Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στα Συστήματα Ασύρματης Επικοινωνίας

Σύστημα Απενεργοποίησης Drone

Κωνσταντίνος Αντωνίου

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σταύρου

Μάιος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Σύστημα Απενεργοποίησης Drone

Κωνσταντίνος Αντωνίου

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σταύρου

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Συστήματα Ασύρματης Επικοινωνίας

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2018

Περίληψη

Η μεταπτυχιακή διατριβή αποσκοπεί στη μελέτη και ανάπτυξη ενός συστήματος απενεργοποίησης drone. Ο απώτερος σκοπός είναι να αποδείξει ότι υπάρχει η δυνατότητα ανάπτυξης low-cost συστήματος, που να έχει ως βάση εξαρτήματα RF που κυκλοφορούν στην αγορά, το οποίο να απενεργοποιεί ή να εμποδίζει αποτελεσματικά την λειτουργία των υφιστάμενων commercial drones σύμφωνα με την υφιστάμενη τεχνολογία και την αρχή λειτουργίας τους και συνεπώς την αντιμετώπιση των κινδύνων που εγκυμονεί η ανεξέλεγκτη χρήση τους. Με αυτό τον τρόπο θα αποδειχθεί ότι η τεχνολογία που χρησιμοποιούν τα drones που κυκλοφορούν στην αγορά επιτρέπει την αντιμετώπιση των κινδύνων που μπορούν να προκαλέσουν και ότι είναι εφικτή η ενίσχυση της ασφάλειας ανθρώπων, σημαντικών περιοχών και εγκαταστάσεων αποτελεσματικά και με χαμηλό κόστος.

Η διατριβή αυτή ξεκινά προβαίνοντας σε μια αναλυτική βιβλιογραφική ανασκόπηση όσον αφορά γενικά τα drones, την προέλευση τους, τις χρήσεις και εφαρμογές τους αλλά και τους κινδύνους και τις απειλές που ενέχονται από την ανεξέλεγκτη χρήση τους. Ακολούθως γίνεται αναφορά στην τεχνολογία των Ασύρματων Επικοινωνιών και συγκεκριμένα στις ευπάθειες που παρουσιάζει και οι οποίες μπορούν να τύχουν εκμετάλλευσης για επιθέσεις. Για την προετοιμασία του αναγνώστη για το στάδιο ανάπτυξης του συστήματος, προηγούνται κάποια κεφάλαια τα οποία εισάγουν στην υφιστάμενη τεχνολογία των drones με παρουσίαση των διαφόρων κατηγοριών αλλά και των πιο σημαντικών συστημάτων που υπάρχουν στην αγορά. Επίσης γίνεται ανάλυση και περιγραφή των τεχνολογιών που χρησιμοποιούν αυτά τα συστήματα, οι οποίες και αναπτύσσονται στα κεφάλαια που ακολουθούν. Στο στάδιο της ανάπτυξης του συστήματος, αφού περιγραφεί η μεθοδολογία που θα ακολουθηθεί, παρουσιάζονται βήμα προς βήμα, με εκτενή περιγραφή και με την βοήθεια εικόνων και διαγραμμάτων, τόσο τα υλικά, εξαρτήματα και συσκευές που χρησιμοποιήθηκαν για την κατασκευή, όσο και οι ενέργειες που εκτελέστηκαν για την ολοκλήρωση του συστήματος. Ακολούθως παρουσιάζεται ο πειραματικός έλεγχος του συστήματος που πραγματοποιήθηκε σε εργαστήριο, η διαδικασία και τα αποτελέσματα του οποίου παρατίθενται, όπου και επιβεβαιώθηκε η αρχική πρόταση, όπως διατυπώθηκε στο δεύτερο κεφάλαιο της διατριβής αυτής.

Summary

This Thesis aims to study and develop a drone deactivation system. The main goal is to prove the possibility of developing a low-cost system based on RF components available on the market which effectively deactivates or prevents the operation of existing commercial drones in accordance with existing technology and operating principle and thus addressing the dangers of their uncontrolled use. This will prove that the technology used by drones available on the market enables them to address the risks they can cause and that it is feasible to enhance the safety of people, important areas and facilities efficiently and at low cost.

This thesis begins with a detailed bibliographic review of drones in general, their origins, uses and applications, and the dangers and threats involved in their uncontrolled use. Then reference is made to wireless communications technology, in particular the vulnerabilities it presents and which can be exploited for attacks. In order to prepare the reader for the system's development stage, some chapters are introduced into the existing drones technology with a presentation of the different categories and of the most important systems available on the market. It also analyzes and describes the technologies used by these systems, which are developed in the following chapters. At the stage of developing the system, after describing the methodology to be followed, step by step, with extensive description and with the help of pictures and diagrams, the materials, components and devices used for the construction, as well as the actions performed to complete the system. The experimental control of the system was carried out in a laboratory, the procedure and the results of which are listed, where the initial proposal was confirmed, as stated in the second chapter of this dissertation.

Αφιερώνεται στην Ελεάνα…

Για την τεράστια χαρά που μου πρόσφερε όταν έγινα νονός της λίγες μέρες μετά την ολοκλήρωση της Διατριβής αυτής

Ευχαριστίες

Πρωτίστως, θα ήθελα να ευχαριστήσω την οικογένεια μου για την αμέριστη υποστήριξη που μου παρείχε κατά τη διάρκεια της φοίτησης μου στο Μεταπτυχιακό Πρόγραμμα στα Συστήματα Ασύρματης Επικοινωνίας.

Θα ήθελα επίσης να ευχαριστήσω τον Επιβλέπων Καθηγητή Δρ. Σταύρο Σταύρου, ο οποίος είναι ο άνθρωπος που μου έδωσε τις κατευθύνσεις για τη σωστή προσέγγιση του θέματος και τη διεξαγωγή της έρευνας. Εκφράζω την ευγνωμοσύνη μου, τόσο για τις συμβουλές όσο και για την καθοδήγηση στην υλοποίηση του εργαστηριακού κομματιού της Διατριβής αυτής.

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ ΑΓΓΛΙΚΩΝ ΟΡΩΝ

CRC – Cyclic Redundancy Check

DFS – Dynamic Frequency Selection

DoD – Department of Defense

Dos – Denial 0f Service

DSSS – Direct Sequence Spread Spectrum

EMR – Electromagnetic Radiation

FAA – Federal Aviation Administration

FCC – Federal Communication Commission

FFT – Fast Fourier Transform

FPV – First Person View

GNSS – Global Navigation Satellite System

GPS – Global Positioning System

HD – High Definition

IEEE – Institute of Electrical and Electronics Engineers

IF – Intermediate Frequencies

LNA – Low Noise Amplifier

MAC – Medium Access Control

MEO – Medium Earth Orbit

MIMO – Multiple Input Multiple Output

NMEA – National Marine Electronic Association

NSA – National Security Agency

OFDM – Orthogonal Frequency Decision Multiplexing

PLL – Phase Lock Loop

PoC - Proof of Concept

RF – Radio Frequencies

RHCP – Right Hand Circular Polarization

RNSS – Radio Navigation Satellite Service

SNIR – Signal to Noise plus Interference Ratio

SNR – Signal to Noise Ratio

UAV – Unmanned Air Vehicle

USAF – United States Air Force

VCO – Voltage Control Oscillator

VSWR – Voltage Standing Wave Ratio

WiMAX – Worldwide Interoperability for Microwave Access

ΣΥΝΤΜΗΣΕΙΣ

Amp – Ampere

EMF – Electromagnetic Field

Glonass – Global Navigation Satellite System

PHY – Physical Layer

SMA – Subminiature version A

Κεφάλαιο 1
Εισαγωγή

Κατά τον εικοστό αιώνα ο άνθρωπος άρχισε να βλέπει οχήματα στον ουρανό ως συνέχεια της εξέλιξης τους από τις άμαξες, τις οποίες έσερναν ζώα, στα τρένα και τα αυτοκίνητα, για να φτάσουμε στη μαζική χρήση των αεροσκαφών τα οποία με χειριστή τον άνθρωπο έφεραν την ανθρωπότητα σε μια νέα εποχή. Οι μεγάλες δυνατότητες και ευκαιρίες που πρόσφερε η εκμετάλλευση του εναέριου χώρου από τον άνθρωπο, οδήγησαν στην ραγδαία εξέλιξη της αεροπορικής επιστήμης η οποία έχει να επιδείξει τεράστια επιτεύγματα ειδικά την τελευταία εικοσαετία. Στον εικοστό πρώτο αιώνα γίναμε μάρτυρες της μαζικής εμφάνισης στον αέρα μη επανδρωμένων οχημάτων, γνωστών και ως drones. Η απουσία πιλότου από το όχημα και η καθοδήγηση του από πιλότο στο έδαφος είναι αυτό που χαρακτηρίζει την νέα αυτή πρωτοποριακή μέθοδο χειρισμού εναέριων οχημάτων. Ο χειρισμός του μη επανδρωμένου οχήματος μπορεί να γίνει είτε από χειριστή σε κοντινή απόσταση στο έδαφος είτε από χειριστή ο οποίος βρίσκεται χιλιόμετρα μακριά είτε και ακόμα από την άλλη άκρη του πλανήτη.

Η ραγδαία αναδυόμενη τεχνολογία των drones αποτελεί εξέλιξη και ολοκλήρωση των πρώτων αμυντικών συστημάτων που αναπτύχθηκαν κατά το τέλος του εικοστού αιώνα από αμυντικές βιομηχανίες για καθαρά στρατιωτικούς σκοπούς. Με την εξέλιξη όμως

της τεχνολογίας και την γεωμετρική πρόοδο που παρουσιάζεται στον τομέα της μικροηλεκτρονικής, η κατασκευή όλο και μικρότερων αλλά και φθηνότερων μη επανδρωμένων οχημάτων, έχουν δώσει τη δυνατότητα σε πάρα πολλές εταιρείες να αναπτύξουν Drones διαφόρων κατηγοριών και πολλαπλών ρόλων και δυνατοτήτων για ιδιωτική χρήση από τον άνθρωπο. Η δυνατότητες τους να συλλέγουν δεδομένα, να μεταφέρουν φορτία και να προσεγγίζουν δυσπρόσιτα μέρη χωρίς κίνδυνο για το χειριστή, έχουν επανακαθορίσει τον τρόπο με τον οποίο βλέπουμε και αντιλαμβανόμαστε το φυσικό περιβάλλον. Η επιρροή τους πλέον σε τομείς όπως η επιστήμη, η κοινωνία, η τεχνολογία αλλά και η ασφάλεια είναι σημαντική και καθοριστική με αποτέλεσμα να θεωρείται ένα απαραίτητο και πολύτιμο εργαλείο για πολλούς τομείς και υπηρεσίες. Ο αμυντικός τομέας αποτελεί τον πιο δυνατό οδηγό για την ανάπτυξη και εξέλιξη των drones. Λόγω της συνεχής και επιβεβλημένης ανάγκης των κρατών να υπερασπίσουν την κυριαρχία τους και την ασφάλεια των πολιτών τους, επενδύουν τεράστια ποσά για έρευνα, ανάπτυξη και αγορά συστημάτων και εφαρμογών που θα τους δίνουν το ζωτικό πλεονέκτημα στο συγκεκριμένο τομέα. Οι δυνατότητες που δίνει ένα μη επανδρωμένο όχημα στις Ένοπλες Δυνάμεις και τα Σώματα Ασφαλείας των κρατών, ειδικά στην πρόληψη και αποτροπή εχθρικών επιθετικών ενεργειών, ήταν καθοριστικός παράγοντας στην εξέλιξη και βελτίωση τους εντάσσοντας πλέον αυτό το εργαλείο σε όλα τα επιχειρησιακά σχέδια των κυβερνητικών υπηρεσιών ασφαλείας.

Τα τελευταία χρόνια η εξάπλωση των drones είναι ραγδαία και η χρήση τους από τον άνθρωπο έχει αρχίσει να γίνεται ανεξέλεγκτη. Λόγω της σημαντικής εξέλιξης της τεχνολογίας στον τομέα αυτό, η αγορά έχει πλέον να επιδείξει μια μεγάλη γκάμα μοντέλων των οποίων το κόστος αγοράς δεν είναι πλέον απαγορευτικό για τον πολίτη. Τα διάφορα μεγέθη, ο εξοπλισμός που κουβαλούν, η εύκολη χρήση τους, το βάρος αλλά και η αυτονομία τους, τους επιτρέπουν να απευθύνονται σε όλες σχεδόν τις ομάδες του πληθυσμού, τόσο ηλικιακές όσο και κοινωνικές και οικονομικές με αποτέλεσμα να χρησιμοποιείται από ένα ανήλικο παιδί μέχρι από μια επιχείρηση, από την αστυνομία και το στρατό. Η ολοένα και αυξανόμενη χρήση τους όμως χωρίς περιορισμούς εγκυμονεί αρκετούς κινδύνους και είναι θέμα χρόνου να αρχίσουν να χρησιμοποιούνται για τους λάθος σκοπούς. Είναι πλέον εφικτό για οποιοδήποτε αποσκοπεί σε δολιοφθορά ή ακόμα και τρομοκρατική ενέργεια, να εξοπλιστεί με τέτοιου είδους μέσα τα οποία εύκολα μπορούν να τροποποιηθούν και να μετατραπούν σε πολύ επικίνδυνα

όπλα με καταστροφικές συνέπειες για τον απλό πολίτη ή και ακόμα για τα Σώματα Ασφαλείας. Διάφορα μεμονωμένα περιστατικά ανά την υφήλιο μέχρι στιγμής έχουν αποδείξει ότι το συγκεκριμένο σύστημα μπορεί να προκαλέσει ακούσια ή εκούσια από μικρές ζημιές μέχρι και θανάτους κρούοντας τον κώδωνα του κινδύνου ότι πλέον ο πλανήτης βρίσκεται αντιμέτωπος με μια νέα ασύμμετρη απειλή. Η απειλή αυτή όμως μπορεί να προληφθεί και να αντιμετωπιστεί τόσο με νομοθεσίες και κανονισμούς όσο και με αντίμετρα. Ήδη τα τελευταία χρόνια έχουν εκδοθεί οδηγίες και κανονισμοί για το χειρισμό των drones έτσι ώστε να προληφθούν ακούσια ατυχήματα. Στην περίπτωση όμως που το drone χρησιμοποιείται με σκοπό την εκούσια πρόκληση ζημιάς οι κανονισμοί και οι νομοθεσίες παραβιάζονται και πλέον απαιτούνται αντίμετρα για την αντιμετώπιση τους. Είναι γνωστό ότι ένα εχθρό μπορείς να τον αντιμετωπίσεις αν γνωρίζεις τον τρόπο που λειτουργεί αλλά και τις αδυναμίες του. Η λειτουργία των drones όμως δεν είναι ιδιαίτερα πολύπλοκη και βασίζεται στις σύγχρονες τεχνολογίες Ασύρματης Επικοινωνίας με αποτέλεσμα το σύνολο των εμπορικών κυρίως drones να λειτουργούν με τον ίδιο περίπου τρόπο. Έτσι η ανάπτυξη αντιμέτρων είναι εφικτή και ήδη εφαρμοσμένη.

Οι Ένοπλες Δυνάμεις αρκετών κρατών είναι πλέον εξοπλισμένες με πανάκριβα, ισχυρά συστήματα παρεμβολής τα οποία με τη χρήση ευρυζωνικού σήματος θορύβου, απενεργοποιούν τέτοιες απειλές και προστατεύουν ευαίσθητες περιοχές, εγκαταστάσεις και ανθρώπινες ζωές. Τα συστήματα αυτά αρχικά αναπτύχθηκαν και χρησιμοποιήθηκαν για την αντιμετώπιση στρατιωτικών απειλών και συγκεκριμένα μη επανδρωμένων αεροσκαφών UAVs γι’ αυτό και οι απαιτήσεις, οι δυνατότητες τους και εν συνεπεία η τιμή τους ήταν σχετικά υψηλές. Με το νέο κίνδυνο όμως που παρουσιάζεται με την ανορθόδοξη χρήση των commercial drones, η απαίτηση για ανάπτυξη μικρών και χαμηλού κόστους συστημάτων απενεργοποίησης τους είναι επιβεβλημένη.

Στα επόμενα κεφάλαια της μεταπτυχιακής διατριβής θα γίνει εκτενέστερη αναφορά στα προβλήματα που παρουσιάζονται από την ανεξέλεγκτη χρήση των drones και θα προταθεί τρόπος αντιμετώπισης τους. Στη συνέχεια θα προχωρήσουμε σε σύντομη αναφορά σε ιστορικά γεγονότα χρήσης παρεμβολών σε συστήματα Ασύρματης Επικοινωνίας, θα αναφερθούν οι υφιστάμενες τεχνολογίες jamming αλλά και η νομοθεσία που διέπει αυτό τον τομέα. Θα παρουσιαστούν και θα περιγραφούν διάφορα μοντέλα drones της αγοράς, τα χαρακτηριστικά και οι τεχνολογίες που χρησιμοποιούν

και στα τελευταία κεφάλαια του πρώτου μέρους θα γίνει αναλυτική περιγραφή στις τεχνολογίες επικοινωνίας και καθοδήγησης των drones.

Στο δεύτερο μέρος της μεταπτυχιακής διατριβής θα περιγραφεί μια μεθοδολογία ανάπτυξης συστήματος απενεργοποίησης drone και στη συνέχεια θα παρουσιαστεί η εφαρμογή της μεθοδολογίας αυτής και η ανάπτυξη του συστήματος. Στο τέλος θα παρατεθούν τα αποτελέσματα των εργαστηριακών ελέγχων και τα συμπεράσματα της Διατριβής αυτής.

Κεφάλαιο 2
UAVs-Drones

2.1 Προέλευση-Ορισμοί

Η χρήση των UAVs ή drones όπως είναι ευρέως γνωστά, έχει γίνει αντικείμενο συζήτησης κατά πόσο αποτελεί ένα χρήσιμο και αποτελεσματικό εργαλείο για διάφορες υπηρεσίες ή μια συσκευή η οποία παραβιάζει την ασφάλεια και την προστασία της ιδιωτικής ζωής και ιδιοκτησίας του ανθρώπου. Η ευρεία χρήση της συσκευής αυτής ως εξοπλισμού επιτήρησης και η μαζική εμπορική χρήση της έχει επικριθεί αρκετά παρόλο που τα drones έχουν νομιμοποιηθεί με κανονισμούς και άδειες από κρατικές υπηρεσίες. Παρά τις πολλαπλές επικρίσεις από διάφορες ανθρωπιστικές οργανώσεις οι οποίες τονίζουν την ανικανότητά των αεροχημάτων αυτών να ξεχωρίσουν και να αξιολογήσουν εκούσιες και ακούσιες ενέργειες εν δυνάμει στόχων, η επίσημη στάση των κυβερνήσεων είναι ότι τα αεροχήματα αυτά εμποδίζουν τις ανθρώπινες απώλειες παρέχοντας ακριβείς πληροφορίες επιτήρησης και ικανότητες άμεσης αντίδρασης και κρούσης.

Παραδοσιακά, οι συζητήσεις γύρω από UAVs επικεντρώνονται γύρω από τη χρήση τους για στρατιωτική επιτήρηση ή ακόμα και μάχη. Από τότε που πρωτοεμφανίστηκαν, η χρήση τους σε πολεμικές επιχειρήσεις υπήρξε έντονη με αποτέλεσμα να γίνεται αρκετή συζήτηση όσον αφορά τη δεοντολογία, την αποτελεσματικότητα, την διαφάνεια αλλά και νομιμότητα [1].

Τα μη επανδρωμένα αεροχήματα (UAVs), κοινώς γνωστά και ως drones, έχουν ένα ευρύ ορισμό κάτι που είναι λογικό αν λάβουμε υπόψη το ευρύ φάσμα των διαμορφώσεων τους. Μια ερμηνεία του drone από τον Villasenor J. στο βιβλίο του 'What is a drone anyway?' είναι "ένα μη επανδρωμένο αεροσκάφος που μπορεί να πετάξει αυτόνομα "[2]. Από την άλλη όμως, πολλά αεροσκάφη με τηλεχειρισμό έχουν πολύ περιορισμένη ανεξαρτησία, οπότε είναι ακατάλληλο να καθορίσουμε την ικανότητα πτήσης αυτόνομα ως υποχρεωτικό χαρακτηριστικό.

Η πρώτη χρήση του όρου "drone" φαίνεται να προέρχεται από το Ναυτικό των ΗΠΑ το 1935 όταν και είχε ξεκινήσει ένα πρόγραμμα για την παραγωγή τηλεχειριζόμενου αεροχήματος ως στόχου. Μετά από μια επίσκεψη Αμερικανών για παρακολούθηση του αντίστοιχου προγράμματος από το Βασιλικό Ναυτικό της Αγγλίας, καθώς τους έγινε επίδειξη των αντίστοιχων μοντέλων 'Fairy Queen' και 'Queen B' ή αλλιώς 'Queen Bee', το Πολεμικό ναυτικό της Αμερικής υιοθέτησε τον όρο "drone" για τα δικά του μοντέλα βασισμένα στις ονομασίες που έδωσε το Βασιλικό ναυτικό, Queen Bees ("Bee"=μέλισσα, "drone"=κηφήνας). Η χρήση αυτού του όρου εντοπίζεται για πρώτη φορά στο Oxford English Dictionary και επίσης εμφανίζεται το 1947 στην Εγκυκλοπαίδεια Britannica [2].

Πολύ σημαντικοί αποτελούν και οι ορισμοί που χρησιμοποιούνται από τους αρμόδιους οργανισμούς σε όλο τον κόσμο. Για παράδειγμα, ο FAA των ΗΠΑ ορίζει ένα UAV ως "Μια συσκευή που χρησιμοποιείται ή προορίζεται για να χρησιμοποιείται για πτήση στον αέρα και δεν έχει επιβιβασμένο χειριστή. Αυτή η συσκευή αποκλείει πυραύλους, όπλα ή εκρηκτικές κεφαλές, αλλά περιλαμβάνει όλες τις κατηγορίες αεροπλάνων, ελικόπτερα, αερόπλοια, και αεροσκάφη χωρίς χειριστή. Επίσης δεν περιλαμβάνει τα παραδοσιακά μπαλόνια, ρουκέτες, συνδεδεμένα αεροσκάφη και ανεμοπλάνα χωρίς κινητήρα." Γενικά μπορούμε να πούμε ότι κάθε εναέριο όχημα το οποίο για να πετάξει δεν βασίζεται σε χειριστή ο οποίος να βρίσκεται επιβιβασμένος στο όχημα, είτε λειτουργεί αυτόνομα είτε εξ αποστάσεως, θεωρείται UAV [1].

Η ανάπτυξη των μη επανδρωμένων εναέριων οχημάτων (UAVs) προέρχεται από τη στρατιωτική έρευνα. Αν και αρχικά σχεδιάστηκε ως όπλο με σκοπό τη μείωση του ρίσκου για τους χειριστές σε εχθρικό έδαφος, η τεχνολογία, οι δυνατότητες, και η χρήση των UAVs έχει εξελιχθεί από τότε ώστε να περιλαμβάνει πλέον παρακολούθηση και συλλογή δεδομένων. Κομβικό σημείο αποτέλεσε η εμφάνιση του τυφώνα Κατρίνα το 2005 όπου από αποκλειστικά στρατιωτική εφαρμογή το drone έγινε πολιτική εφαρμογή. Στις μεγάλες προσπάθειες διάσωσης που ακολούθησαν, τα στρατιωτικά drones εξοπλισμένα με ακριβείς υπέρυθρες κάμερες αναγνωρίστηκαν ευρέως πλέον ως ένα χρήσιμο εργαλείο στην υπηρεσία του πολίτη. Αυτό οδήγησε την Ομοσπονδιακή Υπηρεσία Αεροπορίας (FAA) να εκδώσει για πρώτη φορά πιστοποιητικά που να επιτρέπουν τη χρήση στρατιωτικών drones του τύπου M7RQ να πετούν στον εναέριο χώρο πάνω από τους πολίτες το 2006. Έκτοτε, τα drones έχουν εισέλθει στην εμπορική αγορά μετά από χρόνια ανάπτυξης [1].

2.2 Χρήσεις

Κατά τη διάρκεια των τελευταίων δεκαετιών, οι διάφορες τεχνολογικές εξελίξεις συνδυάστηκαν έτσι ώστε να επιτρέψουν την σημαντική βελτίωση των δυνατοτήτων των drones. Οι πηγές τροφοδοσίας πλέον καταλαμβάνουν πολύ μικρό χώρο επιτρέποντας όμως τόσο στο σύστημα πλοήγησης όσο και στον υπόλοιπο ενσωματωμένο εξοπλισμό να τροφοδοτούνται για αρκετή ώρα. Υπάρχει πλέον η δυνατότητα χρήσης του GPS το οποίο επιτρέπει στο drone να γνωρίζει τη θέση του. Έχουν ενσωματωθεί αισθητήρες χαμηλής κατανάλωσης οι οποίοι παρέχουν συνεχώς στοιχεία για τη θέση και την κατεύθυνση του αεροχήματος. Υπάρχουν επίσης ολοκληρωμένα συστήματα για εκτέλεση υπολογισμών όσον αφορά τη πτήση αλλά και επικοινωνία με το έδαφος.

Πριν από μερικά χρόνια η χρήση των drones περιοριζόταν σε εναέριες επιδείξεις κυρίως για ψυχαγωγία. Ο άνθρωπος ο οποίος από τη φύση του ελκύεται και εντυπωσιάζεται από καθετί διαφορετικό το οποίο καταρρίπτει τα όσα γνώριζε και αντιλαμβανόταν μέχρι πρότινος, ποτέ δεν φανταζόταν ότι τα όρια αυτού του τεχνολογικού επιτεύγματος θα έσπαζαν τόσο γρήγορα και από ένα μικρό όχημα το οποίο απλά πετά τηλεχειριζόμενο από το έδαφος σήμερα θα αποτελούσε ένα φανταστικό εργαλείο μεταφοράς φορτίου και συλλογής όλων των ειδών πληροφοριών.

Τα μικρά αυτά drones δίνουν πλέον τη δυνατότητα στον άνθρωπο να έχει απομακρυσμένη πρόσβαση σε τοποθεσίες όπου η συνήθης πρόσβαση είναι αρκετά δύσκολη έως αδύνατη, σε περιοχές όπου δεν υπάρχει εύκολα οπτική επαφή ή άλλες δυσπρόσιτες περιοχές όπως θάλασσες, λίμνες φαράγγια και μονοπάτια όπου δύσκολα προσεγγίζει ο άνθρωπος είτε πεζός είτε με όχημα.

Όσον αφορά τα μεγάλα drones, το πιο σημαντικό είναι η εξοικονόμηση που υπάρχει από την απουσία χειριστή πάνω στο αεροσκάφος. Αυτό έχει διάφορες επιπτώσεις όσον αφορά το σχεδιασμό του αεροσκάφους όπως:

1. Αφαιρεί την ανάγκη για χώρο και δυνατότητα μεταφοράς:

    1.1. πιλότου

    1.2. οθονών και χειριστηρίων δεδομένων

    1.3. εγκαταστάσεων υποστήριξης του πιλότου, όπως ρύθμισης της πίεσης του αέρα, παροχή οξυγόνου και μέσα για εγκατάλειψη του σκάφους

2. Επιτρέπει μια πολύ μεγαλύτερη αναλογία χώρου και βάρους με επιπτώσεις στο καύσιμο, στην αυτονομία και στις λειτουργίες που πρέπει να εκτελεστούν.

3. Επίσης μειώνεται το κόστος από την χρήση εξοπλισμού και υλικών για προστασία του πιλότου στο σκάφος [2].

Τα μικρά drones απολαμβάνουν ένα σημαντικό πλεονέκτημα έναντι των μεγάλων drones, αφού δεν χρειάζονται να προσαρμόσουν χαρακτηριστικά ασφαλείας τα οποία απαιτούνται τόσο σε μεγάλα drones όσο και σε επανδρωμένα αεροσκάφη. Επίσης τα μικρά drones τείνουν να υποκαθιστούν όλο και περισσότερο τα μεγάλα drones αφού η εξέλιξη της τεχνολογίας και η βελτίωση των ικανοτήτων τους, τους δίνουν τη δυνατότητα να εκτελούν λειτουργίες τις οποίες προηγουμένως μπορούσαν να εκτελούν μόνο μεγάλα drones όπως είναι ο αεροψεκασμός που ήδη εφαρμόζεται στην Ιαπωνία.

Οι τιμές αγοράς για μικρά drones αυτή τη στιγμή κυμαίνονται για χομπίστες από 100-1000 USD/EUR και για επαγγελματική χρήση από 5000-10000 USD/EUR. Για ορισμένες

εφαρμογές, το ενδεικτικό κόστος ανά ώρα πτήσης είναι σήμερα της τάξης των 25 USD/EUR για μικρά αεροσκάφη σε σύγκριση με 750 USD/EUR για επανδρωμένα αεροσκάφη σταθερής πτέρυγας και 1350 USD/EUR για επανδρωμένα ελικόπτερα [2]. Για εφαρμογές τις οποίες κάποιοι περιορισμοί μπορούν να γίνουν αποδεκτοί, όπως η καταγραφή εικόνας και βίντεο μέτριας έως καλής ποιότητας, τα μικρά drones είναι τώρα πολύ πιο οικονομικά από τα επανδρωμένα αεροσκάφη και από τα μεγάλα drones.

Στον εμπορικό χώρο, τα drones θεωρούνται πλατφόρμες αισθητήρων όλων των ειδών και χρησιμοποιούνται κυρίως για επιτήρηση και την αναγνώριση. Σήμερα, τα drones χρησιμοποιούνται ακόμα και σε παρακολούθηση των αγροτικών καλλιεργειών, σε επιχειρήσεις έρευνας και διάσωσης, για μέτρηση και καταγραφή της άγριας ζωής, στην τοπογραφία, την έρευνα δασικών πυρκαγιών, για να επιθεωρούν τους αγωγούς πετρελαίου, τις γραμμές μεταφοράς ηλεκτρικής ενέργειας και άλλες απομακρυσμένες υποδομές. Η ικανότητά τους να μεταφέρουν βαρύ εξοπλισμό αποτέλεσε καθοριστική για τη χρήση τους στην καλλιέργεια με τον ψεκασμό καλλιεργειών σε μεγάλες εκμεταλλεύσεις, την παράδοση τροφής, ιατρικών προμηθειών και φαρμάκων σε απρόσιτες θέσεις [1].

Η πιο κοινή εφαρμογή για ιδιώτες, επιχειρήσεις και χομπίστες είναι η αεροφωτογραφία. Τα εμπορικά drones διατίθενται με ενσωματωμένες κάμερες ή αρθρωτές ρυθμίσεις που επιτρέπουν την εγκατάσταση ελαφρών συσκευών. Παρόλο που ο κανονισμός ορίζει ότι τα drones στον εσωτερικό εναέριο χώρο μπορούν να πετάξουν μόνο με οπτική επαφή, η μακρινή πτήση είναι δυνατή αυτή τη στιγμή με τη χρήση κάμερας επί του σκάφους για τη ροή ζωντανού βίντεο σε smartphones και φορητούς υπολογιστές.

Χάρη στην εγγύτητα στην οποία μπορεί να λειτουργεί το UAV και τον περιορισμένο θόρυβο σε σύγκριση με ένα πραγματικό αεροσκάφος, μπορεί να χρησιμεύσει για stealthier αποστολές όπως η ανίχνευση και η παρακολούθηση της άγριας ζωής.

Η χρήση των drones ως εργαλείο επιτήρησης και συλλογής δεδομένων και πληροφοριών χρονολογείται στα τέλη του 18ου αιώνα (χρησιμοποιώντας μπαλόνια) και έχει χρησιμοποιηθεί όλο και πιο εντατικά από διάφορες χώρες από τη δεκαετία του 1960.

Τα είδη των δεδομένων που μπορούν να συγκεντρωθούν είναι ποικίλα και περιλαμβάνουν:

- δεδομένα ηλεκτρομαγνητικού φάσματος
- εικόνα και βίντεο στην περιοχή του ορατού φάσματος
- εικόνα και βίντεο που είναι κοντά στον ορατό φάσμα (κυρίως στο υπέρυθρο φάσμα)
- ραδιοφωνικές μεταδόσεις
- άλλες ηλεκτρονικές μεταδόσεις

άλλα είδη δεδομένων όπως:

- ήχος στο ανθρώπινο ακουστικό φάσμα
- κύματα πίεσης αέρα άλλων συχνοτήτων
- βιολογικά δεδομένα
- μαγνητικά και άλλα γεωφυσικά δεδομένα
- μετεωρολογικά δεδομένα [2]

Κατά τη διάρκεια των τελευταίων είκοσι ετών, η εξάπλωση του Διαδικτύου ως πλατφόρμα εμπορίου επέτρεψε στις επιχειρήσεις να κερδίσουν περισσότερη ορατότητα, μείωση του κόστους και ανίχνευση της διαδρομής του εμπορεύματος με αποτέλεσμα να αφήνουν όλο και περισσότερο «το περιβάλλον από τούβλα και κονίαμα». Ωστόσο, η υποδομή της εφοδιαστικής αλυσίδας και συγκεκριμένα της διανομής εξακολουθεί να εξαρτάται από τις επίγειες και εναέριες μεταφορές. Τα drones επιτρέπουν πλέον μια νέα μορφή μεταφοράς και παράδοσης. Η Amazon Prime Air, η DHL και η Google πρωτοπορούν διερευνώντας τον νέο τύπο μηχανισμού παράδοσης. Η Amazon έχει δηλώσει ότι μόλις ολοκληρωθεί η νέα υπηρεσία θα είναι σε θέση να παραδώσει περισσότερο από το 80% των εμπορευμάτων τους μέσω του αέρα [1].

2.2.1 Γενικές εφαρμογές

Μετά τη σύντομη περιγραφή των γενικών χαρακτηριστικών και των ιδιοτήτων των drones, θα αναφερθούμε στις γενικές εφαρμογές αυτών των αεροχημάτων. Πιο κάτω γίνεται αναφορά σε ένα φάσμα συγκεκριμένων εφαρμογών που σχετίζονται με τον

πολιτικό τομέα, ωστόσο, μεγάλο μέρος των δυνατοτήτων των drones, αναπτύχθηκε και εφαρμόστηκε στον στρατό.

Στη συνέχεια μπορούμε να δούμε τις κυριότερες του στρατιωτικές χρήσεις ως τώρα:

- ως στόχος, από τη δεκαετία του '30
- ως μέσον παρενόχλησης και εκτροπής της προσοχής. Τα drones θεωρούνται ότι έχουν χρησιμοποιηθεί με επιτυχία από το Ισραήλ γι' αυτό το σκοπό, κατά τη διάρκεια του πολέμου του Yom Kippur το 1973
- ως συσκευή αναμετάδοσης επικοινωνίας-relay
- ως μέσο ηλεκτρονικού πολέμου, για παρεμβολή ή διακοπή των εχθρικών επικοινωνιών
- ως μέσο πραγματοποίησης επιθέσεων:
    - σε επιφανειακούς και θαλάσσιους στόχους, τεχνική η οποία αναπτύχθηκε όχι αργότερα από το 1915 στις Η.Π.Α. και εφαρμόζεται μέχρι και σήμερα
    - σε εναέριους στόχους, συμπεριλαμβανομένων άλλων αεροσκαφών. Παραδείγματα επίσημα δεν υπάρχουν λόγω της μη επιβεβαιωμένης εμπλοκής μερών που έχουν πρόσβαση σε τέτοιες τεχνολογίες [2]

Όσον αφορά πολιτικές εφαρμογές τα drones μπορούν να εκτελέσουν επικίνδυνες για τον άνθρωπο αποστολές όπως:

- Αναζητήσεις αγνοουμένων και πλοίων, σε αντίξοες καιρικές συνθήκες ή σε δύσκολα-προσβάσιμα εδάφη
- Εκτέλεση επιχειρήσεων για μεγάλες χρονικές περιόδους και σε μεγάλες αποστάσεις
- Συμβολή σε επιχειρήσεις έκτακτης ανάγκης, συμπεριλαμβανομένων ερευνών για πυρκαγιές, ηφαιστειακές δραστηριότητες, σεισμικές ζώνες, πλημμυρισμένες περιοχές ακόμα και σε ατυχήματα σε πυρηνικούς αντιδραστήρες
- Πυρόσβεση
- Παρακολούθηση των ατμοσφαιρικών συνθηκών λίγο πριν και ακόμα και κατά τη διάρκεια του μεγάλης κακοκαιρίας

Άλλες σημαντικές δραστηριότητες στις οποίες δεν απαιτείται σημαντική συμβολή του ανθρώπου είναι:

- η σάρωση ηλεκτρομαγνητικού φάσματος και η συλλογή άλλων ειδών δεδομένων
- η μεταφορά εμπορευμάτων [2]

2.3 Κίνδυνοι για την Ασφάλεια

2.3.1 Περιστατικά

Η ιδιωτική χρήση των drones δημιουργεί προοπτικές για πολλαπλά οφέλη για τον άνθρωπο όμως παράλληλα οδήγησε στην εμφάνιση νέων κινδύνων μέσω παρεμβολών, ατυχημάτων και βίαιων ενεργειών. Τα περισσότερα περιστατικά που έχουν αναφερθεί μέχρι σήμερα δεν είχαν πολύ τραγικές επιπτώσεις στο κοινό. Υπήρξαν όμως περιπτώσεις όπως στο Κονγκό όπου η συντριβή ενός drone είχε ως αποτέλεσμα τον θάνατο [3]. Στην Κορέα επίσης προκλήθηκε θανατηφόρο δυστύχημα που προέκυψε από λάθος του χειριστή σε συνδυασμό με την απώλεια του σήματος GPS από το από το drone [4]. Μεγάλος αριθμός μικροατυχημάτων έχουν αναφερθεί κυρίως πάνω από την Καμπούλ το 2004 [5]. Πολύ σημαντικό είναι το γεγονός ότι έχουν αναφερθεί περιστατικά εμφάνισης drones σε σημεία πολύ κοντά σε αεροδρόμια όπως στο Περθ το 2009, στο Jervis Bay τον Νοέμβριο του 2011, σύμφωνα με μαρτυρία πιλότου, στο αεροδρόμιο του Σύδνεϋ τον Φεβρουάριο 2012, πάλι με μαρτυρία πιλότου εμπορικού ελικοπτέρου, και κοντά σε βάση ελικόπτερων διάσωσης στο Newcastle [6].

Τον Οκτώβριος 2013, αναφέρθηκαν δύο περιστατικά, όπου έγιναν συστάσεις στους χειριστές των drones χωρίς όμως οποιεσδήποτε άλλες κυρώσεις. Σε μια περίπτωση, ένα micro-drone συνετρίβη πάνω στη Λιμενική Γέφυρα του Σύδνεϋ [7], και στην άλλη ένα drone πετούσε κοντά σε πυροσβέστες και σε ελικόπτερο που πραγματοποιούσε ρίψεις νερού [8]. Αρκετά περιστατικά αναφέρθηκαν και στις Ηνωμένες Πολιτείες. Σε μια αναφορά του ο αρχηγός της USAF το 2005 αποκάλυψε ότι "έχουμε είχε ήδη δύο συγκρούσεις μεταξύ UAV και άλλων αεροσκαφών [στο Ιράκ], πρέπει να κάνουμε κάτι για αυτό" [9].

Στο Ηνωμένο Βασίλειο η χρήση drone σε επιχειρήσεις της αστυνομίας είχε ως αποτέλεσμα να χαθεί ένα drone στον ποταμό Mersey του Λίβερπουλ [10]. Στην Αυστραλία, η χρήση drone για κινηματογράφηση από τα ΜΜΕ οδήγησε στη συντριβή του drone, στον Ινδικό Ωκεανό [11]. Μια παρόμοια ιστορία από την επίδειξη του πρώτου drone που χρησιμοποιείτο από την αστυνομία, στο Τέξας των ΗΠΑ είχε ως συνέπεια το μεγάλο και ακριβό drone της υπηρεσίας να συντριβεί σε αστυνομικό όχημα το οποίο ευτυχώς ήταν θωρακισμένο [12]. Στο Incheon της Νότιας Κορέας, ένα μεγάλο εμπορικό drone συνετρίβη στο όχημα ελέγχου, σκοτώνοντας έναν μηχανικό και τραυματίζοντας τους δύο πιλότους-χειριστές [4].

Τον Μάιο του 2013, κυκλοφόρησε βίντεο από ατύχημα που συνέβη τον Αύγουστο του 2004, όταν ένα μικρό drone, ένα γερμανικό Luna με βάρος περίπου 40 κιλά, συνετρίβη αφού πιάστηκε σε air turbulence ενός εμπορικού επιβατικού αεροσκάφους κατά την προσέγγιση του στο αεροδρόμιο της Καμπούλ.

2.3.2 Απειλές

Ο όρος «απειλή» αναφέρεται σε σκόπιμα, τυχαία ή περιβαλλοντικά γεγονότα που, επιδρώντας σε κάποια ευπάθεια, τείνουν να βλάπτουν ένα περιουσιακό στοιχείο. Όπως συμβαίνει και με άλλα αεροσκάφη, οι πτήσεις με drone μπορούν να προκαλέσουν πιθανή βλάβη στη δημόσιας ασφάλεια μέσω άμεσων επιπτώσεων από το drone ή το φορτίο του, σε κάποιο άλλο αντικείμενο ή πρόσωπο. Επιπλέον σε περίπτωση άμεσης επίδρασης, ο αντίκτυπος μπορεί να οδηγήσει σε εκρήξεις ή πυρκαγιές, με αποτέλεσμα περαιτέρω ζημιές [9].

Πολλά drones έχουν πολύ γρήγορα κινούμενα μέρη, όπως έλικες, οι οποίες είναι ικανές να προκαλέσουν πολύ πιο ουσιαστικά φυσικά τραύματα από ότι η ίδια η άτρακτος του drone από τη σύγκρουση. Δεν είναι όμως μόνο οι φυσικές επιπτώσεις που απειλούν τα περιουσιακά στοιχεία. Ένα ανεξέλεγκτο drone μπορεί να προκαλέσει αιφνιδιασμό ή σύγχυση σε άτομα στην εγγύς περιοχή του, με αποτέλεσμα να προκληθούν ατυχήματα, π.χ. όπου ο οδηγός ενός οχήματος ή ο πιλότος ενός άλλου drone, χάνει τον έλεγχο του δικού του οχήματος ή εκτελεί επικίνδυνο ελιγμό αποφυγής.

Επιπλέον, τα drones εξαρτώνται από τη συνεχή ροή δεδομένων και εντολών, καθιστώντας τα ευάλωτα σε παρεμβολές από πηγές ηλεκτρομαγνητικών σημάτων

άλλων συσκευών. Και το ίδιο το drone με τη σειρά του μπορεί να βλάψει τις λειτουργίες άλλων συσκευών.

Ορισμένες μορφές βλάβης μπορεί να προκληθούν σκόπιμα αφού η πρόκληση ζημιάς μπορεί να είναι ο σκοπός της χρήσης ενός drone. Μπορεί σκόπιμα να ρίξει το φορτίο που κουβαλά για να προκαλέσει ζημιά ή μπορεί να χρησιμοποιηθεί σε μια αποστολή «καμικάζι». Ο Εξοπλισμός που μπορεί να φέρει ένα drone, όπως ένας πομπός, μπορεί να χρησιμοποιηθεί για παρεμβολές ή άλλες ζημιογόνες δραστηριότητες.

Τα κίνητρα για τέτοιες σκόπιμες ενέργειες μπορεί να είναι ο ενθουσιασμός, η εκδίκηση, η ενίσχυση άλλων εγκληματικών πράξεων, και η τρομοκρατία [9].

Δεν χρειάζεται να είναι ο ιδιοκτήτης ή ο χειριστής του drone που προκαλεί σκόπιμα τη ζημιά. Ένα drone μπορεί να γίνει hijacked, με αποτέλεσμα η συμπεριφορά του να ελέγχεται από κάποιον άλλο και όχι από τον αρχικό χειριστή. Μπορεί επίσης ο χειριστής να ελέγχει τη συμπεριφορά του drone όμως αυτό να έχει ήδη παρεμβληθεί από σήμα ξένης πηγής η οποία με τη χρήση λάθος δεδομένων προς τη ροή ελέγχου του drone να επηρεάζει σημαντικά τη λειτουργία του κάνοντας το επικίνδυνο τόσο για τον ίδιο το χειριστή όσο και για άλλους. Η συμπεριφορά ενός drone μπορεί να επηρεαστεί επίσης όχι μόνο από ηλεκτρονικά μέσα αλλά και άμεσα, με φυσική επίθεση συμπεριλαμβανομένης της επίθεσης από άλλο drone. Οι πρόσφατες μειώσεις σε κόστος των drones είναι τόσο σημαντικές με αποτέλεσμα το κόστος που απαιτείται για την πραγματοποίηση τέτοιων επιθέσεων να είναι πολύ χαμηλό και τα drones τα ίδια να είναι πλέον αναλώσιμα.

Οι επιθέσεις είναι σχεδόν απίθανο να είναι κοινές. Το πιο πιθανόν είναι το περιστατικό να είναι συνέπεια ατυχήματος και όχι σκόπιμο αν ληφθεί υπόψη η κατασκευή του drone. Όλα τα drones, και κυρίως τα φθηνά, τείνουν να παρουσιάζουν συχνά αστοχία υλικών συχνά κατά τη διάρκεια της πτήσης. Το χειριστικό σφάλμα, οι ηλεκτρομαγνητικές παρεμβολές ή η τεχνική δυσλειτουργία κατά τη διάρκεια μιας προσπάθειας πραγματοποίησης προσγείωσης μπορεί να προκαλέσει συντριβή, με αποτέλεσμα να προκληθούν ζημιές σε ανθρώπους ή σε ιδιοκτησίες.

Στην περίπτωση των ουσιαστικά αυτόνομων drones, λάθη μπορεί να προκύψουν από διάφορες απρόβλεπτες συνθήκες ή σφαλμάτων λόγω προγραμματισμού. Ορισμένες

δυσλειτουργίες μπορεί να οφείλονται σε περιβαλλοντικά περιστατικά, όπως σοβαρές αναταράξεις και αστραπές, σε «Πράξεις του Θεού» (Acts of God), όπως αναφέρεται και στην ορολογία των ασφαλιστών, πράξεις που είναι προβλέψιμες, αλλά όχι προλήψιμες.

Οι περισσότερες από αυτές τις περιστάσεις μπορεί να προκύψουν και σε επανδρωμένα αεροσκάφη. Για παράδειγμα, αν και η παρεμβολή αποτελεί ιδιαίτερη πρόκληση για τα drones, οποιοδήποτε αεροσκάφος μπορεί να απειληθεί από τέτοιο κίνδυνο. Οι σημαντικότερες διαφορές μεταξύ των επανδρωμένων αεροσκαφών και των drones δεν είναι στο γεγονός ότι μπορεί να προκύψει μια βλάβη, αλλά στον τύπο βλάβης που μπορεί να εμφανιστεί, ή στο εύρος των ανθρώπων που μπορεί να είναι υπεύθυνοι για τέτοια βλάβη. Οι βασικοί παράγοντες είναι το χαμηλό κόστος της τεχνολογίας που χρησιμοποιείται στο drone σε συνδυασμό με την έκταση χρήσης τεχνολογίας που σχετίζεται με την ασφάλεια και με τον επακόλουθο υψηλό όγκο της δραστηριότητας του επανδρωμένου αεροσκάφους όπως και με τα αναπόφευκτα υψηλότερα πρότυπα πιλότου και τις επιδόσεις. Τέλος, καθοριστικό ρόλο έχει και το υψηλό κόστος που συνεπάγεται η έρευνα και ο εντοπισμός της ευθύνης σε τέτοια ατυχήματα.

Καθώς ο εναέριος χώρος γίνεται όλο και πιο συμφορημένος, ο κίνδυνος συγκρούσεων αυξάνεται. Ο διογκούμενος εναέριος χώρος οδηγεί επίσης σε ηλεκτρονική συμφόρηση, με αποτέλεσμα την ύπαρξη υψηλών επιπέδων παρεμβολών σήματος και συνεπώς τη συνεχή ροή αναξιόπιστων και διαλειπόντων δεδομένων από και προς τα αεροσκάφη. Στον ελεγχόμενο εναέριο χώρο, τα drones δημιουργούν πλέον νέες προκλήσεις όσον αφορά τις αλληλεπιδράσεις μεταξύ πιλότων και της εναέριας κυκλοφορίας γενικά.

Σύμφωνα με τις ισχύουσες ρυθμίσεις, αυτές οι επικοινωνίες βασίζονται σε line of sight μεταδόσεις ("οπτικής επαφής"). Οι επικοινωνίες στα drones από την άλλη, είναι πιθανό να είναι λιγότερο άμεσες και να εξαρτώνται από πρόσθετες υποδομές, που μπορούν να είναι πιθανά σημεία αποτυχίας, αυξάνουν την καθυστέρηση, και μπορεί να διαψεύσουν την προσδοκία ότι οι πιλότοι μπορούν να απαντούν στις οδηγίες των ελεγκτών μέσα σε λίγα δευτερόλεπτα.

Με το χαμηλό κόστος των περισσότερων drones δημιουργούνται και χαμηλά πρότυπα διασφάλισης ποιότητας υλικού και λογισμικού. Στα μεγάλα drones που χρησιμεύουν για βιομηχανικούς και εμπορικούς σκοπούς γίνονται σημαντικές επενδύσεις που συμβάλλουν σε κάποιο βαθμό στη βελτίωση της ποιότητας.

Όσον αφορά τα στρατιωτικά drones, τα πρότυπα είναι υψηλά για συγκεκριμένους σκοπούς, και αυτό επειδή η δαπάνη αυτή δεν υπόκειται σε περιορισμούς. Επίσης τα λογισμικά για τα μικρά drones γενικά, ιδιαίτερα για τις μικρές επιχειρήσεις, τους καταναλωτές και τους χομπίστες είναι πιο πιθανό να έχουν χαμηλά πρότυπα με τη χρήση της ταχείας ανάπτυξης εφαρμογών ανοικτού κώδικα, των δοκιμαστικών εκδόσεων beta και του crowdsource που επικρατεί σε βιβλιογραφίες, λογισμικό και υπηρεσίες καταναλωτών. Η διασφάλιση της ποιότητας του λογισμικού, η αναγνωσιμότητα, η συντηρησιμότητα, ο έλεγχος και η πιστοποίηση αποτελούν έννοιες ξένες σε αυτούς τους τομείς. Το αποτέλεσμα είναι να εγκυμονούνται συνεχώς σημαντικές πιθανότητες πρόκλησης βλάβης από δυσλειτουργία [9].

2.4 Πρόβλημα-Πρόταση

Σε συνέπεια των πιο πάνω κινδύνων που αναλύσαμε, πολλές επιχειρήσεις και οργανισμοί οι οποίοι ανησυχούν ότι ενδέχεται να υποστούν τέτοιες ανεπιθύμητες επιθέσεις, κάνουν σκέψεις εύρεσης και εφαρμογής πιθανών αμυντικών μέτρων-αντιμέτρων. Επιπλέον, άτομα και οργανώσεις που μπορεί να αποτελέσουν στόχο τέτοιων επιθέσεων και δραστηριοτήτων, εξετάζουν αμυντικά μέτρα για την ενεργητική πρόληψη των απειλών ή των αντιποίνων κατά του δράστη. Τέτοια αντίμετρα περιλαμβάνουν:

- παρεμβολή των σημάτων ελέγχου ή / και μετάδοσης δεδομένων
- παρεμβολή σε δεδομένα γεωγραφικής θέσης, όπως τα δεδομένα GPS
- hacking του λογισμικού
- αρπακτικά drones
- παρομοίως αμυντικά drones
- παρεμβολή στην υποδομή που χρησιμοποιούν οι απομακρυσμένοι χειριστές
- παρεμβολή σε απομακρυσμένους χειριστές [2]

Οποιαδήποτε ενέργεια υπονομεύει τη λειτουργία ενός drone αυξάνει τον κίνδυνο δυσλειτουργίας και, συνεπώς, τη βλάβη όχι μόνο στο drone, αλλά και σε οτιδήποτε επηρεάζεται από αυτό ως αποτέλεσμα της δυσλειτουργίας. Οποιοδήποτε στοιχείο που χρησιμοποιείται για αντιμετώπιση και καταστροφή αυτών των drones (μια σφαίρα,

εκτόξευση νερού, άλλο drone) εμπεριέχει κινδύνους αλλά με το πρόσθετο χαρακτηριστικό ότι το ίδιο το στοιχείο αυτό γίνεται μια πρόσθετη απειλή για άλλα αντικείμενα και άτομα στην περιοχή. Μέχρι σήμερα, φαίνεται ότι υπήρξαν λίγα αμυντικά μέτρα για αυτό το σκοπό. Ωστόσο, μια ακτιβιστική ομάδα για τα δικαιώματα των ζώων στη Νότια Καρολίνα ανέφερε ότι ένα drone που χρησιμοποιούσαν για να βιντεοσκοπήσουν ένα πυροβολισμό περιστεριού καταρρίφθηκε το ίδιο από κυνηγούς, σε κοντινή απόσταση σε μια εθνική οδό. Παρόμοια συμβάντα αναφέρθηκαν και στο Deer Trail, του Κολοράντο με πυροβολισμούς σε drones. Οι υπερβολικές όμως ενέργειες σαν αυτές μπορούν να αποτελούν επικίνδυνες και παράνομες πράξεις [2].

Σοβαρά περιστατικά που αφορούν drones, είναι αρκετές φορές άξια ενδιαφέροντος. Λιγότερο όμως σοβαρά γεγονότα είναι πιθανό να διαστρεβλωθούν από ορισμένα τμήματα των μέσων ενημέρωσης και να παραπληροφορήσουν. Για παράδειγμα, μια ασήμαντη αναφορά για ένα μικρό drone που συνετρίβη στη Λιμενική Γέφυρα του Σύδνεϋ [7] δραματοποιήθηκε στο Λονδίνο και το Μιλάνο σχετίζοντας το με την παρουσία στο διεθνές λιμάνι των πολεμικών πλοίων του Η.Β. και του πρίγκιπα Χάρι του Ηνωμένου Βασιλείου. Αναφορές των ΜΜΕ αυτής της φύσης μπορεί να αναμένεται ότι θα παρακινήσουν πολιτικούς, με αποτέλεσμα πρόσθετες «διασφαλίσεις» ριζικά μέτρα για να τεθούν σε εφαρμογή όμως έχουν εν τέλει ως συνέπεια τη εφαρμογή ατυχών μέτρων αντιμετώπισης τέτοιων κινδύνων που είναι και άχρηστα και αναποτελεσματικά αλλά και επικίνδυνα.

Σκοπός της διατριβής αυτής είναι να επιβεβαιώσει την ακόλουθη υπόθεση:

Δεν υπάρχει λόγος να χρησιμοποιηθούν «θανάσιμα»-καταστροφικά μέσα εξάλειψης για την υπεράσπιση ορισμένων περιμέτρων και εγκαταστάσεων, αρκεί να αποτραπεί ο χειριστής του μη επανδρωμένου αεροχήματος-drone από το να ολοκληρώσει τη διαδικασία της καθοδήγησης του drone στο στόχο, διακόπτοντας τον σήμα ελέγχου από και προς το drone κατά την τελική φάση καθοδήγησης.

Για το σκοπό αυτό προτείνεται η σχεδίαση και ανάπτυξη μια απλής αλλά αποτελεσματικής συσκευής jammer από φθηνά, κοινά ηλεκτρονικά στοιχεία που βρίσκονται διαθέσιμα στην αγορά και που θα επιδρά και θα αποκόπτει τις επικοινωνίες Wi-Fi και GPS του drone.

Κεφάλαιο 3
Ασύρματες Επικοινωνίες

3.1 Ιστορικές αναφορές Παρεμβολών

Από τότε που η χρήση της τεχνολογίας ασύρματων επικοινωνιών μπήκε στο στρατιωτικό περιβάλλον, η παρεμβολή αυτών των επικοινωνιών και η χρήση των πληροφοριών που προκύπτουν παρέχουν πολύτιμα πλεονεκτήματα. Οι συσκευές για jamming στις επικοινωνίες αναπτύχθηκαν και πρώτο-χρησιμοποιήθηκαν από το στρατό. Αυτό το ενδιαφέρον προέρχεται από τον εξαιρετικά σημαντικό στόχο κάθε στρατού, να παρεμποδίσει την επιτυχή μετάδοση πληροφορίας από τον αποστολέα (τακτικοί διοικητές) στον δέκτη (στρατιωτικό προσωπικό) και αντίστροφα [13].

Η εμφάνιση της ηλεκτρονικής παρεμβολής των ασύρματων επικοινωνιών χρονολογείται ήδη από τους Πολέμους των Boers (1900), όπου το Βασιλικό Ναυτικό χρησιμοποίησε τα πρώτα ασύρματα συστήματα Marconi στα τέλη της δεκαετίας του 1890 μαζί με τη χρήση ορισμένων περιορισμένων ασύρματων επικοινωνιών από το

Βρετανικό Στρατό. Οι Boers χρησιμοποίησαν βρετανικά ραδιοφωνικά συστήματα για να μεταδώσουν ζωτικές πληροφορίες, οι οποίες παρεμβάλλονταν από τις βρετανικές δυνάμεις [14].

Τα πρώτα τεκμηριωμένα παραδείγματα σημαντικής χρήσης της Ασύρματης παρεμβολής ήταν πριν και κατά τη διάρκεια του Πρώτου Παγκοσμίου Πολέμου. Ο Οργανισμός Εθνικής Ασφάλειας (NSA) (Οργανισμός Ηνωμένων Πολιτειών υπεύθυνος για την Υπηρεσία Σήμανσης Σημάτων και Ασφάλειας Πληροφοριών (IA)) έχει δημοσιεύσει άρθρα σχετικά με το ιστορικό ασύρματης παρακολούθησης. Ένα έγγραφο, στο βιβλίο του Flicke, W., ("Undated. The Beginnings of Radio Intercept in World War 1 - A Brief history by a German Intelligence Officer. "1954) διερευνά την πρώιμη χρήση της παρακολούθησης από την πλευρά ενός γερμανικού αξιωματικού πληροφοριών. Αυτό το έγγραφο περιγράφει με σαφήνεια το στρατιωτικό και πολιτικό πλεονέκτημα που επιδιώκεται και κερδίζεται μέσω της υποκλοπής ευαίσθητων επικοινωνιών.

Από τότε, τα περισσότερα έθνη έχουν πραγματοποιήσει τέτοιες δραστηριότητες. Κατά τη διάρκεια του 2ου Παγκοσμίου Πολέμου, ο σταθμός παρεμπόδισης μακρών κυμάτων Meacon, από τον οποίο πήρες το όνομα του αυτή η τεχνική, χρησιμοποιήθηκε για να παρεμβάλει τα Γερμανικά Βομβαρδιστικά που πλησίαζαν την ακτογραμμή του Ηνωμένου Βασιλείου [14].

Στην κατεχόμενη Ευρώπη οι Ναζί προσπάθησαν να μπλοκάρουν εκπομπές στην ήπειρο από το BBC και άλλους συμμαχικούς σταθμούς. Μαζί με την συνεχή αύξηση της ισχύος των πομπών και την συνεχή προσθήκη επιπλέον συχνοτήτων, έγιναν προσπάθειες για την εξουδετέρωση του jamming με την ρίψη φυλλαδίων πάνω από τις πόλεις, οι οποίες έδιναν οδηγίες στους ακροατές για το πώς να κατασκευάσουν μια κατευθυντική κεραία που θα τους επιτρέπει να ακούνε τους σταθμούς.

Ο Winston Churchill είχε αναφέρει κάποτε ότι είχε πει στον βασιλιά ΓεώργιοVI. " Χάρη στο μυστικό όπλο του στρατηγού Menzies, που χρησιμοποιήθηκε σε όλα τα μέτωπα, κερδίσαμε τον πόλεμο! ". Επιπλέον, ο Sir Harry Hinsley υποστήριξε ότι το Ultra μείωσε τη διάρκεια του πολέμου "όχι λιγότερο από δύο χρόνια και πιθανόν μέχρι και τέσσερα χρόνια" και ότι, "ελλείψει του Ultra, είναι αβέβαιο πώς θα τελείωνε ο πόλεμος" [14].

Κατά τη διάρκεια μεγάλου μέρους του Ψυχρού Πολέμου, το σοβιετικό μπλοκάρισμα των δυτικών ραδιοτηλεοπτικών φορέων οδήγησε σε μια κούρσα επικράτησης στην οποία οι ραδιοτηλεοπτικοί σταθμοί και οι jammers αύξαναν συνεχώς την ισχύ του σήματος μετάδοσης, χρησιμοποιούσαν πολύ κατευθυντικές κεραίες και πρόσθεταν επιπλέον συχνότητες στης ήδη υπερπλήρεις μπάντες συχνοτήτων σε τέτοιο βαθμό ώστε πολλοί ραδιοτηλεοπτικοί σταθμοί που δεν αποτελούσαν στόχο των jammers να υποφέρουν από τα αυξανόμενα επίπεδα θορύβου και παρεμβολών [15, 16].

Στη δικτατορική Ισπανία του Φράνκο, το καθεστώς έκανε για δεκαετίες jamming στο Radio España Independiente, τον ραδιοφωνικό σταθμό του Κομμουνιστικού Κόμματος της Ισπανίας που μετέδιδε από τη Μόσχα (1941-1955) και το Βουκουρέστι (1955-1977). Ήταν ο σημαντικότερος πειρατικός ραδιοφωνικός σταθμός στην Ισπανία και το καθεστώς το θεωρούσε απειλή, δεδομένου ότι επέτρεπε στους πολίτες του να παρακάμπτουν τη λογοκρισία των τοπικών μέσων ενημέρωσης. Τα χρήματα και η τεχνολογική βοήθεια για το jamming προέρχονταν από τις Ηνωμένες Πολιτείες. (Wikipedia)

Επίσης, στη Λατινική Αμερική υπήρξαν περιπτώσεις κομμουνιστικών ραδιοφωνικών σταθμών όπως ο as Radio Venceremos, που φέρεται να παρεμβαλλόταν από τη CIA, ενώ υπήρχαν και σύντομες περίοδοι με περιπτώσεις όπου η Βρετανία μπλόκαρε κάποιους αιγυπτιακούς σταθμούς (κατά τη διάρκεια της κρίσης του Σουέζ) και Ελληνικούς (πριν την ανεξαρτησία της Κύπρου) [18].

Πιο πρόσφατο παράδειγμα είναι των ρωσικών ενόπλων δυνάμεων που από το καλοκαίρι του 2015, άρχισαν να χρησιμοποιούν ένα πολυλειτουργικό σύστημα EW στην Ουκρανία, γνωστό ως Borisoglebsk 2. Θεωρείται ότι το σύστημα αυτό έχει μπλοκάρει τις επικοινωνίες σε διάφορα μέρη της χώρας, συμπεριλαμβανομένων και των συστημάτων κινητής τηλεφωνίας και GPS. (Wikipedia)

Επιθέσεις Meaconing διεξάγονται μέχρι σήμερα ενάντια σε Στρατιωτικούς στόχους, με το πιο πρόσφατο και ευρέως διαδεδομένο παράδειγμα τη πτώση ενός αμερικανικού RQ-170 από τους Ιρανούς Επαναστατικούς Φρουρούς. Πιστεύεται ότι αυτό επιτεύχθηκε μέσω jamming των καναλιών ελέγχου του UAV αναγκάζοντας το UAV να πραγματοποιήσει μια προσγείωση μέσα σε ένα εκτιμώμενο «ασφαλές» περιβάλλον [19].

Ο Scott Peterson έχει αναφερθεί σε πραγματικά παραδείγματα όπου το video downlink του Predator drone είχε υποκλαπεί από αντάρτες και χρησιμοποιήθηκε για εξακρίβωση των αποστολών του. Αυτό βασίστηκε στην παρακολούθηση και αποκωδικοποίηση του σήματος που χρησιμοποιούσαν οι στρατιώτες, που βρίσκονταν προωθημένοι, για να παρακολουθήσουν τη δραστηριότητα των ανταρτών.

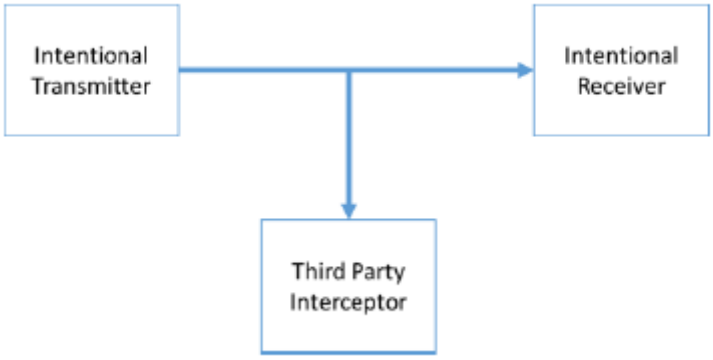
3.2 Ευπάθειες Ασύρματων Επικοινωνιών

Η φύση της ηλεκτρομαγνητικής διάδοσης διασφαλίζει ότι όταν χρησιμοποιείται ένα ασύρματο σήμα, όπως ένα δίκτυο Wi-Fi, το Personal Mobile Radio (PMR) ή το τηλεχειριστήριο-κλειδί του αυτοκινήτου, δεν κατευθύνεται αποκλειστικά στον αποδέκτη, αλλά μεταδίδεται ανοιχτά σε όλες τις κατευθύνσεις και περιορίζεται μόνο από τους κανόνες της φυσικής και την αλληλεπίδραση του σήματος και του περιβάλλοντός του.

Δεδομένων αυτών των αρχών, εξοπλισμός όπως οι ενισχυτές χαμηλού θορύβου (Low Noise Amplifiers), οι κατευθυντήριες κεραίες (Directional Antennas,) και οι τεχνικές επεξεργασίας σημάτων μπορούν να επιτρέψουν σε έναν τρίτο να ανακτήσει τα σήματα πολύ πέρα από την προβλεπόμενη εμβέλεια. Αυτό εξασφαλίζει ότι καμία ασύρματη μετάδοση δεν μπορεί ποτέ να θεωρείται ιδιωτική και εμπιστευτική.

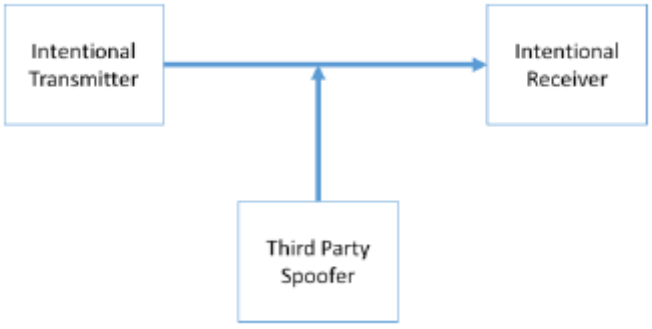
Οι τρεις μηχανισμοί επίθεσης σε ασύρματα συστήματα είναι:

1. **Η παρεμβολή** αποσκοπεί στην εξαγωγή των πληροφοριών που μεταδίδονται από ένα σύστημα, είτε πρόκειται για ψηφιακά δεδομένα είτε για ένα αναλογικό κωδικοποιημένο φωνητικό μήνυμα. Η παρεμβολή κανονικά απαιτεί από το τρίτο μέρος να εξάγει τις πληροφορίες χωρίς να επηρεάζει την ακεραιότητα του εν λόγω σήματος, ωστόσο σε ένα ασύρματο σύστημα αυτό δεν απαιτείται, καθώς παθητικές τεχνικές μπορούν να χρησιμοποιηθούν για την αποδιαμόρφωση και την αποκωδικοποίηση του ενδιαφέροντος σήματος χωρίς ο στόχος να το γνωρίζει. Γι' αυτό το λόγο, είναι δύσκολο να ανιχνευθεί μια τέτοιου είδους επίθεση που βρίσκεται σε εξέλιξη σε ένα ασύρματο δίκτυο [14].



Σχήμα 3.1: Wireless Intercept

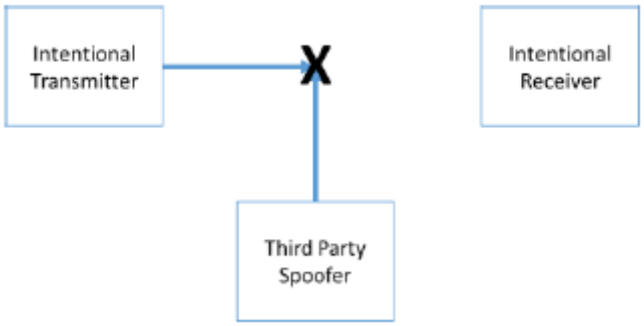
2. **Το Spoofing** συνήθως περιλαμβάνει την εισαγωγή πακέτων σε ασύρματα συστήματα προκαλώντας είτε μικρές επιπτώσεις, όπως για παράδειγμα αύξηση του ρυθμού σφάλματος bit (BER) ή ακόμη και μαζικά σφάλματα στα δεδομένα. Ένα από τα πιο εμφανή παραδείγματα spoofing είναι η αλλοίωση των δεδομένων θέσης του συστήματος Global Positioning System (GPS). Πρόσφατες πηγές [19] έδειξαν ότι η κατάρριψη ενός μη επανδρωμένου αεροσκάφους του αμερικανικού Υπουργείου Άμυνας (DoD) σχετίζεται με GPS spoofing αλλά αυτό δεν επιβεβαιώθηκε ποτέ επισήμως από τις αμερικανικές αεροπορικές δυνάμεις [14].



Σχήμα 3.2: Spoofing

3. **Το jamming** είναι η διαδικασία της εισαγωγής θορύβου σε ένα κανάλι RF προκειμένου να μπλοκαριστεί διαθεσιμότητα του. Υπάρχουν διάφορες τεχνικές jamming που ποικίλλουν από το Barrage, το οποίο μπλοκάρει αδιακρίτως απλά ή πολλαπλά RF κανάλια, η Reactive, που παραμένει «σιωπηλή» μέχρι να ανιχνευθεί η κυματομορφή του στόχου, ή τεχνική jamming πρωτόκολλου, όπου το protocol

layer του ασύρματου σήματος παρεμβάλλεται για να διακοπεί η λειτουργία του. Οι τεχνικές επιθέσεων jamming από τη φύση τους είναι θορυβώδεις και εύκολο να ανιχνευθούν, ωστόσο όταν εκτελούνται με επαρκή ισχύ είναι δύσκολο να αντιμετωπιστούν, εκτός εάν οι στόχοι έχουν επαρκές εύρος ζώνης RF που τους δίνει τη δυνατότητα να απλώνουν το σήμα πέρα από τις δυνατότητες του jammer. Το jamming αν και εύκολα ανιχνεύσιμο είναι ο ευκολότερος τρόπος επίθεσης ενάντια σε ασύρματα δίκτυα που δεν απαιτούν βασική γνώση της κυματομορφής στόχου [14].



Σχήμα 3.3: Jamming

3.3 Jamming

Εξαιτίας του πολλαπλασιασμού των ασύρματων τεχνολογιών, το jamming στα ασύρματα δίκτυα έχει γίνει ένα σημαντικό ερευνητικό πρόβλημα λόγω της ευκολίας στην παρεμπόδιση της επικοινωνίας σε ασύρματα δίκτυα. Οι επιθέσεις jamming αποτελούν ένα υποσύνολο επιθέσεων Denial of Service (DoS) στις οποίες κακόβουλοι κόμβοι εμποδίζουν τη νόμιμη επικοινωνία προκαλώντας σκόπιμη παρεμβολή στο δίκτυο [20].

Υπάρχουν δύο κύριες πτυχές των τεχνικών jamming σε ασύρματα ad hoc δίκτυα: οι τύποι των jammer και η τοποθέτηση των jammers για μέγιστο αποτέλεσμα [20]. Ωστόσο, λόγω της εκτεθειμένης φύσης των ασύρματων συνδέσεων, τα τρέχοντα ασύρματα δίκτυα μπορούν εύκολα να δεχθούν επιθέσεις jamming.

Όσον αφορά τη βέλτιστη τοποθέτηση του jammer, Οι C. Gencer, E. K. Aydogan, C. Celik, [21] καθόρισαν ότι ένα σύστημα jamming θα πρέπει να τοποθετηθεί στη βέλτιστη θέση

έτσι ώστε να μπορεί να καταστρέψει πλήρως την επικοινωνιακή ικανότητα του στοχευόμενου συστήματος. Αυτά τα είδη συστημάτων είναι που χρησιμοποιούνται συνήθως σε στρατιωτικές εφαρμογές. Για την τοποθέτηση υποθέτουν ότι υπάρχει οπτική επαφή μεταξύ του jammer και του στόχου, ο στόχος βρίσκεται εντός της εμβέλειας της κεραίας και του η ισχύς σήματος του συστήματος jamming είναι υψηλότερη από την ισχύ του στόχου.

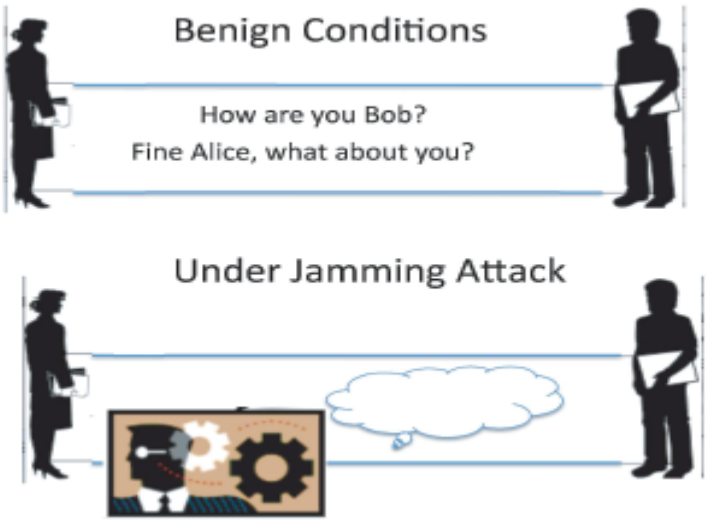
Το jamming είναι διαφορετικό από τις συνήθεις παρεμβολές δικτύου (network interferences), επειδή περιγράφει τη σκόπιμη χρήση ασύρματων σημάτων σε μια προσπάθεια να διαταραχθούν οι επικοινωνίες, ενώ οι παρεμβολές (interferences) αναφέρονται σε ακούσιες μορφές διαταραχών.

Η ακούσια παρεμβολή μπορεί να προκληθεί από επικοινωνίες μέσα στα ίδια δίκτυα ή άλλες συσκευές (π.χ. μικροκυμάτων και τηλεχειριστήρια).

Από την άλλη πλευρά, η σκόπιμη παρέμβαση (jamming) συνήθως διεξάγεται από έναν εισβολέα ο οποίος σκοπεύει να διακόψει ή να αποτρέψει την επικοινωνία στα δίκτυα.

Το **jamming** στα ασύρματα δίκτυα ορίζεται ως η διακοπή των υφιστάμενων ασύρματων επικοινωνιών από την μείωση του λόγου σήματος προς θόρυβο στην πλευρά του δέκτη μέσω της μετάδοσης σημάτων θορύβου [20]. Τεχνικά η εισαγωγή σήματος θορύβου στο ασύρματο κανάλι ενός εκούσιου δέκτη ή πομπού. Αυτό γενικά πραγματοποιείται προκειμένου να διαταραχθεί ή να διακοπεί η επικοινωνία μέσω της μείωσης του αισθητού λόγου σήματος προς θόρυβο (SNR) στον δέκτη [14]. Το jamming είναι μια ευρέως χρησιμοποιούμενη στρατιωτική τεχνική για να παρεμποδίζεται στους εχθρούς η πρόσβαση στο ηλεκτρομαγνητικό φάσμα προσπαθώντας παράλληλα να διατηρηθούν οι φίλιες ασύρματες επικοινωνίες.

Συγκεκριμένα, ένας κακόβουλος κόμβος (jammer) μπορεί να μεταδίδει συνεχώς ένα ραδιοσήμα προκειμένου να εμποδίσει οποιαδήποτε νόμιμη πρόσβαση στο μέσο ή / και να προκαλέσει παρεμβολή στη λήψη του σήματος [22]. Οι τεχνικές jamming ποικίλλουν από απλές, βασισμένες στη συνεχή μετάδοση σημάτων παρεμβολής, σε πιο εξελιγμένες που στοχεύουν στην εκμετάλλευση των τρωτών σημείων του εκάστοτε πρωτόκολλου που χρησιμοποιείται.



Σχήμα 3.4: Σχηματική απεικόνιση μιας οντότητας Jamming.

Μπορούμε να χωρίσουμε τους jammer ανάλογα με τον τρόπο που λειτουργούν σε 4 τύπους:

1. constant jammer
2. deceptive jammer
3. random jammer
4. reactive jammer

Ένας **constant jammer** [22] εκπέμπει συνεχώς ραδιοσήματα χρησιμοποιώντας σαν μέσο τον ελεύθερο χώρο. Τα σήματα αυτά μπορούν να αποτελούνται από μια εντελώς τυχαία ακολουθία δυαδικών ψηφίων. Οι εκπομπές ηλεκτρομαγνητικής ενέργειας δεν χρειάζεται να ακολουθούν τους κανόνες οποιουδήποτε πρωτοκόλλου MAC. Ο ρόλος αυτού του τύπου jammer είναι διττός: (α) να δημιουργεί παρεμβολές σε οποιονδήποτε κόμβο μετάδοσης για να αλλοιώνει τα πακέτα που φτάνουν στο δέκτη και (β) να κάνει ένα νόμιμο πομπό να αντιληφθεί το κανάλι ως απασχολημένο και ως εκ τούτου να το εμποδίσει από το ν αποκτήσει πρόσβασης στο κανάλι.

Παρόμοια λειτουργία με το **constant jammer** είναι ο **deceptive jammer** [22]. Η ομοιότητά τους οφείλεται στο γεγονός ότι και οι δύο συνεχώς μεταδίδουν τα bits. Η κύρια διαφορά είναι ότι με το deceptive jammer, τα μεταδιδόμενα bits δεν είναι τυχαία.

Ο deceptive jammer εισάγει συνεχώς πακέτα στο κανάλι χωρίς κενά μεταξύ των εκπομπών. Αυτό κάνει έναν ακούσιο χρήστη να πιστεύει ότι υπάρχει μια συνεχής νόμιμη μετάδοση πακέτων. Κατά συνέπεια, κάθε κόμβος θα παραμείνει στην κατάσταση ακρόασης ακόμα κι αν έχει δεδομένα για μετάδοση. Μια σημαντική διαφορά από τον constant jammer είναι ότι ο deceptive jammer είναι πιο δύσκολο να εντοπιστεί χρησιμοποιώντας network monitoring tools, καθώς αυτά τα εργαλεία θα αντιληφθούν ότι υπάρχει νόμιμη κίνηση στο μέσο. Ένα μειονέκτημα που έχουν οι προαναφερθέντες jammers είναι η αποδοτικότητά ισχύος τους. Η συνεχής εκπομπή σημάτων στο ασύρματο μέσο περιορίζει την ικανότητά τους να είναι αυτόνομα και να μην εξαρτώνται από μια εξωτερική πηγή ενέργειας.

Ένας πιο αποτελεσματικός jammer, είναι ο **random jammer** [22]. Ένας εισβολέας που χρησιμοποιεί random jamming, εκπέμπει για μερικά δευτερόλεπτα και στη συνέχεια "κοιμάται" για μερικά πάλι δευτερόλεπτα. Ο random jammer μπορεί να χρησιμοποιήσει οποιαδήποτε από τις προηγούμενες τεχνικές jamming και να τις συνδυάσει μεταβάλλοντας το χρόνο εκπομπής και το διάστημα αδράνειας μεταβάλλοντας έτσι και τη κατανάλωση ισχύος.

Μια πιο έξυπνη και πιο αποδοτική μέθοδος είναι η στόχευση μόνο στη λήψη ενός πακέτου. Αυτή η μέθοδος jamming ονομάζεται **reactive jamming** [22]. Αυτός ο jammer ακούει συνεχώς το κανάλι και κατά την ανίχνευση μιας μετάδοσης πακέτων, μεταδίδει αμέσως ένα σήμα προκειμένου να προκαλέσει collision στον δέκτη.

Jamming Model	Implementation Complexity	Energy Efficiency	Stealthiness	Level of DoS	Anti–Jamming Resistance
Constant [10]	Low	Low	Low	High	Medium
Deceptive [10]	Low	Low	Low	High	Medium
Random [10]	Low	Adjustable	Medium	Adjustable	Medium
Reactive [10]	High	High	Medium	High	Low
Packet Corruption [11], [21]	Average	High	Average	High	Low
Narrow-band [20]	High	High	High	High	Average
DIFS Waiting [11], [21]	Medium	Medium	Medium	High	Low
Identity Attacks [22]	Medium	Average	Average	High	High
Layered Attacks [18]	High	Low	Average	High	Medium

Πίνακας 3.1: Χαρακτηριστικά διαφόρων μοντέλων Jamming

Σημαντικό είναι ότι τα τρέχοντα πρότυπα για τις ασύρματες επικοινωνίες δεδομένων ευνοούν τη δραστηριότητα του jammer. Για παράδειγμα, το επίπεδο PHY του IEEE 802.11 δεν υποστηρίζει τη διόρθωση σφαλμάτων. Ως αποτέλεσμα, ο jammer μπορεί να

στείλει αρκετή ενέργεια για να καταστρέψει ένα μόνο bit και να προκαλέσει την αποτυχία του πακέτου κατά τον έλεγχο CRC στο δέκτη. Ο λόγος που υπάρχει αυτή η προδιαγραφή στο πρωτόκολλο είναι επειδή τα ασύρματα συστήματα έχουν σχεδιαστεί για να είναι ανθεκτικά μόνο σε μη κακόβουλες παρεμβολές και θόρυβο. Ένας jammer όμως μπορεί να το εκμεταλλευτεί αυτό και να χρησιμοποιήσει χαμηλή ισχύ αποτελεσματικά για να διαταράξει το σύνολο της επικοινωνίας [22].

3.3.1 Τεχνικές jamming

Υπάρχουν διάφοροι τρόποι να μπλοκαριστεί μια συσκευή RF. Οι τρεις οι πιο κοινές τεχνικές μπορούν να κατηγοριοποιηθούν ως εξής:

Spoofing:

Σε αυτό το είδος jamming, η συσκευή αναγκάζει το κινητό να απενεργοποιηθεί από μόνο του. Αυτός ο τύπος είναι πολύ δύσκολο να εφαρμοστεί αφού η συσκευή jamming εντοπίζει πρώτα οποιοδήποτε κινητό τηλέφωνο στη συγκεκριμένη περιοχή και ακολούθως στέλνει το σήμα για να απενεργοποιήσει το κινητό τηλέφωνο. Μερικοί τύποι αυτής της τεχνικής μπορούν να γίνουν αντιληπτοί εάν ένα κοντινό κινητό τηλέφωνο είναι εκεί και στείλει μήνυμα για να πει στο χρήστη να περάσει το τηλέφωνο σε αθόρυβη λειτουργία (Intelligent Beacon Disablers) [13].

Shielding attacks:

Γνωστές και ως TEMPEST ή EMF attacks. Αυτό το είδος απαιτεί το κλείσιμο μιας περιοχής σε ένα κλωβό faraday έτσι ώστε οποιαδήποτε συσκευή μέσα σε αυτό τον κλωβό να μην μπορεί να μεταδώσει ή να λάβει σήμα RF από έξω [13].

Denial of service (DoS):

Στην τεχνική αυτή, η συσκευή μεταδίδει ένα σήμα θορύβου στην ίδια συχνότητα του κινητού τηλεφώνου προκειμένου να μειωθεί η αναλογία σήματος προς θόρυβο. Αυτή η τεχνική jamming είναι και η πιο απλή αφού η συσκευή είναι πάντα ενεργοποιημένη. Τα κυκλώματα τέτοιου είδους jammer περιλαμβάνουν τμήμα IF, τμήμα RF, Κεραία και τροφοδοτικό [13]. Η συσκευή που θα κατασκευάσουμε θα είναι αυτού του τύπου.

Κεφάλαιο 4
Υφιστάμενα Συστήματα Drones

4.1 Κατηγορίες

Τα drones κυμαίνονται σε μέγεθος από μεγάλα στρατιωτικά UAVs με πτέρυγες ύψους περίπου 200 ποδών μέχρι τα διαθέσιμα στο εμπόριο micro-drones. Η εμβέλεια πτήσης τους διαφέρει, με ορισμένα εμπορικά drones να περιορίζονται σε λίγα πόδια μακριά από τον χειριστή στα προηγμένα στρατιωτικά UAVs που μπορούν πετούν για πάνω από 17.000 μίλια χωρίς να χρειαστεί να προσγειωθούν. Ομοίως, υπάρχουν τεράστιες διακυμάνσεις στο μέγιστο ύψος πτήσης τους, που μπορεί να είναι οτιδήποτε από μερικά πόδια μέχρι το μέγιστο των 65.000 ποδών [1].

Τα περισσότερα εμπορικά διαθέσιμα drones ακολουθούν σήμερα παρόμοια σχεδίαση. Ο βασικός σχεδιασμός έχει ένα μικροελεγκτή που ενεργεί ως flight controller, συνήθως με τέσσερις έως οκτώ κινητήρες και προπέλες, receiver, ηλεκτρονικό έλεγχο ταχύτητας και μπαταρία, προσαρμοσμένα σε ένα ελαφρύ πλαστικό ή μεταλλικό πλαίσιο [23].

Επιπλέον, γυροσκόπια και άλλοι αισθητήρες προστίθενται για να αυξήσουν τη σταθερότητα του μέσου στον αέρα και μπορεί επίσης να χρησιμοποιεί συσκευή GPS. Τα περισσότεροι drones φέρουν επίσης μια φωτογραφική μηχανή για αεροφωτογραφίες, και ένα gimbal για προστιθέμενη σταθερότητα εικόνας. Επιπρόσθετα, μπορούν να συνδεθούν και άλλοι αισθητήρες, αν και υπάρχει ένα tradeoff μεταξύ αυξημένης λειτουργικότητα και βάρους [23]. Οι DJI, 3DRobotics και Parrot είναι μερικοί από τους κορυφαίους hardware κατασκευαστές και οι πωλήσεις τους περιλαμβάνουν τόσο συναρμολογημένα drones όσο και υποσυγκροτήματα [24].

Εικόνα 4.1: Δομή ενός εμπορικού Drone

Οι διαφορετικοί τύποι drones μπορούν να διακριθούν ανάλογα με τον τύπο (fixed-wing, multirotor, κ.λπ.), το βαθμός αυτονομίας, το μέγεθος και το βάρος, και την πηγή τροφοδοσίας. Αυτές οι προδιαγραφές είναι σημαντικές για τα drones όπως το εύρος πλεύσης, τη μέγιστη διάρκεια πτήσης και το φορτίο.

Για την πραγματοποίηση μιας πτήσης, τα drones χρειάζονται ασύρματη επικοινωνία με το χειριστή στο έδαφος. Επιπλέον, στις περισσότερες περιπτώσεις υπάρχει η ανάγκη επικοινωνίας με το payload (κάμερα ή αισθητήρα). Για να καταστεί εφικτό αυτό απαιτείται η εκμετάλλευση ενός συγκεκριμένου φάσματος συχνοτήτων. Οι απαιτήσεις

για το φάσμα αυτών εξαρτώνται από τον τύπο του drone, τα χαρακτηριστικά πτήσης και το payload που κουβαλά. Δεδομένου ότι το φάσμα συχνοτήτων δεν περιορίζεται στα εθνικά σύνορα, απαιτείται διεθνές συντονισμός σχετικά με τη χρήση του φάσματος συχνοτήτων. Νομικά ζητήματα όμως δημιουργούνται σχετικά με τη συχνότητα χρήσης και τον ηλεκτρονικό εξοπλισμό των drones τα οποία περιορίζουν και καθορίζουν τη δραστηριότητα των drones.

Η τάση για το μέλλον είναι να γίνουν τα drones μικρότερα, ελαφρύτερα, πιο αποδοτικά και φθηνότερα. Ως αποτέλεσμα, τα drones θα γίνουν όλο και περισσότερο διαθέσιμα στο ευρύ κοινό και θα χρησιμοποιηθούν σε αυξημένο αριθμό δραστηριοτήτων. Τα drones θα γίνουν ολοένα και πιο αυτόνομα και πιο ικανά να λειτουργούν σε σμήνη.

Το πιο αξιοσημείωτο χαρακτηριστικό είναι ο τύπος του drone. Ο όρος αυτός χρησιμοποιείται για τον ορισμό της διαφοράς μεταξύ συστημάτων σταθερής πτέρυγας, συστήματα multirotor και άλλα συστήματα. Παραδείγματα άλλων συστημάτων είναι τα λεγόμενα υβριδικά συστήματα, τα οποία συνδυάζουν συστήματα multirotor και σταθερής πτέρυγας, τα ορνιθόπτερα, και τα drones που χρησιμοποιούν κινητήρες turbofan. Η τεχνολογία που χρησιμοποιείται για να κρατήσει το drone στον αέρα καθορίζει τον τύπο του drone. Αυτό το χαρακτηριστικό αποτελεί επίσης τον καθοριστικό παράγοντα στο σχήμα και την εμφάνιση του drone. Ένα δεύτερο χαρακτηριστικό είναι το επίπεδο αυτονομίας του drone. Η αυτονομία μπορεί να ποικίλει από την πλήρη αυτόνομη λειτουργία έως τον πλήρη χειρισμό από απομακρυσμένο χειριστή. Ένα άλλο αξιοσημείωτο χαρακτηριστικό είναι η διαφορά στο μέγεθος μεταξύ των drones. Το μέγεθος μπορεί να ποικίλει από τα drones σε μέγεθος εντόμου, σε αεροσκάφη στο μέγεθος ενός εμπορικού αεροπλάνου. Το βάρος είναι επίσης ένα σημαντικό χαρακτηριστικό. Το βάρος των drones μπορεί να κυμαίνεται από μερικά γραμμάρια έως εκατοντάδες κιλά. Τέλος, ένα άλλο σημαντικό χαρακτηριστικό αποτελεί η πηγή τροφοδοσίας όπως μπαταρίες, ηλιακά κύτταρα αλλά και το παραδοσιακό καύσιμο [25].

Η πλειοψηφία των υφιστάμενων drones μπορεί να διαχωριστεί σε δύο τύπους. **Σταθερής πτέρυγας** και **multirotor**.

4.1.1 Συστήματα σταθερής πτέρυγας

Η σταθερή πτέρυγα είναι ένας όρος που χρησιμοποιείται κυρίως στον κλάδο των αερομεταφορών για να καθορίσει τα αεροσκάφη που χρησιμοποιούν σταθερά - στατικά πτερύγια σε συνδυασμό με την εμπρόσθια ταχύτητα αέρα για τη δημιουργία άντωσης. Παραδείγματα αυτού του τύπου αεροσκάφους είναι τα παραδοσιακά αεροπλάνα, οι χαρταετοί που είναι συνδεδεμένοι με το έδαφος και διάφορα είδη ανεμόπτερων. Ακόμα και το απλό χάρτινο αεροπλανάκι μπορεί να οριστεί ως σύστημα σταθερής πτέρυγας. Ένα παράδειγμα ενός drone σταθερής πτέρυγας είναι το ευρέως χρησιμοποιούμενο Raven.

4.1.2 Συστήματα Multirotor

Τα συστήματα Multirotor είναι ένα υποσύνολο των rotorcrafts. Ο όρος rotorcraft χρησιμοποιείται στην αεροπορία για να ορίσει αεροσκάφη που χρησιμοποιούν περιστρεφόμενες πτέρυγες για τη δημιουργία άντωσης. Ένα δημοφιλές παράδειγμα ενός rotorcraft είναι το παραδοσιακό ελικόπτερο. Το Rotorcraft μπορεί να έχει ένα ή περισσότερα στροφεία. Τα drones που χρησιμοποιούν περιστροφικά συστήματα είναι σχεδόν πάντα εξοπλισμένα με πολλαπλούς ρότορες, οι οποίοι είναι απαραίτητοι για τη σταθερότητά του, εξ ού και το όνομα, συστήματα multirotor. Συνήθως, αυτά τα drones χρησιμοποιούν τουλάχιστον τέσσερις ρότορες για να τα βοηθούν να πετούν. Ένα δημοφιλές παράδειγμα αυτών των multirotor drones είναι το ευρέως χρησιμοποιούμενο Phantom drone που κατασκευάζεται από την κινεζική εταιρεία DJI. Οι διαφορές μεταξύ των drones σταθερής πτέρυγας και των drones με πολλά στροφεία είναι σημαντικά για τις διάφορες εφαρμογές στις οποίες θέλουν οι καταναλωτές να τα χρησιμοποιήσουν. Για παράδειγμα, τα multirotor drones δεν χρειάζονται διάδρομο προσγείωσης, κάνουν λιγότερο θόρυβο από τα συστήματα σταθερής πτέρυγας και μπορούν να αιωρούνται. Τα drones σταθερής πτέρυγας μπορούν να πετάξουν πιο γρήγορα και είναι πιο κατάλληλα για μεγάλες αποστάσεις από ότι τα multirotor [25].

4.1.3 Άλλα Συστήματα

Ορισμένοι τύποι drones δεν μπορούν να επισημανθούν ως σταθερής πτέρυγας ή multirotor. Μερικές φορές, επειδή το drone απλά δεν είναι ούτε σταθερής πτέρυγας ούτε multirotor και μερικές φορές επειδή το drone έχει χαρακτηριστικά και των δύο

τύπων. Τα υβριδικά συστήματα είναι συστήματα που έχουν χαρακτηριστικά τόσο των συστημάτων multirotor όσο και των fixed-wing. Το υβριδικό quadcopter είναι ένα παράδειγμα ενός τέτοιου drone. Αυτό το drone χρησιμοποιεί πολλαπλούς ρότορες για να απογειωθεί και να προσγειωθεί κάθετα αλλά έχει και φτερά ώστε να μπορεί να πετάξει σε μεγαλύτερες αποστάσεις.

Τα αεροσκάφη που δεν είναι ούτε συστήματα σταθερής πτέρυγας ούτε συστήματα multirotor είναι πολύ πιο σπάνια. Ένα παράδειγμα τέτοιου drone είναι το ορνιθόπτερο. Αυτά τα drones πετούν μιμούμενα τις κινήσεις πτερυγίων εντόμων ή πτηνών. Αυτά τα μικρά drones ως επί το πλείστον αναπτύσσονται μόνο και δεν χρησιμοποιούνται ευρέως στην πράξη. Παραδείγματα ορνιθόπτερων είναι το Delfly Explorer, ένα drone που μιμείται ένα ιπτάμενο έντομο και που ακόμα βρίσκεται σε εξέλιξη και πρόκειται τελικά να προσομοιάζει μια μύγα τόσο σε μέγεθος όσο και στην κίνηση.

Ένα άλλο παράδειγμα drone που δεν είναι ούτε σταθερής πτέρυγας ούτε multirotor είναι τα drones που χρησιμοποιούν κινητήρες αεριωθουμένων. Το T-Hawk drone είναι ένα παράδειγμα ενός τέτοιου drone. Αυτό το drone χρησιμοποιεί έναν turbofan, κάνοντας το drone να μοιάζει περισσότερο με ένα μη επανδρωμένο (hydro) jetpack απ' ότι ένα σταθερής πτέρυγα ή multirotor [25].

Άλλα σημαντικά χαρακτηριστικά ενός drone είναι το μέγεθος και το βάρος του. Το χαμηλότερο όριο βάρους των μεγάλων drones είναι 150 Kg για τα σταθερής πτέρυγας και 100 Kg για τα multirotor drones.

Η ανάπτυξη των drones σήμερα επικεντρώνεται στην κατασκευή μικρότερων και ελαφρύτερων drones για το ευρύ κοινό. Τα μεγάλα drones χρησιμοποιούνται κυρίως για στρατιωτικούς σκοπούς. Προτείνεται συνήθως ο όρος μεγάλα drones για fixed-wing drones μεταξύ 20 και 150 Kg και multirotor drones μεταξύ 25 και 100 Kg.

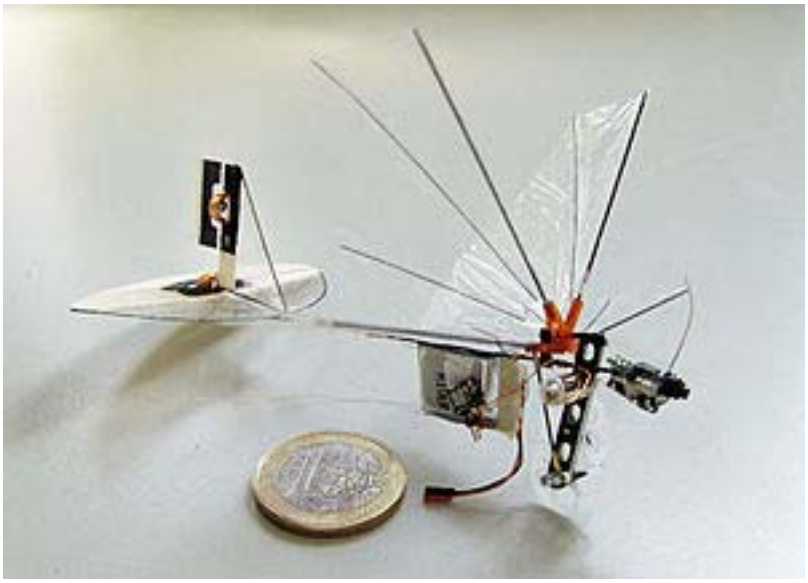
Τα μικρά drones είναι fixed-wing μέχρι 20 Kg και multirotor drones μέχρι 25 Kg [25]. Στην κατηγορία των μικρών drones υπάρχει και μια υποκατηγορία, mini-drones. Τα mini-drones μπορούν να ποικίλουν σε βάρος από μερικά γραμμάρια έως αρκετά κιλά. Αυτά τα mini-drones είναι κυρίως κατάλληλα για εσωτερικές εφαρμογές και ψυχαγωγία.

4.2 Ευρέως χρησιμοποιούμενα μοντέλα Drone

Λόγω της αυξανόμενης δημοτικότητας της τεχνολογίας drone, τα νέα μοντέλα αναπτύσσονται με γρήγορους ρυθμούς. Ως εκ τούτου, είναι αδύνατο να περιγραφεί κάθε μοντέλο drone που υπάρχει σήμερα. Μπορούν να παρουσιαστούν αντιπροσωπευτικά μερικά μοντέλα που χρησιμοποιούνται ευρέως τόσο από διάφορες υπηρεσίες, όσο και από πολίτες και εμπίπτουν στις κατηγορίες που προαναφέρθηκαν. Κάποια από τα μοντέλα αυτά είναι αρκετά δημοφιλή και σε ευρεία χρήση και είναι αυτά με τα οποία ο κόσμος είναι περισσότερο οικείος, τόσο στην εμφάνιση του όσο και στη χρήση του. Τα drones αυτά αναφέρθηκαν και πιο πάνω στην περιγραφή κάθε κατηγορίας.

4.2.1 Delfly Explorer

Το Delfly Explorer είναι ένα ορνιθόπτερο στο μέγεθος μεγάλου εντόμου το οποίο αναπτύχθηκε από το Delft University of Technology στην Ολλανδία. Το drone μπορεί να απογειωθεί και να πετάξει πλήρως αυτόνομα μέσα σε ένα κλειστό χώρο. Μπορεί να αποφύγει εμπόδια χρησιμοποιώντας δύο κάμερες. Το drone έχει βάρος 20g και μπορεί να λειτουργήσει επί του παρόντος για μόνο εννέα λεπτά λόγω των περιορισμών μεγέθους και βάρους της μπαταρίας [25].



Εικόνα 4.2: Το Delfly Explorer.

4.2.2 Hubsan x4 Drone

Το Hubsan x4 είναι ένα μικρό multirotor drone που αναπτύχθηκε από την κινεζική εταιρεία Hubsan. Αυτό το mini-drone είναι αρκετά απλό στο σχεδιασμό και τη λειτουργία. Έχει τέσσερις ρότορες και μπορεί να λειτουργήσει με χειριστή. Ορισμένα μοντέλα του x4 drone έρχονται με μια ενσωματωμένη κάμερα για λήψη φωτογραφιών και εγγραφή βίντεο. Το drone είναι επί του παρόντος μια δημοφιλής και σχετικά φθηνή εναλλακτική λύση για τα πιο εξελιγμένα drones. Το drone έχει βάρος 30g, ακτίνα περίπου 100m και μπορεί να λειτουργήσει για 7 λεπτά με μια πλήρως φορτισμένη μπαταρία. Σε αντίθεση με τα περισσότερα από τα άλλα μοντέλα, αυτό το drone δεν έχουν προηγμένες λειτουργίες και είναι κυρίως κατασκευασμένο για ψυχαγωγικούς σκοπούς [25].

Εικόνα 4.3: Το Hubsan x4 Drone

4.2.3 Parrot AR Drone

Το Parrot είναι ένα drone που κατασκευάστηκε κυρίως για ψυχαγωγικούς σκοπούς. Έχει multirotor σύστημα που μπορεί να ελεγχθεί από ένα smartphone ή tablet. Το drone μπορεί να λειτουργήσει για 12-18 λεπτά και ζυγίζει περίπου 400g. Η ταχύτητα του είναι περίπου 18 Km/h και έχει εμβέλεια περίπου 50m. Το drone διαθέτει δύο κάμερες, τεχνολογία Bluetooth και Wi-Fi και χρησιμοποιεί το GPS για να πετάξει μια προκαθορισμένη διαδρομή. Το Parrot είναι παρόμοιο με το Phantom, τόσο σε

εφαρμογές όσο και σε λειτουργίες. Έχει λογισμικό κινηματογράφησης και φωτογράφισης. Ο χρήστης μπορεί επίσης να προγραμματίσει εκ των προτέρων το drone με μια διεργασία αλλά και τις ρυθμίσεις όπως τη διατήρηση ενός συγκεκριμένου ύψους, τα οποία μετά εκτελεί από μόνο του. Το Parrot είναι ένα από τα πιο ευρέως χρησιμοποιούμενα και δημοφιλή μοντέλα για δραστηριότητες ψυχαγωγίας αυτή τη στιγμή [25].

Εικόνα 4.4: Το Parrot AR Drone

4.2.4 DJI Phantom

Το Phantom drone είναι ένα multirotor drone με τέσσερις ρότορες και είναι κατασκευασμένο κυρίως για δραστηριότητες ψυχαγωγίας. Το drone έρχεται με μια κάμερα και μπορεί να τύχει χειρισμού χρησιμοποιώντας ένα smartphone ή ένα Wi-Fi control. Το smartphone μπορεί επίσης να ελέγξει την κάμερα, να μετακινήσει και να βγάλει φωτογραφίες ή να εγγράψει βίντεο. Το Phantom μπορεί να πετάξει περίπου στα 54 Km/h και μπορεί να λειτουργήσει για περίπου 25 λεπτά. Απλά προγραμματίζοντας το ύψος πτήσης και ορισμένα σημεία της διαδρομής μπορεί να απογειωθεί, να προσγειωθεί, να κάνει καταγραφές και να επιστρέψει πίσω αυτόματα [25].

Εικόνα 4.5: Το DJI Phantom

4.2.5 DJI Inspire 1 PRO

Το DJI Inspire 1 PRO είναι ένα κορυφαίο drone για αεροφωτογράφιση, βιντεογράφηση αλλά και φωτογράφιση. Έχει βάρος 6,2 lb., αυτονομία 18 λεπτά και εμβέλεια 2Km. Τα άκρα του, κατασκευασμένα από ίνες άνθρακα, κινούνται προς τα επάνω αλλά και έξω από το οπτικό πεδίο της κάμερας κατά την πτήση, δίνοντας μια άποψη 360 μοιρών του κόσμου γύρω από το drone. Η φωτογραφική του μηχανή καταγράφει βίντεο 4K, βγάζει φωτογραφίες μεγέθους 16 megapixel και επιτρέπει την αλλαγή φακών. Καταγράφει επίσης αμοντάριστα βίντεο - ιδανικό για επαγγελματική κινηματογράφηση. Μπορεί επίσης να στέλλει εικόνα σε πραγματικό χρόνο στην κινητή συσκευή. Η εφαρμογή του δίνει επίσης χειροκίνητο έλεγχο της κάμερας, δεδομένα τηλεμετρίας πτήσης και αυτόματη απογείωση και προσγείωση.

Το Inspire 1 PRO είναι επίσης ικανό για έλεγχο διπλού χειριστή, επιτρέποντάς τον έλεγχο του quadcopter από δύο πομπούς και δύο άτομα. Μπορεί ένα άτομο να είναι επικεντρωμένο στον έλεγχο πτήσης και το άλλο να ελέγχει την κάμερα. Το DJI Inspire 1 PRO αποτελεί ένα drone κατάλληλο για επαγγελματικές εναέριες εργασίες [26].

Εικόνα 4.6: Το DJI Inspire 1 PRO

4.2.6 Yuneec H520

Το H520 είναι εφοδιασμένο με έξι ρότορες, μια φωτογραφική μηχανή με adaptor 360 μοιρών και ανακλινόμενο σύστημα προσγείωσης. Είναι έτοιμο από το κουτί, εύκολο και ασφαλές στη πτήση, με εκπληκτικές δυνατότητες βίντεο Ultra HD και 4K φωτογραφίες. Έχει βάρος 3,6 lb., αυτονομία 25 λεπτά και εμβέλεια 500m.

Το H520 της Yuneec κατασκευάστηκε τόσο για βιομηχανική χρήση όσο και για επαγγελματίες. Έρχεται με φακούς μεγάλου εστιακού μήκους που επιτρέπουν στο drone να πετάει σε μεγαλύτερη απόσταση από ένα αντικείμενο και να αποθηκεύει δεδομένα που μπορεί να μοιραστεί άμεσα με τον σταθμό εδάφους ST16S ή να μετατραπούν απευθείας σε εικόνες 4K / 2K / HD ή 20MP [26].

Εικόνα 4.7: Το Yuneec's H520

4.2.7 3DR Solo

Το Solo είναι ένα εξαιρετικό quadcopter για αθλητικές φωτογραφίσεις και βιντεογραφήσεις. Είναι το μοναδικό drone που μπορεί να μεταφέρει ροή ασύρματου βίντεο HD από κάμερα GoPro απευθείας σε iOS και συσκευές Android.

Το Solo είναι εξοπλισμένο με την τεχνολογία Smart Shot, καθιστώντας εύκολη τη λήψη υψηλής ποιότητας βίντεο χωρίς να προαπαιτεί ιδιαίτερα προσόντα. Είναι επίσης το πρώτο drone που επιτρέπει την πρόσβαση κατά την πτήση στην GoPro, επιτρέποντάς εκκίνηση εγγραφής, παύση εγγραφής και προσαρμογή των ρυθμίσεων της κάμερας από το έδαφος [26].

Εικόνα 4.8: Το 3DR Solo

4.2.8 Raven

Εκτός από τα multirotor drones υπάρχουν και παραδείγματα fixed-wing όπως είναι το Raven το οποίο αναπτύχθηκε το 2002. Το drone αρχικά αναπτύχθηκε για τον αμερικανικό στρατό, αλλά χρησιμοποιείται συχνά και από πολλές άλλες χώρες, καθιστώντας το ένα από τα πιο ευρέως χρησιμοποιούμενα drones στον κόσμο αυτή τη

στιγμή. Ο κύριος σκοπός του Raven είναι η επιτήρηση και μπορεί να ελεγχθεί εξ αποστάσεως ή να προγραμματιστεί εκ των προτέρων για αυτόνομη λειτουργία. Το Raven έχει πλάτος 1,4 m, ζυγίζει περίπου 2 κιλά και μπορεί να παραμείνει σε λειτουργία για 60-90 λεπτά σε απόσταση 10 χλμ. Είναι επίσης εξοπλισμένο με οπτική και υπέρυθρη κάμερα. Όπως και τα συνηθισμένα μοντέλα αεροπλάνα, το Raven μπορεί να πετάξει ρίχνοντας τον στον αέρα. Προσγειώνεται ολισθαίνοντας σε προγραμματισμένο μέρος προσγείωσης και μπορεί να αντισταθμίσει την πρόσκρουση όταν χτυπά το έδαφος αφού αποσυναρμολογείται αυτόματα κατά την πρόσκρουση [25].

Εικόνα 4.9: Το Raven

4.3 Θέματα Συχνοτήτων

Για να εκτελεστεί μια πτήση, τα περισσότερα drones χρειάζονται ένα συγκεκριμένο φάσμα συχνοτήτων έτσι ώστε να μπορούν να επικοινωνούν με το χειριστή στο έδαφος. Επιπλέον, στις περισσότερες περιπτώσεις υπάρχει ανάγκη για ραδιοεπικοινωνία για το payload, όπως τη κάμερα ή κάποιο είδος αισθητήρα. Για να μπορεί η ραδιοεπικοινωνία να πραγματοποιηθεί επιβάλλεται η χρήση συγκεκριμένων συχνοτήτων οι οποίες εξαρτώνται από τον τύπο του drone, τα χαρακτηριστικά πτήσης και το payload. Οι 2,4 GHz και 5,8 GHz είναι δύο από τις πιο συνηθισμένες συχνότητες επικοινωνίας και ελέγχου στα FPV Quadcopter.

Η 2,4 GHz είναι η κοινή RF που χρησιμοποιείται από τα Quadcopters για τη σύνδεση του πομπού εδάφους με το drone. Η συχνότητα όμως των 2,4 GHz είναι ίδια με εκείνη που χρησιμοποιούν κάποια πρότυπα στα ασύρματα δίκτυα υπολογιστών. Αυτό μπορεί να οδηγήσει σε interference κάτι που συμβαίνει συχνά αφού υπήρξαν πολλά περιστατικά

που ανέφεραν την απώλεια ελέγχου των drones αυτών σε πυκνοκατοικημένες περιοχές όπου υπάρχουν πάρα πολλά ασύρματα σήματα.

Ένα άλλο πρόβλημα που σχετίζεται με τα Quadcopters είναι ότι μπορεί να υπάρξει interference και μεταξύ των συστημάτων τους. Αυτό οφείλεται κυρίως στη ύπαρξη δύο πομπών - ένα για τη μεταφορά των σημάτων χειρισμού στο όχημα και το άλλο για τη μεταφορά των σημάτων βίντεο πίσω στον χειριστή.

Τα 5.8 GHz είναι μια άλλη συχνότητα που χρησιμοποιείται σε τεχνολογίες quadcopter, για να αποφευχθεί η εμπλοκή των συχνοτήτων στην ίδια μπάντα. Αυτή η συχνότητα βρίσκεται συνήθως στα μοντέλα DJI Phantom. Πιο κάτω βλέπουμε πώς αντιμετωπίζεται το πρόβλημα αυτό στα Phantom drones.

Phantom 1 - Αυτό το drone λειτουργεί στα 2,4 GHz. Εάν προβλέπεται και ένα FPV, τότε χρησιμοποιείται η συχνότητα των 5,8 GHz για να αποφεύγονται τα προβλήματα αλληλοπαρεμβολών. Σε περίπτωση που χρησιμοποιείται GoPro ή οποιαδήποτε άλλη κάμερα με το ασύρματο της σύστημα, τότε πρέπει να απενεργοποιείται η επιλογή Wireless. Διαφορετικά, υπάρχει interference.

Phantom FC40 - Αυτό το drone χρησιμοποιεί τη συχνότητα 5.8 GHz για να πετάξει επειδή έχει ένα ξεχωριστό σύστημα των 3,4 GHz για να μεταδώσει βίντεο και φωτογραφίες στον χειριστή.

Phantom 2 - Αυτό το drone χρησιμοποιεί τη συχνότητα 2,4 GHz για τον έλεγχο και έτσι πρέπει να χρησιμοποιούνται κιτς πρόσθετων που χρησιμοποιούν συχνότητα 5,8 GHz για τη μετάδοση σημάτων FPV.

Phantom 2 Vision and Vision + - Και τα δύο αυτά drones χρησιμοποιούν τα 5,8 GHz για έλεγχο και 2,4 GHz για σύνδεση FPV, σύνδεση με smartphone και τηλεμετρία [27].

4.4 Νομοθεσία

Υφιστάμενη Νομοθεσία χειρισμού Drones/UAVs στην Κυπριακή Δημοκρατία.

Όπως σε άλλες χώρες, στις οποίες η χρήση μη επανδρωμένων οχημάτων drones ή UAVs έχει γίνει πλέον μαζική σε όλους τους τομείς και υπηρεσίες, έτσι και στην Κύπρο, ακολουθώντας την ολοένα και αυξανόμενη εμφάνιση αυτών των αεροχημάτων στους κυπριακούς ουρανούς, η κυβέρνηση της Κυπριακής Δημοκρατίας, και συγκεκριμένα το υπουργείο Συγκοινωνιών και Έργων ως το καθ' ύλην αρμόδιο, έχει προχωρήσει στην έκδοση διατάγματος ως Διάταγμα του τμήματος Πολιτικής Αεροπορίας με τίτλο «Διαδικασίες χειρισμού πτήσης μη επανδρωμένων αεροχημάτων στη Δημοκρατία της Κύπρου» με ημερομηνία δημοσίευσης στην εφημερίδα της κυβέρνησης την 27.11.2015.

Το διάταγμα αυτό, το οποίο παρατίθεται στο παράρτημα, κατηγοριοποιεί τα αεροχήματα αυτά ανάλογα με το βάρος τους και την χρήση τους και αναφέρει ρητώς τους περιορισμούς χρήσης τους από τον εκάστοτε ιδιοκτήτη ή/και χειριστή.

Πιο κάτω θα αναφέρουμε τα βασικότερα σημεία του διατάγματος αυτού. Σημαντικό είναι να αναφέρουμε ότι η μη συμμόρφωση σε τέτοια διατάγματα και νομοθεσίες είναι που καθιστούν επικίνδυνη την πτήση αυτών των μη επανδρωμένων αεροχημάτων καθιστώντας επιβεβλημένη την ανάπτυξη συστημάτων απενεργοποίησης τους προς όφελος της κρατικής και δημόσιας ασφάλειας και πάντα στα πλαίσια κανονισμών και δημοσίου συμφέροντος.

Σύμφωνα με το διάταγμα αυτό, η ανάγκη εξασφάλισης ειδικής άδειας για πτήση εξαρτάται από το είδος χρήσης αλλά και το βάρος του drone. Αν η χρήση είναι καθαρά προσωπική τότε το drone υπάγεται στην Ανοικτή κατηγορία στην οποία δεν απαιτείται εξασφάλιση ειδικής άδειας. Αυτό προϋποθέτει όμως ότι το βάρος του drone είναι λιγότερο από 3Kg. Αν είναι 3Kg και πάνω τότε, ανεξαρτήτως του σκοπού που γίνεται χρήση του, εμπίπτει στην Ειδική κατηγορία όπου απαιτείται τόσο διεθνής άδεια κύπριου πιλότου drone όσο και διεθνής άδεια χειρισμού drone. Αν η πτήση πραγματοποιείται για εμπορικούς σκοπούς, τότε ανεξαρτήτως του βάρους του, εμπίπτει στην ειδική κατηγορία όπου απαιτείται η εξασφάλιση ειδικής άδειας.

Οποιοσδήποτε τουρίστας έχει το δικαίωμα να μεταφέρει ένα drone, για προσωπική χρήση, μέχρι 3Kg στο έδαφος της Κυπριακής Δημοκρατίας χωρίς να το δηλώσει στο τελωνείο, οφείλει όμως να το εγγράψει με ειδική αίτηση στο τμήμα Πολιτικής Αεροπορίας. Η εγγραφή των drones στο τμήμα πολιτικής αεροπορίας είναι υποχρεωτική για όλους τους χειριστές ανεξαρτήτων κατηγορίας στην οποία εμπίπτουν. Επίσης το τμήμα πολιτικής αεροπορίας δεν αναγνωρίζει οποιαδήποτε άδεια άλλης χώρας για πτήση drone και απαιτείται έκδοση από το τμήμα της Κυπριακής Δημοκρατίας.

Όσον αφορά την πτήση των drones υπάρχουν περιορισμοί σύμφωνα με το διάταγμα. Για την Ανοικτή κατηγορία, το μέγιστο ύψος πτήσης είναι 50m (170 ft.) πάνω από το έδαφος ή το επίπεδο της θάλασσας και για την Ειδική κατηγορία, 120m (400 ft.). Ανεξαρτήτου κατηγορίας είναι υποχρεωτικό να υπάρχει πάντα οπτική επαφή με το drone και η απόσταση drone με το χειριστή να μην υπερβαίνει τα 500m. Απαγορεύεται η πτήση κοντά σε κατοικημένες περιοχές και ανθρώπους. Πρέπει να υπάρχει απόσταση ασφαλείας 1Km από κατοικημένες περιοχές. Απαιτείται απόσταση ασφαλείας 500m από απομονωμένα κτίρια, ανθρώπους, οχήματα, ζώα, οικοδομές κλπ, εκτός από του χειριστή. Απαγορεύεται η πτήση κοντά σε αεροδρόμια ή ελικοδρόμια. Απαιτείται απόσταση ασφαλείας 8Km από αεροδρόμια και 3Km από ελικοδρόμια. Επίσης απαγορεύεται οποιαδήποτε πτήση τους κατά τη νύχτα. Στην Κύπρο αυτή τη στιγμή υπάρχουν δύο δεσμευμένες περιοχές για πτήση drones, μια στο Μαρκί και μια στην Τερσεφάνου.

Άλλοι περιορισμοί που προβλέπει το διάταγμα είναι:

- Απαγορεύεται η πτήση σε απαγορευμένες, δεσμευμένες και επικίνδυνες περιοχές οι οποίες δημοσιεύονται από το τμήμα Πολιτικής Αεροπορίας.
- Απαγορεύεται η εναέρια φωτογράφιση/βιντεογράφιση υποδομών και εγκαταστάσεων της Εθνικής Φρουράς.
- Απαγορεύεται η πτήση σε περιοχές όπου πραγματοποιούνται πτήσεις ελικοπτέρων ή αεροσκαφών για σκοπούς Έρευνας-Διάσωσης, πυρόσβεσης και στρατιωτικών ασκήσεων.
- Απαγορεύεται η πτήση πάνω από στρατιωτικές εγκαταστάσεις, δημόσιες εγκαταστάσεις, και αρχαιολογικούς χώρους. Μόνο υπό εξασφάλιση ειδικής άδειας από την αρμόδια αρχή επιτρέπεται αυτού του είδους πτήση.

Απαγορεύεται η πτήση πάνω από στρατιωτικές εγκαταστάσεις, δημόσιες εγκαταστάσεις

- Απαγορεύεται η εκτόξευση ή άφεση αντικειμένων από το drone.
- Η χρήση των drones πρέπει να συνάδει με τους νόμους περί σεβασμού στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων.

Για οποιαδήποτε παραβίαση των πιο πάνω, ο παραβάτης υπόκειται στις ποινές σύμφωνα με το σχετικό διάταγμα.

Κεφάλαιο 5
Global Navigation Satellite System (GNSS)

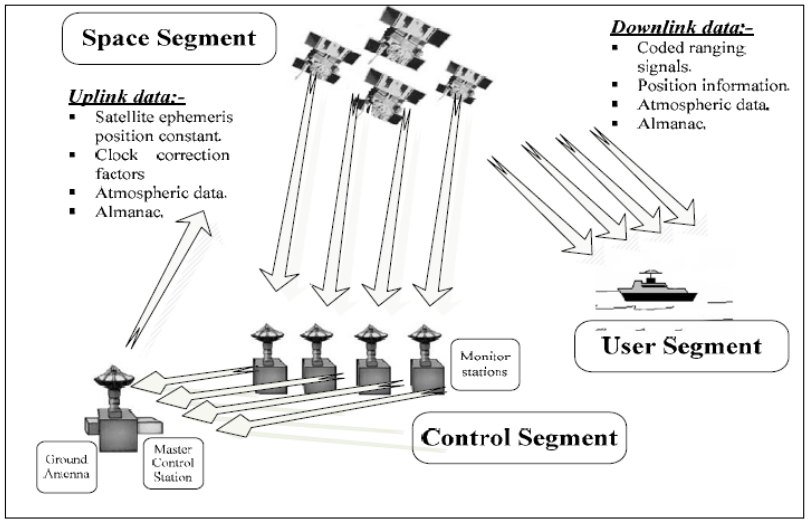
5.1 Συστατικά GNSS

Το GNSS αποτελείται από τρεις κύριες δορυφορικές τεχνολογίες: το **GPS**, το **Glonass** και το **Galileo**. Καθένα από αυτά τα συστήματα αποτελείται κυρίως από τρία τμήματα: (α) space segment, (β) control segment και (γ) user segment. Αυτά τα τμήματα είναι σχεδόν όμοια στις τρεις δορυφορικές τεχνολογίες, οι οποίες μαζί αποτελούν το GNSS. Σήμερα, η πιο πλήρης δορυφορική τεχνολογία είναι η τεχνολογία GPS και το μεγαλύτερο μέρος από τις υπάρχουσες παγκόσμιες εφαρμογές, σχετίζονται με τη GPS τεχνολογία. Η τεχνολογία GNSS θα γίνει πιο ολοκληρωμένη μετά τη λειτουργία του Galileo και την επαναλειτουργία του Glonass στα επόμενα χρόνια.

5.1.1 Παγκόσμιο σύστημα εντοπισμού θέσης GPS

Το αμερικανικό Υπουργείο Άμυνας (DoD) έχει αναπτύξει το Navstar GPS, το οποίο είναι ένα παντός καιρού, σύστημα πλοήγησης με σκοπό την κάλυψη των αναγκών των στρατιωτικών δυνάμεων των ΗΠΑ προσδιορίζοντας με ακρίβεια τη θέση, την ταχύτητα και τον χρόνο σε ένα κοινό σύστημα αναφοράς, οπουδήποτε πάνω ή κοντά στη Γη σε συνεχή βάση [28].

Το GPS έχει επηρεάσει σημαντικά σχεδόν όλες τις positioning, navigation, timing και monitoring εφαρμογές παρακολούθησης. Παρέχει ειδικά κωδικοποιημένα δορυφορικά σήματα που μπορούν να τύχουν επεξεργασίας σε ένα Δέκτη GPS, επιτρέποντας στον δέκτη να υπολογίζει τη θέση, την ταχύτητα και το χρόνο. Υπάρχουν τέσσερα δορυφορικά σήματα GPS που χρησιμοποιούνται για τον υπολογισμό θέσεων στις τρεις διαστάσεις και την χρονική μετατόπιση στο ρολόι του δέκτη [28].



Σχήμα 5.1: GPS Segments

5.1.2 GLONASS

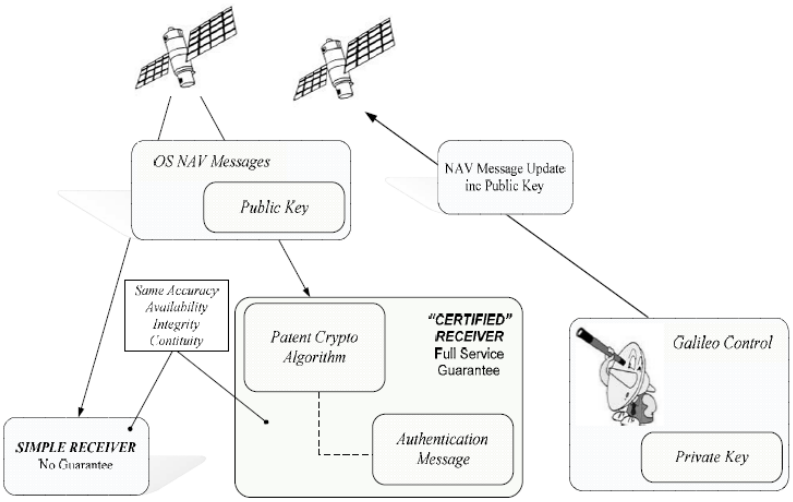
Το GLONASS (GLObal NAvigation Satellite System or "GLObalnaya NAvigatsionnaya Sputnikovaya Sistema") είναι σχεδόν πανομοιότυπο με το GPS. Το Δορυφορικό σύστημα Glonass παρέχει πληροφορίες σχετικά με τη θέση και το χρόνο στους χρήστες. Λειτουργεί από το Υπουργείο Άμυνα της Ρωσικής Ομοσπονδίας [29].

Το space segment του Glonass αποτελείται από 24 δορυφόρους, που κατανέμονται εξίσου σε 3 τροχιές που χωρίζονται από 120^{o} στο ύψος του ισημερινού. Το ύψος τροχιάς του δορυφόρου είναι περίπου 19.130χλμ. πάνω από την επιφάνεια του εδάφους. Αυτό οδηγεί σε μια τροχιακή περίοδο 11:15:44 που αντιστοιχεί σε 8/17 μιας ημέρας. Το μέλλον του GLONASS φαντάζει αβέβαιο λόγω των οικονομικών προβλημάτων που αντιμετωπίζει η ρωσική Ομοσπονδία. Ο αριθμός των επιχειρησιακών δορυφόρων μειώθηκε σταθερά τα τελευταία χρόνια [28].

5.1.3 GALILEO

Το GALILEO αποτελεί μια πρωτοβουλία της Ευρώπης για ένα σύγχρονο παγκόσμιο δορυφορικό σύστημα πλοήγησης, παρέχοντας μια άκρως ακριβή, εγγυημένη παγκόσμια υπηρεσία προσδιορισμού θέσης υπό πολιτικό έλεγχο. Το GALILEO δεν θα είναι πολύ διαφορετικό από τα άλλα τμήματα του GNSS (GPS και Glonass). Θα παρέχει αυτόνομες υπηρεσίες πλοήγησης και εντοπισμού θέσης, αλλά ταυτόχρονα θα είναι διαλειτουργικό με τα δύο άλλα παγκόσμια δορυφορικά συστήματα πλοήγησης το GPS και το GLONASS. Ένας χρήστης θα είναι σε θέση να λάβει τη θέση του με τον ίδιο δέκτη από οποιοδήποτε από τους δορυφόρους σε οποιονδήποτε συνδυασμό. Ωστόσο, παρέχοντας διπλές συχνότητες ως standard, το GALILEO θα παρέχει ακρίβεια εντοπισμού σε πραγματικό χρόνο μέχρι το εύρος του μέτρου. Θα εγγυάται πάνω από όλα τη διαθεσιμότητα της υπηρεσίας και στις πιο ακραίες συνθήκες και θα ενημερώνει τους χρήστες μέσα σε λίγα δευτερόλεπτα για την αποτυχία οποιουδήποτε δορυφόρου. Αυτό θα το καταστήσει κατάλληλο για εφαρμογές όπου η ασφάλεια είναι ζωτικής σημασίας, όπως τρένα, οδήγηση αυτοκινήτων και προσγείωση αεροσκαφών. Η συνδυασμένη χρήση του GALILEO και των άλλων συστημάτων GNSS μπορεί να προσφέρει πολύ καλύτερες επιδόσεις σε όλους τους χρήστες παγκοσμίως [28].

Το space segment του GALILEO αποτελείται από 30 μέσης τροχιάς (MEO) δορυφόρους (27 και 3 ενεργούς εφεδρικούς δορυφόρους), κατανεμημένους ομοιόμορφα και τακτικά σε τρία επίπεδα τροχιάς. Το ύψος τροχιάς είναι ελαφρώς μεγαλύτερο από το GPS, στα 23.616 Km και η κλίση είναι 56°. Το Galileo θα παρέχει πολλά σήματα πλοήγησης στην δεξιά κυκλική πόλωση (RHCP) στις μπάντες συχνοτήτων 1164-1215 MHz (E5a και E5b), 1260-1300 MHz (E6) και 1559-1592 MHz (E2-L1-E1) που αποτελούν μέρος της κατανομής της δορυφορικής υπηρεσίας ραδιοπλοήγησης (RNSS) [28].



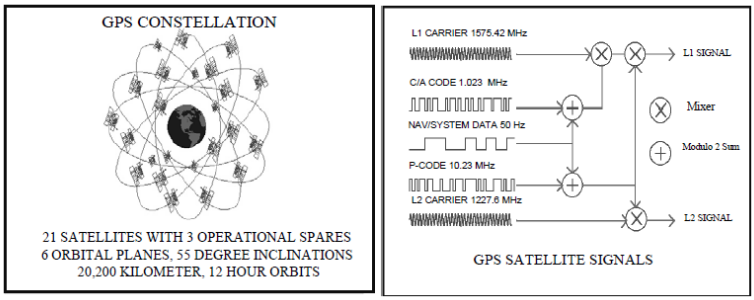
Σχήμα 5.2: Η αρχιτεκτονική του συστήματος GALILEO

Λόγω του ότι τα drones που κυκλοφορούν στο εμπόριο χρησιμοποιούν το σύστημα εντοπισμού θέσης GPS, στο οποίο θα στοχεύσουμε για την απενεργοποίηση του drone στο στάδιο υλοποίησης του συστήματος που προτείνει η διατριβή, ακολουθεί αναλυτικότερη περιγραφή του συγκεκριμένου συστήματος εντοπισμού θέσης στις επόμενες παραγράφους.

5.2 GPS

5.2.1 Ιστορία του GPS

Το GPS (Global Positioning System), είναι ένας τύπος παγκόσμιου δορυφορικού συστήματος πλοήγησης που σήμερα αποτελείται από 27 δορυφόρους που περιστρέφονται γύρω από σταθερά σημεία στη γη. Αρχικά σχεδιασμένο για στρατιωτική χρήση, το GPS δεν χρησιμοποιήθηκε για εμπορικές και πολιτικές εφαρμογές μέχρι τις αρχές της δεκαετίας του 1980 [30].



Σχήμα 5.3: Αριστερά ο σχηματισμός του GPS. Δεξιά παρουσίαση των σημάτων ενός δορυφόρου GPS

Το 2000, η κυβέρνηση των ΗΠΑ απενεργοποίησε την επιλεκτική διαθεσιμότητα του πρωτοκόλλου GPS. Αυτό το χαρακτηριστικό αποτελούσε τη σκόπιμη υποβάθμιση της ποιότητας για συγκεκριμένες χρήσεις του GPS σε ορισμένες περιοχές. Η επιλεκτική διαθεσιμότητα εφαρμόστηκε αρχικά ως μέτρο ασφάλειας κατά της κακόβουλης χρήσης της παρακολούθησης [31]. Τα οφέλη του χρήστη από την απενεργοποίηση της επιλεκτικής διαθεσιμότητας είναι προφανή, η μεγαλύτερη ακρίβεια για πολιτικές εφαρμογές.

Τα κυβερνητικά προγράμματα προχώρησαν με τρία νέα Civilian layers σήματος GPS [32]. Αυτά περιλαμβάνουν:

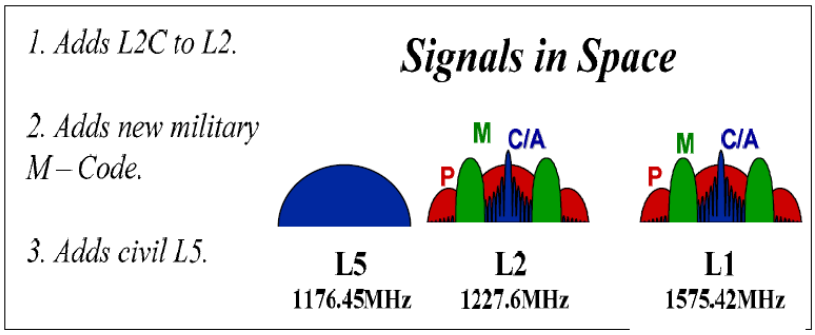
L2C: Ένα σήμα 1227 MHz για πολιτικές ανάγκες με στρατιωτική ακρίβεια ή και καλύτερη

L1C: Ένα σήμα 1575 MHz για τη διαλειτουργικότητα του GPS με άλλα συστήματα GNSS για αστική χρήση

L5: Ένα σήμα 1176MHz για χρήση σε αποκλειστικά συστήματα ασφαλείας ζωής όπως μεταφορές, εμπορικά αεροσκάφη και μεταφορές έκτακτης ανάγκης

Κατά την ανάλυση πληροφοριών σχετικά με αυτές τις μπάντες σημάτων, η ασφάλεια αναφέρεται μόνο για προστασία της μετάφρασης σήματος L1C μεταξύ των αμερικάνικων συστημάτων GPS και συστημάτων της ΕΕ όπως το Galileo από τον αστικό θόρυβο. Δεν προβλέπεται ούτε καν η πιθανότητα κακόβουλων επιθέσεων. Στο σήμα L5 υπάρχει αλλαγή στο πεδίο της ασφάλειας. Προστέθηκαν μέτρα ελέγχου από το Υπουργείο Άμυνας της Αμερικής. Αυτά τα μέτρα σκοπεύουν στο να διασφαλιστεί ότι

από το νέο κύμα των δορυφόρων GPS, στους σταθμούς ελέγχου, η επικοινωνία θα είναι ισχυρή και πλεοναστική[32].



Σχήμα 5.4: Οι μπάντες του GPS.

5.2.2 Πώς λειτουργεί το GPS

Τα συστήματα GPS λαμβάνουν σήμα από ένα σύνολο από 27 δορυφόρους που πετούν σε μεσαία τροχιά γύρω από τη γη. Χρησιμοποιώντας πλειάδες σήματος από οποιουσδήποτε τρεις (αλλά τυπικά τέσσερις ή περισσότερους για ακρίβεια) δορυφόρους ο client μπορεί να χρησιμοποιήσει το trilateration για να βρει το intersection Latitudinal και Longitudinal γύρω από τρία σταθερά σημεία, δίνοντας του μια ακριβή θέση στην επιφάνεια της Γης. Τα δεδομένα του σήματος περιέχουν την ατομική χρονική σήμανση, τη θέση του δορυφόρου και προαιρετικά ένα checksum. Δεδομένου ότι τα ραδιοκύματα ταξιδεύουν κοντά στην ταχύτητα του φωτός, αγνοώντας τις παρεμβολές, οι clients χρησιμοποιούν τη χρονική σήμανση για τον υπολογισμό της απόστασης από το δορυφόρο. Εάν το checksum χρησιμοποιείται στην πλευρά του client και ο τρέχον δορυφόρος GPS το υποστηρίζει αυτό, τότε η ποιότητα (που το σήμα δεν έχει παραμορφωθεί λόγω θορύβου) είναι εγγυημένη. Το Checksum μπορεί να θεωρηθεί ότι επαληθεύει την ακεραιότητα του σήματος. Ωστόσο, δεν εξασφαλίζει την αυθεντικότητα του σήματος [33].

5.2.3 Επιθέσεις

Τα παγκόσμια δορυφορικά συστήματα πλοήγησης (GNSS) είναι ευάλωτα σε διάφορες απειλές, συμπεριλαμβανομένου του jamming και του spoofing.

Το jamming είναι η σκόπιμη μετάδοση ισχυρών ραδιοσημάτων (RF) τα οποία μπορούν εύκολα να υπερνικήσουν τα πολύ ασθενέστερα συστατικά στοιχεία του GNSS με αποτέλεσμα να διαταράσσουν και, σε ορισμένες περιπτώσεις, να μπλοκάρουν τις λειτουργίες του GNSS.

Οι narrow-band δέκτες επηρεάζονται λιγότερο από το jamming αφού είναι σε θέση να φιλτράρουν ένα μεγαλύτερο μέρος του σήματος παρεμβολής. Η ύπαρξη ενός καθαρού πιλοτικού καναλιού στο τμήμα διαμόρφωση του Galileo E1 επιτρέπει στους δέκτες να χρησιμοποιούν ένα pure Phase Lock Loop (PLL), το οποίο με τη σειρά του επιτρέπει τη λήψη σήματος παρουσία ισχυρότερων σημάτων jamming [34].

Οι δέκτες GPS λαμβάνουν ένα πολύ ασθενές σήμα από τον δορυφόρο, έτσι το jamming του δέκτη είναι ένα σημαντικό μέσο παρεμβολής GPS. Από τεχνικής άποψης, το jamming του δέκτη μπορεί να χωριστεί σε δύο είδη: το blanket jamming, και το deception jamming.

Υπάρχουν δύο βασικοί τύποι επιθέσεων που έχουν χρησιμοποιηθεί στο παρελθόν. Το Signal Jamming είναι η μετάδοση θορύβου πάνω από τη συχνότητα GPS που λειτουργεί ως επίθεση Denial-of-Service κατά των clients. Το Spoofing μεταδίδει ψευδή δεδομένα χρησιμοποιώντας τον κωδικό C/A ενός δορυφόρου για να κάνει τους clients να κάνουν λανθασμένες εκτιμήσεις για το πού είναι ο δορυφόρος αυτή τη στιγμή. Το μοντέλο τέτοιας απειλής αναπτύσσεται όσο αυξάνονται οι επιθέσεις σε τέτοιες υπηρεσίες.

Signal Jamming

Όπως το Wi-Fi, το WiMax και τα κυψελοειδή σήματα όπως το 3G και το 4G, έτσι και το GPS είναι ευαίσθητο στο θόρυβο και στις παρεμβολές. Σε αντίθεση όμως με αυτά τα σήματα, το μέγεθος του πακέτου δεδομένων είναι γνωστό και ο ρυθμός συγχρονισμού των δεδομένων είναι επίσης γνωστά εξ ορισμού.

Το Blanket jamming στο οποίο οι επιτιθέμενοι, πραγματοποιούν μια επίθεση η οποία εξάγει θόρυβο στη ζώνη συχνοτήτων GPS είναι η κοινή και απλή έκδοση αυτής της επίθεσης. Αυτή η επίθεση περιέχει ρίσκο για τους επιτιθέμενους, καθώς είναι εύκολο να εντοπιστεί ένα τέτοιο σήμα και είναι εξαιρετικά παράνομο.

Δεδομένου ότι το signal Jamming είναι μια πολύ ενοχλητική επίθεση σε ζωτικά συστήματα όπως της αστυνομίας και των ιατρικών μεταφορών, καθώς και μεγάλα εμπορικά συστήματα όπως τις μεταφορές και τα αεροδρόμια, η FCC έχει καταστήσει ρητώς παράνομη την αγορά, πώληση, εμπορία, ή λειτουργία τέτοιων εξοπλισμών jamming [35].

Η ρυθμική φύση του GPS επιτρέπει στους επιτιθέμενους που επικεντρώνονται στις επιθέσεις jammer να είναι πιο αθόρυβοι από εκείνους που προσπαθούν να αποφύγουν το ραντάρ της αστυνομίας ή να απενεργοποιήσουν το Wi-Fi. Επειδή οι clients GPS χρειάζονται συγχρονισμό με το C/A κώδικα ενός δορυφόρου και στη συνέχεια να υπολογίσει το offset στο χρόνο για να βρει τη θέση, ο εισβολέας χρειάζεται μόνο σήματα jamming κατά τη διάρκεια του χρόνου που ο κωδικός μεταδίδεται και όχι κάθε μετάδοσης του GPS. Επίσης, δεδομένου ότι δεν υπάρχει ανατροφοδότηση από τους clients GPS, ένας jammer μπορεί να είναι πολύ μακριά από τους clients στους οποίους επιτίθεται και καλύπτει εύκολα μια μεγάλη περιοχή. Ενδεικτικά, μια τυχαία επίθεση, όπως ενός υπαλλήλου που προσπαθεί να ξεγελάσει τον εργοδότη του για την τοποθεσία του, ένας μικρός jammer που λειτουργεί με 12 volts μπορεί να διαταράξει τη λειτουργία μιας υπηρεσίας όπως είναι ο έλεγχος εναέριας κυκλοφορίας σε ένα πύργο ελέγχου από έναν κύριο δρόμο που απέχει περισσότερο από δύο χιλιάδες πόδια [33].

Signal Spoofing

Ένα από τα σημαντικότερα προβλήματα των clients GPS είναι ότι αντιμετωπίζουν καλά διαμορφωμένες εισροές ως αξιόπιστες. Οι παραδοσιακές επιθέσεις Signal Spoofing μπορούν να πραγματοποιηθούν σε ένα από τα δύο συστήματα που λαμβάνουν οι clients από την είσοδο σήματος GPS. Μπορούν να επιτεθούν στο ρολόι ή μπορούν να επιτεθούν στη θέση. Η επίθεση θα προκαλέσει σφάλμα στην βασική λειτουργικότητα του client, και έτσι η πληροφορία από τον δορυφόρο θα είναι ανακριβής. Αν υπάρξει επίθεση στο χρόνο, τότε οι κύκλοι που ο client πρέπει να μετρήσει για να υπολογίσει την απόσταση θα είναι λάθος. Η θέση θα έχει τότε εσφαλμένη τιμή. Το position spoofing είναι ευκολότερο στην ανίχνευση και τη διόρθωση, αφού μια σωστή θέση θα αντικαταστήσει ένα λάθος και το ιστορικό θέσης στη συνέχεια δεν θα διατηρείται στον υπολογισμό της νέας θέσης. Με επίθεση στο χρόνο, όμως, το ιστορικό εισόδου του πελάτη από το δορυφόρο θα μπλοκάρει και θα πάρει πολλούς κύκλους για να διορθωθεί, εάν διορθωθεί καθόλου [33].

Οι απλές επιθέσεις χρησιμοποιούν προσομοιωτές GPS, οι οποίοι αποτελούν εμπορικές συσκευές που χρησιμοποιούνται για τη δοκιμή της απόδοσης των clients GPS. Οι προσομοιωτές παράγουν το σήμα L1 χρησιμοποιώντας είτε προεπιλεγμένα δεδομένα είτε ο χρήστης μπορεί να μεταφορτώσει τις προδιαγραφές ενός σήματος σε τυποποιημένη μορφή, π.χ. το Spirent χρησιμοποιεί το NMEA. Ο κύριος σκοπός των προσομοιωτών είναι οι offline δοκιμές[33].

Παράδειγμα επίθεσης σε GPS από το Πανεπιστήμιο του Τέξας

Σε ένα παράδειγμα τέτοιας επίθεσης, ερευνητές από το εργαστήριο Todd Humphreys στο Πανεπιστήμιο του Τέξας χρησιμοποιώντας signal spoofing σε GPS ήταν σε θέση να πείσουν ένα πλοίο να αλλάξει πορεία και ότι κινδύνευε. Συγκεκριμένα το ξεγέλασαν στο να νομίζει ότι το υψόμετρο του ήταν κάτω από την επιφάνεια της θάλασσας. Οι δοκιμές τους έδειξαν ότι αυτό το ψεύτικο σήμα GPS, είχε αποτέλεσμα μέχρι και τριάντα χιλιόμετρα μακριά [33].

Η χρήση πολιτικών δεκτών GPS για στρατιωτική χρήση έχει γίνει κοινή πρακτική, λόγω της ταχείας ανάπτυξης της τεχνολογίας των υπολογιστών και της μείωσης στο μέγεθος, στο βάρος και στην κατανάλωση ισχύος. Για παράδειγμα, το Garmin Fortrex 401 είναι ένας ευρέως χρησιμοποιούμενος προσωπικός δέκτης GPS για χρήση από στρατιώτες για να δημιουργεί ίχνη των περιπολιών τους ή για την αναφορά δεδομένων θέσης για διαδρομές που ακολουθούν ή περιοχές ενδιαφέροντος κλπ. Δεν είναι γνωστό αν οποιοδήποτε anti-spoof ή anti-jam ανάλυση έχει πραγματοποιηθεί γι' αυτή την τεχνολογία, ωστόσο λόγω της εμπορικής διαθεσιμότητας αυτών των συσκευών είναι λίγο απίθανο, επιτρέποντας έτσι την εξάπλωση των αδυναμιών του συστήματος και αυξάνοντας την ικανότητα των κακόβουλων παραγόντων να διεξάγουν επιθέσεις Meaconing [14].

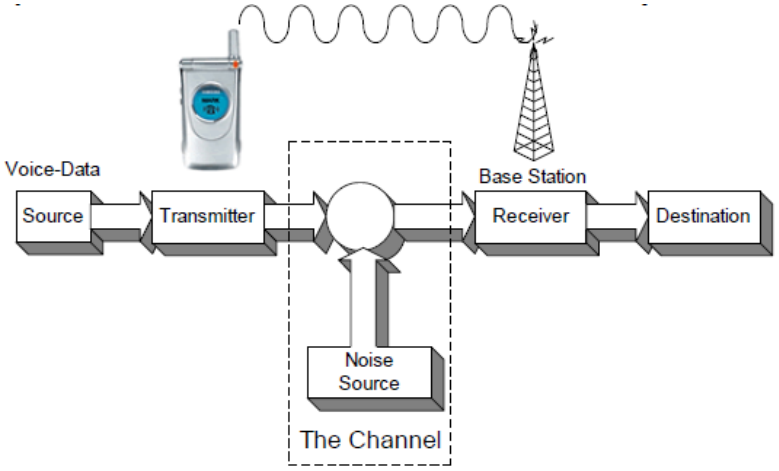
Κεφάλαιο 6
Επικοινωνία Wi-Fi

6.1 Wi-Fi

Το Wi-Fi πλέον δίνει τη δυνατότητα στις περισσότερες ηλεκτρονικές συσκευές να επικοινωνούν μεταξύ τους κάνοντας πλέον και την επικοινωνία των ανθρώπων δυνατή και εύκολη στα πιο απίθανα μέρη του πλανήτη. Όπως είπε και ο Tesla κάποτε, σε κάποια χρόνια οι άνθρωποι θα μπορούν να μεταφέρουν πληροφορίες χωρίς σύνδεση, αλλά χρησιμοποιώντας ειδικά μηχανήματα. Παράλληλα, προέβλεψε ότι χάρη στη τεχνολογία θα μπορούμε να μιλάμε και να βλέπουμε ο ένας τον άλλον ακόμη και αν δεν βρισκόμαστε στον ίδιο χώρο.

Ίσως η πιο διαδεδομένη τεχνολογία ασύρματης σύνδεσης σήμερα είναι τα πρωτόκολλα ασύρματων τεχνολογιών 802.11 τα οποία αντικαθιστούν ολοένα και περισσότερο τα ενσύρματα δίκτυα υποκαθιστώντας την λειτουργία των Ethernet.

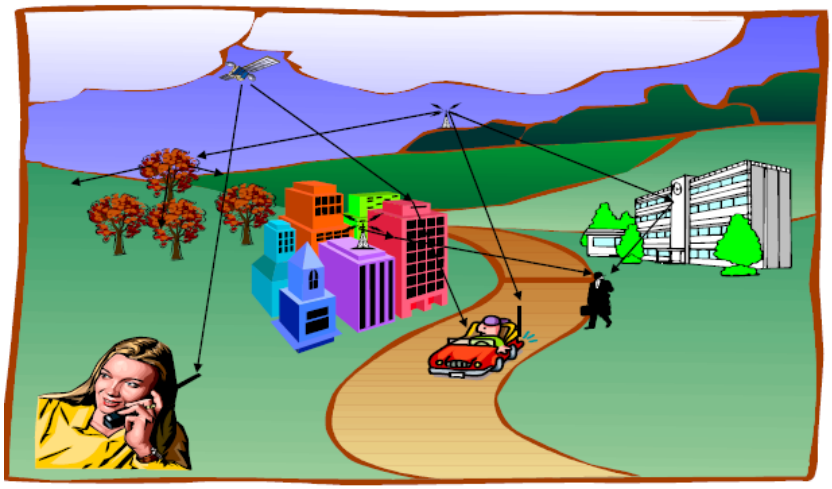
Όπως όλες οι ασύρματες συνδέσεις έτσι και το Internet βασίζεται στην αρχιτεκτονική ενός ασύρματου επικοινωνιακού συστήματος βάσει του μοντέλου που όρισε ο Shannon με τα διάφορα μέρη του. Σύμφωνα με το μοντέλο αυτό υλοποιείται η επικοινωνία μεταξύ της πηγής (source) και του προορισμού (destination) μέσω ενός διαύλου επικοινωνίας, στην περίπτωση μας ασύρματου δηλαδή με τη χρήση του ελευθέρου χώρου. Η πηγή σε ένα Wi-Fi δίκτυο αποτελεί ένα Access Point και ο προορισμός τη συσκευή του χρήστη, κινητή ή σταθερή. Η πληροφορία η οποία μεταδίδεται διαμορφώνεται ανάλογα έτσι ώστε να μπορεί να μεταδοθεί από το κανάλι και να ανακτηθεί όσο καλύτερα γίνεται στον δέκτη χωρίς όμως να μπορεί να αποφύγει τον θόρυβο που καλύπτει όλο το φάσμα και προστίθεται αναπόφευκτα σε όλα τα σήματα.



Σχήμα 6.1: Μοντέλο ενός ασύρματου επικοινωνιακού συστήματος κατά Shannon

Στο Wi-Fi όπως είπαμε ο δίαυλος επικοινωνίας αποτελεί τον ελεύθερο χώρο στον οποίο διαδίδεται το σήμα το οποίο χρησιμοποιεί του διάφορους μηχανισμούς διάδοσης βασισμένους στην κυματική ιδιότητα του Ηλεκτρομαγνητικού Κύματος σύμφωνα με την οποία συμπεριφέρεται το φως κατά τη διάδοση του. Οι μηχανισμοί αυτοί, εκτός από τη διάδοση με οπτική επαφή (Line-of-Sight) στην οποία το σήμα διαδίδεται στον ελεύθερο χωρίς εμπόδια χώρο προς ένα δέκτη με τον οποίο έχει οπτική επαφή, είναι η Ανάκλαση (Reflection), η περίθλαση (diffraction), η διάθλαση (refraction) και η σκέδαση (scattering). Η ανάκλαση επιτρέπει στο κύμα να διαδοθεί ανακλώμενο σε διαφορετικές επιφάνειες όπως έδαφος, τοίχοι, κτίρια, βουνά αλλά και την ιονόσφαιρα ανάλογα με το μήκος κύματος του σήματος. Η περίθλαση προκαλεί «καμπύλωση» στο κύμα όταν αυτό χτυπήσει σε αιχμηρές ακμές (edges) δίνοντας του τη δυνατότητα να μεταδοθεί και σε περιοχές non-Line-of-Sight. Η περίθλαση αποτελεί μηχανισμό

διάδοσης διαμέσου άλλων υλικών είτε στερεών είτε υγρών είτε αέριων αλλάζοντας του τη γωνία διάδοσης ανάλογα με το μήκος κύματος, το είδος και το πάχος του υλικού. Τέλος κατά τη σκέδαση το προσπίπτον κύμα σε επιφάνεια η οποία είναι συγκρίσιμη με το μήκος κύματος, σκεδάζεται δηλαδή σκορπίζεται σε διάφορες κατευθύνσεις.



Σχήμα 6.2: Οι διάφοροι μηχανισμοί διάδοσης ενός σήματος

Τα ασύρματα δίκτυα 802.11 είναι ευρέως διαδεδομένα και σε χρήση τόσο σε ιδιωτικούς χώρους, όσο και σε επιχειρήσεις και σε δημόσιους χώρους λόγω διαφόρων παραγόντων. Τα συγκεκριμένα δίκτυα είναι αρκετά οικονομικά έχοντας έτσι απήχηση σε όλες σχεδόν τις κοινωνικές ομάδες. Υπάρχουν πλέον πάρα πολλές συσκευές υλοποίησής αυτών των δικτύων από όλο και περισσότερες εταιρείες και η υλοποίηση τους είναι πάρα πολύ εύκολη. Έχει το πλεονέκτημα της μεταφοράς και τοποθέτησης σχεδόν παντού λόγω της απουσίας καλωδιώσεων καλύπτοντας έτσι όλο και περισσότερους χώρους. Πλεονεκτεί επίσης η τεχνολογία αυτή σε σχέση με τη ενσύρματη μεταφορά ιντερνέτ λόγω και της δυνατότητας εύκολης επέκτασης του δικτύου με τη χρήση περισσότερων Access Points χωρίς να χρειαστεί να τραβήξουμε καλώδια.

Παρ' όλα τα πλεονεκτήματα της τεχνολογία αυτής όμως παρουσιάζονται και σημαντικά μειονεκτήματα. Η ταχύτητα μετάδοσης των δεδομένων παρόλο που βελτιώνεται συνεχώς επιτυγχάνοντας πολύ μεγάλες ταχύτητες, δεν μπορεί να φτάσει τις ταχύτητες των ενσύρματων δικτύων λόγω και του μέσου μετάδοσης. Ο ελεύθερος χώρος πάντα προσθέτει θόρυβο στο σήμα μειώνοντας έτσι την ισχύ του ωφέλιμου σήματος ακολούθως το SNR και ως αποτέλεσμα το throughput. Αυτό έχει ως συνέπεια επίσης να

περιοριζόμαστε όσον αφορά την απόσταση μεταξύ πηγής και δέκτη λόγω απώλειας ελευθέρου χώρου,

6.1.1 Περιγραφή ασύρματων δικτύων 802.11 a/b/g/n/ac

Στον πιο κάτω πίνακα βλέπουμε επιγραμματικά τα διάφορα χαρακτηριστικά για το κάθε πρότυπο 802.11 για μια γενικότερη σύγκριση.

IEEE 802.11 PHY standards						
Release Date	**Standard**	**Frequency Band (GHz)**	**Bandwidth (MHz)**	**Modulation**	**Advanced Antenna Technologies**	**Maximum Data Rate**
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	N/A	11 Mbits/s
1999	802.11a	5 GHz	20 MHz	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4GHz, 5GHz	20 MHz, 40 MHz	OFDM	MIMO, up to 4 spartial streams	600 Mbits/s
2013	802.11ac	5 GHz	40 MHz, 80MHz, 160 MHz	OFDM	MIMO, MU-MIMO, up to 8 spartial streams	6.93 Gbits/s

Πίνακας 6.1: Τα χαρακτηριστικά των διαφόρων προτύπων 802.11

Πρότυπο 802.11a

Το πρότυπο 802.11a είναι το πρώτο πρότυπο από τα 802.11 και εμφανίστηκε πρώτη φορά το 1999. Δουλεύει στη ζώνη των 5 GHz συχνότητα η οποία είναι κεντρική από το εύρος στο οποίο βρίσκονται τα κανάλια του. Έχει μέγιστο ρυθμό δεδομένων 54Mbit/s με το throughput του να κυμαίνεται γύρω στα 20Mb/s. Το πρότυπο αυτό σήμερα λειτουργεί μέχρι και τις συχνότητες των 5,725GHz και χρησιμοποιεί orthogonal frequency-decision multiplexing (OFDM). Η ευρεία χρήση της μπάντας των 2,4GHz σήμερα δίνει το πλεονέκτημα στο πρότυπο 802.11a αφού αποφεύγει το θόρυβο που

δημιουργείται από τα διάφορα Access Points με την ίδια συχνότητα και έχει σαφώς καλύτερη ποιότητα σήματος και συνεπώς μεγαλύτερο throughput λόγω μικρότερων παρεμβολών.

Το μειονέκτημα αυτού του προτύπου είναι ότι λόγω υψηλότερης συχνότητας τα κύματα έχουν μικρότερη διείσδυση και απορροφούνται σε μεγαλύτερο βαθμό από τοίχους, σε σχέση με τα πρωτόκολλα με χαμηλότερη φέρουσα συχνότητα. Έτσι το μειωμένο effective range τους επιβάλλει την χρήση περισσοτέρων Access Points για την κάλυψη του χώρου από ότι σε χαμηλότερες συχνότητες.

Παρόλα αυτά το είδος της διαμόρφωσης του διευκολύνει τη διάδοση σε περιβάλλον με πολλαπλές διαδρομές όπως μεγάλα κτίρια. Επίσης έχει το πλεονέκτημα του μεγάλου αριθμού καναλιών τα οποία μειώνουν την πιθανότητα παρεμβολής από άλλα Access Points και αυξάνει την εξυπηρέτηση περισσοτέρων κινητών συσκευών χρηστών. Αυτό κάνει το συγκεκριμένο πρότυπο πιο αξιόπιστο από άλλα.

Το 802.11a λειτουργεί σε συχνότητα των 5GHz με εύρος 20MHz για κάθε κανάλι και χρησιμοποίει το φάσμα 4.915–5.825GHz. Κάθε ένα από αυτά τα φάσματα υποδιαιρούνται σε κανάλια με κεντρική συχνότητα και εύρος ζώνης.

Το 802.11a χρησιμοποιεί ένα από τα δώδεκα non-overlapping 20MHz κανάλια στα 5GHz.

Η ισχύ εκπομπής του 802.11a ανάλογα με την συχνότητα παρουσιάζεται στο πιο κάτω πίνακα.

802.11a			
Band	**Channel numbers**	**Frequency (MHz)**	**Maximum output power**
U-NII lower band 5.15 to 5.25 MHz	36	5180	40mW (2.5mW/MHz)
	40	5200	
	44	5220	
	48	5240	
U-NII middle band (5.25-5.35)	52	5260	200mW (12.5mW/MHz)
	56	5280	

	60	5300	
	64	5320	
U-NII upper band (5.725-5.825)	149	5745	800mW (50mW/MHz)
	153	5765	
	157	5785	
	161	5805	

Πίνακας 6.2: Η ισχύ εκπομπής του 802.11a

Επίσης πιο κάτω παρατηρούμε τη σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11a ανάλογα με την ισχύ του σήματος. Σύμφωνα με τον πίνακα όσο αυξάνεται το minimum sensitivity, τόσο πιο εξειδικευμένες διαμορφώσεις μπορεί να υποστηρίξει το πρότυπο με αποτέλεσμα τον υψηλότερο ρυθμό δεδομένων που μπορεί να μεταδώσει.

802.11 a/g		
Minimum Sensitivity (dBm) (20MHz Channel spacing)*	Supported Modulation	Data rate (Mb/s) (20MHz Channel spacing)*
-82	BPSK	6
-81	BPSK	9
-79	QPSK	12
-77	QPSK	18
-74	16-QAM	24
-70	16-QAM	36
-66	64-QAM	48
-65	64-QAM	54

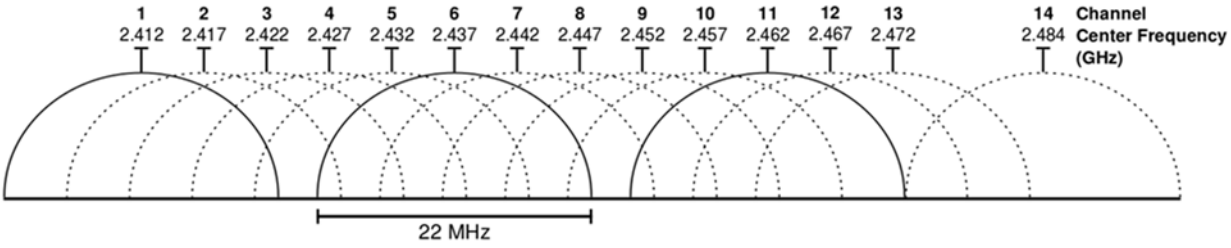
Πίνακας 6.3: Σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11a

Πρότυπο 802.11b

Το συγκεκριμένο πρότυπο δουλεύει στη συχνότητα των 2,4GHz και εμφανίστηκε πρώτη φορά στην αγορά το 2000. Ο ρυθμός μετάδοσης του είναι στα 11Mbit/s και η διαμόρφωση του χρησιμοποιεί την τεχνική του προτύπου DSSS. Το 802.11b έχει γίνει ευρέως αποδεκτό λόγω και της αύξησης στην απόδοση του και στη σημαντική μείωση στην τιμή του. Λόγω της κεντρικής του συχνότητας η οποία βρίσκεται στα 2,4GHz έχει

αυξημένη πιθανότητα παρεμβολής από άλλες συσκευές που δουλεύουν σε αυτή τη συχνότητα μειώνοντας έτσι την απόδοση του και εν συνεπεία το throughput.

Η ζώνη των 2,4GHz του προτύπου αυτού χωρίζεται σε 14 κανάλια με απόσταση 5MHz μεταξύ τους, με αρχικό το κανάλι 1 στην 2,412GHz. Τα κανάλια και οι συχνότητες τους φαίνονται στο ακόλουθο σχήμα.



Σχήμα 2.1: Η κατανομή των καναλιών στη ζώνη των 2,4 GHz του υφιστάμενου προτύπου

Η ισχύ εκπομπής του 802.11b ανάλογα με τη χώρα στην οποία χρησιμοποιείται διαφέρει λόγω διαφορετικών standards και παρουσιάζεται στο πιο κάτω πίνακα.

Maximum out power	Geographic location
1000 mW = 30dBm	USA
100 mW (EIRP) =20dBm	Europe
10 mW/MHz	Japan

Πίνακας 6.4: Η μέγιστη ισχύ εκπομπής του 802.11b

Επίσης πιο κάτω παρατηρούμε τη σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11b ανάλογα με την ισχύ του σήματος. Σύμφωνα με τον πίνακα όσο αυξάνεται το minimum sensitivity, τόσο πιο εξειδικευμένες διαμορφώσεις μπορεί να υποστηρίξει το πρότυπο με αποτέλεσμα τον μεγαλύτερο ρυθμό δεδομένων που μπορεί να μεταδώσει.

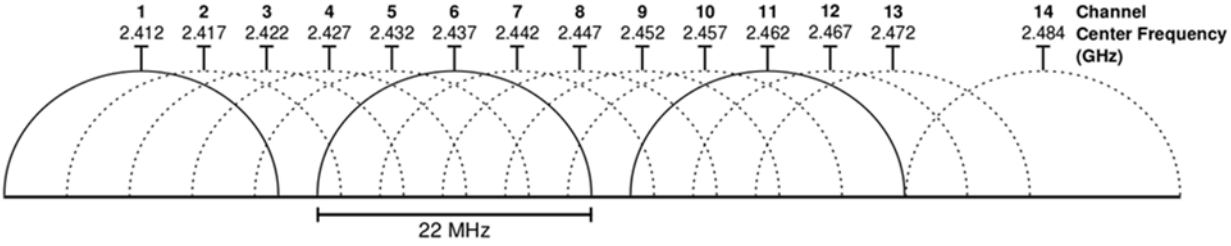
802.11 a/g		
Minimum Sensitivity (dBm) (20MHz Channel spacing)*	Supported Modulation	Data rate (Mb/s) (20MHz Channel spacing)*
-82	BPSK	6
-81	BPSK	9
-79	QPSK	12
-77	QPSK	18
-74	16-QAM	24
-70	16-QAM	36
-66	64-QAM	48
-65	64-QAM	54

Πίνακας 6.5: Σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11b

Πρότυπο 802.11g

Το πρότυπο αυτό μπήκε σε χρήση το 2003 και διαδόθηκε πολύ σύντομα λόγω του χαμηλού κόστους και των υψηλότερων ταχυτήτων που πρόσφερε. Το 802.11g λειτουργεί στη ζώνη των 2,4GHz όπως και το 802.11b και χρησιμοποιεί τη διαμόρφωση OFDM που χρησιμοποιεί και το 802.11a. Ο ρυθμός μετάδοσης του φτάνει τα 54Mbit/s και είναι συμβατό με το 802.11b. Το πρότυπο αυτό όπως και αυτά της ίδιας συχνότητας παρουσιάζει το μειονέκτημα των αυξημένων παρεμβολών λόγω της ύπαρξης συσκευών με την ίδια συχνότητα και της ευρείας χρήσης τους. Στο συγκεκριμένο πρότυπο υπάρχουν 3 μη επικαλυπτόμενα κανάλια (1,6,11) τα οποία μπορούν να χρησιμοποιηθούν σε διαφορετικά Access Points με τέτοιο τρόπο ώστε να αποφευχθούν οι παρεμβολές και να μειωθεί ο θόρυβος από κοντινές συσκευές που έχουν την ίδια συχνότητα.

Η ζώνη των 2,4GHz του προτύπου αυτού χωρίζεται σε 14 κανάλια με απόσταση 5MHz μεταξύ τους, με αρχικό το κανάλι 1 στην 2,412GHz. Τα κανάλια και οι συχνότητες τους φαίνονται στον ακόλουθο πίνακα.



Σχήμα 6.3: Η κατανομή των καναλιών στη ζώνη των 2 ,4 GHz του υφιστάμενου προτύπου

Η ισχύ εκπομπής του 802.11g ανάλογα με τη χώρα στην οποία χρησιμοποιείται διαφέρει λόγω διαφορετικών standards και παρουσιάζεται στο πιο κάτω πίνακα.

Maximum out power	Geographic location
1000 mW = 30dBm	USA
100 mW (EIRP) =20dBm	Europe
10 mW/MHz	Japan

Πίνακας 6.6: Η μέγιστη ισχύ εκπομπής του 802.11g

Επίσης πιο κάτω παρατηρούμε τη σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11g ανάλογα με την ισχύ του σήματος. Σύμφωνα με τον πίνακα όσο αυξάνεται το minimum sensitivity, τόσο πιο εξειδικευμένες διαμορφώσεις μπορεί να υποστηρίξει το πρότυπο με αποτέλεσμα τον μεγαλύτερο ρυθμό δεδομένων που μπορεί να μεταδώσει.

802.11 a/g		
Minimum Sensitivity (dBm) (20MHz Channel spacing)*	Supported Modulation	Data rate (Mb/s) (20MHz Channel spacing)*
-82	BPSK	6
-81	BPSK	9
-79	QPSK	12
-77	QPSK	18
-74	16-QAM	24
-70	16-QAM	36
-66	64-QAM	48
-65	64-QAM	54

Πίνακας 6.7: Σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11g

Πρότυπο 802.11n

Το πρότυπο 802.11n αποτελεί βελτίωση των προηγούμενων προτύπων όσον αφορά την αξιοπιστία και την απόδοση. Χρησιμοποιεί νέες τεχνολογίες οι οποίες κάνουν δυνατή τη αξιοποίηση πολλαπλών κεραιών ευρύτερων καναλιών. Οι βελτιώσεις του προτύπου αυτού επιτρέπουν την μεταφορά δεδομένων πλέον σε ταχύτητες μέχρι και 600Mbps δεκαπλασιάζοντας την ταχύτητα του προτύπου 802.11g. Η κεντρική συχνότητα λειτουργίας βρίσκεται στα 2,4 GHz αλλά και 5 GHz προαιρετικά. Βασίζεται σε προηγούμενα πρωτόκολλα με διαφορά την προσθήκη multiple–input multiple-output (MIMO) και το frame aggregation στο Media Access Control (MAC) επίπεδο.

Το μεγαλύτερο πλεονέκτημα του που το κάνει να ξεχωρίζει είναι η δυνατότητα του να χρησιμοποιεί πολλαπλές κεραίες για εκπομπή και λήψη με συνδυασμό κεραιών "MXN" από "1X1" έως "4X4".

Η τεχνολογία αυτή που ονομάζεται MIMO χρησιμοποιεί πολλαπλές κεραίες για να μεταφέρει περισσότερες πληροφορίες κάτι το οποίο επιτυγχάνεται με τη χρήση Spatial Division Multiplexing η οποία μεταφέρει ταυτόχρονα σε ένα κανάλι (spectral channel of bandwidth) πολλαπλές ροές δεδομένων (spatially multiplexes multiple independent data streams). Αυτό βελτιώνει την απόδοση του συστήματος καθώς αυξάνονται και τα spatial data streams.

Ένα άλλο χαρακτηριστικό του 802.11n είναι ότι οι συσκευές των 802.11n έχουν τη δυνατότητα να χρησιμοποιούν 20 ή 40MHz εύρους καναλιών. Αυτά τα κανάλια μπορούν να διαχωρίζονται είτε στη λειτουργία των 2,4GHz είτε των 5GHz.

Ο μέγιστος ρυθμός μετάδοσης δεδομένων στο πρότυπο αυτό φτάνει τα 495 Mbit/s, με την χρήση 4 MIMO streams.

Η ζώνη των 2,4GHz χωρίζεται σε 14 κανάλια σε απόσταση 5GHz μεταξύ τους, αρχίζοντας με τα κανάλια 1, η οποία επικεντρώνεται στην 2,412GHz.

Η ισχύ εκπομπής του 802.11n ανάλογα με τη χώρα στην οποία χρησιμοποιείται διαφέρει λόγω διαφορετικών standards και παρουσιάζεται στο πιο κάτω πίνακα.

Maximum out power	Geographic location
1000 mW = 30dBm	USA
100 mW (EIRP) =20dBm	Europe
10 mW/MHz	Japan

Πίνακας 6.8: Η μέγιστη ισχύ εκπομπής του 802.11n

Η μέγιστη επιτρεπόμενη ισχύς εξόδου για την πάντα 5GHz, σύμφωνα τα πρότυπα που εφαρμόζονται για την Ευρώπη στο πρότυπο 802.11n, παρουσιάζεται στον παρακάτω πίνακα.

802.11n Europe			
Band	**Channel numbers**	**Frequency (MHz)**	**Maximum output power**
5170 MHz - 5330 MHz	36	5180	20mW
	40	5200	
	44	5220	
	48	5240	
	52	5260	
	56	5280	
	60	5300	
	64	5320	
5490 MHz – 5710 MHz	100	5500	1000mW
	104	5520	
	108	5540	
	112	5560	
	116	5580	
	120	5600	
	124	5620	
	128	5640	
	132	5660	
	136	5680	
	140	5700	

Πίνακας 6.9: Η Η μέγιστη ισχύ εκπομπής του 802.11n

Επίσης πιο κάτω παρατηρούμε τη σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11n ανάλογα με την ισχύ του σήματος. Σύμφωνα με τον πίνακα όσο αυξάνεται το minimum sensitivity, τόσο πιο εξειδικευμένες διαμορφώσεις μπορεί να υποστηρίξει το πρότυπο με αποτέλεσμα τον μεγαλύτερο ρυθμό δεδομένων που μπορεί να μεταδώσει αλλά και coding rate.

802.11 n								
Minimum Sensitivity (dBm) (20MHz Channel spacing)	Minimum Sensitivity (dBm) (40MHz Channel spacing)	MCS index	Supported Modulation	Coding Rate (R)	Data Rate* (Mb/s) Guard Interval GI=800ns		Data rate* (Mb/s) Guard Interval GI=400ns	
					20MHz Channel	40MHz channel	20MHz channel	40MHz channel
-82	-79	0	BPSK	1/2	6.5	13.5	7.2	15.0
-79	-76	1	QPSK	1/2	13.0	27.0	14.4	30.0
-77	-74	2	QPSK	3/4	19.5	40.5	21.7	45.0
-74	-71	3	16-QAM	1/2	26.0	54.0	28.9	60.0
-70	-67	4	16-QAM	3/4	39.0	81.0	43.3	90.0
-66	-63	5	64-QAM	2/3	52.0	108.0	57.8	120.0
-65	-62	6	64-QAM	3/4	58.5	121.5	65.0	135.0
-64	-61	7	64-QAM	5/6	65.0	135.0	72.2	150.0

Πίνακας 6.10: Σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11n

Πρότυπο 802.11ac

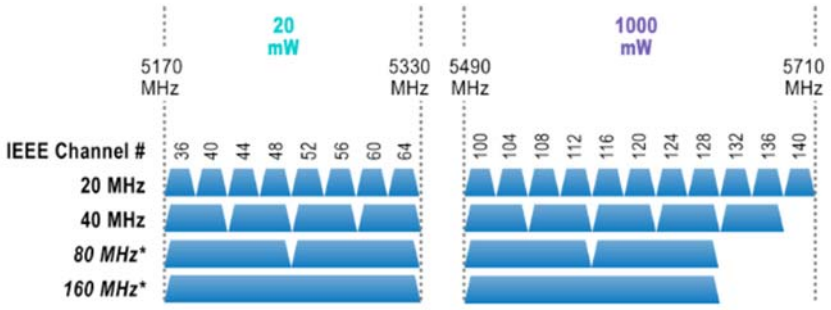
Το IEEE 802.11ac (γνωστός και ως VHT, Very High Throughput) δουλεύει στην μπάντα των 5GHz. Βασίζεται στα χαρακτηριστικά του 802.11n και 802.11a κάνοντας το έτσι συμβατό με παλαιότερες τεχνολογίες.

Το πρότυπο αναπτύχθηκε από το 2011 μέχρι το 2013 και τελικά κυκλοφόρησε το 2014. Οι συσκευές 802.11ac υποστηρίζουν κανάλια με εύρος ζώνης 20, 40, και 80MHz και ένα spatial stream.

Οι 802.11ac συσκευές με χρήση παραμέτρων 80 MHz bandwidth, 1 spatial stream, και 64-QAM 5/6 έχουν ρυθμό μετάδοσης δεδομένων περίπου 293 Mbps. Οι συσκευές με χρήση παραμέτρων 8 spatial streams, 160 MHz bandwidth και 256-1QAM 5/6 με short guard interval μπορούν να φτάσουν το ρυθμό δεδομένων των 7 Gbps.

Η μπάντα των 5GHz στο πρότυπο 802.11ac έχει 24 μη επικαλυπτόμενα κανάλια με εύρος ζώνης 20MHz. Λόγω κινδύνου παρεμβολών στο πρότυπο αυτό χρησιμοποιούνται μόνο τα 4 αρχικά και τα 5 τελευταία κανάλια. Για να μπορούν να χρησιμοποιηθούν τα 15 μεσαία κανάλια θα πρέπει το wireless router να υποστηρίζει την τεχνολογία Dynamic Frequency Selection (DFS), η οποία εφαρμόζεται συνήθως σε συνδυασμό με έλεγχο ισχύος μετάδοσης (Transmit Power Control (TPC)). Η τεχνολογία DFS επιτρέπει σε μια ασύρματη συσκευή να εντοπίζει την παρουσία radar που δουλεύει στο κανάλι που χρησιμοποιείται και εάν η ισχύς είναι πάνω από ένα threshold, μετακινείται σε άλλο κανάλι.

Στο ακόλουθο σχεδιάγραμμα παρατηρούμε την κατανομή των καναλιών στην Ευρώπη σύμφωνα με το συγκεκριμένο πρότυπο για εύρος καναλιών 20MHz, 40MHz, 80MHz, 160MHz.



Σχήμα 6.4: Η κατανομή των καναλιών στη ζώνη των 5 GHz του υφιστάμενου προτύπου

Η ισχύ εκπομπής του 802.11ac ανάλογα με τη χώρα στην οποία χρησιμοποιείται διαφέρει λόγω διαφορετικών standards και παρουσιάζεται στο πιο κάτω πίνακα.

Maximum out power	Geographic location
1000 mW = 30dBm	USA
100 mW (EIRP) =20dBm	Europe
10 mW/MHz	Japan

Πίνακας 6.11: Η μέγιστη ισχύ εκπομπής του 802.11ac

802.11ac Europe			
Band	**Channel numbers**	**Frequency (MHz)**	**Maximum output power**
5170 MHz - 5330 MHz	36	5180	20mW
	40	5200	
	44	5220	
	48	5240	
	52	5260	
	56	5280	
	60	5300	
	64	5320	
5490 MHz – 5710 MHz	100	5500	1000mW
	104	5520	
	108	5540	
	112	5560	
	116	5580	
	120	5600	
	124	5620	
	128	5640	
	132	5660	
	136	5680	
	140	5700	

Πίνακας 6.12: Η μέγιστη επιτρεπόμενη ισχύς εξόδου, σύμφωνα τα πρότυπα που εφαρμόζονται για την Ευρώπη στο πρότυπο 802.11ac

Επίσης πιο κάτω παρατηρούμε τη σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11ac ανάλογα με την ισχύ του σήματος. Σύμφωνα με τον πίνακα όσο αυξάνεται το minimum sensitivity, τόσο πιο εξειδικευμένες διαμορφώσεις μπορεί να υποστηρίξει το πρότυπο με αποτέλεσμα τον μεγαλύτερο ρυθμό δεδομένων που μπορεί να μεταδώσει αλλά και coding rate.

Minimum Sensitivity (dBm) (20MHz Channel spacing)	Minimum Sensitivity (dBm) (40MHz Channel spacing)	Minimum Sensitivity (dBm) (80MHz Channel spacing)	Minimum Sensitivity (dBm) 80+80MHz Channel spacing)	MCS index	Supported Modulation	Coding Rate (R)
-82	-79	-76	-73	0	BPSK	1/2
-79	-76	-73	-70	1	QPSK	1/2
-77	-74	-71	-68	2	QPSK	3/4
-74	-71	-68	-65	3	16-QAM	1/2
-70	-67	-64	-61	4	16-QAM	3/4
-66	-63	-60	-57	5	64-QAM	2/3
-65	-62	-59	-56	6	64-QAM	3/4
-64	-61	-58	-55	7	64-QAM	5/6
-59	-56	-53	-50	8	256-QAM	3/4
-57	-54	-51	-48	9	256-QAM	5/6

Πίνακας 6.13: Σχέση received power (minimum sensitivity), υποστηριζόμενης διαμόρφωσης και data rate (wireless link rate) στο 802.11ac

Κεφάλαιο 7
Μεθοδολογία

7.1 Περιγραφή Συστήματος-Στόχου

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, ο σκοπός της διατριβής αυτής είναι να επιβεβαιώσει την υπόθεση ότι δεν υπάρχει λόγος να χρησιμοποιηθούν «θανάσιμα»-καταστροφικά μέσα εξάλειψης για την υπεράσπιση ορισμένων περιμέτρων και εγκαταστάσεων, αρκεί να αποτραπεί ο χειριστής του μη επανδρωμένου αεροχήματος-drone από το να ολοκληρώσει τη διαδικασία της καθοδήγησης του drone στο στόχο, διακόπτοντας τον σήμα ελέγχου από και προς το drone κατά την τελική φάση καθοδήγησης. Πιο απλά, για να επιτευχθεί ο στόχος διατήρησης της ασφάλειας των περιοχών που θέλουμε να προστατέψουμε, δεν χρειάζεται να χρησιμοποιηθούν μέσα και εξοπλισμός που να καταστρέψει ή να προκαλέσει ζημιές σε ένα drone που καθοδηγείται με ύποπτες ή εχθρικές διαθέσεις. Μπορούμε να επιτύχουμε το στόχο μας διακόπτοντας την επικοινωνία με το χειριστή του και να το αναγκάσουμε να προσγειωθεί με ασφάλεια στο έδαφος για περισυλλογή.

Σε αυτό το μέρος της Διατριβής θα παρουσιαστεί όλη η μεθοδολογία σχεδιασμού και ανάπτυξης του συστήματος για επίτευξη του προαναφερθέντος στόχου το οποίο εκτός από αποτελεσματικό, θα είναι και φθηνό αφού θα αποτελείται από κοινά ηλεκτρονικά στοιχεία που βρίσκονται διαθέσιμα στην αγορά.

7.1.1 Στόχος-Target

Κατ' αρχάς πρέπει να αναφερθούμε στο drone το οποίο θα αποτελέσει στόχο για δοκιμή και επιβεβαίωση της λειτουργικότητας του συστήματος απενεργοποίησης. Το Phantom της κινέζικης εταιρείας DJI, η οποία έχει συνδέσει το όνομα της με την παραγωγή quadcopters drones, αποτελεί ένα από τα πιο γνωστά και πιο διαδεδομένα drones τόσο στο design όσο και στην ευρεία χρήση του παγκόσμια. Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, το συγκεκριμένο drone μπορεί να τύχει χειρισμού χρησιμοποιώντας ένα smartphone ή ένα Wi-Fi control, μπορεί να πετάξει περίπου στα 54 Km/h και μπορεί να λειτουργήσει για περίπου 25 λεπτά. Τα στοιχεία που μας ενδιαφέρουν κυρίως γι' αυτό το drone είναι ο τρόπος πλοήγησης και επικοινωνίας του με το χειριστή, σημεία στα οποία στοχεύουμε για να το απενεργοποιήσουμε.

Το Phantom λοιπόν, είναι γνωστό ότι επικοινωνεί και καθοδηγείται από το χειριστή του μέσω Wi-Fi control στη μπάντα των 2,4GHz. Επίσης χρησιμοποιεί τη μπάντα L1 του συστήματος προσδιορισμού θέσης GPS στη συχνότητα των 1575MHz με σκοπό να μεταβαίνει αυτόνομα σε μια προκαθορισμένη θέση που δόθηκε από το χρήστη ή να επιστρέφει πίσω στην αρχική του θέση σε περίπτωση που διακοπεί η επικοινωνία του με τον χειριστή.

7.1.2 Jammer

Με δεδομένα τα πιο πάνω και για να μπορεί το σύστημα απενεργοποίησης να είναι αποτελεσματικό θα πρέπει να έχει τις εξής δύο δυνατότητες: Α) Να απενεργοποιεί τον χειρισμό του drone από το control και Β) να διακόπτει την λήψη του σήματος GPS από το δορυφόρο. Εκτελώντας αυτές τις δύο λειτουργίες το σύστημα μας, θα αναγκάσει το drone να σταματήσει τη πτήση και να προσγειωθεί στο σημείο που βρίσκεται όπου στη συνέχεια μπορούμε να το μαζέψουμε.

Το σύστημα που θα κατασκευαστεί θα αποτελείται από 2 band jammers στεγασμένα σε μια ενιαία κατασκευή και τα οποία θα δουλεύουν ταυτόχρονα. Το κάθε band jammer θα στοχεύει σε

μια ασύρματη λειτουργία του drone και θα έχει τη δική του κεραία. Όλα τα ηλεκτρονικά στοιχεία που θα χρησιμοποιηθούν θα έχουν την ίδια πηγή τροφοδοσίας για εξοικονόμηση πόρων και χώρου. Το RF κύκλωμα που θα κατασκευαστεί θα στοχεύει στη δημιουργία σήματος παρεμβολής με τη χρήση VCOs το οποίο θα ενισχύεται από Power Amplifiers στην έξοδο και θα κατευθύνεται μέσω κατευθυντικής κεραίας προς το drone στοχεύοντας στη διακοπή της επικοινωνίας με το ωφέλιμο σήμα. Εκτενέστερη θεωρητική επεξήγηση θα γίνει σε επόμενο κεφάλαιο κατά την ανάπτυξη του συστήματος.

Συγκεκριμένα τα σύστημα θα αποτελείται από τα ακόλουθα μέρη:

Τροφοδοσία: Όλα τα υλικά που θα χρησιμοποιηθούν λειτουργούν με συνεχή τάση 5V και η μέγιστη κατανάλωση ρεύματος που απαιτείται είναι 2A. Γι' αυτό το λόγο ως τροφοδοσία θα χρησιμοποιηθεί Power Bank με 2 εξόδους, η μια στα 5V-1A και η άλλη στα 5V-2,4A. Με αυτό τον τρόπο διασφαλίζεται η τροφοδοσία του συστήματος με συνεχή τάση αλλά και η κινητικότητα του συστήματος.

Κύκλωμα RF: Το κύκλωμα RF θα αποτελείται από 2 VCOs όπως προαναφέρθηκε, κάθε ένας από τους οποίους θα δημιουργεί ένα RF σήμα στην έξοδο του, το οποίο θα επικεντρώνεται στην επιθυμητή μπάντα που θέλουμε να παρεμβάλουμε. Για τη δημιουργία του tuning signal για κάθε VCO, θα χρησιμοποιηθεί μια μικρή γεννήτρια σήματος με δυνατότητα δύο καναλιών ταυτόχρονα στην έξοδο, η οποία θα τροφοδοτείται από το Power Bank ξεχωριστά από το υπόλοιπο κύκλωμα λόγω της μεγάλης κατανάλωσης που απαιτεί. Το tuning signal θα δημιουργηθεί σε λογισμικό που συνοδεύει τη συσκευή και θα αποθηκευτεί στη γεννήτρια για άμεση χρήση. Στην έξοδο των VCOs το σήμα που θα παραχθεί θα οδηγείται μέσω attenuator στον Power Amplifier ο οποίος θα το ενισχύει και μέσω καλωδίου θα οδηγείται στην αντίστοιχη κατευθυντική κεραία, για κάθε μπάντα, για εκπομπή.

Κεραίες: Οι κεραίες που θα χρησιμοποιηθούν θα είναι κατευθυντικές και θα αντιστοιχούν στην μπάντα που θέλει να παρεμβάλει η κάθε μια. Επίσης θα έχουν υψηλό Gain έτσι ώστε το σήμα πριν εκπεμφθεί στον χώρο να έχει ενισχυθεί αρκετά για να είναι όσο το δυνατό πιο αποτελεσματικό.

Όλα τα πιο πάνω θα στεγαστούν σε μια μικρή ξύλινη, αυτοσχέδια, φορητή συσκευή, τόσο για προστασία όσο και για την εύκολη μεταφορά και χρήση του συστήματος.

Στο κεφάλαιο της ανάπτυξης του συστήματος θα γίνει εκτενέστερη παρουσίαση και περιγραφή των πιο πάνω στοιχείων του συστήματος.

7.2 Βήματα

Για την διασφάλιση και επαλήθευση της λειτουργικότητας και αποτελεσματικότητας του συστήματος jammer θα πρέπει να ακολουθηθεί μια μεθοδολογία η οποία σε κάθε στάδιο της θα ελέγχει την ικανότητα και τις δυνατότητες των διαφόρων τμημάτων του συστήματος έτσι ώστε αν το αποτέλεσμα δεν είναι ικανοποιητικό, να μπορούν να προσδιοριστούν οι ελλείψεις, τα λάθη ή τυχών παραλείψεις που έγιναν κατά την κατασκευή.

Αρχικά θα πρέπει να στηθεί εργαστήριο με όλα τα απαραίτητα υλικά και εργαλεία που απαιτούνται για την κατασκευή. Εκτός από τα επιμέρους ηλεκτρονικά στοιχεία που απαρτίζουν το σύστημα, χρειάζονται καλώδια, πλακέτες PCB, χάλκινα strips, αυτόματη κόλλα, καλάι και κολλητήρι, κολλητική ταινία, βάση στερέωσης με φακό και φανάρι, πολύμετρο, cutters, απογυμνωτές καλωδίων και άλλα εργαλεία για ηλεκτρονικές κατασκευές. Χρειάζονται επίσης συσκευές όπως επιτραπέζιο τροφοδοτικό, spectrum analyzer, oscilloscope, γεννήτρια συχνοτήτων.

Το βασικό κομμάτι του συστήματος θα αποτελείται από την πλακέτα με τους δύο VCOs. Άρα στα πρώτα βήματα θα πρέπει:

- Να κολληθεί πρώτα ο ένας VCO πάνω στην πλακέτα και να ελεγχθεί με ένα πολύμετρο ότι οι επαφές του εκεί που πρέπει δεν παρουσιάζουν short circuit.

- Στην έξοδο του VCO να εφαρμοστεί RF connector.

- Στην συνέχεια, με οδηγό πάντα το sheet του VCO, τροφοδοτούμε με το κατάλληλο Vcc στην αντίστοιχη επαφή του VCO και με tuning signal επιτρεπόμενου εύρους τάσης, από τη γεννήτρια σήματος στην επαφή Vtune.

- Παίρνουμε ακολούθως το RF σήμα από την έξοδο του VCO και το οδηγούμε με καλώδιο RF στο spectrum analyzer με σκοπό την επιβεβαίωση της δημιουργίας του σήματος που χαρακτηρίζει τον VCO.

- Στη συνέχεια ακολουθούμε τα ίδια βήματα ακριβώς και για τον VCO της δεύτερης μπάντας ο οποίος συγκολλείται πάνω στην ίδια πλακέτα απέναντι από τον άλλο.

Μετά την επιβεβαίωση της παραγωγής των σημάτων τα οποία επιθυμούμε, προχωρούμε στην δοκιμή σε τοπικό ιδιωτικό δίκτυο Wi-Fi, εφαρμόζοντας μικρή κεραία εκπομπής στα 2,4GHz στην έξοδο του αντιστοίχου VCO και εκπέμποντας μόνο με την ισχύ εξόδου του VCO σε κοντινή απόσταση από το τοπικό Access Point. Με την εκπομπή στοχεύουμε στην ελαχιστοποίηση ή ακόμα και διακοπή της επικοινωνίας σύνδεσης ενός δέκτη όπως αυτή ενός smartphone με το Access Point. Αυτό θα επιτευχθεί μειώνοντας το SNR αφού προστίθεται το σήμα-θόρυβος που δημιουργούμε στον VCO αναγκάζοντας τη σύνδεση να αλλάξει τη διαμόρφωση της σε χαμηλότερο throughput ή αν είναι δυνατόν να τη διακόψει τελείως.

Αν το αποτέλεσμα δεν είναι ικανοποιητικό, μειώνουμε την απόσταση του σήματος παρεμβολής με το δέκτη για να επιβεβαιώσουμε ότι το πρόβλημα είναι θέμα ισχύος το οποίο μπορεί να ξεπεραστεί με άλλους τρόπους που θα αναφερθούν παρακάτω.

Αφού επιτευχθεί η διακοπή επικοινωνίας σε δίκτυο Wi-Fi προχωρούμε με την ίδια διαδικασία στοχεύοντας σε σύνδεση GPS. Αυτό μπορεί να επιτευχθεί εύκολα με την στόχευση σε smartphone το οποίο προσπαθεί να τρέξει εφαρμογή προσδιορισμού θέσης. Αν η μπάντα του GPS στην οποία στοχεύουμε είναι η σωστή τότε πολύ εύκολα η σύνδεση θα διακοπεί λόγω και της πολύ χαμηλής ισχύς του σήματος GPS που φθάνει σε ένα επίγειο δέκτη.

Μετά την επιτυχή δοκιμή σε δίκτυα Wi-Fi και GPS σε κλειστό χώρο, προχωρούμε στις πρώτες δοκιμές στον πραγματικό στόχο. Το drone DJI Phantom. Αυτό το κομμάτι στοχεύει σε δύο πράγματα. Πρώτον, την επιβεβαίωση της δυνατότητας του συστήματος να αποκόπτει τις επικοινωνίες του στόχου από το χειριστή του και δεύτερον, τον προσδιορισμό της απαιτούμενης ενίσχυσης του εκπεμπόμενου σήματος μέσω της πρόσθεσης αναγκαίου αριθμού Power Amplifiers στο σύστημα ή πρόσθεση του απαιτούμενου noise signal στο σήμα εισόδου. Για να γίνει αυτό ακολουθούμε τα πιο κάτω βήματα:

- Κατ' αρχάς τοποθετούμε στο σύστημα τις κατάλληλες κεραίες που σκοπεύουμε να χρησιμοποιήσουμε με το επιθυμητό κέρδος.

- Ενεργοποιούμε το Jammer και στοχεύουμε στο drone το οποίο βρίσκεται ακριβώς μπροστά μας σε ελάχιστη απόσταση. Ο χειριστής του βρίσκεται και αυτός πολύ κοντά. Σκοπός είναι το drone να χάσει την επικοινωνία και να προσγειωθεί μπροστά μας.

- Αν επιτευχθεί ο στόχος, τότε απομακρυνόμαστε με το Jammer σταδιακά από το drone μέχρι αποτυχίας του συστήματος.

- Αν η απόσταση είναι ικανοποιητική όπως θα καθοριστεί, τότε ο σκοπός μας έχει επιτευχθεί και το σύστημα μας είναι αποτελεσματικό και ολοκληρωμένο χωρίς να απαιτούνται άλλοι ενισχυτές στο σήμα.

- Αν δεν μας ικανοποιεί η απόσταση, προσθέτουμε αρχικά noise signal στην είσοδο του VCO διαφόρων εντάσεων. Δοκιμάζουμε διάφορους συνδυασμούς κυματομορφών προσπαθώντας να βελτιώσουμε την ισχύ του Jammer μέσω της συνολικής μείωσης του SNR.

- Ακολούθως αν ακόμα χρειαζόμαστε περεταίρω ενίσχυση προσθέτουμε στην έξοδο των VCOs, Power Amplifiers για προενίσχυση του σήματος εκπομπής πριν οδηγηθεί στην κεραία.

- Συνεχίζουμε με την ίδια τακτική προσθέτοντας αν απαιτούνται επιπλέον Amplifiers σε σειρά μέχρι να φτάσουμε στο επιθυμητό αποτέλεσμα.

Η εφαρμογή της πιο πάνω μεθοδολογία υλοποίησης της ανάπτυξης του συστήματος, περιγράφεται στο επόμενο κεφάλαιο βήμα-βήμα όπου γίνεται επεξήγηση και εκτενέστερη παρουσίαση των επιμέρους τμημάτων με τη βοήθεια εικόνων αλλά και βάση της θεωρίας Ασύρματων Επικοινωνιών.

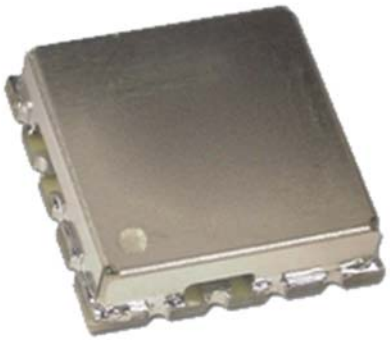
Κεφάλαιο 8
Ανάπτυξη Συστήματος

8.1 Υλικά-Εξαρτήματα

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, το RF κύκλωμα θα αποτελείται από 2 VCOs, κάθε ένας από τους οποίους θα παράγει το σήμα που θα παρεμβάλει την αντίστοιχη μπάντα στην οποία στοχεύουμε. Ο στόχος (target) που θα απενεργοποιήσουμε όπως προαναφέραμε χρησιμοποιεί δύο μπάντες συχνοτήτων για την καθοδήγηση και πλοήγηση του. Η μια στα 2,4GHz για την επικοινωνία με το χειριστή και η δεύτερη στη μπάντα L1 του GPS στη συχνότητα των 1575MHz. Στο εμπόριο υπάρχουν αρκετοί και φθηνοί VCOs διαφόρων γνωστών εταιρειών κατασκευής ηλεκτρονικών στοιχείων οι οποίοι συνοδεύονται από το φυλλάδιο χαρακτηριστικών (specifications sheet) το οποίο παρέχει όλες τις απαραίτητες πληροφορίες για τα χαρακτηριστικά, την απόδοση, το σχεδιασμό και άλλα πολύ χρήσιμα στοιχεία για τη σωστή χρήση τους. Επιλέξαμε λοιπόν τους δύο πιο κάτω VCOs.

8.1.1 Voltage Controlled Oscillator-VCO 1200-2300

Ο πρώτος VCO μπορεί να παράξει με την είσοδο του αντίστοιχου σήματος, συχνότητες από 1200-2300MHz. Το σήμα εισόδου στο VCO που απαιτείται για τη δημιουργία αυτών των συχνοτήτων, κυμαίνεται από 0.5-20VDC. Η τροφοδοσία του είναι γύρω στα 5VDC και η μέγιστη ένταση ρεύματος στα 25 mA. Το φορτίο του έχει impedance 50Ω και η ισχύς του σήματος στην έξοδο είναι 4 dBm typical με μέγιστη τα 8 dBm. Αποτελείται από 16 pins, εκ των οποίων τα 13 συνδέονται με επαφή Ground και τα υπόλοιπα 3, εκ των οποίων τα 2 είναι pins εισόδου και το ένα εξόδου, συνδέονται με την παροχή Vcc και το Vtune και στο pin εξόδου (RF out) το connector για τη συλλογή του σήματος που παράχθηκε στο VCO. Όπως γίνεται εύκολα αντιληπτό, ο συγκεκριμένος VCO θα χρησιμοποιηθεί για τη δημιουργία σήματος παρεμβολής για τη μπάντα L1 των 1575MHz του GPS.



Εικόνα 8.1: Voltage Controlled Oscillator-VCO 1200-2300MHz

8.1.2 Voltage Controlled Oscillator-VCO 2328-2536

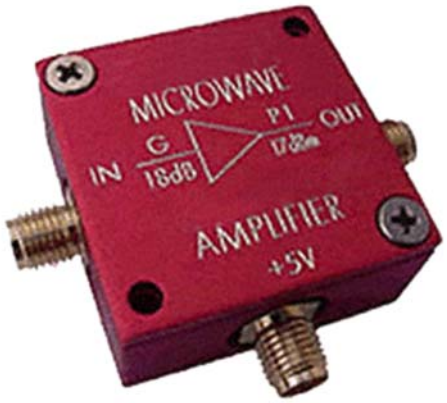
Ο δεύτερος VCO μπορεί να παράξει με την είσοδο του αντίστοιχου σήματος, συχνότητες από 2328-2536MHz. Το σήμα εισόδου στο VCO που απαιτείται για τη δημιουργία αυτών των συχνοτήτων, κυμαίνεται από 0.5-4.5VDC. Η τροφοδοσία του είναι γύρω στα 5VDC και η μέγιστη ένταση ρεύματος στα 35mA με typical τα 20mA. Το φορτίο του έχει impedance 50Ω και η ισχύς του σήματος στην έξοδο είναι 7 dBm typical με μέγιστη τα 9 dBm. Αποτελείται από 16 pins, εκ των οποίων τα 13 συνδέονται με επαφή Ground και τα υπόλοιπα 3, εκ των οποίων τα 2 είναι pins εισόδου και το ένα εξόδου, συνδέονται με την παροχή Vcc και το Vtune και στο pin εξόδου (RF out) το connector για τη συλλογή του σήματος που παράχθηκε στο VCO. Το εύρος λειτουργίας του συγκεκριμένου VCO μας δίνει τη δυνατότητα να τον χρησιμοποιήσουμε για την μπάντα των 2,4GHz στην οποία επικοινωνεί ο χρήστης με το drone μέσω του control.

Εικόνα 8.2: Voltage Controlled Oscillator-VCO 2328-2536MHz

Το σήμα που θα παραχθεί στον κάθε VCO, πριν οδηγηθεί στην κεραία για εκπομπή μπορούμε να το ενισχύσουμε με τη χρήση Power Amplifier του οποίου η είσοδος θα συνδεθεί στην έξοδο του VCO και η έξοδος του στην είσοδο της κεραίας. Για το σκοπό αυτό επιλέξαμε τον πιο κάτω ενισχυτή.

8.1.3 Broadband Low-Noise Amplifier

Ο συγκεκριμένος ενισχυτής αποτελεί ένα low-noise ενισχυτή γενικής χρήσης ο οποίος καλύπτει ένα ευρύ φάσμα συχνοτήτων, από 100-6000MHz. Έχει στις 3 πλευρές του 3 SMA connectors τόσο για την είσοδο σήματος, όσο και για την έξοδο αλλά και την τροφοδοσία του. Η τροφοδοσία του είναι στα 5VDC με κατανάλωση στα 60mA. Το κέρδος του είναι στα 18dB με ισχύ εξόδου 17dBm (P1dB). Το typical noise figure του είναι στα 3.5dB με IP3 30dBm. Επίσης σύμφωνα με τα διαγράμματα λειτουργίας που υπάρχουν στο specifications sheet, το κέρδος στην έξοδο φτάνει στα 18dB στις συχνότητες που μας ενδιαφέρουν και επίσης η ισχύς του σήματος στην έξοδο του είναι από 16dBm-16.7dBm στις μπάντες των 2.4GHz και 1.5GHz αντίστοιχα. Σημαντικό είναι επίσης και το γεγονός ότι το VSWR δεν ξεπερνά το 1.7 στα 2.4GHz ενώ στα 1.5GHz περιορίζεται περίπου στο 1.4.



Εικόνα 8.3: Broadband Low-Noise Amplifier

Για την προσαρμογή της impedance στο κύκλωμα έτσι ώστε να διατηρηθεί το VSWR κοντά στο 1, χρησιμοποιούμε SMA Fixed Attenuators των 50Ω. Για το συγκεκριμένο κύκλωμα χρησιμοποιούμε 2 Attenuators, κάθε ένα μεταξύ της εξόδου του VCO και της εισόδου του ενισχυτή, του πιο κάτω τύπου.

8.1.4 Coaxial SMA Fixed Attenuator

Ο συγκεκριμένος Attenuator έχει Impedance 50Ω με εξασθένιση 5dB, 1Watt rating και καλύπτει ένα μεγάλο εύρος συχνοτήτων, μέχρι τα 6 GHz. Οι συνδέσεις του είναι male SMA από τη μια πλευρά και female SMA από την άλλη.

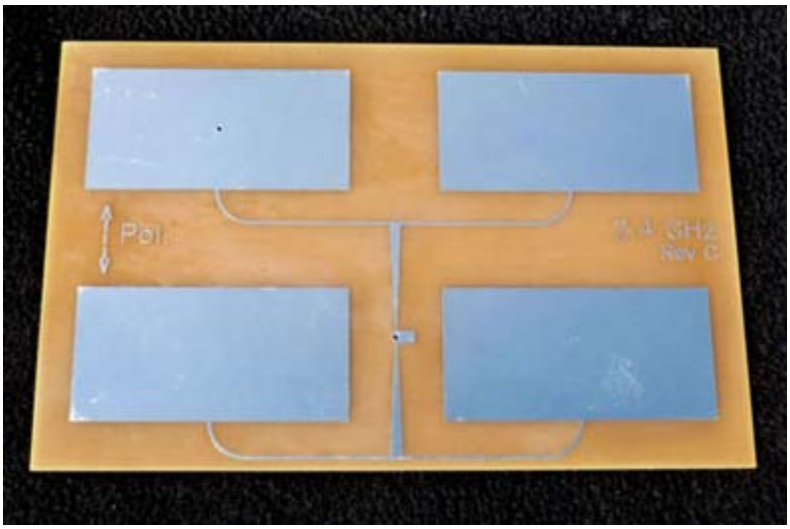
Εικόνα 8.4: Coaxial SMA Fixed Attenuator

Η εκπομπή των σημάτων στο χώρο θα γίνει όπως αναφέρθηκε και πριν με τη χρήση δύο κατευθυντικών κεραιών οι οποίες δουλεύουν στις 2 μπάντες συχνοτήτων που στοχεύουμε. Οι δύο αυτές κεραίες προσαρμόζονται στην έξοδο των ενισχυτών και με το κέρδος που έχει η κάθε

μια, ενισχύουν το σήμα αυξάνοντας την εμβέλεια και εν γένει την αποτελεσματικότητα του συστήματος. Για το λόγο αυτό θα χρησιμοποιηθούν οι 2 πιο κάτω κεραίες.

8.1.5 Broad Band 2400-2480 MHz Quad Patch

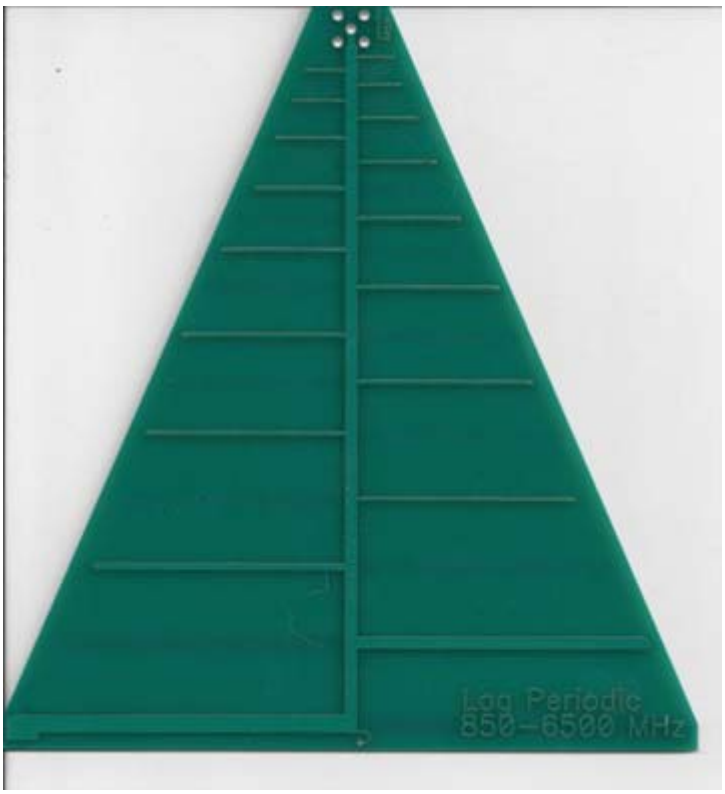
Η κεραία αυτή αποτελεί μια τύπου Patch κεραία η οποία είναι κατασκευασμένη για μέγιστη απόδοση στα 2.4-2.48GHz, η οποία και θα χρησιμοποιηθεί όπως είναι λογικό για την μπάντα χειρισμού του drone στα 2.4GHz. Έχει υψηλό κέρδος στα 11-12dBi και δυνατότητα εφαρμογής coaxial sma cable. Έχει nominal impedance 50Ω και το Polarization της είναι Vertical με τον κύριο λοβό της κάθετο στην επιφάνεια.



Εικόνα 8.5: Broad Band 2400-2480 MHz Quad Patch

8.1.6 PCB Log Periodic 850-6500

Η συγκεκριμένη, τριγωνικής μορφής κεραία, αποτελεί μια wideband κεραία με εύρος εκπομπής 850-6500MHz. Είναι PCB κατασκευής με δυνατότητα εφαρμογής SMA connector στην κορυφή και σύνδεση του με coaxial SMA cable. Έχει typical Forward Gain 6dBi και θα χρησιμοποιηθεί για την μπάντα του GPS στα 1575MHz.



Εικόνα 8.6: PCB Log Periodic 850-6500

Για τη σύνδεση των ηλεκτρονικών στοιχείων μεταξύ τους και με τις κεραίες, θα χρησιμοποιηθούν καλώδια SMA τα οποία λειτουργούν σε RF συχνότητες και είναι κατάλληλα για τέτοιου είδους κατασκευές. Στη συγκεκριμένη περίπτωση θα χρησιμοποιηθεί ο πιο κάτω τύπος.

8.1.7 SMA-to-SMA Microwave Cables

Το πιο πάνω αποτελεί ένα ομοαξονικό καλώδιο με connectors male SMA και στις δύο άκρες του και δουλεύει στις συχνότητες των 2.4GHz. Έχει impedance 50Ω και οι απώλειες του στις συχνότητες αυτές είναι λιγότερες του 1dB.

Εικόνα 8.7: SMA-to-SMA Microwave Cable

8.1.8 RF coaxial connector terminal

Πέραν των καλωδίων, θα χρησιμοποιηθούν 2 female RF coaxial connector terminals όπως φαίνονται στην εικόνα πιο κάτω, οι οποίοι θα κολληθούν στο pin του RFout σε κάθε VCO και στην άλλη πλευρά θα προσαρμοστούν τα cables που αναφέραμε πιο πάνω για τη μεταφορά του σήματος.

Η προσαρμογή του κυκλώματος και η σύνδεση των βασικών ηλεκτρονικών στοιχείων θα γίνει πάνω σε copper clad board με τη μέθοδο χρήσης copper board strips για τη μεταφορά του ρεύματος. Με αυτό τον τρόπο χρησιμοποιείται η επιφάνεια της πλακέτας ως ground όπου συγκολλούνται όλες οι ground επαφές και πάνω σε αυτή συγκολλούνται strips στα οποία μεταφέρεται το ρεύμα. Έτσι μπορεί η πλακέτα να κατασκευαστεί εύκολα και να τροποποιηθεί οποιαδήποτε στιγμή με πρόσθεση νέων στοιχείων απλά χρησιμοποιώντας επιπλέον strips.

Εικόνα 8.9: Κομμάτια copper clad board

Εικόνα 8.10: Κομμάτια χάλκινων strips

Για τη δημιουργία του σήματος Vtune που θα εφαρμοστεί στον κάθε VCO θα χρησιμοποιηθεί μια μικρή εύχρηστη γεννήτρια σημάτων 2 καναλιών με τη δυνατότητα αποθήκευσης διαφόρων custom σημάτων τα οποία μπορούμε να δοκιμάσουμε στα πειράματα μας για τον προσδιορισμό του αποτελεσματικότερου σήματος. Η συγκεκριμένη γεννήτρια θα προσαρμοστεί στο σύστημα αφού το μέγεθος της και η κατανάλωση της επιτρέπουν τη μεταφορά και τροφοδοσία της από φορητή πηγή τάσης 5V. Το σήμα Vtune θα μπορούσε να δημιουργηθεί με τη κατασκευή μικρού tuning κυκλώματος με τη χρήση ενός timer όπως τον NE555 όπως θα αναφερθεί και εκτενέστερα πιο κάτω. Οι δυνατότητες όμως που μας δίνει αυτή η χαμηλού κόστους γεννήτρια συχνοτήτων θα μας βοηθήσει ώστε να βρεθεί πιο γρήγορα και πιο αποτελεσματικά η ιδανική κυματομορφή tuning του VCO. Πιο κάτω αναφέρονται τα χαρακτηριστικά και οι δυνατότητες της γεννήτριας αυτής.

8.1.9 Signal Generator

Η γεννήτρια σημάτων που θα χρησιμοποιηθεί αποτελεί μια ψηφιακή, γεννήτρια, μικρή και εύκολη στη μεταφορά. Τα κανάλια της είναι αποκλειστικά ανεξάρτητα και τα σήματα εξόδου μπορούν να παραχθούν ταυτόχρονα. Μπορεί να παράξει διάφορες συναρτήσεις, παλμικά και ψηφιακά σήματα αλλά και custom arbitrary κυματομορφές. Έχει τη δυνατότητα μέτρησης σημάτων και ο χειρισμός της μπορεί να γίνει εύκολα τόσο από λογισμικό στον υπολογιστή, όσο και από την LCD οθόνη που έχει ενσωματωμένη. Με τη χρήση τεχνολογίας DDS, τα σήματα που παράγει είναι ακριβή, σταθερά και με πολύ χαμηλή παραμόρφωση. Η μέγιστη συχνότητα εξόδου που μπορεί να παραχθεί σε ημιτονοειδές σήμα είναι 15MHz /30MHz /40MHz /50MHz με sampling rate 266MSa/s. Υπάρχει η δυνατότητα αποθήκευσης 60 group arbitrary κυματομορφών και 100 groups παραμέτρων που μας επιτρέπει να δημιουργήσουμε από πριν διάφορα σήματα για γρήγορη εφαρμογή και δοκιμή. Η γεννήτρια αυτή έχει επίσης τη δυνατότητα εφαρμογής πλάτους σήματος 0Vpp~20Vpp με minimum resolution 1mV. Πολύ

σημαντικό χαρακτηριστικό είναι το DC offset range που κυμαίνεται από -9.99V~9.99V, με offset resolution 0.01V. Η τροφοδοσία της όπως προαναφέρθηκε είναι 5VDC και το βάρος της 800g χαρακτηριστικά που μας επιτρέπουν να την κάνουμε φορητή και να την ενσωματώσουμε στο σύστημα.

Τέλος για την τροφοδοσία τόσο του κυκλώματος όσο και της γεννήτριας σημάτων μπορούμε να χρησιμοποιήσουμε ένα Power Bank 2 εξόδων αφού τόσο οι VCOs όσο και οι Amplifiers αλλά και η γεννήτρια λειτουργούν με τάση τροφοδοσίας 5VDC. Η κατανάλωση της γεννήτριας είναι λίγο πιο κάτω από το 1A ενώ του υπόλοιπου κυκλώματος κοντά στα 60mA. Έτσι με ένα Power Bank 2 εξόδων, οι οποίες έχουν ως γνωστό τάση εξόδου 5V και ένταση ρεύματος 1-2A, μπορούμε να τροφοδοτούμε όλο το σύστημα και έτσι να είναι και φορητό για ευκολότερη χρήση.

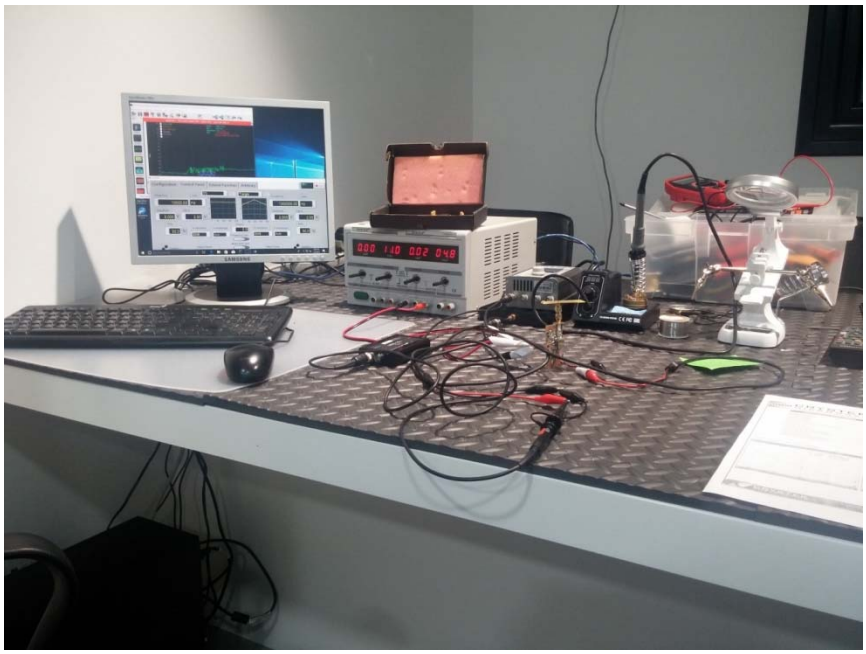
Εικόνα 8.12: Power Bank 2 εξόδων

Με την ολοκλήρωση του συστήματος, όλα τα πιο πάνω θα τοποθετηθούν σε αυτοσχέδια ξύλινη κατασκευή που θα παρέχει τόσο προστασία όσο και φορητότητα του συστήματος αλλά και ευκολία στη χρήση όπως θα δείξουμε και πιο κάτω.

8.2 Κατασκευή

Ακολούθως θα προχωρήσουμε στην περιγραφή της κατασκευής τους συστήματος βήμα προς βήμα κάνοντας αναφορά και στη θεωρία που διέπει τη λειτουργία των τμημάτων που αποτελούν το σύστημα. Όπως αναφέρθηκε και προηγουμένως, η κατασκευή έγινε σε

εργαστήριο και συγκεκριμένα σε πάγκο εργασίας όπου υπήρχαν όλα τα απαραίτητα υλικά και εργαλεία για ασφαλή και σωστή εργασία.



Εικόνα 8.13: Το εργαστήριο με τον εξοπλισμό για την κατασκευή του συστήματος

8.2.1 Πλακέτα

Ξεκινώντας την κατασκευή, σαν πρώτο βήμα έγινε η συγκόλληση του ενός VCO πάνω στην χάλκινη πλακέτα, πάντα συμβουλευόμενοι το specifications sheet του VCO όπου περιγράφονται και απεικονίζονται όλα τα pins μαζί με τη θέση τους και το ρόλο τους. Για τον προσανατολισμό και των προσδιορισμό του κάθε pin στον VCO, υπάρχει στην κάτω αριστερά γωνία dot mark το οποίο χρησιμοποιούμε για να αριθμήσουμε όλες τις επαφές σύμφωνα με το specifications sheet. Αρχικά έγινε η συγκόλληση των Ground pins τα οποία αποτελούσαν το μεγάλο μέρος της περιμέτρου του VCO. Επειδή η επιφάνεια της πλακέτας χρησιμοποιήθηκε ως ground, για να μην έρχονται σε επαφή τα 3 pins που αφορούν Vcc, Vt και RFout, τοποθετήθηκε πλαστικό υλικό πάχους μερικών mm κάτω από τον VCO που χρησιμεύει ως «σκαλί» για να μην πατούν οι υπόλοιπες επαφές στην επιφάνεια της πλακέτας. Ακολούθως τα 13 ground pins συγκολλήθηκαν ένα-ένα προσεκτικά πάνω στην επιφάνεια, ενώ στα εναπομείναντα 3 κολλήθηκαν μικρά κομμάτια χάλκινων strips όπως φαίνεται και στις ακόλουθες φωτογραφίες.

Εικόνα 8.14: Ο VCO συγκολλημένος στην πλακέτα. Ξεχωρίζει η κόλληση σε κάθε pin

Εικόνα 8.15: Χάλκινο strip συγκολλημένο σε pin του VCO (κάτοψη)

Εικόνα 8.16: Χάλκινο strip συγκολλημένο σε pin του VCO (πλάγια όψη)

Εικόνα 8.17: Πλάγια όψη του συγκολλημένου στην πλακέτα VCO

Τα strips αυτά θα χρησιμοποιηθούν ως επαφές σύνδεσης άλλων καλωδίων για τη μεταφορά του ρεύματος αλλά και των απαραίτητων connectors.

Μετά την ολοκλήρωση της συγκόλλησης, γίνεται έλεγχος των επαφών του VCO για επιβεβαίωση της σωστής εφαρμογής και την απουσία βραχυκυκλώματος μεταξύ επαφών που δεν πρέπει να είναι συνδεδεμένες. Ο έλεγχος αυτός πραγματοποιείται με ένα πολύμετρο όπου ελέγχονται η επαφές μία προς μία.

Κατά την συγκόλληση ενός RF ηλεκτρονικού στοιχείου απαιτείται αρκετή προσοχή λόγω της ευαισθησίας τέτοιων στοιχείων στο ρεύμα και στη θερμότητα. Ένα κολλητήρι ζεσταίνεται σε θερμοκρασία άνω των 250-300^{o}C και η θερμοκρασία λειτουργίας τέτοιων στοιχείων δεν ξεπερνά τους 90-100^{o}C. Επίσης η ευαισθησία στον στατικό ηλεκτρισμό είναι μεγάλη γι' αυτό η επαφή με γυμνά χέρια πάνω στην επιφάνεια τους είναι απαγορευτική.

Μετά την επιβεβαίωση της σωστής εφαρμογής του VCO, προχωρούμε στην εφαρμογή ενός female RF coaxial connector terminal στο pin RFout του VCO. Αυτό μπορεί να γίνει είτε με τη συγκόλληση του εσωτερικού pin κατευθείαν στο pin του RFout είτε πάνω σε strip το οποίο είναι με τη σειρά του συνδεδεμένο με το pin RFout για αποφυγή υπερθέρμανση του VCO ή κίνδυνου βραχυκυκλώματος με γειτονικό pin. Το pin του connector δεν πρέπει να έρχεται σε επαφή με την επιφάνεια της πλακέτας πάνω στην οποία συγκολλείται ο εξωτερικός μεταλλικός αγωγός του RF connector. Τα δύο μεταξύ τους δεν πρέπει να βραχυκυκλώνουν για τη σωστή λειτουργία του ομοαξονικού αυτού αγωγού. Η σύνδεση του connector φαίνεται στην πιο κάτω φωτογραφία.

Εικόνα 8.18: RF connector εφαρμοσμένο στο strip που συνδέεται με το RFout

Για τη μεταφορά ρεύματος στις 2 επαφές που χρειάζεται η εφαρμογή τάσης, δηλαδή το Vcc και το Vt, χρησιμοποιούμε λεπτά καλώδια χρώματος κόκκινο και μαύρο για καθορισμό της πολικότητας. Έτσι για την εφαρμογή Vcc, χρησιμοποιούμε ζεύγος καλωδίων όπως προαναφέρθηκε, με το μαύρο να συγκολλείται στην επιφάνεια της πλακέτας και το κόκκινο στο strip το οποίο είναι συνδεδεμένο με το pin Vcc. Την ίδια διαδικασία ακολουθούμε και για τη Vt. Πάλι με ζεύγος καλωδίων με αντίστοιχη εφαρμογή.

Εικόνα 8.19: Εφαρμογή καλωδίων για μεταφορά του Vcc

Μετά την ολοκλήρωση της εφαρμογής του πρώτου VCO, συνεχίζουμε με τον δεύτερο ακολουθώντας την ίδια ακριβώς διαδικασία. Τον τοποθετούμε λοιπόν απέναντι και η συγκόλληση μαζί με τα strips γίνεται σε θέση mirror με τον προηγούμενο. Αυτό γίνεται κυρίως για πρακτικούς λόγους περιορίζοντας την έκταση που θα καταλαμβάνουν τα καλώδια που θα εφαρμόζονται πάνω στην πλακέτα. Ο δεύτερος VCO, της μπάντας 1200-2300MHz, κατασκευαστικά έχει όλη την κάτω επιφάνεια ground στην οποία εφάπτονται όλα τα ground pins. Αυτό κάνει την κόλληση πάνω στην πλακέτα πιο εύκολη αφού δεν χρειάζεται να κολληθούν ένα-ένα τα pins. Για την αποφυγή όμως σύνδεσης των 3 pins Vcc, Vt και RFout με την επιφάνεια ground, χρησιμοποιούμε παρόμοια τεχνική με πριν κρατώντας τον VCO πιο ψηλά από την επιφάνεια. Αυτή τη φορά χρησιμοποιούμε ως «σκαλί» μικρά κομμάτια strips, τοποθετημένα κάθετα και κολλημένα από την μια πλευρά περιμετρικά της επιφάνειας του VCO πάνω στα ground pins και από την άλλη πάνω στην πλακέτα. Έτσι υπάρχει αγώγιμη σύνδεση των ground pins διαμέσου των strips πάνω στην πλακέτα. Όπως και πριν, για τις υπόλοιπες 3 επαφές χρησιμοποιούμε μικρά κομμάτια strips ως δρομολογητές. Με την συγκόλληση του δεύτερου σε θέση mirror, το RFout βρίσκεται στην αντίθετη πλευρά της πλακέτας όπου συγκολλείται το RF coaxial connector terminal με την ίδια ακριβώς διαδικασία με πριν. Αυτή η διάταξη εξοικονομεί χώρο και κάνει πιο εύκολη την εφαρμογή των καλωδίων όπως για παράδειγμα στην εφαρμογή

της τάσης τροφοδοσίας Vcc, όπου δεν είναι αναγκαία η χρήση 2 ζευγών καλωδίων. Με την εφαρμογή ενός ζεύγους καλωδίων τροφοδοσίας στον ένα VCO και με τη σύνδεση των 2 Vcc pins μεταξύ τους με καλώδιο όπως φαίνεται και πιο κάτω, εξασφαλίζεται η τροφοδοσία και των 2 VCOs. Στις πιο κάτω φωτογραφίες φαίνεται η εφαρμογή της πιο πάνω διαδικασίας.

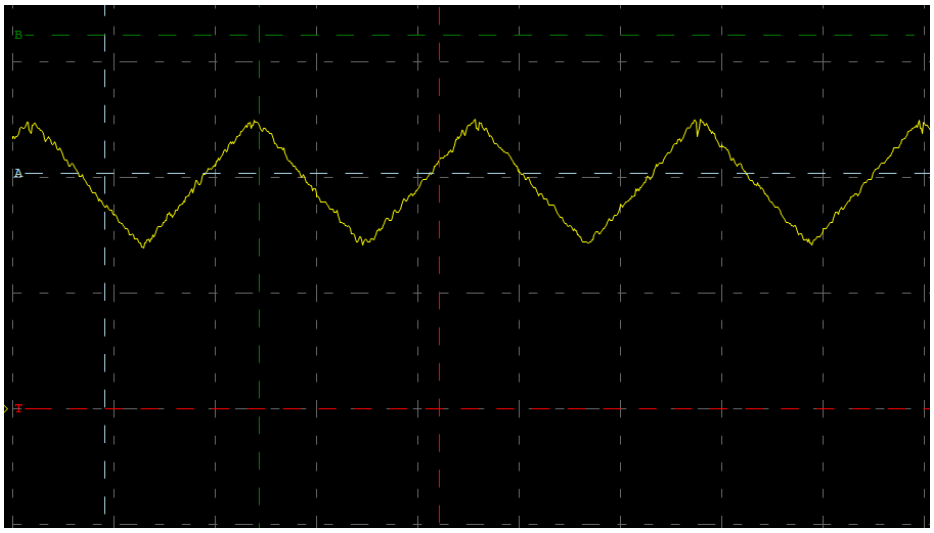
Εικόνα 8.20: Η πλευρά του VCO συγκολλημένη ολόκληρη στην ground plain

Εικόνα 8.21: Mirror διάταξη των 2 VCOs

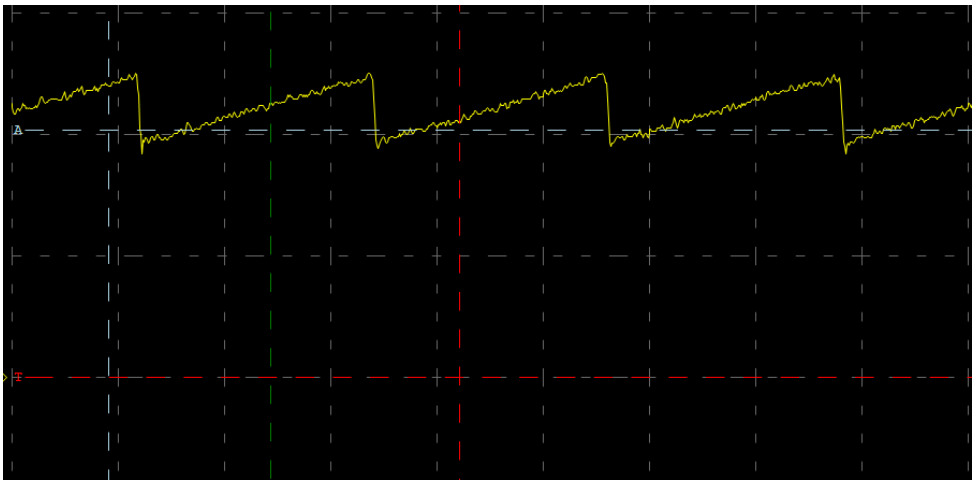
Στις εργαστηριακές δοκιμές χρησιμοποιούμε επιτραπέζιο τροφοδοτικό με το οποίο μπορούμε να ρυθμίσουμε την τάση με την οποία θα τροφοδοτούμε την πλακέτα και παράλληλα να βλέπουμε την κατανάλωση ρεύματος για καλύτερο έλεγχο έτσι ώστε να συμβαδίζουμε με τους περιορισμούς του κατασκευαστή. Στα specification sheets και των 2 VCOs μπορούμε να δούμε τόσο το typical VDC που μπορούμε να εφαρμόσουμε για ιδανική και ασφαλή λειτουργία, όσο και το εύρος που μπορούμε να κυμανθούμε για να λειτουργεί με ασφάλεια το στοιχείο αυτό. Σε αυτή την περίπτωση η VDC typical είναι στα 5V με εύρος 4.75-5.25 VDC. Με ένα πολύμετρο ακριβείας επιβεβαιώνουμε πάντα την ένδειξη του τροφοδοτικού πριν την εφαρμογή της τάσης για να είμαστε σίγουροι. Μπορούμε επίσης να δούμε και την μέγιστη κατανάλωση ρεύματος που πρέπει πάντα να παρακολουθούμε ώστε να μην καεί ο VCO. Σε αυτή την περίπτωση στον πίνακα των χαρακτηριστικών τους καθορίζεται ότι η κατανάλωση στον VCO της μπάντας των 1200-2300MHz δεν πρέπει να ξεπερνά τα 25mA ενώ στην άλλο όχι μεγαλύτερη από 35mA με typical τα 20mA.

Για τη δημιουργία του σήματος Vtune, το οποίο θα εισάγεται στο VCO, χρησιμοποιούμε τη γεννήτρια σημάτων που παρουσιάσαμε πιο πάνω. Για την καλύτερη κατανόηση του ρόλου του Vtune, θα πρέπει να περιγράψουμε τη λειτουργία ενός VCO. Ο VCO αποτελεί ένα ηλεκτρονικό ολοκληρωμένο κύκλωμα του οποίου η έξοδος ανά χρονική στιγμή είναι μια συγκεκριμένη συχνότητα η οποία εξαρτάται από την τιμή της τάσης εισόδου. Έτσι με την εισαγωγή μιας περιοδικής κυματομορφή (Vtune) με ένα συγκεκριμένο εύρος τιμών V, θα πάρουμε αντίστοιχα στην έξοδο ένα περιοδικό σήμα συγκεκριμένης ισχύος το οποίο θα καλύπτει ένα εύρος συχνοτήτων όπως καθορίζεται στο Specification sheet σε κάθε VCO. Όπως προαναφέραμε, το σήμα αυτό το οποίο θα ρυθμίζει τον VCO, μπορούμε να το παράξουμε με μια διάταξη αντιστάσεων και πυκνωτών που θα περιλαμβάνει ένα timer NE555. Σε αυτή την περίπτωση όμως, η γεννήτρια σημάτων που θα χρησιμοποιήσουμε, μας δίνει τη δυνατότητα να δημιουργήσουμε προκατασκευασμένα ή και τυχαία σήματα οποιονδήποτε χαρακτηριστικών θέλουμε και να τα αποθηκεύσουμε έτσι ώστε ανά πάσα στιγμή να χρησιμοποιήσουμε ό, τι σήμα θέλουμε και να προσδιορίσουμε το βέλτιστο στις δοκιμές μας. Με τη βοήθεια λογισμικού το οποίο συνοδεύεται, μπορούμε εύκολα και γρήγορα να δημιουργήσουμε στο εργαστήριο τα σήματα αυτά που θέλουμε στην περίπτωση μας. Ως βασικό σήμα επιλέγουμε ένα σήμα με τριγωνική μορφή. Συνήθως σε τέτοιες εφαρμογές όπου θέλουμε να καλύπτουμε γρήγορα και περιοδικά ένα εύρος συχνοτήτων, χρησιμοποιείται σήμα τριγωνικής μορφής. Δύο σήματα τέτοιας μορφής που ταιριάζουν στην περίπτωση αυτή είναι το απλό τριγωνικό (triangular) και

το πριονωτής μορφής (sawtooth). Η μορφή των σημάτων αυτών φαίνεται και στις εικόνες πιο κάτω.



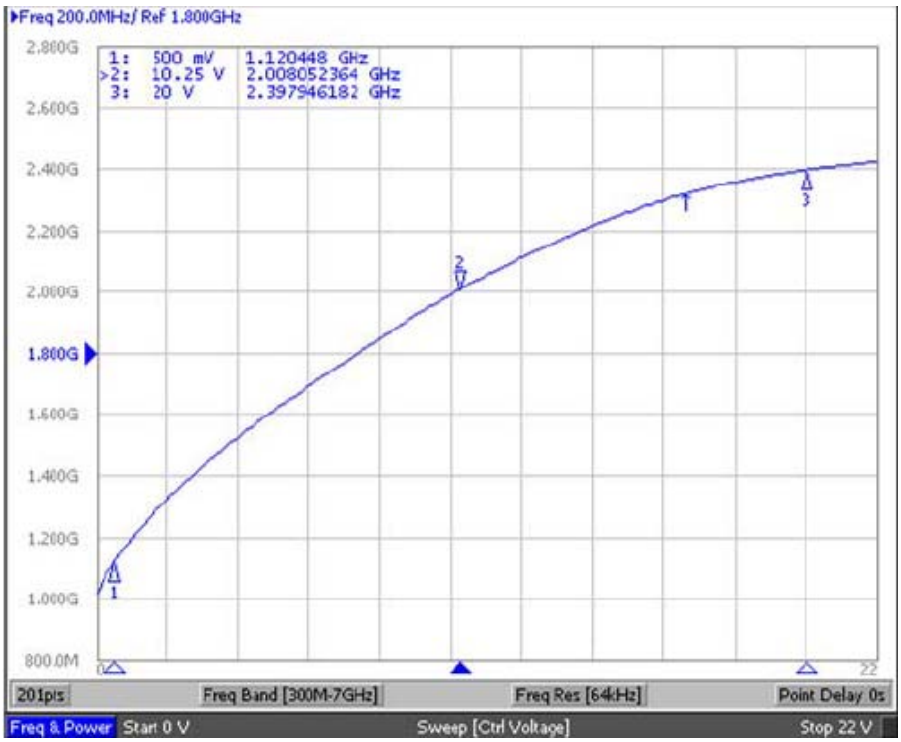
Εικόνα 8.22: Triangular signal όπως εμφανίζεται στον oscillator



Εικόνα 8.23: Sawtooth signal όπως εμφανίζεται στον oscillator

Και στις δύο περιπτώσεις, τα σήματα αυτά έχουν ελάχιστη και μέγιστη τιμή και οι τιμές τους αυξομειώνονται γραμμικά σε συνάρτηση με το χρόνο. Η διαφορά τους είναι ότι στην περίπτωση του triangular, το σήμα αυξάνει την τιμή του γραμμικά από την ελάχιστη στη μέγιστη και στη συνέχεια μειώνεται μέχρι να φτάσει ξανά στην ελάχιστη. Στο sawtooth, η τιμή αυξάνεται από την ελάχιστη μέχρι τη μέγιστη και ακολούθως πέφτει κατευθείαν στην ελάχιστη για να ξανακάνει την ίδια διαδικασία. Αυτή η διαφορά στις δύο αυτές κυματομορφές επιδρά στον VCO με αποτέλεσμα η παραγωγή των συχνοτήτων στην έξοδο να γίνεται αντίστοιχα με διαφορετικό τρόπο. Στην περίπτωση του triangular wave, μπορούμε να φανταστούμε την μπάντα των

παραγόμενων συχνοτήτων να ακολουθεί μια κάλυψη από τα αριστερά (μικρότερη) στα δεξιά (μεγαλύτερη) και ακολούθως επιστροφή από τα δεξιά στα αριστερά, ενώ στο sawtooth η κάλυψη γίνεται από τα αριστερά στα δεξιά και κατευθείαν επιστροφή στα αριστερά και στην μικρότερη συχνότητα για να ακολουθήσει ξανά την ίδια πορεία. Πρακτικά αυτό σημαίνει ότι αν οι δύο κυματομορφές έχουν την ίδια συχνότητα τότε, στην μεν περίπτωση του triangular, η κάλυψη γραμμικά της μπάντας γίνεται 2 φορές στον ίδιο χρόνο που η sawtooth καλύπτει μια φορά αλλά στην δεύτερη περίπτωση υπάρχει μεγαλύτερη παραμονή σε κάθε συχνότητα και η επιστροφή από τη μέγιστη παραγόμενη συχνότητα στην ελάχιστη γίνεται κατευθείαν. Τα βασικά μεγέθη με τα οποία καλούμαστε να διαμορφώσουμε τις κυματομορφές τις οποίες θα σχεδιάσουμε για το tuning του VCO είναι το Amplitude και το offset. Το πλάτος (Amplitude) ως η απόλυτη τιμή της διαφοράς της τιμής στην κορυφή του κύματος με το 0, είναι αυτό που θα καθορίσει ανάλογα με την τιμή του offset, ποιο είναι το εύρος των συχνοτήτων που θα καλύπτει ο κάθε VCO. Το εύρος συχνοτήτων που καλύπτει κάθε VCO είναι συγκεκριμένο όπως και το εύρος τιμών του Vt το οποίο καθορίζεται στο specifications sheet. Ο κατασκευαστής μας δίνει την ελάχιστη και την μέγιστη τιμή του Vt που αντιστοιχούν στις δύο ακραίες συχνότητες της μπάντας. Από ‘κει και πέρα, μας δίνει το διάγραμμα της καμπύλης tuning (tuning curve typical). Η συγκεκριμένη καμπύλη η οποία φαίνεται και πιο κάτω, ακολουθεί μια μορφή στην οποία όσο αυξάνεται η τάση Vt τόσο αυξάνεται και η συχνότητα και έτσι από την καμπύλη μπορείς να προσδιορίσεις με σχετική ακρίβεια την συχνότητα που αντιστοιχεί σε κάθε τιμή Vt. Ενδεικτικά ο κατασκευαστής μας δίνει 3 συγκεκριμένες τιμές όπως έχουν προσδιοριστεί και επιβεβαιωθεί με τη χρήση συγκεκριμένου signal analyzer το οποίο και αναφέρεται.



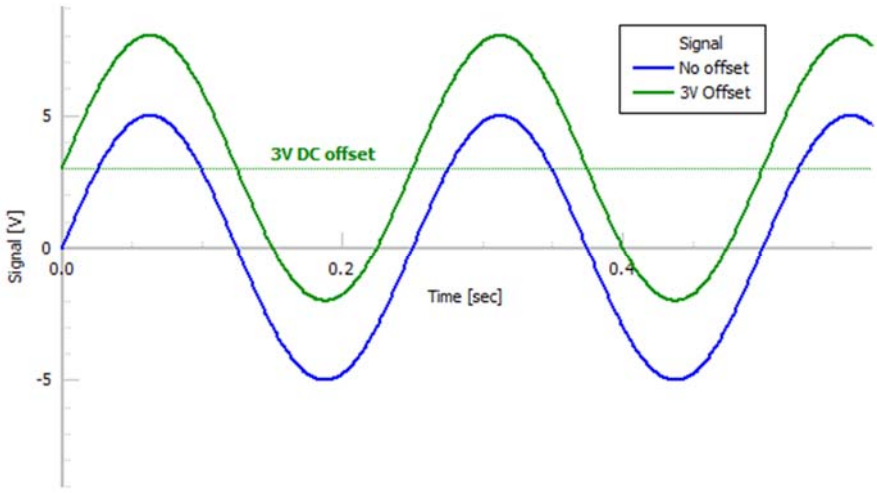
Διάγραμμα 8.1: Η tuning curve του VCO 1200-2300

Για δική μας επαλήθευση της καμπύλης, πήραμε στο εργαστήριο αριθμό μετρήσεων με τη χρήση τιμών κατά μήκος της καμπύλης αυτής και συγκρίναμε. Αυτό έγινε και με τους δύο VCOs. Παρ' όλο που ο κάθε VCO μας δίνει ένα συγκεκριμένο εύρος συχνοτήτων, εμάς δεν μας ενδιαφέρει όλο το εύρος αυτό. Γνωρίζοντας από πριν ποιες τεχνολογίες χρησιμοποιεί το drone για να πετάξει και εν συνεπεία τις συχνότητες όπως περιγράφηκαν και σε προηγούμενα κεφάλαια, μπορούμε να περιορίσουμε τις παραγόμενες συχνότητες γύρω από τις συχνότητες που θέλουμε να προσβάλουμε. Με αυτό μπορούμε να πετύχουμε, όπως θα περιγράψουμε και πιο κάτω, τον περιορισμό της διασποράς ισχύος σε μεγάλο εύρος συχνοτήτων, μειώνοντας έτσι της ισχύ που θα έχει το εκπεμπόμενο σήμα στις συχνότητες που μας ενδιαφέρει. Έτσι με τη βοήθεια της tuning curve βρίσκουμε τις δύο ακραίες συχνότητες που θέλουμε στην παραγόμενη μπάντα και στη συνέχεια προσδιορίζουμε την Vtmin και Vtmax. Γνωρίζοντας αυτές τις δύο τιμές διαμορφώνουμε τον συνδυασμό Amplitude και offset με τέτοιες τιμές έτσι ώστε το tuning signal να έχει ως μέγιστη και ελάχιστη τιμή τις τιμές αυτές. Όπως φαίνεται και στο specification sheet, το Vt παίρνει θετικές τιμές άρα η κυματομορφή πρέπει να έχει ως ελάχιστη τιμή την θετική τιμή Vtmax που αναφέραμε και πιο πάνω.

PERFORMANCE SPECIFICATION	MIN	TYP	MAX	UNITS
Lower Frequency:			1200	MHz
Upper Frequency:	2300			MHz
Tuning Voltage:	0.5		20.0	VDC
Supply Voltage:	4.75	5.0	5.25	VDC
Output Power:	0	+4.0	+8.0	dBm
Supply Current:			25	mA
Harmonic Suppression (2nd Harmonic):		-10		dBc
Pushing:			5.0	MHz/V
Pulling, all Phases:			15.0	MHz pk-pk
Tuning Sensitivity:		58		MHz/V
Phase Noise @ 10kHz offset:		-100		dBc/Hz
Phase Noise @ 100kHz offset:		-122		dBc/Hz
Load Impedance:		50		Ω
Input Capacitance:			47	pF
Operating Temperature Range:	-40		+85	°C
Storage Temperature Range:	-45		+90	°C

Πίνακας 8.1: Πίνακας με τα specifications του VCO 1200-2300

Γνωρίζουμε όμως ότι σε ένα περιοδικό σήμα, το κύμα ξεκινά από το 0 (αν έχει αρχική φάση 0) αυξάνεται η τιμή του μέχρι μια μέγιστη τιμή και στη συνέχεια μειώνεται περνώντας από το 0 και παίρνοντας αρνητικές τιμές μέχρι μια ελάχιστη αρνητική τιμή. Με τη χρήση όμως offset θετικής τιμής, μετακινούμε το σημείο 0 ανεβάζοντας την κυματομορφή πάνω από τον μηδενικό άξονα κατά τόσο όση είναι η τιμή του offset. Πιο κάτω επεξηγείται καλύτερα η χρήση του offset γραφικά.

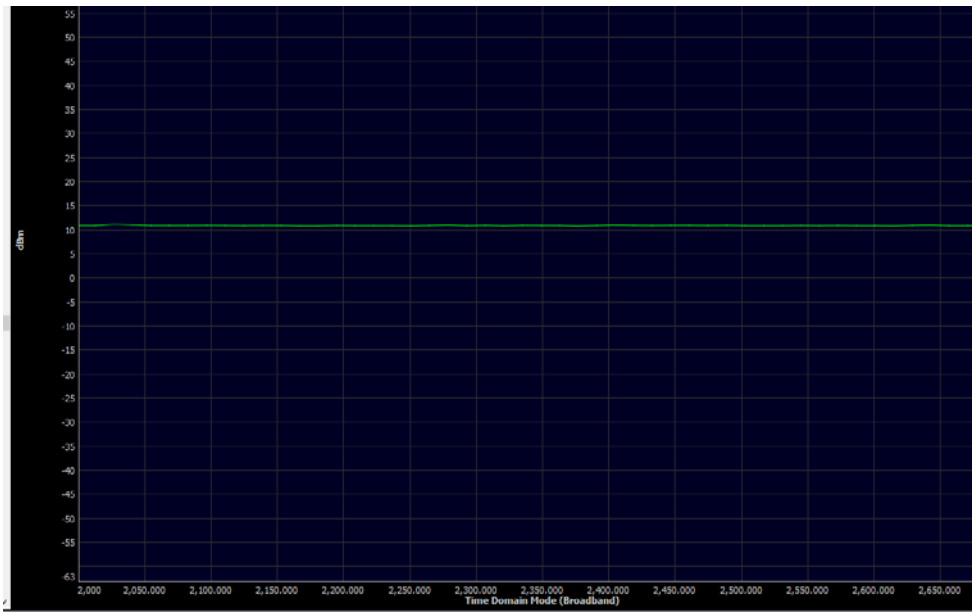


Διάγραμμα 8.2: Απεικόνιση της πρόσθεσης offset σε περιοδικό σήμα

Προσθέτοντας το offset στο σήμα, ανεβάζουμε την κυματομορφή όμως το κύμα παίρνει τιμές τόσο πάνω από το offset όσο και κάτω από το offset. Έτσι το πλάτος του σήματος πρέπει να

διαμορφωθεί με τέτοια τιμή έτσι ώστε το νέο σήμα να έχει ως ελάχιστη και μέγιστη τιμή τις θετικές τιμές που αναφέραμε ποιο πάνω. Στα σήματα που θα φτιάξουμε για να δοκιμάσουμε, η γεννήτρια σημάτων που χρησιμοποιούμε μας δίνει τη δυνατότητα να προσθέσουμε θόρυβο (noise) διαφόρων εντάσεων. Με την πρόσθεση θορύβου συγκεκριμένου πλάτους, απλώνεται σε όλο το tuning σήμα και μεταφέρεται στην έξοδο του VCO και στο σήμα εκπομπής. Συνήθως στα RF κυκλώματα ο θόρυβος είναι ανεπιθύμητος αλλά στην περίπτωση μας όπου όλο το σύστημα πρόκειται για jammer, ο θόρυβος είναι ενισχυτικός στην αποτελεσματικότητα του συστήματος αφού αντικειμενικός σκοπός εν γένει είναι η μείωση του SNIR στο δέκτη (drone) και την πλήρη απενεργοποίηση του. Το πλάτος του θορύβου όμως πρέπει να είναι αρκετό για να αυξήσει την παρεμβολή αλλά ένα σήμα θορύβου με πολύ μεγάλο πλάτος μπορεί να αλλοιώσει αρκετά το tuning signal μετακινώντας την μπάντα των παραγόμενων συχνοτήτων από το σημείο που μας ενδιαφέρει.

Με τη χρήση ενός φασματοσκοπίου (spectrum analyzer), έχουμε τη δυνατότητα να δούμε τόσο τις συχνότητες που παράγονται στους δύο VCOs όσο και την ισχύ του σήματος στις συχνότητες αυτές. Γενικά μια τέτοια συσκευή μετρά το μέγεθος ενός σήματος εισόδου συναρτήσει της συχνότητας εντός της πλήρους περιοχής συχνοτήτων του οργάνου. Το σήμα εισόδου που μετράει ένας αναλυτής φάσματος είναι ηλεκτρικό. Με την ανάλυση των φασμάτων των ηλεκτρικών σημάτων μπορεί να παρατηρηθεί κυρίαρχη συχνότητα, ισχύς, παραμόρφωση, αρμονικές, εύρος ζώνης και άλλα φασματικά συστατικά ενός σήματος που δεν είναι εύκολα ανιχνεύσιμα στις κυματομορφές του χρονικού πεδίου. Η απεικόνιση ενός αναλυτή φάσματος έχει συχνότητα στον οριζόντιο άξονα και το πλάτος που εμφανίζεται στον κατακόρυφο άξονα. Συνήθως τα spectrum analyzers χρησιμοποιούν μέθοδο με FFT μετατροπή για να παρουσιάσουν την είσοδο ενός σήματος που βρίσκεται στο πεδίο του χρόνου, στο πεδίο της συχνότητας όπου μπορούμε να δούμε τόσο τις συχνότητες όσο και το πλάτος κάθε μιας. Λόγω της παραγωγής ενός εύρους συχνοτήτων από τον VCO, η ισχύς που παράγεται από το κύκλωμα απλώνεται σε όλη την μπάντα. Όσο πιο πολύ περιορίσουμε το εύρος αυτής της μπάντας στις συχνότητες που θέλουμε να επικεντρωθούμε, τόσο μεγαλύτερη ισχύς θα συσσωρευτεί στις συχνότητες αυτές. Το spectrum analyzer μπορεί να δουλέψει και σε mode Power meter με αποτέλεσμα να μπορούμε να δούμε το σύνολο της ισχύς που διασπείρεται στην μπάντα. Στην πιο κάτω εικόνα μπορούμε να δούμε σε mode Power meter την ένταση της ισχύς η οποία παίρνει τη συγκεκριμένη τιμή όμως γιατί απλώνεται σε όλο το επιλεγμένο εύρος της μπάντας.



Εικόνα 8.24: Το spectrum analyzer σε mode Power meter όπου φαίνεται το σύνολο της ισχύς που διασπείρεται στην μπάντα

Την ισχύ θα μπορούσαμε να τη δούμε επίσης τροφοδοτώντας τον VCO με ένα επίπεδο σήμα σταθερής τάσης το οποίο να αντιστοιχεί σε μια συχνότητα. Έτσι στην έξοδο του θα παραχθεί η συχνότητα αυτή φέροντας την ισχύ. Το spectrum analyzer με αυτή την επιλογή θα μας προβάλει τότε θεωρητικά τη συνάρτηση δέλτα η οποία συγκεντρώνει όλη την ισχύ και στις υπόλοιπες συχνότητες κυμαίνεται στο 0 όπως φαίνεται και στην φωτογραφία πιο κάτω. Η διαφορά στην ισχύ με πιο πάνω οφείλεται στο γεγονός ότι τροφοδοτώντας με ένα σήμα σταθερής τάσης, συγκεντρώνεται όλη η ισχύς στη συχνότητα που αντιστοιχεί το συγκεκριμένο σήμα. Έτσι μπορούμε να δούμε καλύτερα τις δυνατότητες του συστήματος όσον αφορά την ισχύ.

Εικόνα 8.25: Προβολή στο spectrum analyzer της συνάρτησης δέλτα η οποία συγκεντρώνει όλη την ισχύ σε συγκεκριμένη συχνότητα

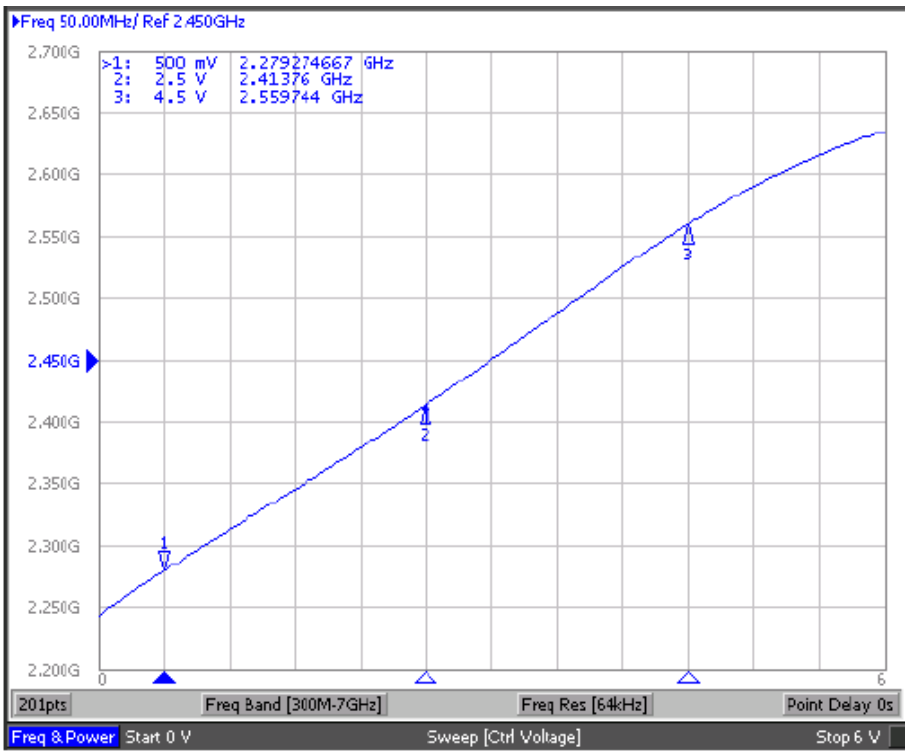
Όπως περιγράψαμε και πιο πάνω, με την είσοδο μιας σταθερής τάσης, ενός επιπέδου δηλαδή σήματος, η συχνότητα που αντιστοιχεί στη συγκεκριμένη τιμή θα παραχθεί από το VCO συγκεντρώνοντας το σύνολο της ισχύς. Το spectrum analyzer μας δίνει τη δυνατότητα να επιβεβαιώσουμε τις typical tuning curves που μας παρέχει ο κατασκευαστής, επιλέγοντας ένας εύρος συχνοτήτων που θέλουμε και προσδιορίζοντας ακολούθως το εύρος του Vt με το οποίο διαμορφώνουμε το tuning signal του VCO. Στη συνέχεια, αλλάζοντας το amplitude και το offset, όπως περιγράψαμε και πριν, επιλέγουμε τόσο τα όρια της μπάντας συχνοτήτων όσο και την ισχύ του σήματος σε κάθε συχνότητα. Η πρόσθεση θορύβου στο tuning signal, θα μας προσθέσει θόρυβο στο παραγόμενο προς εκπομπή σήμα αλλά δύναται να μας μετακινήσει τα όρια της μπάντας. Γι' αυτό το λόγο, επιβεβαιώνουμε με το spectrum analyzer ότι η πρόσθεση θορύβου δεν μας απομακρύνει από τις συχνότητες που μας ενδιαφέρουν ούτε μας ανοίγει πολύ την μπάντα και εν συνεπεία να μας διασπείρει την ισχύ.

Στην περίπτωση του jammer που αναπτύσσουμε, όπως περιγράφηκε αρκετές φορές, επικεντρωνόμαστε στις συχνότητες 2.4GHz και 1.575GHz οι οποίες αποτελούν τις συχνότητες επικοινωνίας του Drone. Από τις καμπύλες που μας δίνει ο κατασκευαστής, επιλέγουμε ένα

εύρος συχνοτήτων το οποίο να κυμαίνεται γύρω από αυτές και να είναι όσο το δυνατό πιο περιορισμένο για τους λόγους που προαναφέραμε. Επιλέγοντας ένα εύρος και όχι μια συχνότητα αποκλειστικά, αντιμετωπίζουμε τον κίνδυνο να μην επικοινωνεί το drone ακριβώς σε αυτή τη συχνότητα, αλλά σε μια γειτονική όπως είναι πολύ πιθανόν να συμβαίνει με την Wi-Fi επικοινωνία του drone όταν επιλεγεί άλλο κανάλι ή κατά την αναπήδηση συχνοτήτων (frequency hopping). Επίσης η καμπύλη είναι ενδεικτική και μπορεί να μην καταφέρουμε πρακτικά να παράξουμε ακριβώς τη συχνότητα που θέλουμε ή ακόμη και το σήμα εισόδου, λόγω θορύβου ή λόγω αστάθειας να μετακινεί την επιλογή συχνότητας. Όπως βλέπουμε και στην καμπύλη πιο κάτω που αφορά τον VCO της μπάντας 2328-2536MHz, επιλέγοντας τα όρια της μπάντας από 2,34GHz-2,49GHz, το σήμα εισόδου Vt στον VCO θα πρέπει να παίρνει τιμές από 1,8V-3,5V. Επιλέγοντας offset 2,65V και Amplitude 0,85V το σήμα θα μετακινήσει το 0 στο σημείο 2,65 και με πλάτος το αντίστοιχο που αναφέραμε το σήμα θα παίρνει τιμές από 2,65-0,85V μέχρι 2,65+0,85V. Με την επιλογή αυτών των παραμέτρων δεν ξεφεύγουμε από τους περιορισμούς του κατασκευαστή που καθορίζει ότι το Vt παίρνει τιμές από 0,5-4,5V.

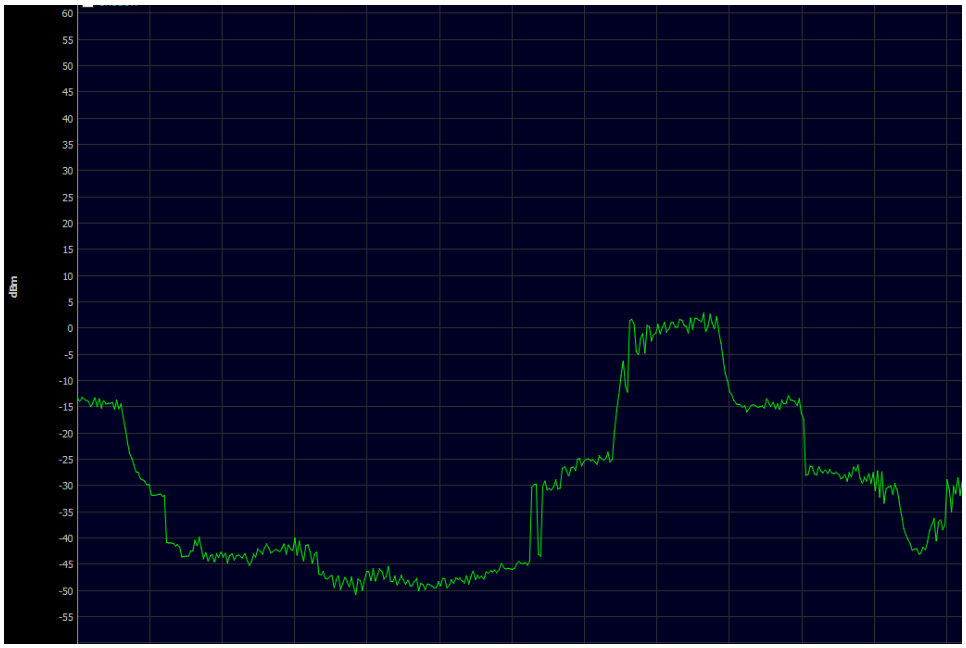
PERFORMANCE SPECIFICATION	MIN	TYP	MAX	UNITS
Lower Frequency:			2328	MHz
Upper Frequency:	2536			MHz
Tuning Voltage:	0.5		4.5	VDC
Supply Voltage:	4.75	5.0	5.25	VDC
Output Power:	+5.0	+7.0	+9.0	dBm
Supply Current:		20	35	mA
Harmonic Suppression (2nd Harmonic):		-15	-10	dBc
Pushing:			1.5	MHz/V
Pulling, all Phases:			1.5	MHz pk-pk
Tuning Sensitivity:		78		MHz/V
Phase Noise @ 10kHz offset:		-105	-101	dBc/Hz
Phase Noise @ 100kHz offset:		-126		dBc/Hz
Load Impedance:		50		Ω
Input Capacitance:			15	pF
Operating Temperature Range:	-40		+85	°C
Storage Temperature Range:	-45		+90	°C

Πίνακας 8.2: Πίνακας με τα specifications του VCO 2328-2536



Διάγραμμα 8.3: Η tuning curve του VCO 2328-2536

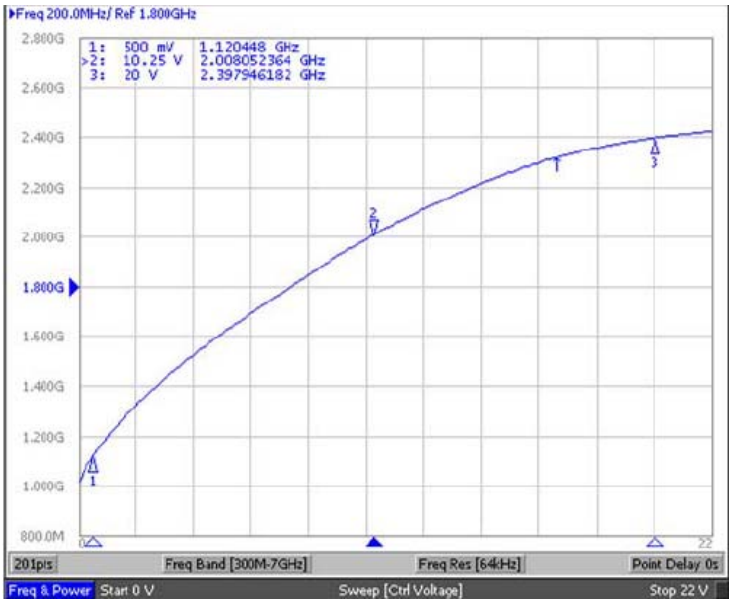
Στις εικόνες που ακολουθούν βλέπουμε πώς διαμορφώνεται η παραγόμενη μπάντα συχνοτήτων με τις τιμές που δώσαμε στις μεταβλητές offset και Amplitude και πώς μεταβάλλεται αν αλλάξουμε τις τιμές αυτές.



Εικόνα 8.26: Παραγόμενη μπάντα συχνοτήτων επικεντρωμένη στη συχνότητα των 2,4GHz

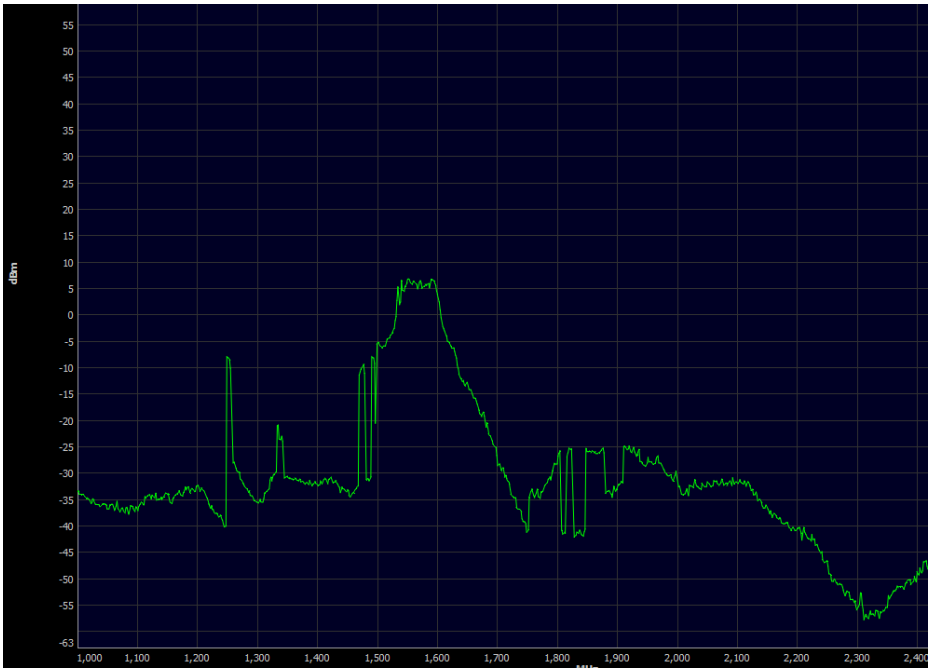
Εικόνα 8.27: Η μεταβολή στο εύρος και ισχύς της παραγόμενης μπάντας μετά από μεταβολή στο offset και στο amplitude

Αντίστοιχα για την μπάντα του GPS, από την καμπύλη που βλέπουμε πιο κάτω, επιλέγοντας τα όρια της μπάντας από 1,5GHz-1,7GHz, το σήμα εισόδου Vt στον VCO θα πρέπει να παίρνει τιμές από 3,5V-6V. Επιλέγοντας offset 4,75V και Amplitude 1,25V το σήμα θα παίρνει τιμές από 3,5-1,25V μέχρι 3,5+1,25V. Με την επιλογή αυτών των παραμέτρων δεν ξεφεύγουμε από τους περιορισμούς του κατασκευαστή που καθορίζει ότι το Vt παίρνει τιμές από 0,5-20V.



Διάγραμμα 8.4: Η tuning curve του VCO 1200-2300

Εικόνα 8.28: Η παραγόμενη μπάντα επικεντρωμένη στη συχνότητα L1 του GPS



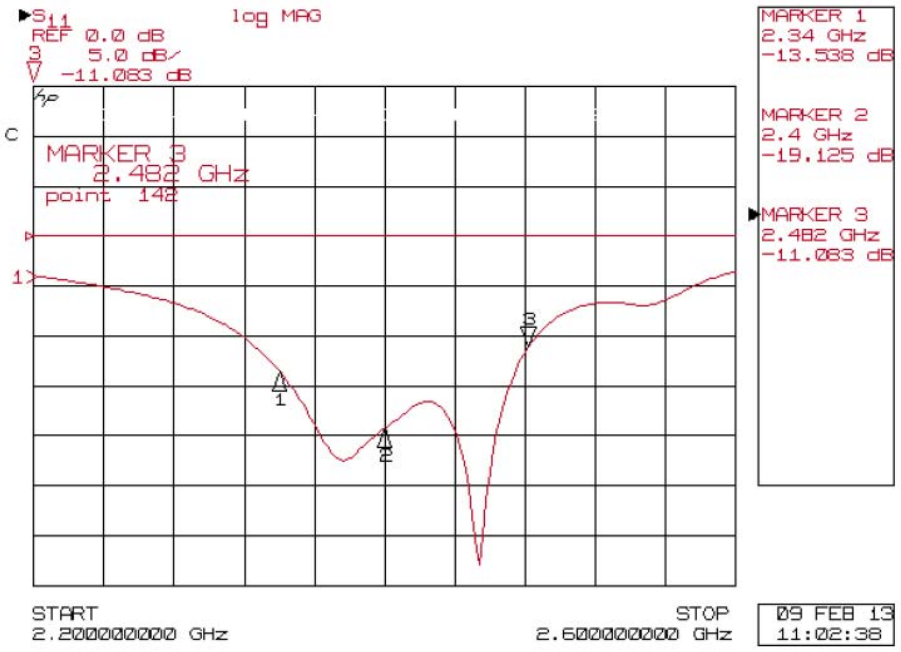
Εικόνα 8.29: Η μεταβολή στο εύρος και ισχύς της προηγούμενης παραγόμενης μπάντας μετά από μεταβολή στο offset και στο amplitude

Τα δύο σήματα που θα εκπεμφθούν από τις δύο κεραίες του συστήματος, χρειάζεται να έχουν αποκτήσει την απαραίτητη ενίσχυση έτσι ώστε να μπορούν να αποκόψουν τη σύνδεση του drone με τον χειριστή. Για να αποκοπεί η σύνδεση πρέπει ο λόγος σήματος προς την παρεμβολή και τον υπόλοιπο θόρυβο (SNIR) να είναι όσο το δυνατό πιο μικρός. Τα commercial drones

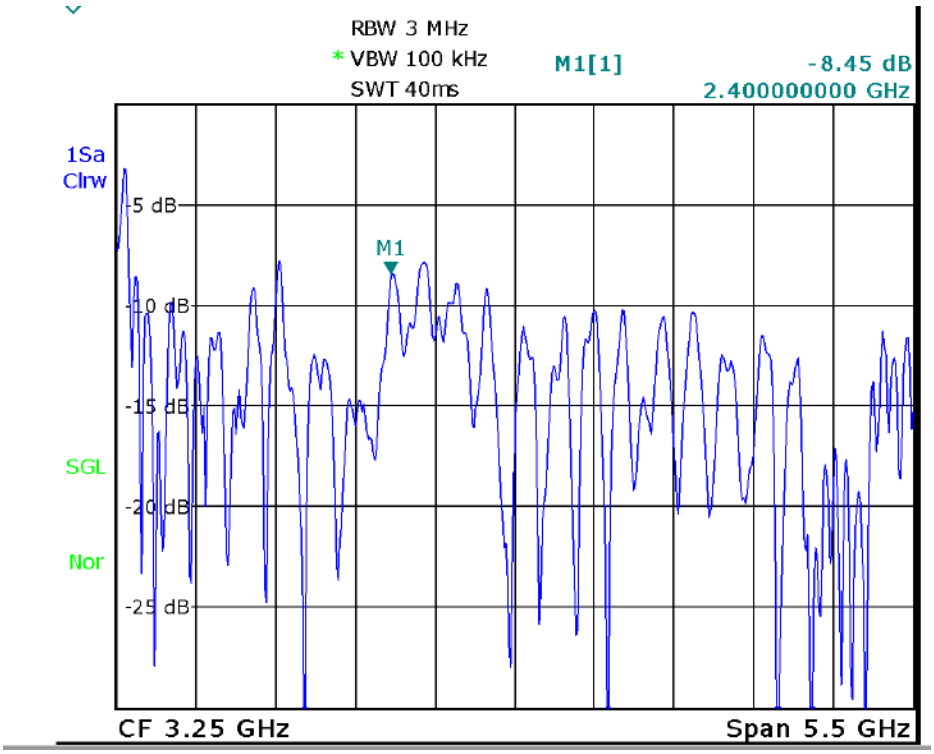
διέπονται από κανονισμούς περιορισμού εκπομπών τόσο στην Ευρώπη όσο και στην Αμερική. Στην Αμερική, η FCC Licence καθορίζει ότι η μέγιστη απόσταση εκπομπής Line of Sight του controller εκτείνεται στα 1000m με μέγιστη ισχύ εκπομπής στα 19dBm. Στην Ευρώπη η αντίστοιχη οδηγία περιορίζει την εκπομπή στα 500m με μέγιστη ισχύ εκπομπής στα 14dBm. Όπως παρουσιάσαμε και πιο πάνω, η κατευθυντική κεραία των 2.4GHz που θα χρησιμοποιηθεί έχει στη συχνότητα αυτή κέρδος (Gain) 11-12dBi. Άρα το σήμα που οδηγείται στην κεραία δεν πρέπει να ξεπερνά τα 2dBm για χρήση στην Ευρώπη και τα 7dBm για χρήση στην Αμερική. Στο κύκλωμα χρησιμοποιήσαμε LNA για την ενίσχυση του σήματος πριν το οδηγήσουμε στην κεραία. Ο τύπος ενισχυτή όμως του κυκλώματος αυτού ο οποίος περιγράφηκε και σε προηγούμενο κεφάλαιο, έχει κέρδος 18dB με μέγιστο σήμα εξόδου τα 17dBm. Ο λόγος είναι επειδή όλοι οι ενισχυτές έχουν ένα σημείο γνωστό και ως 1dB compression point που στην περίπτωση μας είναι τα 17dBm, πέρα από το οποίο υπάρχει κορεσμός στον ενισχυτή με αποτέλεσμα να μην λειτουργεί ως ενισχυτής και να γίνεται εξασθένηση του σήματος. Επίσης πέρα από το σημείο αυτό αρχίζουν να δημιουργούνται αρμονικές που επιδρούν καταστροφικά στο σήμα. Για να κρατήσουμε όμως το σήμα χαμηλά έτσι ώστε στον ενισχυτή να μην ξεπεραστεί το 1dB compression point, χρησιμοποιούμε ένα attenuator με απώλεια 5dB του τύπου που παρουσιάσαμε σε προηγούμενο κεφάλαιο, στοιχείο απαραίτητο στο κύκλωμα αφού η typical ισχύς εξόδου στον VCO της μπάντας των 2.4GHz είναι στα 7dBm.

Η πιο πάνω διάταξη εκτός από την μέγιστη αξιοποίηση της ισχύς μέσα στα επιτρεπόμενα όρια εκπομπής, μας δίνει τη δυνατότητα να προσαρμόσουμε την impendance όλου του κυκλώματος και την όσο το δυνατό επίτευξη καλύτερου δείκτη VSWR που θα έχει ως αποτέλεσμα την μέγιστη εμβέλεια λειτουργίας του συστήματος. Ο δείκτης VSWR (Voltage Standing Wave Ratio), που αναφέρεται και πολλές φορές ως SWR (Standing Wave Ratio), αποτελεί μέτρηση της προσαρμογής της impedance των φορτίων με την impedance της γραμμής μεταφοράς ή του κυματοδηγού. Αν υπάρχει mismatch τότε δημιουργείται στατικό κύμα (standing wave) κατά μήκος της γραμμής μεταφοράς λόγω της ανάκλασης του κύματος από την κεραία πίσω οδηγώντας σε απώλειες στο σήμα. Ο δείκτης SWR αποτελεί τον λόγο του πλάτους του standing wave σε σημείο όπου έχει μέγιστη τιμή με το πλάτος του σε σημείο που παίρνει ελάχιστη τιμή. Η τιμή αυτή αποτελεί πάντα μια θετική τιμή και όσο μικρότερη είναι τόσο καλύτερα προσαρμοσμένη είναι η κεραία προς τη γραμμή μεταφοράς και τόσο περισσότερη ισχύς παραδίδεται στην κεραία. Το ιδανικό είναι η επίτευξη SWR μοναδιαίας τιμής που σημαίνει ότι καθόλου ισχύς δεν ανακλάται από την κεραία προς τα πίσω. Κάθε μπάντα συχνοτήτων έχει κάποιο περιορισμό στον δείκτη VSWR. Στον πίνακα που ακολουθεί παρατηρούμε τη σχέση του

VSWR με το ποσό της ανακλώμενης ισχύς που αντιστοιχεί σε κάθε τιμή. Στα specification sheets κάθε κεραίας, παρατίθεται διάγραμμα που παρουσιάζει την πραγματική μέτρηση της κεραίας και τις τιμές της ανακλώμενης ισχύς στις διάφορες συχνότητες καθορίζοντας μας και το ιδανικό εύρος συχνοτήτων στις οποίες μπορούμε να τις χρησιμοποιήσουμε.



Διάγραμμα 8.5: Διάγραμμα που παρουσιάζει τη σχέση του VSWR με το ποσό της ανακλώμενης ισχύς που αντιστοιχεί σε κάθε τιμή για την κεραία Broad Band 2400-2480 Quad Patch



Διάγραμμα 8.6: Διάγραμμα που παρουσιάζει τη σχέση του VSWR με το ποσό της ανακλώμενης ισχύς που αντιστοιχεί σε κάθε τιμή για την κεραία PCB Log Periodic 850-6500

8.2.2 Ξύλινο Κουτί-Κέλυφος

Τόσο η πλακέτα όσο και τα υπόλοιπα μέρη του συστήματος πρέπει να είναι προσαρμοσμένα σε μια συμπαγής, προστατευτική κατασκευή έτσι ώστε να μπορούν να μεταφέρονται αλλά και να χρησιμοποιούνται ως ένα ενιαίο, ολοκληρωμένο σύστημα jammer. Μια τέτοια κατασκευή πρέπει να έχει κάποια χαρακτηριστικά τα οποία να επιτρέπουν την εύκολη χρήση του και στόχευση, τη μεταφορά, την προστασία των ευαίσθητων τμημάτων του (πλακέτα, καλωδιώσεις, signal generator), την προσβασιμότητα και την δυνατότητα μετατροπών και διορθώσεων. Παραδείγματα τέτοιων συστημάτων υπάρχουν αρκετά με πολλά από αυτά να έχουν την σχεδίαση ενός φορητού τυφεκίου το οποίο στοχεύει τον ιπτάμενο στόχο, άλλα με τη χρήση σακιδίου πλάτης το οποίο περιέχει το σύστημα μαζί με την τροφοδοσία του και την ύπαρξη handheld διάταξης κεραιών που στοχεύουν με τον προσανατολισμό του χεριού. Μερικά παραδείγματα εμφανίζονται στις πιο κάτω εικόνες.

Εικόνα 8.30: Jammer τύπου Drone Gun

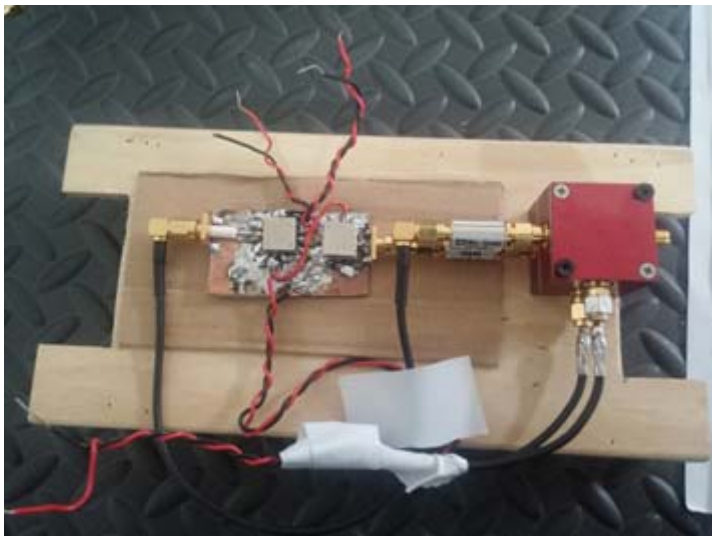
Εικόνα 8.31: Drone Jammer με φορητή κεραία

Εικόνα 8.32: Χρήση Drone Jammer με φορητή κεραία

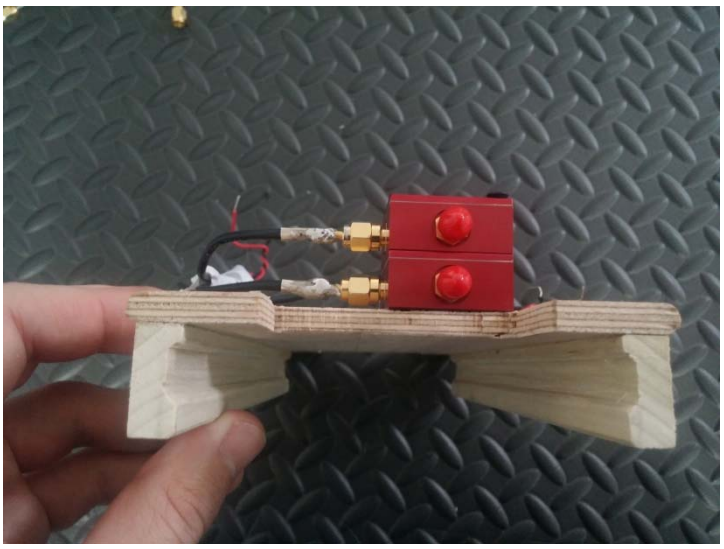
Η κατασκευή αυτή πρέπει να είναι ελαφριά και να μπορεί να κατασκευαστεί εύκολα, γρήγορα και οικονομικά. Αυτές τις δυνατότητες μας τις δίνει η χρήση λεπτού ξύλου κόντρα πλακέ. Όπως αναφέρθηκε και πιο πάνω υπάρχουν διάφοροι σχεδιασμοί τέτοιων συστημάτων, κυρίως υπό τη μορφή τυφεκίου αλλά στη συγκεκριμένη περίπτωση, τα διάφορα τμήματα που συναρμολογήθηκαν για να αποτελέσουν το σύστημα, δεν ευνοούσαν τέτοιας μορφής κατασκευή. Αποφασίστηκε ότι προτιμότερο θα ήταν να έχει τη μορφή φορητού κουτιού στο οποίο να βρίσκονται προσαρμοσμένα όλα τα στοιχεία συμπεριλαμβανομένης και της πηγής τροφοδοσίας. Οι κεραίες με αυτή τη σχεδίαση θα βρίσκονται σε διάταξη ξεχωριστής κατασκευή η οποία να μπορεί να χρησιμοποιηθεί με το χέρι όπως θα παρουσιαστεί και πιο κάτω.

Το σχετικά μεγάλο μέγεθος του signal generator μας περιορίζει όσον αφορά το συνολικό μέγεθος της ξύλινης κατασκευής. Η πλακέτα με το κύκλωμα καταλαμβάνει σχετικά μικρό χώρο έτσι το συνολικό μέγεθος της κατασκευής διαμορφώθηκε λαμβάνοντας υπόψη το μέγεθος της generator. Η ανάγκη για δυνατότητα πρόσβασης στο κύκλωμα οποιαδήποτε στιγμή, οδήγησε στη σχεδίαση που φαίνεται και πιο κάτω, όπου η πλακέτα βρίσκεται εφαρμοσμένη σε ξύλινη επιφάνεια η οποία εισέρχεται συρταρωτά στο εσωτερικό του κουτιού με τη χρήση οδηγών οι οποίοι σχηματίστηκαν με ειδικό εργαλείο στην εσωτερική πλευρά των πλευρικών επιφανειών. Η στερέωση του signal generator στην άλλη πλευρά της επιφάνειας που στερεώθηκε η πλακέτα, εξοικονομεί αρκετό χώρο και κάνει την πρόσβαση στο ηλεκτρονικό μέρος του συστήματος άμεση και πολύ εύκολη αφού με μια κίνηση αφαιρείται το κυρίως κομμάτι και ξανατοποθετείται.

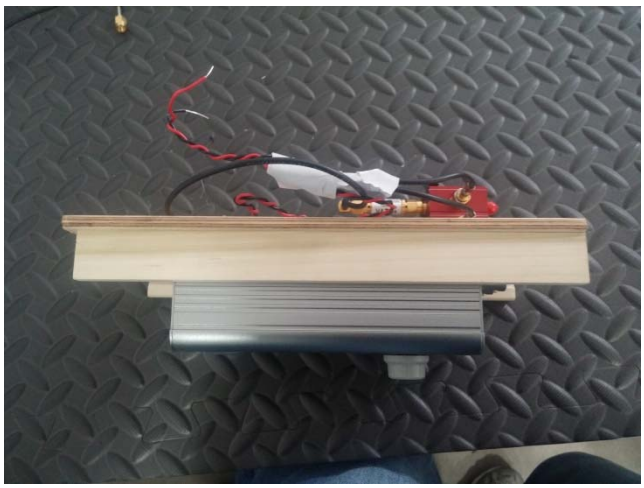
Επίσης για την δυνατότητα πρόσβαση στο εσωτερικό εφαρμόστηκε μικρή πόρτα στη μια πλευρά η οποία ασφαλίζει με μαγνήτη όπως φαίνεται στη φωτογραφία.



Εικόνα 8.33: Η τοποθέτηση και ασφάλιση της πλακέτας πάνω στη ξύλινη συρταρωτή βάση



Εικόνα 8.34: Πλάγια όψη της συρταρωτής βάσης όπου φαίνεται πάνω η εφαρμογή της πλακέτας και κάτω η θέση εφαρμογής της γεννήτριας σημάτων



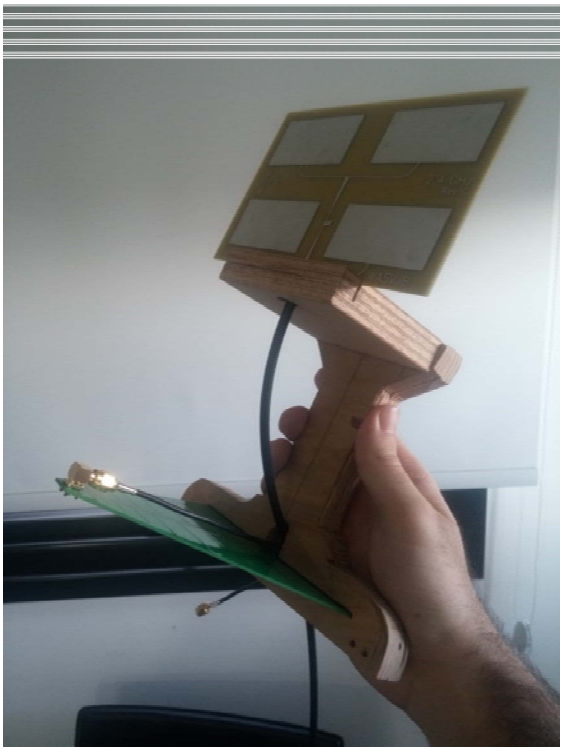
Εικόνα 8.36: Πλάγια όψη του συστήματος, που περιλαμβάνει την πλακέτα και την γεννήτρια σημάτων, εφαρμοσμένου σε ξύλινη συρταρωτή βάση

Εικόνα 8.37: Το εσωτερικό του ξύλινου κουτιού με το σύστημα εφαρμοσμένο και ασφαλισμένο

8.2.3 Antenna Holder

Η κατεύθυνση του jamming signal προς το στόχο, θα γίνεται όπως προαναφέραμε με τη χρήση 2 κατευθυντικών κεραιών. Αυτές θα προσαρμοστούν σε μια ξύλινη κατασκευή η οποία θα έχει διαμορφωμένη μια λαβή για τον χειρισμό και τον προσανατολισμό των κεραιών όπως φαίνεται πιο κάτω. Τα δύο σήματα που θα εκπέμπονται θα μεταφέρονται με SMA coaxial cables από την πλακέτα και με αυτό τον τρόπο το σύστημα ολόκληρο θα αποτελείται από τις δύο αυτές κατασκευές, το κουτί στο οποίο βρίσκεται η πλακέτα με το signal generator και η διάταξη των δύο κεραιών. Έτσι η χρήση του συστήματος θα γίνεται κρατώντας στο ένα χέρι το jammer generator και στο άλλο το antenna holder.

Όσον αφορά την προσαρμογή των 2 κεραιών, φροντίζουμε έτσι ώστε να μην έρχονται σε επαφή με το χέρι και να είναι στερεωμένες έχοντας τον ίδιο προσανατολισμό με τον λοβό να στοχεύει στην ίδια κατεύθυνση. Επίσης όσο μεγαλύτερο μέρος της κεραίας πρέπει να είναι ελεύθερο στον αέρα και να είναι στερεωμένες σε κάποιο σημείο στην άκρη για να μην επηρεάζεται η αποδοτικότητα της κεραίας. Αυτό γίνεται λόγω αύξησης της αντίστασης της κεραίας και εν συνεπεία μεταβολής του VSWR μειώνοντας την εμβέλεια του συστήματος. Ένας άλλος παράγοντας που μπορεί να επηρεάσει την αποδοτικότητα των κεραιών είναι η τοποθέτηση τους πολύ κοντά με τους δύο λοβούς να έχουν αρκετή αλληλοεπικάλυψη. Αυτή η εγγύτητα των δύο κεραιών μπορεί να οδηγήσει σε απώλειες με αποτέλεσμα η εμβέλεια του συστήματος να μειωθεί αρκετά. Γι αυτό το λόγω χρησιμοποιήθηκε στην προσαρμογή των κεραιών η διάταξη που φαίνεται πιο κάτω.



Εικόνα 8.38: Η εφαρμογή των δύο κεραιών σε ξύλινο handle και ο τρόπος χρήσης του

Οι κεραίες είναι και οι δύο κατευθυντικές με την κεραία της μπάντας των 2,4GHz να είναι πιο κατευθυντική δικαιολογώντας έτσι και το υψηλό Gain που ανέρχεται στα 11-12dBi όπως αναφέραμε σε προηγούμενο κεφάλαιο. Η κεραία Log Periodic 850-6500 που θα χρησιμοποιηθεί για τη μπάντα του GPS είναι wideband και συνεπώς έχει μικρότερη κατευθυντικότητα αλλά και συνεπώς και χαμηλότερο Gain που περιορίζεται στα 6dBi. Το χαμηλό Gain όμως της κεραίας

αυτής δεν μας προκαλεί πρόβλημα λόγω του αρκετά χαμηλότερου σε ισχύ σήματος που απαιτείται για να διακοπεί η σύνδεση στη μπάντα αυτή.

8.2.4 Τροφοδοσία Συστήματος

Τέλος, όσον αφορά την τροφοδοσία του συστήματος, όπως περιγράφηκε και πιο πάνω, θα τοποθετηθεί Power Bank δύο εξόδων. Αυτό μας δίνει τη δυνατότητα να κάνουμε το σύστημα πλήρως φορητό και αυτόνομο, χωρίς την απαίτηση ύπαρξης σημείου σύνδεσης σε δίκτυο ρεύματος. Τόσο το signal generator, όσο οι VCOs αλλά και οι Amplifiers, χρειάζονται τάση λειτουργίας 5V τα οποία μπορεί να μας δώσει το Power Bank. Η κατανάλωση ρεύματος από την άλλη, όπως μετρήθηκε στο εργαστήριο με τη χρήση Bench Power Supply, είναι λίγο πιο κάτω από 1Amp για το Signal generator και κοντά στα 0.65Amp για τη διάταξη της πλακέτας (VCOs και Amplifiers). Έτσι με τη χρήση ενός Power Bank στο οποίο οι έξοδοι του, όπως και στα περισσότερα στην αγορά, έχουν τη δυνατότητα παροχής τάσης 5V και ρεύματος 1-2.4A μπορούμε να καλύψουμε τις ανάγκες του συστήματος. Τα καλώδια μεταφοράς του ρεύματος από το Power Bank είναι αυτοσχέδια και έγιναν στο εργαστήριο έχοντας τις προδιαγραφές που αναφέρθηκαν και πιο πάνω.

Εικόνα 8.39: Τα δύο αυτοσχέδια καλώδια τροφοδοσίας του συστήματος τα οποία θα μεταφέρουν ρεύμα από το Power Bank

Η προσαρμογή του Power Bank στο σύστημα αποφασίστηκε να γίνει σε εξωτερικό σημείο στο κουτί και σε θέση που να μην επηρεάζει τη χρήση του. Έτσι θα μπορεί να γίνεται εύκολη και

γρήγορη αφαίρεση του για φόρτιση και προσαρμογή του πίσω στο σύστημα. Επίσης αυτή η θέση ευνοεί την ταχεία αποσύνδεση του από το σύστημα για λόγους ασφαλείας. Τέλος, οι κίνδυνοι εμφάνισης υψηλής θερμοκρασίας σε μια μπαταρία όπως αυτής ενός Power Bank αλλά και ο κίνδυνος ανάφλεξης, απαιτεί την τοποθέτηση του σε σημείο στο οποίο να αποφευχθεί η ολική καταστροφή του συστήματος.

Εικόνα 8.40: Πλάγια όψη του κουτιού όπου φαίνεται η θέση εφαρμογής του Power Bank και οι είσοδοι των καλωδίων τροφοδοσίας και των 2 antenna cables

Εικόνα 8.41: Εφαρμογή του Power Bank πάνω στο κουτί

Κεφάλαιο 9
Έλεγχος Συστήματος

9.1 Πειραματικοί Έλεγχοι στο εργαστήριο

Μετά την ολοκλήρωση του συστήματος, όπως παρουσιάστηκε στο προηγούμενο κεφάλαιο, ακολούθησαν μια σειρά από πειραματικούς ελέγχους στο εργαστήριο με σκοπό να αποδειχθεί όλο το concept της διατριβής αυτής. Η λειτουργικότητα και αποτελεσματικότητα του συστήματος μπορούν να επιβεβαιωθούν πάντα σε ένα εργαστήριο με ασφάλεια πριν να θεωρηθεί ότι είναι έτοιμο προς χρήση. Στο κεφάλαιο αυτό, το οποίο ολοκληρώνει τη διατριβή αυτή, γίνεται εργαστηριακή προσομοίωση της χρήσης του συστήματος σε drone, η οποία σκοπό έχει να επιβεβαιώσει την λειτουργικότητα του σε περίπτωση χρήσης του για αντιμετώπιση ενός drone σε μη ελεγχόμενο περιβάλλον.

Εικόνα 9.1: Το σύστημα Jammer μετά την ολοκλήρωση του

Τα εργαστηριακά πειράματα που έγιναν, έλεγξαν τις ακόλουθες δύο κύριες δυνατότητες του συστήματος.

1. Δυνατότητα διακοπής της σύνδεσης του drone με το σύστημα δορυφόρων GPS.

2. Δυνατότητα διακοπής της σύνδεσης Wi-Fi του drone με το χειριστή του.

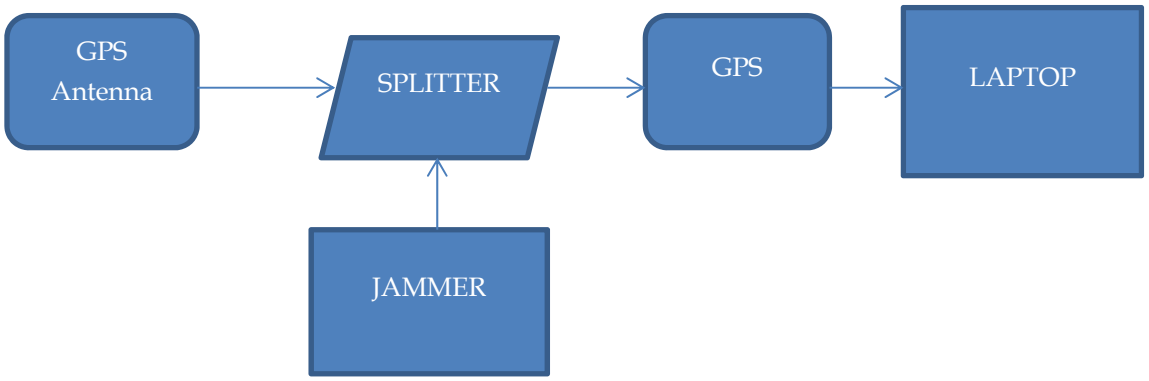
Για την επιβεβαίωση των πιο πάνω χρησιμοποιήθηκε στο εργαστήριο κλωβός υφάσματος YShield ο οποίος παρέχει EMR μόνωση στο εσωτερικό του. Ο κλωβός αυτός, ο οποίος φαίνεται στην πιο κάτω εικόνα, αποτελείται από πλαστικό πτυσσόμενο σκελετό, πάνω στον οποίο εφαρμόζεται το ειδικό ύφασμα το οποίο έχει την ιδιότητα της εξασθένησης σήματος κατά 30dB. Στις δύο γωνιές του υπάρχουν δύο είσοδοι-έξοδοι τύπου μανίκια, οι οποίες χρησιμοποιούνται για την διέλευση καλωδίων για έλεγχο του εξοπλισμού που βρίσκεται στο εσωτερικό. Με αυτό τον τρόπο παρέχεται η δυνατότητα πλήρους χειρισμού των συσκευών που βρίσκεται στο εσωτερικό με εκπομπές EMR οι οποίες περιορίζονται στο εσωτερικό του κλωβού χωρίς να εκπέμπονται στον ελεύθερο χώρο λόγω αδυναμίας διείσδυσης στο ύφασμα που τον περιβάλλει.

Εικόνα 9.2: Ο πτυσσόμενος κλωβός με το Yshield ύφασμα που παρέχει EMR insulation

Εικόνα 9.3: Το εσωτερικό του κλωβού. Η μπροστινή πλευρά όπως φαίνεται στην εικόνα σφραγίζει το εσωτερικό με φερμουάρ

9.1.1 Jamming σε σήμα GPS

Για την επιβεβαίωση της δυνατότητας jamming σε GPS σχεδιάστηκε η πιο κάτω διάταξη η οποία στη συνέχεια υλοποιήθηκε.



Σχήμα 9.1: Σχηματική απεικόνιση της διάταξης Jamming σε GPS Signal

Όπως φαίνεται και στο σχήμα, χρησιμοποιήθηκε GPS στο οποίο συνδέθηκε συσκευή splitter και στις εισόδους της οποίας συνδέθηκαν τόσο το jammer, όσο και μια κεραία GPS. Ακολούθως το GPS έτρεξε σε λογισμικό σε υπολογιστή Laptop όπου έγινε ανάκτηση των NMEA strings του σημείου της κεραίας. Μετά την επιβεβαίωση καλής λήψη σήματος από τα NMEA strings έγινε ενεργοποίηση του jammer του οποίου το σήμα μέσω καλωδίου τροφοδοτείτο στο splitter στο οποίο έφτανε και το σήμα από το GPS. Αμέσως παρατηρήθηκε αδυναμία ανάκτησης των strings αφού το jamming signal είχε μειώσει αρκετά το SNR διακόπτοντας τη σύνδεση του συστήματος GPS.

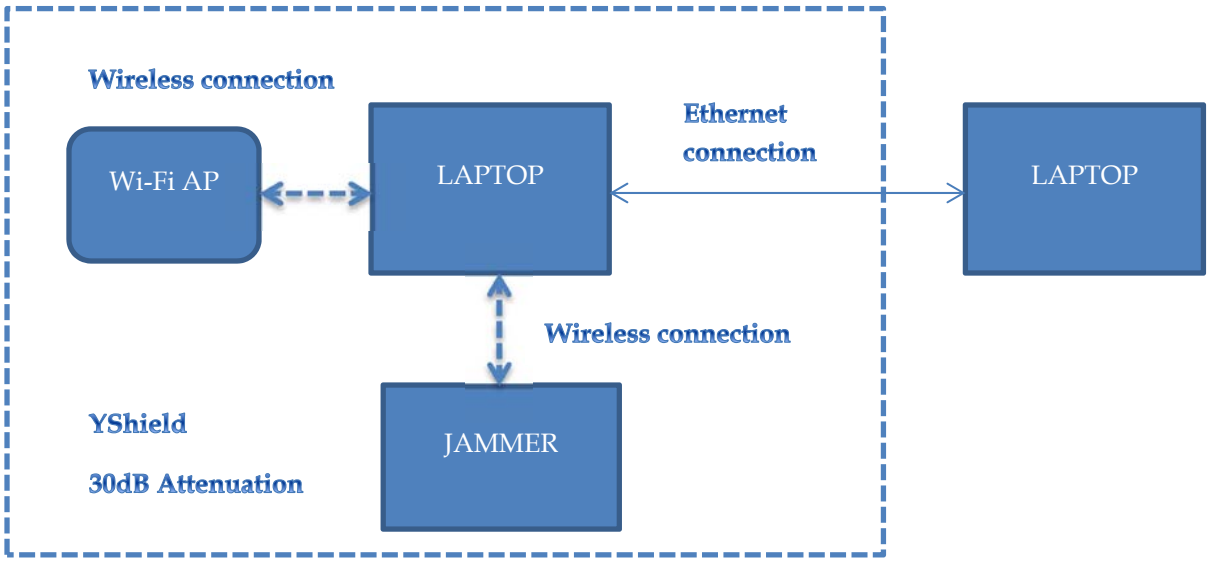
Στο πείραμα αυτό δεν χρειάστηκε να χρησιμοποιηθεί ο EMR Shield κλωβός αφού δεν έγινε καμιά εκπομπή σήματος. Το jamming signal για την μπάντα του GPS μεταφέρθηκε στο GPS, μέσω καλωδίου και διαμέσου του splitter.

Πιο κάτω φαίνεται η υλοποίηση της διάταξης που σχεδιάστηκε για επιβεβαίωση της δυνατότητας διακοπής της σύνδεσης GPS όπως παρουσιάστηκε και στο σχήμα που προηγήθηκε.

Εικόνα 9.4: Απεικόνιση της διάταξης υλοποίησης Jamming σε GPS Signal

9.1.2 Jamming σε σήμα Wi-Fi

Όπως προαναφέρθηκε, η σύνδεση του χειρίστη με το drone γίνεται με τη χρήση επικοινωνίας Wi-Fi στην μπάντα των 2,4GHz. Ένας ασφαλής τρόπος επιβεβαίωσης της δυνατότητας διακοπής της σύνδεσης αυτής, είναι με την προσομοίωση σε μια σύνδεση ενός υπολογιστή με ένα Wi-Fi Access Point. Μπορούμε έτσι πολύ εύκολα να δούμε αν με την ενεργοποίηση του Jammer ο υπολογιστής, ο οποίος θα ανταλλάζει πακέτα με ένα αποστολέα κατά την εκτέλεση μιας ασφαλούς διαδικτυακής σύνδεσης https, σταματήσει να ανταλλάζει πακέτα. Αυτή την διεργασία μπορούμε να τη δούμε πολύ εύκολα με τη χρήση ενός γνωστού network analyzer λογισμικού. Το εργαλείο αυτό είναι το Wireshark. Όπως φαίνεται στο σχήμα πιο κάτω, η διάταξη που σχεδιάστηκε περιλάμβανε το Access Point, το Jammer και ένα υπολογιστή laptop.



Σχήμα 9.2: Σχηματική απεικόνιση της διάταξης Jamming σε Wi-Fi Signal

Σκοπός ήταν να δούμε αν με την ενεργοποίηση του το jammer θα μπορούσε να μειώσει τόσο πολύ το SNR, έτσι ώστε να διακοπεί τελείως η σύνδεση του υπολογιστή με το Access Point. Σύμφωνα με τη θεωρία των Ψηφιακών Επικοινωνιών, το σήμα που εκπέμπεται από ένα Access Point μπορεί να υποστηρίξει ταχύτητες μετάδοσης δεδομένων οι οποίες εξαρτώνται από τη διαμόρφωση του φέροντος σήματος. Όπως παρουσιάστηκε πιο αναλυτικά στο 6ο Κεφάλαιο, κάθε τεχνολογία 802.11 μπορεί να προσφέρει συγκεκριμένες εξειδικευμένες διαμορφώσεις και συνεπώς ταχύτητες δεδομένων οι οποίες όμως καθορίζονται από το minimum sensitivity στο δέκτη. Όσο πιο ψηλό είναι, τόσο πιο εξειδικευμένη διαμόρφωση εκτελείται και έτσι επιτυγχάνονται μεγάλες ταχύτητες. Με την ύπαρξη όμως ενός Jamming Signal, το SNIR πέφτει με αποτέλεσμα η σύνδεση να αναγκάζεται να ρίξει τη διαμόρφωση της σε χαμηλότερο επίπεδο προσπαθώντας να μείνει "ζωντανή". Έτσι αναγκαστικά πέφτει σημαντικά η ταχύτητα της σύνδεσης και αν το Jamming Signal είναι αρκετά ισχυρό τότε η σύνδεση αφού φτάσει στο χαμηλότερο επίπεδο διαμόρφωσης, διακόπτεται πλήρως.

Η πιο πάνω διάταξη αναγκαστικά υλοποιήθηκε μέσα στον κλωβό για τον περιορισμό της ακτινοβολίας στο εσωτερικό του και αποτροπής εκπομπής σήματος έξω από αυτόν. Όλα τα τμήματα τοποθετήθηκαν μέσα και με τη χρήση καλωδίου Ethernet, έγινε σύνδεση remote desktop με το laptop που βρισκόταν μέσα στον κλωβό έτσι ώστε να μπορούμε να βλέπουμε τα αποτελέσματα της εκτέλεσης του Wireshark. Στις εικόνες που ακολουθούν βλέπουμε τη διάταξη που παρουσιάστηκε στο σχήμα προηγουμένως, πριν την ενεργοποίηση του Jammer και την εκτέλεση του πειράματος. Σημειώνεται επίσης ότι κατά την εκτέλεση του πειράματος, η κεραία

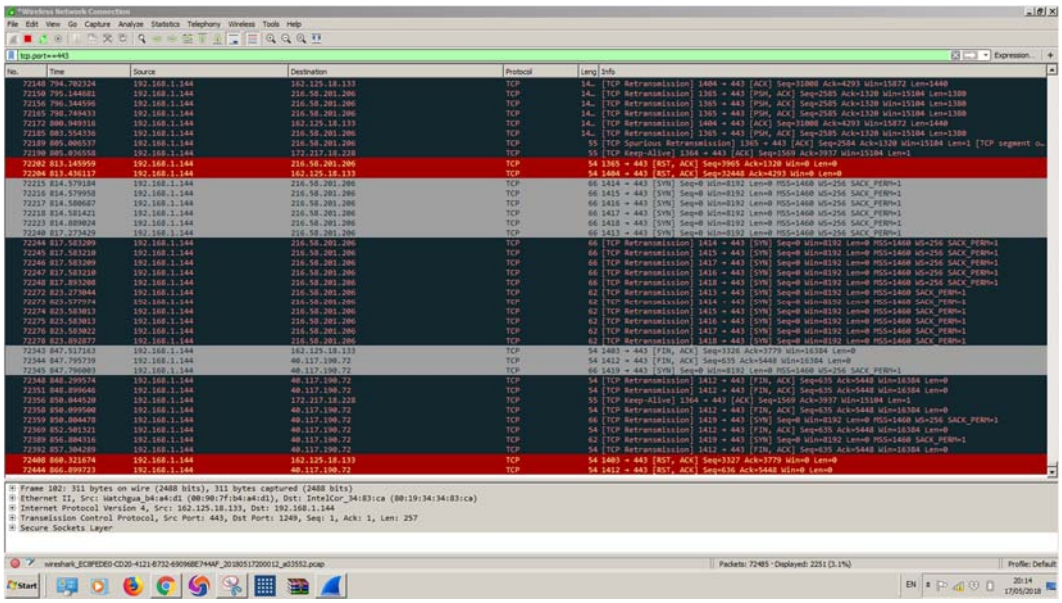
Wi-Fi του Jammer που βλέπουμε στην εικόνα αντικαταστάθηκε από μικρή, χαμηλότερου Gain έτσι ώστε να μειωθεί η ισχύς του σήματος το οποίο σε τέτοιο περιορισμένο χώρο και με τις αποστάσεις αυτές θα μπορούσε να καταστρέψει τόσο το Access Point όσο και το Laptop.

Εικόνα 9.5: Απεικόνιση της διάταξης υλοποίησης Jamming σε Wi-Fi Signal με τη χρήση του EMR Insulation κλωβού

Εικόνα 9.6: Το σημείο διέλευσης των SMA Cables τα οποία μεταφέρουν το Jamming Signal στο εσωτερικό του κλωβού

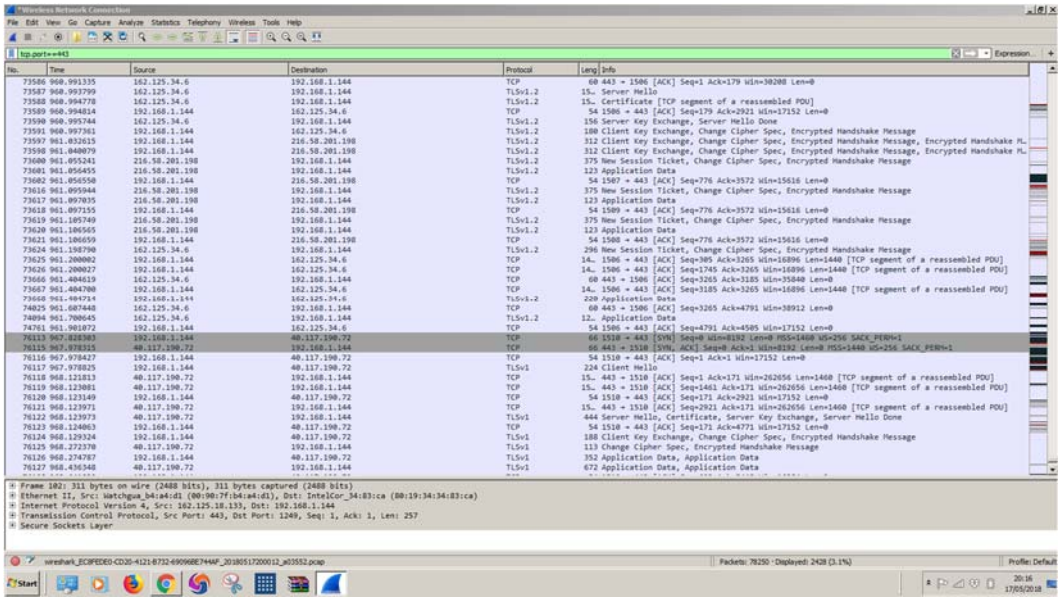
Για την εκτέλεση του πειράματος αυτού, αφού συνδέθηκε ο υπολογιστής στο Access Point, τρέξαμε μια συνεχή σύνδεση την οποία μπορούσε να μας την προσφέρει μια εκτέλεση ενός

βίντεο στο YouTube. Στη συνέχεια παρακολουθούσαμε στο Wireshark την κατάσταση της σύνδεσης σε πραγματικό χρόνο, φιλτράροντας στον πίνακα των live αποτελεσμάτων το tcp port 443. Έτσι μπορούσαμε να παρακολουθήσουμε την ανταλλαγή των πακέτων μέσα από την "συνομιλία" των δύο μερών της σύνδεσης. Ακολούθως αφού ενεργοποιήθηκε το Jammer στην μπάντα των 2,4GHz, είδαμε την σύνδεση να διακόπτεται και τα αποτελέσματα στο Wireshark να το επιβεβαιώνουν. Όπως φαίνεται και στην εικόνα που ακολουθεί η Source αποστέλλει συνεχώς την εντολή Retransmission ζητώντας επανάληψη της αποστολής των πακέτων επιβεβαιώνοντας την διακοπή στη σύνδεση και την αδυναμία λήψης πακέτων.



Εικόνα 9.7: Τα αποτελέσματα σε πραγματικό χρόνο στο Wireshark μετά την ενεργοποίηση του Jammer. Παρατηρούμε τη συνεχή αποστολή της εντολής Retransmission αλλά και την ένδειξη διακοπής της σύνδεσης κάτω δεξιά στην οθόνη του υπολογιστή

Ακολούθως απενεργοποιήθηκε το Jammer και επιβεβαιώσαμε ότι η σύνδεση επανήλθε παρατηρώντας ξανά στο Wireshark την συνομιλία μεταξύ Source και Destination όπως φαίνεται και στην εικόνα που ακολουθεί.



Εικόνα 9.8: Τα αποτελέσματα σε πραγματικό χρόνο στο Wireshark μετά την απενεργοποίηση του Jammer. Παρατηρούμε την επαναφορά στην ανταλλαγή πακέτων αλλά και την ένδειξη ύπαρξης σύνδεσης κάτω δεξιά στην οθόνη του υπολογιστή

Κεφάλαιο 10
Συμπεράσματα

Η ραγδαία εξάπλωση και η ανεξέλεγκτη χρήση των drones στις μέρες σαφώς αποτελούν ένα τεράστιο κίνδυνο για την ασφάλεια τόσο των ανθρώπων όσο και κρατικών και ιδιωτικών περιουσιών. Οι διάφορες προσπάθειες για έλεγχο αυτής της νέας τεχνολογίας και περιορισμό των ανεπιθύμητων καταστάσεων που μπορούν να προκληθούν από την κακόβουλη χρήση τους δεν είχαν τα αναμενόμενα αποτελέσματα. Η θέσπιση νομοθεσιών και η έκδοση οδηγιών και διαταγμάτων μπορούν να ελέγξουν ως ένα σημείο την απειλή, όμως όπως έχει αποδειχθεί μέχρι στιγμής δεν είναι αρκετό για να καθησυχάσουν τους φόβους από την ανορθόδοξη χρήση τους ή και την εκούσια, και σε κάποιες φορές ακούσια, πρόκληση ζημιών και καταστροφών.

Η διατριβή αυτή επιχείρησε να εξετάσει τη δυνατότητα αποτελεσματικής αντιμετώπισης των πιο πάνω ανησυχιών προτείνοντας ένα low-cost, ολοκληρωμένο σύστημα απενεργοποίησης drone το οποίο να μπορεί κατασκευαστεί εύκολα από υλικά που βρίσκονται στην αγορά. Η ολοκλήρωση και δοκιμή του συστήματος αυτού οδήγησε στην εξαγωγή χρήσιμων συμπερασμάτων τα οποία και παρατίθενται πιο κάτω.

- Το κυριότερο και γενικότερο συμπέρασμα είναι ότι είναι εφικτή η δυνατότητα ανάπτυξης αποτελεσματικού συστήματος εύκολα, γρήγορα και φθηνά το οποίο να μπορεί να αντιμετωπίσει τους κινδύνους που εγκυμονεί η μαζική και ανεξέλεγκτη χρήση των drones.

- Είναι πλέον εφικτή η προστασία ιδιωτικών ή δημόσιων περιοχών και εγκαταστάσεων από την άνευ άδειας προσέγγιση ή και παράνομης κινηματογράφησης από τέτοια συστήματα. Ευαίσθητες εγκαταστάσεις και περιοχές υψηλής ασφαλείας μπορούν πλέον να λύσουν ένα μεγάλο πρόβλημα που τις ταλανίζει τα τελευταία χρόνια και το οποίο αδυνατούσαν να αντιμετωπίσουν αποτελεσματικά.

- Αποδείχθηκε ότι έχοντας εις βάθος γνώση της επιστημονικής θεωρίας των Ασύρματων Επικοινωνιών, μπορείς αρχικά να καταλάβεις τον τρόπο με τον οποίο λειτουργούν τέτοια συστήματα drones και ακολούθως να εντοπίσεις τις ευπάθειες τους κάνοντας πλέον πιο εύκολο τον προσδιορισμό του τρόπου αντιμετώπισης τους.

- Επιβεβαιώνεται επίσης ότι όσο εξελιγμένη και να είναι μια τεχνολογία, θα έχει πάντα κάποιες αδυναμίες οι οποίες να μπορούν να τύχουν εκμετάλλευσης.

- Ένα τέτοιο σύστημα όπως αυτό που μελέτησε η Διατριβή αυτή, μπορεί να χρησιμοποιηθεί για την ασφάλεια ανθρώπινων ζωών, περιουσιών και εγκαταστάσεων αλλά στα λάθος χέρια μπορεί να αποτελέσει ένα πολύ επικίνδυνο όπλο που να έχει ακριβώς αντίθετα αποτελέσματα. Μια τέτοια τεχνολογία πρέπει να αναπτύσσεται και να διανέμεται με εξαιρετική προσοχή και αφού καθοριστεί προσεκτικά και επιβεβαιωθεί η σωστή χρήση της.

- Ως πιο ειδικό συμπέρασμα αποτελεί η απόδειξη μέσα από πειραματικούς εργαστηριακούς ελέγχους η δυνατότητα διακοπής της σύνδεσης ενός δέκτη με το σύστημα GPS προσθέτοντας στο Link Budget την απαραίτητη ισχύ Noise Signal το οποίο να έχει επίδραση στην ισχύ του σήματος στο δέκτη. Αντίστοιχη επιβεβαίωση έγινε και για την επικοινωνία Wi-Fi με πραγματοποίηση εργαστηριακής διεργασίας πλήρους διακοπής της σύνδεσης προσομοιώνοντας έτσι την διακοπή της επικοινωνίας μεταξύ ενός drone και του χειριστή του.

- Η απόδειξη της δυνατότητας διακοπής των δύο αυτών τεχνολογιών επικοινωνιών σε εργαστηριακό περιβάλλον χρησιμοποιώντας το σύστημα απενεργοποίησης το οποίο αναπτύχθηκε, επιβεβαίωσε την αρχική υπόθεση της Διατριβής αυτής. Το PoC (Proof of Concept) συνεπώς είναι αυτό που μας δίνει τη δυνατότητα μετά βεβαιότητας να προτείνουμε το σύστημα που αναπτύχθηκε στη διατριβή αυτή του οποίου πλέον η αποτελεσματική εφαρμογή του σε οποιοδήποτε drone και σε οποιοδήποτε σενάριο απόστασης αποτελεί θέμα ισχύος (Link Budget).

Κεφάλαιο 11
Επίλογος

Αποτελεί πλέον αδιαμφισβήτητο γεγονός ότι η τεχνολογία των drones έχει μπει για τα καλά στην καθημερινότητα των σημερινών ανθρώπων. Κάτι που φάνταζε κάποτε ως επιστημονική φαντασία, σήμερα αποτελεί κάτι συνηθισμένο λόγω της ταχέως εξελισσόμενης τεχνολογίας. Όπως το αυτοκίνητο κάποτε, στη συνέχεια η τηλεόραση και το κινητό τηλέφωνο και ακολούθως ο ηλεκτρονικός υπολογιστής, το drone από μια ευφυής ανακάλυψη για λίγους που ήταν κάποτε, σήμερα κατασκευάζεται και πωλείται τόσο φθηνά και μαζικά που ο καθένας θεωρεί ότι αποτελεί μια τεχνολογία που σίγουρα θα δοκιμάσει.

Όπως σε όλες τις επαναστατικές τεχνολογίες που εμφανίζονται κατά καιρούς, έτσι και σε αυτή, οι τρομερές λειτουργίες της και οι δυνατότητες που προσφέρει εγκυμονούν κινδύνους και μπορεί πάντα στα λάθος χέρια να έχουν πολύ αρνητικές συνέπειες. Ήδη η συγκεκριμένη τεχνολογία, όπως αναφέρθηκε και στη διατριβή αυτή, έχει χρησιμοποιηθεί τόσο εκούσια όσο και ακούσια προκαλώντας καταστροφικά αποτελέσματα καθιστώντας πλέον τον κίνδυνο από την ανεξέλεγκτη χρήση των drones προτεραιότητα τα τελευταία χρόνια. Η θέσπιση κανόνων και

οδηγιών για τη χρήση μπορεί να έβαλε μια τάξη όσον αφορά τη χρήση αλλά το πρόβλημα δύσκολα αντιμετωπίζεται χωρίς πραγματικά αντίμετρα.

Όπως αναλύθηκε και παρουσιάστηκε στη διατριβή αυτή, έχοντας εις βάθος γνώση των τεχνολογιών και του τρόπου λειτουργίας τέτοιων εξοπλισμών, μπορείς να εντοπίσεις τις αδυναμίες και τα τρωτά σημεία στα οποία να στοχεύσεις για να αντιμετωπίσεις αποτελεσματικά τους κινδύνους που ενέχονται. Αυτός ήταν και ο σκοπός της διατριβής που επιβεβαιώθηκε μέσα από μια διαδικασία αρχικά μελέτης του drone και των τεχνολογιών του, στη συνέχεια προσδιορισμού των αδυναμιών του και τέλος ανάπτυξης και επιτυχούς δοκιμής ενός συστήματος απενεργοποίησης.

Βιβλιογραφία

[1] B. Rao, A. G. Gopi, and R. Maione, “The societal impact of commercial drones,” *Technol. Soc.*, vol. 45, pp. 83–90, 2016.

[2] R. Clarke, “Understanding the drone epidemic,” *Comput. Law Secur. Rev.*, vol. 30, no. 3, pp. 230–246, 2014.

[3] PETER LA FRANCHI, “Kinshasa UAV accident highlights need for standards development,” 2006. [Online]. Available: https://www.flightglobal.com/news/articles/kinshasa-uav-accident-highlights-need-for-standards-209768/.

[4] Paul Marks, “One Per Cent: GPS loss kicked off fatal drone crash,” 2012. [Online]. Available: https://www.newscientist.com/blogs/onepercent/2012/05/gps-loss-kicked-off-fatal-dron.html.

[5] SPIEGEL, “Drohne "Luna": Bundeswehr verheimlicht Beinahe-Crash mit Airbus - SPIEGEL ONLINE,” 2013. [Online]. Available: http://www.spiegel.de/politik/deutschland/drohne-luna-bundeswehr-verheimlicht-beinahe-crash-mit-airbus-a-903337.html.

[6] Allie Coyne, “Drone almost collides with Westpac Rescue chopper - Hardware - iTnews,” 2014. [Online]. Available: https://www.itnews.com.au/news/drone-almost-collides-with-westpac-rescue-chopper-380875.

[7] Kontominas, “Mystery drone collides with Sydney Harbour Bridge,” 2013. [Online]. Available: http://www.smh.com.au/nsw/mystery-drone-collides-with-sydney-harbour-bridge-20131004-2uzks.html.

[8] Crozier, “CASA blasts ‘irresponsible’ drone bushfire flyover - Hardware - iTnews,” 2013. [Online]. Available: https://www.itnews.com.au/news/casa-blasts-irresponsible-drone-bushfire-flyover-361940.

[9] R. Clarke, “The regulation of civilian drones’ impacts on behavioural privacy,” *Comput. Law Secur. Rev.*, vol. 30, no. 3, pp. 286–305, 2014.

[10] BBC, “Police drone crashes into River Mersey - BBC News,” 2011. [Online]. Available: http://www.bbc.com/news/uk-england-merseyside-15520279.

[11] Mark Corcoran, “Drone journalism takes off,” 2012.

[12] Sam Biddle, “Police Drone Crashes Into Police | Gizmodo Australia,” 2012. [Online]. Available: https://www.gizmodo.com.au/2012/03/police-drone-crashes-into-police/.

[13] P. Naresh, P. R. Babu, and K. Satyaswathi, “Mobile Phone Signal Jammer for GSM , CDMA with Pre-scheduled Time Duration using ARM7,” vol. 2, no. 9, pp. 1781–1784, 2013.

[14] S. Ballantyne, “Wireless Communication Security : Software Defined Radio-based Threat Assessment Wireless Communication Security : Software Defined Radio-based Threat Assessment . by,” 2016.

[15] U. Office of Research, *Radio Free Europe archive documents*. United States Information Agency, 1983.

[16] “ARCHIVE DOCUMENTS,” *www.radiojamming.info*, 2012.

[17] Wikipedia, “No Title.” [Online]. Available: https://en.wikipedia.org/wiki/Radio_jamming.

[18] R. Pleikys, “JAMMING BY THE FREE WORLD,” *JAMMING by Rimantas Pleikys*, p. 11, 2012.

[19] Scott Peterson, “Exclusive: Iran hijacked US drone, says Iranian engineer - CSMonitor.com,” 2011. [Online]. Available: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer.

[20] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: a survey,” *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, p. 197, 2014.

[21] C. Gencer, E. K. Aydogan, and C. Celik, “A decision support system for locating VHF/UHF radio jammer systems on the terrain,” *Inf. Syst. Front.*, vol. 10, no. 1, pp. 111–124, 2008.

[22] K. Pelechrinis, M. Iliofotou, and S. V Krishnamurthy, “Denial of Service Attacks in Wireless Networks : The Case of Jammers,” vol. 13, no. 2, pp. 245–257, 2011.

[23] M. L. Cummings, S. Bruni, S. Mercier, and P. J. Mitchell, “Decision Support for Network-Centric Command and Control,” *Int. C2 J.*, vol. 1, no. 2, pp. 1–24, 2007.

[24] “Drone startups swoop up millions - Jan. 7, 2015,” 2015. [Online]. Available: http://money.cnn.com/2015/01/07/technology/ghost-drone/.

[25] B. Vergouw, H. Nagel, G. Bondt, and B. Custers, “The Future of Drone Use,” vol. 27, pp. 21–46, 2016.

[26] “Top 12 Professional Drones of 2018: Buy Professional Drones Now,” 2017. [Online]. Available: https://uavcoach.com/professional-drones/.

[27] “All you need to know about frequencies on which drones operate,” 2017. [Online]. Available: https://www.jammer-store.com/drones-frequencies.html.

[28] B. Haltli, P. Ewing, and H. Williams, “Global navigation satellite system (GNSS) and area navigation (RNAV) benefiting general aviation,” *AIAA/IEEE Digit. Avion. Syst. Conf. - Proc.*, vol. 2, pp. 1–39, 2005.

[29] “INFORMATION-ANALYTICAL CENTER of coordinate-time and navigation support,” 2017. [Online]. Available: https://www.glonass-iac.ru/ICD02_e.pdf.

[30] “History of GPS - Mio Technology,” 2017. [Online]. Available: http://www.mio.com/technology-history-of-gps.htm.

[31] “GPS: The Global Positioning System,” 2017. [Online]. Available: https://www.gps.gov/.

[32] “GPS.gov: New Civil Signals,” 2017. [Online]. Available: https://www.gps.gov/systems/gps/modernization/civilsignals/.

[33] M. Ahrens, “Gps and Wireless Signal Jamming : AT TACKS AND DEFENSES,” pp. 1–11, 2014.

[34] D. Borio, C. O’Driscoll, and J. Fortuny, “Jammer impact on Galileo and GPS receivers,” *2013 Int. Conf. Localization GNSS, ICL-GNSS 2013*, 2013.

[35] “Jammer Enforcement | Federal Communications Commission,” 2017. [Online]. Available: https://www.fcc.gov/general/jammer-enforcement.

Παράρτημα Α

Στο Παράρτημα της Διατριβής αυτής παρατίθενται:

1. Το διάταγμα του Υπουργείου Συγκοινωνιών, Επικοινωνιών και Έργων της Κυπριακής Δημοκρατίας όπως παρουσιάστηκε και στο Κεφάλαιο 4 της Διατριβής αυτής.

2. Σχηματική Απεικόνιση του ολοκληρωμένου συστήματος Jammer που αναπτύχθηκε στα πλαίσια της Διατριβής αυτής, όπου φαίνονται τα διάφορα τμήματα του.

A.1 UAVs Decree

Note: The following is not an official legal translation of the Ministerial Decree. Where disparity occurs, the original Greek text is binding.

Cyprus Government Gazette III (I) **Statutory Instrument 402/2015**
No. 4907, 27.11.2015
No.402

Civil Aviation Act 2002 (as amended)

Ministerial Decree Issued in accordance with Articles 5 (1) and 260.

In accordance with Articles 5 (1) and 260 of the Civil Aviation Act 2002 (as amended) and the powers vested in him, the Minister of Transport, Communications and Works issues the following Decree:

1. This Decree shall be referred to as the Civil Aviation Decree, (Conditions for the Operation of Flights by Unmanned Aerial Vehicles in the Republic of Cyprus) 2015.

2-(1) In accordance with this Decree and unless a different meaning arises from the text, the following terms apply:

Competent Authority: Means the Department of Civil Aviation of the Ministry of Transport, Communications and Works.

Republic: Means the Republic of Cyprus.

Commercial Activity: Means the activity for which valuable consideration is expected. The only exceptions are charitable activities which are carried out on a non-profit basis for the benefit of an approved charity.

Unmanned Aerial Vehicles: Means unmanned aircraft, including all remotely-piloted and autonomous aircraft, irrespective of their total take-off mass.

Aeromodelling Air-strip: Means a landing strip which has been approved by the Competent Authority and which is used for air-sports or recreational purposes by unmanned aircraft.

Law: Means the Civil Aviation Act 2002 (as amended).

Minister: Means the Minister of Transport, Communications and Works.

(2) Any other terms, included in this Decree which are not specifically defined herewith, are to be defined according to the Civil Aviation Act 2002 (as amended).

3-(1) The purpose of the present Decree, is to contribute to the safe and effective operation of unmanned aircraft under specific conditions.

(2) Unmanned aircraft, operating within Approved Aeromodelling Sites, as well as unmanned aircraft with a total take-off mass of more than 150 kg, are exempt from the provisions of this Decree.

4. Every unmanned aircraft should be registered by its owner and/ or operator at the following e-mail address: uav@dca.mcw.gov.cy, by providing the information required by document DCA/UAV/01.

5. Flight operation of unmanned aircraft, is divided into two categories: The Open Category and the Special Category.

6-(1) Open Category
This includes unmanned aircraft, having a total take-off mass of less than three (3) kilogrammes, which are not involved in commercial activities, and whose maximum flight-height does not exceed 50 meters (170 feet) above the ground or water.

(2) Unmanned aircraft that fall into the Open Category are not required to hold an Operating License from the Competent Authority, in order to operate flights within the airspace of the Republic of Cyprus.

(3) The flight safety of unmanned aircraft, operating in the Open Category, is safeguarded through specific operational restrictions and regulations. All flight operations of such aircraft shall be carried out in accordance with the following defined conditions:

i. Flights are not permitted unless the operator has direct visual contact with the unmanned aircraft, at a distance of not more than 500 metres. The operator must rely on this visual contact to carry out any necessary operating actions, in order to monitor the flight path of the aircraft in relation to other aircraft, persons, animals, vehicles, buildings and structures for the purpose of avoiding collisions.

ii. The operator is only allowed to carry out flights in the Open Category, with an unmanned aircraft of a total take off-mass of less than 3 kg and which is used for recreational, sports, training, display or racing purposes and which does not involve any kind of commercial activity.

iii. The operator has undergone the necessary training to be able to operate the unmanned aircraft.

iv. The operator of the unmanned aircraft is only allowed to fly the aircraft during the daytime and when reasonably satisfied that the flight can be conducted safely and will immediately interrupt the flights when conditions become unsuitable.

v. Dropping of any object or material during the flight is prohibited.

vi. The operator of the unmanned aircraft shall not operate a flight whilst under the influence of alcohol and psychotropic drugs that may impair his/her judgement and cognitive reasoning.

vii. The operator of the unmanned aircraft, is not allowed to operate flights with more than one aircraft at the same time.

viii. A safety distance of one (1) kilometre from residential areas and five hundred (500) metres from isolated buildings, people, vehicles, animals, structures, etc (except with the permission of the owner), should be maintained. This does not apply to the operator, supporting staff, vehicles or other auxiliary apparatus that serve the flight.

ix. A safety distance of at least eight (8) kilometres from an airport/landing strip and three (3) kilometres from a heliport shall be maintained.

x. Flights within prohibited, restricted, dangerous and reserved areas as mentioned in the relevant aeronautical publications of the Competent Authority, as well as flights above, within, or in proximity to military

installations, public utility installations, archaeological sites and public or private facilities, are not permitted, except with the permission of the owner or the relevant Competent Authority.

xi. Aerial Photography of National Guard installations and infrastructure is strictly prohibited.

xii. The operator of the unmanned aircraft, is responsible for maintaining a safe distance from all other airspace users, giving them priority and ensuring that during the flight activity of the unmanned aircraft, no other aircraft is put into danger.

xiii. Unmanned aircraft of the open category are not allowed to fly at a height of more than fifty (50) metres (170 feet) above the ground or water.

xiv. The operator is responsible for complying with the legislation in force in relation to the Right to Privacy and Personal Data Protection.

xv. Any faults, malfunctions, defects or other incidents which lead to serious injury or death should be reported to the Competent Authority.

xvi. Flights by an unmanned aircraft which has been manufactured, modified, re-manufactured or added to, by non-qualified persons, are not permitted, except with the permission of the Competent Authority.

7-(1) Special Category

This includes unmanned aircraft, irrespective of their total take-off mass, which carry out commercial activities and also unmanned aircraft , of a total take- off mass of more than 3 kilogrammes ,which carry out either commercial or non-commercial activities. Their flight-height shall not exceed 120 metres (400ft) from the ground or water, except if in accordance with a special permit issued by the Competent Authority, a temporary permission has been granted to fly higher.

(2) Unmanned aircraft of the special category are not allowed to operate flights within Cypriot Airspace, unless they hold an Operating Licence and the operator is a holder of an Unmanned Aircraft Pilot Licence, issued by the Competent Authority.

(3) The Operating Licence, issued by the Competent Authority, defines the flight activities for which the unmanned aircraft of the Special Category is licensed.

(4) The Unmanned Aircraft Pilot Licence, issued by the Competent Authority, defines the aircraft categories and types in each Category, for which the Unmanned Aircraft Pilot is licensed. The Unmanned Aircraft Pilot Licence should be accompanied by a valid, Category 3, Medical Certificate.

(5) The Competent Authority is responsible for the evaluation, the licensing and oversight of the Unmanned Aircraft Pilots Training Schools.

(6) Special Category Unmanned Aircraft operations, are safeguarded through operating restrictions and regulations which are described in detail in the conditions and restrictions defined by the Competent Authority and which form an integral part of the Operating Licence.

(7) The Special Category Unmanned Aircraft Operating Licence, the Special Category Unmanned Aircraft Pilot Licence and the Unmanned Aircraft Pilots Training Schools Licence, is granted by the Competent Authority when it is satisfied that the owner or operator complies with specific requirements as described in the ¨Unmanned Aircraft Operating Licence, Pilots and Training Schools Manual.¨

(8) Interested persons may obtain the ¨Unmanned Aircraft Operating Licence, Pilots and Training Schools Manual¨ from the Competent Authority, on submission of their application.

(9) The granting of the Special Category, Unmanned Aircraft Operating Licence, requires that the owner or operator provides for insurance cover against death, personal injury and damages, caused to third parties, for the minimum amount of one million Euros.

8-(1) Those who contravene the present Decree and the orders, directions and restrictions issued by the Competent Authority, in accordance with the Decree, or those who operate flights without the required Licence or approval from the Competent Authority, or are acting beyond its scope, or are not in compliance with all its conditions, are committing an administrative offence and will be subject to penalties in accordance with articles 245,246 and 247 of the Civil Aviation Act 2002 (as amended).

(2) Violations which constitute a criminal act, in accordance with article 250 of the Civil Aviation Act or other laws of the Republic, are exempt from the provisions of paragraph 1 above.

9-(1) As from the date of effect of this Decree, all owners and operators of unmanned aircraft, will be obliged to comply with its provisions.

(2) The Provisions of paragraphs (2) and (4) of Article 7, regarding the obligation on users of unmanned aircraft to be in possession of an Unmanned Aircraft Pilot's Licence, are put into force six (6) months after the publication date of the present Decree.

10. The present Decree is put into force on the date of its publication in the Cyprus Government Gazette.

Done on 9th November 2015
Marios Demetriades
Minister of Transport, Communications and Works.

A.2 Jammer Circuit