ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ
ΠΑΡΑΡΤΗΜΑ ΝΑΥΠΑΚΤΟΥ
ΤΜΗΜΑ ΤΕ.ΣΥ.Δ

ΤΙΤΛΟΣ: WLAN 802.11 a & b συγκρίσεις RF transceiver

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σακονίδου Σουζάνα Α.Μ 0323

Υπεύθυνος καθηγητής: κ. Λούβρος Σπύρος

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Με τι θα ασχοληθούμε;

Σε αυτή την εργασία θα μάθουμε τα πάντα σχετικά με το πρότυπο 802.11. Θα μελετήσουμε αρχικά προγενέστερα πρότυπα για να μπορέσουμε να κατανοήσουμε τις ανάγκες για τις οποίες δημιούργησαν το IEEE 802.11. Τέλος θα καταλήξουμε σε μεταγενέστερα πρότυπα τα οποία στηρίχτηκαν πάνω στα πρότυπα που θα επικεντρωθούμε ώστε να έχουμε μία ιδέα για το ποια κατεύθυνση ακολουθεί αυτή η τεχνολογία.

Πιο συγκεκριμένα, στόχος της πτυχιακής είναι η σε βάθος κατανόηση των χαρακτηριστικών που παρουσιάζουν οι πομποδέκτες (rf transceiver) για εφαρμογές WLAN 802.11a & b καθώς και η μεταξύ τους σύγκριση.

Τι περιέχει η εργασία;

Η εργασία χωρίζετε σε δύο τμήματα: 1. Στο θεωρητικό κομμάτι (θα μελετήσουμε το πρότυπο 802.11 πιο συγκεκριμένα στα 802.11a 802.11b με βάση προηγούμενες εργασίες, μελέτες και αναφορές).

2. Στο πρακτικό κομμάτι (θα χρησιμοποιήσουμε το μαθηματικό πρόγραμμα Matlab και με την βοήθεια των κατάλληλων βιβλιοθηκών θα φτιάξουμε ένα δίκτυο βασισμένο στο πρότυπο που θα μελετήσουμε θα κάνουμε διάφορες μετρήσεις και θα τις καταγράψουμε. Ανάλογα τα αποτελέσματα που θα έχουμε θα γράψουμε το συμπέρασμα μας).

Αντικείμενο

Στα πλαίσια της εργασίας αυτής θα ολοκληρωθούν τα εξής βήματα:

- Ανάλυση του φυσικού επιπέδου των ασύρματων δικτύων WLAN 802.11 a & b
- Σύντομη ανάλυση των χαρακτηριστικών τους
- Παρουσίαση των τεχνικών προδιαγραφών ενός ασύρματου πομποδέκτη WLAN 802.11
- Ανάλυση, υλοποιήσηση και σύγκριση Αλγορίθμων

ΚΕΦΑΛΑΙΟ 1^{ο}

Με λίγα λόγια…

Η ανάπτυξη προτύπων για τα ασύρματα τοπικά δίκτυα σε συνδυασμό με το χαμηλό κόστος της ασύρματης τεχνολογίας επέτρεψε την ραγδαία εξάπλωση των ασυρμάτων δικτύων σε κοινόχρηστους και σε ιδιωτικούς χώρους όπως πανεπιστήμια, πλατείες, αεροδρόμια, γραφεία επιχειρήσεων, οικίες, κλπ. Η παρούσα εργασία μελετά το πρωτόκολλο IEEE 802.11 το οποίο κυριαρχεί στα ασύρματα τοπικά δίκτυα. Ειδικότερα ερευνά την απόδοση της κατανεμημένης διαδικασίας πρόσβασης DCF του επιπέδου MAC του IEEE 802.11.
Σκοπός της παρούσας ερευνητικής προσπάθειας είναι η συμβολή στην έρευνα για την ανάπτυξη ενός απλού και αποτελεσματικού επιπέδου πρόσβασης μέσου MAC στα ασύρματα δίκτυα που βασίζονται στο πρωτόκολλο IEEE 802.11. Αναπτύσσονται μαθηματικά μοντέλα για τον υπολογισμό των παρακάτω:

α) την μέση καθυστέρηση των πακέτων ανά βαθμίδα οπισθοχώρησης και την πιθανότητα ανά βαθμίδα οπισθοχώρησης,

β) την μέση καθυστέρηση των πακέτων,

γ) την κατανομή των καθυστερήσεων των πακέτων,

δ) την αθροιστική κατανομή των καθυστερήσεων,

ε) την διακύμανση των καθυστερήσεων των πακέτων και στ) την χωρητικότητα του καναλιού (μέσου) σε φωνητικές συνομιλίες. Επίσης αναπτύσσεται ένας αλγόριθμος ελέγχου εισόδου (admission control).

Τα προτεινόμενα μαθηματικά μοντέλα:

α) υπολογίζουν τις παραπάνω μετρικές με σχετικά απλές μαθηματικές σχέσεις,

β) είναι ακριβή (η ακρίβεια προσδιορίζεται μετά από σύγκριση με αποτελέσματα προσομοιώσεων) και

γ) παράγουν αποτελέσματα σε σύντομο χρονικό διάστημα.

Αναπτύσσονται διάφορα σενάρια λειτουργίας των ασυρμάτων τοπικών δικτύων και μελετάται η επίδραση των τιμών των παραμέτρων της DCF στην απόδοση με απώτερο σκοπό τον καθορισμό βέλτιστων τιμών και συνθηκών για την βέλτιστη απόδοση του πρωτοκόλλου IEEE 802.11.

Η ανάλυση των μετρικών και τα αποτελέσματα εφαρμογής τους στα ασύρματα δίκτυα συμβάλουν στην επιστημονική γνώση, καθώς συμβάλουν στην δημιουργία καλυτέρων μεθόδων πρόσβασης στο ασύρματο μέσο. Η πιο σημαντική συμβολή αυτής της διατριβής είναι το γεγονός ότι για πρώτη φορά πραγματοποιήθηκε πλήρης, συστηματική και εκτεταμένη έρευνα για τις καθυστερήσεις των πακέτων ως κριτήριο απόδοσης των ασυρμάτων δικτύων.

1.1 Τι είναι το πρότυπο IEEE 802.11;

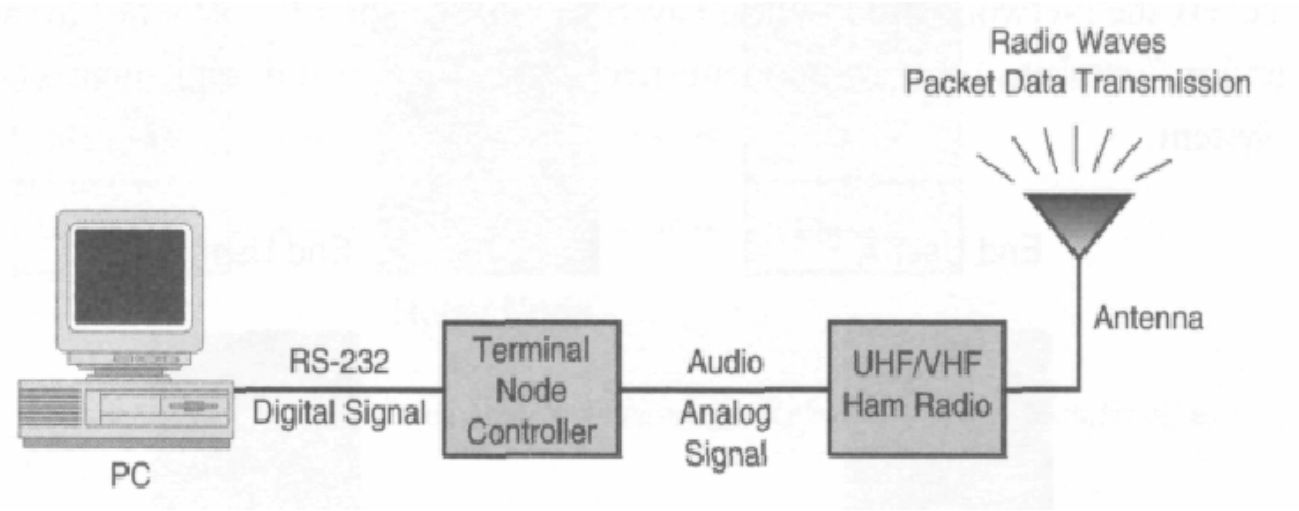
Το **IEEE 802.11** είναι μια οικογένεια προτύπων της IEEE για ασύρματα τοπικά δίκτυα (WLAN) που είχαν ως σκοπό να επεκτείνουν το 802.3 (Ethernet, το συνηθέστερο πρωτόκολλο ενσύρματης δικτύωσης υπολογιστών) στην ασύρματη περιοχή. Τα πρότυπα 802.11 είναι ευρύτερα γνωστά ως «WiFi» επειδή η WiFi Alliance, ένας οργανισμός ανεξάρτητος της IEEE, παρέχει την πιστοποίηση για τα προϊόντα που υπακούν στις προδιαγραφές του 802.11. Αυτή η οικογένεια πρωτοκόλλων αποτελεί το καθιερωμένο πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων.

Περιγράφονται τα δύο πρώτα επίπεδα του OSI, δηλαδή το φυσικό επίπεδο (PHY, Physical Layer) και το επίπεδο σύνδεσης δεδομένων (MAC, Medium Access Control). Τα πρωτόκολλα αυτά δημοσιεύονται από την IEEE γεγονός που είναι σημαντικό για την διαλειτουργικότητα των συσκευών που το ακολουθούν.

Περιγράφοντας μόνο τα δύο κατώτερα επίπεδα, επιτρέπει σε οποιαδήποτε εφαρμογή να εργάζεται πάνω σε συσκευή 802.11 όπως ακριβώς θα εργαζόταν πάνω από Ethernet. Δηλαδή τα πιο πάνω επίπεδα δεν γνωρίζουν και δεν απασχολούνται από το τι βρίσκεται πιο κάτω.

1.2 Ιστορικά στοιχεία

Οι τεχνολογία δικτύων και οι ασύρματες επικοινωνίες συνδυάσθηκαν για πρώτη φορά το 1971 στο πανεπιστήμιο της Χαβάης χάρης σε ένα ερευνητικό πρόγραμμα που ονομάζονταν ALOHANET. Το σύστημα ALOHANET επέτρεπε την επικοινωνία μεταξύ των υπολογιστών που βρίσκονταν σε επτά πανεπιστημιουπόλεις χτισμένες πάνω σε τέσσερα νησιά. Οι υπολογιστές επικοινωνούσαν με τον κεντρικό υπολογιστή χωρίς τη χρήση των υπαρχουσών αναξιόπιστων και ακριβών τηλεφωνικών γραμμών. Το ALOHANET πρόσφερε τις αμφίδρομες επικοινωνίες, σε μια τοπολογία αστεριών, μεταξύ του κεντρικού υπολογιστή και κάθε ενός από τους χρήστες. Στη δεκαετία του '80, ραδιοερασιτέχνες με την ονομασία «hams », διατήρησαν την ασύρματη δικτύωση ενεργή μέσα στις Ηνωμένες Πολιτείες και τον Καναδά. Σχεδίασαν και υλοποίησαν τα terminal node controllers (TNCs) για να διασυνδέσουν τους υπολογιστές τους μέσω του ράδιο εξοπλισμού τους. Τα TNC λειτουργούν σαν ένα modem, που μετατρέπουν το ψηφιακό σήμα του υπολογιστή σε ένα που το ραδιοερασιτεχνικό δίκτυο « ham » μπορεί να διαμορφώσει και να στείλει μέσω του μέσου μετάδοσης κυμάτων χρησιμοποιώντας μιας τεχνική μεταγωγής πακέτων.Στην πραγματικότητα, η American Radio Relay League (ARRL) και η Canadian Radio Relay League (CRRL) έχουν υποστηρίξει τη διάσκεψη δικτύωσης υπολογιστών από την αρχή της δεκαετίας του '80 για να παρέχουν ένα φόρουμ για την ανάπτυξης ασύρματου δικτύων. Κατά συνέπεια, οι ραδιοερασιτέχνες « hams » έχουν χρησιμοποιήσει την ασύρματη δικτύωση για χρόνια, πολύ νωρίτερα από την εμπορική αγορά.



Σχήμα. Ένας ελεγκτής τερματικός κόμβος μπορεί να κάνει ένα PC να επικοινωνήσει μέσω μια ραδιοφωνικές μπάντας και να δημιουργήσει ένα δικτύου ασύρματης μετάδοσης πληροφοριών .

Το 1985, η Federal Communications Commission (FCC) κατέστησε δυνατή την εμπορική ανάπτυξη ασύρματων τμημάτων ενός τοπικού LAN με την έγκριση της δημόσιας χρήσης των βιομηχανικών, επιστημονικών, και ιατρικών (ISM) ζωνών. Αυτή η ζώνη συχνοτήτων ανήκει ανάμεσα στους 902MHz και στους 5,85 GHz, ακριβώς επάνω από τις κυψελοειδείς τηλεφωνικές συχνότητες. Η ζώνη ISM αποδείχθηκε πολύ ελκυστική για τους προμηθευτές προϊόντων ασύρματης δικτύωσης διότι παραχωρείται μέρος του
φάσματος στο οποίο θα λειτουργήσουν τα προϊόντα τους, όπου οι τελικοί χρήστες δεν ειναι απαραίτητο να λάβουν ειδικές άδειες για να χρησιμοποιήσουν τα προϊόντα. Η κατανομή των ζωνών

ISM είχε μια δραματική επίδραση στην ασύρματη βιομηχανία. Συντέλεσε στην έντονη ανάπτυξη των ασύρματων δικτύων. Παρόλα αυτά, δίχως πρότυπα, οι προμηθευτές άρχισαν να υλοποιούν συσκευές ασύρματης δικτύωσης.

Προς το τέλος της δεκαετίας του '80, το Institute for Electrical and Electronic Engineers (IEEE), αρμόδιο για την ανάπτυξη των προτύπων του τοπικού LAN, όπως το ethernet και το token ring, άρχισε την ανάπτυξη των προτύπων για τα ασύρματα δίκτυα. Υπό την προεδρία του Vic Hayes, ένος μηχανικού από τη NCR, η ομάδα εργασίας του IEEE για το 802.11 ανέπτυξετις προδιαγραφές Ελέγχου Προσπέλασης Μέσου και Φυσικού Επιπέδου για τα ασύρματα δίκτυα.

Η πρώτη έκδοση του WiFi εισήχθη το 1997 και στο φυσικό επίπεδο περιελάμβανε δύο μεθόδους διασποράς φάσματος για τη μετάδοση στη ζώνη συχνοτήτων 2.4GHz, η εκπομπή στην οποία δεν απαιτεί άδεια. Η πρώτη μέθοδος λειτουργούσε με Frequency Hopping (FHSS) και υποστήριζε ρυθμό μετάδοσης 1 Mbps, ενώ η δεύτερη λειτουργούσε με Direct Sequence(DSSS) και υποστήριζε ρυθμό μετάδοσης 1-2 Mbps. Περιλαμβανόταν επίσης και μία υπέρυθρη εκδοχή (IR). Πριν από την εμφάνιση του 802.11 δεν υπήρχε κάποιο ευρέως αποδεκτό πρότυπο για ασύρματα τοπικά δίκτυα υπολογιστών, ούτε ανάλογες εμπορικές εφαρμογές, καθώς η τεχνολογία ασύρματης δικτύωσης δεν ήταν ακόμα αρκετά ώριμη.

Το 1999 το 802.11b ώθησε την ταχύτητα στα 11 Mbps χρησιμοποιώντας DSSS. Οι ρυθμοί λειτουργίας 1-2 Mbps με DSSS ισχύουν ακόμα, έτσι ώστε οι συσκευές να μπορούν να πέσουν σε χαμηλότερες ταχύτητες για να διατηρήσουν μια σύνδεση όταν τα σήματα είναι αδύνατα. Με την έκδοση αυτή ο όρος WiFi άρχισε να χρησιμοποιείται ευρέως και οι ασύρματες κάρτες δικτύου 802.11 να εξαπλώνονται ταχέως.

Χρησιμοποιώντας τη μέθοδο μετάδοσης Orthogonal Frequency Division Multiplexing (OFDM), δύο πρότυπα υψηλής ταχύτητας ακολούθησαν το 802.11b τα οποία παρέχουν μέχρι 54 Mbps: το 802.11a εκπέμπει στη ζώνη συχνοτήτων των 5GHz αλλά δεν είναι συμβατό με τις ασύρματες κάρτες δικτύου οι οποίες υποστηρίζουν 802.11b, ενώ το 802.11g εκπέμπει στη ζώνη συχνοτήτων των 2.4GHz και είναι συμβατό με το 802.11b. Η επικοινωνία μεταξύ συσκευών εξοπλισμένων με κάρτες 802.11b και 802.11g γίνεται στην υψηλότερη δυνατή κοινή ταχύτητα, αυτήν του 802.11b.

Με τη διάδοση του WiFi κατά τις αρχές της δεκαετίας του 2000 εμφανίστηκε μία νέα μέθοδος πρόσβασης στο Internet: μία ψηφιακή συσκευή με κάρτα ασύρματης δικτύωσης WiFi, π.χ. ένας ηλεκτρονικός υπολογιστής ή ένα PDA, μπορεί να συνδεθεί στο Διαδίκτυο όταν βρίσκεται σε ακτίνα κάλυψης ασύρματου δικτύου ήδη συνδεδεμένου στο Internet, το οποίο ονομάζεται σημείο πρόσβασης (Access Point). Μία περιοχή που καλύπτεται από ένα ή περισσότερα σημεία πρόσβασης συνδεδεμένα μεταξύ τους λέγεται *hotspot*. Ένα hotspot μπορεί να καλύπτει έναν χώρο έκτασης δωματίου ή και πολλών τετραγωνικών μέτρων, με εναλλασσόμενα σημεία πρόσβασης.

Έτσι η τεχνολογία WiFi επιτρέπει τη σύνδεση μεταξύ δύο συσκευών μεταξύ τους, τη σύνδεση ενός προσωπικού υπολογιστή με ένα τοπικό δίκτυο και άλλους υπολογιστές και, στη συνέχεια, μέσω αυτών στο Internet. Ένας φορητός υπολογιστής μπορεί να συνδεθεί οπουδήποτε υπάρχει σημείο πρόσβασης (π.χ. σε πάρκα ή πλατείες μεγάλων πόλεων, καφετέριες, βιβλιοθήκες κλπ).

1.3 Τι πρότυπα ανήκουν στην οικογένεια του IEEE 802.11;

- **IEEE 802.11**

  Δημοσιεύθηκε το 1997 από την IEEE , μετά από επτά χρόνια μελέτης
  Προβλέπει ρυθμούς μετάδοσης 1 και 2 Mbps
  Υποστηρίζει ασύγχρονη, connectionless υπηρεσία
  Στο φυσικό επίπεδο προβλέπει τεχνική FHSS ή DSSS σε ζώνες συχνοτήτων 915MHz , 2.4MHz , 5.2MHz ή υπέρυθρη μετάδοση στα 850nm ως 900nm
  Υποστηρίζει δυνατότητες όπως προτεραιότητα της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής

- **IEEE 802.11a**
  Το πρότυπο αυτό υποστηρίζει μεγαλύτερους ρυθμούς μετάδοσης με διαμόρφωση OFDM από 6 ως 54 Mbps , στην ζώνη των 5.7GHz. Η χρήση της OFDM , Orthogonal Frequency Division Multiplexing έχει σαν αποτέλεσμα την πιο αποτελεσματική χρήση του διαθέσιμου φάσματος.
- **IEEE 802.11b**
  Το πιο δημοφιλές από όλα τα πρότυπα, δημοσιεύθηκε το Σεπτέμβριο του 1999
  Στην ουσία είναι το 802.11 με προσθήκη δύο μεγαλύτερων ρυθμών μετάδοσης, του 5.5Mbps και του 11Mbps και αναγκαστικά της τεχνικής φυσικού επιπέδου DSSS.
  Το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα.
  Είναι ένα στιβαρό, αποτελεσματικό και δοκιμασμένο πρότυπο.
  Οι προσθήκες της 802.11b σε σχέση με την 802.11 αφορούν μόνο το φυσικό επίπεδο, ορίζοντας μεγαλύτερους ρυθμούς μετάδοσης και πιο στιβαρή συνδεσιμότητα.
- **IEEE 802.11c**
  Λειτουργία γεφύρωσης (bridging) πλαισίων 802.11
- **IEEE 802.11d**
  Επεκτάσεις στο πρότυπο ώστε να λειτουργεί σε επιπλέον ρυθμιστικά πλαίσια άλλες ζώνες συχνοτήτων)
- **IEEE 802.11e**
  Προσπαθεί να διασφαλίσει ποιότητα υπηρεσιών για εφαρμογές πραγματικού χρόνου που εκτελούνται πάνω σε ένα WLAN ελαχιστοποιώντας ή μεγιστοποιώντας ένα από τα παρακάτω κριτήρια: μέση καθυστέρηση από άκρο σε άκρο, μέση μεταβολή της καθυστέρηση ή μέσο ποσοστό επιτυχούς παράδοσης πλαισίων. Αυτό το επιτυγχάνει βελτιώνοντας τους μηχανισμούς DCF και PCF με τους μηχανισμούς EDCF, ο οποίος αναθέτει προτεραιότητες στα πλαίσια δεδομένων ανάλογα με το πόσο χρονικά κρίσιμη είναι η παράδοση τους και με τα μεγαλύτερης προτεραιότητας πλαίσια να έχουν περισσότερες πιθανότητες να κερδίσουν στον ανταγωνισμό για την πρόσβαση στο κοινό μέσο, και HCF, ο οποίος περιορίζει το μέγιστο χρόνο δέσμευσης του καναλιού από ένα τερματικό, αντίστοιχα. Υποστήριξη QoS στο MAC επίπεδο (EDCF, Enhanced DCF και HCF, Hybrid Coordination Function)
- **IEEE 802.11f**
  Επιτρέπει άμεση επικοινωνία μεταξύ διαφορετικών AP ώστε να εξαλειφθεί η απώλεια πλαισίων κατά τη μεταγωγή. Ο σχετικός μηχανισμός ενεργοποιείται από ένα αίτημα επανασυσχέτισης. Συνιστώμενη πρακτική για το πρωτόκολλο IAPP, Inter Access Point Protocol
- **IEEE 802.11g**
  Επέκταση στο 802.11b ώστε να υποστηρίζει μεγαλύτερους ρυθμούς
- **IEEE 802.11h**
  Διαχείριση φάσματος στο 802.11a (DCS, Dynamic Channel Selection και TPC, Transmit Power Control)
- **IEEE 802.11i**
  Επεκτάσεις στο MAC επίπεδο για ενισχυμένη ασφάλεια
- **IEEE 802.11n**
  Με χρήση πολλαπλών κεραιών (μέθοδος γνωστή ως **MIMO**, εκ του Multiple Inputs Multiple Outputs) αναμένεται να παρέχει ονομαστικό ρυθμό μετάδοσης τουλάχιστον 108 Mbps. Σε αντίθεση με τα δύο προηγούμενα πρόκειται να τυποποιηθεί σύντομα και να κυκλοφορήσουν εμπορικά προϊόντα βασισμένα σε αυτό. Μάλιστα κάρτες ασύρματης δικτύωσης συμβατές με το 802.11n έχουν ήδη βγει στην αγορά από ορισμένους προμηθευτές, χωρίς να έχει οριστικοποιηθεί ακόμα το επίσημο πρότυπο.

1.4 Είναι οι τεχνολογίες συμπληρωματικές ή ανταγωνιστικές μεταξύ τους;

Η πραγματικότητα είναι ότι οι τεχνολογίες αυτές λειτουργούν μάλλον συμπληρωματικά καλύπτοντας η κάθε μία τις εφαρμογές που μπορεί καλύτερα.

802.11b/g – 802.11a

Οι 802.11b/g έχουν το πλεονέκτημα ότι λειτουργούν στη ζώνη των 2.4GHz, η οποία παγκόσμια, είναι ελεύθερη προς χρήση με ελάχιστους ρυθμιστικούς περιορισμούς που θα δούμε πιο αναλυτικά όταν αναφερθούμε στα κανάλια λειτουργίας. Από την άλλη πλευρά η ζώνη των 5GHz και η 802.11a έχει τη δυνατότητα να επιτρέψει υλοποίηση με περισσότερους χρήστες, μεγαλύτερη διαπερατότητα, καλύτερη σχεδίαση δικτύου, αλλά υπόκειται σε αρκετές χώρες σε σοβαρούς περιορισμούς ή δεν επιτρέπεται καθόλου η χρήση της. Αυτό μπορεί να οφείλεται στο ότι στην ίδια ζώνη υπάρχουν στρατιωτικές εφαρμογές, εκπομπές radar και υπάρχει κίνδυνος παρεμβολών σε υψίστης σημασίας συστήματα. Ήδη σε ευρωπαϊκές χώρες όπως η Αγγλία και η Ελλάδα η ζώνη συχνοτήτων των 5GHz έχει απελευθερωθεί.Επίσης λόγω της μεγαλύτερης συχνότητας λειτουργίας στο 802.11a η εμβέλεια, δηλαδή η μέγιστη απόσταση στην οποία είναι εφικτή η ασύρματη επικοινωνία, είναι αρκετά μικρότερη.Τέλος ο εξοπλισμός 802.11a είναι ακριβότερος λόγω της μεγαλύτερης συχνότητας λειτουργίας, αλλά και της μικρότερης διείσδυσης του προτύπου στην αγορά.

802.11g – 802.11a

Η 802.11g προσφέρει συμβατότητα προς τα πίσω με την 802.11b και επίσης μπορεί να θεωρηθεί σαν μία λύση κάλυψης, έχοντας μεγαλύτερη εμβέλεια από την 802.11a. Αντίθετα η 802.11a μπορεί να θεωρηθεί μια λύση για πυκνό και με μεγάλες ανάγκες ασύρματο δίκτυο.

802.11b – 802.11g

Η 802.11g προσφέρει μια ομαλή μετάβαση προς μεγαλύτερους ρυθμούς, επιτρέποντας μας να συνεχίσουμε τη λειτουργία στην ζώνη των 2.4GHz. Η συμβατότητα προς τα πίσω με το 802.11b, προστατεύει τις επενδύσεις που έχουν ήδη γίνει, ενώ παράλληλα χρησιμοποιεί μια ανώτερη τεχνική μετάδοσης.

Η διαμόρφωση που χρησιμοποιεί απαιτεί περισσότερη λαμβανόμενη ισχύ, έχει δηλαδή χειρότερη ευαισθησία. Έτσι η εμβέλεια είναι μικρότερη από αυτή του 802.11b, αφού βέβαια δεν υπάρχει η δυνατότητα να αυξήσουμε την ισχύ εκπομπής των συσκευών μας. Για το λόγο αυτό η χρήση του περιορίζεται για κάλυψη εσωτερικών χώρων, μικρής σχετικά επιφάνειας.

Από την άλλη το 802.11g θα επιβαρύνει σημαντικά το ήδη φορτωμένο και κοντά στον κορεσμό φάσμα των 2.4GHz. Επίσης προβλήματα συμβατότητας – διαλειτουργικότητας ανάμεσα σε b-g, g-g συσκευές ενδέχεται να παρουσιαστούν, ενώ η απόδοση ενός ασύρματου δικτύου σε μικτό περιβάλλον με 802.11b και 802.11g συσκευές είναι σημαντικά μειωμένη.

1.5 Χαρακτηριστικά του 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.

a) **Παρεμβολές**

Τα ασύρματο LAN μπορεί να δεχτεί και να προκαλέσει παρεμβολές σε άλλα 2.4GHz προϊόντα όπως μερικά ασύρματα τηλέφωνα ή φούρνοι μικροκυμάτων. Γενικά πάντως δεν έχει παρατηρηθεί να έχουν σημαντικό πρόβλημα με παρεμβολές από φούρνους μικροκυμάτων. Μπορεί επίσης να δεχθεί 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)

b) **Εμβέλεια**

Η εμβέλεια ενός ασύρματου δικτύου σε περιβάλλον γραφείου μπορεί να είναι μερικές δεκάδες μέτρα. Τα ραδιοκύματα σε εσωτερικό χώρο διαπερνούν 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.

c) **Ρυθμός μετάδοσης**

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

d) **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.

e) **Συμβατότητα με το υπάρχον δίκτυο**

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

f) **Διαλειτουργικότητα**

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

- ✓ **Διαφορετικές τεχνολογίες**

  Ένα ράδιο βασισμένο σε τεχνολογία FHSS δεν μπορεί να συνεργαστεί με κάποιο τεχνολογίας DSSS.
- ✓ **Διαφορετικές συχνότητες**

  Προφανώς συσκευές 802.11a στους 5.7GHz δεν 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.

1.6 Υπηρεσίες IEEE802.11

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:

1. Υπηρεσίες σταθμού (SS, Station Service)
   Οι υπηρεσίες αυτές υλοποιούνται σε κάθε ασύρματο σταθμό.

   a)Authentication
   b) Deauthentication
   c) Privacy
   d) MSDU delivery

2. 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

Μπορεί να υποθέσει κανείς ότι η διαφορά ενός AP από έναν client είναι μόνο η υλοποίηση των υπηρεσιών της δεύτερης κατηγορίας. Οι υπηρεσίες αυτές υλοποιούνται με λογισμικό και όχι με επιπλέον υλικό και έτσι η μεγάλη διαφορά κόστους που συνήθως υπάρχει ανάμεσα στις αντίστοιχες συσκευές δεν δικαιολογείται από την πλευρά του πραγματικού κόστους τους.

1.7 Υπηρεσίες σταθμού

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 κα 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 Serviec 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 ή ESS δικτύου πρέπει να χρησιμοποιήσουν την υπηρεσία αυτή πριν επικοινωνήσουν με άλλον 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-authentcation**
  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 μύνημα απο-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 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 ανταλλάσονται, 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 toy 802.11
  Πέρα από τις υπηρεσίες ασφαλείας δευτέρου επιπέδου, μπορεί να χρησιμοποιηθούν και υπηρεσίες ανωτέρω επιπέδων για έλεγχο της πρόσβασης και κωδικοποίηση, όπως το IPsec 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.
- **Data Delivery Data**
  Παρόμοια με αυτή που παρέχεται από άλλα δίκτυα IEEE 802. Η υπηρεσία αυτή παρέχει αξιόπιστη μεταφορά των πακέτων δεδομένων από το MAC του ενός σταθμού στο MAC ενός άλλου, με ελάχιστα διπλότυπα και αναδιατάξεις. Ο όρος αξιόπιστη μεταφορά σημαίνει ότι θα ζητηθεί επανεκπομπή των πακέτων αν διαπιστωθεί ότι αυτά έχουν λάθη. Ο λόγος που δεν αφήνουμε στα ανώτερα επίπεδα να χειριστούν το θέμα αυτό είναι ότι ο ραδιοφορέας είναι μη αξιόπιστος φορέας μετάδοσης και πολλά λάθη συμβαίνουν, άρα πολλές επανεκπομπές θα χρειαστούν να γίνουν.

1.8 Υπηρεσίες συστήματος διανομής

Παρέχουν διάφορες λειτουργίες στο DS. Τυπικά αυτές παρέχονται από τα AP

- **Association**
  Υπηρεσία με την οποία δημιουργείται μία λογική σύνδεση μεταξή ενός ασύρματου σταθμού και ενός AP. Κάθε σταθμός σχετίζεται με ένα AP, πριν του επιτραπεί να στείλει δεδομένα μέσω του AP προς το DS. 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..
- **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 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
- **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.
- **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.
- **Roaming**
  Ο τρόπος με τον οποίο γίνεται η συσχέτιση ενός σταθμού με το AP είναι εργασία του MAC επιπέδου. Όταν ένας σταθμός βρεθεί εντός εμβέλειας ενός ή περισσοτέρων AP, διαλέγει εκείνο το AP το οποίο έχει καλύτερο σήμα ή μικρότερο αριθμό λαθών. Η διαδικασία αυτή λέγεται **Joining a Basic Service Set** . Όταν γίνει αποδεκτή η συσχέτιση από το AP, ο σταθμός συντονίζεται στο κανάλι εκπομπής του AP. Περιοδικά γίνεται ανίχνευσή των καναλιών και στην περίπτωση που βρεθεί κανάλι με καλύτερα χαρακτηριστικά, γίνεται επανασυσχέτιση με το καινούργιο AP και συντονισμός του σταθμού στην καινούρια συχνότητα. Η επανασυσχέτιση μπορεί να γίνει λόγω **φυσικής μετακίνησης** του σταθμού ή

μπορεί να γίνει σαν αποτέλεσμα **υψηλού φόρτου** στο δίκτυο. Η λειτουργία αυτή γνωστή ως " **load balancing** " κατανέμει τον συνολικό φόρτο του WLAN με αποτελεσματικό τρόπο στην ασύρματη δομή του. Αυτός ο δυναμικός τροπος συσχέτισης επιτρέπει την διάρθρωση ενός WLAN με πολύ ευρεία κάλυψη απλώς δημιουργόντας μία σειρά από 802.11 κυψέλες. Για να πετύχει μια τέτοια σχεδίαση πρέπει οι κυψέλλες να σχεδιαστούν σωστά, δηλαδή να γίνει επιλογή της τοποθεσίας, της συχνότητας, των κεραιών.

Με χρήση των παραπάνω υπηρεσιών οι χρήστες (τα ανώτερα επίπεδα) μπορούν να απολαμβάνουν τις ακόλουθες δυνατότητες:

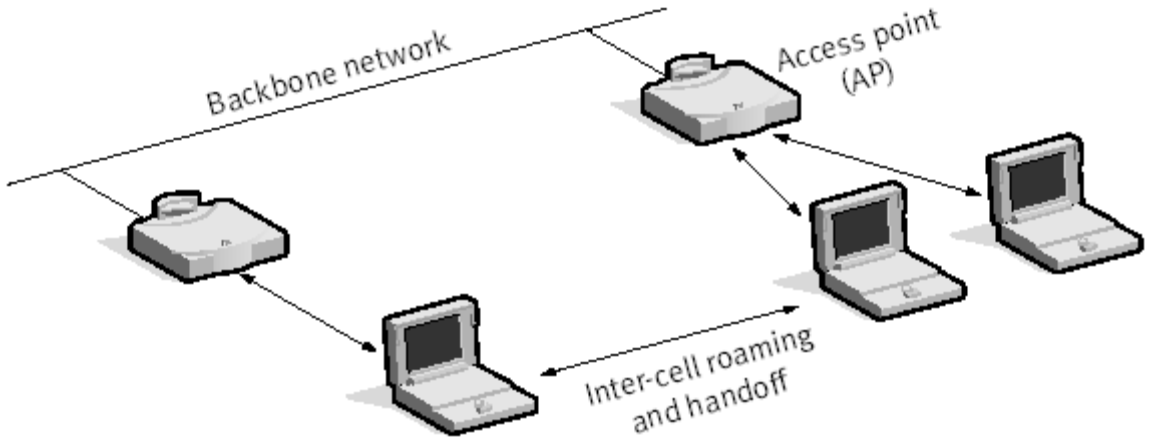
- **Mobility**

  Ενώ το πρότυπο περιγράφει πως ένας σταθμός συσχετίζεται σε ένα AP, δεν ορίζει **πως** τα AP ανιχνεύουν τους χρήστες, καθώς αυτοί περιάγονται. Αυτό μπορεί να γίνει είτε σε επίπεδο 2, μεταξύ δύο AP στο ίδιο υποδίκτυο, είτε σε επίπεδο 3, όταν ο χρήστης διασχίζει το σύνορο μεταξύ υποδικτύων.

  Ο πρώτος τρόπος μπορεί να γίνει με πρωτόκολλα που έχουν δημιουργηθεί από τον κατασκευαστή και τα οποία μπορεί να είναι διαφορετικά και να ποικίλουν στην επίδοση τους. Αν το πρωτόκολλο δεν είναι αποτελεσματικό, υπάρχει πιθανότητα να χαθούν πακέτα καθώς ο χρήστης περιάγεται από AP σε AP. Η WECA και η IEEE δημιουργούν πρότυπα και σε αυτό το κομμάτι.

  Ο δεύτερος τρόπος μπορεί να υλοποιηθεί με αντίστοιχα πρωτόκολλα, όπως το Mobile IP ή αλλιώς RFC2002. Σε αυτό κάθε χρήστης έχει ορισμένο ένα AP, σαν "home agent". Όταν ένας σταθμός μπαίνει σε άλλη περιοχή, το νέο AP ρωτάει το σταθμό για τον "home agent". Στη συνέχεια εγκαθίσταται ένας μηχανισμός προώθησης πακέτων από το ένα AP στο άλλο, έτσι ώστε η IP του χρήστη να διατηρηθεί και ο χρήστης να λαμβάνει διαφανώς τα δεδομένα του. Το πρωτόκολλο αυτό δεν είναι ακόμα στην τελική του μορφή, οπότε οι κατασκευαστές μπορεί να παρέχουν τα δικά τους αντίστοιχα.

  Τέλος μία ατελής αλλά αποτελεσματική λύση είναι το πρωτόκολλο DHCP , ώστε να ανατίθενται αυτόματα νέες διευθύνσεις στον χρήστη που περιάγεται στο δίκτυο.



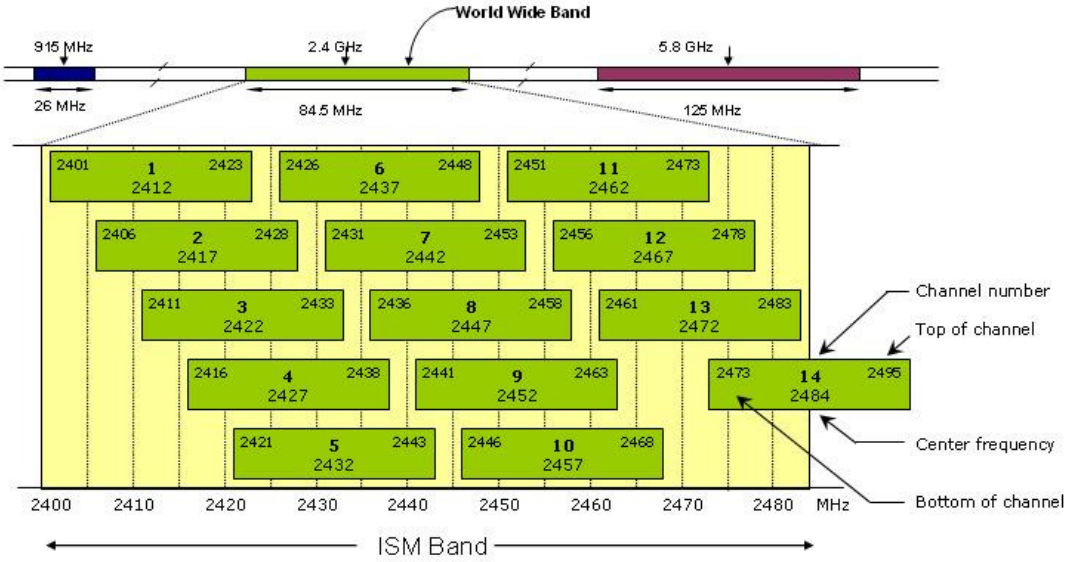
1.9 Τι μηχανισμοί υπάρχουν;

Το 802.11 υποστηρίζει δύο τρόπους λειτουργίας: ομότιμα, όπου δεν υπάρχει κάποιος κεντρικός σταθμός βάσης-σημείο πρόσβασης, οι κόμβοι είναι ισότιμοι και η πρόσβαση στο κοινό μέσο (τον κενό χώρο) ρυθμίζεται από κάποιο κατανεμημένο πρωτόκολλο όπως το CSMA (έτσι λειτουργούν τα ad hoc WLAN), και με σημείο πρόσβασης, έναν κεντρικό κόμβο του τοπικού δικτύου δηλαδή -συνήθως συνδεδεμένο σε ενσύρματο δίκτυο κορμού (π.χ. στο Internet ή σε κάποιο μεγάλο Ethernet LAN)- ο οποίος αναλαμβάνει τον έλεγχο πρόσβασης στο κοινό μέσο και δρα ως αμφίδρομος επαναλήπτης. Τα WLAN με σημείο πρόσβασης ονομάζονται δίκτυα υποδομής ή

δομημένα (infrastructure). Το σύνηθες μοντέλο που περιγράφει τέτοια δίκτυα είναι το εξής: υπάρχει ένα ενσύρματο δίκτυο κορμού (σύστημα κατανομής, DS) στο οποίο συνδέονται τα σημεία πρόσβασης (AP). Μία ομάδα κοινών κόμβων (STA) που επικοινωνούν ασύρματα με ένα συγκεκριμένο AP σε συγκεκριμένη συχνότητα ονομάζεται Βασικό Σύνολο Υπηρεσιών (BSS). Τα BSS διασυνδέονται μεταξύ τους μέσω του DS. Ας σημειωθεί ότι μπορεί τα STA ενός BSS να μην είναι όλα στην εμβέλεια όλων αλλά πρέπει οπωσδήποτε όλα να είναι στην εμβέλεια του σημείου πρόσβασης.

Όλα τα πρωτόκολλα 802.11x έχουν κοινό επίπεδο MAC και διαφέρουν στο φυσικό μέσο. Το επίπεδο LLC, που αναλαμβάνει τον έλεγχο ροής, τον έλεγχο σφαλμάτων και τη διασύνδεση προς το επίπεδο δικτύου, ταυτίζεται με το καθιερωμένο κοινό πρωτόκολλο 802.2 που χρησιμοποιείται και στο Ethernet και στα περισσότερα ενσύρματα χτοπικά δίκτυα -με αποτέλεσμα την άμεση και χωρίς ανάγκη μετατροπών συνδεσιμότητα ενός 802.11 WLAN με το Internet ή άλλα WAN/διαδίκτυα που χρησιμοποιούν το IP ως πρωτόκολλο δικτύου. Το βασικό πρωτόκολλο MAC του 802.11 είναι το **DCF**, το οποίο βασίζεται στη μέθοδο CSMA/CA, ενώ στα δομημένα WLAN πάνω από το DCF τρέχει επιπλέον το πρωτόκολλο **PCF** το οποίο, αξιοποιώντας το AP, προσφέρει στα τερματικά όταν χρειάζεται πρόσβαση στο κοινό μέσο χωρίς ανταγωνισμό και συγκρούσεις.

Ο ρυθμός μετάδοσης δεδομένων στο 802.11 εξαρτάται από την απόσταση μεταξύ των κόμβων. Όσο πιο μακριά βρίσκεται η ασύρματη συσκευή από το σημείο πρόσβασης, τόσο χαμηλότερη είναι η ταχύτητα. Επίσης, λόγω της χρήσης του CSMA/CA αντί του CSMA/CD, η πραγματική διαμεταγωγή δεν υπερβαίνει το ήμισυ της ονομαστικής ταχύτητας: τα 54 Mbps του φυσικού επιπέδου στην πραγματικότητα δεν υπερβαίνουν ποτέ τα 27 Mbps στο LLC. Επιπλέον τα σημεία πρόσβασης που υποστηρίζουν ένα μεικτό δίκτυο b και g ρίχνουν τη διαμεταγωγή σε 18 Mbps, αρχικά, για να καταλήξουν σε περίπου 6 έως 9 Mbps όταν εκπέμπουν οι πελάτες.



1.10 Κανάλια μετάδοσης

Το 802.11 διαιρεί τις ζώνες συχνοτήτων που αναφέραμε παραπάνω σε κανάλια. Για παράδειγμα, η ζώνη 2.4000–2.4835 GHz διαιρείται σε 13 κανάλια, με μέγεθος 22 MHz το κάθε ένα και με 5 Mhz κενό ανάμεσα από κάθε κανάλι (σχήμα 1). Η διαθεσιμότητα των καναλιών εξαρτάται από το νομοσχέδιο κάθε χώρας. Όταν τα AP βρίσκονται κοντά το ένα στο άλλο, είναι καλό να επιλέγεται διαφορετικό κανάλι μετάδοσης για το κάθε ένα, έτσι ώστε να μην έχουμε δυσλειτουργία.

1.11 Τύποι συσκευών

Ορίζονται από το πρότυπο 802.11 οι εξής τύποι συσκευών:

➔ Το σημείο πρόσβασης (Access Point) και ο ασύρματος σταθμός (wireless station) . Και τα δύο μπορεί να είναι ένα PC ή Laptop ή κάποια συσκευή χειρός, εφοδιασμένα με την κατάλληλη κάρτα ή να είναι ξεχωριστή αυτόνομη συσκευή η οποία να επικοινωνεί με το PC με κάποιο interface (ethernet ή Usb). Και τα δύο πρέπει να εμπεριέχουν τη λειτουργικότητα του 802.11 πρωτοκόλλου δηλαδή το MAC και φυσικό επίπεδο. Οι λειτουργίες αυτές υλοποιούνται με υλικό και λογισμικό.

➔ AP, Access Point

Αποτελείται από ένα ράδιο, μία διεπαφή δικτύου, όπως 802.3 και το λογισμικό που επιτελεί τη λειτουργία της γεφύρωσης (bridging).

Το AP λειτουργεί σαν σταθμός βάσης κάνοντας συγκέντρωση της κίνησης από τους ασύρματους σταθμούς (aggregation) και κατευθύνοντας την προς το ενσύρματο δίκτυο. Παρέχουν επίσης τις λειτουργίες της ανίχνευσης σταθμού (tracking) και της αυθεντικοποίησης κ.α.

➔ Ασύρματοι σταθμοί

Μπορεί να είναι PCI, PCMCIA, ISA NIC κάρτες σε ένα υπολογιστή, ή να πρόκειται για άλλου τύπου συσκευές, όπως τηλεφωνικές συσκευές με 802.11 λειτουργικότητα. Είναι απλούστεροι από τους σταθμούς βάσης.

1.12 PCF και DCF

Το DCF δίνει λύση στα, έμφυτα στις ασύρματες επικοινωνίες, προβλήματα του **κρυμμένου τερματικού** και του **εκτεθειμένου τερματικού**, τα οποία είναι και ο λόγος για τον οποίον δεν μπορεί να εφαρμοστεί η μέθοδος CSMA/CD του Ethernet σε WLAN. Το πρόβλημα του κρυμμένου τερματικού έγκειται στο ότι αν ένα τερματικό Γ εκπέμπει σε ένα τερματικό Β, ένα άλλο τερματικό Α που θέλει να αποστείλει δεδομένα στο Β αλλά είναι εκτός εμβέλειας του Γ δε θα ανιχνεύσει ότι το κανάλι είναι απασχολημένο και θα εκπέμψει. Το αντίστροφο πρόβλημα του εκτεθειμένου τερματικού αφορά το ότι ένα τερματικό Α μπορεί να μη μεταδώσει πλαίσιο σε ένα άλλο τερματικό Β, νομίζοντας ότι το κανάλι είναι κατειλημμένο γιατί ανιχνεύει εκπομπή από ένα τερματικό Γ προς ένα τερματικό Δ. Τα Γ και Δ όμως είναι εκτός εμβέλειας του Β άρα στην πραγματικότητα δεν επρόκειτο να γίνει σύγκρουση.

Τα προβλήματα αυτά επιλύονται συνήθως με την ανίχνευση εικονικού καναλιού (με πλαίσια ελέγχου RTS και CTS) που εκτελεί το DCF: η κεντρική ιδέα πίσω από τη λειτουργία του πρωτοκόλλου είναι η μετάθεση των συγκρούσεων μεταξύ των πλαισίων σε μικρά πλαίσια ελέγχου (RTS, CTS), αντί για τα πλαίσια δεδομένων, ώστε να εξοικονομείται εύρος ζώνης. Συγκεκριμένα, ένας σταθμός που θέλει να εκπέμψει αποστέλλει ένα πακέτο RTS στον παραλήπτη ζητώντας έτσι άδεια να καταλάβει το κανάλι. Αν ο παραλήπτης είναι διαθέσιμος απαντά με ένα πλαίσιο CTS, το οποίο μόλις ληφθεί από τον αποστολέα τού δίνει τη δυνατότητα να αρχίσει να εκπέμπει τα δεδομένα του (ενεργοποιώντας ταυτόχρονα ένα χρονόμετρο επιβεβαίωσης) χωρίς πιθανότητα σύγκρουσης, αφού οι υπόλοιποι κόμβοι που άκουσαν το RTS ή το CTS γνωρίζουν ότι το κανάλι είναι κατειλημμένο και εισέρχονται σε κατάσταση αναμονής για κατάλληλο χρονικό διάστημα (NAV), το οποίο υπολογίζεται από τις πληροφορίες που μεταφέρουν τα πλαίσια ελέγχου. Όταν λήξει το διάστημα αυτό οι κόμβοι που έχουν πλαίσια προς αποστολή επιχειρούν να καταλάβουν το κανάλι με την ίδια διαδικασία αλλά σε διαφορετικές χρονικές στιγμές (με χρήση του αλγορίθμου δυαδικής εκθετικής οπισθοχώρησης που χρησιμοποιείται και στο CSMA/CD), ώστε να μειωθεί η πιθανότητα σύγκρουσης. Αν, παρ' όλα αυτά, δύο σταθμοί συγκρουστούν, τίθενται ξανά σε αναμονή, περιμένουν ένα τυχαίο χρονικό διάστημα και ξαναπροσπαθούν.

Το PCF ενεργοποιείται αυτόματα για συγκεκριμένα διαστήματα όταν το AP το κρίνει απαραίτητο ώστε, αν π.χ. πρόκειται να μεταδοθεί χρονικά κρίσιμη πληροφορία να εξασφαλιστεί ότι δε θα υπάρξουν συγκρούσεις για κάποιο διάστημα. Στην αρχή κάθε τέτοιας περιόδου χωρίς ανταγωνισμό το AP στέλνει σε όλους τους κόμβους ένα πλαίσιο συγχρονισμού (Beacon) και στη συνέχεια διαμοιράζει το χρόνο σε θυρίδες και αναθέτει σε κάθε σταθμό μία θυρίδα κατά την οποία μόνο αυτός μπορεί να εκπέμψει ή να λάβει δεδομένα. Τα πλαίσια από έναν κόμβο Α σε έναν κόμβο Β μπορούν είτε να μεταδοθούν από τον Α στο AP (κατά τη θυρίδα του Α) και στη συνέχεια από τον

AP στον Β (κατά τη θυρίδα του Β), είτε απευθείας από τον Α στον Β κατά τη θυρίδα του Α. Η έναρξη κάθε θυρίδας σηματοδοτείται από την αποστολή ενός πλαισίου ελέγχου Poll από τον AP στον κόμβο που του ανήκει η τρέχουσα θυρίδα.

1.13 Το μέλλον…

Αναρωτιέται κανείς ποια θα είναι η πορεία της ασύρματης δικτύωσης. Ποια θα είναι η ανάπτυξη της τεχνολογίας καθώς και τα προϊόντα της την επόμενη πενταετία. Η προοπτική για τα ασύρματα δίκτυα είναι ελπιδοφόρα. Η ωρίμανση των προτύπων αποτελεί κίνητρο για τους προμηθευτές ώστε να παράγουν νέα προϊόντα ασύρματης δικτύωσης και να μειώσουν τις τιμές σε επίπεδα πιο προσιτά στο καταναλωτικό κοινό.

Η παρουσία προτύπων θα παρακινήσει τις μικρότερες επιχειρήσεις να κατασκευάσουν τα ασύρματα προϊόντα επειδή δεν θα πρέπει να επενδύσουν μεγάλα χρηματικά ποσά στους τομείς της έρευνας και ανάπτυξης των προϊόντων. Αυτές οι επενδύσεις ήδη θα έχουν γίνει και θα έχουν ενσωματωθεί μέσα στα πρότυπα, τα οποία θα είναι διαθέσιμα σε κάθε ενδιαφερόμενο που επιθυμεί να εγκαταστήσει ασύρματα δίκτυα.

ABI Research: 802.11n στο 87% των smartphones, το 2014

Σύμφωνα με πρόσφατα δημοσιευμένη έρευνα της ABI Research, περίπου το 87% των smartphones ενδέχεται να υποστηρίξουν το πρότυπο 802.11n του Wi-Fi το 2014. Οι δηλώσεις αυτές έρχονται φυσικά σε πλήρη αντιδιαστολή με τη σημερινή πραγματικότητα, καθώς μόλις το 1% του συνόλου των smartphones που διατέθηκαν τον προηγούμενο χρόνο υποστηρίζει το πρότυπο αυτό.

Σύμφωνα με τις δηλώσεις του κ. Michael Morgan της ABI Research, *«Η υιοθέτηση του προτύπου 802.11n εξαρτάται περισσότερο από τους κατασκευαστές ολοκληρωμένων κυκλωμάτων παρά από τους κατασκευαστές κινητών τηλεφώνων. Παρ' όλα αυτά, το 2010 είναι πλέον η σωστή στιγμή, ώστε να πραγματοποιηθεί το... "επίσημο ντεμπούτο" σε high-end κυρίως smartphones. Έπρεπε βέβαια να περιμένουμε από τους καταναλωτές να κάνουν μεταστροφή σε 802.11n access points. Τώρα που το 50% περίπου των access points υποστηρίζουν το 802.11n και οι χρήστες είναι περισσότερο εξοικειωμένοι με τις δυνατότητές του είναι η κατάλληλη στιγμή για την εμφάνιση του.»*

Αξιοσημείωτο είναι βέβαια το γεγονός πως οι κάτοχοι κινητών τηλεφώνων που υποστηρίζουν το πρότυπο n δε θα μπορούν, τουλάχιστον εξαρχής, να έχουν την ίδια απόδοση με αντίστοιχα laptops ή netbooks. Ο κ. Michael Morgan δηλώνει επίσης πως οι εφοδιασμένες με 802.11n συσκευές κινητών, τουλάχιστον στα πρώτα στάδια δε θα υποστηρίζουν την τεχνολογία MIMO (Multiple Input Multiple Output) ή τις υπόλοιπες βελτιώσεις που θα παρέχει το πρότυπο n. *«Οι χρήστες κινητών τηλεφώνων δε θα είναι σε θέση εξαρχής να καταλάβουν τον ίδιο βαθμό βελτίωσης όπως στα laptops. Παρ' όλο που το 802.11n θα αρχίσει να διείσδυσή του στα low και mid-end smartphones εντός του 2012, δε θα υπάρξουν θεαματικές αλλαγές μέχρι τουλάχιστον το 2014»*, επισημαίνει χαρακτηριστικά.

Η ABI Research προσδιορίζει πως η διαφορά του κατασκευαστικού κόστους της ενσωμάτωσης του προτύπου n σε σχέση με τα b/g πρότυπα είναι σχεδόν μηδαμινή. Επιπλέον, τα ήδη υπάρχοντα πρότυπα θα συνεχίσουν να συνυπάρχουν με το πρότυπο n καθώς αυτό θα καθιστά τη συσκευή λειτουργική σε πολλά περιβάλλοντα. Όσον αφορά τις συχνότητες λειτουργίας *«το πρότυπο n λειτουργεί αποδοτικότερα στα 5 GHz, ενώ τα υπόλοιπα πρότυπα είναι περιορισμένα στα 2.4 GHz»*, δηλώνει ο κ. Michael Morgan και καταλήγει αναφέροντας πως *«είναι σημαντικό για τους κατασκευαστές να συνεχίσουν να παρέχουν όλα αυτά τα διαφορετικά πρωτόκολλα και, εάν είναι δυνατόν, επιλεγόμενες συχνότητες λειτουργίας.*

ΚΕΦΑΛΑΙΟ 2ο
IEEE 802.11a

Στο κεφάλαιο αυτό παρουσιάζεται η αρχιτεκτονική του συστήματος 802.11a με αναφορά στο μοντέλο OSI, εξετάζοντας τα δύο κατώτερα επίπεδα του μοντέλου. Οι προδιαγραφές που έχει εκδώσει η IEEE αφορούν στο φυσικό επίπεδο (PHY) και στο επίπεδο ελέγχου πρόσβασης στο μέσο (MAC). Αυτά τα δύο επίπεδα θα περιγραφούν παρακάτω.

2.1 Το επίπεδο ελέγχου πρόσβασης στο μέσο

Ο βασικός μηχανισμός πρόσβασης στο MAC του 802.11a είναι η Πολλαπλή Πρόσβαση με Ανίχνευση Φέροντος και Αποφυγή Συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA). Σύμφωνα με τον μηχανισμό αυτό ένα τερματικό πρέπει να ανιχνεύσει αν το μέσο χρησιμοποιείται από κάποιο άλλο τερματικό. Αν το μέσο δεν είναι κατηλλειμμένο τότε μπορεί να προχωρήσει σε εκπομπή. Ο αλγόριθμος CSMA/CA καθορίζει πως το τερματικό που θέλει να εκπέμψει πρέπει να ανιχνεύσει το κανάλι ελεύθερο για καθορισμένο χρονικό διάστημα και μετά να το καταλάβει. Σε αντίθετη περίπτωση τα τερματικό πρέπει να αποφύγει την κατάληψη μέχρι το μέσο να ελευθερωθεί εκ νέου για τον παραπάνω καθορισμένο χρόνο. Για να μειωθεί περαιτέρω η πιθανότητα σύγκρουσης χρησιμοποιείται η μέθοδος ανταλλαγής μηνυμάτων RTS/CTS. Η διαδικασία που περιγράφηκε καθορίζει τη Διανεμημένη Συνάρτηση Συντονισμού (Distributed Coordination Function, DCF) που είναι υποχρεωτικό να υποστηρίζεται από όλα τα τερματικά που συμμετέχουν στο δίκτυο. Όλα τα παραπάνω περιγράφονται με λεπτομέρειες στις παραγράφους που ακολουθούν.

2.1.1 Ο μηχανισμός ανίχνευσης φέροντος

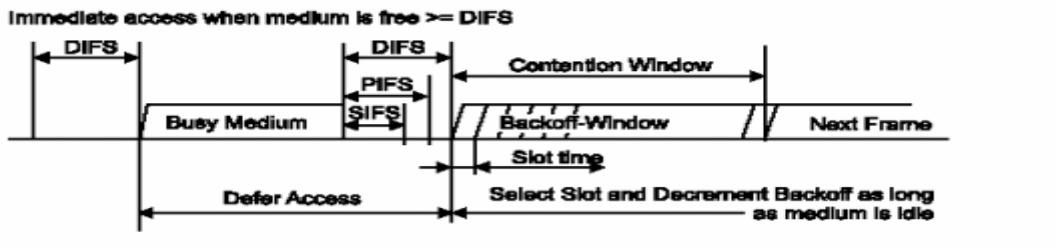
Ο μηχανισμός ανίχνευσης φέροντος γίνεται τόσο με φυσικό όσο και με εικονικό τρόπο. Ο φυσικός τρόπος βασίζεται στην ανίχνευση, μέσω της κεραίας στο φυσικό επίπεδο, φέροντος, στη συχνότητα που λειτουργεί το σύστημά μας. Ο εικονικός μηχανισμός παρέχεται από το MAC και αναφέρεται ως Διάνυσμα Κατανομής Δικτύου (Network Allocation Vector, NAV). Το NAV πετυχαίνει μια πρόβλεψη της μελλοντικής κίνησης στο μέσο βασιζόμενος στις πληροφορίες για τη διάρκεια των πακέτων που υπάρχουν στα πακέτα RTS και CTS. Το NAV μπορεί να θεωρηθεί ως ένας μετρητής που μετράει αντίστροφα το χρόνο μέχρι το κανάλι να ελευθερωθεί, βασισμένος στη γνώση που έχει για την κίνηση στο κανάλι. Όταν είναι μη μηδενικόςτο κανάλι θεωρείται κατηλλειμένο ενώ όταν μηδενιστεί ελεύθερο.

2.1.2 Πλαίσια επιβεβαίωσης επιπέδου MAC

Η παραλαβή κάποιων πακέτων απαιτεί από τον παραλήπτη την αποστολή πλαισίου επιβεβαίωσης (acknowledgment frame, ACK) στον αποστολέα. Η τεχνική αυτή είναι γνωστή σαν θετική επιβεβαίωση. Απώλεια παραλαβής ενός αναμενόμενου πλαισίου ACK δείχνει στον αποστολέα του αρχικού πακέτου πως κάποιο λάθος έγινε στη μετάδοση. Ωστόσο υπάρχει και η περίπτωση το αρχικό πακέτο να παραδόθηκε σωστά και το λάθος να έγινε στη μετάδοση του ACK. Ο αποστολέας δεν μπορεί να ξεχωρίσει μεταξύ των δυο περιπτώσεων. Ο παραλήπτης από τη στιγμή που δέχεται σωστά κάποιο πακέτο πληροφορίας είναι υποχρεωμένος μετά παρέλευση χρόνου SIFS να στείλει στον αποστολέα πλαίσιο επιβεβαίωσης ACK χωρίς να ελέγξει αν το μέσο είναι ελεύθερο ή κατηλλειμμένο. Από την πλευρά του ο αποστολέας μετά την αποστολή του πλαισίου πληροφορίας θα περιμένει χρονικό διάστημα ACKTimeout και αν δε λάβει πλαίσιο ACK τότε θα προγραμματίσει επανεκπομπή.

2.1.3 Χρονικά διαστήματα μεταξύ πλαισίων

Το χρονικό διάστημα μεταξύ πλαισίων ονομάζεται IFS (InterFrame Space). Με αναφορά στο σχήμα 2.1 παρατηρούμε ότι υπάρχουν δύο είδη χρονικών διαστημάτων.



Σχήμα 2.1
Είδη IFS

Το μικρότερο από τα IFS είναι το SIFS (Short IFS). Χρησιμοποιείται πριν από την αποστολή πλαισίων ACK, RTS, CTS. Η διάρκειά του καθορίζεται από το πρωτόκολλο και είναι 16μs . Το DIFS (DCF IFS) είναι ο χρόνος για τον οποίο ένα τερματικό πρέπει να ανιχνεύσει το κανάλι ελεύθερο προτού προχωρήσει σε εκπομπή. Η διάρκειά του είναι 34μs.

2.1.4 Χρόνος οπισθοχώρησης (Backoff Time)

Ένα τερματικό που θέλει να στείλει δεδομένα μέσω του μηχανισμού ανίχνευσης φέροντος καθορίζει αν το μέσο είναι ελεύθερο ή κατηλλειμμένο. Αν είναι ελεύθερο για χρόνο μεγαλύτερο του DIFS τότε το τερματικό δεν εκπέμπει αμέσως αλλά μετά από έναν τυχαίο χρόνο οπισθοχώρησης (random backoff time) που υπολογίζει. Το χρονικό διάστημα που διαρκεί ο χρόνος οπισθοχώρησης ονομάζεται παράθυρο συγκράτησης (contention window, CW). Η διαδικασία αυτή βοηθά στην αποφυγή συγκρούσεων μεταξύ τερματικών που προσπαθούν να καταλάβουν το μέσο στο τέλος κάποιου χρόνου DIFS. Η διαδικασία για τον υπολογισμό του τυχαίου χρόνουοπισθοχώρησης είναι

Backoff Time = Random() × aSlotTime

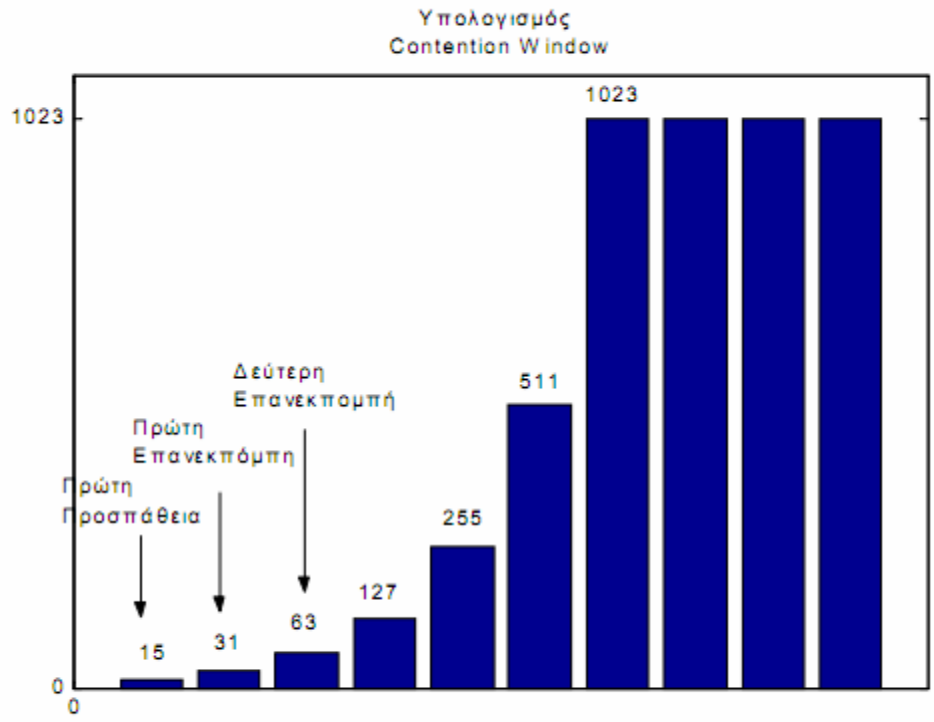
Όπου Random() είναι ψευδοτυχαίος αριθμός με ομοιόμορφη κατανομή στο διάστημα [0,CW], aCWmin $\leq$ CW $\leq$ aCWmax. Είναι σημαντικό τα τερματικά να έχουν διαφορετικές ακολουθίες τυχαίων αριθμών προς αποφυγή συγκρούσεων. Τα aCWmin, aCWmax καθορίζονται από το πρωτόκολλο και για το 802.11a έχουν τις τιμές

aCWmin = 15 × aSlotTime

aCWmax = 1023 × aSlotTime

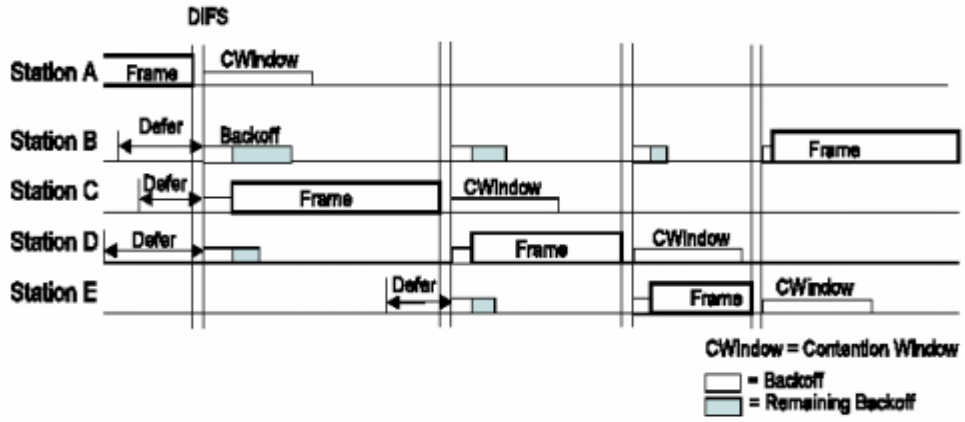
aSlotTime είναι το μικρότερο χρονικό διάστημα στο οποίο μπορούμε νααναφερόμαστε στο πρότυπο 802.11a και έχει τιμή 9μs. Στην πρώτη απόπειρα κατάληψης του μέσου το Backoff Time παίρνει τιμή μεταξύ [0,15] × aSlotTime. Το πρότυπο καθορίζει επίσης ένα μέγιστο αριθμό προσπαθειών για εκπομπή για κάθε πακέτο. Όταν αυτό το όριο ξεπεραστεί το πακέτο απορρίπτεται. Αν στην πρώτη προσπάθεια υπάρξει σύγκρουση, που ο αποστολέας αντιλαμβάνεται μέσω της έλλειψης πακέτου ACK, τότε το τερματικό υπολογίζει νέο χρόνο οπισθοχώρησης αυτή τη φορά στο διάστημα [0,31] × aSlotTime. Αυτό επαναλάμβάνεται μετά από κάθε αποτυχημένη εκπομπή μέχρι να φτάσουμε στο όριο aCWmax. Το όριο του Contention Window μέσα στο οποίο υπολογίζεται ο χρόνος οπισθοχώρησης αυξάνεται κάθε φορά κατά μία δύναμη του 2 μείον 1 (σχήμα 2.2). Δηλαδή

CW = 2(i+4)-1 , όπου i = 0,1,2,…,6 αντίστοιχα για την πρώτη προσπάθεια, την πρώτη επανεκπομπή, τη δεύτερη επανεκπομπή κ.ο.κ.



Σχήμα 2.2

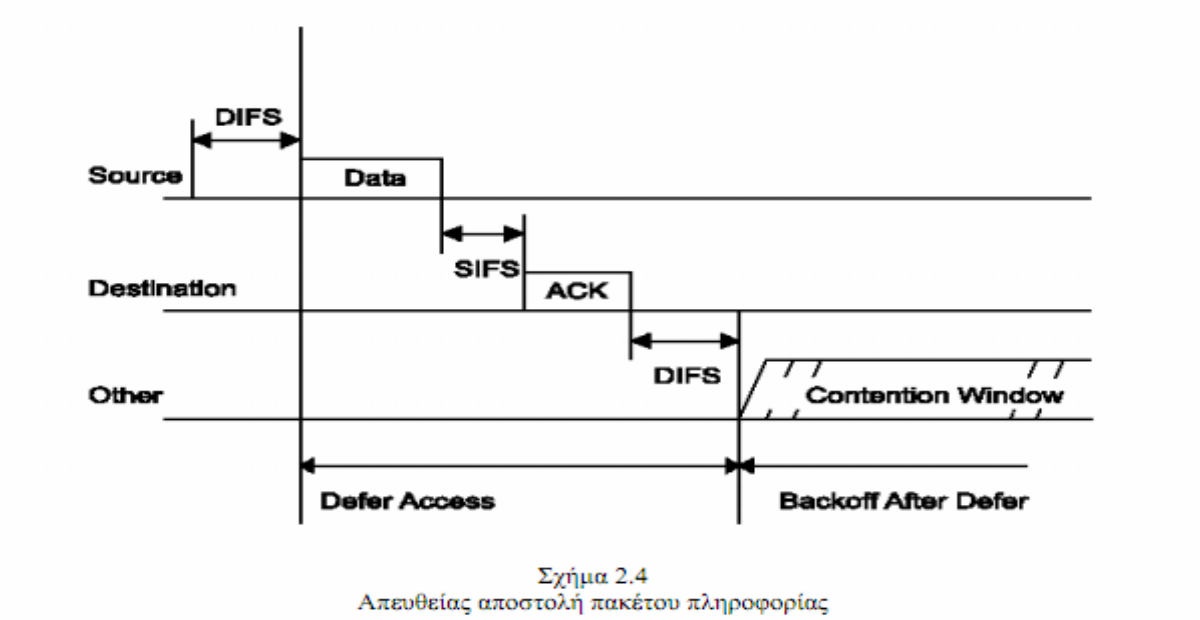
Αφού το τερματικό έχει ανιχνεύσει το μέσο ελεύθερο για χρόνο DIFS αρχίζει να μειώνει το Backoff Time κατά aSlotTime κάθε φορά, εφόσον κατά τη διάρκεια του aSlotTime το μέσο είναι ελεύθερο. Στην αντίθετη περίπτωση το τερματικό σταματά να μειώνει το Backoff Time και συνεχίζει τη διαδικασία την επόμενη φορά που το μέσο γίνεται ελεύθερο για χρόνο DIFS. Όταν ο χρόνος οπισθοχώρησης φτάσει στο μηδέν το τερματικό εκπέμπει. Μετά από κάθε επιτυχημένη εκπομπή το Contention Window επιστρέφει στη μικρότερη τιμή του aCWmin. Τα παραπάνω φαίνονται χαρακτηριστικά στο σχήμα 2.3.



Σχήμα 2.3
Διαδικασία μείωσης του χρόνου οπισθοχώρησης

2.1.5 Βασική διαδικασία αποστολής

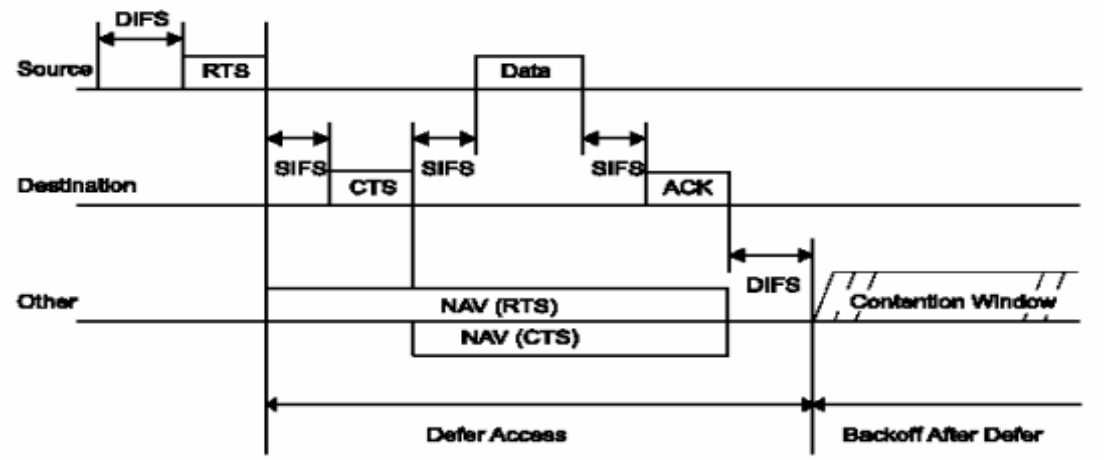
Η βασική διαδικασία αποστολής, όπως είδαμε και παραπάνω, είναι το τερματικό να στέλνει το πλαίσιο πληροφορίας μετά από χρόνο DIFS και την παρέλευση του χρόνου οπισθοχώρησης. Τα τερματικά που διαβάζουν τη διάρκεια του πακέτου υπολογίζουν το χρόνο που το μέσο θα είναι κατηλλειμμένο και δίνουν αυτή την τιμή στο NAV. Για αυτό το χρόνο αποφεύγουν κατάληψη του μέσου. Το τερματικό για το οποίο προορίζεται το πακέτο, εάν το λάβει σωστά, στέλνει μετά από χρόνο SIFS πλαίσιο επιβεβαίωσης ACK. Η διαδικασία αυτή φαίνεται χαρακτηριστικά στο παρακάτω σχήμα.



Σχήμα 2.4
Απευθείας αποστολή πακέτου πληροφορίας

2.1.6 Διαδικασία αποστολής με πλαίσια RTS/CTS

Εκτός από τη βασική διαδικασία αποστολής όπου το τερματικό στέλνει το πακέτο αμέσως αφού έχει ανιχνεύσει το μέσο ελεύθερο για χρόνο DIFS και μετά την παρέλευση του χρονου οπισθοχώρησης, το πρωτόκολλο υποστηρίζει και τη διαδικασία αποστολής με χρήση πακέτων RTS/CTS. Κατά τη διαδικασία αυτή το τερματικό που θέλει να στείλει ένα πακέτο σε κάποιο άλλο, μετά την παρέλευση του χρόνου οπισθοχώρησης δε στέλνει απευθείας το πακέτο αλλά αρχικά ένα πλαίσιο αίτησης αποστολής (Request To Send, RTS). Όλα τα τερματικά που λαμβάνουν το πλαίσιο RTS, υπολογίζουν από την πληροφορία που περιέχεται σε αυτό για το μήκος του πακέτου πληροφορίας, το χρόνο, που το κανάλι θα παραμείνει κατηλλειμμένο. Αυτή είναι και η τιμή που παίρνει το NAV για όλα τα τερματικά που έχουν λάβει το RTS. Το τερματικό προς το οποίο απευθύνεται η αίτηση αποστολής πρέπει μετά από χρόνο SIFS να απαντήσει στον αποστολέα με ένα πλαίσιο ελεύθερος προς αποστολή (Clear To Send, CTS) αν το NAV του τερματικού αυτού δείχνει ότι το κανάλι είναι ελεύθερο. Με το πλαίσιο CTS ουσιαστικά το κανάλι έχει δεσμευθεί για όσο χρόνο χρειάζεται για να γίνει η αποστολή του πακέτου που ζήτησε αρχικά το τερματικό που έστειλε το πλαίσιο RTS. Το παρακάτω σχήμα δείχνει χαρακτηριστικά πως λειτουργεί η διαδικασία RTS/CTS για τον αποστολέα σταθμό, τον παραλήπτη σταθμό και τους υπόλοιπους σταθμούς που συμμετέχουν στο δίκτυο.



Σχήμα 2.5
Αποστολή RTS/CTS/data/ACK και καθορισμός του NAV

2.1.7 Ανίχνευση διπλοτύπων και αποκατάσταση

Με την παραπάνω διαδικασία αποστολής υπάρχει η περίπτωση ένα πακέτο να σταλεί περισσότερες από μία φορά προς κάποιο τερματικό. Αυτό μπορεί για παράδειγμα να συμβεί στην περίπτωση που ενώ το πλαίσιο πληροφορίας έχει ληφθεί σωστά από ένα τερματικό το ACK που έστειλε αυτό ως επιβεβαίωση να καταστραφεί και να μη φτάσει στον αποστολέα. Τότε ο αποστολέας θα ξαναστείλει το πλαίσιο πληροφορίας. Για την αποφυγή λήψης διπλοτύπων κάθε πακέτο έχει έναν αύξοντα αριθμό (Sequence number). Ο αριθμός αυτός μπαίνει στο πακέτο από τον αποστολέα. Ο παραλήπτης κρατά ένα αρχείο με τους αύξοντες αριθμούς των πρόσφατα ληφθέντων πακέτων και τους συγκρίνει με αυτόν του πακέτου που μόλις έλαβε. Στην περίπτωση που είναι ίδιος με κάποιον από τα πακέτα που ήδη έλαβε, απορρίπτει το εν λόγω πακέτο. Ακόμα και στην περίπτωση αυτή όμως ο παραλήπτης είναι υποχρεωμένος να στείλει πλαίσιο ACK.

2.2 Τύποι πλαισίων στο 802.11a

Στο πρωτόκολλο 802.11a υπάρχουν τρεις διαφορετικοί τύποι πλαισίων για μετάδοση. Αυτοί χρησιμοποιούνται για διαχείριση, έλεγχο και αποστολή πακέτων πληροφορίας. Τα πλαίσια διαχείρισης χρησιμοποιούνται για τη σύνδεση και αποσύνδεση ενός τερματικού από το δίκτυο. Τα πλαίσια ελέγχου χρησιμοποιούνται για την αποστολή αιτήσεων και επιβεβαιώσεων. Τα πλαίσια ελέγχου που μας ενδιαφέρουν είναι τα RTS, CTS, ACK. Παρακάτω θα δούμε κάπως πιο αναλυτικά τη μορφή των πλαισίων που αναφέραμε.

2.2.1 Πλαίσιο αποστολής πληροφορίας

Το πλαίσιο αποστολής πληροφορίας έχει τη μορφή του σχήματος

Σχήμα 2.7
Μορφή πλαισίου μετάδοσης πληροφορίας

Η επικεφαλίδα του MAC (MAC header) αποτελείται από 30 bytes. Σε αυτό το τμήμα του πλαισίου υπάρχουν

- οι διευθύνσεις του αποστολέα και του παραλήπτη σταθμού
- πληροφορία για το μήκος του πλαισίου ώστε τα τερματικά που το διαβάζουν να θέτουν την τιμή στο NAV

• πληροφορία για το αν το πλαίσιο έχει αποσταλεί για πρώτη φορά ή για το αν πρόκειται για επανεκπομπή καθώς και ο αύξων αριθμός του πλαισίου για την αναγνώριση από τον παραλήπτη τυχόν διπλοτύπων. Το επόμενο πεδίο περιέχει την πληροφορία και το μήκος του μπορεί να είναι από 0 εώς 4095 bytes. Τέλος υπάρχει το πεδίο CRC (Cyclic Redundancy Check) που αποτελείται από 4 bytes. Στο πεδίο αυτό περιέχεται το αποτέλεσμα της εφαρμογής του πολυωνύμου CRC-32

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

στα πεδία MAC header και data. Το ίδιο γίνεται και στην πλευρά του δέκτη με σκοπό την ανίχνευση λαθών αν το αποτέλεσμα δεν είναι το ίδιο.

2.2.2 Πλαίσιο αίτησης αποστολής

Το πλαίσιο αίτησης αποστολής (Request To Send, RTS) έχει τη μορφή του σχήματος

Σχήμα 2.8
Πλαίσιο RTS

Το πλαίσιο RTS είναι το πρώτο από τα τέσσερα πλαίσια που ανταλλάσσονται κατά τη διαδικασία αποστολής RTS/CTS/data/ACK. Το πεδίο MAC header περιέχει τη διεύθυνση του αποστολέα και του παραλήπτη. Επίσης περιέχει τη διάρκεια του πακέτου data που θα επακολουθήσει έτσι ώστε τα τερματικά που το λαμβάνουν να ενημερώσουν το NAV τους. Το πεδίο CRC χρησιμοποιείται για ανίχνευση λαθών.

2.2.3 Πλαίσιο ελεύθερος προς αποστολή

Η μορφή του πλαισίου ελεύθερος προς αποστολή (Clear To Send, CTS) φαίνεται στο σχήμα

Σχήμα 2.9
Πλαίσιο CTS/ACK

Στο πεδίο MAC header υπαρχουν οι διευθύνσεις του πομπού και του δέκτη καθώς και η διάρκεια της συγκεκριμένης ανταλλαγής πακέτων της οποίας το πλαίσιο CTS είναι τμήμα. Έτσι ενημερώνουν το NAV τους τα τερματικά που δεν έλαβαν το πλαίσιο RTS. Το πλαίσιο CTS ακολουθεί μετά χρόνο SIFS από τη λήψη του RTS και αποτελεί απάντηση σε αυτό.

2.2.4 Πλαίσιο επιβεβαίωσης

Το πλαίσιο επιβεβαίωσης (ACK) έχει την ίδια μορφή με το πλαίσιο CTS όπως φαίνεται στο σχήμα 2.9. Στο MAC header περιέχονται οι διευθύνσεις του αποστολέα και του παραλήπτη καθώς και πληροφορία σχετικά με ποιο πακέτο data επιβεβαιώνει. Το πλαίσιο ACK ακολουθεί μετά χρόνο SIFS απο την επιτυχή λήψη του πλαισίου data. Ενημερώνει τον αποστολέα ότι δεν χρειάζεται επανεκπομπή του πλαισίου πληροφορίας.

2.2.5 Τεμαχισμός πλαισίων

Το επίπεδο MAC έχει τη δυνατότητα τεμαχισμού και επανασύνθεσης των πακέτων που φτάνουν από τα ανώτερα επίπεδα. Με το μηχανισμό αυτό κάθε τεμάχιο του αρχικού πακέτου μεταδίδεται αυτόνομα σύμφωνα με τις διαδικασίες που περιγράφηκαν. Για κάθε πακέτο που τεμαχίζεται τα κομμάτια πρέπει να έχουν όλα το ίδιο μήκος ,εκτός από το τελευταίο που μπορεί να είναι και μικρότερο. Το μήκος των πλαισίων στα οποία τεμαχίζεται ένα πακέτο δεν πρέπει να υπερβαίνει σε κάθε περίπτωση το κατώφλι τεμαχισμού (fragmentation threshold). Από τη στιγμή που ένα τμήμα του αρχικού πακέτου μεταδίδεται για πρώτη φορά, το περιεχόμενο και το μήκος του παραμένουν σταθερά μέχρι να παραδοθεί επιτυχώς στον προορισμό του. Όλα τα τερματικά πρέπει να έχουν τη δυνατότητα λήψης πλαισίων πληροφορίας διαφόρων μηκών. Όταν κάποιο τμήμα απαιτεί επανεκπομπή το μήκος και τα περιεχόμενά του παραμένουν σταθερά για το χρόνο ζωής του αρχικού πλαισίου στο συγκεκριμένο τερματικό. Δεν είναι επιτρεπτή η αλλαγή των παραπάνω στοιχείων με στόχο την παραμονή μέσα στα χρονικά όρια του πακέτου. Κάθε πλαίσιο περιέχει ένα πεδίο ελέγχου αλληλουχίας (Sequence Control field) το οποίο αποτελείται από έναν αύξοντα αριθμό και έναν αριθμό τεμαχίου. Όταν ένα τερματικό εκπέμπει ο αύξων αριθμός πρέπει να παραμείνει ο ίδιος για όλα τα κομμάτια του μεγαλύτερου πακέτου που μεταδίδονται. Τα πλαίσια – τεμάχια πρέπει να στέλνονται με σειρά από το χαμηλότερο αριθμό τεμαχίου προς το μεγαλύτερο, όπου οι αριθμοί τεμαχίου ξεκινούν από το μηδέν και αυξάνουν κατά ένα για κάθε διαδοχικό τεμάχιο. Επίσης το πεδίο ελέγχου πλαισίου περιέχει ένα bit που είναι ίσο με το μηδέν για να υποδηλώσει το τελευταίο (ή το μοναδικό) κομμάτι ενός μεγαλύτερου πακέτου.

Το τερματικό – αποστολέας πρέπει να διατηρεί ένα χρονομετρητή για κάθε πακέτο που πρόκειται να μεταδώσει. Για κάθε πακέτο υπάρχει ένας μέγιστος χρόνος στον οποίο πρέπει να μεταδοθεί. Αν ο χρονομετρητής ξεπεράσει αυτό το μέγιστο χρόνο τότε όλα τα εναπομείναντα κομμάτια του πακέτου απορρίπτονται και καμιά προσπάθεια δε γίνεται για να ολοκληρωθεί η μετάδοση.

2.2.6. Επανασύνθεση πλαισίων

Κάθε πλαίσιο – τεμάχιο περιέχει πληροφορίες που επιτρέπουν την επανασύνθεση του αρχικού πλαισίου από εκείνα που το συνιστούν. Κάθε πλαίσιο περιέχει τις ακόλουθες πληροφορίες που χρησιμοποιούνται από τον παραλήπτη για να ανασυντεθεί το αρχικό πλαίσιο.

- Είδος πλαισίου
- Διεύθυνση του αποστολέα
- Διευθυνση του παραλήπτη
- Πεδίο ελέγχου αλληλουχίας : Το πεδίο αυτό επιτρέπει στο τερματικό – παραλήπτη να ελέγχει ότι όλα τα εισερχόμενα πλαίσια – τεμάχια ανήκουν στο ίδιο πακέτο αλλά και να αναγνωρίζει τη σειρά με την οποία αυτά πρέπει να ανασυντεθούν. Ο αύξων αριθμός στο πεδίο ελέγχου αλληλουχίας παραμένει ο ίδιος για όλα τα κομμάτια του ίδιου πακέτου ενώ ο αριθμός τεμαχίου αυξάνει κατά ένα για τα διαδοχικά κομμάτια - Ενδείκτης άλλων τεμαχίων (More Fragments Indicator) : Δείχνει, αν είναι διάφορος του μηδενός, ότι το πλαίσιο που λαμβάνεται δεν είναι το τελευταίο ή το μοναδικό της σειράς. Ο παραλήπτης πρέπει να ανακατασκευάσει το αρχικό πακέτο συνδυάζοντας όλα τα κομμάτια σύμφωνα με τον αριθμό τεμαχίου που το καθένα έχει στο πεδίο ελέγχου αλληλουχίας. Όσο δεν έχει ληφθεί το πλαίσιο με μηδενισμένο το bit του ενδείκτη άλλων τεμαχίων ο παραλήπτης γνωρίζει ότι η λήψη του πακέτου δεν έχει ολοκληρωθεί. Από τη στιγμή που το συγκεκριμένο πλαίσιο θα ληφθεί ο παραλήπτης ξέρει ότι δεν πρόκειται να λάβει άλλα κομμάτια από το συγκεκριμένο πακέτο. Όλα τα τερματικά πρέπει να υποστηρίζουν την ταυτόχρονη λήψη τουλάχιστων τριών πακέτων. Για κάθε πακέτο το τερματικό πρέπει να διατηρεί ένα χρονομετρητή λήψης. Ο παραλήπτης πρέπει να απορρίπτει όλα τα πλαίσια – τεμάχια για τα οποία δεν υπάρχει χρονομετρητής. Υπάρχει και ένας χαρακτηριστικός χρόνος, ο μέγιστος χρόνος λήψης ενός πακέτου (Max Receive Lifetime), που καθορίζει το μέγιστο χρόνο στον οποίο πρέπει να ολοκληρωθεί η λήψη του πακέτου. Ο χρονομετρητής αρχίζει ναμετρά από τη στιγμή που έρχεται το πρώτο κομμάτι του πακέτου. Αν ο χρονεμετρητής ξεπεράσει το μέγιστο χρόνο λήψης τότε όσα πλαίσια ληφθούν από το

διάστημα αυτό και πλέον απορρίπτονται. Ωστόσο και γι' αυτά τα πλαίσια πρέπει να σταλεί επιβεβαίωση. Για να επανασυντεθεί σωστά ένα πακέτο στο σταθμό προορισμού πρέπει να απορρίπτονται όλα τα διπλότυπα με τη διαδικασία που αναφέρθηκε σε προηγούμενη παράγραφο. Ακόμα όμως και για τα πλαίσια που λαμβάνονται για δεύτερη φορά πρέπει να σταλεί επιβεβαίωση ACK.

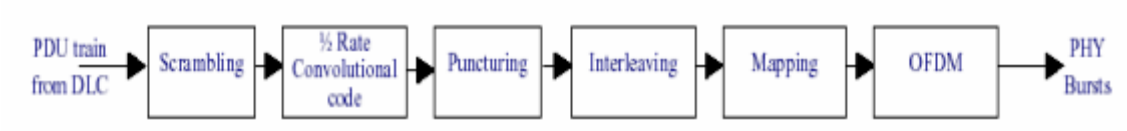
2.3. Το φυσικό επίπεδο

Στο φυσικό επίπεδο το 802.11a χρησιμοποιεί την τεχνική Ορθογωνικής Πολυπλεξίας στη Συχνότητα (OFDM). Το σύστημα εκπέμπει στην ISM μπάντα της περιοχής των 5GHz. Σ'αυτή την περιοχή έχει οριστεί ένας αριθμός από κανάλια μέσα στα οποία μπορεί να εκπέμπει το σύστημα. Καθένα από αυτά είναι 20MHz. Κάθε κανάλι διαιρείται σε 52 υπο-φέροντα 0.3125MHz το καθένα. Από αυτά τα 48 χρησιμοποιούνται για μεταφορά δεδομένων. Κάθε υποφέρον διαλέγεται να είναι ορθογώνιος παλμός. Αυτό έχει το πλεονέκτημα η μορφοποίηση του παλμού να γίνεται αποτελεσματικά με τη χρήση Αντίστροφου Γρήγορου Μετασχηματισμού Fourier (Inverse Fast Fourier Transformation, IFFT). Έτσι αντί για ένα φέρον 20MHz κάνουμε χρήση πολλών υποφερόντων που επικαλύπτονται με την αρχή της ορθογωνιότητας. Εκεί δηλαδή που ένα υποφέρον έχει μέγιστη τιμή τα άλλα έχουν μηδέν. Με τον τρόπο αυτό έχει αποδειχτεί ότι αντιμετωπίζονται καλύτερα οι επιλεκτικές στη συχνότητα διαλείψεις καθώς και η ενδοσυμβολική παρεμβολή σε κανάλια με διαλείψεις ευρείας ζώνης. Οι ειδικές παράμετροι της τεχνικής OFDM στο πρότυπο 802.11a φαίνονται στον πίνακα που ακολουθεί.

Παράμετρος	Τιμή
Ρυθμός δειγματοληψίας (f_s)	20 MHz
Διάρκεια συμβόλου (T_{total})	4μsec
Αριθμός υποφερόντων για δεδομένα (N_D)	48
Μέγεθος FFT	64
Εύρος υποφέροντος	0.3125MHz
Εύρος καναλιού	20MHz

Πίνακας 2.1
Παράμετροι OFDM

Τα δεδομένα προς μετάδοση έρχονται από το ανώτερο επίπεδο με τη μορφή συρμών από bytes. Ο συρμός εισάγεται σε έναν scrambler ο οποίος εμποδίζει την ύπαρξη μεγάλων σειρών από 0 και 1. Τα scrambled δεδομένα αποτελούν είσοδο στον συνελικτικό κωδικοποιητή. Ο κωδικοποιητής αποτελείται από ένα κύριο συνελικτικό κώδικα με ρυθμό ½ και στη συνέχεια εφαρμόζεται puncturing. Οι μορφές puncturing διευκολύνουν τη χρήση ρυθμών ½, ¾, και 2/3. Τα κωδικοποιημένα δεδομένα αναδιατάσσονται με σκοπό την αποφυγή της εισόδου ριπών από λάθη στον συνελικτικό αποκωδικοποιητή στο δέκτη. Στη συνέχεια τα αναδιατεταγμένα δεδομένα τοποθετούνται στα σύμβολα με χρήση διαφόρων ειδών κωδικοποιήσεων BPSK, QPSK, 16-QAM, 64-QAM. Η διαμόρφωση OFDM εφαρμόζεται με τη χρήση αντίστροφου FFT. Ως αποτέλεσμα μεταδίδονται 48 σύμβολα δεδομένων και 4 σύμβολα πιλότοι.



Σχήμα. Διαδικασία εκπομπής συμβόλου OFDM

Για την αντιμετώπιση της ενδοσυμβολικής παρεμβολής εφαρμόζεται ένα διάστημα προστασίας με τη μορφή της κυκλικής επέκτασης του συμβόλου. Έτσι πριν από κάθε σύμβολο OFDM προηγείται μια περιοδική επέκταση του ίδιου του συμβόλου. Η συνολική διάρκεια του OFDM συμβόλου είναι

$$Ttotal = Tg + T$$

όπου Tg είναι το διάστημα προστασίας και T η χρήσιμη διάρκεια του συμβόλου. Στον OFDM δέκτη ακολουθείται η ακριβώς αντίστροφη διαδικασία. Δύο σύμβολα στην αρχή της μετάδοσης βοηθούν στον συγχρονισμό πομπού και δέκτη. Η αποκωδικοποίηση του συνελικτικού κώδικα γίνεται με τη βοήθεια ενός αποκωδικοποιητή Viterbi. Με αυτή τη διαδικασία πετυχαίνονται διαφορετικές ταχύτητες μετάδοσης δεδομένων όπως φαίνεται στον παρακάτω πίνακα

Ρυθμός	Κωδικο-ποίηση	Ρυθμός Κώδικα	Ονομαστικός ρυθμός bit (Mb/s)	Αριθμός bits ανά υποφέρον	Αριθμός bits ανά OFDM σύμβολο	Αριθμός bits δεδομένων ανά OFDM σύμβολο
1	BPSK	½	6	1	48	24
2	BPSK	¾	9	1	48	36
3	QPSK	½	12	2	96	48
4	QPSK	¾	18	2	96	72
5	16-QAM	½	24	4	192	96
6	16-QAM	¾	36	4	192	144
7	64-QAM	¾	54	6	288	216
8	64-QAM	2/3	48	6	288	192

Πίνακας 2.2
Παράμετροι εξαρτώμενοι από το ρυθμό

ΚΕΦΑΛΑΙΟ 3ο
IEEE 802.11b

3.1 Η ασύρματη Πραγματικότητα

Κάνοντας μια έρευνα αγοράς στην αγορά πληροφορικής, κάποιος θα παρατηρούσε την μεγάλη αφθονία σε προϊόντα που υλοποιούν πρωτόκολλα, τα οποία υπόσχονται ασύρματες, εύκολες και κυρίως γρήγορες λύσεις για τις δικτυακές μας ανάγκες. Την τελευταία δεκαετία πολλά είναι τα πρότυπα που διεκδικούν ένα κομμάτι της αγοράς. Bluetooth, HiperLAN, HomeRF, 802.11a, 802.11b, 802.11g
είναι κάποια από τα πολυδιαφημιζόμενα ονόματα προτύπων, αλλά και να μην ξεχνάμε το PACKET radio που έρχεται αρκετά χρόνια πριν. Στις παρακάτω παραγράφους θα περιγράψουμε το πιο διαδεδομένο μέλος της οικογένειας 802.11, το πρότυπο b. Αναλύοντας τα χαρακτηριστικά του, θα γίνει φανερό γιατί το wifi είναι

από τα ελάχιστα success stories μιας αγοράς τηλεπικοινωνιών που χαρακτηρίζεται από γενική ύφεση.

3.2 Το πρότυπο IEEE802.11b

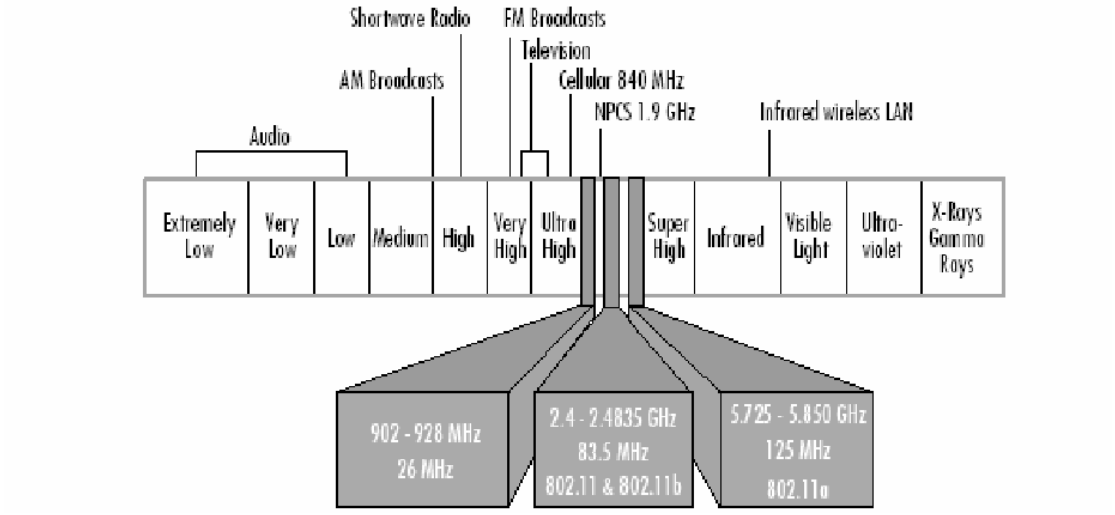
Το IEEE 802.11 b χρησιμοποιεί τη συμπληρωματική διαμόρφωση κώδικα (CCK) για την επίτευξη μεγαλύτερου ρυθμού δεδομένων στη συχνότητα 2.4 GHz, ο οποίος φτάνει τα 11 Mbps. Η περιοχή κάλυψης αυτής της προδιαγραφής φτάνει τα 38m. Ένα σοβαρό πρόβλημα για τις συσκευές που χρησιμοποιούν το 802.11 b είναι οι παρεμβολές από τη λειτουργία άλλων συσκευών που λειτουργούν στην ίδια συχνότητα, όπως συσκευές bluetooth, φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα.

3.3 Κύρια χαρακτηριστικά του πρωτοκόλλου

Το 802.11b είναι το πρώτο wireless πρωτόκολλο που κατάφερε να μπει τόσο δυναμικά στον χώρο της δικτύωσης, έναν χώρο που γνωρίζει ελάχιστες επαναστάσεις και αλλαγές. Το πρωτόκολλο 802.11, του οποίου το b αποτελεί επέκταση, και είναι ένας ορισμός του Media Access Control (MAC) Layer καθώς και τριών διαφορετικών και ασύμβατων Physical Layers στο υπάρχον δικτυακό μοντέλο OSI. Το πρωτόκολλο εγκρίθηκε από την ομάδα 802 της IEEE στις 26 Ιουνίου του 1997 και θέτει το πλαίσιο για μια προτυποποιημένη ασύρματη δικτυακή επικοινωνία ευρείας ζώνης. Στις παρακάτω σελίδες δίνουμε μια περιγραφή του 802.11 πρωτοκόλλου, και επεκτείνουμε την έρευνά μας στις επεκτάσεις και τροποποιήσεις που προσέθεσε το 802.11b.

3.4 Φάσμα εκπομπής

Για την μετάδοση των δεδομένων το πρωτόκολλο χρησιμοποιεί την μπάντα των 2.4GHz. Για να αποφεύγονται παρεμβολές από ραδιοφωνικά σήματα στις ΗΠΑ, η Federal Communications Commission (FCC) είναι υπεύθυνη για την εκχώρηση μικρών περιοχών στο φάσμα των ραδιοσυχνοτήτων. Η χρήση οποιασδήποτε από της ζώνες που ορίζει η FCC, πρέπει να συνοδεύεται από ειδική άδεια. Η FCC παράλληλα χαρακτηρίζει ελεύθερα κάποια τμήματα του ραδιοφωνικού φάσματος. Αυτές οι μπάντες ονομάζονται ISM(Industrial Scientific and Medical) και μπορούν να χρησιμοποιηθούν χωρίς άδεια. Στο σχήμα μπορούμε να δούμε αναλυτικά το ραδιοφωνικό φάσμα και τις ελεύθερες περιοχές του.



Εικόνα. ελεύθερες συχνότητες

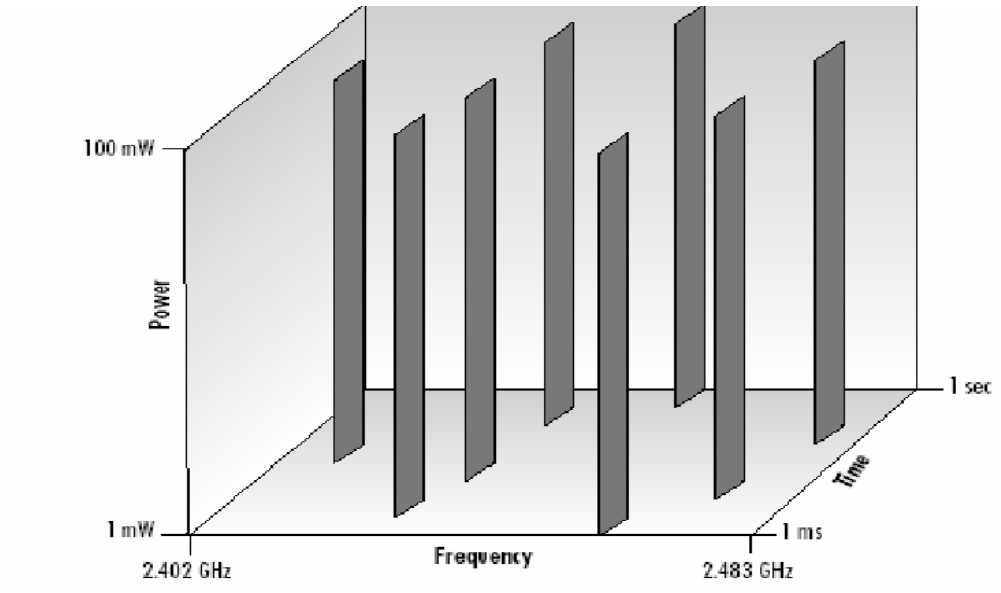
Το 802.11(b) χρησιμοποιεί όπως βλέπουμε μια ελεύθερη ζώνη η οποία είναι πλήρως ελεύθερη για εκπομπή χαμηλής ισχύος. Όλα τα παραπάνω βέβαια, ισχύουν στις ΗΠΑ. Ευτυχώς και οι υπόλοιπες παρόμοιας ευθύνης οργανώσεις κάθε χώρας συμβαδίζουν, λιγότερο η περισσότερο με αυτά τα

πρότυπα της FCC. Δυστυχώς, το νομικό πλαίσιο που διέπει τις λεπτομέρειες χρήσης αυτής της μπάντας, εξαρτάται σε μεγάλο βαθμό από την νομοθεσία κάθε χώρας. Μεγάλα είναι τα νομικά κενά σε πολλές χώρες, όπως και στην Ελλάδα, που αφήνουν πολλά ερωτηματικά ως προς την μέγιστη νόμιμη εκπεμπόμενη ισχύ, την εμπορική ή όχι χρήση του ραδιοφωνικού φάσματος αυτού και πολλά άλλα. Η ισχύς που ορίζει το στάνταρτ στις εξόδους κεραίας των εμπορικών συσκευών είναι τα 0.2mw, το οποίο με τις μικρές εργοστασιακές κεραίες που συνοδεύουν τις συσκευές WiFi, δίνει στο 802.11b εμβέλεια της τάξεως των 300μ σε ανοιχτό χώρο.

Λόγω της φύσης των μικροκομματικών συχνοτήτων, η εμβέλεια συσκευών WiFi μειώνεται αισθητά όταν μεταξύ τους παρεμβάλλονται τοίχοι, δέντρα(και γενικώς αντικείμενα που περιέχουν νερό) ή μεταλλικές πόρτες. Μείωση της ποιότητας σύνδεσης, σημαίνει αρχικά μειωμένο throughput του δικτύου με υψηλά error rates, και στην χειρότερη περίπτωση αδυναμία σύνδεσης των συσκευών. Για τον ίδιο λόγο, μακρινές συνδέσεις (>300μ) επιτυγχάνονται μόνο σε καταστάσεις όπου η μία συσκευή έχει οπτική επαφή με την άλλη (Line of Site), ένας κανόνας που ευτυχώς δεν είναι τόσο αυστηρός(καταστάσεις near-LOS). Αντανακλάσεις του σήματος μπορεί να επιτρέψουν σύνδεση χωρίς LOS. Βεβαίως, όπως είναι αναμενόμενο, για την επίτευξη ζεύξεων πολύ μεγάλων αποστάσεων, υπάρχει το φυσικό εμπόδιο της καμπυλότητας της γης. Ακόμη και αν καταφέρουμε δηλαδή να ενισχύσουμε την εκπομπή και την λήψη των 802.11 συσκευών μας, προσπαθώντας να καταστήσουμε δυνατή μια σύνδεση μμεγάλης απόστασης, δεν είναι δυνατό να ξεπεράσουμε την δεδομένη μέγιστη απόσταση (~20μίλια), στην οποία η ίδια η γη εμποδίζει την οπτική επαφή.

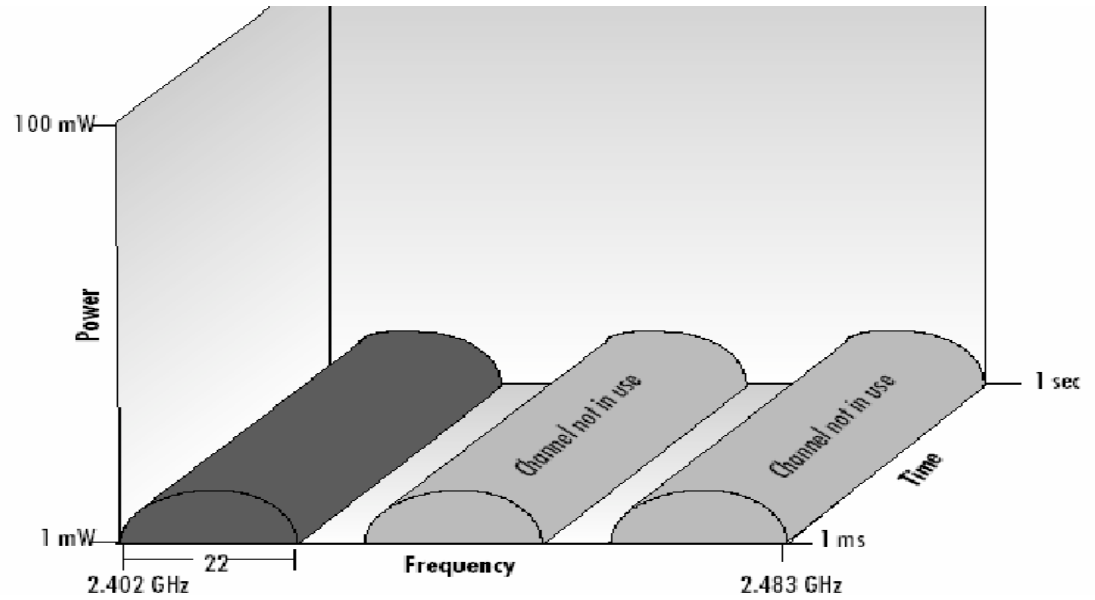
3.5 Διαμόρφωση

Στο αρχικό πρωτόκολλο 802.11, καθορίζονται δύο τρόποι κωδικοποίησης, ο FHSS (Frequency Hopping Spread Spectrum) και ο DSSS (Direct Sequence Spread Spectrum). Στον FHSS, η εκπομπή-λήψη μμοιράζεται σε 75 κανάλια του ενός MHz και εναλλάσσεται συνεχώς σε ένα από αυτά. Χρησιμοποιώντας αυτή την τεχνική, ο πομπός στέλνει τα δεδομένα διαδοχικά σε μια ακολουθία από φαινομενικά τυχαίες συχνότητες(frequency hopping). Ο δέκτης ακολουθεί την ίδια ακολουθία εναλλαγής καναλιών συχνότητας με τον πομπό και λαμβάνει το μήνυμα. Το μήνυμα μπορεί να ληφθεί ακέραιο, μόνο όταν είναι γνωστή η ακολουθία της εναλλαγής συχνοτήτων. Καθώς μόνον ο δέκτης γνωρίζει την σωστή ακολουθία, το μήνυμα είναι αναγνώσιμο μόνο από τον πραγματικό του παραλήπτη. Με αυτή την τεχνική, ηλεκτρομαγνητικές παρεμβολές στον χώρο της λήψης θα επηρεάσουν μόνο ένα τμήμα του μηνύματος, έχοντας ως αποτέλεσμα την ανάγκη για επανεκπομπή μόνο μικρού όγκου μηνυμάτων. Ο συγκεκριμένος τρόπος κωδικοποίησης μπορεί να δώσει ταχύτητες μεταφοράς δεδομένων έως και 2mbit. Ακολουθεί γράφημα που δείχνει την τεχνική FHSS συναρτήσει της ισχύος και του χρόνου.



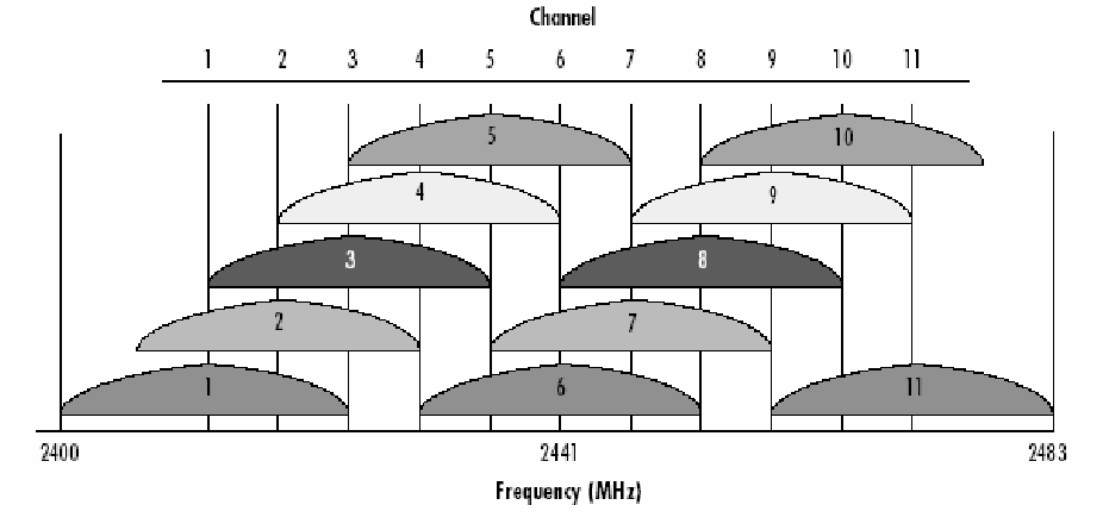
FSSS συναρτήσει ισχύος και χρόνου

Στον DSSS το φάσμα χωρίζεται σε 14 μερικώς (ανά ~4) επικαλυπτόμενα κανάλια πλάτους 22MHz, και χρησιμοποιείται ένα κάθε φορά για επικοινωνία.



DSSS συναρτήσει ισχύος και χρόνου

Ένας πομπός direct sequence επικοινωνεί προσθέτοντας bits εφεδρείας που καλούνται chips, στα δεδομένα. Σε κάθε bit πληροφορίας προστίθενται τουλάχιστον 10 chips. Κατόπιν τα τμήματα των δεδομένων στέλνονται σε όσες περισσότερες συχνότητες είναι δυνατόν, εντός του καναλιού λειτουργίας, ταυτόχρονα. Η μέγιστη ταχύτητα φτάνει σε αυτόν τον τρόπο τα 11mbit. Στο ακόλουθο σχήμα βλέπουμε την κατανομή των καναλιών στο φάσμα των 2.4GHz, καθώς και τον τρόπο με τον οποίο επικαλύπτονται.

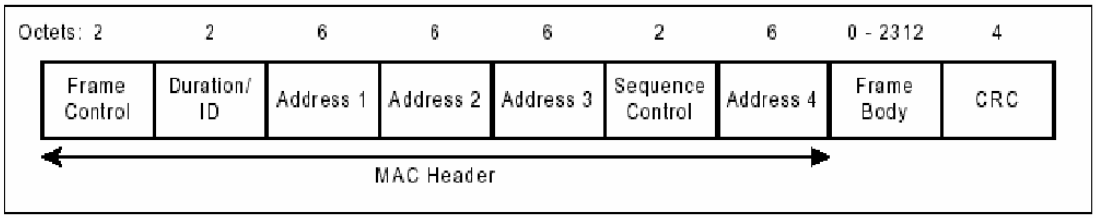


BSSS κανάλια

Τελικά με την έλευση του 802.11b το Σεπτέμβρη του 1999, η επιτροπή αποφάσισε να αφήσει στο πρότυπο μόνο την κωδικοποίηση DSSS, παρόλο που το FHSS αρχικά φαίνονταν σαν ευκολότερο αλλά και φθηνότερο στην υλοποίηση του. Με αυτό τον τρόπο το 802.11b απέκτησε ένα από τα μεγαλύτερά του πλεονεκτήματα, την υψηλή μεταγωγή δεδομένων.

3.6 Εύρος Ζώνης

Η ταχύτητα σύνδεσης που ορίζει το IEEE802.11b είναι τα 11mbps, και όπως εξηγήσαμε επιβάλλεται από την κωδικοποίηση BSSS που χρησιμοποιεί. Μιας και από την φύση τους οι ασύρματες συνδέσεις είναι επιρρεπής σε σφάλματα μετάδοσης, το overhead μετάδοσης πακέτων ελέγχου και διόρθωσης λαθών, μεταφράζεται σε πραγματική ταχύτητα μεταφοράς δεδομένων πολύ χαμηλότερη της ονομαστικής. Επίσης, λόγω του γεγονότος ότι όλες οι συσκευές WiFi έχουν ένα και μόνο ραδιοφωνικό πομποδέκτη, η λειτουργία τους σαν δικτυακές συσκευές είναι σε half-duplex mode, καθώς ο πομποδέκτης μπορεί να ακούει το δίκτυο ή να στέλνει σε αυτό, αλλά όχι και τα δύο ταυτόχρονα. Έτσι το πραγματικό όριο για το bandwidth μιας 802.11b σύνδεσης είναι διαμορφώνεται στα 5mbps. Πολλές εταιρίες υπόσχονται ονομαστικές διπλάσιες ή και περισσότερο ταχύτητες. Τέτοια χαρακτηριστικά είναι εκτός του στάνταρ, και λειτουργούν **μόνο** μεταξύ των προϊόντων της ίδιας εταιρίας. Από την στιγμή που επιτευχθεί σύνδεση με μια άλλη συσκευή WiFi, τότε ισχύουν όλοι οι κανόνες ενός κοινού Ethernet δικτύου.



Περιγραφή MAC επιπέδου

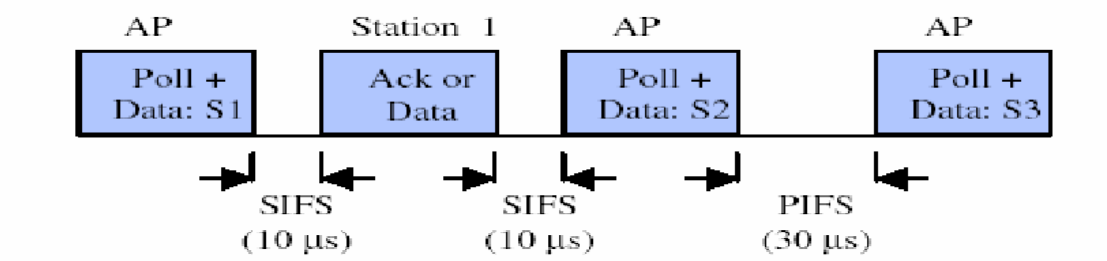
3.7 Μέθοδος πρόσβασης στο μέσο (Access Method)

Η μέθοδος που υποστηρίζεται από το 802.11 πρωτόκολλο για την πρόσβαση στο φυσικό μέσο, είναι το PCF (Point Coordination Function) και DCF (Distributed Coordination Function) με Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) σε αναλογία με το Ethernet που υλοποιεί το CSMA/CD(Collision Detection). Το CSMA στο Ethernet λειτουργεί ως ακολούθως: όταν κάποιος επιθυμεί να στείλει δεδομένα, ελέγχει αν το κανάλι είναι κατειλημμένο από μια άλλη μεταφορά δεδομένων. Αν είναι, τότε περιμένει ένα τυχαίο χρονικό περιθώριο(μικρό) σύμφωνα με τον αλγόριθμο exponential random backoff. Ο τρόπος πρόσβασης αυτός δεν μπορεί να είναι αποδοτικός στο 802.11 για δύο λόγους: 1. Η υλοποίηση αυτής της μεθόδου θα απαιτούσε ραδιοφωνικούς πομπούς που θα είχαν την δυνατότητα Full – Duplex επικοινωνίας (αποστολή και λήψη ταυτόχρονα), κάτι το οποίο θα αύξανε το κόστος. 2. Σε ένα ασύρματο περιβάλλον δεν μπορούμε με ασφάλεια να υποθέσουμε ότι όλοι οι σταθμοί θα μπορούν να ακούν ο ένας τον άλλον. Ένας σταθμός που ελέγχει το μέσο και το βρίσκει ελεύθερο, δεν σημαίνει και ότι είναι ελεύθερο στην περιοχή του λήπτη.

Ας δούμε όμως πιο αναλυτικά από τι απαρτίζεται ο μηχανισμός. Το 802.11 ορίζει πέντε διαφορετικά χρονικά διαστήματα για συγχρονισμό στο MAC επίπεδο, το short interframe space (SIPS), το slot time, το priority interframe space (PIFS), το distributed interframe space (DIFS), και το extended interframe space (EIFS).Τα δύο από αυτά θεωρούνται βασικά και καθορίζονται από το MAC: το χρονικό διάστημα SIPS(short interframe space) και το slot time. Τα υπόλοιπα διαστήματα καθορίζονται βάσει των παραπάνω διαστημάτων. Το SIPS είναι το μικρότερο όλων των χρονικών αυτών διαστημάτων, ακολουθούμενο από το slot time, το οποίο μπορεί να ερμηνευθεί σαν η μονάδα χρόνου για το MAC του 802.11, παρόλο που το πρωτόκολλο δεν βασίζεται σε αρχιτεκτονική με χρονικές «θυρίδες» (time slots). Ειδικά στο 802.11b, οι χρόνοι SIFS και slot είναι 20μs, χρόνος που επιλέχθηκε έτσι ώστε να δώσει ένα λογικό σε διάρκεια διάστημα για τις καθυστερήσεις διάδοσης και επεξεργασίας από τις συσκευές. Ο χρόνος PIFS ισούται με τον χρόνο SIFS επαυξημένο κατά ένα slot και ο DIFS κατά δύο slots. Ο χρόνος EIFS είναι μεγαλύτερος και από τους τέσσερις προηγούμενους, και χρησιμοποιείται για την επανεκπομπή πακέτων που ελήφθησαν λανθασμένα.

Το 802.11 υποστηρίζει δύο τρόπους λειτουργίας: τον PCF και τον DCF. Με την πρώτη μέθοδο λειτουργίας, το κεντρικό AP της κυψέλης(θα μιλήσουμε παρακάτω για αυτό) στέλνει μηνύματα στους σταθμούς πελάτες, κάνοντας Polling σε κάθε ένα από αυτούς, ρωτώντας στην ουσία

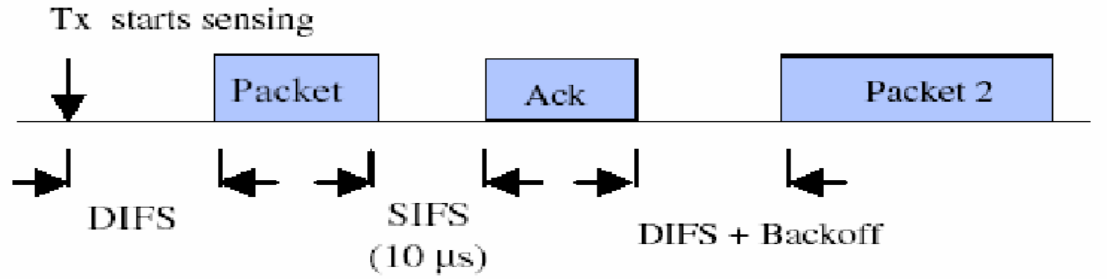
για το αν έχει δεδομένα για αποστολή ή όχι. Αν ο σταθμός απαντήσει, μπορεί να στείλει την θετική του απάντηση (ACK) στο ίδιο πακέτο με τα δεδομένα προς αποστολή. Αν δεν απαντήσει εντός του χρονικού ορίου SIFS, τότε το Access Point προχωρά στον επόμενο σταθμό.



Μέθοδος PCF στο 802.11b MAC

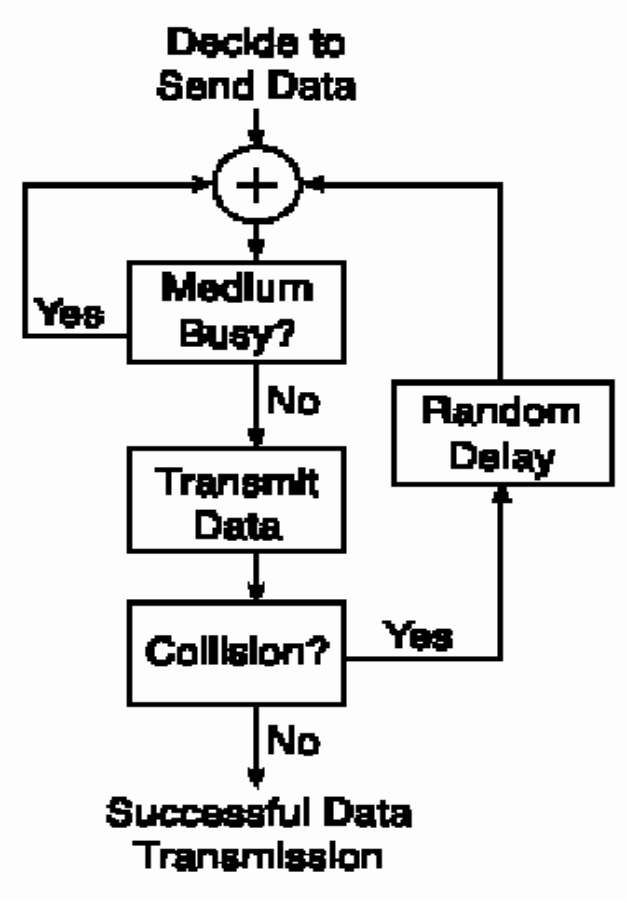
Είναι σημαντικό να δώσουμε έμφαση στο γεγονός ότι οι απαιτήσεις χρονισμού SIFS και PIFS είναι πολύ αυστηρά ορισμένες από την επιτροπή προτυποποίησης 802.11b. Για την ακρίβεια, ένα ACK πακέτο, η απάντηση δηλαδή στην ερώτηση poll ενός σταθμού, πρέπει να φτάσει στο Access Point εντός του χρόνου SIFS, που είναι 10μs. Σε ένα ασύρματο δίκτυο που εκτείνεται σε μια ευρύτερη περιοχή (>1,5χλμ), ο round trip(χρόνος για να λάβει χώρα μια αίτηση-απάντηση) χρόνος ενός σήματος είναι 15μs. Είναι δηλαδή ολοφάνερο ότι το ACK πακέτο θα εκπεμφθεί κανονικά από τον σταθμό πελάτη, αλλά δεν θα διαβαστεί ποτέ από το Access Point λόγω έλλειψης σωστού χρονισμού. Έτσι η μέθοδος PCF δεν χρησιμοποιείται στις περισσότερες υλοποιήσεις του 802.11b, καθώς περιορίζει εμμέσως αλλά αυστηρώς την εμβέλεια ενός ασύρματου δικτύου.

Στην μέθοδο λειτουργίας DCF, το 802.11 χρησιμοποιεί έναν μηχανισμό Αποφυγής Συγκρούσεων μαζί με αναγνώριση βεβαίωσης λήψης των πακέτων που στέλνονται. Αν ο πομπός, κατά την έναρξη διαδικασία αποστολής, δει ότι το μέσο είναι ελεύθερο (κανείς δεν χρησιμοποιεί το κανάλι) για χρόνο ίσο με DIFS, τότε αρχίζει την εκπομπή. Σε αντίθετη περίπτωση, συνεχίζει να ελέγχει το κανάλι για να δει αν βρίσκεται σε κατάσταση busy ή idle. Εφόσον βρει το κανάλι ελεύθερο για χρόνο DIFS, τότε ξεκινά να μετράει τον χρόνο χρήσης του καναλιού σε μονάδες slot time, παράγει τυχαία χρονικά διαστήματα αναμονής σε μονάδες slot time, σύμφωνα με κατάλληλο αλγόριθμο, και συνεχίζει τον έλεγχο της κατάστασης του καναλιού. Κατά το τελευταίο βήμα, για κάθε time slot που ο πομπός βρίσκει ελεύθερο το κανάλι, ο τυχαίος χρόνος αναμονής μειώνεται κατά ένα time slot. Όταν ο χρόνος αυτός μηδενιστεί, τότε και μόνο ο πομπός μπορεί να εκκινήσει την διαδικασία μετάδοσης. Με αυτή τη μέθοδο αποφεύγονται οι συγκρούσεις πακέτων διαφορετικών εκπομπών, αλλά και αποκλείεται η μονοπώληση του καναλιού από έναν και μόνο σταθμό που θα ίσως να προσπαθούσε συνεχείς εκπομπές.



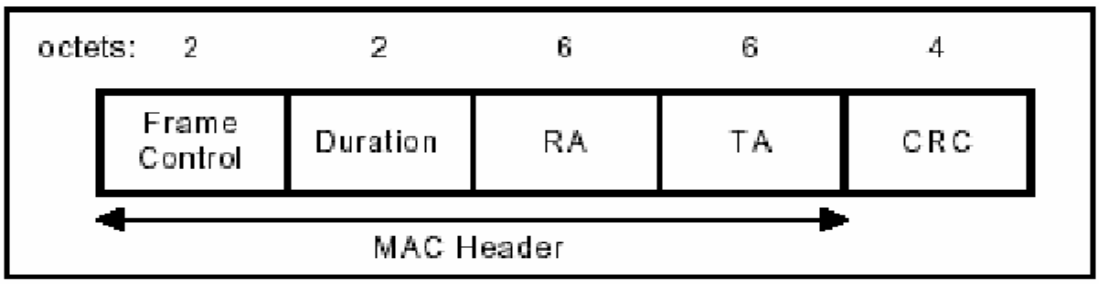
Εικόνα 7 – Μέθοδος DCF στο 802.11b MA

Ο δέκτης θα ελέγξει την «υπογραφή» CRC του πακέτου που πήρε, και αν την βρει έγκυρη, τότε στέλνει ένα πακέτο ACK στον αποστολέα. Αν ο αρχικός αποστολέας δεν πάρει ACK πακέτο, τότε συνεχίζει να εκπέμπει την πληροφορία ως που να λάβει ένα ACK ή να σταματήσει να προσπαθεί και να απορρίψει το αρχικό πακέτο.

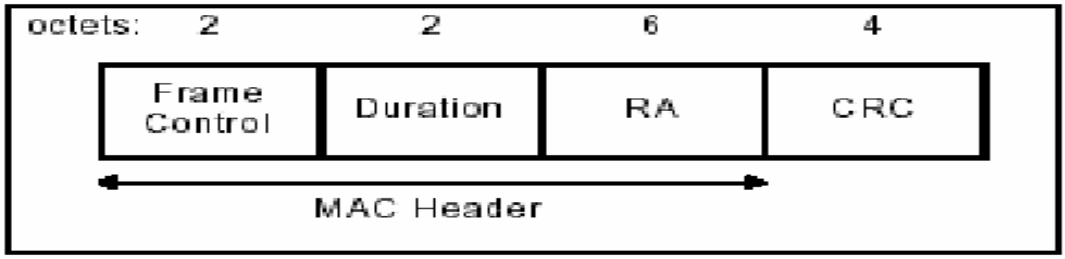


Εικόνα 8 – απλουστευμένος αλγόριθμος εκπομπής

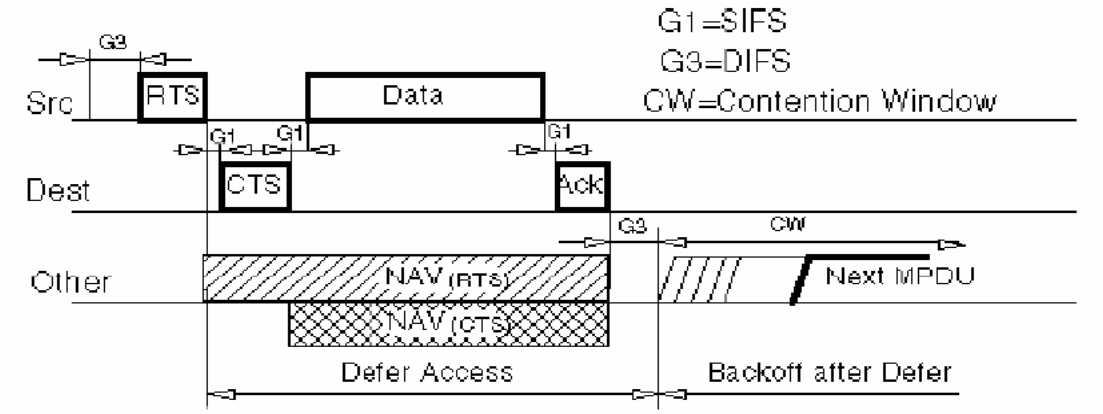
Η επιτροπή IEEE εισήγαγε έναν μηχανισμός Virtual Carrier Sense στο 802.11 για να αμβλύνει το φαινόμενο κατά το δύο σταθμοί δεν μπορούν να ακούσουν ο ένας
τον άλλον και προκαλούνται συγκρούσεις. Ο μηχανισμός λέγεται CTS/RTS(clear to send/request to send). Όταν ενεργοποιείται, κάθε client πριν ξεκινήσει την αποστολή δεδομένων, στέλνει ένα ειδικό πακέτο με πληροφορίες που έχουν σχέση με το χρόνο που θα πάρει η εκπομπή του. Αν το κανάλι είναι ελεύθερο, το AP στέλνει σαν απάντηση ένα πακέτο CTS. Ο client ξεκινά την εκπομπή του, αλλά και όλοι οι υπόλοιποι clients ακούν το CTS και αναβάλλουν τις δικές τους εκπομπές. Όλοι οι σταθμοί που ακούσουν το RTS και/ή το CTS, θέτουν το δείκτη Virtual Carrier Sense(που ονομάζεται NAV) για τον χρόνο που αναγράφει το πακέτο RTS, και χρησιμοποιούν την πληροφορία αυτή για να αποκτήσουν πρόσβαση στο μέσο.
Μάλιστα, τα πακέτα RTS στέλνονται από client/AP, ανάλογα με κάποιο κατώφλι(RTS threshold). Αν το πακέτο που θα εκπεμφθεί, έχει μέγεθος μεγαλύτερο του κατωφλίου σε KB, τότε πριν το πακέτο αυτό, αποστέλλεται ένα RTS. Βλέπε τις παρακάτω εικόνες για την ακριβή μορφή των πακέτων RTS/CTS, αλλά και για την χρονική ακολουθία της διαδικασίας αποστολής ενός πακέτου δεδομένων.



Εικόνα 9 - Το πλαίσιο RTS



Εικόνα 10 – Το πλαίσιο CTS



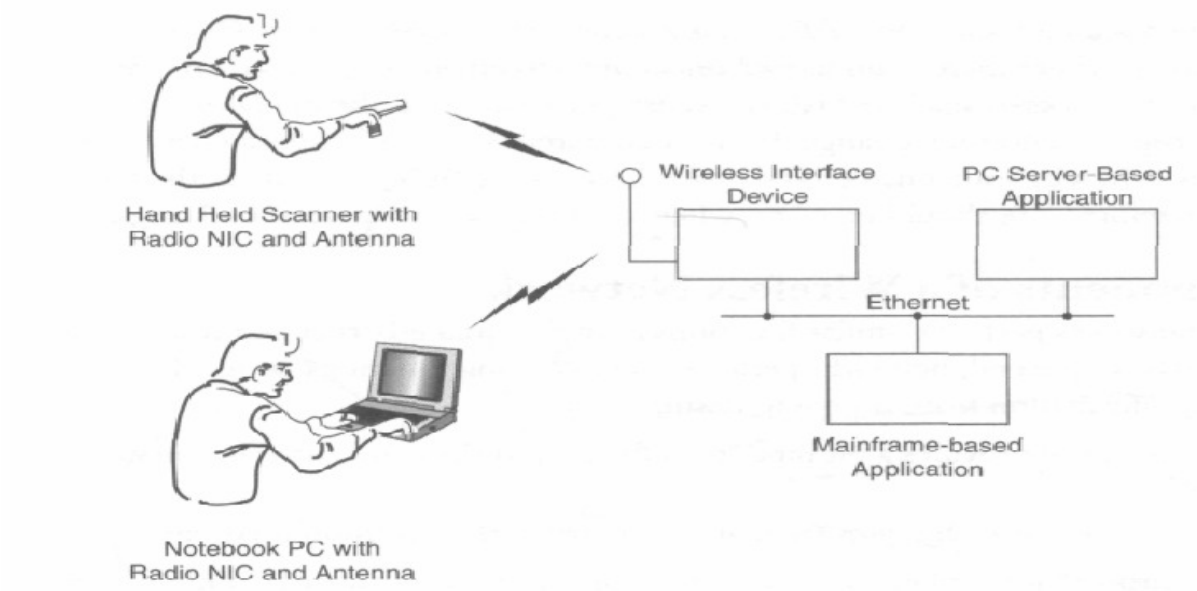
Εικόνα 11 – Η διαδικασία αποστολής των RTS-CTS

3.8.1 Τα συστατικά ενός ασύρματου δικτύου

Τα ασύρματα δίκτυα εκτελούν παρόμοιες λειτουργίες με τα ενσύρματα δίκτυα όπως το ethernet και το token ring. Γενικά, τα δίκτυα εκτελούν τις ακόλουθες λειτουργίες για να επιτρέψουν τη μεταφορά των πληροφοριών από την πηγή στον προορισμό:

1. Το μέσο παρέχει ένα δίαυλο διαβίβασης στοιχείων.
2. Οι μέσες τεχνικές πρόσβασης διευκολύνουν τη διανομή ενός κοινού μέσου.
3. Τα δεδομένα παραμένουν αναλλοίωτα.
4. Οι μηχανισμοί δρομολόγησης επιτρέπουν τη μετάδοση των δεδομένων από την πηγή δημιουργίας προς τον αποδέκτη
5. Το λογισμικό συνδετικότητας διασυνδέει μια συσκευή, όπως ο light pen ανιχνευτής κώδικα υπολογιστών ή φραγμών, στα προγράμματα εφαρμογών που φιλοξενούνται σε έναν κεντρικό υπολογιστή.

Ένας καλός τρόπος να απεικονιστούν αυτές οι λειτουργίες είναι να διευκρινιστεί η δικτυακή αρχιτεκτονική. Αυτή η αρχιτεκτονική περιγράφει τα πρωτόκολλα, το σημαντικό υλικό, και τα στοιχεία λογισμικού που αποτελούν το δίκτυο. Μια δικτυακή αρχιτεκτονική, είτε ασύρματη είτε ενσύρματη, μπορεί να αντιμετωπισθεί με δύο τρόπους, φυσικά και λογικά.



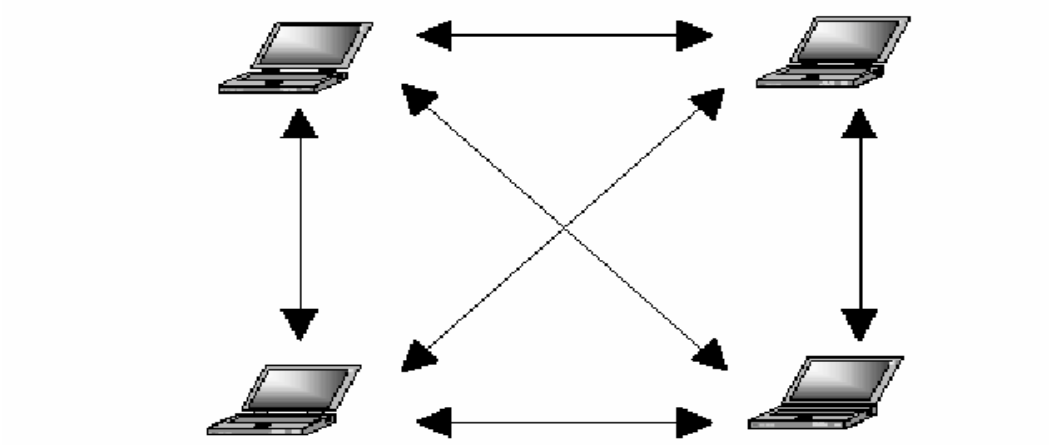
Τα συστατικά ενός ασύρματου δικτύου επεκτείνουν τις δυνατότητες του ενσύρματου.

3.8.2 Φυσική αρχιτεκτονική ενός ασύρματου δικτύου

Τα φυσικά συστατικά ενός ασύρματου δικτύου εφαρμόζουν τη φυσική, σύνδεση στοιχείων, και τις λειτουργίες στρώματος δικτύων για να ικανοποιήσουν τη λειτουργία που απαιτείται μέσα στις τοπικές, μητροπολιτικές, και ευρείες περιοχές. Τα εξής τμήματα εξηγούν τα διάφορα συστατικά του ασύρματου τοπικού LAN.

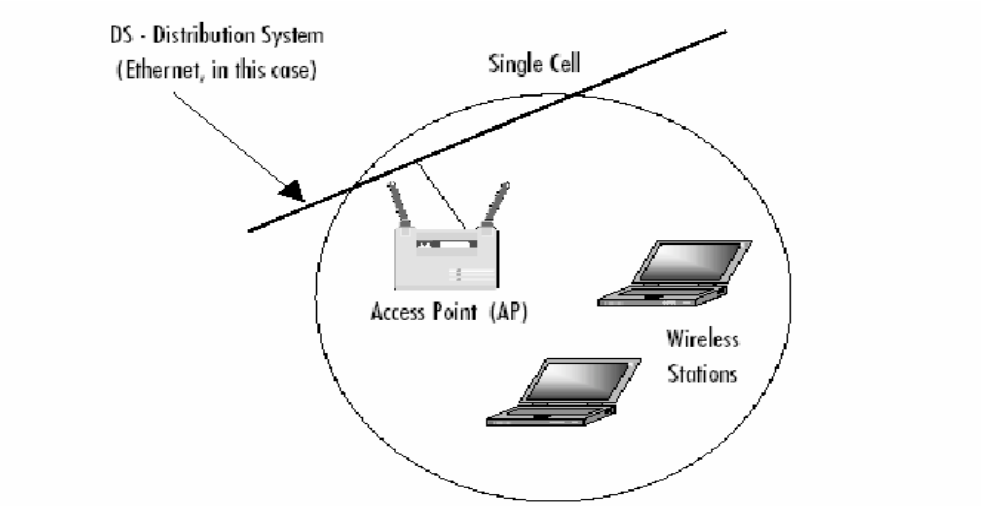
3.9 Τοπολογία ενός Wireless δικτύου

Το πρότυπο του wifi ορίζει τρεις τρόπους επικοινωνίας μεταξύ κόμβων ενός δικτύου, τον IBSS (Independent Basic Service Set) ή ad hoc ,τον BSS (Basic Service Set) ή infrastructure και τον ESS(Extended Service Set). Με τον πρώτο τρόπο, 2 η περισσότερες συσκευές επικοινωνούν άμεσα η μία με την άλλη. Κάθε κόμβος θεωρείται ομότιμος(peer) και έτσι το δίκτυο απαρτίζεται από μονοπάτια. Συνήθως αυτός ο τρόπος χρησιμοποιείται για μικρά δίκτυα. Έχει παρόλαυτα μεγάλο ερευνητικό ενδιαφέρον, καθώς ένα ad hoc δίκτυο μπορεί να περιέχει πολλά μονοπάτια για επικοινωνία μεταξύ δύο κόμβων, και έτσι παρέχει μεγάλη αξιοπιστία λόγω εφεδρείας μονοπατιών, αλλά και αυξημένη ταχύτητα.



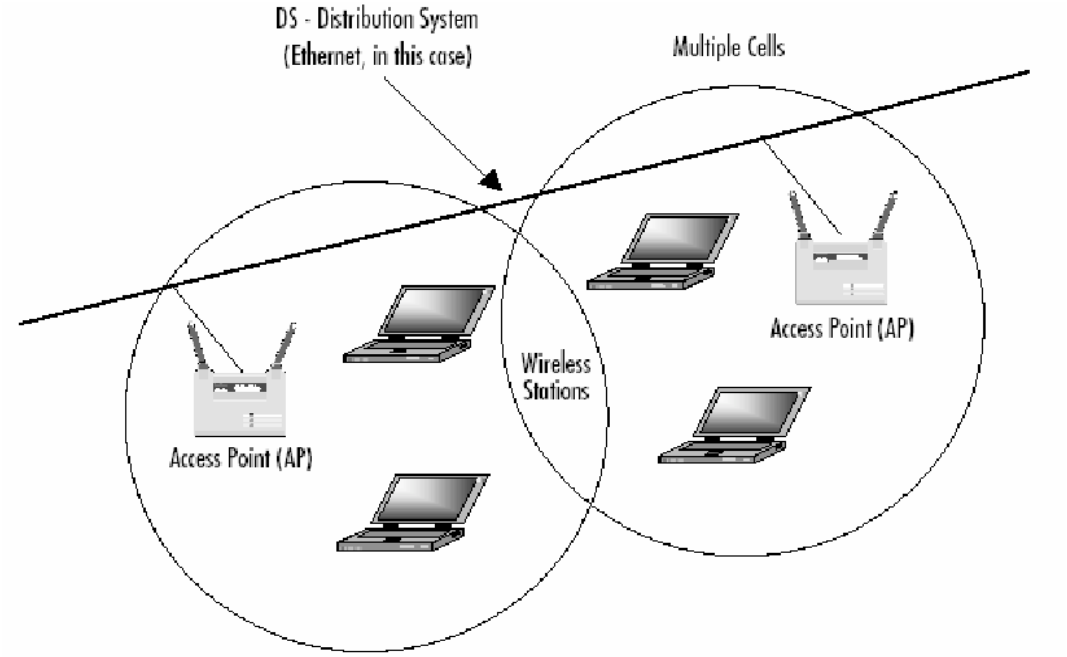
Εικόνα 12 - IBSS

Στην δεύτερη τοπολογία, το 802.11 δίκτυο αποτελεί ένα κυψελωτό δίκτυο, παρόμοιο των δικτύων κινητής τηλεφωνίας. Η κυψέλη στην ορολογία του 802.11 ονομάζεται Basic Service Set (BSS). Όλα μέλη του επικοινωνούν μεταξύ τους μέσω ενός κεντρικού διανομέα που ονομάζεται Base Station ή κοινώς Access Point, κατά το μοντέλο client – server. Σε αυτή την περίπτωση δεν χρειάζεται η άμεση οπτική επαφή ανάμεσα σε όλους τους κόμβους. Αρκεί όλοι να μπορούν να επικοινωνήσουν με το Access Point. Κάθε Access Point, έχει ένα όνομα που το αναγνωρίζει ανάμεσα σε άλλα που ίσως να βρίσκονται στον ίδιο χώρο, το SSID. Το SSID είναι πολλές φορές και αυτό που πρέπει να ξέρουμε, για να συνδεθούμε σε κάποιο ελεύθερο Access Point. Επίσης, κάθε Access Point εκπέμπει σε ένα από τα 14 κανάλια(λιγότερα ίσως σε κάποιες χώρες) εκπομπής που ορίζει το πρωτόκολλο. Για την μείωση των παρεμβολών μεταξύ των APs, είναι προτιμότερο να επιλέγονται κανάλια λειτουργίας που διαφέρουν κατά 4(ας πούμε τα 1-5-9-13 για τέσσερα APs στον ίδιο χώρο) έτσι ώστε να μην επικαλύπτονται οι εκπομπές τους. Ένα Access Point χρησιμοποιεί πολυκατευθυντική κεραία (Omnidirectional), καθώς πρόκειται για κεραίες που εκπέμπουν κυκλικά το σήμα τους, πράγμα που είναι και το ζητούμενο όταν θέλουμε να έχουμε την μέγιστη κάλυψη του περιβάλλοντος χώρου. Εν αντιθέσει, οι σταθμοί μπορούν να χρησιμοποιούν κατευθυντικές κεραίες για να επιτύχουν συνδέσεις με μακρινά(>300m) APs, κάτι βέβαια που εισάγει νέα προβλήματα στο δίκτυο. Για λειτουργία εντός της αποστάσεως των 300μ, είναι καλό να χρησιμοποιούνται πολυκατευθυντικές κεραίες πολύ μικρού κέρδους (<5dBi), καθώς επαρκούν για την επίτευξη σύνδεσης.



Εικόνα 13 – BSS

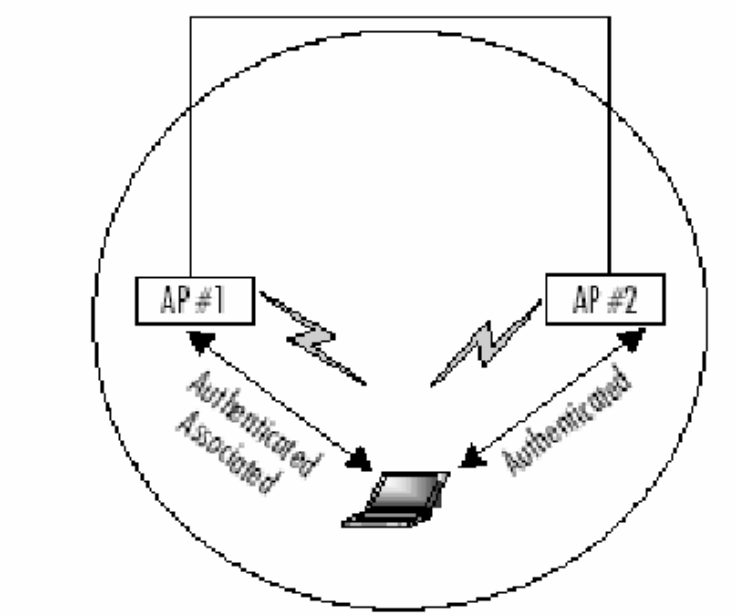
Ένα ασύρματο δίκτυο μπορεί να έχει την μορφή μίας και μόνο κυψέλης, όμως πολλές κυψέλες μπορούν να γεφυρωθούν μέσω ενός Συστήματος Διανομής (Distribution System). Το σύστημα διανομής μπορεί να είναι μια ενσύρματη εγκατάσταση, ή δεσμευμένοι ασύρματοι clients που αναλαμβάνουν την γεφύρωση των δύο υπό-δικτύων. Όλο το διασυνδεδεμένο δίκτυο, συμπεριλαμβανομένου του συστήματος διανομής και των Access Points, είναι ορατό στα ανώτερα επίπεδα του OSI μοντέλου σαν ένα μοναδικό 802 δίκτυο, το οποίο στο στάνταρτ περιγράφεται σαν Extended Service Set.



Εικόνα 14 – Τοπολογία Infrastructure

Ας μιλήσουμε όμως λίγο περισσότερο για τις υπηρεσίες που προσφέρει το ESS, καθώς δίνει στα δίκτυα 802.11 ένα τεράστιο πλεονέκτημα: το roaming χρηστών ανά τα διαθέσιμα Access Points. Ένας σταθμός ενός BSS, μπορεί να κινείται ελεύθερα αλλάζοντας BSSs(δηλαδή Access Points) χωρίς ούτε αυτός, ούτε και το δίκτυο να βλέπουν κάποια αλλαγή, ή να χρειάζονται νέες ρυθμίσεις. Κάθε BSS επικοινωνεί με τα υπόλοιπα BSSs για την διαμεταγωγή των πακέτων, αλλά και για την εναλλαγή των σταθμών, καθώς αυτοί αλλάζουν BSS, μέσω του Συστήματος Διανομής που περιγράψαμε ποιο πάνω. Την ευθύνη για αυτές τις λειτουργίες έχουν εννέα υπηρεσίες που προσφέρει το σχήμα ESS. Τέσσερις από αυτές ανήκουν στην ομάδα των υπηρεσιών σταθμού (station services) και οι υπόλοιπες ανήκουν στην ομάδα υπηρεσιών διανομής(distribution services). Οι υπηρεσίες σταθμού απαρτίζονται από τις authentication, de authentication, data delivery, και privacy, και παρέχουν στο ασύρματο δίκτυο λειτουργικότητα παρόμοια με αυτή ενός στάνταρ ενσύρματου δικτύου 802.3. Η πρώτη υπηρεσία παρέχει ένα είδος ταυτότητας σε κάθε σταθμό. Χωρίς αυτήν, ο σταθμός δεν έχει το δικαίωμα να συνδεθεί στο WLAN. Ένας σταθμός έχει την δυνατότητα να πιστοποιήσει την ύπαρξή του σε περισσότερα από ένα Access Points. Αυτού του είδους η προ-πιστοποίηση, παρέχει την δυνατότητα στα κοντινά του συγκεκριμένου σταθμού BSSs, να είναι έτοιμα για να δεχθούν το σταθμό αυτό καθώς αυτός θα κινηθεί στον χώρο του. Η υπηρεσία του de-authentication χρησιμοποιείται για να καταστραφεί η ταυτότητα ενός σταθμού που για οποιοδήποτε λόγο δεν μπορεί πλέον να υπάρχει στο τοπικό ασύρματο δίκτυο. Όταν η διαδικασία αυτή ξεκινήσει, ο σταθμός δεν μπορεί πλέον να έχει πρόσβαση στο δίκτυο, μέχρι να ξαναπεράσει από την φάση authentication. Με αυτό τον τρόπο ελευθερώνονται πόροι στο Access Point για άλλες συσκευές. Η υπηρεσία privacy χρησιμοποιεί έναν RC4 αλγόριθμο για να παρέχει κρυπτογράφηση στα δεδομένα που εκπέμπονται. Περισσότερα για αυτήν την υπηρεσία στο αντίστοιχο κεφάλαιο. Το data delivery στο επίπεδο του MAC,
περιγράφεται πιο κάτω. Πέντε διαδικασίες διανομής αναλαμβάνουν την αποστολή των δεδομένων καθώς
ένας ασύρματος σταθμός κινείται μεταξύ πολλαπλών BSSs : association, reassociation, disassociation, integration, και distribution. Ένας σταθμός χρησιμοποιεί την διαδικασία association μόλις συνδεθεί στο AP. Αυτή η λειτουργία δημιουργεί τα λογικά μονοπάτια για μεταξύ των συσκευών, και αποφασίζει για τον τρόπο με τον οποίο θα επικοινωνήσει το Σύστημα Διανομής με τον σταθμό. Αν δεν συμβεί αυτή η διαδικασία, τότε το ΣΔ δεν θα ξέρει που να στείλει τα πλαίσια

δεδομένων. Όπως βλέπουμε στο σχήμα, ένας σταθμός μπορεί να είναι authenticated σε περισσότερα από ένα Access Point αλλά associated μόνο με ένα.



Εικόνα 13 – Authentication/Association

Η λειτουργία disassociation χρησιμοποιείται για να σταματήσει την «συνεργασία» ενός σταθμού και ενός BSS, λόγω του είτε αυτός σταμάτησε την λειτουργία του, ή κινήθηκε προς κάποιο άλλο BSS. Η λειτουργία distribution χρησιμοποιείται από τα APs για να αποφασίσει τον στόχο των πακέτων που εκπέμπονται, δηλαδή αν είναι για κάποια άλλη ασύρματη συσκευή ή προορίζονται για το ΣΔ. Τέλος, η υπηρεσία intergration είναι αυτή που «μεταφράζει» τα πακέτα που προέρχονται από ασύρματους σταθμούς (802.11b πακέτα) σε πακέτα για το ενσύρματο ΣΔ(πακέτα 802.3), αλλά και το αντίθετο.

Κάθε Access Point, πολυπλέκει στο χρόνο τις αιτήσεις από κάθε client και εξυπηρετεί το υποδίκτυο του. Καθώς το μέσο μετάδοσης είναι μοναδικό, όσους περισσότερους ταυτόχρονους clients έχουμε σε ένα AP, τόσο πέφτει και η απόδοση του δικτύου. Θεωρητικά η πτώση της απόδοσης είναι αντιστρόφως ανάλογη του αριθμού των μελών του δικτύου. Δυστυχώς λόγω πολλών άλλων παραγόντων(βλέπε κεφάλαιο Hidden Node), υπό συγκεκριμένες συνθήκες η μείωση της απόδοσης είναι δραματική.

Ένα ασύρματο δίκτυο είναι πιθανότητα ένα δίκτυο με μεγάλους ρυθμούς λαθών. Για τέτοιες περιπτώσεις που τα λάθη μετάδοσης είναι πραγματικότητα και όχι πιθανότητα, όπως εγκαταστάσεις με υψηλές παρεμβολές RF ή πολύ μακρινές ζεύξεις, υπάρχει η παράμετρος του *fragme ntation* που βοηθά στην εξομάλυνση του φαινομένου. Ο διαχειριστής του AP μπορεί να θέσει το πόσο μικρό ή μεγάλο θα είναι το μέγεθος των πακέτων που εκπέμπονται. Μικρότερα πακέτα έχουν μεγαλύτερη πιθανότητα να φτάσουν ανέπαφα στον προορισμό τους από μεγαλύτερα. Με αυτόν τον τρόπο μπορεί ο διαχειριστής να μειώσει το error rate του δικτύου, με το κόστος βεβαίως της μειωμένης απόδοσης, καθώς μεταδίδοντας πολλά μικρά πακέτα, έχουμε μετάδοση περισσότερου overhead και όχι χρήσιμης πληροφορίας.

3.10 Πρότυπα συμβατότητας και πιστοποίηση προτύπου WiFi

Το εμπόριο έχει κατακλυστεί πλέον από προϊόντα εταιριών που υλοποιούν με κάποιο τρόπο κάποιο μέρος του πρωτοκόλλου 802.11b(Access Points, clients, routers, VoIP terminals, cameras κτλ). Την λύση στην ερώτηση «τι εγγύηση έχει ο καταναλωτής για την συμβατότητα λειτουργίας όλων των 802.11b συσκευών;» έρχεται να δώσει η WECA(Wireless Ethernet Compatibility Alliance). Πρόκειται για μια οργάνωση που εξετάζει και πιστοποιεί την συμβατότητα των 802.11

συσκευών. Πρόκειται για μια πολύ σημαντική πρωτοβουλία, καθώς ένα wireless δίκτυο μπορεί να αποτελείται από συσκευές διαφορετικών εταιριών. Μια πιστοποιημένη από την weca συσκευή, έχει την εγγύηση ότι θα μπορεί να συνεργαστεί με άλλο ασύρματο ή όχι υλικό, που υποδεικνύεται από το πρωτόκολλο 802.11b για τον συγκεκριμένο τύπο συσκευής(π.χ. ένα Access Point πρέπει να μπορεί να συνδεθεί με οποιονδήποτε client, αλλά και να μπορεί να δεχτεί και μια Ethernet σύνδεση). Η WECA έχει θεσπίσει το Wireless Fidelity πρότυπο, και σε κάθε συσκευή που περνάει επιτυχώς όλες τις δοκιμές συμβατότητας, απονέμεται η «σφραγίδα συμβατότητας».

Εικόνα 14 – WiFi trademark

Αυτή η σφραγίδα δίνει στους καταναλωτές την εγγύηση ότι, τα προϊόντα που την φέρουν, θα μπορούν να λειτουργούν μεταξύ τους. Παρόλα αυτά, το wifi δεν είναι ένα τεχνολογικό στάνταρ. Είναι απλά μια εγγύηση συμβατότητας μεταξύ προϊόντων. Βεβαίως τα πράγματα ποτέ δεν είναι τόσο απλά. Πολλές φορές ερχόμαστε
αντιμέτωποι με προϊόντα που είτε απλά δεν μπορούν να συνεργαστούν, είτε η συνεργασία τους αυτή είναι προβληματική. Τέτοια προβλήματα τις περισσότερες φορές βρίσκονται στο υλικό των συσκευών, οπότε είναι απίθανο να λυθούν. Έτσι η προσωπική δοκιμή των προϊόντων πριν την αγορά, ή η έρευνα για παραδείγματα
αποδεδειγμένης συνεργασίας ενδείκνυται πριν από μια σοβαρή επένδυση σε υλικό διαφορετικών κατασκευαστών.

3.11 Εφαρμογές Wifi δικτύων στο σπίτι, το γραφείο, την βιομηχανία

Τα πολλά πλεονεκτήματα του 802.11 το καθιστούν ιδανικό για εγκατάσταση είτε σαν ένα αυτόνομο δίκτυο, είτε σαν ένα δίκτυο που επεκτείνει τις δυνατότητες μιας ενσύρματης δικτυακής εγκατάστασης. Το χαμηλό κόστος των συσκευών και η χαμηλή τους κατανάλωση, δύο σχεδιαστικοί στόχοι της ομάδας 802.11, κάνουν ιδανική την χρήση του στην βιομηχανία. Συχνά μια βιομηχανία χρειάζεται την συνεχή παρακολούθηση ενός συνόλου από συσκευές που ελέγχουν την εύρυθμη λειτουργία της εγκατάστασης και
επικοινωνούν με έναν κεντρικό υπολογιστή που συλλέγει τις πληροφορίες. Ένα peer to peer (ομότιμο) δίκτυο από wifi-enabled αισθητήριων συσκευών (sensors) μπορεί να εγκατασταθεί για την παρακολούθηση συγκεκριμένων εργασιών. Ένα τέτοιο δίκτυο, μπορεί εύκολα να γίνει «έξυπνο». Οι συσκευές αυτές μπορούν να βρίσκουν εναλλακτικές διαδρομές για να επικοινωνούν με τον κεντρικό εξυπηρετητή, δίνοντας 100% uptime στο σύστημα. Μπορούν λόγω της υψηλής διαμεταγωγής του πρωτοκόλλου να διακινούν μεγάλους όγκους δεδομένων, και σε πραγματικό χρόνο, πράγμα που εγγυάται την παρακολούθηση του συστήματος σε πραγματικό χρόνο. Βέβαια η ασύρματη επικοινωνία είναι από μόνη της το μεγαλύτερο πλεονέκτημα της
τεχνολογίας, καθώς δεν χρειάζονται άλλες καλωδιώσεις στον ήδη επιβαρημένο χώρο της εγκατάστασης. Στο γραφείο, το wifi γίνεται συνώνυμο της ευελιξίας. Οι εργαζόμενοι μπορούν ελεύθερα να κινούνται με φορητούς υπολογιστές στους εργασιακούς τους χώρους, χωρίς να χάνουν ούτε λεπτό την σύνδεσή τους στο εταιρικό δίκτυο και το διαδίκτυο. Με αυτό τον τρόπο αυξάνεται η παραγωγικότητά τους καθώς μπορούν να συνεργάζονται ευκολότερα και να έχουν συνεχή πρόσβαση σε κρίσιμες πληροφορίες.

Πολλά τοπικά δίκτυα σε κάθε κτίριο μπορούν εύκολα να συνενωθούν με Links μεγάλων αποστάσεων, αποδοτικά και κυρίως οικονομικά. Δεν πρέπει βεβαίως να ξεχνάμε τους κινδύνους

ασφάλειας που παρουσιάζονται, κινδύνους που θα αναλύσουμε στην αντίστοιχη παράγραφο. Στο σπίτι, μια wifi enabled συσκευή, μπορεί να δώσει την δυνατότητα για περιήγηση στο διαδίκτυο, παρακολούθηση video, εσωτερική βιντεοδιάσκεψη, σε οποιοδήποτε σημείο του σπιτιού. Φυσικά το στήσιμο ενός τοπικού δικτύου μπορεί να γίνει χωρίς τον βραχνά των καλωδίων, hubs και λοιπών δικτυακών συσκευών, που δύσκολα χωρούν σε ένα σπίτι. Όλη ή υποδομή αντικαθιστάται από μόνο ένα ή περισσότερα κεντρικά Access Points.

ΚΕΦΑΛΑΙΟ 4ο

Προβλήματα

4.1 Ασφάλεια δικτύων 802.11b

Όσο οι συσκευές wifi εισέβαλλαν σε όλο και περισσότερα δίκτυα, τόσο οι χρήστες τους έβλεπαν πιο σοβαρά το ζήτημα της ασφάλειας των δεδομένων που διακινούσαν μέσω αυτών. Αναρίθμητες μελέτες, τόσο από κοινούς χρήστες, όσο και από την επιστημονική κοινότητα, βοήθησαν στο να ξεσκεπαστούν πολλές θεμελιώδεις ατέλειες στο μοντέλο ασφάλειας του πρωτοκόλλου. Θα προσπαθήσουμε να δώσουμε μια γενική εικόνα της όλης κατάστασης, προτείνοντας τελικά κάποιες λύσεις. Η επιτροπή IEEE, για λόγους ασφάλειας και πιστοποίησης (authentication) χρηστών, όρισε το WEP(wired equivalent prinvacy), με σκοπό την ενθυλάκωση των πακέτων των δεδομένων για την επίτευξη ασφάλειας παρόμοιας με ένα ενσύρματο δίκτυο. Η υλοποίηση του WEP σε εμπορικές συσκευές άργησε να υποστηριχτεί από όλους τους κατασκευαστές. Μια γρήγορη λύση για την υποκατάστασή του, ήταν η πιστοποίηση χρηστών μέσω λιστών επιτρεπόμενων MAC διευθύνσεων. Η MAC διεύθυνση είναι ένας μοναδικός δεκαεξαδικός αριθμός, που είναι «γραμμένος» στο υλικό κάθε δικτυακής συσκευής. Το Access Point κρατούσε μια λίστα με όλες τις διευθύνσεις MAC που ο διαχειριστής του δικτύου επέτρεπε να συνδεθούν. Αν η MAC μιας client συσκευής δεν ανήκε στη λίστα, αυτή η συσκευή δεν θα μπορούσε να συνδεθεί στο Access Point. Αυτή είναι μια πολύ αδύναμη μέθοδος πιστοποίησης στοιχείων των σταθμών πελατών. Κάποιος εκτός λίστας, με αρκετά δικαιώματα σε ένα unix like λειτουργικό σύστημα, μπορεί με διάφορους τρόπους να αλλάξει την MAC διεύθυνση που παρουσιάζει στο δίκτυο, έτσι ώστε να μπορέσει να χρησιμοποιήσει μια MAC που να είναι αποδεκτή από το AP. Τέτοιες επιθέσεις ονομάζονται mac spoofing attacks. Χρησιμοποιώντας εξειδικευμένο «ανιχνευτικό» λογισμικό (network sniffer), που πολλές φορές είναι δωρεάν, μπορεί με μια απλή WiFi κάρτα και ένα λάπτοπ να φτιάξει μια λίστα με τις MAC διευθύνσεις που βλέπει ότι συνδέονται επιτυχώς στο Access Point-στόχο. Έτσι, αλλάζοντας την MAC διεύθυνσή του σε οποιαδήποτε από αυτές, έχει την δυνατότητα να συνδεθεί επιτυχώς στο δίκτυο, χωρίς κανείς να μπορεί να καταλάβει την διαφορά. Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Δυστυχώς, ο σχεδιασμός του προτύπου, συνέπεσε χρονικά με την φρενίτιδα της κυβέρνησης των ΗΠΑ κατά της δημόσιας χρήσης συστημάτων ισχυρής κρυπτογράφησης, που σημαίνει μεγάλο μήκος κλειδιού. Έτσι το μήκος κλειδιού που υποστηρίζει το WEP, περιορίστηκε στα 40 ψηφία. Επιπλέον, ένα τέτοιο μήκος κλειδιού θα καθιστούσε το WEP ευκολότερο να υλοποιηθεί, καθώς η κατασκευή των MAC πλαισίων από το τότε υλικό ήταν ήδη μια διαδικασία που απαιτούσε μεγάλη υπολογιστική ισχύ, πόσο μάλλον η ενθυλάκωση τους με WEP. Η εισαγωγή μιας δυνατής κρυπτογράφησης θα επιβάρυνε ακόμη περισσότερο τις επιδόσεις των συσκευών. Καθώς όλοι είχαν πλέον καταλάβει ποσό τρωτό είναι ένα ανοιχτό δίκτυο, βιάστηκαν να υιοθετήσουν το πρότυπο αυτό. Δύο επιστημονικές εργασίες όμως, από ομάδες του πανεπιστημίου του Berkeley και του Maryland, έμελλαν να ταράξουν τα νερά για το πρότυπο, και να καταστήσουν εμφανή τα τρωτά του σημεία. Η εργασία της ομάδας του Berkeley καταδεικνύει τις αδυναμίες του προτύπου λόγω της συνεχούς επαναχρησιμοποίησης κλειδιών, ενώ η εργασία του Maryland θίγει της αδυναμίες στους μηχανισμούς πρόσβασης, ακόμη και αυτούς που λειτουργούν με βάση το WEP. Άλλες εργασίες που ακολούθησαν πρότειναν τρόπους για την τοποθέτηση πλαστών πακέτων στην κίνηση του δικτύου,

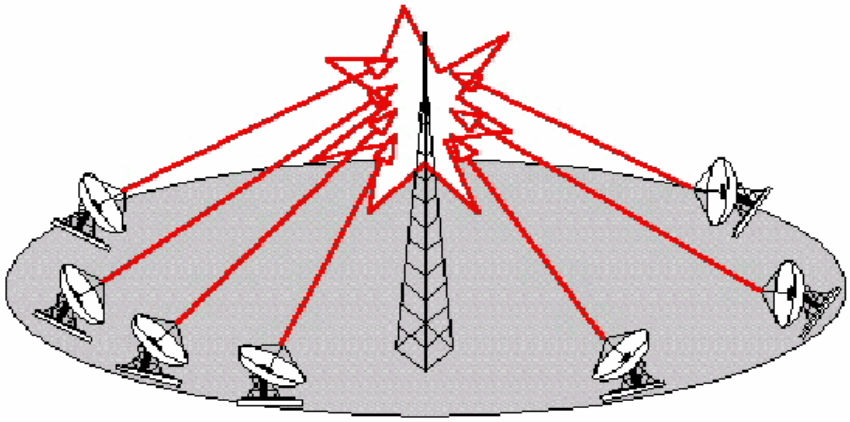
με αποκορύφωμα το άρθρο ενός μέλους της ομάδας 802.11 που μιλούσε για το WEP σαν «ανασφαλές για οποιοδήποτε μήκος κλειδιού» («WEP:unsafe at any key length»). Όλες οι προηγούμενες εργασίες βασίζονταν σε σχεδιαστικές ατέλειες του προτύπου για να προτείνουν την ύπαρξη κενών ασφάλειας. Ο ίδιος ο αλγόριθμος κρυπτογράφησης(RC4 της RCA), παρόλαυτα, θεωρούνταν επαρκής και δεν είχε δεχθεί αμφισβήτηση. Τότε οι Scott Fluhrer, Itsik Mantin, και Adi Shamir, ανακάλυψαν ένα ελάττωμα του αλγόριθμου χρονοδρομολόγησης κλειδιών που καθιστούσε κάποια κλειδιά «αδύναμα». Ένας εισβολέας, θα μπορούσε να βρει το μυστικό κλειδί WEP, απλά συλλέγοντας αρκετά αδύναμα κλειδιά. Δεν δημοσίευσαν ωστόσο κάποια υλοποίηση των ευρημάτων τους. Δυστυχώς ή ευτυχώς, ακολούθησαν πολλοί που το έκαναν. Πάμπολλα προγράμματα ανοιχτού λογισμικού, όπως το AirSnort έχουν την δυνατότητα να σπάσουν την κρυπτογράφηση WEP σε δευτερόλεπτα, δεδομένης μιας συλλογής αδύναμων κλειδιών του δικτύου – στόχος. Η πραγματικότητα είναι ακόμη πιο οδυνηρή. Πολλές έρευνες σε περιοχές με μεγάλη πυκνότητα wifi δικτύων έχουν δείξει ότι μόνο ένα πολύ μικρό ποσοστό Access Points που ανιχνεύτηκαν, έχουν πράγματι το WEP ενεργοποιημένο. Το μεγαλύτερο ποσοστό των εταιρικών δικτύων, είναι ορθάνοιχτο σε «επισκέπτες». Μάλιστα η μη νόμιμη πρόσβαση σε ασύρματα δίκτυα είναι τόσο εκτεταμένη, που υπάρχουν web sites στα οποία συγκεντρώνονται οι συντεταγμένες ανοιχτών εταιρικών δικτύων. Τέτοιες ομάδες χρηστών χρησιμοποιούν προγράμματα όπως το netstumbler για να ανακαλύπτουν όλα τα ασύρματα δίκτυα εντός της εμβέλειας της κεραίας του φορητού τους υπολογιστή, αλλά και να βλέπουν χρήσιμες πληροφορίες όπως το SSID του Access Point, αν έχει ενεργοποιημένο το WEP, αλλά και την ποιότητα της εκπομπής της κεραίας – στόχου. Μια βόλτα με αυτοκίνητο στους εμπορικούς δρόμους της Νέας Υόρκης, έχοντας ένα φορητό υπολογιστή, μια φτηνή wifi κάρτα και μια ακόμα φθηνότερη κεραία, μπορεί να αποδείξει την ύπαρξη τρυπών στα περισσότερα ασύρματα εταιρικά δίκτυα. Πολλοί έχουν αναγάγει την δραστηριότητα αυτή σε «σπορ», ονόματι wardriving, επωφελούμενοι κυρίως από την δωρεάν broadband σύνδεση στο διαδίκτυο που μπορεί να «προσφέρει» ένα απροστάτευτο δίκτυο. Η επίθεση parking lot, συνεπάγεται την χρήση της εμβελείας ενός wifi δικτύου σε συνδυασμό με κάποια τρύπα ασφαλείας, για την εισβολή στο δίκτυο αυτό από έναν ασφαλή για τον εισβολέα χώρο, όπως ο εταιρικός χώρος πάρκιν. Με μια δόση χιούμορ, πολλά άρθρα στο διαδίκτυο, για να ωθήσουν τους network administrators να αυξήσουν την ασφάλεια των ασύρματων δικτύων τους, ρωτούν: «μοιράζεστε την εταιρική σας σύνδεση στο ίντερνετ με εκείνο τον κύριο στο πάρκιν;».

Αυτό το είδος επίθεσης είναι μόνο μία από τις μεθόδους πρόκλησης κατάρρευσης σε ένα ασύρματο δίκτυο. Ένας αρκετά έξυπνος και δύσκολα αντιμετωπίσιμος τρόπος επίθεσης, είναι η ηθελημένη εκπομπή ψευδών πακέτων «αποσύνδεσης χρήστη»(disassociation/deauthentication packets) προς το Access Point. Εφόσον ο εισβολέας συλλέξει τις MAC διευθύνσεις των σταθμών πελατών μιας κυψέλης, μπορεί να απλά να στείλει πολλά πακέτα αποσύνδεσης για κάθε μια MAC-πελάτη. Το AP απλά δεν θα καταλάβει ότι τα πακέτα αυτά είναι κακόβουλα, και θα αποσυνδέσει όσους σταθμούς του ζητηθούν, προκαλώντας έτσι την κατάρρευση του δικτύου. Όλα τα παραπάνω συνηγορούν ότι η προτυποποίηση της ασύρματης ασφάλειας, είναι μια εργασία σε εξέλιξη. Νέα πρότυπα μελετούνται, όπως το 802.11i, που υπόσχονται μια καλύτερη λύση από το WEP. Βέβαια ένας τέτοιος στόχος φαίνεται εύκολος, δεδομένης της πλήρους και πέρα για πέρα αποτυχίας του WEP πρωτοκόλλου. Πολλοί χρησιμοποιούν λύσεις λογισμικού που κρυπτογραφούν την κίνηση δεδομένων σε υψηλότερο δικτυακό επίπεδο, όπως το IPsec, το ssl κτλ.

4.2 Το πρόβλημα του Κρυμμένου Κόμβου(Hidden Node)

Στην παράγραφο αυτό θα ορίσουμε και θα περιγράψουμε ίσως ένα από τα μεγαλύτερα μειονεκτήματα του 802.11b, το πρόβλημα του κρυμμένου κόμβου, το οποίο είναι καθαρά εγγενές στο σχεδιασμό του πρωτοκόλλου και οφείλεται πιθανότατα στους ίδιους τους στόχους τους οποίους έθεσε η ομάδα εργασίας της IEEE για το WiFi σαν εναλλακτικό τρόπο δικτύωσης σε τοπικό

επίπεδο. Είναι ένα πρόβλημα που εμφανίζεται μόνο σε infrastructure mode, όπως θα γίνει κατανοητό στις πιο κάτω γραμμές. Ας υποθέσουμε ότι έχουμε ένα κεντρικό Access Point και πολλούς clients σε διαφορετικές τοποθεσίες, έτσι ώστε όλοι οι clients να έχουν οπτική επαφή με το AP, αλλά όχι και καθένας με τον άλλο. Μιλάμε δηλαδή για μια
αρκετά τυπική περίπτωση ενός π.χ., ενδοπανεπιστημιακού δικτύου. Από τον ορισμό του το 802.11b προορίζονταν για ένα κλειστό περιβάλλον γραφείου. Σε αυτό το περιβάλλον, η επιτροπή της IEEE θεώρησε λογικό το ότι όλοι οι client κόμβοι που είναι συνδεδεμένοι σε ένα Access Point θα μπορούν «ακούν» το τι στέλνει ο γείτονάς τους. Χωρίς δηλαδή στην πραγματικότητα να λαμβάνουν τα δεδομένα που εκπέμπει ο διπλανός client προς το AP, έχουν την πληροφορία ότι αυτή την στιγμή κάποιος χρησιμοποιεί το κανάλι, στέλνοντας δεδομένα. Η κύρια μέθοδος αποφυγής συγκρούσεων στο 802.11 είναι το CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Η λειτουργία Carrier Sense πραγματοποιείται με παρακολούθηση του καναλιού πριν της έναρξη εκπομπής. Αν κάποιος άλλος client εκείνη την ώρα τύχει να εκπέμπει, τότε ο πρώτος περιμένει, έως ότου να βρεθεί στιγμή που το κανάλι να είναι ελεύθερο. Όπως καταλαβαίνουμε, για να επιτευχθεί ένα καλό ποσοστό συγχρονισμού, που θα εξασφαλίσει την εύρυθμη λειτουργία του δικτύου, πρέπει οι περισσότεροι client να βρίσκονται σε θέση να ακούν τις εκπομπές όλων των άλλων. Όταν δηλαδή ένας σταθμός ελέγχει το μέσο για να δει αν είναι σε χρήση, μπορεί εσφαλμένα να αποφασίσει ότι είναι ελεύθερο, μιας και δεν είναι σε θέση να λαμβάνει τις εκπομπές όλων των άλλων σταθμών του Access Point. Σε αυτήν την περίπτωση, το αποτέλεσμα θα είναι συνεχείς συγκρούσεις. Σε περίπτωση σύγκρουσης, το αποτέλεσμα είναι όμως δεν είναι τυχαίο, κάτι που αν συνέβαινε θα οδηγούσε ίσως σε ισορροπία. Συνήθως το Access Point τείνει να ευνοεί τον πομπό με το καλύτερο σήμα, καθώς λαμβάνει το σήμα του ασθενέστερου σαν θόρυβο και απορρίπτοντάς το. δεομένων λοιπόν των συνθηκών, μια και μόνο συσκευή μπορεί να μονοπωλήσει ολόκληρο το εύρος ζώνης του AP. Ευνοϊκές συνθήκες για την εμφάνιση προβλήματος κρυμμένου κόμβου δεν είναι όμως μόνο οι περιπτώσεις που υπάρχουν εμπόδια μεταξύ δύο ή περισσότερων σταθμών. Η επικοινωνία τύπου «όλοι ακούν όλους», μπορεί να είναι εφικτή μόνο όταν χρησιμοποιούμε μη κατευθυντικές(omni directional) κεραίες, οι οποίες εκπέμπουν κυκλικά το σήμα τους. Πολλές φορές όμως, η χρήση κατευθυντικών κεραιών(yagi, parabolic grid) υψηλού κέρδους σήματος, είναι μονόδρομος για να επιτευχθεί σύνδεσή (βλέπε εικόνα 7). Κάτω από αυτές τις συνθήκες, μια και μόνο client συσκευή είναι δυνατόν να μονοπωλήσει όλο το εύρος ζώνης του Access Point, προκαλώντας έτσι τεράστια συμφόρηση στις διακινήσεις δεδομένων των υπόλοιπων κόμβων.



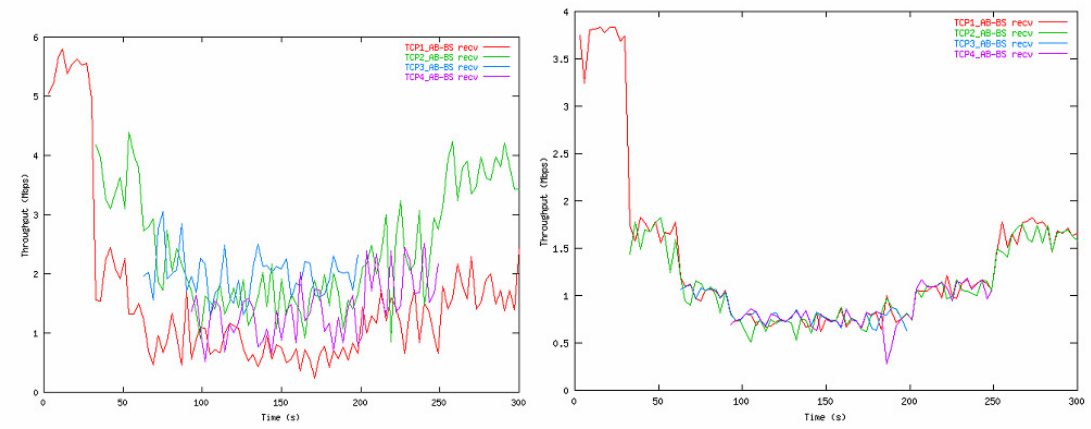
Εικόνα 15 – Wlan με πελάτες κατευθυντικής εκπομπής

Η εισαγωγή του μηχανισμού RTS/CTS έδωσε κάποια ελπιδοφόρα μηνύματα στην κοινότητα χρηστών του 802.11b. Η υλοποίηση βέβαια του μηχανισμού αυτού δεν είναι υποχρεωτική, και υπάρχουν πάρα πολλές συσκευές που δεν το υποστηρίζουν. Τελικά όμως ο μηχανισμός αυτός αποτυγχάνει πλήρως να αμβλύνει

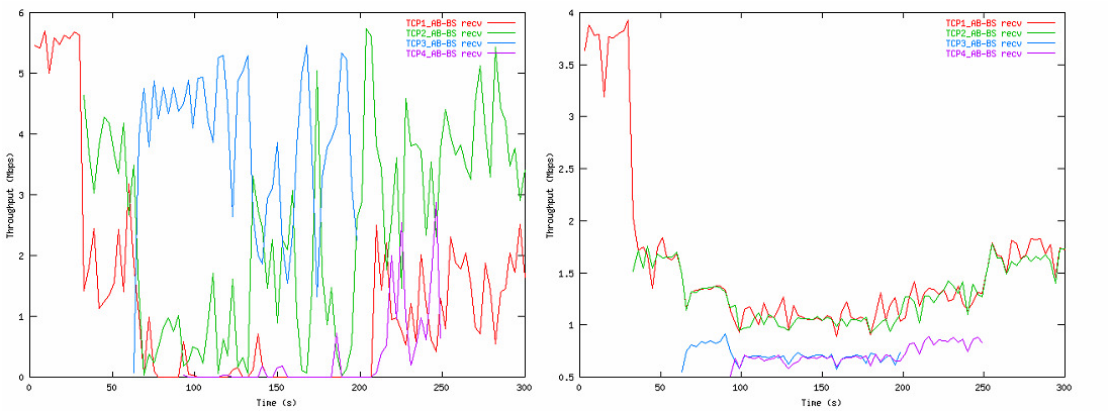
το φαινόμενο του Hidden Node, εν μέρει λόγω συγκρούσεων στα ίδια τα πακέτα RTS (περνάνε μόνο τα RTS του δυνατότερου). Παρόλο τον σχεδιασμό του, με πακέτα μικρού μεγέθους και ως εκ τούτου μικρότερη πιθανότητα σύγκρουσης, αλλά και γρηγορότερη διόρθωση των συγκρούσεων, η πραγματική χρήση τους σε δίκτυα εξωτερικού χώρου δεν φαίνεται να έχει αποτέλεσμα. Λύσεις υπάρχουν, και διαφέρουν σε προσέγγιση αλλά και κόστος. Υπάρχουν ειδικές συσκευές (ή firmware για συσκευές) οι οποίες εφαρμόζουν ένα είδος polling στο δίκτυο. Τέτοιες λύσεις έχουν θεωρικά αλλά και πρακτικά μεγάλη επιτυχία στην σωστή χρήση του εύρους ζώνης, αλλά έχουν μεγάλο κόστος, καθώς είναι παντελώς ασύμβατες με τα κλασσικά wifi προϊόντα, μιας και βγαίνουν εκτός του προτύπου. Λύσεις για bandwidth control σε υψηλότερο επίπεδο ερευνούνται, μα και πάλι δεν παρέχουν καμία εγγύηση για την εξάλειψη συγκρούσεων. Ίσως η καλύτερη λύση στο πρόβλημα έχει να προσφέρει η κοινότητα ανοιχτού κώδικα, και για την ακρίβεια, η ομάδα του Patras Wireless. Μια ελπιδοφόρος λύση είναι το πρωτόκολλο WiCCP(Wireless Central Coordination Protocol), το οποίο γράφτηκε και υλοποιήθηκε από δύο μέλη του PWN.

Το πρωτόκολλο υλοποιείται σε δύο κομμάτια λογισμικού, ένα master και ένα client network driver. Το πρώτο μπαίνει σε έναν υπολογιστή με wired σύνδεση στο AP και το client κομμάτι στο network driver stack κάθε υπολογιστή-χρήστη του AP. Στο πρωτόκολλο υπάρχει η ιδέα του token. Ο master δίνει το token σε κάθε client για ένα συγκεκριμένο χρονικό περιθώριο (timeslice). Μόνο ένας client μπορεί να έχει το token κάθε φορά. Όταν ο client θέλει να στείλει κάποιο πακέτο, κοιτάει αν το master τμήμα(στο access point) του έχει δώσει το token. Αν ναι, τότε προχωρά στην αποστολή, που θα κρατήσει όσο χρόνο του αφήνει το token. Αν δεν το έχει, τότε ο driver κρατά τα πακέτα που στέλνει ο χρήστης σε προσωρινή ουρά, και περιμένει να ξαναπάρει το token, αδειάζοντας την ουρά. Στην ουσία δημιουργεί ένα είδος token- ring στο standard Ethernet που χρησιμοποιεί το δίκτυο, τελείως transparent στις εφαρμογές χρήστη. Έτσι εγγυημένα αποφεύγονται όλες οι συγκρούσεις, καθώς μόνο ένας μιλάει κάθε φορά στο Access Point. Δείτε το patraswireless.net για περισσότερες πληροφορίες πάνω στο πρωτόκολλο, το οποίο ονομάζεται WiCCP(Wireless Central Coordinated Protocol), και βρίσκεται αισίως στην έκδοση 0.5. Η ανάπτυξη του driver γίνεται σε συνεργασία με άλλες μεγάλες ασύρματες κοινότητες, όπως το Perth Wireless της Αυστραλίας.

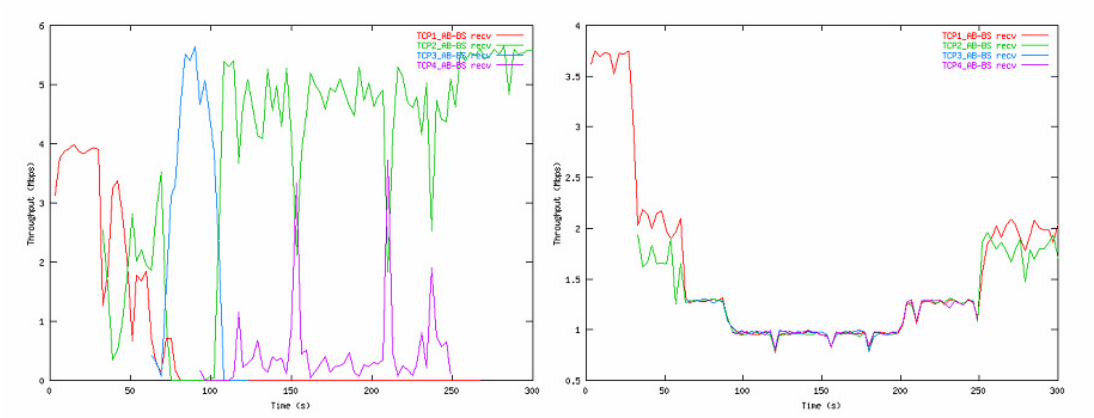
Ας δούμε μερικές χαρακτηριστικές συναρτήσεις χρόνου(ms)/διαμεταγωγής(Mbps) που δημιουργήθηκαν χρησιμοποιώντας αληθινά πειραματικά δεδομένα, ενός δικτύου με τέσσερις σταθμούς και ένα Access Point, με διάφορα σενάρια διακίνησης δεδομένων μεταξύ όλων των κόμβων. Συγκρίνονται οι δύο τρόποι πρόσβασης στο μέσο, ο CSMA/CA και ο τρόπος του polling. Δεν μας ενδιαφέρει η ακριβής υλοποίηση του polling, καθώς με σωστή υλοποίηση του σε κάποιο δικτυακό επίπεδο, θα έδινε τα ίδια περίπου αποτελέσματα, απλά μετατοπισμένα στον Y άξονα λόγω της διαφορετικής υλοποίησης (και διαφορετικής
ποσότητας overhead). Ξεκινάμε με την βέλτιστη περίπτωση για την μέθοδο CSMA.
Το Access Point στέλνει μία ροή σε κάθε ένα σταθμό. Όλοι οι πελάτες ακούν εξ ορισμού το AP, και έτσι η σωστή λειτουργία του CSMA είναι εφικτή.



Παρατηρούμε ότι ακόμη και στην βέλτιστη περίπτωση, η διακύμανση της διαμεταγωγής είναι πολύ μεγάλη με την μέθοδο CSMA(δεξιά εικόνα). Αντίθετα η λύση του polling δείχνει την υπεροχή της. Η μέση περίπτωση είναι αυτή κατά την οποία 2 σταθμοί στέλνουν στο Access Point και το AP στέλνει στους υπόλοιπους 2 σταθμούς.



Οι συγκρούσεις στα πακέτα δεδομένων είναι μαζικές με το CSMA(δεξιά εικόνα). Μία και μόνο σύνδεση μονοπωλεί σχεδόν το εύρος ζώνης, ενώ άλλες ακυρώνονται πλήρως. Αντίθετα το polling δίνει και πάλι ανεκτά αποτελέσματα. Μπορούμε εύκολα να φανταστούμε την γραφική παράσταση που θα παρουσιάζει μια μετάδοση από τους τέσσερις σταθμούς προς το AP. Οι συγκρούσεις είναι τρομακτικές, και οι διακυμάνσεις δείχνουν δραματικά την πλήρη κατάρρευση της κυψέλης.



Τα παραπάνω πειραματικά δεδομένα δείχνουν με τον πιο πειστικό τρόπο την ανεπάρκεια του CSMA/CA - RTS/CTS μηχανισμού. Μια ασύρματη δικτυακή εγκατάσταση μπορεί δεδομένων κάποιων συνθηκών να καταρρεύσει πλήρως. Θα μπορούσαμε να περιγράψουμε κάτι τέτοιο σαν μια (distributed) denial of service attack, που μπορεί να προκληθεί είτε από κακοπροαίρετους παρείσακτους κόμβους, είτε από απλούς χρήστες που θέλουν να κάνουν την δουλειά τους. Οι σχεδιαστές δικτύου πρέπει να είναι καλά ενημερωμένοι για το πρόβλημα, και να προσπαθούν να
κατασκευάζουν δίκτυα που θα επηρεάζονται από hidden node σε μικρές κλίμακες. Η επιλογή point to point ad hoc των συνδέσεων ραχοκοκαλιάς(backbone) του δικτύου είναι προτιμότερη από αρχιτεκτονικές AP-client.

4.3 Συμπερασματικά

Άλλα πρωτόκολλα ασύρματης δικτύωσης

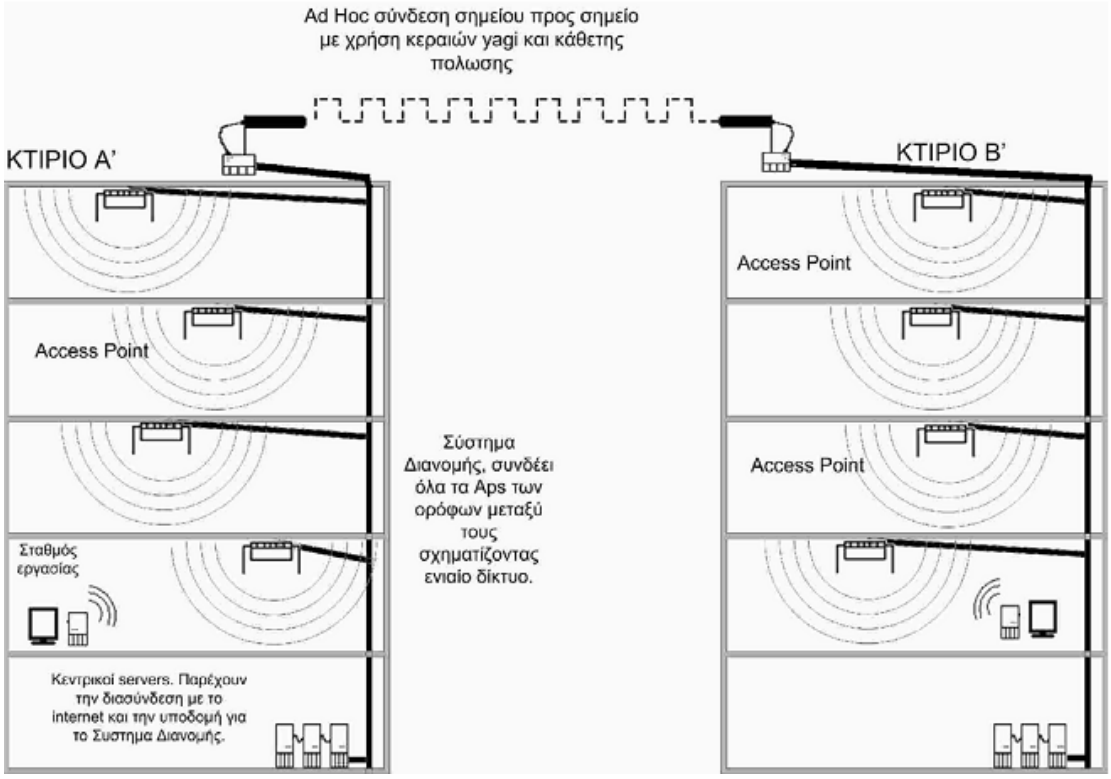
Το 802.11 και η οικογένεια πρωτοκόλλων του b, a και g δεν είναι βεβαίως οι μοναδικοί παίκτες στο παιχνίδι της ασύρματης δικτύωσης. Ας κάνουμε μια αναφορά στα υπόλοιπα πρωτόκολλα, απαριθμώντας κάποια σύντομα χαρακτηριστικά. Το HiperLAN είναι μια πρωτοβουλία της ευρωπαϊκής οργάνωσης ETSI(European Telecommunications Standards Institute) που ξεκίνησε το 1996. Η πρώτη έκδοση του πρωτοκόλλου υποστηρίζει λειτουργία στο φάσμα των 5GHz και εύρος ζώνης στα 22Mbps. Χρησιμοποιεί connectionless τρόπο πρόσβασης στο ασύρματο δίκτυο για τους χρήστες του, όπως το Ethernet. Υποστηρίζει QoS για ανάγκες όπως το streaming video, VoIP κτλ. Η δεύτερη έκδοση του πρωτοκόλλου που είναι υπό κατασκευή (HiperLAN2) θα λειτουργεί και πάλι στα 5GHz με ταχύτητα της τάξης των 54Mbps, θα έχει connection-oriented τρόπο πρόσβασης και θα είναι ικανό να μεταφέρει πακέτα Ethernet, ATM και IP. Το HomeRF ξεκίνησε από την HomeRF Working Group η οποία προσέφερε στην αγορά μια ανοιχτή βιομηχανική προδιαγραφή με το όνομα SWAP(Shared Access Wireless Protocol), με προορισμό την ασύρματη ψηφιακή επικοινωνία μεταξύ ηλεκτρονικών υπολογιστών και ηλεκτρονικών συσκευών στο οικιακό περιβάλλον.
Υποστηρίζει διαμόρφωση Frequency Hopping spread spectrum με ταχύτητα του 1Mbps. Αναμένεται νέα δημοσίευση του πρωτοκόλλου με ταχύτητα στα 10Mbps. Περνώντας στο πεδίο των προσωπικών δικτύων (Personal Area Networks, εν αντιθέσει με τα LANs), πρέπει να αναφερθούμε στο Bluetooth, ένα πρωτόκολλο με μεγάλη αποδοχή από τους μεγαλύτερους κατασκευαστές στον χώρο. Λειτουργεί και αυτό στους 2.4 μεγακύκλους και έχει μέγιστη ταχύτητα το 1mbps. Έχει σκοπό την δημιουργία ενός δικτύου μικρής εμβέλειας γύρω από τον χρήστη του, το οποίο μπορεί να αλληλεπιδρά με αντίστοιχες Bluetooth-enabled συσκευές.

Η τεχνολογία 802.11(b) ήταν η πρώτη εδώ και αρκετά χρόνια πρωτοβουλία, για την εισαγωγή ενός πρωτοκόλλου ασύρματης τοπικής δικτύωσης μεγάλου εύρους ζώνης. Τα πλεονεκτήματα που περιγράψαμε ποιο πάνω, σε συνδυασμό με το γεγονός ότι δεν είναι αναγκαία η απόκτηση ειδικής άδειας χρήσης αυτής της ραδιοφωνικής συχνότητας, έκανε την αποδοχή του από τους καταναλωτές και τις εταιρίες ταχύτατη. Μάλιστα οι δυνατότητες της οικογένειας πρωτοκόλλων 802.11, είναι τέτοιες που το καθιστούν μια καλή λύση του προβλήματος του τελευταίου χιλιομέτρου (last mile problem), δηλαδή την παροχή broadband υπηρεσιών στον τελικό χρήστη από το δίκτυο μεταφοράς δεδομένων του ήδη εγκατεστημένου τηλεφωνικού δικτύου. Στο εξωτερικό ανθεί η αγορά των wISPs (wireless Internet service provider), που προσφέρουν ευρυζωνικό internet μέσω της ασύρματης υποδομής που κατασκευάζουν οι ίδιοι, και μισθώνοντας γρήγορες συνδέσεις στο διαδίκτυο, τις οποίες και παρέχουν στους τελικούς πελάτες. Στην Ελλάδα κάτι τέτοιο είναι ανέφικτο για την ώρα, λόγω του ασαφούς νομικού πλαισίου περί της εμπορικής χρήσης της συχνότητας των 2,4GHz. Είναι επιτακτική λοιπόν η ανάγκη για νομοθετικές αλλαγές, που θα βοηθήσουν να αρθεί το μονοπώλιο των κρατικών τηλεπικοινωνιακών φορέων, και θα δώσει νέες ανταγωνιστικές δυνατότητες σε μικρότερες επιχειρήσεις. Παρατηρώντας την μεγάλη αποδοχή του 802.11b, σε σχέση με το πόσο πρόσφατα έγινε η προτυποποίηση, είναι ξεκάθαρη η επιτυχία του σαν standard. Επιπλέον, δεν μπορούμε παρά να αναγνωρίσουμε πως αυτός ο νέος τρόπος ασύρματης επικοινωνίας και ανταλλαγής δεδομένων, είναι μια νέα και σχετικά ανεξερεύνητη περιοχή, που ίσως μας επιφυλάσσει μεγάλες αλλαγές στην ποιότητα, την αποδοτικότητα αλλά και την αντίληψη που έχουμε για τις ψηφιακές τηλεπικοινωνίες.

4.4 Παράδειγμα ασύρματου δικτυακής εγκατάστασης: Η εταιρία Χ

Η εταιρία Χ δραστηριοποιείται στον χώρο των web services. Σε κάθε όροφο του τετραώροφου κτιριακού της συγκροτήματος πρέπει να παρέχεται σύνδεση στο εταιρικό LAN στους υπαλλήλους, καθώς και διασύνδεση με το internet. Access Points στημένα σε κάθε όροφο, συνδεδεμένα στον ενσύρματο «κορμό» του εταιρικού δικτύου, θα δίνουν αυτή τη δυνατότητα στους

υπαλλήλους. Οι εργαζόμενοι μπορούν είτε να εργάζονται στους σταθμούς εργασίας τους, είτε να κινούνται με φορητούς υπολογιστές ανά τους ορόφους χωρίς να χάνουν την σύνδεση με το δίκτυο. Ένα προφανές πρόβλημα, είναι ότι η επιχείρηση έχει κτίρια και στις δύο μεριές μιας λεωφόρου. Θα ξεπεράσουμε αυτό το εμπόδιο, εγκαθιστώντας μια ad hoc σύνδεση μεταξύ των δύο κτιρίων, χρησιμοποιώντας μια συσκευή σταθμό σε κάθε ταράτσα, εφοδιασμένη με κατευθυντικές yagi κεραίες μικρού σχετικά κέρδους, μιας και η απόσταση που πρέπει να καλυφθεί είναι μικρή. Η χρήση αυτού του τύπου κεραίας(ιδιαίτερα κατευθυντικής εκπομπής) γίνεται για δύο σημαντικούς λόγους. Α) Χρειαζόμαστε ένα απόλυτα κατευθυντικό Link. Δεν θέλουμε να συνδεθούμε η να παρέχουμε κάποια υπηρεσία σε κανέναν άλλον εκτός από το απέναντι κτίριο. Με αυτό το δεδομένο, οποιαδήποτε ποσότητα ενέργειας της εκπομπής μας γίνεται σε χώρο εκτός της απέναντι κεραίας, θεωρείται σπατάλη, καθώς επιζητούμε την μέγιστη ποιότητα σύνδεσης που μπορούμε να έχουμε με μία δεδομένη ισχύ. Η ισχύς της κεραίας πρέπει πάντα να κρατηθεί εντός νομικών ορίων. Β) Κατευθυντική εκπομπή στην ελάχιστη δυνατή ισχύ, σε αυτή την περίπτωση, σημαίνει αυξημένη ασφάλεια. Ένας υποθετικός εισβολέας, για να μπορέσει να εκμεταλλευτεί όλα τα μειονεκτήματα ασφαλείας του 802.11b που αναφέραμε ποιο πάνω, πρέπει αρχικά να έχει πρόσβαση στην ίδια την μικροκομματική εκπομπή της κεραίας μας. Σε ένα ιδανικά και απόλυτα κατευθυντικό link, κάποιος θα μπορούσε να υποκλέψει την πληροφορία που διακινείτο στον αέρα, μόνο αν ήταν πάνω στην νοητή ευθεία των δύο κεραιών. Εφόσον η πρόσβαση στις ταράτσες των κτιρίων είναι απαγορευμένη, είναι πολύ μικρή η πιθανότητα να καταφέρει κάποιος την κακοπροαίρετη λήψη πακέτων χωρίς να αποθαρρυνθεί από την κακή ποιότητα σήματος που θα έχει από παραδείγματος χάριν, τον δρόμο.



Εικόνα 16 – Η εταιρία Χ

Σε όλα τα Access Points μπορούμε να εφαρμόσουμε ρυθμίσεις ασφαλείας αναλόγως τις απαιτήσεις μας. Συνίσταται η ενεργοποίηση του WEP, όσο ανασφαλές και αν είναι, καθώς αποτελεί ένα πρώτο «φράκτη» για οποιονδήποτε εισβολέα. Μπορούμε επίσης να κρατάμε βάση δεδομένων με τις επιτρεπόμενες hardware

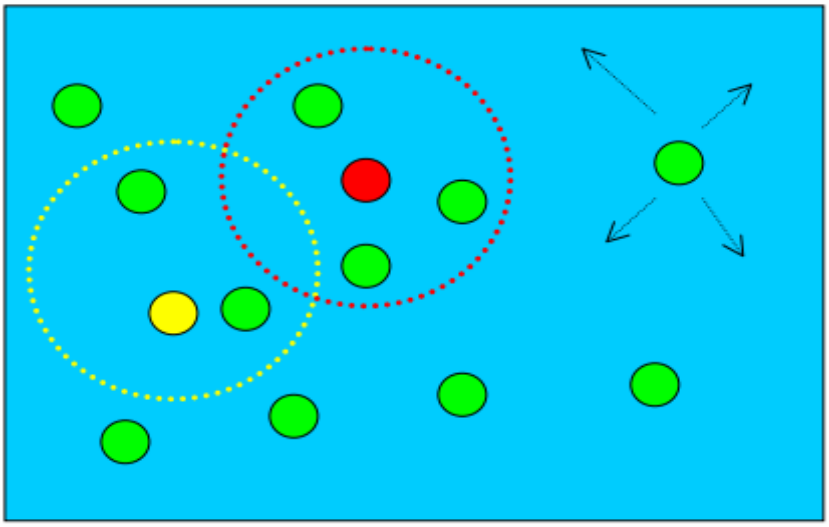
διευθύνσεις(MAC address) και απαγορέψουμε όλες τις άλλες. Αυτό βέβαια χρειάζεται την επίπονη δουλειά της συνεχούς ενημέρωσης μιας βάσης δεδομένων με τα επιτρεπόμενα MACs, και κάτι τέτοιο μπορεί να είναι απαγορευτικό σε ένα δυναμικόπεριβάλλον. Για να αυξήσουμε ακόμη περισσότερο την ασφάλεια του εξωτερικού link μεταξύ των κτιρίων, μπορούμε να εφαρμόσουμε κάποια μέθοδο κρυπτογράφησης των δεδομένων σε υψηλότερο δικτυακό επίπεδο ακριβώς πριν και μετά την έξοδό τους από αυτό, όπως IPsec ή κάποιο είδος secure tunnel.

ΚΕΦΑΛΑΙΟ 5ο

Αλγόριθμοι Δρομολόγησης σε ad hoc δίκτυα

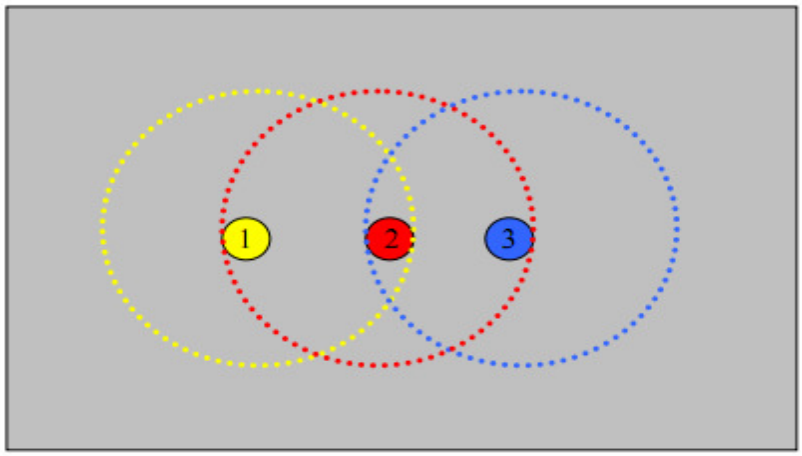
5.1 Γενική περιγραφή των ασύρματων ad hoc δικτύων

Μέχρι στιγμής ασχοληθήκαμε με μια συγκεκριμένη τοπολογία ασύρματου δικτύου όπου όλα τα πακέτα δρομολογούνταν μέσω ενός κεντρικού τερατικού είτε προς το σταθερό δίκτυο είτε προς κάποιο άλλο τερματικό που συμμετέχει στο δίκτυο. Στο παρών κεφάλαιο θα ασχοληθούμε με ένα άλλο είδος τοπολογίας δικτύου όπου δεν υφίσταται κεντρικός έλεγχος. Τα δίκτυα αυτού του είδους ονομάζονται ad hoc δίκτυα.



Εικόνα 5.1
Ασύρματο ad hoc δίκτυο. Κάθε κύκλος αντιπροσωπεύει έναν κόμβο.
Διακρίνονται τα όρια εμβέλειας δύο κόμβων του.

Ένα ασύρματο ad hoc δίκτυο είναι είναι ένα σύνολο κινητών κόμβων σε μια έκταση όπου δεν προυπάρχει εγκατεστημένη υποδομή, οι οποίοι σχηματίζουν ένα προσωρινό δίκτυο. Κάθε κόμβος του δικτύου έχει τη δυνατότητα επικοινωνίας με τους υπόλοιπους μέσω ενός ασύρματου πρωτοκόλλου επικοινωνίας όπως είναι το 802.11a. Η παραπάνω εικόνα δείχνει ένα απλό ad hoc δίκτυο αποτελούμενο από έναν αριθμό κόμβων. Οι κόμβοι έχουν τη δυνατότητα να κινούνται ελεύθερα προς οποιαδήποτε κατεύθυνση. Έτσι η τοπολογία του δικτύου αλλάζει αφού χάνονται και δημιουργούνται συνδέσεις συνεχώς. Αυτό οφείλεται στην περιορισμένη εμβέλεια των τερματικών που τους δίνει τη δυνατότητα επικοινωνίας με έναν αριθμό τερματικών που μπορούν να θεωρηθούν γειτονικά. Στην εικόνα που ακολουθεί οι ακραίοι κόμβοι δεν έχουν τη δυνατότητα απ'ευθείας επικοινωνίας μεταξύ τους. Ωστόσο ο μεσαίος κόμβος μπορεί να λειτουργήσει ως ενδιάμεσος σταθμός προώθησης μηνυμάτων από το ένα τερματικό στο άλλο. Με τον τρόπο αυτό ο μεσαίος κόμβος δρα σαν δρομολογητής (router).



Εικόνα 5.2
Όρια εμβέλειας τριών κόμβων ad hoc δικτύου

Ένα ad hoc δίκτυο δε χρησιμοποιεί κεντρική διαχείριση. Αυτό εξασφαλίζει ότι το δίκτυο δεν θα καταρρεύσει στην περίπτωση που κάποιος από τους κόμβους του δικτύου περάσει εκτός εμβέλειας των άλλων κόμβων. Κάθε κόμβος του δικτύου μπορεί να εισέλθει ή να εγκαταλείψει το δίκτυο οποιαδήποτε στιγμή μεταβάλλοντας έτσι την τοπολογία του δικτύου. Εξαιτίας της περιορισμένης εμβέλειας εκπομπής κάθε κόμβου είναι δυνατό να χρειαστούν πολλοί ενδιάμεσοι σταθμοί μέχρι το πακέτο να φτάσει στον προορισμό του. Όλοι οι κόμβοι του δικτύου πρέπει να έχουν τη δυνατότητα να προωθούν πακέτα προς άλλους κόμβους. Έτσι κάθε κόμβος λειτουργεί και ως τερματικό για την εξυπηρέτηση των χρηστών αλλά και ως δρομολογητής για την εξυπηρέτηση της συνολικής κίνησης στο δίκτυο. Ο δρομολογητής είναι μια οντότητα του δικτύου στην οποία αναφερόμαστε με κάποια διεύθυνση που ορίζει μοναδικά την ύπαρξή του. Για να λειτουργεί κάποιος κόμβος ως δρομολογητής πρέπει να έχει ενσωματωμένο έναν αλγόριθμο δρομολόγησης. Το ad hoc δίκτυο έχει τη δυνατότητα να αναγνωρίσει όποιες αλλαγές στην τοπολογία ή δυσλειτουργίες σε συγκεκριμένους κόμβους. Αν για παράδειγμα ένας κόμβος εγκαταλείψει το δίκτυο θα χαθούν κάποιοι από τις οδούς δρομολόγησης των πακέτων. Οι υπόλοιποι κόμβοι θα αναζητήσουν νέους δρόμους λύνοντας το πρόβλημα. Το δίκτυο συνεχίζει να λειτουργεί στο σύνολό του παρόλο που μπορεί να αυξηθεί η καθυστέρηση παράδοσης των πακέτων. Το ίδιο το ασύρματο μέσο μετάδοσης παρά τα όποια προβλήματα δημιουργεί παρέχει ένα σημαντικό πλεονέκτημα στο δίκτυο. Αντίθετα με ένα ενσύρματο δίκτυο σε ένα ασύρματο κάθε κόμβος έχει δυνατότητα απευθείας επικοινωνίας με οποιονδήποτε κόμβο είναι εντός εμβέλειας. Έτσι για την επικοινωνία απομακρυσμένων κόμβων υπάρχει η δυνατότητα να βρεθούν πολλοί δρόμοι για την ανταλλαγή πακέτων κάνοντας το δίκτυο λιγότερο ευάλωτο σε πιθανή δυσλειτουργία κάποιου κόμβου.

5.2 Είδη αλγορίθμων δρομολόγησης

Εξαιτίας του γεγονότος ότι για τη μεταφορά ενός πακέτου από ένα κόμβο του δικτύου σε έναν άλλο μπορεί να χρειαστούν πολλοί ενδιάμεσοι σταθμοί είναι απαραίτητη η χρήση ενός πρωτοκόλλου δρομολόγησης. Τα πρωτόκολλα δρομολόγησης έχουν δυο κύριες λειτουργίες. Η μία είναι η επιλογή των δρόμων για διάφορα ζευγάρια αποστολέα - παραλήπτη και η παράδοση του πακέτου στο σωστό προορισμό. Η δεύτερη λειτουργία είναι η ανάλυση του δικτύου μέσα από μια σειρά πρωτοκόλλων και δομών δεδομένων (πίνακες δρομολόγησης, routing tables). Τα πρωτόκολλα δρομολόγησης για ad hoc δίκτυα βασίζονται στα ήδη υπάρχοντα πρωτόκολλα δρομολόγησης με ορισμένες μετατροπές για να ανταποκρίνονται στις απαιτήσεις του ασύρματου δικτύου. Για το λόγο αυτό θα παρουσιάσουμε σύντομα τα είδη των πρωτοκόλλων δρομολόγησης.

5.2.1 Πρωτόκολλα κατάστασης σύνδεσης, Link State Protocols

Στο είδος αυτό της δρομολόγησης κάθε κόμβος έχει αντίληψη της συνολικής τοπολογίας του δικτύου κρατώντας ένα συντελεστή βάρους για κάθε σύνδεση. Για τη διαρκή ενημέρωση αυτών των συντελεστών κάθε κόμβος εκπέμπει περιοδικά τους συντελεστές του σε όλους τους άλλους κόμβους. Αυτό γίνεται με την ακόλουθη διαδικασία: το τερματικό εκπέμπει τις πληροφορίες σε όσα τερματικά βρίσκονται εντός εμβέλειας εκπομπής του. Κάθε ένα από αυτά εκτελεί την αντίστοιχη διαδικασία με τα γειτονικά τερματικά του μέχρις ότου η πληροφορία φτάσει σε όλα τα τερματικά που αποτελούν το δίκτυο. Καθώς κάθε κόμβος λαμβάνει τις πληροφορίες μεταβάλλει την αντίληψη που έχει για το δίκτυο και εφαρμόζει έναν αλγόριθμο εύρεσης του μικρότερου δρόμου ώστε να επιλέξει τον επόμενο σταθμό για κάθε προορισμό. Μερικοί συντελεστές βάρους μπορεί να είναι λανθασμένοι εξαιτίας καθυστέρησης στη μετάδοση για παράδειγμα. Αυτή η ασυμβατότητα στον τρόπο με τον οποίο οι διαφορετικοί κόμβοι βλέπουν την τοπολογία του δικτύου μπορεί να οδηγήσει τα πακέτα να περιφέρονται συνεχώς στο δίκτυο αναζητώντας τον προορισμό τους. Το πρόβλημα όμως γίνεται αντιληπτό και διορθώνεται από τη στιγμή που ένα πακέτο θα περάσει δυο φορές από το ίδιο τερματικό.

5.2.2 Πρωτόκολλα διανύσματος απόστασης, Distance Vector Protocols

Στα πρωτόκολλα αυτού του είδους κάθε κόμβος υπολογίζει τους συντελεστές βάρους για κάθε σύνδεση με τους άλλους κόμβους, αλλά αντί να στείλει αυτή την πληροφορία σε όλους τους άλλους κόμβους, εκπέμπει περιοδικά στα γειτονικά του τερματικά μια εκτίμηση για το συντομότερο δρόμο προς κάθε κόμβο του δικτύου. Τα τερματικά που λαμβάνουν αυτή την πληροφορία τη χρησιμοποιούν για να επαναπροσδιορίσουν τους πίνακες δρομολόγησης, χρησιμοποιώντας κάποιον αλγόριθμο εύρεσης του συντομότερου δρόμου.

Συγκρινόμενα με το παραπάνω είδος πρωτοκόλλων, τα πρωτόκολλα διανύσματος απόστασης απαιτούν μικρότερη υπολογιστική δύναμη, είναι ευκολότερο να εφαρμοστούν και απαιτούν πολύ μικρότερο χώρο αποθήκευσης. Ωστόσο με το συγκεκριμένο πρωτόκολλο είναι δυνατό να δημιουργηθούν βρόγχοι μέσα στους οποίους θα κινούνται τα πακέτα χωρίς να φτάνουν στον τελικό τους προορισμό. Η πρωταρχική αιτία γι' αυτό είναι ότι οι κόμβοι επιλέγουν τον επόμενο κόμβο στον οποίο θα προωθήσουν το πακέτο βασιμένοι σε πληροφορίες που μπορεί να είναι ξεπερασμένες λόγω αλλαγής στην τοπολογία του δικτύου.

5.2.3 Πρωτόκολλα πληροφορίας από την πηγή, Source routing

Στα πρωτόκολλα αυτού του είδους κάθε πακέτο φέρει πληροφορία για το δρόμο που ακολούθησε μέσα στο δίκτυο. Με τον τρόπο αυτό η απόφαση για τη δρομολόγηση γίνεται στον κόμβο του αποστολέα. Το πλεονέκτημα στην περίπτωση αυτή είναι η αποφυγή δημιουργίας βρόχων κατά τη δρομολόγηση. Ωστόσο υπάρχει το μειονέκτημα ότι κάθε πακέτο 'φορτώνεται' με μια επιπλέον πληροφορία.

Ταξινόμηση πρωτοκόλλων. Τα διάφορα πρωτόκολλα δρομολόγησης μπορούν να ταξινομηθούν σε κατηγορίες βάσει των ιδιοτήτων τους.

Κεντρικού ελέγχου και διανεμημένα

Στα πρωτόκολλα κεντρικού ελέγχου όλες οι αποφάσεις για δρομολόγηση παίρνονται από ένα κεντρικό κόμβο. Αντίθετα στα διανεμημένα ο υπολογισμός των βέλτιστων δρόμων μοιράζεται ανάμεσα στους κόμβους του δικτύου.

Στατικά και προσαρμοζόμενα

Η κατηγοριοποίηση αυτή γίνεται με βάση το κατά πόσο ένα πρωτόκολλο λαμβάνει υπόψη τις συνθήκες κίνησης στο δίκτυο. Στους στατικούς αλγόριθμους ο δρόμος που ακολουθείται από τον αποστολέα στον παραλήπτη είναι σταθερός και δεν αλλάζει με την αλλαγή των συνθηκών κίνησης. Μόνο στην περίπτωση που υπάρξει κάποιο σφάλμα κατα τη δρομολόγηση η διαδρομή θα αλλάξει. Αυτός ο τύπος αλγορίθμου δεν μπορεί να επιτύχει υψηλή ρυθμαπόδοση στην περίπτωση ενός φορτωμένου από πλευράς κίνησης δικτύου. Έτσι στις περισσότερας περιπτώσεις γίνεται χρήση προσαρμοζόμενων αλγορίθμων για την απόφυγη της συμφόρησης σε συγκεκριμένους κόμβους.

Αντι-δραστικά (Re-active) και Προ-δραστικά (Pro-active)

Η τρίτη αυτή κατηγοριοποίηση αναφέρεται σε πρωτόκολλα που αφορούν κυρίως σε ad hoc δίκτυα. Τα proactive πρωτόκολλα συνεχώς κάνουν εκτιμήσεις για τις διαδρομές μέσα στο δίκτυο, έτσι ώστε όταν ένα πακέτο χρειαστεί να προωθηθεί προς τον προορισμό του, ο δρόμος είναι ήδη γνωστός και χρησιμοποιείται αμέσως. Τα πρωτόκολλα διανύσματος απόστασης ανήκουν σ' αυτή την κατηγορία. Από την άλλη πλευρά τα reactive πρωτόκολλα προσπαθούν να βρούν το βέλτιστο δρόμο μόνο όταν τους ζητηθεί. Τα πρωτόκολλα της πρώτης κατηγορίας έχουν το πλεονέκτημα να δρομολογούν το πακέτο με την ελάχιστη καθυστέρηση. Ωστόσο χρειάζονται χρόνο για να φτάσουν σε σταθερή κατάσταση. Αυτό μπορεί να προκαλέσει προβλήματα στην περίπτωση που η τοπολογία του δικτύου μεταβάλλεται συχνά.

5.3 Επιθυμητά χαρακτηριστικά

Από τους αλγορίθμους δρομολόγησης που αναφέρονται σε ασύρματα ad hoc δίκτυα έχουμε κάποιες ειδικές απαιτήσεις.

Διανεμημένη λειτουργία

Το πρωτόκολλο ασφαλώς πρέπει να είναι διανεμημένο και δεν πρέπει να βασίζεται σε κάποιο κεντρικό κόμβο. Αυτό συμβαίνει βέβαια και με τα σταθερά δίκτυα. Η διαφορά ωστόσο είναι πως σε ένα ad hoc δίκτυο, ένα τερματικό μπορεί να εισέλθει ή να εξέλθει από το δίκτυο ή λόγω κίνησης να βγει εκτός εμβέλειας των άλλων τερματικών

Αποφυγή δημιουργίας βρόχων

Για τη βέλτιστη συνολική λειτουργία του δικτύου είναι απαραίτητο ο αλγόριθμος δρομολόγησης να εγγυάται την αποφυγή δημιουργίας βρόχων. Αυτό βοηθά στο να μην καταναλώνεται χρήσιμο φάσμα και υπολογιστική δύναμη.

Λειτουργία σύμφωνα με τις απαιτήσεις

Για την ελαχιστοποίηση των πληροφορίων ελέγχου και τη διατήρηση των πόρων του δικτύου είναι απαραίτητο το πρωτόκολλο να είναι reactive. Αυτό σημαίνει ότι κάθε κόμβος θα ανταποκρίνεται μόνο όταν του ζητηθεί και δε θα αποστέλλει περιοδικά πληροφορίες ελέγχου.

Συντομότερος δρόμος σε ασύρματο δίκτυο

Σε ένα ασύρματο δίκτυο δεν μπορούμε, σε αρκετές περιπτώσεις, να πούμε ότι ο συντομότερος δρόμος μεταξύ δυο τερματκών είναι αυτός που εμπλέκει το μικρότερο αριθμό ενδιάμεσων κόμβων. Το κανάλι μπορεί να περιέλθει εύκολα σε κατάσταση διαλείψεων, κάνοντας κάποια σύνδεση μη αποτελεσματική και δημιουργώντας μεγάλη καθυστέρηση. Χάνεται έτσι το πλεονέκτημα των λιγότερων ενδιάμεσων κόμβων.

- Υποστήριξη μονοκατευθυντικών συνδέσεων

Το ασύρματο μέσο είναι δυνατό να δημιουργήσει μονοκατευθυντικές συνδέσεις. Η χρήση αυτών των συνδέσεων και όχι μόνο των διπλής κατεύθυνσης βελτιώνει την απόδοση του πρωτοκόλλου.

- Ασφάλεια

Το ασύρματο μέσο είναι εξαιρετικά ευπαθές σε προσπάθειες υποκλοπής πληροφοριών. Για το λόγο αυτό απαιτείται το πρωτόκολλο δρομολόγησης να παρέχει προληπτικά μέτρα ασφαλείας. Η χρήση κωδικοποίησης είναι μία λύση σε συνδιασμό με τη διανομή κωδικών κλειδιών στα μέλη του δικτύου.

- Διατήρηση ενέργειας

Οι κόμβοι ενός ασύρματου δικτύου είναι συνήθως φορητοί υπολογιστές με περιορισμένους ενεργειακούς πόρους. Για το λόγο αυτό οι κόμβοι του δικτύου αδρανοποιούνται όταν ο χρήστης δεν

τους χρησιμοποιεί με σκοπό να εξοικονομήσουν ενέργεια. Το πρωτόκολλο δρομολόγησης πρέπει να λαμβάνει υπόψη αυτή την ιδιαιτερότητα τών ασύρματων κόμβων. Από την άλλη χρησιμοποιώντας τη συντομότερη διαδρομή πάντα, σημαίνει ότι οι κόμβοι που συμμετέχουν σε αυτή πολύ γρήγορα θα χάσουν την ενέργειά τους και θα απενεργοποιηθούν αν δεν μπορούμε να εξασφαλίσουμε την τροφοδοσία τους.

- Πολλαπλοί δρόμοι

Για την αντιμετώπιση των συχνών αλλαγών στην τοπολογία του δικτύου και της συμφόρησης πρέπει να είναι δυνατή η χρήση διαφορετικών διαδρομών. Έτσι αν καποια διαδρομή δεν ισχύει πλέον τότε γίνεται χρήση κάποιας από τις εναλλακτικές διαδρομές χωρίς να χρειαστεί να υπολογιστεί από την αρχή μια νέα διαδρομή. Υποστήριξη ποιότητας υπηρεσιών (Quality of Service support, QoS). Απαραίτητη κρίνεται η υποστήριξη κάποιου είδους QoS από το πρωτόκολλο αφού τα ασύρματα ad hoc δίκτυα χρησιμοποιούνται συνήθως για εφαρμογές πραγματικού χρόνου.

5.4 Πρωτόκολλα δρομολόγησης

5.4.1 Ad-Hoc On-Demand Distance Vector - AODV

Το πρωτόκολλο επικοινωνίας AODV επιτρέπει δρομολόγηση μέσω πολλαπλών ενδιάμεσων κόμβων με σκοπό να διατηρηθεί λειτουργικό το ασύρματο δίκτυο. Το AODV βασίζεται στον αλγόριθμο του διανύσματος απόστασης. Η διαφορά είναι ότι το AODV ενεργεί όταν ζητηθεί ένας δρόμος επικοινωνίας (ανήκει στα reactive πρωτόκολλα) σε αντίθεση με τα πρωτόκολλα που διατηρούν και ανανεώνουν συνεχώς τις πληροφορίες δρομολόγησης. Το AODV ζητά ένα νέο δρόμο όταν του ζητηθεί και δεν απαιτεί από τους κόμβους να διατηρούν πληροφορίες για δρόμους προς κόμβους που δε συμμετέχουν ενεργά στην επικοινωνία. Από τη στιγμή που οι κόμβοι που θέλουν να επικοινωνήσουν έχουν πληροφορίες για το δρόμο που πρέπει να ακολουθήσουν για να είναι επιτυχής η επικοινωνία, το AODV δεν παίζει κανένα ρόλο. Χαρακτηριστικά αυτού του πρωτοκόλλου είναι η αποφυγή δημιουργίας βρόχων και η απώλεια κάποιας σύνδεσης προκαλεί άμεση ειδοποίηση προς την ομάδα των κόμβων που επηρεάζονται και μόνο προς αυτή. Επιπλέον, το AODV υποστηρίζει δρομολόγηση προς πολλαπλούς παραλήπτες. Η χρήση αύξοντα αριθμού για τον προορισμό εγγυάται ότι οι πληροφορίες για τη διαδρομή είναι πρόσφατες.

Το πρωτόκολλο χρησιμοποιεί διάφορα μηνύματα για την εύρεση και διατήρηση των συνδέσεων. Όποτε κάποιος κόμβος θέλει να επικοινωνήσει με έναν άλλο κόμβο, εκπέμπει μία Αίτηση Διαδρομής (Route Request, RREQ) προς όλους τους γειτονικούς του. Η RREQ διατρέχει το δίκτυο ώσπου να φτάσει στον προορισμό ή ένα κόμβο με αρκετά πρόσφατες πληροφορίες για τη διαδρομή προς τον ζητούμενο κόμβο. Η διαδρομή γίνεται γνωστή επιστρέφοντας μια Απάντηση Διαδρομής (Route Reply, RREP) στον αποστολέα.

Ο αλγόριθμος χρησιμοποιεί μηνύματα χαιρετισμού (hello messages) τα οποία εκπέμπονται περιοδικά στους άμεσους γείτονες. Τα μηνύματα αυτά επιβεβαιώνουν τοπικά τη συνεχιζόμενη παρουσία του συγκεκριμένου κόμβου στο δίκτυο. Με τον τρόπο αυτό οι γείτονες που χρησιμοποιούν διαδρομές μέσω του κόμβου που εκπέμπει συνεχίζουν να θεωρούν τις διαδρομές έγκυρες. Αν τα μηνύματα χαιρετισμού πάψουν να έρχονται από ένα κόμβο τότε η γειτονιά του υποθέτει ότι ο κόμβος βγήκε εκτός δικτύου. Η σύνδεση μέσω αυτού του κόμβου θεωρείται πλέον ότι έχει καταστραφεί και όλες οι ομάδες κόμβων που επηρεάζονται από την απώλεια της συγκεκριμένης σύνδεσης ειδοποιούνται μέσω μηνύματος λάθους διαδρομής (Route Error, RERR).

<u>Διαχείριση του πίνακα διαδρομών</u>

Απαιτείται να διατηρούνται οι παρακάτω πληροφορίες για κάθε εγγραφή στον πίνακα διαδρομών

- Η διεύθυνση του κόμβου – παραλήπτη.
- Ο αύξων αριθμός για το συγκεκριμένο προορισμό.
- Αριθμός ενδιάμεσων κόμβων μέχρι τον παραλήπτη.

• Ο επόμενος κόμβος. Είναι ο γείτονας που έχει καθορισθεί για να προωθεί τα μηνύματα προς τον προορισμό για τη συγκεκριμένη εγγραφή διαδρομής.
• Διάρκεια κατά την οποία η διαδρομή θεωρείται έγκυρη.
• Λίστα ενεργών γειτόνων. Γειτονικοί κόμβοι που χρησιμοποιούν τη διαδρομή.
• Μνήμη αιτήσεων. Εξασφαλίζει ότι κάθε αίτηση επεξεργάζεται μια φορά.

Εύρεση διαδρομής

Ένας κόμβος εκπέμπει μία RREQ όταν χρειάζεται μια διαδρομή προς κάποιον προορισμό για τον οποίο δεν έχει διαθέσιμη διαδρομή. Αυτό μπορεί να συμβεί είτε γιατί η διαδρομή προς τον προορισμό είναι άγνωστη, είτε γιατί η ήδη γνωστή διαδρομή έχει εκπνεύσει. Μετά την εκπομπή της RREQ, ο κόμβος αναμένει για RREP. Αν η απάντηση δε φτάσει εντός συγκεκριμένου χρονικού ορίου, ο κόμβος που κάνει αίτηση διαδρομής μπορεί να στείλει νέα αίτηση ή να υποθέσει ότι δεν υπάρχει διαδρομή για το συγκεκριμένο προορισμό. Προώθηση των αιτήσεων διαδρομής από ένα κόμβο γίνεται όταν ο κόμβος που τις δέχεται δεν έχει υπολογισμένη διαδρομή προς τον προορισμό που του ζητείται. Ο κόμβος επίσης δημιουργεί μια προσωρινή αντίστροφη διαδρομή προς τον αρχικό αποστολέα στον πίνακα διαδρομών του με διεύθυνση επόμενου κόμβου τη διεύθυνσηαυτού που του έστειλε την RREQ. Αυτό γίνεται ώστε να είναι γνωστή η διαδρομή προς τον κόμβο που έκανε την αρχική αίτηση και να μπορεί να επιστραφεί η RREP στην περίπτωση που βρεθεί διαδρομή. Η διαδρομή είναι προσωρινή με την έννοια ότι ισχυει για πολύ λιγότερο χρόνο από μια πραγματική εγγραφή διαδρομής. Όταν η RREQ φτάσει στον προορισμό ή σε έναν κόμβο που έχει κάποια έγκυρη διαδρομή προς τον προορισμό δημιουργείται μία RREP και στέλνεται στον αρχικό αποστολέα. Όσο το μήνυμα προωθείται αντίστροφα, δημιουργείται η διαδρομή. Όταν το μήνυμα φτάσει στον αρχικό παραλήπτη έχει δημιουργηθεί μια έγκυρη διαδρομή από τον αποστολέα προς τον παραλήπτη.

Συντήρηση διαδρομής

Όταν ένας κόμβος ανιχνεύει ότι η διαδρομή προς κάποιο γειτονικό κόμβο δεν είναι πλέον έγκυρη, θα διαγράψει τη συγκεκριμένη εγγραφή και θα στείλει μήνυμα λάθους στην ομάδα των τερματικών που άμεσα χρησιμοποιούν τη συγκεκριμένη διαδρομή. Για το λόγο αυτό το AODV διατηρεί λίστα ενεργών γειτονικών κόμβων ώστε να ξέρει ποιοι από αυτούς χρησιμοποιούν μια συγκεκριμένη διαδρομή. Τα τερματικά που λαμβάνουν το μήνυμα επαναλαμβάνουν τη διαδικασία με τους γειτονικούς τους κόμβους. Το μήνυμα θα φτάσει τελικά και στον κόμβο που ζήτησε τη συγκεκριμένη διαδρομή οπότε το τερματικό μπορεί να αποφασίσει να σταματήσει να στέλνει δεδομένα ή να ζητήσει μια νέα διαδρομή στέλνοντας RREQ.

Ιδιότητες

Το πλεονέκτημα με το AODV συγκρινόμενο με τα κλασσικά πρωτόκολλα όπως διανύσματος απόστασης και κατάστασης σύνδεσης είναι ότι μειώνει σημαντικά τον αριθμό των μηνυμάτων δρομολόγησης στο δίκτυο. Το AODV το πετυχαίνει αυτό χρησιμοποιώντας reactive προσέγγιση. Αυτό κρίνεται απαραίτητο σε ένα ad hoc δίκτυο για να έχουμε καλή απόδοση εφόσον και η τοπολογία του δικτύου αλλάζει συχνά.

Το AODV έχει σχεδιαστεί για κινητά ad hoc δίκτυα με δεκάδες ή και εκατοντάδες κινητούς κόμβους. Μπορεί να αντιμετωπίσει καταστάσεις με χαμηλή, μέση και σχετικά υψηλή κινητικότητα των τερματικών, όπως επίσης και ποικιλία ρυθμών δεδομένων. Σχεδιάστηκε για να μειώσει τη διασπορά των δεδομένων ελέγχου και εξαλείψει τη μεταφορά πληροφοριών δρομολόγησης μαζί με τα δεδομένα επιβαρύνοντας το δίκτυο και μειώνοντας το χρήσιμο ρυθμό μετάδοσης. Έτσι βελτιώνεται η απόδοση και το δίκτυο προσαρμόζεται εύκολα σε αλλαγές της τοπολογίας όπως αλλαγή θέσης των κόμβων ή αυξομοιώσεις του αριθμού των τερματικών.

5.4.2 Δυναμική δρομολόγηση πηγής, Dynamic Source Routing, DSR

Το πρωτόκολλο DSR επίσης ανήκει στα reactive πρωτόκολλα και επιτρέπει στους κόμβους να βρουν δυναμικά μια διαδρομή προς όποιον προορισμό μέσω πολλαπλών ενδιάμεσων κόμβων.

Δρομολόγηση πηγής σημαίνει ότι κάθε πακέτο έχει γραμμένη τη λίστα των ενδιάμεσων κόμβων από τους οποίους πρέπει να περάσει. Το DSR δε χρησιμοποιεί περιοδικά μηνύματα δρομολόγησης. Βασίζεται στη βοήθεια του επιπέδου MAC, με την έννοια ότι το επίπεδο MAC ενημερώνει το πρωτόκολλο δρομολόγησης για λάθη στις συνδέσεις. Οι δυο βασικές μορφές λειτουργίας του DSR είναι η εύρεση διαδρομής και η συντήρηση των διαδρομών.

Εύρεση διαδρομής

Η εύρεση διαδρομής είναι ο μηχανισμός όπου ένας κόμβος Χ που επιθυμεί να στείλει ένα πακέτο σε ένα κόμβο Υ, αποκτά τη διαδρομή προς τον Υ. Ο κόμβος Χ ζητά μια διαδρομή εκπέμποντας ένα πακέτο RREQ. Κάθε κόμβος που δέχεται το RREQ ψάχνει στη μνήμη των αποθηκευμένων διαδρομών για μια διαδρομή προς τον ζητούμενο προορισμό. Το DSR αποθηκεύει όλες τις γνωστές διαδρομές στη μνήμη του τερματικού. Αν δε βρεθεί διαδρομή το τερματικό, προωθεί το RREQ και προσθέτει και τη δικιά του διεύθυνση στην αλληλουχία των διευθύνσεων των κόμβων από τους οποίους πέρασε το πακέτο. Η αίτηση συνεχίζει να μεταδίδεται μέσα στο δίκτυο ώσπου είτε φτάσει στον προορισμό, είτε σε ένα κόμβο με γνωστή τη διαδρομή προς τον προορισμό. Όταν αυτό συμβεί μια Απάντηση διαδρομής (Route Reply, RREP) στέλνεται πίσω στον αρχικό αποστολέα. Η RREP περιέχει και την αλληλουχία των ενδιάμεσων κόμβων μέσω των οποίων ο αποστολέας μπορεί να στείλει το μήνυμα στον παραλήπτη. Στη διαδικασία εύρεσης διαδρομής ένας κόμβος πρώτα στέλνει μια RREQ με το όριο ενδιάμεσων σταθμών στο 0. Αυτό αποτρέπει τους γειτονικούς σταθμούς που θα το λάβουν από το να το επανεκπέμψουν. Αυτός ο μηχανισμός επιτρέπει με κόστος ενός και μόνο πακέτου στον κόμβο να ψάξει στη μνήμη όλων των γειτονικών τερματικών για τη διαδρομή που θέλει. Επίσης οι κόμβοι μπορούν να λειτουργούν σε 'αδιάκριτη' μορφή επιτρέποντας τη λήψη πακέτων που μπορεί να μην προορίζονται για το συγκεκριμένο τερματικό. Οι διευθύνσεις που είναι γραμμένες πάνω στο πακέτο αναλύονται με σκοπό την εύρεση χρήσιμων διαδρομών ή μηνυμάτων λάθους και στη συνέχεια απορρίπτονται. Η διαδρομή προς τον αποστολέα μπορεί να ανακτηθεί με διάφορους τρόπους. Ο πιο απλός από αυτούς είναι αντιστρέφοντας την αλληλουχία των ενδιάμεσων σταθμών στο αρχείο του πακέτου. Αυτό προυποθέτει συμμετρικές συνδέσεις. Για να αντιμετωπιστεί το πρόβλημα το DSR ελέγχει τις αποθηκευμένες διαδρομές. Αν βρεθεί διαδρομή χρησιμοποιείται, αντί να ακολουθηθεί η διαδρομή της αντίστροφης πορείας. Άλλος τρόπος είναι η πληροφορία για τη διαδρομή να μεταφερθεί με μια RREQ που προορίζεται για τον αρχικό αποστολέα. Αυτό σημαίνει ότι το DSR μπορεί να υπολογίσει σωστές διαδρομές ακόμα και στην περίπτωση ασύμμετρων συνδέσεων.Από τη στιγμή που βρίσκεται μια διαδρομή αποθηκεύεται στη μνήμη του τερματικού μαζί με μία χρονική ένδειξη και ξεκινά η φάση της συντήρησης της διαδρομής.

Συντήρηση διαδρομής

Η συντήρηση της διαδρομής είναι ο μηχανισμός με τον οποίο ο αποστολέας του πακέτου S ανιχνεύει αλλαγές στην τοπολογία του δικτύου που δεν κάνουν πλέον δυνατή τη χρήση της διαδρομής προς τον προορισμό D. Αυτό μπορεί να συμβεί επειδή ένα τερματικό που βρίσκεται στη λίστα μιας διαδρομής, κινείται εκτός εμβέλειας ή τίθεται εκτός λειτουργίας κάνοντας τη διαδρομή μη χρησιμοποιούμενη πλέον. Μία σύνδεση με βλάβη μπορεί να ανιχθευθεί είτε ενεργά με παρακολούθηση των πακέτων επιβεβαίωσης, είτε παθητικά με τα τερματικά να διαβάζουν τα πακέτα που προωθούνται από τα γειτονικά τους τερματικά και να εξάγουν χρήσιμες πληροφορίες από τις διευθύνσεις που είναι αποθηκευμένες πάνω τους.

Όταν ανιχνευθεί πρόβλημα με μια διαδρομή που βρίσκεται σε χρήση, ένα πακέτο λάθους στέλνεται πίσω στον αρχικό κόμβο. Όταν το μήνυμα λάθους λαμβάνεται από τον κόμβο–αποστολέα ο κόμβος που δημιουργεί το πρόβλημα απομακρύνεται από τη μνήμη του τερματικού και όλες οι διαδρομές που χρησιμοποιούν τον προβληματικό κόμβο παύουν να ισχύουν.

Ιδιότητες

Το πρωτόκολλο DSR έχει το πλεονέκτημα ότι χρησιμοποιεί πληροφορίες δρομολόγησης που βρίσκονται στο τερματικό που αποστέλλει την πληροφορία. Οι ενδιάμεσοι κόμβοι δεν είναι απαραίτητο να διατηρούν ενημερωμένες πληροφορίες δρομολόγησης ώστε να δρομολογούν τα πακέτα που πρέπει να προωθήσουν. Επιπλέον δεν υπάρχει η υποχρέωση περιοδικών μηνυμάτων ενημέρωσης, με αποτέλεσμα να γίνεται καλύτερη εκμετάλλευση του εύρους ζώνης του καναλιού ειδικά στην περίπτωση που υπάρχει μικρή κινητικότητα των ασύρματων κόμβων. Παράλληλα υπάρχει μικρότερη σπατάλη της ενέργειας των ασύρματων κόμβων και με το να μη στέλονται περιοδικά μηνύματα και με το να μη λαμβάνονται και να υπόκεινται τη διαδικασία της επεξεργασίας. Έτσι οι κόμβοι μπορούν κατά τις περιόδους που δεν είναι ενεργοί να μπαίνουν σε διαδικασία αναμονής εξοικονομώντας ενέργεια.

Το πρωτόκολλο έχει το πλεονέκτημα ότι οι κόμβοι μαθαίνουν για τις διαδρομές ψάχνοντας για πληροφορίες στα πακέτα που λαμβάνουν. Μια διαδρομή από το Α στο Γ μέσω του κόμβου Β σημαίνει ότι το Α μαθαίνει τη διαδρομή προς το Γ αλλά ταυτόχρονα και τη διαδρομή προς το Β. Οι πληροφορίες για τη διαδρομή που κουβαλά το πακέτο σημαίνουν ότι το Β μαθαίνει τη διαδρομή προς τα Α και Γ και αντίστοιχα το Γ μαθαίνει τη διαδρομή προς Α και Β. Αυτή η μορφή ενεργούς μάθησης μειώνει τις επιπλέον πληροφορίες δρομολόγησης που αυξάνουν την κίνηση στο δίκτυο. Ωστόσο κάθε πακέτο κουβαλά μια επιπλέον πληροφορία για τη διαδρομή που έχει ακολουθήσει το πακέτο. Η επιπλέον πληροφορία μεγαλώνει όταν το πακέτο περνά πολλούς ενδιάμεσους σταθμούς μέχρι να φτάσει στον προορισμό του. Με τον τρόπο αυτό τα πακέτα θα είναι ελαφρώς μεγαλύτερα λόγω της πληροφορίας για τη διαδρομή.

Επίσης είναι σημαντικό ζήτημα για την ασφάλεια του δικτύου, το ότι τα τερματικά μπορούν να διαβάζουν πακέτα που δεν προορίζονται γι' αυτά με σκοπό να αποσπάσουν πληροφορίες δρομολόγησης. Ένας πιθανός εισβολέας θα μπορούσε να διαβάσει όλα τα πακέτα και να υποκλέψει πληροφορίες. Στην περίπτωση αυτή τα ανώτερα επίπεδα κάθε εφαρμογής οφείλουν να κρυπτογραφούν τις πληροφορίες πριν την αποστολή. Τα πρωτόκολλα δρομολόγησης αποτελούν πρωταρχικούς στόχους επιθέσεων προς την ασφάλεια των δικτύων και για το λόγο αυτό πρέπει και τα ίδια τα πρωτόκολλα να κρυπτογραφούνται.

5.4.3 Ο αλγόριθμος ARA

Βασικός αλγόριθμος μυρμηγκιών

Η βασική ιδέα του αλγορίθμου των μυρμηγκιών προέρχεται από τη μελέτη της συμπεριφοράς των μυρμηγκιών όταν ψάχνουν για την τροφή τους. Όταν τα μυρμήγκια ψάχνουν για τροφή ξεκινούν από τη φωλιά τους και προχωρούν προς την τροφή. Μόλις ένα μυρμήγκι φτάσει σε κάποια διασταύρωση στη διαδρομή που ακολουθεί πρέπει να αποφασίσει ποιο δρόμο θα ακολουθήσει. Ενώ περπατούν τα μυρμήγκια εναποθέτουν φερομόνη που σημαδεύει την επιλεγμένη διαδρομή. Η συγκέντρωση της φερομόνης σε ένα μονοπάτι είναι ένδειξη ότι αυτό χρησιμοποιείται. Με το πέρασμα του χρόνου η συγκέντρωση της φερομόνης μειώνεται λόγω φαινομένων εξάτμισης.

Η συμπεριφορά αυτή των μυρμηγκιών μπορεί να χρησιμοποιηθεί για την εύρεση του συντομότερου μονοπατιού σε δίκτυα. Ειδικά η δυναμική φύση της μεθόδου παρέχει μεγάλο βαθμό προσαρμογής στις αλλαγές της τοπολογίας των ασύρματων ad hoc δικτύων, εφόσον σε τέτοια δίκτυα καμία σύνδεση δεν μπορεί να είναι εγγυημένη και αλλαγές στις συνδέσεις συμβαίνουν συχνά. Ένας απλός αλγόριθμος εμπνευσμένος από τα μυρμήγκια.

Έστω G = (V,E) ένα προσανατολισμένο γράφημα με n = | V | κόμβους και Ε το σύνολο των δρόμων μεταξύ αυτών. Η απλή μετα-ευριστική μέθοδος της αποικίας μυρμηγκιών μπορεί να χρησιμοποιηθεί για την εύρεση του συντομότερου μονοπατιού μεταξύ του κόμβου αποστολέα vs και του κόμβου παραλήπτη vd στο γράφημα G. Το μήκος του δρόμου δίνεται από τον αριθμό των ενδιάμεσων κόμβων στο μονοπάτι. Η μεταβλητή φi,j (τεχνητή φερομόνη), η οποία τροποποιείται από τα μηρμύγκια όταν επισκέπτονται τον κόμβο, σχετίζεται με μια ακμή (,) e i j E∈ του γραφήματος που ενώνει τους κόμβους vi και vj

Τα ίχνη της φερομόνης γράφονται και διαβάζονται από τα ίδια τα μυρμήγκια. Η συγκέντρωση της φερομόνης φi,j αποτελεί ένδειξη της χρήσης του κόμβου από τα μυρμήγκια που προσπαθούν να βρουν τη βέλτιστη λύσηγια το μήκος της διαδρομής μεταξύ του αποστολέα και του παραλήπτη. Αρχικά η φi,j είναι σταθερή για κάθε ακμή e(i,j). Ένα μυρμήγκι που βρίσκεται στον κόμβο vi χρησιμοποιεί την τιμή της φερομόνης φi,j του κόμβου j i∈ v N για να υπολογίσει την πιθανότητα ο κόμβος vj να είναι ο επόμενος κόμβος. Ni είναι οι άμεσοι γείτονες του κόμβου vi. Οι πιθανότητες μετάβασης pi,j του κόμβου vi δηλαδή η πιθανότητα ότι το μυρμήγκι θα επιλέξει σαν επόμενο κόμβο τον vj μετά τον vi ορίζεται από τις ακόλουθες σχέσεις

$$p_{i,j} = \begin{cases} \dfrac{\varphi_{i,j}}{\sum_{j \in N_i} \varphi_{i,j}} & \text{αν } j \in N_i \\ 0 \text{ αν } j \notin N_i \end{cases} \qquad \textit{(Εξίσωση 5.1)}$$

$$\sum_{j \in N_i} p_{i,j} = 1 \ , \ i \in [1, N]$$

Κατά τη διαδικασία εύρεσης διαδρομής, τα μυρμήγκια εναποθέτουν φερομόνη στις ακμές. Στην απλούστερη μορφή του αλγορίθμου τα μυρμήγκια εναποθέτουν ένα σταθερό ποσό φερομόνης Δφ. Αυτό σημαίνει ότι το ποσό της φερομόνης στην ακμή e(vi,vj) όταν το μυρμήγκι κινείται από τον κόμβο vi στον κόμβο vj μεταβάλλεται όπως φαίνεται παρακάτω

$$\varphi_{i,j} = \varphi_{i,j} + \Delta\varphi \quad \textit{(Εξίσωση 5.2)}$$

Σύμφωνα με τον κανόνα αυτό ο οποίος προσομοιώνει την εναπόθεση φερομόνης από τα πραγματικά μυρμήγκια ένα μυρμήγκι που χρησιμοποιεί μια ακμή αυξάνει την πιθανότητα και άλλα μυρμήγκια να κάνουν χρήση της ακμής στο μέλλον. Για να αποφευχθεί η γρήγορη σύγκλιση των μυρμηγκιών προς κάποιο μη βέλτιστο μονοπάτι ένας επιπλέον μηχανισμός χρησιμοποιείται: οπως και η πραγματική φερομόνη έτσι και η τεχνητή εξατμίζεται με το χρόνο με αποτέλεσμα να μειώνεται η συγκέντρωσή της επιτρέποντας την εξερεύνηση διαφορετικών ακμών κατά τη διαδικασία της εύρεσης διαδρομής. Στην απλή μορφή του αλγορίθμου αυτή η μείωση εκφράζεται από την παρακάτω σχέση

$$\varphi_{i,j}(t+\tau) = (1-q) \cdot \varphi_{i,j}(t) \quad , \quad q \in (0,1] \qquad \textit{(Εξίσωση 5.3)}$$

Γιατί οι εμνευσμένοι από μυρμήγκια αλγόριθμοι είναι κατάλληλοι για ad hoc δίκτυα. Ο απλός αλγόριθμος που παρουσιάστηκε στην παραπάνω παράγραφο φανερώνει κάποιους από τους λόγους που κάνει τους συγκεκριμένους αλγόριθμους κατάλληλους για ασύρματα δίκτυα. Μερικοί από αυτούς τους λόγους είναι

<u>Δυναμική τοπολογία</u>

Η ιδιότητα αυτή των ασύρματων δικτύων είναι υπεύθυνη για τη φτωχή απόδοση των κλασσικών αλγορίθμων δρομολόγησης σε ασύρματα ad hoc δίκτυα. Ο αλγόριθμος των μυρμηγκιών βασίζεται σε αυτόνομα συστήματα πρακτόρων που μιμούνται τα πραγματικά μυρμήγκια. Αυτό επιτρέπει υψηλή προσαρμοστικότητα στην τοπολογία που κάθε στιγμή έχει το δίκτυο

Τοπική επεξεργασία

Σε αντίθεση με άλλες προσεγγίσεις δρομολόγησης ο συγκεκριμένος αλγόριθμος βασίζεται μόνο σε τοπικές πληροφορίες, ώστε να μην υπάρχει η ανάγκη για πίνακες δρομολόγησης ή πληροφορίες δρομολόγησης που πρέπει να εκπέμπονται περιοδικά.

Ποιότητα των συνδέσεων

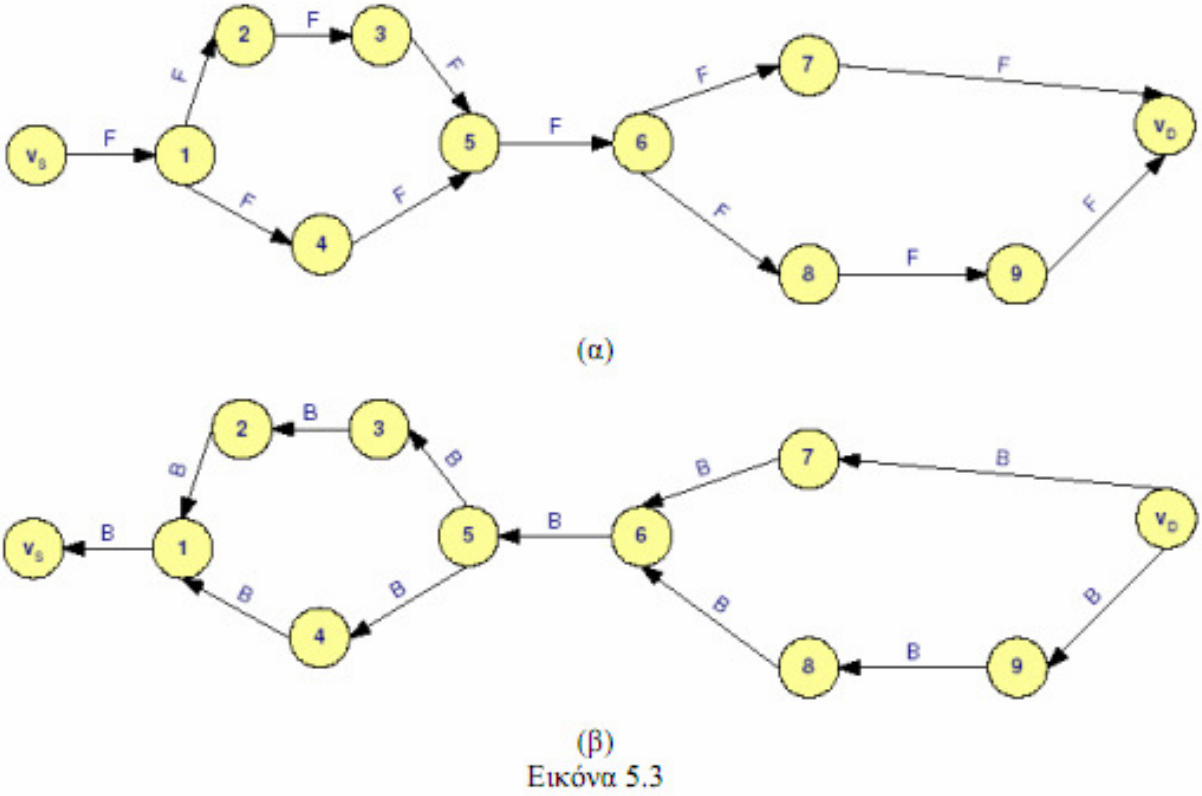
Είναι δυνατό να ενσωματώσουμε την πληροφορία για την ποιότητα μιας σύνδεσης στον υπολογισμό της συγκέντρωσης της φερομόνης. Αυτό θα βελτιώσει τη διαδικασία απόφασης λαμβάνοντας υπόψη την ποιότητα της σύνδεσης. Είναι σημαντικό να πούμε πως και ο ίδιος ο κόμβος ανεξάρτητα από τα μυρμήγκια μπορεί να μεταβάλλει τη συγκέντρωση της φερομόνης αν ανιχνεύσει κάποια αλλαγή στην ποιότητα της σύνδεσης

Υποστήριξη πολλαπλών δρόμων

Κάθε κόμβος έχει έναν πίνακα δρομολόγησης με εγγραφές για όλους τους γείτονες και τη συγκέντρωση της φερομόνης. Ο κανόνας απόφασης για τον επόμενο κόμβο βασίζεται στη συγκέντρωση φερομόνης στον κόμβο για κάθε πιθανή σύνδεση. Έτσι αυτή η προσέγγιση υποστηρίζει δρομολόγηση μέσω πολλαπλών δρόμων.

Εύρεση διαδρομής

Νέες διαδρομές δημιουργούνται κατά τη φάση εύρεσης διαδρομής. Η δημιουργία νέων διαδρομών απαιτεί ένα προς τα εμπρός κινούμενο μυρμήγκι (forward ant, FANT) και ένα προς τα πίσω κινούμενο μυρμήγκι (backward ant, BANT). Ένα FANT είναι ένας πράκτορας που αφήνει τα ίχνη της φερομόνης ξεκινώντας από τον κόμβο αποστολέα. Σε πλήρη αναλογία ένα BANT είναι ένας πράκτορας που ακολουθεί την αντίθετη διαδρομή από τον κόμβο παραλήπτη αφήνοντας τα ίχνη φερομόνης προς τον αρχικό κόμβο. Το FANT είναι ένα μικρό πακέτο με ένα μοναδικό αύξοντα αριθμό. Οι κόμβοι είναι σε θέση να ανιχνεύσουν διπλότυπα βασιζόμενοι στον αύξοντα αριθμό και τη διεύθυνση του αποστολέα. Ένας κόμβος που για πρώτη φορά λαμβάνει ένα FANT δημιουργεί μια εγγραφή στον πίνακα δρομολόγησής του. Μια καινούργια εγγραφή αποτελείται από τρία στοιχεία (διεύθυνση παραλήπτη, επόμενος κόμβος, ποσότητα φερομόνης). Ο κόμβος μεταφράζει τη διεύθυνση του αποστολέα που αναγράφεται στο FANT σαν διεύθυνση προορισμού, τη διεύθυνση του κόμβου από τον οποίο προήλθε το FANT σαν επόμενο κόμβο και υπολογίζει την ποσότητα της φερομόνης βασιζόμενος στον αριθμό των ενδιάμεσων κόμβων μέχρι το FANT να φτάσει στο συγκεκριμένο κόμβο. Στη συνέχεια προωθεί το FANT στους γειτονικούς του κόμβους. Τα FANT που λαμβάνονται για δεύτερη φορά ανιχνεύονται μέσω του αύξοντα αριθμού και απορρίπτονται. Όταν το FANT φτάσει στον προορισμό του ο κόμβος-παραλήπτης διαβάζει τις πληροφορίες που περιέχει και δημιουργεί ένα BANT το οποίο και στέλνει πίσω στον κόμβο-αποστολέα. Ο στόχος του BANT είναι όμοιος με αυτόν του FANT δηλαδή να δημιουργήσει μια διαδρομή μεταξύ αυτών των δύο κόμβων. Όταν ο αρχικός αποστολέας λάβει το BANT έχει δημιουργηθεί το μονοπάτι μεταξύ των δύο κόμβων και μπορεί να αρχίσει η αποστολή των πακέτων.



Εικόνα 5.3

Φάση εύρεσης διαδρομής του πρωτοκόλλου ARA (α) Ένα μυρμήγκι κατευθυνόμενο προς τα εμπρός (F) στέλνεται από τον κόμβο v_S στον κόμβο v_D. Το F περνάει από τους άλλους κόμβους αρχικοποιώντας τα δεδομένα των πινάκων δρομολόγησης και της φερομόνης (β) Το προς τα πίσω κατευθυνόμενο μυρμήγκι (B) έχει τον ίδιο σκοπό με το F. Το B στέλνεται από τον κόμβο v_D στον κόμβο v_S.

Στην παραπάνω εικόνα μπορούμε να δούμε τη φάση εύρεσης διαδρομής του πρωτοκόλλου ARA. Στην εικόνα (α) δημιουργείται το μονοπάτι που δείχνει από ποιο κόμβο vS έγινε η αποστολή αρχικά. Το FANT δημιουργεί ένα μονοπάτι προς τον αποστολέα στον κόμβο 6, αλλά δύο μονοπάτια στον κόμβο 5 μέσω των κόμβων 3 και 4. Η εικόνα (β) δείχνει μια παρόμοια κατάσταση για το BANT όπου έχουμε μια διαδρομή προς τον παραλήπτη στον κόμβο 5 και δύο στον κόμβο 6. Το παράδειγμα δείχνει ότι το πρωτόκολλο μπορεί να υποστηρίξει δρομολόγηση μέσω πολλαπλών διαδρομών.

<u>Συντήρηση της διαδρομής</u>

Η δεύτερη λειτουργία του αλγόριθμου δρομολόγησης είναι η συντήρηση της διαδρομής κατά τη διάρκεια της επικοινωνίας. Ο αλγόριθμος ARA δε χρειάζεται τη συνδρομή ειδικών πακέτων για το σκοπό αυτό. Από τη στιγμή που τα FANT και BANT έχουν δημιουργήσει τη διαδρομή τα τακτικά πακέτα πληροφορίας χρησιμοποιούνται για να διατηρήσουν τη διαδρομή. Όπως και στο αντίστοιχο βιολογικό πρότυπο, τα μονοπάτια που δημιουργούνται δε διατηρούν τις αρχικές τιμές φερομόνης για πάντα. Όταν ένας κόμβος ui προωθεί ένα πακέτο προς τον κόμβο uD μέσω του γειτονικού του κόμβου uj, αυξάνει την τιμή της φερομόνης της εγγραφής (uD, uj, φ) κατά Δφ. Αυτό σημαίνει ότι το συγκεκριμένο μονοπάτι ισχυροποιείται με κάθε πέρασμα ενός πακέτου πληροφορίας. Με τον ίδιο τρόπο ο επόμενος κόμβος uj αυξάνει την τιμή της φερομόνης της εγγραφής (uD, ui, φ) κατά Δφ με απότελεσμα και η αντίστροφη διαδρομή προς τον κόμβο-αποστολέα να ισχυροποιείται επίσης. Η εξάτμιση της φερομόνης που συμβαίνει στο πραγματικό πρότυπο μοντελοποιείται με μείωση της τιμής της φερομόνης σύμφωνα με την εξίσωση. Βασιζόμενοι στο παράδειγμα της εικόνας

δίνουμε ένα παράδειγμα της διαδικασίας που ακολουθείται στο πρωτόκολλο ARA. Ακολουθούν οι πίνακες δρομολόγησης των κόμβων 5 και 6.

Πίνακας δρομολόγησης κόμβου 5

Προορισμός	Επόμενος κόμβος	Φερομόνη
v_S	4	φ_1
v_D	6	φ_2
.	.	.
.	.	.
.	.	.

Πίνακας δρομολόγησης κόμβου 6

Προορισμός	Επόμενος κόμβος	Φερομόνη
v_S	5	$\varphi_3+\Delta\varphi$
v_D	7	φ_4
.	.	.
.	.	.
.	.	.

Τώρα γράφουμε τους πίνακες δρομολόγησης και των δύο κόμβων αφού ο κόμβος 5 έχει προωθήσει ένα πακέτο δεδομένων στον κόμβο 6. Μόνο η εγγραφή για τον κόμβο προορισμού vD αλλάζει στον πίνακα δρομολόγησης του κόμβου 5. Στον πίνακα δρομολόγησης του κόμβου 6 οι αλλαγές είναι ανάλογες. Μόνο η τιμή της φερομόνης για τον κόμβο αποστολής vS άλλαξε. Αυτό γίνεται με τον ίδιο τρόπο όπως στον κόμβο 5 για τον προορισμό.

Πίνακας δρομολόγησης κόμβου 5

Προορισμός	Επόμενος κόμβος	Φερομόνη
v_S	4	φ_1
v_D	6	$\varphi_2+\Delta\varphi$
.	.	.
.	.	.
.	.	.

Πίνακας δρομολόγησης κόμβου 6

Προορισμός	Επόμενος κόμβος	Φερομόνη
v_S	5	φ_3
v_D	7	φ_4
.	.	.
.	.	.
.	.	.

Η ποσότητα της φερομόνης μειώνεται σε τακτά χρονικά διαστήματα τ κατά μία σταθερή ποσότητα (1-q). Οι πίνακες δρομολόγησης των τερματικών μετά τη διαδικασία μείωσης της φερομόνης θα δείχνουν όπως παρακάτω

Πίνακας δρομολόγησης κόμβου 5 (μετά χρόνο τ)

Προορισμός	Επόμενος κόμβος	Φερομόνη
v_S	4	$\varphi_1(1-q)$
v_D	6	$(\varphi_2+\Delta\varphi)\ (1-q)$
.	.	.
.	.	.
.	.	.

Πίνακας δρομολόγησης κόμβου 6 (μετά χρόνο τ)

Προορισμός	Επόμενος κόμβος	Φερομόνη
v_S	4	$(\varphi_3+\Delta\varphi)\ (1-q)$
v_D	6	$\varphi_4(1-q)$
.	.	
.	.	.
.	.	.
		.

Αντιμετώπιση αποτυχίας διαδρομής

Το τρίτο σκέλος του αλγορίθμου είναι υπεύθυνο για την αντιμετώπιση αποτυχίας κάποιας διαδρομής που συμβαίνει συχνά λόγω κίνησης των κόμβων φαινόμενο αρκετά συχνό σε ασύρματα ad hoc δίκτυα. Υποθέτωντας ότι το επίπεδο MAC λειτουργεί με πρωτόκολλο 802.11 το πρωτόκολλο δρομολόγησης ARA αντιλαμβάνεται την αποτυχία μιας διαδρομής μέσω της έλλειψης πακέτου επιβεβαίωσης. Αν ένας κόμβος λάβει μήνυμα σφάλματος για κάποια διαδρομή (ROUTE_ERROR) απενεργοποιεί τη συγκεκριμένη σύνδεση θέτοντας την τιμή της φερομόνης που αναφέρεται στη σύνδεση στο 0. Στη συνέχεια ψάχνει στον πίνακα δρομολόγησης για εναλλακτική σύνδεση στον πίνακα δρομολόγησής του. Αν υπάρχει και άλλη διαδρομή προς τον προορισμό θα στείλει τα πακέτα μέσω αυτής. Αν όχι ο κόμβος ενημερώνει τους γείτονές του ελπίζοντας ότι μπορούν να προωθήσουν το πακέτο στον προορισμό του. Το πακέτο είτε θα φτάσει στον παραλήπτη είτε θα επιστραφεί στον αποστολέα. Αν το πακέτο δε φτάσει στον προορισμό του ο κόμβος αποστολέας πρέπει να αρχίσει νέα διαδικασία εύρεσης διαδρομής.

Ιδιότητες του πρωτοκόλλου ARA

Το πρωτόκολλο ARA καλύπτει πολλές από τις απαιτήσεις που έχουμε από ένα πρωτόκολλο δρομολόγησης ασύρματου δικτύου. Οι ιδιότητές του είναι

Διανεμημένη λειτουργία

Στο πρωτόκολλο ARA κάθε κόμβος έχει μια ομάδα από μετρητές φερομόνης φi,j στον πίνακα δρομολόγησης για μια σύνδεση μεταξύ των κόμβων ui και uj. Κάθε κόμβος ελέγχει τους μετρητές φερομόνης ενεξάρτητα όταν τα FANT και BANT επισκέπτονται τον κόμβο κατά τη φάση αναζήτησης διαδρομής ή όταν ο κόμβος ανιχνεύσει αποτυχία σε κάποια ήδη υπάρχουσα διαδρομή.

Αποφυγή βρόχων

Η χρήση αύξοντα αριθμού στα πακέτα που ψάχνουν για νέες διαδρομές εξασφαλίζουν την αποφυγή δημιουργίας βρόχων.

Λειτουργία βασισμένη στις ανάγκες

Οι διαδρομές δημιουργούνται με τη διαχείριση των μετρητών φερομόνης φi,j Με το χρόνο η ποσότητα φερομόνης μειώνεται όσο ο κόμβος δε χρησιμοποιείται για μετάδοση πακέτων. Η διαδικασία εύρεσης διαδρομής ενεργοποιείται μόνο μετά από απαίτηση συγκεκριμένου αποστολέα.

Περίοδος ανάπαυσης

Τα τερματικά μπορούν να περιέλθουν σε περίοδο ανάπαυσης στην περίπτωση που η τιμή της φερομόνης σε αυτά φτάσει το κατώτερο επίπεδο. Οι υπόλοιποι κόμβοι δεν θα θεωρούν τον κόμβο ενεργό εκτός και αν τα πακέτα προορίζονται γι' αυτό.

Τοπική λειτουργία

Οι πίνακες δρομολόγησης και οι στατιστικές πληροφορίες κάθε κόμβου είναι τοπικές και δεν εκπέμπονται προς άλλους κόμβους.

Πολλαπλές διαδρομές

Κάθε κόμβος διαθέτει διάφορες διαδρομές προς κάθε προορισμό. Η επιλογή συγκεκριμένης διαδρομής βασίζεται στην κατάσταση κάθε σύνδεσης, για παράδειγμα την ποιότητα κάθε σύνδεσης τη συγκεκριμένη χρονική στιγμή.

Επιπλέον πληροφορία στο πρωτόκολλο ARA

Η επιπλέον πληροφορία στο πρωτόκολλο αναμένεται να είναι μικρή εφόσον δεν ανταλλασσονται πίνακες δρομολόγησης μεταξύ των κόμβων. Αντίθετα με άλλους αλγόριθμους δρομολόγησης τα πακέτα FANT και BANT δε φέρουν μεγάλη πληροφορία. Μόνο ο αύξων

αριθμός μεταδίδεται με κάθε πακέτο. Η συντήρηση των διαδρομών γίνεται μέσω των πακέτων πληροφορίας δηλαδή από τις διευθύνσεις αποστολέα και παραλήπτη που υπάρχουν σε αυτά.

5.4.4 Destination Sequenced Distance Vector – DSDV

Ο αλγόριθμος DSDV είναι ένας βήμα προς βήμα αλγόριθμος με διανύσματα απόστασης όπου σε κάθε κόμβο έχει ένα πίνακα δρομολόγησης για όλους τους προορισμούς και αποθηκεύει τον επομένο κόμβο καθώς και τον αριθμό των ενδιάμεσων κόμβων προς κάθε προορισμό. Το πρωτόκολλο DSDV απαιτεί την περιοδική εκπομπή ανανεωμένων πληροφοριών δρομολόγησης στους γειτονικούς κόμβους. Το πλεονέκτημα του πρωτοκόλλου είναι ότι εγγυάται την αποφυγή δημιουργίας βρόχων.
Για να εγγυηθεί την αποφυγή βρόχων το DSDV χρησιμοποιεί έναν αύξοντα αριθμό για να σημειώσει κάθε διαδρομή. Οι αύξοντες αριθμοί είναι μία έκφραση του πόσο καινούρια είναι κάθε διαδρομή και για το λόγο αυτό διαδρομές με μεγαλύτερους αύξοντες αριθμούς προτιμώνται. Μια διαδρομή Δ προτιμάται από μια διαδρομή Δ΄ αν η Δ έχει μεγαλύτερο αύξοντα αριθμό, ή στην περίπτωση που οι διαδρομές έχουν τον ίδιο αύξοντα αριθμό η Δ προτιμάται στην περίπτωση που οι ενδιάμεσοι κόμβοι ως τον τελικό προορισμό είναι λιγότεροι. Ο αριθμός διαδρομής αυξάνεται κατά ένα στην περίπτωση που ένας κόμβος αντιληφθεί πως η διαδρμή παύει πλέον να ισχύει αλλά ο αριθμός των ενδιάμεσων κόμβων γίνεται άπειρος.

Ο αλγόριθμος δρομολόγησης DSDV ανήκει στην κατηγορία των αλγορίθμων διανύσματος απόστασης με μικρές τροποποιήσεις για να είναι κατάλληλος για ad hoc δίκτυα. Οι τροποποιήσεις αυτές περιλαμβάνουν περιοδικές ενημερώσεις για την κατάσταση του δικτύου που λόγω της κίνησης των τερματικών αλλάζει συνεχώς η τοπολογία του. Για να μειωθεί η ποσότητα της πληροφορίας σ'αυτά τα πακέτα υπάρχουν δύο τύποι μηνυμάτων ενημέρωσης: πλήρη μηνύματα και μηνύματα που περιλαμβάνουν τις αλλαγές από την τελευταία ενημέρωση.

Ιδιότητες

Επειδή το DSDV βασίζεται σε περιοδικές εκπομπές χρειάζεται κάποιο χρόνο για να συγκλίνει προτού κάποια διαδρομή αρχίσει να χρησιμοποιείται Αυτός ο χρόνος σύγκλισης είναι αμελητέος σε ένα στατικό ενσύρματο δίκτυο όπου η τοπολογία δεν αλλάζει συχνά. Ωστόσο σε ένα ασύρματο δίκτυο όπου η τοπολογία αλλάζει δυναμικά ο χρόνος σύγκλισης μπορεί να οδηγήσει σε μεγάλο αριθμό πακέτων που χάνονται μέχρι να βρεθεί μια διαδρομή. Επιπλέον η περιοδική εκπομπή των πληροφοριών δρομολόγησης προσθέτει μεγάλη ποσότητα επιπλέον πληροφορίας επιβαρύνοντας το δίκτυο.

5.4.5 Πρωτόκολλο δρομολόγησης με ζώνες, Zone Routing Protocol – ZRP

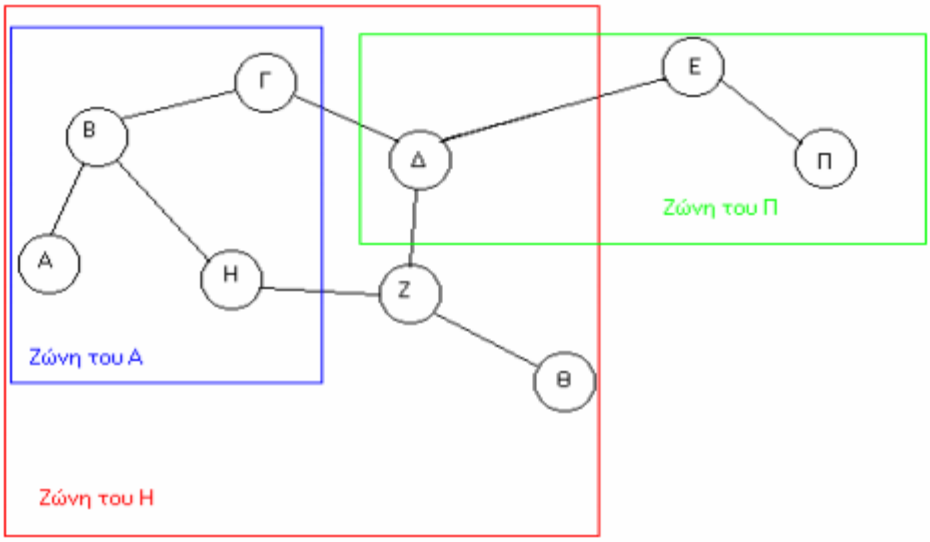
Περιγραφή

Το πρωτόκολλο ZRP είναι ένα υβριδικό που συνδιάζει ιδιότητες reactive και proactive πρωτοκόλλων. Χωρίζει το δίκτυο σε ζώνες δρομολόγησης και καθορίζει δυο πλήρως ανεξάρτητα πρωτόκολλα που λειτουργούν εντός και μεταξύ των ζωνών.Το Ενδοζωνικό Πρωτόκολλο Δρομολόγησης (Intrazone Routing Protocol – IARP) λειτουργεί μέσα στα όρια της ζώνης και σκοπός του είναι η γνώση των ελάχιστων αποστάσεων και των διαδρομών προς όλους τους κόμβους εντός της ζώνης. Το πρωτόκολλο που χρησιμοποιείται δεν καθορίζεται και μπορεί να είναι οποιοδήποτε από τα proactive πρωτόκολλα που αναφέρθηκαν. Ακόμη επιτρέπεται οι διαφορετικές ζώνες να λειτουργούν με ξεχωριστά πρωτόκολλα αρκεί αυτά να είναι περιορισμένα στα όρια της ζώνης. Αλλαγή στην τοπολογία προκαλεί πληροφορία που αποστέλλεται εντός της ζώνης αποφεύγοντας να επηρεάσει ολόκληρο το δίκτυο. Το δεύτερο πρωτόκολλο, το Διαζωνικό Πρωτόκολλο Δρομολόγησης (Interzone Routing Protocol – IERP) είναι reactive και χρησιμοποιείται για να βρίσκει διαδρομές μεταξύ των ζωνών. Αυτό είναι χρήσιμο όταν ο κόμβος

προορισμού και αποστολής δεν βρίσκονται στην ίδια ζώνη. Το πρωτόκολλο στην περίπτωση αυτή εκπέμπει μία Αίτηση Διαδρομής (Route REQuest – RREQ) σε όλους τους κόμβους που ελέγχουν μια ζώνη. Αν ο κόμβος προορισμού δεν βρίσκεται εντός της ζώνης τους προωθούν την αίτηση σε κόμβους των υπόλοιπων ζωνών. Η διαδικασία συνεχίζεται ωσότου το μήνυμα φτάσει στον προορισμό οπότε στέλνεται στον αποστολέα απάντηση που ουσιαστικά καθορίζει τη διαδρομή. Το IERP χρησιμοποιεί ένα πρωτόκολλο που ανταλλάσει πληροφορίες μεταξύ ακραίων κόμβων κάθε ζώνης.

Ζώνη Δρομολόγησης

Η ζώνη δρομολόγησης ορίζεται ως το σύνολο των κόμβων που βρίσκονται εντός καθορισμένης ελάχιστης απόστασης μετρημένης σε αριθμό βημάτων από ένα συγκεκριμένο κόμβο. Η απόσταση αυτή αναφέρεται ως η ακτίνα της ζώνης. Στο δίκτυο του παραδείγματος οι κόμβοι Α, Β, Γ, Δ, Ζ, Θ βρίσκονται σε απόσταση μικρότερη ή ίση των δύο βημάτων από τον κόμβο Η. Ο κόμβος Δ έχει δύο εναλλακτικές διαδρομές από τον Η. Η μία περιλαμβάνει τρεις ενδιάμεσους κόμβους και η άλλη δύο γι'αυτό και ο Δ περιλαμβάνεται στη ζώνη του Η. Περιφερειακοί κόμβοι ονομάζονται εκείνοι των οποίων η ελάχιστη απόσταση από τον κόμβο στον οποίο ανήκει η ζώνη είναι ίση με την ακτίνα της ζώνης. Στο παράδειγμα οι κόμβοι Γ και Η είναι περιφερειακοί κόμβοι όταν αναφερόμαστε στη ζώνη του Α. Θεωρούμε το δίκτυο με την τοπολογία του παραδείγματος. Έστω ο κόμβος Α θέλει να στείλει ένα πακέτο στον κόμβο Π. Εφόσον ο Π δεν είναι στη ζώνη δρομολόγησης του του Α στέλνεται αίτηση εύρεσης διαδρομής στους περιφερειακούς κόμβους Γ και Η. Με τη σειρά τους οι κόμβοι Γ και Η δεν βρίσκουν τον Π εντός της ζώνης δρομολόγησής τους οπότε προωθούν το μήνυμα στους περιφερειακούς ως προς αυτούς κόμβους. Ο Γ στέλνει την αίτηση στους Ε, Η, Ζ ενώ ο Η το στέλνει στους Θ, Δ, Γ. Τελικά ο ζητούμενος κόμβος Π βρίσκεται εντός της ζώνης δρομολόγησης του Δ και του Η οπότε ένα μήνυμα επεστρέφεται ακολουθώντας την αντίστροφη πορεία προς τον Α που περιέχει τη ζητούμενη διαδρομή.



Εικόνα 5.4
Ζώνες δρομολόγησης στο πρωτόκολλο ZRP

Για να αποφευχθεί η επιστροφή της αίτησης σε ζώνες από τις οποίες έχει ήδη περάσει σε κάθε τερματικό διατηρείται μια λίστα με αιτήσεις που έχουν ήδη ελεχθεί. Έτσι από τη στιγμή που μια αίτηση ληφθεί για δεύτερη φορά το γεγονός ανιχνεύεται και η αίτηση απορρίπτεται.

Ιδιότητες

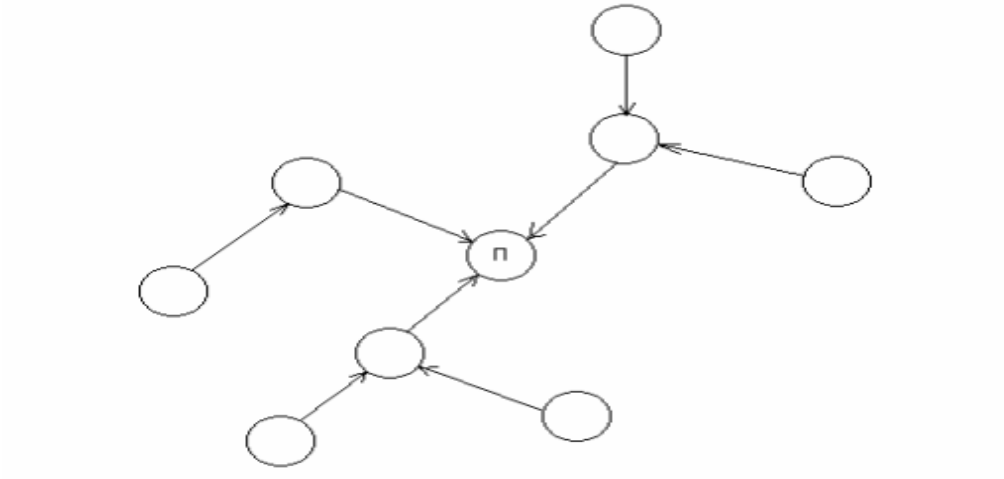
Το πρωτόκολλο ZRP είναι ένα αρκετά ενδιαφέρον πρωτόκολλο και μπορεί να προσαρμοσθεί στις ειδικές συνθήκες της τοπολογίας του δικτύου όπου θέλουμε να το εφαρμόσουμε (για παράδειγμα να μεταβληθει η διάμετρος της ζώνης). Ωστόσο αυτό δεν γίνεται δυναμικά παρά ανά περίσταση η κεντρική διαχείριση του δικτύου πρέπει να αποφασίζει για τη βέλτιστη λύση. Η απόδοση του πρωτοκόλλου εξαρτάται σε μεγάλο βαθμό από την επιλογή αυτή. Εφόσον το ZRP είναι υβριδικό proactive και reactive πρωτοκόλλων συνδιάζει τα πλεονεκτήματα και των δύο. Οι διαδρομές βρίσκονται πολύ γρήγορα όταν πρόκειται για κόμβους εντός της ζώνης δρομολόγησης. Για διαδρομές προς κόμβους εκτός ζώνης το τερματικό στέλνει αίτηση στα αντίστοιχα περιφερειακά τερματικά. Πρόβλημα ωστόσο αποτελεί το γεγονός ότι το πρωτόκολλο που χρησιμοποιείται εντός της ζώνης δεν καθορίζεται. Το γεγονός ότι περισσότερα από ένα πρωτόκολλα είναι δυνατό να χρησιμοποιούνται σε συνδιασμό με το γεγονός ότι πολλές ζώνες αλληλοκαλύπτονται σημαίνει ότι και τα τερματικά πρέπει να υποστηρίζουν όλα τα δυνατά πρωτόκολλα. Αυτό είναι αρνητικό για την απόδοση του δικτύου γι' αυτό είναι καλύτερο να χρησιμοποιείται το ίδιο πρωτόκολλο σε όλο το δίκτυο.

Το ZRP επίσης περιορίζει τη διάδοση της πληροφορίας για μια τοπική αλλαγή στην τοπολογία σε όλο το δίκτυο συμβάλλοντας έτσι στη μείωση της επιπλέον πληροφορίας με την οποία επιβαρύνεται (σε αντίθεση με τα proactive πρωτόκολλα που διαδίδουν την πληροφορία σε όλη την έκταση του δικτύου). Ωστόσο μια αλλαγή στην τοπολογία είναι δυνατό να επηρεάσει πολλές ζώνες.

5.4.6 Temporally Ordered Routing Algorithm – TORA

Περιγραφή

Το TORA είναι ένα διανεμημένο πρωτόκολλο δρομολόγησης. Ο βασικός αλγόριθμος κάτω από το TORA ανήκει στην οικογένεια των πρωτοκόλλων αντίστροφης σύνδεσης (link reversal protocols). Είναι έτσι σχεδιασμένο ώστε να ελαχιστοποιεί τις αντιδράσεις σε τοπολογικές αλλαγές. Η βασική σύλληψη του σχεδιασμού του είναι ότι τα μηνύματα ελέγχου περιορίζονται σε μια μικρή ομάδα κόμβων. Εγγυάται ότι οι διαδρομές δεν περιέχουν βρόχους αν και βρόχοι περιορισμένης διάρκειας είναι δυνατό να σχηματιστούν. Τυπικά παρέχει πολλαπλές διαδρομές για κάθε ζεύγος αποστολέα – παραλήπτη. Το πρωτόκολλο παρέχει μόνο το μηχανισμό δρομολόγησης και βασίζεται στο IMEP (Internet MANET Encapsulation Protocol) για την υλοποίηση των υπόλοιπων συναρτήσεων. Το TORA μπορεί να διαιρεθεί σε τρεις βασικές συναρτήσεις: δημιουργία, διατήρηση και διαγραφή διαδρομών. Η δημιουργία διαδρομών βασικά γίνεται με την ανάθεση κατευθύνσεων στις συνδέσεις ενός μη προσανατολισμένου δικτύου ή μέρους του δικτύου δημιουργώντας έτσι ένα προσανατολισμένο ακυκλικό γράφημα που οδηγεί στον προορισμό.



Εικόνα 5.5
Δημιουργία προσανατολισμένου γραφήματος στο πρωτόκολλο TORA. Το γράφημα είναι προσανατολισμένο προς κόμβους με χαμηλότερα ύψη (downstream).

Ο αλγόριθμος συνδέει ένα ύψος με κάθε κόμβο του δικτύου. Όλα τα μηνύματα στο δίκτυο 'ρέουν' προς τα κάτω δηλαδή από ένα κόμβο με μεγαλύτερο ύψος προς κάποιον με μικρότερο ύψος. Οι διαδρομές βρίσκονται χρησιμοποιώντας πακέτα Ερώτησης (Query - QRY) και Ενημέρωσης (Update - UPD). Όταν κάποιος κόμβος χωρίς συνδέσεις προς χαμηλότερα ύψη χρειάζεται μια διαδρομή προς κάποιο προορισμό θα εκπέμψει ένα πακέτο QRY. Το πακέτο αυτό θα διατρέξει το δίκτυο ωσότου φτάσει σε κάποιο κόμβο που έχει διαδρομή προς τον προορισμό ή στον ίδιο τον προορισμό. Ο κόμβος αυτός στη συνέχεια θα εκπέμψει ένα πακέτο που περιέχει το ύψος του. Κάθε κόμβος που λαμβάνει το πακέτο θα αυξήσει το ύψος του πάνω από αυτό που αναγράφεται στο UPD. Στη συνέχεια θα εκπέμψει το UPD με το δικό του ύψος. Αυτό θα έχει ως αποτέλεσμα τη δημιουργία μιας σειράς προσανατολισμένωνσυνδέσεων από τον αποστολέα προς τον προορισμό. Η παραπάνω διαδικασία μπορεί να οδηγήσει και σε πολλαπλές διαδρομές. Η συντήρηση των διαδρομών αναφέρεται στην αντίδραση του πρωτοκόλλου σε τοπολογικές αλλαγές με τέτοιο τρόπο ώστε οι διαδρομές προς τον προορισμό να αποκαθίστανται εντός περιορισμένου χρονικού διαστήματος, πράγμα που σημαίνει ότι τα προσανατολισμένα τμήματα του δικτύου πρέπει να δημιουργούν ένα προσανατολισμένο προς τον προορισμό γράφημα στο συγκεκριμένο χρόνο. Κατά την ανίχνευση της καταστροφής των συνδεσεων σε ένα τμήμα του δικτύου όλες οι συνδέσεις αυτού του τμήματος παύουν να είναι προσανατολισμένες για να διαγραφούν τυχόν άκυρες διαδρομές. Η διαγραφή των διαδρομών γίνεται με τη χρήση πακέτων διαγραφής (Clear – CLR messages).
Ιδιότητες

Τα πρωτόκολλα που υπάρχουν κάτω από τον αλγόριθμο αντίστροφης σύνδεσης θα αντιδράσουν στις αλλαγές των συνδέσεων με τοπικό και διανεμημένο τρόπο. Αυτό αποτρέπει τα μηνύματα CLR να διατρέξουν όλη την έκταση του δικτύου. Το γράφημα οδηγεί στον προορισμό με το μικρότερο ύψος. Ωστόσο το τερματικό που δημιουργεί την αίτηση QRY δεν έχει απαραίτητα το μεγαλύτερο ύψος. Αυτό μπορεί να οδηγήσει σε μια κατάσταση όπου πολλαπλές διαδρομές προς τον προορισμό είναι δυνατές αλλά μόνο μία βρίσκεται τελικά. Ο λόγος είναι ότι το ύψος αρχικά ορίζεται βασισμένο στην απόσταση, σε αριθμό ενδιάμεσων κόμβων, από τον προορισμό.

5.4.7 Internet MANET Encapsulation Protocol – IMEP

Περιγραφή

Το IMEP είναι ένα πρωτόκολλο σχεδιασμένο για να υποστηρίζει τη λειτουργία διαφόρων πρωτοκόλλων δρομολόγησης σε ad hoc δίκτυα. Η βασική ιδέα είναι η ύπαρξη ενός κοινού πρωτοκόλλου που θα μπορεί να χρησιμοποιηθεί από όλα τα πρωτόκολλα δρομολόγησης. Ενσωματώνει πολλούς μηχανισμούς που τα πρωτόκολλα των ανωτέρων στρωμάτων μπορεί να χρειαστούν. Αυτά μπορεί να είναι :

- Ανίχνευση κατάστασης σύνδεσης
- Συσσώρρευση και ενσωμάτωση των μηνυμάτων ελέγχου
- Αξιοπιστία μετάδοσης
- Ανάλυση διευθύνσεων του επιπέδου του δικτύου
- Είναι υπεύθυνο για την ασφάλεια μεταξύ των δρομολογητών αφού περιλαμβάνει τις διαδικασίες πιστοποίησης. Το IMEP παρέχει την αρχιτεκτονική για την ταυτοποίηση των δρομολογητών, ταυτοποίηση της διεπιφάνειας και τη διευθυνσιοδότηση. Στόχος του είναι η βελτίωση της συνολικής απόδοσης μειώνοντας τον αριθμό των μηνυμάτων ελέγχου και προσθέτωντας λειτουργικότητα δημιουργώντας ένα ενοποιημένο, γενικής χρήσης πρωτόκολλο χρήσιμο σε όλα τα πρωτόκολλα των ανώτερων επιπέδων. Η δομή του πρωτοκόλλου φαίνεται στο παρακάτω σχήμα

Εικόνα 5.6
Δομή του πρωτοκόλλου IMEP

5.5 ΑΝΑΛΥΣΗ ΚΑΙ ΣΥΓΚΡΙΣΗ ΑΛΓΟΡΙΘΜΩΝ

Υλοποιήσαμε τους Αλγορίθμους DSR και AODV με την βοήθεια των παρακάτω γράφων:

```
function [path,cost]=hopbyhop(start,stop,admatrix)

%Me ti voi8eia tis 8ewrias twn grafwn, mporoume na epekteinoyme ti xrisi
%tous gia ti dimiourgia enos hop routing epilegontas to epomeno hop me to
%megalytero dynato kostos.

%Dedomena:
%start = O komvos-pigi
%stop= O komvos-proorismos
%admatrix = H mitra dianysmatos

%E3agomena:
%To en logw monopati kai ta kosti tou
%[path,cost]=hopbyhop(start,stop,admatrix)

%Arxikopoiisi
noOfNodes = size(admatrix, 1);
rpath=[];
rpath(1)=start;
pathS=start;
parent=pathS;
cosy = 0;

%Elegxos ean to monopati stin pigi kai ton proorismo yparxei
[route]=hopsdij(pathS,stop,admatrix);
if (pathS~=stop && route ==1)
   %Edw xreiazomaste enan metriti na metraei tous "geitones" tou komvou
   k=1;
   %Kai enan gia ton ari8mo twn monopatiwn
   i=2;
   while(pathS~=stop)
      %Xrisi enos dianysmatos pou diatirei plirofories gia tous geitones
      %kai ta kosti twn monopatiwn
      B=[];
      jj=1;
      for j= 1:noOfNodes
```

```
          if admatrix(pathS, j)~=inf
             B(jj,1)=j;
             B(jj,2)=admatrix(pathS,j);
             jj=jj+1;
          end
       end
 B =sortrows(B,-2);
 %To epomeno hop me to megalytero kostos diadromis
 nexthop = B(k,1);
 chk = searchp(rpath,nexthop);
 if chk==1

[route]=hopsdij(nexthop,stop,admatrix);
      if(route==0)
        k=k+1;
      else
         rpath(i)=nexthop;
         pathS=nexthop;
         k =1;
         i=i+1;

      end
   else
     k = k+1;
 end
   end
else
   disp('source =dest or cannot reach destination')
end
path =rpath;    %Epilegmeno monopati
cost=0;
for d=2:length(path)
       cost= cost+admatrix(path(d-1),path(d));
end

%Mesos oros kostous monopatiou
cost=cost/length(path);

%Me8odos anazitisis komvwn pou episkef8ikame
function c =searchp(rp,np)
counter =0;
for z=1:length(rp)
   if np==rp(z)
      counter=counter+1;
   end
end
if counter>0
   c = 0;
else
   c = 1;
end

function [route]=hopsdij(pathS,stop,admatrix)
if admatrix(pathS,stop)~=0 || admatrix(pathS,stop)~=inf
   route=1;
else
   route=0;
end
return
```

```
function [r_path, r_cost] = dijkstra(pathS, pathE, transmat)

%O algori8mos gia tin kataskevi tis topologias xrisimopoiei protistws tin
%8ewria twn grafwn kai pio sygkekrimena ton algori8mo tou Dijkstra
%me entopismo kyklikwn monopatiwn.

%Oi parametroi pou xrisimopoiountai edw einai
%[path, cost]= dijkstra(pathStart, pathEnd,  transMatrix)

%me:
%pathS: To simeio-deiktis tou komvou arxis i alliws tou komvou-pigi me arxiki timi 1
%pathE: O deiktis tou komvou-proorismos, me arxiki timi 1
%transmat: H mitra dianysmatwn. O pinakas dld poy diatirei plirofories gia to
%poios komvos syndeetai me poion


%noOfNode: O ari8mos twn komvwn sto grafo
%parent(i): Ta dedomena tou patrikou komvou i
%distance(i):H kontinoteri apostasi, dld i apostasi me to mikrotero kostos apo to i sto pathS
%queue: Xrisimo gia tin diasxisi tou komvou kata platos kata tin anazitisi
%komvwn

noOfNode = size(transmat, 1);
for i = 1:noOfNode
  parent(i) = 0;
  distance(i) = inf;
end

queue = [];


%Ekkinisi apo ton pathS
for i=1:noOfNode
  if transmat(pathS, i)~=inf
    distance(i)=transmat(pathS, i);
    parent(i)=pathS;
    queue=[queue i];
  end
end

%Diasxisi grafou kata platos prwta
while length(queue) ~= 0
  hopS  = queue(1);
  queue = queue(2:end);
  for hopE = 1:noOfNode
      if distance(hopE)>(distance(hopS) + transmat(hopS,hopE))
      distance(hopE)=distance(hopS) + transmat(hopS,hopE);
      parent(hopE)=hopS;
      queue=[queue hopE];
    end
  end
end

distance
parent

%Back-trace to monopati me to mikrotero kostos
r_path=[pathE];
i=parent(pathE);
```

```
while i~=pathS && i~=0
  r_path=[i r_path];
  i=parent(i)
end

if i==pathS
  r_path=[i r_path];
else
  r_path=[];
end

%Epistrefei telika to kostos tou monopatiou
r_cost = distance(pathE);
```

Αλγόριθμος DSR

Κώδικας σε Matlab

```
function TDSR
%Dynamic Source Routing

%H me8odos vriskei monopatia apo ton komvo-pigi ston komvo-proorismo
%H e3odos toy programmatos einai ena diktyo (i kalytera mia topologia
%diktyou, to monopati apo tin pigi ston proorismo, to meso oro tou kostous
%twn diadromwn kai ton ari8mo twn "hops", dld sti logiki tis 8ewrias twn
%grafwn, o ari8mos twn vimatwn apo ton ena komvo ston allon)

clear;
noOfNodes  =10;
figure(1);
clf;
hold on;
R =5; % node transmission range
sor =1;%Komvos-pigi
des =10;%Komvos-proorismos
X = [1 2 3 4 8 6 7 9 10 10];%Tetmimenes twn komvwn
Y = [6 2 5 8 5 1 10 2 8 5];%Tetagmenes twn komvwn
Z =[1 1 0.7 0.4 0.1 0.1 0.1 1 1 1];%Ta kosti twn komvwn


%plotting network topology
for i = 1:noOfNodes
 plot(X(i), Y(i), '.');
    text(X(i), Y(i), num2str(i));
    for j = 1:noOfNodes
        distance = sqrt((X(i) - X(j))^2 + (Y(i) - Y(j))^2);
        if distance <= R % there is a link;
            matrix(i, j) =1;
            trust(i,j)=1-((Z(i)+Z(j))/2);
            line([X(i) X(j)], [Y(i) Y(j)], 'LineStyle', ':','LineWidth',5);
            matriz(i,j)=distance;
        else
            matrix(i, j) =inf;
            trust(i,j)= inf;
            matriz(i,j)=inf;
        end;

    end;
end;
```

```
[path, cost] = dijkstra(sor,des,trust);%finding the path from source to destination
trusted_path=path
trusted_path_trust=1-cost

trusted_path_hops=length(path)-1
trusted_path_distance=0;
for d=2:length(path)

   trusted_path_distance= trusted_path_distance + matriz(path(d-1),path(d));
end
trusted_path_distance

%plotting the selected path
for p =1:(length(path)-1)
    line([X(sor) X(path(1))],[Y(sor) Y(path(1))],'Color','r','LineWidth', 5, 'LineStyle', '=')
    line([X(path(p)) X(path(p+1))], [Y(path(p)) Y(path(p+1))],'Color','r','LineWidth',5, 'LineStyle','=')
end
grid
hold on
return;
```

Ο αλγόριθμος AODV

Κώδικας σε Matlab

```
function TAODV
%Ad Hoc On-demand Distance Vector routing protocol
%To programma einai sxediasmeno mesa se mia me8odo.
%H me8odos afti evriskei to monopati apo to node1 sto node10, opou einai o
%telikos komvos.

%H e3odos toy programmatos einai ena diktyo (i kalytera mia topologia
%diktyou, to monopati apo tin pigi ston proorismo, to meso oro tou kostous
%twn diadromwn kai ton ari8mo twn "hops", dld sti logiki tis 8ewrias twn
%grafwn, o ari8mos twn vimatwn apo ton ena komvo ston allon)

clc;
noOfNodes  =10;
figure(1);
clf;
hold on;
sor =1;%o prwtos komvos apo ton opoion 3ekiname
des=10;%o komvos-proorismos

R =5; %node transmission range
X = [1 2 4 4 8 6 7 9 10 10];%Oi tetmimenes twn komvwn
Y = [6 2 5 8 5 1 10 2 8 5 ];%Oi tetagmenes twn komvwn
Z =[1 0.1 0.6 0.8 0.6 0 0.1 1 1 1];%Ta kosti twn komvwn (trust values)

%plotting network topology
for i = 1:noOfNodes
 plot(X(i), Y(i), '.');
    text(X(i), Y(i), num2str(i));
    for j = 1:noOfNodes
        distance = sqrt((X(i) - X(j))^2 + (Y(i) - Y(j))^2);
        if distance <= R
            matrix(i, j) =1;
            trust(i,j)=(Z(i)+ Z(j))/2;
```

```
        line([X(i) X(j)], [Y(i) Y(j)], 'LineStyle', ':', 'LineWidth',5);
        matriz(i,j)=distance;
    else
        matrix(i,j) = inf;
        trust(i,j)= inf;
        matriz(i,j)=inf;
    end

  end
end
grid


%Evresi monopatiou apo tin pigi ston proorismo
[path,cost]=hop(sor,des,trust);
trusted_path=path
hopbyhop_cost=cost
trusted_path_hops=length(path)-1
trusted_path_distance=0;
for d=2:length(path)

  trusted_path_distance= trusted_path_distance + matriz(path(d-1),path(d));
end
trusted_path_distance

for p =1:(length(path)-1)
  line([X(sor) X(path(1))],[Y(sor) Y(path(1))],'Color','r','LineWidth', 5, 'LineStyle', '-')
  line([X(path(p)) X(path(p+1))], [Y(path(p)) Y(path(p+1))], 'Color','r','LineWidth', 5, 'LineStyle','-')

end
return
```

Έχοντας απεικονίσει στη MATLAB τα δύο αρχικά είδη αλγορίθμων για την ανάπτυξη δικτύων, τον Ad-Hoc on-demand distance Vector (AODV) και Dynamic Source Routing (DSR), θα δείξουμε στις επόμενες παραγράφους για τους υπόλοιπους αλγορίθμους την ειδοποιό διαφορά τους σε σχέση με τους προαναφερθέντες.

Ο αλγόριθμος ARA (Ant Routing Algorithm)

Ποια τα χαρακτηριστικά;

Όταν ένα πακέτο παραλαμβάνεται από το επίπεδο δικτύου του προτύπου OSI και δρομολογείται προς τα ανώτερα επίπεδα, ο κόμβος στον οποίο αναφερόμαστε ελέγχει αν οι πληροφορίες δρομολόγησης είναι διαθέσιμες για τον παραλήπτη του πακέτου.

Αν οι απαραίτητες πληροφορίες συμβαδίζουν με αυτές που έχει ο κόμβος στον δικό του πίνακα δρομολόγησης, προωθεί το πακέτο. Διαφορετικά, κάνει broadcasting ένα είδος μηνύματος που καλείται ant (μερμήγκι), ώστε να βρει το κατάλληλο μονοπάτι για τον συγκεκριμένο προορισμό. Αυτό το «μερμήγκι» έχει την ιδιότητα να πηγαίνει μόνο μπροστά, διαγράφοντας μια νοητή τροχιά, ανάλογα με το ποιούς κόμβους θα συναντήσει μπροστά του ως τον τελικό κόμβο.

Αν ο κάθε ενδιάμεσος κόμβος έχει ξανασυναντήσει το «μερμήγκι», το παραβλέπει. Αλλιώς, το «σκοτώνει». Όταν τελικά φτάσει στον προορισμό του, τότε αλλάζει ιδιότητα και κατευθύνεται «με την όπισθεν» μέχρι την πηγή ή «φωλιά». Αν τώρα οι ενδιάμεσοι κόμβοι ξαναείδαν το «μερμήγκι» το παραβλέπουν, διαφορετικά ενημερώνουν τους πίνακες δρομολόγησής τους ανάλογα με το πόσα βήματα έκανε το «μερμήγκι» ως τον κόμβο τους και στη συνέχεια το προωθούν παρακάτω.

Τί αλλάζει;

Παίρνοντας για παράδειγμα τον αλγόριθμο AODV, για την εύρεση του κατάλληλου μονοπατιού, συγκρίνει όλα τα κόστη των δρομολογίων, πριν επιλέξει τον κατάλληλο. Ο αλγόριθμος ARA, θα μπορούσαμε να πούμε ότι «αντιγράφει τη Φύση» σχετικά με την συμπεριφορά του, απλά επιλέγοντας αυτό που θα βρεθεί μπροστά του.

Για να κατανοηθεί αυτό, θα πρέπει να ρίξουμε μια ματιά στα τεχνικά χαρακτηριστικά του. Πρωτίστως, αυτός ο αλγόριθμος δεν αποστέλλει πακέτα αναγνώρισης και αποκατάστασης επικοινωνίας μεταξύ των «γειτόνων» του. Παρατηρούμε πως ο αλγόριθμος αν και βρίσκει το συντομότερο μονοπάτι μεταξύ πηγής και προορισμού, εν αντιθέσει με τον AODV, δεν θεωρείται τόσο ανταγωνιστικός.

Ποια τα θετικά του αλγορίθμου;

Είναι γνωστό πως σε θέματα δικτύων τέτοιου είδους ερωτήσεις δεν υφίστανται. Μπορεί να κερδίζουμε κάτι από έναν αλγόριθμο, αλλά να χάνουμε σε κάτι άλλο. Θέτοντας αυτή την ερώτηση σε σχέση με τους δυο υλοποιημένους αλγορίθμους, το πρώτο θετικό είναι πως δεν αποστέλλει πακέτα αναγνώρισης. Πράγμα που σημαίνει πως δεν φορτώνει το μέσο με περιττά μηνύματα.

Ως αλγόριθμος, θα λέγαμε ότι είναι καθαρά «αντανακλαστικός». Ας μεταφέρουμε την έννοια των δικτύων, στα δίκτυα που δημιουργούνται μέσω των νευρώνων στον ανθρώπινο εγκέφαλο, ώστε να κατανοήσουμε πλήρως της χρησιμότητά τους.

Ο κάθε αλγόριθμος είναι σαν ένας τρόπος να αντιλαμβάνεται ένα τέτοιο δίκτυο τον εξωτερικό κόσμο, παρέχοντας ερεθίσματα. Στο παράδειγμά μας, το δίκτυο θα βοηθήσει τον εγκέφαλο να αναγνωρίζει τα αντικείμενα που έχει μπροστά του, ή πιο απλά, ότι μπροστά του υπάρχει κάποιο εμπόδιο.

Ο άνθρωπος, προχωράει μόνο μπροστά, χωρίς να νοιάζεται για τα υπόλοιπα αντικείμενα τριγύρω. Μόλις συναντήσει ένα αντικείμενο, «σκοντάφτει» επάνω του. Τα αντανακλαστικά θα μεταφέρουν μαζί με τον πόνο, την πληροφορία πως εκεί βρέθηκε ένα αντικείμενο. Στην συνέχεια, το δίκτυο θα αρχίσει να εξετάζει τί είδους εμπόδιο συνάντησε. Έτσι κάθε φορά που θα προχωράει μπροστά και σκοντάφτει κάπου, θα καταλαβαίνει ότι βρήκε ένα εμπόδιο.

Στο επόμενο βήμα, το δίκτυο διατηρεί έναν μετρητή, ώστε να υπολογίζει στα πόσα βήματα από το προηγούμενο εμπόδιο βρήκε πάλι εμπόδιο. Έτσι, όταν τελικά θα φτάσει στον προορισμό του, θα κατασκευάσει ένα είδους «πίνακα δρομολόγησης». Γυρνώντας ο άνθρωπος στη συνέχεια προς τα πίσω, θα είναι σε θέση να αναγνωρίζει από ποια σημεία πέρασε και πόσα βήματα έκανε.

Από τα παραπάνω καταλαβαίνουμε ότι είναι ένας αλγόριθμος που βασίζεται στην «εμπειρία», αντιγράφοντας το φυσικό περιβάλλον. Είναι μια καλή μορφή για πειραματισμούς, αφού περικλείει όλο το φάσμα των πρωτοκόλλων δρομολόγησης.

Ποια τα αρνητικά στοιχεία;

Εδώ θα μπορούσαμε απλά να πούμε ότι ο αλγόριθμος ARA δεν ανήκει στους ανταγωνιστικούς αλγορίθμους, οι οποίοι γνωρίζουνε εξ΄αρχής το κόστος κάθε διαδρομής μέχρι και τον προορισμό, ώστε τελικά να επιλέξουν το κατάλληλο μονοπάτι.

Ο αλγόριθμος DSDV (Destination Sequenced Distance Vector)

Ποιά τα χαρακτηριστικά;

Επειδή έχουμε να κάνουμε με ad-hoc δίκτυα και με κινητούς (ή κινούμενους) υπολογιστές, κάθε ένας από αυτούς μπορεί να συνδέεται με τους άλλους μέσω ενός υπολογιστή βάσης. Κάθε ένας τέτοιος υπολογιστής ορίζει την εμβέλειά του, ή αλλιώς τη «γειτονιά» του. Ο κινητός υπολογιστής, μπορεί να κινείται οπουδήποτε μέσα στο χώρο της ίδιας γειτονιάς, ή σε κάποια άλλη γειτονιά.

Για να γίνει πιο αντιληπτό αυτό, παραθέτουμε την παρακάτω εικόνα που δείχνει ένα δυναμικό δίκτυο, όπου οι κόμβοι μετακινούνται τόσο στη δική τους «γειτονιά», όσο και σε διαφορετική.

Τί γίνεται λοιπόν στην περίπτωση που έχουμε ένα τόσο δυναμικό περιβάλλον;

Οι προηγούμενοι αλγόριθμοι δεν έχουν τόσο μεγάλη ευελιξία, ώστε να χρησιμοποιηθούν σε ένα δίκτυο που ένας κόμβος υπάρχει υποχρεωτικά μπροστά από κάποιον άλλον, όπως στην περίπτωση του ARA. Εδώ χρειάζονται «ανοιχτοί ορίζοντες», δηλαδή στην περίπτωση ενός δικτύου, να γνωρίζουμε όλες τις πιθανές διαδρομές που μπορεί να ακολουθήσει ένα μήνυμα, προκειμένου να φτάσει στον προορισμό του.

Έτσι φτάνουμε στην ιδέα της διατήρησης ενός πίνακα με στοιχεία δρομολόγησης, ο οποίος με κάποιο τρόπο θα πρέπει να ενημερώνεται πολύ συχνά (έστω κάθε 1 λεπτό), ώστε να ελέγχεται η μετακίνηση κόμβων από το σημείο που βρισκόταν (γιατί ακόμη και στην ίδια «γειτονιά» να βρίσκεται ο υπολογιστής, μπορεί να μετακινηθεί σε μια θέση πιο μακρυά ή πιο κοντά σε σχέση με τη βάση, οπότε καταλαβαίνουμε πως αλλάζει και το κόστος της απόστασης για ολόκληρο το μονοπάτι). Η πρώτη προσπάθεια ανάπτυξης του αλγορίθμου έγινε με τη βοήθεια του γνωστού αλγόριθμου διανύσματος-απόσταση, ή αλλιώς του Bellman-Ford. Ένας κατανεμημένος (distributed) αλγόριθμος εύρεσης συντομότερης διαδρομής.

Ο αλγόριθμος που εξετάζουμε έχει πάρει πολλά από τα στοιχεία του Bellman-Ford, του οποίου η χρήση βασίζεται αποκλειστικά στους πίνακες δρομολόγησης με όλα τα μονοπάτια. Κάθε κόμβος, γνωρίζει τους άμεσα συνδεδεμένους κόμβους, αποδίδοντας ένα κόστος απόστασης ίσο με 0, δηλαδή 0 hops για να φτάσει το μήνυμα σε αυτούς. Έτσι, πρέπει ανά τακτά χρονικά διαστήματα να αποστέλλει ο ένας κόμβος στον άλλο τέτοιου είδους μηνύματα, ώστε να καλύψουν την περίπτωση που ένας κόμβος μετακινήθηκε ή αναιρέθηκε, ή ακόμη και αν προστέθηκε κι άλλος.

Τί αλλάζει;

Με λίγα λόγια, οι παραπάνω κόμβοι αποστέλλουν κάθε φορά ένα αντίγραφο του πίνακα δρομολόγησής τους, ούτως ώστε να γίνεται ενημέρωση δρομολογίων και κόστους απόστασης.

Απώτερος λοιπόν σκοπός του αλγορίθμου, είναι να μπορεί ένας υπολογιστής να ανταλλάσσει μηνύματα με κάποιον άλλον υπολογιστή της «ομάδας» στην οποία βρίσκεται προσωρινά, ακόμη και αν ο προορισμός του μηνύματος βρίσκεται εκτός εμβέλειας. Τούτο επιτυγχάνεται με τρόπο εύρεσης συντομότερου μονοπατιού που παρέχει ο Bellman-Ford. Βασική προϋπόθεση, ένας υπολογιστής να αποστέλλει δεδομένα, όποτε αυτό του ζητηθεί.

Αυτό που το διαφοροποιεί από τον απλό αλγόριθμο διανύσματος –απόστασης, είναι πως όλες οι μέθοδοι δρομολόγησης αναπτύσσονται στο $2^{ο}$ επίπεδο του TCP/IP, που δεν είναι κατά παράδοση το επίπεδο για ζητήματα δρομολόγησης. Παρακάτω παραθέτουμε μια εικόνα με τα 5 επίπεδα του πρωτοκόλλου TCP/IP.

Εντελώς εγκυκλοπαιδικά αναφέρουμε πως το επίπεδο Network Interface είναι υπεύθυνο για τη λήψη πακέτων IP (δηλαδή IP frames με τις πληροφορίες Διεύθυνσης IP, την θύρα και τέλος τα δεδομένα) και τη μεταφορά τους σε κάποιο δίκτυο. Το πακέτο πληροφορίας για τους πίνακες δρομολόγησης, όταν ταξιδεύει από τον έναν υπολογιστή στον άλλον, συμπεριλαμβάνει στην κεφαλίδα του (header), πέρα από τις διευθύνσεις υλικού (hardware) και δικτύου. Για να αντιμετωπιστεί το πρόβλημα των μη ανανεωμένων πινάκων δρομολόγησης (λόγω του Bellman-Ford), κάθε πίνακας δρομολόγησης διαθέτει ένα σειριακό αριθμό που παράγεται από τον

υπολογιστή που απέστειλε τα δεδομένα. Αυτός ο σειριακός αριθμός είναι μοναδικός για κάθε πακέτο.

Όταν ένα πακέτο καταφθάνει στον δέκτη, γίνεται πρώτα σύγκριση του σειριακού αριθμού σε σχέση με τα προηγούμενα πακέτα που έλαβε, ώστε να δει ποιός από αυτούς είναι ο πιο πρόσφατος. Έτσι ο δέκτης «έχει ένα πλάνο στο μυαλό του» σχετικά με την δρομολόγηση, ώστε να πάρει τις κατάλληλες αποφάσεις κατά την προώθηση των πακέτων. Στην περίπτωση που δυο σειριακοί αριθμοί είναι ίδιοι, άρα δυο μονοπάτια έχουν τον ίδιο σειριακό αριθμό, τότε επιλέγεται αυτός με το μικρότερο κόστος μονοπατιού.

Ποια τα θετικά;

Σαν ιδέα, ο DSDV υπόσχεται να επιλύσει προβλήματα σχετικά με τα ad-hoc δίκτυα, προκειμένου να μπορεί κάποιος ασύρματος υπολογιστής που δεν βρίσκεται κοντά σε κάποιον υπολογιστή-βάση, να ανταλλάσσει δεδομένα ακόμα και σε δίκτυα που αλλάζουν συνεχώς ή ακόμη και σε αυθαίρετα (arbitrary) δίκτυα.

Η διατήρηση πληροφοριών σε πίνακες δρομολόγησης είναι καλή μέθοδος γνώσης του τί πραγματικά συμβαίνει στο δίκτυό μας.

Ποια τα αρνητικά;

Όπως είπαμε και προηγουμένως, ο DSDV έχει πάρει πολλά στοιχεία του Bellman-Ford. Πράγμα που σημαίνει ότι δεν έχει πάρει μόνο τις θετικές ιδιότητές του, αλλά πολλές και από τις «ιδιορρυθμίες» του.

Αρχικά, η δυσκολία έγκειται στο ότι πρέπει να είναι γνωστά όλα τα δρομολόγια, πράγμα που είναι πολλές φορές δύσκολο σε δυναμικά δίκτυα με πολλές αλλαγές. Ως εκ τούτου, ο αλγόριθμος δεν μπορεί να ανταπεξέλθει, καθώς βαδίζει σχετικά πιο αργά με τα γεγονότα που συμβαίνουν.

Επειδή λοιπόν και ο Bellman-Ford δεν κλιμακώνεται καλά λόγω του τύπου δρομολόγησης, περιμένουμε κάτι ανάλογο και από τον DSDV. Πολλές έρευνες πάνω στον συγκεκριμένο αλγόριθμο, μένουν στο σημείο των θετικών χαρακτηριστικών του, με σχόλια ή υποσημειώσεις του τύπου «δεν θα αναλύσουμε την δυσκολία και τους χρόνους δρομολόγησης του Bellman-Ford. Θεωρούμε ότι εφαρμόζεται σε ένα δίκτυο μετρίως δυναμικό»

Αναφορικά με τον host που ανταλλάσσει μηνύματα με τον κινούμενο υπολογιστή (ή ακόμα και με τον host που ανταλλάσσει μηνύματα με κάποιον άλλο host), ο συγχρονισμός είναι άλλες φορές σχετικά μεγάλος και άλλες πάλι φορές σχετικά μικρός. Ο Bellman-Ford δεν έχει και την καλύτερη φήμη πάνω σε αυτόν τον τομέα, οπότε μάλλον και ο χρόνος που χρειάζεται για να συγχρονιστούν οι κόμβοι με τον DSDV, θα είναι και αυτός μεγάλος.

Απόρροια όλων των παραπάνω, μοιραία οι κόμβοι θα έχουν λανθασμένες πληροφορίες στους πίνακές τους. Που συνεπάγεται μεγαλύτερος χρόνος μεταφοράς μηνύματος (αφού πρέπει να γίνεται και έλεγχος ορθότητας του μονοπατιού που επέλεξε το μήνυμα), οπότε θα έχουμε και περισσότερα σφάλματα (failures) δικτύου, με συχνές απορρίψεις ακόμη και κρίσιμων πακέτων, προτού καν φτάσουν στον προορισμό τους. Άρα, θα έχουμε και μεγάλες χρηματικές απώλειες.

Ο αλγόριθμος TORA (Temporally Ordered Routing Algorithm)

Ποια τα χαρακτηριστικά;

Ανήκοντας και αυτός γενικά στα on-demand πρωτόκολλα, έρχεται υποσχόμενο να μειώσει τον χρόνο απόκρισης (ή χρόνο αντίδρασης) στις πολλαπλές αλλαγές τοποθεσίας στα δυναμικά δίκτυα, καθώς επίσης να περιορίσει τα μηνύματα ελέγχου μεταφοράς μέσα σε αυτά.

Λειτουργεί οργανώνοντας την τοπολογία δικτύου σαν ένα γράφο. Για να κατανοήσουμε τις έννοιες που ακολουθούν, πρέπει να κάνουμε μια μικρή αναφορά στην θεωρία των γράφων.

Γράφος είναι μια δομή, η οποία απαρτίζεται από κορυφές (τους κόμβους) και ακμές. Κάθε ακμή, μπορεί να έχει ένα συγκεκριμένο κόστος ή όχι. Ακριβώς όπως συμβαίνει και στα δίκτυα μεταξύ των κόμβων. Έτσι ένας γράφος μπορεί να αντιπροσωπεύει ένα δίκτυο με καλύτερο τρόπο αναφορικά με την σχηματική του αναπαράσταση.

Κάθε κόμβος μπορεί να έχει τους γείτονές του, ή και την ομάδα του. Αυτό καθορίζεται από το αν είναι ενωμένοι μεταξύ τους με κάποια ακμή. Μόνο οι κόμβοι που είναι συνδεδεμένοι μεταξύ του με ακμή μπορούν να επικοινωνήσουν. Η επικοινωνία μεταξύ τους είναι αμφίδρομη. Δηλαδή γίνεται και προς τις δύο κατευθύνσεις. Κάτι ανάλογο με τη full duplex επικοινωνία στις τηλεπικοινωνίες. Ένα τέτοιο σχεδιάγραμμα φαίνεται στην παρακάτω εικόνα:

Έτσι για παράδειγμα ο κόμβος 1 μπορεί να επικοινωνήσει μόνο με τους γείτονες 2 και 3, ενώ ο 6 μπορεί να επικοινωνήσει με τους 3 και 4, αφού και οι δυο είναι συνδεδεμένοι με αυτόν.

Αν η επικοινωνία προϋποθέτει μετακίνηση πληροφοριών όπως τα πακέτα εντός κάποιου δικτύου, θέλουμε τα δεδομένα που κινούμε να έχουν ένα συγκεκριμένο αποστολέα και παραλήπτη. Επομένως, χρειάζεται με κάποιον τρόπο να τους «δείχνουμε το δρόμο» που πρέπει να ακολουθήσουν κάθε φορά.

Επομένως στον παραπάνω γράφο πρέπει να κάνουμε μια μικρή τροποποίηση, βάζοντας σε κάθε μια ακμή ένα βέλος, ώστε να δείχνουμε την κατεύθυνση την οποία υποχρεωτικά πρέπει να πάρουν τα δεδομένα αποστολής.

Έτσι τώρα για να μεταδώσει για παράδειγμα ο κόμβος 2 ένα μήνυμα στον κόμβο 6, θα πρέπει να ακολουθήσει τη διαδρομή 2-1-3-6 ή 2-1-3-4-6. Γίνεται αντιληπτό πως αυτός ο τρόπος απαγορεύει την «full-duplex» επικοινωνία που είχαμε προηγουμένως. Ο γράφος αυτός καλείται κατευθυνόμενος γράφος και είναι μια απ' τις τεχνοτροπίες που ακολουθεί ο αλγόριθμος TORA (όπως επίσης και τον μη κατευθυνόμενο).

Επιστρέφοντας στα χαρακτηριστικά του αλγορίθμου, οι κόμβοι του λοιπόν μπορεί να βρίσκονται σε μια από τις παρακάτω καταστάσεις:

1. Μη κατευθυνόμενοι (Undirected), οπότε έχουμε και τους μη κατευθυνόμενους γράφους
2. Κατευθυνόμενοι (Directed - Upstream), δηλαδή κατευθυνόμενος γράφος και
3. Αντιστρεπτός κατευθυνόμενοι (Directed - Dowstream)

Η τελευταία κατάσταση είναι όπως ο κατευθυνόμενος γράφος, μόνο που τα βέλη του δείχνουν στην αντίθετη κατεύθυνση από αυτή που έδειχναν στους κατευθυνόμενους. Για να γίνεται διαχωρισμός των μεν με τα δε, έχει υιοθετηθεί ο όρο upstream δεδομένα, όταν μεταφέρονται σε κατευθυνόμενο γράφο και downstream δεδομένα, όταν μεταφέρονται σε αντιστρεπτός κατευθυνόμενο γράφο.

Ο TORA ανήκει σε μια ξεχωριστή κλάση αλγορίθμων που ονομάζονται link reversal. Αν στον παραπάνω γράφο καταργηθεί κάποιος κόμβος – έστω ο 4-τότε αλλάζει φορά στις κατευθύνσεις τον ακμών που αφορούν τον κατηργημένο κόμβο.

Η αντιστροφή των κόμβων μπορεί να είναι ολική, αντιστρέφοντας όλες τις ακμές που είχαν αναφορά στον κατηργημένο κόμβο, ή μερική, αντιστρέφοντας μόνο τις ακμές που δείχνουν προς αυτόν.

Οι βασικές προϋποθέσεις που πρέπει να ισχύουν για να λειτουργήσει ο συγκεκριμένος αλγόριθμος, είναι οι εξής:

1. Όλοι οι κόμβοι αναγνωρίζουν τους γείτονές τους με χρήση κάποιου link-state πρωτόκολλο που λειτουργεί στο επίπεδο σύνδεσης
2. Όλα τα πακέτα πληροφοριών έχουν παραληφθεί με τη σειρά (άλλωστε η λογική του γράφου είναι η απόλυτη κατάταξη των δεδομένων) και χωρίς σφάλματα

3. Κάθε ακμή στο γράφο απαραιτήτως πρέπει να έχει μία και μόνο κατεύθυνση και δεν επιτρέπονται οι δυο κατευθύνσεις προς και από ένα κόμβο (bi-directional)

4. Ο τρόπος αποστολής των πακέτων γίνεται με broadcasting

Το θέμα που προκύπτει τώρα, είναι με ποιά κριτήρια αυτός ο αλγόριθμος θέτει κατευθύνσεις στις ακμές του γράφου. Ως ένας ακόμη αλγόριθμος που αντιγράφει τη φύση, παρομοιάζει την κίνηση των δεδομένων πληροφορίας σαν ένα ρυάκι, το οποίο λόγω δυναμικού πεδίου, ρέει από τα υψηλότερα στρώματα (στους κόμβους), στα χαμηλότερα. Επομένως, αντί για «κόστος», έχουμε «ύψος» στο οποίο βρίσκεται κάθε κόμβος.

Για να μπορέσει το πρωτόκολλο να κατοχυρώσει την σωστή σειρά των πληροφοριών, διαθέτει επίσης και 3 βασικές μεθόδους, που έχουν να κάνουν με την δημιουργία, πρόσθεση και αφαίρεση κόμβων:

Τί αλλάζει;

Να σημειωθεί κάπου εδώ πως μπορεί οι ακμές του γράφου να είναι σεσημασμένες με κάποιο κόστος (όπως ακριβώς και στις τοπολογίες δικτύου), αλλά το θέμα του αλγορίθμου δεν είναι να αναζητήσει τα δρομολόγια με το λιγότερο δυνατό κόστος. Αντ' αυτού, το ζητούμενό του είναι να ανακαλύψει πολλαπλά δρομολόγια για κάποιον προορισμό.

Ποια τα θετικά;

Εδώ συναντάμε πολλά θετικά στοιχεία όσο αναφορά τους χρόνους και την απόδοση των αλγορίθμων. Πιο συγκεκριμένα, η πλήρης αντιστροφή των ακμών χρειάζεται χρόνο n, όσος δηλαδή και ο αριθμός των κόμβων που είχαν αναφορά στον κατηργημένο κόμβο και χρονική πολυπλοκότητα $O(n^2)$. Αντιστοίχως, η μερική αντιστροφή έχει χρονική πολυπλοκότητα $O(n * h + n^2)$, όπου

Ακόμη, είναι εξαιρετικά θετικό το γεγονός ότι υπάρχουν πολλαπλά δίκτυα και πως ο ίδιος ο αλγόριθμος είναι τελείως αποκολλημένος από την λογική εύρεσης μιας συγκεκριμένης διαδρομής που απαραιτήτως έχει το μικρότερο δυνατό κόστος, όπως οι προηγούμενοι αλγόριθμοι που χρησιμοποιούσαν τον Bellman-Ford. Πράγμα που τον κάνει να αποδίδει καλύτερα σε πολύ δυναμικά δίκτυα.

Ποια τα αρνητικά;

Ανήκοντας στα on-demand πρωτόκολλα, κληρονομεί και αυτό τα αρνητικά των αλγορίθμων της σειράς του, με την μετάδοση πολλών πληροφοριών κατάστασης προς όλους, «γεμίζοντας» το μέσο. Επίσης, δεν υπάρχει δυνατότητα κλιμάκωσης του αλγορίθμου με κανέναν τρόπο.

Στην πράξη, δεν χρησιμοποιείται και τόσο, μιας και οι δυο προηγούμενοι αλγόριθμοι AODV και DSR τον «αναιρούν» κατά κάποιο τρόπο, αφού είναι ευρέως πιο διαδεδομένοι λόγω ευκολίας κατασκευής τους.

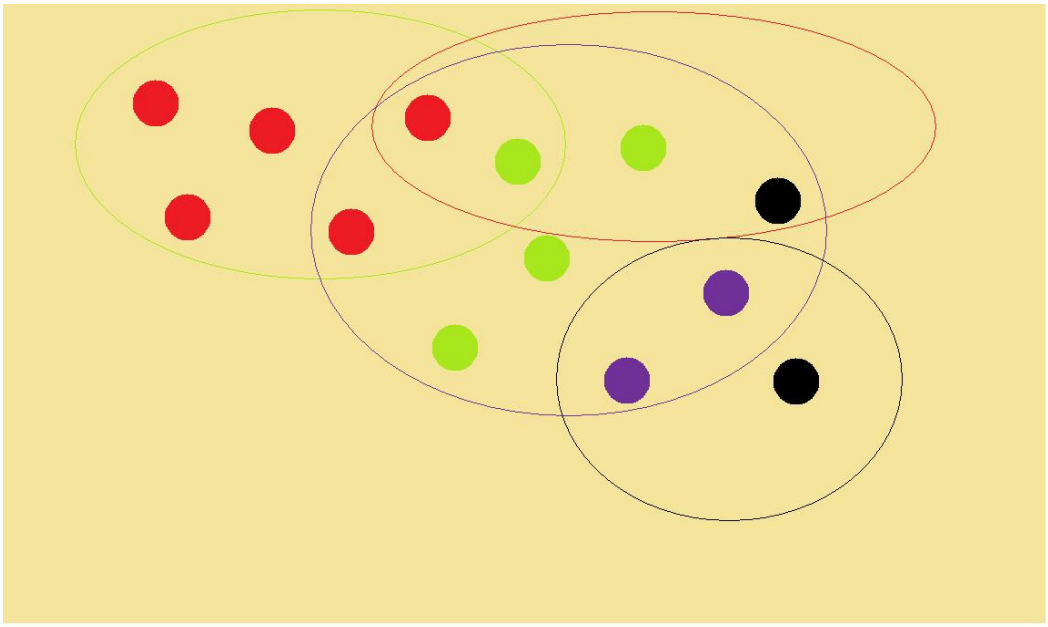
Ο αλγόριθμος ZRP (Zone Routing Protocol)

Ποια τα χαρακτηριστικά;

Ο αλγόριθμος ZRP είναι ένας υβριδικός αλγόριθμος που συνδυάζει έναν ενεργό αλγόριθμο δρομολόγησης (όπως αυτόν που αναλύθηκε πιο πάνω), με τον διαχωρισμό κόμβων σε ξεχωριστές ομάδες, αναλόγως με την εμβέλειά τους. Ένα χαρακτηριστικό που ορίζεται χειροκίνητα (manually)

από τον χρήστη, ο οποίος στην ουσία ορίζει την περίμετρο ενός κύκλου που θα περικλείει έναν συγκεκριμένο αριθμό κόμβων.

Για να το εξηγήσουμε καλύτερα, παραθέτουμε την παρακάτω εικόνα



Παρατηρούμε ότι ανάλογα με την ακτίνα κάθε κύκλου, δημιουργούνται και ξεχωριστές ομάδες κόμβων Ο χρήστης, μπορεί να ορίσει το μήκος της ακτίνας, για παράδειγμα με γνώμονα τον αριθμό των hops.

Κάθε κόμβος, διατηρεί πληροφορίες δρομολόγησης μόνο για τους κόμβους που βρίσκονται στην ίδια ζώνη με εκείνον. Ο τρόπος που επικοινωνούν εντός ζώνης, είναι ο ίδιος με κάποιον αλγόριθμο που αναφέραμε προηγουμένως. Στην περίπτωση που η επικοινωνία αφορά κάποιον κόμβο που δεν διατηρεί στον πίνακα δρομολόγησής του, τότε καταλαβαίνει ότι πρόκειται για προσπάθεια επικοινωνίας εκτός ζώνης.

Έχουμε δηλαδή δύο ειδών επικοινωνίες, όπως τις αναφέραμε παραπάνω: Την intra-zone και την inter-zone επικοινωνία.

Ποια τα θετικά;

Πρώτα απ' όλα η ασφάλεια των πληροφοριών. Μια ζώνη δεν γνωρίζει τί πακέτα μεταφέρονται σε μια άλλη ζώνη. Ακόμη, εμφανίζει καλύτερη κλιμάκωση σε σχέση με οποιονδήποτε άλλον αλγόριθμο, καθώς επίσης έχει καλύτερη επαναφορά του δικτύου, αν για παράδειγμα κάποιος κόμβος πάθει βλάβη.

Ελέγχοντας την εμβέλεια της «γειτονιάς» των κόμβων, μπορούμε να διαχειριστούμε μεγαλύτερα και πιο πυκνά δίκτυα, χρησιμοποιώντας οποιονδήποτε προαναφερθέντα αλγόριθμο (έστω τον DSDV).

5.6 CASE STUDY ΓΙΑ ΤΟΝ ΑΛΓΟΡΙΘΜΟ AODV

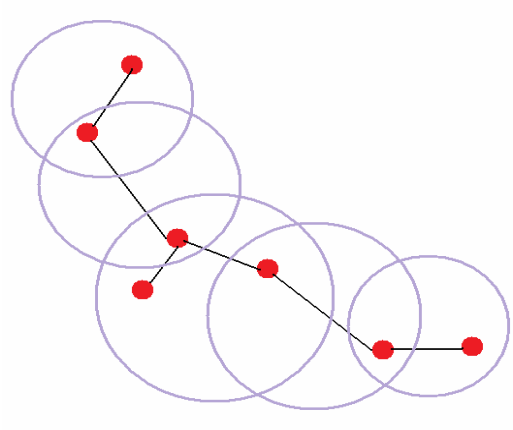
Όπως έχουμε μελετήσει και στα προηγούμενα, οι πρωταρχικοί σκοποί αυτού του αλγορίθμου, είναι να κάνει broadcasting σε πακέτα μόνο όταν αυτό είναι απαραίτητο, να μπορεί κάνει τη διάκριση μεταξύ τοπικής συνδεσμολογίας και γενικής τοπολογίας του δικτύου, καθώς επίσης και να γνωρίζει πώς γίνεται η διατήρησή του. Τέλος, πρέπει να μπορεί να διαδίδει πληροφορίες που αφορούν αλλαγές στην τοπική συνδεσμολογία, μόνο στους κόμβους που τους είναι απαραίτητες.

Επειδή είναι ο πρώτος αλγόριθμος στη σειρά των αλγορίθμων που ανακαλύφθηκαν για τα κινητά δίκτυα (Mobile Ad-hoc NETworks - MANET), είναι σαφώς ο σχετικά πιο «εύκολος» αλγόριθμος, οπότε έχει μελετηθεί σε μεγαλύτερο εύρος. Αυτή η μελέτη, έφερε στο φως πολλές από τις ατέλειές του. Γι' αυτό, θεώρησα σε αυτό το case study θα ήταν πιο ενδιαφέρον να αναφέρω πώς είναι δυνατόν να προξενήσουμε βλάβη στο δίκτυο που χρησιμοποιεί τον αλγόριθμο AODV, διακινώντας «παράνομες» πληροφορίες στο δίκτυο.

Πριν προχωρήσουμε στο υποθετικό σενάριο, είναι σημαντικό να τονίσουμε ότι η επίθεση σε ένα τέτοιο δίκτυο μπορεί να γίνει μόνο «εκ των έσω». Με λίγα λόγια, ο «εισβολέας» πρέπει να βρίσκεται συνδεδεμένος με κάποιο τρόπο στο δίκτυο, άρωντας την ασφάλειά του.

Η ασφάλεια του δικτύου έγγυται στους αλγορίθμους κρυπτογράφησης πληροφοριών. Εφόσον ο «εισβολέας» έχει υπό τον έλεγχό του κάποιον, ή κάποιους από τους κόμβους του δικτύου, μπορεί εύκολα να διαχειριστεί και τους τρόπους κρυπτογράφησης πληροφοριών. Έτσι μπορεί να εξαπολήσει για παράδειγμα μια απλή επίθεση, γράφοντας ένα λανθασμένο πακέτο μηνύματος προς μετάδοση, ή μια πιο πολυσύνθετη επίθεση, όπου τηρουμένου του πρωτοκόλλου δικτύου, να υπάρχουν πολλά μεμονωμένα μηνύματα σφάλματος.

Έστω ότι ο «εισβολέας» του case study, θέλει να δημιουργήσει ένα απλό σφάλμα. Είναι γνωστό πως όταν η πηγή έχει μηνύματα προς αποστολή σε κάποιο προορισμό, τον αναζητά στους πίνακες δρομολόγησής της. Αν δεν τον βρει, τότε κάνει broadcasting σε όλους τους γειτονικούς κόμβους ένα μήνυμα που λέγεται RREQ (Route REQuest). Το μήνυμα αυτό μεταδίδεται με τον ίδιο τρόπο από κάθε κόμβο σε κάθε γειτονικό του κόμβο, έως ότου κάποιος από αυτούς βρει τον κόμβο-προορισμό. Η διαδικασία αυτή φαίνεται στην παρακάτω εικόνα:

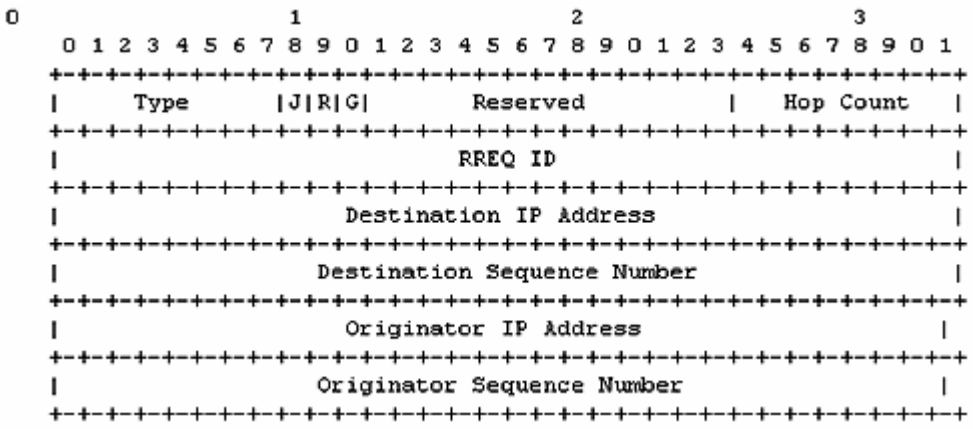


Σε κάθε πρωτόκολλο δικτύου, η κεφαλή κάθε μηνύματος, περιέχει την ταυτότητα (ID) κάθε κόμβου. Όταν μιλάμε για μηνύματα αίτησης, αυτά περιέχουν και έναν κωδικό που είναι μοναδικός για κάθε αίτηση, και παίζουν το ρόλο του ID. Η συσχέτηση κωδικού κόβου με κωδικό αίτησης, εξασφαλίζουν την γνησιότητα του μηνύματος. Έτσι κάθε επόμενος κόβος αποδέχεται το μήνυμα που έστειλε ο προηγούμενος. Η διαδικασία από εδώ και πέρα ακολουθεί τη διαδικασία «HELLO». Τί γίνεται όμως εάν μεταδοθούν λανθασμένα μηνύματα δρομολόγησης;

Ας «πειράξουμε» λοιπόν τα μηνύματα RREQ. Συνήθως έχουμε τριών ειδών RREQ μηνύματα «πειράγματος», τα οποία παρατίθενται στον παρακάτω πίνακα:

ΟΝΟΜΑΣΙΑ	ΕΞΗΓΗΣΗ	ΛΕΙΤΟΥΡΓΙΑ
RREQ_DR	Route REQuest DRop	Ο «εισβολέας» κάνει drop τα μηνύματα δρομολόγησης που φτάνουν στον κόμβο
RREQ_MF	Route REQuest Modify and Forward	Ο «εισβολέας» κάνει μετατροπές στα μηνύματα δρομολόγησης (σε νευραλγικά πεδία τους), που φτάνουν στον κόμβο και κατόπιν τα προωθεί στους γειτονικούς κόμβους
RREQ_AF	Route REQuest Active Forge	Ο «εισβολέας» αποστέλλει ψεύτικα μηνύματα δρομολόγησης, δίχως να παραλαμβάνει κάποιο σχετικό μήνυμα

Έστω τώρα ότι ο «εισβολέας» μας θα χρησιμοποιήσει τον δεύτερο τρόπο, όπως περιγράφεται στον παραπάνω πίνακα. Μέσα από αυτό το μήνυμα δρομολόγησης, θα προσπαθήσει να απομονώσει κάποιον κόμβο από τους υπόλοιπους (ώστε το θύμα να είναι πιο ευάλωττο). Ας δούμε λίγο πώς μοιάζει ένα RREQ πακέτο, ώστε να αντιληφθούμε καλύτερα την επίθεση που θα κάνουμε:



Στην εικόνα παρατηρούμε τα εξείς πεδία:

1. Το πεδίο Hop Count που μετράει τα hops που κάνει το μήνυμα μέχρι να φτάσει στον προορισμό του,
2. Το RREQ ID,
3. Την IP διεύθυνση του προορισμού,
4. Την IP διεύθυνση της πηγής και

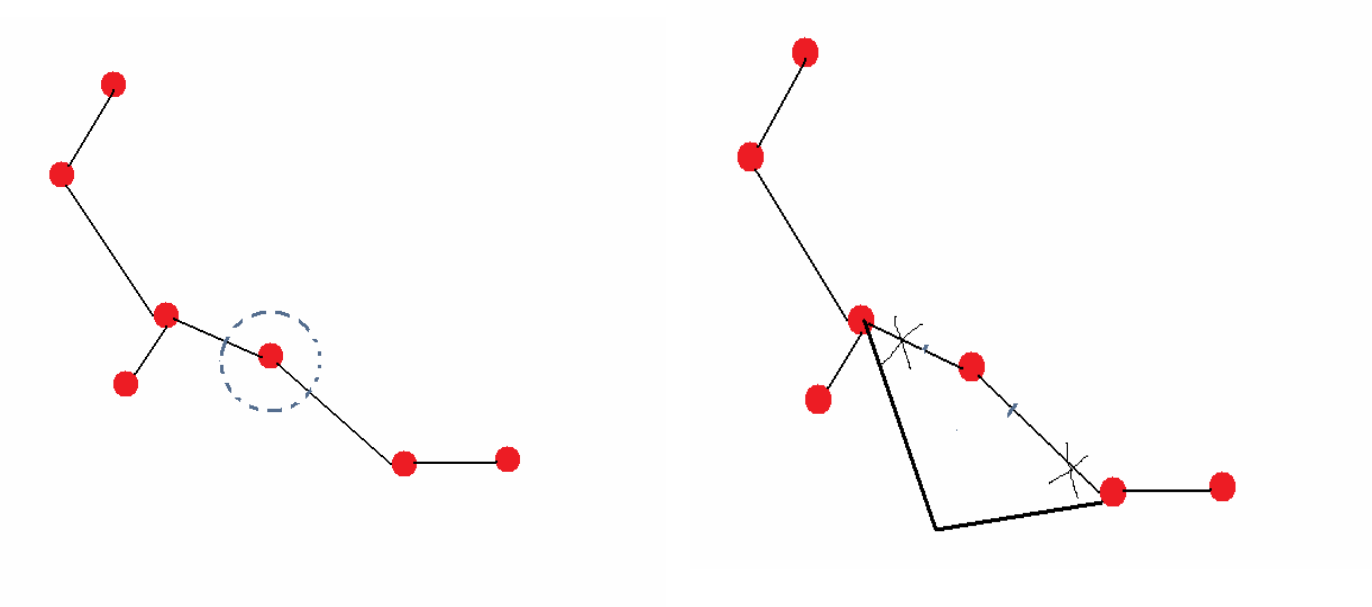
5. Τον αύξοντα αριθμό πακέτου.

Επομένως οι violations που μπορούμε να κάνουμε είναι

1. Να αυξήσουμε το RREQ ID κατά ένα ελάχιστο αριθμό,
2. Να αντικαταστήσουμε το IP προορισμού με κάποια μη υπαρκτή διεύθυνση,
3. Να αντικαταστήσουμε το IP της πηγής με κάποια μη υπαρκτή διεύθυνση, ή τέλος
4. Να αυξήσουμε τον αριθμό πακέτου κατά τουλάχιστον μια μονάδα.

Με αυτούς τους τρόπους καταφέρνουμε να απομονώσουμε για μικρό χρονικό διάστημα κάποιον κόμβο, δίχως να αποστέλλονται σε αυτόν μηνύματα. Έτσι ο ενδιάμεσος κόμβος-εισβολέας, μπορεί να «σπάσει» το δίκτυο στα 2, κάνοντας διαφορετική συνδεσμολογία από αυτή που υπήρχε προηγουμένως.

Στις πιο κάτω εικόνες ο κόμβος που βρίσκεται στη μέση του δικτύου έχει υποστεί εισβολή, με αποτέλεσμα να αποκοπεί από το υπόλοιπο δίκτυο και η συνδεσμολογία να αλλάξει, μιας που και οι πίνακες δρομολόγησης των κόμβων έχουν ενημερωθεί (update) με τα καινούρια, ψεύτικα δεδομένα.



CASE STUDY ΓΙΑ ΤΟΝ ΑΛΓΟΡΙΘΜΟ DSR

Το Dynamic Source Protocol (DSR), έχει αποδειχτεί πως είναι το πιο απλό και συνάμα πιο αποτελεσματικό πρωτόκολλο για multi-hop[1] δίκτυα, που αναφέραμε προηγουμένως με τον γενικότερο τίτλο MANETs.

Σε αντίθεση με τον προηγούμενο αλγόριθμο, ο DSR υποστηρίζει μετάδοση μηνυμάτων, όχι μόνο σε άμεσα συνδεδεμένους κόμβους[2] με την πηγή. Εδώ, όλοι οι κόμβοι συνεργάζονται αποτελεσματικά, ώστε να προωθηθούν μηνύματα και εκτός εμβέλειας της πηγής (που φυσικά μεταφράζεται σε πολλάπλα hops).

[1]

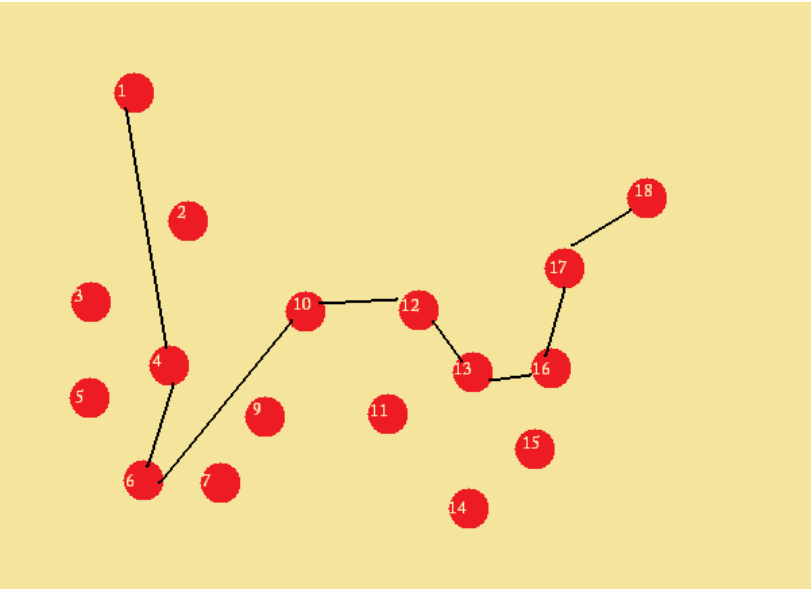
[2] Εδώ έχει περισσότερο την έννοια του να βρίσκεται στην ακτίνα, ή διαφορετικά στην εμβέλεια (range) της πηγής.

Αυτό επιτυγχάνεται κρατώντας μέσα στην κεφαλίδα (header) κάθε πακέτου την πλήρη διαδρομή του, μέχρι να φτάσει στον προορισμό. Επαγωγικά, ο προορισμός μπορεί να αντιληφθεί ποια είναι η πηγή του μηνύματος. Όλη η παραπάνω διαδικασία είναι γνωστή ως δυναμική εύρεση πηγής.

Στην παρακάτω εικόνα φαίνεται η διαδρομή που ακολουθεί το μήνυμα από την πηγή μέχρι τον προορισμό, τοποθετώντας κάθε φορά στην λίστα της κεφαλίδας του τον νέο κόμβο.

Κάτι επίσης σημαντικό που πρέπει να αναφέρουμε, είναι πως το αριθμός των hop που μπορεί να κάνει ένα πακέτο εντός δικτύου, πρέπει να είναι μέσα σε λογικά πλαίσια (σίγουρα μεγαλύτερο της μονάδας και μικρότερο από 10 ή 11 hops θα ήταν μια χαρά), ούτως ώστε να μην έχουμε μια τεράστια λίστα μέσα στο header που θα κουβαλάει το πακέτο. Αποτέλεσμα μιας τέτοιας ενέργειας θα ήταν η μεγάλη καθυστέρηση στην εύρεση πηγής.

Ο αριθμός των hop καθορίζει με λίγα λόγια το εύρος, την διάμετρο, του ad-hoc ασύρματου δικτύου.



Ενώ το header που θα λάβει ο προορισμός, θα μοιάζει κάπως έτσι:

0.Διεύθυνση κόμβου 1
1.Διεύθυνση κόμβου 2
2.Διεύθυνση κόμβου 3
3.Διεύθυνση κόμβου 4
4.Διεύθυνση κόμβου 5
5.Διεύθυνση κόμβου 6
6.Διεύθυνση κόμβου 7
7.Διεύθυνση κόμβου 8
8.Διεύθυνση κόμβου 9

Η διαδιακασία εξεύρεσης του κόμβου-πηγή, είναι πάνω-κάτω ίδια με αυτή του αλγόριθμου AODV. Και εδώ χρειάζονται κάποια μηνύματα αίτησης (RREQ), τα οποία ανάλογα με την απάντηση που παίρνουν,

προχωρούν σε κατάλληλα μηνύματα κατάστασης του δικτύου. Τα τελευαία μηνύματα έχουν ως στόχο την αναδιαμόρφωση του πίνακα δρομολόγησής τους.

Σύμφωνα με τα παραπάνω, τα «πειράγματα» που μπορούμε να κάνουμε σε ένα τέτοιο δίκτυο είναι παρόμοια. Στον πιο κάτω πίνακα, δίνονται αναλυτικά οι πιο σημαντικές καταστάσεις από τις οποίες περνάει κάθε μήνυμα αιτήματος απόκρισης. Ο «εισβολέας» μπορεί να τα τροποποιήσει, προκειμένουν να προξενήσει ανεπανόρθωτα σφάλματα και να έχει όλο το δίκτυο υπό τον έλεγχό του.

ΤΡΕΧΟΥΣΑ ΚΑΤΑΣΤΑΣΗ	**ΤΥΠΟΣ ΕΙΣΒΟΛΗΣ**	**ΤΙ ΠΡΟΚΑΛΕΙ**
Τα δεδομένα ελήφθησαν και αναμένεται προώθησή τους	Time-out packet drop	Black hole
Το RREQ εστάλη και αναμένεται απάντηση.	RREP sent	Flooding
Το RREP εστάλη και αναμένεται προώθηση.	Route modified	Tampering

Το RREP είναι η απάντηση του RREQ πακέτου μηνύματος. Ο κόμβος που το δημιουργεί, τοποθετεί παράλληλα στο τέλος το πακέτου το όνομα του πρηγούμενου κόμβου-πηγή, και κατόπιν το στέλνει πίσω στην πηγή.

Για να καταλάβουμε καλύτερα την εισβολή, πρέπει να αναφέρουμε τις 5 βασικές ενέργειες (που στις γλώσσες προγραμματισμού μεταφράζονται σε εντολές ή μεθόδους) που μπορεί να κάνει κάποιος κόμβος, όταν βρίσκεται αντιμέτωπος με κάποιο πακέτο μηνύματος:

ΚΑΤΑΣΤΑΣΗ	**ΜΕΘΟΔΟΣ**	**ΕΝΤΟΛΗ**
Κατάσταση_0	Λήψη Δεδομένων()	Λάβε Δεδομένα
Κατάσταση_1	Ανανέωση TTL[3]()	Ανανέωσε TTL
Κατάσταση_2	Δημιουργία σφάλματος στο Data Link Layer()	Δημιούργησε σφάλμα τύπου Data Link Layer
Κατάσταση_3	Δημιουργία RouteERRor-RERR()	Δημιούργησε RERR
Κατάσταση_4	Αποστολή RERR()	Απέστειλε RERR
Κατάσταση_5	Αποθήκευση πακέτου()	Αποθήκευσε πακέτο

Θεωρούμε πως αρχικά βρισκόμαστε στην κατάσταση_0, όπου ο κόμβος έχει ήδη λάβει τα δεδομένα. Θα μπορούσαμε να δημιουργήσουμε έναν αλγόριθμο, ο οποίος θα δείχνει με αρκετή κατατοπιστικότητα πώς «κινείται» ένα δίκτυο με αλγόριθμο DSR:

[3] Όπου TTL, ο χρόνος ζωής του πακέτου Time To Live

```
Αν ( Λήψη Δεδομένων() ) τότε
        Κατάσταση <- κατάσταση_1
        Ανανέωσε TTL
        Κατάσταση <- κατάσταση_2
        Αν TTL = 0 τότε
                Απέρριψε πακέτο
                Δημιούργησε σφάλμα τύπου Data Link Layer
                Έξοδος
                Κατάσταση <- κατάσταση_3
        Αλλιώς
                Προώθησε πακέτο
                Έξοδος
        Τέλος_αν
        Όσο (Κατάσταση = κατάσταση_3) επανέλαβε
                Αν Πλήθος_RERR > max τότε
                        Απέρριψε πακέτο
                        Έξοδος
                Αλλιώς
                        Δημιούργησε RERR
                        Κατάσταση <- κατάσταση_4
                Τέλος_Αν
        Τέλος_επανάληψης
        Αν Κατάσταση = κατάσταση_4 τότε
                Δημιούργησε RERR
                Κατάσταση <- κατάσταση_5
                Αποθήκευσε πακέτο
        Τέλος_ Αν
Τέλος_ Αν
```

Έστω σε αυτό το case study ότι μελετούμε την δημιουργία «Μαύρης Τρύπας». Στην ουσία, τροποποιούμε τον χρόνο λήψης των πακέτων, ούτως ώστε αυτά να απορρίπτονται και κατόπιν να επιστρέφονται πίσω στον αποστολέα. Αναφορικά με τον αλγόριθμο πιο πάνω, αυτό που επιτυγχάνουμε είναι να τοποθετήσουμε τον κόμβο σε μια άλλη κατάσταση, δίχως να έχει περάσει από τις προηγούμενες, προωθώντας πακέτα δεδομένων.

Αυτό σημαίνει πως κατά την ανανέωση του TTL, επειδή το πακέτο θα αποστέλεται συνεχώς στον αποστολέα, ο χρόνος ζωής του πακέτου θα μειώνεται συνεχώς κατά 1, έως ότου φτάσει να είναι 0. Όταν λοιπόν γίνει 0, το πακέτο απορρίπτεται.

Είναι η πιο απλή και συνάμα πιο «ύπουλη» επίθεση σε ένα δίκτυο που χρησιμοποιεί τον αλγόριθμο DSR.

ΚΕΦΑΛΑΙΟ 6^{ο} ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ιδέα της ασύρματης δικτύωσης είναι αρκετά ώριμη μετρώντας ήδη περισσότερες από δύο δεκαετίες ύπαρξης. Οι πρώτες υλοποιήσεις, αν και πολλά υποσχόμενες, οδήγησαν σε απογοήτευση, καθώς αποδείχθηκαν ανεπαρκείς και προβληματικές. Η εμφάνιση του προτύπου 802.11 άλλαξε ριζικά το κλίμα και, αφού απέδειξε την αξία του στις κάθετες αγορές της υγείας, της εκπαίδευσης, και των επιχειρήσεων λιανικών πωλήσεων, επεκτείνεται δυναμικά σε όλο το εύρος των επιχειρήσεων και για πρώτη φορά στους οικιακούς χρήστες. Στη πράξη τα ασύρματα δίκτυα δεν είναι απλώς μια διαφορετική εκδοχή των ενσύρματων δικτύων, καθώς προσφέρουν πρωτόγνωρες δυνατότητες μετατρέποντας τον προσωπικό υπολογιστή σε μέσο επικοινωνίας παρά προσωπικής ενασχόλησης. Το Internet έφερε το πρώτο κύμα της αλλαγής ενοποιώντας τα υπολογιστικά συστήματα σε παγκόσμιο επίπεδο και πλέον τα ασύρματα δίκτυα έχουν την δυναμική να κάνουν το ίδιο σε τοπικό. Όσον αφορά στις επιχειρήσεις, τα οφέλη είναι πολλά: τόσα ώστε η επιτυχία των ασύρματων δικτύων στο χώρο αυτών είναι απλώς δεδομένη. Το μόνο που μπορεί να πει κανείς με βεβαιότητα για το μέλλον των ασύρματων επικοινωνιών είναι ότι θα γνωρίσουν σημαντική ανάπτυξη.

Υπάρχουν αρκετές προτάσεις για ασύρματη δικτύωση πέρα από το 802.11 και σίγουρα πολλές εξειδικευμένες που δεν αναφέραμε. Το σίγουρο είναι ότι δεν πρόκειται να επικρατήσει ούτε το καλύτερο ούτε το πιο οικονομικό πρότυπο. Για τη ώρα το 802.11b δείχνει να κυριαρχεί στην αγορά χωρίς ιδιαίτερο ανταγωνισμό και οι τιμές των προϊόντων που βασίζονται σ' αυτό σημειώνουν συνεχή μείωση. Ιδιαίτερη προσοχή έχει δοθεί στην ανάπτυξη και στην υποστήριξη του προτύπου 802.11. Έτσι παρουσιάστηκε η έκδοση 802.11b η οποία επιτυγχάνει ταχύτητες διαμεταγωγής δεδομένων ως 11Mbits ή ως 22 Mbits καθώς και η έκδοση 802.11g η οποία υπόσχεται μεταφορά δεδομένων έως και 54Mbits. Η βελτίωση και η ανάπτυξη των προτύπων θα δώσει νέα ώθηση στην αγορά της ασύρματης δικτύωσης αφού θα προσθέτει νέα χαρακτηριστικά και θα λύνει σημαντικά προβλήματα. Σημαντικό ρόλο στην επίτευξη αξιόπιστων, σταθερών και γρήγορων ζεύξεων διαδραματίζουν οι κεραίες. Η συνεισφορά τους σε μια πετυχημένη σύνδεση είναι καθοριστική. Σημαντικοί παροχής υπηρεσιών internet στην Ευρώπη έχουν ανακοινώσει ότι μελετούν και δημιουργούν δίκτυα αποτελούμενα από σημεία πρόσβασης (hot spots) τα οποία θα παρέχουν πρόσβαση στο internet ασύρματα. Δεδομένου ότι σε λίγα χρόνια θα υπάρχει πρόσβαση στο internet σχεδόν από παντού, και οπωσδήποτε στους κυριότερους δημόσιους χώρους, θα μπορεί να χρησιμοποιηθεί αυτό για την επικοινωνία αντί για τα κινητά τηλέφωνα, είτε για την ανταλλαγή δεδομένων, είτε για φωνητική επικοινωνία με voice over IP. Η ταχύτητα και η ασφάλεια των ασύρματων δικτύων είναι από τα σημαντικότερα ζητήματα που απασχολούν μακροπρόθεσμα τις ομάδες ανάπτυξης τους, αλλά και τις εταιρείες που σκοπεύουν να τα υιοθετήσουν. Η ασφάλεια που είναι σήμερα το αδύνατο σημείο, είναι το πρώτο θέμα που θα πρέπει να αντιμετωπιστεί. Σύντομα νέες τεχνικές αλλά και αυξημένη επίγνωση των διαχειριστών θα διασφαλίσουν τα ασύρματα δίκτυα, καθιστώντας τα τόσο ασφαλή όσο είναι και τα ενσύρματα. Η ταχύτητα σύνδεσης αυξάνει συνεχώς, όμως εδώ υπάρχουν αντικειμενικοί περιορισμοί από τις διαθέσιμες συχνότητες. Η αυξημένες ανάγκες της αγοράς θα οδηγήσουν σε εμπορική εκμετάλλευση σε νέες ζώνες ραδιοσυχνοτήτων και ίσως σε ελευθέρωση άλλων για ερασιτεχνική χρήση. Εκτός από τις τεχνολογίες, ιδιαίτερη προσοχή χρήζουν οι εφαρμογές ασύρματης δικτύωσης και επικοινωνίας. Μέχρι τώρα οι υλοποιήσεις έχουν μεταβάλλει σημαντικά τις κοινωνίες μας μέσω της κινητής τηλεφωνίας. Οι μελλοντικές εφαρμογές θα εισβάλουν σε πολλούς τομείς της καθημερινής ζωής, με το εμπόριο και τις υπηρεσίες να υφίστανται τις μεγαλύτερες αλλαγές. Η κοινωνία που θα προσφέρει δικτύωση και επικοινωνία παντού είναι ήδη σε αναμονή, γι' αυτό θα πρέπει να διαφυλάξουμε τις ατομικές και συλλογικές ελευθερίες μας.

- **Ακρωνύμια**

AP - Access Point
BPSK - Binary Phase Shift Keying
BSS - Basic Service Set
CCK - Complementary Code Keying
CRC - Cyclic Redundancy Check
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD - Carrier Sense Multiple Access with Collision Detection
CTS - Clear to Send
DCF - Distribution Coordination Function
DHCP - Dynamic Host Configuration Protocol
DS - Distribution system
DSSS - direct sequence spread spectrum
ESS - Extended Service Set
ETSI - European Telecommunications Standards Institute
FCC - Federal Communications Commission (USA)
FHSS - Frequency Hopping Spread Spectrum
IBSS - Independent Basic Service Set
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force IP Internet Protocol
IPSec - Internet Protocol Security
ISA - Integrated Services Architecture
ISM - Industry, Scientific, and Medical
ISO - International Organization for Standardization
LLC - Logical Link Control
MAC - Media Access Control
MIB - Management information base
MKK -Radio Equipment Inspection and Certification Institute (Japan)
NIC - Network interface card
NOS -Network operating system
PCF -Point Coordination Function
PCI -Peripheral Component Interconnect
PRNG - Pseudo Random Number Generator
QPSK - Quadrature Phase Shift Keying
RC4 - Ron's Code or Rivest's Cipher
RTS - Request to Send
SNMP - Simple Network Management Protocol
TCP/IP - Transmission Control Protocol/Internet Protocol
WECA - Wireless Ethernet Compatibility Alliance
WEP - Wired Equivalent Privacy
WLAN - Wireless Local Area Network
WLANA - Wireless LAN Alliance

ΓΛΩΣΣΑΡΙ

Ad hoc Mode
Μερικές φορές αναφέρεται ως head-to-head ή peer-to-peer, adhoc λειτουργίες αναμονής χωρίς τη βοήθεια ενός σημείου πρόσβασης (AP). Adhoc είναι 802,11 δικτύωση ρύθμιση σύμφωνα με την οποία ενσύρματες ή ασύρματες συσκευές επικοινωνούν μεταξύ τους, συχνά χρησιμοποιείται με κονσόλες παιχνιδιών για τους σκοπούς του gaming LAN μέρους.

Beacon Interval
Ένας φάρος είναι ένα πακέτο πληροφοριών που αποστέλλεται από μια συνδεδεμένη συσκευή σε όλες τις άλλες συσκευές όπου ανακοινώνει την διαθεσιμότητα και την ετοιμότητά της. Ένα διάστημα beacon είναι ένα χρονικό διάστημα (αποστέλλεται με το φάρο) πριν στείλετε το φάρο και πάλι. Το διάστημα φάρος μπορεί να ρυθμιστεί σε χιλιοστά του δευτερολέπτου (ms).

Bit Rate
Ο αριθμός των δυαδικών ψηφίων, ή bits, μεταφέρονται ανά δευτερόλεπτο (bps). Οι ανακοινώσεις κανάλια χρησιμοποιώντας μόντεμ και τηλέφωνο, με έδρα το τιμολογιακής bit, κοινώς 300, 1200, 2400, 4800, 9600 και 14400.

Bluetooth
Το Bluetooth είναι μια υπολογιστική και τηλεπικοινωνιών προδιαγραφή της βιομηχανίας, που περιγράφει τον τρόπο με τον οποίο τα κινητά τηλέφωνα, υπολογιστές και προσωπικούς ψηφιακούς βοηθούς (PDAs) - όπως μια PalmPilot - μπορούν εύκολα να διασυνδεθούν μεταξύ τους. Η τεχνολογία αυτή χρησιμοποιείται με το σπίτι και τα τηλέφωνα των επιχειρήσεων, καθώς και υπολογιστές μέσω ασύρματης σύνδεσης.

Διεπαφή
Η φυσική και λογική διευθέτηση υποστήριξη της κατάσχεσης οποιασδήποτε συσκευής σε μια σύνδεση ή σε άλλη συσκευή.

Δρομολογητής (Router)
Είναι μια συσκευή που μετακινεί δεδομένα ανάμεσα σε διαφορετικά δίκτυα και μπορεί να έχει πρόσβαση στην κεφαλίδα των πακέτων δεδομένων για να αποφασίσει τη βέλτιστη διαδρομή που πρέπει να ακολουθήσει. Οι δρομολογητές μπορούν να συνδέσουν δίκτυα που χρησιμοποιούν διαφορετικά πρωτόκολλα. Επιτρέπουν επίσης σε όλους του χρήστες του δικτύου να μοιράζονται μια κοινή σύνδεση με το Internet ή κάποιο WAN.

IEEE
Είναι μια μη κερδοσκοπική επαγγελματική οργάνωση που ιδρύθηκε από μια ομάδα μηχανικών το 1884 με σκοπό την παγίωση των ιδεών που αφορούν την τεχνολογία της ηλεκτρονικής. Στα τελευταία 100 έτη, η IEEE έχει διατηρήσει μια σταθερή ανάπτυξη. Σήμερα, η IEEE είναι βασισμένο στις Ηνωμένες Πολιτείες, έχει πάνω από 320.000 μέλη που προέρχονται από 150 χώρες. Η IEEE αποτελείται από 35 μεμονωμένες οργανώσεις, συμπεριλαμβανομένης της οργάνωσης επικοινωνιών, της οργάνωσης υπολογιστών, και της οργάνωσης κεραιών και μετάδοσης.

Independent Basic Service Set (IBSS) Networks
Ένα IBSS είναι ένα αυτόνομο BSS που δεν έχει καμία backbone υποδομή και αποτελείται από τουλάχιστον δύο ασύρματους σταθμούς . Αυτός ο τύπος δικτύου αναφέρεται συχνά ως ad hoc επειδή μπορεί να κατασκευαστεί γρήγορα χωρίς ιδιαίτερη σχεδίαση.

Extended Service Set (ESS) Networks
Για τις απαιτήσεις που υπερβαίνουν τους περιορισμούς ενός ανεξάρτητου BSS, το 802.11 καθορίζει το Extended Service Set (ESS)) LAN. Αυτός ο τύπος διαμόρφωσης ικανοποιεί τις ανάγκες των δικτύων μεγάλης κάλυψης που είναι αυθαίρετα από πλευράς μεγέθους και πολυπλοκότητας.

Internet Connection Sharing (ICS)
ICS είναι μια μέθοδος για τη σύνδεση πολλαπλών υπολογιστών σε ένα τοπικό δίκτυο στο Internet μέσω μίας μόνο σύνδεσης και μία μόνο διεύθυνση IP. ΙΠ ακολουθεί ένα μοντέλο υπολογιστή-πελάτη/διακομιστή. Για να ρυθμίσετε ICS, ένας υπολογιστής πρέπει να επιλεγεί ως ο "server". Αυτός ο υπολογιστής πρέπει να υποστηρίζει δύο διασυνδέσεις δικτύου, το ένα είναι άμεσα συνδεδεμένα με το Διαδίκτυο και τα άλλα που συνδέονται με το υπόλοιπο του LAN. Σε ένα παραδοσιακό σπίτι dial-up δικτύου, για παράδειγμα, ο υπολογιστής server είναι άμεσα συνδεδεμένα με το μόντεμ.

Intranet
Intranet είναι ένα δίκτυο TCP / IP μέσα σε μια εταιρεία που συνδέει την εταιρία με το Διαδίκτυο. Οι περισσότεροι Intranets είναι προσβάσιμα μόνο μέσα από τη θέση ή την εταιρεία που εκτελεί το Intranet.

ISP
Internet Service Provider-Μία εταιρεία η οποία παρέχει πρόσβαση στο Διαδίκτυο είτε πρόκειται για προσωπική dial-up λογαριασμό ή συνεργάζονται σε δίκτυο σύνδεσης. Οι περισσότεροι πάροχοι υπηρεσιών Ίντερνετ θα παρέχει επιπλέον υπηρεσίες περιλαμβάνουν βοήθεια σχετικά με το σχεδιασμό, δημιουργία και διαχείριση ιστοσελίδων, καθώς και την υποστήριξη intranet για τις επιχειρήσεις.

Διεύθυνση MAC
Η MAC (Media Access Control) διεύθυνση αριθμό υλικού του υπολογιστή σας στο τοπικό δίκτυο (LAN). Όταν είστε συνδεδεμένοι στο Internet από τον υπολογιστή σας, έναν πίνακα αντιστοιχίας αφορά τη διεύθυνση IP σας στον υπολογιστή σας φυσική (MAC) για το LAN.

Infrastructure Mode
Ένα 802,11 δικτύωση πλαίσιο μέσα στο οποίο συσκευές επικοινωνούν μεταξύ τους με τον πρώτο να έχει μεσολαβήσει Access Point (AP). Στη λειτουργία υποδομής, ασύρματες συσκευές μπορούν να επικοινωνούν μεταξύ τους ή μπορούν να επικοινωνήσουν με ένα ενσύρματο δίκτυο. Σε γενικές γραμμές, η πλειοψηφία των εταιρικών ασύρματα δίκτυα LAN λειτουργεί κατά τον τρόπο τις υποδομές, γιατί χρειάζονται την πρόσβαση στο ενσύρματο LAN για να χρησιμοποιήσετε υπηρεσίες όπως εξυπηρετητές αρχείων ή εκτυπωτών.

peer-to-peer (P2P)
Peer-to-peer είναι ένα είδος δικτύου στο Διαδίκτυο, επιτρέποντας μια ομάδα χρηστών του ηλεκτρονικού υπολογιστή με το ίδιο πρόγραμμα δικτύωσης για να συνδέσετε μεταξύ τους για τους σκοπούς του απευθείας πρόσβαση σε αρχεία από το ένα του άλλου σκληρούς δίσκους.

Wi-Fi

Wi-Fi είναι μικρή για "Wireless Fidelity". Wi-Fi είναι χρησιμοποιείται στη θέση του 802.11b με τον ίδιο τρόπο που Ethernet χρησιμοποιείται στη θέση του IEEE 802,3. Ένας χρήστης με ένα προϊόν Wi-Fi μπορείτε να χρησιμοποιήσετε οποιαδήποτε μάρκα του σημείου πρόσβασης με οποιοδήποτε άλλο προϊόν υλικού πελάτη που είναι χτισμένο το πρότυπο Wi-Fi.

ΠΗΓΕΣ

Ασύρματες Επικοινωνίες και Δίκτυα, Stallings William, Εκδ. Τζιόλα

Δίκτυα υπολογιστών, Tanenbaum Andrew S., Εκδ. Κλειδάριθμος

IEEE 802.11 WG, IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), International Standard [for] Information Technology - Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 2007, ISBN 0-7381-5655-8

http://www.umts-forum.org/

http://www.umtsworld.com/

http://www.3gpp.org/

http://www.hellascams.gr/grc/wi_fi_calculators/knowledge_base/wi_fi_protocols.html

http://www.usr-emea.com/education/net10.asp?loc=grec

http://geekay.freehostingcloud.com/home/index.php?option=com_content&view=article&id=102:0-80211&catid=58:aircrackcat&Itemid=76

802.11 Wireless Networks - Definitive Guide, O'Reilly Press Broadband Telecommunications Handbook 2

nd

edition, McGraw – Hill Building Wireless Community Networks, O'Reilly Press Wireless LANs – Second Edition, SAMS publishing Hack Proofing Your Wireless Network, Syngress Designing a Wireless Network, Syngress IEEE P802.11 Wireless LANs, Unsafe at any key size; An analysis of the WEP encapsulation Final draft ETSI EN 300 328 V1.4.1 (2002-11) Candidate Harmonized European Standard (Telecommunications series)

http://aqua.comptek.ru/test/HiddenNode/hidden_node_en.html