται σε τεχνικές και μεθόδους που χρησιμοποιούνται για να παραβλέψουν, παραπλανήσουν ή αποκρούσουν τη λειτουργία ενός drone και του χειριστή του. Ο στόχος είναι να δημιουργηθεί σύγχυση ή απώλεια ελέγχου επί του drone, είτε με σκοπό την αποτροπή εχθρικών δραστηριοτήτων είτε για αντι-κατασκοπευτικούς σκοπούς.

Οι τεχνικές παραπλάνησης μπορεί να περιλαμβάνουν την εκπομπή ψευδών σημάτων ελέγχου ή επικοινωνίας για να αποπροσανατολίσουν το drone. Μπορεί επίσης να χρησιμοποιηθούν μέθοδοι όπως η εμφάνιση ψευδών σημάτων GPS ή η δημιουργία παρεμβολών στο φάσμα των επικοινωνιών για να αποτραπεί η σωστή λειτουργία του drone. Οι τεχνικές παραπλάνησης του ελεγκτή πτήσης(flight controller)στοχεύουν στην παρέμβαση στην επικοινωνία μεταξύ του ελεγκτή του drone, είτε αποκόπτοντας την επικοινωνία εντελώς είτε παραπλανώντας τον ελεγκτή για να λάβει λανθασμένες εντολές ή να μην ανταποκριθεί σωστά στις εντολές που δίνονται από τη βάση του.

13.4. Καταστροφή drone

Οι μέθοδοι καταστροφής drone περιλαμβάνουν:

1)Φυσική καταστροφή: Αυτή η μέθοδος περιλαμβάνει τη χρήση φυσικών μέσων όπως εκτοξευτήρες με δίχτυα, εκρήξεις ή εμπόδια για να απενεργοποιήσει ή να καταστρέψει το drone.

2)Κατάρριψη: Αυτή η μέθοδος περιλαμβάνει τη χρήση πυραύλων, εναέριων οχημάτων ή άλλων μέσων για να καταρρίφθεί ένα drone.

3)Ανίχνευση και απόκρουση: Αυτή η μέθοδος εστιάζει στην ανίχνευση του drone και στην διακοπή της πτήσης του με τη χρήση ειδικών συστημάτων ανίχνευσης και εξουδετέρωσης.

14. Μέθοδοι και Λειτουργίες Αντι-Drone Παθητικών Συστημάτων:

14.1. Παθητικός Εντοπισμός RF συχνοτήτων

Ο εντοπισμός RF εκπομπών που εκπέμπουν τα drones, όπως πληροφορίες τηλεμετρίας και δεδομένα λειτουργίας, με σκοπό τη διακοπή επικοινωνίας σε αντι-drone συστήματα, μπορεί να επιτευχθεί μέσω των παρακάτω μεθόδων:

1)Απευθείας περιορισμένης απόστασης τυπική επικοινωνία RF στα 2.4/5.8 GHz: Με τη χρήση συστημάτων εντοπισμού RF, μπορεί να ανιχνευθεί η παρουσία εκπομπών από drones σε περιορισμένη ακτίνα λειτουργίας, όπως τα κλασικά συχνότητας 2.4 GHz και 5.8 GHz που χρησιμοποιούνται για την επικοινωνία των drones με τον χειριστή.

2)Εντοπισμός επικοινωνίας κινητής τηλεφωνίας 4G/5G: Με τη χρήση κινητής τηλεφωνίας υψηλής ταχύτητας, όπως το 4G ή το 5G, μπορεί να παρακολουθηθεί η επικοινωνία των drones με τον χειριστή τους. Αυτή η μέθοδος επιτρέπει την ανίχνευση και τη διακοπή της επικοινωνίας μεταξύ του χειριστή και του drone, αποτρέποντας έτσι την ανεπιθύμητη λειτουργία του.

3)Εντοπισμός Custom RF επικοινωνιών: Ορισμένα drones μπορεί να χρησιμοποιούν προσαρμοσμένες μορφές RF επικοινωνίας. Για τον εντοπισμό και τη διακοπή αυτών των εκπομπών, απαιτούνται εξειδικευμένοι αισθητήρες και συστήματα ανίχνευσης που μπορούν να αναγνωρίσουν και να απομονώσουν τις προσαρμοσμένες συχνότητες.

Ο εντοπισμός των drones μπορεί να γίνει είτε με έναν μόνο αισθητήρα, που επιτρέπει την εύρεση της γενικής κατεύθυνσης του drone, είτε με πολλαπλούς αισθητήρες, που επιτρέπουν τον τριγωνισμό για τον εντοπισμό της θέσης του UAV και του χειριστή (Controller). Ο συνδυασμός περισσοτέρων αισθητήρων επιτρέπει την ακριβέστερη και πιο αξιόπιστο εντοπισμό των drones και των χειριστών τους.

Η υλοποίηση του συστήματος εντοπισμού για μεγαλύτερες απαιτούμενες αποστάσεις και ευρύτερα φάσματα εντοπιζόμενων συχνοτήτων απαιτεί αυξημένη ακρίβεια και περισσότερη πολυπλοκότητα (Απαιτούμενο εύρος παρακολουθούμενων συχνοτήτων: από 2 MHz έως 18 GHz). [11]

Όσο αυξάνεται η απαιτούμενη απόσταση εντοπισμού, τόσο πιο εξειδικευμένοι αισθητήρες και συστήματα ανίχνευσης απαιτούνται για να ανιχνεύσουν τα σήματα σε αυτήν τη μεγαλύτερη απόσταση. Επιπλέον, όσο αυξάνεται το φάσμα των εντοπιζόμενων συχνοτήτων, τόσο πιο πολύπλοκη γίνεται η υλοποίηση του συστήματος, καθώς απαιτούνται πιο ευρυζωνικοί αισθητήρες και περισσότερο προηγμένη τεχνολογία ακριβείας για την ανίχνευση και την ανάλυση των σημάτων σε αυτό το ευρύ φάσμα συχνοτήτων.

Συνεπώς, η υλοποίηση ενός συστήματος εντοπισμού με μεγαλύτερη απόσταση εντοπισμού και ευρύτερο φάσμα συχνοτήτων απαιτεί εξειδικευμένες τεχνολογικές λύσεις και αυξημένο κόστος, καθώς πρέπει να διασφαλιστεί η ακρίβεια και η αποτελεσματικότητα του συστήματος σε αυτές τις απαιτητικές συνθήκες.

14.2. Παθητικός Εντοπισμός UAV -Μέθοδος Passive RF UCAV Detector

Ο παθητικός εντοπισμός UAV με χρήση της μεθόδου Passive RF UCAV Detector βασίζεται στην ανίχνευση και ανάλυση των ραδιοσυχνοτήτων που εκπέμπονται από τα ασύρματα

επικοινωνιακά συστήματα των UAV (Unmanned Aerial Vehicles) ή UCAV (Unmanned Combat Aerial Vehicles) χωρίς τη χρήση ενεργών σημάτων παρεμβολής.

Η μέθοδος αυτή εκμεταλλεύεται το γεγονός ότι τα UAV εκπέμπουν συνήθως ραδιοσήματα για επικοινωνία με τον χειριστή τους ή για λήψη δεδομένων από αισθητήρες και συστήματα πλοήγησης. Οι παθητικοί αισθητήρες του συστήματος εντοπισμού καταγράφουν αυτά τα ραδιοσήματα και αναλύουν τα χαρακτηριστικά τους, όπως η συχνότητα, η ισχύς, το πλάτος και ο χρόνος διάρκειας.

Με βάση τα δεδομένα που συλλέγονται, ο παθητικός ανιχνευτής μπορεί να αναγνωρίσει τα ραδιοσήματα που σχετίζονται με τα UAV και να τα διαχωρίσει από τα υπόλοιπα σήματα που προέρχονται από άλλες πηγές, όπως κινητά τηλέφωνα ή άλλα ασύρματα συστήματα. Μέσω ανάλυσης των χαρακτηριστικών των εντοπισμένων ραδιοσημάτων, ο ανιχνευτής μπορεί επίσης να παράσχει πληροφορίες σχετικά με την κατεύθυνση και την απόσταση του UAV από τον αισθητήρα.

Ο παθητικός εντοπισμός UAV με τη χρήση της μεθόδου Passive RF UCAV Detector προσφέρει το πλεονέκτημα της απόκρυψης και της αποφυγής παρεμβολής στις επικοινωνίες των UAV, καθώς δεν απαιτεί την εκπομπή ενεργών σημάτων για τον εντοπισμό τους. Επίσης, η μέθοδος αυτή μπορεί να χρησιμοποιηθεί για την παρακολούθηση και τον εντοπισμό πολλαπλών UAV ταυτόχρονα.

Συνολικά, ο παθητικός εντοπισμός UAV με τη μέθοδο Passive RF UCAV Detector αποτελεί μια αποτελεσματική τεχνική για την ανίχνευση και τον εντοπισμό ασύρματων επικοινωνιών των UAV, παρέχοντας σημαντικές πληροφορίες για την αντιμετώπιση ανεπιθύμητων και επικίνδυνων εναέριων συσκευών.

14.3 **Παθητικός εντοπισμός UAV με χρήση οπτικού ανιχνευτή** UAV

Ο οπτικός ανιχνευτής χρησιμοποιεί ειδικούς οπτικούς αισθητήρες, cmos κάμερες, ψηφιακές πυξίδες, λέιζερ και θερμικές κάμερες, για να ανιχνεύσει την παρουσία των UAV στον αέρα. Οι αισθητήρες αυτοί είναι προσαρμοσμένοι για την ανίχνευση και τον εντοπισμό αεροσκαφών.

Ο οπτικός ανιχνευτής παρακολουθεί τον ορίζοντα του ουρανού ή την ευρύτερη περιοχή του ενδιαφέροντος, ανιχνεύοντας τυχόν κινούμενα αντικείμενα που πληρούν τα χαρακτηριστικά ενός UAV, όπως το σχήμα, το μέγεθος και η κίνηση. Με τη χρήση προηγμένων αλγορίθμων επεξεργασίας εικόνας και μηχανικής μάθησης, ο ανιχνευτής μπορεί να αναγνωρίσει την παρουσία ενός UAV και να εξάγει πληροφορίες όπως η θέση, η ταχύτητα και η κατεύθυνση του UAV. Η οπτική μέθοδος παρέχει τη δυνατότητα ανίχνευσης

και εντοπισμού UAV σε μεγάλες αποστάσεις, ανάλογα με την ανάλυση και τις δυνατότητες των οπτικών αισθητήρων

14.4 Παθητικός Εντοπισμός UAV με στερεοσκοπική σάρωση πεδίου με χρήση LIDAR Optical detector

Ο LIDAR αισθητήρας τοποθετείται σε μια θέση όπου μπορεί να σαρώσει το περιβάλλον προς όλες τις κατευθύνσεις. Με τη χρήση πολλαπλών παλμών, ο LIDAR πραγματοποιεί στερεοσκοπική σάρωση, καταγράφοντας τις αποστάσεις και τις θέσεις των αντικειμένων στο πεδίο όρασης. Με τη βοήθεια εξειδικευμένων αλγορίθμων επεξεργασίας δεδομένων, οι πληροφορίες που συλλέγονται από το LIDAR αναλύονται για τον εντοπισμό των UAV. Οι πληροφορίες αυτές περιλαμβάνουν την απόσταση του UAV από τον αισθητήρα, το ύψος του UAV και το σχήμα του. Με βάση αυτές τις πληροφορίες, είναι δυνατή η αναγνώριση και η παρακολούθηση του UAV. Ο παθητικός εντοπισμός UAV με στερεοσκοπική σάρωση πεδίου χρησιμοποιώντας LIDAR προσφέρει υψηλή ακρίβεια και αξιοπιστία στον εντοπισμό UAV.

14.5 Παθητικός Εντοπισμός UAV με ακουστικό ανιχνευτή

1)Ακουστική ανίχνευση: Ο ακουστικός ανιχνευτής αποτελείται από ένα δίκτυο ακουστικών αισθητήρων που τοποθετούνται σε στρατηγικά σημεία στο πεδίο δράσης. Οι αισθητήρες αυτοί καταγράφουν τους ήχους που παράγονται από τα UAV.

2)Ανάλυση των ήχων: Οι ήχοι που καταγράφονται από τους αισθητήρες αναλύονται για να εξαχθούν χαρακτηριστικά όπως η συχνότητα, η διάρκεια και η ένταση. Αυτά τα χαρακτηριστικά μπορούν να χρησιμοποιηθούν για την αναγνώριση των ήχων που παράγονται από τα UAV.

3)Ανίχνευση UAV: Με τη χρήση εξειδικευμένων αλγορίθμων και μοντέλων μηχανικής μάθησης, οι ήχοι που καταγράφονται αναλύονται για την ανίχνευση και τον εντοπισμό των ήχων που παράγονται από τα UAV. Με βάση τα χαρακτηριστικά των ήχων και τις πληροφορίες από τους αισθητήρες, είναι δυνατό να προσδιοριστεί η θέση και η κατεύθυνση του UAV.Ο παθητικός εντοπισμός UAV με ακουστικό ανιχνευτή προσφέρει τη δυνατότητα ανίχνευσης UAV χωρίς την ανάγκη ενεργοποίησης προηγμένων αισθητήρων ή ραντάρ.

15. Σημεία τρωτότητας των Drone και Ενεργητικός Εντοπισμός τους:

15.1. Soft-kill μέθοδοι αντιμετώπισης

Οι "soft-kill" μέθοδοι αντιμετώπισης αποσκοπούν στην αποτροπή ή απενεργοποίηση ενός drone ή του ελέγχου του από μια απομακρυσμένη αντι-drone πλατφόρμα, χωρίς να προκαλούν καταστροφή ή ζημία σε αυτό. Δύο από τις κύριες μεθόδους "soft-kill" αντιμετώπισης είναι ο αποπροσανατολισμός/απαγόρευση του drone φορέα αισθητήρων/όπλων και ο αποπροσανατολισμός/απαγόρευση του controller [10] .

1)Αποπροσανατολισμός/απαγόρευση drone φορέα αισθητήρων/όπλων: Αυτή η μέθοδος αποσκοπεί στον αποπροσανατολισμό ή την απαγόρευση της λειτουργίας των αισθητήρων ή των όπλων που είναι ενσωματωμένα στο drone. Αυτό μπορεί να γίνει μέσω ηλεκτρονικής παρεμβολής, που περιλαμβάνει την διακοπή της επικοινωνίας ή την παρεμπόδιση των σημάτων μεταξύ του drone και των αισθητήρων/όπλων, εμποδίζοντας την ορθή λειτουργία τους.

2)Αποπροσανατολισμός/απαγόρευση RC controller: Αυτή η μέθοδος στοχεύει στην αποπροσανατολισμό ή απαγόρευση του ελέγχου του drone από τον RC controller, δηλαδή τη συσκευή ή τον προγραμματισμένο σταθμό ελέγχου που χρησιμοποιείται για να διαχειριστεί και να κατευθύνει το drone. Αυτό μπορεί να γίνει μέσω της διακοπής ή παρεμπόδισης των σημάτων επικοινωνίας μεταξύ του drone και του controller, αποτρέποντας έτσι την αποτελεσματική χρήση και έλεγχο του drone.

Αυτές οι μέθοδοι "soft-kill" επιτρέπουν την αντιμετώπιση ενός drone χωρίς την ανάγκη για ρίψης ή καταστροφής του. Είναι χρήσιμες για την προστασία περιοχών ή εγκαταστάσεων χωρίς να προκαλούν μεγάλες επιπτώσεις ή κινδύνους.

Τα σημεία τρωτότητας των drone που επικεντρώνονται τα αντι-drone αυτά συστήματα είναι: Στις επικοινωνίες RF (Radio Frequency) ελέγχου / τηλεχειρισμού / τηλεμετρίας .Δηλαδή στη χρήση ραδιοκυμάτων για τη μετάδοση δεδομένων, ελέγχου, τηλεχειρισμού και τηλεμετρίας μεταξύ δύο ή περισσότερων συσκευών ή συστημάτων. Οι επικοινωνίες RF στις UAV περιλαμβάνουν συνήθως την χρήση ασύρματων συστημάτων δικτύου (Wireless Network Systems) και τηλεπικοινωνιακών πρωτοκόλλων για τη μετάδοση των δεδομένων. Οι πιο συνηθισμένες ασύρματες συχνότητες συνήθως είναι οι 2.4 GHz, 5.8 GHz, 433 MHz και υπάρχουν και άλλες, ανάλογα με τον τύπο του drone και των απαιτήσεων του συστήματος επικοινωνίας.

Οι επικοινωνίες RF ελέγχου/τηλεχειρισμού/τηλεμετρίας είναι κρίσιμης σημασίας για τη λειτουργία και τον έλεγχο των UAV, καθώς επιτρέπουν στον τηλεχειριστή να αποστέλλει εντολές, να λαμβάνει δεδομένα αισθητήρων και να παρακολουθεί την κατάσταση του UAV κατά τη διάρκεια της πτήσης.

Η διακοπή επικοινωνίες RF μετάδοσης βίντεο και δεδομένων και σε επικοινωνίες με δορυφορικά συστήματα για μετάδοση στοιχείων χρόνου/θέσεως, βίντεο και δεδομένων των drone επιτυγχάνεται με διαφορετικούς τρόπους:

Με απώλεια σήματος: Η μετάδοση RF μπορεί να επηρεαστεί από τις παρεμβολές, με μεθόδους πολλαπλής διαδρομής (multipath),με δημιουργία φυσικών εμποδίων με στόχο την απώλεια σήματος και πτώση της ποιότητας της μετάδοσης.

Με παρεμβολές: Με εκπομπή σήματος RF μπορεί να προκληθεί παρεμβολή στη μετάδοση RF του drone, περιορίζοντας έτσι την αξιοπιστία και την μετάδοση σημάτων βίντεο και δεδομένων.

Με παραβίαση στην ασφάλειας του Drone: Οι μεταδιδόμενες πληροφορίες μπορούν να είναι ευάλωτες σε παραβίαση ασφαλείας, απώλειας δεδομένων ή ακόμη και αποκρυπτογράφηση, ειδικά σε περιπτώσεις που δεν έχουν ληφθεί τα κατάλληλα μέτρα προστασίας και της κρυπτογράφησης.

15.1.1. Soft-Kill συστήματα

1) Παρεμβολείς (jammers) RF εκπομπών: (Απαίτηση παρεμβαλλόμενου φάσματος: από 2 MHz μέχρι 18 GHz)

Οι κύριες μέθοδοι παρεμβολής περιλαμβάνουν:

Περιορισμένης απόστασης τυπική επικοινωνία RF σε 2.4/5.8 GHz: Οι παρεμβολείς μπορούν να εκπέμψουν ισχυρά RF σήματα στις συχνότητες 2.4 GHz και 5.8 GHz, που ανατρέπουν ή διαταράσσουν την επικοινωνία των drones σε αυτά τα εύρη συχνοτήτων.

Επικοινωνία μέσω κινητής τηλεφωνίας 4G/5G: Οι παρεμβολείς μπορούν να δημιουργήσουν παρεμβολές στα δίκτυα κινητής τηλεφωνίας 4G και 5G, που χρησιμοποιούνται από τα drones για τη μετάδοση δεδομένων ή τηλεχειρισμό.

Custom RF επικοινωνίας: Οι παρεμβολείς μπορούν να σχεδιαστούν για να παρεμβάλλουν σε ειδικές συχνότητες ή πρωτόκολλα επικοινωνίας που χρησιμοποιούνται από τα drones, ανατρέποντας ή διαταράσσοντας την επικοινωνία τους.

GNSS (GPS, GLONASS, Galileo κλπ): Οι παρεμβολείς μπορούν επίσης να εκπέμψουν παραπλανητικά σήματα GNSS (Global Navigation Satellite System), όπως GPS, GLONASS, Galileo κλπ, που χρησιμοποιούνται από τα drones μέσω του αισθητήρα για τον καθορισμό της θέσης τους. Αυτό μπορεί να οδηγήσει σε απώλεια ή παραπλάνηση του σήματος θέσης και να περιορίσει την ικανότητα των drones να λειτουργούν σωστά.

2) Spoofing**:** Με τη χρήση τεχνικών spoofing στα δορυφορικά συστήματα χρόνου/θέσης (GNSS). Αυτή η μέθοδος στοχεύει στη μίμηση του γνήσιου σήματος που παράγεται από τους δορυφόρους GNSS, με σκοπό την παραπλάνηση των κυκλωμάτων ανίχνευσης του δέκτη GNSS και την χειραγώγηση του drone.

Συγκεκριμένα, η διαδικασία του spoofing περιλαμβάνει την εκπομπή παραπλανητικών σημάτων GNSS που μοιάζουν με τα γνήσια σήματα που εκπέμπονται από τους δορυφόρους. Αυτά τα παραπλανητικά σήματα κατευθύνονται προς τον δέκτη GNSS του εισβολέα-drone , και εισέρχονται στα tracking loops του δέκτη του. Οι tracking loops είναι υπεύθυνοι για την αποκωδικοποίηση και την ακριβή παρακολούθηση των γνήσιων σημάτων GNSS. Με τη μίμηση των γνήσιων σημάτων, τα παραπλανητικά σήματα εισάγονται στα tracking loops και επηρεάζουν τη λειτουργία του δέκτη GNSS.

Για να επιτευχθεί αποτελεσματική παραπλάνηση, απαιτείται η χρήση κατά το λιγότερο "N-1" αριθμού κεραιών GNSS spoofing, όπου "N" είναι ο αριθμός των κεραιών GNSS που χρησιμοποιεί το UAV. Αυτό επιτρέπει την εξασφάλιση μίας πιο αξιόπιστης παραπλάνησης, καθώς επηρεάζονται όλες οι κεραίες του δέκτη GNSS.

Η μέθοδος αυτή επιτρέπει την παρεμπόδιση της σωστής λειτουργίας των drones που εξαρτώνται από την ακρίβεια των σημάτων GNSS για τον καθορισμό της θέσης και τον συγχρονισμό τους. Με το spoofing, οι επιτιθέμενοι μπορούν να παραπλανήσουν τα drones και UAVs, οδηγώντας τα να αλλάξουν τη θέση τους, να αποκτήσουν λανθασμένες πληροφορίες θέσης ή ακόμη και να χάσουν τη σύνδεσή τους με τον χειριστή τους. Αυτό μπορεί να επηρεάσει τις επιχειρησιακές τους δυνατότητες και να προκαλέσει αστάθεια στη λειτουργία τους και απομάκρυνση από την πορεία τους.

3) Παρεμβολείς δορυφορικών συστημάτων επικοινωνίας/ελέγχου/μεταφοράς δεδομένων στα UAV): Οι παρεμβολείς δορυφορικών συστημάτων επικοινωνίας/ελέγχου/μεταφοράς δεδομένων αποτελούν συσκευές που χρησιμοποιούνται για το παρεμπόδιση ή τον περιορισμό της λειτουργίας δορυφορικών συστημάτων που χρησιμοποιούνται από UAVs. Αυτοί οι παρεμβολείς είναι συνήθως σχεδιασμένοι για να εκπέμπουν ισχυρά ηλεκτρομαγνητικά σήματα στη συχνότητα K-Band, που αντιστοιχεί σε μια συχνότητα λειτουργίας περίπου 18-27 GHz.

Οι παρεμβολείς δορυφορικών συστημάτων επικοινωνίας/ελέγχου/μεταφοράς δεδομένων εκπέμπουν ισχυρά σήματα jamming στη συχνότητα των δορυφόρων επικοινωνιών K-Band. Τα σήματα jamming αναμειγνύονται με τα γνήσια σήματα που εκπέμπονται από τους δορυφόρους, καθιστώντας δυσκολότερη ή αδύνατη την αποτελεσματική λήψη και αποκωδικοποίηση των σημάτων από τα UAVs.

Η ισχύς εξόδου των παρεμβολέων δορυφορικών συστημάτων μπορεί να φτάσει τα 300 watt, και η εμβέλειά τους μπορεί να φτάσει τα 30-35 χιλιόμετρα. Αυτό σημαίνει ότι μπορούν να επηρεάσουν τη λειτουργία των δορυφορικών συστημάτων που

χρησιμοποιούνται από UAVs σε μεγάλες αποστάσεις.Ο παρεμβολέας δημιουργεί θόρυβο και παραπλανητικά σήματα στη συχνότητα επικοινωνίας των δορυφορικών συστημάτων, καθιστώντας δυσκολότερη την αξιόπιστη επικοινωνία και ελέγχο των UAVs. Αυτό μπορεί να προκαλέσει απώλεια της σήματος, μη ακριβείς πληροφορίες θέσης, μη αποτελεσματική ανταπόκριση σε εντολές και γενικότερα προβλήματα στη λειτουργία των UAVs.

Η χρήση παρεμβολέων δορυφορικών συστημάτων αποτελεί μια από τις τεχνικές που χρησιμοποιούνται για την αντιμετώπιση και αποτροπή των UAVs σε ευαίσθητες περιοχές ή σε περιπτώσεις παραβίασης αεροδιαστημικού χώρου.

4) Πομποί ηλεκτρομαγνητικού παλμού υψηλής ισχύος): Αυτοί οι πομποί είναι σχεδιασμένοι για να εκπέμπουν ισχυρούς ηλεκτρομαγνητικούς παλμούς σε ειδικές συχνότητες και φάσματα που μπορούν να επηρεάσουν τη λειτουργία των UAVs.

Η λειτουργία των πομπών ηλεκτρομαγνητικού παλμού βασίζεται στην απελευθέρωση μιας υψηλής ισχύος ηλεκτρομαγνητικής ενέργειας μέσω μιας κεραίας - πηνίου. Αυτή η ενέργεια μεταδίδεται σε συγκεκριμένες συχνότητες και μπορεί να επηρεάσει ή και να καταστρέψει τα ηλεκτρονικά συστήματα των UAVs, όπως τους δέκτες επικοινωνίας, τους αισθητήρες, τα συστήματα πλοήγησης και άλλα.

Οι πομποί ηλεκτρομαγνητικού παλμού υψηλής ισχύος μπορούν να προκαλέσουν παρεμβολές στα σήματα επικοινωνίας και πλοήγησης των UAVs, καθιστώντας την επικοινωνία με τον χειριστή του UAV ανέφικτη, αλλοιώνοντας τις πληροφορίες θέσης ή προκαλώντας πλήρης απώλεια της ελέγχου του UAV. Αυτό μπορεί να οδηγήσει σε αναγκαστική προσγείωση ή και πτώση του UAV. Χρησιμοποιούνται συνήθως σε περιπτώσεις αδρανοποίησης σμήνους εισβολέων - αυτοκτονικών drones που βρίσκονται στην τελευταία φάση προσέγγισης του στόχου.

5) Οπτικοί σαρωτές Dazzlers (Laser Dazzlers): Αυτές οι συσκευές χρησιμοποιούν έναν ισχυρό λέιζερ για να δημιουργήσουν έναν οπτικό αποπροσανατολισμό που μπορεί να επηρεάσει τους αισθητήρες του UAV και να περιορίσει την ικανότητά του να λειτουργεί αποτελεσματικά.Οι οπτικοί τυφλωτές Dazzlers λειτουργούν εκπέμποντας μια ισχυρή δέσμη λέιζερ προς το UAV. Η δέσμη αυτή μπορεί να είναι ορατή για το UAV ή να περιλαμβάνει οπτικές συχνότητες που είναι ευαίσθητες για τους αισθητήρες του. Όταν η δέσμη λέιζερ προσπίπτει στο drone, μπορεί να προκαλέσει προσωρινή απώλεια οπτικής αναγνώριση στους οπτικούς αισθητήρες του, εμποδίζοντας την σωστή λειτουργία και την ανίχνευση του περιβάλλοντος.

15.2. Hard-kill μέθοδοι για αντιμετώπιση Drone

Δηλαδή με καταστροφή του φορέα αισθητήρων ή ολόκληρου του drone . Οι "hard-kill" μέθοδοι αντιμετώπισης των drone αναφέρονται σε τεχνικές που στοχεύουν στην φυσική καταστροφή ή πλήρης απενεργοποίηση των drone. Αυτές οι μέθοδοι περιλαμβάνουν τη χρήση εξειδικευμένων συσκευών και τεχνολογιών για να απενεργοποιήσουν ή να καταρρίψουν τα drone Κύριες "hard-kill" μέθοδοι αποτελούν :

1)Κατάρριψη με ρουκέτες ή πυρομαχικά: Σε ορισμένες περιπτώσεις, όπου η επίθεση απαιτεί άμεση και αποτελεσματική αντίδραση, μπορούν να χρησιμοποιηθούν εξειδικευμένα όπλα για να καταρρίψουν τα τρομορατικά drone. Αυτές οι μέθοδοι συνήθως εφαρμόζονται από στρατιωτικές ή αστυνομικές δυνάμεις.

2)Επίθεση με μικροκύματα: Οι μικροκυματικές επιθέσεις μπορούν να χρησιμοποιηθούν για την ανατίναξη των ηλεκτρονικών συστημάτων των drone. Αυτό μπορεί να προκαλέσει την απώλεια της συνδεσιμότητας, την απενεργοποίηση του ελέγχου ή ακόμη και την πλήρη κατάρρευση του drone.

3)Επίθεση με λέιζερ(Laser Guns): Οι επιθέσεις με λέιζερ μπορούν να στοχεύσουν στα συστήματα ελέγχου των drone ή στα μηχανικά τους στοιχεία, όπως οι έλικες ή οι κινητήρες. Αυτό μπορεί να προκαλέσει ανάπτυξη μεγάλης θερμοκρασίας ή και ανάφλεξη προκαλώντας δυσλειτουργία ή και πλήρη καταστροφή του drone.

4)Εκτοξευόμενα δίχτυα(shooting nets): Αυτή η τεχνολογία χρησιμοποιείται για να αιφνιδιάσει και να αποκλείσει φυσικά τα drones μέσω της εκτόξευσης ειδικά σχεδιασμένων διχτών προς την κατεύθυνση του drone εισβολέα .Οι εκτοξευτήρες διχτυών είναι εφοδιασμένοι με μηχανισμούς εκτόξευσης που επιτρέπουν την ακριβή και γρήγορη απελευθέρωση των διχτών. Μόλις εκτοξευτούν, τα δίχτυα απλώνονται , αγκαλιάζουν και σχηματίζουν ένα φυσικό εμπόδιο που εμποδίζει την πτήση την πορεία του εισβολέα drone. Οι βολές αυτές τον διχτυών συνήθως συνοδεύονται και με μια μικρή συσκευή που απελευθερώνει ένα μικρό αλεξίπτωτο και οδηγεί καθοδικά το UAV στο έδαφος χωρίς να το καταστρέψει εάν είναι αυτός ο σκοπός.

5) Anti-UAVs σε ρόλο κυνηγού εισβολέων UAVs (Drone hunter-killer) εξοπλισμένα με μικρούς πυραύλους. Αυτοί οι "κυνηγοί-εξολοθρευτές" UAVs μπορούν να είναι εξοπλισμένοι με διάφορους αισθητήρες και συστήματα όπως ραντάρ, οπτικούς αισθητήρες, θερμικές κάμερες, λέιζερ, ηλεκτρονικά συστήματα κατάλληλα για πυροβολισμό. Μπορούν να ανιχνεύουν τα εχθρικά UAVs που λειτουργούν στον ίδιο εναέριο χώρο και να προβαίνουν σε επιθέσεις για να τα απενεργοποιήσουν ή να τα καταστρέψουν. Πρόκειται δηλαδή για εναέρια αντι-drone συστήματα.

Σε πολλές περιπτώσεις, η αποτελεσματική αντιμετώπιση των drone γίνεται μέσω της συνδυασμένης χρήσης "hard-kill" και "soft-kill" τεχνικών, όπως η ανίχνευση και η

αποκλεισμός των σημάτων επικοινωνίας των drone. Επιπλέον ένα σημαντικό κριτήριο επιλογής μεθόδου αντιμετώπισης εισβολέων drone είναι να μην ξοδεύουμε περισσότερα από τον αντίπαλο.

16. Πρωτόκολλα Επικοινωνίας των Drones

Για να είναι δυνατή η ανίχνευση από τα αντι-drone συστήματα καθώς και η παραπλάνηση μέσω ψευδών πακέτων επικοινωνίας των drone που λειτουργούν σε σμήνος είτε μεμονωμένα είναι απαραίτητη η γνώση των πρωτοκόλλων επικοινωνίας τους και η ικανότητα ανάλυσή τους .Ακολουθούν τα επικρατέστερα από αυτά.

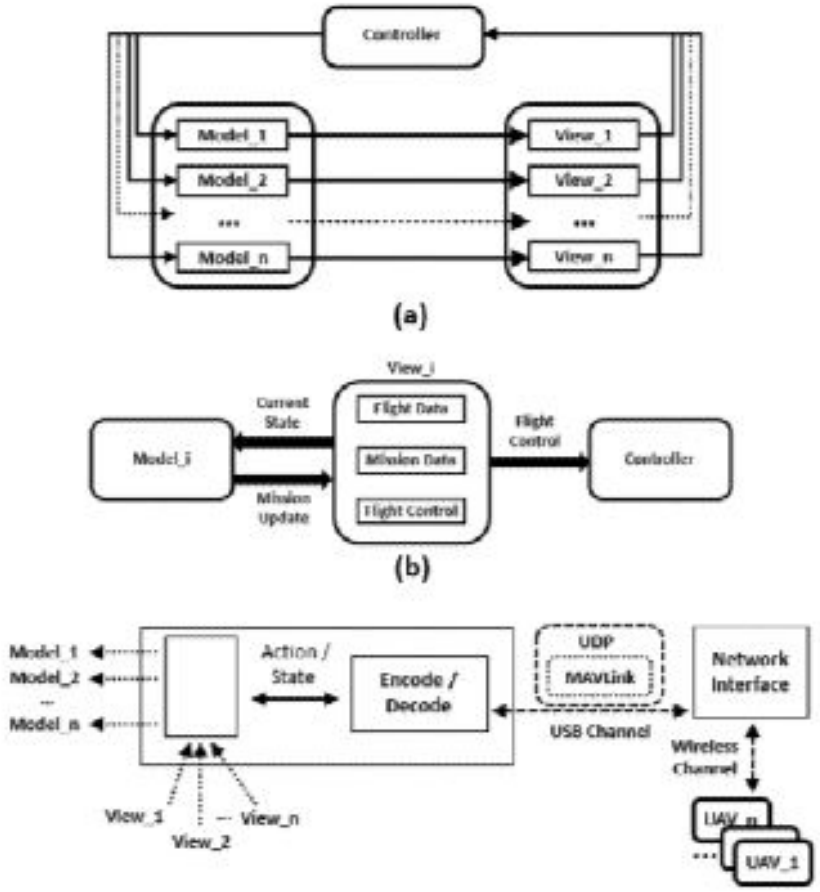
1) DroidPlanner - MAVLink: Το DroidPlanner /Tower [12]είναι ένας επίγειος σταθμός ελέγχου για UAV, που επιτρέπει τον έλεγχο ενός μόνο UAV τη φορά. Παρά τις διάφορες βελτιώσεις της τρίτης έκδοσης, γνωστής ως Tower, που παρέχεται από την εταιρεία 3D Robotics, ο DroidPlanner εξακολουθεί να υποστηρίζει την έλεγχο ενός UAV τη φορά. Το DroidPlanner διατίθεται υπό τη Γενική Δημόσια Άδεια (GNU), προωθώντας την ανάπτυξη από ανοιχτή κοινότητα προγραμματιστών.

Η βασική λειτουργία της εφαρμογής βασίζεται στην ανταλλαγή μηνυμάτων μεταξύ φορητών συσκευών (όπως έξυπνα τηλέφωνα ή ταμπλέτες βασισμένες στο λειτουργικό σύστημα Android) και UAV-Drones, χρησιμοποιώντας το πρωτόκολλο MAVLink. Τα μηνύματα που αποστέλλονται από το DroidPlanner στο UAV αντιπροσωπεύουν ενέργειες που χρησιμοποιούνται για τον έλεγχο του drone. Τα μηνύματα που αποστέλλονται στη βάση από τα UAV περιγράφουν την τρέχουσα κατάστασή τους, περιλαμβάνοντας πληροφορίες τηλεμετρίας και τοποθεσίας. Εκτός από τις εντολές, ο σταθμός ελέγχου μπορεί να δημιουργήσει πορεία πτήσης, ορίζοντας σημεία ενδιαφέροντος (POI) στον χάρτη που το UAV θα επισκεφθεί, καθώς και σημεία διαδρομής που περιγράφουν τη διαδρομή προς τα POI..Η αντίστοιχη εφαρμογή που χρησιμοποιείται σε desktop pc είναι η mission planner .

Το πρωτόκολλο MAVLink είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο επικοινωνίας για μικρά UAV και drones, αναπτυγμένο με άδεια LGPL. Είναι ελαφρύ πρωτόκολλο ιδανικό για την ανταλλαγή μικρών ποσοτήτων δεδομένων μεταξύ του σταθμού ελέγχου και του UAV, με αποφυγή του υψηλού κόστους επεξεργασίας που απαιτείται για τη διαχείριση αυτών των μηνυμάτων. Η δομή των μηνυμάτων περιλαμβάνει ένα σύνολο υποχρεωτικών πεδίων σταθερού μεγέθους (1 Byte το καθένα), όπως η κεφαλίδα, καθώς και ένα προαιρετικό ωφέλιμο πεδίο που περιέχει τα δεδομένα του μηνύματος που πρόκειται να μεταδοθούν. Το μέγεθος του μηνύματος μπορεί να κυμαίνεται από 8 έως 263 Byte.

Κάθε μήνυμα MAVLink προσδιορίζεται από μια τιμή στο πεδίο αναγνωριστικού στην κεφαλίδα του πακέτου και περιλαμβάνει το περιεχόμενό του στο πεδίο δεδομένων του

φορτίου. Τα μηνύματα ορίζονται λογικά μέσω ενός αρχείου XML, το οποίο περιγράφει τους τύπους δεδομένων που μεταδίδονται και τη σειρά με την οποία η εφαρμογή πρέπει να ερμηνεύει και να επεξεργάζεται τα ληφθέντα byte. Το πρωτόκολλο επιτρέπει επίσης τον καθορισμό νέων μηνυμάτων για την επικοινωνία μεταξύ συγκεκριμένων εφαρμογών. Για τον καθορισμό ενός νέου μηνύματος, απαιτείται η παράστασή του σε ένα αρχείο XML, το οποίο στη συνέχεια αυτοματοποιημένα μετατρέπεται από ένα εργαλείο δημιουργίας κώδικα.



Σχήμα 8. Αρχιτεκτονική σταθμού ελέγχου εδάφους: (α) Συνολικός σχεδιασμός MVC. (β) Λεπτομερής αλληλεπίδραση των αρχιτεκτονικών στοιχείων. (κάτω) Διεπαφές ελέγχου και δικτύου. [13]

2) Πρωτόκολα FANETS (Flying ad-hoc network -FANETs Protocols) [14]: Τα ιπτάμενα ad-hoc δίκτυα (FANETs) αναφέρονται σε δίκτυα που δημιουργούνται από μη επανδρωμένα εναέρια οχήματα (UAVs) και λειτουργούν σε συνεργασία μεταξύ τους ως σμήνος για τη μετάδοση δεδομένων και την επικοινωνία. Η λειτουργία των FANETs βασίζεται σε πρωτόκολλα δρομολόγησης που επιτρέπουν στα UAVs να συνεργάζονται για την ανταλλαγή πληροφοριών και την επιλογή κατάλληλης δρομολόγησης των πακέτων δεδομένων.

Τα FANETs αντιμετωπίζουν προκλήσεις στη δρομολόγηση λόγω των εξής χαρακτηριστικών των UAVs:

α)Υψηλή κινητικότητα: Τα UAVs μετακινούνται σε μεγάλες αποστάσεις και αλλάζουν συνεχώς τη θέση τους, οπότε η δρομολόγηση πρέπει να είναι ευέλικτη και να προσαρμόζεται στην κίνηση των UAVs.

β)Συχνή αλλαγή τοπολογίας: Η σύνθεση του δικτύου μπορεί να αλλάξει συχνά λόγω της κίνησης και των αλλαγών στη διάταξη των UAVs, οπότε η δρομολόγηση πρέπει να είναι ευέλικτη και να μπορεί να προσαρμοστεί στις νέες συνθήκες.

γ)Τρισδιάστατη κίνηση: Τα UAVs μπορούν να κινούνται στους τρεις άξονες (x, y, z), οπότε η δρομολόγηση πρέπει να λαμβάνει υπόψη αυτήν την τρισδιάστατη κίνηση για να εξασφαλίσει τη σταθερή και αξιόπιστη επικοινωνία.

Για τη δρομολόγηση στα FANETs, χρησιμοποιούνται πολλά πρωτόκολλα, όπως το AODV (Ad-hoc On-Demand Distance Vector), το OLSR (Optimized Link State Routing), το DSR (Dynamic Source Routing) και το MANET (Mobile Ad-hoc Network) Routing Protocols. Αυτά τα πρωτόκολλα επιτρέπουν στα UAVs να επικοινωνούν μεταξύ τους, να ανιχνεύουν τους γειτονικούς κόμβους και να επιλέγουν τις κατάλληλες διαδρομές για τη μετάδοση των δεδομένων.Η σωστή λειτουργία των πρωτοκόλλων δρομολόγησης εξασφαλίζει την αξιοπιστία, την αποδοτικότητα και την ευελιξία της επικοινωνίας μεταξύ των UAVs στα FANETs.

Η δρομολόγηση με βάση το σμήνος είναι εμπνευσμένη από τη φυσική συμπεριφορά των συνεργαζόμενων εντόμων, όπου είναι οργανωμένα, προσαρμοστικά και συνεργάσιμα για να βρουν τη βέλτιστη διαδρομή. Παρόλα αυτά, η κύρια αδυναμία της δρομολόγησης με βάση το σμήνος είναι η υψηλή καθυστέρηση λόγω της υψηλής κινητικότητας των UAVs. Στα πρωτόκολλα δρομολόγησης με βάση τη θέση, η προώθηση πακέτων γίνεται με βάση τη γεωγραφική θέση των UAVs. Το κύριο μειονέκτημα αυτής της προσέγγισης είναι η μετάδοση καθυστερημένων χρονικά πληροφοριών σχετικά με τη διαδρομή λόγω των συχνά μεταβαλλόμενων θέσεων των UAVs. Αντίθετα, η δρομολόγηση με βάση την τοπολογία επιδιώκει να παρέχει μια βέλτιστη διαδρομή μεταξύ των UAVs, μειώνοντας την επιβάρυνση του ελέγχου.

Τα FANET πρωτόκολλα διακρίνονται σε Proactive(Ενεργά-Προληπτικά) ,Reactive(Αναδραστικά) και Hybrid(Υβριδικά).

Α) **Proactive (**PRP) :Στα πρωτόκολλα αυτά ο πίνακας δρομολόγησης ενημερώνεται τακτικά και αποθηκεύεται σε κάθε UAV, αποτυπώνοντας ολόκληρη την τοπολογία του δικτύου. Αυτό επιτρέπει την αμεσότερη διαθεσιμότητα των διαδρομών δρομολόγησης για τη μετάδοση πακέτων δεδομένων όταν απαιτείται. Το κύριο πλεονέκτημα αυτής της προσέγγισης είναι ότι περιλαμβάνει τις πιο ενημερωμένες πληροφορίες για τις διαδρομές.

Ωστόσο, αυτό επιφέρει πρόσθετη επιβάρυνση στην επικοινωνία λόγω της διατήρησης ενημερωμένων πληροφοριών σχετικά με το δίκτυο. Κατά συνέπεια, η απόδοση του δικτύου μπορεί να επηρεαστεί αφού τα μηνύματα ελέγχου μεταδίδονται άσκοπα. Επιπλέον, τα PRPs δεν είναι κατάλληλα για δίκτυα υψηλής κινητικότητας και μεγάλης κλίμακας. Επίσης, όταν συμβεί αποτυχία σύνδεσης ή αλλαγή της τοπολογίας, τα PRPs αντιδρούν αργά. Υπάρχουν διάφορα πρωτόκολλα που ανήκουν σε αυτήν την κατηγορία.

- Το πρωτόκολλο Διάνυσμα Απόστασης Προορισμού (DSDV) βασίζεται στον αλγόριθμο Bellman-Ford-Moore, με μερικές τροποποιήσεις για να είναι πιο κατάλληλο για FANET. Στο DSDV, κάθε UAV πρέπει να έχει πλήρη γνώση για όλα τα άλλα UAV που είναι συνδεδεμένα στο δίκτυο, λόγω των ενημερωμένων πληροφοριών δρομολόγησης. Αυτό συμβαίνει λόγω της περιοδικής ενημέρωσης του πίνακα δρομολόγησης για ολόκληρο το δίκτυο. Ωστόσο, αυτές οι περιοδικές ενημερώσεις μπορεί να δημιουργήσουν βρόχους δρομολόγησης. Για να αντιμετωπιστεί αυτό το πρόβλημα, το DSDV χρησιμοποιεί αριθμούς ακολουθίας με τα πακέτα δεδομένων.

-Το πρωτόκολλο OLSR(Optimized Link State Routing) είναι ένα από τα πιο δημοφιλή και συχνά προτεινόμενα πρωτόκολλα δρομολόγησης για το FANET. Αυτό το πρωτόκολλο διατηρεί συνεχώς ενημερωμένο τον πίνακα δρομολόγησης, καταχωρώντας και ενημερώνοντας τις διαδρομές που οδηγούν σε κάθε πιθανό UAV προορισμού. Αυτό επιτρέπει την άμεση καθορισμό της διαδρομής για τη μετάδοση δεδομένων χωρίς μεγάλη καθυστέρηση. Το OLSR χρησιμοποιεί ένα μοναδικό πακέτο το οποίο περιέχει πολλά μηνύματα για την επικοινωνία μεταξύ των UAV στο δίκτυο. Αυτό το πακέτο μπορεί να μεταφέρει τρεις διαφορετικούς τύπους μηνυμάτων για διάφορες λειτουργίες, όπως την ανίχνευση γειτονικών UAV (μέσω μηνύματος HELLO), την κοινοποίηση της τοπολογίας του δικτύου (μέσω μηνύματος TC) και τη δήλωση πολλαπλών διεπαφών σε ένα UAV (μέσω μηνύματος MID).

-Τα πρωτόκολλα ανάδρασης- δρομολόγησης (RRP- Reactive Routing Protocols) είναι γνωστά και ως πρωτόκολλα δρομολόγησης κατ' απαίτηση ή παθητικής δρομολόγησης. Αυτά τα πρωτόκολλα χρησιμοποιούνται για την ανακάλυψη ή τη διατήρηση μιας διαδρομής δρομολόγησης μόνο όταν αιτηθεί μετάδοση δεδομένων. Ο πίνακας δρομολόγησης ενημερώνεται μόνο όταν υπάρχουν δεδομένα για αποστολή. Δεν χρειάζεται να υπολογιστεί μια διαδρομή αν δεν υπάρχει σύνδεση μεταξύ των δύο UAV. Αυτό επιτρέπει στα πρωτόκολλα αυτά να ενημερώνουν τους πίνακες δρομολόγησης μόνο για τις διαδρομές που χρησιμοποιούνται επί του παρόντος. Έτσι, αποφεύγονται τα γενικά ζητήματα που σχετίζονται με τα προληπτικά πρωτόκολλα δρομολόγησης. Σε αυτό το μοντέλο δρομολόγησης, χρησιμοποιούνται δύο τύποι μηνυμάτων: (i) Αίτημα Διαδρομής (RouteRequest) και (ii) Απάντηση Διαδρομής (RouteReply). Ένα μήνυμα RouteRequest αποστέλλεται από το UAV πηγής σε όλα τα γειτονικά UAV, χρησιμοποιώντας αλγόριθμους κωδικοποίησης για τον υπολογισμό της βέλτιστης διαδρομής. Αντίθετα, ένα μήνυμα RouteReply δημιουργείται από το UAV που λαμβάνει το αίτημα και μεταδίδεται στο UAV αποστολέα με unicast επικοινωνία. Δεν απαιτείται η ανανέωση όλων των πινάκων

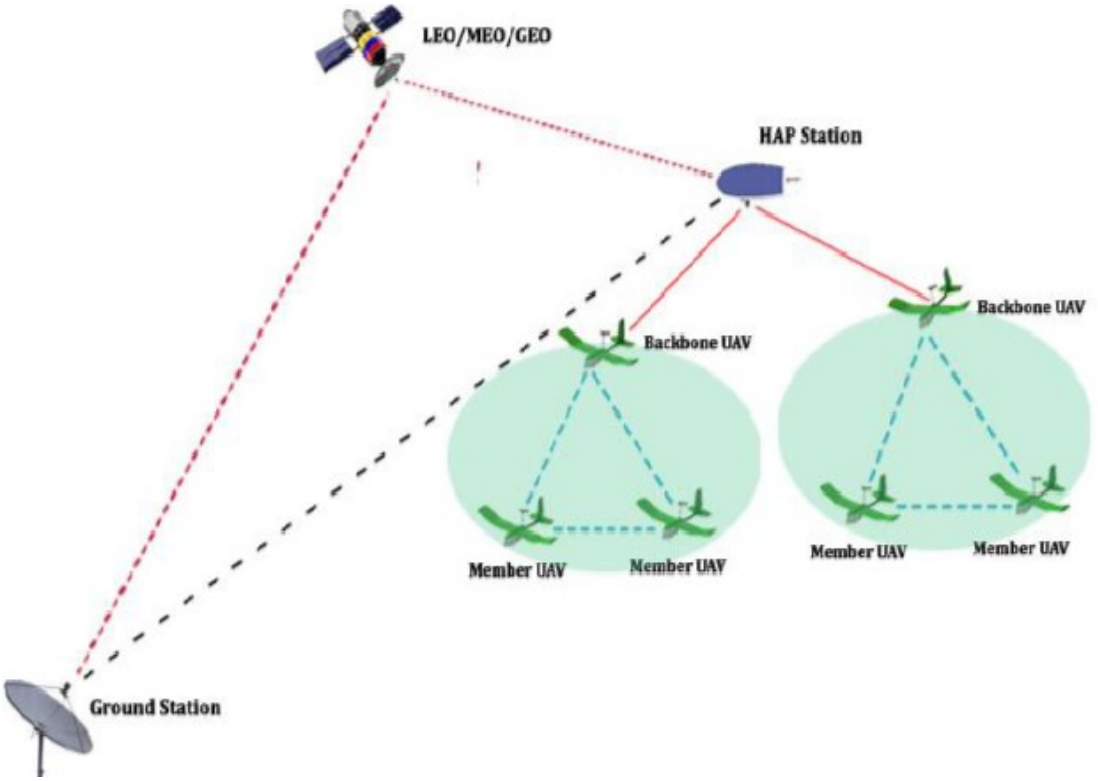
δρομολόγησης στο δίκτυο σε αυτήν την προσέγγιση δρομολόγησης. Το RRP είναι αποδοτικό όσον αφορά το εύρος ζώνης, καθώς δεν υπάρχουν περιοδικές ενημερώσεις(updates).

- Το πρωτόκολλο δρομολόγησης πηγής (DSR- Dynamic Source Routing) είναι ένα αναδραστικό πρωτόκολλο που επιτρέπει την αυτο-διαμόρφωση και αυτο-οργάνωση ενός δικτύου χωρίς υποδομή. Στο DSR, το UAV πηγής δημιουργεί μονοπάτια δρομολόγησης προς τον UAV προορισμό μόνο όταν χρειάζεται. Αυτό γίνεται μέσω της ανακάλυψης διαδρομής και της συντήρησης διαδρομής. Το DSR έχει σχεδιαστεί κυρίως για ασύρματα πολυβηματικά δίκτυα.Τα πρωτόκολλά αυτά έχουν την ανάγκη για επαναλαμβανόμενη αναζήτηση δρομολογήσεων πριν από κάθε παράδοση πακέτου, και μπορεί να είναι χρονοβόρα. Ως εκ τούτου, το DSR δεν χρησιμοποιείται σε δίκτυα με έντονη δυναμικότητα της τοπολογίας.

- Το πρωτόκολλο AODV(Ad-Hoc On-Demand Distance Vector) είναι ένα βελτιωμένο πρωτόκολλο δρομολόγησης που συνδυάζει τα καλύτερα χαρακτηριστικά των πρωτοκόλλων DSDV και DSR. Αυτό το πρωτόκολλο λειτουργεί με ανάδραση, ανακαλύπτοντας μια διαδρομή μόνο όταν απαιτείται. Ο στόχος του AODV είναι η αποφυγή συμφόρησης στο δίκτυο και η βελτίωση της αναλογίας παράδοσης πακέτων. Το AODV περιλαμβάνει τρεις φάσεις: ανακάλυψη διαδρομής, μετάδοση πακέτων και διατήρηση διαδρομής. Κάθε φορά που ένα UAV πηγής επιθυμεί να στείλει ένα πακέτο, προσπαθεί να ανακαλύψει μια διαδρομή προς τον προορισμό, προωθεί τα πακέτα μέσω αυτής της διαδρομής και διατηρεί τη διαδρομή με τη βοήθεια ενημερώσεων.Το AODV μπορεί να αντιμετωπίσει προβλήματα συμφόρησης σε δίκτυα FANET, λόγω της δυναμικής φύσης του συστήματος.

- Το πρωτόκολλο δρομολόγησης κατ' απαίτηση με χρονική αυλάκωση TSODR(Time-Slotted On-Demand Routing) είναι μια παραλλαγή του AODV που χρησιμοποιεί χρονικές χρονοθυρίδες για τη μετάδοση πακέτων. Αυτό το πρωτόκολλο στέλνει πακέτα ελέγχου μόνο κατά τη διάρκεια αποκλειστικών χρονοθυρίδων, όπου μόνο ένα UAV μπορεί να μεταδώσει τα πακέτα δεδομένων του. Αυτή η μέθοδος δρομολόγησης επιτρέπει αποτελεσματική χρήση του εύρους ζώνης και αποφεύγει τις συγκρούσεις πακέτων, βελτιώνοντας έτσι την αναλογία παράδοσης πακέτων.

- Το υβριδικό πρωτόκολλο δρομολόγησης (HRP- Hybrid Routing Protocols) ενσωματώνει προληπτικές και αναδραστικές μεθόδους για την αποτελεσματική δρομολόγηση. Σχεδιασμένο για να συνδυάζει τα πλεονεκτήματα και να αντιμετωπίσει τους περιορισμούς και των δύο μεθόδων, το HRP αποτελεί μια ιδανική λύση. Τα πρωτόκολλα αντιδραστικής δρομολόγησης χρειάζονται περισσότερο χρόνο για να βρουν τη βέλτιστη διαδρομή, ενώ τα πρωτόκολλα προληπτικής δρομολόγησης προκαλούν υψηλή φόρτιση μηνυμάτων ελέγχου. Με το HRP, υπερνικούνται οι προκλήσεις που συνδέονται με τη μεγάλη επιβάρυνση της προληπτικής δρομολόγησης και τις καθυστερήσεις από άκρο σε άκρο της αναδραστικής δρομολόγησης. Το HRP βασίζεται στην έννοια των ζωνών, με προληπτική δρομολόγηση εντός ζώνης και αντιδραστική δρομολόγηση για την εσωτερική ζώνη. Είναι σημαντικό να σημειωθεί ότι τα υβριδικά πρωτόκολλα δεν είναι κατάλληλα για πάνω από 100 UAV εντός της ίδιας ζώνης λόγω πιθανής αλληλεπικάλυψης



Σχήμα 9. FANET . Επικοινωνία Σμήνους Drone UAV [15]

- Το πρωτόκολλο δρομολόγησης ζώνης (ZRP-Zone Routing Protocol) είναι κατάλληλο για τα μεταβλητά μοτίβα κινητικότητας των UAV και βασίζεται στην έννοια των ζωνών. Κάθε UAV τοποθετείται σε μια ζώνη, με τις ζώνες των γειτονικών UAV να τέμνονται. Το μέγεθος της ζώνης καθορίζεται από μια ακτίνα "R" που αντιπροσωπεύει τον αριθμό των UAV στην περίμετρο της ζώνης. Ρυθμίζοντας την ισχύ μετάδοσης, μπορεί να ελεγχθεί ο αριθμός των UAV στη ζώνη. Η δρομολόγηση εντός ζώνης πραγματοποιείται με προληπτική δρομολόγηση για τη διατήρηση των μονοπατιών, ενώ η δρομολόγηση μεταξύ ζώνης χρησιμοποιεί αναδραστικούς μηχανισμούς για την εύρεση των βέλτιστων διαδρομών. Η ενσωμάτωση συνόρων μειώνει την καθυστέρηση που σχετίζεται με την ανακάλυψη διαδρομής. Τα UAV στα σύνορα μιας ζώνης δημιουργούν μόνο μηνύματα απάντησης, ενώ η δρομολόγηση αποφασίζεται εντός των ζωνών με βάση την επιλογή των γειτονικών UAV.

-Το πρωτόκολλο (TORA) Temporarily Ordered Routing Algorithm .Ο αλγόριθμος δρομολόγησης προσωρινής παραγγελίας (TORA) είναι ευέλικτος και κατάλληλος για πολλαπλά δίκτυα δρομολογίων. Χρησιμοποιείται για ασύρματη μετάδοση σε περιβάλλοντα υψηλής κινητικότητας και αντιμετωπίζει αποτελεσματικά τις τοπολογικές αλλαγές. Ο αλγόριθμος αυτός χρησιμοποιεί αναδραστική και προληπτική δρομολόγηση για την κατασκευή και διατήρηση ενός κατευθυνόμενου ακυκλικού γράφου (DAG) μεταξύ των UAV. Παρέχει πολλαπλές διαδρομές για τη μετάδοση πακέτων και χρησιμοποιείται για γρήγορο υπολογισμό ενημερωμένων διαδρομών και ανακάλυψη διαδρομής σε αποσυνδεδεμένα

μονοπάτια. Ο TORA προτιμά μακρύτερες διαδρομές για τη μείωση της επιβάρυνσης του σήματος και εξασφαλίζει αποφυγή βρόχων δρομολόγησης. Κάθε UAV έχει ένα μοναδικό "ύψος" και οι πακέτα δεδομένων ρέουν από τα ανώτερα UAV στα χαμηλότερα με προσέγγιση από πάνω προς τα κάτω. Οι πίνακες δρομολόγησης ενημερώνονται από τα κεντρικά UAV με βάση την εισερχόμενη διαδρομή και τις πληροφορίες ύψους. Το TORA έχει συγκριτικά πλεονεκτήματα και χαρακτηριστικά σε σχέση με άλλα πρωτόκολλα δρομολόγησης βασιζόμενα σε τοπολογία.

Routing Protocol	Protocol Type	Route Updates	Topology Size	Signaling Overhead	Communication Latency	Bandwidth Utilization
DSDV	Proactive	Periodic	Small	Large	Low	Minimum
OLSR	Proactive	Periodic	Small	Large	Low	Minimum
DOLSR	Proactive	Periodic	Small	Large	Low	Minimum
DSR	Reactive	On need	Large	Small	High	Maximum
AODV	Reactive	On need	Large	Small	High	Maximum
TSODR	Reactive	On need	Large	Small	High	Maximum
ZRP	Hybrid	Hybrid	Both	Average	Low	Medium
TORA	Hybrid	Hybrid	Both	Average	Low	Medium

Σχήμα 10. Σύγκριση των διαφόρων πρωτοκόλλων δρομολόγησης βασισμένων σε τοπολογία για FANET [14]

Συμπερασματικά τα δίκτυα FANET που αναφέρθηκαν έχουν αναδειχθεί ως ένας αναδυόμενος τομέας έρευνας. Χαρακτηρίζονται από υψηλή κινητικότητα, συχνές αλλαγές τοπολογίας και τρισδιάστατη χωρική κίνηση των UAV, πράγμα που αποτελεί πρόκληση για τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται. Η επιλογή κατάλληλων και αξιόπιστων πρωτοκόλλων δρομολόγησης είναι απαραίτητη για τον έλεγχο της ασφάλειας της επικοινωνίας μεταξύ των UAV και η ικανότητα αναγνώρισης και υποκλοπής αυτών από τα αντι-drone συστήματα είναι καταλυτική στην αποτελεσματικότητα του αντι-drone συστήματος , στην αντιμετώπιση περιπτώσεων εχθρικών σμήνους Drone ή μεμονομένων.

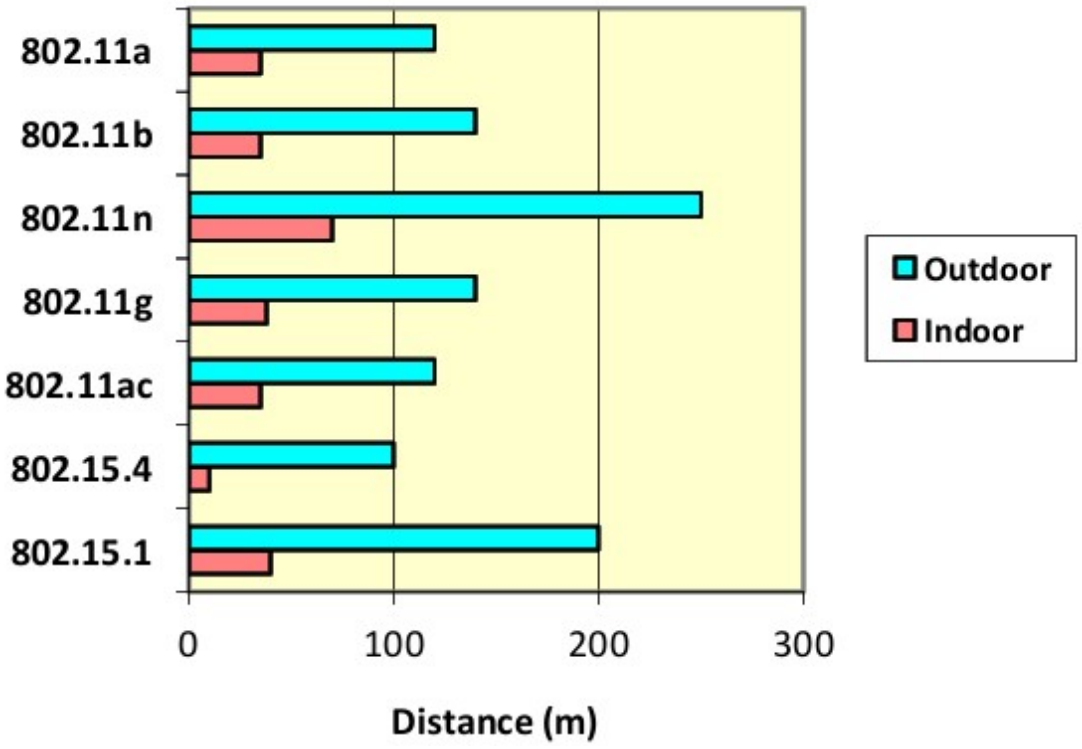
17. Τεχνολογίες Ασύρματων Επικοινωνιών Drone

Υπάρχουν πολλές τεχνολογίες ασύρματης επικοινωνίας που μπορούν να αποτελέσουν πιθανές επιλογές χρήσης μεταξύ των UAV Drones για την επικοινωνία μεταξύ τους ή με τη βάση τους. Η επιλογή της κατάλληλης τεχνολογίας εξαρτάται από τη φύση της εφαρμογής και το είδος της αποστολής. Οι ασύρματες επικοινωνίες στα drone χωρίζονται σε δύο κύριες κατηγορίες: ασύρματες επικοινωνίες μικρής εμβέλειας και ασύρματες επικοινωνίες μεγάλης εμβέλειας.

Οι ασύρματες επικοινωνίας μικρής εμβέλειας, όπως το Wi-Fi, το ZigBee και το Bluetooth, χρησιμοποιούνται για επικοινωνία σε μικρές αποστάσεις, ενώ οι τεχνολογίες επικοινωνίας μεγάλης εμβέλειας, όπως τα κυψελοειδή δίκτυα, το WiMAX και οι δορυφορικές

επικοινωνίες, μπορούν να χρησιμοποιηθούν για κάλυψη πολύ μεγαλύτερων περιοχών. Και οι δύο κατηγορίες αυτές εξετάζονται περαιτέρω παρακάτω.

1) Ασύρματες Επικοινωνίας Μικρής Εμβέλειας (Short-Range Communication Technologies)**:** Οι ασύρματες επικοινωνίες μικρής εμβέλειας δεν περιορίζονται μόνο στην παροχή ασύρματης πρόσβασης σε κοντινές αποστάσεις, αλλά, από μια ευρύτερη οπτική γωνία, προσφέρουν επίσης ετοιμοπαράδοτες, ελαφριές και οικονομικά αποδοτικές συνδέσεις επικοινωνίας λόγω των μη συνωστισμένων ζωνών συχνοτήτων. Οι ασύρματες επικοινωνίες μικρής εμβέλειας μπορούν να μεταφέρουν πληροφορίες σε αποστάσεις από μερικά εκατοστά έως μερικές εκατοντάδες μέτρα.



Σχήμα 11. Ασύρματες Επικοινωνίες Μικρής Εμβέλειας [15]

Communication Technology	IEEE Standard	Frequency/Medium	Spectrum Type	Device Mobility	Theoretical Data Rate	Range Indoor-Outdoor	Network Typology	Latency	Advantages	Limitations
Wi-Fi [7,8]	802.11	2.4 GHz IR	Unlicensed	Yes	Up to 2 Mbps	20 m–100 m	Ad-hoc, star, mesh, hybrid	<5 ms	High speed and cheap	Limited range
	802.11a	5 GHz	Unlicensed	Yes	Up to 54 Mbps	35 m–120 m	Ad-hoc, star, mesh, hybrid			
	802.11b	2.4 GHz	Unlicensed	Yes	Up to 11 Mbps	35 m–140 m	Ad-hoc, star, mesh, hybrid			
	802.11n	2.4 /5 GHz	Unlicensed	Yes	Up to 600 Mbps	70 m–250 m	Ad-hoc, star, mesh, hybrid			
	802.11g	2.4 GHz	Unlicensed	Yes	Up to 54 Mbps	38 m–140 m	Ad-hoc, star, mesh, hybrid			
	802.11ac	5 GHz	Unlicensed	Yes	Up to 3466 Mbps	35 m–120 m	Ad-hoc, star, mesh, hybrid			
Bluetooth 5 [9–12]	802.15.1	2.4 GHz	Unlicensed	Yes	Up to 2 Mbps	40 m–200 m	Ad-hoc, piconet	3 ms	Energy-efficient	Low data rate
ZigBee [13–15]	802.15.4	2.4 GHz	Unlicensed	Yes	250 Kbps	10 m–100 m	Ad-hoc, star, mesh, tree, cluster	15 ms	Low cost	Low data rate
WiMAX [16–18]	802.16a	2 to 11 GHz	Licensed	Yes	Up to 75 Mbps	Up to 48 km	Wide-area wireless backhaul	30 ms	High throughput	Interference issues
LTE [19–22]	LTE	Up to 20 MHz	Licensed	Yes	Up to 300 Mbps	Up to 100 km	Flat, IP based	5 ms	High bandwidth	Expensive
5G [23–29]	5G (eMBB)	28 GHz	Licensed	Yes	Up to 20 Gbps	Wide Area	IP based	1 ms	High data rate	Expensive
Satellite [30,31]	Satellite	Up to 40 GHz	Licensed	Yes	Up to 1 Gbps	World Wide	-	550 ms	Wide coverage	High delay and high cost

Σχήμα 12. Ασύρματες επικοινωνίες που είναι διαθέσιμες για UAV [15]

- Wi-Fi (IEEE 802.11): Το Wi-Fi (Wireless Fidelity) είναι μια τεχνολογία ασύρματης επικοινωνίας μικρής εμβέλειας που περιλαμβάνει ένα σύνολο προτύπων για τον σχεδιασμό WLAN (Ασύρματο τοπικό δίκτυο) στις ζώνες συχνοτήτων 2,4 GHz, 3,6 GHz, 5 GHz και 60 GHz. Οι παραλλαγές του IEEE 802.11a/b/g/n/ac μπορούν να παρέχουν την απαιτούμενη απόδοση για μεταδόσεις δεδομένων μεγάλου μεγέθους, όπως βίντεο και εικόνες, και είναι ιδανικές για πολλές εφαρμογές FANET. Η εμβέλεια μετάδοσης σε ένα παραδοσιακό σύστημα Wi-Fi είναι περίπου 100 μέτρα, αλλά μπορεί να επεκταθεί αρκετά χιλιόμετρα μέσω ad-hoc δικτύωσης μεταξύ UAV. Σε ένα δίκτυο 802.11, τα UAV Drones ανιχνεύουν και συνδέονται με ασύρματα τοπικά δίκτυα (WLAN) μέσω των σημείων πρόσβασης (APs). Μια συσκευή μπορεί να λειτουργήσει είτε ως client είτε ως AP, και οι ρόλοι αυτοί μπορούν να εκχωρηθούν δυναμικά και να εκτελεστούν από την ίδια συσκευή ταυτόχρονα. Με τη χρήση μιας ασύρματης σύνδεσης 802.11a για τα UAV και τα GS(Ground Stations), μπορεί να επιτευχθεί αποδοτική δικτύωση βασιζόμενη σε UAV.

- Bluetooth (IEEE 802.15.1): Το Bluetooth (IEEE 802.15.1) είναι μια τεχνολογία ασύρματης επικοινωνίας μικρής εμβέλειας που λειτουργεί στη ζώνη συχνοτήτων 2,4 GHz. Έχει εύρος επικοινωνίας από 10 έως 200 μέτρα και μπορεί να παρέχει ρυθμό μετάδοσης δεδομένων από 1 έως 3 Mbps, με μέγιστο ρυθμό δεδομένων έως και 24 Mbps. Η τεχνολογία Bluetooth έχει εξελιχθεί με τον χρόνο, και η πιο πρόσφατη έκδοση είναι το Bluetooth 6, που εστιάζει στη βελτίωση της ταχύτητας, του εύρους μετάδοσης, της χαμηλής ενεργειακής κατανάλωσηςς και της συνύπαρξης με άλλες τεχνολογίες μικρής εμβέλειας. Το Bluetooth 6 μπορεί να μεταδίδει πλούσια δεδομένα, συμπεριλαμβανομένων αρχείων πολυμέσων και URL. Η τεχνολογία Bluetooth έχει προταθεί και χρησιμοποιηθεί για την επικοινωνία σε δίκτυα FANET με Drones, χρησιμοποιώντας υβριδικά σχήματα και πλατφόρμες που εκμεταλλεύονται τα πλεονεκτήματα του Bluetooth.

- ZigBee (IEEE 802.15.4): Το ZigBee (IEEE 802.15.4) είναι μια τεχνολογία που χρησιμοποιείται συνήθως σε εφαρμογές χαμηλού ρυθμού δεδομένων, με έμφαση στην μεγάλη διάρκεια ζωής της μπαταρίας και την ασφαλή δικτύωση. Καλύπτει μια απόσταση από 10 έως 100 μέτρα και λειτουργεί στην περιοχή συχνοτήτων 2,4 GHz με ρυθμό μετάδοσης δεδομένων 250 kbps. Το ZigBee είναι λιγότερο ακριβό και απλούστερο σε σύγκριση με το Bluetooth και το Wi-Fi. Έχει 16 κανάλια με εύρος ζώνης 5 MHz το καθένα. Το ZigBee έχει χρησιμοποιηθεί με επιτυχία σε διάφορες εφαρμογές, όπως ο εντοπισμός εσωτερικού χώρου από τετρακόπτερα drones, την εκτίμηση θέσης κατά την προσγείωση UAV και την επικοινωνία μεταξύ σμήνους. Οι μελέτες έχουν δείξει ότι το ZigBee είναι αποτελεσματικό και εύκολο στην ανάπτυξη για αυτές τις εφαρμογές, και μπορεί να είναι μια επιλογή επικοινωνίας μεταξύ Drone για χαμηλό ρυθμό δεδομένων στο πλαίσιο των δικτύων FANET.

2) Τεχνολογίες Επικοινωνίας Μεγάλης Εμβέλειας (Long-Range Communication Technologies): Οι τεχνολογίες ασύρματης επικοινωνίας μεγάλης εμβέλειας αποτελούν αποτελεσματικές λύσεις για τη μεταφορά δεδομένων σε μεγάλες αποστάσεις. Μπορούν να χρησιμοποιηθούν ως backhaul συνδέσεις μεταξύ δύο σημείων για την παροχή υπηρεσιών επικοινωνίας δεδομένων μεγάλης εμβέλειας(το backhaul αναφέρεται γενικά στην πλευρά του δικτύου που επικοινωνεί με το παγκόσμιο Διαδίκτυο). Επιπλέον, αυτές οι ασύρματες επικοινωνίες μπορεί να χρησιμοποιούνται από τα UAV, καθώς επιτρέπουν την απευθείας επικοινωνία μεταξύ τους (U2U) και με τη σταθερή υποδομή (U2I).

-WiMAX (IEEE 802.16): Το WiMAX (Worldwide Interoperability for Microwave Access) είναι ένα πρότυπο τεχνολογίας που στοχεύει στην παροχή ευρυζωνικής πρόσβασης σε μεγάλες αποστάσεις. Αυτή η τεχνολογία παρέχει διάφορους τρόπους σύνδεσης, από συνδέσεις από σημείο σε σημείο έως πλήρη πρόσβαση κινητού τύπου κινητής τηλεφωνίας. Έχει σχεδιαστεί για να εξυπηρετεί τόσο σταθερές όσο και κινητές ευρυζωνικές εφαρμογές.Το WiMAX υποστηρίζει υψηλές ταχύτητες μετάδοσης δεδομένων, φτάνοντας έως και 75 Mbps για σταθερές εφαρμογές (20 έως 30 Mbps ανά συνδρομητή) και 30 Mbps για εφαρμογές κινητής τηλεφωνίας (3 έως 5 Mbps ανά συνδρομητή) . Η τεχνολογία αυτή έχει αναπτυχθεί με σκοπό να παρέχει υψηλής ποιότητας ροή φωνής και βίντεο, διατηρώντας ταυτόχρονα την επιθυμητή ποιότητα υπηρεσίας (QoS).

Όσον αφορά στα UAV, το WiMAX θεωρείται η καταλληλότερη τεχνολογία για συστήματα διάσωσης που βασίζονται σε UAV σε αποστολές σε εχθρικά περιβάλλοντα . Μελέτες έχουν προτείνει μεθοδολογίες για τον προγραμματισμό δικτύου που αφορούν τον αριθμό και τη θέση των UAV, με την προσομοίωση να καταδεικνύει τη δυνατότητα υπολογισμού των αποστάσεων των Drone Swarms χρησιμοποιώντας WiMAX.

-Long-Term Evolution (LTE): Η τεχνολογία προτοκόλλου Long-Term Evolution (LTE) παρέχει ασφαλή ασύρματη συνδεσιμότητα, κινητικότητα και υψηλή ταχύτητα μετάδοσης δεδομένων, η οποία μπορεί να βελτιώσει σημαντικά τον έλεγχο και την ασφάλεια πέρα από τις περιπτώσεις χρήσης οπτικής επαφής (LOS-Line of Sight). Το LTE είναι βελτιστοποιημένο από το πρωτόκολλο IP, με κλιμακούμενα εύρη ζώνης 20 MHz, 15 MHz, 10 MHz και

μικρότερα από 5 MHz. Υποστηρίζει και τα δύο φάσματα διπλής όψης διαίρεσης συχνότητας (FDD) και διαίρεσης χρόνου (TDD) . Το βέλτιστο μέγεθος κυψέλης είναι 5 km, παρόλο που μπορεί να επιτύχει καλή απόδοση έως 30 km και να παρέχει αποδεκτή απόδοση έως και 100 km. Για το λόγο αυτό η χρήση ενός δικτύου LTE από τα UAV έχει αυξηθεί τα τελευταία χρόνια.

-LoRa and LoRaWan protocols: Το LoRaWAN είναι ένα πρωτόκολλο ασύρματης επικοινωνίας μεγάλης εμβέλειας, το οποίο χρησιμοποιείται συχνά για τη δημιουργία δικτύων χαμηλής ισχύος ευρείας περιοχής (LPWAN). Έχει μεγάλη εμβέλεια μετάδοσης από περίπου 300 μέτρα έως περίπου 15 χιλιόμετρα. [16]

Το LoRa είναι μια διαμόρφωση που έχει κατοχυρωθεί με δίπλωμα ευρεσιτεχνίας από την Semtech Corporation . Αυτή η διαμόρφωση βασίζεται στην τεχνική Chirp Spread Spectrum (CSS) και χρησιμοποιείται στο επίπεδο PHY (Physical Layer) του πρωτοκόλλου. Το LoRaWAN είναι ένα πρωτόκολλο επιπέδου MAC (Medium Access Control) που βασίζεται στο LoRa στο επίπεδο PHY και υλοποιεί μια αρχιτεκτονική ανοιχτού δικτύου.

Επιπλέον, το LoRaWAN ορίζει τους κανόνες του επιπέδου πρόσβασης μέσων δικτύου, τη μέθοδο ελέγχου ταυτότητας, το προφίλ συσκευής και την κρυπτογράφηση δεδομένων. Αυτά τα στοιχεία είναι σημαντικά για τη λειτουργία του δικτύου LoRaWAN και την επίτευξη ασφάλειας, αποδοτικότητας και αξιοπιστίας στην ανταλλαγή δεδομένων μεταξύ των συσκευών LoRaWAN και των πύλων δικτύου (network gateways).

Συνολικά, το LoRaWAN παρέχει ένα αξιόπιστο και αποδοτικό πρωτόκολλο επικοινωνίας για τα δίκτυα LPWAN, τα οποία χαρακτηρίζονται από μεγάλη εμβέλεια και χαμηλή κατανάλωση ισχύος και μπορούν να χρησιμοποιηθούν και από UAV Drones.

Για τη μετάδοση και λήψη δεδομένων μέσω δικτύων LoRaWAN, οι τερματικοί κόμβοι LoRaWAN (στα Drones) πρέπει να είναι καταχωρημένοι και ενεργοποιημένοι στο AS (Application Server) του παρόχου δικτύου LoRaWAN, ο οποίος διαχειρίζεται τα LoRaWAN Gateways (GW).

Ένα UAV με δυνατότητα LoRaWAN μπορεί να συνδεθεί στο δίκτυο με δύο τρόπους: με τη μέθοδο Over-The-Air-Activation (OTAA) ή με τη μέθοδο Activation-By-Personalization (ABP).

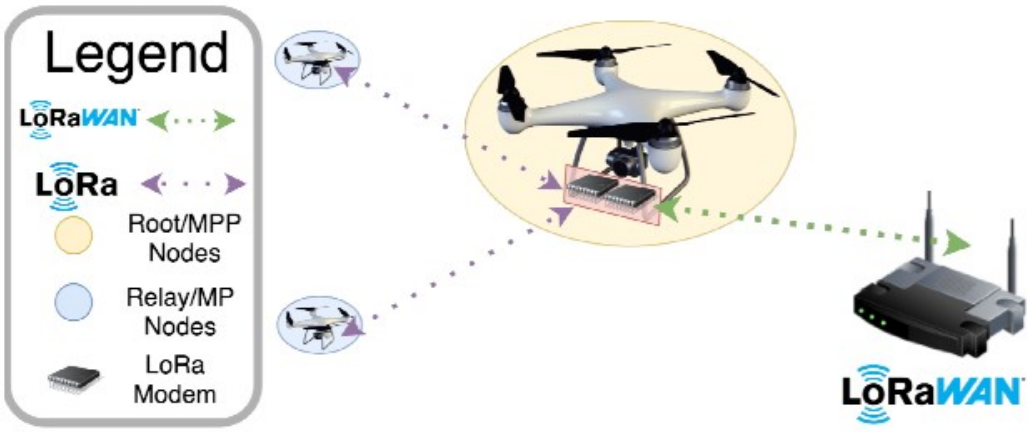
Και οι δύο προσεγγίσεις είναι αποτελεσματικές, αλλά το OTAA είναι πιο ασφαλές. Με τη μέθοδο OTAA, κάθε φορά που ο τερματικός κόμβος-UAV στέλνει ένα πακέτο αίτησης σύνδεσης, λαμβάνει μια αποδοχή σύνδεσης που περιλαμβάνει τα εξής στοιχεία: (i) Το αναγνωριστικό δικτύου (NetID) (ii) Ένα αναγνωριστικό 32-bit της τελικής συσκευής εντός του δικτύου (DevAddr) (iii) Μια τιμή nonce ασφαλείας (AppNonce)

Αυτά τα στοιχεία θα χρησιμοποιηθούν από τη συσκευή για τη δημιουργία ενός κλειδιού συνεδρίας δικτύου (NwkSKey) και ενός κλειδιού συνεδρίας εφαρμογής (AppSKey).

Ένα Drone που ενεργοποιείται με ABP είναι εσωτερικά εξοπλισμένο με τα παρακάτω στοιχεία:

- DevAddr: Αναγνωριστικό της συσκευής
- AppSKey: Κλειδί συνεδρίας εφαρμογής
- NwkSKey: Κλειδί συνεδρίας δικτύου

Αυτά τα στοιχεία αποστέλλονται μέσω του δικτύου LoRaWAN σε κάθε μετάδοση που πραγματοποιεί το UAV, προκειμένου να αναγνωρίζεται το ίδιο ως κόμβος μετάδοσης



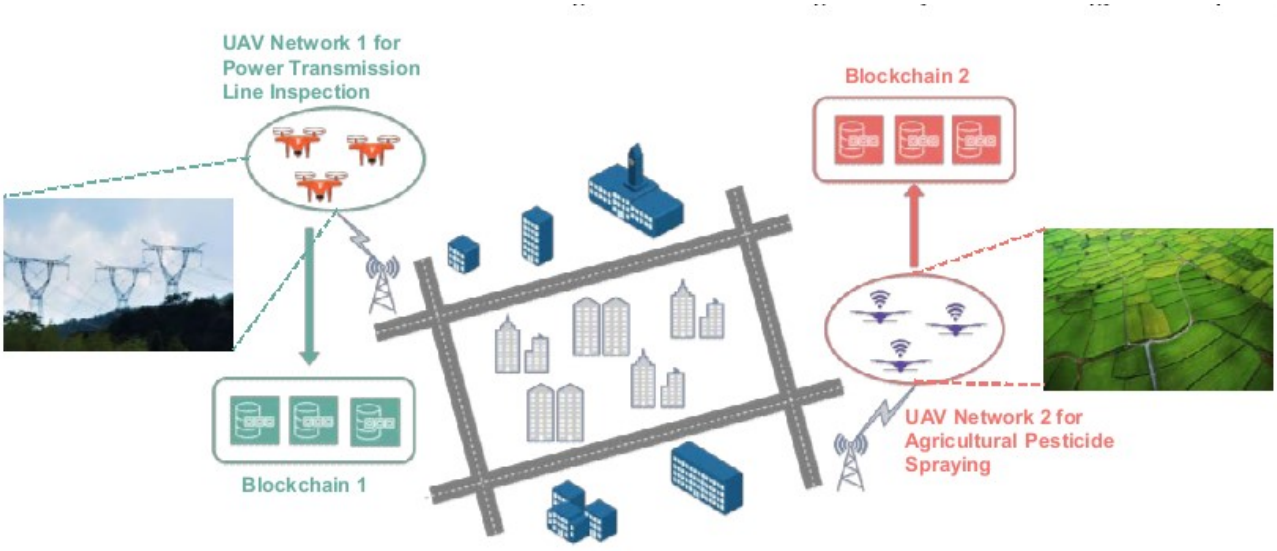
Σχήμα 13. Διπλή υλοποίηση με βάση το πρωτόκολλο LoRa για κεντρικούς κόμβους[16].

-Δίκτυα 5ης και 6ης Γενιάς-Fifth and Sixth Generation (5G,6G): Η πέμπτη γενιά ή 5G αποτελεί πλέον την τελευταία εφαρμοσμένη εξέλιξη στην κυψελοειδή κινητή επικοινωνία και η 6η είναι σε εξέλιξη, ακολουθώντας τις προηγούμενες γενιές 2G (GSM), 3G (UMTS) και 4G (LTE/WiMAX). Η τεχνολογία 5G προσφέρει αρκετά εντυπωσιακά χαρακτηριστικά, όπως υψηλό ρυθμό μετάδοσης δεδομένων, μειωμένη καθυστέρηση, εξοικονόμηση ενέργειας, βελτιωμένη χωρητικότητα συστήματος και απρόσκοπτη συνδεσιμότητα. Παρέχει ταχύτητες ανά χρήστη έως και 100 GB/s και χωρητικότητα που είναι έως και 1000 φορές μεγαλύτερη από τα προηγούμενα δίκτυα και έχει αρχίσει ήδη να εφαρμόζεται στα UAV.

Λόγω των παραπάνω χαρακτηριστικών, η τεχνολογία παίζει κρίσιμο ρόλο στα συστήματα επικοινωνίας των UAV. Στο πλαίσιο των UAV στο περιβάλλον του 5G, μικρότερα τμήματα δικτύου της αρχιτεκτονικής FANET θα μπορούσαν να συνδεθούν με το κεντρικό δίκτυο,

επιτρέποντας την παροχή υπηρεσιών όπως η μετάδοση πολυμέσων και η παρακολούθηση .Η σύνδεση των UAV με μια μονάδα βασικής ζώνης (BBU) και η σύνδεση με σταθμό βάσης μακρο-κυψελών (MBS), μπορούν να διασφαλίσουν την απαιτούμενη απρόσκοπτη συνδεσιμότητα.

- LECast: Πρωτόκολλο εκπομπής χαμηλής κατανάλωσης για δίκτυα Blockchain UAV. Για να προστατευθεί το απόρρητο των δεδομένων και η ασφάλεια των επικοινωνιών των drones, εξετάζεται το blockchain ως τεχνολογία ενεργοποίησής τους. Ωστόσο, τα drones δεν μπορούν να υποστηρίξουν απευθείας ενεργοβόρες εφαρμογές blockchain λόγω του μικρού μεγέθους και της περιορισμένης αποθήκευσης ενέργειας. Επιπλέον, οι μελλοντικές επικοινωνίες 6G απαιτούν επικοινωνίες εξαιρετικά χαμηλής κατανάλωσης (ELPC- Extremely Low Power Consumption"). Το πρωτόκολλο LECast σχεδιάστηκε για να καταστήσει το blockchain κατάλληλο για τις απαιτήσεις ELPC στις επικοινωνίες 6G και στα δίκτυα μη επανδρωμένων εναέριων οχημάτων . Το LECast αναλύει το μοντέλο κατανάλωσης ενέργειας της επικοινωνίας μεταξύ δύο drones ή και βάσης ελέγχου και δημιουργεί ένα δέντρο εκπομπής συντομότερης διαδρομής (SPB Tree) για τα δίκτυα UAV, με στόχο την ελαχιστοποίηση της κατανάλωσης ενέργειας. [17]



Σχήμα 14. Δίκτυα Blockchain σε σμήνος Drone

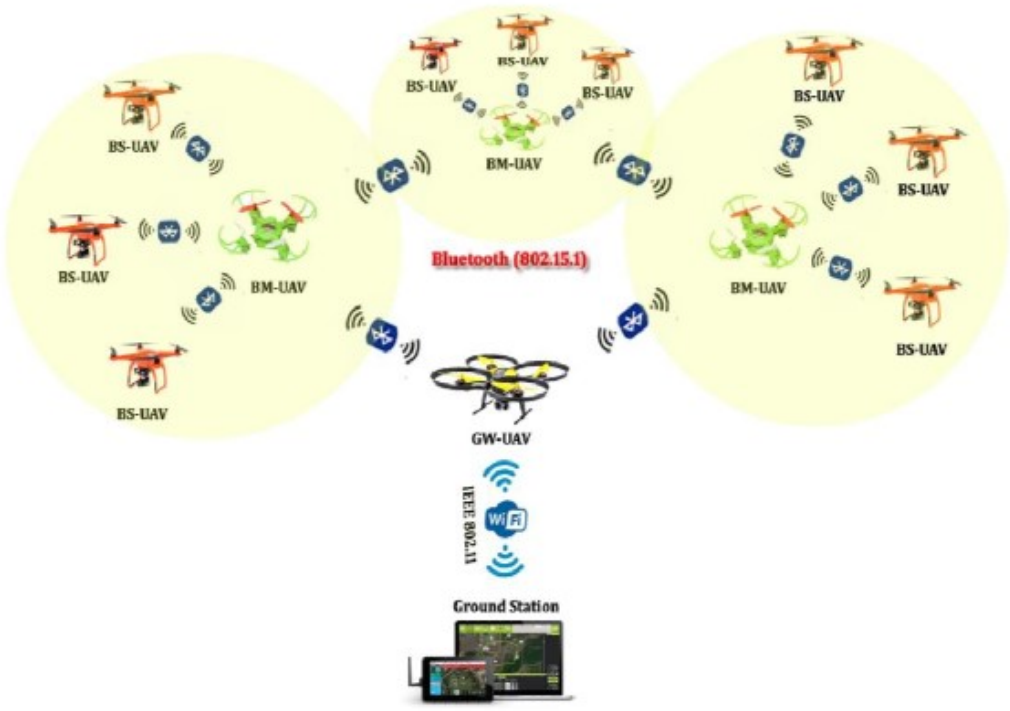
-Δορυφορική Επικοινωνία-Satellite Communication (SATCOM): Η τεχνολογία των επικοινωνιών μέσω δορυφόρων (SATCOM) χρησιμοποιείται για τη μετάδοση ηλεκτρομαγνητικών σημάτων ανάμεσα σε επίγειους σταθμούς και δορυφόρους, επιτρέποντας την αμφίδρομη επικοινωνία. Στο πλαίσιο του SATCOM, χρησιμοποιούνται

διάφορες ζώνες συχνοτήτων από διάφορους δορυφόρους. Για παράδειγμα, οι ζώνες C περιλαμβάνουν μια ζώνη ανόδου με ζεύξη στα 6 GHz και μια ζώνη καθόδου με ζεύξη στα 4 GHz. Οι X-Band, που συνήθως χρησιμοποιούνται σε στρατιωτικά και κυβερνητικά συστήματα, χρησιμοποιούν τα 8 GHz για uplink και τα 7 GHz για downlink. Οι λεγόμενες ζώνες Ku-Band λειτουργούν στα 14 GHz για uplink και στα 11-12 GHz για downlink. Ωστόσο, αυτές οι ζώνες μπορεί να είναι κορεσμένες, και γι' αυτό εξελίσσονται οι ζώνες Ka-Band λειτουργώντας στα 30 GHz για uplink και στα 20 GHz για downlink.

Η δορυφορική σύνδεση παρέχει μεγαλύτερη κάλυψη και υψηλή ποιότητα εικόνας για μετάδοση εικόνων με μεγάλη εμβέλεια. Προβλήματα όμως αντιμετωπίζονται στην εφαρμογή του SATCOM για τη ζωντανή μετάδοση εικόνων και βίντεο με τη χρήση μικρών UAV. Αυτά περιλαμβάνουν το περιορισμένο εύρος ζώνης και το υψηλό κόστος μετάδοσης δεδομένων.

Communication Technology	Standard/Service Category	Spectrum Type	Frequency/Medium	Device Mobility	Theoretical Data Rate	Range Indoor-Outdoor	Latency
Wi-Fi	802.11 802.11a 802.11b 802.11n 802.11g 802.11ac	Unlicensed Unlicensed Unlicensed Unlicensed Unlicensed Unlicensed	2.4 GHz IR 5 GHz 2.4 GHz 2.4/5 GHz 2.4 GHz 5 GHz	Yes Yes Yes Yes Yes Yes	Up to 2 Mbps Up to 54 Mbps Up to 11 Mbps Up to 600 Mbps Up to 54 Mbps Up to 866.7 Mbps	20–100 m 35–120 m 35–140 m 70–250 m 38–140 m 35–120 m	<5 ms
ZigBee	802.15.4	Unlicensed	2.4 GHz	Yes	Up to 25 kbps	10–100 m	15 ms
Bluetooth V5	802.15.1	Unlicensed	2.4 GHz	Yes	Up to 2 Mbps	10–200 m	3 ms
LoRaWAN	IEEE 802.15.4g	Unlicensed	868 MHz, 915 MHz	Yes	Up to 50 kbps	05–15 km	Device Class Dependent
Sigfox	-	Unlicensed	868 MHz, 902 MHz	Yes	Up to 100 bps	03–30 km	2 s
NB-IoT	• LTE Cat NB1 • LTE Cat NB2	licensed	200 KHz	Yes	Up to 250 kbps	10–35 km	1.6–10 s
5G	• mMTC • URLLC • eMBB	licensed	• Sub-6 GHz • MmWave for fixed access	Yes	Up to 1 Gbps	Wide Area	1 ms
B5G	• mMTC • URLLC • eMBB • Hybrid (URLLC + eMBB)	licensed	• Sub-6 GHz • MmWave for fixed access	Yes	Up to 100 Gbps	Wide Area	1 ms
6G	• MBRLLC • mURLLC • HCS • MPS	licensed	• Sub-6 GHz • MmWave for mobile access • Exploration of higher frequency and THz bands (above 300 GHz) • Non-RF (e.g., optical, VLC, etc.)	Yes	Up to 1 Tbps	Wide Area	<1 ms

Σχήμα 15. Σύγκριση μεταξύ των διαφόρων τεχνολογιών επικοινωνίας για FANET [16]



Σχήμα 16. Τοπολογία Multi Layer FANET [16]

18. Πλατφόρμες -Τεχνικές των Αντι-Drone Αμυντικών Συστημάτων

Μια επίθεση σε επίπεδο δικτύου σε UAV από ένα αμυντικό σύστημα αντι-drone παρέχει τη δυνατότητα επίθεσης στο στόχο από απόσταση. Αυτή η επίθεση χρησιμοποιεί μια σειρά τεχνικών παραβίασης για να αποκτήσει πρόσβαση στο σύστημα, ανεξάρτητα από το προστατευτικό σύστημα που μπορεί να υπάρχει. Μία από τις συνηθέστερες τεχνικές είναι η λεγόμενη ‘ επίθεση με ωμή βία’ (brute force attack), η οποία αναφέρεται και ως επίθεση με βία κατά των κρυπτογραφημένων συστημάτων. Αν και αυτές οι προσπάθειες συνήθως απαιτούν πολύ χρόνο, μπορούν να επιτύχουν την απόκτηση του κλειδιού κρυπτογράφησης από τα περισσότερα συστήματα. [17]

Σε πιο προηγμένες επιθέσεις, χρησιμοποιούνται ενεργειακοί ανιχνευτές. Αυτοί οι ανιχνευτές μπορούν να περιλαμβάνουν εστιασμένες δέσμες ηλεκτρονίων, ιόντων ή φωτός, οι οποίες χρησιμοποιούνται για την ανίχνευση ασυνήθιστων εκπομπών ενέργειας. Οι προηγμένοι ανιχνευτές ενέργειας μπορούν επίσης να διαβάζουν και να γράφουν στη μνήμη του συστήματος, καθώς και να προσαρμόζουν τα σήματα ελέγχου.

Μια άλλη τεχνική επίθεσης είναι η επίθεση με βάση τη θερμοκρασία, όπου προσπαθείται να υπερβληθεί το όριο λειτουργίας του τσιπ. Μειώνοντας τη θερμοκρασία της CMOS RAM,

τα περιεχόμενα της μνήμης μπορούν να διατηρηθούν για ώρες χωρίς ρεύμα, παραβιάζοντας την ασφάλεια των δεδομένων. Επιπλέον, η εξαναγκασμένη λειτουργία της CPU με ασυνήθιστα χαμηλή ή υψηλή τάση εισόδου μπορεί να οδηγήσει σε παρανόηση των εντολών ή στην αποθήκευση δεδομένων όταν δεν είναι επιθυμητό. Μία άλλη μέθοδος επίθεσης είναι το "Clock glitching", όπου η περίοδος του ρολογιού είτε μειώνεται είτε επιμηκύνεται, παρακάμπτοντας τις εντολές της CPU.

Υπάρχουν διάφορες τεχνικές που μπορούν να χρησιμοποιηθούν σε επιθέσεις επίπεδου δικτύου κατά των συστημάτων UAV drones. Ορισμένες από αυτές τις τεχνικές είναι:

Αναγνώριση και εκμετάλλευση των ευπαθειών του λογισμικού: Αναζήτηση και εκμετάλλευση ευπαθειών στο λογισμικό που εκτελεί το UAV, όπως ευπάθειες σε λειτουργικά συστήματα, πρωτόκολλα επικοινωνίας, διακομιστές, ή λογισμικό ελέγχου της πτήσης.

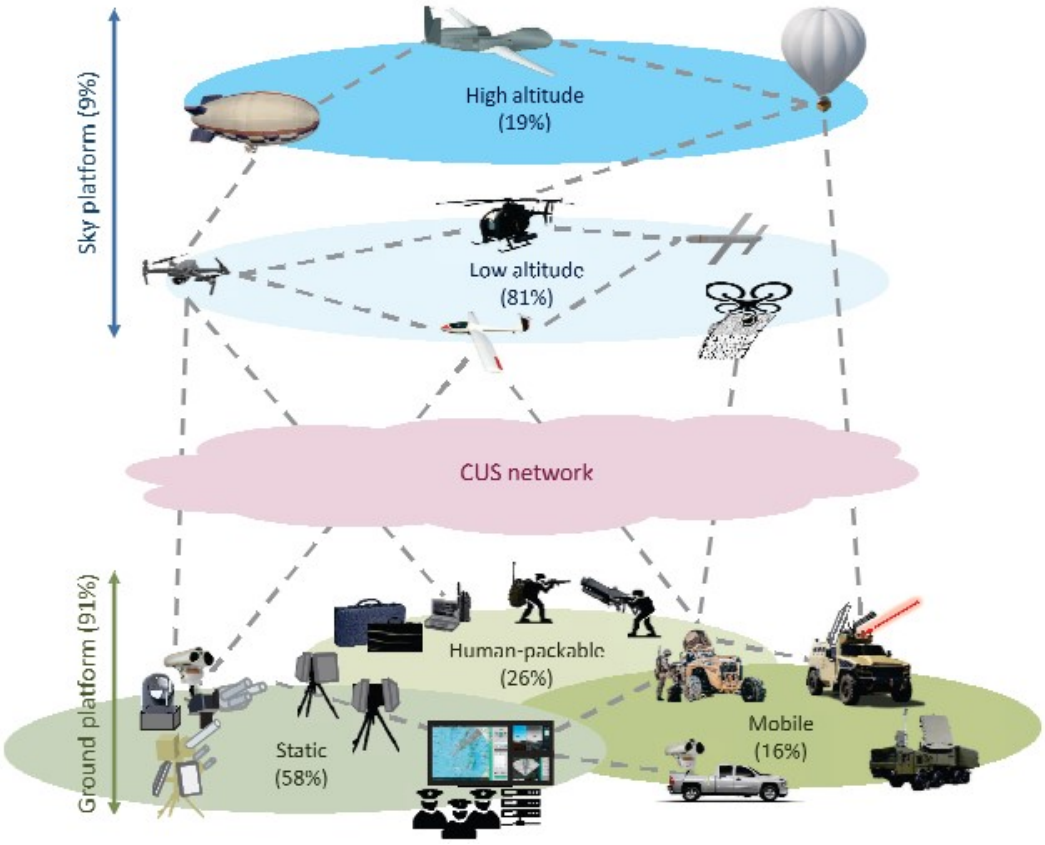
Ανακάλυψη και εκμετάλλευση ευπαθειών στο δίκτυο: Αναζήτηση αδυναμιών στην ασφάλεια των δικτύων που συνδέουν τα UAV, όπως ευπάθειες στους δρομολογητές, τα πρωτόκολλα δικτύου, τα συστήματα αυθεντικοποίησης .

Κατασκοπεία κίνησης και παρεμβολή: Παρακολούθηση της κίνησης των UAV και ανίχνευση των ευπαθειών στην επικοινωνία τους, με σκοπό την παρεμβολή και την αποκόμιση πληροφοριών ή τον έλεγχο του UAV.

Επίθεση με χρήση κακόβουλου λογισμικού (malware): Εγκατάσταση κακόβουλου λογισμικού στο UAV ή στα συστήματα ελέγχου του, με σκοπό τον έλεγχο του UAV ή την απώλεια πληροφοριών του.

Αναίρεση ή παρεμπόδιση της επικοινωνίας: Παρεμπόδιση ή διακοπή των συνδέσεων επικοινωνίας μεταξύ του UAV και των εδαφικών σταθμών ελέγχου, με σκοπό την απώλεια ελέγχου ή την απομόνωση του UAV.

19. Δίκτυα CUS- Επίγειες πλατφόρμες και πλατφόρμες Sky



Σχήμα 17. Επίγειες πλατφόρμες και πλατφόρμες Sky-Δίκτυο CUS [20]

Για την αντιμετώπιση των τεχνολογικά προηγμένων Drone απαιτείται ένα προηγμένο αμυντικό αντι-Drone σύστημα για την ενεργό προστασία της ασφάλειας, της περιουσίας και της ζωής. Τα αμυντικά αυτά συστήματα αποτελούνται από μέτρα πρόληψης ανεπιθύμητων περιστατικών, εγκλημάτων και επιθέσεων από την κακή χρήση μη συμμαχικών αεροσκαφών (UAV). Τα συστήματα αυτά αναφέρονται και ως CUS(Counter UAS Systems). Ένα CUS ανιχνεύει, αναγνωρίζει, παρακολουθεί και μετριάζει τα UAVs, ενώ μπορεί επίσης να εντοπίσει τον πιλότο του UAV. Οι πλατφόρμες των CUS κατηγοριοποιούνται σε δύο κατηγορίες: πλατφόρμες εδάφους και πλατφόρμες αέρος, όπως φαίνεται στο πάνω σχήμα . Οι πλατφόρμες εδάφους και αέρος λειτουργούν στο έδαφος και στον αέρα αντίστοιχα. Οι επίγειες πλατφόρμες μπορούν να χωριστούν περαιτέρω σε στατικές πλατφόρμες, κινητές πλατφόρμες εδάφους και φορητές(χειρός)

Α)Πλατφόρμες Εδάφους:

Οι πλατφόρμες εδάφους ταξινομούνται σε τρεις κατηγορίες σύμφωνα με τη μέθοδο λειτουργίας τους. Υπάρχουν οι πλατφόρμες στατικής γείωσης, οι οποίες είναι συνήθως βαριές και λειτουργούν σε μια σταθερή θέση. Δεύτερον, υπάρχουν οι κινητές πλατφόρμες εδάφους, οι οποίες είναι τοποθετημένες σε όχημα και μπορούν να λειτουργήσουν είτε

κινούμενες είτε σε σταθερή τοποθεσία. Τέλος, υπάρχουν οι πλατφόρμες που μπορούν να συσκευαστούν από τον άνθρωπο, γνωστές και ως χειροκίνητες ή φορητές πλατφόρμες. Αυτές οι πλατφόρμες είναι συμπαγείς και φορητές, επιτρέποντας τη μεταφορά και τη λειτουργία τους από άνθρωπο.

Σχήμα 18. RIFF-P Anti-Drone.Φορητό σύστημα χειρός [21]

Τα αντι-drone συστήματα CUS προσπαθούν να περιορίσουν και να αποτρέψουν τα UAV, ενώ τα UAV προσπαθούν να ολοκληρώσουν τις κακόβουλες αποστολές τους, όπως να φτάσουν στον προορισμό τους για να εκτελέσουν επιβλαβή συμπεριφορά. Τα UAV μπορεί να επιλέξουν μια διαδρομή που δεν είναι απαραίτητα η συντομότερη, αλλά η πιο κατάλληλη για την επίτευξη των κακόβουλων αποστολών τους, λαμβάνοντας υπόψη την αντίδραση του CUS. Αντίστοιχα, το CUS μπορεί να προβλέψει την κακόβουλη συμπεριφορά των UAV και να καθορίσει αποτελεσματικές στρατηγικές άμυνας.

Α1)Στατικές Αντι-Drone Πλατφόρμες Εδάφους:

Οι στατικές επίγειες πλατφόρμες των CUS αποτελούν την πλειονότητα (περίπου 60%) και έχουν σχεδιαστεί για να λειτουργούν ως σταθερές εγκαταστάσεις σε διάφορα περιβάλλοντα όπως αεροδρόμια, πυρηνικοί σταθμοί, διυλιστήρια πετρελαίου, κυβερνητικές εγκαταστάσεις και νοικοκυριά. Αυτοί οι τύποι πλατφόρμας έχουν λιγότερους περιορισμούς σε μέγεθος, βάρος και ισχύ . Είναι περίπλοκες κατασκευές και αποτελεσματικές, και μπορούν να προσαρμοστούν για να εκτελούν συγκεκριμένες εργασίες

σχετικά με την άμυνα απέναντι σε UAV. Ωστόσο, οι στατικές πλατφόρμες εδάφους είναι λιγότερο ευέλικτες στο να αντιμετωπίσουν απρόβλεπτες απειλές από UAV.

Α2)Κινητές Αντι-Drone Πλατφόρμες:

Οι κινητές επίγειες πλατφόρμες των CUS αποτελούν περίπου το 18% των συνολικών CUS και είναι τοποθετημένες σε οχήματα εδάφους. Αυτές οι πλατφόρμες επιτρέπουν την ευελιξία στην ανάπτυξη στόχων, χρησιμοποιώντας την κινητικότητα των οχημάτων. Είναι κατάλληλες για χρήση σε πεδία μάχης και σε δυναμικά και απρόβλεπτα περιβάλλοντα. Ωστόσο, σε σύγκριση με τις στατικές πλατφόρμες εδάφους, οι κινητές πλατφόρμες έχουν περιορισμούς σε μέγεθος, βάρος και ισχύ. Αυτό σημαίνει ότι οι διαθέσιμες δυνατότητες και οι τύποι συστημάτων ανίχνευσης και αποτελεσματικότητας μπορεί να είναι περιορισμένες σε αυτές τις πλατφόρμες. Επίσης, η χρήση των κινητών πλατφορμών εδάφους επηρεάζονται από τις δυνατότητες των οχημάτων που τις φέρουν.

Α3)Φορητές Πλατφόρμες ως Ανθρώπινος Εξοπλισμός:

Οι φορητές πλατφόρμες για ανθρώπους στο πλαίσιο των CUS αποτελούν περίπου το 22% του συνόλου των CUS. Αυτές οι πλατφόρμες έχουν σχεδιαστεί για να λειτουργούν από ένα άτομο με το χέρι. Οι περισσότερες από αυτές τις φορητές πλατφόρμες με συστήματα ανίχνευσης μοιάζουν με σακίδιο ή χαρτοφύλακα, ενώ αυτές με συστήματα παρεμβολής μοιάζουν με τουφέκια. Οι πλατφόρμες αυτές είναι ελαφριές και μπορούν να μεταφερθούν από ένα άτομο, γεγονός που τις καθιστά φορητές. Οι συνήθεις μορφές παρεμβολής που χρησιμοποιούνται είναι οι παρεμβολές RF και GNSS.

Β) Εναέριες Πλατφόρμες (Sky Platforms):

Οι εναέριες πλατφόρμες αναφέρονται σε συστήματα που τοποθετούνται σε διάφορα UAV , όπως αερόπλοια, μπαλόνια, αεροσκάφη με σταθερά πτερύγια και αεροσκάφη με περιστροφικά φτερά(πολυκόπτερα). Λόγω της ικανότητάς τους να ελιχθούν στον αέρα, μπορούν να τοποθετηθούν στον χώρο ευέλικτα ανάλογα με τις ανάγκες. Οι πλατφόρμες αυτές είναι ακόμη πιο ευέλικτες και γρήγορες από τις κινητές πλατφόρμες εδάφους.Οι πλατφόρμες αυτές εκμεταλλεύονται την ευελιξία τους και μπορούν να χρησιμοποιηθούν ως πολλαπλά UAV καταδιώξεων, τα οποία παρακολουθούν και καταδιώκουν τα επιτιθέμενα UAV.

Όσον αφορά τις εναέριες πλατφόρμες , έχουν κάποιους περιορισμούς σε σύγκριση με τις πλατφόρμες εδάφους επειδή διαθέτουν περιορισμένο ωφέλιμο φορτίο και καυσίμων ή ισχύ μπαταρίας, γεγονός που σημαίνει ότι μπορούν να μεταφέρουν μόνο ελαφριά και χαμηλής ισχύος συστήματα ανίχνευσης ή/και συστήματα παρεμβολής. Οι πλατφόρμες αυτές απαιτούν ασύρματες συνδέσεις και συστήματα επικοινωνίας αέρος-εδάφους. Η

αρχιτεκτονική επικοινωνίας μπορεί να είναι είτε ένα ad-hoc δίκτυο χωρίς υποδομή, είτε ένα κεντρικό δίκτυο με έναν κεντρικό κόμβο δικτύου. Αυτές οι απαιτήσεις και περιορισμοί στο φορτίο και την ισχύ μπαταρίας καθιστούν τις πλατφόρμες αυτές πιο απαιτητικές στην υλοποίηση σε σύγκριση με τις πλατφόρμες εδάφους.

Β1)Πλατφόρμες Χαμηλού Υψόμετρου (Low Altitude Platforms-LAPS):

Τα Low-Altitude Platforms (LAP) αναπτύσσονται για να αντιμετωπίσουν αποτελεσματικά τα UAV σε χαμηλά υψόμετρα, κυμαινόμενα από λίγα μέτρα έως μερικά χιλιόμετρα. Τα LAP είναι πιο προσιτά και η διαδικασία ανάπτυξής τους είναι πιο γρήγορη και ευέλικτη σε σύγκριση με τα High-Altitude Platforms (HAP). Λόγω της υψηλής ευελιξίας και της οικονομικότερης δυνατότητας εκτέλεσης αποστολών, τα LAP μπορούν να διαδραματίσουν σημαντικό ρόλο ως μέρος ενός ολοκληρωμένου συστήματος παρακολούθησης και ασφάλειας.

Τα LAP είναι συνήθως ελαφριά σε σχέση με τα HAP και, συνεπώς, έχουν περιορισμένο ωφέλιμο φορτίο και ενεργειακή χωρητικότητα. Για να αντιμετωπιστούν αυτοί οι περιορισμοί, έχουν γίνει εκτενείς έρευνες για τον σχεδιασμό ενεργειακά αποδοτικών UAV. Επιπλέον, έχουν προταθεί διάφορες μέθοδοι για την αντιμετώπιση του περιορισμένου ενεργειακού/ισχύος, όπως σε σμήνη πολλαπλών UAV, για τη γρήγορη αντικατάσταση των μπαταριών, την ασύρματη μετάδοση ισχύος και τη χρήση δεμένων (tether) UAV όπου λαμβάνουν ισχύ μέσω καλωδίου. Τα συνδεδεμένα UAV μπορούν επίσης να έχουν ενσύρματη σύνδεση επικοινωνίας για αξιόπιστη και ασφαλή επικοινωνία.

Τα περισσότερα LAP που ασχολούνται με τα UAV είναι εξοπλισμένα με συστήματα αποτροπής μόνο. Ο τυπικός τρόπος αποτροπής ενός LAP περιλαμβάνει τη χρήση διχτύου ή άλλου UAV για αντιμετώπιση του απειλούντος UAV. Ωστόσο, ένα μικρό ποσοστό των LAP διαθέτει ένα σύστημα ανίχνευσης, συνήθως με έναν αισθητήρα EO και/ή IR. Παρά την δυνατότητα εξοπλισμού των LAP με συστήματα ανίχνευσης και αποτροπής, η απόδοσή τους εξακολουθεί να είναι περιορισμένη, εκτός αν συνεργάζονται με άλλους τύπους επίγειων πλατφορμών.

Β2)Πλατφόρμες Υψηλού Υψόμετρου(High Altitude Platform-HAP):

Τα High-Altitude Platforms (HAP) είναι αεροσκάφη είτε μη επανδρωμένα drone που πετούν σε υψηλά υψόμετρα, φτάνοντας έως και δεκάδες χιλιόμετρα. Λόγω της μεγαλύτερης ευελιξίας στην εξοπλισμένη πλατφόρμα, τα HAP μπορούν να φέρουν περισσότερα συστήματα, όπως συστήματα επικοινωνίας και συστήματα μπαταρίας/καυσίμου, αναπτύσσοντας μεγαλύτερη αυτονομία και δυνατότητες.

Σε σύγκριση με τα LAP, τα HAP μπορούν να πετούν για μεγαλύτερα χρονικά διαστήματα και σε υψηλότερα υψόμετρα, προσφέροντας μεγαλύτερη εμβέλεια επικοινωνίας και ευρύτερο οπτικό πεδίο λόγω της λειτουργίας τους σε μεγάλο υψόμετρο και της υψηλής πιθανότητας

εμφάνισης επικοινωνιακής οπτικής επαφής (LOS). Αυτό καθιστά τα HAP αποτελεσματικά στην αντιμετώπιση UAV που προσεγγίζουν από μεγάλα υψόμετρα, ενώ μπορούν επίσης να υποστηρίξουν και άλλες πλατφόρμες.

Ωστόσο, τα HAP είναι πιο δαπανηρά και προκαλούν μεγαλύτερες προκλήσεις στη λειτουργία τους σε σύγκριση με τα LAP. Επιπλέον, η ανάπτυξη των HAP απαιτεί περισσότερο χρόνο σε σύγκριση με την ανάπτυξη των LAP.

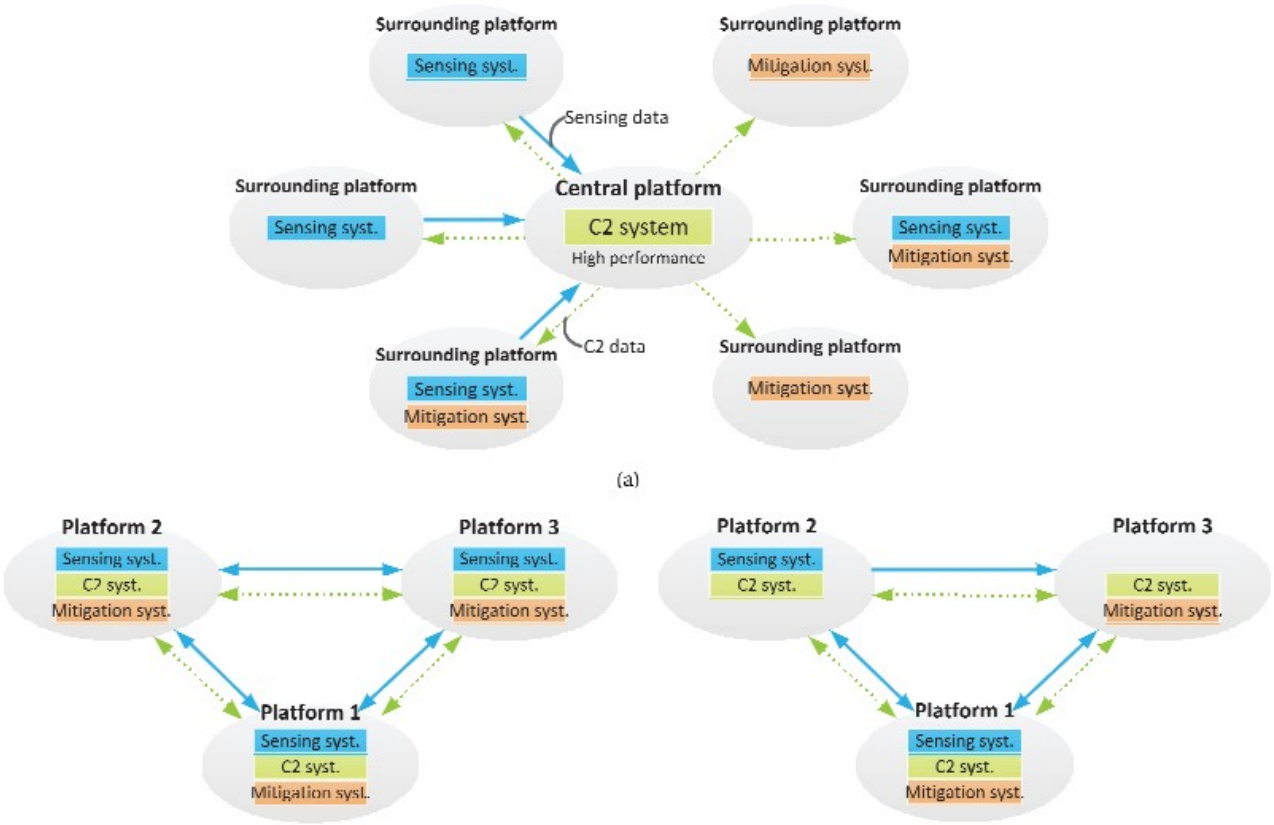
Τα τυπικά High-Altitude Platforms (HAP) είναι εξοπλισμένα με συστήματα ανίχνευσης και αποτροπής, παρέχοντας ολοκληρωμένες δυνατότητες για την αντιμετώπιση απειλών. Τα συστήματα ανίχνευσης περιλαμβάνουν διάφορους τύπους αισθητήρων, όπως οπτικούς (EO), υπέρυθρους (IO) και ραντάρ, ενώ οι μέθοδοι μετριασμού περιλαμβάνουν τη χρήση βλημάτων. Από την άλλη πλευρά, τα HAP που χρησιμοποιούνται για επιτήρηση είναι εξοπλισμένα μόνο με συστήματα ανίχνευσης.

Τα HAP έχουν υποστεί εκτεταμένη μελέτη και ανάπτυξη για να υποστηρίξουν και να συνεργαστούν με άλλες πλατφόρμες. Σε αυτές τις περιπτώσεις, οι δορυφορικές επικοινωνίες μπορούν να θεωρηθούν ως το στοιχείο που συνδέει πολλαπλές πλατφόρμες πέρα από τα HAP. Αυτή η ολοκληρωμένη προσέγγιση επιτρέπει τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ διάφορων πλατφορμών, επιτρέποντας την αποτελεσματική λειτουργία και εκτέλεση αποστολών.

Συνολικά, τα HAP αποτελούν προηγμένες πλατφόρμες υψηλής τεχνολογίας με ευρεία εφαρμογή στον τομέα των επικοινωνιών και της παρακολούθησης. Με την ικανότητά τους να λειτουργούν σε υψηλά υψόμετρα και να επιτυγχάνουν ευρύτερο εύρος επικοινωνίας και οπτικού πεδίου, τα HAP μπορούν να ανταποκριθούν αποτελεσματικά σε προκλήσεις και απειλές που προκύπτουν από αεροπορικά οχήματα χαμηλού υψομέτρου (UAV) και να παρέχουν υποστήριξη σε άλλες πλατφόρμες.

Γ) Υβριδικά CUS Δίκτυα:

Το υβριδικό CUS Δίκτυο αναπαριστά μια υβριδική πλατφόρμα που συνδυάζει συστήματα εδάφους και αέρος, επιτρέποντας την αντιστάθμιση των ελλείψεων και την αξιοποίηση των πλεονεκτημάτων κάθε συστήματος. Με την αξιοποίηση των πλεονεκτημάτων των συστημάτων εδάφους και αέρος, οι υβριδικές πλατφόρμες μπορούν να βελτιώσουν σημαντικά την απόδοση των CUS. Οι υβριδικές πλατφόρμες συνήθως περιλαμβάνουν συστήματα ανίχνευσης και αποτροπής, καθώς και διάφορους τύπους αισθητήρων και πομπών. Η ικανότητα ενός ολοκληρωμένου CUS καθορίζεται όχι μόνο από την απόδοση κάθε μεμονωμένης πλατφόρμας, αλλά και από τις ιδιότητες του συνολικού συστήματος δικτύων. Ένα δίκτυο μπορεί να ενισχύσει τη συνεργασία μεταξύ των πλατφορμών και να μεγιστοποιήσει την αποτελεσματικότητα του CUS. Τα ολοκληρωμένα δίκτυα μπορούν να κατηγοριοποιηθούν σε κεντρικά και αποκεντρωμένα δίκτυα, ανάλογα με τον βαθμό ομοιογένειας των πλατφορμών.



Σχήμα 19. Δίκτυα CUS: (α) κεντρικό δίκτυο, (κάτω αριστερά) αποκεντρωμένο ομοιογενές δίκτυο και (κάτω δεξιά) αποκεντρωμένο ετερογενές δίκτυο [17].

Συνολικά, το CUS δίκτυο προσφέρει μια ευέλικτη και αποδοτική λύση, εκμεταλλευόμενο τις δυνατότητες και των δύο συστημάτων (εδάφους και αέρος) για να παράσχει βελτιωμένη λειτουργικότητα και απόδοση στο πλαίσιο των CUS.

20. Αρχιτεκτονική Αντι-Drone Τεχνολογίας CUS

Η ενσωματωμένη αρχιτεκτονική του CUS (Counter Unmanned Systems) μπορεί να κατηγοριοποιηθεί σε τρεις τύπους βάσει των ρόλων τους .

Συστήματα Ανίχνευσης C1: Αυτά τα συστήματα συλλέγουν δεδομένα από το περιβάλλον και μεταδίδουν τα παρατηρούμενα δεδομένα στα συστήματα C2. Ο ρόλος τους είναι να ανιχνεύουν και να συλλέγουν πληροφορίες για το περιβάλλον, όπως ανίχνευση αντικειμένων ή αναγνώριση UAV, και να τις μεταδίδουν στα συστήματα C2 για περαιτέρω επεξεργασία.

Συστήματα C2: Αυτά τα συστήματα εκτελούν υπολογιστικές εργασίες και λαμβάνουν αποφάσεις βασιζόμενα στα δεδομένα που λαμβάνουν από τα συστήματα ανίχνευσης. Οι λειτουργίες τους περιλαμβάνουν αλγόριθμους ανίχνευσης/αναγνώρισης, παρακολούθησης/χαρτογράφησης και λήψη αποφάσεων, όπως δήλωση εντοπισμού/αναγνώρισης αντικειμένων, δήλωση εντοπισμού/παρακολούθησης και καθορισμός χρόνου και μεθόδου εξουδετέρωσης των UAV.

Συστήματα Μετριασμού C3: Αυτά τα συστήματα είναι υπεύθυνα για την αντιμετώπιση και εξουδετέρωση των UAV, βασιζόμενα στις αποφάσεις που λαμβάνονται από τα συστήματα C2. Οι λειτουργίες τους περιλαμβάνουν την ανίχνευση και εξουδετέρωση των UAV με βάση τις αποφάσεις που παίρνονται από τα συστήματα C2.

Κάθε ένα από αυτά τα συστήματα μπορεί να είναι εξοπλισμένο με μία ή περισσότερες πλατφόρμες. Από την άλλη πλευρά, μια πλατφόρμα μπορεί να χρησιμοποιεί πολλαπλά συστήματα, σχηματίζοντας μια ολοκληρωμένη αρχιτεκτονική. Ωστόσο, λόγω των απαιτήσεων αυτονομίας για την αποτελεσματική λειτουργία του CUS, λίγες εφαρμογές πλατφόρμας χρησιμοποιούν αυτόν τον ενσωματωμένο τύπο αρχιτεκτονικής. Οι περιορισμοί αυτοί αντισταθμίζονται μέσω του δικτύου αλληλεπίδρασης μεταξύ των πλατφορμών, το οποίο ενισχύει τη συνεργασία και την απόδοση του CUS.

A. C1 Systems:

Συλλογή Δεδομένων (Gathering Data) :

Η συλλογή δεδομένων αποτελεί σημαντικό κομμάτι των συστημάτων ανίχνευσης. Τα συστήματα αυτά μπορούν να αξιοποιήσουν διάφορες μεθόδους για τη συλλογή δεδομένων, συμπεριλαμβανομένων των ηχητικών κυμάτων, των ραδιοκυμάτων και των φωτεινών κυμάτων. Αυτά τα δεδομένα κυμάτων μπορούν να ληφθούν μέσω διάφορων τύπων συσκευών και αισθητήρων, προσφέροντας διαφορετικές δυνατότητες ανίχνευσης και συλλογής πληροφοριών. Ορισμένες από αυτές τις συσκευές περιλαμβάνουν: Σόναρ, Αισθητήρες ακουστικών/υπερήχων, Ραντάρ, Αισθητήρες ραδιοσυχνοτήτων, LiDAR. Αυτές οι συσκευές συνεργάζονται για να συλλέξουν πληροφορίες από το περιβάλλον και να τις παράσχουν στα συστήματα C2 για επεξεργασία και λήψη αποφάσεων. Η ενσωμάτωση διαφόρων τύπων αισθητήρων επιτρέπει στα συστήματα ανίχνευσης να αποκτήσουν πληρέστερη και πολυσύνθετη πληροφορία για το περιβάλλον και τα αντικείμενα που ανιχνεύουν.

Δεδομένα ηχητικών κυμάτων:

Τα ηχητικά κύματα είναι μηχανικά κύματα που περιλαμβάνουν τρεις κατηγορίες: τα υπερήχων, τα ακουστικά και τα υπερηχητικά κύματα. Οι υπέρηχοι αναφέρονται σε κύματα με συχνότητες μέχρι 20 Hz, τα ακουστικά κύματα κυμαίνονται μεταξύ 20 Hz και 20 kHz, ενώ τα υπερηχητικά κύματα έχουν συχνότητες πάνω από 20 kHz, φτάνοντας μέχρι τα GHz.

Οι ηχητικές κυματικές ταχύτητες είναι χαμηλότερες από αυτές των ηλεκτρομαγνητικών κυμάτων, όπως τα ραδιοκύματα και το φως. Τα ηχητικά κύματα είναι διαμήκη και δεν μπορούν να πολωθούν, γεγονός που τα διαφοροποιεί από τα ηλεκτρομαγνητικά κύματα.Για να διαδοθούν, τα ηχητικά κύματα απαιτούν ένα μέσο, όπως ο αέρας ή το νερό. Αυτό σημαίνει ότι για να μεταδοθούν και να ανιχνευθούν, τα ηχητικά κύματα χρειάζονται ένα μέσο διάδοσης.Η συλλογή δεδομένων ηχητικών κυμάτων μπορεί να βελτιώσει την αξιοπιστία των συστημάτων ανίχνευσης παρέχοντας επιπλέον πληροφορίες σε συνδυασμό με τα δεδομένα ηλεκτρομαγνητικών κυμάτων (EM). Η προσθήκη δεδομένων ηχητικών κυμάτων μπορεί να ενισχύσει την ακρίβεια και την ευαισθησία των συστημάτων ανίχνευσης, παρέχοντας πληροφορίες για την παρουσία, τη θέση και τα χαρακτηριστικά των ανιχνευόμενων αντικειμένων.

Για την ακρόαση των ηχητικών δεδομένων, χρησιμοποιούνται ενεργοί αισθητήρες, όπως τα βυθόμετρα, ενώ οι ακουστικοί/υπερηχητικοί αισθητήρες λειτουργούν παθητικά. Οι ακουστικοί/υπερηχητικοί αισθητήρες χρησιμοποιούνται ευρέως για την ανίχνευση αντικειμένων UAV, καθώς παρέχουν αξιόπιστα δεδομένα και ευκολία στην ανίχνευση.Αντίθετα, το σόναρ χρησιμοποιείται συνήθως για εφαρμογές υποβρύχιας πλοήγησης και επικοινωνίας, καθώς η διάδοση των ηχητικών κυμάτων στον αέρα είναι περιορισμένη. Έτσι, οι ακουστικοί/υπερηχητικοί αισθητήρες αποτελούν συνήθως την προτιμώμενη επιλογή για την ανίχνευση UAV.

Δεδομένα ραδιοκυμάτων (Radio wave data):

Τα ραδιοκύματα αποτελούνται από κύματα στο ηλεκτρομαγνητικό φάσμα, τα οποία κυμαίνονται συνήθως στην περιοχή συχνοτήτων από 3 MHz έως 300 GHz. Η πληροφορία που μεταφέρεται μέσω των ραδιοκυμάτων έχει χρησιμοποιηθεί ευρέως για την ανίχνευση UAV. Σε αυτήν την περίπτωση, οι πληροφορίες σχετικά με την κατάσταση του ασύρματου καναλιού είναι κρίσιμες για την ανάκτηση των πληροφοριών από τα ραδιοκύματα.Για παράδειγμα, η απώλεια διαδρομής είναι μια σημαντική μέτρηση για τον προσδιορισμό της παρουσίας των UAV. Στην ανίχνευση UAV στον αέρα, είναι σημαντικό να γνωρίζουμε τα ραδιοφωνικά κανάλια αέρος-εδάφους (A2G) και αέρος-αέρος (A2A). Τα μοντέλα καναλιού A2G και A2A διαφέρουν από τα παραδοσιακά επίγεια κανάλια. Τα κανάλια A2G μπορούν να χαρακτηριστούν από την ύπαρξη ή μη άμεσης οπτικής επαφής (LOS) μεταξύ του αντικειμένου (UAV) και του δέκτη. Επιπλέον, τα κανάλια A2G αναλύονται σε σχέση με την πιθανότητα της άμεσης οπτικής επαφής (LOS) ανάλογα με το περιβάλλον. Αντίθετα, τα κανάλια A2A τείνουν να έχουν χαμηλότερη απώλεια διαδρομής σε σύγκριση με τα κανάλια A2G και τα επίγεια κανάλια.

Επομένως, αξιοποιώντας την άμεση οπτική επαφή (LOS) στα κανάλια A2A, τα αεροσκάφη στον αέρα που είναι εξοπλισμένα με ραντάρ σύνθετου διαφράγματος ή αισθητήρες ραδιοσυχνοτήτων μπορούν να συλλέγουν αξιόπιστες πληροφορίες ραδιοκυμάτων. Ένας αισθητήρας ραδιοσυχνοτήτων συλλέγει τα περιβαλλοντικά ραδιοσήματα που εκπέμπονται από τα UAV, λειτουργώντας ως παθητικός αισθητήρας.

Δεδομένα φωτεινών κυμάτων(Light wave data):

Τα δεδομένα φωτεινών κυμάτων παρουσιάζουν ορισμένες διαφορές σε σχέση με τα δεδομένα ραδιοκυμάτων. Τα φωτεινά κύματα έχουν υψηλότερες συχνότητες και μικρότερα μήκη κύματος σε σύγκριση με τα ραδιοκύματα. Το φάσμα του φωτός περιλαμβάνει το υπέρυθρο φως (300 GHz - 430 THz) και το οπτικό φως (430 THz - 750 THz). Η μικρότερη εμβέλεια των φωτεινών κυμάτων σε σύγκριση με τα ραδιοκύματα σημαίνει ότι τα φωτεινά κύματα μπορούν να μεταδοθούν μόνο σε σχετικά μικρές αποστάσεις. Ωστόσο, λόγω του μικρότερου μήκους κύματος και της υψηλότερης συχνότητας, τα φωτεινά κύματα προσφέρουν καλύτερη ανάλυση σε σύγκριση με τα ραδιοκύματα.Έτσι, τα φωτεινά κύματα επηρεάζονται από διάφορα καιρικά φαινόμενα, όπως σύννεφα, ομίχλη, βροχή, χιόνι, χιονόνερο και άμεσο ηλιακό φως, λόγω του μικρού μήκους κύματος τους. Επίσης, η παροχή οπτικών εικόνων υψηλής ποιότητας μπορεί να είναι περιορισμένη σε συνθήκες χαμηλού φωτισμού, όπως τη νύχτα ή τις συννεφιασμένες μέρες.

Η υπέρυθρη ακτινοβολία εκπέμπεται από αντικείμενα σύμφωνα με το νόμο ακτινοβολίας μαύρου σώματος, επιτρέποντας την ανίχνευση της θερμοκρασίας ανεξάρτητα από τον βαθμό ορατού φωτισμού. Ωστόσο, οι υπέρυθρες εικόνες επηρεάζονται από την εκπομπή και την ανάκλαση του ηλιακού φωτός.

Τόσο οι αισθητήρες LiDAR όσο και οι αισθητήρες EO/IR χρησιμοποιούνται ευρέως για τη συλλογή δεδομένων φωτός. Οι αισθητήρες LiDAR χρησιμοποιούν την αποστολή και την ανίχνευση των επαναλαμβανόμενων παλμών φωτός για την ανίχνευση και τη διάταξη των αντικειμένων. Οι αισθητήρες EO/IR ανιχνεύουν και εγγράφουν την οπτική και υπέρυθρη ενέργεια για την ανάλυση του περιβάλλοντος.Συνολικά, τα φωτεινά κύματα παρέχουν διαφορετικές δυνατότητες συλλογής δεδομένων σε σύγκριση με τα ραδιοκύματα. Ενώ έχουν μικρότερη εμβέλεια, προσφέρουν υψηλότερη ανάλυση και δυνατότητα ανίχνευσης θερμοκρασίας. Η επιλογή του κατάλληλου αισθητήρα εξαρτάται από τις απαιτήσεις της συγκεκριμένης εφαρμογής και το περιβάλλον στο οποίο λειτουργεί.

Συγχώνευση Δεδομένων(Data Fusion):

Η συγχώνευση δεδομένων αποτελεί μια προσέγγιση που χρησιμοποιείται για να αντισταθμιστούν οι περιορισμοί των μεμονωμένων τύπων αισθητήρων και να επιτευχθεί ακριβής και αξιόπιστη ανίχνευση, εντοπισμός, αναγνώριση και παρακολούθηση. Αντί να βασίζεται μόνο σε έναν τύπο αισθητήρα ή σε πανομοιότυπους αισθητήρες, η συγχώνευση δεδομένων συνδυάζει πολλαπλούς τύπους αισθητήρων και πηγές πληροφορίας για να παρέχει ολοκληρωμένη πληροφορία ανίχνευσης.

Η συγχώνευση δεδομένων μπορεί να κατηγοριοποιηθεί με βάση διάφορα κριτήρια. Ένα από αυτά είναι ο τύπος των πληροφοριών πηγής, που μπορεί να είναι περιττές

πληροφορίες που σχετίζονται με τον ίδιο στόχο, συμπληρωματικές πληροφορίες από διαφορετικές πηγές ή συνδυαστικές πληροφορίες που χρησιμοποιούνται για τη δημιουργία νέων πληροφοριών. Η συγχώνευση δεδομένων μπορεί επίσης να ταξινομηθεί βάσει του τύπου των αλγορίθμων που χρησιμοποιούνται για την επεξεργασία των δεδομένων. Οι κύριοι τύποι αλγορίθμων συγχώνευσης δεδομένων περιλαμβάνουν την απλή συνένωση (συγχώνευση) δεδομένων, τον υπολογισμό στατιστικών παραμέτρων όπως ο μέσος όρος και η διακύμανση, τον υπολογισμό πιθανοτήτων και πιθανοτικών μοντέλων, καθώς και τη χρήση μη γραμμικών αλγορίθμων όπως νευρωνικά δίκτυα και μηχανές υποστήριξης δεδομένων.

B) C2 Ssstems:

Τα C2 Systems είναι συνήθως μια κεντρική πλατφόρμα που προσφέρει ευέλικτη λειτουργικότητα και εκτελεί πολλούς ρόλους σε ένα σύστημα. Αν και τεχνικά διακρίνεται από ένα μόνο σύστημα C2, το υλικό και το λογισμικό του μπορεί να ενσωματωθεί σε πολλές πλατφόρμες. Οι διάφοροι τύποι αρχιτεκτονικής συστημάτων C2 μπορούν να διαδοθούν σε πολλαπλές πλατφόρμες, και κάθε πλατφόρμα μπορεί να λειτουργεί αυτόνομα και να λαμβάνει αποφάσεις μεμονωμένα. Ένα σύστημα C2 αποτελεί μια βασική μονάδα επεξεργασίας που μπορεί να συντονίσει πολλές πλατφόρμες για την επίτευξη της κορυφαίας απόδοσης του CUS και να διαθέτει υψηλή υπολογιστική ισχύ.

Τα συστήματα C2 λαμβάνουν αποφάσεις σχετικά με τις απαιτούμενες εργασίες, όπως το συντονισμό και οι επίπεδα απειλής των κινούμενων UAV και εκτελούν υπολογισμούς για τον συντονισμό και τις αποφάσεις αυτές. Το επίπεδο απειλής μπορεί να καθοριστεί βάσει των εξής κριτηρίων:

-την απόσταση μεταξύ του UAV και της περιοχής προστασίας,

-την ταχύτητα και την κατεύθυνση του UAV,

-το φορτίο που μεταφέρεται από το UAV (π.χ. εκρηκτικά),

-το μέγεθος και τον τύπο του UAV, και

-τα χαρακτηριστικά της περιοχής προστασίας.

Με βάση αυτά τα κριτήρια, το επίπεδο απειλής κατατάσσεται ως εξής:

-Επίπεδο 1 (Χαμηλό): Η απειλή είναι απίθανη.

-Επίπεδο 2 (Μέτριο): Η απειλή είναι πιθανή, αλλά όχι βέβαιη.

-Επίπεδο 3 (Ουσιαστικό): Η απειλή έχει υψηλή πιθανότητα να συμβεί.

- Επίπεδο 4 (Σοβαρό): Η απειλή είναι πολύ πιθανή.

- Επίπεδο 5 (Κρίσιμο): Η απειλή αναμένεται άμεσα.

Τα συστήματα C2 μπορούν να λαμβάνουν αποφάσεις αυτόνομα ή να απαιτούν έγκαιρη ανθρώπινη παρέμβαση. Ωστόσο, η ανθρώπινη παρέμβαση μπορεί να αποτελέσει πρόκληση στην αντιμετώπιση των γρήγορα κινούμενων UAV.

21. Συντονισμός και Λειτουργία των CUS

1) Ανίχνευση/Αναγνώριση: Τα συστήματα C2 συλλέγουν δεδομένα από τα συστήματα ανίχνευσης για τον εντοπισμό ύποπτων αντικειμένων. Στη συνέχεια, πραγματοποιούν σύνταξη δεδομένων και λήψη αποφάσεων για το εάν το αντικείμενο είναι UAV ή άλλο μικρό αντικείμενο, όπως πουλί, χαρταετός ή μπαλόνι. Οι αποφάσεις μπορούν να βασιστούν σε ανεπεξέργαστα δεδομένα, χαρακτηριστικά ή τοπικές αποφάσεις. Επιπλέον, μπορούν να ταξινομήσουν το ωφέλιμο φορτίο που μεταφέρει το UAV για την καθορισμό του επιπέδου απειλής.

2) Εξουσιοδότηση: Μετά τον εντοπισμό ενός UAV, τα συστήματα C2 μπορούν να επαληθεύσουν εάν το UAV είναι εξουσιοδοτημένο ή όχι. Ανάλογα με την επαλήθευση, ενημερώνουν το επίπεδο απειλής του UAV.

3) Εντοπισμός: Εάν το επίπεδο απειλής υπερβαίνει ένα προκαθορισμένο επίπεδο, τα συστήματα C2 προσδιορίζουν την τοποθεσία του UAV και καταλήγουν εάν αυτό κινείται προς μια ευαίσθητη περιοχή,.

Μηχανισμός Αντιμετώπισης Παράνομων UAV: Τα συστήματα αποτροπής και αντιμετώπισης χρησιμοποιούνται για την αντιμετώπιση των απειλών που προκαλούν τα UAV. Αυτά τα συστήματα λειτουργούν όπως αναφέρθηκε βάσει του επιπέδου απειλής που καθορίζεται από το σύστημα C2 (Ελέγχου και Επικοινωνίας) αλλά και σύμφωνα με τους κανονισμούς των αρμόδιων αρχών.

Τα συστήματα μετριασμού μπορούν να ενεργοποιηθούν ταυτόχρονα και να συνεργαστούν για τον αποτελεσματική αντιμετώπιση των mUAV. Ανάλογα με το επίπεδο απειλής και τα αντίμετρα που απαιτούνται, τα συστήματα αποτροπής μπορούν να προειδοποιήσουν, να ελέγξουν, να διαταράξουν, να απενεργοποιήσουν και να καταστρέψουν τα UAV.

Οι πιθανές μέθοδοι αντιμετώπισης περιλαμβάνουν:

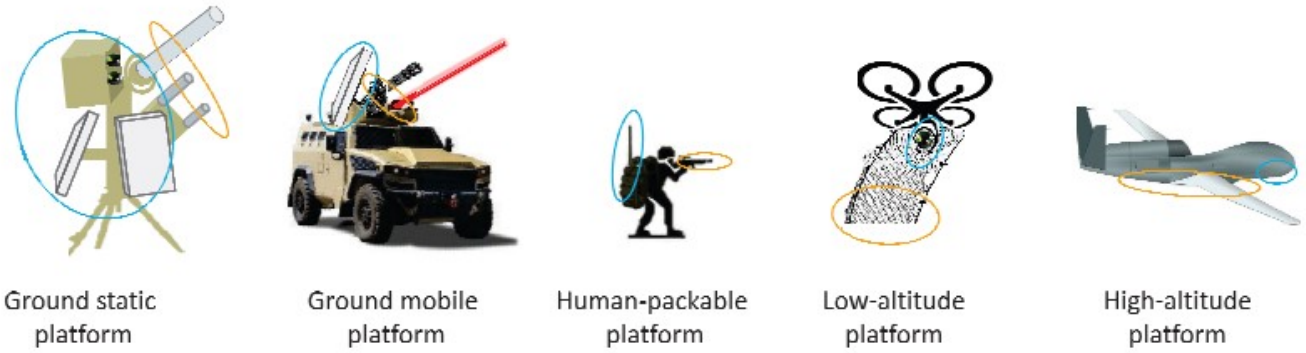
-Προειδοποίηση: Τα συστήματα αυτά μπορούν να προειδοποιήσουν τον χειριστή του UAV επικοινωνώντας με αυτόν με περιορισμένους όρους, όταν το επίπεδο απειλής είναι μέτριο

(Επίπεδο 2). Αυτή η προειδοποίηση μπορεί να γίνει μέσω ραντάρ ή αισθητήρων που ανιχνεύουν την παρουσία των UAV και μεταδίδουν πληροφορίες στον χειριστή.

-Ελέγχος: Οι μέθοδοι ελέγχου χρησιμοποιούνται για τον περιορισμό της κίνησης των UAV. Αυτό μπορεί να γίνει μέσω της αναγνώρισης και της παρέμβασης στο σήμα ελέγχου του UAV, περιορίζοντας την κίνησή του ή αναγκάζοντάς το να προσγειωθεί.

-Διατάραξη: Οι μέθοδοι διατάραξης χρησιμοποιούνται για τον περιορισμό των δυνατοτήτων επικοινωνίας του UAV. Αυτό μπορεί να γίνει μέσω της εκπομπής σημάτων παρεμβολής που παρεμβάλλονται στις συχνότητες που χρησιμοποιούνται από τα UAV για την επικοινωνία τους.

-Απενεργοποίηση: Οι μέθοδοι απενεργοποίησης χρησιμοποιούνται για την πρόκληση αποτυχίας ή απενεργοποίησης του drone. Αυτό μπορεί να γίνει μέσω της αναγνώρισης και της παρέμβαση με εκπομπή σήματος μέσω συχνοτήτων στο σύστημα ελέγχου του drone, καθιστώντας το ανίκανο να λειτουργήσει.



Σχήμα 20. Πλατφόρμες CUS [20]

Λειτουργία Αισθητήρων RF (RF Sensors): Οι αισθητήρες ραδιοσυχνοτήτων καταγράφουν τα σήματα ηλεκτρομαγνητικών κυμάτων που εκπέμπονται από τα drones ή τους απομακρυσμένους χειριστές, προκειμένου να ανιχνεύσουν τα UAV. Τα περισσότεροι εμπορικά UAV ελέγχονται εξ αποστάσεως από τους χειριστές τους. Αυτή η επικοινωνία μεταξύ των drone και των χειριστών περιλαμβάνει πληροφορίες τηλεχειρισμού και τηλεμετρίας, όπως υψόμετρο, θέση, διάρκεια ζωής της μπαταρίας και δεδομένα βίντεο. Έτσι, οι αισθητήρες ραδιοσυχνοτήτων μπορούν να ανιχνεύσουν τα UAV, εκτός αν αυτά είναι προ-προγραμματισμένα και αυτόνομα.

Οι αισθητήρες ραδιοσυχνοτήτων έχουν ευρεία εφαρμογή σε διάφορα συστήματα λόγω της απλότητας τους. Χρησιμοποιούν δέκτες Wi-Fi και ραδιοφωνικές πλακέτες που καθορίζονται από λογισμικό, οι αισθητήρες ραδιοσυχνοτήτων ακούνε τη σύνδεση μεταξύ του UAV και του χειριστή και καταγράφουν τα μοτίβα κίνησης του UAV για τον εντοπισμό του.

Παρόλο που οι αισθητήρες ραδιοσυχνοτήτων έχουν ευρεία χρήση, υπάρχουν ορισμένοι περιορισμοί. Οι αισθητήρες ραδιοσυχνοτήτων έχουν χαμηλή αξιοπιστία στην ανίχνευση του στόχου και υψηλά ποσοστά λανθασμένων συναγερμών. Επιπλέον, επειδή οι αισθητήρες ραδιοσυχνοτήτων είναι παθητικοί, δεν παρέχουν πληροφορίες σχετικά με την εμβέλεια των UAV. Επίσης, απαιτείται γνώση της ζώνης συχνοτήτων που χρησιμοποιείται για την ανίχνευση, καθώς και των πρωτοκόλλων διαμόρφωσης που χρησιμοποιούνται από τα Drone. Επιπλέον, η παρουσία άλλων σημάτων στην ίδια ζώνη συχνοτήτων με τα UAV, όπως ηλεκτρομαγνητικές παρεμβολές, δυσκολεύουν την ανίχνευση των drone βασιζόμενη σε ραδιοσυχνότητες. Για τη βελτίωση της απόδοσης ανίχνευσης, μπορεί να χρησιμοποιηθεί η ανίχνευση φάσματος για την απόκτηση πληροφοριών.

Λειτουργία Radar: Για τον προσδιορισμό της εμβέλειας, της γωνίας ή της ταχύτητας ενός drone, το ραντάρ χρησιμοποιείται ευρέως ως ενεργός αισθητήρας σε συστήματα ανίχνευσης σε έναν ανιχνευτή χώρου αναχαίτισης CUS. Ένα σύστημα ραντάρ αποτελείται από έναν πομπό, έναν δέκτη και έναν επεξεργαστή. Ο πομπός εκπέμπει σήματα ηλεκτρομαγνητικών κυμάτων (EM) με συχνότητα που κυμαίνεται συνήθως μεταξύ 3 MHz και 300 GHz, ανάλογα με την εφαρμογή. Τα σήματα EM αντανακλώνται από το UAV και επιστρέφουν στο ραντάρ. Τα επιστρεφόμενα σήματα EM που αντανακλώνται από το UAV παρέχουν βασικές πληροφορίες για τη θέση και την ταχύτητα του UAV. Έτσι, η ισχύς των ληφθέντων σημάτων είναι κρίσιμη για την απόδοση ανίχνευσης του ραντάρ. Ωστόσο, επειδή τα ανακλώμενα σήματα ραντάρ που λαμβάνονται από την κεραία του δέκτη είναι αδύναμα, απαιτείται ενίσχυση στον επεξεργαστή. Τα ανακλώμενα σήματα ραντάρ που λαμβάνονται από τον δέκτη υποβάλλονται σε διάφορες επεξεργαστικές τεχνικές για την εξαγωγή πληροφοριών. Ο επεξεργαστής αναλύει τα σήματα, εκτιμά την απόσταση, την κατεύθυνση, την ταχύτητα και άλλες παραμέτρους του UAV.

Στη συνέχεια, οι πληροφορίες που εξάγονται από τον επεξεργαστή μπορούν να χρησιμοποιηθούν για την αναγνώριση και την καταγραφή του UAV. Το σύστημα ραντάρ μπορεί να ειδοποιήσει τους χειριστές σχετικά με την παρουσία του UAV και να παράσχει πληροφορίες για την πορεία και την ταχύτητά του, αποτελώντας ένα σημαντικό εργαλείο για τη λήψη αποφάσεων.

Οι τεχνολογίες ραντάρ συνεχώς εξελίσσονται για να βελτιώσουν την απόδοση και την ακρίβεια της ανίχνευσης. Παραδείγματα προηγμένων τεχνολογιών ραντάρ περιλαμβάνουν το ανοικτό ραντάρ (SAR), το ραντάρ με σάρωση φάσης (Pulse-Doppler), και το ραντάρ με πολλαπλές κεραίες (MIMO). Αυτές οι τεχνολογίες επιτρέπουν μεγαλύτερη ακρίβεια, ευελιξία και ανίχνευση σε διάφορες συνθήκες λειτουργίας.

22. Ανάλυση Λειτουργίας RF/GNSS Jamming

Η παρεμβολή των ραδιοσυχνοτήτων (RF) και των συστημάτων πλοήγησης GNSS μπορεί να οδηγήσει στη διακοπή ή απενεργοποίηση των UAV μέσω της παρεμβολής στις επικοινωνίες τους. Η παρεμβολή μειώνει τον λόγο σήματος προς θόρυβο (SNR) του mUAV και μπορεί να προκαλέσει τη διακοπή της σύνδεσης μεταξύ των drone και των κακόβουλων χειριστών.Για να ανακτηθούν οι διαταραγμένες επικοινωνίες, το σήμα επικοινωνίας μεταξύ του UAV και των κακόβουλων χειριστών πρέπει να επανεκπεμφθεί , αλλά αυτό εκθέτει το UAV σε περαιτέρω επιθέσεις. Όταν η σύνδεση επικοινωνίας διακοπεί ή υποβαθμιστεί, τα UAV μπορεί να χάσουν τη σύνδεση με το τηλεχειριστήριο και να προβούν σε επιστροφή στο σημείο απογείωσης (RTH) ή ακόμα και να προσγειωθούν επί τόπου.

Υπάρχουν διάφορες μέθοδοι παρεμβολής. Ένας "jammer" μπορεί να μεταδώσει ολόκληρη την ισχύ του σε μία συχνότητα (spot jamming), να μετακινήσει γρήγορα την ισχύ από μία συχνότητα σε μία άλλη (sweep jamming) ή να μεταδώσει ισχύ σε ένα εύρος συχνοτήτων ταυτόχρονα (barrage jamming). Επιπλέον, οι παρεμβολές μπορούν να διακριθούν σε ενεργές παρεμβολές και αντιδραστικές παρεμβολές. Ένας ενεργός παρεμβολέας μεταδίδει συνεχώς σήματα ραδιοσυχνοτήτων ή το κάνει τυχαία για εξοικονόμηση ενέργειας. Ένας παραπλανητικός παρεμβολέας, που είναι ένας τύπος ενεργού παρεμβολέα, αναγκάζει το UAV να δέχεται συνεχώς πακέτα χωρίς κενά, έτσι ώστε το UAV να παραμένει σε λειτουργία λήψης. Αντιδραστικές παρεμβολές είναι όταν μεταδίδονται σήματα μόνο όταν ανιχνεύεται ότι τα παρακολουθούμενα φάσματα/κανάλια καταλαμβάνονται από άγνωστα σήματα, δηλαδή από UAVs. Ωστόσο, η παρεμβολή RF μπορεί να είναι αναποτελεσματική για αυτόνομα UAV που δεν απαιτούν τηλεχειριστήριο ή για mUAV που ακολουθούν μια προ-προγραμματισμένη διαδρομή μέσω σημείων ελέγχου του συστήματος παγκόσμιου συστήματος εντοπισμού θέσης (GNSS) . Επομένως, απαιτείται η παρεμβολή και του GNSS για την αντιστάθμιση των περιορισμών της εμπλοκής RF.

Οι παρεμβολές GNSS επηρεάζουν τα συστήματα πλοήγησης. Επειδή το σήμα GNSS προέρχεται από δορυφόρους, η ισχύς του είναι αδύναμη και ευάλωτη σε σήματα παρεμβολής. Μόλις το UAV χάσει το σήμα GNSS, θα παραμείνει αιωρούμενο ή θα προσγειωθεί χωρίς να ολοκληρώσει την αποστολή του . Ωστόσο, η εμπλοκή GNSS μπορεί να είναι αναποτελεσματική για UAV που είναι εξοπλισμένα με αισθητήρες αδρανείας (IMU) και κρυπτογραφημένα σήματα για την πλοήγηση. Επομένως, απαιτείται η αλληλεπίδραση μεταξύ των παρεμβολών εμπλοκής RF και GNSS.

Είναι σημαντικό να αναφερθεί ότι οι εναέριες πλατφόρμες CUS μπορούν να χρησιμοποιηθούν για ενίσχυση των παρεμβολών, καθώς η απόδοση της παρεμβολήw μπορεί να βελτιωθεί δραματικά όταν η απόσταση μεταξύ των jammers και των UAV μειωθεί.

23. Ανάλυση Λειτουργίας Πλαστογράφησης Σήματος (Spoofing):

Λαμβάνοντας υπόψη τη σημαντική τεχνολογική πρόοδο και τη γνώση που υπάρχει για τα UAV, είναι δυνατό να γίνει έλεγχος και να δοθεί εντολή σε ένα κακόβουλο UAV να αποφύγει μια προστατευόμενη περιοχή με Geofencing .Η αντιμετώπιση ενός custom Drone που μπορεί να παρακάμψει τους κανόνες πτήσης μιας περιοχής μπορεί να γίνει μέσω μιας τεχνικής που ονομάζεται πλαστογράφηση (spoofing). Η πλαστογράφηση μπορεί να αντιγράψει και να παραποιήσει τα λαμβανόμενα σήματα και έτσι να απενεργοποιήσει ή να πάρει τον έλεγχο των UAV. Στην πλαστογράφηση παραποιούνται τα σήματα ραδιοσυχνοτήτων (RF) του χειριστή ή στους δορυφορικούς δείκτες πλοήγησης GNSS (Global Navigation Satellite System) για να αποτραπεί ή και εκτραπεί η πτήση των UAV. Η πλαστογράφηση απαιτεί προηγμένες τεχνολογίες που κατανοούν πλήρως τα πρωτόκολλα επικοινωνίας, τις υπηρεσίες GNSS και τα ευάλωτα σημεία των UAV για την υλοποίησή της. Η πλαστογράφηση του σήματος των δεκτών GNSS είναι μια κοινή μέθοδος όταν τα πρωτόκολλα (όπως ο τύπος του κώδικα και η διαμόρφωση) είναι γνωστά. Η πλαστογράφηση του GPS μπορεί να οδηγήσει τα UAV σε αιωρητική κατάσταση, να επηρεάσει τον αυτόματο πιλότο, να προκαλέσει εσφαλμένη προσγείωση ή να τα κατευθύνει προς μια πλαστογραφημένη διαδρομή. Για τη διαχείριση των UAV που αποσυνδέονται από τα εξουσιοδοτημένα σήματα GNSS, απαιτούνται κατάλληλες στρατηγικές πλαστογράφησης Ακόμη, μπορούν να παραποιηθούν τα συνδεδεμένα σε σμήνος UAV μελετώντας τα ευάλωτα σημεία των κυψελοειδών δικτύων. Επιπλέον, λόγω της ποικιλίας ενσωματωμένων συστημάτων στα UAV, περιλαμβανομένων των συστημάτων πλοήγησης και επικοινωνίας, πολλά ευάλωτα σημεία μπορούν να αξιοποιηθούν για πλαστογράφηση. Με τη χρήση ακριβής ανάλυσης και προηγμένων τεχνολογιών, είναι εφικτή η πλαστογράφηση μέσω επιθέσεων στα ευάλωτα σημεία των λειτουργικών συστημάτων, των συστημάτων GNSS και των ασύρματων συνδέσεων επικοινωνίας.

24. Ανάλυση Εκπομπής Υψηλής Ηλεκτρομαγνητικής Ισχύος (High-power electromanetics-HPEM)

Η εκπομπή υψηλής ηλεκτρομαγνητικής ισχύος αποτελεί μια μέθοδο για την απενεργοποίηση ενός mUAV μέσω της πρόκλησης ζημιάς στα ηλεκτρονικά του συστήματα. Αυτή η μέθοδος κατηγοριοποιείται σε δύο κατηγορίες: τις μεθόδους που χρησιμοποιούν κύματα στενής ζώνης και εκείνες που χρησιμοποιούν κύματα ευρείας ζώνης.

Τα κύματα ΕΜ στενής ζώνης αναφέρονται στην υψηλή ισχύ σε συχνότητα single-tone και είναι γνωστά και ως HPM (High Power Microwaves). Τα HPM μπορεί να συνδεθούν με το UAV και να προκαλέσουν ζημιά που οδηγεί στην απενεργοποίησή του. Για να επιτευχθεί αυτό, απαιτείται υψηλή ισχύς σε μία μόνο συχνότητα, συνήθως σε χιλιάδες βολτ. Η κατευθυνόμενη ενέργεια του HPM μπορεί να χρησιμοποιηθεί για να απενεργοποιήσει ένα UAV.Επίσης, τα κύματα ΕΜ ευρείας ζώνης περιλαμβάνουν βραχείς παλμούς στο χρόνο. Η

ενέργεια κατανέμεται σε μια ευρεία ζώνη συχνοτήτων, με χαμηλή ενεργειακή πυκνότητα σε όλο το εύρος της ζώνης. Πρέπει να σημειωθεί ότι η εφαρμογή μιας μη πυρηνικής EMP (Electromagnetic Pulse) μεγάλης ισχύος μπορεί να επιτευχθεί με έναν μεγάλο πυκνωτή χαμηλής επαγωγής που εκφορτίζεται σε μια κεραία βρόχου.

Τα κύματα ΕΜ υψηλής ισχύος πρέπει να κατευθύνονται με ακρίβεια προς τον στόχο UAV για να επιτύχουν αποτελεσματικά την απενεργοποίησή του. Αν δεν γίνει αυτό, η αποτελεσματικότητα μειώνεται σημαντικά, καθώς ορισμένες συσκευές, όπως τα ραντάρ και οι αισθητήρες ραδιοσυχνοτήτων, μπορούν να συνεχίσουν να λειτουργούν εν μέρει.

25. Παρουσίαση αντιπροσωπευτικών Αντι-Drone εμπορικών συστημάτων

Υπάρχουν αρκετά αξιόλογα συστήματα αντι-drone που μπορούν να αντιμετωπίσουν εχθρικά drones. Ορισμένα από αυτά είναι ανοιχτού κώδικα (open-source) ή έχουν ανοιχτές προδιαγραφές για προσαρμογές και προσαρμογές από τους χρήστες και κάποια άλλα είναι στρατιωτικού τύπου και απευθύνονται σε οργανισμούς ή κράτη. Ακολουθούν κάποια αντιπροσωπευτικά ανοιχτού κώδικα από αυτά τα συστήματα:

DroneWatcher: Το DroneWatcher είναι ένα ανοιχτού κώδικα σύστημα ανίχνευσης UAV drones που χρησιμοποιεί ένα δίκτυο αισθητήρων και λογισμικό για την ανίχνευση και την αναγνώριση των drones. Μπορεί να εγκατασταθεί σε διάφορες πλατφόρμες και συστήματα, και παρέχει επίσης δυνατότητες ειδοποίησης για αποτελεσματική ανίχνευση.

Air Guard: Το Air Guard είναι ένα ανοιχτού κώδικα σύστημα ανίχνευσης και αποκλεισμού UAV drones. Χρησιμοποιεί αισθητήρες και αλγόριθμους για την ανίχνευση και την αποτροπή των εχθρικών drones. Το Air Guard διαθέτει ανοιχτές προδιαγραφές και παρέχει ευελιξία για προσαρμογές.

Αξίζει να σημειωθεί ότι η επιλογή του κατάλληλου συστήματος θα εξαρτηθεί από τις ακριβείς ανάγκες και απαιτήσεις , καθώς και από τη διαθεσιμότητα και τη συμβατότητα με τα υπόλοιπα συστήματα ασφαλείας. Για την επιλογή του κατάλληλου θα πρέπει να εξεταστούν οι προδιαγραφές και οι δυνατότητες του κάθε συστήματος και να διερευνηθεί η δυναμική της ανοιχτής κοινότητας χρηστών και η υποστήριξή .

Το Drone Guard COMJAM (ESM) είναι ένα σύστημα αντι-drone που βασίζεται στην τεχνολογία του Ηλεκτρονικού Πολέμου (Electronic Warfare). Το COMJAM αναφέρεται στο "Communication Jamming" που σημαίνει τον αποκλεισμό ή την παρεμπόδιση των επικοινωνιών μεταξύ των drones και των σταθμών ελέγχου.Ο σκοπός του Drone Guard COMJAM είναι η παθητική ανίχνευση και αντιμετώπιση των αεροσκαφών UAV.

Χρησιμοποιεί την τεχνολογία ESM για την ανίχνευση των ηλεκτρονικών υπογραφών που εκπέμπονται από τα drones, όπως σήματα ελέγχου, τηλεμετρίας, εικόνας και άλλα σήματα επικοινωνίας.Μετά την ανίχνευση του drone, το σύστημα COMJAM μπορεί να προβεί σε διάφορες ενέργειες για τη μείωση των επιπτώσεων ή την αποτροπή της απειλής του. Αυτές οι ενέργειες μπορεί να περιλαμβάνουν την παρεμπόδιση της επικοινωνίας μεταξύ του drone και του χειριστή του ή την απενεργοποίηση των συστημάτων του drone.Ως παθητικό σύστημα, το Drone Guard COMJAM δεν χρησιμοποιεί ενεργή απευθείας επίθεση κατά του drone, αλλά επικεντρώνεται στην ανίχνευση και την αντιμετώπιση των επικοινωνιακών συνδέσεων του. Έχει σχεδιαστεί για να λειτουργεί ως μέρος ενός ευρύτερου συστήματος ασφαλείας, ενσωματώνοντας την τεχνολογία COMJAM σε μια ολοκληρωμένη αντι-drone προσέγγιση.

Το AeroScope είναι ένα σύστημα ανίχνευσης και παρακολούθησης UAV drones που αναπτύχθηκε από την εταιρεία DJI, μια από τις κορυφαίες εταιρείες κατασκευής drones. Το AeroScope είναι σχεδιασμένο να παρέχει ανίχνευση και αναγνώριση των drones που είναι εξοπλισμένα με την τεχνολογία DJI.Οι βασικές λειτουργίες του AeroScope περιλαμβάνουν:

Ανίχνευση: Το σύστημα μπορεί να ανιχνεύει την παρουσία των drones που εκπέμπουν σήματα συνδεσιμότητας με την τεχνολογία DJI. Αυτό του επιτρέπει να αναγνωρίσει τα drones που είναι σε κοντινή απόσταση.

Ταυτοποίηση: Μπορεί να αναγνωρίσει το μοντέλο, τον αριθμό σειράς και άλλες πληροφορίες των drones της DJI που βρίσκονται στην εμβέλειά του.

Παρακολούθηση: Μπορεί να παρακολουθεί την κίνηση και την τοποθεσία των drones της DJI που είναι ενεργά στην περιοχή, παρέχοντας αναλυτικές πληροφορίες στον χειριστή του AeroScope.

Το AeroScope είναι μια εμπορική λύση της DJI και έχει χρησιμοποιηθεί σε διάφορα πεδία όπως οι αστυνομικές και στρατιωτικές επιχειρήσεις, σε αεροδρόμια, πολιτικές εκδηλώσεις και οι εκδηλώσεις ασφαλείας. Η κοινότητα χρηστών AeroScope περιλαμβάνει επαγγελματίες από αυτούς τους τομείς και έχει σχηματίσει μια ανοιχτή κοινότητα που μοιράζεται εμπειρίες, προβλήματα και λύσεις σχετικά με τη χρήση του AeroScope.Το AeroScope χρησιμοποιεί έναν συνδυασμό αισθητήρων για την ανίχνευση και την παρακολούθηση των UAV drones της DJI. Αν και οι λεπτομέρειες σχετικά με τους ακριβείς αισθητήρες δεν είναι πλήρως γνωστές, ορισμένοι από τους αισθητήρες που χρησιμοποιούνται περιλαμβάνουν:

Αντένα: Το AeroScope χρησιμοποιεί μια ή περισσότερες αντένες για τη λήψη των σημάτων επικοινωνίας που εκπέμπονται από τα drones της DJI.

Ραντάρ: Χρησιμοποιεί ραντάρ για την ανίχνευση των drones βάσει των ραδιοκυμάτων που ανακλώνται από τα αντικείμενα.

Αισθητήρες RF (Radio Frequency): Οι αισθητήρες RF του μπορούν να ανιχνεύουν τη χρήση ραδιοσυχνοτήτων από τα drones και να αναγνωρίζουν τα συγκεκριμένα σήματα επικοινωνίας που χρησιμοποιούνται από τα μοντέλα της DJI.

26. Προτεινόμενα Αντι-Drone Συστήματα (DIY)

Στις επόμενες ενότητες ακολουθούν ερασιτεχνικές προτάσεις hardware και software ανοιχτού κώδικα χαμηλού κόστους, με άριστες επιδόσεις για την κατηγορία τους που μπορούν ως έμπνευση να αποτελέσουν συνδυαστικά τη βάση για την ανάπτυξη και εξέλιξη ενός αποτελεσματικού φορητού συστήματος αντι-drone που θα μπορεί να αντιμετωπίσει τα περισσότερα εμπορικά drone της αγοράς που χρησιμοποιούντα για κακόβουλη χρήση. Η παρακάτω ανάλυση γίνεται καθαρά για ακαδημαϊκούς σκοπούς με κίνητρο την μάθηση για την τεχνολογία και να αποτελέσει έμπνευση για εξέλιξη των συστημάτων αυτών από τους Έλληνες μηχανικούς βιομηχανικής σχεδίασης και παραγωγής τεχνολογικών συστημάτων.

27. HackRF One- Portapack H2+DDoS attack - NodeMCU ESP8266 module

HackRF One [23]**:** Το HackRF One είναι μια συσκευή λήψης και εκπομπής ραδιοσυχνοτήτων SDR (Software-Defined Radio) διαθέτει 8-Bit ADC (Analog-to-Digital Converter) και μπορεί να λειτουργήσει σε εύρος από 10 MHz έως 6 GHz, με εύρος ζώνης έως 20 MHz. Το HackRF One προσφέρει τη δυνατότητα εκπομπής και λήψης ραδιοφωνικών σημάτων και ρυθμίζεται και ελέγχεται στη βασική του έκδοση μέσω ενός υπολογιστή(λαπτοπ ή ακόμα και με ένα raspberry pi2) .

Η συσκευή προσφέρει πολλές ενδιαφέρουσες δυνατότητες, όπως την ανίχνευση και την ανάλυση των σημάτων, την υλοποίηση πρωτοτύπων επικοινωνίας, την παρακολούθηση δικτύων και πολλές άλλες εφαρμογές που λόγω της ανοιχτής κοινότητας συνεχώς αναπτύσσονται .Δίνεται δηλαδή τη δυνατότητα ένας μηχανικός να το εξελίξει γράφοντας ο ίδιος κώδικα και να το επεκτείνει με δικής του σχεδίασης hardware . Η δυνατότητα εκπομπής επιτρέπει τη δημιουργία δικών μας σημάτων στο φάσμα και στη συχνότητα που μας ενδιαφέρει και την προσομοίωση διάφορων περιβαλλόντων για πειραματισμό και μάθηση.

Η τιμή του HackRF One στη βασική του μορφή είναι μόλις $300 USD. Η ευρεία κάλυψη συχνοτήτων και το μεγάλο εύρος ζώνης καθιστούν το HackRF One ένα ευέλικτο εργαλείο για πολλούς ερασιτέχνες αλλά και επαγγελματίες στον τομέα των επικοινωνιών. Παράλληλα, η υποστήριξη του Kickstarter και η ανοιχτή κοινότητα προγραμματιστών που το περιβάλλει σημαίνουν ότι το HackRF One εξελίσσεται συνεχώς με νέες βελτιώσεις και

λειτουργίες.Συνολικά, το HackRF One προσφέρει εντυπωσιακές δυνατότητες SDR με μια προσιτή τιμή.

Στην κατηγορία του προτεινόμενου HackRF One υπάρχουν και κάποιες ανταγωνιστικές λύσεις όπως το PlutoSDR και το LimeSDR Mini που σε κάποια χαρακτηριστικά ίσως υπερτερούν όπως η εμβέλεια .Δεν είναι όμως πλήρως open source και δεν έχουν τόσο μεγάλη υποστήριξη από την ανοιχτή κοινότητα προγραμματιστών και δεν έχουν επίσης τόσο μεγάλη ευρεία εφαρμογών. Για αυτό το λόγο επιλέχτηκε ως καλύτερη λύση συνολικά το HackRF One σε συνδιασμό με το Portapack.H2.

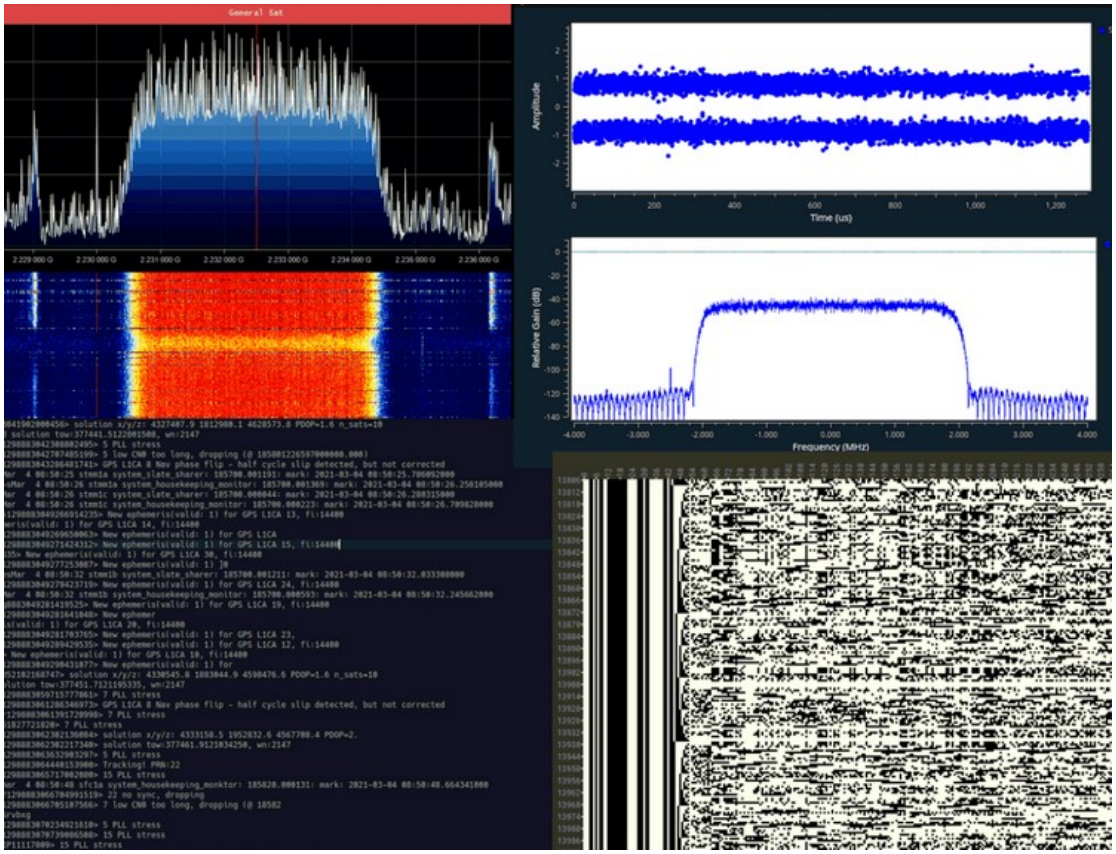
Επίσης από πλευράς τεχνικών προδιαγραφών και απόδοσης, σίγουρα υστερεί σε σχέση με πανάκριβα συστήματα που σχεδιάστηκαν ειδικά για στρατιωτικές εφαρμογές και διαθέτουν προηγμένες λειτουργίες. Είναι όμως αρκετά ικανό για να χρησιμοποιηθεί αποτελεσματικά σε ένα μεγάλο πεδίο εφαρμογών και να προσφέρει λύσεις ως φορητό αντι-drone σύστημα χειρός.

Είναι σημαντικό να ληφθεί υπόψη ότι ο ανταγωνισμός και η τεχνολογική εξέλιξη στον τομέα των αντι-drone ανιχνευτών και των στρατιωτικών συστημάτων είναι συνεχής, και οι προδιαγραφές και οι δυνατότητες των συστημάτων διαμορφώνονται διαρκώς. Έτσι, η σύγκριση μεταξύ του HackRF One καιάλλων επαγγελματικών συστημάτων εξαρτηται και από τις συγκεκριμένες απαιτήσεις και το πεδίο εφαρμογής.

Το HackRF One λοιπόν μπορεί να χρησιμοποιηθεί και ως ένα εργαλείο για την αντιμετώπιση εχθρικών εμπορικών UAV drones με τις κατάλληλες βελτιώσεις

Σχήμα 21. HackRF One [24]

Ένα άλλο σημαντικό πλεονέκτημα του HackRF One είναι η συμβατότητά του με το λογισμικό ανοιχτού κώδικα, όπως το GNU-Radio. Αυτό σημαίνει ότι οι χρήστες έχουν τη δυνατότητα να προσαρμόσουν τη συσκευή στις ανάγκες τους και να αναπτύξουν δικές τους εφαρμογές και λειτουργίες.



Σχήμα 22. HackRF One -Ανίχνευση σημάτων RF [25]

Το HackRF One είναι μια εξαιρετικά πολύπλευρη συσκευή που προσφέρει τη δυνατότητα να εκτελεστούν μια μεγάλη ποικιλία επιθέσεων και πειραματισμών. Οι δυνατότητές του περιλαμβάνουν:

Επιθέσεις παρεμβολής: Με την ικανότητά του να εκπέμπει θόρυβο, μπορεί να δημιουργήσει παρεμβολές σε σήματα και να εμποδίσει την αποδοχή τους από άλλες συσκευές. Αυτό μπορεί να χρησιμοποιηθεί για την προστασία της ιδιωτικότητας ή για αντιμετώπιση εισβολέων UAV.

Επαναληπτικές επιθέσεις: Με τη δυνατότητα καταγραφής και αναπαραγωγής σημάτων, το HackRF One μπορεί να καταγράψει ένα σήμα και να το αναπαράγει ξανά χωρίς την αρχική

συσκευή πηγής. Αυτό μπορεί να χρησιμοποιηθεί για ανάλυση πρωτοκόλλων ,για ανακάλυψη ευπαθειών σε συστήματα ασφάλειας και παρεμβολή σε εχθρικά UAV.

Πλαστογράφηση GPS: Με την υψηλή ευαισθησία του στα σήματα GPS, το HackRF One μπορεί να χρησιμοποιηθεί για την πλαστογράφηση σημάτων GPS.

Επιθέσεις πλευρικού καναλιού: Με την ικανότητά του να λαμβάνει και να εκπέμπει σε μεγάλο εύρος συχνοτήτων, το HackRF One μπορεί να χρησιμοποιηθεί για να παρακολουθεί την πλευρική επικοινωνία που εκτελείται μεταξύ σμήνους UAVs. Αυτό μπορεί να επιτρέψει να αναγνωρίσει drones ή να παρέμβει σε επικοινωνίες και πληροφορίες.

Τεχνικά Χαρακτηριστικά**:**

Συχνότητα λειτουργίας: 1 MHz έως 10 MHz: 5 dBm έως 15 dBm, γενικά αυξάνεται καθώς αυξάνεται η συχνότητα **[26]**.

10 MHz έως 2170 MHz: 5 dBm έως 15 dBm, γενικά μειώνεται καθώς αυξάνεται η συχνότητα

2170 MHz έως 2740 MHz: 13 dBm έως 15 dBm

2740 MHz έως 4000 MHz: 0 dBm έως 5 dBm, μειώνεται καθώς αυξάνεται η συχνότητα

4000 MHz έως 6000 MHz: -10 dBm έως 0 dBm, γενικά μειώνεται καθώς αυξάνεται η συχνότητα Στο μεγαλύτερο μέρος του εύρους συχνοτήτων έως 4 GHz, η μέγιστη ισχύς TX είναι μεταξύ 0 και 10 dBm. Το εύρος συχνοτήτων με την καλύτερη απόδοση είναι 2170 MHz έως 2740 MHz.

Η μέγιστη ισχύς RX του HackRF One είναι -5 dBm. Θεωρητικά, το HackRF One μπορεί να δεχτεί με ασφάλεια έως και 10 dBm με τον μπροστινό ενισχυτή RX απενεργοποιημένο.

Εγκατάσταση λογισμικού HackRF (Great Scott Gadgets)**:**

Το λογισμικό HackRF περιλαμβάνει δύο βασικά στοιχεία: τα Εργαλεία HackRF (HackRF Tools) και τη βιβλιοθήκη libhackrf. Τα Εργαλεία HackRF αποτελούν ένα σύνολο βοηθητικών προγραμμάτων γραμμής εντολών που επιτρέπουν να αλληλοεπιδράμε με τη συσκευή HackRF. Μέσω αυτών των εργαλείων, μπορούμε να πραγματοποιήσουμε διάφορες λειτουργίες, όπως την εγγραφή και αναπαραγωγή σημάτων RF, τον έλεγχο των ρυθμίσεων του HackRF και άλλες παρόμοιες λειτουργίες.

Η βιβλιοθήκη libhackrf είναι μια χαμηλού επιπέδου βιβλιοθήκη που επιτρέπει στο λογισμικό στον υπολογιστή μας να επικοινωνεί με τη συσκευή HackRF. Αυτή η βιβλιοθήκη παρέχει τις απαραίτητες λειτουργίες και δυνατότητες για την εκτέλεση διαφόρων εργασιών

με το HackRF, όπως η ρύθμιση των παραμέτρων λειτουργίας, η αποκωδικοποίηση και η αναπαραγωγή των σημάτων RF και πολλά άλλα.

Προτεινόμενο λειτουργικό σύστημα για χρήση με το HackRF είναι το Ubuntu.

Η εγκατάσταση γίνεται με την εντολή: sudo apt-get install hackrf

(git clone https://github.com/mossmann/hackrf.git)

Τα εργαλεία HackRF που παρέχονται από την Great Scott Gadgets είναι πολύτιμα για την αλληλεπίδραση με τη συσκευή HackRF μέσω της γραμμής εντολών. Αυτά τα εργαλεία επιτρέπουν να εκτελέσουμε διάφορες λειτουργίες και να αποκτήσουμε πληροφορίες για τη συσκευή.

Το hackrf_info μας επιτρέπει να διαβάσουμε πληροφορίες σχετικά με τη συσκευή HackRF, όπως τον σειριακό αριθμό και την έκδοση του υλικολογισμικού.

Με το hackrf_transfer μπορεί να αποστέλλει και να λάβει σήματα. Τα αρχεία εισόδου/εξόδου που χρησιμοποιούνται είναι δείγματα τετραγωνισμού με υπογραφή 8 bit.

Με το hackrf_sweep, ένα αναλυτή φάσματος γραμμής εντολών, μπορεί να εξερευνήσει το φάσμα συχνοτήτων.

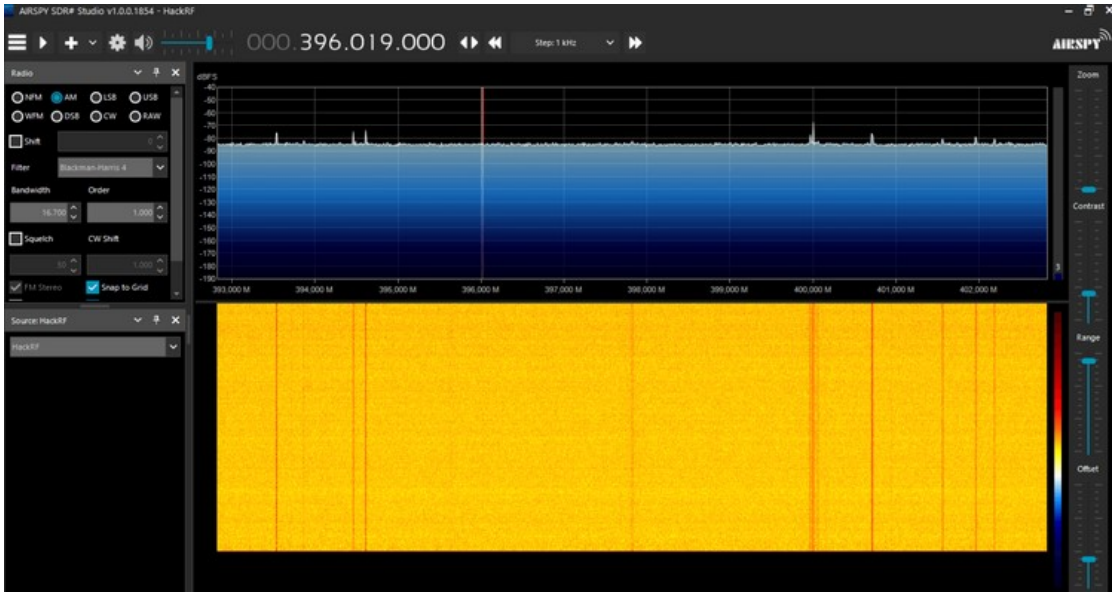
Το hackrf_clock μας επιτρέπει να διαβάζει και να εγγράφει τις ρυθμίσεις εισόδου και εξόδου του ρολογιού.

Με το hackrf_operacake μπορεί να διαμορφώσει τον διακόπτη κεραίας Opera Cake που είναι συνδεδεμένος στο HackRF.

Το hackrf_spiflash είναι ένα εργαλείο που επιτρέπει να δημιουργήσει νέο υλικολογισμικό στο HackRF. Αυτό είναι χρήσιμο για ενημέρωση του υλικολογισμικού της συσκευής.

Το hackrf_debug επιτρέπει να διαβάζει και να εγγράφει καταχωρητές και άλλες ρυθμίσεις παραμέτρων χαμηλού επιπέδου για εντοπισμό σφαλμάτων.

Αυτά τα εργαλεία συνοδεύουν το HackRF και επιτρέπουν στους χρήστες να αξιοποιήσουν πλήρως τις δυνατότητες της συσκευής για διάφορες εφαρμογές SDR.

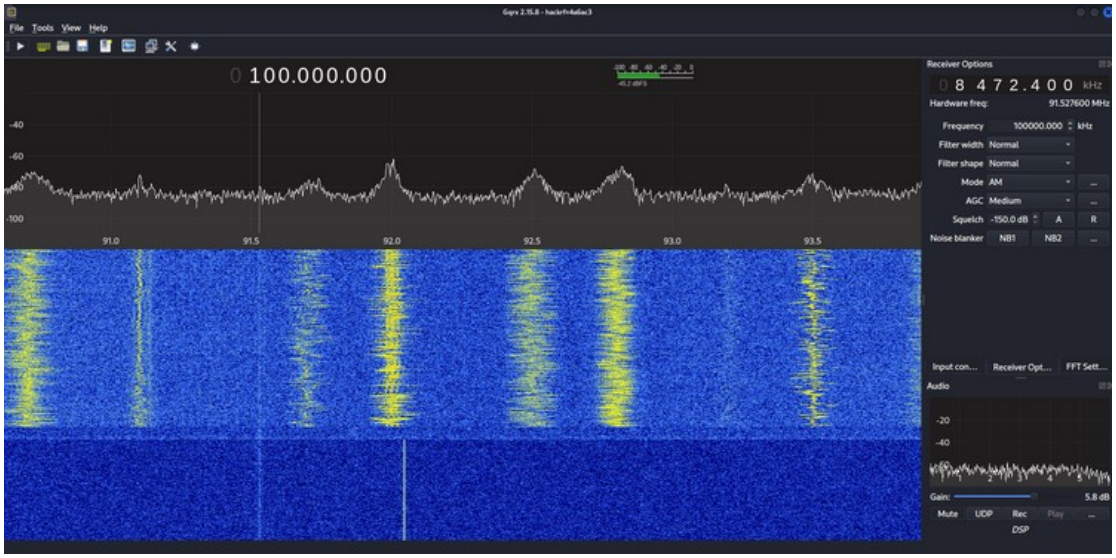


Σχήμα 23. SDR# Γραφική Διεπαφή Χρήστη

Για να χρησιμοποιήσει κάποιος το HackRF One στο Linux, η εγκατάσταση των πακέτων προγραμμάτων οδήγησης είναι απαραίτητη. Σε διανομές που βασίζονται στο Debian, πρέπει να εγκατασταθεί το πακέτο "hackrf" για να αποκτήσουμε τα απαραίτητα εργαλεία επικοινωνίας.

Ένα από τα δημοφιλή προγράμματα για την επεξεργασία σημάτων RF είναι το Gqrx. Το Gqrx είναι ένα ανοιχτού κώδικα πρόγραμμα SDR παρόμοιο με το SDR# και είναι διαθέσιμο στα αποθετήρια (repos) του Debian. Μετά την εγκατάστασή του το Gqrx χρησιμοποιείται άμεσα για λήψη και εγγραφή σημάτων RF με το HackRF One.

Εγκαθιστώντας το πακέτο "hackrf" και το Gqrx στο Linux, έχουμε την πλήρη λειτουργικότητα του HackRF One για την εξερεύνηση και την ανάλυση των σημάτων RF.

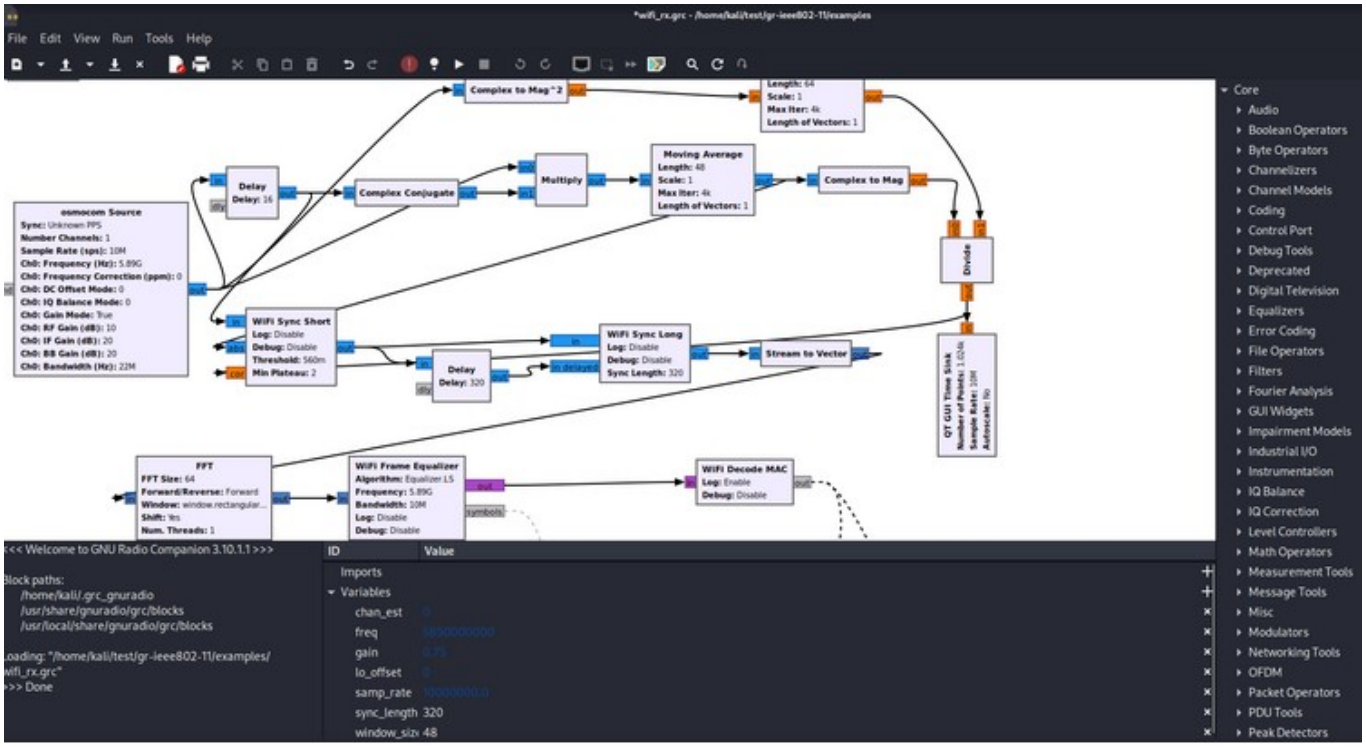


Σχήμα 24. Γραφική διεπαφή χρήστη Gqrx

Και τα δύο εργαλεία είναι παρόμοια στη λειτουργία τους και προσφέρουν παρόμοιες δυνατότητες στους χρήστες. Και το Gqrx και το SDR# επιτρέπουν την παρακολούθηση του φάσματος ραδιοσυχνοτήτων, τη λήψη σημάτων σε συγκεκριμένες συχνότητες και την αποδιαμόρφωση τους σε διάφορες λειτουργίες όπως FM, AM ή USB. Με αυτόν τον τρόπο, είναι δυνατή η ανάκτηση των πληροφοριών που μεταφέρονται, όπως από ένα UAV.

Και τα δύο προγράμματα έχουν παρόμοια διάταξη, με το πάνω μέρος να προβάλλει το φάσμα RF (ισχύς σήματος για μια συγκεκριμένη συχνότητα σε ένα συγκεκριμένο χρονικό σημείο) και το κάτω μέρος να παρουσιάζει ένα αναλογικό διάγραμμα που αντιπροσωπεύει την ισχύ του σήματος κατά τη διάρκεια του χρόνου. Το HackRF, επειδή μπορεί επίσης να εκπέμπει, επιτρέπει την εγγραφή και αναπαραγωγή αυτών των σημάτων μέσω RF.

Ωστόσο, όταν έρχεται στην αλληλεπίδραση με τις ραδιοσυχνότητες με έναν πιο προγραμματιστικό τρόπο, το GNU Radio είναι η κατάλληλη επιλογή. Το GNU Radio είναι ένα ανοιχτού κώδικα λογισμικό ανάπτυξης που παρέχει ένα σύνολο από μπλοκ επεξεργασίας σήματος που μπορούν να συνδυαστούν και να συνδεθούν γραφικά, καθιστώντας τη δημιουργία προγραμμάτων που αλληλεπιδρούν με τη ραδιοσυχνότητα πιο εύκολη.



Σχήμα 25. GNU Radio Διαδικασία κατά τη λήψη πακέτων Wi-Fi

Το HackRF One αποτελείται από διάφορα εξαρτήματα υλικού που επιτρέπουν τη λειτουργία της συσκευής. Ανάμεσα στα κύρια εξαρτήματα που χρησιμοποιούνται στο HackRF One περιλαμβάνονται:

Πομποδέκτης MAX2837 2,3 έως 2,7 GHz: Αυτός ο πομποδέκτης καλύπτει ένα ευρύ φάσμα συχνοτήτων για την εκπομπή και λήψη σημάτων.

Πομποδέκτης MAX2839 2,3 έως 2,7 GHz: Αυτός ο πομποδέκτης επίσης χρησιμοποιείται για την εκπομπή και λήψη σημάτων σε παρόμοιο εύρος συχνοτήτων.

MAX5864 ADC/DAC: Αυτός ο μετατροπέας αναλογικού-ψηφιακού/ψηφιακού-αναλογικού χρησιμοποιείται για τη μετατροπή των αναλογικών σημάτων σε ψηφιακή μορφή και αντίστροφα.

Γεννήτρια ρολογιού Si5351: Αυτή η γεννήτρια ρολογιού χρησιμοποιείται για την παραγωγή ακριβών χρονισμένων σημάτων ρολογιού που απαιτούνται για τη λειτουργία του HackRF.

CoolRunner-II CPLD: Προγραμματιζόμενος λογικός πίνακας, χρησιμοποιείται για τον έλεγχο και τη διαχείριση των σημάτων μέσων στο HackRF.

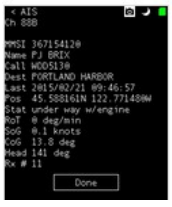
Μικροελεγκτής LPC43xx ARM Cortex-M4: Αυτός ο μικροελεγκτής βασίζεται στην αρχιτεκτονική ARM Cortex-M4 και χρησιμοποιείται για τον έλεγχο των λειτουργιών του HackRF. Παρέχει επίσης συνδεσιμότητα JTAG/SWD για προγραμματισμό και αποσφαλμάτωση.

Μίκτης/συνθεσάιζερ RFFC5072: Αυτός ο μίκτης/συνθεσάιζερ χρησιμοποιείται για την ανάμιξη και σύνθεση των σημάτων στην επιθυμητή συχνότητα.

Flash μνήμη W25Q80BV 8M-bit: Αυτή η μνήμη χρησιμοποιείται για την αποθήκευση δεδομένων και υλικολογισμικού.

Αυτά τα εξαρτήματα συνεργάζονται μεταξύ τους για να επιτρέψουν τη λειτουργία του HackRF One ως φορητή συσκευή SDR.

PortaPack H2 για HackRF One



Σχήμα 26. Portapack [27]

Το PortaPack είναι μια επέκταση που συνδέεται στο HackRF και προσφέρει πολλές επιπλέον δυνατότητες. Αυτή η επέκταση περιλαμβάνει τα εξής χαρακτηριστικά:

Οθόνη αφής LCD: Το PortaPack προσθέτει μια οθόνη αφής LCD που επιτρέπει την εύκολη πλοήγηση και αλληλεπίδραση με τις λειτουργίες του HackRF.

Χειριστήρια χρήστη: Υπάρχουν προστατευτικά χειριστήρια που επιτρέπουν την ευκολία χειρισμού και προσαρμογής των ρυθμίσεων.

Υποδοχή ακουστικών: Υπάρχει μια υποδοχή ακουστικών για άμεση ακρόαση των εισερχόμενων σημάτων ήχου.

Αναφορά ρολογιού υψηλής ακρίβειας: Το PortaPack παρέχει μια ακριβή αναφορά ρολογιού για την εκτέλεση προηγμένων λειτουργιών.

Ρολόι σε πραγματικό χρόνο: Υπάρχει ένα ενσωματωμένο ρολόι σε πραγματικό χρόνο που επιτρέπει τον συγχρονισμό του χρόνου σε εφαρμογές και μετρήσεις.

Υποδοχή κάρτας micro SD: Το PortaPack διαθέτει μια υποδοχή κάρτας micro SD για την αποθήκευση δεδομένων και τη δυνατότητα εγγραφής και αναπαραγωγής αρχείων.

Προσαρμοσμένη θήκη αλουμινίου: Το PortaPack περιλαμβάνει μια ειδικά σχεδιασμένη θήκη αλουμινίου που προσφέρει προστασία, φορητότητα και ανθεκτικότητα στη συσκευή.

Με τη σύνδεση μιας μπαταρίας USB, το PortaPack είναι έτοιμο για να μας επιτρέψει να εξερευνήσουμε το ραδιοφάσμα ενός Drone οπουδήποτε. Το υλικολογισμικό του PortaPack εκτελείται στους γρήγορους επεξεργαστές ARM που βρίσκονται στο HackRF . Αυτό σημαίνει ότι δεν απαιτείται υπολογιστής για την λειτουργία του (εκτός από την προγραμματιστική διαδικασία του υλικολογισμικού).

Όπως ήδη αναφέρθηκε το PortaPack είναι μια πλατφόρμα που λειτουργεί με ανοιχτό κώδικα, και τόσο το υλικό όσο και το υλικολογισμικό του είναι διαθέσιμα για το κοινό. Αυτό σημαίνει ότι οι πηγές του κώδικα δημοσιεύονται στο GitHub, μια δημοφιλής πλατφόρμα ανάπτυξης λογισμικού.

Η δημοσίευση των αρχείων πηγαίου κώδικα στο GitHub [27] επιτρέπει σε προγραμματιστές και ενδιαφερόμενους να προσαρμόσουν, να επεκτείνουν και να βελτιώσουν το υλικολογισμικό του PortaPack σύμφωνα με τις ανάγκες τους.

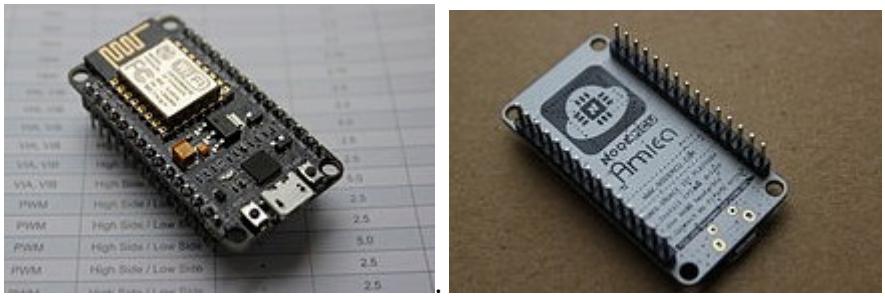
28. DDOS 2.4G Attack σε εχθρικό UAV:

Το DDOS (Distributed Denial of Service) είναι μια είδους κυβερνοεπίθεσης που στοχεύει στο να καταρρίψει ή να καθυστερήσει ένα ασύρματο δίκτυο, έναν διακομιστή ή ένα τερματικό και στην περίπτωση που εδώ εξετάζεται ένα εμπορικό κακόβουλο UAV Drone που χρησιμοποιείται για μια τρομοκρατική ενέργεια, που δεν έχει ιδιαίτερα συστήματα ασφαλείας , καθιστώντας την επικοινωνία με τον σταθμό βάσης του μη προσβάσιμη και έτσι να χάθεί η επικοινωνία. Κατά τη διάρκεια μιας DDOS επίθεσης, ο επιτιθέμενος χρησιμοποιεί συνεχή πακέτα request για σύνδεση με το ασύρματο δίκτυο ,χωρίς κενά ώστε να μη μπορεί να απαντήσει ο δέκτης των πακέτων .Ο στόχος της επίθεσης είναι να καταναλώσει όλους τους πόρους του στόχου, όπως η εύρεση εύκολων διαθέσιμων συνδέσεων ή η επεξεργαστική ισχύς, ώστε να μην είναι πλέον σε θέση να εξυπηρετήσει νόμιμους συνδεδεμένους χρήστες ή να τους παρέχει τις απαιτούμενες υπηρεσίες. Αυτό μπορεί να προκαλέσει σημαντική διακοπή λειτουργίας των υπηρεσιών του δικτύου, επηρεάζοντας την προσβασιμότητα και την απόδοση των υπηρεσιών στο εχθρικό drone.

Οι DDOS επιθέσεις μπορούν να εκτελεστούν με διάφορους τρόπους, συμπεριλαμβανομένων επιθέσεων ενίσχυσης της χωρητικότητας (amplification attacks), επιθέσεων στρατοπέδευσης εφαρμογών (application layer attacks) και επιθέσεων απομάκρυνσης εξυπηρετητών (server congestion attacks).

Το "deauther" που παρουσιάζεται εδώ είναι μια συσκευή και ένα υλικολογισμικό που χρησιμοποιείται για εκτέλεση επιθέσεων "deauthentication" (αποσύνδεσης) σε ασύρματα δίκτυα εμπορικών απειλιτικών UAV .Πρόκειται για ένα οικονομικό module το NodeMCU ESP8266 που κατασκευάζεται από την εταιρεία Espressif Systems με κόστος κάτω από 10 ευρώ.

Το NodeMCU αποτελεί ένα υλικολογισμικό ανοιχτού κώδικα, για το οποίο υπάρχουν διαθέσιμα σχέδια πλακέτας πρωτοτύπων ανοιχτού κώδικα. Το όνομα "NodeMCU" συνδυάζει τον όρο "node" και το "MCU" (μονάδα μικροελεγκτή). Όπως προαναφέρθηκε τόσο το υλικολογισμικό όσο και τα σχέδια πλακέτας πρωτοτύπων είναι ανοιχτού κώδικα , αυτό σημαίνει ότι ο πηγαίος κώδικας του NodeMCU είναι ελεύθερα διαθέσιμος και μπορεί να τροποποιηθεί από την κοινότητα των προγραμματιστών ή ένα μηχανικό. Αυτή η ανοιχτή φιλοσοφία παρέχει ευελιξία και δυνατότητες προσαρμογής και πειραματισμού για την ανάπτυξη διάφορων εφαρμογών με το NodeMCU. Όπως η παρακάτω που θα χρησιμοποιήσω για την παρεμπόδιση επικοινωνίας με τον σταθμό βάσης ή τον χειριστή ενός εχθρικού Drone.



Σχήμα 27. NodeMCU ESP8266 module

Τρόπος λειτουργίας: Το πρωτόκολλο Wi-Fi με αριθμό 802.11 παρέχει ένα πλαίσιο εξακρίβωσης ταυτότητας, γνωστό και ως Deauthentication frame. Αυτό το πλαίσιο χρησιμοποιείται για την ασφαλή αποσύνδεση όλων των χρηστών που είναι συνδεδεμένοι σε ένα δρομολογητή Wi-Fi. Αν κάποιος θέλει να αποσυνδέσει μια συσκευή από ένα δίκτυο Wi-Fi, δεν απαιτείται να έχει πρόσβαση στο δίκτυο ή να γνωρίζει τον κωδικό πρόσβασης. Αρκεί να έχει τη διεύθυνση MAC του δρομολογητή Wi-Fi και της συσκευής πελάτη που επιθυμεί να αποσυνδέσει και να βρίσκεται στην εμβέλεια του συγκεκριμένου δικτύου Wi-Fi.

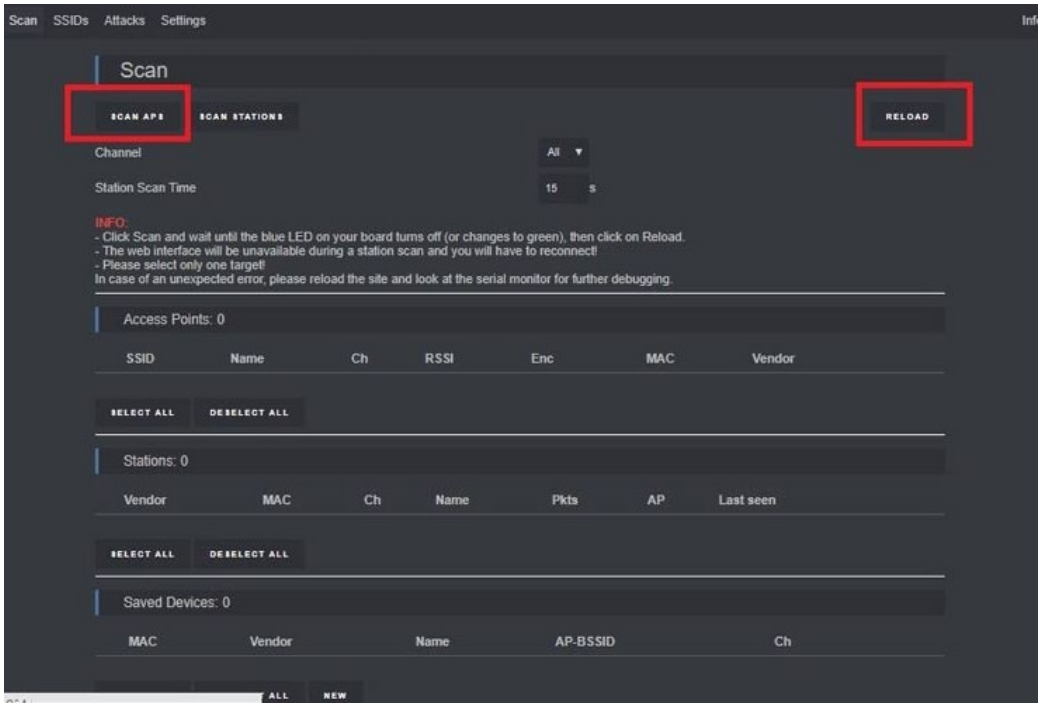
Για την εφαρμογή αυτής της μεθόδου, χρειάζεται για το υλικολογισμικό Jammer το NodeMCU ESP8266 module.

Εγκαθιστούμε το υλικολογισμικό Jammer με ένα flasher [29] για το NodeMCU από την σελίδα github το οποίο είναι ανοιχτού κώδικα και τον τροποποιούμε για να τον φέρουμε στα μέτρα της εφαρμογής μας. [29]

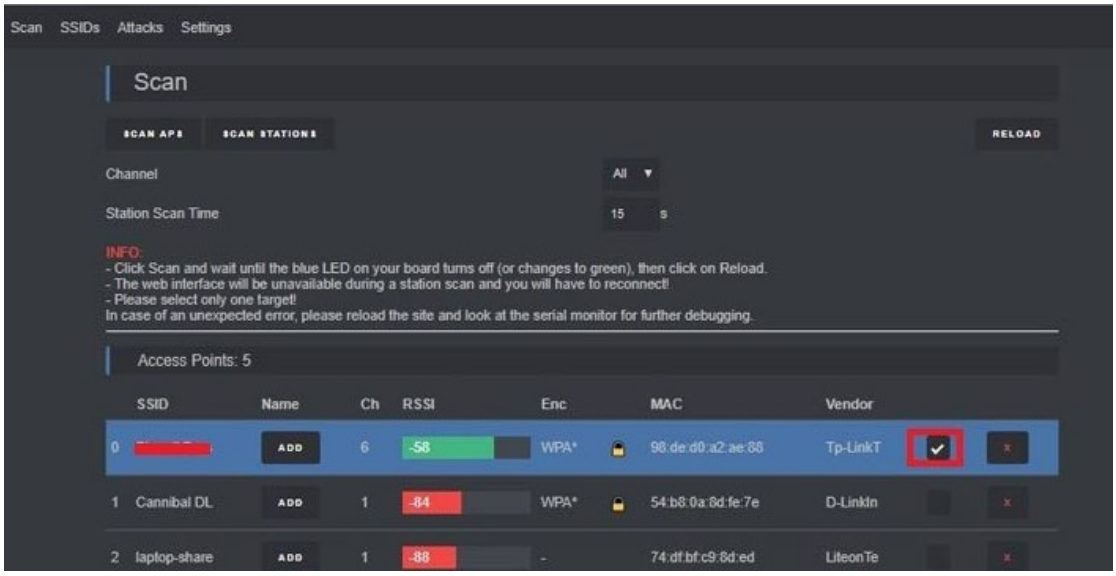
Σχήμα 28. Εγκατάσταση βιβλιοθήκης ino μέσω Arduino ide

ΣΗΜΑΝΤΙΚΗ ΣΗΜΕΙΩΣΗ: Τα project που παρουσιάζονται εδώ έχουν διδακτικό σκοπό και σκοπό πειραματισμού σε επίπεδο έρευνας για το πως θα μπορούσαν να συνδυαστούν ώστε να υλοποιηθούν με χαμηλό κόστος φορητά anti drone συστήματα ως αμυντική μέθοδος σε επίθεση εχθρικών Drone που απειλούν τη ζωή.

Συνδέουμε το φορητό υπολογιστή ή το smartphone μας με το Access Point που δημιουργήθηκε από το NodeMCU. Ο κωδικός είναι αυτός που δημιουργήσαμε στην εγκατάσταση. Η διεπαφή που δημιουργείται μας εμφανίζει τα διαθέσιμα WiFi στην εμβέλια του module.



Σχήμα 29. Η διεπαφή που δημιουργούμε για την επιλογή του Drone-Wifi -DDOS παρεμβολή. [31]



Σχήμα 30. Επίθεση στο wifi που χρησιμοποιει το drone με το κέντρο ελέγχου του-βάση.

29. Συμπεράσματα , Προκλήσεις και Μελλοντική Εξέλιξη Αντί-Drone Συστημάτων

Όρια και προκλήσεις των αντι-drone συστημάτων CUS:

Η αντιμετώπιση απρόβλεπτων απειλών από αναδυόμενα UAV και η πολλαπλότητα των πλατφορμών στα συστήματα αντι -drone CUS αποτελούν μείζονες προκλήσεις για μια ενιαία πλατφόρμα. Μια προσέγγιση που παρέχει ποικιλομορφία και αξιοπιστία μέσω πολλαπλών αντι-drone πλατφορμών είναι πολλά υποσχόμενη. Η ενδοεπικοινωνία μεταξύ των πλατφορμών αποτελεί κρίσιμο παράγοντα για την αποτελεσματική λειτουργία του συνολικού συστήματος, επομένως η δημιουργία ολοκληρωμένων δικτύων CUS απαιτεί προσοχή στη σωστή απόδοση του δικτύου και της επικοινωνίας των επιμέρους τεχνολογικών αντι-drone λύσεων για την επίτευξη της αποστολής.

Τα ολοκληρωμένα αντι-drone συστήματα λοιπόν μπορούν να αποτελούνται από διάφορους τύπους πλατφορμών. Οι πλατφόρμες εδάφους μπορεί να περιλαμβάνουν σταθερές βάσεις και μπορούν να συνδυαστούν με εναέρια αντι-drone συστήματα και υβριδικά συστήματα παρεμβολής χειρός.

Αυτές οι πλατφόρμες θα μπορούν να μετακινούνται σε διάφορες περιοχές και να παρέχουν αντι-drone λύση εκεί που χρειάζεται έτσι ώστε να υπάρχουν λύσεις μεγάλης και μικρής

κλίμακας ανάλογα την απειλή. Εάν πρόκειται για μεγάλη απειλή από Drones -αεροπλάνα και οπλισμένα δηλαδή στρατιωτικού τύπου θα πρέπει να δημιουργηθούν εξειδικευμένα και ακριβείας υβριδικά συστήματα CUS όπως αναλύθηκαν στις προηγούμενες ενότητες.

Όταν πρόκειται όμως για μικρότερου μεγέθους απειλή ως προς την καταστροφή που μπορεί να προκληθεί προτείνω να χρησιμοποιούνται συστήματα παρεμβολής χειρός τα οποία χρησιμοποιούν την τεχνολογία Jamming και Spoofing και μπορούν να κατασκευαστούν με ασύγκριτα χαμηλότερο κόστος.

Κάποιες αρκετά φθηνές λύσεις με πολύ καλές επιδόσεις για την κατηγορία της παρουσιάστηκε στην προηγούμενη ενότητα. Όπου εάν συνδυαστούν και εξελιχθούν στα σημεία και συνδυαστούν σε ένα πακέτο φορητής συσκευής και βελτιωθούν στις επιδόσεις όπως δοκιμάζοντας πιο ακριβή κυκλώματα και προσθέτοντας εξωτερικές ποιοτικές κεραίες μπορούν να προσφέρουν μια καλή anti drone λύση για την αντιμετώπιση εμπορικών drone.Πρόκειται για εξοπλισμό που στηρίζεται σε open source hardware και software και που μπορεί να συνδυαστεί σε μια συσκευή χειρός και να χρησιμοποιεί τις τεχνολογίες anti-drone Jamming ,Spoofing ,DDOS Attack. Επίσης θα μπορεί να ανιχνεύσει τα λαμβανόμενα σήματα ενός UAV και να αναγνωρίσει τις επικοινωνίες του.

Βιβλιογραφία

[1] Π. Π. (. Ι. Ανδρουλάκης, «Επιχειρησιακή αξιοποίηση Anti-UAV Συστημάτων,» σε *Επιχειρησιακή αξιοποίηση Anti-UAV συστημάτων*, 2022.

[2] P. ,. K. L. H. K. Seongjoon, «Survey on Anti-Drone Systems: Components, Designs, and Challenges,» 2021.

[3] S. P. T. K. L. H. Kima, «Survey on Anti-Drone Systems: Components, Designs, and Challenges,» 2021.

[4] B. Hubbard, P. Karasz, and S. Reed,, «Two major saudi oil installations hit by drone strike, and us blames iran,» 2019.

[5] T. R. M. M. a. J. I. P. Andraši, «Night-time detection of uavs using thermal infrared camera,».

[6] D. K. Barton, «Radar system analysis and modeling.,» *Artech House,* 2004.

[7] M. L. Y. C. E. a. X. W. L. Zheng, «Radar and communication coexistence: An overview: A review of recent methods,,» *IEEE Signal Processing Magazine,,* pp. 89-96, 2019.

[8] V. C. Chen, «The micro-Doppler effect in radar.,» *Artech House,* 2019.

[9] A. Bello, «Radio Frequency Toolbox for Drone Detection and Classification,» 2019.

[10] H. Stärker, «https://cdn.rohde-schwarz.com/us/campaigns_2/a_d/Spectrum-Monitoring-with-Hybrid-AOA-TDOA-Geolocation.pdf,» σε *Spectrum Monitoring with Hybrid AOA/TDOA Geolocation*, Version 01.0, 2014.

[11] Ι. Ανδρουλάκης, «Επιχειρησιακή αξιοποίηση Anti-UAV συστημάτων-Διάλεξη,» 2022.

[12] Tower g+ community, «DroidPlanner/Tower,» 2014.

[13] I. Z. Maik Basso, «A Practical Deployment of a Communication Infrastructure to Support the Employment of Multiple Surveillance Drones Systems,» 2018.

[14] I. ,. I. U. K. ,. A. S. a. I. M. Q. Muhammad Asghar Khan, «Dynamic Routing in Flying Ad-Hoc Networks Using Topology-Based Routing Protocols,» Πακιστάν, Air University, Islamabad 44000, Pakistan; imqureshi@mail.au.edu.pk, 2018.

[15] I. M. Q. a. F. K. Muhammad Asghar Khan, «A Hybrid Communication Scheme for Efficient and Low-Cost Deployment of Future Flying Ad-Hoc Network (FANET),» 2019, p. 2.

[16] E. P. a. G. F. Luca Davoli, «Hybrid LoRa-IEEE 802.11s Opportunistic Mesh Networking for Flexible UAV Swarming,» p. 8, 2021.

[17] S. L. ,. S. X. a. J. L. Haoxiang Luo, «LECast: A Low-Energy-Consumption Broadcast Protocol for UAV Blockchain Networks,» 2023.

[18] M. A. K. ,. A. A.-Z. ,. I. U. a. K. A. A.-D. Fazal Noor, «A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics,» 2020. [Ηλεκτρονικό].

[19] A. M. a. M. T. R. Md Sadik Awal, «Nearfield RF Sensing for Feature-Detection and Algorithmic Classification of Tamper Attacks,» 2022.

[20] (. M. I. J. J. 2. (. M. I. J. K. (. I. J. K. ,. (. I. HONGGU KANG 1, «Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems,» p. 10, 2020.

[21] D. Express, «RIFF-P Anti-Drone Gun,» 2020.

[22] www.iai.co.il, «eli-4030-drone-guard,» 2023.

[23] «hackrf-portapack-with-havok-firmware».

[24] «www.jtsec.es/blog-entry/111/common-use-cases-and-getting-started-with-the-hackrf-one».

[25] «/monitor-spacex-rocket-launches-with-software-defined-radio».

[26] «hackrf.readthedocs.io».

[27] «PortaPack for HackRF One».

[28] «github.com/sharebrained/portapack-hackr».

[29] «Github-Flasher nodemcu».

[30] «circuitdigest.com/microcontroller-projects/diy-wifi-jammer-using-nodemcu».

[31] «/circuitdigest.com/microcontroller-projects».

[32] I. Z. E. T. L. ,. W. 3. a. E. P. d. F. Maik Basso, «A Practical Deployment of a Communication Infrastructure to Support the Employment of Multiple Surveillance Drones Systems,» p. 3, 2018.

[33] Ι. Ανδρουλάκης, «Επιχειρησιακή αξιοποίηση Anti-UAV συστημάτων,» 2022.

[34] Ι. Ανδρουλάκης, «Επιχειρησιακή αξιοποίηση Anti-UAV συστημάτω».

[35] Hubbard, P. Karasz, and S. Reed, ‘‘Two major Saudi oil installations hit by drone strike, and US blames Iran,’’ The New York Times, Sep. 14, 2019.

[36] C. W. Ripley. (2015). Drone With Radioactive Material Found on Japanese Prime Minister’s Roof. Accessed: Apr. 22, 2015. [Online]. Available:

https://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html