**Τ.Ε.Ι. ΗΠΕΙΡΟΥ**
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ
( Σ.Δ.Ο. )

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

# ΘΕΜΑ : AD HOC ΔΙΚΤΥΑ

***ΥΠΕΥΘΥΝΗ ΚΑΘΗΓΗΤΡΙΑ : ΜΑΡΓΑΡΙΤΗ ΣΠΥΡΙΔΟΥΛΑ***

**ΥΠΕΥΘΥΝΟΣ ΕΡΓΑΣΙΑΣ :**
**ΠΑΝΑΓΟΠΟΥΛΟΣ ΠΕΡΙΚΛΗΣ**

# ΠΕΡΙΕΧΟΜΕΝΑ

# ΠΕΡΙΛΗΨΗ

Στην συγκεκριμένη εργασία θα γίνει παρουσίαση των ad hoc δικτύων, θα εξεταστεί η IEEE τεχνολογία βάση της οποίας θεσπίζονται τα πρότυπα για τα ασύρματα δίκτυα, θα αναλυθεί η συγκεκριμένη τεχνολογία και θα αποδειχθεί πως συνδέονται τα ad hoc δίκτυα με τη συγκεκριμένη επιτροπή. Έπειτα θα δούμε πως λειτουργεί ένα τέτοιο δίκτυο, πως μπορεί να εγκατασταθεί σε υπολογιστή έτσι ώστε να μπορούν να επικοινωνήσουν μεταξύ τους. Θα γίνει αναλυτική αναφορά για τα πρωτόκολλα δρομολόγησης που χρησιμοποιούν τα ad hoc δίκτυα, θα αναλυθούν λεπτομερώς έτσι ώστε να κατανοηθούν πλήρως και με τη βοήθεια εικόνων. Ένα σημαντικό κομμάτι σε κάθε δίκτυο και εφαρμογή είναι η ασφάλειά τους, κάθε πρωτόκολλο που χρησιμοποιείται παρουσιάζει διάφορες αδυναμίες που πρέπει να προσεχθούν έτσι ώστε να μην δημιουργηθεί πρόβλημα στη σωστή λειτουργία του δικτύου. Θα παρουσιασθούν τα είδη των επιθέσεων και πως μπορούν αυτές να αντιμετωπισθούν από κάποιον διαχειριστή του δικτύου. Ακόμα θα εξετασθούν οι εφαρμογές των ad hoc δικτύων, θα δούμε που συναντάμε τα συγκεκριμένα δίκτυα , τι πλεονεκτήματα υπάρχουν από τη χρήση του συγκεκριμένου δικτύου έτσι ώστε να τα επιλέξουμε για εφαρμογή. Θα παρουσιασθεί μια ανάλυση που είχε γίνει στην περιοχή του Δουβλίνου και μας δείχνει πως μπορεί να αναπτυχθεί ένα ad hoc δίκτυο κατά μήκος μιας μεγάλης απόστασης με τη χρήστη φορητών ηλεκτρονικών υπολογιστών και κινητών τηλεφώνων.

# ΕΙΣΑΓΩΓΗ

Ad hoc δίκτυο είναι ένα δίκτυο από αυτόνομες συσκευές όπως φορητοί υπολογιστές,PDA,ακόμα και κινητά οι οποίες επικοινωνούν μεταξύ τους χωρίς κάποια συγκεκριμένη δομή δικτύου. Αυτή η τεχνολογία είναι ιδιαίτερα διαδεδομένη στις ημέρες μας και χρησιμοποιείται ολοένα και περισσότερο. Πολλοί από εμάς θα έχουμε παρατηρήσει το φαινόμενο διάφοροι άνθρωποι να στέκονται στα αεροδρόμια ή σε κάποια καφετερία και να σερφάρουν στο Internet , να λαμβάνουν τα email τους και γενικά να επικοινωνούν με κάποια δίκτυο. Αυτό συμβαίνει γιατί υπάρχει κάποιο δίκτυο σε αυτούς τους χώρους και πολύ απλά ένας καινούργιος χρήστης συνδέεται στο δίκτυο ασύρματα. Τώρα τελευταία πολλοί φορητοί υπολογιστές έχουν ασύρματες κάρτες δικτύου τοποθετημένες by default πράγμα που κάνει ακόμα πιο εύκολη και πιο άνετη τη σύνδεση σε κάποιο δίκτυο.

Η σύνδεση μεταξύ δύο συσκευών σε ένα δίκτυο ad hoc δεν είναι πάντα άμεση, δηλαδή μπορεί ο κάθε χρήστης να παίζει και το ρόλο του router σε μια multihop κατάσταση. Οι χρήστες του δικτύου ad hoc μπορούν να χρησιμοποιήσουν πρωτόκολλα όπως το IEEE 802.11 για να επικοινωνούν μέσω της ίδιας συχνότητας, ή ακόμα μπορούν να χρησιμοποιήσουν την τεχνολογία Bluetooth. Επειδή η κατανάλωση ισχύος είναι άμεσα ανάλογη προς την απόσταση μεταξύ των χρηστών, άμεσες συνδέσεις μεταξύ χρηστών μπορεί να απαιτήσουν σημαντική δύναμη προκαλώντας πρόβλημα με άλλες μεταδόσεις. Για να αποφύγουμε αυτό το πρόβλημα μπορεί να χρησιμοποιηθεί η multihop μετάδοση έτσι ώστε να έχουμε επικοινωνία μέσω άλλων χρηστών του δικτύου.

# ΚΕΦΑΛΑΙΟ 1ο

# AD HOC ΔΙΚΤΥΑ

Η τεχνολογία Wireless Local Area Network εμφανίστηκε στα μέσα της δεκαετίας του 1980, κατά τη διάρκεια της δεκαετίας του ’80 και στις αρχές της δεκαετίας του ’90 η αύξηση ήταν σχετικά αργή. Στις ημέρες μας η συγκεκριμένη τεχνολογία γνωρίζει τεράστια αύξηση, ο βασικός λόγος για αυτήν την αύξηση είναι το αυξανόμενο εύρος ζώνης που πραγματοποιείται από τα IEEE 802.11 πρότυπα.
Η Motorola ανέπτυξε ένα από τα πρώτα εμπορικά συστήματα WLAN με τα Altair προιόντα της. Εντούτοις, οι πρόωρες τεχνολογίες WLAN είχαν διάφορα προβλήματα που απαγόρευσαν την κυρίαρχη χρήση του. Αυτά τα LANs ήταν καταρχήν ιδιαίτερα ακριβά, εξασφαλίζοντας χαμηλά ποσοστά στοιχείων, ήταν επιρρεπής σε ράδιο παρεμβάσεις και σχεδιάστηκαν κυρίως στις ιδιόκτητες Radio Frequency τεχνολογίες.
Η IEEE – οργανισμός ο οποίος αναπτύσσει και επικυρώνει πρότυπα για δίκτυα υπολογιστών - άρχισε το 802.11 έργο της το 1990 με σκοπό να αναπτύξει ένα μέσο έλεγχου πρόσβασης ( MAC – Medium Access Control) στο φυσικό επίπεδο PHY - Physical Layer για την ασύρματη συνδετικότητα για τους σταθερούς, φορητούς και κινούμενους σταθμούς μέσα σε μια περιοχή. Το 1997 η IEEE ενέκρινε αρχικά τα διεθνή πρότυπα διαλειτουργικότητας 802.11, κατόπιν το 1999 η IEEE πάλι επικύρωσε το 802.11a και το 802.11b ως ασύρματα πρότυπα επικοινωνίας δικτύωσης. Το 802.11a πρότυπο χρησιμοποιεί ένα πολυπλέκτη συχνότητας (Orthogonal Frequency Division Multiplexing ) για να μειώσει την παρέμβαση. Αυτή η τεχνολογία χρησιμοποιεί το φάσμα συχνότητας 5 GHz και μπορεί να επεξεργαστεί τα στοιχεία μέχρι 54 Mbps.

Η IEEE ανάπτυξε το 802.11 πρότυπο για να παράσχει την ασύρματη τεχνολογία δικτύωσης όπως το συνδεδεμένο με καλώδιο Ethernet που είναι διαθέσιμο εδώ και πολύ καιρό . Το IEEE 802.11a πρότυπο είναι το ευρύτατα υιοθετημένο μέλος της 802.11 οικογένειας, λειτουργεί στην εξουσιοδοτημένη ζώνη 5 GHz χρησιμοποιώντας την τεχνολογία OFDM. Το δημοφιλές 802.11b πρότυπο λειτουργεί στη χωρίς άδεια

2.4 GHz – 2.5 GHz βιομηχανική, επιστημονική, ιατρική (ISM - Industry, Scientific, and Medical ) ζώνη συχνότητας χρησιμοποιώντας μια άμεση τεχνολογία απλωμένου φάσματος ακολουθίας.

Η ISM ζώνη έχει γίνει δημοφιλής για τις ασύρματες επικοινωνίες επειδή είναι διαθέσιμη παγκοσμίως. Η τεχνολογία 802.11b WLAN επιτρέπει τις ταχύτητες μετάδοσης μέχρι 11 Mbits ανά δευτερόλεπτο. Αυτό την κάνει αρκετά γρηγορότερη από το αρχικό IEEE 802.11 πρότυπο ( που στέλνει τα στοιχεία μέχρι 2 Mbps) και ελαφρώς γρηγορότερη από το τυποποιημένο Ethnernet.

# ΑΡΧΙΤΕΚΤΟΝΙΚΗ IEEE 802.11

Το 802.11 ορίζει δύο στοιχεία εξοπλισμού : έναν ασύρματο σταθμό ο οποίος συνήθως είναι ένας προσωπικός υπολογιστής εφοδιασμένος με μια κάρτα δικτύου για ασύρματα δίκτυα (NIC - Network Iinterface Card)[1] και ένα σημείο πρόσβασης – Access Point , το οποίο συμπεριφέρεται σαν γέφυρα μεταξύ του ασύρματου και του ενσύρματου δικτύου. Το σημείο πρόσβασης συνήθως αποτελείται από έναν ραδιοπομπό, μια ενσύρματη κάρτα δικτύου ( π.χ. 802.3 ) και λογισμικό για γεφύρωση το οποίο να είναι συμβατό με το πρότυπο 802.1d για την γεφύρωση. Το σημείο πρόσβασης ενεργεί ως σταθμός – βάση για το ασύρματο δίκτυο συγκεντρώνοντας την δυνατότητα προσπέλασης του ενσύρματου δικτύου από πολλαπλούς ασύρματους σταθμούς. Οι ασύρματοι τερματικοί σταθμοί μπορεί να είναι δικτυακές κάρτες PCI, ISA βάσει του 802.11 ή ακόμη συσκευές ενσωματωμένες σε άλλου είδους συστήματα όπως ένα 802.11b μικροτηλέφωνο.

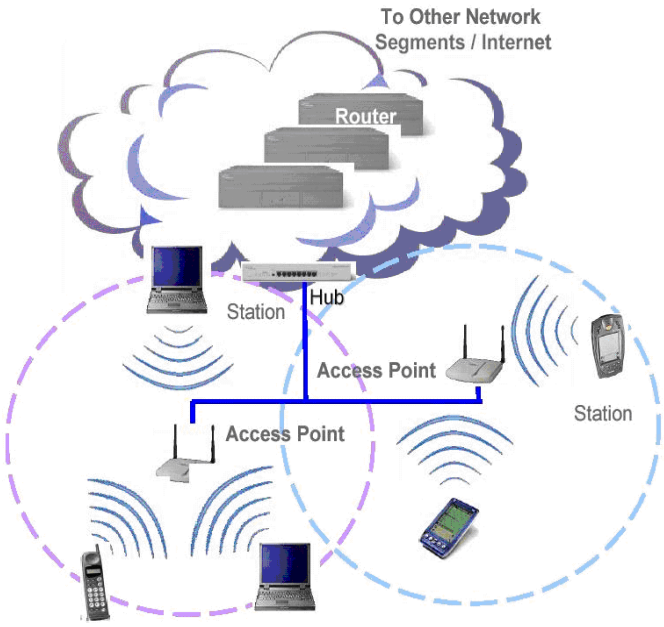
Το 802.11 πρότυπο καθορίζει δύο τρόπους λειτουργίας : λειτουργία infrastructure (υποδομής) και ad hoc λειτουργία. Στην πρώτη περίπτωση το ασύρματο δίκτυο αποτελείται από τουλάχιστον 1 σημείο πρόσβασης το οποίο συνδέεται με το καλωδιωμένο δίκτυο και ένα σύνολο από ασύρματους σταθμούς. Αυτή η σχεδίαση ονομάζεται βασικό σύνολο υπηρεσίας ( Basic Service Set – BBS). Μια επέκταση του BBS ονομάζεται Extended Service Set και είναι ένα σύνολο από δύο ή περισσότερους BBSs που σχηματίζει ένα μόνο υποδίκτυο. Εφόσον τα περισσότερα WLANs

[1] NIC : Κάρτα δικτύου η οποία βρίσκεται ενσωματωμένη σε κάθε σταθμό του δικτύου. Η κάρτα του σταθμού είναι εκείνη η οποία προετοιμάζει το πλαίσιο δεδομένων και έχει πάντα μία και μοναδική φυσική διεύθυνση η οποία είναι χρήσιμη για τη δρομολόγηση των πλαισίων δεδομένων.

απαιτούν πρόσβαση στο ενσύρματο Local Area Network λόγω του διαμοιρασμού υπηρεσιών ( διαμοιρασμός αρχείων, εκτυπωτές, σύνδεσμοι με το διαδίκτυο) θα λειτουργήσουν με τον τρόπο της infrastructure.

Η ad hoc λειτουργία ( η οποία λέγεται και peer to peer) είναι απλά ένα σύνολο από 802.11 σταθμούς που επικοινωνούν μεταξύ τους κατευθείαν χωρίς τη χρήση σημείων πρόσβασης ή οποιαδήποτε σύνδεση με το καλωδιωμένο δίκτυο. Αυτός ο τρόπος λειτουργίας είναι χρήσιμος για τη γρήγορη και εύκολη εγκατάσταση ενός ασυρμάτου δικτύου οπουδήποτε δεν υπάρχει καλωδιακή υποδομή ή δεν απαιτείται η χρήση των παραπάνω υπηρεσιών , για παράδειγμα σε ένα συνεδριακό κέντρο, σε δωμάτια ξενοδοχείου, αεροδρόμια, ή όπου η πρόσβαση στο δίκτυο δεν επιτρέπεται.

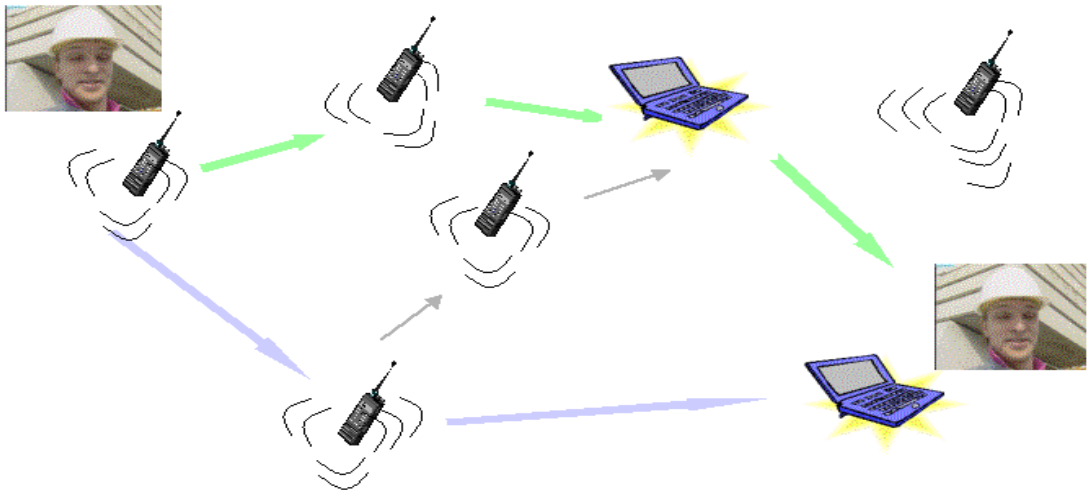
Η βασική τοπολογία ενός WLAN απεικονίζεται στην εικόνα 1.




**Εικόνα 1 : Βασική τοπολογία WLAN δικτύου**

Αν και τα περισσότερα WLANs λειτουργούν στον τρόπο και την αρχιτεκτονική υποδομής που περιγράφτηκαν προηγουμένως, μια άλλη τοπολογία είναι δυνατή επίσης, αναφερόμαστε στην ad hoc τοπολογία. Αυτή η δεύτερη τοπολογία, το ad hoc

δίκτυο, όπως αναφέραμε προηγουμένως προορίζεται για να διασυνδέσει εύκολα τις κινητές συσκευές που είναι στη ίδια περιοχή (π.χ., στο ίδιο δωμάτιο). Σε αυτήν την αρχιτεκτονική, οι σταθμοί πελατών ομαδοποιούνται σε μια ενιαία γεωγραφική περιοχή και μπορούν να εργαστούν στο Διαδίκτυο χωρίς πρόσβαση στο συνδεδεμένο με καλώδια τοπικό δίκτυο Lan ( δίκτυο υποδομής). Οι διασυνδεμένες συσκευές στο ad hoc δίκτυο αναφέρονται ως ανεξάρτητο βασικό σύνολο υπηρεσιών (IBSS). Η ad hoc τοπολογία φαίνεται στην παρακάτω εικόνα.



**Εικόνα 2 : Τοπολογία Ad Hoc δικτύου**

Η διαμόρφωση του ad hoc δικτύου είναι παρόμοια με ένα peer to peer δίκτυο γραφείου στο οποίο κανένας κόμβος δεν απαιτείται για να λειτουργήσει ως server (κεντρικός υπολογιστής). Σε ένα ad hoc WLAN , laptops, επιτραπέζιου ηλεκτρονικοί υπολογιστές και άλλες 802.11 συσκευές μπορούν να μοιραστούν τα αρχεία χωρίς την χρήση ενός AP.

# ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ IEEE 802.11

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

1. **Παρεμβολές**

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

2. **Εμβέλεια**

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

κεραιών, το επίπεδο παρεμβολών και θορύβου. Πάντως αποστάσεις αρκετών χιλιομέτρων είναι δυνατό να επιτευχθούν με πολύ καλή ποιότητα ζεύξης.

**3. Ρυθμός μετάδοσης**

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

**4. Ποιότητα επικοινωνίας**

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

**5. Συμβατότητα με το υπάρχον δίκτυο**

Τα περισσότερα WLAN έχουν προτυποποιημένο τρόπο σύνδεσης με τα υπάρχοντα ενσύρματα δίκτυα. Συστήματα διαχείρισης επιβλέπουν τους ασύρματους κόμβους όπως και οποιοδήποτε άλλο στοιχείο δικτύου.

**6. Διαλειτουργικότητα**

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

- **Διαφορετικές τεχνολογίες**
  Ένα ράδιο βασισμένο σε τεχνολογία FHSS - Frequency Hopping Spread Spectrum δεν μπορεί να συνεργαστεί με κάποιο τεχνολογίας DSSS - Direct Sequence Spread Spectrum .

- **Διαφορετικές συχνότητες**

  Προφανώς συσκευές 802.11a στους 5.7GHz δεν μπορούν να δουλέψουν μαζί με συσκευές 802.11b/g που εργάζονται στους 2.4GHz.

- **Διαφορετικές υλοποιήσεις**

  Προϊόντα διαφορετικών κατασκευαστών μπορεί να μην συνεργάζονται ή να συνεργάζονται μερικώς μεταξύ τους. Για παράδειγμα υπάρχει ένας αριθμός προϊόντων βασισμένα σε chipsets της Texas Instruments τα οποία υποστηρίζουν ένα τρόπο μετάδοσης 22Mbps. Αυτός όμως ισχύει μόνο μεταξύ συσκευών της ίδιας εταιρίας. Για μία λύση του προβλήματος της διαλειτουργικότητας δημιουργήθηκε το Wifi πιστοποιητικό

# ΥΠΗΡΕΣΙΕΣ IEEE 802.11

Η IEEE802.11 ορίζει υπηρεσίες που πρέπει να προσφέρονται, δεν ορίζει συγκεκριμένες υλοποιήσεις. Αφήνει έτσι τους κατασκευαστές να υλοποιήσουν με τον δικό τους τρόπο την κάθε υπηρεσία, αφήνοντας έτσι περιθώριο για κάτι πιο αποδοτικό.

Οι υπηρεσίες που περιγράφονται υλοποιούνται από το MAC επίπεδο και μπορούν να χωριστούν σε δύο κατηγορίες:

***Υπηρεσίες σταθμού (SS, Station Service)***

Οι υπηρεσίες αυτές υλοποιούνται σε κάθε ασύρματο σταθμό :

a)Authentication
b)Security
c)Deauthentication
d)Privacy

***Υπηρεσίες συστήματος διανομής (DSS, Distribution System Service)***

Οι υπηρεσίες αυτές υλοποιούνται μόνο στα AP - Access Point

a)Association
b)Disassociation
c)Distribution
d)Integration
e)Reassociation

## ***Υπηρεσίες σταθμού (SS, Station Service)***

Το 802.11 ορίζει έναν αριθμό από παρεχόμενες υπηρεσίες μεταξύ των σταθμών.

**Security**

Η λειτουργία της ασφάλειας είναι ευθύνη του MAC επιπέδου και περιλαμβάνει τον έλεγχο της πρόσβασης και τη λειτουργία της κωδικοποίησης και οι οποίες είναι γνωστές σαν WEP, Wired Equivalent Privacy. Η ονομασία είναι αρκετά πομπώδης και υπονοεί ότι καταφέρνει να εξασφαλίσει ισοδύναμο βαθμό ασφαλείας στο ασύρματο μέσο με αυτό του ενσύρματου.

Για τον έλεγχο της πρόσβασης κάθε AP προγραμματίζεται με ένα μοναδικό ESSID (WLAN Service Area ID). Κάθε σταθμός πρέπει να γνωρίζει το ESSID προκειμένου να συσχετιστεί με το AP. Αυτό έχει το νόημα ελέγχου αυθεντικότητας. Επίσης το AP έχει έναν πίνακα με MAC διευθύνσεις (Access Control List) , και οι σταθμοί προκειμένου να μπορούν να συνδεθούν πρέπει να έχουν την MAC τους στον πίνακα αυτό. Επίσης ο πίνακας αυτός μπορεί να περιέχει τις διευθύνσεις που αποκλείονται από την πρόσβαση.

**Authentication**

Ορίζονται διαδικασίες αυθεντικοποίησης ώστε να ελεγχθεί η πρόσβαση στο WLAN. Ο σκοπός της αυθεντικοποίησης είναι να παρέχει έλεγχο πρόσβασης όμοιο με αυτόν στα ενσύρματα LAN.

Παρέχει ένα μηχανισμό για ένα σταθμό να προσδιορίζει άλλον. Χωρίς απόδειξη της ταυτότητας του ένας σταθμός δεν επιτρέπεται να χρησιμοποιεί το WLAN. Όλοι οι 802.11 σταθμοί είτε είναι μέρος ενός ανεξάρτητου BSS – Basic Service Set ή ESS - Extended Service Set δικτύου πρέπει να χρησιμοποιήσουν την υπηρεσία αυτή πριν πριν επικοινωνήσουν με άλλο σταθμό.

Ορίζονται δύο τύποι αυθεντικοποίησης:

- **Open system authentication**

Είναι ο εξ' ορισμού τρόπος, είναι πολύ απλός και έχει δύο βήματα. Πρώτα ο σταθμός που θέλει να κάνει την αυθεντικοποίηση στέλνει ένα πλαίσιο αυθεντικοποίησης το οποίο περιέχει την ταυτότητα του. Ο άλλος σταθμός στέλνει πίσω ένα πλαίσιο που περιέχει την πληροφορία αναγνώρισης ή μη της ταυτότητας του αποστολέα.

- **Shared key authentication**

Ο κάθε σταθμός έχει λάβει ένα κρυφό κλειδί, μέσω ενός καναλιού το οποίο είναι ανεξάρτητο του 802.11 δικτύου. Οι σταθμοί κάνουν αυθεντικοποίηση μέσω της κοινής γνώσης του κρυφού κλειδιού. Η υλοποίηση αυτή απαιτεί την κρυπτογράφηση μέσω αλγορίθμου WEP, Wired Equivalent Privacy.

**De-authentication**

Η υπηρεσία αυτή αφορά την απομάκρυνση ενός σταθμού που είχε προηγούμενα αυθεντικοποιηθεί από το δίκτυο. Για να αποκτήσει πάλι ο σταθμός πρόσβαση πρέπει να επαναληφθεί η διαδικασία αυθεντικοποίησης. Το μήνυμα από-αυθεντικοποίησης έχει το νόημα ειδοποίησης και δεν μπορεί να απορριφθεί. Το αντίστοιχο πλαίσιο μπορεί να σταλεί από ένα σταθμό ή από το AP.

**Privacy**

Το πρότυπο προτείνει για την κωδικοποίηση των δεδομένων τη χρήση κλειδιού μήκους 40-bit. Η υπηρεσία αυτή είναι προαιρετική. Ο αλγόριθμος είναι ο RC4 PRNG - Pseudo Random Number Generator από την RSA Data Security. Όλα τα δεδομένα που στέλνονται και λαμβάνονται μεταξύ του AP και των συσχετιζόμενων σταθμών

του, έχουν κωδικοποιηθεί με αυτό το κλειδί. Επιπρόσθετα όταν ένας σταθμός προσπαθήσει να συσχετιστεί με ένα AP, το AP του στέλνει ένα κωδικοποιημένο πακέτο, ο σταθμός πρέπει κωδικοποιήσει την σωστή απάντηση χρησιμοποιώντας το κλειδί του ώστε να κερδίσει πρόσβαση στο δίκτυο.

Η υπηρεσία αυτή έχει σκοπό να παρέχει ένα ισοδύναμο επίπεδο προστασίας με αυτό που παρέχεται στα ενσύρματα δίκτυα, όπου η φυσική πρόσβαση είναι περιορισμένη. Παρέχει προστασία στα δεδομένα στο κομμάτι της διαδρομής τους στο ασύρματο μέσο. Δεν παρέχει πλήρη προστασία από άκρο σε άκρο μεταξύ εφαρμογών που λειτουργούν σε ένα μικτό δίκτυο. Στο ασύρματο δίκτυο όλοι ο σταθμοί καθώς και άλλες συσκευές μπορούν να αφουγκραστούν τα δεδομένα που ανταλλάσσονται, και έτσι να θέσουν σημαντικά προβλήματα ασφαλείας στο δίκτυο. Το πρότυπο προσφέρει μία υπηρεσία η οποία αυξάνει την ασφάλεια του δικτύου και την κάνει παρόμοια με αυτή ενός ενσύρματου δικτύου. Έτσι κωδικοποιεί τα πακέτα δεδομένων καθώς και κάποια πακέτα διαχείρισης με ένα αλγόριθμο βασισμένο στον αλγόριθμο WEP, Wired Equivalent Privacy του 802.11

Πέρα από τις υπηρεσίες ασφαλείας δευτέρου επιπέδου, μπορεί να χρησιμοποιηθούν και υπηρεσίες ανωτέρων επιπέδων για έλεγχο της πρόσβασης και κωδικοποίηση, όπως το IPsec - Internet Protocol Security ή κωδικοποίηση επιπέδου εφαρμογής. Αυτές οι τεχνολογίες ανωτέρων επιπέδων μπορεί να δημιουργήσουν ένα δίκτυο ασφαλές από άκρο σε άκρο, που να περιλαμβάνει ασύρματες και ενσύρματες τεχνολογίες.

## ***Υπηρεσίες συστήματος διανομής (DSS, Distribution System Service)***

**Association**

Υπηρεσία με την οποία δημιουργείται μία λογική σύνδεση μεταξύ ενός ασύρματου σταθμού και ενός AP. Κάθε σταθμός σχετίζεται με ένα AP, πριν του επιτραπεί να

στείλει δεδομένα μέσω του AP προς το DS- Distribution system[2]. Η σύνδεση αυτή είναι απαραίτητη έτσι ώστε το DS να γνωρίζει που και πως θα παραδώσει δεδομένα στον ασύρματο σταθμό. Ο ασύρματος σταθμός επικαλείται την υπηρεσία αυτή μόνο μία φορά κατά την είσοδο του στο BSS. Κάθε σταθμός σχετίζεται με μόνο ένα AP και ένα AP μπορεί να σχετιστεί με πολλούς σταθμούς.

**Disassociation**

Υπηρεσία που σκοπό έχει να επιβάλλει σε σταθμό να εγκαταλείψει μία συσχέτιση με ένα AP ή για ένα σταθμό να ενημερώσει το AP ότι δεν χρειάζεται πλέον τις υπηρεσίες του DS. Όταν ένας σταθμός αποσυσχετιστεί, πρέπει να ξεκινήσει μία καινούργια συσχέτιση με ένα AP. Ένα AP μπορεί να αναγκάσει ένα ή περισσότερους σταθμούς να απομακρυνθούν, λόγω περιορισμένων πόρων ή γιατί το AP απομακρύνεται από το δίκτυο. Όταν ο σταθμός ενημερωθεί ότι δεν θα έχει πλέον τις υπηρεσίες ενός AP, μπορεί να επικαλεστεί την υπηρεσία αποσυσχέτισης ώστε να ειδοποιήσει το AP ότι η λογική σύνδεση μεταξύ τους δεν απαιτείται πλέον. Οι σταθμοί πρέπει να αποσυσχετίζονται όταν αφήνουν το δίκτυο. Η αποσυσχέτιση έχει τη μορφή ειδοποίησης και μπορεί να σταλεί από οποιοδήποτε από τα συσχετιζόμενα μέρη και κανένα από τα δύο δεν μπορεί να την αρνηθεί.

**Distribution**

Η διανομή είναι βασική υπηρεσία η οποία παρέχεται από έναν 802.11 σταθμό. Ο σταθμός χρησιμοποιεί την υπηρεσία κάθε φορά που στέλνει ένα MAC πλαίσιο προς το DS. Το DS αναλαμβάνει τη διανομή του χρησιμοποιώντας την πληροφορία που έχει αποκτήσει με τις υπηρεσίες συσχέτισης. Ο σταθμός πρέπει να έχει συσχετιστεί με ένα AP ώστε να γίνει η προώθηση των πλαισίων σωστά

**Re-association**

Η επανασυσχέτιση επιτρέπει σε ένα σταθμό να αλλάξει τη τρέχουσα συσχέτιση του με ένα AP. Είναι παρόμοια υπηρεσία με τη συσχέτιση με τη διαφορά ότι περιέχει πληροφορία για το AP στο οποίο ο σταθμός ήταν πριν συσχετισμένος. Ένας σταθμός

[2] DS - Distribution System : Ορίζεται επίσης σαν σύστημα διανομής (DS, Distribution System) το δίκτυο μεταφοράς (συνήθως ενσύρματο) που διασυνδέει τα AP μεταξύ τους καθώς και με τα υπόλοιπα δίκτυα . Το πρότυπο δεν ορίζει τη μορφή του, έτσι μπορεί να είναι ένα ενσύρματο δίκτυο ethernet 803.2, κάποιο ασύρματο ειδικής μορφής είτε μπορεί και να είναι και ασύρματο 802.11, Ad-Hoc.

χρησιμοποιεί την υπηρεσία αυτή καθώς μετακινείται διαρκώς σε ένα ESS δίκτυο, χάνει την επαφή με το AP με το οποίο είχε συσχετιστεί και χρειάζεται να συσχετιστεί με κάποιο καινούργιο. Με την υπηρεσία αυτή. Στέλνοντας πληροφορία για το προηγούμενο AP με το οποίο είχε συσχετιστεί, το καινούργιο AP μπορεί να επικοινωνήσει με το προηγούμενο και να αποκτήσει τα πακέτα τα οποία μπορεί να έχουν παραμείνει εκεί προς παράδοση στον σταθμό. Η υπηρεσία επανασυσχέτισης αρχικοποιείτε πάντα από τον σταθμό

**Integration**

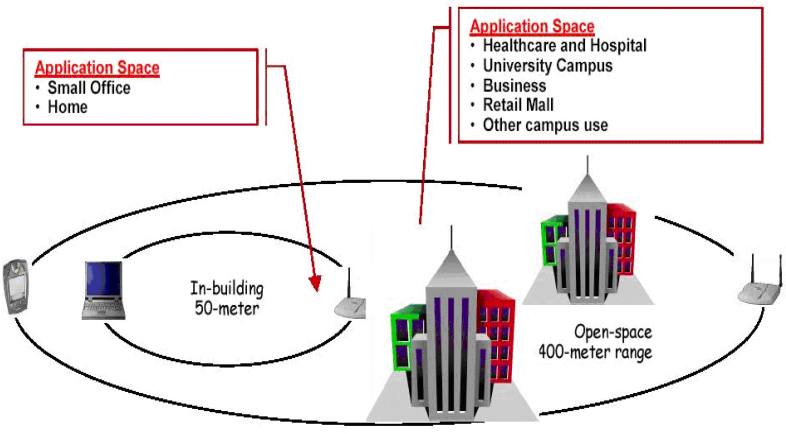
Η υπηρεσία αυτή συνδέει ένα δίκτυο 802.11 WLAN σε άλλα LANs ενσύρματα ή ασύρματα. Ένα portal είναι αυτό που υλοποιεί την υπηρεσία αυτή. Τυπικά βρίσκεται σε ένα AP, μπορεί όμως και να είναι τμήμα ενός διαφορετικού δικτύου. Η υπηρεσία αυτή μεταφράζει πλαίσιο 802.11 σε πλαίσια που μπορούν να μεταδοθούν σε άλλο δίκτυο και το ανάστροφο.

# ΣΥΣΤΑΤΙΚΑ ΜΕΡΗ ΕΝΟΣ WLAN

Ένα WLAN περιλαμβάνει δύο τύπους εξοπλισμών: ένα ασύρματο σταθμό και ένα σημείο πρόσβασης ( access point). Ένας σταθμός ή ένας πελάτης είναι χαρακτηριστικά ένα laptop ή ένας προσωπικός υπολογιστής ( PC) με ασύρματη κάρτα NIC. Ένας πελάτης WLAN μπορεί επίσης να είναι ένας υπολογιστής γραφείου ή μια φορητή συσκευή ( π.χ. PDA , ή κάποια συσκευή όπως ένας ανιχνευτής κωδικών – barcode scanner)**.** Τα ασύρματα laptop και οι ασύρματοι προσωπικοί υπολογιστές που έχουν την ασύρματη τεχνολογία είναι ίδια με τα απλά laptop και προσωπικούς υπολογιστές με τη διαφορά ότι χρησιμοποιούν ασύρματες NIC κάρτες για να συνδεθούν σε κάποιο δίκτυο με τον ασύρματο αυτό τρόπο. Η ασύρματη κάρτα NIC συνδέεται συνήθως στην PCMCIA θύρα του υπολογιστή ή ακόμα και στη USB θύρα αν ένας υπολογιστής είναι πιο καινούργιος. Τα NICs χρησιμοποιούν τα ράδιο σήματα για να εγκαταστήσουν τις συνδέσεις στο WLAN. Το Access Point, που ενεργεί ως γέφυρα μεταξύ των ασύρματων και συνδεδεμένων με καλώδιο δικτύων, χαρακτηριστικά περιλαμβάνει ένα ραδιόφωνο, μια συνδεδεμένη με καλώδιο διεπαφή δικτύων όπως το 802.3 και το λογισμικό γεφυρώματος. Το AccessPoint λειτουργεί ως

σταθμός βάσεων για το ασύρματο δίκτυο, που αθροίζει τους πολλαπλάσιους ασύρματους σταθμούς επάνω στο συνδεμένο με καλώδιο δίκτυο.

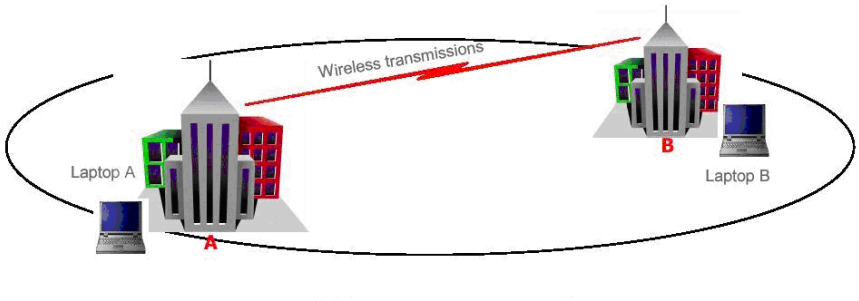
Η αξιοπιστία κάλυψης για τα 802.11 WLANs δίκτυα εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του ποσοστού στοιχείων που απαιτούνται και της ικανότητας, τις πηγές παρέμβασης RF, της φυσικής περιοχής και χαρακτηριστικών, δύναμης, συνδετικότητας, και χρήσης κεραιών. Η θεωρητική εμβέλεια είναι από 29 μέτρα (για 11 Mbps) σε μια κλειστή περιοχή γραφείων σε 485 μέτρα (για 1 Mbps) σε μια ανοικτή περιοχή. Εντούτοις, μέσω της εμπειρικής ανάλυσης, η χαρακτηριστική εμβέλεια για τη συνδετικότητα του 802.11 εξοπλισμού είναι περίπου 50 μέτρα σε εσωτερικό χώρο.
Μια εμβέλεια 400 μέτρων, σχεδόν 1/4 μίλι, κάνει WLAN την ιδανική τεχνολογία για πολλές εφαρμογές πανεπιστημιουπόλεων. Είναι σημαντικό να αναγνωριστεί ότι οι ειδικές κεραίες υψηλού-κέρδους μπορούν να αυξήσουν την εμβέλεια σε περισσότερα μίλια. Αυτό φαίνεται και στην παρακάτω εικόνα.




**Εικόνα 3 : Συστατικά μέρη ενός WLAN**

Τα Access Points μπορούν επίσης να παράσχουν μια λειτουργία γεφυρώματος-bridging. Το γεφύρωμα συνδέει δύο ή περισσότερα δίκτυα και επιτρέπει σε αυτά να επικοινωνήσουν, να αλλάξουν τη κυκλοφορία του δικτύου. Το γεφύρωμα περιλαμβάνει είτε από σημείο σε σημείο είτε πολυσημειακή διαμόρφωση. Σε μια από σημείο σε σημείο αρχιτεκτονική, δύο LANs συνδέονται το ένα με το άλλο μέσω του αντίστοιχου LAN Access Point. Στο πολυσημειακό γεφύρωμα, ένα υποδίκτυο στο τοπικό LAN συνδέεται με διάφορα άλλα υποδίκτυα το σε ένα άλλο τοπικό LAN μέσω κάθε AccessPoint υποδικτύου. Παραδείγματος χάριν, εάν ένας υπολογιστής στο υποδίκτυο A θέλει να επικοινωνήσει με τους υπολογιστές στα υποδίκτυα B, C, και D, το AccessPoint του υποδικτύου A θα συνδεθεί με τα αντίστοιχα AccessPoints του B,C,D αντίστοιχα.

Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν το γεφύρωμα για να συνδέσουν LANs μεταξύ των διαφορετικών κτηρίων στις εταιρικές πανεπιστημιουπόλεις. Οι συσκευές AccessPoints γεφυρώματος τοποθετούνται χαρακτηριστικά πάνω από τα κτήρια για να επιτύχουν τη μεγαλύτερη υποδοχή κεραιών.
Η χαρακτηριστική απόσταση πέρα από την οποία ένα AccessPoint μπορεί να συνδεθεί ασύρματα με ένα άλλο με τη βοήθεια του γεφυρώματος είναι περίπου 2 μίλια. Αυτή η απόσταση μπορεί να ποικίλει ανάλογα με διάφορους παράγοντες συμπεριλαμβανομένου του συγκεκριμένου δέκτη ή του πομποδέκτη που χρησιμοποιείται. Η παρακάτω εικόνα νούμερο 4 επεξηγεί το από σημείο σε σημείο γεφύρωμα μεταξύ δύο LANs. Στο παράδειγμα μας, τα στοιχεία ασύρματα διαβιβάζονται από το laptop A στο laptop B, από ένα κτήριο στο επόμενο, χρησιμοποιώντας το τοποθετημένο AccessPoint κάθε κτιρίου κατάλληλα**.** Το laptop A συνδέεται με το πιο κοντινό AccessPoint μέσα στο κτίριο A. Το λαμβάνον AP στο κτίριο A διαβιβάζει έπειτα τα στοιχεία (πάνω από το ενσύρματο τοπικό LAN) στη γέφυρα AP που είναι τοποθετημένη στη στέγη του κτιρίου. Εκείνη η γέφυρα AccessPoint διαβιβάζει έπειτα τα στοιχεία στη γέφυρα στο κοντινό κτίριο B. Η γέφυρα AccessPoint του κτιρίου τότε στέλνει τα στοιχεία μέσω του ενσύρματου δικτύου στο laptop B.
Την δομή που προηγουμένως σχολιάσαμε την βλέπουμε στην παρακάτω εικόνα:




Εικόνα 4 : Επικοινωνία LAN

# ΚΕΦΑΛΑΙΟ 2ο

# ΛΕΙΤΟΥΡΓΙΑ AD HOC ΔΙΚΤΥΟΥ

## ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΕΝΑ AD HOC ΔΙΚΤΥΟ

Η τεχνολογία ad hoc σχεδιάστηκε για να εξαφανιστεί τελείως η χρήση των σημείων πρόσβασης – Access Points. Για να καταλάβουμε πόσο χρήσιμη είναι η τεχνολογία ad hoc ας φανταστούμε ένα σενάριο στο οποίο κάποια ομάδα διάσωσης φτάνει σε κάποιο σημείο καταστροφής στο οποίο πρέπει να δουλέψουν αμέσως, αυτό σημαίνει ότι δεν έχουν την πολυτέλεια του χρόνου να εγκαταστήσουν κάποια δομή, απλά θέλουν να επικοινωνούν ο ένας με τον άλλον κάνοντας ταυτόχρονα τη δουλειά για την οποία έχουν έρθει.

Άρα έχουμε κάποιο σύνολο συσκευών που είναι απολύτως ανεξάρτητες μεταξύ τους και κάποιος πρέπει να βρει έναν τρόπο έτσι ώστε να επικοινωνήσουν αυτές οι συσκευές μεταξύ τους.

Ας υποθέσουμε ότι η συσκευή Α θέλει να στείλει δεδομένα στη συσκευή Β, οπότε θα συμβεί ακριβώς αυτή η διαδικασία :

- Οι συσκευές Α και η Β είναι στην ίδια ευθεία μετάδοσης η μία με τον άλλη και τότε μπορούν να επικοινωνήσουν άμεσα, σε αυτή την περίπτωση η συσκευή Α στέλνει άμεσα στοιχεία στη συσκευή Β.
- Οι συσκευές Α και Β δεν μπορούν να ακούσουν άμεσα η μία την άλλη, λόγω κάποιων παρεμβολών στο σήμα ή ακόμα και την ύπαρξη άλλων συσκευών που επηρεάζουν την απευθείας μετάδοση σε αυτή την περίπτωση η Α προσπαθεί να βρει ένα μονοπάτι μέσω άλλων γειτονικών κόμβων στη Β. Η διαδρομή που βρίσκει τον αλγόριθμο πρέπει να είναι γρήγορη και να χρησιμοποιεί όσο το δυνατόν λιγότερα πακέτα για επικοινωνία, αυτή η μέθοδος είναι γνωστή ως multi – hopping.

Ως εκ τούτου , τα πακέτα πρέπει να δρομολογηθούν μέσω multi – hopping τις περισσότερες φορές και αυτό απαιτεί τους πιο αποδοτικούς και αξιόπιστους τρόπους για εύρεση μονοπατιών στο δίκτυο.

Υπάρχουν διάφορα ζητήματα τα οποία εξετάζονται στα ah hoc δίκτυα :

1. **Η Δρομολόγηση** των πακέτων δεν είναι εύκολη υπόθεση και οι αλγόριθμοι πρέπει να φροντίσουν τις ακόλουθες πτυχές:
    - Ένας ενδιάμεσος κόμβος μπορεί να απομακρυνθεί στη μέση της μεταφοράς στοιχείων ως εκ τούτου ένα νέο μονοπάτι πρέπει να σχεδιαστεί.
    - Σε περίπτωση που η εφαρμογή επιθυμεί ποιότητα των υπηρεσιών (QoS – Quality of Service) ,κάποια πρέπει να έχει έναν μηχανισμό για να τον προβάλλει.
2. **Η διαχείριση ενέργειας** είναι ένα πολύ σημαντικό στοιχείο. Δεδομένου ότι όλες οι συσκευές επιτρέπεται να είναι κινητές, πάσχουν από τους αυστηρούς περιορισμούς ισχύος. Έτσι η διαχείριση των πόρων ισχύος και η στρατηγική ύπνου χρειάζεται να επιλυθούν. Λέγοντας στρατηγική ύπνου εννοούμε το φαινόμενο διάφορες συσκευές οι οποίες είναι συνδεδεμένες στο δίκτυο να μείνουν για μεγάλο χρονικό διάστημα ανενεργές, με αποτέλεσμα να καταναλώνεται η ενέργεια τους και να προκαλέσουν πρόβλημα στο δίκτυο.
3. **Πρόβλημα μεταφοράς από χρήστες – κόμβους,** μερικές συσκευές μπορεί να θέλουν να διαφυλάξουν τη δύναμη τους ( διαφύλαξη μπαταρίας) και αρνιούνται να δρομολογήσουν κάποια πακέτα σε άλλους κόμβους, έτσι έχουμε παρακώλυση της λειτουργείας του δικτύου. Οπότε πρέπει να παρθούν κάποιοι αυστηροί κανόνες και μέτρα τα οποία θα αποτρέψουν τέτοιες καταστάσεις οι οποίες μπορεί να καταστρέψουν τη λειτουργεία του δικτύου, για παράδειγμα μπορεί να αποβάλλεται κάποιος χρήστης ο οποίος εμποδίζει τη σωστή λειτουργεία του δικτύου.

## Εγκαθιστώντας ένα ad hod δίκτυο

Για να εγκαταστήσουμε μια ad hoc σύνδεση θα πρέπει από πλευράς συσκευών να έχουμε εγκαταστήσει μια ασύρματη 802.11 κάρτα. Αυτή η κάρτα μπορεί να είναι μια

PCMCIA στα laptops ή μια PCI κάρτα στους προσωπικούς υπολογιστές. Υπάρχουν δύο τύποι καρτών οι οποίες φαίνονται στην εικόνα 5, είναι η εξωτερική κάρτα ( η οποία συνδέεται στον υπολογιστή με τη USB σύνδεση) και η εσωτερική που προηγουμένως είπαμε πως συνδέεται στον υπολογιστή.
Η εγκατάσταση στον υπολογιστή μας των καρτών γίνεται πολύ εύκολα, αφου τις τοποθετήσουμε στο μηχάνημα, ανοίγωντας τον υπολογιστή τα Windows XP αμέσως υα αναγνωρίσουν ότι μια καινούργια συσκευή προστέθηκε στο μηχάνημα, θα μας εμφανιστεί ο οδηγός εγκατάστασης του νέου υλικού " Found new hardware wizard ", θα μας ζητηθεί να τοποθετήσουμε το cd εγκατάστασης της κάρτας μας έτσι ώστε να εγκατασταθεί σωστά, και με λίγα βήματα εγκατάστασης η κάρτα θα μας θα είναι έτοιμη για χρήση. Μετά θα πρέπει να της δηλώσουμε ότι είμαστε σε ad hoc δίκτυο, κάτι το οποίο θα εξετάσουμε αμέσως.
Στις ιδιότητες της κάρτας δικτύου μας θα πρέπει να επιλέξουμε την επιλογή " Computer to computer ( ad hoc) networks only), έπειτα θα πρέπει να δώσουμε ένα όνομα Set the Service Set ID ( SSID) το οποίο είναι μοναδικό και θα μας αναγνωρίζει στο δίκτυο το οποίο θα συνδεθούμε ( όλες οι συσκευές θα πρέπει να έχουν το ίδιο όνομα έτσι ώστε να μπορούν να αναγνωριστούν και να επικοινωνούν μεταξύ τους).

Έπειτα θα πρέπει να ενεργοποιήσουμε την επιλογή WEP , η συγκεκριμένη επιλογή χρησιμοποιεί μέθοδο κρυπτογράφησης έτσι ώστε να έχουμε μεγαλύτερη ασφάλεια στο δίκτυο, ακόμα θα καθορίσουμε και το επίπεδο κρυπτογράφησης που θα χρησιμοποιήσουμε το οποίο εκτείνεται από 64 bit εώς 256 bit. Όσο μεγαλύτερη ασφάλεια χρησιμοποιούμε τόσο πιο έμπιστο είναι το δίκτυό μας.

Αν θελήσουμε να έχουμε Internet θα πρέπει να χρησιμοποιήσουμε κάποιον δρομολογητή ή να διαμοιράσουμε σύνδεση από έναν υπολογιστή, το γνωστό Internet sharing έτσι ώστε όλοι οι υπολογιστές να έχουν πρόσβαση στο Internet.

**Εικόνα 5: Εσωτερική και εξωτερική ασύρματη κάρτα**

# ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ AD HOC ΔΙΚΤΙΟΥ

Σε αυτή την ενότητα θα περιγράψουμε τα γενικά χαρακτηριστικά των ad – hoc δικτύων:

- **Infrastructure-less or with minimum infrastructure support – Έλλειψη υποδομής ή μειωμένη δομή,** βασικά το ad hoc δίκτυο δεν έχει ή δεν υποστηρίζει κάποια δομή για τη διαχείριση του δικτύου.
- **Self - organizing and self - managing Αυτό – οργάνωση και αυτό – διαχείριση**, από τη στιγμή που δεν υποστηρίζεται κάποια δομή τότε οι συσκευές – κόμβοι πρέπει να οργανώνουν και να διαχειρίζονται το δίκτυο απο μόνες τους για να υπάρχει σωστή διαχείριση.
- **Όλες οι συσκευές είναι κινητές,** αυτό σημαίνει ότι η τοπολογία του δικτύου αλλάζει δυναμικά γιατί μπορεί εύκολα και απλά να συνδεθούν / αφαιρεθούν διάφορες κινητές συσκευές στο δίκτυο. Αυτό σημαίνει ότι ανα πάσα στιγμή αλλάζει η τοπολογία του δικτύου με την πρόσθεση ή την αφαίρεση κάποιων συσκευών, οπότε η συχνή, προσωρινή και μη ανακοινωθείσα απώλεια συνδετικότητας δικτύων είναι πολύ συνηθισμένη.
- **Wireless – Ασύρματη,** από τη στιγμή που οι συσκευές που αποτελούν το δίκτυο είναι κινητές τότε μιλάμε για ασύρματη επικοινωνία.
- **Μια συσκευή παίζει το ρόλο και του χρήστη και του δρομολογητή,** ένας χρήστης μπορεί να θέλει να συνδεθεί με μια άλλη συσκευή που είναι εκτός απλής σύνδεσης απόστασης, άρα κάποια συσκευή θα παίξει και τον ρόλο του δρομολογητή από τη στιγμή που δεν υποστηρίζεται κάποια συγκεκριμένη δομή.

- **Multi – hop,** από τη στιγμή που κάθε συσκευή μπορεί να δρομολογεί πακέτα τότε η πολύ-σύνδεση είναι δυνατή. Η πολύ-σύνδεση είναι μια επιθυμητή ικανότητα στο ad hoc δίκτυο γιατί η απλή σύνδεση δεν έχει μεγάλη απόσταση περιορίζοντας κατά συνέπεια την επικοινωνία μεταξύ των συσκευών.
- **Περιορισμός ενέργειας,** ένα πρόβλημα το οποίο έχει το ad hoc δίκτυο έχει να κάνει με τη διάρκεια λειτουργίας των κινητών συσκευών, επειδή όπως προαναφέραμε όλες οι συσκευές είναι κινητές τότε υπάρχει το πρόβλημα της ενέργειας, η πλειοψηφία των συσκευών αυτών λειτουργεί με μπαταρίες, αυτό μπορεί να προκαλέσει μεγάλο πρόβλημα επειδή οι μπαταρίες μετά από κάποιο χρονικό διάστημα τελειώνουν. Συνήθως το πρόβλημα είναι μεγαλύτερο στα laptops , όλοι γνωρίζουμε ότι η διάρκεια λειτουργίας των laptops που δεν τροφοδοτούνται με ρεύμα είναι πολύ μικρή, οπότε αν ο χώρος στον οποίο συνδεόμαστε στο δίκτυο δεν έχει κάποια πηγή ενέργειας τότε η συσκευή μετά από κάποιο χρονικό διάστημα δεν θα μπορεί να είναι συνδεδεμένη.
- **Ποικιλία συσκευών,** στο ad hoc δίκτυο μπορούν να βρεθούν όλων των ειδών συσκευές, αυτό σημαίνει ότι έχουμε ποικιλλία συσκευών, π.χ. μπορεί να συνδεθούν δύο υπολογιστές που ο ένας είναι ιδιαίτερα γρήγορος ενώ κάποιος άλλος είναι αργός, αυτό σημαίνει ότι η επικοινωνία μεταξύ των συσκευών αυτών δεν θα είναι και τόσο γρήγορη. Όταν έχεις όμως ένα ενσύρματο δίκτυο που συνήθως όλοι οι υπολογιστές που συνδέονται σε αυτό είναι ίδιας τεχνολογίας τότε η μεταφορά δεδομένων θα είναι σταθερή.

Αξίζει να παρατηρήσουμε ότι το ad hoc δίκτυο συναντάται σε δύο μορφές, στο **απλό** ad hoc δίκτυο το οποίο αποτελείται από πελάτες – χρήστες μόνο που θέλουν να αλλάζουν δεδομένα και από το **υβριδικό** δίκτυο ( hybrid) το οποίο αποτελείται και από συσκευές πελάτες και από συσκευές διασύνδεσης, αυτό σημαίνει ότι πολλές συσκευές μεταφέρουν και δεδομένα και σε άλλες συσκευές ,παίζουν δηλαδή το ρόλο του δρομολογητή. Το υβριδικό δίκτυο συναντάται περισσότερο.

# ΣΥΝΤΗΡΗΣΗ ΙΣΧΥΟΣ

Προηγουμένως αναφερθήκαμε στην ενέργεια που καταλάνουν οι συσκευές – χρήστες. Η δύναμη είναι ένας πολύτιμος πόρος στις κινητές συσκευές, και η δικτύωση είναι μία από τις μεγαλύτερες διαδικασίες κανατάλωσης ενέργειας.

Σύμφωνα με ένα πείραμα από τους Kravets και Krishman το 1998, η κατανάλωση ισχύος προκαλούμενη από τις σχετικές με την δικτύωση δραστηριότητες είναι περίπου 10% της γενικής κατανάλωσης ισχύος ενός φορητού υπολογιστή laptop. Αυτός ο αριθμός αυξάνεται μέχρι 50 % στις φορητές συσκευές. Ο στόχος για να σώσουμε την ισχύ ενός δικτύου είναι να μειώσουμε την ενέργεια που καταναλώνουν οι χρήστες, η τακτική είναι να έχουμε σε ανενεργή κατάσταση συσκευές οι οποίες δεν κάνουν κάποια εργασία για κάποιο χρονικό διάστημα.

Βασικός μας στόχος είναι να μεγιστοποιηθεί η διάρκεια ζωής του δικτύου μέσα από τη λειτουργεία των συσκευών.

Υπάρχουν δύο σενάρια σε σχέση με την ενέργεια στα ad hoc δίκτυα,1) η ενέργεια είναι μια ακριβή αλλά μη περιορισμένη πηγή (οι μπαταρίες μπορούν να επαναφορτιστούν ή να εγκατασταθούν πολύ εύκολα),2) η ενέργεια είναι περιορισμένη / πεπερασμένη. Το πρώτο σενάριο του οποίου η ενέργεια είναι ακριβή είναι αληθινό στα δίκτυα κοινοτήτων και τα επιχειρηματικά δίκτυα, κατα συνέπεια ο στόχος στα δίκτυα που ανήκουν σε αυτό το σενάριο είναι να ελαχιστοποιηθεί η συνολική ενέργεια που καταναλώνεται ανά πακέτο για να το διαβιβάσει από την πηγή στον προορισμό, χωρίς να εξετάζει το υπόλοιπο ενέργειας του ενδιάμεσου κόμβου.

Το σενάριο της πεπερασμένης ενέργειας είναι αληθινό στο δίκτυο αισθητήρων. Ο στόχος είναι έτσι να μεγιστοποιηθεί η διάρκεια ζωής δικτύων εκτός από τη συντήρηση της ενέργειας και για τους ενδιάμεσους κόμβους. Η υπόλοιπη ενέργεια των ενδιάμεσων κόμβων πρέπει έτσι να εξεταστεί.

# ΚΕΦΑΛΑΙΟ 3ο

# ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ AD HOC ΔΙΚΤΥΟΥ

Η δρομολόγηση στα ad hoc δίκτυα επιτρέπει τη συνδετικότητα μεταξύ ενός συνόλου κινητών ασυρμάτων συσκευών, απαιτεί από τις ασύρματες συσκευές να ενεργούν και ως δρομολογητές για να προωθούν κάποιο πακέτο στον επόμενο χρήστη. Τα πρωτόκολλα δρομολόγησης πρέπει να είναι δυναμικά έτσι ώστε να αντιδρούν σε κάποια αλλαγή της δομής του δικτύου, γιατί πολύ συχνά συσκευές προστίθενται ή φεύγουν από το ad hoc δίκτυο, να έχουν χαμηλή κατανάλωση σε ενέργεια, εύρος δικτύου και δύναμη, να είναι ευέλικτα στον αριθμό των συσκευών, επειδή μπορεί σε κάποιο ad hoc δίκτυο να συνδεθούν πολλές συσκευές να μπορεί να τις εξυπηρετεί χωρίς κανένα πρόβλημα όπως θα εξυπηρετούσε λιγότερες συσκευές.

## *ΠΑΡΑΔΟΣΙΑΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ*

Πολλά πρωτόκολλα βασίζονται στις παραδοσιακές μεθόδους αλγορίθμων, με πολλές όμως τροποποιήσεις έτσι ώστε να βελτιστοποιούν τις αποδόσεις τους σε δυναμικά περιβάλλοντα. Στη δρομολόγηση link- state, κάθε συσκευή σχηματίζει μια τοπική κατάσταση της τοπολογίας του δικτύου και διατηρεί πίνακες δρομολόγησης που ορίζονται από τη κάθε γειτονική συσκευή. Κάθε φορά που κάποια συσκευή λαμβάνει κάποια πληροφορία, οι συσκευές υπολογίζουν τον προτιμητέο γείτονα για επικοινωνία με τις άλλες συσκευές χρησιμοποιώντας το πιο σύντομο μονοπάτι αλγόριθμου, όπως τον αλγόριθμο shortest path first (SPF) [3]. Αν για κάποιο λόγο η τοπολογία του δικτύου αλλάξει, μερικές συσκευές μπορεί να χρησιμοποιήσουν την ξεπερασμένη σύνδεση και οι βρόχοι δρομολόγησης μπορούν να αλλάξουν. Εντούτοις, αυτοί οι βρόγχοι έχουν μικρή διάρκειας ζωή από τη στιγμή που επιδιορθώνονται όταν οι αναβαθμισμένες πληροφορίες δρομολόγησης διαβιβάζονται.

[3] SPF – Shortest path first : Αλγόριθμος σύμφωνα με τον οποίο η πιο κοντινή διαδρομή επιλέγεται για δρομολόγηση.

Στον distance – vector αλγόριθμο δρομολόγησης. Όπως ο Distributed Bellman –Ford (DBF) αλγόριθμος, οι συσκευές υπολογίζουν την απόσταση προς κάθε προορισμό μέσω καθενός από τους γείτονες. Για να μειώσουν το σύνολο των πληροφοριών που διαβιβάζονται στο δίκτυο, οι συσκευές περιοδικά ανακοινώνουν μόνο την πιο σύντομη πληροφορία αντίθετα από την πλήρους link – state πληροφορίας. Στον distance – vector αλγόριθμο η έλλειψη μιας λεπτομερούς άποψης της τοπολογίας του δικτύου μπορεί να οδηγήσει στον σχηματισμό μακράς διάρκειας ζωής των βρόχων.

Στον source routing αλγόριθμο την απόφαση για την πλήρη πορεία που τα πακέτα πρέπει να ακολουθήσουν για να φθάσουν στον προορισμό τους λαμβάνεται στην πηγή. Χρησιμοποιώντας αυτή τη μέθοδο, οι κόμβοι απαιτήσεων επεξεργασίας ελαχιστοποιούνται και τα προβλήματα επανάληψης αποφεύγονται. Το κυριότερο μειονέκτημα είναι ότι κάθε πακέτο πρέπει να φέρει τις πλήρης πληροφορίες δρομολόγησης στην κεφαλή του, καταναλώνοντας περισσότερο εύρος ζώνης.

Τα **πρωτόκολλα δρομολόγησης** μπορούν να διαιρεθούν σε δύο κατηγορίες : τα **Table Driven Routing Protocols** και τα **On-Demand Routing Protocols**, η κύρια διαφορά τους είναι στις πληροφορίες δρομολόγησης . Στα table driven routing protocols οι πληροφορίες δρομολόγησης διατηρούνται σε κάθε συσκευή ενώ στα on-demand πρωτόκολλα οι δρομολογήσεις δημιουργούνται μόνο όταν το επιθυμούν κάποιες συσκευές.

## ***TABLE DRIVEN ROUTING PROTOCOLS***

Στα συγκεκριμένα πρωτόκολλα , η διαδικασία δρομολόγησης εκτελείται χρησιμοποιώντας μερικά στοιχεία που είναι αποθηκευμένα στους πίνακες. Κάθε χρήστης διατηρεί έναν ή περισσότερους πίνακες που περιέχουν τις πληροφορίες δρομολόγησης σε κάθε άλλο κόμβο στο δίκτυο. Όλοι οι κόμβοι ενημερώνουν αυτούς τους πίνακες έτσι ώστε να διατηρηθεί μια συνεπής και ενημερωμένη η άποψη του δικτύου. Όταν η τοπολογία του δικτύου αλλάζει οι χρήστες αναπαραγάγουν μηνύματα σε όλο το δίκτυο προκειμένου να διατηρηθούν συνεπής και ενημερωμένες οι πληροφορίες δρομολόγησης σε ολόκληρο το δίκτυο. Αυτά τα πρωτόκολλα

δρομολόγησης διαφέρουν στη μέθοδο με την οποία οι πληροφορίες αλλαγής τοπολογίας διανέμονται μέσα στο δίκτυο και στον αριθμό των απαραίτητων πινάκων δρομολόγησης.

Τα table driven routing protocols είναι τα εξής **: *Destination Sequenced Distance Vector ( DSDV) , Wireless Routing Protocol (WRP) , Global State Routing ( GSR) , Fisheye State Routing (FSR), Hierarchical State Routing (HSR), Zone – based Hierarchical Link State Routing Protocol (ZHLS), Clusterhead Gateway Switch Routing Protocol (CGSR) .***

# DESTINATION SEQUEENCED DISTANCE VECTOR PRTOCOL ( DSDV)

Το DSDV πρωτόκολλο είναι σχεδιασμένο με βάση τον κλασσικό Bellman-Ford αλγόριθμο, τροποποιημένος κατάλληλα στον σχηματισμό της δρομολόγησης των βρόχων και για να παράσχει τη γρηγορότερη απάντηση στις αλλαγές της τοπολογίας. Οι πίνακες δρομολόγησης αποθηκεύονται σε κάθε συσκευή και περιέχουν πληροφορίες για όλους τις διαθέσιμους προορισμούς. Σε κάθε πίνακα δρομολόγησης τοποθετείται ένας αριθμός ακολουθίας ο οποίος δημιουργείται από τον σταθμό προορισμού. Όταν τα πακέτα στοιχείων πρέπει να διαβιβαστούν από έναν ενδιάμεσο κόμβο, επιλέγει την διαδρομή με τον πιο πρόσφατο αριθμό ακολουθίας.

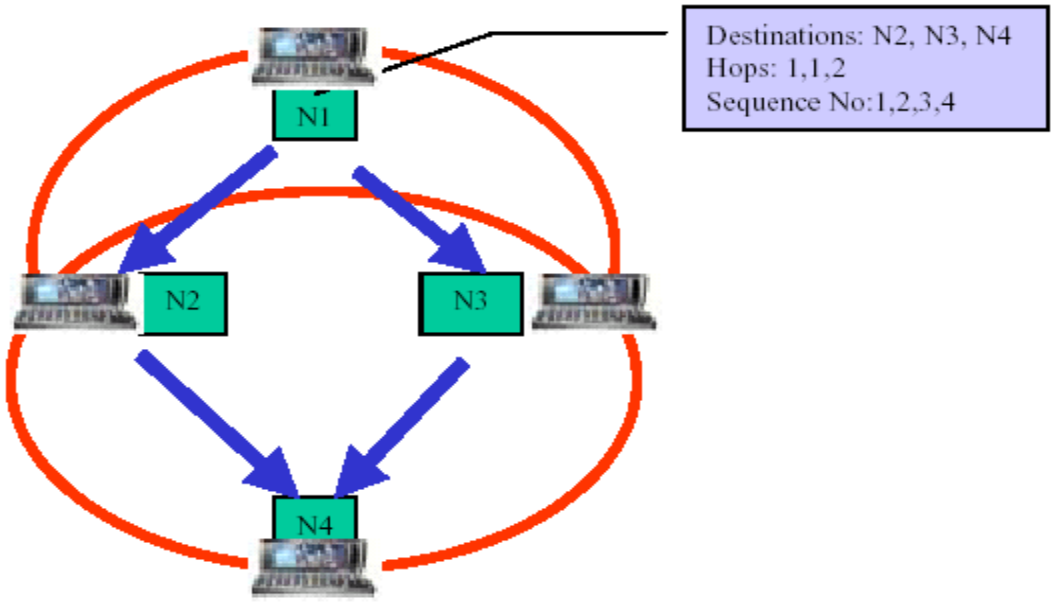
Χρησιμοποιώντας αυτήν την διαδικασία, οι παλαιότερες διαδρομές, που μπορεί να είχαν σπάσει, αποκλείονται, και έτσι ο σχηματισμός της δρομολόγησης των βρόχων αποφεύγεται. Σπασμένες συνδέσεις που είναι αποτέλεσμα μετακίνησης συσκευών του δικτύου μπορεί να καθορίζονται από το πρωτόκολλο DSDV αν καθόλου πακέτα έχουν φτάσει από κάποια γειτονική συσκευή.

Όταν μια σύνδεση σπάσει ορίζεται ένας αριθμός ακολουθίας που είναι μεγαλύτερος από τον προηγούμενο. Οι τροποποιημένες διαδρομές διαβιβάζονται αμέσως, όπως οι πληροφορίες για τις σπασμένες συνδέσεις θεωρούνται ως σημαντική αλλαγή τοποθεσίας.

Γενικά μπορούμε να πούμε ότι το πρωτόκολλο DSDV εξαρτάται από : **την ανταλλαγή συχνότητας και τον αριθμό των συσκευών που είναι συνδεδεμένοι στο δίκτυο**. Μπορούμε όμως να πούμε ότι είναι ανεξάρτητο από την κίνηση στο δίκτυο.

Στην παρακάτω εικόνα 6 βλέπουμε ένα δίκτυο το οποίο αποτελείται από τέσσερις χρήστες ( N1 , N2, N3, N4). Οι συσκευές 1,2 και 3 είναι σε μια περιοχή κάλυψης και οι συσκευές 2,3 και 4 είναι σε άλλη περιοχή κάλυψης.

Το σχήμα 1 παρουσιάζει ότι ένα δίκτυο αποτελείται από τέσσερις κόμβους (N1, N2, N3, και N4). Οι κόμβοι 1, 2 και 3 είναι σε μια περιοχή και οι κόμβοι 2,3 και 4 σε μια άλλη περιοχή κάλυψης. Αν εξετάσουμε την συσκευή 1, έχει να δρομολογήσει στη συσκευή 2, στη συσκευή 3 και δύο δρομολογήσεις στη συσκευή 4, μία μέσω της συσκευής 2 και άλλη μία μέσω της συσκευής 3. Οπότε η συσκευή 1 έχει ένα πίνακα δρομολόγησης που περιέχει όλες τις πληροφορίες για τις τέσσερις συσκευές όπως φαίνονται στην εικόνα 6.




**Εικόνα 6 : DSDV Πρωτόκολλο**

# WIRELESS ROUTING PROTOCOL (WRP)

Στο συγκεκριμένο πρωτόκολλο κάθε συσκευή διατηρεί τέσσερις πίνακες : **Distance Table, Routing Table , Link – Cost Table και Message Retransmission list ( MRL)**. Ο **distance table** δείχνει τον αριθμό των hops ανάμεσα σε μια συσκευή και τον προορισμό της. Ο **routing table** δείχνει τον επόμενο hop συσκευής. Ο **link – cost**

**table** απεικονίζει την καθυστέρηση που συνδέεται με μια σύνδεση. Το **MRL** περιέχει τον αριθμό ακολουθίας σε ένα ενημερωμένο μήνυμα, ένα μετρητή αναμετάδοσης και ένα κατάλογο των αναπροσαρμογών που στέλνονται στο μήνυμα αναπροσαρμογών. Το MRL γράφει τις αναβαθμίσεις σε ένα μήνυμα αναπροσαρμογής που χρειάζεται να αναμεταδοθούν και ποιες γειτονικές συσκευές πρέπει να γνωρίσουν την αναμετάδοση.

Οι συσκευές ανταλλάσσουν πίνακες δρομολόγησης με τους γείτονές τους χρησιμοποιώντας αναβαθμισμένα μηνύματα περιοδικά έτσι όπως αλλάζουν οι συνδέσεις.

Οι κόμβοι παρουσιάζονται στον πίνακα απάντησης του μηνύματος αναπροσαρμογής που χρειάζονται να αναγνωρίσουν την παραλαβή του μηνύματος αναπροσαρμογών. Εάν δεν υπάρχει καμιά αλλαγή στον πίνακα δρομολόγησης από την τελευταία αλλαγή, απαιτείται από τον κόμβο να στέλνει ένα **Hello** μήνυμα για να εξασφαλίσει τη συνδετικότητα. Στη λήψη ενός μηνύματος αναπροσαρμογών, η συσκευή τροποποιεί τον πίνακα απόστασής του και αναζητεί για καλύτερα μονοπάτια χρησιμοποιώντας τις νέες πληροφορίες.

Οποιαδήποτε νέα διαδρομή βρίσκεται αναμεταδίδεται πίσω στους αρχικούς κόμβους έτσι ώστε και αυτοί να ενημερώσουν τους πίνακές τους. Η συσκευή επίσης ενημερώνει τον πίνακα δρομολόγησής του αν το καινούργιο μονοπάτι είναι καλύτερο από το υπάρχον μονοπάτι. Στη λήψη μιας αναγνώρισης ο κόμβος ενημερώνει το MRL του.

Όταν μια συσκευή λαμβάνει ένα **Hello** μήνυμα από έναν καινούργιο κόμβο, όπου οι καινούργιες πληροφορίες της συσκευής προστίθενται στον πίνακα δρομολόγησης της συσκευής, και η συσκευή στέλνει στο νέο κόμβο ένα αντίγραφο των πληροφοριών δρομολόγησής του.

Ένα μοναδικό χαρακτηριστικό γνώρισμα αυτού του αλγόριθμου είναι ότι ελέγχει την συνέπεια όλων των γειτόνων του κάθε φορά που ανιχνεύει μια αλλαγή στη σύνδεση οποιωνδήποτε γειτόνων του.

# CLUSTER SWICH GATEWAY ROUTING PROTOCOL (CSGR)

Στο συγκεκριμένο πρωτόκολλο οι συσκευές ομαδοποιούνται σε στοιβάδες και κάθε στοιβάδα έχει ένα ελεγμένο κεφάλι στοιβάδων. Όλοι οι κόμβοι που είναι στη σειρά

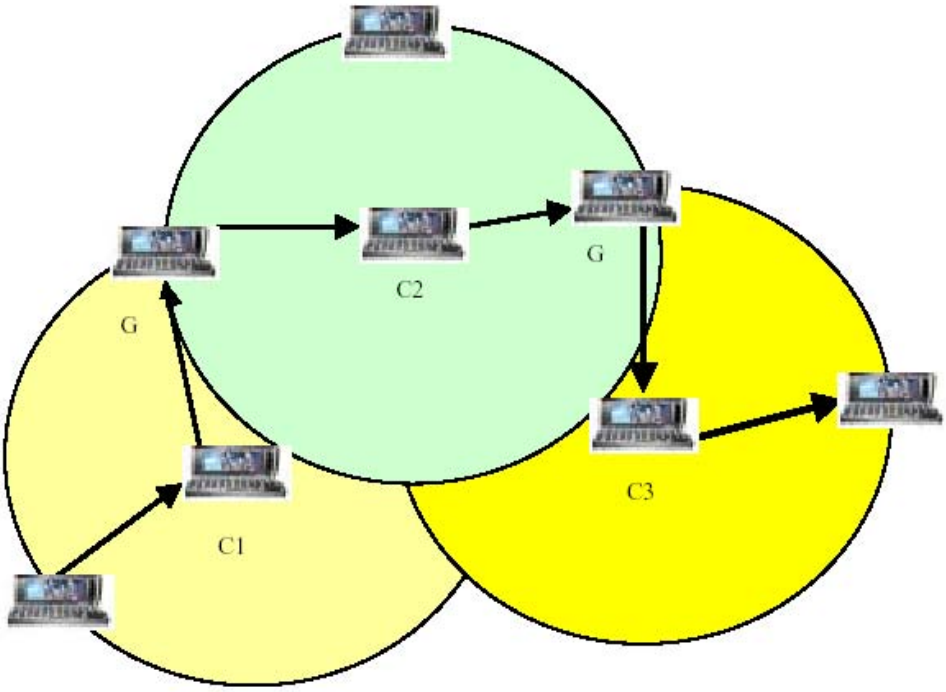
επικοινωνίας του κεφαλιού της στοιβάδας ανήκουν στη στοιβάδα του. Ένα κεφάλι στοιβάδας μπορεί να ελέγξει μια ομάδα από ad hoc χρήστες, και να παρέχει ένα κανάλι πρόσβασης, και μια κατανομή ενός εύρου ζώνης. Ένας κόμβος πυλών είναι ένας κόμβος που είναι στη σειρά επικοινωνίας σε δύο ή περισσότερες στοιβάδες κεφαλιών.

Όπως φαίνεται στη παρακάτω εικόνα 7 ένα πακέτο που στέλνεται από ένα κόμβο δρομολογείται πρώτα στο κεφάλι στοιβάδας και έπειτα το πακέτο δρομολογείται από το κεφάλι στοιβάδας σε μια πύλη σε ένα άλλο κεφάλι στοιβάδων, έως ότου επιτυγχάνεται το κεφάλι στοιβάδων του κόμβου προορισμού. Το πακέτο διαβιβάζεται έπειτα στον προορισμό.

Σε ένα δυναμικό κεφάλι στοιβάδων δικτύου το σχέδιο μπορεί να προκαλέσει την υποβάθμιση απόδοσης λόγω της συχνής εκλογής κεφαλιού στοιβάδας, έτσι το **CSGR** χρησιμοποιεί ένα **Least Cluster Change (LCC)** αλγόριθμο για να εκλέξει ένα κεφάλι στοιβάδας. Στο **LCC** το κεφάλι στοιβάδας εμφανίζεται μόνο εάν μια αλλαγή στο δίκτυο αναγκάζει δύο κεφάλια στοιβάδων να ενωθούν σε μια στοιβάδα ή μία από τις συσκευές κινείται έξω από τη σειρά όλων των άλλων κεφαλιών στοιβάδων.

Στο CSGR κάθε κόμβος κρατά ένα **πίνακα μελών στοιβάδων( cluster member table),** όπου αποθηκεύει το κεφάλι στοιβάδων προορισμού για κάθε κινητή συσκευή στο δίκτυο. Αυτοί οι πίνακες μελών στοιβάδων μεταδίδονται περιοδικά από κάθε κόμβο χρησιμοποιώντας το πρωτόκολλο **DSDV**.

Οι κόμβοι λαμβάνουν αυτή την αναπροσαρμογή και έτσι θα ανανεώσουν τους πίνακες μελών στοιβάδων τους έτσι ώστε να εξασφαλίσουν την ισχύ τους. Κάθε κόμβος επίσης διατηρεί ένα πίνακα δρομολόγησης, που χρησιμοποιείται για να αποφασίσει το επόμενο hop για να φτάσει στον προορισμό. Η ενημέρωση και για τους πίνακες δρομολόγησης και για τους πίνακες μελών στοιβάδων απαιτούνται στο CSGR.




**Εικόνα 7 : CSGR πρωτόκολλο**

# GLOBAL STATE ROUTING PROTOCOL (GSR)

Το **GSR** πρωτόκολλο δρομολόγησης είναι παρόμοιο με το **DSDV**. Το συγκεκριμένο πρωτόκολλο προσπαθεί να αποφύγει την πλημμύρα της δρομολόγησης των μηνυμάτων. Κάθε κόμβος περιέχει μια **λίστα γειτόνων – neightbor list**, **έναν πίνακα τοπολογίας - topology table** ,**έναν πίνακα επόμενου hop – next hop table και έναν πίνακα απόστασης – distance table**. Η λίστα γειτόνων ενός κόμβου περιέχει τον κατάλογο των γειτόνων του. Για κάθε κόμβο προορισμού, ο πίνακας τοπολογίας περιέχει τις πληροφορίες της σύνδεσης όπως αναφέρονται από τον προορισμό και το χρονικό όριο των πληροφοριών. Για κάθε προορισμό, ο επόμενος hop πίνακας περιέχει το επόμενο hop του οποίου τα πακέτα για τον αυτόν τον προορισμό πρέπει να διαβιβαστούν. Ο πίνακας απόστασης περιέχει την πιο σύντομη απόσταση σε κάθε κόμβο προορισμού. Στην λήψη ενός μηνύματος δρομολόγησης, ο κόμβος ενημερώνει τον πίνακα τοπολογίας του εάν ο αριθμός ακολουθίας του μηνύματος είναι νεώτερος από τον αριθμό ακολουθίας που αποθηκεύεται στον πίνακα. Μετά από αυτό ο κόμβος αναδημιουργεί τον πίνακα δρομολόγησής του και μεταδίδει τις πληροφορίες στους γείτονές του.

Το κύριο μειονέκτημα του συγκεκριμένου πρωτοκόλλου είναι το μεγάλο μέγεθος του μηνύματος δρομολόγησης. Δεδομένου ότι ολόκληρος ο πίνακας τοπολογίας μεταδίδεται με κάθε αναπροσαρμογή, ένα μη αμελητέο ποσό εύρους ζώνης καταναλώνεται.

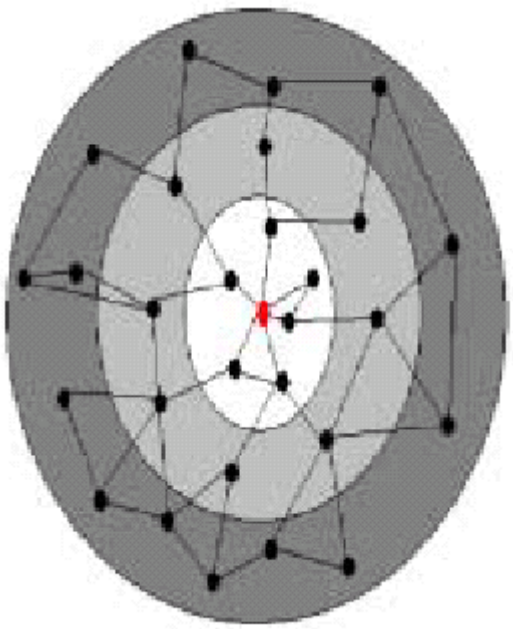
# FISHEYE STATE ROUTING PROTOCOL ( FSR)

Αυτό το πρωτόκολλο είναι μια βελτίωση του **GSR**. Ένα μειονέκτημα του **GSR** είναι το μεγάλο μέγεθος των μηνυμάτων αναπροσαρμογών, το οποίο αποσπά ένα μη αμελητέο ποσό εύρους ζώνης δικτύων. Αντί να στέλνει πληροφορίες για όλους τους κόμβους στα μηνύματα αναπροσαρμογών όπως στο GSR, οι πληροφορίες για τους πιο κοντινούς κόμβους διαβιβάζονται στο **FSR**. Ανταλλάσσονται οι πληροφορίες για τους πιο στενούς κόμβους συχνότερα απ'ότι για τους πιο μακρινούς κόμβους, οι οποίες μειώνουν το μέγεθος του μηνύματος αναπροσαρμογών. Έτσι κάθε κόμβος παίρνει τις εξακριβωμένες πληροφορίες για τους γείτονές του και την λεπτομέρεια και την ακρίβεια των μειωμένων πληροφοριών καθώς η απόσταση από τον κόμβο αυξάνεται.

Η εικόνα 8 παρουσιάζει το πεδίο του fisheye για τον κεντρικό (κόκκινο κόμβο). Το πεδίο καθορίζεται από την άποψη των κόμβων που μπορούν να επιτευχθούν σε ένα ορισμένο αριθμό από hops. Ο κεντρικός κόμβος έχει τις πιο εξακριβωμένες πληροφορίες για όλους τους κόμβους στον άσπρο κύκλο. Ακόμα και αν ένας κόμβος δεν έχει τις εξακριβωμένες πληροφορίες για τους απόμακρους κόμβους, τα πακέτα καθοδηγούνται σωστά επειδή οι πληροφορίες δρομολόγησης γίνονται όλο και περισσότερο εξακριβωμένες καθώς το πακέτο κινείται πιο κοντά προς τον προορισμό. Γενικά το FSR είναι κατάλληλο για τα μεγάλα κινητά δίκτυα δεδομένου ότι δεν προκαλεί κανένα μήνυμα ελέγχου σε αποτυχίες συνδέσεων. Οι σπασμένες συνδέσεις δεν θα περιληφθούν στην επόμενη ανταλλαγή μηνυμάτων κατάστασης σύνδεσης. Αυτό σημαίνει ότι μια αλλαγή σε μια σύνδεση μακρινή δεν θα προκαλέσει απαραίτητα μια αλλαγή στον πίνακα δρομολόγησης.

Το FSR είναι κυρίως βασισμένο στην απλότητα , δεδομένου ότι χρησιμοποιεί τις ενημερωμένες κοντινότερες διαδρομές, ανταλλάσσει πληροφορίες δρομολόγησης μόνο με τους γείτονές του μειώνοντας κατά συνέπεια την κυκλοφορία δρομολόγησης.

Ένα μειονέκτημα του συγκεκριμένου πρωτοκόλλου είναι ο περιορισμός στην εξελιξιμότητα , και ότι είναι εύκολο να βρεθούν οι προορισμοί λόγω της τοπολογίας που χρησιμοποιεί. Άλλο ένα αρνητικό στοιχείο είναι η πολυπλοκότητα στους πίνακες δρομολόγησης.



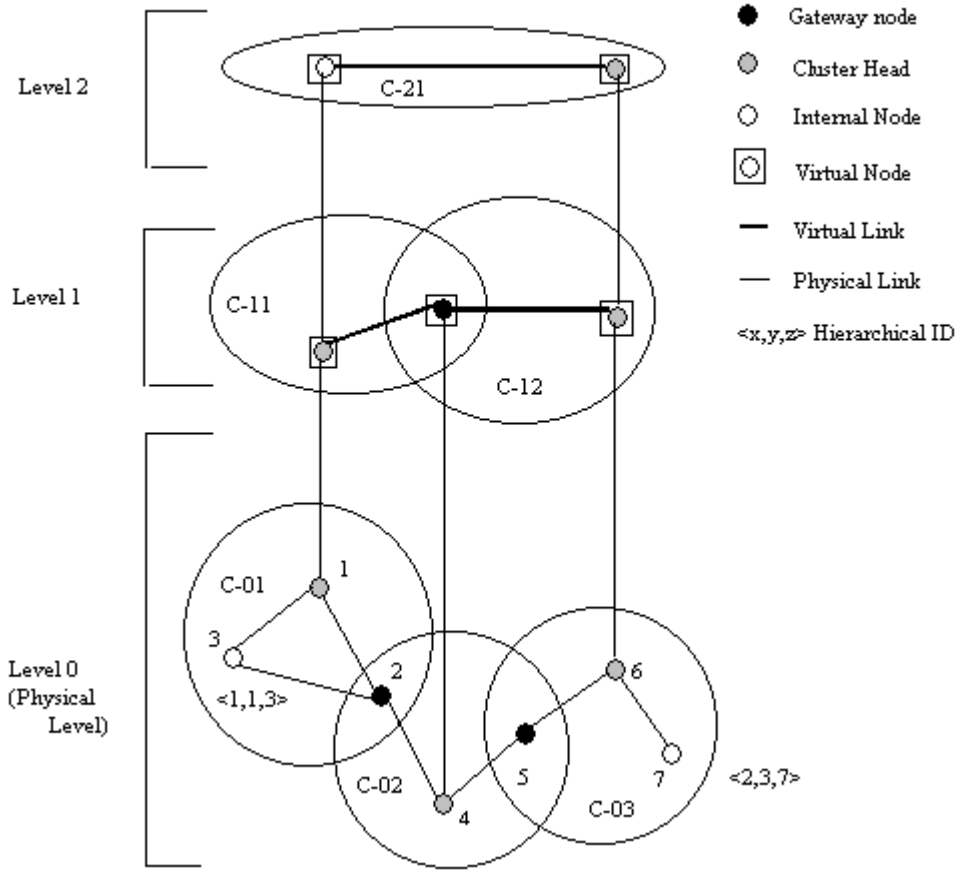
**Εικόνα 8 : FSR πρωτόκολλο**

# HIERARCHICAL STATE ROUTING PROTOCOL ( HSR)

Η πολλαπλή συγκέντρωση στοιβάδων και ο λογικός χωρισμός των κινητών κόμβων μπορούν να χρησιμοποιηθούν για να κατασκευάσουν την ιεραρχική δομή του δικτύου. Αυτή η ιεραρχική δομή μπορεί να χρησιμοποιηθεί για να εκτελέσει τους στόχους δρομολόγησης. Αυτό κάνει το **HSR.** Το δίκτυο χωρίζεται στις στοιβάδες και ένα κεφάλι στοιβάδων εκλέγεται όπως στο **CSGR.** Στο HSR, τα κεφάλια στοιβάδων ξανά οργανώνονται σε στοιβάδες και προχωρούν έτσι. Οι κόμβοι μιας φυσικής στοιβάδας μεταδίδουν τις πληροφορίες σύνδεσής τους ο ένας στον άλλον. Το κεφάλι στοιβάδων συνοψίζει τις πληροφορίες στοιβάδας του και τις στέλνει στα γειτονικά κεφάλια στοιβάδων μέσω της πύλης.

Όπως φαίνεται στην εικόνα 9 αυτά τα κεφάλια στοιβάδων είναι μέλη της στοιβάδας σε ένα επίπεδο πιο ψηλά και ανταλλάσσουν τις πληροφορίες σύνδεσής τους όπως και τις συνοψισμένες χαμηλότερες πληροφορίες επιπέδου το ένα μεταξύ του άλλου. Ένας

κόμβος σε κάθε επίπεδο πλημμυρίσει στο χαμηλότερο επίπεδο τις πληροφορίες που λαμβάνει μετά από τον αλγόριθμο που έχει τρέξει σε εκείνο το επίπεδο. Έτσι το χαμηλότερο επίπεδο έχει ιεραρχικές πληροφορίες τοπολογίας. Κάθε κόμβος έχει μια ιεραρχική διεύθυνση. Ένας τρόπος για να οριστεί μια ιεραρχική διεύθυνση είναι οι αριθμοί στοιβάδων στον δρόμο από η ρίζα ( root) στον κόμβο όπως φαίνεται στην εικόνα 9. Μια πύλη μπορεί να επιτευχθεί από την ρίζα μέσω περισσότερων διαδρομών, έτσι η πύλη μπορεί να έχει παραπάνω από μια ιεραρχικές διευθύνσεις. Μια ιεραρχική διεύθυνση είναι αρκετή για να εξασφαλίσει την παράδοση από οπουδήποτε στο δίκτυο στον χρήστη.




**Εικόνα 9 : HSR πρωτόκολλο**

Επίσης κάθε υποδίκτυο περιέχει έναν διοικητικό υπολογιστή θέσης – location management server (**LMS**). Όλοι οι κόμβοι σε αυτό το υποδίκτυο καταχωρούνται με **LMS.** Τα LMS πρέπει να ενημερώσουν τα ανώτερα επίπεδα, και οι ανώτερες πληροφορίες έρχονται στον τοπικό LMS server. Όταν δύο κόμβοι προσπαθούν να μιλήσουν στέλνουν τα αρχικά LMS στοιχεία τους . Τα LMS τα διαβιβάζουν στον

προορισμό τους. Όταν η πηγή και ο προορισμός γνωρίζουν τις ιεραρχικές τους διευθύνσεις επικοινωνούν αμέσως. Το πρωτόκολλο είναι ιδιαίτερα προσαρμοστικό στις αλλαγές του δικτύου.

# ZONE BASED HIERARCHICAL LINK STATE ROUTING PROTOCOL (ZHLS)

Στο **ZHLS,** το δίκτυο διαιρείται σε μη- επικαλυπτόμενες ζώνες. Αντίθετα από άλλα ιεραρχικά πρωτόκολλα δεν υπάρχει κανένα ζώνη – κεφάλι. Το **ZHLS** καθορίζει δύο επίπεδα τοπολογιών : **το επίπεδο κόμβων ( node level) και το επίπεδο ζώνης ( zone level).** Μια τοπολογία επιπέδου κόμβων λέει πόσοι κόμβοι μιας ζώνης συνδέονται ο ένας με τον άλλον φυσικά. Μια εικονικά σύνδεση μεταξύ των δύο κόμβων υπάρχει εάν τουλάχιστον ένας κόμβος μιας ζώνης συνδέεται φυσικά με κάποιο κόμβο της άλλης ζώνης. Η τοπολογία επιπέδου ζώνης λέει πως οι ζώνες συνδέονται μεταξύ τους. Υπάρχουν δύο τύποι *Link State Packets (LSP*) ,ο **LSP** κόμβος και η ζώνη LSP. Ένας κόμβος LSP ενός κόμβου περιέχει τις πληροφορίες του γειτονικού κόμβου και διαδίδεται με τη ζώνη όπου μια ζώνη LSP περιέχει τις πληροφορίες ζώνης και διαδίδεται συνολικά. Έτσι κάθε κόμβος έχει την πλήρη γνώση συνδετικότητας κόμβων για τους κόμβους στη ζώνη του και μόνο τις ζώνες πληροφορίες συνδετικότητας για άλλες ζώνες στο δίκτυο. Έτσι με βάση τη ζώνη **ID** $_{\textbf{Zone}}$ και τον κόμβο ID $_{\text{node}}$ ενός προορισμού, το πακέτο καθοδηγείται με βάση τη ζώνη ID $_{\text{Zone}}$ έως ότου φτάσει σωστή ζώνη. Έπειτα σε εκείνη τη ζώνη, καθοδηγείται βασισμένος στον κόμβο ID $_{\text{node}}$ . Το **(zone ID** $_{\textbf{Zone}}$**,node ID** $_{\textbf{node}}$**)** του προορισμού είναι ικανοποιητικό για δρομολόγηση έτσι είναι προσαρμόσιμο σε αλλαγές της τοπολογίας.

# SOURCE TREE ADAPTIVE ROUTING PROTOCOL (STAR)

Το **STAR** είναι ένα πρωτόκολλο δρομολόγησης που δεν απαιτεί περιοδικές αναπροσαρμογές της δρομολόγησης, ούτε αυτό προσπαθεί να διατηρήσει τις βέλτιστες διαδρομές στους προορισμούς.

Εάν οι αλλαγές τοπολογία εμφανίζονται συχνά, το ποσοστό στις αναπροσαρμογές δρομολόγησης αυξάνεται δραματικά. Αυτό έχει σαν αποτέλεσμα να είναι παρόντα στο δίκτυο περισσότερα μηνύματα ελέγχου παρά δεδομένα χρηστών, κάτι το οποίο είναι ανεπιθύμητο. Το **STAR** προσπαθεί να μειώσει τον αριθμό δρομολόγησης των αναπροσαρμογών. Το STAR χρησιμοποιεί ένα γειτονικό πρωτόκολλο ανακαλύψεων για να επιτρέψει σε αυτό να ανακαλύψει την παρουσία και την κινητικότητα των γειτονικών κόμβων. Κάθε κόμβος περιέχει ένα **δέντρο πηγής – source tree.** Το σύνολο των συνδέσεων που χρησιμοποιούνται από έναν δρομολογητή στο επιθυμητό μονοπάτι σε έναν προορισμό καλείται **δέντρο πηγής – source tree** του δρομολογητή. Κάθε κόμβος γνωρίζει τις παρακείμενες συνδέσεις του και τα δέντρα πηγής αναφερόμενα από τους γείτονές του. Κάθε ένας κόμβος τρέχει έναν αλγόριθμο επιλογής διαδρομών στο δέντρο πηγής του για να παράγει έναν πίνακα δρομολόγησης που διευκρινίζει τον διάδοχο σε κάθε προορισμό. Για να μειώσει τον αριθμό αναπροσαρμογών, μόνο αλλαγές στην ισχύ του δέντρου πηγής διαδίδονται. Τέτοιες αλλαγές περιλαμβάνονται όταν η πηγή χάσει όλα τα μονοπάτια της σε ένα προορισμό, ανιχνεύει έναν νέο γείτονα, ή αντιμετωπίζει έναν εκκρεμή μακροπρόθεσμο βρόχο δρομολόγησης. Μια ακόμα διαφορά του STAR εντοπίζεται στο γεγονός ότι ολόκληρες πληροφορίες τοπολογίας ούτε χρησιμοποιούνται ούτε στέλνονται.

## ***ON DEMAND ROUTING PROTOCOLS***

Στη συγκεκριμένη κατηγορία πρωτοκόλλων γίνεται προσπάθεια να αποβληθούν οι συμβατικοί πίνακες δρομολόγησης και να μειωθεί η ανάγκη για αναπροσαρμογή στους πίνακες για να ακολουθήσουν τις αλλαγές στην τοπολογία δικτύων. Σε αντίθεση με τα **table – driven routing protocols** όλες οι ενημερωμένες διαδρομές δεν διατηρούνται σε κάθε κόμβο, αντ'αυτού οι διαδρομές δημιουργούνται σε περίπτωση ανάγκης. Στα **On demand routing protocols** υπολογίζεται μια διαδρομή

πριν την μετάδοση στοιχείων. Όταν μια πηγή θέλει να στείλει σε ένα προορισμό πρέπει να επικαλεσθεί τις ακόλουθες διαδικασίες :

- **Route discovery** – Ανακάλυψη διαδρομών
- **Route maintenance** – Συντήρηση διαδρομών
- **Route deletion** – Διαγραφή διαδρομών

Η Route discovery δεν απαιτείται για την μετάδοση κάθε ενιαίου πακέτου στοιχείων, δεδομένου ότι η ανακαλυμμένη διαδρομή πιθανό να ισχύσει για μια χρονική περίοδο που επιτρέπει πολλές μεταδόσεις στον ίδιο προορισμό.

Τα on demand routing protocols είναι τα εξής : ***Ad hoc On Demand Distance Vector (AODV) routing protocol, Dynamic Source Routing (DSR) protocol, Power Aware Routing (PAR) protocol, Location Aided Routing (LAR) protocol, Signal Stability Routing (SSR) protocol, Cluster Based Routing (CBR) protocol , Temporally Order Routing Algorithm (TORA), Associativity Based Routing (ABR) protocol.***

# AD HOC ON – DEMAND DISTANCE VECTOR ROUTING PROTOCOL (AODV)

Το πρωτόκολλο AODV βασίζεται στον αλγόριθμο δρομολόγησης distance – vector όπως στο DSDV. Η κύρια διαφορά μεταξύ των δύο αυτών πρωτοκόλλων είναι ότι το AODV προσπαθεί να ελαχιστοποιήσει τον αριθμό των μεταδόσεων δημιουργώντας διαδρομές κατά παραγγελία αντί της διατήρησης ενός καταλόγου διαδρομών για κάθε πιθανό προορισμό. Το AODV χρησιμοποιεί ένα αριθμό ακολουθίας για κάθε είσοδο διαδρομών, που δημιουργείται από τον προορισμό όταν στέλνει τις πληροφορίες δρομολόγησης στην αίτηση των συσκευών. Όταν δύο ή περισσότερες διαδρομές σε έναν προορισμό είναι διαθέσιμες, ο διαβιβάζοντας κόμβος επιλέγει αυτόν με τον μέγιστο αριθμό ακολουθίας για να εξασφαλίσει ελευθερία βρόχων. Το AODV χρησιμοποιεί τρεις τύπους μηνυμάτων : **Route Requests (RREQs), Route Replies (RREPs)** και **Route Errors (RERRs**).

Όταν μια πηγή συσκευή θέλει να στείλει ένα πακέτο σε κάποιο προορισμό, μεταδίδει ένα **RREQ** για να βρει μια διαδρομή για εκείνο τον προορισμό. Μια διαδρομή βρίσκεται όταν φθάσει το RREQ είτε από μόνο του στον προορισμό είτε μέσω ενός ενδιάμεσου κόμβου με μια διαδρομή της οποίας ο αριθμός ακολουθίας είναι τουλάχιστον τόσο μεγάλος όσο αυτός που περιλαμβάνεται στο RREQ.
Η διαδρομή γίνεται διαθέσιμη με την αποστολή ενός **RREP** πακέτου στη πηγή του RREQ. Όταν ένας κόμβος διαδιβάζει ένα πακέτο RREQ στους γείτονές του, επίσης καταγράφει τον κόμβο από αυτόν που το αίτημα προήλθε, προκειμένου να είναι σε θέση να επιστρέψει το RREP στον κόμβο πηγής.

Όταν ένας κόμβος ανιχνεύει ότι μια σύνδεση με έναν γείτονα έχει σπάσει, στέλνει ένα μήνυμα Route Error για να ενημερώσει όλους τους άλλους κόμβους ότι η σύνδεση δεν ισχύει πλέον. Αυτό το μήνυμα διαδίδεται μέσω του δικτύου και φθάνει στους κόμβους πηγής των σπασμένων διαδρομών, οι οποίες μπορούν να επαναλάβουν τη διαδικασία για να ανακαλύψουν μια νέα διαδρομή για τον ίδιο προορισμό. Οι σπασμένες διαδρομές εντοπίζονται από το MAC επίπεδο πρωτόκολλο ή από το ίδιο το AODV πρωτόκολλο. Στην πιο πρόσφατη περίπτωση περιοδικά στέλνει ένα RREP πακέτο ( το οποίο είναι το **Hello** μήνυμα) και περιμένει για Hello μηνύματα από τους γείτονες. Αν δεν πάρει κάποια απάντηση για κάποιο χρονικό διάστημα τότε σημαίνει ότι η διαδρομή δεν υφίσταται.
Το συγκεκριμένο πρωτόκολλο εξαρτάται από τη κίνηση στο δίκτυο και τον αριθμό των συσκευών στο δίκτυο.

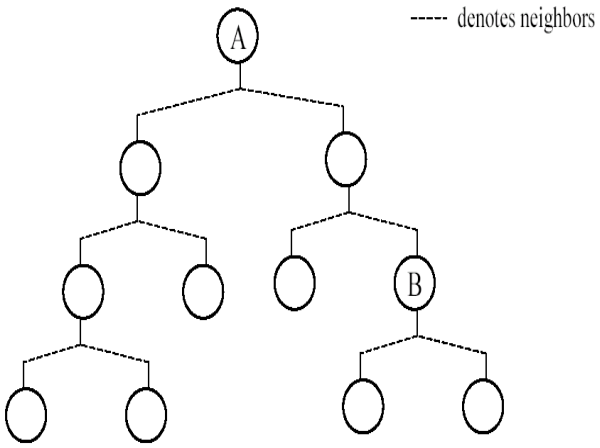
# DYNAMIN SOURCE ROUTING PROTOCOL ( DSR)

Το DSR είναι ένα source –routing πρωτόκολλο, οι δύο σημαντικοί μηχανισμοί του πρωτοκόλλου είναι **ανακάλυψη διαδρομών (route discovery)** και **η συντήρηση διαδρομών ( route maintenance).** Όταν ένας κόμβος πρέπει να επικοινωνήσει με έναν κόμβο προορισμού ανατρέχει στον πίνακα δρομολόγησής του για μια διαδρομή στον προορισμό. Εάν ο κόμβος δεν έχει μια τέτοια διαδρομή στέλνει ένα πακέτο Route Request που περιέχει την διεύθυνση της πηγής και του προορισμού και ενός

μοναδικού αριθμού αναγνώρισης. Εάν ένας ενδιάμεσος κόμβος δεν ξέρει μια διαδρομή στον προορισμό επισυνάπτει τη διεύθυνσή του στο αρχείο διαδρομών του πακέτου και διαβιβάζει το πακέτο στους γείτονές του.

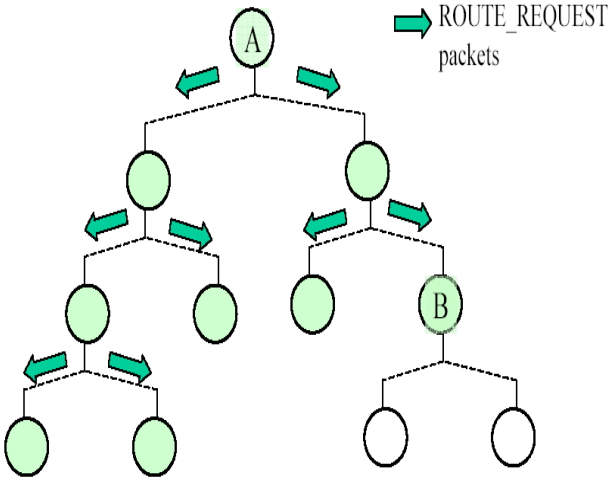
Ένα πακέτο **Route Reply packet** παράγεται όταν είτε ο προορισμός είτε ένας ενδιάμεσος κόμβος με τις τρέχουσες πληροφορίες λαμβάνει το Route Request.
Ένα **Route Request** πακέτο περιέχει στο αρχείο διαδρομών του, την ακολουθία hops που λαμβάνονται από την πηγή σε αυτόν τον κόμβο. Εάν η Route Reply παράγεται από τον προορισμό, κατόπιν τοποθετεί το αρχείο διαδρομών από το πακέτο Rote Request στην Route Reply. Από την άλλη πλευρά εάν ο κόμβος που παράγει τη Route Reply είναι ένας ενδιάμεσος κόμβος, τότε συγχωνεύει τη γνωστή διαδρομή του στον προορισμό με το αρχείο διαδρομών του πακέτου Route Request, διαμορφώνοντας μια πλήρη πορεία από την πηγή στον προορισμό και πηγαίνει τις πληροφορίες αυτές στο πακέτο Route Reply.

Ο μηχανισμός συντήρησης διαδρομών DSR χρησιμοποιεί δύο τύπους πακέτων: **Route Error** πακέτα και αναγνωρίσεις λάθους διαδρομών. Όταν ένας κόμβος ανιχνεύει μια θραύση συνδέσεων, ειδοποιεί τους γείτονές του με ένα πακέτο Route Error. Τα πακέτα αναγνώρισης λάθους διαδρομών χρησιμοποιούνται για να ελέγξουν την σωστή λειτουργία των συνδέσεων διαδρομών. Αυτό περιλαμβάνει επίσης την παθητική αναγνώριση στην οποία ένας κόμβος ακούει το επόμενο hop ακολουθώντας το πακέτο κατα μήκος της διαδρομής.
Γενικά το πρωτόκολλο DSR εξαρτάται από τη κίνηση στο δίκτυο και τον αριθμό των συσκευών που βρίσκονται στο δίκτυο.




**Εικόνα 10 : Διάγραμμα δρομολόγησης**

Εδώ βλέπουμε πως λειτουργεί η διαδικασία όταν η συσκευή Α θέλει να επικοινωνήσει με τη συσυσκευή Β στέλνοντας Route_Request πακέτα.




**Εικόνα 11 : Route Request packets**

# TEMPORALLY ORDERED ROUTING ALGORITHM ( TORA)

Το TORA είναι ένα source – initiated πρωτόκολλο δρομολόγησης σχεδιασμένο για δυναμικά mobile ad hoc ασύρματα δίκτυα. Ο βασικός αλγόριθμος δρομολόγησης που χρησιμοποιείται από το TORA ανήκει στην οικογένεια των αλγόριθμων αντίστροφων συνδέσεων. Διατηρεί πολλαπλές διαδρομές από έναν κόμβο πηγής σε έναν κόμβο προορισμού.Το πρωτόκολλο προσπαθεί να μειώσει τις γενικές δρομολογήσεις περιορίζοντας την διάδοση των μηνυμάτων ελέγχου σε μια μικρή περιοχή κοντά στο περιστατικό μιας τοπολογικής αλλαγής.

Το TORA αποτελείται από τρεις βασικές λειτουργίες : **Route creation ( δημιουργία διαδρομών), route maintenance ( συντήρηση διαδρομών)** και **route erasure ( εξάλειψη διαδρομών).** Όταν μια πηγή θέλει να εγκαταστήσει μια σύνδεση σε έναν προορισμό στέλνει ένα Query Packet ( πακέτο ερώτησης) προσδιορίζοντας τον προορισμό για τον οποίο η διαδρομή ζητείται.
Ο προορισμός ή ένας κόμβος που έχει μια έγκυρη διαδρομή σε αυτό, αποκρίνεται με την αποστολή ενός πακέτου αναπροσαρμογών που περιέχει "το ύψος του" όσον αφορά τον προορισμό.
Οι κόμβοι που λαμβάνουν την αναπροσαρμογή θέτουν μια μεγαλύτερη αξία στο ύψος τους, διαμορφώνοντας κατά συνέπεια ένα γράφημα από την πηγή στον προορισμό. Όταν η επόμενη σύνδεση προς ένα προορισμό έχει σπάσει , ο κόμβος θέτει το ύψος του να είναι ένα τοπικό μέγιστο έναντι των υψών των γειτόνων του και διαβιβάζει ένα πακέτο αναπροσαρμογών.

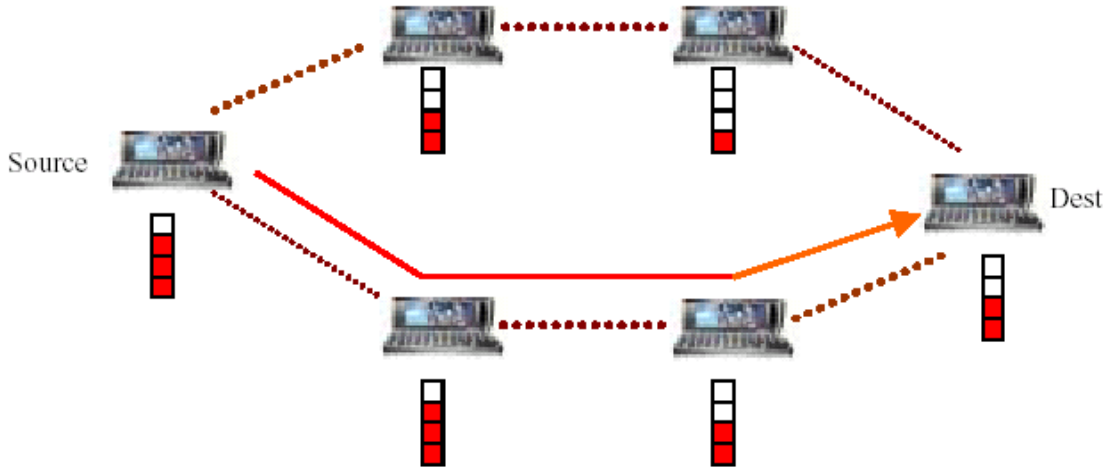
# POWER AWARE ROUTING PROTOCOL ( PAR)

Στο συγκεκριμένο πρωτόκολλο η ζωή της μπαταρίας λαμβάνεται ως μετρική δρομολόγηση. Το **PAR** συνηγορεί για :

- Ελαχιστοποίηση για μείωση της ενέργεια που καταναλώνεται ανά πακέτο : αυτό υπονοεί την συντομότερη hop πορεία.

- Μεγιστοποιεί το χρόνο στο χωρισμό του δικτύου : Η δρομολόγηση του πρωτοκόλλου προσπαθεί να διαιρέσει την εργασία μεταξύ των κόμβων για να μεγιστοποιήσει τη ζωή του δικτύου.
- Μεγιστοποιεί η διαφορά στα επίπεδα δύναμης κόμβων : Αυτό υπονοεί τη διανομή φορτίων των διανεμημένων συστημάτων και είναι ισοδύναμο, με το πρόβλημα δοχείο – συσκευασίας.
- Ελαχιστοποιεί το κόστος ανά πακέτο : Εδώ ο στόχος είναι να μεγιστοποιηθεί η ζωή των μεμονωμένων κόμβων στο δίκτυο συμπεριλαμβανομένων των δαπανών εκτός από την ενέργεια.
- Ελαχιστοποιώντας το μέγιστο κόστος του κόμβου : Εδώ η ελαχιστοποίηση γίνεται για κατανάλωση ενέργειας ανά κόμβο καθώς οι κόμβοι στέλνουν πακέτα.

Το πρωτόκολλο επιλέγει τις διαδρομές που έχουν μια μακρύτερη ζωή διαδρομών, παράδειγμα της κατάστασης φαίνεται στην εικόνα 12, βλέπουμε ότι η διαδρομή με την μεγαλύτερη ισχύ επιλέγεται για δρομολόγηση πακέτων.

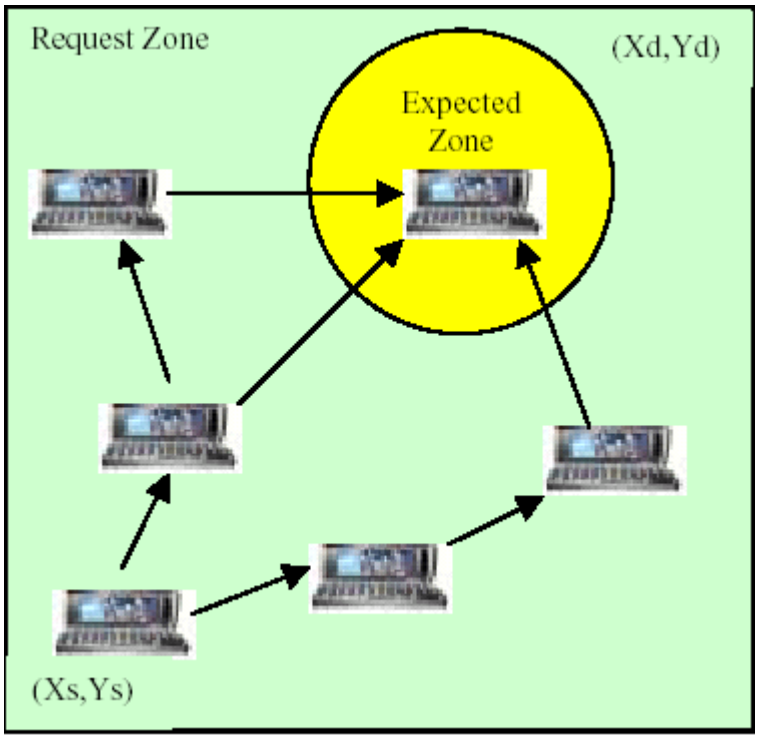



**Εικόνα 12 : PAR πρωτόκολλο**

# LOCATION AIDED ROUTING PROTOCOL (LAR)

Το **LAR** πρωτόκολλο χρησιμοποιεί τις πληροφορίες θέσης για να βελτιώσει την απόδοση του ad hoc δικτύου. Το LAR περιορίζει την αναζήτηση μιας νέας διαδρομής

στη μικρότερη ζώνη αιτήματος που μειώνει την κυκλοφορία του σήματος. Το LAR καθορίζει δύο τύπους ζώνης : **expected zone – αναμενόμενη ζώνη και request zone – ζώνη αιτήματος.** Το LAR υποθέτει ότι οι κόμβοι έχουν τις πληροφορίες για να μαντέψουν τη **request zone** προορισμού. Έτσι ο αποστολέας διευκρινίζει ρητά τη **request zone** στο μήνυμα αιτήματος διαδρομών του. Κόμβοι που λαμβάνουν το μήνυμα αιτήματος αλλά δεν εμπίπτουν στη **request zone** απορρίπτουν το πακέτο. Στην παρακάτω εικόνα 13 βλέπουμε πως λειτουργεί το συγκεκριμένο πρωτόκολλο.




**Εικόνα 13 : LAR πρωτόκολλο**

# SIGNAL STABILITY ROUTING PROTOCOL ( SSR)

Το **SSR** επιλέγει διαδρομές βασισμένες στη δύναμη σημάτων μεταξύ των κόμβων και στη σταθερότητα θέσης ενός κόμβου. Το SSR περιλαμβάνει δύο πρωτόκολλα που

συνεργάζεται μαζί τους : **το Dynamic Routing Protocol (DRP) και το Static Routing Protocol (SRP).**

Το **DRP** διατηρεί το **Signal Stability Table (SST)** και το **Routing Table** (**RT**). Το **SST** αποθηκεύει η δύναμη των σημάτων των γειτονικών κόμβων που αποκτούνται από τα περιοδικά αναγνωριστικά σήματα από το στρώμα συνδέσεων κάθε γειτονικού κόμβου. Η δύναμη σήματος είτε καταγράφεται ως ισχυρό είτε αδύνατο κανάλι. Όλες οι μεταδόσεις παραλαμβάνονται από το **DRP** και υποβάλλονται σε επεξεργασία. Μετά από την ενημέρωση των κατάλληλων καταχωρήσεων στους πίνακες, το DRP περνά το πακέτο στο **SRP**. Το SRP περνά το πακέτο στον επάνω σωρό εάν είναι ο προοριζόμενος δέκτης. Αν όχι, ανατρέχει ο προορισμός στο **RT** και μεταδίδει το πακέτο. Αν δεν υπάρχει καμιά είσοδος για τον προορισμό RT, κινεί μια διαδικασία διαδρομή – αναζήτησης για να βρει μια διαδρομή.

Τα πακέτα διαδρομής αιτήματος- route request διαβιβάζονται στον επόμενο hop μόνο εάν παραλαμβάνονται πέρα από τα ισχυρά κανάλια και δεν έχουν υποβληθεί σε επεξεργασία προηγουμένως ( για να αποφύγουν την επανάληψη). Ο προορισμός επιλέγει το πρώτο **πακέτο διαδρομής – αναζήτησης - route search packet** για να στείλει πίσω όπως είναι ιδιαίτερα πιθανό ότι το πακέτο έφτασε πέρα από την κοντινότερη ή και λιγότερο κορεσμένη πορεία. Το **DRP** αντιστρέφει την επιλεγμένη διαδρομή και στέλνει ένα **μήνυμα διαδρομή απάντησης – route reply message** πίσω στον ιδρυτή της **διαδρομής- αιτήματος route request**. Το **DRP** των κόμβων κατά μήκος της διαδρομής ενημερώνει την **RT** αναλόγως. Τα **πακέτα διαδρομής αναζήτησης route search packets** που φτάνουν στον προορισμό έχουν φτάσει απαραιτήτως στη διαδρομή της ισχυρότερης σταθερότητας σημάτων επειδή τα πακέτα που φτάνουν πέρα από ένα αδύνατο κανάλι πέφτουν στους ενδιάμεσους κόμβους. Εάν περάσει ο χρόνος της πηγής πριν ληφθεί μια απάντηση τότε αλλάζουν το **PREF** πεδίο στην επιγραφή για να δείξουν ότι τα αδύνατα κανάλια είναι αποδεκτά , δεδομένου ότι αυτά μπορούν να είναι οι μόνες συνδέσεις πέρα από τις οποίες το πακέτο μπορεί να διαδοθεί.

Όταν μια σύνδεση αποτύχει μέσα στο δίκτυο, οι ενδιάμεσοι κόμβοι στέλνουν ένα **μήνυμα λάθους –error message** στη πηγή προσδιορίζοντας ποιο κανάλι έχει αποτύχει. Η πηγή τότε στέλνει ένα **μήνυμα διαγραφής – erase message** για να δηλώσει σε όλους τους κόμβους τη σπασμένη σύνδεση και ξεκινά μια νέα **διαδικασία αναζήτησης – route search process** για να βρεθεί ένα καινούργιο μονοπάτι για τον προορισμό.

# CLUSTER BASED ROUTING PROTOCOL ( CBR)

Στο **CBR** οι κόμβοι διαιρούνται σε στοιβάδες. Για να διαμορφωθεί η στοιβάδα ο ακόλουθος αλγόριθμος χρησιμοποιείται. Όταν ένας κόμβος εμφανίζεται , μπαίνει σε αναποφάσιστη κατάσταση, ξεκινά ένα χρονόμετρο και μεταδίδει ένα **Hello message**. Όταν ένα κεφάλι –στοιβάδα λαμβάνει αυτό το hello μήνυμα αποκρίνεται με ένα προκαλούμενο Hello μήνυμα αμέσως. Όταν ο αναποφάσιστος κόμβος λαμβάνει αυτό το μήνυμα θέτει σε κατάσταση μέλους. Αν ο χρόνος του αναποφάσιστου κόμβου τελειώσει, τότε κάνει τον εαυτό του κεφάλι – στοιβάδας αν έχει την αμφίδρομη σύνδεση με κάποιον γειτονικό κόμβο ειδάλλως παραμένει σε αναποφάσιστη κατάσταση και επαναλαμβάνει αυτή τη διαδικασία ξανά.

Κάθε κόμβος περιέχει ένα πίνακα γειτόνων. Για κάθε γείτονα, ο πίνακας γειτόνων ενός κόμβου περιέχει τη θέση της σύνδεσης ( πολύ ή αμφίδρομη) και την κατάσταση του γείτονα ( κεφάλια – στοιβάδας ή μέλος). Ένα κεφάλι –στοιβάδας κρατά πληροφορίες για τα μέλη της στοιβάδας του και επίσης διατηρεί έναν πίνακα στοιβάδων για τις γειτονικές στοιβάδες.

Για κάθε γειτονική στοιβάδα , ο πίνακας έχει είσοδο που περιέχει την πύλη μέσω της οποίας η στοιβάδα μπορεί να επιτευχθεί και το κεφάλι – στοιβάδα της στοιβάδας. Όταν η πηγή θέλει να στείλει δεδομένα σε ένα προορισμό πλημμυρίζει πακέτα αιτήματος δρομολόγησης – **route request packets** ( αλλά μόνο στα γειτονικά κεφάλια στοιβάδας). Στη λήψη του αιτήματος ένα κεφάλι στοιβάδας ελέγχει αν ο προορισμός είναι στη στοιβάδα του. Εάν ναι τότε στέλνει άμεσα το αίτημα στον προορισμό αλλιώς στέλνει σε όλα τα παρακείμενα κεφάλια στοιβάδων. Η διεύθυνση του κεφαλιού στοιβάδας καταγράφεται στο πακέτο έτσι ώστε ένα κεφάλι στοιβάδας να απορρίπτει ένα πακέτο αιτήματος – **request packet** που έχει ήδη δει. Όταν ο προορισμός λαμβάνει το πακέτο αιτήματος – request packet , απαντάει πίσω με την διαδρομή που έχει καταγραφεί στο πακέτο αιτήματος – request packet. Εάν η πηγή δεν λαμβάνει μια απάντηση εντός ενός χρονικού διαστήματος, υπαναχωρεί πριν να προσπαθήσει να στείλει ένα πακέτο αιτήματος διαδρομής – route request packet ξανά.

Στο **CBR**, η δρομολόγηση γίνεται χρησιμοποιώντας δρομολόγηση πηγής. Χρησιμοποιεί τη κοντύτερη διαδρομή που είναι στη λήψη ενός πακέτου διαδρομών πηγής – **source route packet**, ο κόμβος ψάχνει να βρει τη συντομότερη διαδρομή που είναι ο γείτονάς του ( αυτό μπορεί να συμβεί κατά τη διάρκεια μια αλλαγής τοπολογίας) και στέλνει το πακέτο στον κόμβο ο οποίος μειώνει τη διαδρομή. Καθώς δρομολογείται ένα πακέτο εάν ένας κόμβος ανιχνεύει μια σπασμένη διαδρομή στέλνει πίσω ένα μήνυμα λάθους – **error message** στην πηγή και χρησιμοποιεί τοπικό μηχανισμό επισκευής.

Στον τοπικό μηχανισμό επισκευής όταν ένας κόμβος βρίσκει ότι η επόμενη hop είναι απρόσιτη, ελέγχει για να δει αν το επόμενο hop μπορεί μα επιτευχθεί μέσω κάποιου γείτονά του.

# ASSOCIATIVITY BASED ROUTING PROTOCOL ( ABR)

Το συγκεκριμένο πρωτόκολλο καθορίζει ένα νέο μετρικό για τη δρομολόγηση γνωστό ως βαθμό σταθερότητας. Είναι ελεύθερο σε επαναλήψεις και επιτρέπει διπλότυπα πακέτων. In **ABR**, ένας κόμβος επιλέγεται βασισμένος στη συνδετικότητα των κόμβων. Οι διαδρομές που επιλέγονται πρέπει να είναι μακρόβιες. Όλοι οι κόμβοι παράγουν τα περιοδικά αναγνωριστικά σήματα για να δηλώσουν την ύπαρξή τους. Όταν ένας γειτονικός κόμβος λαμβάνει ένα αναγνωριστικό σήμα , ανανεώνει τη συνδετικότητα των πινάκων του.

Για κάθε αναγνωριστικό σήμα που λαμβάνεται, ένας κόμβος αυξάνει τη συνδετικότητά του όσον αφορά το κόμβο από τον οποίο έλαβε το αναγνωριστικό σήμα. Η σταθερότητα της ένωσης σημαίνει τη σταθερότητα σύνδεσης ενός κόμβου. Μια υψηλή αξία συνδετικότητας δείχνει μια χαμηλή κατάσταση της κινητικότητας των κόμβων ενώ μια χαμηλή αξία της συνδετικότητας μπορεί να δείξει μια υψηλή κατάσταση κινητικότητας των κόμβων. Αλλαγές στην συνδετικότητα επαναρυθμίζονται όταν κινούνται οι γείτονες ενός κόμβου ή κινείται ο ίδιος ο κόμβος . Ο θεμελιώδης στόχος του ABR είναι να βρεθούν οι μακράς ζωής δρομολογητές για ένα ad hoc δίκτυο. Οι τρεις φάσεις ενός **ABR** είναι : **Route discovery, Route reconstruction και Route deletion**.

Η route discovery φάση είναι μια μετάδοσης ερώτησης και περιμένει τον κύκλο απάντησης (**BQ-REPLY).** Ο κόμβος πηγής μεταδίδει ραδιοφωνικά ένα **BQ** μήνυμα

σε αναζήτηση των κόμβων που έχουν μια διαδρομή στον προορισμό. Ένας κόμβος δεν διαβιβάζει ένα BQ αίτημα περισσότερο από μία φορά. Στη λήψη ενός μηνύματος BQ, ένας ενδιάμεσος κόμβος επισυνάπτει τη διεύθυνσή του και τη κινητικότητά του στο πακέτο ερώτησης – **query packet**. Ο επόμενος επιτυχών κόμβος σβήνει τις καταχωρήσεις της κινητικότητας των προς τα πάνω γειτόνων κόμβων του και διατηρεί μόνο την είσοδο ενδιαφερόμενη για το και τον προς τα πάνω κόμβο του. Κάθε πακέτο που φτάνει στον προορισμό του περιέχει πληροφορίες συνδετικότητας για τους κόμβους κατά μήκος της διαδρομής από την πηγή στον προορισμό του. Ο προορισμός μπορεί τώρα να επιλέξει την καλύτερη διαδρομή με την εξέταση των αριθμών κινητικότητας κατά μήκος της κάθε πορείας. Εάν πολλά μονοπάτια έχουν τον ίδιο γενικό βαθμό σταθερότητας η διαδρομή τον μικρότερο αριθμό hops επιλέγεται. Μόλις επιλεχτεί μια πορεία, ο προορισμός στέλνει ένα **REPLY** πακέτο πίσω στην πηγή κατά μήκος αυτής της πορείας. Οι κόμβοι στην διαδρομή που το REPLY πακέτο ακολουθεί σημαδεύουν τις διαδρομές ως έγκυρες. Όλες οι άλλες διαδρομές παραμένουν ανενεργές, έτσι αποφεύγονται κατά συνέπεια διπλότυπα πακέτων που φτάνουν στον προορισμό.

Η **Route reconstruction** φάση αποτελείται από τη μερική ανακάλυψη των διαδρομών – partial route discovery, άκυρη εξάλειψη των διαδρομών – **invalid route erasure**, έγκυρες αναπροσαρμογές κόμβων – **valid route updates**, και ανακάλυψη νέων διαδρομών – **new route discovery** ανάλογα με ποιους κόμβους ανήκουν στη κίνηση της διαδρομής.

Η μετακίνηση των κόμβων πηγής οδηγεί σε μια νέα διαδικασία **BQ - REPLY** επειδή το πρωτόκολλο δρομολόγησης είναι πρωτόκολλο πηγής. Το μήνυμα ανακοίνωσης (**RN- route notification**) χρησιμοποιείται για να σβήσει τις καταχωρήσεις διαδρομών που συνδέονται με τους προς τα κάτω κόμβους. Όταν ο προορισμός κινείται, ο αμέσως προς τα πάνω κόμβος προορισμού σβήνει αυτή τη διαδρομή. Μια εντοπισμένη διαδικασία ερώτησης (**LQ [H]**) όπου **H** αναφέρεται στην αρίθμηση του Hop από τον προς επάνω κόμβο στον προορισμό, κινείται για να καθορίσει εάν ο κόμβος είναι ακόμα εφικτός. Εάν ο προορισμός λαμβάνει το πακέτο **LQ** επιλέγει την καλύτερη διαδρομή και **REPLYs** διαφορετικά οι χρόνοι κόμβων έναρξης μεταφέρονται στον επόμενο κόμβο. Ένα **RN** μήνυμα στέλνεται στον επόμενο προς τα επάνω κόμβο για να σβήσει την άκυρη διαδρομή να ενημερώσει αυτόν τον κόμβο ότι πρέπει να επικαλεσθεί τη διαδικασία **LQ [H].** Εάν αυτή η διαδικασία οδηγεί σε οπισθοδρόμηση περισσότερα από τα μισά του δρόμου, η διαδικασία LQ διακόπτεται

και η πηγή κινεί μια νέα διαδικασία **BQ**. Όταν μια ανακαλυμμένη διαδρομή δεν απαιτείται πλέον, ο κόμβος πηγής αρχίζει μια διαδρομή διαγραφής μετάδοσης ( **RD – route delete**). Όλοι οι κόμβοι κατά μήκος της διαδρομής διαγράφουν την είσοδο διαδρομών από τους πίνακες δρομολόγησής τους. Το μήνυμα **RD** διαδίδεται από μια πλήρη μετάδοση, σε αντιδιαστολή με μια ευθεία μετάδοση, επειδή ο κόμβος πηγής μπορεί να μην αναγνωρίσει οποιεσδήποτε αλλαγές κόμβων διαδρομής που εμφανίστηκαν κατά τη διάρκεια **RRCs.**

## ***ΣΥΜΠΕΡΑΣΜΑ ΠΡΩΤΟΚΟΛΛΩΝ***

Υπάρχουν πολλά πρωτόκολλα δρομολόγησης για τα ad hoc δίκτυα. Αυτά τα πρωτόκολλα κατηγοριοποιούνται σε δύο κατηγορίες : **Table driven protocols ( proactive) και on demand protocols ( reactive).**
Στα table driven protocols η διαδικασία δρομολόγησης εκτελείται βάση των αποθηκευμένων πληροφοριών στους πίνακες του κάθε κόμβου του δικτύου. Αυτοί οι πίνακες πρέπει να ενημερώνονται περιοδικά. Λόγω της ενημέρωσης αυτών των πινάκων περισσότερος έλεγχος θα υπάρχει στο δίκτυο με αποτέλεσμα να μειώνεται η αποδοτικότητα του δικτύου. Όλα αυτά τα πρωτόκολλα προσπαθούν να μειώσουν τον έλεγχο του σήματος χρησιμοποιώντας διάφορες τεχνικές για να ανανεώσουν αυτούς τους πίνακες.

Στα on demand πρωτόκολλα δρομολόγησης, οι δρομολογήσεις δεν είναι έτοιμες αλλά εγκαθίστανται μόνο όταν ζητηθούν. Οι διαφορετικοί στόχοι στις on demand διαδικασίες δρομολόγησης μπορούν να περιγραφτούν σε τρεις φάσεις : **route discovery, route maintenance, and route deletion**. Αυτά τα πρωτόκολλα προσπαθούν να μειώσουν τη σηματοδότηση ελέγχου που απαιτείται για να επιτύχει αυτούς τους στόχους

# Κ Ε Φ Α Λ Α Ι Ο 4ο

# ΑΣΦΑΛΕΙΑ

Προσπαθούμε να επιτύχουμε με τους εξής τρόπους :

- **Διαθεσιμότητα,** εξασφαλίζει ικανότητα επιβίωσης παρά την άρνηση των επιθέσεων, DOS – Denial Of Service. Στο στρώμα δικτύου ο επιτιθέμενος μπορεί να αναστατώσει το πρωτόκολλο δρομολόγησης. Στα υψηλότερα στρώματα, ο επιτιθέμενος θα μπορούσε να ρίξει τις υπηρεσίες υψηλού επιπέδου π.χ,: βασική διοικητική υπηρεσία.
- **Εμπιστευτικότητα,** εξασφαλίζει ότι ορισμένες πληροφορίες δεν αποκαλύπτονται ποτέ στις αναρμόδιες οντότητες.
- **Ακεραιότητα,** το μήνυμα που διαβιβάζεται δεν αλλοιώνεται ποτέ.
- **Πιστοποίηση:** Επιτρέπει σε έναν κόμβο να εξασφαλίσει την ταυτότητα με αυτόν που επικοινωνεί**.** Ένας εισβολέας πάντα προσπαθεί να προσποιηθεί κάποιον χρήστη του δικτύου έτσι ώστε να πάρει τη θέση του στο δίκτυο και να καταστρέψει τη σωστή λειτουργία του δικτύου.
- **Μη αποκήρυξη,** εξασφαλίζεται ότι ένας δέκτης θα στείλει ένα μήνυμα όταν του ζητηθεί.

## ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ

Υπάρχουν δύο ειδών επιθέσεων : **η παθητική και ενεργητική**.

Σε μια παθητική επίθεση ένας κακόβουλος κόμβος είτε αγνοεί τις διαδικασίες που πρέπει να ολοκληρωθούν είτε ακούει το κανάλι και προσπαθεί να ανακτήσει τις πολύτιμες πληροφορίες.

Οι ενεργές επιθέσεις χαρακτηρίζονται από το σβήσιμο μηνυμάτων, απόρριψη μηνυμάτων, προσωποποίηση ενός χρήστη για να εισέλθει στο δίκτυο και να του προκαλέσει ζημιά.

Επιθέσεις από κακόβουλους χρήστες δεν γίνονται μόνο από εξωτερικές συσκευές, γίνονται και από συσκευές που ανήκουν στο ίδιο το δίκτυο, εδώ έρχεται το θέμα της

εμπιστοσύνης των συσκευών που συνδέονται στο δίκτυο, συνήθως οι χρήστες του δικτύου είναι γνωστοί στους υπόλοιπους χρήστες αλλά μερικοί άγνωστοι χρήστες προσπαθούν να συνδεθούν, άρα θα πρέπει να προσέχουμε ποιοι χρήστες συνδέονται στο δίκτυο.

# ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

Τα κρυπτογραφικά σχέδια όπως οι ψηφιακές υπογραφές υιοθετούνται συχνά για να προστατεύσουν και τις πληροφορίες δρομολόγησης καθώς επίσης και τα δεδομένα.
Στη δημόσια βασική υποδομή κάθε κόμβος έχει ένα δημόσιο / ιδιωτικό βασικό ζευγάρι. Τα δημόσια κλειδιά διανέμονται σε άλλους κόμβους ενώ τα ιδιωτικά κλειδιά διατηρούνται στους ίδιους τους κόμβους και είναι άκρως εμπιστευτικά.
Μια τρίτη αρχή ονομάζεται Αρχή Πιστοποίησης – Certification Authority ( CA) χρησιμοποιείται για τη διαχείριση των κλειδιών. Η CA έχει ένα δημόσιο / ιδιωτικό βασικό ζευγάρι κλειδιών, με το κάθε δημόσιο κλειδί να είναι γνωστό σε κάθε κόμβο και να υπογράφει πιστοποιητικά που δεσμεύουν τα δημόσια κλειδιά στους κόμβους. Η πιστοποιημένη Αρχή Πιστοποίησης πρέπει να μένει σε απευθείας σύνδεση για να απεικονίζει τις τρέχουσες συνδέσεις, δεδομένου ότι οι συνδέσεις μπορούν να αλλάξουν ανά πάσα στιγμή. Το δημόσιο κλειδί πρέπει να ανακληθεί εάν ο κόμβος που το έχει στην κατοχή του δεν είναι πλέον έμπιστος προς τους άλλους ή ακόμα είναι εκτός δικτύου. Μια ενιαία βασική διοικητική υπηρεσία για ένα ad hoc δίκτυο ίσως δεν είναι και τόσο καλή ιδέα, δεδομένου ότι μπορεί να γίνει η Αχίλλειος πτέρνα του δικτύου. Ο λόγος ότι αν η αρχή πιστοποίησης είναι εκτός λειτουργίας για κάποιο λόγο τότε οι διαθέσιμοι κόμβοι δεν θα μπορούν να πάρουν τα τρέχοντα δημόσια κλειδιά άλλων κόμβων για να εγκαταστήσουν μια ασφαλή σύνδεση. Επίσης αν η αρχή πιστοποίησης συμβιβάζεται, ο επιτιθέμενος μπορεί να υπογράψει οποιαδήποτε λανθασμένα πιστοποιητικά με το ιδιωτικό κλειδί. Αυτά τα περιστατικά μπορούν να καταστήσουν το δίκτυο πιο τρωτό και αυτό μπορεί να έχει ως αποτέλεσμα την καθολική κατάρρευση του δικτύου. Ως εκ τούτου είναι πιο συνετό να διανεμηθεί η εμπιστοσύνη σε ένα σύνολο κόμβων έτσι ώστε να αφήσει αυτούς τους κόμβους να μοιράζονται τη διαχείριση του κλειδιού για να μην παρουσιάζονται προβλήματα που συζητήθηκαν προηγουμένως.

# ΑΣΦΑΛΗ ΔΡΟΜΟΛΟΓΗΣΗ

Τα σύγχρονα πρωτόκολλα δρομολόγησης για τα ad hoc δίκτυα αντιμετωπίζουν καλά και σωστά μια δυναμικά μεταβαλλόμενη τοπολογία αλλά δεν σχεδιάζονται για να προσαρμόσουν την υπεράσπιση ενάντια στους κακόβολους επιτιθέμενους.

Οι δρομολογητές ανταλλάσσουν την τοπολογία των δικτύων προκειμένου να καθιερώσουν ανεπίσημα τις διαδρομές μεταξύ των κόμβων. Αυτός είναι ένας άλλος πιθανός στόχος για τους κακόβολους επιτιθέμενους που σκοπεύουν να ρίξουν το δίκτυο.

Οι εξωτερικοί επιτιθέμενοι επαναλαμβάνουν τις παλαιές πληροφορίες δρομολόγησης ή διαστρεβλώνουν τις πληροφορίες με σκοπό να χωρίσουν ένα δίκτυο ή να υπερφορτώσουν ένα δίκτυο με τις συνεχείς αναμεταδόσεις και την ανεπαρκή δρομολόγηση.

Οι εσωτερικοί συμβιβασμένοι κόμβοι έχουν αυστηρότερες πληροφορίες δρομολόγησης. Αυτές οι πληροφορίες υπογράφονται από τον κάθε κόμβο και δεν πρόκειται να λειτουργήσουν αν οι συμβιβασμένοι κόμβοι δεν παράγουν τις έγκυρες υπογραφές χρησιμοποιώντας τα ιδιωτικά κλειδιά τους.

Η δρομολόγηση των πρωτοκόλλων για τα ad hoc δίκτυα πρέπει να χειριστεί τις ξεπερασμένες πληροφορίες δρομολόγησης για να προσαρμόσει τη δυναμική μεταβαλλόμενη πληροφορία. Οι ψεύτικες πληροφορίες δρομολόγησης που παράγονται από τους συμβιβασμένους κόμβους μπορούν επίσης να θεωρηθούν ως ξεπερασμένες πληροφορίες δρομολόγησης. Εφ' όσον υπάρχει ικανοποιητικός αριθμός έγκυρων κόμβων, το πρωτόκολλο δρομολόγησης πρέπει να είναι σε θέση να παρακάμψει τους συμβιβασμένους κόμβους, αυτό εντούτοις χρειάζεται την ύπαρξη του πολλαπλάσιου, πρέπει να χωρίσουμε ενδεχομένως τις διαδρομές μεταξύ των κόμβων.

Η δρομολόγηση του πρωτοκόλλου πρέπει να είναι σε θέση να χρησιμοποιήσει μια εναλλάσουσα διαδρομή εάν η υπάρχουσα εμφανίζεται να σφάλει.

# ΣΥΜΦΩΝΙΑ ΚΛΕΙΔΙΩΝ ΣΤΑ ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ

## Το σενάριο

Ας υποθέσουμε μια ομάδα ανθρώπων που βρίσκονται ταυτόχρονα σε ένα δωμάτιο και προσπαθούν να εγκαταστήσουν μια ασύρματη σύνδεση για επικοινωνία μέσω των laptop τους. Εμπιστεύονται προσωπικά ο ένας τον άλλον αλλά όμως δεν έχουν κάποιο συνθηματικό κωδικό τον οποίο θα χρησιμοποιούν για να επικυρώσουν ο ένας τον άλλον. Δεν θέλουν κάποιος που βρίσκεται έξω από το δωμάτιο να εμπλακεί στην επικοινωνία τους με σκοπό ίσως να προκαλέσει κάποια δυσλειτουργία στο δίκτυο. Το συγκεκριμένο σενάριο είναι ιδιαίτερα τρωτό σε οποιοδήποτε επιτιθέμενο που όχι μόνο μπορεί να ελέγξει την επικοινωνία αλλά ακόμα μπορεί να τροποποιήσει τα μηνύματα και μπορεί επίσης να παρεμβάλει τα μηνύματα και να τα κάνει να εμφανίζονται ότι προέρχονται μέσα από το δωμάτιο. Αυτό είναι ένα κλασικό παράδειγμα ad hoc δικτύου και ο απλούστερος τρόπος να αντιμετωπιστεί αυτό το παράδειγμα είναι να υπάρξει μια συμφωνία κλειδιών , χαρτογράφηση των θέσεων έτσι ώστε να υπάρχει ταυτοποίηση της θέσης ( με κάποιο μηχανισμό ταυτοποίησης) για τη συμφωνία των κλειδιών, π.χ. συμμετέχοντες που γράφουν τις διευθύνσεις IP σε ένα κομμάτι χαρτιού και τις περνούν γύρω γύρω στους συμμετέχοντες. Έπειτα ένα πιστοποιητικό βασισμένο σε μηχανισμό κλειδιού μπορεί να χρησιμοποιηθεί. Αυτά τα δημόσιο βασικά πιστοποιητικά μπορούν να επιτρέψουν στους συμμετέχοντες να ελέγξουν τη σύνδεση μεταξύ της διεύθυνσης IP και των κλειδιών των συμμετεχόντων.

## Ο κωδικός που βασίζεται στην επικύρωση της ανταλλαγής του κλειδιού

Ένας κωδικός επιλέγεται και μοιράζεται μεταξύ των παρόντων στο δωμάτιο , αυτός ο κωδικός πρέπει να αποτελείται από πολλούς χαρακτήρες έτσι ώστε να είναι δύσκολος να βρεθεί, σίγουρα θα είναι λιγότερο φιλικός στους χρήστες, θα πρέπει να αποφεύγονται κωδικοί που χαρακτηρίζουν κάποιο χρήστη ( όπως όνομα ή ημερομηνία γέννησης) γιατί είναι οι πρώτες προσπάθειες που κάνουν οι εισβολείς έτσι ώστε να μαντέψουν τον κωδικό.

## 1. Επιθυμητές ιδιότητες για ένα τέτοιο πρωτόκολλο

### Μυστικότητα

Μόνο εκείνοι οι χρήστες που γνωρίζουν τον αρχικό μυστικό κωδικό πρέπει να μάθουν το κλειδί και κανένας άλλος.

### Τέλεια Μυστικότητα Επόμενης κίνησης

Ακόμα και στην περίπτωση που ένας εισβολέας πετύχει συμβιβασμό με κάποιον συμμετέχοντα δεν θα μπορεί να υπολογίσει το κλειδί ως αποτέλεσμα προηγούμενου τρεξίματος του πρωτοκόλλου.

### Ανοχή στις προσπάθειες διάσπασης

Όχι μόνο οι δυνατοί εισβολείς ( δηλαδή αυτοί που προσπαθούν να καταστρέψουν το δίκτυο τελείως) αλλά και οι αδύνατοι εισβολείς ( αυτοί που προσπαθούν να εισέλθουν στο δίκτυο αλλά δεν μπορούν να σβήσουν ή να μετατρέψουν κάποιο μήνυμα) πρέπει να αντιμετωπίζονται σωστά από το συγκεκριμένο πρωτόκολλο.

## 2. ΤΟ ΕΠΙΘΥΜΗΤΟ ΠΡΩΤΟΚΟΛΛΟ

Το A και το B είναι δύο κόμβοι επικοινωνίας με ένα κοινό μυστικό κωδικό p. ($E_A$, $D_A$) είναι τα κλειδιά του A. Τα βήματα που ακολουθούνται είναι τα εξής :

(1) A --> B : A, P($E_A$).
Το A κρυπτογραφεί $E_A$ με τον κωδικό και το στέλνει στο B. Στέλνει επίσης μια ετικέτα 'A' για να προσδιορίσει τον εαυτό του.

(2) Το B ξέρει το 'P έτσι αποκρυπτογραφεί p($E_A$) αποσπώντας τα $E_A$ .Το B παράγει το 'R' τυχαία, το κρυπτογραφεί χρησιμοποιώντας το $E_A$ και ολόκληρο το πράγμα κρυπτογραφείται με το P και στέλνεται στο A.

B --> A : P($E_A$ (R)).

Αυτό το μήνυμα επικυρώνει το Β στο Α, δεδομένου ότι τι το Β μπορεί να εξαγάγει το $E_A$ από το μήνυμα που στέλνεται από το Α στο Β μόνο αν το Β ξέρει το κωδικό 'P'.

(3) Το Α αποκρυπτογραφεί αυτό το μήνυμα, εξάγει το R , παράγει $(challenge)_A$ και $S_A$, κρυπτογραφούν χρησιμοποιώντας το R και το στέλνουν στο Β.

A --> B : $R((challenge)_A, S_A)$.

Αυτό το μήνυμα επικυρώνει το Α στο Β, δεδομένου ότι το Α μπόρεσε να εξαγάγει το R μόνο εάν ήξερε το σύνθημα P.

(4) Το Β αποκρυπτογραφεί αυτό το μήνυμα, εξάγει το $(challenge)_A$ και $S_A$. Έπειτα υπολογίζει το $h( ((challenge)_A)$ όπου το h() είναι μια hash λειτουργία. Β έπειτα παράγει (challenge)B και $S_B$ και έπειτα στέλνει $h((challenge)_A)$, $((challenge)_B$ και $S_B$ στο Α, που κρυπτογραφείται από το R.

B --> A : $R(h((challenge)_A), (challenge)_B, S_B)$.

Αυτό το μήνυμα χρησιμεύει ως μια αναγνώριση στο προηγούμενο μήνυμα του Α από το βήμα (3) κι δηλώνει επίσης στο Α ότι το $S_A$ έχει σημειωθεί επιτυχώς.

(5) Το Α αποκρυπτογραφεί αυτό το μήνυμα, εξάγει $(challenge)_B$ και $S_B$. Το Α υπολογίζει το $h((challenge)_B)$, το κρυπτογραφεί χρησιμοποιώντας το R και το στέλνει στο Β.

A --> B : $R((challenge)_B)$.

Αυτό το μήνυμα χρησιμεύει ως μια αναγνώριση στο Β λέγοντας ότι το $S_B$ έχει σημειωθεί.

Τώρα και τα δύο μέρη Α και Β γνωρίζουν το $S_A$ και το $S_B$ οπότε και τα δύο μπορούν να υπολογίσουν το κλειδί συνόδου $K = f(S_A, S_B)$ και μπορούν να επικοινωνήσουν.

Αυτό το πρωτόκολλο μπορεί να επεκταθεί έτσι ώστε να χρησιμοποιήσει έναν ηγέτη. Ο ηγέτες θα μεταδώσει το μήνυμα στο βήμα (1) ,το υπόλοιπο των μηνυμάτων θα είναι σημείο προς σημείο με το Α να παίζει το ρόλο του ηγέτη.

Κάθε φορά που τρέχει το πρωτόκολλο, κάθε χρήστης μοιράζεται ένα κλειδί με τον ηγέτη. Ένας πρόσθετος κύκλος θα απαιτηθεί για τον ηγέτη για ένα επιλέξει ένα κοινό κλειδί συνόδου και για να το διανείμει μεταξύ άλλων χρηστών χρησιμοποιώντας το ζευγάρι κλειδιού που ο χρήστης μοιράζεται με τους συμμετέχοντες. Το μόνο μειονέκτημα για αυτό το πρωτόκολλο είναι ότι το κλειδί επιλέγεται μόνο από τον ηγέτη.

Εντούτοις, μπορούμε ελαφρώς να τροποποιήσουμε το πρωτόκολλο για να το κάνουμε να ενεργήσει ως συμβάλλον πολύ- χρηστικό πρωτόκολλο.
Οι προκλήσεις $(\text{challenge})_A$ και$(\text{challenge})_B$ χρησιμοποιούνται από το A και B για να επιβεβαιώσουν ότι ο άλλος γνωρίζει τον κωδικό P.
Οι τυχαίες ποσότητες $S_A$ και $S_B$ που ήδη έχουν παραχθεί θα μπορούσαν να χρησιμοποιηθούν με σκοπό να επιβεβαιωθούν .
Αυτές οι ποσότητες χρησιμοποιούνται για να παραγάγουν το τελικό κλειδί συνόδου K = $f(S_A, S_B)$, τα $S_A$ και $S_B$ θα μπορούσαν να χρησιμοποιηθούν για να επιβεβαιώσουν ο ένας τον άλλον στο K.

Έτσι το τροποποιημένο πρωτόκολλο είναι :

(1) A --> B : A, $P(E_A)$.

(2) B --> A : $P(E_A (R, S_B))$.

Σημείωση : $(\text{challenge})_B$ αντικαταστάθηκε από το $S_B$ .

(3) A --> B : $R(S_A)$.

Το $S_A$ χρησιμοποιήθηκε στη θέση του $(\text{challenge})_A$.

(4) A --> B : $K(S_A, h(S_A, S_B))$.

(5) B --> A : $K(S_B, h(S_A, S_B))$.

Τα τελευταία δύο βήματα 4 και 5 χρησιμοποιούνται από τα λαμβάνον μέρη ( B και A αντίστοιχα) ότι το σταλμένο μέρος ( A και B αντίστοιχα) γνωρίζουν το K ( και ως εκ τούτου το P ). Το h(., .) είναι μια δημόσια hash λειτουργία.

Αυτό το πρωτόκολλο μπορεί να επεκταθεί εύκολα σε πολλαπλά μέρη.

Ας υποθέσουμε ότι Mi i = 1 με n το σύνολο των n χρηστών και το $M_n$ ο αρχηγός, Si το τυχαίο μερίδιο που συμβάλλει στο $M_i$ προς την παραγωγή του τελικού κλειδιού K.

(1) $M_n$ --> ALL : $M_n$, P(E).
(2) $M_i$ --> $M_n$ : $M_i$, $P(E(R_i, S_i))$, i = 1 to n-1.
(3) $M_n$ --> $M_i$ : $R_i(\{S_j, j = 1 \text{ to } n\})$, i = 1 to n-1.
(4) $M_i$ --> $M_n$ : $M_i$.

Το τελευταίο βήμα επιβεβαιώνει σε κάθε χρήστη ότι ένας άλλος χρήστης ξέρει το ίδιο κλειδί K. Το πολύ σχεδιασμένο πρωτόκολλο είναι συμβάλλον δεδομένου ότι ο κάθε χρήστης έχει συμβολή ως προς την παραγωγή του τελικού κλειδιού. Το $M_n$ παίρνει τις συνεισφορές από κάθε χρήστη και συνδυάζει καθεμία τους για να παράσχει το τελικό κλειδί 'K'.
Το πρωτόκολλο επίσης παρέχει τέλεια μυστικότητα για όλα τα μέρη εκτός από αυτά που ξέρουν το κλειδί αποκρυπτογράφησης D, εκτός και αν το κλειδί αποκρυπτογράφησης επίσης καταστραφεί στο τέλος του πρωτοκόλλου. Ο εισβολέας που πετυχαίνει συμβιβασμό με τον αρχηγό $M_n$ είναι σε θέση να αποκρυπτογραφήσει ένα αντίγραφο της προηγούμενης συνόδου.
Το πρωτόκολλο είναι επίσης ανεκτικό των προσπαθειών διάσπασης από τον καθένα εκτός από τον $M_n$ . Ο επιτιθέμενος που δεν ξέρει κάποια στοιχεία θα προσπαθήσει να στείλει κάποια ψεύτικα στοιχεία, έτσι οι αληθινοί χρήστες συμφωνούν σε ένα κλειδί που έχει μια συμβολή από τον επιτιθέμενο, εντούτοις ο επιτιθέμενος δεν μπορεί να καθορίσει το κλειδί συνόδου γιατί δεν έχει τη γνώση του αρχικού κοινού κωδικού P.
Δεδομένου ότι το πρωτόκολλο είναι συμβαλλόμενο, ένα ορισμένο ποσό καθυστέρησης εισάγεται με αυτό, δεδομένου ότι ο ηγέτης πρέπει να περιμένει τις συνεισφορές από τον κάθε χρήστη πριν ξεκινήσει να στέλνει μηνύματα.

# 3. ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΚΩΔΙΚΟΥ Diffie – Hellman ΑΝΤΑΛΛΑΓΗ ΚΛΕΙΔΙΟΥ

## *1. Έκδοση δύο συμβαλλόμενων μερών*

Στο στοιχειώδες πρωτόκολλο DH, δύο συμβαλλόμενα μέρη Α και Β συμφωνούν σε ένα πρωταρχικό ρ και σε ένα παραγόμενο g σε μια πολλαπλασιαστική ομάδα Zp* ( το σύνολο {1, 2, …, p-1}. Α και Β επιλέγουν τα τυχαία μυστικά SA και SB έτσι ώστε 1 <= $S_A$, $S_B$ <= p-1.

(1) Το Α υπολογίζει $g^{SA}$ , το κρυπτογραφεί με το κοινό κρυφό κωδικό Ρ και το στέλνει στο Β.

A --> B : A, P($g^{SA}$).

(2) Το Β εξάγει το $g^{SA}$ από το μήνυμα υπολογίζει το $g^{SB}$ και επίσης υπολογίζει το κλειδί συνόδου K = $(g^{SA})^{SB}$ . Το Β έπειτα διαλέγει μια τυχαία πρόκληση $C_B$ και την κρυπτογραφεί χρησιμοποιώντας το βασικό κλειδί Κ. Το Β κρυπτογραφεί το $S_B$ χρησιμοποιώντας το Ρ. Κατόπιν στέλνει τις δύο ποσότητες στο Α.

B --> A : P($S_B$), K($C_B$).

(3) Το Α εξάγει το $S_B$ από το P($S_B$) και υπολογίζει το κλειδί K = $(g^{SA})^{SB}$ . Εξάγει έπειτα το $C_B$ με την αποκρυπτογράφηση του K($C_B$). Το Α έπειτα παράγει το τυχαίο $C_A$ κρυπτογραφώντας και το $C_A$ και το $C_B$ με το Κ και το στέλνει στο Β.

A --> B : $K(C_A, C_B)$.

(4) Αυτό το μήνυμα (3) πείθει το Β ότι το Α ήταν σε θέση να αποκρυπτογραφήσει το μήνυμα στο (2) σωστά. Το Β κρυπτογραφεί το $C_A$ χρησιμοποιώντας Κ και το στέλνει στο Α.

B --> A : $K(C_A)$.

Το Α κρυπτογραφεί το μήνυμα για να δει αν το καθαρό κείμενο είναι πράγματι $C_A$ . Αυτό θα έπειθε το Α ότι το Β γνωρίζει το Κ. Αυτό θα έπειθε στη συνέχεια το Α ότι το Β ήξερε το Ρ.

## *2. Έκδοση πολλών μερών*

Υπάρχουν ακριβώς ας υποθέσουμε n χρήστες $M_1, M_2, \ldots, M_n$ που όλοι μοιράζονται τον κωδικό Ρ, κάθε χρήστης παράγει μια τυχαία ποσότητα Si που είναι η συμβολή του στο ενδεχόμενο κλειδί συνόδου $K = g^{S1S2\_\_\_Sn\text{-}1Sn}$ .
Το πρωτόκολλο διαιρείται σε τρία μέρη. Στο πρώτο μέρος ( τα βήματα 1 και 2 ) οι χρήστες $M_i$ to $M_{n-1}$ παράγουν ένα ενδιάμεσο κλειδί.

$PI = g^{S1S2\_\_\_Sn-1}$ στα n-1 βήματα

Στο δεύτερο μέρος ( βήματα 3 και 4) κάθε $M_i$ (i = 1 to n-1) έχει ένα χωριστό με το $M_n$, στο τέλος του οποίου όλοι οι χρήστες είναι σε θέση να υπολογίσουν το Κ.
Το τρίτο μέρος ( βήμα 5) είναι η επιβεβαίωση του κλειδιού.

(1) $M_i$ --> $M_{i+1}$ : $g^{S1S2\_\_\_Si}$, i = 1 to n-2 στη σειρά
(2) $M_{n-1}$ --> ALL : $PI = g^{S1S2\_\_\_Sn-1}$, στη μετάδοση
(3) $M_i$ --> $M_n$ : $P(C_i)$, i = 1 to n-1, παράλληλα, όπου $C_i = PI^{Si'/Si}$ και $S_i$ ‘ είναι ο παράγοντας που τυχαία επιλέγεται από το Mi.
(4) $M_n$ --> $M_i$ : $(C_i)\ S_n$, i = 1 to n-1, παράλληλα.
(5) $M_i$ --> ALL : $M_i$, $K(M_i, h(M_1, M_2,\ldots, M_n)$ στη μετάδοση.

Το βήμα 1 αποτελείται από (n-2) υποβήματα. Στο πρώτο υποβήμα ο χρήστης $M_1$ υπολογίζει το $g^{S1}$ και το στέλνει στο $M_2$ . Στο τέλος του (n-2) υποβήματος, $M_{n-1}$ λαμβάνει το $g^{S1S2\_\_\_Sn-2}$ το οποίο αυξάνεται από το ($S_{n-1}$) για να πάρει το ενδιάμεσο κλειδί $PI = g^{S1S2\_\_\_Sn-1}$.

Στο βήμα 2, $M_{n-1}$ μεταδίδει αυτό το PI στον καθένα. Τώρα κάθε $M_i$ (i = 1 to n-1) αφαιρεί τη συμβολή του δηλαδή, το $S_i$ (i = 1 to n-1) από το PI αντίστοιχα αλλά επίσης εισάγει ένα τυχαία επιλεγμένο παράγοντα $S_i$ , κρυπτογραφώντας ολόκληρο το πράγμα με τον κοινό μυστικό P.
Στο βήμα 3, κάθε $M_i$ θα στείλει παράλληλα την κρυπτογράφηση στο $M_n$.Το $M_n$ αποκρυπτογραφεί το λαμβανόμενο μήνυμα για να εξάγει το $C_i$.
Έπειτα αυξάνει το κάθε $C_i$ από το $S_n$ και γυρνάει το αποτέλεσμα παράλληλα σε κάθε Mi. Σε αυτό το σημείο κάθε χρήστης μπορεί να υπολογίσει το κλειδί συνόδου ως εξής : $K = g^{S1S2\_\_\_Sn-1Sn}$. $M_n$ αυξάνει το PI από $S_n$ : $K = (PI)^{Sn}$. Κάθε $M_i$ λαμβάνει την ποσότητα από το $M_n$ και ξανά - εισάγει το αυθεντικό $S_i$ για να κατασκευάσει το κλειδί συνόδου $K = g^{S1S2\_\_\_Sn-1Sn} = (PI)^{Sn}$.

Τέλος, κάποιος χρήστης μεταδίδει ένα βασικό μήνυμα επιβεβαίωσης που επιτρέπει σε κάθε χρήστη να ελέγξει ότι τουλάχιστον ένας άλλος χρήστης έχει αποφασίσει το ίδιο κλειδί K.

Ο τυχαίος παράγοντας $S_i$ χρησιμοποιείται για τους ακόλουθους λόγους :
(a) Χωρίς την τυχαία αναζήτηση, η ποσότητα που κρυπτογραφείται μαζί με το P από το $M_{n-1}$ από το βήμα 3 είναι η ίδια όπως τη λαμβάνει από το βήμα 1.

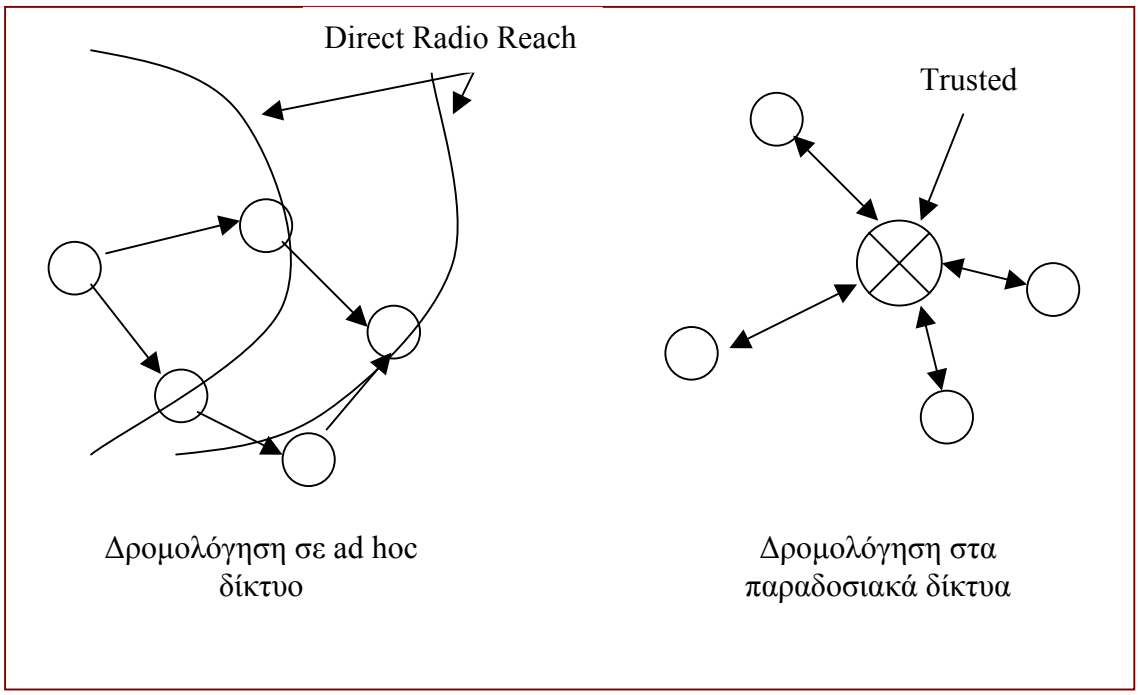
(b) Ένας επιτιθέμενος θα μπορούσε να στείλει ένα $g^{S1S2\_\_\_Si}$ στο $M_i$ στο βήμα 2 αντί της μετάδοσης του μηνύματος ( ενδιάμεσο κλειδί ) PI. Αν το $M_i$ χρησιμοποιεί την ποσότητα για να παράγει ένα μήνυμα στο βήμα 3, το προκύπτον μήνυμα είναι ίδιο με το βήμα που λαμβάνεται από το $M_i$ στο βήμα 1. Για να αποτρέψει τις επιθέσεις αυτή η λειτουργία είναι απαραίτητη.

Αυτό το πρωτόκολλο παρέχει την τέλεια μυστικότητα.

# ΠΡΟΒΛΗΜΑΤΑ ΣΤΗ ΔΡΟΜΟΛΟΓΗΣΗ AD HOC ΔΙΚΤΥΩΝ

## 1. Υποδομή

Όπως έχουμε προαναφέρει ένα ad hoc δίκτυο είναι μειωμένης δομής δίκτυο. Αντίθετα με τα παραδοσιακά δίκτυα δεν υπάρχει κάποια προ αναπτυγμένη υποδομή όπως η ύπαρξη δρομολογητών που θα παίξουν τον ρόλο του διαχειριστή ή κάποια αυστηρή πολιτική για την υποστήριξη της δρομολόγησης. Οι κόμβοι οι ίδιοι είναι αρμόδιοι για τη δρομολόγηση των πακέτων, κάθε κόμβος στηρίζεται στους άλλους κόμβους για να πάρει κάποια πακέτα από αυτούς. Οι κινητοί κόμβοι στην άμεση ράδιο σειρά με έναν άλλον μπορούν να επικοινωνήσουν άμεσα, αλλά οι συσκευές που βρίσκονται πολύ μακριά εξαρτώνται από τους ενδιάμεσους κόμβους έτσι ώστε να λάβουν δρομολογημένα πακέτα από αυτούς. Οι δύο διαφορετικές υποδομές φαίνονται στην παρακάτω εικόνα 14.




**Εικόνα 14: Διαφορετικές υποδομές**

## 2. Συχνές αλλαγές στην τοπολογία του δικτύου

Τα ad hoc δίκτυα περιέχουν κόμβους οι οποίοι μπορούν συχνά να αλλάξουν τις θέσεις τους, ως εκ τούτου η τοπολογία σε αυτά τα δίκτυα είναι ιδιαίτερα δυναμική. Αυτό οδηγεί στους συχνά μεταβαλλόμενους γείτονες στους οποίους ένας κόμβος στηρίζεται για τη δρομολόγηση. Κατά συνέπεια τα παραδοσιακά πρωτόκολλα δρομολόγησης δεν μπορούν πλέον να χρησιμοποιηθούν σε ένα τέτοιο περιβάλλον. Αυτό εξουσιοδοτεί τα νέα πρωτόκολλα δρομολόγησης που μπορούν να χειριστούν την δυναμική τοπολογία με τη διευκόλυνση των ανακαλύψεων νέων διαδρομών.

## 3. Προβλήματα που συνδέονται με την ασύρματη επικοινωνία

Δεδομένου ότι η επικοινωνία είναι μέσω του ασύρματου μέσου, είναι δυνατό για οποιοδήποτε εισβολέα να τρυπήσει την επικοινωνία εύκολα.
Τα ασύρματα κανάλια προσφέρουν ιδιαίτερα φτωχή προστασία και τα σχετικά μηνύματα ελέγχου δρομολόγησης μπορούν να πειραχτούν. Το ασύρματο μέσο είναι ιδιαίτερα ευαίσθητο στην παρέμβαση και στη διαστρέβλωση σημάτων. Ένας εισβολέας μπορεί εύκολα να κρυφακούσει έτσι ώστε να ξέρει τις ευαίσθητες πληροφορίες δρομολόγησης ή να φράξει τα σήματα για να αποτρέψει τη διάδοση της δρομολόγησης των πληροφοριών ή ακόμα χειρότερα να διακόψει τα μηνύματα και να χειριστεί τις διαδρομές όπως αυτός θέλει. Η δρομολόγηση των πρωτοκόλλων πρέπει να σχεδιαστεί καλά για να χειριστεί τέτοια προβλήματα.

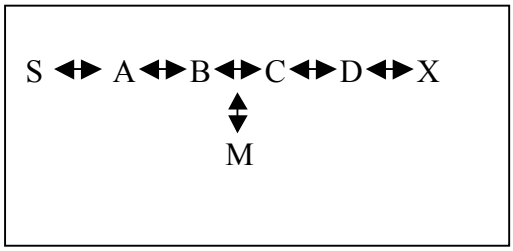
## 4. Προβλήματα με τα υπάρχοντα πρωτόκολλα δρομολόγησης

- **Υπονοούμενη σχέση εμπιστοσύνης μεταξύ των γειτόνων**, τα τρέχοντα πρωτόκολλα δρομολόγησης ad hoc εμπιστεύονται όλους τους συμμετέχοντες στο δίκτυο. Τα περισσότερα ad hoc πρωτόκολλα δρομολόγησης είναι ιδιαίτερα συνεργάσιμα από τη φύση τους και εξαρτώνται από τους γειτονικούς κόμβους όσον αφορά τα πακέτα διαδρομών. Αυτό το αφελές πρότυπο εμπιστοσύνης επιτρέπει στους κακόβολους χρήστες να παραλύσουν ένα ad hoc δίκτυο με την παρεμβολή των λανθασμένων αναπροσαρμογών δρομολόγησης,

επανάληψη παλαιών μηνυμάτων, αλλαγή των αναπροσαρμογών δρομολόγησης ή διαφήμιση των ανακριβών πληροφοριών δρομολόγησης. Αυτές οι επιθέσεις μπορεί να συμβούν και σε ένα δομημένο δίκτυο, το ad hoc περιβάλλον κάνει αυτή την ανίχνευση δύσκολη.

- **Ρυθμαπόδοση:** τα ad hoc δίκτυα μεγιστοποιούν τη συνολική ρυθμαπόδοση δικτύου χρησιμοποιώντας όλους τους διαθέσιμους κόμβους για τη δρομολόγηση και την αποστολή πακέτων. Εντούτοις έχει παρατηρηθεί το φαινόμενο ένας κόμβος να μην συμπεριφέρεται σωστά σε σχέση με τη συμφωνία, να διαβιβάζει πακέτα επειδή είναι υπερφορτωμένος , κακόβουλος ή σπασμένος. Οι κόμβοι απρεπής συμπεριφοράς μπορούν να είναι ένα σημαντικό πρόβλημα, αυτή η απώλεια στη ρυθμαπόδοση λόγω συσκευών με απρεπή συμπεριφορά μπορεί να προκαλέσει πρόβλημα στο δίκτυο.

- **Επιθέσεις που χρησιμοποιούν την τροποποίηση των τομέων πρωτοκόλλου των μηνυμάτων:** Τα τρέχοντα πρωτόκολλα δρομολόγησης υποθέτουν ότι οι κόμβοι δεν αλλάζουν τους τομείς πρωτοκόλλου των μηνυμάτων που περνούν μεταξύ των κόμβων. Τα πακέτα πρωτοκόλλου δρομολόγησης φέρνουν τις σημαντικές πληροφορίες ελέγχου που κυβερνούν τη συμπεριφορά της μετάδοσης στοιχείων στα ad hoc δίκτυα. Δεδομένου ότι το επίπεδο εμπιστοσύνης σε ένα παραδοσιακό ειδικό δίκτυο δεν μπορεί να μετρηθεί ή να επιβληθεί, οι εχθρικοί κόμβοι μπορούν να συμμετάσχουν άμεσα στην ανακάλυψη διαδρομών και μπορούν να παρεμποδίσουν και πακέτα πρωτοκόλλου δρομολόγησης φίλτρων για να αναστατώσουν την επικοινωνία. Οι κακόβουλοι κόμβοι μπορούν εύκολα να προκαλέσουν τον επαναπροσανατολισμό της κυκλοφορίας δικτύου και να επιχειρήσουν DOS επιθέσεις αλλάζοντας απλά αυτούς τους τομείς. Για παράδειγμα, σε ένα δίκτυο όπως απεικονίζεται στην εικόνα 15, ένας κακόβουλος κόμβος M μπορεί να κρατά την κυκλοφορία από την επίτευξη του X με συνέπεια να διαφημίζει στο B μια γρηγορότερη διαδρομή στο X από αυτή που διαφημίζει ο κόμβος C.




**Εικόνα 15 : Δομή δικτύου**

Οι επιθέσεις μπορούν να ταξινομηθούν ως μακρινές επιθέσεις επαναπροσανατολισμού και άρνηση των επιθέσεων υπηρεσιών - DOS attacks. Ας εξετάσουμε τις επιθέσεις αυτές :

a) **Επαναπροσανατολισμός με τον τροποποιημένο αριθμό ακολουθίας διαδρομών – Remote redirection with modified route sequence number AODV.** Οι μακρινές επιθέσεις επαναπροσανατολισμού καλούνται επίσης επιθέσεις μαύρων τρυπών .Σε αυτού του είδους τις επιθέσεις ένας κακόβουλος χρήστης χρησιμοποιεί ένα πρωτόκολλο δρομολόγησης για να διαφημιστεί ως η πιο σύντομη πορεία στους κόμβους των οποίων τα πακέτα θέλει να παρεμποδίσει να μεταδοθούν σωστά. Τα πρωτόκολλα όπως το AODV διατηρούν διαδρομές με την ανάθεση των αυξανόμενων αριθμών ακολουθίας στις διαδρομές προς έναν συγκεκριμένο προορισμό. Στο AODV οποιοσδήποτε κόμβος μπορεί να εκτρέψει την κυκλοφορία μέσω του εαυτού διαφημίζοντας μια διαδρομή σε ένα κόμβο με ένα αριθμό ακολουθίας μεγαλύτερο από την πραγματική αξία.

   Στην εικόνα 15 είδαμε τη δομή ενός τυπικού ad hoc δικτύου, υποθέτουμε ότι ένας κακόβουλος χρήστης M λαμβάνει ένα μήνυμα RREQ το οποίο προέρχεται από τον κόμβο S και έχει ως προορισμό τον κόμβο X μετά από τον κόμβο B . Ο κόμβος M επαναπροσανατολίζει την κίνηση προς το B περιέχοντας μια σημαντικά υψηλότερη ακολουθία προορισμού για το X μεγαλύτερη από αυτή που είχε σχεδιαστεί αρχικά για το X.

b) **Επαναπροσανατολισμός με την τροποποιημένη αρίθμηση Hop – Redirection with modified hopc count (AODV).** Μια επίθεση επαναπροσανατολισμού είναι επίσης δυνατή σε ορισμένα πρωτόκολλα όπως το AODV, από την τροποποίηση του τομέα αρίθμησης των hop στα μηνύματα ανακαλύψεων διαδρομών. Όταν οι αποφάσεις για τη δρομολόγηση δεν μπορούν να ληφθούν από άλλα συστήματα , το AODV χρησιμοποιεί τον τομέα αρίθμησης hop για να καθορίσει μια σύντομη διαδρομή. Στο AODV οι κακόβουλοι χρήστες μπορούν να προσελκύσουν τη διαδρομή θέτοντας στον τομέα αρίθμησης hop του μηνύματος RREP την τιμή μηδέν. Ομοίως με τον καθορισμό του τομέα αρίθμησης hop του μηνύματος RREP στο άπειρο, οι διαδρομές θα τείνουν να δημιουργηθούν χωρίς να περιλαμβάνουν τον κακόβουλο κόμβο.

   Από τη στιγμή που ένας κακόβουλος χρήστης είναι σε θέση να παρεμβληθεί μεταξύ δυο συσκευών επικοινωνίας μπορεί να κάνει τα πάντα με τα πακέτα που περνούν ανάμεσα από αυτούς τους κόμβους. Μπορεί να καταστρέψει τα πακέτα αυτά ή ακόμα να μην τα αφήσει να κινηθούν μέσα στο δίκτυο.

c) **Άρνηση της υπηρεσίας με τις τροποποιημένες διαδρομές πηγής - Denial of service with modified source routes.** Το DSR είναι ένα πρωτόκολλο δρομολόγησης το οποίο δηλώνει ρητά τις διαδρομές στα πακέτα δεδομένων. Αυτές οι διαδρομές στερούνται οποιουδήποτε ελέγχου ακεραιότητας και μια απλή επίθεση άρνησης υπηρεσιών μπορεί να προωθηθεί στο DSR με αποτέλεσμα να αλλαχθεί η διαδρομή της πηγής στις επιγραφές των πακέτων.

   Η τροποποίηση στις διαδρομές πηγής σε DSR μπορεί επίσης να περιλάβει την εισαγωγή των βρόχων στη διευκρινισμένη πορεία . Αν και το DSR αποτρέπει την εισαγωγή βρόχων κατά τη διάρκεια της διαδικασίας ανακαλύψεων διαδρομών, υπάρχουν ανεπαρκή μέτρα προστασίας να αποτραπεί η εισαγωγή των βρόχων σε μια διαδρομή πηγής αφότου έχει σωθεί μια διαδρομή.

**5. Επιθέσεις που χρησιμοποιούν την προσωποποίηση.**

Τα πρωτόκολλα ενός ad hoc δικτύου δεν επικυρώνουν τη διεύθυνση πηγής IP. Ένας κακόβουλος κόμβος μπορεί να προωθήσει πολλές επιθέσεις αλλάζοντας την MAC ή IP διεύθυνση του, και τα δύο πρωτόκολλα AODV και DSR είναι ιδιαίτερα ευαίσθητα σε αυτή την επίθεση.

## 6. Επιθέσεις που χρησιμοποιούν την επεξεργασία.

Η παραγωγή των λανθασμένων μηνυμάτων δρομολόγησης καλείται ως επεξεργασία μηνυμάτων. Τέτοιες επιθέσεις είναι δύσκολο να ανιχνευθούν.

### I. Πλαστογράφηση των μηνυμάτων λάθους διαδρομών σε AODV ή DSR - Falsifying route error messages in AODV or DSR.

Τα πρωτόκολλα AODV και DSR εφαρμόζουν τα μέτρα συντήρησης πορειών για να ανακτηθούν οι σπασμένες πορείες όταν κινούνται οι κόμβοι. Εάν ένας κόμβος προορισμού ή ένας ενδιάμεσος κόμβος σε ένα μονοπάτι διαδρομής κινηθεί, ο πιο κοντινός κόμβος σε αυτό στέλνει ένα μήνυμα λάθους διαδρομής έτσι ώστε να ειδοποιήσει όλους τους γύρω γείτονες. Ο κόμβος ακυρώνει επίσης την διαδρομή για αυτόν τον προορισμό στον πίνακα δρομολόγησής του.

Το πρόβλημα σε αυτή την περίπτωση είναι ότι κάποιες επιθέσεις μπορούν να εμφανιστούν στέλνοντας ψεύτικα μηνύματα λάθους διαδρομών. Ας εξετάσουμε ένα παράδειγμα, υποθέτουμε ότι ο κόμβος S έχει μια διαδρομή στον κόμβο X μέσα από τους κόμβους A,B,C όπως φαίνονται στην εικόνα 15. Ένας κακόβουλος κόμβος M μπορεί να προωθήσει μια άρνηση επίθεσης υπηρεσιών ενάντια στο X κόμβο, στέλνοντας συνεχώς μηνύματα λάθους διαδρομών στο κόμβο B όσον αφορά τον κόμβο C , δείχνοντας μια σπασμένη σύνδεση μεταξύ των κόμβων C και X. Ο κόμβος B λαμβάνει το μήνυμα λάθους διαδρομών νομίζοντας ότι προήλθε από το C. Τότε ο κόμβος B διαγράφει την εισαγωγή του πίνακα δρομολόγησης του για τον κόμβο X και διαβιβάζει το μήνυμα λάθους στον A που και αυτός με τη σειρά του διαγράφει αυτή τη διαδρομή από τον πίνακα δρομολόγησής του. Εάν ο κόμβος M ακούσει τα μηνύματα λάθους διαδρομών όποτε μια

διαδρομή καθιερώνεται από το S και το X , ο κόμβος M μπορεί επιτυχώς να αποτρέψει την επικοινωνία μεταξύ των δύο αυτών κόμβων.

### II. Δηλητηρίαση διαδρομών στο DSR

Αυτό είναι μια παθητική επίθεση που μπορεί να εμφανιστεί στο DSR λόγω του τρόπου με τον οποίο ενημερώνει τον πίνακα δρομολόγησής του το συγκεκριμένο πρωτόκολλο.
Αυτό εμφανίζεται όταν διαγράφονται ή αλλάζονται πληροφορίες που αποθηκεύονται στον πίνακα δρομολόγησης.
Εκτός από την αναγνώριση των διαδρομών από τις επιγραφές των πακέτων, καθώς ένας κόμβος επεξεργάζεται κατά μήκος μιας πορείας, η διαδρομή μπορεί να μαθευτεί από προηγούμενα ληφθείσα πακέτα.
Ένας κόμβος που κρυφακούει οποιοδήποτε πακέτο μπορεί να προσθέσει πληροφορίας δρομολόγησης που περιέχεται στην επιγραφή του πακέτου στη δική του μνήμη ακόμα και αν εκείνος ο κόμβος δεν είναι στην πορεία του προορισμού του πακέτου.

Το πρόβλημα με τη συγκεκριμένη μέθοδο είναι ότι ένας επιτιθέμενος μπορεί εύκολα να εκμεταλλευτεί αυτή την μέθοδο μαθαίνοντας τις διαδρομές με σκοπό να τις χρησιμοποιήσει έπειτα για δικό του σκοπό. Ας υποθέσουμε ότι ένας κακόβουλος κόμβος M προσπαθεί να δηλητηριάσει τις διαδρομές στον κόμβο X, αν ο κόμβος M ήθελε να μεταδώσει πακέτα στον κόμβο X τότε οι γειτονικοί κόμβοι που κρυφακούνε τη μετάδοση πακέτων μπορεί να προσθέσουν τη διαδρομή στη δικιά τους μνήμη.

### III. Επίθεση υπερχείλισης δρομολόγησης

Στη συγκεκριμένη μέθοδο ο επιτιθέμενος προσπαθεί να δημιουργήσει τη διαδρομή στους ανύπαρκτους κόμβους. Ο στόχος του επιτιθέμενου είναι να δημιουργήσει αρκετούς δρομολογητές για να αποτρέψει νέες διαδρομές να δημιουργηθούν ή να συντρίψουν το πρωτόκολλο.

Η εφαρμογή και κατακλύζει τις νόμιμες διαδρομές από τη δρομολόγηση των πινάκων.

Οι δυναμικοί αλγόριθμοι δρομολόγησης προσπαθούν να ανακαλύψουν τις πληροφορίες δρομολόγησης ακόμη και προτού να απαιτηθούν ενώ οι αντιδραστικοί αλγόριθμοι δρομολόγησης δημιουργούν μόνο όταν απαιτούνται. Αυτό καθιστά τους δυναμικούς αλγόριθμους πιο τρωτούς στις επιθέσεις υπερχείλισης δρομολόγησης.

**7. Αδυναμία εντοπισμού και απομόνωσης κόμβων απρεπής συμπεριφοράς.**

Όπως προαναφέραμε οι κόμβοι απρεπής συμπεριφοράς μπορούν να επιδράσουν σημαντικά στη ρυθμαπόδοση του δικτύου. Τα υπάρχοντα πρωτόκολλα για τα ad hoc δίκτυα δεν περιλαμβάνουν οποιοδήποτε μηχανισμό για να προσδιορίσουν τους κόμβους απρεπής συμπεριφοράς, είναι απαραίτητο στοιχείο να βρεθούν αυτοί οι κόμβοι όσο το δυνατόν γρηγορότερα γίνεται. Ένας κόμβος θεωρείται απρεπής συμπεριφοράς όταν παρουσιάζει προβλήματα με χαμηλή μπαταρία ή με υπερφόρτωση. Ένα πρωτόκολλο δρομολόγησης τα πρέπει να απομονώνει αμέσως τους προβληματικούς κόμβους έτσι ώστε να μην επηρεαστεί άμεσα η λειτουργία του δικτύου με πιθανόν καταστροφικά αποτελέσματα για αυτό.

**8. Εύκολη διαρροή πληροφοριών για την τοπολογία δικτύων**

Τα πρωτόκολλα δρομολόγησης ad hoc όπως το AODV και DSR χρησιμοποιούν πακέτα ανακαλύψεως διαδρομής σε καθαρό κείμενο. Αυτά τα πακέτα περιέχουν τις διαδρομές που ακολουθούνται από ένα πακέτο, με την ανάλυση των πακέτων αυτών οποιοσδήποτε εισβολέας μπορεί να ανακαλύψει την δομή του δικτύου. Αυτός που κάνει την επίθεση χρησιμοποιεί πληροφορίες σχετικά με τους κόμβους που είναι γύρω από τον κόμβο που θέλουν να χτυπήσουν ή κάποιο ενδιάμεσο κόμβο, μια τέτοια επίθεση μπορεί να γίνει παθητικά. Μπορεί να ανακαλύψει πόλους των κόμβων στο δίκτυο και τη θέση την οποία έχουν, με βάση όλες αυτές τις πληροφορίες ένας εισβολέας μπορεί να επιτεθεί στο συγκεκριμένο δίκτυο.

## 9. Έλλειψη σταθεροποίησης σε γρήγορο χρόνο

Τα πακέτα δρομολόγησης πρέπει να είναι σε θέση να επανακτηθούν αμέσως μετά την επίθεση. Ένας εισβολέας δεν θα πρέπει να είναι σε θέση να θέσει εκτός λειτουργίας ένα ολόκληρο δίκτυο πειράζοντας μόνο κάποιους κόμβους. Το AODV για παράδειγμα είναι επιρρεπή σε προβλήματα σταθεροποίησης δεδομένο ότι οι αριθμοί ακολουθίας χρησιμοποιούνται για να ελέγξουν χρόνους ισχύος διαδρομών και μια ανακριβής πληροφορίας μπορεί να μείνει αποθηκευμένη στο πίνακα δρομολόγησης για πάρα πολύ καιρό.

# ΚΕΦΑΛΑΙΟ 5ο

# ΕΦΑΡΜΟΓΕΣ – ΔΟΚΙΜΗ AD HOC ΔΙΚΤΥΟΥ

## ΔΟΚΙΜΗ ΔΙΚΤΥΟΥ ΔΟΥΒΛΙΝΟΥ

Σε αυτή την ενότητα θα εξετάσουμε την περίπτωση του κολλεγίου στο Δουβλίνου, το οποίο έστησε ένα ad hoc δίκτυο έτσι ώστε να τεστάρει τις δυνατότητες και τις αδυναμίες του δικτύου μέσα από αυτή την δοκιμή.

Το Τμήμα διαχείρισης της επιστήμης της πληροφορικής - Department of Computer Science στην περιοχή του Δουβλίνου στο κολλέγιο Trinity, σε συνεργασία με το Media Lab Europe (MLE), παρουσίασαν το WAND - Wireless Ad hoc Network for Dublin, σαν μια μεγάλης κλίμακας δοκιμή για τα πρωτόκολλα ad hoc δικτύου και τις εφαρμογές του. Το δίκτυο το οποίο θα εξεταστεί θα καλύψει το κέντρο του Δουβλίνου κατά μήκος μιας διαδρομής 2 km από το κολλέγιο στο MLE.

Αυτή η περιοχή θα είναι γεμάτη από υπολογιστές κατάλληλα εξοπλισμένους για σύρματη δικτύωση. Αυτοί οι υπολογιστές θα βρίσκονται παντού, σε διαμερίσματα, σε καταστήματα, στα φανάρια σηματοδοσίας έτσι ώστε να υπάρχει ένα κατώτατο επίπεδο συνδετικότητας.

Η δοκιμή μπορεί να επεκταθεί περισσότερο μέσω της εισαγωγής κινητών κόμβων όπως laptops, PDAs και άλλων κινητών συσκευών με ασύρματη συνδετικότητα.

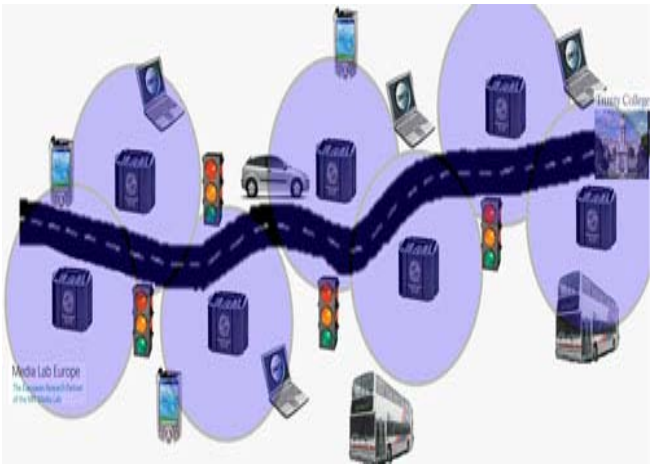
Αυτή η δυνατότητα που διαμορφώνεται με τους διάφορους τρόπους επιτρέπει στους ερευνητές μα αναπτύξουν και να ερευνήσουν τα συγκεκριμένα πρωτόκολλα και εφαρμογές που εμπλέκονται στην περιοχή του ad hoc δικτύου με διαφορετικούς τρόπους. Ένα παράδειγμα μιας τέτοιας έρευνας είναι η εξέταση των πρωτοκόλλων δρομολόγησης για τα ad hoc δίκτυα. Η δρομολόγηση των μηνυμάτων σε ένα ad hoc δίκτυο αντιπροσωπεύει ένα δύσκολο πρόβλημα το οποίο εμφανίζεται στα πρόσφατα πρωτόκολλα δρομολόγησης.

Αυτά τα πρωτόκολλα έχουν διάφορα πλεονεκτήματα και μειονεκτήματα, σημαντικό είναι να καθοριστούν κάτω από ποιες προυποθέσεις ένα από αυτά τα πρωτόκολλα αντιπροσωπεύει μια καλή επιλογή.

Η δοκιμή στο πρόγραμμα WAND προσφέρει μια μοναδική ευκαιρία να ερευνηθεί η συμπεριφορά και η απόδοση της δρομολόγησης των πρωτοκόλλων σε πραγματικό – αληθινό περιβάλλον και να ερευνηθούν οι απαιτήσεις ενός ad hoc δικτύου.
Ένας άλλος τομέας της έρευνας που ερευνάται με τη βοήθεια της δοκιμής WAND αφορά την προσαρμογή των εφαρμογών στα ασύρματα ειδικά δίκτυα. Οι υπάρχουσες εφαρμογές έχουν ως σκοπό να εκμεταλλευθούν τις πρόσθετες πληροφορίες και τις υπηρεσίες που προσφέρονται από τα ad hoc δίκτυα.
Ένα παράδειγμα των εφαρμογών που θα εξερευνηθούν με τη βοήθεια της δοκιμής WAND είναι επικοινωνία μεταξύ των οχημάτων. Αυτή η εφαρμογή θα βοηθήσει τους κινητούς κόμβους δικτύων όπως τα αυτοκίντητα, λεωφορεία και τα φορτηγά να επικοινωνήσουν μεταξύ τους και με άλλους σταθμούς, όπως με τα φανάρια κυκλοφορία , με στάσεις λεωφορείων και με κάμερες κυκλοφορίας. Οι κινητοί συμμετέχοντες μπορούν να ενημερώσουν ο ένας τον άλλον για κάποια εμπόδια στους δρόμους, για ενέργεις που πρέπει να ληφθούν για να αποφύγουν τα εμπόδια ή ακόμα και τις διαδρομές που πρέπει να ακολουθήσουν τα οχήματα άμεσης ανάγκης, αυτό είναι πολύ σημαντικό, φανταστείτε ένα ασθενοφόρο το οποίο πρέπει να διαλέξει κάποιο γρήγορο δρόμο για να φτάσει σύντομα στον προορισμό του, μια τέτοια τεχνολογία φαίνεται ιδιαίτερα χρήσιμη και σωτήρια.

Η δοκιμή WAND προσφέρει στους ερευνητές μια μοναδική ευκαιρία να ερευνήσει του χαμηλού επιπέδου μηχανισμούς όπως η δρομολόγηση των πρωτοκόλλων και των χαμηλών υπηρεσιών επιπέδων, καθώς επίσης και τις εφαρμογές επιπέδου χρήστη σε ένα πραγματικό περιβάλλον που απεικονίζει το τυχαίο και το μη προβλέψιμο που είναι εξαιρετικά δύσκολο να αναπαραχθεί με κάποιου είδους προσομοίωση.

Η όλη δομή του δικτύου το οποίο αναλύσαμε φαίνεται στην παρακάτω εικόνα 16 φαίνονται καθαρά οι συσκευές που χρησιμοποιήθηκαν και η απόσταση που υπήρχε.




**Εικόνα 16 : Η δομή του δικτύου που εξετάσαμε**

# ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΠΟ ΤΗ ΧΡΗΣΗ AD HOC ΔΙΚΤΥΟΥ

Τα πλεονεκτήματα από τη χρήση του συγκεκριμένου δικτύου είναι :

- Το ad hoc δίκτυο υποστηρίζει την κινητικότητα. Με τη συγκεκριμένη τεχνολογία διαθέσιμη, οπουδήποτε ένας χρήστης πηγαίνει μπορεί να επικοινωνήσει με γειτονικούς κόμβους. Αυτό δίνει στο χρήστη μεγάλη ευκαίρια κινήσεων.
- Απαιτείται ελάχιστη υποστήριξη δομής..
- Από τη στιγμή που δεν απαιτείται κάποια συγκεκριμένη υποστήριξη δομής, το κόστος ανάπτυξης ενός τέτοιου δικτύου είναι πολύ χαμηλό, λογικό είναι οι χρήστες να προτιμήσουν αυτό το πρότυπο γιατί πάντα ο χρήστης αναζητά το χαμηλότερο κόστος.
- Σε καταστάσεις υψηλής επικινδυνότητας τη λύση δίνει ένα ad hoc δίκτυο, άρα η εφαρμογή του συγκεκριμένου προτύπου μπορεί να σώσει από πολύ δύσκολες καταστάσεις.

Είδαμε τα πλεονεκτήματα από την πλευρά του χρήστη, από την πλευρά του δικτύου και της τεχνολογίας τα πλεονεκτήματα είναι :

- Με την εμφάνιση μια νέας τεχνολογίας όπως γίνεται σε όλες τις περιπτώσεις, οι φορείς παροχής υπηρεσιών μπαίνουν στην αγορά και παρέχουν πολλές και ποικίλες νέες υπηρεσίες.
- Η συγκεκριμένη τεχνολογία είναι συμβατή με τις περισσότερες συσκευές που κυκλοφορούν, ακόμα και αυτές που δεν είναι συμβατές μπορούν εύκολα να προστεθούν σε ένα ad hoc δίκτυο.
- Η βελτίωση μιας υπάρχουσας υποδομής εξαρτάται από οικονομικούς λόγους κυρίως και έτσι είναι αβέβαιη. Ένα ad hoc είναι μια ενδιάμεση λύση.
- Ένα ad hoc δίκτυο χρησιμοποιεί κινητές συσκευές, όπως PDAs, άρα είναι πολύ εύκολο να λειτουργήσει σε κάποια σημεία όπου δεν μπορούν να στηθούν άλλων ειδών δίκτυα.

# Που χρησιμοποιούμε ad hoc

Εδώ θα μελετήσουμε διάφορα σενάρια στα οποία συναντάμε χρήση των ad hoc δικτύων.

## Δίκτυα κοινοτήτων

Με αυτή την έννοια μιλάμε για δίκτυα σε πανεπιστήμια, σε σχολεία τα οποία προσφέρουν κυρίως πρόσβαση στο internet, ο χρήστης μπορεί να γίνει μέρος του δικτύου πολύ απλά και εύκολα. Ο χρήστης μόλις συνδεθεί στο κτίριο θα έχει άμεση πρόσβαση σε κοινόχρηστες συσκευές, όπως εκτυπωτές, scanners, χρησιμοποιώντας τα όπως εκείνος θέλει. Ακόμα μπορεί να παίξει και διάφορα δικτυακά παιχνίδια, γεγονός το οποίο το συναντάμε πολύ συχνά στις ημέρες μας και σε Internet café. Η συγκεκριμένη επιλογή συναντάται πολύ όταν τα πανεπιστήμια και γενικά αυτές οι δικτυακές κοινότητες προσφέρουν υψηλές ταχύτητες στο Internet οπότε οι χρήστες έχουν δικαίωμα να απολαμβάνουν μια ιδιαίτερα ακριβή υπηρεσία.

## Δίκτυο σε σπίτι

Μπορούμε να βρισκόμαστε σε οποιοδήποτε σημείο στο σπίτι και να επικοινωνούμε με το δίκτυο, είναι ιδιαίτερα βολικό γιατί μας δίνει ευκολία κινήσεων και δεν μας

περιορίζει στη χρήση του. Ακόμα μπορούμε με τον προσωπικό μας υπολογιστή να μεταφέρουμε τη δουλειά μας από το γραφείο και να μεταφέρουμε τα δεδομένα στο δίκτυο έτσι ώστε να μπορούμε να δουλέψουμε με την ηρεμία μας στο σπίτι μας.

### Εταιρικά Δίκτυα

Τη συγκεκριμένη επιλογή τη συναντάμε όταν έχουμε κάποια συνεδρίαση σε κάποια εταιρεία, πολύ απλά και εύκολα μπορούν οι χρήστες να συνδεθούν στο ίδιο δίκτυο και να κρατούν τις σημειώσεις τους ή οτιδήποτε άλλο θέλουν, ακόμα ένα ιδιαίτερα σημαντικό στοιχείο είναι η παρουσίαση, συχνά σε μια συνεδρίαση κάποιος κάνει κάποια παρουσίαση, οι υπόλοιποι χρήστες μέσω του δικτύου μπορούν να παρακολουθούν τη παρουσίαση. Όλα αυτά γίνονται από υπολογιστές που ανήκουν σε διαφορετικά κτίρια πριν βρεθούν στον ίδιο χώρο.

### Σε καταστάσεις άμεσης ανάγκης

Τα ad hoc δίκτυα μπορούν να χρησιμοποιηθούν σε καταστάσεις αναζήτησης και διάσωσης, σε καταστάσεις που πρέπει να βρεθεί άμεσα λύση.
Σαν παράδειγμα της λειτουργίας αναζήτησης και διάσωσης μπορούμε να αναφέρουμε τους πυροσβέστες που πηγαίνουν σε κάποιο κτίριο το οποίο έχει φωτιά, έχοντας ένα ραδιόφωνο επικοινωνίας που διαμορφώνει ένα ad hoc δίκτυο στην περιοχή. Έτσι διαμορφώνονται οι δρομολογητές  για να μπορούν να παράσχουν τη συνδετικότητα καθώς οι πυροσβέστες εισέρχονται στο κτίριο, άρα το προσωπικό που θα καταφτάσει αργότερα θα μπορεί να συνδεθεί με το ad hoc δίκτυο και να έχει επικοινωνία με τους άλλους πυροσβέστες.
Ακόμα πολλές φορές έχει παρατηρηθεί μετά από φυσικό φαινόμενο να μην λειτουργούν τα δίκτυα, ειδικά όταν κάτι είναι επείγον και πρέπει να δουλέψει μπορεί να στηθεί ένα ad hoc δίκτυο το οποίο δεν απαιτεί κάποια συγκεκριμένη δομή.

## ΠΡΙΝ ΚΑΝΟΥΜΕ ΤΗΝ ΕΠΙΛΟΓΗ...

Για τη χρήση ενός ad hoc δίκτυο πρέπει να λάβουμε υπόψη μας κάποια στοιχεία όπως:

- **Μείωση κόστους:** Χωρίς την ανάγκη να αγοραστούν ή να εγκατασταθούν Access points - σημεία πρόσβασης, θα μειωθεί κατά πολύ το κόστος που θα πρέπει να δαπανήσουμε.
- **Γρήγορος χρόνος οργάνωσης:** το δίκτυο ad hoc απαιτεί μόνο την εγκατάσταση της εγκατάσταση της κάρτας NIC στις συσκευές των χρηστών. Κατά συνέπεια ο χρόνος για να εγκαταστήσεις ένα ασύρματο δίκτυο LAN είναι πολύ λιγότερος από το να εγκαταστήσεις ένα ασύρματο τοπικό LAN υποδομής.
- **Πιθανή καλύτερη απόδοση:** το θέμα της απόδοσης στα ad hoc δίκτυα είναι σίγουρα αμφισβητήσιμη. Παραδείγματος χάριν, η απόδοση μπορεί να είναι υψηλότερη στο ad hoc δίκτυο επειδή δεν υπάρχει η ανάγκη να ταξιδέψουν τα πακέτα μέσω ενός σημείου πρόσβασης – Access Point, αυτό όμως προυποθέτει ένα μικρό αριθμό χρηστών. Εάν όμως στο δίκτυο υπάρχουν πολλοί χρήστες θα πετύχουμε καλύτερη απόδοση αν χρησιμοποιήσουμε πολλαπλά σημεία πρόσβασης στους ξεχωριστούς χρήστες. Οπότε θα αποφύγουμε κάποιες συγκρούσεις πακέτων και θα μειώσουμε την ισχύ που θα καταναλώσουμε.
- **Περιορισμένη πρόσβαση στο δίκτυο.** Επειδή δεν υπάρχει κάποιο σύστημα διανομής σε ένα ad hoc δίκτυο οι χρήστες δεν έχουν αποτελεσματική πρόσβαση στο Διαδίκτυο και σε άλλες συνδεδεμένες συσκευές στο δίκτυο.Φυσικά θα μπορούμε να εγκαταστήσουμε στον υπολογιστή μια κάρτα NIC και να διαμορφώσουμε το PC να έχει μια κοινόχρηστη σύνδεση στο Διαδίκτυο. Αυτό όμως δεν θα ικανοποιούσε μια μεγαλύτερη ομάδα χρηστών τόσο πολύ. Κατά συνέπεια, το ad hoc δίκτυο δεν είναι και τόσο καλή ιδέα για μια εταρεία η οποία θέλει να έχει πολλές εφαρμογές και να χρησιμοποιεί κάποιον κεντρικό υπολογιστή – server.
- **Δύσκολη διαχείριση δικτύου:** Η διαχείριση δικτύων είναι ένας πονοκέφαλος για τα ad hoc δίκτυα λόγω της ρευστότητας της τοπολογίας και της έλλειψης μια κεντρικής συσκευής. Χωρίς κάποιο Access Point οι διαχειριστές δικτύων δεν μπορούν εύκολα να ελέγξουν την απόδοση του δικτύου ή την ασφάλεια..Μια αποτελεσματικά διαχείριση δικτύου ad hoc απαιτεί διαχείριση

δικτύου σε επίπεδο χρήστη – συσκευής, άρα είναι κάτι το οποίο πρέπει να προσέγξει κάθε συσκευή που συνδέεται στο δίκτυο, αυτό γίνεται με τη συνεχή αποστολή πακέτων στο δίκτυο.

# ΣΥΜΠΕΡΑΣΜΑ

Τα ad hoc δίκτυα είναι ένας βασικός παράγοντας στην εξέλιξη των ασύρματων επικοινωνιών, πολύ χαρακτηρίζουν τη συγκεκριμένη τεχνολογία ως επανάσταση στα ασύρματα δίκτυα. Ένα ad hoc δίκτυο μπορεί να χρησιμεύσει παντού λόγω του ότι αποτελείται από κινητές συσκευές που μπορούν να στηθούν παντού, τέτοιες συσκευές είναι τα laptops , τα pdas. Τα ασύρματα δίκτυα μπορούν να αναπτυχθούν γρήγορα και εύκολα , ακόμα και σε μέρη όπου είναι δύσκολο ή και αδύνατο να δημιουργηθούν ενσύρματα δίκτυα είτε λόγω της τοποθεσίας είτε διότι το κόστος για την υλοποίηση τους είναι πολύ μεγάλο είναι τις περισσότερες φορές εφικτή και ιδιαίτερα αποδοτική η λύση ενός ασύρματου δικτύου.

Μια επιχείρηση χαρακτηρίζεται από το πόσο εύκολα μπορεί να δημιουργήσει γρήγορα μικρές ομάδες εργασίας και από το πόσο εύκολα μπορεί να αναδιατάξει αυτές τις ομάδες για να ασχοληθούν με καινούργια ζητήματα. Επομένως μια σύγχρονη εταιρεία πρέπει να χρησιμοποιήσει τα ασύρματα δίκτυα ώστε να πετύχει αυτούς τους στόχους. Τα δίκτυα αυτά επιτρέπουν τη δημιουργία ομάδων εργαζομένων σε οποιαδήποτε τοποθεσία και τους δίνει τη δυνατότητα να επικοινωνούν μεταξύ τους με φορητούς υπολογιστές χωρίς απαραίτητα να βρίσκονται στον ίδιο χώρο.

Ένα σημαντικό πλεονέκτημα των ασυρμάτων δικτύων είναι ότι επιτρέπουν τη σύνδεση νέων συσκευών σε οποιοδήποτε χώρο και χρόνο χωρίς την δαπανηρή καθυστέρηση της εγκατάστασης νέων καλωδίων, η οποία πολλές φορές είναι και τεχνικά ιδιαίτερα δύσκολη.

Αυτά τα δίκτυα κληρονομούν τα παραδοσιακά προβλήματα της ασύρματης τεχνολογίας όπως η βελτιστοποίηση του εύρους ζώνης, η δύναμη του ελέγχου και η ποιοτική αύξηση της μετάδοσης. Ακόμα τα ad hoc όπως προαναφέραμε στερούνται κάποιας σταθερής δομής ,αυτό μπορεί να προκαλέσει επιπρόσθετα προβλήματα όπως δυσκολία εντοπισμού κάποιας συσκευής.

Τα μελλοντικά ad hoc δίκτυα θα χρησιμοποιούν κινητούς δρομολογητές για να παρέχουν δυνατότητα Internet στους κινητούς χρήστες ad hoc δικτύου. Υπάρχει ανάγκη για τη δυναμική τοπολογία ενός ad hoc δικτύου,γι'αυτό πρόσφατα οργανώσεις εξετάζου τη δυνατότητα για δυναμικά δίκτυα. . Τα κινητά ad hoc δίκτυα είναι αυξανόμενου ενδιαφέροντος για ένα διανεμημένο σύνολο εφαρμογών, όπως τα πιθανά συστήματα τέταρτης γενεάς.

Παρά όμως τα θετικά στοιχεία τα ασύρματα τοπικά δίκτυα παρουσιάζουν και σημαντικά μειονεκτήματα σε σχέση με τα ενσύρματα δίκτυα, οι ασύρματες τεχνολογίες είναι αργές σε σχέση με τις αντίστοιχες ενσύρματες ( επηρεάζονται από παράγοντες όπως καιρός, καθαρό σήμα που μπορούν να επιβραδύνον σημαντικά την απόδοση) . Ένα σημαντικό πρόβλημα ήταν η έλλειψη ενιαίων προτύπων γεγονός που είχε ως συνέπεια οι παλαιότερες ασύρματες τεχνολογίες να είναι ακριβές , μη συνεργαζόμενες μεταξύ τους και πολύ συχνά μη αξιόπιστες. Λύση στο συγκεκριμένο πρόβλημα ήρθε να δώσει λύση το πρότυπο 802.11 της IEEE το οποίο φιλοδοξεί να αποτελέσει μια ολοκληρωμένη λύση στα ασύρματα δίκτυα.

# URLS

Οι πηγές της πτυχιακής εργασίας είναι :


http://www.homenethelp.com/

http://www.homenethelp.com/web/diagram/access-point.asp

http://www.homenethelp.com/web/diagram/ad-hoc.asp

http://clarinet.u-strasbg.fr/rge/reunions/rge14101999/manet/sld001.htm

http://www.computingunplugged.com/issues/issue200407/00001326001.html

http://dmz02.kom.e-technik.tu-darmstadt.de/Research/Dependable/

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

http://www.ercim.org/publication/Ercim_News/enw57/santi.html

http://www.wi-fitechnology.com/Wi-Fi_Reports_and_Papers/Mobile_Ad-hoc_Networks.html

http://adhoc-symposium.site.uottawa.ca/site_07/aboutus.html

http://www.cylab.cmu.edu/default.aspx?id=54

http://www.scs.carleton.ca/~adhocnow/

http://www.usabilitynews.com/news/article2222.asp

http://sar.informatik.hu-berlin.de/teaching/2004-w%20Ad-Hoc%20Networks/

http://www.mobitopia.com/1000006.html