



ΤΕΙ ΗΠΕΙΡΟΥ

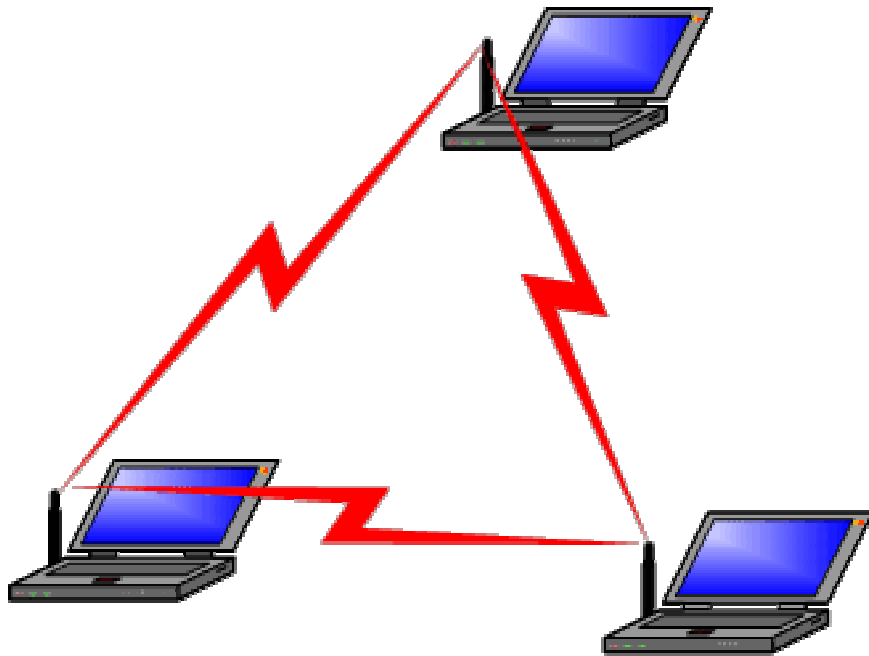
Τμήμα: Τηλεπληροφορικής και Διοίκησης

ΕΠΙΣΚΟΠΗΣΗ ΤΩΝ AD HOC ΔΙΚΤΥΩΝ

Ροκόπουλος Παναγιώτης
Κουκαλιώτης Παναγιώτης

ΕΠΙΣΚΟΠΗΣΗ ΤΩΝ AD HOC ΔΙΚΤΥΩΝ

23 ΙΟΥΝΙΟΥ 2006



ΡΟΚΟΠΟΥΛΟΣ ΠΑΝΑΓΙΩΤΗΣ

ΚΟΥΚΑΛΙΩΤΗΣ ΠΑΝΑΓΙΩΤΗΣ



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕΡΟΣ ΤΩΝ ΑΠΑΙΤΗΣΕΩΝ ΤΟΥ ΤΜΗΜΑΤΟΣ
ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΔΗΛΩΣΗ ΠΕΡΙ ΛΟΓΟΚΛΟΠΗΣ

Όλες οι προτάσεις οι οποίες παρουσιάζονται σε αυτό το κείμενο και οι οποίες ανήκουν σε άλλους αναγνωρίζονται από τα εισαγωγικά και υπάρχει η σαφής δήλωση του συγγραφέα. Τα υπόλοιπα γραφόμενα είναι επινόηση του γράφοντος ο οποίος φέρει και την καθολική ευθύνη γι' αυτό το κείμενο και δηλώνω υπεύθυνα ότι δεν υπάρχει λογοκλοπή γι' αυτό το κείμενο.

Ονοματεπώνυμο.....
.....

Υπογραφή..... Ημερομηνία.....

ΕΙΣΑΓΩΓΗ

Ασύρματα Δίκτυα(Wireless Networks).....	1
Ασύρματα δίκτυα: Επικοινωνία χωρίς καλώδια.....	1
Υπάρχουν οι εξής τρόποι σύνδεσης:.....	2
Πλεονεκτήματα από τη χρήση ασύρματων τοπικών δικτύων.....	3
Παρά τα πλεονεκτήματα αυτά, η υλοποίηση ασύρματων δικτύων υπόκειται σε κάποιους περιορισμούς.	4
Χρήση ασύρματων τοπικών δικτύων	4
ΕΦΑΡΜΟΓΕΣ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ.....	5
1.2.1 ΕΠΕΚΤΑΣΗ ΤΟΠΙΚΟΥ ΔΙΚΤΥΟΥ	5
1.2.2 ΔΙΑ-ΚΤΙΡΙΑΚΗ ΔΙΑΣΥΝΔΕΣΗ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ	7
1.2.3 ΝΟΜΑΔΙΚΗ ΠΡΟΣΒΑΣΗ	7
1.2.4 ΔΙΚΤΥΩΣΗ ΕΙΔΙΚΟΥ ΣΚΟΠΟΥ (Ad Hoc Networking).....	8

ΚΕΦΑΛΑΙΟ 1

Τα Ad_Hoc Δίκτυα.....	10
1. Ας δούμε λοιπόν τι είναι Ad Hoc τρόπος(Ασύρματα Δίκτυα Ad_Hoc) στην ασύρματη δικτύωση.....	11
2. Μοντέλο Λειτουργίας	14

2.1	Η ανάλυση στηρίζεται στα παρακάτω χαρακτηριστικά:	15
2.2	Συγκεκριμένα, τα μοντέλα λειτουργίας Ad_Hoc Δικτύων που προτείνουμε είναι:.....	16
2.2.1	Συμμετρικές Ζεύξεις	16
2.2.2	Λύσεις Ad Hoc Επιπέδου 2	16
2.2.3	Πολυεκπομπή (multicast)	17
3	Ασύρματες λύσεις.....	17
4	Πλεονεκτήματα και μειονεκτήματα που εξετάζουν.....	19
5.	VITAN – Εργαλείο απεικόνισης για τα Ad Hoc δίκτυα.....	21
	Συμπεράσματα.....	22

ΚΕΦΑΛΑΙΟ 2

	ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΔΡΟΜΟΛΟΓΗΣΗ.....	23
2.1	ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ ΤΩΝ AD HOC ΔΙΚΤΥΩΝ.....	24
2.2	ΣΤΟΧΟΙ ΠΡΩΤΟΚΟΛΛΩΝ ΕΙΔΙΚΩΝ ΔΙΚΤΥΩΝ.....	24
2.3	Οι τρεις αλγόριθμοι δρομολόγησης.....	25
2.3.1	Table-driven Προσεγγίσεις	26
2.3.2	Source initiated/On demand Προσεγγίσεις	30
2.3.3	ΥΒΡΙΔΙΚΟ	38
	Συμπεράσματα και μελλοντική έρευνα.....	40

ΚΕΦΑΛΑΙΟ 3

	AD HOC ΠΡΟΔΙΑΓΡΑΦΕΣ	41
--	---------------------------	----

3.1. IEEE 802.11	41
3.1.1. Βασικές Ιδέες	42
3.1.2. Επίπεδα, Υπηρεσίες και Ενότητες	43
3.1.3. IEEE 802.11 ως Ad Hoc Δίκτυο	46
3.2. HIPERLAN/2	47
3.2.1. Το Δίκτυο HIPERLAN/2	48
3.2.2. Χαρακτηριστικά Στοιχεία του HIPERLAN/2	49
3.2.3. Τρόπος Λειτουργίας του Δικτύου	51
3.2.3.1. Παραδείγματα Εφαρμογών	53
3.2.3.2. Απόδοση	54
3.2.4. HIPERLAN/2 ως Ad Hoc Δίκτυο	54
3.3. BLUETOOTH	55
3.3.1. Βασική Αρχιτεκτονική Συστήματος	56
3.3.2. Εγκατάσταση Συνδέσεων	60
Συμπεράσματα	62
ΚΕΦΑΛΑΙΟ 4	
ΑΣΦΑΛΕΙΑ	
4.1 Τα Ad Hoc ασύρματα δίκτυα.....	63
4.2 Οι περιορισμοί συστημάτων	63
4.3.Η διαθεσιμότητα.....	64
4.3.1. Το ράδιο μπλοκάρισμα.....	64
4.3.2. Εξαγωγή μπαταριών.....	64
4.4. Η αυθεντικότητα.....	65

4.4.1. Παροδική Σύνδεση.....	65
4.4.2. Πολιτική ασφάλειας	66
4.5. Η ακεραιότητα.....	66
4.6. Τα Ad Hoc δίκτυα παρέχουν την ασύρματη επικοινωνία στους κινητούς hosts (που καλούμε κόμβους).....	67
4.6.1. Η ασφάλεια	68
4.6.2. Οι προκλήσεις	69
4.7. Εμπιστοσύνη και βασική διανεμημένη διαχείριση	70
4.7.1. Εμπιστοσύνη στα Ad Hoc δίκτυα.....	70
4.8. Το σύστημα & ο αντίπαλος.....	72
4.9. Επιθέσεις στα Ad Hoc δίκτυα.....	73
4.10. Εξασφάλιση AODV.....	74
4.10.1. Μια ασφαλής κατόπιν παραγγελίας δρομολόγηση πρωτόκολλο για τα Ad Hoc δίκτυα.....	74
4.11. SEAD σε κινητά ασύρματα Ad Hoc δίκτυα.....	75
 ΚΕΦΑΛΑΙΟ 5	
ΕΦΑΡΜΟΓΕΣ.....	76
5.1. Οι εφαρμογές Ad Hoc δικτύων	76
5.2. ΕΦΑΡΜΟΓΕΣ BLUETOOTH	77
5.3. ΕΦΑΡΜΟΓΕΣ HIPERLAN/2 – HIPERSPOT	78
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	79

ΠΑΡΑΡΤΗΜΑ

ΔΙΑΜΟΡΦΩΣΗ ΤΩΝ AD_HOC ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΝΔΕΣΗ ΤΟΥΣ ΜΕ ΤΟ ΔΙΑΔΙΚΤΥΟ.....81

1 Αυτή η διαμόρφωση προϋποθέτει την εξής υποδομή81

2 Τα βήματα που θα πρέπει να ακολουθήσουμε για τη διαμόρφωση της ειδικής διανομής Διαδικτύου είναι τα ακόλουθα:.....82

2.1. Σύνδεση του οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων με το Διαδίκτυο.....83

2.2. Ρυθμίστε τον υπολογιστή σας έτσι ώστε ο οικοδεσπότης υπολογιστής, να μοιράζεται τη σύνδεση με το Διαδίκτυο, με άλλους χρήστες του ειδικού δικτύου.84

2.3. Δημιουργία ενός ειδικού ασύρματου δικτύου στον οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων.....85

2.4. Σύνδεση με το νέο ειδικό ασύρματο δίκτυο από τους άλλους υπολογιστές lap-top. (σύνδεση χρηστών).....87

ΕΙΣΑΓΩΓΗ

Ασύρματα Δίκτυα(Wireless Networks)

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

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

Με αρχιτεκτονική παραπλήσια ενός ενσύρματου δικτύου λοιπόν και με το πλεονέκτημα της σύνδεσης του χρήστη ενώ βρίσκεται σε κίνηση, τα ασύρματα τοπικά δίκτυα καθιερώθηκαν γρήγορα σε μια πλειάδα εφαρμογών. Η πραγματική, όμως, έκρηξη της χρήσης των WLANs θα προέλθει από την ολοένα αυξανόμενη παρουσία τους στο καθημερινό περιβάλλον εργασίας των επιχειρήσεων. Με ασύρματη διασύνδεση στο υπάρχον ενσύρματο δίκτυο, οι εργαζόμενοι μπορούν να λάβουν και να στείλουν email ή να συνδεθούν στο εταιρικό intranet γρήγορα και εύκολα από οπουδήποτε μέσα στην εταιρία.

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

Ασύρματα δίκτυα: Επικοινωνία χωρίς καλώδια

Σε όλα τα νέα πρότυπα ασύρματων δικτύων, εκτός από το πρότυπο IRDA (Infrared Data Association), το οποίο ούτως ή άλλως δεν αφορά ασύρματα δίκτυα αλλά ασύρματη επικοινωνία, δεν απαιτείται οπτική επαφή. Σε κάθε ασύρματο δίκτυο υπάρχουν δύο μέρη: η ασύρματη κάρτα δικτύου (wireless LAN adapter), η οποία επικοινωνεί είτε με άλλες συσκευές που έχουν ασύρματη κάρτα δικτύου, είτε με τον πομποδέκτη-κόμβο (Access Point) που λειτουργεί και ως γέφυρα με το ενσύρματο δίκτυο. Τα AP (ACCESS POINT) είναι απλές συσκευές που συνδέονται με το ενσύρματο δίκτυο της εταιρείας, το ISP ή το

οικιακό δίκτυο. Ο ρόλος τους είναι η ασύρματη αποστολή και λήψη δεδομένων. Πρόκειται για ειδικές συσκευές, που διαθέτουν θύρα Ethernet και λειτουργούν κατά κάποιον τρόπο όπως τα hub, παρέχοντας όμως κάποιες επιπλέον δυνατότητες. Έχουν μεγαλύτερη ακτίνα δράσης από τις απλές ασύρματες κάρτες, επεκτείνοντας έτσι την εμβέλεια του ασύρματου δικτύου. Αυτό, με απλά λόγια σημαίνει ότι, αν δύο κόμβοι βρίσκονται έξω από την ακτίνα δράσης τους, είναι δυνατόν να επικοινωνήσουν μέσω του σημείου πρόσβασης. Επιπλέον, τα Access Points ελέγχουν την κίνηση του δικτύου, κατανέμουν ανάλογα με τον αριθμό των υπολογιστών το διαθέσιμο εύρος και φροντίζουν να κατευθύνουν τα πακέτα πληροφοριών. Για την εμβέλεια τους ισχύει ότι και για τις απλές ασύρματες κάρτες, ενώ ο αριθμός των κόμβων που μπορούν να "σηκώσουν" εξαρτάται από τον κατασκευαστή. Με τον τρόπο αυτό, και χωρίς τη χρήση καλωδίων, επιτυγχάνεται η διασύνδεση όλων των υπολογιστικών συστημάτων του χώρου.

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



Εικόνα 1: ΚΑΡΤΑ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ



Εικόνα 2: ACCESS POINT

Η εμβέλεια των ασύρματων καρτών και συσκευών εξαρτάται από πολλές παραμέτρους: από την ποιότητα κατασκευής του προϊόντος (κυρίως από τον πομποδέκτη που ενσωματώνουν), από την τεχνολογία μετάδοσης που χρησιμοποιείται, από τον περιβάλλοντα χώρο και από την ταχύτητα μετάδοσης των δεδομένων. Οποιαδήποτε στιγμή βρεθούν δύο ή περισσότεροι υπολογιστές στην ακτίνα δράσης των ασύρματων καρτών τους, αυτόματα συνθέτουν ένα ομότιμο δίκτυο (peer to peer). Αυτή είναι και η απλούστερη μορφή ενός ασύρματου δικτύου, η οποία εξυπηρετεί περιορισμένες ανάγκες και τη συναντάμε περισσότερο στα οικιακά δίκτυα ή σε μικρά δίκτυα στο γραφείο. Όλοι οι υπολογιστές σε ένα ομότιμο δίκτυο έχουν τα ίδια δικαιώματα και μοιράζονται εξίσου τους πόρους του δικτύου.

Υπάρχουν οι εξής τρόποι σύνδεσης:

Σχετικά με τη δόμηση των δικτύων, να αναφέρουμε ότι υπάρχουν **δύο κύριοι τρόποι σύνδεσης**:

- **Peer-to-Peer:** Χωρίς access point και χωρίς κεντρικό σημείο διαχείρισης. Δίκτυα τέτοιου τύπου είναι κατάλληλα για μικρές εταιρείες ή για οικιακή χρήση. Η καλυπτόμενη

περιοχή (Basic Service Area ή BSA) καταλαμβάνει μια ακτίνα περίπου 100 μέτρων και υποστηρίζει από 6 έως 25 χρήστες.

- **Infrastructure wireless network:** Περιλαμβάνει access point. Η πλειοψηφία των δικτύων στήνεται με AP, καθώς έτσι εξασφαλίζεται μεγαλύτερη ευελιξία στην εγκατάσταση και τη διαχείριση. Η καλυπτόμενη περιοχή εδώ εξαρτάται από την εμβέλεια του εκάστοτε access point ή από την ύπαρξη περισσότερων του ενός σημείων πρόσβασης στον χώρο λειτουργίας (Extended Service Area ή ESA).

Πλεονεκτήματα από τη χρήση ασύρματων τοπικών δικτύων

Το κατεξοχήν πλεονέκτημα που παρέχει ένα ασύρματο δίκτυο στους χρήστες του είναι η δυνατότητα πρόσβασης, σε πραγματικό χρόνο, σε βάσεις δεδομένων, ακόμη και αν εκείνοι βρίσκονται εν κινήσει. Μάλιστα, η προσβασιμότητα από παντού των δικτυακών πόρων μιας εταιρείας ή επιχείρησης, για παράδειγμα, διευκολύνει το έργο των υπαλλήλων, εκείνοι με τη σειρά τους αποδίδουν καλύτερα και έτσι αυξάνεται η παραγωγικότητα.

Όσον αφορά στην **εγκατάσταση** ενός WLAN, να διευκρινίσουμε ότι αυτή απαιτεί ελάχιστο χρόνο. Επιπλέον, είναι **αρκετά εύκολη** ως διαδικασία, αφού εδώ, σε αντίθεση με τα ενσύρματα δίκτυα, ούτε προβλήματα καλωδίωσης συναντάμε ούτε λαμβάνεται υπ' όψη η κτηριακή δομή.

Φτάνουμε τώρα στο κρίσιμο ερώτημα: θα υπάρξει **οικονομικό όφελος** από μια τέτοια εγκατάσταση; Η απάντηση είναι καταφατική. Μπορεί το αρχικό κόστος για τον εξοπλισμό ενός ασύρματου τοπικού δικτύου να είναι συγκριτικά ακριβότερο από αυτό ενός ενσύρματου, ωστόσο τα **οφέλη** είναι **μακροπρόθεσμα**. Αυτό συμβαίνει κυρίως σε περιπτώσεις δυναμικών χώρων εργασίας που απαιτούν συχνές αλλαγές, καθώς το κόστος επαναδιαμόρφωσης του προϋπάρχοντος ασύρματου δικτύου θα είναι αμελητέο.

Ο εξοπλισμός που χρησιμοποιείται είναι εντελώς ακίνδυνος για τον ανθρώπινο οργανισμό. Η ακτινοβολία είναι μη ιονίζουσα και τα επίπεδα ακτινοβολίας είναι πολύ πιο χαμηλά από τα επιτρεπτά για τον ανθρώπινο οργανισμό όρια. Αρκεί να αναφέρουμε ότι μια ασύρματη κάρτα δικτύου (802.11b) ακτινοβολεί ισχύ 50 - 100 mwatt, ενώ ένα κινητό τηλέφωνο φτάνει και τα 2000 mwatt.

Παρά τα πλεονεκτήματα αυτά, η υλοποίηση ασύρματων δικτύων υπόκειται σε κάποιους περιορισμούς.

Ας εξετάσουμε, όμως, και ποιες αδυναμίες παρουσιάζουν τα WLANs.

- Καταρχάς, τα ασύρματα δίκτυα **υστερούν** στον τομέα παρεχόμενης **ασφάλειας**, καθώς υπάρχουν πολλοί τρόποι επίθεσης από επίδοξους εισβολείς. Ασφάλεια επένδυσης: Σήμερα είναι διαθέσιμο στην αγορά ένα μεγάλο εύρος λύσεων, αλλά μόνο λίγες από αυτές θα σημειώσουν εμπορική επιτυχία μεσαίου μεγέθους. Αν η ασφάλεια επένδυσης είναι πρωταρχικής σημασίας, η κατάσταση αυτή μπορεί να καθυστερήσει αποφάσεις για μελλοντικές επενδύσεις.

- Επιπλέον, τα ασύρματα τοπικά δίκτυα, κυρίως όσα βρίσκονται σε ζώνες χαμηλής συχνότητας, είναι **ευάλωτα στις παρεμβολές**. Τα ασύρματα LANs μεταφέρουν δεδομένα μέσω του αέρα. Σε αντίθεση με τα ενσύρματα δίκτυα, χρησιμοποιούν ένα κοινό μέσο, γνωστό ως διαμοιραζόμενο μέσο, με την αίσθηση ότι, όχι μόνο οι σταθμοί ενός καναλιού, αλλά και διαφορετικά κανάλια και τεχνολογίες έχουν πρόσβαση στο ίδιο, διαμοιραζόμενο μέσο. Οι τελευταίες ενδέχεται να οφείλονται στην ύπαρξη γειτονικών ηλεκτρονικών συσκευών (για παράδειγμα, ασύρματα τηλέφωνα στα 900 MHz ή φούρνοι μικροκυμάτων στα 2.4 GHz), αλλά ακόμη και στην ίδια τη γεωμετρία του χώρου λειτουργίας..
- Η **χαμηλή, σχετικά, ταχύτητα ανταλλαγής δεδομένων** και το **υψηλό**, προς το παρόν, **κόστος** του **εξοπλισμού** αποτελούν δύο ακόμη μειονεκτήματα. Ωστόσο, είναι θέμα χρόνου να βελτιωθεί η κατάσταση προς όφελος των χρηστών και να επεκταθεί η χρήση των WLANs. Η αλλαγή αυτή θα επέλθει φυσιολογικά ως απόρροια του αυξημένου ανταγωνισμού των κατασκευαστριών εταιρειών αλλά και εξαιτίας της επικράτησης στην αγορά συμβατών προϊόντων που θα συνεργάζονται μεταξύ τους (interoperable).
- Η εμβέλεια των ασύρματων συστημάτων είναι αρκετά περιορισμένη σε πολλές περιπτώσεις και η λειτουργικότητα που αναμένεται από τους χρήστες είτε δεν μπορεί να επιτευχθεί, ή μπορεί να επιτευχθεί σε περιορισμένη έκταση.
- Ηλεκτρομαγνητική ακτινοβολία: Αν και η ισχύς των κυμάτων που χρησιμοποιούνται από τα ασύρματα τοπικά δίκτυα είναι μόλις το 5% της ισχύος των σημάτων των κινητών τηλεφώνων, αυξάνεται η ηλεκτρομαγνητική επιβάρυνση του περιβάλλοντος.

Χρήση ασύρματων τοπικών δικτύων

Ενδεικτικά, τα ασύρματα δίκτυα μπορούν να χρησιμοποιηθούν μέσα στο χώρο μιας επιχείρησης, μιας σχολικής μονάδας, μιας δημόσιας υπηρεσίας, κλπ., για:

- Επικοινωνία των υπολογιστών χωρίς τη χρήση και το κόστος της δομημένης καλωδίωσης
- Επέκταση του ήδη υπάρχοντος δικτύου με αμελητέο κόστος και υποδομή
- Χρήση ασύρματης τηλεφωνίας μέσα από το ήδη υπάρχον ασύρματο δίκτυο
- Επισκόπηση χώρων χρησιμοποιώντας ασύρματες κάμερες
- Ως hotspot.:

Το hotspot είναι ένα ασύρματο σημείο πρόσβασης στο internet. Στην πραγματικότητα, δεν είναι απλώς ένα σημείο, αλλά μια περιοχή η οποία καλύπτεται από συσκευές που επιτρέπουν και διαχειρίζονται την ασύρματη πρόσβαση των χρηστών στο internet. Ένα hotspot μπορεί να έχει εμβέλεια από μερικά μέτρα και να φτάσει ακόμη και το ένα χιλιόμετρο κάλυψης, αν αυτό είναι επιθυμητό. Ένας χρήστης, εκμεταλλευόμενος τις δυνατότητες που του παρέχει η ασύρματη σύνδεση του με το hotspot, είναι σε θέση να πραγματοποιήσει στον υπολογιστή του

οποιαδήποτε εργασία έχει σχέση με το internet σαν να ήταν στο σπίτι του ή στο γραφείο του. Ήδη τέτοια σημεία εντοπίζονται σε εστιατόρια, καφέ, ξενοδοχεία, πανεπιστήμια, βιβλιοπωλεία, αεροδρόμια (ένα από αυτά είναι και το **Διεθνές Αεροδρόμιο Αθηνών** «Ελευθέριος Βενιζέλος», όπου, σε συνεργασία με την ΟΤΕnet, παρέχεται δωρεάν δοκιμαστική πρόσβαση), νοσοκομεία, γραφεία –ακόμη και πάρκα! Συνήθως, υπάρχει άμεση χρέωση του χρήστη κάθε φορά που συνδέεται στο Διαδίκτυο. Άλλοτε, πάλι, πληρώνει μηνιαίο πάγιο, ενώ σε άλλες περιπτώσεις είναι δωρεάν. Σίγουρα, οι δυνατότητες που προκύπτουν για τις επιχειρήσεις μέσω των hot spots είναι απεριόριστες. Μην ξεχνάμε ότι επενδύοντας στα WLANs καταφέρνουν να επεκτείνουν την πελατεία τους, αλλά και να αυξήσουν τα έσοδά τους προσφέροντας διάφορες online υπηρεσίες. Ο χρήστης του hotspot μπορεί να το χρησιμοποιήσει για τις ακόλουθες εργασίες: Πλοήγηση στο Διαδίκτυο (web surfing) , Ανταλλαγή αρχείων και online επικοινωνία μεταξύ των χρηστών, Πρόσβαση σε εφαρμογές πολυμεσικού περιεχομένου (multimedia), για τη λήψη εικόνων, βίντεο και μουσικής. Λήψη ενημερωτικού ή εκπαιδευτικού περιεχομένου.

ΕΦΑΡΜΟΓΕΣ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Τέσσερις περιοχές εφαρμογής των ασύρματων τοπικών δικτύων είναι:

- Η χρήση τους ως η επέκταση ενός τοπικού δικτύου
- Η χρήση τους στη διασύνδεση τοπικών δικτύων που βρίσκονται σε διαφορετικά κτίρια
- Η νομαδική πρόσβαση και
- Η δικτύωση Ad Hoc

1.2.1 ΕΠΕΚΤΑΣΗ ΤΟΠΙΚΟΥ ΔΙΚΤΥΟΥ

Παλαιότερα, τα ασύρματα τοπικά δίκτυα θεωρούνταν ως ένα *υποκατάστατο* των τοπικών δικτύων με καλώδιο. Με ένα ασύρματο τοπικό δίκτυο αποφεύγονται τα διάφορα έξοδα που σχετίζονται με την εγκατάσταση της καλωδίωσης και παράλληλα διευκολύνονται οι λειτουργίες της αναδιάρθρωσης - ανακατάταξης της δικτυακής υποδομής (όταν βέβαια αυτή χρειάζεται να λάβει χώρα).

Ωστόσο, αυτό το πολύ σημαντικό κίνητρο για τη χρήση των ασύρματων τοπικών δικτύων επικαλύφθηκε από μια σειρά άλλων γεγονότων. Καταρχήν, καθώς η ανάγκη για τοπική δικτύωση γινόταν ολοένα και μεγαλύτερη, τα νέα κτίρια σχεδιάζονταν με τέτοιο τρόπο ώστε να μπορούν να συμπεριλάβουν επιπλέον καλωδίωση για εφαρμογές δεδομένων. Επίσης, με την εξέλιξη της τεχνολογίας στη μετάδοση των δεδομένων,

άρχισε να υπάρχει μια αυξανόμενη εμπιστοσύνη στην καλωδίωση συνεστραμμένου ζεύγους (twisted pair) και ειδικά στην ποιότητα κατηγορίας 3, από την οποία τα περισσότερα (και ειδικά τα παλαιότερα) κτίρια διέθεταν αρκετή. Κατά συνέπεια, η χρήση των ασύρματων τοπικών δικτύων ως αντικαταστάτες των τοπικών δικτύων με καλώδιο δε γνώρισε μεγάλη αποδοχή.

Εν τούτοις, υπάρχουν και μερικά περιβάλλοντα στα οποία τα ασύρματα τοπικά δίκτυα αποτελούν καλύτερη λύση από ένα δίκτυο με καλώδιο. Στην κατηγορία αυτή ανήκουν:

- Περιβάλλοντα μεγάλων εκτάσεων, όπως οι χώροι παραγωγής ενός εργοστασίου ή μιας αποθήκης.
- Πολύ παλιά κτίρια, στα οποία είτε το άνοιγμα τρυπών στους τοίχους απαγορεύεται, είτε η καλωδίωση είναι ανεπαρκής ή ανύπαρκτη.
- Μικρά γραφεία, όπου η εγκατάσταση και η συντήρηση ενός δικτύου με καλώδιο είναι αντισυμβαλλόμενη.

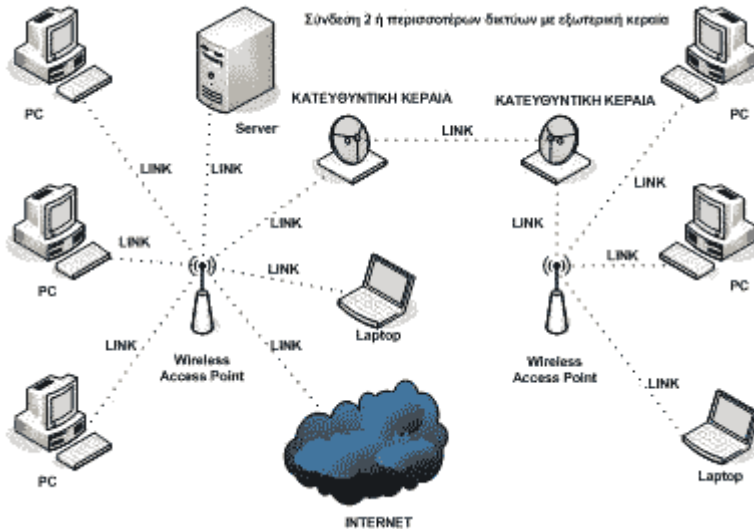
Σε όλες αυτές τις περιπτώσεις, ένα ασύρματο δίκτυο αποτελεί μια αποδοτική και ελκυστική εναλλακτική λύση. Στις περισσότερες από αυτές τις περιπτώσεις, θα υπάρχει επίσης και ένα δίκτυο με καλώδιο το οποίο θα πρέπει να διασυνδεθεί με ένα ασύρματο δίκτυο. Για παράδειγμα, είναι πολύ συνηθισμένο μια εργοστασιακή επιχείρηση να αποτελείται από ένα χώρο γραφείων, ο οποίος βρίσκεται ξεχωριστά από το χώρο παραγωγής, αλλά πρέπει να είναι συνδεδεμένος με αυτόν, έτσι ώστε να παρέχονται δικτυακές υπηρεσίες στο προσωπικό (π.χ. παρακολούθηση των χώρων λειτουργίας από τον επόπτη, ηλεκτρονική διαχείριση της αποθήκης κλπ). Μια τυπική λύση στην περίπτωση αυτή είναι η σύνδεση ενός ενσύρματου με ένα ασύρματο τοπικό δίκτυο, με το πρώτο να βρίσκεται στο χώρο των γραφείων και το δεύτερο στο χώρο της παραγωγής. Ο τύπος αυτός της εφαρμογής των ασύρματων τοπικών δικτύων αναφέρεται ως *επέκταση τοπικού δικτύου*.

1.2.2 ΔΙΑ-ΚΤΙΡΙΑΚΗ ΔΙΑΣΥΝΔΕΣΗ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Μία άλλη χρήση των ασύρματων τοπικών δικτύων βρίσκεται στη σύνδεση τοπικών δικτύων (ασύρματων ή μη) που βρίσκονται σε διπλανά κτίρια. Στην περίπτωση αυτή, χρησιμοποιείται μια ασύρματη σύνδεση από σημείο-σε-σημείο (wireless point-to-point

link) μεταξύ των δύο κτιρίων. Οι συσκευές που συνήθως διασυνδέονται είναι γέφυρες ή δρομολογητές. Σε πολλές περιπτώσεις και παρά τον συγκριτικά ακριβότερο εξοπλισμό η χρήση ασύρματου δικτύου ενδέχεται να μειώσει σημαντικά το κόστος δικτύωσης.

π.χ.:



Εικόνα 3: WAN (Εξωτερική δικτύωση)

WAN : Αν μία επιχείρηση καταλαμβάνει περισσότερα από ένα κτίρια, είναι θεμιτή η επικοινωνία μεταξύ των δικτύων τους. Η χρήση ασύρματου Link κοστίζει όσο και ο απαιτούμενος εξοπλισμός (Hardware) ενώ η χρήση μιας μισθωμένης γραμμής (leased line) δημιουργεί ένα μηνιαίο κόστος αρκετά υψηλό.

Σημείωση : Σε αυτή την περίπτωση απαιτείτε οπτική επαφή μεταξύ των σημείων που θέλουμε συνδέσουμε.

1.2.3 ΝΟΜΑΔΙΚΗ ΠΡΟΣΒΑΣΗ

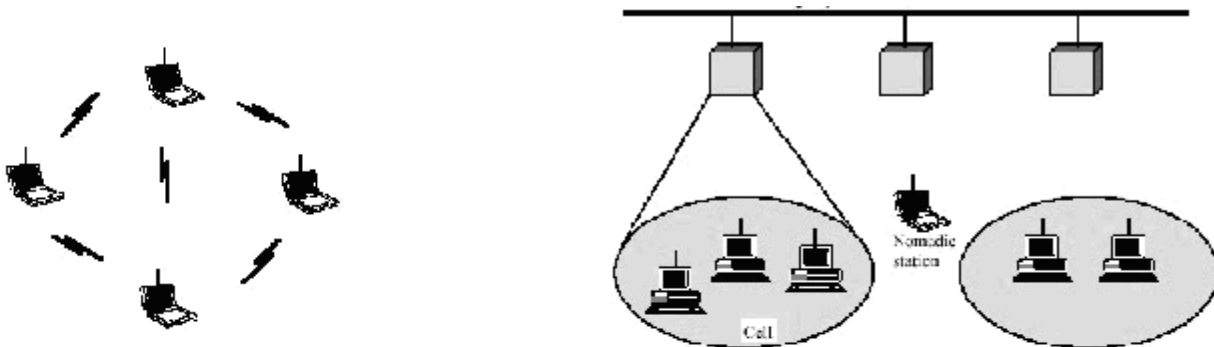
Η νομαδική πρόσβαση παρέχει μία ασύρματη σύνδεση μεταξύ ενός τοπικού δικτύου και ενός φορητού υπολογιστή, ο οποίος είναι εξοπλισμένος με μια κεραία, όπως είναι ένα laptop ή ένα notepad. Ένα παράδειγμα χρήσης μιας τέτοιου είδους σύνδεσης είναι να μπορεί ένας υπάλληλος που γυρίζει από ένα ταξίδι να μεταφέρει πληροφορίες από τον προσωπικό του υπολογιστή στον υπολογιστή στο γραφείο του. Η νομαδική πρόσβαση είναι επίσης χρήσιμη και σε χώρους όπως μια επιχείρηση, ή μια πανεπιστημιούπολη, στους οποίους τα κτίρια βρίσκονται συγκεντρωμένα ανά ομάδες. Στις περιπτώσεις αυτές, οι χρήστες μπορούν να μετακινούνται μέσα στο χώρο της επιχείρησης ή του

πανεπιστημίου και με τους φορητούς υπολογιστές τους να προσπελαίνουν αρχεία των servers και των υπολογιστών που βρίσκονται συνδεδεμένοι σε κάποιο τοπικό δίκτυο.

1.2.4 ΔΙΚΤΥΩΣΗ ΕΙΔΙΚΟΥ ΣΚΟΠΟΥ (Ad Hoc Networking)

Μία ακόμη χρήση των ασύρματων δικτύων είναι εκείνη της δικτύωσης ειδικού σκοπού ή αλλιώς της Ad Hoc Networking, η οποία θα αποτελέσει και το αντικείμενο της παρούσας εργασίας. Στην περίπτωση αυτή δεν υπάρχει κάποιος κεντρικός υπολογιστής που να διαχειρίζεται το δίκτυο, αλλά απλά οι υπολογιστές είναι συνδεδεμένοι ο ένας με τον άλλο. Δίκτυα τέτοιου είδους συνήθως εγκαθίστανται προσωρινά και έχουν ως σκοπό την εξυπηρέτηση μιας άμεσης ανάγκης. Για παράδειγμα, μπορούμε να σκεφτούμε την περίπτωση όπου μια ομάδα υπαλλήλων συνδέουν τους φορητούς υπολογιστές τους, ώστε να εξυπηρετηθούν οι ανάγκες μιας on-line σύσκεψης ή παρουσίασης, όπου σε έναν υπολογιστή θα γίνεται η παρουσίαση και οι υπόλοιποι θα μπορούν να την παρακολουθούν από τους προσωπικούς τους υπολογιστές.

Στο παρακάτω σχήμα απεικονίζονται ένα ασύρματο δίκτυο ειδικού σκοπού (Ad Hoc Wireless LAN) και ένα ασύρματο δίκτυο το οποίο υποστηρίζει LAN extension και νομαδική πρόσβαση.



Εικόνα 5: ασύρματο δίκτυο το οποίο υποστηρίζει LAN extension και νομαδική πρόσβαση.

Εισάγουμε την έννοια των ad hoc δικτύων, εστιάζουμε στην σπουδαιότητα και σημασία τους στην εξέλιξη των δικτύων τρίτης γενιάς και παρουσιάζουμε με

λεπτομέρεια τις σύγχρονες εφαρμογές τους. Η εφαρμογή των ad hoc δικτύων έρχεται να ικανοποιήσει τις απαιτήσεις μιας εξελισσόμενης κοινωνίας όπου οι υπηρεσίες κινητών επικοινωνιών οφείλουν να παρέχονται στον καταναλωτή χωρίς περιορισμούς και δυσκολίες.

Οι ρίζες της ειδικής δικτύωσης μπορούν να επισημανθούν πίσω μέχρι το 1968, όταν άρχισε η εργασία για το δίκτυο ALOHA (ο στόχος αυτού του δικτύου ήταν να συνδεθούν οι εκπαιδευτικές εγκαταστάσεις στη Hawaii). Αν και οι σταθεροί σταθμοί υιοθετήθηκαν, το πρωτόκολλο ALOHA παραχωρήθηκε στη διανεμημένη διαχείριση πρόσβασης καναλιών και ως εκ τούτου παρείχε μια βάση για την επόμενη ανάπτυξη των διανεμημένων σχεδίων κανάλι-πρόσβασης που ήταν κατάλληλα για την Ad Hoc δικτύωση.

ΚΕΦΑΛΑΙΟ 1

«Τα Ad_Hoc Δίκτυα»

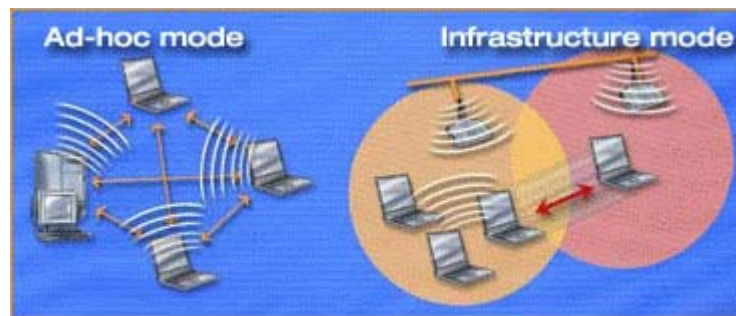
Το υπουργείο άμυνας των ΗΠΑ άρχισε το 1973 την εργασία, για το PRnet (πακέτο ράδιο τεχνολογίας). Οι κόμβοι θα συνεργάζοντουσαν ώστε να φθάσουν τα πακέτα στους απόμακρους σταθμούς. Είναι μια τεχνολογία που επιτρέπει, ασύρματη δικτύωση στα περιβάλλοντα όπου δεν υπάρχει καμία συνδεδεμένη με καλώδιο ή κυψελοειδής υποδομή (π.χ., πεδίο μάχη, αποκατάσταση καταστροφής, κλπ.) ή, εάν υπάρχει μια υποδομή, δεν είναι επαρκές ή οικονομικώς αποδοτικό. Τα ασύρματα κινητά δίκτυα και οι συσκευές γίνονται όλο και περισσότερο δημοφιλή δεδομένου ότι παρέχουν την πρόσβαση χρηστών στην ενημέρωση και την επικοινωνία οποτεδήποτε και οπουδήποτε.

Τα τελευταία χρόνια, η χρήση προσωπικών υπολογιστών από κινούμενους χρήστες παρουσιάζει ιδιαίτερη αύξηση. Η συνεχόμενη σμίκρυνση των συσκευών και η αύξηση της υπολογιστικής ισχύος των κινητών υπολογιστών (lap-tops), συνδυάζονται έτσι ώστε να δώσουν τη δυνατότητα καλύτερων εφαρμογών σε ένα αυξανόμενο τμήμα του πληθυσμού. Έτσι οι αγορές ασύρματων τηλεφώνων και άλλων τηλεπικοινωνιακών συσκευών παρουσιάζουν σημαντική μεγέθυνση. Το κυριότερο μέρος της εν λόγω μεταστροφής έχει να κάνει με τη διατήρηση της επαφής με το Internet. Αυτή η ταχύτατη τεχνολογική πρόοδος έχει ωθήσει σε εξίσου εντυπωσιακή ανάπτυξη στη ζήτηση για σύνδεση στο δίκτυο κινητών χρηστών. Είναι πιθανό να θέλουμε άμεσα να χρησιμοποιήσουμε ένα χάρτη για να εντοπίσουμε τι είναι διαθέσιμο στη συγκεκριμένη περιοχή. Επίσης, είναι πιθανό να θέλουμε να μας αποσταλούν οδηγίες κατεύθυνσης από κάποιο δικτυακό τόπο, οι οποίες θα βασίζονται στις πληροφορίες που προέρχονται από το σύστημα GPS που είναι εγκατεστημένο στο αυτοκίνητο. Μπορεί λοιπόν κανείς να έχει πρόσβαση σε διάφορες εφαρμογές-εργασίες, είτε είναι στην εργασία, στο σπίτι, σε κίνηση. Ο συνδυασμός γρήγορων και φθηνών ασύρματων ζεύξεων με επίσης φθηνές συσκευές κινητών υπολογιστών, κάνουν σήμερα πραγματικότητα όλα τα παραπάνω. Στο μέλλον, ο μέσος ταξιδιώτης θα θεωρεί δεδομένες τέτοιες συσκευές. Οι άνθρωποι αρχίζουν να συνηθίζουν στα πλεονεκτήματα του να έχουν μια συχνή και εξυπηρετική πρόσβαση στο Internet. Σαν αποτέλεσμα, όλο και περισσότερη λειτουργικότητα δικτύου θα θεωρείται δεδομένη από τους χρήστες φορητών συσκευών. Φαίνεται έτσι ότι μετά από περισσότερο από 30 έτη ανεξάρτητης εξέλιξης, η ειδική δικτύωση θα πάρει μια νέα περιστροφή και ένα συνδεδεμένο με καλώδιο Διαδίκτυο και τα Ad Hoc δίκτυα θα ενωθούν τελικά να παραγάγουν τις βιώσιμες εμπορικές εφαρμογές.

Η παρούσα εργασία έχει ως στόχο την καταγραφή της σημερινής πραγματικότητας γύρω από τα ad hoc δίκτυα, την εξέλιξη αυτών των δικτύων, κατευθύνσεις και προκλήσεις μελλοντικών προγραμμάτων. Το δεύτερο κεφάλαιο παρέχει μια σε βάθος συζήτηση για τις προδιαγραφές των ad hoc δικτύων καθώς και των πρωτοκόλλων δρομολόγησης που χρησιμοποιούνται. Έπειτα (κεφάλαιο 3^ο) "παρέχουμε μια συζήτηση για τις προδιαγραφές των Ad Hoc δικτύων και τις τεχνολογίες που έχουν προκύψει. Τελικά (κεφάλαιο 4^ο) "έχουμε ένα κεφάλαιο σχετικά με την ασφάλεια" ένα ζωτικής σημασίας συστατικό που θα καθορίσει την επιτυχία επέκταση και την εμφάνιση των Ad Hoc δικτύων.

1. Ας δούμε λοιπόν τι είναι Ad Hoc τρόπος(Ασύρματα Δίκτυα Ad_Hoc) στην ασύρματη δικτύωση.

Είναι η πιο βασική και η πιο απλή τοπολογία ασύρματης δικτύωσης. Τα ασύρματα ad hoc δίκτυα διαμορφώνονται από ένα σύνολο host που επικοινωνούν ο ένας με τον άλλον πέρα από ένα ασύρματο κανάλι. Το δίκτυο που διαμορφώνεται χωρίς οποιαδήποτε κεντρική διοίκηση, αποτελείται από κινητούς κόμβους που χρησιμοποιούν μια ασύρματη διεπαφή για να στείλουν τα πακέτα. Χαρακτηρίζονται από τον αυτόνομο τρόπο λειτουργίας του κάθε κόμβου και την έλλειψη σταθερής υποδομής δικτύου κορμού. Κάθε κόμβος έχει τη δυνατότητα να επικοινωνήσει άμεσα με έναν άλλο κόμβο (ή αρκετούς από τους) στη φυσική γειτονιά του. Λειτουργούν με αυτοδιοργάνωση και αποκεντρωμένο τρόπο και η επικοινωνία μηνυμάτων πραγματοποιείται μέσω της διάδοσης multi-hop. Αυτό σημαίνει ότι οποιοδήποτε πακέτο που στέλνεται από έναν κόμβο σε ένα άλλο μπορεί να περάσει μέσω διάφορων ενδιάμεσων κόμβων που ενεργούν ως δρομολογητές. Η λειτουργία στον Ad Hoc τρόπο επιτρέπει σε όλες τις ασύρματες συσκευές, να ανακαλύψουν η μια την άλλη και να επικοινωνήσουν ως όμοιος-προς-όμοιο χωρίς ανάμειξη των κεντρικών σημείων πρόσβασης (συμπεριλαμβανομένων εκείνων που ενσωματώνονται στους ευρυζωνικούς ασύρματους [δρομολογητές](#)). Δεδομένου ότι οι κόμβοι σε ένα δίκτυο αυτού του είδους μπορούν να χρησιμεύσουν και ως δρομολογητές και οι οικοδεσπότες, μπορούν να διαβιβάσουν τα πακέτα εξ ονόματος άλλων κόμβων και να τρέξουν τις εφαρμογές χρηστών.

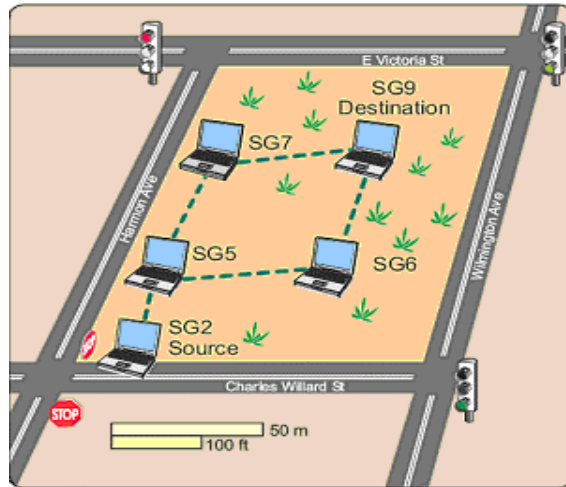


Εικόνα 1: Ad Hoc δικτύωση.

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

επικοινωνία ασυρμάτων σταθμών μέσω των ασυρμάτων ειδικών ad-hoc δικτύων Ad_Hoc.

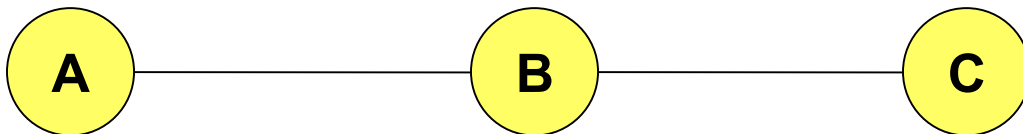
ΠΑΡΑΔΕΙΓΜΑ 1



- Μπορεί να χρειαστεί να διασχίσουμε πολλούς συνδέσμους για να φτάσουμε στον προορισμό.

ΠΑΡΑΔΕΙΓΜΑ 2

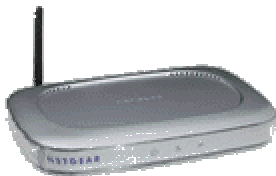
Οποιοδήποτε πακέτο που στέλνεται από έναν κόμβο σε ένα άλλο μπορεί να περάσει μέσω διάφορων ενδιάμεσων κόμβων που λειτουργούν ως δρομολογητές.



- Ο κόμβος B μπορεί να επικοινωνήσει και με τον A και με τον C
- Οι A και C δεν μπορούν να ακούσουν ο ένας τον άλλον.
- Όταν ο A μεταδίδει στον B, ο C δεν μπορεί να ανιχνεύσει τη μετάδοση χρησιμοποιώντας το μηχανισμό *ανίχνευσης φέροντος* (*carrier sensing*).
- Αν ο C μεταδώσει την ίδια στιγμή με τον A, θα έχουμε παρεμβολή στον B

Η ad hoc δικτύωση επιτρέπει στους χρήστες να διαμορφώσουν αυθόρμητα το ασύρματο τοπικό LAN. Οι κόμβοι σε ένα ad hoc δίκτυο, θα είναι κινητοί, και σύντομα ή αργότερα θα οδηγηθούμε σε μια ποικίλη τοπολογία δικτύων. Θα πρέπει ωστόσο η συνδετικότητα μέσα στο δίκτυο να διατηρηθεί για να επιτρέψει σε εφαρμογές και υπηρεσίες να λειτουργήσουν. Είναι πολύ σημαντικό μάλιστα, το Ad Hoc δίκτυο να αποκτήσει πρόσβαση στο διαδίκτυο. Πώς όμως μπορεί να επιτευχθεί αυτό;

Για να εξηγήσουμε με ποιο τρόπο μπορεί να γίνει η σύνδεση του ad hoc δικτύου με το διαδίκτυο, θα χρειαστεί αρχικά να καθορίσουμε, τι είναι τα **APs (ACCESS POINT)**. Τα ασύρματα σημεία πρόσβασης (APs) είναι ειδικά διαμορφωμένοι κόμβοι στα ασύρματα δίκτυα τοπικής περιοχής (WLANs). Ενεργούν ως κεντρικές συσκευές αποστολής και λήψης των ράδιο σημάτων WLAN. Τα σημεία πρόσβασης που χρησιμοποιούνται στα δίκτυα σπιτιών ή μικρών επιχειρήσεων είναι μικρές συσκευές που χαρακτηρίζονται από έναν ενσωματωμένο προσαρμοστή δικτύων, μια κεραία, και μια συσκευή αποστολής σημάτων (Περισσότερες πληροφορίες για τεχνικά χαρακτηριστικά αναφέρθηκαν στην εισαγωγή). Τα σημεία πρόσβασης υποστηρίζουν τα ασύρματα πρότυπα επικοινωνίας WI-FI.



Εικόνα 2: ACCESS POINT

Απλές συσκευές που συνδέονται με το ενσύρματο δίκτυο.

Στα Ad Hoc δίκτυα, οι ασύρματοι σταθμοί μπορούν να επικοινωνούν κατευθείαν μεταξύ τους, ένας προς έναν (peer to peer), χωρίς να υπάρχει κεντρικός σταθμός AP. Χωρίς το διαθέσιμο κεντρικό υπολογιστή DHCP, τα windows XP παρέχουν μια αυτόματη ιδιωτική διεύθυνση IP μεταξύ 169.254.0.0 και 169.254.255.255 στους προσαρμοστές δικτύων. Οι σταθμοί είναι ισότιμοι μεταξύ τους. Αν και ένα πολύ μικρό WLAN μπορεί να λειτουργήσει όμως χωρίς σημεία πρόσβασης, με ένα σημείο πρόσβασης – AP (ACCESS POINT), έχετε πρόσβαση στην υποδομή - υποστήριξη σημείων. Αυτός ο τρόπος γεφυρώνει WLANs με το συνδεδεμένο με καλώδιο τοπικό LAN Ethernet, όπως επίσης και τις κλίμακες του δικτύου για την υποστήριξη περισσότερων πελατών. Σε παλαιότερα πρότυπα, τα σημεία πρόσβασης **AP (ACCESS POINT)**, υποστήριζαν 10 - 20 πελάτες. Σήμερα, τα σημεία πρόσβασης υποστηρίζουν μέχρι 255 πελάτες. Θα πρέπει ωστόσο να αναφέρουμε ότι η απόδοση υποφέρει καθώς ο αριθμός συσκευών αυξάνεται, και ένα μεγάλο Ad Hoc δίκτυο γίνεται γρήγορα δύσκολο να διαχειριστεί.

Για να πετύχουμε σύνδεση του Ad Hoc δικτύου με το διαδίκτυο, θα χρειαστεί να διαμορφώσουμε ένα κεντρικό(οικοδεσπότη) υπολογιστή, τον οποίο συνδέουμε με το Διαδίκτυο, και στη συνέχεια ο κεντρικός αυτός υπολογιστής θα μοιράζεται τη σύνδεση που έχει με το Διαδίκτυο, με άλλους χρήστες του ειδικού δικτύου. Πρέπει λοιπόν να

συνδέσετε ένα καλώδιο Ethernet που οδηγεί από την τηλεφωνική γραμμή, στον προσαρμοστή Ethernet(modem ή net mode) του οικοδεσπότη υπολογιστή.

Ο προσαρμοστής για την δικτύωσή σας με το Ad Hoc δίκτυο μπορεί να είναι μια ασύρματη κάρτα δικτύωσης, ή ένα **σημείο πρόσβασης – (AP) (ACCESS POINT)**. Η διαφορά τους είναι ότι τα ACCESS POINT (AP) παρέχουν κάποιες επιπλέον δυνατότητες, όπως αναφέραμε πιο πάνω. Δηλ. έχουν μεγαλύτερη ακτίνα δράσης από τις απλές ασύρματες κάρτες, επεκτείνοντας έτσι την εμβέλεια του ασύρματου δικτύου, ελέγχουν την κίνηση του δικτύου, κατανέμουν το διαθέσιμο εύρος ανάλογα με τον αριθμό των υπολογιστών και φροντίζουν να κατευθύνουν τα πακέτα πληροφοριών, ενώ ο αριθμός των κόμβων που μπορούν να "σηκώσουν" μπορεί να είναι μεγαλύτερος, κάτι που πάντα εξαρτάται και από τον κατασκευαστή.

Πιο κάτω θα αναλύσουμε: **I)** Το μοντέλο λειτουργίας των ειδικών δικτύων Ad_Hoc, **II)** Σε ποιες περιπτώσεις θα πρέπει να χρησιμοποιήσουμε τα Ad Hoc δίκτυα Ad_Hoc, καθώς και **III)** Τα πλεονεκτήματα και μειονεκτήματα τους.

1. Μοντέλο Λειτουργίας

Ο εντοπισμός των συνδέσεων μεταξύ υπολογιστών είναι κάτι τόσο βασικό που ένα δίκτυο υπολογιστών δεν μπορεί εξ' ορισμού να υπάρξει χωρίς αυτό. Ο τρόπος που τα πακέτα διαβιβάζονται στα Ad Hoc ασύρματα δίκτυα είναι αρκετά διαφορετικός από τον τρόπο που αυτά διαβιβάζονται στα συνδεδεμένα με καλώδιο δίκτυα. Η σημαντική διαφορά είναι ότι όταν στέλνει ένας οικοδεσπότης ένα πακέτο, όλοι οι γείτονές του θα λάβουν εκείνο το πακέτο. Υπάρχουν πολλά είδη πρωτοκόλλων που υποστηρίζονται από κάθε υποδομή. Τα πρωτόκολλα που χρησιμοποιούνται αξίζουν μελέτη, αλλά χρειάζονται προσαρμογή πριν να καταστούν χρήσιμα σε ένα δίκτυο που δεν συνδέεται πλέον με την υποδομή του Internet. Μερικά από αυτά δεν θα είναι κατάλληλα για χρήση όταν δεν είναι διαθέσιμη η υποδομή. Για παράδειγμα, τέτοια είναι τα πρωτόκολλα επικύρωσης πιστωτικών καρτών και διαχείρισης δικτύου.

Στο χώρο σχεδιασμού ενός ad hoc δικτύου υπάρχει μια ποικιλία διαστάσεων. Σκεφθείτε για παράδειγμα, αν η περιοχή ασύρματης μετάδοσης πρέπει να είναι μεγάλη ή μικρή σύμφωνα πάντα με την γεωγραφική κατανομή των κινητών κόμβων. Αν όλοι οι κινητοί κόμβοι είναι εντός του μεταξύ τους εύρους, τότε δεν χρειάζεται δρομολόγηση και το ad hoc δίκτυο είναι πλήρως συνδεδεμένο. Θα συζητήσουμε κάποιες προτάσεις, που παρέχουν λύσεις στην περίπτωση που κάποιοι από τους κινητούς κόμβους δεν βρίσκονται στην περιοχή κάλυψης των υπολοίπων. Σε συνδυαζόμενο με την απουσία δρομολογητών υποδομής, το περιορισμένο εύρος της ασύρματης μετάδοσης καταδεικνύει την ανάγκη για δρομολόγηση πολλαπλών αλμάτων (multihop). <<**Multihopping:** ένα δίκτυο multihop είναι ένα δίκτυο όπου η πορεία από την πηγή στον προορισμό διαπερνά διάφορους άλλους κόμβους. Τα Ad Hoc δίκτυα εκθέτουν συχνά τους πολλαπλάσιους λυκίσκους για τη διαπραγμάτευση εμποδίων, την επαναχρησιμοποίηση φάσματος, και την ενεργειακή συντήρηση. Οι συγκεκριμένες

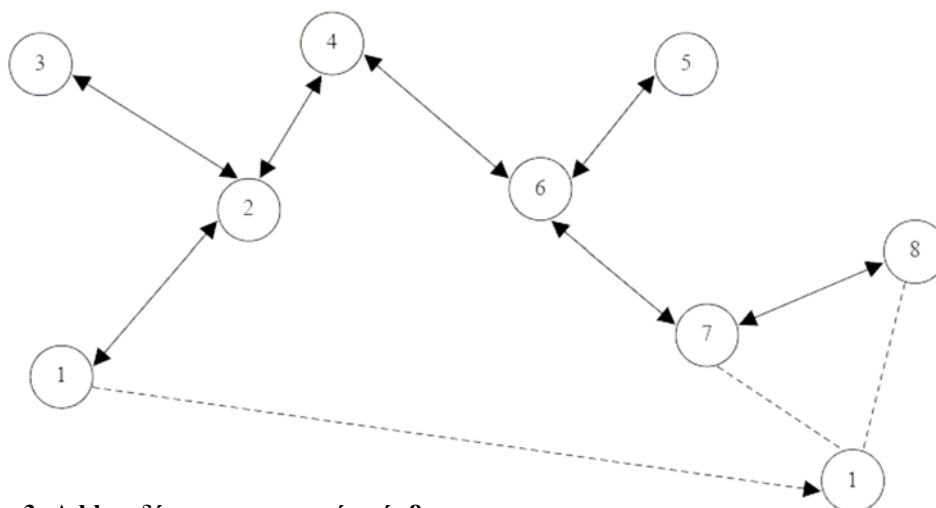
διαδικασίες πεδίων μαχών ευνοούν επίσης μια ακολουθία κοντών λυκίσκων για να μειώσουν την ανίχνευση από τον εχθρό>>.

Σαν ένα επιπλέον παράδειγμα, μπορούμε να υποθέσουμε ότι οι χρήστες των ασύρματων συσκευών μπορούν να μετρήσουν τις σχετικές τους θέσεις και κατ' επέκταση να διαμορφώσουν τους φορητούς υπολογιστές τους χρησιμοποιώντας τις μετρηθείσες αποστάσεις, έτσι ώστε οι απαραίτητες πληροφορίες ζεύξης να είναι διαθέσιμες σε όλους τους κόμβους. Μια τέτοια μορφή θα λειτουργούσε, αλλά δεν θα ήταν και τόσο εξυπηρετική. Ακόμα χειρότερα, οι πληροφορίες ζεύξης πιθανότατα θα άλλαζαν καθώς οι χρήστες κινούνται σε σχέση με τους υπολοίπους. Ουσιαστικά, δεν μας ενδιαφέρει το να απλοποιήσουμε το πρόβλημα σε βάρος της εξυπηρέτησης του χρήστη, αλλά θα περιορίσουμε την προσοχή μας στις προτάσεις που παρέχουν αυτόματη εγκατάσταση της τοπολογίας και δυναμική διαχείριση αυτής, δίνοντας στο χρήστη δυνατότητα κινητικότητας.

2.1 Η ανάλυση στηρίζεται στα παρακάτω χαρακτηριστικά:

- Οι κόμβοι χρησιμοποιούν το πρωτόκολλο δικτύου IP και φέρουν διευθύνσεις IP οι οποίες καθορίζονται από ακανόνιστα μέσα.
- Οι κόμβοι είναι αρκετά μακριά έτσι ώστε να μην βρίσκονται όλοι στην περιοχή κάλυψης των υπολοίπων
- Οι κόμβοι μπορούν να είναι κινητοί, ούτως ώστε δύο κόμβοι που βρίσκονται στην ίδια περιοχή κάποια χρονική στιγμή να μην βρίσκονται στην ίδια περιοχή αργότερα
- Οι κόμβοι έχουν τη δυνατότητα να βοηθούν τους υπολοίπους στη διαδικασία παράδοσης πακέτων δεδομένων.

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



Εικόνα 3: Ad hoc δίκτυο με κινητούς κόμβους

Οι περισσότεροι αλγόριθμοι επιτρέπουν την εμφάνιση νέων κόμβων και την εξαφάνιση παλαιότερων.

2.2 Συγκεκριμένα, τα μοντέλα λειτουργίας Ad_Hoc Δικτύων που προτείνουμε είναι:

- Συμμετρικές Ζεύξεις
- Λύσεις Ad Hoc Επιπέδου 2
- Πολυεκπομπή (multicast)

2.2.1 Συμμετρικές Ζεύξεις

Ένα από τα μοντέλα που θα ασχοληθούμε εξαρτάται από την ύπαρξη συμμετρικών ζεύξεων επικοινωνίας μεταξύ των κόμβων σε ένα ad hoc δίκτυο. Δυστυχώς, οι ασύρματες ζεύξεις στον πραγματικό κόσμο δεν συμβαδίζουν απαραίτητα με τον παραπάνω συμβιβασμό. Η υπόθεση της συμμετρίας γίνεται επειδή η δρομολόγηση σε δίκτυα με μονόπλευρες ζεύξεις είναι ως γνωστόν αρκετά δύσκολη. Βέβαια, αν το δίκτυο παρουσιάζει υψηλό βαθμό συνδεσιμότητας και σχετικά χαμηλό αριθμό μονόπλευρων ζεύξεων, τότε μπορούν να εντοπιστούν εναλλακτικές διαδρομές που περιλαμβάνουν αποκλειστικά συμμετρικές ζεύξεις.

Υπάρχει ακόμα ένας παράγοντας που μετριάζει τη σημασία της απόφασης να αγνοηθούν οι ασύμμετρες διαδρομές. Μια μονόπλευρη ζεύξη είναι μερικές φορές στα πρόθυρα κατάρρευσης ούτως ή άλλως. Σε τέτοιες περιπτώσεις, η επέκταση του βασικού πρωτοκόλλου των ad hoc δικτύων, μπορεί να προκαλέσει τον προσδιορισμό λιγότερο εύρωστων διαδρομών, έτσι ώστε να αντιμετωπίζει τις μονόπλευρες ζεύξεις, πράγμα που οδηγεί σε πρόωρη κατάρρευση του συστήματος και κατ' επέκταση στην ανάγκη για νέο κύκλο αναζήτησης διαδρομής, ο οποίος συνήθως είναι πιο περίπλοκος.

2.2.2 Λύσεις Ad Hoc Επιπέδου 2

Τα πρωτόκολλα ad hoc δικτύων που θα παρουσιάσουμε στη συνέχεια της εργασίας στοχεύουν κυρίως στη λειτουργία του επιπέδου 3. Είναι δυνατόν, πρακτικά σε όλες τις περιπτώσεις, να προσαρμοστεί το πρωτόκολλο για χρήση στο επίπεδο 2. Για να γίνει αυτό θα πρέπει αρχικά το πεδίο διεύθυνσης IP να μεγεθυνθεί ώστε να περιλαμβάνει 48 (ή περισσότερα) bits αντί για 32 που απαιτούνται στο IP, αφού η διεύθυνση IEEE MAC έχει τυπικό μήκος 48 ή 64 bits. Αυτό δεν αποτελεί πρόβλημα αφού μια τέτοια προσαρμογή θα χρειαστεί ούτως ή άλλως για να δοθεί η δυνατότητα στο πρωτόκολλο να λειτουργεί σε δίκτυα υπολογιστών που χρησιμοποιούν διευθυνσιοδότηση IPv6.

Παρόλα αυτά, δεδομένης της ανάπτυξης των εφαρμογών IP στη δημιουργία δικτύων, κάθε εφαρμογή τελικά θα προκαλέσει σε ένα υποσύστημα επικοινωνιών την ανάγκη να «μεταφράσει» τη διεύθυνση IP σε μια γειτονική διεύθυνση του επιπέδου 2, ή αλλιώς σε μια διεύθυνση επιπέδου 2 ενός κόμβου στη γειτονιά, που μπορεί να μεταφέρει τα πακέτα προς την IP διεύθυνση του επιθυμητού προορισμού. Όταν ο πίνακας δρομολόγησης στον

κόμβο πηγής έχει τις IP διευθύνσεις των επιθυμητών προορισμών, τότε η προώθηση μέσω IP πλαισιώνει τα δεδομένα με μια επικεφαλίδα επιπέδου 2 που περιέχει τη διεύθυνση προορισμού του επιπέδου 2 για το επόμενο άλμα κατά μήκος του μονοπατιού προς τον τελικό προορισμό.

Η ευχάριστη αυτή κατάσταση εξαλείφεται όμως όταν η δρομολόγηση βασίζεται σε διευθύνσεις επιπέδου 2. Σε αυτή την περίπτωση ο πίνακας δρομολόγησης περιλαμβάνει διευθύνσεις προορισμού επιπέδου 2. Αυτό υπονοεί ότι η IP διεύθυνση του προορισμού θα πρέπει να «μεταφραστεί» σε μια διεύθυνση προορισμού επιπέδου 2 ακόμα κι αν ο προορισμός βρίσκεται αρκετά άλματα μακριά. Τότε, εκτός αν η αναζήτηση διαδρομής στο επίπεδο 2 κατέχει τις απαραίτητες πληροφορίες διευθυνσιοδότησης επιπέδου 3 με τις κατάλληλες προεκτάσεις. Αν οι πληροφορίες επιπέδου 3 περιλαμβάνονται για καλύτερη απόδοση, τότε η όλη λειτουργία μπορεί να θεωρηθεί ως μια αναζήτηση διαδρομής επιπέδου 3 ούτως ή άλλως, παρά την ασυνήθιστη δομή των δεδομένων για την αποθήκευση των διαδρομών.

2.2.3 Πολυεκπομπή (multicast)

Τα ad hoc δίκτυα παρουσιάζουν ενδιαφέρον σε μεγάλο βαθμό λόγω της πρόκλησης να διατηρηθεί το μονοπάτι επικοινωνίας μεταξύ πηγής και προορισμού, ακόμα κι όταν κάποιοι από τους ενδιάμεσους κόμβους αναμετάδοσης δεν είναι δυνατό να συνεχίσουν να μεταδίδουν τα πακέτα και πρέπει να αντικατασταθούν από άλλους κόμβους σε εναλλακτικά μονοπάτια. Η διατήρηση μονοπατιών ανάμεσα σε μια πηγή και πολλαπλούς προορισμούς είναι σχετικά πιο δύσκολη εργασία. Δεδομένης της αυξανόμενης σημασίας της πολυεκπομπής σαν μέσο για μείωση της χρήσης του εύρους ζώνης κατά τη μαζική μετάδοση δεδομένων και της πιεστικής ανάγκης για εξοικονόμηση του σπάνιου εύρους ζώνης σε ασύρματα μέσα, είναι φυσικό ότι η δρομολόγηση πολυεκπομπής θα πρέπει να προσεχθεί ιδιαίτερα στα ad hoc δίκτυα.

Ένα ανοικτό ερώτημα είναι αν οι αλγόριθμοι δρομολόγησης πολυεκπομπής θα πρέπει να ενσωματωθούν με τους αλγορίθμους δρομολόγησης που χρησιμοποιούνται για τη δημιουργία μονοπατιών επικοινωνίας ανάμεσα σε μοναδικούς κόμβους. Από τη μια πλευρά, το πρόβλημα μπορεί να είναι αρκετά διαφορετικό, ώστε το να προσπαθήσει κάποιος να δημιουργήσει έναν απλό αλγόριθμο που να εξυπηρετεί και τις δυο περιπτώσεις να είναι ανέφικτο. Από την άλλη πλευρά, το πρόβλημα της επαναδημιουργίας μονοπατιών που δημιουργήθηκε από την κίνηση των ενδιάμεσων κόμβων σε μια διαδρομή ή ένα δένδρο μπορεί να υπερισχύει και στις δυο περιπτώσεις.

3 Ασύρματες λύσεις.

Αυτός ο τύπος δικτύου παρατάχτηκε με στόχους πολύ διαφορετικούς από την κινητή τηλεφωνία και την πρόσβαση Διαδικτύου. Ο αρχικός στόχος ήταν να οργανωθούν οι επικοινωνίες για εξειδικευμένους σκοπούς, όπως αυτοσχέδιες εφαρμογές στις περιοχές όπου δεν υπάρχει καμία προϋπάρχουσα υποδομή (π.χ., εξερεύνηση της ζούγκλας, πεδίο μάχης), ή πού η υποδομή έχει αποτύχει (π.χ., διάσωση σεισμού), ή δεν είναι επαρκές για τις τρέχουσες ανάγκες (π.χ., διασύνδεση των χαμηλών ενεργειακών περιβαλλοντικών αισθητήρων).



Εικόνα 4: Παραδείγματα ad hoc δικτύων.

Η ασύρματη κινητή δικτύωση έχει αλλάξει σημαντικά τα συστήματα επικοινωνιών για τον Αμερικανικό στρατό, το ναυτικό, την Πολεμική Αεροπορία, και τα ναυτικά. Οι επικοινωνίες σε κίνηση είναι ουσιαστικές για τις επιτυχείς διαδικασίες αποστολής. Η σημασία τέτοιων δικτύων αυξάνεται γρήγορα με τις προόδους στην τεχνολογία που οδηγούν στις μικρότερες, φτηνότερες, και αποδοτικές συσκευές. Σήμερα η ιδιαίτερη μορφή τους τα καθιστά κατάλληλα για μια πλειάδα εφαρμογών, όπως η παρατήρηση χώρων, λειτουργία σε πεδία μάχης, περιπτώσεις εκτάκτου ανάγκης, διάρθρωση επικοινωνιακής υποδομής με προσωρινό χαρακτήρα. Η χρήση των ειδικών δικτύων φαίνεται πολύ σημαντική και στην καθημερινή μας ζωή.

- I. Μια ομάδα ανθρώπων μπορεί να συνεργαστεί σε μια επιχειρησιακή συνεδρίαση στην εταιρική έδρα τους. Η ανάγκη για συνεργασία μέσω υπολογιστή είναι μεγαλύτερη σε αυτή την περίπτωση παρά στο περιβάλλον γραφείου. Οι συμμετέχοντες θα μπορούσαν εύκολα να διαμορφώσουν το μικρό ασύρματο τοπικό LAN μέσα στην αίθουσα συνεδριάσεών τους και να μπορούσαν να μοιραστούν τα έγγραφα, διαγράμματα παρουσιάσεις, καθώς μπαίνουν στο γραφείο όλη η επικοινωνία θα μπορούσε αυτόματα να καθοδηγηθεί μέσω του ασύρματου εταιρικού δικτύου.
- II. Σκεφθείτε το σενάριο που θα προκύψει όταν οι ασύρματοι υπολογιστές γίνουν δημοφιλείς στο οικιακό περιβάλλον. Αυτοί οι υπολογιστές θα μεταφέρονται στο περιβάλλον εργασίας, στο σπίτι αλλά και σε επαγγελματικά ταξίδια Έχοντας υπόψη την ευκολία που προσφέρει στο χρήστη η σταθερή διεύθυνση IP, θα ήταν καλό να επιτρέπουμε στις διάφορες κινητές συσκευές να δημιουργούν ένα ad hoc δίκτυο στο σπίτι, ακόμα κι αν στο οικιακό περιβάλλον υπάρχουν ήδη σταθεροί κόμβοι υποδικτύου. Τα δίκτυα ad hoc προσφέρουν την προοπτική της συνδεσιμότητας σε όλους τους κόμβους του σπιτιού, ανεξάρτητα από το σταθερό σημείο σύνδεσής τους, το οποίο καταδεικνύεται από το πρόθεμα του δικτύου που είναι τμήμα κάθε IP διεύθυνσης. Επιπλέον, χρησιμοποιώντας πρωτόκολλα όπως το Mobile IP, οι κόμβοι στα οικιακά ad hoc δίκτυα λειτουργούν σα να ήταν συνδεδεμένοι στο σταθερό τους περιβάλλον και επιπρόσθετα συμμετέχουν (με μεγαλύτερη απόδοση) σε ένα τοπικό ad hoc δίκτυο.

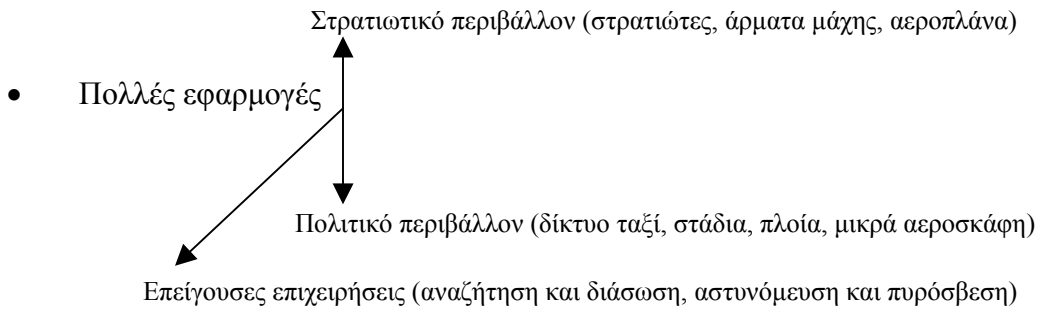
- III. Θα μπορούσατε κάλλιστα να παραμείνετε σε απευθείας σύνδεση με το διαδίκτυο, και να έχετε άμεση πρόσβαση στο εισερχόμενο ηλεκτρονικό ταχυδρομείο και να παρακολουθείτε τα μηνυματά σας όταν βρισκόσαστε στο πεδίο εύρους ενός ειδικού δικτύου.
- IV. Όταν εσείς και οι συνεταίροι σας περιμένετε μια πτήση στον αερολιμένα, και πρέπει να μοιραστείτε ένα σχετικά μεγάλο αρχείο PDF. Μέσω του Ad Hoc τρόπου, μπορείτε εύκολα να μεταφέρετε το αρχείο από ένα lap-top σε άλλο.
- V. Η Ad Hoc μορφή επικοινωνιών είναι ιδιαίτερα χρήσιμη για τη δημόσια ασφάλεια(πχ. αναζήτηση και διάσωση). Οι ιατρικές ομάδες απαιτούν γρήγορα, αποτελεσματικές επικοινωνίες, σε περιπτώσεις έκτακτης ανάγκης για να θεραπεύσουν τα θύματα. Δεν μπορούν να αντέξουν το χρόνο να γίνει αρχικά η επικοινωνία και αφετέρου να εγκατασταθεί το υλικό δικτύωσης. Η ιατρική ομάδα μπορεί να χρησιμοποιήσει 802.11 ράδιο NICs στα lap-top και να επιτρέψει τις ευρυζωνικές ασύρματες μεταδόσεις στοιχείων μόλις φθάνουν στη σκηνή.
- VI. Οι κινητές συσκευές παρέχουν τους μηχανισμούς δρομολόγησης προκειμένου να επεκταθεί η σειρά του συστήματος. Παραδείγματος χάριν, ένας χρήστης σε μια πλευρά του κτηρίου μπορεί να στείλει ένα πακέτο που προορίζεται σε κάποιο χρήστη σε μακρινή πλευρά του κτηρίου, πέρα από την σημείο σε σημείο σειρά 802.11. Αυτό μπορεί να επεκτείνει το ασύρματο τοπικό LAN από τις εκατοντάδες των ποδιών σε μίλια, ανάλογα με τη συγκέντρωση των ασύρματων χρηστών.

Αυτά τα παραδείγματα της αυθόρμητης, Ad Hoc ασύρματης επικοινωνίας μεταξύ των συσκευών μπορούν να μας δώσουν μια ιδέα για τις δυνατότητες της Ad Hoc δικτύωσης, η οποία επιτρέπει στις συσκευές να καθιερώσουν την επικοινωνία, οποτεδήποτε και οπουδήποτε χωρίς την ενίσχυση μιας κεντρικής υποδομής.

4 Πλεονεκτήματα και μειονεκτήματα που εξετάζουν

Θετικά

- Χαμηλό κόστος
- Ταχύτητα ανάπτυξης



Αρνητικά

- Περιορισμένη εμβέλεια ασύρματης μετάδοσης
- Broadcast(εκπομπή) φύση του ασύρματου μέσου
- Απώλειες πακέτων λόγω λαθών μετάδοσης
- Κινητικότητα κόμβων
- Ενεργειακοί περιορισμοί
- Ευκολία παρακολούθησης ασύρματων μεταδόσεων (κίνδυνος ασφάλειας)

Έτσι πριν λάβετε την απόφαση να χρησιμοποιήσετε τον Ad Hoc τρόπο δικτύωσης, θα πρέπει να εξετάσετε τα εξής:

- **Μείωση κόστους.** Χωρίς την ανάγκη να αγοραστούν ή να εγκατασταθούν τα σημεία πρόσβασης, θα κερδίσετε μη αμελητέο χρηματικό ποσό κατά την ανάπτυξη ειδικού ασύρματου δικτύου. Φυσικά αυτό κάνει αυτούς που υπολογίζουν το κόστος ευτυχισμένους, αλλά είναι βέβαιο ότι θα σκεφτείτε για όλα τα πλεονεκτήματα και μειονεκτήματα πριν πάρετε μια τελική απόφαση για τον τρόπο δικτύωσης.
- **Γρήγορος χρόνος οργάνωσης.** Ο Ad Hoc τρόπος δικτύωσης απαιτεί μόνο την εγκατάσταση των κατάλληλων καρτών ασύρματης δικτύωσης στις συσκευές χρηστών. Κατά συνέπεια, ο χρόνος στην οργάνωση του Ad Hoc ασύρματου δικτύου είναι πολύ μικρός.
- **Καλύτερη απόδοση πιθανή.** Το θέμα της απόδοσης με τον Ad Hoc τρόπο είναι βεβαίως αμφισβητήσιμο. Παραδείγματος χάριν, η απόδοση μπορεί να είναι υψηλότερη με τον Ad Hoc τρόπο λόγω του ότι δεν υπάρχει η ανάγκη για τα πακέτα να ταξιδέψουν μέσω ενός σημείου πρόσβασης. Αυτό εντούτοις υποθέτει έναν σχετικά μικρό αριθμό χρηστών. Επίσης εξαιτίας της ανάγκης, οι σταθμοί να απαντούν κατά τη διάρκεια αναγνωριστικών σημάτων, η απόδοση μπορεί να είναι χαμηλότερη με τον Ad Hoc τρόπο, λόγω των πρόσθετων μεταδόσεων πακέτων.
- **Περιορισμένη πρόσβαση στο δίκτυο.** Επειδή δεν υπάρχει κανένα σύστημα διανομής με Ad Hoc ασύρματο δίκτυο, οι χρήστες δεν έχουν αποτελεσματική πρόσβαση στο Διαδίκτυο και άλλες συνδεδεμένες με καλώδιο υπηρεσίες δικτύων.

Φυσικά θα μπορούσατε να διαμορφώσετε ένα PC με μια κοινή σύνδεση στο Διαδίκτυο, με τη χρήση ενός καλωδίου Ethernet και οι υπόλοιποι υπολογιστές του (ειδικού) δικτύου να μπορούν να συνδέσουν με το Διαδίκτυο μέσω του οικοδεσπότη υπολογιστή.

- **Δύσκολη διαχείριση δικτύων.** Η διαχείριση δικτύων γίνεται ένας πονοκέφαλος με τα Ad Hoc δίκτυα λόγω της ρευστότητας της τοπολογίας δικτύων και της έλλειψης μιας συγκεντρωτικής συσκευής. Έτσι οι διευθύνοντες δικτύων δεν μπορούν να ελέγξουν εύκολα την απόδοση τους, να εκτελέσουν τους λογιστικούς ελέγχους ασφάλειας, την αποτελεσματική διαχείριση δικτύων κ.λπ. Το Ad Hoc ασύρματο δίκτυο LAN απαιτεί τη διαχείριση δικτύων σε επίπεδο συσκευών χρηστών, πράγμα το οποίο απαιτεί την αυξημένη μετάδοση πακέτων στο δίκτυο. Αυτό κάνει πάλι τον Ad Hoc τρόπο δικτύωσης να βρίσκεται μακριά από ασύρματες εφαρμογές του μεγαλύτερου επιχειρηματικού τοπικού LAN.

Σημαντικοί περιορισμοί σε ασύρματες εφαρμογές. Ο αυτόνομος χαρακτήρας και η κινητικότητα των κόμβων στα δίκτυα αυτά, επιβάλλουν σημαντικούς περιορισμούς στην κατανάλωση ενέργειας των τερματικών σταθμών, περιορίζοντας τις λειτουργικές ικανότητες του κάθε ασύρματου κόμβου. Δύο προσεγγίσεις για τη βελτίωση της μεταφορικής ικανότητας του δικτύου και τον παράλληλο περιορισμό της κατανάλωσης ενέργειας του ασύρματου τερματικού είναι οι **γωνίες κώνων (cone angles)** και οι **περιοχές σκυτάλης (relay regions)**.

Στην πρώτη περίπτωση, χρησιμοποιούνται οι εγγενείς γωνίες μεταξύ των ασύρματων συνδέσεων ως κριτήριο για ελάττωση της ακτίνας κάλυψης. Η δεύτερη προσέγγιση επιδιώκει τον προσδιορισμό ενός υποσυνόλου γειτόνων, στους οποίους είναι πιο οικονομικό να προωθηθεί δικτυακή κίνηση, χρησιμοποιώντας καθαρά γεωμετρικά στοιχεία και ιδιότητες της ασύρματης διάδοσης κυμάτων. Φτάσαμε λοιπόν στο σημείο, όπου θα αναλύσουμε τη διαμόρφωση των Ad_Hoc δικτύων, καθώς και τη σύνδεσή τους με το διαδίκτυο.

5. VITAN – Εργαλείο απεικόνισης για τα Ad Hoc δίκτυα.

Τέλος σημαντικό θα ήταν να παρουσιάσουμε το VITAN, εργαλείο απεικόνισης για τα Ad Hoc δίκτυα. Είναι ένα εργαλείο για τις συνδέσεις και τις ιδιότητες (ικανότητες) τους μεταξύ των τερματικών στα ασύρματα Ad Hoc δίκτυα.

Το εργαλείο παίρνει τη θέση των τερματικών (που διευκρινίζονται από τις συντεταγμένες X και Y) και των ιδιοτήτων συνδέσεων μεταξύ των τερματικών (που διευκρινίζονται από θετικούς ακέραιους αριθμούς), ως εισαγωγή. Το εργαλείο παράγει μια απεικόνιση των συνδέσεων των τερματικών, με σχήμα σύκων, το οποίο μπορεί στη συνέχεια να μετατραπεί σε οποιοδήποτε κοινό γραφικό σχήμα. Το VITAN δεν αξιολογεί τις συνδέσεις και τις ιδιότητες συνδέσεων στα Ad Hoc δίκτυα. Το VITAN παίρνει τις ιδιότητες συνδέσεων που λαμβάνονται από άλλα εργαλεία, προσομοιώσεις, ή αναλυτικές

αξιολογήσεις ως εισαγωγή και απεικονίζει γραφικά αυτές τις ιδιότητες συνδέσεων και τις προκύπτουσες συνδέσεις στο δίκτυο. Διευκολύνει λοιπόν την οπτική μελέτη των σύνθετων ειδικών δικτύων με την απεικόνιση των ιδιοτήτων συνδέσεων. Επιτρέπει την εκλεκτική επίδειξη και την οπτική μελέτη των συνδέσεων που παρέχονται με μια συγκεκριμένη ποιοτική σειρά.

Το πρόγραμμα VITAN πραγματοποιήθηκε σε συνεργασία με το κρατικό πανεπιστήμιο της Αριζόνα (ASU) και το πανεπιστήμιο της Φερράρα.. Το εργαλείο γράφεται σε Perl και λειτουργεί σε Linux Mandrake, Linux Red hut , και Windows XP.

Συμπεράσματα

Σε αυτό το άρθρο έχουμε κάνει μια προσπάθεια να διευκρινίσουμε τι είναι ένα ad hoc δίκτυο καθώς και να ερευνήσουμε την ad hoc δικτύωση κυρίως από τεχνική άποψη. Η κινητικότητα των κόμβων και η αλλαγή δομής του δικτύου είναι αυτό που διέκρινε τα ad hoc δίκτυα από άλλα δίκτυα. Όπως μπορείτε να δείτε, τα ad hoc δίκτυα προσφέρουν αρκετά πλεονεκτήματα που εξετάζουν κατά την ανάπτυξη ασύρματου LANs. Η σκέψη της εξοικονόμησης του κόστους στα σημεία πρόσβασης είναι βεβαίως ένας αναγκάζοντας λόγος να εξεταστεί έντονα αυτή η διαμόρφωση. Βέβαια θα διαπιστώσετε αν εφαρμόζετε τη δρομολόγηση μεταξύ των ασύρματων χρηστών, ότι τα ad hoc δίκτυα ισχύουν συνήθως για τα μικρότερα, αυθόρμητα δίκτυα όταν δεν υπάρχει μια ισχυρή ανάγκη για με ένα συνδεδεμένο με καλώδιο δίκτυο. Η πρόωρη εμπειρία προσομοίωσης με τα ασύρματα Ad Hoc δίκτυα δείχνει ότι η ικανότητά τους μπορεί να είναι εκπληκτικά χαμηλή, λόγω της απαίτησης, οι κόμβοι να διαβιβάζουν πολλαπλά πακέτα. Η επιτεύξιμη ικανότητα εξαρτάται από το μέγεθος δικτύων, τα σχέδια κυκλοφορίας, και τις λεπτομερείς τοπικές αλληλεπιδράσεις. Μπορούμε λοιπόν να πούμε με σιγουριά, ότι τα ad hoc δίκτυα χρησιμοποιούνται "ευκαιριακά"! Τα δίκτυα αυτά έχουν νόημα σε περιπτώσεις που πρέπει να χτιστεί ένα μικρό, τοπικό LAN γρήγορα και να που θέλετε να ξοδέψετε το ελάχιστο χρηματικό ποσό για τον εξοπλισμό, ή ακόμη για να επεκτείνει ένα δίκτυο σε περιοχές που επιτυγχάνονται όχι εύκολα ενσύρματα δίκτυα. Εντούτοις, αντιπροσωπεύουν μια πολύ σημαντική αναπτυσσόμενη αγορά.

ΚΕΦΑΛΑΙΟ 2

ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΔΡΟΜΟΛΟΓΗΣΗ

Ένα δίκτυο Υπολογιστών είναι ένα σύνολο Ηλεκτρονικών Υπολογιστών, οι οποίοι είναι συνδεδεμένοι μεταξύ τους με κάποιο φυσικό μέσο και επικοινωνούν μεταξύ τους, μέσω αυτού του φυσικού μέσου, χρησιμοποιώντας κάποιους κοινά αποδεκτούς κανόνες. Οι κανόνες αυτοί που διέπουν τον τρόπο επικοινωνίας των υπολογιστών ενός δικτύου, ονομάζονται "**πρωτόκολλα του δικτύου**". Ένα ειδικό πρωτόκολλο μπορεί να καθιερωθεί για έναν ιδιαίτερο συγκεκριμένο σκοπό.

Ο όρος AD_HOC υπονοεί ότι αυτό το δίκτυο είναι ένα δίκτυο που καθιερώνεται για μια ειδική, συχνά αυτοσχέδια υπηρεσία που προσαρμόζεται στις εφαρμογές. Έτσι, το χαρακτηριστικό Ad Hoc δίκτυο οργανώνεται για μια περιορισμένη χρονική περίοδο. Τα πρωτόκολλα είναι συντονισμένα στην ιδιαίτερη εφαρμογή. Η εφαρμογή μπορεί να είναι δυναμική, όπως επίσης και το περιβάλλον μπορεί να αλλάξει δυναμικά. Συνεπώς, τα ειδικά πρωτόκολλα πρέπει να προσαρμοστούν στις αλλαγές περιβάλλοντος, κυκλοφορίας και αποστολής. Οι κόμβοι δεν έχουν την γνώση τοπολογίας του δικτύου γύρω τους και πρέπει να την ανακαλύψουν. Η βασική ιδέα είναι ότι ένας νέος κόμβος (προαιρετικά) αναγγέλλει την παρουσία του και ακούει για να μεταδώσει ραδιοφωνικά τις ανακοινώσεις από τους γείτονές του. Ο κόμβος μαθαίνει για τους νέους κοντινούς κόμβους και τους τρόπους να επιτευχθεί επικοινωνία, και μπορεί να αναγγείλει τον τρόπο για να φθάσει σε εκείνους τους κόμβους. Καθώς ο χρόνος συνεχίζεται, κάθε κόμβος ξέρει για όλους τους άλλους κόμβους και έναν ή περισσότερους τρόπους πώς να φθάσει σε αυτούς. Αυτά τα δίκτυα φαίνεται ότι θα υποστηρίζουν δυναμικές τοπολογίες, που μερικές φορές θα αλλάζουν γρήγορα.

Τα μοναδικά χαρακτηριστικά σχεδιασμού των ad hoc δικτύων που τα κάνουν να ξεχωρίζουν από τα άλλα δίκτυα είναι στις περιοχές πρωτοκόλλου δικτύων και μεταφορών (ειδικό TCP, πρωτόκολλα δρομολόγησης). Αφού αρχικά δούμε κάποιες πληροφορίες για το πρωτόκολλο που χρησιμεύει στη μεταφορά δεδομένων μεταξύ δικτύων Ηλεκτρονικών Υπολογιστών **TCP/ATP**, στη συνέχεια θα αναλύσουμε τα πρωτόκολλα δρομολόγησης ειδικών δικτύων.

Το **TCP** είναι ένα πρωτόκολλο που χρησιμεύει στη μεταφορά δεδομένων μεταξύ δικτύων Ηλεκτρονικών Υπολογιστών. Είναι το πρωτόκολλο εκείνο το οποίο εξασφαλίζει ότι τα δεδομένα που στέλνονται από ένα υπολογιστή σε έναν άλλον, θα φτάσουν σωστά και οπωσδήποτε. Διάφορες προηγούμενες εργασίες έχουν δείξει ότι το TCP εκφέρει κακή απόδοση στα κινητά Ad hoc δίκτυα. Ο λόγος είναι ότι κινητά Ad Hoc δίκτυα συμπεριφέρονται με έναν σημαντικά διαφορετικό τρόπο από τα παραδοσιακά συνδεδεμένα με καλώδιο δίκτυα. Ειδικότερα, οι αποτυχίες διαδρομών και οι αλλαγές διαδρομών λόγω στην κινητικότητα κόμβων μπορούν να είναι συχνά γεγονότα σε MANETs. Επιπλέον, τα

φαινόμενα συμφόρησης σε MANETs είναι ουσιαστικά διαφορετικά από τα παραδοσιακά συνδεδεμένα με καλώδιο δίκτυα. Στη συνέχεια θα αναλύσουμε τα πρωτόκολλα δρομολόγησης των Ad Hoc δικτύων.

2.1 ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ ΤΩΝ AD HOC ΔΙΚΤΥΩΝ

Τα παραδοσιακά πρωτόκολλα δρομολόγησης είναι δυναμικά δεδομένου ότι διατηρούν τις διαδρομές σε όλους τους κόμβους, συμπεριλαμβανομένων των κόμβων στους οποίους κανένα πακέτο δεν στέλνεται. Αντιδρούν σε οποιαδήποτε αλλαγή στην τοπολογία ακόμα κι αν καμία κυκλοφορία δεν επηρεάζεται από την αλλαγή, και απαιτούν τα περιοδικά μηνύματα ελέγχου για να διατηρήσουν τις διαδρομές σε κάθε κόμβο στο δίκτυο. Καταλαβαίνουμε λοιπόν, ότι τα κλασικά πρωτόκολλα δρομολόγησης δεν μπορούν να εξυπηρετήσουν τις απαιτήσεις των ειδικών δικτύων.

Για τα κινητά Ad Hoc δίκτυα, το ζήτημα της δρομολόγησης των πακέτων μεταξύ οποιουδήποτε ζευγαριού κόμβων γίνεται ένας προκλητικός στόχος επειδή οι κόμβοι μπορούν να κινηθούν τυχαία μέσα στο δίκτυο. Ολόκληρο το δίκτυο είναι βασισμένο στην ιδέα των συσκευών που χρησιμεύουν και ως δρομολογητές και ως οικοδεσπότες συγχρόνως. Η κινητικότητα αυτή των κόμβων μπορεί να επηρεάσει σημαντικά την απόδοση του δικτύου. Μια πορεία που θεωρήθηκε βέλτιστη σε ένα δεδομένο χρονικό σημείο μπορεί να μην λειτουργήσει λίγο αργότερα. Επιπλέον, οι πιθανολογικές ιδιότητες των ασύρματων καναλιών προσθέτουν στην αβεβαιότητα της ποιότητας πορειών. Επομένως, η τυχαιότητα και η μεταβλητότητα της τοπολογίας ενός ad hoc δικτύου απαιτεί την διαμόρφωση κανόνων (αποδοτικά πρωτόκολλα δρομολόγησης) σύμφωνα με τους οποίους θα δρομολογείται κατάλληλα η κίνηση των δεδομένων ανάμεσα στους κόμβους. Το δίκτυο πρέπει να είναι σε θέση να αλλάξει προσαρμοστικά τη δρομολόγηση για να αποφύγει οποιαδήποτε από αυτά τα αποτελέσματα. Τα πρωτόκολλα δρομολόγησης ειδικών δικτύων είναι αυτό-εκκινούμενα, προσαρμόζονται στις αλλαγές ενός δικτύου, και σχεδόν εξ ορισμού προσφέρουν μονοπάτια πολλαπλών αλμάτων διαμέσου του δικτύου, από την πηγή προς τον προορισμό.

2.2 ΣΤΟΧΟΙ ΠΡΩΤΟΚΟΛΛΩΝ ΕΙΔΙΚΩΝ ΔΙΚΤΥΩΝ

1. Υψηλή ρυθμαπόδοση
2. Χαμηλή μέση καθυστέρηση
3. Υποστήριξη ετερογενούς κίνησης (δεδομένα, φωνή, video)
4. Κλιμάκωση
5. Εξοικονόμηση ενέργειας
6. QoS (ποιότητα της υπηρεσιών)

Είναι σημαντικό να συζητηθούν εν συντομία τα υπάρχοντα πρωτόκολλα δρομολόγησης που υπάρχουν για τα Ad Hoc δίκτυα. Πολλά πρωτόκολλα δρομολόγησης έχουν σχεδιαστεί για να ανακαλύψουν και να διατηρήσουν τις διαδρομές μεταξύ των κόμβων πηγής και προορισμού. Τα πρωτόκολλα δρομολόγησης μπορούν γενικά να κατηγοριοποιηθούν στους τρεις αλγόριθμους δρομολόγησης που θα δούμε στη συνέχεια, οι οποίοι είναι και οι σημαντικότεροι. Κάθε ένας από αυτούς τους τρεις βασικούς τύπους

έχει τα πλεονεκτήματα, τα μειονεκτήματα, και την καταλληλότητα χρήσης του σε ορισμένους τύπους ειδικών δικτύων ανάλογα με την κινητικότητα, τον αριθμό κόμβων σχετικών, την πυκνότητα κόμβων, την ελλοχεύουσα τεχνολογία στρώματος συνδέσεων, και τα γενικά χαρακτηριστικά του υποστήριξης του περιβάλλοντος και των εφαρμογών.

2.3 Οι τρεις αλγόριθμοι δρομολόγησης είναι:

(1) **PROACTIVE (table-driven) (δυναμικός)** όπως το διανυσματικό πρωτόκολλο απόστασης (DSDV).

(2) **REACTIVE (on-demand) (αντιδραστικός)** όπως DSR, AODV, και TORA.

(3) Κατηγορία των υβριδικών (**HYBRID**) σχημάτων δρομολόγησης που, στην ουσία, συνδυάζει χαρακτηριστικά και των δύο παραπάνω κατηγοριών (Εδώ ανήκει το ZRP πρωτόκολλο δρομολόγησης).

Οι αλγόριθμοι δρομολόγησης πρέπει να:

- Κρατούν τον πίνακα δρομολόγησης εύλογα μικρό
- Επιλέγουν *την καλύτερη* διαδρομή για το δεδομένο προορισμό (Αυτό μπορεί να γίνει με βάση, ποια είναι η γρηγορότερη, ποιο αξιόπιστη, υψηλότερη ρυθμαπόδοση, ή φτηνότερη διαδρομή)
- Ενημερώνουν τον πίνακα όταν κινούνται οι κόμβοι, ή ενώνονται σε μια ομάδα
- Απαιτούν μικρό ποσό μηνυμάτων/χρόνο σύγκλισης.

Στον παρακάτω πίνακα μπορούμε να δούμε πώς τα πρωτόκολλα δρομολόγησης κατηγοριοποιούνται στα: α) Proactive/Table-Driven, β) Reactive/On-Demand και γ) HYBRID

Πίνακας 1: ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ

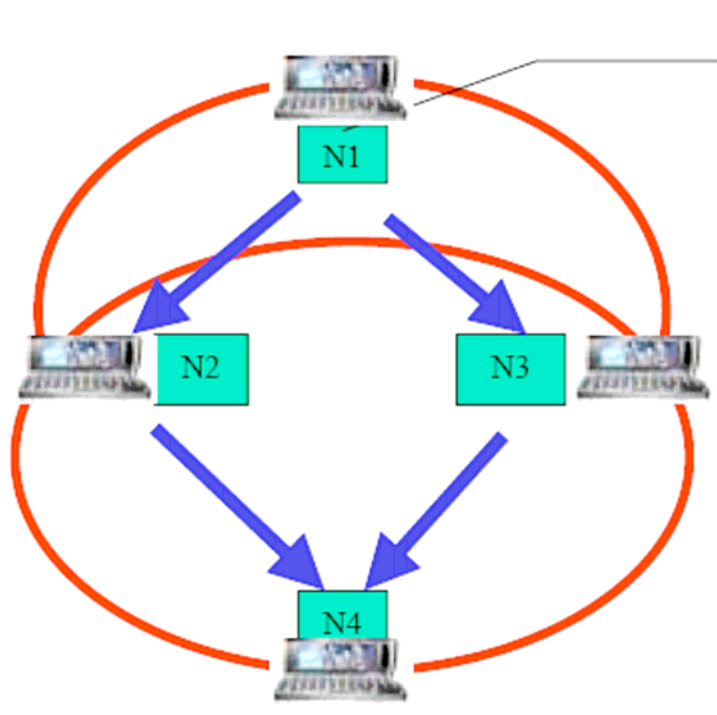
Table driven (proactive) Καθοδηγούμενος από πίνακα δρομολόγησης (δυναμικός)	On-demand driven (reactive) Καθοδηγούμενος κατ' απαίτηση (αντιδραστικός)	Hybrid Υβριδικό
Διανυσματικό πρωτόκολλο απόστασης (DSDV)	Δρομολόγηση σταθερότητας σημάτων (SSR)	Πρωτόκολλο δρομολόγησης ζώνης (ZRP)
Ασύρματο πρωτόκολλο δρομολόγησης (wtrp)	Δυναμική δρομολόγηση πηγής (DSR)	Πρωτόκολλο δρομολόγησης κρίσιμων πορειών (CPR)
Δρομολόγηση πυλών διακοπών συστάδων (CSGR)	Προσωρινός διαταγμένος αλγόριθμος δρομολόγησης (TORA)	
Προσαρμοστική δρομολόγηση δέντρων πηγής (STAR)	AD HOC στη διανυσματική δρομολόγηση απόστασης απαίτησης (AODV)	
	Σχετική δρομολόγηση Microdiversity απόστασης (RDMAR)	
	Βασισμένο στο Associativity πρωτόκολλο δρομολόγησης (ABR)	

2.3.1 Table-driven Προσεγγίσεις

Στα δυναμικά πρωτόκολλα, οι κόμβοι ψάχνουν συνεχώς για τη δρομολόγηση των πληροφοριών μέσα σε ένα δίκτυο, έτσι ώστε όταν απαιτείται μια διαδρομή, η διαδρομή είναι ήδη γνωστή. Επιδιώκουν συγκεκριμένα να διατηρήσουν συνεκτική και συνεχώς ενημερωμένη την πληροφορία δρομολόγησης από κάθε κόμβο σε οποιοδήποτε άλλο κόμβο στο δίκτυο. Αυτά τα σχήματα δρομολόγησης απαιτούν από κάθε κόμβο να διατηρεί έναν ή περισσότερους πίνακες ώστε να συντηρεί την πληροφορία δρομολόγησης, και να έχει τη δυνατότητα να ανταποκρίνεται στις αλλαγές της δικτυακής τοπολογίας. Υπάρχουν κυρίως τέσσερα πρωτόκολλα κάτω από αυτήν την κατηγορία:

DSDV - Είναι ένα διανυσματικό πρωτόκολλο απόστασης. Αυτό το πρωτόκολλο είναι βασισμένο στον κλασικό αλγόριθμο δρομολόγησης Bellman-Ford. Στο DSDV, κάθε κόμβος διατηρεί έναν πίνακα (κατάλογο) δρομολόγησης που συνεχώς και περιοδικά ενημερώνεται (μη κατόπιν παραγγελίας) και διαφημίζεται σε κάθε ένα από τους τρέχοντες γείτονες του κόμβους. Κάθε είσοδος είναι μαρκαρισμένη με έναν αριθμό

ακολουθίας. Προκειμένου να τηρηθούν οι εκτιμήσεις απόστασης ενήμερες κάθε κόμβος ελέγχει τις εξερχόμενες συνδέσεις του, και μεταδίδει περιοδικά σε όλους τους γείτονές του την τρέχουσα εκτίμησή του, της πιο σύντομης απόστασης με κάθε άλλο κόμβο στο δίκτυο. Το διάλυσμα απόστασης που μεταδίδεται περιοδικά περιέχει μια είσοδο για κάθε κόμβο στο δίκτυο που περιλαμβάνει την απόσταση από τον κόμβο που εκπέμπει στον προορισμό. Κάθε κόμβος ενημερώνεται περιοδικά με νέες πληροφορίες που είναι διαθέσιμες. Τα στοιχεία που μεταδίδονται ραδιοφωνικά από κάθε κόμβο περιέχουν το νέο αριθμό ακολουθίας του και τις ακόλουθες πληροφορίες για κάθε νέα διαδρομή: διεύθυνση προορισμού, αριθμός σταθμών για να φθάσει στον προορισμό και αριθμό ακολουθίας των πληροφοριών που παραλαμβάνονται σχετικά με εκείνο τον προορισμό, όπως αρχικά σφραγίζεται από τον προορισμό. Οι διαδρομές με τους πιο πρόσφατους αριθμούς ακολουθίας είναι πάντα η προτιμητέα βάση για τις αποφάσεις. Από τις πορείες με τον ίδιο αριθμό ακολουθίας, εκείνοι με μικρότερο αριθμό σταθμών στον προορισμό τους θα χρησιμοποιηθούν.



Εικόνα 2: Απεικόνιση του πρωτοκόλλου δρομολόγησης DSDV

Το σχήμα παρουσιάζει ότι ένα δίκτυο αποτελείται από τέσσερις κόμβους (N1, N2, N3, και N4). Οι κόμβοι 1, 2 και 3 είναι σε μια περιοχή κάλυψης και οι κόμβοι 2, 3 και 4 σε μια άλλη περιοχή κάλυψης. Εάν εξετάσουμε τον κόμβο 1, έχει μόνο μία διαδρομή που μπορεί να ακολουθήσει για να επικοινωνήσει με τον κόμβο 2 και 3 και δύο διαδρομές που μπορεί να ακολουθήσει για να επικοινωνήσει με στον κόμβο 4. Μια, μέσω του κόμβου 2 και άλλη μια μέσω του κόμβου 3. Κατόπιν ο πρώτος κόμβος έχει έναν πίνακα δρομολόγησης που έχει όλες τις πληροφορίες για αυτές τις τέσσερις διαδρομές όπως φαίνεται στην εικόνα 1.

Μειονεκτήματα: Το πρωτόκολλο απαιτεί την επιλογή των ακόλουθων παραμέτρων: το περιοδικό διάστημα αναπροσαρμογών, η μέγιστη τιμή του " χρόνου εγκατάστασης" για έναν προορισμό και ο αριθμός διαστημάτων αναπροσαρμογών που απαιτούνται πριν από μια διαδρομή. Ακόμη υπάρχει και ο καταναγκασμός κάθε κόμβου να εκτελεί ελέγχους συνοχής σε πληροφορίες που αναφέρθηκαν από όλους τους γείτονές του.

WRP - Η καινοτομία του WRP σχετίζεται με τον τρόπο με τον οποίο επιτυγχάνεται η αποφυγή βρόχων. Στο WRP, οι κόμβοι δρομολόγησης επικοινωνούν και ανταλλάσσουν πληροφορία για την απόσταση και τα άλματα από το δεύτερο μέχρι και το τελευταίο, για κάθε προορισμό στο ασύρματο δίκτυο. Το WRP ανήκει στην κατηγορία των αλγορίθμων εύρεσης μονοπατιού με μία σημαντική εξαίρεση. Αποφεύγει τα προβλήματα μέτρησης μέχρι το άπειρο με το να υποχρεώνει κάθε κόμβο να εκτελεί ελέγχους συνοχής σε προηγούμενες πληροφορίες που αναφέρθηκαν από όλους τους γείτονές του. Για να διασφαλιστεί η ακρίβεια της πληροφορίας δρομολόγησης, οι κόμβοι στέλνουν περιοδικά μηνύματα ενημέρωσης στους γείτονές τους. Ένα τέτοιο μήνυμα περιλαμβάνει μία λίστα από ενημερώσεις (τον προορισμό, την απόσταση από τον προορισμό, τον προκάτοχο του προορισμού), όπως επίσης και μία λίστα από απαντήσεις που υποδεικνύουν ποιο κινητό τερματικό θα έπρεπε να επιβεβαιώσει την ενημέρωση. Ένα κινητό στέλνει μηνύματα ενημέρωσης αφού επεξεργαστεί τις ενημερώσεις από τους γείτονες ή όταν ανιχνεύσει μία αλλαγή στη ζεύξη. Στην περίπτωση μιας αποτυχίας στην ζεύξη, οι κόμβοι που ανιχνεύουν τη βλάβη θα στείλουν μηνύματα ενημέρωσης στους γείτονές τους, και αυτοί οι γείτονες θα τροποποιήσουν τις εισόδους στους πίνακες απόστασης και θα ελέγξουν για νέα πιθανά μονοπάτια μέσω άλλων κόμβων.

Στο WRP, οι κόμβοι μαθαίνουν για την ύπαρξη των γειτόνων τους από την απόδειξη των επιβεβαιώσεων και άλλα μηνύματα. Αν ένας κόμβος δεν στέλνει πακέτα, πρέπει να στείλει ένα HELLO μήνυμα μέσα σε ένα συγκεκριμένο χρονικό διάστημα ώστε να διασφαλίσει την έγκυρη κι άμεση πληροφορία συνδεσιμότητας. Αλλιώς, η έλλειψη μηνυμάτων από τον κόμβο μπορεί να υποδείξει την αποτυχία αυτής της ασύρματης ζεύξης, γεγονός που μπορεί να προκαλέσει λανθασμένο συναγερμό. Όταν ένας κόμβος λαμβάνει ένα HELLO μήνυμα από ένα νέο κόμβο, αυτή η νέα πληροφορία για τον κόμβο προστίθεται στον πίνακα δρομολόγησης του κόμβου, και ο κόμβος αυτός στέλνει στο νέο κόμβο ένα αντίγραφο από την πληροφορία που έχει στον πίνακα δρομολόγησης του.

Το WRP πρέπει να διατηρεί τέσσερις πίνακες, ονομαστικά:

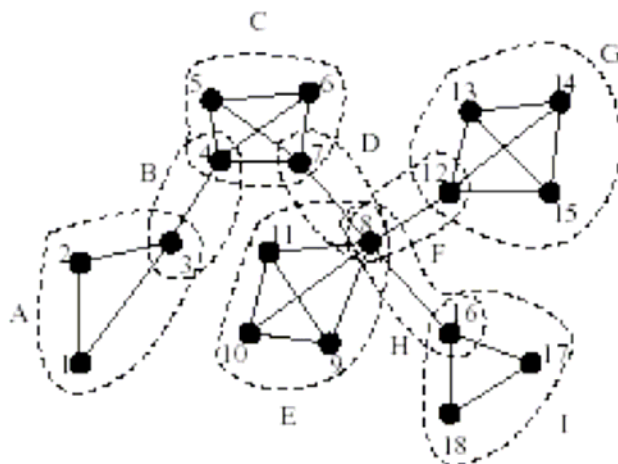
- α) πίνακας απόστασης,
- β) πίνακας δρομολόγησης,
- γ) πίνακας κόστους ζεύξης, και
- δ) πίνακας λίστας επαναμεταδιδόμενων μηνυμάτων (Message Retransmission List – MRL).

Ο πίνακας απόστασης αναφέρει τον αριθμό αλμάτων μεταξύ ενός κόμβου και του προορισμού του. Ο πίνακας δρομολόγησης αναφέρει τον κόμβο κατά το επόμενο άλμα. Ο πίνακας κόστους ζεύξης αντανακλά την συσχέτιση μεταξύ καθυστέρησης και μίας συγκεκριμένης ζεύξης. Ο MRL περιλαμβάνει τον σειριακό αριθμό των μηνυμάτων

ενημέρωσης, έναν μετρητή επαναμετάδοσης, ένα διάνυσμα σημαίας που απαιτεί επιβεβαίωση, και μία λίστα από επιβεβαιώσεις που στάλθηκαν με τα αντίστοιχα μηνύματα. Ο MRL καταγράφει ποιες ενημερώσεις σε ένα μήνυμα πρέπει να ξανά μεταδοθούν και ποιοι γείτονες πρέπει να επιβεβαιώσουν την επαναμετάδοση.

CSGR - Το CSGR είναι ένα πρωτόκολλο δρομολόγησης όπου οι κινητοί κόμβοι ταξινομούνται σε ομάδες και κάθε ομάδα έχει έναν επικεφαλής. Αυτή η ομαδοποίηση εισάγει μία μορφή ιεραρχίας. Ο επικεφαλής της ομάδας μπορεί να ελέγξει έναν αριθμό από κινητά τερματικά, και η ομαδοποίηση προσφέρει ένα πλαίσιο εργασίας για το διαχωρισμό του κώδικα (ανάμεσα στις ομάδες), την πρόσβαση καναλιών, τη δρομολόγηση, και την κατανομή εύρους ζώνης. Χρησιμοποιεί DSDV κρυμμένο κάτω από αλγόριθμο δρομολόγησης και κάθε κόμβος διατηρεί έναν πίνακα μελών συστάδων και έναν πίνακα δρομολόγησης. Για την επιλογή του επικεφαλής, εφαρμόζεται ένας καταναμημένος αλγόριθμος επιλογής. Αν και η χρησιμοποίηση ενός επικεφαλής ομάδας επιτρέπει κάποιο βαθμό ελέγχου και συνεργασίας, από την άλλη πλευρά υποθέτει την εξάρτηση από άλλους κόμβους μέσα στην ομάδα. Όταν ένας επικεφαλής της ομάδας κινηθεί μακριά, κάποιος άλλος επικεφαλής πρέπει να εκλεγεί. Αυτό μπορεί να προκαλεί πρόβλημα αν ένας επικεφαλής αλλάζει συχνά και οι κόμβοι σπαταλούν μεγάλο μέρος του χρόνου συγκλίνοντας προς το νέο επικεφαλής αντί να προωθούν δεδομένα προς την επιθυμητή κατεύθυνση. Για να αποφευχθεί η πρόκληση επανεκλογής επικεφαλής κάθε φορά που η σύσταση της ομάδας αλλάζει, εισάγεται ένας αλγόριθμος κατά τον οποίο οι επικεφαλής αλλάζουν μόνο όταν δύο επικεφαλής έρθουν σε επαφή ή όταν ένας κόμβος κινηθεί έξω από τα όρια όλων των άλλων κόμβων που είναι επικεφαλής.

Όπως φαίνεται και στο σχήμα παρακάτω, ένας αριθμός από κόμβους (18 στην συγκεκριμένη περίπτωση) μπορούν να χωριστούν σε ομάδες (Α μέχρι Ι) ανάλογα με την τοπολογία του δικτύου που συνιστούν και την συνδεσιμότητα κάθε κινητού τερματικού. Στη συνέχεια, σε κάθε ομάδα επιλέγεται ο επικεφαλής και γίνεται διαπραγμάτευση για τους κόμβους-πύλες που θα είναι υπεύθυνοι για την ανταλλαγή της πληροφορίας με τις άλλες ομάδες.



Εικόνα 2: Επικοινωνία σύμφωνα με το CSGR πρωτόκολλο δρομολόγησης

Μειονεκτήματα: Μερικοί κόμβοι (επικεφαλής συστάδων και οι κόμβοι πυλών) έχουν υψηλότερο φορτίο υπολογισμού και επικοινωνίας από άλλους κόμβους. Η αξιοπιστία δικτύων μπορεί επίσης να επηρεαστεί λόγω αποτυχίας σύνδεσης των κόμβων που είναι επικεφαλής των ομάδων.

STAR – Το STAR είναι ένα πρωτόκολλο δρομολόγησης που δεν απαιτεί τις περιοδικές αναπροσαρμογές δρομολόγησης (δεν χρησιμοποιεί περιοδικά μηνύματα για να ενημερώσει τους γείτονές του), ούτε προσπαθεί να διατηρήσει τις βέλτιστες διαδρομές στους προορισμούς (δεν παίρνει τις κοντινότερες πορείες για την κράτηση των μηνυμάτων ελέγχου). Το STAR είναι μια προσπάθεια να δημιουργηθεί η ίδια απόδοση δρομολόγησης με τα άλλα table driven πρωτόκολλα και να είναι ακόμα ίσο ή καλύτερο στην απόδοση εύρους ζώνης.

Εάν αλλαγές τοπολογίας εμφανίζονται συχνά, το ποσοστό στις αναπροσαρμογές αυξάνεται εντυπωσιακά. Αυτό οδηγεί σε ένα σενάριο όπου περισσότερα μηνύματα ελέγχου είναι παρόντα στο δίκτυο από το στοιχείο χρηστών, το οποίο είναι ανεπιθύμητο. Το STAR προσπαθεί να μειώσει τον αριθμό δρομολόγησης των αναπροσαρμογών. Το STAR χρησιμοποιεί ένα ελλοχεύον πρωτόκολλο ανακαλύψεων γειτόνων για να ανακαλύψει την παρουσία και την κινητικότητα των γειτονικών κόμβων. Κάθε κόμβος διατηρεί ένα δέντρο πηγής. “Το σύνολο συνδέσεων που χρησιμοποιούνται από έναν δρομολογητή στην προτιμημένη πορεία του σε έναν προορισμό καλείται δέντρο πηγής του δρομολογητή.” Κάθε κόμβος ξέρει τις παρακείμενες συνδέσεις του και τα δέντρα πηγής που αναφέρονται από τους γείτονές του. Κάθε κόμβος τρέχει έναν αλγόριθμο επιλογής διαδρομών στο δέντρο πηγής του για να παράγει έναν πίνακα δρομολόγησης που διευκρινίζει το διάδοχο σε κάθε προορισμό. Για να μειωθεί ο αριθμός αναπροσαρμογών, μόνο οι αλλαγές στην ισχύ του δέντρου πηγής διαδίδονται. Τέτοιες αλλαγές συμβαίνουν όταν η πηγή χάνει όλες τις πορείες σε έναν προορισμό, ανιχνεύει έναν νέο γείτονα, ή αντιμετωπίζει έναν εκκρεμή μακροπρόθεσμο βρόχο δρομολόγησης.

2.3.2 Source initiated/On demand Προσεγγίσεις

Αυτός ο τύπος δρομολόγησης δημιουργεί μονοπάτια μόνο όταν είναι επιθυμητό από τον κόμβο της πηγής. Όταν ο κόμβος απαιτεί ένα δρόμο για τον προορισμό, εκκινεί μία διαδικασία εύρεσης δρόμου μέσα στο δίκτυο. Αυτή η διεργασία ολοκληρώνεται μόλις βρεθεί μία διαδρομή ή έχουν εξεταστεί όλοι οι πιθανοί συνδυασμοί δρόμων. Όταν ανακαλυφθεί κι εγκατασταθεί μία διαδρομή, διατηρείται με την βοήθεια ενός είδους διαδικασίας συντήρησης του δρόμου μέχρι που ο προορισμός να καταστεί μη προσβάσιμος από οποιοδήποτε μονοπάτι ή από την πηγή, ή διαδρομή να μην είναι πλέον επιθυμητή. Υπάρχουν κυρίως πέντε πρωτόκολλα κάτω από αυτήν την κατηγορία:

SSR - Είναι ένα πρωτόκολλο δρομολόγησης που επιλέγει διαδρομές βασισμένες στην ισχύ των καναλιών μεταξύ των κόμβων και στη σταθερότητα θέσης ενός κόμβου. Το SSR συμπεριλαμβάνει δύο πρωτόκολλα που συνεργάζονται μεταξύ τους: το δυναμικό πρωτόκολλο δρομολόγησης (**DRP**) και το στατικό πρωτόκολλο δρομολόγησης (**SRP**).

Το DRP διατηρεί τον πίνακα σταθερότητας σημάτων (Signal Stability Table (SST)) και τον πίνακα δρομολόγησης (Routing Table (RT)). Ο SST αποθηκεύει την ισχύ σημάτων των γειτονικών κόμβων που λαμβάνεται από τα περιοδικά αναγνωριστικά σήματα από το στρώμα συνδέσεων κάθε γειτονικού κόμβου. Ανάλογα την ισχύ σημάτων κάθε κανάλι καταγράφεται σαν ισχυρό ή αδύνατο. Όλες οι μεταδόσεις παραλαμβάνονται από DRP και επεξεργάζονται. Αφού ενημερώσει κατάλληλα το πίνακα καταχωρήσεων, το DRP παραχωρεί το πακέτο στο SRP.

Το SRP προωθεί το πακέτο, αν εντοπίσει τον προοριζόμενο δέκτη. Αν όχι, επανεξετάζεται ο προορισμός στο RT και προωθείται το πακέτο. Εάν δεν υπάρχει καμία είσοδος για τον προορισμό στο RT, κινείται μια διαδικασία αναζήτησης-διαδρομής για να βρεθεί μια διαδρομή. Τα πακέτα αιτήματος-διαδρομής διαβιβάζονται στον επόμενο σταθμό μόνο εάν παραλαμβάνονται από ισχυρά κανάλια και δεν έχουν υποβληθεί σε επεξεργασία προηγουμένως (για αποφυγή επανάληψης). Ο προορισμός παίρνει το πρώτο πακέτο αναζήτησης-διαδρομής που φτάνει για να απαντήσει όπως είναι ιδιαίτερα πιθανό ότι το πακέτο έφθασε πέρα από την κοντύτερη ή/και λιγότερη κορεσμένη πορεία. Το DRP αντιστρέφει την επιλεγμένη διαδρομή και στέλνει ένα μήνυμα αποδοχής της διαδρομής. Το DRP των κόμβων κατά μήκος της πορείας ενημερώνει τον πίνακα δρομολόγησης (RTs) τους αναλόγως. Τα πακέτα αναζήτησης-διαδρομής που φθάνουν στον προορισμό έχουν φθάσει σίγουρα από το κανάλι με το πιο ισχυρό σήμα επειδή τα πακέτα που φθάνουν πέρα από ένα αδύνατο κανάλι πέφτουν στους ενδιάμεσους κόμβους. Όταν μια αποτυχία συνδέσεων ανιχνεύεται μέσα στο δίκτυο, οι ενδιάμεσοι κόμβοι στέλνουν ένα μήνυμα λάθους στην πηγή που προσδιορίζει ποιο κανάλι έχει αποτύχει. Η πηγή στέλνει έπειτα ένα μήνυμα για να ενημερώσει όλους τους κόμβους για τη σπασμένη σύνδεση και κινεί μια νέα διαδικασία αναζήτησης-διαδρομής για να βρει μια νέα πορεία στον προορισμό.

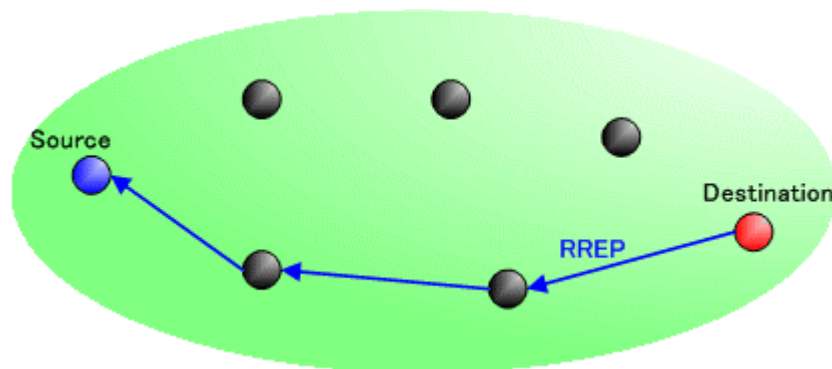
DSR - Είναι ένα πρωτόκολλο δρομολόγησης πηγής. Κάθε κόμβος διατηρεί κρύπτη διαδρομών που περιέχει όλες τις πηγές διαδρομών που γνωρίζει. Ο κόμβος ενημερώνει τις καταχωρήσεις στην κρύπτη διαδρομών όταν μαθαίνει για νέες διαδρομές. Το DSR απαιτεί κάθε πακέτο να κρατά τις πληροφορίες διαδρομών του, εξαλείφοντας κατά συνέπεια την ανάγκη για κάθε κόμβο στο δίκτυο να κάνει περιοδικές εκπομπές ανακαλύψεων διαδρομών σε άλλους κόμβους. Οι δύο σημαντικές φάσεις του πρωτοκόλλου είναι ανακάλυψη διαδρομών και συντήρηση διαδρομών. Όταν ο κόμβος πηγής θέλει να στείλει ένα πακέτο σε έναν προορισμό, ανατρέχει στην κρύπτη διαδρομών του για να καθορίσει εάν περιέχει ήδη μια διαδρομή στον προορισμό αυτό. Εάν διαπιστώνει ότι μια ισχύουσα διαδρομή στον προορισμό υπάρχει, κατόπιν χρησιμοποιεί αυτήν την διαδρομή για να στείλει το πακέτο. Αλλά εάν ο κόμβος δεν έχει μια τέτοια διαδρομή, τότε κινεί τη διαδικασία ανακαλύψεων διαδρομών με τη ραδιοφωνική αναμετάδοση ενός RREQ. Το πακέτο RREQ περιέχει τη διεύθυνση της πηγής και του προορισμού, και έναν μοναδικό αριθμό αναγνώρισης. Για να περιορίσει τον αριθμό αιτημάτων διαδρομών που διαδίδονται, ένας κόμβος επεξεργάζεται το πακέτο αιτήματος διαδρομών μόνο εάν δεν έχει δει ήδη το πακέτο και η διεύθυνσή του (κόμβου) δεν είναι παρούσα στο αρχείο διαδρομών του πακέτου. “Ένα πακέτο RREQ που φθάνει σε έναν τέτοιο κόμβο περιέχει ήδη, στο αρχείο διαδρομών του και την ακολουθία των σταθμών που ακολουθεί για να φτάσει σε αυτό τον κόμβο”. Κάθε ενδιάμεσος κόμβος ελέγχει εάν ξέρει μια διαδρομή προς στον προορισμό. Εάν όχι, επισυνάπτει τη διεύθυνσή

του στο αρχείο διαδρομών του πακέτου και διαβιβάζει το πακέτο στους γείτονές του. Όταν ένας κόμβος αντιμετωπίζει ένα πρόβλημα μετάδοσης πακέτου, παράγει ένα πακέτο λάθους διαδρομών. Όταν ένας κόμβος λαμβάνει ένα πακέτο λάθους διαδρομών, αφαιρεί το σταθμό που έχει το πρόβλημα από την κρύπτη διαδρομών του. Όλες οι διαδρομές που περιέχουν το σταθμό που έχει πρόβλημα στη μετάδοση πακέτου, διακόπτονται σε εκείνο το σημείο. Τα πακέτα αναγνώρισης χρησιμοποιούνται για να ελέγξουν τη σωστή λειτουργία των συνδέσεων διαδρομών. Αυτό περιλαμβάνει επίσης τις αναγνώρισεις στις οποίες ένας κόμβος ελέγχει αν ο επόμενος σταθμός μπορεί να δεχτεί πακέτα κατά μήκος της διαδρομής που τους ενώνει.

Μειονεκτήματα: Τα πακέτα διαβιβάζονται κατά μήκος των παλαιότερων διαδρομών. Το DSR υποφέρει επίσης από ένα πρόβλημα εξελισσιμότητας λόγω στη φύση της δρομολόγησης πηγής. Δεδομένου ότι το δίκτυο μεγαλώνει, τα πακέτα ελέγχου και τα πακέτα μηνυμάτων γίνονται επίσης μεγαλύτερα. Αυτό δίνει έναν αρνητικό αντίκτυπο λόγω του περιορισμένου εύρους ζώνης.

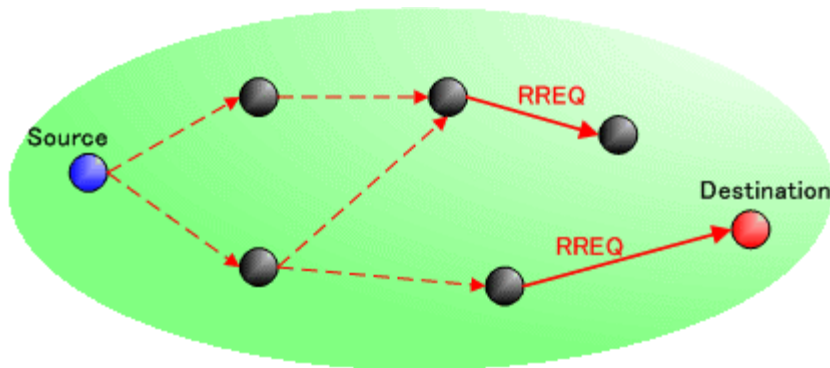
AODV – Αυτός ο αλγόριθμος δρομολόγησης στηρίζεται στον αλγόριθμο DSDV και η βελτίωση είναι στην ελαχιστοποίηση του αριθμού ραδιοφωνικών μεταδόσεων, με τη δημιουργία των διαδρομών σε κατόπιν παραγγελίας βάση, σε αντιδιαστολή με τη διατήρηση ενός πλήρους καταλόγου διαδρομών όπως στον αλγόριθμο DSDV.

Το πρωτόκολλο αυτό χτίζει τις διαδρομές μεταξύ των κόμβων μόνο όπως επιδιώκονται από τους κόμβους πηγής. Διατηρεί αυτές τις διαδρομές εφ' όσον απαιτούνται από τις πηγές. Στο AODV, κάθε κόμβος διατηρεί έναν πίνακα δρομολόγησης που χρησιμοποιείται για να αποθηκεύσει τον προορισμό και τις επόμενες διευθύνσεις σταθμών (IP) καθώς επίσης και τους αριθμούς ακολουθίας προορισμού. Κάθε είσοδος στον πίνακα δρομολόγησης έχει μια διεύθυνση προορισμού, έναν επόμενο σταθμό, έναν κατάλογο κόμβων που θα ακολουθηθούν, μια διάρκεια ζωής, και μια απόσταση στον προορισμό. Για να κινήσει μια διαδικασία ανακαλύψεων διαδρομών ένας κόμβος δημιουργεί ένα πακέτο αιτήματος διαδρομών (RREQ). Το πακέτο περιέχει τη διεύθυνση IP του κόμβου πηγής καθώς επίσης και τη διεύθυνση IP του προορισμού.



Εικόνα 3: Αλγόριθμος δρομολόγησης AODV

Το RREQ περιέχει μια ταυτότητα ραδιοφωνικής μετάδοσης, η οποία αυξάνεται κάθε φορά που εκπέμπει ο κόμβος πηγής ένα RREQ. Η ταυτότητα ραδιοφωνικής μετάδοσης και η διεύθυνση IP του κόμβου πηγής διαμορφώνουν ένα μοναδικό προσδιοριστικό για το RREQ. Ο κόμβος πηγής μεταδίδει ραδιοφωνικά έπειτα το πακέτο και περιμένει μια απάντηση. Όταν ένας ενδιάμεσος κόμβος λαμβάνει ένα RREQ, ελέγχει εάν το έχει δει πριν. Εάν έχει δει το πακέτο προηγουμένως, το απορρίπτει. Διαφορετικά επεξεργάζεται το πακέτο RREQ. Για να επεξεργαστεί το πακέτο ο κόμβος οργανώνει μια αντίστροφη είσοδο διαδρομών για τον κόμβο πηγής στον πίνακα διαδρομών του που περιέχει την ταυτότητα του γείτονα μέσω της οποίας έλαβε το πακέτο RREQ. Όταν ένας κόμβος λαμβάνει το RREQ, καθορίζει εάν πράγματι είναι ο υποδειγμένος προορισμός. Εάν καθένας από τους όρους(που αναφέραμε πιο πάνω) που εξετάζει είναι αληθινός, κατόπιν αυτό στέλνει ένα μήνυμα επανάληψης διαδρομών (RREP) πίσω στην πηγή.



Εικόνα 4: Αλγόριθμος δρομολόγησης AODV

Εάν και οι δύο όροι είναι ψεύτικοι, δηλ. εάν δεν έχει μια διαδρομή και δεν είναι ο υποδειγμένος προορισμός, μεταδίδει ραδιοφωνικά έπειτα το πακέτο στους γείτονές του. Τελικά, ο κόμβος προορισμού θα είναι σε θέση πάντα να αποκριθεί στο μήνυμα RREQ. Όταν ένας ενδιάμεσος κόμβος λαμβάνει το RREP, οργανώνει μια είσοδο πορειών του προορισμού στον πίνακα δρομολόγησης του. Αυτή η είσοδος περιέχει τη διεύθυνση IP του προορισμού, τη διεύθυνση IP του γείτονα από την οποία το RREP έφθασε, και μια αρίθμηση του τελευταίου σταθμού από τον οποίο παρέλαβε το RREP. Μετά από την επεξεργασία του πακέτο RREP, ο κόμβος το διαβιβάζει προς την πηγή. Ο κόμβος μπορεί αργότερα να ενημερώσει τις πληροφορίες δρομολόγησης του εάν ανακαλύπτει μια καλύτερη διαδρομή.

Πλεονεκτήματα: Χρησιμοποιεί το εύρος ζώνης αποτελεσματικά (με την ελαχιστοποίηση του φορτίου δικτύων για την κυκλοφορία ελέγχου και στοιχείων), ανταποκρίνεται στις αλλαγές στην τοπολογία, είναι εξελικτικό και εξασφαλίζει ελεύθερη δρομολόγηση βρόχων.

Μειονεκτήματα: οι κόμβοι χρησιμοποιούν τις κρύπτες δρομολόγησης για να απαντήσουν στις ερωτήσεις διαδρομών. Αυτό οδηγεί στις ανεξέλεγκτες "απαντήσεις" και στις επαναλαμβανόμενες αναπροσαρμογές κρυπτών των κόμβων.

TORA - Ανήκει στην οικογένεια των αλγορίθμων δρομολόγησης αντιστροφής συνδέσεων. Είναι ένα προσαρμοστικό και ιδιαίτερα εξελικτικό πρωτόκολλο δρομολόγησης. Έχει ως σκοπό να ελαχιστοποιήσει την αντίδραση στις τοπολογικές αλλαγές. Τα μηνύματα ελέγχου TORA είναι εντοπισμένα σε ένα πολύ μικρό σύνολο κόμβων κοντά στο περιστατικό μιας τοπολογικής αλλαγής. Για να επιτύχουν αυτό, οι κόμβοι διατηρούν τις πληροφορίες δρομολόγησης για τους παρακείμενους κόμβους (σταθμούς με άμεση επικοινωνία). Το TORA ανακαλύπτει γρήγορα τις πολλαπλάσιες διαδρομές μετά από την απαίτηση. Η διαδρομή δεν είναι απαραίτητο να είναι βέλτιστη, αλλά εγγυάται ότι όλες οι διαδρομές είναι ελεύθερες. Κάθε κόμβος κρατά τις ακόλουθες τιμές: Την παλαιά μοναδική ταυτότητα του κόμβου που καθόρισε το νέο επίπεδο αναφοράς. Μια ετικέτα ρολογιών όπου καταγράφεται ο χρόνος της αποτυχίας συνδέσεων, όπου οι κόμβοι πρέπει να έχουν συγχρονίσει τα ρολόγια με μια εξωτερική χρονική πηγή όπως το GPS.

Ένα μήνυμα που επιστρέφεται από τον προορισμό στην πηγή κρατά τις ακόλουθες τιμές: μια διάδοση που παρουσιάζει την παράμετρο, ύψος του τελευταίου από αυτόν κόμβου και την τρέχουσα μοναδική ταυτότητα του κόμβου αυτού (του αρχικού προορισμού). Τα πρώτα τρία στοιχεία αντιπροσωπεύουν συλλογικά το επίπεδο αναφοράς. Ένα νέο επίπεδο αναφοράς καθορίζεται κάθε φορά που ένας κόμβος χάνει τον τελευταίο προς τα κάτω κρίκο του λόγω αποτυχία συνδέσεως. Όταν ένας κόμβος απαιτεί μια διαδρομή σε έναν προορισμό, θέτει το ύψος (αριθμό) του προορισμού σε 0 και το ύψος όλων των άλλων κόμβων καθορισμένο ως απροσδιόριστο. Μεταδίδει ραδιοφωνικά έπειτα ένα πακέτο ΕΡΩΤΗΣΗΣ με την ταυτότητα του κόμβου προορισμού. Οποιοσδήποτε κόμβος που λαμβάνει αυτό το πακέτο ΕΡΩΤΗΣΗΣ, αποκρίνεται με ένα μήνυμα ΑΝΑΠΡΟΣΑΡΜΟΣΜΕΝΟ. (Η διαφορά στο μήνυμα αυτό από το παλιό είναι ότι το νέο μήνυμα ΕΡΩΤΗΣΗΣ θα φέρει πλέον την ταυτότητά του κόμβου αυτού, καθώς και το ύψος του μέσα στο δίκτυο). Οποιοσδήποτε κόμβος που λαμβάνει ένα πακέτο ΑΝΑΠΡΟΣΑΡΜΟΓΩΝ θέτει το ύψος του στο ένα περισσότερο από τον κόμβου που παρήγαγε την ΑΝΑΠΡΟΣΑΡΜΟΓΗ (Τον προηγούμενο κόμβο). Ένας κόμβος με το υψηλότερο ύψος εξετάζεται προς τα πάνω και ένας κόμβος με το χαμηλότερο ύψος προς τα κάτω. Πλημμύρα πακέτων ΑΝΑΠΡΟΣΑΡΜΟΓΩΝ ολοκληρώνει τις πληροφορίες διαδρομών. Ο προορισμός απαντά με μήνυμα ΑΝΑΠΡΟΣΑΡΜΟΓΩΝ με το τρέχον ύψος του όσον αφορά τον προορισμό. Ενώ το μήνυμα ΑΝΑΠΡΟΣΑΡΜΟΓΩΝ διαδίδεται προς τα πίσω, κάθε κόμβος στην πορεία θέτει το ύψος του σε μια αξία μεγαλύτερη από το ύψος του προηγούμενου γειτονικού κόμβου, και τελικά διαβιβάζεται το μεγαλύτερο ύψος στον αρχικό κόμβο. Όταν ένας ενδιαμέσος κόμβος ανακαλύπτει ότι δεν μπορεί να διαβιβάσει τα στοιχεία στον επόμενο σταθμό, αυξάνει το ύψος του σε έναν αριθμό μεγαλύτερο από τους γείτονές του, και διαβιβάζει το πακέτο ΑΝΑΠΡΟΣΑΡΜΟΓΩΝ. Εάν κανένας από τους γειτονικούς κόμβους του δεν έχει οποιοδήποτε ύψος, ξανά ξεκινά τον αλγόριθμο από εκείνο το σημείο. Εάν οποιοσδήποτε κόμβος ανιχνεύει το υπερβολικό χάρισμα διαδρομών ή δικτύων, στέλνει ένα ΣΑΦΕΣ μήνυμα και αφαιρεί τις άκυρες

διαδρομές από το δίκτυο. Στη φάση συντήρησης διαδρομών, ένα πακέτο ραδιοφωνικής μετάδοσης (CLR) στο δίκτυο αναλαμβάνει να σβήσει τις άκυρες διαδρομές

Πλεονεκτήματα : Παρέχει τις ελεύθερες πορείες βρόχων κάθε στιγμή. Παρέχει πολλαπλάσιες διαδρομές έτσι ώστε εάν μια πορεία δεν είναι διαθέσιμη, άλλη είναι εύκολα διαθέσιμη. Καθιερώνει τις διαδρομές γρήγορα έτσι ώστε μπορούν να χρησιμοποιηθούν πριν από τις αλλαγές τοπολογίας. Ελαχιστοποιεί τις αλγοριθμικά αντιδράσεις/τα γενικά έξοδα επικοινωνίας και συντηρεί έτσι το διαθέσιμο εύρος ζώνης και αυξάνει την προσαρμοστικότητα. Είναι επίσης ικανό να ανιχνεύσει τα χωρίσματα δικτύων πολύ γρήγορα.

Μειονεκτήματα : Όσο μεγαλώνει το δίκτυο παρουσιάζεται συμπεριφορά αστάθειας, με το πρόβλημα αρίθμησης (0) - ΑΠΕΙΡΟΥ στα διανυσματικά πρωτόκολλα δρομολόγησης απόστασης.

RDMAR - Αυτός ο τύπος δρομολόγησης υπολογίζει την απόσταση στους ράδιο βρόχους, μεταξύ δύο κόμβων χρησιμοποιώντας το σχετικό αλγόριθμο εκτίμησης απόστασης και χρησιμοποιεί τους αριθμούς ακολουθίας για να διατηρήσει την ελευθερία βρόχων κατά τη διάρκεια της διαδικασίας ανακαλύψεων διαδρομών. Μια βασική έννοια πίσω από το RDMAR είναι η προσέγγισή της συντήρηση των ενεργών πορειών (διαδικασία συντήρησης διαδρομών). Ο αλγόριθμος συντήρησης διαδρομών σε RDMAR είναι μια διανεμημένη λειτουργία που εκμεταλλεύεται τη χωρική σχέση των κόμβων όταν εμφανίζεται μια αποτυχία κατά μήκος μιας ενεργού διαδρομής και ανάλογα με τη σχετική απόσταση του κόμβου, που εκφέρει την αποτυχία από την κλήση σε άλλους κόμβους, υπάρχουν δύο περιπτώσεις:

α) Ελέγχεται η πιο κοντινή διαδρομή από το σημείο που παρατηρήθηκε το πρόβλημα. Κατόπιν RDM πρόκειται να εφαρμοστεί για να εντοπίσει τον κόμβο που προκάλεσε την αποτυχημένη διαδρομή στο δίκτυο.

β) Ο κόμβος προχωρά και ενημερώνει τον καλώντα(προηγούμενο) κόμβο για την αποτυχία να παραδοθεί η κλήση μέσω αυτής της πορείας.

ABR - Σε ABR, μια διαδρομή επιλέγεται βασισμένη στις καταστάσεις associativity των κόμβων. Οι διαδρομές που επιλέγονται έτσι ώστε να είναι μακρόβιες. Όλοι οι κόμβοι παράγουν τα περιοδικά αναγνωριστικά σήματα για να δηλώσουν την ύπαρξή τους. Όταν ένας κόμβος γειτόνων λαμβάνει ένα αναγνωριστικό σήμα, ενημερώνει τους πίνακές συνδεσιμότητας(associativity) του. Για κάθε αναγνωριστικό σήμα που λαμβάνει κάθε κόμβος καταγράφει στους πίνακες αυτούς πληροφορίες για τον κόμβο από τον οποίο έλαβε το αναγνωριστικό σήμα. Μια υψηλή αξία του κρότωνα associativity όσον αφορά έναν κόμβο δείχνει μια χαμηλή κατάσταση της κινητικότητας κόμβων, ενώ μια χαμηλή αξία του κρότωνα associativity μπορεί να δείξει μια υψηλή κατάσταση της κινητικότητας κόμβων. Οι Associativity επαναρυθμίζονται όταν κινούνται οι γείτονες ενός κόμβου ή ο

ίδιος κόμβος στον οποίο ανήκει. Ο θεμελιώδης στόχος ABR είναι να βρεθούν οι μακρινές υπάρχουσες διαδρομές για τα Ad Hoc κινητά δίκτυα.

Το πρωτόκολλο ABR αποτελείται από τρεις φάσεις. Φάση ανακαλύψεων διαδρομών, φάση αναδημιουργίας διαδρομών και φάση διαγραφής διαδρομών.

1. Φάση ανακαλύψεων διαδρομών

Η φάση ανακαλύψεων διαδρομών είναι μια ερώτηση ραδιοφωνικής μετάδοσης και περιμένει τον κύκλο απάντησης (BQ-APANTISI). Αρχικά, όλοι οι κόμβοι δεν έχουν καμία διαδρομή ως προορισμό. Ένας κόμβος που επιθυμεί μια διαδρομή, ο κόμβος SRC (πηγής), θα μεταδώσει ραδιοφωνικά ένα μήνυμα BQ σε αναζήτηση των κόμβων που έχουν μια διαδρομή ως προορισμό. Όλοι οι ενδιαμέσοι κόμβοι που λαμβάνουν αυτό το BQ θα ελέγξουν εάν έχουν επεξεργαστεί προηγουμένως το πακέτο BQ. Ένας κόμβος δεν διαβιβάζει ένα αίτημα BQ περισσότερο από μία φορά. Εάν το έχει επεξεργαστεί, το πακέτο BQ θα απορριφθεί. Εάν δεν είναι αυτός ο προορισμός (DEST), το μεταδίδει ραδιοφωνικά στους γείτονές. Στη λήψη ενός μηνύματος BQ, ένας ενδιάμεσος κόμβος επισυνάπτει τη διεύθυνσή του και τις πληροφορίες δρομολόγησης (associativity) που γνωρίζει στο πακέτο ερώτησης. Ο επόμενος κόμβος σβήνει τις καταχωρήσεις associativity των προηγούμενων γειτονικών κόμβων του. Κάθε πακέτο που φθάνει στον προορισμό περιέχει associativity των κόμβων κατά μήκος της διαδρομής από την πηγή στον προορισμό. Ο προορισμός μπορεί τώρα να επιλέξει την καλύτερη διαδρομή αφού εξετάσει το associativity του μηνύματος BQ. Εάν οι πολλαπλάσιες πορείες έχουν τον ίδιο γενικό βαθμό σταθερότητας ένωσης, η διαδρομή με τον ελάχιστο αριθμό σταθμών επιλέγεται. Μόλις επιλεγεί μια πορεία, ο προορισμός στέλνει ένα πακέτο ΑΠΑΝΤΗΣΗΣ πίσω στην πηγή κατά μήκος αυτής της πορείας. Οι κόμβοι στην πορεία του πακέτου ΑΠΑΝΤΗΣΗΣ ακολουθούν τη διαδρομή που έχει επιλεγεί. Όλες οι άλλες διαδρομές παραμένουν ανενεργές, αποφεύγοντας κατά συνέπεια την πιθανότητα των διπλών πακέτων φθάνοντας στον προορισμό.

Το πακέτο BQ είναι μεταβλητό στο καθώς μεταδίδεται από κόμβο σε κόμβο.

2. Φάση αναδημιουργίας διαδρομών (RRC)

Η επόμενη φάση σε ABR είναι η κατόπιν παραγγελίας φάση αποκατάστασης διαδρομών. Αυτή η φάση είναι πρακτική επειδή οι διαδρομές μπορούν να αλλάξουν και η τοπολογία δικτύων μπορεί να αλλάξει επίσης. Η επιλογή μιας μακρόβιας διαδρομής δεν είναι αρκετή. Οι αλλαγές διαδρομών εμφανίζονται όταν απομακρύνονται η πηγή, ο προορισμός ή ο ενδιάμεσος κόμβος, ή εάν υπάρχουν οι ταυτόχρονες μετακινήσεις κόμβων, όταν έχουμε μερική ανακάλυψη διαδρομών, εξάλειψη διαδρομών λόγω μετακινήσεων, αναπροσαρμογές διαδρομών, ή και τη νέα ανακάλυψη διαδρομών κατά μήκος της κίνησης διαδρομών που ακολουθούν οι κόμβοι.

Τα κύρια χαρακτηριστικά γνωρίσματα μιας φάσης αποκατάστασης διαδρομών είναι:

Μερική ανακάλυψη διαδρομών με τη χρήση του πακέτου ελέγχου ερώτησης (LQ)

Εξάλειψη άκυρων διαδρομών

Έγκυρη αναπροσαρμογή διαδρομών

Νέα ανακάλυψη διαδρομών (χειρότερη περίπτωση)

Η μετακίνηση κόμβων πηγής οδηγεί σε μια νέα διαδικασία ανακάλυψης διαδρομών BQ-APANTISIS. Το μήνυμα ανακοίνωσης (RN) διαδρομών χρησιμοποιείται για να σβήσει τις καταχωρήσεις διαδρομών που συνδέονται με τους προς τα κάτω κόμβους. Όταν ο προορισμός κινείται, ο άμεσος προς τα πάνω κόμβος του προορισμού σβήνει τη διαδρομή του. Μια διαδικασία εντόπισης (LQ [χ]), όπου το χ αναφέρεται στην αρίθμηση σταθμού από τον προς τα πάνω κόμβο στον προορισμό, ξεκινά για να καθορίσει εάν ο κόμβος είναι ακόμα εφικτός. Εάν ο προορισμός λαμβάνει το πακέτο LQ, επιλέγει την καλύτερη διαδρομή και το μήνυμα θα σταλεί στον προορισμό. Όταν μια διαδρομή δεν εντοπίζει τον προορισμό, τότε ένα μήνυμα RN στέλνεται στον επόμενο προς τα πάνω κόμβο για να σβήσει την άκυρη διαδρομή και να ενημερώσει αυτόν τον κόμβο ότι πρέπει να επικαλεσθεί τη διαδικασία LQ [χ]. Εάν αυτή η διαδικασία οδηγεί να οπισθοδρομήσει περισσότερο από στα μισά του δρόμου στην πηγή, η διαδικασία LQ διακόπτεται και η πηγή κινεί μια νέα διαδικασία BQ.

3. Φάση διαγραφής διαδρομών

Η τρίτη φάση σε ABR είναι η κατόπιν παραγγελίας φάση διαγραφής διαδρομών. Η ανάγκη για τη διαγραφή διαδρομών έρχεται καθώς διατήρηση των αχρησιμοποίητων διαδρομών λαμβάνει γενικά πολλά έξοδα. Όταν μια ανακαλυμμένη διαδρομή δεν απαιτείται πλέον, ο κόμβος πηγής αρχίζει ραδιοφωνική μετάδοση (RD) μια διαδρομή για διαγραφή της. Όλοι οι κόμβοι κατά μήκος της διαδρομής διαγράφουν τις πληροφορίες διαδρομών από τους πίνακες δρομολόγησής τους. Το μήνυμα RD διαδίδεται από μια πλήρη ραδιοφωνική μετάδοση, σε αντιδιαστολή με μια κατευθυνόμενη ραδιοφωνική μετάδοση, επειδή ο κόμβος πηγής μπορεί να μην γνωρίζει οποιεσδήποτε αλλαγές κόμβων διαδρομών που εμφανίστηκαν κατά τη διάρκεια RRCs [

Υπάρχουν δύο προσεγγίσεις στη διαγραφή διαδρομών, το μαλακό κράτος και το σκληρό κράτος.

Για τη μαλακή κρατική προσέγγιση, η λήξη είναι βασισμένη στην παρατήρηση κυκλοφορίας ή το προκαθορισμένο διάλειμμα. Ελέγχει τη δραστηριότητα κυκλοφορίας και εάν καμία κυκλοφορία σχετική με μια ενεργό διαδρομή δεν παρατηρείται πέρα από ένα επίπεδο κατώτατων ορίων, η διαδρομή διακόπτεται αυτόματα. Για τη σκληρή κρατική προσέγγιση, η λήξη είναι βασισμένη σε μια συγκεκριμένη διαδρομή διαγράφει τη ραδιοφωνική μετάδοση.

Όταν μια ανακαλυμμένη διαδρομή δεν επιδιώκεται πλέον ή χρησιμοποιείται, μια διαδρομή διαγράφει τη ραδιοφωνική μετάδοση (RD) θα άρχιζε από το SRC έτσι ώστε όλο INs θα ενημερώσει τα επιτραπέζια λήμματα δρομολόγησής τους.

2.3.3 ΥΒΡΙΔΙΚΟ

Το πρωτόκολλο δρομολόγησης ζώνης (ZRP) - Το ZRP ανήκει στην κατηγορία των υβριδικών πρωτοκόλλων ενσωματώνοντας τις δυνατότητες και τα πλεονεκτήματα τόσο των reactive όσο και των proactive πρωτοκόλλων.

Ενσωματώνει τις δυνατότητες των κατόπιν παραγγελίας και δυναμικών πρωτοκόλλων δρομολόγησης. Το ZRP είναι παρόμοιο με μια συστάδα CSGR με εξαίρεση ότι κάθε κόμβος ενεργεί ως επικεφαλής μιας ομάδας και μέλος άλλων ομάδων. Οι ζώνες μπορεί να αλληλεπικαλύπτονται. Στο ZRP, μία ζώνη δρομολόγησης αποτελείται από μερικούς κινητούς κόμβους μέσα στα πλαίσια ενός, δύο, ή περισσότερων αλμάτων μακριά από τον κεντρικό κόμβο. Το μέγεθος μιας επιλεγμένης ζώνης μπορεί, επομένως, να επηρεάσει την απόδοση της επικοινωνίας ad hoc.

Μέσα στα όρια της ζώνης, χρησιμοποιείται ένα πρωτόκολλο δρομολόγησης που βασίζεται και εκκινεί από την διατήρηση πινάκων (table-driven). Αυτό σημαίνει ότι οι ενημερώσεις για τους δρόμους διενεργούνται για τους κόμβους μέσα στα όρια κάθε ζώνης. Κάθε κινητό τερματικό, επομένως, έχει μία διαδρομή για οποιοδήποτε άλλο κόμβο μέσα στην ζώνη που ανήκει. Αν ο κόμβος του προορισμού βρίσκεται έξω από την ζώνη της πηγής, χρησιμοποιείται μία μέθοδος εύρεσης δρόμου που βασίζεται σε διαδικασίες κατ' απαίτηση (on-demand).

Το ZRP έχει τρία υπό-πρωτόκολλα: (α) το proactive Intrazone Routing Protocol (IARP), (β) το reactive Interzone Routing Protocol (IERP), και (γ) το Bordercast Resolution Protocol (BRP). Το IARP μπορεί να εφαρμοστεί χρησιμοποιώντας μεθόδους δρομολόγησης που βασίζονται στις καταστάσεις των ζεύξεων και στα διανύσματα απόστασης. Η παραγόμενη πληροφορία δρομολόγησης διαδίδεται μέχρι το σύνορο της ζώνης δρομολόγησης και όχι σε όλο το δίκτυο.

Το IARP στηρίζεται σε ένα υποκείμενο πρωτόκολλο ανεύρεσης γειτόνων για την ανίχνευση της παρουσίας και απουσίας γειτονικών κόμβων, κι επομένως, την αξιολόγηση της συνδεσιμότητας των ζεύξεων αυτών των κόμβων. Ο βασικός του ρόλος είναι η διασφάλιση ότι κάθε κόμβος μέσα στην ζώνη έχει ένα συνεκτικό πίνακα δρομολόγησης που είναι πλήρως, εγκαίρως και επαρκώς ενημερωμένος, ενώ ταυτόχρονα απεικονίζει την πληροφορία για το πώς κάποιο κινητό μπορεί να φθάσει οποιοδήποτε άλλο κόμβο μέσα στην ζώνη.

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

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

Η διεργασία της εύρεσης δρόμου του ZRP είναι, επομένως, μία εξέταση στον πίνακα δρομολόγησης και /ή μία έρευνα εύρεσης δρόμου μέσα στα πλαίσια της ζώνης. Όταν ένας δρόμος δεν είναι πλέον έγκυρος εξαιτίας της κινητικότητας των κόμβων, εάν η πηγή της κινητικότητας βρίσκεται μέσα στην ζώνη, θα αντιμετωπιστεί όπως και ένα γεγονός αλλαγής της κατάστασης μιας ζεύξης και θα προκληθεί η παραγωγή και διάδοση ενημερώσεων όπως και στην proactive μέθοδο, ενημερώνοντας όλους τους κόμβους μέσα στην ζώνη. Αν η πηγή της κινητικότητας είναι αποτέλεσμα ενός συνοριακού κόμβου ή άλλων κινητών τερματικών στη ζώνη, τότε η αποκατάσταση της διαδρομής εκτελείται με την μορφή της έρευνας για ένα δρόμο, ή στην χειρότερη περίπτωση, ο κόμβος της πηγής ενημερώνεται για την αποτυχία του δρόμου.

Πλεονεκτήματα : Παρέχει καλύτερη απόδοση.

Μειονεκτήματα : Δεδομένου ότι κάθε κόμβος έχει τις τοπολογικές πληροφορίες πιο υψηλού επιπέδου, η απαίτηση μνήμης είναι μεγαλύτερη.

Το μέγεθος μιας επιλεγμένης ζώνης μπορεί, επομένως, να επηρεάσει την απόδοση της επικοινωνίας ad hoc.

CPR - Ειδικό πρωτόκολλο δρομολόγησης **κρίσιμων πορειών CPR**. Το πρωτόκολλο αυτό προσπαθεί να ενσωματώσει τις αξίες και των αντιδραστικών και δυναμικών ειδικών αλγορίθμων δρομολόγησης, όπως και το ZRP υβριδικό πρωτόκολλο. Το CPR κληρονομεί κάποια στοιχεία από το DSR πρωτόκολλο δρομολόγησης. Η κυκλοφορία δικτύων ελέγχεται στην προσπάθεια να ανακαλυφθούν βαθμιαία τα ζευγάρια των ιδιαίτερα διαλογικών κόμβων που συμμετέχουν και να στέλνουν τα στοιχεία ο ένας στον άλλο συχνότερα από άλλους κόμβους στο δίκτυο. CPR κατασκευάζει έπειτα τις κρίσιμες πορείες (CPs) μεταξύ αυτών των ζευγαριών των κόμβων. Ο στόχος είναι να επιτευχθεί η χαμηλή λανθάνουσα κατάσταση μεταξύ των ιδιαίτερα ενεργών ζευγαριών των κόμβων, αυξάνοντας κατά συνέπεια τη γενική απόδοση του δικτύου.

Πίνακας 2: ΣΥΓΚΡΙΣΗ ΤΩΝ ΣΗΜΑΝΤΙΚΟΤΕΡΩΝ ΠΡΩΤΟΚΟΛΛΩΝ ΔΡΟΜΟΛΟΓΗΣΗΣ

Protocol Property	DSDV	AODV	DSR	ZRP	TORA
Loop free	Yes	Yes	Yes	Yes	Yes
Multiple routes	No	No	Yes	No	Yes
Distributed	Yes	Yes	Yes	Yes	Yes
Reactive	No	Yes	Yes	Variable	Yes
Unidirectional link support	No	No	Yes	No	Yes
QoS support	No	No	No	No	No
Multicast	No	Yes	No	No	No
Security	No	No	No	No	Possible
Power efficiency	No	No	No	No	No
Periodic broadcasts	Yes	Yes	No	Yes	Yes

Συμπεράσματα και μελλοντική έρευνα

Σε αυτό το κεφάλαιο, συζητήσαμε τα σημαντικότερα πρωτόκολλα δρομολόγησης ειδικών δικτύων. Πρωτόκολλα δρομολόγησης όπως DSDV, WRP, DSR, AODV, TORA (κλπ) παρουσιάστηκαν με μια συνοπτική περιγραφή κάθε ένα. Σημαντικές πρόοδοι πραγματοποιούνται συνεχώς για να αυξήσουν τις ικανότητες και τη χρήση των ασύρματων συσκευών.

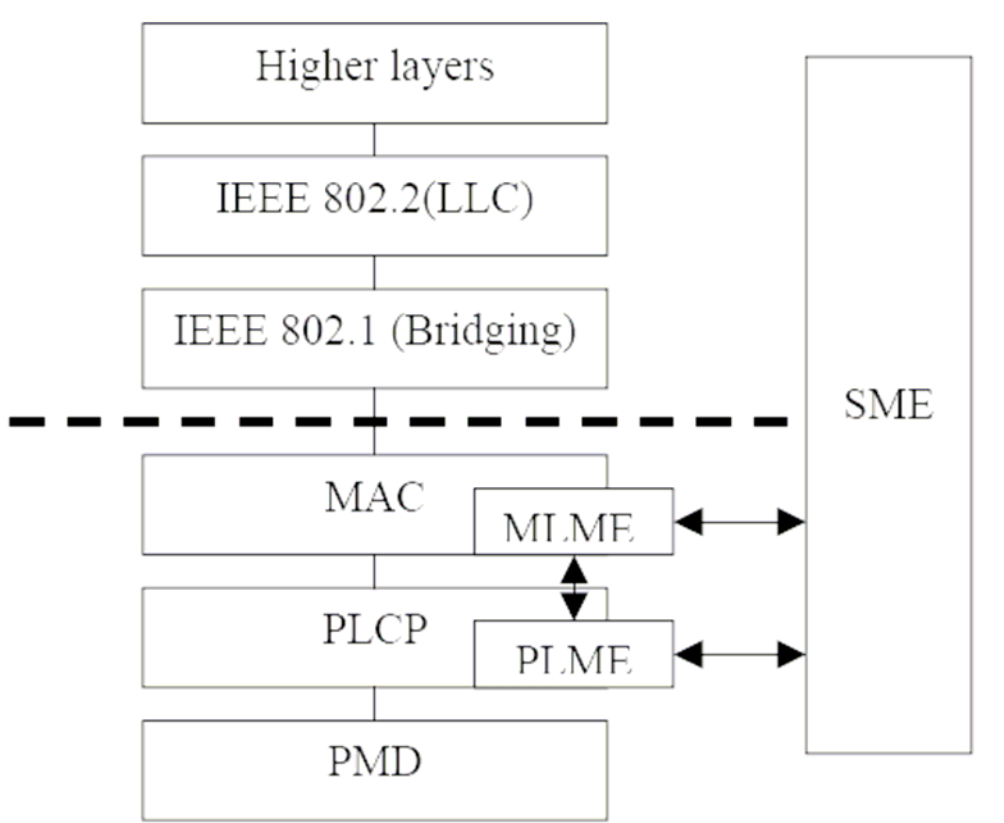
ΚΕΦΑΛΑΙΟ 3

AD HOC ΠΡΟΔΙΑΓΡΑΦΕΣ

Στο κεφάλαιο αυτό θα διαπραγματευτούμε τρεις από τις βασικότερες προδιαγραφές για τα ασύρματα δίκτυα που έχουν την δυνατότητα, από κατασκευής των προτύπων, να υποστηρίξουν ad hoc επικοινωνία ή μπορούν να την προσφέρουν μέσα από τροποποιήσεις και αλλαγές που μπορούν να γίνουν εύκολα και άμεσα: α) IEEE 802.11, β) HIPERLAN/2 και γ) Bluetooth.

3.1. IEEE 802.11

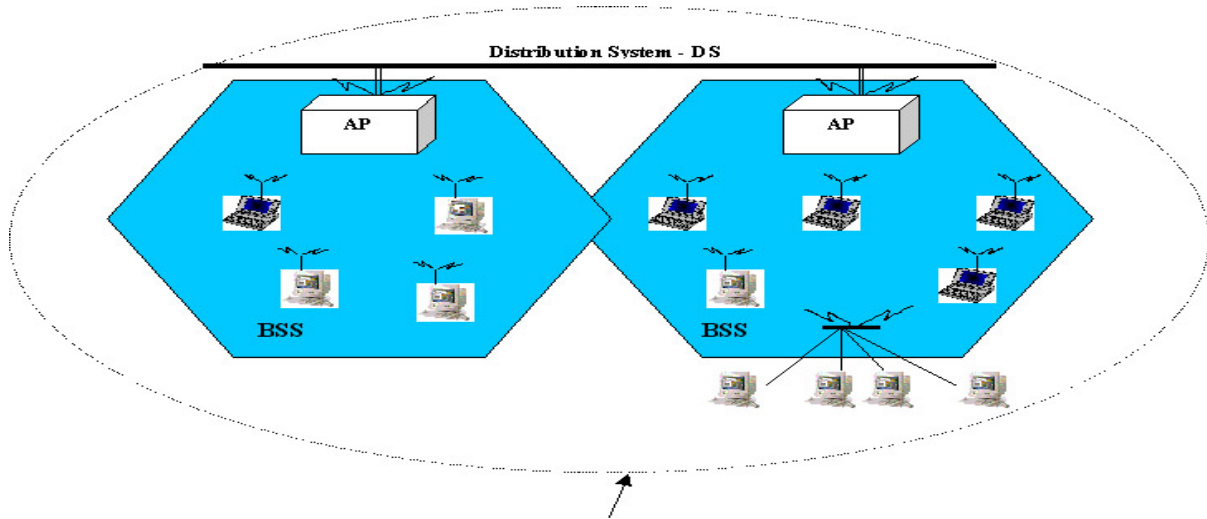
Η προδιαγραφή IEEE 802.11 για τα ασύρματα τοπικά δίκτυα εκδόθηκε το 1997 και ενσωματώθηκε στο πλαίσιο εργασίας του IEEE 802.



Εικόνα 1: Μοντέλο αναφοράς IEEE 802.11

Στο πρότυπο αυτό προδιαγράφεται η λειτουργικότητα του MAC και του φυσικού επιπέδου ενός τοπικού ασύρματου δικτύου και παρουσιάζεται μία ιδέα ενσωμάτωσης και σύνδεσης αυτού του τύπου του δικτύου στην φόρμα του IEEE 802. Με δύο προσθήκες

για υψηλούς ρυθμούς δεδομένων, το 1999 οι προδιαγραφές πέτυχαν να παρέχουν ρυθμούς δεδομένων από 1 Mbit/s μέχρι και 54 Mbit/s στην ζώνη των 2,4 GHz ISM και στην ζώνη των 5 GHz U-NII. Το σχήμα πρόσβασης στο μέσο βασίζεται στο CSMA/CA και υποστηρίζει κεντροποιημένο έλεγχο στα δίκτυα με σταθερή δομή.



Εικόνα 2: Η αρχιτεκτονική δικτύου κατά το πρότυπο 802.11 της IEEE.

3.1.1. Βασικές Ιδέες

Η προδιαγραφή IEEE 802.11, αρχικά, εισάγει μια εννοιολογική προσέγγιση σε ένα ασύρματο δίκτυο. Μία βασική διάκριση γίνεται μεταξύ των δικτύων με, και αυτών χωρίς σταθερή δομή. Η ιδέα περιλαμβάνει όλα τα επίπεδα πρόσβασης του δικτύου αλλά επικεντρώνεται στο MAC και το φυσικό επίπεδο.

Τα ασύρματα δίκτυα με σταθερή δομή αποτελούνται από τις ομάδες βασικής υπηρεσίας (Basic Service Set – BSS), η κάθε μία από τις οποίες αναγνωρίζεται από το σημείο πρόσβασής της, επιπλέον ένα σύστημα κατανομής (Distribution System – DS), και τις λεγόμενες πύλες σε άλλα δίκτυα IEEE 802. Το BSS είναι μία ομάδα από σταθμούς με κοινή περιοχή εμβέλειας-επικοινωνίας που συσχετίζονται με ένα σημείο πρόσβασης. Μπορεί, επίσης, να θεωρηθεί ως ένα υποδίκτυο.

Το σημείο πρόσβασης, εκτός της λειτουργίας ως ένας κανονικός σταθμός, έχει μία διακριτή θέση μέσα στο υποδίκτυο: Παρέχει πρόσβαση στο σύστημα κατανομής. Επίσης, μπορεί να ενεργήσει σαν συντονιστής σημείου (θα δούμε παρακάτω) για να προσφέρει υπηρεσίες ελεύθερες συγκρούσεων στους συσχετισμένους σταθμούς.

Το DS είναι υπεύθυνο για την σύνδεση διαφορετικών BSS και άλλων δικτύων για να δημιουργήσουν μία εκτεταμένη ομάδα υπηρεσίας (Extended Service Set – ESS). Το DS είναι μία λογική ενότητα στο πλαίσιο εργασίας του συγκεκριμένου προτύπου και δεν προδιαγράφεται καμία εφαρμογή ή τύπος εφαρμογής του. Οι υπηρεσίες του DS αναφέρονται ως υπηρεσίες συστήματος κατανομής (DS Services – DSS) και περιλαμβάνουν έλεγχο συσχέτισης, κατανομή των πλαισίων πάνω από λογικά σύνορα

και ενσωμάτωση του WLAN IEEE 802.11 σε άλλα LAN IEEE 802. Σε αντίθεση με τα DSS υπάρχουν οι υπηρεσίες σταθμών (Station Services – SS) που συμβάλλουν στην πιστοποίηση, την μυστικότητα της επικοινωνίας και την παράδοση των δεδομένων.

Αν ένα υποδίκτυο, όπου όλοι οι κόμβοι βρίσκονται σε αμοιβαία περιοχή επικοινωνίας, δεν συνδέεται με ένα σημείο πρόσβασης (κι επομένως δεν έχει πρόσβαση στο DS), τότε αυτό λέγεται ανεξάρτητη ομάδα βασικής υπηρεσίας (Independent Basic Service Set – IBSS). Αυτά τα δίκτυα αναφέρονται ως ad hoc δίκτυα ή δίκτυα χωρίς σταθερή δομή. Οι ιδιαιτερότητες ενός IBSS περιγράφονται με μεγαλύτερη λεπτομέρεια παρακάτω. Το ESS αποτελείται από DS και BSS με αυθαίρετο τρόπο, πολυπλοκότητα και συνδυασμό. Ένα ESS φαίνεται να είναι ένα IBSS από την πλευρά του υπό-επίπεδου ελέγχου της λογικής ζεύξης.

3.1.2. Επίπεδα, Υπηρεσίες και Ενότητες

Το φυσικό επίπεδο του IEEE 802.11 αποτελείται από δύο υποεπίπεδα, το φυσικό υποεπίπεδο εξαρτώμενο από το μέσο (Physical Medium Dependant – PMD), και το υπό-επίπεδο σύγκλισης φυσικού επιπέδου (Physical Layer Convergence Protocol – PLCP). Το PMD προδιαγράφει τον τρόπο αποστολής και λήψης των δεδομένων στο ασύρματο επίπεδο και το PLCP απεικονίζει τα πλαίσια MAC για τις λειτουργίες του PMD.

Υπάρχουν πέντε φυσικά επίπεδα που προδιαγράφονται στο πρότυπο IEEE 802.11:

- IR βασικής ζώνης
- Διασκορπισμένο φάσμα με άλματα συχνότητας (Frequency Hopping Spread Spectrum – FHSS) στην μπάντα των 2,4 GHz ISM.
- Διασκορπισμένο φάσμα απευθείας σειράς (Direct Sequence Spread Spectrum – DSSS) στην μπάντα των 2,4 GHz ISM.
- Διασκορπισμένο φάσμα απευθείας σειράς υψηλού ρυθμού (High Rate Direct Sequence Spread Spectrum – HR/DSSS) στην περιοχή των 2,4 GHz.
- Φυσικό επίπεδο υψηλής ταχύτητας βασισμένο στην ορθογώνια πολυπλεξία διαίρεσης συχνότητας (Orthogonal Frequency Division Multiplexing) στην περιοχή των 5 GHz.

Τα πρώτα δύο φυσικά επίπεδα υποστηρίζουν ρυθμούς δεδομένων μέχρι 2 Mbps, το HR/DSSS υποστηρίζει μέχρι και 11 Mbps και το OFDM μέχρι και 54 Mbps. Κάθε προδιαγραφή καθορίζει τόσο το PMD όσο και το PLCP ανάλογα με το αντίστοιχο φυσικό σύστημα.

Το υποεπίπεδο πρόσβασης στο μέσο παρέχει ασύγχρονη παράδοση δεδομένων, ασφαλείς υπηρεσίες, κρυπτογράφηση και πιστοποίηση μεταξύ σταθμών, και διάταξη των πακέτων. Επιπλέον περιγράφονται στις ενότητες του MAC επιπέδου μέθοδοι ελέγχου ζεύξης και διαχείρισης, τμηματοποίησης και επανένωσης πακέτων. Το βασικό σχήμα πρόσβασης στο μέσο, το CSMA/CA, είναι ενσωματωμένο ως κατανομημένη λειτουργία συντονισμού (Distributed Coordination Function – DCF) στο επίπεδο MAC. Για να αποφευχθούν οι συγκρούσεις, μπορεί να χρησιμοποιηθεί ένα σχήμα RTS/CTS πριν από την εκκίνηση οποιασδήποτε μετάδοσης. Πάνω από το DCF υπάρχει η λειτουργία συντονισμού σημείου (Point Coordination Function – PCF) που παρέχει πρόσβαση στο

μέσο χωρίς συγκρούσεις στην διαμόρφωση δικτύων με σταθερή δομή. Το DCF και το PCF εξετάζονται παρακάτω.

Η διευθυνσιοδότηση σε ένα δίκτυο IEEE 802.11 ακολουθεί τους κανόνες του προτύπου, για παράδειγμα κάθε συσκευή έχει μία μοναδική διεύθυνση σταθμού με 48 bit. Επιπλέον, κάθε υποδίκτυο έχει ένα μοναδικό, δικό του, αναγνωριστικό που είναι η διεύθυνση MAC του σημείου πρόσβασης στα δίκτυα με σταθερή δομή ή μία τυχαία διεύθυνση IEEE 802, που διαχειρίζεται τοπικά, για τις περιπτώσεις έλλειψης σταθερής δομής.

Υπάρχουν διαφορετικοί τύποι μηνυμάτων σε επίπεδο MAC, που είναι δεδομένα, πακέτα διαχείρισης και μηνύματα ελέγχου. Τα πλαίσια δεδομένων περιέχουν δεδομένα του χρήστη, τα πλαίσια διαχείρισης περιλαμβάνουν δεδομένα οντοτήτων διαχείρισης επιπέδου MAC (MAC Layer Management Entity – MLME), και τα πλαίσια ελέγχου (όπως τα RTS/CTS πλαίσια) έχουν την έννοια της υποστήριξης του ελέγχου παράδοσης των δεδομένων και των πακέτων διαχείρισης.

Πριν μιλήσουμε για το DCF και το PCF με λεπτομέρεια, θα ήταν ωφέλιμο να εισάγουμε την έννοια του χώρου διαπλαισίωσης του IEEE 802.11. Μπορεί να θεωρηθεί ως μία ομάδα από χρονιστές, που ξεκινούν αφού ελευθερωθεί το μέσο. Κάθε χρονιστής εκπνέει μετά από ένα συγκεκριμένο χρονικό διάστημα. Ανάλογα με το ποιοι χρονιστές έχουν ήδη εκπνεύσει, τα πακέτα μπορούν να σταλούν ή όχι, σύμφωνα με την προτεραιότητά τους. Μετά το διάστημα διαπλαισίωσης του DCF (DCF Interframe Space – DIFS) – που χρησιμοποιείται από το DCF για να παρέχει πρόσβαση στις συγκρούσεις, ή το εκτεταμένο διάστημα διαπλαισίωσης (Extended Interframe Space – EIFS) – που χρησιμοποιείται αν ένας σταθμός λάβει ένα εσφαλμένο πακέτο, ένας σταθμός μπορεί να συναγωνιστεί για την πρόσβαση στο μέσο. Η ιδέα του διαστήματος διαπλαισίωσης (Interframe Space - IFS) έχει εισαχθεί για να παρέχει πρόσβαση στο μέσο βάσει προτεραιοτήτων. Το IFS και οι κανόνες πρόσβασης εφαρμόζονται σε κάθε σταθμό. Οι πραγματικοί χρόνοι επιλέγονται σύμφωνα με τις ιδιαιτερότητες του φυσικού επιπέδου, που καθορίζονται στην αντίστοιχη βάση πληροφορίας διαχείρισης (Management Information Base – MIB), που αποθηκεύεται σε κάθε σταθμό.

Το DCF ορίζει τις βασικές λειτουργίες πρόσβασης στο μέσο του CSMA/CA, και τις υπηρεσίες σύγκρουσης. Αυτές είναι χρονισμοί πρόσβασης του μέσου για διαφορετικούς τύπους πακέτων, διαδικασίες μεταφοράς πλαισίων, διαδικασίες επιβεβαιώσεων, και μέθοδοι RTS/CTS. Επιπρόσθετα, παρέχεται ένας εικονικός μηχανισμός αίσθησης του μέσου που βασίζεται στην πληροφορία που σχετίζεται με την διάρκεια κατά την οποία είναι απασχολημένο το μέσο. Αυτή η πληροφορία παρέχεται στο πεδίο της τιμής της διάρκειας στην επικεφαλίδα του πλαισίου MAC. Αυτός ο μηχανισμός ονομάζεται διάνυσμα παραχώρησης δικτύου (Network Allocation Vector – NAV).

Το DCF διασφαλίζει ότι υπάρχει ένα χρονικό παράθυρο μεταξύ των πλαισίων, που χρησιμοποιείται για πρόσβαση σύμφωνα με προτεραιότητες. Αν, για παράδειγμα, ένας σταθμός θέλει να μεταδώσει, και το χρονόμετρο καθυστέρησης είναι μηδενισμένο, τότε, αν το μέσο έχει ελευθερωθεί για χρονικό διάστημα τουλάχιστον ίσο με DIFS, μεταδίδει αμέσως. Σε αντίθεση με αυτό, από την στιγμή που μία επιβεβαίωση είναι πιο σπουδαία από μία μετάδοση, τα πακέτα ACK μεταδίδονται μετά από ένα βραχύ διάστημα διαπλαισίωσης (Short Interframe Space – SIFS) – που χρησιμοποιείται για υψηλής προτεραιότητας πρόσβαση, και είναι το συντομότερο από τα διαστήματα

διαπλαισίωσης. Άρα, καθώς τα πακέτα ACK συναγωνίζονται για το μέσο νωρίτερα από τις συνηθισμένες μεταδόσεις, ο σταθμός θα πετύχει και θα εκπέμψει πρώτος.

Το DCF είναι η βάση για όλους τους σταθμούς, αναφορικά με την πρόσβαση στο μέσο, και χρησιμοποιείται και στα δίκτυα που έχουν, αλλά και σε αυτά που δεν έχουν, σταθερή δομή.

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

Όλα τα προδιαγεγραμμένα επίπεδα του IEEE 802.11 περιλαμβάνουν την δικιά τους οντότητα διαχείρισης. Αυτές οι οντότητες περιέχουν τα ονομαζόμενα MIB. Τα MIB περιλαμβάνουν την πληροφορία που είναι χαρακτηριστική για το αντίστοιχο επίπεδο σε μια συγκεκριμένη κατάσταση. Η αλλαγή των τιμών μπορεί να συντελέσει στην λήψη των απαραίτητων ενεργειών από την ενότητα διαχείρισης.

Οι τρεις ενότητες διαχείρισης (PLME, MLME, SME) αλληλεπιδρούν αμοιβαία χρησιμοποιώντας τις υπηρεσίες τους μέσω καθορισμένων σημείων πρόσβασης υπηρεσίας.

Εκτός από αυτό, η ενσωμάτωση του PLME και του MLME στα αντίστοιχα επίπεδα δεν έχει προδιαγραφθεί, όπως και οι υπηρεσίες και οι λειτουργίες του SME.

Το PLME παρέχει υπηρεσίες για τον καθορισμό του φυσικού καναλιού μετάδοσης, όπως και το σχήμα αλμάτων στο σύστημα FHSS. Αυτό γίνεται με τον χειρισμό του MIB του φυσικού επιπέδου με τα αντίστοιχα μηνύματα.

Το MLME είναι υπεύθυνο για την εγκατάσταση και την διατήρηση, καθώς και για τη διαχείριση της ισχύος. Παρέχει τις παρακάτω υπηρεσίες:

- Διαχείριση ισχύος
- Ανίχνευση
- Συγχρονισμός
- Πιστοποίηση
- Από-πιστοποίηση
- Συσχέτιση
- Από-συσχέτιση
- Επανασυσχέτιση
- Επαναρύθμιση
- Εκκίνηση

Η μέθοδος ανίχνευσης των σταθμών για την εύρεση άλλων κινητών στην περιοχή εμβέλειας, προδιαγράφεται από το πρότυπο. Υπάρχει η παθητική και η ενεργητική ανίχνευση. Για τον συγχρονισμό όλων των χρονιστών στους σταθμούς σε ένα BSS ή IBSS, το MLME παρέχει την υπηρεσία συγχρονισμού. Η πληροφορία συγχρονισμού προσφέρεται είτε κεντριοποιημένα από το σημείο πρόσβασης σε ένα BSS ή μέσω ενός

κατανεμημένου αλγορίθμου σε ένα IBSS. Στην κεντρικοποιημένη διαμόρφωση, το σημείο πρόσβασης στέλνει ένα beacon πλαίσιο που περιλαμβάνει τις ιδιότητες του BSS και την πληροφορία του συγχρονισμού σε τακτά διαστήματα. Ένας σταθμός πρέπει πρώτα να πιστοποιήσει τον εαυτό του πριν τον πιθανό συσχετισμό με ένα BSS. Οι συσχετισμένοι σταθμοί μπορεί να χρησιμοποιούν το DS (επικοινωνία με άλλους σταθμούς σε άλλα υποδίκτυα, αίτηση για υπηρεσίες PC), ενώ το ίδιο δεν συμβαίνει για ένα μη συσχετισμένο σταθμό. Η υπηρεσία επαναρύθμισης ρυθμίζει εκ νέου την οντότητα του MAC, και η υπηρεσία εκκίνησης χρησιμοποιείται είτε για να ξεκινήσει ένα BSS ή ένα IBSS, αν ο σταθμός δεν προσπάθησε, ήδη, να συγχρονιστεί με ένα BSS.

Οι υπηρεσίες της οντότητας διαχείρισης σταθμού (Station Management Entity – SME) δεν προδιαγράφονται σε αυτό το πρότυπο. Είναι μία οντότητα ανεξάρτητη από επίπεδα και θα έπαιρνε και θα καθόριζε, τυπικά, τιμές από το MLME και το PLME, για να τις περάσει σε λειτουργίες διαχείρισης υψηλότερου επιπέδου. Μπορεί να θεωρηθεί ότι βρίσκεται στο επίπεδο ελέγχου.

3.1.3. IEEE 802.11 ως Ad Hoc Δίκτυο

Όπως αναφέρθηκε και προηγούμενα, το πρότυπο IEEE 802.11 επιτρέπει την διαμόρφωση δικτύων που δεν έχουν σταθερή δομή. Αυτή η παράγραφος σημειώνει τις διαφορές και τα ιδιαίτερα χαρακτηριστικά του ad hoc τρόπου λειτουργίας.

Όταν γίνεται λόγος για ένα ad hoc δίκτυο, το IEEE 802.11 αναφέρεται στο IBSS όπου όλοι οι σταθμοί βρίσκονται σε αμοιβαία περιοχή επικοινωνίας και έχουν την δυνατότητα της απευθείας σύνδεσης. Λογικά, μόνο αυτό το IBSS υπάρχει, και οι σταθμοί δεν μπορούν να φύγουν από την περιοχή κάλυψης του IBSS χωρίς να αποσυνδεθούν. Το IBSS δεν έχει σημείο πρόσβασης και, επομένως, δεν μπορεί να χρησιμοποιήσει το DS. Άρα, οι σταθμοί χρησιμοποιούν, απλά, τις υπηρεσίες σταθμών. Οι βασικές αλλαγές λαμβάνουν χώρα στο επίπεδο MAC, συγκεκριμένα το MLME και το φυσικό επίπεδο παραμένουν αναλλοίωτα. Το PCF δεν χρησιμοποιείται σε ad hoc τρόπο. Το επίπεδο MAC παρέχει μόνο υπηρεσίες σύγκρουσης, πιστοποίηση και μυστικότητα στα υψηλότερα επίπεδα. Από την στιγμή που δεν υπάρχει διαθέσιμο σημείο πρόσβασης, οι σταθμοί δεν μπορούν να συσχετιστούν με κανένα BSS, κι έτσι επιτρέπονται μόνο τα πλαίσια που δεν χρησιμοποιούν το DS.

Επιπρόσθετα, το αναγνωριστικό του BSS (στην περίπτωση σταθερής δομής) παραχωρείται, πλέον, τοπικά.

Το MLME αντανακλά τον τύπο του δικτύου με περισσότερο προφανή τρόπο. Ο συγχρονισμός μεταξύ των σταθμών επιτυγχάνεται, πλέον, με τα μέσα ενός κατανεμημένου αλγορίθμου. Αυτός ο αλγόριθμος δείχνει, επίσης, και την ιδέα της διαχείρισης πίσω από τον ad hoc τρόπο.

Ο πρώτος σταθμός που εγκαθιστά ένα IBSS καθορίζει το beacon διάστημα, ένα διάστημα σταθερού μήκους και το σημείο εκκίνησης αυτού, που έχει τον χαρακτήρα της ευρυεκπομπής και προσαρμόζεται στο IBSS από κάθε σταθμό. Επομένως, κάθε σταθμός στο IBSS γνωρίζει πότε θα έπρεπε να μεταδοθεί το επόμενο beacon. Αυτή την στιγμή, κάθε σταθμός υπολογίζει ένα τυχαίο διάστημα “beacon backoff” και μεταδίδει το πλαίσιο beacon, αν δεν έχει λάβει ένα νωρίτερα από την εκπνοή του backoff διαστήματος. Κατά την περίοδο του συναγωνισμού, σταματούν οι μεταδόσεις πακέτων δεδομένων και μηνυμάτων ένδειξης ανακοίνωσης κίνησης. Ο αλγόριθμος διασφαλίζει ότι

θα υπάρχει πάντοτε ένα beacon που θα μεταδίδεται στο IBSS. Ο σταθμός που μετέδωσε τελευταίος ένα beacon πλαίσιο επιλέγεται να απαντήσει στις αιτήσεις διερεύνησης πρόσβασης στο μέσο.

Με την λήψη ενός beacon με μία χρονική σφραγίδα μεγαλύτερη από αυτή του σταθμού, ο σταθμός προσαρμόζει το χρονόμετρό του ανάλογα. Μαζί με το γεγονός ότι ένας σταθμός που συνδέεται με ένα IBSS ορίζει τον χρονιστή του στο μηδέν αυτό σημαίνει ότι ένας παλιότερος σταθμός θα υπέρβαινε τους κανόνες των νέο-συσχετισμένων τερματικών. Ένας νέος σταθμός σε ένα IBSS δεν μεταδίδει κανένα beacon ή μήνυμα απόκρισης σε αιτήσεις διερεύνησης του μέσου μέχρι να ακούσει κάποιο από το IBSS του.

Ο μηχανισμός εξοικονόμησης ισχύος σε ad hoc τρόπο βασίζεται σε μία περιοδική ενεργοποίηση των σταθμών ανά χρονικά παράθυρα. Μέσα στα πλαίσια ενός τέτοιου παραθύρου τοποθετούνται οποιεσδήποτε αιτήσεις για εκπομπές, και αν ένας σταθμός σε ανενεργή κατάσταση λάβει μία, ενεργοποιείται για, τουλάχιστον, το επόμενο διάστημα του beacon. Το παράθυρο καθορίζεται, επίσης, από τον πρώτο σταθμό που αρχικοποιεί το IBSS. Αν το χρονικό παράθυρο είναι μηδέν, δεν χρησιμοποιείται η μέθοδος εξοικονόμησης ενέργειας. Σε αντίθεση με τον ad hoc τρόπο λειτουργίας, η εξοικονόμηση ισχύος σε περιπτώσεις σταθερής δομής ελέγχεται από το σημείο πρόσβασης.

Το SME, πρέπει να ενεργεί σύμφωνα με τις τιμές που παρέχονται από το MLME. Η συμπεριφορά του δεν προδιαγράφεται από το πρότυπο. Θα ήταν εργασία του SME η επιλογή ανίχνευσης μιας συγκεκριμένης περιοχής συχνотήτων με σκοπό την ανεύρεση όσο το δυνατόν περισσότερων τερματικών στην περιοχή επικοινωνίας.

Συνοψίζοντας, οι αλλαγές για την υποστήριξη ad hoc δικτύων είναι:

1. Εγκατάλειψη του κεντριοποιημένου τρόπου, όχι υπηρεσίες ελεύθερες συγκρούσεων (όχι PCF).
2. Προσφορά ενός κατανεμημένου μηχανισμού για να επιτρέπεται ο συγχρονισμός των σταθμών.
3. Παροχή ενός αποδοτικού μηχανισμού εξοικονόμησης ισχύος.
4. Παροχή ενός μηχανισμού αυτό-διεύθυνσης για τις ανάγκες του IBSS.

3.2. HIPERLAN/2

Μέχρι σήμερα, τα ασύρματα δίκτυα είναι περισσότερο ή λιγότερο συνώνυμα με τα κυψελωτά δίκτυα ευρείας περιοχής που βασίζονται σε διαφορετικά πρότυπα, όπως, για παράδειγμα το GSM, το AMPS, κ.τ.λ. Έχουν οριστεί να έχουν ως κύριο στόχο την υποστήριξη φωνής, αν και κάποια προσφέρουν επίσης υπηρεσίες δεδομένων σε πολύ χαμηλή ταχύτητα (~10kbps).

Ασύρματες υπηρεσίες δεδομένων που προσφέρουν την αναγκαία ρυθμιζόμενη ώστε να ικανοποιήσουν τις πραγματικές απαιτήσεις για την πρόσβαση στο εσωτερικό του δικτύου ή στο διαδίκτυο βρίσκονται, μόλις, στο αρχικό στάδιο της αναμενόμενης εξέλιξής τους στην αγορά. Στο περιβάλλον των τοπικών δικτύων (Local Area Network – LAN), τα προϊόντα για τα ασύρματα δίκτυα (Wireless LAN – WLAN), που βασίζονται σε διαφορετικές αποχρώσεις του 802.11, διατίθενται στην αγορά. Ανάλογα με το εφαρμοζόμενο σχήμα μετάδοσης, τα προϊόντα μπορούν να προσφέρουν εύρος ζώνης από

1Mbps έως 11Mbps. Οι τιμές αναμένεται να πέσουν, γεγονός που θα καταστήσει τα ασύρματα τοπικά δίκτυα ολοένα και πιο σοβαρή εναλλακτική λύση στην σταθερή πρόσβαση Ethernet. Στην ευρεία περιοχή, οι υπηρεσίες GPR (General Packet Radio) θα έχουν την δυνατότητα να αυξήσουν το διαθέσιμο εύρος ζώνης μέχρι τα 64 kbps, καθιστώντας αυτού του είδους την υπηρεσία συγκρίσιμη με το dial-in.

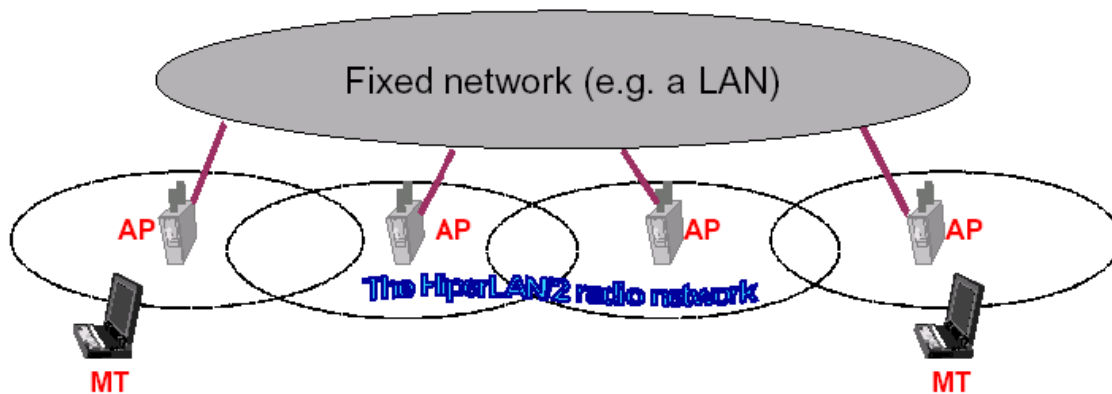
Για να ικανοποιηθούν οι μελλοντικές απαιτήσεις των δικτύων, μία νέα γενιά τεχνολογιών που συνδυάζει ασύρματα τοπικά και κυψελωτά δίκτυα βρίσκεται υπό ανάπτυξη. Αυτές οι απαιτήσεις περιλαμβάνουν υποστήριξη για QoS (ώστε να κατασκευαστούν δίκτυα πολλαπλών υπηρεσιών), ασφάλεια, δυνατότητα μεταβίβασης κατά την κίνηση μεταξύ τοπικής και ευρείας περιοχής, αυξημένη ρυθμαπόδοση για την ανάγκη καλύτερης απόδοσης τόσο για τις υπηρεσίες δεδομένων όσο και για τις εφαρμογές video.

Η παράγραφος αυτή εισάγει τα χαρακτηριστικά στοιχεία της γενιάς της τεχνολογίας των ασύρματων τοπικών δικτύων που ονομάζεται HIPERLAN/2. Το HIPERLAN/2 είναι ένα πρότυπο-προδιαγραφή που αναπτύχθηκε από τον ETSI και μπορεί να χρησιμοποιηθεί σε παγκόσμια κλίμακα. Οι προδιαγραφές του HIPERLAN/2 είναι διαθέσιμες από τις αρχές του 2000.

3.2.1. Το Δίκτυο HIPERLAN/2

Το δίκτυο HIPERLAN/2 τυπικά έχει μία τοπολογία όπως φαίνεται στην Εικόνα 3 παρακάτω. Τα κινητά τερματικά (Mobile Terminals – MT) επικοινωνούν με τα σημεία πρόσβασης (Access Points – AP) ασύρματα – μέσω του αέρα – όπως ορίζεται από την προδιαγραφή του HIPERLAN/2. Υπάρχει, επίσης, ο απευθείας τρόπος επικοινωνίας μεταξύ δύο συσκευών, ο οποίος βρίσκεται ακόμη στα αρχικά στάδια ανάπτυξης και δεν περιγράφεται περαιτέρω σε αυτό το σημείο του κειμένου. Ο χρήστης του κινητού τερματικού μπορεί να κινείται ελεύθερα στο δίκτυο του HIPERLAN/2, το οποίο και θα διασφαλίζει ότι ο χρήστης και το τερματικό θα λαμβάνουν την μέγιστη δυνατή απόδοση μετάδοσης. Ένα κινητό τερματικό, αφού συντελεστεί η σύνδεσή του με το δίκτυο, μπορεί να επικοινωνεί μόνο με ένα σημείο πρόσβασης κάθε φορά. Τα σημεία πρόσβασης είναι υπεύθυνα για την αυτόματη διαμόρφωση του ασύρματου δικτύου, αφού λάβουν υπόψη τους αλλαγές στην τοπολογία, π.χ. δεν υφίσταται ανάγκη για χειρονακτικό προγραμματισμό συχνοτήτων.

Τα χαρακτηριστικά και τα πρωτόκολλα του HIPERLAN/2 δικτύου περιγράφονται με μεγαλύτερη λεπτομέρεια στις επόμενες παραγράφους.



Εικόνα 3: Ένα δίκτυο HIPERLAN/2

3.2.2. Χαρακτηριστικά Στοιχεία του HIPERLAN/2

Τα γενικά χαρακτηριστικά της τεχνολογίας του HIPERLAN/2 είναι τα παρακάτω:

- Μετάδοση υψηλής ταχύτητας

Το HIPERLAN/2 έχει έναν πολύ υψηλό ρυθμό μετάδοσης, που στο φυσικό επίπεδο φθάνει τα 54Mbps και στο τρίτο επίπεδο τα 25Mbps. Για να επιτευχθεί αυτό, το HIPERLAN/2 χρησιμοποιεί μία μέθοδο διαμόρφωσης που ονομάζεται ορθογώνια ψηφιακή πολυπλεξία διαίρεσης συχνότητας (Orthogonal Frequency Division Multiplexing – OFDM) για την μετάδοση αναλογικών σημάτων. Η OFDM είναι πολύ αποδοτική σε περιβάλλοντα διασποράς χρόνου, όπως, για παράδειγμα, μέσα σε γραφεία όπου τα μεταδιδόμενα σήματα αντανακλώνται από πολλά σημεία, με αποτέλεσμα να καταλήξουν με διαφορετικούς χρόνους διάδοσης, τελικά, στο σημείο λήψης. Πάνω από το φυσικό επίπεδο, το πρωτόκολλο ελέγχου πρόσβασης του μέσου (Medium Access Control – MAC) είναι στο σύνολό του νέο και εφαρμόζει μία μορφή δυναμικής διμερούς διαίρεσης χρόνου που επιτρέπει την πιο αποδοτική χρησιμοποίηση των ασύρματων πόρων.

- Υπηρεσίες με σύνδεση

Σε ένα HIPERLAN/2 δίκτυο, τα δεδομένα μεταδίδονται πάνω στις συνδέσεις μεταξύ του κινητού τερματικού και του σημείου πρόσβασης που έχουν εγκατασταθεί πριν την μετάδοση η οποία χρησιμοποιεί λειτουργίες του επιπέδου ελέγχου που σχετίζονται με την σηματοδότηση. Οι συνδέσεις πολυπλέκονται με διαίρεση χρόνου μέσω της διεπαφής του αέρα. Υπάρχουν δύο τύποι συνδέσεων, σημείο προς σημείο και σημείο προς πολλαπλά σημεία. Οι συνδέσεις σημείο προς σημείο είναι αμφίδρομες ενώ οι συνδέσεις σημείο προς πολλαπλά σημεία είναι μονοκατευθυντικές προς την κατεύθυνση του κινητού τερματικού. Επιπρόσθετα, υπάρχει ένα αφιερωμένο κανάλι ευρυεκπομπής, μέσω του οποίου, η κίνηση των δεδομένων που εκπέμπονται από το σημείο πρόσβασης φθάνει σε όλα τα τερματικά.

- Υποστήριξη QoS

Η φύση του HIPERLAN/2 με τις προσφερόμενες υπηρεσίες με σύνδεση, καθιστούν άμεση την εφαρμογή παραμέτρων για την υποστήριξη του QoS. Σε κάθε σύνδεση μπορεί να ανατεθεί μία συγκεκριμένη τιμή για QoS, για παράδειγμα σε όρους εύρους ζώνης, καθυστέρησης, μεταβλητότητας, ρυθμού σφαλμάτων, κ.τ.λ. Είναι, επίσης, δυνατή η χρήση μίας πιο απλοϊκής προσέγγισης, όπου σε κάθε σύνδεση μπορεί να παραχωρηθεί ένα επίπεδο προτεραιότητας σε σχέση με τις άλλες συνδέσεις.

Αυτή η υποστήριξη του QoS σε συνδυασμό με τον υψηλό ρυθμό μετάδοσης καθιστά πιο εύκολη την ταυτόχρονη εκπομπή πολλών διαφορετικών τύπων ροής πληροφορίας, π.χ. video, φωνή και δεδομένα.

- Αυτόματη κατανομή συχνοτήτων

Σε ένα HIPERLAN/2 δίκτυο, δεν υπάρχει ανάγκη για χειρονακτικό προγραμματισμό των συχνοτήτων όπως σε κυψελωτά δίκτυα σαν το GSM. Οι σταθμοί βάσης, που στο HIPERLAN/2 ονομάζονται σημεία πρόσβασης, υποστηρίζουν την αυτόματη επιλογή του κατάλληλου καναλιού για μετάδοση μέσα στα όρια της περιοχής κάλυψής τους. Ένα σημείο πρόσβασης ακούει τα γειτονικά σημεία πρόσβασης όπως επίσης και τις υπόλοιπες πηγές σημάτων στον περιβάλλοντα χώρο, και επιλέγει ένα κατάλληλο κανάλι βασιζόμενο τόσο στην πληροφορία για το ποια άλλα κανάλια χρησιμοποιούνται από τους γειτονικούς σταθμούς βάσης, όσο και στην ελαχιστοποίηση των παρεμβολών.

- Υποστήριξη ασφάλειας

Το HIPERLAN/2 δίκτυο έχει την δυνατότητα υποστήριξης πιστοποίησης και κρυπτογράφησης. Με την διαδικασία της πιστοποίησης τόσο το σημείο πρόσβασης όσο και το κινητό τερματικό μπορούν να πιστοποιήσουν το ένα το άλλο ώστε να διασφαλίσουν διαπιστευμένη πρόσβαση στο δίκτυο (από την πλευρά του σημείου πρόσβασης) ή να εξασφαλίσουν πρόσβαση σε έναν έγκυρο παροχέα υπηρεσιών του δικτύου (από την πλευρά του κινητού τερματικού). Η πιστοποίηση στηρίζεται στην ύπαρξη μίας βοηθητικής λειτουργίας, όπως μία υπηρεσία καταλόγου που, όμως, είναι έξω από τους σκοπούς του HIPERLAN/2.

Η κίνηση των δεδομένων στις συνδέσεις που έχουν εγκατασταθεί μπορεί να κρυπτογραφηθεί για την προστασία απέναντι, για παράδειγμα, στις περιπτώσεις υποκλοπών.

- Υποστήριξη κινητικότητας

Το κινητό τερματικό είναι υπεύθυνο για την αποστολή και την λήψη δεδομένων προς/από το “κοντινότερο” σημείο πρόσβασης, ή πιο σωστά, η συσκευή χρησιμοποιεί το σταθμό βάσης με το καλύτερο δυνατό σήμα όπως μετράται από τον σηματοθορυβικό λόγο. Επομένως, καθώς ο χρήστης και το κινητό τερματικό μετακινούνται, η συσκευή μπορεί να ανιχνεύσει ότι υπάρχει ένα εναλλακτικό σημείο πρόσβασης με καλύτερη απόδοση στη μετάδοση από ότι το σημείο πρόσβασης με το οποίο είναι μέχρι εκείνη την στιγμή συνδεδεμένη. Στην συνέχεια, το κινητό τερματικό θα προχωρήσει στην μεταβίβαση της ευθύνης της κλήσης του στο νέο σημείο πρόσβασης. Όλες οι εγκατεστημένες συνδέσεις θα μετατεθούν προς το νέο σημείο πρόσβασης έτσι, ώστε το κινητό τερματικό να παραμένει συνδεδεμένο με το HIPERLAN/2 δίκτυο και να έχει την

δυνατότητα να συνεχίσει την επικοινωνία του. Κατά την διάρκεια της μεταβίβασης από σταθμό βάσης σε άλλον, μερικά πακέτα μπορεί να χαθούν.

Αν κάποιο κινητό τερματικό κινείται έξω από την περιοχή κάλυψης για ένα συγκεκριμένο χρόνο, η συσκευή μπορεί να χάσει την επαφή της με το HIPERLAN/2 δίκτυο με αποτέλεσμα την απώλεια όλων των συνδέσεων.

- Ανεξαρτησία από άλλα δίκτυα και εφαρμογές

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

- Εξοικονόμηση ισχύος

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

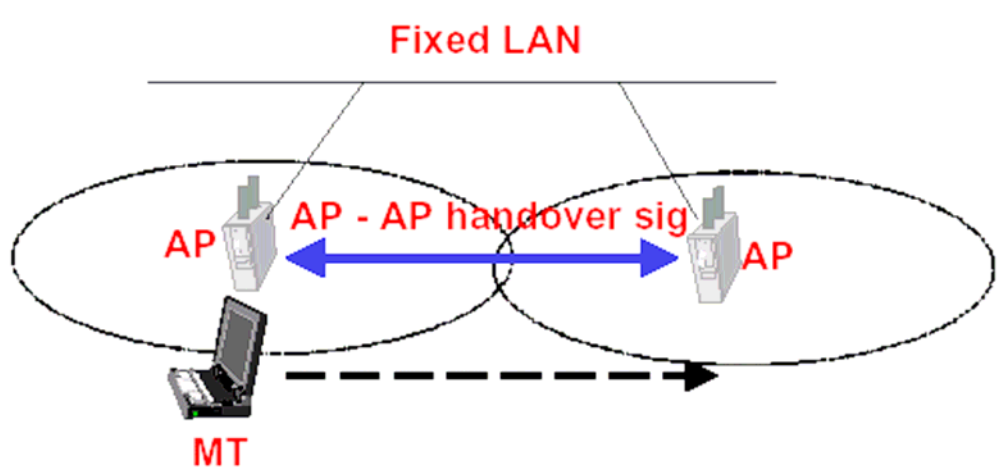
3.2.3. Τρόπος Λειτουργίας του Δικτύου

Η Εικόνα 4 δείχνει ένα σενάριο που περιλαμβάνει ένα κινητό τερματικό και δύο σημεία πρόσβασης που είναι συνδεδεμένα με ένα σταθερό δίκτυο και υποστηρίζουν το σχήμα με τις ενδείξεις προτεραιοτήτων.

Τα σημεία πρόσβασης έχουν επιλέξει, το καθένα, κατάλληλες συχνότητες σύμφωνα με τον αλγόριθμο DFS.

Το κινητό τερματικό (MT) ξεκινά μετρώντας την ισχύ του σήματος και επιλέγει το αρμόζον σημείο πρόσβασης (AP) με το οποίο θέλει να συσχετιστεί. Από το επιλεγθέν σημείο πρόσβασης το κινητό τερματικό λαμβάνει ένα αναγνωριστικό (MAC-ID). Ακολουθεί η ανταλλαγή των δυνατοτήτων της ζεύξης ώστε να αποφασιστεί, ανάμεσα σε όλα τα υπόλοιπα, η διαδικασία πιστοποίησης και ο αλγόριθμος κρυπτογράφησης όπως επίσης και ποιο επίπεδο σύγκλισης θα χρησιμοποιηθεί για τις ανάγκες της κίνησης του επιπέδου του χρήστη. Έπειτα από μία πιθανή ανταλλαγή κλειδιού και πιστοποίηση, το

κινητό τερματικό συσχετίζεται με το σημείο πρόσβασης. Τελικά, οι DLC συνδέσεις χρήστη εγκαθίστανται και μέσω αυτών μεταδίδεται η κίνηση του επιπέδου του χρήστη.



Εικόνα 4: Δείγμα ενός δικτύου HIPERLAN/2 που συνδέεται μέσω σταθερού δικτύου

Το κινητό τερματικό θα στείλει και θα λάβει δεδομένα σε δύο εγκατεστημένες συνδέσεις υποστηρίζοντας δύο διαφορετικής προτεραιότητας ουρές (παραπάνω από δύο ουρές με διαφορετική προτεραιότητα μπορούν να υποστηριχθούν). Το Ethernet CL διασφαλίζει ότι οι προτεραιότητες για κάθε Ethernet πλαίσιο απεικονίζονται στις αντίστοιχες συνδέσεις σύμφωνα με το προκαθορισμένο σχήμα απεικόνισης.

Το κινητό τερματικό μπορεί, στη συνέχεια, να αποφασίσει να μετάσχει σε μία ή περισσότερες ομάδες πολυεκπομπής. Το HIPERLAN/2 δίκτυο μπορεί να διαμορφωθεί ώστε να χρησιμοποιήσει μονοεκπομπή για βέλτιστη ποιότητα, ή να κρατήσει μία MAC-ID για κάθε μία ομάδα στην οποία συμμετέχει και, έτσι, να καταναλώσει μικρότερο εύρος ζώνης. Εάν ένα ξεχωριστό MAC-ID χρησιμοποιηθεί για μία ομάδα πολυεκπομπής, η απεικόνιση θα είναι ως εξής:

IP διεύθυνση IEEE διεύθυνση MAC-ID

Καθώς κινείται το τερματικό, μπορεί να αποφασίσει να εκτελέσει μία μεταβίβαση εάν ανιχνεύσει ότι υπάρχει ένα σημείο πρόσβασης που είναι πιο κατάλληλο για τις ανάγκες της επικοινωνίας (για παράδειγμα με μεγαλύτερη ισχύ σήματος). Όλες οι εγκατεστημένες συνδέσεις καθώς και οι πιθανές συσχετίσεις ασφάλειας θα μεταβιβαστούν αυτόματα στο νέο σημείο πρόσβασης χρησιμοποιώντας την σηματοδότηση μεταξύ των σταθμών βάσης μέσω του σταθερού δικτύου. Όταν το κινητό τερματικό (ή πιο σωστά ο χρήστης) επιθυμεί να αποσυνδεθεί από το τοπικό δίκτυο, η συσκευή κάνει αίτηση αποσυσχέτισης που έχει σαν αποτέλεσμα την απελευθέρωση όλων των συνδέσεων μεταξύ του κινητού τερματικού και του σημείου πρόσβασης. Αυτό μπορεί να συμβεί και στην περίπτωση που το κινητό τερματικό κινηθεί έξω από τα όρια της περιοχής κάλυψης για ένα συγκεκριμένο χρονικό διάστημα.

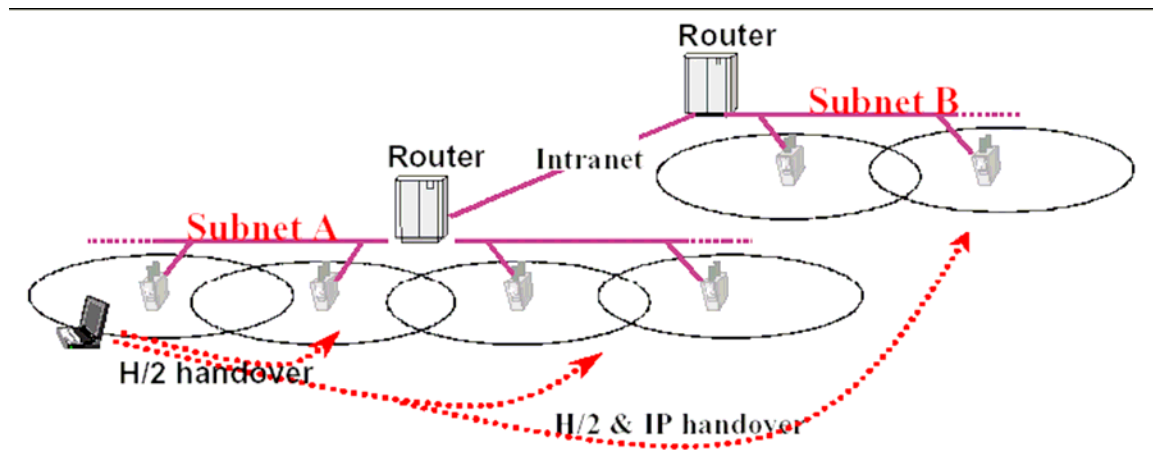
3.2.3.1. Παραδείγματα Εφαρμογών

Συλλογικό τοπικό δίκτυο

Η Εικόνα 5 δείχνει ένα παράδειγμα μιας τοπολογίας συλλογικού δικτύου μεταξύ Ethernet και δρομολογητών IP. Ένα δίκτυο HIPERLAN/2 χρησιμοποιείται ως το τελευταίο κομμάτι σύνδεσης μεταξύ των κινητών τερματικών και του δικτύου. Το δίκτυο HIPERLAN/2 υποστηρίζει την κινητικότητα μέσα στα όρια του ίδιου τοπικού δικτύου/υποδικτύου. Η κίνηση μεταξύ των υποδικτύων υπονοεί IP κινητικότητα η οποία αναλαμβάνεται από ένα επίπεδο πιο πάνω από το HIPERLAN/2.

Hot spots

Το δίκτυο HIPERLAN/2 μπορεί να αναπτυχθεί σε περιοχές hot spots. Τέτοιες είναι για παράδειγμα τα αεροδρόμια, τα ξενοδοχεία, κ.τ.λ. Έτσι, παρέχεται η δυνατότητα της εύκολης απομακρυσμένης πρόσβασης και των υπηρεσιών διαδικτύου σε εργαζόμενους. Ένας server πρόσβασης, με τον οποίο το δίκτυο HIPERLAN/2 θα συνδέεται, θα έχει την δυνατότητα της δρομολόγησης μίας αίτησης για σύνδεση σημείο-προς-σημείο είτε στο συνολικό δίκτυο είτε στο ISP όταν πρόκειται για πρόσβαση στο διαδίκτυο.



Εικόνα 5: Χρήση του HIPERLAN/2 σε ένα συλλογικό δίκτυο

Πρόσβαση σε τρίτης γενιάς κυψελωτά δίκτυα

Το HIPERLAN/2 μπορεί να χρησιμοποιηθεί σαν μία εναλλακτική λύση πρόσβασης σε ένα 3^{ης} γενιάς κυψελωτό δίκτυο. Μπορεί κάποιος να σκεφτεί την πιθανότητα κάλυψης των hot spots και των αστικών περιοχών με την βοήθεια του HIPERLAN/2 ενώ οι ευρείες περιοχές να καλύπτονται από την τεχνολογία CDMA. Με αυτό τον τρόπο, ένας χρήστης μπορεί να επωφεληθεί από ένα δίκτυο υψηλής απόδοσης, όποτε είναι εφικτή η ανάπτυξη HIPERLAN/2, και να χρησιμοποιεί οπουδήποτε αλλού W-CDMA. Το κυρίως δίκτυο θα έχει την ευθύνη της αυτόματης και διαφανούς, για τον χρήστη, μεταβίβασης μεταξύ των δύο τύπων δικτύων πρόσβασης καθώς εκείνος θα κινείται ανάμεσά τους.

Οικιακό δίκτυο

Άλλο ένα παράδειγμα του HIPERLAN/2 είναι η χρησιμοποίηση της τεχνολογίας σε ένα οικιακό περιβάλλον με σκοπό την δημιουργία μίας σταθερής δομής για τις οικιακές συσκευές (PC, VCR, κάμερες, εκτυπωτές κ.α). Η υψηλή ρυθμαπόδοση και τα στοιχεία QoS του HIPERLAN/2 μπορούν να υποστηρίξουν την μετάδοση ροών video σε σύνδεση με εφαρμογές datacom. Το σημείο πρόσβασης μπορεί, σε αυτή την περίπτωση, να περιλαμβάνει μία “ανερχόμενη ζεύξη” για το δημόσιο δίκτυο, για παράδειγμα ένα καλωδιακό modem.

3.2.3.2. Απόδοση

Η απόδοση σε όρους ρυθμαπόδοσης του χρήστη και της καθυστέρησης εξαρτάται από έναν αριθμό από παράγοντες, όπως είναι ο διαθέσιμος αριθμός συχνοτήτων, οι συνθήκες διάδοσης στο κτίριο και η παρουσία παρεμβολών (παρουσία άλλου HIPERLAN/2 συστήματος στην κοντινή γειτονιά).

3.2.4. HIPERLAN/2 ως Ad Hoc Δίκτυο

Το HIPERLAN/2 μπορεί να λειτουργήσει και σύμφωνα με τον απευθείας τρόπο (καθαρά ad hoc), που επιτρέπει την ανάπτυξη και υποστήριξη ad hoc δικτύων. Για ένα ad hoc δίκτυο, εφαρμόζεται η επέκταση για οικιακό περιβάλλον (Home Environment Extension) του HIPERLAN/2. Στο οικιακό περιβάλλον κυριαρχεί η αμοιβαία ανταλλαγή δεδομένων μεταξύ των κινητών τερματικών χρησιμοποιώντας την απευθείας ζεύξη, αντίθετα με το σενάριο του σημείου πρόσβασης σε δίκτυα σταθερής δομής. Παρόλ’ αυτά, το σχήμα TDMA/TDD στο HIPERLAN/2 απαιτεί έναν κεντρικό ελεγκτή (Central Controller) στο δίκτυο, που θα σχεδιάζει και θα προγραμματίζει όλη την κίνηση. Μολαταύτα, στην προδιαγραφή του HIPERLAN/2 για το οικιακό περιβάλλον ο κεντρικός ελεγκτής, που επιλέγεται τυχαία από τα υπάρχοντα κινητά τερματικά (που έχουν την λειτουργική ικανότητα να γίνουν κεντρικοί ελεγκτές) σχεδιάζουν και προγραμματίζουν το σύνολο της κίνησης, συντηρούν το δίκτυο και παραχωρούν πόρους όπως ακριβώς κι ένα σημείο πρόσβασης κατά τον κεντριοποιημένο τρόπο λειτουργίας του HIPERLAN/2.

Το φυσικό επίπεδο δεν αλλάζει σημαντικά στο οικιακό περιβάλλον. Για να αντιμετωπιστεί η πιθανότητα διασποράς των διαφορών στην καθυστέρηση μεταξύ δύο σταθμών, εισάγεται, από τον κεντρικό ελεγκτή, μία περίοδος φύλαξης μεταξύ δύο διαδοχικών φάσεων απευθείας ζεύξης. Επιπλέον, υπάρχει ένα κομμάτι προλόγου που προστίθεται από τον κεντρικό ελεγκτή για να δηλώσει την απευθείας ζεύξη. Όπως και στον κεντριοποιημένο τρόπο λειτουργίας, πολλαπλά υποδίκτυα μπορούν να δημιουργηθούν χρησιμοποιώντας διάφορα κανάλια συχνοτήτων. Αυτά τα υποδίκτυα μπορούν να συνδεθούν από οποιαδήποτε οικιακή συσκευή HIPERLAN/2. Στο MAC επίπεδο, οι αιτήσεις για πόρους στην απευθείας ζεύξη στέλνονται σε ένα διαφορετικό κανάλι, το οποίο και ονομάζεται “ανερχόμενο κανάλι”. Ο κεντριοποιημένος έλεγχος του μέσου παραμένει. Κάθε κινητό τερματικό ακολουθεί το σύνολο των γνωστών διαδικασιών με την πρόσβαση να ζητείται από τις συσκευές και να παραχωρείται από τον

κεντρικό ελεγκτή. Το πρόβλημα του κρυμμένου τερματικού δεν λύνεται σε αυτή την προδιαγραφή, όμως, ένας κόμβος που δεν μπορεί να δει τον κεντρικό ελεγκτή δεν μπορεί να θεωρηθεί κρυμμένος. Σε μελλοντικές εκδόσεις της προδιαγραφής η ETSI BRAN σχεδιάζει να υποστηρίξει και τα κρυμμένα τερματικά. Το σχήμα διευθυνσιοδότησης παραμένει το ίδιο. Με την απευθείας ζεύξη, ο κεντρικός ελεγκτής παραχωρεί μία MAC-ID στον εαυτό του και σε άλλους συσχετισμένους σταθμούς (αφού η επιλογή των κεντρικών ελεγκτών έχει περατωθεί). Το αναγνωριστικό του σημείου πρόσβασης (AP-ID) επιλέγεται τυχαία, όπως επίσης και το αναγνωριστικό του δικτύου (NET-ID) το οποίο είναι και μοναδικό για τον κάτοχο της ομάδας των συσκευών. Στο υποεπίπεδο του EC υποστηρίζεται ένας τέταρτος τρόπος για τον έλεγχο των σφαλμάτων που ονομάζεται πρόωρος έλεγχος σφαλμάτων (Forward Error Control – FEC). Οι άλλοι τρόποι (επιβεβαίωση, επανάληψη, έλλειψη επιβεβαίωσης) παραμένουν ως έχουν. Συμπερασματικά, οι επεκτάσεις του DLC στο οικιακό περιβάλλον υποστηρίζουν την εκτεταμένη χρήση της απευθείας ζεύξης από ότι της ανερχόμενης και κατερχόμενης ζεύξης. Προδιαγράφονται μηχανισμοί υποστήριξης της αυτό-οργάνωσης των υποδικτύων, στοιχείο ιδιαίτερα ουσιώδες για ένα ad hoc δίκτυο.

3.3. BLUETOOTH

Bluetooth είναι το όνομα που δόθηκε σε ένα νέο πρότυπο το οποίο χρησιμοποιεί ραδιοζεύξεις μικρής εμβέλειας και πρόκειται να αντικαταστήσει τις καλωδιακές συνδέσεις μεταξύ των κινητών και των σταθερών ηλεκτρονικών συσκευών. Το πρότυπο αυτό, καθορίζει μια ομοιόμορφη δομή για ένα μεγάλο εύρος συσκευών, ώστε να επικοινωνούν μεταξύ τους με ελάχιστη προσπάθεια από το χρήστη. Οι κυριότερες ιδιότητές του είναι η ευρωστία, η μικρή πολυπλοκότητα, η χαμηλή ισχύς και το χαμηλό κόστος.

Ένα τυπικό σχήμα μιας τοπολογίας που χρησιμοποιεί το πρωτόκολλο Bluetooth φαίνεται στη συνέχεια.

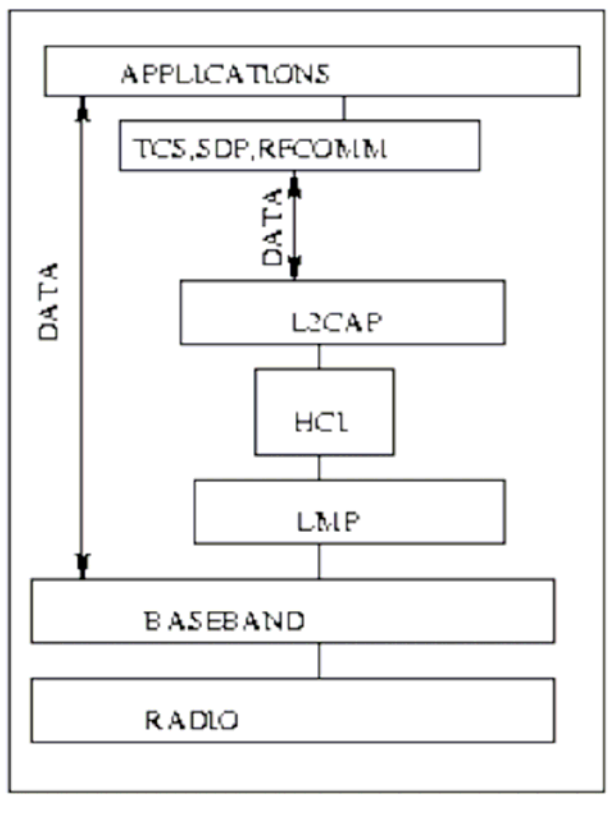


Εικόνα 6: Τοπολογία Πρωτοκόλλου Bluetooth

Η άμεση ανάγκη για Bluetooth όπως αναφέρεται νωρίτερα προήλθε από την επιθυμία να συνδεθούν οι περιφερειακές μονάδες και οι συσκευές χωρίς τα καλώδια. Η διαθέσιμη τεχνολογία - IRDA OBEX είναι βασισμένη στις υπέρυθρες συνδέσεις που είναι περιορισμένες στο LOS. Το Bluetooth τροφοδοτείται περαιτέρω από την ζήτηση για την κινητή και ασύρματη πρόσβαση σε LANs, το διαδίκτυο πάνω από κινητά και τα άλλα υπάρχοντα δίκτυα, όπου η υποδομή συνδέεται με καλώδιο αλλά τα διασυνδεδεμένα μέρη είναι ελεύθερα να κινούνται. Αυτό όχι μόνο καθιστά το δίκτυο ευκολότερο να χρησιμοποιηθεί, αλλά και επεκτείνει την προσιτότητά του. Τα πλεονεκτήματα και ο γρήγορος πολλαπλασιασμός των LANs έχουν ως αποτέλεσμα ότι η δημιουργία προσωπικών δικτύων περιοχής (PANs), δηλαδή συνδέσεις μεταξύ των συσκευών στην εγγύτητα του χρήστη, θα έχει πολλές ευεργετικές χρήσεις. Το Bluetooth θα μπορούσε επίσης να χρησιμοποιηθεί στις οικιακές δικτυακές εφαρμογές. Με τους αυξανόμενους αριθμούς σπιτιών που κατέχουν πολλαπλά PCs, η ανάγκη για τα δίκτυα που είναι απλά να εγκατασταθούν και να διατηρηθούν, διευρύνεται. Υπάρχει επίσης η εμπορική ανάγκη να παρασχεθούν οι δυνατότητες κάλυψης "προώθησης πληροφοριών", η οποία είναι σημαντική για τα handhelds και άλλες τέτοιες κινητές συσκευές και αυτό έχει ενσωματωθεί μερικώς στο Bluetooth. Η βασική δύναμη του Bluetooth είναι η δυνατότητά του να χειριστεί ταυτόχρονα και τα δεδομένα και τη μεταφορά φωνής, που επιτρέπουν καινοτόμες λύσεις όπως μια κινητή με ελεύθερα χέρια κάσκα για τις κλήσεις φωνής, δυνατότητα αποστολής φαξ, αυτόματος συγχρονισμός PDA και κινητού υπολογιστή και εφαρμογές βιβλίων τηλεφωνικών διευθύνσεων. Αυτές οι χρήσεις προτείνουν ότι μια τεχνολογία όπως το Bluetooth είναι εξαιρετικά χρήσιμη και θα έχει μια σημαντική επίδραση στον τρόπο που οι πληροφορίες προσεγγίζονται και χρησιμοποιούνται.

3.3.1. Βασική Αρχιτεκτονική Συστήματος

Η αρχιτεκτονική του συστήματος του πρωτοκόλλου Bluetooth θα περιγραφεί εν συντομία στη συνέχεια. Ο σχεδιασμός έχει τμηματοποιηθεί σε ανεξάρτητα σχεδόν επίπεδα, έτσι ώστε να είναι εύκολη η περιγραφή. Η στοίβα πρωτοκόλλων του Bluetooth παρατίθεται παρακάτω.



Εικόνα 7:Στοιβα Πρωτοκόλλων

Στη συνέχεια θα δούμε ξεχωριστά αυτά τα υποεπίπεδα και θα αναφερθούμε στα βασικότερα στοιχεία τους.

Επίπεδο Ραδιοζεύξεων

Το επίπεδο αυτό δημιουργεί τις φυσικές συνδέσεις μεταξύ των συσκευών. Οι συνδέσεις αυτές λειτουργούν στη μάντα ISM (2.4 GHz) και χρησιμοποιούν τεχνολογία FHSS (Frequency Hopping Spread Spectrum) με 1600 hops/sec. Η επιλογή αυτής της τεχνολογίας έγινε γιατί σε αυτή την ελεύθερη μάντα θα λειτουργούν πολλά διαφορετικά συστήματα και θα πρέπει με κάποιο τρόπο να προστατεύονται οι επικοινωνίες από παρεμβολές. Επιπλέον, η διαμόρφωση είναι GFSK (Gaussian Frequency Shift Keying).

Επίπεδο Baseband

Το επίπεδο αυτό ουσιαστικά ελέγχει το επίπεδο ραδιοζεύξεων. Συγκεκριμένα, καθορίζει την ακολουθία των αλμάτων της συχνότητας (FH), πραγματοποιεί κρυπτογράφηση κατώτερου επιπέδου για ασφάλεια των ζεύξεων και διαχειρίζεται τα πακέτα δεδομένων όσον αφορά τον έλεγχο σφαλμάτων και την επαναμετάδοση τους. Επίσης, στο επίπεδο αυτό πραγματοποιούνται οι συνδέσεις και οι έλεγχοι των διευθύνσεων των γειτονικών συσκευών όπως θα δούμε σε επόμενη παράγραφο, που αναφέρεται στην εγκατάσταση συνδέσεων. Επιπρόσθετα, υποστηρίζονται δύο ειδών υπηρεσίες:

- Υπηρεσίες με Σύνδεση (SCO): Χρησιμοποιούνται για σύγχρονα δεδομένα όπως φωνή.
- Υπηρεσίες χωρίς Σύνδεση (ACL): Χρησιμοποιούνται για **εφαρμογές** μεταφοράς δεδομένων που δεν απαιτούν σύγχρονες ζεύξεις.

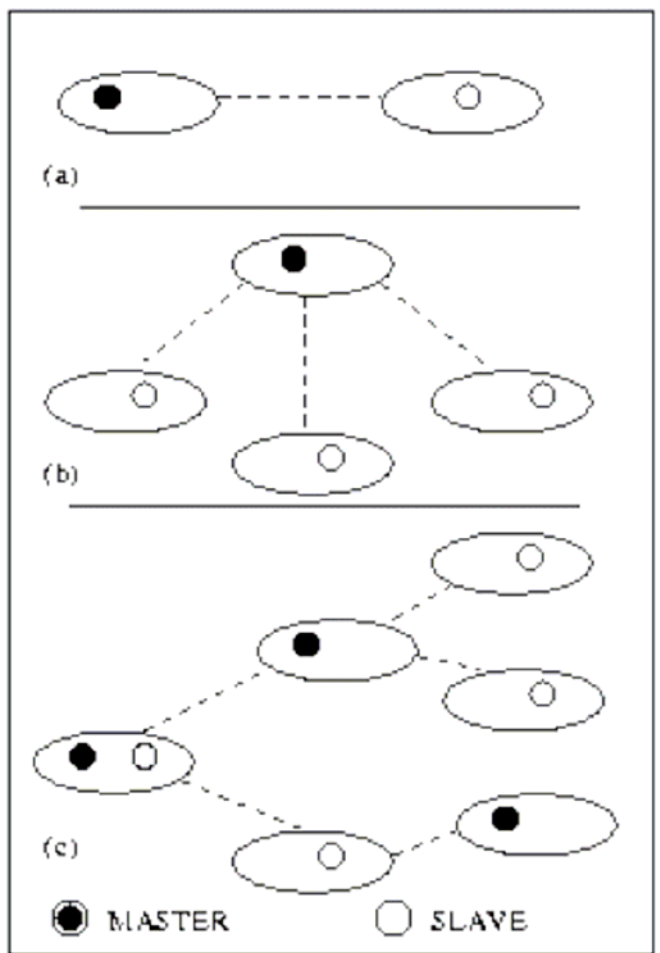
LMP (Link Manager Protocol)

Οι βασικότερες λειτουργίες του LMP κατατάσσονται ως εξής:

1. Διαχείριση των Piconets
2. Διαμόρφωση των Ζεύξεων
3. Λειτουργίες Ασφάλειας

Το piconet είναι ένα σύνολο συσκευών που συνδέονται σε ένα κοινό κανάλι και το οποίο αναγνωρίζεται από μια μοναδική ακολουθία αλμάτων στη συχνότητα. Η ακολουθία αυτή καθορίζεται από το εσωτερικό ρολόι του κόμβου που εκκίνησε τη δημιουργία του piconet (διαδικασία που θα αναλύσουμε στη συνέχεια) και αποκαλείται master. Με αυτό το master μπορούν να είναι συνδεδεμένες μέχρι επτά ενεργές συσκευές και μέχρι 255 συσκευές που θα βρίσκονται σε μια κατάσταση χαμηλής κατανάλωσης ισχύος που ονομάζεται “parked mode”. Οι κόμβοι εκτός του master ονομάζονται slaves. Οι συσκευές σε ένα piconet επικοινωνούν με τις υπόλοιπες μέσω του master χρησιμοποιώντας ζεύξεις SCO και ACL. Η διαχείριση του καναλιού γίνεται από το master και συγκεκριμένα χρησιμοποιείται σχήμα TDMA/TDD (Time Division Multiple Access / Time Division Duplex), όπου ο κάθε slave επικοινωνεί σε εναλλασσόμενες χρονοθυρίδες με το master, μόνο όταν του δίνει το δικαίωμα ο δεύτερος. Το συγκεκριμένο σύστημα μετάδοσης αναφέρεται και ως polling.

Για την επικοινωνία δύο οποιωνδήποτε συσκευών απαιτείται η δημιουργία ενός piconet. Τα piconets εγκαθίστανται δυναμικά και αυτόματα καθώς οι συσκευές Bluetooth εισέρχονται ή εξέρχονται από την κοινή περιοχή κάλυψης. Με βάση το παραπάνω σκεπτικό, κάποιες συσκευές μπορούν να ανήκουν ταυτόχρονα σε περισσότερα piconets οπότε έχουμε τη δημιουργία των λεγόμενων scatternets. Βέβαια, οι κόμβοι μπορούν να είναι slaves σε πολλά piconets, αλλά master μόνο σε ένα. Σχηματικά τα παραπάνω φαίνονται στη συνέχεια.



Εικόνα 8: Piconets – Scatternets

Το LMP δίνει τη δυνατότητα σύνδεσης και αποσύνδεσης των slaves, εναλλαγής των ρόλων μεταξύ ενός master και ενός slave και εγκατάστασης SCO και ACL ζευξέων. Επίσης, χειρίζεται τις καταστάσεις εξοικονόμησης ενέργειας - “hold”, “sniff”, “park” – που μπορούν να περιέλθουν οι συσκευές όταν δεν έχουν δεδομένα προς αποστολή.

Τα ζητήματα διαμόρφωσης ζευξέων περιλαμβάνουν τον καθορισμό των παραμέτρων της ζεύξης και θέματα QoS και ελέγχου ισχύος εκπομπής, αν υποστηρίζονται από τη συσκευή. Επίσης, πραγματοποιείται πιστοποίηση των συνδεδεμένων συσκευών και διαχείριση των απαραίτητων κλειδιών.

L2CAP (Logical Link Control and Adaptation Protocol)

Αυτό είναι το πρωτόκολλο με το οποίο αλληλεπιδρούν οι περισσότερες εφαρμογές. Οι βασικές λειτουργίες του είναι:

1. Πολυπλεξία: Επιτρέπει σε πολλές εφαρμογές να χρησιμοποιούν τη ζεύξη μεταξύ δύο συσκευών ταυτόχρονα.
2. Τμηματοποίηση και Επανένωση: Προσαρμόζει το μέγεθος των πακέτων των εφαρμογών σε αυτό που υποστηρίζεται από το επίπεδο baseband και αντίστροφα.

3. QoS: Ελέγχει αν είναι δυνατή η υποστήριξη από μια ζεύξη των απαιτήσεων σε παραμέτρους QoS (εύρος ζώνης, καθυστέρηση, διασπορά καθυστέρησης) που θέτουν οι ανώτερες εφαρμογές.

Ουσιαστικά το πρωτόκολλο L2CAP παρέχει τις λειτουργίες επιπέδου δικτύου (σύμφωνα με το OSI) στα ανώτερα πρωτόκολλα και τις εφαρμογές.

Επίπεδο Εφαρμογών

Το επίπεδο L2CAP χρησιμοποιείται όπως είδαμε είτε από εφαρμογές είτε από ανώτερα πρωτόκολλα. Τα σημαντικότερα από αυτά είναι τα παρακάτω:

- RFCOMM: Αποτελεί εξομοιωτή σειριακής θύρας
- SDP (Service Discovery Protocol): Επιτρέπει στις συσκευές να ανακαλύπτουν ποιες υπηρεσίες είναι διαθέσιμες στους γειτονικούς κόμβους
- TCS (Telephony Control Protocol): Περιγράφει τις διαδικασίες ελέγχου και σηματοδότησης για τα κανάλια φωνής.

Υπάρχουν, βέβαια, και άλλα ανώτερα πρωτόκολλα αλλά είναι γνωστά πρωτόκολλα που απλά έχουν εφαρμοστεί πάνω από την τεχνολογία Bluetooth και δεν θα τους δώσουμε περαιτέρω σημασία.

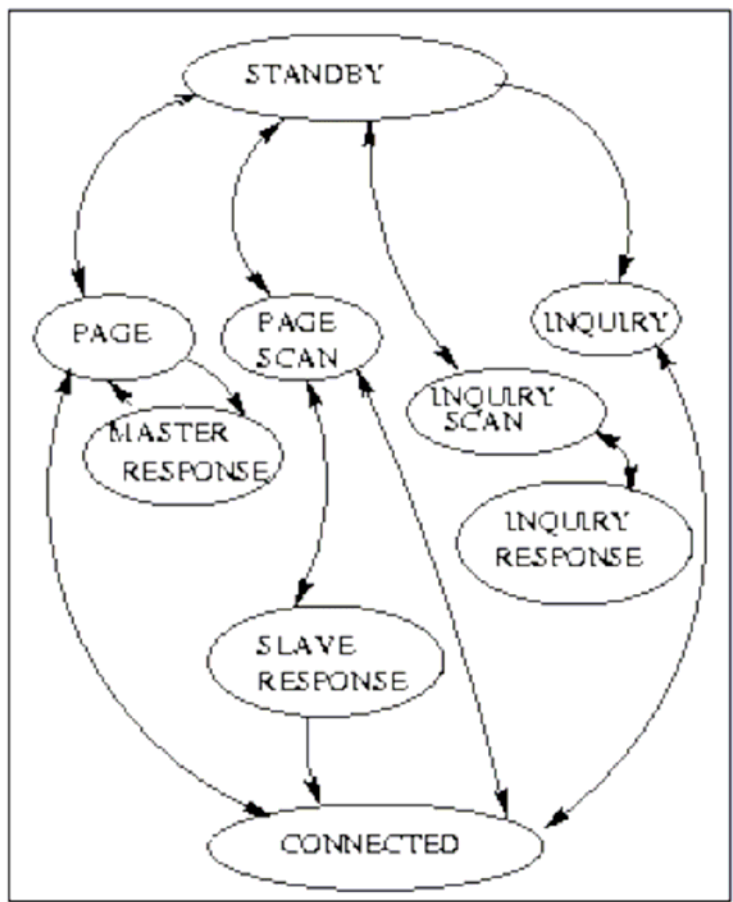
3.3.2. Εγκατάσταση Συνδέσεων

Η εγκατάσταση συνδέσεων στο Bluetooth όπως ήδη αναφέραμε, έχει να κάνει με τη δημιουργία piconets. Η όλη διαδικασία για τη δημιουργία ενός piconet μεταξύ δύο συσκευών – κόμβων μπορεί να περιγραφεί από μια εναλλαγή καταστάσεων στις οποίες περνάνε ακολουθιακά οι κόμβοι. Οι καταστάσεις αυτές φαίνονται στο σχήμα της επόμενης σελίδας και θα συνεχίσουμε δίνοντας μια σύντομη περιγραφή για κάθε μια από αυτές.

Κατ' αρχήν, κάθε συσκευή έχει ως default κατάσταση την κατάσταση Standby. Αυτή είναι μια κατάσταση ελάχιστης κατανάλωσης ενέργειας. Οι καταστάσεις στις οποίες μπορεί να μεταπηδήσει ένας κόμβος τότε, είναι οι Inquiry, Inquiry Scan, Page, ή Page Scan.

Inquiry

Σε αυτή την κατάσταση, η συσκευή προσπαθεί να εντοπίσει άλλες συσκευές που βρίσκονται στον περιβάλλοντα χώρο, μεταδίδοντας ένα κατάλληλο πακέτο σε συγκεκριμένες συχνότητες. Αν αυτή η διαδικασία γίνεται αυτόματα θα πρέπει να έχει ληφθεί μέριμνα ώστε να αποφευχθεί ο συγχρονισμός και κατ' επέκταση οι συγκρούσεις με τα αντίστοιχα πακέτα μια άλλης συσκευής.



Εικόνα 9: Διάγραμμα Καταστάσεων για τη Δημιουργία Piconets

Inquiry Scan

Σε αυτή την κατάσταση, οι συσκευές που επιτρέπουν την ανακάλυψη τους από τις υπόλοιπες, εισέρχονται περιοδικά, και μπορούν να ακούσουν για μηνύματα Inquiry στις αντίστοιχες συχνότητες. Οι συσκευές μπορούν να εισέλθουν σε αυτή την κατάσταση από την κατάσταση Inquiry ή από την κατάσταση Connected. Αν η είσοδος γίνεται από την τελευταία, οι ζεύξεις SCO παραμένουν, ενώ οι ACL διακόπτονται. Η παρουσία ζεύξεων SCO μπορεί να παρατείνει τη διάρκεια της διαδικασίας Inquiry.

Inquiry Response

Όταν ληφθεί ένα μήνυμα Inquiry, αποστέλλεται πίσω ένα μήνυμα που περιέχει τη διεύθυνση του κόμβου και στοιχεία του χρονισμού του. Τα στοιχεία αυτά αποθηκεύονται από τον κόμβο που εκκίνησε τη διαδικασία και θα χρησιμοποιηθούν όταν απαιτηθεί κάποια σύνδεση μεταξύ αυτών των δύο κόμβων. Μετά το τέλος αυτής της αρχικής διαδικασίας ο κάθε κόμβος έχει πληροφορίες για τις διευθύνσεις των γειτόνων του και όταν απαιτηθεί θα ξεκινήσει τη διαδικασία Page.

Page

Όπως είπαμε, ένας κόμβος που θα θελήσει να δημιουργήσει μια σύνδεση – αναλαμβάνει έτσι το ρόλο του master – θα περιέλθει στην κατάσταση Page. Ο master, θα αποστείλει ένα κατάλληλο μήνυμα σε προκαθορισμένες συχνότητες, ζητώντας να επικοινωνήσει με τον συγκεκριμένο κόμβο που επιθυμεί, του οποίου βέβαια γνωρίζει τη διεύθυνση. Η διαδικασία αυτή διαρκεί έως ότου ληφθεί μήνυμα Page Response, όπως θα δούμε παρακάτω.

Page Scan

Στην κατάσταση αυτή εισέρχονται περιοδικά οι συσκευές από τις καταστάσεις Standby και Connected. Ο slave ακούει στις κατάλληλες συχνότητες για πακέτα Page που φέρουν τη δική του διεύθυνση.

Page Response

Μετά τη λήψη ενός Page μηνύματος, ο slave εισέρχεται σε αυτή την κατάσταση. Σε περίπτωση αποδοχής της αίτησης του master για επικοινωνία, ο slave θα πρέπει να αποστείλει ένα κατάλληλο μήνυμα αποδοχής ώστε να περάσει και ο master στην ίδια κατάσταση. Τότε, ο master αποστέλλει ένα πακέτο το οποίο θα περιλαμβάνει πληροφορίες για το χρονισμό του και τη διεύθυνσή του, ώστε να μπορέσει ο slave να προσδιορίσει την ακολουθία των αλμάτων στη συχνότητα στην οποία θα πραγματοποιείται από εκείνη τη στιγμή και πέρα η επικοινωνία.

Μετά την επιτυχή ολοκλήρωση της όλης διαδικασίας, ουσιαστικά έχει δημιουργηθεί ένα piconet μεταξύ του master και του slave και οι συσκευές περνούν στην κατάσταση Connected, οπότε μπορούν να εγκαταστήσουν τις απαραίτητες για την επικοινωνία ζεύξεις.

Συμπεράσματα

Το HIPERLAN/2 και τα πρότυπα IEEE, αν και συγκρίσιμα στην ρυθμαπόδοση, διαφέρουν σε ορισμένα σημαντικά στοιχεία. Το HIPERLAN/2 υποστηρίζει μόνο ένα φυσικό επίπεδο ενώ το IEEE 802.11 υποστηρίζει πέντε. Το πλεονέκτημα του IEEE απέναντι στο HIPERLAN/2, σε αυτό το σημείο, παρουσιάζεται στο ότι είναι πιο επεκτάσιμο μέσω των πιο πρόσφατων φυσικών τεχνικών και ότι έχει ήδη δοκιμαστεί με κάποια φυσικά επίπεδα μέτριου ρυθμού. Στην πραγματικότητα, υπάρχουν, ήδη, προϊόντα διαθέσιμα για το πρότυπο IEEE 802.11 ενώ μέχρι τώρα, δεν υπάρχουν εμπορικά προϊόντα στην αγορά για το HIPERLAN/2, παρά μόνο σε ερευνητικό επίπεδο.

Η κύρια διαφορά στην τεχνική πρόσβασης στο μέσο επηρεάζει την προσέγγιση της διαχείρισης και τους τομείς των εφαρμογών.

Εξαιτίας της κυψελωτής δομής, ένα HIPERLAN/2 ad hoc δίκτυο φαίνεται να είναι πιο κατάλληλο για μικρά (ενός άλματος) δίκτυα μικρής περιοχής, ενώ η προσέγγιση του IEEE 802.11 καθιστά πιο εύκολη την αντιμετώπιση πολυαλματικών δικτύων. Η απευθείας κατανεμημένη προσέγγιση, από την άλλη πλευρά, μπορεί να περιορίσει την πυκνότητα των κόμβων στο IEEE περισσότερο από όσο στο HIPERLAN/2.

ΚΕΦΑΛΑΙΟ 4

ΑΣΦΑΛΕΙΑ

4.1 Τα Ad Hoc ασύρματα δίκτυα

Το όραμα της ενσωμάτωσης της ασύρματης συνδετικότητας ήταν στην ανάπτυξη για αρκετά έτη στα εργαστήρια Καίμπριτζ AT&T στα πλαίσια του προγράμματος Piconet και ακολουθούνται επίσης, αν και με έμφαση στις διαφορετικές πτυχές, από διάφορες άλλες ομάδες συμπεριλαμβανομένου HomeRF , IrDA (που χρησιμοποιεί τις υπέρυθρες ακτίνες αντί του ραδιοφώνου) και Bluetooth.

Ο καθένας- συμπεριλαμβανομένων των χρηστών- ξέρει ότι η ασύρματη δικτύωση είναι περισσότερη επιρρεπής σε παθητική φωνή κρυφακούοντας τις επιθέσεις. Αλλά θα ήταν ιδιαίτερα παραπλανητικό για να πάρει αυτό ως μόνο, ή ακόμα και κεντρικό αγωγό, ανησυχία ασφάλειας.

Σε αυτό το έγγραφο ερευνάμε τα ζητήματα ασφάλειας ενός περιβάλλοντος που χαρακτηρίζεται από την παρουσία πολλών προϊσταμένων που ενεργούν ως λόρδοι δικτύων σε διαλείπουσα επαφή η μια με την άλλη. Για να βασίσουμε τη συζήτηση σχετικά με ένα συγκεκριμένο παράδειγμα θα θεωρήσουμε έναν ασύρματο αισθητήρα θερμοκρασίας. Οι κοντινοί κόμβοι μπορούν να εγκριθούν για να ζητήσουν την τρέχουσα θερμοκρασία, ή για να καταχωρήσουν ένα “ ρολόι ” που θα αναγκάσει το θερμόμετρο για να στείλει μια ανάγνωση όταν εισάγει η θερμοκρασία μια συγκεκριμένη σειρά.

Επιθυμούμε να καταστήσουμε το θερμόμετρό μας χρήσιμο στο ευρύτερο φάσμα των περιβαλλόντων συμπεριλαμβανομένης της περιβαλλοντικής παρακολούθησης, του ελέγχου βιομηχανικής διεργασίας και της ιατρικής.

Επομένως θα εξετάσουμε πώς μπορούμε να επιτρέψουμε στο θερμόμετρό μας για να υποστηρίξουμε όλες τις ιδιότητες ασφάλειας που να απαιτηθούν, συμπεριλαμβανομένου της εμπιστευτικότητας, της ακεραιότητας (και της στενής σχετικής αυθεντικότητάς του) και της διαθεσιμότητας. Αντίθετο στην ακαδημαϊκή παράδοση, εντούτοις, θα τους εξετάσουμε στην αντίθετη διαταγή, όπως αυτό συχνά (και βεβαίως στην περίπτωσή μας) απεικονίζει την πραγματική σημασία τους. Κατ' αρχάς, εντούτοις, πρέπει να αναφέρουμε μερικούς από τους περιορισμούς των πόρων κάτω από τους οποίους τέτοια δίκτυα λειτουργούν.

4.2 Οι περιορισμοί συστημάτων

Οι τρεις κύριοι περιορισμοί σε Piconet, και στα παρόμοια συστήματα που υποστηρίζουν τα Ad Hoc δίκτυα των μπαταριών που χρησιμοποιούν προσωπικές συσκευές, είναι οι ακόλουθοι:

- **Peanut CPU:** η δύναμη υπολογισμού του επεξεργαστή στον κόμβο είναι χαρακτηριστικά μικρή, έτσι και οι μεγάλοι υπολογισμοί είναι αργοί.

- **Battery power:** η συνολική ενέργεια που είναι διαθέσιμη στον κόμβο είναι ένας λιγιστός πόρος. Ο κόμβος επιθυμεί να πάει στον ύπνο όποτε είναι δυνατόν. Δεν είναι επιθυμητό να χρησιμοποιηθεί ο χρόνος μη απασχόλησης για να εκτελεστούν οι μεγάλοι υπολογισμοί στο υπόβαθρο.
- **High latency:** για να συντηρήσουν τη δύναμη, οι κόμβοι τις περισσότερες φορές και μόνο ανοίγουν το δέκτη τους περιοδικά. Η επικοινωνία με τέτοιους κόμβους περιλαμβάνει την αναμονή έως ότου ξυπνούν έπειτα.

4.3. Η διαθεσιμότητα

Διαθεσιμότητα σημαίνει ότι η υπηρεσία που προσφέρεται από τον κόμβο θα είναι διαθέσιμη στους χρήστες της όταν αναμένεται. Στα περισσότερα μη στρατιωτικά σενάρια, αυτό είναι η ιδιοκτησία ασφάλειας της μέγιστης σχετικότητας για το χρήστη. Όλες οι άλλες μετρούν λίγο εάν η συσκευή δεν μπορεί να κάνει ότι πρέπει

4.3.1. Το ράδιο μπλοκάρισμα

Στο παραδοσιακό πρότυπο απειλής-προερχόμενος από τους στρατιωτικούς- ένας επιτιθέμενος μπορεί να αρνηθεί την υπηρεσία στους κόμβους σε μια δεδομένη περιοχή με το μπλοκάρισμα των ραδιοσυχνοτήτων που χρησιμοποιούν. Οι παραδοσιακές υπερασπίσεις περιλαμβάνουν hopping φάσματος και συχνότητας, και οι δύο από τις οποίες αναγκάζουν τον επιτιθέμενο να φράξουν μια ευρύτερη ζώνη συχνότητας και να χρησιμοποιήσουν έτσι περισσότερη ισχύ.

4.3.2. Εξαγωγή μπαταριών

Ο κακόβουλος χρήστης μπορεί να αλληλεπιδράσει με έναν κόμβο με έναν ειδικά νόμιμο τρόπο, αλλά για κανέναν άλλο σκοπό από το να καταναλώσει την ενέργεια μπαταριών του. Η ζωή μπαταριών είναι η κρίσιμη παράμετρος για πολλές φορητές συσκευές, και πολλές τεχνικές χρησιμοποιούνται για να το μεγιστοποιήσουν σε Piconet, παραδείγματος χάριν, οι κόμβοι προσπαθούν να ξοδέψουν τις περισσότερες φορές σε έναν τρόπο ύπνου στον οποίο αφουγκράζονται μόνο τα ράδιο σήματα πότε-πότε (η περίοδος μπορεί να τεθεί από μερικά δευτερόλεπτα σε αρκετά πρακτικά). Σε αυτό το περιβάλλον, δύναμη των επιθέσεων εξαγωγής είναι μια πραγματική απειλή, και είναι ισχυρότερες από την καλύτερη γνωστή άρνηση των υπηρεσιών απειλών όπως η εξαγωγή CPU. Μόλις τρέξει έξω η μπαταρία ο επιτιθέμενος μπορεί να σταματήσει και να περπατήσει μακριά, αφήνοντας το θύμα εκτός λειτουργίας. Καλούμε αυτήν την τεχνική επίθεση βασανιστηρίων στέρησης ύπνου. Για οποιοδήποτε δημόσιο κεντρικό υπολογιστή πρόσβασης, υπάρχει αναγκαστικά μια ένταση μεταξύ των αντιπαραβαλλόμενων στόχων χρήσιμο στους άγνωστους χρήστες και στους βανδάλους. Εκτιμώντας ότι μερικές εφαρμογές μπορούν να περιορίσουν την πρόσβαση στους γνωστούς προϊσταμένους, από την άλλη (όπως οι κεντρικοί υπολογιστές δικτύου και οι κεντρικοί υπολογιστές

ονόματος) αυτό είναι απραγματοποίητο δεδομένου ότι η ίδια η χρησιμότητα της υπηρεσίας προέρχεται από την ύπαρξή της, παγκοσμίως διαθέσιμη.

4.4. Η αυθεντικότητα

4.4.1. Παροδική Σύνδεση

Το νέο και ενδιαφέρον πρόβλημα επικύρωσης στα Ad Hoc δίκτυα των ασύρματων συσκευών είναι αυτό της ασφαλούς παροδικής ένωσης. Εάν ένας ιδιοκτήτης είναι κύριος μιας συσκευής, για παράδειγμα ένας καθολικός τηλεχειρισμός, ο οποίος αφήνει τον έλεγχό της σε διάφορες άλλες συσκευές στο σπίτι της (όπως hi-fi- και τηλεόρασης, το σύστημα θέρμανσης, φώτα, κουρτίνες και ακόμη και οι κλειδαριές και ο συναγερμός διαρρηκτών) έπειτα αυτή θα πρέπει να εξασφαλίσει ότι κάθε μια νέα συσκευή που αγοράζει από το κατάστημα θα υπακούει τις εντολές της, και όχι του γείτονά της. Θα θελήσει να βεβαιωθεί ότι ένας διαρρήκτης δεν μπορεί να αναλάβει τον αισθαμένος προβολέα θερμότητας στον κήπο, ή να ξεκλειδώσει την πίσω πόρτα, με την αποστολή μιας εντολής από έναν τηλεχειρισμό που αγοράζεται στο ίδιο κατάστημα.

Όπως και με την ύπαρξη ασφάλειας (οτιδήποτε αυτό σημαίνει), η ένωση μεταξύ του ελεγκτή και ο απομακρυσμένος πρέπει επίσης να είναι παροδικός. Όταν ένας ιδιοκτήτης μεταπωλεί ή δίνει μακριά την τηλεόραση ή το hi-fi ή το ψυγείο της, θα πρέπει να υπακούσει έναν άλλο ελεγκτή όταν ο ελεγκτής της παθαίνει βλάβη (ή αποφασίζει να το αντικαταστήσει ή να αναβαθμίσει το λειτουργικό σύστημά της), πρέπει να είναι σε θέση να επανακτήσει τον έλεγχο όλων των συσκευών όπου είναι κύρια ήδη.

Μια κεντρική υπηρεσία επικύρωσης είναι δυνατή για τα ακριβά καταναλωτικά διαρκή αγαθά, οι περισσότερες κυβερνήσεις τρέχουν τέτοιες υπηρεσίες για τα σπίτια και τα αυτοκίνητα. Αλλά δεν υπάρχει καμία προοπτική ότι αυτό θα επεκταθεί σε όλα τα ανθεκτικά καταναλωτικά αγαθά. Η βρετανική κυβέρνηση εγκατέλειψε το σκυλί εξουσιοδοτώντας μερικά έτη πριν όπως τα αντισυμβατικά. Εν πάση περιπτώσει, θα υπήρχαν πολύ σοβαρές αστικές αντιρρήσεις ελευθεριών στην κυβέρνηση που διατηρεί τους καταλόγους όλων των PCs, hi-fi και DVD στη χώρα. Η κατακραυγή πέρα από το Pentium III ταυτότητας επεξεργαστών δείχνει το πιθανό επίπεδο πολιτικής αντίστασης. Ακόμη και οι υπάρχουσες κεντρικές υπηρεσίες σταματούν λίγο πριν από τη διαχείριση των κλειδιών. Η αντικατάσταση των κλειδιών αυτοκινήτων αφήνεται στο εμπόριο μηχανών, ενώ οι κλειδαριές σπιτιών είναι απολύτως ανεξέλεγκτες. Έτσι είναι επιθυμητό να εκτελεστεί τοπικά η βασική διαχείριση: το τελευταίο πράγμα που θέλουμε να επιβάλουμε είναι μια ακριβή και μη δημοφιλή κεντρική λύση. Ακόμα θα ήταν συμπαθητικό εάν θα μπορούσαμε να παρέχουμε μερικά μέσα που κάνουν έναν κλεμμένο φορέα DVD δυσκολότερο να μεταπωληθεί.

Μια άλλη διορατικότητα προέρχεται από τα σενάρια όπου έχουμε μια ομάδα των ίδιων συσκευών, όπως ένα κύπελλο του απολυμαντικού που περιέχει δέκα θερμόμετρα. Ο γιατρός δεν φροντίζει πραγματικά ποιο θερμόμετρο παίρνει όταν επιλέγει ένα, αλλά φροντίζει ότι το palmtop της είναι το ίδιο που κρατά και όχι οποιοδήποτε άλλο στο κοντινό θάλαμο.

4.4.2. Πολιτική ασφάλειας

Μια μεταφορά που εμπνέεται ένωση από τη βιολογία θα μας βοηθήσει να περιγράψουμε τη συμπεριφορά μιας συσκευής που εφαρμόζει κατάλληλα την ασφαλή παροδική ένωση.

Ένας νεοσσός που προκύπτει από το αυγό του θα αναγνωρίσει ως μητέρα του το πρώτο κινούμενο αντικείμενο που βλέπει και κάνει έναν ήχο, ανεξάρτητα από αυτό που μοιάζει: αυτό το φαινόμενο καλείται αποτύπωση. Ομοίως, η συσκευή μας (το της οποίας αυγό είναι το στενέψτε- τυλίζτε κιβώτιο που το εσωκλείει καθώς βγαίνει από το εργοστάσιο) θα αναγνωρίσει ως ιδιοκτήτη της την πρώτη οντότητα που του στέλνει ένα μυστικό κλειδί. Μόλις αυτό το "κλειδί ανάφλεξης" παραλαμβάνεται, η συσκευή δεν είναι πλέον νεογέννητη και θα μείνει πιστή στον ιδιοκτήτη της για το υπόλοιπο της ζωής της. Εάν διάφορες οντότητες είναι παρούσες στη γέννηση της συσκευής, κατόπιν ο πρώτος που του στέλνει ένα κλειδί γίνεται ο ιδιοκτήτης: για να χρησιμοποιήσει μια άλλη βιολογική μεταφορά, μόνο το πρώτο σπέρμα παίρνει να λιπάνει το αυγό.

Μπορούμε να δούμε το υλικό της συσκευής ως σώμα, και το λογισμικό (ιδιαίτερα το κράτος) ως ψυχή. Εφ' όσον μένει η ψυχή στο σώμα, ο νεοσσός παραμένει ζωντανός και συνδεδεμένος στην ίδια μητέρα στον οποίο αποτυπώθηκε. Αλλά αυτόν τον δεσμό σπάζει ο θάνατος: κατά συνέπεια, η ψυχή διαλύεται και οι επιστροφές σωμάτων στο κράτος προ-γέννησής της, μαζί με το νεοσσό ανάστασης αναμένουν μια άλλη αποτύπωση που θα αρχίσει μια νέα ζωή με μια άλλη ψυχή. Ο θάνατος είναι το μόνο γεγονός που επιστρέφει μια ζωντανή συσκευή στο κράτος προ-γέννησής στο οποίο θα δεχτεί μια αποτύπωση. Καλούμε αυτήν την διαδικασία αντίστροφη μετεμψύχωση.

4.5. Η ακεραιότητα

Ακεραιότητα σημαίνει ότι τον κόμβο δεν τον έχουν αλλάξει κακόβουλα. Ο παραλήπτης θέλει να είναι βέβαιος ότι οι μετρήσεις προέρχονται από το γνήσιο θερμόμετρο και όχι από έναν κόμβο που έχει τροποποιηθεί και να στείλει τις ανακριβείς τιμές θερμοκρασίας (η εφαρμογή να μην είναι μετεωρολογία ή ιατρική, αλλά ένα σύστημα προειδοποίησης συναγερμών πυρκαγιάς).

Το πρότυπο απειλής εδώ υποθέτει ότι ο αισθαμένος κόμβος μπορεί να αφεθεί αφύλακτος για τις μακριές χρονικές περιόδους και ότι, σύντομα ή αργότερα, ένας επιτιθέμενος θα το επιλέξει, θα βρωμίσει γύρω με τα internals του και θα το βάλει πίσω όπου ήταν. Ένας νόμιμος κόμβος μπορεί έπειτα να καταλήξει άγνωστος να πραγματοποιήσει συναλλαγές κακόβουλα. Αυτό μπορεί θεωρητικά να αποφευχθεί με το να καταστήσει τους κόμβους μη παραποιήσιμους, αλλά είναι πολύ ευκολότερο να μιλήσει για αυτήν την ιδιοκτησία από το να εφαρμοστεί στην πράξη, ειδικά μέσα στους περιορισμούς στους παράγοντες δαπανών και μορφής των προσωπικών συσκευών ηλεκτρονικών ειδών ευρείας κατανάλωσης. Κάτω από τις περιστάσεις, δεν είναι σαφές εάν οποιαδήποτε πρόσθετη διαβεβαίωση δίνεται με τον εφοδιασμό του θερμομέτρου μας με τη δυνατότητα να γίνει το δημόσιο βασικό σύστημα κρυπτογραφίας. Μια τέτοια συσκευή μπορεί να έχει το

ιδιωτικό κλειδί της να διαβάσει ακριβώς ως συσκευή με ένα πιστοποιητικό. Σε τέτοια περιβάλλοντα μπορεί συχνά να είναι καταλληλότερο να χρησιμοποιηθούν οι μηχανισμοί πλαστογράφησης στοιχείων (όπως οι σφραγίδες) παρά ακριβότερες πλαστογραφήσεις ενισχύοντας (όπως οι αισθαμένοι διακόπτες που σβήνουν τη μνήμη). Σε αυτήν την περίπτωση, κάποιος πρέπει ακόμα να σχεδιάσει τη συσκευή έτσι ώστε οι μη-παρεισφρητικές επιθέσεις (όπως εκείνοι βασισμένοι στη διακοπή πρωτοκόλλου, την ανάλυση ρεύματος και τις επιθέσεις δυσλειτουργίας) δεν είναι πρακτικές, είναι επίσης απαραίτητο να ληφθεί υπόψη ο χρόνος που θα περάσει προτού να παρατηρηθεί μια σπασμένη σφραγίδα, και η πιθανότητα των επιτυχών επιθέσεων στο σφραγίζοντας μηχανισμό. Πρέπει επίσης να συνειδητοποιηθεί ότι δεν μπορεί να περιοριστεί στον εν πλω κώδικα και τα κλειδιά: μια πολύ αποτελεσματική επίθεση στο αφύλακτο θερμόμετρο είναι να αντικατασταθεί απλά το αναλογικό αισθαμένος στοιχείο της με ένα κακό. Αυτή η επίθεση τονίζει ότι ακόμη και εσωκλείοντας ολόκληρο τον επεξεργαστή, τη μνήμη και τη εφεδρική μπαταρία αρίστης ποιότητας σε μια ανθεκτική περίφραξη πλαστογραφήσεων, με μόνο έναν συνδετήρα κορδελών για να το διασυνδέσουν με τον εξωτερικό κόσμο, θα μας άφηναν ακόμα τρωτούς στις άμεσες επιθέσεις "στις περιφερειακές μονάδες της".

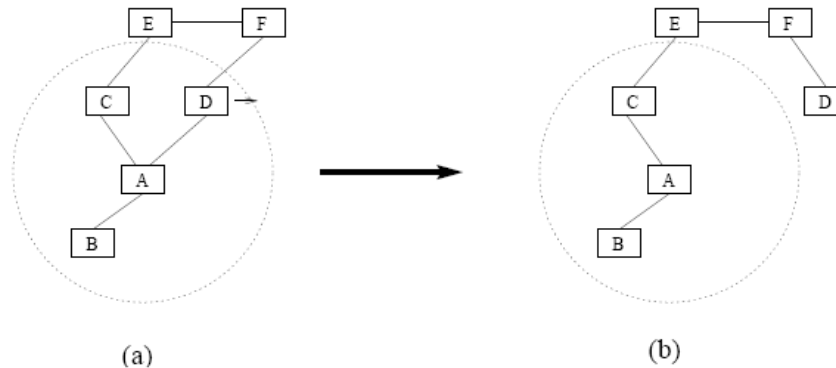
Να φέρει ο ίδιος τον αισθητήρα μέσα στην ανθεκτική περίφραξη πλαστογραφήσεων μπορεί να καταστήσει την κατασκευή πάρα πολύ ακριβή (ο πυρήνας υπολογισμού και επικοινωνίας δεν είναι πλέον μια μορφωματική δομική μονάδα) και μπορεί ακόμη και να παρεμποδίσει την κατάλληλη εργασία του αισθητήρα. Έτσι ο μετατροπέας μπορεί να μην αξίζει τα μεγάλα ποσά να πλαστογραφήσει-ενισχύσει τον πυρήνα εάν ο αισθητήρας δεν μπορεί οικονομικά να προστατευθεί.

4.6. Τα Ad Hoc δίκτυα παρέχουν την ασύρματη επικοινωνία στους κινητούς hosts (που καλούμε κόμβους).

Σε ένα Ad Hoc δίκτυο, δεν υπάρχει καμία σταθερή υποδομή όπως οι σταθμοί βάσεων ή τα κινητά κέντρα μετατροπής. Οι κινητοί κόμβοι που είναι μέσα μεταξύ τους σε ράδιο σειρά επικοινωνούν άμεσα μέσω των ασύρματων συνδέσεων, ενώ εκείνοι που είναι μακριά, χώρια, στηρίζονται σε άλλους κόμβους στα μηνύματα ηλεκτρονικών ως δρομολογητές. Η κινητικότητα κόμβων σε ένα Ad Hoc δίκτυο προκαλεί τις συχνές αλλαγές της τοπολογίας δικτύων. Η Εικόνα 1 παρουσιάζει ένα τέτοιο παράδειγμα: αρχικά, οι κόμβοι A και D έχουν μια άμεση σύνδεση μεταξύ τους. Όταν το D κινείται από τη ράδιο σειρά του A, η σύνδεση είναι σπασμένη. Εντούτοις, το δίκτυο συνδέεται ακόμα, επειδή το A μπορεί να φθάσει στο D μέσω του C, E, και F. οι Στρατιωτικές τακτικές διαδικασίες είναι ακόμα η κύρια εφαρμογή των ειδικών δικτύων σήμερα. Παραδείγματος χάριν, οι στρατιωτικές μονάδες (π.χ., στρατιώτες, δεξαμενές, ή αεροπλάνα), που εξοπλίστηκαν με τις ασύρματες συσκευές επικοινωνίας, θα μπορούσαν να διαμορφώσουν ένα Ad Hoc δίκτυο όταν περιπλανώνται σε ένα πεδίο μάχης. Τα ad hoc δίκτυα μπορούν επίσης να χρησιμοποιηθούν για την έκτακτη ανάγκη, την επιβολή νόμου, και τις αποστολές διάσωσης. Δεδομένου ότι ένα Ad Hoc δίκτυο μπορεί να επεκταθεί γρήγορα με το σχετικά χαμηλότερο κόστος, γίνεται μια ελκυστική επιλογή για τις εμπορικές χρήσεις όπως τα δίκτυα αισθητήρων ή οι ιδεατές τάξεις.

4.6.1. Η ασφάλεια

Ασφάλεια είναι ένα σημαντικό ζήτημα για τα Ad Hoc δίκτυα, ειδικά για εκείνες τις ασφαλείς -ευαίσθητες εφαρμογές. Για να εξασφαλίσει ένα Ad Hoc δίκτυο, θεωρούμε τις ακόλουθες ιδιότητες: διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, επικύρωση, και μη- αποκήρυξη.



Εικόνα 1:Αλλαγή τοπολογίας στα Ad Hoc δίκτυα: οι κόμβοι A, B, C, D, E, και F αποτελούν ένα Ad Hoc δίκτυο. Ο κύκλος αντιπροσωπεύει τη ράδιο σειρά του κόμβου A. Το δίκτυο έχει αρχικά την τοπολογία σε (α). Όταν ο κόμβος D κινείται από τη ράδιο σειρά του A, η τοπολογία δικτύων αλλάζει σε αυτή σε (β).

- Η διαθεσιμότητα εξασφαλίζει την ικανότητα επιβίωσης των δικτυακών υπηρεσιών παρά την άρνηση των υπηρεσιακών επιθέσεων. Μια άρνηση της επίθεσης υπηρεσιών θα μπορούσε να προωθηθεί σε οποιοδήποτε στρώμα ενός ειδικού δικτύου. Στα στρώματα ελέγχου φυσικής και πρόσβασης μέσων, ένας αντίπαλος θα μπορούσε να υιοθετήσει το μπλοκάρισμα για να παρεμποδίσει την ανακοίνωση σχετικά με τα φυσικά κανάλια. Στο στρώμα δικτύων, ένας αντίπαλος θα μπορούσε να αναστατώσει το πρωτόκολλο δρομολόγησης και να αποσυνδέσει το δίκτυο. Στα υψηλότερα στρώματα, ένας αντίπαλος θα μπορούσε να ρίξει τις υψηλού επιπέδου υπηρεσίες. Ένας τέτοιος στόχος είναι η βασική διοικητική υπηρεσία, μια ουσιαστική υπηρεσία για οποιοδήποτε πλαίσιο ασφάλειας.
- Η εμπιστευτικότητα εξασφαλίζει ότι ορισμένες πληροφορίες δεν αποκαλύπτονται ποτέ στις αναρμόδιες οντότητες. Η μετάδοση δικτύων ευαίσθητων πληροφοριών, όπως οι στρατηγικές ή στρατιωτικές πληροφορίες τακτικής, απαιτεί την εμπιστευτικότητα. Η διαρροή τέτοιων πληροφοριών στους εχθρούς θα μπορούσε να έχει καταστρεπτικές συνέπειες. Οι πληροφορίες δρομολόγησης πρέπει επίσης να παραμείνουν εμπιστευτικές σε ορισμένες περιπτώσεις, επειδή οι πληροφορίες μπορεί να είναι χρήσιμες για τους εχθρούς και μπορούν να προσδιορίσουν και να εντοπίσουν τους στόχους τους σε ένα πεδίο μάχης.

- Η ακεραιότητα εγγυάται ότι ένα μήνυμα που μεταφέρεται δεν αλλοιώνεται ποτέ. Ένα μήνυμα θα μπορούσε να αλλοιωθεί λόγω των καλοκάγαθων αποτυχιών, όπως η ράδιο εξασθένιση διάδοσης, ή λόγω των κακόβουλων επιθέσεων στο δίκτυο.
- Η επικύρωση επιτρέπει σε έναν κόμβο για να εξασφαλίσει την ταυτότητα του όμοιου κόμβου που επικοινωνεί. Χωρίς επικύρωση, ένας αντίπαλος θα μπορούσε να μεταμφιέσει έναν κόμβο, κερδίζοντας κατά συνέπεια την αναρμόδια πρόσβαση στον πόρο και τις ευαίσθητες πληροφορίες και παρεμποδίζοντας τη λειτουργία άλλων κόμβων.
- Τέλος, η μη- αποκήρυξη εξασφαλίζει ότι η προέλευση ενός μηνύματος δεν μπορεί να αρνηθεί την αποστολή του μηνύματος. Η μη-αποκήρυξη είναι χρήσιμη για την ανίχνευση και την απομόνωση των συμβιβασμένων κόμβων. Όταν ένας κόμβος Α λαμβάνει ένα λανθασμένο μήνυμα από έναν κόμβο Β, η μη-αποκήρυξη επιτρέπει στο Α να κατηγορήσει το Β χρησιμοποιώντας αυτό το μήνυμα και για να πείσει άλλους κόμβους ότι το Β συμβιβάζεται. Υπάρχουν άλλοι στόχοι ασφάλειας (π.χ., έγκριση) που είναι υπόθεση ορισμένων εφαρμογών, αλλά δεν θα ακολουθήσουμε αυτά τα ζητήματα σε αυτό το έγγραφο.

4.6.2. Οι προκλήσεις

Τα εμφανή χαρακτηριστικά γνωρίσματα των ειδικών δικτύων θέτουν και τις προκλήσεις και τις ευκαιρίες στην επίτευξη αυτών των στόχων ασφάλειας.

- Κατ' αρχάς, η χρήση των ασύρματων συνδέσεων καθιστά ένα Ad Hoc δίκτυο ευαίσθητο στις επιθέσεις συνδέσεων που κυμαίνονται από το ενεργητικό κρυφακούοντας στην ενεργό προσωποποίηση, την επανάληψη μηνυμάτων, και τη διαστρέβλωση μηνυμάτων. Να κρυφακούσει να δώσει μια αντίπαλη πρόσβαση στις μυστικές πληροφορίες, που παραβιάζουν την εμπιστευτικότητα. Οι ενεργές επιθέσεις να επιτρέψουν στον αντίπαλο να διαγράψουν τα μηνύματα, να εγχύσουν τα λανθασμένα μηνύματα, να τροποποιήσουν τα μηνύματα, παραβιάζοντας κατά συνέπεια τη διαθεσιμότητα, την ακεραιότητα, την επικύρωση, και την μη-αποκήρυξη.
- Αφετέρου, οι κόμβοι, που περιπλανώνται σε ένα εχθρικό περιβάλλον (π.χ., ένα πεδίο μάχη) με τη σχετικά φτωχή φυσική προστασία, έχουν την μη-αμελητέα πιθανότητα του συμβιβασμού. Επομένως, πρέπει όχι μόνο να εξετάσουμε τις κακόβουλες επιθέσεις από έξω από ένα δίκτυο, αλλά και να λάβουμε υπόψη τις επιθέσεις που προωθούνται από μέσα από το δίκτυο από τους συμβιβασμένους κόμβους. Επομένως, για να επιτύχουν την υψηλή ικανότητα επιβίωσης, τα Ad Hoc δίκτυα πρέπει να έχουν μια διανεμημένη αρχιτεκτονική χωρίς τις κεντρικές οντότητες. Η εισαγωγή οποιασδήποτε κεντρικής οντότητας στη λύση ασφάλειάς μας θα μπορούσε να οδηγήσει στη σημαντική ευπάθεια δηλαδή εάν αυτή η

συγκεντρωμένη οντότητα συμβιβάζεται, κατόπιν το ολόκληρο δίκτυο υπονομεύεται.

- Τρίτον, ένα Ad Hoc δίκτυο είναι δυναμικό λόγω των συχνών αλλαγών και στην τοπολογία του και στην ιδιότητα μέλους του (δηλ., οι κόμβοι ενώνουν συχνά και αφήνουν το δίκτυο). Η σχέση εμπιστοσύνης μεταξύ των κόμβων αλλάζει επίσης, παραδείγματος χάριν, όταν ανιχνεύονται ορισμένοι κόμβοι όταν είναι συμβιβασμένοι. Αντίθετα από άλλα ασύρματα κινητά δίκτυα, όπως η κινητή IP, οι κόμβοι σε ένα Ad Hoc δίκτυο μπορούν δυναμικά να γίνουν συνδεδεμένοι με τις διοικητικές περιοχές. Οποιαδήποτε λύση ασφάλειας με μια στατική διαμόρφωση δεν θα αρκούσε. Είναι επιθυμητό για τους μηχανισμούς ασφάλειάς μας να προσαρμοστεί σε ώρα πτήσης σε αυτές τις αλλαγές. Τέλος, ένα Ad Hoc δίκτυο μπορεί να αποτελείτε από εκατοντάδες ή ακόμα και χιλιάδες κόμβους. Οι μηχανισμοί ασφάλειας πρέπει να είναι εξελικτικοί για να χειριστούν ένα τέτοιο μεγάλο δίκτυο.

Το πεδίο και οι παραδοσιακοί μηχανισμοί ασφάλειας, όπως τα πρωτόκολλα επικύρωσης, η ψηφιακή υπογραφή, και η κρυπτογράφηση, διαδραματίζουν ακόμα τους σημαντικούς ρόλους στην επίτευξη της εμπιστευτικότητας, της ακεραιότητας, της επικύρωσης, και της μη- αποκήρυξης της επικοινωνίας στα Ad Hoc δίκτυα. Εντούτοις, αυτοί οι μηχανισμοί δεν είναι ικανοποιητικοί μόνοι τους. Στηριζόμαστε περαιτέρω στις ακόλουθες δύο αρχές. Κατ' αρχάς, εκμεταλλευόμαστε τους πλεονασμούς στην τοπολογία δικτύων (δηλ., πολλαπλάσιες διαδρομές μεταξύ των κόμβων) για να επιτύχουμε τη διαθεσιμότητα. Η δεύτερη αρχή είναι διανομή της εμπιστοσύνης. Αν και ούτε ένας κόμβος δεν είναι αξιόπιστος σε ένα Ad Hoc δίκτυο λόγω της χαμηλών φυσικών ασφάλειας και της διαθεσιμότητας, μπορούμε να διανείμουμε την εμπιστοσύνη σε μια συνάθροιση των κόμβων..

4.7. Εμπιστοσύνη και βασική διανεμημένη διαχείριση

4.7.1. Εμπιστοσύνη στα Ad Hoc δίκτυα

Προτείνουμε ένα παράδειγμα ασφάλειας που στρέφεται γύρω από την έννοια της διανεμημένης εμπιστοσύνης για τα Ad Hoc δίκτυα. Η διανεμημένη εμπιστοσύνη ενισχύει την ασφάλεια με τη σύνθεση των ανέμπιστων μεμονωμένων οντοτήτων σε μια αξιόπιστη συνάθροιση, μια που παραμένει διαθέσιμη και σωστή ακόμα κι αν μερικές από τις οντότητές της αποτυγχάνουν ή γίνονται συμβιβασμένες. Η πρόκληση της κατασκευής μιας τέτοιας αξιόπιστης συνάθροισης βρίσκεται όχι μόνο στο πώς να δημιουργήσει και να διαμορφώσει τη συνάθροιση, αλλά και στο πώς η συνάθροιση διατηρεί την ασφάλειά της με το να προσαρμοστεί στις αλλαγές στην τοπολογία δικτύων και το περιβάλλον, καθώς επίσης και στους συμβιβασμούς των μεμονωμένων οντοτήτων. Καταδεικνύουμε πώς εφαρμόζουμε τη διανεμημένη εμπιστοσύνη στην οικοδόμηση των ασφαλών υπηρεσιών και στην ασφαλή δρομολόγηση.

Διανεμημένες ασφαλείς υπηρεσίες : Για μια ασφαλή-ευαίσθητη υπηρεσία, όπως μια αρχή πιστοποίησης, διανέμουν συνηγόρους εμπιστοσύνης που παρέχουν την υπηρεσία μέσω ενός συνόλου κόμβων ως κεντρικούς υπολογιστές, έτσι ώστε η υπηρεσία παραμένει διαθέσιμη και σωστή ακόμα κι αν ένας μικρός αριθμός κεντρικών υπολογιστών γίνεται συμβιβασμένος. Οι μηχανισμοί ανοχής ελαττωμάτων, όπως τα αναδιπλωμένα συστήματα προσέγγισης και απαρτίας statemachine, έχουν αποδειχθεί αποτελεσματικοί ενάντια στις αποτυχίες κεντρικών υπολογιστών. Εντούτοις, η αντένσταση ενός μυστικού στους κεντρικούς υπολογιστές αυξάνει την πιθανότητα της κοινοποίησης επειδή ο συμβιβασμός οποιουδήποτε κεντρικού υπολογιστή εκθέτει το μυστικό. Η λύση είναι εδώ μυστική διανομή. Ένα μυστικό σχέδιο διανομής επιτρέπει στους κεντρικούς υπολογιστές για να αποθηκεύσει τις μετοχές ενός μυστικού, έτσι ώστε το μυστικό μπορεί να ανακτηθεί εάν και μόνο εάν αρκετές μετοχές λαμβάνεται από τους κεντρικούς υπολογιστές. Το σύστημα κρυπτογραφίας κατώτατων ορίων μπορεί να χρησιμοποιηθεί για τους κεντρικούς υπολογιστές για να εκτελέσει την υπογραφή και την αποκρυπτογράφηση όταν το μυστικό είναι ένα ιδιωτικό κλειδί. Η μυστική διανομή μόνο δεν υπερασπίζει ενάντια στους κινητούς αντιπάλους, τα οποία επιτίθενται, συμβιβάζουν, και ελέγχουν σε έναν κεντρικό υπολογιστή για μια περιορισμένη περίοδο πριν κινηθούν προς τον επόμενο. Κατά τη διάρκεια του χρόνου, ένας κινητός αντίπαλος θα μπορούσε να συμβιβάσει αρκετούς κεντρικούς υπολογιστές και να ανακτήσει το μυστικό.

Μοιραστείτε την αναζωογόνηση : όπου οι κεντρικοί υπολογιστές δημιουργούν ένα νέο, ανεξάρτητο σύνολο μετοχών και αντικαθιστούν τις παλαιές μετοχές με τις νέες, παρέχει μια υπεράσπιση στους κινητούς αντιπάλους. Επειδή οι νέες μετοχές δεν μπορούν να συνδυαστούν με παλαιές για να ανακτήσουν το μυστικό, ένας κινητός αντίπαλος πρέπει να συμβιβάσει αρκετούς κεντρικούς υπολογιστές μεταξύ δύο διαδοχικών εκτελέσεων της αναζωογόνησης μεριδίου. Η αναζωογόνηση μεριδίου μπορεί να γενικευτεί για τις νέες μετοχές που ανακατανέμονται σε ένα διαφορετικό σύνολο κεντρικών υπολογιστών με μια ενδεχομένως διαφορετική διαμόρφωση. Τέτοια γενίκευση επιτρέπει σε μια υπηρεσία να προσαρμοστεί όταν συμβιβάζονται μόνιμα ορισμένοι κεντρικοί υπολογιστές ή όταν αντιμετωπίζει η υπηρεσία ένα πιο κακόβουλο περιβάλλον. Η δυνατότητα μιας τέτοιας ασφαλούς διανεμημένης υπηρεσίας έχει καταδειχθεί για τα δίκτυα όπως το internet. Τα εμπόδια στην ανάπτυξη μιας τέτοιας υπηρεσίας σε ένα Ad Hoc δίκτυο προέρχονται όχι μόνο από την έλλειψη των πόρων υπολογισμού και επικοινωνίας σε ένα Ad Hoc δίκτυο, αλλά και από την έλλειψη ασφαλούς υποδομής δικτύων. Το τελευταίο πρόβλημα εξετάζεται με την ασφαλή δρομολόγηση.

Εξασφαλίστε τη δρομολόγηση : Εξασφαλίστε ότι η δρομολόγηση ενδιαφέρεται για τη διατήρηση της συνδετικότητας σε ένα Ad Hoc δίκτυο παρά τους συμβιβασμένους κόμβους που αναστατώνουν την ανακάλυψη διαδρομών και τη μετάδοση μηνυμάτων. Μετά από τη φιλοσοφία της διανεμημένης εμπιστοσύνης, πολλαπλάσια (ιδανικά χωρίστε) οι πορείες μεταξύ δύο κόμβων πρέπει να ανακαλυφθούν και να διατηρηθούν έτσι ώστε ένας μικρός αριθμός συμβιβασμένων κόμβων δεν μπορεί να αναστατώσει όλες τις πορείες. Πιστεύουμε ότι η ανακάλυψη διαδρομών πρέπει να συνδεθεί με τη μετάδοση μηνυμάτων, επειδή, διαφορετικά, ακόμη και με ένα ασφαλές πρωτόκολλο ανακαλύψεων διαδρομών που αποτρέπει τους συμβιβασμένους κόμβους από την εξαπάτηση, ένας συμβιβασμένος κόμβος μπόρεσε να συνεργαστεί κατά τη διάρκεια της ανακάλυψης

διαδρομών, αλλά συμπεριφέρεται απρεπώς κατά τη διάρκεια της μετάδοσης μηνυμάτων εάν ο κόμβος συμβαίνει να είναι στην ανακαλυμμένη πορεία. Προτείνουμε έτσι ένα πιθανολογικό ασφαλές σχέδιο δρομολόγησης, όπου ένας κόμβος διατηρεί, για κάθε πιθανό προορισμό, μια διανομή πιθανότητας σε όλους τους γείτονές του. Η πιθανότητα που συνδέεται με έναν γείτονα απεικονίζει τη σχετική πιθανότητα εκείνου του γείτονα που διαβιβάζει και τελικά που παραδίδει ένα μήνυμα στον προορισμό. Κάθε μήνυμα καθοδηγείται σε κάθε λυκίσκο βασισμένο στη διανομή πιθανότητας για τον προορισμό. Οι πολλαπλάσιες πορείες έτσι σιωπηρά διατηρούνται μέσω των διανομών πιθανότητας. Η μετάδοση μηνυμάτων παρέχει την ανατροφοδότηση για τους κόμβους για να ρυθμίσει τις διανομές πιθανότητας. Παραδείγματος χάριν, μια αναγνώριση, της οποίας η ακεραιότητα προστατεύεται κρυπτογραφικά (π.χ., από μια ψηφιακή υπογραφή), της παραλαβής ενός μηνύματος παρέχει μια θετική ανατροφοδότηση για την πορεία μέσω της οποίας το μήνυμα διαπέρασε. Συνεπώς, το σύνολο πολλαπλάσιων πορειών που διατηρείται από το σχέδιο δρομολόγησης για οποιουδήποτε δύο κόμβους προσαρμόζεται καθώς οι διανομές πιθανότητας αλλάζουν. Αν και τα πιθανολογικά σχέδια δρομολόγησης έχουν μελετηθεί στη νοημοσύνη σμηνών, η εφαρμογή για να εξασφαλιστεί η δρομολόγηση προκύπτει τα διάφορα νέα ζητήματα, όπως το πώς να εξασφαλίσει την ακεραιότητα των ανατροφοδοτήσεων παρά τους συμβιβασμένους κόμβους χωρίς υπερβολικές δαπάνες. Και η ανάλυση και τα πειράματα με τέτοια σχέδια απαιτούνται επίσης για να καθιερώσουν την πρακτικότητά τους.

4.8. Το σύστημα & ο αντίπαλος

Αυτή την εργασία εξετάζουν ένα Ad Hoc ασύρματο δίκτυο, όπου οι κινητοί κόμβοι επικοινωνούν με ένα άλλο, μέσω του εύρους ζώνης-περιορισμένου, επιρρεπούς σε λάθη, και επισφαλούς ασύρματου καναλιού. Υποθέτουμε τους κινητούς κόμβους v , και το v μπορεί δυναμικά να αλλάζει καθώς οι κινητοί κόμβοι ενώνονται, φεύγουν, ή αποτυγχάνουν κατά τη διάρκεια του χρόνου. Εκτός αυτού, το v δεν περιορίζεται δεδομένου ότι μπορεί να υπάρξει ένας μεγάλος πληθυσμός συσκευών. Το δίκτυο δεν παρέχει ούτε τη φυσική ούτε λογική υποστήριξη υποδομής, και η αξιοπιστία της αποστολής πακέτων multihop είναι βασισμένη στο ελλοχεύον στρώμα μεταφορών. Κάνουμε επίσης τις ακόλουθες υποθέσεις.

1. Κάθε κόμβος έχει μια μοναδική διαφορετική από το μηδέν ταυτότητα και έναν μηχανισμό για να ανακαλύψει τον ένα-λυκίσκο γείτονες του.
2. Η επικοινωνία μεταξύ του γειτονικού κόμβου ενός-λυκίσκου είναι πιο αξιόπιστη έναντι με την επικοινωνία multihop πέρα από το επιρρεπές σε λάθη ασύρματο κανάλι.
3. Κάθε κόμβος έχει τουλάχιστον τον ένα-λυκίσκο νόμιμο γειτονικό nodes2 K .
4. Η κινητικότητα χαρακτηρίζεται από μια μέγιστη κινούμενη ταχύτητα S_{max} κόμβων.

5. Κάθε κόμβος είναι εξοπλισμένος με κάποιο τοπικό μηχανισμό ανίχνευσης για να προσδιορίσει τους κόμβους άπρεπης συμπεριφοράς μεταξύ της γειτονιάς ένας-λुकίσκου του, π.χ., εκείνοι που είναι προτεινόμενοι μέσα. Αυτή η υπόθεση είναι βασισμένη στην παρατήρηση ότι αν και η ανίχνευση παρείσφρησης στα Ad Hoc δίκτυα είναι γενικά δυσκολότερη απ'ό,τι στα συνδεδεμένα με καλώδιο δίκτυα, η ανίχνευση των συμπεριφορών μεταξύ των γειτόνων ένας-λुकίσκου είναι ευκολότερος και πρακτικός και οφείλεται στη φύση ραδιοφωνικής μετάδοσης της ασύρματης μετάδοσης.

Το σχέδιό μας χειρίζεται δύο είδη επιθέσεων: οι επιθέσεις DoS και οι διαρρήξεις κόμβων. Οι αντίπαλοι μπορούν να εκδώσουν τις επιθέσεις DoS από τα διάφορα στρώματα του σωρού δικτύων που κυμαίνεται από το στρώμα Smurf δικτύων και το *Teardrop*, την πλημμύρα TCP στρώματος μεταφορών και την πλημμύρα SYN, και τις διάφορες επιθέσεις στο στρώμα εφαρμογής. Για τους αντιπάλους που επιδιώκουν να συμβιβάσουν τους κόμβους δικτύωσης, υποθέτουμε ότι οι ελλοχεύοντες κρυπτογραφικοί πρωτόγονοι όπως η RSA είναι υπολογιστικά ασφαλείς. Εντούτοις, επιτρέπουμε τις περιστασιακές διαρρήξεις μέσω των παραγόντων όπως το επισφαλές OS, τα ζώφια λογισμικού και τα backdoors κ.λπ. Διάφοροι αντίπαλοι μπορούν να συνωμοτήσουν και να διαμορφώσουν μια ομάδα. Για την ευκολία της παρουσίασης, δείχνουμε μια τέτοια αντίπαλη ομάδα από έναν ενιαίο αντίπαλο. Χαρακτηρίζουμε τους αντιπάλους στα ακόλουθα δύο πρότυπα όπως προτείνονται:

- Πρότυπο I: Κατά τη διάρκεια της ολόκληρης διάρκειας ζωής του δικτύου, ο αντίπαλος δεν μπορεί να σπάσει ή να ελέγξει το K ή περισσότερους κόμβους.
- Πρότυπο II: Εξετάστε το χρόνο που διαιρείται σε διαστήματα του μήκους T. Κατά τη διάρκεια οποιουδήποτε χρονικού διαστήματος τ , ο αντίπαλος δεν μπορεί να σπάσει ή να ελέγξει το K ή περισσότερους κόμβους.

Αν και οποιαδήποτε στιγμή σταθερά δεν μπορεί να σπάσει ή να ελέγξει το K ή περισσότερους κόμβους, οι αντίπαλοι του προτύπου II μπορούν να επιλέξουν τα θύματά τους κάθε φορά. Καθώς το χρόνο που πηγαίνει σε κάθε κόμβο στο δίκτυο μπορεί να σπάσει κατά τη διάρκεια κάποιου χρονικού διαστήματος. Χειρισμός του αντίπαλου του προτύπου I. Σε αυτό το έγγραφο, επεκτεινόμαστε με τις εξελικτικές παράλληλες τεχνικές αναπροσαρμογών μεριδίου για να χειριστούν οι αντίπαλοι το πρότυπο II.

4.9. Επιθέσεις στα Ad Hoc δίκτυα

Επιθέσεις στα ειδικά πρωτόκολλα δρομολόγησης δικτύων και η πτώση της μίας από τις δύο κατηγορίες:

- Επιθέσεις καθοδήγησης-διάσπασης. Ο επιτιθέμενος προσπαθεί να προκαλέσει τα νομιμοποιημένα πακέτα στοιχείων που καθοδηγούνται με δυσλειτουργικούς τρόπους.

- Επιθέσεις πόρων-κατανάλωσης. Ο επιτιθέμενος επεμβαίνει σε πακέτα στο δίκτυο σε μία προσπάθεια να καταναλωθούν πολύτιμοι πόροι δικτύων όπως το εύρος ζώνης ή για να καταναλώσει πόρους κόμβων όπως η μνήμη (αποθήκευσης) ή τη δύναμη υπολογισμού.

Από μια προοπτική εφαρμογή-στρώματος, και οι δύο επιθέσεις είναι περιπτώσεις μιας επίθεσης άρνησης υπηρεσιών (DOS).

Ένα παράδειγμα μιας επίθεσης καθοδήγησης-διάσπασης ,είναι το εξής : για έναν επιτιθέμενο που στέλνει τα σφυρηλατημένα πακέτα δρομολόγησης για να δημιουργήσει μια δρομολόγηση βρόχος, δηλαδή να αναγκάσει τα πακέτα να διαπεράσουν τους κόμβους σε έναν κύκλο χωρίς την επίτευξη των προορισμών τους, καταναλώνοντας κατά συνέπεια ενέργεια και το διαθέσιμο εύρος ζώνης. Ένας επιτιθέμενος ομοίως, δημιουργεί ένα blackhole, στο οποίο προσελκύει και ρίχνει τα πακέτα στοιχείων.

Ένας επιτιθέμενος δημιουργεί ένα blackhole κατά τη διανομή των πληροφοριών δρομολόγησης δηλαδή ο επιτιθέμενος προσελκύει την κυκλοφορία και μπορεί κατόπιν να την απορρίψει. Σε μια ειδική περίπτωση μαύρης τρύπας, ένας επιτιθέμενος θα μπορούσε να δημιουργήσει μια γκρίζα τρύπα, στην οποία ρίχνει επιλεκτικά μερικά πακέτα, παραδείγματος χάριν, με την αποστολή πακέτα δρομολόγησης αλλά όχι πακέτα στοιχείων. Ένας επιτιθέμενος επίσης προσπαθεί να αναγκάσει έναν κόμβο να χρησιμοποιήσει μια λοξοδρόμηση διαδρομών (suboptimal διαδρομή), ή να χωρίσει το δίκτυο με την έγχυση των πληροφοριών δρομολόγησης για να αποτρέψει ένα σύνολο κόμβων από την επίτευξη των προορισμών τους. Ένας επιτιθέμενος μπορεί να προσπαθήσει να κάνει μια διαδρομή να εμφανιστεί μακρύτερη με την προσθήκη εικονικών κόμβων στη διαδρομή. Καλούμε αυτήν την επίθεση δωρεάν λοξοδρόμηση επειδή η κοντύτερη διαδρομή υπάρχει και μπορεί να είχε χρησιμοποιηθεί.

Στα ειδικά πρωτόκολλα δρομολόγησης δικτύων που προσπαθούν να κρατήσουν τη διαδρομή των αντιληπτών κακόβουλων κόμβων σε μια μαύρη λίστα ,σε κάθε κόμβο ένας επιτιθέμενος προσπαθεί να συκοφαντεί έναν καλό κόμβο, για να προκαλέσει άλλους καλούς κόμβους και να προσθέσει εκείνο τον κόμβο στις μαύρες λίστες και κατά συνέπεια να αποφεύγει εκείνο τον κόμβο στις μελλοντικές διαδρομές . Ένας λεπτότερος τύπος επίθεσης καθοδήγησης-διάσπασης δημιουργεί ένα wormhole στο δίκτυο, χρησιμοποιώντας ο επιτιθέμενος ένα ζευγάρι κόμβων Α και Β που συνδέονται μέσω μιας ιδιωτικής σύνδεσης δικτύων.

4.10. Εξασφάλιση AODV

Το ειδικό κατόπιν παραγγελίας πρωτόκολλο δρομολόγησης απόστασης (Ad hoc On-demand Distance Vector routing protocol [AODV]) διαδίδει τις διανυσματικές πληροφορίες δρομολόγησης απόστασης κατά τρόπο κατόπιν παραγγελίας.

4.10.1. Μια ασφαλής κατόπιν παραγγελίας δρομολόγηση πρωτόκολλο για τα Ad Hoc δίκτυα

Το Ariadne12 είναι ένα ασφαλές κατόπιν παραγγελίας πρωτόκολλο δρομολόγησης αυτό αντιστέκεται στο συμβιβασμό κόμβων και στηρίζεται μόνο στο ιδιαίτερα αποδοτικό

συμμετρικό σύστημα κρυπτογραφίας. Το Ariadne μπορεί να επικυρώσει μηνύματα δρομολόγησης που χρησιμοποιούν το ένα από τρία σχέδια:

1. κοινά μυστικά μεταξύ κάθε ζευγαριού των κόμβων,
2. κοινά μυστικά μεταξύ της επικοινωνίας των κόμβων που συνδυάζεται με την επικύρωση ραδιοφωνικής μετάδοσης, ή
3. ψηφιακές υπογραφές.

Η βασική ιδέα του Ariadne είναι βασισμένη σε DSR: το Ariadne ανακαλύπτει διαδρομές κατόπιν παραγγελίας (δεδομένου ότι απαιτούνται) μέσω της διαδρομής.

4.11. SEAD σε κινητά ασύρματα Ad Hoc δίκτυα

Η ασφαλής αποδοτική ειδική διανυσματική δρομολόγηση απόστασης, το πρωτόκολλο SEAD είναι γερό ενάντια σε ασυντόνιστα επιτιθέμενους που δημιουργούν το ανακριβές κράτος καθοδηγώντας σε οποιοδήποτε άλλο κόμβο, παρά τους ενεργούς επιτιθέμενους ή συμβιβασμένους κόμβους στο δίκτυο. Βασίσαμε το σχέδιο SEAD εν μέρει στο πρωτοκόλλο (DSDV), Για να υποστηρίξει τη χρήση SEAD με τους κόμβους της περιορισμένης ικανότητας επεξεργασίας, και για να φρουρήσει ενάντια στις επιθέσεις DoS στις οποίες ένας επιτιθέμενος προσπαθεί να αναγκάσει άλλους κόμβους να καταναλώσει το χρόνο στο δίκτυο εύρους ζώνης ή επεξεργασίας, χρησιμοποιούμε αποδοτικό μονόδρομο.

ΚΕΦΑΛΑΙΟ 5

ΕΦΑΡΜΟΓΕΣ

5.1. Οι εφαρμογές Ad Hoc δικτύων

Παραδείγματα των εφαρμογών για την ειδική σειρά δικτύων είναι: οι στρατιωτικές διαδικασίες, η κοινοτική δικτύωση και η αλληλεπίδραση μεταξύ της συνεδρίασης των συμμετεχόντων ή σπουδαστών κατά τη διάρκεια μιας διάλεξης. Σε αυτές και άλλες ειδικές εφαρμογές δικτύωσης, ασφάλεια στη δρομολόγηση παρέχει το πρωτόκολλο που είναι απαραίτητο για να φρουρεί ενάντια σε επιθέσεις όπως είναι η κακόβουλος εσφαλμένη κατεύθυνση δρομολόγησης.

Αυτό το άρθρο αναθεωρεί τις επιθέσεις στα Ad Hoc δίκτυα και συζητά τις τρέχουσες προσεγγίσεις για την καθιέρωση κρυπτογραφικών κλειδιών στα Ad Hoc δίκτυα.

5.2. ΕΦΑΡΜΟΓΕΣ BLUETOOTH

Λόγω της εξαιρετικής χρησιμότητας του Bluetooth, οι διάφοροι κατασκευαστές έχουν αρχίσει να προτείνουν εμπορικές εφαρμογές, οι ενδεικτικότερες από τις οποίες αναφέρονται στη συνέχεια:

- **Αυτόματος Συγχρονισμός**

Διαφανής σύνδεση μεταξύ του κινητού υπολογιστή, του PDA και του κινητού τηλεφώνου του χρήστη, η οποία θα δίνει τη δυνατότητα στις εφαρμογές να ενημερώνονται αυτόματα και να συγχρονίζουν τα προγράμματα και τα άλλα δεδομένα όταν πραγματοποιούνται αλλαγές σε κάποια από τις συσκευές.

- **Ασύρματες Συσκευές Χειρός**

Αυτές οι εφαρμογές θα δίνουν τη δυνατότητα πρόσβασης στις κινητές συσκευές του χρήστη, ακόμα κι αν αυτές βρίσκονται στην τσέπη του.

- **Τριπλή Χρήση Τηλεφωνικής Συσκευής**

Μια απλή συσκευή χειρός θα μπορεί να λειτουργεί σαν ενδοεπικοινωνία στο γραφείο (χωρίς χρέωση), σαν σταθερό τηλέφωνο PSTN, όταν υπάρχει αντίστοιχο σημείο πρόσβασης, και σαν κινητή συσκευή σε κάθε άλλη περίπτωση.

5.3. ΕΦΑΡΜΟΓΕΣ HIPERLAN/2 – HIPERSPOT

Αν και το HIPERLAN/2 πρωταρχικά στοχεύει, κυρίως, σε περιβάλλοντα γραφείου και οικίας, αυτό το σύστημα φαίνεται να συμπληρώνει την σταθερή δομή των κυψελωτών δικτύων ευρείας περιοχής ώστε να παρέχει στους χρήστες μεγαλύτερες δυνατότητες σε έναν εξωτερικό χώρο όπου υπάρχει υψηλή πυκνότητα κόμβων: τα λεγόμενα hotspots. Επομένως, προβλέπεται ότι θα συμβεί σημαντική ανάπτυξη τέτοιων συστημάτων σε αρκετές πόλεις της Ευρώπης. Από την στιγμή που μόνο ένας περιορισμένος αριθμός από κανάλια είναι διαθέσιμος (19 στην Ευρώπη, 9 στις Η.Π.Α), είναι προφανές ότι οι παρεμβολές στο εσωτερικό του συστήματος θα έχουν άσχημο αντίκτυπο στην ρυθμαπόδοση του δικτύου. Σε πολλές περιπτώσεις η δυναμική επιλογή συχνότητας δεν θα είναι ικανή να αντιμετωπίσει το πρόβλημα. Ακόμη και η εφαρμογή κεραιών που αρμόζουν για την περίπτωση της σταθερής πρόσβασης στο εξωτερικό περιβάλλον δεν θα μπορούσε, με χαμηλό κόστος, να διευθετήσει το ζήτημα. Σε τέτοιες περιπτώσεις, θα ήταν προτιμότερο να υπάρχει ένας άλλος τρόπος για την αποσυμφόρηση των καναλιών του HIPERLAN/2 από τις παρεμβολές, ώστε να αποφευχθεί η υπερβολική ζήτηση φάσματος καθώς διατηρούνται αποδόσεις υψηλού ρυθμού δεδομένων. Γι' αυτό και η προσέγγιση του κεφαλαίου αυτού στοχεύει στην ανάπτυξη μιας τέτοιας επέκτασης του HIPERLAN/2 που θα λειτουργεί στην περιοχή των 60GHz. Όπως αναφέραμε και στην προηγούμενη παράγραφο, έχουν αναγνωριστεί τρία κύρια σενάρια εφαρμογών που απαιτούν τέτοιου είδους τεχνολογία:

- Σενάριο 1, κάλυψη εμπορικών σημείων – hotspots: Πρόκειται για μία πολύ σημαντική εφαρμογή και αναφέρεται στην δυνατότητα κάλυψης πλήρως καθορισμένων φυσικών περιοχών σε περιβάλλον εξωτερικού χώρου σε αστική περιοχή με υψηλή πυκνότητα κόμβων. Κάτι παραπάνω από μία, απλώς, προοπτική παροχής Internet οπουδήποτε και οποιαδήποτε στιγμή, αποτελεί, επίσης, και απαίτηση από πλευράς πωλητών και καταστηματαρχών που θα έχουν τη δυνατότητα να προσελκύσουν το κοινό στους χώρους τους με το να προσφέρουν, χωρίς επιβάρυνση, συγκεκριμένες ασύρματες υπηρεσίες. Είναι απαραίτητος ο ακριβής καθορισμός της περιοχής κάλυψης σε αυτή την περίπτωση και είναι πιθανή η ικανοποίηση αυτής της απαίτησης με την βοήθεια κατευθυντικών κεραιών μικρού μεγέθους στην συχνότητα των 60GHz. Η σύνδεση των συσκευών με το δίκτυο κορμού θα επιτυγχάνεται μέσω του συμβατικού δικτύου HIPERLAN/2.

- Σενάριο 2, ανάπτυξη σε κτίρια και διαμερίσματα όπου υπάρχει μεγάλη πυκνότητα χρηστών: Επεκτείνοντας το HIPERLAN/2 στα 60GHz, όπου τα σήματα με δυσκολία μπορούν να διαπεράσουν τοίχους ή στερεά εμπόδια, θα εγγυηθούμε, έμμεσα, την έλλειψη παρεμβολής από τις γειτονικές κυψέλες (π.χ. άλλο δωμάτιο/γραφείο, άλλο διαμέρισμα). Σε περιοχές, όπου υφίστανται καλές συνθήκες επικοινωνίας μεταξύ των χρηστών (για παράδειγμα συνθήκη οπτικής επαφής), οι συσκευές θα συντονίζονται στα 60GHz, ώστε να μην φορτώνεται σημαντικά το δίκτυο κορμού στα 5GHz από πλευράς κίνησης δεδομένων και παρεμβολών. Γειτονικά σπίτια θα γίνουν πραγματικά ιδιωτικά σε ένα φυσικό επίπεδο.

- Σενάριο 3, παιχνίδια: Μία τρίτη εφαρμογή (δυννητικά μαζικής αγοράς), ως απαίτηση της βιομηχανίας παιχνιδιών, είναι η κατευθυνόμενη ομότιμη επικοινωνία μεταξύ μικρών συσκευών, σε συχνότητα που δεν χρειάζεται σχετική επίσημη άδεια, με την μικρότερη δυνατή παρεμβολή με άλλα ζευγάρια επικοινωνίας που χρησιμοποιούν το ίδιο σύστημα.

Στην πραγματικότητα, το HIPERLAN/2 υποστηρίζει ότι προσφέρει γύρω στα 50Mbps ανά κυψέλη με περιοχή κάλυψης τα 50 μέτρα, και συνεπώς θα μπορούσαν να αυξήσουν την δυνατότητα για download που παρέχει το δίκτυο UMTS. Παρόλ' αυτά, σε μεγαλοαστικές περιοχές, ο αριθμός των χρηστών ανά κυψέλη μπορεί να είναι ιδιαίτερα υψηλός με αποτέλεσμα τον μειωμένο χρησιμοποιούμενο ρυθμό δεδομένων για υπηρεσίες download. Στην προσέγγιση των 60GHz, η περιοχή κάλυψης της κυψέλης είναι πράγματι μικρότερη: γύρω στα 10 μέτρα, αλλά το εύρος ζώνης του καναλιού συχνότητας, εικονικά, δεν μπορεί να περιοριστεί. Εκτιμάται ότι μέσω της κάλυψης των σημείων hotspots από τα 60GHz, είναι δυνατός ο στόχος για μεγαλύτερη χωρητικότητα ανά χρήστη σε πολυπληθή αστικά περιβάλλοντα για υπηρεσίες download. Για παράδειγμα: σαν ένας πρόχειρος κανόνας, οι κυψέλες ακτίνας 50 μέτρων που παρέχουν συνολικό ρυθμό δεδομένων 54Mbps, και μοιράζονται ανάμεσα σε 872 χρήστες (θεωρείται μία πυκνότητα ενός χρήστη ανά 9 τετραγωνικά μέτρα), οδηγούν σε μία μέγιστη εγγυημένη στιγμιαία χωρητικότητα περίπου 60kbps ανά χρήστη. Στα 60GHz, χρησιμοποιώντας κυψέλες των 10 μέτρων με ένα εύρος ζώνης καναλιού των 80MHz, που είναι 4 φορές το μέγεθος του καναλιού για το HIPERLAN/2 (20MHz): 35 άτομα θα έχουν την δυνατότητα να μοιράζονται στιγμιαία γύρω στα 216Mbps οδηγώντας σε μία ρυθμαπόδοση των 6Mbps ανά χρήστη: αυτό αντιπροσωπεύει ένα κέρδος της τάξης του 100 σε όρους χωρητικότητας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

<http://www.microshop.gr/company.asp?to=24>

<http://egnatia.ee.auth.gr/~aalexioy/bloutoot.htm>

http://www.go-online.gr/ebusiness/specials/article.html?article_id=392&PHPSESSID=475a54194ffaeaaedbf6052a9b7a643e

http://www.go-online.gr/ebusiness/specials/article.html?article_id=405

http://www.go-online.gr/ebusiness/specials/article.html?article_id=405

http://www.go-online.gr/ebusiness/specials/article.html?article_id=394

http://www.go-online.gr/ebusiness/specials/article.html?article_id=407

http://www.go-online.gr/ebusiness/specials/article.html?article_id=395

http://www.go-online.gr/ebusiness/specials/article.html?article_id=396

http://www.go-online.gr/ebusiness/specials/article.html?article_id=404

http://www.go-online.gr/ebusiness/specials/article.html?article_id=393

<http://www.papaki.panteion.gr/teuxos18/diktya.htm>

http://2tee-n-smyrn.att.sch.gr/txn_site/txn2.htm

http://www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/teaching_m/WirelessNetworks-Web/Chapter1.html

<http://www.actapress.com/PaperInfo.aspx?PaperID=23950>

<http://citeseer.ist.psu.edu/royer99review.html>

<http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/trans/td/&toc=comp/trans/td/2004/12/lztoc.xml&DOI=10.1109/TPDS.2004.73>

<http://moment.cs.ucsb.edu/AODV/aodv.html>

http://en.wikipedia.org/wiki/Ad_hoc_protocols_implementations

<http://www.answers.com/topic/ad-hoc-routing-protocol-list>

<http://www.comp.brad.ac.uk/~sburuha1/routingprot.htm>

<http://www.comp.brad.ac.uk/~sburuha1/abr.htm>

[http://wiki.uni.lu/secan-lab/Ad-Hoc+Protocols+\(\\$28\)Classification\(\\$29\).html](http://wiki.uni.lu/secan-lab/Ad-Hoc+Protocols+($28)Classification($29).html)

http://www.absoluteastronomy.com/enc1/ad_hoc_protocol_list

<http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group11/index.html>

<http://www.netmeister.org/misc/zrp/zrp.html>

wwwbib.informatik.tu-muenchen.de/inferichte/2003/TUM-I0311.pdf

[www.control.hut.fi/Kurssit/AS-74.4340/
slides_and_reports_adhoc_net/Routing_repot_abouda.pdf](http://www.control.hut.fi/Kurssit/AS-74.4340/slides_and_reports_adhoc_net/Routing_repot_abouda.pdf)

<http://www.tik.ee.ethz.ch/~beutel/positioning.html>

<http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group3/index.html>

http://www.geocities.com/prashthy/secure_routing_ad_hoc.html

<http://www.wi-fiplanet.com/tutorials/article.php/1451421>

<http://www.wi-fiplanet.com/tutorials/article.php/3494246>

ΠΑΡΑΡΤΗΜΑ

ΔΙΑΜΟΡΦΩΣΗ ΤΩΝ AD_HOC ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΝΔΕΣΗ ΤΟΥΣ ΜΕ ΤΟ ΔΙΑΔΙΚΤΥΟ.

Το πρώτο βήμα που θα πρέπει να γίνει, είναι να εγκατασταθεί μια ασύρματη κάρτα 802.11b στον κεντρικό υπολογιστή και να διαμορφωθεί ως Ad Hoc ασύρματη σύνδεση υπολογιστής- προς - υπολογιστή . Υπάρχουν τρία καθιερωμένα πρότυπα WI-FI : 802.11b, 802.11a και 802.11g. Δυστυχώς όμως το 802.11a πρότυπο δεν είναι συμβατό με 802.11b/g. Έτσι η αγορά WIFI παραμένει κάπως τεμαχισμένη. Πιο κάτω μπορείτε να δείτε μία κάρτα WiFi, **που ακολουθεί το 802.11b πρότυπο.**



Εικόνα 1: D-LINK Κάρτα PCI WiFi 54 Mb DWL-G510
Data Link Protocol --> IEEE 802.11b

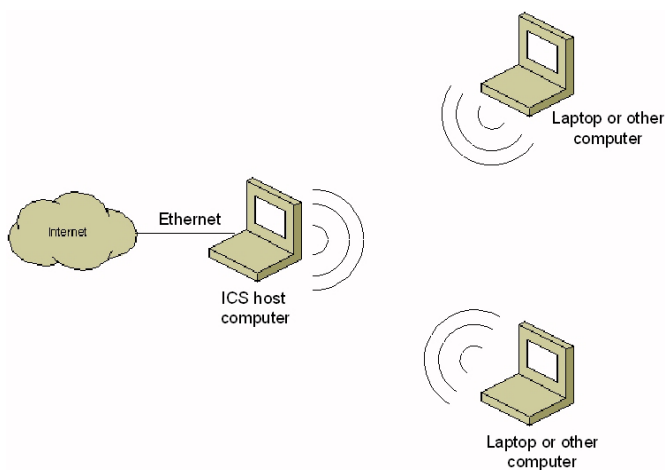
Ο Ad Hoc τρόπος δικτύωσης πρέπει γενικά να αντιμετωπισθεί όπως "πιο αργός". Πρέπει να αναμείνετε ότι οι συσκευές WiFi που υποστηρίζουν 54 Mbps ή υψηλότερη ταχύτητα στον ειδικό τρόπο δικτύωσης θα έχουν μικρότερη απόδοση, με μέγιστο τα 11 Mbps, λόγω του τρόπου υποδομής. Ακόμη θα πρέπει να αναφέρουμε ότι οι συσκευές WiFi στον ειδικό τρόπο προσφέρουν την ελάχιστη ασφάλεια ενάντια στις ανεπιθύμητες εισερχόμενες συνδέσεις.

Το δεύτερο βήμα θα είναι να εγκατασταθεί μια ασύρματη κάρτα σε έναν δεύτερο υπολογιστή.

Για να ολοκληρώσει το δίκτυο και να παρέχεται η σύνδεση με το Διαδίκτυο σε όλους τους χρήστες του, θα πρέπει να γίνουν κάποιες ενέργειες από τον οικοδεσπότη υπολογιστή.

1 Αυτή η διαμόρφωση προϋποθέτει την εξής υποδομή :

- Ένα lap-top υπολογιστή που τρέχοντας windows XP περιβάλλον και που είναι εξοπλισμένος και με Ethernet κάρτα δικτύου αλλά και με 802.11 προσαρμοστή δικτύων WLAN. Αυτός ο υπολογιστής αναφέρεται ως οικοδεσπότης υπολογιστής ολοκληρωμένων κυκλωμάτων.
- Μια Ethernet σύνδεση στο Διαδίκτυο.



- Laptops ή άλλους υπολογιστές που τρέχουν σε windows XP περιβάλλον και είναι εξοπλισμένα με 802.11 προσαρμοστές δικτύων WLAN.

Εικόνα 2: προκύπτουσα διαμόρφωση

Έτσι όταν έχετε έναν υπολογιστή που συνδέεται με το Διαδίκτυο, με χρήση ενός καλωδίου Ethernet, συνδέεστε ως οικοδεσπότης υπολογιστής και οι άλλοι υπολογιστές ενός μικρού ειδικού δικτύου μπορούν να συνδέσουν με το Διαδίκτυο μέσω του οικοδεσπότη υπολογιστή. Θα περιγράψουμε τα βήματα που απαιτούνται μέσα από το περιβάλλον των windows XP , για να συνδέσουμε με το Διαδίκτυο έναν υπολογιστή, χρησιμοποιώντας μια σύνδεση Ethernet και να μοιραστούμε έπειτα αυτή την σύνδεση με το Διαδίκτυο με άλλους υπολογιστές χρησιμοποιώντας ένα ειδικό ασύρματο δίκτυο.

2 Τα βήματα που θα πρέπει να ακολουθήσουμε για τη διαμόρφωση της ειδικής διανομής Διαδικτύου είναι τα ακόλουθα:

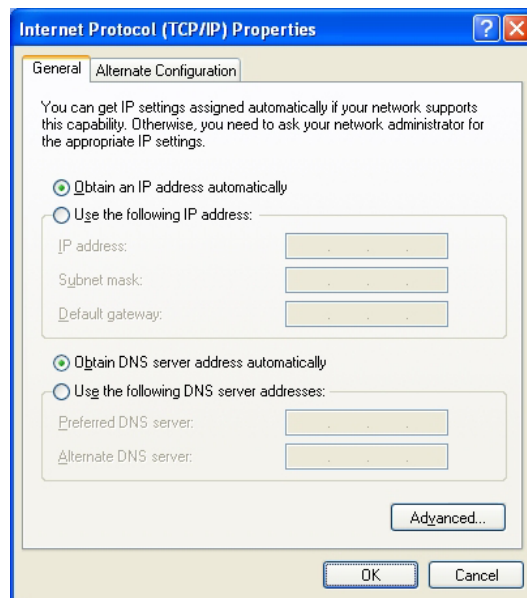
1. Συνδέστε τον οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων με το Διαδίκτυο.
2. Ρυθμίστε τον υπολογιστή σας έτσι ώστε ο οικοδεσπότης υπολογιστής, να μοιράζεται τη σύνδεση με το Διαδίκτυο , με άλλους χρήστες του ειδικού δικτύου.
3. Δημιουργήστε ένα ειδικό ασύρματο δίκτυο στον οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων(ICS).
4. Συνδεθείτε με το νέο ειδικό ασύρματο δίκτυο από τους άλλους υπολογιστές lap-top.

Πιο κάτω περιγράφονται αυτά τα βήματα λεπτομερώς.

2.1. Σύνδεση του οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων με το Διαδίκτυο

Α) Συνδέστε ένα καλώδιο Ethernet που οδηγεί από την τηλεφωνική γραμμή, στον προσαρμοστή Ethernet του οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων. Σε πολλές περιπτώσεις, η σύνδεση με το Διαδίκτυο θα παράσχει την αυτόματη απόδοση IP. Για να χρησιμοποιήσετε αυτήν την δυνατότητα της σύνδεσης με το Διαδίκτυο η σύνδεση Ethernet, πρέπει κάνετε κάποιες ρυθμίσεις μέσα από τις συνδέσεις δικτύου των windows XP. Θα πρέπει λοιπόν να ακολουθήσετε τα εξής βήματα:

- i. Πατήστε έναρξη από την επιφάνεια εργασίας των windows XP. Αφού ανοίξετε τον πίνακα ελέγχου αρχικά, πατήστε συνδέσεις Δικτύου.
- ii. Επιλέξτε τη σύνδεσή σας και κάνετε δεξί κλικ-ιδιότητες πάνω σε αυτή.
- iii. Επιλέξτε τώρα την ετικέτα δίκτυο και πατήστε διπλό κλικ στο πρωτόκολλο Διαδικτύου (TCP/IP).
- iv. Στη γενική ετικέτα, επιλέξτε “αυτόματη απόδοση διεύθυνσης IP” και “αυτόματη απόδοση διεύθυνσης διακομιστή DNS” ώστε να λαμβάνει τη διεύθυνση κεντρικών υπολογιστών αυτόματα. Η καρτέλα αυτή φαίνεται σε φωτογραφία που ακολουθεί.



Εικόνα 3

- v. Επιλέξτε OK για να σώσετε τις αλλαγές στη διαμόρφωση της σύνδεσής σας. Εάν η σύνδεση με το Διαδίκτυο δεν παρέχει την αυτόματη εξέταση IP, πρέπει με το χέρι να αποδώσετε μια IP διεύθυνση για τον υπολογιστή σας.

Για να λάβετε μια διεύθυνση IP, θα πρέπει να έρθετε σε επαφή με το διαχειριστή δικτύων του δικτύου με το οποίο συνδέεστε.

Για να διαμορφώσετε με το χέρι τα τρέχοντας παράθυρα XP υπολογιστών για μια διαμόρφωση διευθύνσεων IP, κάνετε τα εξής: Θα πρέπει να ανοίξετε πάλι την γενική ετικέτα στο πρωτόκολλο Διαδικτύου, όπως περιγράψαμε πιο πάνω, και στη συνέχεια επιλέξτε “χρήση της παρακάτω διεύθυνση IP” και δακτυλογραφήστε τη διεύθυνση IP. Υπάρχει ακόμη η ρύθμιση για τη μάσκα υποδικτύου (subnet mask). Επιλέξτε “χρήση των παρακάτω διευθύνσεων διακομιστή DNS”, και δακτυλογραφήστε τη διεύθυνση IP ενός προτιμημένου και εναλλακτικού κεντρικού υπολογιστή συστημάτων (dns). Πατήστε OK για να σώσετε τις αλλαγές στη σύνδεσή σας

B) Έπειτα, θα πρέπει να ενεργοποιήσετε το firewall των windows XP, ή μια αντιτυρική ζώνη τρίτων για να βοηθήσουν να προστατεύσετε τον οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων από τους κακόβουλους χρήστες Διαδικτύου. Για να ενεργοποιήσετε το firewall των windows XP στον οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων, κάνετε τα εξής: Πατήστε την έναρξη στην επιφάνεια εργασίας των windows XP, και έπειτα ανοίξτε τον πίνακα ελέγχου. Πατήστε ‘συνδέσεις Δικτύου, επιλέξτε τη σύνδεσή σας για το διαδίκτυο και κάνετε δεξί κλικ-ιδιότητες πάνω σε αυτή. Επιλέξτε την καρτέλα ‘ασφάλεια(firewall)’. Μπορείτε τώρα να κάνετε τις ρυθμίσεις ασφαλείας που θέλετε και στη συνέχεια πατήστε OK για να σώσετε τις αλλαγές.

2.2. Ρυθμίστε τον υπολογιστή σας έτσι ώστε ο οικοδεσπότης υπολογιστής, να μοιράζεται τη σύνδεση με το Διαδίκτυο, με άλλους χρήστες του ειδικού δικτύου.

Για να επιτρέψει στον οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων να μοιράζεται τη σύνδεση με το διαδίκτυο με άλλους χρήστες του ειδικού δικτύου, κάνετε τα εξής:

- i. Πατήστε έναρξη από την επιφάνεια εργασίας των windows XP, ανοίξτε τον πίνακα ελέγχου και στη συνέχεια πατήστε “συνδέσεις Δικτύου”.
- ii. Επιλέξτε τώρα τη σύνδεσή σας για το διαδίκτυο και κάνετε δεξί κλικ-ιδιότητες πάνω σε αυτή.
- iii. Στην καρτέλα “για προχωρημένους”, επιλέξτε “να επιτρέπεται η πρόσβαση σε όλους τους χρήστες του δικτύου στο Διαδίκτυο”. Κάνετε ακόμη τις κατάλληλες ρυθμίσεις ώστε οι άλλοι χρήστες δικτύων να μην μπορούν να έχουν πρόσβαση στις ρυθμίσεις που κάναμε .
- iv. Πατήστε OK για να σώσετε τις αλλαγές στη σύνδεσή σας.

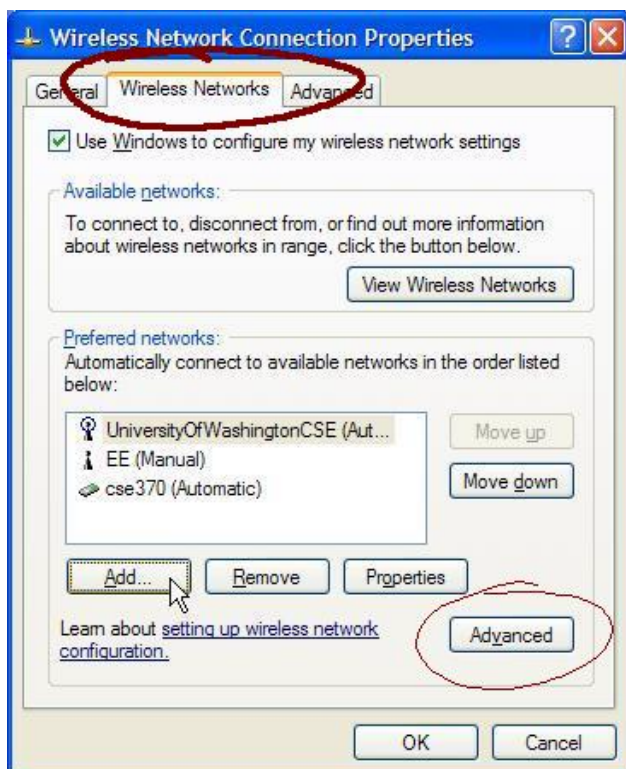
- v. Τότε θα εμφανιστεί ένα τοπικό παράθυρο μηνυμάτων δικτύων που εξηγεί τις αλλαγές που θα επέλθουν στη δικτύωση του υπολογιστή σας. Χτυπήστε ναι για να επιτρέψετε τη διανομή Διαδικτύου.

2.3. Δημιουργία ενός ειδικού ασύρματου δικτύου στον οικοδεσπότη υπολογιστή ολοκληρωμένων κυκλωμάτων.

Αφότου εγκαθιστάτε έναν προσαρμοστή 802.11b σε έναν υπολογιστή, τα windows XP θα ανιχνεύσουν αυτόματα την κάρτα. Εσείς πρέπει να εγκαταστήσετε τους οδηγούς(drivers), και στη συνέχεια θα εμφανιστεί μια εικόνα στην περιοχή ανακοίνωσης''task bar''(χρησιμοποιώ την «εξής..... κάρτα» για να κατασκευάσω το ειδικό ασύρματο δίκτυο.

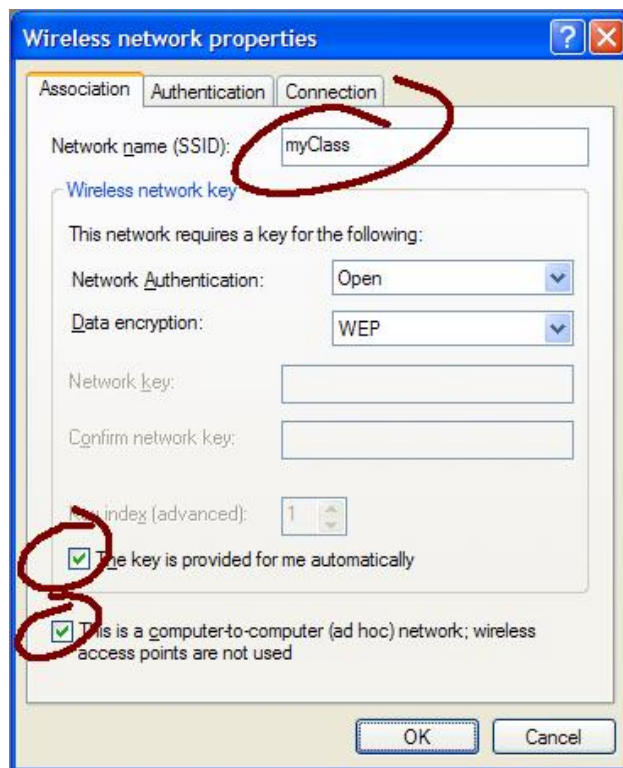
Για να δημιουργήσετε ένα ειδικό ασύρματο δίκτυο και να μοιραστείτε την πρόσβαση Διαδικτύου με τους άλλους υπολογιστές WLAN, σε περιβάλλον WINDOWS XP κάνετε τα εξής:

- i. Ανοίξτε το Control Panel (Πίνακα ελέγχου).Έπειτα Network Connections (συνδέσεις δικτύων).
- ii. Πατήστε κλικ στην ετικέτα Wireless Network (Ασύρματων δικτύων) και έπειτα το κουμπί add για προσθήκη. Ένα νέο παράθυρο θα εμφανιστεί.



Εικόνα 4

- iii. Δώστε στο δίκτυό σας ένα όνομα (PIX AdHocInternet), και ελέγξτε τα δύο Check boxes στο κάτω μέρος του παραθύρου.
- iv. Στην επικύρωση δικτύων, επιλέξτε “ανοικτό” ώστε να γίνεται πιστοποίηση.
- v. Στην κρυπτογράφηση στοιχείων, επιλέξτε WEP.
- vi. Στο κλειδί δικτύων, δακτυλογραφήστε το κλειδί WEP. Το κλειδί WEP πρέπει να είναι μια τυχαία ακολουθία δεκαεξαδικών ψηφίων ή αριθμών, επιστολών, και στίξης. <<Το κλειδί δικτύων, μπορείτε να το δώσετε οι ίδιοι, ή να τσεκάρετε την επιλογή για αυτόματη απόδοση >>.
- vii. Στο κλειδί δικτύων, δακτυλογραφήστε εκ νέου το κλειδί WEP.
- viii. Επιλέξτε το κλειδί για προστασία.



Ποιός ο λόγος Διαμόρφωσης WEP;

Οι τοποθετήσεις WEP διαμορφώνονται ούτως ώστε να εξασφαλιστεί η καλύτερη δυνατή ασφάλεια του Ad hoc δικτύου. Να είστε βέβαιος ότι εάν χρησιμοποιείτε ένα κλειδί δικτύων ASCII και επιλέξετε τυχαίους χαρακτήρες (αριθμούς και γράμματα) που δεν μπορούν να υποτεθούν εύκολα, εξασφαλίζετε σε μεγάλο βαθμό την ασφάλεια του ειδικού δικτύου. Το τελικό βήμα είναι να χρησιμοποιηθούν οι ίδιες τοποθετήσεις κλειδιών και κρυπτογράφησης και να διαμορφωθεί υπολογιστής πελατών. Σημείωση: για την πρόσθετη ασφάλεια, κάνετε αλλαγή του κλειδιού σε κανονική εβδομαδιαία βάση.

Εικόνα 5

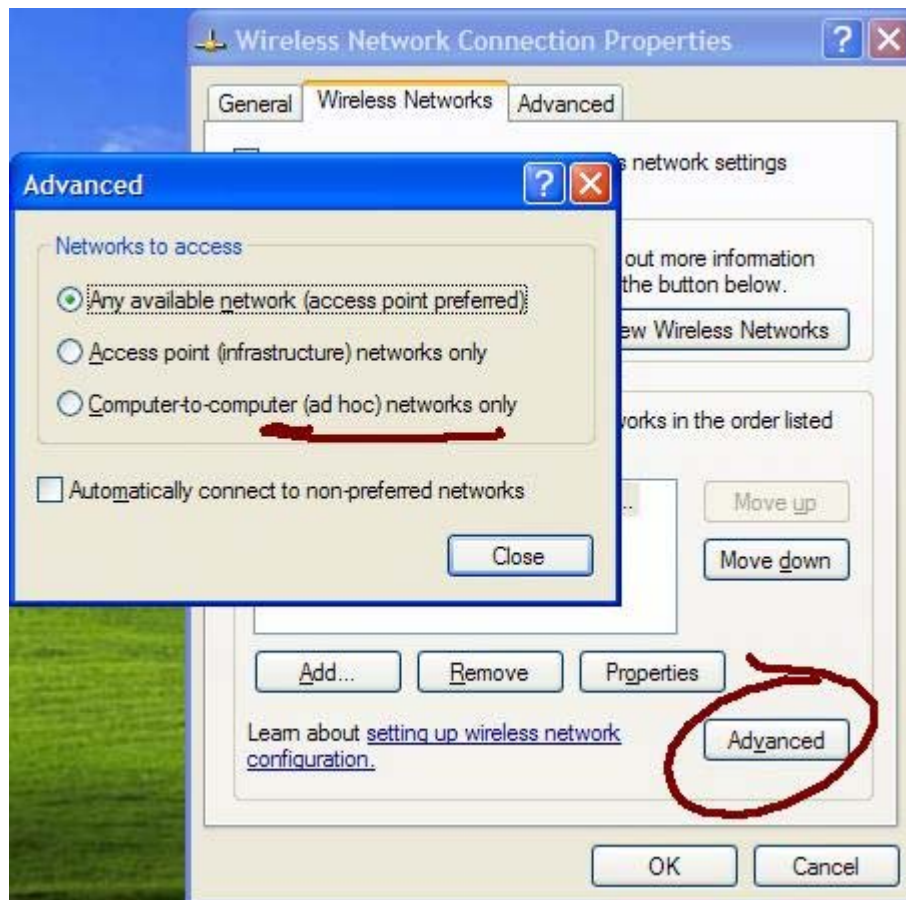
- ix. Επιλέξτε αυτό είναι ένα παράθυρο ελέγχου δικτύων υπολογιστής-σε – υπολογιστή.
- x. Πατήστε Ok για να σώσετε τις αλλαγές και ξανά OK για να κλείσει το παράθυρο. Σιγουρευτείτε ότι πρώτα έχετε πατήσει το κουμπί Ok και οι αλλαγές σας πιθανό να έχουν σωθεί.

Το ειδικό δίκτυό Ad_Hoc έχει εγκατασταθεί !

2.4. Σύνδεση με το νέο ειδικό ασύρματο δίκτυο από τους άλλους υπολογιστές lap-top. (σύνδεση χρηστών).

A) Για να συνδεθεί ο ένας υπολογιστής lap-top στον άλλον, στο πρόσφατα δημιουργημένο ειδικό ασύρματο δίκτυο, πρέπει να κάνει τα εξής:

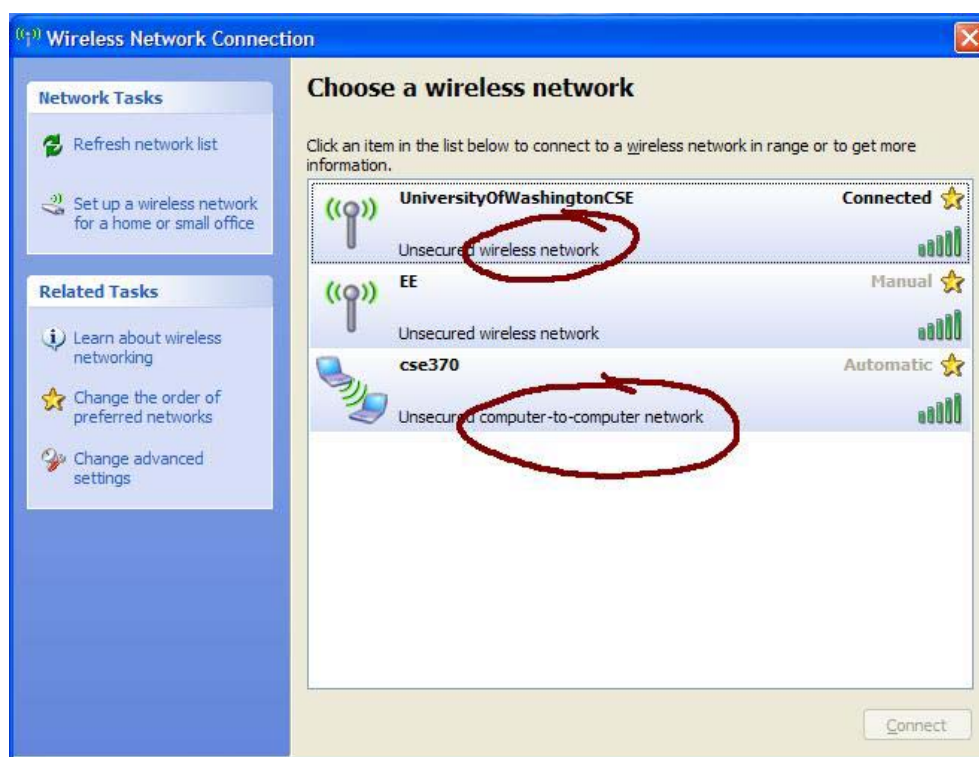
- i. Μόλις δημιουργηθεί το νέο Ad Hoc ασύρματο δίκτυο, θα ανιχνευθεί και θα δείτε το Ad_Hoc δίκτυο ,ως δίκτυο υπολογιστή-πρός-υπολογιστή στην περιοχή ανακοίνωσης taskbar του υπολογιστή σας. Ίσως χρειαστεί να ανανεώσετε τη λίστα. Εσείς επιλέξτε τη σύνδεση αυτή και κάντε κλικ στο Connect(κουμπί στο κάτω μέρος του παραθύρου). Μπορεί να πάρει ένα λεπτό ή δύο για να συνδεθεί στο δίκτυο
- ii. Εάν δεν βλέπετε το δίκτυό σας, πηγαίνετε συνδέσεις δικτύων. Μπορεί να πρέπει να αλλάξετε τις ρυθμίσεις σας για να συνδέσετε μόνο με τα ειδικά Ad_Hoc δίκτυα.. Επιλέξτε αλλαγές για προχωρημένους χρήστες(advanced settings). Στο νέο παράθυρο, επιλέξτε την ετικέτα ασυρμάτων δικτύων, και κατόπιν το κουμπί που δίνει πρόσβαση για προχωρημένους χρήστες(advanced).



Εικόνα 6

- iii. Επιλέξτε την Τρίτη επιλογή και πατήστε το Ok. Ανοίξτε τις συνδέσεις δικτύων πάλι, και ακολουθήστε τα βήματα για να συνδεθείτε με το δίκτυο.

Πρέπει να δείτε το ασύρματο πλαίσιο διαλόγου σύνδεσης δικτύων, ένα πλαίσιο διαλόγου με το όνομα της ασύρματης σύνδεσης, ή Connect στο ασύρματο πλαίσιο διαλόγου δικτύων. Το νέο Ad Hoc δίκτυο θα εμφανίζεται με μια εικόνα καρτών PC για να υποδείξει ότι αυτό είναι ένα δίκτυο υπολογιστής-σε- υπολογιστή. Ένα παράδειγμα του ασύρματου πλαισίου διαλόγου σύνδεσης δικτύων παρουσιάζεται πιο κάτω.



Εικόνα 7

- iv. Επιλέξτε το όνομα του νέου ειδικού ασύρματου δικτύου στον κατάλογο, και έπειτα σύνδεση. Όταν προσπαθήσετε να συνδεθείτε, θα σας ζητηθεί το κλειδί WEP του δικτύου. Πληκτρολογήστε το όνομα του νέου Ad Hoc ασύρματου δικτύου, δακτυλογραφήστε το κλειδί WEP στο κλειδί δικτύων και επιβεβαιώστε το κλειδί δικτύων, και χτυπήστε έπειτα σύνδεση.

B) Τώρα που συνδέεται ο υπολογιστής lap-top με το Ad Hoc ασύρματο δίκτυο, πρέπει να τον διαμορφώσετε έτσι ώστε να υπάρχει κάποια ασφάλεια είτε με τη χρήση firewall των windows XP είτε με διαμόρφωση διευθύνσεων IP από τον οικοδεσπότη υπολογιστή. Θα πρέπει λοιπόν να κάνετε τα εξής:

- i. Πατήστε έναρξη από την επιφάνεια εργασίας των windows XP, ανοίξτε τον πίνακα ελέγχου. Στη συνέχεια επιλέξτε “συνδέσεις δικτύου”
- ii. Επιλέξτε τη σύνδεση δικτύου που αντιστοιχεί στον ειδικό ασύρματο δίκτυο που έχουμε δημιουργήσει, και έπειτα κάντε πάνω σε αυτό δεξί κλικ-ιδιότητες.
- iii. Για τους υπολογιστές που τρέχουν σε περιβάλλον windows XP, επιλέξτε την προηγμένη ετικέτα, και επιλέξτε έπειτα τις τοποθετήσεις. Εκεί μπορείτε να κάνετε τις ρυθμίσεις για την προστασία του υπολογιστή σας, όπως Πχ. να τσεκάρετε την επιλογή “Protect my computer and network by limiting or preventing access to this computer from the Internet “
- iv. Ακόμη επιλέξτε τη γενική ετικέτα, και πατήστε διπλό κλικ στο πρωτόκολλο Διαδικτύου (TCP/IP). Επιλέξτε “αυτόματη απόδοση διεύθυνσης IP” και “αυτόματη απόδοση διεύθυνσης διακομιστή DNS” ώστε να λαμβάνει τη διεύθυνση κεντρικών υπολογιστών αυτόματα. Επιλέξτε εντάξει για να σώσετε τις αλλαγές στη διαμόρφωση του πρωτοκόλλου Διαδικτύου (TCP/IP), και τέλος επιλέξτε ξανά εντάξει για να σώσετε τις αλλαγές στη διαμόρφωση της σύνδεσής σας

Ο υπολογιστής lap-top πρέπει να λάβει μια διαμόρφωση διευθύνσεων IP 192.168.0. * σειρά διευθύνσεων μέσω του DHCP από τον οικοδεσπότη υπολογιστή και πρέπει να έχει την πλήρη συνδεσιμότητα Διαδικτύου.