



Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Ψηφιακός Πολιτισμός, Έξυπνες Πόλεις, IoT και Προηγμένες Ψηφιακές Τεχνολογίες»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Διαδίκτυο των ΣμηΕΑ και εφαρμογές – Προκλήσεις και προοπτικές Internet of Drones and applications – Challenges and prospects
Όνοματεπώνυμο Φοιτητή	Ψυχογιός Ηλίας
Πατρώνυμο	Ιωάννης
Αριθμός Μητρώου	ΨΠΟΛ20086
Επιβλέπων	Δρ. Σταύρος Ι. Παπαπαναγιώτου, Διδάσκων ΠΜΣ

Ημερομηνία Παράδοσης Δεκέμβριος 2023

Τριμελής Εξεταστική Επιτροπή

Σταύρος Παπαπαναγιώτου
Διδάσκων ΠΜΣ

Δημήτριος Βέργαδος
Καθηγητής

Δρ. Εμμανουήλ Σκόνδρας
Διδάσκων ΠΜΣ

Περίληψη

Το Διαδίκτυο των Drones (Internet of Drones – IoD) έχει κερδίσει τον τελευταίο καιρό την προσοχή της παγκόσμιας τεχνολογικής και επιχειρηματικής κοινότητας λόγω της προσαρμοστικότητας των drones σε ποικίλα σενάρια χρήσης και εφαρμογής τους.

Όντως, τα ΣΜηΕΑ (Συστήματα Μη επανδρωμένων Αεροσκαφών – a.k.a. drones) χρησιμοποιούνται ήδη με επιτυχία σε πολλά και διαφορετικά πεδία εφαρμογής όπως η γεωργία ακριβείας, οι αποστολές έρευνας και διάσωσης, οι υπηρεσίες ασφαλείας και επίτευσης χώρων καθώς και σε κρίσιμες, αναφορικά με το αποτέλεσμα τους, αποστολές.

Η χρήση τους σε όλους τους παραπάνω, και αρκετούς ακόμα, τομείς, οφείλεται σε ορισμένα εξαιρετικής σημασίας πλεονεκτήματα, τόσο τεχνικά όσο και πρακτικά: υψηλή κινητικότητα, δυνατότητα πρόσβασης σε σημεία δυσπρόσιτα με άλλες μεθόδους, δυνατότητα παροχής ασύρματης πρόσβασης στο διαδίκτυο σε απομακρυσμένες περιοχές ή σε περιοχές όπου έχουν συμβεί φυσικές καταστροφές και, φυσικά, χαμηλό κόστος παραγωγής, χρήσης και συντήρησης συγκριτικά με όλες τις πιθανές εναλλακτικές, όπου αυτές υπάρχουν.

Επιπλέον, η χρήση ΣΜηΕΑ (από εδώ και στο εξής θα αναφέρονται ως drones για μεγαλύτερη ευκολία) βελτιώνει τις παραμέτρους απόδοσης διαφορετικών αρχιτεκτονικών δικτύου όπως αξιοπιστία σύνδεσης, απόδοση, συνδεσιμότητα, επεκτασιμότητα.

Ωστόσο, η χρήση δικτύων drones δημιουργεί επιπλέον ζητήματα σχετικά με την εγγενή αναξιπιστία της ασύρματης επικοινωνίας, τη διάρκεια των μπαταριών και τον υψηλό βαθμό κινητικότητας των drones ο οποίος μπορεί να προκαλέσει συχνές αλλαγές της τοπολογίας του δικτύου.

Στην παρούσα εργασία θα παρουσιαστεί η υπάρχουσα κατάσταση αναφορικά με τις μελέτες επάνω στο IoD, τις μελλοντικές προοπτικές του, τα ζητήματα ασφαλείας καθώς και πεδία στα οποία ήδη τα drones χρησιμοποιούνται με μεγάλη επιτυχία και αποτελεσματικότητα.

Λέξεις κλειδιά : drones, Διαδίκτυο των ΣμηΕΑ, IoD, Internet of Drones, UAV

Abstract

Internet of Drones (IoD) has recently gained the attention of the global technological and business community due to the adaptability of drones to a variety of usages and application scenarios.

Indeed, UAVs (a.k.a. drones) are already successfully used in many different fields of application such as precision agriculture, search and rescue missions, security and site surveillance services as well as in mission-critical missions.

Their use in all the above, and several more, sectors is due to some extremely important advantages, both technical and practical: high mobility, accessibility to places inaccessible by other methods, ability to provide wireless internet access in remote areas or areas where natural disasters have occurred and, of course, low production, use and maintenance costs compared to all possible alternatives, where they exist.

In addition, the use of SMEA (from now on they will be referred to as drones for greater convenience) improves the performance parameters of different network architectures such as connection reliability, performance, connectivity, scalability. However, the use of drone networks creates additional issues related to the inherent unreliability of wireless communication, battery life and the high degree of mobility of drones which can cause frequent changes in network topology.

This paper will present the current situation regarding studies on IoD, its future prospects, security issues as well as areas in which drones are already used with great success and effectiveness.

Keywords :drones, IoD, Internet of Drones, UAV

Ευχαριστίες

Η παρούσα εργασία εκπονήθηκε στο Τμήμα Πληροφορικής της Σχολής Τεχνολογιών Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πειραιά. Το θέμα της εργασίας προτάθηκε από τον γράφοντα στον Δρ. Σταύρο Παπαπαναγιώτου, ο οποίος έδωσε καίριες κατευθυντήριες γραμμές, εκτενή βιβλιογραφία και επιστημονική υποστήριξη.

Θα ήθελα να ευχαριστήσω ιδιαίτερα την εταιρεία Flybot A.E. καθώς και τον κ. Δημήτρη Χρηστάκο, ιδιοκτήτη της εταιρείας Smartec A.E. για τη χρήση των εγκαταστάσεων και του εξοπλισμού των δύο εταιρειών στο πλαίσιο της συγκεκριμένης εργασίας.

Επίσης θα ήθελα να ευχαριστήσω την αδελφή μου Βασιλική για την δημιουργική της πίεση και την ψυχολογική, και όχι μόνο, υποστήριξη.

Τέλος, πιστεύω ότι ο πατέρας μου, ο οποίος ήταν πάντα υποστηρικτής της νοοτροπίας «αν δεν σηκωθείς όταν πέσεις, σου άξιζε να πέσεις» θα χαίρεται που, έστω και με μεγάλη καθυστέρηση, ολοκλήρωσα αυτό που είχα αφήσει στη μέση στο παρελθόν.

Πίνακας περιεχομένων

Περίληψη	3
Ευχαριστίες	5
Πίνακας περιεχομένων	6
Πίνακας Εικόνων	9
1. Εισαγωγή.....	10
2. Εισαγωγή στα ΣμηΕΑ	13
2.1 Τύποι και Χαρακτηριστικά των ΣμηΕΑ	13
2.1.1 Ωφέλιμο Φορτίο (Payload)	13
2.1.2 Μηχανισμός πτήσης	13
2.1.3 Εμβέλεια και Υψόμετρο.....	15
2.1.4 Ταχύτητα και χρόνος πτήσης.....	15
2.1.5 Παροχή ενέργειας.....	16
3. ΣμηΕΑ, δικτύωση και IoD	17
3.1 Προκλήσεις και δυσκολίες για τα δίκτυα ΣμηΕΑ.....	17
3.2 Κύρια ζητήματα	18
3.3 Τι είναι το Διαδίκτυο των ΣμηΕΑ (IoD – Internet of Drones)	21
4. Φυσικό επίπεδο (Physical layer).....	23
4.1 Τεχνικές διαμόρφωσης (Modulation techniques)	23
4.1.1 Βελτίωση ποιότητας σήματος (Signal quality enhancement)	23
4.1.2 Φάσμα Διασποράς με εναλλαγή συχνότητας (FHSS – frequency-hopping spread spectrum)	24
4.1.3 Σύστημα Ευθείας Αλληλουχίας Ευρέως Φάσματος (DSSS – direct-sequence spread spectrum)	24
4.1.4 Ορθογώνια Πολύπλεξη Διάρθρωσης Συχνοτήτων (OFDM – Orthogonal Frequency Division Multiplexing).....	24
4.1.5 Πολλαπλή Πρόσβαση Διάρθρωσης Συχνότητας Μονού Φέροντος (SC-FDM – Single Carrier Frequency Division Multiplex).....	25
4.2 Συνδεσιμότητα (Connectivity)	25
4.2.1 Ανάλυση και βελτιστοποίηση κάλυψης	25
4.2.2 Κατανομή και βελτιστοποίηση πόρων (Resource allocation and optimization) 29	
ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΡΟΣΟΜΟΙΩΣΗΣ ΚΑΙ ΑΝΑΛΥΣΗ	30
4.2.3 Αναμετάδοση και δρομολόγηση	34
4.3 Μεγιστοποίηση και αξιολόγηση απόδοσης.....	37
4.3.1 Μεγιστοποίηση απόδοσης στο φυσικό επίπεδο	37
4.3.2 Μεγιστοποίηση απόδοσης σε επίπεδο δικτύου	37

4.4	Μοντελοποίηση και χαρακτηρισμός καναλιών	38
4.4.1	Βελτιστοποίηση θέσης	38
4.4.2	Ανάλυση και βελτιστοποίηση μετρήσεων απόδοσης	42
4.5	Τεχνολογίες επικοινωνίας	45
4.5.1	Τεχνολογία επικοινωνίας WiFi	45
4.5.2	Τεχνολογία επικοινωνίας mmWave	46
4.5.3	Επικοινωνίες Machine-type	47
5.	Επίπεδο ζεύξης δεδομένων (Data link layer)	49
5.1	Κατανομή και βελτιστοποίηση πόρων	49
5.1.1	Συνεργατικά περιβάλλοντα	49
5.1.2	Προβλήματα βελτιστοποίησης	50
5.2	Coding strategies	51
5.2.1	Στρατηγικές προστασίας από σφάλματα	51
6.	Επίπεδο δικτύου (Network layer)	53
6.1	Στρατηγικές συνεργασίας	53
6.1.1	Ενεργειακή απόδοση, βελτίωση συνδεσιμότητας και συλλογή δεδομένων	53
6.2	Πρωτόκολλα δρομολόγησης	57
6.2.1	FANETs	57
6.2.2	Δρομολόγηση A2G	59
6.2.3	VANETs	61
6.3	Σχήματα αναμετάδοσης	62
6.3.1	Αναμετάδοση UAV-BS	62
6.3.2	Επικοινωνίες mmWave	65
7.	Επιχειρησιακή εφαρμογή	68
7.1	Συλλογή και αποστολή δεδομένων	68
7.2	Ανανεώσιμες πηγές ενέργειας	69
7.3	Ιχθυοκαλλιέργειες	69
7.4	Αναδασώσεις	69
7.5	Τηλεπικοινωνίες	69
7.6	Αγροτική παραγωγή	69
7.7	Στρατιωτικές εφαρμογές	70
7.8	Έρευνα και διάσωση	70
7.9	Ψυχαγωγία	71
7.10	Υπηρεσίες υγείας	71
7.11	Έλεγχος κυκλοφορίας	71
8.	Εφαρμογή πεδίου: Επόπτευση Φ/Β πάρκων και εντοπισμός σφαλμάτων ..	72
8.1	Εξοπλισμός	72

8.2	Προσωπικό	72
8.3	Κατεύθυνση λήψης	72
8.4	Λήψη εικόνων	73
8.5	Ηλιοφάνεια	74
8.6	Ανάλυση δεδομένων.....	74
8.7	Βλάβες που εντοπίζονται	74
8.8	Λογισμικό	75
8.9	Report βλαβών	76
9.	Ασφάλεια και απόρρητο.....	78
9.1	Απαιτήσεις Ασφαλείας του IoD	78
9.2	Κυβερνοεπιθέσεις στο IoD	79
9.2.1	Επιθέσεις παρεμβολής σήματος (Jamming)	79
9.2.2	Επιθέσεις αλλοίωσης δεδομένων	79
9.2.3	Συγκρούσεις.....	79
9.2.4	Επιθέσεις επιλεκτικής προώθησης δεδομένων.....	79
9.2.5	Επιθέσεις “Flooding”	80
9.2.6	Επιθέσεις «κατάληψης»	80
9.2.7	Επιθέσεις “Man-in-the-middle”	80
9.2.8	Επίθεση Denial-of-Service (DOS)	80
9.3	Υπάρχουσες λύσεις ασφάλειας IoD.....	80
9.3.1	Τεχνικές πιστοποίησης πρόσβασης χρήστη.....	81
9.3.2	Συστήματα blockchain	82
9.4	Ανίχνευση εισβολής.....	83
9.5	Σχήματα προστασίας της ιδιωτικότητας.....	84
9.5.1	Πολιτικές προστασίας της ιδιωτικότητας	84
9.5.2	Τεχνολογικές λύσεις προστασίας της ιδιωτικότητας	84
9.6	Προκλήσεις.....	85
9.6.1	Προκλήσεις των συστημάτων blockchain	85
9.6.2	Θέματα σχετικά με την ιδιωτικότητα	86
10.	Συμπεράσματα – Περίληψη.....	87
11.	Βιβλιογραφία	88
12.	Ορολογία	93

Πίνακας Εικόνων

Εικόνα 1: Το Parrot Swing, υβριδικό ΣμηΕΑ, με δυνατότητα πτήσης με ρότορες και σταθερή πτέρυγα	14
Εικόνα 2: Πιθανότητα κάλυψης δεδομένης πυκνότητας ΣμηΕΑ 25 /km²	27
Εικόνα 3: Πιθανότητα κάλυψης για πολλαπλές πυκνότητες ΣμηΕΑ με όριο SINR 0 dB	27
Εικόνα 4: Πιθανότητα κάλυψης με όριο SINR 0 dB και πυκνότητα ΣμηΕΑ 50 /km²	28
Εικόνα 5: Κατατμήσεις κυψελών που σχετίζονται με ΣμηΕΑ δεδομένης της μη ομοιόμορφης χωρικής κατανομής των χρηστών	31
Εικόνα 6: Ο Δείκτης δικαιοσύνης του Jain για τη μέση υπηρεσία δεδομένων στους χρήστες	32
Εικόνα 7: : Μέση υπηρεσία δεδομένων έναντι παράγοντα παρεμβολών	33
Εικόνα 8: Χάρτης έντασης αθροιστικής χωρητικότητας σε σχέση με τις θέσεις του UAV-BS 2 εντός του δικτύου. Η μέγιστη χωρητικότητα αθροίσματος παρατηρήθηκε όταν το UAV-BS 1 βρισκόταν στη θέση του, (90, 245) m και το UAV-BS 2 ήταν στη θέση (510, 245) m ($\sigma_2 = -95$ dB)	36
Εικόνα 9: Ελάχιστη απαιτούμενη ισχύς μετάδοσης	40
Εικόνα 10: Απόδοση κάλυψης δύο DSC με παρεμβολές παρουσία παρεμβολών	40
Εικόνα 11: Συνολικός λόγος κάλυψης έναντι ενδιάμεσης απόστασης των DSC	41
Εικόνα 12: Βέλτιστη απόσταση DSC σε σχέση με το μήκος της περιοχής-στόχου	41
Εικόνα 13: Το πρόβλημα διαχωρισμού ενός κύκλου με τρεις άλλους κύκλους	42
Εικόνα 14: Μοντέλο δοκιμών	43
Εικόνα 15: Συνολική κάλυψη και διάρκεια ζωής κάλυψης έναντι αριθμού UAVs για $R_c = 5000$m	43
Εικόνα 16: Το υπόμετρο πτήσης του ΣμηΕΑ έναντι του αριθμού των UAVs	44
Εικόνα 17: Αριθμός απαιτούμενων ΣμηΕΑ σε σχέση με την ακτίνα της επιθυμητής περιοχής	44
Εικόνα 18: Συνολική δομή της προτεινόμενης μεθόδου μείωσης του θορύβου με τη χρήση αυτοκωδικοποιητή βαθιάς συνελκτικής αποθορυβοποίησης	52
Εικόνα 19: Σύγκριση κυματομορφών και φασμάτων σχετικά με το σήμα ομιλίας από το οποίο αφαιρείται η πτήση drone και ο θόρυβος του ανέμου με τη χρήση αυτόματου κωδικοποιητή βαθιάς συνελκτικής αποθορυβοποίησης	52
Εικόνα 20: Εναέρια δίκτυα αναμετάδοσης χρησιμοποιώντας συνεργατικά ΣμηΕΑ, όπου αυτά αναμεταδίδουν δεδομένα από απομακρυσμένους αισθητήρες προς σταθμό βάσης	54
Εικόνα 21: απεικόνιση του προτεινόμενου αλγορίθμου, όπου το αριστερό πλαίσιο περιγράφει τη διαδικασία εξισορρόπησης ενέργειας δεδομένης της διαμόρφωσης κάθε ΣμηΕΑ. Το δεξί πλαίσιο δείχνει την αύξηση της διαμόρφωσης ώστε να ταιριάζει στον διαθέσιμο χρόνο μετάδοσης.	55
Εικόνα 22: Ο αλγόριθμός	56
Εικόνα 23: Παραμετροποίηση προσομοιώσεων	56
Εικόνα 24: Επισκόπηση εδάφους από ΣμηΕΑ	62
Εικόνα 25: Υποτιθέμενο δίκτυο ΣμηΕΑ	63
Εικόνα 26: Επίδραση του μεγέθους του δικτύου στο ανώτερο όριο ταχύτητας μεταγωγής	64
Εικόνα 27: Επίδραση της εξασθένησης που προκαλείται από εμπόδια στο ανώτερο όριο ταχύτητας μεταγωγής	64
Εικόνα 28: Επίδραση της διακύμανσης τόσο του μεγέθους του δικτύου όσο και του ρυθμού εξασθένησης στο ανώτερο όριο ταχύτητας μεταγωγής	65
Εικόνα 29: Σκίαση, βαρύτητα 5	75
Εικόνα 30: Hotspot, βαρύτητα 1	75
Εικόνα 31: Βραχυκύκλωμα, βαρύτητα 2	75
Εικόνα 32: Δίοδος, βαρύτητα 1	75

1. Εισαγωγή

Ως IoD ορίζεται μια αρχιτεκτονική δικτύου που στοχεύει ειδικά στην υποστήριξη επικοινωνιών μεταξύ αυτόνομων εναέριων οχημάτων αλλά αυτών των αυτόνομων εναερίων οχημάτων και συσκευών που αναπτύσσονται στο έδαφος.

Στο IoD, τα drones θεωρούνται ως «έξυπνες συσκευές» επιφορτισμένες να πετούν σε έναν συγκεκριμένο γεωγραφικό χώρο, εκτελώντας μίας σειρά αποστολών, οι οποίες εκτείνονται από τις περιπολίες για λόγους ασφαλείας και τη συγκέντρωση περιβαλλοντικών δεδομένων έως την πραγματοποίηση εργασιών ακριβείας όπως η από αέρος φύτευση σπόρων, οι αεροψεκασμοί και η εκπομπή ηχητικών και οπτικών σημάτων για την αποτροπή εισβολών σε φυλασσόμενους χώρους.

Κάθε μία από τις παραπάνω αποστολές μπορεί να αναλύεται επιπλέον σε πιο εξειδικευμένες κατηγορίες. Οι εφαρμογές ασφαλείας, όπως οι περιπολίες, εκτείνονται από την επόπτευση συγκεκριμένων ιδιωτικών χώρων έως την παρακολούθηση των θαλασσιών και χερσαίων συνόρων μίας χώρας. Η συγκέντρωση περιβαλλοντικών δεδομένων περιλαμβάνει από την μέτρηση της ατμοσφαιρικής ρύπανσης έως την καταγραφή των ροών ύδατος σε ποτάμια. Ακόμα και οι αεροψεκασμοί μπορεί να είναι από μαζικοί, όπως για την καταπολέμηση των κουνουπιών έως τους ψεκασμούς ακριβείας σε καλλιέργειες αμπελιών και ελιάς.

Στο σύνολο των ανωτέρων αποστολών τα ΣμηΕΑ (drones) λειτουργούν ως το βασικό μέσο για την εκτέλεσή τους, συνεργαζόμενα με επίγειες εγκαταστάσεις, όπως οι σταθμοί βάσης και οι κεραιές των δικτύων κινητής τηλεφωνίας ή ακόμα και με εναέριες υποδομές όπως τα Εναέρια Κέντρα Ελέγχου που διαθέτουν οι ένοπλες δυνάμεις μίας χώρας

Στην αρχιτεκτονική του IoD, τα ΣμηΕΑ έχουν σχεδιαστεί ως συσκευές δικτύου που μπορούν να ομαδοποιηθούν σε σμήνη, ώστε να προσδιοριστεί λειτουργικά η ομαδική αποστολή τους και ο στόχος αυτής. Ακόμα όμως και όταν δεν είναι διαμορφωμένα σε σμήνη, τα ΣμηΕΑ μπορούν να επικοινωνούν μεταξύ τους ανταλλάσσοντας απαραίτητα για την πτήση τους δεδομένα, όπως αυτά που σχετίζονται με τον συντονισμό πτήσης.

Ταυτόχρονα, τα ΣμηΕΑ επικοινωνούν με επίγειες υποδομές, επιφορτισμένες με την αποθήκευση και την επεξεργασία δεδομένων για την εξαγωγή συγκεκριμένων πληροφοριών σε ενδιαφερόμενους εξουσιοδοτημένους χρήστες ή για την εκκίνηση και πραγματοποίηση συγκεκριμένων υπηρεσιών.

Οι επίγειες υποδομές είναι όμως ταυτόχρονα υπεύθυνες για τον έλεγχο του εναερίου χώρου, με την παροχή την βέλτιστης θέσης του ΣμηΕΑ ανάλογα με την αποστολή που εκτελείται καθώς και για να παρακολουθούν τις δραστηριότητές τους.

Καθώς οι επίγειες υποδομές λογίζονται ως ένα σύνολο κόμβων με υψηλές υπολογιστικές δυνατότητας, μπορούν να εκτελούν τον συντονισμό των εργασιών των ΣμηΕΑ και την ενημέρωση των σχεδίων πτήσης, χωρίς να αναλώνονται οι περιορισμένοι πόροι που έχουν ενσωματωμένοι τα ΣμηΕΑ.

Το IoD έχει προσελκύσει μεγάλο ενδιαφέρον λόγω της ευελιξίας και της προσαρμοστικότητας των δικτύων ΣμηΕΑ, σε πολλά και διαφορετικά επιχειρησιακά σενάρια και στην ικανότητά τους να βελτιώνουν την απόδοση άλλων αρχιτεκτονικών δικτύου.

Τα ΣμηΕΑ γίνονται όλο και πιο διαδεδομένα σε πολλούς τομείς λόγω ορισμένων τεχνολογικών, τακτικών αλλά και πρακτικών πλεονεκτημάτων: α. Υψηλή κινητικότητα, β.

Εύκολη ανάπτυξή τους επί του πεδίου και δυνατότητα επαναχρησιμοποίησης, γ. Παρακολούθηση και συντονισμός σε πραγματικό χρόνο (αυτό εξαρτάται σε μεγάλο βαθμό από τις σχετικές αρχιτεκτονικές συστημάτων και τις τεχνολογίες επικοινωνίας), δ. Μεταφορά φορτίου (ανάλογα με τις απαιτήσεις κάθε αποστολής).

Τα ΣμηΕΑ μπορούν να χρησιμοποιηθούν σε περιοχές ή για την εκτέλεση εργασιών που είτε δεν είναι εύκολα προσβάσιμες είτε ενέχουν κινδύνους αν εκτελεστούν από άνθρωπο, ενισχύουν την συνδεσιμότητά των δικτύων επικοινωνιών, αυξάνουν την γεωγραφική κάλυψη και την χωρητικότητα του δικτύου, ειδικά αν χρησιμοποιούνται συνδυαστικά με άλλες ασύρματες/ενσύρματες αρχιτεκτονικές δικτύου.

Με δεδομένο αυτό το ευρύ φάσμα λειτουργιών, μπορεί να αναπτυχθεί ένας σημαντικός αριθμός εφαρμογών για το IoD, μεταξύ των οποίων βρίσκονται οι ακόλουθες: Έξυπνη γεωργία, εφαρμογές έρευνας και διάσωσης, συστήματα επιτήρησης, αθλητισμός, εκπαίδευση, τηλεπικοινωνίας, ακόμα και υπηρεσίες σχετικές με την τέχνη και την ανθρώπινη δημιουργικότητα.

Αντίστοιχα, υπάρχουν πολλά επιπλέον ζητήματα που πρέπει να εξεταστούν σωστά, αναφορικά με τα σενάρια χρήσης του IoD.

Αρχικά, η ασύρματη επικοινωνία, είναι από την φύση της αναξιόπιστη, συγκρινόμενη με την ενσύρματη, επομένως είναι επιρρεπής σε σφάλματα και εξασθένηση σήματος, γεγονότα που μπορούν να οδηγήσουν σε απώλεια δεδομένων και διακοπή σύνδεσης του ΣμηΕΑ. Αν και αυτό το χαρακτηριστικό των ασύρματων επικοινωνιών δεν είναι κάτι το οποίο ανακαλύφθηκε πρόσφατα αλλά είναι γνωστό από τα πρώτα ασύρματα δίκτυα, αποκτά μία εντελώς διαφορετική βαρύτητα όταν οι διασυνδεδεμένες συσκευές είναι ιπτάμενες και μετακινούνται ξαφνικά και με μεγάλη ταχύτητα από ένα σημείο ενδιαφέροντος σε ένα άλλο.

Στην βιβλιογραφία αυτό έχει αντιμετωπιστεί με την αναφορά σε Ασύρματα Δίκτυα Αισθητήρων (WSN), Ασύρματα Ad-hoc δίκτυα (Mobile Ad-hoc NETWORKS – MANETs) και Ιπτάμενα Ad-hoc Δίκτυα (Flying Ad-hoc NETWORKS – FANETs). Δυστυχώς, στο IoD, τα ΣμηΕΑ εκτελούν πολλαπλές αποστολές οι οποίες εκτείνονται από τη βελτίωση γεωγραφικής κάλυψης, όταν χρησιμοποιούνται ως ιπτάμενοι σταθμοί βάσης (FBS), έως την αναγνώριση προτύπων σε συγκεντρώσεις πλήθους ατόμων. Σε αυτές τις καταστάσεις, η εγγενής αναξιοπιστία του ασύρματου μέσου επικοινωνίας ωθεί στην ανάγκη σχεδιασμού σταθερού μέσου επικοινωνίας.

Στην πραγματικότητα, το εύρος επικοινωνίας είναι συχνά περιορισμένο, ειδικά σε περιβάλλοντα όπου η εξασθένηση του τηλεπικοινωνιακού σήματος είναι σημαντική [5]. Ο υψηλός βαθμός κινητικότητας των ΣμηΕΑ επιβαρύνει αυτή την κατάσταση, απαιτώντας ακριβή έλεγχο και συντονισμό των σμηνών ΣμηΕΑ προς αποφυγή συγκρούσεων, ιδίως όσον αφορά τους αεροδιαδρόμους πτήσης και την ανταλλαγή δεδομένων.

Η κατανάλωση ενέργειας είναι ένα ακόμα κρίσιμο σημείο στις συσκευές οι οποίες τροφοδοτούνται ενεργειακά από μπαταρίες, όπως είναι τα περισσότερα ΣμηΕΑ. Αυτό το πρόβλημα δεν είναι άγνωστο σε όσους ασχολούνται με το Διαδίκτυο των Πραγμάτων (IoT) καθώς η εξοικονόμηση ενέργειας και χρήσης των μπαταριών στη λειτουργία των αισθητήρων των σκαφών, στην επικοινωνία και στην επεξεργασία δεδομένων είναι βασικό σχεδιαστικό και κατασκευαστικό κριτήριο των ΣμηΕΑ.

Αυτό στηρίζεται στο γεγονός ότι στον τομέα του IoT, οι κόμβοι του δικτύου υποτίθεται ότι αναπτύσσονται με ελάχιστη έως μηδενική ανάγκη συντήρησης. Συνεπώς, πολιτικές χαμηλής κατανάλωσης ενέργειας κατά τη μεταφορά δεδομένων βρίσκονται υποχρεωτικά εντός αυτού του πλαισίου.

Αυτό που κάνει το IoD να είναι ένα ακόμα δυσκολότερο σενάριο λειτουργίας είναι το γεγονός ότι η κατανάλωση ενέργειας από τις εμπλεκόμενες συσκευές δεν σχετίζεται

μόνο με τη χρήση των αισθητήρων και την επικοινωνία αλλά και με την κίνηση των ΣμηΕΑ και την εκτέλεση πτήσεων.

Επιπλέον, ενώ οι συσκευές IoT συχνά μεταφέρουν χαμηλό όγκο δεδομένων, τα ΣμηΕΑ συχνά εμπλέκονται σε εφαρμογές οι οποίες απαιτούν τη μεταφορά υψηλού όγκου δεδομένων. Αυτό συμβαίνει όταν, για παράδειγμα τα ΣμηΕΑ λειτουργούν ως Ιπτάμενοι Σταθμοί Βάσης (FBS) ή «τρέχουν» εφαρμογές video streaming, συνεπώς εμφανίζονται ζητήματα με την ενσωματωμένη μνήμη του σκάφους.

Συνεπώς θα πρέπει να εφαρμοστεί μία αποτελεσματική κατανομή των πόρων ενέργειας του σκάφους αναφορικά με την μεταφορά δεδομένων και τη λειτουργία της πτήσης του.

Στις περιπτώσεις όπου τα ΣμηΕΑ χρησιμοποιούνται ως σημεία αναμετάδοσης κατά τη συλλογή και/ή την διαβίβαση δεδομένων σε multi-hop εναέρια δίκτυα, η συνεργασία και η επικοινωνία μεταξύ των ΣμηΕΑ είναι υποχρεωτική προκειμένου να επιτευχθεί αύξηση συνδεσιμότητας δικτύου, αύξηση γεωγραφικής κάλυψης και μείωση καθυστέρησης σήματος. Επιπλέον, οι συχνές αλλαγές της τοπολογίας δικτύου κάνουν πολύ πιο δύσκολη την εφαρμογή αποτελεσματικών πρωτοκόλλων δρομολόγησης (routing protocols) προκειμένου να διατηρηθεί τόσο η αυξημένη αξιοπιστία που απαιτείται αναφορικά με τα δεδομένα που μεταφέρονται καθώς και η συνδεσιμότητα του δικτύου.

Τέλος, η ιδέα ότι τα ΣμηΕΑ μπορούν να επικοινωνούν λογικά, συνεπάγεται τη δημιουργία ανησυχιών σχετικά με την ασφάλεια και το απόρρητο των στοιχείων των ΣμηΕΑ και των δεδομένων που αυτά συλλέγουν, φέρουν και μεταφέρουν. Δεδομένων των υπαρκτών περιορισμών αναφορικά με την κατανάλωση ενέργειας και τις υπολογιστικές δυνατότητες των ΣμηΕΑ, η ελαφρά κρυπτογραφία και οι λύσεις ασφαλείας κρίνονται ως ιδιαίτερα σημαντικές

Συνολικά προτείνεται το IoD να επιτρέπει την ανάπτυξη δικτύων αποτελούμενων από ετερογενείς συσκευές και διασυνδεδεμένα ΣμηΕΑ, με τον ταυτόχρονο σχεδιασμό κατανομής πόρων μεταξύ των τρίτων μερών που συμμετέχουν σε ένα δίκτυο IoD (εταιρείες, υπηρεσίες κ.λπ).

2. Εισαγωγή στα ΣμηΕΑ

2.1 Τύποι και Χαρακτηριστικά των Σμηεα

Τα ΣμηΕΑ, ευρύτερα γνωστά ως drones, είναι διαθέσιμα τόσο σε διαφορετικά μεγέθη και σχεδιαστικές προσεγγίσεις όσο και σε προδιαγραφές (Εικόνα 1).

Μπορούν να αναπτυχθούν με ταχύτητα, μόλις παρουσιαστεί η ανάγκη, ένα χαρακτηριστικό το οποίο τα καθιστά ιδανικά για την παροχή συνδεσιμότητας ασύρματων τηλεπικοινωνιών αλλά και για πληθώρα άλλων εφαρμογών. Στο παρόν κεφάλαιο θα εξετάσουμε τα χαρακτηριστικά και τις δυνατότητες ορισμένων διαδεδομένων μοντέλων ΣμηΕΑ, με ιδιαίτερη έμφαση στην επίδρασή τους στις υποστηριζόμενες από ΣμηΕΑ κυψελοειδείς επικοινωνίες, καθώς αυτού του είδους οι επικοινωνίες είναι εξέχουσας σημασίας για τη διαμόρφωση και λειτουργία του Διαδικτύου των ΣμηΕΑ (Internet of Drones – IoD).

2.1.1 Ωφέλιμο Φορτίο (Payload)

Το ωφέλιμο φορτίο αναφέρεται στο μέγιστο βάρος που μπορεί να φέρει ένα ΣμηΕΑ, το οποίο είναι δείκτης της ανυψωτικής του ικανότητας. Το ωφέλιμο φορτίο των ΣμηΕΑ κυμαίνεται από μερικά γραμμάρια έως εκατοντάδες κιλά, συνεπώς η δυνατότητα ανύψωσης μεγαλύτερου ωφέλιμου φορτίου συνεπάγεται περισσότερο εξοπλισμό, μεγαλύτερο αεροσκάφος, μπαταρίες μεγαλύτερης χωρητικότητας και, συνήθως, μικρότερη διάρκεια πτήσης (ειδικά όταν αναφερόμαστε σε ΣμηΕΑ που λειτουργούν με τη χρήση ηλεκτρικής ενέργειας και όχι με άλλου τύπου καύσιμα).

Στα συνήθη εξαρτήματα του ωφέλιμου φορτίου περιλαμβάνονται κάμερες (οπτικές, θερμικές, wide), μία πλειάδα αισθητήρων (αποστασιόμετρο, GPS, αισθητήρες εντοπισμού αερίων) καθώς και τα λεγόμενα «ειδικά φορτία» (ειδικός φωτισμός, μεγάφωνα, συστήματα ψεκασμού, εκτόξευσης σπόρων για δένδροφύτευση, πυρόσβεσης κ.ά.), τα οποία, είτε κατά μονάς είτε συνδυαστικά χρησιμοποιούνται για πολλές και διαφορετικές αποστολές όπως αναγνώριση προσώπων και αντικειμένων, επιτήρηση καθώς και για αμιγώς εμπορικές και επιχειρηματικές χρήσεις.

Κατά την υποστήριξη κυψελοειδών επικοινωνιών (cellular communications), τα ΣμηΕΑ μπορούν να φέρουν αντίστοιχες συμβατές συσκευές όπως κινητά τηλέφωνα και tablets, των οποίων το βάρος είναι συνήθως χαμηλότερο του ενός κιλού. Τα ΣμηΕΑ μπορούν επίσης να φέρουν εναέριες βάσεις επικοινωνιών (aerial Base Stations) ή αναμεταδότες ραδιοφωνικού σήματος (remote radio heads – RHHs) προκειμένου να παρέχουν υπηρεσίες κυψελοειδών επικοινωνιών. Στην τελευταία αυτή περίπτωση, το ωφέλιμο φορτίο θα είναι τουλάχιστον μερικά κιλά. [1]

2.1.2 Μηχανισμός πτήσης

Ανάλογα με τον τύπο του μηχανισμού πτήσης που χρησιμοποιεί κάθε ΣμηΕΑ, αυτό κατηγοριοποιείται σε έναν από τους ακόλουθους τρεις τύπους:

Πολλαπλών ροτόρων (ελίκων): πραγματοποιεί κάθετη απογείωση & προσγείωση, μπορεί να πραγματοποιήσει υπερπτήσεις επάνω από ένα συγκεκριμένο σημείο ώστε να εκτελεί συγκεκριμένες αποστολές όπως βιντεοσκοπήσεις, λήψεις φωτογραφιών αλλά και να παρέχει επέκταση τηλεπικοινωνιακού σήματος.

Η δυνατότητα εύκολης μετακίνησης των ΣμηΕΑ τα καθιστά ιδανικά για την υποστήριξη των κυψελοειδών επικοινωνιών, καθώς μπορούν να χρησιμοποιηθούν ως

Σταθμοί Βάσης (Base Stations) με μεγάλη αποτελεσματικότητα και ακρίβεια ή να μεταφέρουν Σταθμούς Βάσης.

Από την άλλη μεριά, τα ΣμηΕΑ πολλαπλών ροτόρων έχουν χαμηλή εμβέλεια και καταναλώνουν μεγάλη ποσότητα ενέργειας καθώς, βάσει μηχανικής, πετούν αντιμετωπίζοντας συνεχώς τη δύναμη της βαρύτητας.

Σταθερής πτέρυγας (fixed wing drones): Τα ΣμηΕΑ αυτού του τύπου «γλιστρούν» στον αέρα, γεγονός το οποίο τα καθιστά, από την άποψη της κατανάλωσης ενέργειας, περισσότερο αποτελεσματικά και ικανά να φέρουν μεγαλύτερο ωφέλιμο φορτίο ενώ ταυτόχρονα, λόγω κατασκευής, τα ΣμηΕΑ σταθερής πτέρυγας ταξιδεύουν με μεγαλύτερη ταχύτητα.

Εκτός από τα ανωτέρω πλεονεκτήματα, τα ΣμηΕΑ σταθερής πτέρυγας έχουν και σημαντικά μειονεκτήματα:

1. Απαιτείται η ύπαρξη διαδρόμου απογείωσης/προσγείωσης καθώς η κάθετη απογείωση/προσγείωση δεν είναι δυνατή.
2. Δεν μπορούν να πραγματοποιήσουν υπερπήδηση επάνω από ένα σταθερό σημείο ενδιαφέροντος
3. Είναι περισσότερο κοστοβόρα τόσο στην κατασκευή όσο και στη συντήρηση, συγκρινόμενα με τα ΣμηΕΑ πολλαπλών ροτόρων.\

Υβριδικά ΣμηΕΑ σταθερής πτέρυγας/ροτόρων (fixed/rotary wing drones): Ο συγκεκριμένος τύπος ΣμηΕΑ δημιουργήθηκε προκειμένου να καλύψει το λειτουργικό κενό ανάμεσα στους άλλους δύο τύπου. Ένα από τα πρώτα σκάφη αυτού του τύπου είναι το Parrot Swing, το οποίο απογειώνεται κάθετα, στη συνέχεια κατευθύνεται στον προορισμό του χρησιμοποιώντας την πτήση σταθερής πτέρυγας και στη συνέχεια πραγματοποιεί υπερπήδηση επάνω από το σημείο ενδιαφέροντος με τη χρήση τεσσάρων ροτόρων (Εικόνα 1)



Εικόνα 1: Το Parrot Swing, υβριδικό ΣμηΕΑ, με δυνατότητα πτήσης με ρόtores και σταθερή πτέρυγα

2.1.3 Εμβέλεια και Υψόμετρο

Η εμβέλεια ενός ΣμηΕΑ αναφέρεται στην απόσταση στην οποία μπορεί να φτάσει το σκάφος ενώ ταυτόχρονα συνεχίζει να ελέγχεται επαρκώς εξ αποστάσεως. Η εμβέλεια ενός ΣμηΕΑ κυμαίνεται από μερικά μέτρα, για τα μικρά ΣμηΕΑ έως αρκετά χιλιόμετρα για τα μεγάλα μεγέθους (κυρίως αυτά της σταθερής πτέρυγας).

Το υψόμετρο αναφέρεται στο μέγιστο ύψος από την επιφάνεια της θάλασσας το οποίο μπορεί να προσεγγίσει ένα ΣμηΕΑ, υπό ιδανικές καιρικές συνθήκες και ανεξάρτητα από τους κατά τόπους εθνικούς κανονισμούς.

Το μέγιστο υψόμετρο πτήσης ενός ΣμηΕΑ είναι καίρια παράμετρος αναφορικά με τις κυψελοειδείς τηλεπικοινωνίες καθώς ένα ΣμηΕΑ που λειτουργεί ως σταθμός βάσης τηλεπικοινωνιών οφείλει να μεταβάλλει το ύψος πτήσης προκειμένου να μεγιστοποιεί την γεωγραφική κάλυψη που παρέχει και να ικανοποιεί διαφορετικές προδιαγραφές ποιότητας τηλεπικοινωνιών (QoS). Αναφορικά με το υψόμετρο, τα ΣμηΕΑ διαχωρίζονται σε δύο κατηγορίες:

Πλατφόρμες χαμηλού υψομέτρου (Low-altitude platforms – LAPs), οι οποίες αναφέρονται σε ΣμηΕΑ τα οποία συνήθως χρησιμοποιούνται για την υποστήριξη κυψελοειδών τηλεπικοινωνιών καθώς είναι πιο αποδοτικές και μπορούν να αναπτυχθούν γρήγορα «επί του πεδίου». Επιπλέον τα LAPs συνήθως παρέχουν σύνδεση χαμηλής εμβέλειας και σε ευθεία, άμεση οπτική επαφή (line-of-sight – LOS), το οποίο αυξάνει την απόδοση.

Πλατφόρμες μεγάλου υψομέτρου (HAPs), όπως τα «μπαλόνια επικοινωνιών», έτσι και οι HAPs μπορούν επίσης να παρέχουν κυψελοειδή συνδεσιμότητα. Σε σύγκριση με τις LAPs, τα HAPs έχουν δυνατότητα ευρύτερης γεωγραφικής κάλυψης, και μπορούν να παραμείνουν για μεγαλύτερο διάστημα εν πτήση.

Ωστόσο, η ανάπτυξη HAP είναι πιο περίπλοκη και θεωρούνται κυρίως ως μέσο παροχής σύνδεσης στο διαδίκτυο σε μεγάλα τμήματα πληθυσμού τα οποία είτε λόγω γεωγραφικής θέσης είτε λόγω έκτακτων συνθηκών (φυσικές καταστροφές κ.λπ), δεν έχουν πρόσβαση σε δίκτυα κινητής τηλεφωνίας.

Επιπλέον, η ανάπτυξη HAPs για την παροχή σήματος κινητής τηλεφωνίας (κυψελοειδή συνδεσιμότητα) μπορεί να προκαλέσει ολική πτώση του δικτύου κινητής τηλεφωνίας λόγω μεγάλων παρεμβολών μεταξύ των κυψελών. Για αυτόν τον λόγο τα HAPs χρησιμοποιούνται, όπως αναφέραμε παραπάνω, κυρίως για την παροχή σύνδεσης στο διαδίκτυο από εταιρείες (π.χ. Google ή Facebook). [1]

2.1.4 Ταχύτητα και χρόνος πτήσης

Τα μικρά ΣμηΕΑ κινούνται συνήθως με ταχύτητες κάτω από 15 m/s, ενώ τα μεγάλα drones μπορούν να φτάσουν σε εντυπωσιακές ταχύτητες μεγαλύτερες από 100 m/s. Όταν ένα ΣμηΕΑ το οποίο λειτουργεί ως σταθμός βάσης τηλεπικοινωνιών (base station) σε καθορισμένη τροχιά για τη μεγιστοποίηση τόσο της ενεργειακής όσο και της φασματικής του απόδοσης, η ταχύτητά του πρέπει να εξετάζεται προσεκτικά εάν η τροχιά κίνησης απαιτεί υψηλές ταχύτητες.

Ο μέγιστος παραμονής στον αέρα ενός ΣμηΕΑ χωρίς επαναφόρτιση ή ανεφοδιασμό αναφέρεται ως χρόνος πτήσης ή αντοχή πτήσης. Μικρά εμπορικά ΣμηΕΑ συνήθως έχουν χρόνο πτήσης 25-45 λεπτά, ορισμένα μεγαλύτερα μπορούν να πετάξουν έως δύο ώρες ενώ κάποια ακόμα ισχυρότερα ξεπερνούν και αυτό το επίπεδο διάρκειας πτήσης.

Η εξέλιξη της τεχνολογίας στις μπαταρίες και στα είδη των κινητήρων με τους οποίους εξοπλίζονται τα ΣμηΕΑ (κιροζίνης, φυσικού αερίου), έχουν παρατείνει την

διάρκεια πτήσης των ΣμηΕΑ. Ειδικά για τα μικρά ΣμηΕΑ, όπως π.χ. το Skyfront Tailwind, η διάρκεια πτήσης έχει φτάσει έως και τις 4,5 ώρες με υβριδικές-ηλεκτρικές πηγές ενέργειας. Παρ' όλα αυτά, η περιορισμένη διάρκεια πτήσης των υπαρχόντων μη προσαρμοσμένων (non-customized) και έτοιμων προς πώληση στην αγορά ΣμηΕΑ είναι επί του παρόντος ένας από τους σημαντικότερους πρακτικούς παράγοντες που περιορίζουν τη χρήση των μικρών ΣμηΕΑ για παροχή συνδεσιμότητας κινητής τηλεφωνίας. [1]

2.1.5 Παροχή ενέργειας

Η παροχή ενέργειας ενός ΣμηΕΑ καθορίζει σε μεγάλο βαθμό τον χρόνο πτήσης του. Ενώ οι επαναφορτιζόμενες μπαταρίες τροφοδοτούν τα περισσότερα εμπορικά ΣμηΕΑ, ορισμένα μεγάλα ΣμηΕΑ μπορούν να τροφοδοτούνται από καύσιμα όπως π.χ φυσικό αέριο, ώστε να πετυχαίνουν μεγαλύτερους χρόνους πτήσης.

Η χρήση ηλιακής ενέργειας για την τροφοδότηση των ΣμηΕΑ είναι μία υποσχόμενη προοπτική. Για τηλεπικοινωνιακούς σταθμούς βάσης ενσωματωμένους σε ΣμηΕΑ η τροφοδοσία ενέργειας πρέπει να υποστηρίζει ταυτόχρονα τόσο την πτητική λειτουργία του ΣμηΕΑ όσο και τον τηλεπικοινωνιακό εξοπλισμό, όπως η κεραία, ο ενισχυτής σήματος, τα ψηφιακά κυκλώματα κ.λπ. [1]

3. ΣμηΕΑ, δικτύωση και IoD

Τα μη επανδρωμένα εναέρια οχήματα (UAV/drones) είναι μια αναδυόμενη τεχνολογία που μπορεί να αξιοποιηθεί τόσο για στρατιωτικές όσο και για πολιτικές ή δημόσιες εφαρμογές. Η χρήση των ΣμηΕΑ από τον στρατό, σε παγκόσμιο επίπεδο, χρονολογείται ήδη από το 1990, κυρίως για την επόπτευση συνόρων, την αναγνώριση προσώπων και πιθανώς επικίνδυνων καταστάσεων αλλά και για τη διαβίβαση εντολών από το κέντρο των αποφάσεων προς τις δυνάμεις που βρίσκονται «επί του πεδίου».

Η χρήση του από το δημόσιο κάθε κράτους γίνεται από υπηρεσίες όπως η αστυνομία, η πυροσβεστική και η πολιτική προστασία για την παροχή δημόσιας ασφάλειας, για την καλύτερη διαχείριση των μεταφορών αλλά και για την προειδοποίηση και επόπτευση της κατάστασης πριν και κατά τη διάρκεια φυσικών καταστροφών. Ειδικά για την τελευταία περίπτωση, τα ΣμηΕΑ μπορούν να παρέχουν καίρια υποστήριξη σε επιχειρήσεις έρευνας και διάσωσης όταν τα δίκτυα τηλεπικοινωνιών έχουν υποστεί σοβαρές φθορές όπως, π.χ. από έναν μεγάλο σεισμό, μία δασική πυρκαγιά ή ένα τσουνάμι. Στις δασικές πυρκαγιές και την προστασία της άγριας πανίδας, τα ΣμηΕΑ μπορούν να προσεγγίσουν σημεία όπου οι επίγειες δυνάμεις θα ήταν σχεδόν αδύνατο να επέμβουν, όχι μόνο λόγω της φωτιάς αλλά και των δηλητηριωδών αερίων που εκλύονται από την καύση των υλικών του δάσους.

Τα ΣμηΕΑ όμως μπορούν να έχουν και ενεργή συμμετοχή στις αποστολές έρευνας και διάσωσης με τη μεταφορά ιατροφαρμακευτικού εξοπλισμού σε περιοχές όπου είτε η πρόσβαση είναι αδύνατη, λόγω καταστροφών, είτε η μεταφορά τους με άλλο τρόπο θα ήταν εξαιρετικά χρονοβόρα.

Για την εκτέλεση όλων αυτών των αποστολών, χρησιμοποιούνται ΣμηΕΑ όλων των τύπων και των μεγεθών, ανάλογα με την αναγκαιότητα, με τα μεγάλα ΣμηΕΑ να εκτελούν συνήθως αποστολές «κατά μόνος» ενώ τα μικρότερα εκτελούν αποστολές σε σμήνη. Τα σμήνη ΣμηΕΑ έχουν αποδειχθεί εξαιρετικά χρήσιμα σε πολιτικές εφαρμογές.

Χαρακτηριστικό παράδειγμα διαφοροποίησης χρήσης είναι η χρήση των ΣμηΕΑ «κατά μόνος» από την αστυνομία ή την πυροσβεστική σε καταστάσεις έκτακτης ανάγκης σε αντιπαραβολή με τη χρήση σμηνών ΣμηΕΑ για την επόπτευση της οδικής κυκλοφορίας ή για την μέτρηση καιρικών δεδομένων. Τα σμήνη ΣμηΕΑ έχουν τραβήξει το ενδιαφέρον της διεθνούς επιστημονικής και επιχειρηματικής κοινότητας μετά τις ραγδαίες εξελίξεις στον τομέα των αισθητήρων, της τεχνητής νοημοσύνης και της ηλεκτρονικής, που κατέστησαν την κατασκευή πολύπλοκων ψηφιακών συστημάτων οικονομικότερη και σε πολύ μικρότερο μέγεθος από το παρελθόν. [2]

3.1 Προκλήσεις και δυσκολίες για τα δίκτυα ΣμηΕΑ

Παρότι η ανάπτυξη δικτύων (σμηνών) ΣμηΕΑ μπορεί να ακούγεται ως «η εύκολη λύση» για μία πληθώρα καθημερινών προβλημάτων, στην πραγματικότητα οι δυσκολίες, τεχνικές και θεσμικές, είναι πολλές και πολύπλοκες.

Στις θεσμικές δυσκολίες περιλαμβάνονται οι κανονισμοί για την πτήση των ΣμηΕΑ, οι οποίοι, με εξαίρεση την πτήση σε απομακρυσμένες περιοχές, για την Ελλάδα ουσιαστικά δεν υπάρχουν ενώ, ακόμα και στο εξωτερικό, οι θεσμικές διαφορές δεν είναι ιδιαίτερα μεγάλες. (Σημ.: Στην παρούσα εργασία δεν θα ασχοληθούμε με τις θεσμικές δυσκολίες καθώς δεν συνδέονται με την τεχνολογία του IoD ή των ΣμηΕΑ αλλά αποτελούν κυρίως πολιτικό και τεχνοκρατικό ζήτημα).

Αναφορικά τις τεχνικές δυσκολίες, σε αντίθεση με άλλα ασύρματα δίκτυα, η τοπολογία των δικτύων ΣμηΕΑ είναι ακανόνιστη, ρευστή καθώς ο αριθμός των συσκευών που εισέρχονται στο δίκτυο καθώς και οι θέσεις τους αλλάζουν σε πραγματικό χρόνο.

Επίσης, ανάλογα με την αποστολή που είναι εντεταλμένο ένα δίκτυο ΣμηΕΑ να εκτελέσει, η ταχύτητα που κινείται κάθε σκάφος μπορεί να είναι διαφορετική από το ένα στο άλλο, με αποτέλεσμα η μορφοποίηση του δικτύου να αλλάζει συνεχώς.

Η ρευστή τοπολογία του δικτύου καθώς και η ακανόνιστη είσοδος και αποχώρηση κάθε συσκευής από το δίκτυο, σχεδόν αυτόματα ξεπερνά την διαμόρφωση του παραδοσιακού “ad hoc” δικτύου.

Επιπλέον, τα πρωτόκολλα δρομολόγησης δικτύου, δεν μπορούν να είναι σταθερά καθώς το δίκτυο ΣμηΕΑ πρέπει να αναπροσαρμόζεται συνεχώς λόγω της συνεχούς αλλαγής του αριθμού, της ταχύτητας και της θέσης των ΣμηΕΑ μέσα στο δίκτυο.

Τέλος, η επικοινωνία των χρηστών του δικτύου με τα ΣμηΕΑ του δικτύου πρέπει να πραγματοποιείται απρόσκοπτα, ανεξάρτητα από το ποιο ΣμηΕΑ παραμένει στο δίκτυο και ποιο αποχωρεί.

Γίνεται λοιπόν εύκολα αντιληπτό ότι το IoD, όσο και αν φαίνεται πως είναι μία «επέκταση» του IoT, στην πραγματικότητα είναι μία εντελώς διαφορετική, εντελώς ξεχωριστή και ανεξάρτητη κατηγορία δικτύωσης ασύρματων (και ενσύρματων) μη επανδρωμένων συσκευών, με δικές της ανάγκες επικοινωνίας, κανονισμού και διαμόρφωσης.

3.2 Κύρια ζητήματα

Στα δίκτυα κινητής τηλεφωνίας αλλά και στα δίκτυα οχημάτων, οι κόμβοι του δικτύου (οι συσκευές του δικτύου, τηλέφωνα και αυτοκίνητα), εισέρχονται και εξέρχονται συχνά από το δίκτυο και αυτό προκάλεσε την ανάπτυξη της τεχνολογίας των ad hoc δικτύων, η οποία έλυσε σε μεγάλο βαθμό το πρόβλημα της σταθερότητας του σήματος και της επικοινωνίας των συσκευών με το κεντρικό δίκτυο (backbone).

Τα ΣμηΕΑ, όταν λειτουργούν υπό μορφή σμήνους, μπορούν να παραμένουν σχεδόν ακίνητα επάνω από μία περιοχή ή να κινούνται προς μία κατεύθυνση με ταχύτητα ενώ ταυτόχρονα κάποια από αυτά θα αποχωρούν από το δίκτυο (λόγω βλαβών ή λόγω μείωσης διαθέσιμης ενέργειας) και θα αντικαθίστανται από άλλα.

Τα δίκτυα ΣμηΕΑ, παρόλο που έχουν αρκετές ομοιότητες με τα ασύρματα δίκτυα κινητών συσκευών (Mobile Ad hoc Networks – MANETs) και οχημάτων (Vehicular Ad hoc Networks – VANETs), ταυτόχρονα έχουν και πολλές διαφορές. Ο πίνακας 1 περιέχει μία συνοπτική σύγκριση και καταγραφή ομοιοτήτων και διαφορών ανάμεσα στα δίκτυα ΣμηΕΑ, στα MANETs και στα VANETs.

	MANET	VANET	Δίκτυα ΣμηΕΑ
Περιγραφή	Κινητοί ασύρματοι κόμβοι συνδέονται μεταξύ τους ad-hoc (Δεν απαιτείται η ύπαρξη κεντρικής υποδομής - backbone)	Ad-hoc δίκτυα στα οποία τα οχήματα είναι οι κόμβοι του δικτύου. Η επικοινωνία πραγματοποιείται τόσο μεταξύ των οχημάτων όσο και με συστήματα παραπλεύρως του δρόμου	Δίκτυα Ad-hoc ή Infrastructure based μεταξύ αερομεταφερόμενων κόμβων. Η επικοινωνία πραγματοποιείται τόσο μεταξύ των ΣμηΕΑ όσο και με τον σταθμό ελέγχου.
Κινητικότητα	Χαμηλή. Τυπικές ταχύτητες 2 m/sec. Τυχαία κίνηση. Εναλλασσόμενη Πυκνότητα κόμβων, υψηλότερη σε σημεία υψηλής συγκέντρωσης	Υψηλή ταχύτητα, τυπικά 20-30 m/s στους αυτοκινητόδρομους, 6-10 m/s σε αστικές περιοχές. Προβλέψιμο δίκτυο, περιορισμένο από τη χάραξη του δρόμου, την κυκλοφορία οχημάτων και τον Κ.Ο.Κ	Ταχύτητες από 0 m/sec έως και 100 m/s. Η κίνηση του κόμβου (ΣμηΕΑ) μπορεί να πραγματοποιείται σε 2 ή 3 διαστάσεις. Συνήθως η κίνηση ακολουθεί τις ανάγκες της αποστολής που εκτελείται.
Τοπολογία	Τυχαία, ad-hoc	Τοπολογία «Αστέρα» με τις οδικές υποδομές επικοινωνίας οχημάτων που βρίσκονται παραπλεύρως του οδού και τοπολογία "ad-hoc" μεταξύ των οχημάτων	Τοπολογία «Αστέρα» με το κέντρο ελέγχου, τοπολογία "ad-hoc/mesh" μεταξύ των ΣμηΕΑ.
Αλλαγές τοπολογίας	Δυναμική τοπολογία, οι κόμβοι του δικτύου εισέρχονται και αποχωρούν απρόβλεπτα. Δίκτυο επιρρεπές στον κατακερματισμό.	Πιο δυναμική τοπολογία από αυτή των MANETS. Γραμμική κίνηση των κόμβων.	Εναλλασσόμενη σε ταχύτητα από σταθερή έως πολύ γρήγορη. Μπορεί να χρησιμοποιηθεί σε ελεγχόμενα σμήνη ΣμηΕΑ. Δίκτυο επιρρεπές στον κατακερματισμό.
Ενεργειακοί περιορισμοί	Οι περισσότεροι κόμβοι του δικτύου χρησιμοποιούν μπαταρίες, συνεπώς οι ενεργειακές ανάγκες πρέπει να λαμβάνονται υπόψη	Οι κόμβοι μπορούν να τροφοδοτούνται είτε από τη δική τους είτε από την μπαταρία του οχήματος.	Τα μικρά ΣμηΕΑ έχουν περιορισμούς λόγω παροχής ενέργειας από μπαταρίες, η χρήση των οποίων επηρεάζει το ωφέλιμο φορτίο του ΣμηΕΑ και τη διάρκεια πτήσης.
Τυπική χρήση από δημόσιους και ιδιωτικούς φορείς	<ul style="list-style-type: none"> Διάχυση πληροφορίας (καταστάσεις έκτακτης ανάγκης, διαφήμιση, αγορές, εκδηλώσεις) internet hot-spots 	<ul style="list-style-type: none"> Πληροφορίες κυκλοφορίας οχημάτων & καιρού, προειδοποιήσεις σε καταστάσεις έκτακτης ανάγκης, Υπηρεσίες βάσει τοποθεσίας Infotainment 	Επιχειρήσεις έρευνας & διάσωσης Έξυπνη Γεωργία-επόπτευση καλλιεργειών Έρευνας άγριας πανίδας Επόπτευση εγκαταστάσεων άντλησης πετρελαίου & φυσικού αερίου

Πίνακας 1: Συγκριτική περιγραφή διαφορετικών ad hoc δικτύων [2]

Από τον Πίνακα 1 εξάγεται εύκολα το συμπέρασμα ότι υπάρχουν πολλά στοιχεία των δικτύων ΣμηΕΑ τα οποία τα διαχωρίζουν από τα ασύρματα ad-hoc και τα οχηματικά ad-hoc δίκτυα. Οι κύριες διαφορές είναι:

Τα μοντέλα κινητικότητας, όπως η μέθοδος των «τυχαίων περιπάτων» (random walks), που έχουν χρησιμοποιηθεί για να περιγράψουν τη συμπεριφορά των κόμβων σε ασύρματα ad-hoc δίκτυα και η μέθοδος του «οδικού τυχαίου περιπάτου» (street random walk) aka «Μοντέλο Manhattan» για τα οχηματικά ad-hoc δίκτυα, δεν είναι μέθοδοι απόλυτα κατάλληλοι για τα δίκτυα ΣμηΕΑ. Τα ΣμηΕΑ μπορούν να κινηθούν τυχαία ή σε οργανωμένο σμήνη όχι μόνο σε δύο αλλά και σε τρεις διαστάσεις με ταχύτατη μεταβολή της θέσης τους ενώ τα οχήματα (οχηματικοί κόμβοι – vehicular nodes), είναι περιορισμένα να κινούνται επί των οδών και μόνο σε δύο διαστάσεις.

Οι αλλαγές στην τοπολογία του δικτύου όπως και οι σχετικές θέσεις των ΣμηΕΑ μπορούν να αλλάζουν με μεγάλη ταχύτητα. Ορισμένα ΣμηΕΑ μπορεί να αποφορτιστούν εντελώς και να απαιτηθεί η προσγείωσή τους για επαναφόρτιση ενώ κάποια άλλα μπορεί να παρουσιάσουν βλάβες και να τεθούν εκτός δικτύου. Η σύνδεση μεταξύ των ΣμηΕΑ μπορεί να πραγματοποιηθεί ή να διακοπεί επίσης με μεγάλη συχνότητα λόγω της ταχείας μεταβολής θέσης των κόμβων του δικτύου ενώ σε πολλές περιπτώσεις η πυκνότητα των κόμβων μπορεί να μην είναι υψηλή και το δίκτυο να «πέφτει» περιοδικά.

Στην περίπτωση των οχηματικών δικτύων, υπάρχει τηλεπικοινωνιακή υποδομή παραπλεύρως των δρόμων για την υποστήριξη της επικοινωνίας μεταξύ των οχημάτων. Στην περίπτωση όμως των ΣμηΕΑ, με το δίκτυο μεταξύ τους να είναι ρευστό, οι τηλεπικοινωνιακοί σταθμοί βάσης οι οποίοι είναι συνδεδεμένοι με ένα συγκεκριμένο ΣμηΕΑ θα χρειαστεί να συνδεθούν με ένα άλλο σκάφος χωρίς να διακοπούν τα user sessions, γεγονός το οποίο αποτελεί σημείο πολλών επιστημονικών ερευνών αναφορικά με τη βέλτιστη μέθοδο επίτευξης αυτής τη ομαλής μετάβασης του σήματος από τον ένα σταθμό βάσης στον άλλο.

Οι περιορισμοί ενέργειας είναι πολύ μεγαλύτεροι στα μικρά δίκτυα ΣμηΕΑ, ενώ στα οχηματικά δίκτυα η ενέργεια για τη λειτουργία τους παρέχεται σε μεγάλο βαθμό από την μπαταρία του οχήματος η οποία φορτίζεται όσο το όχημα βρίσκεται εν κινήσει. Ακόμα και στην περίπτωση των ad-hoc ασύρματων δικτύων κινητής τηλεφωνίας, οι κόμβοι του δικτύου (έξυπνα κινητά τηλέφωνα, tablets) έχουν μπαταρίες ικανές να διατηρήσουν τις συσκευές του δικτύου εν λειτουργία για αρκετές ώρες, ενώ τα μικρά ΣμηΕΑ συνήθως έχουν επαρκή ενέργεια για μία πτήση μόλις λίγων λεπτών.

Από τη μία, το σήμα επικοινωνίας θα είχε χαμηλότερη ισχύ και από την άλλη τα ΣμηΕΑ του δικτύου θα αποσυνδέονταν από το δίκτυο λόγω της μείωσης της ενέργειάς τους και της απενεργοποίησής τους. Η δυναμικότητα των κόμβων σε ένα δίκτυο ΣμηΕΑ προκαλεί την συνεχή επανοργάνωση του δικτύου, γεγονός το οποίο ωθεί σε ιδιαίτερες απαιτήσεις δρομολόγησης με τα πρωτόκολλα επικοινωνίας να αναγκάζονται σε πιο αποτελεσματική χρήση της ενέργειας των ΣμηΕΑ ώστε να αυξάνεται η σταθερότητα του δικτύου ΣμηΕΑ.

Τα δίκτυα ΣμηΕΑ συνήθως αναπτύσσονται και χρησιμοποιούνται σε έκτακτες καταστάσεις όπου το δίκτυο κατατμείται συχνά, ορισμένες φορές για μεγάλα χρονικά διαστήματα. Σε αυτές τις περιπτώσεις λοιπόν, οι παραδοσιακές λύσεις δικτύωσης δεν εγγυώνται τη συνδεσιμότητα στο δίκτυο. Έχει προταθεί η λύση της χρήσης δυνατοτήτων "store-carry-forward" (αποθήκευσης – μεταφοράς) και αυτή η λύση όμως έχει προβλήματα. Αν υιοθετήσουμε τη λύση κάθε κόμβος του δικτύου να έχει πλήρη γνώση της τοπολογίας του δικτύου, θα μπορούσαμε να εφαρμόσουμε ντετερμινιστικά πρωτόκολλα επικοινωνίας, αλλά αυτή δεν είναι απαραίτητα η βέλτιστη επιλογή. Αν υποθέσουμε ότι οι κόμβοι του δικτύου έχουν τυχαία συμπεριφορά, θα αντιμετωπίσουμε προβλήματα επεκτασιμότητας του δικτύου ΣμηΕΑ.

Ένα δίκτυο πολλαπλών ΣμηΕΑ, το οποίο είναι πλήρως αυτόνομο, απαιτεί ένα ισχυρό πλέγμα επικοινωνίας μεταξύ των ΣμηΕΑ τα οποία θα συνεργάζονται ώστε να διατηρούν οργανωμένο το δίκτυο ακόμα και στην περίπτωση που θα «πέσει» μία σύνδεση ή θα υποστεί βλάβη ένας κόμβος του δικτύου.

Τα δίκτυα ΣμηΕΑ θα απαιτήσουν αλλαγές στο επίπεδο MAC των ΣμηΕΑ όπως και στο επίπεδο της δικτύωσής τους. Θα απαιτήσουν δυνατότητες αυτό-οργάνωσης, αντοχή στις καθυστερήσεις σήματος επικοινωνίας, περισσότερη ευελιξία και έλεγχο σε επίπεδο SDN (Software Defined Networking) αλλά και την ανάπτυξη νέων τεχνολογιών για τον περιορισμό της κατανάλωσης ενέργειας κατά την εκτέλεση των αποστολών τους. Αυτό περιλαμβάνει τόσο τα ΣμηΕΑ που λειτουργούν με μπαταρίες, όπου το πρόβλημα της διαθέσιμης ενέργειας είναι πιο έντονο, όσο και τα ΣμηΕΑ που χρησιμοποιούν υγρά καύσιμα. [2]

3.3 Τι είναι το Διαδίκτυο των ΣμηΕΑ (IoD – Internet of Drones)

Ο όρος «Διαδίκτυο των ΣμηΕΑ» (IoD) διαμορφώθηκε ως εξέλιξη του «Διαδικτύου των Πραγμάτων» (IoT) αντικαθιστώντας τη λέξη «πράγματα» με τη λέξη «ΣμηΕΑ» (Drones), το οποίο όμως διαθέτει παρόμοιες ιδιότητες (τεχνικές, προγραμματιστικές, τοπολογίας κ.λπ) και αναμένεται να αποτελέσει το ορόσημο για την περαιτέρω ανάπτυξη των ΣμηΕΑ.

Το IoD έχει χαρακτηριστεί ως «αρχιτεκτονική ελέγχου δικτύου σε επίπεδα» [3], η οποία υποστηρίζει τον συντονισμό των ΣμηΕΑ τόσο μεταξύ τους όσο και με τους υπόλοιπους κόμβους του δικτύου.

Στο περιβάλλον του IoD, πολλά και διαφορετικά ΣμηΕΑ συνδέονται, επικοινωνούν, ανταλλάσσουν δεδομένα και διαμορφώνουν ένα δίκτυο.

Το IoD παρέχει τη δυνατότητα ελέγχου του από απόσταση ή μέσω διαδικτύου με διεύθυνση IP.

Τα ΣμηΕΑ «ανοίγουν το δρόμο» σε πολλές εφαρμογές ενώ ταυτόχρονα αποκαλύπτουν μία σειρά προκλήσεων στην υιοθέτηση της χρήσης τους, της σχεδίασης και της ανάπτυξης.

Ενδεικτικοί τομείς χρήσης ΣμηΕΑ
Επικοινωνίες (Telecoms)
Υπηρεσίες ασφαλείας (Security)
Περιβάλλον (Environment)
Επιμελητείας ή εφοδιασμού (Logistics)
Στρατιωτικές και Αμυντικές εφαρμογές (Military and Defensive applications)
Υπηρεσίες υγείας (Health services)
Έλεγχος εναέριας κυκλοφορίας (Air Traffic Control)
Εφαρμογές κινητής τηλεφωνίας (Mobile communications)

Πίνακας 2: Ενδεικτικοί τομείς χρήσης ΣμηΕΑ

Η αρχιτεκτονική σχεδίαση της επικοινωνίας των ΣμηΕΑ υπολείπεται σε ενοποίηση και standards από τα άλλα δίκτυα που γνωρίζαμε έως σήμερα. Επίσης τα δίκτυα ΣμηΕΑ πάσχουν στην αποκλειστική χρήση του τηλεπικοινωνιακού φάσματος. Η ανάπτυξη δικτύου ΣμηΕΑ και ο σχεδιασμός διαδρομών πτήσης είναι ακόμα δύο θέματα που πρέπει να εξετάζονται κατά την χορήγηση φάσματος καθώς έχουν αντίκτυπο στην ενεργειακή απόδοση των ΣμηΕΑ.

Επιπλέον, οι UAV επικοινωνίες απαιτούν συνέπεια και μεγάλα, αξιόπιστα δίκτυα, μαζί με την απαραίτητη ασφάλεια. Το IoD μπορεί να θεωρηθεί ως σημαντική λύση στην υποστήριξη του συντονισμού των ΣμηΕΑ και σε άλλα ζητήματα σχετικά με τις UAV επικοινωνίες. Το IoD ενισχύει τις δυνατότητες αποθήκευσης και αυξάνει τη χρήση αλγοριθμικών λύσεων, οι οποίες επιτρέπουν την εφαρμογή λύσεων εμπνευσμένων από τη Μηχανική Μάθηση και την Τεχνητή Νοημοσύνη στους συνεργατικούς σχηματισμούς ΣμηΕΑ. Όσον αφορά τις εφαρμογές που μπορεί να χρησιμοποιηθεί το IoD, αυτές μπορεί να φτάνουν από την ρύθμιση του εναέριου χώρου έως την παροχή υπηρεσιών υψηλής αξιοπιστίας, ακρίβειας και πλοήγησης σε ΣμηΕΑ τα οποία ενεργούν σε τομείς όπως αυτοί στον πίνακα 2.

Επιπλέον, τεχνολογίες όπως τα δίκτυα μεγάλης εμβέλειας και ευρείας περιοχής (LoRaWAN - long-range wide-area), τα δίκτυα ευρείας περιοχής χαμηλής κατανάλωσης (LPWAN - low-power wide-area), και τα δίκτυα IoT «στενής ζώνης φάσματος» (NB IoT - NarrowBand IoT) μπορούν να «συγχωνευθούν» με το IoD και να παράξουν βιώσιμες λύσεις.

Το IoD, το οποίο έχει χαρακτηριστικά το χαμηλό κόστος, το μικρό μέγεθος των συσκευών και της υψηλής δυνατότητας αναδιαμόρφωσης, λειτουργικότητας και αμεσότητας στη διαθεσιμότητα, θεωρείται μεγάλη ευκαιρία για τα επόμενα χρόνια. Οι τάσεις της αγοράς κινούνται προς την υιοθέτηση του IoD με τα ακόλουθα χαρακτηριστικά:

- Να υποστηρίζει επικοινωνίες από συσκευή σε συσκευή καθώς και από συσκευή σε πολλές συσκευές ταυτόχρονα.
- Να διευκολύνει τη συνδεσιμότητα με τα υπόλοιπα σχετικά δίκτυα.
- Να μπορεί να λειτουργήσει ως υπηρεσία συλλογής δεδομένων και διαχείρισης πληροφοριών.
- Να βοηθά στην πλοήγηση και στη βελτίωση της ικανότητας λειτουργίας των οχημάτων μέσω του V2X ή V2V (λειτουργία Drone to Drone).

Ανεξάρτητα από την εξέλιξη στις επικοινωνίες ΣμηΕΑ και την πληθώρα των λύσεων που έχουν αναπτυχθεί και πρόκειται να αναπτυχθούν μέσα στα επόμενα χρόνια, η ασφάλεια παραμένει η κύρια ανησυχία για το IoD καθώς τα δεδομένα που μεταφέρονται μέσω των ΣμηΕΑ περιέχουν κρίσιμες πληροφορίες.

Τα ΣμηΕΑ συνήθως επιχειρούν λαμβάνοντας εντολές από τους σταθμούς βάσης και συντονίζονται μέσω του IoD. Όμως, ορισμένου τύπου αποστολές, εμπεριέχουν αυτόνομα ΣμηΕΑ. Σε αυτές τις περιπτώσεις, οι εντολές θα φτάνουν στα ΣμηΕΑ μέσω πολλών και διαφορετικών καναλιών επικοινωνίας και με διαφορετική συχνότητα αποστολής, γεγονός το οποίο απαιτεί επιπλέον επιστημονική ενασχόληση για τη διαχείριση και τον έλεγχο των ΣμηΕΑ που εκτελούν τέτοιες αποστολές. Συνεπώς, η ασφάλεια του IoD είναι το πιο σημαντικό προαπαιτούμενο προκειμένου να αναπτυχθούν μεγάλου μεγέθους λύσεις οι οποίες θα περιλαμβάνουν τη χρήση πολλαπλών ΣμηΕΑ. [4]

4. Φυσικό επίπεδο (Physical layer)

Σε αυτό το κεφάλαιο θα εξεταστούν οι βασικές τεχνολογικές παράμετροι του φυσικού επιπέδου (physical layer) του IoD, όπως είναι οι τεχνικές διαμόρφωσης, η συνδεσιμότητα, η μεγιστοποίηση απόδοσης, η μοντελοποίηση και ο χαρακτηρισμός καναλιών καθώς και οι Τεχνολογίες επικοινωνίας.

4.1 Τεχνικές διαμόρφωσης (Modulation techniques)

4.1.1 Βελτίωση ποιότητας σήματος (Signal quality enhancement)

Τα ΣμηΕΑ ελέγχονται είτε με τηλεχειρισμό από χειριστή πιλότο είτε αυτόνομα με μικροϋπολογιστές επί του σκάφους (on-board computers).

Ο τρόπος, το κανάλι επικοινωνίας των ΣμηΕΑ είναι παράγοντας ο οποίος μπορεί να επηρεάσει την απόδοση του συνδέσμου δεδομένων του ΣμηΕΑ (data link) αναφορικά με την ταχύτητα και την αξιοπιστία μεταφοράς των δεδομένων.

Συνεπώς, η αποτελεσματικότητα της επικοινωνίας των ΣμηΕΑ αντιπροσωπεύει μία από τις σημαντικότερες προκλήσεις σχετικά με ένα σύστημα επικοινωνίας βασισμένο σε ΣμηΕΑ (IoD).

Το σύστημα επικοινωνίας βασισμένο σε ΣμηΕΑ έχει τις ακόλουθες βασικές απαιτήσεις:

- Αποτελεσματικός σύνδεσμος μεταφοράς δεδομένων
- Λειτουργία μεγάλης εμβέλειας
- Αμφίδρομη επικοινωνία
- Χαμηλή καθυστέρηση μεταφοράς δεδομένων
- Μεγάλη διάρκεια πτήσης των ΣμηΕΑ
- Λειτουργικές δυνατότητες
- Αξιόπιστη επικοινωνία

Καθώς η μετάδοση των εντολών ελέγχου και των δεδομένων που συγκεντρώνονται από τα ΣμηΕΑ, τα οποία μπορούν να είναι βίντεο, φωτογραφίες, δεδομένα από άλλους αισθητήρες (φωτιάς, καπνού, τοξικών αερίων, μικρόφωνα), επιτυγχάνεται μέσω του καναλιού επικοινωνίας μεταξύ του UAV και του σταθμού ελέγχου εδάφους (GCS), μια σύνδεση δεδομένων ΣμηΕΑ απαιτεί την υψηλότερη δυνατή αξιοπιστία στη μετάδοση δεδομένων καθώς και υψηλό ρυθμό μεταφοράς τους.

Προκειμένου να παρέχεται μία αποτελεσματική σύνδεση επικοινωνίας μεταξύ ΣμηΕΑ και σταθμού εδάφους, πολλά ΣμηΕΑ χρησιμοποιούν τεχνολογία φάσματος η οποία επιτρέπει σε πολλούς και διαφορετικούς χειριστές – πιλότους να επιχειρούν στην ίδια ζώνη των 2,5 GHz, χωρίς να εμφανίζονται προβλήματα. Οι δέκτες που λειτουργούν σε αυτό το φάσμα είναι ουσιαστικά απρόσβλητοι στις παρεμβολές.

Ουσιαστικά, δύο τύποι διασποράς φάσματος χρησιμοποιούνται για τη σύνδεση επικοινωνίας των ΣμηΕΑ, ο FHSS και ο DSSS. Η σύγκρισή μεταξύ τους δεν πραγματοποιείται για να γίνει μία οριστική επιλογή αλλά για να γίνει επίδειξη των δυνατοτήτων τους και του τρόπου χρήσης κάθε μεθόδου, σε διαφορετικές περιπτώσεις η κάθε μία. (Μαζί με αυτούς θα παρουσιάσουμε και ορισμένες πρόσφατες εναλλακτικές λύσεις που έχουν προταθεί από την επιστημονική κοινότητα)

4.1.2 Φάσμα Διασποράς με εναλλαγή συχνότητας (FHSS – frequency-hopping spread spectrum)

Ο πρώτος είναι το «φάσμα διασποράς με εναλλαγή συχνότητας» (FHSS - frequency-hopping spread spectrum) όπου η narrowband συχνότητα αλλάζει πολλές φορές ανά δευτερόλεπτο εντός του εύρους συχνοτήτων των 2,4 GHz. Ο δέκτης αναγνωρίζει τα μοτίβα συχνότητας που χρησιμοποιούνται από έναν πομπό και επειδή ο πομπός αλλάζει συχνότητες μεταξύ μοτίβων, ο δέκτης μπορεί να υιοθετήσει την κατάλληλη συχνότητα.

4.1.3 Σύστημα Ευθείας Αλληλουχίας Ευρέως Φάσματος (DSSS – direct-sequence spread spectrum)

Σε αντίθεση με το FHSS, το «σύστημα ευθείας αλληλουχίας ευρέως φάσματος» (DSSS - direct-sequence spread spectrum) μπορεί να παρέχει εν γένει μεγαλύτερο εύρος ζώνης αλλά είναι πολύ ευαίσθητο σε περιβαλλοντικούς παράγοντες (θόρυβος, αντακλάσεις κ.λπ). Για το λόγο αυτό συνίσταται η χρήση του σε point-to-point εφαρμογές και κάνοντας χρήση κατευθυντικών κεραιών (δηλαδή κεραιών που δεν εκπέμπουν σε ακτίνα μεγάλου εύρους), όπου τα προβλήματα αυτά εμφανίζονται σε μικρότερη κλίμακα. [5]

Στο DSSS ο πομπός στέλνει ένα αρχικό σήμα narrowband μέσω μιας γεννήτριας παραγωγής κώδικα διασποράς η οποία πολλαπλασιάζει το σήμα χρησιμοποιώντας μία πολύ υψηλότερη συχνότητα.

Και στους δύο τύπους διασποράς φάσματος (FHSS και DSSS) το σήμα μεταδίδεται εντός της ζώνης συχνοτήτων των 2,4 GHz. Στην πράξη, η Ορθογώνια Πολύπλεξη Διαίρεσης Συχνοτήτων (OFDM- orthogonal frequency division multiplexing) έχει θεωρηθεί πιο αποτελεσματική από τα FHSS και DSSS λόγω της μεγαλύτερης ανοχής στην παραμόρφωση πολλαπλών διαδρομών, της υψηλότερης απόδοσης και του δυναμικού ρυθμού μετάδοσης δεδομένων.

4.1.4 Ορθογώνια Πολύπλεξη Διαίρεσης Συχνοτήτων (OFDM – Orthogonal Frequency Division Multiplexing)

Η Ορθογώνια Πολύπλεξη Διαίρεσης Συχνοτήτων (OFDM – Orthogonal Frequency Division Multiplexing) αποτελεί μία τεχνική διαμόρφωσης πολλαπλών φορέων (multicarrier modulation technique), η οποία έχει υιοθετηθεί σε ένα μεγάλο αριθμό τηλεπικοινωνιακών εφαρμογών. Βασικά πλεονεκτήματά της είναι η παροχή υψηλών ταχυτήτων πρόσβασης, η αποδοτική εκμετάλλευση του διαθέσιμου εύρους ζώνης, ο πολύ ικανοποιητικός τρόπος διαχείρισης των καναλιών πολυόδευσης (multipath channels) τόσο στη συχνότητα όσο και στο χρόνο, καθώς και η εξάλειψη τόσο της διασυμβολικής (InterSymbol Interference – ISI) όσο και της διακαναλικής (Intercarrier Interference – ICI) παρεμβολής. Η τεχνική OFDM εφαρμόζεται στα απαιτητικά συστήματα των ασύρματων επικοινωνιών, στις ενσύρματες επικοινωνίες (για παράδειγμα στο DSL), τις γραμμές ρεύματος (Power Line Communication – PLC) και αλλού, ενώ αποτελεί και τη βάση των συστημάτων 4^{ης} γενιάς. [6]

4.1.5 Πολλαπλή Πρόσβαση Διάρθρωσης Συχνότητας Μονού Φέροντος (SC-FDM – Single Carrier Frequency Division Multiplex)

Το SC-FDM είναι μια υβριδική τεχνική διαμόρφωσης που συνδυάζει την ευελιξία κατανομής συχνότητας και την διαχείριση των καναλιών πολυόδευσης της OFDM μαζί με άλλα σημαντικά χαρακτηριστικά μίας τεχνικής μονού φορέα.

Το κρίσιμο χαρακτηριστικό της παραγωγής σήματος SC-FDM είναι ότι το PAPR του σήματος μετατόπισης πεπερασμένης συχνότητας καταλήγει να είναι το ίδιο με αυτό των αρχικών συμβόλων διαμόρφωσης δεδομένων και αυτό είναι πολύ διαφορετικό από αυτό του OFDM για το ίδιο κατειλημμένο εύρος ζώνης στα ίδια δεδομένα τιμή.

Ωστόσο, εάν το εύρος ζώνης του καναλιού είναι ευρύτερο, η σύνδεση μεταξύ του μήκους του συμβόλου και του εύρους ζώνης του καναλιού μπορεί να θεωρηθεί ως το μειονέκτημα του SC-FDM σε σύγκριση με το OFDM [33].

Το πρώτο βήμα είναι το ίδιο όπως για το OFDM, διαμορφώνοντας τα δεδομένα με ένα από τα σχήματα διαμόρφωσης για μετάδοση δεδομένων μέσω των στοιχείων πόρων. Τα δεδομένα τοποθετούνται πάνω από τα στοιχεία πόρων προσαρμόζοντας τη φάση και το πλάτος του υποφορέα σε αυτά που προέρχονται για τη ροή δεδομένων. Μαθηματικά, σημαίνει πολλαπλασιασμό του συμβόλου σύνθετης διαμόρφωσης στην αντίστοιχη συχνότητα υποφορέα. Μετά από αυτή τη διαδικασία, υπάρχει ένα άλλο μπλοκ στην αλυσίδα επεξεργασίας σήματος. Για τη μετατροπή των συμβόλων δεδομένων από τον τομέα χρόνου στον τομέα συχνότητας, το DFT εκτελείται μετά τη σειριακή σε παράλληλη μετατροπή. Ως OFDM, στη συνέχεια, υπάρχει αντιστοίχιση υποφορέα και IDFT για τη μετατροπή του σήματος στον τομέα συχνότητας σε σήμα του τομέα χρόνου. Το κυκλικό πρόθεμα μπορεί να εισαχθεί όταν γίνει η παράλληλη σε σειριακή μετατροπή. Πριν από τη διαμόρφωση του σήματος με υψηλή συχνότητα, μπορεί να χρησιμοποιηθεί ένα φίλτρο διαμόρφωσης παλμών για να ληφθεί το επιθυμητό φάσμα [34].

Οι αρχικές τιμές των συμβόλων μπορούν να ανακτηθούν πλήρως εάν το εκπεμπόμενο σήμα δειγματοληπτείται σωστά στον δέκτη. Τα δύο τελευταία βήματα είναι τα ίδια με αυτά του OFDM. Έτσι, δεν υπάρχει διαφορά στην αλυσίδα παραγωγής σήματος κατερχόμενη ζεύξης. Με τον ίδιο τρόπο, το αντίστροφο από αυτό που έγινε στον πομπό μπορεί να επιτευχθεί στον δέκτη. Όπως αναφέρθηκε στην Ενότητα 5.1.3, κάθε δευτερεύων φορέας φέρει μόνο ένα συγκεκριμένο σύμβολο διαμόρφωσης στο OFDM, ενώ το DFT παίρνει ένα σύμβολο και το διαδίδει μέσω ενός διαθέσιμου υποφορέα στο SC-FDM. Για το λόγο αυτό, το SC-FDM αναφέρεται επίσης ως DFT-spread OFDM [35].

Δεδομένου ότι το PAPR είναι ανάλογο με το τετράγωνο του αριθμού των υποφορέων που εμπλέκονται, το SC-FDM μειώνει το PAPR μειώνοντας τον αριθμό των υποφορέων. [7]

4.2 Συνδεσιμότητα (Connectivity)

4.2.1 Ανάλυση και βελτιστοποίηση κάλυψης

Προκειμένου να καλυφθούν οι αυξανόμενες απαιτήσεις στη μεταφορά δεδομένων και λόγω των νέων τεχνολογιών οι οποίες αναπτύσσονται στον τομέα των τηλεπικοινωνιών, οι εταιρείες που δραστηριοποιούνται σε αυτόν τον τομέα και οι πάροχοι των υπηρεσιών τηλεπικοινωνιών έχουν επενδύσει χρόνο και χρήματα στη μελέτη χρήσης των ΣμηΕΑ για την παροχή ασύρματου τηλεπικοινωνιακού σήματος.

Οι πλατφόρμες που έχουν μελετηθεί και αναπτυχθεί ποικίλουν, τόσο στον τύπο, το μέγεθος και τα χαρακτηριστικά των ΣμηΕΑ που χρησιμοποιούνται όσο και στο υψόμετρο που αυτά επιχειρούν.

Υπάρχουν τα γιγάντια ΣμηΕΑ τα οποία επιχειρούν σε υψόμετρο πολλών χιλιομέτρων, εκεί όπου μέχρι πρόσφατα ήταν αποκλειστικός επιχειρησιακός χώρος επανδρωμένων αεροσκαφών καθώς επίσης υπάρχουν και τα μικρότερα ΣμηΕΑ τα οποία επιχειρούν σε υψόμετρο μερικών εκατοντάδων μέτρων.

Η δεύτερη περίπτωση είναι αυτή που απασχολεί περισσότερο τον τομέα έρευνας του ΙοΤ.

Στις προτάσεις που έχουν εμφανιστεί στην κοινότητα, έδαφος έχει κερδίσει αυτή που προτείνει τα χαμηλού επιχειρησιακού υψομέτρου ΣμηΕΑ να μην πετούν ψηλότερα από 300 μέτρα, πρώτον γιατί σε αυτή την περίπτωση τα ΣμηΕΑ θα είναι χαμηλότερου κόστους και, δεύτερον, γιατί θα έχουν μεγαλύτερη ευελιξία κίνησης και χρήσης καθώς θα κινούνται σε χώρο που υπόκειται σε λιγότερους κανονισμούς αερομεταφορών.

Στην Ελλάδα, για παράδειγμα, ο νόμος ορίζει ότι τα ΣμηΕΑ που χρησιμοποιούνται για πολιτική χρήση δεν μπορούν να πετούν σε υψηλότερο υψόμετρο από τα 120 μέτρα (υπάρχουν ειδικές κατηγορίες πτητικών αδειών που πετούν υψηλότερα αλλά δεν αφορούν την παρούσα εργασία).

Το υψόμετρο των 300 μέτρων δίνει τη δυνατότητα στα ΣμηΕΑ που λειτουργούν σε δίκτυο για παροχή υπηρεσιών να λειτουργούν και να παρέχουν τις υπηρεσίες τους ελεύθερα είτε πολύ πάνω από το ύψος των κτιρίων μίας αστικής περιοχής είτε κάτω από αυτό.

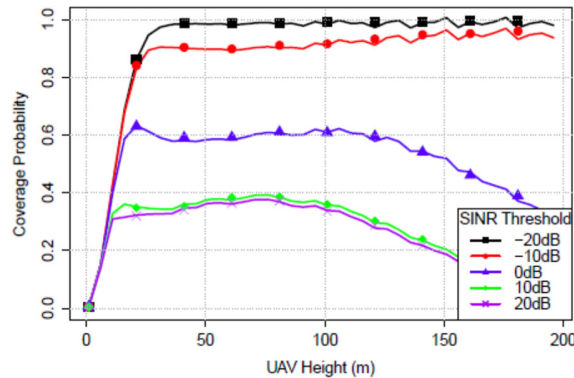
Ακριβώς για το θέμα της γεωγραφικής κάλυψης και της παροχής σήματος έχουν διενεργηθεί πολλαπλές έρευνες οι οποίες λαμβάνουν υπόψη τόσο το υψόμετρο λειτουργίας των ΣμηΕΑ όσο και τα κτίρια, καθώς ο κύριος σκοπός είναι η παροχή υπηρεσιών εντός αστικού ιστού όπου τα εμπόδια (κτίρια) είναι πολλαπλά.

Προς τούτο, χρησιμοποιήθηκε ο δείκτης SINR (signal-to-interference-and-noise-ratio). [8]

$$\int_0^{u(\omega, \gamma)} \left(\mathbb{P}(\text{SINR} \geq \theta | R_1 = r_1, t_1 = L) f_{R_1, t_1}(r_1, t_1 = L) + \mathbb{P}(\text{SINR} \geq \theta | R_1 = r_1, t_1 = N) f_{R_1, t_1}(r_1, t_1 = N) \right) dr_1$$

Σε μετρήσεις που πραγματοποιήθηκαν στο Monte Carlo, συνδυαστικά με τον δείκτη SINR διαπιστώθηκε ότι αρχικά για όλες τις οριακές τιμές του SINR, οι πιθανότητες κάλυψης αυξάνονται καθώς αυξάνεται το ύψος που επιχειρούν τα ΣμηΕΑ.

Αυτό συμβαίνει γιατί τα ΣμηΕΑ αυξάνουν την περιοχή κάλυψής τους μεγιστοποιώντας την πιθανότητα να υπάρχει τουλάχιστον ένα ΣμηΕΑ εντός της εμβέλειας του χρήστη το οποίο να παρέχει επαρκή SINR.



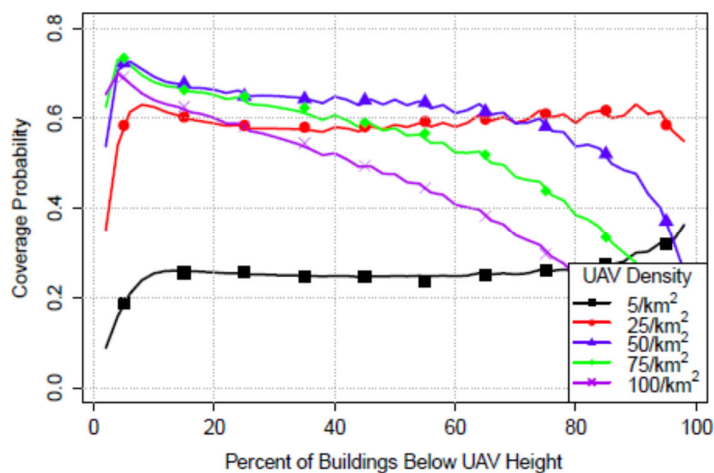
Εικόνα 2: Πιθανότητα κάλυψης δεδομένης πυκνότητας ΣμηΕΑ 25 /km²

Στην εικόνα 2 εμφανίζεται η επίδραση της μεταβολής του ύψους του ΣμηΕΑ στην πιθανότητα κάλυψης, δεδομένων διαφορετικών οριακών τιμών SINR.

Μετά από ένα ορισμένο ύψος ωστόσο οι καμπύλες δείχνουν διαφορετική συμπεριφορά: για υψηλή οριακή τιμή SINR, η πιθανότητα κάλυψης μειώνεται με την αύξηση του ύψους. Αυτό δείχνει ότι το σήμα επικοινωνίας είναι πιο ευάλωτο στον αυξανόμενο αριθμό παρεμβολών LOS (Line-of-sight) τα οποία εμφανίζονται όσο αυξάνεται το υψόμετρο του ΣμηΕΑ. Ωστόσο, οι καμπύλες κάλυψης που λαμβάνουν υπόψη ένα χαμηλό δείκτη SINR παρουσιάζουν διαφορετική συμπεριφορά, η πιθανότητα κάλυψης αυξάνεται.

Αυτό υποδηλώνει ότι ενώ τα σήματα χαμηλού SINR επηρεάζονται αρνητικά από τον αυξανόμενο αριθμό παρεμβολών LOS, η αυξανόμενη πιθανότητα να υπάρχει ΣμηΕΑ εντός LOS προκαλεί συνολική αύξηση της πιθανότητας κάλυψης.

Οι κυματισμοί που εμφανίζονται στο γράφημα οφείλονται στο περίπλοκο αστικό περιβάλλον το οποίο προκαλεί διακυμάνσεις στην απόδοση καθώς μεταβάλλονται οι θέσεις των ΣμηΕΑ.



Εικόνα 3: Πιθανότητα κάλυψης για πολλαπλές πυκνότητες ΣμηΕΑ με όριο SINR 0 dB

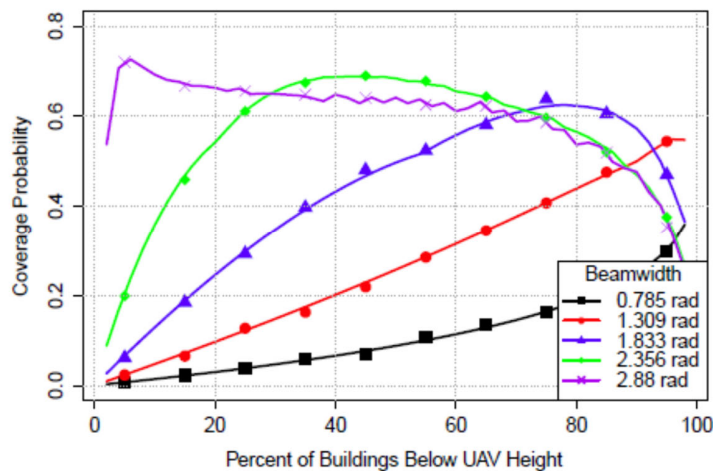
Στην εικόνα 3 εξετάζουμε πώς η αύξηση του υψομέτρου λειτουργίας του ΣμηΕΑ επάνω από ένα ορισμένο ποσοστό των κτιρίων επηρεάζει την πιθανότητα κάλυψης, για δίκτυα ΣμηΕΑ διαφορετικών πυκνοτήτων.

Η εικόνα δείχνει δύο πολύ διαφορετικές συμπεριφορές: η πιθανότητα κάλυψης για το δίκτυο χαμηλότερης πυκνότητας φαίνεται να βελτιώνεται καθώς αυξάνουμε το ύψος του ΣμηΕΑ, ενώ η αύξηση του ύψους επιδεινώνει την κάλυψη των δικτύων υψηλής πυκνότητας.

Αυτό εξηγείται λαμβάνοντας υπόψη την επίδραση των κτιρίων στα δίκτυα. Σε χαμηλές πυκνότητες το ΣμηΕΑ που εξυπηρετεί τον χρήστη αναφοράς μπορεί να κρύβεται πίσω από πολλά κτίρια και η αύξηση του ύψους του ΣμηΕΑ αυξάνει τις πιθανότητες δημιουργίας καναλιού LOS. Ο χαμηλός αριθμός παρεμβολών εντός εμβέλειας σημαίνει ότι καθώς βελτιώνεται το κανάλι μεταξύ ενός χρήστη και του ΣμηΕΑ, ο καθαρός αντίκτυπος στην απόδοση του δικτύου είναι θετικός.

Η συνολική πιθανότητα κάλυψης για το δίκτυο χαμηλής πυκνότητας ΣμηΕΑ είναι χαμηλή ακριβώς επειδή λίγα ΣμηΕΑ καλύπτουν την περιοχή λειτουργίας, με αποτέλεσμα η πιθανότητα ένα ΣμηΕΑ να βρίσκεται εντός της εμβέλειας του χρήστη αναφοράς να είναι μικρή. Σε ένα δίκτυο υψηλής πυκνότητας το ΣμηΕΑ που εξυπηρετεί έναν χρήστη αναφοράς είναι πιθανό να είναι αρκετά κοντά ώστε ο αριθμός των κτιρίων που παρεμβαίνουν στο σήμα να είναι μικρός. Τα κτίρια σε αυτό το σενάριο δεν εμποδίζουν το σήμα εξυπηρέτησης ΣμηΕΑ, αλλά αντιθέτως προστατεύουν τον χρήστη από παρεμβολές.

Η αύξηση του ύψους του ΣμηΕΑ θα εκθέσει τον χρήστη σε αυτούς τους παρεμβολείς ενώ ταυτόχρονα θα επιδεινώσει το σήμα, με αποτέλεσμα την πτώση της κάλυψης.



Εικόνα 4: Πιθανότητα κάλυψης με όριο SINR 0 dB και πυκνότητα ΣμηΕΑ 50 /km²

Στην εικόνα 4 φαίνεται η επίδραση του beamwidth της κεραίας του ΣμηΕΑ στην πιθανότητα κάλυψης. Οι καμπύλες κάλυψης υποδηλώνουν ότι στενότερο beamwidth αποδίδει καλύτερα σε μεγαλύτερα υψόμετρα λειτουργίας ΣμηΕΑ. Αυτό οφείλεται στην επίδραση των beamwidths στην πιθανότητα ο χρήστης να βρίσκεται εντός εμβέλειας ενός ΣμηΕΑ: τα ΣμηΕΑ με μικρό beamwidth δημιουργούν έναν στενό κώνο κάλυψης και ως εκ τούτου πρέπει να λειτουργούν σε μεγαλύτερα ύψη για να διασφαλιστεί ότι οι χρήστες μπορούν να βρίσκονται εντός της εμβέλειάς τους. Βλέπουμε ότι κάθε τιμή beamwidth έχει ένα συσχετισμένο βέλτιστο ύψος λειτουργίας ενός ΣμηΕΑ για ένα δεδομένο δείκτη SINR, πυκνότητα ΣμηΕΑ και περιβάλλον λειτουργίας.

4.2.2 Κατανομή και βελτιστοποίηση πόρων (Resource allocation and optimization)

Η παροχή ευρυζωνικής ασύρματης επικοινωνίας μέσω της χρήσης των ΣμηΕΑ ως ιπτάμενων σταθμών βάσης για την παροχή αυτής της επικοινωνίας σε επίγειους χρήστες, είτε συστηματικά είτε σε περιπτώσεις έκτακτης ανάγκης όπου οι επίγειες δυνατότητες σύνδεσης είναι μη διαθέσιμες ή δεν επαρκούν, είναι καίριας σημασίας.

Κατά την παροχή όμως αυτής της υπηρεσίας, πρέπει να λαμβάνεται υπόψη τόσο η βέλτιστη θέση των ΣμηΕΑ επάνω από την περιοχή ενδιαφέροντος όσο και ο διαθέσιμος χρόνος πτήσης των σκαφών, ο οποίος δεν είναι απεριοριστός.

Για την βελτιστοποίηση, τόσο της θέσης των ΣμηΕΑ στην περιοχή ενδιαφέροντος όσο και της ποιότητας και της διάρκειας παροχής ευρυζωνικής ασύρματης επικοινωνίας, έχουν διεξαχθεί πολλές έρευνες, οι πλέον ενδιαφέρουσες εκ των οποίων εξετάζουν είτε α. τη βελτιστοποίηση της απόδοσης τέτοιων ασύρματων συστημάτων που βασίζονται σε UAV, όσον αφορά τον μέσο αριθμό bits (υπηρεσία δεδομένων) που μεταδίδονται στους χρήστες υπό περιορισμούς χρόνου πτήσης [9] είτε β. μία μέθοδο regret-based learning (RBL) δυναμικής επιλογής κύκλου λειτουργίας (Dynamic Duty Cycle Selection - DDCS) για τη διαμόρφωση των κενών μετάδοσης στα LTE-UABS ώστε να εξασφαλιστεί ικανοποιητική παροχή υπηρεσίας για όλους τους χρήστες [10]

Στην πρώτη περίπτωση, μελετήθηκε από τους Mohammad Mozaffari, Walid Saad, Mehdi Bennis, and Merouane Debbah, η απόδοση ενός τηλεπικοινωνιακού δικτύου βασιμένου σε ΣμηΕΑ, υπό τον περιορισμό που έχουν τα σκάφη στη διάρκεια πτήσης (περίπου 30 λεπτά). Η υπόθεση αφορούσε την δημιουργία ενός δικτύου αποτελούμενου από πολλαπλά ΣμηΕΑ τα οποία χρησιμοποιούνται ως εναέριοι σταθμοί βάσης για να παρέχουν ασύρματη επικοινωνία σε επίγειους χρήστες. Υπό τον περιορισμό του χρόνου πτήσης, αναπτύχθηκε ένα μοντέλο μεγιστοποίησης των παρεχόμενων bits κάτω από ένα σύστημα δίκαιης κατανομής πόρων.

Χρησιμοποιώντας το ισχυρό μαθηματικό πλαίσιο της *θεωρίας βέλτιστων μεταφορών*, προτάθηκε ένας αλγόριθμος που κατανέμει βέλτιστα τη γεωγραφική περιοχή με βάση την κατανομή των χρηστών καθώς και τους χρόνους πτήσης και τις τοποθεσίες των ΣμηΕΑ. Τα αποτελέσματα έδειξαν ότι η προτεινόμενη προσέγγιση κατανομής τηλεπικοινωνιακών κυψελών, υπό το πρίσμα του χρόνου πτήσης, οδηγεί σε σημαντικά δικαιότερη εξυπηρέτηση των επίγειων χρηστών σε σύγκριση με την κλασική σταθμισμένη προσέγγιση Voronoi. Συγκεκριμένα, ο δείκτης δικαιοσύνης του Jain [11] βελτιώνεται κατά 2,6 φορές.

```

1: Inputs:  $f(x, y), \rho, \tau_i, s_i, \forall i \in \mathcal{M}$ .
2: Outputs:  $\psi_i^*, \mathcal{A}_i, \forall i \in \mathcal{M}$ .
3: Set initial values for  $\psi_t^T, (t = 1)$ .
4: while  $\|\nabla F(\psi_t^T)\|_2 > \rho$  do
5:   Set  $k = 1, \epsilon_1 = 1$ .
6:   Update  $\psi_{t+1}^T = \psi_t^T + \epsilon_k \nabla F(\psi_t^T), k, t \in \mathbb{N}$ .
7:   if  $F(\psi_t^T) < F(\psi_{t+1}^T)$  then
8:     Go to Step 12.
9:   else
10:    Go to Step 17.
11:   end if
12:   while  $F(\psi_t^T) < F(\psi_{t+1}^T)$  do
13:      $k \rightarrow k + 1$ .
14:      $\epsilon_k = 2^{k-1} \epsilon_1$ .
15:     Update  $\psi_{t+1}^T = \psi_t^T + \epsilon_k \nabla F(\psi_t^T), k, t \in \mathbb{N}$ .
16:   end while
17:   while  $F(\psi_t^T) > F(\psi_{t+1}^T)$  do
18:      $k \rightarrow k + 1$ .
19:      $\epsilon_k = 2^{-k+1} \epsilon_1$ .
20:     Update  $\psi_{t+1}^T = \psi_t^T + \epsilon_k \nabla F(\psi_t^T), k, t \in \mathbb{N}$ .
21:   end while
22:    $t \rightarrow t + 1$ .
23: end while
24:  $\psi_i^* = \psi_i^T(i), \forall i \in \mathcal{M}$ .
25:  $\mathcal{A}_i = \{(x, y) | J(x, y, s_i) - \psi_i^* \leq J(x, y, s_j) - \psi_j^*, \forall j \neq i\},$ 
 $\forall i \in \mathcal{M}$ .

```

Ο αλγόριθμος των Mohammad Mozaffari, Walid Saad, Mehdi Bennis, and Merouane Debbah

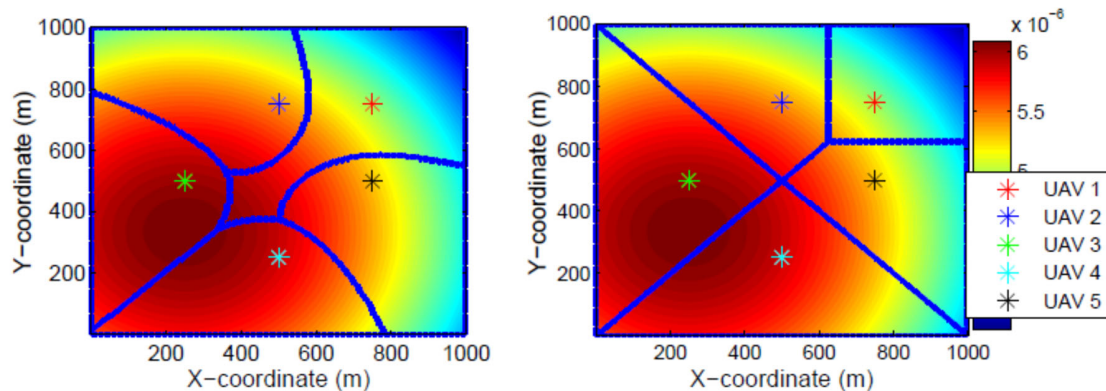
ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΡΟΣΟΜΟΙΩΣΗΣ ΚΑΙ ΑΝΑΛΥΣΗ

Πίνακας Ι: Παράμετροι προσομοίωσης

Παράμετρος	Περιγραφή	Τιμή
f_c	Φέρουσα συχνότητα	2 GHz
P_i	Ισχύς μετάδοσης UAV	0.5W
N_o	Φασματική ισχύς θορύβου	-170 dbm/Hz
N	Αριθμός επίγειων χρηστών	300
μ_{LoS}	Πρόσθετη απώλεια διαδρομής σε ελεύθερο χώρο για LoS	3 dB
μ_{NLoS}	Πρόσθετη απώλεια διαδρομής σε ελεύθερο χώρο για NLoS	23 dB
B	Bandwidth	1 MHz
A	Συντελεστής χρόνου ελέγχου	0.01
h	Ύψος ΣμηΕΑ	200 m
μ_x, μ_y	Μέσος όρος της κατανομής Gauss	250m, 330m
b_1, b_2	Περιβαλλοντικές παράμετροι (πυκνότητα κατοικίας)	0.36, 0.21

Για την προσομοίωση, χρησιμοποιήθηκε μία έκταση επιφάνειας ενός τετραγωνικού χιλιομέτρου με πλευρές 1000X1000 μέτρα, στην οποία έκταση οι επίγειοι χρήστες κατανέμονται σύμφωνα με περικομμένη κατανομή Gauss η οποία είναι κατάλληλη για την μοντελοποίηση μίας περιοχής ενδιαφέροντος. Παρότι χρησιμοποιείται η συγκεκριμένη κατανομή, η ανάλυση αυτή μπορεί να χρησιμοποιήσει οποιαδήποτε άλλη γενική κατανομή. Τα ΣμηΕΑ αναπτύχθηκαν σε μορφή πλέγματος (grid-based deployment) σε υψόμετρο 200 m. Εκτός κι αν αναφέρεται διαφορετικά, εξετάστηκε ένα πλήρες σενάριο παρεμβολής με παράγοντα παρεμβολής $\beta = 1$. Για τη συνάρτηση χρόνου ελέγχου, θεωρούμε $g_i(z) = \alpha z^2$, με ένα α να είναι ένας αυθαίρετος σταθερός παράγοντας.

Αυτή η συνάρτηση είναι μια λογική επιλογή στο μοντέλο, καθώς είναι μια υπεργραμμική συνάρτηση του αριθμού των χρηστών και η τιμή της μπορεί να ρυθμιστεί με τον παράγοντα α . Ωστόσο, οποιαδήποτε αυθαίρετη λειτουργία συνεχούς ελέγχου Lipschitz μπορεί επίσης να ληφθεί υπόψη στο μοντέλο. Οι παράμετροι προσομοίωσης παρατίθενται στον Πίνακα Ι. Συγκρίνουμε τα αποτελέσματά, που λαμβάνονται με βάση την προτεινόμενη προσέγγιση βέλτιστης κατανομής κυψελών, με την κλασική σταθμισμένη γραμμή βάσης του διαγράμματος Voronoi. Όλα τα στατιστικά αποτελέσματα υπολογίζονται κατά μέσο όρο σε μεγάλο αριθμό ανεξάρτητων εκτελέσεων.



Εικόνα 5: Καταμήσεις κυψελών που σχετίζονται με ΣμηΕΑ δεδομένης της μη ομοιόμορφης χωρικής κατανομής των χρηστών

(α) Προτεινόμενη βέλτιστη διαμερισματοποίηση κυψελών	(β) Σταθμισμένο διάγραμμα Voronoi
--	-----------------------------------

Η εικόνα 5 δείχνει την προτεινόμενη βέλτιστη διαμερισματοποίηση κυψελών και το κλασικό σταθμισμένο διάγραμμα Voronoi. Σε αυτήν την περίπτωση, θεωρούμε 5 ΣμηΕΑ που παρέχουν υπηρεσία σε μη ομοιόμορφα κατανεμημένους χρήστες επί του εδάφους (περικομμένη κατανομή Gaussian). Επιπλέον, υποθέτουμε ότι ο μέγιστος χρόνος πτήσης κάθε ΣμηΕΑ είναι 30 λεπτά που αντιστοιχεί στον τυπικό χρόνο πτήσης τετρακόπτερων ΣμηΕΑ. Στην εικόνα 5, οι περιοχές που εμφανίζονται με πιο σκούρο χρώμα έχουν υψηλότερη πυκνότητα πληθυσμού.

Όπως μπορούμε να δούμε από το Σχ. 5β, οι καταμήσεις κελιών που σχετίζονται με τα ΣμηΕΑ 3 και 4 έχουν σημαντικά περισσότερους χρήστες από την κατάτμηση κελιών 1. Επομένως, δεδομένων των περιορισμένων χρόνων πτήσης, οι χρήστες που βρίσκονται στα διαμερίσματα κυψελών 3 και 4 δεν μπορούν να εξυπηρετηθούν δίκαια. Ωστόσο, στην προτεινόμενη περίπτωση βέλτιστης διαμερισματοποίησης κελιών (που λαμβάνεται από τον αλγόριθμο 1), οι καταμήσεις κελιών αλλάζουν έτσι ώστε να μεγιστοποιείται η μέση παροχή υπηρεσίας δεδομένων με δίκαιη κατανομή πόρων. Για παράδειγμα, όπως φαίνεται

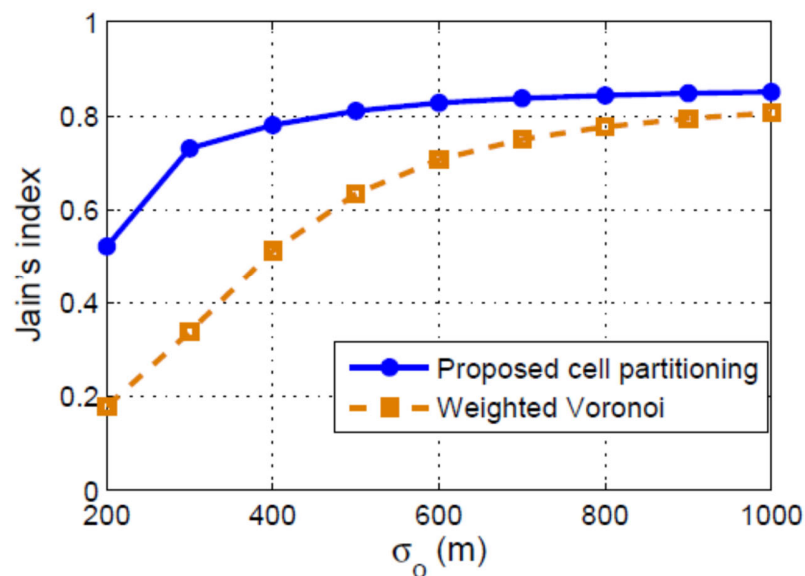
στο Σχ. 2α, το μέγεθος των κυψελών στις κατατμήσεις 3 και 4 μειώνεται σε σύγκριση με το σταθμισμένο διάγραμμα Voronoi. Ως αποτέλεσμα, οι προτεινόμενες κατατμήσεις κυψελών οδηγούν σε υψηλότερο επίπεδο δίκαιης παροχής της υπηρεσίας μεταξύ των χρηστών από τη σταθμισμένη περίπτωση Voronoi.

Για να δείξουμε πόσο δίκαια μπορούν να εξυπηρετηθούν οι χρήστες σε διαφορετικές περιπτώσεις διαμερισματοποίησης κυψελών, χρησιμοποιούμε τον δείκτη δικαιοσύνης του Jain. Υπολογίζουμε το index του Jain με βάση την υπηρεσία δεδομένων που προσφέρεται σε κάθε χρήστη, η οποία δίνεται από ακόλουθη συνάρτηση:

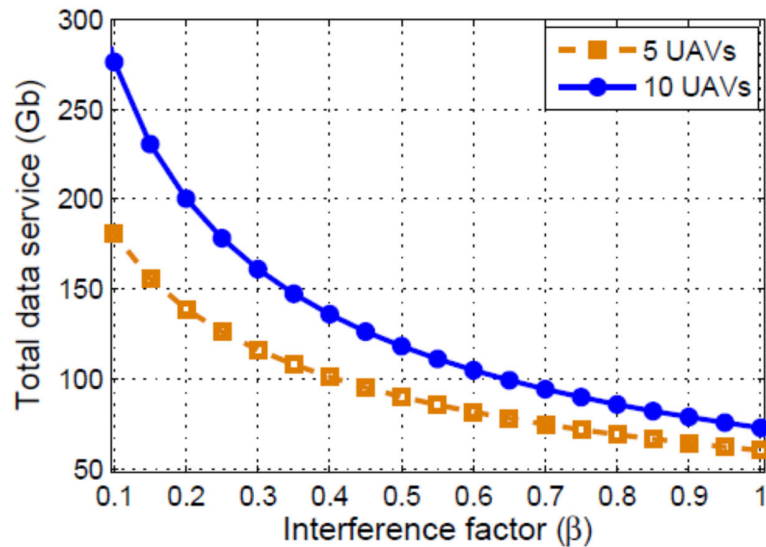
$$F_{\text{Jain}}(l_1, l_2, \dots, l_N) = \left(\sum_{i=1}^N l_i \right)^2 \times \left(N \sum_{i=1}^N l_i^2 \right)^{-1}$$

όπου N είναι ο αριθμός των χρηστών και l_i είναι η παροχή δεδομένων στον χρήστη i .

Σαφώς, το $1/N \leq F_{\text{Jain}} \leq 1$, με το $F_{\text{Jain}} = 1/N$ και το $F_{\text{Jain}} = 1$ να υποδεικνύει το χαμηλότερο και υψηλότερο επίπεδο δίκαιης παροχής της υπηρεσίας.



Εικόνα 6: Ο Δείκτης δικαιοσύνης του Jain για τη μέση υπηρεσία δεδομένων στους χρήστες



Εικόνα 7: : Μέση υπηρεσία δεδομένων έναντι παράγοντα παρεμβολών

Η εικόνα 6 δείχνει τον δείκτη δικαιοσύνης του Jain για διαφορετικές τιμές της τυπικής απόκλισης στην περικομμένη κατανομή Gaussian, σ_0 . Καθώς αυξάνεται το σ_0 , η χωρική κατανομή των χρηστών πλησιάζει σε μια ομοιόμορφη κατανομή. Όπως μπορούμε να δούμε, ο ελάχιστος δείκτης του Jain που αντιστοιχεί στην προτεινόμενη μέθοδο διαμερισμού κυψελών είναι πάνω από 0,5. Ωστόσο, στη σταθμισμένη περίπτωση Voronoi, μπορεί να μειωθεί σε 0,18 για μια εξαιρετικά μη ομοιόμορφη κατανομή χρηστών με $\sigma = 200$ m. Αυτό οφείλεται στο γεγονός ότι, στην Voronoi, οι χρήστες που βρίσκονται σε κατατμήσεις με μεγάλη συμφόρηση λαμβάνουν υπηρεσία χαμηλότερης ποιότητας από τις κατατμήσεις με χαμηλό αριθμό χρηστών. Στην προτεινόμενη προσέγγιση, ωστόσο, οι πόροι (χρόνος πτήσης και εύρος ζώνης) κατανέμονται δίκαια μεταξύ των χρηστών, οδηγώντας έτσι σε υψηλότερο δείκτη δίκαιης πρόσβασης στην υπηρεσία. Από την εικόνα 6 μπορούμε επίσης να παρατηρήσουμε ότι, για υψηλότερες τιμές του σ (πιο ομοιόμορφη κατανομή), ο δείκτης δικαιοσύνης για την προτεινόμενη προσέγγιση πλησιάζει πιο κοντά στη περίπτωση της σταθμισμένης Voronoi.

Η εικόνα 7 δείχνει τη μέση συνολική υπηρεσία δεδομένων ως συνάρτηση του συντελεστή παρεμβολής β , που χρησιμοποιείται στην εικόνα 6. Σαφώς, καθώς η παρεμβολή μεταξύ των ΣμηΕΑ μειώνεται, η συνολική υπηρεσία δεδομένων που μπορούν να παρέχουν στους επίγειους χρήστες αυξάνεται. Για παράδειγμα, μειώνοντας τον συντελεστή παρεμβολής β από 1 (περίπτωση πλήρους παρεμβολής) σε 0,1, η συνολική υπηρεσία δεδομένων τριπλασιάζεται όταν αναπτύσσονται 5 ΣμηΕΑ. Η εικόνα 6 δείχνει επίσης ότι το κέρδος από την παροχή της υπηρεσίας με τη χρήση αυξημένου αριθμού ΣμηΕΑ είναι σημαντικό εάν και μόνο εάν η παρεμβολή μεταξύ των ΣμηΕΑ μετριάζεται αισθητά (χαμηλές τιμές του δείκτη παρεμβολής β).

Για παράδειγμα, η αύξηση των ΣμηΕΑ που χρησιμοποιούνται από 5 σε 10 μπορεί να οδηγήσει σε βελτίωση της υπηρεσίας παροχής δεδομένων κατά 56% όταν ο δείκτης παρεμβολής $\beta = 0,1$, ενώ η ίδια αύξηση στον αριθμό των ΣμηΕΑ οδηγεί σε βελτίωση της υπηρεσίας μόνο κατά 5% όταν ο δείκτης παρεμβολής είναι $\beta = 1$ (πλήρης παρεμβολή). [9]

4.2.3 Αναμετάδοση και δρομολόγηση

Οι στρατηγικές αναμετάδοσης και δρομολόγησης είναι απαραίτητες για τη διατήρηση της συνδεσιμότητας στα δίκτυα ΣμηΕΑ, καθώς τα drones ενδέχεται να αντιμετωπίσουν διάφορα εμπόδια και παρεμβολές που μπορούν να διαταράξουν τη σύνδεση. Στο φυσικό επίπεδο, η αναμετάδοση και η δρομολόγηση επιτυγχάνονται μέσω ενός συνδυασμού πρωτοκόλλων και τεχνικών επικοινωνίας.

Ένα από τα πρωτόκολλα που χρησιμοποιούνται συνήθως για αναμετάδοση και δρομολόγηση στο IoD είναι το πρότυπο IEEE 802.11, γνωστό και ως Wi-Fi. Το Wi-Fi επιτρέπει στα drones να συνδέονται σε ασύρματο δίκτυο και να επικοινωνούν με άλλες συσκευές, όπως επίγειους σταθμούς, άλλα drones και άλλες συσκευές με δυνατότητα Wi-Fi. Το Wi-Fi παρέχει επίσης μια σειρά σχημάτων διαμόρφωσης, συμπεριλαμβανομένης της ψηφιοποίησης μετατόπισης φάσης (PSK), της διαμόρφωσης πλάτους τετραγωνισμού (QAM) και της ορθογωνίας πολυπλεξίας διαίρεσης συχνότητας (OFDM), τα οποία μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση των ρυθμών μεταφοράς δεδομένων και τη μείωση των παρεμβολών.

Ένα άλλο πρωτόκολλο που χρησιμοποιείται συνήθως για τη μετάδοση και τη δρομολόγηση στο IoD είναι το Zigbee. Το Zigbee είναι ένα ασύρματο πρωτόκολλο χαμηλής ισχύος και χαμηλού ρυθμού δεδομένων που είναι κατάλληλο για εφαρμογές drone. Το Zigbee επιτρέπει στα drones να σχηματίσουν ένα δίκτυο πλέγματος, όπου κάθε drone μπορεί να αναμεταδώσει δεδομένα σε άλλα drones μέχρι να επιτευχθεί ο προορισμός. Αυτή η προσέγγιση βελτιώνει την ανθεκτικότητα και την αξιοπιστία του δικτύου, καθιστώντας το ιδανικό για εφαρμογές όπου τα drones πρέπει να λειτουργούν σε απομακρυσμένα ή απαιτητικά περιβάλλοντα.

Εκτός από τα πρωτόκολλα επικοινωνίας, η αναμετάδοση και η δρομολόγηση στο φυσικό επίπεδο του IoD περιλαμβάνει επίσης τη χρήση προηγμένων τεχνικών, όπως τεχνικές διαμόρφωσης δέσμης και ποικιλομορφίας. Η διαμόρφωση δέσμης περιλαμβάνει τη χρήση συστοιχιών κεραιών για την εστίαση της μετάδοσης σε μια συγκεκριμένη κατεύθυνση, μειώνοντας τις παρεμβολές και αυξάνοντας την ισχύ του σήματος. Οι τεχνικές ποικιλομορφίας περιλαμβάνουν τη χρήση πολλαπλών κεραιών για τη μετάδοση και λήψη σημάτων, μειώνοντας τον αντίκτυπο της εξασθένησης και βελτιώνοντας τη συνολική αξιοπιστία της σύνδεσης επικοινωνίας.

Η επιλογή των στρατηγικών αναμετάδοσης και δρομολόγησης στο IoD εξαρτάται από τη συγκεκριμένη εφαρμογή και το περιβάλλον στο οποίο λειτουργούν τα drones. Για παράδειγμα, σε αστικά περιβάλλοντα με υψηλές παρεμβολές, το Zigbee μπορεί να είναι μια καλύτερη επιλογή λόγω της ικανότητάς του να σχηματίζει ένα δίκτυο πλέγματος και να διατηρεί τη συνδεσιμότητα ακόμη και όταν οι άμεσες συνδέσεις δεν είναι διαθέσιμες. Αντίθετα, σε ανοιχτές περιοχές με λιγότερα εμπόδια, το Wi-Fi μπορεί να είναι μια πιο αποτελεσματική επιλογή λόγω των υψηλότερων ρυθμών μεταφοράς δεδομένων και της χαμηλότερης καθυστέρησης.

Η αναμετάδοση και η δρομολόγηση στο φυσικό επίπεδο του Internet of Drones είναι ζωτικής σημασίας για τη διατήρηση της συνδεσιμότητας και την αποτελεσματική επικοινωνία μεταξύ των drones και του επίγειου σταθμού. Η επιλογή των στρατηγικών αναμετάδοσης και δρομολόγησης εξαρτάται από τη συγκεκριμένη εφαρμογή και το περιβάλλον και οι συνεχείς εξελίξεις στην τεχνολογία drone και τα πρωτόκολλα επικοινωνίας αναμένεται να οδηγήσουν σε περαιτέρω βελτιώσεις στο IoD.

Αναφορικά με τους αλγόριθμους δρομολόγησης, δύο από τους πλέον γνωστούς είναι ο αλγόριθμος A* και ο αλγόριθμος του Dijkstra.

Αλγόριθμος A* [12]:

Ο αλγόριθμος A* είναι ένας αλγόριθμος εύρεσης διαδρομής που χρησιμοποιείται συνήθως για την εύρεση της συντομότερης διαδρομής μεταξύ δύο σημείων σε ένα γράφημα. Στο πλαίσιο της δρομολόγησης drone, ο αλγόριθμος A* μπορεί να χρησιμοποιηθεί για να βρει τη βέλτιστη διαδρομή για ένα drone να φτάσει στον προορισμό του. Ο αλγόριθμος λαμβάνει υπόψη την απόσταση και τον εκτιμώμενο χρόνο που απαιτείται για την επίτευξη κάθε κόμβου στο γράφημα και, στη συνέχεια, καθορίζει την καλύτερη διαδρομή με βάση μια ευρετική συνάρτηση που υπολογίζει την απόσταση που απομένει στον προορισμό. Αυτή η ευρετική συνάρτηση χρησιμοποιείται για την ιεράρχηση κόμβων που βρίσκονται πιο κοντά στον προορισμό, γεγονός που μπορεί να μειώσει τον χρόνο αναζήτησης και να βελτιώσει την αποτελεσματικότητα του αλγορίθμου δρομολόγησης.

Αλγόριθμος του Dijkstra [13]:

Ο αλγόριθμος του Dijkstra είναι ένας άλλος δημοφιλής αλγόριθμος δρομολόγησης που χρησιμοποιείται στην τεχνολογία drone. Αυτός ο αλγόριθμος χρησιμοποιείται για την εύρεση της συντομότερης διαδρομής μεταξύ δύο κόμβων σε ένα σταθμισμένο γράφημα. Στο πλαίσιο της δρομολόγησης drone, ο αλγόριθμος του Dijkstra μπορεί να χρησιμοποιηθεί για τον προσδιορισμό της βέλτιστης διαδρομής που πρέπει να ακολουθήσει ένα drone με βάση την απόσταση και την ισχύ του σήματος μεταξύ των κόμβων. Ο αλγόριθμος λαμβάνει υπόψη την απόσταση μεταξύ κάθε κόμβου και του κόμβου προέλευσης και εκχωρεί μια δοκιμαστική απόσταση σε κάθε κόμβο. Στη συνέχεια, επιλέγει επαναληπτικά τον κόμβο με τη χαμηλότερη δοκιμαστική απόσταση και ενημερώνει τις δοκιμαστικές αποστάσεις των γειτόνων του μέχρι να επιτευχθεί ο κόμβος προορισμού.

Σχεδιασμός διαδρομής και βελτιστοποίηση θέσης

Ο σχεδιασμός διαδρομής και η βελτιστοποίηση θέσης είναι κρίσιμες πτυχές των δικτύων ΣμηΕΑ, καθώς επηρεάζουν άμεσα τη συνολική αποτελεσματικότητα και ασφάλεια του συστήματος. Ο σχεδιασμός διαδρομής περιλαμβάνει τον προσδιορισμό της βέλτιστης διαδρομής που θα ακολουθήσει ένα ΣμηΕΑ για να μεταβεί από την τρέχουσα θέση του στον προορισμό του, αποφεύγοντας παράλληλα εμπόδια και ελαχιστοποιώντας την κατανάλωση ενέργειας. Από την άλλη, η βελτιστοποίηση θέσης περιλαμβάνει τον προσδιορισμό των βέλτιστων τοποθεσιών για την τοποθέτηση ΣμηΕΑ, προκειμένου να μεγιστοποιηθεί η κάλυψη και η συνδεσιμότητα, ελαχιστοποιώντας παράλληλα τις παρεμβολές.

Προκειμένου να επιτευχθεί αποτελεσματικός σχεδιασμός διαδρομής και βελτιστοποίηση θέσης, τα δίκτυα drone βασίζονται σε διάφορες τεχνολογίες και τεχνικές όπως GPS, LiDAR και υπολογιστική όραση. Αυτές οι τεχνολογίες βοηθούν τα drones να αντιλαμβάνονται με ακρίβεια το περιβάλλον τους και να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την πορεία και τη θέση τους.

Ένα σημαντικό ζήτημα στον σχεδιασμό διαδρομών και τη βελτιστοποίηση της θέσης είναι ο αντίκτυπος των καιρικών συνθηκών στις λειτουργίες των ΣμηΕΑ. Ο άνεμος, η βροχή και άλλα καιρικά φαινόμενα μπορούν να επηρεάσουν σημαντικά τη διαδρομή πτήσης και τη θέση των ΣμηΕΑ, καθιστώντας απαραίτητη την προσαρμογή των αλγορίθμων βελτιστοποίησης διαδρομής και θέσης ανάλογα. Επιπλέον, το έδαφος και η γεωγραφία της περιοχής στην οποία λειτουργεί το δίκτυο drone μπορούν επίσης να επηρεάσουν τον σχεδιασμό διαδρομής και τη βελτιστοποίηση θέσης.

Ένας άλλος σημαντικός παράγοντας στον σχεδιασμό της διαδρομής των ΣμηΕΑ και στη βελτιστοποίηση της θέσης είναι η ανάγκη ελαχιστοποίησης των παρεμβολών και

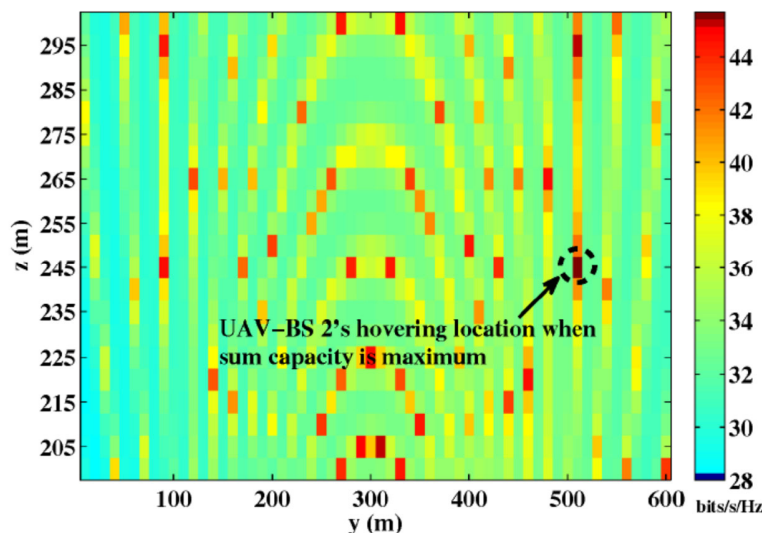
των συγκρούσεων μεταξύ τους. Για να επιτευχθεί αυτό, τα drones πρέπει να είναι εξοπλισμένα με συστήματα αποφυγής συγκρούσεων και πρωτόκολλα επικοινωνίας που τους επιτρέπουν να συντονίζουν τις κινήσεις τους με άλλα ΣμηΕΑ στο δίκτυο. Επιπλέον, η χρήση αλγορίθμων τεχνητής νοημοσύνης και μηχανικής μάθησης μπορεί να βοηθήσει τα ΣμηΕΑ να προβλέψουν τις κινήσεις άλλων drones και να προσαρμόσουν ανάλογα τις δικές τους διαδρομές.

Μία από τις πλέον αναγνωρίσιμες μελέτες για την βελτιστοποίηση θέσης ΣμηΕΑ είναι αυτή των Nadisanka Rupasinghe, Ahmed S. Ibrahim και Ismail Guvenc [14] όπου προτείνεται μία μέθοδος για την βελτιστοποίηση της θέσης των ΣμηΕΑ ώστε να βελτιωθεί η επικοινωνία και η κάλυψη ασύρματων δικτύων.

Η εργασία εισάγει την έννοια του Angular Domain User Separation (ADUS), η οποία είναι μια τεχνική που διαχωρίζει τους ασύρματους χρήστες με βάση τη γωνία λήψης των σημάτων τους. Αυτό επιτρέπει την αποτελεσματικότερη χρήση των διαθέσιμων ζωνών συχνοτήτων και μειώνει τις παρεμβολές μεταξύ των χρηστών. Οι συγγραφείς προτείνουν τη χρήση του ADUS για τη βελτιστοποίηση της τοποθέτησης των UAVs σε ένα δίκτυο, βρίσκοντας τις καλύτερες θέσεις για τα UAVs, προκειμένου να επιτευχθεί η μέγιστη κάλυψη, ελαχιστοποιώντας παράλληλα τις παρεμβολές.

Η προτεινόμενη μέθοδος χρησιμοποιεί έναν αλγόριθμο για να βρει τις βέλτιστες θέσεις αιώρησης για τα UAV. Ο αλγόριθμος λαμβάνει υπόψη παράγοντες όπως ο αριθμός των χρηστών στο δίκτυο, η κατανομή των χρηστών και η ισχύς του σήματος που απαιτείται για τη δημιουργία σύνδεσης με κάθε χρήστη. Στη συνέχεια, ο αλγόριθμος καθορίζει τις καλύτερες θέσεις για να αιωρούνται τα UAV, προκειμένου να επιτευχθεί η μέγιστη κάλυψη με ελάχιστες παρεμβολές.

Η εργασία παρουσιάζει επίσης αποτελέσματα προσομοίωσης που αποδεικνύουν την αποτελεσματικότητα της προτεινόμενης μεθόδου. Οι προσομοιώσεις δείχνουν ότι η προτεινόμενη μέθοδος είναι σε θέση να επιτύχει σημαντικές βελτιώσεις στην κάλυψη και τη χωρητικότητα του δικτύου σε σύγκριση με άλλες υπάρχουσες μεθόδους.



Εικόνα 8: Χάρτης έντασης αθροιστικής χωρητικότητας σε σχέση με τις θέσεις του UAV-BS 2 εντός του δικτύου. Η μέγιστη χωρητικότητα αθροίσματος παρατηρήθηκε όταν το UAV-BS 1 βρισκόταν στη θέση του, (90, 245) m και το UAV-BS 2 ήταν στη θέση (510, 245) m ($\sigma_2 = -95$ dB

4.3 Μεγιστοποίηση και αξιολόγηση απόδοσης

4.3.1 Μεγιστοποίηση απόδοσης στο φυσικό επίπεδο

Η μεγιστοποίηση της απόδοσης στο φυσικό επίπεδο είναι ένας σημαντικός στόχος για τα δίκτυα drone, καθώς επηρεάζει άμεσα την αποτελεσματικότητα και την απόδοση του συστήματος. Σε ένα δίκτυο drone, το φυσικό επίπεδο αναφέρεται στο φυσικό κανάλι επικοινωνίας και στην ασύρματη μετάδοση δεδομένων μεταξύ των ΣμηΕΑ.

Μια προσέγγιση για τη μεγιστοποίηση της απόδοσης στο φυσικό επίπεδο είναι η βελτιστοποίηση των παραμέτρων μετάδοσης, όπως τα σχήματα διαμόρφωσης και κωδικοποίησης, η ισχύς μετάδοσης και η συχνότητα φορέα. Αυτές οι παράμετροι μπορούν να ρυθμιστούν δυναμικά με βάση τις συνθήκες του καναλιού και την ποιότητα του λαμβανόμενου σήματος. Για παράδειγμα, εάν το κανάλι έχει «θόρυβο», μπορεί να χρησιμοποιηθεί ένα χαμηλότερο σχήμα διαμόρφωσης με υψηλότερη κωδικοποίηση διόρθωσης σφαλμάτων για τη διασφάλιση αξιόπιστης μετάδοσης δεδομένων.

Μια άλλη προσέγγιση είναι η βελτιστοποίηση της θέσης των ΣμηΕΑ για τη μείωση των παρεμβολών και την αύξηση της ισχύος του σήματος. Με τη στρατηγική τοποθέτηση των ΣμηΕΑ, η ισχύς και η ποιότητα του σήματος μπορούν να βελτιωθούν, οδηγώντας σε υψηλότερη απόδοση. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας αλγόριθμους όπως ο έλεγχος ισχύος, η διαμόρφωση δέσμης και οι κατευθυντικές κεραιές.

Επιπλέον, είναι σημαντικό να εξεταστεί ο αντίκτυπος περιβαλλοντικών παραγόντων, όπως οι καιρικές συνθήκες και η παρουσία εμποδίων στην απόδοση του φυσικού στρώματος. Για παράδειγμα, οι ισχυροί άνεμοι μπορούν να επηρεάσουν τη σταθερότητα και τη θέση των drones, οδηγώντας σε υποβάθμιση της ποιότητας και της απόδοσης του σήματος. Ομοίως, εμπόδια όπως κτίρια ή δέντρα μπορούν να προκαλέσουν εξασθένηση σήματος και παρεμβολές.

Για την αντιμετώπιση αυτών των προκλήσεων, προηγμένες τεχνικές όπως συστήματα πολλαπλών κεραιών, προσαρμοστική διαμόρφωση και κωδικοποίηση και εκτίμηση καναλιών μπορούν να χρησιμοποιηθούν για τη βελτίωση της απόδοσης του φυσικού στρώματος των δικτύων drone. Επιπλέον, αλγόριθμοι μηχανικής μάθησης και τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση των παραμέτρων μετάδοσης και της τοποθέτησης του drone σε πραγματικό χρόνο με βάση τις τρέχουσες συνθήκες καναλιού.

4.3.2 Μεγιστοποίηση απόδοσης σε επίπεδο δικτύου

Η μεγιστοποίηση της απόδοσης σε επίπεδο δικτύου είναι μια σημαντική πτυχή του διαδικτύου των ΣμηΕΑ, καθώς επηρεάζει άμεσα την απόδοση και την αποτελεσματικότητα του συστήματος. Το IoD είναι ένα δίκτυο διασυνδεδεμένων ΣμηΕΑ που επικοινωνούν μεταξύ τους και με άλλες συσκευές για την εκτέλεση εργασιών όπως η επιτήρηση, η μεταφορά υλικών, η αντιμετώπιση φυσικών και άλλων καταστροφών καταστροφών και η παροχή υπηρεσιών επικοινωνίας σε σημεία και υπό συνθήκες που άλλος τρόπος δεν είναι διαθέσιμος. Για να μεγιστοποιηθεί η απόδοση του συστήματος, μπορούν να χρησιμοποιηθούν διάφορες τεχνικές στο επίπεδο δικτύου.

Μια τέτοια τεχνική είναι η κωδικοποίηση δικτύου, η οποία περιλαμβάνει το συνδυασμό πολλαπλών πακέτων δεδομένων σε ένα ενιαίο πακέτο για μετάδοση. Αυτό μπορεί να βελτιώσει την αποτελεσματικότητα του συστήματος μειώνοντας τον αριθμό των πακέτων που πρέπει να μεταδοθούν και αυξάνοντας τη συνολική απόδοση. Μια άλλη τεχνική είναι η χρήση της πολλαπλής δρομολόγησης, όπου τα δεδομένα μεταδίδονται

μέσω πολλαπλών drones πριν φτάσουν στον προορισμό τους. Αυτό μπορεί να βελτιώσει την κάλυψη του συστήματος και να μειώσει τον αντίκτυπο των εμποδίων και των παρεμβολών στη μετάδοση.

Εκτός από αυτές τις τεχνικές, η χρήση μηχανισμών ποιότητας υπηρεσίας (QoS) μπορεί επίσης να συμβάλει στη μεγιστοποίηση της απόδοσης του συστήματος. Οι μηχανισμοί QoS δίνουν προτεραιότητα σε ορισμένους τύπους δεδομένων, όπως βίντεο σε πραγματικό χρόνο ή σήματα έκτακτης ανάγκης, έναντι άλλων τύπων. Αυτό μπορεί να διασφαλίσει ότι τα κρίσιμα δεδομένα μεταδίδονται χωρίς καθυστέρηση, βελτιώνοντας τη συνολική απόδοση του συστήματος.

Ένα άλλο σημαντικό ζήτημα για τη μεγιστοποίηση της απόδοσης στο επίπεδο δικτύου είναι η επιλογή των κατάλληλων πρωτοκόλλων δικτύου. Για παράδειγμα, η χρήση ελαφρών πρωτοκόλλων όπως το CoAP (Constrained Application Protocol) και το MQTT (Message Queuing Telemetry Transport) μπορεί να βελτιώσει τη συνολική αποτελεσματικότητά του.

Συμπερασματικά, η μεγιστοποίηση της απόδοσης σε επίπεδο δικτύου είναι ζωτικής σημασίας για την αποτελεσματική και αξιόπιστη λειτουργία του διαδικτύου των drones. Η χρήση τεχνικών όπως η κωδικοποίηση δικτύου, η δρομολόγηση πολλαπλών αναπηδήσεων, οι μηχανισμοί QoS και τα κατάλληλα πρωτόκολλα δικτύου μπορούν να βοηθήσουν στην επίτευξη αυτού του στόχου, επιτρέποντας στο σύστημα να εκτελεί ένα ευρύ φάσμα εφαρμογών σε διάφορους τομείς.

4.4 Μοντελοποίηση και χαρακτηρισμός καναλιών

4.4.1 Βελτιστοποίηση θέσης

Η ασύρματη επικοινωνία αφορά τη μετάδοση σήματος μεταξύ δύο ή περισσότερων συσκευών χωρίς τη χρήση καλωδίου. Η μοντελοποίηση καναλιών και η βελτιστοποίηση θέσης είναι δύο σημαντικές πτυχές της ασύρματης επικοινωνίας που διαδραματίζουν βασικό ρόλο στη διασφάλιση αξιόπιστης και αποτελεσματικής επικοινωνίας.

Η μοντελοποίηση καναλιών είναι η διαδικασία χαρακτηρισμού του ασύρματου καναλιού μεταξύ δύο ή περισσότερων συσκευών, λαμβάνοντας υπόψη παράγοντες όπως η εξασθένηση του σήματος, οι παρεμβολές και ο θόρυβος. Αυτές οι πληροφορίες χρησιμοποιούνται για την ανάπτυξη μαθηματικών μοντέλων που μπορούν να προβλέψουν πώς θα συμπεριφέρεται το ασύρματο σήμα καθώς ταξιδεύει μέσω του καναλιού. Αυτά τα μοντέλα μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση του σχεδιασμού συστημάτων ασύρματης επικοινωνίας, όπως η τοποθέτηση κεραιών και οι αλγόριθμοι επεξεργασίας σήματος.

Η βελτιστοποίηση θέσης συσχετιζόμενη με τη μοντελοποίηση καναλιών είναι η διαδικασία προσδιορισμού της βέλτιστης τοποθέτησης των ασύρματων συσκευών, εν προκειμένω των ΣμηΕΑ για τη μεγιστοποίηση της ισχύος του σήματος και την ελαχιστοποίηση των παρεμβολών ταυτόχρονα με την μεγιστοποίηση χωρικής κάλυψης.

Ένα από τα πλέον διαδεδομένα μοντέλα που χρησιμοποιούνται για τη βελτιστοποίηση θέσης είναι το A2G (air-to-ground) το οποίο είναι ένας τύπος μοντέλου καναλιού ασύρματης επικοινωνίας που χρησιμοποιείται για να περιγράψει τη διάδοση ηλεκτρομαγνητικών κυμάτων μεταξύ ενός αερομεταφερόμενου οχήματος (όπως ένα αεροσκάφος ή ένα ΣμηΕΑ) και ενός επίγειου δέκτη ή σταθμού βάσης.

Το A2G λαμβάνει υπόψη διάφορους παράγοντες που μπορούν να επηρεάσουν τη μετάδοση των κυμάτων, όπως:

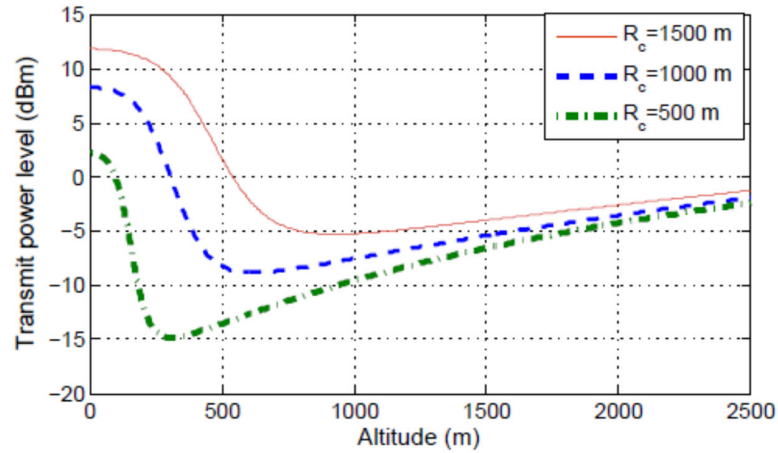
- Απώλεια διαδρομής: Η εξασθένηση του σήματος λόγω της απόστασης μεταξύ του αεροσκάφους και του επίγειου δέκτη ή σταθμού βάσης
- Σκίαση: Η εξασθένηση του σήματος λόγω εμποδίων όπως κτίρια, δέντρα ή έδαφος μεταξύ του αεροσκάφους και του επίγειου δέκτη ή σταθμού βάσης.
- Εξασθένηση πολλαπλών διαδρομών: Η επίδραση των αντανάκλασεων σήματος από αντικείμενα στο περιβάλλον, η οποία μπορεί να προκαλέσει την άφιξη του σήματος στον δέκτη ή στο σταθμό βάσης από πολλαπλές διαδρομές, με διαφορετική φάση και εύρος.
- Doppler shift: Η αλλαγή στη συχνότητα του σήματος λόγω της κίνησης του αεροσκάφους σε σχέση με τον επίγειο δέκτη ή τον σταθμό βάσης.
- Ατμοσφαιρική εξασθένηση: Η εξασθένηση του σήματος λόγω απορρόφησης από την ατμόσφαιρα, η οποία μπορεί να προκληθεί από παράγοντες όπως οι καιρικές συνθήκες και το υψόμετρο.

Στο συγκεκριμένο μοντέλο, ο επίγειος δέκτης λαμβάνει τρεις τύπους σημάτων, συμπεριλαμβανομένων των LOS (Line-of-sight), των ισχυρών ανακλώμενων σημάτων (NLOS) και των πολλαπλών ανακλώμενων σημάτων που προκαλούν εξασθένηση σήματος λόγω πολλαπλών δρομολόγησης. Αυτοί οι τύποι σημάτων μπορούν να εξεταστούν ξεχωριστά με διαφορετικές πιθανότητες εμφάνισης. Τυπικά θεωρείται ότι το λαμβανόμενο σήμα κατηγοριοποιείται μόνο σε μία από τις αναφερόμενες ομάδες. Κάθε ομάδα έχει μια συγκεκριμένη πιθανότητα εμφάνισης που είναι συνάρτηση του περιβάλλοντος, της πυκνότητας και του ύψους των κτιρίων και της υψομετρικής γωνίας. Η πιθανότητα λήψης LOS και ισχυρών NLOS είναι σημαντικά υψηλότερη από την εξασθένηση και, ως εκ τούτου, ο αντίκτυπος της εξασθένησης μικρής κλίμακας μπορεί να αγνοηθεί. Στις συνδέσεις NLOS λόγω της επίδρασης σκίασης και της αντανάκλασης των σημάτων από εμπόδια, η απώλεια διαδρομής είναι υψηλότερη από τις συνδέσεις LOS.

Στην εξαιρετικά ενδιαφέρουσα έρευνα των Mohammad Mozaffari, Walid Saad, Mehdi Bennis και Merouane Debda, εξετάστηκαν τρεις περιπτώσεις: χρήση ενός ΣμηΕΑ, δύο μη παρεμβαλλομένων ΣμηΕΑ και δύο παρεμβαλλομένων ΣμηΕΑ [15] με στόχο τη μέγιστη επικοινωνιακή κάλυψη των χρηστών εδάφους και την ελάχιστη δυνατή κατανάλωση ενέργειας.

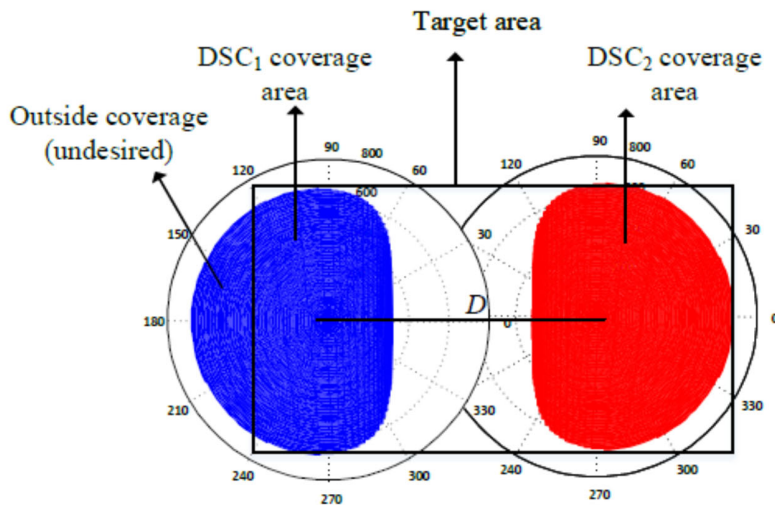
Η εικόνα 9 δείχνει την ελάχιστη ισχύ μετάδοσης που απαιτείται για μία συγκεκριμένη περιοχή κάλυψης, σε συνάρτηση με το υψόμετρο του DSC (drone small cell).

Η ανάπτυξη ενός DSC στο βέλτιστο υψόμετρο ελαχιστοποιεί την ελάχιστη απαιτούμενη ισχύ μετάδοσης για την κάλυψη της περιοχής-στόχου. Στην πραγματικότητα, για πολύ χαμηλά υψόμετρα, λόγω της σκίασης, η πιθανότητα συνδέσεων LOS μεταξύ πομπού και δέκτη μειώνεται και κατά συνέπεια μειώνεται η ακτίνα κάλυψης. Από την άλλη, σε πολύ μεγάλο υψόμετρο είναι πιο πιθανές οι συνδέσεις LOS. Ωστόσο, λόγω της μεγάλης απόστασης μεταξύ πομπού και δέκτη, η απώλεια διαδρομής αυξάνεται και κατά συνέπεια μειώνεται η απόδοση. Για παράδειγμα, το βέλτιστο υψόμετρο για την παροχή ακτίνας κάλυψης 500 m ενώ καταναλώνεται ελάχιστη ισχύς μετάδοσης είναι 310 m. Επιπλέον, μπορούμε να δούμε ότι υπάρχει μόνο ένα τοπικό ελάχιστο για την ισχύ μετάδοσης ως συνάρτηση του υψομέτρου. Τα αποτελέσματα παρέχουν πολύ χρήσιμες οδηγίες για την ελαχιστοποίηση της ισχύος, η οποία είναι ένα από τα κύρια μελήματα στο σχεδιασμό δικτύων DSC. Η εικόνα δείχνει ότι καθώς αυξάνεται η ακτίνα της περιοχής-στόχου, αυξάνεται τόσο το βέλτιστο υψόμετρο όσο και η ελάχιστη ισχύς μετάδοσης που απαιτείται για την κάλυψη της περιοχής. [15]



Εικόνα 9: Ελάχιστη απαιτούμενη ισχύς μετάδοσης

Στην εικόνα 10, εμφανίζεται ο αντίκτυπος των παρεμβολών στην απόδοση κάλυψης όταν δύο DSC (ΣμηΕΑ) βρίσκονται σε υψόμετρο 300 m και η μεταξύ τους απόσταση είναι 1100 m. Η συνολική περιοχή-στόχος είναι ένα ορθογώνιο με μήκος 2000 m και πλάτος 700 m. Η περιοχή κάλυψης περιλαμβάνει δύο μέρη εντός και εκτός της περιοχής-στόχου ενώ πραγματική περιοχή κάλυψης είναι το τμήμα της περιοχής κάλυψης εντός της περιοχής στόχου. Η εικόνα 10 δείχνει επίσης τον αντίκτυπο των παρεμβολών μεταξύ των DSC που δημιουργούν κενά μεταξύ των περιοχών κάλυψης που παρέχονται από τα δύο DSC. Για να μεγιστοποιηθεί η αποτελεσματικότητα, η απόσταση μεταξύ δύο DSC θα πρέπει να ρυθμιστεί σωστά έτσι ώστε οι παρεμβολές μεταξύ τους να μην είναι υψηλές, ενώ η περιοχή κάλυψης εκτός της περιοχής στόχου ελαχιστοποιείται.



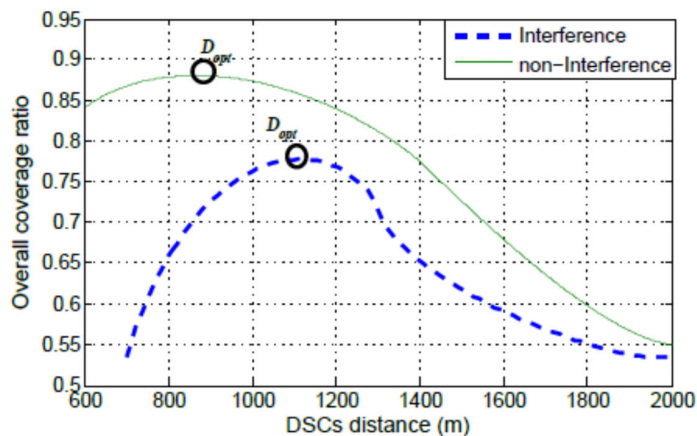
Εικόνα 10: Απόδοση κάλυψης δύο DSC με παρεμβολές παρουσία παρεμβολών

Στην εικόνα 11 δείχνει τον λόγο της πραγματικής περιοχής κάλυψης προς την περιοχή-στόχο που μπορεί να επιτευχθεί χρησιμοποιώντας δύο DSC για διαφορετικές τιμές D , όπου D η απόσταση μεταξύ των DSC.

Σε περίπτωση παρεμβολής για υψηλές τιμές D , αν και η απόσταση μεταξύ των DSC είναι επαρκής για να μετριάσει τον αντίκτυπο των παρεμβολών, παρέχεται κάλυψη κυρίως εκτός της περιοχής στόχου, κάτι που δεν είναι επιθυμητό. Από την άλλη, εάν τα DSC είναι

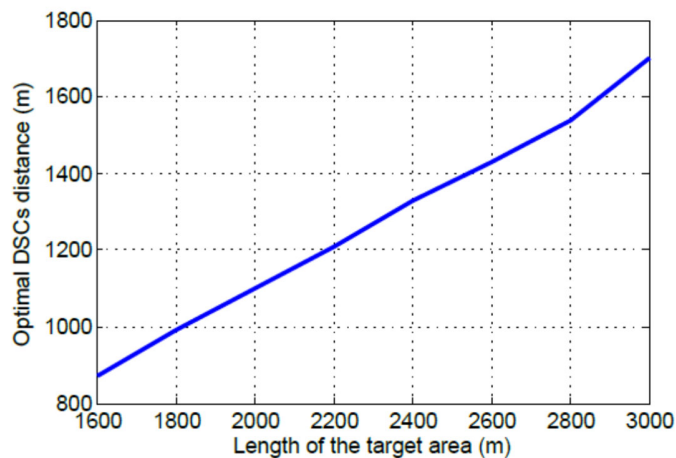
πολύ κοντά μεταξύ τους, οι παρεμβολές μεταξύ τους θα μειώσουν σημαντικά τη συνολική απόδοση κάλυψης. Όπως φαίνεται, η βέλτιστη απόσταση μεταξύ των DSC για μέγιστη κάλυψη, τόσο σε περιπτώσεις ύπαρξης παρεμβολών όσο και σε περιπτώσεις ύπαρξης μη παρεμβολών είναι περίπου 1100 m και 900 m αντίστοιχα.

Στην περίπτωση μη ύπαρξης παρεμβολών, όπως αναμένεται, η συνολική κάλυψη είναι υψηλότερη και η βέλτιστη απόσταση μεταξύ των DSC είναι χαμηλότερη σε σύγκριση με εκείνη της περίπτωσης μη ύπαρξης παρεμβολής. Ο λόγος είναι ότι όταν δεν υπάρχουν παρεμβολές, μπορούμε να μειώσουμε την απόσταση ανάμεσα στα DSC χωρίς να χάσουμε την απόδοση κάλυψης που μπορεί να προκύψει παρουσία παρεμβολών.



Εικόνα 11: Συνολικός λόγος κάλυψης έναντι ενδιάμεσης απόστασης των DSC

Στην εικόνα 12 εμφανίζεται η βέλτιστη απόσταση ανάμεσα στα DSC ως συνάρτηση του μήκους της περιοχής-στόχου. Σύμφωνα αυτό, η βέλτιστη απόσταση μεταξύ των DSC αυξάνεται σχεδόν γραμμικά ανάλογα με το μέγεθος της περιοχής. Για παράδειγμα, όταν το μήκος της περιοχής στόχου αλλάζει από 1800 m σε 2400 m, η βέλτιστη απόσταση μεταξύ των DSC αυξάνεται από 1000 m σε 1350 m. Στην πραγματικότητα, για να αποφύγουμε τις παρεμβολές μεταξύ των DSC, θα πρέπει να τα τοποθετήσουμε όσο το δυνατόν πιο ξεχωριστά, αλλά εντός της περιοχής-στόχου. Αυτό μπορεί να ερμηνευτεί ως κλιμάκωση της απόστασης μεταξύ των DSC μαζί με την περιοχή-στόχο.



Εικόνα 12: Βέλτιστη απόσταση DSC σε σχέση με το μήκος της περιοχής-στόχου

4.4.2 Ανάλυση και βελτιστοποίηση μετρήσεων απόδοσης

Στις ασύρματες επικοινωνίες, η ανάλυση και η βελτιστοποίηση των μετρήσεων απόδοσης είναι ζωτικής σημασίας για την επίτευξη αξιόπιστης και αποτελεσματικής επικοινωνίας. Η μοντελοποίηση καναλιών διαδραματίζει κρίσιμο ρόλο σε αυτή τη διαδικασία, καθώς επιτρέπει τον χαρακτηρισμό και την πρόβλεψη ασύρματων καναλιών, η οποία με τη σειρά της ενημερώνει το σχεδιασμό συστημάτων επικοινωνίας που μπορούν να αποδώσουν καλά υπό ποικίλες συνθήκες.

Μια σημαντική μέτρηση απόδοσης στις ασύρματες επικοινωνίες είναι ο ρυθμός σφάλματος bit (BER – bit error rate), ο οποίος μετρά την πιθανότητα λήψης ενός μεταδιδόμενου bit κατά λάθος. Άλλες σημαντικές μετρήσεις περιλαμβάνουν την αναλογία σήματος προς θόρυβο (SNR), η οποία μετρά την ποιότητα του λαμβανόμενου σήματος και, η χωρητικότητα του καναλιού η οποία μετρά τον μέγιστο ρυθμό με τον οποίο οι πληροφορίες μπορούν να μεταδοθούν αξιόπιστα μέσω του συγκεκριμένου καναλιού.

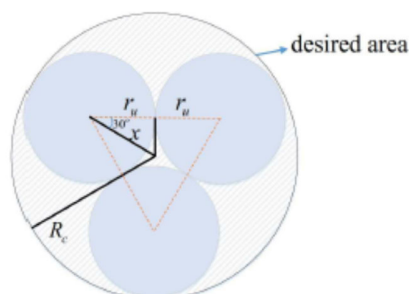
Για τη βελτιστοποίηση αυτών των μετρήσεων απόδοσης, μπορούν να χρησιμοποιηθούν διάφορες τεχνικές. Μια προσέγγιση είναι η χρήση συστημάτων κωδικοποίησης καναλιών, τα οποία προσθέτουν redundancy στο μεταδιδόμενο σήμα για να βελτιώσουν την αξιοπιστία του, όταν υπάρχει «θόρυβος» και παρεμβολές.

Μια άλλη προσέγγιση είναι η χρήση προσαρμογής του modulation format και του επιπέδου ισχύος με βάση τις εκτιμώμενες συνθήκες του καναλιού.

Επιπλέον, η βελτιστοποίηση των μετρήσεων απόδοσης μπορεί επίσης να επιτευχθεί μέσω της χρήσης πολλαπλών κεραιών, γνωστών και ως τεχνολογία MIMO (multiple-input, multiple-output). Το MIMO μπορεί να βελτιώσει τη χωρητικότητα και την αξιοπιστία των ασύρματων καναλιών αξιοποιώντας τη χωρική ποικιλομορφία του ασύρματου καναλιού και χρησιμοποιώντας πολλαπλές κεραιές εκπομπής και λήψης για ταυτόχρονη μετάδοση και λήψη πολλαπλών ροών δεδομένων.

Η πιο διαδεδομένη προσέγγιση για τη βελτιστοποίηση επικοινωνιακής κάλυψης ενός συγκεκριμένου χώρου, ταυτόχρονα με τη βέλτιστη χρήση ενέργειας, χρησιμοποιεί τη θεωρία διαχωρισμού του κύκλου.

Η θεωρία διαχωρισμού του κύκλου είναι ένας κλάδος των μαθηματικών που ασχολείται με τη διάταξη κύκλων μέσα σε ένα δεδομένο χώρο. Ο στόχος είναι να προσδιοριστεί ο μέγιστος αριθμός μη επικαλυπτόμενων κύκλων που μπορούν να τοποθετηθούν σε μια δεδομένη περιοχή.

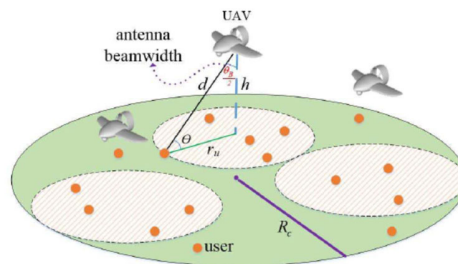


Εικόνα 13: Το πρόβλημα διαχωρισμού ενός κύκλου με τρεις άλλους κύκλους

Στην περίπτωση των ΣμηΕΑ, εκτός από τον σωστό διαχωρισμό της περιοχής ώστε να καλύπτεται το μέγιστο αυτής από τον βέλτιστο αριθμό ΣμηΕΑ, πρέπει να συνυπολογίζεται η κατανάλωση ενέργειας, οι παρεμβολές και το υψόμετρο λειτουργίας των ΣμηΕΑ.

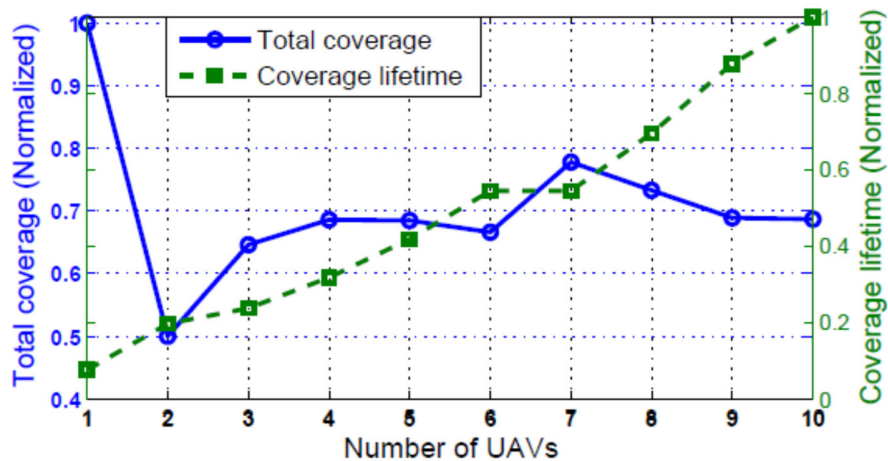
Στην μελέτη των Mohammad Mozaffari, Walid Saad, Mehdi Bennis, και M' erouane Debbaah με τίτλο "[16]", πραγματοποιήθηκαν μετρήσεις των ανωτέρω παραμέτρων ώστε να προσδιοριστεί ο βέλτιστος συνδυασμός αριθμού σκαφών, ύψους και σημείου λειτουργίας για την επίτευξη της μέγιστης ικανοποιητικής τηλεπικοινωνιακής κάλυψης με την ελάχιστη δυνατή κατανάλωση ενέργειας.

Το βασικό πρόβλημα που έπρεπε να επιλυθεί ήταν η βέλτιστη ανάπτυξη των ΣμηΕΑ σε τρισδιάστατο επίπεδο, οι παρεμβολές και ο σχεδιασμός πτήσης.



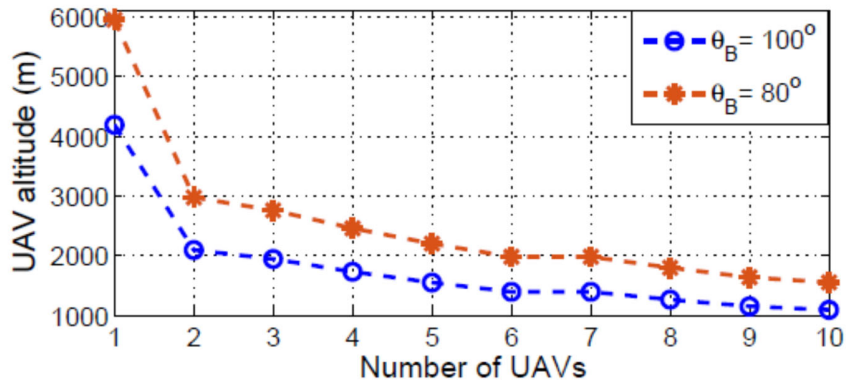
Εικόνα 14: Μοντέλο δοκιμών

Το case study έλαβε ως δεδομένα μία κυκλική γεωγραφική περιοχή ακτίνας R_c , όπως απεικονίζεται στην εικόνα 14, εντός της οποίας πρέπει να αναπτυχθεί M αριθμός ΣμηΕΑ για την παροχή ασύρματης κάλυψης σε επίγειους χρήστες που βρίσκονται εντός της περιοχής. Ως ΣμηΕΑ αναφοράς θεωρήθηκε ένα σκάφος χαμηλού υψομέτρου, όπως τα ΣμηΕΑ με έλικες, μη σταθερής πτέρυγας. Για όλα θεωρήθηκε ότι έχουν την ίδια ισχύ μετάδοσης σήματος και υψομετρικής λειτουργίας.



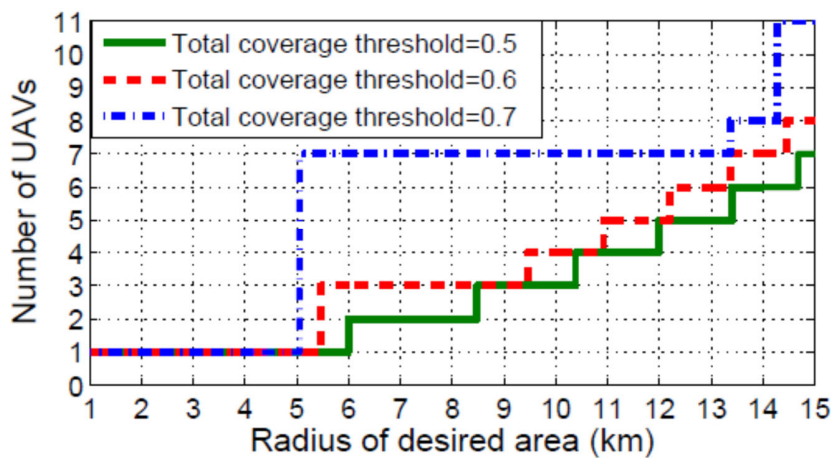
Εικόνα 15: Συνολική κάλυψη και διάρκεια ζωής κάλυψης έναντι αριθμού UAVs για $R_c = 5000m$

Όπως γίνεται φανερό από τα δεδομένα της εικόνας 15, αυξάνοντας τον αριθμό των ΣμηΕΑ που επιχειρούν στην συγκεκριμένη περιοχή, αυξάνεται η διάρκεια ζωής της κάλυψης λόγω της μείωσης της ισχύος μετάδοσης κάθε ΣμηΕΑ.



Εικόνα 16: Το υψόμετρο πτήσης του ΣμηΕΑ έναντι του αριθμού των UAVs

Στην εικόνα 16 απεικονίζεται το βέλτιστο υψόμετρο λειτουργίας των ΣμηΕΑ σε σχέση με τον αριθμό τους και γίνεται εύκολα κατανοητό ότι το υψόμετρο λειτουργίας θα πρέπει να μειωθεί καθώς αυξάνεται ο αριθμός. Για μεγαλύτερο αριθμό ΣμηΕΑ και για να αποφευχθεί η επικάλυψη μεταξύ των περιοχών κάλυψης κάθε ενός, η ακτίνα κάλυψης πρέπει να μειωθεί μειώνοντας το ύψος τους σύμφωνα με $h = r_u / \tan(\theta_B/2)$. Όπως φαίνεται, διπλασιάζοντας τον αριθμό των ΣμηΕΑ από 3 σε 6, το βέλτιστο υψόμετρο μειώνεται από 2000m σε 1300m. Επιπλέον, το βέλτιστο υψόμετρο είναι χαμηλότερο για υψηλότερα πλάτη δέσμης κεραίας.



Εικόνα 17: Αριθμός απαιτούμενων ΣμηΕΑ σε σχέση με την ακτίνα της επιθυμητής περιοχής

Η εικόνα 17 μας δείχνει τον ελάχιστο απαιτούμενο αριθμός ΣμηΕΑ, προκειμένου να ικανοποιηθεί η απαίτηση κάλυψης της δεδομένης γεωγραφικής περιοχής. Το όριο κάλυψης αντιστοιχεί στο ελάχιστο τμήμα της δεδομένης περιοχής που πρέπει να καλύπτεται από τα ΣμηΕΑ. Αυτό το αποτέλεσμα βασίζεται σε $P_t = 35$ dBm, $\theta_B = 80^\circ$ και βέλτιστο υψόμετρο $h < 5000$ m. Είναι ενδιαφέρον ότι για να ικανοποιηθεί τουλάχιστον η απαίτηση κάλυψης 0,7 με μέγιστη διάρκεια ζωής της κάλυψης, απαιτούνται είτε ένα ΣμηΕΑ είτε περισσότερα από 6. Με άλλα λόγια, για $1 < M < 7$, η απόδοση κάλυψης 0,7 δεν μπορεί να επιτευχθεί. Γενικά, καθώς αυξάνεται το μέγεθος της περιοχής ενδιαφέροντος, απαιτούνται περισσότερα σκάφη για την κάλυψή της. Σαφώς, για το $R_c < 5400$ m, η χρήση ενός μόνο UAV μπορεί να ικανοποιήσει ένα όριο κάλυψης 0,6. Ωστόσο, για μια

μεγαλύτερη περιοχή-στόχο, πρέπει να χρησιμοποιηθούν περισσότερα ΣμηΕΑ για να επιτευχθεί το ζητούμενο όριο κάλυψης. Επομένως, ο βέλτιστος αριθμός ΣμηΕΑ που απαιτείται για τον σωστό σχεδιασμό ενός συστήματος επικοινωνίας βασισμένων σε ΣμηΕΑ εξαρτάται σημαντικά από την απαίτηση κάλυψης και το μέγεθος της γεωγραφικής περιοχής.

4.5 Τεχνολογίες επικοινωνίας

Η επιλογή της τεχνολογίας επικοινωνίας των ΣμηΕΑ (LTE, Wi-Fi, VLC, WiMax κ.λπ.) είναι υψίστης σημασίας για τη βελτιστοποίηση της επικοινωνιακής απόδοσης των δικτύων ΣμηΕΑ.

Τα κριτήρια επιλογής υπόκεινται σε πολλαπλούς παράγοντες όπως, η αποστολή που θα εκτελέσει το ΣμηΕΑ, η διάρκεια της αποστολής και της πτήσης, η κινητικότητα των ΣμηΕΑ, ο τύπος των μεταδιδόμενων δεδομένων και η κατανάλωση ενέργειας.

Για να γίνει πιο κατανοητό αυτό μπορούμε να αναφέρουμε ότι τα κυβελωτά δίκτυα, οι δορυφορική σύνδεση ή το WiMax ενώ παρέχουν ευρεία γεωγραφική κάλυψη, υψηλό bandwidth, απόδοση και αξιοπιστία διαθεσιμότητας, είναι ενεργοβόρες τεχνολογίες και έχουν καθυστέρηση μετάδοσης δεδομένων. Από την άλλη, τεχνολογίες όπως το Bluetooth και το ZigBee ενώ είναι ενεργειακά πιο αποδοτικές, έχουν χαμηλό κόστος και μικρές καθυστερήσεις στη μετάδοση δεδομένων, είναι πιο ευάλωτες σε παρεμβολές λόγω εμποδίων και έχουν χαμηλό bandwidth.

4.5.1 Τεχνολογία επικοινωνίας WiFi

Η χρήση της τεχνολογίας του WiFi στην επικοινωνία των ΣμηΕΑ υποκινείται από την ευκολία ανάπτυξης, τη χρήση unlicensed φάσματος

Η επιλογή του Wi-Fi υποκινείται από την ευκολία ανάπτυξής του, τη χρήση μη αδειοδοτημένου φάσματος και την ανάγκη υποστήριξης πολλών και διαφορετικού τύπου και αναγκών εφαρμογών στο ίδιο δίκτυο.

Για παράδειγμα, το WiFi μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός ad-hoc δικτύου ΣμηΕΑ και την ανάπτυξη ενός πρωτοκόλλου επικοινωνίας για τη μετάδοση υψηλής ποιότητας βίντεο σε μία περιοχή ανάμεσα σε ΣμηΕΑ και κινητές συσκευές.

Μία από τις πλέον διαδεδομένες χρήσεις των ad-hoc δικτύων ΣμηΕΑ και κινητών συσκευών είναι η επόπτευση καλλιεργιών (αρδευτικά ύδατα, έλεγχος παρασίτων και εντόμων, παρακολούθηση παραγωγής καλλιεργειών κ.λπ), ο έλεγχος για πυρκαγιές, φυσικές ή άλλες καταστροφές κ.λπ.

Ειδικά για την περίπτωση της Ελλάδας, όπου η καλλιέργεια σιτηρών είναι διαδεδομένη, η χρήση ad-hoc δικτύων με ΣμηΕΑ και κινητές συσκευές θα μπορούσε να αποδειχθεί εξαιρετικά χρήσιμη.

Σε έρευνα η οποία πραγματοποιήθηκε στην Ισπανία [17], χρησιμοποιήθηκαν 3 AR drones τα οποία συνδέθηκαν μέσω WiFi σε ad-hoc δίκτυο. Η έκταση την οποία μπόρεσαν να εποπτεύσουν με τη μετάδοση υψηλής ποιότητας βίντεο ήταν 1,5 -2 εκτάρια ανά λεπτό για χρόνο πτήσης 30 λεπτών (λόγω περιορισμού κατανάλωσης ενέργειας). Σε αυτή την περίπτωση μιλάμε για 45 – 60 εκτάρια, ήτοι 0.6 km² (600.000 τετραγωνικά μέτρα), μία πραγματικά τεράστια έκταση.

4.5.2 Τεχνολογία επικοινωνίας mmWave

Η τεχνολογία επικοινωνίας mmWave διαθέτει σημαντικά πλεονεκτήματα (πολύ υψηλή συχνότητα και αυξημένο εύρος ζώνης, μικρό μήκος κύματος που επιτρέπει το σχηματισμό δέσμης) και μειονεκτήματα (εξασθένιση όταν το σήμα διαχέεται σε ανοιχτό χώρο, αποκλεισμός σήματος λόγω εμποδίων και αντικειμένων)

Η συγκεκριμένη τεχνολογία αναφέρεται στη μετάδοση ασύρματου σήματος στην περιοχή συχνοτήτων 30 έως 300 gigahertz (GHz), που αντιστοιχεί σε μήκη κύματος μεταξύ 1 και 10 χιλιοστών. Είναι ένα υποσύνολο της επικοινωνίας ραδιοσυχνοτήτων (RF) που λειτουργεί σε σημαντικά υψηλότερες συχνότητες από τα παραδοσιακά δίκτυα κινητής τηλεφωνίας και Wi-Fi, τα οποία συνήθως χρησιμοποιούν συχνότητες κάτω των 6 GHz.

Ορισμένες βασικές πτυχές της τεχνολογίας επικοινωνίας mmWave είναι οι ακόλουθες:

1. Εύρος συχνοτήτων: Η τεχνολογία mmWave λειτουργεί στο φάσμα συχνοτήτων μεταξύ μικροκυμάτων και υπέρυθρων κυμάτων. Περιλαμβάνει ένα ευρύ φάσμα συχνοτήτων, συμπεριλαμβανομένων ζωνών όπως 24 GHz, 28 GHz, 39 GHz και 60 GHz, μεταξύ άλλων.
2. Αυξημένο εύρος ζώνης: Ένα από τα κύρια πλεονεκτήματα της τεχνολογίας mmWave είναι η ικανότητά της να προσφέρει σημαντικά μεγαλύτερο εύρος ζώνης σε σύγκριση με τις ασύρματες τεχνολογίες χαμηλότερης συχνότητας. Αυτό το αυξημένο εύρος ζώνης επιτρέπει ταχύτερους ρυθμούς μεταφοράς δεδομένων, επιτρέποντας συνδέσεις επικοινωνίας υψηλής χωρητικότητας.
3. Διάδοση μικρής εμβέλειας και οπτικής επαφής (LoS – Line of Sight): τα σήματα mmWave έχουν σχετικά μικρή εμβέλεια και είναι ευαίσθητα σε εμπόδια και ατμοσφαιρικές συνθήκες. Εμφανίζουν εξασθένιση όταν περνούν μέσα από αντικείμενα όπως κτίρια, δέντρα ή ακόμα και βροχή. Επιπλέον, τα σήματα mmWave απαιτούν γενικά μια διαδρομή οπτικής επαφής (LOS) μεταξύ του πομπού και του δέκτη ώστε να αποδίδουν ικανοποιητικά.
4. Υψηλοί ρυθμοί μετάδοσης δεδομένων: Λόγω του μεγάλου εύρους ζώνης, η τεχνολογία mmWave μπορεί να υποστηρίξει εξαιρετικά υψηλούς ρυθμούς μετάδοσης δεδομένων, επιτρέποντας τη μετάδοση μεγάλων όγκων δεδομένων σε σύντομο χρονικό διάστημα. Αυτό την καθιστά κατάλληλη για εφαρμογές που απαιτούν εξαιρετικά γρήγορες μεταφορές δεδομένων, όπως ροή βίντεο 4K / 8K, εικονική πραγματικότητα (VR), επαυξημένη πραγματικότητα (AR) και αυτόνομα οχήματα, στα οποία περιλαμβάνονται τα ΣμηΕΑ.
5. Μικρά μήκη κύματος και διαμόρφωση δέσμης: Το μικρό μήκος κύματος των σημάτων mmWave επιτρέπει τη χρήση συστοιχιών κεραιών με μεγάλο αριθμό στοιχείων κεραιάς. Αυτές οι συστοιχίες μπορούν να χρησιμοποιηθούν για τη δημιουργία δοκών υψηλής κατεύθυνσης μέσω μιας τεχνικής που ονομάζεται διαμόρφωση δέσμης. Η διαμόρφωση δέσμης επιτρέπει την εστίαση του μεταδιδόμενου σήματος σε μια συγκεκριμένη κατεύθυνση, αυξάνοντας το εύρος και την ποιότητα του σήματος προς αυτήν την κατεύθυνση, μειώνοντας παράλληλα τις παρεμβολές σε άλλες κατευθύνσεις.
6. Χωρητικότητα και πυκνά δίκτυα: Η τεχνολογία mmWave μπορεί να αξιοποιηθεί για τη δημιουργία δικτύων υψηλής πυκνότητας, καθώς οι στενές δέσμες και η κατευθυντική φύση των σημάτων mmWave μπορούν να επιτρέψουν την καλύτερη χωρική επαναχρησιμοποίηση του φάσματος. Αυτό είναι ιδιαίτερα χρήσιμο σε αστικά περιβάλλοντα όπου πολλές συσκευές επικοινωνούν ταυτόχρονα.
7. Πιθανές προκλήσεις: Ενώ η τεχνολογία mmWave προσφέρει μεγάλες δυνατότητες, υπάρχουν ορισμένες προκλήσεις που σχετίζονται με την ανάπτυξή της. Όπως αναφέρθηκε προηγουμένως, τα σήματα mmWave έχουν περιορισμένη εμβέλεια

και εμποδίζονται εύκολα από εμπόδια. Αυτό απαιτεί την ανάπτυξη μεγάλου αριθμού μικρών κυψελών και κεραιών για να εξασφαλιστεί η κάλυψη. Επιπλέον, τα σήματα υψηλής συχνότητας είναι πιο ευαίσθητα στις περιβαλλοντικές συνθήκες, όπως η βροχή και η ομίχλη, γεγονός που μπορεί να εξασθενήσει περαιτέρω το σήμα.

Η τεχνολογία επικοινωνίας mmWave υπόσχεται πολλά για στις χρήσεις ασύρματης επικοινωνίας υψηλής ταχύτητας με τεράστια χωρητικότητα δεδομένων. Οι πιθανές εφαρμογές της κυμαίνονται από το 5G έως τις Έξυπνες Πόλεις, το Internet of Things (IoT) και διάφορες αναδυόμενες τεχνολογίες που απαιτούν εξαιρετικά γρήγορη και υψηλού εύρους ζώνης συνδεσιμότητα.

4.5.3 Επικοινωνίες Machine-type

Οι επικοινωνίες machine-type (MTC), γνωστές και ως επικοινωνίες μηχανής-προς-μηχανή (M2M), αναφέρονται στην ανταλλαγή δεδομένων ή στην επικοινωνία μεταξύ συσκευών χωρίς άμεση ανθρώπινη συμμετοχή. Περιλαμβάνει την επικοινωνία και την αλληλεπίδραση συσκευών, αισθητήρων ή μηχανών μεταξύ τους ή με ένα κεντρικό σύστημα.

Αυτή η συνδεσιμότητα μπορεί να επιτευχθεί μέσω διαφόρων ασύρματων τεχνολογιών όπως κυψελοειδή δίκτυα, Wi-Fi, Bluetooth, Zigbee ή άλλα εξειδικευμένα πρωτόκολλα MTC. Το MTC χρησιμοποιεί συνήθως εξειδικευμένα πρωτόκολλα επικοινωνίας βελτιστοποιημένα για αλληλεπιδράσεις μηχανής με μηχανή. Αυτά τα πρωτόκολλα εξασφαλίζουν αποτελεσματική ανταλλαγή δεδομένων, χαμηλή κατανάλωση ενέργειας και αξιόπιστη επικοινωνία μεταξύ συσκευών. Παραδείγματα πρωτοκόλλων MTC περιλαμβάνουν MQTT (Message Queuing Telemetry Transport), CoAP (Restricted Application Protocol) και LWM2M (Lightweight Machine-to-Machine).

Η MTC έχει ένα ευρύ φάσμα εφαρμογών σε διάφορους τύπους της ανθρώπινης δραστηριότητας. Χρησιμοποιείται σε τομείς όπως η υγειονομική περίθαλψη, οι μεταφορές, η εφοδιαστική αλυσίδα, η γεωργία, η μεταποίηση, οι επιχειρήσεις κοινής ωφέλειας και οι έξυπνες πόλεις. Παραδείγματα περιλαμβάνουν την απομακρυσμένη παρακολούθηση ιατρικών συσκευών, την παρακολούθηση και διαχείριση περιουσιακών στοιχείων, τα συστήματα έξυπνων δικτύων, την προληπτική συντήρηση σε βιομηχανικά περιβάλλοντα και την έξυπνη γεωργία.

Μαζική ανάπτυξη συσκευών: Το MTC συχνά περιλαμβάνει την ανάπτυξη μεγάλου αριθμού συσκευών ή αισθητήρων που επικοινωνούν μεταξύ τους ή με ένα κεντρικό σύστημα. Αυτές οι συσκευές μπορούν είτε να αναπτυχθούν και να εστιάσουν σε μια συγκεκριμένη περιοχή ή να εξαπλωθούν σε μια ευρεία γεωγραφική περιοχή. Η δυνατότητα αποτελεσματικής σύνδεσης και διαχείρισης ενός μεγάλου αριθμού συσκευών αποτελεί βασική πτυχή του MTC.

Περιορισμοί χαμηλής ισχύος και πόρων: Πολλές συσκευές MTC λειτουργούν με περιορισμένων δυνατοτήτων πηγές ενέργειας, όπως μπαταρίες, και έχουν περιορισμένους υπολογιστικούς πόρους. Επομένως, τα πρωτόκολλα και τα συστήματα MTC έχουν σχεδιαστεί για να είναι ενεργειακά αποδοτικά. Αυτό επιτρέπει στις συσκευές να λειτουργούν για μεγάλα χρονικά διαστήματα χωρίς συχνή αντικατάσταση ή επαναφόρτιση της μπαταρίας.

Συλλογή και ανάλυση δεδομένων: Το MTC επιτρέπει τη συλλογή δεδομένων από καταναμημένες συσκευές ή αισθητήρες. Αυτά τα δεδομένα μπορούν να διαβιβαστούν σε ένα κεντρικό σύστημα ανάλυσης και λήψης αποφάσεων. Η επεξεργασία των δεδομένων που παράγονται από MTC συχνά περιλαμβάνει τεχνικές όπως η ανάλυση δεδομένων, η μηχανική μάθηση και η τεχνητή νοημοσύνη για την εξαγωγή ουσιαστικών πληροφοριών και την αυτοματοποίηση ή την έξυπνη λήψη αποφάσεων.

Αλληλεπίδραση με υπάρχοντα δίκτυα: Οι συσκευές MTC συχνά πρέπει να ενσωματωθούν σε υπάρχοντα δίκτυα επικοινωνίας, όπως κυψελοειδή δίκτυα ή πλατφόρμες cloud, για να καταστεί δυνατή η απρόσκοπτη συνδεσιμότητα και ανταλλαγή δεδομένων. Αυτή η ενσωμάτωση ενδέχεται να απαιτεί τη χρήση gateways ή middleware λογισμικού για την πραγματοποίηση της επικοινωνίας μεταξύ των συσκευών MTC και της υπάρχουσας υποδομής.

Με την ανάπτυξη των ΣμηΕΑ, οι επικοινωνίες MTC αναφέρονται τόσο στην επικοινωνία και τον συντονισμό μεταξύ ΣμηΕΑ όσο και με την επικοινωνία τους με άλλες συσκευές στο έδαφος.

Το MTC επιτρέπει την επικοινωνία μεταξύ ενός σμήνους ΣμηΕΑ για τον συντονισμό τους προκειμένου να εκτελέσουν ομαδικά μία συγκεκριμένη αποστολή. Τα ΣμηΕΑ μπορούν να ανταλλάσσουν πληροφορίες, όπως τοποθεσία, ταχύτητα και αναθέσεις εργασιών, για την εκτέλεση συνεργατικών εργασιών όπως έρευνα και διάσωση, επιτήρηση ή συντονισμένη παράδοση υλικών αντικειμένων.

Επιπλέον το MTC επιτρέπει στους σταθμούς ελέγχου εδάφους ή στους χειριστές να στέλνουν εντολές και να λαμβάνουν δεδομένα τηλεμετρίας από τα ΣμηΕΑ. Επιτρέπει επίσης τον έλεγχο σε πραγματικό χρόνο, τον σχεδιασμό αποστολής πτήσης και την παρακολούθηση των ΣμηΕΑ κατά τη διάρκεια των επιχειρήσεων.

Διαχείριση εναέριας κυκλοφορίας: Το MTC διαδραματίζει κρίσιμο ρόλο στη διαχείριση της επικοινωνίας και του συντονισμού των ΣμηΕΑ στον εναέριο χώρο. Επιτρέπει την επικοινωνία drone-to-drone και drone-to-ground για τη διασφάλιση των πτήσεων, την αποφυγή συγκρούσεων μεταξύ των ΣμηΕΑ αλλά και άλλων αεροσκαφών και τη συμμόρφωση με τους κανονισμούς του εναέριου χώρου.

Μετάδοση δεδομένων αισθητήρων: Τα ΣμηΕΑ που είναι εξοπλισμένα με διάφορους αισθητήρες, όπως κάμερες, lidar ή κάμερες θερμικής απεικόνισης, μπορούν να μεταδώσουν τα δεδομένα που συλλέγονται σε πραγματικό χρόνο χρησιμοποιώντας MTC. Αυτό επιτρέπει την αυτοματοποίηση αλλά και την γρήγορη εκτέλεση αποστολών όπως η εναέρια χαρτογράφηση, η επιτήρηση, η περιβαλλοντική παρακολούθηση και η επιθεώρηση υποδομών.

Επικοινωνία Beyond Visual Line of Sight (BVLOS): Το MTC είναι απαραίτητο για την ενεργοποίηση λειτουργιών BVLOS, όπου τα ΣμηΕΑ μπορούν να λειτουργούν πέρα από την οπτική δυνατότητα του πιλότου στο έδαφος. Το MTC διευκολύνει την αξιόπιστη επικοινωνία μεταξύ των ΣμηΕΑ και του επίγειου σταθμού ελέγχου, επιτρέποντας τον τηλεχειρισμό και την τηλεμετρία, είτε απευθείας είτε μέσω επίγειων κεραιών οι οποίες «παρεμβάλλονται» ανάμεσα στον επίγειο σταθμό ελέγχου και το ΣμηΕΑ.

5. Επίπεδο ζεύξης δεδομένων (Data link layer)

5.1 Κατανομή και βελτιστοποίηση πόρων

5.1.1 Συνεργατικά περιβάλλοντα

Με την ραγδαία ανάπτυξη, ειδικά από το 2010 και μετά, εξαιρετικά σύνθετων συστημάτων που αποτελούνται από διασυνδεδεμένα οχήματα, η οποία ακολούθησε τις εξελίξεις στη ρομποτική, τις επικοινωνίες και την τεχνολογία των υπολογιστών, οι ερευνητές μπόρεσαν να μελετήσουν και να δημιουργήσουν νέα ρομποτικά συστήματα τα οποία επικοινωνούν και αλληλεπιδρούν αυτόματα με άλλες συσκευές αλλά και με τον άνθρωπο.

Τα συστήματα αυτά ονομάστηκαν από την IEEE, «Ασύρματα δικτυωμένα ρομποτικά συστήματα» (Wireless Networked Robot systems - WNR). Σύμφωνα με την περιγραφή του, ένα WNR αναγνωρίζεται από δύο στοιχεία: α. Δυνατότητες αυτόνομης δράσης και β. Συνεργασία μέσω δικτύου.

Οι δυνατότητες αυτόνομης δράσης αναφέρονται στην απαραίτητη προϋπόθεση ένα ρομποτικό σύστημα να κινείται αυτόνομα και να αλληλεπιδρά με το περιβάλλον ενώ η συνεργασία μέσω δικτύου αναφέρεται στη δυνατότητά του να επικοινωνεί με τα υπόλοιπα ρομποτικά συστήματα με ασύρματο τρόπο.

Η ανάπτυξη των αισθητήρων, σε συνδυασμό με τα WNRs, οδήγησε στη δημιουργία των WSANs (Wireless Sensor and Actuator Networks) στα οποία οι συσκευές που συμμετέχουν μπορούν αυτόνομα να αλληλεπιδρούν με το φυσικό περιβάλλον και να προσαρμόζουν την συμπεριφορά τους ανάλογα με τα δεδομένα που ανταλλάσσουν.

Αναφορικά με τα ΣμηΕΑ, τα συνεργατικά περιβάλλοντα αναφέρονται στη συνεργατική συμπεριφορά και τις αλληλεπιδράσεις μεταξύ πολλαπλών κόμβων (drones) για την ενίσχυση της συνολικής απόδοσης του επιπέδου ζεύξης δεδομένων. Το επίπεδο ζεύξης δεδομένων είναι το δεύτερο επίπεδο στο μοντέλο OSI και είναι υπεύθυνο για την αξιόπιστη μετάδοση δεδομένων μέσω ενός φυσικού συνδέσμου.

Σε ένα συνεργατικό περιβάλλον, τα drones συνεργάζονται για να ξεπεράσουν πολλαπλές προκλήσεις που σχετίζονται με τις ασύρματες επικοινωνίες. Ακολουθούν ορισμένες βασικές πτυχές στο επίπεδο ζεύξης δεδομένων στις ασύρματες επικοινωνίες, ειδικά για τα ΣμηΕΑ:

Cooperative Relaying: Τα ΣμηΕΑ μπορούν να βοηθήσουν στη δημιουργία συνδέσεων επικοινωνίας μεταξύ άλλων ΣμηΕΑ ή μεταξύ ΣμηΕΑ και ενός επίγειου σταθμού. Με την αναμετάδοση πακέτων δεδομένων, επεκτείνουν το εύρος επικοινωνίας και βελτιώνουν την ισχύ του σήματος. Η συνεργατική αναμετάδοση μπορεί να μετριάσει τις επιπτώσεις της πτώσης ισχύος σήματος και των παρεμβολών, αυξάνοντας έτσι την αξιοπιστία και την κάλυψη των ασύρματων συνδέσεων επικοινωνίας.

Cooperative Beamforming: Η συνεργατική διαμόρφωση δέσμης είναι μια τεχνική που χρησιμοποιείται για τη συγκέντρωση της ισχύος μετάδοσης σε μια συγκεκριμένη κατεύθυνση, αυξάνοντας την ισχύ του σήματος προς τον δέκτη. Σε ένα συνεργατικό περιβάλλον, τα ΣμηΕΑ μπορούν να συνεργαστούν για να σχηματίσουν ένα δίκτυο διαμόρφωσης δέσμης. Συντονίζοντας τις μεταδόσεις τους και προσαρμόζοντας τα μοτίβα των κεραιών τους, μπορούν να δημιουργήσουν μια συνδυασμένη δέσμη με αυξημένη κατευθυντικότητα, οδηγώντας σε βελτιωμένη ποιότητα σήματος και μειωμένες παρεμβολές.

Multi-Hop Networking: Σε περιπτώσεις όπου η άμεση επικοινωνία μεταξύ ΣμηΕΑ δεν είναι εφικτή λόγω απόστασης ή εμποδίων, μπορεί να χρησιμοποιηθεί συνεργατική

δικτύωση multi-hop. Τα ΣμηΕΑ λειτουργούν ως μεσάζοντες για την προώθηση πακέτων δεδομένων από την πηγή στον προορισμό μέσω μιας σειράς αναπηδήσεων (hops). Κάθε ΣμηΕΑ μεταδίδει τα δεδομένα στο επόμενο ΣμηΕΑ μέχρι αυτά να φτάσουν στον προορισμό τους. Αυτή η συνεργατική προσέγγιση συμβάλλει στην επέκταση της περιοχής κάλυψης και στη βελτίωση της συνδεσιμότητας σε περιβάλλοντα μεγάλης κλίμακας ή με φυσικά και τεχνητά εμπόδια.

Συνεργατικά πρωτόκολλα MAC: Το πρωτόκολλο Medium Access Control (MAC) διέπει τον τρόπο με τον οποίο πολλές συσκευές μοιράζονται το διαθέσιμο ασύρματο μέσο. Σε συνεργατικά περιβάλλοντα, τα ΣμηΕΑ μπορούν να χρησιμοποιήσουν πρωτόκολλα συνεργασίας MAC που επιτρέπουν την αποτελεσματική κατανομή πόρων και τη διαχείριση παρεμβολών.

Ωστόσο, οι τρέχουσες προσεγγίσεις, δεν επιδεικνύουν ανθεκτικότητα στη διακοπή του επικοινωνιακού σήματος, κάτι συνηθισμένο στα ασύρματα δίκτυα.

5.1.2 Προβλήματα βελτιστοποίησης

Με δεδομένο ότι τα ΣμηΕΑ είναι συσκευές χαμηλής ενεργειακής ισχύος, η κατανάλωση ενέργειας κατά τη χρήση τους ως επικοινωνιακούς κόμβους είναι υψίστης σημασίας.

Για αυτό το λόγο τα σχήματα πολλαπλής πρόσβασης (multiple access – MA) ανάμεσα σε ΣμηΕΑ και σταθμούς βάσης, παίζουν σημαντικό ρόλο στην ενεργειακή απόδοση των σκαφών κατά την τηλεπικοινωνιακή τους χρήση.

Τα σχήματα RSMA (rate-splitting MA) και NOMA (non-orthogonal MA) για τη σύνδεση των ΣμηΕΑ σε δίκτυο κινητής τηλεφωνίας (δίκτυο κυψελών) σε συνδυασμό με τη βελτιστοποίηση των διανυσμάτων προκωδικοποίησης των δύο μέσω των μοτίβων διάδοσης σήματος των κεραιών 3GPP, σε ένα σενάριο κατερχόμενης ζεύξης κυμάτων mmWave, μας δίνουν μία ρεαλιστική απάντηση αναφορικά με την ενεργειακή απόδοση της χρήσης των δύο σχημάτων.

Στην περίπτωση των ΣμηΕΑ τα οποία συνδέονται μεταξύ τους με δίκτυα κυψελών, τα επίγεια ασύρματα δίκτυα εξυπηρετούν τα αεροσκάφη την ίδια στιγμή που οι χρήστες των υπηρεσιών των ΣμηΕΑ βρίσκονται στο έδαφος. Ενώ οι επίγειοι σταθμοί βάσης (base stations – BS) έχουν σχετικά σταθερά χαρακτηριστικά (π.χ. η κλίση των κεραιών εκπομπής σήματος), το μοτίβο διάδοσης σήματος μπορεί να διαμορφωθεί λαμβάνοντας υπόψη όχι μόνο τους επίγειους χρήστες αλλά και τα συμμετέχοντα ΣμηΕΑ μέσω προηγμένων τεχνικών διαμόρφωσης δέσμης σήματος.

Η μετάδοση σήματος NOMA επιτρέπει την εξυπηρέτηση πολλαπλών ΣμηΕΑ ταυτόχρονα, με τη συχνότητα και τους χωρικούς πόρους να ενισχύουν την αποδοτικότητα του φάσματος. Ωστόσο το NOMA πιθανώς να μην είναι το βέλτιστο σχήμα MA για κανάλι MISO (multiple input single output) εκτός από συνθήκες υπεροφόρτωσης όπου τα κανάλια των χρηστών συσχετίζονται σε μεγάλο βαθμό.

Επιπλέον, η βέλτιστη σειρά σύζευξης και αποκωδικοποίησης χρήστη είναι δύο κύρια μειονεκτήματα της στρατηγικής NOMA σε πρακτικές εφαρμογές, τα οποία αυξάνουν την πολυπλοκότητα του συστήματος. Η διαίρεση χώρου MA (SDMA), από την άλλη πλευρά, είναι πιο κατάλληλη για συνθήκες υποφόρτωσης, η οποία ωστόσο επιτυγχάνει χαμηλότερη απόδοση όταν το φορτίο δικτύου είναι υψηλό.

Το rate splitting MA (RSMA) από την άλλη θεωρείται ως αποτελεσματικότερο σχήμα MA συστήματα ασύρματης επικοινωνίας επόμενης γενιάς. Το RSMA είναι προτιμότερο

ανεξάρτητα από τις συνθήκες φόρτωσης δικτύου και στην πραγματικότητα επιτρέπει την ήπια γεφύρωση μεταξύ των δύο άκρων, του NOMA και του SDMA. [18]

5.2 Coding strategies

Αναφερόμενοι στα coding strategies στο link layer, εστιάζουμε κύρια στο network coding (κωδικοποίηση δικτύου).

Η κωδικοποίηση δικτύου είναι μια τεχνική δικτύωσης όπου οι λειτουργίες, οι οποίες στην πράξη τείνουν να είναι αλγεβρικοί αλγόριθμοι, εκτελούνται στα μεταδιδόμενα δεδομένα καθώς αυτά περνούν από τους κόμβους ενός δικτύου. Ενώ θεωρητικά οποιοσδήποτε τύπος αλγορίθμου θα μπορούσε να εκτελεστεί στα δεδομένα ενός κόμβου, οι τρέχοντες αλγόριθμοι NC (network coding) τείνουν να ασχολούνται με τη συσσώρευση των διαφόρων μεταδόσεων που διέρχονται από έναν δεδομένο κόμβο.

Στα παραδοσιακά δίκτυα δρομολόγησης, τα πακέτα απλώς αποθηκεύονται προσωρινά και στη συνέχεια προωθούνται στον επόμενο κόμβο του δικτύου. Ως εκ τούτου, εάν ένας κόμβος δρομολόγησης λαμβάνει δύο πακέτα από δύο διαφορετικές πηγές, θα τα προωθήσει διαδοχικά, ακόμη και αν και τα δύο απευθύνονται στον ίδιο προορισμό, ενώ θα τοποθετήσει στην «ουρά» τυχόν άλλα που μπορεί να λάβει στο μεταξύ. Αυτό έχει ως αποτέλεσμα ο κόμβος να δημιουργεί ξεχωριστά «πακέτα μετάδοσης» για κάθε μήνυμα που παραδίδεται, γεγονός που έχει ως αποτέλεσμα τη μείωση της αποτελεσματικότητας του δικτύου.

Το NC χρησιμοποιείται για να μετριάσει αυτό το φαινόμενο συγχωνεύοντας σχετικά μεταξύ τους μηνύματα στον κόμβο αναμετάδοσης, χρησιμοποιώντας μια δεδομένη κωδικοποίηση και, στη συνέχεια, προωθώντας αυτό το συσσωρευμένο αποτέλεσμα στον προορισμό για αποκωδικοποίηση. Για να λειτουργήσει αυτό, ο κόμβος προορισμού πρέπει να συγχρονιστεί με τους κόμβους μετάδοσης, ένας περιορισμός ιδιαίτερα σημαντικός όταν πρόκειται για κωδικοποίηση δικτύου που γίνεται στο φυσικό επίπεδο. [19]

5.2.1 Στρατηγικές προστασίας από σφάλματα

Εκτός από τις στρατηγικές κωδικοποίησης δεδομένων δικτύου, υπάρχουν και άλλες στρατηγικές κωδικοποίησης οι οποίες χρησιμοποιούνται για να προστατεύσουν την μεταδιδόμενη πληροφορία από λάθη και από τον, αποκαλούμενο, «θόρυβο».

Ο «θόρυβος» στα ασύρματα δίκτυα αναφέρεται σε οποιαδήποτε ανεπιθύμητα ή ενοχλητικά σήματα ή παρεμβολές που μπορούν να υποβαθμίσουν την ποιότητα της ασύρματης επικοινωνίας. Είναι ένα ανεπιθύμητο φαινόμενο που μπορεί να επηρεάσει αρνητικά την αξιοπιστία και την απόδοση των ασύρματων δικτύων.

Ο θόρυβος μπορεί να εκδηλωθεί με διάφορες μορφές:

Εξωτερικές παρεμβολές: Αυτός ο τύπος θορύβου προκύπτει από πηγές εκτός του ασύρματου δικτύου. Για παράδειγμα, γειτονικά ασύρματα δίκτυα που λειτουργούν στην ίδια ζώνη συχνοτήτων μπορεί να προκαλέσουν παρεμβολές. Άλλες συσκευές όπως φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα ή συσκευές Bluetooth μπορούν επίσης να εκπέμπουν σήματα που παρεμβαίνουν στην ασύρματη επικοινωνία.

Ατμοσφαιρικές παρεμβολές: Φυσικά φαινόμενα όπως ατμοσφαιρικές διαταραχές, κεραυνοί ή ηλιακή ακτινοβολία μπορούν να εισάγουν θόρυβο στο ασύρματο κανάλι. Παρόλο που αυτές οι πηγές είναι συνήθως πέρα από τον έλεγχό μας, μπορούν να επηρεάσουν την απόδοση του ασύρματου δικτύου.

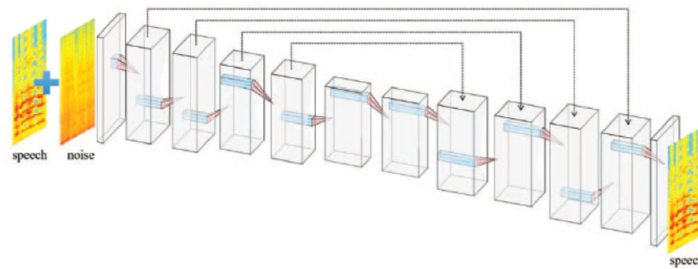
Εσωτερικές παρεμβολές: Οι εσωτερικές παρεμβολές συμβαίνουν όταν συσκευές εντός του δικτύου εισάγουν θόρυβο. Αυτό μπορεί να συμβεί όταν πολλές συσκευές σε

κοντινή απόσταση μεταδίδουν σήματα ταυτόχρονα, με αποτέλεσμα συγκρούσεις σήματος ή παρεμβολές.

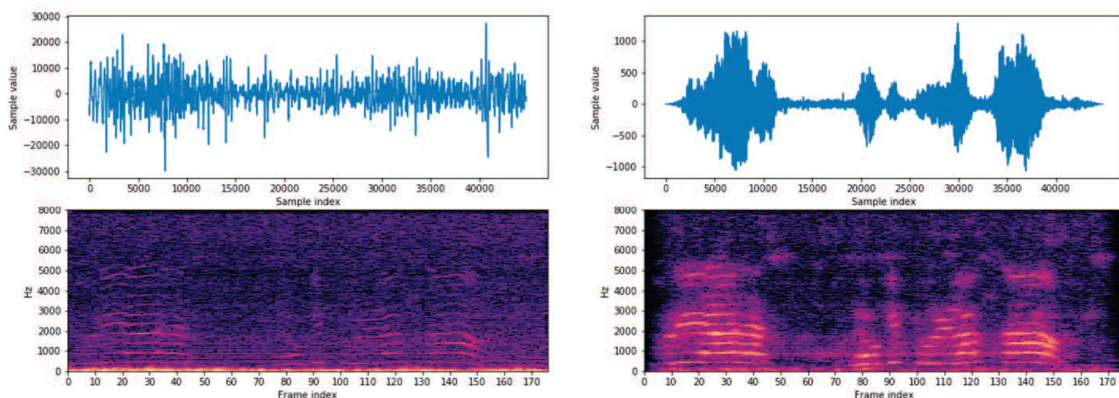
Χαρακτηριστικό παράδειγμα τεχνικής μείωσης του «θορύβου» είναι η χρήση ενός Deep Convolutional Autoencoder (συνελικτικός κωδικοποιητής) για τη μείωση του θορύβου στη λήψη ήχου από το ενσωματωμένο μικρόφωνο του drone. Αυτό είναι εξαιρετικά χρήσιμο όχι μόνο σε χρήσης λήψης βίντεο και ήχου για λόγους ευχαρίστησης αλλά ιδιαίτερα σε επιχειρήσεις όπου χρησιμοποιούνται ΣμηΕΑ σε δίκτυο και χρησιμοποιούν τον ήχο για ιδιαίτερα κρίσιμες εφαρμογές, π.χ. σε περιπτώσεις αναζήτησης αγνοουμένων μετά από φυσικές καταστροφές.

Ένας DCA χρησιμοποιείται για τη μείωση του θορύβου λόγω της πτήσης του drone και του ανέμου κατά τη μετάδοση εγγεγραμμένων ηχητικών σημάτων σε δίκτυα αισθητήρων ΣμηΕΑ. Χρησιμοποιεί συνελικτικά νευρωνικά δίκτυα (CNN) που εκπαιδεύονται με σύνολα δεδομένων που λαμβάνονται από την ανάμειξη των ήχων που παράγουν τα ΣμηΕΑ και των ήχων του ανέμου με ήχους ομιλίας.

Προκειμένου να εκπαιδευτεί ένα τέτοιο μοντέλο αυτόματου κωδικοποιητή, τα ηχητικά σήματα μετατρέπονται σε αναπαραστάσεις χρόνου-συχνότητας χρησιμοποιώντας βραχυπρόθεσμο μετασχηματισμό Fourier (STFT – short-time Fourier transform). [20]



Εικόνα 18: Συνολική δομή της προτεινόμενης μεθόδου μείωσης του θορύβου με τη χρήση αυτοκωδικοποιητή βαθιάς συνελικτικής αποθορυβοποίησης



Εικόνα 19: Σύγκριση κυματομορφών και φασμάτων σχετικά με το σήμα ομιλίας από το οποίο αφαιρείται η πτήση drone και ο θόρυβος του ανέμου με τη χρήση αυτόματου κωδικοποιητή βαθιάς συνελικτικής αποθορυβοποίησης

6. Επίπεδο δικτύου (Network layer)

6.1 Στρατηγικές συνεργασίας

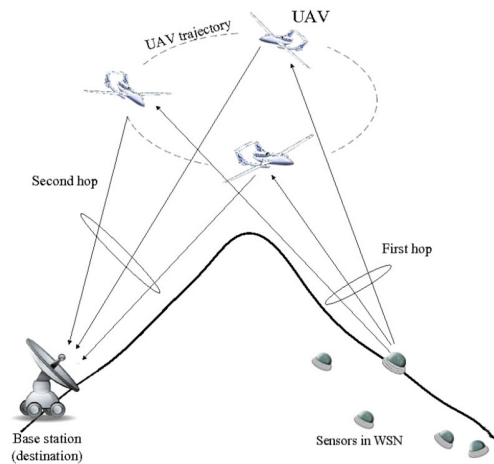
6.1.1 Ενεργειακή απόδοση, βελτίωση συνδεσιμότητας και συλλογή δεδομένων

Η συλλογή, μεταφορά και μετάδοση δεδομένων μέσω εναέριων μέσων (ΣμηΕΑ) θεωρείται μία εξαιρετικά ικανή λύση για την επέκταση της κάλυψης ασύρματων δικτύων αισθητήρων (WSN – wireless sensor networks) σε γεωγραφικές περιοχές ιδιαίτερων χαρακτηριστικών και υπό αντίξοες συνθήκες, όπως φυσικές καταστροφές και πεδία μάχης.

Η ίδια λύση προκρίνεται και σε περιπτώσεις συμβάντων έρευνας και διάσωσης αλλά και σε εμπορικές εφαρμογές όπως η γεωργική καλλιέργεια ακριβείας, η επόπτευση εγκαταστάσεων ΑΠΕ και εγκαταστάσεων εξόρυξης υδρογονανθράκων.

Η ανάπτυξη όμως τέτοιων δικτύων αντιμετωπίζει δύο εξαιρετικά κρίσιμες προκλήσεις, οι παράμετροι των οποίων δημιουργούν δυσκολίες. Η πρώτη είναι η αστάθεια του σήματος μεταξύ των εναέριων (ΣμηΕΑ) και των επίγειων κόμβων του δικτύου (σταθμοί βάσης και αισθητήρες δεδομένων), καθώς αυτή η αστάθεια προκαλεί απώλεια δεδομένων (πακέτων δεδομένων – packet loss). Η δεύτερη, και ίσως σημαντικότερη πρόκληση είναι η περιορισμένη χωρητικότητα των μπαταριών των ΣμηΕΑ, η οποία προκαλεί διακοπή της αναμετάδοσης δεδομένων λόγω ανάγκης επαναφόρτισης. Η ανάπτυξη δικτύων με τη συνεργασία πολλαπλών ΣμηΕΑ και χρήση των κατάλληλων αλγορίθμων προτεραιοποίησης μεταφοράς των δεδομένων μπορεί, σε ένα βαθμό, και τις δύο αυτές προκλήσεις.

Στην εικόνα 20 βλέπουμε μία τυπική διάταξη ενός συνεργατικού WSN για αναμετάδοση σε πραγματικό χρόνο περιβαλλοντικών δεδομένων, π.χ. από αισθητήρες φωτιάς μέσα σε δασική έκταση. Τα ΣμηΕΑ μεταφέρουν άμεσα τα δεδομένα από τους αισθητήρες στον Σταθμό Βάσης ώστε η καθυστέρηση μεταφοράς τους να μειώνεται στο μέγιστο δυνατό. Σε αυτήν όμως την περίπτωση η κατανάλωση ενέργειας των ΣμηΕΑ πρέπει να προσαρμόζεται διαφορετικά, ΣμηΕΑ τα οποία λαμβάνουν περισσότερα πακέτα δεδομένων από άλλα ή έχουν δυσκολία επικοινωνίας με τον Σταθμό Βάσης, θα καταναλώσουν περισσότερη ενέργεια και θα σταματήσει η λειτουργία τους με συνέπεια την «διάλυση» του δικτύου ή την σταδιακή υπερφόρτωση και των υπολοίπων ΣμηΕΑ.



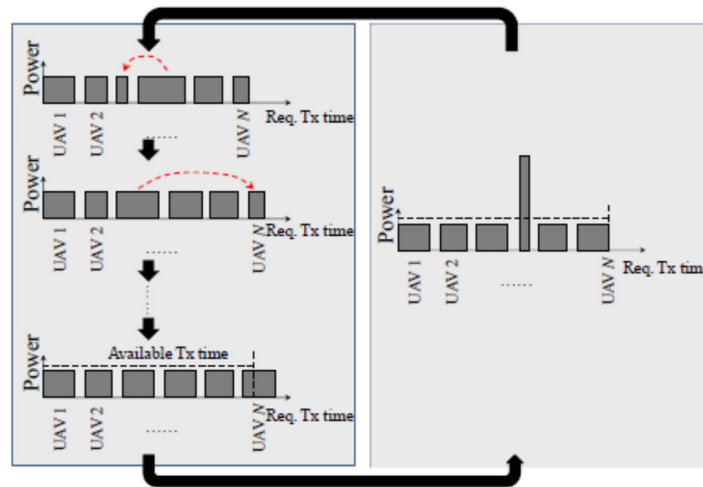
Εικόνα 20: Εναέρια δίκτυα αναμετάδοσης χρησιμοποιώντας συνεργατικά ΣμηΕΑ, όπου αυτά αναμεταδίδουν δεδομένα από απομακρυσμένους αισθητήρες προς σταθμό βάσης

Έχει αναπτυχθεί λύση για αυτό το διπλό πρόβλημα η οποία βελτιστοποιεί το πρόγραμμα αναμετάδοσης δεδομένων των ΣμηΕΑ, έτσι ώστε η κατανάλωση ενέργειάς του να ελαχιστοποιείται κάτω από ένα εγγυημένο BAR (bit error rate). Η ίδια λύση προτείνει έναν αποδοτικό μη βέλτιστο αλγόριθμο για τη μείωση της πολυπλοκότητας δημιουργίας του χρονοδιαγράμματος, όπου οι ενέργειες των ΣμηΕΑ είναι ισορροπημένες και οι ρυθμοί μετάδοσης των δεδομένων προσαρμόζονται με εναλλασσόμενο τρόπο. [21]

Η εικόνα 21 απεικονίζει τον προτεινόμενο αλγόριθμο προγραμματισμού που πραγματοποιήθηκε στον Σταθμό Βάσης, όπου οι δύο διαδικασίες ενεργειακής εξισορρόπησης και προσαρμογής ρυθμού αποσυνδέονται και αλληλοεπιδρούν μεταξύ τους.

Στη διαδικασία εξισορρόπησης ενέργειας, ο αλγόριθμος μειώνει τη διαφορά κατανάλωσης ενέργειας μεταξύ οποιουδήποτε ζεύγους ΣμηΕΑ, δεδομένης της διαμόρφωσης κάθε ενός. Όπως υποδεικνύεται από τα κόκκινα βέλη, η μεγαλύτερη διαφορά κατανάλωσης ενέργειας μειώνεται με τον επαναπρογραμματισμό μεταφοράς ορισμένων πακέτων δεδομένων από το πιο ενεργοβόρο ΣμηΕΑ στο λιγότερο ενεργοβόρο.

Η απαίτηση του χρόνου μετάδοσης μπορεί να αυξηθεί. Αυτό οφείλεται στο γεγονός ότι η ενεργειακή απόδοση είναι υψηλότερη όταν ισχύουν καλύτερες συνθήκες στο κανάλι επικοινωνίας του ΣμηΕΑ και του Σταθμού Βάσης. Επομένως, ο αλγόριθμος έχει σχεδιαστεί για να εκχωρεί περισσότερα πακέτα στα ΣμηΕΑ τα οποία έχουν καλύτερης ποιότητας κανάλια επικοινωνίας.



Εικόνα 21: απεικόνιση του προτεινόμενου αλγορίθμου, όπου το αριστερό πλαίσιο περιγράφει τη διαδικασία εξισορρόπησης ενέργειας δεδομένης της διαμόρφωσης κάθε ΣμηΕΑ. Το δεξί πλαίσιο δείχνει την αύξηση της διαμόρφωσης ώστε να ταιριάζει στον διαθέσιμο χρόνο μετάδοσης.

Στην εικόνα 22 είναι ο προτεινόμενος αλγόριθμος με όλες τις απαραίτητες λεπτομέρειες. Τα βήματα 4 έως 15 περιγράφουν τη διαδικασία εξισορρόπησης ενέργειας, όπου το i UAV στη διατεταγμένη ακολουθία ευρετηριάζεται με $I'(i)$ (βλέπε βήμα 12). Από το Βήμα 4 έως το 10, τα πακέτα δεδομένων εκχωρούνται δοκιμαστικά στα ΣμηΕΑ. Στα βήματα 11 έως 15, η διαφορά κατανάλωσης ενέργειας ελαχιστοποιείται αξιολογώντας κατά ζεύγη τα ΣμηΕΑ. Τα βήματα 16 έως 22 περιγράφουν τη διαδικασία προσαρμογής του ρυθμού μετάδοσης, όπου επιλέγεται το ΣμηΕΑ που μπορεί να μειώσει περισσότερο τον συνολικό χρόνο μετάδοσης. Αυτές οι δύο διαδικασίες επαναλαμβάνονται συνεχώς μέχρι να ικανοποιηθεί ο χρονικός περιορισμός, όπως υλοποιείται από τον εξωτερικό βρόχο, συγκεκριμένα, τα βήματα 3 και 23.

Algorithm 1 EPLA Algorithm

```

1: Initialise  $\rho_i = 1$ .
2: Sort all UAVs by  $\frac{\kappa_2^{-1} \ln(\frac{\kappa_1}{\epsilon})}{\gamma_t}$  in ascending order.
3: while EPLA is not completed do
4:   for  $i = [1, N_R]$  do
5:     if  $\frac{\kappa_2^{-1} \ln(\frac{\kappa_1}{\epsilon}) \cdot (2^{\rho_{\ell(i)}} - 1)}{\gamma_{\ell(i)}(t)} \leq P_{max}$  then
6:       Schedule UAV  $\ell(i)$  to transmit the data
       packets which have not been allocated.
7:     else
8:       The  $\gamma_{\ell(i)}(t)$  is too small, UAV  $\ell(i)$  is not
       scheduled to transmit.
9:     end if
10:  end for
11:  while  $|\pi(s_{\ell'(i)}, \rho_{\ell'(i)}, t) - \pi(s_{\ell'(j)}, \rho_{\ell'(j)}, t)|$  is min-
  imised do
12:    Sort the UAVs by  $\left[ |s_{\ell'(i)}| \cdot \delta_{\ell'(i)}(t) \cdot \frac{(2^{\rho_{\ell'(i)}} - 1)}{\rho_{\ell'(i)}} \right]$ 
    in descending order.
13:    UAV  $i$  has largest  $\pi(s_{\ell'(i)}, \rho_{\ell'(i)}, t)$  and UAV  $j$ 
    has smallest one.
14:    Allocate packet load from  $s_{\ell'(i)}$  to  $s_{\ell'(j)}$ .
15:  end while
16:  if  $\sum_{i=1}^{N_R} \frac{|s_{\ell'(i)}|}{\rho_{\ell'(i)}} \leq \frac{T}{\Sigma_p}$  then
17:    EPLA is completed.
18:    break
19:  else
20:    Sort the UAVs by  $\frac{|s_{\ell'(i)}| \cdot (2^{\rho_{\ell'(i)}} - 1)}{\rho_{\ell'(i)}}$  in descend-
    ing order,  $\ell'(i)$  has the largest value.
21:     $\rho_{\ell'(i)} \leftarrow \rho_{\ell'(i)} + 1$ .
22:  end if
23: end while

```

Εικόνα 22: Ο αλγόριθμός

Parameters	Values
\mathcal{Q}_p	32 bytes
M_R	100
T	10 milliseconds
P_{max}	5 W
N_0	3.98×10^{-12} W
N_R	$1, \dots, 20$
ϵ	0.05%
κ_1	0.2
κ_2	3
γ_0	3 dB

Εικόνα 23: Παραμετροποίηση προσομοιώσεων

Από τις προσομοιώσεις που πραγματοποιήθηκαν αποδείχθηκε ότι το προτεινόμενο σύστημα αναμετάδοσης δεδομένων με τη χρήση δικτύου ΣμηΕΑ είναι ενεργειακά αποδοτικό ενώ ταυτόχρονα πέτυχε να ισορροπήσει την σωστή μεταφορά δεδομένων με την βέλτιστη κατανάλωση ενέργειας.

Τα αποτελέσματα της προσομοίωσης έδειξαν ότι ο μη βέλτιστος αλγόριθμος μπόρεσε να μειώσει σημαντικά την υπολογιστική πολυπλοκότητα με αμελητέα υποβάθμιση της απόδοσης και της διάρκειας ζωής του δικτύου, σε σύγκριση με τη βέλτιστη λύση. Εξοικονομήθηκε ενέργεια σε ποσοστό 50%, αυξήθηκε η απόδοση του δικτύου κατά 15% ενώ η διάρκεια ζωής του αυξήθηκε κατά 33%, συγκριτικά με τους υπολοίπους αλγορίθμους που έχουν αναπτυχθεί για τον ίδιο σκοπό.

6.2 Πρωτόκολλα δρομολόγησης

6.2.1 FANETs

FANET σημαίνει Flying Ad hoc Network. Είναι ένας τύπος ad hoc δικτύου που αποτελείται από μια ομάδα αυτόνομων μη επανδρωμένων εναέριων οχημάτων (UAV - ΣμηΕΑ), τα οποία επικοινωνούν μεταξύ τους για να δημιουργήσουν ένα αυτορυθμιζόμενο εναέριο δίκτυο. Τα FANET έχουν σχεδιαστεί για να επιτρέπουν την επικοινωνία, τον συντονισμό και τη συνεργασία μεταξύ των ΣμηΕΑ για πολλές διαφορετικές εφαρμογές και επιχειρησιακά σενάρια.

Σε ένα FANET, κάθε ΣμηΕΑ λειτουργεί ως κόμβος του δικτύου, ικανός τόσο για μετάδοση όσο και για λήψη δεδομένων. Τα ΣμηΕΑ επικοινωνούν μεταξύ τους χρησιμοποιώντας τεχνολογίες ασύρματης επικοινωνίας όπως Wi-Fi, Bluetooth ή εξειδικευμένα πρωτόκολλα επικοινωνίας για ΣμηΕΑ ενώ αποτελούν μια δυναμική τοπολογία δικτύου, όπου η συνδεσιμότητα μεταξύ των ΣμηΕΑ αλλάζει συνεχώς.

Τα FANETs προσφέρουν πολλά πλεονεκτήματα και εφαρμογές, όπως:

Επιχειρήσεις έρευνας και διάσωσης: Τα FANETs μπορούν να χρησιμοποιηθούν σε αποστολές έρευνας και διάσωσης, όπου πολλαπλά ΣμηΕΑ συνεργάζονται για να αναζητήσουν επιζώντες ή να εντοπίσουν αντικείμενα σε απομακρυσμένες ή δυσπρόσιτες περιοχές.

Επιτήρηση και παρακολούθηση: Τα ΣμηΕΑ σε ένα FANET μπορούν να αναπτυχθούν και να εκτελέσουν επιχειρήσεις επιτήρησης και παρακολούθησης, όπως η παρακολούθηση της κυκλοφορίας, δασικών πυρκαγιών ή της άγριας ζωής, μεταδίδοντας δεδομένα σε πραγματικό χρόνο μεταξύ τους.

Αναμεταδότες πληροφορίας και δεδομένων: Τα FANET μπορούν να λειτουργήσουν ως αναμεταδότες πληροφορίας και δεδομένων, παρέχοντας προσωρινή συνδεσιμότητα δικτύου σε περιοχές όπου η επίγεια υποδομή δεν είναι διαθέσιμη ή έχει υποστεί ζημιά. Τα ΣμηΕΑ μπορούν να δημιουργήσουν ένα προσωρινό δίκτυο για την αναμετάδοση του τηλεπικοινωνιακού σήματος σε μεγάλες αποστάσεις, επεκτείνοντας το υπάρχον επίγειο δίκτυο.

Περιβαλλοντική παρακολούθηση: Τα FANET εξοπλισμένα με διάφορους αισθητήρες μπορούν να χρησιμοποιηθούν για σκοπούς περιβαλλοντικής παρακολούθησης, όπως η μέτρηση της ποιότητας του αέρα, της θερμοκρασίας ή των επιπέδων ρύπανσης.

Γεωργία ακριβείας: Τα ΣμηΕΑ σε ένα FANET μπορούν να χρησιμοποιηθούν για εφαρμογές γεωργίας ακριβείας, όπως η παρακολούθηση των καλλιεργειών, ο ψεκασμός

φυτοφαρμάκων ή η εκτίμηση της απόδοσης καλλιεργιών, με την ανταλλαγή δεδομένων και τον συντονισμό των μεταξύ τους ενεργειών.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι τα FANET αντιμετωπίζουν προκλήσεις όπως το περιορισμένο εύρος ζώνης, η δυναμική τοπολογία δικτύου, οι ενεργειακοί περιορισμοί και η διασφάλιση ασφαλούς και αξιόπιστης επικοινωνίας παρουσία άλλων εναέριων οχημάτων ή εμποδίων. Η έρευνα επικεντρώνεται στην αντιμετώπιση αυτών των προκλήσεων και στην ανάπτυξη αποτελεσματικών πρωτοκόλλων επικοινωνίας, αλγορίθμων δρομολόγησης και μηχανισμών αποφυγής συγκρούσεων ειδικά για τα FANET.

Υπάρχουν δύο κύριοι τύποι πρωτοκόλλων ad-hoc δρομολόγησης: Πρωτόκολλα αντίδρασης και προληπτικά πρωτόκολλα.

- Πρωτόκολλα αντίδρασης (Reactive Protocols)

Το Reactive πρωτόκολλο χωρίζεται σε δύο τύπους - Ad hoc On-Demand Distance Vector (AODV) και Temporary Ordering Routing Algorithms (TORA). Στο πρωτόκολλο δρομολόγησης AODV, το έργο του κόμβου είναι ανεξάρτητο και δεν μεταφέρει τις πληροφορίες άλλων κόμβων ή παρακείμενου κόμβου στο δίκτυο. Αυτοί οι κόμβοι αποτελούνται από τις πληροφορίες της διαδρομής από την οποία πρέπει να μεταφερθούν τα δεδομένα, έτσι ώστε η διαβίβαση του πακέτου πληροφοριών να ακολουθείται από προκαθορισμένη διαδρομή. Το TORA είναι μια πολύ προσαρμοστική και αποτελεσματική διαδικασία, καθώς λειτουργεί με όλες τις συντομότερες δυνατές διαδρομές από την πηγή στον προορισμό. Σε αυτόν τον τύπο πρωτοκόλλου, κάθε κόμβος μεταφέρει τις πληροφορίες των γειτονικών κόμβων του. Έχει επίσης τη δυνατότητα να εξασφαλίσει τη διαδρομή των δεδομένων, τη δημιουργία διαδρομής και να διαγράψει τη διαδρομή εάν υπάρχει οποιαδήποτε εσωτερική διαμερισματοποίηση εντός του δικτύου. [22]

- Προληπτικά πρωτόκολλα (Proactive Protocols)

Τα προληπτικά πρωτόκολλα δρομολόγησης, γνωστά και ως πρωτόκολλα δρομολόγησης βάσει πίνακα, είναι ένας τύπος πρωτοκόλλου δρομολόγησης που χρησιμοποιείται σε ad hoc δίκτυα, όπως είναι τα FANETs. Σε αντίθεση με τα reactive πρωτόκολλα που καθορίζουν διαδρομές κατ' απαίτηση, τα προληπτικά πρωτόκολλα διατηρούν και ενημερώνουν συνεχώς τις πληροφορίες δρομολόγησης, ανεξάρτητα από το αν υπάρχει άμεση ανάγκη μετάδοσης δεδομένων. Αυτά τα πρωτόκολλα διασφαλίζουν ότι κάθε κόμβος στο δίκτυο έχει ενημερωμένες πληροφορίες δρομολόγησης, οι οποίες επιτρέπουν ταχύτερη μετάδοση δεδομένων όταν χρειάζεται.

Ένα ευρέως χρησιμοποιούμενο πρωτόκολλο προληπτικής δρομολόγησης σε ad hoc δίκτυα είναι το πρωτόκολλο Optimized Link State Routing (OLSR). Ας εμβαθύνουμε στις λεπτομέρειες του OLSR για να κατανοήσουμε πώς λειτουργούν τα προληπτικά πρωτόκολλα δρομολόγησης:

Περιοδική ενημέρωση:

Στα προληπτικά πρωτόκολλα, κάθε κόμβος μεταδίδει περιοδικά μηνύματα ελέγχου, γνωστά ως μηνύματα "hello", στους γειτονικούς κόμβους του. Τα μηνύματα Hello χρησιμοποιούνται για την ανίχνευση της παρουσίας γειτονικών κόμβων και τη διατήρηση μιας λίστας γειτόνων.

Ενημέρωση κατάστασης σύνδεσης:

Εκτός από τα μηνύματα hello, τα προληπτικά πρωτόκολλα χρησιμοποιούν ενημερώσεις κατάστασης σύνδεσης (LSA: link-state advertisement) για τη διάδοση πληροφοριών δρομολόγησης σε όλο το δίκτυο. Οι LSA περιέχουν πληροφορίες σχετικά με τους γείτονες του κόμβου και την κατάσταση σύνδεσής τους. Κάθε κόμβος στέλνει το LSA του σε όλους τους άλλους κόμβους του δικτύου για να διασφαλίσει ότι έχουν ακριβή αναπαράσταση της τοπολογίας του δικτύου.

Συντήρηση πίνακα δρομολόγησης:

Με βάση τις ληφθείσες LSA, κάθε κόμβος δημιουργεί και διατηρεί τον πίνακα δρομολόγησης του, ο οποίος περιέχει πληροφορίες σχετικά με τις διαθέσιμες διαδρομές για να επικοινωνήσει με τους υπόλοιπους κόμβους του δικτύου. Ο πίνακας δρομολόγησης ενημερώνεται δυναμικά καθώς αλλάζει η τοπολογία δικτύου ή λαμβάνονται νέες LSA.

Υπολογισμός συντομότερης διαδρομής:

Τα προληπτικά πρωτόκολλα χρησιμοποιούν έναν αλγόριθμο συντομότερης διαδρομής, όπως ο αλγόριθμος Dijkstra, για τον υπολογισμό των συντομότερων διαδρομών από έναν κόμβο σε όλους τους άλλους κόμβους του δικτύου. Αυτές οι πληροφορίες αποθηκεύονται στον πίνακα δρομολόγησης και χρησιμοποιούνται για την προώθηση πακέτων δεδομένων κατά μήκος των συντομότερων διαδρομών.

Βελτιστοποίηση διαδρομής:

Για τη μείωση του overhead, τα προληπτικά πρωτόκολλα χρησιμοποιούν τεχνικές βελτιστοποίησης διαδρομής. Αντί να προωθούν τις LSA σε ολόκληρο το δίκτυο, τα προληπτικά πρωτόκολλα χρησιμοποιούν επιλεκτική προώθηση με βάση τους υπολογισμούς της συντομότερης διαδρομής. Αυτή η βελτιστοποίηση ελαχιστοποιεί την ποσότητα των πληροφοριών δρομολόγησης που ανταλλάσσονται και μειώνει τη συμφόρηση του δικτύου.

Τα προληπτικά πρωτόκολλα δρομολόγησης προσφέρουν πλεονεκτήματα όπως χαμηλή καθυστέρηση εγκατάστασης διαδρομής και άμεση διαθεσιμότητα διαδρομών όταν απαιτείται μετάδοση δεδομένων. Είναι ιδιαίτερα χρήσιμα σε σενάρια όπου αναμένεται συχνή και συνεχής επικοινωνία και η διατήρηση μιας προκαθορισμένης υποδομής δρομολόγησης είναι εφικτή.

Ωστόσο, τα προληπτικά πρωτόκολλα έχουν ορισμένους περιορισμούς. Ενδέχεται να επιβαρυνθούν με υψηλότερο overhead μηνυμάτων ελέγχου σε σύγκριση με τα reactive πρωτόκολλα λόγω συνεχών ενημερώσεων των LSA. Επιπλέον, τα προληπτικά πρωτόκολλα καταναλώνουν περισσότερους πόρους του δικτύου, όπως εύρος ζώνης και ενέργεια, καθώς κάθε κόμβος διατηρεί πληροφορίες δρομολόγησης ανεξάρτητα από το αν συμμετέχει ενεργά στη μετάδοση δεδομένων.

Αξίζει να σημειωθεί ότι υπάρχουν και άλλα προληπτικά πρωτόκολλα δρομολόγησης εκτός από το OLSR, όπως το πρωτόκολλο Destination-Sequenced Distance Vector (DSDV) και το πρωτόκολλο ασύρματης δρομολόγησης (WRP). Κάθε πρωτόκολλο έχει τους δικούς του μηχανισμούς και βελτιστοποιήσεις, αλλά η βασική ιδέα της συνεχούς διατήρησης των πληροφοριών δρομολόγησης παραμένει σταθερή.

6.2.2 Δρομολόγηση A2G

Οι στρατηγικές δρομολόγησης αέρος-εδάφους (A2G) αναφέρονται στις τεχνικές δρομολόγησης και τα πρωτόκολλα που χρησιμοποιούνται σε δίκτυα επικοινωνίας όπου μεταδίδονται δεδομένα μεταξύ αερομεταφερόμενων οχημάτων, όπως μη επανδρωμένα εναέρια οχήματα (ΣμηΕΑ) ή αεροσκάφη, και επίγειων κόμβων ή υποδομών. Αυτές οι στρατηγικές δρομολόγησης διαδραματίζουν κρίσιμο ρόλο στην αποτελεσματική και αξιόπιστη επικοινωνία σε περιβάλλοντα A2G.

Ορισμένες βασικές στρατηγικές δρομολόγησης σε περιβάλλοντα A2G είναι οι ακόλουθες:

Άμεση επικοινωνία:

Σε ορισμένες περιπτώσεις, η επικοινωνία A2G μπορεί να επιτευχθεί μέσω άμεσων συνδέσεων μεταξύ αερομεταφερόμενων οχημάτων και επίγειων κόμβων. Αυτή η στρατηγική είναι κατάλληλη όταν η απόσταση μεταξύ του αεροσκάφους και των επίγειων κόμβων είναι σχετικά μικρή και δεν υπάρχουν σημαντικά εμπόδια ή περιορισμοί σήματος. Η άμεση επικοινωνία μπορεί να επιτευχθεί χρησιμοποιώντας τεχνολογίες όπως Wi-Fi, κυψελοειδή δίκτυα ή dedicated communication links.

Δρομολόγηση βάσει προτεραιοποίησης:

Η επικοινωνία A2G συχνά περιλαμβάνει την αναμετάδοση δεδομένων μέσω ενδιάμεσων κόμβων ή προτεραιοποίησης, τα οποία μπορεί να είναι είτε άλλα εναέρια οχήματα είτε επίγεια υποδομή. Οι στρατηγικές δρομολόγησης relaying είναι χρήσιμες όταν το εύρος άμεσης επικοινωνίας μεταξύ του αεροσκάφους και των κόμβων εδάφους είναι περιορισμένο. Οι αναμεταδοτές (relays) μπορούν να τοποθετηθούν στρατηγικά για να επεκτείνουν το εύρος επικοινωνίας ή να ξεπεράσουν φυσικά και τεχνητά εμπόδια που βρίσκονται στη διαδρομή. Πρωτόκολλα δρομολόγησης όπως το Ad hoc On-Demand Distance Vector (AODV) ή το Optimized Link State Routing (OLSR) μπορούν να χρησιμοποιηθούν για τη δημιουργία και τη συντήρηση των διαδρομών αναμετάδοσης.

Δρομολόγηση πολλαπλών διαδρομών (multi-hop routing):

Σε σενάρια όπου η απόσταση μεταξύ του αεροσκάφους και των επίγειων κόμβων είναι σημαντική ή όταν η άμεση επικοινωνία δεν είναι εφικτή, μπορούν να χρησιμοποιηθούν στρατηγικές δρομολόγησης πολλαπλών διαδρομών. Η δρομολόγηση πολλαπλών αναπηδήσεων περιλαμβάνει την αναμετάδοση δεδομένων μέσω μιας σειράς ενδιάμεσων κόμβων, σχηματίζοντας μια διαδρομή από το αεροσκάφος προέλευσης στον κόμβο εδάφους. Κάθε ενδιάμεσος κόμβος λαμβάνει το πακέτο δεδομένων και το προωθεί στον επόμενο μέχρι να φτάσει στον προορισμό. Πρωτόκολλα δρομολόγησης όπως το Dynamic Source Routing (DSR) ή το Ad hoc Multicast Routing Protocol (AMRoute) μπορούν να χρησιμοποιηθούν για τη δημιουργία και τη διατήρηση των multihop διαδρομών.

Δρομολόγηση υποβοηθούμενη από υποδομή (Infrastructure-Assisted Routing):

Τα δίκτυα A2G μπορούν επίσης να αξιοποιήσουν επίγειες υποδομές, όπως σταθμούς βάσης ή σημεία πρόσβασης, για να διευκολύνουν την επικοινωνία με το αεροσκάφος. Αυτοί οι κόμβοι υποδομής μπορούν να χρησιμεύσουν ως αναδρομολογητές, παρέχοντας συνδεσιμότητα μεταξύ του αεροσκάφους και των επίγειων δικτύων. Οι στρατηγικές δρομολόγησης μπορούν να σχεδιαστούν για να επωφεληθούν από τους κόμβους υποδομής, βελτιστοποιώντας την επιλογή διαδρομής και βελτιώνοντας τη συνολική απόδοση του δικτύου.

Δρομολόγηση ανάλογα με την κίνηση (Traffic-Aware Routing):

Σε περιβάλλοντα A2G με διαφορετικές συνθήκες δικτύου και φόρτο traffic, οι στρατηγικές δρομολόγησης με επίγνωση της κυκλοφορίας καθίστανται ζωτικής σημασίας. Αυτές οι στρατηγικές περιλαμβάνουν τη δυναμική προσαρμογή των αποφάσεων δρομολόγησης με βάση τη συμφόρηση του δικτύου, την ποιότητα σύνδεσης ή άλλες μετρήσεις απόδοσης. Τα πρωτόκολλα δρομολόγησης ανάλογα με την κυκλοφορία μπορούν να χρησιμοποιήσουν την παρακολούθηση του δικτύου, την εξισορρόπηση του φόρτου κυκλοφορίας ή τους μηχανισμούς ελέγχου συμφόρησης για τη βελτιστοποίηση της παροχής δεδομένων και τη διασφάλιση της αποτελεσματικής χρήσης των πόρων του δικτύου.

Η επιλογή μιας συγκεκριμένης στρατηγικής δρομολόγησης εξαρτάται από παράγοντες όπως οι απαιτήσεις της εφαρμογής, η τοπολογία δικτύου, η διαθέσιμη υποδομή και τα χαρακτηριστικά του περιβάλλοντος A2G. Ενδέχεται να απαιτούνται προσαρμοσμένες ή υβριδικές στρατηγικές δρομολόγησης για την αντιμετώπιση των

ιδιαιτερών καταστάσεων και περιορισμών της επικοινωνίας, συμπεριλαμβανομένων των παρεμβολών σήματος, της κινητικότητας και των δυναμικών συνθηκών του δικτύου.

6.2.3 VANETs

VANET σημαίνει Vehicular Ad hoc Network. Πρόκειται για ένα είδος ad hoc δικτύου ειδικά σχεδιασμένου για την επικοινωνία μεταξύ οχημάτων και μεταξύ οχημάτων και παρόδων υποδομών. Τα VANET αξιοποιούν τεχνολογίες ασύρματης επικοινωνίας για να επιτρέψουν την επικοινωνία οχήματος προς όχημα (V2V) και οχήματος προς υποδομή (V2I), σχηματίζοντας ένα δυναμικό δίκτυο που διευκολύνει την ανταλλαγή πληροφοριών για διάφορους σκοπούς.

Ακολουθούν ορισμένες βασικές πτυχές και χαρακτηριστικά των VANET:

Τεχνολογίες Επικοινωνιών:

Τα VANET χρησιμοποιούν τεχνολογίες ασύρματης επικοινωνίας, όπως η αποκλειστική επικοινωνία μικρής εμβέλειας (DSRC) ή η κυψελοειδής επικοινωνία οχήματος προς τα πάντα (C-V2X) για τη δημιουργία συνδεσιμότητας μεταξύ οχημάτων και υποδομών. Το DSRC λειτουργεί στη ζώνη συχνοτήτων των 5,9 GHz και έχει σχεδιαστεί ειδικά για επικοινωνία V2V και V2I, ενώ το C-V2X αξιοποιεί τα υπάρχοντα κυψελοειδή δίκτυα για να επιτρέψει την επικοινωνία.

Επικοινωνία V2V:

Τα VANET επιτρέπουν την άμεση επικοινωνία μεταξύ οχημάτων σε κοντινή απόσταση. Η επικοινωνία V2V επιτρέπει στα οχήματα να ανταλλάσσουν πληροφορίες σε πραγματικό χρόνο, όπως θέση, ταχύτητα, επιτάχυνση και άλλα σχετικά δεδομένα. Αυτό επιτρέπει συνεργατικές εφαρμογές, συμπεριλαμβανομένης της αποφυγής συγκρούσεων, της διαχείρισης της κυκλοφοριακής συμφόρησης, για τη βελτίωση της κίνησής τους και της ασφάλειας.

Επικοινωνία V2I:

Τα VANET υποστηρίζουν επίσης την επικοινωνία μεταξύ οχημάτων και οδικών υποδομών, όπως φανάρια, πινακίδες κυκλοφορίας και ευφυή συστήματα μεταφορών. Η επικοινωνία V2I επιτρέπει στα οχήματα να λαμβάνουν πληροφορίες σχετικά με τις συνθήκες κυκλοφορίας, τους οδικούς κινδύνους, τα σήματα κυκλοφορίας και άλλα σχετικά δεδομένα. Αυτές οι πληροφορίες βοηθούν τους οδηγούς στη λήψη αποφάσεων και βελτιώνουν τη συνολική διαχείριση της κυκλοφορίας και την ασφάλεια.

Εφαρμογές Ασφάλειας:

Οι εφαρμογές ασφάλειας αποτελούν σημαντικό στόχο των VANET. Οι εφαρμογές αυτές αποσκοπούν στη βελτίωση της οδικής ασφάλειας, επιτρέποντας στα οχήματα να ανταλλάσσουν κρίσιμες πληροφορίες σχετικά με την ασφάλεια. Παραδείγματα εφαρμογών ασφάλειας περιλαμβάνουν την προειδοποίηση σύγκρουσης, την ασφάλεια μίας διασταύρωσης, την ειδοποίηση για παρουσία οχήματος έκτακτης ανάγκης και συστήματα προειδοποίησης οδικού κινδύνου. Τα VANET παρέχουν την υποκείμενη επικοινωνιακή υποδομή που απαιτείται για την αποτελεσματική λειτουργία τέτοιων εφαρμογών ασφάλειας.

Αποδοτικότητα και διαχείριση της κυκλοφορίας:

Τα VANET προσφέρουν δυνατότητες βελτιστοποίησης της κυκλοφοριακής ροής και τη βελτίωση της συνολικής αποδοτικότητας της κυκλοφορίας. Με την ανταλλαγή πληροφοριών σχετικά με τις συνθήκες κυκλοφορίας, τη συμφόρηση και τις εναλλακτικές διαδρομές, οι οδηγοί (ή ακόμα και τα μελλοντικά αυτόνομα οχήματα) μπορούν να

αποφάσεις για την αποφυγή κυκλοφοριακής συμφόρησης, τη βελτιστοποίηση της διαδρομής κίνησης, ακόμα και τη μείωση κατανάλωσης καυσίμου.

Προκλήσεις και δυσκολίες:

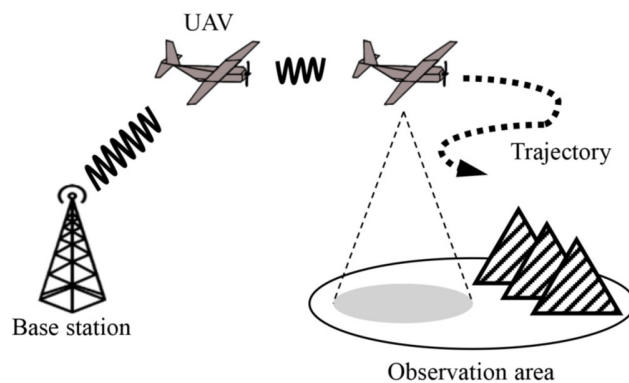
Τα VANET αντιμετωπίζουν προκλήσεις όπως τη δυναμική τοπολογία δικτύου, τη συχνή κινητικότητα των οχημάτων-κόμβων, τις παρεμβολές σήματος και την επεκτασιμότητα. Επιπλέον, η διασφάλιση της ασφάλειας, του απορρήτου και της αξιοπιστίας της επικοινωνίας στα VANET είναι ζωτικής σημασίας για την πρόληψη κακόβουλων δραστηριοτήτων και την προστασία ευαίσθητων πληροφοριών.

Για όλους τους παραπάνω λόγους, τα VANET βρίσκονται συνεχώς κάτω από το «μικροσκόπιο» των ερευνητών, με πολυάριθμες συνεχιζόμενες προσπάθειες για την τυποποίηση των πρωτοκόλλων επικοινωνίας, τη βελτίωση των διαθέσιμων τεχνολογιών και την ανάπτυξη προηγμένων εφαρμογών για τα συστήματα μεταφορών. Η ενσωμάτωση των VANET με αναδυόμενες τεχνολογίες όπως τα αυτόνομα οχήματα και οι έξυπνες πόλεις παρέχει εξαιρετικές προοπτικές για την ενίσχυση της ασφάλειας των μεταφορών, της αποδοτικότητας των οχημάτων και της συνολική βελτίωση της οδηγικής εμπειρίας.

6.3 Σχήματα αναμετάδοσης

6.3.1 Αναμετάδοση UAV-BS

Είναι αξιοσημείωτη η ικανότητα των ΣμηΕΑ να παρατηρούν το έδαφος σε μία περιοχή ενδιαφέροντος και με μεγάλη ευκολία να συλλέγουν πληροφορίες (εικόνες, βίντεο και δεδομένα εναέριων και επίγειων αισθητήρων) ενώ ταυτόχρονα μπορούν να μεταδίδουν τις πληροφορίες αυτές στους σταθμούς εδάφους. Λόγω όμως του πεπερασμένου ορίου λειτουργίας των ΣμηΕΑ (λόγω τροφοδοσίας ενέργειας και λόγω απόστασης από τους σταθμούς βάσης), είναι απαραίτητη η μεταξύ τους επικοινωνία και συνεργασία για τη μετάδοση των δεδομένων, ειδικά αυτών που απαιτείται να διατηρούν υψηλή την ποιότητά τους, σε μεγάλες αποστάσεις.



Εικόνα 24: Επισκόπηση εδάφους από ΣμηΕΑ

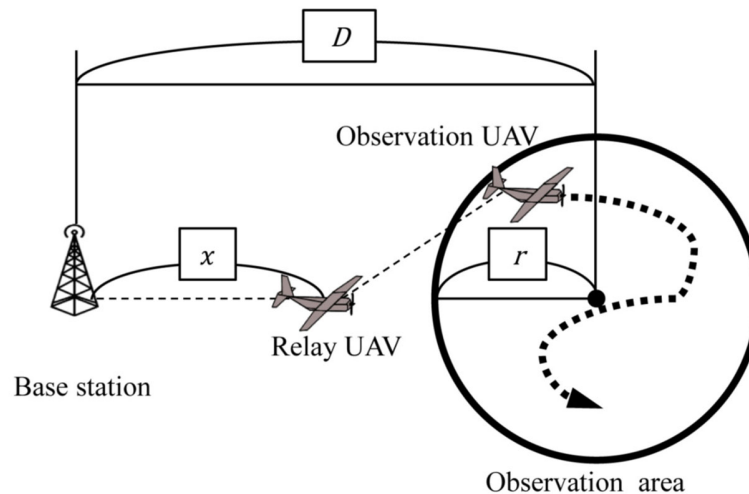
Παραδείγματα χρήσης των ΣμηΕΑ για επόπτευση, παρατήρηση περιοχών και συλλογή δεδομένων είναι η στρατιωτική επιτήρηση συνόρων, η επόπτευση περιοχών μετά από φυσικές καταστροφές, η δημιουργία χαρτών κ.λπ.

Εάν για τις ανωτέρω επιχειρήσεις χρησιμοποιηθούν επανδρωμένα αεροσκάφη (αεροπλάνα ή ελικόπτερα), η προσέγγιση της περιοχής ενδιαφέροντος είναι δύσκολη τόσο λόγω του πιθανού κινδύνου για τους επιβάτες και το αεροσκάφος όσο και λόγω της πιθανότατης έλλειψης χώρους προσγείωσης και απογείωσης.

Σε αντίθεση με το παραπάνω, τα ΣμηΕΑ μπορούν να προσεγγίσουν την περιοχή με μηδενικό κίνδυνο για τον χειριστή, με ευκολία προσγείωσης και απογείωσης αλλά και με εξαιρετικά χαμηλό κόστος λειτουργίας, συντήρησης ή, ακόμα, και αντικατάστασης σε περίπτωση πτώσης.

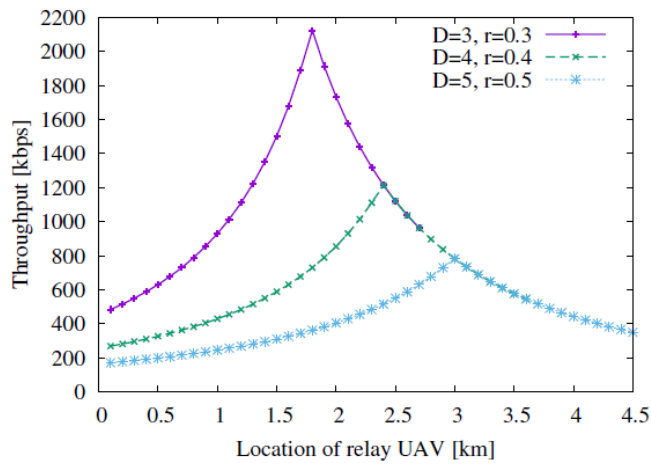
Επιπλέον, τα ΣμηΕΑ μπορούν να μεταδώσουν οποιοδήποτε είδος πληροφορίας και δεδομένων, αρκεί να είναι εξοπλισμένα με τον κατάλληλο τύπο και μέγεθος κεραίας. Σε αυτή όμως την περίπτωση υπάρχει περιορισμός καθώς το μειωμένο payload των ΣμηΕΑ περιορίζει και το μέγεθος της κεραίας που μπορεί να τοποθετηθεί σε αυτά με αποτέλεσμα τον περιορισμό της περιοχής που μπορεί να εφοπτευθεί και τον χρόνο που μπορεί να διατηρηθεί το ΣμηΕΑ σε πτήση. Συνεπώς, εάν ένα και μόνο ΣμηΕΑ έχει ως αποστολή τη λήψη και μετάδοση εικόνων από μία περιοχή όπου έχει συμβεί μία φυσική καταστροφή το εύρος επικοινωνίας είναι περιορισμένο. Προς τούτο και κατευθυνόμεστε στη χρήση σμηνών ΣμηΕΑ τα οποία επικοινωνούν μεταξύ τους. Αυτό αποκαλείται "UAV network" («Δίκτυο ΣΜηΕΑ»). Το ένα ΣμηΕΑ συλλέγει τα δεδομένα και τα μεταδίδει σε ένα άλλο το οποίο βρίσκεται εγγύτερα στον σταθμό βάσης. Αυτό σε κάποιο άλλο κ.ο.κ έως ότου τα δεδομένα μεταφερθούν στον σταθμό βάσης επιτυγχάνοντας την επιτήρηση περιοχών, κυριολεκτικά, σε πραγματικό χρόνο και με υψηλή ποιότητα μετάδοσης.

Στην εξαιρετική τους εργασία με τον τίτλο «Throughput Maximization for Long-Distance Real-Time Data Transmission over Multiple UAVs» οι ερευνητές εξέτασαν ένα απολύτως αληθοφάνες σενάριο όπου ένα ΣμηΕΑ επιτηρεί μία κυκλική περιοχή, μεταδίδει σε πραγματικό χρόνο τα δεδομένα σε ένα ΣμηΕΑ-αναμεταδότη και αυτό με τη σειρά του στον σταθμό βάσης. [23]



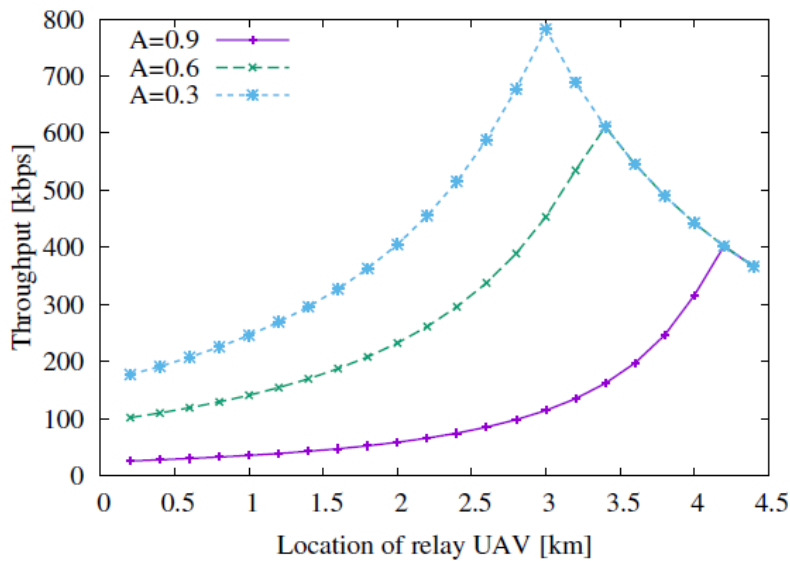
Εικόνα 25: Υποτιθέμενο δίκτυο ΣμηΕΑ

Σύμφωνα με τα αποτελέσματα της έρευνάς τους και όπως φαίνεται στην εικόνα 26, λόγω της αύξησης του μεγέθους του δικτύου, η απόδοση μειώνεται στο σύνολό της. Επιπλέον, η βέλτιστη θέση του ΣμηΕΑ-αναμεταδότη είναι μακρύτερα από το σταθμό βάσης όσο μεγαλύτερο είναι το δίκτυο. Αυτό συμβαίνει επειδή η απόσταση μετάδοσης είναι μεγαλύτερη, καθώς το μέγεθος του δικτύου είναι μεγαλύτερο. Επίσης, η βέλτιστη θέση του ΣμηΕΑ-αναμεταδότη είναι πάντα στην καμπύλη του ρυθμού σύνδεσης μεταξύ του σταθμού βάσης και του ΣμηΕΑ-αναμεταδότη.



Εικόνα 26: Επίδραση του μεγέθους του δικτύου στο ανώτερο όριο ταχύτητας μεταγωγής

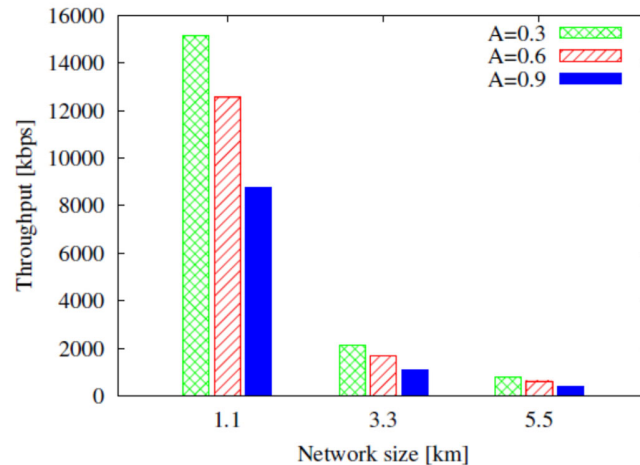
Στην εικόνα 27 φαίνεται ότι λόγω της αύξησης του ρυθμού εξασθένησης, η απόδοση μειώνεται επίσης στο σύνολό της. Στη σύνδεση μεταξύ του αναμεταδότη και του ΣμηΕΑ παρατήρησης, ο ρυθμός σύνδεσης μειώνεται λόγω των εμποδίων. Δεδομένου ότι αυτό δημιουργεί συμφόρηση, η απόδοση μειώνεται. Η βέλτιστη θέση του αναμεταδότη είναι πάντα στην καμπύλη του ρυθμού σύνδεσης μεταξύ του σταθμού βάσης και του αναμεταδότη.



Εικόνα 27: Επίδραση της εξασθένησης που προκαλείται από εμπόδια στο ανώτερο όριο ταχύτητας μεταγωγής

Τέλος, η αξιολόγηση της διακύμανσης του ανώτερου ορίου ταχύτητας μεταγωγής που επηρεάζεται από το μέγεθος του δικτύου και τον ρυθμό εξασθένησης καταδεικνύεται στην εικόνα 28. Εκεί φαίνεται η διακύμανση των θεωρητικών τιμών της μέγιστης απόδοσης όταν αλλάζουμε το μέγεθος του δικτύου ή το ρυθμό εξασθένησης. Επομένως, εάν ρυθμιστούν οι παράμετροι που σχετίζονται με το μέγεθος του δικτύου και διαγραφεί ο ρυθμός εξασθένησης, ο ρυθμός μετάδοσης δεδομένων σε πραγματικό χρόνο είναι

προβλέψιμος. Με άλλα λόγια, εάν αποφασιστεί ο απαιτούμενος ρυθμός δεδομένων για τη συλλογή των παρατηρούμενων δεδομένων, η κατά προσέγγιση τιμή του μεγέθους του δικτύου είναι φυσικά σταθερή.



Εικόνα 28: Επίδραση της διακύμανσης τόσο του μεγέθους του δικτύου όσο και του ρυθμού εξασθένισης στο ανώτερο όριο ταχύτητας μεταγωγής

6.3.2 Επικοινωνίες mmWave

Οι επικοινωνίες mmWave, επίσης γνωστές ως επικοινωνίες χιλιοστομετρικών κυμάτων, είναι μια τεχνολογία ασύρματης επικοινωνίας που λειτουργεί στην περιοχή συχνοτήτων 3 έως 300 gigahertz (GHz).

Στα βασικά χαρακτηριστικά της τεχνολογίας mmWave περιλαμβάνεται:

Υψηλοί ρυθμοί δεδομένων: Λόγω του μεγάλου εύρους ζώνης που διατίθεται στις συχνοότητες mmWave, επιτρέπονται σημαντικά υψηλότεροι ρυθμοί μετάδοσης δεδομένων σε σύγκριση με τις ζώνες χαμηλότερων συχνοτήτων. Αυτό καθιστά τη συγκεκριμένη τεχνολογία κατάλληλη για εφαρμογές που απαιτούν εξαιρετικά γρήγορη μεταφορά δεδομένων, όπως ροή βίντεο 4K/8K, εικονική πραγματικότητα (VR) και επαυξημένη πραγματικότητα (AR).

Αυξημένη χωρητικότητα: Το μεγάλο εύρος ζώνης στο mmWave επιτρέπει σε πολλούς χρήστες να έχουν ταυτόχρονη πρόσβαση σε εφαρμογές υψηλού εύρους ζώνης χωρίς να αντιμετωπίζουν πρόβλημα.

Επικοινωνία μικρής εμβέλειας: Ένας περιορισμός της τεχνολογίας mmWave είναι το περιορισμένο εύρος της. Τα σήματα υψηλότερης συχνότητας εξασθενούν ευκολότερα και είναι ευάλωτα στις παρεμβολές όπως κτίρια, δέντρα, ακόμη και στις καιρικές συνθήκες. Ως αποτέλεσμα, τα σήματα mmWave έχουν συνήθως μικρότερο εύρος σε σύγκριση με τα σήματα χαμηλότερης συχνότητας.

Τα παραδοσιακά συστήματα ασύρματης επικοινωνίας λειτουργούν κυρίως σε ζώνες χαμηλότερων συχνοτήτων, όπως η περιοχή κάτω των 6 GHz. Ωστόσο, η τεχνολογία mmWave αξιοποιεί το άφθονο φάσμα που διατίθεται στις ζώνες υψηλότερων συχνοτήτων για να προσφέρει βελτιωμένη χωρητικότητα και ταχύτερους ρυθμούς μετάδοσης δεδομένων. Το μικρό όμως μήκος κύματος κάνει επίσης την τεχνολογία mmWave

ευάλωτη στα εμπόδια που παρεμβάλλονται. Προκειμένου να αντιμετωπιστεί αυτό το ζήτημα η χρήση αναμεταδοτών (ρελέ) είναι εξαιρετικά συνήθης.

Τα τελευταία χρόνια, με την ανάπτυξη και βελτίωση των δυνατοτήτων των ΣμηΕΑ, συνδυαστικά με το χαμηλό τους κόστος και την ευκολία ανάπτυξής του στο πεδίο, έχουν τραβήξει το ενδιαφέρον τόσο της ακαδημαϊκής όσο και την επιχειρηματικής κοινότητας που δραστηριοποιούνται στις mmWave επικοινωνίες για την δυνατότητα χρήσης τους ως αναμεταδοτών (ρελέ). Είναι όμως δύσκολο για ένα ΣμηΕΑ (ή για ένα αυτοκινούμενο όχημα) να εντοπίσει αυτόματα τη βέλτιστη θέση του ως αναμεταδότης. Από τη μία, είναι δύσκολο να βρεθεί η τοποθεσία με ακρίβεια λόγω του πολύπλοκου και δυναμικού ασύρματου περιβάλλοντος αλλά από την άλλη, οι περισσότερες εφαρμογές που βασίζονται σε mmWave απαιτούν την ύπαρξη αναμεταδότη για την άμεση προώθηση των δεδομένων, οπότε η αυτόνομη διαδικασία εύρεσης της βέλτιστης θέσης του πρέπει να είναι ταχεία.

Για την επίλυση του ανωτέρω προβλήματος, έχει αναπτυχθεί η μέθοδος AutoRealy (αυτόματος αναμεταδότης) η οποία έχει δύο βασικά πλεονεκτήματα:

- Μπορεί να εκτιμήσει με ακρίβεια τη βέλτιστη θέση συνδυάζοντας το μοντέλο mmWave, τη δειγματοληψία σε πραγματικό χρόνο και τη θεωρία συμπιεστικής ανίχνευσης (compressive sensing theory).
- Ο αναμεταδότης μπορεί να φτάσει γρήγορα στην βέλτιστη θέση αναμετάδοσης χρησιμοποιώντας online update και τον μηχανισμό συνεχούς προσέγγισης.

Ένα βασικό πειραματικό σύστημα περιλαμβάνει έναν πομπό (Tx) και έναν δέκτη (Rx). Ο πομπός μεταδίδει σήμα στον δέκτη, αλλά λόγω του μικρότερου μήκους κύματος του mmWave, αυτό μπορεί εύκολα να διακοπεί από παρεμβαλόμενα εμπόδια.

Δημιουργείται ένα τρισδιάστατος χώρος 3D λαμβάνοντας τον πομπό mmWave ως αρχή o με συντεταγμένες $(0, 0, 0)$ και τον δέκτη mmWave ως το σημείο c με συντεταγμένες (n_1, n_2, n_3) . Η βέλτιστη θέση του αναμεταδότη είναι κάπου μέσα σε αυτόν τον χώρο.

Δημιουργείται ένας τρισδιάστατος πίνακας Q ο οποίος αναπαριστά τις ιδιότητες σύνδεσης όπου (n_1, n_2, n_3) είναι οι κλίμακες των τριών διαστάσεων. Ο χώρος χωρίζεται σε (n_1, n_2, n_3) μικρούς κύβους και η ποιότητα σύνδεσης σε κάθε συγκεκριμένο κύβο θεωρείται ότι είναι ίδια. Η τιμή κάθε κύβου $Q(i, j, k)$ του πίνακα υποδηλώνει την ποιότητα σύνδεσης της μετάδοσης σήματος mmWave εάν ο αναμεταδότης έχει οριστεί στο (i, j, k) .

Προκειμένου να μετρηθεί η ποιότητα σύνδεσης για κάθε θέση, παρέχεται ένα μοντέλο για τη μετάδοση σήματος mmWave λαμβάνοντας υπόψη τα πιθανά λάθη πορείας του ΣμηΕΑ και την απώλεια σήματος.

Τόσο η πλευρά του πομπού όσο και του δέκτη πρέπει να λαμβάνονται υπόψη για την αξιολόγηση της ποιότητας ζεύξης. Η προφανής μέθοδος για την περιγραφή της ποιότητας σύνδεσης είναι η λαμβανόμενη ποιότητα μετάδοσης σε κάθε ορισμένο σημείο. Η ποιότητα μετάδοσης σήματος στο σημείο προορισμού που λαμβάνεται από το σημείο αναμετάδοσης είναι ισοδύναμη με εκείνη στο σημείο αναμετάδοσης που λαμβάνεται από το σημείο προορισμού. Έτσι, θεωρούμε τις ιδιότητες λήψης στο σημείο αναμετάδοσης τόσο από το σημείο προέλευσης όσο και από το σημείο προορισμού ως παράγοντες στην αναπαράσταση των μετρήσεων της ποιότητας σύνδεσης.

Έστω S_o είναι η ποιότητα αποστολής σήματος στην αρχή o , S_c είναι η ποιότητα αποστολής στον παραλήπτη c , $R_o(i, j, k)$ είναι η ποιότητα λήψης από το σημείο o στο σημείο (i, j, k) και $R_c(i, j, k)$ είναι η ποιότητα λήψης από το σημείο c στο σημείο (i, j, k) .

Η ποιότητα σύνδεσης $Q(i, j, k)$ περιγράφεται ως το γινόμενο των ιδιοτήτων λήψης $R_o(i, j, k)$ στο σημείο (i, j, k) από το σημείο προέλευσης o και $R_c(i, j, k)$ στο σημείο (i, j, k) από τον δέκτη c , σύμφωνα με το μοντέλο μετάδοσης δεδομένων. Το γινόμενο αυτών των δύο τιμών λαμβάνεται ως το μέτρο σύγκρισης για την επίτευξη της βέλτιστης ποιότητας μετάδοσης για τον αναμεταδότη.

Ο αναμεταδότης ΣμηΕΑ στοχεύει στην εύρεση της βέλτιστης τοποθεσίας στην οποία θα επιτύχει την καλύτερη ποιότητα σύνδεσης ανάμεσα στον πομπό και τον δέκτη. Αναπτύσσεται μια στρατηγική επιλογής ιδανικής διαδρομής για τον αναμεταδότη και μια μέθοδος για την ενημέρωση του πίνακα ποιότητας Q σε πραγματικό χρόνο. Το ΣμηΕΑ-αναμεταδότης χρησιμοποιεί το μοντέλο μετάδοσης δεδομένων και πετάει κατά μήκος της διαδρομής σύμφωνα με την αρχικοποίηση του πίνακα ποιότητας Q .

Το χωρικό μοντέλο βασίζεται στον πομπό $o(0, 0, 0)$ και στον δέκτη $c(n_1, n_2, n_3)$.

Για να εντοπίσει το ΣμηΕΑ-αναμεταδότης το βέλτιστο σημείο $P(P_x, P_y, P_z)$ έτσι ώστε η ποιότητα σύνδεσης $Q(Q_x, Q_y, Q_z)$ να μεγιστοποιηθεί, δεδομένου του σημείου εκκίνησης του $S(S_x, S_y, S_z)$ και του αρχικού πίνακα ποιότητας Q , σχεδιάζεται η αντίστοιχη στρατηγική: Επειδή ο θόρυβος στο σήμα, η δυναμική του χώρου και άλλοι παράγοντες δεν μπορούν να μοντελοποιηθούν τέλεια, η ποιότητα σύνδεσης που υπολογίζεται από το θεωρητικό μοντέλο περιέχει σφάλματα. Ως εκ τούτου, η μέτρηση σε πραγματικό χρόνο και η ενημέρωση του πίνακα είναι απαραίτητες για τη διόρθωση των θεωρητικών αποτελεσμάτων. Ωστόσο, η μέτρηση της ποιότητας σύνδεσης σε όλες τις τοποθεσίες του υποψήφιου χώρου κοστίζει πολύ σε χρόνο. Συνεπώς το μοντέλο AutoRelay λαμβάνει δείγματα μόνο σε λίγα σημεία και εκτιμά την ποιότητα του σήματος στα υπόλοιπα σημεία χρησιμοποιώντας συμπίεστική ανίχνευση (comprehensive sensing). [24] [25]

7. Επιχειρησιακή εφαρμογή

Στο επίπεδο των εφαρμογών του IoD, η αναφορά γίνεται στην επιχειρησιακή χρήση των ΣμηΕΑ για την οποία όλα τα προηγούμενα επίπεδα συνδυάζονται ώστε να παραχθεί το ζητούμενο αποτέλεσμα, να συλλεχθούν τα απαιτούμενα δεδομένα και να εξαχθούν τα ζητούμενα συμπεράσματα.

Η πιο διαδεδομένη εφαρμογή των ΣμηΕΑ είναι η λήψη εικόνων και βίντεο. Αυτή εκτείνεται από την απλή ερασιτεχνική λήψη έως την απολύτως επαγγελματική ή ακόμα και για εφαρμογές ασφαλείας. Η επόπτευση συγκεντρώσεων, η παρακολούθηση συνόρων, η αναγνώριση προσώπων και η μεταφορά αυτών των δεδομένων σε πραγματικό χρόνο στους σταθμούς βάσης προς ανάλυση είναι μία επιχειρησιακή εφαρμογή των ΣμηΕΑ και του Internet of Things η οποία είναι γνωστή και εύκολα αναγνωρίσιμη τόσο από την επιστημονική κοινότητα όσο και από το κοινό.

Ακόλουθούν ορισμένοι μόνο από τους τομείς επιχειρησιακής χρήσης των ΣμηΕΑ:

7.1 Συλλογή και αποστολή δεδομένων

Τα ΣμηΕΑ με τους πολλαπλούς αισθητήρες που έχουν ενσωματωμένους ή αυτούς που μπορούν να προστεθούν στο σώμα του σκάφους, έχουν τη δυνατότητα της συλλογής τεράστιου όγκου δεδομένων από το περιβάλλον τους και την αποστολή αυτών στους αντίστοιχους σταθμούς βάσης.

Ορισμένα μόνο από τα δεδομένα τα οποία μπορούν να συλλέξουν είναι: θερμοκρασία, υγρασία, παρουσία συγκεκριμένου τύπου αερίων, ταχύτητα ανέμου, ποσότητα βροχής κ.ά

Η ανάπτυξη σμηνών ΣμηΕΑ για τη συλλογή δεδομένων παρέχει το πλεονέκτημα της κάλυψης μεγάλων γεωγραφικών περιοχών και της ταχείας εξαγωγής συμπερασμάτων.

Συλλογή εικόνων και βίντεο

Εκτός από τις γνωστές σε όλους μας χρήσεις των ΣμηΕΑ για βιντεοσκόπηση για ερασιτεχνικούς ή επαγγελματικούς λόγους οι εικόνες και τα βίντεο χρησιμοποιούνται και για αμιγώς επιχειρησιακούς σκοπούς υψηλών απαιτήσεων.

Για παράδειγμα, στην περίπτωση φυσικών καταστροφών τα υψηλής ποιότητας βίντεο μπορούν να παρέχουν στις ομάδες αρωγής την απαραίτητη πληροφόρηση για το σημείο της καταστροφής, την έκτασή της, εγκλωβισμένα άτομα και δρόμους διαφυγής.

Επιπλέον, με τη χρήση τεχνικών μηχανικής μάθησης αναπτύσσονται υπηρεσίες οι οποίες χρησιμοποιούν τα δεδομένα που λαμβάνουν τα ΣμηΕΑ προς βοήθεια των πληττόμενων. Χαρακτηριστικό παράδειγμα είναι οι περιπτώσεις των δασικών πυρκαγιών όπου με τη συνδυασμένη χρήση των λήψεων από ΣμηΕΑ και των δεδομένων από αισθητήρες εδάφους, εκτός από την έγκαιρη αντιμετώπιση της πυρκαγιάς μπορούν να εντοπιστούν δρόμοι διαφυγής των πολιτών που βρίσκονται στο σημείο καθώς και να υπολογιστούν οι διαδρομές τις οποίες πρέπει να ακολουθήσουν οι ομάδες πυρόσβεσης ώστε να προσεγγίσουν με ασφάλεια και ταχύτητα το σημείο της πυρκαγιάς.

Σε αυτή την περίπτωση τα ΣμηΕΑ δεν λειτουργούν μόνο ως συλλέκτες των δεδομένων αλλά και ως πομποί εκπομπής των απαραίτητων πληροφοριών προς τις ομάδες πυρόσβεσης.

7.2 Ανανεώσιμες πηγές ενέργειας

Η ταχεία ανάπτυξη των ανανεώσιμων πηγών ενέργειας, της αιολικής και της ηλιακής, έκανε ορατή την αναγκαιότητα χρήσης των ΣμηΕΑ τόσο κατά την κατασκευή όσο και κατά τη συντήρηση των εγκαταστάσεων φωτοβολταϊκών και αιολικών πάρκων.

Η δυνατότητα των ΣμηΕΑ να φέρουν θερμικές κάμερες υψηλής ανάλυσης παρέχει λύσεις εντοπισμού των φθορών στα φωτοβολταϊκά πάνελ και τις ανεμογεννήτριες με τη χρήση εξειδικευμένου λογισμικού μηχανικής μάθησης. Αυτό έχει ως αποτέλεσμα την επέκταση της ζωής χρήσης των εγκαταστάσεων και τη μη κατασπατάληση φυσικών και οικονομικών πόρων. Συνεπώς τα ΣμηΕΑ σε αυτή την περίπτωση συνεισφέρουν στο sustainability και στην μείωση του οικολογικού αποτυπώματος των εγκαταστάσεων ΑΠΕ.

7.3 Ιχθυοκαλλιέργειες

Ίσως να φαίνεται περίεργο αλλά η χρήση των ΣμηΕΑ στις ιχθυοκαλλιέργειες είναι πλέον εκτεταμένη. Ιπτάμενα ΣμηΕΑ επιτηρούν τις εγκαταστάσεις ενώ εξειδικευμένα ΣμηΕΑ εκτελούν την υπηρεσία τσίψματος των ψαριών από αέρος ελαχιστοποιώντας το χρόνο που απαιτείται για αυτή την λειτουργία.

Θαλάσσια drones επιτηρούν την εγκατάσταση κάτω από την επιφάνεια της θάλασσας για πιθανές φθορές ενώ χρησιμοποιούνται και για τις μετρήσεις ποιότητας των υδάτων κάπως και για την επόπτευση της υγείας των ψαριών.

7.4 Αναδασώσεις

Είναι γνωστό ότι μετά από μία δασική πυρκαγιά πρέπει, προκειμένου να αποκατασταθεί το φυσικό περιβάλλον, να πραγματοποιηθεί αναδάσωση

Μέχρι σήμερα οι αναδασώσεις γίνονται με τον παραδοσιακό τρόπο όπου ομάδες ανθρώπων τοποθετούν τους σπόρους στο έδαφος ώστε αυτοί να αναπτυχθούν και να φυτρώσει νέο δάσος.

Η διαδικασία αυτή είναι χρονοβόρα και συχνά προκαλείται επιπλέον φθορά στο έδαφος από τα χιλιάδες ή και εκατομμύρια πατήματα πελμάτων που μπορεί να απαιτηθούν προκειμένου να πραγματοποιηθεί αναδάσωση.

Πλέον, με τη χρήση ειδικών ΣμηΕΑ τα οποία φέρουν, εκτός από δοχείο αποθήκευσης σπόρων, ειδικό σύστημα εκτόξευσής τους με μεγάλη ταχύτητα προς το έδαφος, η αναδάσωση γίνεται ταχύτερα, με μεγάλη ακρίβεια αναφορικά με την πυκνότητα ανά τετραγωνικό χιλιόμετρο των σπόρων και χωρίς να προκληθεί καμία επιπλέον φθορά στο έδαφος.

7.5 Τηλεπικοινωνίες

Η ταχεία ανάπτυξη, το χαμηλό κόστος και ο πολλαπλών τύπων τηλεπικοινωνιακός εξοπλισμός τον οποίο μπορούν να φέρουν τα ΣμηΕΑ δίνουν τη δυνατότητα προσωρινής αποκατάστασης τηλεπικοινωνιακών υπηρεσιών σε σημεία όπου είτε δεν υπάρχουν επίγειες εγκαταστάσεις είτε αυτές έχουν καταστραφεί από φυσικά αίτια ή από ανθρώπινη δραστηριότητα.

7.6 Αγροτική παραγωγή

Στη γεωργία, τα ΣμηΕΑ, εξοπλισμένα με κάμερες προηγμένης τεχνολογίας και αισθητήρες μπορούν να παρέχουν δεδομένα σε πραγματικό χρόνο βοηθώντας τους αγρότες ακριβείς

πληροφορίες για την υγρασία του εδάφους, την εξάτμιση, την υφή του εδάφους, τη γονιμότητα και παραγωγικότητα της καλλιέργειας, τις μολύνσεις κ.λπ

Εκτός όμως από proactive πληροφόρηση, τα ΣμηΕΑ μπορούν να εκτελέσουν και ενεργητικές αποστολές στις καλλιέργειες, με τον αεροψεκασμό ακριβείας.

Το ψεκαστικό ΣμηΕΑ πλοηγείται είτε χειροκίνητα είτε αυτόματα μέσω των συντεταγμένων GPS και ψεκάζει με ακρίβεια, με ασφάλεια για τον χειριστή και με πολύ μεγαλύτερη ταχύτητα από τις παραδοσιακές μεθόδους.

7.7 Στρατιωτικές εφαρμογές

Η στρατιωτική χρήση των ΣμηΕΑ έχει αναδειχθεί ως η κορυφαία, από πλευράς τεχνολογικής εξέλιξης και σημασίας, εφαρμογή του IoD. Τα ΣμηΕΑ είναι πλέον αναπόσπαστο μέρος όλων των σύγχρονων στρατών και χρησιμοποιούνται όπου η επανδρωμένες πτήσεις είναι επικίνδυνες, δύσκολες ή εξαιρετικά κοστοβόρες.

Τα στρατιωτικά ΣμηΕΑ συνδράμουν σε συνθήκες μάχης παρακολουθώντας τις κινήσεις του εχθρού, συνδράμουν στην επιλογή στόχων, βελτίωσης των στρατιωτικών επικοινωνιών αλλά και εκτοξεύοντας πυραυλικό ή άλλο υλικό προς τις εχθρικές θέσεις.

Οι Kreps και Wallace [26] διερεύνησαν τη χρήση μη επανδρωμένων αεροσκαφών στην αντιμετώπιση της αντιτρομοκρατίας. Η εργασία τους απαντά στο ερώτημα σχετικά με το εάν η νομική κριτική σε διεθνές επίπεδο επηρεάζει τόσο τη δημόσια υποστήριξη για επιθέσεις με μη επανδρωμένα αεροσκάφη όσο και το επίκεντρο των αντιτρομοκρατικών πολιτικών των ΗΠΑ. Οι συγγραφείς εξέτασαν επίσης εάν τα άτομα πείθονται πειστικά από επιχειρήματα που βασίζονται στην αποτελεσματικότητα των drones.

Ο Chand et al. [27] ανέπτυξε ένα ασύρματο δίκτυο mesh υψηλής ταχύτητας βασισμένο σε ΣμηΕΑ, για περιοχές χωρίς υποδομή επικοινωνιών, όπως ακριβώς περιγράφουν σενάρια φυσικών καταστροφών ή στρατιωτικών επιχειρήσεων.

Η μελέτη δείχνει ότι κατά την άφιξή του στην περιοχή προορισμού, το ΣμηΕΑ μπορεί να χρησιμοποιήσει το ασύρματο δίκτυο mesh για να παρέχει Wi-Fi και ταυτόχρονα να εποπτεύει την περιοχή με την κάμερά του.

Το μεταδιδόμενο βίντεο μπορεί να προβληθεί στο κέντρο ελέγχου ή σε κινητά τηλέφωνα επιτελικών που βρίσκονται στο πεδίο σε πραγματικό χρόνο. Το προτεινόμενο δίκτυο προσφέρει ασύρματη επικοινωνία έως 160 Mbps σε εμβέλεια περίπου 200 μέτρων.

7.8 Έρευνα και διάσωση

Με την επιδείνωση της κλιματικής κρίσης, οι φυσικές καταστροφές γίνονται όλο και συχνότερες με αποτέλεσμα οι επιχειρήσεις έρευνας και η διάσωσης ατόμων ευρισκόμενων σε κίνδυνο να διαδραματίζουν έναν όλο και αυξανόμενης σημασίας ρόλο.

Η διαθεσιμότητα και η τεχνολογική επάρκεια πληθώρας αισθητήρων (θερμικών, κίνησης κ.λπ) και καμερών καθιστά τα ΣμηΕΑ ένα εργαλείο πολλαπλασιαστή αποτελεσματικότητας στις αποστολές έρευνας και διάσωσης.

Τα ΣμηΕΑ μπορούν να εντοπίσουν τη θέση αγνοουμένων και τραυματιών σε σημεία όπου η μορφολογία του εδάφους δεν διευκολύνει τις επίγειες ομάδες αναζήτησης και να παραδώσουν φάρμακα και προμήθειες εκτάκτου ανάγκης γρήγορα και με ακρίβεια.

Ο ερευνητής Tilburg [28] ανέφερε δύο μελέτες περιπτώσεων για να αποδείξει τις επιχειρησιακές δυνατότητες των ΣμηΕΑ σε αποστολές έρευνας και διάσωσης. Στην περίπτωση 1, μια ομάδα διάσωσης ανακάλυψε έναν νεκρό μέσω της κάμερας του ΣμηΕΑ και στη συνέχεια έστειλε τις συντεταγμένες του σημείου ανεύρεσης οι οποίες βρίσκονταν

μέσα σε μία κοιλάδα. Στην περίπτωση 2, το ΣμηΕΑ επέκτεινε την περιοχή έρευνας πραγματοποιώντας φωτογραφικές λήψεις ιδιαίτερα δυσπρόσιτων περιοχών βοηθώντας στην αποστολή έρευνας και διάσωσης.

7.9 Ψυχαγωγία

Μεγάλη είναι η ζήτηση για ΣμηΕΑ τα οποία χρησιμοποιούνται στον κλάδο της διασκέδασης.

Οι Quiroz και Kim [29] παρήγαγαν ένα αρχικό σχέδιο ενός ΣμηΕΑ ψυχαγωγίας - ένα ΣμηΕΑ το οποίο σκορπά κονφετί. Η ιδέα τους υλοποιήθηκε με τη χρήση ενός μικροελεγκτή και ένα βάζο τυπωμένου σε 3D. Το βάζο χρησιμοποιήθηκε για να δοκιμαστεί η δυνατότητα χρήσης ΣμηΕΑ για τη εκτόξευση στον αέρα κονφετί. Οι Kim, Yeong και Park [30] διερεύνησαν τη χρήση των ΣμηΕΑ τόσο στον τομέα της ψυχαγωγίας όσο και της επαυξημένης και εικονικής πραγματικότητας (AVR), μετά την διαπίστωση της συνεχώς αυξανόμενης χρήσης τους στην επιστήμη και στην επιχειρηματικότητα.

7.10 Υπηρεσίες υγείας

Στον τομέα της υγείας, τα ΣμηΕΑ μπορούν να χρησιμοποιηθούν για τη μεταφορά φαρμάκων, εμβολίων, δειγμάτων αίματος αλλά και προμηθειών πρώτης ανάγκης σε περιοχές όπου έχουν συμβεί φυσικές και άλλες καταστροφές αλλά και σε περιοχές όπου το οδικό ή άλλο επικοινωνιακό δίκτυο δεν είναι κατάλληλο.

Οι J. Scott και C. Scott [31] εξέτασαν τη δυνατότητα παράδοσης με ΣμηΕΑ υγειονομικού υλικού. Οι συγγραφείς μελέτησαν τα πλέον πρόσφατα μοντέλα αποφάσεων διαχείρισης στόλου ΣμηΕΑ αποκλειστικά για τέτοιες παραδόσεις.

7.11 Έλεγχος κυκλοφορίας

Οι Μπαρμπουνάκης και Γερολιμίνης [32] δημιούργησαν ένα ολοκληρωμένο σύνολο αστικών δεδομένων για να εξετάσουν την κυκλοφοριακή συμφόρηση στο κέντρο της Αθήνας. Αυτό το σύνολο δεδομένων περιλάμβανε αρχεία ροής κυκλοφορίας, τα οποία συγκεντρώνονταν από έναν στόλο 10 ΣμηΕΑ, για αρκετές μέρες.

Η δημιουργία αυτού του συνόλου δεδομένων είναι χρήσιμη για άλλους ερευνητές οι οποίοι επιθυμούν να μελετήσουν σε βάθος τα βασικά κυκλοφοριακά φαινόμενα της πόλης, να αναπτύξουν μοντέλα αντιμετώπισης του φαινομένου της κυκλοφοριακής συμφόρησης και να τα δοκιμάσουν με πραγματικά στοιχεία.

Σε άλλη έρευνα [33], επίσης για την Αθήνα, σχεδιάστηκαν διαδρομές τις οποίες παρακολουθούσε ένας στόλος ΣμηΕΑ για ταχεία επιτήρηση της κυκλοφοριακής κίνησης σε συγκεκριμένες περιοχές. Οι συγγραφείς, Χριστοδούλου και Κολιό, πρώτα σχεδίασαν τα σημεία επάνω από τα οποία πέταξαν τα ΣμηΕΑ και στη συνέχεια βέλτιστες διαδρομές υπολογίζοντας τον ελάχιστο απαιτούμενο χρόνο για τα οχήματα στο έδαφος, υπολογίζοντας πάντα και την ενεργειακή επάρκεια των ΣμηΕΑ.

Η μέθοδος που πρότειναν δοκιμάστηκε σε πραγματικές συνθήκες, αποδείχθηκε η αξιοπιστία της καθώς και τα πλεονεκτήματα των ΣμηΕΑ όπως η ευελιξία ανάπτυξης και κίνησης, η ποσότητα των δεδομένων που συγκεντρώνονται σε πραγματικό χρόνο αλλά και η σχέση κόστους-απόδοσης.

Είναι βέβαιο ότι με την βελτίωση των δυνατοτήτων των ΣμηΕΑ, τόσο στη διάρκεια πτήσης όσο και στον εξοπλισμό τον οποίο μπορούν να φέρουν, οι εφαρμογές οι οποίες θα αναπτυχθούν βασιζόμενες σε αυτά και στα πρωτόκολλα επικοινωνίας, τόσο μεταξύ τους όσο και με τους σταθμούς βάσης, θα αυξηθούν ραγδαία τα επόμενα χρόνια.

8. Εφαρμογή πεδίου: Επόπτευση Φ/Β πάρκων και εντοπισμός σφαλμάτων

Όπως αναφέρθηκε και στο 7.2, μία από τις πιο άμεσες και πρακτικές εφαρμογές της χρήσης των ΣμηΕΑ (σε συνδυασμό με εξελιγμένο λογισμικό), είναι η επόπτευση φωτοβολταϊκών πάρκων και ο εντοπισμός φθορών στα panel. Προκειμένου να γίνει πλήρως αντιληπτή η ποιότητα αυτής της εφαρμογής, είναι χρήσιμο να εξετάσουμε τη διαδικασία υλοποίησης από τον αρχικό σχεδιασμό μέχρι την τελική εξαγωγή των αποτελεσμάτων του ελέγχου.

Σε αυτό το κεφάλαιο της εργασίας, θα παρουσιαστεί μία πραγματική επόπτευση Φ/Β πάρκου με drone, οι τεχνικές προδιαγραφές αλλά και ένα δείγμα report αναφοράς βλαβών.

8.1 Εξοπλισμός

Για την πραγματοποίηση της επόπτευσης, ο εξοπλισμός που χρησιμοποιήθηκε περιλαμβάνει:

- α. ΣμηΕΑ εξοπλισμένο με θερμική κάμερα ανάλυσης 640x512 pixels και αποστασιόμετρο με laser. Το ΣμηΕΑ τροφοδοτείται από δύο μπαταρίες ώστε να αποφευχθεί πιθανή απότομη απώλεια ενέργειας από τη μία. Στην εφαρμογή που θα περιγράψουμε χρησιμοποιήθηκε το DJI M30T.
- β. Μετρητής φωτός (lux)
- γ. 2 ζεύγη μπαταριών ΣμηΕΑ
- δ. Φορτιστής μπαταριών ΣμηΕΑ

8.2 Προσωπικό

Προκειμένου η πτήση να είναι ασφαλής και σύμφωνη με τους ελληνικούς και ευρωπαϊκούς κανονισμούς, στην πραγματοποίησή της έλαβαν μέρος δύο άτομα: Ένας πιλότος και ένας επόπτης.

Ο πιλότος ήταν υπεύθυνος για τον χειρισμό του αεροσκάφους καθώς και για τη λήψη των θερμικών εικόνων των Φ/Β πάνελ ενώ ο επόπτης (spotter) είναι υπεύθυνος για την συνεχή επόπτευση του χώρου για πιθανά εμπόδια ή την εμφάνιση ξαφνικών «κινδύνων» όπως πουλιών.

8.3 Κατεύθυνση λήψης

Για τη λήψη εικόνων IR (infrared – θερμική) και RGB (red-green-blue οπτική) η κατεύθυνση της κάμερας θα πρέπει να παραμένει σταθερή καθ'όλη τη διάρκεια της πτήσης.

Για παράδειγμα, αν η πτήση πραγματοποιείται σε Φ/Β πάρκο του οποίου τα πάνελ είναι στραμμένα προς το νότο, η κάμερα θα πρέπει να «κοιτάει» προς βορρά.

Επειδή, ειδικά σε μεγάλα Φ/Β πάρκα, η κατεύθυνση των πανελ αλλάζει, σε κάθε αλλαγή κατεύθυνσης θα πρέπει να πραγματοποιείται νέο session πτήσης και τα δεδομένα να αποθηκεύονται σε διαφορετικό σετ για την μετέπειτα επεξεργασία τους.

8.4 Λήψη εικόνων

Κατά την λήψη των θερμικών και οπτικών εικόνων των πάνελ, προκειμένου να είμαστε απολύτως βέβαιοι ότι το σύνολό τους έχει απεικονιστεί σωστά, θα πρέπει να υπάρχει επικάλυψη λήψεων τόσο ανάμεσα στις σειρές των πάνελ όσο και μεταξύ διπλανών πάνελ. Επιπλέον, η γωνία λήψης σε σχέση με το panel θα πρέπει να είναι τέτοια ώστε να υπάρχουν οι ελάχιστες δυνατές αντανakλάσεις από τον ήλιο.

Εμπρόσθια επικάλυψη εικόνων: 50%

Πλάγια επικάλυψη εικόνων: 20%

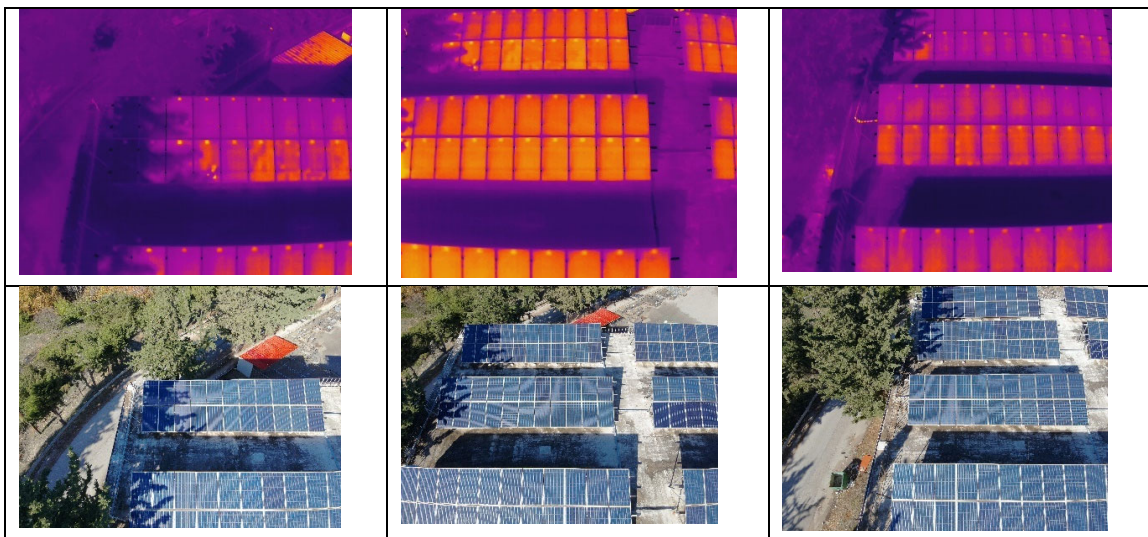
Τύπος αρχείου: RJPG (radiometric JPG)*

Μέγεθος θερμικής εικόνας (ελάχιστο): 640x512 pixels

Μέγεθος οπτικής εικόνας (ελάχιστο): 4000x3000 pixels



Πίνακας 1: Πλάγια επικάλυψη εικόνων



Πίνακας 2: Οριζόντια επικάλυψη εικόνων

*Μια εικόνα RJPG (radiometric JPG) είναι μια εικόνα τύπου .jpg η οποία στα μεταδεδομένα της (image metadata) έχει ενσωματωμένα και ραδιομετρικά δεδομένα. Το RJPG είναι ο προτεινόμενος τύπος εικόνων για θερμογραφία υψηλών απαιτήσεων.

8.5 Ηλιοφάνεια

Προκειμένου να λάβουμε καλής ποιότητας εικόνας, θα πρέπει τα panel να βρίσκονται υπό ηλιοφάνεια και μάλιστα, όχι απλά να είναι φωτεινά αλλά ζεστά. Στην πράξη, απαιτείται η ηλιακή ακτινοβολία που δέχονται τα πανελ να είναι ίση ή μεγαλύτερη από 600 Watts ανά τετραγωνικό μέτρο.

Προκειμένου να είμαστε βέβαιοι ότι η ακτινοβολία την ημέρα και ώρα της λήψης είναι επαρκής, χρησιμοποιούμε έναν μετρητή φωτισμού.



8.6 Ανάλυση δεδομένων

Με την ολοκλήρωση της πτήσης (αυτόματης ή χειροκίνητης), το σύνολο των εικόνων πρέπει να υποστεί την διαδικασία επιλογής βέλτιστης λήψης. Αυτό σημαίνει ότι στη διαδικασία εντοπισμού των βλαβών ίσως να μην χρησιμοποιηθούν όλες οι θερμικές εικόνες αλλά μόνο αυτές οι οποίες θα περάσουν με επιτυχία τον ποιοτικό έλεγχο.

Τα κριτήρια επιλογής είναι: α. οι ελάχιστες αντανάκλασεις, β. οι ελάχιστες σκιάσεις και γ. η μέγιστη καθαρότητα της εικόνας.

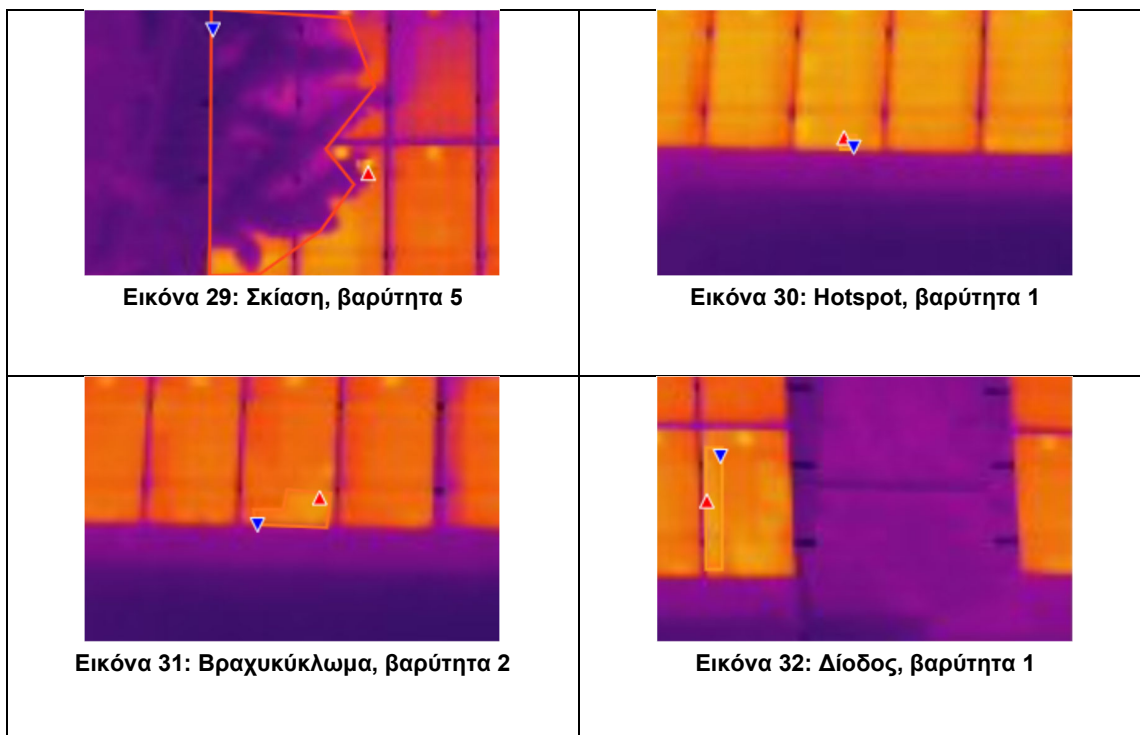
8.7 Βλάβες που εντοπίζονται

Οι βλάβες οι οποίες μπορούν να εντοπιστούν σε Φ/Β πάνελ με τη χρήση θερμικών εικόνων οι οποίες έχουν ληφθεί από ΣμηΕΑ είναι οι ακόλουθες:

- a. Κατεστραμμένες κυψέλες
- b. Ραγίσματα
- c. Υπολειπουσες κυψέλες
- d. Βραχυκυκλώματα
- e. Δίοδοι
- f. Προσωρινές σκιάσεις
- g. Κατασκευαστικές ατέλειες

Κάθε μία από τις παρακάτω βλάβες έχει, εκτός από τον ίδιο τον χαρακτηρισμό, και έναν συντελεστή βαρύτητας από (ελαφρά, μεσαία, βαριά, πλήρης βλάβη).

Παραδείγματα βλαβών:



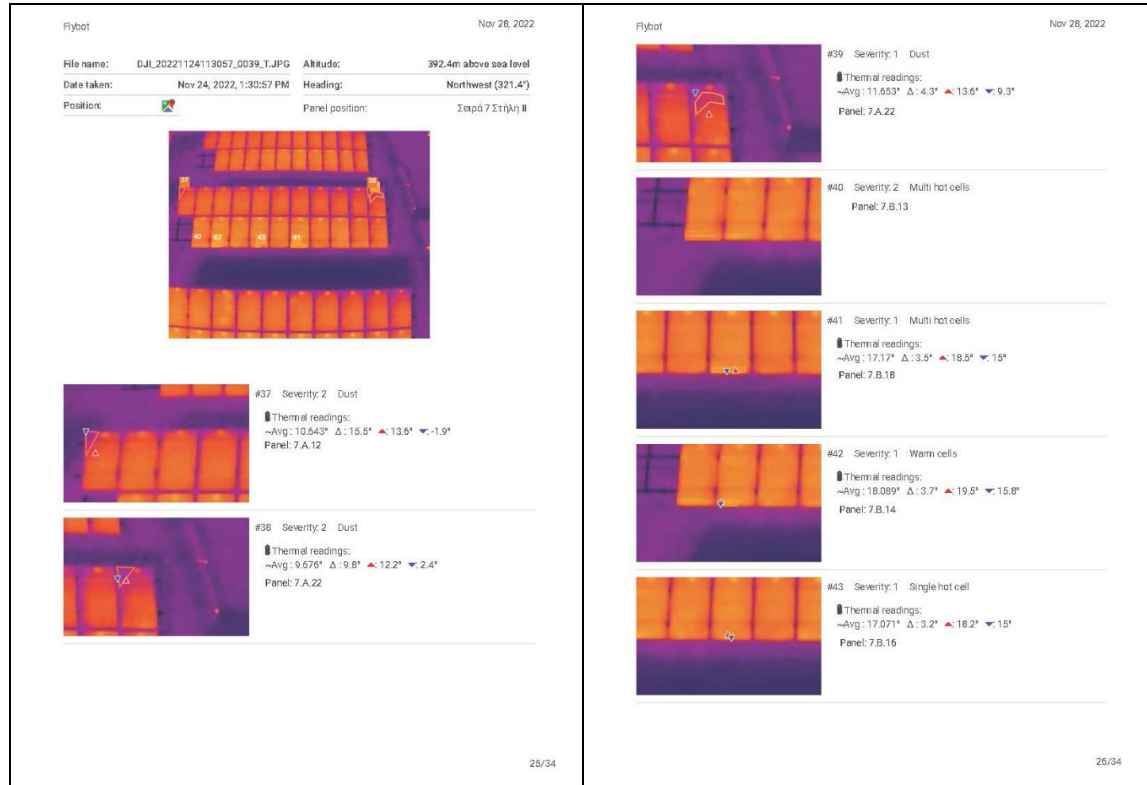
8.8 Λογισμικό

Επειδή τόσο ο εντοπισμός όσο και το reporting των βλαβών ενός μεγάλου πάρκου μπορεί να περιλαμβάνει εκατοντάδες χιλιάδες πάνελ και, αντιστοίχως, εκατοντάδες χιλιάδες φωτογραφίες, η διαδικασία δεν μπορεί να πραγματοποιηθεί χειροκίνητα.

Η εταιρεία Flybot, η οποία παραχώρησε στον γράφοντα τις θερμικές εικόνες Φ/Β πάνελ που παρουσιάζονται, έχει αναπτύξει λογισμικό βασισμένο στην μηχανική μάθηση το οποίο δέχεται τις εικόνες της πτήσης και δημιουργεί αυτόματα το report εντοπισμού των βλαβών.

8.9 Report βλαβών

Παράδειγμα report



Στο report απεικονίζονται, για κάθε φωτογραφία που λήφθηκε, τα παρακάτω στοιχεία:

- Όνομα αρχείου εικόνας,
- Ύψος πτήσης (από την επιφάνεια της θάλασσας)
- Ημερομηνία λήψης εικόνας
- Κατεύθυνση panel
- Γεωγραφική τοποθεσία
- Θέση εικόνας στο Φ/Β πάρκο*

Στη συνέχεια, για κάθε σφάλμα που εντοπίζεται στην εικόνα, το λογισμικό δημιουργεί ένα ξεχωριστό στιγμιότυπο (snapshot), στο οποίο, με τη σειρά του, απεικονίζεται:

- Είδος βλάβης
- Βαρύτητα βλάβης
- Θερμικά χαρακτηριστικά: (Μέση θερμοκρασία, Ανώτατη θερμοκρασία, χαμηλότερη θερμοκρασία, διαφορά μεταξύ ανώτατης/κατώτατης)
- Θέση του panel στο πάρκο

(*Για λόγους προστασίας επαγγελματικών δεδομένων, από το δείγμα του report έχει αφαιρεθεί η ακριβής τοποθεσία του φωτοβολταϊκού πάρκου).

Χάρτης Φ/Β πάρκου

	1	2	3	4	5	6	7	8	9	10	11				12	13	14	15	16	17	18	19	20	21	22	
1																										
A	1A.1	1A.2	1A.3	1A.4	1A.5	1A.6	1A.7	1A.8	1A.9	1A.10	1A.11				1A.12	1A.13	1A.14	1A.15	1A.16	1A.17	1A.18	1A.19	1A.20	1A.21	1A.22	
B	1B.1	1B.2	1B.3	1B.4	1B.5	1B.6	1B.7	1B.8	1B.9	1B.10	1B.11				1B.12	1B.13	1B.14	1B.15	1B.16	1B.17	1B.18	1B.19	1B.20	1B.21	1B.22	
2																										
A	2A.1	2A.2	2A.3	2A.4	2A.5	2A.6	2A.7	2A.8	2A.9	2A.10	2A.11				2A.12	2A.13	2A.14	2A.15	2A.16	2A.17	2A.18	2A.19	2A.20	2A.21	2A.22	
B	2B.1	2B.2	2B.3	2B.4	2B.5	2B.6	2B.7	2B.8	2B.9	2B.10	2B.11				2B.12	2B.13	2B.14	2B.15	2B.16	2B.17	2B.18	2B.19	2B.20	2B.21	2B.22	

Ο χάρτης του πάρκου δημιουργείται αυτόματα από το λογισμικό ώστε να συνδέονται τα εντοπιζόμενα στις εικόνες σφάλματα με το panel στο οποίο εντοπίστηκαν.

Κατάλογος εντοπισμένων σφαλμάτων

Στο report σφαλμάτων, μετά τον χάρτη του Φ/Β πάρκου, καταγράφονται αυτόματα από το λογισμικό κάθε μία από τις βλάβες, η βαρύτητά της, τα πιθανά σχόλια του ειδικού θερμογραφίας καθώς και η σελίδα του report στην οποία είναι καταγεγραμμένες οι λεπτομέρειες της βλάβης και η φωτογραφία που την εντοπίζει.

#	Severity	Issues	Comments	Page
1	1	Substring short-circuit	έλεγχος module και διόδου για σωστή λειτουργία υπό αντίστροφη πόλωση	6
2	1	Multiple hotspots		6
3	2	Multiple hotspots		7
4	1	Multi hot cells		8
5	1	Multi hot cells		8
6	5	Shading		9
7	5	Shading	Λόγω παρακείμενης σκίασης	9
8	2	Multi hot cells		10
9	1	Hotspot		10
10	2	Multi hot cells		11

9. Ασφάλεια και απόρρητο

Τα ΣμηΕΑ, ανάμεσα στους πολλαπλούς αισθητήρες με τους οποίους είναι συχνά εξοπλισμένα, έχουν συσκευές για τη συλλογή κάθε είδους πληροφοριών, όπως εικόνες, βίντεο αλλά και δεδομένα θέσης τα οποία συχνά είναι αντικείμενο προστασίας της ιδιωτικότητας. Ο τρόπος συλλογής αυτών των δεδομένων, η επεξεργασία τους, η χρήση τους μετά την επεξεργασία αλλά και το που και σε ποιον αυτά διαβιβάζονται, είναι ζητήματα που απασχολούν τόσο την επιστημονική κοινότητα όσο και την κοινωνία.

Τα ευαίσθητα προσωπικά δεδομένα ατόμων και εταιριών πρέπει να προστατεύονται από κάθε παράνομη χρήση, υποκλοπή ή κατάχρηση. Το IoD όμως, ως εκ της φύσης του αλλά και των πληροφοριών οι οποίες συλλέγονται και μεταφέρονται μέσω αυτού, αποτελεί συχνά στόχο επιθέσεων για υποκλοπή αυτών των δεδομένων.

Για παράδειγμα, αν ένα ΣμηΕΑ το οποίο συγκεντρώνει και διαβιβάζει κρίσιμα δεδομένα για την κρατική ασφάλεια ή την προστασία των συνόρων της χώρας, καταρριφθεί ή υποκλαπεί η χρήση του, το διακύβευμα είναι εξαιρετικά μεγάλο. Και αυτό δεν αφορά μόνο τα δεδομένα ή τα εξαρτήματα του σκάφους, τα οποία συχνά είναι εξαιρετικά μεγάλης αξίας αλλά το ίδιο το ΣμηΕΑ μπορεί να χρησιμοποιηθεί από τους αντιπάλους ως όπλο. Να υποστεί δηλαδή «πειρατεία».

Ας εξετάσουμε λοιπόν ορισμένες βασικές προδιαγραφές ασφαλείας του IoD αλλά και κάποια είδη κυβερνοεπιθέσεων τις οποίες μπορεί να δεχθεί.

9.1 Απαιτήσεις Ασφαλείας του IoD

Καθώς τα δεδομένα που διακινούνται μέσα από το IoD ενδέχεται να περιλαμβάνουν ευαίσθητες προσωπικές ή εθνικού ενδιαφέροντος πληροφορίες, κρίσιμης αξίας, η ασφάλεια του συνολικού συστήματος αποτελεί μείζον θέμα.

Τα ΣμηΕΑ λειτουργούν ως επί το πλείστον ασύρματα και από απόσταση ενώ ο έλεγχος πραγματοποιείται από επίγειους ή επιπλέοντες σταθμούς βάσης (σταθμοί βάσης μπορεί να είναι και πλοία).

Τα σήματα χειρισμού μεταδίδονται μέσω διαφορετικών πηγών με διαφορετικούς ρυθμούς μετάδοσης και τα ίδιο συμβαίνει και με τα δεδομένα που μεταδίδονται από τα ΣμηΕΑ προς τους σταθμούς βάσης. Στο IoD συνεπώς, δεδομένου ότι η ανταλλαγή πληροφοριών είναι κρίσιμη, κανένα σήμα χειρισμού και καμία μεταδιδόμενη πληροφορία δεν πρέπει να διαρρεύσει ή να τεθεί σε κίνδυνο σε καμία περίπτωση [34]. Ωστόσο, τα ΣμηΕΑ ενδέχεται να μην είναι σε θέση να ενσωματώσουν πολύπλοκες λειτουργίες ασφαλείας λόγω περιορισμένων ενεργειακών πόρων.

Η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα, η αυθεντικότητα και η διατήρηση της ιδιωτικής ζωής και των δεδομένων αυτής αποτελούν βασικές απαιτήσεις ασφαλείας και απορρήτου του IoD. Οι απαιτήσεις αυτές αντικατοπτρίζουν τις δυνατότητες και τις λειτουργίες του IoD για την αντιμετώπιση απειλών και παραβιάσεων της ασφαλείας [34].

Εμπιστευτικότητα: Η εμπιστευτικότητα των καναλιών ασύρματης επικοινωνίας αποτρέπει τη διαρροή πληροφοριών στο IoD.

Ακεραιότητα: Διασφαλίζει ότι οι πληροφορίες που περνούν μέσα από το IoD είναι άθικτες.
Διαθεσιμότητα: Οι σχετικές υπηρεσίες IoD θα πρέπει να είναι διαθέσιμες σε εξουσιοδοτημένους και μόνο χρήστες.

Αυθεντικότητα: Αφορά τον έλεγχο ταυτότητας των ΣμηΕΑ, των χρηστών και των gateways πριν από την εξουσιοδότηση πρόσβασης ή την αποκάλυψη κρίσιμων πληροφοριών.

Απόρρητο: Η προστασία της ιδιωτικής ζωής είναι επιτακτική ανάγκη για το IoD. Τα δεδομένα γεωεντοπισμού ή ταυτοποίησης που συλλέγονται από τα ΣμηΕΑ μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ συγκεκριμένων ατόμων και η διαρροή αυτών των δεδομένων εγείρει σοβαρές ανησυχίες.

9.2 Κυβερνοεπιθέσεις στο IoD

Η ασφάλεια του IoD δεν είναι καθόλου εύκολη υπόθεση λόγω των διαφορετικών προτύπων επικοινωνίας μεταξύ ΣμηΕΑ, σταθμών βάσεων και άλλων συσκευών και αισθητήρων, καθώς και του εύρους των εφαρμογών στις οποίες τα ΣμηΕΑ χρησιμοποιούνται. Λόγω των ανωτέρω δεδομένων, τα ΣμηΕΑ αποτελούν στόχο πολλαπλών τύπων επιθέσεων, ορισμένες από τις οποίες αναφέρονται στη συνέχεια [35].

9.2.1 Επιθέσεις παρεμβολής σήματος (Jamming)

Στις επιθέσεις παρεμβολής σήματος, ο επιτιθέμενος παρεμβαίνει στα ραδιοσήματα επικοινωνίας του ΣμηΕΑ προκαλώντας προβλήματα στη συνδεσιμότητα του IoD και αυξάνοντας ταυτόχρονα την κατανάλωση ενέργειας των ΣμηΕΑ. Το αποτέλεσμα μίας επιτυχημένης τέτοιας επίθεσης είναι είτε η συντριβή του σκάφους είτε η διακοπή των παρεχομένων από το IoD υπηρεσιών.

9.2.2 Επιθέσεις αλλοίωσης δεδομένων

Στις επιθέσεις αλλοίωσης δεδομένων ο επιτιθέμενος καταστρέφει, παραποιεί ή επεξεργάζεται δολίως δεδομένα μέσω μη εξουσιοδοτημένων καναλιών IoD. Τα δεδομένα, όταν μεταφέρονται μεταξύ συσκευών IoD ή καθώς βρίσκονται αποθηκευμένα σε μία συσκευή του IoD ενδέχεται να υποκλαπούν, να αλλοιωθούν και στη συνέχεια να προωθηθούν αλλοιωμένα σε άλλες συσκευές του IoD. Για παράδειγμα, εάν ένα πακέτο δεδομένων μεταφέρεται μέσω ενός καναλιού IoD το οποίο δεν έχει την ενδεδειγμένη προστασία, θα μπορούσε να υποκλαπεί, να τροποποιηθεί αλλά και να αλλάξει η διεύθυνση προορισμού του.

9.2.3 Συγκρούσεις

Όταν δύο ή περισσότερα ΣμηΕΑ λειτουργούν στην ίδια συχνότητα, αυτό μπορεί να προκαλέσει αστάθεια στη λειτουργία του δικτύου, με πιθανό αποτέλεσμα τη σύγκρουση ή την πτώση του σκάφους. Η κακή ποιότητα της επικοινωνίας και οι περιορισμένοι υπολογιστικοί πόροι του IoD είναι οι πλέον συνήθεις αιτίες εμφάνισης αυτού του προβλήματος.

9.2.4 Επιθέσεις επιλεκτικής προώθησης δεδομένων

Στις επιθέσεις επιλεκτικής προώθησης, ένα κακόβουλο ΣμηΕΑ έχει «εισβάλλει» στο IoD ή έχει καταληφθεί από τον εισβολέα και ενώ λειτουργεί ως κανονικός κόμβος του IoD, μπορεί είτε να υποκλέψει είτε να «διαγράψει» και απορρίψει από την ροή μεταφοράς σημαντικά ή ευαίσθητης φύσης πακέτα δεδομένων. Οι επιθέσεις επιλεκτικής προώθησης είναι πιο αποτελεσματικές όταν το κακόβουλο ΣμηΕΑ είναι μέρος της διαδρομής των ροών δεδομένων και όχι απλά «εισβολέας» [36]. Ενός τέτοιου τύπου επίθεση μπορεί να καταστήσει άχρηστο ολόκληρο το δίκτυο IoD.

9.2.5 Επιθέσεις “Flooding”

Ένας από τους βασικούς στόχους των κακόβουλων ΣμηΕΑ είναι να «πλημμυρίσουν» τα κανονικά ΣμηΕΑ του IoD με τεράστιες ποσότητες ακατέργαστων ή αντιγραμμένων πακέτων δεδομένων. Αυτός ο τύπος επίθεσης εκμεταλλεύεται τους περιορισμένους πόσους ενός ΣμηΕΑ (π.χ. εύρος ζώνης επικοινωνίας και αποθηκευτικό χώρο του ΣμηΕΑ), με αποτέλεσμα εξαιρετικά μεγάλη συμφόρηση σε όλο το δίκτυο IoD και, σε περίπτωση μη αντιμετώπισης, την κατάρρευση του δικτύου [37].

9.2.6 Επιθέσεις «κατάληψης»

Σε αυτόν τον τύπο επίθεσης, ορισμένα εκ των ΣμηΕΑ τα οποία συμμετέχουν στο δίκτυο καθίστανται μη λειτουργικά προκαλώντας διακοπή των υπηρεσιών που παρέχει το IoD. Μία εκ των τεχνικών που χρησιμοποιούνται για την «κατάληψη» ή «αεροπειρατεία» ενός ΣμηΕΑ είναι η κατάργηση ελέγχου ταυτότητας (de-authentication) ή το Wi-Fi Aircrack [38].

9.2.7 Επιθέσεις “Man-in-the-middle”

Οι επιθέσεις τύπου “man-in-the-middle” προϋποθέτουν την ύπαρξη τριών εμπλεκόμενων μερών σε ένα δίκτυο. Το πρώτο μέρος είναι η συσκευή-στόχος του εισβολέα, το θύμα. Το δεύτερο μέρος είναι η συσκευή με την οποία επικοινωνεί, υπό κανονικές συνθήκες, το θύμα και το τρίτο μέρος είναι ο “man-in-the-middle”, η συσκευή η οποία παρακολουθεί και επιτίθεται στην επικοινωνία των δύο πρώτων μερών.

Στην περίπτωση του IoD, ο εισβολέας αναπτύσσει κακόβουλα ΣμηΕΑ τα οποία μεταμφιέζονται σε λειτουργικά ΣμηΕΑ του δικτύου ή αναπτύσσει ψευδείς σταθμούς βάσης για να υποκλέψει τις επικοινωνίες με τα λειτουργικά ΣμηΕΑ του δικτύου.

Ο σκοπός μίας τέτοιας επίθεσης είναι είτε η εν γένει διακοπή της λειτουργίας του IoD είτε η υποκλοπή των πληροφοριών που μεταδίδονται μεταξύ των ΣμηΕΑ και των σταθμών βάσης ή ακόμα και η ματαίωση μεταφοράς κάποιας συγκεκριμένης πληροφορίας [39].

9.2.8 Επίθεση Denial-of-Service (DOS)

Με τις επιθέσεις DoS (Denial-of-service), οι εισβολείς προσπαθούν να αποκλείσουν τους νόμιμους χρήστες των υπηρεσιών του IoD από τους πόρους του δικτύου. Ο επιτιθέμενος στέλνει έναν τεράστιο αριθμό αιτήσεων στο διακομιστή του δικτύου για να προκαλέσει συμφόρηση του δικτύου [40].

9.3 Υπάρχουσες λύσεις ασφάλειας IoD

Η απουσία μέτρων ασφάλειας στα κανάλια επικοινωνίας των συσκευών που απαρτίζουν ένα IoD αφήνει ανοιχτές «πόρτες» επιθέσεων στο δίκτυο.

Συνεπώς, είναι απαραίτητο να θεσπιστούν μηχανισμοί προστασίας ανάμεσα στους οποίους είναι η προστασία σε πραγματικό χρόνο, η επικαιροποίηση των υπάρχουσών λύσεων ασφάλειας και μηχανισμοί για την αντιμετώπιση των επιθέσεων αφού αυτές συμβούν.

Ανάμεσα στις λύσεις που εξετάζονται από την επιστημονική και επιχειρηματική κοινότητα είναι οι τεχνικές ελέγχου ταυτότητας πρόσβασης, η χρήση της τεχνολογίας blockchain και η επικαιροποίηση των υπάρχουσών λύσεων ασφάλειας.

9.3.1 Τεχνικές πιστοποίησης πρόσβασης χρήστη

Η πλειοψηφία των εφαρμογών του IoD βασίζεται στην ταχύτητα και στην μετάδοση σε πραγματικό χρόνο των δεδομένων που συλλέγονται αλλά και τον εντολών που αποστέλλονται στα ΣμηΕΑ από τους σταθμούς βάσης. Αυτό σημαίνει ότι οι χρήστες του IoD αναμένουν να λαμβάνουν τα δεδομένα των ΣμηΕΑ που εκτελούν μία πτήση σε μία συγκεκριμένη περιοχή ενδιαφέροντος, κατά το δυνατόν στον μικρότερο χρόνο. Αυτό όμως ταυτόχρονα δημιουργεί προβλήματα ασφάλειας αν έχουν πρόσβαση στα δεδομένα των ΣμηΕΑ μέσω του περιβάλλοντος του IoD χωρίς να γίνεται έλεγχος της ταυτότητάς τους. [41].

Ταυτόχρονα, τα δεδομένα που συλλέγονται κατά την πραγματοποίηση των διαφορετικών αποστολών των ΣμηΕΑ μέσα στο πλαίσιο ενός IoD θα πρέπει να πιστοποιούνται αναφορικά με την γνησιότητα και την πληρότητά τους, καθώς σε διαφορετική περίπτωση ολόκληρο το IoD τίθεται σε κίνδυνο. Συνεπώς, κανένας χρήστης δεν πρέπει να έχει πρόσβαση στα δεδομένα χωρίς πρώτα να έχει περάσει από έλεγχο ταυτότητας.

- Έλεγχος ταυτότητας χαμηλού επιπέδου

Η χρήση παραδοσιακών μεθόδων ελέγχου ταυτότητας όπως είναι τα συστήματα υπογραφής δημοσίου κλειδιού δεν είναι κατάλληλοι για χρήση από το IoD καθώς τα ΣμηΕΑ έχουν συνήθως περιορισμένους ενεργειακούς πόρους, συνεπώς θα πρέπει να χρησιμοποιηθούν ελαφριές τεχνικές ελέγχου ταυτότητας του χρήστη που επιθυμεί να αποκτήσει πρόσβαση στα δεδομένα (lightweight authentication techniques) [42].

Οι ερευνητές Srinivas, Das, Kumar, και Rodrigues [43][45] χρησιμοποίησαν κινητές συσκευές, κωδικούς πρόσβασης αλλά και βιομετρικά στοιχεία προκειμένου να αναπτύξουν και να δοκιμάσουν μία χαμηλής ενεργειακής κατανάλωσης μέθοδο πιστοποίησης ταυτότητας χρήστη η οποία βασίζεται σε προσωρινά διαπιστευτήρια (temporal credentials).

Για το παράδειγμά τους, σε μία συγκεκριμένη περιοχή ενδιαφέροντος, τα ΣμηΕΑ επικοινωνούν μεταξύ τους αλλά και με τους σταθμούς βάσης οι οποίοι είναι και οι μόνοι που έχουν αρμοδιότητα συνολικής διαχείρισης των παραμέτρων και των δεδομένων του IoD. Οι εξωτερικοί χρήστες του IoD μπορούν να έχουν πρόσβαση μέσω των δικών τους κινητών συσκευών σε συγκεκριμένα τμήματα των δεδομένων του IoD αλλά και σε προκαθορισμένα ΣμηΕΑ, αρκεί να είναι εξουσιοδοτημένοι χρήστες. Τα διαπιστευτήριά τους είναι σε ισχύ μόνο για το διάστημα που έχει οριστεί από τους σταθμούς βάσης.

Οι Nyangaresi και Petrovic [44] προχώρησαν ακόμα παραπέρα και ανέπτυξαν ένα ελαφρύ φυσικό πρωτόκολλο ελέγχου και πιστοποίησης της ταυτότητας, βασισμένο στη χαμηλή ενεργειακή επάρκεια ενός IoD. Το πρωτόκολλο είναι αποδοτικό και χρησιμοποιεί μόνο lightweight λειτουργίες OR (π.χ. XOR) συνένωσης και κατακερματισμού (concatenation & hashing).

Στην συγκεκριμένη προτεινόμενη λύση, τα κλειδιά συνεδρίας (session keys) και οι μεταβατικές παράμετροι ασφαλείας (transient security parameters) ενημερώνονται συνεχώς και δυναμικά, καθιστώντας πρακτικά αδύνατο για τους υποψήφιους εισβολείς να αποκτήσουν πρόσβαση είτε στα κλειδιά συνεδρίας είτε στα προσωρινά διαπιστευτήρια. Η δοκιμή του συγκεκριμένου πρωτοκόλλου έδειξε ότι είναι αποτελεσματικό στην αντιμετώπιση επιθέσεων man-in-the-middle και σε επιθέσεις επιλεκτικής προώθησης δεδομένων.

- Κρυπτογραφικός έλεγχος ταυτότητας

Η επαλήθευση της ταυτότητας συσκευών και ατόμων που συμμετέχουν σε ένα IoD, πριν από οποιαδήποτε ανταλλαγή δεδομένων και εντολών είναι σημαντικότερη για την αποτελεσματική και ασφαλή λειτουργία του δικτύου.

Ο Hussain και οι συνεργάτες του [45] επινόησαν ένα σύστημα ελέγχου ταυτότητας βασισμένο στην κρυπτογραφία ελλειπτικής καμπύλης (elliptic curve cryptography (ECC) και στη χρήση συμμετρικού κλειδιού (symmetric key) για την προστασία και πιστοποίηση της επικοινωνίας μεταξύ ΣμηΕΑ και χρηστών του IoD.

Το σύστημα βασίζεται σε τρία στοιχεία: Βιομετρικά στοιχεία, κρυπτογραφία και κινητές συσκευές.

Οι Nikooghadam, Amintoosi, Islam, και Moghadam [46] από την άλλη, πρότειναν επίσης μία λύση βασισμένη στην κρυπτογραφία ελλειπτικής καμπύλης (ECC) για το IoD, για την ασφαλή επόπτευση και την μετακίνηση των κατοίκων μελλοντικών έξυπνων πόλεων. Στη λύση που πρότειναν, συμμετέχουν οι χρήστες (οι κάτοικοι των πόλεων και οι χρήστες των ΣμηΕΑ), τα ΣμηΕΑ και ο διακομιστής ελέγχου (control server). Τόσο οι χρήστες όσο και τα ΣμηΕΑ εγγράφονται και καταγράφονται στον διακομιστή ελέγχου προκειμένου να αποκτήσουν τα απαιτούμενα διαπιστευτήρια πρόσβασης στο IoD ενώ ταυτόχρονα πιστοποιούνται και μεταξύ τους (οι χρήστες και τα ΣμηΕΑ) με τη βοήθεια του διακομιστή προκειμένου να αποκτήσουν ένα session key ώστε να επικοινωνούν απευθείας, χωρίς την παρεμβολή του διακομιστή.

Η πειραματική εφαρμογή της λύσης έδειξε ότι η προσέγγιση αυτή είναι ικανή να αποτρέψει γνωστούς τύπους επιθέσεων.

Να σημειωθεί ότι τα πρωτόκολλα ελέγχου ταυτότητας και συμφωνίας κλειδιού (AKA) ως υποσύνολο του ελέγχου ταυτότητας που βασίζεται στην κρυπτογραφία παράγουν κοινόχρηστα session keys μεταξύ των ΣμηΕΑ και των χρηστών για την κρυπτογράφηση των μεταδιδόμενων πληροφοριών.

- Έλεγχος ταυτότητας με χρήση βιομετρικών στοιχείων

Τα βιομετρικά στοιχεία [47] είναι μετρήσεις σχετιζόμενες τόσο με φυσικά όσο και με συμπεριφορικά χαρακτηριστικά των ατόμων (π.χ. εικόνα προσώπου, δακτυλικό αποτύπωμα, ίριδα ματιού) τα οποία μπορούν να χρησιμοποιηθούν για τον έλεγχο ταυτότητας του ατόμου και τη διαχείριση της πρόσβασής του στο IoD.

Ο Singandhup κ.ά [48], σε μία πρωτοποριακή προσέγγισή τους, παρουσίασαν ένα σύστημα ελέγχου και πιστοποίησης ταυτότητας χρήστη με τη χρήση ηλεκτροεγκεφαλογραφήματος (EEG), το οποίο κρυπτογραφεί την επικοινωνία μεταξύ των ΣμηΕΑ και του σταθμού βάσης με την παραγωγή ενός κλειδιού επικοινωνίας από το ηλεκτροεγκεφαλογράφημα του χρήστη που ζητά πρόσβαση.

Αρχικά, εξάγονται οι συντελεστές των δεδομένων του ηλεκτροεγκεφαλογραφήματος, χρησιμοποιώντας πολυώνυμα Legendre. Ακολούθως, χρησιμοποιείται η κωδικοποίηση Bose-Chaudhuri-Hocquenghem (BCH) και στη συνέχεια το κλειδί επικοινωνίας παράγεται από μια συνάρτηση hash (κατακερματισμού), έτσι ώστε να μην είναι δυνατή η αντιγραφή ή η αναπαραγωγή του.

Ο πειραματικός έλεγχος έδειξε ότι το προτεινόμενο σύστημα είναι ανθεκτικό σε πολλές από τις πλέον γνωστές επιθέσεις ασφαλείας, ανθεκτικότερο μάλιστα από τις υπάρχουσες συμβατικές μεθόδους.

9.3.2 Συστήματα blockchain

Η χρήση της τεχνολογίας blockchain εισήλθε και στο IoD παρέχοντας λύσεις ελέγχου ταυτότητας χρήστη αλλά και ασφαλούς αποθήκευσης και μεταφοράς δεδομένων.

Η συγκεκριμένη τεχνολογία προσφέρει τη δυνατότητα αποκεντρωμένης αποθήκευσης των δεδομένων ενώ με την κρυπτογραφία καταγράφεται κάθε αλληλεπίδραση μεταφοράς τους με απόλυτα ασφαλή τρόπο. [49].

Τα blockchains αποτελούνται από μπλοκ δεδομένων τα οποία συνδέονται μεταξύ τους με τη χρήση κρυπτογραφημένων συναρτήσεων hash. Όσοι βρίσκονται στον

κατάλογο παραληπτών των δεδομένων γνωρίζουν κάθε transaction που πραγματοποιείται από το blockchain συνεπώς είναι εξαιρετικά δύσκολο να πραγματοποιηθεί μία επιτυχημένη επίθεση στο συγκεκριμένο σύστημα [50].

- Έλεγχος πρόσβασης και ταυτότητας με τη χρήση τεχνολογίας blockchain

Οι Bera, Chattaraj και K. Das. [51] πρότειναν για το IoD μία λύση ελέγχου πρόσβασης βασισμένη στην τεχνολογία blockchain, η οποία επιτρέπει τόσο την ασφαλή επικοινωνία μεταξύ των ΣμηΕΑ όσο και μεταξύ των ΣμηΕΑ και των διακομιστών επίγειων σταθμών βάσης (ground station servers – GSS). Στη λύση τους, τα ασφαλή δεδομένα που συλλέγονται στον διακομιστή επίγειου σταθμού βάσης διαμορφώνουν τα transactions τα οποία στη συνέχεια ομαδοποιούνται σε block δεδομένων. Αυτά τα block δεδομένων εισέρχονται στο blockchain από τους cloud servers οι οποίοι συνδέονται με το GSS μέσω του αλγορίθμου Ripple Protocol Consensus (RPCA), σε ένα δίκτυο cloud διακομιστών peer-to-peer.

Τα transactions τα οποία έχουν εισαχθεί σε blocks δεν μπορούν να τροποποιηθούν ή να διαγραφούν από τη στιγμή που το συγκεκριμένο block δεδομένων προστεθεί στο blockchain.

Για τον έλεγχο ταυτότητας σε ένα 5G-enabled IoD, οι Feng, Liu, Guo, Yu, Qin και Choo [52] πρότειναν ένα σύστημα βασισμένο σε blockchain το οποίο είναι cross-domain.

Στη λύση που πρότειναν, χρησιμοποιούνται πολλαπλές υπογραφές (multi-signatures) με διαμοιρασμό threshold για τη δημιουργία μίας ταυτοτικής ένωσης μεταξύ των συνεργαζομένων τομέων.

Στο σύστημα αυτό η ασφαλής επικοινωνία επιτυγχάνεται μέσω smart contracts για την πιστοποίηση ταυτότητας χρήσης ενώ τα session keys είναι απολύτως εγγυημένα από την επικοινωνία μεταξύ των συσκευών.

9.4 Ανίχνευση εισβολής

Η εισβολή είναι η κακόβουλη ενέργεια προς μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο η οποία έχει ως στόχο είτε την καταστροφή του δικτύου είτε την υποκλοπή ευαίσθητων πληροφοριών και δεδομένων. Ως σύστημα εντοπισμού εισβολής (IDS – Intrusion Detection System) ονομάζουμε το λογισμικό ή την συσκευή το οποίο έχει ως αποστολή την συνεχή παρακολούθηση του δικτύου για τον εντοπισμό οποιασδήποτε απόπειρας εισβολής ή μη εξουσιοδοτημένης πρόσβασης [53].

Αναφορικά με το IoD, ο Perumalla και οι συνεργάτες του [54] ανέπτυξαν μία μέθοδο εντοπισμού εισβολής η οποία βασίζεται σε ένα βαθύ νευρο-ασαφές δίκτυο (deep neuro-fuzzy network), με πολύ μεγάλη ταχύτητα εντοπισμού και υψηλή ακρίβεια ανίχνευσης της εισβολής ενώ ο Ramadan με τους δικούς του συνεργάτες [55] μελέτησε τα είδη εισβολής σε ένα IoD και ανέπτυξε ένα πλαίσιο εντοπισμού το οποίο βασίζεται στη βαθιά μάθηση (deep-learning) για ανάλυση δεδομένων σε πραγματικό χρόνο.

Το συγκεκριμένο framework βασίζεται στα Επαναλαμβανόμενα νευρωνικά δίκτυα (Recurrent Neural Networks – RNN), συλλέγει δεδομένα από το RNN και στη συνέχεια χρησιμοποιεί Big Data analytics για την ανίχνευση των αποπειρών εισβολής.

Περιλαμβάνει module επεξεργασίας ροής το οποίο καταγράφει σε πραγματικό χρόνο την επικοινωνία μεταξύ των ΣμηΕΑ, στην οποία συμπεριλαμβάνονται και δεδομένα για την ανίχνευση της εισβολής. Αυτά τα δεδομένα αποστέλλονται στη συνέχεια σε δύο RNN modules για ανάλυση δεδομένων αλλά και για περαιτέρω εκπαίδευση του RNN για μελλοντικές απόπειρες εισβολής.

9.5 Σχήματα προστασίας της ιδιωτικότητας

Τα ΣμηΕΑ τα οποία είναι εξοπλισμένα με συσκευές καταγραφής εικόνας και βίντεο μπορούν να χρησιμοποιηθούν σε πολλές και διαφορετικές αποστολές, από την καταγραφή μίας κοινωνικής εκδήλωσης έως την επίτευξη συνόρων και συγκεντρώσεων ατόμων.

Με την συνεχή εξέλιξη της ποιότητας των συσκευών καταγραφής που διαθέτουν τα ΣμηΕΑ, εγείρονται σημαντικά ερωτήματα αναφορικά με την προστασία των προσωπικών δεδομένων των πολιτών.

9.5.1 Πολιτικές προστασίας της ιδιωτικότητας

Ο Yaxing Yao και η ομάδα του [56] δημοσίευσε μία πολύ ενδιαφέρουσα έρευνα για την οποία χρησιμοποιήθηκαν στοιχεία τα οποία συγκεντρώθηκαν διαδικτυακά σε δύο φάσεις.

Στην έρευνα πήραν μέρος 169 ελεγκτές ΣμηΕΑ και 717 άτομα τα οποία λειτουργούν δίπλα σε περιοχές όπου χρησιμοποιούνται ΣμηΕΑ. Οι ερωτώμενοι κλήθηκαν να απαντήσουν αναφορικά με το πως αντιλαμβάνονται τις τεχνολογικές λύσεις ή τις πολιτικές για την προστασία της ιδιωτικής ζωής.

Από τις απαντήσεις τους αποκαλύπτεται ότι η καταγραφή των ιδιοκτητών των ΣμηΕΑ και η αυτόματη θόλωση προσώπου για όσους καταγράφονται από τις κάμερες των αεροσκαφών, έλαβαν τις περισσότερες θετικές απαντήσεις.

Στη μελέτη συστήνεται η συνδυαστική χρήση πολλαπλών λύσεων για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων στο πλαίσιο της ευρείας χρήσης ΣμηΕΑ.

9.5.2 Τεχνολογικές λύσεις προστασίας της ιδιωτικότητας

Οι Chen και Wang [57] σχεδίασαν ένα βελτιωμένο security pseudonym για την προστασία των δεδομένων του IoD τα οποία βρίσκονται στο cloud. Σε αυτό η κωδικοποίηση δύο επιπέδων (two-level network encoding) είναι σχεδιασμένη έτσι ώστε τα δεδομένα cloud να είναι αποσυνδεδεμένα από το «ψευδώνυμο» του ιδιοκτήτη τους.

Με τη μέθοδο αυτή αντιμετωπίζονται τόσο οι εξωτερικοί εισβολείς όσο και οι εσωτερικοί κακόβουλοι χρήστες και δύναται να εφαρμοστεί σε μη ασφαλείς cloud βάσεις δεδομένων. Η πειραματική δοκιμή της λύσης απέδειξε ότι ο χρόνος επεξεργασίας μειώθηκε κατά 90% και η κατανάλωση ενέργειας κατά 10%, συγκρινόμενη με λύσεις οι οποίες βασίζονται στο hash.

Αναφορικά με την εικόνα των ατόμων που καταγράφονται από τα ΣμηΕΑ, αναπτύχθηκε [58] ένα σύστημα προστασίας της ιδιωτικότητας για IoD βασισμένο στην «γενετική αρχιτεκτονική αντίπαλου δικτύου» και σε τεχνικές βαθιάς μάθησης.

Σε αυτό το σύστημα, στις εικόνες και στα βίντεο των ατόμων που καταγράφονται από τα ΣμηΕΑ πραγματοποιούνται ελαφρές αλλαγές έτσι ώστε να συνεχίζουν μεν να αναγνωρίζονται ως άνθρωποι αλλά να μην μπορεί να γίνει ταυτοποίηση κάθε ατόμου. Με αυτόν τον τρόπο οι σημασιολογικές πληροφορίες διατηρούνται άθικτες χωρίς να απειλείται η ιδιωτικότητα κάθε προσώπου.

Τέλος, αναφορικά με την καταγραφή της τοποθεσίας των ΣμηΕΑ, έχει προταθεί μία μέθοδος [59] που ονομάζεται MixDrones η οποία εκτός από το ψευδώνυμο των ΣμηΕΑ αλλάζει και την καταγεγραμμένη τροχιά τους, προστατεύοντας έτσι την τοποθεσία στην οποία επιχειρούν.

9.6 Προκλήσεις

9.6.1 Προκλήσεις των συστημάτων blockchain

- Υπολογιστικό κόστος

Η χρήση της τεχνολογίας blockchain στα IoDs ενώ είναι μία πολλά υποσχόμενη λύση για την ασφάλεια, ταυτόχρονα απαιτεί σημαντικούς υπολογιστικούς και ενεργειακούς πόρους.

Δεδομένου ότι τόσο οι υπολογιστικοί όσο και οι ενεργειακοί πόροι των ΣμηΕΑ είναι πεπερασμένοι και χρησιμοποιούνται για πολλαπλές διαφορετικές εργασίες, η πρόκληση είναι στο πως αυτοί οι πόροι θα εμπλακούν στη χρήση του blockchain χωρίς να τεθούν σε κίνδυνο οι υπόλοιπες λειτουργίες του IoD.

Το Edge computing είναι μία τεχνολογία η οποία μπορεί να χρησιμοποιηθεί για την ανακούφιση των ΣμηΕΑ από το υπολογιστικό βάρος της τεχνολογίας blockchain, απαιτείται όμως βελτιστοποίηση στη ροή των δεδομένων και μείωση της καθυστέρησης μετάδοσης δεδομένων έτσι ώστε να αποφευχθεί η απώλεια σήματος κατά τη διάρκεια της μεταφοράς δεδομένων από τα ΣμηΕΑ προς τους διακομιστές edge. Συνεπώς, η ενσωμάτωση της συγκεκριμένης τεχνολογίας στο IoD είναι ένα από τα πλέον επίκαιρα ζητήματα έρευνας. [60]

- Αύξηση χρόνου επεξεργασίας κατά τη χρήση του blockchain

Η εισαγωγή και εξαγωγή δεδομένων στα blockchains γίνεται με τη χρήση «έξυπνων συμβολαίων», με συνέπεια την αύξηση του χρόνου επεξεργασίας. Αν και αυτή η αύξηση είναι απαραίτητη για τη διασφάλιση της ποιότητας και ασφάλειας επικοινωνίας αποκεντρωμένων δικτύων blockchain, για πολλές χρήσεις του IoD είναι μη αποδεκτή (π.χ. στην επόπτευση χώρων για λόγους ασφαλείας), με συνέπεια τον περιορισμό της χρήσης του blockchain στο IoD. [61]

- Αύξηση του μεγέθους των blockchains

Το μέγεθος ενός blockchain αφορά την απόδοσή του (ο αριθμός των συναλλαγών ανά δευτερόλεπτο) αλλά και το συνολικό μέγεθος του συστήματος blockchain (ο αριθμός των peer σε blockchain).

Εάν το μέγεθος ενός blockchain σε ένα IoD αυξάνεται συνεχώς όπως και ο αριθμός των δεδομένων, ο απαιτούμενος αποθηκευτικός χώρος και η υπολογιστική ισχύς θα γίνει μη διαχειρίσιμη με αποτέλεσμα να δημιουργηθούν προβλήματα στο σύνολο του IoD. [62]

- Επιθέσεις σε συστήματα blockchain

Λόγω της εξαιρετικής τους ανθεκτικότητας στις απόπειρες παραβίασης, η εφαρμογή της τεχνολογίας blockchain στο IoD αυξάνεται συνεχώς. Παρόλα αυτά, η ίδια η τεχνολογία έχει αδυναμίες και αντιμετωπίζει σοβαρά προβλήματα ασφαλείας [61]:

Majority attacks: Εάν οι εισβολείς καταφέρουν να ελέγξουν ένα σημαντικό τμήμα της υπολογιστικής ισχύος του IoD τότε, το πρωτόκολλο συναίνεσης μπορεί να παραβιαστεί. Για παράδειγμα, εάν οι εισβολείς κατέχουν περισσότερο από το 50% της ισχύος κατακερματισμού (hash power), η οποία είναι απαραίτητη για το Blockchain, τότε, μπορούν να κάνουν να blockchains να αποδέχονται επιβλαβή block δεδομένων [62].

Επιθέσεις DOS: Οι χρησιμοποιούμενοι για το blockchain πόροι του IoD (π.χ. η ικανότητα επεξεργασίας του δικτύου) μπορούν να εξαντληθούν από τους εισβολείς μέσω της πραγματοποίησης DOS attacks [61].

Παραβίαση των ιδιωτικών κλειδιών επικοινωνίας: Οι λογαριασμοί των χρηστών του IoD μπορούν να παραβιαστούν αν οι εισβολείς καταφέρουν να αποκτήσουν πρόσβαση στο «ιδιωτικό κλειδί» (private key) του λογαριασμού κάθε χρήστη [61].

9.6.2 Θέματα σχετικά με την ιδιωτικότητα

Η ευρεία ανάπτυξη των ΣμηΕΑ, του IoD και των υπηρεσιών για τις οποίες αυτό μπορεί να χρησιμοποιηθεί, είναι πιθανό να εμφανίσει κινδύνους για την προστασία της ιδιωτικότητας, τόσο ατόμων όσο και οργανισμών. Τα ΣμηΕΑ μπορούν να συλλέγουν δεδομένα τα οποία ανήκουν σε άτομα και αντικείμενα, όσο βρίσκονται μέσα στο LOS (Line-of-sight) του ΣμηΕΑ, στις περισσότερες όμως περιπτώσεις τα άτομα που βρίσκονται μέσα σε αυτόν τον αόρατο «κύκλο» δεν μπορούν να δώσουν τη συναίνεσή τους στη συλλογή των δεδομένων ή να την αρνηθούν. [63]

Προς τούτο και οι αρμόδιες αρχές ήδη εξετάζουν τη σύνταξη κανονισμών και πολιτικών οι οποίες θα σχετίζονται με την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων, σε ευθεία όμως συσχέτιση με τη μη παρεμπόδιση της ανάπτυξης και επέκτασης χρήσης των ΣμηΕΑ και του IoD. Η πράξη έχει άλλωστε δείξει ότι τα ΣμηΕΑ μπορούν να προσφέρουν υψηλού επιπέδου και χαμηλού κόστους υπηρεσίες προς το κοινωνικό σύνολο και την εθνική ασφάλεια.

10. Συμπεράσματα – Περίληψη

Τα ΣμηΕΑ πλέον βρίσκονται σε χρήση σχεδόν σε κάθε πτυχή της δημόσιας και ιδιωτικής ζωής. Από την βιντεοσκόπηση κοινωνικών εκδηλώσεων και την προστασία των συνόρων μίας χώρας έως την έξυπνη γεωργία και τις ανανεώσιμες πηγές ενέργειας.

Η δυνατότητά τους τόσο να συλλέγουν δεδομένα όσο και να παρέχουν τηλεπικοινωνιακές υπηρεσίες (π.χ. σε περιοχές όπου έχουν συμβεί φυσικές καταστροφές), η ταχύτητα με την οποία μπορούν να μεταβούν στο σημείο ενδιαφέροντος και η ευκολία στην συσχέτιση μεταξύ των ΣμηΕΑ και άλλων συσκευών (σταθμών βάσης, τηλεπικοινωνιακού εξοπλισμού κ.λπ) τα κάνουν εξαιρετικά ενδιαφέρον αντικείμενο έρευνας για επέκταση των χρήσεών τους.

Επιπλέον, η δυνατότητα δικτύωσης με τη δημιουργία των IoD (Internet of Drones), μπορεί να επεκτείνει τόσο την εμβέλεια χρήσης των ΣμηΕΑ όσο και την αθροιζόμενη υπολογιστική ισχύ τους για τη διενέργεια πολύπλοκων αποστολών.

Την ίδια όμως στιγμή ανακύπτουν σοβαρά ζητήματα ασφάλειας, αντίστοιχα με αυτά που αντιμετωπίζει το διαδίκτυο καθώς και ζητήματα προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας.

Τόσο οι δυνατότητές τους όσο και τα ζητήματα που ανακύπτουν, ωθούν την επιστημονική και επιχειρηματική κοινότητα εν συνόλω στην υιοθέτηση των πλέον σύγχρονων τεχνολογιών στη χρήση των ΣμηΕΑ και του IoD (blockchain, μηχανική μάθηση, βαθιά μάθηση, νευρωνικά δίκτυα).

Με την επέκταση του 5G, το οποίο σταδιακά θα καλύψει το σύνολο του δυτικού κόσμου, θα δούμε εφαρμογές των ΣμηΕΑ και του IoD οι οποίες έως σήμερα μας φαίνονται σχεδόν αδιανόητες: Αυτόνομα εναέρια ταξί, αυτόνομα οχήματα μεταφοράς δεμάτων και ανθρώπων, ψηφιακά δίδυμα πόλεων, έξυπνες πόλεις, καθοδήγηση επίγειων και θαλασσίων μεταφορικών μέσων.

Χωρίς να προσπαθούμε να προβλέψουμε το μέλλον, μπορούμε να πούμε με σχετική βεβαιότητα ότι το IoD μαζί με την τεχνητή νοημοσύνη θα φέρουν τέτοιες αλλαγές στον τρόπο που ζούμε και εργαζόμαστε μέσα στα επόμενα χρόνια, σχεδόν αντίστοιχης σημασίας με αυτές που έφερε η ανάπτυξη του Διαδικτύου πριν από σχεδόν τριάντα χρόνια.

11. Βιβλιογραφία

- [1] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L.G. Giordano, A. Garcia-Rodriguez,, «Survey on UAV cellular communications: Practical aspects, standardization,» σε *IEEE Commun. Surv.*, 2018.
- [2] Lav Gupta, Senior Member IEEE, Raj Jain, Fellow, IEEE, and Gabor Vaszkun, «Survey of Important Issues in UAV Communication Networks,» σε *IEEE Commun. Surv. Tutor.* 18 (2), 2016.
- [3] R. B. a. S. L. W. M. Gharibi, «Internet of drones 4,» σε *IEEE Access*, 2016.
- [4] V. S. , T. G. , J. K. a. I. Y. Gaurav Choudhary, «Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives,» 2018.
- [5] Η. Στραβάκος, «Διπλωματική Εργασία: Μελέτη εφαρμογής ασύρματου δικτύου δεδομένων,» Θεσσαλονίκη, Πανεπιστήμιο Μακεδονίας, 2003, p. 17.
- [6] «Πανεπιστήμιο Πατρών - eclass,» [Ηλεκτρονικό]. Available: <https://eclass.upatras.gr/modules/document/file.php/EE799/OFDM.pdf>.
- [7] O.-H. K. S.-H. L. a. K.-R. K. Sukhrob Atoev, «An Efficient SC-FDM Modulation Technique for a UAV Communication Link,» 25 11 2018. [Ηλεκτρονικό]. Available: <https://www.mdpi.com/2079-9292/7/12/352>.
- [8] J. K. L. D. B. Galkin, «Coverage analysis for low-altitude UAV networks in urban environments,» σε *2017 IEEE Global Communications Conference, GLOBECOM*, 2017.
- [9] W. S. M. B. M. D. M. Mozaffari, «Performance optimization for UAV-enabled wireless communications under flight time constraints,» σε *IEEE Global Communications Conference, GLOBECOM*, 2017.
- [10] I. G. W. S. M. B. D. Athukoralage, «Regret based learning for UAV assisted LTE-U/WiFi public safety networks,» σε *IEEE Global Communications Conference, GLOBECOM*, 2016, 2016.
- [11] D.-M. C. W. R. H. R. Jain, «A quantitative measure of fairness and discrimination for resource allocation in shared computer system,» σε *Digital Equipment Corporation, DEC-TR-301*, 1984.
- [12] M. L. Z. Y. a. Q. G. J. Chen, «An Improved A* Algorithm for UAV Path Planning Problems,» σε *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chongqing, China, 2020.
- [13] A. D. H. T. Elaf Jirjees Dhulkefi, «DIJKSTRA ALGORITHM USING UAV PATH PLANNING,» *Selcuk University Journal of Engineering Science and Technology*, December 2020.
- [14] I. A. G. I. upasinghe Nadisanka, «Optimum Hovering Locations with Angular Domain User Separation for Cooperative UAV Networks,» σε *IEEE Global Communications Conference, GLOBECOM*, 2016.
- [15] W. S. M. B. m. D. Mohammad Mozaffari, «Drone Small Cells in the Clouds: Design, Deployment and Performance Analysis,» σε *GLOBECOM 2015 - 2015 IEEE Global Communications Conference*, 2015.

- [16 W. S. M. B. a. M. D. Mohammad Mozaffari, «Efficient Deployment of Multiple Unmanned Aerial Vehicles for Optimal Wireless Coverage,» σε *IEEE Communications Letters*, vol. 20, no. 8, 2016, pp. 1647-1650.
- [17 J. L. J. R. D. Carlos Cambra, «Communication Ad Hoc Protocol for Intelligent Video Sensing Using AR Drones,» σε *Proceedings of the 2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, 2013.
- [18 Y. Y. N. R. I. G. H. D. A. B. Ali Rahmati, «arxiv.org,» 13 Φεβρουάριος 2019. [Ηλεκτρονικό]. Available: <https://arxiv.org/abs/1902.04721>.
- [19 E. Worlanyo, 17 Απρίλιος 2016. [Ηλεκτρονικό]. Available: <https://www.cse.wustl.edu/~jain/cse574-16/ftp/netcode/index.html>.
- [20 K. M. J. T. K. Chanjun Chun, «Drone Noise Reduction using Deep Convolutional Autoencoder for UAV Acoustic Sensor Networks,» σε *IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW)*, 2019.
- [21 W. N. X. W. R. P. L. S. S. K. S. J. Kai Li, «Energy-Efficient Cooperative Relaying for Aerial Vehicles,» σε *IEEE Transactions on Mobile Computing*, 2015.
- [22 R. Bhardwaj, «Network Interview,» [Ηλεκτρονικό]. Available: <https://networkinterview.com/proactive-vs-reactive-routing-protocols/>.
- [23 H. N. N. K. F. O. R. M. M. Horiuchi, «Throughput maximization for long-distance real-time data transmission over multiple UAVs,» σε *International Conference on Communications, ICC*, 2016.
- [24 L. Y. F. W. M. T. G. C. a. A. V. V. L. Kong, «Autonomous Relay for Millimeter-Wave Wireless Communications,» σε *IEEE Journal on Selected Areas in Communications*, 2017.
- [25 S. C. C. GREESHMA SOSA THOMAS, «A Review on Autonomous Relay For Millimeter Wave Wireless Communications,» σε *IOP Conference Series: Materials Science and Engineering*, 2018.
- [26 S. E. K. a. G. P. Wallace, «International law, military effectiveness, and public support for drone strikes,» *Journal of Peace Research*, 2016.
- [27 M. L. S. Y. S. G. S. L. K. Chand, «Drone based wireless mesh network for disaster/military environment,» *Journal of Computer and Communications*, 2018.
- [28 C. V. Tilburg, «First Report of Using Portable Unmanned Aircraft Systems (Drones) for Search and Rescue,» *Wilderness and Environmental Medicine*, τόμ. 28, αρ. 2, pp. 116-118, 2017.
- [29 S. J. K. G. Quiroz, «A confetti drone: Exploring drone entertainment,» σε *Proc. IEEE Int. Conf. Consum. Electron.*, 2017.
- [30 Y. J. S. P. K. R. G. O. S. J. Kim, *A Survey of Drone Use*, Springer, 2018, pp. 339-352.
- [31 J. Scott και C. Scott, «Drone delivery models for healthcare,» σε *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017.
- [32 E. Barmounakis και N. Geroliminis, «On the new era of urban traffic monitoring with massive drone data: The pneuma large-scale field experiment,» σε *Transp. Res. Part C: Emerg. Technol.*, 2020.

- [33 C. Christodoulou και P. Kolios, «Optimized tour planning for drone-based urban traffic monitoring,» σε *IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, Antwerp, Belgium, 2020.
- [34 M. Wazid, A. K. Das και J.-H. Lee, «Authentication protocols for the internet of drones: taxonomy, analysis and future directions,» *Journal of Ambient Intelligence and Humanized Computing*, 2018.
- [35 M. Yahuza, «Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges,» *IEEE Access*, τόμ. 9, pp. 57243-57270, 2021.
- [36 «Detecting selective forwarding attacks in wireless sensor networks,» σε *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*, Rhodes Island, 2006.
- [37 C. Pu και P. Zhu, «Defending against flooding attacks in the internet of drones environment,» σε *IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, 2021.
- [38 J.-P. Yaacoub, H. Noura, O. Salman και A. Chehab, «Security analysis of drones systems: Attacks, limitations, and recommendations,» September 2020. [Ηλεκτρονικό]. Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/>.
- [39 Y. Li και C. Pu, «Lightweight Digital Signature Solution to Defend Micro Aerial Vehicles Against Man-In-The-Middle Attack,» σε *IEEE 23rd International Conference on Computational Science and Engineering (CSE)*, Guangzhou, China, 2020.
- [40 A. Fotouhi, «Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges,» σε *IEEE Communications Surveys & Tutorials*, 2019.
- [41 M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos και J. J. Rodrigues, «Design and analysis of secure lightweight remote user authentication,» 2019.
- [42 V. O. Nyangaresi και M. Morsy, «Towards Privacy Preservation in Internet of Drones,» σε *IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI)*, 2021.
- [43 J. Srinivas, A. K. Das, N. Kumar και J. J. Rodrigues, «Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment,» σε *IEEE Transactions on Vehicular Technology*, 2019.
- [44 V. O. Nyangaresi και N. Petrovic, «Efficient PUF Based Authentication Protocol for Internet of Drones,» σε *International Telecommunications Conference (ITC-Egypt)*, Alexandria, 2021.
- [45 S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan και N. Kumar, «Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones,» σε *IEEE Systems Journal*, 2021.
- [46 M. Nikooghadam, H. Amintoosi, S. H. Islam και M. F. Moghadam, «A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance,» Μάιος 2021. [Ηλεκτρονικό].
- [47 W. Yang, S. Wang, J. Hu, G. Zheng και C. Valli, «Security and Accuracy of Fingerprint-Based Biometrics: A Review,» 2019. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/330711092_Security_and_Accuracy_of_Fingerprint-Based_Biometrics_A_Review.

- [48 A. Singandhupe, H. M. La και D. Feil-Seifer, «IEEE Access,» 2018.
- [49 «Survey on blockchain for Internet of Things,» *Computer Communications*, αρ. 136, pp. 10-29, Φεβρουάριος 2019.
- [50 M. Singh, G. S. Aujla και R. S. Bali, «A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment,» *IEEE Transactions on Intelligent Transportation Systems*, τόμ. 22, αρ. 7, pp. 4404-4413, 2021.
- [51 B. Bera, D. Chattaraj και A. K. Das, «Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment,» *Computer Communications*, αρ. 153, pp. 229-249, 2020.
- [52 C. Feng, B. Liu, Z. Guo, K. Yu,, Z. Qin και K.-K. R. Choo, «Blockchain-Based Cross-Domain Authentication for Intelligent 5G-Enabled Internet of Drones,» *IEEE Internet of Things Journal*, τόμ. 9, αρ. 8, pp. 6224-6238, Σεπτέμβριος 2021.
- [53 M. Wazid, A. K. Das και J.-H. Lee, «Authentication protocols for the internet of drones: taxonomy, analysis and future directions,» *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-10, 2018.
- [54 S. Perumalla, S. Chatterjee και A. P. S. Kumar, «Block Chain-based access control and intrusion detection system in IoD,» σε *6th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatre, India, 2021.
- [55 R. A. Ramadan, A.-H. Emara, M. Al-Sarem και M. Elhamahmy, «Internet of Drones Intrusion Detection Using Deep Learning,» *Electronics*, τόμ. 10, αρ. 21, p. 2633, 2021.
- [56 Y. Yao, H. Xia, Y. Huang και Y. Wang, «Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders,» σε *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.
- [57 Y.-J. Chen και L.-C. Wang, «Privacy Protection for Internet of Drones: A Network Coding Approach,» *IEEE Internet Things Journal*, 2018.
- [58 H. Lee, M. U. Kim, Y. Kim, H. Lyu και H. J. Yang, «Development of a Privacy-Preserving UAV System With Deep Learning-Based Face Anonymization,» *IEEE Access*, τόμ. 9, pp. 132652-132662, 2021.
- [59 A. R. Svaigen, A. Boukerche, L. B. Ruiz και A. A. Loureiro, «MixDrones: A Mix Zones-based Location Privacy Protection Mechanism for the Internet of Drones,» σε *MSWiM '21: 24th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2021.
- [60 Z. Chang, «Blockchain-Empowered Drone Networks: Architecture, Features, and Future,» *IEEE Network*, τόμ. 35, αρ. 1, pp. 86-93, 2021.
- [61 X. Wang, «Survey on blockchain for Internet of Things,» *Computer Communications*, τόμ. 136, p. 1029, 2019.
- [62 I.-C. Lin και T.-C. Liao, «A survey of blockchain security issues and challenges,» *International Journal of Network Security*, τόμ. 19, αρ. 5, pp. 653-659, 2017.
- [63 S. Mayer, L. Lischke και P. W. Woźniak, «Drones for Search and Rescue,» σε *International workshop on Human-Drone Interaction*, 2019.

- [64 X. T. a. W. Y. Yinsen Jia, «An UAV Wireless Communication Noise Suppression Method Based on OFDM Modulation and Demodulation,» 5 2 2020. [Ηλεκτρονικό]. Available: <https://www.mdpi.com/2079-9292/7/12/352>.
- [65 Τ. Χρήστος, «ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ - Βελτιστοποίηση Πόρων σε Δίκτυα Τηλεπικοινωνιών Ασύρματης Φόρτισης υποβοηθούμενα από UAV,» 10 2021. [Ηλεκτρονικό]. Available: http://ikee.lib.auth.gr/record/335328/files/Christos_Tsakos_thesis.pdf.
- [66 C. Ρυ και P. Zhu, «Defending against Flooding Attacks in the Internet of Drones Environment,» σε *IEEE Global Communications Conference (GLOBECOM)*, Μαδρίτη, Ισπανία, 2021.

12. Ορολογία

Drone	Συστήματα μη Επανδρωμένων Αεροσκαφών (ΣμηΕΑ)
Unmanned Aerial Vehicle – UAV	Μη επανδρωμένο εναέριο όχημα
IoD (Internet of Drones)	Διαδίκτυο των ΣμηΕΑ
WSN (Wireless Sensor Networks)	Ασύρματα Δίκτυα Αισθητήρων
Mobile Ad-hoc NETworks – MANETs	Ασύρματα Ad-hoc δίκτυα
Flying Ad-hoc NETworks – FANETs	Ιπτάμενα Ad-hoc Δίκτυα
GPS – Global Positioning System	Παγκόσμιο Σύστημα Τοποθεσίας (γεωεντοπισμού)
BS – Base Stations	Σταθμοί βάσης
Aerial BS	Εναέριοι σταθμοί βάσης
Remote radio heads – RHHs	Αναμεταδότες ραδιοφωνικού σήματος
Fixed/rotary wing drones	Υβριδικά ΣμηΕΑ σταθερής πτέρυγας/ροτόρων
Low-altitude platforms – LAPs	Πλατφόρμες χαμηλού υψομέτρου
LOS – Line of Sight	Άμεση οπτική επαφή
High-altitude platforms -HAPs	Πλατφόρμες μεγάλου υψομέτρου
Vehicular nodes	Οχηματικοί κόμβοι
Physical layer	Φυσικό επίπεδο
Modulation techniques	Τεχνικές διαμόρφωσης
Signal quality enhancement	Βελτίωση ποιότητας σήματος
FHSS – frequency-hopping spread spectrum	Φάσμα Διασποράς με εναλλαγή συχνότητας
DSSS – direct-sequence spread spectrum	Σύστημα Ευθείας Αλληλουχίας Ευρέως Φάσματος
OFDM – Orthogonal Frequency Division Multiplexing	Ορθογώνια Πολύπλεξη Διαίρεσης Συχνοτήτων
Multipath channels	Κανάλια πολυόδευσης
InterSymbol Interference – ISI	Διασυμβολική παρεμβολή
Intercarrier Interference – ICI	Διακαναλική παρεμβολή
Power Line Communication – PLC	Επικοινωνίες μέσω γραμμές ρεύματος
SC-FDM – Single Carrier Frequency Division Multiplex	Πολλαπλή Πρόσβαση Διαίρεσης Συχνότητας Μονού Φέροντος
Signal-to-interference-and-noise-ratio SINR	Δείκτης λόγου σήματος προς παρεμβολές και θόρυβο
Constrained Application Protocol – CoAP	Πρωτοκολλο περιορισμένης εφαρμογής
Message Queuing Telemetry Transport – MQTT	Μεταφορά ουράς μηνυμάτων μέσω τηλεμετρίας
BER – bit error rate	Ρυθμός σφάλματος bit
MIMO (multiple-input, multiple-output)	Πολλαπλή είσοδος, πολλαπλή έξοδος
Wireless Networked Robot systems – WNR	Ασύρματα δικτυωμένα ρομποτικά συστήματα
Wireless Sensor and Actuator Networks – WSN	Ασύρματα δίκτυα αισθητήρων και ενεργοποιητών
Cooperative Relaying	Συνεργατική μεταγωγή
Cooperative Beamforming	Συνεργατική διαμόρφωση δέσμης

Multi-Hop Networking	Δικτύωση πολλαπλών μεταπηδήσεων
Medium Access Control (MAC)	Έλεγχος πρόσβασης φυσικού μέσου
CNN	Συνελικτικό νευρωνικό δίκτυο
STFT – short-time Fourier transform	Βραχυπρόθεσμος μετασχηματισμός Fourier
mmWave communications	Επικοινωνίες χιλιοστομετρικών κυμάτων
Blockchain technology	Τεχνολογία αλυσίδας μπλοκ δεδομένων