ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗΤΕΧΝΟΛΟΓΙΩΝΠΛΗΡΟΦΟΡΙΚΗΣΚΑΙΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝΣΥΣΤΗΜΑΤΩΝ
ΠΜΣ : «ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ»
ΚΑΤΕΥΘΥΝΣΗ:«ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ»

ΜΕΛΕΤΗ AD-HOC ΔΙΚΤΥΩΝ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ ΣΥΣΚΕΥΩΝ

Επιβλέπων Καθηγητής: Γεώργιος Π. Ευθύμογλου

ΜΑΚΡΗΣ ΚΥΡΙΑΚΟΣ ΑΜ: ΜΕ1555

ΠΕΙΡΑΙΑΣ 2017

ΠΕΡΙΛΗΨΗ

Η εξέλιξη των ασύρματων επικοινωνιών και της ηλεκτρονικής έχει οδηγήσει στη δημιουργία δικτύων από συσκευές χαμηλού κόστους χωρίς συγκεκριμένη δομή. Τα δίκτυα αυτά, όπως είναι τα δίκτυα αισθητήρων, αποτελούνται από μικρού μεγέθους κόμβους, οι οποίοι δεν έχουν μια κεντρική διαχείριση. Η απουσία σταθερής υποδομής καθιστά αυτά τα δίκτυα κατάλληλα για επικοινωνία σε καταστάσεις έκτακτης ανάγκης, σε δύσβατες περιοχές, δικτύωση μεταξύ αυτοκινήτων κλπ., δημιουργεί όμως και ένα σύνολο από νέες απαιτήσεις για το σχεδιασμό τους. Η παρούσα πτυχιακή εργασία μελετά τα σύγχρονα ad hoc δίκτυα για την ασύρματη διασύνδεση συσκευών.

Στο Κεφάλαιο 1 παρουσιάζονται τα ασύρματα συστήματα κινητών επικοινωνιών και περιγράφονται τα ασύρματα τοπικά δίκτυα και τα κυψελωτά δίκτυα επικοινωνιών. Στο Κεφάλαιο 2 παρουσιάζονται διάφορες περιπτώσεις ασύρματων ad hoc δικτύων, όπως είναι τα κινητά ad hoc δίκτυα (MANET), τα δίκτυα σώματος (body area network – BAN), και τα ασύρματα προσωπικά δίκτυα (wireless personal area network -WPAN).

Στο Κεφάλαιο 3 παρουσιάζονται τα πιο γνωστά πρωτόκολλα δρομολόγησης που μπορούν να χρησιμοποιηθούν στα ασύρματα ad hoc δίκτυα και περιγράφονται οι κατηγορίες και τα χαρακτηριστικά των πρωτοκόλλων αυτών. Στο Κεφάλαιο 4 παρουσιάζονται τα πιο γνωστά πρωτόκολλα επικοινωνίας και τεχνολογίες οι οποίες υποστηρίζουν ή έχουν τη δυνατότητα να υποστηρίξουν ad hoc τοπολογίες. Περιγράφονται τα πρότυπα 802.11, HIPERLAN-2, Bluetooth, η αρχιτεκτονική Scatternet και το πρότυπο Zigbee. Στο Κεφάλαιο 5 παρουσιάζονται τα θέματα ασφάλειας των ad hoc δικτύων και περιγράφονται οι απαιτήσεις ασφάλειας, οι απειλές και οι επιθέσεις που μπορούν να λάβουν χώρα στα ad hoc δίκτυα.

Στο Κεφάλαιο 6 παρουσιάζεται η ανάλυση και το μοντέλο προσομοίωσης για τη μελέτη της σύνδεση μίας συσκευής με γειτονικές συσκευές οι οποίες είναι τυχαία κατανεμημένες στο χώρο παρουσία διάλειψης με κατανομή Nakagami-m αλλά και ομοδιαυλικής παρεμβολής. Η ανάλυση αλλά και τα αποτελέσματα του μοντέλου προσομοίωσης δείχνουν την επίδραση διαφόρων παραμέτρων του συστήματος, όπως ισχύς εκπομπής, ισχύ παρεμβολής, περιβάλλον διάδοσης και χωρική πυκνότητα των συσκευών στην πιθανότητα διασύνδεσης της κάθε συσκευής. Στο Παράρτημα Α παρουσιάζεται ο κώδικας Matlab των προγραμμάτων του μοντέλου προσομοίωσης βάσει των οποίων εξάγονται τα αποτελέσματα του προηγούμενου κεφαλαίου.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επιβλέποντα της πτυχιακής μου εργασίας κ. Γεώργιο Ευθύμογλου, Αναπληρωτή Καθηγητή του τμήματος των Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά, για την αμέριστη βοήθεια και συμπαράσταση του καθώς και για το προσωπικό χρόνο, που αφιέρωσε για την διεκπεραίωση της παρούσας πτυχιακής εργασίας.

ΚΕΦΑΛΑΙΟ 1

ΑΣΥΡΜΑΤΑ ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

1.1 Ασύρματες επικοινωνίες και δίκτυα

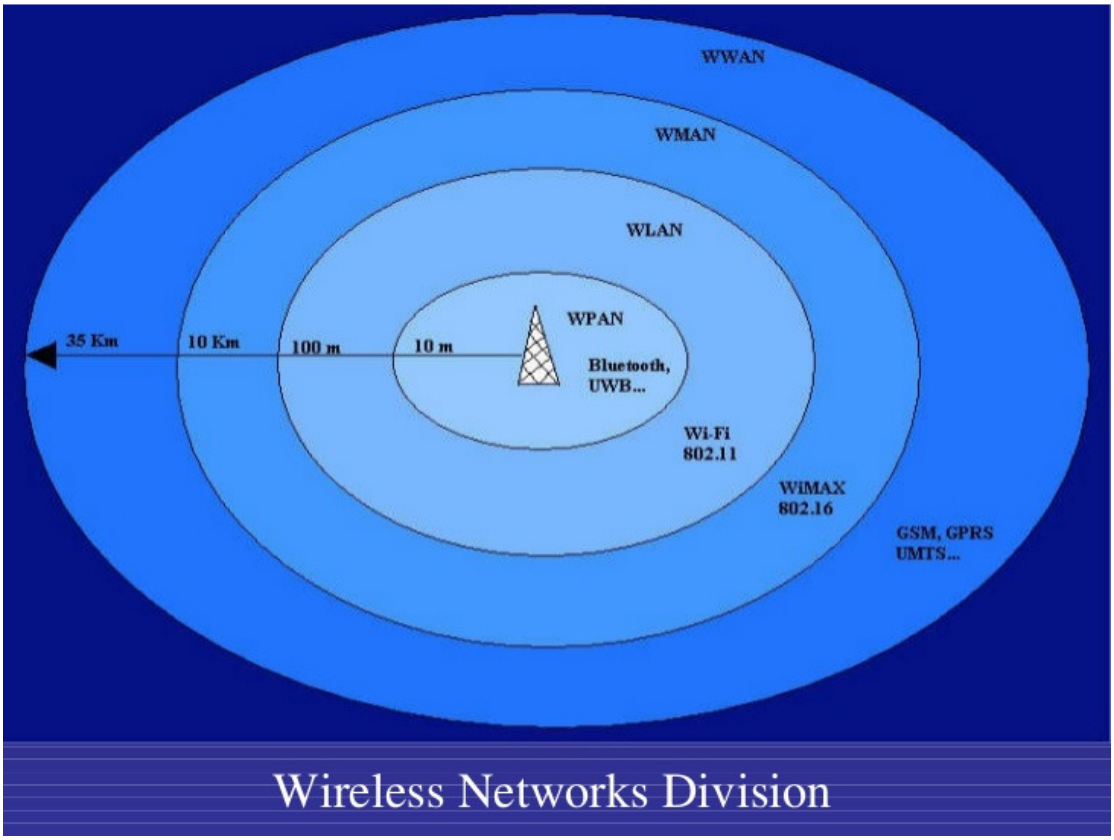
Ασύρματη επικοινωνία είναι η επικοινωνία μεταξύ δύο σημείων, ενός πομπού και ενός δέκτη, η οποία χρησιμοποιεί ραδιοκύματα ως μέσο για τη μετάδοση της πληροφορίας. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου.

Τα ασύρματα δίκτυα επικοινωνιών, όπως και τα ενσύρματα δίκτυα, μπορούν να ταξινομηθούν σε κατηγορίες, με βάση κυρίως το μέγεθός τους και την περιοχή κάλυψής τους, όπως παρακάτω (Σχήμα 1.1) [1].

- **Ασύρματα δίκτυ ευρείας περιοχής (Wireless Wide Area Networks – WWAN)**. Ο βασικός ρόλος αυτών των δικτύων είναι να παρέχουν διασύνδεση μεταξύ ηπείρων, παρέχοντας δυνατότητες μεταφοράς φωνής, τηλεοπτικού σήματος, υπηρεσίες εντοπισμού θέσης (π.χ. GPS) και διάφορες άλλες. Στα δίκτυα WWAN, μπορούμε να κατατάξουμε τα δορυφορικά δίκτυα, τα οποία καλύπτουν μια μεγάλη γεωγραφική περιοχή και εξυπηρετούν έναν μεγάλο αριθμό χρηστών.
- **Ασύρματα δίκτυα μητροπολιτικής περιοχής (Wireless Metropolitan Area Networks – WMAN)**. Αποτελούνται από την ασύρματη διασύνδεση σημείων τα οποία απέχουν πολύ μεταξύ τους. Τυπικά παραδείγματα μητροπολιτικών ασύρματων συνδέσεων είναι η σύνδεση δύο κτιρίων μιας εταιρείας στην ίδια πόλη, η διασύνδεση δύο σημείων σε διαφορετικές πόλεις, κ.λ.π.. Η βασική διαφορά με τα τοπικά ασύρματα δίκτυα είναι το υλικό το οποίο χρησιμοποιείται στη διασύνδεση, καθώς η διασύνδεση γίνεται μεταξύ δύο σημείων (**point-to-point**) και η απόσταση είναι μεγαλύτερη.
- **Ασύρματα δίκτυα τοπικής περιοχής (Wireless Local Area Networks – WLAN**. Είναι η πλέον διαδεδομένη κατηγορία. Ο βασικός λόγος ύπαρξης των δικτύων αυτών είναι η ασύρματη τοπική δικτύωση, και καλύπτουν μια μικρή γεωγραφική περιοχή η οποία μπορεί να είναι ένα εργαστήριο υπολογιστών, ένας όροφος, ένα συγκρότημα γραφείων, κ.λ.π.. Υπάρχουν διάφορες τοπολογίες στα ασύρματα τοπικά δίκτυα αναλόγως με τον τρόπο με τον οποίο πραγματοποιείται η

επικοινωνία αλλά οι σταθμοί εργασίας συνδέονται χρησιμοποιώντας ασύρματες κάρτες δικτύου σε κάποιο κεντρικό διανομέα, ο οποίος ονομάζεται **access point**.

- **Ασύρματα δίκτυα προσωπικής περιοχής (Wireless Personal Area Networks – WPAN ή απλώς PAN)**. Είναι μια νέα κατηγορία δικτύων που αναφέρεται στις σύγχρονες τεχνολογίες οι οποίες επιτρέπουν την ασύρματη διασύνδεση και επικοινωνία σε αποστάσεις λίγων μέτρων, φορητών προσωπικών συσκευών, όπως είναι τα ακουστικά, τα πληκτρολόγια, φωτογραφικές μηχανές, τα κινητά τηλέφωνα, τα PDA's και οι Ultra Mobile υπολογιστές. Η επικοινωνία αυτή επιτρέπει στις συσκευές αυτές υπηρεσίες όπως ανταλλαγή αρχείων, διαμοίραση εφαρμογών, άμεση επικοινωνία κ.λ.π.



Σχήμα 1.1 Κατηγορίες ασύρματων δικτύων

1.2 Ασύρματες κινητές επικοινωνίες

Τα ασύρματα συστήματα κινητών επικοινωνιών σχεδιάζονται με στόχο να επιτρέπουν την επικοινωνία του ανθρώπου που μετακινείται, με οποιονδήποτε συνδρομητή του ίδιου ή

διαφορετικού συστήματος, οπουδήποτε και αν βρίσκεται , οποιαδήποτε στιγμή, παρέχοντας υπηρεσίες πολυμέσων. Η τεράστια ανάπτυξη των κυψελωτών συστημάτων σε συνδυασμό με την μεγάλη ανάπτυξη των φορητών υπολογιστών, των tablets, και των έξυπνων τηλεφώνων αποτελούν μια ισχυρή ένδειξη για την ταχύτατη εξέλιξη των ασύρματων δικτύων στο μέλλον.

Στα δίκτυα σταθερών επικοινωνιών το σημείο πρόσβασης του κάθε χρήστη είναι σταθερό. Στα δίκτυα κινητών επικοινωνιών σε αντίθεση με τα δίκτυα σταθερών επικοινωνιών , το σημείο πρόσβασης του κάθε χρήστη δεν είναι σταθερό. Καθώς ο χρήστης μετακινείται το σημείο πρόσβασης του κινητού τερματικού στο δίκτυο αλλάζει από ένα σταθμό βάσης σε άλλο. Στα δίκτυα προσωπικών επικοινωνιών δεν υπάρχει μονοσήμαντη σχέση του χρήστη με ένα συγκεκριμένο τερματικό. Ο κάθε χρήστης μπορεί να χρησιμοποιεί διαφορετικό τερματικό κάθε φορά, είτε σταθερό είτε κινητό, και πάντοτε ο χρήστης συνοδεύεται με τον προσωπικό του τηλεπικοινωνιακό αριθμό (Personal telecommunication Number PTN) σε κάθε είδους τερματικό.

Υπάρχουν τρεις κύριες περιοχές εφαρμογών των ασύρματων κινητών επικοινωνιών, οι οποίες παρουσιάζουν μεγάλη ανάπτυξη και μεγάλο σχεδιαστικό και ερευνητικό ενδιαφέρον [2].

- Η ασύρματη πρόσβαση σε μεγάλα δίκτυα για προσωπικές επικοινωνίες χαμηλής κινητικότητας.
- Τα κυψελωτά δίκτυα κινητών επικοινωνιών (Cellular Networks) για προσωπικές επικοινωνίες υψηλών απαιτήσεων κινητικότητας.
- Τα ασύρματα τοπικά δίκτυα (Wireless Local Area Netwoks)

1.3 Ασύρματα Τοπικά Δίκτυα (Wireless Local Area Networks - WLAN)

Μέχρι πρόσφατα, τα ασύρματα τοπικά δίκτυα δεν είχαν μεγάλη ζήτηση. Μερικές από τις αιτίες ήταν το υψηλό κόστος, η χαμηλή χωρητικότητα μεταφοράς δεδομένων, η απαίτηση κατοχής ειδικής άδειας για τη μετάδοση σε συγκεκριμένες περιοχές συχνοτήτων, κλπ. Με την αντιμετώπιση όμως όλων αυτών των προβλημάτων και χάρη στα πλεονεκτήματα και τα ελάχιστα μειονεκτήματα έναντι των ενσύρματων λύσεων η δημοτικότητα της ασύρματης τοπικής δικτύωσης αυξήθηκε σημαντικά.

1.3.1 Βασική ιδέα WLAN

Ένα ασύρματο τοπικό δίκτυο (Wireless Local Area Network ή WLAN) αποτελεί ένα επικοινωνιακό σύστημα που δεν αποσκοπεί στην αντικατάσταση του κοινού ενσύρματου δικτύου (Ethernet). Αντιθέτως, λειτουργεί συμπληρωματικά ή εναλλακτικά, καθώς επιτρέπει την επέκταση της γεωγραφικής κάλυψης του προϋπάρχοντος δικτύου. Τα ασύρματα δίκτυα επιτρέπουν σε ηλεκτρονικές συσκευές (από υπολογιστές μέχρι video) να επικοινωνούν μεταξύ τους και να ανταλλάσσουν δεδομένα χωρίς την ύπαρξη καλωδίων. Όταν οι υπολογιστές βρίσκονται μακριά και ευρέως σε όλο το σπίτι, είναι δύσχρηστη η χρησιμοποίηση καλωδίων επάνω στα σκαλοπάτια ή η διάτρηση των τοίχων. Η εγκατάσταση ενσύρματου δικτύου σε κτήριο παρουσιάζει σημαντικές δυσκολίες, καθώς απαιτούνται το πέρασμα καλωδίων από τοίχους και άλλες μετατροπές από εξειδικευμένο προσωπικό. Τα ασύρματα δίκτυα προσφέρουν την λύση καθώς ο χρόνος εγκατάστασης είναι ελάχιστος ανεξάρτητα από την κτηριακή υποδομή.

Με αρχιτεκτονική παραπλήσια ενός ενσύρματου δικτύου και με το πλεονέκτημα της σύνδεσης του χρήστη ενώ βρίσκεται σε κίνηση, τα ασύρματα τοπικά δίκτυα καθιερώθηκαν γρήγορα σε μια πλειάδα εφαρμογών. Η πραγματική, όμως, έκρηξη της χρήσης των WLANs έχει προέλθει από την ολοένα αυξανόμενη παρουσία τους στο καθημερινό περιβάλλον εργασίας των επιχειρήσεων.

Τα ασύρματα τοπικά δίκτυα (Wireless Local Area Network, WLAN) έχουν σχεδιαστεί για να παρέχουν υψηλό ρυθμό μετάδοσης (αρκετά Mbps) και υψηλό εύρος ζώνης σε φορητά τερματικά, που μετακινούνται σε περιορισμένης έκτασης περιοχές. Επίσης σχεδιάζονται έτσι ώστε να μπορούν να υποστηρίζουν mobile computing σε μικρές περιοχές όπως κτίρια, πάρκα, αεροδρόμια, συγκροτήματα γραφείων, ή σε πανεπιστημιουπόλεις, νοσοκομειακούς χώρους, εμπορικά κέντρα κλπ.

Το ελκυστικότερο χαρακτηριστικό των WLAN είναι η ευελιξία τους. Μπορούν να επεκτείνουν την ασύρματη πρόσβαση σε τοπικά δίκτυα , όπως δίκτυα εταιρειών, καθώς επίσης να υποστηρίξουν ασύρματη πρόσβαση στο Internet με μεγάλες ταχύτητες σε τόπους όπου παρατηρείται υψηλή συγκέντρωση χρηστών (hot spots). Τα WLAN παρέχουν ταχεία και εύκολη ασύρματη σύνδεση σε υπολογιστές και συστήματα σε χώρους όπου δεν υπάρχει τηλεπικοινωνιακή υποδομή ή δεν επιτρέπεται εγκατάσταση τέτοιας υποδομής. Οι υπολογιστές μπορεί να είναι σταθεροί, φορητοί, επιπαλάμιοι ή ακόμα και προσαρμοσμένοι σε κινούμενα οχήματα

Σε γενικές γραμμές, τα ασύρματα δίκτυα είναι τουλάχιστον το ίδιο αξιόπιστα με τα ενσύρματα και πιο εύκολα στην αντιμετώπιση προβλημάτων. Όμως είναι ακόμα ευάλωτα στις παρεμβολές. Οι παρεμβολές αυτές μπορεί να προέρχονται από απλές ηλεκτρονικές ή ηλεκτρομηχανικές συσκευές.

Τα WLAN προσφέρουν κινητικότητα τερματικού μόνο σε περιορισμένο χώρο. Η απαίτηση για απεριόριστη κινητικότητα των τερματικών και ασύρματη επικοινωνία, προϋποθέτει ύπαρξη ραδιοδικτύου πλήρους κάλυψης και αυτός ήταν ο κύριος παράγοντας που συνετέλεσε στην ανάπτυξη της τεχνολογίας των κυψελωτών δικτύων κινητών επικοινωνιών. Τα δύο κύρια χαρακτηριστικά των κυψελωτών δικτύων είναι: [2]

- Η διαρκής παρακολούθηση και καταγραφή της τρέχουσας περιοχής που περιφέρεται ο χρήστης (περιοχή εντοπισμού, Location Area LA) για να καταστεί δυνατή η δρομολόγηση των εισερχόμενων κλήσεων
- Η διαπομπή της επικοινωνίας του κινητού τερματικού μεταξύ κυψελών, ώστε να μη διακόπτεται η επικοινωνία καθώς αυτό κινείται.

Ένα πεδίο εφαρμογών των WLAN είναι η εγκατάσταση περιστασιακών (Ad hoc) δικτύων, π.χ. σε μια συνεδρίαση ή σε άλλες θέσεις για προσωρινή χρήση. Οι σταθμοί που εμπλέκονται είναι δυνατόν να αποτελέσουν ένα αυτοδιαχειριζόμενο και δυναμικό δίκτυο, δηλαδή οι φορητοί υπολογιστές μπορεί ελεύθερα να μπαίνουν σε μια σύνοδο ή να βγαίνουν από αυτή. Το ad hoc δίκτυο μπορεί να εγκατασταθεί εύκολα και για το λόγο αυτό αποτελεί φθηνό μέσο για τοπική δικτύωση. Μια ομάδα από κινητούς χρήστες μπορεί να αποτελέσει ένα αυτόνομο τοπικό δίκτυο οπουδήποτε, οποιαδήποτε στιγμή, με αμελητέα προσπάθεια.

1.3.2 Τρόποι σύνδεσης

Σχετικά με τη δόμηση των δικτύων υπάρχουν **δύο κύριοι τρόποι σύνδεσης:**

- **Peer-to-Peer:** Χωρίς access point και χωρίς κεντρικό σημείο διαχείρισης. Δίκτυα τέτοιου τύπου είναι κατάλληλα για μικρές εταιρείες ή για οικιακή χρήση. Η καλυπτόμενη περιοχή (Basic Service Area ή BSA) καταλαμβάνει μια ακτίνα περίπου 100 μέτρων.
- **Infrastructure wireless network:** Περιλαμβάνει access point. Η πλειοψηφία των δικτύων στήνεται με AP, καθώς έτσι εξασφαλίζεται μεγαλύτερη ευελιξία στην εγκατάσταση και τη διαχείριση. Η καλυπτόμενη περιοχή εδώ εξαρτάται από την

εμβέλεια του εκάστοτε access point ή από την ύπαρξη περισσότερων του ενός σημείων πρόσβασης στον χώρο λειτουργίας (Extended Service Area ή ESA).

1.3.3 Μηχανισμός σύνδεσης

Σε όλα τα νέα πρότυπα ασύρματων δικτύων, εκτός από το πρότυπο IRDA (Infrared Data Association), το οποίο ούτως ή άλλως δεν αφορά ασύρματα δίκτυα αλλά ασύρματη επικοινωνία, δεν απαιτείται οπτική επαφή. Σε κάθε ασύρματο δίκτυο υπάρχουν δύο μέρη: Η ασύρματη κάρτα δικτύου (wireless LAN adapter), η οποία επικοινωνεί είτε με άλλες συσκευές που έχουν ασύρματη κάρτα δικτύου, είτε με τον πομποδέκτη-κόμβο (Access Point) που λειτουργεί και ως γέφυρα με το ενσύρματο δίκτυο. Τα AP (ACCESS POINT) είναι απλές συσκευές που συνδέονται με το ενσύρματο δίκτυο της εταιρείας, το ISP (Internet service provider ή το οικιακό δίκτυο. Ο ρόλος τους είναι η ασύρματη αποστολή και λήψη δεδομένων. Πρόκειται για ειδικές συσκευές, που διαθέτουν θύρα Ethernet και λειτουργούν κατά κάποιον τρόπο όπως τα hub, παρέχοντας όμως κάποιες επιπλέον δυνατότητες. Έχουν μεγαλύτερη ακτίνα δράσης από τις απλές ασύρματες κάρτες, επεκτείνοντας έτσι την εμβέλεια του ασύρματου δικτύου. Αυτό, με απλά λόγια σημαίνει ότι, αν δύο κόμβοι βρίσκονται έξω από την ακτίνα δράσης τους, είναι δυνατόν να επικοινωνήσουν μέσω του σημείου πρόσβασης. Επιπλέον, τα Access Points ελέγχουν την κίνηση του δικτύου, κατανέμουν ανάλογα με τον αριθμό των υπολογιστών το διαθέσιμο εύρος και φροντίζουν να κατευθύνουν τα πακέτα πληροφοριών. Για την εμβέλεια τους ισχύει ότι και για τις απλές ασύρματες κάρτες, ενώ ο αριθμός των κόμβων που μπορούν να "σηκώσουν" εξαρτάται από τον κατασκευαστή. Με τον τρόπο αυτό, και χωρίς τη χρήση καλωδίων, επιτυγχάνεται η διασύνδεση όλων των υπολογιστικών συστημάτων του χώρου.

Ο χρήστης πρέπει να έχει κάποια συσκευή που να διαθέτει κατάλληλη κάρτα (είτε εξωτερική, που θα τοποθετείται σε θύρα επέκτασης, είτε ενσωματωμένη στη συσκευή), η οποία θα επικοινωνεί με το access point. Με τον τρόπο αυτό, ο οποιοσδήποτε, φορητός ή σταθερός, υπολογιστής ή PDA (personal digital assistant) (υπολογιστής παλάμης ή ηλεκτρονική ατζέντα) θα μπορεί να μετατραπεί σε ασύρματο.

Η εμβέλεια των ασύρματων καρτών και συσκευών εξαρτάται από πολλές παραμέτρους: από την ποιότητα κατασκευής του προϊόντος (κυρίως από τον πομποδέκτη που ενσωματώνουν), από την τεχνολογία μετάδοσης που χρησιμοποιείται, από τον περιβάλλοντα χώρο και από την ταχύτητα μετάδοσης των δεδομένων. Οποιαδήποτε στιγμή

βρεθούν δύο ή περισσότεροι υπολογιστές στην ακτίνα δράσης των ασύρματων καρτών τους, αυτόματα συνθέτουν ένα ομότιμο δίκτυο (peer to peer). Αυτή είναι και η απλούστερη μορφή ενός ασύρματου δικτύου, η οποία εξυπηρετεί περιορισμένες ανάγκες και τη συναντάμε περισσότερο στα οικιακά δίκτυα ή σε μικρά δίκτυα στο γραφείο. Όλοι οι υπολογιστές σε ένα ομότιμο δίκτυο έχουν τα ίδια δικαιώματα και μοιράζονται εξίσου τους πόρους του δικτύου.

1.3.4 Πλεονεκτήματα ασύρματων τοπικών δικτύων WLANs

Τα βασικά πλεονεκτήματα που παρέχει ένα ασύρματο τοπικό δίκτυο προέρχονται από την φύση της ασύρματης τεχνολογίας, η οποία προσφέρει πολλές ευκολίες. Τα βασικότερα πλεονεκτήματα αυτών των δικτύων είναι: [2] [10]

- **Ευρυζωνικότητα.** Ένα καλά σχεδιασμένο δίκτυο επιτρέπει την πρόσβαση με μια φορητή συσκευή ασχέτως από την τοποθεσία του χρήστη. Επιπλέον οι τωρινές υλοποιήσεις των ασύρματων τεχνολογιών επιτρέπουν υψηλές ταχύτητες αλλά και τη συνύπαρξη πολλών τύπων δεδομένων, όπως streaming voice over ip και απλά δεδομένα δικτύου τα οποία συνυπάρχουν σε διαφορετικές ραδιοσυχνότητες.
- **Ευκολία υλοποίησης**. Το να υλοποιήσει κανείς ένα ασύρματο δίκτυο είναι πολύ πιο εύκολο και απλό από την παραδοσιακή υλοποίηση με καλωδίωση. Για παράδειγμα μπορεί να διασυνδέσει κάποιος δύο κτίρια χωρίς το κόστος της εγκατάστασης οπτικών ινών μεταξύ των κτιρίων. Μια ασύρματη συσκευή σε έναν όροφο μπορεί να προσφέρει πρόσβαση στο δίκτυο σε όλο τον όροφο χωρίς την επιβάρυνση της διερεύνησης προβλημάτων στην (πολύπλοκη πολλές φορές) καλωδίωση.
- **Χαμηλότερο κόστος επέκτασης**. Τα ασύρματα δίκτυα επιτρέπουν την γρήγορη, εύκολη και με μικρό κόστος επέκταση δικτύων σε περιοχές που είτε η καλωδίωση είναι πολύ δύσκολη να υλοποιηθεί, είτε η υπάρχουσα είναι πολύ δύσκολο να επεκταθεί. Μπορεί το αρχικό κόστος για τον εξοπλισμό ενός ασύρματου τοπικού δικτύου να είναι συγκριτικά ακριβότερο από αυτό ενός ενσύρματου, ωστόσο τα οφέλη είναι μακροπρόθεσμα. Αυτό συμβαίνει κυρίως σε περιπτώσεις δυναμικών χώρων εργασίας που απαιτούν συχνές αλλαγές, καθώς το κόστος επαναδιαμόρφωσης του προϋπάρχοντος ασύρματου δικτύου θα είναι αμελητέο.
- **Γρήγορη εγκατάσταση/τοποθέτηση**. Ένα ασύρματο δίκτυο μπορεί να χρησιμοποιηθεί σαν εργαλείο γρήγορης εγκατάστασης για ένα υποκατάστημα μιας εταιρείας ή απομακρυσμένης περιοχής. Εάν οι απαιτήσεις σε bandwidth δεν είναι

ιδιαίτερα υψηλές, μια ασύρματη συσκευή μπορεί να παρέχει δικτυακή διασύνδεση σε αρκετούς χρήστες χωρίς το χρόνο και τα έξοδα που χρειάζεται η καλωδίωση για να παρέχει τα ίδια σε κάθε χρήστη. Με την ασύρματη τεχνολογία η πρόσβαση στο δίκτυο μιας απομακρυσμένης περιοχής μπορεί να υλοποιηθεί σε ώρες αντί για μέρες. Ο εξοπλισμός που χρησιμοποιείται είναι εντελώς ακίνδυνος για τον ανθρώπινο οργανισμό. Η ακτινοβολία είναι μη ιονίζουσα και τα επίπεδα ακτινοβολίας είναι πολύ πιο χαμηλά από τα επιτρεπτά για τον ανθρώπινο οργανισμό όρια. Αρκεί να αναφέρουμε ότι μια ασύρματη κάρτα δικτύου (802.11b) ακτινοβολεί ισχύ 50 - 100 mwatt, ενώ ένα κινητό τηλέφωνο φτάνει και τα 2000 mwatt.

1.3.5 Μειονεκτήματα ασύρματων τοπικών δικτύων WLANs

Τα βασικότερα μειονεκτήματα των δικτύων WLANs είναι: [2] [10]

- **Ασφάλεια.** Καταρχάς, τα ασύρματα δίκτυα υστερούν στον τομέα παρεχόμενης ασφάλειας, καθώς υπάρχουν πολλοί τρόποι επίθεσης από επίδοξους εισβολείς. Ασφάλεια επένδυσης: Σήμερα είναι διαθέσιμο στην αγορά ένα μεγάλο εύρος λύσεων, αλλά μόνο λίγες από αυτές θα σημειώσουν εμπορική επιτυχία μεσαίου μεγέθους. Αν η ασφάλεια επένδυσης είναι πρωταρχικής σημασίας, η κατάσταση αυτή μπορεί να καθυστερήσει αποφάσεις για μελλοντικές επενδύσεις.
- **Παρεμβολές**. Τα ασύρματα τοπικά δίκτυα, κυρίως όσα βρίσκονται σε ζώνες χαμηλής συχνότητας, είναι ευάλωτα στις παρεμβολές. Τα ασύρματα LANs μεταφέρουν δεδομένα μέσω του αέρα. Σε αντίθεση με τα ενσύρματα δίκτυα, χρησιμοποιούν ένα κοινό μέσο, γνωστό ως διαμοιραζόμενο μέσο, με την αίσθηση ότι, όχι μόνο οι σταθμοί ενός καναλιού, αλλά και διαφορετικά κανάλια και τεχνολογίες έχουν πρόσβαση στο ίδιο, διαμοιραζόμενο μέσο. Οι τελευταίες ενδέχεται να οφείλονται στην ύπαρξη γειτονικών ηλεκτρονικών συσκευών, αλλά ακόμη και στην ίδια τη γεωμετρία του χώρου λειτουργίας.
- **Κατανομή συχνοτήτων.** Η λειτουργία ενός WLAN προϋποθέτει ότι όλοι οι χρήστες του εξυπηρετούνται από μια κοινή ζώνη συχνοτήτων. Οι ζώνες συχνοτήτων για συγκεκριμένες χρήσεις πρέπει να εγκρίνονται από κεντρική κρατική επιτροπή και να χορηγείται η σχετική άδεια, διαδικασία που είναι χρονοβόρα, λόγω της μεγάλης ζήτησης για το διαθέσιμο ασύρματο φάσμα συχνοτήτων.

- **Εμβέλεια.** Η εμβέλεια των ασύρματων συστημάτων είναι αρκετά περιορισμένη σε πολλές περιπτώσεις και η λειτουργικότητα που αναμένεται από τους χρήστες είτε δεν μπορεί να επιτευχθεί, ή μπορεί να επιτευχθεί σε περιορισμένη έκταση.
- **Ηλεκτρομαγνητική ακτινοβολία.** Αν και η ισχύς των κυμάτων που χρησιμοποιούνται από τα ασύρματα τοπικά δίκτυα είναι μόλις το 5% της ισχύος των σημάτων των κινητών τηλεφώνων, αυξάνεται η ηλεκτρομαγνητική επιβάρυνση του περιβάλλοντος.

1.4 Κυψελωτά συστήματα κινητών επικοινωνιών

Από το σύνολο των εξελίξεων στις επικοινωνίες δεδομένων και στις τηλεπικοινωνίες ίσως η πλέον επαναστατική είναι η ανάπτυξη των κυψελωτών δικτύων. Η κυψελωτή τεχνολογία είναι το θεμέλιο των κινητών ασύρματων επικοινωνιών και αποτελεί τη βασική τεχνολογία για τα κινητά τηλέφωνα, τα προσωπικά συστήματα επικοινωνιών, το ασύρματο Internet, τις ασύρματες δικτυακές εφαρμογές (Web) και άλλα [4].

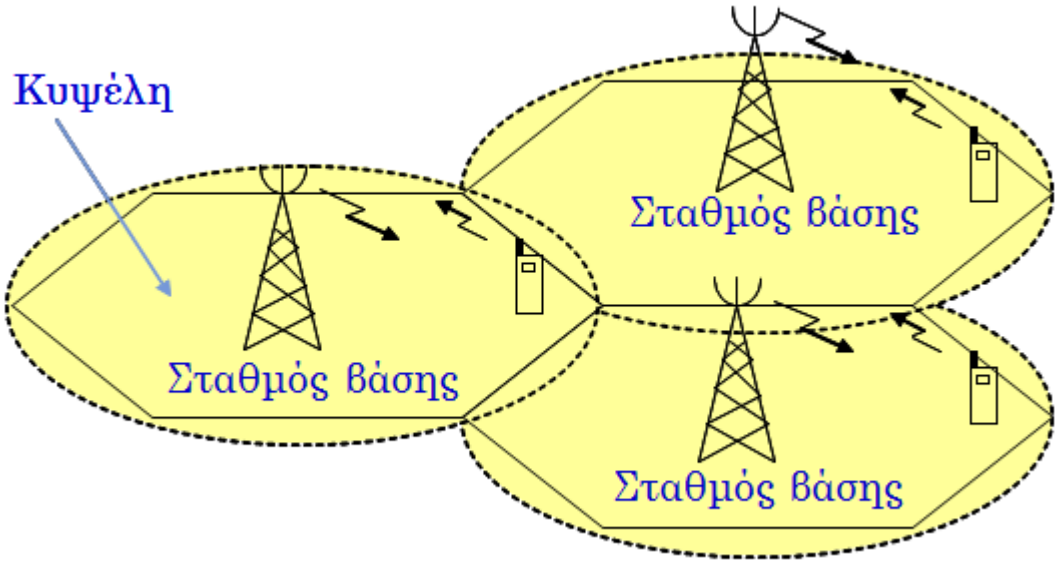
1.4.1 Έννοια Κυψέλης και Κυψελωτή Δομή

Οι βασικές αρχές των κυψελωτών συστημάτων πηγάζουν από την ανάγκη για την αποδοτική χρήση του φάσματος και τη δυνατότητα για εξυπηρέτηση μεγάλου αριθμού χρηστών. Η κυψελωτή δομή αποτέλεσε τη λύση του προβλήματος της συμφόρησης στο φάσμα συχνοτήτων και της χωρητικότητας χρηστών [3].

Πριν την εμφάνιση της κυψελωτής ασύρματης μετάδοσης η υπηρεσία κινητών ασύρματων τηλεφώνων παρέχονταν μόνο από ένα πομποδέκτη υψηλής ισχύος.

Η βασική ιδέα του κυψελωτού συστήματος είναι ο περιορισμός της εκπεμπόμενης ισχύος από τους Σταθμούς Βάσης, ώστε να περιοριστεί η έκταση της κάλυψης σε μια μικρή γεωγραφική περιοχή, που καλείται **κυψέλη (cell)**, καθώς και η επαναχρησιμοποίηση των συχνοτήτων ενός Σταθμού Βάσης από άλλο Σταθμό Βάσης, που βρίσκεται σε κάποια απόσταση. Κάθε κυψέλη έχει ένα Σταθμό Βάσης με πομποδέκτη περιορισμένης ισχύος και κεραίες, που επιτυγχάνουν την επιθυμητή κάλυψη στη γεωγραφική περιοχή. Με τον τρόπο αυτό χρησιμοποιούνται πολλαπλοί πομποδέκτες χαμηλής ισχύος σε αντικατάσταση ενός πομποδέκτη μεγάλης ισχύος (Σχήμα1.2).

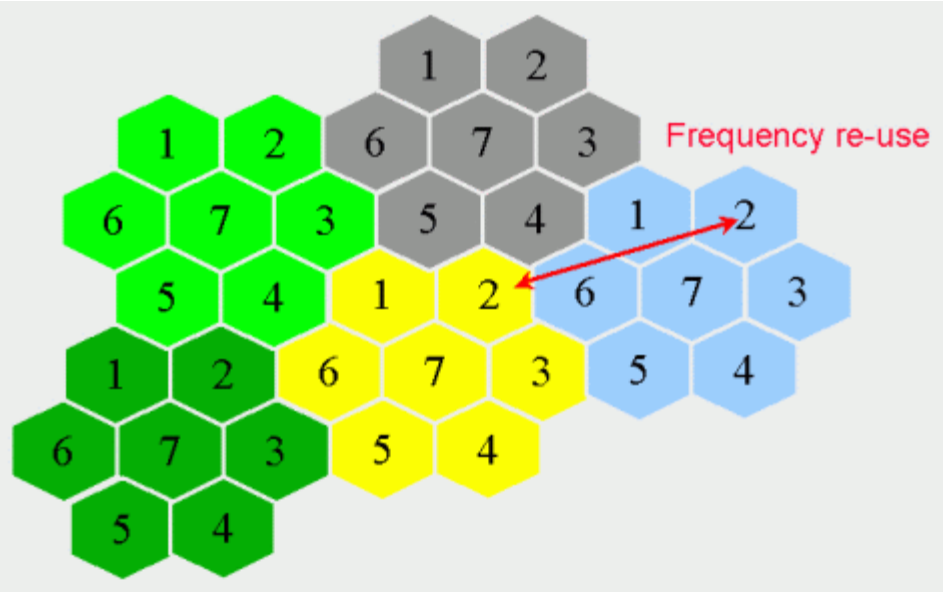
Ο συνολικός αριθμός των διαύλων που διατίθεται διαιρείται σε ομάδες. Στο σταθμό βάσης κάθε κυψέλης κατανέμεται μια ομάδα από το συνολικό αριθμό των ραδιοδιαύλων του συστήματος, η οποία ομάδα δεν χρησιμοποιείται σε γειτονικές κυψέλες. Σε γειτονικές κυψέλες κατανέμονται διαφορετικές ομάδες διαύλων. Οι κυψέλες διατάσσονται σε ομάδες. Το σύνολο των κυψελών που αθροιστικά χρησιμοποιούν το σύνολο των διαθέσιμων διαύλων αποτελεί μια ομάδα που ονομάζεται **συστάδα (cluster).** Ο αριθμός των κυψελών στο cluster καθορίζει πόσες διαφορετικές ομάδες διαύλων πρέπει να χρησιμοποιηθούν. Κανένας δίαυλος (κανάλι) δεν επαναχρησιμοποιείται μέσα σε μια συστάδα.



Σχήμα 1.2 Γεωγραφική κάλυψη κυψέλης

Κάθε κινητός σταθμός χρησιμοποιεί ένα ξεχωριστό κανάλι (δίαυλο) για να επικοινωνήσει με το σταθμό βάσης στην περιοχή της κυψέλης. Ο σταθμός βάσης επικοινωνεί ταυτόχρονα με πολλούς κινητούς σταθμούς χρησιμοποιώντας ένα κανάλι για κάθε κινητό. Για την επικοινωνία στις δύο κατευθύνσεις χρησιμοποιούνται δύο δίαυλοι (κανάλια).Το ένα κανάλι με κατεύθυνση από το σταθμό βάσης προς τον κινητό σταθμό ονομάζεται **ζεύξη καθόδου (down-link)**. Το άλλο κανάλι με κατεύθυνση από τον κινητό σταθμό προς το σταθμό βάσης ονομάζεται **ζεύξη ανόδου (up-link)**.

Στην περιοχή κάλυψης ενός κυψελωτού συστήματος, για να επιτευχθεί καλύτερη εκμετάλλευση του φάσματος που διατίθεται, επαναχρησιμοποιούνται ραδιοδίαυλοι της ίδιας συχνότητας σε διάφορες μη γειτονικές περιοχές. Αυτή η επαναχρησιμοποίηση διαύλων (συχνοτήτων)(frequency reuse) έχει ως αποτέλεσμα να υπάρχουν πολλές κυψέλες στην περιοχή εξυπηρέτησης του συστήματος οι οποίες χρησιμοποιούν την ίδια ομάδα συχνοτήτων. Οι κυψέλες αυτές ονομάζονται **ομοδιαυλικές (co-channel cells)**.



Σχήμα 1.3 Απεικόνηση συστάδων (με το ίδιο χρώμα) και ομοδιαυλικών κυψελών (με τον ίδιο αριθμό)

Στο σχήμα 1.3 απεικονίζονται οι συστάδες και η επαναχρησιμοποίηση των συχνοτήτων, όπου οι κυψέλες με το ίδιο χρώμα αποτελούν μια συστάδα με μέγεθος N=7 και οι κυψέλες με τον ίδιο αριθμό χρησιμοποιούν την ίδια ομάδα διαύλων (ομοδιαυλικές).

Ένα σημαντικό θέμα σε κυψελωτά δίκτυα είναι η κινητικότητα των χρηστών, η οποία δημιουργεί ένα σύνολο από προβλήματα τα οποία πρέπει να αντιμετωπιστούν. Το βασικότερο πρόβλημα που προκύπτει από την κινητικότητα των χρηστών είναι η ανάγκη για αλλαγή του χρησιμοποιούμενου ραδιοδιαύλου (καναλιού). Αν κατά τη μετάβαση ενός κινητού σταθμού (χρήστη) από μια κυψέλη σε άλλη ο κινητός σταθμός είναι σε αναμονή τότε υπάρχει περιοδική ανταλλαγή μηνυμάτων μεταξύ χρήστη και δικτύου ώστε να είναι γνωστή η θέση του χρήστη. Η διαδικασία αυτή ονομάζεται **περιαγωγή (roaming**). Αν κατά τη μετάβαση ενός κινητού σταθμού (χρήστη) από μια κυψέλη σε άλλη υπάρχει κλήση σε

εξέλιξη, τότε το δίκτυο φροντίζει για τη μεταφορά της κλήσης συνδέοντας τον χρήστη στη νέα κυψέλη. Η διαδικασία αυτή ονομάζεται **μεταπομπή ή διαπομπή (handoff ή handover)**. Η διαδικασία αυτή μπορεί να συμβεί ακόμη και μέσα στην ίδια κυψέλη, μεταφέροντας την κλήση σε ραδιοδίαυλο που έχει καλύτερη απόδοση από τον εξυπηρετούνται. Η μεταφορά της κλήσης γίνεται χωρίς διακοπή και χωρίς ο συνδρομητής να το αντιληφθεί.

Για τη σχεδίαση και ανάλυση των κυψελωτών συστημάτων το θεμελιώδες σχήμα των κυψελών θεωρείται το εξάγωνο, το οποίο σχήμα προσεγγίζει τον κύκλο, που είναι η ιδανική περιοχή ραδιοκάλυψης από την εκπεμπόμενη ισχύ. Σήμερα η τάση είναι να αναπτύσσονται νέου τύπου ετερογενή και ad hoc δίκτυα τα οποία χρησιμοποιούν κυψέλες διαφορετικής ακτίνας λόγω είτε της εκπεμπόμενης ισχύος, είτε του ύψους της κεραίας του Σταθμού Βάσης, είτε της διαφορετικής πυκνότητας των χρηστών. Αυτή η τάση οδηγεί σε ένα πολύ σημαντικό πρόβλημα που ονομάζεται παρεμβολή από άλλες κυψέλες (Other Cell Interference - OCI). Στις συνθήκες αυτές είναι δύσκολη η αξιολόγηση της επίδοσης του συστήματος με το απλό μοντέλο των εξαγωνικών κυψελών και απαιτούνται διαφορετικά μοντέλα ανάπτυξης του δικτύου.

1.4.2 Δομικά Στοιχεία Κυψελωτού Συστήματος Κινητών Επικοινωνιών

Τα βασικά δομικά στοιχεία ενός κυψελωτού συστήματος κινητών επικοινωνιών φαίνονται στο σχήμα 1.4 και είναι τα ακόλουθα [2] [3]:

MS ή UE ή MT (Mobile Station ή User Equipment ή Mobile Terminal) : Κινητός Σταθμός ή χρήστης συσκευής ή κινητό τερματικό. Είναι όλα τα τερματικά είτε χειρός είτε φορητά που χρησιμοποιεί ο κινούμενος χρήστης για πρόσβαση στο δίκτυο. Η ίδια συσκευή χρησιμοποιείται και για την πρόσβαση σε όλα τα συνδεδεμένα δίκτυα. Μια οντότητα που σχετίζεται με το κινητό τερματικό είναι η κάρτα ταυτότητας του χρήστη (συνδρομητή), SIM (Subscriber Identity Module), που εισάγεται μέσα στο τερματικό.

BTS ή BS (Base Transceiver Station) : Σταθμός Βάσης. Βρίσκεται στο κέντρο ή στα όρια της περιοχής κάλυψης και περιλαμβάνει τις κεραίες εκπομπής/λήψης και τους πομποδέκτες. Κάθε BTS εξυπηρετεί μια περιοχή που ονομάζεται κυψέλη (cell) η οποία και έχει δεδομένους ραδιοπόρους (ραδιοδιαύλους, κώδικες κλπ). Οι MS συνδέονται με τους BTSs χρησιμοποιώντας ραδιοδιαύλους και την αντίστοιχη ραδιοεπαφή. Με τον όρο **ραδιοεπαφή (air interface** ή **radio interface)** εννοούμε το σύνολο κανόνων που καθορίζουν πως γίνεται η πρόσβαση στο ραδιοδίαυλο.

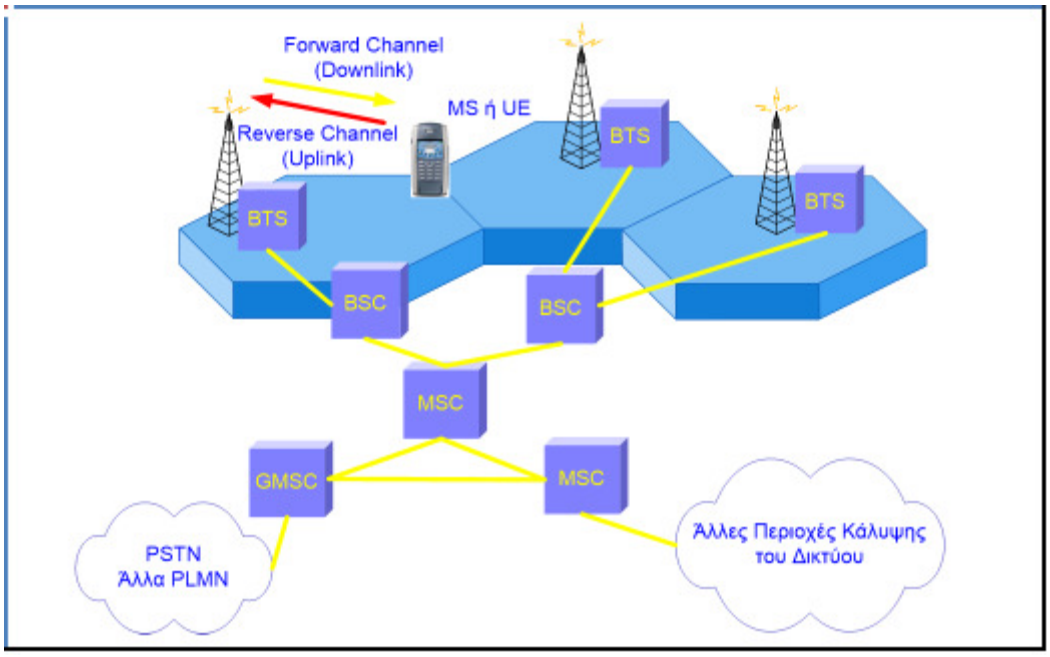
BSC (Base Station Controller): Ελεγκτής Σταθμών Βάσης. Έχει ως σκοπό τη διαχείρηση της ασύρματης διεπαφής μέσω εντολών προς τους σταθμούς βάσης και τους κινητούς σταθμούς (κινητά τερματικά). Ο BSC συνδέεται από τη μια πλευρά προς αρκετούς BTSs και από την άλλη προς ένα MSC.

MSC (Mobile Switching Centre) : Κέντρο μεταγωγής. Διαχειρίζεται και δρομολογεί τις κλήσεις από και προς τα κινητά τερματικά σε μια μεγάλη περιοχή εξυπηρέτησης. Το MSC

GMSC (Gateway Mobile Switching Centre) : Πύλη MSC. Είναι Το MSC που αναλαμβάνει τη διασύνδεση του δικτύου κινητών επικοινωνιών (Public Land Mobile Network - PLMN) με το σταθερό δίκτυο επικοινωνιών (Public Subscriber Telephone Network - PSTN).

Με βάση τα παραπάνω δομικά στοιχεία, το κυψελωτό δίκτυο κινητών επικοινωνιών μπορεί να διαιρεθεί σε τρία βασικά μέρη.

- Τον **κινητό σταθμό MS**
- Το **σύστημα πρόσβασης**, το οποίο περιλαμβάνει έναν ελεγκτή σταθμών βάσης BSC και τους σταθμούς βάσης BTS που ελέγχει.
- Το **δίκτυο κορμού**, το οποίο περιλαμβάνει τα κέντρα μεταγωγής κινητών επικοινωνιών MSC και τις πύλες των κέντρων μεταγωγής GMSC.



Σχήμα 1.4 Δομικά Στοιχεία Κυψελωτού Συστήματος Κινητών Επικοινωνιών

1.4.3 Τύποι Κυψελών

Τα δίκτυα κινητών επικοινωνιών παρέχουν κάλυψη σε περιοχές με διαφορετική συγκέντρωση χρηστών (κέντρο πόλης, προάστια, αγροτικές περιοχές, κτίρια, αυτοκινητοδρόμους κλπ). Η αύξηση χωρητικότητας επιτυγχάνεται με μείωση της εκπεμπόμενης ισχύος και άρα μείωση της ακτίνας κάλυψης. Οι διάφοροι τύποι των κυψελών που χρησιμοποιούνται για να καλύψουν τις ανάγκες της τηλεπικοινωνιακής κίνησης στα διάφορα περιβάλλοντα είναι τα εξής και απεικονίζονται στο Σχήμα 1.5 [3].

Macrocells (Μακροκυψέλες). Είναι κυψέλες με μεγάλη ακτίνα μέχρι μερικές δεκάδες χιλιόμετρα. Οι Σταθμοί βάσης τοποθετούνται σε ψηλά κτήρια ή πύργους με καλή ορατότητα κάλυψης. Χρησιμοποιούνται για την ραδιοκάλυψη ευρύτερων γεωγραφικών περιοχών με μέση ή μικρή πυκνότητα αριθμού χρηστών και μεγάλη κινητικότητα (π.χ. αγροτικές περιοχές, αυτοκινητόδρομοι).

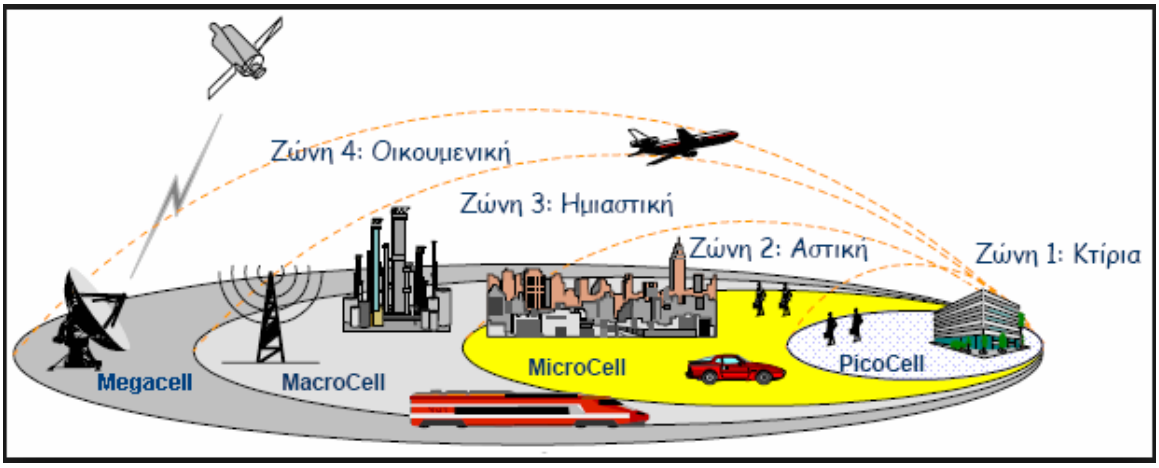
Microcells (Μικροκυψέλες). Είναι κυψέλες με ακτίνα συνήθως μέχρι 1-2 χιλιόμετρα. Χρησιμοποιούνται για να ικανοποιήσουν τις απαιτήσεις εξυπηρέτησης περιοχών που εμφανίζουν μεγάλη συγκέντρωση χρηστών (π.χ. πυκνοκατοικημένες περιοχές, εμπορικά κέντρα, σιδηροδρομικούς σταθμούς). ΟΙ Σταθμοί βάσης τοποθετούνται σε στέγες κτηρίων.

Ρicocells (Πικοκυψέλες). Είναι κυψέλες με μικρή ακτίνα συνήθως μέχρι 100-200 μέτρα. Χρησιμοποιούνται για κάλυψη περιοχών με μεγάλες απαιτήσεις σε τηλεπικοινωνιακή κίνηση (π.χ. hot spots, εμπορικά κέντρα, σιδηροδρομικούς σταθμού, δωμάτια). ΟΙ Σταθμοί βάσης τοποθετούνται σε χαμηλά ύψη (συνήθως κάτω από 4 μέτρα). Οι πικοκυψέλες έχουν τη δυνατότητα υποστήριξης ευρυζωνικών υπηρεσιών.

Femtocells. Είναι κυψέλες με πολύ μικρή ακτίνα συνήθως 10 μέτρα. Οι κυψέλες αυτές καλύπτουν πολύ μικρές περιοχές, αντίστοιχες των Access Points των WiFi (σπίτια, μικρές επιχειρήσεις). Υποστηρίζονται από μικρούς, χαμηλού κόστους και με χαμηλή εκπεμπόμενη ισχύ BSs, οι οποίοι εγκαθίστανται από τους τελικούς καταναλωτές και οι οποίοι είναι συνδεδεμένοι στο δίκτυο κορμού είτε μέσω ευζωνικών DSL γραμμών είτε μέσω άλλου τύπου ασύρματων ευρυζωνικών συνδέσεων. Οι σταθμοί βάσης μοιάζουν με τα Access Points των WiFi αλλά σε αντίθεση με αυτά μπορούν να χρησιμοποιήσουν τεχνολογίες ραδιοπρόσβασης κυψελωτών συστημάτων καθώς και διαφορετικές περιοχές του φάσματος. Θεωρούνται ένας οικονομικός και αποδοτικός τρόπος για να απαλλάξουν το δίκτυο των μακροκυψελών από την αυξημένη τηλεπικοινωνιακή κίνηση. Υπάρχουν σημαντικές τεχνικές προκλήσεις με την ανάπτυξη των femtocells όπως η διαχείρηση των

παρεμβολών, η αντιστοίχηση των χρηστών στις υπάρχουσες κυψέλες, η διαχείρηση της κινητικότητας των χρηστών και των μεταπομπών και η ανάπτυξη **αυτο-οργανούμενων δικτύων (Self-Organizing Networks - SON)**.

Megacells Η κατηγορία αυτή των κυψελών είναι για τα δορυφορικά συστήματα και καλύπτει μεγάλες γεωγραφικές περιοχές.



Σχήμα 1.5 Τύποι κυψελών

1.4.4 Συστήματα ιεραρχημένων κυψελών

Κατά την ανάπτυξη των κυψελωτών συστημάτων και προκειμένου να γίνει εκμετάλλευση των πλεονεκτημάτων όλων των τύπων των κυψελών, σχεδιάστηκαν δίκτυα με ιεραρχική δομή κυψελών, δηλαδή με επικάλυψη διαφορετικών τύπων κυψελών. Έτσι προκύπτουν δύο τύποι συστημάτων ιεραρχημένων κυψελών [3].

Τα **συστήματα χαμηλής βαθμίδας ιεράρχησης (Low Tier Systems)**, όπου συνδυάζονται Picocells και Microcells.

Τα **συστήματα υψηλής βαθμίδας ιεράρχησης (High Tier Systems)**, όπου συνδυάζονται Microcells και Macrocells.

Τα χαμηλής βαθμίδας συστήματα χρησιμοποιούνται για την κάλυψη μικρών περιοχών με πεζούς χρήστες, ενώ τα υψηλής βαθμίδας υποστηρίζουν και χρήστες κινούμενους με υψηλές ταχύτητες.

Τα τελευταία χρόνια που υπάρχει μια συνεχώς αυξανόμενη χρήση των femtocells, δημιουργούνται δίκτυα ιεραρχικά δομημένα με macrocells και femtocells τα οποία βέβαια είναι τυχαία τοποθετημένα στο χώρο των macrocells. Ένα από τα σημαντικά προβλήματα

σε αυτές τις δομές είναι η παρεμβολή μεταξύ διαφορετικών επιπέδων ιεραρχίας (cross tier interference), δηλαδή μεταξύ των χρηστών που συνδέονται με femtocells και των Σταθμών Βάσης των macrocells. Η παρεμβολή προκύπτει γιατί σε αυτή τη μορφή ιεραρχικής δομής γίνεται χρήση κοινών ραδιοπόρων από femtocells και macrocells.

1.4.5 Παρεμβολές

Ένα σημαντικό χαρακτηριστικό της ασύρματης διάδοσης είναι η παρουσία παρεμβολών, που αποτελεί το σημαντικότερο παράγοντα περιορισμού της χωρητικότητας των συστημάτων κινητών επικοινωνιών και επομένως των κυψελωτών δικτύων. Οι κυριότερες παρεμβολές που εμφανίζονται στα κυψελωτά συστήματα και οι οποίες καθορίζουν κατά συνέπεια τον παράγοντα επαναχρησιμοποίησης συχνοτήτων είναι [3]:

Co-channel interference (ομοδιαυλικές παρεμβολές). Είναι οι παρεμβολές που προέρχονται από ομοδιαυλικές κυψέλες και είναι οι αμοιβαίες παρεμβολές διαύλων της ίδιας συχνότητας, οι οποίοι λειτουργούν σε διαφορετικές θέσεις στην περιοχή κάλυψης του κυψελωτού συστήματος. Δηλαδή όταν χρησιμοποιείται το ίδιο κανάλι σε διαφορετικές κυψέλες στα πλαίσια επαναχρησιμοποίησης των διαύλων (συχνοτήτων). Με κατάλληλη σχεδίαση, προσδιορίζεται η ικανή απόσταση μεταξύ των κυψελών που χρησιμοποιούν διαύλους της ίδιας συχνότητας, ώστε να εξασφαλίζεται το επίπεδο των ομοδιαυλικών παρεμβολών σε ανεκτά όρια.

Adjacent-channel interference (παρεμβολές γειτονικών διαύλων). Είναι οι παρεμβολές που προέρχονται από γειτονικά κανάλια και συνήθως οφείλεται σε προβληματικά φίλτρα του δέκτη. Δηλαδή όταν χρησιμοποιούνται γειτονικά κανάλια στην ίδια κυψέλη. Οι παρεμβολές γειτονικών διαύλων περιορίζονται τόσο με τη χρήση ικανοποιητικών φίλτρων, όσο και με την προσεκτική απόδοση των συχνοτήτων στους Σταθμούς Βάσης.

Οι κυψελωτές ροδιοζεύξεις συνήθως παρουσιάζουν το φαινόμενο του **κατωφλίου (threshold effect)**, δηλαδή η ποιότητα της ζεύξης είναι αποδεκτή όταν ο μέσος λαμβανόμενος λόγος ισχύος φέροντος προς θόρυβο C/N και ο μέσος λόγος ισχύος φέροντος προς παρεμβολή C/I υπερβαίνουν συγκεκριμένες τιμές κατωφλίου. Για γρήγορα κινούμενους σταθμούς οι απώλειες διάδοσης και η σκίαση καθορίζουν την ποιότητα ζεύξης για δεδομένες τιμές κατωφλίου C/N και C/I. Όταν η ταχύτητα κίνησης είναι μικρή, τότε η ποιότητα της ζεύξης μπορεί να γίνει μη αποδεκτή, όταν ο δίαυλος παρουσιάζει ισχυρές διαλείψεις.

1.4.6 Επαναχρησιμοποίηση συχνοτήτων

Ας υποθέσουμε ότι η συνολική ζώνη συχνοτήτων που διατίθεται για ένα κυψελωτό σύστημα είναι B Hz, και ότι κάθε ημι-αμφίδρομο (half-duplex) κανάλι απαιτεί W Hz, τότε ο αριθμός των πλήρως-αμφίδρομων (full-duplex) καναλιών S που η συνολική ζώνη υποστηρίζει (ένα κανάλι για εκπομπή και ένα για λήψη) είναι S=B/2W [2].

Έστω ότι ο συνολικός αριθμός των full-duplex καναλιών μοιράζεται εξίσου μεταξύ N κυψελών, οι οποίες αποτελούν μια ομάδα - συστάδα (cluster) (σε ένα σύστημα N-κυψελών επαναχρησιμοποίησης συχνοτήτων χωρίς να δημιουργούνται παρεμβολές), τότε ο συνολικός αριθμός των καναλιών κ που αποδίδεται σε κάθε κυψέλη είναι κ=S/N. Αν αυτή η συστάδα επαναλαμβάνεται M φορές μέσα στην περιοχή κάλυψης του συστήματος, δηλαδή M είναι το πλήθος των συστάδων, αυτό δίνει ένα συνολικό αριθμό full-duplex καναλιών C στην περιοχή κάλυψης ίσο με C=MkN=MS (S=kN), όπου C αντιπροσωπεύει την χωρητικότητα του κυψελωτού συστήματος. Το N που αντιπροσωπεύει το μέγεθος του cluster (ή το 1/N σύμφωνα με άλλους) ονομάζεται **συντελεστής επαναχρησιμοποίησης συχνότητας (frequency reuse factor)** (και τυπικά είναι ίσος με 3, 4, 7, 9, 12).

Η απόσταση επαναχρησιμοποίησης συχνότητας D, είναι η ελάχιστη απόσταση των κέντρων δύο κυψελών που χρησιμοποιούν την ίδια ζώνη συχνοτήτων (ομοδιαυλικές κυψέλες) και είναι ίση με D=R*sqrt(3N), όπου R είναι η ακτίνα της κυψέλης και N το μέγεθος της συστάδας. Ο λόγος D/R=sqrt(3N) καλείται **λόγος ομοδιαυλικής παρεμβολής (co-channel reuse ratio)**. Όσο αυξάνει το N, αυξάνει και το D και συνεπώς μειώνεται η πιθανότητα για ομοδιαυλική παρεμβολή. Για το λόγο αυτό ο **λόγος D/R καλείται και συντελεστής μείωσης ομοδιαυλικής παρεμβολής (co-channel interference reduction factor)** [3].

ΚΕΦΑΛΑΙΟ 2

ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ

2.1 Ad-Hoc Δίκτυα

Η έρευνα για τα ασύρματα ad-hoc δίκτυα βρίσκεται σε εξέλιξη εδώ και δεκαετίες. Η ιστορία των ad-hoc δικτύων, μπορεί να αναζητηθεί πίσω στα ραδιοφωνικά δίκτυα πακέτων της Υπηρεσίας Προηγμένων Ερευνητικών Έργων Άμυνας (**Defense Advanced Research Projects Agency, DARPA)**, τα οποία εξελίχθηκαν στο προσαρμοστικό πρόγραμμα ραδιοφωνικών δικτύων **survivable adaptive (SURAD**). Τα ad-hocδίκτυα παίζουν σημαντικό ρόλο στις στρατιωτικές εφαρμογές και τις σχετικές ερευνητικές προσπάθειες.

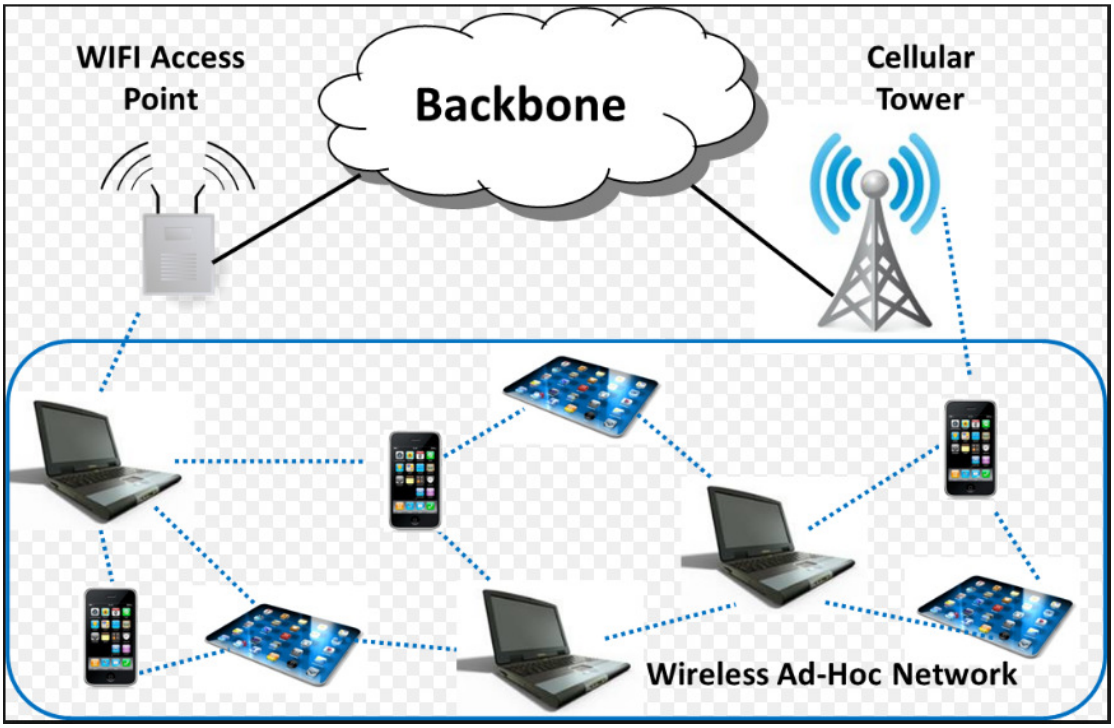
2.1.1 Αρχιτεκτονική ad hoc δικτύων

Ένα ad hoc δίκτυο είναι μία συλλογή αυτόνομων κόμβων που δεν στηρίζονται σε μία προκαθορισμένη δομή για να κρατάει το δίκτυο σε συνοχή. Οι κόμβοι επικοινωνούν μεταξύ τους χρησιμοποιώντας ασύρματη επικοινωνία. Μπορούν να διαμορφώνονται να συγχωνεύονται ή να διαχωρίζονται σε διαφορετικά δίκτυα χωρίς να στηρίζονται σε κάποια σταθερή υποδομή. Το ad hoc δίκτυο είναι ετερογενές (heterogeneous), δηλαδή δεν αποτελείται από έναν τύπο συσκευών, αλλά μπορεί να αποτελείται από ένα σύνολο διαφορετικών συσκευών όπως, PDA, κινητών τηλεφώνων, φορητών υπολογιστών κτλ., τα οποία πρέπει να έχουν δυνατότητα ασύρματης επικοινωνίας μεταξύ τους [2] [7]. Στο Σχήμα 2.1 απεικονίζεται ένα τυπικό ασύρματο Ad Hoc δίκτυο. Ένα ad hoc δίκτυο που αποτελείται από κινητούς κόμβους ονομάζεται **MANET (Mobile Ad hoc Network)**.

Τα δίκτυα ad-hoc εντάσσονται σε μια ευρύτερη κατηγορία δικτύων **(Distributed Transient Network)** η οποία ορίζεται σαν τα δίκτυα αυτά τα οποία είναι εν γένει αποκεντρωμένα και αποτελούνται κυρίως από κόμβους τα οποία δεν ανήκουν εξ ορισμού και διαρκώς στο δίκτυο αλλά έχουν την δυνατότητα να εισέρχονται ή να αποχωρούν από το δίκτυο οποιαδήποτε στιγμή και από οποιοδήποτε σημείο του.

Τα ad hoc δίκτυα επιτρέπουν την εύκολη ανάπτυξη και λειτουργία τους σε πολύ σύντομο χρονικό διάστημα χωρίς να είναι απαραίτητη η χρήση εξειδικευμένων εφαρμογών και η εκτέλεση διαχειριστικών λειτουργιών ή άλλων ενεργειών από τους χρήστες. Ένα άλλο πλεονέκτημα είναι το γεγονός ότι δεν απαιτείται η χρήση σταθερών δικτυακών υποδομών για τη λειτουργία του δικτύου ενώ η τοπολογία του δικτύου μπορεί να είναι δυναμική.

Η ασύρματη επικοινωνία επιτρέπει τη μεταφορά πληροφοριών μεταξύ ενός δικτύου αποσυνδεδεμένων και συχνά κινητών χρηστών. Τα δημοφιλή ασύρματα δίκτυα, όπως τα δίκτυα κινητής τηλεφωνίας και τα ασύρματα LANs είναι παραδοσιακά βασισμένα σε υποδομή, δηλ. οι σταθμοί βάσεως, τα σημεία πρόσβασης και οι κεντρικοί υπολογιστές (servers) αναπτύσσονται (παίρνουν συγκεκριμένες θέσεις) προτού να μπορέσει να χρησιμοποιηθεί το δίκτυο. Αντίθετα, τα δίκτυα ad hoc, διαμορφώνονται δυναμικά μεταξύ μιας ομάδας ασύρματων χρηστών και δεν απαιτούν καμία υπάρχουσα υποδομή ή προ-διαμόρφωση.

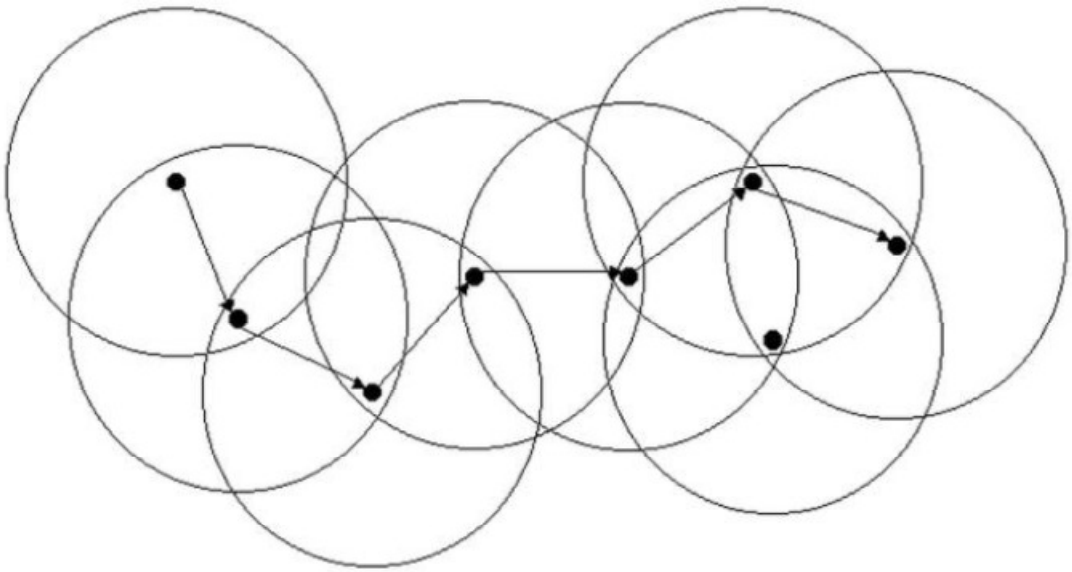


Σχήμα 2.1 Αρχιτεκτονική Ad hoc δικτύου.

Τα ασύρματα ad hoc δίκτυα διαμορφώνονται από ένα σύνολο host που επικοινωνούν ο ένας με τον άλλον πέρα από ένα ασύρματο κανάλι. Το δίκτυο που διαμορφώνεται χωρίς οποιαδήποτε κεντρική διοίκηση, αποτελείται από κινητούς κόμβους που χρησιμοποιούν μια ασύρματη διεπαφή για να στείλουν τα πακέτα. Χαρακτηρίζονται από τον αυτόνομο τρόπο λειτουργίας του κάθε κόμβου και την έλλειψη σταθερής υποδομής δικτύου κορμού. Κάθε κόμβος έχει τη δυνατότητα να επικοινωνήσει άμεσα με έναν άλλο κόμβο (ή αρκετούς από τους) στη φυσική γειτονιά του. Λειτουργούν με αυτοδιοργάνωση και αποκεντρωμένο τρόπο και η επικοινωνία μηνυμάτων πραγματοποιείται μέσω της διάδοσης **multi-hop**. Αυτό

σημαίνει ότι οποιοδήποτε πακέτο που στέλνεται από έναν κόμβο σε έναν άλλο μπορεί να περάσει μέσω διάφορων ενδιάμεσων κόμβων που ενεργούν ως δρομολογητές.

Ένα ad hoc δίκτυο τείνει να χαρακτηρίσει μια μικρή ομάδα συσκευών όλα στην πολύ στενή εγγύτητα το ένα με το άλλο. Βασικός περιορισμός είναι προκειμένου να γίνει επικοινωνία μεταξύ δύο σταθμών, είναι να βρίσκεται ο ένας εντός της εμβέλειας του άλλου. Σε αυτό τον τρόπο λειτουργίας μία συσκευή που θέλει να εκπέμψει, ελέγχει καταρχήν αν η ραδιοσυχνότητα είναι ελεύθερη. Αν είναι καταλυμένη περιμένει για κάποιο χρονικό διάστημα να ελευθερωθεί. Όταν βρει την ευκαιρία δοκιμάζει να εκπέμψει στέλνοντας πακέτα που περιέχουν την πληροφορία προς μετάδοση και επιπρόσθετη πληροφορία, όπως η διεύθυνση του παραλήπτη. Τα εκπεμπόμενα πακέτα τα ακούνε όλοι οι υπόλοιποι ασύρματοι σταθμοί. Αυτός που αναγνωρίζει τη δική του διεύθυνση σαν διεύθυνση παραλήπτη, παραλαμβάνει και επεξεργάζεται τα λαμβανόμενα πακέτα, οι υπόλοιποι απλά τα αγνοούν.



Σχήμα 2.2 Ακτίνα κάλυψης Ad hoc δικτύου

Σε κάθε αδόμητο δίκτυο σημαντικό ρόλο διαδραματίζει η ακτίνα μετάδοσης κάθε κόμβου. Συγκεκριμένα, όσο μεγαλύτερη είναι η ακτίνα μετάδοσης των κόμβων, τόσο μικρότερος θα είναι ο μέσος αριθμός μεταδόσεων που θα απαιτείται για την αποστολή ενός πακέτου από ένα κόμβο σε κάποιον άλλο. Επίσης η μικρή ακτίνα εκπομπής των κόμβων μειώνει την πιθανότητα συγκρούσεων, καθώς και τις παρεμβολές μεταξύ των κόμβων. Με άλλα λόγια,

όσο μικρότερη είναι η ακτίνα εκπομπής, τόσο περισσότερες μεταδόσεις θα μπορούν να πραγματοποιούνται ταυτόχρονα. Επιπρόσθετα, η ακτίνα μετάδοσης παίζει καθοριστικό ρόλο και στην κατανάλωση ενέργειας κάθε κόμβου, η οποία είναι μια πολύ σημαντική παράμετρος στα περισσότερα αδόμητα δίκτυα. Έτσι, η ακτίνα μετάδοσης θα πρέπει να επιλέγεται όσο το δυνατό μικρότερη, φροντίζοντας όμως ταυτόχρονα να μην είναι τόσο μικρή ώστε το δίκτυο να παύει να είναι συνεκτικό (Σχήμα 2.2).

2.2 Κατηγορίες ad hoc δικτύων

Τα ad hoc δίκτυα μπορούν να ταξινομηθούν σε 2 κατηγορίες με βάση την κινητικότητα των κόμβων: Στα **στατικά** και στα **κινητά.** Στα στατικά δίκτυα οι κόμβοι από τη στιγμή που εισέρχονται στο δίκτυο, συνήθως δε μετακινούνται. Παράδειγμα αυτής της κατηγορίας αποτελούν τα δίκτυα που σχηματίζονται μεταξύ κεραιών που βρίσκονται στις οροφές κτηρίων. Αντίθετα στα κινητά ad hoc δίκτυα (**Mobile Ad hoc Networks – MANET**), οι κόμβοι μπορούν να κινούνται προς οποιαδήποτε κατεύθυνση.

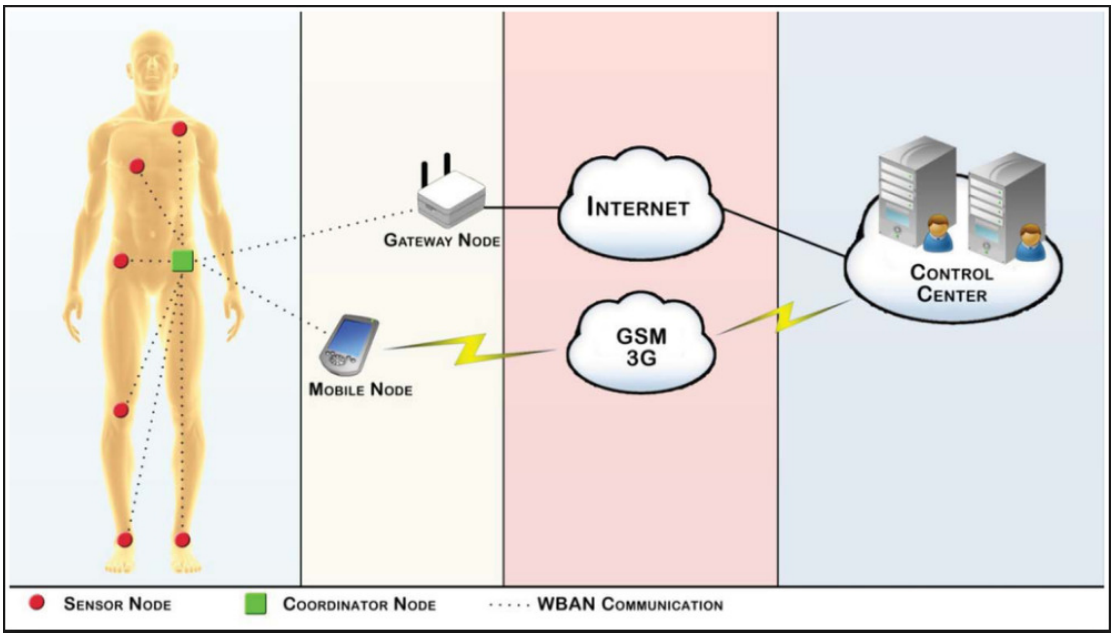
Μία ειδική κατηγορία δικτύων που χρησιμοποιούν ad hoc τεχνολογία είναι τα δίκτυα σώματος (BAN) και τα προσωπικά δίκτυα(PAN).

2.3 Δίκτυα Σώματος (Body area network - BAN)

Ένα δίκτυο περιοχής σώματος (BAN), που αναφέρεται επίσης ως ένα ασύρματο δίκτυο περιοχής σώματος (WBAN) ή ως ένα δίκτυο αισθητήρων σώματος (body sensor network, BSN), είναι ένα ασύρματο δίκτυο που σχετίζονται με ηλεκτρονικές συσκευές οι οποίες μπορούν να φορεθούν. Οι συσκευές ενός τέτοιου συστήματος μπορεί να είναι ενσωματωμένες στο εσωτερικό του σώματος, εμφυτεύματα, μπορεί να είναι επιφανειακά τοποθετημένες στο σώμα σε μια σταθερή θέση ή μπορεί να είναι συσκευές που οι άνθρωποι μπορούν να μεταφέρουν σε διαφορετικές θέσεις, σε ρούχα τσέπες, με το χέρι ή σε διάφορες σακούλες. Ένα BAN παρέχει σύνδεση αυτών των μονάδων αισθητήρων σώματος (body sensor units, BSUs) μαζί με μία κεντρική μονάδα σώματος (body central unit, BCU). Στο Σχήμα 2.3 απεικονίζεται η φιλοσοφία της αρχιτεκτονικής ενός WBAN [5] [6].

Η ανάπτυξη της τεχνολογίας WBAN ξεκίνησε περίπου το 1995 γύρω από την ιδέα της χρήσης των τεχνολογιών του ασύρματου προσωπικού δικτύου (WPAN) για την εφαρμογή

επικοινωνιών σχετικά με, κοντά και γύρω από το ανθρώπινο σώμα. Ένα σύστημα WBAN μπορεί να χρησιμοποιήσει WPAN ασύρματες τεχνολογίες ως πύλες για να φτάσει σε μεγαλύτερες αποστάσεις. Μέσω των συσκευών πύλης, είναι δυνατό να συνδεθούν οι φορητές συσκευές στο ανθρώπινο σώμα με το διαδίκτυο. Με αυτό τον τρόπο, το ιατρικό προσωπικό μπορεί να έχει πρόσβαση στα δεδομένα των ασθενών σε απευθείας σύνδεσης, ή χρησιμοποιώντας το διαδίκτυο ανεξάρτητα από τη θέσης του ασθενούς.



Σχήμα 2.3 Ασύρματο δίκτυο σώματος WBAN.

Η ακτίνα μετάδοσης ενός BAN αντιστοιχεί στην έκταση του ανθρώπινου σώματος (για παράδειγμα μπορεί να είναι 1-2 μέτρα). Καθώς η καλωδίωση ενός σώματος είναι μία δύσκολη διαδικασία, οι ασύρματες τεχνολογίες αποτελούν την καλύτερη λύση για την διασύνδεση αυτού του τύπου συσκευών (που έχουν την δυνατότητα να φορεθούν).

2.4 Ασύρματα προσωπικά δίκτυα (Wireless personal area network -WPAN)

Τα Ασύρματα προσωπικά δίκτυα (Wireless personal area network -WPAN) έχουν στόχο την ασύρματη δικτύωση φορητών υπολογιστών, κινητών υπολογιστικών μανάδων όπως τα PDA (Personal Digital Assistants), περιφεριακών, κυψελωτών και έξυπνων τηλεφώνων, και άλλων ηλεκτρονικών συσκευών, που βρίσκονται σε μικρές αποστάσεις μεταξύ τους, μέχρι

10 μέτρα περίπου. Οι ασύρματες συσκευές μπορεί να έχουν ασύρματη συνδεσμολογία μεταξύ τους με βάση τις προδιαγραφές Bluetooth. Τα PAN έχουν τοπολογία ad hoc, υποστηρίζουν συσκευές φωνής και δεδομένων και μικρή κατανάλωση ισχύος. Οι συσκευές που χρησιμοποιούν τεχνολογία Bluetooth, αποτελούν ένα ad hoc δίκτυο , που καλείται και piconet [2] [7].

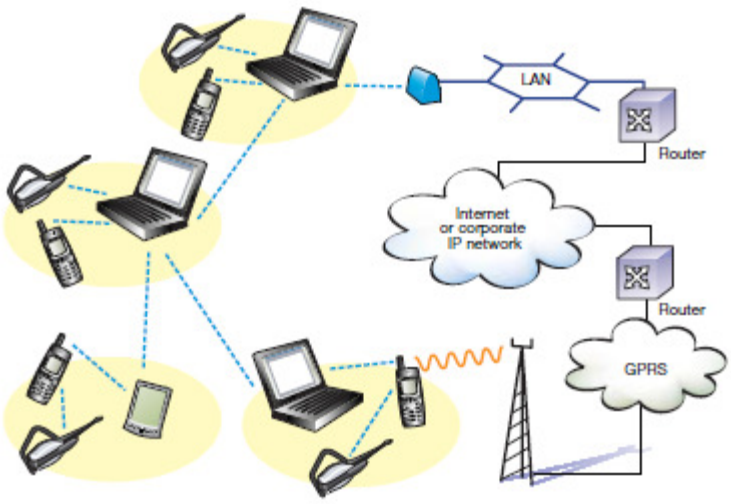
Τα προσωπικά δίκτυα διασυνδέουν κινητές συσκευές οι οποίες μεταφέρονται από χρήστες με άλλες κινητές ή σταθερές συσκευές Ενώ ένα δίκτυο BAN διασυνδέει τις συσκευές που μπορούν να φορεθούν από ένα άτομο, ένα PAN αποτελεί ένα δίκτυο στο περιβάλλον γύρω από ένα άτομο. Η ακτίνα επικοινωνίας ενός PAN είναι τυπικά μέχρι 10 μέτρα, επιτρέποντας έτσι την διασύνδεση BANs μεταξύ ατόμων που βρίσκονται το ένα κοντά στο άλλο και την διασύνδεση ενός BAN με το περιβάλλον γύρω από αυτό.

Οι τεχνολογίες των ασυρμάτων PAN στην μπάντα ISM των 2,4GHz αποτελούν τις πιο πολλά υποσχόμενες τεχνολογίες για την υλοποίηση δικτύων PAN. Η εξάπλωση φάσματος χρησιμοποιείται στις περισσότερες περιπτώσεις για την μείωση των παρεμβολών και την χρησιμοποίηση του εύρους ζώνης.

Βλέποντας από την άποψη του παραδοσιακού δικτύου κινητής τηλεφωνίας, ένα Bluetooth-based PAN ανοίγει ένα νέο τρόπο επέκτασης δικτύων κινητής τηλεφωνίας στο πεδίο του χρήστη. Κάποιος σε ένα ταξίδι που έχει πρόσβαση σε PAN Bluetooth θα μπορούσε να χρησιμοποιήσει το GPRS / UMTS κινητό τηλέφωνο ως πύλη στο Internet ή σε ένα εταιρικό IP δίκτυο. Από την άποψη του ωφέλιμου φορτίου το δίκτυο, η συνολική κίνηση του PAN τυπικά θα είναι μεγαλύτερη από εκείνη του κινητού τηλεφώνου. Επιπλέον, εάν τα PANs Bluetooth θα μπορούσαν να διασυνδεθούν με scatternets, αυτή η ικανότητα θα αυξηθεί. Το Σχήμα 2.4 παρουσιάζει ένα σενάριο στο οποίο τέσσερα Bluetooth PANs χρησιμοποιούνται. Τα PANs είναι διασυνδεδεμένα μέσω φορητών υπολογιστών με Bluetooth συνδέσεις. Επιπλέον, δύο από τα PANs είναι συνδεδεμένα σε ένα δίκτυο κορμού IP, μία μέσω ενός σημείου πρόσβασης LAN και το άλλο μέσω ενός ενιαίου GPRS / UMTS τηλεφώνου [7].

Ένα PAN μπορεί επίσης να περιλαμβάνει πολλές διαφορετικές τεχνολογίες πρόσβασης κατανεμημένες μεταξύ των συσκευών μελών της οι οποίες εκμεταλλεύονται τη λειτουργικότητα ad hoc στο PAN. Για παράδειγμα, ένας φορητός υπολογιστής θα μπορούσε να έχει μια ασύρματη LAN (WLAN) διεπαφή (όπως IEEE 802.11 ή HIPERLAN / 2) που παρέχει πρόσβαση στο δίκτυο όταν χρησιμοποιείται ο υπολογιστής εντός κτιρίου. Έτσι, το PAN θα επωφεληθεί από το συνολικό άθροισμα όλων των τεχνολογιών πρόσβασης που βρίσκονται στις συσκευές PAN. Καθώς η ιδέα των PAN ωριμάζει, θα επιτρέψει νέες συσκευές και νέες

τεχνολογίες πρόσβασης να ενσωματωθούν στο πλαίσιο PAN. Θα πρέπει επίσης να εξαλείψει την ανάγκη για τη δημιουργία υβριδικών συσκευών, όπως ένας συνδυασμός τηλέφωνο PDA-mobile, επειδή το δίκτυο PAN αντίθετα θα επιτρέπει την ασύρματη ολοκλήρωση. Σε όλα τα σενάρια που συζητήθηκαν παραπάνω, πρέπει να τονιστεί ότι η τεχνολογία μικρής εμβέλειας , όπως το Bluetooth, είναι ένας βασικός καταλύτης για την εισαγωγή της ευελιξίας που αντιπροσωπεύεται από την έννοια PAN.



Σχήμα 2.4 Προσωπικό δίκτυο PAN.

Οι τεχνολογίες των ασυρμάτων PAN προσφέρουν πρωτοποριακές λύσεις και εφαρμογές οι οποίες μπορούν να προκαλέσουν ριζικές αλλαγές στην καθημερινή μας ζωή. Μπορούμε να προμηνήσουμε ότι ένα ασύρματο PAN θα μπορεί να διασυνδέει όχι μόνο φορητές συσκευές όπως είναι τα κινητά τηλέφωνα, οι φορητοί υπολογιστές, τα PDAs αλλά και κάθε άλλη ψηφιακή συσκευή. Για παράδειγμα όταν φτάνουμε στο αεροδρόμιο θα μπορούμε να αποφύγουμε την ουρά στο ckeck-in χρησιμοποιώντας μία συσκευή χειρός με την οποία θα παρουσιάζουμε ένα ηλεκτρονικό εισιτήριο για έλεγχο και αυτόματα θα επιλέγουμε την θέση της αρεσκείας μας.

2.5 Δίκτυα MANET (Mobile Ad hoc Network)

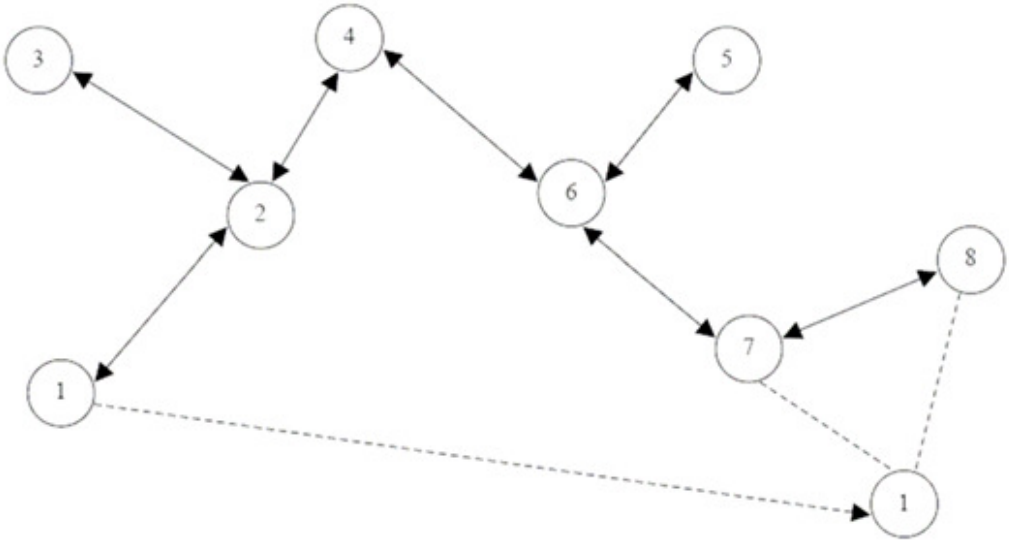
2.5.1 Αρχιτεκτονική των MANET

MANET (Mobile Ad hoc Network) είναι ένα ad hoc δίκτυο που αποτελείται από κινητούς κόμβους. Τα MANET έχουν τη δυνατότητα να διευκολύνουν την ανάπτυξη του δικτύου και να επιτρέπουν σε σταθμούς με ασύρματη διεπαφή να περιφέρονται ελεύθερα και να

επικοινωνούν μεταξύ τους χωρίς να εξαρτώνται από την διαδικτυακή υποδομή. Η κινητικότητα των κόμβων αλλάζει δυναμικά την τοπολογία του δικτύου. Όλοι οι κόμβοι που έχουν ασύρματες κάρτες δικτύου μπορούν να επικοινωνούν μεταξύ τους ακόμη και αν δεν βρίσκονται σε απόσταση άμεσης επικοινωνίας. Στην περίπτωση αυτή η επικοινωνία επιτυγχάνεται μέσω ενδιάμεσων κόμβων, οι οποίοι προωθούν τα πακέτα από την πηγή στον προορισμό [2].

Το MANET μπορεί να αναπτυχθεί απλά και ευέλικτα σχεδόν σε κάθε περιβάλλον, αλλά έχει περιορισμένη ασύρματη κάλυψη και η συνδεσιμότητά του περιορίζεται στα όρια του ίδιου του δίκτυο. Η ταχεία ανάπτυξη του διαδικτύου καθώς και των υπηρεσιών και εφαρμογών του και η πορεία των ασύρματων δικτύων (τέταρτης γενιάς) προς την κατεύθυνση των δικτύων αποκλειστικής χρήσης (**All-IP networks**), έχουν οδηγήσει σε μια αυξανόμενη απαίτηση για τη δυνατότητα των κόμβων MANET να συνδέονται με το διαδίκτυο και να χρησιμοποιούν τις υπηρεσίες και τις εφαρμογές του. Οι κινητές IP διευθύνσεις και τα πρωτόκολλα κινητών IP επιτρέπουν σε έναν κινητό κόμβο να έχει πρόσβαση στο διαδίκτυο και ν’ αλλάζει το σημείο πρόσβασής του χωρίς να χάνει τη σύνδεση. Ο κινητός κόμβος πρέπει να βρίσκεται μέσα στην ακτίνα κάλυψης του σημείου πρόσβασης και να έχει άμεση σύνδεση με αυτό. Έτσι, με τη συνεργασία μεταξύ των πρωτοκόλλων δρομολόγησης του MANET και του πρωτοκόλλου κινητών IP, η συνδεσιμότητα του διαδικτύου με τους κόμβους του δικτύου MANET μπορεί να επιτευχθεί. Η επικοινωνία μεταξύ των κόμβων και η προώθηση-δρομολόγηση των μηνυμάτων (routing-forwarding) μπορεί να περιλαμβάνει ένα ή περισσότερα άλματα (one-hop ή multi-hop) ανάλογα με το πόσο απέχουν οι κόμβοι που επιθυμούν να επικοινωνήσουν Τα Mobile Ad-Hoc Δίκτυα έχουν χαρακτηριστικά που τα κάνουν ιδιαίτερα δημοφιλή και ενδιαφέροντα σαν αντικείμενο μελέτης. Ένα MANET απαρτίζεται από κόμβους (για παράδειγμα ένα δρομολογητή με πολλαπλούς εξυπηρετητές και ασύρματες συσκευές), οι οποίοι κινούνται αυθαίρετα.

Ένα παράδειγμα από ένα μικρό MANET δίκτυο φαίνεται στο Σχήμα 2.5, όπου παρατίθενται 8 κόμβοι με τις ζεύξεις μεταξύ τους. Οι κόμβοι αυτοί έχουν τη δυνατότητα να κινούνται σε σχέση με τους υπολοίπους. Καθώς συμβαίνει αυτό οι ζεύξεις μεταξύ τους καταστρέφονται και δημιουργούνται νέες. Στο Σχήμα 2.5, ο κόμβος 1 κινείται μακριά από τον 2 και δημιουργεί καινούργιες ζεύξεις με τους 7 και 8 [8].



Σχήμα 2.5 MANET - κινητικότητα κόμβων.

2.5.2 Χαρακτηριστικά στοιχεία MANET

Τα Manet έχουν ορισμένα αξιοπρόσεκτα χαρακτηριστικά, τα σημαντικότερα από αυτά είναι τα εξής: [9] [11]

• **Αυτοδυναμία.** Τα Mobile Ad-Hoc Δίκτυα δε συνδέονται με άλλα τοπικά δίκτυα ή το Internet προκειμένου να σχηματίσουν το Ad-Hoc Δίκτυο και να λειτουργήσουν. Οι κόμβοι σχηματίζουν το δίκτυο αυτοδύναμα και επικοινωνούν μεταξύ τους. Βέβαια, η σύνδεση οποιουδήποτε κόμβου είτε με κάποιο τοπικό δίκτυο είτε με το Internet δεν είναι απαγορευμένη. Αν κάποιος κόμβος το επιθυμεί μπορεί να συνδεθεί με οποιοδήποτε άλλο κόμβο.

• **Έλλειψη κεντρικού συντονιστή.** Δεν υπάρχει κάποιος κεντρικός κόμβος που να συντονίζει την επικοινωνία των κόμβων του δικτύου. Δυο κόμβοι επικοινωνούν είτε απευθείας (one-hop communication), αν η μεταξύ τους απόσταση το επιτρέπει, είτε μέσω άλλων ενδιάμεσων κόμβων (multi-hop communication) που απλώς προωθούν τα μηνύματα επικοινωνίας, χωρίς όμως να εκτελούν χρέη συντονιστή.

• **Ισοδυναμία κόμβων.** Όλοι οι κόμβοι του δικτύου είναι ισοδύναμοι, όσον αφορά τις αρμοδιότητες που έχουν ως μέλη του δικτύου. Αυτό σημαίνει ότι κάθε κόμβος μπορεί να δρα ως πηγή, δέκτης ή ενδιάμεσος κόμβος επικοινωνίας, χωρίς να υπάρχουν κόμβοι που μπορεί να έχουν περισσότερα ή λιγότερα «δικαιώματα» από κάποιους άλλους.

• **Μεταβλητή τοπολογία και αυξημένη κινητικότητα των κόμβων.** Λόγω της κίνησης των κόμβων η συνολική εικόνα του δικτύου διαρκώς αλλάζει. Έτσι μπορεί να υπάρχουν κόμβοι που α) ενώ δε συνδέονταν, μετά από κάποιο χρονικό διάστημα να συνδέονται και β) ενώ συνδέονται για κάποιο χρονικό διάστημα μετά από λίγο να παύουν να επικοινωνούν. Γι' αυτό και δεν μπορεί να υπάρξει κεντρικό firewall.

• **Μικρή διάρκεια ζωής των κόμβων.** Η διάρκεια ζωής των κόμβων μπορεί να είναι μικρή σχετικά με τη διάρκεια ζωής του δικτύου. Για παράδειγμα μερικοί ταξιδιώτες στην αίθουσα αναμονής του αεροδρομίου ανοίγουν τα palmtop τους, τους φορητούς υπολογιστές τους ή άλλες ηλεκτρονικές φορητές συσκευές και γίνονται μέλη ενός Ad-Hoc δικτύου. Μετά από λίγα λεπτά ένας από τους ταξιδιώτες κλείνει το palmtop του και φεύγει για να επιβιβαστεί στην πτήση του, οπότε αυτόματα βγαίνει από το δίκτυο. Το δίκτυο ωστόσο συνεχίζει να υπάρχει.

• **Μικρό εύρος ζώνης συχνοτήτων κόμβων**. Οι κόμβοι του δικτύου έχουν σχετικά μικρό bandwidth, με εμβέλεια μερικών δεκάδων ή χιλιάδων μέτρων, καλύπτοντας μια σχετικά μικρή γεωγραφική περιοχή.

• **Περιορισμένη ισχύς.** Οι κόμβοι ενός τέτοιου δικτύου είναι κινητοί και άρα λειτουργούν με μπαταρίες. Αυτό, σε συνδυασμό με το γεγονός ότι κινούνται και δεν είναι εύκολο να βρίσκονται συνεχώς κοντά σε μια σταθερή βάση απ' όπου θα προμηθεύουν ενέργεια, οδηγεί αναπόφευκτα σε μικρή διάρκεια λειτουργίας των κόμβων. Αυτό σημαίνει ότι ένας κόμβος μπορεί να λειτουργεί για ένα διάστημα, έπειτα για να εξοικονομήσει ενέργεια να σταματάει τη λειτουργία του, μετά να λειτουργεί ξανά κ.ο.κ.

2.5.3 Εφαρμογές MANET

Τα δίκτυα MANET λόγω της κινητικότητάς τους, άρα και της δυναμικής τους τοπολογίας είναι πολύ χρήσιμα σε πολλές περιπτώσεις. Ένα τέτοιο δίκτυο λοιπόν είναι ιδιαίτερα χρήσιμο σε περιπτώσεις που η σταθερή δομή δεν υφίσταται ή είναι ανεπαρκής ή έχει καταστραφεί. Μερικές από τις εφαρμογές ενός τέτοιου δικτύου είναι οι παρακάτω: [9] [11]

- **Εκπαιδευτικές**: για παράδειγμα στα συνέδρια ή σε διάφορες διαλέξεις, όπου όλα τα τερματικά και τα access points είναι απαραίτητο να είναι κινητά και στις οποίες έχουμε συγκέντρωση ατόμων με φορητούς υπολογιστές σε μια περιοχή που δεν διαθέτει δίκτυο 802.11. Αφού είναι άμεση ανάγκη για τους σύνεδρους να μετακινούνται, να ανταλλάσσουν πληροφορίες και να επικοινωνούν χωρίς να

εξαρτώνται αποκλειστικά από ένα σταθερό σημείο πρόσβασης, το MANET υλοποιεί επιτυχώς όλες αυτές τις απαιτήσεις.

- **Στρατιωτικές**: τα MANET δίκτυα είναι ιδιαίτερα σημαντικά και για τις ένοπλες δυνάμεις, για εφαρμογές όπως: στα στρατιωτικά οχήματα σ' ένα πεδίο μάχης, στα τηλεκατευθυνόμενα εναέρια οχήματα, σ' έναν στόλο πλοίων στη θάλασσα, στους τομείς των αισθητήρων και στα γοργά αναπτυσσόμενα δίκτυα πεδίου μάχης.
- **Disaster Management**: χρησιμοποιείται εκεί που δημιουργούνται ομάδες αποκατάστασης και διαχείρισης καταστροφής, οι οποίες δεν θα μπορούσαν να στηριχθούν στην υπάρχουσα υποδομή, π.χ. το προσωπικό άμεσης ανάγκης σ' ένα σεισμό που κατάστρεψε την υπάρχουσα υποδομή
- **Neighborhood Area Networks (NANs)**: τα οποία είναι δίκτυα που αναφέρονται στη διαμοιρασμένη πρόσβαση στο Internet σε αστικές τοποθεσίες υψηλής πυκνότητας.
- **Εμπορικές**: όπως η αυτοματοποίηση των πωλήσεων ή τα Personal Area Networks (PANs).

2.6 Φορητό IP

2.6.1 Γενική ιδέα φορητού IP

Για να μπορεί κάθε χρήστης που συνδέεται σε ένα δίκτυο να χρησιμοποιεί συνδεσμοστρεφείς υπηρεσίες (π.χ. TCP) πρέπει να χρησιμοποιεί διαρκώς μια σταθερή διεύθυνση IP. Η διεύθυνση IP όμως, πρέπει να αντιπροσωπεύει κάθε φορά το επικοινωνιακό μέσο που χρησιμοποιείται, καθώς και το σημείο που βρίσκεται ο χρήστης. Αυτό συμβαίνει επειδή οι δρομολογητές δεν χρησιμοποιούν ολόκληρη την διεύθυνση IP (αφού κάτι τέτοιο θα απαιτούσε οι δρομολογητές να έχουν αποθηκευμένους και να διαχειρίζονται τεράστιους πίνακες δρομολόγησης), αλλά μόνο κάποιο τμήμα της που καθορίζει το δίκτυο στο οποίο ανήκει. Κατά συνέπεια, κάθε φορά που κάποιο τερματικό μετακινείται σε διαφορετικό δίκτυο ανατίθεται σε αυτό μια διαφορετική διεύθυνση, που αντιστοιχεί στο νέο δίκτυο. Το πρόβλημα αυτό είναι ιδιαίτερα έντονο στα ασύρματα συστήματα και κυρίως στα κινητά δίκτυα, τα οποία είναι από την φύση τους δυναμικά και οι κόμβοι τους επιτρέπεται να μετακινούνται από δίκτυο σε δίκτυο συνεχώς.

Με βάση την κινητικότητα των τερματικών, μπορούμε να τους κατατάξουμε σε στάσιμους (stationary), που είναι οι υπολογιστές που δεν μετακινούνται ποτέ, σε αποδημητικούς (migratory), που είναι συνήθως φορητοί υπολογιστές, που είναι κατά βάση στάσιμοι, αλλά μετακινούνται από μια σταθερή τοποθεσία σε μια άλλη από καιρό σε καιρό και η τελευταία

κατηγορία είναι οι περιπλανώμενοι (roaming) που είναι υπολογιστές που λειτουργούν εν κινήσει και θέλουν να διατηρούν τις συνδέσεις τους καθώς μετακινούνται. Οι αποδημητικοί και οι περιπλανώμενοι υπολογιστές αναφέρονται συχνά και ως κινητοί υπολογιστές υπηρεσίας (mobile hosts).

Για την επίλυση του παραπάνω προβλήματος αναπτύχθηκε το φορητό IP (mobile IP), το οποίο είναι ένας μηχανισμός που υποστηρίζει την ξεκάθαρη δικτυακή συνδεσιμότητα στους κινητούς σταθμούς. Το φορητό IP επιτρέπει στον κινητό σταθμό να συνεχίσει να χρησιμοποιεί την διεύθυνση IP που του έχει ανατεθεί στο μητρικό δίκτυο (home IP address), ανεξάρτητα από το δίκτυο στο οποίο ο σταθμός είναι υλικά προσαρτημένος. Κάθε δίκτυο που θέλει να επιτρέψει στους χρήστες του να «περιπλανιούνται» πρέπει να εγκαταστήσει έναν οικείο πράκτορα (home agent). Κάθε δίκτυο που θέλει να επιτρέπει επισκέπτες πρέπει να εγκαταστήσει έναν ξένο πράκτορα (foreign agent). Η λειτουργία κάθε ξένου πράκτορα είναι να παρακολουθεί όλους τους κινητούς υπολογιστές υπηρεσίας που συνδέονται στο δίκτυο αυτό, ενώ η λειτουργία κάθε οικείου πράκτορα είναι να παρακολουθεί όλους τους κινητούς υπολογιστές υπηρεσίας που ανήκουν στο «οικείο» δίκτυο, αλλά έχουν «μετακομίσει» σε κάποιο άλλο δίκτυο [4] [12].

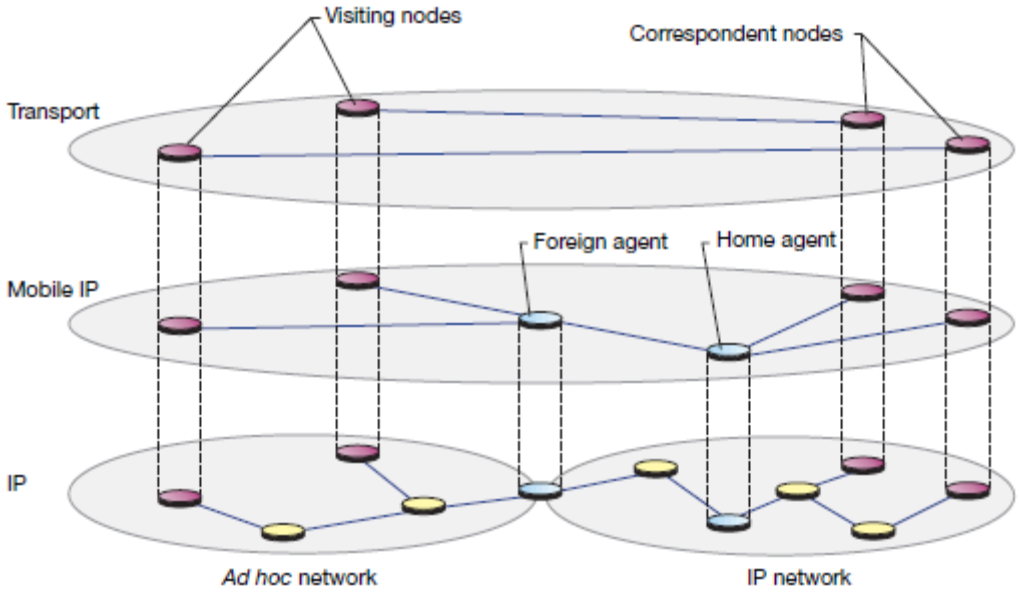
2.6.2 Mobile IP for mobile *ad hoc* networks (MIPMANET)

Το Mobile IP για κινητά ad hoc δίκτυα (MIPMANET)έχει σχεδιαστεί για να παρέχει στα ad hoc δίκτυα

- πρόσβαση στο Internet
- τις υπηρεσίες της κινητής τηλεφωνίας IP.

Η λύση αυτή χρησιμοποιεί ξένους πράκτορες (foreign agents) του κινητούIPως σημεία πρόσβασης στο Internet για να παρακολουθείται το δίκτυο ad hoc στο οποίο κάθε δεδομένος κόμβος είναι τοποθετημένος , και να κατευθύνει τα πακέτα προς την άκρη του δικτύου ad hoc [7].

Το Σχήμα 2.6 δείχνει ότι το mobile IP και η λειτουργικότητα δρομολόγησης ad hoc είναι πολυεπίπεδες.



Σχήμα 2.6 Απεικόνηση αρχιτεκτονικής MIPMANET.

Το ad hoc πρωτόκολλο δρομολόγησης χρησιμοποιείται για να παραδώσει πακέτα μεταξύ του ξένου πράκτορα (foreign agent) και του επισκεπτόμενου κόμβου (visiting node). Μια πολυεπίπεδη προσέγγιση που απασχολεί διάνοιξη - δικτύωση σηράγγων (tunneling) εφαρμόζεται στην προς τα έξω ροή δεδομένων, για να διαχωρίσει τη λειτουργικότητα του κινητού IP από το ad hoc πρωτόκολλο δρομολόγησης.

Αυτό καθιστά δυνατό για το MIPMANET να παράσχει πρόσβαση στο Internet, επιτρέποντας στους κόμβους να επιλέξουν πολλαπλά σημεία πρόσβασης και να εκτελέσουν απρόσκοπτη εναλλαγή μεταξύ τους. Εν συντομία, το MIPMANET λειτουργεί ως εξής:

- Κόμβοι σε ένα δίκτυο ad hoc που θέλουν πρόσβαση στοInternetχρησιμοποιούν τις οικίες τους διευθύνσεις IP (home IP adddress) για κάθε επικοινωνία και εγγράφονται με ένα ξένο πράκτορα.
- Για να στείλει ένα πακέτο σε έναν κεντρικό υπολογιστή στο διαδίκτυο, ο κόμβος στο ad hoc δίκτυο διοχετεύει το πακέτο προς τον ξένο πράκτορα (ανοίγει πέρασμα στο πακέτο ώστε να πάει στο ξένο πράκτορα).
- Για να λάβει πακέτα από κεντρικούς υπολογιστές στο Internet, τα πακέτα δρομολογούνται προς τον ξένο πράκτορα (foreign agent) από τους συνηθισμένους μηχανισμούς mobile IP.Ο ξένος πράκτορας παραδίδει στη συνέχεια τα πακέτα προς τον κόμβο του ad hoc δικτύου.

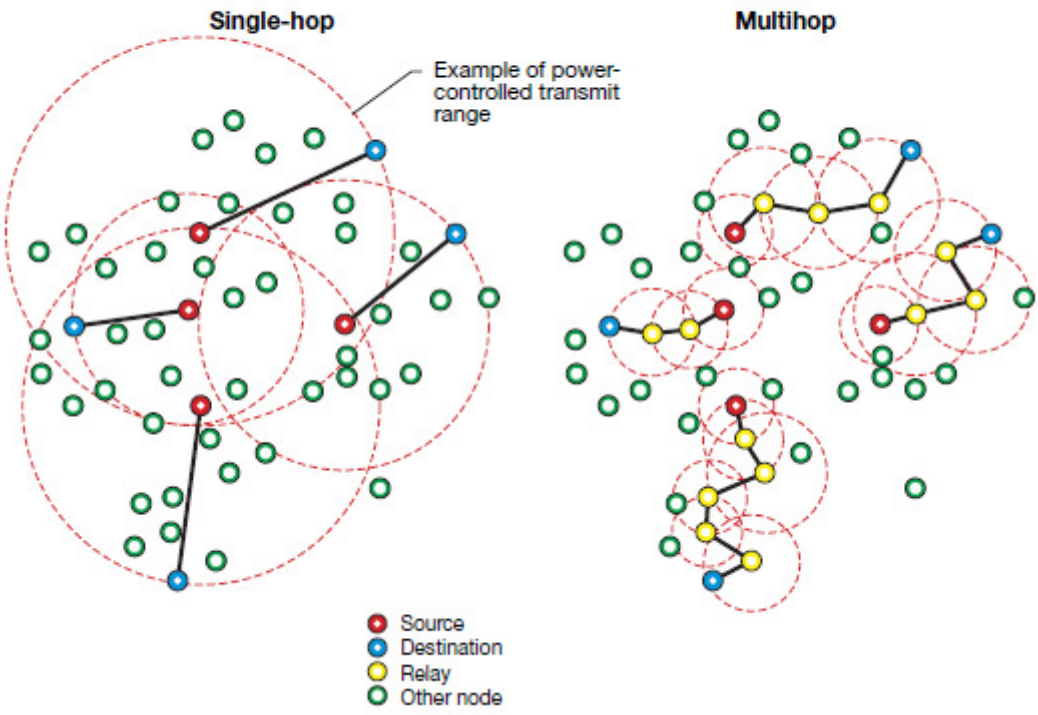
- Οι κόμβοι που δεν απαιτούν πρόσβαση στο Internet αλληλεπιδρούν με το ad hoc δίκτυο σαν να ήταν ένα αυτόνομο δίκτυο, δηλαδή δεν απαιτούν δεδομένα σχετικά με διαδρομές προς προορισμούς έξω από το δίκτυο ad hoc.
- Αν ένας κόμβος δεν μπορεί να προσδιοριστεί από την διεύθυνση IP ανεξάρτητα ή όχι αν ο προορισμός βρίσκεται μέσα στο ad hoc δίκτυο, πρώτα θα ψάξει για τον επισκεπτόμενο κόμβο μέσα στο ad hoc δίκτυο πριν διοχετεύσει (δρομολογήσει) το πακέτο

Με τη χρήση της σήραγγας, τα MIPMANET μπορούν να ενσωματώσουν προεπιλεγμένη διαδρομή σε ad hoc πρωτόκολλα δρομολόγησης κατ' απαίτηση (on demand) , όπως AODV και DSR, χωρίς να απαιτείται οποιασδήποτε σημαντικές τροποποιήσεις. Πακέτα που απευθύνονται σε προορισμούς που δεν βρίσκονται εντός του ad hoc δικτύου διοχετεύονται προς ξένους πράκτορες. Σε MIPMANET, μόνο εγγεγραμμένοι επισκέψιμοι κόμβοι έχουν πρόσβαση στο διαδίκτυο, επομένως η μόνη κίνηση που θα εισέλθει στο δίκτυο ad hoc από το διαδίκτυο είναι η κυκλοφορία που διοχετεύεται στον ξένο πράκτορα από ένα εγγεγραμμένο κόμβο του οικείου πράκτορα. Ομοίως, η κίνηση που αφήνει το δίκτυο ad hoc διοχετεύεται προς το ξένο πράκτορα από ένα εγγεγραμμένο κόμβο. Αυτό οδηγεί σε διαχωρισμό μεταξύ τους, και με αυτόν τον τρόπο έχει την ικανότητα να ελέγχει την κίνηση που είναι τοπική στο δίκτυο ad hoc και την κίνηση που εισέρχεται στο ad hoc δίκτυο.

2.7 Χαρακτηριστικά Multiple hops και Single hops δικτύων

Σε ένα αναξιόπιστο ασύρματο μεταδιδόμενο μέσο, οι βασικές θεωρήσεις θα πρέπει να απευθύνονται στο σύστημα ενός δίκτυο ad hoc δικτύου, για να εξασφαλιστεί η αξιόπιστη και αποτελεσματική λειτουργία. Ένας τρόπος για να γίνει αυτό είναι να χρησιμοποιήσουμε multihopping, το οποίο διευκολύνει την επαναχρησιμοποίηση των πόρων και στα δύο επίπεδα, το χωρικό και το χρονικό,_υπό την προϋπόθεση ότι οι κόμβοι που συμμετέχουν στο δίκτυο έχουν διανεμηθεί αρκετά καλά στο χώρο. Αντίθετα, τα SingleHop δίκτυα μοιράζονται κυρίως τους πόρους καναλιού στο χρονικό πεδίο. Το Σχήμα 2.7 δείχνει μια σχηματική απεικόνιση της χωρικής παρεμβολής σε multihopping και singlehopping σενάρια. Κάθε περίπτωση θεωρεί μια πανομοιότυπη κατάσταση όσον αφορά τη διανομή κόμβων, πηγών και τους προορισμούς. Στο multihopping σενάριο, τα πακέτα δρομολογούνται πάνω από ενδιάμεσους αναμεταδότες. Ωστόσο, στο singlehopping σενάριο τα δεδομένα στέλνονται απευθείας από την πηγή στον προορισμό. Οι κύκλοι στο σχήμα δείχνουν την εμβέλεια της ελεγχόμενης ισχύος των κόμβων μετάδοσης. Η εικόνα απεικονίζει επίσης

ανενεργούς κόμβους που δεν συμμετέχουν ως πηγές, προορισμοί, ή ενδιάμεσοι αναμεταδότες. Από αυτό το σχήμα, έχουμε την αίσθηση ότι το σενάριο multihop (πολλαπλών αναπηδήσεων) παρέχει μεγαλύτερη φασματική απόδοση (Bit / s / Hz / m^2).



Σχήμα 2.7 Multihop & Singlehop δίκτυο.

Αν το multihopping είναι απαραίτητο, κατάλληλο ή ακόμα και δυνατό, εξαρτάται από παράγοντες όπως ο αριθμός και η κατανομή των τερματικών στο δίκτυο, η σχετική πυκνότητα της κυκλοφορίας, τα χαρακτηριστικά του ραδιοδιαύλου, πρακτικοί περιορισμοί επικοινωνίας, και λόγοι για βελτιστοποίηση ορισμένων παραμέτρων. Υπό ορισμένες συνθήκες, ένα δίκτυο πολλαπλών αναπηδήσεων μπορεί στην πραγματικότητα να εκφυλιστεί σε ένα δίκτυο μονής αναπήδησης. Ένας προφανής λόγος για την πρόσληψη (χρήση) multihopping είναι να παρέχει συνδεσιμότητα, δεδομένου ότι κάποια τερματικά μπορεί να είναι εκτός της εμβέλειας το ένα με το άλλο, και δεν μπορεί επομένως να σχηματιστεί ένα singlehop δίκτυο [7].

Σε ένα σενάριο multihop (πολλαπλών βημάτων), είναι λογικό να μην σπαταλάμε περισσότερη ενέργεια από ό, τι κάθε hop απαιτεί. Στην ουσία, το κλειδί για τη διατήρηση ενέργειας είναι να ελέγχουμε την ισχύ μετάδοσης, προκειμένου να αντισταθμιστούν οι απώλειες διαδρομής που συμβαίνουν όταν ένα μήνυμα στέλνεται μεταξύ γειτονικών

κόμβων. Προφανώς, όταν ισχύς μετάδοσης είναι περιορισμένη, αυτό μπορεί να μην είναι δυνατό για να φθάσει στον επιθυμητό σταθμό χωρίς πολλαπλά βήματα.

Η μέθοδος multihopping είναι ευεργετική, επειδή αυτό εξοικονομεί ενεργειακούς πόρους μετάδοσης, μειώνει τις παρεμβολές και αυξάνει την συνολική απόδοση του δικτύου. Θα μπορούσε επίσης να είναι μια αναγκαιότητα, να παρέχει κάθε είδους σύνδεσης μεταξύ πολύ μακρινών τερματικών.

ΚΕΦΑΛΑΙΟ 3

ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ AD HOC ΔΙΚΤΥΩΝ

3.1 Εισαγωγή

Η ανάγκη για αδιάλειπτη επικοινωνία ανεξάρτητα από την τοποθεσία των κινητών συσκευών, έχει οδηγήσει στο σχεδιασμό και την ανάπτυξη ασύρματων δικτύων τα οποία αποτελούνται από κινητά τερματικά και παρέχουν τη δυνατότητα επικοινωνίας ακόμα και σε περιπτώσεις χωρίς σταθερή υποδομή.

Τα ασύρματα κινητά δίκτυα ή Mobile Ad Hoc Networks (MANETs) είναι μια συλλογή κινητών κόμβων, οι οποίοι μπορούν δυναμικά να συνδεθούν στο δίκτυο σε οποιαδήποτε χρονική στιγμή χωρίς να γίνει χρήση κάποιας προϋπάρχουσας υποδομής. Αυτή είναι και η κύρια διαφορά τους από τα ασύρματα δίκτυα που βασίζονται σε σταθερή δικτυακή υποδομή στα οποία οι κόμβοι είναι συνήθως σταθεροί και επικοινωνούν χωρίς ενδιάμεσους κόμβους με ένα κεντρικοποιημένο σημείο πρόσβασης ή έναν σταθμό βάση. Τα κινητά Ad Hoc δίκτυα είναι αυτόνομα δίκτυα στα οποία οι κόμβοι είναι ελεύθεροι να κινηθούν τυχαία προς οποιαδήποτε κατεύθυνση, με αποτέλεσμα να αλλάζει συχνά η τοπολογία του δικτύου. Σε αυτά τα δίκτυα τα δεδομένα που διακινούνται από ένα κομβο δεν είναι κατ' ανάγκη δεδομένα που έχουν ως αποστολέα ή παραλήπτη τον ίδιο κόμβο, αλλά πολλές φορές πρόκειται για δεδομένα που αναμεταδίδονται μέσω του συγκεκριμένου κόμβου με παραλήπτη κάποιον άλλο κόμβο του δικτύου .Αυτό σημαίνει ότι ο κόμβος είναι και ένας δρομολογητής μέσα στο δίκτυο.

Με βάση τα παραπάνω, η κύρια πρόκληση που υπάρχει στα ασύρματα κινητά δίκτυα είναι να διατηρεί κάθε κόμβος τις πληροφορίες που απαιτούνται για τη σωστή επικοινωνία. Επιπλέον, πρέπει να είναι σε θέση να δρομολογούν την κίνηση έτσι ώστε δυναμικά να αποκαθιστούν την επικοινωνία χωρίς κεντρική διαχείριση.

Η επικοινωνία στα κινητά Ad Hoc δίκτυα μεταξύ δυο κόμβων χωρίζεται σε δύο ομάδες:

- στην επικοινωνία μεταξύ κόμβων οι οποίοι είναι σχετικά κοντά ώστε να μπορούν να επικοινωνούν απευθείας,
- στην επικοινωνία μέσω ενδιάμεσων κόμβων.

Η **δρομολόγηση (routing)** είναι υπεύθυνη για τη μεταφορά των δεδομένων της από τον αποστολέα στον παραλήπτη μέσα στο δίκτυο. Η **μεταγωγή πακέτων (packet switching)** είναι η τεχνολογία με την οποία τα δεδομένα στέλνονται σε μικρά πακέτα μέσω των

δρομολογητών του δικτύου. Στην επικεφαλίδα του κάθε πακέτου εκτός από τη διεύθυνση του παραλήπτη αποθηκεύεται και η σειρά του πακέτου, ώστε να είναι δυνατή η συναρμολόγηση των πακέτων στο δέκτη.

Πιο συγκεκριμένα, δρομολόγηση είναι η διαδικασία κατά την οποία δεδομένα (πακέτα) μεταφέρονται από ένα δίκτυο σ' ένα άλλο και βασίζεται στην λογική διεύθυνση (IP address) του παραλήπτη. Για αυτήν την διαδικασία είναι υπεύθυνες κάποιες συσκευές δικτύου, οι οποίες ονομάζονται δρομολογητές (routers). Η μεταφορά δεδομένων από το ένα δίκτυο σε ένα άλλο, απαιτεί να συμβούν ορισμένες διαδικασίες: μία κατάλληλη διαδρομή για τα δεδομένα πρέπει να καθοριστεί και ύστερα τα δεδομένα πρέπει να φθάσουν στον τελικό προορισμό τους. Τόσο η δρομολόγηση των πακέτων, όσο και ο καθορισμός της διαδρομής, συμβαίνουν στο επίπεδο 3 (επίπεδο δικτύου-network layer), στο μοντέλο του OSI. Το πρόβλημα της δρομολόγησης σε ένα ασύρματο ad-hoc τηλεπικοινωνιακό δίκτυο, το οποίο αποτελείται από κινητούς κόμβους, ορίζεται ως η διαδικασία εύρεσης μιας διαδρομής από έναν κόμβο του δικτύου προς ένα άλλο κόμβο του ίδιου δικτύου με σκοπό την μεταφορά δεδομένων.

Ως διαδρομή σε ένα ασύρματο ad-hoc δίκτυο ορίζουμε την ακολουθία των κόμβων μέσω των οποίων θα διαβιβαστούν τα πακέτα δεδομένων στον προορισμό τους. Υποθέτουμε ότι οι κόμβοι στο δίκτυο αυτό, δεν μπορούν να μεταβιβάσουν απευθείας τα δεδομένα ο ένας στον άλλο, λόγω της περιορισμένης εμβέλειας του ασύρματου πομπού και γι' αυτό χρησιμοποιούνται **ενδιάμεσοι κόμβοι** για να μπορέσουν να μεταδοθούν τα δεδομένα στον προορισμό τους. Οι κόμβοι σε ένα ασύρματο ad-hoc δίκτυο στις περισσότερες περιπτώσεις μπορούν και κινούνται, με αποτέλεσμα η θέση τους στο δίκτυο ν' αλλάζει συνεχώς. Καθώς αλλάζει η θέση τους, αλλάζει και η κατάσταση του δικτύου, άλλες συνδέσεις γίνονται ενεργές, άλλες ανενεργές, νέοι κόμβοι εισέρχονται και προσθέτονται στο δίκτυο, ενώ άλλοι απομακρύνονται και αποβάλλονται [9].

Το γεγονός αυτό επιβάλει οι κόμβοι ου δικτύου άλλες φορές να παίζουν το ρόλο τερματικών κόμβων, που είναι είτε οι κόμβοι προέλευσης είτε οι κόμβοι του προορισμού των πακέτων, που ταξιδεύουν στο δίκτυο και άλλες το ρόλο των δρομολογητών ή των μεταγωγέων, που φροντίζουν να προωθήσουν πακέτα, τα οποία δεν προορίζονται γι' αυτούς στους κόμβους προορισμού. Για το λόγο αυτό, σε ένα ασύρματο ad-hoc δίκτυο είναι απαραίτητο ένα πρωτόκολλο δρομολόγησης, για να διατηρηθούν οι βασικές λειτουργίες του δικτύου, τις οποίες τώρα έχουν επιφορτιστεί οι κόμβοι.

Για τον συντονισμό μεταξύ των κόμβων ενός ad hoc δικτύου και τη διευκόλυνση της επικοινωνίας μεταξύ οποιονδήποτε ζευγαριών από αυτούς, χρησιμοποιούνται **πρωτόκολλα δρομολόγησης**, τα οποία ανακαλύπτουν διαδρομές μεταξύ των κόμβων αυτών. Τα ad hoc κινητά δίκτυα, έχουν όπως προαναφέρθηκε, αρκετά ιδιαίτερα χαρακτηριστικά, τα οποία καθιστούν τα παραδοσιακά πρωτόκολλα δρομολόγησης που έχουν σχεδιαστεί για ενσύρματα δίκτυα, ακατάλληλα γι' αυτά.

3.2 Κατηγορίες πρωτοκόλλων δρομολόγησης

Τα πρωτόκολλα δρομολόγησης για ad hoc δίκτυα μπορούν να διαιρεθούν σε τρεις βασικές κατηγορίες: [9] [13]

- **Table-driven (proactive) πρωτόκολλα**
- **On-demand (reactive) πρωτόκολλα**
- **Hybrid πρωτόκολλα**

Τα παραδοσιακά πρωτόκολλα δρομολόγησης είναι ταProactiveτα οποία διατηρούν τα δρομολόγια προς όλους τους κόμβους, συμπεριλαμβανομένων των κόμβων στους οποίους δεν υπάρχουν πακέτα να σταλούν. Αντιδρούν σε κάθε αλλαγή στην τοπολογία, ακόμη και αν καμία κίνηση δεν επηρεάζεται από την αλλαγή αυτή, και απαιτούν περιοδικό έλεγχο μηνυμάτων για να διατηρήσουν τις διαδρομές σε κάθε κόμβο στο δίκτυο. Ο ρυθμός με τον οποίο τα εν λόγω μηνύματα ελέγχου που αποστέλλονται πρέπει να αντικατοπτρίζουν τη δυναμικές του δικτύου προκειμένου να διατηρηθούν έγκυρες διαδρομές. Έτσι, σπάνιες πηγές, όπως ισχύς και σύνδεση εύρους ζώνης θα χρησιμοποιηθούν περισσότερο συχνά για έλεγχο κυκλοφορίας , καθώς η κινητικότητα των κόμβων αυξάνει.

Μια εναλλακτική προσέγγιση περιλαμβάνει τη θέσπιση reactive διαδρομών, που υπαγορεύει ότι οι διαδρομές μεταξύ κόμβων καθορίζονται αποκλειστικά όταν αυτοί απαιτούνται ρητά να δρομολογήσουν πακέτα. Αυτό αποτρέπει τους κόμβους από την ενημέρωση κάθε πιθανής διαδρομής στο δίκτυο, αντί να τους επιτρέπει να εστιάσει είτε σε διαδρομές που χρησιμοποιούνται, ή στις διαδρομές που βρίσκονται στη διαδικασία της εγκατάστασης.

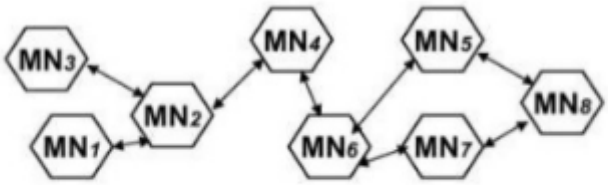
Μια κατηγορία που έχει δημιουργηθεί πρόσφατα είναι αυτή των υβριδικών πρωτοκόλλων. Στην υβριδική δρομολόγηση, κάθε κόμβος συμπεριφέρεται ωςreactive στην κοντινή περιοχή του και ως proactive έξω από αυτή την περιοχή ή ζώνη. Τα υβριδικά πρωτόκολλα δρομολόγησης έχουν τα πλεονεκτήματα των reactiveκαι proactive πρωτοκόλλων αλλά απαιτούν επιπλέον υλικό, όπως συσκευέςGPS συνδεδεμένες στους κόμβους ή

ενσωματωμένες σε αυτούς. Αυτή η βασική τους απαίτηση είναι και το βασικότερο τους μειονέκτημα.

3.3 Proactive πρωτόκολλα δρομολόγησης

3.3.1 Destination sequence distance vector Protocol (DSDV)

Το DSDV είναι ένα proactive hop by hop πρωτόκολλο δρομολόγησης. Κάθε κόμβος του δικτύου διατηρεί ένα πίνακα δρομολόγησης που περιέχει όλους τους πιθανούς προορισμούς, το επόμενο hop σε οποιοδήποτε προσβάσιμο προορισμό, καθώς και τον αριθμό των hops που θα απαιτηθούν και τον sequence number ο οποίος έχει οριστεί από τον προορισμό. Οι περιοδικές μεταδόσεις με ενημερώσεις δρομολογίων χρησιμοποιούνται για να κρατήσουν το πίνακα δρομολόγησης ενημερωμένο πλήρως όλες τις φορές. Για να εγγυηθεί loop-freedom, το DSDV χρησιμοποιεί μια έννοια που βασίζεται σε αριθμούς ακολουθίας για να δείξει πώς είναι οι νέες ή μια συγκεκριμένη διαδρομή. Ο DSDV βασίζεται στο κλασσικό αλγόριθμο δρομολόγησης των Bellman-Ford με κάποιες βελτιώσεις. Η διαδρομή με τη μεγαλύτερη αριθμητική ακολουθία, δηλαδή η πιο πρόσφατη, είναι αυτή που χρησιμοποιείται. Στην περίπτωση που δύο διαδρομές έχουν την ίδια αριθμητική ακολουθία, τότε η διαδρομή με την καλύτερη μετρική, δηλαδή η μικρότερη διαδρομή, χρησιμοποιείται (Σχήμα 3.1).



Dest	Nexthop	Metric	DestSequence	InstallTime
MN1	MN2	2	406	
MN2	MN2	1	128	
MN3	MN2	2	564	
MN4	MN4	0	710	
MN5	MN6	2	392	
MN6	MN6	1	076	
MN7	MN6	2	128	
MN8	MN6	3	050	

Σχήμα 3.1 Routing Table for MN4

Όταν κάποιος κόμβος Α αντιληφθεί ότι η διαδρομή μέχρι τον προορισμό D έχει πάψει να είναι έγκυρη, τότε αυξάνεται ο αριθμός hop-count της διαδρομής αυτής. Έτσι, την επόμενη φορά που ο Α θα κοινοποιήσει στους γείτονές του τον πίνακα δρομολόγησής του, θα δώσει στη διαδρομή προς τον D, άπειρο hop-count και μια αριθμητική ακολουθία που είναι μεγαλύτερη από πριν. Οι κόμβοι υπολογίζουν επίσης το χρόνο εγκατάστασης μιας διαδρομής, δηλαδή το μέσο χρόνο κατά τον οποίο κυμαίνονται οι διαδρομές για έναν προορισμό, μέχρι να ληφθεί η καλύτερη διαδρομή. Έτσι καθυστερούν την εκπομπή μιας ενημέρωσης διαδρομής κατά ένα ποσό χρόνου ίσο με το χρόνο εγκατάστασης, μειώνοντας με αυτό τον τρόπο την κίνηση του δικτύου και βελτιστοποιώντας τις διαδρομές, αφού εξαλείφονται οι εκπομπές αυτές οι οποίες θα συνέβαιναν αν μια καλύτερη διαδρομή βρισκόταν πολύ σύντομα [7] [9].

3.3.2 Optimized Link State Routing Protocol (OLSR)

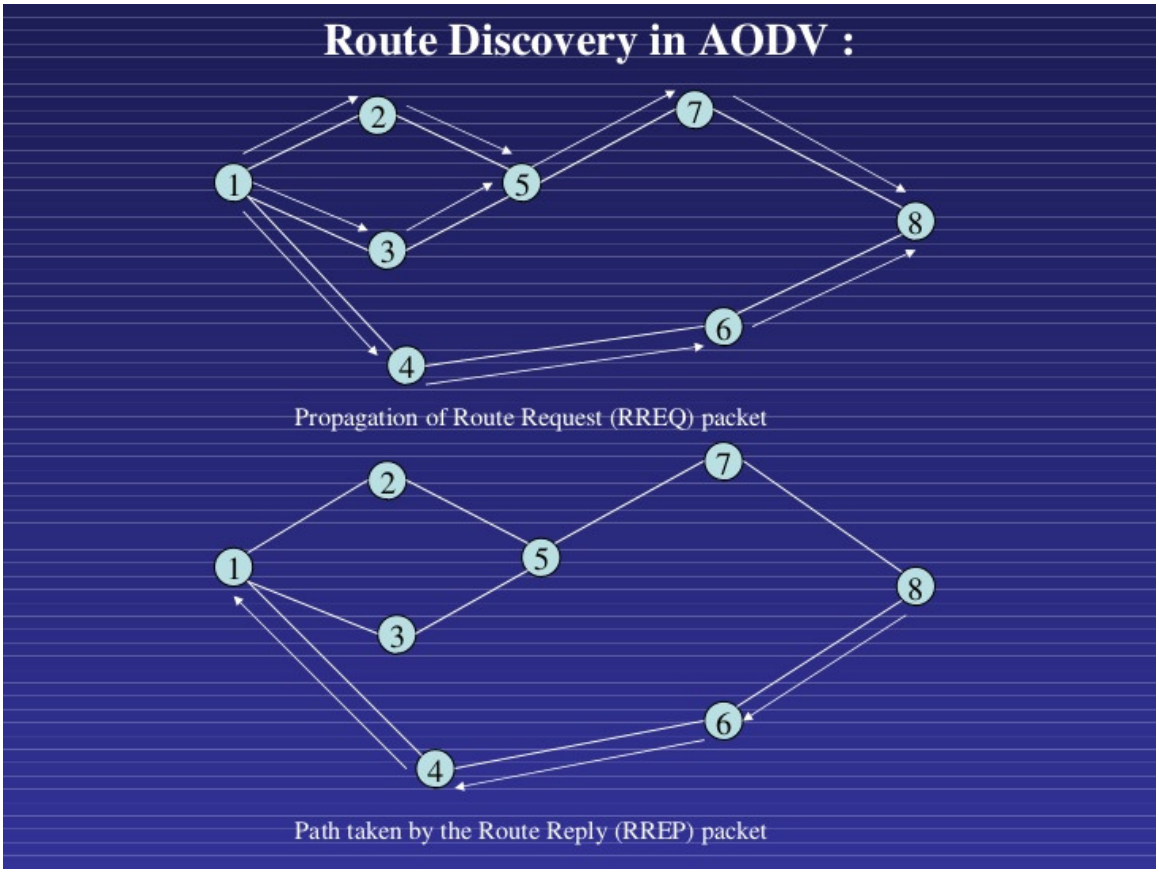
Το πρωτόκολλο OLSR είναι ένα πρωτόκολλο δρομολόγησης σχεδιασμένο για κινητά Ad Hoc δίκτυα. Το OLSR ανήκει στα proactive πρωτόκολλα με αποτέλεσμα οι διάφορες διαδρομές να είναι διαθέσιμες οποιανδήποτε στιγμή χρειαστούν. Το πρωτόκολλο OLSR είναι ένα πρωτόκολλο κατάστασης σύνδεσης στο οποίο η πληροφορία σύνδεσης διαδίδεται μέσα στο δίκτυο με έναν αλγόριθμο εκπομπής προς όλους (flooding).Η λειτουργία του OLSR ελαχιστοποιεί την πιθανότητα υπερχείλισης του δικτύου αφού χρησιμοποιεί μόνο συγκεκριμένους κόμβους που ονομάζονται Multipoint Relays ή MPRs. Κάθε κόμβος στο δίκτυο, επιλέγει ένα σύνολο κόμβων ως τους MPRs του. Η επιλογή αυτών των κόμβων γίνεται με τέτοιο τρόπο ώστε το σύνολο των MPRs να καλύπτει όλους τους κόμβους που είναι δύο βήματα μακριά. Αξίζει να σημειωθεί ότι όσο πιο μικρό είναι το σύνολο αυτών των κόμβων τόσο λιγότερη θα είναι και η επιφόρτιση του δίκτυο εξαιτίας της κυκλοφορίας μηνυμάτων ελέγχου Ένας κόμβος διατηρεί πληροφορίες για το σύνολο των κόμβων που έχουν επιλεχθεί ως τα MPRs του και ενημερώνει αυτές τις πληροφορίες σε τακτά χρονικά διαστήματα μέσω των HELLO μηνυμάτων από τους γειτονικούς κόμβους του.

Όταν ένα πακέτο ελέγχου διαδίδεται από ένα κόμβο, μόνο οι κόμβοι που ανήκουν στον πίνακα MPR του κόμβου συμμετέχουν στην προώθηση του πακέτου. Στο OLSR ένας κόμβος δημιουργεί πακέτα ελέγχου λαμβάνοντας υπόψιν μόνο τις συνδέσεις μεταξύ αυτού του κόμβου και στους MPRs του. Αυτό έχει σαν αποτέλεσμα, οι διαδρομές να υπολογίζονται ανάλογα με την εικόνα που έχει ο κόμβος για την τοπολογία του δικτύου [9] [16].

3.4 Reactive πρωτόκολλα δρομολόγησης

3.4.1 Ad hoc on demand distance vector Protocol (AODV)

Όπως το DSDV έτσι και το AODV είναι distance vector routing protocol, αλλά είναι reactive. Αυτό σημαίνει ότι το AODV ζητά μόνο μια διαδρομή όταν χρειάζεται, και δεν απαιτεί ότι οι κόμβοι πρέπει διατηρούν δρομολόγια προς προορισμούς που δεν επικοινωνούν. Το AODV χρησιμοποιεί αριθμούς ακολουθίας με έναν τρόπο παρόμοιο με το DSDV για να αποφευχθούν οι loop διαδρομές. Κάθε φορά που ένας κόμβος πρέπει να βρει μια διαδρομή σε ένα άλλο κόμβο, μεταδίδει ένα αίτημα διαδρομής (RREQ) προς όλους τους γείτονές της. Το μήνυμα RREQ κατακλύζεται μέσω του δικτύου έως ότου να φτάσει στον προορισμό. Στο δρόμο του μέσα από το δίκτυο, το μήνυμα RREQ ξεκινά τη δημιουργία προσωρινών καταχωρήσεων στο πίνακα δρομολογίων για την αντίστροφη διαδρομή στους κόμβους που περνά. Εάν ο προορισμός ή μια διαδρομή βρεθεί σε αυτό, η διαθεσιμότητά του θα υποδεικνύεται από μια απάντηση διαδρομής (RREP) το οποίο μήνυμα είναι unicast, πίσω στην πηγή κατά μήκος της προσωρινής αντίστροφης διαδρομής των ληφθέντων μηνυμάτων RREQ. Στο δρόμο της επιστροφής στην πηγή, το μήνυμα RREP εκκινεί στους ενδιάμεσους κόμβους καταχωρήσεις στο πίνακα δρομολόγησης για τον προορισμό. Με κάθε εγγραφή διαδρομής είναι συσχετισμένο ένα χρονόμετρο διαδρομής, το οποίο θα προκαλέσει τη διαγραφή της αντίστοιχης εγγραφής, αν αυτή δε χρησιμοποιείται μέσα στον προκαθορισμένο χρόνο ζωής. Επειδή το RREP προωθείται κατά μήκος του μονοπατιού που έχει εγκατασταθεί από το RREQ, ο AODV υποστηρίζει μόνο τη χρήση συμμετρικών συνδέσεων. Αν η απάντηση (RREP) δεν φτάσει μέσα σε ένα συγκεκριμένο χρονικό διάστημα, ο κόμβος μπορεί να επαναλάβει την αποστολή του RREQ μηνύματος, ή να υποθέσει ότι δεν υπάρχει κάποια διαδρομή προς τον απαιτούμενο προορισμό (Σχήμα 3.2) [7] [9] [13].



Σχήμα 3.2 Ad hoc on demand distance vector Protocol

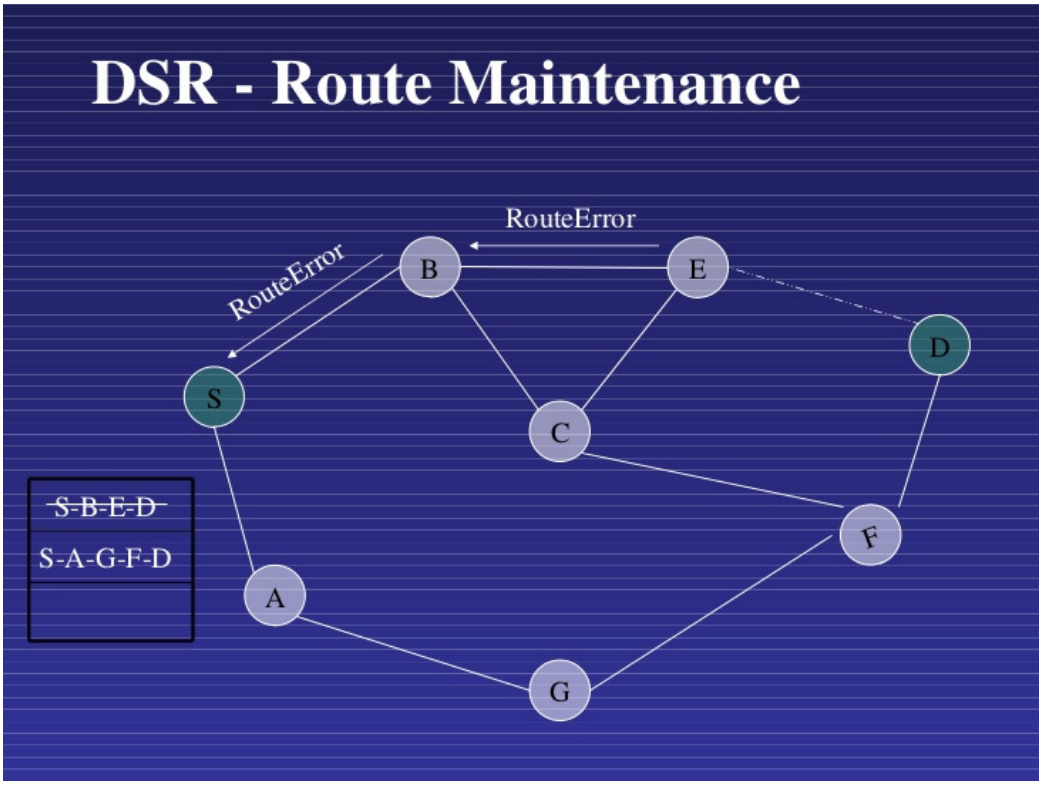
3.4.2 Dynamic source routing protocol (DSR)

Είναι ένα reactive πρωτόκολλο δρομολόγησης οποίο βασίζεται στην έννοια της δρομολόγησης πηγής κατ' απαίτηση. Το DSR είναι κατανεμημένο πρωτόκολλο αφού δεν εξαρτάται από κάποιον κεντρικοποιημένο κόμβο. Όπως και στα περισσότερα πρωτόκολλα Ad Hoc δικτύων οι εγγραφές στην κρυφή μνήμη διαδρομών ενημερώνονται συνεχώς αφού ανακαλύπτονται νέες διαδρομές.

Το πρωτόκολλο αποτελείται από δύο κύριες φάσεις: την ανακάλυψη διαδρομής και τη διατήρηση διαδρομής. Όταν ένας κινητός κόμβος θέλει να στείλει ένα πακέτο σε κάποιον προορισμό, ελέγχει την κρυφή μνήμη διαδρομών του για να καθορίσει αν ήδη έχει μια διαδρομή για τον προορισμό αυτό. Αν βρει ότι υπάρχει μια διαδρομή για τον προορισμό που δεν έχει λήξει, χρησιμοποιεί τη διαδρομή αυτή για να στείλει το πακέτο. Αν όμως ο κόμβος δεν έχει μια τέτοια διαδρομή, τότε ξεκινάει τη διαδικασία ανακάλυψης διαδρομής εκπέμποντας ένα πακέτο αίτησης διαδρομής. Αυτό το πακέτο αίτησης διαδρομής, περιέχει τη διεύθυνση της πηγής και του προορισμού και ένα μοναδικό αριθμό αναγνώρισης

ταυτότητας. Κάθε ενδιάμεσος κόμβος που λαμβάνει το πακέτο αυτό, ελέγχει αν ξέρει μια διαδρομή για τον προορισμό. Αν δεν ξέρει μια τέτοια διαδρομή, προσαρτά τη διεύθυνσή του στο αρχείο διαδρομής του πακέτου και στη συνέχεια προωθεί το πακέτο στους γείτονές του [7] [9].

Για να μειωθεί ο αριθμός των αιτήσεων διαδρομής που μεταδίδονται, ένας κόμβος προωθεί το πακέτο αίτησης διαδρομής μόνο αν δεν έχει δει ήδη το πακέτο αυτό και η διεύθυνσή του δεν εμφανίζεται ήδη στο αρχείο διαδρομής του πακέτου. Μια απάντηση διαδρομής παράγεται όταν το πακέτο αίτησης διαδρομής φτάσει είτε στον ίδιο τον προορισμό, είτε σε έναν ενδιάμεσο κόμβο που περιέχει στην κρυφή μνήμη διαδρομών του μια διαδρομή για τον προορισμό που δεν έχει λήξει. Καθώς το πακέτο αίτησης διαδρομής μεταδίδεται διαμέσου του δικτύου, σχηματίζεται το αρχείο διαδρομής. Αν η απάντηση διαδρομής παράγεται από τον προορισμό, τότε αυτός τοποθετεί το αρχείο διαδρομής, που περιέχεται στο πακέτο αίτησης διαδρομής, στο πακέτο απάντησης διαδρομής. Αν όμως ο κόμβος που παράγει την απάντηση διαδρομής είναι ένας ενδιάμεσος κόμβος, τότε αυτός προσαρτά την αποθηκευμένη του διαδρομή για τον προορισμό στο αρχείο διαδρομής του πακέτου αίτησης διαδρομής Όπως και το πρωτόκολλο AODV, έτσι και το DSR διαθέτει μηχανισμούς αποφυγής ατέρμονων βρόγχων (Σχήμα 3.3).



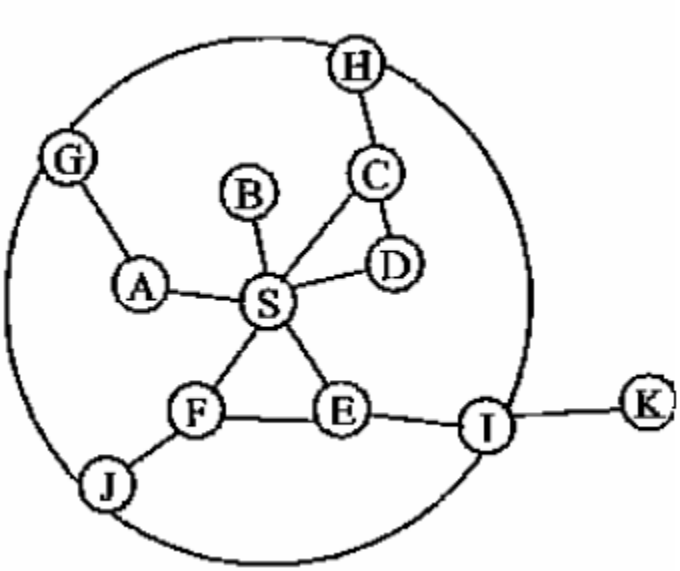
Σχήμα 3.3 Dynamic source routing protocol

3.5 Hybrid πρωτόκολλο δρομολόγησης

3.5.1 Zone Routing Protocol (ZRP)

Το ZRP είναι ένα υβριδικό πρωτόκολλο δρομολόγησης, με χαρακτηριστικά reactive και proactive πρωτοκόλλου. Ενσωματώνει τις δυνατότητες των κατόπιν παραγγελίας και δυναμικών πρωτοκόλλων δρομολόγησης. Στο ZRP, μία ζώνη δρομολόγησης αποτελείται από μερικούς κινητούς κόμβους μέσα στα πλαίσια ενός, δύο, ή περισσοτέρων αλμάτων μακριά από τον κεντρικό κόμβο. Το μέγεθος μιας επιλεγμένης ζώνης μπορεί, επομένως, να επηρεάσει την απόδοση της επικοινωνίας ad hoc. Μια ζώνη δρομολόγησης καθορίζεται για κάθε κόμβο ξεχωριστά και οι ζώνες γειτονικών κόμβων επικαλύπτουν η μία την άλλη. Η ζώνη δρομολόγησης έχει μια ακτίνα ρ εκφρασμένη σε **βήματα (hops).** Έτσι η ζώνη περιλαμβάνει τους κόμβους εκείνους, των οποίων η απόσταση από τον αντίστοιχο κόμβο (τον κόμβο στον οποίο αντιστοιχεί η συγκεκριμένη ζώνη δρομολόγησης) είναι το πολύ ρ βήματα.

Ένα παράδειγμα μιας ζώνης δρομολόγησης φαίνεται στο παρακάτω σχήμα, όπου η ζώνη δρομολόγησης του S περιλαμβάνει τους κόμβους A-I, αλλά όχι τον K. Στις εικόνες, η ακτίνα σημειώνεται σαν ένας κύκλος γύρω από τον συγκεκριμένο κόμβο. Θα πρέπει όμως παρόλα αυτά να σημειωθεί ότι η ζώνη καθορίζεται με βάση τα βήματα (hops), όχι με βάση τη φυσική απόσταση [14] [16].



Σχήμα 3.4 Zone Routing Protocol με ρ=2

Οι κόμβοι μιας ζώνης διαιρούνται σε περιφερειακούς και εσωτερικούς κόμβους. Οι περιφερειακοί είναι κόμβοι των οποίων η ελάχιστη απόσταση από τον κεντρικό κόμβο είναι

ακριβώς ίση με την ακτίνα ρ της ζώνης. Οι κόμβοι των οποίων η ελάχιστη απόσταση είναι μικρότερη από την ρ είναι εσωτερικοί κόμβοι. Στο Σχήμα 3.4, οι κόμβοι A-F είναι εσωτερικοί κόμβοι, οι κόμβοι G- J είναι περιφερειακοί κόμβοι και ο κόμβος K βρίσκεται εκτός της ζώνης δρομολόγησης. Σημειώνουμε ότι ο κόμβος H μπορεί να προσεγγιστεί μέσω δύο μονοπατιών (από τον S), το ένα με μήκος 2 hops και το άλλο με μήκος 3 hops .Παρόλα αυτά, ο κόμβος είναι μέσα στη ζώνη, εφόσον το μικρότερο μονοπάτι είναι μικρότερο ή ίσο με την ακτίνα της ζώνης.

Το ZRP έχει τρία υπό-πρωτόκολλα: [15]

- το proactive Intrazone Routing Protocol (IARP),
- το reactive Interzone Routing Protocol (IERP),
- το Bordercast Resolution Protocol (BRP).

Το IARP μπορεί να εφαρμοστεί χρησιμοποιώντας μεθόδους δρομολόγησης που βασίζονται στις καταστάσεις των ζεύξεων και στα διανύσματα απόστασης. Η παραγόμενη πληροφορία δρομολόγησης διαδίδεται μέχρι το σύνορο της ζώνης δρομολόγησης και όχι σε όλο το δίκτυο. Το IARP στηρίζεται σε ένα υποκείμενο πρωτόκολλο ανεύρεσης γειτόνων για την ανίχνευση της παρουσίας και απουσίας γειτονικών κόμβων, κι επομένως, την αξιολόγηση της συνδεσιμότητας των ζεύξεων αυτών των κόμβων. Ο βασικός του ρόλος είναι η διασφάλιση ότι κάθε κόμβος μέσα στην ζώνη έχει ένα συνεκτικό πίνακα δρομολόγησης που είναι πλήρως, εγκαίρως και επαρκώς ενημερωμένος, ενώ ταυτόχρονα απεικονίζει την πληροφορία για το πώς κάποιο κινητό μπορεί να φθάσει οποιοδήποτε άλλο κόμβο μέσα στην ζώνη.

Το IERP, από την άλλη πλευρά, στηρίζεται στους συνοριακούς κινητούς σταθμούς οι οποίοι είναι υπεύθυνοι για την εκτέλεση του reactive κομματιού δρομολόγησης για να βρεθεί η απαραίτητη πληροφορία για τα κινητά που ανήκουν σε άλλες ζώνες. Αντί να επιτρέπεται η εκπομπή των αιτήσεων στο σύνολο των κόμβων μέσα στις άλλες ζώνες, οι συνοριακοί σταθμοί σε άλλες ζώνες που λαμβάνουν αυτό το μήνυμα δεν θα το προωθήσουν περαιτέρω. Το IERP χρησιμοποιεί το πρωτόκολλο ανάλυσης της συνοριακής εκπομπής.

Επειδή σε μέρη ενός ad hoc δρόμου εφαρμόζονται διαφορετικά πρωτόκολλα δρομολόγησης, τα χαρακτηριστικά αυτών θα είναι στην ουσία διαφορετικά. Μερικά μέρη της διαδρομής εξαρτώνται από την καθαυτή σύγκλιση του δρόμου, ενώ τα υπόλοιπα εξαρτώνται από το κατά πόσο ακριβής είναι η ευρεθείσα διαδρομή μέσα στα όρια της ίδιας της ζώνης. Αυτό μπορεί να εξασφαλίσει τη σταθερότητα ενός δρόμου με ιδιαίτερη δυσκολία.

Ένας κόμβος ο οποίος θέλει να στείλει ένα πακέτο σε έναν άλλο κόμβο, ελέγχει πρώτα αν ο προορισμός βρίσκεται εντός της τοπικής του ζώνης δρομολόγησης, χρησιμοποιώντας πληροφορίες που παρέχονται από το IARP. Στην περίπτωση αυτή, το πακέτο μπορεί να δρομολογηθεί proactive. Reactive δρομολόγηση χρησιμοποιείται αν ο προορισμός βρίσκεται εκτός της ζώνης. Η reactive διαδικασία δρομολόγησης διαιρείται σε δύο φάσεις: τη φάση αίτησης διαδρομής (route request) και τη φάση απάντησης διαδρομής (route reply).

- Στην αίτηση διαδρομής, η πηγή στέλνει ένα πακέτο αίτησης διαδρομής στους περιφερειακούς της κόμβους χρησιμοποιώντας το BRP. Αν ο δέκτης ενός πακέτου αίτησης διαδρομής ξέρει ένα μονοπάτι για τον προορισμό, απαντά στέλνοντας μια απάντηση διαδρομής στον αποστολέα. Διαφορετικά, συνεχίζει την ίδια διαδικασία στέλνοντας το πακέτο στους περιφερειακούς του κόμβους. Με τον τρόπο αυτό, η αίτηση διαδρομής διαδίδεται μέσα στο δίκτυο μέχρι να βρεθεί ο ζητούμενος κόμβος (προορισμός) ή κάποιος κόμβος που γνωρίζει κάποιο μονοπάτι για τον προορισμό, οποιοσδήποτε από τους οποίους στέλνει μια απάντηση διαδρομής πίσω στον αποστολέα, υποδεικνύοντας του τη διαδρομή. Αν κάποιος κόμβος λάβει περισσότερα από ένα αντίγραφα της ίδιας αίτησης διαδρομής, αυτά θεωρούνται ως πλεονάζοντα και απορρίπτονται.
- Η απάντηση διαδρομής μπορεί να σταλεί από οποιονδήποτε κόμβο ο οποίος μπορεί να παρέχει μια διαδρομή για τον προορισμό. Για να μπορεί να σταλεί μια απάντηση πίσω στον κόμβο αποστολέα, θα πρέπει να συσσωρεύονται οι πληροφορίες δρομολόγησης, καθώς η αίτηση διαδρομής στέλνεται διαμέσου του δικτύου. Οι πληροφορίες αυτές καταγράφονται είτε στο πακέτο αίτησης διαδρομής, είτε σαν διευθύνσεις επόμενου βήματος στους κόμβους κατά μήκος του μονοπατιού.

Η διατήρηση της διαδρομής, είναι ένα θέμα το οποίο είναι ιδιαίτερα σημαντικό στα ad hoc δίκτυα, στα οποία οι συνδέσεις σπάνε και εγκαθίστανται καθώς οι κόμβοι κινούνται ο ένας σε σχέση με τον άλλο. Στο ZRP, η γνώση της τοπικής τοπολογίας μπορεί να χρησιμοποιηθεί για τη διατήρηση της διαδρομής.. Εισερχόμενα πακέτα μπορούν να κατευθυνθούν γύρω από τη σπασμένη σύνδεση μέσω ενός ενεργού μονοπατιού πολλαπλών βημάτων. Παρομοίως, η τοπολογία μπορεί να χρησιμοποιηθεί για να μικρύνει διαδρομές, για παράδειγμα, όταν δύο κόμβοι έχουν μετακινηθεί ο ένας μέσα στο εύρος κάλυψης του άλλου. Κάποιες φορές, ένα τμήμα πολλαπλών βημάτων μπορεί να αντικατασταθεί από ένα μόνο βήμα.

ΚΕΦΑΛΑΙΟ 4

ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ- ΤΕΧΝΟΛΟΓΙΕΣ ADHOC ΔΙΚΤΥΩΝ

4.1 Πρότυπο 802.11

Το πρωτόκολλο **802.11** είναι αποτέλεσμα της ομάδας εργασίας του **IEEE** που αφορούσε ασύρματα τοπικά δίκτυα (Wireless LAN-WLAN). Πρωταρχικός στόχος της ομάδας ήταν η κατάργηση των καλωδίων ανάμεσα στους υπολογιστές σε ένα τοπικό δίκτυο .

Το 802.11 υποστηρίζει τόσο την **δισημειακή (point to point) επικοινωνία**, όσο και την **επικοινωνία σημείου προς πολλαπλά σημεία (poin to multipoint).** Έτσι οι υπολογιστές που βρίσκονται στον ίδιο χώρο μπορούν να οργανωθούν σε κατάσταση ad hoc με στόχο την άμεση επικοινωνία τους. Η ανάγκη για ασύρματο δίκτυο προκύπτει όταν χρειάζεται να υπάρχει επικοινωνία με ενσύρματα δίκτυα, περιφερειακά, ή στην περίπτωση της περιαγωγής (roaming), δηλαδή όταν ο χρήστης ενός φορητού υπολογιστή πρέπει να κινείται σε ένα κτίριο. Το IEEE 802.11 ορίζει δύο φυσικά χαρακτηριστικά για ασύρματα τοπικά δίκτυα: **direct-sequence spread spectrum(DSSS**), και **frequency hopping spread spectrum (FHSS)**, τα οποία λειτουργούν στη μπάντα των 2.4 GHz.

Το 802.11 ορίζει δύο στοιχεία εξοπλισμού: Έναν **ασύρματο σταθμό**, ο οποίος είναι συνήθως ένας προσωπικός υπολογιστής εφοδιασμένος με μία κάρτα δικτύου διασύνδεσης (network interface controller - NIC) για ασύρματα δίκτυα και έναν πομποδέκτη ή **σημείο πρόσβασης** (AP), που συμπεριφέρεται ως γέφυρα μεταξύ του ενσύρματου και του ασύρματου δικτύου [16].

4.1.1 Τοπολογίες δικτύου στο πρότυπο 802.11

Το πρότυπο 802.11 διακρίνεται σε δύο τοπολογίες δικτύου: την **τοπολογία με δίκτυο υποδομής** και την **ad hoc δικτύωση** [2].

- **Στην τοπολογία με δίκτυο υποδομής** τα κινητά τερματικά επικοινωνούν με το δίκτυο κορμού μέσω ενός σημείου πρόσβασης (Access Point, AP). Η περιοχή που καλύπτεται από ένα AP καλείται βασική περιοχή εξυπηρέτησης (Basic Service Area, BSA)και το σύνολο των κινητών σταθμών που ελέγχονται από ένα AP αποτελεί τη βασική ομάδα εξυπηρέτησης (Basic Service Set, BSS). Πολλές BSS συνδεόμενες με κοινό δίκτυο κορμού σχηματίζουν μια ενιαία υποδομή που ονομάζεται εκτεταμένη ομάδα εξυπηρέτησης (Extended Service Set, ESS). Ένα κινητό τερματικό μπορεί να

περιφέρεται σε διαφορετικές BSS μιας ESS χωρίς να χάνει τη σύνδεση του με το δίκτυο κορμού. Στην τυπική εφαρμογή αυτής της τοπολογίας, μια ομάδα από φορητούς υπολογιστές συνδέεται μέσω ενός WLAN σε ένα ενσύρματο LAN κορμού.

- **Στην ad hoc δικτύωση** τα κινητά τερματικά επικοινωνούν μεταξύ τους σε ανεξάρτητη BSS χωρίς σύνδεση προς το ενσύρματο δίκτυο κορμού. Στην περίπτωση αυτή μερικές από τις λειτουργίες του AP που χρειάζονται για τον σχηματισμό και τη διατήρηση μιας BSS παρέχονται από ένα κινητό τερματικό. **Επιπλέον με τη μέθοδο πολλαπλής πρόσβασης CSMA/CA παρέχει και ένα μηχανισμό με προτεραιότητες χωρίς ανταγωνισμό και ελεγχόμενο από ένα σημείο.**

4.1.2 Τρόποι αρχιτεκτονικής δικτύου στο πρότυπο IEEE 802.11

Δύο τρόποι αρχιτεκτονικής του δικτύου έχουν οριστεί στο πρότυπο IEEE 802.11.**Η λειτουργία σημειακού συντονισμού, point coordination function (PCF) και η λειτουργία κατανεμημένου συντονισμού, distributed coordination function (DCF)**. Ο πρώτος τρόπος PCF χρησιμοποιεί μια συγκεντρωτική προσέγγιση στην οποία ένα σημείο πρόσβασης ελέγχει όλη την κίνηση στο δίκτυο, συμπεριλαμβανομένης της τοπικής κυκλοφορίας μεταξύ των ασυρμάτων πελατών στο δίκτυο. Η λειτουργία DCF υποστηρίζει την άμεση επικοινωνία μεταξύ των πελατών ασύρματου δικτύου. Το DCF είναι η βάση για όλους τους σταθμούς, αναφορικά με την πρόσβαση στο μέσο, και χρησιμοποιείται και στα δίκτυα που έχουν, αλλά και σε αυτά που δεν έχουν, σταθερή δομή.

Στην περίπτωση σταθερής δομής, η επικοινωνία μπορεί να ελεγχθεί από το PCF χρησιμοποιώντας τις υπηρεσίες DCF. Το PC βρίσκεται στο σημείο πρόσβασης. Προγραμματίζει μία περίοδο ελεύθερη από συγκρούσεις, που την ανακοινώνει στέλνοντας ένα beacon πλαίσιο μετά σε χρόνο (Short Interframe Space – SIFS) υποδεικνύοντας υψηλότερη προτεραιότητα από ότι τα συνηθισμένα πακέτα συναγωνισμού. Επιπλέον, διατηρεί μία λίστα με τους σταθμούς που έχουν ζητήσει να ρωτηθούν κατά την διάρκεια της περιόδου που είναι ελεύθερη από συγκρούσεις, και τους ρωτά. Ο σταθμός μεταφράζει την απόκριση αυτή ως μία παραχώρηση πόρων για την επικοινωνία με άλλον σταθμό. Επομένως, θα μπορούσε να προσφερθεί και QoS.

Το επίπεδο ελέγχου πρόσβασης μέσου (media access control - MAC) χρησιμοποιεί τον αλγόριθμο λογικής πολλαπλής πρόσβασης με ανίχνευση φέροντος και με αποφυγή

σύγκρουσης carrier-sense multiple access with collision avoidance (CSMA/CA). Για την αντιμετώπιση του προβλήματος των κρυμμένων τερματικών το πρωτόκολλο MAC διαθέτει μηχανισμό με μηνύματα request-to-send/clear-to-send (RTS/CTS).

Ένα τερματικό που λειτουργεί σε DCF τρόπο όταν θέλει να στείλει δεδομένα ακούει για να επιβεβαιώσει ότι το κανάλι είναι ελεύθερο και στη συνέχεια περιμένει για μια τυχαία χρονική περίοδο (backoff). Αν κανένας άλλος σταθμός δεν επιχειρήσει να αποκτήσει πρόσβαση μετά την περίοδο αναμονής, το τερματικό μπορεί να αποκτήσει πρόσβαση σύμφωνα με μία από τις δύο λειτουργίες: [7]

- Με handshake ο κόμβος στέλνει ένα πακέτο αίτησης request to send (RTS) στο τερματικό υποδοχής. Αν ο δέκτης δέχεται το αίτημα, απαντάει με ένα πακέτο clear to send(CTS). Αν δεν έχουν συμβεί συγκρούσεις, ο αποστολέας τότε αρχίζει τη μετάδοση των δεδομένων του.
- Ο αποστολέας ξεκινά αμέσως την αποστολή των δεδομένων του. Αυτή η λειτουργία χρησιμοποιείται όταν τα δεδομένα πακέτων είναι σύντομα.

Σε κάθε τρόπο λειτουργίας, ο δέκτης αποκρίνεται με μια αναγνώριση acknowledgement(ACK) πακέτων, αν το πακέτο ελήφθη επιτυχώς. Ο μηχανισμός CSMA / CA δραστηριοποιείται επίσης για την PCF λειτουργία. Ωστόσο, επειδή το σημείο πρόσβασης έχει μεγαλύτερη προτεραιότητα από τους τερματικούς σταθμούς, έχει τον απόλυτο έλεγχο του καναλιού. Το πρότυπο IEEE 802.11 δεν προσδιορίζει μια μέθοδο για multihop ad hoc δικτύωση. Ωστόσο, σε αρκετά πειραματικά δίκτυα MANET με βάση δρομολόγησης IP έχει χρησιμοποιηθεί.

4.1.3 Πρότυπα που ανήκουν στην οικογένεια του IEEE 802.11

IEEE 802.11

Το αρχικό πρότυπο IEEE 802.11 δημοσιεύθηκε το 1997 από την IEEE, μετά από επτά χρόνια μελέτης. Προβλέπει ρυθμούς μετάδοσης 1 και 2 Mbps. Υποστηρίζει ασύγχρονη, connectionless υπηρεσία. Στο φυσικό επίπεδο προβλέπει τεχνικές απλωμένου φάσματος **FHSS (Frequency Hopping Spread Spectrum)** και **DSSS (Direct Sequence Spread Spectrum)** σε ζώνες συχνοτήτων 915MHz, 2.4MHz, 5.2MHz καθώς και υπέρυθρης ακτινοβολίας (**diffused infrared, DFIR)** στα 850nm ως 900nm. Υποστηρίζει δυνατότητες όπως κατανομή προτεραιοτήτων της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής. Στη συνέχεια έχουν προκύψει αρκετές εκδόσεις του προτύπου IEEE

802.11. Όλες οι εκδόσεις υποστηρίζουν το ίδιο στρώμα MAC, το οποίο χρησιμοποιεί πολλαπλή πρόσβαση με ανίχνευση φέροντος και αποφυγή συγκρούσεων (CSMA/CA) [4].

IEEE 802.11a

Το πρότυπο 802.11a εισήλθε στην αγορά αφού το 802.11b είχε ήδη ένα μεγάλο μερίδιο αυτής. Παρόλα αυτά η τεχνολογία που χρησιμοποιεί προσφέρει αρκετά πλεονεκτήματα σε σχέση με αυτή του 802.11b. Χρησιμοποιεί τις μπάντες UNII στα 5 Ghz για μετάδοση που είναι γενικά πολύ λιγότερο χρησιμοποιούμενη από αυτή των 2,4 Ghz, οπότε και με λιγότερες παρεμβολές. Οι τρεις μπάντες UNII χωρίζονται με τρόπο σχετικό με την καταλληλότητα τους για μετάδοση σε εσωτερικά ή εξωτερικά περιβάλλοντα και επιτρέπουν την δημιουργία μακρινών ασύρματων ζεύξεων σε μεγάλες ταχύτητες. Το 802.11a παρέχει ταχύτητες μέχρι 54 mpbs (ωφέλιμο περί τα 25 mpbs), μια αύξηση στην ταχύτητα πέντε φορές από το 802.11b. Αυτό καθίσταται δυνατό λόγω μιας ανώτερης τεχνικής διαμόρφωσης των ραδιοκυμάτων που λέγεται **OFDM (Orthogonal Frequency Division Multiplexing)**. Παρόλα αυτά οι υψηλότερες ραδιοσυχνότητες μειώνουν κατά πολύ την απόσταση κάλυψης καθώς και την διεισδυτική δύναμη του 802.11a, ειδικά σε εσωτερικούς χώρους. Εκεί που μια μετάδοση 802.11b θα περνούσε έναν τοίχο, μια μετάδοση 802.11a μπορεί να εμποδιστεί. Το γεγονός αυτό μπορεί να εμποδίσει την εγκατάσταση σε μεγάλη κλίμακα ενός δικτύου 802.11a καθώς απαιτούνται πιο πολλά Access Points για την κάλυψη του χώρου.

IEEE 802.11b

Είναι το πρώτο πρότυπο που χρησιμοποιήθηκε ευρέως στα τοπικά ασύρματα δίκτυα. Είναι σε γενικές γραμμές μια τεχνολογία μικροκυμάτων που χρησιμοποιεί την **μπάντα ISM** στα **2.83 Ghz** για επικοινωνία χωρίζοντας το εύρος των συχνοτήτων σε τρεις μη αλληλοκαλυπτόμενες περιοχές (κανάλια).Η συγκεκριμένη μπάντα χρησιμοποιείται ευρέως από συσκευές όπως ασύρματα τηλέφωνα και φούρνους μικροκυμάτων. Το 802.11b παρέχει ταχύτητες 11Mbps σε half-duplex οι οποίες μοιράζονται μεταξύ όλων των σταθμών που συνδέονται στο ίδια ασύρματη βάση (Access Point). Λόγω επιβαρύνσεων στη μεταδιδόμενη πληροφορία από τα πρωτόκολλα διασύνδεσης, το ωφέλιμο bandwidth μειώνεται στα 6Mbps. Η τυπική απόσταση μεταξύ συσκευών είναι περί τα 30 μέτρα σε εσωτερικό χώρο και πάνω από 120 μέτρα σε εξωτερικό χώρο. Αυτές οι αποστάσεις μπορούν να αυξηθούν τοποθετώντας εξωτερικές κεραίες που ενισχύουν το σήμα.

IEEE 802.11g

Το 802.11g είναι στην πραγματικότητα μια τροποποίηση του πρότυπου 802.11b επιτρέποντας ταχύτητες 54 Mbps στην μπάντα ISM των 2,4 Ghz χρησιμοποιώντας την διαμόρφωση σήματος που χρησιμοποιεί και το πρότυπο 802.11a. Το 802.11g αντιμετωπίζει τους περιορισμούς σε bandwidth του 802.11b και παράλληλα προσφέρει την διεισδυτική δύναμη της μπάντας των μικροκυμάτων καθώς και την ικανότητα μετάδοσης σε μεγάλες αποστάσεις. Παρόλα αυτά δεν περιορίζει το πρόβλημα της συμφόρησης στην συγκεκριμένη μπάντα στην οποία λειτουργούνε πολλές συσκευές. Το 802.11g είναι επίσης περιορισμένο σε τρία μη αλληλοεπικαλυπτόμενα κανάλια όπως και ο προκάτοχος του , το 802.11b. Το 802.11g μπορεί να έχει τα ίδια προβλήματα απόδοσης όπως και το 802.11b λόγω της συμβατότητας προς τα πίσω που έχει. Εάν ένας σταθμός 802.11b είναι παρών σε ένα δίκτυο 802.11g , όλοι οι σταθμοί θα πρέπει να χρησιμοποιήσουν την διαμόρφωση σήματος του 802.11b για συμβατότητα.

IEEE 802.11n

Το πρότυπο αυτό το οποίο εφαρμόζει τη χρήση πολλαπλών κεραιών, μέθοδος γνωστή ως **MIMO (Multiple Inputs Multiple Outputs),** δύναται να παρέχει ονομαστικό ρυθμό μετάδοσης με ταχύτητες μέχρι 135 Mbps.. Επιπλέον ενσωματώνει νέες τεχνολογίες οι οποίες του επιτρέπουν να συνυπάρχει με συσκευές οι οποίες λειτουργούν με τα προαναφερθέντα πρότυπα χωρίς να επηρεάζεται η λειτουργία του.

Νέες τεχνολογίες IEEE 802.11

Από το 2012 αναπτύσσονται νέα πρότυπα της ασύρματης τοπικής δικτύωσης από τον οργανισμό IEEE τα οποία παρουσιάζουν μεγάλο ακαδημαϊκό ενδιαφέρον και υπόσχονται σημαντικά γρηγορότερες ταχύτητες μετάδοσης ακόμη και μέχρι 100 Gbps. Τα νέα αυτά πρότυπα είναι, IEEE 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj, 802.11aq, 802.11ax, 802.11ay.

Τα βασικότερα πρότυπα WLAN της σειράς IEEE802.11 και τα κυριότερα χαρακτηριστικά τους παρατίθενται στον Πίνακα 4.1

V·T·E	802.11 network PHY standards					
802.11 protocol	Release date[6]	Fre-quency	Band-width	Stream data rate[7]	Allowable MIMO streams	Modulation
		(GHz)	(MHz)	(Mbit/s)		
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS
a	Sep 1999	5 3.7[A]	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM
n	Oct 2009	2.4/5	20	400 ns GI : 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 [B] 800 ns GI : 6.5, 13, 19.5, 26, 39, 52, 58.5, 65 [C]	4	MIMO-OFDM
			40	400 ns GI : 15, 30, 45, 60, 90, 120, 135, 150 [B] 800 ns GI : 13.5, 27, 40.5, 54, 81, 108, 121.5, 135 [C]		
ac	Dec 2013	5	20	400 ns GI : 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3 [B] 800 ns GI : 6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 86.7 [C]	8	
			40	400 ns GI : 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 [B] 800 ns GI : 13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180 [C]		
			80	400 ns GI : 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 [B] 800 ns GI : 29.2, 58.5, 87.8, 117, 175.5, 234, 263.2, 292.5, 351, 390 [C]		
			160	400 ns GI : 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 [B] 800 ns GI : 58.5, 117, 175.5, 234, 351, 468, 702, 780 [C]		
ad	Dec 2012	60	2,160	Up to 6,912 (6.75 Gbit/s) [10]	N/A	OFDM, single carrier, low-power single carrier
ah	Est. 2016[6]	0.9				
aj	Est. 2016[6]	45/60				
ax	Est. 2019[6]	2.4/5				MIMO-OFDM
ay	2017	60	8000	Up to 100,000 (100 Gbit/s)	4	OFDM, single carrier,

Πίνακας 4.1 Πρότυπα WLAN της σειράς IEEE 802.11.

4.2 Πρότυπο HIPERLAN-2

Το πρότυπο HIPERLAN-2 υποστηρίζει δύο τρόπους λειτουργίας, τον **κεντρικό τρόπο και τον άμεσο** [2]**.** Ο κεντρικός τρόπος λειτουργίας χρησιμοποιείται στην κυψελωτή τοπολογία δικτύου, όπου κάθε κυψέλη ελέγχεται από ένα σημείο πρόσβασης (AP), που καλύπτει ασύρματα συγκεκριμένη γεωγραφική περιοχή. Στην κυψελωτή τοπολογία ένα κινητό τερματικό επικοινωνεί με άλλα κινητά τερματικά ή με το δίκτυο κορμού μέσω του AP. Ο χρήστης ενός κινητού τερματικού μπορεί να κυκλοφορεί ελεύθερα στο δίκτυο του HIPERLAN/ 2, το οποίο εξασφαλίζει ότι το τερματικό, και ως εκ τούτου, ο χρήστης, παίρνει την καλύτερη δυνατή απόδοση μετάδοσης. Ο κεντρικός τρόπος λειτουργίας χρησιμοποιείται κυρίως σε δίκτυα επιχειρήσεων, τόσο σε εσωτερικούς όσο και σε εξωτερικούς χώρους, όπου πρέπει να καλυφθεί γεωγραφική έκταση μεγαλύτερη από εκείνη της μίας κυψέλης.

Ο άμεσος τρόπος λειτουργίας χρησιμοποιείται στην ad hoc τοπολογία δικτύου, η οποία συνηθίζεται κυρίως σε ιδιωτικές κατοικίες , όπου η κυψέλη καλύπτει ολόκληρη την περιοχή εξυπηρέτησης . Με αυτόν τον τρόπο τα κινητά τερματικά σε ένα ad hoc δίκτυο μπορούν άμεσα να ανταλλάσσουν δεδομένα. Το σημείο πρόσβασης πρέπει να ελέγχει την επικοινωνία μεταξύ κινητών τερματικών ακόμη και αν η ραδιοζεύξη είναι άμεση μεταξύ των κόμβων. Έτσι, οποιαδήποτε δύο κινητά τερματικά Hiperlan-2 δικτύου δεν μπορούν να επικοινωνήσουν σε ad hoc βάση χωρίς να έχει ένα σημείο πρόσβασης. Αυτό διαφέρει στο τρόπο διαχείρισης ad hoc επικοινωνίας από το πρότυπο IEEE 802.11. Και στις δύο περιπτώσεις η πρόσβαση στο μέσο μετάδοσης καθώς και η εκχώρηση ασύρματων πόρων στα κινητά τερματικά ελέγχονται από το AP.

Η ανάπτυξη ενός περιβάλλοντος υψηλής ταχύτητας μετάδοσης με ελεγχόμενη QoS αποτέλεσε το επίκεντρο όσον αφορά τις επιλογές σχεδιασμού για το δίκτυο H2. Ο ρυθμός μετάδοσης του H2 δικτύου θα δώσει μέχρι και 54 Mbit /s στο επίπεδο 3 και θα λειτουργεί στη ζώνη συχνοτήτων των 5 GHz. Η προσανατολισμένη σύνδεση του H2 καθιστά εύκολο να υποστηρίξει την εφαρμογή του QoS. Σε κάθε σύνδεση μπορεί να ανατεθεί μια συγκεκριμένη QoS, για παράδειγμα, από την άποψη του εύρους ζώνης, την καθυστέρηση, και το ποσοστό σφάλματος bit. Είναι επίσης δυνατό να χρησιμοποιηθεί μια πιο απλή προσέγγιση, όπου στην κάθε σύνδεση μπορεί να εκχωρηθεί ένα επίπεδο προτεραιότητας σε σχέση με τις άλλες συνδέσεις. Αυτό το είδος της υποστήριξης QoS σε συνδυασμό με το ποσοστό υψηλής μετάδοσης θα διευκολύνει την ταυτόχρονη μετάδοση πολλών διαφορετικών τύπων δεδομένων, όπως βίντεο και φωνής [7].

Το φυσικό στρώμα του HYPERLAN-2 χρησιμοποιεί ορθογωνική πολυπλεξία διαίρεση συχνότητας (Orthogonal Frequency Division Multiplexing, OFDM). Η απόσταση μεταξύ των φερουσών συχνοτήτων είναι 20 MHzώστε να είναι δυνατό να υπάρξουν αρκετοί δίαυλοι στο εύρος ζώνης των 100 MHz, που είναι πολλές φορές το ελάχιστο διαθέσιμο μονοκόμματο εύρος ζώνης. Η απόσταση των υποφερουσών (subcarriers) συχνοτήτων που επιτυγχάνονται είναι 312,5 KHz. Για να διευκολυνθεί η χρησιμοποίηση φίλτρων και να επιτευχθεί επαρκής απομόνωση μεταξύ γειτονικών διαύλων, χρησιμοποιούνται 52 υποφέρουσες ανά δίαυλο, από τις οποίες 48 χρησιμοποιούνται για δεδομένα και οι 4 είναι πιλότοι που διευκολύνουν την ομόδυνη αποδιαμόρφωση.

Ένα κύριο χαρακτηριστικό του φυσικού στρώματος είναι ότι υποστηρίζει πολλούς τρόπους λειτουργίας με διαφορετικούς ρυθμούς κωδικοποίησης και διαφορετικά σχήματα διαμόρφωσης. Τα σχήματα διαμόρφωσης που υποστηρίζονται είναι BPSK, QPSK, 16-QAM,

64-QAM ενώ οι ρυθμοί κωδικοποίησης είναι 1/2, 3/4, και 9/16. Στον Πίνακα 4.2 φαίνονται οι επτά τρόποι λειτουργίας φυσικού στρώματος που έχουν προδιαγραφεί, αναφορικά με τα σχήματα διαμόρφωσης και τους ρυθμούς κωδικοποίησης [2].

Table 1: PHY modes defined for HIPERLAN/2.

Mode	Modulation	Code rate	PHY bit rate	bytes/OFDM
1	BPSK	1/2	6 Mbps	3.0
2	BPSK	3/4	9 Mbps	4.5
3	QPSK	1/2	12 Mbps	6.0
4	QPSK	3/4	18 Mbps	9.0
5	16QAM	9/16	27 Mbps	13.5
6	16QAM	3/4	36 Mbps	18.0
7	64QAM	3/4	54 Mbps	27.0

Πίνακας 4.2 Τρόποι λειτουργίας του φυσικού στρώματος HIPERLAN-2

4.2.1 Χαρακτηριστικά Στοιχεία του HIPERLAN-2

Υποστήριξη QoS

Η φύση του HIPERLAN-2 με τις προσφερόμενες υπηρεσίες με σύνδεση, καθιστούν άμεση την εφαρμογή παραμέτρων για την υποστήριξη του QoS. Σε κάθε σύνδεση μπορεί να ανατεθεί μία συγκεκριμένη τιμή για QoS, για παράδειγμα σε όρους εύρους ζώνης, καθυστέρησης, μεταβλητότητας, ρυθμού σφαλμάτων, κ.τ.λ. Είναι, επίσης, δυνατή η χρήση μίας πιο απλοϊκής προσέγγισης, όπου σε κάθε σύνδεση μπορεί να παραχωρηθεί ένα επίπεδο προτεραιότητας σε σχέση με τις άλλες συνδέσεις. Αυτή η υποστήριξη του QoS σε συνδυασμό με τον υψηλό ρυθμό μετάδοσης καθιστά πιο εύκολη την ταυτόχρονη εκπομπή πολλών διαφορετικών τύπων ροής πληροφορίας, π.χ. video, φωνή και δεδομένα [7].

Υποστήριξη ασφάλειας

Το HIPERLAN-2 δίκτυο έχει την δυνατότητα υποστήριξης πιστοποίησης και κρυπτογράφησης. Με την διαδικασία της πιστοποίησης τόσο το σημείο πρόσβασης όσο και το κινητό τερματικό μπορούν να πιστοποιήσουν το ένα το άλλο ώστε να διασφαλίσουν διαπιστευμένη πρόσβαση στο δίκτυο (από την πλευρά του σημείου πρόσβασης) ή να εξασφαλίσουν πρόσβαση σε έναν έγκυρο παροχέα υπηρεσιών του δικτύου (από την

πλευρά του κινητού τερματικού). Η πιστοποίηση στηρίζεται στην ύπαρξη μίας βοηθητικής λειτουργίας, όπως μία υπηρεσία καταλόγου που, όμως, είναι έξω από τους σκοπούς του HIPERLAN-2. Η κίνηση των δεδομένων στις συνδέσεις που έχουν εγκατασταθεί μπορεί να κρυπτογραφηθεί για την προστασία απέναντι, για παράδειγμα, στις περιπτώσεις υποκλοπών.

Ανεξαρτησία από άλλα δίκτυα και εφαρμογές

Η στοίβα πρωτοκόλλων του HIPERLAN-2 έχει μία ελαστική αρχιτεκτονική για την εύκολη προσαρμογή και ενσωμάτωση με μία ποικιλία από σταθερά δίκτυα. Ένα HIPERLAN/2 δίκτυο μπορεί, για παράδειγμα, να χρησιμοποιηθεί ως ένα δίκτυο πρόσβασης για τα κυψελωτά δίκτυα τρίτης γενιάς ή για οποιαδήποτε άλλη διαμόρφωση. Όλες οι εφαρμογές που υφίστανται, σήμερα, για σταθερές δομές δικτύου μπορούν, επίσης, να “τρέξουν” πάνω από το δίκτυο HIPERLAN/2.

Εξοικονόμηση ισχύος

Στο HIPERLAN-2, ο μηχανισμός που επιτρέπει σε ένα κινητό τερματικό να εξοικονομεί ισχύ βασίζεται σε μία διαπραγμάτευση ανενεργών περιόδων που εκκινούνται από την συσκευή. Το κινητό τερματικό μπορεί σε οποιαδήποτε στιγμή να ζητά από το σημείο πρόσβασης να εισέλθει στην κατάσταση χαμηλής ισχύος (συγκεκριμένη για κάθε συσκευή), και ζητά μία συγκεκριμένη περίοδο κατά την οποία θα μείνει ανενεργό. Κατά την εκπνοή αυτού του χρονικού διαστήματος, το κινητό τερματικό ψάχνει για την παρουσία κάποιας ένδειξης ενεργοποίησης από πλευράς του σημείου πρόσβασης. Όταν η συσκευή δεν έχει λάβει μία τέτοια ένδειξη επανέρχεται, εκ νέου, στην κατάσταση χαμηλής ισχύος για την διάρκεια της επόμενης ανενεργής περιόδου, και συνεχίζει με τον ίδιο τρόπο. Ένα σημείο πρόσβασης θα αναβάλλει κάθε πληροφορία που εκκρεμεί προς έναν κινητό προορισμό μέχρις ότου η αντίστοιχη ανενεργή περίοδος εκπνεύσει. Ανενεργές περίοδοι διαφορετικής διάρκειας υποστηρίζονται προκειμένου να επιτραπεί η ικανοποίηση των απαιτήσεων για χαμηλή καθυστέρηση και μικρή κατανάλωση ενέργειας.

4.3 Bluetooth

Το Bluetooth είναι ένα βιομηχανικό πρότυπο για ασύρματα προσωπικά δίκτυα υπολογιστών (Wireless Personal Area Networks, WPAN). Πρόκειται για μια ασύρματη τηλεπικοινωνιακή τεχνολογία μικρών αποστάσεων, η οποία μπορεί να μεταδώσει σήματα μέσω μικροκυμάτων σε ψηφιακές συσκευές. Επομένως το Bluetooth

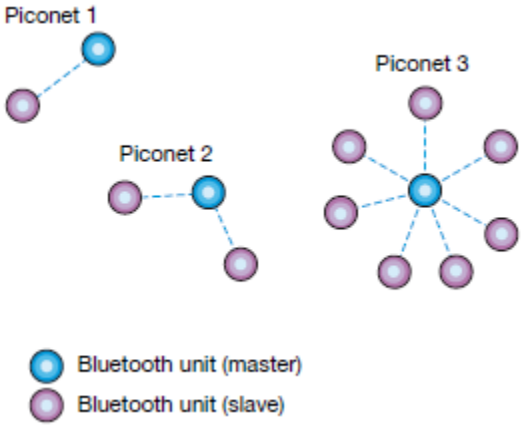
είναι ένα πρωτόκολλο το οποίο παρέχει προτυποποιημένη, ασύρματη επικοινωνία ανάμεσα σε PDA, κινητά τηλέφωνα, φορητοί υπολογιστές, προσωπικοί υπολογιστές, εκτυπωτές, καθώς και ψηφιακές φωτογραφικές μηχανές ή ψηφιακές κάμερες, μέσω μιας ασφαλούς, φθηνής και παγκοσμίως διαθέσιμης χωρίς ειδική άδεια ραδιοσυχνότητας μικρής εμβέλειας.

Η αρχή που βρίσκεται πίσω από το Bluetooth είναι η παροχή ασύρματης δυνατότητας μικρής εμβέλειας γενικής χρήσης. Χρησιμοποιώντας τη ζώνη των 2.4 GHz, δυο συσκευές Bluetooth σε απόσταση 10 μέτρων η μια από την άλλη μπορούν να μοιραστούν χωρητικότητα μέχρι και 720 kbps. Το Bluetooth προορίζεται για την υποστήριξη μιας μεγάλης και εξελισσόμενης λίστας εφαρμογών, όπως δεδομένα ήχο, γραφικά ακόμα και βίντεο. Ο ι κυριότερες ιδιότητές του είναι η ευρωστία, η μικρή πολυπλοκότητα, η χαμηλή ισχύς και το χαμηλό κόστος.Τα πλεονεκτήματα και ο γρήγορος πολλαπλασιασμός των LANs έχουν ως αποτέλεσμα ότι η δημιουργία προσωπικών δικτύων περιοχής (PANs), δηλαδή συνδέσεις μεταξύ των συσκευών στην εγγύτητα του χρήστη, θα έχει πολλές ευεργετικές χρήσεις. Το Bluetooth θα μπορούσε επίσης να χρησιμοποιηθεί στις οικιακές δικτυακές εφαρμογές. Με τους αυξανόμενους αριθμούς σπιτιών που κατέχουν πολλαπλά PCs, η ανάγκη για τα δίκτυα που είναι απλά να εγκατασταθούν και να διατηρηθούν, διευρύνεται [4].

4.3.1 Τοπολογία Bluetooth

Το Bluetooth είναι σχεδιασμένο για να λειτουργεί σε ένα περιβάλλον με πολλούς χρήστες. Δύο ή περισσότερες μονάδες Bluetooth που μοιράζονται το ίδιο κανάλι σχηματίζουν ένα μικρό δίκτυο που ονομάζεται **piconе**t (Σχήμα 4.1). Σε ένα δίκτυο piconet μπορούν να επικοινωνήσουν μέχρι οχτώ συσκευές. Για την παροχή ασφάλειας, κάθε ζεύξη είναι κωδικοποιημένη και προστατεύεται από τις υποκλοπές και τις παρεμβολές.

Το piconet αποτελείται από μια κύρια συσκευή (master) και από μια ως επτά δευτερεύουσες συσκευές (slave). Η κύρια συσκευή πραγματοποιεί τον καθορισμό του καναλιού με χρήση ακολουθίας αναπήδησης συχνότητας καθώς και την μετατόπιση χρονισμού δηλαδή πότε πρέπει να εκπέμπει που θα πρέπει να χρησιμοποιηθούν από όλες τις συσκευές που ανήκουν σε αυτό το piconet. Η κύρια συσκευή πραγματοποιεί αυτόν τον καθορισμό χρησιμοποιώντας τη δική της διεύθυνση ως μια παράμετρο ενώ οι δευτερεύουσες συσκευές πρέπει να συντονιστούν στο ίδιο κανάλι και στην ίδια φάση. Μια δευτερεύουσα συσκευή μπορεί να επικοινωνεί μόνο με τη κύρια συσκευή και μόνο όταν της έχει δοθεί άδεια από την κύρια [7], [16].



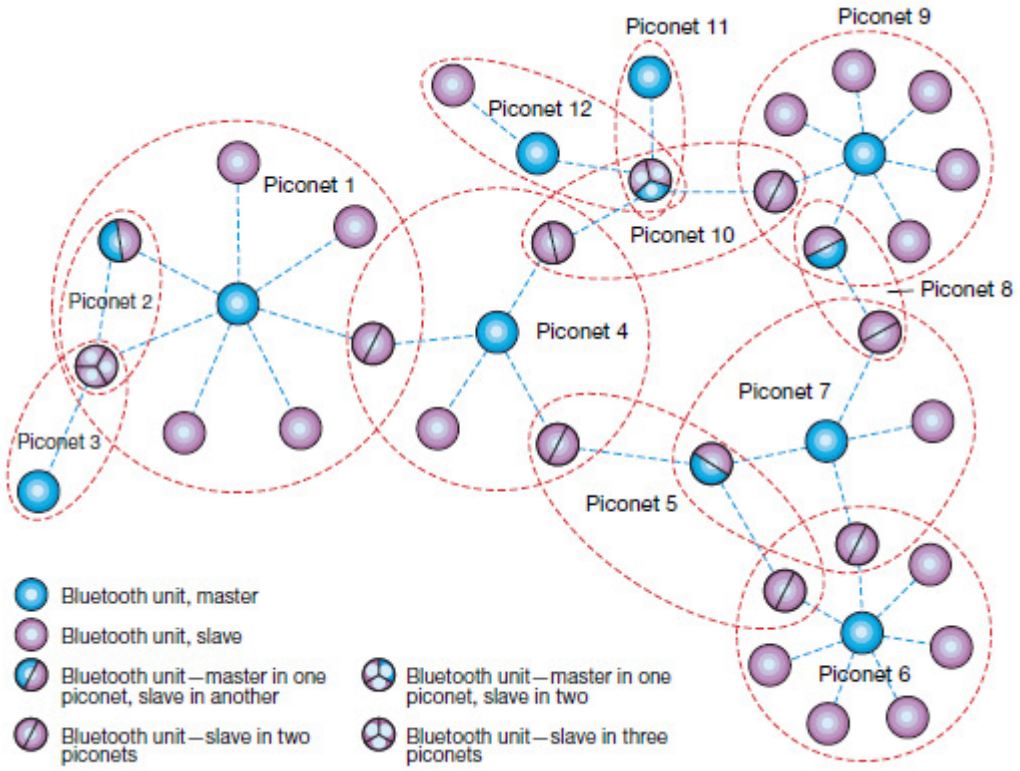
Σχήμα 4.1 Παραδείγματα Bluetooth piconets

Δύο ή περισσότερα piconets μπορεί να είναι διασυνδεδεμένα, με μια μορφή επικάλυψης διαμορφώνοντας αυτό που ονομάζεται **scatternet** (Σχήμα 4.2). Το σημείο σύνδεσης μεταξύ δύο piconets αποτελείται από μια Bluetooth μονάδα που είναι μέλος και των δύο piconets. Σε αυτή τη μορφή μια συσκευή σε ένα piconet μπορεί να συνυπάρχει και ως μέρος ενός άλλου piconet και μπορεί να λειτουργεί είτε ως δευτερεύουσα είτε ως κύρια στο καθένα από αυτά. Μια μονάδα Bluetooth μπορεί ταυτόχρονα να είναι slave μέλος πολλών piconets, αλλά master μόνο σε ένα piconet. Επιπλέον, επειδή μια Bluetooth μονάδα μπορεί μόνο να εκπέμπει και να λαμβάνει δεδομένα σε ένα piconet κάθε φορά, η συμμετοχή της σε πολλαπλά piconets πρέπει να είναι σε βάση time division multiplex (TDM).

Το σύστημα Bluetooth παρέχει αμφίδρομη μετάδοση που βασίζεται σε σχισμές (θυρίδες) διαίρεσης χρόνου time division duplex (TDD), όπου η διάρκεια της κάθε σχισμής είναι 0,625 ms. Δεν υπάρχει άμεση μετάδοση μεταξύ slavei σε ένα piconet Bluetooth, παρά μόνο από τον master στον slave και το αντίστροφο.

Το πλεονέκτημα μιας διάταξης piconet/scatternet είναι ότι επιτρέπει σε πόλλες συσκεύες να μοιράζονται την ίδια φυσική περιοχή και να κάνουν αποδοτική χρήση του εύρους ζώνης. Ένα σύστημα Bluetooth χρησιμοποιεί τη μέθοδο αναπήδησης συχνότητας με διαχωρισμό φερουσών 1MHz. Με την αναπήδηση συχνότητας ορίζεται ένα λογικό κανάλι από την ακολουθία αναπήδησης συχνότητας και κάθε χρονική στιγμή το διαθέσιμο εύρος ζώνης είναι 1MHz, με μέγιστο οκτώ συσκευές που μοιράζονται αυτό το εύρος ζώνης. Διαφορετικά λογικά κανάλια με διαφορετικές ακολουθίες αναπήδησης μπορούν να μοιραστούν

ταυτόχρονα το ίδιο εύρος ζώνης των 80MHz. Σε αυτή τη περίπτωση θα εμφανιστούν συγκρούσεις, όταν συμβαίνει συσκευές που ανήκουν σε διαφορετικά piconet, σε διαφορετικά λογικά κανάλια, να χρησιμοποιούν την ίδια συχνότητα αναπήδησης την ίδια χρονική στιγμή. Όσο αυξάνεται ο αριθμός των piconet σε μια περιοχή, αυξάνεται και ο αριθμός των συγκρούσεων και μειώνεται η απόδοση. Με λίγα λόγια, η φυσική περιοχή και το συνολικό εύρος ζώνης μοιράζονται από το scatternet ενώ το λογικό κανάλι και η μεταφορά δεδομένων μοιράζονται από το piconet [7].

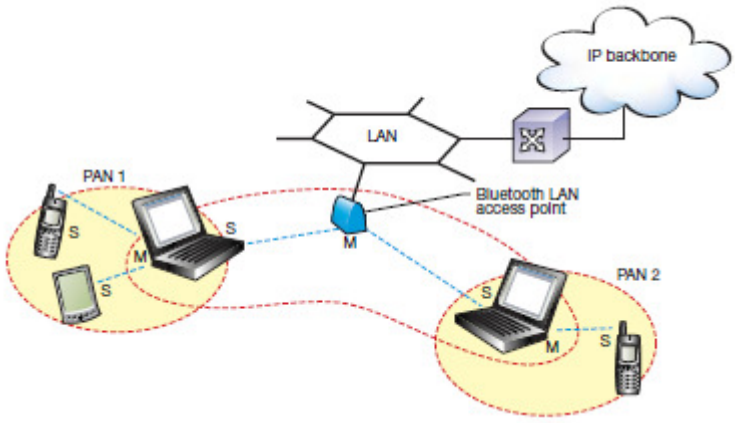


Σχήμα 4.2 Παράδειγμα Bluetooth scatternet

4.3.2 Scatternet- based PANs

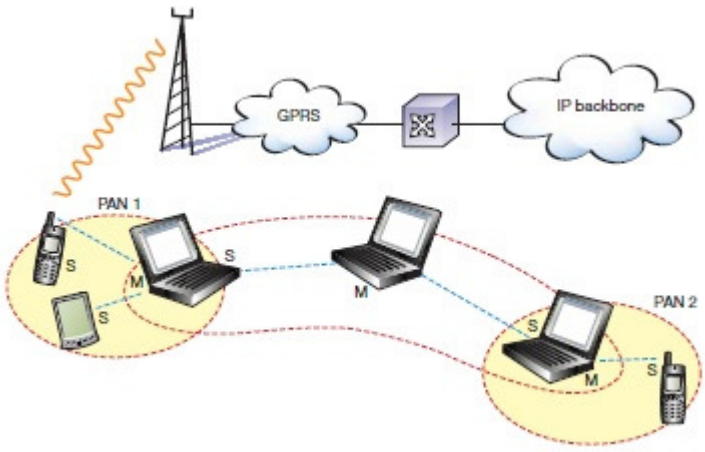
Πιθανότατα τα δίκτυα Bluetooth θα χρησιμοποιηθούν για τη διασύνδεση συσκευών όπως κυψελοειδή τηλέφωνα, PDAs, και φορητούς υπολογιστές, μέσω ενός PAN. Το ίδιο το PAN μπορεί να είναι ένα Bluetooth-based IP δίκτυο όπου πιθανότατα θα βασίζεται σε μια ενιαία piconet τοπολογία. Ωστόσο, όταν ένας PAN χρήστης θέλει να συνδεθεί με ένα ή περισσότερα άλλαPANs, η δυνατότητα του Bluetooth scatternet θα χρησιμεύσει ως ο ιδρυτής για το δίκτυο IP. Ομοίως, αν ένα ή περισσότερα PANs συνδεθούν προς ένα Internet

σημείο πρόσβασης σε ένα LAN (LAN access point LAP), ένα scatternet θα παρέχει τη βασική υποδομή Bluetooth. Στο Σχήμα 4.3. απεικονίζεται ένα δίκτυο scatternet με τρία αλληλοσυνδεόμενα piconets, στο οποίο δύο είναι PANs και ένα χρησιμοποιείται για να παρέχει πρόσβαση δικτύου προς δύο PANs μέσω ενός Bluetooth LAN σημείου πρόσβασης. Σε αυτό το σενάριο, τα γράμματα M και S προσδιορίζουν την κατανομή των master και slave μονάδων [7].



Σχήμα 4.3 Scatternet- based PAN μέσω Bluetooth LAN

Μπορούμε να περιμένουμε να δούμε ένα συνδυασμό PAN διασύνδεσης internet πρόσβασης. Επιπλέον, η Internet πρόσβαση σε ένα PAN ή πολλά διασυνδεδεμένα PANs μπορεί να παρέχεται με τη χρήση ενός κυψελωτού τηλεφώνου (για παράδειγμα, μέσω GPRS / UMTS) σαν μια γέφυρα/δρομολογητής πύλη. Στο Σχήμα 4.4 απεικονίζεται ένα δίκτυο scatternet με τρία αλληλοσυνδεόμενα piconets. Μέσω ενός GPRS / UMTS κυψελωτού τηλέφωνο, ένα piconet παρέχει πρόσβαση IP δικτύου προς τα άλλα δύο piconets [7].



Σχήμα 4..4 Scatternet- based PANs μέσω GPRS / UMTS

Τα scatternets μπορεί επίσης να αναδιαμορφωθούν για να δώσουν καλύτερη συνολική απόδοση. Για παράδειγμα, αν δύο slave κόμβοι χρειάζεται να επικοινωνήσουν, αυτό θα είναι σοφότερο να δημιουργήσουμε ένα νέο piconet το οποίο αποκλειστικά περιέχει αυτούς τους δύο κόμβους. Οι κόμβοι μπορεί ακόμα να είναι μέρος των αρχικών τους piconets αν η κίνηση ρέει προς ή από αυτούς, ή αν χρειάζεται να λάβουν πληροφορίες ελέγχου. Δεδομένου ότι το σύστημα αναπήδησης συχνότητας φάσματος (frequency hopping spread spectrum, FHSS) κάνει το Bluetooth πολύ ισχυρό ενάντια σε παρεμβολές, νέα piconets κερδίζουν σημαντικά μεγαλύτερη χωρητικότητα από ότι χάνουν ως αποτέλεσμα της αυξημένης παρεμβολής μεταξύ τους.

4.3.3 Αρχιτεκτονική πρωτοκόλλων

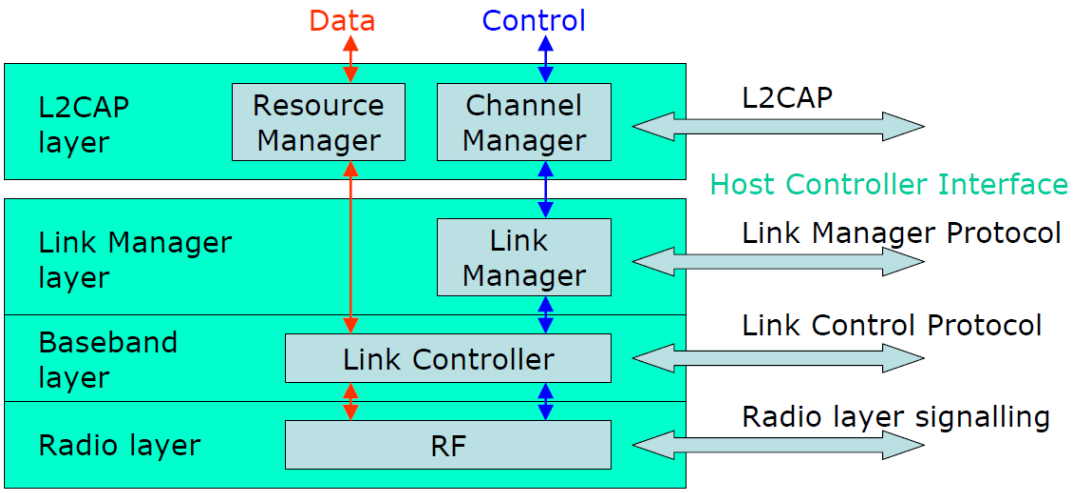
Το πρότυπο του Bluetooth περιέχει πολλά πρωτόκολλα που ομαδοποιούνται σε επίπεδα. Η δομή των επιπέδων δεν ακολουθεί το μοντέλο OSI, το μοντέλο TCP/IP, το μοντέλο 802, ή κάποιο άλλο γνωστό μοντέλο. Παρόλα αυτά, το IEEE προσπαθεί να τροποποιήσει το Bluetooth έτσι ώστε να το κάνει να ταιριάζει καλύτερα με το μοντέλο του 802. Το επίπεδο βασικής ζώνης (base band) είναι κάπως ανάλογο με το υποεπίπεδο MAC, περιέχει όμως και στοιχεία του φυσικού επιπέδου. Καθορίζει πώς θα ελέγχει ο κύριος τις χρονικές υποδοχές και πώς οι υποδοχές αυτές θα ομαδοποιούνται σε πλαίσια. Το Bluetooth ορίζεται ως μια αρχιτεκτονική πρωτοκόλλων με στρώματα που αποτελείται από τα πρωτόκολλα πυρήνα, το πρωτόκολλο αντικατάστασης καλωδίου, τα πρωτόκολλα ελέγχου τηλεφωνίας και τα υιοθετημένα πρωτόκολλα [3] [4]

Τα **πρωτόκολλα πυρήνα (core protocols**) σχηματίζουν μια στοίβα πέντε στρωμάτων που αποτελείται από τα εξής στοιχεία (Σχήμα 4.5):

- **Ασύρματη μετάδοση (Radio):** Καθορίζει τις λεπτομέρειες της διεπαφής αέρα, όπως η συχνότητα, η χρήση αναπήδησης συχνότητας, η μέθοδος διαμόρφωσης και η ισχύς εκπομπής.
- **Βασική ζώνη (Base band):** Ασχολείται με την αποκατάσταση σύνδεσης μέσα σε ένα piconet, τη διευθυνσιοδότηση, τη μορφή των πακέτων, το χρονισμό και τον έλεγχο ισχύος.
- **Πρωτόκολλο διαχειριστή ζεύξεων (Link Manager Protocol):** Έχει την ευθύνη για την αποκατάσταση ζεύξης μεταξύ των συσκευών Bluetooth και της εξελισσόμενης διαχείρισης ζεύξεων, στην οποία περιλαμβάνονται θέματα ασφάλειας όπως η

πιστοποίηση και η κρυπτογράφηση, καθώς επίσης ο έλεγχος και η διαπραγμάτευση των μεγεθών των πακέτων βασικής ζώνης.

- **Πρωτόκολλο ελέγχου λογικής ζεύξης και προσαρμογής (L2CAP):** Προσαρμόζει τα πρωτόκολλα ανωτέρων στρωμάτων στο στρώμα βασικής ζώνης. Το L2CAPπαρέχει και υπηρεσίες με σύνδεση και υπηρεσίες χωρίς σύνδεση.
- **Πρωτόκολλο αναζήτησης υπηρεσιών (SDP):** Έχει την ευθύνη για τη διαδικασία αναζήτησης πληροφοριών συσκευών, υπηρεσιών και των χαρακτηριστικών των υπηρεσιών για την αποκατάσταση μιας σύνδεσης μεταξύ δυο ή περισσοτέρων συσκευών Bluetooth.



Σχήμα 4.5 πρωτόκολλα πυρήνα

Το RFCOMM είναι το **πρωτόκολλο αντικατάστασης καλωδίου** που περιλαμβάνεται στην προδιαγραφή του Bluetooth. Το RFCOMM χρησιμοποιεί μια εικονική σειριακή θύρα που έχει σχεδιαστεί για να υλοποιήσει την αντικατάσταση των τεχνολογιών καλωδίου με ελάχιστη δυνατή τροποποίηση των υπαρχόντων συσκευών. Το RFCOMM υποστηρίζει τη μεταφορά δυαδικών δεδομένων και εξομοιώνει τα σήματα ελέγχου πάνω στο στρώμα βασικής ζώνης του Bluetooth.

Το **πρωτόκολλο ελέγχου τηλεφωνίας (telephony control protocol)** λειτουργεί σε επίπεδο bitto οποίο ορίζει τη σηματοδοσία ελέγχου κλήσεων για την αποκατάσταση κλήσεων ομιλίας και δεδομένων μεταξύ Bluetooth. Επιπλέον ορίζει τις διαδικασίες διαχείρισης κινητικότητας για το χειρισμό ομάδων συσκευών TCS Bluetooth.

Τα **υιοθετημένα πρωτόκολλα (adopted protocols)** ορίζονται στις προδιαγραφές που εκδίδονται από άλλους οργανισμούς δημιουργίας προτύπων και ενσωματώνονται μέσα στη συνολική αρχιτεκτονική του Bluetooth. Η στρατηγική του Bluetooth είναι να δημιουργεί

μόνο τα απαραίτητα πρωτόκολλα και να χρησιμοποιεί τα υπάρχοντα πρότυπα όπου αυτό είναι δυνατό. [4]

4.3.4 Το επίπεδο βασικής ζώνης του Bluetooth

Το επίπεδο βασικής ζώνης είναι το πλησιέστερο πράγμα που έχει το Bluetooth ως προς το υποεπίπεδο MAC. Μετατρέπει την ανεπεξέργαστη ροή bit σε πλαίσια και ορίζει κάποιες βασικές μορφές πλαισίων. Στην απλούστερη περίπτωση, ο κύριος κάθε μικροσκοπικού δικτύου καθορίζει μια ακολουθία χρονικών υποδοχών των 625 μsec, με τις μεταδόσεις του κυρίου να ξεκινούν στις άρτιες υποδοχές και τις μεταδόσεις των υπηρετών να ξεκινούν στις περιττές υποδοχές. Η μέθοδος αυτή είναι κλασική πολυπλεξία με διαίρεση χρόνου, με τον κύριο (master) να παίρνει τις μισές υποδοχές και τους υπηρέτες (slaves) να μοιράζονται τις άλλες μισές. Τα πλαίσια μπορεί να έχουν μήκος 1, 3, ή 5 υποδοχές. Κάθε πλαίσιο μεταδίδεται μέσω ενός λογικού καναλιού, που ονομάζεται σύνδεσμος, ανάμεσα στον κύριο και έναν υπηρέτη. Υπάρχουν δύο είδη συνδέσμων [4].

1. **Σύγχρονη με σύνδεση (Synchronous Connection Oriented, SCO):** Εκχωρεί ένα σταθερό εύρος ζώνης μεταξύ μιας σύνδεσης από σημείο σε σημείο που περιέχει την κύρια και μια μόνο δευτερεύουσα συσκευή. Η κύρια συσκευή διατηρεί τη ζεύξη SCO χρησιμοποιώντας δεσμευμένες χρονοθυρίδες σε τακτά χρονικά διαστήματα. Η βασική μονάδα της δέσμευσης είναι δυο συνεχόμενες χρονοθυρίδες μια προς κάθε κατεύθυνση εκπομπής. Η κύρια συσκευή μπορεί να υποστηρίξει μέχρι τρεις ταυτόχρονες ζεύξεις ενώ μια δευτερεύουσα συσκευή μπορεί υποστηρίξει δυο ή τρεις ζεύξεις SCO. Τα πακέτα SCO δεν επανεκπέμπονται ποτέ.

2. **Ασύγχρονη χωρίς σύνδεση (Asynchronous Connectionless, ACL):** είναι μια ζεύξη από σημείο προς πολλά σημεία μεταξύ της κύριας συσκευής και όλων των δευτερευουσών συσκευών σε ένα piconet. Σε χρονοθυρίδες που δεν είναι δεσμευμένες για ζεύξεις SCO, η κύρια συσκευή μπορεί να ανταλλάξει πακέτα με οποιαδήποτε δευτερεύουσα συσκευή ανά θυρίδα, περιλαμβάνοντας ήδη μια δευτερεύουσα συσκευή απασχολημένη σε μια ζεύξη SCO. Μπορεί να υπάρχει μόνο μια ζεύξη ACL. Για πακέτα ACL, ισχύει η επανεκπομπή πακέτων.

Οι ζεύξεις SCO χρησιμοποιούνται κυρίως για την ανταλλαγή χρονικά περιορισμένων δεδομένων που απαιτούν εγγυημένο ρυθμό δεδομένων αλλά χωρίς εγγυημένη παράδοση. Ένα παράδειγμα που χρησιμοποιείται σε πολλά προφίλ Bluetoothείναι τα ψηφιακά κωδικοποιημένα δεδομένα ακουστικών σημάτων με εγγενή ανοχή στην απώλεια

δεδομένων. Ο εγγυημένος ρυθμός δεδομένων επιτυγχάνεται μέσω της δέσμευσης ενός συγκεκριμένου αριθμού χρονοθυρίδων. Οι ζεύξεις ACL παρέχουν μια σύνδεση τύπου μεταγωγής πακέτων. Δεν είναι δυνατή η δέσμευση εύρους ζώνης και η παράδοση μπορεί να είναι εγγυημένη μέσω της ανίχνευσης σφαλμάτων και της επανεκπομπής. Μια δευτερεύουσα συσκευή έχει το δικαίωμα να επιστρέψει ένα πακέτο ACL στη χρονοθυρίδα δευτερεύουσα προς κύρια συσκευή αν και μόνο αν έχει διευθυνσιοδοτηθεί στη προηγούμενη χρονοθυρίδα κύρια προς δευτερεύουσα συσκευή. Για τις ζεύξεις ACL, έχουν οριστεί πακέτα μιας χρονοθυρίδας , τριών χρονοθυρίδων, και πέντε χρονοθυρίδων. Τα δεδομένα μπορούν να σταλούν χωρίς προστασία (αν και μπορεί να χρησιμοποιηθεί ARQ σε κάποιο υψηλότερο στρώμα) ή με προστασία με έναν κώδικα 2/3 αυτοδύναμης διόρθωσης σφαλμάτων.

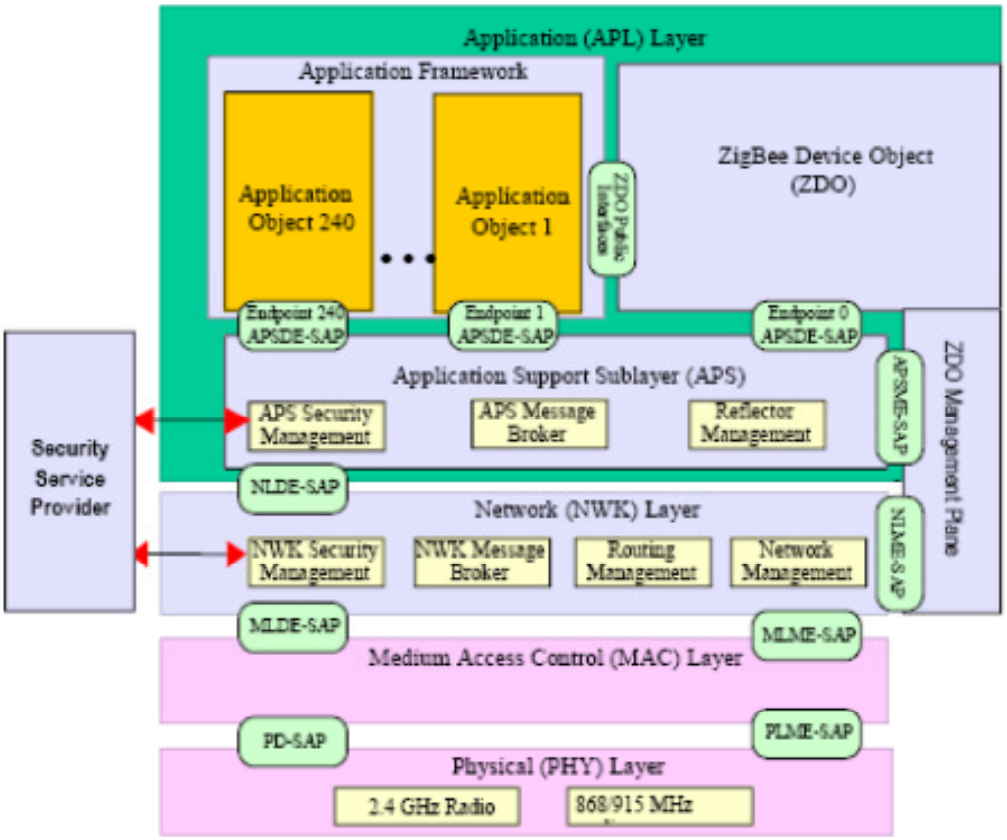
4.4 Zigbee

4.4.1 Η στοίβα πρωτοκόλλων του Zigbee

Η στοίβα πρωτοκόλλων του ZigBee αποτελείται από 4 επίπεδα. Κάθε επίπεδο εκτελεί ένα συγκεκριμένο σύνολο λειτουργιών και παρέχει τις υπηρεσίες του στο ανώτερο επίπεδο μέσω μιας διεπαφής που ονομάζεται **σημείο πρόσβασης υπηρεσιών (service access point, SAP)**. Τα 4 επίπεδα της στοίβας πρωτοκόλλων του ZigBee είναι τα παρακάτω (Σχήμα 4.6):

- **Το φυσικό επίπεδο (Physical layer, PHY).** Είναι υπεύθυνο για την ενεργοποίηση και απενεργοποίηση του πομποδέκτη, μετάδοση και λήψη δεδομένων, ανίχνευση ενέργειας στο κανάλι, εκτίμηση της κατάστασης των καναλιών για την πολλαπλή πρόσβαση με ανίχνευση φέροντος και με αποφυγή συγκρούσεων (CSMA-CA) και τη μέτρηση της ποιότητας των λαμβανομένων πακέτων.
- **Το επίπεδο ελέγχου πρόσβασης στο μέσο (Medium access control layer, MAC).** Παρέχει υπηρεσίες μεταφοράς δεδομένων και διαχείρισης. Είναι υπεύθυνο για την πρόσβαση στο κανάλι, για τη διαχείριση των χρονοσχισμών και για την παροχή μιας αξιόπιστης σύνδεσης μεταξύ δύο επιπέδων MAC. Επιπρόσθετα παρέχει τα μέσα για την εφαρμογή διαφόρων μηχανισμών ασφάλειας.
- **Το επίπεδο δικτύου (Network layer, NWK)**. Είναι υπεύθυνο για τη δημιουργία του δικτύου, για την είσοδο και την έξοδο μία συσκευής από ένα δίκτυο, για την ασφάλεια και για τη δρομολόγηση των μεταδιδόμενων πακέτων.

- **Το επίπεδο εφαρμογών (Application layer, APL)**. Περιλαμβάνει το υποεπίπεδο υποστήριξης εφαρμογών (Application support sublayer, APS), το πλαίσιο εφαρμογών (Application framework, AF), τα αντικείμενα συσκευής ZigBee (ZigBee Device Objects, ZDO) και τις καθορισμένες από τον κατασκευαστή εφαρμογές. Το υποεπίπεδο APS είναι υπεύθυνο για τη σύνδεση δύο συσκευών βάση των αναγκών και των υπηρεσιών τους και για την αποστολή δεδομένων μεταξύ τους. Τα ZDO είναι αυτά που καθορίζουν το ρόλο της κάθε συσκευής στο δίκτυο και το επίπεδο ασφάλειας. Επίσης συμβάλλουν στην ανίχνευση των συσκευών σε ένα δίκτυο και στον προσδιορισμό των υπηρεσιών που αυτές παρέχουν. Το πλαίσιο εφαρμογών είναι το περιβάλλον στο οποίο φιλοξενούνται οι εφαρμογές μέσα σε μία συσκευή ZigBee [17].

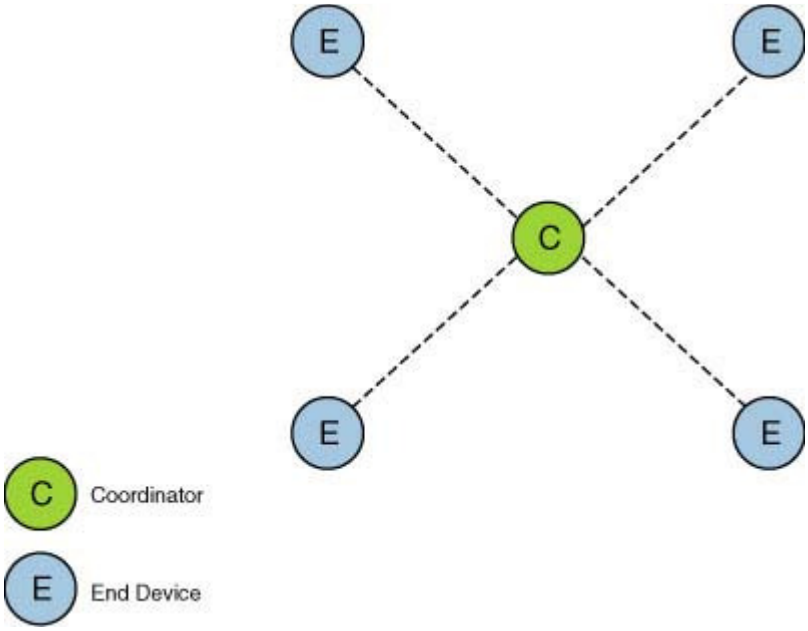


Σχήμα 4.6 Η στοίβα πρωτοκόλλων του ZigBee

4.4.2 Τοπολογίες δικτύων

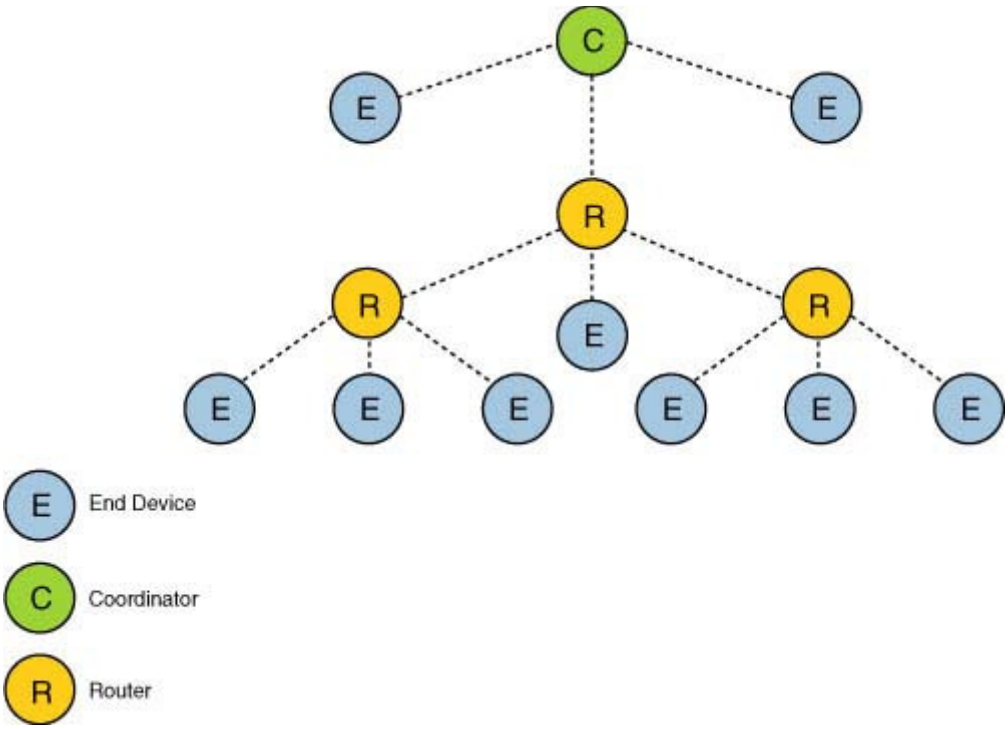
Το ZigBee χρησιμοποιεί την προδιαγραφή IEEE 802.15.4 2003 για το φυσικό στρώμα και στρώμα MAC. IEEE 802.15.4 προσφέρει τοπολογίες όπως star, tree, cluster tree και mesh. Ωστόσο, το ZigBee υποστηρίζει μόνο τοπολογίες star, tree, και mesh. Χρησιμοποιεί μια ιεραρχική ένωση όπου μια συσκευή που ενώνει το δίκτυο μπορεί να είναι είτε ένας δρομολογητής ή μια τερματική συσκευή, και οι δρομολογητές μπορούν να δεχθούν περισσότερες συσκευές [17].

Τοπολογία star: Η τοπολογία αστέρα αποτελείται από έναν συντονιστή και αρκετές τερματικές συσκευές (κόμβους), όπως φαίνεται στο Σχήμα 4.7. Σε αυτή την τοπολογία, η συσκευή επικοινωνεί μόνο με τον συντονιστή. Κάθε ανταλλαγή πακέτων μεταξύ end συσκευών πρέπει να περάσουν από τον συντονιστή. Το μειονέκτημα αυτής της τοπολογίας είναι ότι η λειτουργία του δικτύου εξαρτάται από τον συντονιστή του δικτύου, και επειδή όλα τα πακέτα μεταξύ των συσκευών πρέπει να περάσουν από συντονιστή, ο συντονιστής μπορεί να αποσυμφοριστεί. Επίσης, δεν υπάρχει εναλλακτική διαδρομή από την πηγή στον προορισμό. Το πλεονέκτημα της τοπολογίας αστέρι είναι ότι είναι απλή και τα πακέτα περνούν από το πολύ δύο αναπηδήσεις για να φθάσουν στον προορισμό τους. [17]



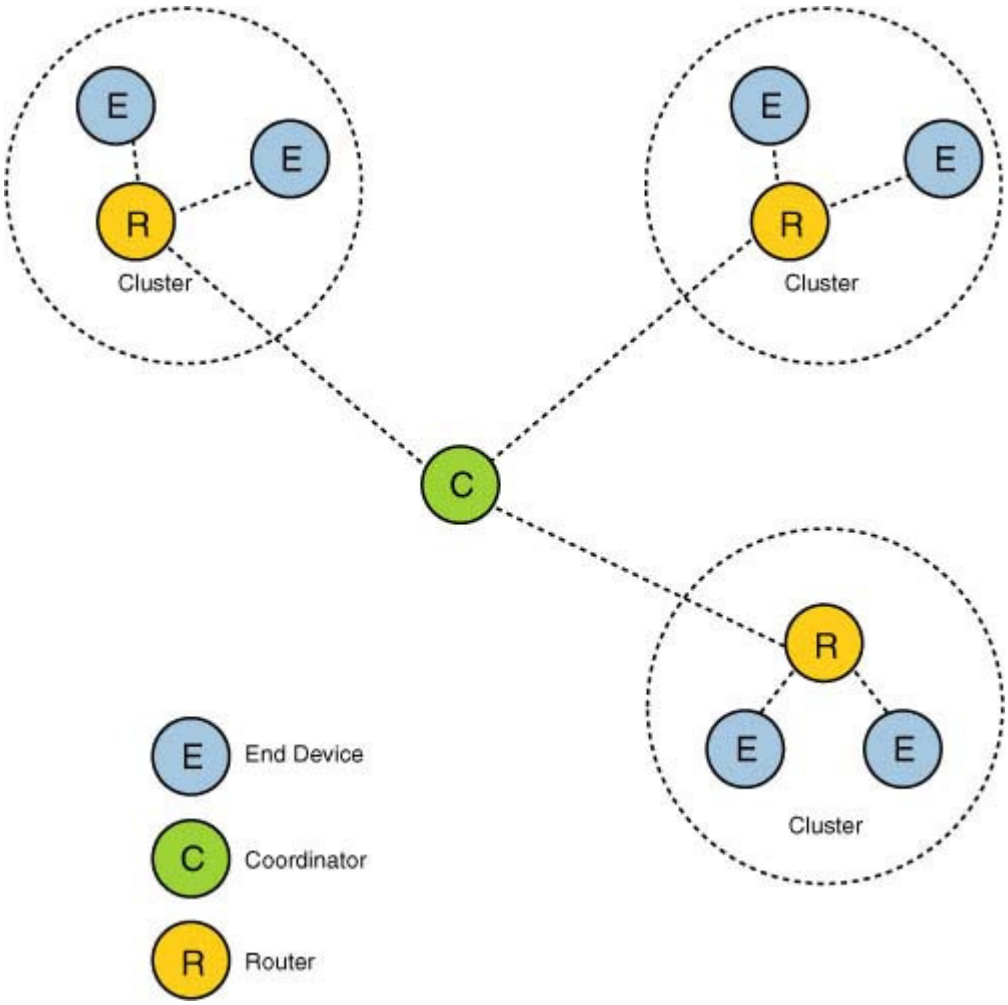
Σχήμα 4.7 Τοπολογία star

Τοπολογία tree: Σε αυτή την τοπολογία, το δίκτυο αποτελείται από ένα κεντρικό κόμβο (δέντρο ρίζα), ο οποίος είναι ένας συντονιστής, πολλά routers, και τερματικές συσκευές όπως φαίνεται σχήμα 4.8. Η λειτουργία του δρομολογητή είναι να επεκταθεί η κάλυψη του δικτύου. Οι κόμβοι που συνδέονται με το συντονιστή ή δρομολογητές ονομάζονται παιδιά. Μόνο οι δρομολογητές και ο συντονιστής μπορεί να έχουν τα παιδιά. Κάθε τερματική συσκευή είναι μόνο σε θέση να επικοινωνήσει με τη μητρική της (δρομολογητής ή ο συντονιστής). Ο συντονιστής και οι δρομολογητές μπορούν να έχουν παιδιά και, ως εκ τούτου, είναι οι μόνες συσκευές που μπορεί να είναι γονείς. Ένα άκρο της συσκευής δεν μπορεί να έχει παιδιά και, ως εκ τούτου, δεν μπορεί να είναι ένας γονέας. Μια ειδική περίπτωση της τοπολογίας δέντρου ονομάζεται τοπολογία δέντρου συμπλέγματος [17].



Σχήμα 4.8 Τοπολογία tree.

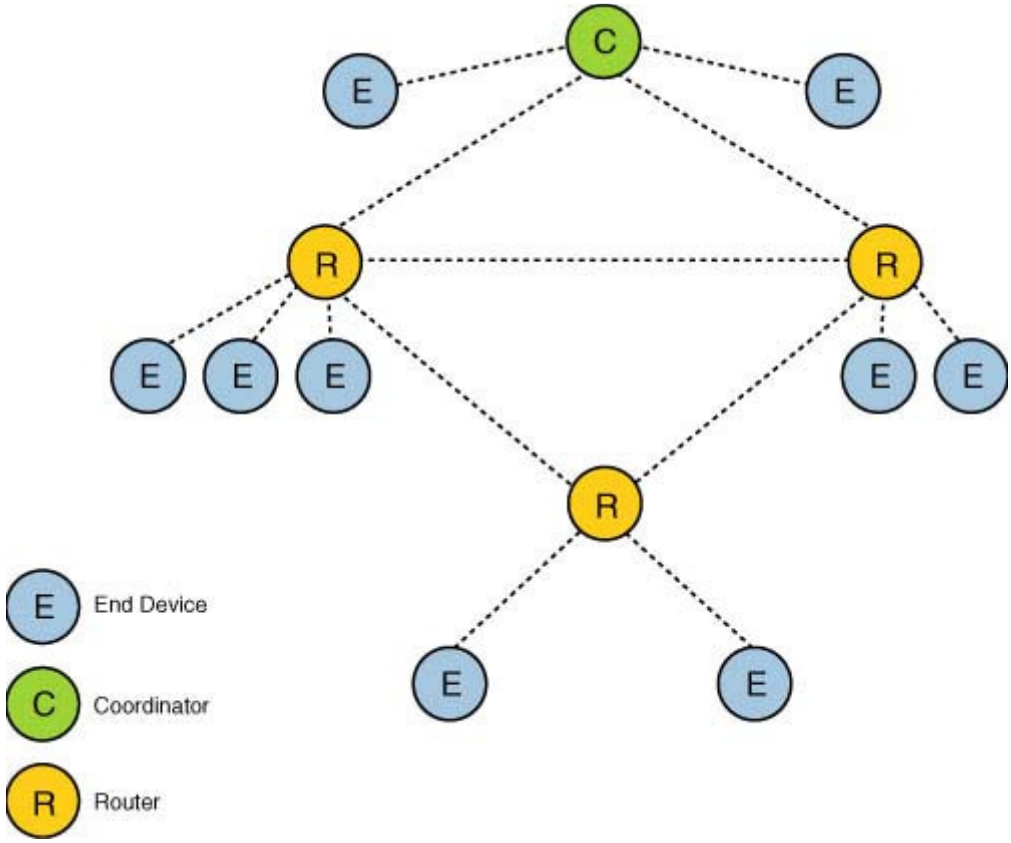
Τοπολογία Cluster Tree: Μια τοπολογία σύμπλεγμα δέντρου είναι μια ειδική περίπτωση της τοπολογίας δέντρου στην οποία ένας γονέας με παιδιά της, ονομάζεται ένα σύμπλεγμα, όπως φαίνεται στο σχήμα 4.9. Κάθε ομάδα αναγνωρίζεται από ένα αναγνωριστικό cluster. Το ZigBee δεν υποστηρίζει τοπολογία σύμπλεγμα δέντρου [17].



Σχήμα 4.9 Τοπολογία Cluster tree

Τοπολογία Mesh: αναφέρεται επίσης ως δίκτυο peer-to-peer, αποτελείται από έναν συντονιστή, αρκετές δρομολογητές, και τερματικές συσκευών, όπως φαίνεται στο σχήμα 4.10. Τα παρακάτω είναι τα χαρακτηριστικά της τοπολογίας πλέγματος: Μια τοπολογία πλέγματος είναι ένα δίκτυο πολλαπλών ανακλάσεων και τα πακέτα περνούν μέσα από

πολλαπλές διαδρομές για να φθάσουν στον προορισμό τους. Το εύρος ενός δικτύου μπορεί να αυξηθεί με την προσθήκη περισσότερων συσκευών στο δίκτυο. Μπορεί να εξαλείψει νεκρές ζώνες. Μια τοπολογία πλέγματος κατά τη διάρκεια της μετάδοσης, εάν μια διαδρομή αποτύχει, ο κόμβος θα βρει μια εναλλακτική διαδρομή για τον προορισμό. Οι συσκευές μπορεί να είναι κοντά η μια στην άλλη, ώστε να χρησιμοποιούν λιγότερη ενέργεια. Η προσθήκη ή η αφαίρεση μιας συσκευής είναι εύκολη. Κάθε συσκευή πηγής μπορεί να επικοινωνεί με οποιαδήποτε συσκευή προορισμού στο δίκτυο. Σε σύγκριση με τοπολογία αστέρα, τοπολογία πλέγματος απαιτεί μεγαλύτερη επιβάρυνση. Πλέγμα δρομολόγησης χρησιμοποιεί ένα πιο πολύπλοκο πρωτόκολλο δρομολόγησης από μια τοπολογία αστέρα [17].



Σχήμα 4.10 Τοπολογία Mesh.

4.4.3 Αρχιτεκτονική Zigbee

Τρεις είναι οι περιοχές στις οποίες εστιάζει η αρχιτεκτονική Zigbee:

Το φυσικό και το MAC στρώματα αξιοποιούν πλήρως τις φυσικές ραδιοσυχνότητες που καθορίζονται από το πρότυπο IEEE 802.15.4. Οι προδιαγραφές IEEE 802.15.4 περιγράφουν ένα peer-to-peer σχήμα το οποίο χρησιμοποιεί ένα εξαπλωμένο φάσμα. Οι προδιαγραφές επίσης καλούν προς ενεργοποίηση τις λειτουργίες των ρυθμών δεδομένων, της καναλοποίησης και των τεχνικών διαμόρφωσης [17].

Το **ZigbeeAlliance** συγκεκριμενοποιεί το λογικό δίκτυο, το λογισμικό ασφάλειας και εφαρμογών και τα οποία υλοποιούνται πάνω σε μια σταθερή στοίβα. Η δικτυακή στοίβα Zigbee δημιουργεί την δυνατότητα διασύνδεσης των δικτύων. Κάθε μικροελεγκτής ή συνδυασμός ορισμένων RF τσιπ απαιτεί τη δική του Zigbee στοίβα εξαιτίας των διαφορών που υπάρχουν στους μικροελεγκτές και στα RF τσιπ. Τυπικά, η στοίβα Zigbee συμπεριλαμβάνεται είτε με το μικροελεγκτή είτε με το RF τσιπ. Το στρώμα εφαρμογής ορίζεται από τα προφίλ, από τα οποία υπάρχουν δυο είδη: τα δημόσια προφίλ είναι εκείνα που πιστοποιούνται από το ZigbeeAlliance και εξυπηρετούν σκοπούς διαλειτουργικότητας και τα ιδιωτικά προφίλ τα οποία είναι για χρήση στα κλειστά συστήματα.

4.4.4 Εφαρμογές

Το ZigBee είναι μία τεχνολογία ασύρματης μετάδοσης η οποία θα βρει εφαρμογές στην αποστολή μικρού μεγέθους δεδομένων, όπως κείμενα, ακόμα και σε μεγάλη απόσταση.

Ένα σημαντικό μέρος των εφαρμογών που θα στηριχτούν στο ZigBee είναι αυτές που μέχρι σήμερα ήταν βασιζόμενες σε κλειστές τεχνολογίες ή ακόμα και σε γνωστές, όπως οι υπέρυθρες. Μεγάλο ατού των υλοποιήσεων του ZigBee είναι η χαμηλή κατανάλωση ενέργειας των συσκευών που το ενσωματώνουν, γεγονός που οδηγεί σε αξιοποίηση για μεγάλη χρονική περίοδο, ίσως ακόμα και για χρόνια, της ίδιας μπαταρίας. Μέσω του ZigBee μπορεί να επιτευχθεί επικοινωνία σε σημαντική απόσταση η οποία μπορεί να κυμαίνεται από 70 έως και 300 μέτρα, σε ταχύτητες οι οποίες αγγίξουν ακόμη και τα 250Kbps. Το πεδίο εφαρμογών της συγκεκριμένης τεχνολογίας είναι πράγματι πολύ μεγάλο. Το ZigBee θα μπορεί να χρησιμοποιηθεί σε τηλεχειριστήρια, τηλεχειριζόμενες πόρτες, ηλεκτρικά παράθυρα και γενικά στην διαχείριση ηλεκτρονικών συσκευών (τηλεόραση, βίντεο, συσκευές ψηφιακών μεταδόσεων). Παράλληλα, είναι δυνατό να έχει μία σειρά περισσότερο εξειδικευμένων εφαρμογών όπως η παρακολούθηση των επιδόσεων πορείας ενός αθλητή ή ακόμα και ενός ασθενούς, ενώ ακόμα και η διαχείριση ενέργειας σε ένα κτίριο, μπορεί να επιτευχθεί με την χρήση τεχνολογίας και συσκευών ZigBee [17].

Για τους λόγους όπου οι αισθητήρες και οι συσκευές πληροφοριακού ελέγχου απαιτούν ζώνες πληροφοριών μικρού εύρους, με μικρό ποσοστό σφάλματος και πολύ μικρή κατανάλωση ισχύος η Ανάπτυξη Ασύρματων Αισθητήρων και Διεργασιών Πληροφοριακού Ελέγχου μέσω Ενσωματωμένου Υπολογιστικού Συστήματος πρωτοκόλλου IEEE 802.15.4 έρχεται για να λύσει προβλήματα σε ζητήματα μετρήσεων και ανίχνευσης φυσικών μεγεθών κυρίως σε εφαρμογές με κινούμενα μέρη. Λόγω της υψηλής συχνότητας εκπομπής των δεδομένων, οι μετρήσεις και ο έλεγχος των συστημάτων είναι ασφαλής από θορύβους του βιομηχανικού περιβάλλοντος εργασίας.

Η ανάπτυξη της μεθόδου ασύρματων αισθητήρων και πληροφοριακού ελέγχου μέσω πρωτοκόλλου IEEE 802.15.4 παρουσιάζει:

- χαμηλό κόστος σε συνάρτηση των ειδικών καλωδίων διασύνδεσης αισθητήρων για κάλυψη αποστάσεων μεγαλύτερη των 30m,
- χαμηλή κατανάλωση ισχύος και αποφυγή φαινόμενου λευκού θορύβου λόγω μη χρήσης ενδιάμεσων ενισχυτών σήματος που χρησιμοποιούνταν έως τώρα,
- αποδέσμευση του χώρου από ενσύρματες διασυνδέσεις και της ελευθερίας κινήσεων του ανθρώπου μέσα στο περιβάλλον εργασίας του,
- άμεση Ad-hoc διασύνδεση αισθητήρων σε RDF μονάδα προς επέκταση του συστήματος.

ΚΕΦΑΛΑΙΟ 5

ΑΣΦΑΛΕΙΑ ADHOC ΔΙΚΤΥΩΝ

5.1 Απαιτήσεις ασφαλείας

Στο κεφάλαιο αυτό αναλύονται τα θέματα ασφαλείας που διέπουν τα ad hoc δίκτυα. Αναπτύσσονται όλα τα θέματα ασφαλείας των δικτύων, όπως είναι οι απαιτήσεις ασφαλείας, τα είδη απειλών και επιθέσεων, η ασφάλεια που παρέχεται στα επίπεδα των συστημάτων, τα μέτρα αντιμετώπισης των απειλών κ.ά. Η ασφάλεια είναι ίσως το σημαντικότερο κομμάτι κατά τη δημιουργία και ανάπτυξη ενός ασύρματου δικτύου. Οι σημαντικότερες απαιτήσεις ασφαλείας αναφέρονται παρακάτω.

5.1.1 Διαθεσιμότητα (Availability)

Η διαθεσιμότητα εξασφαλίζει την βιωσιμότητα των υπηρεσιών του δικτύου, παρά τις **επιθέσεις άρνησης υπηρεσιών (denial of services, DoS)** που δέχεται. Μια DoS επίθεση μπορεί να εκκινήσει σε οποιοδήποτε επίπεδο ενός ad hoc δικτύου. Επίσης, τα συστήματα που εξασφαλίζουν τη διαθεσιμότητα προσπαθούν να καταπολεμήσουν τις επιθέσεις κατανάλωσης ενέργειας, καθώς επίσης την παρεκτροπή των κόμβων και την εγωιστική συμπεριφορά τους κατά την προώθηση μηνυμάτων. Στο φυσικό επίπεδο, ένας αντίπαλος μπορεί να προκαλέσει **συνωστισμό (jamming)** για να παρέμβει στις επικοινωνίες. Στο επίπεδο δικτύου, μπορεί να διαταραχτεί το πρωτόκολλο δρομολόγησης και να διακοπεί το δίκτυο. Σε ανώτερα επίπεδα μπορούν να ανατραπούν οι αντίστοιχες υπηρεσίες, όπως είναι η υπηρεσία διαχείρισης κλειδιού [20].

5.1.2 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα εξασφαλίζει ότι ορισμένη πληροφορία δεν εκτίθεται σε μη εξουσιοδοτημένες οντότητες. Η μετάδοση ευαίσθητων πληροφοριών, όπως είναι στρατηγικές ή τακτικές στρατιωτικές πληροφορίες, απαιτεί εμπιστευτικότητα. Η διαρροή τέτοιων πληροφοριών σε εχθρούς μπορεί να έχει καταστροφικές συνέπειες. Η πληροφορία δρομολόγησης πρέπει επίσης να μείνει εμπιστευτική σε ορισμένες περιπτώσεις γιατί αυτή μπορεί να είναι πολύτιμη για τον εχθρό ώστε να εξακριβώσει και να προσδιορίσει τους στόχους του στο πεδίο της μάχης. Η συνήθης τακτική για να κρατηθούν ευαίσθητα δεδομένα ασφαλή είναι η κρυπτογράφηση των δεδομένων με ένα μυστικό κλειδί, το οποίο μόνο οι επίδοξοι λήπτες κατέχουν. Επειδή η κρυπτογράφηση δημόσιου κλειδιού απαιτεί μεγάλη κατανάλωση ενέργειας, τα περισσότερα από τα προτεινόμενα πρωτόκολλα χρησιμοποιούν μεθόδους κρυπτογράφησης συμμετρικού κλειδιού [18] [20].

5.1.3 Αυθεντικότητα (Authentication)

Η αυθεντικότητα (ή πιστοποίηση) επιτρέπει σ' ένα κόμβο να διασφαλίσει την ταυτότητα του επικοινωνούντα κόμβου. Χωρίς την αυθεντικότητα, ένας αντίπαλος μπορεί να μεταμφιέσει έναν κόμβο και έτσι να κερδίσει μη εξουσιοδοτημένη πρόσβαση σε πηγές του δικτύου, σε ευαίσθητες πληροφορίες και να παρέμβει στις λειτουργίες άλλων κόμβων. Έτσι, η αυθεντικότητα είναι απαραίτητη για πολλούς εκτελεστικούς σκοπούς του προγράμματος, όπως εκ νέου προγραμματισμός του δικτύου, έλεγχος κύκλου ασφαλείας σ' ένα κόμβο κ.ά. Η αυθεντικότητα πληροφορίας επιτρέπει στον δέκτη να επιβεβαιώσει ότι η πληροφορία στάλθηκε τοπικά από τον πραγματικό αποστολέα. Σε επικοινωνία δύο μερών, η αυθεντικότητα μπορεί να επιτευχθεί με έναν καθαρά συμμετρικό μηχανισμό: Ο αποστολέας και ο λήπτης μοιράζονται ένα μυστικό κλειδί με το οποίο υπολογίζουν έναν κώδικα αυθεντικότητας μηνύματος (message authentication code-MAC) για όλα τα αποστελλόμενα δεδομένα. Όταν ένα μήνυμα με τον σωστό MAC φτάσει, ο λήπτης ξέρει ότι στάλθηκε από τον αποστολέα. Όμως, κατά την εκπομπή μηνύματος προς πολλούς αποδέκτες, χρειάζονται ισχυρότεροι δεσμοί εμπιστοσύνης [20].

5.1.4 Μη αποποίηση (Non-repudiation)

Η μη αποποίηση (ή μη αποκύρηξη) εξασφαλίζει ότι ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί ότι έχει στείλει το μήνυμα. Η μη αποποίηση είναι χρήσιμη στην επισήμανση και απομόνωση εκτεθειμένων κόμβων. Έτσι, όταν ένας κόμβος Α λαμβάνει ένα λανθασμένο μήνυμα από έναν κόμβο Β, η μη αποποίηση επιτρέπει στον Α να κατηγορήσει τον Β ότι αυτός έστειλε το μήνυμα και να πείσει τους υπόλοιπους κόμβους του δικτύου ότι ο Β είναι εκτεθειμένος. Οι ψηφιακές υπογραφές μπορεί να είναι μία λύση για την παραπάνω περίπτωση [18].

5.1.5 Ανανέωση-Φρεσκάδα (Freshness)

Η απαίτηση για ανανέωση και φρεσκάδα των δεδομένων δηλώνει ότι οι πληροφορίες και τα μηνύματα που ανταλλάσσονται είναι πρόσφατα και διαβεβαιώνει ότι δεν επαναλαμβάνεται αναμετάδοση παλαιών μηνυμάτων. Σε όλα τα μηνύματα συνήθως παρέχεται ένας καταμετρητής χρόνου. Βάσει αυτού του μετρητή μπορούμε να διασφαλίσουμε ότι ένα μήνυμα είναι φρέσκο. Όταν ανανεώνουμε την πληροφορία, διασφαλίζουμε ότι η πληροφορία αυτή είναι πρόσφατη και έτσι αποτρέπουμε κάποιον εχθρό να ξαναγράψει παλαιά μηνύματα. Ένας κοινός τρόπος αντιμετώπισης απειλών είναι να περιλάβουμε έναν μονοτονικά αυξανόμενο μετρητή με κάθε αποστελλόμενο μήνυμα και

να απορρίψουμε μηνύματα με παλαιές τιμές του μετρητή. Επίσης η ανανέωση μπορεί να αφορά στην ανανέωση του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Στην περίπτωση αυτή, κάθε κλειδί βεβαιωμένης μεθόδου μπορεί να βεβαιώσει ότι το διαμοιραζόμενο κλειδί ανάμεσα στους εμπλεκόμενους είναι καινούργιο (δηλαδή δεν έχει ξαναχρησιμοποιηθεί από τους εμπλεκομένους).

5.1.6 Ακεραιότητα πληροφορίας (Integrity)

Η ακεραιότητα πληροφορίας δηλώνει την γνησιότητα των δεδομένων που στέλνονται μεταξύ εμπλεκομένων. Η ακεραιότητα εγγυάται ότι ένα μήνυμα που μεταφέρεται δεν αλλοιώνεται ποτέ. Ένα μήνυμα θα μπορούσε να αλλοιωθεί ή να καταστραφεί λόγω των συνθηκών εξασθένιση διάδοσης, ή λόγω των κακόβουλων επιθέσεων στο δίκτυο Ως παράδειγμα, ένα μήνυμα που στέλνεται από έναν κόμβο Α σ' ένα κόμβο Β δεν έχει τροποποιηθεί από έναν κακόβουλο κόμβο Γ κατά τη διάρκεια της μετάδοσης. Η υπηρεσία της ακεραιότητας πληροφορίας παρέχεται συχνά από την υπηρεσία της αυθεντικότητας ώστε να εξασφαλιστεί η ασφάλεια του δικτύου. Ένα καλό και ασφαλές σύστημα θα ήταν ικανό να ανιχνεύσει οποιοδήποτε πρόβλημα ακεραιότητας ώστε αν μια παράβαση διαπιστωθεί, τότε άμεσα η υπηρεσία να αναφέρει αυτό το πρόβλημα. Εάν έχει εφαρμοσθεί ένας εύρωστος μηχανισμός εμπιστευτικότητας, η ακεραιότητα πληροφορίας είναι τόσο απλή, όπως η προσθήκη κατατεμαχισμών πριν την κρυπτογράφηση των μηνυμάτων [20].

5.1.7 Επεκτασιμότητα και αυτό-οργάνωση

Συνήθως τα δίκτυα που εξετάζουμε χρειάζονται επέκταση με προσθήκη μεγάλου αριθμού νέων κόμβων. Η ανάγκη αυτή απαιτεί δίκτυα τα οποία να μπορούν να έχουν ιδιότητες επέκτασης, είτε ως προς το ενεργειακό μέρος είτε ως προς το θέμα αναδιοργάνωσης του δικτύου. Ο αριθμός των γειτόνων, οι αποστάσεις μεταξύ τους και η απαιτούμενη ισχύς για την αποστολή μηνυμάτων από έναν κόμβο στον άλλο, πιθανόν να μην είναι γνωστά κατά τη διάρκεια ζωής ενός δικτύου. Έτσι οι κόμβοι στα υπό εξέταση δίκτυα πρέπει να είναι ικανοί να αυτό-οργανώνονται και να επιλέγουν τους κατάλληλους μηχανισμούς που ταιριάζουν σε κάθε περίσταση.

5.2 Είδη απειλών-επιθέσεων

5.2.1 Απειλές

Τα ad hoc δίκτυα τις περισσότερες φορές αναπτύσσονται σε εχθρικά περιβάλλοντα, στα οποία δεν μπορεί να γίνει εύκολα η συντήρηση του δικτύου. Έτσι, πρέπει το δίκτυο να γνωρίζει τις πιθανές απειλές καθώς επίσης και τα αντίμετρα που μπορεί να πάρει για να

αποφύγει αυτές τις επιθέσεις, αλλά και αν ένα τμήμα του δικτύου προσβληθεί, να μπορέσει να απομονωθεί από το υπόλοιπο υγειές δίκτυο. Οι απειλές που δέχεται ένας κόμβος του δικτύου μπορούν να χωριστούν σε δύο κλάσεις, στις **επιθέσεις** και στην **κακή συμπεριφορά**. [20]

5.2.2 Επιθέσεις

Σαν επίθεση λογίζεται οποιαδήποτε πράξη που σκόπιμα προσπαθεί να προκαλέσει οποιαδήποτε ζημιά στο δίκτυο. Μπορούν να χωριστούν ανάλογα με την προέλευση τους και την φύση τους. Οι επιθέσεις με βάση την προέλευσή τους χωρίζονται σε δύο κατηγορίες, τις **εξωτερικές** και **εσωτερικές** επιθέσεις. Ως εξωτερικές επιθέσεις λογίζονται οι επιθέσεις που ξεκινάνε από κόμβους που δεν ανήκουν στο δίκτυο ή δεν επιτρέπεται η πρόσβαση τους στο δίκτυο. Ως εσωτερικές επιθέσεις θεωρούνται επιθέσεις που ξεκινάνε από εσωτερικούς εκτεθειμένους ή κακόβουλους κόμβους. Αυτή είναι μια πιο σοβαρή απειλή, αφού η προτεινόμενη άμυνα για τις εξωτερικές επιθέσεις είναι άχρηστη εναντίον εσωτερικών εχθρών [9].

Οι επιθέσεις ανάλογα με την φύση τους ταξινομούνται σε δύο κατηγορίες και χωρίζονται σε **παθητικές** και **ενεργητικές** επιθέσεις. Οι παθητικές επιθέσεις είναι μια συνεχής ροή πληροφοριών από το δίκτυο, η οποία μπορεί να χρησιμοποιηθεί αργότερα σε κάποια ενεργητική επίθεση. Έτσι ο επιτιθέμενος «κρυφακούει» τα πακέτα που στέλνονται και τα αναλύει για να πάρει χρήσιμες πληροφορίες. Λόγω της φύσης του μέσου διάδοσης των ασύρματων επικοινωνιών που είναι ευρέως διαμοιραζόμενο, είναι εύκολο για έναν επιτιθέμενο να εκκινήσει μια τέτοια επίθεση σε αυτό το περιβάλλον, παρά σε ένα κλασικό ενσύρματο περιβάλλον. Το χαρακτηριστικό ασφαλείας που χρειάζεται σε αυτές τις περιπτώσεις είναι η εμπιστευτικότητα πληροφορίας [20].

Οι ενεργητικές επιθέσεις περιλαμβάνουν σχεδόν όλες τις υπόλοιπες επιθέσεις που ξεκινάνε με ενεργή αλληλεπίδραση με το θύμα, όπως είναι: sleep deprivation torture το οποίο στοχεύει τις μπαταρίες, hijacking στην οποία ο επιτιθέμενος ελέγχει την επικοινωνία μεταξύ δύο οντοτήτων και «μεταμφιέζεται» σε έναν από τους δύο, jamming το οποίο προκαλεί μη διαθεσιμότητα του καναλιού λόγω υπερβολικής χρήσης κ.ά. Οι περισσότερες από αυτές τις επιθέσεις προκαλούν μια κατάσταση που είναι γνωστή ως άρνηση υπηρεσίας (Denial of Service-DoS), η οποία είναι ένας υποβιβασμός ή μια ολική απώλεια επικοινωνίας μεταξύ κόμβων. Ως απειλές κακής συμπεριφοράς ορίζονται αυθαίρετες συμπεριφορές εσωτερικών κόμβων που μπορούν να οδηγήσουν αθέλητα σε καταστροφή άλλων κόμβων. Ο στόχος του

κόμβου δεν είναι να επιτεθεί σε έναν άλλο κόμβο, αλλά μπορεί να έχει άλλους στόχους, όπως να αποκτήσει ένα άδικο πλεονέκτημα σε σύγκριση με άλλους κόμβους.

Κατά την εκτέλεση μιας επίθεσης, οι επιτιθέμενοι έχουν μεγαλύτερη ενέργεια από τους κόμβους του δικτύου. Συνήθως αναγκάζουν τα θύματα να χρησιμοποιούν όλη τους την ενέργεια και τελικά να πεθαίνουν. Έτσι, είναι αναγκαία η άμεση πρόληψη και γνώση μιας απειλής. Οι επιθέσεις σε ένα ασύρματο δίκτυο δεν περιορίζονται σε επιθέσεις άρνησης υπηρεσίας αλλά περιλαμβάνουν μια ποικιλία τεχνικών όπως κατάληψη κόμβου, επιθέσεις εναντίον του πρωτόκολλου δρομολόγησης και επιθέσεις στην φυσική ασφάλεια ενός κόμβου.

5.2.3 Κακή συμπεριφορά

Απειλές κακής συμπεριφοράς ορίζονται οι αυθαίρετες συμπεριφορές εσωτερικών κόμβων που μπορούν να οδηγήσουν αθέλητα σε καταστροφή άλλων κόμβων. Ο στόχος του κόμβου δεν είναι να επιτεθεί σε έναν άλλο κόμβο, αλλά μπορεί να έχει άλλους στόχους, όπως να αποκτήσει ένα άδικο πλεονέκτημα σε σύγκριση με άλλους κόμβους. Σαν παράδειγμα, ένας κόμβος μπορεί να μην εκτελέσει σωστά το πρωτόκολλο MAC με σκοπό να λάβει μεγαλύτερο εύρος ζώνης ή μπορεί να αρνηθεί να προωθήσει πακέτα για άλλους για να μην καταναλώσει κομμάτι της ενέργειάς του, ενώ χρησιμοποιεί την ενέργειά του και ζητά από άλλους κόμβους να προωθούν τα δικά του πακέτα [9].

5.3 Ασφάλεια επιπέδων

5.3.1 Ασφάλεια στο επίπεδο ζεύξης δεδομένων

Το πρότυπο αναφοράς διασύνδεσης ανοικτών συστημάτων (γνωστό ως πρότυπο αναφοράς OSI) αποτελεί μια συνοπτική θεωρητική περιγραφή για τις τηλεπικοινωνίες και το σχεδιασμό πρωτοκόλλου δικτύων. Το στρώμα ζεύξης δεδομένων είναι το δεύτερο από τα επτά επίπεδα του πρότυπου OSI και είναι εκείνο που εξασφαλίζει ότι τα δεδομένα μεταφέρονται σωστά μεταξύ των παρακείμενων κόμβων των δικτύων. Το στρώμα ζεύξης δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για την μεταφορά των δεδομένων μεταξύ των οντοτήτων δικτύων ενώ παράλληλα ανιχνεύει και ενδεχομένως διορθώνει τα λάθη που μπορεί να εμφανιστούν στο φυσικό στρώμα. Οι κύριες λειτουργίες του επιπέδου αυτού που σχετίζονται με την ad hoc δικτύωση είναι η συνδεσιμότητα μονού άλματος (one-hop) και η μετάδοση πλαισίων. Τα πρωτόκολλα του επιπέδου ζεύξης

δεδομένων διατηρούν τη συνδεσιμότητα μεταξύ γειτονικών κόμβων και εξασφαλίζουν την ορθότητα των πλαισίων που μεταφέρονται. Είναι ουσιαστικό να διακριθεί η σχέση των μηχανισμών ασφάλειας που εφαρμόζονται στο στρώμα ζεύξης δεδομένων, όσον αφορά στις απαιτήσεις MANET [19].

Στην περίπτωση των κινητών ad hoc δικτύων, υπάρχουν αξιόπιστα και μη αξιόπιστα περιβάλλοντα. Σε ένα αξιόπιστο περιβάλλον, οι κόμβοι του ad hoc δικτύου ελέγχονται από ένα τρίτο μέρος και μπορούν να καταστούν αξιόπιστοι με βάση την πιστοποίηση (authentication). Η ασφάλεια του στρώματος ζεύξης δεδομένων δικαιολογείται σε αυτήν την περίπτωση από την ανάγκη να καθιερωθεί μια αξιόπιστη υποδομή βασισμένη σε λογικά μέσα ασφάλειας. Εάν μπορεί να εξασφαλισθεί η ακεραιότητα των λειτουργιών υψηλότερων επιπέδων που εφαρμόζονται από τους αξιόπιστους κόμβους, τότε η ασφάλεια του στρώματος ζεύξης δεδομένων μπορεί ακόμη και να καλύψει τις απαιτήσεις ασφάλειας που εγείρονται από υψηλότερα στρώματα συμπεριλαμβανομένων των πρωτοκόλλων δρομολόγησης και εφαρμογής.

Στα μη-αξιόπιστα περιβάλλοντα, η εμπιστοσύνη στα υψηλότερα στρώματα όπως τα πρωτόκολλα δρομολόγησης ή εφαρμογής, δεν μπορεί να βασιστεί στους μηχανισμούς ασφάλειας του στρώματος ζεύξης δεδομένων. Η μόνη σχετική χρήση των τελευταίων εμφανίζεται να είναι η πιστοποίηση κόμβου προς κόμβο και η ακεραιότητα των δεδομένων, όπως απαιτείται από το στρώμα δρομολόγησης. Επιπλέον, ο κύριος περιορισμός στην επέκταση των υπαρχουσών λύσεων ασφάλειας στρώματος ζεύξης δεδομένων είναι η έλλειψη υποστήριξης για την αυτοματοποιημένη διαχείριση κλειδιών, που είναι επιβεβλημένη στα ανοικτά περιβάλλοντα όπου η χειροκίνητη εγκατάσταση κλειδιών δεν είναι κατάλληλη.

Η κύρια απαίτηση για τους μηχανισμούς ασφάλειας του στρώματος ζεύξης δεδομένων είναι η ανάγκη να αντιμετωπιστεί η έλλειψη φυσικής ασφάλειας στα ασύρματα τμήματα της επικοινωνιακής υποδομής. Οι μηχανισμοί στρώματος ζεύξης δεδομένων, όπως αυτοί που παρέχονται από το 802.11 και το Bluetooth, χρησιμεύουν βασικά για τις ενισχύσεις ελέγχου και ατομικότητας πρόσβασης ώστε να αντιμετωπιστούν οι ευπάθειες των ράδιο-τηλεπικοινωνιακών ζεύξεων. Εντούτοις, η ασφάλεια ζεύξης δεδομένων που εκτελείται σε κάθε άλμα δεν μπορεί να καλύψει τις από άκρο σε άκρο απαιτήσεις ασφάλειας των εφαρμογών, ούτε στις ασύρματες συνδέσεις που προστατεύονται από το IEEE 802.11 ή το Bluetooth, ούτε στις φυσικά προστατευμένες ενσύρματες συνδέσεις.

Οι πρόσφατες ερευνητικές προσπάθειες έχουν προσδιορίσει τις ευπάθειες στο WEP και υπάρχουν διάφοροι τύποι κρυπτογραφικών επιθέσεων λόγω της κακής χρήσης των αρχών κρυπτογράφησης. Το πρωτόκολλο IEEE 802.11 είναι επίσης ευάλωτο στις επιθέσεις DoS όπου ο αντίπαλος μπορεί να εκμεταλλευτεί το δυαδικό εκθετικό back-off σχήμα του και να αρνηθεί την πρόσβαση στο ασύρματο κανάλι από τους τοπικούς γείτονές του. Επιπλέον, ένας συνεχώς μεταδίδων κόμβος μπορεί πάντα να 'συλλάβει' το κανάλι και να θέσει τους άλλους κόμβους σε μια ατέρμονη back-off κατάσταση, έτσι ώστε να προκαλέσει μια αλυσιδωτή αντίδραση από τα πρωτόκολλα ανωτέρων επιπέδων (π.χ. διαχείριση παραθύρων TCP).Μια άλλη επίθεση DoS ισχύει επίσης στο IEEE 802.11 με τη χρήση του πεδίου NAV, το οποίο δείχνει τη δέσμευση καναλιών και μεταφέρεται στο αίτημα να σταλούν ή να χαθούν τα πλαίσια RTS/CTS. Ο αντίπαλος μπορεί να 'κρυφακούσει' τις πληροφορίες NAV και έπειτα σκόπιμα να εισάγει ένα λάθος ενός bit στο πλαίσιο του στρώματος ζεύξης του θύματος μέσω ασύρματης παρεμβολής. Τα πρωτόκολλα ασφάλειας του στρώματος ζεύξης πρέπει να παρέχουν ασφάλεια μεταξύ ομότιμων (peer to peer), όπου οι ομότιμοι είναι οι άμεσα συνδεδεμένοι κόμβοι και να εξασφαλίσουν τις μεταδόσεις πλαισίων με την αυτοματοποίηση των κρίσιμων διαδικασιών ασφάλειας συμπεριλαμβανομένων της πιστοποίησης κόμβων, της κρυπτογράφησης πλαισίων, της επαλήθευσης ακεραιότητας δεδομένων και της διαθεσιμότητας κόμβων [20].

5.3.2 Ασφάλεια στο επίπεδο δικτύου

Το στρώμα δικτύου είναι το τρίτο επίπεδο του προτύπου OSI, το οποίο δίνει την κατάλληλη διεύθυνση στα μηνύματα και μεταφράζει τις λογικές διευθύνσεις και τα ονόματα στις φυσικές διευθύνσεις. Καθορίζει επίσης τη διαδρομή από την πηγή στον υπολογιστή προορισμού και διαχειρίζεται τα προβλήματα κυκλοφορίας, όπως η μεταγωγή, η δρομολόγηση και ο έλεγχος συμφόρησης των πακέτων δεδομένων.

Οι κύριες λειτουργίες δικτύων, οι σχετικές με την ad hoc δικτύωση, είναι η δρομολόγηση και η αποστολή πακέτων δεδομένων [19].

- Τα πρωτόκολλα δρομολόγησης ανταλλάσσουν τα δεδομένα δρομολόγησης μεταξύ των κόμβων και διατηρούν τις καταστάσεις δρομολόγησης σε κάθε κόμβο αναλόγως. Με βάση τις καταστάσεις δρομολόγησης, τα πακέτα δεδομένων διαβιβάζονται από τον ενδιάμεσο κόμβο κατά μήκος μιας ορισμένης διαδρομής προς τον προορισμό. Οι επιτιθέμενοι στα πρωτόκολλα δρομολόγησης μπορούν να εξαγάγουν την κυκλοφορία προς ορισμένους προορισμούς στους συμβιβασμένους κόμβους και να προωθήσουν τα πακέτα κατά μήκος μιας διαδρομής που δεν είναι

η καλύτερη. Οι αντίπαλοι μπορούν επίσης να δημιουργήσουν βρόχους δρομολόγησης στο δίκτυο και να εισάγουν συμφόρηση δικτύων και ανταγωνισμό καναλιού σε ορισμένες περιοχές.

- Εκτός από τις επιθέσεις δρομολόγησης, ο αντίπαλος μπορεί να εκτελέσει επιθέσεις ενάντια στις λειτουργίες προώθησης πακέτου. Τέτοιες επιθέσεις αναγκάζουν τα πακέτα δεδομένων να παραδοθούν με έναν τρόπο που είναι ασυμβίβαστος με τις καταστάσεις δρομολόγησης. Σαν παράδειγμα, ο επιτιθέμενος κατά μήκος μιας ορισμένης διαδρομής μπορεί να απορρίψει τα πακέτα, να τροποποιήσει το περιεχόμενό τους, ή να αναπαράγει πακέτα που έχουν ήδη προωθηθεί. Το DoS είναι ένας άλλος τύπος επίθεσης που στοχεύει στα πρωτόκολλα προώθησης πακέτων και εισάγει ανταγωνισμό ασύρματου καναλιού και ανταγωνισμό δικτύου στα ad hoc δίκτυα.

Τα πρωτόκολλα δρομολόγησης όπως έχει αναφερθεί, μπορούν να διαιρεθούν σε δυναμικά (proactive), αντιδραστικά (reactive) και υβριδικά (hybrid) ανάλογα με την τοπολογία δρομολόγησης. Οι τρέχουσες προσπάθειες για τον σχεδιασμό ασφαλών πρωτοκόλλων δρομολόγησης στρέφονται κυρίως στα αντιδραστικά πρωτόκολλα, όπως η δυναμική δρομολόγηση πηγής (DSR) ή το ad hoc κατόπιν παραγγελίας διάνυσμα απόστασης (AODV), που προτυποποιήθηκαν για να αποδώσουν καλύτερα από τα δυναμικά, με τη σημαντικά χαμηλότερη επιβάρυνση, δεδομένου ότι είναι σε θέση να αντιδρούν γρήγορα στις αλλαγές τοπολογίας κρατώντας την επιβάρυνση δρομολόγησης χαμηλή σε περιόδους ή περιοχές του δικτύου όπου οι αλλαγές είναι λιγότερο συχνές. Τα υφιστάμενα ασφαλή πρωτόκολλα δρομολόγησης λαμβάνουν υπόψη τις ενεργές επιθέσεις που πραγματοποιούνται από τους συμβιβασμένους κόμβους και που αποσκοπούν να διαστρεβλώσουν την εκτέλεση των πρωτοκόλλων δρομολόγησης, ενώ οι ενεργητικές επιθέσεις και τα προβλήματα ιδιοτέλειας κόμβων δεν εξετάζονται.

5.4 Συστήματα ανίχνευσης εισβολών (Industrial Detection System, IDS)

Όπως κάθε επίθεση χρειάζεται μια ανάλογη άμυνα για να υπάρξει αντίσταση, έτσι και στα δίκτυά μας, κάθε τύπος εισβολής χρειάζεται μια αντίστοιχη ηλεκτρονική άμυνα ώστε να αποτρέψουμε κάθε επίδοξο εισβολέα-επιτιθέμενο να καταφέρει να καταλάβει το δίκτυό μας. Μια εισβολή μπορεί να οριστεί ως ένα σύνολο ενεργειών που προσπαθούν να θέσουν σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα, ή τη διαθεσιμότητα ενός πόρου, ή οποιαδήποτε αναρμόδια ή ανεπιθύμητη δραστηριότητα σε ένα σύστημα ή ένα δίκτυο. Ένα

IDS μπορεί να οριστεί ως ένα σύστημα που προσπαθεί να ανιχνεύσει και να προειδοποιήσει για αποπειραθείσες παρεισφρήσεις σε ένα σύστημα ή ένα δίκτυο [9], [18].

Η εμπειρία από την έρευνα σε θέματα ασφάλειας έχει δείξει ότι ανεξάρτητα από το πόσα μέτρα πρόληψης εισβολών παρεμβάλλονται στα δίκτυα, υπάρχουν πάντα μερικές αδυναμίες στα συστήματα που κάποιος εισβολέας θα μπορούσε να εκμεταλλευτεί για να παρεισφρήσει. Αυτές οι αδυναμίες περιλαμβάνουν κυρίως τα λάθη σχεδιασμού και προγραμματισμού. Ως εκ τούτου, τα μέτρα πρόληψης εισβολών δεν μπορούν να αποτρέψουν τις επιθέσεις και πρέπει να ενισχυθούν με IDSs. Ένα IDS παρουσιάζει έναν δεύτερο τοίχο άμυνας και είναι ζωτικό για οποιοδήποτε δίκτυο υψηλής ικανότητας επιβίωσης. Οι αρχικές παραδοχές της ανίχνευσης εισβολής είναι:

- Οι δραστηριότητες χρηστών και προγράμματος είναι παρατηρήσιμες, παραδείγματος χάριν μέσω των μηχανισμών ελέγχου συστημάτων.
- Το πιο σημαντικό, οι κανονικές (normal) δραστηριότητες και οι δραστηριότητες που προέρχονται από εισβολή έχουν διακριτή συμπεριφορά.

Επομένως, η ανίχνευση εισβολής περιλαμβάνει τη σύλληψη των στοιχείων ελεγκτικής παρακολούθησης και την εύρεση ενδείξεων στα στοιχεία για να καθοριστεί εάν το σύστημα είναι υπό επίθεση. Ένα πρότυπο ανίχνευσης εισβολής έχει δύο συστατικά: τα χαρακτηριστικά γνωρίσματα (ιδιότητες ή μέτρα) και τον αλγόριθμο διαμόρφωσης.

Το σημαντικότερο βήμα στην οικοδόμηση ενός αποτελεσματικού προτύπου ανίχνευσης εισβολής είναι ο καθορισμός ενός συνόλου χαρακτηριστικών πρόγνωσης που συλλαμβάνουν με ακρίβεια τις αντιπροσωπευτικές συμπεριφορές των παρεισφρητικών ή κανονικών δραστηριοτήτων και μπορεί να είναι ανεξάρτητο από τον σχεδιασμό του αλγόριθμου διαμόρφωσης. Πρόσφατα, μερικά IDSs έχουν προταθεί για τα MANETs. Η συνεργασία, εντούτοις, μπορεί να διανεμηθεί πλήρως και εξίσου μεταξύ των κόμβων, ή μπορεί να βασιστεί στην ιεραρχική οργάνωση των κόμβων. Κάθε σχέδιο IDS διαφέρει από τη μία λύση στην άλλη.

5.4.1 Αντιμετώπιση εισβολών

Η προσέγγιση για ανθεκτικά στις εισβολές ασύρματα δίκτυα ad hoc που γίνεται βασίζεται σε τρεις ιδέες-κλειδιά:

- Ένας πλήρως αποκεντρωμένος και δυναμικά διευθετούμενος μηχανισμός προστασίας (firewall) που περιορίζει την επίδραση μιας επίθεσης πλημμυρίδας πακέτων στο άμεσο γειτονικό περιβάλλον του κόμβου-εισβολέα.
- Μία αμερόληπτη τεχνική αλγορίθμου δρομολόγησης για ανίχνευση και ανάκτηση από αποτυχημένη δρομολόγηση που προκλήθηκε από εισβολή.
- Μία αρχιτεκτονική ασύρματης επέκτασης δρομολογητή που επιτρέπει στους μηχανισμούς επιβίωσης από επιθέσεις DoS να ενσωματωθούν με μικρή προσπάθεια στις υπάρχουσες ασύρματες υλοποιήσεις συστημάτων.

Το ασύρματο περιβάλλον δικτύωσης χαρακτηρίζεται από τις ακόλουθες τρεις ιδιότητες:

- Υπάρχει μία σχέση εμπιστοσύνης μεταξύ όλων των κόμβων στο ad hoc δίκτυο. Αυτή είναι μία εύλογη παραδοχή για τα είδη των εφαρμογών που υλοποιούνται από τέτοια δίκτυα. Κάθε κόμβος πρέπει να είναι διευθετημένος με τα δημόσια κλειδιά όλων των άλλων κόμβων του δικτύου.
- Χρησιμοποιείται η πιστοποίηση πακέτων για την προστασία της ακεραιότητας όλων των πακέτων δεδομένων που μεταδίδονται στο δίκτυο.
- Όλες οι ασύρματες συνδέσεις στο δίκτυο είναι διπλής κατεύθυνσης και έτσι το δίκτυο χαρακτηρίζεται συμμετρικό.

5.4.2 Κατανεμημένη ασύρματη αντιπυρική ζώνη (firewall)

Σε ένα παραδοσιακό ενσύρματο περιβάλλον δικτύου, το firewall εγκαθίσταται στο σημείο εισόδου/εξόδου του δικτύου ώστε να φιλτράρεται η μη επιτρεπτή κυκλοφορία που προέρχεται από έξω από το όριο του προστατευόμενου δικτύου. Σε ένα ad hoc ασύρματο περιβάλλον όπου οι κόμβοι μπορούν ενδεχομένως να είναι κινητοί, η τοπολογία δικτύων είναι δυναμική και δεν έχει επομένως κανένα νόημα ένα καλά καθορισμένο σημείο εισόδου/εξόδου για το δίκτυο. Επίσης, οποιοσδήποτε κόμβος μέσα στο δίκτυο θα μπορούσε να είναι ο εισβολέας και έτσι η κυκλοφορία επίθεσης θα μπορούσε να δημιουργηθεί από μέσα από το ίδιο το δίκτυο. Επιπλέον, οι παραδοσιακές αντιπυρικές ζώνες δεν σχεδιάζονται για να προστατεύσουν από επιθέσεις πλημμυρίδας πακέτων όπου η κυκλοφορία επίθεσης μεταμφιέζεται σε νόμιμα πακέτα που περνούν από τους κανόνες ελέγχου πρόσβασης του firewall [18].

Εννοιολογικά, η λειτουργία αντιπυρικών ζωνών διανέμεται πλήρως σε όλους τους κόμβους (δηλ. στους ασύρματους δρομολογητές IP) μέσα στο δίκτυο. Κάθε κόμβος στο δίκτυο διατηρεί έναν πίνακα αντιπυρικών ζωνών που περιέχει έναν κατάλογο από τις

επιτρεπόμενες ροές πακέτων που μπορούν να περάσουν μέσω αυτού του κόμβου-δρομολογητή. Μια ροή πακέτων είναι ένα ρεύμα πακέτων από έναν κόμβο πηγής σε έναν προορισμό και προσδιορίζεται μονοσήμαντα από τις IP διευθύνσεις της πηγής και του προορισμού των πακέτων. Το κατανεμημένο ασύρματο firewall σχεδιάζεται για να είναι δυναμικά ρυθμιζόμενο, δηλαδή οι καταχωρήσεις του πίνακα δημιουργούνται και διατηρούνται στο χρόνο εκτέλεσης και δεν είναι στατικά προ-διαμορφωμένες πριν από τη λειτουργία του δικτύου. Οι καταχωρήσεις των πινάκων των αντιπυρικών ζωνών είναι αυτόματα επαναδιαμορφώσιμες σε απάντηση στις αλλαγές της τοπολογίας του δικτύου, καθώς επίσης και στις ανιχνευμένες επιθέσεις πλημμυρίδας. Επιπλέον, η διαμόρφωση και ο έλεγχος του firewall ολοκληρώνεται με ένα συνολικά αποκεντρωμένο τρόπο. Δεν υπάρχει κανένας κεντρικός ελεγκτής ή διαχειριστής αντιπυρικών ζωνών του δικτύου για την εκτέλεση αυτής της λειτουργίας.

Η τελική επίδραση της διανεμημένης αντιπυρικής ζώνης είναι ότι όταν ο κόμβος-εισβολέας παράγει μια πλημμύρα της πλαστής κυκλοφορίας (παραπλανητικά και επαναλαμβανόμενα πακέτα), οι ασύρματοι μηχανισμοί αντιπυρικών ζωνών στους άμεσους one-hop γείτονες του εισβολέα φιλτράρουν την κυκλοφορία επίθεσης. Η δυναμική διαμόρφωση και η συντήρηση των καταχωρήσεων του πίνακα του firewall μέσα στο δίκτυο ενεργοποιείται με το πρωτόκολλο χειραψίας που εκτελείται μεταξύ του αποστολέα και του δέκτη μιας ροής.

5.4.3 Επικαλυπτόμενη δρομολόγηση

Για την ανίχνευση μιας προκληθείσης από εισβολέα αποτυχίας της τρέχουσας διαδρομής μιας ροής, ο αποστολέας της ροής επικαλείται το μηχανισμό δρομολόγησης επικαλύψεων για να ανακαλύψει μια διαδρομή προς τον δέκτη που παρακάμπτει τον εισβολέα. Αυτός ο μηχανισμός σχεδιάζεται ώστε να είναι ανεξάρτητος από τον αλγόριθμο δρομολόγησης. Η νέα διαδρομή μεταξύ της πηγής και του προορισμού είναι μια διαδρομή επικαλύψεων που διαμορφώνεται από μια αλληλουχία δύο tunnel στον φίλιο κόμβο. Εάν ο φίλιος κόμβος δεν παράκαμψε τον εισβολέα και τον περιέλαβε στη διαδρομή, η πρόσφατα επιλεγμένη διαδρομή θα αποτύχει πάλι. Ο αποστολέας επιλέγει έπειτα έναν νέο φίλιο κόμβο και προσπαθεί πάλι έως ότου πετύχει τον σκοπό του ή εξαντλήσει όλους τους φίλιους κόμβους.

5.4.4 Ανίχνευση αποτυχημένης δρομολόγησης

Αυτός ο μηχανισμός όχι μόνο επιτρέπει τον ανασχηματισμό της κατανεμημένης ασύρματης αντιπυρικής ζώνης αλλά και ενεργοποιεί τον μηχανισμό επικαλυπτόμενης δρομολόγησης

που είναι ανθεκτικός σε εισβολές. Η προσέγγιση ανίχνευσης αποτυχημένης δρομολόγησης χρησιμοποιεί ένα μηχανισμό βασισμένο στον δέκτη για να ανιχνεύσει μια επίθεση πλημμυρίδας ή διακοπής της ροής που αρχίζει από ένα εισβολέα στη διαδρομή. Ο αποστολέας τοποθετεί έναν υπογεγραμμένο κώδικα επικύρωσης μηνυμάτων (MAC) στο πεδίο επικεφαλίδας πιστοποίησης ενός πακέτου IP. Ο δέκτης ελέγχει τη MAC του πακέτου ώστε να πιστοποιηθεί η ακεραιότητά του. Η επικεφαλίδα IPSEC περιέχει επίσης ένα πεδίο αριθμού ακολουθίας πακέτων που χρησιμοποιείται από το δέκτη για να ανιχνεύσει τη διπλή παραλαβή πακέτων καθώς επίσης και για να ανιχνεύσει τις απώλειες πακέτων.

Ο δέκτης ελέγχει τρεις παραμέτρους κάθε ροής που καταλήγει σε αυτόν:

- ποσοστό απώλειας πακέτων,
- ποσοστό παραλαβών διπλών πακέτων και
- ποσοστό αποτυχίας επικύρωσης πακέτων, για να ανιχνεύσει τις ανωμαλίες στη συμπεριφορά της ροής που συνιστούν μια επίθεση.

ΚΕΦΑΛΑΙΟ 6

ΣΥΝΔΕΣΗ ΓΕΙΤΟΝΙΚΩΝ ΣΥΣΚΕΥΩΝ ΣΕ ΜΙΚΡΕΣ ΚΥΨΕΛΕΣ ΜΕ ΤΗ ΠΑΡΟΥΣΙΑ ΔΙΑΛΕΙΨΗΣ NAKAGAMI-m ΚΑΙ ΟΜΟΔΙΑΥΛΙΚΗΣ ΠΑΡΕΜΒΟΛΗΣ

6.1 Εισαγωγή

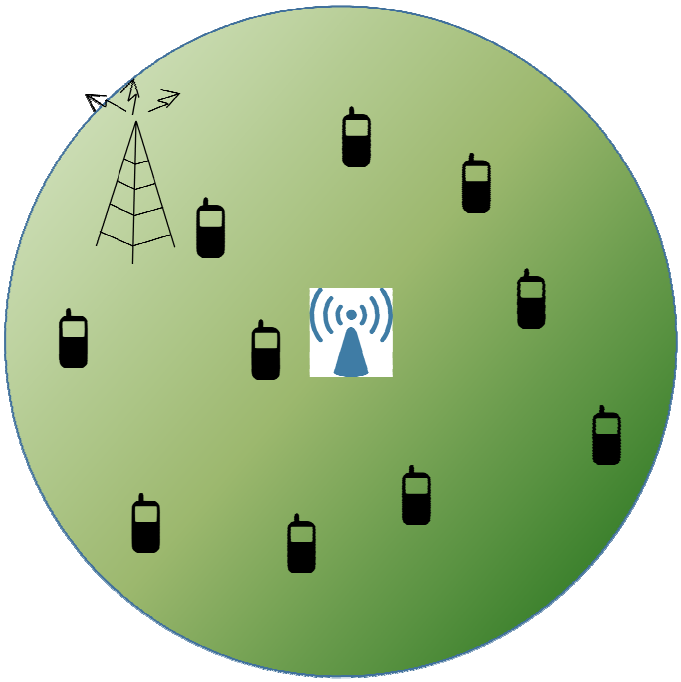
Σε αυτό το κεφάλαιο θα μελετήσουμε τη σύνδεση μίας συσκευής με κάποια άλλη θεωρώντας ότι υπάρχουν πολλές συσκευές τυχαία κατανεμημένες γύρω από την εν λόγω συσκευή σύμφωνα με μια ομογενή σημειακή διαδικασία Poisson. Στην ανάλυση, θα θεωρήσουμε τρεις μετρικές επίτευξης σύνδεσης: i) βασισμένη στο πηλίκο σήματος προς θόρυβο, ii) βασισμένη στο πηλίκο σήματος προς παρεμβολή–και–θόρυβο, και iii) βασισμένη στο πηλίκο σήματος προς παρεμβολή για συστήματα με ισχυρή παρεμβολή. Για κάθε περίπτωση μετρικής σύνδεσης, δημιουργούμε μία προσομοίωση στο Matlab για να υπολογίσουμε την πιθανότητα σύνδεσης με μία ή περισσότερες γειτονικές συσκευές σε περιβάλλον διάλειψης Nakagami-m [21].

Η σύνδεση μίας συσκευής χρήστη με μία άλλη γειτονική μπορεί να επιτευχθεί με βάση είτε τη μέγιστη μακροπρόθεσμη μέση λαμβανόμενη ισχύ, ή με το λόγο λαμβανόμενου σήματος-προς-παρεμβολή-συν-θόρυβο (signal-to-interference-and-noise ratio, SINR). Για την πρώτη μετρική σύνδεσης η διάλειψη του σήματος λήψης και οι παρεμβολές από άλλου πομπούς στην ίδια συχνότητα εκπομπής δεν λαμβάνονται υπόψιν, το οποίο συμβαίνει στη δεύτερη για τον υπολογισμό του στιγμιαίου SINR.

Στη μελέτη μας, θεωρούμε σύνδεση χρήστη με βάση το λόγο σήματος προς θόρυβο (signal-to-noise ratio, SNR) για συστήματα μόνο θορύβου, λόγο σήματος-προς-παρεμβολή (signal-to-interference ratio, SIR) για συστήματα μεγάλης παρεμβολής και SINR για συστήματα με θόρυβο συν παρεμβολή. Η ανάλυση καθώς και το σύστημα προσομοίωσης θεωρούν μία τυπική συσκευή χρήστη που βρίσκεται στο κέντρο ενός δισδιάστατου χώρου, ενώ άλλες συσκευές βρίσκονται τυχαία κατανεμημένες σε μια μεγάλη δισδιάστατη κυκλική περιοχή με μια πυκνότητα συσκευών λ. Χρησιμοποιώντας αυτό το μοντέλο συστήματος, μπορεί να προκύψουν ομοδιαυλικές παρεμβολές από συγκεκριμένες θέσεις εντός της περιοχής επικοινωνίας. Η προτεινόμενη ανάλυση μπορεί να χρησιμοποιηθεί για να εκτιμηθεί η πιθανότητα σύνδεσης της συσκευής που μας ενδιαφέρει με κάποια άλλη.

Με βάση το μοντέλο προσομοίωσης, μπορούμε να μελετήσουμε την επίδραση διαφόρων παραμέτρων του συστήματος, όπως της χωρικής πυκνότητας των άλλων συσκευών, την

ισχύ εκπομπής της συσκευής που μας ενδιαφέρει, το κατώφλι για επίτευξη σύνδεσης, την απόσβεση ισχύος με την απόσταση που καθορίζεται από τον εκθέτη απωλειών διαδρομής, και το ποσό της ομοδιαυλικής παρεμβολής στην επίτευξη συνδεσιμότητας με τουλάχιστον μία άλλη συσκευή.



Σχήμα 6.1 Μοντέλο συστήματος με συσκευές τυχαία κατανεμημένες γύρω από μία συσκευή εκπομπής που βρίσκεται στο κέντρο.

6.2 Μοντέλο συστήματος

Σε αυτή την ενότητα, παρουσιάζουμε το μοντέλο του δικτύου που αποτελείται από μία συσκευή εκπομπής στο κέντρο μιας περιοχής επικοινωνίας με ακτίνα R και έναν αριθμό από άλλες συσκευές, όπως απεικονίζεται στο Σχήμα 6.1. Υποθέτουμε ότι η συσκευή προτιμά να συνδεθεί απευθείας με μία γειτονική συσκευή, αντί του σταθμού βάσης του κυψελωτού συστήματος που την εξυπηρετεί. Ως εκ τούτου, η συσκευή ψάχνει για μία άλλη με την οποία το λαμβανόμενο SINR είναι μεγαλύτερο από ένα προκαθορισμένο κατώφλι SINR β. Εξαιτίας της χωρικής κατανομής Poisson (Poisson point process, PPP), όλες οι συσκευές έχουν τα ίδια στατιστικά στοιχεία του λαμβανόμενου σήματος. Ως εκ τούτου μπορούμε να διεξάγουμε την ανάλυση σε μία τυπική συσκευή χρήστη που βρίσκεται στην αρχή και οι άλλες συσκευές είναι τυχαία κατανεμημένες πάνω σε μια κυκλική περιοχή με ακτίνα R. Υποθέτουμε ότι οι συσκευές είναι ομοιόμορφα κατανεμημένοι σύμφωνα με μια

ομοιογενή PPP με πυκνότητα λ, με λ να είναι ο μέσος όρος των χρηστών MUs ανά μονάδα επιφάνειας [21].

Για μία συσκευή δέκτη που βρίσκεται σε απόσταση d από τη συσκευή πομπού, η υπό συνθήκη συνάρτηση πυκνότητας πιθανότητας του λαμβανόμενου SNR, δίνεται από

$$f_X\left(x|d\right)=\left(\frac{m_s}{\Omega_s}\right)^{m_s}\frac{d^{m_s-1}}{\Gamma\left(m_s\right)}\exp\left(-\frac{m_s}{\Omega_s}x\right) \tag{1}$$

όπου m_S και Ω_S είναι οι παράμετροι της κατανομής. Όταν η λαμβανόμενη ισχύς μειώνεται με το νόμο της δύναμης, το λαμβανόμενο SNR Ω_S σε απόσταση d είναι

$$\Omega_s = P_t \cdot K \cdot r^{-a} / N = \tilde{P}_t \cdot r^{-a} \tag{2}$$

όπου Pt είναι η ισχύς εκπομπής, K είναι μία σταθερά η οποία εξαρτάται από τα χαρακτηριστικά μας κεραίας και την απόσβεση ελευθέρου χώρου μέχρι απόσταση d_0 = 1 m, d είναι μία τυχαία μεταβλητή, α είναι ο εκθέτης μας απώλειας ισχύος, N είναι η ισχύς θορύβου στο δέκτη, και $\tilde{P}_t$ είναι το SNR εκπομπής.

Υποθέτοντας ότι μία άλλη συσκευή βρίσκεται τυχαία τοποθετημένη σε μια κυκλική περιοχή κάλυψης ακτίνας R γύρω από τη συσκευή που μας ενδιαφέρει, η απόσταση d είναι μια τυχαία μεταβλητή $d\in$ [0, R] με συνάρτηση πιθανότητας πυκνότητας (probability density function, PDF)

$$f_d\left(r\right)=\frac{2r}{R^2} \tag{3}$$

Προκύπτει ότι η κατανομή του λαμβανόμενου SNR μπορεί να αποκτηθεί από το μέσο όρο της σχέσης (1) με την PDF της απόστασης που δίνεται στη (2). Κάνοντας την αλλαγή των μεταβλητών $u=(d/R)^{\alpha}$, η PDF του λαμβανόμενου SNR δίνεται από τη σχέση

$$f_X(x)=\frac{1}{\alpha\Gamma(m_s)}\left(\frac{m_s}{\Omega_0}\right)^{-\left(\frac{2}{\alpha}\right)}x^{-\left(\frac{2}{\alpha}+1\right)}\gamma\left(m_s+\frac{2}{\alpha},\frac{m_s x}{\Omega_0}\right) \tag{4}$$

όπου $\Omega_0=\tilde{P}_t R^{-\alpha}$ είναι η λαμβανόμενη ισχύς σε απόσταση R και $\gamma(v,z)=\int_0^z x^{v-1}e^{-x}dx$ είναι η μη ολοκληρωμένη συνάρτηση Γάμμα του πρώτου είδους (incomplete gamma function of the first kind).

Η αθροιστική συνάρτηση κατανομής (CDF) του λαμβανόμενου SNR δίνεται από τη σχέση

$$F_X(x) = \frac{1}{\Gamma(m_s)} \left[\gamma\left(m_s, \frac{m_s x}{\Omega_0}\right) - \left(\frac{m_s x}{\Omega_0}\right)^{-\frac{2}{\alpha}} \gamma\left(m_s + \frac{2}{\alpha}, \frac{m_s x}{\Omega_0}\right) \right] \tag{5}$$

Αν ορίσουμε την πιθανότητα ότι μία συσκευή δέκτης δεν μπορεί να συνδεθεί με τη συσκευή που βρίσκεται στην αρχική θέση, ως την πιθανότητα ότι το λαμβανόμενο SNR στη θέση της συσκευής δέκτη είναι μικρότερο από ένα κατώφλι β, τότε έχουμε

$$F_{\text{SNR}}(\beta) \triangleq \Pr\{X \leq \beta\} = F_X(\beta) \tag{6}$$

6.3 Θεωρητική επίδοση συστήματος

Θεωρούμε έναν κύκλο ακτίνας R με κέντρο τη συσκευή που μας ενδιαφέρει και υποθέτουμε ότι άλλες συσκευές είναι ομοιόμορφα κατανεμημένες πάνω από μια περιοχή δυο διαστάσεων A= πR^2 σύμφωνα με μια ομοιογενή PPPμε πυκνότητα λ. Η πιθανότητα ότι υπάρχουν Q = q συσκευές εντός της περιοχής A είναι μια διακριτή τυχαία μεταβλητή με PDF

$$P_Q(q) = \frac{(\lambda \pi R^2)^q}{q!} e^{-\lambda \pi R^2}, \quad q = 0, 1, \ldots \tag{7}$$

ενώ ο μέσος όρος των συσκευών εντός της περιοχής A δίνεται από

$$\bar{Q}(R, \lambda) = \lambda \pi R^2 \tag{8}$$

Η πιθανότητα ότι τουλάχιστον N συσκευές μπορούν να συνδεθούν στη συσκευή του ενδιαφέροντος μπορεί να ληφθεί με τη βοήθεια της ημιτελούς βήτα συνάρτησης

$$I_p(r, n - r + 1) = \sum_{i=r}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

ως εξής

$$P_{A,N}^{\text{SNR}} = \sum_{q=N}^{\infty} \Pr\left[\text{at least N SNRs exceed } \beta\right] \Pr\left[Q = q\right]$$
$$= \sum_{q=N}^{\infty} \sum_{k=N}^{q} \binom{q}{k} \left[1 - F_{\text{SNR}}\left(\beta\right)\right]^{k} \left[F_{\text{SNR}}\left(\beta\right)\right]^{q-k} \Pr\left[Q = q\right]$$
$$= \sum_{q=N}^{\infty} I_{1-F_{\text{SNR}}(\beta)}\left(N, q - N + 1\right) \frac{\bar{Q}^{q}\left(R, \lambda\right)}{q!} e^{-\bar{Q}(R,\lambda)}$$

(9)

Χρησιμοποιώντας το ορισμένο ολοκλήρωμα της συνάρτησης βήτα

$$I_x(a,b) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \int_0^x t^{a-1}(1-t)^{b-1} dt$$

και αντικαθιστώντας $k = q - N$, η πιθανότητα τουλάχιστον N συσκευές να συνδεθούν με την κεντρική συσκευή λαμβάνεται σε κλειστή μορφή ως

$$P_{\text{A},N}^{\text{SNR}} = \frac{e^{-\bar{Q}(R,\lambda)}}{\Gamma(N)} \int_0^{1-F_{\text{SNR}}(\beta)} t^{N-1}(1-t)^{-N} \times \sum_{k=0}^{\infty} \frac{\left[(1-t)\,\bar{Q}\left(R,\lambda\right)\right]^{N+k}}{k!} dt$$
$$= \frac{\left[\bar{Q}\left(R,\lambda\right)\right]^{N}}{\Gamma(N)} \int_0^{1-F_{\text{SNR}}(\beta)} t^{N-1} e^{-\bar{Q}(R,\lambda)t} dt$$
$$= \frac{1}{\Gamma(N)} \gamma\left(N, [1 - F_{\text{SNR}}(\beta)]\bar{Q}\left(R,\lambda\right)\right), \quad N = 1, 2, \ldots$$

(10)

Επιπλέον, για την ειδική περίπτωση του $N = 1$, παίρνουμε την έκφραση κλειστής μορφής

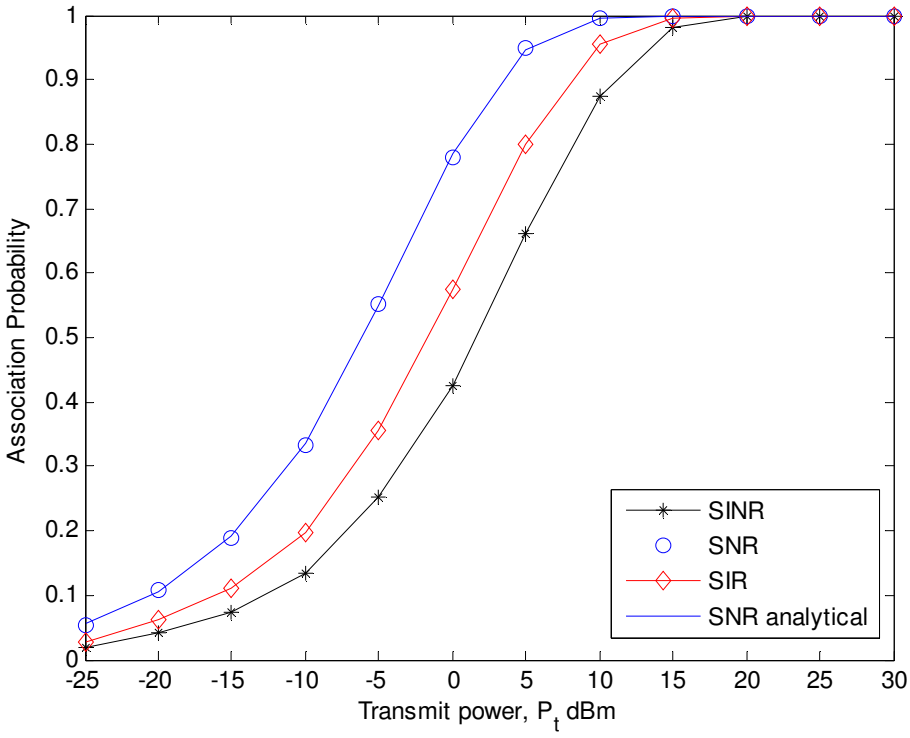
$$P_{\text{A},N=1}^{\text{SNR}} = \frac{1}{\Gamma(N)} \gamma\left(N, [1 - F_{\text{SNR}}(\beta)]\bar{Q}\left(R,\lambda\right)\right)\Big|_{N=1}$$
$$= 1 - \exp\left([F_{\text{SNR}}(\beta) - 1]\bar{Q}\left(R,\lambda\right)\right)$$

(11)

6.4 Αριθμητικά αποτελέσματα προσομοίωσης

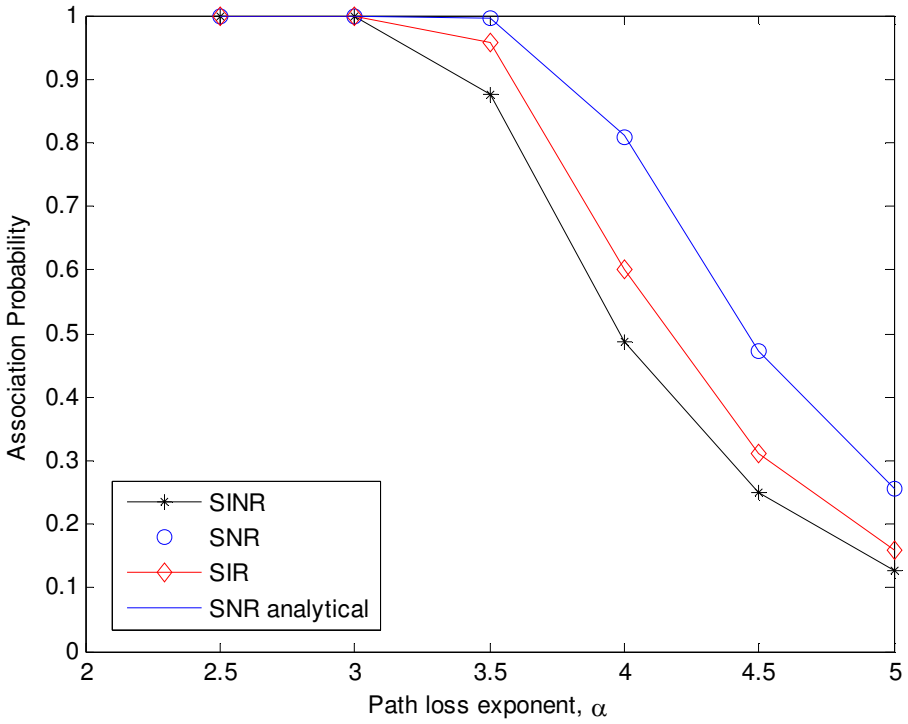
Στην ενότητα αυτή παρουσιάζουμε τα αριθμητικά αποτελέσματα και τα αποτελέσματα προσομοίωσης για να απεικονίσουμε την επίδραση των παραμέτρων του συστήματος στην πιθανότητα σύνδεσης συσκευών δέκτη με μία συσκευή πομπού που βρίσκεται στο κέντρο μίας περιοχής. Το μοντέλο προσομοίωσης υλοποιείται στο Matlab. Μια περιοχή εξυπηρέτησης ακτίνας R = 500 m χρησιμοποιείται για να διαμορφώσει την πολύ μεγάλη περιοχή του PPP. Όλα τα γραφήματα θεωρούν ένα περιβάλλον διάλειψης Nakagami με m_s = 2 για το σήμα λήψης και m_I = 1 για το σήμα παρεμβολής στη συσκευή δέκτη. Για όλες τις συσκευές δέκτη θεωρούμε σήμα παρεμβολής με λόγο ισχύος παρεμβολής προς θόρυβο (INR) 10 dB. Το κατώφλι σύνδεσης λαμβάνεται να είναι β = 5 dB. Η απόσταση αναφοράς είναι d_0 = 1 m. Στο μοντέλο προσομοίωσης, δημιουργούμε τυχαίες μεταβλητές για την απόσταση και για τη διάλειψη Nakagami της κάθε συσκευής εντός της περιοχής εξυπηρέτησης και παίρνουμε το λαμβανόμενο SINR, προκειμένου να διαπιστώσουμε αν μπορούν να συνδεθούν με τη συσκευή πομπού που βρίσκεται στο κέντρο.

Στο Σχήμα 6.2 σχεδιάζουμε την πιθανότητα ότι τουλάχιστον N = 1 συσκευές δέκτη μπορούν να συνδεθούν με τη συσκευή πομπού για μετρικές σύνδεσης: SNR, SIR, SINR. Το διάγραμμα θεωρεί $\lambda=10^{-4}$ ($\lambda*\pi*R^2$ = 80 συσκευές δέκτη κατά μέσο όρο), εκθέτη απώλειας ισχύος διάδοσης α=4, και δείχνει την επίδραση της ισχύος εκπομπής αλλά και της μετρικής σύνδεσης στη πιθανότητα εύρεσης τουλάχιστον μίας γειτονικής συσκευής για σύνδεση. Για κάθε μια περίπτωση SNR, SIR, SINR καθώς αυξάνεται η ισχύς εκπομπής αυξάνεται και η πιθανότητα σύνδεσης και από κάποια τιμή και άνω του μέσου SNR οι πιθανότητες σύνδεσης και των τριών περιπτώσεων αρχίζουν να λαμβάνουν την τιμή 1. Σημειώνεται ότι με βάση τη σχέση (2) με K=-35 dB και N = -105 dBm, το SNR εκπομπής με εύρος τιμών [45, 100] dB αντιστοιχεί σε ισχύ εκπομπής με εύρος τιμών [-25, 30] dBm.



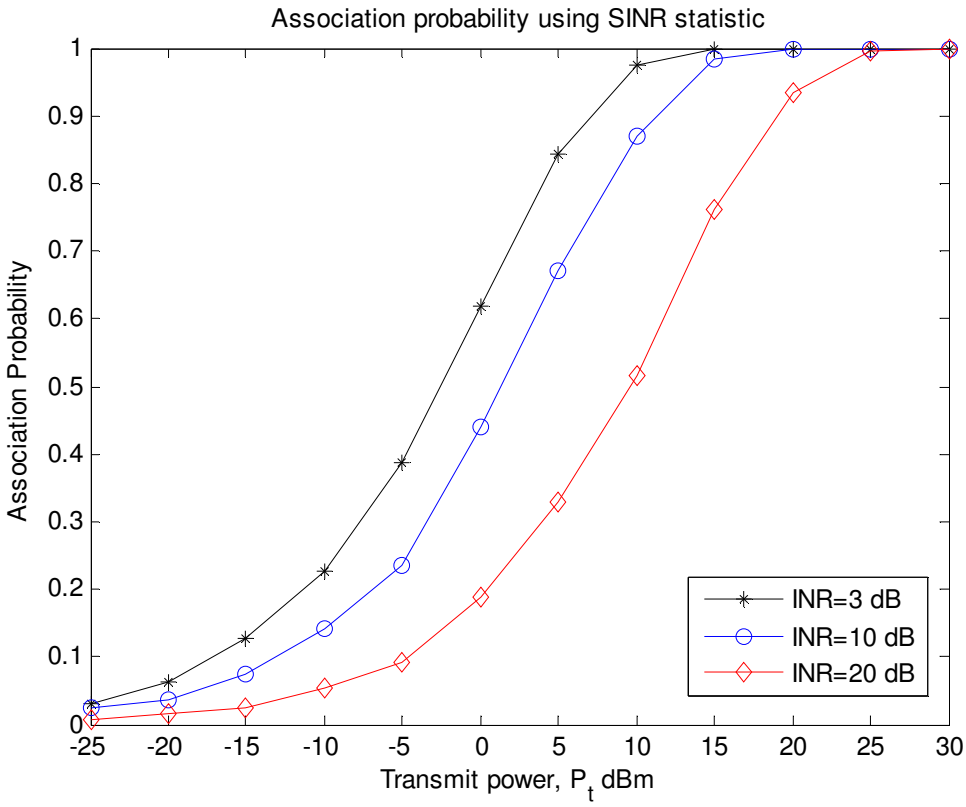
Σχήμα 6.2 Πιθανότητα σύνδεσης με τουλάχιστον μία συσκευή δέκτη συναρτήσει του SNR εκπομπής

Στο Σχήμα 6.3 εξετάζουμε την επίδραση του συντελεστή απωλειών διαδρομής στην πιθανότητα σύνδεσης για κάθε περίπτωση SNR, SIR, SINR. Θεωρούμε ισχύ εκπομπής 10 Bm (SNR εκπομπής 80 dB) και $\lambda = 10^{-4}$. Από το σχεδιάγραμμα παρατηρούμε ότι για κάθε περίπτωση καθώς ο συντελεστής απωλειών αυξάνεται τότε η πιθανότητα σύνδεσης μειώνεται αφού το σήμα λήψης παρουσιάζει μεγαλύτερη εξασθένιση με την απόσταση.



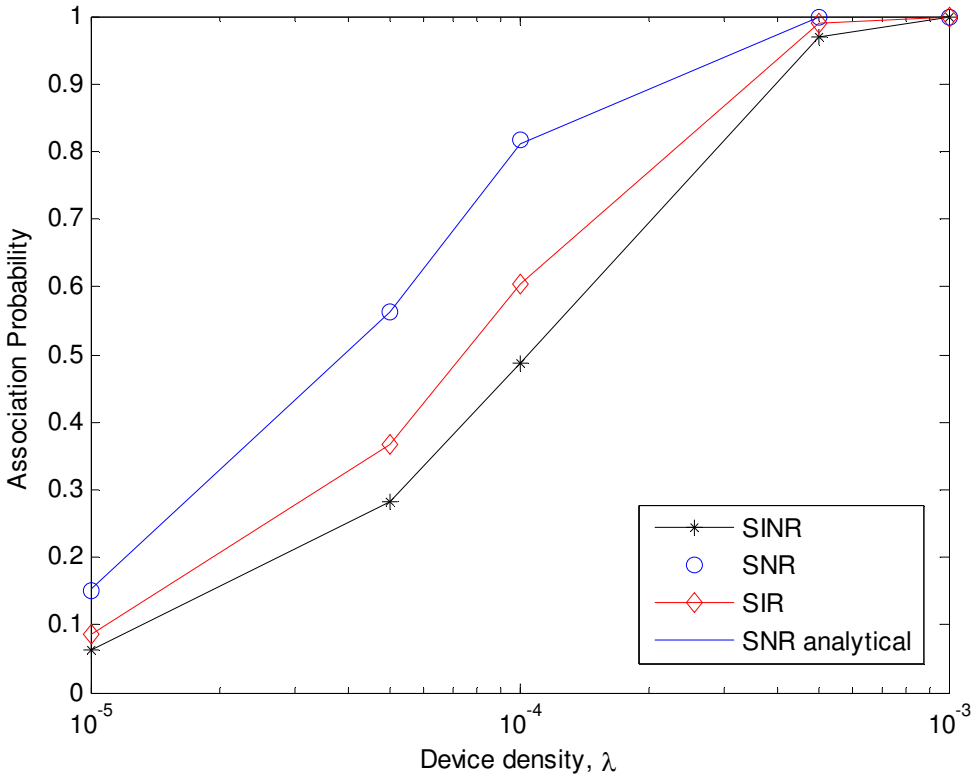
Σχήμα 6.3 Πιθανότητα σύνδεσης με τουλάχιστον μία συσκευή δέκτη συναρτήσει του συντελεστή απώλειας ισχύος, α

Στο Σχήμα 6.4 εξετάζουμε την επίδραση της παρεμβολής (πηλίκο ισχύος παρεμβολής προς θόρυβο INR) στην πιθανότητα σύνδεσης συναρτήσει της εκπεμπόμενης ισχύος για τη περίπτωση SINR, θεωρώντας $\lambda=10^{-4}$ και α=3.5. Από το σχεδιάγραμμα παρατηρούμε ότι με την αύξηση της παρεμβολής η πιθανότητα σύνδεσης μειώνεται.



Σχήμα 6.4 Πιθανότητα σύνδεσης με τουλάχιστον μία συσκευή δέκτη συναρτήσει του SNR εκπομπής

Στο σχήμα 6.5 εξετάζουμε την επίδραση της πυκνότητας χρηστών λ=[1, 5, 10, 20, 50]*10^{-5} όπου ο μέσος αριθμός των χρηστών μέσα σε μια επιφάνεια A= π*R^2 είναι λ*A=λ* π*R^2 =[11, 56, 113, 565, 1131] συσκευές χρηστών στην πιθανότητα σύνδεσης για κάθε περίπτωση SNR, SIR, SINR. Θεωρούμε ισχύ εκπομπής 10 Bm (SNR εκπομπής 80 dB) και εκθέτη απώλειας ισχύος α=4. Από το σχεδιάγραμμα παρατηρούμε ότι για κάθε περίπτωση καθώς αυξάνεται η πυκνότητα χρηστών αυξάνεται και η πιθανότητα σύνδεσης με τουλάχιστον μία συσκευή δέκτη.



Σχήμα 6.5 Πιθανότητα σύνδεσης με τουλάχιστον μία συσκευή δέκτη συναρτήσει της πυκνότητας των χρηστών δέκτη, λ.

6.5 Συμπεράσματα

Στο κεφάλαιο αυτό μελετήσαμε την πιθανότητα σύνδεσης μίας συσκευής πομπού με τουλάχιστον μία άλλη συσκευή δέκτη. Οι συσκευές δέκτη κατανέμονται τυχαία στο χώρο γύρω από τον πομπό. Θεωρήσαμε κανάλι διάλειψης Nakagami-m με την παρουσία ομοδιαυλικής παρεμβολής. Στη θεωρία δώσαμε μία κλειστής μορφής έκφραση για την πιθανότητα ότι τουλάχιστον N συσκευές δέκτη συνδέονται, χρησιμοποιώντας ως κριτήριο το SNR, με τη συσκευή πομπού που μας ενδιαφέρει το οποίο βρίσκεται στο κέντρο μίας γεωγραφικής περιοχής. Επίσης δημιουργήσαμε μία προσομοίωση στο Matlab ώστε να υπολογίσουμε τη πιθανότητα σύνδεσης με βάση τα κριτήρια SNR, SIR και SINR για σύνδεση. Στα αριθμητικά αποτελέσματα, διερευνήσαμε την επίδραση της ισχύος εκπομπής, του εκθέτη απωλειών διάδοσης, την πυκνότητα των συσκευών δέκτη, και της ισχύος της ομοδιαυλικής παρεμβολής στην πιθανότητα σύνδεσης με τουλάχιστον μία συσκευή δέκτη.

ΠΑΡΑΡΤΗΜΑ Α

ΚΩΔΙΚΑΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΠΡΟΣΟΜΟΙΩΣΗΣ

Α.1 Κώδικας προγράμματος σχήματος 6.2

```
clear
num_snapshots=10^4;
r_cell=600;          %cell radius in meters
Lamda = 10^(-4);     %for Poisson distributed devices
n_path=3.5;            %path loss factor

m_s=2;           % Nakagami fading parameter for D2D
m_I=1;           % Nakagami fading parameter for interferer
omega=1;         % average channel power
omega_I=10;      % Interference-to-Noise Ratio (INR)

g_th_dB = 5; %dB
g_th = 10^(g_th_dB/10);
K=-35;
N=-105;

% transmit power = Pt_SNR - K + Noise
Pt = [-25:5:30];  % transmit power
Pt_SNR = Pt + K -N

La=Lamda*pi*r_cell^2;

for kk=1:length(Pt)

    P_max = 10^(Pt_SNR(kk)/10);  % maximum power
    Omega = P_max*(1/r_cell)^(n_path);  % received power at distance
R

    s = (gamma(m_s)*gammainc(m_s*g_th/Omega,m_s)-...
        (m_s*g_th/Omega)^(-2/n_path)*gamma(m_s+2/n_path)*...
        gammainc(m_s*g_th/Omega, m_s+2/n_path));

outage =(1/gamma(m_s))*s; %outage probability, matrix

conn_SNR_theory(kk) = 1-exp((outage -1)*La) %association probability

for ii=1:num_snapshots

    connect1=0;
    connect2=0;
    connect3=0;

for jj=1:La

%---place the desired mobile within the selected sector---
des_user_r=sqrt(rand(1).*(r_cell^2));

%desired user
P_rec_desired = Pt_SNR(kk) + 10*log10(gamrnd(m_s,omega/m_s,1))-
10.*n_path.*log10(des_user_r);
```

```
%Computation of received interference
clear P_rec_I
P_rec_I=gamrnd(m_I,omega_I/m_I,1);

%Computation of received SNR, SIR, SINR
P_SINR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I+1));
P_SNR_dB = P_rec_desired;
P_SIR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I));

if P_SINR_dB >= g_th_dB
    connect1 = connect1+1;
end
if P_SNR_dB >= g_th_dB
    connect2 = connect2+1;
end
if P_SIR_dB >= g_th_dB
    connect3 = connect3+1;
end

end
conn1(ii)=connect1;
conn2(ii)=connect2;
conn3(ii)=connect3;
end

conn_SNIR(kk) = sum(conn1>=1)/num_snapshots
conn_SNR(kk) = sum(conn2>=1)/num_snapshots
conn_SIR(kk) = sum(conn3>=1)/num_snapshots

end

plot(Pt, conn_SNIR, 'k*-')
hold on
plot(Pt, conn_SNR, 'bo')
hold on
plot(Pt, conn_SIR, 'rd-')
hold on
plot(Pt, conn_SNR_theory, '-')
axis([-25 30 0 1])
xlabel('Transmit power, P_t dBm')
ylabel('Association Probability')
legend('SINR','SNR','SIR','SNR analytical')


save plot_pt_a35_lamda-4_gth5 conn_SNIR conn_SNR conn_SIR
conn_SNR_theory
```

A.2 Κώδικας προγράμματος σχήματος 6.3

```
clear
num_snapshots=5*10^3;
r_cell=600;          %cell radius in meters
Lamda = 10^(-4);  %for Poisson distributed MUs
n_path=[2.5, 3, 3.5, 4, 4.5, 5];           %path loss factor for MUs

m_s=2;           % Nakagami fading parameter for MU
m_I=1;           % Nakagami fading parameter for interferer
omega=1;         % average channel power
omega_I=10;      % Interference-to-Noise Ratio (INR)

g_th_dB = 5; %dB
g_th = 10^(g_th_dB/10);
K=-35;
N=-105;

% transmit power = Pt_SNR - K + Noise
Pt = 10;  % transmit power
Pt_SNR = Pt + K -N
P_max = 10^(Pt_SNR/10);  % maximum power

for kk=1:length(n_path)

    Omega = P_max*(1/r_cell)^(n_path(kk));  % received power at
distance R
    La = Lamda*pi*r_cell^2

    s = (gamma(m_s)*gammainc(m_s*g_th/Omega,m_s)-...
        (m_s*g_th/Omega)^(-2/n_path(kk))*gamma(m_s+2/n_path(kk))*...
        gammainc(m_s*g_th/Omega, m_s+2/n_path(kk)));

outage =(1/gamma(m_s))*s; %outage probability, matrix

conn_SNR_theory(kk) = 1-exp((outage -1)*La) %association probability

for ii=1:num_snapshots

    connect1=0;
    connect2=0;
    connect3=0;

for jj=1:La

%---place the desired mobile within the selected sector---
des_user_r=sqrt(rand(1).*(r_cell^2));

%desired user
P_rec_desired = Pt_SNR + 10*log10(gamrnd(m_s,omega/m_s,1))-
10.*n_path(kk).*log10(des_user_r);

%Computation of received interference
clear P_rec_I
P_rec_I=gamrnd(m_I,omega_I/m_I,1);

%Computation of received SNR, SIR, SINR
P_SINR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I+1));
```

```
P_SNR_dB = P_rec_desired;
P_SIR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I));

if P_SINR_dB >= g_th_dB
    connect1 = connect1+1;
end
if P_SNR_dB >= g_th_dB
    connect2 = connect2+1;
end
if P_SIR_dB >= g_th_dB
    connect3 = connect3+1;
end

end
conn1(ii)=connect1;
conn2(ii)=connect2;
conn3(ii)=connect3;
end

conn_SNIR(kk) = sum(conn1>=1)/num_snapshots
conn_SNR(kk) = sum(conn2>=1)/num_snapshots
conn_SIR(kk) = sum(conn3>=1)/num_snapshots

end

plot(n_path, conn_SNIR, 'k*-')
hold on
plot(n_path, conn_SNR, 'bo')
hold on
plot(n_path, conn_SIR, 'rd-')
hold on
semilogx(n_path, conn_SNR_theory, '-')
axis([2 5 0 1])
xlabel('Path loss exponent, \alpha')
ylabel('Association Probability')
legend('SINR','SNR','SIR', 'SNR analytical')

save plot_alpha_lamda4_pt10_gth5 conn_SNIR conn_SNR conn_SIR
conn_SNR_theory
```

A.3 Κώδικας προγράμματος σχήματος 6.4

```
clear
num_snapshots=5*10^3;
r_cell=600;          %cell radius in meters
Lamda = 10^(-4);  %for Poisson distributed MUs
n_path=3.5;           %path loss factor for MUs

m_s=2;          % Nakagami fading parameter for MU
m_I=1;          % Nakagami fading parameter for interferer
omega=1;        % average channel power
omega_I_dB=[3 10 20];     % Interference-to-Noise Ratio (INR)
omega_I=10.^(omega_I_dB/10);

g_th_dB = 5; %dB
g_th = 10^(g_th_dB/10);
K=-35;
N=-105;
 % transmit power = Pt_SNR - K + Noise
Pt = [-25:5:30];  % transmit power
Pt_SNR = Pt + K -N

La=Lamda*pi*r_cell^2;

for gg=1:length(omega_I_dB)

    for kk=1:length(Pt)

        for ii=1:num_snapshots

    connect1=0;
    connect2=0;
    connect3=0;

for jj=1:La

%---place the desired mobile within the selected sector---
des_user_r=sqrt(rand(1).*(r_cell^2));

%desired user
P_rec_desired = Pt_SNR(kk) + 10*log10(gamrnd(m_s,omega/m_s,1))-
10.*n_path.*log10(des_user_r);

%Computation of received interference
clear P_rec_I
P_rec_I=gamrnd(m_I,omega_I(gg)/m_I,1);

%Computation of received SNR, SIR, SINR
P_SINR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I+1));
P_SNR_dB = P_rec_desired;
P_SIR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I));

if P_SINR_dB >= g_th_dB
    connect1 = connect1+1;
end
if P_SNR_dB >= g_th_dB
    connect2 = connect2+1;
end
if P_SIR_dB >= g_th_dB
```

```
    connect3 = connect3+1;
end

end
conn1(ii)=connect1;
conn2(ii)=connect2;
conn3(ii)=connect3;
end

conn_SNIR(gg,kk) = sum(conn1>=1)/num_snapshots
conn_SNR(gg,kk) = sum(conn2>=1)/num_snapshots
conn_SIR(gg,kk) = sum(conn3>=1)/num_snapshots


    end

end

plot(Pt, conn_SNIR(1,:), 'k*-')
hold on
plot(Pt, conn_SNIR(2,:), 'bo-')
hold on
plot(Pt, conn_SNIR(3,:), 'rd-')
axis([-25 30 0 1])
title('Association probability using SINR statistic')
xlabel('Transmit power, P_t dBm')
ylabel('Association Probability')
legend('INR=3 dB','INR=10 dB','INR=20 dB')

save plot_INR_a35_lamda-4_gth5 conn_SNIR conn_SNR conn_SIR
```

A.4 Κώδικας προγράμματος σχήματος 6.5

```
clear
num_snapshots=5*10^3;
r_cell=600;          %cell radius in meters
Lamda = [1 5 10 50 100]*10^(-5);  %for Poisson distributed MUs
n_path=4;            %path loss factor for MUs

m_s=2;           % Nakagami fading parameter for MU
m_I=1;           % Nakagami fading parameter for interferer
omega=1;         % average channel power
omega_I=10;      % Interference-to-Noise Ratio (INR)

g_th_dB = 5; %dB
g_th = 10^(g_th_dB/10);
K=-35;
N=-105;

% transmit power = Pt_SNR - K + Noise
Pt = 10;  % transmit power
Pt_SNR = Pt + K -N
P_max = 10^(Pt_SNR/10);  % maximum power
Omega = P_max*(1/r_cell)^(n_path);  % received power at distance R

for kk=1:length(Lamda)

    La=Lamda(kk)*pi*r_cell^2

        s = (gamma(m_s)*gammainc(m_s*g_th/Omega,m_s)-...
        (m_s*g_th/Omega)^(-2/n_path)*gamma(m_s+2/n_path)*...
        gammainc(m_s*g_th/Omega, m_s+2/n_path));

outage =(1/gamma(m_s))*s; %outage probability, matrix

conn_SNR_theory(kk) = 1-exp((outage -1)*La) %association probability

for ii=1:num_snapshots

    connect1=0;
    connect2=0;
    connect3=0;

for jj=1:La

%---place the desired mobile within the selected sector---
des_user_r=sqrt(rand(1).*(r_cell^2));

%desired user
P_rec_desired = Pt_SNR + 10*log10(gamrnd(m_s,omega/m_s,1))-
10.*n_path.*log10(des_user_r);

%Computation of received interference
clear P_rec_I
P_rec_I=gamrnd(m_I,omega_I/m_I,1);

%Computation of received SNR, SIR, SINR
P_SINR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I+1));
P_SNR_dB = P_rec_desired;
```

```
P_SIR_dB = 10*log10((10.^(P_rec_desired/10))/(P_rec_I));

if P_SINR_dB >= g_th_dB
    connect1 = connect1+1;
end
if P_SNR_dB >= g_th_dB
    connect2 = connect2+1;
end
if P_SIR_dB >= g_th_dB
    connect3 = connect3+1;
end

end
conn1(ii)=connect1;
conn2(ii)=connect2;
conn3(ii)=connect3;
end

conn_SNIR(kk) = sum(conn1>=1)/num_snapshots
conn_SNR(kk) = sum(conn2>=1)/num_snapshots
conn_SIR(kk) = sum(conn3>=1)/num_snapshots

end

semilogx(Lamda, conn_SNIR, 'k*-')
hold on
semilogx(Lamda, conn_SNR, 'bo')
hold on
semilogx(Lamda, conn_SIR, 'rd-')
hold on
semilogx(Lamda, conn_SNR_theory, '-')
axis([10^(-5) 10^(-3) 0 1])
xlabel('Device density, \lambda')
ylabel('Association Probability')
legend('SINR','SNR','SIR','SNR analytical')

save plot_lamda_a4_pt10_gth5 conn_SNIR conn_SNR conn_SIR
conn_SNR_theory
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Department of Telecommunications (Bandwidth Efficiency of Wireless Networks of WPAN, WLAN, WMAN and WWAN), Ing. Milan Šimek, Ing. Ivan Míča, Ing. Jan Kacálek, Ing. Radim Burget, Brno University of Technology, Czech Republic , 2007

[2] Μ. Θεολόγου. Δίκτυα Κινητών και Προσωπικών Επικοινωνιών. Εκδόσεις Τζιόλα 2015

[3] Α. Κανάτας, Φ. Κωνσταντίνου, Γ. Πάντος. Συστήματα Κινητών Επικοινωνιών. Εκδόσεις Παπασωτηρίου 2013

[4] W. Stallings. Ασύρματες Επικοινωμίες και Δίκτυα. Εκδόσεις Τζιόλα 2007

[5] Movassaghi, Samaneh; Abolhasan, Mehran; Lipman, Justin; Smith, David; Jamalipour, Abbas (2014). "Wireless Body Area Networks: A Survey". *IEEE Communications Surveys and Tutorials*. IEEE.

[6] *M. R. Yuce & J. Y. Khan (2011). "Wireless Body Area Networks: Technology, Implementation, and Applications". Pan Stanford Publishing. Retrieved December 2011*

[7] Wireless ad hoc networking—The art of networking without a network, Magnus Frodigh, Per Johansson and Peter Larsson, Ericsson Review No. 4, 2000

[8] Ad Hoc Networking An Introduction, Charles E. Perkins, Nokia Research Center,2000

[9] Prasant Mohapatra, Srikanth V. Krishnamurthy. Ad hoc Networks Technologies and Protocols. Springer Science + Business Media Inc. 2005 Boston

[10] Performance of Ad Hoc Routing Protocols: Characteristics and Comparison Sampo Naski Helsinki University of Technology Telecommunications Software and Multimedia Laboratory 2004

[11] International Journal of Engineering Research and General Science Volume 3, Issue 4, Part-2, July-August, 2015 ISSN 2091-2730 139 www.ijergs.org Analysis of MANET Characteristics, Applications and its routing challenges Mayur Bhalia Electronics & Communication Engineering

[12] Internet Connectivity for Ad hoc Mobile Networks Yuan Sun Elizabeth M. Belding-Royer Department of Computer Science University of California, Santa Barbara suny, ebelding E. Perkins Communications System Laboratory Nokia Research Center

[13] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 3, March 2012) 356 Comparison Of

Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property:

[14] http://www.netlab.tkk.fi/opetus/s38030/k02/Papers/08-Nicklas.pdf (Zone Routing Protocol (ZRP) Nicklas Beijar Networking Laboratory, Helsinki University of Technology P.O. Box 3000, FIN-02015 HUT, Finland)

[15] https://arxiv.org/ftp/arxiv/papers/1012/1012.2510.pdf Analyzing Zone Routing Protocol in MANET Applying Authentic Parameter Kamaljit I. Lakhtaria MCA Department, Atmiya Institute of Technology & Science Yogidham, Rajkot, Gujarat, INDIA (3.5) (upoprotokolla)

[16] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, Mobile Ad Hoc Networking. IEEE Pres. john wiley & sons, inc., 2004

[17] ZigBee Wireless Sensor and Control Network. By Ata Elahi, Adam Gschwender Published Oct 29, 2009 by Prentice Hall. Part of the Prentice Hall Communications Engineering and Emerging Technologies Series from Ted Rappaport series.

[18] W. Stallings, *Cryptography and Network Security Principles and Practices,* 3rd ed., Pearson Education Inc., 2003.

[19] Secure Routing for Mobile Ad hoc Networks Panagiotis Papadimitratos and Zygmunt J. Haas Wireless Networks Laboratory, School of Electrical and Computer Engineering, Cornell University, 395 and 323 F.T. Rhodes Hall, Ithaca NY 14853

[20] Security Issues in Mobile Ad Hoc Networks - A Survey Wenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.

[21] George P. Efthymoglou, Constantine Mukasa, and Valentine A. Aalo. User Association to Small Cells in the Presence of Nakagami-m Fading and Co-Channel Interference. ICT 2016, Thessaloniki, Greece.