



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
& ΠΛΗΡΟΦΟΡΙΚΗΣ**

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗΣ

ΔΙΚΤΥΩΝ

IEEE 802.11

ΕΥΘΑΛΗ ΙΩΑΝΝΑ

A.M 4789

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2014

Π Ε Ρ Ι Ε Χ Ο Μ Ε Ν Α

1 Εισαγωγή

1.1	Εισαγωγή στα Ασύρματα Δίκτυα.....	4
1.2	Κατηγορίες Ασύρματων Δικτύων.....	5

2 Το πρότυπο IEEE 802.11

2.1	Ιστορική Αναδρομή.....	6
2.2	Αρχιτεκτονική του IEEE 802.11.....	7
2.3	Μηχανισμοί και τρόποι λειτουργίας.....	9
2.3.1	Το φυσικό επίπεδο του 802.11.....	9
2.3.2	Το υπόστρωμα MAC.....	10
2.4	Ασφάλεια δεδομένων.....	11
2.5	Υπηρεσίες του προτύπου IEEE 802.11.....	12
2.6	Το πρωτόκολλο IEEE 802.11 και οι επεκτάσεις του.....	14

3 Ασύρματα Ad hoc δίκτυα

3.1	Εισαγωγή στα ad hoc δίκτυα.....	17
3.1.1	Κατηγορίες ad hoc δικτύων.....	18
3.1.2	Εφαρμογές ad hoc δικτύων.....	18
3.2	Παραλλαγές στα ad hoc δίκτυα.....	20
3.3	Δρομολόγηση στα ad hoc δίκτυα.....	20
3.3.1	Proactive αλγόριθμοι.....	22
3.3.2	Reactive αλγόριθμοι.....	23
3.4	Το πρωτόκολλο IEEE 802.11 στα ad hoc δίκτυα.....	26

4 Αλγόριθμοι δρομολόγησης στα ad hoc δίκτυα

4.1	Destination-Sequenced Distance-Vector (DSDV).....	27
4.2	Ad hoc on Demand Distance Vector (AODV).....	28
4.3	Dynamic Source Routing (DSR).....	29
4.4	Temporally Ordered Routing Algorithm (TORA).....	30

5 Κινητά ad hoc δίκτυα-Mobile ad hoc networking (MANET)

5.1	Τύποι MANETs.....	36
-----	-------------------	----

5.1.1	VANETs(Vehicular Ad hoc Networks).....	37
5.1.2	Αρχιτεκτονικές των VANETs.....	38
5.1.3	Πρότυπα.....	40
5.1.4	Εφαρμογές.....	41

1. ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγή στα ασύρματα δίκτυα

Με την πάροδο των χρόνων, οι ασύρματες τεχνολογίες διαδραματίζουν όλο και πιο έντονο ρόλο στη καθημερινή ζωή των ανθρώπων. Η ευελιξία που παρέχουν φάνηκε από νωρίς πως θα άνοιγε ένα τεράστιο πεδίο νέων εφαρμογών. Παράλληλα η τεχνολογική εξέλιξη έκανε δυνατή την παραγωγή συσκευών μικρού κόστους και σε μεγάλες ποσότητες. Το αποτέλεσμα όλων αυτών είναι ότι την τελευταία δεκαετία βιώνουμε την όλο και πιο έντονη παρουσία των ασύρματων τεχνολογιών φθάνοντας στην ασύρματη επανάσταση.

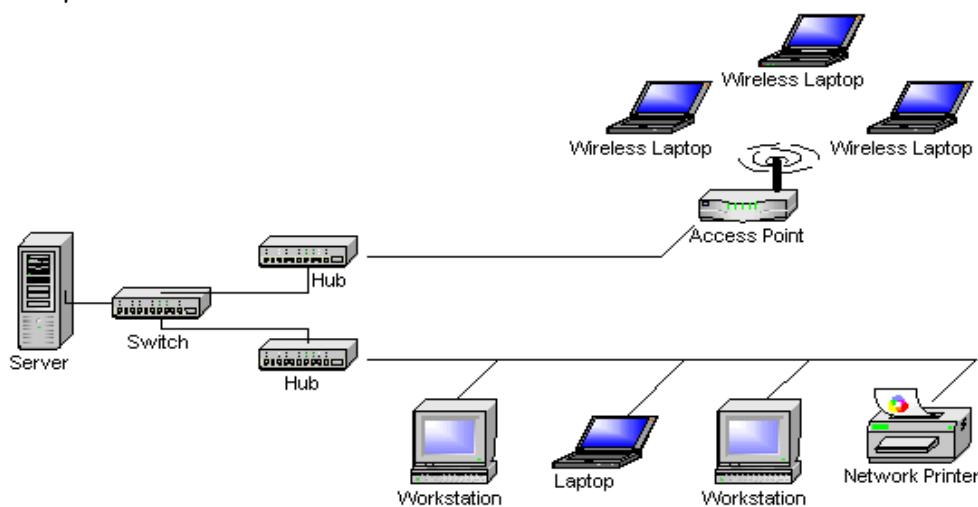
Σύμφωνα με τον ορισμό του, ως ασύρματο δίκτυο χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίξει το δίκτυο. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου. Σε παλαιότερες εποχές τα τηλεφωνικά δίκτυα ήταν αναλογικά, αλλά σήμερα όλα τα ασύρματα δίκτυα βασίζονται σε ψηφιακή τεχνολογία και, επομένως, κατά μία έννοια, είναι ουσιαστικώς δίκτυα υπολογιστών.

Στα δίκτυα υπολογιστών, μέχρι πριν κάποιο καιρό, η πιο συνηθισμένη επιλογή ήταν η δικτύωση μέσω καλωδίου Ethernet. Τα τελευταία χρόνια όμως τα ασύρματα δίκτυα αναπτύσσονται ραγδαία. Οι λόγοι είναι πολλοί και κυρίως έχουν να κάνουν με την ευελιξία και την ευκολία στην εγκατάσταση ενός ασύρματου δικτύου. Επιπλέον, τα ασύρματα δίκτυα προσφέρουν τεράστιες δυνατότητες σε επίπεδο δικτύωσης και άλλων συσκευών εκτός των ηλεκτρονικών συσκευών.

1.2 Κατηγορίες Ασύρματων Δικτύων

Στα ασύρματα δίκτυα εντάσσονται τα δίκτυα κινητής τηλεφωνίας, οι δορυφορικές επικοινωνίες, τα ασύρματα δίκτυα ευρείας περιοχής (WWAN), τα ασύρματα μητροπολιτικά δίκτυα (WMAN), τα ασύρματα τοπικά δίκτυα (WLAN) και τα ασύρματα προσωπικά δίκτυα (WPAN). Στην εργασία αυτή θα εξεταστούν τα ασύρματα τοπικά δίκτυα (WLAN).

Τα WLAN's είναι συστήματα στα οποία κάθε υπολογιστής έχει ένα ασύρματο modem και μια κεραία μέσω των οποίων μπορεί να επικοινωνεί με άλλα συστήματα. Το ασύρματο LAN με τη σειρά του μπορεί να συνδεθεί σε ένα ενσύρματο LAN ή να αποτελέσει βάση για ένα καινούργιο δίκτυο. Η βασική δομική μονάδα (building block) του WLAN είναι το κελί (cell). Το κελί είναι ουσιαστικά η περιοχή όπου η ασύρματη επικοινωνία λαμβάνει χώρα. Η περιοχή που καλύπτει ένα κελί εξαρτάται από τη ισχύ διάδοσης του ραδιοκύματος και από κάποια φυσικά χαρακτηριστικά που υπάρχουν στην περιοχή του δικτύου. Μπορούμε να φανταστούμε τη περιοχή που καλύπτει το κελί ως κυκλική. Οι σταθμοί του δικτύου μπορούν να μετακινούνται στο κελί χωρίς να χάνουν την επαφή με το δίκτυο. Η επικοινωνία μεταξύ των σταθμών μέσα στο κελί του ασύρματου δικτύου συντονίζονται από ένα σταθμό βάσης που ονομάζεται σημείο πρόσβασης (access point). Το access point μπορεί να συνδέσει πολλά κελιά ενός WLAN μεταξύ τους και μπορεί επίσης να συνδέσει τα cells του WLAN με ένα ενσύρματο Ethernet LAN μέσω καλωδίου σε μια έξοδο του Ethernet LAN. Στο παρακάτω σχήμα παρουσιάζεται μια τοπολογία WLAN.



2. ΤΟ ΠΡΟΤΥΠΟ IEEE 802.11

2.1 Ιστορική Αναδρομή

Το πρότυπο IEEE 802.11 δημιουργήθηκε τον Ιούνιο του 1997 και αποτελεί το αρχικό πρότυπο για ασύρματη δικτύωση με ρυθμό μετάδοσης μέχρι 2 Mbps. Αρχικά, το πρότυπο ήταν μέρος του προτύπου IEEE 802.4, με ονομασία 802.4L. Το 1990, η ομάδα του 802.4L μετανομάστηκε σε IEEE 802.11 W-LAN Project Committee που δημιούργησε το ανεξάρτητο πρότυπο 802 που περιελάμβανε τρία specification για το φυσικό επίπεδο (PHY) και ένα κοινό στο επίπεδο MAC. Ο στόχος του 802.11 ήταν να υπάρχει συμβατότητα μεταξύ των προϊόντων ασύρματης δικτύωσης, κατά αντιστοιχία με το πρότυπο 802.3 για την ενσύρματη δικτύωση. Πριν το 802.11 υπήρχαν Στην συνέχεια δημιουργήθηκαν υποπρότυπα του IEEE 802.11, όπως το IEEE 802.11a, IEEE 802.11b, IEEE 802.11e, IEEE 802.11f, IEEE 802.11g, IEEE 802.11n. Σήμερα τα ασύρματα δίκτυα που βασίζονται σε αυτήν την οικογένεια προτύπων είναι τα πλέον διαδεδομένα, ενώ κυκλοφορεί μεγάλη ποικιλία σχετικών προϊόντων στην αγορά.

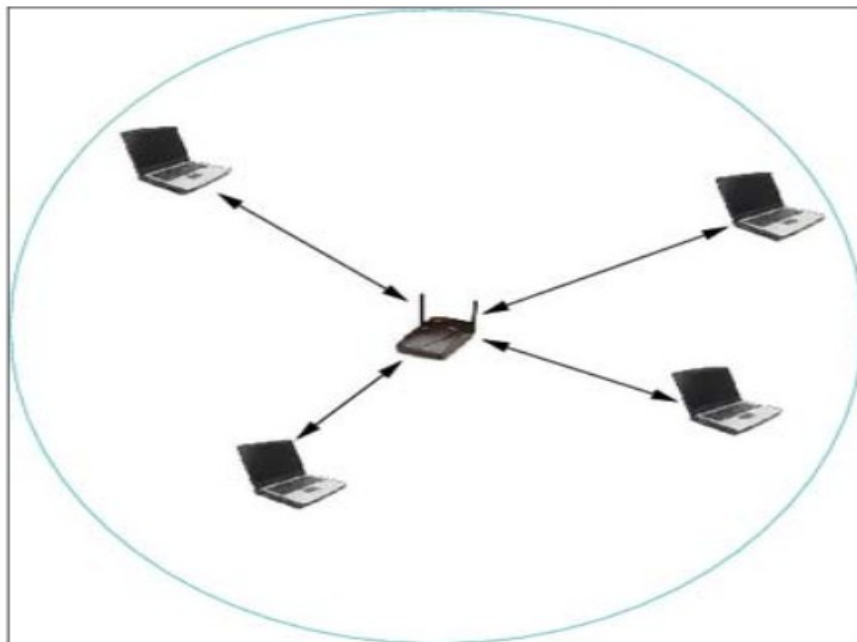
Σε πρώτη φάση το πρότυπο IEEE 802.11 θεσπίστηκε με σκοπό να εξυπηρετήσει τις ανάγκες μικρών δικτύων υπολογιστών WLAN. Η τεχνολογία Spread Spectrum χρησιμοποιήθηκε για την ανάπτυξή του πρωτοκόλλου αλλά και των διαδόχων του. Η Spread Spectrum είναι μια τεχνολογία διαμόρφωσης σήματος που διαδίδει τα προς εκπομπή δεδομένα σε όλο το διαθέσιμο φάσμα συχνοτήτων.

2.2 Αρχιτεκτονική του IEEE 802.11

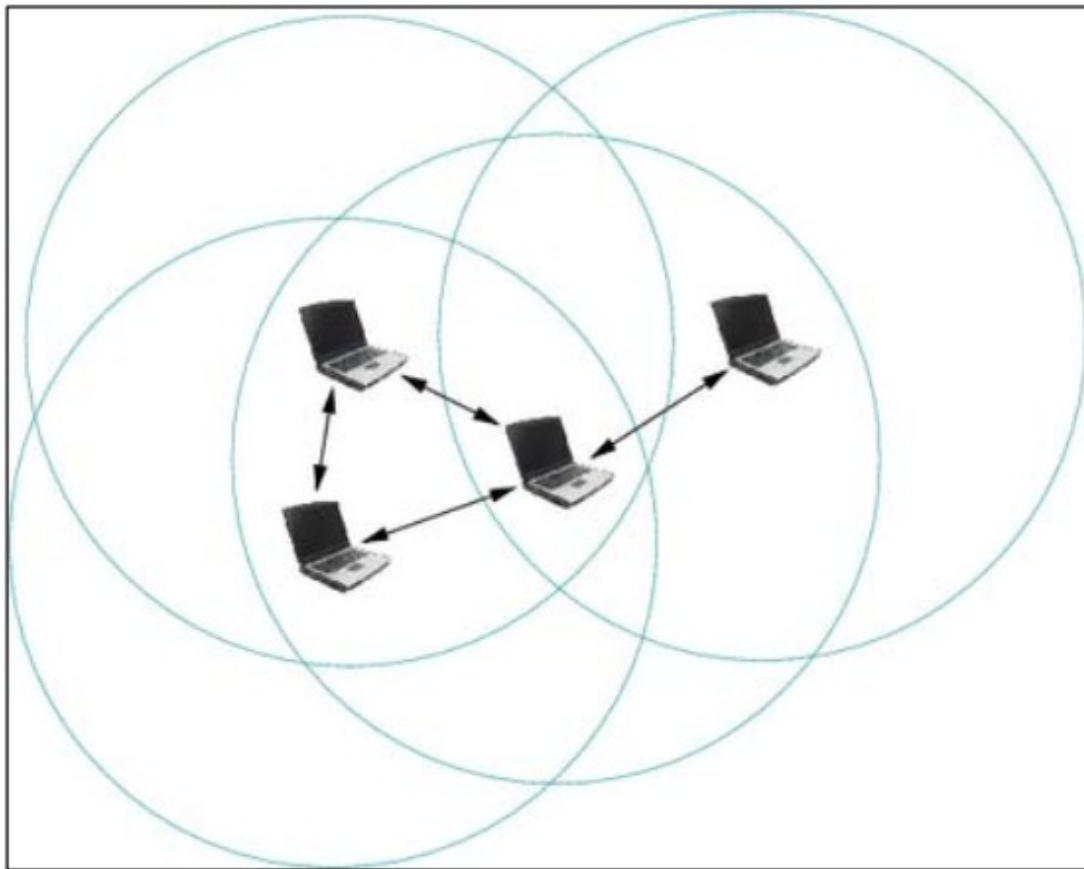
Η βασική δομική μονάδα ενός δικτύου IEEE 802.11 ονομάζεται βασικό σύνολο εξυπηρέτησης (Basic Service Set - BSS). Το βασικό σύνολο εξυπηρέτησης αποτελείται από ένα σύνολο σταθμών, οι οποίοι βρίσκονται κάτω από τον έλεγχο μιας συνάρτησης συντονισμού, είτε της DCF(**Distributed coordination function**) ή της PCF(**Point coordination function**), οι οποίες συντονίζουν την λειτουργία των

σταθμών μέσα στο δίκτυο. Έτσι οι σταθμοί μπορούν να επικοινωνούν απευθείας μεταξύ τους χρησιμοποιώντας το κοινό μέσο, δηλαδή τον αέρα ή μέσω μιας ενδιάμεσης συσκευής που αναλαμβάνει τον κεντρικό έλεγχο της επικοινωνίας. Η γεωγραφική περιοχή μέσα στην οποία μπορούν τα μέλη ενός βασικού συνόλου εξυπηρέτησης να επικοινωνούν μεταξύ τους είναι γνωστή ως βασική περιοχή εξυπηρέτησης (Basic Service Area - BSA), και είναι ανάλογη της «κυψέλης» που χρησιμοποιούν τα κυψελωτά δίκτυα επικοινωνίας. Αν κάποιος σταθμός βγει από αυτή την περιοχή, τότε πλέον δεν αποτελεί μέλος του συγκεκριμένου βασικού συνόλου εξυπηρέτησης και άρα δεν μπορεί να επικοινωνήσει πλέον με τους υπόλοιπους σταθμούς. Αντίστοιχα αν κάποιος σταθμός εισέλθει στην βασική περιοχή εξυπηρέτησης ενός βασικού συνόλου εξυπηρέτησης, τότε μπορεί να αρχίσει την επικοινωνία με τα υπόλοιπα μέλη του. Ένα παράδειγμα ενός συνόλου εξυπηρέτησης που ελέγχεται από μια μοναδα εξυπηρέτησης ή σημείο πρόσβασης (AP) φαίνεται στο παρακάτω σχήμα.

Βασικό σύνολο εξυπηρέτησης-BSS



Το βασικό σύνολο εξυπηρέτησης - BSS θα μπορούσε να χρησιμοποιηθεί για να σχηματιστεί ένα αδόμητο δίκτυο (ad hoc network). Το αδόμητο δίκτυο μπορεί να σχηματιστεί με την ομαδοποίηση δυο ή περισσότερων τερματικών σε ένα βασικό σύνολο εξυπηρέτησης, χωρίς την παρουσία κάποιας κεντρικής μονάδας που να συντονίζει την επικοινωνία τους. Η τοπολογία αυτή είναι γνωστή ως ανεξάρτητο βασικό σύνολο εξυπηρέτησης (Independent BSS - IBSS). Είναι το είδος δικτύου που δημιουργείται χωρίς προηγούμενο προγραμματισμό για να υπάρχει μόνο για όσο χρόνο χρειάζεται. Ένα τέτοιο παράδειγμα παρουσιάζεται στο παρακάτω σχήμα.

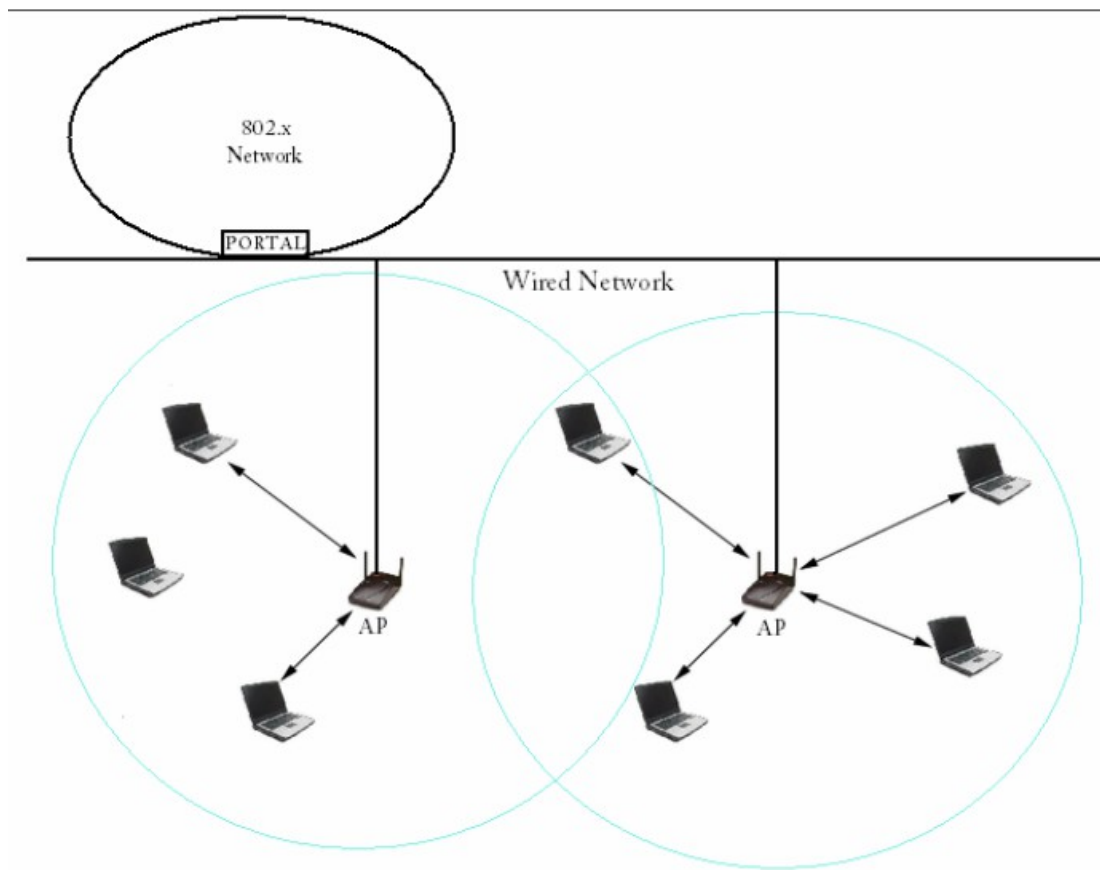


Ανεξάρτητο σύνολο εξυπηρέτησης-IBSS

Μπορούμε να συνδέσουμε δύο ή περισσότερα βασικά σύνολα εξυπηρέτησης μεταξύ τους μέσω ενός συστήματος διανομής (distribution system - DS). Μοναδική προϋπόθεση είναι να υπάρχει ένα τερματικό σε κάθε βασικό σύνολο εξυπηρέτησης το οποίο να έχει αναλάβει τον ρόλο του σημείου εξυπηρέτησης ή σημείου πρόσβασης (Access Point - AP) ανάμεσα στο βασικό σύνολο εξυπηρέτησης και στο σύστημα διανομής. Τα δίκτυα αυτά είναι γνωστά ως δίκτυα υποδομής (infrastructure

networks). Το σύστημα διανομής μπορεί ταυτόχρονα να είναι συνδεδεμένο και με κάποιο άλλο δίκτυο της οικογένειας των 802.x μέσω μίας πύλης (portal).

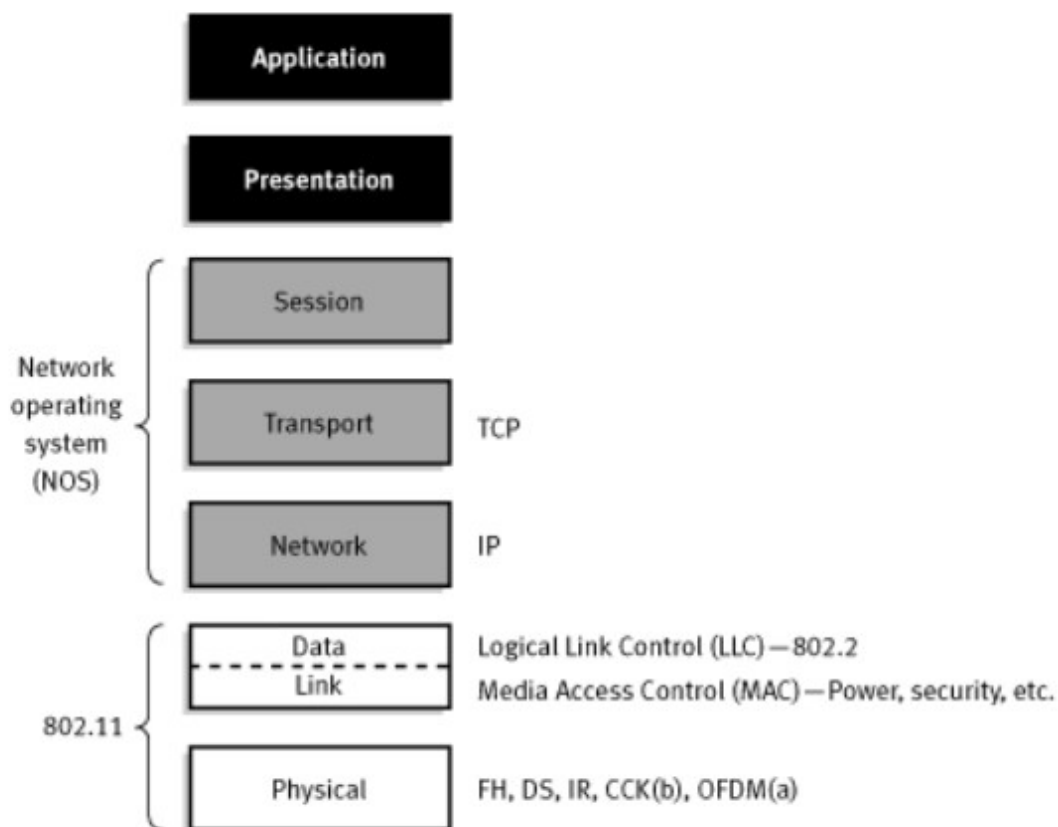
Αν συνδέσουμε πολλά συστήματα διανομής και πολλά βασικά σύνολα εξυπηρέτησης τότε δημιουργείται ένα ασύρματο δίκτυο μεγάλου μεγέθους και μεγάλης πολυπλοκότητας, το οποίο ονομάζεται σύνολο ευρείας εξυπηρέτησης (Extended Service Set - ESS). Ένα σύνολο ευρείας εξυπηρέτησης και ένα ανεξάρτητο βασικό σύνολο εξυπηρέτησης φαίνονται ίδια στο επίπεδο λογικής ζεύξης, έτσι ένα τερματικό μπορεί να κινείται από ένα βασικό σύνολο εξυπηρέτησης σε ένα άλλο, μέσα στο ίδιο σύνολο ευρείας εξυπηρέτησης, χωρίς αυτό να γίνεται αντιληπτό στο επίπεδο λογικής ζεύξης. Δύο βασικά σύνολα εξυπηρέτησης ενός συνόλου ευρείας εξυπηρέτησης μπορεί να καλύπτουν διαφορετικές περιοχές, την ίδια περιοχή, ή να έχουν κατά ένα μέρος κοινή περιοχή κάλυψης. Παράδειγμα τέτοιου δικτύου αποτελεί το σύστημα που φαίνεται παρακάτω.



ESS(Extended service set) και σύνδεση με άλλα δίκτυα μέσω ειδικής πύλης

2.3 Μηχανισμοί και τρόπος λειτουργίας

Όπως όλα τα 802.x πρότυπα, έτσι και το 802.11 επικεντρώνεται στα δύο χαμηλότερα στρώματα του μοντέλου OSI (Open System Interconnection), δηλαδή στο φυσικό στρώμα (Physical Layer-PHY) και στο υπόστρωμα MAC (Medium Access Control-Ελέγχου προσπέλασης μέσου) του στρώματος διασύνδεσης δεδομένων (Data Link Layer) .



2.3.1 Το φυσικό επίπεδο του 802.11

Το πρότυπο 802.11 του 1997 καθορίζει τρεις επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό επίπεδο.

- **Υπέρυθρες.** Η υπέρυθρη επιλογή χρησιμοποιεί διάχυτη μετάδοση στα 0,85 ή στα 0,95 micron. Επιτρέπονται δύο ταχύτητες: 1 Mbps και 2 Mbps. Στο 1Mbps χρησιμοποιείται μια μεθοδος κωδικοποίησης στην οποία κάθε ομάδα των 4 bit κωδικοποιείται ως μια κωδικολέξη των 16 bit που περιέχει δεκαπέντε 0 και ένα μόνο 1, χρησιμοποιώντας τον ονομαζόμενο κώδικα Gray. Στα 2 Mbps η κωδικοποίηση παίρνει 2 bit και παράγει μια κωδικολέξη των 4 bit όπου παλι υπάρχει ένα μόνο 1.

- **Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας ή FHSS.** Η τεχνική FHSS βασίζεται στην ιδέα της αλλαγής της φέρουσας ενός σήματος μέσα σε ένα μεγάλο εύρος συχνοτήτων και σύμφωνα με μία συγκεκριμένη ψευδοτυχαία ακολουθία (hopping pattern). Χρησιμοποιείται μία γεννήτρια ψευδοτυχαίων αριθμών για την παραγωγή της ακολουθίας συχνοτήτων στις οποίες μεταβαίνουν διαδοχικά οι σταθμοί. Όσο όλοι οι σταθμοί χρησιμοποιούν το ίδιο φυτό (seed) στη γεννήτρια ψευδοτυχαίων αριθμών και παραμένουν χρονικά συγχρονισμένοι, θα εκτελούν ταυτόχρονα τη μετάβαση στις ίδιες συχνότητες. Η χρονική διάρκεια στην οποία μένουμε στην ίδια συχνότητα, δηλαδή το **dwell time** (χρόνος παραμονής) είναι μια ρυθμιζόμενη παράμετρος, αλλά θα πρέπει να είναι μικρότερη από 400 msec.
- **Εξάπλωση Φάσματος 'Αμεσης Ακολουθίας ή DSSS.** Η DSSS τεχνική είναι η πιο επιτυχημένη που έχει χρησιμοποιηθεί σε συνδυασμό με τα ασύρματα δίκτυα. Σε σχέση με την FHSS τεχνική μετάδοσης απαιτεί περισσότερη ενέργεια για να επιτύχει παρόμοια διέλευση, όμως το μεγάλο πλεονέκτημά της είναι ότι μπορεί εύκολα να αναβαθμιστεί για την επίτευξη υψηλότερων ρυθμών μετάδοσης. Η DSSS περιορίζεται σε 1 ή 2 Mbps.

Το 1999 παρουσιάστηκαν δύο νέες τεχνικές για επίτευξη υψηλότερου εύρους ζώνης. Οι τεχνικές αυτές ονομάζονται **OFDM** και **HR-DSSS**. Λειτουργούν μέχρι τα 54 Mbps και τα 11 Mbps, αντίστοιχα. Το 2001 παρουσιάστηκε μια δευτερή τεχνική διαμόρφωσης OFDM, αλλά σε διαφορετική ζώνη συχνοτήτων από την πρώτη.

2.3.2 Υποεπίπεδο MAC

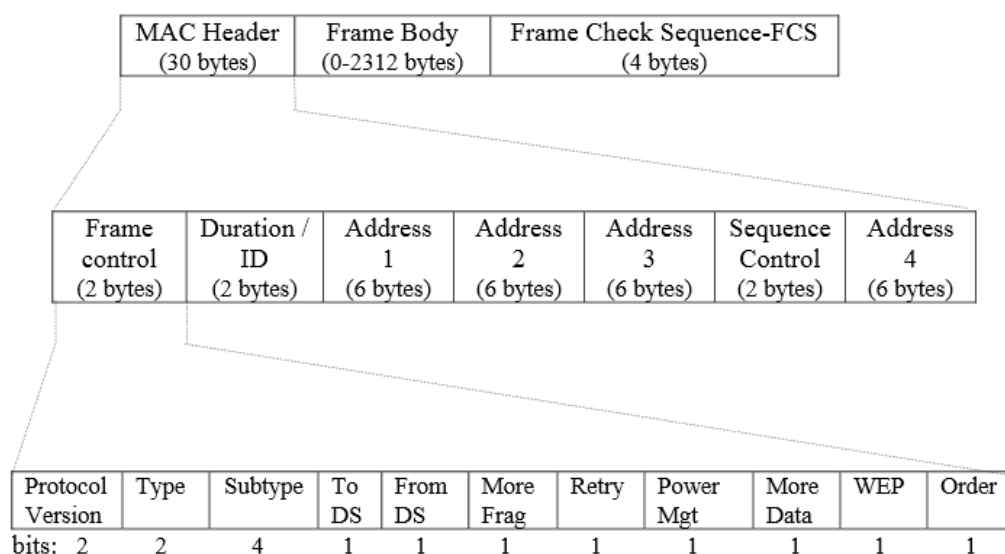
Το τμήμα αυτό καθορίζει τα μέσα για να γίνει δυνατή η πρόσβαση στο ασύρματο μέσο και είναι υπεύθυνο για τα πλαίσια που μεταδίδονται, τη μορφή τους, τον έλεγχο λαθών, τον τεμαχισμό και την επανασυγκόλληση τους. Το πρωτόκολλο MAC που χρησιμοποιείται είναι ένα πρωτόκολλο CSMA/CA που ονομάζεται κατανεμημένη θεμελίωση ασύρματου MAC (Distributed Foundation Wireless MAC, DFWMAC) και είναι παρόμοιο με το αντίστοιχο πρωτόκολλο του προτύπου 802.3 για τα ενσύρματα δίκτυα Ethernet. Το DFWMAC αναφέρεται και ως κατανεμημένη συνάρτηση συντονισμού (Distributed Coordination Function, DCF) η οποία προσφέρει μόνο μια υπηρεσία καλύτερης δυνατής προσπάθειας. Η DCF είναι γνωστή ως μέθοδος πολλαπλής πρόσβασης με ανίχνευση φέροντος και με αποφυγή

συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA). Πρόκειται για μία κατανεμημένη λειτουργία του δικτύου, κατά την διάρκεια της οποίας όλα τα τερματικά έχουν την ίδια προτεραιότητα και ανταγωνίζονται επί ίσοις όροις για την κατάληψη του μέσου.

Επίσης, καθορίζει μια υπηρεσία γνωστή ως σημειακή συνάρτηση συντονισμού(Point Coordination Function, PCF), που χρησιμοποιείται για τις χρονικά εξαρτώμενες υπηρεσίες μέσω χρήσης ενός μηχανισμού που δεν απαιτεί ανταγωνισμό και προσφέρεται μόνο για τα δίκτυα υποδομής (infrastructure networks) . Στην σημειακή λειτουργία συγχρονισμού ένα τερματικό υψηλής προτεραιότητας αναλαμβάνει για ένα χρονικό διάστημα την διαχείριση του δικτύου και δίνει με τη σειρά δυνατότητα εκπομπής στα τερματικά υψηλής προτεραιότητας. Έτσι εξυπηρετούνται καλύτερα τα τερματικά υψηλής προτεραιότητας, αυτά δηλαδή που στέλνουν ευαίσθητα ως προς τον χρόνο δεδομένα , όπως η φωνή και κυρίως το video.

Είδη πλαισίων

Υπάρχουν τρία είδη πλαισίων: τα πλαίσια δεδομένων (data frames), τα πλαίσια ελέγχου (control frames) και τα πλαίσια διαχείρισης (management frames). Η γενική μορφή ενός πλαισίου (frame) του υπό επιπέδου MAC δίνεται στο παρακάτω σχήμα. Κάθε πλαίσιο αποτελείται από τρία τμήματα: την Επικεφαλίδα του υποεπιπέδου ελέγχου πρόσβασης μέσου (MAC Header), το Σώμα πλαισίου (Frame Body) και την Ακολουθία ελέγχου πλαισίου (Frame Check Sequence – FCS).



Το τμήμα του Σώματος πλαισίου (Frame Body) περιέχει είτε τα δεδομένα που στέλνει ένα τερματικό, όταν πρόκειται για πλαίσιο δεδομένων, είτε κάποιες άλλες πληροφορίες χρήσιμες για την λειτουργία του δικτύου, όταν πρόκειται για πλαίσιο διαχείρισης του δικτύου. Σε κάποια είδη πλαισίων μπορεί το τμήμα του Σώματος πλαισίου να μην χρησιμοποιείται και έτσι αυτό παραλείπεται.

Το τμήμα Ακολουθία ελέγχου πλαισίου (Frame Check Sequence – FCS) χρησιμοποιείται στην επαλήθευση της σωστής λήψης του πλαισίου. Στο τμήμα αυτό περιέχεται μία τιμή που προκύπτει από έναν κώδικα που ονομάζουμε Κυκλικό κώδικα ελέγχου σφάλματος με τη μέθοδο προσθήκης πλεονασμού (32-bit Cyclic Redundancy Code - CRC), ο οποίος αναφέρεται στο προηγούμενο τμήμα του πακέτου, δηλαδή στην Επικεφαλίδα και στο Σώμα πλαισίου. Ο παραλήπτης του πακέτου χρησιμοποιεί τον ίδιο κώδικα για το ίδιο τμήμα του πακέτου και συγκρίνει την τιμή που βρίσκει με αυτήν που είναι αποθηκευμένη στο τμήμα της Ακολουθίας ελέγχου πλαισίου. Έτσι, μπορεί να καταλάβει αν το πακέτο που έλαβε έχει σταλεί σωστά, όταν οι δύο αριθμοί ταυτίζονται, ή αν έγινε κάποιο λάθος κατά την μετάδοσή του, όταν οι αριθμοί είναι διαφορετικοί.

Το τμήμα της Επικεφαλίδας (MAC Header) χωρίζεται σε επτά υπό τμήματα, όπως στο σχήμα. Αυτά είναι ο Έλεγχος πλαισίου (Frame Control), η Διάρκεια/αναγνώριση (Duration / Identification - ID), η Διεύθυνση 1 (Address 1), η Διεύθυνση 2 (Address 2), η Διεύθυνση 3 (Address 3), ο Έλεγχος ακολουθίας (Sequence Control) και η Διεύθυνση 4 (Address 4). Κάποια ή ακόμη και όλα από τα τμήματα Διεύθυνση 2, Διεύθυνση 3, Διεύθυνση 4 και Έλεγχος ακολουθίας μπορεί να μην περιέχονται σε κάποια είδη πακέτων.

Το τμήμα της Διάρκειας/αναγνώρισης περιέχει, ανάλογα με το είδος του πλαισίου, είτε την διάρκεια κράτησης του μέσου από κάποιο τερματικό, είτε τον αριθμό αναγνώρισης του βασικού συνόλου εξυπηρέτησης (BSSID). Ο συνδυασμός των τεσσάρων τμημάτων διευθύνσεων μαζί με τα υπό τμήματα «Προς σύστημα διανομής» (To DS) και «Από σύστημα διανομής» (DS) του Ελέγχου πλαισίου, δίνει τις διευθύνσεις του αποστολέα (source address), του παραλήπτη (destination address) και του βασικού συνόλου εξυπηρέτησης (BSSID). Το τμήμα του Ελέγχου ακολουθίας περιέχει τον αριθμό του πλαισίου (sequence number) που εκπέμπεται, καθώς και τον αριθμό του τεμαχίου του πλαισίου (fragment number), όταν πρόκειται για πλαίσιο που έχει τεμαχιστεί σε μικρότερα.

Το τμήμα Έλεγχος πλαισίου χωρίζεται επίσης σε υπό τμήματα όπως στο σχήμα. Αυτά είναι η Έκδοση του πρωτοκόλλου (Protocol Version), ο Τύπος (Type) και ο Υπότυπος (Subtype) του πλαισίου, τα τμήματα Προς σύστημα διανομής (To DS) και Από σύστημα διανομής (From DS), το τμήμα Περισσότερα τεμάχια (More Fragments), το τμήμα Επαναεκπομπής (Retry), η Διαχείριση ισχύος (Power Management), το τμήμα Περισσότερα δεδομένα (More data), το τμήμα κωδικοποίησης WEP (Wired Equivalent Privacy) και το τμήμα Σειράς (Order).

2.4 Ασφάλεια δεδομένων

Τα πρώτα πέντε χρόνια της ύπαρξής του, το πρότυπο IEEE 802.11 για ασύρματα δίκτυα, καθόριζε μόνο μία μέθοδο για την ασφάλεια των δεδομένων που διακινούνται ανάμεσα στους χρήστες του δικτύου. Η μέθοδος αυτή ονομάζεται **Wired Equivalent Privacy (WEP)** και όπως δηλώνει η ονομασία της, σκοπός είναι να παρέχει στο ασύρματο δίκτυο ασφάλεια του ίδιου επιπέδου με τα ενσύρματα δίκτυα. Αυτό είναι εν γένει δύσκολο αφού κάποιος αποκτά πιο εύκολα πρόσβαση στο μέσο που χρησιμοποιείται για τις ασύρματες επικοινωνίες, δηλαδή τον αέρα, παρά στα καλώδια ενός ενσύρματου δικτύου. Το πρότυπο IEEE 802.11 ορίζει δύο μεθόδους ασφάλειας: την ανοικτή ασφάλεια (open security) και την ασφάλεια κοινού κλειδιού (shared key). Η δεύτερη μέθοδος βασίζεται στη χρήση ενός κοινού μυστικού κλειδιού και αποτελεί ουσιαστικά το σύστημα WEP, ενώ η πρώτη συνεπάγεται μηδενική ασφάλεια.

Μέχρι το 2000 η δημοτικότητα των ασύρματων δικτύων αυξήθηκε σημαντικά και προσέλκυσαν το ενδιαφέρον της κρυπτογραφικής κοινότητας. Σύντομα πολλοί επιστήμονες διαπίστωσαν αδυναμίες στη συνολική προσέγγιση της ασφάλειας που παρέχει το WEP. Μέχρι το τέλος του 2001, υπήρχαν στο διαδίκτυο εργαλεία που παραβίαζαν οποιαδήποτε δικλείδα ασφάλειας του WEP και μάλιστα σε σύντομο χρονικό διάστημα.

Το WEP αποτελεί για πολλούς χρήστες ακόμη και σήμερα τη μοναδική επιλογή για την προστασία των δεδομένων που ανταλλάσσουν μέσω ενός ασύρματου δικτύου. Μέχρι την πλήρη μετάβαση στο νέο πρωτόκολλο ασφάλειας (**CCMP**), που απαιτεί την αλλαγή όλων των ασύρματων συσκευών καθώς βασίζεται σε διαφορετικό αλγόριθμο κρυπτογράφησης, υπάρχει η λύση του TKIP, που προσφέρει μεγαλύτερα επίπεδα ασφάλειας απαιτώντας απλά την αναβάθμιση του firmware και πιθανώς του λογισμικού (driver) της συσκευής. Παρόλες τις αδυναμίες του, το WEP είναι πολύ καλύτερη λύση από το να μην υπάρχει καθόλου ασφάλεια, αρκεί να γνωρίζεις κανείς

τις αδυναμίες του. Άλλωστε οι περισσότερες επιθέσεις βασίζονται στη συλλογή μεγάλου δείγματος δεδομένων που μεταδίδονται και επομένως για έναν οικιακό χρήστη, όπου τα πακέτα που διακινούνται είναι λίγα, το WEP αποτελεί αρκετά ασφαλή επιλογή.

2.5 Υπηρεσίες του προτύπου IEEE 802.11

Το πρότυπο 802.11 καθορίζει ότι κάθε ασύρματο LAN που συμμορφώνεται με το πρότυπο πρέπει να παρέχει εννιά υπηρεσίες. Οι υπηρεσίες αυτές διαιρούνται σε δύο κατηγορίες: πέντε υπηρεσίες διανομής και τέσσερις υπηρεσίες σταθμών. Οι υπηρεσίες διανομής σχετίζονται με τη διαχείριση των μελών μιας κυψέλης και την αλληλεπίδραση με σταθμούς εκτός της κυψέλης. Αντιθέτως, οι υπηρεσίες σταθμών ασχολούνται με τις δραστηριότητες μέσα σε μία μόνο κυψέλη.

Οι πέντε υπηρεσίες διανομής παρέχονται από τους σταθμούς βάσης και ασχολούνται με τη δυνατότητα μετακίνησης των σταθμών καθώς αυτοί εισέρχονται και εγκαταλείπουν τις κυψέλες, συνδεδεμένοι και αποσυνδεδεμένοι από τους σταθμούς βάσης. Οι υπηρεσίες αυτές είναι οι ακόλουθες:

1. **Συσχέτιση** (Association). Η υπηρεσία αυτή χρησιμοποιείται από τους κινητούς σταθμούς για να συνδεθούν με τους σταθμούς βάσης.

2. **Αποσυσχέτιση** (Disassociation). Είτε ο σταθμός είτε ο σταθμός βάσης μπορούν να αποσυνδεθούν, τερματίζοντας έτσι τη συσχέτιση. Ο σταθμός θα πρέπει να χρησιμοποιεί την υπηρεσία αυτή πριν απενεργοποιηθεί από την κυψέλη, ενώ ο σταθμός βάσης μπορεί επίσης να τη χρησιμοποιήσει πριν απενεργοποιηθεί για λόγους συντήρησης.

3. **Επανασυσχέτιση** (Reassociation). Με την υπηρεσία αυτή ένας σταθμός μπορεί να αλλάξει τον προτιμώμενο σταθμό βάσης.

4. **Διανομή** (Distribution). Η υπηρεσία αυτή προσδιορίζει πως θα δρομολογούνται τα πλαίσια που στέλνονται στο σταθμό βάσης.

5. **Ενοποίηση** (Integration). Όταν ένα πλαίσιο πρέπει να σταλεί μέσω ενός δικτύου που δεν είναι μορφής 802.11 και χρησιμοποιεί διαφορετική μέθοδο διευθυνσιοδότησης ή μορφή πλαισίων, η υπηρεσία αυτή διαχειρίζεται τη μετατροπή από τη μορφή του 802.11 στη μορφή που απαιτείται από το δίκτυο προορισμού.

Οι υπόλοιπες τεσσέρις υπηρεσίες είναι εσωτερικές στις κυψέλες. Χρησιμοποιούνται αφού πραγματοποιηθεί η συσχέτιση (σύνδεση), και είναι οι ακόλουθες.

1. **Πιστοποίηση ταυτότητας** (Authentication). Επειδή οι ασύρματες μεταδόσεις είναι εύκολο να σταλούν ή να ληφθούν από μη εξουσιοδοτημένους σταθμούς, ο σταθμός θα πρέπει να πιστοποιήσει την ταυτότητά του πριν επιτραπεί να στείλει δεδομένα.

2. **Ακύρωση πιστοποίησης ταυτότητας** (Deauthentication). Όταν ένας σταθμός που έχει ήδη πιστοποιηθεί θέλει να εγκαταλείψει το δίκτυο, ακυρώνεται η πιστοποίησή του.

3. **Προστασία Απορρήτου** (Privacy). Για να διατηρούνται εμπιστευτικές οι πληροφορίες που στέλνονται μέσω ενός ασύρματου LAN, θα πρέπει να κρυπτογραφούνται. Η υπηρεσία αυτή διαχειρίζεται την κρυπτογράφηση και την αποκρυπτογράφηση.

4. **Παράδοση δεδομένων** (Data delivery). Τέλος, αφού η μετάδοση δεδομένων είναι ο σκοπός του δικτύου, το 802.11 είναι φυσικό να παρέχει μια μέθοδο μετάδοσης και λήψης δεδομένων.

2.6 Το πρωτόκολλο IEEE 802.11 και οι επεκτάσεις του

Μετά το αρχικό πρότυπο του 802.11 που δημιουργήθηκε το 1997, με την πάροδο των χρόνων ακολούθησαν και άλλα υποπρότυπα τα οποία αναφέρονται παρακάτω.

IEEE 802.11b

Αναπτύχθηκε το 1999 και αποτελεί μια επέκταση στο αρχικό πρότυπο. Συγκεκριμένα υποστηρίζει μετάδοση επιπλέον σε ρυθμούς 5.5 και 11Mbps με κωδικοποίηση CCK (Complementary Code Keying). Μια δεύτερη κωδικοποίηση, PBCC (Packet Binary Convolutional Code) ορίστηκε για προαιρετική υλοποίηση υποστηρίζοντας μετάδοση 5.5 και 11Mbps και έχοντας ελαφρά καλύτερη ευαισθησία δέκτη με αντίτιμο την πολυπλοκότητα. Η μετάδοση γίνεται στη ζώνη συχνοτήτων των 2.4GHz.

Είναι το πιο δημοφιλές από όλα τα πρότυπα και το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα, όντας ένα στιβαρό, αποτελεσματικό και δοκιμασμένο πρότυπο.

Οι προσθήκες της 802.11b σε σχέση με την 802.11 αφορούν μόνο τον τρόπο μετάδοσης, ενώ ο τρόπος πρόσβασης των συσκευών και οι τρόποι λειτουργίας μένουν οι ίδιοι.

Μία συσκευή που εργάζεται ακολουθώντας το 802.11b, υλοποιεί και τους τρόπους μετάδοσης του 802.11 και έτσι είναι συμβατή με αυτό. Αυτή η ιδιότητα ονομάζεται συμβατότητα προς τα πίσω, δηλαδή ότι οι καινούργιες συσκευές θα μπορούν να συνεργαστούν και με παλιότερες, προκειμένου να μην αναγκαστεί ο καταναλωτής να αλλάξει εξ ολοκλήρου τον εξοπλισμό του.

IEEE 802.11a

Το 1999 δημιουργήθηκε η επέκταση στο αρχικό πρότυπο που προβλέπει μετάδοση στη ζώνη συχνοτήτων U-NII των 5GHz με ρυθμούς μετάδοσης 1, 2, 5.5, 11, 6, 12, 24 Mbps και προαιρετικά 36, 48, 54 Mbps χρησιμοποιώντας OFDM (Orthogonal Frequency Division Multiplexing) διαμόρφωση.

Η επέκταση αυτή αποσκοπούσε να καλύψει την ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης. Επιλέχθηκε η λειτουργία σε μια υψηλότερη ζώνη συχνοτήτων, αφενός για να μπορούν να υποστηριχθούν οι μεγαλύτεροι ρυθμοί, αφετέρου ώστε να μην υπάρχει παρεμβολή από τις προηγούμενες συσκευές.

Οι αντίστοιχες συσκευές είναι ασύμβατες με αυτές που εργάζονται με το 802.11b, αφού ο τρόπος μετάδοσης, αλλά και οι ραδιοσυχνότητες που χρησιμοποιούνται είναι διαφορετικές.

IEEE 802.11g

Το 802.11g αποτελεί επέκταση στο 802.11b ώστε να υποστηρίζει μεγαλύτερους ρυθμούς. Έτσι εκτός από τους ρυθμούς μετάδοσης του 802.11b, με CCK διαμόρφωση, υποστηρίζει και ρυθμούς μέχρι 54Mbps χρησιμοποιώντας OFDM διαμόρφωση. Οι αντίστοιχες συσκευές εργάζονται στη ζώνη συχνοτήτων των 2.4GHz, διατηρώντας συμβατότητα προς τα πίσω με το 802.11b.

Συνοπτικός πίνακας ασύρματων 802.11 τεχνολογιών.

	802.11b	802.11a	802.11g
Μέγιστος ρυθμός μετάδοσης (Mbps)	11	54	54
Τύπος διαμόρφωσης	CCK	OFDM	CCK & OFDM
Υποστηριζόμενοι ρυθμοί μετάδοσης	1, 2, 5.5, 11Mbps	6, 9, 12, 18, 24, 36, 48, 54Mbps	OFDM: 6, 9, 12, 18, 24, 36, 48, 54Mbps CCK: 1, 2, 5.5, 11Mbps
Συχνότητες	2.4 – 2.497 GHz	5.15-5.35GHz 5.425-5.675GHz 5.725-5.875GHz	2.4 – 2.497 GHz

Πέρα των βασικών πρωτοκόλλων η οικογένεια προτύπων 802.11 περιλαμβάνει έναν αριθμό συμπληρωματικών προτύπων που προσθέτουν επιπλέον λειτουργικότητα στα ασύρματα δίκτυα:

IEEE 802.11c

Λειτουργία γεφύρωσης (bridging) πλαισίων 802.11

IEEE 802.11d

Επεκτάσεις στο πρότυπο ώστε να λειτουργεί σε επιπλέον ρυθμιστικά πλαίσια (άλλες ζώνες συχνοτήτων)

IEEE 802.11e

Υποστήριξη QoS στο MAC επίπεδο (EDCF, Enhanced DCF και HCF, Hybrid Coordination Function)

IEEE 802.11f

Συνιστώμενη πρακτική για το πρωτόκολλο IAPP, Inter Access Point Protocol, που αφορά την επικοινωνία μεταξύ σημείων πρόσβασης.

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. Περιγραφή πρωτοκόλλων 802.1X, TKIP και AES.

3. ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ

3.1 Εισαγωγή στα ad hoc δίκτυα

Στα δίκτυα υπολογιστών ο όρος «ad-hoc» χρησιμοποιείται για να δηλώσει μια μέθοδο διασύνδεσης η οποία συνήθως σχετίζεται με ασύρματα δίκτυα. Δεν υπάρχει συγκεκριμένη ορολογία στα ελληνικά η οποία να δηλώνει ένα ad-hoc δίκτυο, και ένα τέτοιο δίκτυο ονομάζεται είτε αδόμητο είτε κατ' απαίτηση δίκτυο, με τον δεύτερο όρο να επικρατεί στη βιβλιογραφία. Τα δίκτυα ad-hoc εντάσσονται σε μια ευρύτερη κατηγορία δικτύων (Distributed Transient Network) η οποία ορίζεται σαν τα δίκτυα αυτά τα οποία είναι εν γένει αποκεντρωμένα και αποτελούνται κυρίως από κόμβους τα οποία δεν ανήκουν εξ ορισμού και διαρκώς στο δίκτυο αλλά έχουν την δυνατότητα να εισέρχονται ή να αποχωρούν από το δίκτυο οποιαδήποτε στιγμή και από οποιοδήποτε σημείο του.

Η σύνδεση που πραγματοποιείται κατά μήκος ενός κατ' απαίτηση δικτύου πραγματοποιείται καθ' όλη τη διάρκεια μιας σύζευξης και δεν απαιτεί την ύπαρξη σταθμού βάσης. Αντίθετα, οι συσκευές ανακαλύπτουν την ύπαρξη άλλων συσκευών που βρίσκονται γύρω τους για να δημιουργήσουν ένα δίκτυο που αποτελείται από αυτές τις συσκευές. Οι συνδέσεις πραγματοποιούνται δια μέσου πολλών κόμβων (multihop ad hoc network). Οι κόμβοι του δικτύου παίζουν ενεργό ρόλο κατά την δρομολόγηση των πακέτων, προωθώντας εκτός από τα δικά τους πακέτα και τα πακέτα γειτονικών κόμβων. Αυτό το χαρακτηριστικό είναι χρήσιμο σε περιπτώσεις που ο αποστολέας και ο παραλήπτης ενός πακέτου δεν βρίσκονται εντός της ακτίνας ο ένας του άλλου (ή πιθανόν μόνο ο ένας από τους δύο βρίσκεται εντός της ακτίνας του άλλου). Κάθε κόμβος έχει τη δυνατότητα να λάβει και να προωθήσει δεδομένα σε άλλους κόμβους. Αυτό έρχεται σε αντίθεση με παλαιότερες δικτυακές τεχνολογίες όπου υπάρχουν κόμβοι με αποκλειστική λειτουργία την προώθηση των δεδομένων σε άλλους κόμβους, όπως για παράδειγμα οι routers.

Τα πρωτόκολλα δρομολόγησης στη συνέχεια αναλαμβάνουν την παροχή αξιόπιστων συνδέσεων ακόμα κι αν οι κόμβοι μετακινούνται. Έτσι η τοπολογία του

δικτύου μπορεί να μεταβάλλεται ραγδαία και απρόβλεπτα. Ένα τέτοιο δίκτυο μπορεί να λειτουργεί αυτόνομα ή μπορεί να συνδέεται στο Internet, και η ύπαρξη του συνήθως δεν είναι μόνιμη. Εξαιτίας της φορητής και μη δομημένης φύσης των δικτύων ad hoc εγείρεται ένα σύνολο από νέες απαιτήσεις κατά το σχεδιασμό τους. Καταρχήν απαιτείται το δίκτυο να είναι αυτορυθμιζόμενο όσον αφορά στις διευθύνσεις και τη δρομολόγηση, ενώ σε επίπεδο εφαρμογής οι χρήστες του δικτύου συνήθως επικοινωνούν και συνεργάζονται ως ομάδες. Αυτό εγείρει ένα μεγάλο σύνολο προβλημάτων και προκλήσεων που θα πρέπει να αντιμετωπιστούν για την αποτελεσματική επικοινωνία.

3.1.1 Κατηγορίες ad hoc δικτύων

Τα ad hoc δίκτυα μπορούν να χωριστούν σε 2 κατηγορίες: Στα **στατικά** και στα **κινητά**. Στα στατικά δίκτυα οι κόμβοι από τη στιγμή που εισέρχονται στο δίκτυο, συνήθως δε μετακινούνται. Παράδειγμα αυτής της κατηγορίας αποτελούν τα δίκτυα που σχηματίζονται μεταξύ κεραιών που βρίσκονται στις οροφές κτηρίων. Αντίθετα στα κινητά ad hoc δίκτυα (**Mobile Ad hoc Networks – MANET**), οι κόμβοι μπορούν να κινούνται αυθαίρετα. Τυπικά παραδείγματα όπου εφαρμόζονται τα MANET είναι η διασύνδεση κινούμενων οχημάτων ή συσκευών χειρός.

3.1.2 Εφαρμογές ad hoc δικτύων

Αν και η έρευνα στα ad hoc δίκτυα έχει ενταθεί τα τελευταία χρόνια, η απαρχή της εντοπίζεται τη δεκαετία του 70 και είχε αρχικά αμιγώς στρατιωτικό χαρακτήρα (κάτι συνηθισμένο στις τεχνολογίες). Η ευελιξία και η δυναμική φύση των ad hoc δικτύων τα κατατάσσουν ως την ιδανική λύση για διάφορες **στρατιωτικές εφαρμογές**, κατά τις οποίες η κατασκευή υποδομών δεν είναι χρονικά εφικτή. Ακόμα όμως κι αν υπήρχε χρόνος για τη δημιουργία σταθμών βάσης, το όλο δίκτυο θα ήταν πολύ ευάλωτο στις επιθέσεις. Τα στρατιωτικά οχήματα σε ένα πεδίο μάχης ή ένας στόλος πλοίων στη θάλασσα αποτελούν περιπτώσεις τέτοιων δικτύων.

Η ανάπτυξη νέων τεχνολογιών, όπως το *Bluetooth* και το *IEEE 802.11*, διευκόλυναν την επέκταση των ad hoc δικτύων πέρα από τον στρατιωτικό τομέα. Σημαντική εφαρμογή των ad hoc δικτύων αποτελούν τα **δίκτυα αισθητήρων** (Sensor Networks). Σε αυτά, οι αυτόνομοι κόμβοι του δικτύου περιέχουν αισθητήρες που καταγράφουν μετρήσεις για διάφορα φυσικά ή περιβαλλοντικά μεγέθη. Έτσι, για

παράδειγμα, αξιοποιώντας τις μετρήσεις που στέλνουν οι αισθητήρες, το κέντρο ελέγχου μιας κρίσιμης υποδομής μπορεί να έχει συνέχεια μια ολοκληρωμένη εικόνα της κατάστασης της υποδομής. Τοποθετώντας αισθητήρες σε δάση, το δασαρχείο μπορεί να ενημερώνεται έγκαιρα για την παρουσία καπνού προλαβαίνοντας την εξάπλωση της φωτιάς. Η χρήση των δικτύων αισθητήρων επεκτείνεται στον ανθρώπινο οργανισμό, στο οδικό δίκτυο, στις μηχανές παραγωγής, στα έξυπνα σπίτια κ.α. με τον πλήθος των εφαρμογών τους να πολλαπλασιάζεται.

Παρακάτω παρουσιάζονται μερικά περιβάλλοντα που εκμεταλλεύονται την ευελιξία και την ευκολία δημιουργίας των ad hoc δικτύων για την επίτευξη επικοινωνίας.

Επιχειρήσεις ομάδων διάσωσης: Τα μέλη της ομάδας, συνήθως κάτω από αντίξοες συνθήκες, πρέπει να βρίσκονται σε συνεχή επικοινωνία για την ανταλλαγή σχετικών πληροφοριών.

Υποανάπτυκτες περιοχές: Χώρες του τρίτου κόσμου αποτελούμενες από δύσβατα εδάφη, έχουν τη δυνατότητα να εγκαταστήσουν απευθείας ad hoc δίκτυα, χωρίς να πρέπει πρώτα να ξοδέψουν τον χρόνο, το χρήμα και την ενέργεια που απαιτούνται κατά την εγκατάσταση ενός ενσύρματου δικτύου.

Εμπορικά περιβάλλοντα: Προσφέρουν υπηρεσίες όπως το ηλεκτρονικό εμπόριο, τη δυναμική πρόσβαση σε στοιχεία πελατών που είναι αποθηκευμένα σε μια κεντρική μονάδα, την παροχή συνεπών βάσεων δεδομένων προς όλους τους πελάτες κ.α.

Εκπαιδευτικές εφαρμογές: Όπως η δημιουργία εικονικών τάξεων ή συνεδριακών αιθουσών, η εγκαθίδρυση ad hoc επικοινωνίας κατά τη διάρκεια συνεδρίων, meetings ή διαλέξεων κ.α.

Υπηρεσίες με γνώση της τοποθεσίας: Περιλαμβάνουν υπηρεσίες πληροφορίας, όπως για παράδειγμα διαφήμιση ειδικών υπηρεσιών της τοποθεσίας ή εμφάνιση σε έναν τουρίστα ενός ταξιδιωτικού οδηγού μόλις εισέρχεται στην συγκεκριμένη περιοχή κ.α.

3.2 Παραλλαγές στα ad hoc δίκτυα

Ανάλογα με τις δυνατότητες και τις ευθύνες κάθε κόμβου προκύπτουν παραλλαγές των ad hoc δικτύων. Διακρίνονται οι εξής περιπτώσεις:

1. Πλήρως Συμμετρικό Περιβάλλον

Όλοι οι κόμβοι έχουν τις ακριβώς τις ίδιες δυνατότητες και ευθύνες.

2. Ασύμμετρες Ευθύνες

- Μόνο κάποιοι κόμβοι μπορούν να δρομολογήσουν πακέτα
- Κάποιοι κόμβοι μπορεί να λειτουργήσουν σαν αρχηγοί των γειτονικών κόμβων (π.χ. αρχηγός συστάδας στα δίκτυα αισθητήρων)

3. Ασύμμετρες Δυνατότητες

- Η εμβέλεια μετάδοσης , η διάρκεια ζωής της μπαταρίας , οι υπολογιστικοί πόροι (CPU, memory) μπορεί να διαφέρουν από κόμβο σε κόμβο.
- Ταχύτητα κίνησης (αν οι κόμβοι είναι κινητοί).

4. Τα χαρακτηριστικά του φορτίου των δεδομένων μπορεί να διαφέρουν σε διαφορετικά ad hoc δίκτυα: bit rate, χρονικοί περιορισμοί, απαιτήσεις αξιοπιστίας, εκπομπή προς έναν ή πολλούς σταθμούς (unicast/multicast), διευθυνσιοδότηση

5. Τα πρότυπα κινητικότητας μπορεί να διαφέρουν: sensor networks, δίκτυα προσωπικής περιοχής (personal area networks)

6. Χαρακτηριστικά κινητικότητας: ταχύτητα, ομοιομορφία (η ελλειψή της) των χαρακτηριστικών κινητικότητας μεταξύ διαφορετικών κόμβων.

3.3 Δρομολόγηση στα ad hoc δίκτυα

Η δρομολόγηση (routing) σε ένα οποιοδήποτε δίκτυο συνίσταται στην εύρεση μονοπατιού από ένα κόμβο πηγής (αποστολέα) σε έναν κόμβο προορισμού (παραλήπτη), κατά μήκος του οποίου θα μεταδοθεί η πληροφορία. Καθώς όμως, στα ad hoc δίκτυα η τοπολογία του δικτύου μπορεί να αλλάζει συνεχώς, με κόμβους να εισέρχονται και να εξέρχονται από αυτό αυθαίρετα και χωρίς προειδοποίηση, η δρομολόγηση σε αυτά χρήζει ιδιαίτερης έρευνας.

Πέρα από τη φύση του δικτύου, οι αλγόριθμοι δρομολόγησης πρέπει να λάβουν υπ' όψη τους τις περιορισμένες δυνατότητες των τερματικών συσκευών. Εξαιτίας της περιορισμένης εμβέλειας επικοινωνίας κάθε κόμβου, η αποστολή ενός μηνύματος από την πηγή στον προορισμό συνήθως απαιτεί την συνεργασία πολλών ενδιάμεσων κόμβων, οδηγώντας σε μονοπάτια με πολλά βήματα. Επιπλέον περιορισμοί, όπως η διάρκεια ζωής της μπαταρίας, καθώς επίσης και συνολικό εύρος ζώνης του δικτύου, υποδεικνύουν ότι η δρομολόγηση πρέπει να γίνεται με ένα ενεργειακά αποδοτικό τρόπο.

Ο πιο απλός αλγόριθμος δρομολόγησης μηνυμάτων, ανεξαρτήτως τύπου δικτύου, είναι η **πλημμύρα**, στον οποίο κάθε εισερχόμενο πακέτο στέλνεται σε κάθε γείτονα με εξαίρεση αυτόν από τον οποίο έφτασε. Μάλιστα, μπορούμε να πούμε ότι τα ασύρματα δίκτυα από τη φύση τους υλοποιούν πλημμύρα, αφού όλα τα μηνύματα που μεταδίδονται από ένα σταθμό μπορούν να ληφθούν από όλους τους άλλους σταθμούς που βρίσκονται εντός της εμβέλειας του. Όπως γίνεται αντιληπτό, ο αλγόριθμος της πλημμύρας δεν είναι καθόλου αποδοτικός, καθώς παράγει πολλά αντίγραφα και αυξάνει τον ανταγωνισμό και τις συγκρούσεις στο κανάλι. Στα ad hoc δίκτυα συγκεκριμένα, η χρήση απλής πλημμύρας οδηγεί στο λεγόμενο “πρόβλημα καταιγίδας ευρυεκπομπών” (broadcast storm problem).

Προχωρώντας την μελέτη μας σε αλγόριθμους που σχεδιάστηκαν ειδικά για ad hoc δίκτυα μπορούμε να διακρίνουμε δύο διαφορετικές προσεγγίσεις δρομολόγησης, την **βασισμένη στην τοπολογία** (topology-based) δρομολόγηση και την **βασισμένη στις θέσεις** (position-based) ή αλλιώς **γεωγραφική** (geographic) δρομολόγηση.

Τα πρωτόκολλα της βασισμένης στην τοπολογία δρομολόγησης αξιοποιούν πληροφορία σχετικά με τους συνδέσμους που υπάρχουν στο δίκτυο για να εκτελέσουν την προώθηση των πακέτων. Ανάλογα με τους αλγόριθμους που χρησιμοποιούν μπορούν να χωριστούν περαιτέρω σε **προδραστικά**(*proactive*), **αντιδραστικά**(*reactive*) και **υβριδικά** πρωτόκολλα.

Οι αλγόριθμοι γεωγραφικής δρομολόγησης εξαλείφουν κάποια από τα προβλήματα των βασισμένων στην τοπολογία αλγορίθμων, χρησιμοποιώντας κάποιες επιπλέον πληροφορίες. Συγκεκριμένα, όπως δηλώνεται κι από το όνομα τους, απαιτούν να γνωρίζουν την γεωγραφική (φυσική) θέση των κόμβων. Συνήθως, κάθε κόμβος ενημερώνεται για τη θέση του μέσω κάποιας υπηρεσίας εντοπισμού θέσης, όπως το GPS. Ο αποστολέας ενός πακέτου προσδιορίζει τη θέση του παραλήπτη με τη

βοήθεια μιας υπηρεσίας τοποθεσίας (location service) και την περιλαμβάνει στην διεύθυνση προορισμού του πακέτου.

3.3.1 Proactive Αλγόριθμοι

Τα Proactive πρωτόκολλα συνεχώς μαθαίνουν την τοπολογία του δικτύου μέσω ανταλλαγής μηνυμάτων ελέγχου (control messages). Έτσι, όταν κάποιο μονοπάτι για ένα προορισμό χρειαστεί, η πληροφορία είναι άμεσα διαθέσιμη. Κάθε κόμβος έχει έναν πλήρη πίνακα προώθησης. Έτσι, εξετάζοντας τον προορισμό κάθε πακέτου που φτάνει σ' αυτόν, κάθε κόμβος μπορεί να προωθήσει το πακέτο στο επόμενο βήμα (next-hop) πάνω στη διαδρομή του πακέτου. Συνήθως, η επιλογή του επόμενου βήματος δεν είναι τυχαία αλλά βασίζεται σε κάποια πολιτική, για παράδειγμα στην επιλογή του μονοπατιού με το ελάχιστο κόστος ή το συντομότερο μονοπάτι. Το μειονέκτημα των πρωτοκόλλων αυτών είναι ότι η κίνηση που δημιουργείται από την ανταλλαγή των μηνυμάτων ελέγχου είναι σημαντική και επιβαρύνει το δίκτυο. Μια σημαντική απόφαση είναι το πόσο συχνά θα εκπέμπονται τα μηνύματα ελέγχου με τις αντίστοιχες συνέπειες για κάθε απόφαση. Αν επιλεγεί να στέλνονται τακτικά μηνύματα ελέγχου, το μεγαλύτερο μέρος του διαθέσιμου εύρους ζώνης θα σπαταληθεί στα μηνύματα ελέγχου και όχι στη μεταφορά δεδομένων. Από την άλλη μεριά, αν επιλεγεί να στέλνονται λιγότερο τακτικά τα μηνύματα ελέγχου, τότε πιθανές αλλαγές στην τοπολογία του δικτύου δε θα γίνονται άμεσα αντιληπτές με αποτέλεσμα την λάθος δρομολόγηση των πακέτων μέσα στο δίκτυο. Το τελευταίο φαινόμενο είναι πολύ βασικό για δυναμικώς μεταβαλλόμενα δίκτυα, η τοπολογία των οποίων αλλάζει συνεχώς. Τα πρώτα πρωτόκολλα που προτάθηκαν για δρομολόγηση σε ad-hoc δίκτυα, ήταν proactive πρωτόκολλα διανύσματος απόστασης (proactive Distance Vector protocols) που ήταν βασισμένα στον κατανεμημένο αλγόριθμο Bellman-Ford (Distributed Bellman-Ford, DBF). Για την αντιμετώπιση των προβλημάτων του παραπάνω αλγόριθμου – σύγκλιση και υπερβολική κίνηση από τα μηνύματα ελέγχου – εξετάστηκαν τροποποιήσεις του αλγορίθμου. Μια άλλη προσέγγιση για την αντιμετώπιση του προβλήματος της σύγκλισης ήταν η εφαρμογή των πρωτοκόλλων κατάστασης ζεύξης (Link State protocols) στο ad hoc περιβάλλον. Έτσι, προέκυψε το πρωτόκολλο OLSR (Optimized Link State Routing protocol). Μια τρίτη προσέγγιση βασίστηκε στους αλγόριθμους Εύρεσης Μονοπατιού

(proactive Path Finding algorithms). Η προσέγγιση αυτή, συνδυάζει τα χαρακτηριστικά των πρωτόκολλων διανύσματος απόστασης και κατάστασης ζεύξης. Κάθε κόμβος στο δίκτυο κατασκευάζει ένα MST (Minimum Spanning Tree), χρησιμοποιώντας την πληροφορία των MST των γειτονικών κόμβων μαζί με το κόστος ζεύξης για κάθε γειτονικό κόμβο. Ο αλγόριθμος Εύρεσης Μονοπατιού επιτρέπει τη μείωση της κίνησης ελέγχου καθώς και τη μείωση της πιθανότητας δημιουργίας προσωρινών βρόχων δρομολόγησης στο δίκτυο. Πρωτόκολλο αυτής της κατηγορίας είναι το Ασύρματο Πρωτοκόλλο Δρομολόγησης (Wireless Routing Protocol, WRP).

Το σημαντικότερο ζήτημα των proactive πρωτόκολλων στα ad hoc δίκτυα προκύπτει από το γεγονός ότι καθώς το δίκτυο συνεχώς μεταβάλλεται, το κόστος της ενημέρωσης για τις τοπολογικές μεταβολές γίνεται απαγορευτικά υψηλό. Ακόμη, αν η κίνηση δικτύου δεν είναι ιδιαίτερα σημαντική, η γνώση της τοπολογίας του δικτύου δε θα χρησιμοποιείται σε μεγάλο βαθμό με αποτέλεσμα οι επενδύσεις στην περιορισμένη εκπομπή και υπολογιστική ισχύ των κόμβων να χαθούν.

3.3.2 Reactive αλγόριθμοι

Μια διαφορετική προσέγγιση στα πρωτόκολλα δρομολόγησης είναι τα reactive πρωτόκολλα, τα οποία βασίζονται σε διάλογο της μορφής ερώτηση-απάντηση. Τα reactive πρωτόκολλα δεν επιχειρούν να γνωρίζουν συνεχώς την τοπολογία του δικτύου. Όταν δημιουργηθεί η ανάγκη, εκκινούν μια διαδικασία για την εύρεση του μονοπατιού για κάποιον προορισμό. Η διαδικασία αυτή εμπεριέχει την “πλημμύρα” του δικτύου με την αίτηση αναζήτησης του μονοπατιού. Για το λόγο αυτό, τα πρωτόκολλα αυτά ονομάζονται και “κατά απαίτηση” (on demand). Παραδείγματα reactive πρωτόκολλων είναι τα **Temporally Ordered Routing Algorithm (TORA)**, **Dynamic Source Routing (DSR)** και **Ad hoc On Demand Distance Vector (AODV)**.

Στο επόμενο κεφάλαιο δίνεται περισσότερη εμφαση και ανάλυση στα πρωτόκολλα αυτά.

3.4 Το πρωτόκολλο IEEE 802.11 στα ad hoc δίκτυα

Η τεχνολογία του ευρέως πλέον διαδεδομένου προτύπου IEEE 802.11 ,είναι μια πολύ καλή πλατφόρμα για την υλοποίηση single-hop ad hoc δικτύων,λόγω της απλότητάς της.Με τον όρο single-hop δίκτυα αναφερόμαστε σε αυτά στα οποία οι κόμβοι πρέπει να είναι στην ίδια ακτινα εκπομπής(50-200 μέτρα) ,ωστε να επικοινωνήσουν.Ο περιορισμός αυτός μπορεί να αρθεί με multi-hop δικτύωση,κάνοντας χρήση αλγορίθμων δρομολόγησης,η οποία επιτρέπει σε κάθε κόμβο να προωθεί κατα περίπτωση τα πακέτα σε γειτονικούς κομβους μέχρι να φτάσουν στο προορισμό τους.

Σε ένα καθαρά ad hoc δίκτυο, οι ίδιες οι συσκευές- κόμβοι αποτελούν το δίκτυο και επομένως απαιτείται να εκτελούν και τις λειτουργίες που κατά κανόνα ανατίθενται στις συσκευές της υποδομής (switches, routers, servers) σε ένα ενσύρματο δίκτυο. Αυτή η προσέγγιση οδηγεί στην προϋπόθεση, της ύπαρξης μιας αρκούσας μεγάλης χωρικής πυκνότητας κόμβων στο δίκτυο, ώστε να εξασφαλίσει την επιτυχή δρομολόγηση των πακέτων από την πηγή στον προορισμό. Παρόλο που η ανάπτυξη τέτοιων πυκνών multihop δικτύων δεν έχει εξαπλωθεί σε μεγάλο επίπεδο, η ενσωμάτωση ασύρματης τεχνολογίας 802.11 σε φορητές συσκευές , σημαίνει την δυνατότητα ανάπτυξης multihop ad hoc δικτύων σε μικρή και μεσαία κλίμακα.

4. ΑΛΓΟΡΙΘΜΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ

Στο κεφάλαιο αυτό θα παρουσιάσουμε επιλεκτικά κάποιους αλγόριθμους δρομολόγησης. Τους DSDV, AODV και DSR. Ο πρώτος ανήκει στη κατηγορία των proactive αλγορίθμων ενώ οι άλλοι στους reactive.

4.1 Destination-Sequenced Distance-Vector (DSDV)

Το πρωτόκολλο DSDV βασίζεται στον αλγόριθμο Bellman-Ford. Παράλληλα, προτείνει σημαντικές βελτιώσεις : εκμηδενίζει τους βρόγχους δρομολόγησης (root looping), αυξάνει την ταχύτητα σύγκλισης και μειώνει τον επιπλέον φόρτο του δικτύου που οφείλεται στα μηνύματα ελέγχου.

Στο πρωτόκολλο DSDV κάθε κόμβος διατηρεί ένα πίνακα επόμενου άλματος (next hop table) τον οποίο και ανταλλάζει με τους γειτονικούς του κόμβους. Υπάρχουν δύο τύποι ανταλλαγών : η περιοδική εκπομπή ολόκληρου του πίνακα (full-table exchange) και η ανταλλαγή που οφείλεται σε κάποιο γεγονός (event-driven incremental updating). Η σχετική συχνότητα των δύο διαφορετικών τρόπων ανταλλαγής εξαρτάται από την κινητικότητα του κόμβου.

Κατά τη διάρκεια ανταλλαγής του πίνακα επόμενου άλματος (ανεξάρτητα της αιτίας που προκάλεσε την ανταλλαγή), ο κόμβος πηγή επισυνάπτει ένα αριθμό ακολουθίας (sequence number) στα δεδομένα αποστολής. Έτσι, κάθε κόμβος που λαμβάνει το νέο διάνυσμα-απόστασης, τροποποιεί τον πίνακα επόμενου άλματος που ήδη έχει ενώ παράλληλα αποθηκεύει τον αντίστοιχο αριθμό ακολουθίας. Έτσι, όταν ένας κόμβος στείλει εκ νέου διάνυσμα-απόστασης στους γειτονικούς του κόμβους, οι κόμβοι που το λαμβάνουν τροποποιούν τους πίνακές τους μόνο εάν ο νέος αριθμός ακολουθίας είναι μεγαλύτερος από αυτόν που έχουν αποθηκεύσει ή εάν ο αριθμός ακολουθίας είναι ίδιος αλλά τα νέα μονοπάτια είναι μικρότερα από τα αποθηκευμένα.

Για μεγαλύτερη μείωση του επιπλέον φόρου λόγω πακέτων ελέγχου, για κάθε νέο μονοπάτι ορίζεται ένας χρόνος ανωφλίου (setting time). Ένας κόμβος ενημερώνει τους γειτονικούς του κόμβους για το νέο μονοπάτι μόνο όταν περάσει ο χρόνος ανωφλίου και το μονοπάτι είναι ακόμη ενεργό.

Το πλεονέκτημα του παραπάνω αλγόριθμου είναι ότι τα μονοπάτια προς τους υπόλοιπους κόμβους του δικτύου είναι γνωστά σε κάθε κόμβο. Έτσι, όταν ένας κόμβος θέλει να ανταλλάξει δεδομένα με κάποιον άλλο κόμβο μέσα στο δίκτυο, ξεκινά αμέσως μιας και γνωρίζει το μονοπάτι ανάμεσα στους δύο κόμβους. Το μειονέκτημα είναι ο σημαντικός επιπλέον φόρτος του δικτύου (overhead) λόγω των πολλών και συχνών ανταλλαγών μηνυμάτων ελέγχου.

4.2 Ad hoc on Demand Distance Vector (AODV)

Ο AODV αποτελεί μια βελτίωση στον DSDV. Η ιδέα είναι να απαλλαχτούμε από την δαπανηρή διαδικασία της συντήρησης των πινάκων δρομολόγησης και οι διαδρομές να ανακαλύπτονται όταν ζητούνται. Για το σκοπό αυτό χρησιμοποιείται η τεχνική της πλημμύρας.

Αρχικά ο κάθε κόμβος θα πρέπει να γνωρίζει τους άμεσους γείτονές του. Έτσι περιοδικά αποστέλλονται μηνύματα χαιρετισμού (hello messages), ώστε να διατηρούνται ενημερωμένοι οι πίνακες γειτνίασης των κόμβων. Για να δημιουργηθεί μια διαδρομή προς τον προορισμό, η αφετηρία δημιουργεί πακέτα αίτησης διαδρομής (route request – RREQ). Κάθε κόμβος που παραλαμβάνει ένα RREQ πακέτο διατηρεί έναν πίσω-δείκτη προς τον κόμβο που του το απέστειλε και το προωθεί στους γείτονές του εφόσον δεν γνωρίζει τον προορισμό (πλημμύρα). Όταν τελικά το πακέτο φθάσει στον κόμβο προορισμό, αυτός θα δημιουργήσει ένα πακέτο απάντησης διαδρομής (route reply – RREP). Κατόπιν ακολουθώντας τους πίσω-δείκτες η απάντηση θα φθάσει στην αφετηρία και ταυτόχρονα οι ενδιάμεσοι κόμβοι θα δημιουργήσουν τους εμπρός-δείκτες (προς τον προορισμό) για την μετάδοση των data πακέτων. Προκειμένου να αποφευχθεί η επαναπροώθηση του ίδιου πακέτου από έναν ενδιάμεσο κόμβο, τα πακέτα προσδιορίζονται μονοσήμαντα μέσω της IP διεύθυνσης της αφετηρίας και ενός id για την συγκεκριμένη ανακάλυψη διαδρομής. Φυσικά για να λειτουργήσει όλο αυτό το σχήμα θα πρέπει οι σύνδεσμοι να είναι διπλής κατεύθυνσης.

Σημειώνεται ότι οι δείκτες που χρησιμοποιούνται παραμένουν ενεργοί μόνο όσο διαρκεί η μετάδοση των δεδομένων, μετά την παρέλευση ενός χρονικού διαστήματος από το τέλος της μετάδοσης διαγράφονται. Επίσης αν σε κάποιον κόμβο δεν υπάρχει

η κατάλληλη καταχώριση στον πίνακα δρομολόγησής του, το RREQ πακέτο απορρίπτεται και αποστέλλεται στην αφετηρία ένα μήνυμα λάθους RRER.

4.3 Dynamic Source Routing (DSR)

Ο DSR βελτιώνει ακόμη περισσότερο την ιδέα που χρησιμοποιείται στον AODV. Η διαφοροποίηση έγκειται στον τρόπο που χρησιμοποιούνται οι πίνακες δρομολόγησης (εμπρός/πίσω δείκτες). Έτσι αντί αυτές οι πληροφορίες να διαγράφονται μετά από κάθε επικοινωνία, διατηρούνται αποθηκευμένες στους ενδιάμεσους κόμβους σε μια προσωρινή μνήμη διαδρομών (route cache), για ένα συγκεκριμένο χρονικό διάστημα. Με αυτόν τον τρόπο ο κάθε κόμβος έχει έναν πίνακα δρομολόγησης προς διάφορους προορισμούς τοπικά στην δική του cache, για όσο διάστημα είναι ενεργή η κάθε εγγραφή.

Το πλεονέκτημα της cache είναι ότι μπορεί έτσι να συντομεύσει τη διαδικασία αναζήτησης. Στον AODV ένα RREQ πακέτο πρέπει να φθάσει έως και τον τελικό προορισμό για να αποσταλεί το RREP στην αφετηρία. Τώρα όμως αν ένας ενδιάμεσος κόμβος διαθέτει μια εγγραφή στην cache προς τον συγκεκριμένο προορισμό, τότε δεν χρειάζεται να συνεχιστεί η αναζήτηση εφόσον γνωρίζουμε ήδη το τμήμα της διαδρομής από τον κόμβο αυτόν έως τον προορισμό. Έτσι επιστρέφεται άμεσα ένα RREP στην αφετηρία με τη διαδρομή προς τον προορισμό. Αντιλαμβανόμαστε πως με αυτό το σχήμα, μπορεί ακόμα και η ίδια η αφετηρία να γνωρίζει ένα δρομολόγιο προς τον προορισμό, για αυτό και η τεχνική ονομάζεται δρομολόγηση πηγής (source routing).

Προκειμένου να εκμεταλλευτούμε την cache των ενδιαμέσων κόμβων, κάθε RREQ πακέτο διατηρεί μια λίστα με τα ενδιάμεσα βήματα μέχρι τον τελικό προορισμό. Οι κόμβοι που γνωρίζουν πώς να δρομολογήσουν το πακέτο στον προορισμό του απλά αντιγράφουν το τμήμα της διαδρομής που γνωρίζουν στο τέλος της λίστας. Επίσης κάθε πακέτο προσδιορίζεται μοναδικά, έτσι ώστε αν ένας κόμβος το είχε παραλάβει και νωρίτερα να το απορρίπτει.

Σχετικά με την διαδικασία της επιστροφής στην αφετηρία RREP, ο DSR υποστηρίζει τόσο τα συμμετρικά όσο και τα ασύμμετρα δίκτυα. Στην περίπτωση που οι σύνδεσμοι είναι μονής κατεύθυνσης ο προορισμός αρχικοποιεί μια αντίστοιχη διαδικασία αναζήτησης της αφετηρίας, διαφορετικά χρησιμοποιείται το μονοπάτι που ανακαλύφθηκε προς την αντίθετη κατεύθυνση.

Μια ακόμη λειτουργία του DSR είναι η συντήρηση των δρομολογίων cache (route maintenance). Συγκεκριμένα όταν το data link επίπεδο του δικτύου εντοπίσει ένα σφάλμα μετάδοσης, τότε επιστρέφεται στην αφετηρία ένα μήνυμα λάθους RRER με πληροφορία για το συγκεκριμένο hop που απέτυχε. Έτσι η αφετηρία μπορεί να εντοπίσει στην cache της τον κόμβο που δεν αποκρίνεται και να διαγράψει τα τμήματα των διαδρομών από εκεί και κάτω.

Τέλος μια ακόμα έξυπνη τεχνική του DSR είναι τα passive acknowledgements. Η ιδέα στηρίζεται στην εκμετάλλευση της broadcast φύσης του ασύρματου δικτύου. Έστω ότι έχουμε μια ακολουθία από ενδιάμεσους κόμβους ...->s1->s2->s3->... και έστω ότι είμαστε στην φάση που ο s1 προωθεί ένα RREQ πακέτο στον s2. Ο s1 γνωρίζει ότι ο s2 δεν είναι ο τελικός προορισμός, επομένως αναμένει ότι και εκείνος με τη σειρά του θα το προωθήσει σε έναν επόμενο κόμβο (τον s3). Έτσι όταν ο s2 προωθήσει το πακέτο στον s3, το μήνυμα θα το «ακούσει» και ο s1. Έτσι ο s1 μπορεί να λάβει μια επιβεβαίωση για την προώθηση του πακέτου.

4.4 Temporally Ordered Routing Algorithm (TORA)

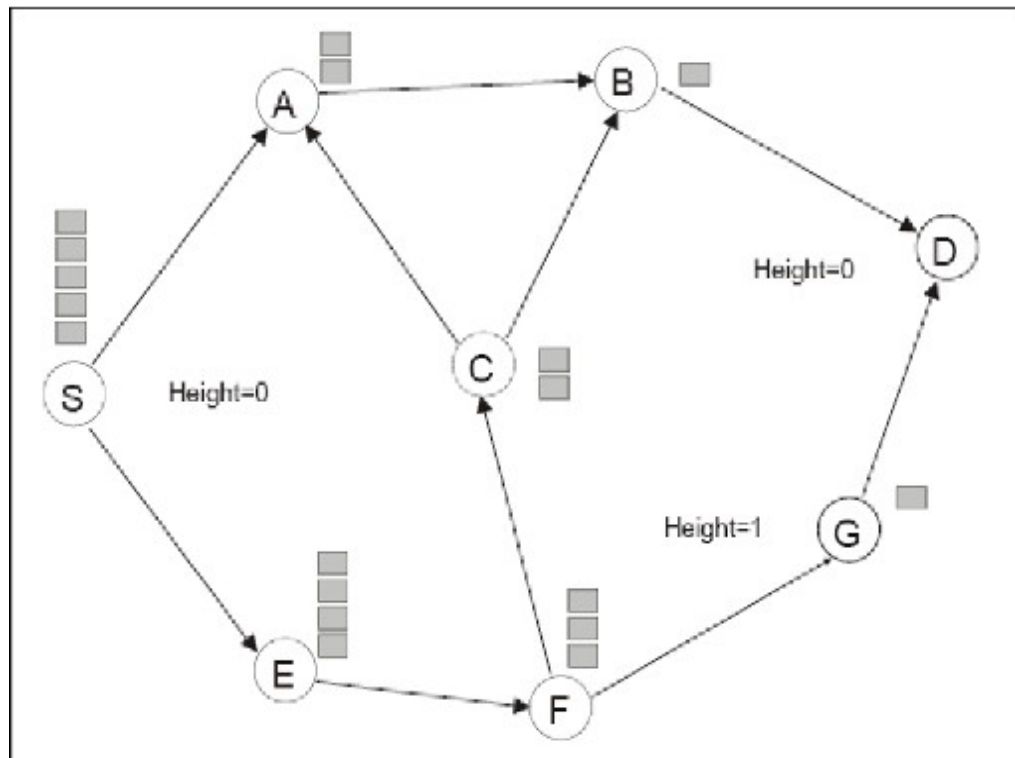
Το πρωτόκολλο TORA ανήκει στην οικογένεια των αλγόριθμων *αντιστροφής-ζεύξης* (link reversal algorithms). Οι αλγόριθμοι αυτοί είναι σχεδιασμένοι για να παρέχουν γρήγορη αντίδραση σε τοπολογικές μεταβολές και για να ελαχιστοποιούν τον επιπλέον φόρτο (overhead) δρομολόγησης, περιορίζοντας την αντίδραση σε μια μικρή ομάδα κόμβων.

Οι αλγόριθμοι αντιστροφής-ζεύξης θεωρούν το δίκτυο σαν ένα συνδεδεμένο γράφο (connected graph) και μετατρέπουν το πρόβλημα δρομολόγησης στη δημιουργία ενός προσανατολισμένου-στον-προορισμό Κατευθυνόμενου Ακυκλικού Γράφου (destination oriented Directed Acyclic Graph, DAG) . Όταν ο γράφος αυτός δημιουργηθεί, θα υπάρχει ένα ακυκλικό μονοπάτι μεταξύ οποιουδήποτε κόμβου και του προορισμού. Η βασική ιδέα για την κατασκευή του γράφου είναι η εξής: ένα ύψος (height) σχετίζεται με κάθε κόμβο και οι ζεύξεις είναι προσανατολισμένες ανάλογα με τα σχετικά ύψη των γειτονικών κόμβων κάθε ζεύξης (από τον κόμβο με το μεγαλύτερο ύψος προς τον κόμβο με το μικρότερο).

Στην παρακάτω εικόνα δίνεται ένα παράδειγμα ενός τέτοιου γράφου. Κάθε κόμβος έχει ένα ύψος (πρόκειται για τον αριθμό των γκρι κουτιών δίπλα σε κάθε

κόμβο), ο κόμβος-προορισμός D έχει το μικρότερο ύψος (0) και οι ζεύξεις έχουν κατεύθυνση από τον κόμβο με το υψηλότερο ύψος προς τον κόμβο με το μικρότερο.

Το πρωτόκολλο TORA είναι ένα reactive πρωτόκολλο που βρίσκει εφαρμογή σε μεγάλα, δυναμικά, με περιορισμένο εύρος ζώνης δίκτυα. Το κύριο χαρακτηριστικό του πρωτόκολλου είναι η γρήγορη αντίδραση σε αποτυχίες ζεύξεων (link failures).



Παράδειγμα προσανατολισμένου-στον-προορισμό Κατευθυνόμενου Ακυκλικού Γράφου. Ο κόμβος-προορισμός είναι ο D.

Η λειτουργία του πρωτόκολλου βασίζεται σε τρεις λειτουργίες: *δημιουργία*, *συντήρηση* και *σβήσιμο* διαδρομών. Κάθε δεδομένη χρονική στιγμή, μια πεντάδα αριθμών σχετίζεται με κάθε κόμβο i του δικτύου: $H_i = (\tau_i, oid_i, r_i, \delta_i, i)$. Οι πρώτοι τρεις αριθμοί καλούνται επίπεδο αναφοράς και χρησιμοποιούνται για τη διατήρηση διαδρομών. Οι δύο τελευταίοι καλούνται επίπεδο δέλτα (delta level) και χρησιμοποιούνται για τη δημιουργία διαδρομών. Για παράδειγμα το σχετιζόμενο με τον κόμβο S διάνυσμα μπορούσε να είναι $H_S = (0,0,0,3,S)$ ενώ το αντίστοιχο διάνυσμα του κόμβου E να ήταν $H_E = (0,0,0,3,E)$. Το μέτρο του διανύσματος H_S είναι μεγαλύτερο από το μέτρο του H_E άρα ο κόμβος S είναι υψηλότερος από τον E. Ο κόμβος S αναφέρεται σαν αντίθετος-προς-την-κυκλοφορία γείτονας (upstream neighbor) του κόμβου E ενώ ο E αναφέρεται σαν προς-την-κυκλοφορία-γείτονας

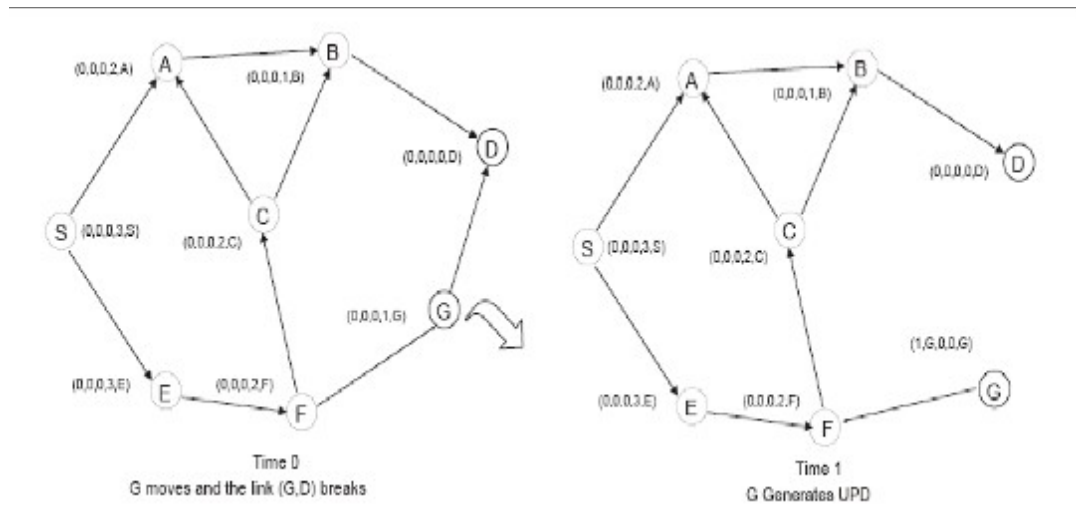
(downstream neighbor) του κόμβου S. Ακολουθεί σύντομη περιγραφή των λειτουργιών του πρωτόκολλου TORA.

Δημιουργία διαδρομών : Η λειτουργία αυτή χρησιμοποιεί δύο τύπους πακέτων, ΕΡΩΤΗΜΑ (συμβολικά QRY) και ΕΝΗΜΕΡΩΣΗ (συμβολικά UPD). Ένα πακέτο QRY περιέχει μόνο τη διεύθυνση του κόμβου προς τον οποίο ζητείται διαδρομή. Ένα πακέτο UPD περιέχει τη διεύθυνση και το ύψος του κόμβου-πηγή.

Η διαδικασία εύρεσης διαδρομής ξεκινά όταν ένας κόμβος δεν έχει προς-την-κυκλοφορία γείτονες (downstream neighbor) για κάποιον προορισμό. Τότε, ένα πακέτο QRY εκπέμπεται στο δίκτυο. Κάθε κόμβος που λαμβάνει ένα πακέτο QRY και έχει μια διαδρομή προς τον προορισμό, απαντά με εκπομπή (broadcast) ενός UDP πακέτου. Καθώς ταξιδεύει μέσα στο δίκτυο, το πακέτο UDP καθορίζει το ύψος (για παράδειγμα ένα νέο επίπεδο δέλτα καθορίζεται) των κόμβων έτσι ώστε να δημιουργείται ένας προσανατολισμένος-στον-προορισμό Κατευθυνόμενος Ακυκλικός Γράφος.

Διατήρηση διαδρομών : ξεκινά όταν ένας κόμβος χάνει τον τελευταίο προς-την-κυκλοφορία γείτονα (downstream neighbor) για ένα δεδομένο προορισμό. Ας υποθέσουμε ότι ο κόμβος X χάνει τον τελευταίο προς-την-κυκλοφορία γείτονα (downstream neighbor) προς τον προορισμό D. Ο κόμβος X αυξάνει το ύψος του (για παράδειγμα καθορίζει ένα νέο επίπεδο αναφοράς) έτσι ώστε ένας αντίθετος-προς-την-κυκλοφορία γείτονας (upstream neighbor) του X προς τον κόμβο D να γίνει ένας προς-την-κυκλοφορία γείτονας (downstream neighbor). Στη συνέχεια, κάνει εκπομπή (broadcast) ενός UPD πακέτου με το νέο του ύψος. Κάθε κόμβος που λαμβάνει ένα UPD πακέτο, ανανεώνει τη λίστα με τους γειτονικούς κόμβους του. Εάν χάσει τον τελευταίο προς-την-κυκλοφορία γείτονα, λειτουργεί όπως ο κόμβος-γεννήτρια του UPD πακέτου, αυξάνοντας το ύψος του και εκπέμποντας ένα νέο UPD πακέτο.

Στο τέλος αυτής της διαδικασίας, ή ένας νέος προσανατολισμένος-στον-προορισμό Κατευθυνόμενος Ακυκλικός Γράφος θα έχει δημιουργηθεί είτε ένας διαμερισμός (partition). Στην περίπτωση του διαμερισμού, μια διαδικασία σβησίματος διαδρομών θα ξεκινήσει. Το πλεονέκτημα αυτής της μεθόδου διατήρησης των διαδρομών είναι ότι δε χρειάζεται να διαδοθεί σε όλο το δίκτυο το UPD πακέτο για να διορθωθεί μια διαδρομή.



Διατήρηση διαδρομών στο πρωτόκολλο TORA

Ένα παράδειγμα της παραπάνω διαδικασίας φαίνεται στο παραπάνω σχήμα. Η ζεύξη ανάμεσα στους κόμβους G και D χάνεται (πιθανώς λόγω μετακίνησης του κόμβου G). Έτσι, ο G χάνει τον τελευταίο προς-την-κυκλοφορία γείτονα για τον προορισμό D. Η λύση στο πρόβλημα δίνεται εάν αντιστραφεί η ζεύξη μεταξύ των κόμβων G και F. Ο G αυξάνει το ύψος του και εκπέμπει ένα UPD πακέτο. Ο κόμβος F λαμβάνει το πακέτο αλλά δεν το επανεκπέμπει γιατί διατηρεί ακόμη ένα προς-την-κυκλοφορία γείτονα για τον προορισμό D, τον κόμβο C.

Σβήσιμο διαδρομών : όταν εντοπίζεται ένας διαμερισμός (partition), ένα πακέτο διαγραφής εκπέμπεται μέσα στο διαμερισμό και όλες οι διαδρομές προς τον απρόσιτο κόμβο διαγράφονται.

4.5 Σύγκριση αλγορίθμων

Αρχικά βλέπουμε μια θεμελιώδη διαφορά στην συμπεριφορά των proactive από τα reactive πρωτόκολλα. Proactive αλγόριθμοι όπως ο DSDV επιτυγχάνουν μικρότερη επιβάρυνση στο δίκτυο κατά τη φάση της αναζήτησης εφόσον η πληροφορία για τη δρομολόγηση υπάρχει ήδη αποθηκευμένη στους κόμβους, ωστόσο επιβαρύνουν το δίκτυο με τα update μηνύματα που απαιτούνται για την δημιουργία / συντήρηση των πινάκων τους. Αυτό έχει επίσης ως αποτέλεσμα την αυξημένη κατανάλωση ενέργειας. Από την άλλη πλευρά τα reactive πρωτόκολλα δημιουργούν μεγαλύτερη επιβάρυνση κατά την αναζήτηση, αλλά αποφεύγουν την άσκοπη επιβάρυνση στο

δίκτυο και την κατανάλωση ενέργειας καθώς αποφεύγουν οποιαδήποτε προετοιμασία.

Στη συνέχεια συγκρίνοντας τον AODV και DSR, παρατηρούμε ότι ο AODV είναι πιο απλός και τα μηνύματά του μικρότερα σε μέγεθος, εφόσον περιέχουν μόνο το id του προορισμού και όχι όλων των ενδιάμεσων κόμβων. Ο DSR είναι πιο έξυπνος, χειρίζεται την πληροφορία που έχει ανακαλυφθεί με πιο αποδοτικό τρόπο, αλλά παρουσιάζει μεγαλύτερες απαιτήσεις σε μνήμη στους κόμβους. Σε γενικές γραμμές ο DSR είναι αρκετά ευέλικτος για να διαχειρίζεται μεγαλύτερα μεγέθη δικτύων και περιορίζει την άσκοπη κατανάλωση bandwidth και ενέργειας. Επίσης μπορεί να λειτουργήσει τόσο σε δίκτυα με συνδέσμους μιας κατεύθυνσης όσο και σε δίκτυα με αμφίδρομους συνδέσμους.

Επομένως καταλήγουμε στο συμπέρασμα πως δεν μπορούμε να βρούμε έναν απόλυτο αλγόριθμο που να ικανοποιεί όλες τις απαιτήσεις μας. Η τελική απόδοση του κάθε αλγορίθμου εξαρτάται από τα χαρακτηριστικά του κάθε ad hoc δικτύου, από το φορτίο του και από την κινητικότητα των κόμβων.

5. ΚΙΝΗΤΑ AD HOC ΔΙΚΤΥΑ - MOBILE AD HOC NETWORKS (MANET)

Ένα MANET (Mobile Ad hoc Network - Κινητό ad hoc δίκτυο) είναι ένα αυτορυθμιζόμενο και χωρίς υποδομή δίκτυο κινητών συσκευών που συνδέονται μέσω ασύρματων ζεύξεων. Δηλαδή είναι ένα ad hoc δίκτυο όπου οι κόμβοι του είναι ελεύθεροι να κινηθούν οπουδήποτε στο χώρο με τυχαίο τρόπο.

Αρα είναι προφανές ότι κληρονομούν τα κοινά χαρακτηριστικά που βρίσκονται σε όλα τα ασύρματα δίκτυα αλλά επιπλέον προσθέτουν και κάποια άλλα λόγω της ad hoc δικτύωσης. Μερικά από τα πλεονεκτήματά τους αναφέρονται παρακάτω.

Τα MANET κληρονομούν τα κοινά χαρακτηριστικά που βρίσκονται σε όλα τα ασύρματα δίκτυα, ενώ παράλληλα προσθέτουν κάποια τα οποία συναντούνται μόνο στην ad hoc δικτύωση.

- Ασύρματη δικτύωση. Οι κόμβοι επικοινωνούν ασύρματα και μοιράζονται το ίδιο φυσικό μέσο.
- Βασίζονται σε απευθείας συνδέσεις (ad hoc-based). Ένα MANET είναι ένα προσωρινό δίκτυο το οποίο σχηματίζεται δυναμικά από ένα σύνολο κόμβων ανάλογα με τις εκάστοτε ανάγκες συνδεσιμότητας.
- Αυτόνομα και χωρίς σταθερή υποδομή (Infrastructureless). Τα MANET δεν εξαρτώνται από προϋπάρχουσα υποδομή ή κεντρική διαχείριση. Ο κάθε κόμβος του δικτύου λειτουργεί με έναν διανεμημένο τρόπο, δρα ως ξεχωριστός δρομολογητής (router) και παράγει ανεξάρτητα δεδομένα.

- Multihop routing. Δεν είναι απαραίτητη η χρήση ειδικών δρομολογητών. Κάθε κόμβος δρομολογεί αυτόνομα τα πακέτα στους γειτονικούς του κόμβους ώστε να επιτρέπει την μετάδοση δεδομένων μεταξύ τους.
- Κινητικότητα. Οι συμμετέχοντες σε ένα MANET κόμβοι κινούνται με τυχαίο τρόπο αλλάζοντας διαρκώς την τοπολογία του δικτύου και την μεταξύ τους συνδεσιμότητα.

Τα δίκτυα MANET εξαλείφουν τους περιορισμούς των δικτύων σταθερής υποδομής , και επιτρέπουν τις συσκευές να δημιουργούν και να συμμετέχουν σε ένα δίκτυο χωρίς εξωτερική παρέμβαση, οποιαδήποτε στιγμή, σε οποιοδήποτε περιβάλλον, παρέχοντας σχεδόν οποιαδήποτε διαθέσιμη υπηρεσία.

5.1 Τύποι MANETs

Τα MANETs μπορούν να χωριστούν σε τρεις τύπους:

1. VANETs (Vehicular Ad hoc Networks - Δίκτυα ad hoc οχημάτων): Χρησιμοποιούνται για την επικοινωνία μεταξύ οχημάτων αλλά και ανάμεσα στα οχήματα και τον εξοπλισμό καθ 'οδόν.
2. InVANETs (Intelligent Vehicular Ad hoc Networks - Ευφυή VANETs): Είναι ένα είδος τεχνητής νοημοσύνης που βοηθά τα οχήματα να συμπεριφέρονται με ευφυείς τρόπους κατά τη διάρκεια συγκρούσεων μεταξύ οχημάτων, ατυχημάτων, οδήγησης υπό την επήρεια αλκόολ κλπ.
3. iMANETs (Internet based Mobile Ad hoc Networks - Διαδικτυακά MANETs): Είναι ad hoc δίκτυα που συνδέουν κινητούς κόμβους με σταθερούς Internet-gateway κόμβους. Σε τέτοιους τύπους δικτύων δεν εφαρμόζονται απευθείας κανονικοί ad hoc αλγόριθμοι δρομολόγησης .

Παρακάτω αναλύονται εκτενέστερα τα δίκτυα ad hoc οχημάτων VANETs.

5.1.1 VANETs(Vehicular Ad hoc Networks)

Οι πρώτες έρευνες για επικοινωνία μεταξύ οχημάτων ξεκίνησαν στις αρχές της δεκαετίας του '80, όμως η τεχνολογία δεν ήταν αρκετά ώριμη για να υποστηρίξει τέτοιες προσπάθειες. Την τελευταία δεκαετία, με τη πρόοδο της ασύρματης τεχνολογίας, η περιοχή των επικοινωνιών μεταξύ οχημάτων απέκτησε μεγάλο ενδιαφέρον και δόθηκε ώθηση στην έρευνα, όχι μόνο από τα πανεπιστήμια αλλά και από τη βιομηχανία.

Το μεγαλύτερο κομμάτι της αυτής της έρευνας έχει επικεντρωθεί στα VANETs. Τα αδόμητα δίκτυα οχημάτων ή αλλιώς VANETs (Vehicular Ad-hoc NETworks) είναι μια νέα μορφή δικτύων που ενσωματώνει τις τεχνολογίες των αδόμητων δικτύων (ad-hoc networks), των ασύρματων τοπικών δικτύων (W-LAN) και των κυψελωτών συστημάτων (cellular systems), και συνδυάζοντάς τες με νέες τεχνικές και μεθόδους επιδιώκει να επιτύχει την έξυπνη επικοινωνία των οχημάτων και τη συνεχή σύνδεση των επιβατών τους με τον κόσμο (internet). Το κύριο πεδίο εφαρμογής των VANETs είναι τα ευφυή συστήματα μεταφορών (ITS - Intelligent Transportation Systems) που έχουν ως σκοπό να βελτιώσουν τις συνθήκες κυκλοφοριακής κίνησης και να αυξήσουν την οδική ασφάλεια.

Ως απόγονος των κινητών αδόμητων δικτύων (MANETs – Mobile Ad-hoc Networks), τα VANETs έχουν κληρονομήσει το κύριο χαρακτηριστικό των αδόμητων δικτύων, την ικανότητα σχηματισμού δικτύου αποκλειστικά από τους κόμβους τους χωρίς να απαιτείται κάποια σταθερή υποδομή. Οι κόμβοι, αναλαμβάνοντας και τη διαδικασία της δρομολόγησης (routing), δίνουν τη δυνατότητα στο δίκτυο να υποστηρίξει επικοινωνία μέσω πολλαπλών συνδέσεων-αλμάτων (hops) σε αντίθεση με τα ασύρματα τοπικά δίκτυα και τα συστήματα κινητής τηλεφωνίας, τα οποία αποτελούνται από ένα σταθερό access point ή base station, αντίστοιχα, και οι κόμβοι τους μπορούν να επικοινωνήσουν μόνο με αυτό.

Ωστόσο οι διαφορές στο περιβάλλον που κινούνται τα οχήματα καθώς και τα ειδικά χαρακτηριστικά της κίνησής τους έχουν ως αποτέλεσμα η συμπεριφορά τους να αποκλίνει πολύ από αυτή των MANETs και να απαιτεί την αντιμετώπισή τους ως ξεχωριστή κατηγορία δικτύων. Τα οχήματα κινούνται με πολύ μεγαλύτερη ταχύτητα απ' ό τι οι κόμβοι ενός MANET και η κίνησή τους δεν είναι τυχαία στο χώρο αλλά είναι σχεδόν γραμμική καθώς ακολουθούν τη χάραξη των δρόμων και των

διασταυρώσεων. Επίσης ο τρόπος διάδοσης των ηλεκτρομαγνητικών κυμάτων στα αστικά περιβάλλοντα διαφέρει πολύ από τη διάδοση στον ελεύθερο χώρο, διότι τα κτίρια παίζουν καθοριστικό ρόλο με το να μην επιτρέπουν στα κύματα να τα διαπεράσουν και με το να τα ανακλούν.

Παρακάτω περιγράφονται οι αρχιτεκτονικές που συναντούνται στα VANETs.

5.1.2 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΤΩΝ VANETs

Οι συνιστώσες των VANET συστημάτων μπορούν να χωριστούν σε τέσσερις κατηγορίες. Αυτές είναι τα οχήματα, οι προσωπικές συσκευές, ο εξοπλισμός δρόμου (RSU – Road-Side Units) και ο κεντρικός εξοπλισμός. Ένα σύστημα VANET δεν είναι απαραίτητο να αποτελείται από συστατικά όλων των παραπάνω κατηγοριών. Με βάση το ποιες κατηγορίες απαρτίζουν το σύστημα γίνεται και ο διαχωρισμός των αρχιτεκτονικών που εμφανίζονται.

Τα *οχήματα* είναι αναπόσπαστο κομμάτι των VANETs και αποτελούν τη βασική συνιστώσα όλων των αρχιτεκτονικών.

Οι *προσωπικές συσκευές* τοποθετούνται από το χρήστη πάνω στο όχημα και μπορεί να είναι είτε συσκευές πλοήγησης GPS είτε συσκευές πολυμεσικών εφαρμογών. Επίσης κινητά τηλέφωνα μπορεί να θεωρηθούν ότι ανήκουν σε αυτήν την κατηγορία αν χρησιμοποιούν το δίκτυο των οχημάτων, για τη σύνδεσή τους στο διαδίκτυο, και όχι κάποιο άλλο δίκτυο (πχ. κινητής τηλεφωνίας).

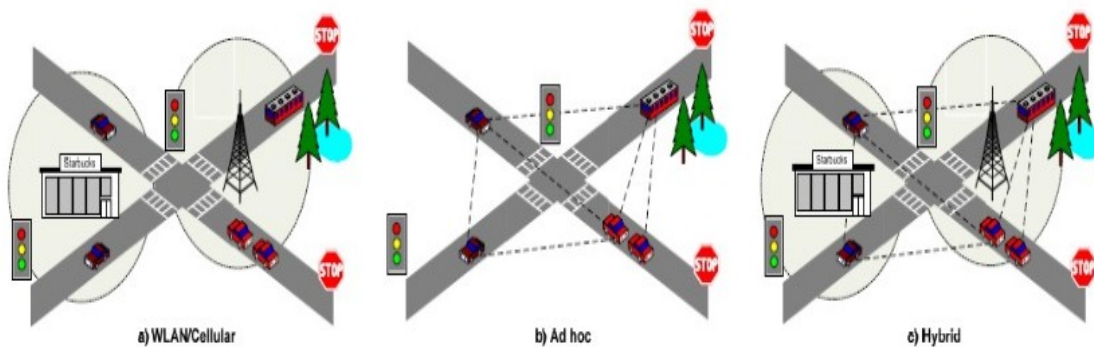
Ο *εξοπλισμός δρόμου* παρουσιάζει μεγάλη ποικιλία ως προς το είδος των συσκευών που μπορεί να αποτελείται. Παραδοσιακές συσκευές όπως φωτεινοί σηματοδότες ή πινακίδες σήμανσης δύναται να ενσωματώνουν τμήματα με υπολογιστική ισχύ και ικανότητα ασύρματης επικοινωνίας (πομπούς), έτσι ώστε να διανέμουν τη πληροφορία τους στο δίκτυο πέρα από την οπτική επαφή. Επίσης σταθεροί αναμεταδότες που λειτουργούν ως ακίνητοι κόμβοι του δικτύου και βοηθούν στην πιο γρήγορη και αποτελεσματική μετάδοση των μηνυμάτων. Τα RSU μπορούν να είναι είτε αποκομμένα είτε να συνδέονται μεταξύ τους με ένα ιδιωτικό δίκτυο (private network). Επίσης μπορούν να συνδέονται με τον κεντρικό εξοπλισμό ή και κατευθείαν στο Διαδίκτυο.

Ο κεντρικός εξοπλισμός λειτουργεί ως το κέντρο ελέγχου του δικτύου. Κύριες λειτουργίες του είναι να συλλέγει δεδομένα από τα RSU, να προβλέπει μελλοντικές συνθήκες του δικτύου (πχ. κυκλοφοριακή συμφόρηση), να δίνει εντολές στα RSU.

Οι τρεις αρχιτεκτονικές δικτύου που εμφανίζονται στα VANETs είναι οι εξής,

- Αμιγώς κυψελωτή/WLAN αρχιτεκτονική
- Αμιγώς αδόμητη (Ad-hoc) αρχιτεκτονική
- Υβριδική αρχιτεκτονική

και παραδείγματά τους φαίνονται στην παρακατω εικόνα



α) Αμιγώς κυψελωτή/WLAN αρχιτεκτονική

Το δίκτυο χρησιμοποιεί πύλες δικτύου (gateways) ή access points, που βρίσκονται συνήθως στις διασταυρώσεις, για να συνδέσει τους κόμβους-οχήματα με το Διαδίκτυο, για να συλλέξει δεδομένα από αυτούς, για να τους μεταδώσει σημαντικές πληροφορίες ή για να κάνει τη δρομολόγηση (routing). Ο σταθερός εξοπλισμός παρέχει στους κινούμενους κόμβους συνδεσιμότητα και καλύτερη ποιότητα επικοινωνίας. Όμως το μειονέκτημα αυτής της αρχιτεκτονικής είναι κόστος εγκατάστασης και λειτουργίας του σταθερού εξοπλισμού, που την κάνει να φαίνεται γενικά ασύμφορη σε σχέση με τις υπόλοιπες.

β) Αμιγώς Ad-hoc αρχιτεκτονική

Σε αυτήν την αρχιτεκτονική υφίστανται μόνο κινητοί κόμβοι (οχήματα) και συσκευές RSU.

Η επικοινωνία γίνεται μέσω γειτονικών κόμβων ή για πιο μακρινές αποστάσεις μέσω πολλαπλών συνδέσεων-αλμάτων (hops). Το δίκτυο οργανώνεται μόνο του και δεν απαιτεί κάποια σταθερή υποδομή. Το μειονέκτημα είναι ότι παρουσιάζει μικρότερη αξιοπιστία λόγω της κίνησης των κόμβων και τη μη συνεχή παρουσία τους σε όλα τα σημεία.

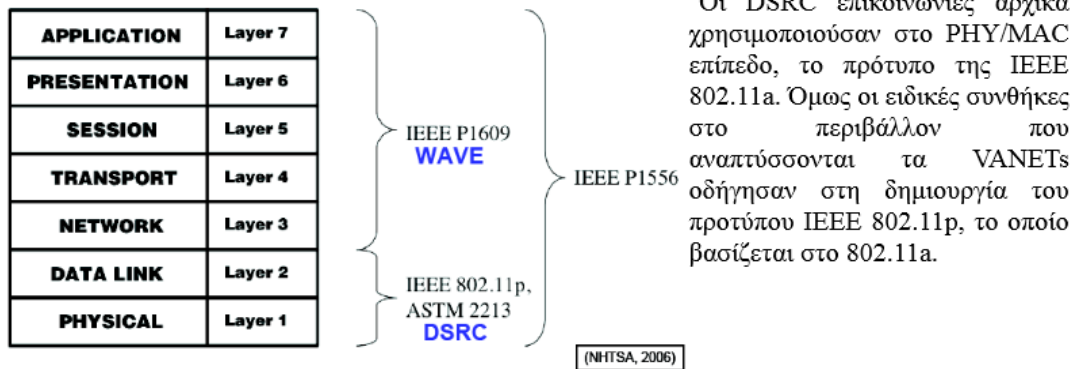
γ) Υβριδική αρχιτεκτονική

Είναι ένας συνδυασμός των προηγούμενων αρχιτεκτονικών. Το δίκτυο υλοποιείται μέσω συνδέσεων οχημάτων-σταθερού εξοπλισμού (V2I – Vehicle to Infrastructure) και μέσω συνδέσεων οχημάτων-οχημάτων (V2V – Vehicle to Vehicle). Ο κάθε τύπος σύνδεσης χρησιμοποιείται ανάλογα με τις συνθήκες που επικρατούν στο δίκτυο και τις ανάγκες της επιθυμητής επικοινωνίας.

5.1.3 ΠΡΟΤΥΠΑ

Η διαδικασία δημιουργίας μιας νέας τεχνολογίας ακολουθεί, κατά κανόνα, ένα συγκεκριμένο τρόπο εξέλιξης. Αρχικά εμφανίζεται ως ερευνητικό αντικείμενο, έπειτα ακολουθούν κάποια πρώιμα πειράματα όπου ελέγχεται η εγκυρότητα της θεωρίας και το τελευταίο και καθοριστικό βήμα πριν την υλοποίησή της είναι η έκδοση προτύπων (standards) για τη συγκεκριμένη τεχνολογία. Τα πρότυπα περιέχουν τις τεχνικές προδιαγραφές, τις μεθόδους, τις διαδικασίες και τις πρακτικές για την υλοποίηση μιας τεχνολογίας. Μετά την έκδοση ενός προτύπου υπάρχει πλέον ένας κοινός κανόνας και ένα κοινό σημείο αναφοράς για τους κατασκευαστές και τους χρήστες, πράγμα που μπορεί να δώσει ώθηση στην εξάπλωση και χρήση της νέας τεχνολογίας.

Στον τομέα των VANETs η προτυποποίηση ξεκίνησε το 1999 όταν η FCC (Federal Communication Commission) των Ηνωμένων Πολιτειών δέσμευσε 75MHz εύρος φάσματος στη ζώνη συχνοτήτων των 5.9GHz με την ονομασία DSRC (Dedicated Short Range Communication). Ο όρος DSRC αναφέρεται σε ασύρματες επικοινωνίες οχημάτων μικρής εμβέλειας. Το 2004 η IEEE ξεκίνησε τις εργασίες για μια νέα σειρά από πρότυπα για VANETs. Αυτή η σειρά προτύπων ονομάστηκε WAVE (Wireless Access in Vehicular Environments).



Μοντέλο OSI και πρότυπα των VANET's

802.11p

Στο DSRC η ζώνη συχνοτήτων χωρίζεται σε 7 κανάλια των 10MHz, όμως υπάρχει και η δυνατότητα να συνδυάζονται 2 κανάλια σε ένα των 20MHz ώστε να αυξάνεται το εύρος ζώνης. Η εμβέλεια κυμαίνεται από 300 έως 1000 μέτρα, ανάλογα με την ισχύ εκπομπής, και ο ρυθμός αποστολής δεδομένων από 3 έως 27Mbps (κανάλια των 10 MHz) και από 6 έως 54Mbps (κανάλια των 20MHz).

5.1.4 ΕΦΑΡΜΟΓΕΣ

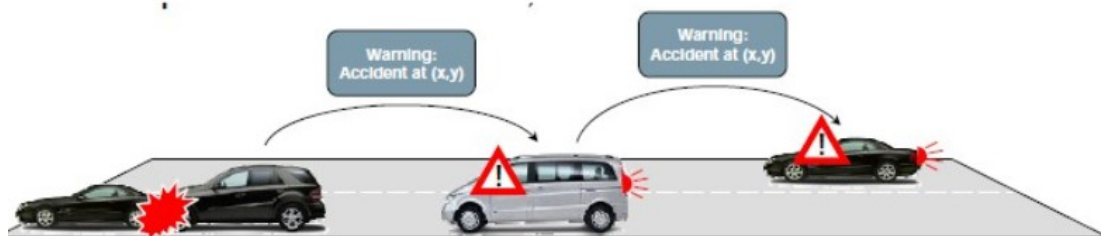
Κύριος σκοπός των VANETs είναι η αύξηση της οδικής ασφάλειας και εκεί στρέφεται και η πλειοψηφία των εφαρμογών που έχουν προταθεί. Επίσης, μελέτη έχει γίνει και σε εφαρμογές για τη βελτίωση των κυκλοφοριακών συνθηκών καθώς και σε μια πληθώρα άλλων υπηρεσιών που δεν σχετίζονται άμεσα με τις δύο προηγούμενες κατηγορίες. Παρακάτω παρουσιάζονται αντιπροσωπευτικά μερικές από αυτές τις εφαρμογές.

Οδική ασφάλεια

Η άμεση επικοινωνία μεταξύ των οχημάτων μπορεί να παίζει καθοριστικό ρόλο στον τομέα των ατυχημάτων που συμβαίνουν στους δρόμους. Κυρίαρχος στόχος είναι η μείωσή τους με την έγκαιρη ειδοποίηση των οδηγών για κίνδυνο ατυχήματος, έτσι ώστε αυτοί να ενεργήσουν κατάλληλα για να το αποφύγουν. Αλλά και στις περιπτώσεις που συμβεί το ατύχημα είναι ζωτικής σημασίας να ληφθούν τα

κατάλληλα μέτρα ώστε να μειωθούν οι συνέπειες. Η ονομαζόμενη και ως “ενεργή ασφάλεια” -σε σύγκριση με την παθητική ασφάλεια, στην οποία ανήκουν οι ζώνες ασφαλείας και οι αερόσακοι- ενεργοποιείται πριν συμβεί το ατύχημα και μερικά παραδείγματά της είναι:

- Ειδοποίηση για απότομο φρενάρισμα του προπορευόμενου αυτοκινήτου.
- Ειδοποίηση διάβασης πεζών.
- Ειδοποίηση συμβάντος ατυχήματος σε οδηγούς τρίτων οχημάτων.
- Ειδοποίηση κινδύνου, λόγω παραβίασης φωτεινού σηματοδότη ή πινακίδας από άλλο όχημα.

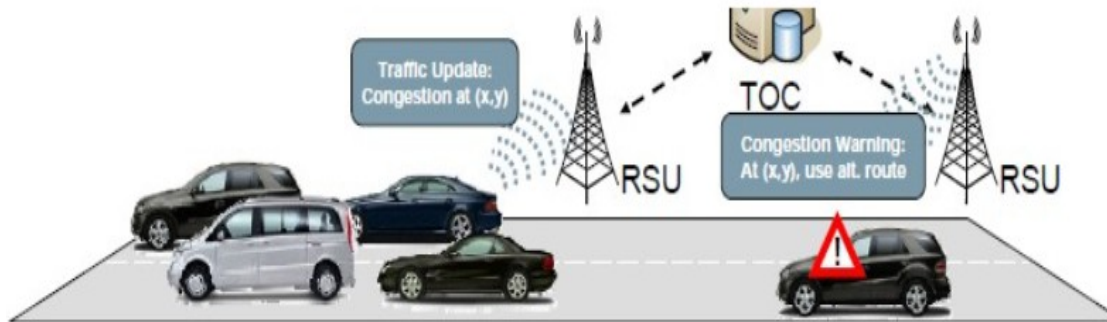


Ειδοποίηση επερχόμενων αυτοκινήτων για συμβάν ατυχήματος

Διευκόλυνση κυκλοφορίας

Σε περιπτώσεις όπου το δίκτυο, εκτός από τα οχήματα, αποτελείται και από σταθερό εξοπλισμό, μπορεί να γίνει ένας κεντρικός έλεγχος του οδικού δικτύου ώστε να διευκολυνθεί η κίνηση των οχημάτων και να αποφεύγεται η κυκλοφοριακή συμφόρηση. Με τη συνεργασία όλων των οχημάτων, το κέντρο ελέγχου γνωρίζει ποια σημεία του οδικού δικτύου έχουν συμφόρηση και έτσι μπορεί να ενημερώσει τα οχήματα που κατευθύνονται προς τα εκεί, ώστε να επιλέξουν μία άλλη διαδρομή.

Επίσης, είναι δυνατή η επικοινωνία και ο συντονισμός ομάδων οχημάτων (αστυνομία, πυροσβεστική, ταξί) που σήμερα γίνεται με άλλα τηλεπικοινωνιακά συστήματα.



Ενημέρωση οδηγών για κυκλοφοριακή συμφόρηση.

Άλλες υπηρεσίες

Οι υπόλοιπες υπηρεσίες που μπορούν να προσφερθούν μέσω ενός δικτύου οχημάτων ανήκουν σε διάφορες κατηγορίες υπηρεσιών.

Οι άμεσα σχετιζόμενες με την οδήγηση μπορεί να είναι η ηλεκτρονική πληρωμή διοδίων, ο εντοπισμός χώρων στάθμευσης σε μία περιοχή, η πληροφόρηση για την ύπαρξη καταστημάτων όπως βενζινάδικα ή συνεργεία αυτοκινήτων, η δυναμική πλοήγηση (navigation).

Ακόμα υπηρεσίες για τους επιβάτες ενός οχήματος -ή για τον οδηγό, όταν το όχημα είναι ακινητοποιημένο- όπως η σύνδεση στο Διαδίκτυο, εφαρμογές πολυμέσων σε συνδυασμό με άλλους χρήστες των VANETs, σχηματισμός Peer-to-Peer (P2P) δικτύων.

Ωστόσο για να αρχίσουν να υλοποιούνται στην πράξη όλες αυτές οι εφαρμογές, θα πρέπει να ληφθούν πολύ αυστηρά μέτρα προφύλαξης από ανεπιθύμητους χρήστες. Αν οι επικοινωνίες δεν είναι ασφαλείς και μπορέσει κάποιος να τις υπονομεύσει, μπορεί να προκληθούν από απλές δυσλειτουργίες μέχρι και ατυχήματα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Δίκτυα Υπολογιστών ,Andrew S.Tanenbaum
- 2.Δίκτυα Υπολογιστών,Εισαγωγή στη Σύγχρονη Τεχνολογία, Patrick Ciccarelli,Christina Faulkner
- 3.Διαφάνεις του μαθήματος “Δίκτυα Δημοσίας Χρήσης και Διασύνδεσης Δικτύων” Χ.Μπούρας
- 4.<http://www.wikipedia.gr/>
- 5.<https://scholar.google.gr/>