ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΠΟΛΥΜΕΣΩΝ

Πτυχιακή Εργασία

" Ασύρματα Ad Hoc Δίκτυα: Πρωτόκολλα – Εφαρμογές "

Καραμπότση Νικολέτα
Α.Μ. 395

Επιβλέπων Καθηγητής:
Νικόλαος Τουμανίδης

Πίνακας περιεχομένων

Κεφάλαιο 1
Εισαγωγή

Ο τρόπος με τον οποίο εργάζονται οι άνθρωποι σε ηλεκτρονικούς υπολογιστές έχει αλλάξει κατά πολύ τα τελευταία χρόνια. Η ανάγκη για συνεχή χρήση κάποιας μορφής ηλεκτρονικού υπολογιστή παντού, είναι διαρκώς αυξανόμενη.

Οι άνθρωποι που χρησιμοποιούν ηλεκτρονικούς υπολογιστές στην καθημερινότητα τους δεν μπορούν πλέον να περιορίζονται στα πλαίσια ενός γραφείου. Έχουν την ανάγκη να μπορούν να χρησιμοποιούν τις δυνατότητες ενός υπολογιστή παντού και μάλιστα με εύκολο τρόπο. Η χρήση υπολογιστή στην οποία γίνεται αναφορά εδώ, είναι βέβαια συνυφασμένη με την ταυτόχρονη χρήση των δικτύων στα οποία διασυνδέονται οι ηλεκτρονικοί υπολογιστές.

Η χρήση των laptop και των pocket pc (pda), έλυσε το πρόβλημα της φορητότητας των υπολογιστών και τα τελευταία χρόνια οι διαρκώς αναπτυσσόμενες τεχνολογίες ασυρμάτων δικτύων έλυσαν το πρόβλημα της διασύνδεσης αυτών των υπολογιστών. Η χρήση ενός φορητού υπολογιστή με ασύρματη σύνδεση σε κάποιο τοπικό δίκτυο και κατ' επέκταση με το διαδίκτυο, είναι πλέον μια συνηθισμένη υπόθεση σε πάρα πολλούς χώρους. Εγκαταστάσεις τοπικών ασύρματων δικτύων υπάρχουν σε πάρα πολλούς δημόσιους χώρους, από αεροδρόμια και αίθουσες συνεδρίων μέχρι κοινόχρηστους χώρους πανεπιστημίων και εταιρειών. Επιπλέον, ασύρματες συνδέσεις ενώνουν απομακρυσμένα δίκτυα (π.χ. δύο κτίρια σε μια πόλη) δίνοντας λύσεις εκεί που τα καλώδια δεν μπορούν.

Στην παρούσα πτυχιακή εργασία θα μελετηθεί μια ενδιαφέρουσα κατηγορία ασύρματων δικτύων, τα **ad hoc δίκτυα**. Στα δίκτυα υπολογιστών ο όρος "ad-hoc" χρησιμοποιείται για να δηλώσει μια μέθοδο διασύνδεσης η οποία συνήθως σχετίζεται με ασύρματα δίκτυα. Δεν υπάρχει συγκεκριμένη ορολογία στα ελληνικά η οποία να δηλώνει ένα ad-hoc δίκτυο και ένα τέτοιο δίκτυο ονομάζεται είτε **αδόμητο είτε κατ' απαίτηση δίκτυο**, με τον δεύτερο όρο να επικρατεί στη βιβλιογραφία. 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 οι οποίοι δεν ανήκουν εξ ορισμού και διαρκώς στο δίκτυο αλλά έχουν τη δυνατότητα να εισέρχονται ή να αποχωρούν από αυτό, οποιαδήποτε στιγμή και από οποιοδήποτε σημείο του. Η απουσία σταθερής υποδομής καθιστά αυτά τα πολύ ευέλικτα δίκτυα κατάλληλα για επικοινωνία σε καταστάσεις έκτακτης ανάγκης, σε δύσβατες περιοχές, δικτύωση μεταξύ αυτοκινήτων κλπ., δημιουργεί όμως και ένα σύνολο από νέες απαιτήσεις κατά το σχεδιασμό τους.

Επίσης θα μελετηθούν ειδικές κατηγορίες Ad Hoc δικτύων (δίκτυα αισθητήρων, MANETs, Mesh Networks, VANETs), οι αλγόριθμοι δρομολόγησης, οι εφαρμογές τους καθώς και τα πρωτόκολλα επικοινωνίας IEEE 802.11x, 802.15x, bluetooth, wi-fi και zigbee. Τέλος θα γίνει προσομοίωση της λειτουργίας τους με τη βοήθεια κατάλληλων εργαλείων, όπως το Comnet III.

Κεφάλαιο 2
Ασύρματα δίκτυα

2.1 Γενικά

Η ασύρματη επικοινωνία επιτυγχάνεται μεταξύ ενός πομπού και ενός δέκτη μεταδίδοντας την πληροφορία με τη βοήθεια ραδιοκυμάτων, τα οποία μεταδίδονται στον ελεύθερο χώρο μεταξύ των δύο σημείων.

2.2 Κατηγορίες ασύρματων δικτύων

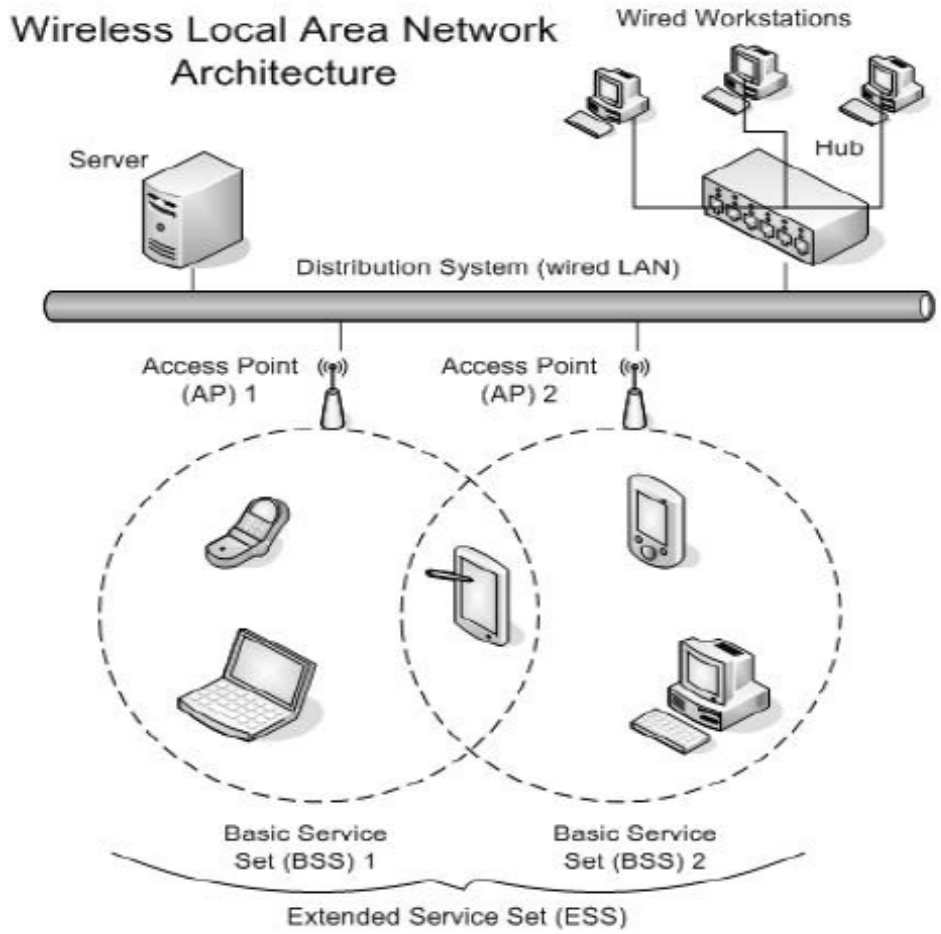
2.2.1 Ασύρματα τοπικά δίκτυα (WLAN)

2.2.1.1 Γενικά

Τα **τοπικά ασύρματα δίκτυα** (**Wireless Local Area Networks – WLAN**) είναι τυπικά παρόμοια με τα τοπικά δίκτυα τα οποία είναι συνδεδεμένα με κάποιας μορφής καλωδίωση. Καλύπτουν μια μικρή γεωγραφική περιοχή η οποία μπορεί να είναι ένα εργαστήριο υπολογιστών, ένας όροφος 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**.

Ένα ασύρματο τοπικό δίκτυο λειτουργεί με παρόμοιο τρόπο με τον οποίο λειτουργεί ένα τοπικό δίκτυο Ethernet. Τα δεδομένα των εφαρμογών κατακερματίζονται σε πακέτα και μεταδίδονται στους άλλους σταθμούς εργασίας. Η διαφορά φυσικά, είναι ότι τα πακέτα μεταδίδονται μέσω ραδιοκυμάτων και όχι μέσω καλωδίων. Όπως και στην περίπτωση του Ethernet (των 10Mbps) το μέσο μετάδοσης είναι κοινό, η επικοινωνία είναι Half-duplex και μόνο ένας σταθμός μπορεί να μεταδίδει πληροφορίες κάθε δεδομένη στιγμή. Ο συναγωνισμός μεταξύ των σταθμών εργασίας για πρόσβαση στο μέσο μετάδοσης γίνεται με ένα **πρωτόκολλο Ανίχνευσης Σήματος / Πολλαπλής Πρόσβασης με αποφυγή συγκρούσεων (Carrier Sense / Multiple Access with Collision Avoidance, CSMA/CA).**

Υπάρχουν πολλά ανταγωνιστικά πρότυπα για ασύρματη δικτύωση σήμερα. Τα πιο δημοφιλή βέβαια (και τα οποία χρησιμοποιούνται πιο πολύ στο εμπόριο) είναι οι διάφορες εκδόσεις του πρότυπου IEEE 802.11. Αυτά είναι το 802.11b (γνωστό και ως Wi-Fi), το 802.11g (επέκταση του 802.11b) και το 802.11a.. Το πρότυπο 802.11 το διαχειρίζεται η Wi-Fi Alliance, γνωστή πιο παλιά ως WECA, ένας μη κερδοσκοπικός οργανισμός που σχηματίστηκε το 1999 για να πιστοποιήσει την διαλειτουργικότητα των προϊόντων ασύρματης τοπικής δικτύωσης.



Εικόνα 1. Αρχιτεκτονική ασύρματου τοπικού δικτύου

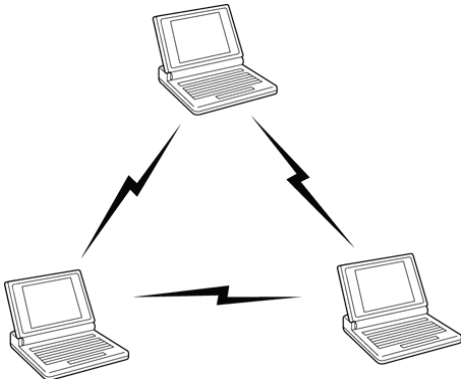
2.2.1.2 Τρόποι σύνδεσης

Το ασύρματο τοπικό δίκτυο μπορεί να είναι ήδη συνδεδεμένο σε ένα υπάρχον ενσύρματο τοπικό δίκτυο σαν επέκταση αυτού ή μπορεί να είναι η βάση για ένα νέο δίκτυο. Παρόλο που τα ασύρματα δίκτυα εφαρμόζονται και σε εσωτερικούς και σε εξωτερικούς χώρους, τα ασύρματα τοπικά δίκτυα ταιριάζουν ειδικότερα σε εσωτερικούς χώρους όπως γραφεία, ακαδημαϊκά ιδρύματα, ξενοδοχεία, νοσοκομεία κ.λ.π.

Η βασική μονάδα ενός ασύρματου τοπικού δικτύου είναι η **κυψέλη**. Η κυψέλη είναι η περιοχή όπου λαμβάνει χώρα η ασύρματη επικοινωνία. Η περιοχή κάλυψης μιας κυψέλης εξαρτάται από την ισχύ του μεταδιδόμενου σήματος και του τύπου και της κατασκευής των τοίχων, των χωρισμάτων και άλλων φυσικών χαρακτηριστικών του εσωτερικού χώρου. Όλοι οι ασύρματοι σταθμοί εργασίας μπορούν να μετακινούνται ελεύθερα μέσα στην κυψέλη.

Independent Basic Service Set (IBSS) ή Ad hoc δίκτυα:

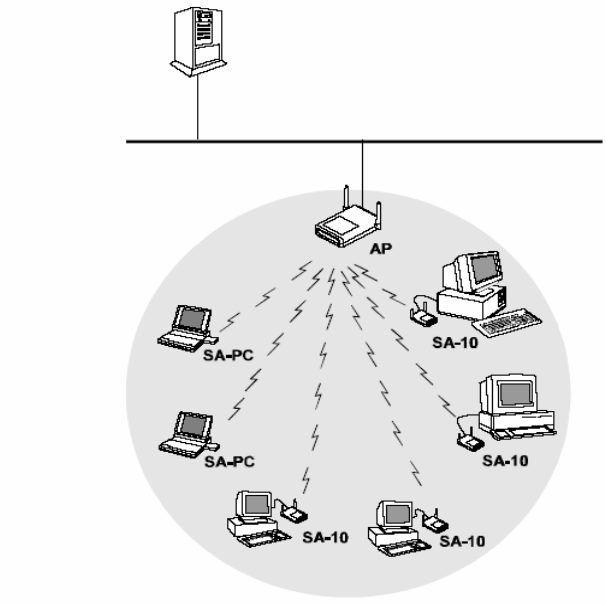
Στα Ad-hoc ασύρματα τοπικά δίκτυα δεν υπάρχει κάποιος κεντρικός διανομέας ο οποίος αναλαμβάνει τη διασύνδεση των υπολογιστών. Οι υπολογιστές επικοινωνούν ο ένας με τον άλλο σε μια αυτόνομη οργάνωση, η οποία δημιουργείται και καταργείται κατά βούληση χωρίς να υπάρχει μια μόνιμη κεντρική υποδομή.



Εικόνα 2. Κυψέλη ad-hoc ασύρματου τοπικού δικτύου.

Basic Service Set (BSS) δίκτυα:

Στα δίκτυα BSS η επικοινωνία μεταξύ των σταθμών επιτυγχάνεται με έναν κεντρικό ασύρματο διανομέα, ο οποίος ονομάζεται **Access Point**. Ο διανομέας αυτός λειτουργεί όπως τα Hub ή Switch στα καλωδιακά δίκτυα Ethernet. Το Access Point μπορεί να είναι συνδεδεμένο ή όχι με καλώδιο σε ένα δίκτυο κορμού ώστε να προωθεί την κίνηση των ασύρματων σταθμών.

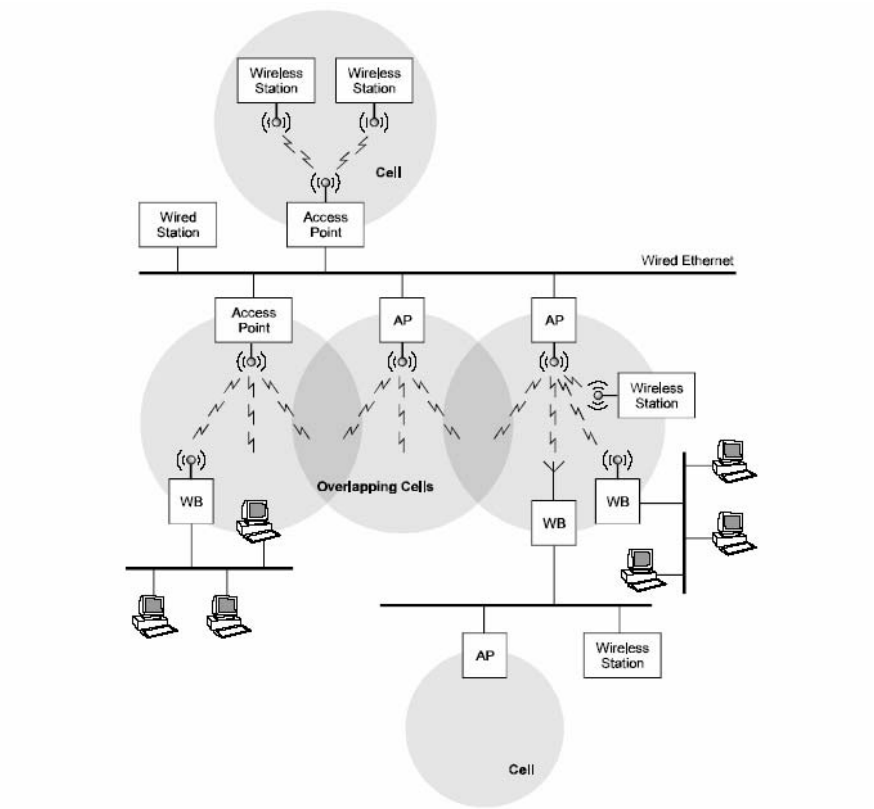


Εικόνα 3. Η κυψέλη ενός τοπικού ασύρματου δικτύου τοπολογίας BSS.

Το Access Point αναλαμβάνει την επικοινωνία μεταξύ των σταθμών και μπορεί να είναι συνδεδεμένο ή όχι σε ένα δίκτυο κορμού.

Extended Service Set (ESS) δίκτυα:

Στην περίπτωση που υπάρχουν πολλά BSS δίκτυα τα οποία συνδέονται με ένα ενσύρματο δίκτυο κορμού για να σχηματίσουν ένα ευρύτερο δίκτυο τότε η τοπολογία ονομάζεται ESS. Σε αυτά τα δίκτυα μπορεί να υπάρχουν και συσκευές οι οποίες ονομάζονται **ασύρματες γέφυρες** (**Wireless Bridge**). Η ακτίνα κάλυψης του συστήματος μπορεί να αυξηθεί έτσι με την συνένωση πολλών σημείων ασύρματης ζεύξης.



Εικόνα 4. Extended Service Set τοπολογία.

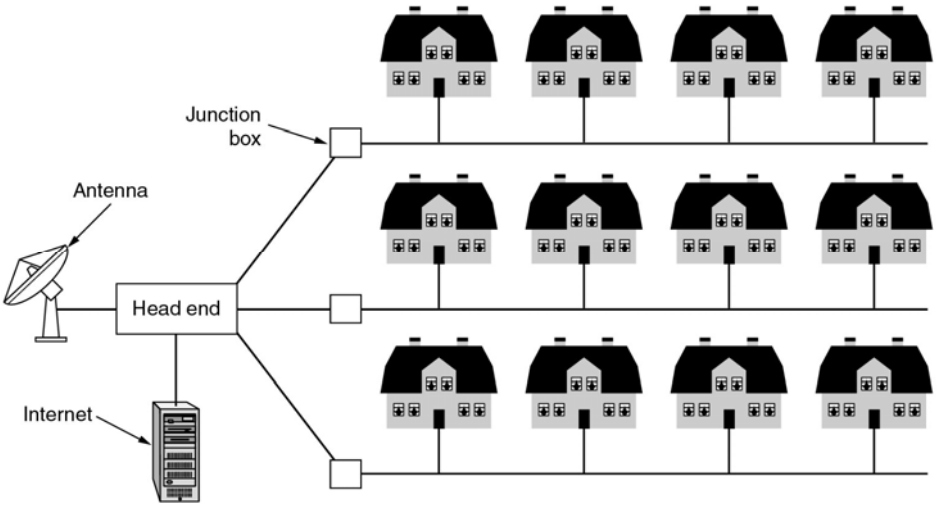
Hot Spots:

Ο όρος **Hot Spot** αναφέρεται στα τοπικά ασύρματα δίκτυα τα οποία παρέχουν πρόσβαση στο Internet και βρίσκονται σε δημόσιους χώρους. Συνήθως είναι προσβάσιμα δωρεάν ή με κάποιο αντίτιμο. Τέτοιο χώροι είναι αεροδρόμια, café ή ακόμα και μεγάλοι κεντρικοί δημόσιοι χώροι σε μια πόλη. Ένα Hot Spot μπορεί να αποτελείται απλά από μια BSS τοπολογία με ασύρματο δρομολογητή που συνδέεται στο Internet ή να απλώνεται σε μεγαλύτερη έκταση με τη χρήση ESS τοπολογίας η οποία περιλαμβάνει και σύνδεση στο Internet.

2.2.2 Ασύρματα μητροπολιτικά δίκτυα (WMAN)

2.2.2.1 Γενικά

Σε αντιστοιχία με τα μητροπολιτικά δίκτυα (MAN) τα οποία συνδέουν απομακρυσμένα σημεία με την χρήση καλωδίων και τεχνολογιών όπως το Frame Relay, το HLDS και τις τεχνολογίες xDSL, τα ασύρματα μητροπολιτικά δίκτυα (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 (Εικόνα 5). Έτσι για την ασύρματη διασύνδεση δύο απομακρυσμένων σημείων θα πρέπει πιθανώς να χρησιμοποιηθεί μια κατευθυντική κεραία υψηλής ισχύος ώστε το σήμα να μην εξασθενεί και να μπορέσει να εστιάσει την ισχύ του στην απέναντι κεραία.

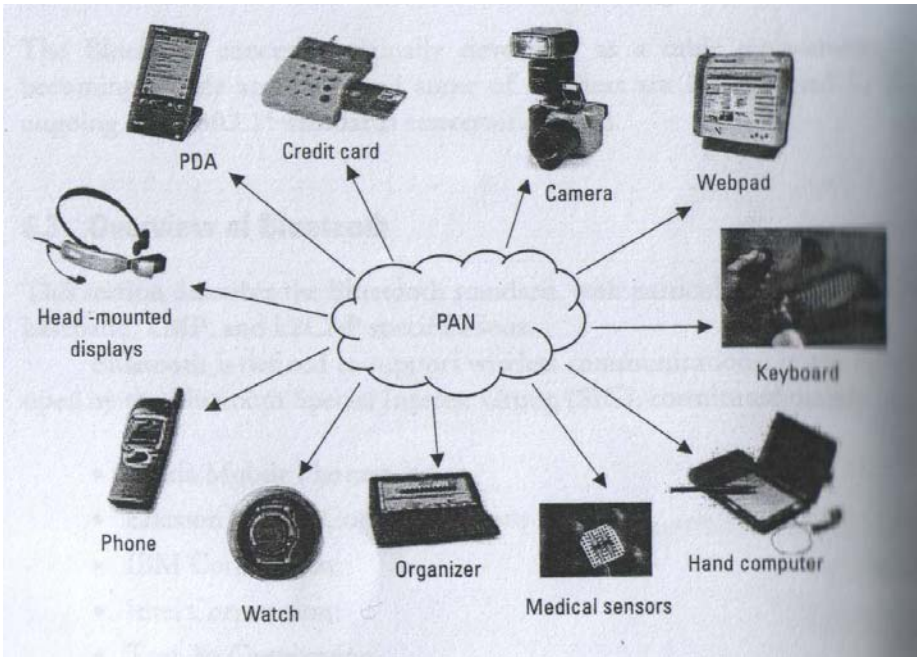


Εικόνα 5. Ασύρματο μητροπολιτικό δίκτυο

2.2.3 Ασύρματα προσωπικά δίκτυα (WPAN)

2.2.3.1 Γενικά

Ο όρος ασύρματα **προσωπικά δίκτυα (Wireless Personal Area Networks – WPAN)** είναι σχετικά σύγχρονος όρος και 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.



Εικόνα 6. Ασύρματο προσωπικό δίκτυο

2.3 Πλεονεκτήματα και μειονεκτήματα των ασύρματων δικτύων

Πλεονεκτήματα:

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

- Οι χρήστες που συνδέονται ασύρματα σε ένα δίκτυο έχουν μια εύκολη, "διαφανή" δικτυακή εμπειρία παρόμοια με αυτή που έχουν οι χρήστες των (συνέχεια συνδεδεμένων) κινητών τηλεφώνων. 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.
- **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.

Τα παραπάνω σαφή πλεονεκτήματα των ασύρματων δικτύων οδηγούν σε κάποια άλλα τα οποία είναι πιο σχετικά με την ακαδημαϊκή εκπαίδευση, όπως:

- Η δικτύωση των φοιτητών και των υπαλλήλων του ιδρύματος με το ακαδημαϊκό δίκτυο και το διαδίκτυο σε αίθουσες διδασκαλίας , εργαστήρια, κοιτώνες και κοινόχρηστες περιοχές, ακόμα και σε εξωτερικούς χώρους.
- Η επέκταση του ακαδημαϊκού δικτύου με μικρό κόστος ακόμα και σε σημεία που πλέον η καλωδίωση είναι δύσκολη, αν όχι αδύνατη.
- Μεγαλύτερη ευελιξία – δεν υπάρχει πλέον η ανάγκη για την μεταφορά των συνδέσεων του τοπικού δικτύου όταν διαμορφώνονται ξανά χώροι όπως γραφεία ή αίθουσες.
- Εύκολη εγκατάσταση δικτυακών συνδέσεων σε μέρη τα οποία χρησιμοποιούνται προσωρινά.
- Εύκολη πρόσβαση των φοιτητών και των υπαλλήλων σε δικτυακές συσκευές όπως εκτυπωτές, σαρωτές και εξυπηρετητές.

Μειονεκτήματα:

Κάθε τεχνολογία έχει και τα μειονεκτήματα της και τα ασύρματα τοπικά δίκτυα δεν αποτελούν εξαίρεση. Πολλές από τις ευκολίες που προσφέρουν έχουν σαν συνέπεια κάποιες αδυναμίες, οι κυριότερες από τις οποίες είναι:

- **Το μέσο στην ασύρματη μετάδοση είναι κοινόχρηστο και half-duplex**. Τα σημερινά ασύρματα τοπικά δίκτυα λειτουργούν παρόμοια με τα παλιά δίκτυα τεχνολογίας Ethernet. Μόνο ένας σταθμός εργασίας μπορεί να μεταδίδει κάθε στιγμή δεδομένα. Το γεγονός αυτό καθιστά το δίκτυο ευάλωτο σε ένα φαινόμενο γνωστό ως "slamming", δηλαδή την απασχόληση του δικτύου για πολλή ώρα από έναν μόνο σταθμό (εάν π.χ αυτός ο σταθμός μεταφέρει ένα πολύ μεγάλο αρχείο). Τα ασύρματα δίκτυα τύπου Dual-Band περιορίζουν αυτό το πρόβλημα επιτρέποντας σε δεδομένα τύπου streaming και δεδομένα τύπου μεταφοράς αρχείων να διαχωρίζονται σε διαφορετικές συχνότητες.
- **Ένα ασύρματο δίκτυο έχει σημαντικά χαμηλότερο bandwidth από τα σημερινά δίκτυα καλωδίων**. Οι πιο πολλές εταιρείες και ακαδημαϊκά ιδρύματα έχουν εγκαταστήσει δίκτυα μεταγωγής ταχυτήτων 100Mbps στους σταθμούς εργασίας και 100Mbps ή 1000Mbps στον κορμό του δικτύου και στους εξυπηρετητές. Το να υπερφορτώσει κανείς τέτοια δίκτυα (ειδικά μόνο ένας υπολογιστής) είναι εξαιρετικά δύσκολο. Ένα ασύρματο δίκτυο τεχνολογίας 802.11b μπορεί να εξασφαλίσει ταχύτητα 11Mbps σε έναν μόνο σταθμό εργασίας κάθε φορά. Το αντίστοιχο σε ασύρματα δίκτυα τεχνολογίας 802.11a ή 802.11g είναι 54Mbps (σε έναν μόνο σταθμό εργασίας κάθε φορά). Επιπλέον η επιβάρυνση του δικτύου από τα πρωτόκολλα ασύρματης διασύνδεσης, διαχείρισης και αποφυγής συγκρούσεων τυπικά μειώνει το χρήσιμο bandwidth στο 45-50%. Έτσι το ωφέλιμο bandwidth στα δίκτυα 802.11b είναι περί τα 6Mbps ενώ στα 802.11a και 802.11g περί τα 25Mbps.
- **Τα ασύρματα δίκτυα είναι ευάλωτα σε παρεμβολές**. Εάν ένας ισχυρός αναμεταδότης που λειτουργεί στην ίδια ραδιοσυχνότητα με ένα ασύρματο δίκτυο, βρίσκεται κοντά σε αυτό, τότε το δίκτυο μπορεί να καταστεί άχρηστο. Αυτό φυσικά μπορεί να γίνει και με κακόβουλη πρόθεση από κάποιον ο οποίος θέλει να εξαπολύσει μια επίθεση προς το δίκτυο.
- **Τα ασύρματα δίκτυα είναι ευάλωτα σε επιθέσεις**. Από τη στιγμή που το μέσο μετάδοσης είναι κοινόχρηστο, όλοι οι σταθμοί εργασίας μπορούν να "δουν" όλη την κίνηση που διασχίζει το μέσο ακριβώς με τον ίδιο τρόπο που ισχύει στους διασυνδεδεμένους με καλώδιο σε ένα hub σταθμούς εργασίας σε ένα Ethernet δίκτυο. Εάν δεν ληφθούν κάποια μέτρα για την προστασία των δεδομένων που μεταδίδονται στο μέσο, τότε αυτά μπορούν να διαβαστούν από εξωτερικούς ή εσωτερικούς κακόβουλους χρήστες. Μια πολιτική ασφαλείας είναι απαραίτητη σε κάθε εγκατάσταση ασύρματου δικτύου.
- **Τα ασύρματα δίκτυα δεν είναι ασφαλή εξ' ορισμού**. Πρέπει να ληφθεί υπόψιν η ασφάλιση του δικτύου σε πολλά επίπεδα συμπεριλαμβανομένων του ποιος έχει πρόσβαση στο μέσο καθώς και της παράνομης υποκλοπής δεδομένων. Τεχνολογίες όπως το WPA έχουν μειώσει σημαντικά τους κινδύνους τέτοιων δικτύων.

2.4 Εφαρμογές των ασύρματων τοπικών δικτύων

Δεδομένων των πλεονεκτημάτων των ασύρματων δικτύων μπορεί κανείς να σκεφτεί πολλές χρήσεις για μια εγκατάσταση ασύρματου δικτύου. Οι πιο τυπικές από αυτές είναι:

- Πρόσβαση σε e-mail.
- Πρόσβαση σε ημερολόγιο και κοινόχρηστες επαφές μέσω κατάλληλων προγραμμάτων (π.χ Lotus Notes).
- Ανταλλαγή άμεσων μηνυμάτων.
- Πρόσβαση σε web sites.
- Εφαρμογές υποστήριξης συνεργασίας με χαμηλές απαιτήσεις σε bandwidth (π.χ ένα κείμενο word το οποίο συζητείται σε ένα δωμάτιο σύσκεψης).
- Μεγάλες βιομηχανικές μονάδες με τεράστιες ανάγκες καλωδίωσης.

Σε αντιδιαστολή, οι παρακάτω εφαρμογές τυπικά είναι ακατάλληλες για ένα ασύρματο δίκτυο. Αυτό δεν σημαίνει ότι δεν μπορούν να δουλέψουν σε ένα ασύρματο δίκτυο, η απόδοση τους είναι φτωχή:

- Εφαρμογές streaming πολυμέσων (έχουν την τάση να υπερφορτώνουν το μέσο. Π.χ το 802.11b μπορεί να χειριστεί τρεις ασυμπίεστες streaming ροές φωνής ενώ οι ροές video υπερφορτώνουν το μέσο).
- Εργασίες με μεγάλα αρχεία καθώς η μεταφορά μεγάλων αρχείων τείνει να μονοπωλεί το μέσο από τον σταθμό που μεταφέρει το αρχείο.
- Εφαρμογές που χρειάζονται υψηλή ποιότητα στις υπηρεσίες (QoS).

Σε γενικές γραμμές οι εφαρμογές με χαμηλές απαιτήσεις σε bandwidth, οι οποίες μεταδίδουν σε κάποιες στιγμές δεδομένα (όχι όλη την ώρα - bursty εφαρμογές) είναι πιο κατάλληλες για ένα ασύρματο δίκτυο από τις εφαρμογές με υψηλές απαιτήσεις σε bandwidth οι οποίες έχουν την μορφή ροής (stream) στην μετάδοση των δεδομένων.

Κεφάλαιο 3
Ασύρματα Ad hoc Δίκτυα

3.1 Ορισμός και ιδιότητες των Ad hoc Δικτύων

Ένα **ad-hoc ασύρματο** τηλεπικοινωνιακό **δίκτυο** αποτελείται από δύο ή περισσότερους κινητούς κόμβους, υπολογιστικές συσκευές (φορητούς υπολογιστές, υπολογιστές χειρός, κινητά τηλέφωνα κ.τ.λ.), οι οποίοι έχουν δυνατότητα για ασύρματη μετάδοση και λήψη δεδομένων. Οι συσκευές μέσα σε ένα τέτοιο δίκτυο έχουν την δυνατότητα επικοινωνίας με οποιαδήποτε άλλη συσκευή, η οποία βρίσκεται στην εμβέλεια τους ή στην εμβέλεια μιας γειτονικής τους συσκευής. Στην πρώτη περίπτωση η επικοινωνία γίνεται απευθείας μεταξύ των δύο κόμβων, ενώ στην δεύτερη περίπτωση η επικοινωνία γίνεται με τη χρήση ενός ή περισσότερων ενδιάμεσων κόμβων, οι οποίοι αναλαμβάνουν την μεταγωγή των δεδομένων από τον αποστολέα στον παραλήπτη.

Ένα ad-hoc ασύρματο τηλεπικοινωνιακό δίκτυο έχει την δυνατότητα να δημιουργείται δυναμικά και αυτόνομα χωρίς να χρειάζεται την παρουσία άλλων ενεργών και μη ενεργών δικτυακών συσκευών. Αυτό σημαίνει ότι έχει την ικανότητα να μεταβάλλει την τοπολογία του καθώς νέοι κόμβοι μπαίνουν σ' αυτό ή αποχωρούν κάποιοι άλλοι. Οι ίδιοι οι κόμβοι αναλαμβάνουν την διαχείριση των πόρων και την επιτέλεση των λειτουργιών του. Ο όρος ad-hoc σημαίνει ότι το δίκτυο μπορεί να πάρει πολλές μορφές, να αποτελείται από κόμβους που κινούνται στο χώρο, να λειτουργεί αυτόνομα και να είναι διασυνδεόμενο με κάποιο άλλο δίκτυο. Οι συσκευές που μετέχουν σε ένα τέτοιο δίκτυο, πρέπει να μπορούν να αντιλαμβάνονται την παρουσία άλλων συσκευών που θα μπορούσαν να συμμετέχουν στο ίδιο δίκτυο, καθώς και να μπορούν να ενεργοποιήσουν τις κατάλληλες διαδικασίες και πρωτόκολλα διασύνδεσης, ούτως ώστε να είναι αυτό εφικτό, με απώτερο σκοπό την επικοινωνία, την ανταλλαγή δεδομένων και την χρήση των υπηρεσιών του δικτύου.

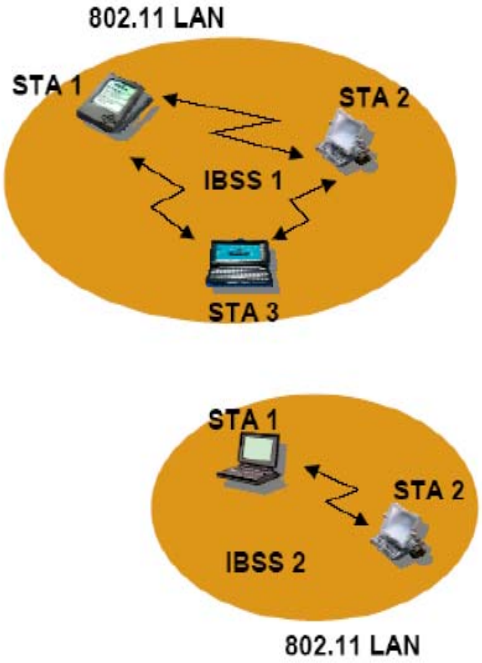
Τα ad hoc δίκτυα επιτρέπουν την εύκολη ανάπτυξη και λειτουργία τους σε πολύ σύντομο χρονικό διάστημα χωρίς να είναι απαραίτητη η χρήση εξειδικευμένων εφαρμογών και η εκτέλεση διαχειριστικών λειτουργιών ή άλλων ενεργειών από τους χρήστες. Ένα άλλο πλεονέκτημα είναι το γεγονός ότι δεν απαιτείται η χρήση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

3.2 Λειτουργία των Ad hoc Δικτύων

Τα ασύρματα δίκτυα ad-hoc αποτελούνται από **κινητούς κόμβους** οι οποίοι πρέπει να επιτελέσουν επιπλέον έργο για να μπορέσει το δίκτυο να λειτουργήσει. Στην περίπτωση που μας αφορά, οι κόμβοι των δικτύων αυτών πρέπει να φροντίσουν να εκτελούνται οι βασικές λειτουργίες ενός δικτύου για τη μεταγωγή δεδομένων μεταξύ των κόμβων του, εργασία που στα κλασσικά δίκτυα την επιτελούν οι δρομολογητές και τα άλλα ενεργά μη τερματικά στοιχεία του δικτύου. Η καταγραφή των βέλτιστων διαδρομών, μέσω των ενεργών συνδέσεων ενός δικτύου για την μεταφορά δεδομένων, είναι από τις βασικότερες λειτουργίες που πρέπει να έχει ένα δίκτυο υπολογιστών, αφού πολύ απλά χωρίς αυτή δεν είναι δυνατό να υπάρξει.

Υπάρχουν πολλά διαφορετικά είδη πρωτοκόλλων διαθέσιμα σήμερα για την δρομολόγηση δεδομένων σε ένα δίκτυο υπολογιστών, τα οποία μπορούν να λειτουργήσουν αρκετά ικανοποιητικά. Τα πρωτόκολλα αυτά είναι σχεδιασμένα να μπορούν να λειτουργήσουν σε ένα ad-hoc δίκτυο, το οποίο δεν έχει την υποδομή που έχουν τα κλασσικά δίκτυα. Πολλά από τα πρωτόκολλα που έχουμε διαθέσιμα, στα κλασσικά ενσύρματα δίκτυα, δεν μπορούν να λειτουργήσουν σε δίκτυα χωρίς υποδομή. Για να είναι δυνατή η λειτουργία τους, είναι απαραίτητες κάποιες αλλαγές για να μπορέσουν να προσαρμοστούν στα χαρακτηριστικά των ad-hoc

δικτύων. Από παρατηρήσεις, πειράματα και προσομοιώσεις που έχουν γίνει, τα πρωτόκολλα αυτά σε καμία περίπτωση δεν μπορούν να έχουν την ίδια απόδοση με αυτή που έχουν όταν εφαρμόζονται στα κλασσικά δίκτυα. Το γεγονός αυτό μας κάνει να πιστεύουμε ότι για να αντιμετωπίσουμε αποτελεσματικά το πρόβλημα της δρομολόγησης χρειαζόμαστε νέα πρωτόκολλα, τα οποία θα δημιουργηθούν για να λειτουργούν αποκλειστικά σε συνθήκες όπως αυτές που υπάρχουν στα ad-hoc δίκτυα.



Εικόνα 7. Ασύρματο Ad hoc δίκτυο

3.3 Χαρακτηριστικά των Ad hoc Δικτύων

Ένα ad hoc δίκτυο συνήθως αποτελείται από μικρό αριθμό κόμβων κάθε φορά, γεγονός όχι απόλυτο, οι οποίοι μπορεί να εισέρχονται και να εξέρχονται από το δίκτυο με εντελώς τυχαία συχνότητα. Το δίκτυο είναι ετερογενές, δεν αποτελείται δηλαδή από έναν τύπο συσκευών. Μπορεί να αποτελείται από ένα σύνολο PDA, κινητών τηλεφώνων, φορητών υπολογιστών κτλ. τα οποία πρέπει να έχουν δυνατότητα επικοινωνίας μεταξύ τους. Η κατανομή των κόμβων αυτών στο χώρο καθορίζει και την τοπολογία που θα χρησιμοποιηθεί. Αν για παράδειγμα όλες οι συσκευές βρίσκονται πολύ κοντά η μία με την άλλη, είναι εφικτή μία σύνδεση απλού hop από κόμβο σε κόμβο. Αντίθετα αν το δίκτυο εκτείνεται σε μεγάλη γεωγραφική έκταση, απαιτείται **multi-hop** διασύνδεση μεταξύ των κόμβων. Η σημασία των ad hoc δικτύων είναι πολύ μεγάλη, κυρίως χάρη στην ευκολία και ταχύτητα με την οποία μπορούν να εγκατασταθούν, αφού δεν απαιτούν την ύπαρξη σταθερής υποδομής. Ένα ακόμα πλεονέκτημα της δυναμικής τους φύσης είναι η εύκολη προσθήκη και απομάκρυνση νέων κόμβων, καθώς και το γεγονός ότι κάθε κόμβος εξαρτάται μόνο από τους γειτονικούς του, με αποτέλεσμα την αυξημένη αξιοπιστία των δικτύων αυτών.

Τα ad hoc δίκτυα παρουσιάζουν σημαντική ανομοιογένεια, αφού κάθε κόμβος

μπορεί να διαφέρει από τους υπόλοιπους σε πολλά χαρακτηριστικά, όπως την υπολογιστική ισχύ, την ακτίνα εκπομπής ή τη διάρκεια ζωής των μπαταριών (αν π.χ. είναι ένας φορητός υπολογιστής ή ένα PDA). Επιπλέον, τα διάφορα ad hoc δίκτυα μπορεί να διαφέρουν σε πολλά χαρακτηριστικά τους, όπως τους χρησιμοποιούμενους ρυθμούς επικοινωνίας, στο αν παρέχουν δυνατότητες broadcast ή multicast, στο αν συνυπάρχουν ή όχι με άλλα δίκτυα τα οποία έχουν κάποια σταθερή υποδομή ή τέλος, αν υποστηρίζουν την κινητικότητα των χρηστών και με τι ρυθμούς.

Σημαντικό ρόλο σε κάθε ad hoc δίκτυο παίζει 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. Από την άλλη μεριά, 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 ad hoc δίκτυα και συχνά η σημαντικότερη στα MANET. Έτσι, η ακτίνα μετάδοσης θα πρέπει να είναι όσο το δυνατό μικρότερη, φροντίζοντας όμως ταυτόχρονα να μην είναι τόσο μικρή που το δίκτυο να παύει να είναι συνεκτικό. Μια καλή επιλογή είναι, συνήθως, να επιλέγεται ακτίνα μετάδοσης, έτσι ώστε κάθε μετάδοση να "ακούγεται" από περίπου 6 κόμβους.

Οι Micah Adler και Christian Scheideler, προτείνουν ένα μοντέλο τριών επιπέδων για την περιγραφή ενός δικτύου ad-hoc. Αρχικά, έχουμε το **επίπεδο ελέγχου προσπέλασης μέσου (Medium Access Control layer)**, το οποίο είναι υπεύθυνο για την επικοινωνία από σημείο–σε-σημείο (node-to-node) στο φυσικό μέσο. Ακολούθως έχουμε το επίπεδο **επιλογής διαδρομής, (route selection layer)**, το οποίο είναι υπεύθυνο για την εύρεση κατάλληλων διαδρομών για τα πακέτα. Τέλος, έχουμε το **επίπεδο χρονοπρογραμματισμού (scheduling layer)**, που είναι υπεύθυνο για τον καθορισμό της σειράς αποστολής των πακέτων.

3.4 Ποιότητα υπηρεσιών στα ad hoc δίκτυα

Η ποιότητα των υπηρεσιών που προσφέρει ένα δίκτυο, γίνεται αντιληπτή διαφορετικά από τον κάθε χρήστη. Αυτό είναι άμεσο αποτέλεσμα κυρίως των απαιτήσεων που έχει ο καθένας από τα εργαλεία-εφαρμογές που χρησιμοποιεί. Έτσι, ανάμεσα σε κάποιους χρήστες ενός δικτύου, ο πρώτος μπορεί να έχει απαίτηση για μεγάλο εύρος ζώνης από το δίκτυο-εφαρμογή του, ένας δεύτερος μπορεί ν' αποζητά πολύ μικρό χρονικό διάστημα από την αποστολή ενός μηνύματος μέχρι τη λήψη του, ενώ ένας τρίτος μπορεί να θέλει επιβεβαίωση ότι κάθε μήνυμα που στέλνει θα φτάσει στον προορισμό του.

Αυτές οι απαιτήσεις είναι πολύ γενικές για να αναλυθούν περαιτέρω. Έχουν ωστόσο κοινό παρονομαστή, την ποιότητα υπηρεσιών.

Είναι γνωστό ότι η ποιότητα υπηρεσιών που μπορεί να προσφέρει ένα δίκτυο σε μία διεργασία εξαρτάται άμεσα από την ποιότητα του δικτύου. Έτσι μπορούν να τεθούν κάποιες πρώτες αρχές:

1. Στις παραμέτρους του δικτύου:

α) οι διαθέσιμοι πόροι

β) η σταθερότητα των πόρων

2. Το πρωτόκολλο πρέπει να είναι πλήρως προσαρμοζόμενο στις γεωγραφικές αλλαγές του δικτύου, στη μεταβολή των διαθέσιμων πόρων αλλά και στη μικρή χωρητικότητα του δικτύου.

Οπότε είμαστε αναγκασμένοι, για ν' απλοποιήσουμε το πρόβλημα, να ορίσουμε κάποιες μετρικές ώστε να μπορούμε να έχουμε κάποια μέτρηση της ποιότητας υπηρεσιών που προσφέρεται. Αυτές μπορούν να χωριστούν στις εξής κατηγόριες:

- **ALMs - Application Layer Metrics**
- **NLMs - Network Layer Metrics**
- **MLMs - MAC Layer Metrics**

Οι MLM και NLM δίνουν μία εκτίμηση της ποιότητας των συνδέσεων, αλλά και τις ικανότητας τους να παράγουν διαδρομές με καλή ποιότητα και σε μικρό χρόνο. Η μετρική ALM διαλέγει το μονοπάτι που είναι πιθανότερο να συναντά τις απαιτήσεις της διεργασίας. Τέλος, θα πρέπει να υπάρχει η δυνατότητα οι προαναφερόμενες μετρικές να μπορούν να προσαρμοστούν, αν αυτό χρειασθεί, σε δυναμικές ανάγκες και αλλαγές του δικτύου.

Μερικές από τις παραμέτρους που θα πρέπει να λαμβάνονται υπόψιν από τις μετρικές είναι οι εξής:

1. Για το **application layer**
α) η συνολική καθυστέρηση που επηρεάζει κυρίως real time εφαρμογές.
β) η ικανότητα μεταφοράς δεδομένων για εφαρμογές multimedia.

2. Για το **network layer**
α) η κατανάλωση ισχύος.
β) το μέγεθος του buffer.
γ) η σταθερότητα του ρυθμού μετάδοσης / λήψης δεδομένων.
δ) η δυνατότητα διόρθωσης λαθών με κώδικα μεταβλητού μήκους.

3. Για το **επίπεδο MAC**
α) το SNR.

Ακόμα θα πρέπει να αναφερθεί η δυνατότητα που υπάρχει για την παροχή δυναμικά **μεταβαλλόμενης ποιότητας υπηρεσιών (dynamic QoS)**. Αυτό μπορεί να επιτευχθεί με τη χρήση κατάλληλου υλικού, που πλέον είναι διαθέσιμο.

3.5 Προβλήματα, Προκλήσεις

Ένα από τα σημαντικότερα προβλήματα στα ad hoc δίκτυα είναι **η δρομολόγηση**. Ο λόγος είναι ότι οι περισσότεροι από τους γνωστούς αλγόριθμους δρομολόγησης έχουν σχεδιαστεί ώστε να λειτουργούν κάτω από συνθήκες οι οποίες είναι πολύ πιο ευνοϊκές από αυτές που ισχύουν σε ασύρματα δίκτυα. Μία από τις βασικότερες ιδιαιτερότητες που πρέπει να αντιμετωπίσουν οι αλγόριθμοι δρομολόγησης των ασύρματων δικτύων είναι η **κινητικότητα των χρηστών**, η οποία αλλάζει πολύ συχνά την τοπολογία του δικτύου, με αποτέλεσμα να απαιτείται η κατασκευή νέων διαδρομών. Επιπρόσθετα, εξαιτίας του περιορισμένου διαθέσιμου εύρους ζώνης στα ασύρματα δίκτυα, απαιτείται ο αριθμός των σχετικών με την δρομολόγηση μηνυμάτων να είναι περιορισμένος. Επίσης, στα ασύρματα δίκτυα το **ποσοστό των πακέτων που χάνονται είναι αρκετά υψηλό**, τόσο λόγω της αυξημένης πιθανότητας λαθών μετάδοσης, όσο και της αυξημένης πιθανότητας καταστροφής συνδέσμων (π.χ. εξαιτίας της μετακίνησης ενός κόμβου).

Όλα τα παραπάνω έχουν σαν αποτέλεσμα την διαφοροποίηση σε σχέση με τα ενσύρματα δίκτυα των ιδιοτήτων που επιθυμούμε να έχουν οι αλγόριθμοι δρομολόγησης στα ad hoc δίκτυα. Έτσι, τα χρησιμοποιούμενα πρωτόκολλα θα πρέπει να είναι κατανεμημένα, με κάθε κόμβο να είναι αρκετά "έξυπνος" ώστε να μπορεί να παίρνει αποφάσεις δρομολόγησης. Αυτό είναι απαραίτητο, αφού ένα κεντρικοποιημένο πρωτόκολλο δρομολόγησης δεν θα ήταν αξιόπιστο σε περίπτωση

κίνησης των κόμβων. Επιπρόσθετα, το πρωτόκολλο θα πρέπει να δημιουργεί γρήγορα δρομολογήσεις, για να μπορούν να χρησιμοποιηθούν πριν αλλάξει η τοπολογία του δικτύου, διατηρώντας παράλληλα το επιπλεόν φορτίο στο δίκτυο, για τους σκοπούς της δρομολόγησης, χαμηλό. Εκτός όλων αυτών, το πρωτόκολλο δρομολόγησης είναι επιθυμητό να μπορεί να παίρνει αποφάσεις δρομολόγησης βασιζόμενες και στην ενεργειακή κατάσταση κάθε κόμβου, καθώς και στην πιθανή επίδραση αυτών των αποφάσεων σε αυτήν. Τέλος, κάθε σύνδεσμος μεταξύ κόμβων θα πρέπει να θεωρείται από το πρωτόκολλο δρομολόγησης ως μίας κατεύθυνσης, αφού η επικοινωνία προς την μία κατεύθυνση μπορεί να περιορίζεται από φυσικούς παράγοντες ή και τη μορφολογία του χώρου, την ακτίνα εκπομπής κάθε κόμβου και άλλα.

Απ' όσα αναφέρθηκαν παραπάνω, η ύπαρξη πληθώρας διαθέσιμων πρωτοκόλλων δρομολόγησης θα πρέπει να είναι αναμενόμενη. Σε γενικές γραμμές μπορούμε να πούμε ότι δεν υπάρχει ένα πρωτόκολλο δρομολόγησης κατάλληλο για την πλειοψηφία των ad hoc δικτύων, αλλά σε κάθε ad hoc δίκτυο το πρωτόκολλο δρομολόγησης επιλέγεται με βάση τα ιδιαίτερα χαρακτηριστικά του.

Οι τρέχουσες προκλήσεις που τα ad hoc ασύρματα δίκτυα καλούνται ν' απαντήσουν είναι :

1) Multicast
2) QOS υποστήριξη
3) Power aware routing
4) Location aid routing

Όπως προαναφέρθηκε, το multicast είναι επιθυμητό ώστε να υποστηρίξει ασύρματες επικοινωνίες πολλαπλών χρηστών. Δεδομένου ότι η ιεραρχία multicast δεν είναι πλέον στατική (η τοπολογία του μεταβάλλεται στο χρόνο), το πρωτόκολλο δρομολόγησης multicast θα πρέπει να μπορεί να ανταπεξέλθει με την κινητικότητα αυτή, συμπεριλαμβανομένου της δυναμικής multicast membership. Σε όρους QOS, είναι ανεπαρκές να θεωρηθεί το QOS μονάχα στο επίπεδο του δικτύου χωρίς να λάβει υπόψη του το υποκείμενο media access control layer. Λαμβάνοντας υπόψη τα προβλήματα που συσχετίζονται με τη δυναμική των κόμβων, τα κρυμμένα τερματικά και τα μεταβαλλόμενα χαρακτηριστικά των επικοινωνιακών δεσμών, η υποστήριξη end to end QOS είναι θέμα που απαιτεί περισσότερη διερεύνηση. Προς το παρόν, υπάρχει η τάση για μια προσέγγιση ενός προσαρμόσιμου QOS από μια απλή μέθοδο συγκράτησης πόρων με QOS guarantees. Άλλος σημαντικός παράγοντας είναι η περιορισμένη δυνατότητα παροχής ισχύος των φορητών συσκευών που μπορούν να δημιουργήσουν προβλήματα στην μετάδοση των πακέτων σε ένα κινητό περιβάλλον ad hoc. Επιπλέον η δρομολόγηση του επικοινωνιακού φόρτου βασιζόμενη στις δυνατότητες ισχύος των κόμβων, είναι ένας τρόπος για το διαχωρισμό των δρομολογητών που έχουν μεγαλύτερη διάρκεια ζωής από κάποιους άλλους. Τέλος αντί της χρήσης αναζήτησης μέσα από beaconing ή broadcast, η δρομολόγηση **location-aided** χρησιμοποιεί πληροφορίες αναφορικά με την τοποθεσία για να προκαθορίσει σχετιζόμενες περιοχές, ώστε η δρομολόγηση να είναι περιορισμένης έκτασης.

Οι υφιστάμενες ad hoc προσεγγίσεις δρομολόγησης έχουν εμφανίσει αρκετά νέα θέματα προς διερεύνηση, όπως είναι η διερεύνηση της ζήτησης του χρήστη και των παραμέτρων που έχουν να κάνουν με τη χρήση της τοποθεσίας, της ισχύος κλπ. Η δυνατότητα προσαρμογής και αυτορύθμισης είναι χαρακτηριστικά κλειδιά αυτών των προσεγγίσεων. Ωστόσο, η ευελιξία αποτελεί ακόμη ένα σημαντικό θέμα. Ένα ευέλικτο ad-hoc πρωτόκολλο δρομολόγησης μπορεί να συμπεριλάβει προσεγγίσεις **table-driven** και **on-demand** που βασίζονται σε δεδομένες καταστάσεις και επικοινωνιακές απαιτήσεις. Η συνύπαρξη των δύο προσεγγίσεων μπορεί να υφίσταται σε ομάδες που είναι **spatially clustered**, με **intra cluster** απασχόληση της table driven προσέγγισης και **inter-cluster** απασχόληση της **demand driven** απασχόλησης ή ανάποδα. Περισσότερη διερεύνηση απαιτείται για

τις δυνατότητες και τη μέτρηση της αποτελεσματικότητας των υβριδικών ad hoc προσεγγίσεων δρομολόγησης.

3.6 Εφαρμογές

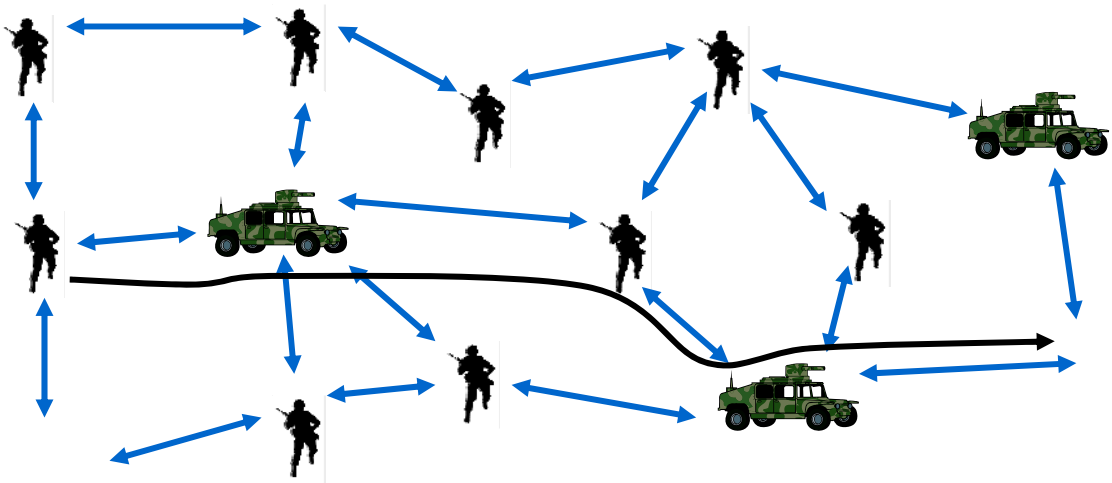
Όπως ακριβώς και τα packet radio networks, έτσι και και τα ad hoc wireless δίκτυα, έχουν σημαντικό ρόλο να διαδραματίσουν σε **στρατιωτικές εφαρμογές**. Στρατιώτες εξοπλισμένοι με κινητές επικοινωνιακές συσκευές που είναι Multi mode μπορούν να επικοινωνούν επί τούτου, χωρίς να χρειάζονται σταθεροί ασύρματοι σταθμοί. Επιπλέον, μικρές κινητές συσκευές εξοπλισμένες με αισθητήρες ακοής και κάμερες μπορούν να τοποθετηθούν σε στρατηγικής σημασίας περιοχές για τη συλλογή πληροφοριών περιβαλλοντικής η χωροταξικής σημασίας, που μπορεί να κατευθυνθούν προς έναν κόμβο επεξεργασίας (processing node) μέσα από συστήματα κινητών επικοινωνιών. Μπορούν να αναπτυχθούν επίσης κινητά συστήματα επικοινωνιών μεταξύ πλοίων, δεδομένου ότι παρέχονται εναλλακτικές διαδρομές επικοινωνίας που δεν στηρίζονται στις υφιστάμενες εναέριες η επίγειες επικοινωνιακές υποδομές.

Εμπορικές εφαρμογές που προτείνονται για ad hoc ασύρματα δίκτυα περιλαμβάνουν:

1) Συνέδρια, συναντήσεις, διαλέξεις
2) Υπηρεσίες έκτακτης ανάγκης

Οι άνθρωποι σήμερα παρακολουθούν διαλέξεις και συνέδρια μέσω φορητών υπολογιστών, υπολογιστών χειρός κλπ. Είναι επιθυμητό επομένως να υπάρχει **άμεση διαμόρφωση δικτύου** και επιπλέον δυνατότητες **διαμοιρασμού αρχείων και πόρων** χωρίς την παρουσία σταθερών σταθμών εργασίας και ειδικών διαχειριστών δικτύου. Ένας παρουσιαστής μπορεί να κάνει multicast διαφάνειες και ήχο σε συγκεκριμένους αποδέκτες.

Επίσης τα ad hoc επικοινωνιακά συστήματα μπορούν να έχουν πρακτική εφαρμογή σε αναμεταδιδόμενες πληροφορίες (π.χ. τρέχουσα κατάσταση, βαθμός ολοκλήρωσης κλπ), μέσω video, data και voice μεταξύ **σωστικών συνεργείων** μέσα από μια μικρή φορητή συσκευή. Αυτό μπορεί να έχει εφαρμογή και σε **αστυνομικές επιχειρήσεις** κλπ.



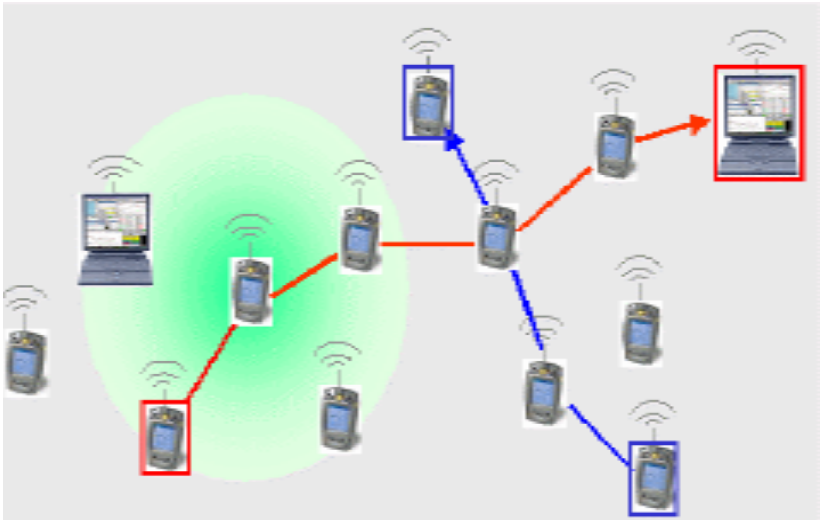
Εικόνα 8. Στρατιωτική εφαρμογή Ad hoc δικτύου

Κεφάλαιο 4
Ειδικές κατηγορίες Ad hoc Δικτύων

4.1 MANETS

4.1.1 Εισαγωγή στα mobile ad hoc networks

Ένα κινητό ειδικό δίκτυο (Mobile Ad hoc Network), είναι ένα **δίκτυο αυτόνομο και χωρίς σταθερή υποδομή**. 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 δικτύου. 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. Πολλές λύσεις έχουν προταθεί για να καταστήσουν τα MANETs ικανά να συνδεθούν με το Διαδίκτυο χρησιμοποιώντας τα πρωτόκολλα κινητών IP.



Εικόνα 9. Mobile ad hoc δίκτυο

4.1.2 Χαρακτηριστικά των MANETS

Ένα manet απαρτίζεται από κόμβους (για παράδειγμα ένα δρομολογητή με πολλαπλούς εξυπηρετητές και ασύρματες συσκευές), οι οποίοι **κινούνται αυθαίρετα**. Οι κόμβοι μπορεί να βρίσκονται πάνω σε αεροπλάνα, πλοία, φορτηγά, ίσως ακόμη και πάνω σε ανθρώπους ή πολύ μικρές συσκευές και μπορεί να υφίστανται πολλαπλοί εξυπηρετητές ανά δρομολογητή. Το σύστημα μπορεί να λειτουργεί απομονωμένα ή διαμέσου πυλών (gateways) και να αλληλεπιδρά με ένα συμβατικό δίκτυο.

Τα Manets έχουν ορισμένα αξιοπρόσεκτα χαρακτηριστικά όπως:

1. **Δυναμικές τοπολογίες:**

Οι κόμβοι δύναται να μετακινούνται αυθαίρετα. Επομένως η τοπολογία του δικτύου, η οποία είναι τυπικά **multihop**, μπορεί να μεταβληθεί τυχαία και με ταχείς ρυθμούς σε απρόβλεπτους χρόνους και μπορεί να απαρτίζεται ταυτόχρονα από δεσμούς διπλής κατεύθυνσης και ασύμμετρους δεσμούς.

2. **Συνδέσμους με χαμηλό εύρος ζώνης και μεταβαλλόμενη χωρητικότητα:**

Οι ασύρματοι σύνδεσμοι θα συνεχίσουν να διατηρούν σημαντικά χαμηλότερη χωρητικότητα από τους αντίστοιχους των συμβατικών δικτύων.

Μια επίδραση των σχετικά χαμηλών χωρητικοτήτων των συνδέσμων, είναι ότι η συμφόρηση αποτελεί περισσότερο τον κανόνα παρά την εξαίρεση, δηλαδή η χωρητικότητα του δικτύου δεν πρόκειται να αγγίξει ή να ξεπεράσει τις συσσωρευμένες απαιτήσεις εφαρμογών. Δεδομένου ότι το κινητό δίκτυο αποτελεί συχνά προέκταση ενός σταθερού συμβατικού δικτύου, οι χρήστες των κινητών δικτύων θα έχουν παρόμοιες απαιτήσεις. Οι απαιτήσεις αυτές θα συνεχίσουν να αυξάνονται καθώς οι αλληλεπιδραστικές εφαρμογές και οι εφαρμογές multimedia θα συνεχίσουν να πληθαίνουν.

3. **Περιορισμούς σε ότι αφορά την κατανάλωση ενέργειας:**

Μερικοί ή όλοι οι κόμβοι σε ένα manet μπορεί να στηρίζονται σε μπαταρίες για την παροχή ισχύος. Για τους κόμβους αυτούς, το θέμα της διαχείρισης ενέργειας αποτελεί ένα από τα σημαντικότερα θέματα βελτιστοποίησης κατά το σχεδιασμό του όλου συστήματος.

4. **Περιορισμένη ασφάλεια:**

Τα κινητά ασύρματα δίκτυα είναι πιο ευάλωτα σε φυσικές απειλές απ’ ότι τα συμβατικά ενσύρματα δίκτυα. Θα πρέπει να δοθεί ιδιαίτερη προσοχή σε θέματα υποκλοπών. Οι υφιστάμενες μέθοδοι ασφάλειας συνδέσμων εφαρμόζονται συχνά στα ασύρματα δίκτυα ώστε να ελαχιστοποιηθούν οι απειλές ασφάλειας. Ως πλεονέκτημα μπορεί να αναφερθεί, ότι η αποκεντρωτική φύση της διαχείρισης ενός manet δικτύου, παρέχει μεγαλύτερη στιβαρότητα σε σχέση με περισσότερο συγκεντρωτικές μεθόδους διαχείρισης.

Επιπλέον, ορισμένα δίκτυα (π.χ. κινητά στρατιωτικά δίκτυα η δίκτυα ταχείας κυκλοφορίας) μπορεί να είναι ιδιαίτερα μεγάλα (δεκάδες ή εκατοντάδες κόμβοι ανά περιοχή δρομολόγησης). Η ανάγκη για εύκολη κλιμάκωση (scalability), αποτελεί κάτι το δεδομένο. Λαμβάνοντας υπόψη τα προαναφερόμενα χαρακτηριστικά, οι μηχανισμοί ώστε να επιτευχθεί η εύκολη κλιμάκωση θεωρούνται επίσης δεδομένοι.

Τα παραπάνω χαρακτηριστικά δημιουργούν ένα σύνολο από υποθέσεις και θέματα αποδοτικότητας που θα πρέπει να ληφθούν υπόψη κατά το σχεδιασμό πρωτοκόλλων που είναι πέρα από αυτά των συμβατικών δικτύων.

4.1.3 Ομάδα εργασίας MANET

Το manet ή Mobile **Ad-hoc NETworking Group** είναι μια ομάδα εργασίας, που στα πλαίσια του **IETF (Internet Engineering Task Force)**, αναπτύσσει και θέτει τα πρότυπα για πρωτόκολλα δρομολόγησης σε ad-hoc δίκτυα. Η κεντρική σελίδα αυτής της ομάδας στο Internet βρίσκεται στη διεύθυνση: **http://www.ietf.org/html.charters/manet-charter.html.**

Ο σκοπός αυτής της ομάδας εργασίας είναι η τυποποίηση πρωτοκόλλων δρομολόγησης IP, κατάλληλα για την εφαρμογή τους σε ασύρματα στατικά και δυναμικά τηλεπικοινωνιακά δίκτυα επικοινωνιών. Η θεμελιώδης σχεδιαστική αρχή των πρωτοκόλλων αυτών είναι τα ιδιαίτερα χαρακτηριστικά που έχουν οι ασύρματες συνδέσεις σε ένα δίκτυο και το πώς αυτά μπορούν να επηρεάσουν ένα πρωτόκολλο δρομολόγησης. Η δρομολόγηση σε ένα δυναμικό ασύρματο δίκτυο επηρεάζεται σε πολύ μεγάλο βαθμό από παράγοντες όπως**, οι σχετικές θέσεις των κόμβων στο δίκτυο, η κίνηση των κόμβων, η εμβέλεια των ασύρματων πομποδεκτών, τα φυσικά εμπόδια ή άλλες πηγές παρεμβολής** που μπορεί να επηρεάζουν την μετάδοση. Τα χαρακτηριστικά αυτά και άλλα τα οποία δεν αναφέρουμε, έχουν σαν αποτέλεσμα η δρομολόγηση να πρέπει να εκτελείται δυναμικά κάτω από διαφορετικές συνθήκες κάθε φορά. Το ζητούμενο λοιπόν και ο στόχος της συγκεκριμένης ομάδας εργασίας είναι η έρευνα και η μελέτη υποψήφιων πρωτοκόλλων δρομολόγησης, τα οποία θα μπορούν να ικανοποιούν τις ιδιαίτερες ανάγκες που παρουσιάζουν τα ασύρματα δίκτυα.

Στο παρελθόν αυτή η ομάδα εργασίας έχει εστιάσει την έρευνα της σε μια ευρεία σειρά από προβλήματα και ζητήματα απόδοσης των σχετικών υποψηφίων πρωτοκόλλων. Πλέον όμως ο σκοπός της είναι η συγκέντρωση και η προώθηση των προδιαγραφών διάφορων πρωτοκόλλων δρομολόγησης σε μορφή RFC (Request For Comments). Μερικά από τα πρωτόκολλα αυτά είναι ο **AODV** και **DSR**. Τα πρωτόκολλα που αναφέραμε είναι αυτά τα οποία παρέμειναν υποψήφια για την έκδοση του τελικού προτύπου, μέσα από μια πλειάδα προτάσεων και υποψηφιοτήτων. Μπορούμε να πούμε ότι είναι τα περισσότερο ώριμα πρωτόκολλα, όσον αφορά την κατανόηση και εφαρμογή των ιδιαίτερων χαρακτηριστικών των MANETs, κάτι που βρίσκουμε σε κάθε ένα από αυτά τα πρωτόκολλα. Αν και αυτά παρέχουν ένα βασικό σύνολο πρωτοκόλλων που καλύπτουν τις απαιτήσεις των MANETs, απαιτείται περισσότερη εμπειρία και πειραματισμός για την απόκτηση μιας καλύτερης άποψης για την συνολική τους απόδοση. Τελικός σκοπός της ομάδας εργασίας αυτής είναι να συντονίσει όλη αυτή την συζήτηση και έρευνα και να βοηθήσει στην καλύτερη και γρηγορότερη αξιοποίηση των γνώσεων και των συμπερασμάτων που εξάγονται από την έρευνα που γίνεται από πολλές ομάδες πάνω στην δρομολόγηση στα Mobile Ad-hoc Networks.

4.1.4 Εφαρμογές

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:

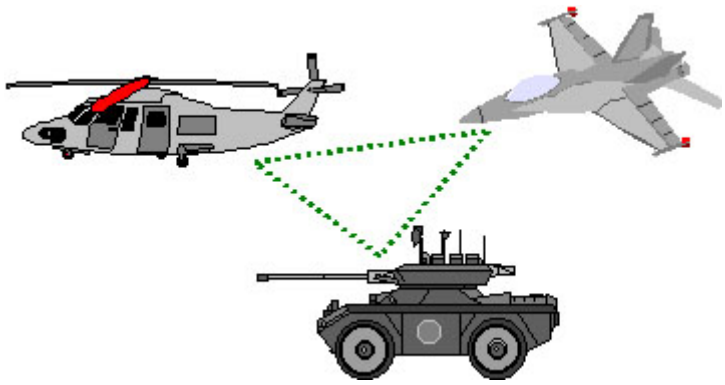
1. Εκπαιδευτικές: για παράδειγμα στα **συνέδρια** ή σε διάφορες διαλέξεις, όπου όλα τα τερματικά και τα access points είναι απαραίτητο να είναι κινητά και στις οποίες έχουμε συγκέντρωση ατόμων με φορητούς υπολογιστές σε μια περιοχή που δεν διαθέτει δίκτυο 802.11. Αφού είναι άμεση ανάγκη για τους σύνεδρους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

2. 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.

3. 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

4. Neighborhood Area Networks (NANs): τα οποία είναι δίκτυα που αναφέρονται στη διαμοιρασμένη πρόσβαση στο Internet σε αστικές τοποθεσίες υψηλής πυκνότητας.

5. Εμπορικές: όπως η αυτοματοποίηση των πωλήσεων ή τα Personal Area Networks (PANs).



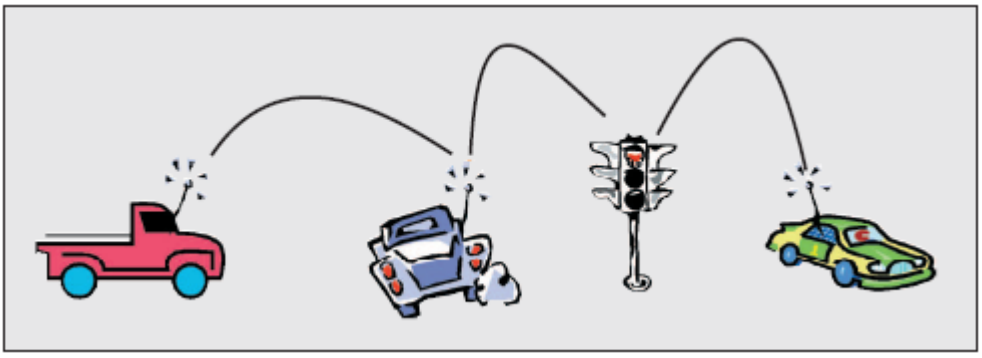
Εικόνα 10. Εφαρμογή Manet σε στρατιωτικά οχήματα

4.2 VANETS

4.2.1 Εισαγωγή στα vehicular ad hoc networks

Ένα **Vehicular Ad-Hoc Network, ή VANET**, είναι μια μορφή Mobile ad-hoc δικτύου, για την παροχή επικοινωνιών μεταξύ οχημάτων και μεταξύ οχημάτων και σταθερού εξοπλισμού, ο οποίος συνήθως περιγράφεται ως οδικός εξοπλισμός.

Ο κύριος στόχος των VANET είναι να παρέχουν ασφάλεια και άνεση στους επιβάτες. Για το σκοπό αυτό, μια ειδική ηλεκτρονική συσκευή θα τοποθετηθεί μέσα σε κάθε όχημα, η οποία θα παρέχει ad hoc σύνδεση δικτύου για την επικοινωνία των οχημάτων σε μια περιοχή. Το δίκτυο αυτό τείνει να λειτουργεί χωρίς καμία υποδομή. Κάθε όχημα εφοδιασμένο με συσκευή VANET, θα είναι ένας κόμβος του ad-hoc δικτύου και θα μπορεί να λαμβάνει και ν' αναμεταδίδει μηνύματα μέσω του ασύρματου δικτύου. **Προειδοποιήσεις σύγκρουσης, προειδοποιήσεις οδικής σηματοδότησης και αξιολόγηση της κυκλοφορίας** θα δώσουν στους οδηγούς τα απαραίτητα εργαλεία για να αποφασίσουν την καλύτερη διαδρομή για να φτάσουν στον προορισμό τους.



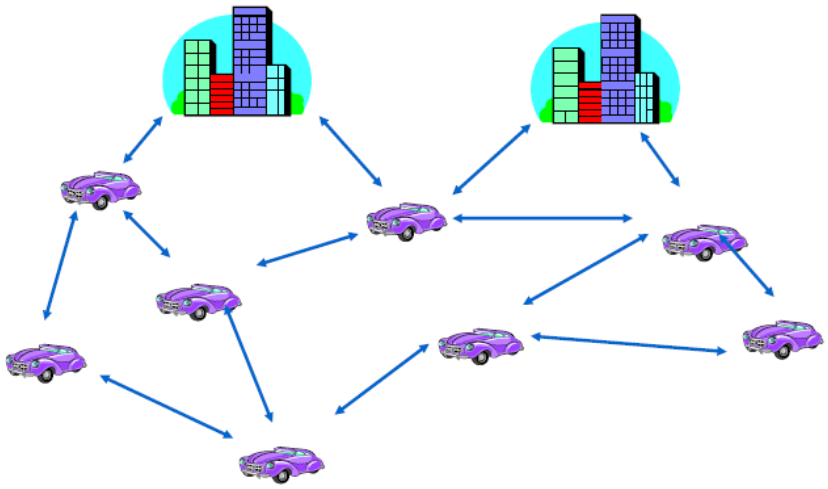
Εικόνα 11. Ένα Vanet

Υπάρχουν επίσης εφαρμογές πολυμέσων και πρόσβαση στο διαδίκτυο για τους επιβάτες, όλα εντός της ασύρματης κάλυψης του κάθε αυτοκινήτου. Η **αυτόματη πληρωμή για χώρους στάθμευσης και η είσπραξη διοδίων** αποτελούν άλλα παραδείγματα των δυνατοτήτων μέσω ενός VANET.

Ότι ισχύει για τα MANets ισχύει και για τα VANets, αλλά οι λεπτομέρειες διαφέρουν. Αντί να κινούνται τυχαία, τα οχήματα τείνουν να κινούνται με οργανωμένο τρόπο. Τα περισσότερα οχήματα περιορίζονται στο εύρος της κίνησής τους, για παράδειγμα με το να περιορίζονται να ακολουθήσουν μια πλακόστρωτη οδό.

Το **InVANET, ή ευφυές Vehicular Ad-Hoc Networking**, καθορίζει ένα ευφυή τρόπο χρήσης Vehicular Networking. Το InVANET ενοποιεί πολλαπλές ad-hoc τεχνολογίες δικτύωσης όπως WiFi IEEE 802,11 b/g, WiMAX IEEE 802,16, Bluetooth, IRDA, ZigBee για εύκολη, ακριβή, αποτελεσματική και απλή επικοινωνία μεταξύ οχημάτων. Το InVANET βοηθά στον καθορισμό των μέτρων ασφαλείας στα οχήματα και στη ροή της επικοινωνίας μεταξύ των οχημάτων.

Τα Vehicular Ad-hoc Networks αναμένεται να εφαρμόσουν διάφορες ασύρματες τεχνολογίες, όπως **Dedicated Short Range Communications (DSRC)**, η οποία είναι ένα είδος WiFi. Άλλες υποψήφιες ασύρματες τεχνολογίες είναι η κυψελοειδής, δορυφορική, και η WiMAX. Τα Vehicular Ad-hoc δίκτυα μπορεί να θεωρηθούν συνιστώσα των **ευφυών συστημάτων μεταφορών (ITS).**



Εικόνα 12. Vehicular ad hoc δίκτυο

4.2.2 Χαρακτηριστικά των VANETS

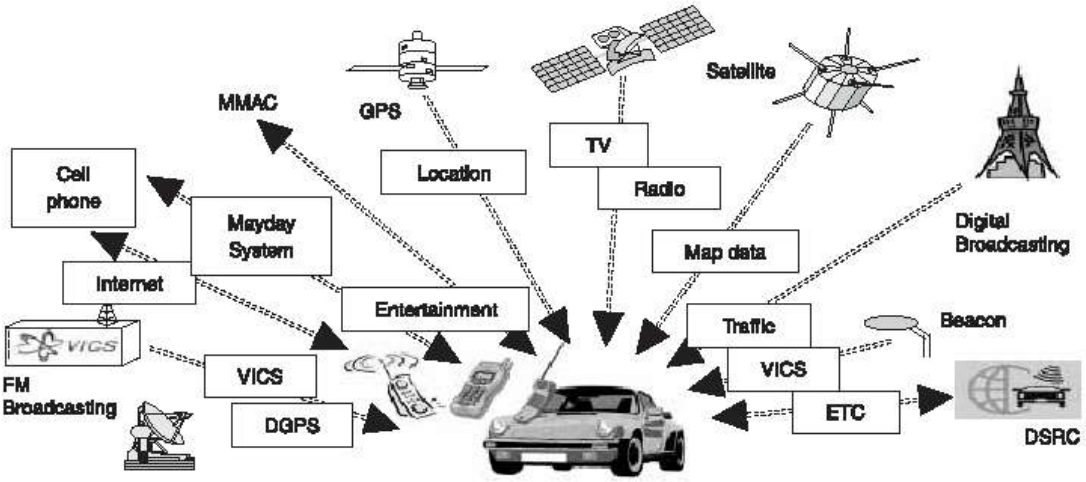
Τα VANETS αποτελούν ένα υποσύνολο των MANETS έχοντας κάποια επιπρόσθετα χαρακτηριστικά:

- Υψηλότερη κινητικότητα των κόμβων
- Επεκτασιμότητα του δικτύου
- Αυξημένος Αριθμός Κόμβων/Χρηστών στο δίκτυο
- Αυξημένη πιθανότητα συγκρούσεων και απώλειας κάποιου κόμβου
- Χρησιμοποιούν συστήματα GPS για εντοπισμό των συντεταγμένων τοποθεσίας τους.

4.2.3 Vehicular networks και ασφάλεια δεδομένων

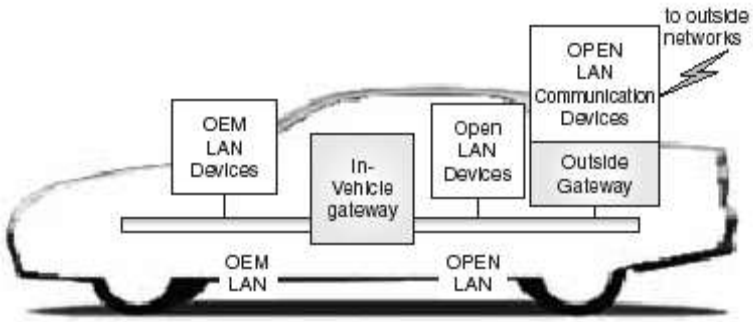
Τα τελευταία χρόνια πολλών ειδών συσκευές επικοινωνίας και μεταφοράς πληροφοριών έχουν εγκατασταθεί στα αυτοκίνητα (Εικόνα 13). Αυτές οι συσκευές μπορούν να συνδεθούν μέσω ενός δικτύου και να παρέχουν ολοκληρωμένη λειτουργικότητα στο όχημα. Επιπλέον υπάρχει η ανάγκη για πύλες που θα συνδέουν είτε συσκευές σε ένα όχημα είτε δίκτυα διαφορετικών οχημάτων.

Ένα δίκτυο μέσα σε ένα όχημα αποτελείται από ένα **OEM LAN**, ένα **OPEN LAN** και μια **πύλη** εγκατεστημένη ανάμεσα στα δίκτυα (Εικόνα 14). Ακόμα υπάρχει και μια πύλη που συνδέει το δίκτυο του αυτοκινήτου με εξωτερικά δίκτυα. Ένα OEM LAN είναι ένα κλειστό δίκτυο όπου οι προδιαγραφές και οι συσκευές σύνδεσης ορίζονται από τον κατασκευαστή του οχήματος. Οι συσκευές που συνδέονται σε ένα τέτοιο δίκτυο είναι πολύ ασφαλείς και έχουν μεγάλη συνεισφορά στην οδική ασφάλεια. Σε αντίθεση, ένα OPEN LAN είναι ένα δίκτυο όπου οι προδιαγραφές του



Εικόνα 13

δεν καθορίζονται από κάποιον συγκεκριμένα και οι συσκευές του μπορούν να επικοινωνήσουν και με συσκευές εκτός δικτύου. Οι συσκευές που είναι συνδεδεμένες σε ένα OPEN δίκτυο δεν έχουν συνεισφορά στην ασφάλεια του οχήματος. Επειδή είναι πιθανόν κάποιοι άλλοι να αποκτήσουν πρόσβαση σε δεδομένα που επηρεάζουν την ασφάλεια του οχήματος και κατ' επέκταση του οδηγού, οι πύλες του OEM δικτύου δεν επιτρέπουν στα εξωτερικά δίκτυα να έχουν πρόσβαση σε "ευαίσθητα" δεδομένα.



Εικόνα 14

Οι πύλες σ' ένα OEM δίκτυο φιλτράρουν τα πακέτα, την επικεφαλίδα και το περιεχόμενό τους και αποφασίζουν αν θα επιτρέψουν την πρόσβαση στο δίκτυο ή όχι. Οι πύλες θα πρέπει να μην επιτρέπουν την είσοδο σε δεδομένα που θα επηρεάσουν την ασφάλεια του οχήματος, να μην επιτρέπουν την είσοδο σε μεγάλες ποσότητες δεδομένων γιατί θα επηρεαστεί η κυκλοφορία των πακέτων στο κλειστό δίκτυο, να ελέγχουν την ταυτότητα του αποστολέα των μηνυμάτων ή του χρήστη που θα ζητάει πρόσβαση σε "ευαίσθητα" δεδομένα. Ο έλεγχος όμως των δεδομένων από κάθε συσκευή που είναι στο δίκτυο δεν είναι εφικτή καθώς η υπολογιστική ισχύς και η διαθέσιμη μνήμη αυτών των συσκευών είναι περιορισμένη. Είναι λοιπόν προτιμότερο να εγκαταστήσουμε λειτουργίες φιλτραρίσματος των μηνυμάτων μόνο στις πύλες των δικτύων.

4.2.4 Εφαρμογές και απαιτήσεις

Τυπικά, οι εφαρμογές των VANET κατηγοριοποιούνται ως εξής:

- **ασφάλεια: αποφυγή σύγκρουσης.**
- **αξιολόγηση διαδρομής: συγχρονισμός φωτεινών σηματοδοτών σύμφωνα με την ταχύτητα.**
- **εφαρμογές που αφορούν πληροφορίες-ψυχαγωγία: πρόσβαση στο Internet.**

Για να εκτιμήσουμε τις πιθανότητες επιτυχίας, οι εφαρμογές αναλύθηκαν σύμφωνα με το αν μπορούν να ικανοποιηθούν οι απαιτήσεις τους και με το αν παρέχουν θετικά αποτελέσματα. Από την πλευρά των απαιτήσεων, ένας προφανής παράγοντας είναι το ποσοστό των οχημάτων το οποίο φέρει την τεχνολογία VANET, σε σχέση με το συνολικό πληθυσμό οχημάτων, για τη διασφάλιση της σωστής λειτουργίας του συστήματος. Οι τεχνικές απαιτήσεις καθορίζουν το μέγεθος των πακέτων, την απαιτούμενη συχνότητα ή ακρίβεια των πληροφοριών, την ακτίνα επικοινωνίας, τα επίπεδα ασφαλείας και την απαραίτητη υποδομή.

Για εφαρμογές σχετικές με την ασφάλεια, ο συνεταιρισμός **Vehicle Safety Communications (VSC)** αναγνωρίζει οχτώ πιθανές εφαρμογές:

- προειδοποίηση παραβίασης οδικής σήμανσης
- καμπύλη ταχύτητας
- φωτεινή ένδειξη σε απότομο φρενάρισμα
- αισθητήρες για την αποφυγή πρόσκρουσης
- επικοινωνία μεταξύ των οχημάτων για προειδοποίηση μποτιλιαρίσματος
- σύστημα υποβοήθησης οδηγού για τη διάσχιση διασταυρώσεων
- σύστημα προειδοποίησης για αλλαγή λωρίδας
- σύστημα προειδοποίησης για σήματα STOP

Τέσσερις από αυτές τις εφαρμογές απαιτούν από όχημα σε όχημα επικοινωνία, ενώ οι άλλες τέσσερις, απαιτούν σύνδεση με σταθερό εξοπλισμό.

Μια μεγάλη έρευνα επιτελείται παγκοσμίως στον τομέα των VANETs. Πολλά project βρίσκονται υπό ανάπτυξη. Ένα από αυτά είναι το Ευρωπαϊκό project **FleetNet**. Στο FleetNet, τα οχήματα ανταλλάσσουν σύντομα μηνύματα με τοπικές πληροφορίες. Τα μηνύματα αυτά ενημερώνουν τους οδηγούς σχετικά με τα εμπόδια ή την κυκλοφοριακή συμφόρηση που μπορεί να συναντήσουν, πέρα από το οπτικό πεδίο του οδηγού ή τους αισθητήρες του οχήματος.

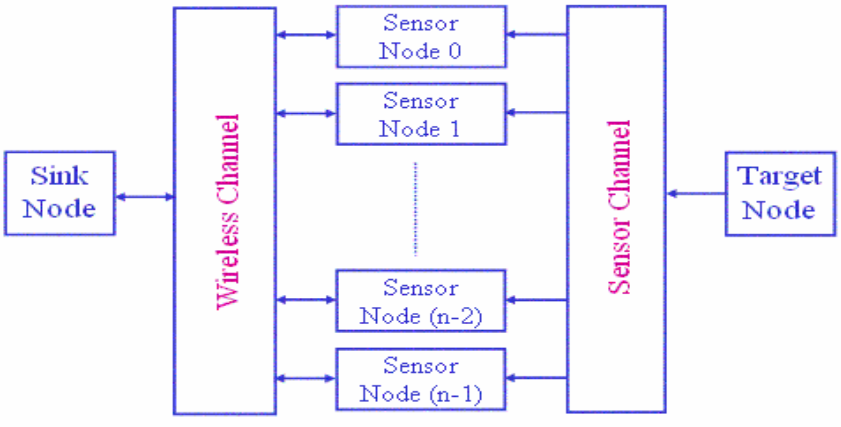
Επιπρόσθετα project, όπως το Ευρωπαϊκό **CarTALK 2000**, αξιοποίησαν την ανάπτυξη συστημάτων υποβοήθησης του οδηγού και την ανάπτυξη ad-hoc δικτύων ως βάση επικοινωνίας, με στόχο την προετοιμασία ενός μελλοντικού προτύπου. Το CarTALK χρησιμοποιεί τόσο τις άμεσες επικοινωνίες όσο και τις επικοινωνίες πολλαπλών κόμβων, για τη μεταφορά των δεδομένων.

4.3 Ασύρματα Δίκτυα Αισθητήρων

4.3.1 Εισαγωγή στα ασύρματα δίκτυα αισθητήρων

Μια νέα πραγματικότητα διαμορφώνεται σήμερα μέσα από την ανάπτυξη των **Ασύρματων Δικτύων Αισθητήρων (wireless sensor networks)** είτε αυτά λειτουργούν αυτοτελώς, είτε διασυνδεδεμένα στα μεγαλύτερα δίκτυα τηλεπικοινωνιών ή στο διαδίκτυο. Τα δίκτυα αυτά αποτελούνται από μεγάλο αριθμό μικρών ηλεκτρονικών διατάξεων (αισθητήρων), κινητών ή μη, που αποστέλλουν σε μια κεντρική μονάδα πληθώρα δεδομένων προς επεξεργασία και λήψη αποφάσεων.

Η ταχύτατη ανάπτυξη της μικροηλεκτρονικής και των υλικών επέτρεψε την κατασκευή πολύ μικρών αισθητήρων, οι οποίοι έχουν την ικανότητα να μετρούν και να καταγράφουν μια κυριολεκτικά ατελείωτη σειρά από περιβαλλοντολογικά ή βιολογικά μεγέθη, όπως τη θερμοκρασία, την ατμοσφαιρική πίεση, την υγρασία, τη φωτεινότητα, τη στάθμη υδάτων, την ωρίμανση καρπών, την ανίχνευση χημικών στοιχείων, την πίεση αίματος, τους σφυγμούς καρδιάς, την κίνηση αντικειμένων και ανθρώπων και πολλές ακόμα παραμέτρους που προστίθενται διαρκώς στον παραπάνω κατάλογο. Αξιοσημείωτο είναι ότι σε μία διάταξη ίση με ένα νόμισμα των 2 ευρώ μπορούμε να συμπεριλάβουμε πολλά από τα παραπάνω αισθητήρια και να καταμετρούμε συγχρόνως διάφορα μεγέθη.



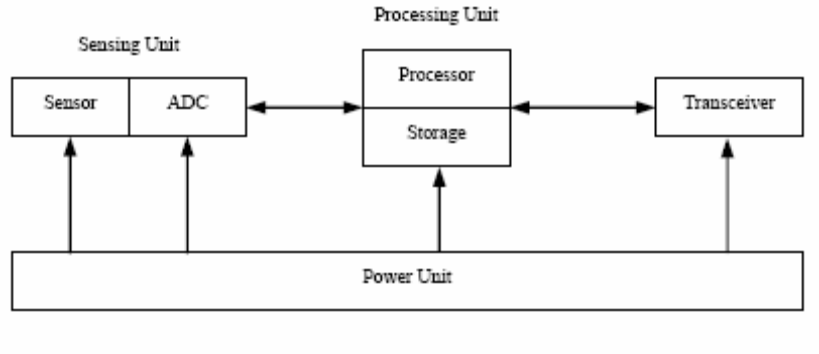
Εικόνα 15. Αρχιτεκτονική ενός δικτύου αισθητήρων

4.3.2 Αρχιτεκτονική του Κόμβου Αισθητήρα

Τα κύρια συστατικά από τα οποία αποτελούνται οι αισθητήρες είναι το κομμάτι που αισθάνεται (sensing unit), το κομμάτι που επεξεργάζεται (processing unit), ο πομποδέκτης (transceiver) και το κομμάτι της ενέργειας (power unit). Αναλυτικότερα:

- **Sensing unit**. Η κύρια λειτουργικότητα του sensing unit είναι να αισθάνεται ή να μετρά τα φυσικά δεδομένα που προκύπτουν από την περιοχή που βρίσκεται. Η αναλογική τάση (analog voltage) που δημιουργείται στον αισθητήρα και ανταποκρίνεται σε κάποιο "γεγονός", ψηφιοποιείται από τον αναλογικό-σε-ψηφιακό μετατροπέα (analog-to-digital converter, ADC) και μεταφέρεται στο processing unit για περισσότερη ανάλυση.

- **Processing unit**. Το processing unit παίζει κύριο ρόλο στη διαχείριση της συνεργασίας με τους υπόλοιπους αισθητήρες για να πετύχει τις προκαθορισμένες εργασίες. Υπάρχουν αρκετές οικογένειες αυτού του κομματιού που συμπεριλαμβάνουν **microcontrollers, microprocessors και field-programmable gate arrays (FPGAs)**. Η μνήμη ROM και οι διασυνδέσεις με το ADCs μπορούν να ενοποιηθούν σε ένα ενοποιημένο κύκλωμα. Το processing unit χρειάζεται τακτική αποθήκευση για να μειώνει το μέγεθος των μηνυμάτων που θα μεταδοθούν με τοπική επεξεργασία και συνάθροιση δεδομένων. Η μνήμη flash χρησιμοποιείται ευρέως λόγω του κόστους της και της χωρητικότητας αποθήκευσής της.
- **Transceiver**. Υπάρχουν τρία αναπτυγμένα σχέδια επικοινωνίας στους αισθητήρες που περιλαμβάνουν οπτική παρακολούθηση (optical communication, laser), υπέρυθρη (infrared) και ραδιοσυχνότητα (radiofrequency,RF). Η ραδιοσυχνότητα είναι η πιο εύκολη στη χρήση αλλά χρειάζεται κεραία.
- **Power unit**. Η κατανάλωση ενέργειας είναι η κύρια αδυναμία των Ασύρματων Δικτύων Αισθητήρων. Οι μπαταρίες που χρησιμοποιούνται στους αισθητήρες μπορούν να κατηγοριοποιηθούν σε δύο ομάδες: στις **επαναφορτιζόμενες** και στις **μη-επαναφορτιζόμενες**. Συχνά, στα δύσκολα περιβάλλοντα είναι αδύνατο να επαναφορτιστεί ή ν' αλλάξει μια μπαταρία.



Εικόνα 16. Αρχιτεκτονική ενός κόμβου αισθητήρα

4.3.3 Διαφορές Δικτύων Αισθητήρων - Ad hoc δικτύων

Ενώ τα Ασύρματα Δίκτυα Αισθητήρων έχουν αρκετές ομοιότητες με τα ήδη υπάρχοντα ad hoc δίκτυα, διαφέρουν σε αρκετές και συγκεκριμένες ιδιότητες. Κάποια σημαντικά σημεία που κάνουν τα Ασύρματα Δίκτυα Αισθητήρων να διαφέρουν είναι τα εξής:

- **Πλήθος των κόμβων.** Ο αριθμός των κόμβων σ' ένα δίκτυο αισθητήρων είναι συνήθως αρκετά μεγαλύτερος απ' ό,τι είναι στα ad hoc δίκτυα.
- **Τοπολογία.** Η τοπολογία στα δίκτυα αισθητήρων είναι συνήθως στατική ενώ στα ad hoc αλλάζει συχνά.
- **Ενέργεια.** Όπως και σε μερικές περιπτώσεις των δικτύων ad hoc, ο ανεφοδιασμός ενέργειας είναι σπάνιος και γι' αυτό η κατανάλωση ενέργειας είναι κύρια παράμετρος που πρέπει να λαμβάνεται υπόψη. Συχνά, η μπαταρία στους αισθητήρες των Ασύρματων Δικτύων Αισθητήρων είναι μη επαναφορτιζόμενη και η ανάγκη για να παρατείνουμε τη ζωή ενός κόμβου

αισθητήρα έχει μεγάλη επίδραση στο σύστημα και στην αρχιτεκτονική του δικτύου.

- **Απουσία ενός μοναδικού χαρακτηριστικού.** Σε αντίθεση με τους κόμβους ενός ad hoc δικτύου, οι κόμβοι ενός δικτύου αισθητήρων, είναι δυνατό να μην έχουν κάποιο διακριτικό(π.χ. μια τύπου MAC ή IP διεύθυνση) που να τους χαρακτηρίζει μοναδικά.
- **Μεθοδολογία εκπομπής.** Η μεθοδολογία εκπομπής στα δίκτυα αισθητήρων είναι συνήθως ένας προς πολλούς (broadcast), ενώ στα ad hoc δίκτυα είναι από σημείο προς σημείο (point to point).
- **Δυνατότητες κόμβου.** Οι κόμβοι στα δίκτυα αισθητήρων διακρίνονται για τους σημαντικούς περιορισμούς που έχουν στους τομείς της ενέργειας, της υπολογιστικής ισχύος και της μνήμης.

4.3.4 Προβλήματα και Περιορισμοί των Ασύρματων Δικτύων Αισθητήρων

Τα Ασύρματα Δίκτυα Αισθητήρων παρουσιάζουν ένα εντελώς διαφορετικό σύνολο από περιορισμούς σε σύγκριση με τους περιορισμούς που παρουσιάζονται στα παραδοσιακά δίκτυα. Το πιο σημαντικό από αυτά είναι η ενέργεια. Αυτά τα δίκτυα αποτελούνται από συλλογές συσκευών οι οποίες πρέπει να είναι ενεργές αρκετή ώρα με μικρές μπαταρίες.

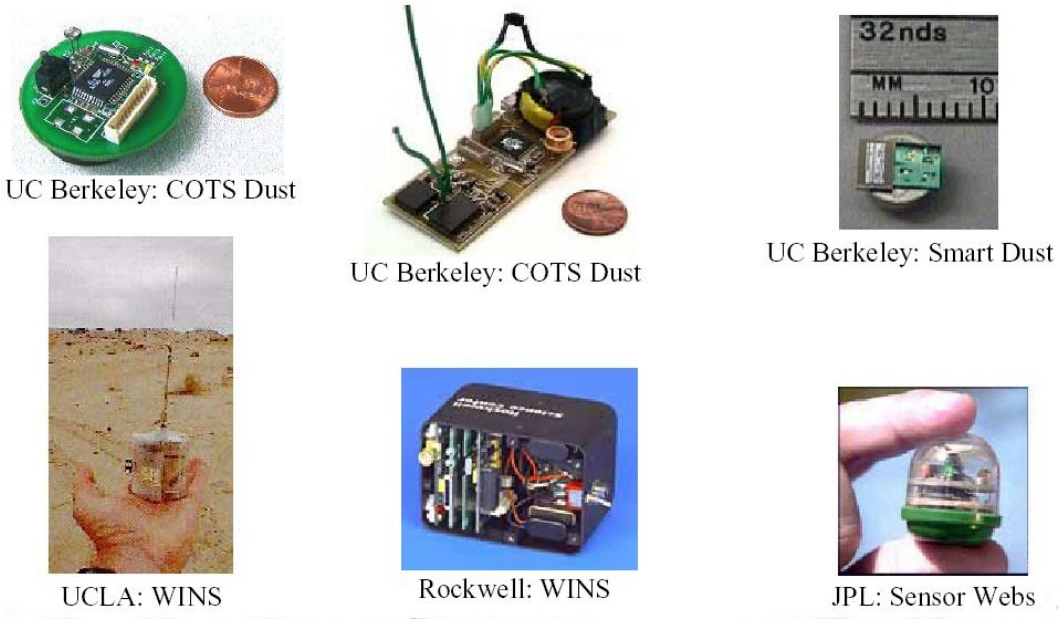
Έρευνες που έχουν γίνει τελευταία, έδειξαν ότι εάν ένας κόμβος λειτουργεί πλήρως, **η διάρκεια ζωής του είναι τέσσερις μέρες**. Αυτές οι τέσσερις μέρες πρέπει να διασκορπιστούν σε αρκετά χρόνια ζωής. Για τα υπόλοιπα συστήματα αυτό δεν είναι κάτι που πρέπει να ληφθεί υπόψη, αλλά για τα Ασύρματα Δίκτυα Αισθητήρων είναι κάτι πολύ σημαντικό. Το δεύτερο πολύ σημαντικό είναι η **τοποθέτησή** τους. Αντίθετα με τους υπόλοιπους υπολογιστές, οι αισθητήρες συχνά πρέπει να τοποθετηθούν σε δύσκολες περιοχές, όπου οι τεχνικοί που θα τους εγκαταστήσουν, δεν έχουν εύκολη πρόσβαση.

Ακόμα, κάτι που γίνεται δύσκολα στους κόμβους αισθητήρων είναι ο καθορισμός του λόγου για τον οποίο χάθηκε ένα πακέτο. Οι πιθανοί λόγοι είναι υπερχείλιση της ουράς, έλλειψη ενέργειας ή έλλειψη ασφάλειας. Ακόμα κάποιος πιθανός λόγος για το χάσιμο πακέτων είναι η συμφόρηση στο δίκτυο, επομένως κάποια πακέτα να μην μπορούν να μεταφερθούν και ειδικότερα, αυτά που βρίσκονται πιο μακριά από το sink.

Τα Ασύρματα Δίκτυα Αισθητήρων πρέπει ν' αντιμετωπίσουν και το πρόβλημα της **κάλυψης**. Δηλαδή, πόσο καλά το δίκτυο, δηλαδή μια περιοχή παρακολουθείται από τους κόμβους αισθητήρες.

Επίσης, αντιμετωπίζουν κάποια προβλήματα λόγω των περιορισμών που υπάρχουν στους αισθητήρες, όπως για παράδειγμα, οι **περιορισμένοι πόροι**, οι **χαμηλές υπολογιστικές δυνατότητες**, η **μικρή μνήμη** και η περιορισμένη και πολλές φορές, μη επαναφορτιζόμενη μπαταρία, λόγω του μεγέθους τους και των περιορισμών που αναφέραμε πιο πάνω. Και το χαμηλό bandwidth λόγω της ασύρματης επικοινωνίας τους.

Λόγω αυτών και άλλων περιορισμών και προβλημάτων που έχουν να αντιμετωπίσουν τα Ασύρματα Δίκτυα Αισθητήρων υπάρχει ανάγκη για καινοτόμα συστήματα, πρωτόκολλα και αλγορίθμους. Εξαιτίας του γεγονότος ότι στα δίκτυα αυτά δεν υπάρχει η σαφής έννοια της διαστρωμάτωσης, τα πιο πάνω προβλήματα επιλύονται σε ένα ή περισσότερα από τα κλασσικά επίπεδα (φυσικό, εφαρμογής, δικτύου κ.τ.λ.). Για παράδειγμα, ο έλεγχος συμφόρησης εμπεριέχεται στο επίπεδο μεταφοράς.



Εικόνα 17. Διάφοροι τύποι αισθητήρων

4.3.5 Εφαρμογές

Είναι ατελείωτη η λίστα των εφαρμογών των δικτύων αισθητήρων, ενώ πολλές από αυτές μας είναι ήδη οικείες καθώς ανταποκρίνονται στις συνήθεις δραστηριότητες και ανάγκες μας: μετρήσεις ακριβείας πολλών ατμοσφαιρικών και μετεωρολογικών παραμέτρων, επιτήρηση δασών, υδροβιότοπων, θερμοκηπίων και γενικά αγροτικών καλλιεργειών για έλεγχο υγρασίας, θερμοκρασίας, πίεσης, ωρίμανσης καρπών, κτλ., επιτήρηση υγρών στοιχείων για ρύπους ή έλεγχο ακραίων καιρικών φαινομένων όπως οι πλημμύρες, επιτήρηση βιομηχανικού περιβάλλοντος για την εξασφάλιση επιθυμητών συνθηκών της παραγωγικής διαδικασίας, στοιχειώδεις ρυθμίσεις λειτουργιών σε κτίρια όπως θέρμανση, φωτισμός, συναγερμοί. Ως λιγότερο οικείες αλλά αρχαιότερες χρονικά μπορούν ν' αναφερθούν οι στρατιωτικές εφαρμογές και οι υποβρύχιες εγκαταστάσεις δικτύων για εντοπισμό αντικειμένων τόσο για στρατιωτικές επιχειρήσεις όσο και για αρχαιολογικές έρευνες και πειράματα. Όλες αυτές οι δράσεις αποτελούν κλασικά πλέον -και διόλου ασήμαντα- προϊόντα της επιστημονικής αυτής περιοχής που απαντώνται διεθνώς όχι μόνο σε ανεπτυγμένες αλλά και σε αναπτυσσόμενες χώρες.

Εικόνα 18. Ζεύγος αισθητήρων μέτρησης ροής χυμών TDP80, DYNAMAX Inc., U.S.A.

Στις πιο πρόσφατες, και επομένως λιγότερο οικείες εφαρμογές μπορούμε ν' αναφέρουμε τη χρήση δικτύων αισθητήρων για τον ακριβή προσδιορισμό της θέσης και της κίνησης αντικειμένων σε εσωτερικούς χώρους, όπως σε κτίρια σε πυκνοδομημένο αστικό περιβάλλον, όπου η απόδοση της κλασικής GPS υπηρεσίας αποδεικνύεται ανεπαρκής. Οι δυνατότητες αυτές θα συμβάλλουν αποφασιστικά στην ασφάλεια και επιτήρηση δημοσίων και ιδιωτικών χώρων.

Στην προσπάθεια για αποτελεσματικότερη διαχείριση του καθημερινού μας περιβάλλοντος, πολλές πειραματικές προσπάθειες διεθνώς επικεντρώνονται στην ανάπτυξη και αξιολόγηση δικτύων που δύνανται να εκτελούν φωνητικές εντολές ή ν' ανιχνεύουν την κίνηση ή τη διάθεση των χρηστών τους και να ρυθμίζουν πλήρως εγκαταστάσεις φωτισμού, ηλεκτρικών και ηλεκτροακουστικών συσκευών, ηλεκτρονικής επικοινωνίας, κτλ.

Οι εφαρμογές που αναφέρθηκαν, αλλάζουν επαναστατικά την οργάνωση της κοινωνικής μας ζωής προσφέροντας αναβαθμισμένο περιβάλλον σε χώρους όπου η περίθαλψη ή η διαβίωση ευπαθών ομάδων (υπερήλικες, βρέφη) απαιτεί αδιάκοπη προσοχή και άμεση επέμβαση. Ετσι, ο σχεδιασμός **των "ψηφιακών πόλεων"**, που αποτελεί το μεγάλο στοίχημα της σύγχρονης πολεοδομίας, θα στηριχθεί καθοριστικά στις δυνατότητες των ασύρματων δικτύων αισθητήρων.

Ανάλογες εφαρμογές βρίσκονται σε εξέλιξη και θα μπορούσαν να χρησιμοποιηθούν στη σχεδίαση και λειτουργία οχημάτων όπου τα ασύρματα δίκτυα αισθητήρων θα μπορούν να λειτουργήσουν συνεργατικά με τον οδηγό για την πλοήγηση του οχήματος, την αποφυγή εμποδίων, την εκκίνηση ή διακοπή της λειτουργίας της μηχανής σε περίπτωση κρίσιμης κατάστασης των επιβαινόντων. Η χρήση των τεχνολογιών αυτών μόνο θετικό αντίκτυπο μπορεί να έχει στην αποφυγή τραγικών γεγονότων και περιστατικών στις οδικές αρτηρίες.

4.3.6 Ασύρματα δίκτυα αισθητήρων. Παρόν και μέλλον

Στις αρχές του 21ου αιώνα, το διαδίκτυο και οι τεχνολογίες ασύρματων επικοινωνιών διευκολύνουν την άμεση πρόσβαση σε πληροφορίες ξεπερνώντας φραγμούς απόστασης και χρόνου. Σε αυτήν τη νέα εποχή, συστήματα αισθητήρων, από τα γνωστά μας μικρόφωνα ως τις "έξυπνες" κεραίες και από τα μικρο-

επιταχυνσιόμετρα και τους βιο-αισθητήρες ως τις κάμερες απεικόνισης, αρχίζουν να έχουν σημαντική απήχηση τόσο στη βιομηχανία, όσο και στην καθημερινή μας ζωή. Στο μέλλον, η ενσωμάτωση των έξυπνων αισθητήρων στις τηλεπικοινωνίες και την πληροφορική θα διαδραματίσει καθοριστικό ρόλο σε πληθώρα σημαντικών εφαρμογών όπως η παρακολούθηση του περιβάλλοντος, η δημόσια ασφάλεια και διάσωση, ο έλεγχος των υποδομών και των κατασκευών, η ιατρική και η βιολογία.

Τα ασύρματα δίκτυα αισθητήρων είναι μια ανερχόμενη τεχνολογία με στόχο την παρακολούθηση και τον έλεγχο του φυσικού κόσμου χρησιμοποιώντας μια διάταξη πυκνής κατανομής αισθητήριων κόμβων με δυνατότητες τοπικής επεξεργασίας της πληροφορίας και ασύρματης επικοινωνίας. Είναι μια τεχνολογία που θα μπορούσε να αποδειχθεί τόσο σημαντική όσο το διαδίκτυο, γιατί ακριβώς όπως το διαδίκτυο επιτρέπει στους υπολογιστές να ανακαλύψουν την ψηφιακή πληροφορία οπουδήποτε και αν είναι αποθηκευμένη, έτσι και τα δίκτυα αισθητήρων θα επεκτείνουν τη δυνατότητα των ανθρώπων να αλληλεπιδρούν με το φυσικό κόσμο.

Όπως το Internet, αλλά και πολλές άλλες τεχνολογικές εφαρμογές που αναπτύχθηκαν αρχικά για λογαριασμό στρατιωτικών προγραμμάτων και κατέληξαν αρκετά χρόνια αργότερα να έχουν μία ευρύτερη πολιτική χρήση, έτσι και τα ασύρματα δίκτυα αισθητήρων ήταν μια στρατιωτική ιδέα του 2000 για το μελλοντικό πεδίο μάχης. Χρηματοδοτήθηκαν από τον ερευνητικό τομέα του Υπουργείου Άμυνας των ΗΠΑ μέσω προγραμμάτων όπως το **SmartDust** και το **SensIT**, σε συνεργασία με κορυφαία αμερικανικά πανεπιστήμια όπως τα Πανεπιστήμια της Καλιφόρνια στο Berkeley και στο Los Angeles.

Στόχος των ερευνητών είναι η υλοποίηση μικροσυσκευών, το μέγεθος των οποίων δεν θα ξεπερνάει κατά πολύ μία μπαταρία ρολογιού και οι οποίες θα περιέχουν ένα μικροεπεξεργαστή, ελάχιστη ποσότητα μνήμης και αισθητήρες για την παρακολούθηση μεγεθών όπως η τάση, η επιτάχυνση, η θερμοκρασία, η υγρασία, η πίεση, κά. Οι συσκευές θα ενσωματώνουν ένα ραδιοδέκτη αλλά και εδικό λογισμικό για να λαμβάνουν και να αποστέλλουν μικρές ποσότητες δεδομένων δημιουργώντας αυτόνομα αδόμητα δίκτυα. Μια θεμελιώδης ιδιότητα των δικτύων αισθητήρων είναι η δυναμική τους. Με το χρόνο, οι κόμβοι βγαίνουν εκτός λειτουργίας καθώς τελειώνει η ενέργειά τους, υπερθερμαίνονται στον ήλιο, μεταφέρονται από τον αέρα και τα ρεύματα ή αχρηστεύονται λόγω λαθών στο λογισμικό τους. Ακόμη κι αν η γεωγραφική θέση των κόμβων παραμείνει σταθερή, το ασύρματο κανάλι και συνεπώς η τηλεπικοινωνιακή τοπολογία του δικτύου μπορεί ν' αλλάξει εντυπωσιακά λόγω της περιβαλλοντικής επίδρασης στη διάδοση των ραδιοκυμάτων. Αυτές οι αλλαγές είναι δύσκολα προβλέψιμες εκ των προτέρων. Αυτό οδηγεί σε μία σημαντική απαίτηση: τα δίκτυα αισθητήρων πρέπει να προσαρμόζονται από μόνα τους στις αλλαγές του περιβάλλοντος.

4.3.7 Επιπτώσεις

Όπως όλες οι καινοτόμες τεχνολογίες, έτσι και τα ασύρματα δίκτυα αισθητήρων μαζί με τις νέες ευκαιρίες που φέρνουν, μπορούν να δημιουργήσουν και σημαντικά προβλήματα στην κοινωνία. Ο έλεγχος μέσω ενός εκτεταμένου δικτύου αισθητήριων καμερών μπορεί πχ. να παράσχει μεγαλύτερη ασφάλεια, αλλά με κόστος την παρέμβαση στην προσωπική μας ζωή. Υπάρχει η δυνατότητα χρήσης τέτοιων δικτύων ως μέσο ελέγχου για αντικοινωνικές πράξεις, αλλά και ως μέσο παρακολούθησης για το πού βρισκόμαστε και τι κάνουμε ανά πάσα στιγμή.

Μπορούμε να πούμε με σιγουριά ότι τα δίκτυα αισθητήρων θα έχουν σημαντικές επιπτώσεις στον τρόπο με τον οποίο βλέπουμε και χρησιμοποιούμε τους δημόσιους χώρους. Αυτά τα ζητήματα θα πρέπει να αντιμετωπιστούν με διάλογο και δημόσιο προβληματισμό, αλλά και μέσα από την εκπαίδευση των φοιτητών τόσο σε σχετικά τεχνικά αντικείμενα, όσο και σε θέματα που άπτονται των κοινωνικών επιστημών, της δημόσιας πολιτικής, ακόμα και της φιλοσοφίας της επιστήμης.

4.4 Ασύρματα Δίκτυα Mesh

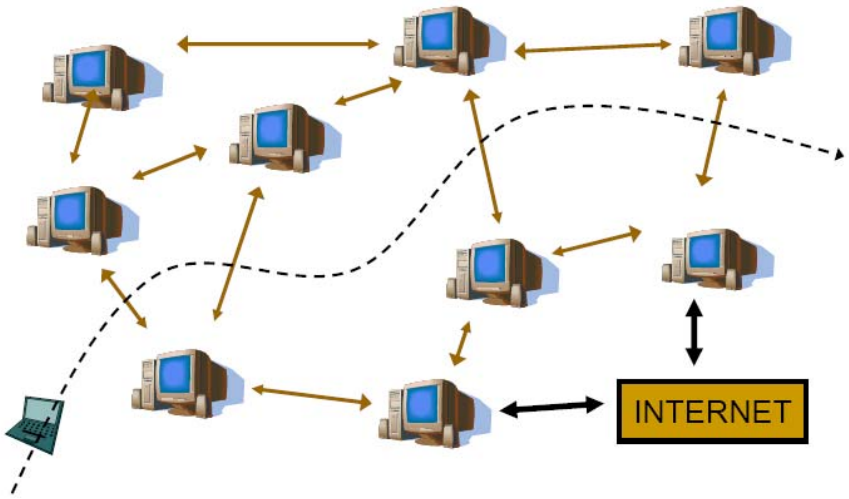
4.4.1 Εισαγωγή στα ασύρματα δίκτυα πλέγματος (Mesh Networks)

Η εξέλιξη και η σημερινή μορφή των ασύρματων δικτύων μονοπωλείται σε μεγάλο βαθμό από τα μεγάλα εμπορικά δίκτυα κινητής τηλεφωνίας (2ης και 3ης γενεάς). Πέρα από την αρχιτεκτονική τους, τα δίκτυα αυτά ελέγχονται από εταιρείες-οικονομικούς κολοσσούς που έχουν πραγματοποιήσει τεράστιες επενδύσεις σε υποδομές και αγορά φάσματος. Είναι προφανές ότι στο πεδίο των δραστηριοτήτων τους δεν υπάρχει χώρος για μικρές ή μικρομεσαίες εταιρείες. Ομως, αυτή η κυρίαρχη θέση που κατέχουν στον τομέα των κινητών επικοινωνιών δεν τους συνοδεύει στον τομέα των ασύρματων ευρυζωνικών δικτύων, γνωστών και ως WiFi ή δικτύων τεχνολογίας 802.11. Εχοντας πολλά διαφορετικά χαρακτηριστικά από τα δίκτυα κινητής τηλεφωνίας, τα ασύρματα ευρυζωνικά δίκτυα έχουν πολλά οικονομικά πλεονεκτήματα όπως πχ. οικονομικό δικτυακό εξοπλισμό ασύρματης πρόσβασης, λειτουργία σε ελεύθερο από τέλη φάσμα και φυσικά σχεδιαστική ευελιξία και εύκολη επεκτασιμότητα.

Είναι προφανές ότι ένα τεχνολογικά εξελιγμένο δίκτυο κορμού, για ασύρματη ευρυζωνική πρόσβαση που θα συνέδεε ασύρματα σημεία πρόσβασης τελικών χρηστών, θα μπορούσε να δώσει νέα ώθηση όχι μόνο στην τεχνολογία των τηλεπικοινωνιών, αλλά και στην οικονομική τους δραστηριότητα, καθώς θα επέτρεπε σε μικρές και μικρομεσαίες επιχειρήσεις, ακόμη και σε ιδιώτες να συνενωθούν δημιουργώντας ένα ιδιότυπο ευρύτερο ασύρματο δίκτυο από πολλαπλούς παρόχους και χρήστες που μπορούν να κάνουν περιαγωγή μεταξύ ενός μεγάλου αριθμού παρόχων (μικρών ή μεγάλων). Βεβαίως, στο εναλλακτικό αυτό μοντέλο θα είχαν θέση και μάλιστα σημαντική και οι υπάρχοντες πάροχοι ενσύρματων ευρυζωνικών υπηρεσιών και διαδικτύου (ISPs), οι οποίοι θα είχαν τη δυνατότητα να διευρύνουν τις υπηρεσίες και το πελατολόγιό τους παρέχοντας, πέρα από τις συνήθεις, και υπηρεσίες καθολικής ευρυζωνικής πρόσβασης σε κινητούς χρήστες. Η πλέον υποσχόμενη τεχνολογία προς την κατεύθυνση αυτή είναι τα **ασύρματα δίκτυα πλέγματος (wireless mesh networks)**.

Τα ασύρματα δίκτυα πλέγματος αποτελούνται από **ομότιμους κόμβους πλέγματος (Mesh Nodes)** που συνδέονται μεταξύ τους μέσω ασύρματων ζεύξεων τεχνολογίας WiFi. Οι κόμβοι πλέγματος διαθέτουν πολλαπλές ασύρματες διεπαφές που επιτρέπουν τη διασύνδεση ενός κόμβου με πολλούς άλλους. Κάποιοι από τους κόμβους διαθέτουν ασύρματες διεπαφές για διασύνδεση τερματικών συσκευών (όπως φορητούς υπολογιστές ή υπολογιστές χειρός - PDAs), ενώ κάποιοι άλλοι διαθέτουν συνδέσεις με το διαδίκτυο. Θα μπορούσε κάποιος απλοϊκά να φανταστεί ένα ασύρματο δίκτυο πλέγματος σαν το διαδίκτυο, ένα πολύπλοκο δίκτυο πολλαπλών μονοπατιών και πολλαπλών συνδέσεων, μόνο που στην περίπτωσή μας οι συνδέσεις μεταξύ των κόμβων είναι ασύρματες.

Τα ασύρματα δίκτυα πλέγματος μπορούν να υλοποιηθούν τόσο σε συγκεντρωτική όσο και σε αποκεντρωτική μορφή. Οι πιο γνωστές προσεγγίσεις είναι αυτές των **ασύρματων δικτύων πλέγματος υποδομής (Infrastructure wireless mesh networks)**, **πελατών (Client wireless mesh networks)** αλλά και τα **υβριδικά (Hybrid wireless mesh networks).** Η ερευνητική δραστηριότητα των δικτύων πλέγματος βρίσκεται σε εξέλιξη και έχουν ήδη προταθεί πολλά διαφορετικά πρωτόκολλα για την λειτουργία τους.



Εικόνα 19. Ασύρματο δίκτυο Mesh

4.4.2 Εφαρμογές

Με βάση τα παραπάνω, γίνεται εύκολα κατανοητό ότι οι εφαρμογές των ασύρματων δικτύων πλέγματος καλύπτουν ένα ευρύ φάσμα δραστηριοτήτων. Ενδεικτικά:

Ευρυζωνική πρόσβαση στο διαδίκτυο: Τα ασύρματα δίκτυα πλέγματος μπορούν να παρέχουν ευρυζωνική πρόσβαση στο διαδίκτυο, αξιοποιώντας αθροιστικά τις διασυνδέσεις ενός αριθμού κόμβων του με το ενσύρματο δίκτυο. Μάλιστα, τα ασύρματα δίκτυα πλέγματος μπορεί να υποστηρίξουν ταχύτητες που ξεπερνούν εκείνες της τεχνολογίας ADSL, όπου η ταχύτητα περιορίζεται από το εύρος ζώνης του ενσύρματου καναλιού και την απόσταση του συνδρομητή από το τηλεφωνικό κέντρο, ενώ έχουν σημαντικά μικρότερο κόστος σε σχέση με την τεχνολογία οπτικών ινών.
Υποστήριξη δημόσιας ασφάλειας: Η κατανεμημένη αρχιτεκτονική και λειτουργία τους βοηθάει τα ασύρματα δίκτυα πλέγματος να είναι ανθεκτικά τόσο σε εξωγενή προβλήματα όσο και σε κακόβουλες επιθέσεις. Έτσι, σε περιπτώσεις φυσικής καταστροφής ή έκτακτων αναγκών, όπου συχνά παρατηρούνται προβλήματα επικοινωνίας με τα κλασικά δίκτυα κινητής τηλεφωνίας, τα ασύρματα δίκτυα κορμού αποτελούν ιδανική εναλλακτική λύση καθώς αφενός δεν πρόκειται να τεθούν εξ' ολοκλήρου εκτός λειτουργίας και αφετέρου έχουν τη δυνατότητα αυτόματα και κατανεμημένα να επανέλθουν στο βέλτιστο, για τα δεδομένα της κατάστασης, επίπεδο λειτουργίας τους.
Έξυπνα συστήματα μεταφορών: Τα ασύρματα δίκτυα πλέγματος αποτελούν ευέλικτη πλατφόρμα για μεταφορά πληροφοριών και δεδομένων, απαραίτητα για τον έλεγχο υπηρεσιών μεταφοράς (λεωφορεία, τραμ, τρένα, κα.) επιτυγχάνοντας μείωση της συμφόρησης στους δρόμους, έλεγχο των ρύπων και αύξηση της απόδοσης και ασφάλειας των μέσων μεταφοράς.

Εκτός από το εμπορικό ενδιαφέρον για την ανάπτυξη ασύρματων δικτύων πλέγματος σε αστικές και μη αστικές περιοχές από παρόχους, ιδιαίτερο ενδιαφέρον παρουσιάζει η ανάπτυξη τέτοιων δικτύων για την ευρυζωνική διασύνδεση σημείων ενδιαφέροντος της τοπικής αυτοδιοίκησης και υπαλλήλων της. Μια άλλη κατεύθυνση -ευρέως διαδεδομένη και στην Ελλάδα- είναι η ανάπτυξη **κοινοτικών ασύρματων δικτύων (community wireless networks)** που χρησιμοποιούνται

για τη διαμοίραση αρχείων, τη σύνδεση στο διαδίκτυο και την επικοινωνία μεταξύ χρηστών.

Πολλές έρευνες διεξάγονται σχετικά με τα δίκτυα mesh, αφού έχουν σημαντικά χαμηλότερο κόστος σε σχέση με τις παραδοσιακές ενσύρματες υποδομές.

Το **project RoofNet** είναι έναι πειραματικό 802.11b/g mesh δίκτυο, το οποίο βρίσκεται υπό ανάπτυξη στο Computer Science and Artificial Intelligence Laboratory of the Massachusetts Institute of Technology (MIT). Απέδειξε οτι είναι δυνατό να παρέχει σε μια πόλη όπως η Βοστώνη, ευρυζωνική πρόσβαση με ένα ασύρματο 802.11b δίκτυο κορμού. Το RoofNet αποτελείται από έναν περιορισμένο αριθμό κόμβων, οι οποίοι είναι τοποθετημένοι σε στέγες και λειτουργούν σε εθελοντική βάση. Οι κόμβοι αυτοί δημιουργούν δυναμικά και υποστηρίζουν το τη δικτύωση mesh. Παρόμοιες μελέτες διεξάγονται και σε άλλες πόλεις, όπως το Βερολίνο. Το **'Berlin Roof Net'** είναι ένα project που εκτελείται από εθελοντές φοιτητές του Τμήματος Επιστήμης Υπολογιστών στο Πανεπιστήμιο Humboldt του Βερολίνου. Ο στόχος του έργου είναι η κατασκευή ενός δικτύου αποτελούμενου από κόμβους (access points), που μοιράζονται την πρόσβαση στο Διαδίκτυο μέσω ασύρματων ραδιο συνδέσεων.

Εικόνα 20. Mesh router

4.4.3 Πλεονεκτήματα - Μειονεκτήματα

Ένα ασύρματο δίκτυα πλέγματος έχει τα εξής πλεονεκτήματα:

- **Αυτοθεραπευόμενο:** Με την άμεση επαναδιαμόρφωση των πινάκων των διαδρομών με επανυπολογισμό των διαδρομών ώστε να διατηρήσουν τη ροή της κίνησης
- **Αυτοδιαμορφώμενο:** Η προσθήκη νέων κόμβων ή η επανατοποθέτηση υπαρχόντων κόμβων είναι πολύ απλή

- **Υψηλά προσαρμοζόμενο:** Με κόμβους επαναλήπτες καλύπτουμε τα κενά που υπάρχουν στο δίκτυο
- **Αξιοπιστία και πλεονασμός:** Κάθε κόμβος είναι ενωμένος με τους υπόλοιπους κόμβους και έτσι υπάρχουν πολλαπλές διαδρομές που μπορεί ν' ακολουθήσει ένα μήνυμα για να φθάσει στο προορισμό του
- **Κλιμακούμενο:** Μπορεί ν' αντέξει εκατοντάδες ή χιλιάδες κόμβους επειδή δεν είναι κεντρικοποιημένο, γεγονός το οποίο δίνει σταθερότητα
- Με την προσθήκη νέων κόμβων γίνεται ισχυρό το σήμα στο δέκτη και έτσι μπορούμε να λύσουμε πολύ απλά το πρόβλημα ενός αδύνατου σήματος ή μιας νεκρής ζώνης

Επίσης έχει και τα παρακάτω μειονεκτήματα:

- Η τοπολογία είναι πολύ ακριβή επειδή χρειάζεται ένας μεγάλος αριθμός συρμάτων και συνδέσεων
- Όταν η σύνδεση μεταξύ δύο κόμβων δεν είναι ισχυρή γι' αποστολή μεγάλων μηνυμάτων, αλλά στέλνονται μικρά μηνύματα και οι δύο κόμβοι πιστεύουν πως η σύνδεση είναι χρησιμοποιήσιμη
- Κάποια προϊόντα δικτύων mesh χρειάζονται ένα κεντρικό εξυπηρετητή στο να παίρνει σημαντικές αποφάσεις για την τοπολογία του δικτύου και των διαδρομών που ακολουθούνται στο δίκτυο. Τα κινητά δίκτυα πλέγματος απαιτούν προϊόντα τα οποία είναι ικανά να λειτουργούν αυτόνομα χωρίς κεντρικό εξυπηρετητή
- Δεν μπορούμε να έχουμε πολλαπλές ταυτόχρονες επικοινωνίες
- Το μέγιστο διαθέσιμο εύρος ζώνης μειώνεται με ένα ρυθμό (1/2)n, όπου n είναι ο αριθμός των ενδιάμεσων κόμβων που χρειάζεται να περάσει ένα πακέτο μηνυμάτων για να φθάσει στο προορισμό του
- Με το πρόβλημα του ανταγωνισμού μεταξύ των μηνυμάτων που στέλνονται από το ένα κόμβο στον άλλο, το εύρος ζώνης μειώνεται ακόμη περισσότερο

4.4.4 Τεχνολογικές προκλήσεις

Τα ασύρματα δίκτυα πλέγματος είναι ένας τομέας έρευνας αιχμής με πολλά ανοικτά πεδία. Σημαντικότεροι επιμέρους τομείς είναι οι ακόλουθοι:

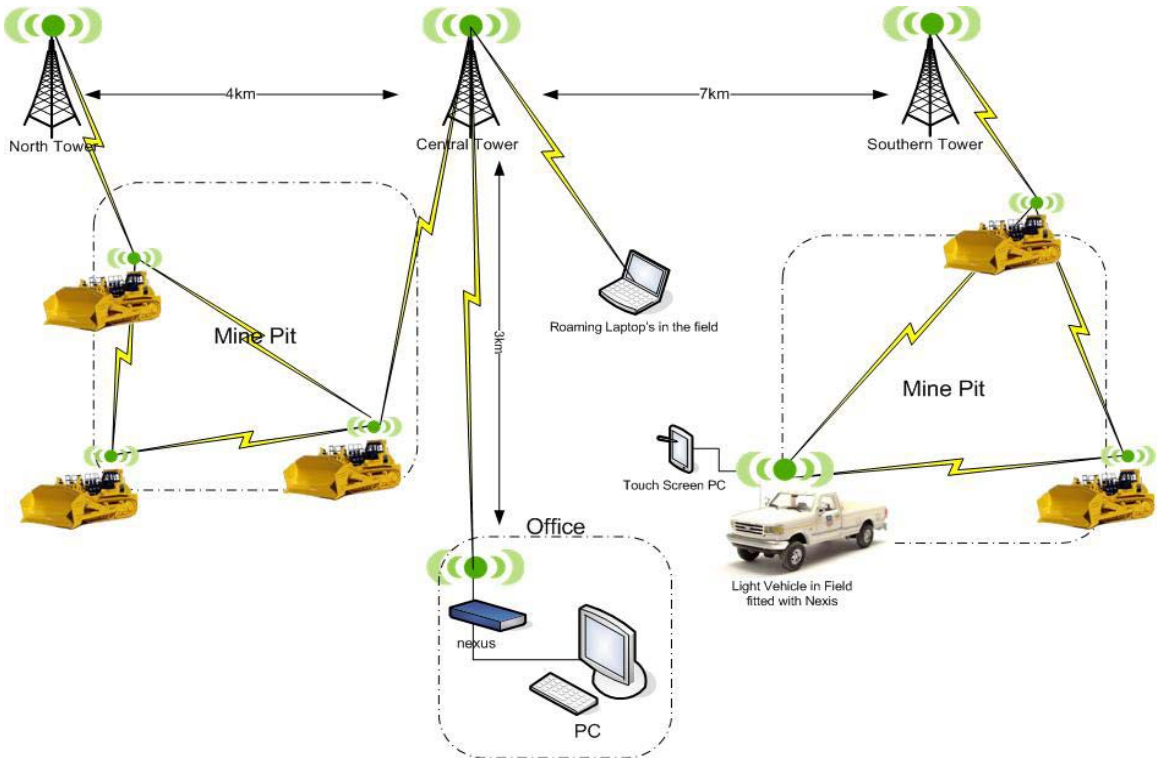
Αυτό-διαμόρφωση και αυτό-διαχείριση: Για την ελαχιστοποίηση του κόστους διαχείρισης και λειτουργίας, καθώς και για τη γρήγορη αντιμετώπιση προβλημάτων, τα ασύρματα δίκτυα πλέγματος θα πρέπει να διαθέτουν αυτόματους μηχανισμούς για τη διαμόρφωση του δικτύου, την προσθήκη νέων κόμβων και την αναπροσαρμογή του δικτύου για παράκαμψη προβληματικών κόμβων ή συνδέσμων.

Αξιοποίηση δικτυακών πόρων: Τα ασύρματα δίκτυα πλέγματος πρέπει να διαθέτουν προηγμένους μηχανισμούς για μέγιστη αξιοποίηση τόσο του ασύρματου φάσματος όσο και των σταθερών συνδέσεων με το διαδίκτυο, επιτυγχάνοντας ταυτόχρονα μείωση της ηλεκτρομαγνητικής ακτινοβολίας που εκπέμπεται.

Διαθεσιμότητα και υποστήριξη εγγυήσεων σε ποιότητα υπηρεσιών (Quality of Service): Η διαθεσιμότητα των ασύρματων δικτύων πλέγματος πρέπει να είναι εφάμιλλη εκείνης των τεχνολογιών ενσύρματης ευρυζωνικής πρόσβασης και των δικτύων κινητής τηλεφωνίας. Επιπλέον, οι εφαρμογές πραγματικού χρόνου όπως η μετάδοση φωνής (voice-over-IP), τηλεόρασης (IPTV) και βίντεο απαιτούν κάποιες ελάχιστες εγγυήσεις σε καθυστέρηση και χωρητικότητα.

Ασφάλεια: Θα πρέπει να διασφαλίζεται η εξουσιοδοτημένη πρόσβαση χρηστών και η εμπιστευτικότητα της επικοινωνίας πάνω από ασύρματα δίκτυα πλέγματος. Επιπλέον, απαιτείται αντιμετώπιση επιθέσεων άρνησης εξυπηρέτησης (Denial of Service) με την ακριβή και έγκαιρη ανίχνευση των επιθέσεων αυτών και την αναδιαμόρφωση του ασύρματου δικτύου ώστε ν' απομονώσει τους επιτιθέμενους κόμβους και συνδέσμους.

Κινητικότητα χρηστών (user mobility): Από τους πιο βασικούς στόχους των ασύρματων δικτύων πλέγματος, είναι η παροχή ευρυζωνικής πρόσβασης σε κινούμενους χρήστες. Αυτό απαιτεί γρήγορη μεταφορά συνδέσεων (hand-off) μεταξύ διαφορετικών κόμβων πρόσβασης, ειδικά για τη μετάδοση φωνής που είναι ευαίσθητη σε καθυστερήσεις, αλλά και δυνατότητα μεταγωγής μεταξύ κόμβων διαφορετικών παρόχων.



Εικόνα 21. Εφαρμογή δικτύου Mesh σε ένα μεταλλείο κάρβουνου

Κεφάλαιο 5
Δρομολόγηση

5.1 Εισαγωγή

Η **δρομολόγηση** κατευθύνει (προωθεί) τα λογικά διευθυνσιοδοτημένα πακέτα από την πηγή τους προς τον προορισμό τους μέσω ενδιάμεσων κόμβων (που λέγονται δρομολογητές). Η διαδικασία της δρομολόγησης κατευθύνει, προωθώντας τα δεδομένα, με βάση πίνακες δρομολόγησης που βρίσκονται στους δρομολογητές, οι οποίοι διατηρούν μια εγγραφή για την καλύτερη διαδρομή προς διάφορες κατευθύνσεις στο δίκτυο. Κατά συνέπεια η κατασκευή των πινάκων δρομολόγησης είναι πολύ σημαντική για αποτελεσματική δρομολόγηση.

Σε μικρά δίκτυα οι πίνακες δρομολόγησης μπορούν να συμπληρωθούν και με το χέρι. Σε μεγάλα δίκτυα που εμπλέκονται και πολύπλοκες τοπολογίες και μπορεί ν' αλλάζουν διαρκώς, κάνει την με το χέρι κατασκευή των πινάκων δρομολόγησης προβληματική. Εντούτοις, τα περισότερα δημόσια τηλεφωνικά δίκτυα μεταγωγής (PSTN) χρησιμοποιούν προ-υπολογισμένους πίνακες δρομολόγησης, με εφεδρικές διαδρομές αν η πιο σύντομη μπλοκαριστεί. Η δυναμική δρομολόγηση προσπαθεί να λύσει αυτό το πρόβλημα κατασκευάζοντας τους πίνακες δρομολόγησης αυτόματα, βασιζόμενη στις πληροφορίες που μεταφέρονται από τα πρωτόκολλα δρομολόγησης και αφήνει το δίκτυο να ενεργεί σχεδόν αυτόνομα στο ν' αποφεύγει βλάβες και μπλοκαρίσματα.

Η δυναμική δρομολόγηση κυριαρχεί στο Ίντερνετ. Εντούτοις όμως, η ρύθμιση των πρωτοκόλλων δρομολόγησης απαιτεί ικανότητες. Δεν θα πρέπει κάποιος να υποθέτει ότι η τεχνολογία των δικτύων έχει εξελιχθεί μέχρι το σημείο της πλήρους αυτοματοποίησης της δρομολόγησης.

Τα **δίκτυα μεταγωγής πακέτων (packet-switched networks)** όπως το Ίντερνετ, χωρίζουν τα δεδομένα σε πακέτα, που το καθένα περιέχει πληροφορίες για τον προορισμό του και δρομολογούνται ξεχωριστά. Τα δίκτυα μεταγωγής κυκλώματος όπως τα τηλεφωνικά δίκτυα, εκτελούν και αυτά δρομολόγηση, με σκοπό να βρούν διαδρομές για κυκλώματα (όπως τηλεφωνικές κλήσεις) πάνω από τις οποίες μπορούν να στείλουν μεγάλες ποσότητες δεδομένων χωρίς να επαναλαμβάνουν συνεχώς την διεύθυνση του προορισμού.

Το υλικό που χρησιμοποιείται στην δρομολόγηση περιλαμβάνει συγκεντρωτές, μεταγωγείς και δρομολογητές.

Στα δίκτυα υπολογιστών ο όρος **δρομολόγηση (routing)** αναφέρεται στη διαδικασία με την οποία επιλέγεται η διαδρομή μέσα σε ένα δίκτυο πάνω από την οποία θα σταλούν δεδομένα.

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 σ' 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. Το γεγονός αυτό επιβάλει οι κόμβοι του 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.

5.2 Πρωτόκολλα δρομολόγησης για ad-hoc δίκτυα

5.2.1 Εισαγωγή

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.

Τα πρωτόκολλα δρομολόγησης για ad hoc δίκτυα μπορούν να διαιρεθούν σε δύο βασικές κατηγορίες:

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

Μια επιπλέον κατηγορία είναι η εξής:

- **Hybrid πρωτόκολλα**

5.2.2 Proactive και Reactive πρωτόκολλα δρομολόγησης

Τα ad-hoc πρωτόκολλα δρομολόγησης μπορούν να ταξινομηθούν ως **Proactive** και **Reactive**. Τα πρώτα εξουσιοδοτούν τους κόμβους σε ένα ad-hoc κινητό δίκτυο ν' ανακαλύπτουν και να γνωρίζουν τις διαδρομές προς όλους τους πιθανούς προορισμούς του δικτύου έτσι ώστε, όταν πρέπει να διαβιβαστεί ένα πακέτο, να είναι ήδη γνωστή η διαδρομή που αυτό πρέπει ν' ακολουθήσει. Τα πρωτόκολλα της δεύτερης κατηγορίας υιοθετούν μια διαφορετική προσέγγιση με την οποία οι κόμβοι ανακαλύπτουν μόνο τις διαδρομές προς αυτούς τους προορισμούς, για τους οποίους γίνεται σχετική αίτηση εύρεσης μιας διαδρομής. Ένας κόμβος δεν χρειάζεται να γνωρίζει μια διαδρομή προς ένα προορισμό, παρά μόνο όταν πακέτα δεδομένων τα οποία πρέπει να προωθήσει, έχουν σαν τελικό προορισμό τους τον κόμβο αυτό. Τα **proactive πρωτόκολλα** έχουν το πλεονέκτημα ότι ένας κόμβος υπόκειται στην ελάχιστη καθυστέρηση για την απόκτηση μιας διαδρομής, αφού αυτή αν υπάρχει θα είναι διαθέσιμη στους πίνακες δρομολόγησης του συγκεκριμένου κόμβου. Εντούτοις τα πρωτόκολλα αυτά δεν είναι αποδοτικά σε όλες τις περιπτώσεις και σενάρια χρήσης, δεδομένου ότι χρησιμοποιούν ένα ουσιαστικό μέρος των πόρων του δικτύου για την διατήρηση και ανανέωση των πληροφοριών δρομολόγησης που γνωρίζουν οι κόμβοι. Για ν' αντιμετωπίσουν ακριβώς αυτό το μειονέκτημα, τα **reactive πρωτόκολλα** υιοθετούν την

προσέγγιση της εύρεσης μιας διαδρομής για έναν προορισμό μόνο όταν αυτό απαιτείται. Τα re-active πρωτόκολλα καταναλώνουν πολύ λιγότερους πόρους σε σχέση με τα προηγούμενα, αλλά η αρχική καθυστέρηση εύρεσης μιας διαδρομής μπορεί να είναι σημαντικά μεγάλη και μπορεί να είναι, αν όχι μεγαλύτερη, συγκρίσιμη με τον χρόνο που απαιτείται για την μεταφορά των πραγματικών δεδομένων ανάμεσα σε δύο κόμβους. Εν συντομία, μπορούμε να καταλήξουμε στο συμπέρασμα ότι κανένα πρωτόκολλο δεν είναι υλοποιημένο να λειτουργεί το ίδιο αποδοτικά και αποτελεσματικά σε όλα τα πιθανά δικτυακά περιβάλλοντα και γι' αυτό έχουν γίνει προτάσεις που χρησιμοποιούν υβριδικές προσεγγίσεις για την αντιμετώπιση αυτού του προβλήματος.

5.2.3 Proactive πρωτόκολλα δρομολόγησης (DSDV, WRP)

Σ' αυτό το τμήμα εξετάζουμε μερικά από τα σημαντικότερα proactive πρωτόκολλα δρομολόγησης.

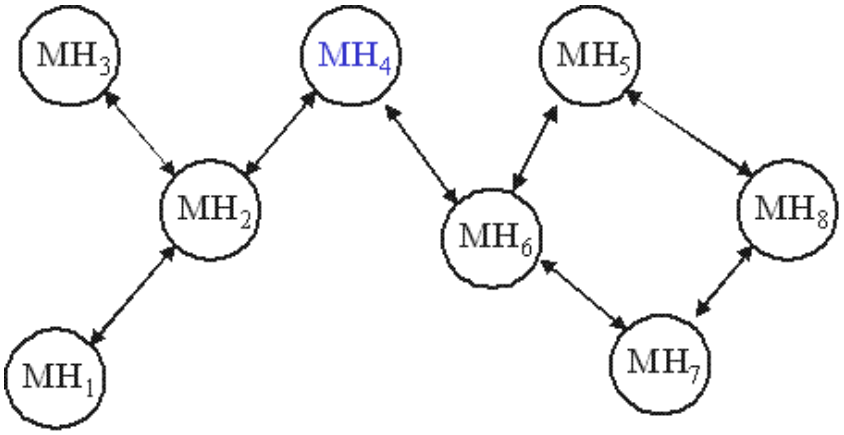
1) Dynamic Destination Sequenced Distance Vector Routing Protocol (DSDV)

Ο **DSDV** βασίζεται στον κλασσικό αλγόριθμο δρομολόγησης των **Bellman-Ford**, με κάποιες βελτιώσεις.

Σύμφωνα με το DSDV, κάθε κινητός κόμβος του δικτύου διατηρεί έναν πίνακα δρομολόγησης, στον οποίο αποθηκεύει όλους τους πιθανούς προορισμούς, τον απαιτούμενο αριθμό των hops για κάθε προορισμό και τον sequence number, ο οποίος έχει οριστεί από τον προορισμό. Ο αριθμός αυτός χρησιμοποιείται για να διαχωριστούν οι παλιές διαδρομές από τις νεώτερες και έτσι αποφεύγεται η δημιουργία loops. Οι κόμβοι μεταδίδουν περιοδικά τους πίνακες δρομολόγησής τους στους άμεσους γείτονές τους, έτσι ώστε να διατηρείται η συνέπεια των πινάκων. Επίσης μεταδίδουν τους πίνακές δρομολόγησής τους αν συμβεί κάποια σημαντική αλλαγή στην τοπολογία του δικτύου (και επομένως στους πίνακές τους), στο χρόνο μεταξύ των περιοδικών μεταδόσεων. Για να μειωθεί η πιθανά μεγάλη κίνηση στο δίκτυο που μπορεί να προκληθεί από τέτοιου είδους ενημερώσεις των πινάκων δρομολόγησης, οι ενημερώσεις αυτές μπορούν να σταλούν με δύο είδη πακέτων. Το πρώτο είδος, είναι γνωστό σαν **"full dump"** πακέτα, περιέχουν ολόκληρους τους πίνακες δρομολόγησης και μπορεί ν' απαιτήσουν πολλαπλές μονάδες δεδομένων του πρωτοκόλλου του δικτύου (NPDUs). Το δεύτερο είδος είναι τα **πακέτα επαύξησης (incremental packets)**, τα οποία χρησιμοποιούνται για να σταλούν μόνο εκείνες οι εγγραφές των πινάκων δρομολόγησης που έχουν αλλάξει από την τελευταία ενημέρωση και πρέπει να χωρούν σε ένα NPDU και έχουν ως αποτέλεσμα να μειώνεται το ποσό της κίνησης που παράγεται. Αν υπάρχει χώρος στα πακέτα επαύξησης, τότε μπορούν να συμπεριληφθούν και οι εγγραφές εκείνες των οποίων έχει αλλάξει ο sequence number. Όταν το δίκτυο είναι σχετικά σταθερό, στέλνονται πακέτα επαύξησης, έτσι ώστε ν' αποφευχθεί η επιπλέον κίνηση, ενώ τα πακέτα "full dump" είναι σχετικά σπάνια. Σ' ένα δίκτυο που αλλάζει συχνά, τα πακέτα επαύξησης μπορεί να μεγαλώσουν, επομένως τα πακέτα "full dump" θα είναι πιο συχνά. Κάθε πακέτο ενημέρωσης, περιέχει τη διεύθυνση του προορισμού, τον αριθμό των hops για να φτάσουμε στον προορισμό αυτό, το sequence number των πληροφοριών που ελήφθησαν σε σχέση με τον προορισμό αυτό, όπως επίσης και ένα sequence number το οποίο είναι μοναδικό για την εκπομπή. Η διαδρομή με το μεγαλύτερο sequence number, δηλαδή η πιο πρόσφατη, είναι αυτή που χρησιμοποιείται. Στην περίπτωση που δύο διαδρομές έχουν το ίδιο sequence number, τότε η διαδρομή με την καλύτερη μετρική, δηλαδή η μικρότερη διαδρομή, χρησιμοποιείται. Όταν κάποιος κόμβος A 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 A θα κοινοποιήσει στους γείτονές του τον πίνακα

δρομολόγησής του, θα δώσει στη διαδρομή προς τον D, άπειρο hop-count και ένα sequence number που είναι μεγαλύτερος 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.



Εικόνα 22. Ο DSDV σε λειτουργία

Πλεονεκτήματα:

- Εγγυάται ότι δεν υπάρχουν loops στους πίνακες δρομολόγησης, χρησιμοποιώντας τα sequence numbers για να διαχωρίσει τις παλιές από τις νέες διαδρομές.
- Ενώ παρέχει μόνο ένα μονοπάτι για κάθε προορισμό, επιλέγει το μικρότερο μονοπάτι βασισμένος στον αριθμό των hops για τον προορισμό.
- Παρέχει δύο είδη πακέτων ενημέρωσης, το ένα από τα οποία είναι σημαντικά μικρότερο από το άλλο και το οποίο μπορεί να χρησιμοποιηθεί για ενημερώσεις επαύξησης έτσι ώστε να μη χρειάζεται να σταλεί ολόκληρος ο πίνακας δρομολόγησης για κάθε αλλαγή στην τοπολογία του δικτύου.
- Διατηρεί ενημερωμένες διαδρομές χρησιμοποιώντας τα sequence numbers.

Μειονεκτήματα:

Ο DSDV είναι μη αποδοτικός γιατί:

- Απαιτεί εκπομπή περιοδικών ενημερώσεων ανεξάρτητα από τον αριθμό των αλλαγών στην τοπολογία του δικτύου, το οποίο έχει ως σαν συνέπεια να

περιορίζεται ο αριθμός των κόμβων που μπορούν να συνδεθούν στο δίκτυο, αφού το συνολικό κόστος του δικτύου αυξάνεται.

- Χρειάζεται κάποιο χρόνο έτσι ώστε να συγκλίνει πριν χρησιμοποιηθεί κάποια διαδρομή. Αυτός ο χρόνος σύγκλισης μπορεί να θεωρηθεί αμελητέος σ' ένα στατικό δίκτυο, όπου η τοπολογία δεν αλλάζει και τόσο συχνά, αλλά στα ad hoc δίκτυα η τοπολογία περιμένουμε να μεταβάλλεται πολύ συχνά. Έτσι ο χρόνος αυτός σύγκλισης μπορεί να σημαίνει ότι ένας μεγάλος αριθμός πακέτων έχουν απορριφθεί προτού βρεθεί μια κατάλληλη διαδρομή.

2) The Wireless Routing Protocol (WRP)

Το **ασύρματο πρωτόκολλο δρομολόγησης (WRP)** [Murthy 1996] είναι ένα πρωτόκολλο που βασίζεται σε πίνακες δρομολόγησης με στόχο την εύρεση και διατήρηση πληροφοριών δρομολόγησης μεταξύ όλων των κόμβων του δικτύου. Κάθε κόμβος στο δίκτυο είναι αρμόδιος για τη διατήρηση τεσσάρων πινάκων: του πίνακα απόστασης, του πίνακα δρομολόγησης, του πίνακα κόστους των συνδέσεων των κόμβων και τέλος ενός πίνακα που περιέχει ένα **κατάλογο μηνυμάτων αναμετάδοσης (Message Retransmission List MRL)**. Κάθε καταχώρηση του MRL περιέχει τον αριθμό ακολουθίας του μηνύματος ενημέρωσης ενός μετρητή αναμετάδοσης, ενός διανύσματος καταχωρήσεων απαιτήσεων επιβεβαιώσεων, μίας για κάθε γειτονικό κόμβο και ενός καταλόγου ενημερώσεων διαδρομών που περιέχονται στα μηνύματα ενημέρωσης. Για τη μετάδοση από ένα κόμβο των αρχείων του MRL στους γείτονες του, μέσω ενός μηνύματος ενημέρωσης, είναι απαραίτητο να λάβει από κάθε κόμβο επιβεβαίωση της ορθής τους μετάδοσης.

Οι κόμβοι ενημερώνουν ο ένας τον άλλο για τις αλλαγές των συνδέσεων μεταξύ τους, λόγω της κινητικότητας, μέσω της χρήσης των μηνυμάτων ενημέρωσης. Ένα μήνυμα ενημέρωσης στέλνεται μόνο μεταξύ γειτονικών κόμβων και περιέχει έναν κατάλογο αναπροσαρμογών (με τον προορισμό, την απόσταση από τον προορισμό και τον προκάτοχο του προορισμού), καθώς επίσης και έναν κατάλογο με τους κόμβους που πρέπει ν' απαντήσουν με μια επιβεβαίωση παραλαβής των δεδομένων αυτών (Acks). Μετά την επεξεργασία των νέων πληροφοριών δρομολόγησης από τους γείτονες ή την ανίχνεύση μιας αλλαγής σε μια σύνδεση, στέλνονται μηνύματα αναπροσαρμογών στους γείτονες κόμβους, περιέχοντας τις αλλαγές που έχουν ανακαλυφθεί. Σε περίπτωση απώλειας μιας σύνδεσης μεταξύ δύο κόμβων, οι κόμβοι στέλνουν μηνύματα ενημέρωσης στους γείτονές τους. Οι γείτονες τροποποιούν έπειτα τις καταχωρήσεις τους και ελέγχουν για νέες πιθανές διαδρομές μέσω άλλων κόμβων, για κάθε πιθανό προορισμό. Οποιεσδήποτε νέες πορείες ανακαλυφθούν, μεταδίδονται και αυτές, έτσι ώστε να μπορούν να ενημερώσουν τους πίνακές τους και οι υπόλοιποι κόμβοι του δικτύου, αναλόγως.

Οι κόμβοι μαθαίνουν για την ύπαρξη των γειτόνων τους από την παραλαβή των μηνυμάτων επιβεβαιώσεων ή άλλων μηνυμάτων. Εάν ένας κόμβος δε μεταδίδει τέτοια μηνύματα, πρέπει να στείλει ένα (HELLO) μήνυμα εντός ενός καθορισμένου χρονικού διαστήματος, για να εξασφαλίσει την διασύνδεση με τους γείτονές του. Διαφορετικά, η έλλειψη μηνυμάτων οποιοδήποτε τύπου από κάποιο κόμβο, δείχνει αποτυχία για εκείνη τη σύνδεση, γεγονός που μπορεί να προκαλέσει ένα λάθος συναγερμό. Όταν ένας κόμβος λαμβάνει ένα (HELLO) μήνυμα από έναν νέο κόμβο του δικτύου, ο νέος κόμβος προστίθεται στον πίνακα δρομολόγησης και λαμβάνει ένα αντίγραφο των πινάκων δρομολόγησής του κόμβου στον οποίο έστειλε αρχικά το (HELLO) μήνυμα.

Μία σημαντική καινοτομία του WRP είναι ο τρόπος με τον οποίο επιτυγχάνει την απομάκρυνση των κυκλικών βρόγχων στις διαδρομές δρομολόγησης. Οι κόμβοι που συμμετέχουν στη διαδικασία δρομολόγησης επιβάλλεται να εκτελούν ελέγχους συνέπειας με τις παλιότερες πληροφορίες δρομολόγησης για κάθε διαδρομή, που αναφέρονται από όλους τους γείτονές τους, με αποτέλεσμα να εξαλείφουν

οποιουσδήποτε κυκλικές διαδρομές. Ταυτόχρονα παρέχουν την δυνατότητα διόρθωσης μιας διαδρομής μετά από την αποτυχία μίας σύνδεσης πάνω σε αυτή.

5.2.4 Reactive πρωτόκολλα δρομολόγησης (AODV, DSR)

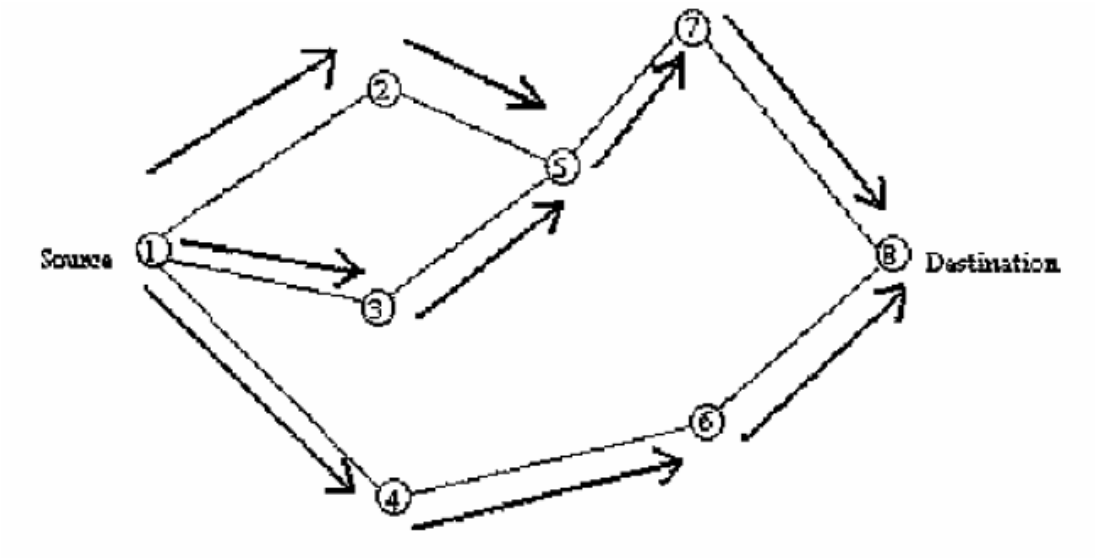
1) Ad hoc On demand Distance Vector Routing Protocol (AODV)

Το **AODV** πρωτόκολλο δρομολόγησης δημιουργείται με βάση τον DSDV αλγόριθμο. Το AODV είναι μια βελτίωση του DSDV, αφού τυπικά ελαχιστοποιεί τον αριθμό των εκπομπών που απαιτούνται, δημιουργώντας διαδρομές όταν απαιτούνται, σε αντίθεση με τον DSDV που διατηρεί μια πλήρη λίστα των διαδρομών. Οι συγγραφείς του AODV το κατατάσσουν σαν ένα απλό σύστημα απόκτησης διαδρομής όταν απαιτείται, αφού οι κόμβοι που δε βρίσκονται στο επιλεγμένο μονοπάτι δε διατηρούν πληροφορίες δρομολόγησης, ούτε συμμετέχουν σε ανταλλαγές πινάκων δρομολόγησης.

Κάθε κόμβος του δικτύου διατηρεί ένα πίνακα Δρομολόγησης, κάθε εγγραφή του οποίου περιέχει τις ακόλουθες πληροφορίες:

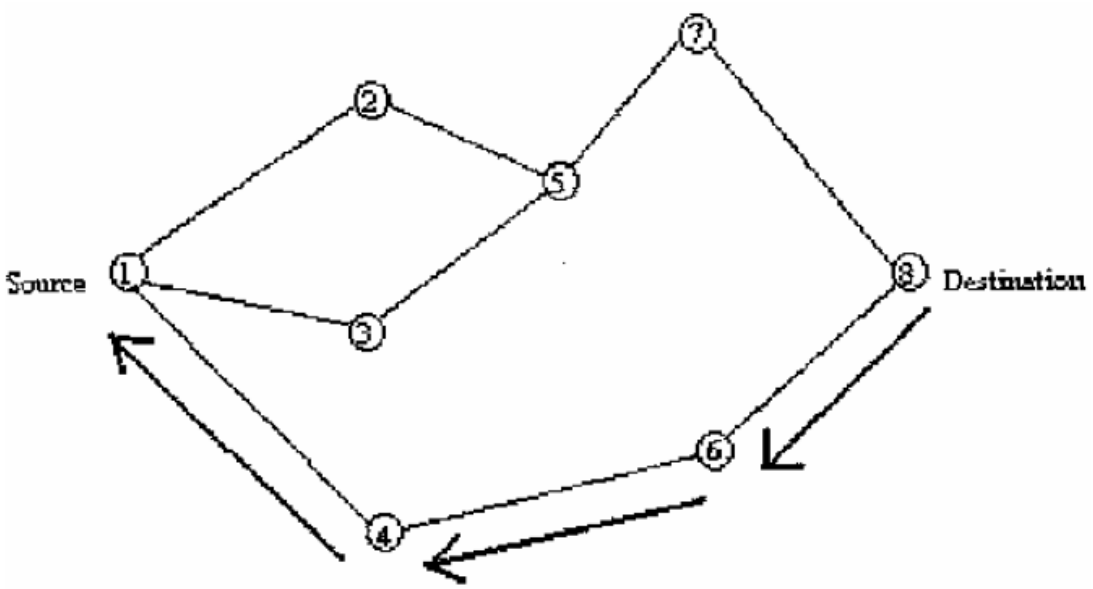
- Την IP διεύθυνση του προορισμού
- Τον sequence number του προορισμού
- Τον αριθμό των hops μέχρι τον προορισμό
- Το επόμενο βήμα-κόμβο, το οποίο έχει επιλεγεί για την αποστολή πακέτων στον προορισμό μέσω αυτής της διαδρομής
- Το χρόνο για τον οποίο η διαδρομή θεωρείται έγκυρη (lifetime)
- Τους γειτονικούς κόμβους, οι οποίοι χρησιμοποιούν ενεργά αυτή τη διαδρομή
- Ένα buffer(Request Buffer), ο οποίος εξασφαλίζει ότι μια αίτηση επεξεργάζεται μόνο μια φορά

Όταν ένας κόμβος-πηγή επιθυμεί να στείλει ένα μήνυμα σε κάποιον κόμβο-προορισμό, για να βρει ένα μονοπάτι για τον προορισμό αυτό, ξεκινά μια διαδικασία ανεύρεσης μονοπατιού για να τον εντοπίσει. Εκπέμπει ένα πακέτο αίτησης διαδρομής (RREQ) στους γείτονές του. Αυτοί με τη σειρά τους προωθούν την αίτηση στους γείτονές τους και ούτω καθεξής, μέχρι να φτάσει σε έναν ενδιάμεσο κόμβο που έχει μια πρόσφατη διαδρομή για τον προορισμό, ή μέχρι να φτάσει στον προορισμό (όπως φαίνεται στην εικόνα 23). Ένας κόμβος πετά ένα πακέτο αίτησης διαδρομής που έχει ξαναδεί. Ο AODV χρησιμοποιεί τους sequence numbers των προορισμών (οι οποίοι αλλάζουν όταν συμβεί κάτι στην περιβάλλουσα περιοχή) για να εξασφαλίσει ότι όλες οι διαδρομές δεν περιέχουν βρόχους (loop-free) και περιέχουν τις πιο πρόσφατες πληροφορίες διαδρομών. Κάθε κόμβος διατηρεί ένα δικό του sequence number, καθώς και ένα ID εκπομπής. Το ID αυτό αυξάνεται για κάθε RREQ που ξεκινά ο κόμβος και μαζί με την IP διεύθυνση του κόμβου, προσδιορίζουν μοναδικά ένα RREQ. Μαζί με το δικό του sequence number και το ID εκπομπής, ο κόμβος-πηγή συμπεριλαμβάνει στο RREQ τον πιο πρόσφατο sequence number που έχει για τον προορισμό. Ενδιάμεσοι κόμβοι μπορούν ν' απαντήσουν στο RREQ μόνο αν έχουν μια διαδρομή για τον προορισμό, της οποίας ο αντίστοιχος sequence number του προορισμού είναι μεγαλύτερος ή ίσος με αυτόν που περιέχεται στο RREQ.



Εικόνα 23. Μετάδοση του πακέτου αίτησης διαδρομής (RREQ)

Κατά τη διάρκεια της διαδικασίας της προώθησης του RREQ, οι ενδιάμεσοι κόμβοι καταγράφουν στον πίνακα δρομολόγησής τους τη διεύθυνση του γείτονα από τον οποίο ήρθε το πρώτο αντίγραφο της αίτησης. Η πληροφορία αυτή χρησιμοποιείται για την κατασκευή του αντίστροφου μονοπατιού για το πακέτο απάντησης διαδρομής (RREP). Όταν το RREQ φτάσει στον προορισμό ή σε έναν ενδιάμεσο κόμβο με μια αρκετά "φρέσκια" διαδρομή, ο προορισμός ή ο ενδιάμεσος κόμβος απαντά μεταδίδοντας ένα RREP πακέτο πίσω προς το γείτονα από τον οποίο έλαβε αρχικά το RREQ. Όσο το RREP προωθείται προς τα πίσω κατά μήκος του αντιστρόφου μονοπατιού, οι κόμβοι κατά μήκος του μονοπατιού αυτού δημιουργούν στους πίνακες δρομολόγησής τους εγγραφές διαδρομών προς τα μπρος, που δείχνουν προς τον κόμβο από τον οποίο ήρθε το RREP. Αυτές οι εγγραφές διαδρομών δείχνουν την ενεργή διαδρομή προς τα μπρος. 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.



Εικόνα 24. Το μονοπάτι που ακολουθείται από το πακέτο απάντησης διαδρομής (RREP)

Οι διαδρομές διατηρούνται ως εξής: Αν ένας κόμβος-πηγή μετακινηθεί, τότε μπορεί να ξαναρχίσει το μηχανισμό ανακάλυψης διαδρομής, για να βρει μια νέα διαδρομή για τον προορισμό. Αν ένας ενδιάμεσος κόμβος κατά μήκος της διαδρομής μετακινηθεί, τότε ο προηγούμενος γείτονάς του παρατηρεί τη μετακίνηση (την αποτυχία της σύνδεσης) και μεταδίδει ένα μήνυμα ειδοποίησης αποτυχίας σύνδεσης (ένα RREP με άπειρη μετρική) σε κάθε έναν από τους ενεργούς προηγούμενους γείτονές του, για να τους ενημερώσει για την εξάλειψη αυτού του τμήματος της διαδρομής. Αυτοί οι κόμβοι με τη σειρά τους, μεταδίδουν το μήνυμα ειδοποίησης στους προηγούμενους γείτονές τους και ούτω καθεξής μέχρι να φτάσει στον κόμβο-πηγή. Η πηγή μπορεί τότε να επιλέξει να ξαναρχίσει την ανακάλυψη διαδρομής για τον προορισμό αυτό, αν η διαδρομή είναι ακόμα επιθυμητή.

Μια επιπλέον άποψη του πρωτοκόλλου είναι η χρήση των "hello" μηνυμάτων (ένα ειδικό τύπο RREP μηνύματος), τα οποία στέλνονται περιοδικά από ένα κόμβο προς όλους τους άμεσους γείτονές του. Αυτά τα μηνύματα έχουν σα στόχο τη διαρκή ενημέρωση κάθε κόμβου για άλλους κόμβους που βρίσκονται στη γειτονιά του. Οι γείτονες που χρησιμοποιούν διαδρομές μέσω του συγκεκριμένου κόμβου θα εξακολουθήσουν να θεωρούν τις διαδρομές σαν έγκυρες. Τα "hello" μηνύματα μπορούν να χρησιμοποιηθούν για να διατηρηθεί η τοπική συνδετικότητα ενός κόμβου. Παρόλα αυτά, η χρήση τους δεν απαιτείται. Οι κόμβοι ελέγχουν τη μετάδοση πακέτων δεδομένων έτσι ώστε να επιβεβαιώσουν ότι μπορούν ακόμη να φτάσουν στον επόμενο κόμβο. Αν μια τέτοια μετάδοση δεν "ακουστεί", ο κόμβος μπορεί να χρησιμοποιήσει οποιαδήποτε από έναν αριθμό τεχνικών, συμπεριλαμβανομένης και της λήψης "hello" μηνυμάτων, έτσι ώστε να καθορίσει αν ο επόμενος κόμβος βρίσκεται εντός της ακτίνας επικοινωνίας. Αν τα "hello" μηνύματα σταματήσουν να φτάνουν από ένα συγκεκριμένο κόμβο, τότε οι γείτονές του μπορούν να υποθέσουν ότι έχει απομακρυνθεί εκτός ακτίνας επικοινωνίας και να σημαδέψουν τη σύνδεση αυτή σα σπασμένη. Ταυτόχρονα, θα πρέπει να γνωστοποιηθεί η αποτυχία της σύνδεσης αυτής σε όλους τους επηρεαζόμενους κόμβους. Τα "hello" μηνύματα μπορούν να δημιουργήσουν μια λίστα των κόμβων από τους οποίους έχει ακούσει ένας κόμβος, αποδίδοντας έτσι μεγαλύτερη γνώση της συνδετικότητας του δικτύου.

Πλεονεκτήματα:

- Πλεονεκτεί σε σχέση με τους κλασσικούς αλγόριθμους δρομολόγησης, όπως ο Distance Vector και ο Link State, στο ότι έχει περιορίσει σημαντικά τον αριθμό των μηνυμάτων δρομολόγησης μέσα στο δίκτυο.
- Με τη χρήση των sequence numbers εξασφαλίζεται ότι μια διαδρομή είναι πρόσφατη και δεν περιέχει βρόχους (loops).
- Προσθέτει τη δυνατότητα multicast, η οποία αυξάνει την απόδοση σημαντικά όταν ένας κόμβος επικοινωνεί με πολλούς.
- Το πρωτόκολλο είναι κατανεμημένο, αφού δεν εξαρτάται από κάποιον κεντρικοποιημένο κόμβο.
- Διατηρεί χαμηλό το overhead δρομολόγησης, αφού τόσο τα πακέτα αναζήτησης διαδρομής, όσο και τα πακέτα απάντησης διαδρομής, περιέχουν μικρό όγκο πληροφοριών.
- Με την αποστολή "hello" μηνυμάτων μπορεί να διατηρηθεί η τοπική συνδετικότητα του κάθε κόμβου.

Μειονεκτήματα:

- Η χρήση των sequence numbers μπορεί να δημιουργήσει προβλήματα, αν για παράδειγμα πάψουν να είναι συγχρονισμένοι
- Υποστηρίζει μόνο μια διαδρομή για κάθε προορισμό.
- Απαιτεί συμμετρικές συνδέσεις μεταξύ των κόμβων και για το λόγο αυτό δε μπορεί να χρησιμοποιήσει διαδρομές με μη-συμμετρικές συνδέσεις.
- Αν προκύψει μια αποτυχία σύνδεσης κατά μήκος ενός μονοπατιού, ο αλγόριθμος ανακάλυψης διαδρομής πρέπει να ξανακληθεί από την πηγή για να βρεθεί ένα νέο μονοπάτι για τον προορισμό. Δε γίνεται καμιά προσπάθεια να χρησιμοποιηθεί τμηματική ανάκτηση διαδρομής, δηλαδή να επιτραπεί στους ενδιάμεσους κόμβους να προσπαθήσουν να ξαναφτιάξουν μόνοι τους τη διαδρομή. Αυτό μπορεί να οδηγήσει σε μεγαλύτερους χρόνους ανακατασκευής διαδρομής.

  - Όμως η προσπάθεια και η αποτυχία ενός ενδιάμεσου κόμβου να ξαναφτιάξει μια διαδρομή, θα προκαλέσει μεγαλύτερη καθυστέρηση απ' ότι αν ο κόμβος-πηγή είχε προσπαθήσει να την ξαναφτιάξει αμέσως μόλις αντιλήφθηκε τη σπασμένη σύνδεση.

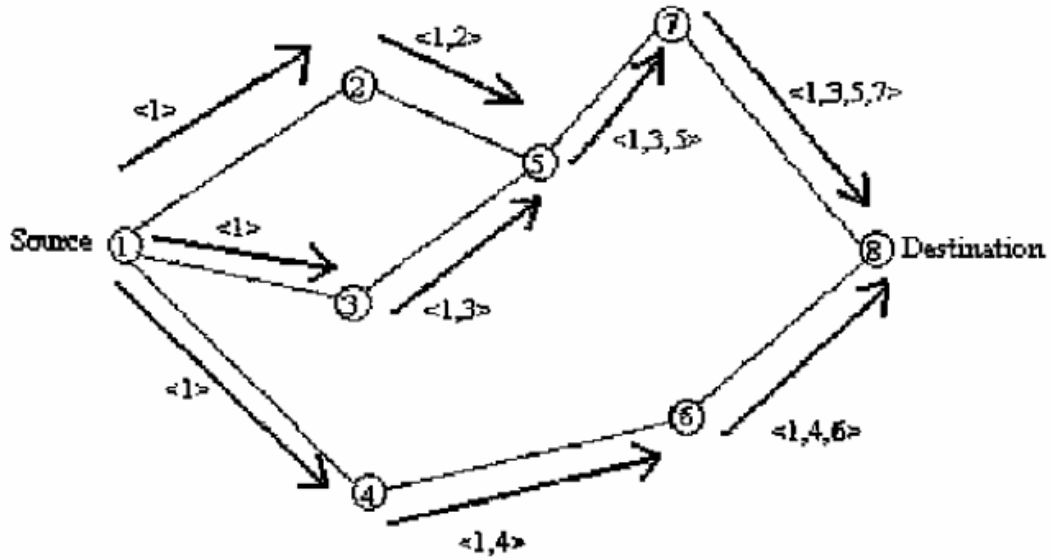
2) Dynamic Source Routing Protocol (DSR)

Το **DSR** πρωτόκολλο, είναι ένα **on-demand πρωτόκολλο δρομολόγησης** το οποίο βασίζεται στην έννοια της δρομολόγησης πηγής. Κάθε κόμβος χρειάζεται να διατηρεί κρυφές μνήμες διαδρομών, οι οποίες περιέχουν τις διαδρομές πηγής για τις οποίες είναι ενήμερος. Οι εγγραφές στην κρυφή μνήμη διαδρομών ενός κόμβου ενημερώνονται συνεχώς, καθώς αυτός μαθαίνει για νέες διαδρομές. Κάθε εγγραφή στην κρυφή μνήμη διαδρομών έχει συσχετισμένη με αυτή μια περίοδο λήξης, μετά την οποία η εγγραφή διαγράφεται από την κρυφή μνήμη.

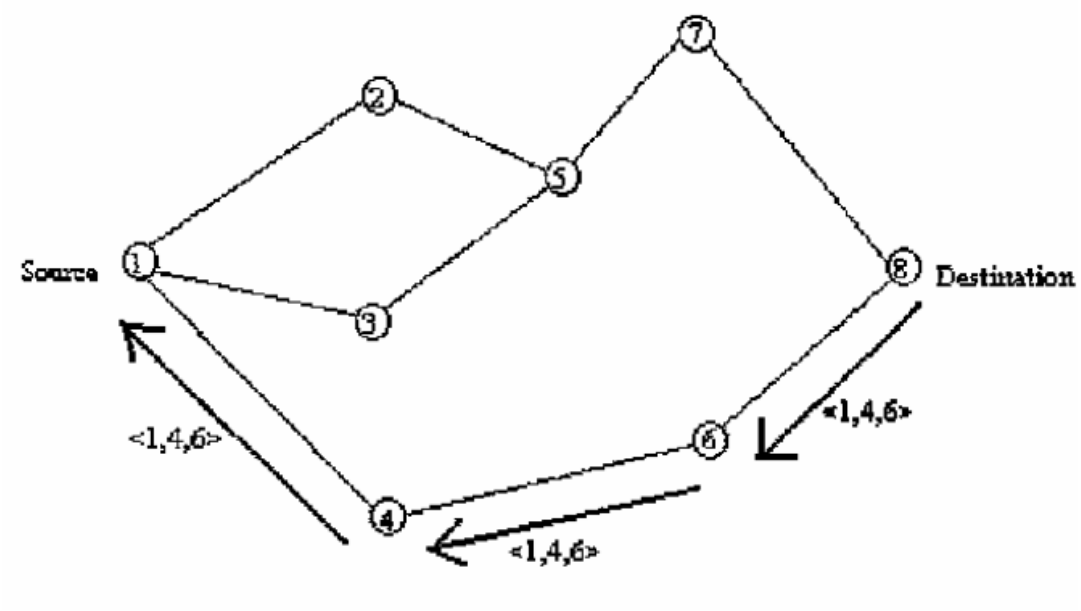
Το πρωτόκολλο αποτελείται από δύο κύριες φάσεις: την ανακάλυψη διαδρομής και τη διατήρηση διαδρομής. Όταν ένας κινητός κόμβος θέλει να στείλει ένα πακέτο σε κάποιον προορισμό, ελέγχει την κρυφή μνήμη διαδρομών του για να καθορίσει αν ήδη έχει μια διαδρομή για τον προορισμό αυτό. Αν βρει ότι υπάρχει μια 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. 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. Ένα πακέτο αίτησης διαδρομής που φτάνει σε έναν από αυτούς τους κόμβους, ήδη περιέχει στο αρχείο διαδρομής του την ακολουθία των βημάτων (κόμβων) που έγιναν από την πηγή μέχρι τον κόμβο αυτό.



Εικόνα 25. Κατασκευή του αρχείου διαδρομής κατά τη διάρκεια της ανακάλυψης διαδρομής



Εικόνα 26. Μετάδοση της απάντησης διαδρομής με το αρχείο διαδρομής

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 και το τοποθετεί στη συνέχεια (το αρχείο διαδρομής) στο πακέτο απάντησης διαδρομής.

Για να επιστρέψει το πακέτο απάντησης διαδρομής, ο κόμβος που απαντά θα πρέπει να έχει μια διαδρομή για την πηγή. Αν έχει μια τέτοια διαδρομή στην κρυφή μνήμη διαδρομών του, μπορεί να τη χρησιμοποιήσει. Αλλιώς, αν υποστηρίζονται οι συμμετρικές συνδέσεις, μπορεί να χρησιμοποιήσει την αντίστροφη διαδρομή του αρχείου διαδρομής. Στην περίπτωση που δεν υποστηρίζονται οι συμμετρικές συνδέσεις, ο κόμβος μπορεί να ξεκινήσει τη δική του διαδικασία ανακάλυψης διαδρομής και να "φορτώσει" την απάντηση διαδρομής στη νέα αίτηση διαδρομής.

Η διατήρηση διαδρομής επιτυγχάνεται μέσω της χρήσης δύο ειδών πακέτων: τα πακέτα Λάθους Διαδρομής και τις Αναγνωρίσεις. Ένα πακέτο Λάθους Διαδρομής παράγεται σε ένα κόμβο, όταν το στρώμα Ζεύξης Δεδομένων αντιμετωπίσει ένα μοιραίο πρόβλημα μετάδοσης. Όταν ένας κόμβος λάβει ένα πακέτο Λάθους Διαδρομής, μετακινεί το hop για το λάθος αυτό από την κρυφή μνήμη διαδρομών του και όλες οι διαδρομές που περιέχουν το βήμα αυτό προς το λάθος, περικόπτονται σε αυτό το σημείο. Επιπρόσθετα με τα πακέτα Λάθους Διαδρομής, χρησιμοποιούνται και πακέτα Αναγνώρισης για την επιβεβαίωση της σωστής λειτουργίας των συνδέσεων των διαδρομών. Τέτοιες Αναγνωρίσεις περιλαμβάνουν και παθητικές αναγνωρίσεις, στις οποίες ο κόμβος είναι σε θέση να "ακούσει" τον επόμενο κόμβο να προωθεί το πακέτο κατά μήκος της διαδρομής.

Πλεονεκτήματα:

- Ένα πλεονέκτημά του σε σχέση με τα υπόλοιπα on-demand πρωτόκολλα, είναι ότι δε χρησιμοποιεί περιοδικά μηνύματα δρομολόγησης και έτσι μειώνεται το πρόσθετο κόστος στο δίκτυο, εξοικονομώντας ενέργεια στους

κόμβους καθώς και πολύτιμο εύρος ζώνης επικοινωνίας. Έτσι το πρωτόκολλο δεν επιφέρει οποιοδήποτε overhead όταν δεν υπάρχουν αλλαγές στην τοπολογία του δικτύου και επιπλέον μπορεί να τεθεί σε κατάσταση sleep mode.

- Χρησιμοποιεί το σημαντικό πλεονέκτημα της δρομολόγησης από την πηγή. Έτσι, οι ενδιάμεσοι κόμβοι δεν χρειάζεται να διατηρούν ενημερωμένες πληροφορίες για τις διαδρομές έτσι ώστε να δρομολογούν τα πακέτα που προωθούν.
- Η μάθηση των διαδρομών γίνεται με τον έλεγχο της πληροφορίας που περιέχεται στα πακέτα που λαμβάνει κάθε κόμβος. Αυτή η μορφή ενεργούς μάθησης είναι πολύ χρήσιμη, αφού μειώνει το πρόσθετο κόστος του δικτύου.
- Παρέχει υποστήριξη για αμφίδρομες συνδέσεις, με τη χρήση νέων αιτήσεων διαδρομής από τον τελικό προς τον αρχικό κόμβο.
- Δεν απαιτεί τη χρήση συμμετρικών συνδέσεων και μπορεί να χρησιμοποιήσει μη-συμμετρικές συνδέσεις όταν δεν είναι διαθέσιμες συμμετρικές.
- Επιτρέπει στους κόμβους να διατηρούν πολλαπλές διαδρομές για έναν προορισμό στην κρυφή τους μνήμη. Έτσι, όταν σπάσει μια σύνδεση σε μια διαδρομή , η πηγή μπορεί να ελέγξει την κρυφή της μνήμη για μια άλλη έγκυρη διαδρομή.
- Είναι loop-free πρωτόκολλο.
- Το πρωτόκολλο είναι κατανεμημένο, αφού δεν εξαρτάται από κάποιον κεντρικοποιημένο κόμβο.

Μειονεκτήματα:

- Κάθε πακέτο στον DSR έχει ένα μικρό πρόσθετο κόστος, αφού πρέπει να περιέχει τη διαδρομή μέχρι τον αρχικό κόμβο που έστειλε το πακέτο. Το πρόσθετο αυτό κόστος αυξάνεται όταν το πακέτο πρέπει να περάσει από πολλά hops μέχρι να φτάσει στον προορισμό του.
- Τα πακέτα απάντησης διαδρομής είναι επίσης μεγαλύτερα (σε σχέση με τον AODV), αφού περιέχουν τη διεύθυνση κάθε κόμβου κατά μήκος της διαδρομής, με αποτέλεσμα να παράγεται μεγαλύτερο overhead ελέγχου.
- Το overhead μνήμης είναι μεγαλύτερο στον DSR (σε σχέση με τον AODV), αφού κάθε κόμβος πρέπει να θυμάται ολόκληρες διαδρομές.
- Λόγω της υπόθεσης που έγινε, ότι η διάμετρος του δικτύου είναι σχετικά μικρή και της απαίτησης της δρομολόγησης από την πηγή, ο DSR δεν κλιμακώνεται σε μεγάλα δίκτυα.
- Αν προκύψει μια αποτυχία σύνδεσης κατά μήκος ενός μονοπατιού, ο αλγόριθμος ανακάλυψης διαδρομής πρέπει να ξανακληθεί από την πηγή για να βρεθεί ένα νέο μονοπάτι για τον προορισμό . Δε γίνεται καμιά προσπάθεια να χρησιμοποιηθεί τμηματική ανάκτηση διαδρομής, δηλαδή να επιτραπεί στους ενδιάμεσους κόμβους να προσπαθήσουν να ξαναφτιάξουν μόνοι τους τη διαδρομή. Αυτό μπορεί να οδηγήσει σε μεγαλύτερους χρόνους ανακατασκευής διαδρομής.

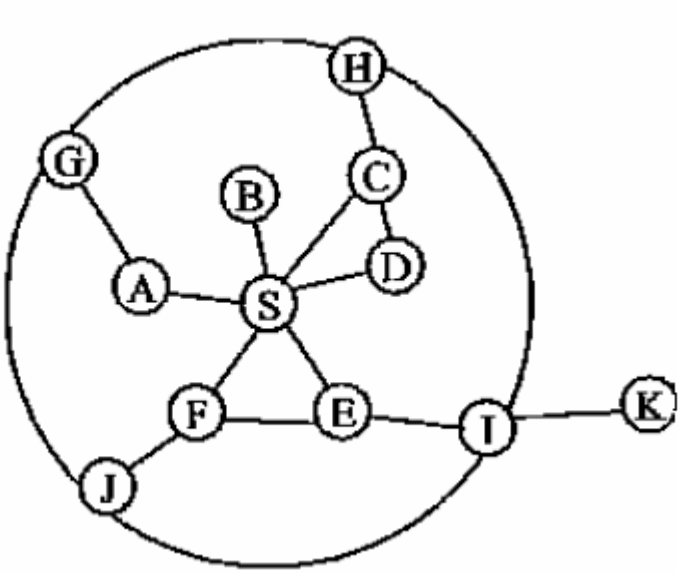
➢ Όμως η προσπάθεια και η αποτυχία ενός ενδιάμεσου κόμβου να ξαναφτιάξει μια διαδρομή, θα προκαλέσει μεγαλύτερη καθυστέρηση από ότι αν ο κόμβος-πηγή είχε προσπαθήσει να την ξαναφτιάξει αμέσως μόλις αντιλήφθηκε τη σπασμένη σύνδεση.

5.2.5 Υβριδικά πρωτόκολλα δρομολόγησης

1) Πρωτόκολλο δρομολόγησης ζώνης (Zone Routing Protocol-ZRP)

Το **ZRP** είναι ένα **υβριδικό πρωτόκολλο δρομολόγησης**, με χαρακτηριστικά reactive και proactive πρωτοκόλλου. Όπως υποδηλώνει και το όνομά του, το πρωτόκολλο αυτό βασίζεται στην έννοια των ζωνών. Συγκεκριμένα, διαιρεί το δίκτυο σε πολλές ζώνες δρομολόγησης και χρησιμοποιεί δύο εντελώς διαφορετικά πρωτόκολλα που λειτουργούν εντός και μεταξύ των ζωνών αυτών.

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.



Εικόνα 27. Παράδειγμα μιας ζώνης δρομολόγησης 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 παραπάνω σχήμα, 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 proactive συστατικό δρομολόγησης του ZRP αναφέρεται σαν το IntrA-zone Routing Protocol (IARP). Το IARP λειτουργεί εντός της ζώνης δρομολόγησης και διατηρεί πληροφορίες δρομολόγησης, όπως είναι η ελάχιστη απόσταση καθώς και η διαδρομή προς κάθε κόμβο εντός της ζώνης, για τους κόμβους που βρίσκονται

εντός της κάθε ζώνης. Το πρωτόκολλο αυτό δεν καθορίζεται ρητά και μπορεί να είναι οποιοδήποτε proactive, Distance-Vector ή Link-State πρωτόκολλο. Διαφορετικές ζώνες δρομολόγησης μπορούν να λειτουργούν και με διαφορετικά πρωτόκολλα εντός της κάθε ζώνης, αρκεί τα πρωτόκολλα αυτά να περιορίζονται στους εντός της ζώνης κόμβους. Μια αλλαγή στην τοπολογία έχει ως αποτέλεσμα οι πληροφορίες ενημέρωσης να διαδίδονται μόνο μέσα στις επηρεαζόμενες ζώνες, αντί να επηρεάζεται ολόκληρο το δίκτυο.

Το σφαιρικό reactive συστατικό δρομολόγησης ονομάζεται IntEr-zone Routing Protocol (IERP). Το IERP ανήκει σε μια οικογένεια reactive πρωτοκόλλων δρομολόγησης και χρησιμοποιείται για την εύρεση διαδρομών μεταξύ διαφορετικών ζωνών και την παροχή υπηρεσιών διατήρησης διαδρομών, βασισμένο στην τοπική συνδετικότητα που παρατηρείται από το IARP. Αυτό είναι απαραίτητο αν ο αποστολέας και ο παραλήπτης δε βρίσκονται εντός της ίδιας ζώνης δρομολόγησης. Το IERP χρησιμοποιεί το πρωτόκολλο Bordercast Resolution Protocol (BRP), το οποίο περιλαμβάνεται στο ZRP .Το BRP παρέχει υπηρεσίες bordercast packet delivery (μετάδοση πακέτων στους συνοριακούς κόμβους). Το bordercasting χρησιμοποιεί τις τοπολογικές πληροφορίες που παρέχονται από το IARP για να κατευθύνει τις αιτήσεις διαδρομής στους συνοριακούς κόμβους της ζώνης.

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.

Εφόσον οι ζώνες δρομολόγησης γειτονικών κόμβων επικαλύπτονται, κάθε κόμβος μπορεί να προωθήσει αιτήσεις διαδρομής περισσότερες από μία φορές, το οποίο έχει ως αποτέλεσμα περισσότερη κίνηση από ότι στο flooding. Όταν ένας κόμβος στέλνει μια αίτηση τους συνοριακούς του κόμβους, ολόκληρη η ζώνη δρομολόγησης καλύπτεται αποτελεσματικά. Οποιαδήποτε άλλα μηνύματα αίτησης εισέρχονται εντός της ζώνης είναι πλεονάζοντα και έχουν ως αποτέλεσμα τη σπατάλη χωρητικότητας μετάδοσης. Η υπερβολική κίνηση είναι αποτέλεσμα των αιτήσεων που επιστρέφουν σε "καλυμμένες" ζώνες. Για να λύσει το πρόβλημα αυτό ο ZRP χρειάζεται μηχανισμούς ελέγχου των αιτήσεων (query-control mechanisms), οι οποίοι μπορούν να κατευθύνουν τις αιτήσεις μακριά από "καλυμμένες" ζώνες και να σταματούν πακέτα αιτήσεων πριν αυτά παραδοθούν σε περιφερειακούς κόμβους που βρίσκονται σε περιοχές του δικτύου που έχουν ήδη καλυφθεί από την αίτηση. Ο ZRP χρησιμοποιεί τρεις τέτοιους μηχανισμούς: την

ανίχνευση αίτησης, τον πρόωρο τερματισμό (early termination) και την τυχαία καθυστέρηση προώθησης αίτησης.

Για τον εντοπισμό νέων γειτονικών κόμβων και αποτυχιών συνδέσεων, ο ZRP βασίζεται στο Neighbor Discovery Protocol (NDP), το οποίο παρέχεται από το Media Access Control (MAC) επίπεδο. Το NDP μεταδίδει "Hello" μηνύματα ("φάρους") σε τακτικά διαστήματα. Όταν λαμβάνεται ένας "φάρος" από ένα κόμβο, ο πίνακας Γειτόνων του ενημερώνεται. Οι γείτονες, για τους οποίους δεν έχει ληφθεί κάποιος "φάρος" μέσα σε ένα καθορισμένο χρονικό διάστημα, αφαιρούνται από τον πίνακα. Αν το MAC επίπεδο δεν περιλαμβάνει το NDP, η λειτουργικότητα θα πρέπει να παρέχεται από το IARP.

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. Οι αποτυχίες συνδέσεων καθώς και ημιβέλτιστα τμήματα διαδρομής εντός μιας ζώνης μπορούν να παρακαμφθούν. 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.

Πλεονεκτήματα:

- Διαφορετικές ζώνες δρομολόγησης μπορούν να λειτουργούν και με διαφορετικά πρωτόκολλα.
- Μια αλλαγή στην τοπολογία του δικτύου έχει ως αποτέλεσμα να διαδοθούν πληροφορίες ενημέρωσης μόνο εντός των επηρεαζόμενων ζωνών, αντί να επηρεάζεται ολόκληρο το δίκτυο.
- Το πρωτόκολλο προσαρμόζει τη λειτουργία του στις τρέχουσες συνθήκες λειτουργίας του δικτύου (μπορεί για παράδειγμα να αλλάξει τη διάμετρο της ζώνης δρομολόγησης) και στη συμπεριφορά των χρηστών.
- Εφόσον είναι συνδυασμός προδραστικών και μεταδραστικών πρωτοκόλλων, εκμεταλλεύεται πλεονεκτήματα και από τα δύο σχήματα. Οι διαδρομές είναι αμέσως διαθέσιμες εντός της ζώνης δρομολόγησης, ενώ για διαδρομές για προορισμούς εκτός της ζώνης, ο ZRP χρησιμοποιεί μια διαδικασία ανακάλυψης διαδρομής, η οποία μπορεί να επωφεληθεί από τις τοπικές πληροφορίες δρομολόγησης που διατηρούνται στις ζώνες.
- Η χρήση των μηχανισμών ελέγχου των αιτήσεων, έχει ως αποτέλεσμα τη μείωση του μεγέθους της κίνησης που παράγεται στη διαδικασία ανακάλυψης διαδρομής, αφού οι αιτήσεις διαδρομής κατευθύνονται μακριά από περιοχές του δικτύου που έχουν ήδη καλυφθεί.
- Μειώνεται το ποσό των πληροφοριών δρομολόγησης που δεν χρησιμοποιείται ποτέ, αφού οι κόμβοι διατηρούν τοπικές πληροφορίες δρομολόγησης που αφορούν μόνο τη ζώνη τους.
- Αντί για broadcasting χρησιμοποιείται η έννοια του bordercasting.
- Η απάντηση διαδρομής μπορεί να σταλεί από οποιονδήποτε κόμβο, ο οποίος μπορεί να παρέχει μια διαδρομή για τον προορισμό.
- Οι τοπολογικές πληροφορίες μπορούν να χρησιμοποιηθούν για να μικρύνουν οι διαδρομές.
- Αποτυχίες συνδέσεων και ημιβέλτιστα τμήματα διαδρομής μέσα σε μια ζώνη μπορούν να παρακαμφθούν.
- Ο ZRP παρέχει τοπική υποστήριξη για μονόδρομες συνδέσεις.
- Αναγνωρίζει πολλαπλές, loop-free διαδρομές για τον προορισμό, αυξάνοντας την αξιοπιστία και την απόδοση.

- Η δρομολόγηση είναι επίπεδη (flat) (αφού οι ζώνες επικαλύπτονται) και όχι ιεραρχική, μειώνοντας έτσι το overhead οργάνωσης, επιτρέποντας την ανακάλυψη βέλτιστων διαδρομών και μειώνοντας την απειλή της συμφόρησης του δικτύου.
- Όπως φαίνεται από όλα τα παραπάνω, ο ZRP αποτελεί μια πολύ καλή λύση για πολύ μεγάλα δίκτυα.

Μειονεκτήματα:

- Η επιλογή της ακτίνας είναι ένα trade-off μεταξύ της αποδοτικότητας της προδραστικής δρομολόγησης και της αυξανόμενης κίνησης για τη διατήρηση της εικόνας της ζώνης.
- Χωρίς τη χρήση των μηχανισμών ελέγχου των αιτήσεων, το πρωτόκολλο έχει ως αποτέλεσμα τη δημιουργία πολύ μεγαλύτερης κίνησης από ότι το flooding.
- Οι διαδικασίες διόρθωσης των διαδρομών που χρησιμοποιούνται τείνουν να μειώσουν τη βελτιστότητα των μονοπατιών (π.χ. μπορούν να αυξήσουν το μήκος κάποιου μονοπατιού). Έτσι, μετά από κάποιο αριθμό διορθώσεων, τα άκρα του μονοπατιού ξεκινούν μια νέα διαδικασία ανακάλυψης διαδρομής για να αντικαταστήσουν το μονοπάτι με ένα νέο βέλτιστο.
- Δεν καθορίζεται το proactive πρωτόκολλο δρομολόγησης που θα χρησιμοποιηθεί εντός των ζωνών δρομολόγησης. Η χρήση διαφορετικών πρωτοκόλλων στο εσωτερικό της κάθε ζώνης, μπορεί να σημαίνει ότι οι κόμβοι θα πρέπει να υποστηρίζουν διάφορα πρωτόκολλα. Αυτό δεν είναι επιθυμητό όταν οι χρήστες έχουν περιορισμένους πόρους και ιδιαίτερα μνήμη. Ίσως να είναι καλύτερα να χρησιμοποιείται το ίδιο πρωτόκολλο για την εντός της ζώνης επικοινωνία σε ολόκληρο το δίκτυο.

5.3 Πρωτόκολλα δρομολόγησης για δίκτυα αισθητήρων

Τα δίκτυα αισθητήρων (sensor networks) έχουν πολλές ομοιότητες με τα δίκτυα ad-hoc, αλλά παράλληλα έχουν και πολλές διαφορές. Όσον αφορά τη δρομολόγηση, ιδιαίτερη σημασία έχει το γεγονός ότι η τυπική επικοινωνία αφορά ένα σύνολο κόμβων που μεταδίδουν προς ένα συγκεκριμένο σταθμό και όχι επικοινωνία μεταξύ δύο κόμβων, όπως συνήθως συμβαίνει. Επίσης, καθώς τα δεδομένα που συλλέγονται από πολλούς αισθητήρες βασίζονται στα ίδια φαινόμενα, υπάρχει πιθανότητα επανάληψης των ίδιων δεδομένων.

Ακόμα, σε σύγκριση με τα ad-hoc, οι κόμβοι των δικτύων αισθητήρων δεν κινούνται τόσο συχνά (παρόλο που τα φαινόμενα που παρατηρούν μπορεί να κινούνται). Τέλος, όμοια με τη μελέτη των πρωτοκόλλων πολλαπλής πρόσβασης, και στους μηχανισμούς δρομολόγησης σημαντικό κριτήριο ποιότητας είναι η περιορισμένη κατανάλωση ισχύος. Γι' αυτούς, και για αρκετούς ακόμα λιγότερο σημαντικούς λόγους, οι μηχανισμοί δρομολόγησης των ad hoc δικτύων δε βρίσκουν εφαρμογή στα δίκτυα αισθητήρων και απαιτείται ο σχεδιασμός νέων, με βάση τις ιδιαίτερες απαιτήσεις τους.

5.3.1 Απαιτούμενα χαρακτηριστικά των πρωτοκόλλων δρομολόγησης

Ένα πρωτόκολλο δρομολόγησης το οποίο προορίζεται για χρήση σε δίκτυα ασύρματων αισθητήρων θα πρέπει να πρέπει να ικανοποιεί όσο το δυνατόν περισσότερα από τα παρακάτω χαρακτηριστικά:

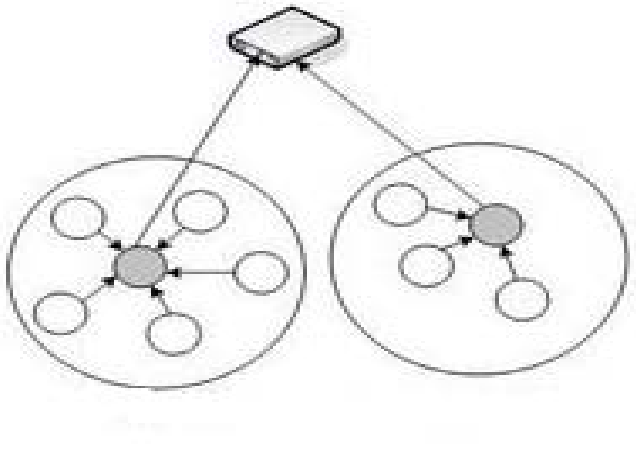
- **Χαμηλή υπολογιστική πολυπλοκότητα**
- **Μικρές απαιτήσεις σε χώρο αποθήκευσης**
- **Μικρές απαιτήσεις σε ανταλλαγή μηνυμάτων**
- **Δικαιοσύνη στην χρήση των διαδρομών**
- **Αποφυγή κυκλικών διαδρομών**
- **Ταχεία ανταπόκριση σε αλλαγές στην τοπολογία ή την συνδεσιμότητα**
- **Υπολογισμός πολλαπλών διαδρομών**
- **Υποστήριξη απαιτήσεων παροχής υπηρεσιών με χαρακτηριστικά QoS (Quality of Service support)**

5.3.2 Ιεραρχικά Πρωτόκολλα Δρομολόγησης με την Υλοποίηση Ομάδων Κόμβων

Αντιπροσωπευτικό πρωτόκολλο αυτής της κατηγορίας είναι το **LEACH (Low Energy Adaptive Clustering Hierarchy)**, το οποίο είναι ένα από τα πιο διάσημα ιεραρχικά πρωτόκολλα δρομολόγησης για δίκτυα αισθητήρων.

Η λειτουργία του βασίζεται στην δημιουργία **ομάδων (clusters) κόμβων**, που βασίζονται στην ένταση του λαμβανόμενου σήματος και στην χρήση των επικεφαλής των ομάδων σαν δρομολογητών μεταξύ των κόμβων και του σταθμού βάσης. Με αυτόν τον τρόπο γίνεται εξοικονόμηση ενέργειας, μιας και εκπομπή δεδομένων προς τον σταθμό βάσης γίνεται μόνο από τους επικεφαλής κόμβους (cluster heads) και όχι από όλους τους κόμβους. Ο βέλτιστος (optimal) αριθμός των επικεφαλής κόμβων είναι το 5% των συνολικών κόμβων. Η επεξεργασία των δεδομένων γίνεται στους κόμβους επικεφαλής των ομάδων. Η λειτουργία του πρωτοκόλλου έχει 2 φάσεις:

α) τη φάση εγκατάστασης και
β) τη φάση κανονικής λειτουργίας.



Εικόνα 28. Αρχιτεκτονική του LEACH

5.3.3 Ιεραρχικά Πρωτόκολλα Δρομολόγησης με την Υλοποίηση Δικτύου Κορμού

Αντιπροσωπευτικό πρωτόκολλο αυτής της κατηγορίας είναι το **Self Organizing ProtocoI.** Το πρωτόκολλο αυτό υποστηρίζει μια διαφορετική μεθοδολογία για την επίτευξη της συνδεσιμότητας του δικτύου, χωρίζοντας τους κόμβους σε δύο κατηγορίες στους **δρομολογητές (gateways)** οι οποίοι σχηματίζουν το δίκτυο κορμού (backbone) για την επικοινωνία, και στους **κοινούς**, οι οποίοι είναι κόμβοι που επικοινωνούν με τον σταθμό βάσης διαμέσου ενός και μόνο ενός δρομολογητή.

Η επιλογή του ποιος κόμβος αντιστοιχεί σε ποιον δρομολογητή γίνεται με βάση την προκαθορισμένη ισχύ εκπομπής κάθε κόμβου. Στην περίπτωση που σε αυτή την προκαθορισμένη ακτίνα εκπομπής βρίσκονται δύο δρομολογητές, επιλέγεται εκείνος ο οποίος βρίσκεται εγγύτερα του κόμβου. Επιπλέον, το πρωτόκολλο παρέχει την δυνατότητα υλοποίησης ενός σχήματος διευθυνσιοδότησης, έτσι κάθε κόμβος είναι αναγνωρίσιμος μέσω της διεύθυνσης του δρομολογητή με τον οποίο είναι συνδεδεμένος.

5.3.4 Πρωτόκολλα δρομολόγησης βασισμένα στην Έμμεση Γνώση της θέσης των κόμβων ενός δικτύου

Το κυριότερο πρωτόκολλο αυτής της κατηγορίας είναι το **Geographical Adaptive Fidelity - GAF.** Το GAF είναι ένα πρωτόκολλο δρομολόγησης που λαμβάνει υπόψη την καταναλισκόμενη ενέργεια και τη θέση που βρίσκεται ο κόμβος. Το πρωτόκολλο αρχικά σχεδιάστηκε για κινητά ad-hoc δίκτυα, αλλά μπορεί να εφαρμοστεί και σε δίκτυα αισθητήρων. Το GAF ελαχιστοποιεί την κατανάλωση ενέργειας θέτοντας εκτός λειτουργίας τους μη αναγκαίους κόμβους του δικτύου, χωρίς όμως να επηρεάζει τα επιθυμητά ποιοτικά χαρακτηριστικά της δρομολόγησης.

Η λειτουργία του έχει ως εξής:

Αρχικά δημιουργεί ένα εικονικό πλέγμα της καλυπτόμενης περιοχής. Οι κόμβοι που ανήκουν στο ίδιο σημείο στο πλέγμα θεωρούνται ισοδύναμοι, θεωρώντας ως μέτρο την καταναλισκόμενη ενέργεια για την δρομολόγηση ενός πακέτου. Έτσι με την παραδοχή αυτή είναι εφικτό, ένας μόνο κόμβος από όλους να μένει ενεργός σε κάθε σημείο του πλέγματος, ενώ όλοι οι υπόλοιποι να θέτουν εκτός λειτουργίας (**κατάσταση ύπνου**), τουλάχιστον το υποσύστημα μετάδοσης δεδομένων τους. Οι κόμβοι στο πρωτόκολλο GAF αλλάζουν την κατάσταση τους από μη ενεργοί (sleeping) σε ενεργούς (active) με δυναμικό τρόπο, έτσι ώστε η ενέργεια που απομένει σε καθένα κόμβο να είναι ισορροπημένη.

Τρεις είναι σύμφωνα με το πρωτόκολλο οι καταστάσεις που μπορούν να βρίσκονται οι κόμβοι:

- **Ανακάλυψης (discovery):** όπου κάθε κόμβος εντοπίζει τους γείτονες που βρίσκονται στο πλέγμα
- **Ενεργή (active):** όπου ο κόμβος μπορεί να στέλνει δικά του δεδομένα ή χρησιμοποιείται για την δρομολόγηση δεδομένων άλλων κόμβων
- **Μη ενεργή (sleep):** όπου το υποσύστημα επικοινωνίας του είναι εκτός λειτουργίας.

Το GAF αγωνίζεται προκειμένου να κρατήσει το δίκτυο συνδεδεμένο, τηρώντας ένα αντιπροσωπευτικό κόμβο σε ενεργή κατάσταση για κάθε περιοχή μέσα στο πλέγμα. Παρόλο που είναι πρωτόκολλο που βασίζεται στη θέση των αισθητήρων (Iocation-based protocol), μπορεί επίσης να θεωρηθεί και σαν ιεραρχικό πρωτόκολλο όπου η δημιουργία, των ομάδων (clusters) βασίζεται στην γεωγραφική θέση. Σε κάθε περιοχή ο αντιπροσωπευτικός κόμβος λειτουργεί σαν αρχηγός της ομάδας που εκπέμπει τα δεδομένα στους άλλους κόμβους. Η διαφορά

είναι ότι στο GAF ο κόμβος αυτός δεν εκτελεί οποιαδήποτε επεξεργασία επί των δεδομένων, όπως στην περίπτωση των άλλων ιεραρχικών πρωτοκόλλων, η μοναδική του εργασία είναι η προώθηση των δεδομένων προς τον σταθμό βάσης.

5.3.5 Πρωτόκολλα δρομολόγησης βασισμένα στην ροή του δικτύου και στην ποιότητα της υπηρεσίας

Το **Sequential Assignment Routing – SAR**, είναι το πρώτο πρωτόκολλο για δίκτυα αισθητήρων το οποίο περιλαμβάνει την έννοια της **ποιότητας υπηρεσίας (QoS)** στις αποφάσεις της δρομολόγησης. Το πρωτόκολλο αυτό δημιουργεί πολλά δέντρα των οποίων οι ρίζες είναι οι άμεσοι προς τον σταθμό βάσης γειτονικοί κόμβοι. Το κάθε δέντρο επεκτείνεται μακριά από τον σταθμό βάσης, αποφεύγοντας να συμπεριλάβει σε αυτό κόμβους με πολύ χαμηλή ποιότητα υπηρεσίας (QoS) ή μικρή απομένουσα ενέργεια. Στο τέλος αυτής της διαδικασίας οι περισσότεροι κόμβοι ανήκουν σε πολλαπλά δέντρα, επιτρέποντας στον κόμβο να επιλέγει το καταλληλότερο δέντρο προκειμένου να αναμεταδώσει προς τον σταθμό βάσης.

Σε κάθε μονοπάτι υπάρχουν δύο παράμετροι, που χρησιμοποιούν οι κόμβοι προκείμενου να επιλέξουν το καταλληλότερο μονοπάτι:

- **Η απομένουσα ενέργεια**, που υπολογίζεται από τον αριθμό των πακέτων που μπορεί να στείλει ένας κόμβος σε μια διαδρομή αν έχει αποκλειστική χρήση
- **Η ποιότητα της υπηρεσίας (QoS)**.

Οι κόμβοι επιλέγουν το καταλληλότερη διαδρομή βασιζόμενοι στις δύο παραπάνω παραμέτρους καθώς και στον βαθμό προτεραιότητάς του πακέτου.

Κεφάλαιο 6
Πρωτόκολλα Επικοινωνίας

6.1 Το IEEE 802.11 Πρωτόκολλο Επικοινωνίας

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 .

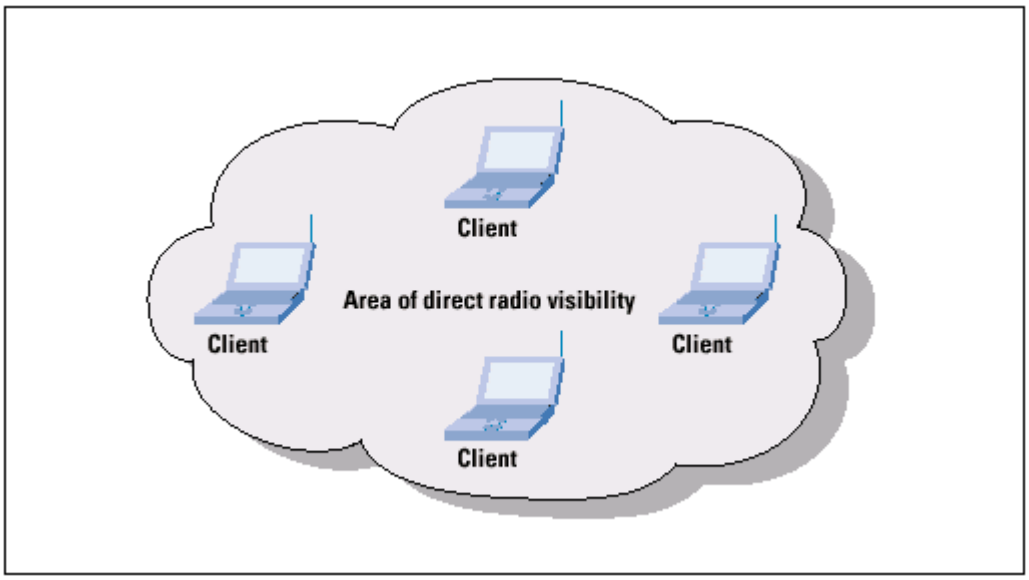
Το 802.11 υποστηρίζει τόσο την **δισημειακή (point to point) επικοινωνία**, όσο και την **επικοινωνία σημείου προς πολλαπλά σημεία (point to multipoint).** Έτσι οι υπολογιστές που βρίσκονται στον ίδιο χώρο μπορούν να οργανωθούν σε κατάσταση ad hoc με στόχο την άμεση επικοινωνία τους. Η ανάγκη για ασύρματο 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.

Εικόνα 29. Ασύρματες κάρτες δικτύου με διάφορες συνδεσμολογίες. (PCMCIA, PCI και USB από αριστερά προς τα δεξιά)

Το 802.11 ορίζει δύο στοιχεία εξοπλισμού: Έναν **ασύρματο σταθμό**, ο οποίος είναι συνήθως ένας προσωπικός υπολογιστής εφοδιασμένος με μία κάρτα δικτύου για ασύρματα δίκτυα (NIC) και έναν πομποδέκτη ή **σημείο πρόσβασης** (AP), που συμπεριφέρεται ως γέφυρα μεταξύ του ενσύρματου και του ασύρματου δικτύου. Το σημείο πρόσβασης ενεργεί ως σταθμός-βάση για το ασύρματο δίκτυο συγκεντρώνοντας τη δυνατότητα προσπέλασης του ενσύρματου δικτύου από πολλαπλούς ασύρματους σταθμούς. Οι ασύρματοι τερματικοί σταθμοί μπορεί να είναι δικτυακές κάρτες PCI, ISA βάσει του 802.11 ή συσκευές ενσωματωμένες σε άλλου είδους συστήματα.

Εικόνα 30. Access Point

Το πρότυπο 802.11 καθορίζει δύο τρόπους λειτουργίας:
1. **Λειτουργία υποδομής**. Εδώ το ασύρματο δίκτυο αποτελείται από ένα τουλάχιστον σημείο πρόσβασης που συνδέεται με το καλωδιωμένο δίκτυο και ένα σύνολο από ασύρματους σταθμούς. Αυτή η σχεδίαση ονομάζεται **βασικό Σύνολο Υπηρεσίας (BSS).** Ως επέκταση του BSS είναι το **Εκτεταμένο Σύνολο Υπηρεσίας (ESS)**, το οποίο αποτελεί σύνολο δύο ή περισσοτέρων BSS και σχηματίζει ένα μόνο υποδίκτυο.
2. **Ad-hoc λειτουργία**. Η συγκεκριμένη λειτουργία (λέγεται και peer-to-peer ή ανεξάρτητο βασικό σύνολο υπηρεσιών IBSS) αποτελείται από ένα σύνολο σταθμών 802.11 που επικοινωνούν μεταξύ τους κατευθείαν χωρίς την χρήση σημείων πρόσβασης ή οποιαδήποτε σύνδεση με το καλωδιωμένο δίκτυο (βλέπε το παρακάτω σχήμα). Η συγκεκριμένη μέθοδος είναι χρήσιμη για την γρήγορη και εύκολη εγκατάσταση ενός ασύρματου δικτύου σε σημεία όπου δεν υπάρχει καλωδιακή υποδομή (όπως σε ένα συνεδριακό κέντρο, σε αεροδρόμια ή οπού η πρόσβαση στο ενσύρματο δίκτυο δεν επιτρέπεται).



Εικόνα 31. IEEE 802.11 ad hoc Network

6.1.1 Πρότυπα που ανήκουν στην οικογένεια του IEEE 802.11

- **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 τεχνική **FHSS** ή **DSSS** σε ζώνες συχνοτήτων 915MHz, 2.4MHz, 5.2MHz ή υπέρυθρη μετάδοση στα 850nm ως 900nm. Υποστηρίζει δυνατότητες όπως κατανομή προτεραιοτήτων της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής.

- **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**
  Το 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 **2.4-2.483Ghz** 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 802.11c**
  Λειτουργία γεφύρωσης (bridging) πλαισίων 802.11

- **IEEE 802.11d**
  Επεκτάσεις στο πρότυπο ώστε να λειτουργεί σε επιπλέον ρυθμιστικά πλαίσια (άλλες ζώνες συχνοτήτων)

- **IEEE 802.11e**
  Υποστήριξη QoS στο MAC επίπεδο (EDCF, Enhanced DCF και HCF, Hybrid Coordination Function)

- **IEEE 802.11f**
  Συνιστώμενη πρακτική για το πρωτόκολλο IAPP, Inter Access Point Protocol

- **IEEE 802.11g**
  Το 802.11g είναι το τελευταίο πρότυπο ασύρματης δικτύωσης και το οποίο έχει επικυρωθεί μόλις πρόσφατα. 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. Παρόλα αυτά σε ένα καθαρά 802.11g δίκτυο μπορεί κάποιος να εκμεταλλευτεί πλήρως τις ικανότητες της τεχνολογίας. Επίσης, σαν σημείωση, μια εξωτερική κεραία που λειτουργεί σε 802.11b δίκτυο μπορεί να λειτουργήσει και σε 802.11g μειώνοντας έτσι το κόστος αναβάθμισης.

- **IEEE 802.11h**
  Διαχείρηση φάσματος στο 802.11a (DCS, Dynamic Channel Selection και TPC, Transmit Power Control)

- **IEEE 802.11i**
  Επεκτάσεις στο MAC επίπεδο για ενισχυμένη ασφάλεια

- **Νέες τεχνολογίες – 802.11n**
  Το νέο πρότυπο της ασύρματης τοπικής δικτύωση το οποίο αναπτύσσεται από τον οργανισμό IEEE ονομάζεται 802.11n και ακόμα βρίσκεται στο στάδιο του σχεδιασμού. Το νέο αυτό πρότυπο υπόσχεται σημαντικά γρηγορότερες ταχύτητες μετάδοσης. Κάποιοι ελπίζουν ότι θα είναι γρηγορότερο και από τα παραδοσιακά καλωδιακά δίκτυα Ethernet (10 mbps) και Fast Ethernet (100 mbps). Επιπλέον θα ενσωματώνει νέες τεχνολογίες οι οποίες θα του επιτρέπουν να συνυπάρχει με συσκευές οι οποίες λειτουργούν με τα προαναφερθέντα πρότυπα χωρίς να επηρεάζεται η λειτουργία του.

6.1.2 Χαρακτηριστικά του προτύπου IEEE 802.11

Η ζώνη των 2.4GHz γίνεται ολοένα και πιο δημοφιλής σήμερα. Ο λόγος γι' αυτό είναι ότι πρόκειται για ελεύθερη ζώνη και έχει κατάλληλα χαρακτηριστικά για μετάδοση σε μικρές αποστάσεις.

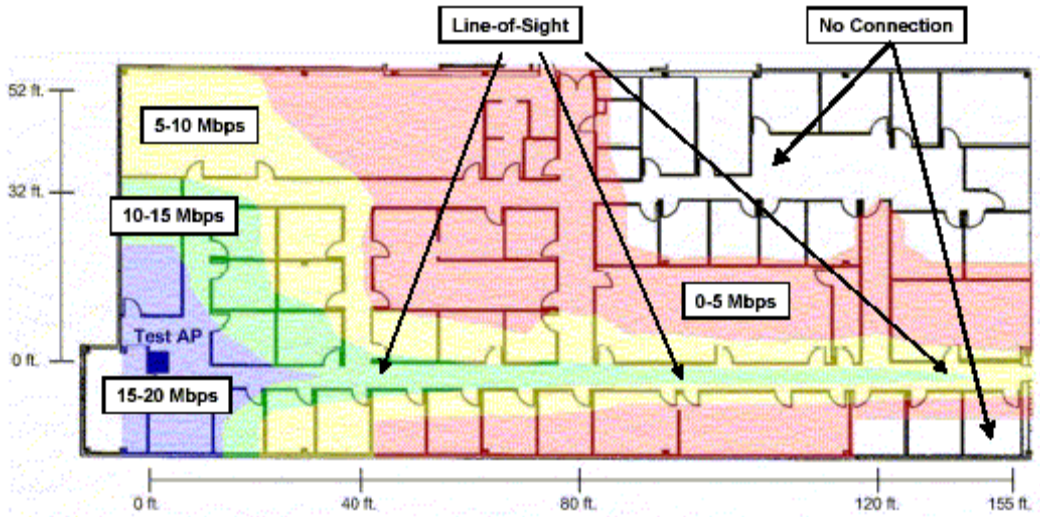
Παρεμβολές

Τα ασύρματο LAN μπορεί να δεχτεί και να προκαλέσει παρεμβολές σε άλλα 2.4GHz προϊόντα όπως μερικά ασύρματα τηλέφωνα ή φούρνοι μικροκυμάτων. Γενικά πάντως δεν έχει παρατηρηθεί να έχουν σημαντικό πρόβλημα με παρεμβολές από φούρνους μικροκυμάτων. Μπορεί επίσης να δεχθεί παρεμβολλές από αρμονικές από συσκευές που εκπέμπουν σε υποπολαπλάσια της συχνότητας λειτουργίας. Το σημαντικότερο πρόβλημα παρεμβολλών πάντως προκύπτει από την κακή σχεδίαση ενός ασύρματου ραδικτύου (μεγάλύτερες ισχείς εκπομπής από το αναγκαίο, κακές και ακατάλληλες καραίες, λάθος επιλογή συχνοτήτων και τοποθεσίας, συσκευές με μικρή ευαισθησία κ.τ.λ)

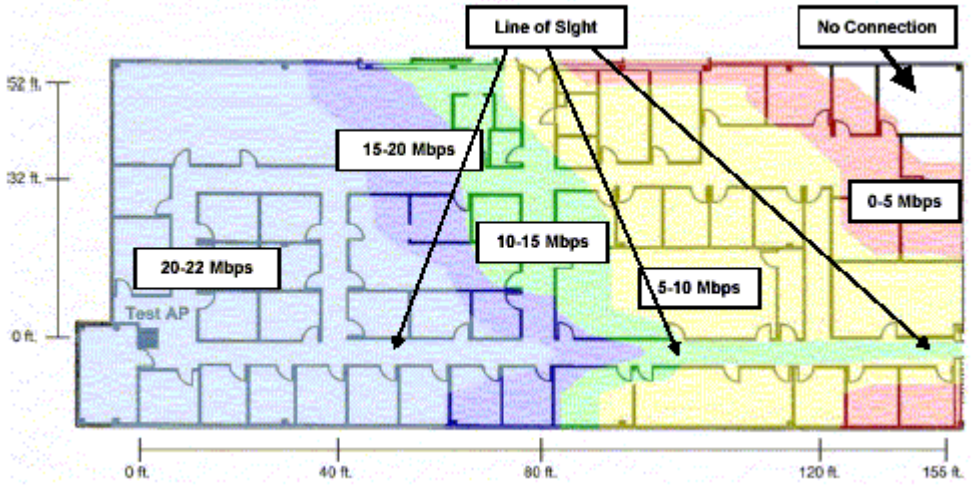
Εμβέλεια

Η εμβέλεια ενός ασύρματου δικτύου σε περιβάλλον γραφείου μπορεί να είναι μερικές δεκάδες μέτρα. Τα ραδιοκύματα σε εσωτερικό χώρο έχουν να διαπεράσουν τοίχους και οροφές οπότε υφίστανται σημαντικές απώλειες. Δηλαδή όταν ένα ραδιοκύμα προσπέσει σε ένα τοίχο ένα μέρος της ισχύος του θα αποροφηθεί από το υλικό του τοίχου και ένα κομμάτι μόνο θα μπορεί να τον διαδοθεί. Επίσης το σήμα θα ανακλαστεί στις περιβάλλουσες επιφάνειες με αποτέλεσμα στο δέκτη τελικά να φτάσουν ένας αριθμός από αντίγραφα του αρχικού σήματος, όλα με διαφορετικά πλάτη και φάσεις. Από την άθροιση τους μπορεί να προκύψει αλληλοαναίρεση και το τελικό σήμα να έχει πολύ μικρότερη ισχύ με αποτέλεσμα την υποβάθμιση της ποιότητας της ζεύξης.
Σε περιβάλλον όπου υπάρχει κατευθείαν οπτική επαφή, σε εξωτερικό χώρο, η εμβέλεια είναι πολύ μεγαλύτερη, εξαρτάται από την ισχύ εκπομπής, την ευαισθησία του δέκτη, τις κεραίες, την απόσταση, την ευθυγράμμιση των κεραιών, το επίπεδο παρεμβολών και θορύβου. Πάντως αποστάσεις αρκετών χιλιομέτρων είναι δυνατό να επιτευχθούν με πολύ καλή ποιότητα ζεύξης.

Στα παρακάτω σχήματα φαίνεται ενδεικτικά η εμβέλεια του κάθε πρωτοκόλλου, συναρτήσει του ρυθμού μετάδοσης. Η διαφορετική συμπεριφορά οφείλεται στη διαφορετική συχνότητα λειτουργίας των δύο προτύπων.



Εικόνα 32. 802.11a



Εικόνα 33. 802.11g

Ρυθμός μετάδοσης

Η πραγματική διαπερατότητα του συστήματος εξαρτάται από ένα πλήθος παραγόντων όπως οι παράμετροι ραδιομετάδοσης (εμβέλεια, ανακλάσεις, απορρόφηση, σκέδαση), όπως και από τον αριθμό των χρηστών. Για τις περισσότερες εφαρμογές το bandwidth είναι επαρκές.

Ποιότητα επικοινωνίας

Έχοντας πίσω τους μισό αιώνα σε εμπορικές και κυρίως σε στρατιωτικές εφαρμογές οι ασύρματες τεχνολογίες έχουν γίνει πολύ στιβαρές και αξιόπιστες. Έτσι μπορούν να περέχουν αξιόπιστες συνδέσεις και μάλιστα ίσως σε καλύτερο επίπεδο από ότι οι αντίστοιχες στην κινητή τηλεφωνία.

Συμβατότητα με το υπάρχον δίκτυο

Τα περισσότερα WLAN έχουν προτυποποιημένο τρόπο σύνδεσης με τα υπάρχοντα ενσύρματα δίκτυα. Συστήματα διαχείρησης επιβλέπουν τους ασύρματους κόμβους οποώς και οποιοδήποτε έλλο στοιχείο δικτύου.

Διαλειτουργικότητα

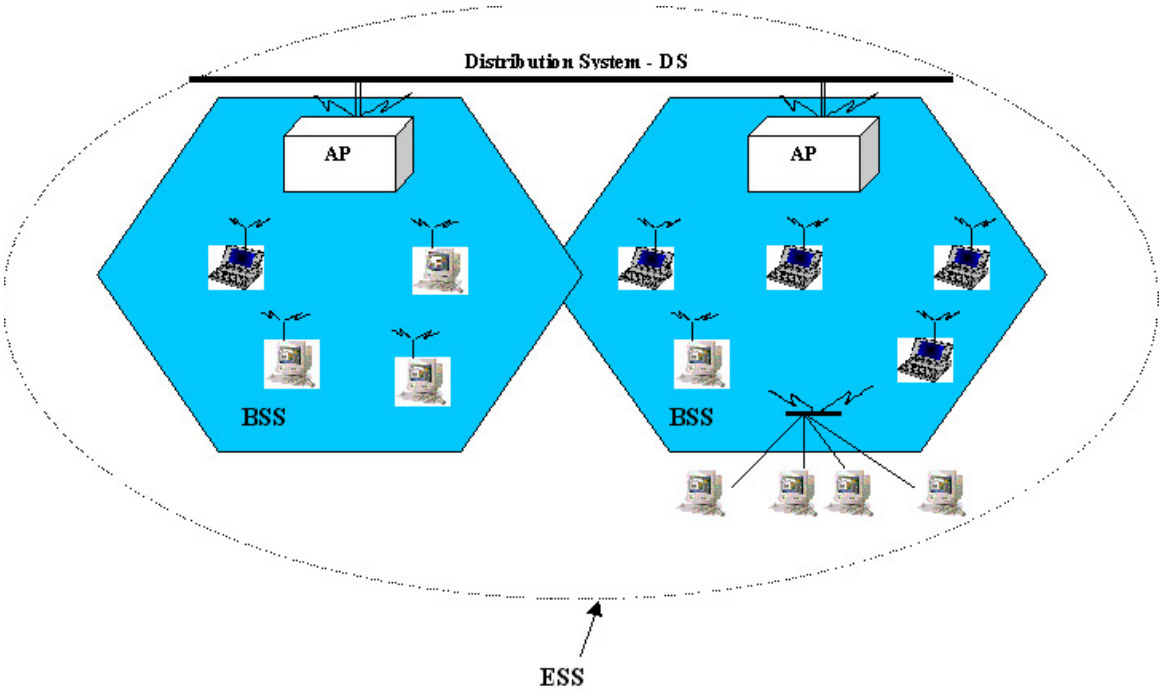
Υπαρχουν οι εξής περιπτώσεις στις οποίες οι συσκευές δεν συνεργάζονται μεταξύ τους:

- **Διαφορετικές τεχνολογίες.** Ένα ράδιο βασισμένο σε τεχνολογία FHSS δεν μπορεί να συνεργαστεί με κάποιο τεχνολογίας DSSS.
- **Διαφορετικές συχνότητες.** Προφανώς συσκευές 802.11a στους 5.7GHz δεν μπορουν να δουλέψουν μαζί με συσκευές 802.11b/g που εργάζονται στους 2.4GHz.
- **Διαφορετικές υλοποιήσεις.** Προϊόντα διαφορετικών κατασκευαστών μπορεί να μην συνεργάζονται ή να συνεργάζονται μερικώς μεταξύ τους. Για παράδειγμα υπάρχει ένας αριθμός προϊόντων βασισμένα σε chipsets της Texas Instruments τα οποία υποστηρίζουν ένα τρόπο μετάδοσης 22Mbps. Αυτός όμως ισχύει μόνο μεταξύ συσκευών της ίδιας εταιρίας. Για μία λύση του προβλήματος της διαλειτουργικότητας δημιουργήθηκε το Wifi πιστοποιητικό.

6.1.3 Αρχιτεκτονική του προτύπου IEEE 802.11

Ένα ασύρματο δίκτυο 802.11 βασίζεται σε μια **κυψελοειδή αρχιτεκτονική**, σύμφωνα με την οποία, ολόκληρο το σύστημα διαιρείται σε **περιοχές ή κελιά** με το κάθε κελί να ελέγχεται από ένα **Σταθμό - Βάσης (Base Station)**. Στην ορολογία του 802.11 ένα κελί ονομάζεται Βασικό Σύνολο Υπηρεσιών (Basic Service Set - BSS) και ο σταθμός βάσης, **Σημείο Πρόσβασης (Access Point - AP).** Παρόλο που ένα δίκτυο μπορεί να αποτελείται από ένα μόνο κελί, οι περισσότερες δικτυακές εγκαταστάσεις 802.11 συνήθως αποτελούνται από πολλά κελιά με τα σημεία πρόσβασης να βρίσκονται συνδεδεμένα σε μια ραχοκοκαλιά, η οποία ονομάζεται Σύστημα Διανομής (Distribution System - DS) και η οποία μπορεί να είναι είτε ένα ενσύρματο (π.χ.Ethernet), είτε ένα ασύρματο δίκτυο.

Το σύνολο όλων των δια-συνδεδεμένων ασύρματων δικτύων, μαζί με τα σημεία πρόσβασης και το σύστημα διανομής, ονομάζεται Εκτεταμένο Σύνολο Υπηρεσιών (Extended Service Set - ESS) και όσον αφορά τα ανώτερα επίπεδα του δικτυακού μοντέλου αναφοράς OSI, σύμφωνα με το πρότυπο, θα πρέπει να θεωρείται ως ένα ενιαίο τοπικό δίκτυο κατηγορίας 802. Στο παρακάτω σχήμα απεικονίζεται η αρχιτεκτονική ενός δικτύου 802.11.



Εικόνα 34. Η αρχιτεκτονική δικτύου κατά το πρότυπο IEEE 802.11

Το πρότυπο ορίζει επίσης και την έννοια της πύλης (Portal). Η πύλη είναι μια συσκευή που χρησιμοποιείται για τη δια-σύνδεση ενός δικτύου 802.11 με ένα άλλο δίκτυο κατηγορίας 802. Η λειτουργία της μπορεί να παρομοιαστεί με τη λειτουργία ενός δρομολογητή (router), ο οποίος είναι ικανός να δια-συνδέει διαφορετικά δίκτυα. Η λειτουργικότητα μιας πύλης μπορεί να βρίσκεται είτε σε ξεχωριστή συσκευή, είτε να είναι ενσωματωμένη με το σημείο πρόσβασης.

6.1.4 Τα επίπεδα του προτύπου IEEE 802.11

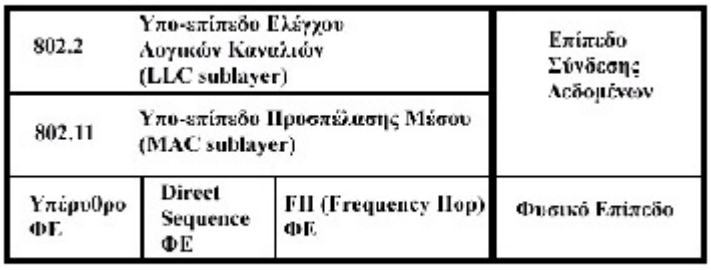
Το πρότυπο 802.11 περιορίζεται στα δύο πρώτα επίπεδα του δικτυακού μοντέλου αναφοράς OSI, ήτοι, στο φυσικό επίπεδο (ΦΕ) και στο επίπεδο σύνδεσης δεδομένων (ΕΣΔ). Για την ακρίβεια, δεν καλύπτει ολόκληρο το ΕΣΔ, αλλά το πρώτο μισό του, δηλαδή το υπο-επίπεδο πρόσβασης στο μέσο (MAC Layer).

6.1.4.1 Το φυσικό επίπεδο

Το πρότυπο 802.11 ορίζει τρία διαφορετικά φυσικά επίπεδα. Η ύπαρξη περισσότερων από μιας επιλογών για το φυσικό επίπεδο επιτρέπει στους σχεδιαστές συστημάτων να επιλέγουν κάθε φορά την τεχνολογία εκείνη, η οποία ταιριάζει καλύτερα με το κόστος, την απόδοση και το προφίλ των λειτουργιών μιας συγκεκριμένης εφαρμογής.

Ειδικότερα, το πρότυπο προσδιορίζει ένα οπτικό ΦΕ που χρησιμοποιεί υπέρυθρες ακτίνες για τη μετάδοση δεδομένων και δύο ΦΕ ραδιοσυχνότητας (RF-based), τα οποία λειτουργούν στην περιοχή συχνοτήτων των 2,4 GHz (από 2,4 - 2,4835 GHz) του ISM.

Στο παρακάτω σχήμα απεικονίζονται τα επίπεδα που καλύπτονται από το πρότυπο:



Εικόνα 35. επίπεδα του προτύπου IEEE 802.11

Οι δύο διαφορετικές τεχνολογίες ΦΕ ραδιοσυχνότητας που απεικονίζονται στο παραπάνω σχήμα, ανήκουν στην κατηγορία των τεχνικών **διασποράς φάσματος (spread spectrum techniques)** οι οποίες όμως δεν καλύπτονται εδώ. Αναφορικά μόνο, οι τεχνολογίες διασποράς φάσματος που προσδιορίζει το 802.11 για τα δύο ΦΕ ραδιοσυχνότητας είναι η τεχνική **διασποράς φάσματος άμεσης ακολουθίας (Direct Sequence Spread Spectrum - DSSS)** και η τεχνική **διασποράς φάσματος αναπήδησης συχνότητας (Frequency Hopping Spread Spectrum - FHSS)**.

Το μικρό εύρος κάλυψης που έχει το υπέρυθρο ΦΕ το καθιστά κατάλληλο μόνο για εφαρμογές κλειστού χώρου, όπως ένα μικρό γραφείο, ένα δωμάτιο, κλπ. Αντίθετα, οι άλλοι δύο τύποι ΦΕ μπορούν να χρησιμοποιηθούν σε εφαρμογές όπου υπάρχει η ανάγκη κάλυψης μεγάλων περιοχών (ανοικτών ή κλειστών), όπως είναι μια πανεπιστημιούπολη, τα κτίρια μιας επιχείρησης, κλπ.

Τέλος, το 802.11 προσδιορίζει ρυθμούς μετάδοσης δεδομένων της τάξεως των 1 και 2 Mbps για όλα τα ΦΕ (οπτικά και ραδιοσυχνότητας).

6.1.4.2 Το επίπεδο σύνδεσης δεδομένων

Σ' ένα δίκτυο 802.11, το υπο-επίπεδο προσπέλασης μέσου (MAC layer), είναι υπεύθυνο για την εκτέλεση των παρακάτω λειτουργιών:

- Τον έλεγχο της πρόσβασης των σταθμών στο κοινό μέσο μετάδοσης
- Τη λειτουργία του κατακερματισμού και της επανασυναρμολόγησης (fragmentation and reassembly)
- Τη λειτουργία της αναμετάδοσης πακέτου (packet retransmission)
- Τη λειτουργία της επιβεβαίωσης λήψης (acknowledges).

Έλεγχος της πρόσβασης στο κοινό μέσο

Η τεχνική που χρησιμοποιείται από το ΕΣΔ στο 802.11 είναι παρόμοια με μια από τις βασικότερες μεθόδους ελέγχου πρόσβασης στο μέσο, τη μέθοδο πολλαπλής πρόσβασης με ανίχνευση φέροντος σήματος και αποφυγή συγκρούσεων **(Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA).**

Σύμφωνα με τη μέθοδο αυτή, ένας σταθμός ο οποίος θέλει να μεταδώσει "αφουγκράζεται" πρώτα το μέσο μετάδοσης, για να διαπιστώσει εάν είναι κατειλημμένο. Εάν είναι, τότε δε μεταδίδει, περιμένει ένα τυχαίο χρονικό διάστημα και προσπαθεί ξανά. Εάν είναι ελεύθερο, τότε στέλνει πρώτα ένα ειδικό σήμα για να προειδοποιήσει ότι πρόκειται να μεταδώσει και στη συνέχεια, αν δε συμβεί καμιά σύγκρουση, στέλνει τα δεδομένα του. Με τον τρόπο αυτό οι υπολογιστές αντιλαμβάνονται πότε υπάρχει πιθανότητα σύγκρουσης, κάτι που τους επιτρέπει να αποφεύγουν τις συγκρούσεις μετάδοσης (εξού και η ονομασία της μεθόδου).

Ωστόσο, η αποστολή του ειδικού σήματος μετάδοσης, αυξάνει την κίνηση στο καλώδιο, υποβαθμίζοντας την επίδοση ολόκληρου του δικτύου.

Παρόλο που αυτοί οι μηχανισμοί είναι αρκετά αποδοτικοί στα παραδοσιακά ενσύρματα δίκτυα, αυτό δε θα μπορούσαμε να πούμε ότι ισχύει και στα ασύρματα δίκτυα, για τους παρακάτω λόγους:

- Η υλοποίηση ενός μηχανισμού ανίχνευσης συγκρούσεων θα απαιτούσε την υλοποίηση ενός αμφίδρομου πομποδέκτη, που θα μπορούσε να στέλνει και να λαμβάνει δεδομένα ταυτόχρονα, κάτι που θα αύξανε κατά πολύ το κόστος υλοποίησης.
- Σε ένα ασύρματο δίκτυο δε θα ήταν σωστό να υποθέσουμε ότι όλοι οι σταθμοί μπορούν να "ακούσουν" όλους τους υπόλοιπους, μια πολύ βασική υπόθεση στις μεθόδους πρόσβασης με ανίχνευση φέροντος. Ακόμη και αν κάποιος σταθμός που επιθυμεί να μεταδώσει και ανιχνεύσει το κανάλι ελεύθερο, αυτό δε σημαίνει απαραίτητα ότι αυτό είναι ελεύθερο γύρω από την περιοχή του δέκτη (αυτό το επιχείρημα αναλύεται αναλυτικότερα παρακάτω, στο τμήμα Δέσμευση του καναλιού).

Λόγω των παραπάνω προβλημάτων, το πρότυπο 802.11 χρησιμοποιεί μια μέθοδο **αποφυγής συγκρούσεων (Collision Avoidance mechanism)**, παράλληλα με ένα **σύστημα θετικής επιβεβαίωσης λήψης (Positive Acknowledgement Scheme)**, που περιγράφεται παρακάτω:

- **Ανίχνευση των Συγκρούσεων (collision detection)**

  Ένας σταθμός ο οποίος επιθυμεί να μεταδώσει, ελέγχει αρχικά το μέσο (τον αέρα στην περίπτωσή μας). Αν είναι κατειλημμένο, τότε αναβάλει τη μετάδοση για αργότερα. Αν είναι ελεύθερο, τότε περιμένει να δει αν θα παραμείνει ελεύθερο για ένα συγκεκριμένο χρονικό διάστημα, το οποίο ονομάζεται **DIFS (Distributed Inter Frame Space** - βλέπε παρακάτω) και στη συνέχεια μεταδίδει το πακέτο που περιέχει τα δεδομένα. Ο δέκτης από την άλλη, λαμβάνοντας το πακέτο ελέγχει να δει εάν αυτό περιέχει τυχόν λάθη και αν όχι τότε στέλνει πίσω στον πομπό μια επιβεβαίωση λήψης (Acknowledgement - ACK). Παραλαβή της επιβεβαίωσης λήψης από τον πομπό σημαίνει ότι το πακέτο παραδόθηκε στον προορισμό του χωρίς να συγκρουστεί με κάποιο άλλο. Αν ο αποστολέας δεν παραλάβει μια επιβεβαίωση, τότε θεωρεί ότι συνέβη μια σύγκρουση και επαναλαμβάνει τη μετάδοση του πακέτου, μέχρις ότου είτε λάβει την επιβεβαίωση, είτε ακυρώσει τη μετάδοση μετά από έναν αριθμό προσπαθειών.

- **Δέσμευση του καναλιού**

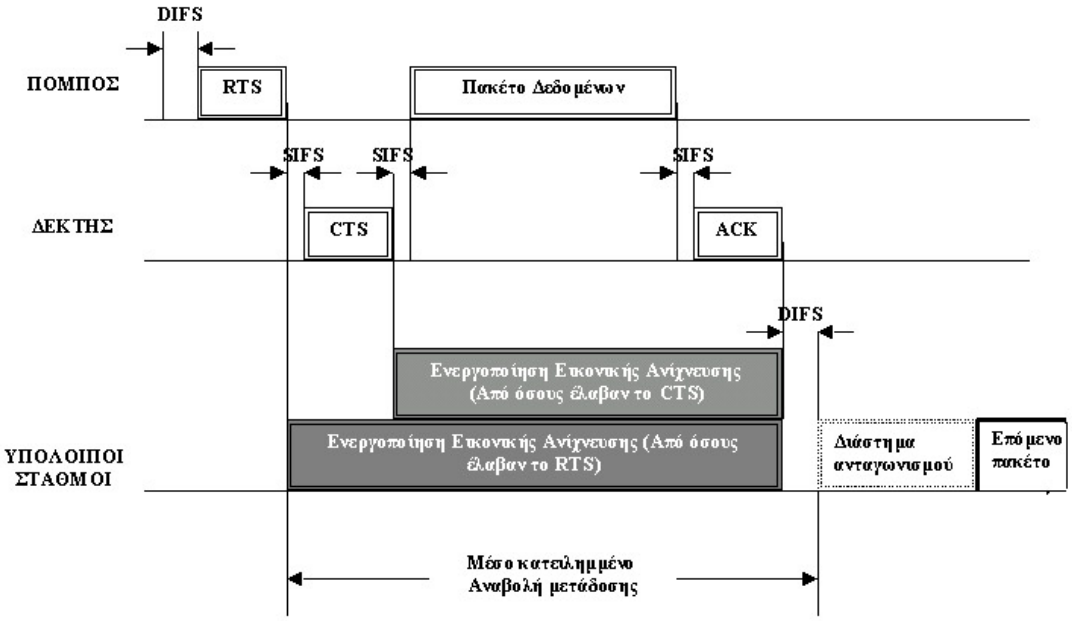
  Μέχρις αυτό το σημείο δε μιλήσαμε ακόμη για τον τρόπο με τον οποίο μπορεί ένας σταθμός να σιγουρευτεί ότι όντως το μέσο μετάδοσης είναι ελεύθερο προτού μεταδώσει. Το πρότυπο 802.11 προσδιορίζει ένα **μηχανισμό εικονικής ανίχνευσης φέροντος (virtual carrier sense mechanism)**, με τον οποίο εξασφαλίζεται ότι όλοι οι σταθμοί που μοιράζονται το ίδιο μέσο θα γνωρίζουν ότι κάποιος σταθμός μεταδίδει ακόμη και αν αυτοί είναι "κρυμμένοι". Για να κατανοήσουμε καλύτερα την παραπάνω έννοια, ας φανταστούμε την ακόλουθη περίπτωση. Θεωρείστε ότι έχουμε ένα ασύρματο δίκτυο που έχει μια αρχιτεκτονική παρόμοια με αυτή της εικόνας 34. Έστω ότι υπάρχουν τρεις σταθμοί στο κάθε κελί, ο Α, ο Β και ο Γ. Ο Α και ο Β έστω ότι αποτελούν απλούς σταθμούς, ενώ ο Γ αποτελεί ένα σημείο πρόσβασης (AP). Φανταστείτε το ακόλουθο σενάριο: ο Α μπορεί να επικοινωνήσει με τον Γ, ο Β μπορεί να επικοινωνήσει με τον Γ, αλλά ο Α δε μπορεί να επικοινωνήσει απευθείας με τον Β, γιατί απέχουν τέτοια απόσταση ο ένας από τον άλλο που δεν είναι δυνατή η άμεση επικοινωνία (το σήμα δε μπορεί να διαδοθεί από τον Α στον Β). Οπότε, αν σε μια δεδομένη χρονική στιγμή και ο Α και ο Β θέλουν να μεταδώσουν, θα ανιχνεύσουν και οι δύο το μέσο ελεύθερο, αφού ο ένας δε μπορεί να "ακούσει"

τον άλλο. Στη συγκεκριμένη περίπτωση θα υπάρξει σύγκρουση στην περιοχή του δέκτη, γιατί μπορεί ο Α να μη μπορεί να επικοινωνήσει με τον Β, αλλά και οι δύο είναι σε θέση να επικοινωνήσουν με το σημείο πρόσβασης, το Γ. Στην περίπτωση αυτή λέμε ότι ο σταθμός Β είναι "κρυμμένος" από το σταθμό Α και αντίστροφα.

Ο μηχανισμός εικονικής ανίχνευσης φέροντος λειτουργεί ως εξής: ένας σταθμός που επιθυμεί να μεταδώσει και έχει ανιχνεύσει το μέσο ελεύθερο (τουλάχιστον στην περιοχή γύρω από αυτόν), στέλνει πρώτα ένα μικρό πακέτο που ονομάζεται RTS **(Request To Send - Αίτηση για αποστολή)** και το οποίο περιέχει τη διεύθυνση αποστολής, τη διεύθυνση προορισμού και το χρονικό διάστημα της όλης διαδικασίας (το χρόνο δηλαδή που απαιτείται για την αποστολή του πακέτου δεδομένων και της λήψης της επιβεβαίωσης από το δέκτη). Στη συνέχεια, ο δέκτης ελέγχει εάν το μέσο είναι όντως ελεύθερο (και στη δική του περιοχή δηλαδή) και αν είναι, τότε αποστέλλει ένα άλλο πακέτο μικρού μεγέθους που ονομάζεται **CTS (Clear To Send - Αποστολή Δεκτή)** το οποίο περιέχει τις ίδιες πληροφορίες με το πακέτο RTS. Σε αντίθετη περίπτωση δεν αποστέλλει τίποτε.

Όλοι οι σταθμοί που λαμβάνουν το RTS ή / και το CTS, ενεργοποιούν έναν ειδικό δείκτη που ονομάζεται δείκτης εικονικής ανίχνευσης (virtual sense indicator), ο οποίος καλείται **NAV** - από το **Network Allocation Vector**. Η ενεργοποίηση διαρκεί για το χρονικό διάστημα που αναφέρεται στο CTS (ή το RTS) και χρησιμοποιείται παράλληλα με την φυσική ανίχνευση φέροντος από τους σταθμούς όταν αυτοί ανιχνεύουν το καλώδιο.

Η μέθοδος αυτή μειώνει κατά πολύ την πιθανότητα συγκρούσεων στην περιοχή του δέκτη, γιατί ακόμη και οι "κρυμμένοι" από τον πομπό σταθμοί (που δε μπορούν να λάβουν το RTS δηλαδή) θα λάβουν σίγουρα το πακέτο CTS και θα θεωρήσουν το μέσο κατειλημμένο για το χρονικό διάστημα που αναφέρεται σ' αυτό. Επίσης, η αποστολή του πακέτου RTS προφυλάσσει τον δέκτη από συγκρούσεις στην περιοχή του πομπού κατά τη διάρκεια αποστολής της επιβεβαίωσης λήψης (ACK), γιατί το RTS θα ληφθεί σίγουρα από όλους τους σταθμούς που είναι "κρυμμένοι" από το δέκτη. Στο παρακάτω σχήμα δίδεται ένα χρονοδιάγραμμα των ενεργειών που λαμβάνουν χώρα κατά τη διάρκεια της επικοινωνίας μεταξύ δύο σταθμών.



Εικόνα 36. Χρονοδιάγραμμα των ενεργειών που λαμβάνουν χώρα κατά την επικοινωνία δύο σταθμών

Στο παραπάνω σχήμα μπορούμε να διακρίνουμε και τα διάφορα χρονικά διαστήματα που μεσολαβούν πριν και μετά τις μεταδόσεις των πλαισίων. Οι χρόνοι αυτοί, κατά λέξη, ονομάζονται δια-πλαισιακά διαστήματα (Inter-Frame Spaces - IFS) και ανήκουν σε διάφορες κατηγορίες:

1. **<u>Short IFS - SIFS (Δια-πλαισιακό διάστημα μικρής διάρκειας):</u>**
Ο χρόνος αυτός χρησιμοποιείται για το διαχωρισμό των μεταδόσεων που ανήκουν σε ένα διάλογο μεταξύ δύο σταθμών (π.χ. πακέτο δεδομένων και ACK) και αποτελεί το μικρότερο από τους δια-πλαισιακούς χρόνους. Έχει σταθερή τιμή, η οποία διαφέρει ανά ΦΕ, και υπολογίζεται με τέτοιον τρόπο, ώστε ο πομπός να έχει αρκετό χρόνο να μεταβεί σε κατάσταση λήψης, για να μπορέσει να λάβει και να αποκωδικοποιήσει το εισερχόμενο πακέτο (π.χ. ACK ή CTS) από το δέκτη. Για παράδειγμα, για τα ΦΕ τεχνολογίας διασποράς φάσματος αναπήδησης συχνότητας, ο χρόνος αυτός ορίζεται στα 28 μsec.

2. **<u>Point Coordination IFS - PIFS (Δια-πλαισιακό διάστημα συντονισμού σημείου):</u>**
Ο χρόνος αυτός χρησιμοποιείται από τα σημεία πρόσβασης (που εδώ ονομάζονται συντονιστές σημείου), όταν θέλουν να προσπελάσουν το μέσο μετάδοσης πριν από τους άλλους σταθμούς. Η τιμή του είναι λίγο μεγαλύτερη από του SIFS, δηλαδή 78 μsec.

3. **<u>Distributed IFS - DIFS (Κατανεμημένο δια-πλαισιακό διάστημα):</u>**
Ο χρόνος αυτός είναι το επιπλέον χρονικό διάστημα που μεσολαβεί προτού ένας σταθμός - που έχει ανιχνεύσει το μέσο ως ελεύθερο - προβεί σε οποιαδήποτε αποστολή πακέτου. Η τιμή του ορίζεται λίγο μεγαλύτερη από του PIFS, στα 128 μsec.

4. **<u>Extended IFS - EIFS (Εκτεταμένο δια-πλαισιακό διάστημα):</u>**
Το χρονικό αυτό διάστημα είναι το μεγαλύτερο από όλα και χρησιμοποιείται από ένα σταθμό ο οποίος έχει λάβει ένα πακέτο το οποίο δε μπόρεσε να

αποκωδικοποιήσει, π.χ. λόγω της ύπαρξης λαθών. Ο χρόνος αυτός είναι απαραίτητος, για να εμποδίσει ένα σταθμό, ο οποίος δε μπόρεσε να αποκωδικοποιήσει π.χ. ένα πακέτο RTS ή CTS, να συγκρουστεί με πακέτα ενός διαλόγου που βρίσκεται σε εξέλιξη.

6.1.5 Θέματα ασφάλειας

Ένα από τα πρώτα θέματα που θα πρέπει να αντιμετωπίζεται από όσους υλοποιούν ένα ασύρματο δίκτυο είναι το θέμα της **ασφάλειας (security).** Τα σπουδαιότερα θέματα που απασχολούν τους διαχειριστές ενός ασύρματου δικτύου σχετικά με τη δράση ενός εισβολέα είναι δύο:

α) η πρόσβαση στους πόρους του τοπικού δικτύου με τη χρήση παρόμοιου ασύρματου εξοπλισμού
β) η υποκλοπή της κυκλοφορίας του δικτύου.

Η αντιμετώπιση της παράνομης πρόσβασης στο δίκτυο γίνεται, όπως έχει ήδη αναφερθεί, με τη χρήση ενός μηχανισμού επικύρωσης, όπου ο ασύρματος σταθμός για να αποκτήσει πρόσβαση στο δίκτυο θα πρέπει να αποδείξει στο σημείο πρόσβασης ότι γνωρίζει ένα μυστικό κωδικό.

Η αντιμετώπιση της υποκλοπής της κυκλοφορίας γίνεται με τη χρήση του αλγορίθμου **WEP (Wired Equivalent Privacy)**, ο οποίος εκτελείται σε όλους τους σταθμούς και δεν είναι τίποτε άλλο από μία γεννήτρια ψευδοτυχαίων αριθμών (Pseudo Random Number Generator), η οποία αρχικοποιείται από ένα διαμοιραζόμενο μυστικό κλειδί. Για κάθε πακέτο που μεταδίδεται από ένα σταθμό, η γεννήτρια παράγει μια ψευδοτυχαία ακολουθία bit, της οποίας το μήκος είναι ίσο με το μεγαλύτερο δυνατό μέγεθος πακέτου και η οποία χρησιμοποιείται για την κρυπτογράφηση των bits του μηνύματος. Ο δέκτης από την πλευρά του θα πρέπει να γνωρίζει το μυστικό κλειδί αρχικοποίησης, έτσι ώστε για κάθε εισερχόμενο πακέτο να μπορεί να παράγει τη σωστή ψευδοτυχαία ακολουθία για την αποκρυπτογράφησή του.

6.1.6 Δίκτυα ειδικού σκοπού με το 802.11 (Ad hoc networks)

Σε μερικές περιπτώσεις μπορεί να χρειάζεται να υλοποιηθεί ένα ασύρματο δίκτυο που να ακολουθεί το πρότυπο 802.11, αλλά του οποίου η δομή να μην είναι απαραίτητο να είναι κυψελοειδής, ή καλύτερα να μην περιέχει Σημεία Πρόσβασης. Παραδείγματα αυτού του τύπου περιλαμβάνουν την ασύρματη διασύνδεση δύο προσωπικών φορητών notebooks, τη διασύνδεση δύο προσωπικών φορητών υπολογιστών (laptops), κλπ.

Το πρότυπο 802.11, αντιμετωπίζει αυτήν την ανάγκη, προσδιορίζοντας τον Ad-Hoc τρόπο λειτουργίας (Ad-Hoc mode). Ένα ασύρματο δίκτυο που βρίσκεται σε Ad-Hoc τρόπο λειτουργίας, δεν περιέχει σημεία πρόσβασης και ένα τμήμα των λειτουργιών του εκτελείται από τους ίδιους τους σταθμούς, όπως είναι ο συγχρονισμός, η εκπομπή πλαισίων - φάρων, κλπ. Επίσης, κάποιες άλλες λειτουργίες δεν υποστηρίζονται, όπως η αναμετάδοση πλαισίων μεταξύ σταθμών του δικτύου που δεν έχουν τη δυνατότητα άμεσης επικοινωνίας, μιας και αυτή η λειτουργία κανονικά εκτελείται από το σημείο πρόσβασης. Αυτό σημαίνει ότι όλοι οι σταθμοί σε ένα ad-hoc δίκτυο θα πρέπει να μπορούν να επικοινωνήσουν με όλους τους υπόλοιπους.

6.2 Το IEEE 802.11b ή Wi-Fi

Το **Wi-**Fi προέρχεται από τα αρχικά των **"Wireless Fidelity" (Ψηφιακή Πιστότητα)** και έχει επικρατήσει σαν όρος για το υψηλής συχνότητας ασύρματο τοπικό δίκτυο (WLAN). Βασικά αποτελεί έναν ασύρματο τρόπο διασύνδεσης, ενώ δίνει την δυνατότητα σύνδεσης και με το Internet. Χρησιμοποιείται για να προσδιορίσει τις συσκευές που βασίζονται στην προδιαγραφή IEEE 802.11 b/g.

Το Wi-Fi είχε σκοπό να επιτρέπει σε φορητές συσκευές, όπως φορητούς υπολογιστές και προσωπικούς ψηφιακούς βοηθούς (PDAs) να συνδέονται σε τοπικά δίκτυα, αλλά τώρα χρησιμοποιείται συχνά για πρόσβαση στο Διαδίκτυο και ασύρματα VoIP τηλέφωνα. Οι επιτραπέζιοι υπολογιστές μπορούν επίσης να χρησιμοποιήσουν Wi-Fi, επιτρέποντας σε γραφεία και σπίτια να δικτυώνονται χωρίς ακριβή καλωδίωση. Πολλοί υπολογιστές πωλούνται σήμερα με ενσωματωμένο Wi-Fi ενώ άλλοι χρειάζονται την προσθήκη κάρτας δικτύου Wi-Fi. Άλλες συσκευές όπως οι ψηφιακές κάμερες είναι μερικές φορές εξοπλισμένες με Wi-Fi.

Μια λειτουργική Wi-Fi συσκευή είναι ικανή να συνδέεται σε ένα τοπικό δίκτυο όταν βρίσκεται κοντά σε ένα από τα σημεία πρόσβασης του δικτύου. Η σύνδεση γίνεται μέσω ραδιοσημάτων. Δεν είναι απαραίτητο να συνδέσουμε την συσκευή στο δίκτυο. Αν το τοπικό δίκτυο είναι συνδεδεμένο στο Διαδίκτυο, η συσκευή Wi-Fi μπορεί να έχει επίσης πρόσβαση. Η γεωγραφική περιοχή που καλύπτεται από ένα ή περισσότερα σημεία πρόσβασης ονομάζεται hotspot. Η εμβέλεια ενός σημείου πρόσβασης ποικίλει. Το σημείο πρόσβασης που βρίσκεται σε έναν τυπικό Wi-Fi δρομολογητή μπορεί να έχει εμβέλεια 45 μέτρων (150 πόδια) εσωτερικά και 90 μέτρα (300 πόδια) εξωτερικά.

Το Wi-Fi ελέγχεται από την Ένωση Wi-Fi (παλιότερα γνωστή ως Ένωση Συμβατότητας Ασύρματου Ethernet), τον εμπορικό οργανισμό που δοκιμάζει και πιστοποιεί την συμβατότητα του εξοπλισμού με τα στάνταρ IEEE 802.11. Η Apple Computer πουλάει Wi-Fi προϊόντα με το AirPort λογότυπο της. Πιστοποιημένα προϊόντα μπορούν να χρησιμοποιούν το επίσημο Wi-Fi λογότυπο, το οποίο υποδεικνύει ότι το προϊόν συνεργάζεται με οποιοδήποτε προϊόν που έχει το ίδιο λογότυπο.

Εικόνα 37. Κάρτα PCMCIA WIFI

Εικόνα 38. Κάρτα PCI-EXPRESS WIFI

6.2.1 Ελεύθερο Wi-Fi

Ενώ οι εμπορικές υπηρεσίες προσπαθούν να μετακινήσουν τα υπάρχοντα μοντέλα εργασίας στο Wi-Fi πολλά γκρουπ, κοινότητες, πόλεις καθώς και μεμονωμένα άτομα έχουν ήδη στήσει ελεύθερα Wi-Fi δίκτυα, συχνά υιοθετώντας μια κοινή συμφωνία ανταλλαγής. Έτσι ώστε τα δίκτυα να μπορούν ελεύθερα να αλληλεπιδρούν το ένα με το άλλο. Ελεύθερα ασύρματα δίκτυα mesh συχνά θεωρούνται το μέλλον του Διαδικτύου.

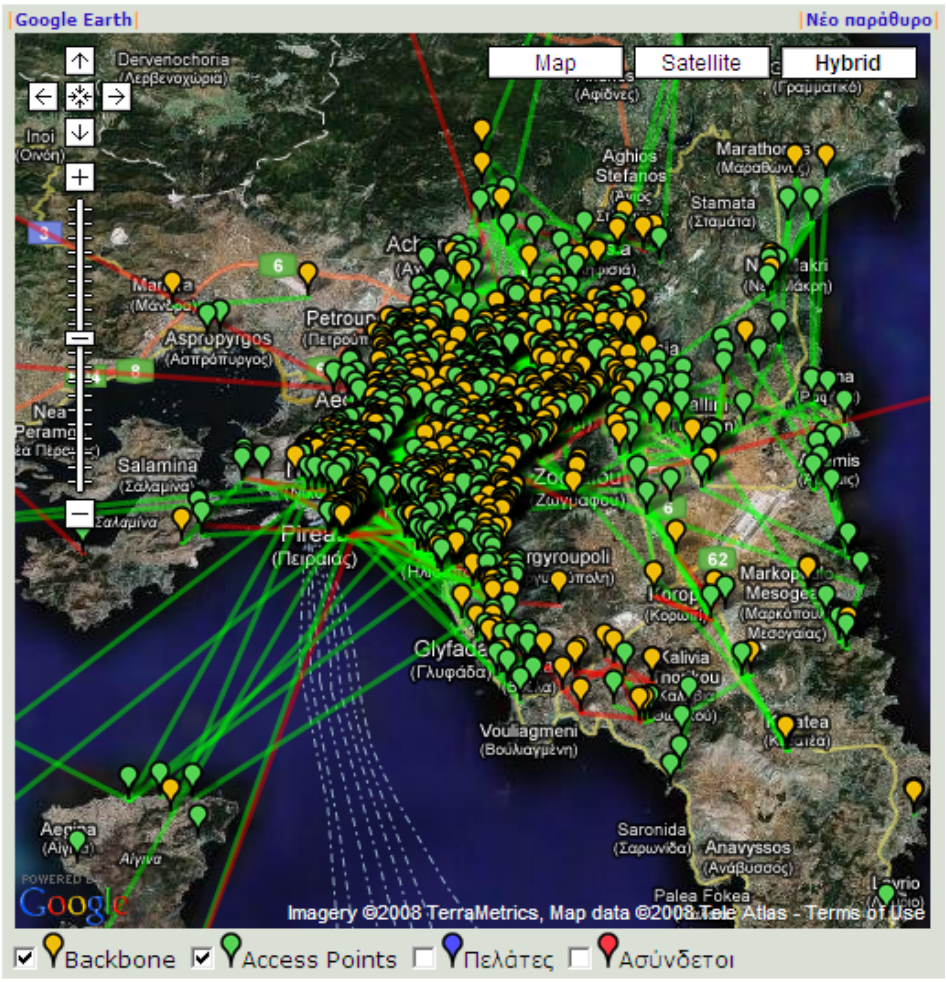
Κάποιες μικρές χώρες και δήμοι ήδη παρέχουν ελεύθερα Wi-Fi hotspots και ελεύθερη τοπική Wi-Fi πρόσβαση στο Διαδίκτυο στον καθένα. Τα παραδείγματα αυτά συμπεριλαμβάνουν το Βασίλειο της Τόγκα και της Εσθονίας που έχουν ήδη ένα μεγάλο αριθμό ελεύθερων Wi-Fi hotspots στις χώρες τους.

Πολλά Πανεπιστήμια παρέχουν ελεύθερη Wi-Fi πρόσβαση στο Διαδίκτυο στους φοιτητές, στους επισκέπτες τους και στον καθένα στον Πανεπιστημιακό χώρο. Παρόμοια κάποιες εμπορικές εταιρίες παρέχουν ελεύθερη Wi-Fi πρόσβαση σε τακτικούς πελάτες.

Παρόλα αυτά, υπάρχει και μία τρίτη υποκατηγορία δικτύων που δημιουργούνται από συγκεκριμένες κοινότητες όπως τα Πανεπιστήμια, όπου η υπηρεσία παρέχεται δωρεάν στα μέλη και στους επισκέπτες της κοινότητας όπως στους μαθητές, ενώ παλαιότερα έβγαζαν λεφτά με το να παρέχουν την υπηρεσία σε εταιρίες και σε τρίτα άτομα. Ένα παράδειγμα τέτοιας υπηρεσίας είναι το Sparknet στην Φιλανδία. Το Sparknet επίσης υποστηρίζει το OpenSparknet, ένα πρόγραμμα στο οποίο άτομα μπορούν να δηλώσουν το δικό τους ασύρματο σημείο πρόσβασης σαν μέρος του Sparknet με αντάλλαγμα συγκεκριμένα πλεονεκτήματα.

Έχει και η Ελλάδα τις δικές της ασύρματες κοινότητες, που στήνουν το ανεξάρτητο δίκτυό τους, στηριγμένο στο WiFi, χωρίς να ενοχλούν κανένα, εξασφαλίζοντας φθηνή επικοινωνία. Τέτοια δίκτυα **(community networks)** υπάρχουν σε αρκετές ελληνικές πόλεις (Αθήνα, Θεσσαλονίκη, Πάτρα, Ιωάννινα, Σέρρες, Ξάνθη, κ.ά) ενώ υπάρχει στα σκαριά η διαμόρφωση πανελλήνιου δικτύου. Στη χώρα μας, οι επίσημοι κόμβοι WiFi έχουν πλέον αυξηθεί κατά πολύ (κυρίως στα αστικά κέντρα), ενώ πληθαίνουν τα hotspots σε ξενοδοχεία, infoκαφετέριες και κάθε είδους επιχειρήσεις. Δυστυχώς, τα ελληνικά ασύρματα δίκτυα παραμένουν ακόμη στην πρώτη εποχή του WiFi, δηλαδή του τοπικού δικτύου, αλλά αυτό δεν μειώνει καθόλου το ενδιαφέρον.

Το Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών (AWMN) είναι ένας μη κερδοσκοπικός σύλλογος, που καλύπτει τις περισσότερες περιοχές της Αθήνας (σύμφωνα με το αντίστοιχο site, 2257 κόμβοι τον Ιούλιο 2004) και συνεχώς επεκτείνεται. Είναι αξιοσημείωτη η ανάπτυξη ενός τέτοιου ασύρματου δικτύου σε τόσο μεγάλη γεωγραφική κλίμακα. Το **Salonica Wireless Network (SWN)**, η ασυρμάτως δικτυωμένη κοινότητα της Θεσσαλονίκης, αυτοπροσδιορίζεται στην ιστοσελίδα της ως εξής: "Το SWN είναι μια ομάδα ατόμων, η οποία επεκτείνεται μέρα με τη μέρα, που ασχολούνται με τη δημιουργία ενός νόμιμου, ψηφιακού, ασύρματου δικτύου υψηλών ταχυτήτων, ελεύθερης πρόσβασης, στην ευρύτερη περιοχή της Θεσσαλονίκης. Κύριος σκοπός είναι να δημιουργηθεί ένα αξιοπρεπές, ελεύθερο δίκτυο, με υψηλό bandwidth ανάμεσα στους κόμβους κάθε ενδιαφερόμενου, μέσω ενός κοινοτικού ασύρματου δικτύου. Το SWN δεν θέτει ως στόχο του αυτήν τη στιγμή την παροχή Ίντερνετ. Ως χρήσεις του τοπικού δικτύου που θέλει να στήσει, είναι η ανταλλαγή δεδομένων και αρχείων, το ηλεκτρονικό ταχυδρομείο, τα παιχνίδια, η ανταλλαγή υπηρεσιών, το voiceoverIP και η τηλεφωνία, η τηλεδιάσκεψη, το video streaming, οι συνομιλίες (chatting) και γενικά οποιαδήποτε λειτουργία μπορεί να αναπτυχθεί στο Ίντερνετ. Ας μην ξεχνάμε πως και το Ίντερνετ ξεκίνησε σαν τοπικό δίκτυο μεταξύ Πανεπιστημίων των ΗΠΑ, χωρίς να είναι βέβαιο το μέλλον του".



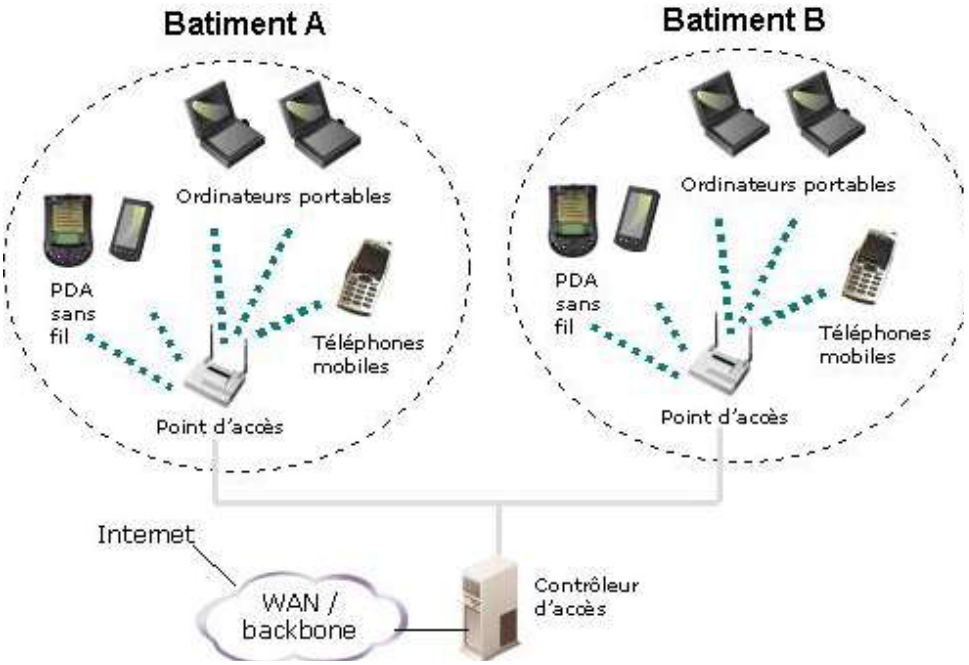
Εικόνα 39. Χάρτης του Ασύρματου Μητροπολιτικού Δικτύου Αθηνών

Το **Ακαδημαϊκό Ασύρματο Δίκτυο Ηρακλείου**, είναι άλλο ένα community network, που έχει δημιουργηθεί εξ ολοκλήρου από την ακαδημαϊκή κοινότητα του Πανεπιστημίου Ηρακλείου και παρουσιάζει σοβαρή ανάπτυξη. Στο Βόλο, το Πανεπιστήμιο Θεσσαλίας έχει υλοποιήσει ένα ασύρματο δίκτυο, το οποίο συνδέει ευρυζωνικά όλα τα σχολεία της περιοχής, στο πλαίσιο του Πανελλήνιου Σχολικού Δικτύου. Αξίζει να σημειωθεί ότι όλα τα Ασύρματα Δίκτυα της Ελλάδας, δεν έχουν εμπορική διάσταση, αλλά αυστηρά συνεργατική. Με βάση το ισχύον κανονιστικό πλαίσιο, τα community networks εντάσσονται στο "καθεστώς ιδίας χρήσης", υπό την προϋπόθεση ότι δεν παρέχουν εμπορικές υπηρεσίες σε τρίτους, δεν κάνουν δηλαδή εμπορική εκμετάλλευση του δικτύου, αλλά χρήση μόνο από τα μέλη τους. Μια εικόνα της ελληνικής ασύρματης κοινωνίας μπορείτε να έχετε, εάν ψάξετε στο Διαδίκτυο με τους κωδικούς Hellas Wireless Network.

Οι κύριες εφαρμογές των ελληνικών WLAN εντοπίζονται στα εξής: Τη δημιουργία hotspots και επομένως την εξυπηρέτηση κινούμενων χρηστών εντός μικρών και συγκεκριμένων περιοχών. Τη δημιουργία ζεύξεων σημείου προς σημείο με συγκεκριμένη χρήση. Την αντικατάσταση του ενσύρματου δικτύου στο οικιακό ή το επιχειρηματικό περιβάλλον.

Με την υπ. αριθμ. 12197/344/25-02-2004 Κοινή Υπουργική Απόφαση των Υπουργών Οικονομίας & Οικονομικών και Μεταφορών & Επικοινωνιών, προκηρύχθηκε το Πρόγραμμα "Χρηματοδότηση Επιχειρήσεων για τη δημιουργία Σημείων Ασύρματης Ευρυζωνικής Πρόσβασης (WIRELESS HOTSPOTS)" στο πλαίσιο του Μέτρου 4.2 "Ανάπτυξη Υποδομών Δικτύων Τοπικής Πρόσβασης" του

Επιχειρησιακού Προγράμματος Κοινωνία της Πληροφορίας. Στο πρόγραμμα μπορούν να συμμετάσχουν επιχειρήσεις που επιθυμούν να αξιοποιήσουν τις τεχνολογίες των ασύρματων δικτύων, με σκοπό την παροχή δικτυακών ή διαδικτυακών υπηρεσιών προστιθέμενης αξίας, σε χρήστες που κινούνται στο χώρο κάλυψης τους επισκέπτες, φιλοξενούμενους και εργαζόμενους.



Εικόνα 40. Μία μορφή του ελεύθερου Wi-Fi

6.2.2 Πλεονεκτήματα - Μειονεκτήματα Wi-Fi

Πλεονεκτήματα:

- Σε αντίθεση με τα συστήματα packet radio το Wi-Fi χρησιμοποιεί μη κατοχυρωμένο ραδιοφάσμα και δεν χρειάζεται έγκριση των αρχών για ιδιωτική ανάπτυξη.
- Επιτρέπει στα LANs να αναπτυχθούν χωρίς καλωδίωση, πιθανώς μειώνοντας το κόστος της ανάπτυξης και επέκτασης του δικτύου. Μέρη όπου τα καλώδια δεν μπορούν να υπάρχουν όπως εξωτερικές περιοχές και ιστορικά κτίρια, μπορούν να φιλοξενήσουν ασύρματα δίκτυα.
- Προϊόντα Wi-Fi χρησιμοποιούνται μαζικά στην αγορά. Διαφορετικές μάρκες σημείων πρόσβασης και διεπαφών δικτύου πελατών συνεργάζονται σε ένα βασικό επίπεδο της υπηρεσίας.
- Ο ανταγωνισμός μεταξύ των πωλητών έχει μειώσει τις τιμές σημαντικά από την κυκλοφορία τους.
- Πολλά δίκτυα Wi-Fi υποστηρίζουν το roaming, στο οποίο μία φορητή συσκευή πελάτη όπως ένας φορητός υπολογιστής, μπορεί να μετακινηθεί από ένα σημείο πρόσβασης σε ένα άλλο καθώς ο χρήστης μετακινείται σε ένα κτίριο ή σε μια περιοχή.

- Πολλά σημεία πρόσβασης και διεπαφές δικτύων υποστηρίζουν διάφορα επίπεδα κρυπτογράφησης για να προστατέψουν τα δεδομένα από υποκλοπή.
- Το Wi-Fi είναι ένα παγκόσμιο σετ από στάνταρς. Αντίθετα με τους πελάτες δικτύου κυψελών, ο ίδιος Wi-Fi πελάτης μπορεί να δουλέψει σε διαφορετικές χώρες ανά τον κόσμο (αν και μπορεί να χρειαστεί κάποιες ρυθμίσεις στο λογισμικό).

Μειονεκτήματα:

- Η χρησιμοποίηση της συχνότητας των 2.4GHz από το Wi-Fi δεν απαιτεί άδεια από τον περισσότερο κόσμο με την προϋπόθεση ότι κάποιος μένει κάτω από τα θεσμοθετημένα τυπικά όρια και με την προϋπόθεση ότι κάποιος δέχεται παρεμβολές από άλλες πηγές, συμπεριλαμβανομένων παρεμβολές που προκαλούν τη δυσλειτουργία των συσκευών του.
- Η νομοθεσία δεν είναι ίδια παντού. Οι περισσότερες ευρωπαϊκές χώρες επιτρέπουν 2 κανάλια παραπάνω από αυτά των προδιαγραφών b, g. Η Ιαπωνία έχει και ένα ακόμα κανάλι και χώρες όπως η Ισπανία απαγορεύουν την χρήση καναλιών με μικρότερους αριθμούς.
- Το 802.11b και το 802.11g χρησιμοποιούν το φάσμα των 2.4GHz, στο οποίο υπάρχει συνωστισμός από άλλες συσκευές όπως το Bluetooth, φούρνων μικροκυμάτων, ασύρματα τηλέφωνα (τα 900MHz ή τα 5.8GHz είναι εναλλακτικές συχνότητες τηλεφωνικές που μπορούν να χρησιμοποιηθούν για αποφυγή παρεμβολών με ένα Wi-Fi δίκτυο) και συσκευές αποστολής βίντεο ανάμεσα σε πολλές άλλες. Αυτό μπορεί να προκαλέσει μία στατική μείωση στην απόδοση. Άλλες συσκευές που χρησιμοποιούν αυτές τις συχνότητες μικροκυμάτων μπορούν επίσης να προκαλέσουν σταδιακή μείωση στην απόδοση.
- Κλειστά σημεία πρόσβασης μπορούν να παρεμβάλλονται με σωστά ρυθμισμένα ανοιχτά σημεία πρόσβασης στην ίδια συχνότητα, εμποδίζοντας την λειτουργία των ανοιχτών σημείων πρόσβασης από άλλους.
- Η κατανάλωση ενέργειας είναι συγκριτικά πολύ μεγαλύτερη σε σχέση με άλλα στάνταρ κάνοντας την διάρκεια ζωής της μπαταρίας και την εκπεμπόμενη θερμότητα.

6.2.3 Ασφάλεια

Ο εξοπλισμός Wi-Fi μπορεί να χρησιμοποιηθεί για την κλοπή προσωπικών πληροφοριών (κωδικών, οικονομικών δεδομένων, δεδομένων αναγνώρισης κτλ) που μεταδίδονται από χρήστες Wi-Fi, αν δεν χρησιμοποιούνται λογικές προστασίες.

Το πρώτο και πιο κοινό στάνταρ ασύρματης κρυπτογράφησης το Wired **Equivalent Privacy ή WEP**, έχει αποδειχθεί ότι παραβιάζεται εύκολα ακόμα και όταν είναι σωστά ρυθμισμένο. Τα περισσότερα ασύρματα προϊόντα στην αγορά υποστηρίζουν το Wi-Fi Protected Access (WPA) πρωτόκολλο κρυπτογράφησης που θεωρείται πολύ πιο δυνατό, αν και κάποια παλιότερα σημεία πρόσβασης πρέπει να αντικατασταθούν για να το υποστηρίξουν. Η υιοθέτηση του στάνταρ **802.11i** (με εμπορικό όνομα **WPA2)** κάνει δυνατό ένα καλύτερο σύστημα προστασίας όταν είναι καλά ρυθμισμένο. Από τα μέσα του 2005, τα Microsoft Windows XP και το MAC OS υποστηρίζουν το WPA2, αλλά μόνο στον πιο σύγχρονο εξοπλισμό. Καθώς περιμέναμε καλύτερα στάνταρ να γίνουν διαθέσιμα, πολλές επιχειρήσεις έχουν επιλέξει να αναπτύξουν επιπλέον βαθμίδες κρυπτογράφησης (όπως τα VPNS) για να προστατευτούν από υποκλοπές.

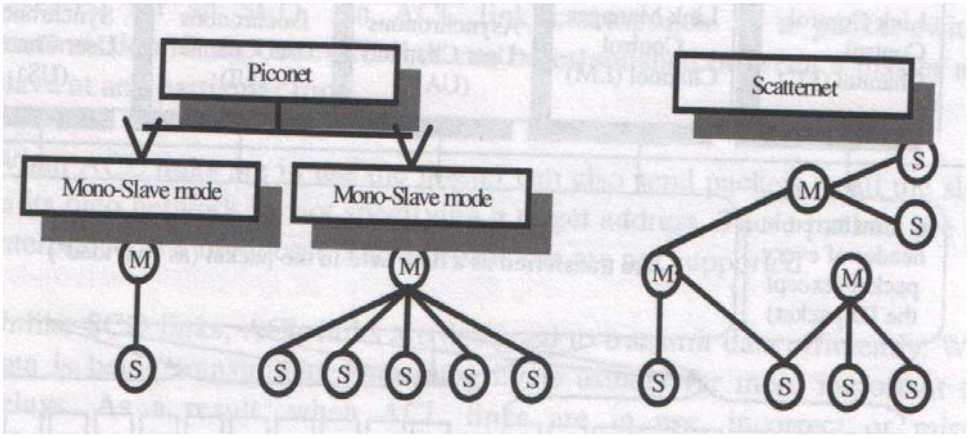
Υπάρχουν πολλές αναφορές ότι η αλληλεπίδραση ενός κλειστού ή κρυπτογραφημένου σημείου πρόσβασης με άλλα ανοιχτά σημεία πρόσβασης στα ίδια ή σε γειτονικά κανάλια μπορεί να αποτρέψει την πρόσβαση στα ανοιχτά σημεία πρόσβασης από άλλους στην περιοχή. Αυτό μπορεί να αποτελέσει πρόβλημα πυκνοκατοικημένες περιοχές , όπως τα μεγάλα συγκροτήματα πολυκατοικιών, όπου πολλοί κάτοικοι χρησιμοποιούν Wi-Fi σημεία πρόσβασης.

Μεγάλες επιχειρήσεις συχνά ανησυχούν για το ρίσκο της ασφάλειας σε ένα ασφαλές εταιρικό δίκτυο από ένα μη εξουσιοδετημένο ασύρματο σημείο πρόσβασης, επίσης γνωστό ως rogue σημείο πρόσβασης. Με την αγορά φθηνών ασύρματων δρομολογητών που υπάρχουν σε καταστήματα ηλεκτρονικών ειδών οι υπάλληλοι μερικές φορές συνδέουν έναν μη εξουσιοδοτημένο σημείο πρόσβασης, είτε από άγνοια είτε με δόλο, εκθέτοντας έτσι το καθ' όλα ασφαλές εταιρικό δίκτυο σε οποιονδήποτε κάνει wardriving. Για να εξαλείψουμε το πιθανό ρίσκο των rogue σημείων πρόσβασης κάποιοι μεγάλοι οργανισμοί άρχισαν (από το 2005) να εγκαθιστούν ασύρματα συστήματα ανίχνευσης εισβολών. Αυτά τα συστήματα είναι σχεδιασμένα να ελέγχουν για ασύρματα σήματα και να αναφέρουν αμέσως την παρουσία μη εξουσιοδοτημένων σημείων πρόσβασης.

6.3 Bluetooth

Το 1994 η εταιρεία **Ericsson** έδειξε ενδιαφέρον για τη σύνδεση των κινητών της τηλεφώνων σε άλλες συσκευές (όπως συσκευές PDA) χωρίς καλώδια. Μαζί με άλλες τέσσερις εταιρείες (IBM, Intel, Nokia, και Toshiba), σχημάτισε μια **Ομάδα Ειδικών Ενδιαφερόντων ή SIG (Special Interest Group**, δηλαδή κοινοπραξία) για την ανάπτυξη ενός προτύπου ασύρματης διασύνδεσης υπολογιστικών και επικοινωνιακών συσκευών και βοηθημάτων με χρήση ραδιοκυματικών πομποδεκτών μικρής εμβέλειας, χαμηλής ισχύος, και χαμηλού κόστους. Το έργο ονομάστηκε **BIuetooth**, από τον Harald Blaatand 11 (ή Bluetooth, δηλαδή μπλε δόντι) (940-981), ένα βασιλιά των Βίκινγκς που ενοποίησε (δηλαδή κατέκτησε) τη Δανία και τη Νορβηγία, επίσης χωρίς να χρησιμοποιεί καλώδια.

Η αιτία για αυτή τη σχεδίαση **κυρίου/υπηρέτη** είναι ότι οι σχεδιαστές ήθελαν να διευκολύνουν την υλοποίηση ολοκληρωμένων κυκλωμάτων Bluetooth με κόστος μικρότερο από $5. Μία συνέπεια αυτής της απόφασης είναι ότι οι υπηρέτες είναι σχετικά "χαζοί", αφού ουσιαστικά κάνουν οτιδήποτε τους λέει ο κύριος. Ουσιαστικά, το μικροσκοπικό δίκτυο είναι ένα συγκεντρωτικό σύστημα TDM, με τον κύριο να ελέγχει το ρολόι και να καθορίζει ποια συσκευή θα επικοινωνήσει σε ποια χρονική υποδοχή. Όλες οι επικοινωνίες πραγματοποιούνται ανάμεσα στον κύριο και έναν υπηρέτη. Δεν είναι εφικτή η άμεση επικοινωνία από υπηρέτη σε υπηρέτη.



Εικόνα 41. Αρχιτεκτονική δικτύου Bluetooth

6.3.1 Η στοίβα πρωτοκόλλων του Bluetooth

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 χαμηλότερο επίπεδο είναι το φυσικό επίπεδο των ραδιοκυμάτων, το οποίο αντιστοιχίζεται αρκετά καλά στο φυσικό επίπεδο των μοντέλων OSI και 802. Ασχολείται με τη μετάδοση των ραδιοκυμάτων και τη διαμόρφωση. Πολλά από τα ζητήματα του επιπέδου αυτού σχετίζονται με το στόχο να είναι το σύστημα φτηνό, έτσι ώστε να μπορεί να γίνει μαζικό προϊόν.

Το επίπεδο βασικής ζώνης (baseband) 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.

Στη συνέχεια έχουμε ένα επίπεδο με μια ομάδα κάπως σχετιζόμενων πρωτοκόλλων. Ο **διαχειριστής συνδέσμου (link manager)** χειρίζεται την εγκαθίδρυση λογικών καναλιών ανάμεσα στις συσκευές, όπου συμπεριλαμβάνεται και η διαχείριση ισχύος, η πιστοποίηση ταυτότητας, και η ποιότητα υπηρεσιών. Το **πρωτόκολλο προσαρμογής ελέγχου λογικού συνδέσμου (logical link control adaptation protocol**, συχνά αποκαλείται **L2CAP**) αποκρύπτει από τα α-νώτερα επίπεδα τις λεπτομέρειες της μετάδοσης. Είναι ανάλογο με το τυπικό υποεπίπεδο LLC του 802, αλλά διαφέρει από τεχνική άποψη. Όπως υποδηλώνουν τα ονόματά τους, τα πρωτόκολλα ήχου (audio) και ελέγχου (control) ασχολούνται με τον ήχο και τον έλεγχο, αντίστοιχα. Οι εφαρμογές μπορούν να φτάσουν απευθείας σε αυτά, χωρίς να χρειαστεί να περάσουν πρώτα από το πρωτόκολλο L2CAP.

Το επόμενο επίπεδο προς τα επάνω είναι το επίπεδο **ενδιάμεσου λογισμικού (middleware),** το οποίο περιέχει ένα μίγμα διαφορετικών πρωτοκόλλων. Το πρωτόκολλο LLC του 802 εισήχθηκε εδώ από το IEEE για συμβατότητα με τα άλλα δίκτυα 802. Τα πρωτόκολλα **RFComm**, τηλεφωνίας (telephony), και **ανακάλυψης υπηρεσιών (service discovery)** είναι εγγενή πρωτόκολλα του Bluetooth. Το RFComm (επικοινωνία ραδιοκυματικών συχνοτήτων, Radio Fre-quency Communication) είναι το πρωτόκολλο που εξομοιώνει την τυπική σειριακή θύρα που υπάρχει στους περισσότερους προσωπικούς υπολογιστές για τη σύνδεση πληκτρολογίων, ποντικιών, μόντεμ, και άλλων συσκευών. Έχει σχεδιαστεί για να επιτρέπει την εύκολη χρήση του από παλαιότερες συσκευές. Το πρωτόκολλο τηλεφωνίας είναι ένα πρωτόκολλο πραγματικού χρόνου που χρησιμοποιείται για τα τρία προφίλ τα οποία είναι προσανατολισμένα στην ομιλία. Διαχειρίζεται επίσης την εγκαθίδρυση και τον τερματισμό των κλήσεων. Τέλος, το πρωτόκολλο ανακάλυψης υπηρεσιών χρησιμοποιείται για τον εντοπισμό υπηρεσιών μέσα στο δίκτυο.

Το υψηλότερο επίπεδο είναι αυτό στο οποίο βρίσκονται οι εφαρμογές και τα προφίλ. Οι εφαρμογές χρησιμοποιούν τα πρωτόκολλα των χαμηλότερων επιπέδων για να κάνουν τη δουλειά τους. Κάθε εφαρμογή έχει το δικό της αποκλειστικό υποσύνολο πρωτοκόλλων. Οι συγκεκριμένες συσκευές, όπως ένα ακουστικό κεφαλής, περιέχουν συνήθως μόνο τα πρωτόκολλα που χρειάζονται για την αντίστοιχη εφαρμογή και τίποτα άλλο.

6.3.2 Το επίπεδο ραδιοκυμάτων του Bluetooth

Το επίπεδο ραδιοκυμάτων μεταφέρει τα bit από τον κύριο στον υπηρέτη, ή αντίστροφα. Είναι ένα σύστημα **χαμηλής ισχύος** με **εμβέλεια 10 μέτρα** που λειτουργεί στη ζώνη ISM των 2,4 GHz. Η ζώνη διαιρείται σε 79 κανάλια του 1 MHZ το καθένα. Η διαμόρφωση είναι η κωδικοποίηση μετατόπισης συχνότητας, με 1 bit ανά HZ, δίνοντας μικτό ρυθμό μετάδοσης δεδομένων ίσο με 1 Mbps - με μεγάλο μέρος από αυτό το φάσμα, όμως, να καταναλώνεται από τις επιβαρύνσεις. Για να κατανέμονται δίκαια τα κανάλια χρησιμοποιείται εξάπλωση φάσματος με συνεχή αλλαγή συχνότητας, με **1600 αλλαγές/sec** και χρόνο παραμονής ίσο με **625 μsec**. Όλοι οι κόμβοι του μικροσκοπικού δικτύου αλλάζουν συχνότητα ταυτόχρονα, με τον κύριο να επιβάλλει την ακολουθία των συχνοτήτων.

Επειδή τόσο το 802.11 όσο και το Bluetooth λειτουργούν στη ζώνη ISM των 2,4 GHz στα ίδια 79 κανάλια, παρεμβάλλονται μεταξύ τους. Αφού το Bluetooth αλλάζει συχνότητες πολύ πιο γρήγορα από το 802.11, είναι πολύ πιο πιθανό μια συσκευή Bluetooth να καταστρέψει τις μεταδόσεις του 802.11, παρά το αντίστροφο. Επειδή το 802.11 και το 802.15 είναι και τα δύο πρότυπα του IEEE, το IEEE αναζητεί μια

λύση σε αυτό το πρόβλημα· αλλά δεν είναι τόσο εύκολο να τη βρει, αφού και τα δύο συστήματα χρησιμοποιούν τη ζώνη ISM για τον ίδιο λόγο: επειδή δεν απαιτείται άδεια χρήσης. Το πρότυπο 802.11 a χρησιμοποιεί την άλλη ζώνη ISM (στα 5 GHz) αλλά έχει πολύ μικρότερη εμβέλεια από το 802.11b (λόγω των φυσικών ιδιοτήτων των ραδιοκυμάτων), έτσι η χρήση του 802.11a δεν είναι η τέλεια λύση για όλες τις περιπτώσεις. Μερικές εταιρείες έχουν λύσει το πρόβλημα απαγορεύοντας εντελώς το Bluetooth. Μια λύση που βασίζεται στην αγορά είναι το δίκτυο με τη μεγαλύτερη ισχύ (πολιτικά και οικονομικά, όχι ηλεκτρικά) να απαιτήσει από το ασθενέστερο δίκτυο να τροποποιήσει το πρότυπό του, έτσι ώστε να σταματήσει να παρεμβάλλεται με τον "ισχυρότερο". Μερικές σκέψεις πάνω σε αυτό το θέμα παρουσιάζονται στο έγγραφο του Lansford και συνεργατών (2001).

6.3.3 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 πολύπλεξη με διαίρεση χρόνου, με τον κύριο να παίρνει τις μισές υποδοχές και τους υπηρέτες να μοιράζονται τις άλλες μισές. Τα πλαίσια μπορεί να έχουν μήκος 1, 3, ή 5 υποδοχές.

Ο χρονισμός της συνεχούς αλλαγής συχνοτήτων επιτρέπει ένα χρόνο σταθεροποίησης 250-260 μsec σε κάθε αλλαγή συχνότητας, ώστε τα κυκλώματα των πομποδεκτών να σταθεροποιηθούν. Μπορεί να γίνεται και ταχύτερα η σταθεροποίηση, αλλά μόνο με υψηλότερο κόστος. Για ένα πλαίσιο μίας υποδοχής, μετά από τη σταθεροποίηση απομένουν 366 από τα 625 bit. Από αυτά τα 126 χρησιμοποιούνται για έναν κωδικό πρόσβασης και μια κεφαλίδα, αφήνοντας 240 bit για δεδομένα. Όταν συνενώνονται πέντε υποδοχές, χρειάζεται μία μόνο περίοδος σταθεροποίησης ενώ χρησιμοποιείται και ελαφρώς μικρότερη περίοδος σταθεροποίησης, έτσι από τα 5 χ 625 = 3125 bit στις πέντε χρονικές υποδοχές είναι διαθέσιμα τα 2781 στο επίπεδο βασικής ζώνης. Έτσι, τα μεγαλύτερα πλαίσια έχουν πολύ μεγαλύτερη απόδοση από τα πλαίσια μίας υποδοχής.

Κάθε πλαίσιο μεταδίδεται μέσω ενός λογικού καναλιού, που ονομάζεται σύνδεσμος (link), ανάμεσα στον κύριο και έναν υπηρέτη. Υπάρχουν δύο είδη συνδέσμων. Το πρώτο είναι ο **Ασύγχρονος Ασυνδεσμικός σύνδεσμος ή ACL (Asynchronous Connection-Less),** ο οποίος χρησιμοποιείται για δεδομένα μεταγωγής πακέτων τα οποία παράγονται σε ακανόνιστα χρονικά διαστήματα. Τα δεδομένα αυτά προέρχονται από το επίπεδο L2CAP στο άκρο του αποστολέα και παραδίδονται στο επίπεδο L2CAP στο άκρο του παραλήπτη. Η κίνηση ACL παραδίδεται με βάση τη βέλτιστη προσπάθεια. Δεν παρέχονται εγγυήσεις. Τα πλαίσια μπορεί να χαθούν και μπορεί να χρειαστεί να αναμεταδοθούν. Ένας Υπηρέτης μπορεί να έχει μόνο ένα σύνδεσμο ACL με τον κύριό του.

Το άλλο είδος είναι ο **Σύγχρονος Συνδεσμοστρεφής σύνδεσμος ή SCO (Synchronous Connection Oriented)** για δεδομένα πραγματικού χρόνου, όπως οι τηλεφωνικές συνδέσεις. Σε αυτόν τον τύπο καναλιού εκχωρείται μια σταθερή υποδοχή σε κάθε κατεύθυνση. Λόγω της φύσης των συνδέσμων SCO (περιέχουν δεδομένα που είναι κρίσιμα ως προς το χρόνο), τα πλαίσια που στέλνονται μέσω αυτών δεν αναμεταδίδονται ποτέ. Αντιθέτως, μπορεί να χρησιμοποιηθεί ευθεία διόρθωση σφαλμάτων για την παροχή υψηλής αξιοπιστίας. Κάθε σύνδεσμος SCO μπορεί να μεταδίδει ένα κανάλι ήχου PCM στα 64.000 bps.

6.3.4 Το επίπεδο L2CAP του Bluetooth

Το επίπεδο L2CAP έχει τρεις κύριες λειτουργίες. Πρώτον, δέχεται πακέτα μέχρι 64 KB από τα ανώτερα επίπεδα και τα τεμαχίζει σε πλαίσια για μετάδοση. Στο άλλο άκρο, τα πλαίσια συναρμολογούνται ξανά σε πακέτα.

Δεύτερον, διαχειρίζεται την πολύπλεξη και αποπολύπλεξη πολλαπλών πηγών πακέτων. Όταν συναρμολογηθεί ξανά ένα πακέτο, το επίπεδο L2CAP προσδιορίζει σε ποιο πρωτόκολλο υψηλότερου επιπέδου πρέπει να το παραδώσει - για παράδειγμα, στο RFcomm ή το πρωτόκολλο τηλεφωνίας.

Τρίτον, το L2CAP χειρίζεται τις απαιτήσεις για ποιότητα υπηρεσιών, τόσο κατά την εγκαθίδρυση των συνδέσμων όσο και κατά την κανονική λειτουργία. Ένα άλλο αντικείμενο διαπραγμάτευσης κατά την εγκαθίδρυση της σύνδεσης είναι το μέγιστο επιτρεπόμενο μέγεθος του ωφέλιμου φορτίου, έτσι ώστε να μην μπορεί μια συσκευή με μεγάλα πακέτα να κατακλύσει μια συσκευή μικρών πακέτων. Αυτό το χαρακτηριστικό απαιτείται επειδή δεν μπορούν όλες οι συσκευές να χειριστούν πακέτα με το μέγιστο μέγεθος των 64 KB.

6.3.5 Εφαρμογές της τεχνολογίας Bluetooth

- Ασύρματη δικτύωση μεταξύ επιτραπέζιου υπολογιστή και φορητού σε ένα περιορισμένο χώρο όπου χρειάζεται ελάχιστο bandwidth.
- Bluetooth περιφερειακά όπως εκτυπωτές, ποντίκια και πληκτρολόγια.
- Μεταφορά αρχείων (εικόνες, mp3) ανάμεσα σε κινητά τηλέφωνα και PDAs.
- Bluetooth ακουστικά για κινητά τηλέφωνα και Smartphones.
- Ιατρικές εφαρμογές – Δοκιμάζονται κάποιες συσκευές από την εταιρίες που παρέχουν ηλεκτρονικές συσκευές προχωρημένης ιατρικής.
- Μερικοί GPS δέκτες μεταφέρουν πληροφορίες σε pocket pc μέσω Bluetooth.
- Bluetooth car kit : Δίνει τη δυνατότητα σε κινητά τηλέφωνα που έχουν εξοπλισμό Bluetooth να χρησιμοποιούν κάποιες βασικές λειτουργίες του με ασύρματα ακουστικά που αποτελούν κάποιο κομμάτι του αμαξιού. Ανάλογο σύστημα υπάρχει ενσωματωμένο και σε κράνη οδηγών μοτοσικλέτας, επιτρέποντας τη συνομιλία κατά την οδήγηση.
- Για απομακρυσμένο έλεγχο όπου χρησιμοποιούνταν η τεχνολογία υπέρυθρων ακτίνων.

Εικόνα 42. USB Bluetooth Adapter

Εικόνα 43. Bluetooth car kit

6.3.6 Ασφάλεια

Οι διαδικασίες ασφάλειας περιλαμβάνουν **authorization**, **authentication** και προαιρετικό **encryption**.

- Η διαδικασία authentication περιλαμβάνει την επίδειξη της ταυτότητας ενός computer ή χρήστη computer, ή στην περίπτωση του Bluetooth επιδεικνύει την ταυτότητα ενός μέλους του **piconet** σε κάποιο άλλο μέλος.
- Authorization είναι η διαδικασία της παροχής ή απόρριψης πρόσβασης σε μια πηγή του δικτύου.
- Encryption είναι η μετατροπή των δεδομένων σε ένα μυστικό κωδικό. Χρησιμοποιείται μεταξύ των συσκευών Bluetooth έτσι ώστε οι εισβολείς **(eavesdroppers**) να μην μπορούν να διαβάσουν ή να υποκλέψουν το περιεχόμενο των δεδομένων και πληροφοριών που αποστέλλονται.

Η έκθεση στους πολλαπλούς κινδύνους μπορεί να αποφευχθεί με σχετικά απλές τροποποιήσεις μερικές από τις οποίες είναι:

- **PIN length:** Έχοντας σκοπό να αποφύγουμε μια κατάσταση στην οποία ένας επιτιθέμενος (attacker) έχει την δυνατότητα να αποσπάσει τα μυστικά κλειδιά (secret keys) από τις συσκευές των θυμάτων του, είναι σημαντικό να χρησιμοποιούμε αρκετά μεγάλα και τυχαία PINs. Εάν οι χρήστες εφαρμόσουν αυτή την μέθοδο τότε ένα 64bit PIN θεωρείται αρκετά ασφαλές.
- **Προστασία των unit keys:** Για να αποφύγουμε το ενδεχόμενο άλλες συσκευές να μάθουν το unit key των συσκευών με τις οποίες επικοινωνεί, παράγει κλειδιά επικοινωνίας χρησιμοποιώντας το δικό της unit key σαν είσοδο σε μια ψευδοτυχαία παραγωγή. Εάν το παραγόμενο κλειδί είναι επίσης βασισμένο στην διεύθυνση της άλλης συσκευής τότε είναι εύκολο να υπολογιστεί ξανά κάθε φορά που θα έχουμε επικοινωνία μεταξύ των δύο συσκευών. Με τον τρόπο αυτό περιορίζεται ο αποθηκευτικός χώρος που θα χρειαζόταν εάν αποθηκεύαμε όλα τα unit keys των συσκευών με τις οποίες είχε επικοινωνία.
- **Πολιτικές Προστασίας Εναντίον των Επιθέσεων του middle-person:** Η επίθεση του **middle-person** βασίζεται στην απόφαση και οι δύο συσκευές να γίνουν masters ή και η δύο να γίνουν slaves, ώστε να αποφευχθεί το μπέρδεμα του επικοινωνιακού καναλιού από τον

επιτιθέμενο. Επομένως, ορισμένες πτυχές της επίθεσης του middle-person μπορούν να αποφευχθούν με τη βοήθεια των πολιτικών που ελέγχουν ποια συσκευή μπορεί να πάρει το ρόλο του master, ποια του slave και κάτω από ποιες συνθήκες.

Εικόνα 44. Ad-hoc Bluetooth δίκτυο

6.3.7 Bluetooth Vs Wi-Fi

Το μόνο «κοινό» ανάμεσα στο Bluetooth και το Wi-Fi (IEEE 802.11b) είναι η «εκμετάλλευση» του «ελεύθερου» φάσματος συχνοτήτων των 2,4 Ghz. Η ασύρματη τεχνολογία Bluetooth σχεδιάστηκε ώστε να «αντικαταστήσει» τα καλώδια που παρεμβάλλονται ανάμεσα σε ψηφιακές συσκευές και κινητά τηλέφωνα, ενώ η μέγιστη ακτίνα «δράσης» του είναι τα 10 μέτρα. Αντίθετα, το Wi-Fi επιτρέπει την ασύρματη δικτύωση, αντικαθιστώντας τα δίκτυα LAN των υπολογιστών. Στο εγγύς μέλλον το Bluetooth και το Wi-Fi είναι πιθανό να συνυπάρχουν, το μεν πρώτο για να αντικαταστήσει τα «κοινά» καλώδια των PDAs, κινητών, ψηφιακών φωτογραφικών μηχανών, ηχείων, ακουστικών κ.ο.κ. και το δεύτερο για την πρόσβαση σε «ασύρματα» δίκτυα Ethernet υψηλής ταχύτητας.

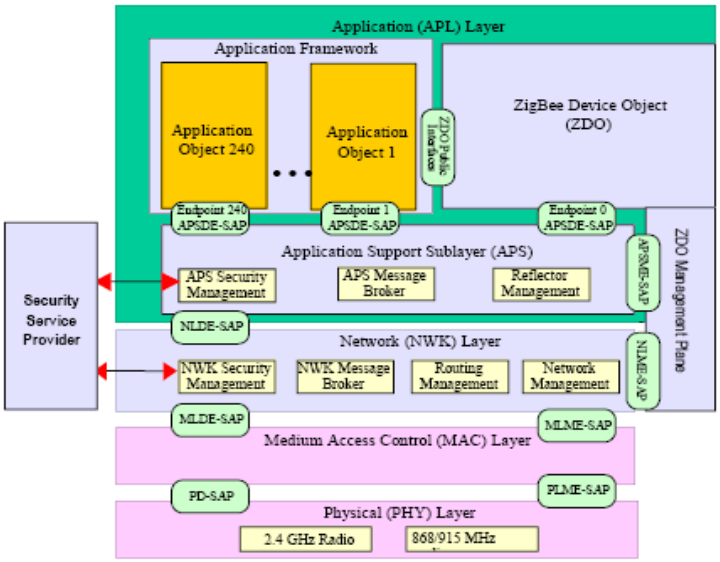
Εφόσον οι δύο αυτές τεχνολογίες «συνυπάρχουν» σε μια συσκευή, αυτή μπορεί να καθορίσει τη χρήση τους, ώστε να μην υπάρχουν παρεμβολές.

6.4 Zigbee

6.4.1 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 (εικόνα 45) είναι τα παρακάτω:

- **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.



Εικόνα 45. Η στοίβα πρωτοκόλλων του ZigBee

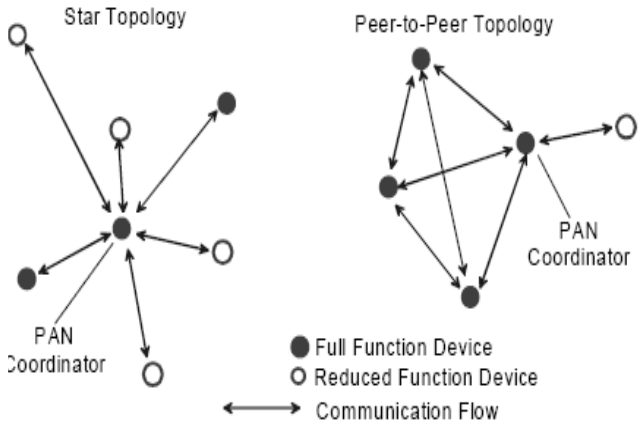
- **Το επίπεδο δικτύου (Network layer, NWK).** Είναι υπεύθυνο για τη δημιουργία του δικτύου, για την είσοδο και την έξοδο μία συσκευής από

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.

6.4.2 Τοπολογίες δικτύων

Ανάλογα με τις απαιτήσεις των εφαρμογών, το ZigBee μπορεί να υποστηρίξει δύο τοπολογίες δικτύων (εικόνα 46). Ανεξαρτήτως τοπολογίας, κάθε συσκευή έχει μία μοναδική διεύθυνση με μήκος 64 bits. Αυτή μπορεί να χρησιμοποιηθεί για την επικοινωνία μέσα σε ένα δίκτυο ή να χρησιμοποιηθεί από το συντονιστή για να χορηγήσει μία συντομευμένη διεύθυνση (16 bits) στη συσκευή. Για κάθε δίκτυο που δημιουργείται, ο συντονιστής επιλέγει μία ταυτότητα (16 bits) που προσδιορίζει μοναδικά το συγκεκριμένο δίκτυο. Ο συνδυασμός ταυτότητας δικτύου και διεύθυνσης συσκευής επιτρέπει την επικοινωνία μεταξύ συσκευών. Κάθε δίκτυο μπορεί να έχει μέχρι και 255 συσκευές.



Εικόνα 46. τοπολογίες δικτύων

- Τοπολογία σε σχήμα αστεριού. Σε αυτή υπάρχει ο συντονιστής του δικτύου, ο οποίος εγκαθιστά συνδέσεις σημείου προς σημείο με άλλες συσκευές. Επίσης ο συντονιστής λειτουργεί και ως δρομολογητής για τη μεταφορά

των δεδομένων μεταξύ των άλλων συσκευών, αφού αυτές δεν μπορούν να επικοινωνήσουν απευθείας.

- Τοπολογία σημείου προς σημείο. Κάθε συσκευή εγκαθιστά συνδέσεις σημείου προς σημείο με άλλες συσκευές που βρίσκονται μέσα στην εμβέλεια της. Με αυτό τον τρόπο δημιουργούνται δίκτυα που έχουν τη μορφή δένδρου ή πλέγματος. Με τη βοήθεια αλγορίθμων δρομολόγησης, όλες οι συσκευές μπορούν να επικοινωνήσουν μεταξύ τους. Πολλά τέτοια δίκτυα μπορούν να ενωθούν μεταξύ τους και να σχηματίσουν ένα μεγαλύτερο. Στο μεγαλύτερο δίκτυο υπάρχει μόνο ένας συντονιστής δικτύου, ενώ κάθε μικρότερο δίκτυο έχει από ένα δρομολογητή.

6.4.3 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.
- Το **Zigbee Alliance** 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 Zigbee Alliance και εξυπηρετούν σκοπούς διαλειτουργικότητας και τα ιδιωτικά προφίλ τα οποία είναι για χρήση στα κλειστά συστήματα.

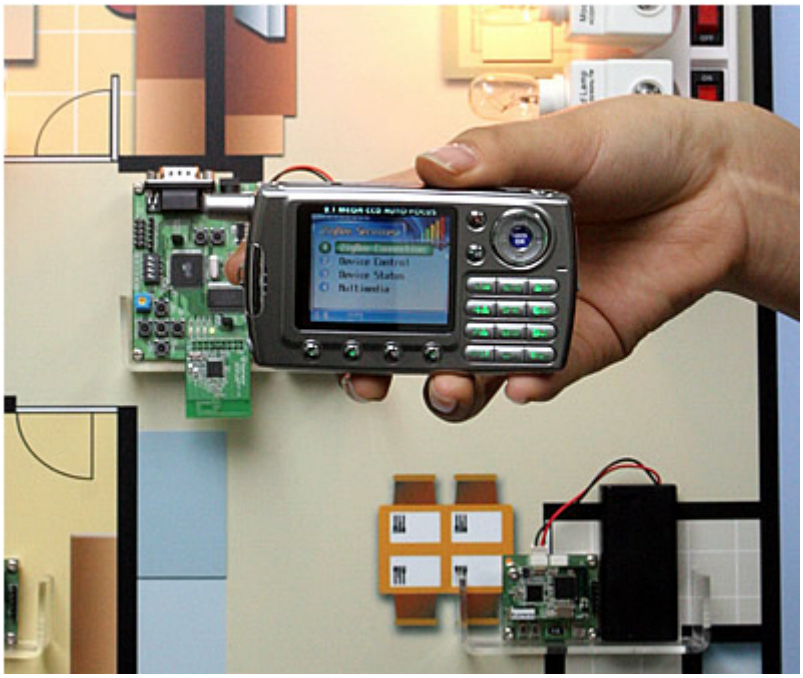
Εικόνα 47. Zigbee router

6.4.4 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 .



Εικόνα 48. Το πρώτο κινητό στον κόσμο που χρησιμοποιεί τεχνολογία Zigbee

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:

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

Κεφάλαιο 7
Προσομοίωση

7.1 Το Comnet III

Το **COMNET III** είναι μία εμπορική εφαρμογή που επιτρέπει εύκολα και γρήγορα την ανάλυση και τον υπολογισμό της απόδοσης ενός δικτύου υπολογιστών. Η περιγραφή του δικτύου γίνεται σε γραφικό περιβάλλον χωρίς να απαιτείται προγραμματισμός από την πλευρά του χρήστη και μπορεί να γίνει προσομοίωση τόσο των Local Area Networks (LAN) όσο και των Wide Area Networks (WAN).

Το COMNET III είναι γραμμένο σε MODSIM ακολουθώντας μια αντικειμενοστραφή σχεδίαση. Χρησιμοποιεί πολλά διαφορετικά αντικείμενα και δομικά στοιχεία (building blocks), των οποίων τα χαρακτηριστικά μπορούν να τροποποιηθούν έτσι ώστε, να ταιριάζουν με αντικείμενα που συναντούμε σε ένα πραγματικό δικτυακό περιβάλλον. Τα στοιχεία αυτά μπορεί να είναι υπολογιστές, links, κόμβοι επικοινωνίας (hubs, routers, bridges), εφαρμογές κ.α.

Το COMNET III αναλύει τη συμπεριφορά και την απόδοση ενός δικτύου χρησιμοποιώντας την **προσομοίωση διακεκριμένων γεγονότων (discrete event simulation)**. Η προσομοίωση διακεκριμένων γεγονότων είναι η πλέον κατάλληλη μέθοδος, γιατί μπορεί να προσομοιώσει ρεαλιστικά και με ακρίβεια τη συμπεριφορά σύνθετων συστημάτων.

Με τη βοήθεια του COMNET III ο υπεύθυνος του δικτύου μπορεί να έχει τις εξής δυνατότητες:

- **Μελέτη υψηλών επιπέδων κίνησης.**
- **Σχεδιασμός ανθεκτικότητας και αντιμετώπισης απρόοπτων καταστάσεων.**
- **Έλεγχος στην περίπτωση εισαγωγής νέων χρηστών και εφαρμογών.**
- **Έλεγχος της απόδοσης και της αναβάθμισης ενός δικτύου.**

Τα βασικά στοιχεία του COMNET III που χρησιμοποιούνται για την δημιουργία ενός μοντέλου προσομοίωσης χωρίζονται σε 8 βασικές κατηγορίες:

1. **Τοπολογία δικτύου (Network Topology) :** Η τοπολογία δικτύου περιγράφει τη δομή και τις συσκευές από τις οποίες αποτελείται το φυσικό μας δίκτυο. Περιλαμβάνει τους **κόμβους (nodes)**, που αναπαριστούν τον hardware εξοπλισμό (υπολογιστές, switches, routers, hubs, πολυπλέκτες), **τις συνδέσεις (links)** που αναπαριστούν το μέσο μετάδοσης των δεδομένων μεταξύ των κόμβων και τα **ports** που αναπαριστάνουν τις θύρες με τις οποίες συνδέονται οι κόμβοι με τα links.

Επιπλέον υπάρχουν δύο ακόμη στοιχεία τα οποία είναι τα υποδίκτυα (subnets) που αναπαριστούν τα ανεξάρτητα routing domains στην περίπτωση πολύπλοκων δικτύων και το WAN cloud που χρησιμοποιείται για την μοντελοποίηση Wide Area Networks.

2. **Κίνηση στο δίκτυο και φόρτος εργασίας (Network Traffic and Workload) :** Η κίνηση στο δίκτυο αναφέρεται στα μηνύματα που μεταδίδονται μεταξύ των κόμβων στο δίκτυο, ενώ ο φόρτος εργασίας αναφέρεται στην εσωτερική δραστηριότητα ενός κόμβου. Οι **application sources (πηγές εφαρμογών)** εκτελούν εντολές που δημιουργούν κίνηση στο δίκτυο ή φόρτο εργασίας στο εσωτερικό του κόμβου, ενώ οι **traffic sources (πηγές κίνησης)** δημιουργούν κίνηση μεταξύ των κόμβων.

3. **Λειτουργία δικτύου (Network Operation) :** Η Network Operation καθορίζει πόσα μηνύματα δρομολογούνται μέσω του δικτύου με έναν αλγόριθμο

δρομολόγησης (Routing Algorithm) και πόσα μεταδίδονται μέσω του δικτύου με ένα πρωτόκολλο μεταφοράς (Transport Protocol).

4. **Έλεγχος προσομοίωσης (Simulation Control) :** Όταν ένα μοντέλο είναι έτοιμο, το COMNET III ελέγχει την ορθότητα και την πληρότητα του πριν ξεκινήσει την εξομοίωση. Τη δυνατότητα αυτή μπορεί να την χρησιμοποιήσει ο χρήστης και κατά την διάρκεια κατασκευής του μοντέλου χωρίς να είναι απαραίτητη η προσομοίωσή του. Κατά τη διάρκεια της προσομοίωσης ο χρήστης βλέπει με γραφικό τρόπο πακέτα να μεταφέρονται ανάμεσα στους κόμβους και στα Links.

5. **Στατιστικές αναφορές (Statistics Reporting) :** Ο κύριος στόχος της δημιουργίας ενός μοντέλου στο COMNET III είναι τα αποτελέσματα που παίρνουμε προσομοιώνοντας το μοντέλο αυτό. Τα reports παράγονται αυτόματα κατά την διάρκεια ή μετά το τέλος της προσομοίωσης. Ο διαχειριστής του δικτύου μπορεί να επιλέξει, ανάλογα με τα στοιχεία του δικτύου που τον ενδιαφέρουν, τα reports που θέλει να μελετήσει, μειώνοντας έτσι τον χρόνο που απαιτείται για να ολοκληρωθεί η προσομοίωση.

6. **Κατανομές του χρήστη (User Distributions) :** Στην προσομοίωση ενός δικτύου με την βοήθεια του COMNET III, η πλειονότητα των χαρακτηριστικών οποιουδήποτε κόμβου, traffic sources ή εφαρμογής μπορεί να περιγραφή είτε από μια στατιστική κατανομή είτε από μια σταθερή κατανομή. Η μέθοδος με την οποία το COMNET III επιλέγει τιμές από μια κατανομή όταν προσομοιώνει ένα μοντέλο βασίζεται στην δημιουργία τυχαίων αριθμών. Μια γεννήτρια ψευδο-τυχαίων αριθμών, δημιουργεί τυχαίους αριθμούς. Ένας αρχικός παράγοντας χρησιμοποιείται για να παράγει έναν τυχαίο αριθμό ανάμεσα στο διάστημα 0-1 και τον επόμενο παράγοντα. Ο νέος παράγοντας που δημιουργείται, χρησιμοποιείται για να παράγει τον επόμενο τυχαίο αριθμό και τον επόμενο παράγοντα. Για να έχουμε πολλαπλές ανεξάρτητες γεννήτριες αριθμών, κάθε κατανομή έχει την δυνατότητα να ορίζει έναν αριθμό ροής (stream number). Μέχρι 99 διαφορετικά streams μπορούν να χρησιμοποιηθούν σε ένα μοντέλο. Κάθε stream έχει τον δικό του αρχικό παράγοντα έτσι, ώστε να δημιουργούνται διαφορετικοί τυχαίοι αριθμοί από οποιοδήποτε άλλο stream. Στην συνέχεια χρησιμοποιούνται συναρτήσεις βαρύτητας (weighting functions) που διαχειρίζονται τους τυχαίους αριθμούς που προήλθαν από την ομοιόμορφη (0,1) κατανομή, για να δημιουργήσουν την επιθυμητή κατανομή. Παρακάτω αναφέρονται μερικές κατανομές που χρησιμοποιούνται στο COMNET III και οι παράμετροι που χρησιμοποιούνται για να ορίσουν την επιθυμητή διαμόρφωση κατανομής:

- **Beta (Βήτα):** Προσαρμοσμένη 1, Προσαρμοσμένη 2, Ελάχιστη, Μέγιστη, Συνεχής.
- **Erlang:** Μέση, Προσαρμοσμένη, Συνεχής.
- **Exponential (Εκθετική):** Μέση, Συνεχής.
- **Gamma (Γάμα):** Μέση, Προσαρμοσμένη, Συνεχής.
- **Geometric (Γεωμετρική):** Ελάχιστη, Μέση, Συνεχής.
- **Hyper-exponential (Υπερεκθετική):** Μέση 1, Μέση 2, Πιθ. Μέση 1, Συνεχής.
- **Ακέραια:** Ελάχιστη, Μέση, Συνεχής.
- **Lognormal (Κανονική Εκθετική):** Μέση, Τυπική απόκλιση, Συνεχής.
- **Normal (Κανονική):** Μέση, Τυπική απόκλιση, Συνεχής.
- **Poisson:** Μέση, Συνεχής.
- **Triangular (Τριγωνική):** Ελάχιστη, Mode, Μέγιστη, Συνεχής
- **Uniform (Ομοιόμορφη):** Προσαρμοσμένη, Κλιμακωτή, Συνεχής.

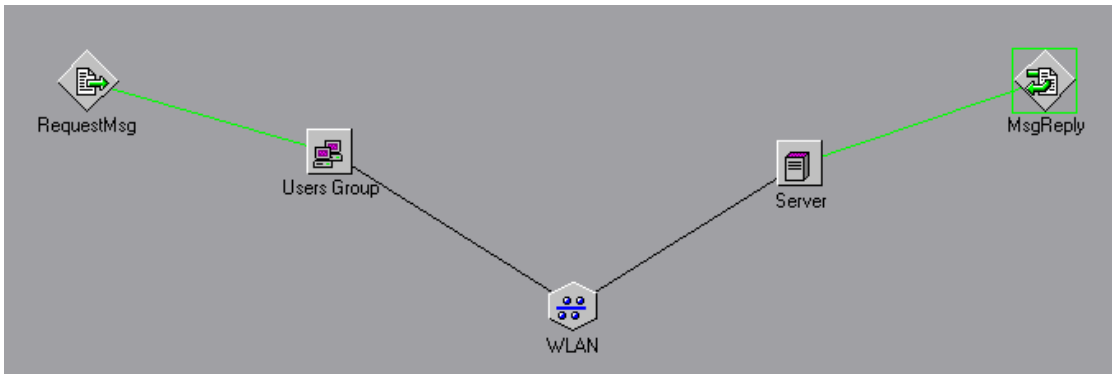
7. **Βιβλιοθήκες (Libraries) :** Το COMNET III περιλαμβάνει μια πλούσια βιβλιοθήκη μοντέλων δικτυακών συσκευών, συνδέσεων, αλγορίθμων

δρομολόγησης και πρωτοκόλλων μεταφοράς. Τα στοιχεία αυτά είτε μπορούν να χρησιμοποιηθούν απευθείας στην δημιουργία νέων μοντέλων, είτε να τροποποιηθούν ώστε να ικανοποιήσουν τις απαιτήσεις του προς μοντελοποίηση συστήματος.

8. **Αρχεία μοντέλων (Model Files) :** Το COMNET III αποθηκεύει το μοντέλο που δημιουργεί ο χρήστης σε δυαδική μορφή. Εάν χρησιμοποιήσουμε μια άλλη υπολογιστική πλατφόρμα, θα πρέπει να μετατρέψουμε το αρχείο μοντέλου σε ASCII μορφή. Επίσης, υπάρχει η δυνατότητα μετατροπής των reports σε αρχεία που μπορούν να εισαχθούν σε κάποια spreadsheet εφαρμογή, όπως είναι το Microsoft Excel.

7.2 Περιγραφή μοντέλου

Το δίκτυο που κατασκευάστηκε για την προσομοίωση είναι ένα ασύρματο δίκτυο αρχιτεκτονικής ad-hoc, που χρησιμοποιεί το πρωτόκολλο επικοινωνίας 802.11. Ως πρωτόκολλο στρώματος μεταφοράς χρησιμοποιήθηκε το TCP/IP. Στην εικόνα 49 φαίνεται και σχηματικά το δίκτυο.



Εικόνα 49. Το μοντέλο δικτύου που χρησιμοποιήθηκε στην προσομοίωση.

Το δίκτυο αποτελείται από τους χρήστες που μοντελοποιήθηκαν ως μια ομάδα κόμβων (users group), οι οποίοι κυμαίνονται από 1 έως 30 και έναν εξυπηρετητή (server), που επικοινωνούν με την τεχνική CSMA/CA μέσω του πρωτοκόλλου IEEE 802.11. Το εύρος ζώνης του είναι 2 Mbps. Κάθε χρήστης θα δημιουργεί ένα μήνυμα (αίτηση μεταφοράς αρχείου – RequestMsg) που θα έχει προορισμό τον server. Όταν ο server λάβει την αίτηση, θα πρέπει ν' απαντήσει σε αυτή με ένα αρχείο απάντησης (MsgReply), που θ' απευθύνεται στον αντίστοιχο χρήστη (κόμβο). Το μέγεθος της αίτησης είναι 1000 bytes. Το μέγεθος της απάντησης κυμαίνεται από 1 έως 5 MB.

Η επιλογή του μεταβαλλόμενου αριθμού χρηστών έγινε για να δούμε με ποιο τρόπο αποκρίνεται ένα ad-hoc δίκτυο τόσο για μικρή χρησιμοποίηση (1-5 χρήστες) όσο και για μεγάλη (>20 χρήστες), ενώ το μέγεθος του αρχείου επιλέχθηκε έτσι ώστε να αντιπροσωπεύει ένα αρχείο που διακινείται συχνά μέσω του Internet (ένα μικρής διάρκειας τραγούδι ή ένα video λίγων δευτερολέπτων).

7.2.1 1^{ο} σενάριο προσομοίωσης

Στην περίπτωση αυτή η προσομοίωση πραγματοποιήθηκε με αριθμό χρηστών 1, 5, 10, 15, 20, 25 και 30. Η διάρκεια της προσομοίωσης είναι 60 sec.

Για την αίτηση μεταφοράς αρχείου οι παράμετροι που δόθηκαν είναι οι εξής:

Ο χρονοπρογραμματισμός έγινε σύμφωνα με την επιλογή Iteration time. Κάθε ένα δευτερόλεπτο δημιουργείται ένα μήνυμα.

- Scheduled by: Iteration time
- Interarrival time: 1.0 (First and Last arrival=0)

Το μέγεθος της αίτησης είναι 1000 bytes.

- Message size calc: Probability Distribution
- Probability Distribution: 1000

Σαν προορισμό της αίτησης μεταφοράς αρχείου, επιλέξαμε τον server.

- Destinations: Random List (server)

Το πρωτόκολλο μεταφοράς που χρησιμοποιήθηκε είναι το TCP/IP MicrosoftV1.0.

- Packet/Protocol: TCP/IP MicrosoftV1.0

Για την ομάδα χρηστών:

Χρησιμοποιήθηκε το computer group. Οι τιμές που δόθηκαν είναι 1, 5, 10, 15, 20, 25 και 30 και αποτελούν την κύρια μεταβαλλόμενη παράμετρο του πρώτου σεναρίου προσομοίωσης.

Για το ασύρματο δίκτυο (WLAN):

Χρησιμοποιήθηκε το CSMA/CA με παραμέτρους που καθορίζονται από το IEEE 802.11. το εύρος ζώνης είναι 2 Mbps.

Για τον server:

Για τον server χρησιμοποιήθηκε ένας processing node κόμβος.

Για την απάντηση του sever στις αιτήσεις μεταφοράς αρχείου οι παράμετροι που δόθηκαν είναι οι εξής:

Ο χρονοπρογραμματισμός στηρίζεται στη λήψη μηνυμάτων από τους χρήστες.

- Edit received messages

Το μέγεθος του αρχείου είναι 1000 bytes:

- Message size calc: Probability Distribution
- Probability Distribution: 1000

Προορισμός των μηνυμάτων είναι οι χρήστες.

Το πρωτόκολλο μεταφοράς που χρησιμοποιήθηκε είναι το TCP/IP MicrosoftV1.0.

- Packet/Protocol: TCP/IP MicrosoftV1.0

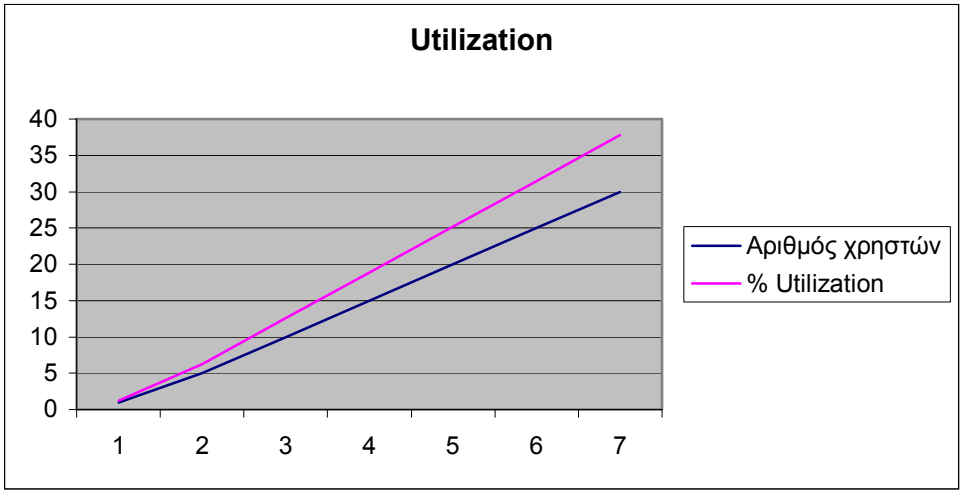
Οι κυριότεροι παράγοντες αξιολόγησης του δικτύου είναι οι εξής:

- Η επί τοις εκατό χρησιμοποίηση του δικτύου (Utilization), η οποία προκύπτει από το πηλίκο των bits που μεταφέρθηκαν, προς τα bits που μπορεί να μεταφέρει το δίκτυο.
- Η ωφέλιμη ταχύτητα μεταφοράς (Throughput) του δικτύου, η οποία προκύπτει από το πηλίκο του μεγέθους του αρχείου που μεταφέρθηκε, προς το χρόνο μεταφοράς.
- Ο αριθμός συκρούσεων των πακέτων (Collision episodes).

Τα αποτελέσματα της προσομοίωσης είναι τα εξής:

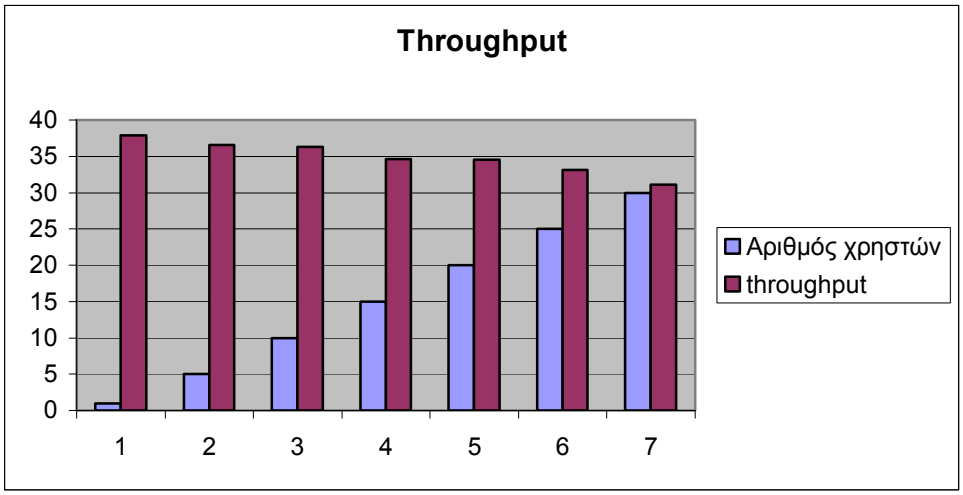
Αριθμός χρηστών	**% Utilization**	**Throughput (kbps)**	**Collision episodes**
1	1,257	37,9	0
5	6,296	36,6	0
10	12,59	36,3	0
15	18,89	34,6	21
20	25,19	34,5	16
25	31,49	33,1	61
30	37,79	31,1	108

Στη συνέχεια παρουσιάζονται οι γραφικές παραστάσεις με τις βασικότερες παραμέτρους των αποτελεσμάτων της προσομοίωσης:

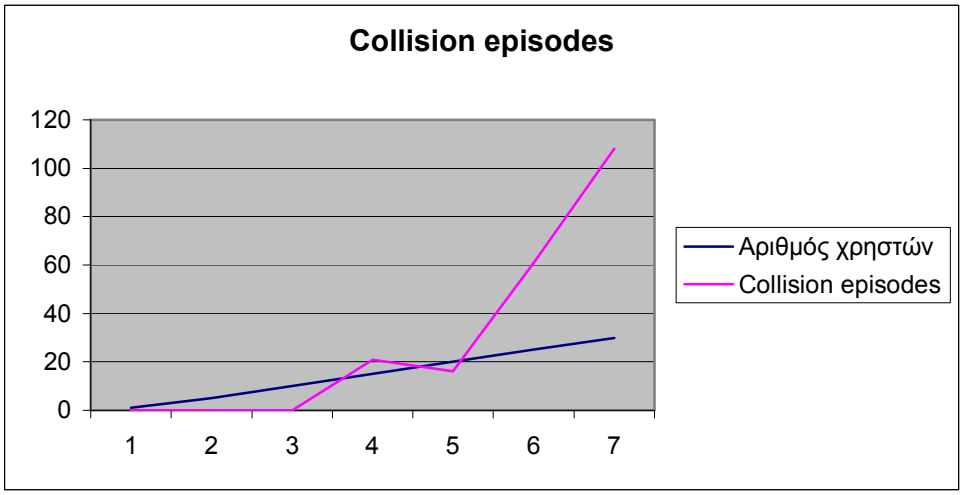


Η χρησιμοποίηση του καναλιού κυμαίνεται μεταξύ 1,2 και 37,7% και βλέπουμε ότι αυξάνεται όσο αυξάνονται και οι χρήστες. Αυτό είναι αναμενόμενο, αφού όταν

έχουμε περισσότερους χρήστες, δημιουργούνται και περισσότερα πακέτα τα οποία πρέπει να διακινηθούν μέσα από το κανάλι.



Η ωφέλιμη ταχύτητα μεταφοράς κυμαίνεται μεταξύ 37 και 31 Kbps. Παρατηρούμε ότι μειώνεται με την αύξηση των χρηστών στο δίκτυο.



Όσο πιο πολλούς χρήστες έχουμε, τόσο αυξάνεται η πιθανότητα συγκρούσεων των πακέτων. Επίσης παρατηρούμε ότι όταν ο αριθμός των χρηστών ξεπερνάει τους 20, τότε οι συγκρούσεις αυξάνονται κατακόρυφα.

7.2.2 2^{ο} σενάριο προσομοίωσης

Στην περίπτωση αυτή η προσομοίωση πραγματοποιήθηκε με σταθερό αριθμό χρηστών ίσο με 5. Η διάρκεια της προσομοίωσης είναι 60 sec. Η μεταβαλλόμενη παράμετρος είναι το μέγεθος του αρχείου απάντησης, το οποίο κυμαίνεται μεταξύ 1 και 5 MB.

Για την αίτηση μεταφοράς αρχείου οι παράμετροι που δόθηκαν είναι οι εξής:

Ο χρονοπρογραμματισμός έγινε σύμφωνα με την επιλογή Iteration time. Κάθε ένα δευτερόλεπτο δημιουργείται ένα μήνυμα.

- Scheduled by: Iteration time
- Interarrival time: 1.0 (First and Last arrival=0)

Το μέγεθος της αίτησης είναι 1000 bytes.

- Message size calc: Probability Distribution
- Probability Distribution: 1000

Σαν προορισμό της αίτησης μεταφοράς αρχείου, επιλέξαμε τον server.

- Destinations: Random List (server)

Το πρωτόκολλο μεταφοράς που χρησιμοποιήθηκε είναι το TCP/IP MicrosoftV1.0.

- Packet/Protocol: TCP/IP MicrosoftV1.0

Για την ομάδα χρηστών:

Χρησιμοποιήθηκε το computer group. Οι τιμή που δόθηκε είναι 5 χρήστες και διατηρείται σταθερή.

Για το ασύρματο δίκτυο (WLAN):

Χρησιμοποιήθηκε το CSMA/CA με παραμέτρους που καθορίζονται από το IEEE 802.11. το εύρος ζώνης είναι 2 Mbps.

Για τον server:

Για τον server χρησιμοποιήθηκε ένας processing node κόμβος.

Για την απάντηση του sever στις αιτήσεις μεταφοράς αρχείου οι παράμετροι που δόθηκαν είναι οι εξής:

Ο χρονοπρογραμματισμός στηρίζεται στη λήψη μηνυμάτων από τους χρήστες.

- Edit received messages

Το μέγεθος του αρχείου είναι 1, 2, 3, 4 και 5MB:

- Message size calc: Probability Distribution
- Probability Distribution: 1000, 2000, 3000, 4000, 5000

Προορισμός των μηνυμάτων είναι οι χρήστες.

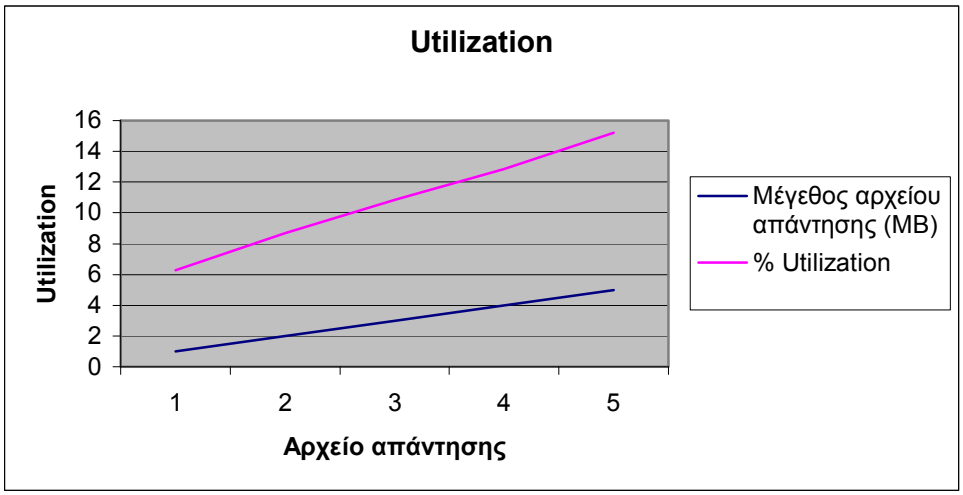
Το πρωτόκολλο μεταφοράς που χρησιμοποιήθηκε είναι το TCP/IP MicrosoftV1.0.

- Packet/Protocol: TCP/IP MicrosoftV1.0

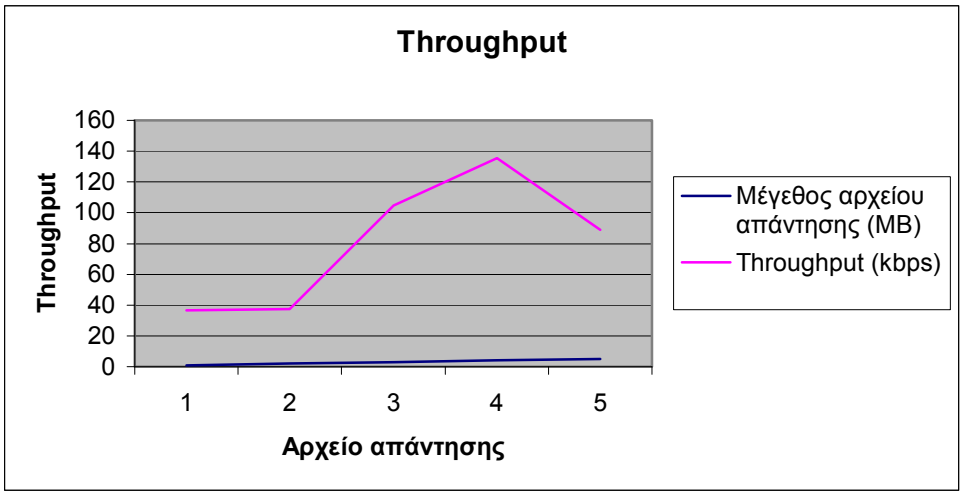
Τα αποτελέσματα της προσομοίωσης είναι τα εξής:

Μέγεθος αρχείου απάντησης (MB)	% Utilization	Throughput (kbps)	Collision episodes
1	6,296	36,6	0
2	8,670	37,6	0
3	10,85	104,8	0
4	12,83	135,5	10
5	15,20	88,8	22

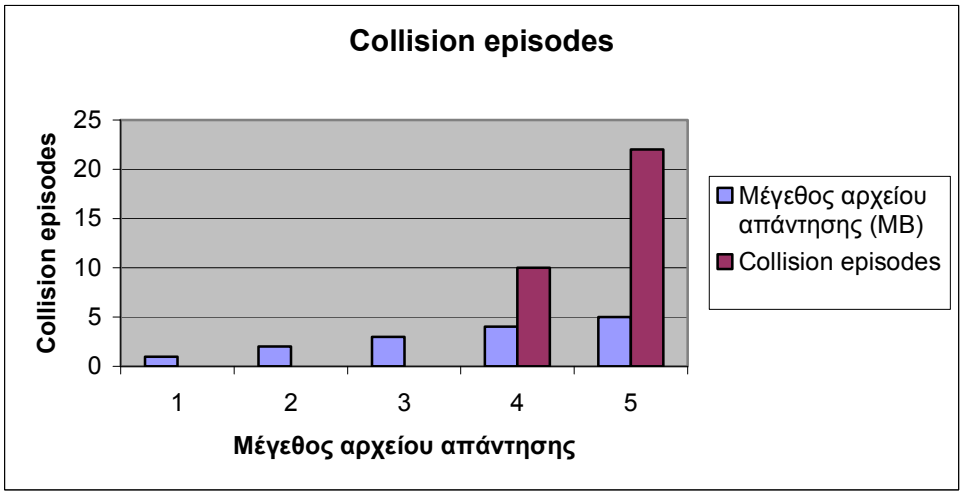
Στη συνέχεια παρουσιάζονται οι γραφικές παραστάσεις με τις βασικότερες παραμέτρους των αποτελεσμάτων της προσομοίωσης:



Εδώ, η χρησιμοποίηση του καναλιού κυμαίνεται μεταξύ 6,2 και 15,2% και βλέπουμε ότι αυξάνεται όσο αυξάνετα το μέγεθος του αρχείου απάντησης. Αυτό είναι αναμενόμενο, αφού το μέγιστο μέγεθος πλαισίου που επιτρέπει το πρωτόκολλο του 802.11 να μεταδοθεί, είναι 2.304 bytes. Κάθε αίτηση χρήστη μεταφέρεται αυτούσια μέσα σ' έναι πλαίσιο TCP/IP, αφού είναι μόνο 1000 bytes. Όταν όμως απαντάει ο server, αφού το μέγεθος της απάντησης είναι μεγαλύτερο από 2 MB, τότε το αρχείο αυτό κατακερματίζεται σε πακέτα ίσα με το μέγιστο μέγεθος πλαισίου που ορίζει τι πρωτόκολλο μεταφοράς. Όταν όλα τα πακέτα φτάσουν στον παραλήπτη, τότε αυτός τα συναρμολογεί για να δημιουργήσει το αρχικό αρχείο απάντησης. Αυτό σημαίνει ότι αφού τα αρχείο των 2, 3, 4 και 5 MB τεμαχίζονται σε μικρότερα πακέτα, με αποτέλεσμα το δίκτυο να έχει περισσότερα πακέτα να διακινήσει.



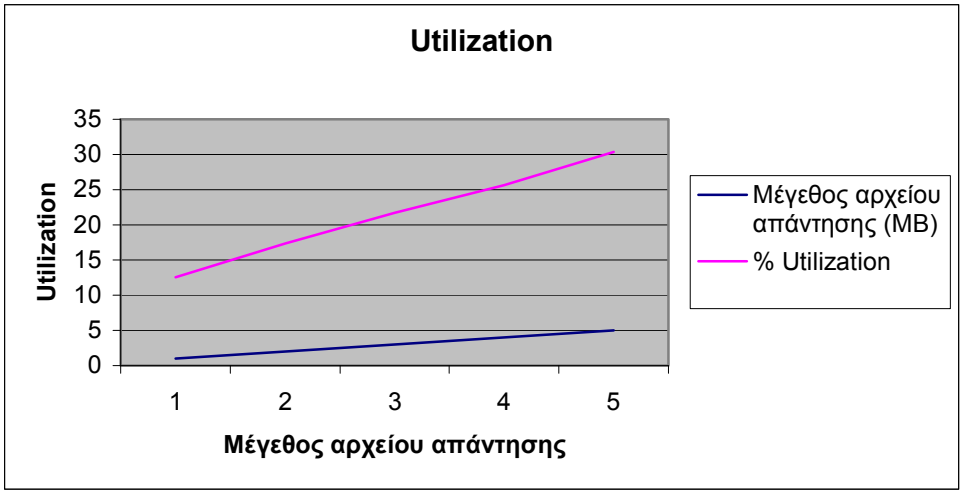
Η ωφέλιμη ταχύτητα μεταφοράς κυμαίνεται μεταξύ 36 και 135 Kbps. Παρατηρούμε ότι για αρχεία μεγέθους 1 έως 2 MB είναι σταθερή, ενώ για αρχεία άνω των 2 MB είναι πολύ μεγαλύτερη. Για αρχεία μεγαλύτερα από 5 MB μειώνεται, αφού αυξάνονται και οι συκγρούσεις και παρατηρούμε ότι πέφτει η απόδοση του δικτύου.



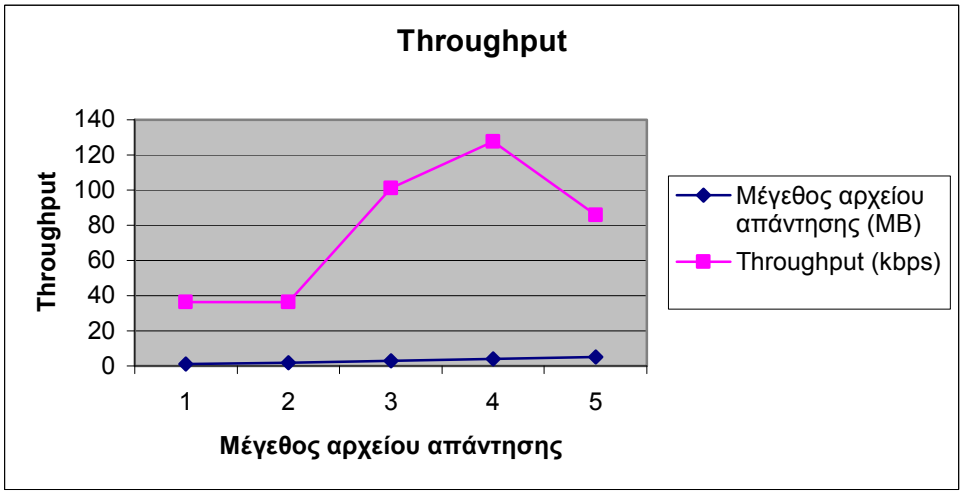
Για το λόγο που εξηγήσαμε παραπάνω, αφού έχουμε περισσότερα πακέτα στο δίκτυο, θα έχουμε και μεγαλύτερο αριθμό συκρούσεων. Αφού έχουμε μικρό αριθμό χρηστών, δεν έχουμε συκρούσεις για αρχεία μεγέθους 1, 2 και 3 MB. Όταν όμως το μέγεθός τους ξεπερνάει τα 3 MB, τότε έχουμε ένα μικρό αριθμό συγκρούσεων.

Στη συνέχεια αυξάνουμε τον αριθμό των χρηστών σε 10, διατηρώντας τον σταθερό καθώς το μέγεθος αρχείου παίρνει τις τιμές 1, 2, 3, 4 και 5MB.
Τα αποτελέσματα της προσομοίωσης είναι τα εξής:

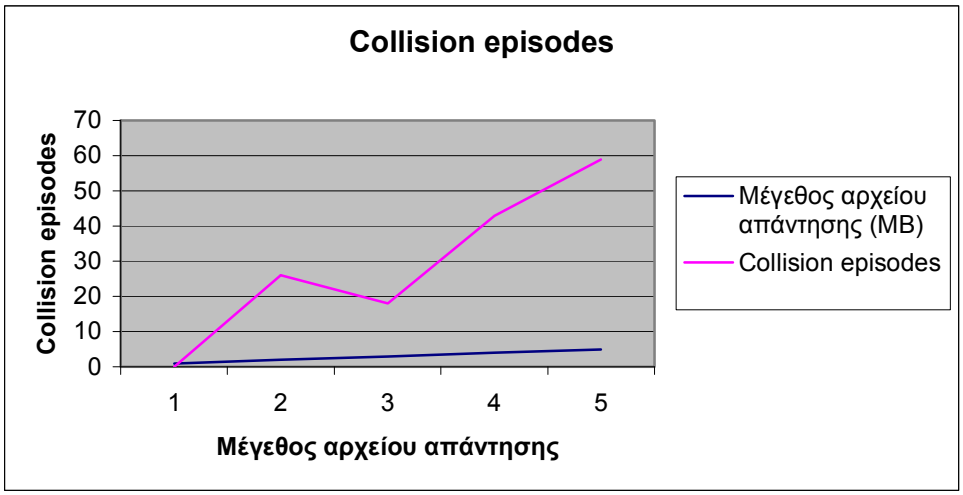
Μέγεθος αρχείου απάντησης (MB)	% Utilization	Throughput (kbps)	Collision episodes
1	12,59	36,36	0
2	17,34	36,28	26
3	21,70	101,26	18
4	25,67	127,49	43
5	30,40	85,836	59



Εδώ, η χρησιμοποίηση του καναλιού κυμαίνεται μεταξύ 12,5 και 30,4% και βλέπουμε ότι αυξάνεται όσο αυξάνετα το μέγεθος του αρχείου απάντησης. Αρκετά μεγάλος αριθμός σε σχέση με τις προηγούμενες περιπτώσεις.



Η ωφέλιμη ταχύτητα μεταφοράς κυμαίνεται μεταξύ 36 και 127 Kbps. Παρατηρούμε ότι για αρχεία μεγέθους 1 έως 2 MB είναι σταθερή, ενώ για αρχεία άνω των 2 MB είναι πολύ μεγαλύτερη. Για αρχεία μεγαλύτερα από 5 MB μειώνεται, αφού αυξάνονται και οι συκγρούσεις και παρατηρούμε ότι πέφτει η απόδοση του δικτύου.



Για το λόγο που εξηγήσαμε παραπάνω, αφού έχουμε περισσότερα πακέτα στο δίκτυο, θα έχουμε και μεγαλύτερο αριθμό συκρούσεων. Με 10 χρήστες στο δίκτυο, δεν έχουμε συκρούσεις για αρχεία μεγέθους 1 MB. Όταν όμως το μέγεθός τους ξεπερνάει το 1 MB, τότε έχουμε μεγάλο αριθμό συγκρούσεων, ειδικά όταν το μέγεθος του αρχείου ξεπερνά τα 4 MB.

7.2.3 Συμπεράσματα προσομοίωσης

Τα συμπεράσματα των προσομοιώσεων αυτών είναι τα εξής:

Καταρχήν παρατηρούμε ότι η ωφέλιμη ταχύτητα μεταφοράς δεν φτάνει σε καμία περίπτωση τα 2 Mbps, που είναι θεωρητικά η μέγιστη ταχύτητα που προσφέρει το κανάλι. Αυτό συμβαίνει επειδή στο κανάλι υπάρχουν συγκρούσεις και επειδή υπάρχουν τα bytes επιβάρυνσης (overhead), τα οποία προστίθενται σε κάθε πλαίσιο. Επίσης βλέπουμε ότι η ωφέλιμη ταχύτητα μεταφοράς μειώνεται με την αύξηση του φόρτου του ad-hoc δικτύου, πράγμα αναμενόμενο αφού έτσι έχουμε περισσότερες συγκρούσεις και περισσότερες καθυστερήσεις στο κανάλι.

Η χρησιμοποίηση του καναλιού αυξάνεται όταν αυξάνεται ο φόρτος του καναλιού, όταν δηλ. έχουμε περισσότερους χρήστες, επειδή το κανάλι επιβαρύνεται με επιπρόσθετα πακέτα έναρξης και λήξης μιας σύνδεσης, εξαιτίας της χρήσης του πρωτοκόλλου TCP/IP. Αντίθετα, η ωφέλιμη ταχύτητα μεταφοράς μειώνεται με την αύξηση του φόρτου του δικτύου. Αυτό επιβεβαιώνεται και από άλλες προσομοιώσεις ασύρματων 802.11 δικτύων, σύμφωνα με τις οποίες, η αύξηση του φόρτου αρχικά οδηγεί σε μεγάλη αύξηση του throughput και στη συνέχεις σε μεγάλη μείωση των τιμών του.

Βλέπουμε ότι το δίκτυο λειτουργεί καλύτερα με μικρό αριθμό χρηστών. Εναλλακτικά μπορεί να λειτουργήσει με μεγαλύτερο αριθμό χρηστών, χωρίς όμως αυτοί να ξεπερνούν τους 20, εφ’ όσον το μέγεθος του αρχείου απάντησης είναι μικρό (δεν ξεπερνάει δηλ. τα 2 MB). Διαφορετικά έχουμε πολλές συγκρούσεις, ενώ ταυτόχρονα μειώνεται η ωφέλιμη ταχύτητα μεταφοράς, που σημαίνει ότι δεν έχουμε καλή απόδοση του δικτύου. Αυτό συμβαίνει επειδή η αύξηση των χρηστών και του φόρτου στο δίκτυο, έχουν σαν αποτέλεσμα την αύξηση του μέσου χρόνου που μεσολαβεί μεταξύ της δημιουργίας διαδοχικών πακέτων. Έτσι ο ρυθμός μετάδοσης των πακέτων μειώνεται.

Γενικά, στα ασύρματα δίκτυα, είναι προτιμότερο να χρησιμοποιούνται αρχεία μικρού μεγάθους. Η χρησιμοποίηση πακέτων μεγάλου μεγέθους είναι χρήσιμη μόνο σε πριπτώσεις που υπάρχει ανάγκη μεταφοράς μεγάλου αριθμού πληροφορίας.

Σύμφωνα και με άλλες προσομοιώσεις ad-hoc δικτύων, στα οποία το μέγεθος πακέτου ήταν σταθερό (αλλά μικρότερο των 2 MB), η επίδραση της αύξησης του αριθμού των κόμβων είναι η μείωση του throughput μετά από κάποιο σημείο φόρτου του δικτύου.

Βιβλιογραφία

[1] Δίκτυα Υπολογιστών : Andrew S. Tanenbaum, 4η Αμερικάνικη έκδοση, εκδόσεις Κλειδάριθμος.
[2] Προσομοίωση δικτύων υπολογιστών : Ανδρέας Πομπόρτσης, Ανέστης Τσουλφάς, εκδόσεις Τζιόλα.
[3] Ad Hoc Networking : C. Perkins, ISBN 0201309769
[4] Θέματα δρομολόγησης σε Ad-hoc τηλεπικοινωνιακά δίκτυα : Μεταπτυχιακή εργασία, Εμμανουήλ Γ. Σπανάκης.

Δικτυακές πηγές

[1] http://de.teikav.edu.gr/telematics/pdf/asyrmata.pdf: Σημειώσεις για το μάθημα της Τηλεματικής, "Τεχνολογίες σύγχρονων ασύρματων δικτύων δεδομένων", Κωνσταντίνος Γεωργακόπουλος.
[2] http://www.eng.auburn.edu/users/lim/wireless.html: Wireless Mobile Networks.
[3] http://en.wikipedia.org/wiki: Δικτυακός τόπος όπου δίνονται συνοπτικές πληροφορίες σχετικά με οποιοδήποτε θέμα.
[4] http://www.conta.uom.gr: Δικτυακός τόπος του πανεπιστημίου Μακεδονίας.
- Διαφάνειες για το μάθημα Vehicular Networks, Βερόνικα Ιωάννου.
- Ασύρματα Δίκτυα Υπολογιστών - Κεφάλαιο 1.htm.
- Ασύρματα Δίκτυα Υπολογιστών - Κεφάλαιο 2.htm.

[5] http://www.ceid.upatras.gr: Πανεπιστήμιο Πατρών, intro.pdf, σημειώσεις για τα πρωτόκολλα δρομολόγησης για ad hoc networks.
[6] http://xanthippi.ceid.upatras.gr/courses/mobile/Presentations/Lecture3.ppt: Ασύρματα Ad-hoc δίκτυα.
[7] http://www.eng.ucy.ac.cy/gellinas/ECE460_Lecture1.pdf: Σημειώσεις στο μάθημα Προχωρημένα δίκτυα υπολογιστών, Γ. Έλληνας και Χ Παναγιώτου.
[8] http://www.eng.ucy.ac.cy/christos/courses/ECE654/Lectures/Routing.ppt: Δρομολόγηση.
[9] http://www.netmode.ntua.gr/courses/postgraduate/Ad-Hoc_Networks/2007/Set1.pdf: Ad-hoc Networks, Συμεών Παπαβασιλείου.
[10] http://www.patraswireless.net/tutorial/basic%20tutorial/tut-network/ieee_802_11b.htm: Πληροφορίες για την οικογένεια προτύπων 802.11.
[11] http://inf-server.inf.uth.gr/courses/CE522/mpc_fall07/lectures /mpc_fall07_lec09_3in1.pdf: Πανεπιστήμιο Θεσσαλίας, σημειώσεις στο μάθημα Κινητός και Διάχυτος Υπολογισμός, Δημήτριος Κατσαρός.
[12] http://research.microsoft.com: Επίσημη σελίδα της Microsoft.
[13] http://ieeexplore.ieee.org: Επίσημη σελίδα του οργανισμού ieee.
[14] http://www.oreillynet.com/pub/a/wireless/2004/01/22/wirelessmesh.html: Ιστοσελίδα που αναφέρεται στα ασύρματα δίκτυα mesh.
[15] www.comsoc.org/pubs/surveys: A SURVEY OF INTEGRATING IP MOBILITY PROTOCOLS AND MOBILE AD HOC NETWORKS, FEKRI M. ABDULJALIL, SHRIKANT K. BODHE.