ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ ΕΥΕΛΠΙΔΩΝ
Τμήμα Στρατιωτικών Επιστημών

Ε Λ Λ Η Ν Ι Κ Η Δ Η Μ Ο Κ Ρ Α Τ Ι Α
ΔΙΙΔΡΥΜΑΤΙΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΑΚΑΔΗΜΑΪΚΟΥ ΕΤΟΥΣ 2016-17
ΣΧΕΔΙΑΣΗ & ΕΠΕΞΕΡΓΑΣΙΑ
ΣΥΣΤΗΜΑΤΩΝ (SYSTEMSENGINEERING)
(ΠΔ 96 /2015/ΦΕΚ 163Α'/20.08.2014)

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
Σχολή Μηχανικών Παραγωγής & Διοίκησης

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΤΕΧΝΙΚΕΣ ΠΑΡΕΜΠΟΔΙΣΗΣ (JAMMING) ΣΗΜΑΤΩΝ ΠΑΓΚΟΣΜΙΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΝΤΟΠΙΣΜΟΥ (GPS) – ΔΥΝΑΤΟΤΗΤΕΣ ΚΑΙ ΑΝΤΙΜΕΤΡΑ

INVASION TECHNIQUES (JAMMING) OF SIGNALS GLOBAL POSITIONING SYSTEM (GPS) – OPPORTUNITIES AND COUNTERMEASURES

ΙΩΑΝΝΗΣ Α. ΚΟΥΤΟΥΝΙΔΗΣ

Α.Μ.: 2017018006

ΜΑΪΟΣ 2020

Η σελίδα αυτή είναι σκόπιμα λευκή

Η Μεταπτυχιακή Διατριβή του Ιωάννη Κουτουνίδη εγκρίνεται:

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Νικολάου Ι. Δάρα
(Επιβλέπων)

Κοσμήτορας ΣΣΕ

Καθηγητής Τομέα
Μαθηματικών & Επιστημών
Μηχανικού.

.....

Παπαδάκης Νικόλαος

Επίκουρος Καθηγητής ΣΣΕ

Τομέα Μαθηματικών &
Επιστημών Μηχανικού.

.....

Νικόλαος Τσουρβελούδης

Καθηγητής

Σχολή Μηχανικών Παραγωγής
& Διοίκησης

Πολυτεχνείου Κρήτης

Digitally signed by Nikolaos Tsourveloudis
Date: 2020.07.09 13:02:33 +03'00'

.....

Η σελίδα αυτή είναι σκόπιμα λευκή

Η παρούσα εργασία αφιερώνεται:

*Στην γυναίκα μου **Κ**ωνσταντίνα*

*και στα παιδιά μου **Χ**ρήστο-Άγγελο και **Θ**εοδώρα-Τσαμπίκα.*

ΕΥΧΑΡΙΣΤΙΕΣ

Καταρχάς θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή, Κοσμήτορα της Στρατιωτικής Σχολής Ευελπίδων (Σ.Σ.Ε.) κ. Δάρα Νικόλαο, χωρίς τη βοήθεια και κατευθύνσεις του οποίου δεν θα είχε υλοποιηθεί η παρούσα εργασία, καθώς επίσης και για την εμπιστοσύνη που μου επέδειξε.

Θα ήθελα να εκφράσω τον σεβασμό και την εκτίμησή μου στους Καθηγητές της εξεταστικής επιτροπής, οι οποίοι συνέδραμαν από την πλευρά τους, στην εκπόνηση αυτής της εργασίας καθώς και στον Υποστράτηγο κ. Χούπη Δημήτριο, πρώην Διοικητή της Σ.Σ.Ε. και τον προκάτοχό του Αντιστράτηγο κ. Λαλούση Χαράλαμπο, για την υπηρεσιακή και ακαδημαϊκή βοήθεια που παρείχαν αυτά τα χρόνια της προσπάθειάς μου στις μεταπτυχιακές σπουδές.

Πολλές ευχαριστίες οφείλονται στην γυναίκα μου, που με στήριξε άοκνα και αμέριστα, τόσο με την κατανόησή της, όσο και ψυχολογικά καθ' αυτήν την ακαδημαϊκή μου πορεία.

Ακόμα, θα ευχαριστήσω ομοίως τα παιδιά μου, Χρήστο-Άγγελο και Θεοδώρα-Τσαμπίκα, για την εκτίμηση που επέδειξαν, για τον χρόνο που δεν είχα μαζί τους για να επιτύχω τις σπουδές αυτές, καθώς και τους γονείς μου για την σωστή διαπαιδαγώγηση που μου παρείχαν στη ζωή μου.

Επίσης θα αναφέρω την εξέχουσα συνεργασία και συνδρομή του φίλου και συναδέλφου Κου Λουβερδή Γεράσιμου, από το Υπουργείο Άμυνας της Αγγλίας, Πρόεδρο σε Task Groups του NATO Science Technology Organization και τεχνικό εμπειρογνώμονα σε συστήματα RF, με τον οποίο είχα συνεργαστεί στο παρελθόν από θέση στο NATO JEWCS (Joint Electronic Warfare Core Staff).

Και, τέλος, οφείλω ένα μεγάλο ευχαριστώ και στον αδελφό μου Δημήτρη, που μου παρείχε ιδιαίτερη βοήθεια στη διαδικασία συγγραφής και μορφοποίησης της Διπλωματικής μου Εργασίας, με την εμπειρία του από τις μεταπτυχιακές σπουδές και τον χώρο εργασίας του στην ανεξάρτητη Ελληνική Επιτροπή Ατομικής Ενέργειας στο χώρο του Δημοκρίτειου Ερευνητικού Κέντρου.

Πίνακας Περιεχομένων

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία, αναπτύσσει τις σύγχρονες δυνατότητες παρεμβολής (τύποι και τρόποι – μέσα που χρησιμοποιούνται), στα Παγκόσμια συστήματα προσδιορισμού θέσης (GPS) στον ευρύτερο τομέα, όπου αποτελούν πλέον ένα κεφάλαιο θεμελιώδους σημασίας λόγω της ευρείας χρήσης τους. Τα υπόψη χρησιμοποιούνται, εκτός από τον προσδιορισμό κατεύθυνσης – διαδρομής, επίσης και στον ιδιαίτερο τομέα των Μη Επανδρωμένων Αεροσκαφών (ΜΕΑ ή Unmanned Aerial Vehicle – UAV ή Drone).

Στο κύριο μέρος της, η εργασία εστιάζεται στα παραπάνω συστήματα και τους τρόπους δυνατής αντιμετώπισης της παρεμβολής σε αυτά, καθώς τα ΜΕΑ παρουσιάζουν την μεγαλύτερη ανάπτυξη στην εποχή μας, όπως και η αντίστοιχη εξέλιξη σε προστασία για εφαρμογή της λειτουργίας τους.

Έπειτα επικεντρώνεται στην χρήση αυτών στον στρατιωτικό τομέα των Ενόπλων Δυνάμεων, όπου παρουσιάζονται χαρακτηριστικά και τρόποι αντιμετώπισης της παρεμβολής στις αρχιτεκτονικές επικοινωνίας (με χρήση διάφορων αλγόριθμων), και ιδιαίτερα σε ανάπτυξη πολλών ΜΕΑ μαζί, όπου κυρίως απαιτείται δικτύωση για μεταφορά και ανταλλαγή δεδομένων (Flying Ad-hoc Network – FANET).

Στο τέλος της εργασίας, γίνεται αναφορά για την χρήση έμβιων εντόμων, με την υποστήριξη της βιολογίας για τον χειρισμό και της νανοτεχνολογίας για τα μικρο-επεξεργαστικά εξαρτήματα, και λειτουργία τους ως υποκατάστατα των ΜΕΑ, κυρίως για αποστολές έρευνας και διάσωσης ή και κατασκοπείας. Πιο συγκεκριμένα, επιχειρείται να παρουσιαστεί η πρωτοποριακή μέθοδος χρήσης ως ΜΕΑ, με επίκεντρο την «λιβελούλα», το γνωστό «ελικοπτεράκι» (dragonfly), σε ένα πρόγραμμα που επιμελείται κυρίως η Υπηρεσία Προηγμένων Ερευνών και Ανάπτυξης της Αμερικής (Defense Advanced Research Project Agency – DARPA) στο πρόγραμμά της, το «DragonflEye».

Λέξεις Κλειδιά: Παρεμβολέας, Ad-hoc δίκτυα, FANET, Έμβια όντα, DARPA, λιβελούλα, Νανοτεχνολογία, DragonflEye πρόγραμμα.

ABSTRACT

The present dissertation, develops the modern abilities of intervention (types and ways - means used), in Global Positioning Systems (GPS) in the wider sector, where they are now a capital of fundamental importance due to their widespread use. These considerations are used, in addition to determining the direction - route, also in the particular sector of Unmanned Aerial Vehicles (UAV or Drone).

In its main part, the work focuses on the above systems and the possible ways to the interference in them, as the UAVs' show the greatest growth in our time, as well as the corresponding evolution in protection for the implementation of its operation.

It then focuses on the use of these in the entire Armed Forces, which presents features and ways to deal with interference in communication architectures (using various algorithms), and especially in developing many UAVs' together, where networking is mainly required for exchange and transfer data (Flying Ad-hoc Network – FANET)

At the end of that work, reference is made to the use of living insects, with the support of biology for handling them and nanotechnology for micro-processing components, and their function as substitutes for UAVs, mainly for search and rescue missions or espionage. In particular, an attempt is being made to present a pioneering method of being use as UAV, focusing on the well-known "dragonfly", in a program which is mainly organized by the Defense Advanced Research Project Agency (DARPA) of the USA, in its program, "DragonflEye".

Keywords: Interpolator, Ad-hoc Networks, FANET, Living insects, DARPA, Dragonfly, Nanotechnology, DragonflEye project.

ΕΙΣΑΓΩΓΗ

Η ανάπτυξη της τεχνολογίας στον τομέα του προσδιορισμού θέσης (GPS), έχει επιφέρει μια επανάσταση στην αξιοποίησή του, καθώς χρησιμοποιείται στις περισσότερες από τις συσκευές που κατασκευάζονται για ευρεία χρήση. Πέραν από την αρχική χρήση του GPS για εξεύρεση θέσεως και διαδρομής, στη συνέχεια βρήκε μεγαλύτερη αξιοποίηση στον κλάδο των μέσων μεταφοράς, και ιδιαίτερα στην χρήση στα ΜΕΑ (UAV), τα οποία και αναλύονται στην παρούσα εργασία.

Στο πρώτο κεφάλαιο γίνεται γενική αναφορά στον όρο της παρεμβολής, στα είδη αυτής, στους διαφόρους τύπους παρεμβολέων και στις τεχνικές παρεμβολής.

Στο δεύτερο κεφάλαιο παρουσιάζονται η τεχνολογία της παρεμβολής στο GPS, η χρήση του στα Μη Επανδρωμένα Αεροσκάφη (ΜΕΑ), η παρεμβολή και οι τεχνικές αυτής, ορισμένες ευπάθειες των ΜΕΑ καθώς και τρόποι αντιμετώπισής της.

Έπειτα, το κεφάλαιο τρία επικεντρώνεται πιο πολύ στα δίκτυα Ad-hoc στα ΜΕΑ και τις δυνατότητες ανταλλαγής πληροφοριών από το σταθμό βάσης σε ένα ή περισσότερα ΜΕΑ σε πραγματικό χρόνο, όταν αυτά θα ενεργούν για συγκεκριμένο σκοπό. Στην περίπτωση των πολλών ΜΕΑ, επεξηγούνται τα πλεονεκτήματα και μειονεκτήματα για διάφορα πρωτόκολλα μεταφοράς και ανταλλαγής δεδομένων.

Στη συνέχεια, στο τέταρτο κεφάλαιο παρατίθενται γενικότερα ζητήματα ασφαλείας στα ιπτάμενα Ad-hoc δίκτυα και στον τρόπο δικτύωσής τους (Flying Ad-hoc Networking – FANET), ανάλυση της παρεμβολής στα πρωτόκολλα δρομολόγησης και θέτονται τρόποι επικοινωνίας των FANET και τυχόν περιορισμοί σε αυτά.

Τέλος στο τελευταίο κεφάλαιο αναπτύσσεται μια προσπάθεια για χρήση, ως ΜΕΑ, έμβιων εντόμων, σε μια έρευνα με συνδυασμό βιολογικών ανακαλύψεων χειρισμού τους και ανάπτυξη νανο-επεξεργαστών, καθόσον χρησιμοποιούνται οι ήδη υπάρχοντες ιπτάμενες «πλατφόρμες» των εντόμων για αποστολές σε ιδιαίτερα δύσβατες περιοχές (έρευνα – διάσωση), είτε σε απαγορευμένες θέσεις, για στρατιωτική κυρίως κατασκοπεία. Σε αυτήν την περίπτωση των εντόμων, σημαντική πρόοδος έχει επιτευχθεί στην λιβελούλα, το γνωστό «ελικοπτεράκι» (Dragonfly), από την αμερικάνικη υπηρεσία ερευνών (DARPA).

Κεφάλαιο 1

Ηλεκτρονικές Παρεμβολές

1.1 Εισαγωγή

Τα ασύρματα δίκτυα διαδραματίζουν σημαντικό ρόλο στην αδιάλειπτη επικοινωνία συστημάτων με άμεση βελτίωση της ποιότητα ζωής. Η φύση των ασύρματων συνδέσεων, χαρακτηριστικό των οποίων είναι η κοινή πρόσβαση στο μέσο επικοινωνίας, προκαλεί ευπάθεια στην παρεμβολή. Οι τεχνικές παρεμβολής είναι επιθέσεις άρνησης της υπηρεσίας που δύνανται να συνδυαστούν με κενά ασφαλείας ανώτερων επιπέδων επικοινωνίας [1].

Παρεμβολή σε ασύρματα δίκτυα ορίζεται η διακοπή υφιστάμενης ασύρματης επικοινωνίας με την μείωση του λόγου σήματος προς θόρυβο στον πομποδέκτη του παραλήπτη, το οποίο είναι αποτέλεσμα εκπομπής ασύρματων σημάτων παρεμβολής. Η ηλεκτρονική παρεμβολή που εξετάζουμε, διαφέρει από τις κλασσικές παρεμβολές σημάτων γιατί έχει ως αποκλειστικό σκοπό την διακοπή της επικοινωνίας, ενώ οι κλασικές παρεμβολές αν προκαλέσουν οποιαδήποτε διακοπή στην επικοινωνία είναι ακούσια. Η ακούσια διακοπή μπορεί να προέλθει από συσκευές που εκπέμπουν ταυτόχρονα ή συσκευές σε διαφορετικό δίκτυο. Οι εκούσιες παρεμβολές υλοποιούνται από ένα επιτιθέμενο, με σκοπό την διακοπή της επικοινωνίας στο δίκτυο. Η παρεμβολή μπορεί να εκτελεστεί σε πολλά επίπεδα, όπως στην παρακώλυση κατά την αποστολή ή την καταστροφή πακέτων στο μέσο.

Για την ευρύτερη κατανόηση των επιθέσεων παρεμβολής σε ασύρματα δίκτυα με σκοπό την παρακώλυση ή και διακοπής της επικοινωνίας εξετάζουμε τους τύπους των παρεμβολέων, καθώς και την τοποθέτηση αυτών στο χώρο.

Ένα δίκτυο δύνανται να παρεμβληθεί με ποικίλους τρόπους και με χρήση διαφόρων τύπων παρεμβολέων. Για την αποφυγή παρεμβολών είναι σημαντικό να εξετάσουμε το πως αυτοί λειτουργούν. Οι τύποι παρεμβολέων που υπάρχουν στην παρούσα περίοδο της εργασίας, είναι προληπτικοί, αντιδραστικοί, εξειδικευμένης λειτουργίας και έξυπνοι-υβριδικοί. Επίσης, εξετάζουμε την ιδανική τοποθεσία των παρεμβολέων για την βελτιστοποίηση της παρεμβολής.

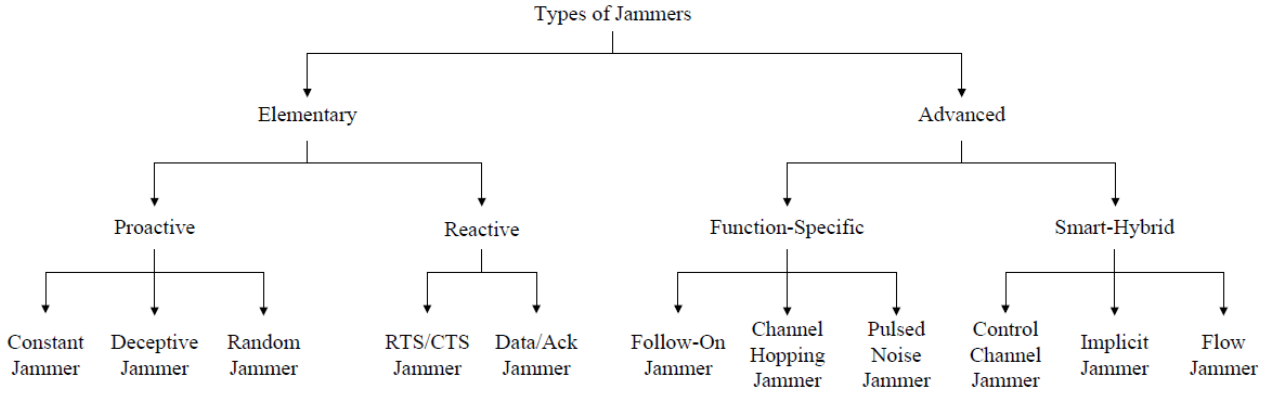
1.2 Τεχνικές Παρεμβολής

Στις εκούσιες παρεμβολές χρησιμοποιούνται οι διεθνείς ασύρματες συχνότητες για να παρακωλυθεί η ασύρματη επικοινωνία. Η παρεμβολή αποσκοπεί στο να καταστήσει το μέσο, μη διαθέσιμο, και είτε να αναγκάσει τις συσκευές να αναβάλλουν την αποστολή στο μέσο, είτε να καταστρέψουν το σήμα πριν ληφθεί από το παραλήπτη. Η παρεμβολή επικεντρώνεται στο φυσικό επίπεδο, αλλά μπορεί να συνδυαστεί και με επιθέσεις σε άλλα επίπεδα. Παρακάτω καταγράφονται οι γνωστοί τύποι παρεμβολέων.

1.3 Τύποι Παρεμβολέων

Οι παρεμβολείς είναι κακόβουλοι ασύρματοι πομποί που τοποθετούνται από έναν επιτιθέμενο για να παρακωλύσουν την ασύρματη επικοινωνία. Ανάλογα με την στρατηγική του επιτιθέμενου, ο παρεμβολέας μπορεί να διαθέτει όμοιες ή και διαφορετικές δυνατότητες από τους νόμιμους πομπούς του δικτύου που δέχεται επίθεση. Η δυνατότητα παρεμβολής εξαρτάται από την ισχύ του σήματος, την τοποθεσία και την επιρροή του στο στοχευμένο δίκτυο.

Ο παρεμβολέας μπορεί να είναι απλοϊκός ή προηγμένος, σύμφωνα με τις λειτουργίες του. Οι απλοϊκοί παρεμβολείς χωρίζονται σε δύο υποκατηγορίες, τους προληπτικούς και τους αντιδραστικούς. Οι προηγμένοι παρεμβολείς χωρίζονται και αυτοί σε δύο υποκατηγορίες, της εξειδικευμένης λειτουργία και τους έξυπνους-υβριδικούς. Στην εικόνα 1 συνοψίζονται οι παραπάνω κατηγορίες.



Εικόνα 1 Τύπος Παρεμβολέων

1.3.1 Προληπτικοί Παρεμβολείς

Οι προληπτικοί παρεμβολείς εκπέμπουν σήματα, είτε υπάρχει, είτε δεν υπάρχει μεταφορά δεδομένων στο δίκτυο. Εκπέμπουν πακέτα ή τυχαία bit στο κανάλι εκπομπής, τοποθετώντας έτσι, τους υπόλοιπους πομπούς σε κατάσταση αναμονής. Δεν έχει την δυνατότητα να εκπέμψει σε άλλο κανάλι και υπάρχουν τρεις βασικοί τύποι: συνεχείς, παραπλανητικοί και τυχαίοι. Στη συνέχεια όποτε αναφερόμαστε σε προληπτικούς παρεμβολείς εννοούμε και τις 3 παραπάνω κατηγορίες.

Συνεχείς Παρεμβολείς: εκπέμπουν αδιάλειπτα τυχαία bit χωρίς να ακολουθείται το πρωτόκολλο CSMA (Carrier-Sense Multiple Access). Σύμφωνα με το πρωτόκολλο CSMA, η συσκευή ανιχνεύει την κίνηση στο μέσο και εκπέμπει μόνο, όταν αυτό είναι ελεύθερο. Ένας συνεχής παρεμβολέας αποτρέπει την επικοινωνία με την συνεχή κατάληψη του μέσου. Αυτού του τύπου η επίθεση απαιτεί πολύ ενέργεια και είναι πολύ εύκολο να εντοπιστεί. Παρόλα αυτά, εκτελείται εύκολα και καθιστά με αποτελεσματικό τρόπο μη διαθέσιμη την επικοινωνία.

Παραπλανητικός Παρεμβολέας: εκπέμπει συνεχώς κανονικά πακέτα [2] αντί για τυχαία bit. Παραπλανεί του άλλους πομπούς, ότι εκτελεί νόμιμη επικοινωνία με άλλους πομπούς και τους τοποθετεί σε κατάσταση μόνιμης λήψης, μέχρι να κλείσει ο παρεμβολέας. Ενώ είναι πιο δύσκολος

να εντοπιστεί, καταναλώνει πολύ ενέργεια, παρά ταύτα όμως είναι και αυτός εύκολος στην υλοποίηση του.

Τυχαίος Παρεμβολέας : εκπέμπει τυχαία bit ή κανονικά πακέτα στο δίκτυο [2]. Σε αντίθεση με τους δύο προηγούμενους, έχει στόχο την μικρότερη κατανάλωση ενέργειας. Εκπέμπει μέχρι να μπει σε κατάσταση ύπνωσης και στην συνέχεια εκπέμπει ξανά. Αυτοί οι χρόνοι εκπομπής και ύπνωσης είναι, είτε τυχαίοι, είτε καθορισμένοι. Η αναλογία μεταξύ ύπνωσης και εκπομπής καθορίζει την εξοικονόμηση ενέργειας (που δεν καταναλώνεται) και την απόδοση της παρεμβολής.

1.3.2 Αντιδραστικοί Παρεμβολείς

Οι αντιδραστικοί παρεμβολείς ξεκινάνε την παρεμβολή μόνο όταν ανιχνευθεί μεταφορά δεδομένων σε ένα συγκεκριμένο κανάλι. Το αποτέλεσμα είναι να αλλοιωθεί το σήμα στον παραλήπτη. Μπορεί να επηρεάσει τόσο μικρά, όσο και μεγάλα δίκτυα. Επειδή συνεχώς ανιχνεύει το μέσο για εκπομπή είναι πιο ενεργοβόρο από ένα τυχαίο παρεμβολέα. Είναι όμως πιο δύσκολο στον εντοπισμό από ένα προληπτικό παρεμβολέα, επειδή ο λόγος παράδοσης πακέτων δεν μπορεί να καθοριστεί με ακρίβεια. Σύμφωνα με μία μελέτη του Pelechrinis [3], υπάρχουν δυο ξεχωριστοί τρόποι εφαρμογής των αντιδραστικών παρεμβολέων, που περιγράφονται παρακάτω.

Αντιδραστικός Παρεμβολέας RTS/CTS (**Request-To-Send/Clear-To-Send**): εκτελεί παρεμβολή όταν ανιχνεύει μήνυμα αίτησης για αποστολή [request-to-send (RTS)] στον αέρα. Με αυτό το τρόπο το μήνυμα παραχώρησης αποστολής [clear-to-send (CTS)] δεν στέλνετε αφού το μήνυμα RTS παρεμβάλετε. Έτσι ο αποστολέας δεν στέλνει, γιατί έχει την εντύπωση ότι το μέσο χρησιμοποιείται. Εναλλακτικά, ο παρεμβολέας μπορεί να περιμένει να καταστρέψει το μήνυμα CTS έχοντας το ίδιο αποτέλεσμα [3].

Αντιδραστικός Παρεμβολέας σε **Δεδομένα (ACK/ Acknowledgement)**: παρεμβάλει το δίκτυο με την καταστροφή εκπομπών με δεδομένα ή επιβεβαιώσεις (ACK). Ο παρεμβολέας ανιχνεύει μεταφορά δεδομένων, ή σήμα (bit) ACK [3]. Η καταστροφή των παραπάνω έχει σαν αποτέλεσμα να εκτελεστεί επανεκπομπή των δεδομένων, είτε γιατί δεν παραλήφθηκαν, είτε γιατί δεν επιβεβαιώθηκε η λήψη τους, με αποτέλεσμα την εσκεμμένη καθυστέρηση εκπομπής και έτσι την μη εκπλήρωση του επιδιωκόμενου αποτελέσματος.

1.3.3 Παρεμβολείς Εξειδικευμένης Λειτουργίας

Οι παρεμβολείς εξειδικευμένης λειτουργίας εκτελούν παρεμβολή σύμφωνα με μία προκαθορισμένη λειτουργία. Μπορούν να είναι, είτε προληπτικοί, είτε αντιδραστικοί. Επίσης, έχουν την δυνατότητα να εκπέμπουν σε ένα, ή περισσότερα κανάλια. Ακόμα και όταν παρεμβάλουν σε ένα κανάλι αυτό το κανάλι δύνανται να αλλαχθεί σύμφωνα με την εξειδικευμένη λειτουργία τους. Αυτοί οι τύποι αναλύονται ως ακολούθως:

Ακολουθητικοί παρεμβολείς : εκτελούν αναπηδήσεις σε όλα τα διαθέσιμα κανάλια, με ρυθμό χιλιάδων φορών ανά δευτερόλεπτο. Έτσι, παρεμβάλει κάθε κανάλι για ένα ελάχιστο χρόνο [4]. Αν ο πομπός εντοπίσει την παρεμβολή και αλλάξει κανάλι, οι ακολουθητικοί παρεμβολείς δύνανται να εντοπίσουν την εκπομπή σε ένα εύρος φάσματος και να συνεχίσουν την παρεμβολή. Επίσης, μπορεί να εκτελεί παρεμβολή σε μία ψευδοτυχαία ακολουθία συχνοτήτων. Με αυτό το τρόπο, εξοικονομεί ενέργεια περιορίζοντας την επίθεση του σε ένα κανάλι πριν μεταπηδήσει στην

επόμενη συχνότητα. Λόγω του ταχύτατου ρυθμού μεταπήδησης συχνοτήτων, οι ακολουθητικοί παρεμβολείς είναι μία αποτελεσματική μέθοδος απέναντι σε αντίμετρα, όπως τη φασματική εξάπλωση με αναπήδηση συχνότητας [frequency hopping spread spectrum (FHSS)], που εκτελεί αναπήδηση σε χαμηλό ρυθμό.

Παρεμβολείς αναπήδησης καναλιών : μεταπηδούν μεταξύ καναλιών προληπτικά και αναζητούν την ύπαρξη επικοινωνίας [5]. Αυτού του τύπου οι παρεμβολείς, έχουν απευθείας πρόσβαση στο μέσο, παρακάμπτοντας τον αλγόριθμο CSMA που παρέχεται από το επίπεδο της σύνδεσης. Επιπλέον, δύνανται να αναπηδήσει ταυτόχρονα μεταξύ καναλιών. Κατά την διάρκεια της φάσης ανακάλυψης και εντοπισμού των φασμάτων, ο παρεμβολέας δεν είναι ορατός από τους γειτονικούς σταθμούς. Στην συνέχεια, ξεκινάει την παρεμβολή σε συχνότητες σε διαφορετικό χρόνο, σύμφωνα με ένα προκαθορισμένο ψευδοτυχαίο προγραμματισμό.

Παρεμβολείς παλμού : μπορούν να αλλάζουν κανάλια και να παρεμβάλουν σε διαφορετικά κανάλια και χρόνο. Όπως και με τους τυχαίους παρεμβολείς, εξοικονομούν ενέργεια, σταματώντας την παρεμβολή, σύμφωνα με το προγραμματισμό τους. Δύνανται να εκτελούν παρεμβολή σε πολλαπλά κανάλια [6].

1.3.4 Έξυπνοι-Υβριδικοί Παρεμβολείς

Ονομάζονται έξυπνοι γιατί εξοικονομούν ενέργεια χωρίς να επηρεάζεται η αποτελεσματικότητά τους. Ο σκοπός αυτού του τύπου είναι να μεγιστοποιήσουν τα αποτελέσματα της παρεμβολής στο δίκτυο. Ταυτόχρονα, φροντίζουν να καταναλώσουν την ελάχιστη ενέργεια. Επικεντρώνουν επαρκή ενέργεια στα σωστά σημεία για να μειώσουν το εύρος επικοινωνίας σε όλο το δίκτυο ή τμήμα αυτού. Υβριδικοί χαρακτηρίζονται γιατί είναι, είτε προληπτικοί είτε αντιδραστικοί.

Παρεμβολείς ελέγχου καναλιών: λειτουργούν σε δίκτυα με πολλαπλά κανάλια επικοινωνίας, επικεντρώνοντας την παρεμβολή στο κανάλι ελέγχου ή το κανάλι που συντονίζει την επικοινωνία [7]. Ένας τυχαίος παρεμβολέας που στοχεύει το κανάλι ελέγχου, μπορεί να υποβαθμίσει σημαντικά την ποιότητα ενός δικτύου, ενώ ένας συνεχής παρεμβολέας προκαλεί πλήρη διακοπή της επικοινωνίας. Αυτές οι επιθέσεις, συνήθως προϋποθέτουν ο ένας νόμιμος κόμβος να έχει καταληφθεί, έτσι οποιοδήποτε μελλοντικό κανάλι ελέγχου να εντοπίζεται ακαριαία.

Έμμεση παρεμβολή είναι η επίθεση, η οποία εκτός από το στόχο προκαλεί άρνηση της υπηρεσίας και σε άλλους κόμβους [8]. Αυτές οι επιθέσεις εκμεταλλεύονται αλγορίθμους προσαρμοστικού ρυθμού, οι οποίοι μειώνουν το ρυθμό εκπομπής στους πιο αδύναμους δέκτες. Με αυτή την διαδικασία, το σημείο πρόσβασης καταναλώνει μεγαλύτερο χρόνο στις εκπομπές του σε ένα αδύναμο δέκτη. Συνέπεια αυτού, είναι οι δέκτες που δεν δέχονται επίθεση, να επηρεάζονται και αυτοί αρνητικά.

Παρεμβολή Ροής : είναι η επίθεση, που περιέχει πολλαπλούς παρεμβολείς στο δίκτυο για να προκαλέσουν μειωμένη ροή δεδομένων. Όπως εφαρμόστηκε από τον Tague στην μελέτη του [8α], αυτές οι επιθέσεις εκτελούνται με πληροφορίες από το επίπεδο δικτύου. Αυτός ο τύπος παρεμβολής παρουσιάζει πλεονεκτήματα για επιτιθέμενους με περιορισμένους πόρους. Εφόσον υπάρχει κεντρική διαχείριση των παρεμβολέων, τότε αυτή μπορεί να υπολογίσει και να επικοινωνήσει στους

παρεμβολείς την ελάχιστη ενέργεια για μία επιτυχημένη παρεμβολή. Εναλλακτικά, υπάρχει η δυνατότητα, γειτονικοί παρεμβολείς να επικοινωνούν μεταξύ τους για το διαμοιρασμό του έργου.

1.3.5 Σύνοψη Παρεμβολέων

Όλες οι παραπάνω λειτουργίες, των διαφόρων τύπων παρεμβολέων, συνοψίζονται στην εικόνα 2.

Jammer	*Proactive*	*Reactive*	*Energy efficient*	*Single channel*	*Multiple channels*
Constant	×			×	
Deceptive	×			×	
Random	×		×	×	
RTS/CTS jammer		×		×	
Data/ACK jammer		×		×	
Follow-on	×		×	×	
Channel hopping		×		×	×
Pulsed noise	×			×	×
Control channel	×	×	×	×	
Implicit	×	×	×	×	
Flow-jamming	×	×	×	×	×

Εικόνα 2 Λειτουργίες των Τύπων Παρεμβολέων

1.4 Τοποθέτηση Παρεμβολέων

Επιπλέον των δυνατοτήτων που αναλύθηκαν παραπάνω, εξίσου σημαντικής σημασίας είναι η τοποθεσία του παρεμβολέα. Οι παρεμβολείς μπορούν να τοποθετηθούν, είτε σε τυχαία, είτε σε προμελετημένα σημεία. Οι τεχνικές μελέτης του χώρου για βελτιστοποίηση της παρεμβολής, είναι το αντικείμενο που θα εξεταστεί παρακάτω.

1.4.1 Βέλτιστες Επιθέσεις Παρεμβολής

Η καθηγήτρια Li στην μελέτη της το 2007 [8β], παρουσιάζει ότι η πιθανότητα παρεμβολής είναι υψηλή όταν ο επιτιθέμενος έχει επίγνωση της στρατηγικής του δικτύου, ενώ σημαντικό ρόλο είχε και η ισχύς της εκπομπής. Επιπλέον, ο παρεμβολέας είναι σημαντικό να γνωρίζει την πιθανότητα πρόσβασης καναλιών, όπως και τον αριθμό των γειτονικών κόμβων από το κόμβο που παρακολουθεί. Όλοι οι υπόλοιποι κόμβοι εκτελούν την επικοινωνία simplex της IEEE 802.11. Ο κόμβος παρακολούθησης χρησιμοποιεί τον έλεγχο Ποσοστού διαδοχικών πιθανοτήτων (Sequential Probability Ratio) για τον έλεγχο μεταξύ δύο υποθέσεων που αφορούν τα λανθασμένα σήματα (false alarm) και την πιθανότητα αδυναμίας ανίχνευσης. Οι παρεμβολείς και οι πομποί/δέκτες κατανέμονται σε μία δεδομένη περιοχή με την χρήση της κατανομής Poisson (distribution). Αυτή είναι μία διακριτή συνάρτηση κατανομής, που εκφράζει την πιθανότητα στατιστικά να συμβεί ένα σταθερό γεγονός (παρεμβολή από μία τοποθεσία), μετά από μία σειρά γεγονότων (παρεμβολές), εάν αυτά συμβαίνουν με γνωστό μέσο ρυθμό επανάληψης (και είναι ανεξάρτητο από το χρονικό διάστημα επανάληψης).

Οι εκτιμώμενες τιμές επιτυχημένων εκπομπών υπολογίζονται με πιθανότητες. Αν σε μία περιοχή εκτελείται παρεμβολή, τότε ο κόμβος παρακολούθησης του δικτύου πρέπει να στείλει την ειδοποίηση για παρεμβολή σε διαφορετική συχνότητα (με την χρήση αναπήδησης), γιατί και αυτό

το σήμα επηρεάζεται από την παρεμβολή στην περιοχή. Με την χρήση πιθανοτήτων κατανομής και μαθηματικής απόδειξης, οι μελετητές κατέληξαν, πως η ιδανική στρατηγική για τον επιτιθέμενο είναι μία ήπια επίθεση με μεγάλο χρονικό ορίζοντα.

1.4.2 Παρεμβολή υπό προϋποθέσεις αβεβαιότητας

Σε μια μελέτη του 2008 [9] εφαρμόστηκε μία δυναμική προσέγγιση για τον υπολογισμό της τοποθέτησης των παρεμβολέων με την ενσωμάτωση των ορίων της περιοχής παρεμβολής. Στην υπόθεση εργασίας που εξετάζουν, θεωρούν μία περιοχή τετράγωνου σχήματος, στην οποία οι παρεμβολείς τοποθετούνται στα σημεία με την μέγιστη κάλυψη. Διατυπώνουν το πρόβλημα της τοποθέτησης παρεμβολέων με σκοπό την παρεμβολή όλων των κόμβων. Υποπροβλήματα εξετάζονται και επιλύονται για να εκπονηθούν τα ιδανικά αποτελέσματα. Βασική υπόθεση είναι ότι διαθέτουν περιορισμένες πληροφορίες για το δίκτυο. Ο επιτιθέμενος γνωρίζει μόνο τα όρια της περιοχής καθώς και πως χρησιμοποιούνται οι πανκατευθυντικές κεραίες. Επίσης, υπολογίζουν ότι η ισχύς εκπομπής μειώνεται αντίστροφα με το τετράγωνο της απόστασης των συσκευών. Τέλος, υπολογίζουν τους ελάχιστους παρεμβολείς που απαιτούνται για την παρεμβολή όλων των κόμβων. Σκοπός του υπολογισμού είναι η ισχύς παρεμβολής σε όλα τα σημεία να είναι υψηλότερη του κατωφλιού ισχύς του δικτύου, που απαιτείται για μία επιτυχημένη επικοινωνία μεταξύ νόμιμων κόμβων.

1.4.3 Περιορισμένου Εύρους Επιθέσεις

Παρεμβολείς με την μισή ισχύ εκπομπής από τους νόμιμους πομπούς δύνανται να παρεμβάλουν ένα δίκτυο, γιατί το εύρος παρεμβολής ασύρματων συσκευών είναι το διπλάσιο του εύρους εκπομπής [9α]. Σε αντίθεση με προηγούμενες μεθόδους επίθεσης που εξετάσαμε, δεν απαιτούνται γενικές γνώσεις. Επιπρόσθετα, λόγω της περιορισμένης ισχύος, παρουσιάζουν ως πλεονέκτημα ότι οι παρεμβολείς δεν εντοπίζονται εύκολα. Οι παρεμβολείς τοποθετούνται σε στρατηγικές τοποθεσίες, συνήθως κοντά σε κόμβους για να έχουν μέγιστο αποτέλεσμα. Οι μελετητές παρουσιάζουν εμπειρικά αποτελέσματα με κανονικό, διπλάσιο και μισό εύρος ισχύος. Οι παρεμβολείς κανονικού εύρους εκπέμπουν στην ίδια ισχύ με τους νόμιμους κόμβους που έχει σαν αποτέλεσμα τον διπλασιασμό του εύρους παρεμβολής τους. Αντίστοιχα με την μισή ισχύ, οι περιορισμένου εύρους παρεμβολείς προκαλούν παρεμβολή ίση με την ισχύ εκπομπής των νόμιμων κόμβων. Πειράματα με αυτού του τύπου παρεμβολέων σε OPNET προσομοιωτή (Optimized Network Engineering Tools), καταδεικνύουν ότι δυσχεραίνεται σημαντικά ο εντοπισμός τους, γιατί οι μετρήσεις SNR (Signal to Noise Ratio) και PDR (Preliminary Design Review), οι οποίες χρησιμοποιούνται για τον εντοπισμό, μειώνονται σε μεγάλο βαθμό.

1.4.4 Defense Security Service (DSS) για τον εντοπισμό VHF/ UHF Παρεμβολέων

Η μελέτη του Gencer [9β] περιγράφει ότι ένα σύστημα παρεμβολής τοποθετείται με σκοπό την πλήρη διακοπή της επικοινωνίας του στόχου. Αυτά τα συστήματα χρησιμοποιούνται συνήθως σε στρατιωτικές εφαρμογές. Επιλέγονται περισσότερα του ενός υποψηφίων σημείων, ανάλογα με τον στόχο και τον αριθμό των συστημάτων παρεμβολέων που διαθέτουμε. Στην υπόθεση της μελέτης θεωρούμε ότι υπάρχει οπτική επαφή μεταξύ κόμβου και παρεμβολέα και ταυτόχρονα η ισχύς εκπομπής του παρεμβολέα είναι υψηλότερη από την ισχύ των νόμιμων κόμβων.

Η κύρια στόχευση είναι να μελετηθεί η βέλτιστη τοποθεσία για την μέγιστη δυνατή κάλυψη στο χώρο. Έτσι, χρησιμοποιείται το μοντέλο μέγιστης κάλυψης και επιλύεται με το πακέτο LINGO-8. Το LINGO είναι ένα πρόγραμμα μετάφρασης στο οποίο περιλαμβάνετε ένα ενσωματωμένο πακέτο που περιγράφει μοντέλα βελτιστοποίησης. Με δεδομένο τον αριθμό των στόχων, των διαθέσιμων σημείων και των συστημάτων παρεμβολής προκύπτουν οι τοποθεσίες για την τοποθέτηση των παρεμβολέων.

1.4.5 Παρεμβολέας Μεγέθους Nano

Ο Panyim [10] στην εργασία του, υποστηρίζει τη χρήση μεγάλου αριθμού μικρών παρεμβολέων με χαμηλή ισχύ, οι οποίοι είναι δύσκολο να εντοπιστούν ακόμα και με γυμνό μάτι. Η εφαρμογή αυτών των παρεμβολέων είναι σε μορφή δικτύου. Η συνολική ισχύς παρεμβολής διατηρείται σταθερή. Ο τύπος αυτών των παρεμβολέων είναι ο αντιδραστικός σε ολόκληρο το δίκτυο. Εμπειρικά αποτελέσματα της μελέτης καταδεικνύουν ότι υπερέχουν σε απόδοση από τους παραδοσιακούς παρεμβολείς. Ο αριθμός των παρεμβολέων μπορεί να αυξηθεί με αποτέλεσμα την εξοικονόμηση ενέργειας. Εφαρμόστηκε η θεωρία διήθησης για να εξεταστεί η επεκτασιμότητα του μοντέλου και αποδείχθηκε η δυσκολία ο εντοπισμός τους λόγω του μικρού μεγέθους τους, της χαμηλής ισχύος και της υψηλής αποτελεσματικότητας του σχηματισμού στο δίκτυο.

1.4.6 Συμπεράσματα Κεφαλαίου

Συνοψίζοντας τα παραπάνω, αναλύθηκαν πέντε στρατηγικές τοποθέτησης που εμφανίζονται στην εικόνα 3, στον οποίο εξετάζονται, σύμφωνα με τα κριτήρια της γνώσης μας για το δίκτυο, η ισχύς εκπομπής, ο αριθμός των παρεμβολέων και η δυνατότητα εντοπισμούς τους.

Placement strategy	*Network Knowledge*	*Transmission power*	*Number of jammers*	*Detection level*
Optimal jamming attacks	Yes	Controllable	One	Difficult
Jamming under complete uncertainty	Limited	Calculated	Many	Moderate
Limited-range jamming attacks	No	Low	Many	Difficult
DSS for locating VHF/UHF jammer	Yes	High	Many	Easy
Nano Size Jammer	No	Low	Many	Very difficult

Εικόνα 3 Ανάλυση Στρατηγικών Τοποθέτηση Παρεμβολέων

Κεφάλαιο 2

Παγκόσμιο Σύστημα Στιγματοθέτησης στα Μη Επανδρωμένα Αεροσκάφη

2.1 Εισαγωγή στο GPS

Το Παγκόσμιο Σύστημα Στιγματοθέτησης [Global Positioning System (GPS)], είναι ένα παγκόσμιο σύστημα εντοπισμού γεωγραφικής θέσης αποσκοπώντας την παροχή της ακριβής θέσης, της ταχύτητας και του χρόνου στους δέκτες , το οποίο βασίζεται σε δορυφόρους εφοδιασμένους με ειδικές συσκευές εντοπισμού, οι οποίες ονομάζονται πομποδέκτες GPS. Το GPS άρχισε να λειτουργεί το 1973 από την πολεμική αεροπορία της Αμερικής για στρατιωτικούς σκοπούς. Στις αρχές της δεκαετίας του 90 έγινε διαθέσιμο στο ευρύτερο κοινό. Αντίστοιχα συστήματα έχουν αναπτυχθεί από διάφορες χώρες και οργανισμούς. Η Ρωσία διαθέτει το GLONASS (Global Navigation Satellite System), η Ευρωπαϊκή Ένωση (Ε.Ε.) διαθέτει το GALILEO και η Κίνα διαθέτει το BDS (BeiDou Navigation Satellite System). Για λόγους οικονομίας όλα τα παραπάνω συστήματα στην εργασία θα αναφέρονται ως GPS. Μεγάλος αριθμός μοντέρνων όπλων και αεροσκαφών επανδρωμένων και μη-επανδρωμένων, βασίζονται στο GPS για πλοήγηση. Για τον καθορισμό του χρόνου επαρκεί ένας μοναδικός δορυφόρος, όμως για την παροχή ακριβών πληροφοριών πλοήγησης, απαιτούνται τουλάχιστον τέσσερις δορυφόροι.

Η παρεμβολή του σήματος του GPS αποκτά ιδιαίτερη σημασία στο θέατρο των επιχειρήσεων και έχει αποτελέσει αντικείμενο μελέτης από την εποχή που ξεκίνησε να λειτουργεί το σύστημα.

Ο δορυφόρος εκπέμπει την τιμή του χρόνου του και ο δέκτης συγκρίνει την τιμή αυτή με το εσωτερικό του ρολόι. Το αποτέλεσμα της σύγκρισης είναι η απόσταση μεταξύ δορυφόρου και δέκτη. Οι δορυφόροι GPS εκπέμπουν δύο ξεχωριστά σήματα, το πρώτο κρυπτογραφημένο για στρατιωτική χρήση (P-Code) και το δεύτερο ανοιχτό για πολιτική χρήση (C/A:Coarse/Acquisition). Μετά το 2000, η ακρίβεια του πολιτικού τύπου σήματος αυξήθηκε, όταν άρθηκαν περιορισμοί στην ακρίβεια της πληροφορίας [11].

2.2 Τεχνολογία παρεμβολής του GPS

Η ισχύς των σημάτων GPS, όταν φτάνουν στο δέκτη, είναι χαμηλή, έτσι η παρεμβολή τους είναι σχετικά εύκολη. Από τεχνικής άποψης, η παρεμβολή του δέκτη χωρίζεται σε δύο είδη, την καθολική παρεμβολή και την παρεμβολή πλαστοπροσωπίας.

Η καθολική παρεμβολή αποτελείται από ισχυρά σήματα παρεμβολής που εμποδίζουν την λήψη των σημάτων GPS. Επομένως, αρνείται την παροχή πληροφοριών χρόνου και θέσης στους δέκτες .

Η παρεμβολή πλαστοπροσωπίας περικλείει την εκπομπή ψεύτικων πληροφοριών (χρόνο, δέκτες, συχνότητες, κτλ), με σκοπό την παραπλάνηση και δημιουργία σύγχυσης.

Η παρεμβολή στο GPS περιλαμβάνει παρεμβολή μονής συχνότητας και παρεμβολή του κώδικα Coarse/Acquisition.

Ο κώδικας C/A είναι ένας από τους δυο ψευδοτυχαίους κώδικες που χρησιμοποιούνται για την μεταφορά της πληροφορία του GPS. Διαμορφώνεται στην μπάντα L1 (1575.42 MHz) και επαναλαμβάνεται κάθε 1023 bit με ρυθμό διαμόρφωσης 1 MHz. Κάθε δορυφόρος διαθέτει μοναδικό ψευδοτυχαίο κώδικα. Το C/A αποτελεί το κύριο συστατικό του πολιτικού GPS. Η παρεμβολή εκτελείται σε αυτό το κώδικα και όχι στον έτερο ψευδοτυχαίο κώδικα, που ονομάζεται Precise (P(Y)), γιατί δημιουργείται με πολύ πιο αργό ρυθμό.

Ο κώδικας P(Y) επαναλαμβάνεται κάθε 7 ημέρες και διαμορφώνεται στις μπάντες L1 και L2 (1227.60 MHz) με ρυθμό 10 MHz. Αυτό ο κώδικας λόγω της δυνατότητας τους να κρυπτογραφείται, χρησιμοποιείται σε στρατιωτικούς σκοπούς. Επειδή είναι πιο δύσκολος στην λήψη του, σε πολλές στρατιωτικές εφαρμογές λαμβάνεται αρχικά ο κώδικας C/A και στην συνέχεια ο κώδικας P(Y). Ο κώδικας P(Y) όταν είναι κρυπτογραφημένος απεικονίζεται ως Y.

Η παρεμβολή στον κώδικα C/A είναι παρεμβολή ευρείας ζώνης. Παρεμβάλει την λήψη από το δορυφόρο στο δέκτη, εκμεταλλευόμενη την αδύναμη συσχέτιση μεταξύ διαφορετικών κωδικών C/A. Τέλος η μονής συχνότητας παρεμβολή είναι μία παρεμβολή στενής ζώνης [12] συχνοτήτων.

2.2.1 Ευπάθειες του GPS

Η χρήση του στρατιωτικού σήματος GPS είναι ασφαλής γιατί υποστηρίζεται από πολλαπλά συστήματα και διάφορα μέτρα ασφαλείας στο επίπεδο του δικτύου, όπως η κρυπτογράφηση και η κρυπτογραφημένη αυθεντικοποίηση. Σε αντίθεση με τα παραπάνω, το πολιτικό σήμα θεωρείται σχετικά ανασφαλές.

Μία δομική ευπάθεια του συστήματος GPS σε επιθέσεις στο σήμα του είναι η χαμηλή ισχύς του 10-16 Watt (-160 dBW) [5], όταν αυτό λαμβάνεται από τους επίγειους δέκτες.

Τα σήματα του GPS διαθέτουν τρεις βασικές κατηγορίες ευπαθειών :

α) ακούσιες παρεμβολές, όπως σήματα από άλλους πομπούς και ιονοσφαιρική παρεμβολή.

β) παρεμβολή με πρόθεση. Αυτές περιλαμβάνουν παρεμβολές, πλαστοπροσωπία και επανεκπομπή λανθασμένου σήματος.

γ) ο ανθρώπινος παράγοντας και η έλλειψη εκπαίδευσής του .

Οι ακούσιες παρεμβολές προκαλούνται από ατμοσφαιρικούς παράγοντες, καθυστέρηση του σήματος και λάθος στο χρονισμό με αποτέλεσμα εσφαλμένη τοποθεσία. Στις εκ προθέσεως παρεμβολές έχουμε καθολική απώλεια του σήματος ή σήματα πλαστοπροσωπίας [13].

Οι ευπάθειες δεν υφίστανται μόνο στη δομή του σήματος και στο συνολικό σχεδιασμό του συστήματος, αλλά και στο λογισμικό του λειτουργικού συστήματος. Στην παραπομπή σημειώνεται ότι σήματα πλαστοπροσωπίας μπορούν να μεταφέρουν κακόβουλο κώδικα και να προσβάλουν το λογισμικό του δέκτη. Με αυτό το τρόπο, μπορούν να αποκτήσουν αναβαθμισμένα δικαιώματα ή να

εκτελέσουν μία επίθεση άρνησης της υπηρεσίας, εξαντλώντας τους υπολογιστικούς πόρους του δέκτη.

2.3 Μη Επανδρωμένα Αεροσκάφη

2.3.1 Χαρακτηριστικά και πλεονεκτήματα

Τα τελευταία χρόνια, τα μη επανδρωμένα αεροσκάφη (ΜΕΑ) αποκτούν ένα συνεχώς αυξανόμενο ρόλο σε διάφορους τομείς. Στο στρατιωτικό τομέα, ο οποίος είναι και ο κινητήριος μοχλός για την ανάπτυξη τους, έχουν αποκτήσει σημαντικό ρόλο σε αποστολές συλλογής πληροφοριών, αντικατασκοπίας, παρακολούθησης και ως επιθετικά όπλα, φέροντας οπλισμό.

Η χρηστικότητά τους δεν περιορίζεται μόνο σε στρατιωτικές εφαρμογές. Πλέον, αποτελεί κομμάτι πολλών τομέων της πολιτικής ζωής μας. Μία από αυτές τις εφαρμογές είναι στην ασφάλεια από πολιτικούς φορείς όπως η αστυνομία, αλλά και ιδιωτικές εταιρίες παροχής ασφάλειας [14].

Τα μοντέρνα ΜΕΑ επιτρέπουν νέες δυνατότητες ανάπτυξης, λειτουργίας και ανάκτησης εξοπλισμού σε επικίνδυνες και δυσπρόσιτες, από τον άνθρωπο, περιοχές . Τα ΜΕΑ δεν υπάγονται σε ανθρώπινους περιορισμούς, όπως ταχύτητα, χωρητικότητα, δύναμη, ισχύ και ανθεκτικότητα.

Τα ΜΕΑ εξασφαλίζουν υπηρεσίες, ιδιαίτερα για το στρατό, για παράδειγμα την μεταφορά εξοπλισμού, την παρατήρηση, την παρακολούθηση, την επίθεση και την υποστήριξη μάχης . Η ανάπτυξη των ΜΕΑ συμβάλλει στη γεωγραφική αποτύπωση σε επιχειρήσεις εντοπισμού και διάσωσης, καθώς και παρακολούθησης οχημάτων [15][16]. Οι πρόσφατες τεχνολογικές εξελίξεις επιτρέπουν την ανάπτυξη ευέλικτων και πολύ μικρών σε μέγεθος ΜΕΑ . Για αυτό το λόγο αποτελούν άριστες επιλογές για παράδειγμα για λαθραίες μεταφορές σε απομακρυσμένες περιοχές. Ένα ΜΕΑ δύναται να φέρει ακόμα και βιολογικούς ή χημικούς παράγοντες και να εισβάλει, χωρίς εντοπισμό, σε μία ιδιωτική περιοχή [17]. Μικρού μεγέθους ΜΕΑ αποφεύγουν τον εντοπισμό από εξελιγμένα ραντάρ αντιαεροπορικών συστημάτων. Παράδειγμα ίσως αποτελεί η πρόσφατη επίθεση σε διαλυστήρια της Σαουδικής Αραβίας (14 Σεπτεμβρίου 2019, εικάζεται η χρήση ΜΕΑ για υποβοήθηση εκτόξευσης πυραύλων).

2.3.2 Ευπάθειες ΜΕΑ

Το βασικό ζήτημα ασφάλειας των ΜΕΑ είναι το μικρό μέγεθος [17] που περιορίζει το φόρτο και συνεπώς και την υπολογιστική του δυνατότητα. Ένας επίσης, σημαντικός περιορισμός είναι, ότι τα ΜΕΑ αποτελούνται από ξεχωριστά πολλαπλά πολύπλοκα υποσυστήματα, στα οποία είναι δύσκολη η καθολική εφαρμογή ασφάλειας στο σύνολό τους. Επιπλέον, υφίσταται μία σχέση μεταξύ ασφάλειας και λειτουργικότητας, την οποία ο σχεδιαστής του συστήματος οφείλει να εξισορροπήσει. Τα επίπεδα που εξετάζονται στην ασφάλεια είναι τρία. Το πρώτο επίπεδο αφορά τη φυσική ασφάλεια, το δεύτερο, τον έλεγχο λογισμικού και διεπαφών (συχνοί στόχοι κυβερνοεπιθέσεων) και το τρίτο τις συνδέσεις και τις δικτυακές δυνατότητες. Το τελευταίο είναι το πιο ευπαθές σημείο λόγω της αλληλοεπίδρασης με εξωτερικά συστήματα. Επομένως, οι απειλές στο τρίτο επίπεδο προέρχονται τόσο από το κυβερνοχώρο, όσο και από τον ηλεκτρονικό πόλεμο.

2.3.3 Κίνητρα για Επίθεση σε ΜΕΑ

Τα ΜΕΑ παρέχουν δυνατότητες σε επιχειρήσεις τόσο επιθετικές, όσο και πληροφοριών . Η ανάπτυξη συστημάτων ΜΕΑ απαιτεί χρόνο και επένδυση σε εξοπλισμό και προσωπικό. Ιδανικά, ο σκοπός των επιθέσεων σε ΜΕΑ είναι να αποκτήσουμε τον έλεγχό τους και όχι να τα καταρρίψουμε (κυρίως με ενέργειες ηλεκτρονικού πολέμου).

Τα κύρια πλεονεκτήματα απόκτησης – κλοπής ενός επιχειρησιακού ΜΕΑ ενός υποτιθέμενου αντιπάλου (εχθρού), είναι τα παρακάτω :

1. Αυτοάμυνα,
2. Πρόκληση στον επιτιθέμενο,
3. Επίδειξη δυνατοτήτων,
4. Διατήρηση πόρων,
5. Απόκτηση Τεχνογνωσίας,
6. Ψυχολογικές επιχειρήσεις,
7. Συλλογή Πληροφοριών,
8. Αντικατασκοπία,
9. Διαπραγματευτικό Χαρτί,
10. Χρήση ενάντια στον ιδιοκτήτη του.

Η κατοχή ενός ΜΕΑ μίας άλλης αρχής είναι ξεκάθαρη δήλωση υπεροχής στο τομέα του ηλεκτρονικού πολέμου και του κυβερνοπολέμου. Λειτουργεί ως παράδειγμα και προειδοποίηση έναντι εχθρικών και φίλιων δυνάμεων. Ένα ΜΕΑ μπορεί να μετατραπεί σε όπλο και να αποτελέσει μήνυμα ενάντια της εχθρικής αεροπορικής επιθετικότητας **[17α]**.

Στην περίπτωση οπλισμένου ΜΕΑ υπάρχει πάντοτε η δυνατότητα να χρησιμοποιηθεί το ίδιο ενάντια στον αρχικό του κάτοχο. Ακόμα και αν το ΜΕΑ δεν είναι οπλισμένο, μπορεί να χρησιμοποιηθεί σε επιθέσεις τύπου καμικάζι (αναλόγως των διαστάσεών του), όπως στην επίθεση των διδύμων πύργων. Τα σύγχρονα ΜΕΑ διαθέτουν έναν αριθμό από τεχνολογίες, όπως stealth, υλικά κατασκευής, μηχανολογίας και τηλεπικοινωνίας, οι οποίες φυλάσσονται αυστηρά. Με την κατάληψη ενός ΜΕΑ, μπορούμε να το αναλύσουμε με σκοπό την καλύτερη αντιμετώπιση του, καθώς και την αντιγραφή της τεχνολογίας του . Τα ΜΕΑ αποτελούν μία αξιόπιστη λύση μεταφοράς όπλων και ιδανικά συστήματα για μεταφορά βιοχημικών παραγόντων . Επομένως, αποτελούν ένα πολυπόθητο στόχο για πολλούς πιθανούς πελάτες σε παγκόσμια κλίμακα.

2.4 Πλαστοπροσωπία, Παρεμβολή και Επανεκπομπή Εσφαλμένου Σήματος

2.4.1 Αρχές των διεθνών παρεμβολών

Η παρεμβολή αναγκάζει τον δέκτη να απολέσει την αυθεντικοποίηση του σήματος GPS και έτσι δίνεται η δυνατότητα σε σήματα πλαστοπροσωπίας να εξαπατήσουν το δέκτη. Η λήψη του σήματος GPS εμποδίζεται με την εκπομπή σημάτων στις ίδιες συχνότητες με μεγαλύτερη ισχύ . Οι τύποι παρεμβολών που χρησιμοποιούνται είναι:

- στενής ζώνης,

- ευρείας ζώνης και

- φασματικής εξάπλωσης .

Η επανεκπομπή εσφαλμένου σήματος εκτελείται με την λήψη του αυθεντικού σήματος GPS, την προσθήκη καθυστέρησης και την επανεκπομπή του. Το τελευταίο, συνιστά πλαστοπροσωπία και αποτελεί μία από τις κύριες απειλές των δορυφορικών συστημάτων πλοήγησης. Η παραπάνω απειλή απλά παράγει ή πλαστογραφεί σήματα GPS με σκοπό την εξαπάτηση των δεκτών σχετικά με την θέση τους, το χρόνο τους και την ταχύτητα τους. Εσφαλμένα σήματα εκπέμπονται για να ακυρώσουν τις δυνατότητες των δεκτών.

Στην πολιτική έκδοση του GPS είναι εφικτό το παραπάνω με σχετική ευκολία, γιατί η διαμόρφωση του σήματος είναι προβλέψιμη, αφού η πληροφορία αυτή είναι διαθέσιμη στο κοινό [18]. Στη στρατιωτική έκδοση, η επίθεση είναι ιδιαίτερα δύσκολη, αφού το σήμα είναι κρυπτογραφημένο και δεν μπορεί να πλαστογραφηθεί. Τα βασικά βήματα για την πλαστοπροσωπία είναι η λήψη και η παρακολούθηση του σήματος C/A, η ρύθμιση ενός ψευδούς χρόνου και η εκπομπή του σε ισχύ υψηλότερη από το αυθεντικό σήμα του GPS [11]. Η υλοποίηση αυτών παρουσιάζει διάφορες δυσκολίες, παρόλα αυτά μας επιτρέπει όχι μόνο να καταστρέψουμε το MEA, αλλά και να το καταλάβουμε.

Η παρεμβολή και η πλαστοπροσωπία διαφέρουν ως προς τον τρόπο διεξαγωγής. Η πιο αρχέγονη μορφή πλαστοπροσωπίας έχει το ίδιο αποτέλεσμα με την παρεμβολή, φράζοντας το σήμα. Εξελιγμένες μορφές πλαστοπροσωπίας αποσκοπούν στην κατάληψη του σήματος GPS και όχι στην φραγή του. Η παρεμβολή λοιπόν, είναι μία επίθεση στην διαθεσιμότητα του μέσου και η πλαστοπροσωπία, μία επίθεση στην ακεραιότητα του στόχου. Ανάλογα με την πολυπλοκότητα των επιθέσεων πλαστοπροσωπίας τις κατατάσσουμε σε διαφορετική κατηγορία. Απλές επιθέσεις παράγουν πλαστά σήματα, χωρίς να υπολογίζουν αν είναι συνεπή με το αυθεντικό σήμα GPS. Υψηλότερης πολυπλοκότητας επιθέσεις συγχρονίζουν το σήμα τους με το αυθεντικό GPS, αλλά απαιτούν περισσότερες πληροφορίες για το σήμα, όπως ισχύ, δεδομένα πλοήγησης, κατεύθυνση και γωνία λήψης από το δορυφόρο. Τέλος, οι πιο πολύπλοκες επιθέσεις συνδυάζουν πολλαπλούς πομπούς πλαστογραφημένου σήματος, που λειτουργούν σε δίκτυο και είναι συντονισμένοι ως προς τα σήματα που εκπέμπουν.

Οι απλές επιθέσεις εντοπίζονται εύκολα και έχουν περιορισμένες δυνατότητες. Η μεσαία κατηγορία είναι δυσκολότερη στον εντοπισμό της και παράγουν σημαντικά πιο πιστευτό σήμα, αυξάνοντας την δυνατότητά τους. Οι πολυπλοκότερες επιθέσεις απαιτούν αυξημένους πόρους,

κατοχυρώνοντας έτσι εξασφαλισμένη επιτυχία. Μόνο η κρυπτογράφηση του σήματος μπορεί να αντιμετωπίσει τέτοιου είδους επιθέσεις [19]. Το αποτέλεσμα αυτής της επίθεσης είναι η σταδιακή μετακίνηση του MEA σε τοποθεσία της επιθυμίας του επιτιθέμενου [20].

2.4.2 Αντιμετώπιση της Πλαστοπροσωπίας

Για μία επιτυχημένη επίθεση απαιτείται η εκπομπή του κατάλληλου πλαστού σήματος με το σωστό χρόνο και την επιβολή στον δέκτη να πειστεί για την ορθότητα του σήματος του επιτιθέμενου . Η επίθεση αυτή θεωρείται μία από τις βασικές απειλές του πολιτικού GPS. Επίσης έχει προταθεί τεχνική εντοπισμού και προστασίας με χρήση της διάκρισης λήψης, του εύρος και της κρυπτογραφημένης αυθεντικοποίησης. Επιπλέον, έχουν προταθεί διάφορες μεθόδους εντοπισμού [21,43] :

α) η σύγκριση της μέσης τιμής ισχύος του σήματος με την ισχύ του σήματος που λαμβάνεται, όπου διαχωρίζουν τα πλαστά από τα αυθεντικά σήματα.

β) ο έλεγχος των χρονικών διαστημάτων των μηνυμάτων, αν είναι περιοδικά, εντοπίζει το πλαστό σήμα.

γ) η παρακολούθηση των κωδικών ταυτοποίησης των δορυφόρων GPS.

δ) η μέτρηση των σημάτων και εντοπισμό ψεύτικων σημάτων.

Η κρυπτογράφηση αποτελεί την μοναδική βιώσιμη επιλογή για την ασφάλιση του διαστημικού συστήματος πλοήγησης. Υφίστανται δύο βασικοί τύποι κρυπτογράφησης κλειδιού. Στο πρώτο τύπο χρησιμοποιείται ένα συμμετρικό κλειδί και στο δεύτερο χρησιμοποιείται ένα ζευγάρι κλειδιών για ασύμμετρη κρυπτογράφηση [23]. Στην συμμετρική κρυπτογράφηση υπάρχει υψηλό κόστος, τόσο στο φυσικό κόσμο, όσο και σε επίπεδο κυβερνοασφάλειας για το διαμοιρασμό του κλειδιού . Για το λόγο αυτό χρησιμοποιείται μόνο από στρατιωτικές εφαρμογές. Στον αντίποδα, η ασύμμετρη κρυπτογράφηση είναι ιδανική για πολιτικές εφαρμογές .

Προτείνονται οι εξής μέθοδοι για την αντιμετώπιση της πλαστοπροσωπίας :

α) Ανάθεση επιπλέον φασμάτων (L1, L2, L5),

β) Εισαγωγή κυρώσεων για διεθνείς παρεμβολές,

γ) Παρακολούθηση της ακεραιότητας του συστήματος,

δ) Αυθεντικοποίηση του σήματος με κρυπτογράφηση,

ε) Υπογραφή των μηνυμάτων του σήματος ή των κωδικών του φάσματος.

2.5 Ανατομική προσέγγιση μοντέλου επιθέσεων σε επιχειρήσεις ηλεκτρονικού πολέμου και κυβερνοασφάλειας

Οποιαδήποτε πρόσβαση χωρίς αυθεντικοποίηση σε ένα σύστημα θεωρείται προσβολή. Στην ανατομική προσέγγιση εξετάζουμε την προσβολή βήμα προς βήμα και περιγράφουμε την επίθεση.

2.5.1 Εντοπισμός Ευπαθειών

Σημαντικό προαπαιτούμενο μίας ανατομικής προσέγγισης είναι η ταυτοποίηση των αδυναμιών του συστήματος στόχου, που οδηγούν σε εκμετάλλευση και απώλεια του ελέγχου. Αυτό είναι το πρώτο στάδιο της προσέγγισης. Είναι κρίσιμο στάδιο, διότι αποτελεί την αρχή για τον σχεδιασμό της επίθεσης και τον καθορισμό των απαραίτητων εργαλείων και δεξιοτήτων.

Υπάρχουν τρεις κύριες οδοί επικοινωνίας στα ΜΕΑ. Αυτές οι οδοί αποτελούν τους υποψήφιους φορείς επιθέσεων. Οι οδοί αυτοί είναι:

α) Η ραδιοεπικοινωνία με τον επίγειο σταθμό βάσης,

β) Η δορυφορική επικοινωνία με GPS και

γ) Τυχόν ασύρματα κανάλια ανταλλαγής πληροφοριών με άλλα ΜΕΑ.

Ο επιτιθέμενος μπορεί να εκτελεί επιθέσεις σε μία από τις παραπάνω οδούς επικοινωνίας για να προσβάλει ένα ΜΕΑ.

Ένας ακόμα φορέας επίθεσης είναι οι ευπάθειες στο υλικό και στο λογισμικό [17]. Κάθε ευπάθεια παρουσιάζει ιδιαίτερα ρίσκα, για αυτό το λόγο τις κατηγοριοποιούμε σύμφωνα με τα επίπεδα που υπάρχουν. Με αυτή την οπτική, τα συστήματα GPS μπορούν να προσβληθούν :

α) Στον Επίγειο Σταθμό Ελέγχου, όπου εκπέμπονται τα μηνύματα.

β) Στις συνδέσεις μεταξύ του Επίγειου Σταθμού και του δορυφόρου GPS, όπου τα μηνύματα μεταφέρονται.

γ) Στα κανάλια εκπομπής μεταξύ δορυφόρου και δέκτη κατά την λήψη των σημάτων GPS.

δ) Στην επεξεργασία των μηνυμάτων εσωτερικά του δέκτη.

Τα πρώτα δύο αντικείμενα κατηγοριοποιούνται σαν λάθη στο επίπεδο του συστήματος, το τρίτο ως επίπτωση του περιβάλλοντος επιχειρήσεων και το τελευταίο ως ελάττωμα στο επίπεδο του χρήστη .

2.5.2 Επιθέσεις σε ΜΕΑ

Το δεύτερο στάδιο εκτελεί επιθέσεις στις τρεις αρχές ασφαλείας: εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

- Η εμπιστευτικότητα στα συστήματα ΜΕΑ τίθεται σε κίνδυνο από κακόβουλο λογισμικό στα επιμέρους συστήματα, από προσβολή στα δίκτυα ή από ανθρώπινο λάθος.
- Η ακεραιότητα προσβάλλεται από διακοπή επικοινωνίας και λήψη με επανεκπομπή σημάτων.
- Τέλος, η διαθεσιμότητα τίθεται σε κίνδυνο από παρεμβολή σήματος, άρνηση της υπηρεσίας και πλαστοπροσωπία .

Σε μία επίθεση σε ΜΕΑ, όλες οι αρχές ασφάλειας βρίσκονται σε κίνδυνο. Ο δέκτης GPS είναι ένας μικρός υπολογιστής, επομένως είναι εκτεθειμένο σε όλες τις επιθέσεις που εκτελούνται σε υπολογιστές. Όλες αυτές οι επιθέσεις αποτελούν απειλή για το ΜΕΑ. Η περιορισμένη υπολογιστική ικανότητα των δεκτών τους, εκθέτει τα ΜΕΑ σε επιθέσεις και άρνηση της υπηρεσίας. Κενά ασφάλειας στις ασύρματες επικοινωνίες μπορούν να προκαλέσουν κατάληψη της επικοινωνίας του ΜΕΑ με την βάση του. Η παραβίαση της εμπιστευτικότητας και της ακεραιότητας στα δεδομένα που μεταφέρονται, μπορεί να επιτευχθεί από ευπάθειες του λειτουργικού συστήματος, όπως και στις ασύρματες επικοινωνίες. Η απόκτηση δικαιωμάτων στο λειτουργικό σύστημα και κλείσιμο του δέκτη είναι μία βασική απειλή στον κυβερνοπόλεμο [17].

Οι επιθέσεις επανάληψης παραμένουν απειλές, ακόμα και μετά από εφαρμογή κρυπτογράφησης . Τρεις τεχνικές χρησιμοποιούνται για την αντιμετώπισή τους :

α) Χρήση εξωτερικών αισθητήρων για την παρακολούθηση εκτροπής από την σωστή θέση

β) Έλεγχος για ανωμαλίες στο χρόνο λήψης των σημάτων πλαστοπροσωπίας

γ) Εξέταση αλλαγών της μετατόπισης Doppler στο δέκτη GPS

Ένα ακραίο σενάριο για την πειρατεία ενός ΜΕΑ θα ήταν ο επιτιθέμενος να εισχωρήσει από τα στάδια σχεδιασμού, εφαρμογής και παραγωγής του ΜΕΑ και να δημιουργήσει κερκόπορτες, να εισάγει κακόβουλο κώδικα ή άλλη ευπάθεια, είτε στο λογισμικό ελέγχου, είτε στα πρωτόκολλα επικοινωνίας. Το επιδιωκόμενο αποτέλεσμα θα ήταν η ενεργοποίηση του κακόβουλου λογισμικού με την χρήση του σήματος GPS για να απόκτηση του ελέγχου του. Στο σύγχρονο περιβάλλον κυβερνοπολέμου το παραπάνω σενάριο αποκτά υπόσταση λόγω της συνεχούς αυξανόμενης τάσης κυβερνήσεων να χρησιμοποιούν τόσο καλόβουλους, όσο και κακόβουλους ειδικούς κυβερνοασφάλειας, Το πλεονέκτημα που αποκτά ο επιτιθέμενος είναι ότι έχει προβάδισμα και είναι έτοιμος να αντιμετωπίσει την απειλή πριν παρουσιαστεί.

Ιδιαίτερα στις στρατιωτικές εφαρμογές είναι ευκολότερη η εισχώρηση σε εξωτερικούς εργολάβους, από το να σπάσουν κρυπτογραφημένα σήματα GPS. Οι επιθέσεις στο λογισμικό ελέγχου του δέκτη ενός στρατιωτικού GPS έχουν περισσότερες πιθανότητες επιτυχίας. Για την προσβολή του GPS μπορεί να χρησιμοποιηθεί λοιπόν, ένας συνδυασμός παρεμβολών και εργαλείων κυβερνοπολέμου.

2.5.3 Ανάπτυξη Αντιμέτρων

Το τρίτο βήμα στο μοντέλο που εξετάζεται είναι πιθανά αντίμετρα που μπορεί να εφαρμόσει ο αυθεντικός ιδιοκτήτης του ΜΕΑ στις επιθέσεις που προκύπτουν από τις ευπάθειες που έχουμε αναδείξει. Παρόλο που η χρήση κρυπτογράφησης είναι η πιο ενδεδειγμένη λύση, [26] δεν είναι εφικτή, κυρίως λόγω κόστους σε λογισμικό και υλικό που στις περισσότερες περιπτώσεις είναι υψηλό.

Άλλη μία επιλογή αποτελεί η χρήση πολλαπλών δεκτών GPS στο ΜΕΑ τους οποίους το σύστημα ελέγχου εξετάζει και συγκρίνει για να εντοπίσει τυχόν ανωμαλίες στα δεδομένα τους, πριν αυτά χρησιμοποιηθούν για τον υπολογισμό της πλοήγησης του ΜΕΑ. Σε παρόμοια σενάρια χρήσης πολλαπλών δεκτών GPS μόνο ένας ή λίγοι από τους δέκτες χρησιμοποιούνται. Οι υπόλοιποι αποτελούν δολώματα, υλοποιώντας μία πολύπλοκη επιφάνεια για επίθεση. Με αυτό το

τρόπο δυσχεραίνεται το έργο του επιτιθέμενου. Ο επιτιθέμενος θα πρέπει να διαθέτει πολλαπλές κεραίες και να εκτελέσει μία πολύπλοκη επίθεση πλαστοπροσωπίας στο σύστημα ελέγχου. Ακόμα και έτσι, η επίθεση μπορεί να κατευθύνεται στους δέκτες δολώματα που δεν συμβάλλουν στην πλοήγηση του ΜΕΑ.

Ένα ενεργό σύστημα εντοπισμού και αποφυγής εισβολής θα αποτελούταν από ένα οι περισσότερους μηχανισμούς εντοπισμού που έχουν προταθεί παραπάνω. Στην συνέχεια για την αποτροπή της εισβολής ο επιτιθέμενος θα μπορούσε να απενεργοποιεί τον δέκτη GPS που προσβάλλεται και να ειδοποιεί το επίγειο σύστημα για περαιτέρω ανάλυση. Παρόμοιο μοντέλο εφαρμόζεται από την Google στα αυτόνομα οχήματα με την ενσωμάτωση δεδομένων από εξωτερικούς αισθητήρες στον υπολογισμό της θέσης [26].

2.5.4 Πιθανές επιπτώσεις πλαστοπροσωπίας στα ΜΕΑ

Το τέταρτο βήμα στο μοντέλο μας είναι η εξέταση των πιθανών επιπτώσεων των επιθέσεων. Οι ευπάθειες στο GPS επηρεάζουν όλες τις εξαρτώμενες από το χρόνο εφαρμογές, όπως τηλεπικοινωνίες και οικονομικές υπηρεσίες καθώς και εφαρμογές εξαρτώμενες από την θέση, κυρίως πλοήγηση και παρακολούθησης. Το ερώτημα που απαντάμε είναι τι μπορούμε να επιτύχουμε με την πλαστοπροσωπία. Μπορούμε να επιτύχουμε τα ακόλουθα :

α) Την ακούσια τροποποίηση της συμπεριφοράς ενός ΜΕΑ,

β) Την αποφυγή και την τροποποίηση του στόχου ενός πυραύλου,

γ) Την προσβολή υπηρεσιών εξαρτώμενες από το χρόνο και χώρο, όπως το χρηματιστήριο ή οι μεταφορές.

Τα παραπάνω αποτελούν ένα μικρό εύρος της απάντησης στο ερώτημα μας δεδομένου του βαθμού εισχώρησης του GPS στην καθημερινότητα του 21ου αιώνα.

Αφού το ΜΕΑ προσβληθεί και ο έλεγχος του αποκτηθεί δυνητικά μπορεί να χρησιμοποιηθεί ως stealth παρεμβολέας. Η παρεμβολή από αέρα είναι ιδιαίτερα εύκολη ακόμα και αν η φάση του σήματος είναι ίδια με του πραγματικού GPS και μία κεραία εντοπίζει την κατεύθυνση του σήματος.

Τα δημοσίως καταγεγραμμένα συμβάντα επιτυχημένων επιθέσεων σε ΜΕΑ είναι περιορισμένα σε αριθμό. Αποτελούν όμως, ένα ικανό δείγμα για να συμπεράνουμε ότι τόσο τα πολιτικού όσο και του στρατιωτικού τύπου ΜΕΑ είναι ευάλωτα σε ηλεκτρομαγνητικές επιθέσεις, ιδιαίτερα αν συνδυάζονται με κυβερνοεπιθέσεις. Οι πιθανότερες επιθέσεις, χωρίς να έχουν επιβεβαιωθεί επίσημα, είναι η παρεμβολή του σήματος GPS και η πλαστοπροσωπία σήματος GPS.

Επίσης γνωστά συμβάντα είναι η προσβολή δορυφόρου από τρομοκράτες [22] και η λήψη ζωντανής εικόνας, χωρίς κρυπτογράφηση από ΜΕΑ, με φθηνό λογισμικό [24], η προσβολή με κακόβουλο λογισμικό σε αμερικάνικη επίγεια βάση ελέγχου ΜΕΑ [25] και τέλος η κατάληψη αμερικάνικου ΜΕΑ από δυνάμεις του Ιράν [26].

Στην περίπτωση αυτή του Ιράν, η κυβέρνηση του Ιράν παρουσίασε φωτογραφία ενός ΜΕΑ των αμερικανικών ενόπλων δυνάμεων. Οι φωτογραφίες απεικόνιζαν το ΜΕΑ χωρίς εμφανείς βλάβες, εκτός από κάποιες ελάχιστες στο αριστερό φτερό, στοιχείο που υποδεικνύει ότι

προσγειώθηκε και δεν καταρρίφθηκε από την αεράμυνα [27]. Οι επιθέσεις εκτελέστηκαν σε ΜΕΑ τύπου RQ-170, ενός μεγάλου σταθερών πτερυγίων, κατασκοπευτικό ΜΕΑ, κατασκευαστής του οποίου είναι η εταιρία "Lockheed Martin". Η επίθεση εκτελέστηκε από τις Ιρανικές ένοπλες δυνάμεις την 4η Δεκεμβρίου 2011, κοντά στην περιοχή της πόλης Κασμάρ. Σύμφωνα με ισχυρισμούς Ιρανών μηχανικών, το ΜΕΑ καταλήφθηκε αρχικά με παρεμβολή του αυθεντικού σήματος GPS και στην συνέχεια με πλαστοπροσωπία του σήματος GPS. Η επίθεση εντοπίστηκε σε ύστερο χρόνο όταν το ΜΕΑ προσγειώθηκε σε διαφορετικό σημείο από εκεί που έπρεπε.

Η επίθεση αυτή, πέρα από την απώλεια ενός ΜΕΑ, είχε πολλά από τα αποτελέσματα που έχουμε παραθέσει. Σημαντική απώλεια και διαρροή για το σχεδιασμό, τις δυνατότητες και την τεχνολογία του τύπου που καταλήφθηκε. Η τεχνολογία αυτή επιτρέπει στις Ιρανικές ένοπλες δυνάμεις να παράξουν καλύτερα ΜΕΑ, για ιδία χρήση ή και εξαγωγή, καθώς και άμεσα οικονομικά οφέλη με την πώληση απευθείας της τεχνολογίας. Επιπλέον, επιτρέπει την εξεύρεση νέων μεθόδων και τρόπων προσβολής αυτού ή άλλων τύπων ΜΕΑ των αμερικανικών ενόπλων δυνάμεων. Οι οικονομοτεχνικές επιπτώσεις είναι σημαντικές, αλλά στον σημερινό υβριδικό πόλεμο, που διεξάγεται στην περιοχή, η σημαντικότερη παράμετρος ήταν στο τομέα των ψυχολογικών επιχειρήσεων. Οι Ιρανοί έδειξαν στην Μέση Ανατολή και στον κόσμο ότι μπορούν να διεξάγουν ηλεκτρονικό πόλεμο με επιτυχία ενάντια του πιο εξελιγμένου στρατού της περιοχής. Τόνωσαν το ηθικό στο εσωτερικό της χώρας όσο και των ενόπλων δυνάμεων και παράλληλα έστειλαν ισχυρό μήνυμα, ότι η κυριαρχία των αμερικανικών ενόπλων δυνάμεων δεν είναι καθολική στο θέατρο επιχειρήσεων.

Μία από τις ελάχιστες δημόσιες αναφορές επιθέσεων παρεμβολής GPS σε ΜΕΑ είναι στην Ν. Κορέα στις 10 Μαΐου 2012. Η παρεμβολή εκτελέστηκε σε τύπου S-100 Camcopter με κατασκευαστή την εταιρία "Schiebel". Το ΜΕΑ συνετρίβει στο όχημα επίγειου ελέγχου, σκοτώνοντας ένα μηχανικό και τραυματίζοντας δύο πιλότος κατά την διάρκεια δοκιμών. Ο επιτιθέμενος μέχρι σήμερα δεν έχει ταυτοποιηθεί. Η επίθεση εντοπίστηκε μετά την συντριβή του ΜΕΑ και τα στοιχεία καταδεικνύουν ότι η παρεμβολή ξεκίνησε από τις 28 Απριλίου. Τα κοντινά αεροδρόμια του Ιντσεόν και της Γκίμπο επηρεάστηκαν από την παρεμβολή του σήματος GPS διακόπτοντας πολιτικές πτήσεις .

Τα παραπάνω πραγματικά συμβάντα καταδεικνύουν ότι θεωρητικά η κατάληψη του ελέγχου ενός ΜΕΑ γίνεται με την παρεμβολή του P(Y) κώδικα και τον εξαναγκασμό του δέκτη GPS να χρησιμοποιήσει το πολιτικού τύπου, χωρίς κρυπτογράφηση, σήματος GPS. Ο P(Y) κώδικας ονομάζεται ακριβής, είναι μια σειρά από ένα και μηδέν, με ρυθμό παραγωγής 10,23 million bits/sec, σε συχνότητες L1 και L2 των δορυφόρων, με εκπομπή μέρους αυτού ανά εβδομάδα και ταυτοποίηση από τον δέκτη GPS με το τμήμα αυτό την συγκεκριμένη εβδομάδα του έτους.

Ισχυρά αποδεικτικά στοιχεία παρουσιάζονται στη παραπομπή [11] για προσβολή πολιτικού τύπου ΜΕΑ και υφίστανται υποψίες ότι και στρατιωτικού τύπου ΜΕΑ μπορούν να επηρεαστούν, παρόλο που θεωρητικά έχουν ανοσία σε αυτού του είδους της παρεμβολές.

2.6 Συμπεράσματα Κεφαλαίου

Οι στρατιωτικές επικοινωνίες χρησιμοποιούν κρυπτογραφημένα σήματα GPS με ασφαλέστερο λογισμικό και υλικό στους δέκτες τους. Αν και παρουσιάζουν λοιπόν, ανοχή σε επιθέσεις και παρεμβολές, δεν θα πρέπει να θεωρούνται απολύτως ασφαλείς.

Στην σημερινή εποχή, ισχυροί παράγοντες στον κυβερνοχώρο είναι έθνη, ομάδες χορηγούμενες από έθνη, διακρατικοί οργανισμοί, επίσημες και ανεπίσημες υπηρεσίες πληροφοριών και τέλος οι ένοπλες δυνάμεις χωρών. Οι προαναφερόμενοι διαθέτουν πόρους και μέσα για να υπερβούν αντίμετρα και μηχανισμούς άμυνας. Για αυτό το λόγο, δεν μπορούμε να αγνοήσουμε απειλές σε κρίσιμες, για τις αποστολές, υπηρεσίες και υποδομές όπως η ασφαλή επικοινωνία MEA με τους δορυφόρος GPS. Επιπρόσθετη απόδειξη είναι οι πρόσφατες προσβολές MEA στο στρατιωτικό τομέα.

Η κρυπτογραφημένη αυθεντικοποίηση του σήματος GPS παρουσιάζεται ως η καλύτερη, αλλά και η πιο δύσκολη στην εφαρμογή της λύσης για πολιτική χρήση. Για αυτό, η ευπάθεια πρέπει να επισημανθεί από τους ίδιους τους κατασκευαστές και να ενημερωθεί το κοινό για τις πιθανές επιπτώσεις. Στο μέλλον θα πρέπει να εφαρμοστούν στα MEA μηχανισμοί αποτροπής και εφεδρικά συστήματα πλοήγησης. Η απόδοση ευθυνών είναι ουσιαστικά ανέφικτη στο κυβερνοχώρο, διότι οι επιτιθέμενοι χρησιμοποιούν ενδιάμεσους για να εκτελέσουν επιθέσεις.

Κεφάλαιο 3

Ιπτάμενα Ad-Hoc (της στιγμής) Δίκτυα

3.1 Εισαγωγή

Η χρησιμοποίηση των ΜΕΑ, γνωστά και ως UAV (Unmanned Aerial Vehicle) ή Drone, αναμένεται να αυξηθεί με ραγδαίους ρυθμούς, λόγο του αυξημένου ενδιαφέροντος από ερασιτέχνες, ερευνητές και επενδυτές. Καθώς ο αριθμός των Drone αυξάνετε, το Internet-of-Drone (IoD) και οι εφαρμογές του θα εξαπλώνονται, καθώς μυριάδες Drone διαφόρων μεγεθών αλληλοεπιδρούν αυτόματα αναμεταξύ τους, μέσω των παρόχων υπηρεσιών ζώνης για την επίτευξη του συντονισμού της πρόσβασης των Drone στον ελεγχόμενο εναέριο χώρο και να παρέχει και υπηρεσίες πλοήγησης . Έχει υπολογιστεί ότι η αγορά των Drone από ερασιτέχνες και από επιχειρήσεις θα αυξηθεί κατά 4.3 εκατομμύρια και 2.7 εκατομμύρια αντίστοιχα, μέχρι το 2020 . Η οικονομική αύξηση στην βιομηχανία των Drone στις Η.Π.Α., συμπεριλαμβανόμενη και της παραγγελίας-παράδοσης πακέτων, την παρακολούθηση της κυκλοφορίας και του περιβάλλοντος, την επιθεώρηση υποδομών, την εναέρια φωτογράφιση, την αστική ασφάλεια, τις στρατιωτική παρακολούθηση κλπ. αναμένετε ότι θα έχει σημαντική συμβολή στις πωλήσεις. Το 2020, η βιομηχανία ΜΕΑ στις Η.Π.Α. αναμένεται να φτάσει τα 4 δισεκατομμύρια δολάρια [28]. Με την πρόοδο των ασύρματων συνδέσεων, τον υπολογισμό ομίχλης σε συνδυασμό με την ραγδαία τεχνολογική ανάπτυξη στα ηλεκτρονικά, στους αισθητήρες και στην τεχνολογία επικοινωνίας, οραματιζόμαστε ένα μέλλον στον οποίο τα Drone έχουν αφομοιωθεί στο IoD και βοηθούν στην καλυτέρευση της καθημερινής ζωής.

Ως μέρος της ραγδαίας ανάδειξης του IoD, τα Flying Ad Hoc Network (FANET) παίζουν πολύ σημαντικό ρόλο στην πραγματοποίηση των διαρκών υπολογισμών και της επικοινωνίας, όπου συγκεκριμένα Drone συνεργάζονται με ακεραιότητα και αξιοπιστία για την μεταφορά δεδομένων σε έναν προορισμό, με στόχο την κοινή χρήση αυτών των πληροφοριών και γνώσεων, και στον συντονισμό λήψης αποφάσεων. Στις προηγούμενες δεκαετίες, οι ερευνητές είχαν επικεντρωθεί στην μελέτη των αλγόριθμων επικοινωνίας και τα πρωτόκολλα διασύνδεσης στο Mobile Ad Hoc Network (MANET) και στα Vehicular Ad Hoc Network (VANET), αντίστοιχα. Παρ' όλα αυτά λόγο της υψηλής κινητικότητας, της αραιής ανάπτυξης, της γρήγορης εναλλαγής τοπικών δικτύων, των συνεχόμενων διακοπτόμενων συνδέσεων των δίαυλων επικοινωνίας, και των σκόπιμων παρεμβολών, αυτές οι τεχνικές σχεδιαστήκαν συγκεκριμένα για MANET και VANET και δεν μπορούν να εφαρμοστούν στα FANET. Με άλλα λόγια, η διασύνδεση απαιτεί από τα FANET να υπερβούν τις ανάγκες των MANET και των VANET [29]. Για παράδειγμα, η επίδοση του δικτύου (π.χ. ρυθμός παράδοσης πακέτων) μπορεί να μειωθεί σημαντικά σε MANET με υψηλή κινητικότητα, λόγο συχνών σφαλμάτων των συνδέσεων .

Στην αραίωση δικτύου, η διακοπή στην σύνδεση μπορεί να διαρκέσει για μεγάλα χρονικά διαστήματα, τα οποία μπορεί να δημιουργήσουν ουρά από εκτελέσιμες εντολές, γιατί οι νέες εντολές δεν προλαβαίνουν να εκτελεστούν, δημιουργώντας καθυστέρηση μετάδοσης των δεδομένων [30]. Στο πρότυπο IEEE 802.11 (Institute of Electrical and Electronics Engineers), που βασίζεται στα ad hoc δίκτυα, ένας σαμποτέρ μπορεί εύκολα να μειώσει σημαντικά την απόδοση του δικτύου, με την διαρκή αναμετάδοση σημάτων παρεμβολής μέσα στο κοινό ασύρματο μέσο επικοινωνίας.

3.2 Αρχιτεκτονικές Επικοινωνίας

Μία αρχιτεκτονική επικοινωνίας προσδιορίζει τον τρόπο ανταλλαγής πληροφοριών μεταξύ του σταθμού βάσης και ενός ΜΕΑ ή μεταξύ πολλών ΜΕΑ. Στην αρχιτεκτονική των FANET, τα ΜΕΑ παρέχουν επικοινωνία σε πραγματικό χρόνο με τρόπο ad hoc, η οποία μπορεί να καταργήσει την ανάγκη για υποδομές και να διορθώσει τον περιορισμό εύρους επικοινωνίας [31]. Η αρχιτεκτονική των FANET διαδραματίζει σημαντικό ρόλο ιδιαίτερα σε ένα σενάριο όπου οι περιορισμοί επικοινωνίας κι εύρους, πάντα σε πραγματικό χρόνο, αποτελούν κύρια ζητήματα και όπου είναι δύσκολο να παρασχεθεί υποδομή [32]. Στην περίπτωση των FANET, τα ΜΕΑ συνδέονται και αποσυνδέονται στο δίκτυο συχνά, για αυτό το λόγο τα ad hoc δίκτυα είναι η καλύτερη λύση για την επικοινωνία μεταξύ των ΜΕΑ.

Επιπλέον, για ταχύτερη και εύρωστη επικοινωνία μεταξύ των ΜΕΑ, η αποκεντρωμένη αρχιτεκτονική επικοινωνίας είναι καταλληλότερη. Υπάρχουν πολλές διαφορετικές αρχιτεκτονικές επικοινωνίας που προτείνονται για συστήματα με πολλά ΜΕΑ . Παρακάτω θα επικεντρωθούμε στις τρεις βασικές αρχιτεκτονικές επικοινωνίας των FANET.

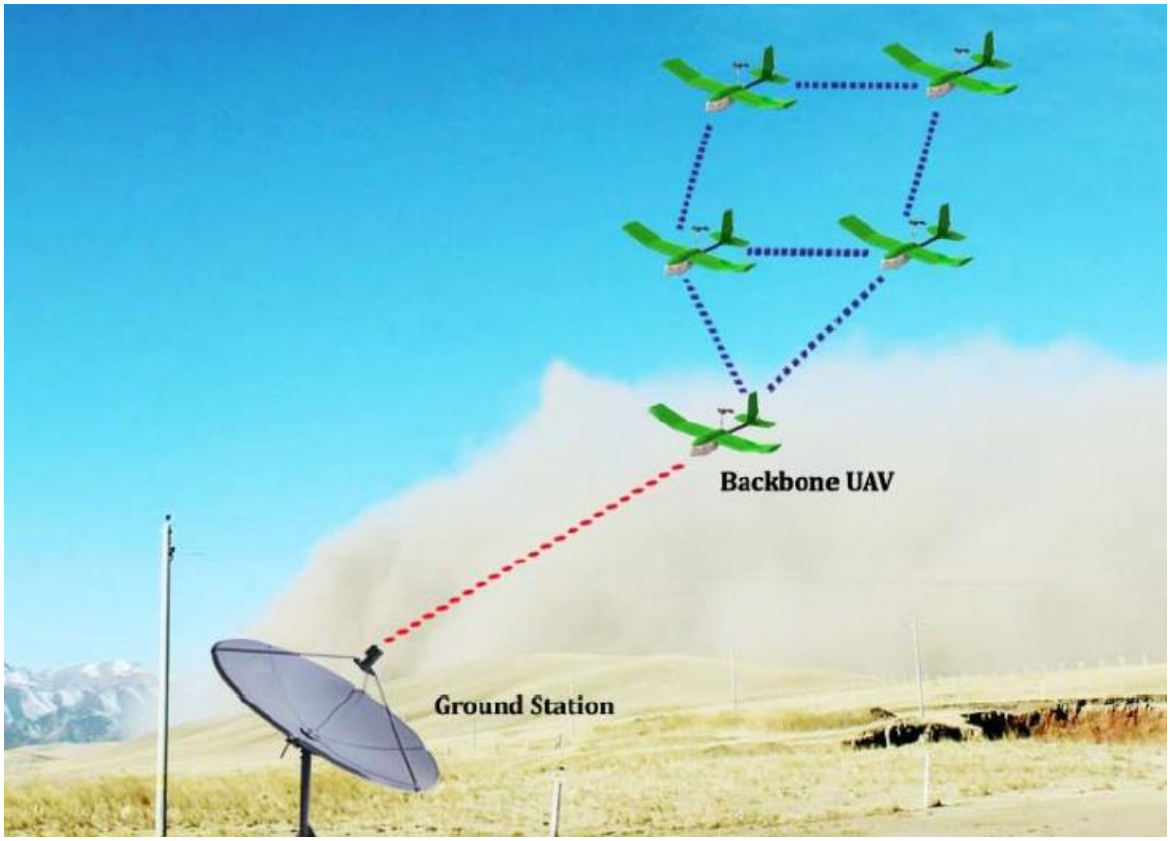
3.2.1 Δίκτυα Ad-Hoc στα ΜΕΑ

Σε μία αρχιτεκτονική δικτύου με ΜΕΑ σε Ad Hoc, όλα τα ΜΕΑ συνδέονται μεταξύ τους και με το σταθμό βάσης, αυτόνομα, χωρίς να έχουν εξαρχής εγκαθιδρύσει επικοινωνία. Σε αυτή τη συγκεκριμένη αρχιτεκτονική, κάθε UAV συμμετέχει στην προώθηση δεδομένων του συστήματος FANET. Στο δίκτυο Ad-hoc, ένα ΜΕΑ λειτουργεί ως πύλη μεταξύ του επίγειου σταθμού και των άλλων ΜΕΑ, όπως φαίνεται στην εικόνα 4.

Το ΜΕΑ πύλη διαθέτει ασύρματες συσκευές επικοινωνίας ικανές να λειτουργούν τόσο σε χαμηλή ισχύ, μικρής εμβέλειας για επικοινωνία με τα ΜΕΑ όσο και υψηλής ισχύος, μεγάλης εμβέλειας για επικοινωνία με το σταθμό εδάφους [33]. Σε μία τέτοια δομή, δεδομένου ότι μόνο το ΜΕΑ πύλη συνδέεται με το σταθμό εδάφους, η εμβέλεια του δικτύου επεκτείνεται σημαντικά. Επιπλέον, η απόσταση μεταξύ των ΜΕΑ είναι σχετικά μικρή.

Το αποτέλεσμα είναι η συσκευή πομποδέκτη στο ΜΕΑ να είναι φθηνή και ελαφριά, γεγονός που την καθιστά καταλληλότερη για ΜΕΑ σε μικρού μεγέθους δίκτυα. Προκειμένου όμως να διατηρηθεί μία συνεχή σύνδεση στο δίκτυο, θα πρέπει η ταχύτητα και η κατεύθυνση να είναι παρόμοια για όλα τα συνδεδεμένα ΜΕΑ στο FANET.

Ως εκ τούτου, αυτή η αρχιτεκτονική δικτύου είναι η πλέον κατάλληλη για μία ομάδα παρόμοιων και μικρού μεγέθους UAV για συγκεκριμένες επιχειρήσεις, όπως η αυτόνομη αποστολή εναέριας επιτήρησης [34].

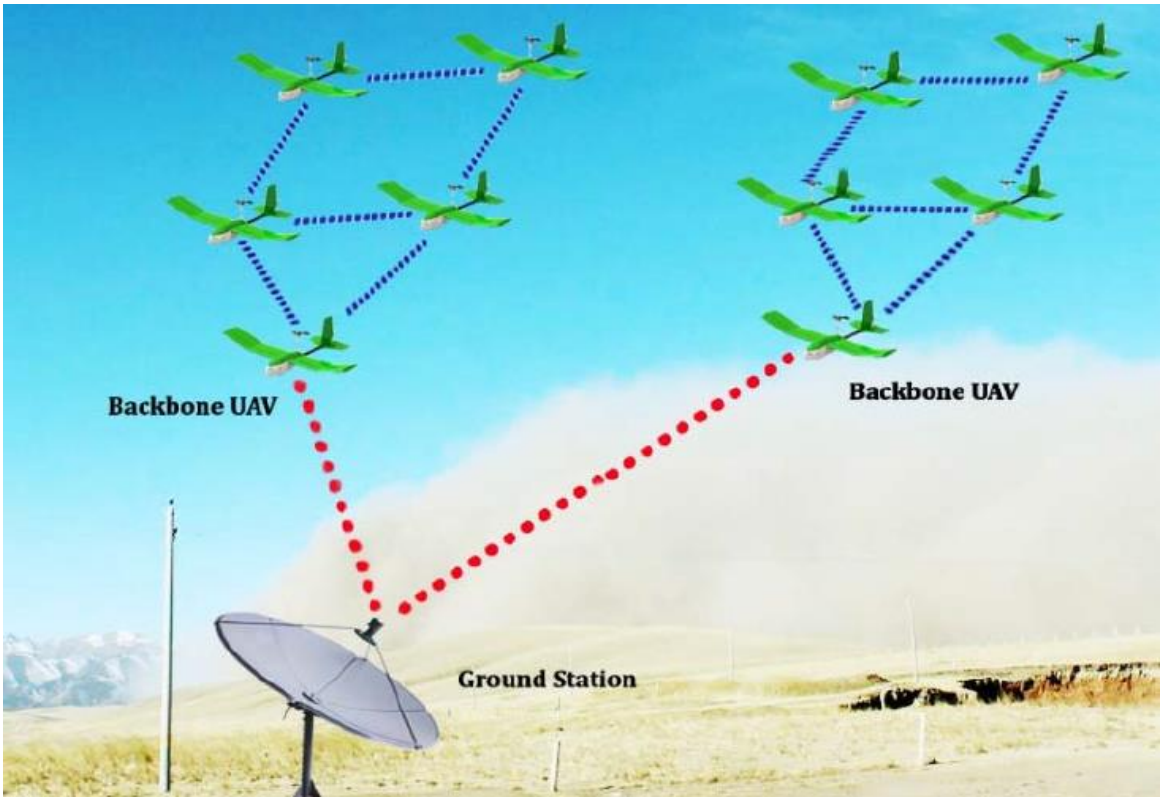


Εικόνα 4 Το ΜΕΑ λειτουργεί ως πύλη μεταξύ επίγειου σταθμού και άλλων ΜΕΑ

3.2.2 Δίκτυα Ad-Hoc σε ομάδες ΜΕΑ

Μία αρχιτεκτονική δικτύου ad hoc με πολλαπλές ομάδες ΜΕΑ είναι η ενσωμάτωση των δικτύων ad-hoc με ένα δικτυοκεντρικού τύπου δίκτυο. Σε αυτό το δίκτυο, όπως φαίνεται στην εικόνα 5, πολλά ΜΕΑ συνδέονται με τρόπο ad hoc εσωτερικά, σε κάθε ομάδα, και οι ομάδες συνδέονται περαιτέρω μέσω των ΜΕΑ πύλης με τον επίγειο σταθμό δικτυοκεντρικά.

Η εσωτερική επικοινωνία εκτελείται χωρίς τη συμμετοχή του επίγειου σταθμού, παράλληλα όμως η επικοινωνία μεταξύ των ομάδων πραγματοποιείται με τη βοήθεια του επίγειου σταθμού. Αυτός ο τύπος αρχιτεκτονικής δικτύου ΜΕΑ είναι κατάλληλος για περιπτώσεις, όπου μεγάλος αριθμός ΜΕΑ συμμετέχει σε μία αποστολή με διαφορετικά χαρακτηριστικά πτήσης και επικοινωνίας. Ωστόσο, λόγω της ημι-συγκεντρωτικής φύσης της, αυτή η επικοινωνιακή αρχιτεκτονική δεν είναι εύρωστη.

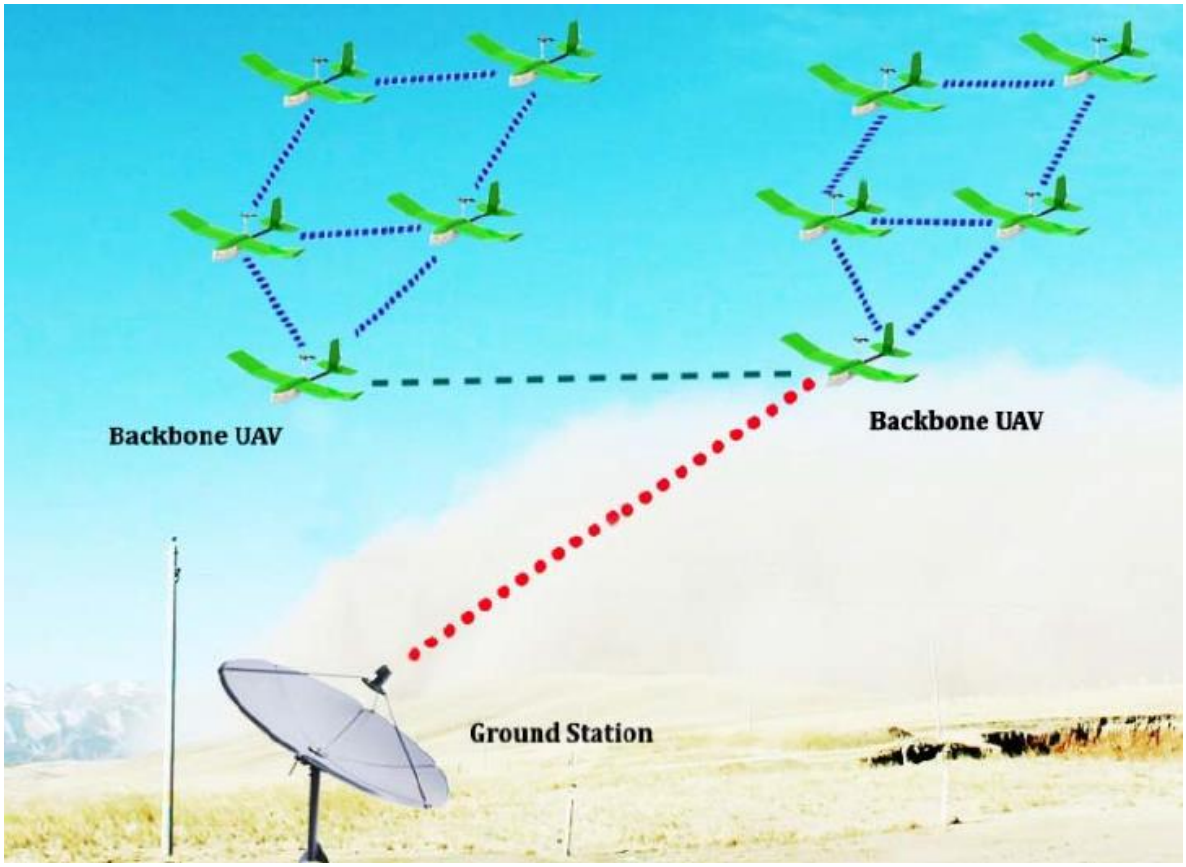


Εικόνα 5 Δίκτυα Ad-Hoc σε ομάδες ΜΕΑ

3.2.3 Δίκτυα Ad-Hoc ΜΕΑ Πολλαπλών Επιπέδων

Ένα δίκτυο ad-hoc ΜΕΑ πολλαπλών επιπέδων εμφανίζεται στην εικόνα 6. Σε αυτή την αρχιτεκτονική έχουμε πολλές ομάδες που αποτελούνται από ετερογενή ΜΕΑ, οι οποίες σχηματίζουν δίκτυα Ad-Hoc σε μεμονωμένες ομάδες. Το χαμηλότερο επίπεδο χρησιμοποιείται για την επικοινωνία μεταξύ αυτών. Το ανώτερο επίπεδο χρησιμοποιείται για την επικοινωνία μεταξύ των ΜΕΑ πύλης της κάθε ομάδας και του επίγειου σταθμού. Τα ΜΕΑ πύλης κάθε ομάδας συνδέονται μεταξύ τους και μόνο ένα ΜΕΑ πύλης συνδέεται περαιτέρω άμεσα με τον επίγειο σταθμό. Η επικοινωνία ή η ανταλλαγή πληροφοριών μεταξύ των ομάδων δεν χρειάζεται να περιλαμβάνει τον επίγειο σταθμό ή να δρομολογείται μέσω αυτού. Ο επίγειος σταθμός επεξεργάζεται μόνο τις πληροφορίες που προορίζονται για τον ίδιο. Το αποτέλεσμα είναι η μείωση του φόρτου επικοινωνίας και του υπολογισμού στον επίγειο σταθμό. Αυτή η αρχιτεκτονική επικοινωνίας είναι η πλέον αρμόδια για λειτουργίες ΜΕΑ ένα-προς-πολλά. Επιπλέον, αυτή η αρχιτεκτονική επικοινωνίας είναι εύρωστη, διότι δεν έχει ένα μοναδικό σημείο αποτυχίας.

Τα ΜΕΑ συνδέονται μεταξύ τους μέσω πολλαπλών συνδέσμων. Συνοπτικά, μία αποκεντρωμένη αρχιτεκτονική επικοινωνίας είναι καταλληλότερη αρχιτεκτονική για τη σύνδεση μίας ομάδας ΜΕΑ [35], ενώ ένα πολυεπίπεδο δίκτυο Ad-Hoc ΜΕΑ αρμόζει καλύτερα για χρήση σε FANET.



Εικόνα 6 Δίκτυα Ad-Hoc ΜΕΑ Πολλαπλών Επιπέδων

3.3 Πρωτόκολλα Δρομολόγησης

Η δυναμική φύση των ΜΕΑ εντός των FANET προκαλεί απότομες αλλαγές στην τοπολογία του δικτύου και, ως εκ τούτου, καθιστά τη δρομολόγηση μεταξύ των ΜΕΑ ένα ιδιαίτερα κρίσιμο έργο [36]. Λαμβάνοντας υπόψη την επικοινωνία μεταξύ των ΜΕΑ, τα πρωτόκολλα δρομολόγησης διαδραματίζουν ζωτικό ρόλο στην αξιόπιστη μεταφορά δεδομένων από άκρο σε άκρο. Επιπλέον, θα πρέπει να εξετάζεται η ελαχιστοποίηση του φορτίου που εισάγει το ίδιο το πρωτόκολλο δρομολόγησης. Μέχρι στιγμής δεν υπάρχει ένα πρωτόκολλο δρομολόγησης κατάλληλο για όλα τα σενάρια και τις συνθήκες. Στις αρχικές μελέτες και πειράματα των FANET, προτιμώνται και διερευνώνται τα υφιστάμενα πρωτόκολλα δρομολόγησης MANET και VANET.

Εντούτοις, λόγω των ειδικών χαρακτηριστικών των ΜΕΑ, όπως οι γρήγορες εναλλαγές στην ποιότητα των συνδέσεων και η γρήγορη μετακίνηση στο τρισδιάστατο χώρο, η δρομολόγηση δικτύων γίνεται μία κρίσιμη διεργασία και τα περισσότερα πρωτόκολλα δρομολόγησης MANET και VANET δεν καλύπτουν τα δίκτυα FANET. Ως εκ τούτου, για να αποκτήσει αυτή η νέα ad-hoc οικογένεια δικτύωσης κάποια προηγούμενα πρωτόκολλα ad-hoc δικτύωσης έχουν τροποποιηθεί και κάποια νέα έχουν προταθεί για την δρομολόγησης σε FANET.

Αυτά τα πρωτόκολλα δρομολόγησης ταξινομούνται στις ακόλουθες έξι κύριες κατηγορίες :

i. Στατικά Πρωτόκολλα Δρομολόγησης
ii. Πρωτόκολλα Προληπτικής Δρομολόγησης
iii. Πρωτόκολλα Αντιδραστικής δρομολόγησης
iv. Πρωτόκολλα Υβριδικής Δρομολόγησης

v. Πρωτόκολλα Δρομολόγησης με βάση την Γεωγραφική Θέση
vi. Ιεραρχικά Πρωτόκολλα Δρομολόγησης

3.3.1 Στατικά Πρωτόκολλα Δρομολόγησης

Στα πρωτόκολλα στατικής δρομολόγησης, κάθε ΜΕΑ διαθέτει έναν πίνακα δρομολόγησης που δεν ενημερώνεται κατά τη διάρκεια της αποστολής. Τα πρωτόκολλα στατικής δρομολόγησης ισχύουν σε περιπτώσεις όπου η τοπολογία του δικτύου δεν αλλάζει και όπου οι δυνατότητες στην επιλογή διαδρομής είναι περιορισμένες. Σε αυτή την περίπτωση, κάθε ΜΕΑ επικοινωνεί με άλλα ΜΕΑ ή το σταθμό εδάφους και αποθηκεύει μόνο τις πληροφορίες τους. Αυτό οδηγεί στη μείωση του αριθμού των συνδέσεων επικοινωνίας. Ωστόσο, σε περίπτωση αποτυχίας ενημέρωσης του πίνακα δρομολόγησης, είναι υποχρεωτική η διατήρηση, μέχρι να ολοκληρωθεί η αποστολή. Το αποτέλεσμα, είναι ότι αυτά τα πρωτόκολλα δεν έχουν καμία ανοχή σε περίπτωση σφάλματος.

3.3.1.1 Φορτίο Μεταφορά και Παράδοση Δρομολόγησης – Load Carry and Deliver Routing (LCAD)

Στο μοντέλο Φορτίου Μεταφοράς και Παράδοσης Δρομολόγησης (ΦΜΠΔ) [68, 69], ένα ΜΕΑ επιφορτίζεται με την εργασία να αποθηκεύσει τα δεδομένα των άλλων ΜΕΑ και να τα μεταφέρει στον επίγειο σταθμό, όπως φαίνεται στην εικόνα 7.

Αρχικά το ΦΔΠΜ, εξετάστηκε ως σενάριο με μία πηγή και ένα προορισμό. Αυτό εύκολα προσαρμόστηκε σε σενάριο με πολλές πηγές προς πολλούς προορισμούς. Αυτός ο μηχανισμός δρομολόγησης είναι εφικτός για εφαρμογές με απαιτήσεις μεταφοράς μεγάλου όγκου δεδομένων αλλά με ανοχή σε καθυστέρηση [37]. Οι κύριοι στόχοι της δρομολόγησης ΦΔΠΜ είναι να μεγιστοποιηθεί η απόδοση μεταφοράς και η αύξηση της ασφάλειας. Ωστόσο, το κύριο μειονέκτημα αυτού του πρωτοκόλλου είναι, ότι όσο αυξάνεται η απόσταση μεταξύ των ΜΕΑ, η καθυστέρηση μετάδοσης γίνεται εξαιρετικά μεγάλη και μη ανεκτή.

Για την μείωση της καθυστέρηση μετάδοσης, μπορούν να χρησιμοποιηθούν πολλά ΜΕΑ στην ίδια διαδρομή. Έτσι, η απόσταση μεταξύ των ΜΕΑ μπορεί να είναι η ελάχιστη δυνατή και ταυτόχρονα να αυξηθεί η ταχύτητα των ΜΕΑ. Επίσης, σε ένα δίκτυο ΦΔΠΜ μπορεί να χωριστεί σε μικρότερα υπο-δίκτυα.

Εικόνα 7 ΜΕΑ σε μοντέλο Φορτίου Μεταφοράς και Παράδοσης Δρομολόγησης

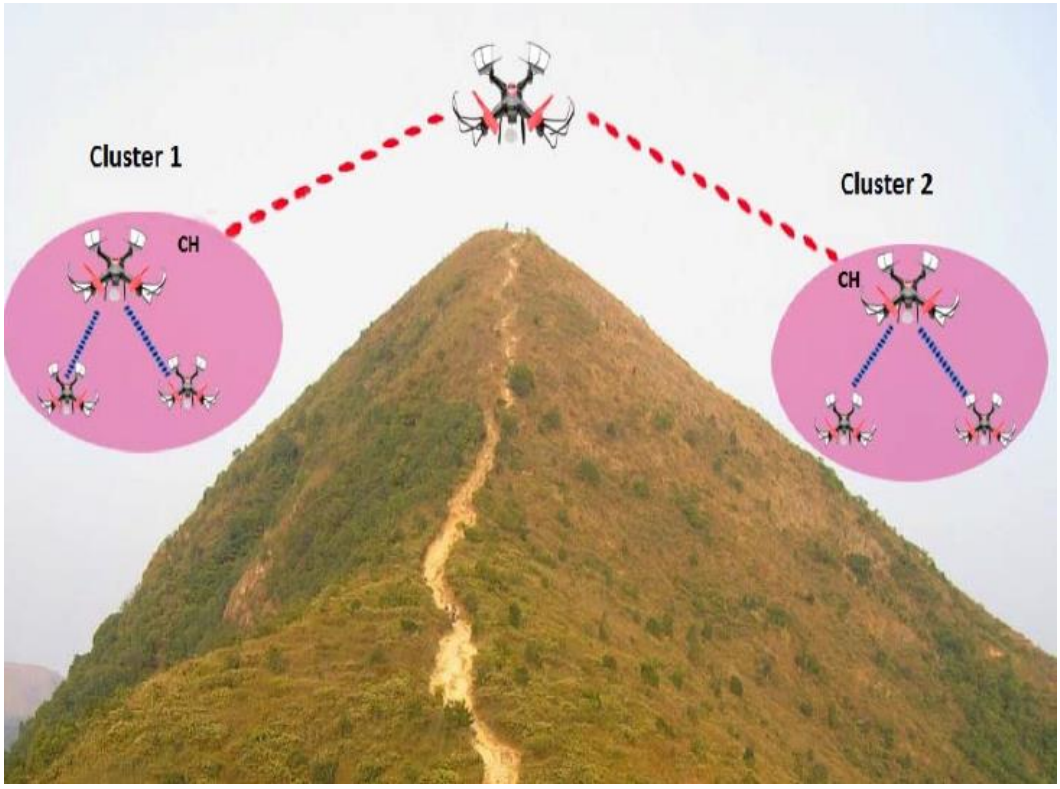
3.3.1.2 Ιεραρχική δρομολόγηση Πολλαπλών Επιπέδων

Μία διαφορετική λύση για πρωτόκολλο δρομολόγησης σε FANET με στατική δρομολόγηση είναι τα Ιεραρχικά Πρωτόκολλα Πολλαπλών Επιπέδων (ΙΠΠΕ) **[37α]**. Το πρωτόκολλο δρομολόγησης ΙΠΠΕ έχει σχεδιαστεί για την αντιμετώπιση του ζητήματος της επεκτασιμότητας του δικτύου. Εδώ, τα δίκτυα ομαδοποιούνται σε μία σειρά από συστάδες που ορίζονται σε διαφορετικές περιοχές λειτουργίας, όπως φαίνεται στην εικόνα 8. Κάθε συστάδα διαθέτει έναν επικεφαλή συστάδας (ΕΣ), ο οποίος έχει τις συνδέσεις εκτός της συστάδας. Επίσης είναι δυνατό να αντιστοιχηθούν διαφορετικές εργασίες σε κάθε συστάδα στο δίκτυο ΙΠΠΕ. Όλα τα ΜΕΑ σε ένα σύμπλεγμα βρίσκονται εντός της εμβέλειας επικοινωνίας του ΕΣ. Ο ΕΣ συνδέεται άμεσα ή έμμεσα με τα ΜΕΑ ή τους δορυφόρους του ανώτερου επιπέδου. Το ΙΠΠΕ παρουσιάζει καλύτερη απόδοση, αν τα ΜΕΑ είναι τοποθετημένα σε συστάδες σε μία μεγάλη γεωγραφική περιοχή και με μεγάλο αριθμό ΜΕΑ. Ωστόσο, το πιο κρίσιμο ζήτημα της σχεδίασης για τη δρομολόγηση ΙΠΠΕ είναι οι πληροφορίες της κάθε συστάδας.

Η υψηλή κινητικότητα των ΜΕΑ απαιτεί συχνή ανταλλαγή πληροφοριών εντός της συστάδας. Το ζήτημα επιλύεται με την χρήση του αλγόριθμου, Πρόβλεψη δομής λεξικού Προσπαθειών (Dictionary Trie Structure Prediction [38]), για την πρόβλεψη των πληροφοριών της τοπολογίας του δικτύου. Στο μοντέλο αυτό, το υψηλότερο σταθμισμένο ΜΕΑ μεταξύ των γειτόνων του, επιλέγεται ως ο ΕΣ. Τα κριτήρια επιλογής ΕΣ ενισχύουν τη σταθερότητα της συστάδας και του ίδιου του ΕΣ. Ο αλγόριθμος της συστάδας για το δίκτυο ΜΕΑ ορίζει πρώτα τις συστάδες στο έδαφος και τις κρατάει ενημερωμένες κατά τη διάρκεια της λειτουργίας. Η συστάδα εδάφους καθορίζει το σχέδιο των συστάδων και στη συνέχεια, επιλέγει τις ΕΣ με βάση τις γεωγραφικές πληροφορίες.

Επιπλέον, αμέσως μετά την ανάπτυξη των ΜΕΑ, η δομή των συστάδων ρυθμίζεται σύμφωνα με την αποστολή.

Αυτό το μοντέλο δρομολόγησης, μπορεί να ενισχύσει σημαντικά τη σταθερότητα και να εξασφαλίσει την δυναμικότητα του δικτύου.



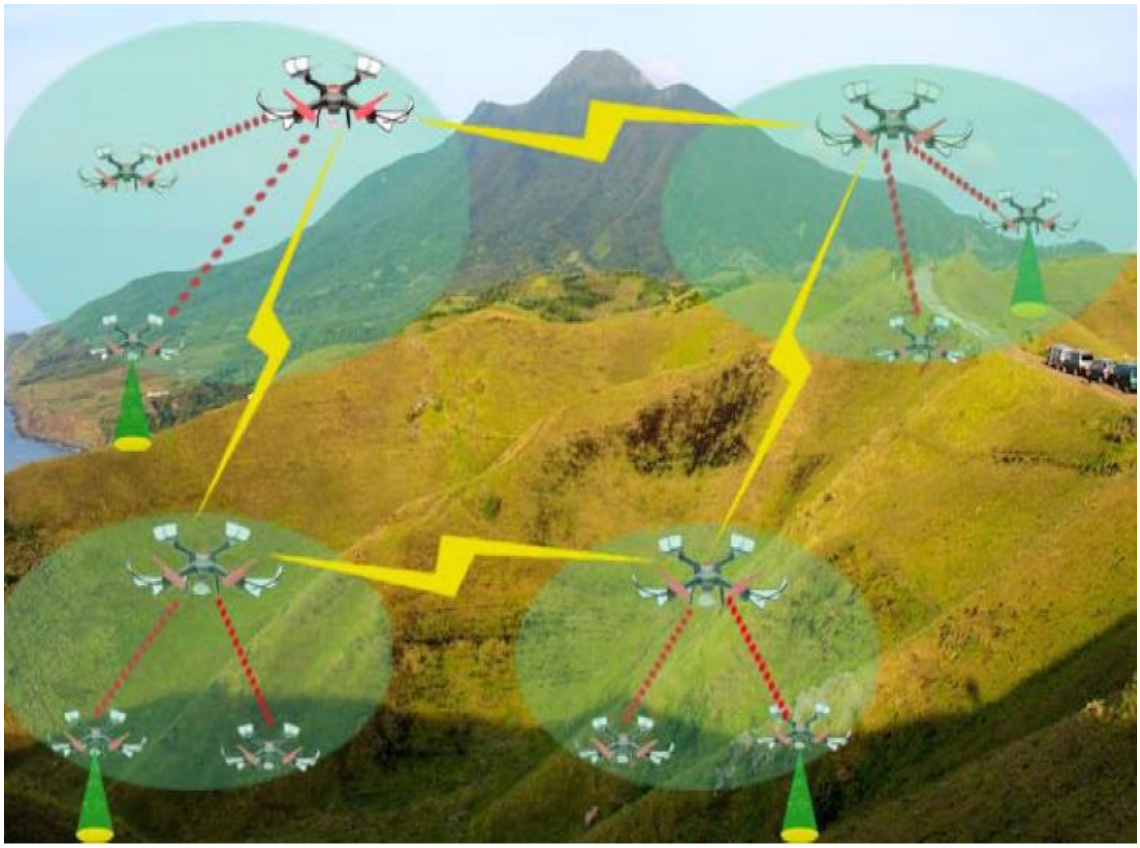
Εικόνα 8 ΜΕΑ σε μοντέλο Ιεραρχικής Δρομολόγησης Πολλαπλών Επιπέδων

3.3.1.3 Δρομολόγηση με Επίκεντρο τα Δεδομένα

Η εφαρμογή αλγόριθμου δρομολόγησης με επίκεντρο τα δεδομένα (ΔΕΔ) σε FANET χρησιμοποιείται, όταν τα δεδομένα που ζητούνται και συλλέγονται, επιλέγονται σύμφωνα με τα χαρακτηριστικά των δεδομένων αντί των αναγνωριστικών αποστολέα ή παραλήπτη, όπως φαίνεται στην εικόνα 9. Προφανώς, λόγω της ασύρματης φύσης του μοντέλου επικοινωνίας των ΜΕΑ, το Multicasting μπορεί να προτιμηθεί αντί του Unicasting. Αυτός ο αλγόριθμος δρομολόγησης επιλέγεται, όταν τα δεδομένα προέρχονται από πολλά ΜΕΑ, αλλά η διανομή των δεδομένων γίνεται ύστερα από αίτημα. Η ΔΕΔ μπορεί να χρησιμοποιηθεί σε FANET για την παροχή πολυάριθμων εφαρμογών σε ένα ομοιογενές σύστημα πολλαπλών ΜΕΑ, προκειμένου να συγκεντρωθούν συγκεκριμένα δεδομένα από μία περιοχή αποστολής. Το μοντέλο δημοσίευσης-εγγραφής ισχύει συνήθως για αυτό το είδος της αρχιτεκτονικής [74, 75]. Συνδέεται αυτόματα με τους παραγωγούς των δεδομένων, οι οποίοι ονομάζονται εκδότες, και με καταναλωτές δεδομένων, που ονομάζονται συνδρομητές. Ο κόμβος παραγωγού καθορίζει ποιες πληροφορίες πρέπει να δημοσιεύονται και στη συνέχεια αρχίζει τη διάδοση δεδομένων.

Αφού τα δημοσιευμένα δεδομένα φτάσουν σε ένα ΜΕΑ στο δίκτυο, τότε προσπαθεί να βρει τα αιτήματα συνδρομής και στη συνέχεια προωθεί αυτά τα δεδομένα προς το κατάλληλο ΜΕΑ. Το κύριο όφελος αυτού του αλγορίθμου δρομολόγησης είναι ότι μπορεί να διαδίδει μόνο τα δεδομένα που αιτούνται οι συνδρομητές. Οι αλγόριθμοι ΔΕΔ αποσυνδέονται σε τρεις διαστάσεις :

- Αποσύνδεση στο χώρο : Η επικοινωνία των ΜΕΑ μπορεί να είναι προς οπουδήποτε, χωρίς η γνώση της ταυτότητας ή της θέσης του ανταποκριτή να είναι υποχρεωτική.
- Αποσύνδεση στο χρόνο : Η επικοινωνία των ΜΕΑ δεν απαιτείται να είναι ταυτόχρονη και τα δεδομένα μπορούν να προωθηθούν στους συνδρομητές άμεσα ή αργότερα.
- •Αποσύνδεση της ροής : Η παράδοση δεδομένων μπορεί να επιτευχθεί αξιόπιστα με ασύγχρονη δομή επικοινωνίας. Αυτό το μοντέλο δρομολόγησης προτιμάται σε μικρό αριθμό ΜΕΑ και όταν δύναται να επανακαθοριστεί το σχέδιο πτήσης με ελάχιστη βοήθεια μεταξύ των συστάδων



Εικόνα 9 ΜΕΑ σε μοντέλο Δρομολόγησης με Επίκεντρο τα Δεδομένα

3.3.2 Πρωτόκολλα Προληπτικής Δρομολόγησης

Στα πρωτόκολλα προληπτικής δρομολόγησης (ΠΠΔ), κάθε κόμβος διατηρεί περιοδικά έναν ή περισσότερους πίνακες που αποτυπώνουν την πλήρη τοπολογία του δικτύου. Λόγω της προληπτικής φύσης, αυτό το πρωτόκολλο δρομολόγησης έχει το πλεονέκτημα της άμεσης πρόσβασης σε διαδρομές, όταν αυτές καλούνται απαραίτητες.

Ωστόσο, υφίσταται πρόσθετο κόστος, λόγω της διατήρησης ενημερωμένων πληροφοριών. Κατά συνέπεια, η διακίνηση του δικτύου μπορεί να επηρεαστεί, δεδομένου ότι τα μηνύματα ελέγχου αποστέλλονται ακόμη και όταν δεν υπάρχει κυκλοφορία δεδομένων. Για το λόγο αυτό, τα ΠΠΔ δεν ενδεικνύονταν για φορητά και μεγάλα δίκτυα ΜΕΑ. Επιπλέον, στην περίπτωση που παρουσιάζεται, είτε αλλαγή τοπολογίας, είτε αποτυχία σύνδεσης, αυτά τα πρωτόκολλα δρομολόγησης προσαρμόζονται αργά. Υπάρχουν διάφορα πρωτόκολλα δρομολόγησης που εμπίπτουν σε αυτή την κατηγορία [39].

3.3.2.1 Πρωτόκολλο Προορισμού Ακολουθίας Διανύσματος Αποστάσεων

Τα πρωτόκολλα προορισμού ακολουθίας διανύσματος αποστάσεων (ΠΠΑΔΑ) βασίζονται στον αλγόριθμο Bellman-Ford με μία μικρή απαραίτητη τροποποίηση, καθιστώντας τον, πιο κατάλληλο για Ad-Hoc δίκτυα ΜΕΑ. Εδώ κάθε ΜΕΑ έχει πλήρη εικόνα για τα άλλα ΜΕΑ που είναι συνδεδεμένα στο δίκτυο. Ο πίνακας δρομολόγησης εδώ, ενημερώνεται περιοδικά για ολόκληρο το δίκτυο με αριθμό ακολουθίας για να αποφεύγονται βρόχοι δρομολόγησης [40]. Η διαδρομή που χρησιμοποιήθηκε πρόσφατα με τον υψηλότερο αριθμό ακολουθίας προτιμάται από μία διαδρομή με το χαμηλότερο αριθμό ακολουθίας.

Τα κύρια οφέλη του ΠΠΑΔΑ είναι τόσο η απλότητα, όσο και η χρήση των αριθμών ακολουθίας, η οποία υπόσχεται τη μετάδοση δεδομένων χωρίς βρόχο [41]. Ωστόσο, το κύριο μειονέκτημα αυτού του αλγορίθμου δρομολόγησης είναι η περιοδική ενημέρωση του ενημερωμένου πίνακα δρομολόγησης, η οποία προσθέτει φόρτο στο δίκτυο. Αυτό το πρωτόκολλο δεν είναι κατάλληλο για δίκτυα ,όπου η τοπολογία αλλάζει συχνά. Επίσης, υποστηρίζει δρομολόγηση μόνο μίας διαδρομής και όχι δρομολόγηση πολλαπλών διαδρομών.

3.3.2.2 Πρωτόκολλο Βελτιστοποιημένης Δρομολόγησης Κατάστασης Σύνδεσης

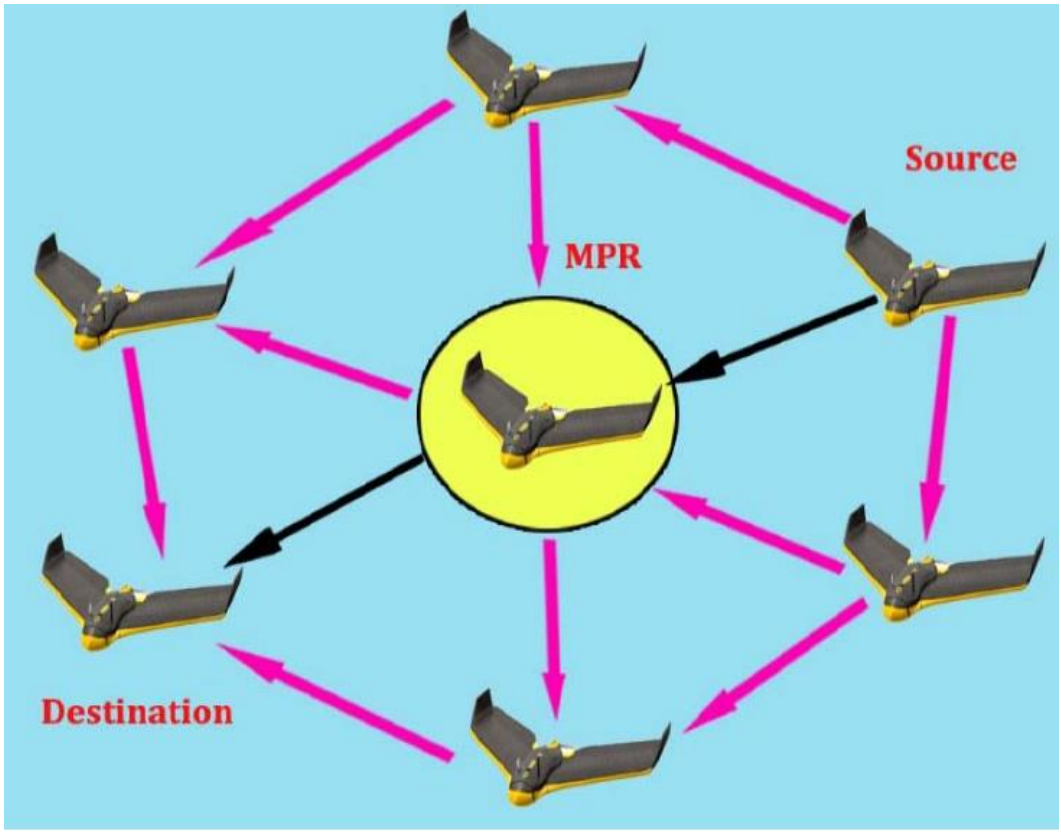
Τα πρωτόκολλα βελτιστοποιημένης δρομολόγησης κατάστασης σύνδεσης (ΠΒΔΚΣ) αποθηκεύουν συνεχώς και ενημερώνουν τους πίνακές τους . Ως εκ τούτου, κάθε φορά που απαιτείται μία διαδρομή, το πρωτόκολλο καθορίζει τη βέλτιστη διαδρομή προς όλους τους πιθανούς προορισμούς χωρίς καμία καθυστέρηση [42]. Με στόχο την εγκαθίδρυση της επικοινωνίας μεταξύ των ΜΕΑ στο δίκτυο, εκτελείται μία διεργασία του πρωτοκόλλου που χρησιμοποιείται ένα μοναδικό πακέτο, το οποίο περιέχει πολλά μηνύματα. Τα πακέτα των πρωτοκόλλων ΠΒΔΚΣ μπορούν να μεταφέρουν τρεις διαφορετικούς τύπους μηνυμάτων. Το καθένα εξυπηρετεί ένα συγκεκριμένο σκοπό:

1) Μήνυμα HELLO, το οποίο μεταδίδεται περιοδικά για να ελέγξει την συνδεσιμότητα με τους γείτονες, την ανακάλυψη συνδέσεων και την σηματοδοσία Αναμετάδοσης Πολλαπλών Σημείων (ΑΠΣ)
2) Μήνυμα Ελέγχου της Τοπολογίας (ΕΤ), το οποίο διαφημίζει τις πληροφορίες των καταστάσεων συνδέσεων
3) Μήνυμα Δήλωσης Πολλαπλών Διεπαφών (ΔΠΔ), το οποίο διαφημίζει τις συνδέσεις του κάθε κόμβου [43]

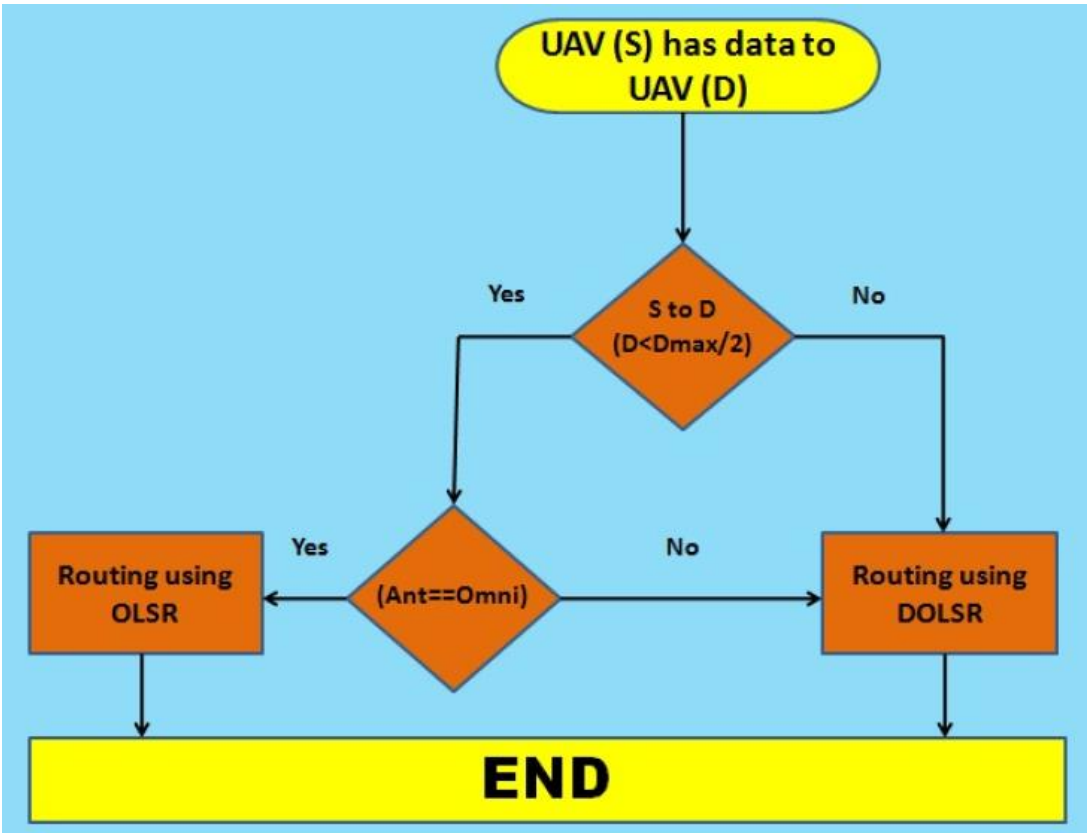
Η συμπεριφορά του πρωτοκόλλου με την περιοδική πλημμύρα πακέτων έχει σαν αποτέλεσμα την προσθήκη μεγάλου φόρτου στο δίκτυο. Με τη χρήση του μηχανισμού ΑΠΣ στα πρωτόκολλα ΠΒΔΚΣ, το πρόσθετο φορτίο και η καθυστέρηση μειώνεται σημαντικά, επειδή το ΜΕΑ που λειτουργεί ως ΑΠΣ μπορεί να προωθήσει τα μηνύματα μόνο κατά την πλημμύρα. Το ΜΕΑ αποστολέας καθορίζει ένα σύνολο από ΜΕΑ ΑΠΣ, έτσι ώστε αυτά να μπορούν να φτάσουν σε απόσταση δύο γειτόνων. Ένα ΜΕΑ που επιλέγει ένα άλλο ΜΕΑ ως ΜΕΑ ΑΠΣ ονομάζεται εκλογέας ΑΠΣ αυτού του κόμβου.

Η εικόνα 10 εμφανίζει την ΑΠΣ που έχει επιλεγεί από το ΜΕΑ εκλογέας. Η πιο σημαντική παράμετρος σχεδιασμού για τα ΠΒΔΚΣ είναι ο αριθμός των ΑΠΣ, ο οποίος επηρεάζει έντονα την καθυστέρηση. Καθώς ο αριθμός των ΑΠΣ μειώνεται, τόσο μειώνεται και το επιπρόσθετο κόστος. Με αυτόν τον τρόπο, προτείνεται μία νέα μέθοδος για τη μείωση του αριθμού των ΑΠΣ ΜΕΑ. Η

εικόνα 11 εμφανίζει ένα διάγραμμα για το προτεινόμενο ΠΒΔΚΣ, στο οποίο συνυπολογίζεται η απόσταση. Για κάθε αποστολή πακέτων δεδομένων, το ΜΕΑ αποστολέας υπολογίζει την απόσταση από το ΜΕΑ δέκτη. Το παραπάνω μπορεί να ολοκληρωθεί εφόσον η απόσταση είναι μεγαλύτερη από τη μέγιστη απόσταση που μπορεί να επιτευχθεί με τη χρήση κατευθυντικής κεραίας (Dmax/2), ή με πανκατευθυντική κεραία. Όπου δεν μπορεί να φτάσει το προορισμό, το ΜΕΑ θα εφαρμόσει τον προτεινόμενο αλγόριθμο. Διαφορετικά, θα χρησιμοποιήσει τον αλγόριθμο ΠΒΔΚΣ [44].



Εικόνα 10 Αναμετάδοση Πολλαπλών Σημείων (ΑΠΣ) που έχει επιλεγεί από ΜΕΑ εκλογέα



Εικόνα 11 Διάγραμμα Προτεινόμενου ΠΒΔΚΣ

3.3.3 Πρωτόκολλα Αντιδραστικής Δρομολόγησης

Τα πρωτόκολλα αντιδραστικής δρομολόγησης (ΠΑΔ) είναι επίσης γνωστά ως πρωτόκολλα δρομολόγησης κατ' απαίτηση, διότι ανακαλύπτουν και διατηρούν μία διαδρομή μόνο αν υπάρχει απαίτηση για αυτή. Ο πίνακας δρομολόγησης ενημερώνεται περιοδικά, μόνο όταν υπάρχουν δεδομένα για αποστολή. Εάν δεν υπάρχει η ανάγκη για σύνδεση μεταξύ δύο κόμβων, δεν χρειάζεται να υπολογιστεί και η διαδρομή μεταξύ τους. Κατά συνέπεια, αυτά τα πρωτόκολλα δρομολόγησης διατηρούν μόνο τις διαδρομές που χρησιμοποιούνται κάθε δεδομένη στιγμή **[44α]**. Με αυτή την μέθοδο αποβάλλει το πρόσθετο φόρτο που εισάγουν τα ΠΠΔ. Σε αυτό το μοντέλο δρομολόγησης, χρησιμοποιούνται δύο τύποι μηνυμάτων :

1) Μηνύματα Αίτησης Διαδρομής
2) Μήνυμα Απάντησης Διαδρομής [41].

Τα μηνύματα Αίτησης Διαδρομής μεταδίδονται από το ΜΕΑ πηγής σε όλα τα γειτονικά του ΜΕΑ, με τον μηχανισμό της πλημμύρας, για να ανακαλύψει τη δρομολόγηση. Κάθε ΜΕΑ επανεκπέμπει το αρχικό μήνυμα μέχρι αυτό να φτάσει στο ΜΕΑ προορισμού. Αντίθετα, το μήνυμα Απάντησης της Διαδρομής εκπέμπεται από το ΜΕΑ προορισμού και φτάνει στο ΜΕΑ πηγής από μία μοναδική διαδρομή. Σε αυτήν την προσέγγιση δρομολόγησης, δεν είναι απαραίτητο οι πίνακες δρομολόγησης να ανανεώνονται συνεχώς. Τα πρωτόκολλα αντιδραστικής δρομολόγησης είναι αποδοτικά ως προς το εύρος ζώνης του δικτύου, επειδή δεν υπάρχουν περιοδικές ενημερώσεις. Το κύριο μειονέκτημα των ΠΑΔ είναι ότι η εύρεση της διαδρομής είναι αργή. Το αποτέλεσμα είναι ότι εισάγεται καθυστέρηση στο δίκτυο.

3.3.3.1 Δυναμική Δρομολόγηση Πηγής Πρωτόκολλα – Dynamic Source Routing (DSR)

Τα πρωτόκολλα Δυναμικής Δρομολόγησης Πηγής (ΠΔΔΠ) επιτρέπουν σε ένα δίκτυο να αυτορυθμίζεται και να αυτό-οργανώνεται χωρίς την απαίτηση υποδομής. Ο κύριος λόγος της επιλογής ενός ΠΔΔΠ είναι η αντιδραστική φύση του. Χρησιμοποιείται κυρίως στα ασύρματα δίκτυα πλέγματος με πολλαπλά άλματα. Στο ΠΔΔΠ, η πηγή προσπαθεί να βρει μία διαδρομή προς έναν προορισμό κάθε φορά που έχει δεδομένα για αποστολή. Το ΠΔΔΠ είναι καταλληλότερο από τις προληπτικές μεθόδους για FANET, όπου η κινητικότητα των ΜΕΑ είναι υψηλή και η τοπολογία δεν είναι σταθερή. Η ενημέρωση ενός πίνακα δρομολόγησης με προληπτικές μεθόδους δεν είναι αποδοτική, λόγω της υψηλής κινητικότητας των ΜΕΑ. Η επαναλαμβανόμενη εύρεση διαδρομής με αντιδραστική μέθοδο, πριν από κάθε παράδοση πακέτου, μπορεί επίσης να είναι εξαντλητική.

3.3.3.2 Ad Hoc Κατ' Απαίτηση Απόσταση Διανύσματος Πρωτόκολλο

Το πρωτόκολλο Ad-Hoc Κατ' Απαίτηση Απόσταση Διανύσματος (ΑΚΑΑΔ) είναι η βελτιωμένη έκδοση των πρωτοκόλλων δρομολόγησης ΠΠΑΔΑ και ΠΔΔΠ. Χρησιμοποιεί τις περιοδικές ενημερώσεις από το ΠΠΑΔΑ και την δρομολόγηση με μεταπήδηση από το ΠΔΔΠ. Η αντιδραστική συμπεριφορά που προκύπτει από το ΠΠΑΔΑ ανακαλύπτει μία διαδρομή, μόνο όταν απαιτείται, και δεν την διατηρεί, αφού εκπληρωθεί αυτή η απαίτηση . Το πρωτόκολλο δρομολόγησης ΑΚΑΑΔ χωρίζεται σε τρεις φάσεις :

(i) εντοπισμό διαδρομής,
(ii) μετάδοσης πακέτων,
(iii) διατήρηση διαδρομής.

Κάθε φορά που ένα ΜΕΑ καλείται να αποστείλει ένα πακέτο, ξεκινά πρώτα μία λειτουργία ανακάλυψη διαδρομής προς το ΜΕΑ προορισμού και στη συνέχεια προωθεί το πακέτο μέσω της διαδρομής. Αποφεύγοντας έτσι βρόχους, κατά τη φάση μετάδοσης των πακέτων. Μία φάση συντήρησης διαδρομής πραγματοποιείται μόνο για να αποκαταστήσει μία αποτυχία σύνδεσης. Αυτό το πρωτόκολλο δρομολόγησης χρησιμοποιεί έναν αριθμό ακολουθίας για να βρει μία νέα βέλτιστη διαδρομή προς τον προορισμό. Χρησιμοποιείται ένας χρόνος λήξης προκειμένου να επιβεβαιωθεί η εγκυρότητα της διαδρομής. Σε αυτήν τη μέθοδο, τα ενδιάμεσα ΜΕΑ ενημερώνουν επίσης τους πίνακες δρομολόγησης τους. Ωστόσο, η συμφόρηση του δικτύου είναι ένα ζήτημα με τα πρωτόκολλα ΑΚΑΑΔ, λόγω της δυναμικής φύσης των συστημάτων FANET.

3.3.3.3 Κατ' Απαίτηση Δρομολόγηση Χρονοθυρίδας

Το πρωτόκολλο κατ' απαίτησης δρομολόγηση χρονοθυρίδας (ΚΑΔΘ) χρησιμοποιεί τον αλγόριθμο δρομολόγησης των πρωτοκόλλων ΑΚΚΑΔ, προσθέτοντας χρονοθυρίδες στην επικοινωνία [44]. Το ΑΚΚΑΔ στέλνει τα πακέτα ελέγχου με την μέθοδο της τυχαίας πρόσβασης, ενώ στην περίπτωση της χρονοθυρίδας, κατ' απαίτηση η μέθοδος που εκτελείται χρησιμοποιεί αφιερωμένες χρονοθυρίδες. Στο διάστημα της κάθε χρονοθυρίδας, μπορεί να στείλει μόνο ένα ΜΕΑ δεδομένα. Αυτή η μέθοδος δρομολόγησης, όχι μόνο αυξάνει την αποδοτικότητα της χρήσης του εύρους ζώνης, αλλά αποφεύγει τις συγκρούσεις πακέτων και αυξάνει την αναλογία παράδοσης πακέτων.

3.3.4 Πρωτόκολλα Υβριδικής Δρομολόγησης

Τα πρωτόκολλα υβριδικής δρομολόγησης (ΠΥΔ) είναι ένας συνδυασμός τόσο προληπτικών, όσο και αντιδραστικών πρωτοκόλλων δρομολόγησης. Εφαρμόζονται οι καλύτερες δυνατότητες τους για να ξεπεραστούν οι περιορισμοί που προκύπτουν από τα δυο αυτά πρωτόκολλα. Τα πρωτόκολλα αντιδραστικής δρομολόγησης, γενικά απαιτούν σημαντικό χρόνο για να ανακαλύψουν τη διαδρομή και τα πρωτόκολλα προληπτικής δρομολόγησης έχουν υπερμεγέθη μηνύματα ελέγχου. Τα μειονεκτήματα τους μπορούν να μετριαστούν με τη χρήση ΠΥΔ. Τα υβριδικά πρωτόκολλα είναι κατάλληλα για μεγάλα δίκτυα και βασίζονται στην έννοια των «ζωνών». Η προληπτική δρομολόγηση εκτελείται μεταξύ των ζωνών και η αντιδραστική δρομολόγηση εκτελείται εσωτερικά στην κάθε ζώνη.

3.3.4.1 Πρωτόκολλο Δρομολόγησης Ζώνης

Αυτός ο αλγόριθμος δρομολόγησης βασίζεται στην έννοια των «ζωνών» [45] και είναι κατάλληλος για δίκτυα μεγάλου μεγέθους και με διαφορετικά μοτίβα κινητικότητας. Σε αυτήν την προσέγγιση δρομολόγησης, κάθε ΜΕΑ έχει την προσωπική ζώνη, στην οποία συμπεριλαμβάνονται και τα γειτονικά ΜΕΑ. Το μέγεθος της ζώνης καθορίζεται από μία ακτίνα με μήκος "R". Το "R" είναι ο αριθμός των ΜΕΑ στην περίμετρο της ζώνης. Ο αριθμός των ΜΕΑ στη κάθε ζώνη ρυθμίζεται με την ισχύ μετάδοσης του πομπού κάθε ΜΕΑ. Η δρομολόγηση μεταξύ των ΜΕΑ της ίδιας ζώνης ονομάζεται δρομολόγηση εντός ζώνης. Η δρομολόγηση εντός ζώνης χρησιμοποιεί την προσέγγιση της προληπτικής δρομολόγησης για την ανακάλυψη και διατήρηση των διαδρομών. Σε περίπτωση που τα ΜΕΑ πηγής και προορισμού βρίσκονται στην ίδια ζώνη, η επικοινωνία ξεκινάει άμεσα. Η δρομολόγηση μεταξύ ζωνών είναι υπεύθυνη για την αποστολή πακέτων δεδομένων εκτός της ζώνης και χρησιμοποιεί την προσέγγιση αντιδραστικής δρομολόγησης για την ανακάλυψη και τη διατήρηση των βέλτιστων διαδρομών. Η καθυστέρηση που προκαλείται από τον εντοπισμό της διαδρομής, ελαχιστοποιείται με την οριοθέτηση της μετάδοσης πακέτων [46].

Τα μηνύματα απάντησης δημιουργούνται μόνο από τα ΜΕΑ που βρίσκονται στα άκρα μίας ζώνης. Στη συνέχεια, τα ακραία ΜΕΑ επανεκπέμπουν τα πακέτα, επιλέγοντας την κατάλληλη δρομολόγηση, είτε μεταξύ τους, είτε εντός των ζωνών.

3.3.4.2 Προσωρινά Διατεταγμένος Αλγόριθμος Δρομολόγησης

Ο προσωρινά διατεταγμένος αλγόριθμος δρομολόγησης (ΠΔΑΔ) είναι ένα εξαιρετικά προσαρμοζόμενο πρωτόκολλο δρομολόγησης κατ' απαίτηση, κατάλληλο για δίκτυα πολλαπλών αλμάτων. Σε αυτήν την προσέγγιση δρομολόγησης, κάθε ΜΕΑ διαφημίζει μόνο πληροφορίες δρομολόγησης σχετικά με γειτονικά του ΜΕΑ. Τα βασικά χαρακτηριστικά της χρήσης αυτού του αλγορίθμου δρομολόγησης, είναι να περιοριστεί η μετάδοση των μηνυμάτων ελέγχου, προκειμένου να ελαχιστοποιηθούν οι απότομες αντιδράσεις σε αλλαγές της τοπολογίας . Διαγράφει άκυρες και αναζητά νέες διαδρομές σε μία μοναδική εκτέλεση του κατανεμημένου αλγορίθμου.

Συγκεκριμένα, το ΠΔΑΔ χρησιμοποιεί πρωτόκολλα αντιδραστικής δρομολόγησης, αλλά χρησιμοποιεί επίσης και την προληπτική προσέγγιση κατά περίπτωση. Κατασκευάζει και διατηρεί ένα κατευθυνόμενο ακυκλικό γράφημα (ΚΑΓ), από την πηγή, μέχρι τον προορισμό. Στο ΚΑΓ περιέχονται διάφορες διαδρομές μεταξύ των ΜΕΑ. Προτιμάται ο γρήγορος υπολογισμός νέων διαδρομών, σε περίπτωση απώλειας σύνδεσης και για την ενίσχυση της προσαρμοστικότητας . Το

ΠΔΑΔ δεν βασίζεται στον αλγόριθμο συντομότερης διαδρομής, ενώ χρησιμοποιούνται πολλαπλές διαδρομές για την ελαχιστοποίηση του φόρτου.

Κάθε ΜΕΑ στο ΚΑΓ έχει μία τιμή παραμέτρου γνωστή ως "ύψος" και δεν υπάρχουν δύο ΜΕΑ με κοινή τιμή ύψους. Τα δεδομένα ρέουν από τα υψηλότερα ΜΕΑ προς τα χαμηλότερα. Προσφέρει δρομολόγηση χωρίς βρόχο, λόγω της απαγόρευσης ροής δεδομένων προς τα υψηλότερα ΜΕΑ. Στη διαδικασία του εντοπισμού της διαδρομής, η παράμετρος ύψους επιστρέφεται στο ΜΕΑ πηγής και όλα τα ενδιάμεσα ΜΕΑ διατηρούν στους πίνακες δρομολόγησής του, τις εισερχόμενες διαδρομές και τις πληροφορίες ύψους.

3.3.5 Πρωτόκολλα Δρομολόγησης με βάση την Γεωγραφία – Θέση

Έχουν προταθεί πρωτόκολλα Δρομολόγησης Βασισμένα στην Γεωγραφία/Θέση (ΠΔΒΓΘ) για την διάδοση των πληροφοριών γεωγραφικής θέσης των ΜΕΑ για την υποστήριξη μίας αποτελεσματικής δρομολόγησης [47]. Σε αυτόν τον τύπο πρωτοκόλλων, υποθέτουν, ότι το ΜΕΑ προέλευσης γνωρίζει τη φυσική θέση των ΜΕΑ στο δίκτυο και εκπέμπει μηνύματα, αποφεύγοντας την διαδικασία εντοπισμού της διαδρομής. Γενικά, κάθε ΜΕΑ καθορίζει τη θέση του με τη βοήθεια του συστήματος GPS. Αυτός ο αλγόριθμος δρομολόγησης εμπνέεται κυρίως από δύο θέματα :

i) Τη γεωγραφική θέση που χρησιμοποιείται συνήθως από τον αποστολέα ενός πακέτου για τον εντοπισμό της φυσικής θέσης του δέκτη και

ii) Χρησιμοποιείται μία προσέγγιση προώθησης για την μετάδοση πακέτων ΜΕΑ προορισμού.

3.3.5.1 Άπληστη Περιμετρική Χωρίς Κατάσταση Δρομολόγηση

Η Άπληστη Περιμετρική Χωρίς Κατάσταση Δρομολόγηση (ΑΠΧΚΔ) είναι ένα πρωτόκολλο βασισμένο στην θέση που έχει την καλύτερη απόδοση, συγκριτικά με τους προληπτικούς και αντιδραστικούς αλγορίθμους δρομολόγησης. Έχει αποδειχθεί, ότι τα πρωτόκολλα ΑΠΧΚΔ λειτουργούν ιδανικά σε πυκνά δίκτυα ΜΕΑ [48]. Ωστόσο, η αξιοπιστία του δικτύου μπορεί να είναι ένα σοβαρό ζήτημα, σε περίπτωση αραιών αναπτύξεων. Για αυτό το λόγο, θα πρέπει να επικουρείται από συνδυασμό άλλων μηχανισμών για τις εφαρμογές που στοχεύουν στην μέγιστη αξιοπιστία. Για τα FANET, οι υπάρχοντες αλγόριθμοι δρομολόγησης MANET που έχουν δοκιμαστεί, αποτυγχάνουν να ικανοποιήσουν τις απαιτήσεις. Οι βασικοί λόγοι είναι η διακύμανση της ποιότητας των συνδέσεων και η πολύ υψηλή κινητικότητα των ιπτάμενων κόμβων. Για αυτό το λόγο, δεν μπορούν να χρησιμοποιηθούν μαζί με υλοποιήσεις ΑΠΧΚΔ.

3.3.5.2 Δρομολόγηση Προσανατολισμένη στην Κινητικότητα της Γεωγραφικής Θέσης

Η Δρομολόγηση Προσανατολισμένη στην Κινητικότητα της Γεωγραφικής Θέσης (ΔΠΚΓΘ) [48], βασίζεται στις κλασσικές πληροφορίες τοποθεσίας των ΜΕΑ, αλλά λαμβάνει υπόψη και το μοντέλο κινητικότητας "Gaussian-Markov" [49]. Οι συμβατικές λύσεις, βασισμένες στην θέση των ΜΕΑ, εξαρτώνται μόνο από τις πληροφορίες τοποθεσίας των ΜΕΑ. Το ΔΠΚΓΘ χρησιμοποιεί τα δεδομένα του μοντέλου, για να εντοπίσει το επόμενο άλμα. Αυτός ο μηχανισμός δρομολόγησης, μπορεί να παρέχει αποτελεσματική διαβίβαση δεδομένων, αυξάνοντας την σχέση αναλογίας-παράδοσης πακέτων προς την καθυστέρηση.

3.3.6 Ιεραρχικά Πρωτόκολλα Δρομολόγησης

Στα ιεραρχικά πρωτόκολλα δρομολόγησης (ΙΠΔ), η δυνατότητα επιλογής προληπτικής ή αντιδραστικής δρομολόγησης, βασίζεται στα ιεραρχικά επίπεδα του δικτύου, στο οποίο κατατάσσεται το κάθε ΜΕΑ. Αυτή η δρομολόγηση καθορίζεται κυρίως από ορισμένες προληπτικά προγραμματισμένες διαδρομές και στη συνέχεια, υποβοηθά τα αιτήματα από κόμβους με την χρήση ενός αντιδραστικού πρωτοκόλλου με τα χαμηλότερα επίπεδα. Το κύριο μειονέκτημα αυτού του πρωτοκόλλου είναι η πολυπλοκότητα.

3.3.6.1 Αλγόριθμος Συστάδας Πρόβλεψης Κινητικότητας

Ο Αλγόριθμος Συστάδας Πρόβλεψης Κινητικότητας (ΑΣΠΚ) που προτείνεται για τη δικτύωση ΜΕΑ [50], βασίζεται στις ιδιότητες των ΜΕΑ. Στηρίζεται στο λεξικό ενός αλγόριθμου πρόβλεψης με δομή δέντρου και το χρόνο λήξης σύνδεσης για την επίλυση των ζητημάτων που συσχετίζονται με την υψηλή κινητικότητα των ΜΕΑ. Το κύριο πλεονέκτημα αυτού του αλγορίθμου είναι η μείωση της αστάθειας της συστάδας και η βελτίωση της απόδοση δικτύου.

3.3.6.2 Αλγόριθμοι Συστάδας για την Δικτύωση ΜΕΑ

Ο Αλγόριθμος Συστάδας για την Δικτύωση ΜΕΑ σχεδιάστηκε για να αντιμετωπίσει την διαχείριση της επικοινωνίας με ΜΕΑ εκτός εμβέλειας. Στην περίπτωση ενός συστήματος με πολλαπλές απομακρυσμένες συστάδες ΜΕΑ, χρησιμοποιούνται δικτυωμένοι επίγειοι σταθμοί εδάφους για να υλοποιηθεί η επικοινωνία. Με αυτό τον τρόπο, αυξάνεται η σταθερότητα και η ευελιξία των συστάδων .

3.4 Συμπέρασμα Κεφαλαίου

Τα FANET αποτελούν ένα αναδυόμενο ερευνητικό πεδίο. Απαρτίζονται από μία ομάδα μικρών ΜΕΑ, που συνδέονται με Ad-Hoc δικτύωση. Τα δίκτυα αυτά, διακρίνονται από την υψηλή κινητικότητα, τις συχνές αλλαγές τοπολογίας και την κίνηση στο τρισδιάστατο χώρο των κόμβων, τα οποία αποτελούν ζητήματα δικτύωσης.

Προκειμένου να ξεπεραστούν τέτοιου είδους ζητήματα, η επιλογή μίας κατάλληλης αρχιτεκτονικής επικοινωνίας και ενός αξιόπιστου πρωτόκολλου δρομολόγησης είναι απαραίτητη για την εγκαθίδρυση μίας εύρωστης επικοινωνίας μεταξύ των ΜΕΑ. Παραπάνω, αναφέρουμε τρεις διαφορετικές αποκεντρωμένες αρχιτεκτονικές επικοινωνίας από τις οποίες προτείναμε ένα πολυεπίπεδο Ad-Hoc δίκτυο κατάλληλο για FANET. Στη συνέχεια, ερευνήσαμε διάφορα πρωτόκολλα δρομολόγησης, επισημαίνοντας ανοικτά ερευνητικά θέματα. Η απόφαση για την επιλογή της αρχιτεκτονικής επικοινωνίας και του πρωτοκόλλου δρομολόγησης είναι κατά περίπτωση, ανάλογα με την αποστολή του ΜΕΑ.

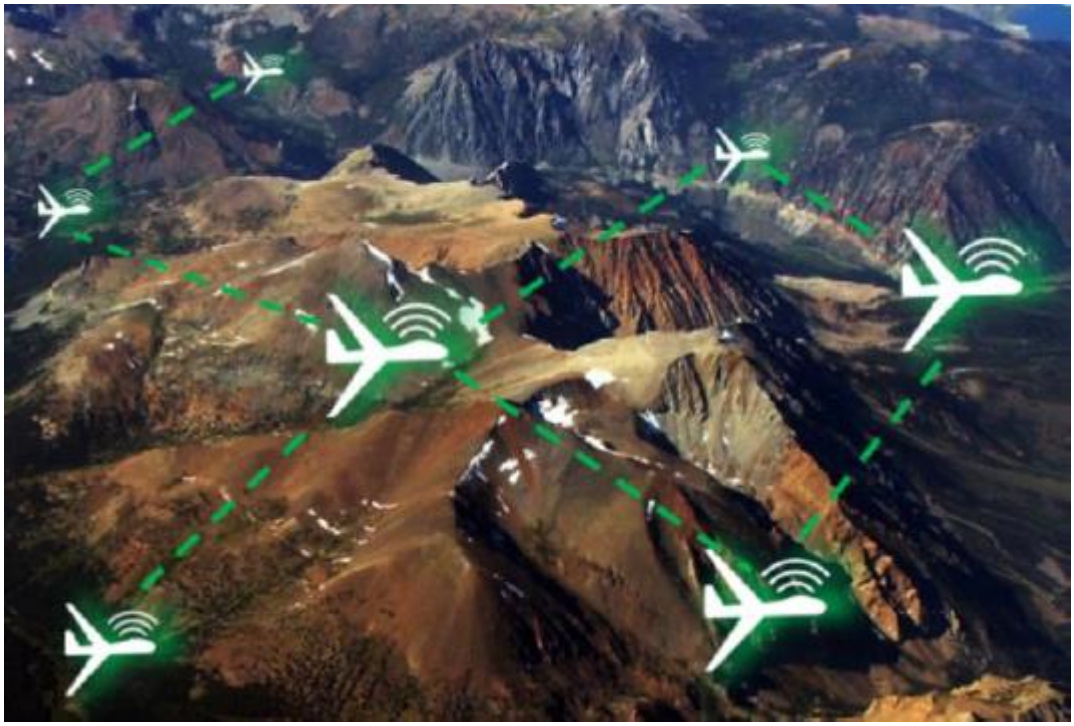
Κεφάλαιο 4

Παρεμβολή στα Πρωτόκολλα Δρομολόγησης Ιπτάμενων Ad-Hoc Δικτύων

4.1 Εισαγωγή

Τα ΜΕΑ γίνονται όλο και πιο δημοφιλή, τόσο στις στρατιωτικές όσο και στις δημόσιες εφαρμογές. Η αναζήτηση και διάσωση, η επιτήρηση των συνόρων, ο εντοπισμός στόχων, η επιτήρηση καταστροφών, η διαχείριση πυρκαγιών, η παρακολούθηση της κυκλοφορίας είναι ορισμένοι τομείς χρήσης των ΜΕΑ [51]. Με τη βοήθεια των τεχνολογικών εξελίξεων στα ηλεκτρονικά και στα πτητικά συστήματα, εξασφαλίζεται η παραγωγή μικρότερων ΜΕΑ. Υπάρχουν πολλά πλεονεκτήματα των μικρότερων συστημάτων ΜΕΑ. Η τιμή αγοράς, καθώς και τα έξοδα συντήρησης και επισκευής μικρών ΜΕΑ είναι μειωμένα. Επιπλέον, κατασκευάζονται και λειτουργούν ευκολότερα . Η διατομή του ραντάρ είναι μικρότερη, και μπορούν να απογειωθούν μέσα σε περιορισμένο χώρο απογείωσης.

Ωστόσο, τα μικρά ΜΕΑ έχουν περιορισμένες δυνατότητες σε σύγκριση με τα μεγαλύτερα ΜΕΑ. Για την επίτευξη των αποστολών με μίνι ΜΕΑ, που προηγουμένως διεξάγονταν από μεγάλα ΜΕΑ, αναπτύχθηκαν συστήματα με πολλαπλά μικρά ΜΕΑ.



Εικόνα 12 Δείγμα Δομής FANET

Ένα από τα πιο βασικά ζητήματα σχεδιασμού των συστημάτων πολλαπλών ΜΕΑ είναι η επικοινωνία. Επίγεια και δορυφορικά συστήματα προσφέρονται έτσι ώστε να παρέχουν επικοινωνία μεταξύ των ΜΕΑ. Ωστόσο, αυτές οι λύσεις έχουν περιορισμούς στην εμβέλεια. Προφανώς, τέτοια

συστήματα απαιτούν υποδομή επικοινωνίας που πρέπει να προετοιμαστεί εκ των προτέρων. Αυτή η βασισμένη στην υποδομή επικοινωνία δεν είναι εύκολη στην εγκατάσταση, ειδικά σε καταστροφές και στρατιωτικές αποστολές. Ένα από τα πιο σημαντικά συστήματα επικοινωνίας πολλαπλών ΜΕΑ είναι τα FANET [52], διότι μπορούν να μεταφέρουν δεδομένα στον σταθμό βάσης, ανεξάρτητα από το εύρος επικοινωνίας και την υποδομή, σε πραγματικό χρόνο. Παρακάτω θα κάνουμε μια ανασκόπηση στα θέματα ασφαλείας των FANET.

Το FANET είναι μια δομή Ad-Hoc δικτύου που σχηματίζεται αποκλειστικά από ΜΕΑ. Ως εκ τούτου, διαφέρει από τα ήδη υπάρχοντα Ad-Hoc δίκτυα, όπως τα MANET και τα VANET, σε ότι αφορά τα θέματα σχεδιασμού και ασφάλειας. Πρώτα απ' όλα, οι κόμβοι FANET έχουν υψηλότερους βαθμούς κινητικότητας και σαν αποτέλεσμα συχνότερες αλλαγές στην τοπολογία των FANET. Επιπλέον, η απόσταση μεταξύ των κόμβων στα FANET είναι μεγαλύτερη σε σύγκριση με τους κόμβους των άλλων τύπων Ad-Hoc δικτύων.

Για τα FANET, η εμβέλεια επικοινωνίας πρέπει να είναι μεγαλύτερη από ό,τι στα MANET και τα VANET, προκειμένου να δημιουργηθούν σύνδεσμοι επικοινωνίας μεταξύ των ΜΕΑ. Επίσης, επειδή οι κόμβοι εντός των FANET είναι μικρότερων διαστάσεων και ο εξοπλισμός που μπορούν να μεταφέρουν είναι περιορισμένος [52]. Οι υφιστάμενες Ad-Hoc μελέτες ασφάλειας είναι αναποτελεσματικές και δεν εφαρμόζονται λόγω της διαφορετικής δομής των FANET. Τα χαρακτηριστικά των FANET, τα οποία αποφεύγουν τα ήδη υπάρχοντα ζητήματα ασφάλειας Ad-Hoc παρέχονται παρακάτω.

Αυτονομία κίνησης κόμβου: Οι κόμβοι των FANET ενδέχεται να εμφανίζουν αυτοματοποιημένες συμπεριφορές για κάποιο συγκεκριμένο γεγονός, συμπεριλαμβανομένης της πορείας δράσης και των εντολών δρομολόγησης. Ως εκ τούτου, μπορεί να μην είναι πάντα σωστό να προβεί κανείς σε υποθετικά σχέδια, σύμφωνα με τις ενέργειες ή τις διαδρομές των κόμβων [52].

Περιορισμός ισχύος: Ειδικά για τα FANET που αποτελούνται από μίνι ΜΕΑ η διαθέσιμη ηλεκτρική ενέργεια είναι πολύ περιορισμένη. Οι επιθέσεις που γίνονται σε τέτοιου είδους ΜΕΑ με περιορισμένη ενέργεια, μπορεί να προκαλέσει την απενεργοποίηση των κόμβων [52].

Μνήμη και Υπολογισμός: Οι δυνατότητες μνήμης και υπολογισμών στους κόμβους των FANET είναι περιορισμένες. Συνεπώς, υπάρχει η πιθανότητα να μην χρησιμοποιηθούν ασφαλείς μέθοδοι κρυπτογράφησης που καταναλώνουν υψηλό επίπεδο μνήμης και υπολογιστικής ικανότητας [52].

Κινητικότητα κόμβων: Οι κόμβοι που σχηματίζουν το FANET, μπορούν να αλλάξουν τις θέσεις τους σε ελάχιστο χρονικό διάστημα συγκριτικά με τα άλλα δίκτυα [52].

Πυκνότητα κόμβου: Οι κόμβοι των FANET μπορεί να βρίσκονται σε μεγάλη απόσταση εν ώρα πτήσης. Έτσι, η πυκνότητα κόμβων στα FANET είναι πολύ χαμηλότερη σε σύγκριση με τα MANET και τα VANET [52].

Εντοπισμός: Είναι δύσκολο να προσδιοριστεί η ακριβής τοποθεσία των κόμβων στα FANET, λόγω του υψηλού βαθμού κινητικότητας τους. Τα δεδομένα εντοπισμού της θέσης πρέπει να ενημερώνονται σε μικρότερα χρονικά διαστήματα [52].

Υπάρχουν αρκετές μελέτες αναφορικά με τα Ad-Hoc δίκτυα στη σχετική βιβλιογραφία [53]. Εντούτοις, οι υπάρχουσες μελέτες και οι αλγόριθμοι ασφαλείας μπορεί να γίνουν αδόκιμες για τα FANET, επειδή διαφέρουν από τα χαρακτηριστικά των MANET και των VANET.

4.2 Γενικά Ζητήματα Ασφαλείας Δικτύων AD-HOC

Ένα Ad-Hoc δίκτυο μπορεί να κριθεί ασφαλές ή όχι, ανάλογα με τα βασικά κριτήρια ασφαλείας που αναφέρονται παρακάτω. Ακόμη και αν το σύστημα πληροί όλα αυτά τα κριτήρια, αυτό δεν σημαίνει απαραίτητα ότι είναι απολύτως ασφαλές. Ωστόσο, εάν το σύστημα δεν πληροί ένα από αυτά τα κριτήρια, τότε κρίνεται ως μη ασφαλές.

Η διαθεσιμότητα ενός κόμβου αναφέρεται στο αν το ΜΕΑ υπάρχει και αν είναι κατάλληλο για χρήση σε οποιαδήποτε χρονική στιγμή και κατάσταση. Όταν ένας κόμβος βρίσκεται υπό επίθεση, ο κόμβος θα πρέπει να εκτελεί την υπηρεσία του χωρίς να επηρεαστεί από την επίθεση. Ένα παράδειγμα τέτοιων επιθέσεων είναι η άρνηση εκτέλεσης υπηρεσίας .

Ακεραιότητα σημαίνει η μη τροποποίηση ενός μηνύματος συνειδητά ή ασυνείδητα. Η διαγραφή ή η αλλαγή του περιεχομένου των μηνυμάτων, με σκοπό κακόβουλη δραστηριότητα, προσβάλει την ακεραιότητα του συστήματος .

Η εμπιστευτικότητα επιτρέπει οι πληροφορίες να είναι προσβάσιμες μόνο από εξουσιοδοτημένους κόμβους [54]. Με τον τρόπο αυτό, ο στόχος είναι να διασφαλιστεί το απόρρητο των εμπιστευτικών πληροφοριών.

Αυθεντικότητα σημαίνει να είναι διασφαλισμένη η υποβολή των πραγματικών ταυτοτήτων των κόμβων [54]. Σε περιπτώσεις όπου δεν υπάρχει εγγύηση, οι επιτιθέμενοι μπορούν να προσδώσουν στον εαυτό τους, άλλες ταυτότητες και να εκτελέσουν επιθέσεις χρησιμοποιώντας αυτές.

Η μη αποποίηση αναφέρεται στο να μην μπορεί ο αποστολέας να αρνηθεί την αποστολή ενός μηνύματος ή μιας ενέργειας [54]. Μπορεί να εμφανίζει αφύσικες συμπεριφορές με σκοπό την πρόκληση βλάβης μέσω ενός κόμβου που στέλνει εσφαλμένα ή λάθος μηνύματα. Αυτές οι ανωμαλίες, μπορούν επίσης να έχουν την πρόθεση να διακόψουν τη χρηστικότητα του δικτύου, προκαλώντας ταυτόχρονα συμφόρηση εντός του δίκτυο. Όταν εντοπιστούν τέτοιες καταστάσεις, ο κόμβος που προκαλεί το πρόβλημα, θα επιβεβαιώσει πως οι σχετικές λειτουργίες διεξήχθησαν αυτόματα.

Εξουσιοδότηση σημαίνει, ότι μπορεί να χορηγηθεί άδεια πρόσβασης σε πόρους σχετικά με την αναγνώριση, ακολουθώντας τη διαδικασία «επιβεβαίωση αναγνώρισης» . Διαφορετικά επίπεδα πρόσβασης δίνονται στις διεργασίες και στους κόμβους. Με αυτό τον τρόπο, οι κόμβοι μπορούν να διεξάγουν λειτουργίες εντός των δικών τους επιπέδων πρόσβασης, μόνο στις διεργασίες που έχουν το ίδιο επίπεδο πρόσβασης.

Ανωνυμία, σημαίνει να διατηρηθούν οι πληροφορίες ταυτοποίησης των κόμβων κρυφές. Επίσης, οι πληροφορίες αυτές δεν πρέπει να διανέμονται από τους κόμβους. Με αυτόν τον τρόπο, ο κόμβος μοιράζεται το επίπεδο πρόσβασής του, μόνο με τους κόμβους που επιθυμεί. Αυτό το κριτήριο επιτρέπει την απόκρυψη της ταυτότητας των κόμβων από κακόβουλους κόμβους.

4.3 Ανάλυση της Παρεμβολής σε Πρωτόκολλα Δρομολόγηση

4.3.1 Επιθέσεις σε δίκτυα Ad-Hoc

Οι επιθέσεις ασφάλειας σε Ad-Hoc δίκτυα έχουν εξεταστεί σε πολλές μελέτες. Αυτές οι μελέτες δείχνουν ότι οι επιθέσεις αποσκοπούν, είτε στην κατάκτηση του ελέγχου, ή απλώς στη διαρροή ευαίσθητων δεδομένων, ή στην κωλυσιεργία της αποστολής, δημιουργώντας ανωμαλίες εντός του δικτύου [55].

Όταν ο έλεγχος ενός δικτύου καταλαμβάνεται από τους αντιπάλους του σε μια επίθεση, είναι σαφές ότι το δίκτυο αυτό έχει ήδη καταληφθεί. Ωστόσο, άλλες επιθέσεις είναι δύσκολο να εντοπιστούν εξαιτίας της δυσκολίας στη διάκριση μεταξύ της συμπεριφοράς των μολυσμένων δικτύων από τα μη μολυσμένα δίκτυα. Σε αυτή την ενότητα, εστιάσαμε στα γνωστά ζητήματα ασφάλειας.

4.3.1.1 Υποκλοπές

Η υποκλοπή είναι πολύ ευκολότερη σε ασύρματο περιβάλλον, παρά σε ενσύρματο [56]. Για ένα ενσύρματο μέσο, η απειλή απαιτείται να έχει πρόσβαση στο ίδιο το καλώδιο. Ωστόσο, αυτή η απαίτηση δεν υπάρχει για το ασύρματο περιβάλλον, αρκεί η απειλή να είναι εντός του περιβάλλοντος της επικοινωνίας. Ακόμα κι αν τα δεδομένα είναι κρυπτογραφημένα στην ασύρματη επικοινωνία, μπορεί ένας κακόβουλος κόμβος να ¨κρυφακούσει¨. Υπάρχει η δυνατότητα να εξακριβωθεί ο τύπος κρυπτογράφησης, αναλύοντας τα κρυπτογραφημένα πακέτα που έχουν ληφθεί από την επικοινωνία εντός του ασύρματου μέσου. Ο μόνος σκοπός αυτού του είδους των επιθέσεων είναι να κρυφακούσουν, και δεν γίνεται καμία αλλαγή στο περιεχόμενο του πακέτου. Επομένως, είναι δύσκολο να κατανοηθεί ότι πραγματοποιείται μια επίθεση.

4.3.1.2 Τροποποίηση και Σκευωρία

Επιθέσεις με «Επίθεση Τροποποίησης»: Πρωτόκολλα όπως τα ΑΚΑΑΔ κάθε φορά που εκπέμπουν ένα πακέτο αυξάνουν τον αριθμό ακολουθίας του. Ένας επιτιθέμενος κόμβος μπορεί να ενημερώσει ότι το πακέτο έχει φτάσει στον προορισμό του, εκπέμποντας μικρότερο αριθμό ακολουθίας [57]. Έτσι, μπορεί να προσπαθήσει να φτάσει στον προορισμό του μέσω μιας διαδρομής που έχει ορίσει ο επιτιθέμενος κόμβος, αντί της ορισμένης διαδρομής.

Καταμέτρηση Αναπηδήσεων: Το σύνολο των αναπηδήσεων είναι αριθμός των ενδιάμεσων κόμβων, μέσω των οποίων πρέπει να περάσει ένα πακέτο μεταξύ της πηγής και του προορισμού. Ο επιτιθέμενος θα μπορούσε να έχει πρόσβαση στις πληροφορίες σχετικά με τον αριθμό των κόμβων που μεταπήδησε ένα πακέτο μέχρι να φτάσει στον στόχο, εξετάζοντας τον αριθμό αναπηδήσεων. Ένας επιτιθέμενος κόμβος μπορεί να αλλάξει αυτή την πληροφορία, με σκοπό να την πλαστογραφήσει ή ακόμα και να την μηδενίσει. Εάν η βέλτιστη διαδρομή μπορεί να βρεθεί μέσω του αριθμού αναπηδήσεων, ενδέχεται να μην είναι δυνατή η μεταβολή αυτής της τιμής. Έτσι, η σύνδεση θα γινόταν μέσω λανθασμένης διαδρομής .

Επιθέσεις Πλαστοπροσωπίας: Είναι η επίθεση που παρουσιάζει την δική της διεύθυνση IP ή MAC ως διαφορετική διεύθυνση IP ή MAC. Δεν χρειάζεται απαραίτητα να αλλάζει τις διευθύνσεις IP/MAC, αλλά δύναται να αλλάζει και άλλο αναγνωριστικό στοιχείο. Ως αποτέλεσμα,

εάν διεξαχθεί μια διεργασία που βασίζεται σε αναγνωριστικά στοιχεία για ταυτοποίηση, μπορεί να έχει σαν αποτέλεσμα μια ευπάθεια.

Επίθεση «Σκευωρίας»: Πρόκειται για ένα τύπο επίθεσης που πραγματοποιείται με την αποστολή ψευδών μηνυμάτων δρομολόγησης. Έτσι, στέλνοντας ψευδή μηνύματα, ο επιτιθέμενος κόμβος μπορεί να προβάλει μια έγκυρη διαδρομή ως άκυρη ή το αντίστροφο.

Επίθεση «Βιασύνης»: Μόλις οι κόμβοι λάβουν ένα μήνυμα «διαφήμισης διαδρομών», έχουν την δυνατότητα να αγνοήσουν επόμενα πακέτα με καλύτερες διαδρομές. Ένας επιτιθέμενος κόμβος μπορεί να στείλει τα μηνύματα «διαφήμισης διαδρομών» ταχύτερα και με επιθετικό τρόπο συγκριτικά με τους νόμιμους κόμβους. Εάν καταφέρει να είναι ο πρώτος που στέλνει αυτά τα μηνύματα, οι κόμβοι δέκτες δεν μπορούν να εκτελέσουν σωστά τις λειτουργίες τους προς άλλους κόμβους, εκτός από τον επιτιθέμενο κόμβο . Προκειμένου να υλοποιηθεί και να συνεχιστεί αυτή η επίθεση, οι επιτιθέμενοι κόμβοι πρέπει να στείλουν τα μηνύματα «διαφήμισης διαδρομών» πριν προλάβουν οι άλλοι κόμβοι. Το τελευταίο προκαλεί πρόσθετο φόρτο στο δίκτυο.

Επίθεση «Σκουληκότρυπας»: Αυτή είναι μια επίθεση, που κυρίως προσπαθεί να διαρρεύσει πληροφορίες, δημιουργώντας τούνελ μεταξύ νόμιμων και κακόβουλων κόμβων. Οι κακόβουλοι κόμβοι αναμεταδίδουν ένα αντίγραφο των πακέτων, εκτός του δικτύου, για ανάλυση ή τα απορρίπτουν για να προκαλέσουν διακοπές στην επικοινωνία [58]. Τα συμπτώματα αυτής της επίθεσης δεν είναι εμφανή, λόγω της κινητής φύσης των Ad-Hoc δικτύων. Η βραδύτητα μπορεί να οφείλεται, είτε στα τούνελ, είτε σε κακές περιβαλλοντικές συνθήκες. Είναι δύσκολο να γίνει μια σαφή διάκριση μεταξύ τους. Είναι επίσης γνωστή ως επίθεση «Τούνελ» [59].

Επίθεση «Γκρίζας Τρύπας»: Εάν ο κακόβουλος κόμβος, κατά κάποιον τρόπο, κατορθώσει να εμπλακεί στη διαδρομή, μπορεί να απορρίψει ληφθέντα πακέτα . Επειδή σε αυτή την περίπτωση δίνεται η ερμηνεία ότι ο κόμβος προορισμού δεν είναι προσβάσιμος τη συγκεκριμένη στιγμή, είναι δύσκολο να προσδιοριστεί ο επιτιθέμενος κόμβος. Επιπλέον, ο επιτιθέμενος κόμβος μπορεί να εκτελέσει ψευδή προώθηση για να προκαλέσει διαταραχή ή μπορεί να διασφαλίσει την μη άφιξη των δεδομένων, αφαιρώντας έναν κόμβο από τον πίνακα δρομολόγησης.

4.3.1.3 Εγωισμός

Ονομάζεται έτσι διότι η εκτέλεση της μετάδοσης δεδομένων δεν είναι θεμελιώδες καθήκον των κόμβων που αποτελούν τα MANET. Αυτό έχει σαν αποτέλεσμα τα καθήκοντα μετάδοσης και δρομολόγησης πακέτων να μην αποτελούν προτεραιότητα τους. Αν κάποιος από τους κόμβους διεξάγει την μετάδοση των δεδομένων πολύ αργά ή καθυστερημένα, αυτό μπορεί να επηρεάσει όλη τη διαδικασία μεταφοράς που διέρχεται μέσω αυτού του κόμβου και να προκαλέσει καθυστέρηση. Επιπλέον, ακόμα κι αν δεν αποτελεί επίθεση, διακόπτει τη λειτουργία του συστήματος .

4.3.2 Υφιστάμενα Αντίμετρα για τις Επιθέσεις σε Ad-Hoc Δίκτυα

Οι μηχανισμοί ασφαλείας μπορούν να ταξινομηθούν ως προληπτικοί και αντιδραστικοί. Η προληπτική προσέγγιση αποσκοπεί στην πρόληψη της παραβίασης της ασφάλειας με τη χρήση μεθόδων, όπως η κρυπτογραφία, ενώ η αντιδραστική προσέγγιση στοχεύει στον προσδιορισμό της ίδιας της παραβίασης ασφάλειας. Τα συστήματα ανίχνευσης εισβολής είναι πιθανά παραδείγματα. Αυτό υποδεικνύει ότι η χρήση και των δύο μηχανισμών καθιστά ασφαλέστερο το δίκτυο. Τα αντίμετρα ασφαλείας των Ad-Hoc δικτύων που εξετάζονται παρακάτω παρουσιάζονται για τα διαφορετικά επίπεδα δικτύου [54].

4.3.2.1 Φυσικό Επίπεδο

Καθώς το φυσικό μέσο επικοινωνίας είναι κοινό μεταξύ των Ad-Hoc κόμβων, τα μηνύματα μπορούν να υποκλαπούν σχετικά εύκολα. Η περιοχή υποκλοπής μπορεί να περιοριστεί με τη χρήση κατευθυντικών κεραιών και με τη χρήση διαφορετικών τεχνικών διαμόρφωσης. Έτσι, οι κόμβοι που προσπαθούν να υποκλέψουν για να αναλύσουν τα δεδομένα, ενδέχεται να αντιμετωπίσουν δυσκολίες. Επιπλέον, μπορεί να πραγματοποιηθούν επιθέσεις παρεμβολής σήματος, προκειμένου να υπάρξει διαταραχή στην επικοινωνία. Η τεχνική διαμόρφωσης φασματικής εξάπλωσης με αναπήδηση συχνότητας (ΦΕΑΣ) και η φασματική εξάπλωση με κατευθυντική συχνότητα (ΦΕΚΣ) προτείνονται ενάντια σε τέτοιες επιθέσεις [60]. Στη συνέχεια, προτείνονται οι τεχνικές μη-συντονισμένης αναπήδησης συχνότητας (ΜΑΣ) και μη-συντονισμένη ΦΕΚΣ, οι οποίες αφαιρούν τα επαναχρησιμοποιημένα κλειδιά που χρησιμοποιούν οι τεχνικές ΦΕΑΣ και ΦΕΚΣ.

Η τεχνική συχνότητας αναπήδησης με τη μέθοδο μη-συντονισμένης αναγνώριση πηγής, με βάση την ανταλλαγή κλειδιών είναι αποτελεσματικότερη από προηγούμενες μελέτες . Επίσης έχει αναπτυχθεί τεχνική τυχαίας διαφοροποίησης ΦΕΚΣ, χωρίς την ανάγκη κοινού κλειδιού [61].

4.3.2.2 Επίπεδο Συνδέσμου

Το επίπεδο συνδέσμου είναι υπεύθυνο για την πρόσβαση στα μέσα διάδοσης, τον έλεγχο σφαλμάτων καθώς και της ροής. Ο εγωιστικός τρόπος χρήσης των μέσων διάδοσης, μπορεί να βλάψει το δίκτυο, με επιθέσεις Άρνηση της Υπηρεσίας [62]. Υπάρχουν μηχανισμοί που ανιχνεύουν και αποτρέπουν την εγωιστική χρήση [63], όπου αναφέρθηκε και παραπάνω. Προτείνει ένα ενεργειακά οικονομικό πρωτόκολλο ασφαλείας στο επίπεδο συνδέσμου, το οποίο διεξάγει έλεγχο ταυτότητας και έλεγχο ακεραιότητας μηνυμάτων .

4.3.2.3 Επίπεδο Δικτύου

α. Επιθέσεις «Σκουληκότρυπας»: Οι μετρήσεις που υποδεικνύουν επιθέσεις «Σκουληκότρυπας» σε Ad-Hoc δίκτυα είναι ως εξής :

(1) Αντοχή: Ο κακόβουλος κόμβος προσπαθεί να προσελκύσει την κυκλοφορία του δικτύου πάνω του. Το γεγονός ότι ο ίδιος κόμβος υπάρχει σε πολλές από τις διαδρομές ενισχύει τη πιθανότητα μιας σκουληκότρυπας.

(2) Μήκος διαδρομής: Εάν υπάρχει διαφορά μεταξύ του μήκους της διαδρομής που ενδείκνυται και της έγκυρης διαδρομής, ενισχύεται η πιθανότητα ύπαρξης μιας σκουληκότρυπας.

(3) Έλξη: Εάν εμφανίστηκε μια νέα συντομότερη διαδρομή κατά μήκους μιας ήδη υπάρχουσας διαδρομής, η αιτία αυτού θα μπορούσε να είναι μια επίθεση με «σκουληκότρυπα».

(4) Ανθεκτικότητα: Αυτό σημαίνει ότι η «σκουληκότρυπα» εξακολουθεί να υφίσταται ακόμα και όταν προκύψει κάποια δομική αλλαγή σε ένα δίκτυο. Εάν ο ίδιος κόμβος εξακολουθεί να υπάρχει εντός της διαδρομής μετά από τοπολογικές αλλαγές, πιθανότατα είναι εξαιτίας μιας σκουληκότρυπας.

Η πρόληψη περιλαμβάνει, είτε εξειδικευμένο εξοπλισμό που ονομάζεται Πρόληψη Επίθεσης Σκουληκότρυπας, είτε χωρίς εξοπλισμό που την εντοπίζει κατά την φάση της αναζήτησης μιας διαδρομής.

β. Επίθεση «Μαύρης Τρύπας»: Ως αμυντικός μηχανισμός κατά των πολλαπλών κόμβων μαύρης τρύπας προτείνεται [64] μια λύση που ανιχνεύει τον κακόβουλο κόμβο στο πρωτόκολλο δρομολόγησης δικτύου ΑΚΑΑΔ [65]. Επιπλέον, αναπτύσσεται μια προσέγγιση που βασίζεται στην εμπιστοσύνη με τους γειτονικούς κόμβους [66]. Επιπρόσθετα, αναφέρεται ότι το πρωτόκολλο ασφαλούς δρομολόγησης των Ad-Hoc δικτύων που βασίζεται σε κατ' απαίτηση πρωτόκολλα μπορεί να χρησιμοποιηθεί για την πρόληψη των επιθέσεων «Μαύρης Τρύπας» [54].

γ. Μίμηση και Αποποίηση: Για την αποφυγή της μίμησης και της αποποίησης απαιτείται μηχανισμός αναγνώρισης ταυτότητας. Η μέθοδος επικυρωμένης δρομολόγησης Ad-Hoc δικτύων, η οποία παρέχει υπηρεσίες αναγνώρισης ταυτότητας, αποτρέπει την μίμηση και την απόκρυψη, εξασφαλίζοντας προκαθορισμένα πιστοποιητικά και έλεγχο αναγνώρισης από άκρο σε άκρο [54].

δ. Επίθεση «Ακεραιότητας»: Αποτρέπονται με αντίμετρα που αποσκοπούν στην προστασία της ακεραιότητας του πακέτου από επιθέσεις που αλλάζουν το περιεχόμενο του, όπως τον αριθμό ακολουθίας του. Το πρωτόκολλο ασφαλούς και βέλτιστης απόστασης δρομολόγησης για κινητά ασύρματα Ad-Hoc δίκτυα, το οποίο προσπαθεί να εμποδίσει την τροποποίηση με την χρήση αλυσίδων κατατεμαχισμού, μπορεί να δοθεί ως παράδειγμα [54].

4.3.2.4 Επίπεδο Μεταφοράς

Οι επιθέσεις που είναι γνωστές, κατά του επίπεδου μεταφοράς, είναι οι πλημμύρες SYN και οι επιθέσεις κατάληψης συνδέσεων [67]. Το γεγονός ότι το πρωτόκολλο ελέγχου μετάδοσης βασίζεται σε καταστάσεις, το καθιστά ευάλωτο έναντι επιθέσεων πλημμύρας SYN. Καθώς το πρωτόκολλο ελέγχου μετάδοσης δεν χρησιμοποιείται επακριβώς στα Ad-Hoc δίκτυα, έχουν επινοηθεί νέα πρωτόκολλα, παρόμοια με αυτό. Ωστόσο, τα ζητήματα ασφαλείας δεν εξετάστηκαν κατά τον σχεδιασμό τους. Νέες τροποποιήσεις στα πρωτόκολλα, σχετικά με τις ανάγκες και τις απαιτήσεις ασφάλειας των δικτύων Ad-Hoc, είναι ένα από τα ανοικτά ζητήματα προς συζήτηση [54].

4.3.2.5 Επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής παρέχει υπηρεσίες, όπως τείχος προστασίας για τον έλεγχο πρόσβασης και αυθεντικοποίησης των χρηστών, φιλτράρισμα και καταγραφή πακέτων. Ωστόσο, λόγω έλλειψης δομής εντός των Ad-Hoc δικτύων, η εφαρμογή τείχους προστασίας, δεν είναι τόσο αποτελεσματική, όσο στις παραδοσιακές μεθόδους.

4.4 Ασφάλεια Επικοινωνίας FANET

Η επικοινωνία είναι το βασικό στοιχείο των εφαρμογών ΜΕΑ. Εκτός από τα προβλήματα της αξιόπιστης και αποτελεσματικής μετάδοσης δεδομένων κατά την επικοινωνία των ΜΕΑ, έχουν επίσης ληφθεί υπόψη και τα ζητήματα ασφάλειας έναντι κακόβουλων πράξεων σε αυτές. Ως εκ τούτου, με την αναγνώριση των ευπαθειών των υποσυστημάτων επικοινωνίας στα ΜΕΑ, έχει αυξηθεί το ενδιαφέρον για την ασφάλεια της επικοινωνίας τους, λόγω της σοβαρότητας των συνεπειών τους [68]. Υπό αυτό το πρίσμα, τα τελευταία χρόνια, έχουν γίνει πολλές έρευνες σχετικά με τα ζητήματα

ασφάλειας των επικοινωνιών των ΜΕΑ. Παρακάτω παρουσιάζονται σημαντικές μελέτες σχετικά με τα ζητήματα ασφάλεια της επικοινωνίας των ΜΕΑ.

α. Μια ολοκληρωμένη μελέτη, σχετικά με την ασφάλεια της επικοινωνίας συστημάτων με πολλαπλά ΜΕΑ, που σχετίζεται περισσότερο με την λειτουργία των FANET, διεξάγεται σε σχέση με την αποτελεσματικότερη ομαδική διαχείριση κλειδιών [69]. Αναλύεται η αρχιτεκτονική μιας ασφαλής ομάδας δορυφορικών δικτύων LEO για να διαπιστωθεί εάν μπορεί να προσαρμοστεί σε ετερογενείς εφαρμογές με ΜΕΑ σε σμήνος, με σκοπό να παρέχει ασφαλή και αποτελεσματική επικοινωνία. Το κύριο μέλημα της μελέτης είναι η παροχή αποτελεσματικής και επεκτάσιμης αρχιτεκτονικής για ανταλλαγή ομαδικών κλειδιών, που αποτελεί απαίτηση για την κρυπτογράφηση και την αποκρυπτογράφηση της ομαδικής επικοινωνίας. Η μελέτη καταλήγει στο συμπέρασμα ότι η αρχιτεκτονική μπορεί να χρησιμοποιηθεί για την ασφαλή ομαδική επικοινωνία μεταξύ σμηνών ΜΕΑ, με ορισμένες βελτιώσεις, όσον αφορά την ομαδική διαχείριση κλειδιών, συγκριτικά με άλλες ευρέως χρησιμοποιούμενες αρχιτεκτονικές ασφαλείας.

β. Σε μια άλλη μελέτη σχετικά με την ασφάλεια επικοινωνίας των ΜΕΑ εξετάζονται τα πιθανά ζητήματα που προκύπτουν από την ασύρματη φύση των επικοινωνιών και προτείνονται αντίστοιχες λύσεις για την ασφαλή επικοινωνία .

γ. Σε μια μελέτη ανάλυσης των πολλαπλών ανεξάρτητων επιπέδων ασφάλειας αναλύονται οι σχεδιαστικές ανάγκες των συστημάτων εντός των ΜΕΑ σε ότι αφορά την ασφάλεια πληροφοριών και επικοινωνιών [70]. Η κύρια εστίαση της μελέτης είναι να εκμεταλλευτεί την τμηματική αρχιτεκτονική για να αποκτήσει επίπεδα διασφάλισης.

δ. Μια μελέτη κατατάσσει τα ευπαθή σημεία ασφαλείας των ήδη υπαρχόντων συστημάτων αυτόματου πιλότου στα ΜΕΑ, σε τρεις ομάδες:

(1) Επιθέσεις υλικού,

(2) Επιθέσεις ασύρματου δικτύου,

(3) Επιθέσεις αισθητήρα.

Επίσης αναλύει και την συμπεριφορά του συστήματος μετά από μια τέτοιου είδους επίθεση. Προτείνει μια αρχιτεκτονική κυβερνοασφάλειας για το σύστημα αυτόματου πιλότου, βασισμένο σε έναν υπεύθυνο επίβλεψης της κυβερνοασφάλειας. Ο τελευταίος είναι υπεύθυνος για την ανίχνευση και απομόνωση κακόβουλων δραστηριοτήτων στο σύστημα αυτόματου πιλότου. Τα αποτελέσματα προσομοίωσης έχουν δείξει ότι η προτεινόμενη αρχιτεκτονική ασφαλείας καθιστά το σύστημα πιο ανθεκτικό έναντι ενδεχόμενων κυβερνοεπιθέσεων.

ε. Διεξάγεται μια μελέτη, σχετικά με τις επιπτώσεις παραποιημένων σημάτων GPS ενός αυτόνομου ΜΕΑ, όπου εξετάζονται οι απαιτήσεις για την επιλογή του συστήματος πλοήγησης του, η οποία πραγματοποιήθηκε βάση αποτελεσμάτων από πρακτικές δοκιμές που έχουν ήδη γίνει σε αριθμό εμπορικών δεκτών GPS. Επανειλημμένα εκτελεσμένες επιθέσεις από διαφορετικές πλεονεκτικές θέσεις, δείχνουν ότι ένας εισβολέας είναι ικανός να καταλάβει το ΜΕΑ-στόχος εντός εμβέλειας 50 μέτρα, με σφάλμα εκτίμησης ταχύτητας 10 m/s .

στ. Σε μια άλλη μελέτη, ερευνάτε η ασφαλής ομαδική επικοινωνία από απόσταση σε πολλαπλά αυτόνομα ΜΕΑ για να αναλυθούν οι επιπτώσεις της επικοινωνίας στη δυναμική της ομάδας, και στην ασφάλεια της επικοινωνίας από απόσταση [71]. Ως προτεινόμενη λύση

παρουσιάζεται μια προσέγγιση σχηματισμού σμήνους ΜΕΑ, η οποία βασίζεται στην τροποποίηση των παραμέτρων της ασύρματης επικοινωνίας για το κάθε μέλος της ομάδας. Η αποτελεσματικότητα της προτεινόμενης λύσης εξετάζεται στο πλαίσιο ενός πιθανού στρατιωτικού σεναρίου.

ζ. Άλλη μια ανάλυση των επιθέσεων παρεμβολής σε σμήνη ΜΕΑ, εξετάζει τις επιθέσεις ως ένα παίγνιο μηδενικού αθροίσματος καταδίωξης – αποφυγής. Προκειμένου να επιτευχθεί η βέλτιστη απόδοση για τα ΜΕΑ με την ύπαρξη ενός κινητού παρεμβολέα, αναπτύχθηκε μια προσέγγιση βασισμένη στη θεωρία παιγνίων . Σε ένα παρόμοιο πλαίσιο, το ζήτημα της παρεμβολής μετατρέπεται σε πρόβλημα κατανομής πόρων, λαμβάνοντας υπόψη τους περιορισμούς ισχύος του κάθε ΜΕΑ και μια διαφορική θεωρία παιγνίου με δύο παίκτες, που ανακατασκευάζεται σε ένα παιχνίδι με δύο ομάδες με πολλαπλούς παίκτες [72].

η. Ένα άλλο ασφαλές σχέδιο επικοινωνίας για τα FANET που διερευνάται, προτείνει μια ενσωματωμένη έξυπνη κάρτα στο ΜΕΑ για την παροχή των απαιτούμενων λειτουργιών ασφάλειας, βάσει της προηγούμενης μελέτης του συντάκτη για την διαχείριση των κατανεμημένων ταυτοτήτων στα MANET . Η χαμηλού επιπέδου ασφάλεια των ραδιοσυχνοτήτων αντιμετωπίζεται με τη χρήση ειδικών εξαρτημάτων για την ορθή επιλογή της ραδιοσυχνότητας. Επιπλέον, η ασφάλεια στο επιπέδου του λογισμικού επιτυγχάνεται με την ενσωμάτωση έξυπνων καρτών, ώστε να διαθέτουν δυνατότητες κρυπτογραφίας για την ασφαλή διαχείριση δυναμικών ομάδων. Στα πλαίσια μιας παρόμοιας λύσης έχουν εντοπιστεί οι απαιτήσεις ασφαλείας για τα αυτόνομα σμήνη ΜΕΑ, με σενάριο παρουσίας ισχυρών αντιπάλων. Επίσης, προτείνεται μια θεωρητική λύση που ονομάζεται Έξυπνη Συσκευή Ασφάλισης Ραδιοσυχνοτήτων, που λειτουργεί ως ένα ενσωματωμένο ασφαλές στοιχείο για να ικανοποιήσει τις απαιτήσεις της αρχιτεκτονική ασφαλείας. Παράλληλα, συγκρίνονται τα ασφαλή στοιχεία που μπορούν να ενσωματωθούν σε ΜΕΑ. Επιπλέον, η προτεινόμενη λύση διαμορφώνεται επιλέγοντας τα βέλτιστα χαρακτηριστικά από τους ¨Ασύρματου Αισθητήρα Κόμβου¨, το ¨Εμπιστευόμενο Μοντέλο Διαδρομής¨, της ¨Έξυπνης Κάρτας¨, και του ενεργού RFID, τα οποία αξιολογούνται ως υποψήφια στοιχεία ασφαλείας [73].

θ. Επίσης προτείνεται μια ασφαλής τρισδιάστατη προσέγγιση τοποθεσίας, βασισμένη σε αλγόριθμο Multilateration και στον Δείκτη Ένδειξής Έντασης Σήματος για σμήνη ΜΕΑ . Ο σκοπός της προτεινόμενης μεθόδου επαλήθευσης είναι για να ανιχνεύει ψευδείς/ψεύτικες θέσεις που το σμήνος ΜΕΑ χρησιμοποιεί. Τα αποτελέσματα δείχνουν τη δυνατότητα της προτεινόμενης αρχιτεκτονικής για την ασφαλή εξακρίβωση των θέσεων των ΜΕΑ.

ι. Ένα άλλο σημαντικό ζήτημα είναι το ερευνητικό περιβάλλον και η προσομοίωση στις οποίες διεξάγονται οι δοκιμές της ασφάλειας των επικοινωνιών των σμηνών ΜΕΑ .

4.5 Ανοιχτά Ζητήματα Έρευνας

Υπάρχουν ορισμένες διαφορές μεταξύ των FANET και των υφιστάμενων δικτύων Ad-Hoc. Ο κύριος λόγος είναι ότι οι κόμβοι FANET αποτελούνται αποκλειστικά από ΜΕΑ, τα οποίοι οδηγούν σε συχνές αλλαγές στην τοπολογία, λόγω του υψηλού βαθμού κινητικότητάς τους. Υπάρχουν επίσης, άλλοι παράγοντες, όπως το περιβάλλον λειτουργίας, η πυκνότητα κόμβων, ο εντοπισμός, η κατανάλωση ενέργειας κλπ. [52].

Παρόλο που ορισμένοι από αυτούς τους παράγοντες ενδέχεται να φέρουν νέες αδυναμίες, κάποιο άλλοι ενδέχεται να συμβάλλουν στην εξάλειψη ορισμένων υφισταμένων αδυναμιών

ασφαλείας. Στο πλαίσιο του FANET, η ανάλυση των υφιστάμενων μηχανισμών άμυνας κατά των απειλών ασφάλειας στα MANET και VANET μπορεί να θεωρηθεί ένας από τους ανοικτούς τομείς έρευνας.

Σε αυτή την ενότητα, διερευνώνται ορισμένα ανοικτά ερευνητικά ζητήματα σχετικά με την ασφάλεια των FANET.

4.5.1 Ζητήματα Επικοινωνίας για τα FANET

Ένα ΜΕΑ επικοινωνεί, ως επί το πλείστων, με οπτική επαφή, επομένως είναι πιο πιθανό να υποκλαπούν στοιχεία από ότι σε άλλα Ad-Hoc δίκτυα. Η χρήση κατευθυντικών κεραιών, αντί για πανκατευθυντικές κεραίες στις εφαρμογές FANET, μπορεί να καταστήσει τις επιθέσεις πιο δύσκολες. Η χρήση κατευθυντικών κεραιών συγκεντρώνει τη μετάδοση δεδομένων προς την επιθυμητή κατεύθυνση και μειώνει την πιθανότητα υποκλοπής και παρεμβολής [74]. Επιπλέον, κατευθυντικές κεραίες μπορούν να χρησιμοποιηθούν για την προστασία του συστήματος από τις επιθέσεις «Σκουληκότρυπας». Οι κατευθυντικές κεραίες προσφέρουν επίσης, μεγαλύτερη ακτίνα εμβέλειας [75].

Καθώς τα ΜΕΑ λειτουργούν με γρήγορο και αυτόνομο τρόπο, η θέση τους αλλάζει συχνά, έχοντας ως αποτέλεσμα τα ΜΕΑ να είναι εκτός εύρους της κατευθυντικής κεραίας. Για το λόγο αυτό, εφαρμόζονται στα ΜΕΑ προσαρμοστικά πρωτόκολλα πρόσβασης του μέσου [75]. Ένα άλλο σημαντικό ζήτημα που επηρεάζει την απόδοση των FANET είναι η αντίληψη της ακριβής θέσης των γειτονικών κόμβων. Έτσι, για τα FANET εφαρμόζεται το «Εύρεσης Τοποθεσίας Κατευθυντικό Πρωτόκολλο Πρόσβασης στο Μέσο», ως διορθωτικό μέτρο για την εκτίμηση της θέσης των γειτονικών ΜΕΑ .

4.5.2 Οπτική Επικοινωνία στον Ανοιχτό Χώρο

Μία από τις πιο ελπιδοφόρες τεχνολογίες για την ασφάλεια της επικοινωνίας των FANET είναι τα οπτικά συστήματα επικοινωνίας ελεύθερου χώρου. Εκτός από την εξαιρετικά υψηλή ταχύτητα επικοινωνίας, υπόσχονται επίσης, υψηλότερα επίπεδα ασφάλειας . Τα συστήματα οπτικών επικοινωνιών ελεύθερου χώρου εκπέμπουν μια στενή δέσμη οπτικών ακτινών, οι οποίες είναι απρόσιτες, εκτός και αν παρεμβάλλονται απευθείας στην διαδρομή τους. Η οπτική επικοινωνία ελεύθερου χώρου μεταδίδει περισσότερα δεδομένα με την εξάπλωση του σήματος σε μικρότερη περιοχή, συγκριτικά με τις κατευθυντικές κεραίες, μειώνοντας έτσι την πιθανότητα υποκλοπής. Ωστόσο, η οπτική επικοινωνία ελευθέρου χώρου επηρεάζεται από τον καιρό.

Επιπλέον, ενδέχεται να προκύψει πρόβλημα εύρεσης του σημείου στόχευσης, λόγω της φύσης της επικοινωνίας που είναι «σημείο σε σημείο». Το μεγαλύτερο μέρος της έρευνας έχει γίνει πάνω στη δομή επικοινωνίας από το έδαφος προς το ΜΕΑ [76]. Η απόκτηση σημείου στόχευσης μπορεί να είναι πιο δύσκολη στα FANET, λόγω του ότι η δομή επικοινωνίας είναι από ΜΕΑ σε ΜΕΑ. Ευτυχώς, υπάρχουν ορισμένες έρευνες που δείχνουν ότι είναι εφικτή η οπτική επικοινωνία ελευθέρου χώρου μεταξύ των αεροσκαφών, και ότι μπορεί να χρησιμοποιηθεί και στα FANET [77]. Ειδικά η εταιρία επικοινωνίας «Vialight», εγκαθιστά μικροσκοπικούς πομποδέκτες λέιζερ, οι οποίοι παρέχουν μια αξιόπιστη, κρυφή επικοινωνία από σημείο σε σημείο.

4.5.3 Περιορισμοί της Πλατφόρμας των MEA

Τα μικρότερα σε μέγεθος MEA προτιμώνται στις εφαρμογές με δίκτυα FANET. Αυτό σημαίνει, ότι κάθε MEA στο FANET έχει περιορισμένη χωρητικότητα. Έτσι, μπορούν εύκολα να υποκλαπούν. Αυτό αποτελεί σοβαρή απειλή, ειδικά για τις στρατιωτικές εφαρμογές. Οι πληροφορίες που μεταφέρονται και οι μέθοδοι κρυπτογράφησης, δεν πρέπει να υποκλέπτονται από κακόβολους. Λόγω των περιορισμών του μεγέθους και του κόστους των MEA, δεν είναι εφικτή η προσάρτηση πολύπλοκων συστημάτων.

Επιπλέον, εξελιγμένες τεχνολογίες που δεν θέλουμε να υποκλαπούν ενδέχεται να μην εφαρμόζονται στα FANET, λόγω αυτής της πιθανότητας. Σε τέτοιες περιπτώσεις, η εφαρμογή της υπάρχουσας τεχνολογίας στο FANET μπορεί να είναι η καταλληλότερη προσέγγιση. Με την κατάληψη ενός MEA, μπορούν κακόβολοι να το μελετήσουν, με την χρήση της αντίστροφης μηχανικής. Με αυτό το τρόπο, μπορεί να προκαλέσουν δυσλειτουργία στους αλγόριθμους ή διαρροή πληροφοριών. Κατά την εφαρμογή των αλγορίθμων στα FANET, θα πρέπει να θεωρηθεί ότι τα MEA δύναται να καταληφθούν από τον εχθρό και κατά συνέπεια, οι αλγόριθμοι που χρησιμοποιούνται σε αυτά μπορούν να εκτεθούν.

4.5.4 Αυτονομία από τον Σταθμό Εδάφους

Ένα από τα πιο σημαντικά χαρακτηριστικά του FANET είναι ότι λειτουργεί χωρίς σταθμό εδάφους. Ωστόσο, οι περισσότερες από τις διαθέσιμες αρχιτεκτονικές ασφαλείας εξαρτώνται από την ύπαρξη σταθμού εδάφους. Η επιτυχής προσαρμογή αυτών και η κάλυψη των αναγκών ασφαλείας των Ad-Hoc δικτύων, όπως στα MANET και τα VANET, λαμβάνοντας υπόψη την εξαιρετική δυναμική φύση των FANET, αποτελεί ένα ανοιχτό ζήτημα έρευνας.

4.6 Συμπεράσματα Κεφαλαίου

Τα FANET και η ασφάλεια τους αποτελούν ένα αναδυόμενο ερευνητικό πεδίο. Η υπάρχουσα βιβλιογραφία είναι περιορισμένη και επικεντρώνεται κυρίως σε διαφορετικού τύπου Ad-Hoc δίκτυα, όπως τα MANET και τα VANET.

Τα χαρακτηριστικά των FANET, τα καθιστούν ως ξεχωριστό πεδίο έρευνας και ως τέτοιο, θα πρέπει να εκλαμβάνεται και στον τομέα της ασφάλειας.

Κεφάλαιο 5

Εναλλακτικές Μέθοδοι ΜΕΑ

5.1 Εισαγωγή

Στο επίκεντρο της υπόψη εργασίας έχει αναλυθεί η περίπτωση των ασύρματων δικτύων στην χρήση των συστημάτων προσδιορισμού θέσεως (γενικά GPS), καθώς και στα Μη Επανδρωμένα Αεροσκάφη (ΜΕΑ), με έμφαση στις παρακάτω περιπτώσεις:

α. Στους τρόπους ανάπτυξης στα υπόψη συστήματα.

β. Τις αρχιτεκτονικές επικοινωνίας αυτών με παρουσίαση των πρωτοκόλλων δρομολόγησης και κύρια στα ειδικού σκοπού (Ad hoc) δίκτυα.

γ. Διάφορες μέθοδοι παρεμβολής (jamming) στις παραπάνω κατηγορίες, με προσήλωση κυρίως στην περίπτωση των ΜΕΑ.

Προχωρώντας σε λίγο πιο ιδιαίτερα θέματα στο υπόψη αντικείμενο, θα επιχειρηθεί μια ανάπτυξη σε μια παράλληλη πλευρά, με την χρήση άλλων ερευνών, τόσο για την εξεύρεση νέων μεθόδων στην εφαρμογή των ΜΕΑ, όσο και σε περιπτώσεις αντιμετώπισης αυτών.

5.2 Ανάπτυξη Εναλλακτικών Μεθόδων για χρήση ως ΜΕΑ

Στο παρελθόν και μετά τα μισά του 19ου αιώνα, οι πιο προηγμένες χώρες του κόσμου, είχαν ξεκινήσει έρευνες για την κατασκευή μικροσκοπικών σύνθετων ρομπότ, με μορφή εντόμων, για να μην γίνονται αντιληπτά, με απώτερο σκοπό τη χρήση ως ΜΕΑ, είτε σε επιχειρήσεις κατασκοπείας (στρατιωτικής ή πολιτικής/ βιομηχανικής), είτε σε αποστολές έρευνας, διάσωσης και εξεύρεσης ατόμων σε δύσβατες περιοχές ή χώρους, μετά από φυσικές καταστροφές.

Η προσπάθεια αυτή παρουσίαζε πολλές προκλήσεις στην κατασκευή, καθώς ήταν ιδιαίτερα δύσκολο να φτιαχτεί κάτι, από την μία πλευρά ικανό για το σκοπό αυτό και από την άλλη ευπροσάρμοστο και ευμετάβλητο. Τα τελευταία χρόνια, με την έλευση της νέας χιλιετηρίδας του 2000, η νανοτεχνολογία ως επιστήμη, ήρθε να βοηθήσει, κατάφερε όμως να επιλύσει το κύριο μέρος της εφαρμογής, όσον αφορά την συλλογή και μεταφορά δεδομένων, όμως παρέμενε ένα δυσεπίλυτο πρόβλημα, το οποίο ήταν το θέμα της απαιτούμενης ενέργειας για τροφοδοσία και λειτουργία.

Στην παρούσα φάση θα αποδεχτούμε ως δεδομένο την ανάπτυξη τέτοιων κατασκευών σύνθετων ρομπότ με μορφή εντόμων, καθώς δεν αποτελεί αντικείμενο αυτής της εργασίας, θα αναπτύξουμε όμως κάποιες δυνατότητες χρήσης αυτών με επίκεντρο στη χρήση τους ως ΜΕΑ και την παρεμβολή – παρεμπόδισή τους.

Συνεχίζοντας για τα παραπάνω, η περίπτωση της χρήσης υλικών για συλλογή ηλιακής ενέργειας δεν ήταν ιδιαίτερα προσοδοφόρα, καθώς εξαρτιόταν από τον ήλιο, ο οποίος δεν ήταν δυνατή η χρήση του για όλες τις εφαρμογές και η επίλυση με κάποιο είδος μικρής γεννήτριας, θα απαιτούσε ιδιαίτερο όγκο και βάρος σε μια τόσο μικρή κατασκευή.

Σε αυτή την φάση κατέληξαν σε μια πρωτοπόρα διαπίστωση, να χρησιμοποιήσουν το πλεονέκτημα αντί να επιχειρήσουν να παράξουν αυτά τα σύνθετα μιμητικά ρομπότ, να επιδοθούν στην προσπάθεια μετατροπής των ήδη υπαρχόντων έμβιων εντόμων σε «κατευθυνόμενα ρομπότ», μέσω της βιο-νανοτεχνολογίας.

5.3 Χρήση των Ιπτάμενων Έμβιων Όντων – Έντόμων ως MEA

5.3.1 Προσπάθειες χρήσης έμβιων όντων

Η πρώτη προσπάθεια χρησιμοποίησης έμβιων όντων ως κατευθυνόμενα ρομπότ, ξεκίνησε πριν την δεκαετία του 2000, με πειράματα σε ζώα, όπως περιστέρια, γάτες, μέλισσες, σκαθάρια κ.ά. Η Υπηρεσία που είχε την περισσότερη δραστηριότητα στον τομέα αυτό είναι των Προηγμένων Ερευνητικών Έργων Άμυνας της Αμερικής (Defense Advanced Research Projects Agency – DARPA), κυρίως με σκοπό τον μεμακρυσμένο έλεγχο από ηλεκτρονικά εμφυτευμένα συστήματα για περιπτώσεις είτε έρευνας – διάσωσης, είτε παρακολούθησης – κατασκοπείας.

Το 2004, ο John Chapin, καθηγητής στο Κρατικό Πανεπιστημιακό Κέντρο Επιστημών Υγείας της Νέας Υόρκης, στο Μπρούκλιν, παρουσίασε τους Rescue Rats [78]. Αυτοί ήταν εργαστηριακοί αρουραίοι με νευρικά εμφυτεύματα που τους ενθάρρυνε να κατευθύνουν (μέσω πασσάλων) εντοπιστή GPS για να βρουν ανθρώπους. Χρησιμοποιώντας ένα ασύρματο τηλεχειριστήριο, ο Chapin διέγειρε ένα μέρος των μυαλών των αρουραίων που μιμούνταν την αίσθηση ότι έχουν αγγιχτεί τα μουστάκια. Σε απάντηση, οι αρουραίοι στράφηκαν προς την κατεύθυνση της αίσθησης. Όταν γύρισαν, ο Chapin τους αντάμειψε με ένα γρήγορο κλονισμό ηλεκτρισμού στο κέντρο ευχαρίστησης των μυαλών τους.

Το 2005 η Jelle Atema, βιολόγος στο Πανεπιστήμιο της Βοστώνης και στο Ωκεανογραφικό Ινστιτούτο Woods Hole, χρηματοδοτήθηκε επίσης από το DARPA, για να διερευνήσει καρχαρίες που κατευθύνονταν με παρόμοια νευρικά εμφυτεύματα. Η Atema είχε πει ότι ενώ επικροτεί το σχέδιο Hybrid Insect Micro-Electro-Mechanical Systems (HI-MEMS), για την τεχνική του φιλοδοξία και τεχνική δεξιοτεχνία, ανησυχούσε για την τελική βιολογική του δυνατότητα. Υποστήριζε ότι ο ηλεκτρονικός έλεγχος θα ανταγωνίζεται τις φυσικές διαδικασίες του εγκεφάλου και παρέθεσε κάποιους περιορισμούς για τα έντομα, συμπεριλαμβανομένης της τάσης των μορίων να πλησιάζουν τις πηγές φωτός (τις παροιμιώδεις φλόγες) και μια ισχυρή απόκριση φερορμόνων σεξ. Αυτές έλεγε ότι θα μπορούσαν να υπερισχύσουν των προσπαθειών απομακρυσμένου ηλεκτρονικού ελέγχου, καθώς είναι απίστευτα ισχυρές.

5.3.2 Προσπάθειες χρήσης έμβιων εντόμων

Μετά τα έμβια όντα, οι προσπάθειες (μέσω της βιο-νανοτεχνολογίας), κατευθύνθηκαν στην δημιουργία εντόμων, με χειρισμό από την μια πλευρά μέσω κυμάτων υπεριώδους ισχύος και από την άλλη πλευρά με μεθόδους συλλογής ενέργειας μέσω συγκεκριμένων κυκλωμάτων.

5.3.3 Προσπάθεια Εφαρμογής Χειρισμού σε Σκώρο

Το έργο ξεκίνησε τον σχεδιασμό του από το 2005, από τον διευθυντή προγράμματος Amit Lal, καθηγητή ηλεκτρολόγου μηχανικού, μετά από την αποχώρησή του από το Πανεπιστήμιο Cornell, υλοποιώντας τον συντονισμό εκ μέρους της DARPA. Το Ινστιτούτο της Μασαχουσέτης (Massachusetts Institute of Technology – MIT) επίσης είναι ένας από τους τρεις μεγάλους

χορηγούς, όπως το Πανεπιστήμιο του Michigan και το Ινστιτούτο Boyce Thompson. Η έρευνα βασίζεται επίσης στο έργο των εντομολόγων, των ηλεκτρολόγων μηχανικών και των Μηχανολόγων μηχανικών στο Πανεπιστήμιο της Καλιφόρνιας, στο Berkley, στο Πανεπιστήμιο της Αριζόνα και στο πανεπιστήμιο της Ουάσινγκτον στο St. Louis, Mo.

Ο στόχος του πρώτου αυτού προγράμματος (έως το 2009) ήταν η δημιουργία σκώρων ή άλλων εντόμων με εμφυτευμένα ηλεκτρονικά χειριστήρια μέσα τους, επιτρέποντάς τους να τα ελέγχει ένας απομακρυσμένος χειριστής. Το υβριδικό πλέον έντομο θα μπορούσε να μεταδώσει δεδομένα από ενσωματωμένους αισθητήρες και να περιλαμβάνουν είτε βίντεο είτε φωνή χαμηλής ποιότητας με τους αισθητήρες εικόνας (για επιτήρηση) ή αερίου (για αναγνώριση σε φυσικές καταστροφές). Για να φτάσουνε σε αυτό το σημείο, το τμήμα Hybrid Insect Micro-Electro-Mechanical Systems (HI-MEMS) ακολούθησε τρεις ξεχωριστές διαδρομές – στάδια:

α) Αυξάνοντας τα υβρίδια Micro-Electro-Mechanical Systems (MEMS) έντομα,

β) Αναπτύσσοντας ηλεκτρονικά διεύθυνσης για τα έντομα αυτά, και

γ) Βρίσκοντας τρόπους για συλλογή ενέργειας στα μηχανικά μέρη των εντόμων, για αύξηση της τροφοδοσίας και κυρίως της αυτονόμησης.

Η πρόοδος που εξελίχτηκε στο πρόγραμμα, παρουσιάστηκε αρχικά στην Ιταλία, στο Sorrento, από 25-29 Ιανουαρίου 2009, στο παγκόσμιο συνέδριο του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers – IEEE) και Μικρο-ηλεκτρονικών Μηχανικών Συστημάτων (Micro Electro Mechanical Systems – MEMS).

Για να θεωρηθεί επιτυχής το τελικό HI-MEMS (cybernetic), πρέπει να είχε αποδεκτό ένα σφάλμα σε πτήση 100 μέτρων από ένα σημείο εκκίνησης και στη συνέχεια να κατευθύνεται σε ελεγχόμενη προσγείωση εντός 5 μέτρων από ένα καθορισμένο τελικό σημείο. Κατά την προσγείωση, το έντομο πρέπει να παραμείνει στη θέση του.

Στο πρώτο στάδιο των εφαρμογών, η καθηγητής Anantha Chandrakasan, ηλεκτρολόγος μηχανικός στο MIT, χρησιμοποίησε σε τσιπ, ένα σύστημα λήψης ultrawide band, ένα διαδιδόμενο κύμα ραδιοφώνου που λειτουργεί σε εξαιρετικά χαμηλή ισχύ σε μια ευρεία περιοχή φάσματος. Σε προηγούμενη έρευνα είχανε δημιουργήσει έναν κατάλληλο πομπό για την διάδοση αυτών των κυμάτων, ενώ τώρα θα χρησιμοποιούνταν ομοίως για την επίτευξη του τηλεχειρισμού των πειραματικών συστημάτων στο έντομο. Η συσκευή – δέκτης προσαρμόστηκε ειδικά για το έργο HI-MEMS στον σκώρο, για να τον κατευθύνει. Για να ελέγξει την κατεύθυνση του σκώρου, ο τότε Διευθυντής εργαστηρίων Chandrakasan και ο μεταπτυχιακός φοιτητής του MIT Denis Daly σχεδίασαν ένα μικρό, ελαφρύ και χαμηλής ισχύος δέκτη – ραδιόφωνο, συνδεδεμένο με έναν νευροδιεγέρτη βολφραμίου 4 ηλεκτροδίων. Όταν αυτό το ραδιόφωνο παίρνει τις σωστές εντολές, η συσκευή διεγείρει τον νευρικό ιστό στο κορμό του κοιλιακού νεύρου του σκώρου. Η διέγερση κάνει την κοιλιά του σκώρου να κινείται με τρόπο που να αλλάζει την κατεύθυνση της πτήσης του. Το ραδιόφωνο και ο διεγέρτης τροφοδοτούνται από μια μικρή μπαταρία ακρόασης.

Το δεύτερο στάδιο περιλαμβάνει ένα micro-τσιπ ψηφιακό επεξεργαστή βασικής ζώνης χαμηλής ισχύος, το οποίο μπορεί να συγχρονιστεί πολύ γρήγορα με ασύρματα σήματα. Αυτό επιλύει ένα συγκεκριμένο πρόβλημα με την ασύρματη επικοινωνία. «Όταν αποστέλλεται ένα κομμάτι δεδομένων μέσω ασύρματης σύνδεσης, ο δέκτης χρειάζεται κάποιο χρονικό διάστημα για

να κλειδώσει στον πομπό», λέει ο Chandrakasan. «Οι νέοι αλγόριθμοι μπορούν να συγχρονιστούν πολύ γρήγορα, πράγμα που σημαίνει ότι μπορείτε να ενεργοποιήσετε το ραδιόφωνο, να πάρετε το κομμάτι των δεδομένων και στη συνέχεια να σβήσετε γρήγορα το ραδιόφωνο». Αυτό επίλυε σε μεγάλο βαθμό το κομμάτι της εξοικονόμησης ενέργειας.

Το τρίτο στάδιο, περιελάμβανε την εξεύρεση τρόπων αποτελεσματικής συγκομιδής ενέργειας από το σκώρο, καθώς η ισχύς που καταναλώνουν τα κυκλώματα ελέγχου των θεριστών μειώνει την ποσότητα της χρησιμοποιήσιμης ηλεκτρικής ενέργειας. Σε αυτήν την περίπτωση παρουσιάστηκε στο International Solid-State Circuits Conference (ISSCC) ένα άλλο micro-τσιπ, για το οποίο ο καθηγητής Chandrakasan, ανέφερε ότι δεν σχετίζεται με τα ραδιοφωνικά τσιπ και δεν χρηματοδοτείται από το HI-MEMS, θα μπορούσε όμως να χρησιμοποιηθεί για την επίτευξη του στόχου του προγράμματος του DARPA.

Τα ηλεκτρονικά και MEMS στοιχεία του συστήματος πρέπει να καταναλώνουν λίγη δύναμη και να είναι απολύτως ελαφρού βάρους (featherweight). Μετά από όλα, για παράδειγμα ένας μέσος σκώρος γερακιών ζυγίζει 2,5 γραμμάρια, οπότε με υπερβολικό βάρος, και καθόσον οι μπαταρίες είναι βαριές δεν θα μπορούσε να πετάξει. Από την άλλη ενώ ένα έντομο-cyborg θα ήταν αρκετά αυτόνομο από ενέργεια, δεν θα υπήρχε τρόπος για να επαναφορτιστεί το ωφέλιμο φορτίο εξοπλισμού του στις αποστολές.

Έτσι οι ερευνητές κατέληξαν στις δυο παρακάτω προτάσεις:

α. Μια μέθοδο με την οποία η πτήση του ίδιου του εντόμου να παράγει την ηλεκτρική ενέργεια που απαιτεί το ηλεκτρονικό φορτίο. Η συγκομιδή της ενέργειας των κραδασμών στο περιβάλλον μέσω πιεζοηλεκτρικών μέσων – στην οποία η ενέργεια μετατρέπεται μεταξύ μηχανικών και ηλεκτρικών μορφών – θα μπορούσε να παρέχει μεταξύ 10 και αρκετών εκατοντάδων μικροκυμάτων ισχύος.

β. Ένα κύκλωμα, που ονομάζεται ανορθωτής αντιστάθμισης πόλωσης, το οποίο βελτιώνει την ικανότητα εξόρυξης ισχύος «περισσότερο από τέσσερις φορές», σύμφωνα με το έγγραφο του Chandrakasan και του μεταπτυχιακού φοιτητή Yogesh K. Ramdass.

Βέβαια, ένα μειονέκτημα για την τροποποίηση ενός σκώρου ή για τα έντομα Cyborg, σε σύγκριση με τα πραγματικά ρομπότ, ήταν το απαγορευτικό κόστος και η χρονοβόρα διαδικασία, πόσο μάλλον με δεδομένο ότι έχουν περιορισμένη διάρκεια ζωής. Τα κύρια όμως πλεονεκτήματα είναι ότι έχουν έτοιμες πλατφόρμες, αποφεύγοντας την ανάγκη κατασκευής πολλών μικρών τεμαχίων και χρησιμοποιούν λιγότερη ενέργεια από τα συγκρίσιμα ρομπότ. **Επίσης ένα μεγάλο πλεονέκτημα – στόχος, είναι ότι ο cyborg εντόμων θα μπορεί να ξεπεράσει εμπόδια μόνο του**.

Τέλος ακόμη και αν το HI-MEMS δεν παράγει ποτέ ένα λειτουργικό cyborg σκώρο ή έντομο, ο καθηγητής Chandrakasan υποστήριζε ότι η χρησιμότητα των επιμέρους συσκευών αυτού του προγράμματος, δεν περιορίζεται στο συγκεκριμένο έργο του DARPA. Θα μπορούν να επαναχρησιμοποιηθούν για βοηθητικές τεχνολογίες και εμφυτεύσιμες συσκευές. Συγκεκριμένα για παράδειγμα, το σύστημα συγκομιδής ενέργειας θα είναι μια πολλά υποσχόμενη τεχνολογία για τα προσθετικά όπλα, τα οποία παρουσιάζουν παρόμοιο πρόβλημα με το βάρος και την εξοικονόμηση ενέργειας, με τον περιορισμό της διάρκειας ζωής μιας μπαταρίας.

5.3.4 Προσπάθεια Εφαρμογής Χειρισμού σε Σκαθάρι

Παρόμοια προσπάθεια επηρεασμού συμπεριφοράς εντόμου (για το σκαθάρι λουλουδιών), πραγματοποιήθηκε και από το Πανεπιστήμιο της Καλιφόρνιας [79], με χρηματοδότηση πάλι από την DARPA, την υπηρεσία της Αμερικής, όπου παρουσιάστηκε και αυτή τον Ιανουάριο του 2009 (αρχικοί σκοποί ήταν η επιτήρηση ή συλλογή πληροφοριών σε αποστολές έρευνας και διάσωσης).

Το επιδιωκόμενο αποτέλεσμα ήταν η διαδρομή πτήσης του εντόμου (τεράστιο σκαθάρι λουλουδιών), να ελέγχεται ασύρματα μέσω ενός νευρικού εμφυτεύματος, με ηλεκτρόδια και ραδιοφωνικό δέκτη στην πλάτη του. Οι επιστήμονες του Πανεπιστημίου της Καλιφόρνιας ανέπτυξαν μια μικροσκοπική εξέδρα που λαμβάνει τα σήματα ελέγχου από έναν υπολογιστή. Τα ηλεκτρικά σήματα τα οποία διανέμονται μέσω των ηλεκτροδίων καθορίζουν στο σκαθάρι να απογειωθεί, να στρίψει αριστερά ή δεξιά ή να αιωρείται στην μέση. Στην εικόνα 13 φαίνονται μερικοί τύποι σκαθαριών από το υπόψη πρόγραμμα της DARPA, με ενσωματωμένα κάποια συστήματα για τον χειρισμό τους.

Εικόνα 13 Τα Cyborg Σκαθάρια από το Πρόγραμμα DARPA

Τα σκαθάρια έχουν ορισμένα πλεονεκτήματα. Το μέγεθός τους κυμαίνεται από τέσσερα έως δέκα γραμμάρια (4-10 gr) και έχει μήκος τέσσερα έως οκτώ εκατοστά (4-8 cm). Αυτό σημαίνει ότι μπορεί να μεταφέρει σχετικά μεγάλα ωφέλιμα φορτία. Για να χρησιμοποιηθεί για αποστολές έρευνας και διάσωσης, για παράδειγμα, το έντομο θα πρέπει να φέρει μια μικρή κάμερα και αισθητήρα θερμότητας.

Επιπλέον, η πτήση του μπορεί να ελεγχθεί σχετικά απλά. Ένα ενιαίο σήμα που αποστέλλεται στους μυς των πτερύγων ενεργοποιεί τη δράση και το σκαθάρι φροντίζει τα υπόλοιπα. «Αυτό επιτρέπει την κανονική λειτουργία για τον έλεγχο της πτύχωσης των φτερών», υποστήριξε ο καθηγητής Jay D. Keasling [80], ο οποίος δεν συμμετείχε στην έρευνα των σκαθαριών αλλά συνεργάζεται με τον καθηγητή Michael M. Maharbiz [81], και οι δύο στο Πανεπιστήμιο της Καλιφόρνιας, Berkeley (ο μεν πρώτος Χημικός Μηχανικός και Βιομηχανικής και ο δεύτερος αναπληρωτής Διευθυντής Εργαστηρίου Βιοεπιστημών στο Εθνικό Εργαστήριο Lawrence Berkeley, με ειδίκευση στη συνθετική βιολογία και ειδικότερα στον τομέα της μεταβολικής μηχανικής).

Η ελάχιστη σηματοδότηση διατηρεί την μπαταρία, επεκτείνοντας τη διάρκεια ζωής του εμφυτεύματος. Οι σκώροι, από την άλλη πλευρά, απαιτούν ένα ρεύμα ηλεκτρικών σημάτων για να κρατήσουν πτήσεις. Η έρευνα έχει οδηγήσει σε μεγάλο βαθμό στην πρόοδο της βιομηχανίας μικροηλεκτρονικής, με τη μικρογράφηση μικροεπεξεργαστών και μπαταριών.

Τα σκαθάρια και τα άλλα ιπτάμενα έντομα είναι κύριοι του ελέγχου πτήσης, ενσωματώνοντας την αισθητηριακή ανατροφοδότηση από το οπτικό σύστημα και άλλες αισθήσεις για να περιηγηθούν και να διατηρήσουν σταθερή πτήση, με χρήση όλο και λιγότερης ενέργειας. Έτσι ο καθηγητής Michel Maharbiz και οι συνεργάτες του, αντί να προσπαθήσουν να επαναδημιουργήσουν αυτά τα συστήματα από το μηδέν, επιδίωξαν να επωφεληθούν από τις φυσικές ικανότητες των σκαθαριών, συνδυάζοντας έντομα και μηχανήματα. Η ομάδα του είχε δημιουργήσει προηγουμένως cyborg σκαθάρια, συμπεριλαμβανομένων εκείνων που έχουν εμφυτευτεί με ηλεκτρονικά εξαρτήματα ως νύμφη χρυσαλίδα. Αλλά η τρέχουσα έρευνα, που παρουσιάστηκε στο IEEE MEMS στην Ιταλία, είναι η πρώτη επίδειξη ενός ασύρματου συστήματος σκαθαριών.

5.3.5 Λοιπές Προσπάθειες Εφαρμογής Χειρισμού σε διάφορα έντομα

Στο πρόγραμμα με τα cybernetic έντομα χρησιμοποίησαν μεγαλύτερους οργανισμούς, όπως τα σκαθάρια και οι ακρίδες, ώστε να μπορούν να ανυψώσουν σχετικά μεγάλα ηλεκτρονικά συστήματα, βάρους μέχρι 1,3 γραμμάρια. Αυτά όμως δεν περιλάμβαναν συστήματα πλοήγησης και απαιτούμενες ασύρματες εντολές για την καθοδήγηση της πτήσης. Οι επιστήμονες τότε επιχείρησαν δύο προσεγγίσεις:

α. Να καταβροχθίζουν αισθητηριακές εισροές για να ενεργοποιούν τις συμπεριφορές πτήσης και να διεγείρουν τους νευρώνες και τους μυς που ελέγχουν τα φτερά. Η μια πρόκληση αφορούσε την πλαστογράφηση των αισθητηριακών εισροών, καθώς τα έντομα συχνά προσαρμόζονται και μαθαίνουν να αγνοούν αυτές τις πληροφορίες που δεν συνάδουν με άλλες αισθήσεις τους. Η άλλη πρόκληση αφορούσε την άμεση χρησιμοποίηση των πτερυγίων και ότι υποβαθμίζεται ο εγγενώς νευρομυϊκός έλεγχος του εντόμου, που απαιτείται για σταθερή πτήση.

β. Στην δεύτερη προσέγγιση τα συστήματα αυτά χρησιμοποίησαν ηλεκτρική διέγερση, η οποία όμως είναι ασαφής και ενεργοποιεί αδιακρίτως όλους τους νευρώνες ή τους μυς κοντά στα ηλεκτρόδια, με αποτέλεσμα να είναι δυσχερής ο καθεαυτού έλεγχος πτήσης.

Η συγκεκριμένη προσπάθεια θέλει αρκετό χρονικό διάστημα για υλοποίηση μέχρι να μπορέσουν να οικοδομήσουν ένα «ρομποτικό έντομο», που θα είναι κοντά στο ικανό ή ευπροσάρμοστο ως πραγματικό. Για το λόγο αυτό, βασίζονται σε μια προσέγγιση στον κυβερνοχώρο για να χρησιμοποιηθούν πραγματικά έντομα για ένα επιτυχές αποτέλεσμα. Τα τελευταία χρόνια, οι ερευνητές κατάφεραν να κατευθύνουν μεγάλα έντομα χρησιμοποιώντας ηλεκτρικά εμφυτεύματα, όμως αποτελεί ένα είδος μεθόδου ωμής βίας με περιορισμένη χρησιμότητα στην πραγματικότητα.

5.3.6 Προσπάθεια Εφαρμογής Χειρισμού σε Λιβελούλα (Ανισόπτερο)/Dragonfly

Τέλος η πιο σύγχρονη έκδοση αντίστοιχου προγράμματος καθοδήγησης και πλοήγησης εντόμων, αποτελεί η λιβελούλα, γνωστή και ως «ελικοπτεράκι»/ Dragonfly. Οι μηχανικοί της εταιρίας Έρευνας και Ανάπτυξης (Research & Development – R&D) DRAPER Company της Αμερικής [82], που εδρεύει στο Cambridge της Μασαχουσέτης, ελπίζουν να ξεπεράσουν τους

παραπάνω περιορισμούς, δημιουργώντας μια «κυβερνητική» λιβελούλα, που συνδυάζει τη μικρογραφία, τη συνθετική βιολογία και τη νευροτεχνολογία. Στην εικόνα 14 βλέπεται την λιβελούλα (Dragonfly) στην φυσική της μορφή.

Η εταιρεία DRAPER ιδρύθηκε το 1932 από τον Charles Stark Draper και συνεργάζεται στενά με την ακαδημαϊκή κοινότητα και την βιομηχανία στην Αμερική για τον εντοπισμό νέων ανακαλύψεων και τεχνολογιών.

Εικόνα 14 Η Λιβελούλα στην Φύση

Οι λιβελούλες έχουν κατοικήσει τη Γη για περισσότερα από 300 εκατομμύρια χρόνια, ενώ οι επιστήμονες το κατατάσσουν ως το πιο γρήγορο έντομο στον πλανήτη [83]. Στο τότε παρελθόν όμως ήταν πολύ μεγαλύτερες, με ένα άνοιγμα φτερών έως 68 εκατοστά και μήκος περίπου 90 εκατοστά. Η ζωή τους διαρκεί από 1-4 χρόνια, ανάλογα με το είδος, αλλά τον περισσότερο χρόνο τον περνούν ως «προνύμφες» κάτω από το νερό, ενώ φτερά έχουν μόνο τους τελευταίους 1-2 μήνες της ζωής τους [84], [85]. Το πλεονέκτημα είναι ότι αναπαράγονται όλο τον χρόνο, απλά απαιτούν γλυκό νερό και ορισμένα είδη αναπτύσσονται σε 6-8 βδομάδες, με την βοήθεια έντονης υγρασίας. Επειδή όμως ζούνε μόνο σε καθαρό περιβάλλον και τρώνε κυρίως κουνούπια, μα και αράχνες, τερμίτες, κ.ά, αποτελούν και δείκτη καθαρότητας μιας περιοχής.

Σε αντίθεση με άλλα ιπτάμενα ζώα, που μπορούν να πετάξουν μόνο σε μία κατεύθυνση, κάθε λιβελούλα μπορεί να αιωρείται στον αέρα, να πετάει στο πλάι και ακόμη και προς τα πίσω.. Αυτό συμβαίνει επειδή καθένα από τα δύο ζεύγη φτερών της λιβελλούλης μπορεί να ελεγχθεί ανεξάρτητα. Αυτή η ικανότητα τους επιτρέπει να ελέγχουν και να αλλάζουν τη γωνία των φτερών τους ξεχωριστά για να κάνουν αδύνατους ελιγμούς, ενώ και τα μάτια τους μπορούν να δουν σε γωνία 360 μοιρών.

Συνολικά, η ικανότητα πτήσης της dragonfly είναι εντυπωσιακή και κάνει πολλούς επιστήμονες να προσπαθούν να αναπτύξουν ρομπότ και αεροπλάνα που να της μοιάζουν. Οι εδαφικές διαμάχες είναι συχνές και κυνηγούν τους εισβολείς σε υψηλές ταχύτητες για μεγάλες αποστάσεις, ενώ συχνά τους χτυπούν μέσα στον αέρα.

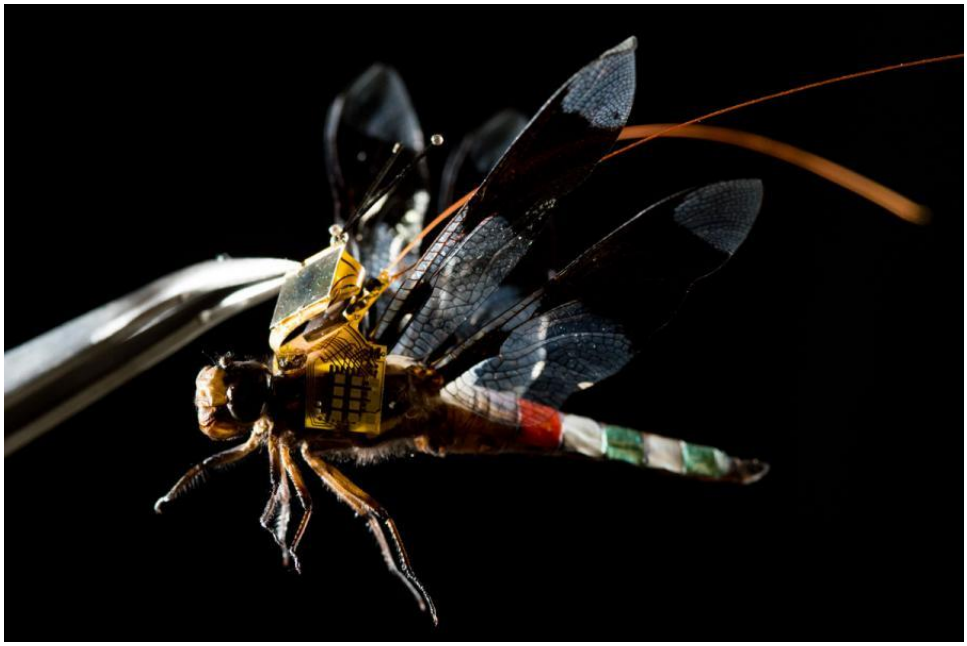
Παρατηρήθηκε ότι η λιβελλούλα στους επιθετικούς ελιγμούς παίρνει θέση έτσι ώστε να εμφανίζεται πάντα στην ίδια περιοχή του αμφιβληστροειδούς του αντιπάλου της. Στον αντίπαλο, αυτό σημαίνει ότι ο επιτιθέμενος θα εμφανίζεται ακίνητος ακόμα και όταν πλησιάζει. Ο ακριβής τρόπος με τον οποίο ο «ιπτάμενος θηρευτής» υπολογίζει τις απαραίτητες κινήσεις και ρυθμίζει την πτήση του, χρησιμοποιώντας την δημιουργία μιας «οπτικής ψευδαίσθησης» στον αντίπαλο (η

ολίσθηση στο πλάι, η αλλαγή πορείας σε χιλιοστά του δευτερολέπτου κ.ά.), παραμένουν ένα μυστήριο.

Για να κατευθύνουν τις λιβελούλες, οι μηχανικοί αναπτύσσουν έναν τρόπο γενετικής τροποποίησης του νευρικού συστήματος των εντόμων [86], ώστε να μπορούν να ανταποκριθούν σε παλμούς φωτός. Μόλις αυτοί επιτύχουν τον σκοπό τους, ενέργεια γνωστή ως οπτογενετική διέγερση, θα μπορούσε να επιτρέψει στις λιβελούλες να μεταφέρουν ωφέλιμες επιβαρύνσεις, να πραγματοποιήσουν επιτήρηση ή ακόμα και να βοηθήσουν τις μέλισσες, τις οποίες χρησιμοποιούν παράλληλα στο υπόψη πρόγραμμα, για να γίνουν καλύτεροι επικονιαστές .

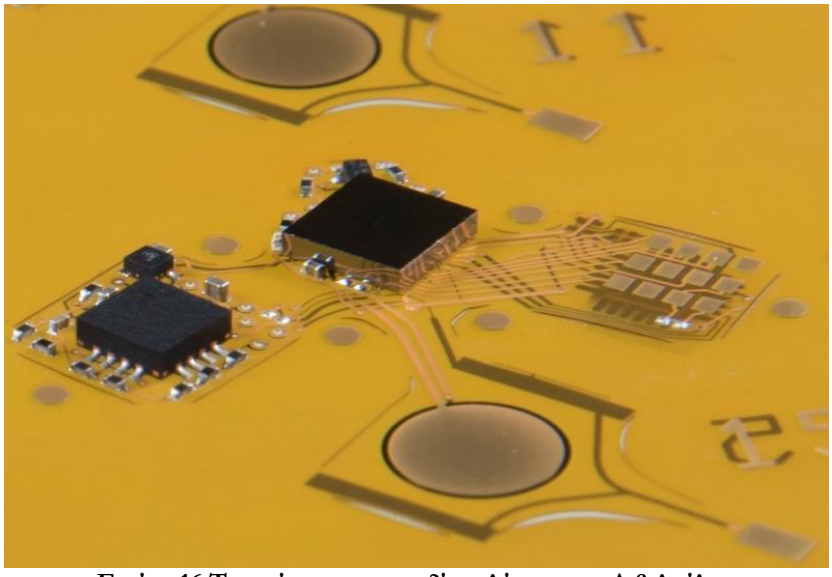
Στο υπόψη σχέδιο, που ονομάζεται DragonflEye, υπάρχει συνεργασία μεταξύ της εταιρείας DRAPER και του Ιατρικού Ινστιτούτου Howard Hughes (HH Medical Institute – HHMI) στο Meryland της Αμερικής και στο Janelia Farm. Υπάρχουν διάφορες μοναδικές τεχνολογίες που έχουν εφαρμοστεί, όπως παρακάτω:

α. Η ομάδα συσκεύασε όλα τα ηλεκτρονικά σε ένα μικρό «σακίδιο» ηλεκτρονικού ελέγχου εντόμων κατάλληλου μεγέθους, με μια συστοιχία αισθητήρων [87], όπου μέσω μιας νευρωνικής δικτύωσης, ελέγχουν την πτήση (εικόνα 15). Το γεγονός αυτό σημαίνει ότι τα μικρά έντομα (όπως οι μέλισσες και οι λιβελούλες σε αντίθεση με τα μεγάλα σκαθάρια) μπορούν να πετάξουν ενώ το φοράνε.



Εικόνα 15 Το σακίδιο με οπτρόδεση στο οπτικό νεύρο της Λιβελούλας

β. Στο «σακίδιο» ορισμένες από τις μειώσεις μεγέθους προέρχονται από τη χρήση ηλιακών συλλεκτών φόρτισης μιας «κυψέλης» για τη συγκομιδή ενέργειας με ενσωματωμένο σύστημα, ελαχιστοποιώντας έτσι την ανάγκη για μπαταρίες. Στην εικόνα 16 είναι τα απάρτια του υπόψη «σακιδίου», πριν την τοποθέτησή τους στο έντομο λιβελούλα.



Εικόνα 16 Τα απάρτια του σακιδίου ελέγχου της Λιβελούλας

γ. Υπάρχουν επίσης ολοκληρωμένα συστήματα καθοδήγησης και πλοήγησης, έτσι ώστε να είναι δυνατή μια πλήρως αυτόνομη πλοήγηση έξω από ένα ελεγχόμενο περιβάλλον.

δ. Τέλος μια άλλη σημαντική πρόοδος είναι ότι αντί να χρησιμοποιούνται ηλεκτρόδια για την ώθηση των μυών ενός εντόμου να κάνει αυτό που επιδιώκουμε, οι μηχανικοί της εταιρείας ακολούθησαν μια πιο λεπτή προσέγγιση, με χρήση των αποκαλούμενων οπτροδίων (optrodes) [88], για ενεργοποίηση μέσω φωτός ενός ειδικού τύπου νευρώνα «διεύθυνσης» με ελαφρούς παλμούς [89]. Αυτοί οι νευρώνες διεύθυνσης λειτουργούν ως γέφυρα μεταξύ των αισθητήρων του dragonfly και των μυών του, πράγμα που σημαίνει ότι η πρόσβαση σε αυτές παρέχει μια πολύ πιο αξιόπιστη μορφή ελέγχου για το πώς κινείται το έντομο.

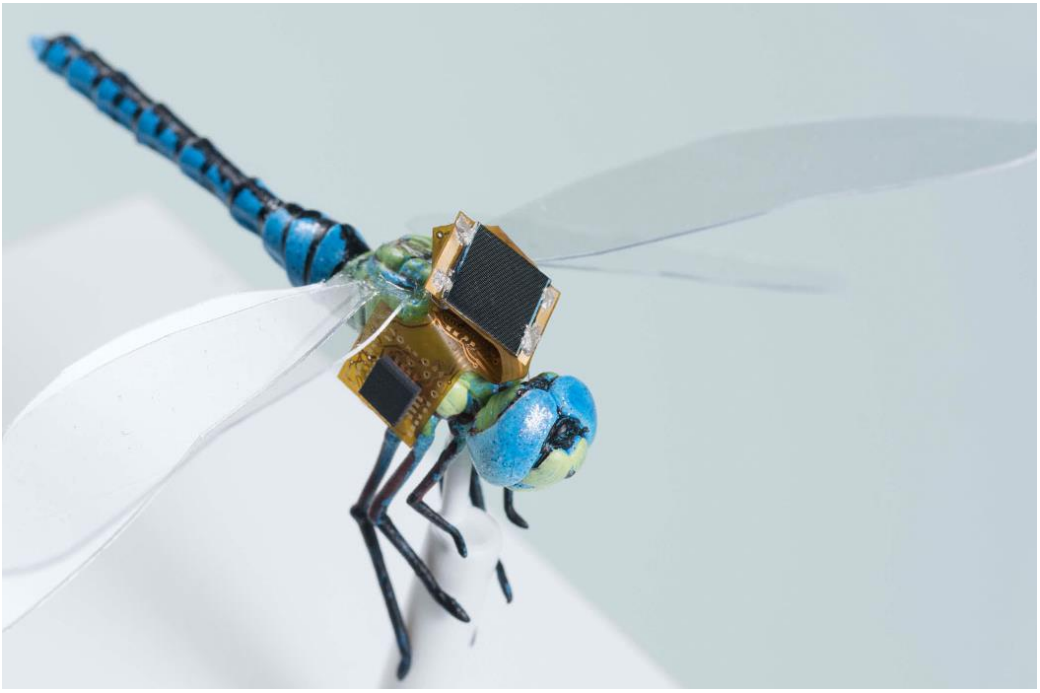
5.3.7 Πρόγραμμα DragonflEye (Λιβελούλα / Ανισόπτερο)

Σε μια προσπάθεια εύρεσης περισσότερων λεπτομερειών για το πρόγραμμα, στις δηλώσεις του Jesse J. Wheeler, ανώτερου βιοϊατρικού μηχανικού και κύριο ερευνητή στο υπόψη πρόγραμμα [90], αναφέρονται τα παρακάτω:

α. Η προσέγγισή της εταιρείας DRAPER για την χρήση εντόμων ήταν διαφορετική, με δεδομένο ότι οι χρησιμοποιούμενες λιβελούλες, είναι μικρότερες και πιο ευκίνητες. Το «σακίδιο» DragonflEye, που αναφέρθηκε παραπάνω, είχε σχεδιαστεί για αυτόνομη πλοήγηση χωρίς ασύρματο χειρισμό, με ενέργεια συγκομιδής από το περιβάλλον και για εκτεταμένη λειτουργία (καθώς έχει κατάλληλα μικρό βάρος για μικρότερα έντομα).

β. Η έρευνα από τον Anthony Leonardo, επικεφαλή της ομάδας Janelia Research Campus, μελέτησε τον τρόπο με τον οποίο ειδικοί νευρώνες «διευθύνουν» την κατεύθυνση πτήσης ελέγχου του εντόμου. Αυτοί αποτελούν έναν τύπο interneuron, ο οποίος δεν είναι ούτε αισθητηριακός ούτε κινητικός. Αυτά πιστεύεται ότι παρέχουν εντολές διεύθυνσης στα νευρομυϊκά κυκλώματα, με συντονισμό στον έλεγχο των μυών πτερυγίων και έτσι διατηρούν σταθερή πτήση. Αυτοί δύναται να ενεργοποιούνται με ακρίβεια, χωρίς άλλη ενεργοποίηση των κοντινών νευρώνων και μυών μέσω οπτογονιδιακής διέγερσης. Αυτή η προσέγγιση επιτρέπει να ενεργοποιούνται οι μεμονωμένοι νευρώνες με το φως, το οποίο δεν μπορεί να γίνει με ηλεκτρισμό.

γ. Επίσης για την χρήση διεπαφών με τους νευρώνες, χρησιμοποιήθηκαν από την εταιρεία DRAPER, τα αποκαλούμενα «οπτρόδια», τα οποία όπως και τα ηλεκτρόδια (που δημιουργούν ηλεκτρική διασύνδεση σε νευρώνες) δημιουργούν οπτική διεπαφή, επιτρέποντας από την μια την παράδοση φωτός στους νευρώνες για διέγερση, και από την άλλη την σύλληψη του εκπεμπόμενου φωτός από τους νευρώνες για την παρακολούθηση της δραστηριότητας. Για παράδειγμα ενώ οι νευρώνες του αμφιβληστροειδούς ενεργοποιούνται φυσικά από το φως, και επιτρέπει στον άνθρωπο να βλέπει, οι νευρώνες στο υπόλοιπο σώμα δεν είναι φυσικά ευαίσθητοι στο φως. Έτσι με την εισαγωγή γενετικού υλικού για κωδικοποίηση ειδικών φωτοευαίσθητων πρωτεϊνών (ονομάζονται opsins), οι νευρώνες μπορούν να τροποποιηθούν για ενεργοποίηση ή ακόμα και αναστολή από διαφορετικά χρώματα του φωτός. Επιπλέον, μπορεί να εισαχθεί γενετικό υλικό που προκαλεί νευρώνες να εκπέμπουν φως όταν είναι ενεργοί. Στην παρακάτω εικόνα 17, είναι μια λιβελούλα με τον ηλεκτρονικό της εξοπλισμό, από την φάση των πειραματικών ελέγχων, ενώ στην εικόνα 18 δίνεται μια σύγκριση μεγέθους της με ένα ανθρώπινο χέρι.



Εικόνα 17 Η πειραματική Λιβελούλα με τον ηλεκτρονικό εξοπλισμό

Εικόνα 18 Η Λιβελούλα σε σύγκριση με ένα ανθρώπινο χέρι

δ. Αυτά τα νέα εργαλεία (optogenetic) επιτρέπουν στα οπτρόδια να παρακολουθούν ή και να διεγείρουν τους νευρώνες με πιο συγκεκριμένη εξειδίκευση από ότι με τα ηλεκτρόδια. Ένας ακόμη λόγος για χρήση αυτής της βελτιωμένης ειδικότητας, είναι ότι τα ηλεκτρικά πεδία αλληλεπιδρούν με όλους τους νευρώνες κοντά στο ηλεκτρόδιο, ενώ το φως θα αλληλεπιδράσει μόνο με τροποποιημένους γενετικά νευρώνες. Επιπλέον, ενώ τα ηλεκτρικά πεδία είναι καλά στην ενεργοποίηση των νευρώνων, είναι πιο δύσκολο να τα εμποδίσουμε. Αντίθετα, διάφοροι τύποι των opsins μπορούν να χρησιμοποιηθούν για να ενεργοποιήσουν και να αναστείλουν τους νευρώνες απλά αλλάζοντας το χρώμα του φωτός που διέρχεται μέσω του «οπτρόδιου».

ε. Για το θέμα του «σακιδίου» που κατασκεύασε η εταιρεία, στο σύστημα πρώτης γενιάς για την ανάπτυξη οδηγιών προς τα έντομα με τη χρήση οπτογενετικής διέγερσης, αυτό είχε σχεδιαστεί με σκοπό:

(1) Την αυτόνομη πλοήγηση,

(2) Την συλλογή ηλιακής ενέργειας σε εκτεταμένη λειτουργία,

(3) Την παράδοση ελαφρών παλμών μέσω optrodes για τον έλεγχο των νευρώνων διεύθυνσης και

(4) Την ασύρματη μετάδοση δεδομένων σε εξωτερικό σταθμό βάσης.

Στα επόμενα βήματα επιδιώχτηκε περαιτέρω μείωση του μεγέθους και του βάρους του συστήματος DragonflEye, με την ανάπτυξη ενός προσαρμοσμένου ολοκληρωμένου συστήματος σε (micro-) τσιπ. Ο στόχος είναι περαιτέρω μείωση των παραπάνω (σε μορφή μινιατούρας), ώστε να μειωθεί το φορτίο ωφέλιμου φορτίου και να επιτραπεί η χρήση του συστήματος και από ακόμη μικρότερα έντομα.

στ. Σε αυτή την περίπτωση οι λιβελούλες (εικόνα 19) είναι πολύ ενδιαφέρουσες, επειδή βρίσκονται σε όλο τον κόσμο και είναι πολύ εύρωστες και ευκίνητες για το μικρό τους μέγεθος. Οι κοινές λιβελούλες ζυγίζουν περίπου 600 χιλιοστόγραμμα (0,6 γραμ.) και μπορούν να αναπτύξουν ταχύτητες έως 97 χλμ/ώρα και να φτάσουν επιταχύνσεις έως και 88 m/sec^2. Τα μηχανικά πετούμενα συγκρίσιμου μεγέθους είναι πολύ λιγότερο αποτελεσματικά στην μετακίνηση, τη σταθεροποίηση της πτήσης και την αποθήκευση ενέργειας.

Εικόνα 19 Η Λιβελούλα πριν το πείραμα του Εργαστηρίου

ζ. Έχει αναφερθεί αποδεδειγμένα το γεγονός ότι μπορούν να μεταναστεύουν σε εντυπωσιακά μεγάλες αποστάσεις, καθώς έχουν παρατηρηθεί να διασχίζουν τον Ινδικό ωκεανό από την Ασία στην Αφρική [91]. Αυτό το κάνουν ετησίως, φεύγοντας από ξηρό μέρος για ένα πιο υγρό, έχοντας τη δυνατότητα να μην κάνουν στάσεις για μεγάλες αποστάσεις, είτε να βρεθούν σε απομονωμένα νησιά στο μέσο των ωκεανών, όπου μπορούν και να ζευγαρώσουν, να εναποθέσουν τα αυγά τους και οι νεογέννητες λιβελούλες να ακολουθήσουν τους γονείς τους. Έτσι ταξιδεύουν περίπου 14.000 έως 18.000 χιλιόμετρα για να πάνε στον προορισμό τους και να επιστρέψουν.

5.3.8 Αποτελέσματα Προγράμματος DragonflEye (Λιβελούλα/ Ανισόπτερο)

Η παραπάνω αναποτελεσματικότητα, όσον αφορά την ενέργεια, δημιουργεί μια θεμελιώδη πρόκληση: Οι μηχανικοί πτητικοί μηχανισμοί μπορούν να μεταφέρουν μόνο πολύ μικρές πηγές ενέργειας, πράγμα που σημαίνει ότι έχουν αρκετή ισχύ για να πετούν μόνο για πολύ σύντομες χρονικές περιόδους. Το σύστημα DragonflEye δεν απαιτεί πηγή ενέργειας για πτήση, μόνο για πλοήγηση. Μπορεί να λειτουργήσει επ' αόριστον εξαιτίας της ικανότητας του εντόμου να αναπληρώνει την ενέργεια από τα τρόφιμα και την ικανότητα του συστήματος πλοήγησης να συλλέγει ενέργεια από το περιβάλλον.

Στο πρόγραμμα DragonflEye προσφέρεται μια νέα μικροσκοπική τεχνολογία για να εξοπλίσει ένα ευρύ φάσμα εντόμων ίσως και με περιβαλλοντικούς αισθητήρες και ενδεχομένως να καθοδηγήσει σημαντικές περιβαλλοντικές συμπεριφορές, όπως η επικονίαση.

Προκειμένου να ξεκινήσει η καθοδήγηση των λιβελούλων, χρειάστηκε να αναπτυχθούν αρκετές βασικές τεχνολογίες. Το Ιατρικό Ινστιτούτο Howard Hughes (HHMI) επικεντρώθηκε στην ανάπτυξη μεθόδων χορήγησης γονιδίων ειδικά για την λιβελούλα, για να κάνουν ευαίσθητους στο φως τους ειδικούς νευρώνες διεύθυνσης.

Η εταιρεία DRAPER ανέπτυξε το μικροσκοπικό «σακίδιο» για αυτόνομη πλοήγηση και το ευέλικτο «οπτρόδιο» (optrode) για τον έλεγχο των τροποποιημένων νευρώνων κατευθύνοντας το φως γύρω από το μικροσκοπικό νεύρο της λιβελούλας. Στο τέλος θα ξεκινήσει μια έρευνα για εφαρμογή στην παρακολούθηση θέσης, τον έλεγχο πτήσης και τη βελτιστοποιημένη οπτική διέγερση του εντόμου.

Η παρακολούθηση εντόμων (αλλά και μικρών ζώων), θα επιτρέψει στους ερευνητές να κατανοήσουν καλύτερα τη συμπεριφορά τους στο φυσικό περιβάλλον και να παρακολουθήσουν την επίδραση των περιβαλλοντικών αλλαγών. Επίσης σημαντικό είναι να βοηθήσουν και στην καθοδήγηση πολιτικών αποφάσεων, τόσο για την προστασία σημαντικών οικοσυστημάτων, όσο και για τυχόν δυνατότητα χρήσης των εντόμων αυτών για περαιτέρω ενέργειες.

Ένα παράδειγμα αποτελούν οι μέλισσες, των οποίων ο πληθυσμός έχει μειωθεί κατά το ήμισυ τα τελευταία 25 χρόνια. Η χρήση της βιοϊατρικής τεχνολογίας της εταιρείας DRAPER, θα μπορούσε να βοηθήσει την αναχαίτιση της απώλειας αυτών των επικονιαστών, παρακολουθώντας τη διαβίωσή τους με σκοπό να αυξήσει την επιβιωσιμότητά τους. Αυτό θα βοηθούσε κατά ένα μέρος την οικονομία, καθόσον για παράδειγμα από μελέτη των Η.Π.Α. Διαπιστώθηκε ότι συνεισφέρουν περισσότερα από 15 δισεκατομμύρια δολάρια στην αξία της γεωργίας.

5.4 Χρήση της Λιβελούλας ως ΜΕΑ, επικοινωνία– παρεμβολές

α. Στην προσπάθεια τώρα χρήσης της λιβελούλας ως ΜΕΑ (drone), αυτό θα αποτελούσε ένα ιδιαίτερο αντικείμενο σύνδεσης με την παρούσα εργασία.

Έχοντας παραθέσει ένα μικρό μέρος από την ακαδημαϊκή έρευνα όσον αφορά την ικανότητα χειρισμού των υπόψη εντόμων, σε συνδυασμό με την ολοκλήρωση αυτού και την επέκταση του προγράμματος, σε μια πιο προχωρημένη εφαρμογή, θα μπορούσε να υποστηριχτεί μια έρευνα και για την χρησιμοποίηση σμήνους από λιβελούλες για χρήση με διάφορους σκοπούς:

(1) Την χρήση σμήνους τέτοιων εντόμων, για πολλαπλότητα αποτελεσμάτων, ανάλογα με την «αποστολή» τους (αναζήτηση σε έρευνα/διάσωση, είτε παρακολούθηση σε κατασκοπεία κ.ά.).

(2) Να αποσταλούν σε ιδιαίτερα μεμακρυσμένες αποστάσεις και με τον τηλεχειρισμό τους μέσω δορυφόρων, να χρησιμοποιηθούν για τους ίδιους παραπάνω λόγους.

(3) Την αμυντική χρήση του σμήνους από λιβελούλες, για την αντιμετώπιση ενός «ανεπιθύμητου» ΜΕΑ σε μια ευαίσθητη περιοχή (αεροδρόμια, στρατιωτικές/ κυβερνητικές/ιδιωτικές εγκαταστάσεις, κ.ά.). Σε αυτήν την περίπτωση ένα επιθυμητό αποτέλεσμα θα μπορούσε να είναι, είτε η παρεμβολή του drone, είτε η κατάρριψή του.

β. Για την εφαρμογή των παραπάνω και την χρήση της λιβελούλας σε σμήνος, την εξασφάλιση των επικοινωνιών μεταξύ τους και την προστασία από τυχόν παρεμβολές, θα ήταν αναγκαίο:

(1) Να διατυπωθεί η δυνατότητα χρήσης τους είτε μεμονωμένα είτε σε σμήνη, με τους τρόπους επικοινωνίας και τα πρωτόκολλα, που αναφέρθηκαν στο 3ο Κεφάλαιο της παρούσας εργασίας, κυρίως για τα Ad-hoc δίκτυα.

(2) Να χρησιμοποιηθούν τρόποι ασφαλούς πτήσης και αποφυγής παρεμβολής, με δυνατότητες αναγνώρισης και εφαρμογών, όπως αυτές περιγράφονται στο 4ο Κεφάλαιο του παρόντος .

γ. Υπάρχει βέβαια μια παράμετρος που αρκεί απλά να αναφερθεί, καθόσον από όλη την έως τώρα έρευνα για την εργασία, δεν τέθηκε ως πρόβλημα από την εταιρεία. Αυτό είναι η διάρκεια ζωής της λιβελούλας ως έντομο [84], [90] διότι τον περισσότερο χρόνο ζούνε ως «προνύμφες», και μόνο τους τελευταίους 1-2 μήνες ενηλικιώνονται και έχουν φτερά. Αυτό όμως δεν αναφέρθηκε ως εμπόδιο, γιατί υπάρχουν και ορισμένα είδη που διατηρούνται λίγο περισσότερο (αντιπροσωπευτικό είναι **το Παγκόσμιο Ανεμόπτερο ή Εξαφριστήρι/Skimmer**), οπότε στην χρήση αυτών θα μπορούσε να επενδυθεί η όλη παραπάνω προσπάθεια, τόσο για τις περιπτώσεις μεμακρυσμένων αποστολών, αλλά και περισσότερο για την ασφάλεια και άμυνα ιδιαίτερων και ευαίσθητων εγκαταστάσεων.

5.4.1 Σενάρια χρήσης της Λιβελούλας

Για τις παραπάνω περιπτώσεις θα παρατεθούν παρακάτω κάποια πιθανά σενάρια για κάθε περίπτωση, με τις λιβελούλες:

Σενάριο «1»: Σε περίπτωση χρήσης των εντόμων αυτών για αναζήτηση και διάσωση σε δύσβατες περιοχές είτε για παρακολούθηση, θα μπορούσε να διατυπωθεί ότι αυτό θα γίνει με κάποια δυνατότητα μεταφοράς εικόνας ή και πιθανότατα και ήχου. Αυτό θα υποβοηθούσε καλύτερα από την μια να αντιληφθούν την κατάσταση οι υπεύθυνοι χειριστές αυτής της έρευνας, είτε από την άλλη, στην κατασκοπεία, να συλλεχθούν οι αναγκαίες πληροφορίες για την συγκρότηση μιας ολοκληρωμένης άποψης για τον επιζητούμενο στόχο ή την κατάσταση. Σε επέκταση της περίπτωσης αυτής η χρήση σμήνους από λιβελούλες, θα ενίσχυε αρκετά, όπως είναι εμφανές, το αποτέλεσμα της κάθε περίπτωσης.

Σενάριο «2»: Για χρήση τώρα σε μεμακρυσμένη απόσταση αναφερόμαστε μόνο σε σμήνος από λιβελούλες και θα είχε πιθανότατα χρήση μόνο για παρακολούθηση ή κατασκοπεία. Όπως αναφέρθηκε υπάρχουν είδη λιβελούλας που μπορούν να ταξιδέψουν ως σμήνος σε χιλιάδες χιλιόμετρα, με την προϋπόθεση ότι λόγω του μέσου όρους της ζωής τους δεν θα μπορούσαν να επιστρέψουν για να επαναχρησιμοποιηθούν. Για τα παραπάνω θα απαιτούνταν βέβαια να επιλυθούν και κάποια άλλα πράγματα, όπως:

α. Ο εξ' αποστάσεως χειρισμός μέσω αναμεταδοτών ή με δορυφορικό σύστημα.

β. Η εξασφάλιση παροχής ενέργειας μέσω του ήλιου ή μέσω των πιεζοηλεκτρικών συστημάτων, συλλέγοντας ενέργεια από τη χρήση των φτερών κατά την διάρκεια της πτήσης. Απλά να αναφέρουμε ότι τα τελευταία έχουν ευρύ φάσμα εφαρμογών, διότι μπορούν να είναι μικρά σε όγκο, έχουν υψηλή ακρίβεια διέγερσης, μικρό χρόνο απόκρισης, απουσία φαινομένων τριβής, λειτουργία σε ακραίες συνθήκες (στο «κενό» ή και σε κρυογονικές θερμοκρασίες) [92], [93].

γ. Η αντιστάθμιση του κόστους «κατασκευής» ενός τέτοιου σμήνους σε συνάρτηση με το επιδιωκόμενο αποτέλεσμα, καθόσον όπως αναφέρθηκε πιθανώς δεν θα είναι δυνατή η επαναχρησιμοποίηση του υλικού/ «σακίδιο» της λιβελούλας.

δ. Η αποστολή στην «βάση» των παρατηρήσεων και δεδομένων που θα ληφθούν από την «αποστολή».

Σενάριο «3»: Η περίπτωση της αμυντικής χρήσης της λιβελούλας, φυσικά μόνο σε σμήνος αυτών, για την ασφάλεια κάποιων ζωτικών ή ευαίσθητων εγκαταστάσεων, αποτελεί έναν χώρο, όπου η χρήση της λιβελούλας θα έβρισκε εξαιρετική απήχηση και εφαρμογή και θα είχε ιδιαίτερη αποτελεσματικότητα. Σε αυτήν την φάση θα αναφέρουμε κάποια απαραίτητα χαρακτηριστικά για την εφαρμογή αυτού:

α. Στο μέρος που αφορά την μαζική αναπαραγωγή τους για κάλυψη των ετήσιων αναγκών, αυτή η προϋπόθεση δύναται να καλυφθεί καθόσον εκκολάπτονται καθ' όλη τη διάρκεια του έτους σε συγκεκριμένο υγρό περιβάλλον.

β. Η ανάπτυξη περαιτέρω του πειραματικού χειρισμού της λιβελούλας, με επέκταση σε ηλεκτρονικό εξοπλισμό για δυνατότητα παρεμβολών, θα μπορούσε να υλοποιηθεί είτε:

(1) Με μόνιμη «πτήση» αυτών για κάλυψη της ασφάλειας,

(2) Τηρώντας πλήρη ετοιμότητα σε περίπτωση εμφάνισης αγνώστου ΜΕΑ (Drone) να εφαρμοστεί η τηλεχειριζόμενη «πτήση» για παρεμβολή **ή κατάρριψή του** (το τελευταίο θα αναπτυχθεί στο επόμενο σενάριο).

Σενάριο «4»: Για την δυνατότητα κατά την ασφάλιση μιας ευαίσθητης περιοχής για προστασία από ΜΕΑ, η περίπτωση της κατάρριψής του με ένα σμήνος από λιβελούλες, θα απαιτούσε μια άλλη, βιολογικού τύπου, προσέγγιση. Στην πράξη η λιβελούλα από τη φύση της είναι ένας από τα πιο καλούς μαχητές/πιλότους στο δικό τους επίπεδο με τα άλλα έντομα. Θα μπορούσαν λοιπόν να υλοποιηθούν τα παρακάτω:

α. Να αντιμετωπίσει ως «εχθρό» το ΜΕΑ και να το αποστείλουμε για την καταστροφή ζωτικών σημείων πτήσης του εχθρικού ΜΕΑ.

β. Να το «αισθανθεί» σαν «τροφή» για να το προσεγγίσει και στην προσπάθειά του για «επικονίαση», να προκαλούσαμε βλάβη στο ΜΕΑ. Μια ακόμα πιο προχωρημένη σκέψη θα ήταν η δυνατότητα δημιουργίας μικρών **«βομβών»** στον εξοπλισμό της λιβελούλας, έτσι ώστε όταν επικαθήσει σε μηχανικά μέρη του ΜΕΑ, να του προκαλούσαμε βλάβη και επομένως μη ικανότητα ομαλής πτήσης και τελικά την κατάρριψή του.

5.5 Συμπεράσματα

Στο Κεφάλαιο αυτό επιχειρήθηκε να αναπτυχθεί μια ιδιαίτερη προσέγγιση για την σχέση της χρήσης των GPS δικτύων στο μέρος που αφορά την παρακολούθηση με τα ΜΕΑ και την εξέταση αντικατάστασης των τελευταίων από έμβια cybernetic έντομα, με κύρια προσέγγιση στην λιβελούλα/ανεμόπτερο (Dragonfly).

Η επί μέρους αυτή μελέτη στηρίχτηκε στην εξέταση, από τον ακαδημαϊκό χώρο, της υπόψη προσπάθειας και στην διαπίστωση ότι η λιβελούλα θα ήταν το μόνο έντομο, το οποίο θα μπορούσε να υλοποιήσει την ιδέα χρήσης τους προς αντικατάσταση μέρους του έργου που πραγματοποιείται τη σημερινή εποχή με τα ΜΕΑ.

Για την επίτευξη βέβαια ενός τόσο αισιόδοξου εγχειρήματος, θα απαιτούνταν τα παρακάτω:

(1) Η υλοποίηση του τηλεχειρισμού της λιβελούλας και η επέκτασή του ακόμα και εξ' αποστάσεως.

(2) Η επιπλέον ανάπτυξη ενός micro-τσιπ για την επικοινωνία του σμήνους μεταξύ τους.

(3) Η ανάπτυξη μιας ιδιαίτερης εφαρμογής, για τον μικρό όγκο του «σακιδίου», που θα αφορούσε (σε περίπτωση παρεμβολής των συστημάτων τηλεχειρισμού) την αυτόματη μετατροπή σε αυτόνομη πλοήγηση σε μεμακρυσμένη απόσταση, και τέλος

(4) Η εξέταση της δυνατότητας, παράλληλα με την ως άνω χρήση τους, για την εξεύρεση τρόπου μετάδοσης των δεδομένων, με ένα συμβατό μέσο επικοινωνίας είτε τυχόν μέσω δορυφορικού συστήματος.

Κεφάλαιο 6

Σύνοψη – Ανοικτά Ζητήματα – Μελλοντικές Προκλήσεις

6.1 Σύνοψη

Για να περιγραφεί καλύτερα ο σκοπός της παρούσας πτυχιακής εργασίας είναι σημαντικό να γίνει μια ανασκόπηση των κεφαλαίων. Αρχικά, επιχειρήθηκε η παρουσίαση και η κατηγοριοποίηση των διαθέσιμων τεχνολογιών, τεχνικών και τακτικών παρεμβολής. Συγκεκριμένα, αναπτύχθηκαν οι κύριοι τύποι παρεμβολέων με έμφαση στην λειτουργία τους. Επιπλέον, κρίθηκε σκόπιμο η εξέταση των παρεμβολέων σε σχέση με την τοποθέτηση τους στο χώρο.

Στο δεύτερο κεφάλαιο, αναλύθηκε το θεωρητικό υπόβαθρο του δεύτερου σκέλους της πτυχιακής εργασίας. Η εργασία επεκτάθηκε στην λειτουργία του GPS και την χρήση του συστήματος από ΜΕΑ για πλοήγηση στο χώρο. Επιπλέον, επισημάνθηκε η ευπάθεια του GPS από διάφορες τεχνικές παρεμβολής και αναλύθηκαν εκτενώς όλες οι απειλές που προκύπτουν από την εξάρτηση των ΜΕΑ από το GPS.

Στο τρίτο κεφάλαιο καταγράφθηκε μια εναλλακτική πηγή που μπορούν να αντλήσουν πληροφορίες γεωδεσίας τα ΜΕΑ. Τα Ιπτάμενα Ad-Hoc ασύρματα δίκτυα χρησιμοποιούνται ευρέως για την διοίκηση και τον έλεγχο ΜΕΑ. Θεωρήθηκε σκόπιμο να εξεταστεί και αυτός ο τρόπος επικοινωνίας λόγω της φύσης του, που είναι ασύρματη. Σύμφωνα με αυτή την συλλογιστική, μια συνολική λύση παρεμβολής των πληροφοριών γεωδεσίας ενός ΜΕΑ, οφείλει να περιλαμβάνει και την παρεμβολή στα Ιπτάμενα Ad-Hoc δίκτυα. Για την κατανόηση των Ιπτάμενων Ad-Hoc δικτύων αναπτύχθηκε η αρχιτεκτονική τους και τα διαθέσιμα πρωτόκολλα επικοινωνίας.

Στο τέταρτο κεφάλαιο η εργασία, επικεντρώθηκε σε μια ενδελεχή ανάλυση της ασφάλειας που υποστηρίζουν τα Ιπτάμενα Ad-Hoc δίκτυα. Επισημάνθηκαν τα ζητήματα ασφαλείας και ο βαθμό ευπάθειας τους σε παρεμβολή. Επιπλέον, καταγράφηκαν ανοικτά ζητήματα που δυνητικά μπορούν να αποτελέσουν πεδίο για την προσβολή των ιπτάμενων Ad-Hoc δικτύων.

Στο πέμπτο και τελευταίο κεφάλαιο, προτάθηκε μια καινοτόμος λύση για την προσβολή των ασύρματων επικοινωνιών των ΜΕΑ. Προτάθηκε με την μέθοδο της βιοιατρικής, η μετατροπή εντόμων και πιο συγκεκριμένα των λιβελούλων σε μεταφορείς εν δυνάμει μικροσκοπικών παρεμβολέων. Οι λιβελούλες θα πρέπει να έλκονται ή να κατευθύνονται στο ΜΕΑ στόχος. Με σκοπό, ανάλογα το μέγεθος, είτε να το παρεμβάλουν, είτε να το καταστρέφουν.

Ο σκοπός της εργασίας ήταν η πρόταση μιας μεθόδου παρεμβολής των πληροφοριών γεωδεσίας των ΜΕΑ και κατ' επέκταση των ασύρματων επικοινωνιών του. Η παρουσίαση έγινε για την δυνατότητα ενός αποτελέσματος συνδυασμού μιας στοιχειοθετημένης συλλογιστικής και της παράθεσης του απαραίτητου θεωρητικού υπόβαθρου που αναπτύχθηκε στα πρώτα κεφάλαια. Επιπρόσθετα, απαντήθηκαν επιμέρους ερωτήματα, όπως, ο βαθμός εξάρτησης των ΜΕΑ από πληροφορίες γεωδεσίας. Επίσης, ότι τα ΜΕΑ αποτελούν συστήματα με εμφανείς ευπάθειες, όσον

αφορά τουλάχιστον τις ασύρματες επικοινωνίες τους. Ως εκ τούτου, δεν θα πρέπει να θεωρούνται ως αποκλειστική λύση, σε περίπτωση κρίσιμων αποστολών ή καταστάσεων.

Τέλος η πρόταση επεκτάθηκε στο τελευταίο κεφάλαιο σε έναν εναλλακτικό τρόπο χρήσης έμβιων εντόμων για την εφαρμογή των παραπάνω, με εστίαση στο έντομο «λιβελούλα», για το οποίο υπάρχει διαρκής προσπάθεια χρησιμοποίησής του, ως υποκατάστατο των MEA, από τμήματα έρευνας και ανάπτυξης, κυρίως της αμερικάνικης υπηρεσίας τέτοιων προγραμμάτων.

6.2 Ανοικτά Ζητήματα – Μελλοντικές Προκλήσεις

Όπως, έχει επισημανθεί στην παρούσα μελέτη η απαίτηση για MEA είναι τεράστια. Αυτό οδηγεί την τεχνολογία τους στο μέλλον με τεράστια άλματα. Οι ασύρματες επικοινωνίες και το GPS ωθούνται και αυτές από τις εξελίξεις. Η ανάπτυξη της τεχνολογίας απαλείφει παλαιότερες ευπάθειες, με αποτέλεσμα οι σημερινές επιτυχείς επιθέσεις, πιθανότατα να μην έχουν αποτέλεσμα στο άμεσο μέλλον.

Ο επιτιθέμενος, την πλευρά του οποίου εξετάσαμε στην παρούσα εργασία, για να διατηρήσει το πλεονέκτημα που διαθέτει, οφείλει να εξελίσσει με τον ίδιο ρυθμό τις επιθέσεις, επιδιώκοντας μεγαλύτερη ακρίβεια και απόδοση. Εκτός από την εξέλιξη, πρέπει να εντοπίζει ευπάθειες και κενά ασφαλείας από τις νέες τεχνολογίες, που αναπτύσσονται. Έχει αποδειχθεί ιστορικά, ότι οι νέες τεχνολογίες, ιδιαίτερα όταν έχουν μεγάλο ρυθμό ανάπτυξης, κυοφορούν νέες ευπάθειες και απειλές. Η περίπτωση των MEA δεν θα αποτελέσει φυσικά εξαίρεση.

Ένα ανοικτό ζήτημα, που οφείλει να εξεταστεί σε επόμενες μελέτες και να συμπληρώσει την παρούσα εργασία, είναι η αξιολόγηση των αδρανειακών συστημάτων πλοήγησης (Inertial Navigation System–INS) [94, 95, 96], τα οποία παρέχουν στον «εγκέφαλό» του, πληροφορίες για την θέση ενός MEA, χωρίς την χρήση ασύρματων επικοινωνιών. Η εξεύρεση των ευπαθειών, των κενών ασφαλείας και τέλος των επιθέσεων σε αυτό το σύστημα, θα είχε σαν αποτέλεσμα την πλήρη προσβολή ενός MEA.

Παραπομπές

[1] Wood A, Stankovic J, Zhou G (2007) DEEJAM:Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. In: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp 60–69

[2] Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp 56–57

[3] Pelechrinis K, Iliofotou M, Krishnamurthy S (2011) Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys Tutorials 13(2):245 –257

[4] Mpitziopoulos A, Gavalas D, Pantziou G,Konstantopoulos C (2007) Defending wireless sensor networks from Jamming attacks. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, pp 1–5

[5]Alnifie G, Simon R (2007) A multi-channel defense against jamming attacks in wireless sensor networks.In: Proceedings of the 3rd ACMWorkshop on QoS and Security for Wireless and Mobile Networks, pp 95–104.

[6] Muraleedharan R, Osadciw LA (2006) Jamming attack detection and countermeasures in wireless sensor network using ant system. In: SPIE the International Society for Optical Engineering, vol 6248, p 62480G.

[7] Lazos L, Liu S, Krunz M (2009) Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In: Proceedings of the 2nd ACM Conference on Wireless Network Security, pp 169–180.

[8] Pelechrinis K, Koutsopoulos I, Broustis I, Krishnamurthy S (2009b) Lightweight jammer localization in wireless networks: System design and implementation. In: IEEE Global Telecommunications Conference, pp 1–6.

[8α] Tague P, Slater D, Poovendran R, Noubir G (2008) Linear programming models for jamming attacks on network traffic flows. 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops pp 207–216.

[8β] Li M, Koutsopoulos I, Poovendran R (2007) Optimal jamming attacks and network defense policies in wireless sensor networks. In: IEEE 26th IEEE International Conference on Computer Communications, pp 1307–1315.

[9] Commander CW, Pardalos PM, Ryabchenko V, Shylo OV, Uryasev S, Zrazhevsky G (2008) Jamming communication networks under complete uncertainty. Optimization Letters 2, pp 53–70.

[9α] Huang H, Ahmed N, Pulluru S (2010) On limited-range strategic/random jamming attacks in wireless ad hoc networks. In: IEEE 34th Conference on Local Computer Networks, pp 1–8.

[9β] Gencer C, Aydogan EK, Celik C (2008) A decision support system for locating VHF/UHF radio jammer systems on the terrain. Information Systems Frontiers 10(1):111–124.

[10] Panyim K, Hayajneh T, Krishnamurthy P, Tipper D (2009) Jamming dust: A low power distributed jammer network. In: 27th Army Science Conference, pp 922–929

[11] D.Majumdar,"Iran's captured RQ-170: How bad is the damage?",Defense News, 9 December 2011

[12] Hui Hu, Kechu Yi , "The study of GPS and GPS jamming technology , " science and technology , vol. 8, pp.4l-44, 2004

[13] A.Dempster, "How Vulnerable is GPS?",Transportation, 2001.

[14] *E.* Ackerman,"Japanese Security Firm to Start Renting Surveillance Drones",IEEE Spectrum, 29 December 2012.

[15] Lele, Ajay and A.Mishra, "Aerial Terrorism and the Threat from Unmanned Aerial Vehicles.", Journal of Defence Studies 3, no. 3, pp.54-65,2009

[16] J. Tisdale, Z. Kim, J. Hedrick, "Autonomous UAV path planning and estimation", IEEE Robotics and Automation Magazine, Volume 16, Issue 2, pp.35–42, 2009.

[17] E.Deligne,"ARDrone corruption.",Journal in Computer Virology pp.1-13, 2012

[18] H.Wen,P.Y.R. Huang, J. Dyer, A. Archinal and J. Fagan. "Countermeasures for GPS signal spoofing.",In ION GNSS, pp. 13-16, 2005.

[19] T.E.Humphreys, M.L.Psiaki and P.M.Kintner,Jr,"GPS Spoofing Threat",2009

[20] D. Hambling, "GPS fail: how a little black box could cause chaos"New Scientist, Volume 209, Issue 2803, pp.44-47,12 March 2011.

[21] J.S.Warner and R.G.Johnston, "GPS spoofing countermeasures.", Homeland Security Journal, 2003.

[22] Iqbal, M.Usman and S.Lim, "Legal and ethical implications of GPS vulnerabilities." J. Int'l Com. L. & Tech. 3 (2008): 178.

[23] S.J.Gustavus, "Symmetric and asymmetric encryption." ACM Computing Surveys (CSUR) 11.4, pp.305-330, 1979

[24] C. Arthur, "SkyGrabber: the $26 software used by insurgents to hack into US drones", Guardian, 17 December 2009

[25] Associated Press, "Computer virus infects drone plane command center in US", Guardian, 9 October 2011

[26] A.Rawnsley, "Iran's Alleged Drone Hack: Tough, but Possible",Wired December 2011

[27] E. Yadereli, C. Gemci, and A. Z. Akta, "A study on cyber-security of autonomous and unmanned vehicles," The Journal of Defense Modeling and Simulation, vol. 12, no. 4, pp. 369–381, 2015

[28] *Projected Direct Economic Impact from the UAV Industry in the United States*, https://www.statista.com/statistics/536486/projecteddirect-economic-impact-from-the-uav-industry-united-states/

[29] L. Gupta, R. Jain, and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1123–1152, 2016

[30] W. Zhao, M. Ammar, and E. Zegura, "Mobility Aware Hybrid Routing Protocol for Mobile Ad hoc Network," in *Proc. ACM MobiHoc*, 2004, pp. 187–198

[31] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1123–1152, 2015

[32] Bekmezci, İ., and Ulku, E, "Location information sharing with multi token circulation in flying Ad Hoc networks," Proceedings of 7th International Conference on Recent Advances in Space Technologies (RAST) Istanbul, Turkey,2015

[33] O. Sahingoz, "Mobile networking with UAVs: Opportunities and challenges," in Unmanned Aircraft Systems (ICUAS), 2013 International Conference on, May 2013, pp. 933–941

[34] R. W. Beard, T. W. Mclain, D. B. Nelson, D. Kingston and D. Johanson, "Decentralized cooperative aerial surveillance using fixed wing miniature UAVs," Proceedings of the IEEE, vol. 94, no. 7, pp. 1306 - 1324, July 2006

[35] E. A Marconato, D. F Pigatto,C. Branco, J. A Maxa, N. Larrieu, et al, "IEEE 802.11n vs. IEEE 802.15.4: A study on communication QOS to provide safe FANETs", 46th annual IEEE/IFIP international conference on dependable systems and networks workshop (DSN-W), june 2016, pp.184-191

[36] W. Zafar and Bilal M. Khan, "Flying ad-hoc networks: Technological and social implications," IEEE Technol. Soc. Mag., vol. 35, no. 2, pp. 67-74, June 2016

[37] Jonson, T., Pezeshki, J., Chao, V., Smith, K., Fazio, J.: Application of Delay Tolerant Networking (DTN) in airborne networks. In: IEEE Military Communications Conference-(MILCOM 2008), pp. 1–7 (2008)

[38] C. Konstantopoulos, D. Gavalas, G. Pantziou, A mobility aware technique for clustering on mobile ad-hoc networks, in: Proceedings of the 8th International Conference on Distributed Computing and Networking, ICDCN'06, Springer-Verlag, Berlin, Heidelberg, 2006, pp. 397–408

[39] P. L. Yang, C. Tian, and Y. Yu, "Analysis on optimizing model for proactive ad hoc routing protocol," in Proc. Military Commun. Conf. (MILCOM), vol. 5, Atlantic City, NJ, USA, pp. 2960-2966, Oct. 2005

[40] Perkins, C.E., Bhagwat, P.: Highly dynamic Destination Sequenced Distance-Vector Routing (DSDV) for mobile computers. In: Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94), pp. 234–244 (1994)

[41] OKSahingoz. "Routing ptocols in flying Ad-hoc networks (FANETs): Concepts and challenges". Journal of Intelligent & Robotic Systems, pp. 513-27.April 2014

[42] A. Zaballos, A. Vallejo, G. Corral and J. Abella, "Ad-Hoc Routing Performance Study Using OPNET Modeler," Barcelona, 2006

[43] A.I. Alshabtat, L. Dong, J. Li, F. Yang, "Low latency routing algorithm for unmanned aerial vehicles ad-hoc networks", International Journal of Electrical and Computer Engineering 6 (1), 2010, pp. 48–54

[44] Habib, S., Saleem, S., & Saqib, K. M., "Review on MANET routing protocols and challenges", IEEE Student Conference on Research and Development SCOReD , pp. 529-533 , 2013

[45] V.R. Khare, F.Z. Wang, S. Wu, Y. Deng, C. Thompson, Ad-hoc network of unmanned aerial vehicle swarms for search & destroy tasks, in: Intelligent Systems, IS, International IEEE Conference, 2008

[46] Z. J. Haas and M. R. Pearlman, "The Zone Routing Protocol (ZRP) for Ad-Hoc Networks," IETF MANET working group, Internet draft, June 1999

[47] Raw, R.S., Lobiyal, D.K. and Das, S. (2012) 'An analytical approach to position-based routing protocol for vehicular ad hoc networks', SNDS'12, Springer (LNCS), IIITM-K, Trivandrum, India, pp.147–156

[48] R. Shirani, M. St-Hilaire, T. Kunz, Y. Zhou, J. Li, L. Lamont, The performance of greedy geographic forwarding in unmanned aeronautical ad-hoc networks, in: Proceedings of the 2011 Ninth Annual Communication Networks and Services Research Conference, CNSR '11, IEEE Computer Society, Washington, DC, USA, 2011, pp. 161–166

[49] L. Lin, Q. Sun, J. Li, F. Yang, A novel geographic position mobility oriented routing strategy for UAVs, Journal of Computational Information Systems 8 (2012) 709–716

[50] C. Zang and S. Zang, "Mobility prediction clustering algorithm for UAV networking," in GLOBECOM Workshops, IEEE, 2011, pp. 1158–1161

[51] Alexey V. Leonov, "Modeling of bio-inspired algorithms AntHocNet and BeeAdHoc for Flying Ad Hoc Networks (FANETs)," 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE),vol.02, pp. 90-99,2016

[52] I. Bekmezci, O. K. Sahingoz, and S¸. Temel, "Flying Ad-Hoc networks (fanets): A survey," Ad Hoc Networks, vol. 11, no. 3, pp. 1254–1270, 2013]

[53] P. M. Jawandhiya, M. M. Ghonge, M. Ali, and J. Deshpande, "A survey of mobile ad hoc network attacks," International Journal of Engineering Science and Technology, vol. 2, no. 9, pp. 4063–4071, 2010

[54] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in Wireless Network Security, pp. 103–135, Springer, 2007

[55] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255–265, ACM, 2000

[56] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," Communications Surveys & Tutorials, IEEE, vol. 15, no. 1, pp. 446–471, 2013

[57] P. Ning and K. Sun, "How to misuse aodv: a case study of insider attacks against mobile Ad-Hoc routing protocols," Ad Hoc Networks, vol. 3, no. 6, pp. 795–819, 2005.

[58] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 370–380, 2006.

[59] S. Shrivastava and S. Jain, "A brief introduction of different type of security attacks found in mobile Ad-Hoc network," International Journal of Computer Science & Engineering Technology (IJCSET), vol. 4, no. 3, 2013

[60] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," Communications Surveys & Tutorials, IEEE, vol. 11, no. 4, pp. 42–56, 2009

[61] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential dsss: Jamming-resistant wireless broadcast communication," in INFOCOM, 2010 Proceedings IEEE, pp. 1–9, IEEE, 2010

[62] X. He, H. Dai, and P. Ning, "Dynamic adaptive anti-jamming via controlled mobility," Wireless Communications, IEEE Transactions on, vol. 13, no. 8, pp. 4374–4388, 2014

[63] A. A. Cardenas, S. Radosavac, and J. S. Baras, "Detection and prevention of mac layer misbehavior in ad hoc networks," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 17–22, ACM, 2004

[64] J. Sen, S. Koilakonda, and A. Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on, pp. 338–343, IEEE, 2011

[65] L. Himral, V. Vig, and N. Chand, "Preventing aodv routing protocol from black hole attack," Lalit Himral et al./International Journal of Engineering Science and Technology (IJEST), vol. 3, no. 5, 2011

[66] F. Thachil and K. Shet, "A trust based approach for aodv protocol to mitigate black hole attack in manet," in Computing Sciences (ICCS), 2012 International Conference on, pp. 281–285, IEEE, 2012

[67] K. Sahadevaiah and P. R. PVGD, "Impact of security attacks on a new security protocol for mobile ad hoc networks," Network Protocols and Algorithms, vol. 3, no. 4, pp. 122–140, 2011

[68] J. Goppert, W. Liu, A. Shull, V. Sciandra, I. Hwang, and H. Aldridge, "Numerical analysis of cyberattacks on unmanned aerial systems," in AIAA Conference on Infotech@ Aerospace, 2012

[69] A. N. Phillips, B. E. Mullins, R. A. Raines, and R. O. Baldwin, "A secure group communication architecture for autonomous unmanned aerial vehicles," Security and Communication Networks, vol. 2, no. 1, pp. 55–69, 2009

[70] C. Constantinides and P. Parkinson, "Security challenges in MEA development," in Digital Avionics Systems Conference, 2008. DASC 2008. IEEE/AIAA 27th, pp. 1–C, IEEE, 2008

[71] S.-W. Kim and S.-W. Seo, "Cooperative unmanned autonomous vehicle control for spatially secure group communications," Selected Areas in Communications, IEEE Journal on, vol. 30, no. 5, pp. 870–882, 2012

[72] S. Bhattacharya and T. Bas¸ar, "Secure communication for mobile agents in an adversarial environment," in Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on, pp. 1–8, IEEE, 2011

[73] R. N. Akram, P.-F. Bonnefoi, S. Chaumette, K. Markantonakis, and D. Sauveron, "Improving security of autonomous MEAs fleets by using new specific embedded secure elements a position paper"

[74] Q. Wang, H.-N. Dai, and Q. Zhao, "Eavesdropping security in wireless ad hoc networks with directional antennas," in Wireless and Optical Communication Conference (WOCC), 2013 22nd, pp. 687–692, IEEE, 2013.

[75] A. I. Alshbatat and L. Dong, "Adaptive mac protocol for MEA communication networks using directional antennas," in Networking, Sensing and Control (ICNSC), 2010 International Conference on, pp. 598–603, IEEE, 2010.

[76] A. Carrasco-Casado, R. Vergaz, and J. M. S. Pena, "Design and early development of a MEA terminal and a ground station for laser communications," in SPIE Security+ Defence, pp. 81840E–81840E, International Society for Optics and Photonics, 2011

[77] M. J. Northcott, A. McClaren, J. Graves, J. Phillips, D. Driver, D. Abelson, D. W. Young, J. E. Sluz, J. C. Juarez, M. B. Airola, et al., "Long distance laser communications demonstration," in Defense and Security Symposium, pp. 65780S–65780S, International Society for Optics and Photonics, 2007

[78] Cyborg Moth Gets a New Radio, 10 Feb 2009, By Sally Adee, Research reported this week advances the goal of turning insects into unmanned aerial vehicles
https://spectrum.ieee.org/robotics/military-robots/cyborg-moth-gets-a-new-radio

[79] The World of Insect Cyborgs, 06/14/18, Len Calderone,
https://www.roboticstomorrow.com/article/2018/06/the-world-of-insect-cyborgs/12087

[80] Professor of Chemical engineering and Bioengineering at the University of California, Berkeley, https://en.wikipedia.org/wiki/Jay_Keasling

[81] Michel M. Maharbiz is a Professor with the Department of Electrical Engineering and Computer Science at the University of California, Berkeley
https://www2.eecs.berkeley.edu/Faculty/Homepages/maharbiz.html

[82] Draper's headquarters is located in Cambridge, Massachusetts.
https://www.draper.com/

[83] Dragonfly Dogfights, By Aparna Sreenivasan, Jun. 6, 2003
https://www.sciencemag.org/news/2003/06/dragonfly-dogfights

[84] Λιβελούλες που διασχίζουν ωκεανούς , Τσαρλς Άντερσον, TEDIndia 2009
https://www.ted.com/talks/charles_anderson_dragonflies_that_fly_across_oceans/transcript?language=el#t-979197

[85] The Metamorphosis of a Dragonfly, Beauty of Science, 2018
https://www.sciencelab.gr/2018/01/05/dragonfly/

[86] DragonflEye Project Wants to Turn Insects Into Cyborg Drones,
R&D lab Draper is using genetic engineering and optoelectronics to build cybernetic insects, By Evan Ackerman, 25 Jan 2017
https://spectrum.ieee.org/automaton/robotics/industrial-robots/draper-dragonfleye-project

[87] Αληθινή λιβελούλη drone κινείται με τη σκέψη…, By SecNews, 6 Ιουνίου 2017,
https://www.secnews.gr/157948/dragonfleye-drone-from-draper/

[88] Πρώτη πτήση για τηλεχειριζόμενη λιβελούλα cyborg στις ΗΠΑ, ΤΕΧΝΟΛΟΓΙΑ – ΕΠΙΣΤΗΜΗ, Παρασκευή, 02 Ιουνίου 2017,

https://www.naftemporiki.gr/story/1242391/protiptisi-gia-tilexeirizomeni-libeloula-cyborgstis-ipa

[89] DragonflEye Has Liftoff, Wednesday, May 31 2017 CAMBRIDGE, MA, https://www.draper.com/news-releases/dragonfleye-has-liftoff

[90] Equipping Insects for Special Service, Thursday, January 19 2017, CAMBRIDGE, MA https://www.draper.com/news-releases/equipping-insects-special-service

[91]«Βασίλισσα» των μεγάλων μεταναστεύσεων η λιβελούλα, Παρά το πολύ μικρό της μέγεθος διανύει από 14.000 έως 18.000 χλμ, 03/03/2016 https://www.newsbeast.gr/environment/arthro/2156987/vasilissa-ton-megalon-metanastefseon-i-liveloula

[92] ΕΥΦΥΗ ΣΥΝΘΕΤΑ ΥΛΙΚΑ, Μηχανική πιεζοηλεκτρικών υλικών (Κεφ. 6.1.1) http://ecourse.uoi.gr/pluginfile.php/112867/mod_resource/content/1/%CE%9A%CE%95%CE%A6%CE%91%CE%9B%CE%91%CE%99%CE%9F-6.pdf

[93] Πιεζοηλεκτρισμός, Βικιπαίδεια, 6 Φεβ 2020, https://el.wikipedia.org/wiki/Πιεζοηλεκτρισμός

[94] An introduction to inertial navigation, Oliver J. Woodman, Technical Report Number 696, University of Cambridge, Computer Laboratory https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf

[95] Inertial Navigation Systems and Its Practical Applications, Chapter 10, Aleksander Nawrat, Karol Jędrasiak, Krzysztof Daniec and Roman Koteras https://pdfs.semanticscholar.org/1c81/9d104a57bc0583dbd560a2d952ed4bba7351.pdf?_ga=2.36724704.1713038805.1589127890-1157333746.1589127890

[96] NASA/TM–2015-218803, A Short Tutorial on Inertial Navigation System and Global Positioning System Integration, Kyle M. Smalling (Northrop Grumman, Hampton, Virginia), Kenneth W. Eure (Langley Research Center, Hampton, Virginia) https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150018921.pdf