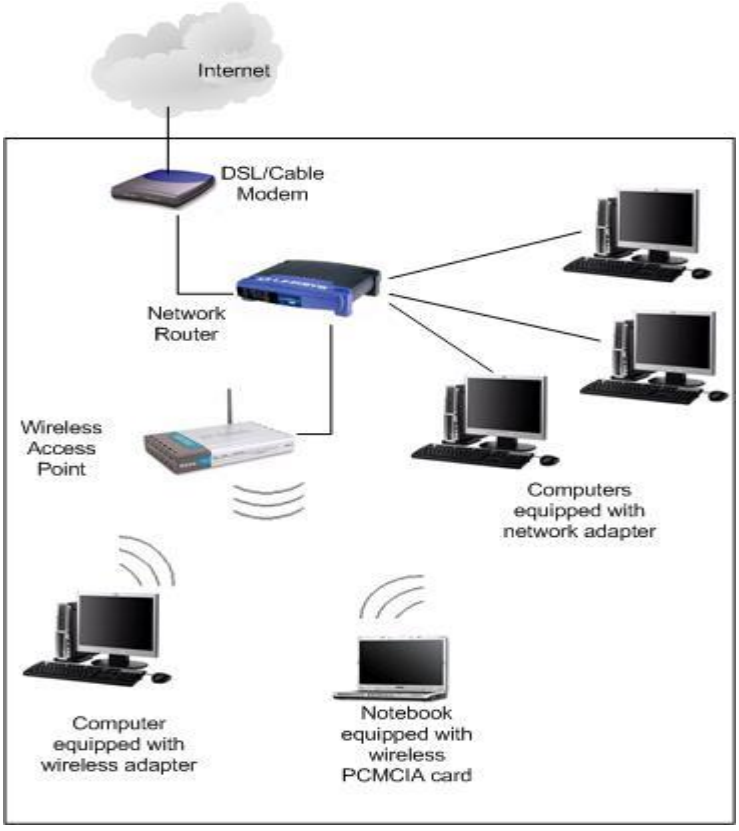
**ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ**
**ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ**
**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

# ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ




**Των φοιτητριών**

**Παπαδοπούλου Δέσποινα** **Επιβλέπον Καθηγητής**

**Αϊβαλιώτου Χριστίνα** **Βασίλειος Βίτσας**

**Αρ. Μητρώου: 04/2559**

**04/2609**

**Θεσσαλονίκη 2011**

# ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

# ΠΡΟΛΟΓΟΣ

Στη σύγχρονη εποχή, οι ανάγκες και οι απαιτήσεις των ανθρώπων συνεχώς αυξάνονται, με συνέπεια την αλματώδη πρόοδο των επιστημών καθώς και τη ραγδαία ανάπτυξη των τεχνολογιών. Οι ρυθμοί της ζωής γίνονται όλο και πιο γρήγοροι και όλοι ψάχνουν τρόπους για να καταφέρουν να εξοικονομήσουν λίγο ελεύθερο χρόνο.

Όπως και με τις υπόλοιπες επιστήμες, έτσι και στον τομέα της πληροφορικής έχουν συμβεί πολλές αλλαγές ώστε να διευκολύνουν τις ζωές των ανθρώπων σε όλους τους τομείς της ζωής τους. Έχουν δημιουργηθεί πολλές νέες φορητές συσκευές, οι οποίες προσφέρουν στους κατόχους τους, την ευελιξία και την κινητικότητα που επιθυμούν. Συγκεκριμένα, στον τομέα των δικτύων, τα τελευταία χρόνια παρατηρείται μία τρομερή ανάπτυξη. Η ανάγκη των ανθρώπων για περισσότερη πληροφόρηση και η ανάπτυξη των πολυμέσων έχει συμβάλει δραματικά στον τομέα των δικτύων.

Ειδικότερα, τα τελευταία χρόνια, έχει σημειωθεί πολύ μεγάλη αύξηση στη χρήση των ασύρματων δικτύων. Το όραμα των ασύρματων δικτύων είναι η δυνατότητα επικοινωνίας παντού, πάντα και με οποιονδήποτε («anywhere, anytime and anyone»). Οι χρήστες των ασύρματων δικτύων έχουν πλέον τη δυνατότητα να ενημερώνονται από οποιοδήποτε σημείο κι αν βρίσκονται και γρήγορα, με τη βοήθεια ενός φορητού υπολογιστή, ακόμα και από το κινητό τους. Επίσης, λόγω των απαιτήσεων των χρηστών, συνεχώς δημιουργούνται νέα πρότυπα και με μεγαλύτερες ταχύτητες. Επιπλέον, με την ανάπτυξη των ασύρματων δικτύων δημιουργήθηκαν νέες εφαρμογές, οι οποίες δε θα μπορούσαν να εφαρμοστούν με τα ενσύρματα δίκτυα. Γενικότερα, η δημοτικότητα των ασύρματων δικτύων οφείλεται όπως είναι λογικό στα πλεονεκτήματα που έχουν.

Στην παρούσα εργασία περιγράφεται η τεχνολογία των ασύρματων δικτύων και ειδικότερα το πρότυπο IEEE 802.11. Τέλος, περιγράφονται και κάποια άλλα πρότυπα ασύρματων δικτύων τα οποία έχουν ήδη δημιουργηθεί και τα χρησιμοποιούν σε καθημερινή βάση. Παραδείγματος χάριν, το γνωστό σε όλους Bluetooth, το οποίο χρησιμοποιούν συχνά στα κινητά τηλέφωνά τους για να μοιραστούν με τους φίλους τους ήχους, βίντεο και εικόνες.

## ΠΕΡΙΛΗΨΗ

Τα ασύρματα δίκτυα έχουν εισβάλει σε κάθε τομέα της ζωής των ανθρώπων και έχουν αναπτυχθεί διάφορες εφαρμογές πάνω σε αυτά. Η ανάπτυξη τους αυτή οφείλεται σε μία πληθώρα πλεονεκτημάτων έναντι των ενσύρματων δικτύων. Η παρούσα πτυχιακή εργασία αφορά τα ασύρματα δίκτυα και ειδικότερα το πρότυπο IEEE 802.11. Το IEEE 802.11, είναι ένα σύνολο προτύπων της IEEE (Institute of Electrical and Electronics Engineers), για τα ασύρματα τοπικά δίκτυα. Τα πρότυπα IEEE 802.11 είναι ευρύτερα γνωστά με την ονομασία «Wi – Fi» επειδή η Wi – Fi Alliance, ένας ανεξάρτητος οργανισμός από την IEEE, παρέχει την πιστοποίηση για τα προϊόντα που υπακούν στις προδιαγραφές του 802.11. Αυτή η οικογένεια προτύπων αποτελεί το καθιερωμένο πρότυπο της βιομηχανίας. Εκτός όμως από το πρότυπο 802.11, το οποίο αναλύεται λεπτομερειακά, υπάρχουν και κάποια άλλα πρότυπα, όπως το Bluetooth και το HIPERLAN τα οποία υποστηρίζουν την ασύρματη μετάδοση.

Όπως έχει τονιστεί πολλές φορές μέχρι τώρα, τα ασύρματα δίκτυα έχουν καταφέρει να γίνουν ένα αναπόσπαστο κομμάτι της καθημερινότητας των ανθρώπων με αποτέλεσμα να εισχωρούν σε όλο και περισσότερες εφαρμογές. Οι χρήστες αποδέχονται κάθε νέο πρότυπο το οποίο τους προσφέρει μεγαλύτερη αξιοπιστία και φυσικά μεγαλύτερες ταχύτητες. Σκοπός αυτής της εργασίας είναι η δημιουργία μιας λεπτομερειακής περιγραφής από τη σύλληψη της ασύρματης επικοινωνίας και την υλοποίηση της μέχρι και τη σημερινή εποχή. Στο πρώτο κεφάλαιο γίνεται εισαγωγή στα ασύρματα δίκτυα, ξεκινώντας με μια ιστορική αναδρομή, τα πλεονεκτήματα και τα μειονεκτήματα τους, καθώς επίσης και τις εφαρμογές τους. Επίσης, αναλύονται οι βασικές μονάδες, η τοπολογία και οι κατηγορίες των ασύρματων δικτύων. Στο δεύτερο κεφάλαιο γίνεται μία μικρή ανάλυση στα κυψελικά δίκτυα. Στο τρίτο κεφάλαιο αναλύουμε την έννοια του ηλεκτρομαγνητικού φάσματος και τους ρυθμιστικούς φορείς οι οποίοι είναι υπεύθυνοι για την αδειοδότηση των συχνοτήτων. Επίσης, αναλύεται το πρότυπο IEEE 802.11 και γίνεται μια σύντομη περιγραφή για όλα τα πρότυπα της οικογένειας IEEE 802.11. Στο τέταρτο κεφάλαιο αναλύεται το φυσικό στρώμα του προτύπου IEEE 802.11, ενώ στο πέμπτο το υπόστρωμα MAC. Στο έκτο κεφάλαιο γίνεται αναφορά σε άλλα πρότυπα ασύρματων δικτύων πέρα από το IEEE 802.11, όπως το HomeRF, το Bluetooth, το HIPERLAN και το IrDA. Στο έβδομο κεφάλαιο

περιγράφεται ένα πρότυπο ασύρματων δικτύων που περιλαμβάνει μία νέα τεχνολογία το WiMAX. Τέλος, στο όγδοο κεφάλαιο, περιγράφονται οι απειλές και η ασφάλεια των ασύρματων δικτύων που προαναφέρθηκαν και φυσικά οι μέθοδοι που χρησιμοποιούνται για να είναι ασφαλής η μετακίνηση των πληροφοριών μέσω των ασύρματων δικτύων.

## ABSTRACT

The wireless networks have spread in every part of our lives and different applications have been developed on them. This development is due to the wide range of advantages against wire networks. This project deals with wireless networks, especially the model IEEE 802.11. IEEE 802.11 is a whole of IEEE's models on local wireless networks. The models IEEE 802.11 are widely known as "WI-FI" because Wi-Fi, an independent organization of the IEEE, gives the certification for its products which are according to the technical specifications of the 802.11. This family of models consists the usual model of industry. Except the model 802.11 that is being examined in detail, there are some other models, such as Bluetooth and HIPERLAN which support the wireless broadcast.

As it has been pointed out several times up to now, wireless networks have managed to become an inseparable part of our lives which results in going into more and more applications. Users accept every new model that offers them greater reliability and, of course, higher speed. The purpose of this project is the creation of an elaborate bibliography from the invention of the wireless communication until the present time. The first unit is an introduction to the wireless networks. There are a historical retrospection, the advantages and disadvantages as well as their applications. In addition, their basic units, topology and types of wireless networks are examined.

The second unit deals with cellular networks. The third unit is about the electromagnetic spectrum and the adjusting vehicles that are responsible for giving license on frequency. Furthermore, the model IEEE 802.11 is being examined and there is a brief description of all the models of the family IEEE 802.11. The fourth unit deals with the natural layer of the model IEEE 802.11 while the fifth unit is about the substratum MAC. The sixth unit is on other models of wireless networks beyond IEEE 802.11, such as HomeRF, Bluetooth, HIPERLAN and IrDa. In unit seven there is a description of a wireless network model that includes the new technology, WiMax. Finally, the eighth unit deals with the threats of the wireless networks, their security and the methods that are used so that the information transfer through wireless network is safe.

## ΕΥΡΕΤΗΡΙΟ ΠΕΡΙΕΧΟΜΕΝΩΝ

## ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

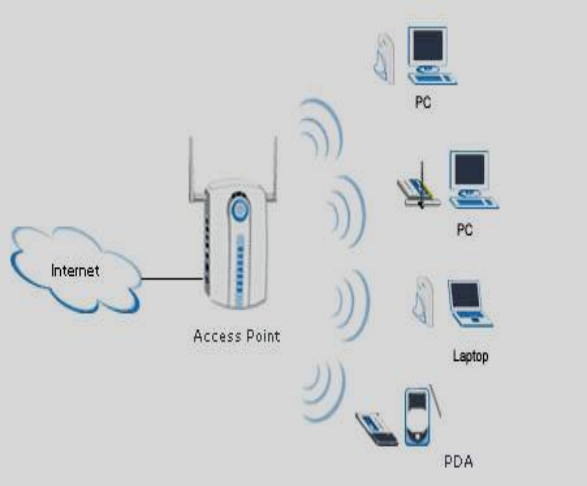
## ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

# 1. ΕΙΣΑΓΩΓΗ

## 1.1 ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια η τεχνολογία των δικτύων έχει αναπτυχθεί σε μεγάλο βαθμό και έχει εισχωρήσει σε κάθε τομέα της ζωής των ανθρώπων. Εκατομμύρια άτομα σε όλον τον κόσμο κάθε μέρα είτε για προσωπική τους χρήση είτε στην εργασία τους, χρησιμοποιούν το διαδίκτυο για την περισυλλογή πληροφοριών, για επικοινωνία και για άλλους σκοπούς όπως θα δείτε και στη συνέχεια. Με λίγα λόγια, έχει γίνει ένα αναπόσπαστο κομμάτι της καθημερινής ζωής όλων.

Παρόλο που η ανάπτυξη του ενσύρματου δικτύου παρείχε πολλές δυνατότητες και ικανές επιδόσεις, ήταν ανεπαρκές σε αρκετές εφαρμογές. Η ευελιξία που



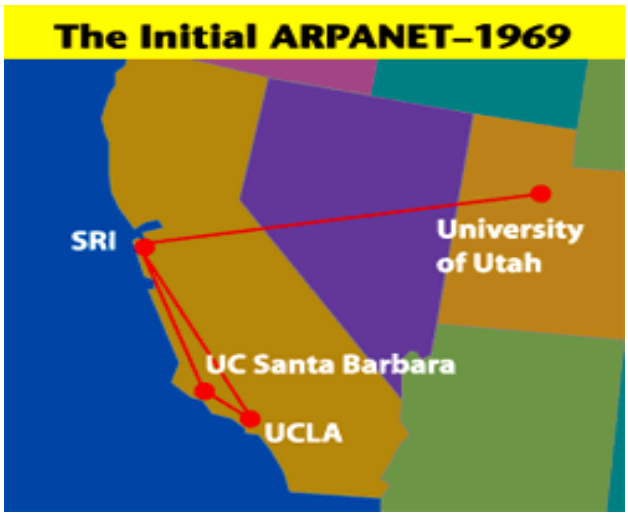

παρείχε το ασύρματο δίκτυο, άνοιξε το δρόμο για νέες εφαρμογές καθώς επίσης, μαζί με τη συνεχώς αναπτυσσόμενη τεχνολογία, κατασκευάστηκαν συσκευές με μικρό κόστος και σε μεγάλες ποσότητες. Τα ασύρματα δίκτυα είναι σχεδιασμένα έτσι ώστε ένα τερματικό να επικοινωνεί με άλλα τερματικά χωρίς τη χρήση καλωδίων. Στα δίκτυα αυτά η μετάδοση των δεδομένων γίνεται μέσω ηλεκτρομαγνητικών κυμάτων και η συχνότητα εξαρτάται από το ρυθμό μετάδοσης που απαιτείται να έχει το δίκτυο. Η ακτίνα δράσης ενός τέτοιου δικτύου είναι αρκετά μέτρα, τα οποία επιτρέπουν τη διασύνδεση ενός κτηρίου, ενός εργοστασίου ή μιας πανεπιστημιούπολης.

## 1.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Όπως πολλοί γνωρίζουν, το Internet είναι γέννημα – θρέμμα του Ψυχρού Πολέμου. Η απόφαση για τη δημιουργία του πρώτου Internet, του ARPANET, ελήφθη μετά από την αποστολή του πρώτου τεχνητού δορυφόρου της γης το 1957, του ρωσικού Sputnik. Στόχος της αμερικανικής κυβέρνησης ήταν η δημιουργία ενός δικτύου το οποίο κατά τη διάρκεια ενός πυρηνικού πολέμου θα

εξακολουθούσε να λειτουργεί, όταν το μεγαλύτερο μέρος των τηλεπικοινωνιών θα κατέρρεε. [2][10][11]

Λύση στο πρόβλημα αυτό έδωσε ένας ερευνητής της εταιρίας Rand, ο Paul Baran, ο οποίος σχεδίασε ένα δίκτυο επικοινωνίας υπολογιστών χωρίς κεντρικό άξονα, κεντρικούς διακόπτες, ούτε καν κεντρική διεύθυνση. Οι ιδέες του Paul Baran οδήγησαν το 1969 στη δημιουργία του πειραματικού δικτύου ARPANET, από τα αρχικά της υπηρεσίας ARPA (Advanced Research Projects Agency) που αργότερα μετονομάστηκε σε DARPA (Defense Advanced Research Projects Agency). Κόμβοι του δικτύου αυτού θα αποτελούσαν οι ισχυρότεροι υπολογιστές της εποχής εκείνης. Ο πρώτος κόμβος τοποθετήθηκε στο UCLA (University of California at Los Angeles) και μέχρι το τέλος του 1969 τοποθετήθηκαν και άλλοι τρεις κόμβοι στο πανεπιστήμιο Utah, στο πανεπιστήμιο California της Santa Barbara και στο ίδρυμα Stanford Research Institute International. Ο χάρτης με τους τέσσερις πρώτους κόμβους φαίνεται στην επόμενη εικόνα. [2][4][9][10][11][13][14]




**ΕΙΚΟΝΑ 1: ΧΑΡΤΗΣ ΜΕ ΤΟΥΣ ΤΕΣΣΕΡΙΣ ΠΡΩΤΟΥΣ ΚΟΜΒΟΥΣ**

Το 1971 ήταν συνδεδεμένοι 23 κόμβοι, ενώ το 1980 ήταν 200 με παράλληλη δημιουργία των πρώτων διεθνών συνδέσεων. Το 1980 χωρίστηκε σε δύο τμήματα από τα οποία το ένα ήταν αποκλειστικά για στρατιωτικές χρήσεις και ονομαζόταν Milnet, ενώ το άλλο για όλες τις υπόλοιπες χρήσεις. Το 1983 το Internet άρχισε να

χρησιμοποιεί το πρωτόκολλο TCP/IP, ενώ από τη δεκαετία του ’80 αναπτύχθηκαν τα πρωτόκολλα Ανοιχτής Διασύνδεσης Συστημάτων OSI και το λειτουργικό σύστημα UNIX, το οποίο διευκόλυνε την επέκταση των διασυνδέσεων μέσω του UUCP (UNIX to UNIX Copy Program). Μια από τις σημαντικότερες εξελίξεις του Internet, ήταν η πρωτοβουλία του NSF (National Science Foundation), κυβερνητικής υπηρεσίας των ΗΠΑ, να δημιουργηθούν πέντε μεγάλα κέντρα υπολογιστών. Μέχρι τότε η πρόσβαση περιοριζόταν στο στρατό και σε λίγους συνεργαζόμενους ερευνητές. Έτσι, το 1986 το NSF δημιούργησε το δίκτυο NSFNET και ο αριθμός των συνδεδεμένων κόμβων στο Internet ήταν 5000. Αυτό είχε ως αποτέλεσμα να αντικαταστήσει το ARPANET, όπου το 1990 διαλύθηκε επισήμως. Η ανάπτυξη του Internet οδήγησε στη συμμετοχή σε αυτό μεγάλων κυβερνητικών υπηρεσιών των ΗΠΑ, όπως το Υπουργείο Ενέργειας και η NASA. Στο μεταξύ, είχε ιδρυθεί το Commercial Internet Exchange (CIX) για εμπορικούς σκοπούς. Όλο και περισσότερες χώρες συνδέονταν στο NSFNET, μεταξύ των οποίων και η Ελλάδα το 1990. Το NSFNET καταργήθηκε επισήμως το 1995. [9][11][12][13]

Το 1991 κυκλοφόρησε το σύστημα αναζήτησης Gopher, ενώ το δίκτυο NSFNET αναβαθμίστηκε σε T3(44.736 Mbps). Το 1992 ιδρύθηκε ένας μη κερδοσκοπικός οργανισμός με την ονομασία Internet Society (ISOC), με σκοπό την ανταλλαγή πληροφοριών μέσω διαδικτύου, ο οποίος λαμβάνει τις τελικές αποφάσεις σε τεχνικά θέματα. Η ISOC διοικείται από το Συμβούλιο Αρχιτεκτονικής του Internet (Internet Architecture Board - IAB), που κατευθύνει κυρίως δύο τομείς, τον τεχνολογικό τομέα (Internet Engineering Task Force - IETF) και τον τομέα έρευνας και ανάπτυξης (Internet Research Task Force – IRTF). Το 1992, το εργαστήριο CERN (Κέντρο Πυρηνικών Ερευνών της Γενεύης) στην Ελβετία παρουσίασε το Παγκόσμιο Ιστό (WWW – World Wide Web) του φυσικού Tim Berners – Lee, το οποίο όμως άρχισε να δημιουργείται το 1989 και τότε είχε σαν τίτλο το “HyperText and CERN”. Το 1993 άρχισε να διαδίδεται ο browser Mosaic, ενώ ο Παγκόσμιος Ιστός παρουσίαζε ρυθμούς ανάπτυξης 341,634%. Σήμερα, καθημερινά, περιοδικά και εφημερίδες εκδίδονται online, επιχειρήσεις και ιδιώτες δημιουργούν τις δικές τους σελίδες στο WWW, το ηλεκτρονικό εμπόριο αναπτύσσεται όλο και περισσότερο, ενώ υπηρεσίες όπως η τηλεργασία, η τηλεκπαίδευση και η τηλεϊατρική είναι ήδη υπό χρήση. [4][9][12][13]

Περνώντας τώρα στο κομμάτι των ασύρματων δικτύων, στο οποίο απευθύνεται η παρούσα εργασία, γυρνώντας στην ιστορία, μπορείτε να διαπιστώσετε ότι τα πρώτα οφέλη αυτής της τεχνολογίας ήρθαν πολύ νωρίς. Η πρώτη εμφάνιση του


ασύρματου δικτύου τοποθετείται το 1971, σε ένα ερευνητικό πρόγραμμα του πανεπιστημίου της Χαβάης με το όνομα ALOHANET. Το ALOHANET έδωσε τη δυνατότητα σε επτά πανεπιστήμια, τα οποία βρισκόντουσαν σε τέσσερα διαφορετικά νησιά να επικοινωνούν μεταξύ τους συνδεδεμένα με τοπολογία αστέρα. Ουσιαστικά, ήταν ένα σύστημα όπου απομακρυσμένοι υπολογιστές είχαν τη δυνατότητα να επικοινωνούν μεταξύ τους μέσω ενός κεντρικού υπολογιστή, ο οποίος ήταν τοποθετημένος στο νησί Oahu, χωρίς τη χρήση των τηλεφωνικών γραμμών, αλλά με τη βοήθεια ραδιοκυμάτων.

Το 1979, ο F.R.Gfeller και ο U.Bapst δημοσίευσαν μία εργασία που περιέγραφε ένα ασύρματο πειραματικό δίκτυο, το οποίο χρησιμοποιούσε την υπέρυθρη ακτινοβολία για την επικοινωνία. Το 1980, ο P.Ferrert περιέγραψε ένα σύστημα ασύρματων δικτύων βασισμένο σε ασύρματο δίαυλο μοναδικού κώδικα εξάπλωσης φάσματος (spread spectrum) και η εργασία του δημοσιεύτηκε στο συνέδριο IEEE National Telecommunications Conference. Το Μάιο του 1985, οι προσπάθειες του Marcus οδήγησαν τον οργανισμό FCC (Federal Communications Commission), ο οποίος καθορίζει το εύρος συχνοτήτων που θα χρησιμοποιείται για κάθε τηλεπικοινωνιακή εφαρμογή, να εξουσιοδοτήσει τη δημόσια χρήση της Βιομηχανικής, της Επιστημονικής και της Ιατρικής ζώνης (ISM bands) που περιλαμβάνει κάποιες συχνότητες ανάμεσα στα 902 MHz έως 5.85 GHz. Η κίνηση αυτή της FCC έδωσε τεράστια ώθηση στην αγορά των ασύρματων δικτύων γιατί στις περισσότερες χώρες του κόσμου δεν απαιτείται καμία ειδική άδεια για την εκπομπή στην περιοχή ISM ζωνών. Αυτό είχε σαν αποτέλεσμα πολλοί κατασκευαστές να πραγματοποιήσουν μαζική παραγωγή ασύρματων προϊόντων. Την εποχή αυτή εξελίσσονται δύο πρότυπα, το ένα στην Ευρώπη από το ETSI (European Telecommunications Standard Institute) και ονομάζεται HIPERLAN (High Performance European Radio LAN) και το άλλο από την IEEE (Institute of Electrical and Electronics Engineers) και ονομάζεται 802.11 WLAN.

Το 1997 η IEEE (Institute of Electrical and Electronics Engineers), η οποία είχε αναλάβει την προτυποποίηση των τοπικών δικτύων (LAN) μέσω της ομάδας 802, δημοσίευσε το πρότυπο 802.11 το οποίο σχεδιάστηκε αρχικά να παρέχει μέγιστη ταχύτητα 2 Mbps στη ζώνη των 2.4 GHz. Το γεγονός αυτό δημιούργησε πολλά προβλήματα γιατί η συγκεκριμένη ζώνη χρησιμοποιείται από ασύρματα τηλέφωνα, από τηλεχειρισμούς των γκαράζ, από φούρνους μικροκυμάτων και άλλες μικροσυσκευές.

Το 1999 παρουσιάστηκαν από το IEEE δύο νέα πρότυπα, το 802.11a και το 802.11b με σκοπό να αυξηθεί η απόδοση των ασύρματων δικτύων στα 54 Mbps. Το πρότυπο 802.11a λειτουργεί στη συχνότητα των 5 GHz ενώ η διακπεραιότητα φτάνει μέχρι τα 54 Mbps, ενώ το πρότυπο 802.11b λειτουργεί στα 2.4 GHz και με διέλευση ως και 11 Mbps. Λόγω των ιδιοτήτων του 802.11b, το οποίο θα αναλυθεί στο ανάλογο κεφάλαιο, έγινε άμεσα αποδεκτό από τους χρήστες του ασύρματου δικτύου και μέχρι σήμερα χρησιμοποιείται από πάρα πολλούς χρήστες. Επίσης, το 1999 πρωτοεμφανίστηκε το Airport στη Νέα Υόρκη από τον Steve Jobs. Το Airport είναι ένα ασύρματο τοπικό δίκτυο το οποίο βασίζεται στο πρωτόκολλο IEEE 802.11b. Από τότε άρχισαν τα ασύρματα δίκτυα να χρησιμοποιούνται και για ιδιωτική χρήση, διότι μέχρι τότε χρησιμοποιούνταν μόνο από εταιρίες εξαιτίας των υψηλών τιμών.

Βέβαια, από το 1999 μέχρι σήμερα έχουν αναπτυχθεί και άλλα πρότυπα της οικογένειας 802.11 τα οποία θα αναλυθούν στη συνέχεια. Τέλος, συγχρόνως με την ανάπτυξη των προτύπων της οικογένειας 802.11, αναπτύχθηκαν και άλλες τεχνολογίες, όπως το 802.16, το HomeRF, το HIPERLAN, το Bluetooth, το WiMax και φυσικά η ανάπτυξη της δορυφορικής τεχνολογίας στον τομέα των επικοινωνιών. Όλα αυτά θα περιγραφούν στα κεφάλαια που ακολουθούν.

## 1.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

Τα τελευταία χρόνια η ανάπτυξη των ασύρματων δικτύων υπήρξε ραγδαία. Μπορούν να χρησιμοποιηθούν σε επιχειρήσεις, σχολεία, νοσοκομεία, αεροδρόμια, βιβλιοθήκες, σε δημόσιες υπηρεσίες καθώς επίσης και σε οποιονδήποτε χώρο επιθυμεί ο χρήστης την επικοινωνία χωρίς τη χρήση καλωδίων. Θα ήταν βέβαια πρέπον να αναφέρουμε ότι τα ασύρματα δίκτυα χρησιμοποιούνται ως συμπλήρωμα των ενσύρματων δικτύων και όχι σαν μία ανταγωνιστική τεχνολογία.

Παρακάτω παρουσιάζονται τα πλεονεκτήματα των ασύρματων δικτύων, στα οποία οφείλεται η άνθισή τους.

**Δυνατότητα Κίνησης**

Στη σημερινή εποχή, όπου οι ρυθμοί της ζωής έχουν γίνει πολύ γρήγοροι και όλοι ψάχνουν τρόπο ώστε να κερδίσουν χρόνο, η κινητικότητα θεωρείται από τα σημαντικότερα πλεονεκτήματα του ασύρματου δικτύου. Οι χρήστες του μπορούν να μετακινούνται εντός της εμβέλειας του ασύρματου δικτύου. Για παράδειγμα, αν έχουν ένα φορητό υπολογιστή, μπορούν να συνδεθούν στο ασύρματο δίκτυο από οποιοδήποτε δωμάτιο, από οποιονδήποτε χώρο του σπιτιού, ακόμα κι αν αυτός ο χώρος βρίσκεται σε διαφορετικό όροφο. Επίσης, μέσα σε μία επιχείρηση, η χρήση ασύρματου δικτύου, μπορεί να αυξήσει την παραγωγικότητα και την απόδοση των εργαζομένων. Οι εργαζόμενοι έχουν πρόσβαση σε δεδομένα οπουδήποτε κι αν βρίσκονται μέσα στην επιχείρηση σε πραγματικό χρόνο, απελευθερώνοντάς τους από τη δέσμευση του γραφείου. [6]

**Ευκολία, ευελιξία και ταχύτητα εγκατάστασης**

Τα ασύρματα δίκτυα εγκαθίστανται με μεγαλύτερη ευκολία και σε λιγότερο χρόνο σε σχέση με τα ενσύρματα δίκτυα. Τα ασύρματα δίκτυα μπορούν να εγκατασταθούν σε περιοχές όπου η εγκατάσταση καλωδίωσης είναι δύσκολη ακόμα και αδύνατη λόγω γεωγραφικής φύσης. Με τη χρήση τους μπορούν να μοιράζονται το ίδιο δίκτυο δύο ή περισσότερα κτήρια, τα οποία πιθανόν να τα χωρίζει ένας αυτοκινητόδρομος, ένα κτήριο ή ακόμα και ένα ποτάμι. Επιπλέον, προβλήματα στην καλωδίωση προκύπτουν και όταν ένα κτήριο είναι παλιό ή ιστορικό. Σε ένα τέτοιο κτήριο πολλών ετών, υπάρχει η πιθανότητα να υπάρξουν υλικές ζημιές κατά την εγκατάσταση των καλωδίων μέσα από τοίχους και ταβάνια.

Ένας τομέας, στον οποίο άρχισαν σχετικά πρόσφατα να χρησιμοποιούνται τα ασύρματα δίκτυα και να φαίνεται η ευελιξία τους, είναι η διασύνδεση των συσκευών. Εκτός, από το να επικοινωνούν οι υπολογιστές μεταξύ τους δια μέσου του δικτύου, σήμερα με τις νέες συσκευές που υπάρχουν στην αγορά, οι χρήστες μπορούν να τις συνδέουν δια μέσου του δικτύου καταργώντας έτσι τα καλώδια. Τέτοιες χρήσεις του ασύρματου δικτύου υπάρχουν στα λεγόμενα «έξυπνα σπίτια».

Επίσης, ένα μειονέκτημα του ενσύρματου δικτύου έναντι του ασύρματου είναι ο χρόνος που χρειάζεται για να πραγματοποιηθεί η εγκατάσταση του. Είναι γνωστό πως η διαδικασία της καλωδίωσης είναι μία χρονοβόρα διαδικασία που μπορεί να διαρκέσει από λίγες ημέρες έως και μερικές εβδομάδες, ανάλογα με την έκταση και τη γεωγραφική θέση του δικτύου, επειδή οι τεχνικοί θα πρέπει να εγκαταστήσουν ομοαξονικά καλώδια ή καλώδια UTP μέσω ειδικών διόδων ανάμεσα στους τοίχους. Επιπλέον, σε περίπτωση που χρειαστεί να σκάψουν για να τοποθετήσουν υπόγειες υποδομές, πιθανόν να χρειαστεί να πάρουν άδεια από το δήμο, κάτι το οποίο θα καθυστερήσει ακόμα περισσότερο την ολοκλήρωση της εγκατάστασης.

Τέλος, με το ασύρματο δίκτυο οι αλλαγές στην τοπολογία του δικτύου γίνονται πολύ πιο εύκολα και σε μικρότερο χρονικό διάστημα. Αυτό οφείλεται στο γεγονός ότι δε χρειάζεται να αφαιρούνται ή να προστίθενται καλώδια. Χωρίς ιδιαίτερο κόπο μπορεί μία εταιρία να επεκτείνει ή να συρρικνώνει τα γραφεία της σε επόμενους ορόφους ακόμα και σε διαφορετικά κτήρια. Αυτό είναι ένα πολύ σημαντικό προτέρημα των ασύρματων δικτύων διότι συχνά επιχειρήσεις αναδιοργανώνονται ανάλογα με τα κέρδη τους. [6][7]

**Κόστος**

Στα ασύρματα δίκτυα, λόγω της έλλειψης των καλωδίων, το κόστος εγκατάστασης και συντήρησης είναι μικρότερο σε σχέση με τα ενσύρματα δίκτυα. Ειδικά στις επιχειρήσεις, όπου υπάρχουν συχνές αλλαγές στο χώρο, επεκτάσεις και συρρικνώσεις, η μείωση του κόστους είναι εμφανής. Μάλιστα σε έρευνα που πραγματοποιήθηκε από την Wireless LAN Association η ανταποδοτικότητα επένδυσης (Return of Investment ,ROI) των ασύρματων δικτύων είναι εντυπωσιακή, επειδή σε όποια επιχείρηση κι αν χρησιμοποιήθηκε, απέδωσε σε 12 μόλις μήνες το κόστος αγοράς του εξοπλισμού και συνέβαλε σημαντικά στην αύξηση της κερδοφορίας. [6]

**Αυξημένη αξιοπιστία**

Η απουσία των καλωδίων προσφέρει αυξημένη αξιοπιστία. Αυτό οφείλεται στο γεγονός ότι δεν αναπτύσσονται φαινόμενα όπως η διάβρωση που προκαλείται από το περιβάλλον, οι ανακλάσεις σήματος οι οποίες οφείλονται στον ατελή

τερματισμό των καλωδίων καθώς επίσης και η ολική κατάρρευση του δικτύου λόγω καταστροφής των καλωδίων.

**Εμβέλεια**

Η εμβέλεια ενός ασύρματου δικτύου μπορεί να είναι μερικές δεκάδες μέτρα. Για παράδειγμα, το πρωτόκολλο 802.11b διαθέτει εμβέλεια 30 μέτρα εντός ενός κτιρίου, ενώ σε ανοιχτό χώρο, όπου υπάρχει οπτική επαφή ανάμεσα στις ασύρματες συσκευές, 90 μέτρα. Η μεγάλη αυτή διαφορά οφείλεται στη μεσολάβηση λιγότερων εμποδίων, μιας και εντός ενός κτιρίου οι τοίχοι απορροφούν ή ανακλούν τα μικροκύματα. Στη μέγιστη απόσταση ο ρυθμός μετάδοσης δε ξεπερνά το 1 Mbps. Στο πρωτόκολλο 802.11a, η ταχύτητα φτάνει τα 54 Mbps σε απόσταση περίπου 20 μέτρα. Επιπλέον, στο πρωτόκολλο 802.11n, η μέγιστη εμβέλεια είναι 70 και 160 μέτρα, για χώρους εντός και εκτός κτιρίου αντίστοιχα. Συγκεκριμένα, το 802.11n φτάνει την ταχύτητα των 70 Mbps σε απόσταση 100 μέτρων. Με βάση τα παραπάνω γίνεται αντιληπτό ότι αυτό που επηρεάζει σημαντικά την εμβέλεια του ασύρματου δικτύου είναι τα μεταλλικά αντικείμενα υψηλής πυκνότητας. Επίσης, άλλα στοιχεία που μπορούν να επηρεάσουν το δίκτυο είναι οι πέτρινοι τοίχοι, τα τούβλα, τα ξύλα και το νερό, αλλά σε μικρότερο βαθμό.

**Συμβατότητα με το υπάρχον δίκτυο**

Ένα επιπλέον πλεονέκτημα, είναι η συμβατότητα των ασύρματων με τα ενσύρματα δίκτυα. Με τον κατάλληλο εξοπλισμό μπορεί να προστεθεί ένα ασύρματο δίκτυο στο υπάρχον ενσύρματο δίκτυο εύκολα, αποτελώντας πολλές φορές επέκταση του. Αυτό έχει ως αποτέλεσμα, να μην απαιτείται η καλωδίωση μέχρι τον τελικό χρήστη, όπου πολλές φορές μπορεί να είναι δύσκολο λόγω εδάφους και οικονομικών.

## 1.4 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

Παρόλο που τα ασύρματα δίκτυα προσφέρουν μια πληθώρα από πλεονεκτήματα τα οποία διευκολύνουν και εξυπηρετούν τις ζωές όλων όσων τα χρησιμοποιούν, είναι φυσικό να υπάρχουν και κάποια μειονεκτήματα.

Το πρώτο μειονέκτημα που έχουν τα ασύρματα δίκτυα είναι η εξασθένιση του σήματος, η οποία εξαρτάται από την απόσταση που υπάρχει ανάμεσα στην ασύρματη συσκευή και στον τελικό χρήστη. Στην εξασθένιση του σήματος, όπως αναφέρθηκε και στην παράγραφο σχετικά με την εμβέλεια, επηρεάζουν τα μεταλλικά αντικείμενα υψηλής πυκνότητας, το ξύλο, το νερό, τα τούβλα και τέλος οι πέτρινοι τοίχοι.

Ένα επιπλέον μειονέκτημα είναι οι παρεμβολές που συμβαίνουν λόγω χρήσης του ίδιου φάσματος και από γειτονικά ασύρματα δίκτυα, αλλά και από άλλες μορφές ασύρματης μετάδοσης όπως είναι τα κινητά τηλέφωνα, τα Bluetooth και άλλες οικιακές συσκευές όπως ο φούρνος μικροκυμάτων.

Επίσης, ένα ακόμα μειονέκτημα είναι η ασφάλεια. Τα ασύρματα δίκτυα είναι ευάλωτα σε παραβιάσεις από κακόβουλους εισβολείς και hackers. Η σύνδεση στο δίκτυο γίνεται μέσω του αέρα και όχι μέσω κάποιου φυσικού μέσου, όπως στα ενσύρματα δίκτυα όπου η σύνδεση γίνεται μέσω των καλωδίων. Βέβαια για να περιοριστούν τα προβλήματα ασφαλείας έχουν ενσωματωθεί στα νέα πρότυπα μέθοδοι κρυπτογράφησης. Επίσης, οι ίδιοι οι χρήστες μπορούν να προστατευτούν με τη χρήση Firewalls, εργαλείων Antispyware και με διάφορα λογισμικά προστασίας από ιούς.

Το ασύρματο δίκτυο προσφέρει ελευθερία κινήσεων, καθώς καταργεί τη χρήση των καλωδίων. Όμως, τα ασύρματα δίκτυα έχουν το μειονέκτημα της ακτινοβολίας. Κάποιοι πιστεύουν πως η ακτινοβολία δεν είναι ιδιαίτερα επικίνδυνη για τον ανθρώπινο οργανισμό διότι βρίσκεται μέσα στα επιτρεπτά όρια. Οι κεραίες ενός ασύρματου δικτύου εκπέμπουν μη ιονίζουσες ηλεκτρομαγνητικές ακτινοβολίες. Συγκεκριμένα, σε ένα άρθρο στην Κυριακάτικη Ελευθεροτυπία, ο καθηγητής Βιοχημείας του πανεπιστημίου Πατρών Χρήστος Γεωργίου (βλ.: www.biology.upatras.gr/cgeorgiou) αναφέρει ότι τα επίπεδα έκθεσης των χρηστών εντός των ορίων ασφαλείας, που έχουν ωστόσο καθοριστεί μόνο για να μην προκαλούν θερμικές επιδράσεις, προσδιορίστηκαν για την προστασία ενός ενήλικα εγκεφάλου. Με αυτό εδώ θέλει να τονίσει πως ακόμα δεν προσδιορίστηκαν οι επιδράσεις τις ακτινοβολίας για τον παιδικό εγκέφαλο αλλά ούτε και για τα υπόλοιπα ευαίσθητα όργανα εκτός του εγκεφάλου. Ειδικά σε άτομα

με ηλεκτρομαγνητική υπερευαισθησία, τα προβλήματα εκδηλώνονται άμεσα, πολλές φορές με κνησμό, τσούξιμο, πυρετό και κοκκινίλες.

Ένα ζωντανό παράδειγμα στην ευαισθησία στην ακτινοβολία, είναι ένας D.J., ο


Steve Miller, ο οποίος λόγω της αλλεργίας του στην ακτινοβολία του ασύρματου δικτύου, έχει καταδικαστεί να ζει στην εξορία. Η ακτινοβολία των ασύρματων δικτύων του προκαλούν ίλιγγο, τάση για εμετό και αποπροσανατολισμό, με αποτέλεσμα να μη μπορεί να μπει σε τρένα, να μείνει σε ξενοδοχεία και γενικά οπουδήποτε υπάρχει ασύρματο δίκτυο. Ο ίδιος του έχει δηλώσει «Αν θέλω να πιω ένα ποτήρι μπύρα, πρέπει να διανύσω πέντε χιλιόμετρα για να πάω στη μοναδική παμπ της περιοχής μου που δεν έχει Wi-Fi. Δεν μπορώ να πάω στα μαγαζιά γιατί τα ηλεκτρομαγνητικά κύματα με επηρεάζουν αμέσως. Μπορώ αμέσως να αισθανθώ τα Wi-Fi και αναγκάζομαι να το βάλω στα πόδια.». Είναι ένας από το περίπου 2% του πληθυσμού που υποφέρει από Ηλεκτρονική Υπερευαισθησία. Το μόνο μέρος όπου μπορεί να βρει καταφύγιο είναι το σπίτι του, το οποίο είναι απομονωμένο με γρανιτένιους τοίχους πάχους μισό μέτρο, σε ένα χωριό κοντά στο Falmouth της Κορνουάλλης, στην Αγγλία. (Πηγή: Telegraph)

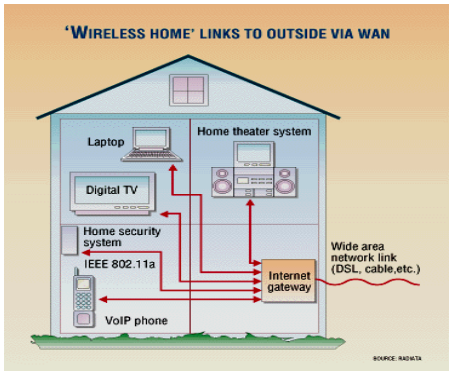
Στο σημείο αυτό, είναι πρέπον να αναφερθεί πως η ακτινοβολία που εκπέμπεται από ένα κινητό τηλέφωνο είναι μεγαλύτερη από αυτή ενός ασύρματου δικτύου, με τη διαφορά ότι το πρώτο εκπέμπει μεγάλη ποσότητα ακτινοβολίας τη στιγμή που πραγματοποιείται μία κλήση, ενώ το δεύτερο όσο το router είναι σε λειτουργία. Ένα πολύ ενδιαφέρον άρθρο, αν και αφορά τη κινητή τηλεφωνία, αναφέρει πως οι επιστήμονες από το κέντρο ερευνών της Φλόριντας για το Άλτσχαϊμερ ανακάλυψαν ότι η έκθεση στην ακτινοβολία από τα κινητά τηλέφωνα προστατεύει τη μνήμη των ποντικιών που ήταν «προγραμματισμένα» να εμφανίσουν τη νόσο. Στο πείραμα, τα αποτελέσματα του οποίου δημοσιεύονται στην επιθεώρηση Journal of Alzheimer’s Disease, χρησιμοποιήθηκαν 96 ποντίκια. Τα περισσότερα είχαν προγραμματιστεί γενετικά ώστε να αναπτύσσουν τις αλλοιώσεις στον εγκέφαλο που συνδέονται με το Άλτσχαϊμερ. Όλα τα ποντίκια εκτέθηκαν στο ηλεκτρομαγνητικό πεδίο που εκπέμπει ένα συνηθισμένο τηλέφωνο για δύο

περιόδους της μιας ώρας καθημερινά για επτά με εννέα μήνες. Τα ποντίκια που άρχισαν να εκτίθενται στην ακτινοβολία σε νεαρή ηλικία και προτού αρχίσουν τα σημάδια απώλειας μνήμης, προστατεύτηκαν από τα συμπτώματα της νόσου, ενώ τα γηραιότερα που είχαν ήδη εμφανίσει συμπτώματα, αυτά εξαφανίστηκαν μετά την έκθεση. Στις αυτοψίες που πραγματοποιήθηκαν στα πειραματόζωα, δεν εντοπίστηκαν προβλήματα ούτε κακοήθεις όγκοι στους εγκεφάλους ή τα ζωτικά όργανα. Οι επιστήμονες πειραματίζονται πλέον με πεδία διαφορετικής συχνότητας και έντασης, επιχειρώντας να βελτιώσουν περαιτέρω το αποτέλεσμα. (Πηγή: BBC). Τέλος, αξίζει να αναφέρουμε πως σε πολλές ευρωπαϊκές χώρες υπάρχουν πολλές ανακοινώσεις σχετικά με τους κινδύνους που μπορεί να έχει η έκθεσή μας στην ακτινοβολία, με πιο αρνητική μέχρι σήμερα τη γερμανική κυβέρνηση.

## 1.5 ΕΦΑΡΜΟΓΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Στη σύγχρονη εποχή, η ασύρματη επικοινωνία έχει ένα ευρύτατο φάσμα εφαρμογών οι οποίες ξεκινάνε από απλές ερασιτεχνικές εφαρμογές στις οικείες μέχρι ποικίλους επιχειρηματικούς κλάδους, είτε απλούς είτε πολύπλοκους. Κάθε μέρα όλο και περισσότεροι κάνουν χρήση των εφαρμογών των ασύρματων δικτύων, με αποτέλεσμα να υπάρχει ένας μεγάλος αριθμός από εφαρμογές οι οποίες περιορίζονται πλέον μόνο από τη φαντασία των χρηστών.

Σε οικιακό επίπεδο, ένα ασύρματο δίκτυο μπορεί να χρησιμοποιηθεί για τη σύνδεση ενός ή περισσότερων ηλεκτρονικών υπολογιστών, ενός ηχοσυστήματος ή μίας κονσόλας παιχνιδιού όπως το Playstation 3, ώστε να μοιράζονται τα δεδομένα. Μέσα σε ένα σπίτι, από άποψη αισθητικής, η χρήση ενός ασύρματου δικτύου, είναι σαφώς καλύτερη λόγω της μη χρήσης καλωδίων. Κοινώς, η ασύρματη δικτύωση μπορεί να αποτελέσει την εύκολη λύση για τη σχεδίαση του «έξυπνου σπιτιού».




Πέρα όμως από τις απλές εφαρμογές στο σπίτι, η ασύρματη δικτύωση έχει πολλές εφαρμογές σε εμπορικούς και επιχειρηματικούς τομείς. Ένα ξενοδοχείο, για παράδειγμα, μπορεί να παρέχει στους πελάτες του ασύρματη πρόσβαση στο Internet με σχετικά μικρό κόστος ακόμα και δωρεάν. Ένα στοιχείο που προσέχουν

πολλοί πελάτες. Άλλωστε, σήμερα, τα περισσότερα ξενοδοχεία διαθέτουν μεγάλους χώρους για συνέδρια και άλλες τέτοιες εκδηλώσεις, όπου πολλές φορές είναι απαραίτητη η πραγματοποίηση συνδιάσκεψης ή η χρήση ενός φορητού υπολογιστή για τη σύνδεση στο διαδίκτυο και την ανάκτηση πληροφοριών. Παρόμοια, σε ένα εκθεσιακό χώρο, σε χώρους συνεστιάσεων, σε αεροδρόμια μέχρι και σε καφετέριες, όπου συχνά εργαζόμενοι κατά τη διάρκεια του διαλείμματος τους πηγαίνουν για καφέ μαζί με το φορητό τους υπολογιστή, ώστε να είναι σε διαρκή επαφή με το γραφείο τους, γεγονός που προσελκύει περισσότερους πελάτες.

Επιπλέον, στον τομέα της υγείας, με τη χρήση PDA με δυνατότητες ασύρματης δικτύωσης, θα μπορούν οι ιατροί και οι νοσοκόμες, να ενημερώνονται πολύ γρήγορα για το ιστορικό ενός ασθενή. Επίσης, στο χώρο της εκπαίδευσης, τα ασύρματα δίκτυα μπορούν να χρησιμοποιηθούν στη δευτεροβάθμια και στην τριτοβάθμια εκπαίδευση ως ένα βοηθητικό μέσω εκμάθησης και περισυλλογής πληροφοριών. Ιδιαίτερα, στους πανεπιστημιακούς χώρους, το διαδίκτυο αποτελεί την κυριότερη πηγή πληροφοριών για την αναζήτηση στοιχείων για τυχόν εργασίες ή για περαιτέρω μελέτη ή για να μοιράζονται οι φοιτητές μεταξύ τους δεδομένα. Με τη χρήση ασύρματων δικτύων, ανοίγονται επιπλέον θέσεις στα εργαστήρια, αρκεί ο φοιτητής να διαθέτει ένα φορητό υπολογιστή. Τέλος, έχουν κάνει ήδη την εμφάνισή τους οι πρώτοι WISPs (Wireless Internet Service Providers), οι οποίοι συναντάνε μεγάλη αποδοχή από τους χρήστες του Internet.

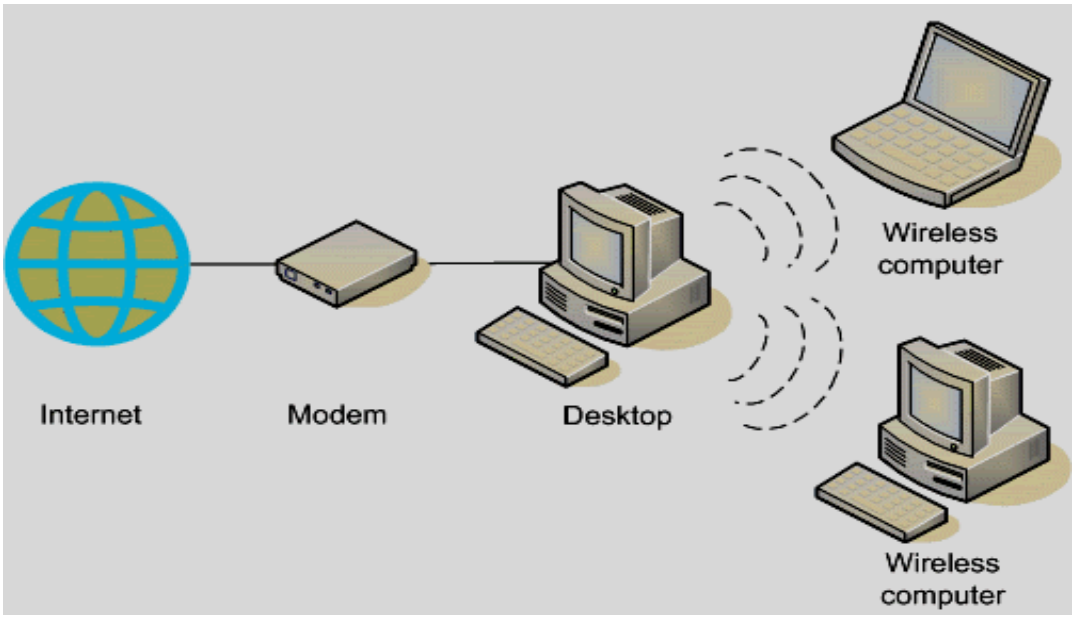
Γενικότερα, οι εφαρμογές των ασύρματων δικτύων χωρίζονται σε τέσσερις κατηγορίες. Οι κατηγορίες αυτές είναι η χρήση τους ως επέκταση ενσύρματων δικτύων, η διασύνδεση μεταξύ κτιρίων, η σποραδική πρόσβαση στο δίκτυο και τέλος η δημιουργία ad hoc δικτύων. Οι κατηγορίες αυτές αναλύονται στη συνέχεια.

Όπως αναφέρθηκε πολλές φορές ως τώρα, είναι δύσκολο να χρησιμοποιηθούν τα ενσύρματα δίκτυα σε μεγάλους χώρους, όπως μία αποθήκη ή ένα εργοστάσιο, σε παλιά κτήρια ή κτήρια που έχουν οριστεί ως διατηρητέα όπου είναι αδύνατη η ύπαρξη καλωδίωσης επειδή απαγορεύεται το άνοιγμα τρυπών. Έτσι τα ασύρματα δίκτυα μπορούν να χρησιμοποιηθούν ως επέκταση των ενσύρματων δικτύων, ώστε να μη χρειάζεται καλωδίωση μέχρι τον τελικό χρήστη, κάτι που θεωρείται δύσκολο και καθόλου οικονομικό.

Με την ανάπτυξη των ασύρματων δικτύων, είναι δυνατή η σύνδεση δύο δικτύων σε διαφορετικά κτήρια με τη βοήθεια συσκευών όπως δρομολογητές ή γέφυρες.

Επίσης, είναι δυνατή και η σποραδική πρόσβαση στο δίκτυο. Οι χρήστες ενός ασύρματου δικτύου μέσα σε μία εταιρία, σε ένα αεροδρόμιο, σε ένα εργοστάσιο, σε μία βιβλιοθήκη, σε ένα πανεπιστήμιο ή ακόμα και σε ένα νοσοκομείο, μπορούν να μετακινούνται μέσα στο χώρο τους και να παραμένουν συνδεδεμένοι έχοντας πρόσβαση στα αρχεία τους.

Τέλος, μία ακόμα εφαρμογή των ασύρματων δικτύων είναι η δημιουργία ad hoc δικτύων. Ένα ad hoc δίκτυο είναι μια σύνδεση μεταξύ υπολογιστών και συσκευών που χρησιμοποιείται για ένα συγκεκριμένο σκοπό, παραδείγματος χάριν για παιχνίδια και για κοινή χρήση δεδομένων. Τέτοιου είδους δίκτυα συνήθως εγκαθίστανται προσωρινά. Ένα παράδειγμα χρήσης ενός τέτοιου δικτύου είναι σε ένα αμφιθέατρο ενός πανεπιστημίου όπου γίνεται παρουσίαση εργασιών και οι υπόλοιποι θα μπορούν να τις παρακολουθούν μέσα από τους υπολογιστές που υπάρχουν μπροστά τους.



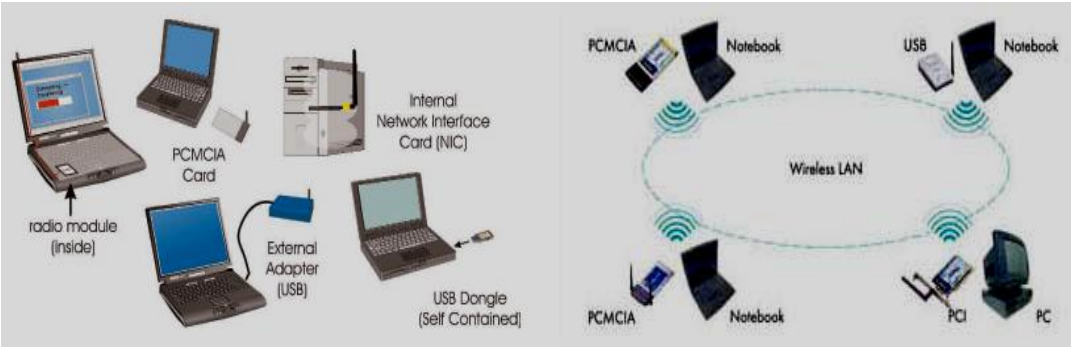

**ΕΙΚΟΝΑ 2: ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ**

## 1.6 ΒΑΣΙΚΕΣ ΜΟΝΑΔΕΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Ένα ασύρματο δίκτυο αποτελείται από σταθμούς, σημεία πρόσβασης, σύστημα διανομής και από το μέσο μετάδοσης, τα οποία θα αναλυθούν στη συνέχεια. Όλα αυτά, βοηθάνε να πραγματοποιηθεί σωστή μετάδοση και λήψη των δεδομένων και επεξεργασία του σήματος.

### Σταθμοί (Stations)

Τα δίκτυα δημιουργούνται με σκοπό να μεταφέρουν πληροφορίες από τον έναν σταθμό στον άλλον. Συνήθως, οι σταθμοί είναι φορητές συσκευές, όπως laptops και κινητά τηλέφωνα. Σε πολλές περιπτώσεις, τα ασύρματα δίκτυα χρησιμοποιούνται για την αποφυγή των καλωδίων καθώς παρατηρείται μεγάλη ευελιξία, ειδικά σε μεγάλους χώρους. Ένας σταθμός μπορεί να λειτουργεί και ως αποστολέας, αλλά και ως δέκτης. [6]




**ΕΙΚΟΝΑ 3: ΣΤΑΘΜΟΙ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ**

### Σημείο πρόσβασης (Access Point – AP)

Τα σημεία πρόσβασης είναι συσκευές οι οποίες παίζουν το ρόλο της γέφυρας ανάμεσα στα ενσύρματα και τα ασύρματα δίκτυα με σκοπό να μετατρέπουν κατάλληλα τα πλαίσια που μεταδίδονται. Βέβαια, στη συνέχεια της παρούσας εργασίας, θα παρατηρήσετε ότι εκτελούν κι άλλες εργασίες. [6]

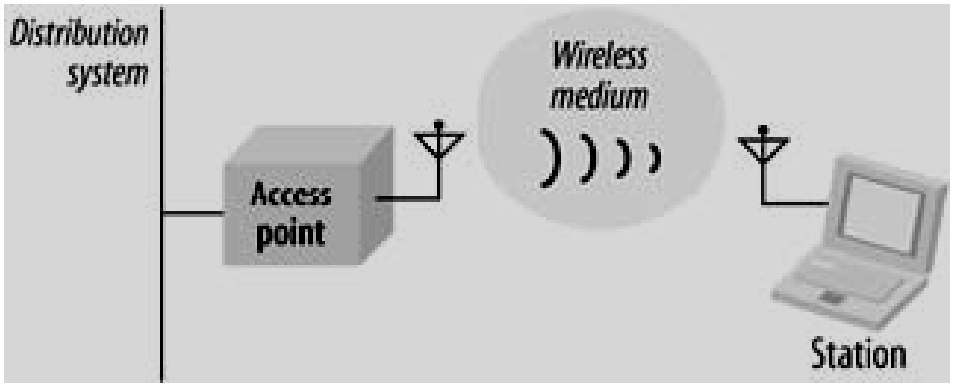
### Ασύρματο μέσο μετάδοσης (Wireless Medium)

Για να μπορέσουν τα πλαίσια να μεταδοθούν από τον ένα σταθμό στον άλλον, χρησιμοποιούν ένα μέσο μετάδοσης. Έχουν οριστεί διάφορα φυσικά επίπεδα, αφού η αρχιτεκτονική επιτρέπει σε πολλαπλά φυσικά επίπεδα να αναπτυχθούν και να υποστηρίξουν το 802.11, τα οποία χρησιμοποιούν είτε υπέρυθρες ακτίνες είτε

ραδιοσυχνότητες για την επίτευξη της μετάδοσης μεταξύ των σταθμών ενός ασύρματου δικτύου. [6]

**Σύστημα Διανομής (Distribution System)**

Όταν συνδέονται περισσότερα του ενός Σημεία Πρόσβασης (Access Point), με σκοπό τη δημιουργία μιας ευρείας περιοχής κάλυψης, πρέπει να επικοινωνούν ώστε να παρακολουθούν τη κίνηση των χρηστών. Το σύστημα διανομής ενώνει τα διάφορα AP του ίδιου δικτύου, με σκοπό να προωθεί τα πλαίσια στον προορισμό τους. Το πρωτόκολλο 802.11 δεν προσδιορίζει κάποια συγκεκριμένη τεχνολογία για το σύστημα διανομής. Σε πολλά εμπορικά προϊόντα, αποτελεί ένα συνδυασμό μιας μηχανής γεφύρωσης (bridging engine) και ενός μέσου διανομής (distribution medium) και είναι το κυρίως δίκτυο που χρησιμοποιείται για την αναμετάδοση των πλαισίων ανάμεσα στα σημεία πρόσβασης, συχνά αποκαλείται και Βασικό Δίκτυο (Backbone Network). [6]



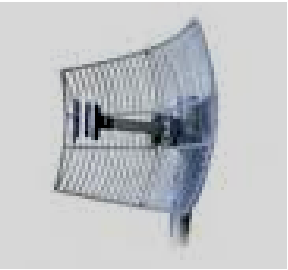

ΕΙΚΟΝΑ 4: ΣΥΣΤΗΜΑ ΔΙΑΝΟΜΗΣ

## 1.7 ΚΕΡΑΙΕΣ

Η κεραία είναι το κομμάτι εκείνο των συσκευών ασύρματης επικοινωνίας, το οποίο ακτινοβολεί και δέχεται το ηλεκτρομαγνητικό σήμα που μεταδίδεται στον αέρα. Συγκεκριμένα, η μετάδοση είναι μια διαταραχή στο ηλεκτρομαγνητικό πεδίο που εκπέμπει η κεραία. Η διαταραχή αυτή παράγεται από τη συσκευή μετάδοσης μεταβάλλοντας την τιμή της τάσης του ρεύματος σε σχέση με το χρόνο σε συγκεκριμένη συχνότητα. Αντίστοιχα, κατά τη λήψη ενός σήματος η κεραία είναι αυτή που δέχεται το σήμα, το οποίο στη συνέχεια ερμηνεύεται σαν δεδομένα από τη συσκευή μετάδοσης / λήψης.

Βασικά χαρακτηριστικά μίας κεραίας είναι ο τύπος της κεραίας, η ενίσχυση του σήματος που παρέχει και το εύρος της ακτινοβολίας της. Με τη βοήθεια αυτών των χαρακτηριστικών, οι χρήστες μπορούν να επιλέξουν ποια κεραία θα χρησιμοποιήσουν για την υλοποίηση του δικτύου τους. Υπάρχουν τρεις βασικές κατηγορίες στις οποίες χωρίζονται οι κεραίες, ανάλογα με τον τρόπο που εκπέμπουν το σήμα. Οι κατευθυντικές, οι μη κατευθυντικές και οι κεραίες διπλής κατεύθυνσης.

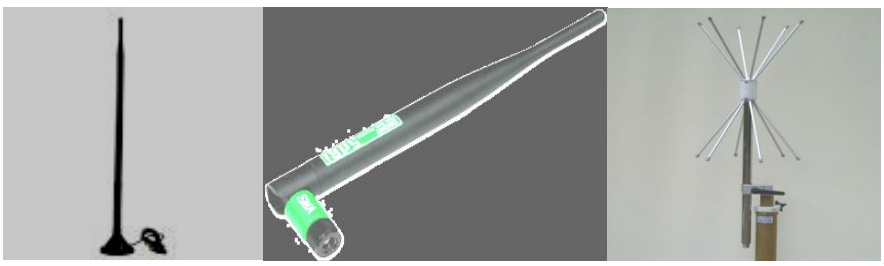
## Κατευθυντικές Κεραίες (Directional)



Οι κατευθυντικές κεραίες εκπέμπουν προς μία μόνο κατεύθυνση και σε μικρή γωνία εκπομπής, με αποτέλεσμα να συγκεντρώνεται η ισχύς του σήματος προς τη συγκεκριμένη κατεύθυνση. Στο γεγονός αυτό οφείλεται και ο χαρακτηρισμός τους ως οι πιο ισχυρές από τις άλλες κατηγορίες κεραιών. Συνήθως, χρησιμοποιούνται για τη δημιουργία point to point συνδέσεων μεταξύ απομακρυσμένων σημείων, όπως μεγάλα κτήρια, σπίτια, ακόμα και πόλεις. Τα «πιάτα» και οι κεραίες πλέγματος ανήκουν σε αυτήν την κατηγορία.

## Μη Κατευθυντικές Κεραίες (Omni directional)

Οι μη κατευθυντικές κεραίες εκπέμπουν κυκλικά σε 360 μοίρες στον οριζόντιο άξονα και ενισχύουν το σήμα μειώνοντας την εκπομπή στον κάθετο άξονα. Χρησιμοποιούνται κυρίως σε τοπικά ασύρματα δίκτυα και σε point to multipoint συνδέσεις Οι κάθετες κεραίες ανήκουν σε αυτήν την κατηγορία και συνήθως αποτελούν μία πιο οικονομική λύση.



**ΕΙΚΟΝΑ 5: ΜΗ ΚΑΤΕΥΘΥΝΤΙΚΕΣ ΚΕΡΑΙΕΣ**

### Κεραίες διπλής κατεύθυνσης (Bidirectional)

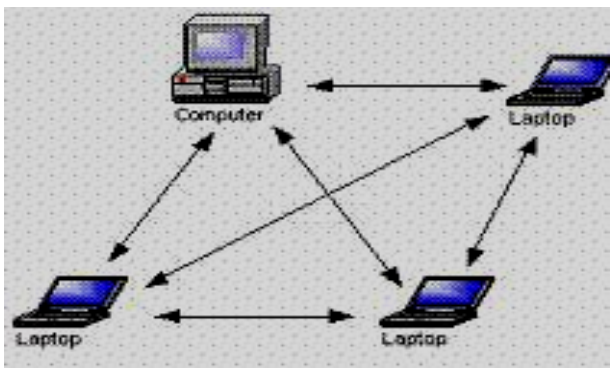
Οι κεραίες διπλής κατεύθυνσης εκπέμπουν προς δύο αντίθετες διευθύνσεις στον οριζόντιο άξονα, σε γωνίες 60 έως 120 μοίρες. Συνήθως χρησιμοποιούνται για την κάλυψη ενός αυτοκινητόδρομου ή ενός διαδρόμου. Οι κεραίες διπλής κατεύθυνσης έχουν μεγαλύτερη ενίσχυση του σήματος σε σχέση με τις μη κατευθυντικές.

ΕΙΚΟΝΑ 6: ΚΕΡΑΙΑ ΔΙΠΛΗΣ ΚΑΤΕΥΘΥΝΣΗΣ

## 1.8 ΤΟΠΟΛΟΓΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Η βασική δομική μονάδα ενός 802.11 δικτύου είναι το Basic Service Set (BSS) και αποτελείται από μία ομάδα σταθμών οι οποίοι επικοινωνούν μεταξύ τους. Τα όρια του Basic Service Set καθορίζονται από την περιοχή ραδιοκάλυψης, η οποία ονομάζεται Basic Service Area (BSA). Ένας σταθμός που ανήκει σε ένα Basic Service Set μπορεί να επικοινωνεί με οποιονδήποτε άλλο σταθμό στο ίδιο Basic Service Set, αλλά δεν μπορεί να επικοινωνήσει άμεσα με άλλα. Οι δύο βασικές τοπολογίες είναι τα Ανεξάρτητα Δίκτυα (Independent Networks) και τα Δίκτυα Υποδομής (Infrastructure Networks). [6]

### 1.8.1 Ανεξάρτητα Δίκτυα (Independent Networks)




ΕΙΚΟΝΑ 7: ΑΝΕΞΑΡΤΗΤΑ ΔΙΚΤΥΑ

Σε ένα Independent δίκτυο, οι σταθμοί μπορούν να επικοινωνούν άμεσα μεταξύ τους από τη στιγμή που βρίσκονται εντός της εμβέλειας του δικτύου. Το BSS στην τοπολογία αυτή ονομάζεται και IBSS (Independent BSS) ή ad-hoc BSS ή απλά ad-hoc δίκτυο. [5][7]

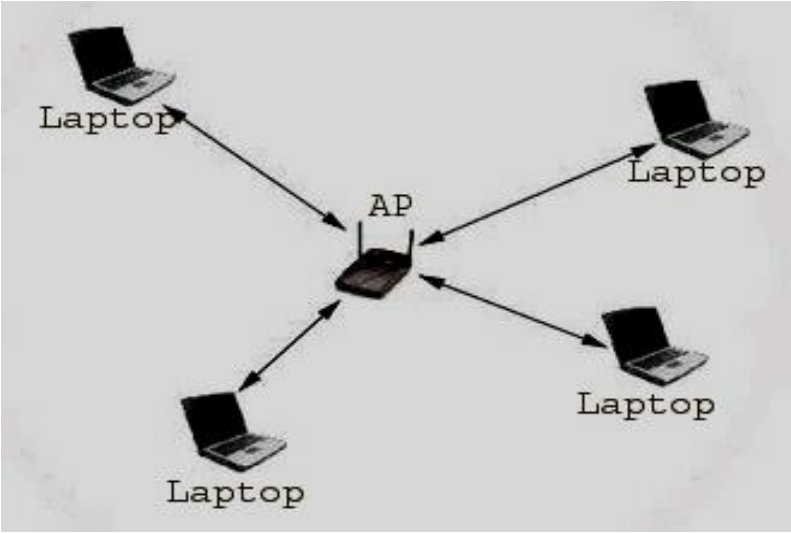
Όλοι οι σταθμοί που βρίσκονται στο δίκτυο είναι ισότιμοι. Ένα Independent δίκτυο αποτελείται από δύο ή περισσότερους σταθμούς, όμως ο αριθμός των σταθμών είναι σχετικά μικρός. Τα Independent δίκτυα είναι τα απλούστερα και συνήθως χρησιμοποιούνται για μικρό χρονικό διάστημα, για προσωρινές συνδέσεις, δηλαδή συνδέσεις για κάποιον συγκεκριμένο σκοπό. Παραδείγματος χάριν, μπορεί να δημιουργηθεί ένα τέτοιο δίκτυο για να εξυπηρετήσει μία τηλεδιάσκεψη. Αυτού του τύπου τα δίκτυα έχουν μεγάλο ερευνητικό ενδιαφέρον, καθώς περιέχονται πολλά μονοπάτια για την επικοινωνία μεταξύ των σταθμών και έτσι παρέχει μεγάλη ευελιξία, αξιοπιστία λόγω εφεδρείας μονοπατιών, αλλά και αυξημένη ταχύτητα. [6]

Τα κυριότερα χαρακτηριστικά αυτής της τοπολογίας είναι τα ακόλουθα:

- **Κατανεμημένη λειτουργία.** Στα Independent δίκτυα δεν υπάρχει κάποια κεντρική οντότητα η οποία να ελέγχει το δίκτυο με αποτέλεσμα κάθε σταθμός να έχει τις ίδιες δυνατότητες αλλά και τις ίδιες ευθύνες. Όλα τα πρωτόκολλα του δικτύου λειτουργούν κατανεμημένα.
- **Δυναμική τοπολογία.** Σε ένα Independent δίκτυα κάθε σταθμός μπορεί να μετακινηθεί ελεύθερα.
- **Πολύοδη επικοινωνία (Multihop).** Λόγω της εξασθένησης στο ασύρματο μέσο, αλλά και της πεπερασμένης εμβέλειας των πομπών, ένα Independent δίκτυο δεν μπορεί να θεωρηθεί ότι έχει μία πλήρως συνδεδεμένη τοπολογία. Έτσι, αν ένας σταθμός θέλει να μεταδώσει δεδομένα σε έναν σταθμό εκτός τις εμβέλειας του, τότε θα πρέπει να υλοποιηθεί η μετάδοση διαμέσου άλλων σταθμών. Τα δίκτυα αυτά είναι γνωστά και ως δίκτυα αποθήκευσης και προώθησης.
- **Μεταβαλλόμενη ποιότητα συνδέσεων.** Το φαινόμενο αυτό παρατηρείται σε δίκτυα αποθήκευσης και προώθησης επειδή η ποιότητα αυτής της σύνδεσης εξαρτάται από την ποιότητα κάθε επιμέρους σύνδεσης από την οποία αποτελείται.

- **Εξάρτηση από τη διάρκεια της μπαταρίας.** Σε ένα Independent δίκτυο, η απόδοσή του εξαρτάται από όλους τους σταθμούς του δικτύου. Ο τερματισμός της λειτουργίας έστω και ενός σταθμού οδηγεί σε μείωση της συνολικής απόδοσης, επειδή λιγοστεύουν οι σταθμοί για την προώθηση των μηνυμάτων, με αποτέλεσμα να μειώνεται η ικανότητα δρομολόγησης του δικτύου.

### 1.8.2 Δίκτυα Υποδομής (Infrastructure Networks)




**ΕΙΚΟΝΑ 8: ΔΙΚΤΥΑ ΥΠΟΔΟΜΗΣ**

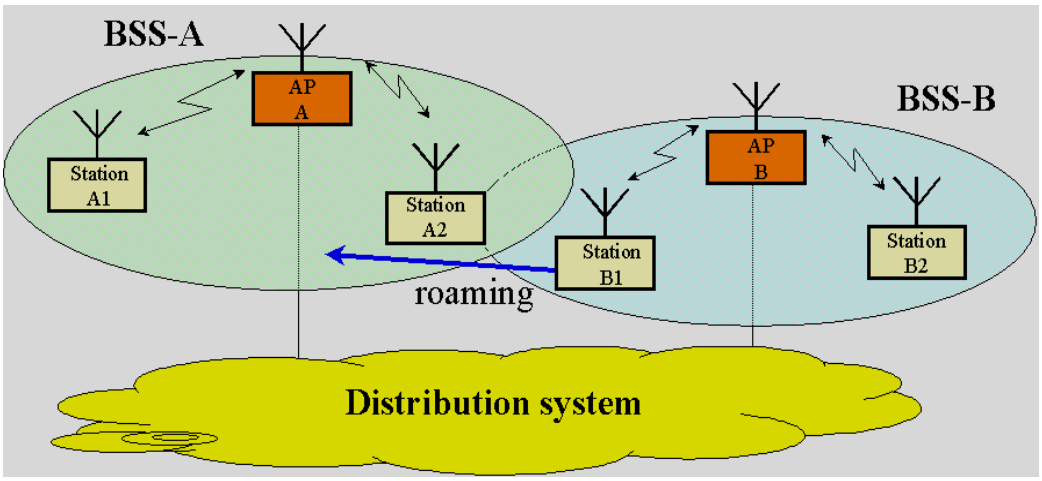
Στο παραπάνω σχήμα παρουσιάζονται τα δίκτυα υποδομής. Αυτού του τύπου τα δίκτυα διακρίνονται εξαιτίας της χρήσης ενός σημείου πρόσβασης (Access Point – AP). Το AP είναι μια συσκευή εξοπλισμένη με θύρα Ethernet και λειτουργεί παρόμοια με ένα Hub και είναι υπεύθυνο για την ανταλλαγή των πλαισίων μεταξύ των σταθμών και γενικότερα για τον κεντρικό έλεγχο της λειτουργίας του δικτύου.

Η προσθήκη του AP αλλάζει τον τρόπο ανταλλαγής των πλαισίων μεταξύ των σταθμών. Αντίθετα, με ένα Independent δίκτυο, όπου οι σταθμοί επικοινωνούν μεταξύ τους, σε ένα Infrastructure δίκτυο η επικοινωνία πραγματοποιείται μέσω του AP, λειτουργεί δηλαδή σαν διαμεσολαβητής. Έτσι, αν ένας σταθμός επιθυμεί να στείλει ένα πλαίσιο σε έναν άλλο σταθμό, αρχικά το πλαίσιο μεταφέρεται στο AP και αυτό με τη σειρά του το στέλνει στον τελικό προορισμό του.

Επίσης, σε αντίθεση με το Independent δίκτυο όπου όλοι οι σταθμοί πρέπει να βρίσκονται εντός της εμβέλειας του δικτύου για να μπορούν να επικοινωνούν μεταξύ τους, στο δίκτυο υποδομής δεν χρειάζεται οι σταθμοί να βρίσκονται ο ένας

εντός της εμβέλειας των άλλων, αλλά αρκεί οι σταθμοί να βρίσκονται εντός της εμβέλειας του AP. Επιπλέον, για να συμμετέχει ένας σταθμός σε ένα τέτοιο δίκτυο, θα πρέπει να υποστηρίζει την υπηρεσία Association (Σύνδεση), η οποία θα αναλυθεί σε επόμενο κεφάλαιο. Το 802.11 δεν ορίζει κάποιο όριο σχετικά με τον αριθμό των σταθμών οι οποίοι μπορούν να είναι συνδεδεμένοι σε ένα δίκτυο, αλλά τίθενται κάποιοι περιορισμοί στις διάφορες υλοποιήσεις AP.

Στην περίπτωση των δικτύων υποδομής ένας αριθμός από BSSs μπορούν να συνδεθούν και να αποτελέσουν ένα Extended Service Set (ESS). Το ESS δημιουργείται ενώνοντας τα APs των BSSs μέσω ενός δικτύου κορμού, το οποίο ονομάζεται Σύστημα Διανομής (Distribution System), όπως φαίνεται και στο σχήμα που ακολουθεί. [5][6][7]

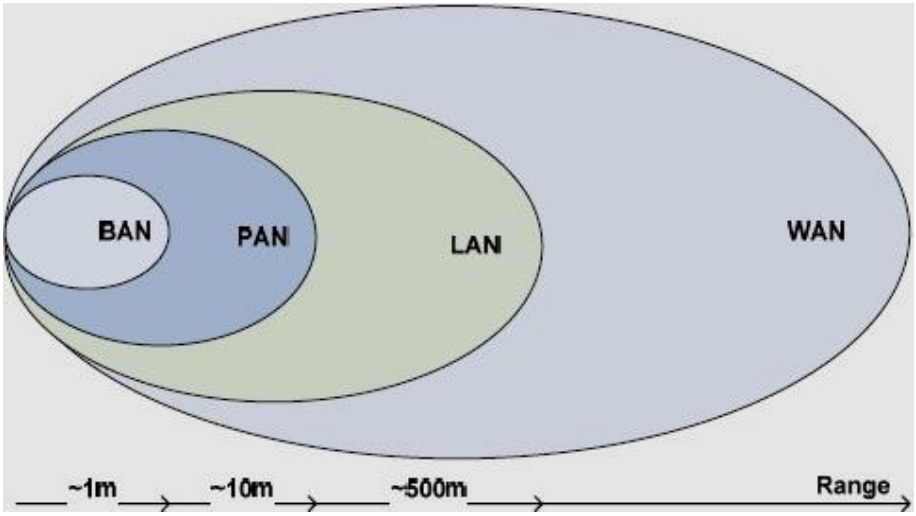



ΕΙΚΟΝΑ 9: ΣΥΣΤΗΜΑ ΔΙΑΝΟΜΗΣ

Το σύστημα διανομής δίνει τη δυνατότητα επικοινωνίας σε δύο σταθμούς που βρίσκονται σε διαφορετικά BSS αλλά βρίσκονται εντός της εμβέλειας του ESS και τα AP λειτουργούν ως γέφυρες.

## 1.9 ΚΑΤΗΓΟΡΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Τα ασύρματα δίκτυα χωρίζονται σε πέντε κατηγορίες ανάλογα με τη γεωγραφική τους έκταση. Συγκεκριμένα αυτά χωρίζονται σε ασύρματα δίκτυα περιοχής σώματος, σε ασύρματα προσωπικά δίκτυα, σε ασύρματα τοπικά δίκτυα, σε ασύρματα μητροπολιτικά δίκτυα και σε ασύρματα δίκτυα ευρείας περιοχής. Στην επόμενη εικόνα φαίνεται η ταξινόμηση των δικτύων ανάλογα με την απόσταση που υπάρχει ανάμεσα στους σταθμούς.




**ΕΙΚΟΝΑ 10: ΚΑΤΗΓΟΡΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ**

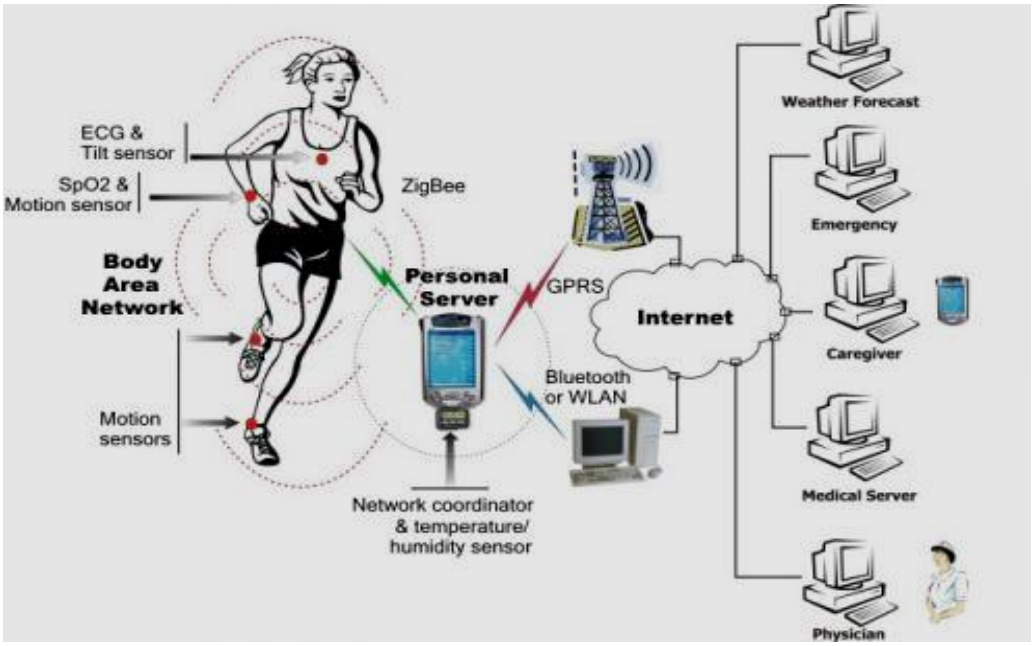
### 1.9.1 Ασύρματα Δίκτυα Περιοχής Σώματος (Wireless Body Area Network – WBAN)

Τα ασύρματα δίκτυα περιοχής σώματος αναφέρονται στην ασύρματη επικοινωνία μεταξύ διάφορων αντικειμένων τα οποία εμφυτεύονται ή τοποθετούνται επάνω στο σώμα ή τα ρούχα ενός ανθρώπου, όπως για παράδειγμα ακουστικά, μικρόφωνα και αισθητήρες, και επιβλέπουν διάφορες ζωτικές λειτουργίες του ανθρώπινου οργανισμού ή μετρούν διάφορους δείκτες υγείας. Οι αισθητήρες, χρησιμοποιώντας τεχνολογίες ασύρματων δικτύων, αποστέλλουν σε πραγματικό χρόνο τα δεδομένα σε ένα κοντινό σημείο κι από εκεί αποστέλλονται σε ένα κέντρο υγείας. Το πρωτόκολλο IEEE 802.15.6 προορίζεται για τα ασύρματα δίκτυα περιοχής σώματος (IEEE 802.15 TG6 2007).

Τα ασύρματα δίκτυα περιοχής σώματος έχουν διάφορες εφαρμογές στους τομείς της ιατρικής, της επιχείρησης ακόμα και στον τομέα της ψυχαγωγίας. Στην ιατρική χρησιμοποιούνται για τη μετάδοση σωματικών παραμέτρων όπως η πίεση του αίματος, ο σφυγμός της καρδιάς και η θερμοκρασία του σώματος. Στην επιχείρηση χρησιμοποιούνται συνήθως για τον έλεγχο της ταυτότητας των εργαζομένων. Τέλος, μπορούν να εφαρμοστούν τέτοια δίκτυα για την ακρόαση μουσικής, για την παρακολούθηση μωρών και ως οδηγοί πόλης.

Στα χαρακτηριστικά αυτών των δικτύων περιλαμβάνονται: η μετάδοση χωρίς παρεμβολές, η ελευθερία χρήσης του παγκοσμίως, η χαμηλή ισχύς μετάδοσης, η χαμηλή πολυπλοκότητα και ο πολύ μικρός όγκος του υλικού μέρους. Ο ρυθμός

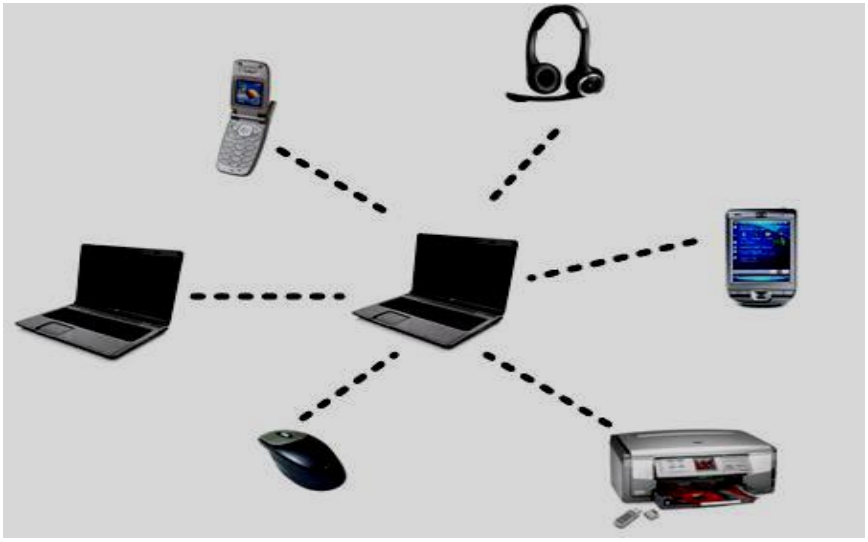
μετάδοσης των δεδομένων φτάνει τα 120 Kbit / s. Η ακτίνα μετάδοσης ενός BAN αντιστοιχεί στην έκταση του ανθρώπινου σώματος, περίπου 1 – 2 μέτρα. [2][3]




**ΕΙΚΟΝΑ 11: ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΠΕΡΙΟΧΗΣ ΣΩΜΑΤΟΣ [2]**

### 1.9.2 Ασύρματα Προσωπικά Δίκτυα (Wireless Personal Area Network – WPAN)

Τα ασύρματα προσωπικά δίκτυα είναι από τα μικρότερα που υπάρχουν από γεωγραφικής απόψεως. Καλύπτουν απόσταση μέχρι δέκα μέτρων γι' αυτό και χρησιμοποιούνται σε εφαρμογές που χρειάζονται μικρή εμβέλεια. Τα ασύρματα προσωπικά δίκτυα συνήθως χρησιμοποιούνται για να διασυνδέουν έναν προσωπικό υπολογιστή με τα διάφορα περιφερειακά του, όπως πληκτρολόγιο, ποντίκι, εκτυπωτή, scanner, αλλά και άλλες συσκευές, όπως φωτογραφικές μηχανές, φαξ, κινητά τηλέφωνα και πολλές ακόμα συσκευές.[7][8]



**ΕΙΚΟΝΑ 12: ΑΣΥΡΜΑΤΑ ΠΡΟΣΩΠΙΚΑ ΔΙΚΤΥΑ**

Στη σημερινή εποχή, το πρότυπο με τη μεγαλύτερη αποδοχή, για τη δημιουργία ασύρματων προσωπικών δικτύων, είναι το Bluetooth. [7] Αρχικά, αναπτύχθηκε από την Ericsson το 1994 με στόχο τη δημιουργία των λεγόμενων hands – free. Λειτουργεί στην περιοχή των συχνοτήτων ISM των 2,4 GHz και υποστηρίζει κανάλια φωνής των 64 kbps, ενώ ασύγχρονα κανάλια δεδομένων μέχρι 721 kbps. Μία ακόμα τεχνολογία, είναι οι υπέρυθρες. Κεντρική ιδέα των υπερύθρων είναι η ασύρματη επικοινωνία δύο συσκευών, έχοντας όμως μεταξύ τους οπτική επαφή. Οι συσκευές θα πρέπει να έχουν μεταξύ τους απόσταση μέχρι ένα μέτρο και η ταχύτητα είναι από 9600 bps έως 4 Mbps. Ένα ακόμα πρότυπο είναι το λεγόμενο HomeRF το οποίο πρωτοκυκλοφόρησε το 1998, ενώ η πιο πρόσφατη έκδοση κυκλοφόρησε το 2001 με κανάλια φωνής των 32 kbps και ταχύτητες μετάδοσης των 10 Mbps. Όπως το Bluetooth, έτσι και το HomeRF λειτουργεί στη συχνότητα ISM των 2,4 GHz και έχει εμβέλεια περίπου 50 μέτρα. Τέλος, ένα ακόμα πρότυπο το οποίο δημιουργήθηκε το 1999, είναι το IEEE 802.15.1 (IEEE 802.15.1 TG1a 2005), όπου στόχος της ομάδας 802.15 είναι να επιτύχει τη διαλειτουργικότητα των δύο προηγούμενων προτύπων, τα οποία προηγήθηκαν (Πηγή: Ασύρματα Δίκτυα, Εκδόσεις Κλειδάριθμος). Τα πρότυπα που αναφέρθηκαν παραπάνω θα αναλυθούν σε επόμενο κεφάλαιο. Στον πίνακα που ακολουθεί φαίνονται τρία πρότυπα ασύρματων προσωπικών δικτύων και οι βασικές ιδιότητές τους.

**ΠΙΝΑΚΑΣ 1: ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ ΤΡΙΩΝ ΑΣΥΡΜΑΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΙΚΤΥΩΝ**

| STANDARD | FREQUENCY | BANDWIDTH | OPTIMUM OPERATING RANGE |
|---|---|---|---|
| IrDA | 875nm wavelength | 9600 bps to 4 Mbps. Future of 15 Mbps | 1-2 meters (3–6 feet) |
| Bluetooth | 2.4 GHz | v1.1: 720 Kbps;<br>v2.0: 10 Mbps | 10 meters (30 feet) to 100 meters (300 feet) |
| IEEE 802.15 | 2.4 GHz | 802.15.1: 1 Mbps<br>802.15.3: 20-plus Mbps | 10 meters (30 feet) to 100 meters (300 feet) |

### 1.9.3 Ασύρματα Τοπικά Δίκτυα (Wireless Local Area Net - WLAN)

Τα ασύρματα τοπικά δίκτυα (Wireless Local Area Network), τα οποία είναι γνωστά ως WLAN, είναι ιδιωτικά δίκτυα τα οποία επεκτείνονται μέσα σε ένα κτήριο ή σε ένα συγκρότημα κτηρίων, για παράδειγμα ένα σχολείο ή ένα αεροδρόμιο, σε ένα εργοστάσιο και γενικά σε μία έκταση μερικών εκατοντάδων μέτρων. Συνήθως, η ακτίνα επικοινωνίας αυτών των δικτύων είναι 100 – 500 μέτρα. Τα ασύρματα τοπικά δίκτυα χρησιμοποιούνται στους προσωπικούς υπολογιστές, σε γραφεία, εταιρείες και γενικά σε χώρους εργασίας με σκοπό την ανταλλαγή πληροφοριών και την κοινή χρήση αρχείων, δεδομένων και συσκευών. [7][8]


**ΕΙΚΟΝΑ 13: ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ**

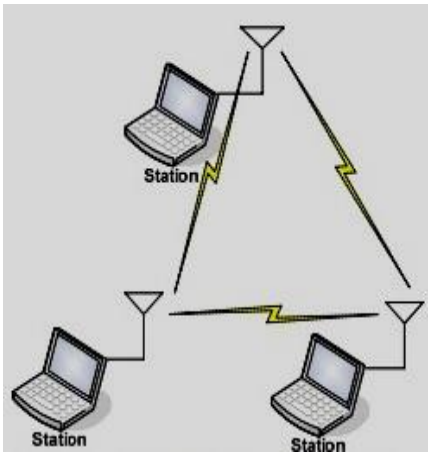
Τρία χαρακτηριστικά κάνουν τα ασύρματα τοπικά δίκτυα να διαφέρουν από τα υπόλοιπα, το μέγεθός τους, η τεχνολογία μετάδοσης και η τοπολογία τους.

Η πρώτη προσπάθεια να καθοριστούν πρότυπα έγινε προς το τέλος της δεκαετίας του ’80 από την ομάδα εργασίας του 802.4 του ιδρύματος ηλεκτρολόγων και ηλεκτρονικών μηχανικών των ΗΠΑ, IEEE (Institute of Electrical and Electronics Engineers). Η ομάδα αυτή ήταν αρμόδια για την ανάπτυξη των ενσύρματων δικτύων που λειτουργούν με τη μέθοδο της μεταβίβασης σκυτάλης σε τοπολογία διαύλου. Η ομάδα αυτή, αποφάσισε ότι η μέθοδος αυτή δεν ήταν αποδοτική για τη ρύθμιση της πρόσβασης σε ασύρματο δίκτυο, έτσι αποφάσισε να προτείνει τη δημιουργία νέων προτύπων. Το IEEE αποφάσισε τη δημιουργία της ομάδας 802.11. Τα πρώτα πρότυπα προσέφεραν ταχύτητες έως 2 Mbps με τη χρήση μετάδοσης μέσω ραδιοκυμάτων στις περιοχές συχνοτήτων ISM ή μέσω υπέρυθρης ακτινοβολίας. Η ανάλυση των προτύπων της ομάδας 802.11 θα γίνει σε επόμενο κεφάλαιο. Στο παρακάτω πίνακα φαίνονται κάποια από τα γνωστά πρότυπα για τα τοπικά δίκτυα και οι βασικές ιδιότητες τους. (Πηγή: www.rfidc.com)

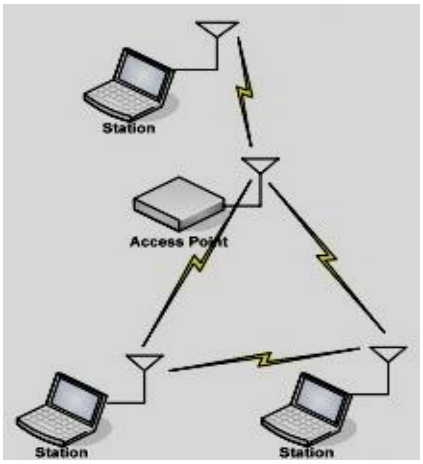
**ΠΙΝΑΚΑΣ 2: ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ ΓΝΩΣΤΩΝ ΠΡΟΤΥΠΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ**

| Protocol | Release Date | Op. Frequency | Data Rate (Typical) | Data Rate (Max) | Range (Indoor) |
|---|---|---|---|---|---|
| Legacy | 1997 | 2.4 -2.5 GHz | 1 Mbit/s | 2 Mbit/s | ? |
| 802.11a | 1999 | 5.15-5.35/5.47-5.725 /5.725-5.875 GHz | 25 Mbit/s | 54 Mbit/s | ~30 meters (~100 feet) |
| 802.11b | 1999 | 2.4-2.5 GHz | 6.5 Mbit/s | 11 Mbit/s | ~50 meters (~150 feet) |
| 802.11g | 2003 | 2.4-2.5 GHz | 11 Mbit/s | 54 Mbit/s | ~30 meters (~100 feet) |
| 802.11n | 2006 (draft) | 2.4 GHz or 5 GHz bands | 200 Mbit/s | 540 Mbit/s | ~50 meters (~160 feet) |

Τα ασύρματα τοπικά δίκτυα χωρίζονται σε δύο κατηγορίες ανάλογα με τον τρόπο σύνδεσης των σταθμών. Έτσι, ένα δίκτυο μπορεί να ρυθμιστεί ως peer – to – peer, γνωστό και ως ad hoc δίκτυο, ή με access point, ακόμα και με συνδυασμό αυτών. Στην peer – to – peer, οι σταθμοί συνδέονται μεταξύ τους ανά δύο, χωρίς να απαιτείται κάποιος κεντρικός έλεγχος, αλλά συνεργάζονται δυναμικά οι σταθμοί μεταξύ τους για την επίτευξη των διαφόρων δικτυακών λειτουργιών. Με τη χρήση access point οργανώνεται καλύτερα η δομή του δικτύου, και όλες οι επικοινωνίες γίνονται μέσω του access point.



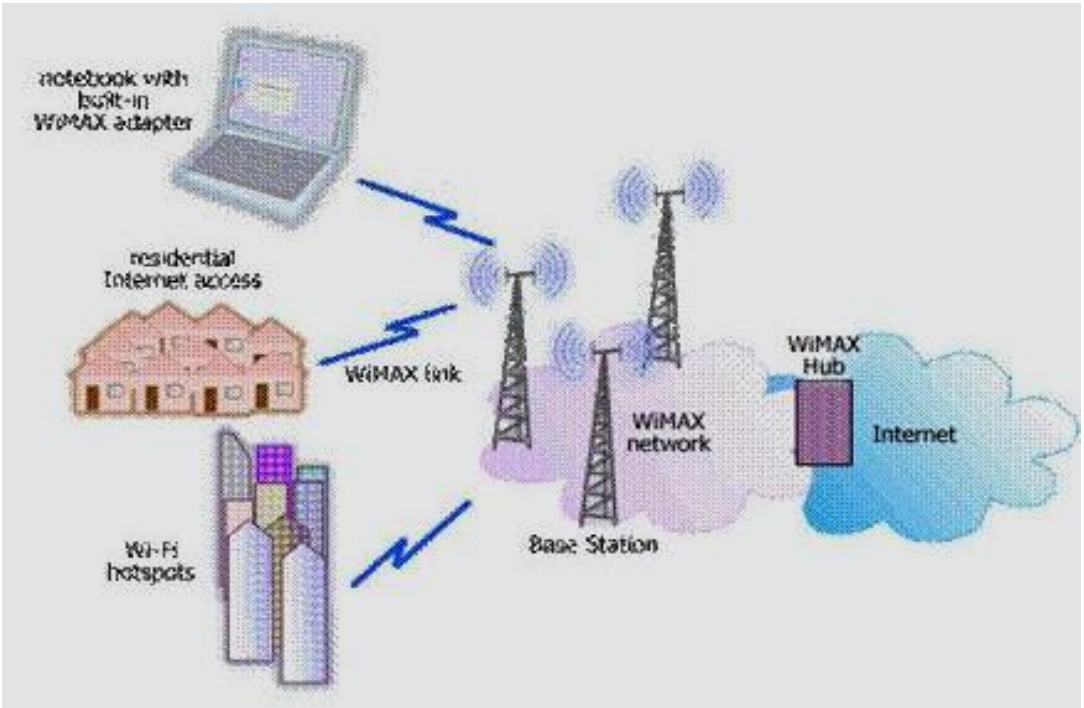

**ΕΙΚΟΝΑ 14: ΔΙΚΤΥΟ AD HOC**




**Εικόνα 15: ΔΙΚΤΥΟ ΜΕ ACCESS POINT**

## 1.9.4 Ασύρματα Μητροπολιτικά Δίκτυα (Wireless Metropolitan Area Network - WMAN)

Τα ασύρματα μητροπολιτικά δίκτυα αποτελούν την ενδιάμεση κατηγορία ανάμεσα στα ασύρματα τοπικά δίκτυα και στα ασύρματα δίκτυα ευρείας περιοχής και εκτείνονται σε έκταση μίας πόλης ή μερικών χιλιομέτρων.

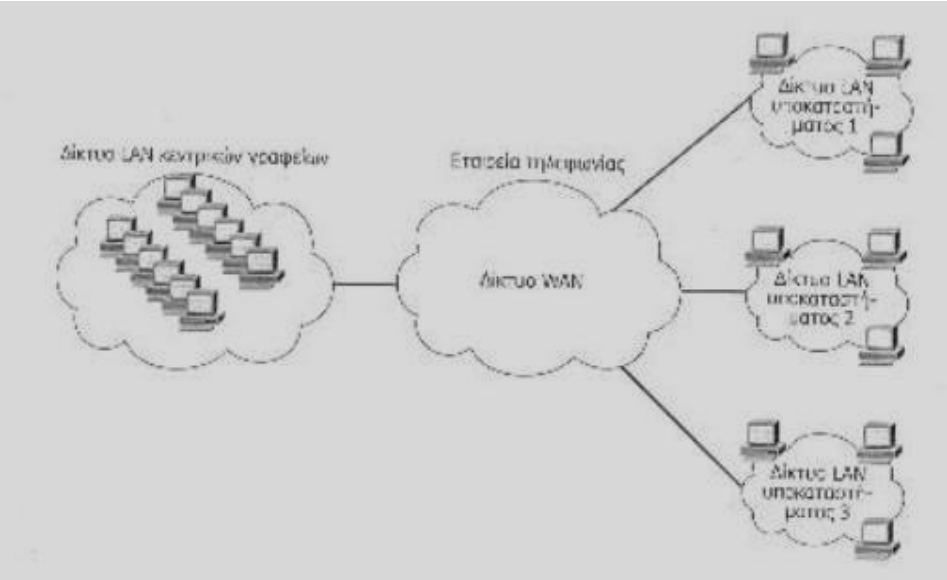



**ΕΙΚΟΝΑ 16: ΑΣΥΡΜΑΤΑ ΜΗΤΡΟΠΟΛΙΤΙΚΑ ΔΙΚΤΥΑ**


Αντιπροσωπευτικό πρότυπο αυτής της κατηγορίας είναι το WiMax ή IEEE 802.16, όπως είναι επίσης γνωστό, το οποίο δημιουργήθηκε από την ομάδα εργασίας IEEE το 2001. Το πρότυπο IEEE 802.16 εκτείνεται στη ζώνη των συχνοτήτων 2 – 66 GHz με μέγιστη απόσταση τα 50 km για τα ασύρματα δίκτυα, ενώ τα 15 km για τα δίκτυα κινητής τηλεφωνίας. Η ταχύτητα μετάδοσης των δεδομένων φτάνει τα 72 Mbps, το εύρος μετάδοσης εκτείνεται από 1,25 έως 20 MHz και χρησιμοποιεί τη διαμόρφωση OFDM. Αναλυτικότερα για το WiMax, θα διαβάσετε στο έβδομο κεφάλαιο. Τα WMAN δίκτυα στη Βόρεια Αμερική χρησιμοποιούν το πρωτόκολλο IEEE 802.16 (WiMAX), ενώ στη Νότια Κορέα το Wi – Bro.

### 1.9.5 Ασύρματα Δίκτυα Ευρείας Περιοχής (Wireless Wide Area Network – WWAN)

Τα ασύρματα δίκτυα ευρείας περιοχής εκτείνονται σε μία μεγάλη γεωγραφική περιοχή, όπως μία χώρα ή μία ήπειρος και είναι ευρέως διαδεδομένα στην κινητή τηλεφωνία και παρέχουν τη δυνατότητα μεταφοράς δεδομένων. Τα ασύρματα δίκτυα ευρείας περιοχής αποτελούνται από συνδεδεμένα WLAN και WMAN με αποτέλεσμα να δημιουργείται ένα διαδίκτυο. Το μεγαλύτερο διαδίκτυο είναι το Internet. Η διασύνδεση των δικτύων γίνεται μέσω τηλεπικοινωνιακών κυκλωμάτων και συσκευών μεταγωγής, όπως οι δρομολογητές (routers). Τα WWAN χρησιμοποιούν τις τεχνολογίες 2.5G, 3G και την τεχνολογία επόμενης γενιάς 4G.



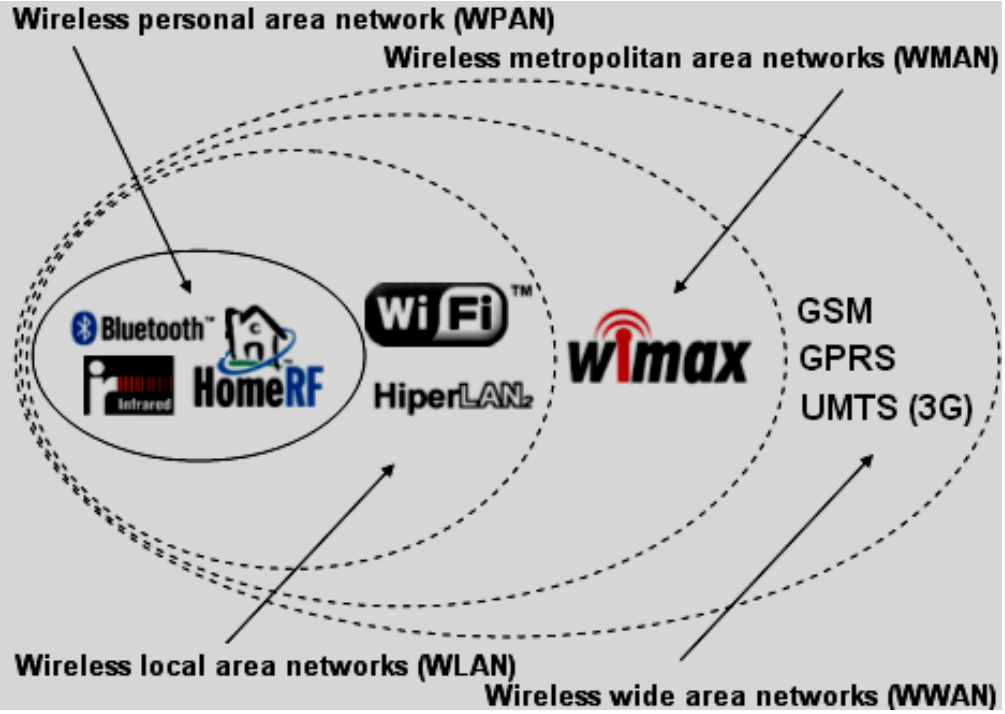

**ΕΙΚΟΝΑ 17: ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΕΥΡΕΙΑΣ ΠΕΡΙΟΧΗΣ**

Τα ασύρματα δίκτυα ευρείας περιοχής υλοποιούνται βάση δύο τεχνολογιών, με μεταγωγή κυκλώματος (circuit switching) και με μεταγωγή πακέτου (packet switching). Σε ένα δίκτυο μεταγωγής κυκλώματος δημιουργείται μία αποκλειστική διαδρομή ανάμεσα στον αποστολέα και στον παραλήπτη για τη μετάδοση ενός μηνύματος όσο το δυνατόν πιο γρήγορα. Η διαδρομή αυτή αποτελείται από φυσικές συνδέσεις ανάμεσα στους κόμβους του δικτύου. Προκειμένου να πραγματοποιηθεί η μεταφορά των δεδομένων εκτελούνται τρεις διαδικασίες. Πρώτα γίνεται δέσμευση του κυκλώματος, ακολουθεί η μεταφορά των δεδομένων και τέλος γίνεται αποδέσμευση του κυκλώματος. Η μεταγωγή κυκλώματος είναι χρήσιμη για ισόχρονα δεδομένα, όπως αυτά των φωνητικών κλήσεων. Αυτό έχει ως αποτέλεσμα το τηλεφωνικό δίκτυο να αποτελεί το πιο γνωστό δίκτυο μεταγωγής κυκλώματος. Αντίθετα, στην περίπτωση που θέλετε να μεταφέρετε δεδομένα, το κανάλι είναι αποδοτικό με τη μεταγωγή κυκλώματος μόνο όταν γίνεται συνεχή μεταφορά δεδομένων, αλλιώς το κανάλι παραμένει αχρησιμοποίητο για μεγάλα χρονικά διαστήματα. Τη λύση στο πρόβλημα αυτό δίνει η χρήση μεταγωγής πακέτων. [1][5]

Σε ένα δίκτυο μεταγωγής πακέτων, το μήνυμα σπάει σε μικρότερα κομμάτια, τα πακέτα, τα οποία είναι αριθμημένα και εκτός από τα δεδομένα που έχουν, περιέχουν και πληροφορία ελέγχου. Δηλαδή, κάθε πακέτο περιέχει και μία επικεφαλίδα στην οποία περιλαμβάνονται όλες οι απαραίτητες πληροφορίες έτσι ώστε να φτάσει το κάθε πακέτο στον προορισμό του. Κάθε πακέτο δρομολογείται

μέσω του δικτύου από κόμβο σε κόμβο από ένα μονοπάτι το οποίο φυσικά οδηγεί στον προορισμό. Κάθε πακέτο παραλαμβάνεται ολόκληρο, αποθηκεύεται και μετά αποστέλλεται στον κόμβο που οδηγεί όσο το δυνατόν πιο σύντομα στον παραλήπτη. Βέβαια, η διαδικασία αποθήκευσης και προώθησης των πακέτων δημιουργεί καθυστερήσεις. Όταν σε ένα δίκτυο μεταγωγής πακέτων παρουσιάζεται συμφόρηση, τα πακέτα συνεχίζουν να φτάνουν στον προορισμό τους, με μεγαλύτερες όμως καθυστερήσεις. Μόλις φτάσουν όλα τα πακέτα στον τελικό παραλήπτη, μπαίνουν στη σωστή θέση, στην περίπτωση όπου τα πακέτα ακολουθήσουν διαφορετικό μονοπάτι και φτάσουν στον παραλήπτη με διαφορετική σειρά, δηλαδή στη μεταγωγή πακέτων με χρήση datagram, για να δημιουργηθεί το αρχικό μήνυμα ολοκληρωμένο. [1][5]

Τα δίκτυα μεταγωγής πακέτων χωρίζονται σε δύο κατηγορίες, στα δίκτυα μεταγωγής πακέτων με χρήση datagram, όπου κάθε πακέτο δρομολογείται ανεξάρτητα από τα προηγούμενα και στα δίκτυα μεταγωγής πακέτων με χρήση εικονικών κυκλωμάτων (virtual circuit switching), όπου όλα τα πακέτα ακολουθούν το ίδιο μονοπάτι, το οποίο είχε εξασφαλισθεί πριν την έναρξη της επικοινωνίας μεταξύ πομπού και δέκτη. [1][5][6][7]




ΕΙΚΟΝΑ 18: ΚΑΤΗΓΟΡΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

## 1. 10 ΣΥΝΟΨΗ

Στο παρόν κεφάλαιο πραγματοποιήθηκε η εισαγωγή του αναγνώστη της παρούσας πτυχιακής εργασίας στην έννοια των ασύρματων δικτύων. Αρχικά, έγινε μια ιστορική αναδρομή, στη συνέχεια ανάλυση των ασύρματων δικτύων και των τμημάτων τους και τέλος των κατηγοριών των ασύρματων δικτύων. Στο επόμενο κεφάλαιο γίνεται ανάλυση των γενεών των ασύρματων δικτύων.

# 2. ΓΕΝΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

## 2. 1 ΕΙΣΑΓΩΓΗ

Στη σημερινή εποχή, η τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς. Οι απαιτήσεις των χρηστών ολοένα και αυξάνονται. Μέρος σε αυτήν την εξέλιξη ήταν και τα ασύρματα δίκτυα, τα οποία από την εποχή που πρωτοεμφανίστηκαν μέχρι σήμερα, δημιουργήθηκαν τρεις γενιές κυψελικών δικτύων ενώ η τέταρτη γενιά έχει ήδη ξεκινήσει. Έτσι, υπάρχουν τα κυψελικά δίκτυα πρώτης γενιάς, τα κυψελικά δίκτυα δεύτερης γενιάς, τα κυψελικά δίκτυα 2.5 γενιάς, τα κυψελικά δίκτυα τρίτης γενιάς και τέλος τα κυψελικά δίκτυα τέταρτης γενιάς τα οποία βρίσκονται υπό εξέλιξη. Τα δίκτυα αυτά βελτίωσαν τις ασύρματες επικοινωνίες, αφού προσέφεραν χρήση περισσότερων καναλιών, επικάλυψη ραδιοσυχνοτήτων, ενώ πομποί και δέκτες χρειάζονταν πλέον λιγότερη ισχύ για τη λειτουργία τους, κάτι που σήμαινε μικρότερο κόστος, βάρος και μέγεθος, καθώς και λιγότερες παρεμβολές.

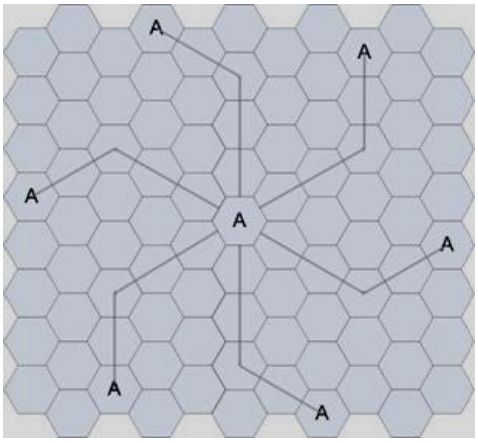
Όμως, πριν ξεκινήσει η ανάλυση των γενιών των ασύρματων κυψελικών δικτύων, πρέπει πρώτα να αναλυθεί η έννοια της κυψέλης, στην οποία βασίζεται και η ονομασία των δικτύων αυτών ως κυψελικών. Η βασική ιδέα πίσω από τα κυψελικά δίκτυα είναι η διαίρεση της γεωγραφικής περιοχής που καλύπτει το δίκτυο σε μικρότερες περιοχές, οι οποίες ονομάζονται κυψέλες (cells). Η ουσία αυτού του διαμοιρασμού είναι η χρήση πολλών πομπών χαμηλής ισχύος, της τάξης των 100W ή και λιγότερο. Η μορφή τους εξαρτάται από τη μορφολογία του εδάφους, αλλά για υπολογιστικούς λόγους έχει υιοθετηθεί η αναπαράσταση της κυψέλης με εξάγωνο. Θα μπορούσε να θεωρηθεί ως καταλληλότερο σχήμα ο κύκλος, όμως με αυτόν τον τρόπο θα δημιουργόντουσαν περιοχές με επικάλυψη, ακόμα και περιοχές χωρίς κάλυψη. Ένα ακόμα στοιχείο που κάνει το εξάγωνο καταλληλότερο για την αναπαράσταση των κυψελικών δικτύων είναι ότι οι κεραίες ισαπέχουν μεταξύ τους. Οι χρήστες που βρίσκονται μέσα σε μια κυψέλη εξυπηρετούνται από ένα σταθμό βάσης, που αποτελείται από κεραίες εκπομπής και λήψης. Κάθε κυψέλη χρησιμοποιεί ένα σύνολο συχνοτήτων, τις οποίες μπορούν να χρησιμοποιούν και άλλες κυψέλες αλλά όχι οι γειτονικές τους. Η απόσταση μεταξύ των δύο κυψελών πρέπει να είναι τέτοια ώστε να μην επηρεάζει η μία την άλλη. Με αυτόν τον τρόπο επιτυγχάνεται το ίδιο σύνολο συχνοτήτων να χρησιμοποιείται ταυτόχρονα σε πολλές κυψέλες. Με τη χρήση πολλών και μικρών

κυψελών, καθώς επίσης και πολλών λιγότερο ισχυρών σταθμών βάσης, επιτυγχάνεται μεγαλύτερη επαναχρησιμοποίηση και αξιοποίηση των συχνοτήτων, με αποτέλεσμα τη μεγαλύτερη πυκνότητα χρηστών. Το μέγεθος μιας κυψέλης εξαρτάται από τον αριθμό των χρηστών και καθορίζεται είτε από μετρήσεις πεδίου είτε από μοντέλα διάδοσης ραδιοκυμάτων. Επειδή κάθε σταθμός βάσης μπορεί να εξυπηρετήσει ταυτόχρονα μικρό αριθμό χρηστών, οι κυψέλες είναι σχετικά μικρές σε μία πόλη και μεγαλύτερες σε αγροτικές περιοχές. [1][2][4]

Μια ομάδα από γειτονικές κυψέλες ονομάζεται συστάδα. Σε μία συστάδα, οι κυψέλες που την αποτελούν, δεν κάνουν χρήση όμοιων συχνοτήτων. Η τιμή του μεγέθους μιας συστάδας *N* είναι συνάρτηση της στάθμης των παρεμβολών που μπορεί να ανεχθεί ο σταθμός βάσης ή το κινητό τηλέφωνο χωρίς η ποιότητα της επικοινωνίας να πέσει σε ανεπίτρεπτα επίπεδα. Από την οπτική γωνία της σχεδίασης συστημάτων είναι επιθυμητό να επιτύχουμε τη μεγαλύτερη δυνατή χωρητικότητα μειώνοντας το μέγεθος της συστάδας, αλλά ταυτόχρονα παρατηρείται αύξηση της στάθμης της συγκαναλικής παρεμβολής. Ο παράγοντας επαναχρησιμοποίησης συχνότητας (frequency reuse factor) ενός συστήματος κυψελωτής τηλεφωνίας ισούται με *1/N,* καθόσον εντός κάθε κυψέλης που ανήκει σε μια συστάδα μεγέθους *N* ο αριθμός των εκχωρηθέντων καναλιών είναι ίσος προς *1/N*. Ο αριθμός των κυψελών, *N*, σε κάθε συστάδα πρέπει να δίδεται από την σχέση: [4]

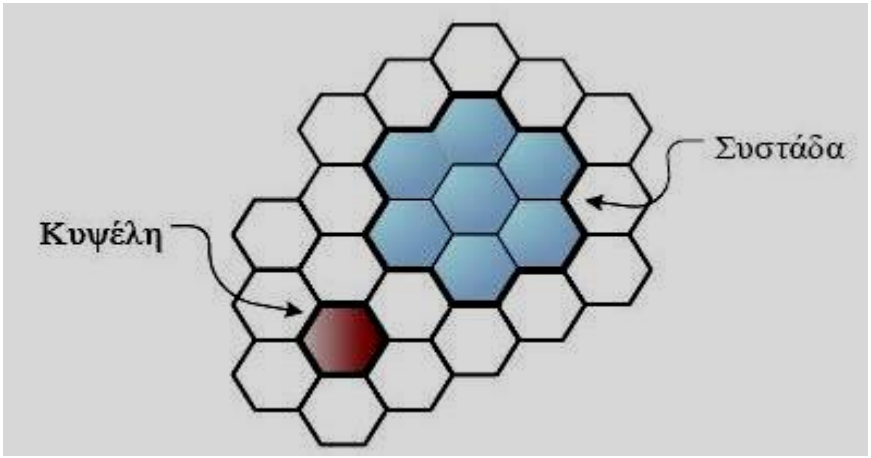
$$N = i^2 + j^2 + (ixj) \qquad [2][4]$$

όπου *i* και *j* είναι μη αρνητικοί ακέραιοι. Στα περισσότερα συστήματα το N λαμβάνει τιμές 4, 7 και 12. Για να προσδιοριστεί η πλησιέστερη συγκαναλική κυψέλη μιας συγκεκριμένης κυψέλης θα πρέπει να μετακινηθούμε *i* κυψέλες κατά μήκος οποιασδήποτε αλυσίδας εξαγώνων, κατόπιν να στρίψουμε εξήντα (60) μοίρες με φορά αντίθετη των δεικτών του ρολογιού και τέλος να μετακινηθούμε *j* κυψέλες κατά μήκος της νέας διεύθυνσης. Η τεχνική αυτή απεικονίζεται στο επόμενο σχήμα για το οποίο i=3, j=2 και N=19.




**ΕΙΚΟΝΑ 19: ΤΕΧΝΙΚΗ ΓΙΑ ΤΗΝ ΕΥΡΕΣΗ ΤΗΣ ΠΛΗΣΙΕΣΤΕΡΗΣ ΣΥΓΚΑΝΑΛΙΚΗΣ ΚΥΨΕΛΗΣ**

Στην εικόνα που ακολουθεί, παρουσιάζονται οι έννοιες της κυψέλης και της συστάδας.




**ΕΙΚΟΝΑ 20: ΑΝΑΠΑΡΑΣΤΑΣΗ ΤΗΣ ΕΝΝΟΙΑΣ ΤΗΣ ΚΥΨΕΛΗΣ ΚΑΙ ΤΗΣ ΣΥΣΤΑΔΑΣ**

## 2. 2 ΤΕΧΝΙΚΕΣ ΑΥΞΗΣΗΣ ΧΩΡΗΤΙΚΟΤΗΤΑΣ ΚΥΨΕΛΙΚΩΝ ΔΙΚΤΥΩΝ

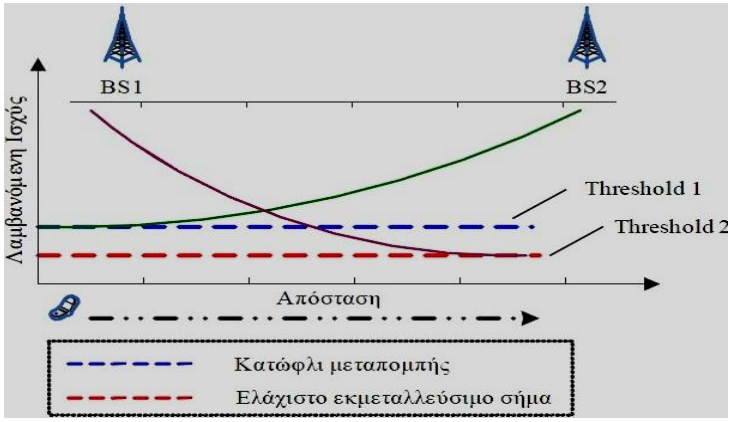
Η αυξημένη ζήτηση της χρήσης κινητών επικοινωνιών οδήγησε στην ανάγκη εύρεσης τρόπων αύξησης της χωρητικότητας των κυψελικών δικτύων, ώστε να μπορούν να εξυπηρετηθούν ακόμα περισσότεροι χρήστες.

Ο πρώτος τρόπος, και ο πιο ακριβός, είναι η αγορά επιπλέον ραδιοφωνικού φάσματος. Ο δεύτερος τρόπος είναι η αλλαγή στην αρχιτεκτονική του δικτύου. Αυτό μπορεί να πραγματοποιηθεί με χρήση κατευθυντικών κεραιών, αντί για μη κατευθυντικών, η τομεοποίηση των κυττάρων και με την υποδιαίρεση των κυττάρων σε άλλα μικρότερα. Ο τρίτος τρόπος είναι η επικάλυψη των κυττάρων, όπου οι συχνότητες που χρησιμοποιούνται μέσα σε ένα κύτταρο διαιρούνται σε αυτές που χρησιμοποιούνται μέσα σε αυτό και στις υπόλοιπες που

χρησιμοποιούνται στα νέα επικαλυπτόμενα κύτταρα. Τέλος, ένας ακόμα τρόπος επέκτασης των δυνατοτήτων ενός κυψελικού δικτύου είναι η βελτίωση των modems και στην τεχνολογία πρόσβασης, εφόσον η ψηφιακή τεχνολογία αυξάνει τη χωρητικότητα του δικτύου. [4][7]

## 2. 3 ΜΕΤΑΠΟΜΠΗ (HANDOFF – HANDOVER)

Η μεταπομπή είναι η διαδικασία μεταφοράς του ελέγχου, της εκπομπής και λήψης της μεταδιδόμενης πληροφορίας από τη δικαιοδοσία του ενός σταθμού βάσης σε έναν άλλον. Η μεταπομπή ενεργοποιείται από το δίκτυο όταν η ισχύς του λαμβανόμενου σήματος πέσει σε μια προκαθορισμένη τιμή πάνω από το ελάχιστο εκμεταλλεύσιμο σήμα λήψης. Η διαδικασία της μεταπομπής πρέπει να εκτελείται όσο το δυνατόν λιγότερο, ώστε να μην υπάρχει διακοπή κατά τη διάρκεια μιας συνομιλίας, αλλά ούτε και απώλεια πακέτων δεδομένων, με αποτέλεσμα τη συμφόρηση του δικτύου. Στο σχήμα που ακολουθεί φαίνεται η διαδικασία της μεταπομπής. [2][4][6][8]

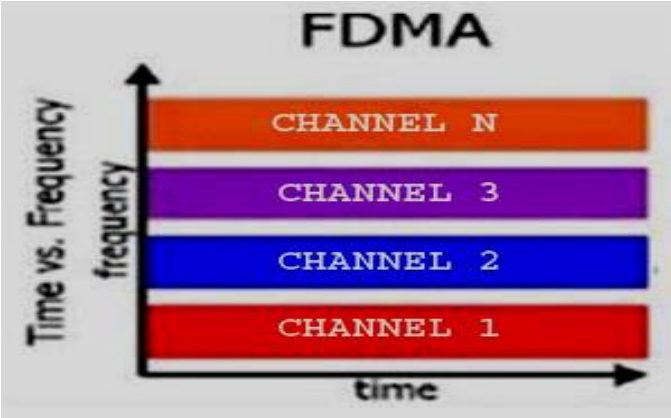



**ΕΙΚΟΝΑ 21: ΔΙΑΔΙΚΑΣΙΑ ΜΕΤΑΠΟΜΠΗΣ**

## 2. 4 ΚΥΨΕΛΙΚΑ ΔΙΚΤΥΑ ΠΡΩΤΗΣ ΓΕΝΙΑΣ (1G)

Τα κυψελικά δίκτυα πρώτης γενιάς εμφανίστηκαν τη δεκαετία του ’80 και ήταν αναλογικά. Δεν αποτέλεσαν την αρχή των κινητών επικοινωνιών, καθώς προϋπήρχαν δίκτυα κινητών επικοινωνιών, τα οποία όμως δεν ήταν κυψελικά. Η πρώτη γενιά χρησιμοποιούσε τεχνικές αναλογικής μετάδοσης για τη μετάδοση αποκλειστικά φωνής και η υποστήριξη της κινητικότητας των χρηστών ήταν υποτυπώδης και προβληματική. Η τεχνική πολυπλεξίας που χρησιμοποίησε η πρώτη γενιά ήταν η πολλαπλή προσπέλαση με διαίρεση συχνότητας (Frequency

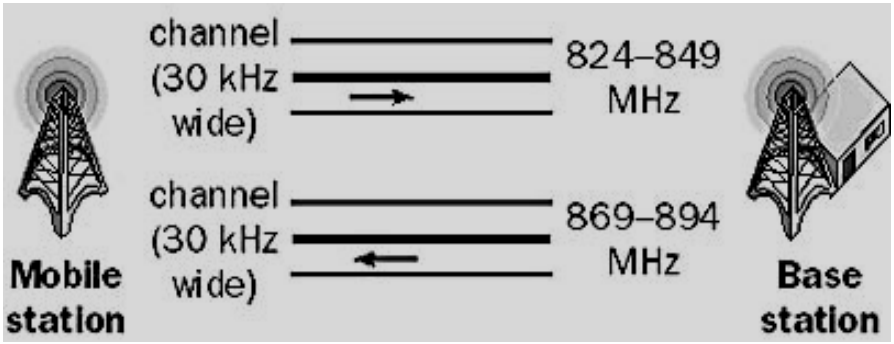
Division Multiple Access – FDMA). Στην τεχνική αυτή οι σταθμοί εκπέμπουν ταυτόχρονα αλλά σε διαφορετική συχνότητα. Αυτό επιτυγχάνεται με τη διαίρεση του διαθέσιμου φάσματος σε τμήματα, τα οποία χρησιμοποιούνται από έναν χρήστη το καθένα, όπως φαίνεται στην εικόνα που ακολουθεί. [2][3][4][6]




**ΕΙΚΟΝΑ 22: Η ΤΕΧΝΙΚΗ ΠΟΛΥΠΛΕΞΙΑΣ FDMA**

Όταν το πλήθος των χρηστών είναι μικρότερο από το πλήθος των τμημάτων του φάσματος, η ανάθεση των τμημάτων μπορεί να γίνει στατικά, ενώ όταν συμβαίνει το αντίθετο, η ανάθεση γίνεται πάντα δυναμικά. Συνήθως, σε κάθε χρήστη ανατίθεται ένα ζευγάρι από κανάλια, ένα για τη μετάδοση από τον χρήστη προς τον σταθμό βάσης και ένα για τη μετάδοση από τον σταθμό προς τον χρήστη. Η συχνότητα του πρώτου ονομάζεται ανωφερής (uplink) και του δεύτερου κατωφερής (downlink), με μικρότερη συνήθως τη συχνότητα του ανωφερούς, όπως φαίνεται στην εικόνα που ακολουθεί.

- **Transmission by mobile station:** 824 MHz to 849 MHz
- **Transmission by base station:** 869 MHz to 894 MHz




**ΕΙΚΟΝΑ 23: ΑΝΩΦΕΡΗΣ ΚΑΙ ΚΑΤΩΦΕΡΗΣ ΣΥΧΝΟΤΗΤΑ**

Σήμερα, τα κυψελικά δίκτυα πρώτης γενιάς θεωρούνται παρωχημένα λόγω της χρήσης αναλογικής αναπαράστασης των μεταδιδόμενων πληροφοριών, με αποτέλεσμα να δημιουργούνται τρία βασικά προβλήματα. Πρώτο πρόβλημα είναι η απουσία κρυπτογράφησης, με αποτέλεσμα οι κλήσεις μέσω ενός τέτοιου δικτύου να είναι ευάλωτες σε υποκλοπές, καθώς επίσης και σε υποκλοπές των αριθμών των χρηστών με σκοπό την παράνομη πραγματοποίηση κλήσεων και χρέωση φυσικά στο νόμιμο κάτοχο. Δεύτερο πρόβλημα είναι η χαμηλή ποιότητα των κλήσεων, διότι δεν εφαρμόζεται καμία κωδικοποίηση ή μέθοδος διόρθωσης λαθών για την εξάλειψη των σφαλμάτων από τις παρεμβολές. Τέλος, ένα ακόμα πρόβλημα που υπάρχει στα κυψελικά δίκτυα πρώτης γενιάς, είναι η μη αποδοτική χρήση του φάσματος. Όπως έχουμε ήδη πει, το φάσμα χωρίζεται σε μικρότερα τμήματα και μοιράζεται στους χρήστες, ανεξάρτητα όμως από το αν ένας χρήστης είναι ενεργός ή όχι.

Σε διάφορες χώρες του κόσμου έχουν εγκατασταθεί ένα πλήθος κυψελικών δικτύων πρώτης γενιάς, τα οποία περιγράφονται ξεχωριστά στη συνέχεια, ανάλογα με τη χώρα στην οποία εγκαταστάθηκαν. Το πρώτο κυψελικό δίκτυο πρώτης γενιάς ονομάζεται Advanced Mobile Phone System (AMPS) και αναπτύχθηκε το 1982 στις ΗΠΑ από τα εργαστήρια Bell. Τέτοια δίκτυα υπάρχουν επίσης στον Καναδά, τη κεντρική και τη νότια Αμερική καθώς επίσης και στην Αυστραλία. Μέχρι και σήμερα υπάρχουν υπό λειτουργία τέτοια δίκτυα στις ΗΠΑ.

Το AMPS διαιρεί το διαθέσιμο φάσμα σε κανάλια συχνοτήτων εύρους 30 KHz. Οι συχνότητες λειτουργίας του AMPS αποτελούνται από δύο τμήματα των 25 MHz. Το πρώτο τμήμα αποτελείται από μονόδρομα κανάλια μετάδοσης στις περιοχές συχνοτήτων 824 – 849 MHz και το δεύτερο τμήμα από μονόδρομα κανάλια στα 869 – 894 MHz. Το AMPS χρησιμοποιεί πολλαπλή προσπέλαση με διαίρεση συχνότητας (Frequency Division Multiple Access – FDMA) για τον διαχωρισμό των καναλιών. [2][8]

Μια πιο εξελιγμένη έκδοση του AMPS αποτέλεσε λίγο αργότερα το NAMPS (Narrowband AMPS), το οποίο ενσωμάτωνε κάποια ψηφιακή τεχνολογία προκειμένου να επιτρέψει στο δίκτυο να αυξήσει τη χωρητικότητά του. Αν και το NAMPS χρησιμοποιούσε ψηφιακή τεχνολογία ήταν κατά βάση αναλογικό.

Συνεχίζοντας την περιγραφή των κυψελικών δικτύων πρώτης γενιάς περνάμε σε αυτά που εγκαταστάθηκαν στην Ευρώπη και παρουσιάζονται στον επόμενο πίνακα.

**ΠΙΝΑΚΑΣ 3: ΚΥΨΕΛΙΚΑ ΔΙΚΤΥΑ ΠΡΩΤΗΣ ΓΕΝΙΑΣ**

| ΣΥΣΤΗΜΑΤΑ | ΧΩΡΕΣ |
|---|---|
| TACS | Βρετανία, Ιταλία, Ισπανία, Αυστρία, Ιρλανδία |
| NMT | Σε διάφορες ευρωπαϊκές χώρες. |
| C – 450 | Γερμανία, Πορτογαλία |
| RADIOCOM 2000 | Γαλλία |
| RTMS | Ιταλία |

Από τα παραπάνω συστήματα, τα δημοφιλέστερα είναι τα TACS και NMT, τα οποία το 1995 τα χρησιμοποιούσαν οι μισοί και περισσότεροι χρήστες αναλογικών συστημάτων. Τα TACS αρχικά αναπτύχθηκαν στη Βρετανία και αργότερα υιοθετήθηκαν από τις υπόλοιπες χώρες. Έχουν εύρος συχνοτήτων 25 KHz. Τα NMT χρησιμοποιήθηκαν αρχικά από τη Σκανδιναβία και αργότερα υιοθετήθηκαν από κάποιες χώρες της κεντρικής και της νότιας Ευρώπης. Υπάρχουν δύο εκδόσεις αυτού του συστήματος, το NMT - 450 το οποίο λειτουργεί στην περιοχή συχνοτήτων γύρο από τα 450 MHz και τα NMT – 900 στην περιοχή γύρο από τα 900 MHz, το οποίο αναπτύχθηκε το 1986. Τα NMT - 450 έχουν εύρος συχνοτήτων 25 KHz, ενώ τα NMT – 900 12,5 KHz. Στο NMT – 450 υπάρχουν 180 διπλά κανάλια, με απόσταση 25 KHz μεταξύ τους. Όμως, υπάρχει μία προαιρετική περιοχή συχνοτήτων η οποία προσφέρει 20 επιπλέον διπλά κανάλια. Τα C – 450 αποτελούσε το πρώτο σύστημα με αλληλοεφαπτόμενες κυψέλες, δηλαδή το σήμα μπορούσε να μεταφέρεται από τη μία κυψέλη στην άλλη χωρίς να διακόπτεται. Τα C – 450 έχουν εύρος συχνοτήτων 10 KHz και το RADIOCOM 2000 12,5 KHz. Τέλος τα RTMS (Radio Telephone Mobile System) έχουν εύρος συχνοτήτων 25 KHz. [8]

Τέλος, ένα ακόμα σύστημα κυψελικών δικτύων που αναπτύχθηκε, αυτή τη φορά στην Ιαπωνία, είναι το NTT (Nippon Telephone and Telegraph). Αξίζει να αναφερθεί πως στην Ιαπωνία το διαθέσιμο φάσμα για αναλογικά κυψελικά δίκτυα είναι 56 MHz. Το NTT άρχισε να λειτουργεί το 1979 στη μητροπολιτική περιοχή

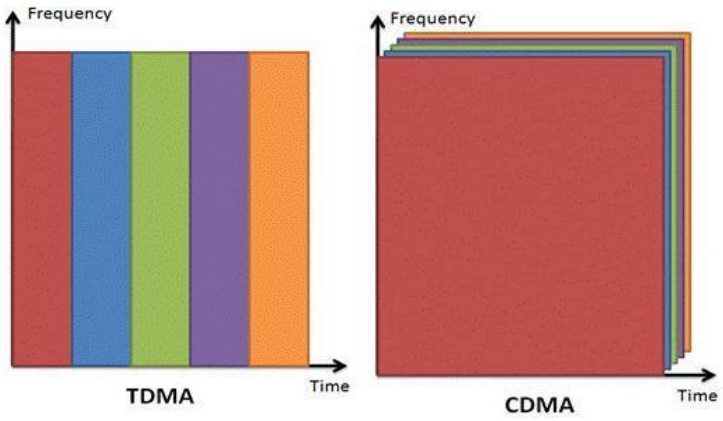
του Τόκυο. Το σύστημα αυτό χρησιμοποιούσε 600 διπλά κανάλια τα οποία μεταξύ τους απείχαν 25 KHz. Τα κανάλια αυτά χρησιμοποιούσαν περιοχές συχνοτήτων των 925 – 940 και 870 – 885 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. Τα κανάλια μεταφοράς φωνής ήταν αναλογικά ενώ τα κανάλια ελέγχου ψηφιακά με ταχύτητα 300 bps. Η ταχύτητα αυτή έφτασε τα 2,4 Kbps το 1988 και το πλήθος των καναλιών αυξήθηκε στα 2400, μέσω διαπλοκής συχνότητας (frequency interleaving) και η απόσταση των καναλιών μειώθηκε στα 6,25 KHz. Το βελτιωμένο αυτό σύστημα ήταν συμβατό «προς τα πίσω», με αποτέλεσμα να μπορούν να χρησιμοποιηθούν και από το παλιό αλλά και από το καινούριο οι νέες συσκευές που κατασκεύαζαν. [7][8]

## 2. 5 ΚΥΨΕΛΙΚΑ ΔΙΚΤΥΑ ΔΕΥΤΕΡΗΣ ΓΕΝΙΑΣ (2G)

Όπως ήταν αναμενόμενο, μετά την πρώτη γενιά των αναλογικών κυψελικών δικτύων, ακολούθησε η δεύτερη γενιά, χρησιμοποιώντας όμως ψηφιακή μετάδοση. Τα κυψελικά δίκτυα δεύτερης γενιάς λύνουν κάποια προβλήματα της πρώτης. Έτσι, σε σύγκριση με τα δίκτυα της πρώτης γενιάς, στα δίκτυα της δεύτερης γενιάς τα ψηφιακά δεδομένα μπορούν εύκολα να κρυπτογραφηθούν με σκοπό την προστασία των προσωπικών δεδομένων των χρηστών. Επιπλέον, γίνεται χρήση μεθόδων ανίχνευσης και διόρθωσης σφαλμάτων στα δεδομένα που μεταδίδονται. Αυτό έχει ως αποτέλεσμα την αύξηση της ποιότητας, τις υψηλότερες ταχύτητες αλλά και την καλύτερη αξιοποίηση του φάσματος. Τέλος, στα ψηφιακά συστήματα, κάθε κανάλι μοιράζεται σε περισσότερους από έναν χρήστες, είτε μέσω χρονικών σχισμών (slots), είτε με τη χρήση διαφορετικού κωδικού από κάθε χρήστη. Οι σχισμές και οι κωδικοί δίνονται όταν κάποιος σταθμός θελήσει να επικοινωνήσει.

Τα κυψελικά δίκτυα δεύτερης γενιάς, για το διαμοιρασμό του φάσματος χρησιμοποιούν πολλαπλή πρόσβαση με διαίρεση χρόνου (Time Division Multiple Access - TDMA) και πολλαπλή πρόσβαση με διαίρεση κώδικα (Code Division Multiple Access - CDMA). Η μέθοδος πρόσβασης TDMA είναι η μέθοδος διαίρεσης χρόνου που κυριαρχεί στα κυψελικά δίκτυα δεύτερης γενιάς, όπως το GSM (Global System for Mobile Communications), το IS – 54 και το DECT (Digital European Cordless Telecommunications). Η μέθοδος πρόσβασης TDMA διαιρεί κάθε κανάλι σε χρονικές σχισμές, και η δομή που προκύπτει είναι γνωστή ως πλαίσιο TDMA. Μέσω αυτής της δομής γίνεται ανάθεση διαφορετικής χρονικής

σχισμής σε κάθε σταθμό που χρησιμοποιεί το συγκεκριμένο κανάλι. Οι σταθμοί ενημερώνονται για τον αριθμό της χρονικής σχισμής κατά την οποία θα εκπέμψουν, έτσι ώστε να γνωρίζουν πόσο χρόνο θα περιμένουν μέχρι να έρθει η σειρά τους. Ουσιαστικά, η πρόσβαση TDMA είναι ημιαμφίδρομη (half – duplex), καθώς μόνο ένας σταθμός μπορεί να εκπέμψει ανά πάσα χρονική στιγμή, παρ' όλο που η διάρκεια των σχισμών είναι πολύ μικρή και μας δημιουργεί τη ψευδαίσθηση της αμφίδρομης επικοινωνίας. Η μικρή όμως διάρκεια των σχισμών οδηγεί σε αυστηρές απαιτήσεις συγχρονισμού, με αποτέλεσμα να χρησιμοποιούνται στη μέθοδο TDMA διαστήματα προστασίας στο χρόνο. Στις επόμενες εικόνες παρουσιάζονται η μέθοδος διαμοιρασμού του φάσματος TDMA και η CDMA, η οποία θα αναλυθεί στη συνέχεια. [2][3][4][7]




**ΕΙΚΟΝΑ 24: ΜΕΘΟΔΟΣ ΔΙΑΜΟΙΡΑΣΜΟΥ ΦΑΣΜΑΤΟΣ TDMA ΚΑΙ CDMA**

Τα συστήματα CDMA αναθέτουν την ίδια συχνότητα σε όλους τους σταθμούς ταυτόχρονα. Οι ταυτόχρονες εκπομπές των σταθμών διαχωρίζονται μέσω του μοναδικού κωδικού που ανατίθεται στον καθένα. Κάθε κωδικός αποτελείται από n bit. Η τιμή της παραμέτρου n είναι γνωστή ως ρυθμός chip (chip rate) του συστήματος. Οι κωδικοί που ανατίθενται σε κάθε σταθμό είναι ορθογώνιοι μεταξύ τους, κάτι που σημαίνει ότι το κανονικοποιημένο εσωτερικό γινόμενο των διανυσματικών αναπαραστάσεων δύο οποιωνδήποτε κωδικών ισούται με μηδέν. Οι σταθμοί μπορούν να εκπέμπουν ταυτόχρονα, και οι παραλήπτες διαχωρίζουν το μήνυμα κάποιου συγκεκριμένου αποστολέα χρησιμοποιώντας το μοναδικό κωδικό. Ο τρόπος χρήσης του κωδικού ενός σταθμού για την εκπομπή είναι ο ακόλουθος: για να εκπέμψει το δυαδικό 1, ο σταθμός εκπέμπει τον κωδικό του,

ενώ για να εκπέμψει το 0, ο σταθμός εκπέμπει το συμπλήρωμα ως προς ένα του κωδικού του. [3]

Υποθέτοντας ότι οι ταυτόχρονες εκπομπές των σταθμών προστίθενται γραμμικά, ο παραλήπτης μπορεί να εξαγάγει την εκπομπή ενός συγκεκριμένου σταθμού συσχετίζοντας το συνολικό λαμβανόμενο σήμα με τον κωδικό του πομπού. Επειδή χρησιμοποιούνται κωδικοί με n δυαδικά ψηφία, κάθε εκπομπή καταλαμβάνει n φορές το εύρος της εκπομπής των ίδιων δεδομένων μέσω ενός καναλιού μικρού εύρους για τον ίδιο ρυθμό μετάδοσης. Συνεπώς, η πρόσβαση CDMA διευρύνει το φάσμα της εκπομπής και προσφέρει αντοχή στην εξασθένηση του σήματος, γι' αυτό χρησιμοποιείται συχνά και ως τρόπος αντιμετώπισης της εξασθένησης του σήματος, όπως συμβαίνει στο φυσικό στρώμα του προτύπου IEEE 802.11.

Επιπλέον, τα κυψελικά δίκτυα δεύτερης γενιάς χρησιμοποιούν ιεραρχικές δομές κελιών, δηλαδή η περιοχή κάλυψης διαιρείται σε μακροκυψέλες (macrocells), μικροκυψέλες (microcells) και πικοκυψέλες (picocells), με σκοπό την περαιτέρω αύξηση των δυνατοτήτων των δικτύων. Οι μακροκυψέλες καλύπτουν ευρύτερες περιοχές, όπου λίγοι χρήστες έχουν πρόσβαση στο δίκτυο. Σε περιοχές με υψηλή πυκνότητα τερματικών που ζητούν πρόσβαση στο δίκτυο, όπως σε μεγάλες πόλεις, χρησιμοποιούνται μικροκυψέλες. Αυτές καλύπτουν αρκετά μικρές περιοχές και προσφέρουν ικανή χωρητικότητα για όλες τις συσκευές που υπάρχουν στην περιοχή τους. Τέλος, οι πικοκυψέλες δημιουργούνται με σκοπό να προσφέρουν γρήγορη και αξιόπιστη πρόσβαση στο δίκτυο, καλύπτοντας έκταση ενός κτηρίου όπου υπάρχει μεγάλη ζήτηση. Στη συνέχεια περιγράφονται τα κύρια πρότυπα αυτής της γενιάς.

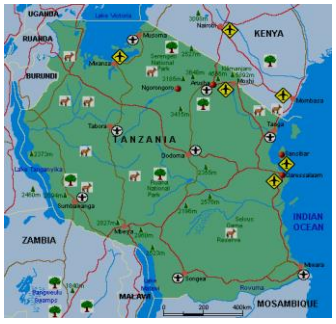
GSM®
GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Το πιο επιτυχημένο και αντιπροσωπευτικό πρότυπο αυτής της γενιάς είναι το GSM (Global System for Mobile Communication). Η μελέτη για αυτό το πρότυπο άρχισε το 1982 από το Ευρωπαϊκό Τηλεπικοινωνιακό Συμβούλιο (European Conference of Postal and Telecommunications Administrations - CEPT), με την ονομασία "Group Special Mobile" – GSM, με σκοπό τη δημιουργία ενός πανευρωπαϊκού συστήματος κινητής τηλεφωνίας. Βέβαια, το σύστημα αυτό θα έπρεπε να τηρεί και κάποιες προϋποθέσεις, όπως η καλή ποιότητα, αποδοτική χρήση φάσματος, μικρό κόστος

τερματικών και υπηρεσιών, δυνατότητα φορητών τερματικών, διεθνής λειτουργία και την υποστήριξη νέων πρωτοτύπων. [7] Το 1989, η ευθύνη για την ανάπτυξη του προτύπου μεταφέρθηκε στο Ευρωπαϊκό Ίδρυμα Προτύπων Τηλεπικοινωνιών (European Telecommunications Standards Institute – ETSI) και το πρότυπο μετονομάστηκε σε Global System for Mobile Communication – GSM και η πρώτη φάση των προδιαγραφών του πρωτοτύπου δημοσιεύτηκε το 1990. [2] Η εμπορική λειτουργία συστημάτων GSM άρχισε το 1991 και μέχρι το τέλος του 1993, υπήρχαν σε λειτουργία 36 δίκτυα GSM σε 22 ευρωπαϊκές χώρες και ως το 1999 οι συνδρομητές αυξάνονταν κατά ένα εκατομμύριο κάθε εβδομάδα. Στην Ελλάδα η ιστορία του GSM ξεκινάει το 1992, όταν η κυβέρνηση Μητσοτάκη προκήρυξε διαγωνισμό για την αδειοδότηση δύο γραμμών, τις οποίες κέρδισαν οι εταιρείες Wind Hellas (πρώην TIM και παλαιότερα Telestet) και Panafon. Πρώτη ξεκίνησε τη λειτουργία της στις 29 Ιουνίου 1993 η Telestet και λίγες ημέρες αργότερα, στις 1 Ιουλίου, ξεκίνησε να προσφέρει τις υπηρεσίες της και η Panafon. Αρχικά, το κόστος των συσκευών και των υπηρεσιών ήταν απαγορευτικό. Επιπλέον, οι προβλέψεις δεν ήταν ιδιαίτερα αισιόδοξες για την ελληνική αγορά, καθώς οι ειδικοί υποστήριζαν πως ο αριθμός των χρηστών θα φτάσει μέχρι τα τέλη της δεκαετίας τους 200000. Ωστόσο, γρήγορα επήλθε η διάψευση όλων των προβλέψεων. Επιπλέον, το 1998 μπήκε στην αγορά και ο ΟΤΕ με τη θυγατρική του Cosmote, κερδίζοντας μέσα σε μικρό χρονικό διάστημα σημαντικό μερίδιο από την πελατεία. Ο ανταγωνισμός οδήγησε σε μείωση των τιμών των υπηρεσιών. Ήδη το 2000 η Ελλάδα καταλάμβανε τις πρώτες θέσεις στην παγκόσμια κατάταξη στην αναλογία κινητών τηλεφώνων ανά κάτοικο, αλλά και βαθμού τεχνολογίας ανάπτυξης στο συγκεκριμένο τομέα. (Πηγή: www.kathimerini.gr με πληροφορίες από SPIEGEL και ΟΤΕ) Η ύπαρξη ενός μόνο προτύπου στην Ευρώπη έδωσε σημαντική ώθηση στην εξέλιξη της ευρωπαϊκής αγοράς κυψελικής τηλεφωνίας, σε αντίθεση με την Αμερική, η οποία οδηγήθηκε σε κατακερματισμό. Μέχρι το 2005 η τεχνολογία GSM κατείχε το 70% της παγκόσμιας αγοράς στα συστήματα κινητής τηλεφωνίας δεύτερης γενιάς.

Σήμερα, υπάρχουν τέσσερις εκδόσεις του προτύπου GSM οι οποίες διαφέρουν στη συχνότητα λειτουργίας. Η πρώτη έκδοση είναι το GSM – 900, το οποίο λειτουργεί στην περιοχή συχνοτήτων των 900 MHz για να επαναχρησιμοποιηθεί το φάσμα που χρησιμοποιούσαν τα αναλογικά συστήματα. Χρησιμοποιούν περιοχές

συχνοτήτων των 890 – 915 και 935 – 960 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. Το διαθέσιμο εύρος ζώνης χωρίζεται σε 124 κανάλια των 200 KHz. Για το διαχωρισμό των εκπομπών των σταθμών, χρησιμοποιεί έναν συνδυασμό του FDMA/TDMA. Σε κάθε σταθμό ανατίθονται κάποια κανάλια, τα οποία στη συνέχεια χωρίζονται στο πεδίο του χρόνου, δημιουργώντας σχισμές διάρκειας 0,577 msec. Η δεύτερη έκδοση είναι το GSM – 1800 και αναπτύχθηκε το 1991 στην Ευρώπη. Τα συστήματα αυτής της έκδοσης είναι επίσης γνωστά και ως DCS (Digital Communications Service) και λειτουργούν στην περιοχή συχνοτήτων των 1800 MHz. Χρησιμοποιούν περιοχές συχνοτήτων των 1710 – 1785 και 1805 – 1880 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. Το διαθέσιμο εύρος ζώνης χωρίζεται σε 374 κανάλια των 200 KHz και το κάθε κανάλι αποτελείται από οχτώ συνδρομητές. Από κάθε κυψέλη μπορούν να εξυπηρετηθούν 2992 επικοινωνίες. Η τρίτη έκδοση είναι το GSM – 1900 και αναπτύχθηκε στην Αμερική. Τα συστήματα αυτής της έκδοσης είναι επίσης γνωστά και ως PCS (Personal Communications Service) και λειτουργούν στην περιοχή συχνοτήτων των 1900 MHz. Χρησιμοποιούν περιοχές συχνοτήτων των 1850 – 1910 και 1930 – 1990 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. Το διαθέσιμο εύρος ζώνης χωρίζεται σε 299 κανάλια των 200 KHz. Τέλος, η τέταρτη έκδοση είναι η GSM – 450, η οποία δεν είναι ιδιαίτερα γνωστή. Χρησιμοποιεί την ίδια ζώνη συχνοτήτων, όπως και τα κυψελικά δίκτυα πρώτης γενιάς, τα NMT , κι έτσι μπορούν να συνυπάρχουν με αυτά. Αρχικά χρησιμοποιήθηκαν στις Σκανδιναβικές χώρες, στη Μπενελούξ, στις χώρες των Άλπεων, στην Ανατολική Ευρώπη και στη Ρωσία, όμως πριν από την εισαγωγή του GSM. Χρησιμοποιούν περιοχές συχνοτήτων των 450,4 – 457,6 ή 478 - 486 και 460,4 – 467,6 ή 488,8 - 496 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. [1][2][6][7]




Η GSM Association απαιτεί ένας μόνο από τους περίπου 680 χειριστές - μέλη, να έχει την άδεια λειτουργίας συστημάτων GSM – 450 στην Τανζανία. (Πηγή: http://en.wikipedia.org/wiki/GSM_frequency_bands) Βέβαια, όλοι πλέον οι δημόσιοι φορείς στην Τανζανία λειτουργούν συστήματα GSM 900 / 1800 MHz. Γενικά, όπου υπάρχει η ζώνη των GSM – 450 NMT, χρησιμοποιούνται είτε συστήματα

NMT, είτε έχουν αντικατασταθεί από το CDMA, το οποίο θα αναλύσουμε στη συνέχεια. Στον παρακάτω πίνακα παρουσιάζονται οι εκδόσεις του προτύπου GSM. (Πηγή: Ασύρματα Δίκτυα, Εκδόσεις Κλειδάριθμος)

**ΠΙΝΑΚΑΣ 4: ΕΚΔΟΣΕΙΣ ΤΟΥ ΠΡΟΤΥΠΟΥ GSM**

| ΕΚΔΟΣΗ GSM | ΑΝΩΦΕΡΗΣ ΣΥΧΝΟΤΗΤΑ MHz | ΚΑΤΩΦΕΡΗΣ ΣΥΧΝΟΤΗΤΑ MHz |
|---|---|---|
| GSM - 900 | 890 – 915 | 935 – 960 |
| GSM – 1800 (DCS) | 1710 – 1785 | 1805 – 1880 |
| GSM – 1900 (PCS) | 1850 – 1910 | 1930 – 1990 |
| GSM - 450 | 450,4–457,6 ή 478-486 | 460,4-467,6 ή 488,8-496 |

Το πρότυπο D – AMPS αναπτύχθηκε το 1991 στην Αμερική σε μία προσπάθεια να βρεθεί ένα σύστημα που θα ήταν πιο αποδοτικό από το AMPS. Το D – AMPS είναι γνωστό και ως IS – 54. Το D – AMPS διατηρεί τα κανάλια εύρους 30 KHz του AMPS και ουσιαστικά αποτελεί μια προσθήκη ψηφιακών καναλιών σε ένα σύστημα AMPS, με αποτέλεσμα να τριπλασιάζεται το πλήθος των χρηστών. Το D – AMPS σχεδιάστηκε έτσι ώστε να είναι συμβατό με το ήδη υπάρχον σύστημα AMPS. Χρησιμοποιούν περιοχές συχνοτήτων των 824 – 849 και 869 – 894 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. Κάθε ψηφιακό κανάλι οργανώνεται σε πλαίσιο των 40 msec και κάθε πλαίσιο αποτελείται από έξι χρονικές σχισμές διάρκειας 6,67 msec η κάθε μία. Κάθε τερματικό μπορεί να χρησιμοποιήσει είτε μία είτε δύο σχισμές ανά πλαίσιο. Όταν υπάρχουν δύο σχισμές χρησιμοποιείται ο κωδικοποιητής φωνής πλήρους ρυθμού (full rate) μεταφέροντας πληροφορίες φωνής με ταχύτητα 7,95 Kbps χωρίς διόρθωση λαθών και 5,05 Kbps με διόρθωση λαθών. Επίσης, οι ταχύτητες μεταφοράς δεδομένων είναι 9,6 Kbps και 3,4 Kbps χωρίς και με διόρθωση λαθών αντίστοιχα. Το IS – 136 είναι μία αναβάθμιση του D – AMPS η οποία λειτουργεί στα 800 MHz με σχέδια αναβαθμίσεων προκειμένου να χρησιμοποιείται και στην περιοχή των 1900 MHz. Αντίθετα με το D – AMPS, το οποίο είναι μία ψηφιακή επέκταση του AMPS, το IS – 136 είναι ένα πλήρως ψηφιακό πρότυπο. [8]

Ένα ακόμα πρότυπο είναι το cdmaOne, το οποίο είναι γνωστό και ως IS – 95, το οποίο προτυποποιήθηκε το 1993 και εγκαταστάθηκε το 1995 στη Νότια Κορέα και

το Χονγκ Κονγκ, ακολουθούμενο από εγκαταστάσεις στην Αμερική την επόμενη χρονιά. Το cdmaOne είναι ασύμβατο με το πρότυπο IS – 136 το οποίο περιγράψαμε νωρίτερα, όμως και τα δύο λειτουργούν στις ίδιες συχνότητες με το AMPS. Το cdmaOne σχεδιάστηκε ώστε να υποστηρίζει τερματικά διπλού τρόπου λειτουργίας (dual mode) για τα δίκτυα cdmaOne και AMPS. Το cdmaOne υποστηρίζει ταχύτητες μεταφοράς δεδομένων 4,8 και 14,4 Kbps. Το cdmaOne χρησιμοποιεί κανάλια εύρους 1,228 MHz τόσο για ανωφερή όσο και για κατωφερή μετάδοση. Για τη συγκρότηση ενός καναλιού cdmaOne απαιτείται φάσμα που χρησιμοποιείται από 41 κανάλια AMPS των 30 KHz.

Ένα ακόμα πρότυπο είναι το PDC (Personal Digital Cellular), το οποίο αναπτύχθηκε το 1991 στην Ιαπωνία. Παρ' όλο που το PDC χρησιμοποιείται μόνο στην Ιαπωνία, είναι το δεύτερο μεγαλύτερο ψηφιακό πρότυπο στον κόσμο με περισσότερους από 48 εκατομμύρια συνδρομητές μέχρι τον Ιούλιο του 2000. Χρησιμοποιεί TDMA τεχνολογία και λειτουργεί στην περιοχή συχνοτήτων των 800 και 1400 MHz. Χρησιμοποιούν περιοχές συχνοτήτων των 810 – 826 ή 1429 - 1453 και 940 – 956 ή 1477 - 1501 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. Το PDC είναι ασύμβατο με τα υπόλοιπα πρότυπα.

## 2. 6 ΚΥΨΕΛΙΚΑ ΔΙΚΤΥΑ 2,5 ΓΕΝΙΑΣ (2,5G)

Ο όρος «γενιά 2,5» αναφέρεται στο σύνολο των αναβαθμίσεων που έγιναν στα κινητά δίκτυα δεύτερης γενιάς. Πολλές από τις αναβαθμίσεις αυτές παρέχουν τις ίδιες δυνατότητες με τα κυψελικά δίκτυα τρίτης γενιάς. Αν και οι διαχωριστική γραμμή ανάμεσα στα δίκτυα δεύτερης και 2,5 γενιάς είναι λεπτή, υπάρχουν κάποια πρότυπα τα οποία χαρακτηρίζουν αυτή τη γενιά. Τα πρότυπα αυτά είναι η HSCSD (High – Speed Circuit – Switched Data), η GPRS (General Packet Radio Services) και η EDGE (Enhanced Data for Global Evolution), τα οποία αναλύονται στη συνέχεια.

Το μεγαλύτερο πρόβλημα που παρουσίαζε το πρότυπο GSM ήταν οι χαμηλοί ρυθμοί μετάδοσης που περιορίζονταν στα 9,6 Kbps. Αργότερα, τέθηκαν οι προδιαγραφές για ταχύτητες 14,4 Kbps αλλά δεν χρησιμοποιήθηκαν ευρέως. Η λύση δόθηκε από το πρότυπο HSCSD (High – Speed Circuit – Switched Data). Σε αντίθεση με το πρότυπο GSM, προσφέρει περισσότερες από μία σχισμές μέσα σε κάθε πλαίσιο του GSM, με αποτέλεσμα να αυξάνεται η ταχύτητα μετάδοσης των

δεδομένων. Το HSCSD επιτρέπει σε ένα τερματικό να χρησιμοποιήσει 2, 3 ή και 4 σχισμές ανά πλαίσιο, προσφέροντας με αυτόν τον τρόπο ταχύτητες 28,8, 43,2 και 57,6 Kbps αντίστοιχα. Ένα μειονέκτημα αυτού του προτύπου είναι ότι μειώνει το χρόνο ζωής των τερματικών, καθώς η αυξημένη χρήση σχισμών ωθεί τα τερματικά να απασχολούνται περισσότερο χρόνο με την εκπομπή και τη λήψη. Όμως, όπως γνωρίζουμε, απαιτείται λιγότερη ισχύς για τη λήψη από ότι για τη μετάδοση, με αποτέλεσμα το πρότυπο να είναι πολύ αποδοτικό για εφαρμογές όπως η περιήγηση. Η υλοποίηση του συγκεκριμένου προτύπου είναι σχετικά απλή και φθηνή. Το βασικότερο μειονέκτημα αυτού του προτύπου είναι η χρήση μεταγωγής κυκλώματος. Αυτός ο τρόπος μεταγωγής είχε ως αποτέλεσμα τη σπατάλη πόρων του δικτύου αφού οι σχισμές δεσμεύονται ακόμα και όταν δεν χρησιμοποιούνται, με αποτέλεσμα το πρότυπο αυτό να θεωρείται καλή επιλογή για εφαρμογές πραγματικού χρόνου, όπως εξηγήθηκε στο πρώτο κεφάλαιο. [4][6]

Ένα ακόμα πρότυπο αυτής της γενιάς είναι το GPRS (General Packet Radio Services), το οποίο επιτυγχάνει ταχύτητες δεδομένων των 115 Kbps ή και ακόμα μεγαλύτερες στο downlink, αν αγνοηθεί η διόρθωση σφαλμάτων. Η λειτουργία του GPRS βασίζεται στην ίδια λογική με το HSCSD, με τη διαφορά ότι το GPRS χρησιμοποίει μεταγωγή πακέτων και όχι μεταγωγή κυκλώματος όπως το HSCSD και το GSM. Το πρότυπο αυτό είναι πιο ακριβό από το HSCSD, όμως προσφέρει πολύ μεγαλύτερες δυνατότητες για την αποστολή δεδομένων. Με την αύξηση της ταχύτητας, δόθηκε η δυνατότητα υλοποίησης και εφαρμογής νέων υπηρεσιών, όπως υπηρεσίες Διαδικτύου, υπηρεσίες MMS (Multimedia Messaging Service) και προηγμένων MMS (Advanced MMS). [1][4][6]

Το τρίτο χαρακτηριστικό πρότυπο αυτής της γενιάς είναι το EDGE Enhanced Data for Global Evolution). Στηρίζεται στην τεχνική Eight – Phase Shift Keying (8PSK). Αυτή η τεχνική επηρεάζει μόνο το λογισμικό των σταθμών βάσης, ενώ προσφέρει έως και τριπλάσιες ταχύτητες από το GSM. Επιπλέον, δεν αντικαθιστά αλλά συνυπάρχει με την τεχνική διαμόρφωσης Gaussian Minimum Shift Keying (GMSK) η οποία χρησιμοποιείται στη βασική έκδοση του GSM. Ο συνδυασμός των προτύπων GPRS και EDGE λέγεται EGPRS (Enhanced GPRS). Με το συνδυασμό αυτό πετυχαίνετε ταχύτητες έως και 384 Kbps. [4][6][8]

## 2. 7 ΚΥΨΕΛΙΚΑ ΔΙΚΤΥΑ ΤΡΙΤΗΣ ΓΕΝΙΑΣ (3G)

Η γρήγορη εξέλιξη των κινητών τηλεπικοινωνιών ήταν ένα από τα αναμφισβήτητα γεγονότα της δεκαετίας του 1990. Το Δεκέμβριο του 2002 υπήρχαν παγκοσμίως 780 εκατομμύρια συνδρομητές σε δίκτυα GSM, οι οποίοι συνιστούσαν το 71% του συνολικού αριθμού των χρηστών κινητής τηλεφωνίας. Παρά τη μεγάλη επιτυχία που σημείωσαν τα κυψελικά δίκτυα δεύτερης γενιάς, τα δίκτυα αυτά πρόσφεραν περιορισμένες ταχύτητες μετάδοσης δεδομένων. Αυτό, αν και δεν αποτελεί περιοριστικό παράγοντα για τη φωνητική επικοινωνία, τα κάνει όμως μη πρακτικά για τις μελλοντικές εφαρμογές οι οποίες θα απαιτούν υψηλές ταχύτητες.

Τα σημαντικότερα χαρακτηριστικά της τρίτης γενιάς κυψελικών δικτύων είναι η «προς τα πίσω» συμβατότητα με τα δίκτυα της προηγούμενης γενιάς, η υποστήριξη περιαγωγής, οι υπηρεσίες μεταγωγής πακέτων και μεταγωγής κυκλώματος, η υποστήριξη παράλληλης εκτέλεσης εφαρμογών στο ίδιο τερματικό, η υποστήριξη ασύμμετρης και συμμετρικής κυκλοφορίας και τέλος, η δυνατότητα δημιουργίας ενός ιδεατού προσωπικού περιβάλλοντος (Virtual Home Environment – VHE). Το VHE είναι ένα σύνολο ρυθμίσεων για τις εφαρμογές του χρήστη που διατηρείται κατά τη μετακίνηση του μεταξύ διαφορετικών παροχών υπηρεσιών.

Η προτυποποίηση των συστημάτων τρίτης γενιάς ξεκίνησε από τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union – ITU) το 1992. Το αποτέλεσμα αυτής της διαδικασίας, γνωστό ως IMT – 2000 (International Mobile Telecommunications 2000), αποτελείται από διάφορα πρότυπα τρίτης γενιάς. Η ύπαρξη περισσότερων από ένα πρότυπα τρίτης γενιάς, είχε σαν σκοπό την ύπαρξη συμβατότητας με τα δίκτυα δεύτερης γενιάς. Έτσι, για τη δημιουργία προτύπων δημιουργήθηκε η ομάδα 3GPP (Third Generation Partnership Proposal). [6] Ανάλογα με τη χώρα και το προϋπάρχον δίκτυο, ορίζεται ένα δίκτυο τρίτης γενιάς, έτσι ώστε να είναι συμβατό τόσο με το ήδη εγκατεστημένο δίκτυο δεύτερης γενιάς, όσο και με τους εθνικούς κανόνες χρήσης του φάσματος. Το UMTS (Universal Mobile Telecommunications System) θεωρείται το κυρίαρχο πρότυπο στα 3G κυψελικά δίκτυα. Επίσης, το EDGE (Enhanced Data Rates for GSM Evolution) είναι ένα ακόμα πρότυπο τρίτης γενιάς. Στην Ιαπωνία , που είναι η πιο εξελιγμένη χώρα όσον αφορά την 3G τεχνολογία, η μετάβαση από τα 2G στα

3G δίκτυα ολοκληρώθηκε το 2006 και πλέον δύο συστήματα χρησιμοποιούνται, το W – CDMA, το οποίο είναι συμβατό με το πρότυπο UMTS, και το CDMA2000.

Το πρότυπο UMTS (Universal Mobile Telecommunications System) αποτελεί την ευρωπαϊκή απάντηση για τα κυψελικά δίκτυα τρίτης γενιάς και συχνά αναφέρεται σαν 3GSM ως συνδυασμός του 3G και του προτύπου GSM. Θεωρητικά μπορεί να υποστηρίξει ταχύτητες έως 2 Mbit / s. Από το 2006 τα δίκτυα UMTS σε πολλές χώρες άρχισαν να αναβαθμίζονται σε High Speed Downlink Packet Access (HSDPA), γνωστό και ως 3,5 G, το οποίο θα αναλυθεί στη συνέχεια. Το UMTS υποστηρίζει κινητή βιντεοδιάσκεψη, κατέβασμα αρχείων πολυμέσων, όπως ήχο, εικόνα και βίντεο καθώς και ζωντανή τηλεόραση. Χρησιμοποιούν περιοχές συχνοτήτων των 1885 – 2025 και 2110 – 2200 MHz για ανωφερή και κατωφερή μετάδοση αντίστοιχα. [1][3][5][8]

Το πρότυπο HSDPA (High Speed Downlink Packet Access) υποστηρίζει downlink ταχύτητες 1,8 Mbit / s, 3,6 Mbit / s και 7,2 Mbit / s. Το HSDPA χρησιμοποιείται ήδη σε 49 χώρες και 64 δίκτυα, και αποτελεί μία σχετικά εύκολη αναβάθμιση εκεί όπου υπάρχει ήδη το UMTS.

Το πρότυπο EDGE (Enhanced Data Rates for GSM Evolution) είναι μία ψηφιακή τεχνολογία κυψελικών δικτύων τρίτης γενιάς το οποίο επιτρέπει την αυξημένη ταχύτητα μετάδοσης δεδομένων και την αύξηση της αξιοπιστίας της μετάδοσης. Μπορεί να λειτουργήσει πάνω σε οποιοδήποτε δίκτυο που έχει GPRS αρκεί να γίνουν οι απαραίτητες αλλαγές από τον κάτοχο. Ο χρήστης δεν χρειάζεται να αλλάξει hardware ή software, όμως ο σταθμός βάσης θα πρέπει να κάνει τις κατάλληλες τροποποιήσεις έτσι ώστε να υποστηρίζουν EDGE. Οι ταχύτητές τους για μεταφορά δεδομένων μπορεί να φτάσουν τα 384 Mbit / s προσφέροντας οχτώ ενωμένα κανάλια για τον κάθε συνδρομητή.

Ένα ακόμα πρότυπο αυτής της γενιάς είναι το cdma2000, το οποίο είναι συμβατό με το cdmaOne και όπως είναι φυσικό προσφέρει πολλά πλεονεκτήματα στους χρήστες του cdmaOne οι οποίοι επιθυμούν να χρησιμοποιήσουν τις υπηρεσίες τρίτης γενιάς. Η αρχική περιγραφή του προτύπου περιλάμβανε δυο τρόπους διασποράς, την πολυκαναλική (Multicarrier) και την άμεση ακολουθία (Direct Spread). Υπάρχουν δυο μέθοδοι για το πρότυπο, οι οποίοι είναι το 1X και το 3X. Η 1X αποτελεί την απλούστερη έκδοση του προτύπου η οποία διπλασιάζει

τη χωρητικότητα του συστήματος για τηλεφωνία σε σύγκριση με το cdmaOne, ενώ προσφέρει κατά μέσο όρο, ρυθμούς μετάδοσης δεδομένων 144 Kbps. Η άλλη μέθοδος, η 3X, είναι μια βελτίωση του 1X, που χρησιμοποιεί τρία κανάλια cdmaOne συνολικού εύρους περίπου 3,75 MHz. Προσφέρει μεγαλύτερες ταχύτητες από την 1X που φτάνουν τα 2 Mbps. [3][4]

Επίσης, ένα ακόμα πρότυπο το οποίο βασίζεται στην τεχνολογία CDMA, είναι το WCDMA (Wideband Code Division Multiple Access), το οποίο απαιτεί συγχρονισμένη λειτουργία των σταθμών βάσης. Το WCDMA είναι ασύγχρονο, διευκολύνοντας τη λειτουργία του κυψελικού δικτύου. Το WCDMA χρησιμοποιεί κανάλια εύρους 5 MHz, πέντε φορές ευρύτερα από τα κανάλια του cdmaOne και είκοσι πέντε από εκείνα του GSM. Προσφέρει μεταφορά δεδομένων της τάξης των 384 Kbit / s για κάλυψη ευρείας περιοχής και 2 Mbit / s για τοπική. Το WCDMA χρησιμοποιεί το chip για τη μετάδοση των δεδομένων. Το chip είναι η μικρότερη μονάδα υψηλού ποσοστού κωδικοποιημένης ακολουθίας. Όταν λοιπόν, ένα σήμα, έχει προηγουμένως χωριστεί σε μικρότερα κομμάτια στα οποία τους έχει δοθεί ένας μοναδικός κωδικός, κι ύστερα στέλνονται στις ραδιοσυχνότητες του δικτύου. Όσο μεγαλύτερο είναι το ποσοστό διακίνησης των chips, τόσο μεγαλύτερο το εύρος του σήματος που καταλήγει. Το εύρος σε κάθε συχνότητα μπορεί να φτάσει τα 3,84 Mchips / s κι έτσι το εύρος ζώνης της κάθε συχνότητας μπορεί να επεκταθεί σε 5 MHz, όπως αναφέρθηκε προηγουμένως.[3][4]

## 2.8 ΚΥΨΕΛΙΚΑ ΔΙΚΤΥΑ ΤΕΤΑΡΤΗΣ ΓΕΝΙΑΣ (4G)

Αν και τα δίκτυα τρίτης γενιάς καλύπτουν πολλές από τις απαιτήσεις των χρηστών και προσφέρουν ταχύτητες μέχρι 2 Mbps, θα πρέπει πλέον να βελτιωθούν έτσι ώστε να καλύπτουν τις νέες απαιτήσεις των επόμενων δεκαετιών. Έτσι, παρά το γεγονός ότι τα δίκτυα τρίτης γενιάς έχουν το πλεονέκτημα του πρωτοκόλλου IP, έχουν το μειονέκτημα της ύπαρξης πολλών προτύπων, με αποτέλεσμα τη μειωμένη περιαγωγή μεταξύ των δικτύων διαφορετικών προτύπων. Η τέταρτη γενιά αφορά την αγορά του 2010 και μετά, και συγκεκριμένα σε μία πρόβλεψη που έγινε το 2009, ότι μεταξύ των ετών 2012 - 2015, θα προσφέρουν ταχύτητες μεταφοράς δεδομένων της τάξης των 50 – 155 Mbps. Υπάρχουν όμως κάποια οικονομικά αλλά και τεχνικά ζητήματα τα οποία θα πρέπει να μελετηθούν πριν την κυκλοφορία των δικτύων τέταρτης γενιάς έτσι ώστε η

επιτυχία τους να είναι εξασφαλισμένη. Κάποια από τα ζητήματα αυτά είναι η ανάπτυξη αποδοτικότερων τεχνικών διαμόρφωσης και η ανεύρεση επιπλέον φάσματος.

Σήμερα, παρόλο που δεν είναι γνωστή η δομή και η λειτουργία των συστημάτων αυτής της γενιάς, μπορούν να γίνουν μόνο κάποιες υποθέσεις. Οι βασικοί στόχοι αυτής της γενιάς είναι η διαλειτουργικότητα, το υποστηριζόμενο εύρος ζώνης και χρόνου ζωής των μπαταριών, το σταθερό δίκτυο μεταγωγής πακέτων, η μεταβολή εύρους ζώνης για την ασύρματη πρόσβαση, οι προηγμένοι σταθμοί βάσης και φυσικά οι υψηλότεροι ρυθμοί μετάδοσης.

Η έννοια της διαλειτουργικότητας θα δίνει στο χρήστη τη δυνατότητα να μετακινείται μεταξύ των δικτύων διαφορετικών πρωτοκόλλων, δηλαδή τη δυνατότητα περιαγωγής, ένα στοιχείο το οποίο δεν υπήρχε στις προηγούμενες γενιές. Ο χρήστης με ένα τερματικό θα μπορεί να έχει πρόσβαση σε δίκτυα με διαφορετικά πρότυπα. Η παγκόσμια επικοινωνιακή υποδομή θα μετατραπεί σε ένα ενιαίο δίκτυο. Για το πρόβλημα αυτό έχουν προσδιοριστεί τρεις πιθανές λύσεις. Πρώτη λύση είναι η δημιουργία τερματικών πολλαπλού τρόπου λειτουργίας κάτι το οποίο έχει δοκιμαστεί στο παρελθόν με τα κυψελικά δίκτυα που ήταν συμβατά με τα AMPS και τα CDMA. Η επιλογή τέτοιων τερματικών θα προσφέρει αυξημένη κάλυψη και αξιόπιστη πρόσβαση στις υπηρεσίες σε περίπτωση που σημειωθεί κάποιο πρόβλημα σε ένα ή περισσότερα δίκτυα της περιοχής. Μια δεύτερη λύση είναι η δημιουργία δικτύου κάλυψης, μέσω του οποίου θα έχουν πρόσβαση στο δίκτυο τέταρτης γενιάς. Και η τρίτη λύση είναι η δημιουργία ενός κοινού πρωτοκόλλου πρόσβασης. Αυτή η επιλογή απαιτεί τη χρήση ενός ή δύο τυποποιημένων πρωτοκόλλων πρόσβασης στα ασύρματα δίκτυα. [4]

Τα δίκτυα τέταρτης γενιάς θα υποστηρίζουν ένα φάσμα εύρους ζώνης μέχρι 100 Mbps ή και παραπάνω, με χρόνο ζωής των μπαταριών περίπου μία βδομάδα. Η μεγαλύτερη διάρκεια ζωής των μπαταριών πρόκειται να συνοδευτεί με αλλαγή στο βάρος και στον όγκο τους, στα οποία όπως είναι φυσικό θα υπάρξει μείωση.

Στα δίκτυα τρίτης γενιάς, γινόταν χρήση δικτύων μεταγωγής κυκλώματος και μεταγωγής πακέτων. Στα δίκτυα τέταρτης γενιάς, θα υπάρχει μόνο η μεταγωγή πακέτων.

Ένας ακόμα στόχος των στοιχείων τέταρτης γενιάς είναι η μεταβολή εύρους ζώνης για την ασύρματη πρόσβαση. Η ένωση των διαφόρων δικτύων σε μία πλατφόρμα, θα παρέχει ένα δίκτυο το οποίο θα αποτελείται από διαφορετικά επίπεδα, τα οποία θα προσφέρουν διαφορετικές ταχύτητες, ανάλογα με τη γεωγραφική θέση του χρήστη. Το επίπεδο διανομής, το οποίο θα υποστηρίζει υπηρεσίες μετάδοσης ψηφιακής τηλεόρασης και ραδιοφωνίας, παρέχοντας μέτριες ταχύτητες σε αγροτικές περιοχές με μικρή πυκνότητα. Το κυψελικό δίκτυο, το οποίο θα περιλαμβάνει κυψελικά συστήματα δεύτερης και τρίτης γενιάς σε περιοχές με μεγάλη πυκνότητα, όπως οι πόλεις. Το επίπεδο «θερμών σημείων» το οποίο θα υποστηρίζει εφαρμογές που απαιτούν πολύ υψηλές ταχύτητες σε μικρής έκτασης περιοχές. Το προσωπικό επίπεδο, το οποίο αφορά πολύ μικρές αποστάσεις, όπως το πρότυπο Bluetooth, το οποίο θα αναλυθεί στα επόμενα κεφάλαια και τέλος το σταθερό επίπεδο, το οποίο περιλαμβάνει σταθερά συστήματα πρόσβασης μέσω ασύρματων ζεύξεων.

Επιπλέον, οι σταθμοί πρόσβασης θα πρέπει να χρησιμοποιούν έξυπνες κεραίες προκειμένου να αυξήσουν τη χωρητικότητα του δικτύου. Τέλος, τα δίκτυα τέταρτης γενιάς θα έχουν ταχύτητες της τάξης των 50 – 155 Mbps με σκοπό να υποστηρίζουν τις νέες εφαρμογές. [4]

Στα δίκτυα αυτής της γενιάς πρόκειται να χρησιμοποιηθεί η ορθογωνική πολύπλεξη διαίρεσης συχνότητας (Orthogonal Frequency Division Multiplexing – OFDM), η οποία αναλύεται στα επόμενα κεφάλαια. [4]

Ένα ακόμα κομμάτι των δικτύων τέταρτης γενιάς το οποίο πρέπει να αναλυθεί είναι οι υπηρεσίες και οι εφαρμογές που θα υποστηρίζουν. Οι υπηρεσίες αυτές είναι η τηλεπαρουσία, η πρόσβαση σε πληροφορίες, η επικοινωνία μεταξύ μηχανών, ευφυείς αγορές, ασφάλεια και οι υπηρεσίες βασισμένες στη γεωγραφική θέση. Η τηλεπαρουσία είναι μία εξέλιξη της σημερινής τηλεδιάσκεψης. Θα παρέχει υψηλά επίπεδα ποιότητας υπηρεσιών με ταχύτητες της τάξης των 100 Mbps. Ουσιαστικά, θα είναι υπηρεσίες πραγματικού χρόνου εικονικής πραγματικότητας και θα υποστηρίζουν εφαρμογές εικονικών συνεδριάσεων. Η πρόσβαση σε πληροφορίες, παρ’ όλο που δε θα είναι πραγματικού χρόνου, θα απαιτεί υπηρεσίες με τη μεγαλύτερη δυνατή ταχύτητα για μετάδοση δεδομένων ήχου και βίντεο σε μεγάλες ποσότητες. Επιπλέον, η επικοινωνία μεταξύ των μηχανών για

λόγους συντήρησης ή πρόσθετης νοημοσύνης και λειτουργικότητας κι οι ευφυείς αγορές με τη βοήθεια των οποίων θα μπορούμε να εισερχόμαστε μέσα σε ένα κατάστημα και θα ενημερωνόμαστε για τα προϊόντα και τις τιμές τους. Όπως και σήμερα η ασφάλεια είναι μία από τις βασικότερες υπηρεσίες. Οι νέες υπηρεσίες ασφάλειας θα πρέπει να εξασφαλίζουν τη μυστικότητα των προσωπικών δεδομένων των χρηστών, ώστε να φτάσουν σε βαθμό να πραγματοποιούνται χωρίς φόβο περισσότερες τραπεζικές εργασίες. Τέλος, με τις νέες υπηρεσίες βασισμένες στη γεωγραφική θέση, θα μπορείτε να εντοπίζετε ακριβώς τη θέση ενός τερματικού και όχι μόνο την κυψέλη στην οποία αυτό ανήκει, όπως συμβαίνει με τα τωρινά συστήματα. [4]

Οι μελλοντικές τάσεις απαιτούν την παγκοσμιοποίηση των προϊόντων, των υπηρεσιών και των επιχειρήσεων. Επίσης, η δημιουργία νέων συσκευών, οι οποίες θα μπορούν να παίρνουν κάποιες αποφάσεις από μόνες τους διαθέτοντας φυσικά και τον κατάλληλο εξοπλισμό, ώστε να μπορούν να επικοινωνούν και με άλλες συσκευές. Επιπλέον, υπάρχει η τάση για κατάργηση των έντυπων μέσων μαζικής ενημέρωσης και λήψη όλων των πληροφοριών μέσω του διαδικτύου. Αυτό θα έχει σαν αποτέλεσμα τη λήψη μεγάλων ποσοτήτων πληροφοριών, με συνέπεια την ανάγκη για φιλτράρισμα και έλεγχο αυτών.

Κλείνοντας την ενότητα των κυψελικών δικτύων τέταρτης γενιάς, είναι πρέπον να αναφέρουμε ότι ήδη έχει δημιουργηθεί ομάδα ερευνητών για τη δημιουργία των δικτύων πέμπτης γενιάς. Στον πίνακα που ακολουθεί είναι συγκεντρωμένα τα χαρακτηριστικά όλων των γενεών που υπάρχουν, καθώς επίσης και οι προτάσεις για την πέμπτη γενιά.

**ΠΙΝΑΚΑΣ 5: ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΠΕΝΤΕ ΓΕΝΕΩΝ**

| Technology / Features | 1G | 2G/2.5G | 3G | 4G | 5G |
|---|---|---|---|---|---|
| **Start/ Deployment** | 1970/ 1984 | 1980/ 1999 | 1990/ 2002 | 2000/ 2010 | 2010/ 2015 |
| **Data Bandwidth** | 2 kbps | 14.4-64 kbps | 2 Mbps | 200 Mbps to 1 Gbps for low mobility | 1 Gbps and higher |
| **Standards** | AMPS | 2G: TDMA, CDMA, GSM 2.5G: GPRS, EDGE, 1xRTT | WCDMA, CDMA-2000 | Single unified standard | Single unified standard |
| **Technology** | Analog cellular technology | Digital cellular technology | Broad bandwidth CDMA, IP technology | Unified IP and seamless combination of broadband, LAN/WAN/ PAN and WLAN | Unified IP and seamless combination of broadband, LAN/WAN/PAN /WLAN and wwww |
| **Service** | Mobile telephony (voice) | 2G: Digital voice, short messaging 2.5G: Higher capacity packetized data | Integrated high quality audio, video and data | Dynamic information access, wearable devices | Dynamic information access, wearable devices with AI capabilities |
| **Multiplexing** | FDMA | TDMA, CDMA | CDMA | CDMA | CDMA |
| **Switching** | Circuit | 2G: Circuit 2.5G: Circuit for access network & air interface; Packet for core network and data | Packet except circuit for air interface | All packet | All packet |
| **Core Network** | PSTN | PSTN | Packet network | Internet | Internet |
| **Handoff** | Horizontal | Horizontal | Horizontal | Horizontal and Vertical | Horizontal and Vertical |

## 2.9 ΔΟΡΥΦΟΡΙΚΑ ΔΙΚΤΥΑ

Η δημιουργία δορυφορικών συστημάτων ξεκίνησε από την ανάγκη εξασφάλισης επικοινωνίας σε οποιονδήποτε σημείο του πλανήτη, την εποχή που ακόμα σχεδιάζονταν τα κυψελικά δίκτυα δεύτερης γενιάς. Αν και κατάφεραν την προσδοκία τους αυτή, τα κυψελικά δίκτυα εξελίχτηκαν πολύ γρήγορα, προσφέροντας πολύ φθηνότερες υπηρεσίες. Όσες εταιρίες ασχολήθηκαν με αυτόν τον τομέα των επικοινωνιών και δεν έφτασαν στη χρεοκοπία, πρόσφεραν υπηρεσίες σε ειδικές περιπτώσεις, όπως στο στρατό, σε ανθρωπιστικές αποστολές και γενικότερα, όπου δεν υπάρχει κάλυψη των κυψελικών δικτύων. Μερικές από αυτές τις εταιρίες είναι:

- Iridium
- Wireless Matrix
- Global Star
- Teledesic
- ICO
- Orbcomm
- Inmarsat
- Hughes Network Systems
- Thuraya Satellite
- Asia Cellular Satellite

## 2.10 ΣΥΝΟΨΗ

Στο κεφάλαιο αυτό αναλύθηκαν οι γενιές των ασύρματων κυψελικών δικτύων ξεκινώντας από μια μικρή εισαγωγή στην έννοια της κυψέλης και στη συνέχεια στην περιγραφή των τεσσάρων γενεών και της γενιάς 2,5 G και των βασικότερων προτύπων της καθεμίας. Τέλος, γίνεται μία απλή αναφορά στις δορυφορικές επικοινωνίες κλείνοντας έτσι τα εισαγωγικά κεφάλαια και συνεχίζοντας με την ανάλυση των προτύπων της ομάδας 802.11.

# 3. ΤΟ ΠΡΟΤΥΠΟ 802.11

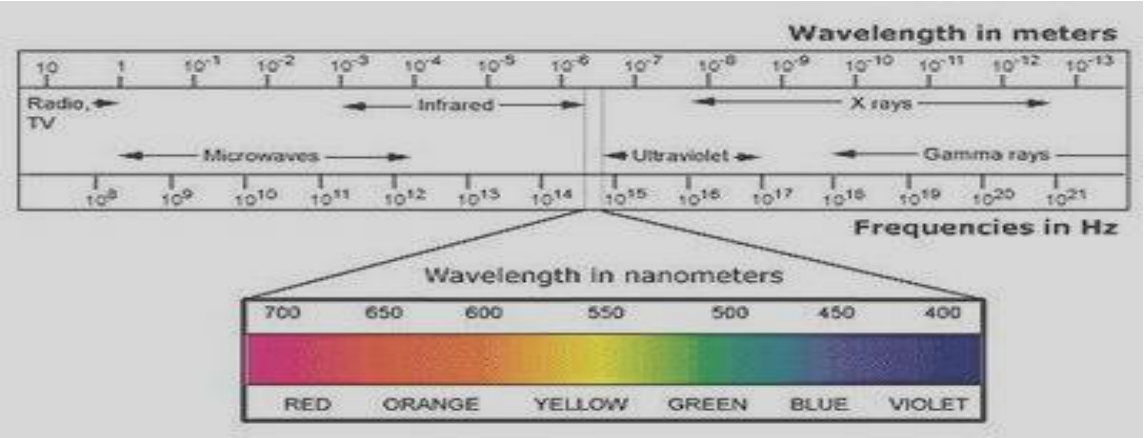
## 3.1 ΕΙΣΑΓΩΓΗ

Τα ασύρματα τοπικά Δίκτυα (Wireless Local Area Networks, WLAN) επιτρέπουν την επικοινωνία μεταξύ των χρηστών και την ανταλλαγή δεδομένων χωρίς να χρειάζεται η χρησιμοποίηση καλωδίων Ethernet όπως στην ενσύρματη επικοινωνία. Η ευρέως διαδεδομένη χρήση των φορητών υπολογιστών, οδήγησε στην ανάγκη για ευκινησία σε πολλούς χώρους και στη τοπική και στη διαδικτύου σύνδεση.

Στα ασύρματα δίκτυα η διάδοση του σήματος δεν είναι περιορισμένη σε μια γεωγραφική περιοχή, για αυτό δημιουργούνται παρεμβολές από γειτονικά ασύρματα δίκτυα που εκπέμπουν στην ίδια συχνότητα. Παρακάτω αναφέρονται: οι έννοιες του ηλεκτρομαγνητικού φάσματος, των ρυθμιστικών φορέων και τα πρότυπα του 802.11 για τα ασύρματα δίκτυα.

## 3.2 ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΟ ΦΑΣΜΑ

Το Ηλεκτρομαγνητικό Φάσμα είναι το εύρος συχνοτήτων των ηλεκτρομαγνητικών κυμάτων, το οποίο είναι χωρισμένο σε ζώνες (bands). Οι ζώνες δεν έχουν φυσική δομή αλλά χρησιμεύουν για να διαχωριστούν οι ιδιότητες των περιοχών του φάσματος, για αυτό και δεν υπάρχει διάκριση μεταξύ των γειτονικών ζωνών. Οι ζώνες αυτές είναι: τα ραδιοκύματα, τα μικροκύματα, τα υπέρυθρα κύματα, το ορατό φως, οι υπεριώδεις ακτίνες, οι ακτίνες Χ και οι Ακτίνες Γάμμα. Παρακάτω αναλύονται τα πιο σημαντικά χαρακτηριστικά των ζωνών αυτών για τα ασύρματα συστήματα επικοινωνιών[14][15].




**ΕΙΚΟΝΑ 25: ΑΝΑΛΥΣΗ ΤΩΝ ΠΙΟ ΣΗΜΑΝΤΙΚΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΤΩΝ ΖΩΝΩΝ ΓΙΑ ΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ**

- **Ραδιοκύματα**. Τα ραδιοκύματα ανήκουν στο χαμηλότερο τμήμα του φάσματος, έχουν συχνότητα μερικών kHz. Για την εκπομπή τηλεοπτικού και ραδιοφωνικού προγράμματος χρησιμοποιούνται οι περιοχές με χαμηλή συχνότητα για μεγαλύτερη εμβέλεια. Στα ασύρματα συστήματα επικοινωνιών χρησιμοποιούνται οι περιοχές με υψηλή συχνότητα για γρήγορη μετάδοση δεδομένων.
- **Μικροκύματα**. Στην μικροκυματική ζώνη τα κύματα έχουν μικρότερο μήκος από τα κύματα των χαμηλότερων συχνοτήτων της ζώνης ραδιοκυμάτων και περιλαμβάνει τις περιοχές των υψηλών συχνοτήτων της ζώνης ραδιοκυμάτων (UHF,SHF,EHF).Τα ασύρματα συστήματα χρησιμοποιούν συχνά τα μικροκύματα γιατί προσφέρουν μεταφορά δεδομένων υψηλών ταχυτήτων.

**ΠΙΝΑΚΑΣ 6: ΣΥΧΝΟΤΗΤΕΣ ΚΑΙ ΜΗΚΟΣ ΚΥΜΑΤΟΣ ΑΕΡΑ[13][14]**

| Συχνότητα και μήκος κύματος αέρα | Όνομα Ζώνης | Εφαρμογές |
|---|---|---|
| <3 kHz<br>100,000 - 100 km | Υπερβολικά Χαμηλής Συχνότητας<br>(Extremely Low Frequency, ELF) | Επικοινωνίες υποβρυχίων |
| 3 kHz - 30 kHz<br>100 - 10 km | Πολύ Χαμηλής Συχνότητας<br>(Very Low Frequency, VLF) | Θαλάσσιες επικοινωνίες, μόνιτορ για τον ρυθμό της καρδιάς, Γεωφυσική, στρατιωτικές και ναυτιλιακές εφαρμογές, ιατρικά εμφυτεύματα |
| 20 kHz - 300 kHz<br>10 km - 1 km | Χαμηλής Συχνότητας (Low Frequency, LF)<br>ή Μεγάλο μήκος κύματος (Long Wave,LW) | Ραδιοφωνία AM, στρατιωτικές και ναυτιλιακές εφαρμογές, ιατρικά εμφυτεύματα |

| Συχνότητα και μήκος κύματος αέρα | Όνομα Ζώνης | Εφαρμογές |
|---|---|---|
| 300 kHz - 3 MHz<br>1 km - 100 m | Μέσης Συχνότητας (Medium Frequency,MF)<br>ή Μεσαίου μήκος κύματος (Medium Wave,LW) | Ραδιοφωνία AM, στρατιωτικές και ναυτιλιακές εφαρμογές, ιατρικά εμφυτεύματα |
| 3 - 30 MHz<br>100 - 10 m | Υψηλής Συχνότητας (High Frequency,HF)<br>ή Μικρού μήκος κύματος (Short Wave,SW) | Ραδιοφωνία AM, στρατιωτικές και ναυτιλιακές εφαρμογές, ιατρικά εμφυτεύματα |
| 30 - 300 MHz<br>10 m - 1 m | Πολύ Υψηλής Συχνότητας ( Very High Frequency, VHF) | Ραδιοφωνία FM,Τηλεόραση, αμυντικά συστήματα |
| 300 MHz -3 GHz<br>1 m - 100 mm | Υπερβολικά Υψηλής Συχνότητας (Ultra-High Frequency, UHF) | Τηλεόραση, μικροκυματικοί αναμεταδότες, κυψελική τηλεφωνία, Ασύρματα Τοπικά Δίκτυα, Bluetooth,GPS,ραντάρ |
| 3–30 GHz<br>100 mm - 10 mm | Superhigh Frequencies ,SHF | Μικροκυματικές συσκευές, Ασύρματα Τοπικά Δίκτυα, Δορυφόροι, ραντάρ,WiMax, ραδιοαστρονομία, μικροκυματικοί αναμεταδότες |

| Συχνότητα και μήκος κύματος αέρα | Όνομα Ζώνης | Εφαρμογές |
|---|---|---|
| 30-300 GHz<br>10 mm - 1 mm | Extremely High Frequencies (EHF) | Δορυφόροι, ραντάρ, ραδιοαστρονομία, μικροκυματικοί αναμεταδότες |

- **Υπέρυθρα κύματα (IR)**.Η υπέρυθρη ακτινοβολία έχει μικρότερη συχνότητα από το φάσμα του κόκκινου ορατού φως και η συχνότητα εκπομπής της εξαρτάται από την θερμοκρασία των αντικειμένων[14].

## 3.3 ΔΙΑΧΕΙΡΙΣΗ ΦΑΣΜΑΤΟΣ

Η διαχείριση του φάσματος είναι η διαδικασία στην οποία αποφεύγονται οι παρεμβολές από ένα σύστημα σε ένα άλλο. Η διαχείριση του φάσματος στα ασύρματα δίκτυα χρειάζεται διότι δεν υπάρχει περιορισμός στη διάδοση των σημάτων και το μέσο μπορεί να χρησιμοποιείται ταυτόχρονα από πολλά συστήματα.

Οι περιοχές του φάσματος χωρίζονται σε δύο μεγάλες κατηγορίες στις αδειοδοτημένες και στις μη-αδειοδοτημένες περιοχές. Η κατηγορία των αδειοδοτημένων περιοχών παρέχει αποκλειστικά δικαιώματα της περιοχής των συχνοτήτων στους κατόχους αυτής της άδειας. Η άλλη κατηγορία περιλαμβάνει την ελεύθερη χρήση των μη-αδειοδοτημένων περιοχών του φάσματος με περιορισμούς χρήσης όπως την χρήση της τεχνολογίας διάχυσης φάσματος και την μετάδοση χαμηλής ισχύος[14].

Σε κάθε χώρα η διαχείριση του φάσματος γίνεται από τον αντίστοιχο ρυθμιστικό κυβερνητικό φορέα. Παρότι τα τελευταία χρόνια γίνεται προσπάθεια ώστε κάθε χώρα να ακολουθεί ενιαίους κανόνες, υπάρχουν χώρες που δεν τους ακολουθούν.

### 3.3.1 Οργανισμός Τηλεπικοινωνιών των Ηνωμένων Εθνών

Το 1865, ιδρύθηκε ο Διεθνής Οργανισμός Τηλεπικοινωνιών (International Telecommunications Union, ITU) των Ηνωμένων Εθνών, ο οποίος είναι υπεύθυνος για θέματα τεχνολογίας των επικοινωνιών και των πληροφοριών. Ο Διεθνής Οργανισμός Τηλεπικοινωνιών χωρίζεται στους παρακάτω τομείς[4][10]:

- Ο Τομέας Ραδιοεπικοινωνιών της ITU (ITU-R). Ο οποίος είναι υπεύθυνος για την παγκόσμια διαχείριση του φάσματος των ραδιοσυχνοτήτων και για την δημιουργία κατάλληλων προτύπων για την καλύτερη διαχείριση του φάσματος από ραδιοεπικοινωνιακά συστήματα,
- ο Τομέας Τυποποίησης Τηλεπικοινωνιών της ITU (ITU-T). Ο οποίος συνθέτει τα πρότυπα για την υποδομή των Τεχνολογιών Ενημέρωσης και Επικοινωνιών (ICT, Information and Communications Technologies),
- ο Τομέας για την ανάπτυξη των Τηλεπικοινωνιών της ITU (ITU-D).Ο οποίος είναι υπεύθυνος για την δημιουργία κανονισμών και τακτικής,
- και ο τομέας ITU TELECOM που ενώνει σημαντικούς ανθρώπους από την Τεχνολογία Ενημέρωσης και Επικοινωνιών και ρυθμιστικές αρχές για την δικτύωση, την ανταλλαγή ιδεών και τη βιομηχανική πρόοδο.

Για την ανάπτυξη δικτύων και υπηρεσιών για κυβερνήσεις και για τον ιδιωτικό τομέα, ο Διεθνής Οργανισμός Τηλεπικοινωνιών αποτελεί σημείο αναφοράς. Οι οδηγίες που εκδίδονται από τον οργανισμό δεν είναι υποχρεωτικές και περιλαμβάνουν συγκεκριμένες περιοχές του φάσματος από συγκεκριμένες εφαρμογές και η χρησιμοποίηση ίδιου εξοπλισμού για όλες τις χώρες. Σε αυτόν τον οργανισμό ανήκουν η Αμερική, η Ευρώπη, η Αφρική και η Ασία.

Ο Διεθνής Οργανισμός Τηλεπικοινωνιών χωρίζει τη γη σε διοικητικές περιοχές: στην ***A*** που περιλαμβάνει την Αμερική, στην ***B*** με την Δυτική Ευρώπη, στην ***C*** με την Ανατολική Ευρώπη και την Βόρεια Ασία, στην ***D*** με την Αφρική και στην ***E*** με την Ασία και την Αυστραλία. Με βάση τους Ράδιο - Κανονισμούς του Διεθνή Οργανισμού Τηλεπικοινωνιών, η γη διαιρείται σε άλλες τρεις περιοχές[4][10] :

- Η Περιοχή 1 περιλαμβάνει την Ευρώπη, την Μέση Ανατολή, την Αφρική και την Ρωσία,
- η Περιοχή 2 περιλαμβάνει την Βόρεια και τη Νότια Αμερική και τον Ειρηνικό

- η Περιοχή 3 περιλαμβάνει την Ασία, την Αυστραλία και την Νοτιοανατολική Ασία.

Οι ζώνες συχνοτήτων που αναφέρθηκαν παραπάνω έχουν θεσπιστεί από τον Διεθνή Οργανισμό Τηλεπικοινωνιών, όπως και οι αδειοδοτημένες συχνότητες που αφορούν τα ασύρματα δίκτυα. Οι ζώνες συχνοτήτων που χρησιμοποιούνται για βιομηχανική, για ιατρική, για επιστημονική και για εκπαιδευτική χρήση (Industrial, Scientific and Medical, ISM), οι οποίες καθορίστηκαν από την ITU-R και που τις ακολουθούν η FCC, ο CEPT και άλλοι εθνικοί ρυθμιστικοί φορείς, είναι στα[4][10]:

- 6.765–6.795 MHz
- 13.553–13.567 MHz
- 26.957–27.283 MHz
- 40.66–40.70 MHz
- 433.05–434.79 MHz
- 902–928 MHz
- 2.400–2.500 GHz
- 5.725–5.875 GHz
- 24–24.25 GHz
- 61–61.5 GHz
- 122–123 GHz
- 244–246 GHz που χρησιμοποιούνται για συσκευές ISM εκτός από συστήματα επικοινωνιών.

### 3.3.2 Ομοσπονδιακή Επιτροπή Επικοινωνιών Αμερικής

Το 1934, ιδρύθηκε η Ομοσπονδιακή Επιτροπή Επικοινωνιών (Federal Communications Committee,FCC) των Ηνωμένων Πολιτειών Αμερικής[7]. Η FCC είναι μια ανεξάρτητη κυβερνητική επιτροπή, η οποία ελέγχει όλες τις εθνικές επικοινωνίες (με την χρήση καλωδίων, των ραδιοσυχνοτήτων, των δορυφόρων αλλά και τις τηλεοπτικές και ραδιοφωνικές συχνότητες) και θέσπισε κάποιες οδηγίες και κάποιους κανόνες ώστε να ελέγχει όσον το δυνατόν καλύτερα την “κυκλοφορία” των συχνοτήτων του ασύρματου εξοπλισμού[14].

Κατά την δεκαετία του 1980, που δημιουργήθηκαν νέα προϊόντα των ασύρματων δικτύων, οι αρχές δεν χορηγούσαν εύκολα άδεια στους κατασκευαστές τους γιατί δεν γνώριζαν αν θα είχαν επιτυχία. Η FCC αποφάσισε να εγκρίνει την δημόσια ελεύθερη χρήση των ISM ζωνών συχνοτήτων για τα ασύρματα τοπικά δίκτυα με αποτέλεσμα την μείωση του κόστους και του χρόνου για την εγκατάσταση και την λειτουργία τους. Με τους κανόνες της FCC, τα ασύρματα τοπικά δίκτυα μεταδίδουν με χαμηλή ισχύ και χρησιμοποιούν τη διασπορά φάσματος για να αποφευχθούν οι παρεμβολές με άλλα προϊόντα που εκπέμπουν στις ζώνες αυτές (47 Part 15)[7]. Οι ζώνες αυτές είναι:

- στα 900 MHz: από 902 ως 928 MHz,
- στα 2.4 GHz: από 2.403 ως 2.483 GHz και
- στα 5 GHz που ανήκουν στην μη-αδειοδοτούμενη εθνική υποδομή πληροφοριών (National Information Infrastructure ,U-NII) και χωρίζονται (47 RFC. Part 15 Subpart E)[7]:

- στην χαμηλή ζώνη που περιέχει τις συχνότητες 5.150-5.250 GHz,
- στην μεσαία ζώνη που περιέχει τις συχνότητες 5.250-5.350 GHz,
- στην παγκόσμια ζώνη που περιέχει τις συχνότητες 5.47-5.725 (FCC NPRM 03-110 Part 15) και
- στην υψηλή ζώνη που περιέχει τις συχνότητες 5.725-5.825 GHz.

Οι ISM ελεύθερες ζώνες των 900 MHz και των 2.4 GHz είναι πιο συνωστισμένες και έχουν μεγαλύτερο ποσοστό παρεμβολών από την ζώνη των 5 GHz. Στη ζώνη των 2.4 GHz, το 802.11 παρεμβάλλεται από τον φούρνο μικροκυμάτων και άλλες συσκευές όταν οι συχνότητες τους διασταυρωθούν. Υπάρχουν και άλλα παραδείγματα παρεμβολών του 802.11 όπως από το Bluetooth και άλλα.

### 3.3.3 CEPT

Το 1959, ιδρύθηκε η Διάσκεψη των Ευρωπαϊκών Ταχυδρομικών και Τηλεπικοινωνιακών Διοικήσεων στην Ευρωπαϊκή Ένωση (CEPT, Conference of European Postal and Telecommunications Administrations), η οποία είναι δημιουργός τακτικής και κανονισμών των Τηλεπικοινωνιών και των Ταχυδρομείων. Στις δραστηριότητες της περιλαμβάνετε η συνεργασία τυποποίησης σε εμπορικά, σε λειτουργικά, σε ρυθμιστικά και σε τεχνικά ζητήματα.

Οι χρονολογίες και τα μέλη που εισχώρησαν στη Διάσκεψη των Ευρωπαϊκών Ταχυδρομικών και Τηλεπικοινωνιακών Διοικήσεων παρουσιάζονται στον ακόλουθο πίνακα[4].

**ΠΙΝΑΚΑΣ 7: ΧΡΟΝΟΛΟΓΙΕΣ ΚΑΙ ΜΕΛΗ ΠΟΥ ΕΙΣΧΩΡΗΣΑΝ ΣΤΗ ΔΙΑΣΚΕΨΗ ΤΩΝ ΕΥΡΩΠΑΙΚΩΝ ΤΑΧΥΔΡΟΜΙΚΩΝ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΟΙΚΗΣΕΩΝ**

| ΧΡΟΝΟΛΟΓΙΑ | ΜΕΛΗ |
|---|---|
| 1959 | Αυστρία, Δανία, Φινλανδία, Βέλγιο, Γαλλία, Ιρλανδία, Ισλανδία, Ολλανδία, Ιταλία, Μάλτα, Λουξεμβούργο, Αγγλία, Γερμανία, Ελλάδα, Νορβηγία, Πορτογαλία, Ισπανία, Σουηδία, Ελβετία, Τουρκία |
| 1963 | Βατικανό, Λιχτενστάιν, Κύπρος |
| 1967 | Σερβία, Σαν Μαρίνο |
| 1969 | Μονακό |
| 1970 | Μάλτα |
| 1990 | Βουλγαρία, Ουγγαρία, Πολωνία, Ρουμανία |
| 1991 | Αλβανία |
| 1992 | Κροατία, Λιθουανία |
| 1993 | Τσεχία, Εσθονία, Μολδαβία, Σλοβακία, Σλοβενία |
| 1994 | Βοσνία Ερζεγοβίνη, Λετονία, Ρωσία |
| 1995 | Ανδόρα, Σκόπια, Ουκρανία |
| 2001 | Αζερμπαϊτζάν |
| 2002 | Σερβία |
| 2003 | Ρωσική Ομοσπονδία (Russian Federation) |
| 2006 | Γεωργία |

| ΧΡΟΝΟΛΟΓΙΑ | ΜΕΛΗ |
|---|---|
| 2007 | Μαυροβούνιο |

Στην Ευρώπη οι ISM ζώνες συχνοτήτων για τα ασύρματα δίκτυα είναι στα:

- 2.4 GHz: από 2.403 ως 2.483 GHz ,
- 5 GHz: από 5.150 ως 5350 GHz και από 5.470 ως 5.725 GHz
- και στην ζώνη των 902 MHz που χρησιμοποιείται για την επικοινωνία των κυψελικών συστημάτων τηλεφώνων GSM.

### 3.3.4 ETSI

Το 1988, ιδρύθηκε μια μη-κερδοσκοπική οργάνωση, το Ινστιτούτο Τυποποίησης Ευρωπαϊκών Τηλεπικοινωνιών (ETSI, European Telecommunications Standards Institute) από το CEPT. Στο ETSI μεταφέρθηκαν οι διαδικασίες τυποποίησης των Τεχνολογιών Ενημέρωσης και Επικοινωνιών (ICT, Information and Communications Technologies), που περιλαμβάνουν τεχνολογίες και πρότυπα σταθερών, κινητών, σύγκλισης, ραδιοτηλεοπτικών μεταδόσεων και Διαδικτύου. Τα μέλη του Ινστιτούτου Τυποποίησης Ευρωπαϊκών Τηλεπικοινωνιών είναι περίπου 700 από 60 χώρες εντός και εκτός της Ευρώπης[6].

### 3.3.5 ΕΕΤΤ & ELOT

Ο εθνικός ρυθμιστικός φορέας της Ελλάδος για την διαχείριση των συχνοτήτων (με τις οδηγίες του CEPT) είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) που είναι υπεύθυνη για την εποπτεία και την έγκριση των προϊόντων των εταιρειών σταθερής και κινητής τηλεφωνίας, των ασύρματων επικοινωνιών, του Διαδικτύου και των υπηρεσιών ταχυδρομείων και ταχυμεταφοράς. Μερικές από τις δραστηριότητες της Εθνικής Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων είναι[2]:

- διαχείριση του Εθνικού Σχεδίου Αριθμοδότησης
- παραχώρηση δικαιωμάτων χρήσης ραδιοσυχνοτήτων και αδειών στους, παρόχους των ηλεκτρονικών επικοινωνιών,

- εκχώρηση Ονομάτων Δικτυακών Τόπων με Κατάληξη [ .gr ],
- συνεργασία με τις Ρυθμιστικές Αρχές των λοιπών κρατών μελών της Ευρωπαϊκής Ένωσης ή τρίτων κρατών, καθώς και με κοινοτικούς ή διεθνείς φορείς σε θέματα των αρμοδιοτήτων της,
- ρύθμιση των θεμάτων της ηλεκτρονικής υπογραφής,
- ρύθμιση των θεμάτων πρόσβασης και διασύνδεσης και
- διαχείριση του εμπορικού φάσματος συχνοτήτων εκτός από την Τηλεόραση και το Ραδιόφωνο.

Στην Ελλάδα οι ISM ζώνες συχνοτήτων είναι ίδιες, αφού ακολουθούν τις συστάσεις της Διάσκεψης των Ευρωπαϊκών Ταχυδρομικών και Τηλεπικοινωνιακών Διοικήσεων της Ευρώπης.

Στην Ελλάδα για τις διαδικασίες τυποποίησης είναι υπεύθυνος ο Ελληνικός Οργανισμός Τυποποίησης Α.Ε. (Hellenic Organization for Standardization, ELOT) που ακολουθεί τις συστάσεις του Ινστιτούτου Τυποποίησης Ευρωπαϊκών Τηλεπικοινωνιών[1].

## 3.4 ΤΟ ΠΡΟΤΥΠΟ IEEE 802.11

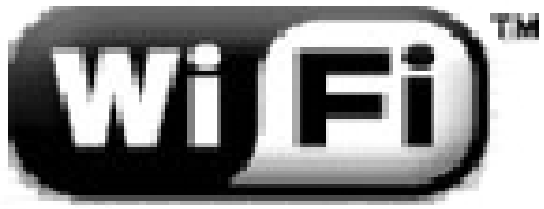
Το 1963 δημιουργήθηκε το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers, IEEE) με την συγχώνευση του Αμερικάνικου Ινστιτούτου Ηλεκτρολόγων Μηχανικών (American Institute of Electrical Engineers, AIEE) και του Ινστιτούτο ΡαδιοΜηχανικών (Institute of Radio Engineers, IRE) και περιλαμβάνει 380000 μέλη από 150 χώρες[11].

Το IEEE είναι ένας Διεθνής μη-κερδοσκοπικός οργανισμός που προωθεί την δημιουργία, την ανάπτυξη, την ενσωμάτωση και την εφαρμογή της ηλεκτρικής και της ηλεκτρονικής τεχνολογίας, παρέχει τεχνικές και επαγγελματικές πληροφορίες για τα αεροδιαστημικά συστήματα, τους υπολογιστές, τις τηλεπικοινωνίες και άλλες προς όφελος της ανθρωπότητας. Το IEEE διαθέτει γύρω στα 900 ολοκληρωμένα και 400 υπό ανάπτυξη πρότυπα[11][17].

Το 1990, το IEEE και ο Διεθνής Οργανισμός Τυποποίησης (International Standards Organization, ISO) όρισε σε μια ομάδα εργασίας 802.11 την ανάπτυξη

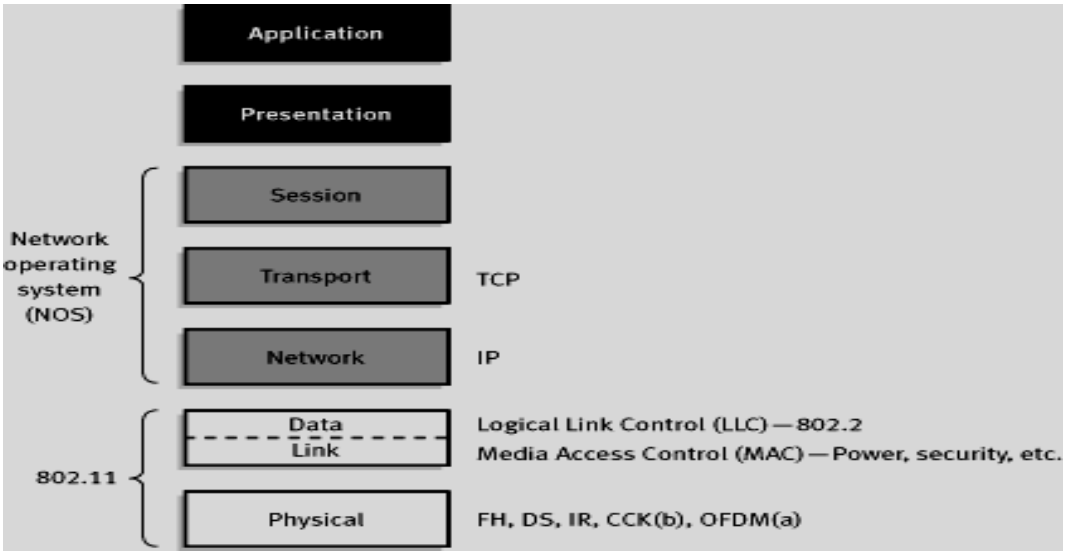
του παγκόσμιου προτύπου 802.11 για την ασύρματη δικτύωση[13][16]. Το IEEE 802.11 είναι μια ομάδα από μεγάλο πλήθος προτύπων, ο οποίος αυξάνεται όσο η τεχνολογία των ασύρματων δικτύων εξελίσσεται. Η ομάδα των προτύπων IEEE 802.11 περιλαμβάνουν δίπλα από το 802.11 και ένα πεζό λατινικό γράμμα και το πλήθος τους περιλαμβάνει τα περισσότερα γράμματα της αγγλικής αλφαβήτου[12].

Τα προϊόντα του πρότυπου IEEE 802.11, πιστοποιούνται από την Wi-Fi Alliance για τη διαλειτουργικότητα τους και για τη χρήση τους στα ασύρματα τοπικά δίκτυα. Η Wi-Fi Alliance (πρώην WECA,Wireless Ethernet Compatibility Alliance) δημιουργήθηκε το 1999 από κατασκευαστές και προμηθευτές και είναι ένας μη-κερδοσκοπικός οργανισμός διεθνούς εμπορίου που εξασφαλίζει ένα παραπάνω επίπεδο διαλειτουργικότητας των επικυρωμένων Wi-Fi (Wireless Fidelity) προϊόντων από τα 802.11 πρότυπα και έχουν την σφραγίδα πιστοποίησης το παρακάτω λογότυπο[19].




**ΕΙΚΟΝΑ 26:13 Wi-Fi ΛΟΓΟΤΥΠΟ**

Ο Διεθνής Οργανισμός Τυποποίησης (International Organization of Standardization, ISO) είναι υπεύθυνος για την δημιουργία του μοντέλου Αναφοράς της Ανοιχτής Διασύνδεσης Συστημάτων (Open System Interconnection, OSI) είναι το πρότυπο για την διαλειτουργικότητα της επικοινωνίας δεδομένων. Το μοντέλο αυτό χωρίζεται σε εφτά επίπεδα τα οποία έχουν διαφορετικές και ανεξάρτητες μεταξύ τους λειτουργίες ώστε οι αλλαγές σε ένα επίπεδο να μην επηρεάζουν τα υπόλοιπα[1][15]. Τα επίπεδα αυτά φαίνονται στην εικόνα που ακολουθεί.




**ΕΙΚΟΝΑ 27: ΜΟΝΤΕΛΟ ΑΝΑΦΟΡΑΣ OSI**

- Το επίπεδο 7 είναι το επίπεδο Εφαρμογών και καθορίζει τη δικτύωση των εφαρμογών που είναι ορατές στον χρήστη υπολογιστών,
- το επίπεδο 6 είναι το επίπεδο Παρουσίασης και απλοποιεί τη μετατροπή των δεδομένων για τις εφαρμογές. Αποτελεί την συμπίεση δεδομένων, τον μετασχηματισμό των κωδικών και των διαφόρων μορφών αρχείων σε δυαδική ακολουθία,
- το επίπεδο 5 είναι το επίπεδο Συνόδου και δημιουργεί, ελέγχει και τερματίζει τις συνόδους μεταξύ της δικτύωσης των Εφαρμογών,
- το επίπεδο 4 είναι το επίπεδο Μεταφοράς και παρέχει τις διαδικασίες που εξασφαλίζει την αξιοπιστία στην από άκρου εις άκρου επικοινωνία μεταξύ δύο δικτυακών συσκευών,
- το επίπεδο 3 είναι το επίπεδο Δικτύου και παρέχει τη δρομολόγηση δεδομένων μέσω του δικτύου,
- το επίπεδο 2 είναι το επίπεδο Ζεύξης και Δεδομένων και καθορίζει πως ταξιδεύουν τα δεδομένα σε δυο συσκευές δικτύου, παρέχει συγχρονισμό των συσκευών, ανίχνευση και διόρθωση σφαλμάτων ώστε τα δεδομένα να μην αλλοιωθούν και
- το επίπεδο 1 είναι το Φυσικό επίπεδο και καθορίζει τη φυσική σύνδεση μεταξύ δύο συσκευών.

Το πρότυπο IEEE 802.11 αφορά τα δύο χαμηλότερα επίπεδα που είναι το φυσικό επίπεδο και το υπόστρωμα MAC (Medium Access Control) του επιπέδου σύνδεσης δεδομένων (Data Link Layer). Αυτά έχουν τροποποιηθεί ώστε κάθε εφαρμογή να δουλεύει σε συσκευές 802.11 όπως θα δούλευε πάνω από το Ethernet. Η διαστρωμάτωση του Φυσικού επιπέδου και το υπόστρωμα MAC αναλύονται στα κεφάλαια που ακολουθούν.

### 3.4.1 Εισαγωγή στο πρότυπο IEEE 802.11

Το 1997, δημιουργήθηκε το πρότυπο IEEE 802.11, το οποίο είναι και το αρχικό, υποστηρίζει ρυθμούς μετάδοσης δεδομένων της τάξεως 1 και 2 Mbps. Η μετάδοση σήματος γίνεται είτε με διαμόρφωση GFSK 2 level για ρυθμούς μετάδοσης 1 Mbps και GFSK 4 level σε ρυθμούς μετάδοσης 2 Mbps. Με σκοπό την ελαχιστοποίηση κατά το δυνατόν του θορύβου στενής ζώνης, χρησιμοποιείται κωδικοποίηση με μεθόδους διασποράς φάσματος, είτε με τις μεθόδους μεταπήδησης συχνότητας (FHSS,Frequency Hopping Spread Spectrum) είτε άμεσης ακολουθίας (DSSS, Direct Sequence Spread Spectrum) που χρησιμοποιούν την ISM ζώνη με συχνότητες από 2.4 ως 2.4835. Επίσης το IEEE 802.11 χρησιμοποιεί και την τεχνική διάχυση της υπέρυθρης ακτινοβολίας κατά την μετάδοση [9][14].

**ΠΙΝΑΚΑΣ 8: ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΠΡΟΤΥΠΟΥ 802.11**

| ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ | ΠΕΡΙΓΡΑΦΗ 802.11 |
|---|---|
| Εφαρμογή | Ασύρματη Δικτύωση Δεδομένων |
| Ρυθμός Μετάδοσης | 1-2 Mbps |
| Τυπική Ζώνη Συχνοτήτων | ISM 2.4 ως 2.4835 GHz |
| Τεχνική | FHSS or DSSS, CRC-16 στην επικεφαλίδα |
| Ασφάλεια | 128-bit WEP |
| Επίπεδο Σύνδεσης | Carrier Sense Multiple Access με Collision Avoidance (CSMA/CA) με request to send (RTS/clear to send (CTS) |

### 3.4.2 Το πρότυπο IEEE 802.11a

Με την τροποποίηση του αρχικού προτύπου IEEE 802.11, το 1999 δημιουργήθηκε το πρότυπο IEEE 802.11a που υποστηρίζει ρυθμούς μετάδοσης 6, 9, 12, 18, 24, 36, 48 και προαιρετικά μέχρι 54 Mbps στη ζώνη συχνοτήτων των 5 GHz U-NII [9][14].

Στο IEEE 802.11a χρησιμοποιούνται διαφορετικές διαμορφώσεις ανάλογα με τους ρυθμούς μετάδοσης:

- για ρυθμούς μετάδοσης 6 και 9 Mbps χρησιμοποιείται η διαμόρφωση δυαδικής μεταβολής μετατόπισης φάσης (BPSK, Binary Phase Shift Keying),
- για ρυθμούς μετάδοσης 12 και 18 Mbps χρησιμοποιείται η διαμόρφωση μεταβολής μετατόπισης τεσσάρων φάσεων (QPSK, Quaternary Phase Shift Keying),
- για ρυθμούς μετάδοσης 24 και 36 Mbps χρησιμοποιείται η διαμόρφωση τετραγωνική μετατόπιση πλάτους 16 σημείων (16QAM, Quadrature Amplitude Modulation) και
- για ρυθμούς μετάδοσης 48 και 54 Mbps χρησιμοποιείται η διαμόρφωση τετραγωνική μετατόπιση πλάτους 64 σημείων (64QAM, Quadrature Amplitude Modulation).

Το IEEE 802.11a χρησιμοποιεί την τεχνική ορθογωνικής πολύπλεξης διαίρεσης συχνότητας OFDM. Ο υψηλός ρυθμός μετάδοσης επιτυγχάνεται χωρίζοντας το κύριο εύρος ζώνης σε πολλά υποκανάλια με χαμηλότερους ρυθμούς για την αποστολή δεδομένων. Αυτά τα υποκανάλια πολυπλέκονται έπειτα σε ένα συνδυασμένο κανάλι με υψηλό ρυθμό χωρίς να υπάρχει επικάλυψη μεταξύ τους. Η OFDM εκμεταλλεύεται σωστά το εύρος ζώνης χωρίς να το σπαταλά.

**ΠΙΝΑΚΑΣ 9: ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΠΡΟΤΥΠΟΥ 802.11a**

| ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ | ΠΕΡΙΓΡΑΦΗ 802.11a |
|---|---|
| Εφαρμογή | Ασύρματη Τοπική Δικτύωση Δεδομένων |
| Ρυθμός Μετάδοσης | 6-54 Mbps |
| Τυπική Ζώνη Συχνοτήτων | ISM 5,15 ως 5,875 GHz |
| Τεχνική | OFDM |
| Ασφάλεια | 128-bit WEP, 64-bit WEP, 152-bit WEP |
| Επίπεδο Σύνδεσης | CSMA/CA με RTS/CTS |

### 3.4.3 Το πρότυπο IEEE 802.11b

Το 1999 δημοσιεύτηκε το IEEE 802.11b, το οποίο είναι η επέκταση του αρχικού προτύπου 802.11 με τεχνική διαμόρφωσης DSSS και χρησιμοποιεί τη ζώνη συχνοτήτων των 2.4 GHz ως 2.4835 GHz και φτάνει τους ρυθμούς μετάδοσης δεδομένων των 11 Mbps. Όταν η ποιότητα επικοινωνίας είναι χαμηλή το σύστημα μπορεί να χαμηλώσει τον ρυθμό μετάδοσης σε 1 Mbps ή σε 2 Mbps ή σε 5.5 Mbps για να διατηρηθεί η σύνδεση των συσκευών ασύρματης δικτύωσης.

Το IEEE 802.11b χρησιμοποιεί την τεχνική DSSS όπως το 802.11 αλλά και την συμπληρωματική μεταλλαγή κωδικών (CCK, Complementary Code Keying) για αυτό επιτυγχάνεται μεγαλύτερος ρυθμός μετάδοσης[9][14]. Το IEEE 802.11b υλοποιεί με δύο τρόπους την ασύρματη επικοινωνία με τη χρήση ενός Σημείου Πρόσβασης (Access Point,AP) τύπου Infrastructure ή τύπου ad-hoc.

**ΠΙΝΑΚΑΣ 10: ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΠΡΟΤΥΠΟΥ 802.11b**

| ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ | ΠΕΡΙΓΡΑΦΗ 802.11b |
|---|---|
| Εφαρμογή | Ασύρματη Δικτύωση Δεδομένων |
| Ρυθμός Μετάδοσης | 1,2,5.5,11 Mbps |
| Τυπική Ζώνη Συχνοτήτων | ISM 2.4 ως 2.4835 GHz |
| Τεχνική | DSSS |
| Ασφάλεια | 128-bit WEP |
| Επίπεδο Σύνδεσης | CSMA/CA με RTS/CTS |

### 3.4.4 Το πρότυπο IEEE 802.11c

Το πρότυπο IEEE 802.11c αποσύρθηκε και συμπεριλήφθηκε στο πρότυπο IEEE 802.1D, το οποίο παρέχει τις απαραίτητες πληροφορίες για να διασφαλιστούν οι λειτουργίες γεφύρωσης (Bridge) του υποεπιπέδου MAC των προτύπων 802.3 (Ethernet), 802.11(Wi-Fi) και 802.16 (WiMax). Οι σχετικές διαδικασίες υπάρχουν στο πρότυπο αυτό και οι κατασκευαστές των προϊόντων το χρησιμοποιούν όταν δημιουργούν σταθμούς πρόσβασης[3][12].

### 3.4.5 Το πρότυπο IEEE 802.11d

Το IEEE 802.11d ονομάζεται Καθολική εναρμόνιση (Global Harmonization) και προσθέτει τις απαιτήσεις και τους ορισμούς που θα επιτρέψουν στον εξοπλισμό των ασύρματων τοπικών δικτύων 802.11 να λειτουργήσει, λόγω της μη εξυπηρέτησής του από τα παραπάνω πρότυπα. Επειδή η ζώνη συχνοτήτων διαφέρει από χώρα σε χώρα, πρέπει η κατασκευαστική αγορά να συμβαδίζει με τους κανόνες αυτούς και να μην την ξεπερνούν[3][4][12].

### 3.4.6 Το πρότυπο IEEE 802.11e

Το πρότυπο IEEE 802.11e δημοσιεύτηκε το 2005 και περιλαμβάνει τον εμπλουτισμό του MAC για την Ποιότητα Υπηρεσιών (MAC Enhancements For QoS)[12]. Ενισχύει τον τρέχοντα MAC μηχανισμό του 802.11, με αποτέλεσμα να

επεκταθεί η υποστήριξη στις δικτυακές εφαρμογές για ποιότητα υπηρεσιών (QoS, Quality of Service), να βελτιωθεί η ασφάλεια, να αναβαθμιστούν οι δυνατότητες και η απόδοση[14]. Το πρότυπο IEEE 802.11e χρησιμοποιεί την μέθοδο HCF (Hybrid Coordination Function) και την μέθοδο EDCF (Enhanced Coordination Function) οι οποίες αναλύονται στο κεφάλαιο 5 που αναφέρεται στο υπόστρωμα MAC[16].

Το αρχικό πρότυπο δεν υποστηρίζει την καλύτερη ποιότητα κατά την μετάδοση ήχου, εικόνας και βίντεο. Αυτό το πρότυπο δημιουργήθηκε για να βελτιώσει το αρχικό πρότυπο και τις υπηρεσίες που προαναφέρθηκαν.

### 3.4.7 Το πρότυπο IEEE 802.11F

Το πρότυπο IEEE 802.11F δημοσιεύτηκε το 2003 και έπειτα αποσύρθηκε. Το πρότυπο αυτό στην ουσία είναι μια συνιστώμενη πρακτική και χρησιμοποιεί το IAPP (Inter Access Point Protocol), το οποίο είναι το Πρωτόκολλο Διασύνδεσης Σημείων Πρόσβασης που περιλαμβάνει τις πληροφορίες ώστε οι χρήστες κατά την περιαγωγή (roaming) να μπορέσουν να επικοινωνήσουν με διαφορετικά Access Points[3]. Το Πρωτόκολλο αυτό ρυθμίζει τις λειτουργίες των Συστημάτων Διανομής (DS, Distribution System) που υποστηρίζει ένα 802.11 ασύρματο δίκτυο από διαφορετικούς κατασκευαστές[12][14].

Αυτή η συνιστώμενη πρακτική δημιουργήθηκε, επειδή το αρχικό πρότυπο IEEE 802.11 δεν προσδιορίζει την επικοινωνία με διαφορετικά συστήματα διανομής (Access Points) με ενσύρματα backbones που συνδέουν Access Points και δεν υπάρχουν προδιαγραφές ασφαλείας μεταξύ των επικοινωνιών κατά την διάρκεια της εναλλαγής των Access Points, για να υποστηρίζεται η κινητικότητα των χρηστών από ένα Access Point σε ένα άλλο..

### 3.4.8 Το πρότυπο IEEE 802.11g

Το πρότυπο IEEE 802.11g δημοσιεύτηκε το 2003 και υποστηρίζει ασύρματη επικοινωνία για κοντινές αποστάσεις με ρυθμό μετάδοσης ως 54 Mbps και την συμβατότητα των 802.11b προϊόντων με την συμπληρωματική μεταλλαγή κωδικών (Complementary Code Keying, CCK). Το πρότυπο IEEE 802.11g χρησιμοποιεί την τεχνική OFDM για να επιτύχει αυτούς τους ρυθμούς μετάδοσης[14]. Όταν συνδέεται ένα δίκτυο 802.11g με την παρουσία ενός

802.11b, ο ρυθμός μετάδοσης του δικτύου 802.11g μειώνεται σημαντικά στα 11 Mbps[4].

Το πρότυπο IEEE 802.11g υποστηρίζει την δυαδική συνελικτική κωδικοποίηση πακέτου (PBCC, Packet Binary Convolutional Coding) που φτάνει τους 33 Mbps ρυθμούς μετάδοσης[14]. Το πρότυπο αυτό είναι πολύ δημοφιλές για τις γρήγορες ταχύτητες του γιατί μπορεί να ανταπεξέλθει στις εφαρμογές που απαιτούν υψηλό εύρος ζώνης, όπως βίντεο και ήχο.

**ΠΙΝΑΚΑΣ 11: ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΠΡΟΤΥΠΟΥ 802.11g**

| ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ | ΠΕΡΙΓΡΑΦΗ 802.11g |
|---|---|
| Εφαρμογή | Ασύρματη Τοπική Πρόσβαση Ευρείας Ζώνης |
| Ρυθμός Μετάδοσης | 6, 9, 12, 18, 24, 36, 48, 54 Mbps |
| Τυπική Ζώνη Συχνοτήτων | ISM 2.4 ως 2.4835 GHz |
| Τεχνική | OFDM με ARF και CRC-32 |
| Ασφάλεια | 128-bit WEP |
| Επίπεδο Σύνδεσης | CSMA/CA με RTS/CTS |

### 3.4.9 Το πρότυπο IEEE 802.11h

Το πρότυπο IEEE 802.11h ασχολείται με τη Διαχείριση φάσματος (Spectrum Managed) του 802.11a. Αρχικά, απευθυνόταν και περιλάμβανε τις ανάγκες που απαιτούν οι Ευρωπαϊκοί κανονισμοί αλλά τώρα απευθύνεται και σε άλλες χώρες. Προσφέρει τη δυναμική επιλογή των καναλιών (DCS ,Dynamic Channel Selection) και τον έλεγχο μετάδοσης ισχύος (TPC ,Transmit Power Control) για την ζώνη συχνοτήτων των 5 GHz για το 802.11a MAC[14][15].

Με το DCS και το TPC αποφεύγονται οι παρεμβολές από τις δορυφορικές επικοινωνίες και τα ραντάρ. Το DCS ανιχνεύει αν υπάρχει η παρουσία συσκευής ραντάρ ή δορυφόρου σε ένα κανάλι και αλλάζει το κανάλι του δικτύου ώστε να

αποφύγει την παρεμβολή. Το TPC μειώνει τη συχνότητα της μετάδοσης ισχύος του πομπού δικτύου σε τέτοιο βαθμό, ώστε να ελαχιστοποιηθεί ο κίνδυνος παρεμβολής σε αυτό και σε άλλα συστήματα, επιτρέποντας την ικανοποιητική απόδοση τους. Το πρότυπο IEEE 802.11h αυξάνει την πώληση των 802.11a δικτύων στην Ευρώπη με αποτέλεσμα να υπάρχει μεγάλη ζήτηση και αισθητή μείωση της τιμής[4].

### 3.4.10 Το πρότυπο IEEE 802.11i

Το IEEE 802.11i περιλαμβάνει την ενίσχυση του MAC υποστρώματος για την αύξηση της ασφάλειας στα ασύρματα τοπικά δίκτυα, τα οποία είναι πιο επιρρεπές σε παραβιάσεις της ασφάλειας των δεδομένων.

Το πρότυπο αυτό χρησιμοποιεί τους παρακάτω αλγόριθμους[3][8][13]:

- Το πρωτόκολλο επέκτασης αυθεντικοποίησης (Extensible Authentication Protocol-EAP),
- Την τυποποιημένη προηγμένη κρυπτογράφηση (Advanced Encryption Standard-AES),
- Το πρωτόκολλο μοναδικού κλειδιού ακεραιότητας (Temporal Key Integrity Protocol-TKIP),
- Την αυτοδύναμη ασφάλεια δικτύου(Robust Security Network-RSN) και το IEEE 802.1X.

Οι αλγόριθμοι που χρησιμοποιούνταν είχαν προβλήματα. Ο WEP(Wired Equivalent) παρουσίαζε σημαντικά κενά ασφαλείας, ενώ ο WPA(Wi-Fi Protected Access) κάλυπτε τα κενά του WEP, όμως δεν κάλυπτε την ουσιαστική ασφάλεια των τοπικών δικτύων. Ο IPSEC εφαρμοζόταν τοπικά σε κάθε χρήστη και κάλυπτε μόνο Point-to-point συνδέσεις. Υπήρξαν προσπάθειες για αύξηση του μήκους κλειδιού ώστε να αποφευχθεί η εξουθενωτική επίθεση επειδή υπήρχαν απαγορευτικοί χρόνοι επιτυχίας.

### 3.4.11 Το πρότυπο IEEE 802.11j

Το πρότυπο IEEE 802.11j ασχολείται με τη Διαχείριση φάσματος (Spectrum Managed) του 802.11a στην Ιαπωνία, όπως το IEEE 802.11h στην Ευρώπη στις ζώνες συχνοτήτων των 4.9 GHz. και 5 GHz[13].

### 3.4.12 Το πρότυπο IEEE 802.11k

Το πρότυπο IEEE 802.11k, δημοσιεύτηκε το 2008. Αφορά την διαχείριση των πόρων της ασύρματης μετάδοσης και καθορίζει την κίνηση του δικτύου. Με βάση τον αριθμό και την γεωγραφική θέση των συνδρομητών οι οποίοι είναι συνδεδεμένοι σε ένα Access Point με ισχυρό σήμα υπάρχει περίπτωση να υπάρξει υπερχρησιμοποίηση αυτού του Access Point. Αυτό έχει ως αποτέλεσμα άλλα Access Point να υποχρησιμοποιούνται και το δίκτυο να έχει χαμηλή απόδοση. Για να έχει την καλύτερη δυνατή απόδοση το δίκτυο, το IEEE 802.11k ρυθμίζει την κυκλοφορία.

Η ρύθμιση κυκλοφορίας γίνεται ως εξής: μια ασύρματη συσκευή συνδέεται σε ένα Access Point ισχυρού σήματος, αν αυτό είναι φορτωμένο τότε η σύνδεση μεταφέρεται σε ένα κοντινό Access Point το οποίο είναι λιγότερο φορτωμένο και έχει χαμηλότερο σήμα. Η μεταφορά της σύνδεσης από ένα φορτωμένο Access Point ισχυρού σήματος σε ένα μη-φορτωμένο Access Point χαμηλού σήματος γίνεται για να είναι πιο αποτελεσματική η χρήση των πόρων του δικτύου.

Κάθε Access Point παρέχει μία λίστα που περιλαμβάνει τον χρόνο που χρησιμοποιήθηκε το κανάλι, πόσο φορτωμένο είναι, τι είδους υπηρεσίες και τύπους κρυπτογράφησης παρέχει. Η δημιουργία αυτής της λίστας προέρχεται από τις πληροφορίες που του παρείχε ένας Client, μετά από μια αίτηση του Access Point να μεταβεί στο συγκεκριμένο κανάλι[4][12].

### 3.4.13 Το πρότυπο IEEE 802.11m

Το πρότυπο IEEE 802.11m ασχολείται με τη συντήρηση, τη βελτίωση, τις διορθώσεις και τις διευκρινήσεις όλων των προτύπων 802.11[4].

### 3.4.14 Το πρότυπο IEEE 802.11n

Το πρότυπο IEEE 802.11n δημοσιεύτηκε τον Οκτώβριο του 2009 και παρότι ενσωματώνει κάποια χαρακτηριστικά των προηγούμενων προτύπων, προσθέτει το σύστημα Πολλαπλής Εισόδου Πολλαπλής Εξόδου (ΠΕΠΕ,MIMO Multiple Input Multiple Output). Το σύστημα αυτό χρησιμοποιεί πολλαπλές κεραίες για την μεγαλύτερη ποσότητα δεδομένων από ένα σημείο σε πολλά και σε συγκεκριμένο χρονικό διάστημα με αποτέλεσμα να έχει μεγάλη κατανάλωση ρεύματος.

Το πρότυπο IEEE 802.11n χρησιμοποιεί την τεχνική OFDM. Το πλάτος του καναλιού είναι διπλάσιο από 20 ως 40 MHz σε σχέση με τα προηγούμενα, γιατί χωρίζει το κανάλι των 40 MHz σε τέσσερα ρεύματα. Στο πρότυπο IEEE 802.11n ο μέγιστος ρυθμός μετάδοσης δεδομένων, κατά την ασύρματη μετάδοση, είναι από 54 Mbps ως 600 Mbps στις συχνότητες των 2.4 GHz και 5 GHz με την προϋπόθεση ότι δε θα υπάρχουν παρεμβάσεις, ενώ η εμβέλεια είναι διπλάσια σε σχέση με τα παλαιότερα πρότυπα[4][19].

Για να συνδεθούν οι χρήστες με συσκευές 802.11b/g σε ένα δίκτυο 802.11n, θα πρέπει να αντικαταστήσουν τις κάρτες wi-fi των επιτραπέζιων υπολογιστών ή να αποσύρουν τους παλιούς φορητούς υπολογιστές τους. Επειδή όμως αυτό είναι ασύμφορο, δημιουργήθηκε η ιδέα να λειτουργήσει ένα μεικτό 802.11b/g/n δίκτυο, στο οποίο η κυκλοφορία των 2.4 GHz να τοποθετείται το 802.11b/g και των 5 GHz στο 802.11n.

Οι βασικές εφαρμογές υψηλών απαιτήσεων σε εύρος ζώνης που υποστηρίζει αυτό το πρότυπο είναι:

- Η πρόσβαση στο διαδίκτυο.
- Η διαδικτυακή τηλεφωνική επικοινωνία (VoIP, Voice over Internet Protocol) με την βέλτιστη ποιότητα.
- Η μεταφορά δεδομένων με περιεχόμενο πολυμέσων
- Η δημιουργία αντιγράφων ασφαλείας σε δικτυακές αποθηκευτικές μονάδες (NAS, Network Attached Storage).

Το πρότυπο IEEE 802.11n χρησιμοποιείται σε επιχειρήσεις και σε οικιακά δίκτυα, κυρίως σε κοινωνικές ομάδες που έχουν υψηλές απαιτήσεις και χειρίζονται εφαρμογές υψηλών απαιτήσεων.

### 3.4.15 Το πρότυπο IEEE 802.11p

Το πρότυπο IEEE 802.11p δεν έχει ολοκληρωθεί ακόμα. Με βάση το προσχέδιο θα προσθέσει στο πρότυπο 802.11 ασύρματη πρόσβαση σε περιβάλλον οχημάτων (WAVE) για την υποστήριξη Intelligent Transportation Systems (ITS) εφαρμογές. Περιλαμβάνει την μετάδοση δεδομένων μεταξύ οχημάτων με άλλα οχήματα με υψηλές ταχύτητες και των οδικών υποδομών (όπως τα Διόδια) στην

αδειοδοτημένη ITS ζώνη των 5.9GHz. Σκοπός του προτύπου αυτού είναι να υπάρχει επικοινωνία, με την ίδια κεραία και τον ίδιο πομπό-δέκτη, σε κοντινές συχνότητες, μεταξύ άλλων χωρών που δεν έχουν ακριβώς την ίδια κατανομή συχνοτήτων, για να υπάρξει ένα πανεθνικό δίκτυο. Το πανεθνικό δίκτυο θα επιτρέπει την επικοινωνία για εφαρμογές όπως η είσπραξη διοδίων, υπηρεσίες ασφάλειας οχημάτων και συναλλαγές σε αυτοκίνητα εν κινήση[3][4][12].

### 3.4.16 Το πρότυπο IEEE 802.11r

Το πρότυπο IEEE 802.11r δημοσιεύτηκε το 2008 και περιλαμβάνει την συνεχή σύνδεση των ασύρματων συσκευών εν κινήσει, όπως στα συστήματα οχημάτων, την γρήγορη και ασφαλή εναλλαγή των Access Points με ένα παρόμοιο τρόπο[3][4][12].

### 3.4.17 Το πρότυπο IEEE 802.11s

Το πρότυπο IEEE 802.11s είναι ένα σχέδιο για Mesh δικτύωση που χρησιμοποιείται για στατικές τοπολογίες και για δικτύωση ad-hoc. Περιλαμβάνει μηχανισμούς για τον έλεγχο της κυκλοφοριακής συμφόρησης και την εξοικονόμηση ενέργειας[3][4][12].

### 3.4.18 Το πρότυπο IEEE 802.11T

Το πρότυπο IEEE 802.11T είναι μία συνιστώμενη πρακτική και περιλάμβανε την ασύρματη πρόβλεψη απόδοσης, τις συστατικές μεθόδους και τις μετρικές δοκιμές. Το πρότυπο αυτό ακυρώθηκε[3][4][12].

### 3.4.19 Το πρότυπο IEEE 802.11u

Το πρότυπο IEEE 802.11u δεν έχει τελειοποιηθεί και περιλαμβάνει προτάσεις για την προδιαγραφή των απαιτήσεων. Περιέχει απαιτήσεις όπως οι περιοχές των εγγραφών, η επιλογή δικτύων, η υποστήριξη κλήσης ανάγκης, ο συναγερμός επείγουσας ανάγκης, η κατάτμηση της κυκλοφορίας των χρηστών και η διαφήμιση των υπηρεσιών[3][4][12].

### 3.4.20 Το πρότυπο IEEE 802.11v

Το πρότυπο IEEE 802.11v, που δεν έχει τελειοποιηθεί, ασχολείται με την διαχείριση των ασύρματων δικτύων και επιτρέπει την διαμόρφωση των συσκευών Client που συνδέονται με 802.11 δίκτυα [3][4][12].

### 3.4.21 Το πρότυπο IEEE 802.11w

Το πρότυπο IEEE 802.11w δημοσιεύτηκε το 2009 και περιλαμβάνει μηχανισμούς για την προστασία των διαχειριζόμενων πλαισίων του υποστρώματος MAC ώστε να υπάρχει ακεραιότητα των δεδομένων, προστασία, αναπαραγωγή και αυθεντικότητα των δεδομένων προέλευσης[3][4][12].

### 3.4.22 Το πρότυπο IEEE 802.11y

Το πρότυπο IEEE 802.11y ,δημοσιεύτηκε το 2008, και δίνει την δυνατότητα της υψηλής απόδοσης των wi-fi συσκευών στην ζώνη συχνοτήτων των 3650 με 3700 MHz στις Ηνωμένες Πολιτείες Αμερικής εκτός κι αν υπάρχει σταθμός επίγειου δορυφόρου[12].

### 3.4.23 Άλλα πρότυπα Υπό Κατασκευή

Τα πρότυπα IEEE 802.11z, IEEE 802.11aa, IEEE 802.11mb, IEEE 802.11ac, IEEE 802.11ad, IEEE 802.11ae, IEEE 802.11af δεν έχουν ολοκληρωθεί ακόμα και δεν υπάρχουν αρκετές πληροφορίες για αυτά. Υπάρχουν σχετικές πληροφορίες για την ενασχόληση των προτύπων αυτών[12].

- Το πρότυπο IEEE 802.11z ασχολείται με τις επεκτάσεις των άμεσων συνδέσεων.
- Το πρότυπο IEEE 802.11aa ασχολείται με τη ροή των μεταδόσεων ήχου και βίντεο.
- Το πρότυπο IEEE 802.11mb ασχολείται με τη συντήρηση των προτύπων.
- Το πρότυπο IEEE 802.11ac ασχολείται με την πολύ υψηλή ρυθμαπόδοση ως 6 GHz, την πιθανή βελτίωση του προτύπου IEEE 802.11n.
- Το πρότυπο IEEE 802.11ad ασχολείται με την πολύ υψηλή ρυθμαπόδοση των 60 GHz.
- Το πρότυπο IEEE 802.11ae ασχολείται με τη διαχείριση των Qos υπηρεσιών.

- Το πρότυπο IEEE 802.11af ασχολείται με τις λευκές ζώνες των τηλεοπτικών εκπομπών.

Το πρότυπο 802.11X συμβολίζει όλα τα πρότυπα που υπάρχουν, αλλά και αυτά που βρίσκονται ακόμα στο στάδιο της έρευνας.

## 3.5 ΣΥΓΚΡΙΣΗ ΠΡΟΤΥΠΩΝ

Παρακάτω συγκρίνονται τα πιο δημοφιλή και τα ευρέως χρησιμοποιούμενα πρότυπα όπως το IEEE 802.11, το IEEE 802.11a, το IEEE 802.11b, το IEEE 802.11g και το IEEE 802.11n.

Το πρότυπο IEEE 802.11a όπως φαίνεται στον πίνακα δεν είναι συμβατό με το πρότυπο IEEE 802.11g διότι λειτουργούν σε διαφορετικές ζώνες συχνοτήτων[18]. Επιπλέον, δεν είναι συμβατό ούτε με το πρότυπο IEEE 802.11b λόγω διαφορετικών ζωνών συχνοτήτων αλλά και λόγω διαφορετικών τεχνικών[18].

**ΠΙΝΑΚΑΣ 12: ΣΥΓΚΡΙΣΗ ΤΩΝ ΔΗΜΟΦΙΛΕΣΤΕΡΩΝ ΠΡΟΤΥΠΩΝ**

| Χαρακτηριστικά | 802.11 | 802.11a | 802.11b | 802.11g | 802.11n |
|---|---|---|---|---|---|
| Ζώνη συχνοτήτων | ISM: 2.4 GHz ως 2.4835GHz | UNII: 5.15-5.25GHz, 5.25-5.35GHz, και 5.725-5.825GHz | ISM: 2.4 ως 2.4835 GHz | ISM: 2.4 ως 2.4835 GHz | ISM: 2.4-2.4835GHz UNII: 5.15-5.25GHz, 5.25-5.35GHz, 5.725-5.825GHz |
| Τεχνική | FHSS ή DSSS | OFDM | DSSS | OFDM ή DSSS | OFDM |
| Μέγιστος Ρυθμός Μετάδοσης | 2 Mbps | 54 Mbps | 11 Mbps | 54 Mbps | 54 Mbps ως 600 Mbps |

| Χαρακτηριστικά | 802.11 | 802.11a | 802.11b | 802.11g | 802.11n |
|---|---|---|---|---|---|
| Συμβατότητα | 802.11 μόνο | 802.11a | 802.11g | 802.11b | 802.11a, 802.11b, 802.11g |

Η αρχική τιμή για τα 802.11a προϊόντα είναι πιο υψηλή, σε σχέση με τα 802.11b και 802.11g προϊόντα, επειδή λειτουργούσαν σε δίκτυο που χρησιμοποιούνταν μόνο 802.11a συσκευές. Με την χρησιμοποίηση dual-band ή dual-mode Access Points και καρτών Διασύνδεσης Δικτύων η τιμή των 802.11a προϊόντων είναι χαμηλότερη από την αρχική τιμή. Επίσης τα 802.11a προϊόντα δεν έχουν υψηλό ποσοστό παρεμβολών γιατί χρησιμοποιούν την ζώνη συχνοτήτων των 5 GHz.


**ΕΙΚΟΝΑ 28: ΛΟΓΟΤΥΠΟ WI – FI**

Τα 802.11b και 802.11g προϊόντα είναι πιο δημοφιλή γιατί έχουν χαμηλό κόστος σε σχέση με τον εξοπλισμό του 802.11a. Τα προϊόντα 802.11g είναι πιο ακριβά από τα 802.11b γιατί επιτυγχάνουν μεγαλύτερους ρυθμούς μετάδοσης. Τα 802.11b και 802.11g προϊόντα χρησιμοποιούν τη ζώνη συχνοτήτων των 2.4 GHz με υψηλό ποσοστό παρεμβολών.

**ΠΙΝΑΚΑΣ 13: ΕΜΒΕΛΕΙΑ ΣΕ ΕΣΩΤΕΡΙΚΟΥΣ ΚΑΙ ΕΞΩΤΕΡΙΚΟΥΣ ΧΩΡΟΥΣ ΤΩΝ ΔΗΜΟΦΙΛΕΣΤΕΡΩΝ ΠΡΟΤΥΠΩΝ**

| Χαρακτηριστικά | 802.11a | 802.11b | 802.11g | 802.11n |
|---|---|---|---|---|
| Δημοτικότητα | Νέα τεχνολογία | Δημοφιλέστερο | Νέα Τεχνολογία Ραγδαία Ανάπτυξη | Νέα Τεχνολογία Ραγδαία Ανάπτυξη<br>Πολλά Υποσχόμενο |

| Χαρακτηριστικά | 802.11a | 802.11b | 802.11g | 802.11n |
|---|---|---|---|---|
| Εμβέλεια σε εσωτερικούς χώρους | 15 μέτρα 54 Mbps<br>91 μέτρα 6 Mbps | 30 μέτρα 11 Mbps<br>91 μέτρα 1 Mbps | 30 μέτρα 54 Mbps<br>91 μέτρα 6 Mbps | 70 μέτρα |
| Εμβέλεια σε εξωτερικούς χώρους | 30 μέτρα 54 Mbps<br>305 μέτρα 6 Mbps | 152 μέτρα 11 Mbps<br>457 μέτρα 1 Mbps | 152 μέτρα 54 Mbps<br>457 μέτρα 6 Mbps | 250 μέτρα |

Τα 802.11n προσφέρουν πολύ μεγάλους ρυθμούς μετάδοσης και είναι πιο ανθεκτικά στις παρεμβολές των εξωτερικών πηγών. Για την μετάδοση ενός αρχείου βίντεο με 802.11n δίκτυο χρειάζεται μόλις ένα λεπτό ενώ μέσω ενός 802.11b δικτύου απαιτούνται 42 λεπτά. Το κόστος του εξοπλισμού 802.11n είναι μεγαλύτερο από τον εξοπλισμό των 802.11g γιατί παρέχει μεγαλύτερη εμβέλεια και μεγαλύτερους ρυθμούς μετάδοσης.

## 3.6 ΣΥΝΟΨΗ

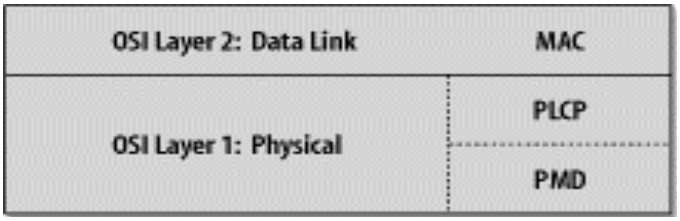
Σε αυτό το κεφάλαιο αναλύθηκαν οι έννοιες του ηλεκτρομαγνητικού φάσματος, των ρυθμιστικών φορέων και του προτύπου IEEE 802.11. Επίσης, έγινε μια σύντομη περιγραφή για τα πρότυπα του IEEE 802.11 και σύγκριση των δημοφιλέστερων προτύπων που χρησιμοποιούνται σήμερα. Στα επόμενα κεφάλαια αναλύονται το φυσικό επίπεδο και το υπόστρωμα MAC του προτύπου IEEE 802.11.

# 4. ΦΥΣΙΚΟ ΣΤΡΩΜΑ ΤΟΥ ΠΡΟΤΥΠΟΥ 802.11

## 4.1 ΕΙΣΑΓΩΓΗ

Το πρότυπο 802.11 αναφέρεται στα δύο χαμηλότερα επίπεδα του μοντέλου OSI, στο φυσικό στρώμα, στο οποίο αναφέρεται το παρόν κεφάλαιο, και στο υπόστρωμα MAC, στο οποίο θα αναφερθούμε σε επόμενο κεφάλαιο. Το φυσικό στρώμα χωρίζεται σε δύο επίπεδα, το Physical Layer Convergence Procedure (PLCP) και το Physical Medium Dependent (PMD).

Το PLCP μετατρέπει τα πλαίσια που λαμβάνει από το υπόστρωμα MAC σε μορφή κατάλληλη για μετάδοση από το PMD. Σε κάθε πλαίσιο MAC, το PLCP προσθέτει την δική του κεφαλίδα. Το PMD είναι υπεύθυνο για την μετάδοση και την παραλαβή των δεδομένων κι επιπλέον είναι αυτό που έρχεται σε επαφή με το μέσο. Το φυσικό στρώμα περιλαμβάνει μια λειτουργία εκτίμησης του καναλιού (CCA, Clear Channel Assessment), η οποία υποδεικνύει στο MAC την ανίχνευση ενός σήματος. Στο σχήμα που ακολουθεί φαίνεται η αρχιτεκτονική του φυσικού στρώματος.

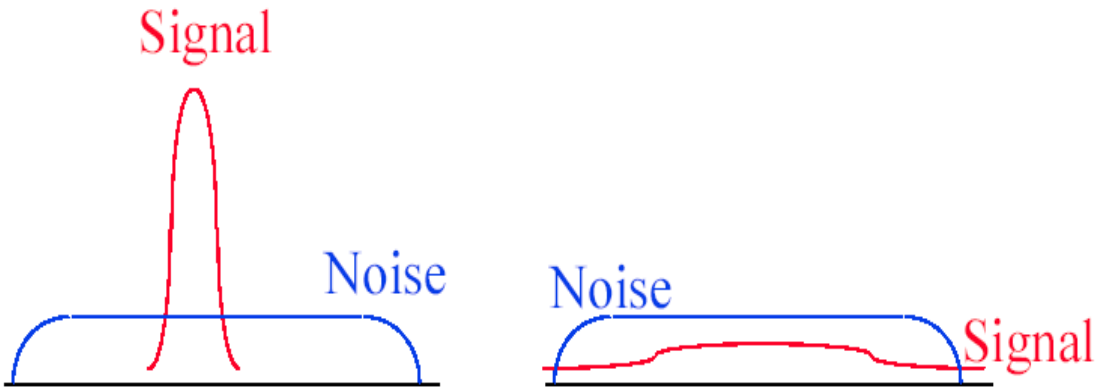



ΕΙΚΟΝΑ 29: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΦΥΣΙΚΟΥ ΣΤΡΩΜΑΤΟΣ

Στο φυσικό στρώμα του IEEE 802.11 προδιαγράφονται τρεις τεχνικές διαμόρφωσης, η Direct Sequence Spread Spectrum DSSS (Εξαπλωμένο Φάσμα Ευθείας Ακολουθίας), η Frequency Hopping Spread Spectrum FHSS (Εξαπλωμένο Φάσμα και Αναπήδησης Συχνότητας) και το Infrared (Υπέρυθρες Ακτίνες).

Οι δύο πρώτες τεχνικές, είναι τεχνικές εξάπλωσης φάσματος (Spread Spectrum). Οι τεχνικές αυτές αποτελούν μεθόδους με τους οποίους η ενέργεια ενός σήματος, το οποίο καταλαμβάνει κάποιο σχετικά περιορισμένο φάσμα συχνοτήτων, κατανέμεται εσκεμμένα σε πολύ μεγαλύτερο φασματικό εύρος με σκοπό την αύξηση της ασφάλειας των τηλεπικοινωνιών και την αποφυγή υποκλοπών. Έτσι, από τη μία καταναλώνετε περισσότερο φάσμα και από την άλλη το σήμα αποκτά

εξαιρετική ανοσία σε παρεμβολές, θόρυβο και φαινόμενα διάδοσης, όπως τις ανακλάσεις. Στην εικόνα που ακολουθεί, φαίνεται ο τρόπος με τον οποίο εκτελούνται οι τεχνικές spread spectrum. [3]




**ΕΙΚΟΝΑ 30: ΤΕΧΝΙΚΕΣ SPREAD SPECTRUM**

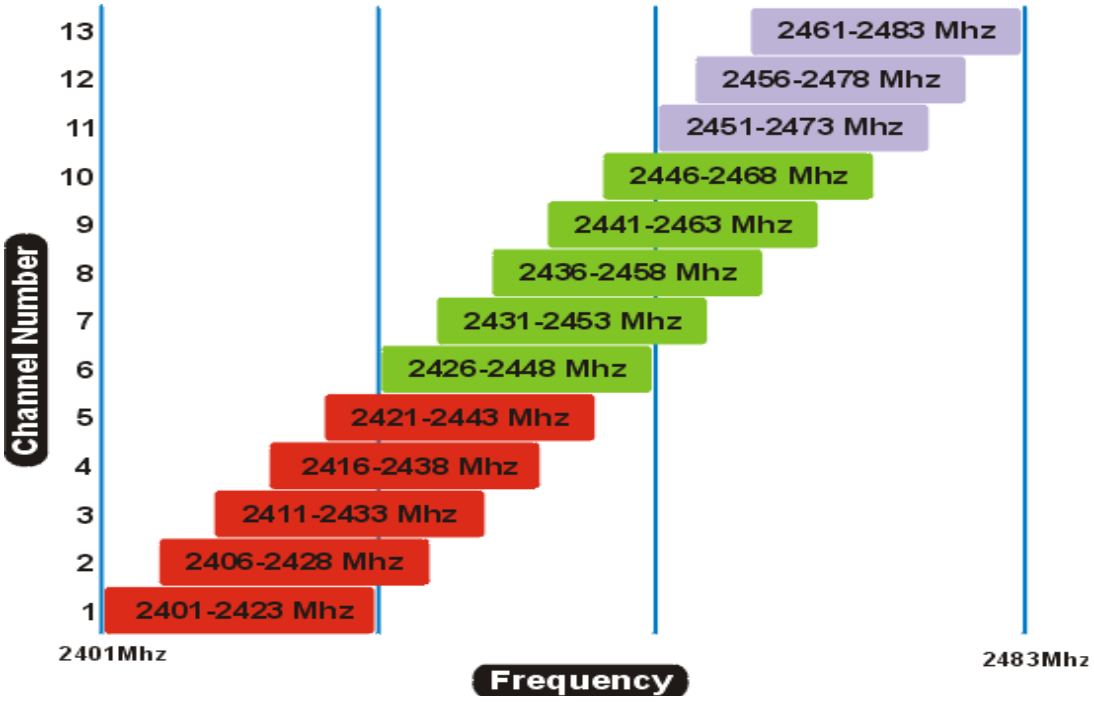
Επίσης, σε αυτό το σημείο, θα πρέπει να αναφερθεί ότι οι δύο πρώτες τεχνικές ανταποκρίνονται στις προδιαγραφές της Ομοσπονδιακής Επιτροπής Τηλεπικοινωνιών (FCC 15.247), για λειτουργία στην ISM περιοχή των 2,4 GHz. Στον παρακάτω πίνακα φαίνεται ο καταμερισμός των συχνοτήτων σε διάφορες χώρες.

**ΠΙΝΑΚΑΣ 14: ΚΑΤΑΜΕΡΙΣΜΟΣ ΣΥΧΝΟΤΗΤΩΝ ΣΕ ΔΙΑΦΟΡΕΣ ΧΩΡΕΣ**

| ΠΕΡΙΟΧΗ | ΚΑΤΑΜΕΡΙΣΜΟΣ ΦΑΣΜΑΤΟΣ |
|---|---|
| ΗΠΑ | 2.4000 – 2.4835 GHz |
| Ευρώπη(εκτός Γαλλία και Ισπανία) | 2.4000 – 2.4835 GHz |
| Γαλλία | 2.4465 – 2.4835 GHz |
| Ισπανία | 2.445 – 2.475 GHz |
| Ιαπωνία | 2.471 – 2.497 GHz |

Στην Ευρώπη υπάρχουν διαθέσιμα 13 κανάλια. Η απόσταση μεταξύ των καναλιών είναι 5MHz και το εύρος κάθε καναλιού είναι περίπου 22MHz. Από τα 13 κανάλια, τα 3 είναι μη επικαλυπτόμενα, δηλαδή κανάλια των οποίων οι συχνότητες δεν συμπίπτουν και πρόκειται για τα κανάλια 1, 6 και 11. Σε

περίπτωση που υπάρχουν επικαλυπτόμενα κανάλια, παρατηρείτε την εμφάνιση παρεμβολών, γεγονός που οδηγεί σε μείωση των επιδόσεων όλων των δικτύων που τα χρησιμοποιούν για τη μετάδοση των δεδομένων. Στην εικόνα που ακολουθεί, παρουσιάζονται οι συχνότητες που εκπέμπει κάθε κανάλι.




ΕΙΚΟΝΑ 31: ΣΥΧΝΟΤΗΤΕΣ ΠΟΥ ΕΚΠΕΜΠΕΙ ΚΑΘΕ ΚΑΝΑΛΙ

## 4.2 ΤΕΧΝΙΚΕΣ SPREAD SPECTRUM

Οι τεχνικές spread spectrum, περιγράφτηκαν αρχικά από μία ηθοποιό, η οποία κάποτε είχε ανακηρυχτεί ως η ωραιότερη γυναίκα του Hollywood, κι ένα μουσικό. Τον Ιούνιο του 1941 η Hedy Lamarr ή αλλιώς Hedy Markey και ο George Antheil

περιέγραψαν μία ασφαλή ράδιο – σύνδεση για τον έλεγχο των τορπιλών. Στις 11 Αυγούστου του 1942 έλαβαν το αμερικανικό δίπλωμα ευρεσιτεχνίας #2.292.387, “Secret Communication System”. Η αναγνώριση βέβαια ήρθε μετά από 55 χρόνια, το 1997, όταν βραβεύτηκαν για τη συνεισφορά τους, από το Αμερικανικό Ίδρυμα «Electronic Frontier Foundation». Χρησιμοποιήθηκαν για την αντιμετώπιση των σκόπιμων παρεμβολών των τηλεπικοινωνιακών συστημάτων. Οι παρεμβολές δημιουργούνται κατά τη μεταβίβαση σημάτων στην ίδια συχνότητα με το

μεταδιδόμενο σήμα, τα οποία δημιουργούν θόρυβο και ταλαντώσεις στη διαμόρφωση. Το όνομα των τεχνικών αυτών οφείλεται στο γεγονός ότι το εύρος ζώνης που απασχολούν είναι πολύ μεγαλύτερο από το ελάχιστο εύρος ζώνης που απαιτείται για τη μετάδοση της πληροφορίας. [3][8]

Σ’ αυτό το σημείο, θα ξεκινήσει μία πιο λεπτομερειακή ιστορική αναδρομή για αυτήν την ανακάλυψη. Η ιδέα των τεχνικών spread spectrum, προτάθηκε στον αμερικανικό ναυτικό ως ασφαλής τρόπος καθοδήγησης των τορπιλών που συχνά έχαναν τον στόχο τους, λόγω της χρήσης κατάλληλων ραδιοπαρεμβολών από το γερμανικό και το ιαπωνικό ναυτικό. Οι αρμόδιοι του υπουργείου αγνόησαν αρχικά αυτές τις τεχνικές και πρότειναν στην Hedy Lamarr έναν κατά τη γνώμη τους πιο αποδοτικό τρόπο για να συνεισφέρει στην κοινή πολεμική προσπάθεια. Θα χρέωνε κάθε φιλί της 50000$. Με αυτόν τον τρόπο, τα έσοδα του αμερικάνικου δημοσίου αυξήθηκαν τότε περίπου 7 εκατομμύρια δολάρια.

Οι τεχνικές spread spectrum, αν και καθυστερημένα, χρησιμοποιήθηκαν από τον αμερικάνικο ναυτικό κατά τη διάρκεια ενός αποκλεισμού της Κούβας. Στη συνέχεια, χρησιμοποιήθηκαν στις διαστημικές επικοινωνίες και στην τηλεμετρία του απώτερου διαστήματος. Η κορύφωση όμως αυτών των τεχνολογιών είναι το αξίας 25 δισεκατομμυρίων δολαρίων σύστημα ελέγχου των διηπειρωτικών πυραύλων MILSTAR. [8]

Η ανάγκη για την ανάπτυξη των τεχνικών spread spectrum, προέκυψε από τις στρατιωτικές ανάγκες του ηλεκτρονικού πολέμου. Ο ηλεκτρονικός πόλεμος συνίσταται στον εντοπισμό των συχνοτήτων επικοινωνίας του αντιπάλου και την ισχυρή εκπομπή σημάτων παρεμβολής, στις ίδιες συχνότητες. Οι ηλεκτρονικοί παρεμβολείς αποτελούν, ουσιαστικά, ένα σχεδόν πλήρες κινούμενο εργαστήριο ικανό να αναλύσει τις συχνότητες, να ξεχωρίσει και να αποφασίσει ποιες είναι φιλικές και ποιες όχι, ώστε να καταφέρει να παρεμβάλει ισχυρά τις εχθρικές. Όλα αυτά συμβαίνουν σε χρόνους της τάξεως του δευτερολέπτου. Εδώ, επεμβαίνουν οι τεχνικές spread spectrum, οι οποίες έχουν σαν σκοπό να εξουδετερώνουν αυτές τις παρεμβολές.

Όπως έχει ήδη αναφερθεί, πειράματα πάνω σε αυτές τις τεχνικές άρχισαν από το 1940 στα εργαστήρια του αμερικάνικου στρατού. Όμως, η ανώριμη ηλεκτρονική τεχνολογία εκείνης της εποχής και η πολυπλοκότητα των συστημάτων αυτών,

καθυστέρησαν την τότε ανάπτυξή τους, μέχρι τη δεκαετία του ’60. Τότε, κατασκευάστηκαν συστήματα επικοινωνιών για να χρησιμοποιηθούν στον αποκλεισμό της Κούβας. Έκτοτε, η ανάπτυξή τους είχε μείνει επτασφράγιστο στρατιωτικό μυστικό, ίδιας σπουδαιότητας με τα πυρηνικά όπλα, μέχρι το 1985, μετά την άρση του απορρήτου.

Σήμερα, έχουν δοθεί για εμπορική και βιομηχανική εκμετάλλευση, και οι συσκευές που διατίθενται μπορούν να θεωρούνται, από τεχνικής φύσεως, μικρά θαύματα. Συνήθως, χρησιμοποιούνται κατά κόρον στην τεχνολογία κυψελοειδών επικοινωνιών (κινητή τηλεφωνία), σε όλα τα συστήματα ασύρματων τοπικών δικτύων(Bluetooth, Home RF, και IEEE 802.11), αλλά και στην ραδιοκαθοδήγηση των διηπειρωτικών βαλλιστικών πυραύλων, τις δορυφορικές επικοινωνίες και την τηλεμετρία του απώτερου διαστήματος. Στις περισσότερες των περιπτώσεων, τα δίκτυα που χρησιμοποιούν τεχνικές εξάπλωσης φάσματος, υποστηρίζουν ρυθμούς μετάδοσης 1 έως 11 Mbps στη ζώνη συχνοτήτων 2.4 - 2.4835GHz. Η ζώνη αυτή είναι μία μη αδειοδοτημένη ζώνη για χρήση ISM (Industrial, Scientific and Medical), δηλαδή όχι για εμπορική εκμετάλλευση. Υπάρχουν δύο τύποι spread spectrum, η Direct Sequence Spread Spectrum (DSSS) και η Frequency Hopping Spread Spectrum (FHSS).

### 4.2.1 Direct Sequence Spread Spectrum (DSSS)

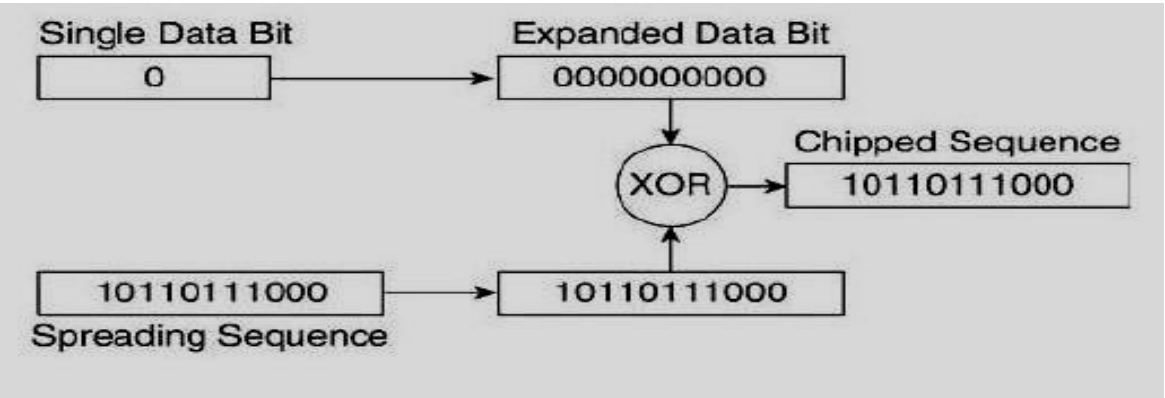
Η τεχνική Direct Sequence Spread Spectrum είναι η πιο επιτυχημένη τεχνική που έχει χρησιμοποιηθεί στα ασύρματα δίκτυα. Η τεχνολογία αυτών των συστημάτων, είναι παρόμοια με αυτήν που χρησιμοποιούν οι δορυφόροι GPS (Global Positioning System) και μερικοί τύποι κινητών τηλεφώνων και χρησιμοποιείται για ρυθμούς δεδομένων 1Mbps και 2Mbps στη ζώνη των 2.4GHz. Σε σχέση όμως με την τεχνική μετάδοσης Frequency Hopping Spread Spectrum, η DSSS είναι πιο πολύπλοκη και απαιτεί περισσότερη ενέργεια για να επιτύχει παρόμοια διέλευση. Το μεγαλύτερο πλεονέκτημά της είναι ότι μπορεί με ευκολία να αναβαθμιστεί ώστε να επιτύχει υψηλότερο ρυθμό μετάδοσης. Όμως, είναι μία πολύ ευαίσθητη τεχνολογία, που επηρεάζεται από πολλούς περιβαλλοντικούς παράγοντες, κυρίως αντανακλάσεις. [7]

Στην τεχνική DSSS το φάσμα χωρίζεται σε 14 μερικώς επικαλυπτόμενα κανάλια πλάτους 22 MHz, και χρησιμοποιείται ένα κάθε φορά για επικοινωνία. Στη DSSS

τεχνική πολυπλέκεται το σήμα πληροφορίας με έναν κώδικα. Ο κώδικας αυτός πρέπει να έχει πολύ καλές μαθηματικές ιδιότητες αυτοσυσχέτισης. Το αποτέλεσμα είναι να προκύπτει ένα σήμα με μεγαλύτερο εύρος συχνοτήτων του αρχικού. Συγκεκριμένα, η τεχνική DSSS αντικαθιστά κάθε bit πληροφορίας με μία σειρά από bits που ονομάζεται spreading code (κώδικας εξάπλωσης). Τα bits του spreading code κατά σύμβαση ονομάζονται chips. Χρησιμοποιούνται μόνο για την κωδικοποίηση και τη μετάδοση και δεν περιέχουν καμία πληροφορία. [2]

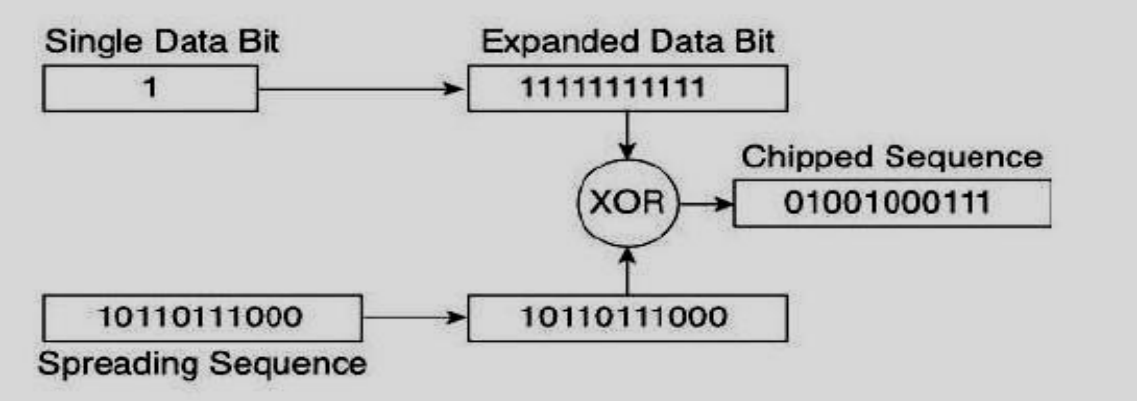
Οι ακολουθίες των chips έχουν πολύ υψηλότερο ρυθμό μετάδοσης από το σήμα πληροφορίας. Το σήμα υψηλής συχνότητας που δημιουργείται μεταδίδεται, και ο παραλήπτης το συγκρίνει με την ίδια ακολουθία για να εξακριβώσει αν το bit πληροφορίας είναι 0 ή 1. Το αποτέλεσμα της μετάδοσης ενός σήματος χαμηλού ρυθμού μετά την κωδικοποίηση από μία ακολουθία υψηλού ρυθμού έχει ως αποτέλεσμα η ενέργεια του σήματος να απλωθεί στο πεδίο της συχνότητας σε μεγάλο εύρος. Όσο μεγαλύτερος είναι ο ρυθμός της ακολουθίας chip τόσο περισσότερο απλώνεται η ενέργεια του σήματος. Η επίτευξη ακολουθίας chip υψηλού ρυθμού απαιτεί πολύπλοκα και ακριβά ηλεκτρονικά μέρη, ενώ η εξάπλωση του σήματος πρέπει να είναι εντός του διαθέσιμου εύρους ζώνης. Για παράδειγμα, αν έχουμε μία ακολουθία από 10 chips, το τελικό σήμα θα καταλαμβάνει δέκα φορές μεγαλύτερο φασματικό εύρος από το αρχικό. Και στις δύο περιπτώσεις, υποθέτουμε ότι ο χρόνος μετάδοσης είναι ίδιος. Ο αριθμός των chips που κωδικοποιούν κάθε bit ονομάζεται και processing gain (κέρδος επεξεργασίας) ή spreading ratio (παράγοντας εξάπλωσης). [1]

**Spreading a Data Bit with Value 0**




**ΕΙΚΟΝΑ 32: SPREADING A DATA BIT WITH VALUE 0 [7]**

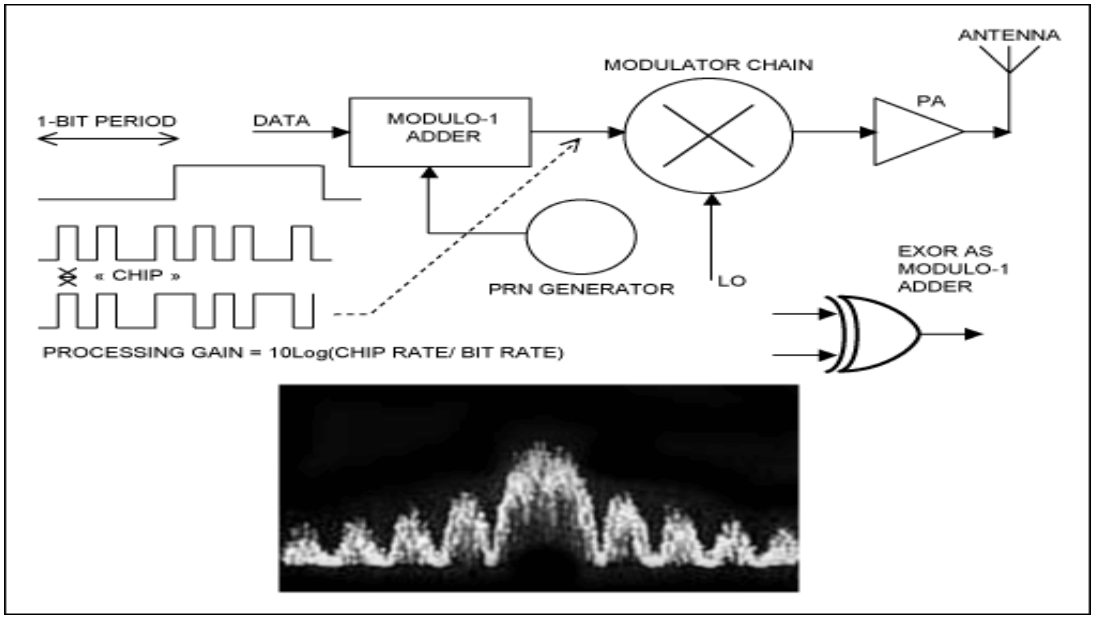
## Spreading a Data Bit with Value 1




**ΕΙΚΟΝΑ 33: SPREADING A DATA BIT WITH VALUE 1 [7]**

Κάθε bit πληροφορίας τοποθετείται στην είσοδο μίας πύλης XOR μαζί με το spreading code. Στην έξοδο του συστήματος προκύπτει μία ψηφιακή ακολουθία υψηλής ταχύτητας, η οποία στη συνέχεια διαμορφώνεται σε μία φέρουσα συχνότητα με τη μέθοδο DPSK (Differential Phase Shift Keying). Στις παραπάνω εικόνες παρουσιάζεται η εξάπλωση για δεδομένα με τιμή 0 bit στην πρώτη και 1 bit στη δεύτερη, αντίστοιχα.

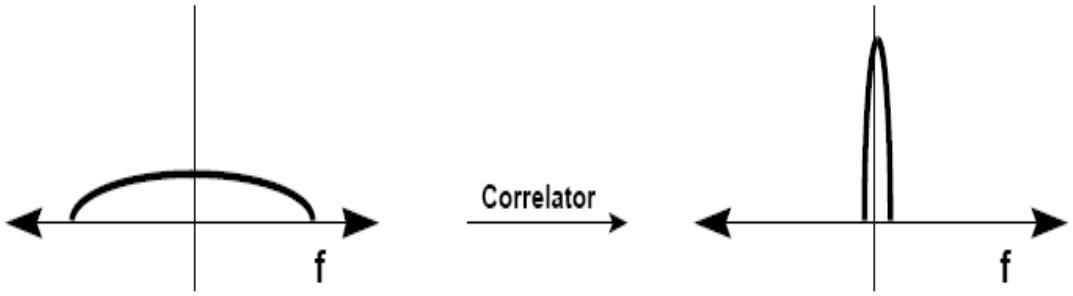
Το σήμα DSSS που λαμβάνεται, τοποθετείται στη συνέχεια σε ένα φίλτρο, το οποίο απομακρύνει το spreading code, έτσι ώστε να απομείνει μόνο η αρχική πληροφορία.




**ΕΙΚΟΝΑ 34: ΑΝΑΛΥΣΗ DSSS ΣΗΜΑΤΟΣ [10]**

Εξαιτίας των υψηλών ρυθμών μετάδοσης, οι DSSS δέκτες διαθέτουν διαφορετικούς spreading codes καθώς και φίλτρα για να καταφέρουν να απομονώσουν την εκπεμπόμενη πληροφορία. Η μέθοδος που χρησιμοποιείται για τη διαμόρφωση σε ρυθμούς 5.5 και 11 Mbps ονομάζεται Complimentary Code Keying (CCK) και χρησιμοποιεί την τεχνική Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA). Η CCK διαιρεί την ακολουθία chip σε κωδικοσύμβολα των 8bit , με αποτέλεσμα να μεταδίδονται 1375 εκατομμύρια το δευτερόλεπτο, σε αντίθεση με την τεχνική DSSS, στην οποία μεταδίδονται ένα εκατομμύριο. [2[4]][7]


**ΕΙΚΟΝΑ 35: ΕΠΙΔΡΑΣΗ ΤΗΣ ΑΚΟΛΟΥΘΙΑΣ PN ΣΤΟ ΦΑΣΜΑ ΜΕΤΑΔΟΣΗΣ [4]**

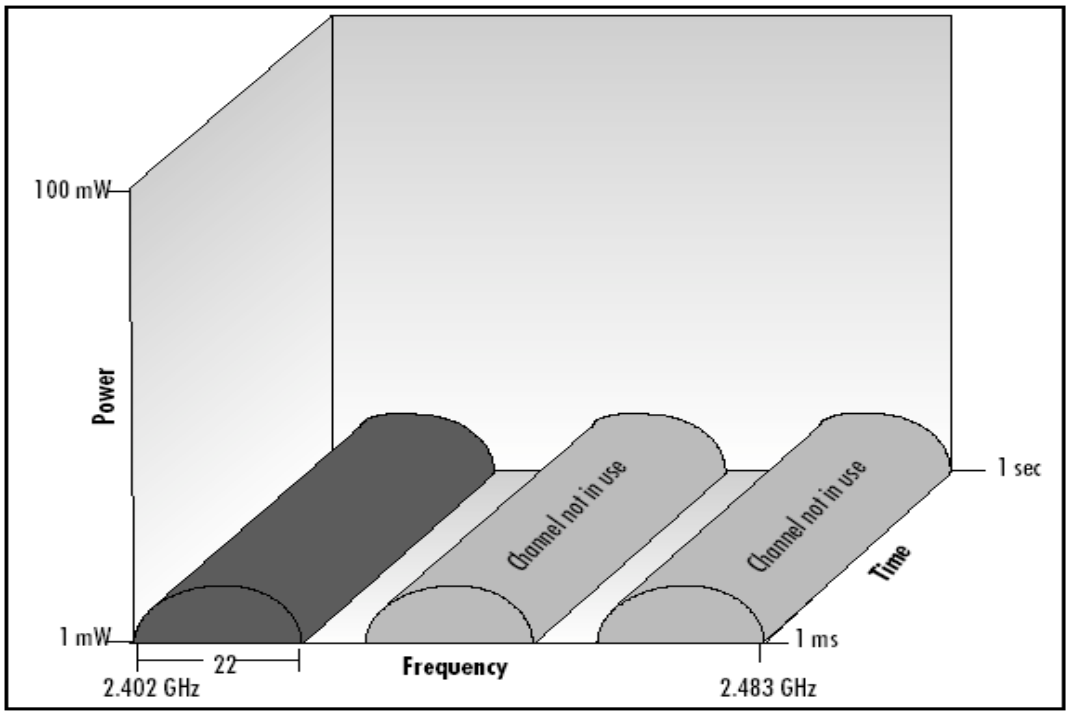



**ΕΙΚΟΝΑ 36: ΤΟ ΛΑΜΒΑΝΟΜΕΝΟ ΣΗΜΑ ΣΥΣΧΕΤΙΖΕΤΑΙ ΜΕ ΤΟ PN ΓΙΑ ΤΗΝ ΑΝΑΚΤΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ [4]**

Στις παραπάνω εικόνες, συγκεκριμένα στην πρώτη, φαίνεται η επίδραση που έχει ο spreading code στο εκπεμπόμενο εύρος, δηλαδή πως το spreading code διευρύνει το εύρος ζώνης του σήματος ενώ παράλληλα ελαττώνει τη μέγιστη ισχύ του σήματος. Αντίθετα, στη δεύτερη εικόνα παρατηρούμε τον τρόπο που το λαμβανόμενο σήμα είναι συσχετισμένο με το spreading code. Το σήμα συσχετίζεται με το spreading code, με αποτέλεσμα να επανακτηθεί πλήρως η αρχική δυαδική πληροφορία. [4]

#### 4.2.1.1 DSSS και 802.11 PHY

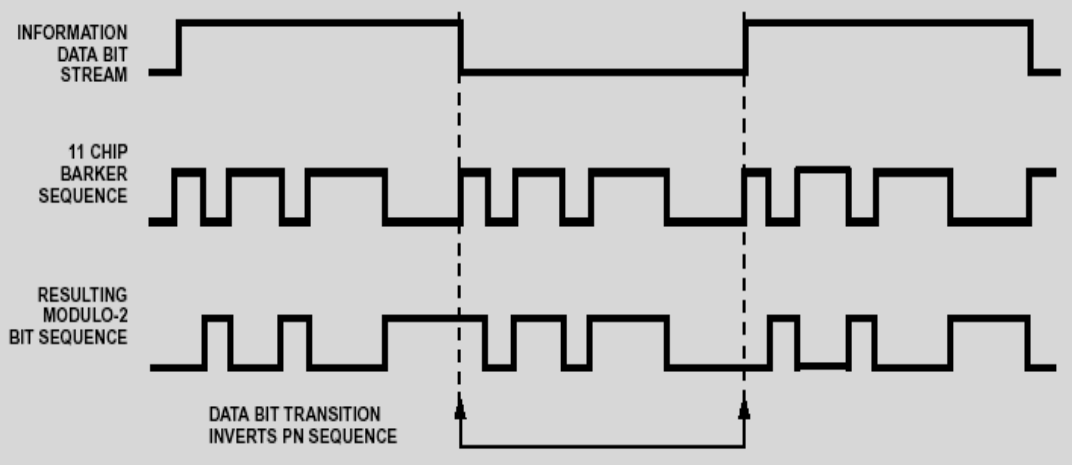
Στην τεχνική αυτή, όπως αναφέρθηκε και προηγουμένως, υπάρχει ένας κωδικός ο οποίος χρησιμεύει στην εξάπλωση του φάσματος και ονομάζεται spreading code ή chip sequence. Ανάλογα με το μέγεθος του chip, υπάρχει ένας αριθμός από ακολουθίες με το ίδιο μήκος οι οποίες μεταξύ τους έχουν την ιδιότητα της ορθογωνιότητας. Για παράδειγμα, αν το μέγεθος ενός chip είναι 255 bits, τότε υπάρχουν 16 διαφορετικές ακολουθίες μεγέθους 255 bits και είναι ορθογώνιες μεταξύ τους. Η έννοια της ορθογωνιότητας σημαίνει ότι αυτές οι ακολουθίες είναι σε μεγάλο βαθμό διαχωρίσιμες μεταξύ τους.




**ΕΙΚΟΝΑ 37: ΔΙΑΧΩΡΙΣΜΟΣ ΚΑΝΑΛΙΩΝ ΣΤΟ DSSS [7]**

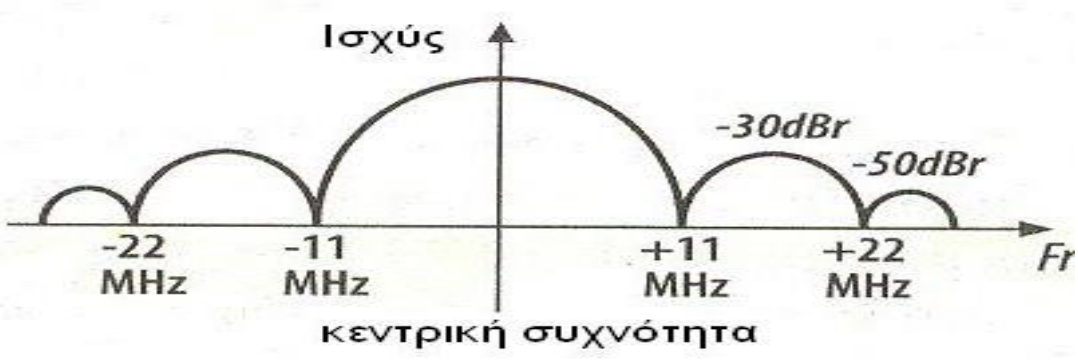
Στην προδιαγραφή αυτού του φυσικού στρώματος, ορίστηκε σαν spreading code η λέξη Barker των 11 bits και συγκεκριμένα η λέξη «10110111000». Η λέξη Barker χρησιμοποιείται με σκοπό τη διάδοση των δεδομένων πριν τη διαβίβαση. Αυτό δίνει στα δεδομένα περισσότερο εύρος ζώνης και λιγότερη πυκνότητα ισχύος. Επίσης, προσφέρει μεγάλη ανοχή στη διασπορά της χρονικής καθυστέρησης λόγω διάδοσης μέσω πολλαπλών διαδρομών και σε παρεμβολές στενής ζώνης. Κάθε bit προστίθεται κατά modulo – 2 στην ακολουθία «10110111000» για να προκύψει η ακολουθία των chips που θα μεταδοθούν. Αυτό σημαίνει πως όταν το bit έχει τιμή «1», όπως παρατηρείται στην εικόνα 32, η

ακολουθία που μεταδίδεται είναι η λέξη Barker με όλα τα bit ανεστραμμένα. Αντίθετα, στην εικόνα 31 μπορείτε να παρατηρήσετε πως όταν το bit έχει τιμή «0» μεταδίδεται αυτούσια η λέξη Barker. Στην εικόνα που ακολουθεί φαίνεται η χρήση του κώδικα Barker μήκους 11 bit. Βέβαια, θα πρέπει να αναφερθεί πως επειδή οι κώδικες Barker έχουν μικρό μήκος, είναι κατάλληλοι για γρήγορο συγχρονισμό. [2][3]




**ΕΙΚΟΝΑ 38: ΚΩΔΙΚΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΤΟΥ ΚΩΔΙΚΑ BARKER ΜΗΚΟΥΣ 11 BIT**

Για το φυσικό στρώμα έχουν οριστεί 14 κανάλια στην μπάντα των 2,4 GHz με εύρος 5 MHz το κάθε ένα. Το πρώτο κανάλι έχει κεντρική συχνότητα 2,412 GHz και τα υπόλοιπα ακολουθούν κάθε 5 MHz. Στην πράξη κάθε κανάλι καταλαμβάνει περίπου 22 MHz εύρος, γύρο από την κεντρική του συχνότητα. Στην τεχνική αυτή, χρησιμοποιούνται φίλτρα RF, με αποτέλεσμα να καταπιέζονται οι πλευρικοί λοβοί έξω από τα 22 MHz κατά 30 και 50 dB κάτω από την ισχύ της κεντρικής συχνότητας. [2][3][7]



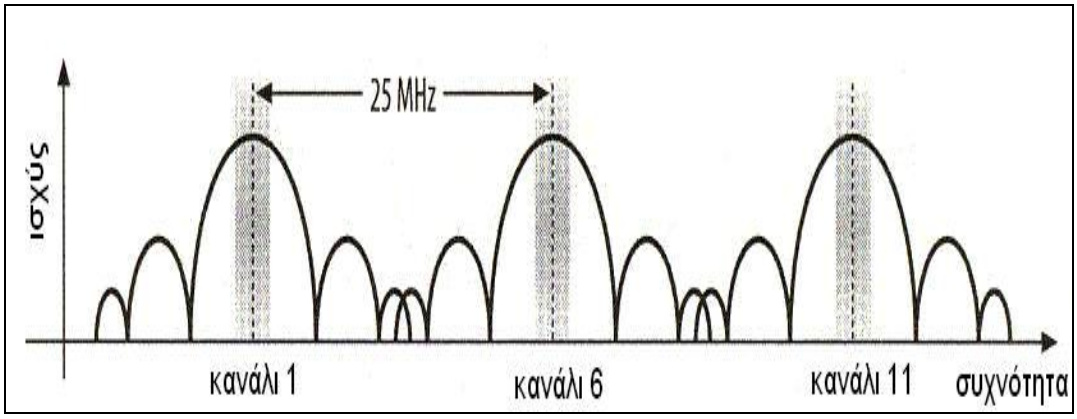

**ΕΙΚΟΝΑ 39: ΑΝΑΛΥΣΗ ΦΑΣΜΑΤΟΣ ΚΑΝΑΛΙΟΥ 802.11 DSSS PHY [3]**

Για να αποφεύγονται οι παρεμβολές, τα κανάλια που χρησιμοποιούνται σε διπλανές «κυψέλες», πρέπει να απέχουν μεταξύ τους 25 MHz, δηλαδή πέντε κανάλια των 5 MHz. Σ' αυτό το γεγονός, οφείλεται και η χρήση συγκεκριμένων καναλιών σε κάθε χώρα, διότι περιορίζει το μέγιστο αριθμό των καναλιών που μπορούν να χρησιμοποιηθούν. Στον επόμενο πίνακα φαίνονται τα διαθέσιμα κανάλια που μπορούν να χρησιμοποιηθούν ανά περιοχή για το φυσικό στρώμα.

**ΠΙΝΑΚΑΣ 15: ΔΙΑΘΕΣΙΜΑ ΚΑΝΑΛΙΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ [3]**

| ΠΕΡΙΟΧΗ/ΥΠΕΥΘΥΝΗ ΑΡΧΗ | ΕΠΙΤΡΕΠΟΜΕΝΑ ΚΑΝΑΛΙΑ |
|---|---|
| ΗΠΑ/FCC – Καναδας /IC | 1 έως 11 (2,412 – 2,462 GHz) |
| Ευρώπη(εκτός Γαλλίας & Ισπανίας)/ETSI | 1 έως 13 (2,412 – 2,472 GHz) |
| Γαλλία | 10 έως 13 (2,457 – 2,472 GHz) |
| Ισπανία | 10 έως 11 (2,457 – 2,462 GHz) |
| Ιαπωνία/MKK | 14 (2,484 GHz) |

Στην Ευρώπη υπάρχουν διαθέσιμα 13 κανάλια τα οποία φαίνονται στον πίνακα 16. Με βάση όμως τον περιορισμό για το διαχωρισμό των καναλιών που χρησιμοποιούνται σε διπλανές κυψέλες, λόγω της επικάλυψης των καναλιών, όπως αναλύθηκε στην αρχή, μένουν τελικά μόνο 3 διαθέσιμα κανάλια, το 1, το 6 και το 11. Τα κανάλια αυτά φαίνονται στο επόμενο σχήμα.




**ΕΙΚΟΝΑ 40: ΔΙΑΤΑΞΗ ΚΑΝΑΛΙΩΝ ΣΕ 802.11 DSSS [3]**

**ΠΙΝΑΚΑΣ 16: ΔΙΑΘΕΣΙΜΑ ΚΑΝΑΛΙΑ ΣΤΗΝ ΕΥΡΩΠΗ**

| Κανάλι | Κεντρική Συχνότητα (MHz) | Εύρος Καναλιού (MHz) |
|---|---|---|
| 1 | 2412 | 2401-2423 |
| 2 | 2417 | 2406-2428 |
| 3 | 2422 | 2411-2433 |
| 4 | 2427 | 2416-2438 |
| 5 | 2432 | 2421-2443 |
| 6 | 2437 | 2426-2448 |
| 7 | 2442 | 2431-2453 |
| 8 | 2447 | 2436-2458 |
| 9 | 2452 | 2441-2463 |
| 10 | 2457 | 2446-2468 |
| 11 | 2462 | 2451-2473 |
| 12 | 2467 | 2456-2478 |
| 13 | 2472 | 2461-2483 |

### 4.2.1.2 DSSS και υπόστρωμα PLCP

Στο παρακάτω σχήμα φαίνεται η μορφή του πλαισίου του υποστρώματος PLCP στο IEEE 802.11.

| PLCP Preamble | | PLCP Header | | | | Data |
|---|---|---|---|---|---|---|
| Sync | SFD | Signal | Service | Length | CRC | Data |
| 128 | 16 | 8 | 8 | 16 | 16 | |

**ΕΙΚΟΝΑ 41: ΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΥΠΟΣΤΡΩΜΑΤΟΣ PLCP ΣΤΟ IEEE 802.11**

Στη συνέχεια, αναλύονται τα τμήματα του πλαισίου του υποστρώματος PLCP.

PLCP Preamble

Το PLCP Preamble χρησιμεύει για το συγχρονισμό του πομπού και του δέκτη και για τη δήλωση της αρχής του πλαισίου. Περιέχει δύο πεδία, το Sync και το SFD. Αναλυτικότερα:

- **Sync**: Το πεδίο αυτό αποτελείται από μία ακολουθία από 128 bits, τα οποία είναι εναλλασσόμενα «0» και «1». Χρησιμεύει για την επίτευξη του συγχρονισμού μεταξύ πομπού και δέκτη, καθώς επίσης και για άλλους

σκοπούς, όπως για μέτρηση της συχνότητας του λαμβανόμενου σήματος ή ανίχνευση δυνατότερου σήματος σε συστήματα που χρησιμοποιούν περισσότερες της μίας κεραίες. [3][7]

- **SFD**: Το πεδίο αυτό σηματοδοτεί το τέλος του PLCP Preamble και την αρχή του υπόλοιπου πλαισίου. Η τιμή του είναι «0000010111001111». [3]

PLCP Header

Η επικεφαλίδα του PLCP πλαισίου αποτελείται από τέσσερα πεδία, το signal, το service, το length, το CRC. Αναλυτικότερα:

- **Signal**: Στο πεδίο αυτό κωδικοποιείται κατάλληλα ο ρυθμός μετάδοσης, δηλαδή τα 1 ή 2 Mbps.
- **Service**: Το πεδίο αυτό είναι διαθέσιμο για μελλοντική χρήση, έχει όλα τα bits ίσα με «0».
- **Length**: Το πεδίο αυτό περιέχει τον αριθμό των microseconds που χρειάζονται για την εκπομπή του πλαισίου ως 16 – μπιτου ακεραίου χωρίς πρόσημο.
- **CRC**: Το CRC είναι η συντομογραφία των λέξεων Cyclic Redundancy Code, όπου στα ελληνικά μεταφράζεται ως Κυκλικός Κώδικας Πλεονασμού και προστατεύει τα υπόλοιπα πεδία του PLCP Header. [3][7]

Data

- Το τμήμα αυτό περιέχει το MAC πλαίσιο και δεν υπάρχει κανένας περιορισμός σχετικά με το τμήμα αυτό.

#### 4.2.1.3 DSSS και υπόστρωμα PMD

Στο PMD υπόστρωμα προβλέπεται η υποστήριξη των δύο διαθέσιμων ρυθμών μετάδοσης, 1 και 2 Mbps. Μετά την κωδικοποίηση τα chips εκπέμπονται με ρυθμό 11 Mbps. Για ρυθμό μετάδοσης 1 Mbps χρησιμοποιείται η διαμόρφωση DBPSK (Differential Binary Phase Shift Keying), όπου το κάθε bit κωδικοποιείται από μία ακολουθία των 11 chips. Ο ρυθμός μετάδοσης αυτής της ακολουθίας είναι 11 Mbps, όπου κάθε μεταδιδόμενο σύμβολο μεταφέρει ένα chip, με συνέπεια ο πραγματικός ρυθμός μετάδοσης του bit να είναι 1 Mbps. Στο δεύτερο ρυθμό

μετάδοσης, δηλαδή των 2 Mbps, χρησιμοποιείται η διαμόρφωση DQPSK (Differential Quadrature Phase Shift Keying), όπου κάθε σύμβολο μεταφέρει δύο chips. Σε αυτήν την περίπτωση, τα τμήματα PLCP Preamble και PLCP Header μεταδίδονται σε ρυθμό 1 Mbps χρησιμοποιώντας διαμόρφωση DBPSK. Αυτό συμβαίνει επειδή η διαμόρφωση DBPSK είναι πιο ανθεκτική από την DQPSK στο θόρυβο, με αποτέλεσμα να δημιουργείται μικρότερη πιθανότητα λανθασμένης λήψης των δύο αυτών τμημάτων. Ακολουθεί ένας πίνακας με επιπλέον παραμέτρους, τις οποίες συναντήσαμε σε προηγούμενες παραγράφους. [1]

**ΠΙΝΑΚΑΣ 17: ΔΙΑΦΟΡΟΙ ΠΑΡΑΜΕΤΡΟΙ ΤΗΣ ΤΕΧΝΙΚΗΣ DSSS**

| ΠΑΡΑΜΕΤΡΟΣ | ΤΙΜΗ |
|---|---|
| Μέγιστο μήκος πλαισίου MAC | 4000 – 8191 bytes |
| Slot time | 20 μsec |
| SIFS time | 10 μsec |
| Contention window size | 31 έως 1023 slots |
| Preamble duration | 144 μsec |
| PLCP header duration | 48 μsec |

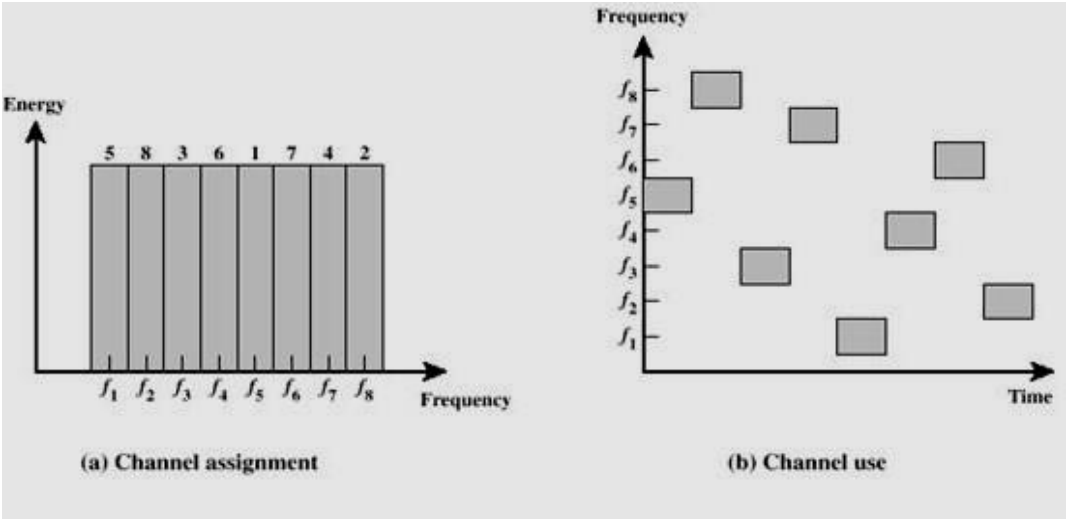
### 4.2.2 Frequency Hopping Spread Spectrum (FHSS)

Η τεχνική Frequency Hopping Spread Spectrum (FHSS) ήταν η πρώτη που χρησιμοποιήθηκε ευρέως σε εμπορικά προϊόντα. Τα πλεονεκτήματα αυτής της τεχνικής έναντι της τεχνικής Direct Sequence Spread Spectrum είναι τα απλούστερα και φθηνότερα ηλεκτρονικά για την υλοποίηση των ανάλογων συσκευών, η χαμηλότερη κατανάλωση ενέργειας και η δυνατότητα συνύπαρξης πολλών τέτοιων δικτύων στην ίδια περιοχή χωρίς να επηρεάζεται η συνολική διέλευση. Δεν μπορεί όμως να δώσει ταχύτητες μεταφοράς δεδομένων πάνω από 2 Mbps.

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). Η τεχνική αυτή μοιάζει με την κλασσική FDMA (Frequency Division Multiple Access), με τη διαφορά ότι κάθε χρήστης χρησιμοποιεί διάφορες φέρουσες ανάλογα με το hopping pattern του. Για να

επιτευχθεί επικοινωνία μεταξύ πομπού και δέκτη πρέπει ο δέκτης να γνωρίζει το hopping pattern του πομπού και να υπάρχει μεταξύ τους καλός συγχρονισμός. Αν οι συσκευές είναι συγχρονισμένες, θεωρητικά μπορούν να συνυπάρξουν μέχρι 79 συστήματα, όπου κάθε ένα θα χρησιμοποιεί μία δεδομένη στιγμή μία από τις 79 φέρουσες. Για να επιτευχθεί βέβαια αυτό, θα απαιτούσε τη χρήση ακριβών και πολύ επιλεκτικών φίλτρων στο δέκτη. Τα περισσότερα συστήματα που εργάζονται σε ζώνες χωρίς αδειοδότηση δε χρησιμοποιούν συγχρονισμό, ενώ αντίθετα, χρησιμοποιούν συγχρονισμό σε ζώνες όπου προβλέπεται η αδειοδότησή τους. [1][7]

Ένα πλεονέκτημα αυτής της τεχνικής, είναι η δυνατότητα συνύπαρξης διαφορετικών ασύρματων δικτύων, αρκεί τα hopping patterns τους να είναι διαφορετικά, δηλαδή σε κάθε χρονική στιγμή κάθε σύστημα να μεταδίδει σε διαφορετική φέρουσα. Είναι δυνατόν δυο FHSS συστήματα να λειτουργούν στην ίδια ζώνη συχνοτήτων και να χρησιμοποιούν τέτοια hopping patterns, ώστε να μην παρεμβάλλονται ποτέ το ένα στο άλλο. Τότε τα hopping patterns ονομάζονται ορθογώνια και η συνολική διέλευση μεγιστοποιείται. [3]

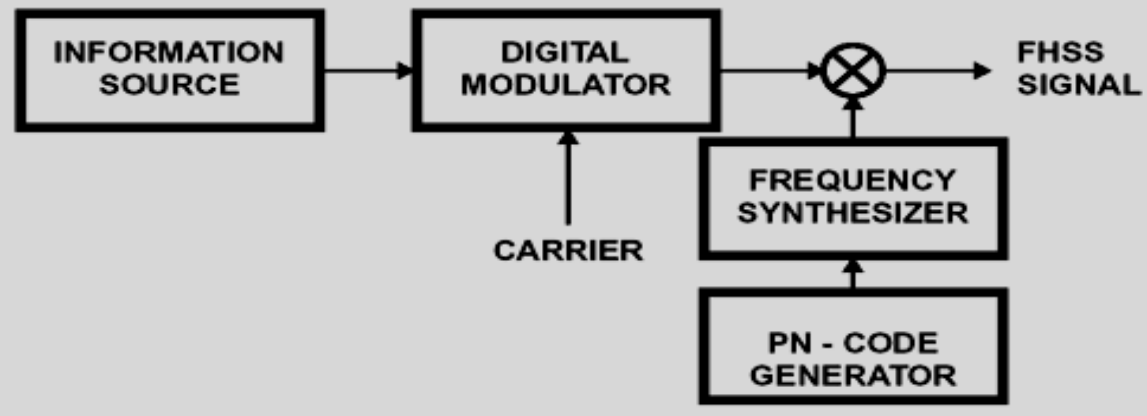



**ΕΙΚΟΝΑ 42: HOPPING PATTERNS [9]**

Επιπλέον, ένα ακόμα πλεονέκτημα της τεχνικής FHSS, είναι η δυνατότητα συνύπαρξης με χρήστες που εκπέμπουν σήματα στενής ζώνης. Αν η εκπομπή γίνεται με αρκετά μεγάλη ισχύ, τότε η παρεμβολή από το Frequency Hopping σύστημα σε αυτούς είναι αμελητέα, όπως επίσης και η δική τους παρεμβολή, εφόσον μπλοκάρουν μία μόνο φέρουσα από όσες αυτό χρησιμοποιεί.

### 4.2.2.1 FHSS και 802.11 PHY

Αρχικά, πριν αρχίσει η ανάλυση του φυσικού στρώματος, είναι πρέπον να αναφερθεί ο τρόπος με τον οποίο δημιουργείται το FHSS σήμα. Το FHSS σήμα δημιουργείται σε δύο στάδια. Στο πρώτο στάδιο, το σήμα πληροφορίας διαμορφώνει μία φέρουσα, με σκοπό τη δημιουργία ενός διαμορφωμένου σήματος στενής ζώνης. Στο δεύτερο στάδιο γίνεται η εξάπλωση του φάσματος (spread spectrum), δηλαδή το διαμορφωμένο σήμα απλώνεται σε εύρος φάσματος πολύ μεγαλύτερο από το αρχικό σήμα. Η διαδικασία αυτή, φαίνεται στην εικόνα που ακολουθεί.




**ΕΙΚΟΝΑ 43: ΔΙΑΔΙΚΑΣΙΑ ΕΞΑΠΛΩΣΗΣ ΦΑΣΜΑΤΟΣ ΣΤΗΝ ΤΕΧΝΙΚΗ FHSS**

Το φυσικό στρώμα διαιρεί την ISM μπάντα των 2,4 GHz σε κανάλια εύρους 1 MHz, με το πρώτο κανάλι, δηλαδή το κανάλι 0, να έχει την κεντρική του συχνότητα στα 2,4 GHz. Επιπλέον, ορίζεται ότι περίπου το 99% της ενέργειας του εκπεμπόμενου σήματος πρέπει να βρίσκεται μέσα στο κανάλι. Διαφορετικά κανάλια είναι διαθέσιμα για χρήση σε διάφορες χώρες, όπως παρατηρείτε στον πίνακα που ακολουθεί. [1][7]

**ΠΙΝΑΚΑΣ 18: ΔΙΑΦΟΡΑ ΚΑΝΑΛΙΑ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ**

| ΠΕΡΙΟΧΗ/ΥΠΕΥΘΥΝΗ ΑΡΧΗ | ΕΠΙΤΡΕΠΟΜΕΝΑ ΚΑΝΑΛΙΑ | ΑΡΙΘΜΟΣ HOPPING PATTERN/ΟΜΑΔΑ |
|---|---|---|
| ΗΠΑ/FCC – Καναδάς/IC | 2 έως 79(2,402 – 2,479 GHz) | 26 |
| Ευρώπη(εκτός Γαλλίας & Ισπανίας)/ETSI | 2 έως 79(2,402 – 2,479 GHz) | 26 |
| Γαλλία | 48 έως 82(2,448 – 2,482 GHz) | 27 |
| Ισπανία | 47 έως 73(2,447 – 2,473 GHz) | 35 |
| Ιαπωνία/MKK | 73 έως 95(2,473 – 2,495 GHz) | 13 |

*FHSS Hopping Pattern for North America and Europe*

| Set | Hopping Pattern |
|---|---|
| 1 | {0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75} |
| 2 | {1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76} |
| 3 | {2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,72,77} |

*FHSS Hopping Pattern for Japan*

| Set | Hopping Pattern |
|---|---|
| 1 | {6,9,12,15} |
| 2 | {7,10,13,16} |
| 3 | {8,11,14,17} |

*FHSS Hopping Pattern for Spain*

| Set | Hopping Pattern |
|---|---|
| 1 | {0,3,6,9,12,15,18,21,24} |
| 2 | {1,4,7,10,13,16,19,22,25} |
| 3 | {2,5,8,11,14,17,20,23,26} |

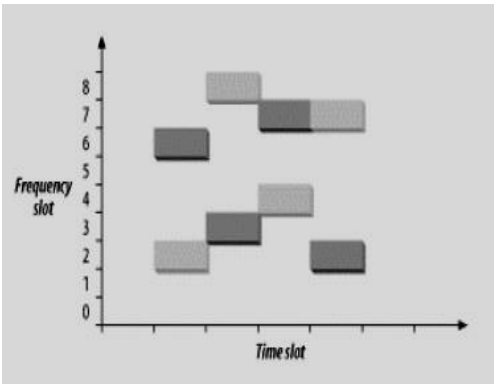
*FHSS Hopping Pattern for France*

| Set | Hopping Pattern |
|---|---|
| 1 | {0,3,6,9,12,15,18,21,24,27,30} |
| 2 | {1,4,7,10,13,16,19,22,25,28,31} |
| 3 | {2,5,8,11,14,17,20,23,26,29,32} |

**ΕΙΚΟΝΑ 44: FHSS HOPPING PATTERNS ΣΕ ΔΙΑΦΟΡΕΣ ΧΩΡΕΣ [7]**

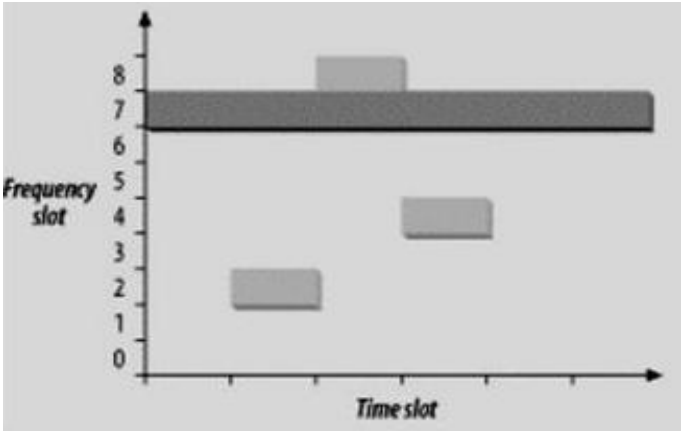
Σε μία ακολουθία μεταπήδησης, σε κάθε βήμα μεταπήδησης (hop), ο πομπός, μεταδίδει σε μία συγκεκριμένη κεντρική συχνότητα λειτουργίας για ένα συγκεκριμένο χρονικό διάστημα (dwell time). Ο χρόνος εκπομπής σε ένα κανάλι, δηλαδή το dwell time, έχει ορισθεί αυστηρά στα 0,4 seconds περίπου, καθώς επίσης, αυστηρά έχουν ορισθεί και οι λεπτομέρειες της μεταπήδησης από κανάλι

σε κανάλι ανάλογα με το hopping pattern. Έχουν οριστεί συγκεκριμένες αριθμητικές ακολουθίες των διαθέσιμων καναλιών ως hopping patterns και έχουν διαιρεθεί σε μη επικαλυπτόμενες ομάδες. Οποιαδήποτε δύο μέλη της ίδιας ομάδας είναι ορθογώνια μεταξύ τους. Όπως και στα διαθέσιμα κανάλια , έτσι και στα hopping patterns, κάθε χώρα έχει διαφορετικούς περιορισμούς, όπως μπορείτε να παρατηρήσετε στους παραπάνω πίνακες. [1][3]




Στις ΗΠΑ και στην Ευρώπη οι αρμόδιοι οργανισμοί έχουν θεσπίσει διαφορετικούς περιορισμούς για τα συστήματα Frequency Hopping. Για παράδειγμα, στις ΗΠΑ η FCC απαιτεί τουλάχιστον 75 διαφορετικά κανάλια, ενώ η Ευρωπαϊκή ETSI μόλις 20, περιορίζοντας όμως περισσότερο την ακτινοβολούμενη ισχύ. Τελικά, για να ικανοποιεί ένα προϊόν τις προδιαγραφές και της FCC και της ETSI πρέπει να ικανοποιεί τις αυστηρότερες από αυτές σε κάθε τομέα.

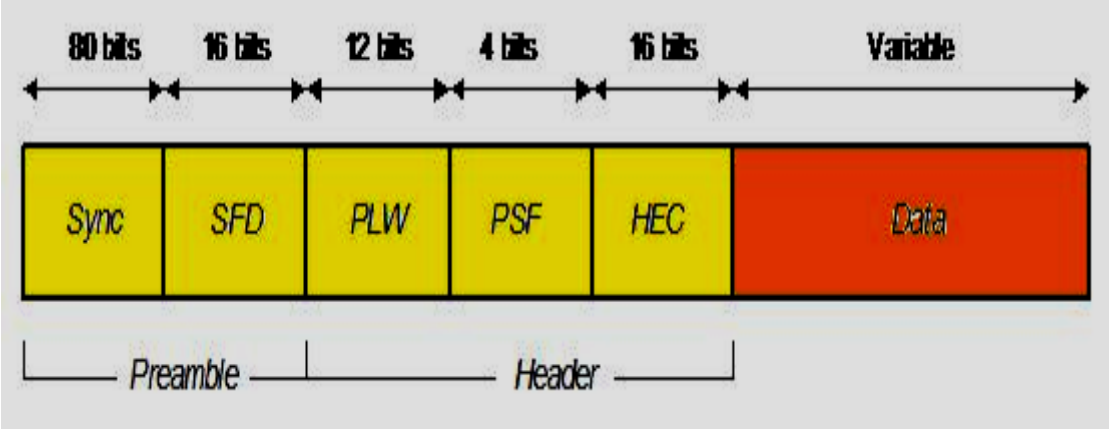
Ολοκληρώνοντας για το φυσικό στρώμα, θα πρέπει να αναφερθεί πως η επίδοση του Frequency Hopping φυσικού στρώματος παρουσία θορύβου και παρεμβολών στενής ζώνης, είναι αρκετά καλή και μειώνεται γραμμικά όσο αυξάνονται οι παρεμβολές. Μεγάλες παρεμβολές σε ένα από τα χρησιμοποιούμενα κανάλια, δεν προκαλεί σπουδαία μείωση της επίδοσης. Όσο όμως ο αριθμός των καναλιών που επηρεάζονται από τις παρεμβολές αυξάνεται, τόσο η μείωση της επίδοσης αρχίζει να γίνεται πιο έντονη.




**ΕΙΚΟΝΑ 45: AVOIDING INTERFERENCES**

### 4.2.2.2 FHSS και υπόστρωμα PLCP

Η γενική μορφή του υποστρώματος PLCP στο IEEE 802.11, παρουσιάζεται στο παρακάτω σχήμα.




**ΕΙΚΟΝΑ 46: ΓΕΝΙΚΗ ΜΟΡΦΗ ΤΟΥ ΥΠΟΣΤΡΩΜΑΤΟΣ PLCP ΣΤΟ IEEE 802.11**

PLCP Preamble

Το PLCP Preamble πλαίσιο χρησιμοποιείται για το συγχρονισμό του πομπού με το δέκτη και για τον ορισμό της αρχής του πλαισίου. Περιέχει δύο πεδία, το Sync και το Start Frame Delimiter (SFD).

- **Sync**: Το πεδίο αυτό χρησιμεύει για την επίτευξη του συγχρονισμού πομπού και δέκτη. Αποτελείται από μία ακολουθία από εναλλασσόμενα «0» και «1». Επίσης, χρησιμοποιείται και για άλλους σκοπούς, όπως για τη μέτρηση της συχνότητας του λαμβανόμενου σήματος ή για την ανίχνευση δυνατότερου σήματος σε συστήματα που χρησιμοποιούν περισσότερες από μία κεραίες.
- **SFD**: Το πεδίο αυτό σηματοδοτεί το τέλος του πλαισίου PLCP Preamble και συγχρόνως την αρχή του υπόλοιπου πλαισίου. Περιέχει την ακολουθία «0000110010111101». [3][7]

PLCP Header

Η επικεφαλίδα του πλαισίου αποτελείται από τρία πεδία, το PSDU Length Word (PLW), το PLCL Signaling (PSF) και το Header Error Check (HEC).

- **PLW**: Το μήκος του MAC πλαισίου που κουβαλάει το PLCP πλαίσιο. Το μήκος του μπορεί να είναι μέχρι 4095 bytes.

- **PSF**: Στο πεδίο αυτό, το πρώτο bit είναι δεσμευμένο για μελλοντική χρήση και τίθεται πάντα ίσο με το «0» και στα υπόλοιπα τρία bits κωδικοποιείται ο χρησιμοποιούμενος ρυθμός μετάδοσης. Παρόλο που το πρότυπο υποστηρίζει ρυθμούς μετάδοσης από 1 Mbps έως και 4,5 Mbps, με διαφορά διαδοχικών ρυθμών 500 kbps, έχει οριστεί σχήμα διαμόρφωσης μόνο για τους ρυθμούς μετάδοσης 1 και 2 Mbps.
- **HEC**: Το πεδίο αυτό περιέχει ένα 16- μπιτο CRC που προστατεύει την επικεφαλίδα του πλαισίου. [3][7]

Data

Το τμήμα αυτό περιέχει το MAC πλαίσιο. Πριν την τοποθέτησή του περνάει από μία διαδικασία ανακατώματος προκειμένου να μοιάζει με λευκό θόρυβο (whitening). Σε αντίθεση με το Direct Sequence φυσικό στρώμα, μόνο το Data υπόκειται σε αυτή τη διαδικασία και όχι ολόκληρο το PLCP πλαίσιο.

### 4.2.2.3 FHSS και υπόστρωμα PMD

Το πρότυπο αυτό υποστηρίζει κανονικά δύο ρυθμούς μετάδοσης, 1 και 2 Mbps. Για ρυθμό μετάδοσης 1 Mbps χρησιμοποιείται διαμόρφωση 2 – GFSK (Gaussian Frequency Shift Keying), όπου κάθε σύμβολο μεταφέρει ένα bit πληροφορίας. Η ισχύς εκπομπής που έχει οριστεί από το πρότυπο είναι μεταξύ 10 και 100 mWatt. Για ρυθμό μετάδοσης 2 Mbps χρησιμοποιείται διαμόρφωση 4 - GFSK (Gaussian Frequency Shift Keying), δηλαδή κάθε σύμβολο μεταφέρει 2 bits πληροφορίας. Δε θα πρέπει να ξεχάσουμε να αναφέρουμε πως η επικεφαλίδα του PLCP πλαισίου μεταδίδεται με χρήση της διαμόρφωσης 2 – GFSK με ρυθμό 1 Mbps. Τέλος, τονίζουμε πως υπάρχει πρόβλεψη για υποβάθμιση του ρυθμού μετάδοσης στο 1 Mbps, αν η ποιότητα του σήματος είναι πολύ χαμηλή. Ακολουθεί ένας πίνακας με επιπλέον παραμέτρους, τις οποίες συναντήσατε σε προηγούμενες παραγράφους.

**ΠΙΝΑΚΑΣ 19: ΔΙΑΦΟΡΟΙ ΠΑΡΑΜΕΤΡΟΙ ΤΗΣ ΤΕΧΝΙΚΗΣ FHSS [3]**

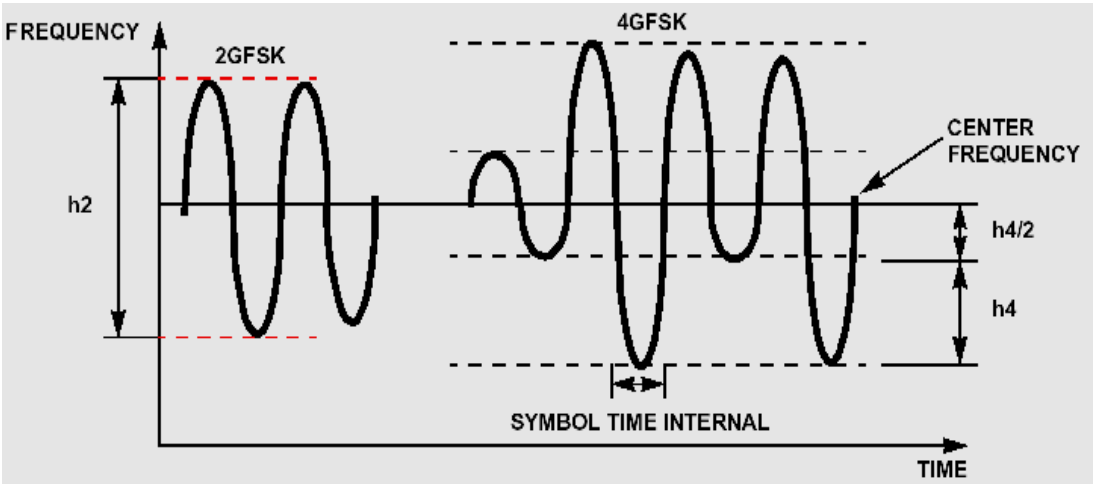
| ΠΑΡΑΜΕΤΡΟΣ | ΤΙΜΗ |
|---|---|
| Μέγιστο μήκος πλαισίου MAC | 4095 bytes |
| Slot time | 50 μsec |
| SIFS time | 28 μsec |

| ΠΑΡΑΜΕΤΡΟΣ | ΤΙΜΗ |
|---|---|
| Contention window size | 15 έως 1023 slots |
| Preamble duration | 96 μsec |
| PLCP header duration | 32 μsec |

## Διαμόρφωση Σήματος κατά GFSK (Gaussian Frequency Shift Keying)

Στην τεχνική FHSS αναφέρθηκε η διαμόρφωση GFSK (Gaussian Frequency Shift Keying), όπως βέβαια και στην τεχνική DSSS, για τη μετάδοση πληροφορίας.

Όπως γνωρίζουμε, το σήμα πληροφορίας διαμορφώνει αρχικά μία φέρουσα, συνήθως με FSK διαμόρφωση. Η FSK διαμόρφωση χρησιμοποιείται για το λόγο ότι είναι εύκολο να αποδιαμορφωθεί ασύμφωνα (non – coherently), δηλαδή ο αποδιαμορφωτής να γνωρίζει τη φάση της φέρουσας. Ένας επιπλέον λόγος που χρησιμοποιείται είναι επειδή είναι δύσκολο να επιτύχουμε σύμφωνη αποδιαμόρφωση στα FH. Στο σχήμα που ακολουθεί περιγράφεται ο τρόπος διαμόρφωσης κατά GFSK. [1][7]




ΕΙΚΟΝΑ 47: ΔΙΑΜΟΡΦΩΣΗ ΚΑΤΑ GFSK

Στην 2 - GFSK

Το 1 μεταδίδεται σαν μία συχνότητα fc + h2/2 x fc.

Το 0 μεταδίδεται σαν μία συχνότητα fc - h2/2 x fc.

Στην 4 - GFSK

Το 10 μεταδίδεται σαν μία συχνότητα fc + 1.5 x h4 x fc.

Το 11 μεταδίδεται σαν μία συχνότητα fc + 0.5 x h4 x fc.

Το 01 μεταδίδεται σαν μία συχνότητα fc - 0.5 x h4 x fc.

Το 00 μεταδίδεται σαν μία συχνότητα fc -1.5 x h4 x fc.

Από τα παραπάνω, παρατηρούμε ότι η αλλαγή συχνότητας γίνεται ομαλά. Αυτό επιτυγχάνεται περνώντας το σήμα από ένα φίλτρο με Gaussian χαρακτηριστική και σ' αυτό οφείλεται και η ονομασία της διαμόρφωσης ως GFSK (Gaussian Frequency Shift Keying). Το φιλτράρισμα αυτό επιτυγχάνει να περιορίσει το φάσμα του εκπεμπόμενου σήματος.

Η IEEE 802.11 προδιαγράφει ελάχιστο ρυθμό μετάδοσης 1 Mbps με διαμόρφωση 2 – GFSK, ενώ προαιρετικά ορίζεται ρυθμός μετάδοσης 2 Mbps με διαμόρφωση 4 – GFSK. Στον επόμενο πίνακα παρουσιάζονται συνοπτικά αυτά που ορίζει το πρότυπο.

**ΠΙΝΑΚΑΣ 20: ΙΔΙΟΤΗΤΕΣ ΤΟΥ GFSK ΟΠΩΣ ΟΡΙΖΟΝΤΑΙ ΑΠΟ ΤΟ ΠΡΟΤΥΠΟ IEEE 802.11**

| Symbol | Carrier Deviation | Modulation Index |
|---|---|---|
| 1 Mbps με διαμόρφωση 2 – GFSK | | |
| 1 | 0.5 x h2 x fclk | 0.16 |
| 0 | -0.5 x h2 x fclk | 0.16 |
| 2 Mbps με διαμόρφωση 4 – GFSK | | |
| 10 | 1.5 x h4 x fclk | 0.216 |
| 11 | 0.5 x h4 x fclk | 0.072 |
| 01 | -0.5 x h4 x fclk | 0.072 |
| 00 | -1.5 x h4 x fclk | 0.216 |

όπου h2=0.32, h4=0.45 x h2, fclk=1MHz.

### 4.2.3 Σύγκριση FHSS με DSSS τεχνική

Στην ενότητα αυτή παρουσιάζετε μία σύγκριση ανάμεσα στο FHSS και στο DSSS.

Κάλυψη και αριθμός χρηστών

Σε εγκαταστάσεις ευρείας κάλυψης με μεγάλο αριθμό χρηστών, τα συστήματα FHSS είναι πιο εύκολα στην εγκατάσταση. Βέβαια μπορούν και τα DSSS συστήματα να χρησιμοποιηθούν σε τέτοιες εγκαταστάσεις, αλλά η σχεδίαση τους θα πρέπει να είναι πιο προσεχτική. Παραδείγματος χάριν, υπάρχει η δυνατότητα τοποθέτησης κατευθυντήρων κεραιών, ώστε να μειωθούν οι επικαλύψεις, όμως αυξάνεται το κόστος εγκατάστασης.

Ανεκτικότητα σε θόρυβο και παρεμβολές

Στην κατηγορία αυτή υπάρχουν δύο περιπτώσεις. Στην πρώτη περίπτωση, όταν η παρεμβολή καλύπτει ένα μεγάλο εύρος ζώνης του φάσματος, η τεχνική FHSS είναι πιο ανεκτική από την DSSS. Για παράδειγμα, όταν έχουμε παρεμβολή με εύρος 22 MHz, το DSSS σύστημα σταματάει να λειτουργεί, σε αντίθεση με το FHSS σύστημα που συνεχίζει να λειτουργεί με απώλεια μόλις 33% της χωρητικότητας του.

Στη δεύτερη περίπτωση, δηλαδή σε παρεμβολή στενής ζώνης, ένα σύστημα FHSS χάνει ένα ή το πολύ δύο κανάλια, ενώ στο DSSS σύστημα, αν η παρεμβολή είναι μεγάλης ισχύος, μπορεί να οδηγήσει σε απώλεια της ζεύξης.

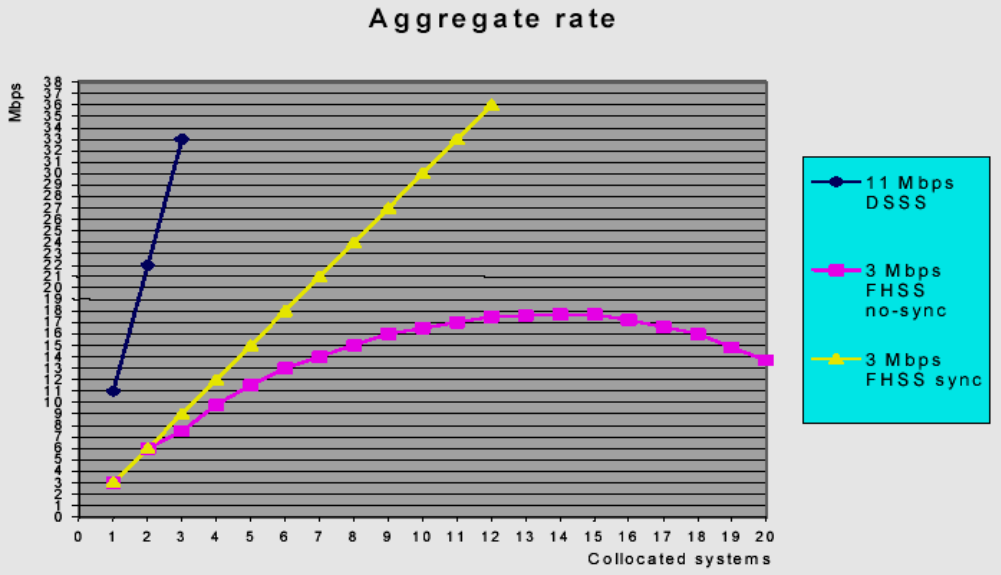
Διαπερατότητα (throughput)

Ένα DSSS σύστημα έχει ρυθμό στο φυσικό μέσο μέχρι 11 Mbps. Έτσι η αποτελεσματικότητα ενός τέτοιου συστήματος είναι 0.5 bps/Hz. Τα FHSS συστήματα έχουν ρυθμούς μέχρι 3 Mbps. Έτσι η αποτελεσματικότητα τους είναι 3 bps/Hz. Μετά την απόφαση της FCC να επιτραπούν κανάλια εύρους 5 MHz είναι δυνατό να υπάρξουν FHSS συστήματα με ρυθμούς 15 Mbps. Η πραγματική διαπερατότητα είναι μέχρι 7 Mbps για ένα DSSS σύστημα και 2 Mbps για ένα FHSS.

Συνολική Διαπερατότητα

Σε μία ζώνη με τρία συστήματα που μπορούν να συνυπάρξουν, η συνολική διαπερατότητα για το DSSS είναι 21 Mbps. Σε ένα τέτοιο σύστημα δεν συμβαίνουν συγκρούσεις, διότι τα κανάλια δεν επικαλύπτονται. Η διαπερατότητα αυξάνεται με γραμμικό τρόπο με την αύξηση του αριθμού των συστημάτων.

Όπως αναφέρθηκε και παραπάνω, τα FHSS συστήματα μπορούν να λειτουργήσουν με συγχρονισμένο και με μη συγχρονισμένο τρόπο στις ζώνες που δεν υπάρχει αδειοδότηση. Όταν έχουμε μη συγχρονισμένη μετάδοση, τότε συμβαίνουν συγκρούσεις οι οποίες μειώνουν τη διαπερατότητα. Ο αριθμός των συγκρούσεων αυξάνεται όσο αυξάνεται και ο αριθμός των συστημάτων. Η αύξηση όμως δεν είναι γραμμική. Όταν ο αριθμός των AP (Access Point) πλησιάζει τους 15, ο αριθμός των συγκρούσεων είναι τόσο μεγάλος, που ελαττώνουν σημαντικά τη συνολική διαπερατότητα. Όπως παρατηρείτε στο επόμενο σχήμα, τα DSSS συστήματα παρέχουν υψηλότερη συνολική διαπερατότητα από τα ασύγχρονα συστήματα FHSS. Βέβαια θα πρέπει να τονιστεί πως τα σύγχρονα FHSS έχουν τη δυνατότητα να παρέχουν συνολικά τη μεγαλύτερη διαπερατότητα. Παρόλα αυτά, τα DSSS συστήματα έχουν τη δυνατότητα να παρέχουν την μεγαλύτερη διαπερατότητα ανά χρήστη.




**ΕΙΚΟΝΑ 48: ΣΥΝΟΛΙΚΗ ΔΙΑΠΕΡΑΤΟΤΗΤΑ ΑΝΑΛΟΓΑ ΜΕ ΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ**

Ασφάλεια ραδιοφορέα

Στην DSSS η ακολουθία chip είναι γνωστή καθώς επίσης και η φέρουσα είναι σταθερή, με αποτέλεσμα να μπορεί εύκολα να γίνει υποκλοπή της μεταδιδόμενης πληροφορίας. Η ασφάλεια επιτυγχάνεται αναγκαστικά στα ανώτερα επίπεδα, κωδικοποιώντας την πληροφορία, το οποίο όμως αυξάνει το κόστος της συσκευής λόγω της επεξεργαστικής ισχύος που απαιτείται.

Σε σύστημα FHSS η σειρά μεταγωγής καναλιών μπορεί να επιλεχθεί από τον χρήστη. Για να υποκλέψει κανείς θα πρέπει να γνωρίζει τον αριθμό των συχνοτήτων, τη σειρά με την οποία χρησιμοποιούνται και το χρονικό διάστημα στο οποίο γίνεται η μετάδοση σε κάθε φέρουσα (dwell time). Έτσι υπάρχει ένας τρόπος κωδικοποίησης που δουλεύει στο φυσικό επίπεδο και δεν απαιτείται κωδικοποίηση σε ανώτερο επίπεδο.

Συμπέρασμα

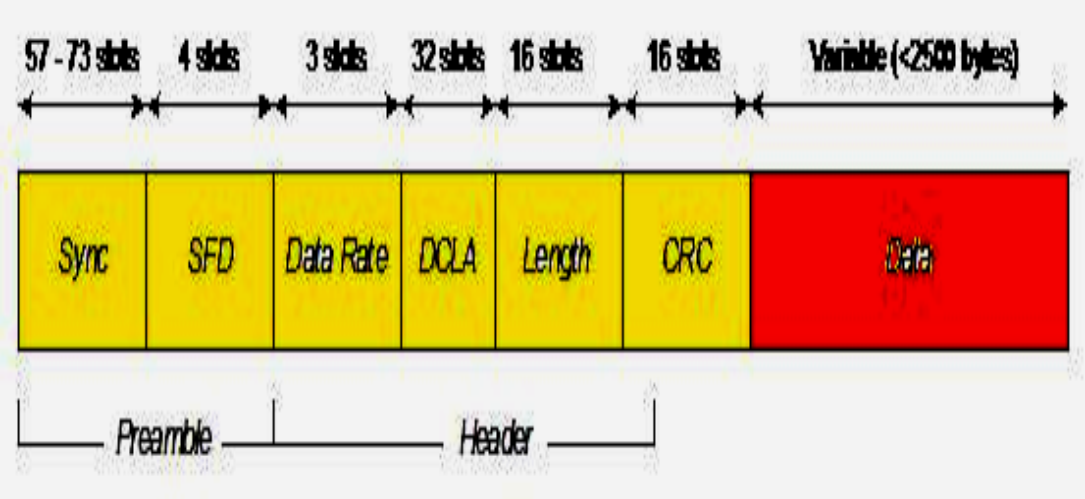
Η DSSS παρέχει ρυθμούς μέχρι 11 Mbps, αλλά είναι αρκετά ευαίσθητη σε παρεμβολές και multipath. Αντίθετα, η FHSS παρέχει μικρότερους ρυθμούς, μέχρι 2 Mbps, αλλά είναι αρκετά ανθεκτική σε περιβάλλον όπου υπάρχουν παρεμβολές και ανακλάσεις. Επιπλέον, η FHSS τεχνολογία παρέχει εξαιρετικές υλοποιήσεις κυψελών, παρέχοντας αξιοπιστία στη μετάδοση.

## 4.3 Υπέρυθρες Ακτίνες (Infrared)

Η τεχνική των υπέρυθρων ακτινών χρησιμοποιείται σπάνια και η λειτουργία τους βασίζεται στην εκπομπή παλμών διάρκειας 250 nsec, που παράγονται από τα LEDs (Light Emitting Diode) του πομπού. Η τεχνική διαμόρφωσης που χρησιμοποιεί είναι η PPM (Pulse Position Modulation) με ρυθμούς μετάδοσης 1 και 2 Mbps, που επιτυγχάνονται μέσω ανάκλασης των υπέρυθρων ακτινών. Η λειτουργία του περιορίζεται κυρίως σε εσωτερικούς χώρους. Η ακτίνα λειτουργίας του μπορεί να φτάσει περίπου τα 20 μέτρα, σε ελεύθερο οπτικό πεδίο.

### 4.3.1 Υπέρυθρες ακτίνες και υπόστρωμα PLCP

Η γενική μορφή του υποστρώματος PLCP στο IEEE 802.11, παρουσιάζεται στο παρακάτω σχήμα.




ΕΙΚΟΝΑ 49: ΓΕΝΙΚΗ ΜΟΡΦΗ ΤΟΥ ΥΠΟΣΤΡΩΜΑΤΟΣ PLCP

Το μήκος του PLCP πλαισίου μετριέται σε σχισμές (slots) των 250 ns, όσο δηλαδή διαρκεί ο βασικός παλμός. Τα τμήματα του πλαισίου περιγράφονται στην συνέχεια.

PLCP Preamble

Όπως στις τεχνικές DSSS και FHSS, το τμήμα αυτό χρησιμεύει για συγχρονισμό και οριοθέτηση της αρχής του πλαισίου. Περιέχει τα πεδία Sync και SFD, μόνο που το μήκος του είναι μικρότερο σε σύγκριση με τα προηγούμενα, επειδή η μέθοδος αποδιαμόρφωσης είναι ασύμφωνη (non-coherent) και δεν απαιτεί ανάκτηση φέροντος σήματος και ακριβή συγχρονισμό.

PLCP Header

Όσον αφορά την επικεφαλίδα, στο πεδίο Data Rate κωδικοποιείται ο ρυθμός μετάδοσης, ενώ τα πεδία Length και CRC είναι τα ίδια με αυτά του φυσικού στρώματος του DSSS. Το πεδίο DCLA (DC Level Adjustment) περιέχει μία ακολουθία 16 σχισμών, επιτρέποντας στο δέκτη να θέσει το κατώφλι ισχύος για τη λήψη απόφασης της τιμής του κάθε bit.

Data

Περιέχει το MAC πλαίσιο προς μετάδοση και το μήκος του περιορίζεται στα 2500 bytes.

### 4.3.2 Υπέρυθρες ακτίνες και υπόστρωμα PMD

Το PMD υπόστρωμα χρησιμοποιεί δύο σχήματα διαμόρφωσης για να πετύχει τους διαθέσιμους ρυθμούς μετάδοσης των 1 και 2 Mbps. Η διαμόρφωση 16 – PPM (Pulse Position Modulation) χρησιμοποιείται για ρυθμό 1 Mbps. Κάθε 4 bits πληροφορίας αντιστοιχίζονται σε μία ακολουθία 16 bits. Κάθε bit διαρκεί 250 nsec και κάθε ακολουθία 16 bits έχει μόνο ένα από αυτά ίσο με «1» και όλα τα υπόλοιπα μηδενικά. Έτσι, κάθε τετράδα από bits πληροφορίας κωδικοποιείται από τη θέση του «1» στη 16 – μπιτη ακολουθία. Για το ρυθμό μετάδοσης των 2 Mbps χρησιμοποιείται η 4 – PPM, όπου με την ίδια λογική κάθε ζευγάρι από bits πληροφορίας κωδικοποιούνται σε μια ακολουθία από 4 bits. Κατά τη μετάδοση τα bits «1» από την παρουσία ισχύος, ενώ τα bits «0» από την απουσία. Τα σήματα μεταδίδονται στο κοντινό ορατό φάσμα των 850 με 950 nm, με μέγιστο όριο ισχύος μετάδοσης να φτάνει τα 2 Watt με μία μέση τιμή ίση με 125 ή 250 mWatt.

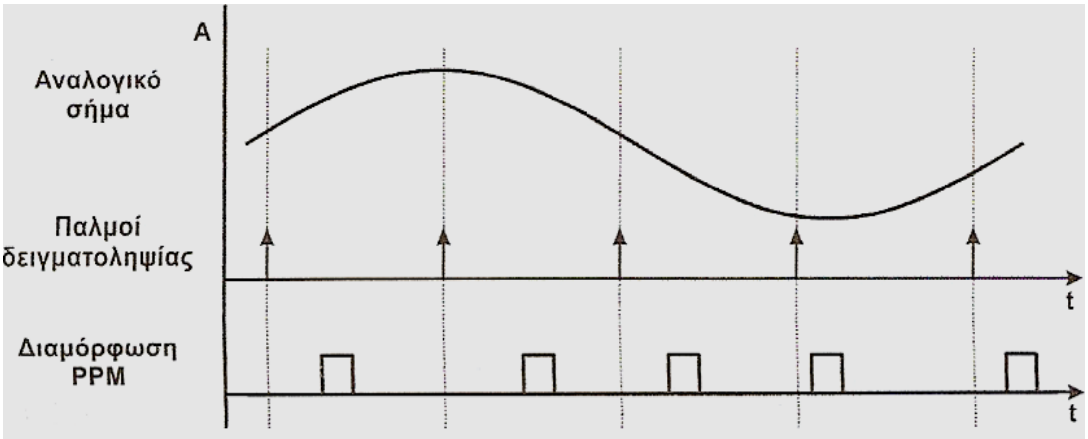
### Διαμόρφωση Σήματος κατά PPM (Pulse Position Modulation)

Η διαμόρφωση PPM (Pulse Position Modulation) χρησιμοποιείται στις υπέρυθρες ακτίνες και δεν είναι τίποτα άλλο από έναν αριθμό από κυματομορφές που βασίζονται στην M – ary διαμόρφωση. Στη διαμόρφωση αυτή κάθε υψηλό επίπεδο σημάτων χρησιμοποιείται για το συμβολισμό δύο ή περισσότερων bit δυαδικής πληροφορίας. Αυτό εκφράζεται από τον τύπο:

$$K = 2m ,$$

Όπου K: ο αριθμός των bits ανά παλμό,

και m: ο αριθμός των σχισμών.




**ΕΙΚΟΝΑ 50: ΔΙΑΜΟΡΦΩΣΗ ΣΗΜΑΤΟΣ ΚΑΤΑ PPM [1]**

Όπως μπορείτε να παρατηρήσετε στην εικόνα που προηγείται, στον άξονα του χρόνου, η θέση των σταθερής διάρκειας παλμών μεταβάλλεται σε συνάρτηση με το πλάτος του αναλογικού σήματος. Ένα μεγάλο πλεονέκτημα αυτής της διαμόρφωσης είναι οι μειωμένες απαιτήσεις σε ισχύ. Αυτό οφείλεται στο γεγονός ότι μεταδίδονται πολύ σύντομοι παλμοί ακολουθούμενοι από σχετικά μεγάλες περιόδους «σιωπής». Η ιδιότητά της αυτή, την καθιστά ιδιαίτερα ελκυστική σε εφαρμογές που απαιτούν χαμηλή κατανάλωση ισχύος. [1]

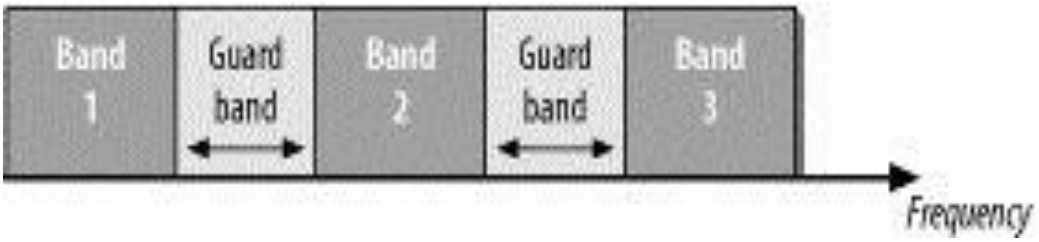
## 4.4 OFDM (Orthogonal Frequency Division Multiplexing)

Η OFDM (Orthogonal Frequency Division Multiplexing) είναι μία τεχνική μετάδοσης πολλαπλών φερόντων του φυσικού στρώματος ιδιαίτερα κατάλληλη για μετάδοση υψηλού ρυθμού δεδομένων σε περιβάλλοντα με διασπορά καθυστέρησης. Με την τεχνική OFDM τα δεδομένα μεταδίδονται χρησιμοποιώντας ένα μεγάλο αριθμό καναλιών μικρού εύρους ζώνης. Συγκεκριμένα, μία συμβολοακολουθία υψηλού ρυθμού χωρίζεται σε πολλές χαμηλότερου ρυθμού που διαμορφώνουν τα φέροντα, στα οποία είναι χωρισμένο το φάσμα (subcarriers), και μεταδίδονται παράλληλα σε στενού εύρους κανάλια. Έτσι, ο χρόνος συμβόλου σε κάθε subcarrier μεγαλώνει κατά τον αριθμό των φερόντων, με αποτέλεσμα την αυξημένη ανθεκτικότητα σε διασπορά καθυστέρησης λόγω της πολύοδης διάδοσης. [5]

Τις βάσεις για την ανάπτυξη του OFDM έθεσε η εισαγωγή της τεχνικής FDM για επικοινωνίες δεδομένων στα τέλη της δεκαετίας του ’50. Και οι δύο τεχνικές, η OFDM και η FDM, διαιρούν το διαθέσιμο εύρος ζώνης σε φέτες που λέγονται μεταφορείς ή υπομεταφορείς (subcarriers), και καθιστά εκείνους τους μεταφορείς

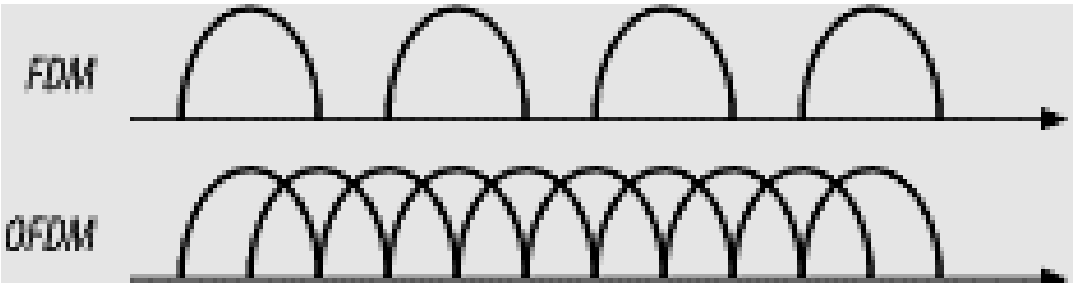
διαθέσιμους ως ευδιάκριτα κανάλια για τη μετάδοση στοιχείων. Το OFDM ωθεί τη ρυθμοαπόδοση με τη χρησιμοποίηση διάφορων υπομεταφορέων παράλληλα και πολλαπλασιάζοντας στοιχεία πέρα από το σύνολο υπομεταφορέων. [3]

Παραδοσιακά το FDM χρησιμοποιήθηκε ευρέως με κινητά πρώτης γενιάς για τη ραδιοκατανομή των καναλιών. Σε κάθε χρήστη δόθηκε ένα αποκλειστικό κανάλι και οι ζώνες φρουράς χρησιμοποιήθηκαν για να εξασφαλίσουν ότι η φασματική διαρροή από έναν χρήστη δεν προκαλούσε προβλήματα στους χρήστες των παρακείμενων καναλιών. Στο σχήμα που ακολουθεί περιγράφονται τα παραπάνω.




**ΕΙΚΟΝΑ 51: ΔΙΑΜΟΡΦΩΣΗ FDM [3]**

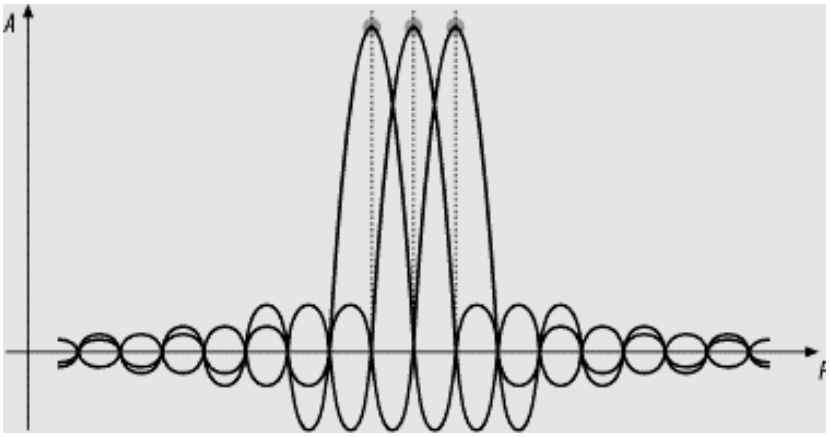
Το μειονέκτημα όμως του παραδοσιακού FDM είναι ότι η φρουρά ξοδεύει άσκοπα, σπαταλάει, το εύρος ζώνης με αποτέλεσμα να μειώνει τις ικανότητες του. Λύση σε αυτό το πρόβλημα δίνει η τεχνική OFDM με το να επιλέγει τα κανάλια που επικαλύπτουν, αλλά δεν παρεμποδίζουν το ένα το άλλο. Αυτή τη διαφορά μεταξύ των δυο τεχνικών μπορείτε εύκολα να τη διακρίνετε στο επόμενο σχήμα. [3]




**ΕΙΚΟΝΑ 52: ΔΙΑΦΟΡΑ ΜΕΤΑΞΥ ΤΩΝ ΤΕΧΝΙΚΩΝ FDM ΚΑΙ OFDM [3]**

Το 1966 ο Chang ήταν ο πρώτος που κατασκεύασε τη δομή ενός συστήματος OFDM και τη δημοσίευσε χρησιμοποιώντας επικαλυπτόμενα ορθογωνικά σήματα για τη μετάδοση των δεδομένων. Η ορθογωνιότητα μεταξύ σημάτων ισχύει όταν αυτά είναι αμοιβαία ανεξάρτητα και εξασφαλίζει τη μετάδοση πολλαπλών σημάτων σε ένα κοινό κανάλι και την ανίχνευσή τους χωρίς παρεμβολές. Τυχόν απώλειά της οδηγεί σε ανεπιθύμητη μίξη των σημάτων και συνεπώς σε υποβιβασμό της

ποιότητας του συστήματος, γεγονός που την καθιστά βασική επιδίωξη σε κάθε τεχνική μετάδοσης. Πρέπει όμως να προσέξουμε στην OFDM ότι τα subcarriers κάθε σήματος τοποθετούνται έχοντας τη μικρότερη θεωρητικά δυνατή απόσταση μεταξύ τους, γεγονός που συντελεί στην αποδοτικότερη αξιοποίηση του φάσματος, ενώ ταυτόχρονα διατηρείται η ορθογωνιότητα.

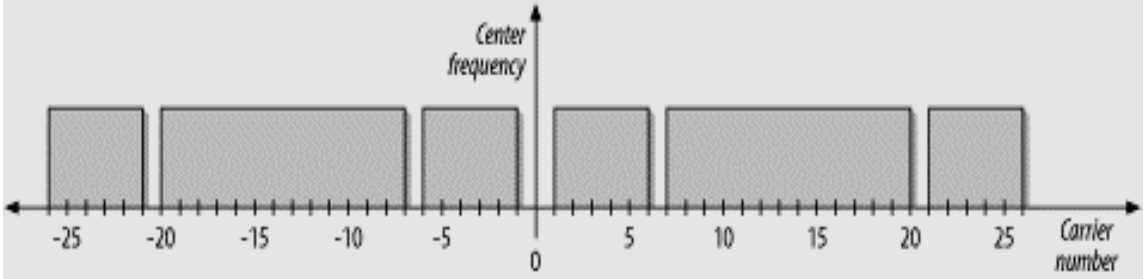


**ΕΙΚΟΝΑ 53: ΟΡΘΟΓΩΝΙΚΟΤΗΤΑ ΣΥΧΝΟΤΗΤΩΝ**

Το 1971 ο Weinstein εισήγαγε την ιδέα χρήσης του Διακριτού Μετασχηματισμού Fourier (DFT – Discrete Fourier Transform), για εκπομπή και λήψη σημάτων OFDM, εξαλείφοντας την ανάγκη ύπαρξης πολλών αναλογικών ταλαντωτών φερουσών. Αυτό παρείχε τη δυνατότητα εύκολης υλοποίησης ενός συστήματος OFDM, ιδιαίτερα με τη χρήση των Γρήγορων Μετασχηματισμών Fourier (FFT – Fast Fourier Transforms), οι οποίοι παρείχαν μια αποτελεσματικότερη υλοποίηση του Διακριτού Μετασχηματισμού Fourier (DFT). Έτσι, η απλούστερη υλοποίηση ενός συστήματος OFDM πραγματοποιείται με τη χρήση Ψηφιακών Επεξεργαστών Σήματος (DSP – Digital Signal Processors) και από το 1980 έχουμε την εισαγωγή της Ψηφιακής Ραδιοφωνικής Εκπομπής (DAB – Digital Audio Broadcasting). [2]

Το 1985 ο Cimini θεώρησε πώς το OFDM είναι κατάλληλο για τις ασύρματες επικοινωνίες. Σήμερα, κυκλοφορούν μερικά πρότυπα που έχουν υιοθετήσει αυτήν την τεχνική και τα οποία είναι το 802.11 a, g, n, το 802.16 ή αλλιώς WIMAX, το 802.20 και το 802.16e (Mobile WIMAX) του IEEE (Institute of Electrical and Electronics Engineers) και τέλος το Hiperlan/2 του ETSI (European Telecommunications Standards Institute). Θα πρέπει να αναφερθεί ότι τα παραπάνω σε συνδυασμό με κωδικοποίηση για τη διόρθωση σφαλμάτων, εξαιτίας των απότομων αλλαγών του ασύρματου περιβάλλοντος, κάνουν χρήση 52 φερουσών συχνοτήτων (48 για αποστολή δεδομένων και 4 για την επίτευξη του

συγχρονισμού) και εκπέμπουν στη ζώνη των 5 GHz με ταχύτητα μετάδοσης μέχρι 54Mbps. Τα κανάλια αριθμούνται από το -26 έως το 26 και οι φέρουσες απέχουν μεταξύ τους 0.3125 MHz. Η φέρουσα 0 δεν χρησιμοποιείται. [3]




**ΕΙΚΟΝΑ 54: ΔΟΜΗ ΕΝΟΣ OFDMA ΚΑΝΑΛΙΟΥ [3]**

Τέλος, η διαμόρφωση που χρησιμοποιείται σε κάθε subcarrier ποικίλει από BPSK μέχρι και 16 – QAM. Ακολουθεί ένας πίνακας με επιπλέον παραμέτρους, τις οποίες συναντήσατε σε προηγούμενες παραγράφους. [2][3]

**ΠΙΝΑΚΑΣ 21: ΔΙΑΦΟΡΟΙ ΠΑΡΑΜΕΤΡΟΙ ΤΗΣ ΤΕΧΝΙΚΗΣ OFDM**

| ΠΑΡΑΜΕΤΡΟΣ | ΤΙΜΗ |
|---|---|
| Μέγιστο μήκος πλαισίου MAC | 4095 bytes |
| Slot time | 9 μsec |
| SIFS time | 16 μsec |
| Contention window size | 15 έως 1023 slots |
| Preamble duration | 20 μsec |
| PLCP header duration | 4 μsec |

## 4.5 ΣΥΝΟΨΗ

Όπως γνωρίζετε το μοντέλο αναφοράς OSI χωρίζεται σε επτά επίπεδα. Το πρότυπο IEEE 802.11 αφορά τα δύο χαμηλότερα επίπεδα. Το χαμηλότερο επίπεδο είναι το φυσικό επίπεδο, το οποίο αναλύθηκε στο παρόν κεφάλαιο και στο οποίο προδιαγράφονται δυο τεχνικές διαμορφώσεις εξάπλωσης φάσματος, η DSSS και η FHSS και η τεχνική των υπέρυθρων ακτινών. Το άλλο επίπεδο είναι το υπόστρωμα MAC, το οποίο θα αναλυθεί στο επόμενο κεφάλαιο.

# 5. ΥΠΟΣΤΡΩΜΑ MAC ΤΟΥ ΠΡΟΤΥΠΟΥ IEEE 802.11

## 5.1 ΥΠΗΡΕΣΙΕΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

Το πρότυπο 802.11 προσφέρει εννέα βασικές υπηρεσίες, όπου οι τρείς από αυτές σχετίζονται με τη μεταφορά δεδομένων και οι υπόλοιπες με τη διαχείριση. Ονομαστικά, οι εννέα αυτές υπηρεσίες είναι: distribution, integration, MSDU (Mac Service Data Unit) Delivery, association, reassociation, disassociation, authentication, deauthentication και privacy.

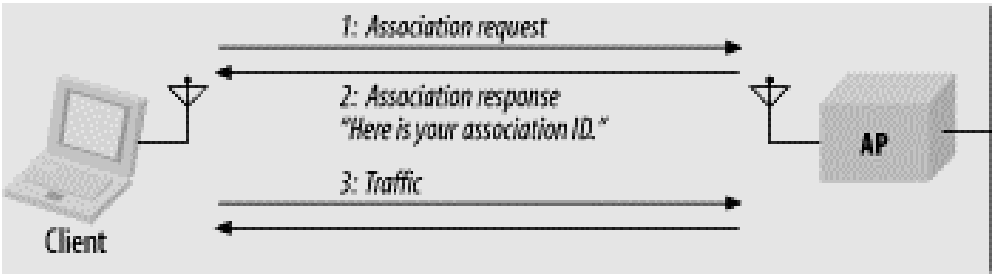
**Distribution:** Η υπηρεσία Distribution (Διανομή) είναι απαραίτητη για την παράδοση ενός πλαισίου από το AP στον τελικό προορισμό του. Βοηθάει στον εντοπισμό του παραλήπτη, ώστε να πραγματοποιηθεί η παράδοση του πλαισίου. Έτσι λαμβάνεται απόφαση αν ένα πλαίσιο πρέπει να σταλεί στο ίδιο BSS (Basic Service Set) ή πρέπει να σταλεί στο DS (Distribution System – Σύστημα Διανομής) προς παράδοση σε σταθμό συσχετιζόμενο με άλλο AP (Access Point). [2][6]

**Integration:** Η υπηρεσία Integration (Ενοποίηση) παρέχεται από το ίδιο το DS και επιτρέπει τη σύνδεσή του σε ένα δίκτυο διαφορετικό του 802.11. Ουσιαστικά μεταφράζει πλαίσια 802.11 σε πλαίσια άλλου τύπου και το αντίστροφο. Η υπηρεσία αυτή είναι συγκεκριμένη για κάθε DS και δεν καθορίζεται από το πρωτόκολλο 802.11. [2][6]

**MSDU Delivery:** Τα δίκτυα δεν είναι πολύ χρήσιμα χωρίς τη δυνατότητα που έχουν να αποστέλλουν δεδομένα. Έτσι, η υπηρεσία MSDU Delivery, είναι αρμόδια για την παράδοση των δεδομένων στον τελικό προορισμό τους. [2][6]

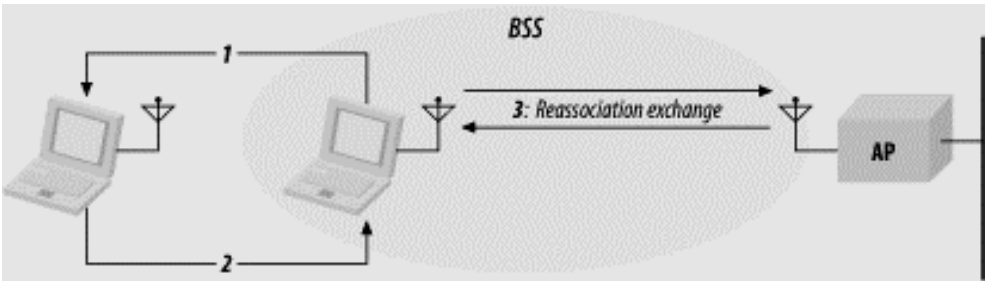
**Association:** Η διανομή στους κινητούς σταθμούς γίνεται εφικτή επειδή οι κινητοί σταθμοί καταχωρούνται ή συνδέονται με τα σημεία πρόσβασης. Το DS μπορεί αργότερα να χρησιμοποιήσει τις πληροφορίες εγγραφής για να καθορίσει ποιο σημείο πρόσβασης θα χρησιμοποιηθεί για κάθε κινητό σταθμό. Έτσι, η υπηρεσία Association (Σύνδεση) είναι απαραίτητη για τη διαδικασία συσχετισμού ενός τερματικού με το AP, προκειμένου να έχουν τη δυνατότητα να ανταλλάζουν πλαίσια μέσω του ασύρματου δικτύου. Για να επιτευχθεί αυτό, το τερματικό εκπέμπει ένα σήμα probe, με το οποίο ψάχνει τα σημεία πρόσβασης που υπάρχουν στην περιοχή. Τα σημεία πρόσβασης που το λαμβάνουν απαντούν με ένα σήμα probe response, και το τερματικό διαλέγει αυτό με το ισχυρότερο σήμα.

Στη συνέχεια, το τερματικό στέλνει ένα πλαίσιο Association request και παίρνει για απάντηση ένα πλαίσιο Association response. [2][6]



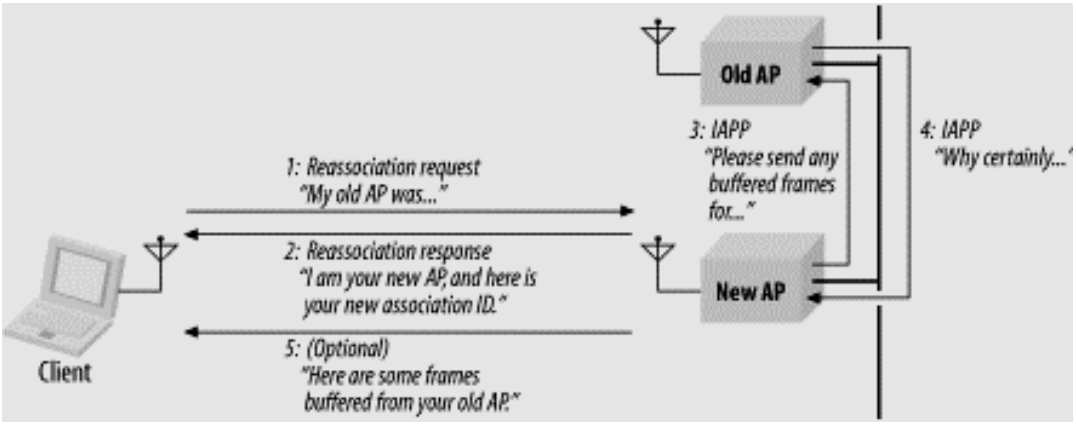

**ΕΙΚΟΝΑ 55: ΔΙΑΔΙΚΑΣΙΑ ASSOCIATION [6]**

**Reassociation:** Η υπηρεσία Reassociation (Επανασύνδεση) χρησιμοποιείται από τους κινητούς σταθμούς όταν θέλουν να μετακινηθούν από μία BSS σε μία άλλη. Έτσι, όταν ένα τερματικό κρίνει ότι η ζεύξη του με το σημείο πρόσβασης δεν είναι αρκετά δυνατή, ψάχνει με ένα σήμα probe να βρει άλλα σημεία πρόσβασης. Μόλις βρεθεί ένα σημείο πρόσβασης με δυνατότερο σήμα, στέλνει ένα πλαίσιο Association request και αν λάβει ένα πλαίσιο Association response συνδέεται με αυτό. Το νέο σημείο πρόσβασης δηλώνει αυτήν την επανασυσχέτιση στο DS, το οποίο στη συνέχεια ενημερώνει το παλιό σημείο πρόσβασης. [2][4][6]




**ΕΙΚΟΝΑ 56: ΔΙΑΔΙΚΑΣΙΑ REASSOCIATION [6]**

**Disassociation:** Για να τερματιστεί μια υπάρχουσα σύνδεση, τα τερματικά χρησιμοποιούν την υπηρεσία Disassociation (Αποσύνδεση). Όταν τα τερματικά χρησιμοποιούν αυτήν την υπηρεσία, όλα τα δεδομένα που αποθηκεύονται στο DS σβήνονται. Το MAC του 802.11 μπορεί να χειριστεί και τερματικά που αφήνουν το δίκτυο χωρίς όμως πρώτα να κάνουν αποσύνδεση. [2][6]




**ΕΙΚΟΝΑ 57: ΔΙΑΔΙΚΑΣΙΑ DISASSOCIATION [6]**

**Authentication:** Τα ασύρματα δίκτυα δεν μπορούν να προσφέρουν την ίδια ασφάλεια που προσφέρουν τα ενσύρματα δίκτυα, με αποτέλεσμα να χρειάζονται κάποιες επιπλέον υπηρεσίες για να διασφαλίσουν την ασφάλεια στους χρήστες. Με την υπηρεσία Authentication (Γνησιότητα), κάθε τερματικό πιστοποιεί την ταυτότητά του πριν να προχωρήσει στη διαδικασία του association, ώστε να διασφαλιστεί ότι όλα τα τερματικά που έχουν πρόσβαση στο δίκτυο είναι εξουσιοδοτημένα. Υπάρχουν δύο είδη ελέγχου και επιβεβαίωσης της ταυτότητας. Το πρώτο είναι ανοιχτού τύπου και το δεύτερο του κοινού κλειδιού. Στην πρώτη περίπτωση, οποιοδήποτε τερματικό μπορεί να ζητήσει επιβεβαίωση και το τερματικό που δέχεται την παράκληση επιβεβαίωσης μπορεί να δεχθεί την επικοινωνία είτε με οποιοδήποτε άλλο τερματικό είτε μόνο με τερματικά που έχουν οριστεί από το χρήστη. Στη δεύτερη περίπτωση, όπως μπορείτε να καταλάβετε από την ονομασία, γίνεται επιβεβαίωση μόνο των τερματικών που χρησιμοποιούν ένα μυστικό κλειδί. [2][6]

**Deauthentication:** Η υπηρεσία Deauthentication τερματίζει μια ισχύουσα κατάσταση authentication. Επίσης, τερματίζεται και η υπηρεσία association, μιας και το authentication είναι προαπαιτούμενο αυτού. [2][6]

**Privacy:** Το πρωτόκολλο 802.11 παρέχει μία προαιρετική υπηρεσία κρυπτογράφησης των δεδομένων που ονομάζεται WEP (Wired Equivalent Privacy). Σκοπός του είναι να παρέχει μυστικότητα κατά προσέγγιση ισοδύναμη με ένα ενσύρματο δίκτυο. Αυτό επιτυγχάνεται με την κρυπτογράφηση των πλαισίων, τη στιγμή που ταξιδεύουν διαμέσου του 802.11 interface. Συγκεκριμένα, σύμφωνα με την υπηρεσία κρυπτογράφησης WEP, αρχικά εφαρμόζεται στο πλαίσιο ο

Κυκλικός Κώδικας Ελέγχου Σφάλματος με τη μέθοδο προσθήκης πλεονασμού (32 – bit Cyclic Redundancy Code – CRC), η τιμή του οποίου αποθηκεύεται στο πλαίσιο. Στη συνέχεια κωδικοποιείται το πλαίσιο με την εφαρμογή της δυαδικής πράξης XOR ανάμεσα στο πλαίσιο και στο κλειδί και μετά μεταδίδεται. Τέλος, στο δέκτη, ο οποίος έχει από πριν συμφωνήσει για το κλειδί με τον πομπό, ακολουθείται η αντίστροφη διαδικασία. Παρ' όλα αυτά, το WEP δεν προσφέρει σε καμία περίπτωση ασφαλή μεταφορά δεδομένων. Παρέχει κάτι περισσότερο από την ελάχιστη ασφάλεια και απλά αποτρέπει άλλους χρήστες από το να εμφανιστούν εύκολα στο ασύρματο δίκτυο. Ήδη μελετάται η αντικατάσταση του με μία πιο αξιόπιστη υπηρεσία. [2][6]

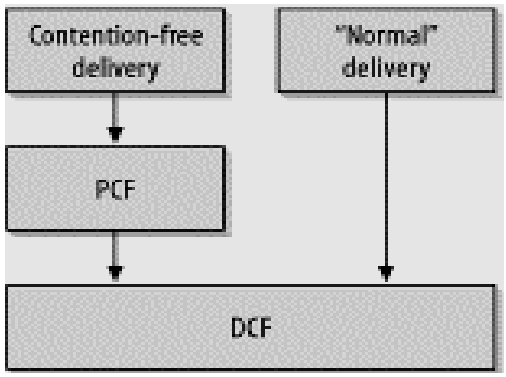
**ΠΙΝΑΚΑΣ 22: ΙΔΙΟΤΗΤΕΣ ΤΩΝ ΒΑΣΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ [2]**

| ΥΠΗΡΕΣΙΑ | ΠΑΡΟΧΕΑΣ | ΑΝΤΙΚΕΙΜΕΝΟ ΥΠΟΣΤΗΡΙΞΗΣ |
|---|---|---|
| Distribution | Σύστημα διανομής | Παράδοση MSDU |
| Integration | Σύστημα διανομής | Παράδοση MSDU |
| MSDU Delivery | Σταθμός | Παράδοση MSDU |
| Association | Σύστημα διανομής | Παράδοση MSDU |
| Reassociation | Σύστημα διανομής | Παράδοση MSDU |
| Disassociation | Σύστημα διανομής | Παράδοση MSDU |
| Authentication | Σταθμός | Πρόσβαση και προστασία LAN |
| Deauthentication | Σταθμός | Πρόσβαση και προστασία LAN |
| Privacy | Σταθμός | Πρόσβαση και προστασία LAN |

## 5.2 ΥΠΟΣΤΡΩΜΑ MAC ΤΟΥ ΠΡΟΤΥΠΟΥ IEEE 802.11

Το υπόστρωμα MAC του 802.11 υποστηρίζει όλα τα φυσικά στρώματα και προσφέρει αξιόπιστη μεταφορά δεδομένων, έχοντας ως κύρια υπηρεσία την παράδοση των πλαισίων MSDUs (MAC Service Data Units). Ουσιαστικά, το υπόστρωμα MAC αναφέρεται στον τρόπο πρόσβασης στο ασύρματο μέσο. Οι διαφορές του υποστρώματος με το αντίστοιχο των ενσύρματων δικτύων οφείλονται, όπως είναι φυσικό, στη φύση του ασύρματου μέσου μετάδοσης που χρησιμοποιείται στο φυσικό επίπεδο.

Μελετώντας το υπόστρωμα MAC, παρατηρείτε ότι υπάρχουν δύο καταστάσεις λειτουργίας, η κατάσταση ανταγωνισμού και η κατάσταση χωρίς ανταγωνισμό. Στην πρώτη περίπτωση, δηλαδή στην κατάσταση με ανταγωνισμό (Contention Period – CP), οι σταθμοί ανταγωνίζονται μεταξύ τους για την απόκτηση του μέσου. Αντίθετα, στη δεύτερη περίπτωση, στην κατάσταση χωρίς ανταγωνισμό (Contention–Free Period – CFP), η πρόσβαση στο μέσο ελέγχεται από το AP, το οποίο είναι αρμόδιο να ορίσει τη σειρά με την οποία θα μεταδώσουν οι σταθμοί τα δεδομένα. Στις δύο αυτές καταστάσεις στηρίζονται οι δυο μέθοδοι πρόσβασης στο μέσον. Οι μέθοδοι αυτοί είναι η Distributed Coordination Function (DCF) και η Point Coordination Function (PCF), οι οποίες θα αναλυθούν στη συνέχεια του κεφαλαίου.




**ΕΙΚΟΝΑ 58: MAC COORDINATION FUNCTIONS [6]**

## 5.2.1 MAC ΠΛΑΙΣΙΟ

Το πλαίσιο του υποστρώματος MAC του 802.11 διαφέρει από το πλαίσιο του Ethernet σε κάποια κλασσικά γνωρίσματα όπως το πεδίο preamble και το πεδίο τύπος/μήκος. Το Preamble και οι λεπτομέρειες ενθυλάκωσης, όπως ο τύπος και το μήκος, βρίσκονται στο header των δεδομένων που μεταφέρονται. Όπως γνωρίζετε, το υπόστρωμα MAC υποστηρίζει τρεις διαφορετικούς τύπους πλαισίων. Τα πλαίσια διαχείρισης, τα οποία χρησιμοποιούνται για λειτουργίες όπως η σύνδεση και η αποχώρηση ενός τερματικού από το δίκτυο. Τα πλαίσια δεδομένων, τα οποία χρησιμοποιούνται για τη μετάδοση των δεδομένων και τέλος τα πλαίσια ελέγχου τα οποία αποστέλλονται για την επιβεβαίωση της σωστής λήψης των δεδομένων. Στο σχήμα που ακολουθεί παρουσιάζεται η δομή ενός πλαισίου MAC καθώς επίσης ακολουθεί και η ανάλυση των επιμέρους τμημάτων του.

| Mac Header (30) | | | | | | | Data (0-2312) | CRC (4) |
|---|---|---|---|---|---|---|---|---|
| FC | ID | Add 1 | Add 2 | Add 3 | SC | Add 4 | Data | CRC |
| 2 | 2 | 6 | 6 | 6 | 2 | 6 | 0-2312 | 4 |

**ΕΙΚΟΝΑ 59: ΔΟΜΗ ΤΟΥ ΠΛΑΙΣΙΟΥ MAC**

Κάθε πλαίσιο MAC αποτελείται από τρία πεδία, την επικεφαλίδα (MAC HEADER), το σώμα του πλαισίου όπου περιέχονται τα δεδομένα και την ακολουθία ελέγχου πλαισίου (Frame Check Sequence – FCS), γνωστή και ως κυκλικός έλεγχος πλεονασμού (Cyclic Redundancy Check – CRC).

### 5.2.1.1 Επικεφαλίδα

Η επικεφαλίδα του πλαισίου MAC αποτελείται από εφτά τμήματα, όπως φαίνεται στην παραπάνω εικόνα. Το πρώτο τμήμα ονομάζεται Frame Control (FC) και χωρίζεται κι αυτό με τη σειρά του σε έντεκα υποτμήματα όπως φαίνεται στο σχήμα που ακολουθεί. Τα υποτμήματα αυτά, με τη σειρά που παρουσιάζονται στο σχήμα και μεταφρασμένα στα ελληνικά, είναι η Έκδοση του πρωτοκόλλου, ο Τύπος και ο Υποτύπος του πλαισίου, τα τμήματα προς και από το DS, το τμήμα Περισσότερα τεμάχια, το τμήμα επανεκπομπής, το τμήμα Διαχείρισης ισχύος, το τμήμα Περισσότερα δεδομένα, το τμήμα Κωδικοποίησης WEP, και το τμήμα Σειράς. [6][7]

| Protocol Version | Type | Sub Type | To DS | From DS | More Frag | Retry | Power Management | More Data | WEP | Order |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

**ΕΙΚΟΝΑ 60: ΔΟΜΗ ΤΗΣ ΕΠΙΚΕΦΑΛΙΔΑΣ ΤΟΥ ΠΛΑΙΣΙΟΥ MAC**

#### 5.2.1.1.1 Τμήμα Protocol

Στο τμήμα Protocol Version προσδιορίζεται η έκδοση του πρωτοκόλλου 802.11 MAC, όπως γίνετε αντιληπτό από την ονομασία του. Μέχρι τώρα όμως, έχει αναπτυχθεί μία μόνο έκδοση και ορίζεται με τον αριθμό πρωτοκόλλου 0. [3][6][7]

#### 5.2.1.1.1.1 Τμήμα Type και Subtype

Τα τμήματα Type και SubType προσδιορίζουν τον τύπο και τον υποτύπο του πλαισίου. Οι τύποι των πλαισίων είναι πλαίσια διαχείρισης, δεδομένων και ελέγχου. Μερικοί υποτύποι είναι RTS, CTS, ACK τα οποία είναι ελέγχου, Beacon, Association Request, Association Response, Reassociation Request, Reassociation Response, τα οποία είναι πλαίσια διαχείρισης. Στον επόμενο πίνακα παρουσιάζονται οι τύποι και οι υποτύποι των πλαισίων. [2]

**ΠΙΝΑΚΑΣ 23: ΤΙΜΕΣ ΤΟΥ ΤΜΗΜΑΤΟΣ TYPE ΚΑΙ SUBTYPE ΤΟΥ ΤΜΗΜΑΤΟΣ PROTOCOL [3]**

| ΠΙΝΑΚΑΣ: TYPE ΚΑΙ SUBTYPE | |
|---|---|
| **ΤΙΜΗ ΤΟΥ SUBTYPE** | **ΟΝΟΜΑ ΤΟΥ SUBTYPE** |
| **Πλαίσια Διαχείρισης (Type:00)** | |
| 0000 | Association Request |
| 0001 | Association Response |
| 0010 | Reassociation Request |
| 0011 | Reassociation Response |
| 0100 | Probe Request |
| 0101 | Probe Response |
| 1000 | Beacon |
| 1001 | Announcement traffic indication message (ATIM) |
| 1010 | Disassociation |
| 1011 | Authentication |
| 1100 | Deauthentication |
| **Πλαίσια Ελέγχου (Type:01)** | |
| 1010 | Power Save (PS) – Poll |
| 1011 | RTS |
| 1100 | CTS |
| 1101 | Acknowledgement (ACK) |
| 1110 | Contention – Free (CF) – End |
| 1111 | CF – End + CF – Ack |

| ΤΙΜΗ ΤΟΥ SUBTYPE | ΟΝΟΜΑ ΤΟΥ SUBTYPE |
|---|---|
| **Πλαίσια Δεδομένων (Type:10)** | |
| 0000 | Data |
| 0001 | Data + CF – Ack |
| 0010 | Data + CF – Poll |
| 0011 | Data + CF – Ack + CF – Poll |
| 0100 | Null Data (Δεν μεταδίδονται δεδομένα) |
| 0101 | CF – Ack (Δεν μεταδίδονται δεδομένα) |
| 0110 | CF – Poll (Δεν μεταδίδονται δεδομένα) |
| 0111 | Data + CF – Ack + CF – Poll |
| **(Ο τύπος πλαισίου 11 δεν διατίθεται)** | |

#### 5.2.1.1.1.2 Τμήμα to DS και from DS

Στα τμήματα to DS και from DS τα bits δείχνουν εάν ένα πλαίσιο προορίζεται για το DS. Στο τμήμα to DS, αν το bit είναι 1, το πλαίσιο στέλνεται προς το DS, ενώ στο τμήμα from DS, αν το bit είναι 1, το πλαίσιο λαμβάνεται από το DS. Επίσης, ανάλογα με τις τιμές των πεδίων to DS και from DS, οι διευθύνσεις έχουν και διαφορετική χρήση όπως φαίνεται στον επόμενο πίνακα. [3][6][7]

**ΠΙΝΑΚΑΣ 24: ΧΡΗΣΗ ΤΩΝ ΔΙΕΥΘΥΝΣΕΩΝ ΑΝΑΛΟΓΑ ΜΕ ΤΙΣ ΤΙΜΕΣ ΤΩΝ ΤΜΗΜΑΤΩΝ TO DS ΚΑΙ FROM DS [9]**

| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|
| 0 | 0 | DA | SA | APA | N/A |
| 0 | 1 | DA | APA | SA | N/A |
| 1 | 0 | APA | SA | DA | N/A |
| 1 | 1 | RA | TA | DA | SA |

DA: Destination Address

SA: Source Address

RA: Recipient Address

TA: Transmitter Address
APA: Access Point Address

#### 5.2.1.1.1.3 Τμήμα More Fragments

Το τμήμα More Fragments ασχολείται με τα πλαίσια τα οποία είναι αρκετά μεγάλα και τεμαχίζονται. Ειδικότερα, αν το bit είναι ίσο με 1, τότε αυτό δηλώνει ότι έχουν μείνει τμήματα του πλαισίου τα οποία ακόμα δεν έχουν σταλεί. [2][3][6][7]

#### 5.2.1.1.1.4 Τμήμα Retry

Το τμήμα Retry είναι υπεύθυνο για τα πλαίσια τα οποία μπορούν να αναμεταδοθούν, έτσι το αναμεταδιδόμενο πλαίσιο θέτει το bit ίσο με 1, με αποτέλεσμα ο δέκτης να αναγνωρίζει τα διπλότυπα. [2][3][6][7]

#### 5.2.1.1.1.5 Τμήμα Power Management

Το bit του τμήματος Power Management υποδεικνύει σε τι κατάσταση θα τεθεί ο πομπός μετά την ολοκλήρωση της ανταλλαγής πλαισίων. Το 1 δείχνει ότι ο σταθμός βρίσκεται σε κατάσταση εξοικονόμησης ενέργειας (power – saving mode) και το 0 ότι ο σταθμός είναι ενεργός. Επειδή τα σημεία πρόσβασης εκτελούν διάφορες σημαντικές λειτουργίες διαχείρισης και δεν επιτρέπεται να βρίσκονται σε κατάσταση εξοικονόμησης ενέργειας, το bit αυτό είναι πάντα 0 για τα πλαίσια που διαβιβάζονται από ένα σημείο πρόσβασης. [3][6][7]

#### 5.2.1.1.1.6 Τμήμα More Data

Το bit του τμήματος More Data όταν είναι 1 δείχνει ότι υπάρχει τουλάχιστον ένα πλαίσιο προς εκπομπή. [3][6][7]

#### 5.2.1.1.1.7 Τμήμα WEP

Το bit του τμήματος WEP όταν είναι 1 δηλώνει ότι ένα πλαίσιο είναι κωδικοποιημένο με τον αλγόριθμο WEP (Wired Equivalent Privacy) με σκοπό την προστασία και την απόδειξη γνησιότητας των δεδομένων. [2][3][6]

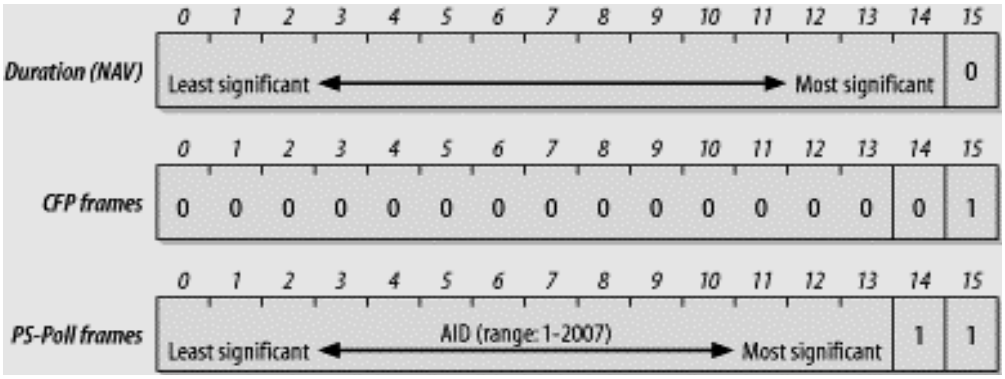
#### 5.2.1.1.1.8 Τμήμα Order

Τέλος, το bit Order όταν ισούται με 1 εφαρμόζεται η διανομή «απόλυτης σειράς». Δηλαδή, τα πλαίσια και τα τμήματα των πλαισίων μπορούν να διαβιβαστούν με τη

σειρά και κατά την αποστολή αλλά και κατά τη λήψη, παρά το κόστος της πρόσθετης επεξεργασίας. [2][6]

#### 5.2.1.1.2 Τμήμα ID/Duration

Συνεχίζοντας την ανάλυση του πλαισίου MAC, το δεύτερο τμήμα του είναι το ID/Duration, στο οποίο αποθηκεύεται πόσο χρόνο ένα πλαίσιο θα απασχολεί το κανάλι μετάδοσης. Σε πλαίσια τύπου Power Save Poll το τμήμα αυτό περιέχει τη διάρκεια, ενώ σε όλα τα υπόλοιπα το NAV(Network Allocation Vector). Η τιμή που έχει το πεδίο αυτό, όταν αναφέρεστε σε πλαίσια που περιέχουν το NAV, αντιστοιχεί στο χρόνο κατά τον οποίο το μέσο θα παραμείνει απασχολημένο για τη μετάδοση ενός πλαισίου που συμβαίνει εκείνη τη στιγμή. Όλοι οι σταθμοί πριν μεταδώσουν ένα πλαίσιο πρέπει να ελέγξουν τις επικεφαλίδες όλων των πλαισίων που λαμβάνουν και να ενημερώνουν ανάλογα το NAV. Έτσι, οποιαδήποτε τιμή παρατείνει το χρονικό διάστημα κατά το οποίο το μέσο είναι απασχολημένο, ενημερώνει το NAV και εμποδίζει για επιπλέον χρονικό διάστημα την πρόσβαση στο μέσο. [3][6][7]




**ΕΙΚΟΝΑ 61: ΤΜΗΜΑ ID/DURATION [6]**

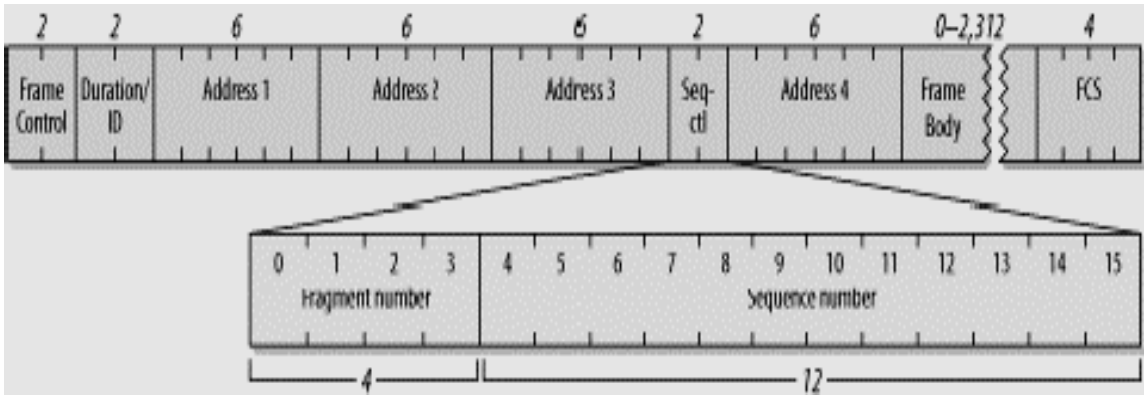
#### 5.2.1.1.3 Τμήμα Address 1, Address 2, Address 3

Ένα πλαίσιο του προτύπου 802.11 περιέχει μέχρι τέσσερα πεδία διευθύνσεων, τα οποία, όπως και στα πλαίσια MAC, είναι αριθμημένα επειδή χρησιμοποιούνται για διαφορετικούς σκοπούς ανάλογα με την τιμή που έχει το πεδίο FC. Οι διευθύνσεις έχουν μήκος 48 bits. Αν το πρώτο bit που στέλνεται στο μέσο είναι 0, τότε η διεύθυνση αντιπροσωπεύει έναν σταθμό (unicast), αν είναι 1 έχουμε μία ομάδα παραληπτών (multicast), ενώ αν όλα τα bits είναι 1, τότε το πλαίσιο διανέμεται σε όλους τους σταθμούς που συνδέονται με το ασύρματο μέσο.

Συνήθως, η διεύθυνση 1 χρησιμοποιείται για τον αποστολέα, η διεύθυνση 2 για τον παραλήπτη, η διεύθυνση 3 για τον πομπό και η διεύθυνση 4 για το δέκτη. Η διεύθυνση προορισμού (Destination address) αντιστοιχεί στον τελικό παραλήπτη. Η διεύθυνση προέλευσης (Source address) προσδιορίζει την πηγή της μετάδοσης, επειδή όμως μόνο ένας σταθμός μπορεί να είναι η πηγή, ο αποστολέας, το χαρακτηριστικό bit είναι πάντα 0 για να ξεχωρίζει. Η διεύθυνση αποδέκτη (Receiver address) καθορίζει ποιος ασύρματος σταθμός θα επεξεργαστεί το πλαίσιο. Με τη διεύθυνση πομπού (Transmitter address) καθορίζεται η ασύρματη διεπαφή που διαβιβάζει το πλαίσιο πάνω στο ασύρματο μέσο. Η διεύθυνση πομπού χρησιμοποιείται μόνο στην ασύρματη γεφύρωση. Τέλος το BSSID (Basic Service Set ID) είναι η διεύθυνση MAC που χρησιμοποιεί η ασύρματη διεπαφή στο σημείο πρόσβασης. [6]

#### 5.2.1.1.4 Τμήμα Sequence Control Field

Το επόμενο τμήμα είναι το Sequence Control Field το οποίο φαίνεται στο σχήμα που ακολουθεί.




**ΕΙΚΟΝΑ 62: ΜΟΡΦΗ ΤΟΥ ΤΜΗΜΑΤΟΣ SEQUENCE CONTROL FIELD [6]**

Το τμήμα αυτό χρησιμοποιείται για την επανασύνδεση των πλαισίων αλλά και για την απόρριψη των διπλότυπων. Όπως παρατηρείτε στην εικόνα, αποτελείται από ένα τμήμα 4 bit, το fragment number και από ένα 12 bit τμήμα, το sequence number. Σε καθένα από τα υψηλότερου επιπέδου πλαίσια δίνεται ένας αριθμός ακολουθίας, καθώς περνούν από το υπόστρωμα MAC για μετάδοση. Ο αριθμός αυτός λειτουργεί ως μετρητής των πλαισίων που μεταδίδονται και αρχίζει από το 0 και για κάθε πακέτο που περνάει από το υπόστρωμα MAC, αυξάνει κατά ένα. Αν ένα πλαίσιο είναι τεμαχισμένο, όλα τα τεμάχια θα έχουν τον ίδιο αριθμό

ακολουθίας καθώς και όταν τα πλαίσια αναμεταδίδονται, ο αριθμός ακολουθίας παραμένει ο ίδιος. Όμως, σε κάθε τεμάχιο ενός πλαισίου υπάρχει και ο αριθμός του τεμαχίου για να ξεχωρίζουν μεταξύ τους. Το πρώτο τεμάχιο έχει τον αριθμό 0 και για κάθε επιτυχημένο τεμάχιο αυξάνεται ο αριθμός κατά 1. Ο αριθμός τεμαχίου βοηθάει στην επανασύνδεση του πλαισίου. [3][6][7]

#### 5.2.1.2 Data

Συνεχίζοντας την ανάλυση του MAC πλαισίου, περνάμε στο πεδίο Data, στο σώμα δηλαδή του πλαισίου. Στο πεδίο αυτό περιέχονται τα δεδομένα τα οποία είναι προς μετάδοση, με μέγιστο αριθμό δεδομένων τα 2312 bytes. [5][6][7]

#### 5.2.1.3 FCS

Το τρίτο και τελευταίο πεδίο του πλαισίου MAC, είναι το FCS ή CRC και χρησιμοποιείται για την επαλήθευση της σωστής λήψης του κάθε πλαισίου. Το CRC (Cyclic Redundancy Check) είναι ένας κώδικας ανίχνευσης λαθών, έχει μήκος 32 – bit και αναφέρεται στα προηγούμενα τμήματα του πλαισίου, δηλαδή στο MAC Header και στο Data. Ο παραλήπτης συγκρίνει την τιμή που βρίσκει με τον κώδικα CRC με αυτήν που βρίσκεται αποθηκευμένη στο τμήμα FCS του πλαισίου που έλαβε. Με αυτόν τον τρόπο ο παραλήπτης καταλαβαίνει αν το πλαίσιο που έλαβε έχει σταλεί σωστά, όταν οι αριθμοί ταυτίζονται, ή έχει σταλεί λανθασμένα, όταν οι αριθμοί είναι διαφορετικοί. [3][5][6]

### 5.3 ΠΛΑΙΣΙΑ

Στην ενότητα αυτή παρουσιάζονται κάποιοι τύποι πλαισίων τα οποία θα συναντήσετε στη συνέχεια του κεφαλαίου. Τα πλαίσια τα οποία θα αναλυθούν είναι τα RTS, CTS, ACK, CF – Poll, CF – End, CF - ACK και Beacon.

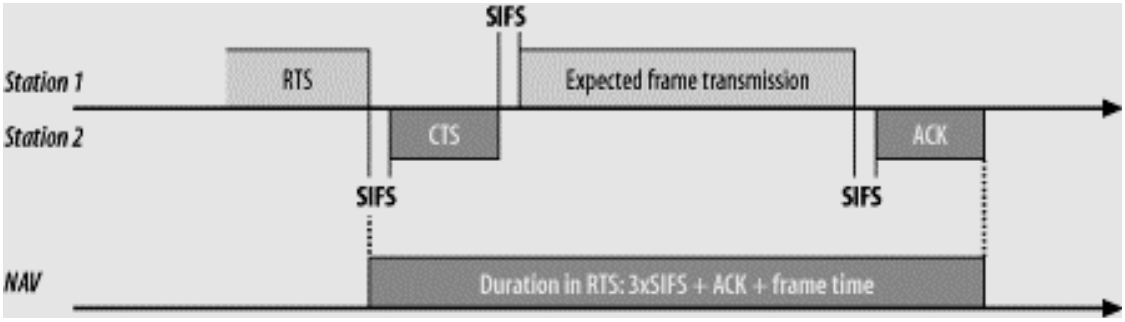
#### 5.3.1 RTS

| Frame control | Duration | RA | TA | FCS |
|---|---|---|---|---|
| (2 bytes) | (2 bytes) | (6 bytes) | (6 bytes) | (4 bytes) |

←———— MAC Header ————→

**ΕΙΚΟΝΑ 63: ΜΟΡΦΗ ΤΟΥ ΠΛΑΙΣΙΟΥ RTS [3]**

Με το πλαίσιο RTS (Request To Sent) ο αποστολέας ζητάει από τον παραλήπτη άδεια για να στείλει μήνυμα και δεσμεύει το μέσον. Οι σταθμοί που ακούνε το μέσον, ενημερώνουν το NAV (Network Allocation Vector) τους, το οποίο υπολογίζει τη διάρκεια που χρειάζεται το πλαίσιο που ανιχνεύθηκε για να μεταδοθεί. Όπως φαίνεται στο παραπάνω σχήμα στο RA (Receiving station Address) περιέχει τα στοιχεία του παραλήπτη, ενώ το TA (Transmitting station Address) περιέχει τη διεύθυνση του αποστολέα. Το τμήμα Duration περιέχει τη χρονική διάρκεια σε μsec κατά την οποία θα καταληφθεί το μέσο, έως την αποστολή του πλαισίου ACK (Acknowledgement) συν την χρονική διάρκεια τριών SIFS, το οποίο αναλύεται στη συνέχεια. [6]




**ΕΙΚΟΝΑ 64: ΔΙΑΡΚΕΙΑ ΤΟΥ ΤΜΗΜΑΤΟΣ RTS [6]**

## 5.3.2 CTS

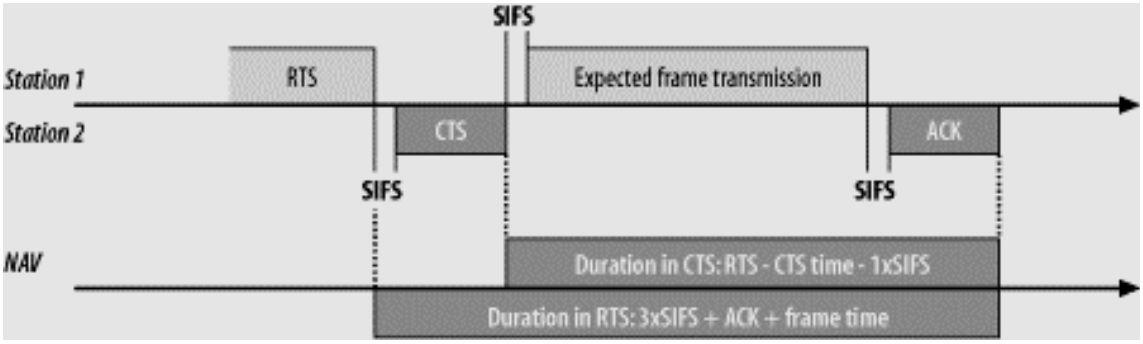
| Frame control | Duration | RA | FCS |
|---|---|---|---|
| (2 bytes) | (2 bytes) | (6 bytes) | (4 bytes) |

MAC Header

**ΕΙΚΟΝΑ 65: ΜΟΡΦΗ ΤΟΥ ΠΛΑΙΣΙΟΥ CTS [3]**

Με το πλαίσιο CTS (Clear To Send) ο παραλήπτης του πλαισίου RTS διαβεβαιώνει στον αποστολέα του πλαισίου ότι το μέσον είναι ελεύθερο για να στείλει τα δεδομένα. Με το πλαίσιο αυτό, ενημερώνουν το NAV τους και όσοι σταθμοί δεν το είχαν κάνει προηγουμένως με το πλαίσιο RTS. Το τμήμα RA περιέχει τη διεύθυνση του παραλήπτη και το τμήμα Duration περιέχει τη χρονική διάρκεια. Παρατηρώντας τη χρονική διάρκεια του πλαισίου αυτού, διαπιστώνετε ότι η χρονική διάρκεια του τμήματος είναι ίδια με τη χρονική διάρκεια του πλαισίου

RTS του τμήματος Duration, αν αφαιρέσετε τη χρονική διάρκεια για την αποστολή ενός πλαισίου CTS και ενός SIFS.




**ΕΙΚΟΝΑ 66: ΔΙΑΡΚΕΙΑ ΤΟΥ ΤΜΗΜΑΤΟΣ CTS [6]**

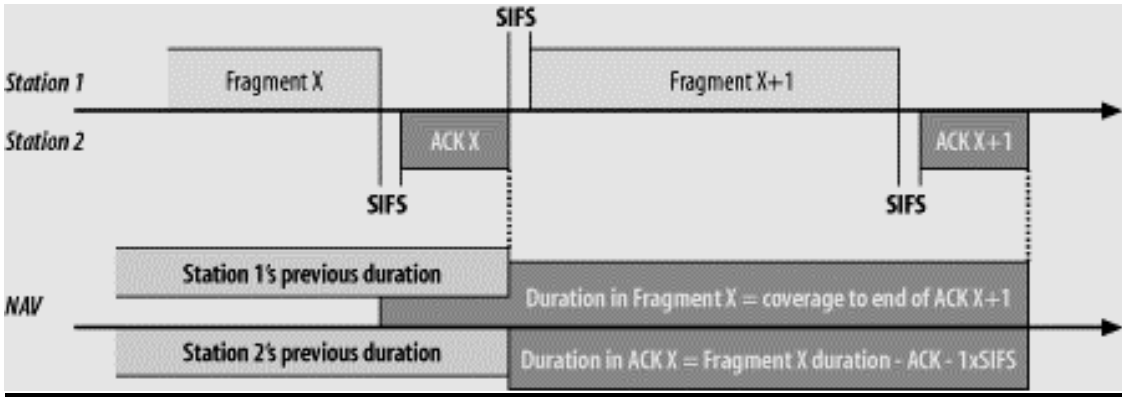
## 5.3.3 ACK

| Frame control | Duration | RA | FCS |
|---|---|---|---|
| (2 bytes) | (2 bytes) | (6 bytes) | (4 bytes) |

MAC Header

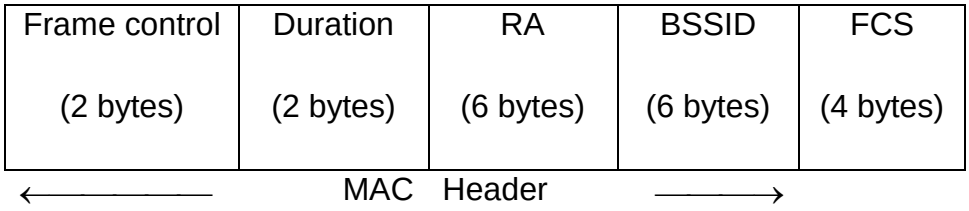
**ΕΙΚΟΝΑ 67: ΜΟΡΦΗ ΤΟΥ ΠΛΑΙΣΙΟΥ ACK [3]**

Το πλαίσιο ACK (Acknowledgement) δηλώνει πως η μετάδοση των δεδομένων έχει ολοκληρωθεί με επιτυχία. Το τμήμα RA περιέχει τη διεύθυνση του σταθμού, ο οποίος θα λάβει το ACK. [2][6]




**ΕΙΚΟΝΑ 68: ΔΙΑΡΚΕΙΑ ΤΟΥ ΤΜΗΜΑΤΟΣ CTS [6]**

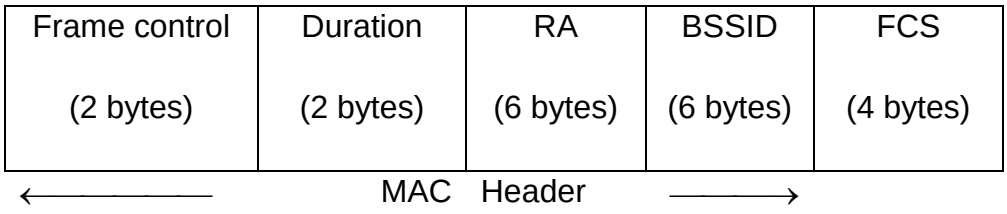
### 5.3.4 CF – Poll




**ΕΙΚΟΝΑ 69: ΜΟΡΦΗ ΤΟΥ ΠΛΑΙΣΙΟΥ CF - POLL**

Αυτό το πλαίσιο χρησιμοποιείται στο PCF (Point Coordination Function) τρόπο πρόσβασης στο μέσον. Με το πλαίσιο αυτό το PC, το οποίο θα αναλυθεί στην ενότητα PCF, δίνει άδεια σε έναν από τους σταθμούς υψηλής προτεραιότητας να εκπέμψει. Το τμήμα RA διαθέτει τη διεύθυνση του τερματικού που παίρνει άδεια να εκπέμψει, το πλαίσιο Duration περιέχει την τιμή 0 και το τμήμα BSSID (Basic Service Set ID) περιέχει τη διεύθυνση του σταθμού PC.

### 5.3.5 CF – End και CF – ACK




**ΕΙΚΟΝΑ 70: ΜΟΡΦΗ ΤΟΥ ΠΛΑΙΣΙΟΥ CF - END ΚΑΙ CF - ACK**

Η μορφή των δυο αυτών πλαισίων είναι η ίδια εκτός από το τμήμα του υποτύπου του τμήματος Frame Control. Επίσης, όπως και το πλαίσιο CF – Poll, χρησιμοποιούνται στο PCF. Το πλαίσιο CF – End τερματίζει την περίοδο χωρίς ανταγωνισμό και αποδεσμεύει τους σταθμούς από τους περιορισμούς που αφορούν αυτήν την περίοδο, ενώ το πλαίσιο CF – ACK βεβαιώνει τη λήψη του CF – End. Το τμήμα Duration περιέχει την τιμή 0, το τμήμα RA περιέχει μία διεύθυνση η οποία δηλώνει μετάδοση προς όλους τους σταθμούς ταυτόχρονα και το τμήμα BSSID περιέχει τη διεύθυνση του PC. [2]

### 5.3.6 Data + CF – Ack

Το πλαίσιο αυτό ανήκει στα πλαίσια δεδομένων και μπορεί να σταλεί μόνο κατά την περίοδο χωρίς ανταγωνισμό. Μεταφέρει δεδομένα και επιπλέον βεβαιώνει τη λήψη δεδομένων που έχουν ληφθεί προηγουμένως. [2]

## 5.3.7 Data + CF – Poll

Το πλαίσιο αυτό χρησιμοποιείται από το PCF για την παράδοση δεδομένων σε ένα κινητό σταθμό και για να γνωστοποιεί ότι ο κινητός σταθμός έστειλε ένα πλαίσιο δεδομένων το οποίο μπορεί να έχει αποθηκευτεί προσωρινά. [2]

**ΠΙΝΑΚΑΣ 25: ΙΔΙΟΤΗΤΕΣ ΤΩΝ ΠΛΑΙΣΙΩΝ [6]**

| Frame type | Contention-based service | Contention-free service | Carries data | Does not carry data |
|---|---|---|---|---|
| Data | ✓ | | ✓ | |
| Data+CF-Ack | | ✓ | ✓ | |
| Data+CF-Poll | | AP only | ✓ | |
| Data+CF-Ack+CF-Poll | | AP only | ✓ | |
| Null | ✓ | ✓ | | ✓ |
| CF-Ack | | ✓ | | ✓ |
| CF-Poll | | AP only | | ✓ |
| CF-Ack+CF-Poll | | AP only | | ✓ |

## 5.3.8 Beacon

| Frame control (2 bytes) | Duration (2 bytes) | DA (6 bytes) | SA (6 bytes) | BSSID (6 bytes) | Sequence Control (2 bytes) | Frame Body (0-2312) | FCS (4 bytes) |
|---|---|---|---|---|---|---|---|
| ← | | MAC | Header | | → | | |

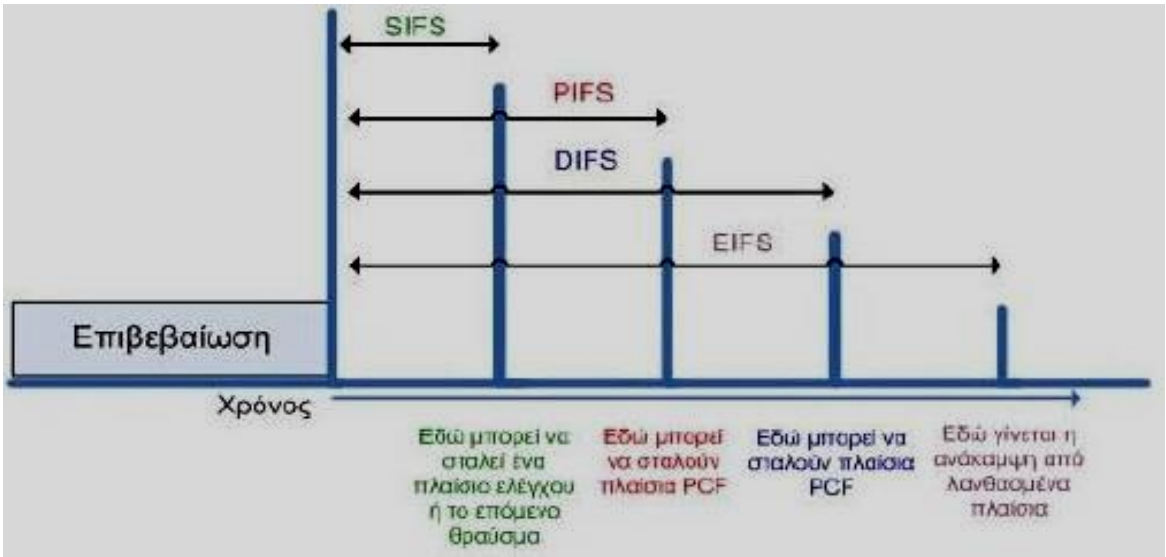
**ΕΙΚΟΝΑ 71: ΜΟΡΦΗ ΤΟΥ ΠΛΑΙΣΙΟΥ BEACON**

Το πλαίσιο Beacon ανήκει στα πλαίσια διαχείρισης του δικτύου, σε αντίθεση με τα υπόλοιπα πλαίσια, τα οποία ήταν πλαίσια ελέγχου. Το πλαίσιο αυτό περιέχει τη μέγιστη διάρκεια της CFP (Contention – Free – Period), το οποίο θα αναλυθεί στη συνέχεια του κεφαλαίου. Όπως και τα προηγούμενα, και αυτό χρησιμοποιείται στην αρχή κάθε περιόδου της PCF. Το τμήμα Duration περιέχει τη χρονική διάρκεια κατάληψης του μέσου για τη PCF. Το τμήμα Frame Body αποτελείται από δέκα υποτμήματα ενός byte το καθένα, τα οποία μπορείτε να δείτε στον πίνακα που ακολουθεί.

**ΠΙΝΑΚΑΣ 26: ΤΑ ΔΕΚΑ ΥΠΟΤΜΗΜΑΤΑ ΤΟΥ ΤΜΗΜΑΤΟΣ FRAME BODY**

| Order | Information | Notes |
|---|---|---|
| 1 | Timestamp | |
| 2 | Beacon interval | |
| 3 | Capability information | |
| 4 | SSID | |
| 5 | Supported rates | |
| 6 | FH Parameter Set | The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs. |
| 7 | DS Parameter Set | The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs. |
| 8 | CF Parameter Set | The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF. |
| 9 | IBSS Parameter Set | The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS. |
| 10 | TIM | The TIM information element is only present within Beacon frames generated by APs. |

## 5.4 ΧΡΟΝΟΙ ΑΝΑΜΟΝΗΣ (INTERFRAME SPACING - IFS)




**ΕΙΚΟΝΑ 72: ΧΡΟΝΟΙ ΑΝΑΜΟΝΗΣ**

Κάθε σταθμός που θέλει να στείλει ένα πλαίσιο πρέπει πρώτα να περιμένει κάποιο χρονικό διάστημα και αν δεν ανιχνεύσει καμία άλλη μετάδοση, τότε προχωράει στο επόμενο στάδιο για την αποστολή του πλαισίου. Το χρονικό αυτό διάστημα διαφέρει ανάλογα με τον τύπο του πλαισίου. Στο παραπάνω σχήμα φαίνονται οι χρόνοι αναμονής καθώς επίσης και οι σχέσεις μεταξύ τους.

### 5.4.1 SIFS (Short Interframe Space)

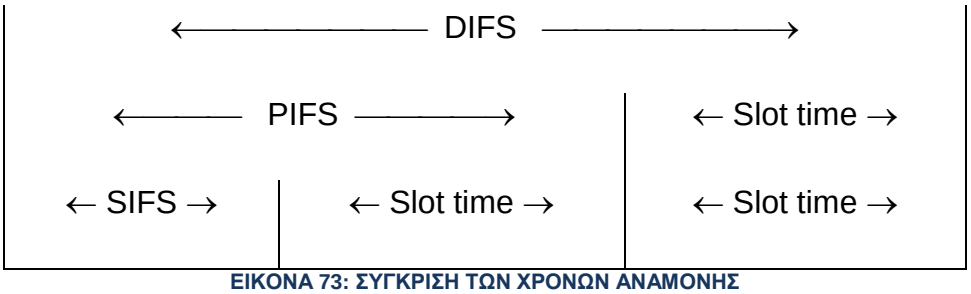
Το SIFS είναι ο μικρότερος χρόνος αναμονής. Χρησιμοποιείται για μεταδόσεις μέγιστης προτεραιότητας, όπως είναι τα πλαίσια RTS / CTS και ACK, τα οποία τα έχουμε ήδη αναλύσει. [2][3][6][7]

### 5.4.2 PIFS (PCF Interframe Space)

Το PIFS είναι μεγαλύτερος χρόνος από το SIFS. Χρησιμοποιείται στο PCF τρόπο πρόσβασης στο μέσο. Ένας σταθμός περιμένει PIF χρόνο πριν μεταδώσει ένα πλαίσιο σε ένα δίκτυο χωρίς ανταγωνισμό. [2][3][6][7]

### 5.4.3 DIFS (DCF Interframe Space)

Το DIFS είναι μεγαλύτερο σε διάρκεια, σε σύγκριση με τους δύο προηγούμενους χρόνους αναμονής, όπως παρατηρείτε στο παρακάτω σχήμα, αλλά είναι ο μικρότερος χρόνος αναμονής για τη λειτουργία DCF. [6][7]




**ΕΙΚΟΝΑ 73: ΣΥΓΚΡΙΣΗ ΤΩΝ ΧΡΟΝΩΝ ΑΝΑΜΟΝΗΣ**

### 5.4.4 EIFS (Extended Interframe Space)

Το EIFS είναι ο μεγαλύτερος χρόνος αναμονής. Δεν έχει κάποια συγκεκριμένη τιμή. Χρησιμοποιείται στη λειτουργία DCF όταν εντοπιστεί κάποιο σφάλμα στη μετάδοση ενός πακέτου. Όταν πραγματοποιείται μία σωστή λήψη κατά τη διάρκεια του EIFS, μετά, χρησιμοποιείται και πάλι χρόνος DIFS. [3][6]

### 5.4.5 SLOT TIME

Ο χρόνος χωρίζεται σε σταθερές ποσότητες χρόνου τα οποία ονομάζονται slot. Το μέγεθος ενός slot καθορίζεται από το φυσικό στρώμα. [6]

### 5.4.6 BACK OFF TIME

Στη λειτουργία DCF όταν χρησιμοποιείτε το μηχανισμό CSMA / CA, ο σταθμός αντιλαμβάνεται εάν το κανάλι είναι κατειλημμένο ή ελεύθερο. Εφόσον το κανάλι είναι κατειλημμένο, ο σταθμός περιμένει μέχρι να ελευθερωθεί το κανάλι για DIFS χρόνο και στη συνέχεια επιλέγει ένα τυχαίο back off time στο διάστημα [0,CW (contention window)]. Η διαδικασία back off time βοηθάει για μία πιο δίκαιη αντιμετώπιση των σταθμών. Όταν ένας σταθμός δεν προλάβει να καταλάβει το μέσο, κρατά την τιμή του χρόνου αναβολής στην οποία σταμάτησε για την επόμενη φορά που θα προσπαθήσει να καταλάβει το μέσο. Έτσι, ο σταθμός θα πρέπει να περιμένει μικρότερο χρονικό διάστημα σε σχέση με έναν σταθμό που προσπαθεί για πρώτη φορά να καταλάβει το μέσο.

Στον επόμενο πίνακα φαίνονται οι τιμές των χρόνων αναμονής σε κάθε σύστημα μετάδοσης.

**ΠΙΝΑΚΑΣ 27: ΤΙΜΕΣ ΤΩΝ ΧΡΟΝΩΝ ΑΝΑΜΟΝΗΣ ΓΙΑ ΚΑΘΕ ΤΕΧΝΙΚΗ**

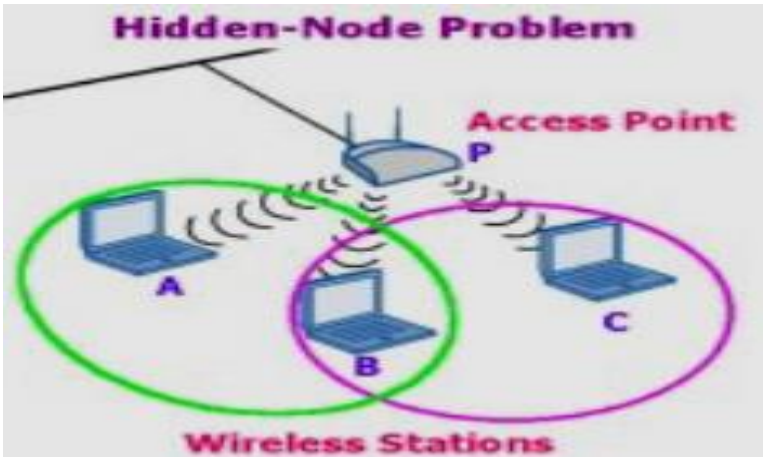
| | FHSS | DSSS | IR |
|---|---|---|---|
| **Slot Time** | 50 μsec | 20 μsec | 8 μsec |
| **SIFS** | 28 μsec | 10 μsec | 10 μsec |
| **PIFS** | 78 μsec | 30 μsec | 18 μsec |
| **DIFS** | 128 μsec | 50 μsec | 26 μsec |
| **EIFS** | 1024 μsec | 1088 μsec | 953 μsec |

## 5.5 ΠΑΡΑΘΥΡΟ ΑΝΤΑΓΩΝΙΣΜΟΥ (CONTENTION WINDOW - CW)

Στις προηγούμενες παραγράφους έχει ήδη γίνει αναφορά για το CW και επίσης θα το συναντήσετε και στις επόμενες. Το CW χωρίζεται σε slots, ίσα μεταξύ τους και η διάρκειά τους εξαρτάται από το φυσικό στρώμα. Κάθε σταθμός επιλέγει τυχαία ένα slot και περιμένει τη σειρά του για να αποκτήσει πρόσβαση στο μέσο. Η επιλογή αυτού του τυχαίου slot, γίνετε με τη χρήση μιας διαδικασίας η οποία ονομάζεται δυαδική εκθετική υποχώρηση. Νικητής στη διεκδίκηση του δικτύου, θα αναδειχθεί αυτός που θα επιλέξει το πρώτο slot, δηλαδή αυτό που είναι μπροστά από όλα τα υπόλοιπα slots τα οποία επιλέχθηκαν από τους σταθμούς του δικτύου. Μόλις έρθει η σειρά του slot, ο σταθμός μεταδίδει το πλαίσιο που επιθυμεί. Αν η μετάδοση είναι αποτυχημένη, εξαιτίας της μη λήψης του πλαισίου ACK, θεωρείται ότι έχει συμβεί κάποια σύγκρουση (collision). Τότε ο σταθμός επιλέγει πάλι ένα slot τυχαία και μεταδίδει ξανά το πλαίσιο. Το εύρος τιμών από το οποίο καλείται να επιλέξει τυχαία κάθε σταθμός είναι πάντα αριθμός κατά ένα μικρότερος από κάποια δύναμη του 2. Κάθε φορά που αποτυγχάνει το εύρος τιμών υπολογίζεται ξανά με βάση την αμέσως επόμενη δύναμη του 2. Αυτή η διαδικασία επαναλαμβάνεται μέχρι να υπάρξει επιτυχής μετάδοση ή στην περίπτωση που έχει φτάσει το εύρος στη μέγιστη τιμή, όπου τότε η διαδικασία επαναλαμβάνεται με εύρος τιμών τη μέγιστη τιμή. Το εύρος τιμών επανέρχεται στην ελάχιστη τιμή μετά από μία επιτυχημένη μετάδοση ή από απόρριψη του πλαισίου. [5][6]

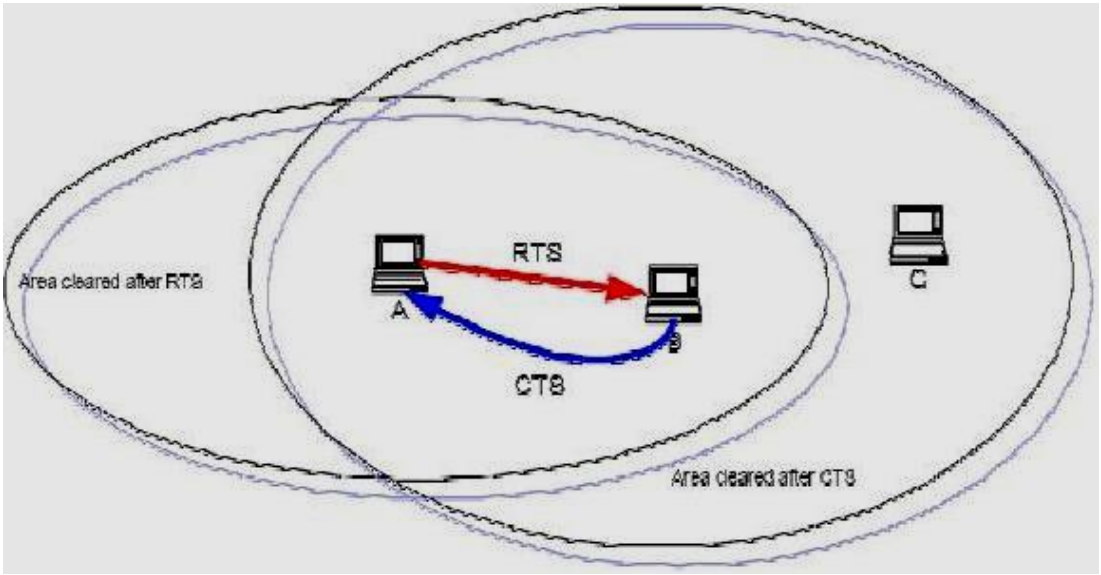
## 5.6 ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ «ΚΡΥΜΕΝΟΥ ΚΟΜΒΟΥ» (HIDDEN NODE)

Το πρόβλημα του κρυμμένου κόμβου είναι χαρακτηριστικό των ασύρματων δικτύων. Σε ένα ασύρματο δίκτυο η ακτίνα εκπομπής και λήψης κάθε σταθμού είναι συγκεκριμένη και πεπερασμένη, με αποτέλεσμα κάθε σταθμός να έχει μία διαφορετική εικόνα ως προς το μέσο μετάδοσης και φυσικά των σταθμών που ανήκουν στο δίκτυο. Ειδικότερα, το πρόβλημα του κρυμμένου κόμβου γίνεται αντιληπτό στο μηχανισμό CSMA/CA, όπου ένας σταθμός «ακούει» το μέσον για να δει αν κάποιος άλλος σταθμός μεταδίδει. Το πρόβλημα αυτό δημιουργείται επειδή ένας σταθμός δεν είναι πάντα σε θέση να ανιχνεύσει κάποιον άλλον σταθμό ο οποίος είτε μεταδίδει είτε ετοιμάζεται να μεταδώσει δεδομένα εξαιτίας της μεγάλης απόστασής τους. Για παράδειγμα, αν δύο σταθμοί (A, C) είναι εκτός εμβέλειας και αν υπάρχει ένας σταθμός ο οποίος βρίσκεται στο ενδιάμεσό τους (B) και μπορεί να μεταδώσει δεδομένα και στους δύο, τότε πιθανόν να διακοπεί η μετάδοση από τον A στο B λόγω της ταυτόχρονης αποστολής δεδομένων από τον C στο B. Τα παραπάνω φαίνονται στην εικόνα που ακολουθεί.




**ΕΙΚΟΝΑ 74: ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ "ΚΡΥΜΕΝΟΥ ΚΟΜΒΟΥ" [9]**

Ουσιαστικά, λύση στο πρόβλημα του κρυμμένου κόμβου, δίνει η ανταλλαγή μικρών πλαισίων ελέγχου, RTS και CTS τα οποία έχουν ήδη αναλυθεί, ανάμεσα στον αποστολέα και τον παραλήπτη ή τους παραλήπτες.

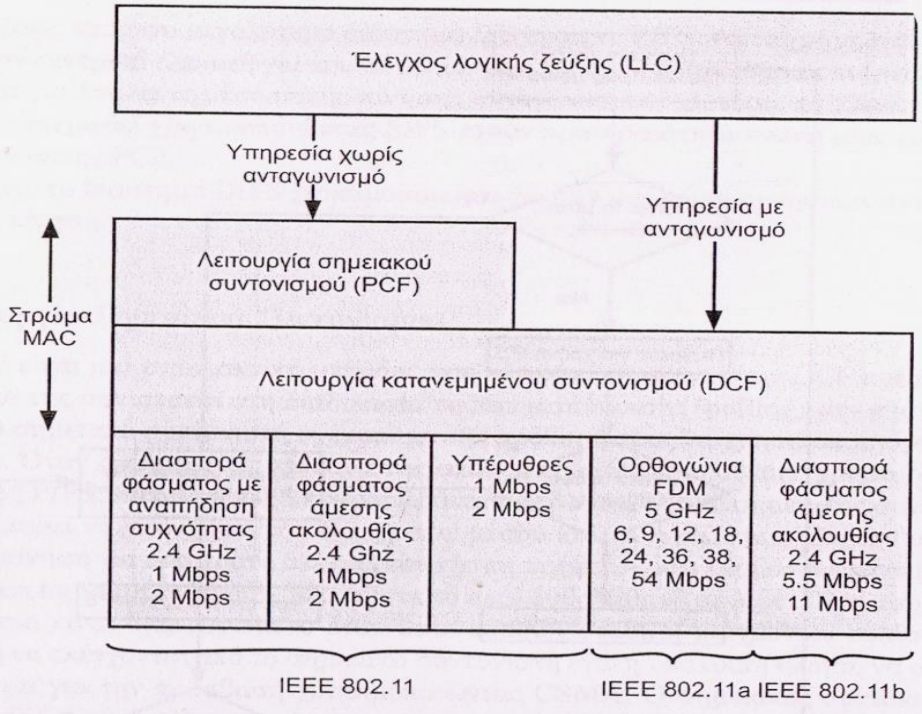



**ΕΙΚΟΝΑ 75: ΑΝΤΑΛΛΑΓΗ ΜΙΚΡΩΝ ΠΛΑΙΣΙΩΝ ΕΛΕΓΧΟΥ, RTS ΚΑΙ CTS ΑΝΑΜΕΣΑ ΣΤΟΥΣ ΣΤΑΘΜΟΥΣ ΕΚΠΟΜΠΗΣ ΚΑΙ ΛΗΨΗΣ**

Σύμφωνα με το παραπάνω σχήμα, ο σταθμός Α στέλνει ένα αίτημα στο σταθμό Β ζητώντας άδεια για να του στείλει δεδομένα. Ο σταθμός Β, αν είναι ελεύθερος, δεν μεταδίδει ή δε δέχεται δεδομένα, απαντάει στέλνοντας ένα CTS. Ο σταθμός C, καθώς και όλοι οι σταθμοί που βρίσκονται στην εμβέλεια του Β, ακούει το CTS και αντιλαμβάνεται πως δεν πρέπει να μεταδώσει προς τον σταθμό Β μέχρι να ακούσει τη μετάδοση του πλαισίου ACK, το οποίο θα δηλώνει την ολοκλήρωση της μετάδοσης. [7][9]

## 5.7 ΤΡΟΠΟΙ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΑΣΥΡΜΑΤΟ ΜΕΣΟ

Για να αρχίσει η μετάδοση ενός πλαισίου, το υπόστρωμα MAC πρέπει πρώτα να επιτύχει την πρόσβαση στο ασύρματο μέσο. Στο IEEE 802.11 υπάρχουν δύο βασικοί μέθοδοι πρόσβασης στο μέσον, η Distributed Coordination Function (DCF) και η Point Coordination Function (PCF). Επιπλέον, υπάρχουν άλλοι δύο μέθοδοι οι οποίες χρησιμοποιούνται στο πρότυπο 802.11e, η Enhanced Coordination Function (EDCF) και η Hybrid Coordination Function (HCF).




**ΕΙΚΟΝΑ 76: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΠΡΩΤΟΚΟΛΛΟΥ IEEE 802.11 [2]**

## 5.7.1 DCF (DISTRIBUTED COORDINATION FUNCTION)

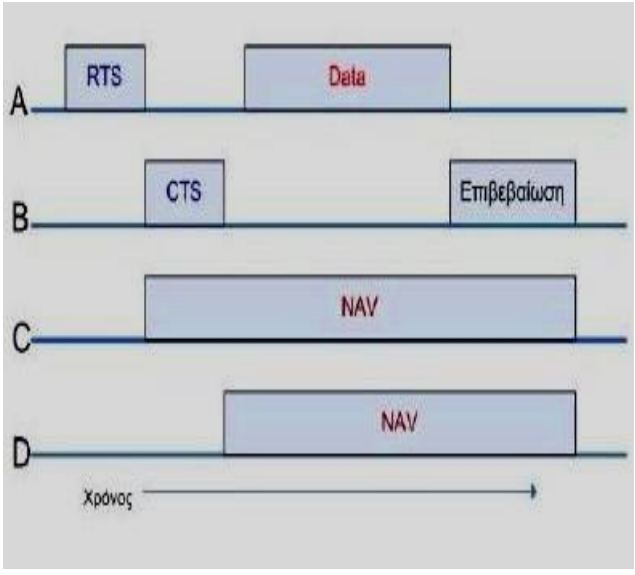
Το DCF είναι ο βασικός τρόπος πρόσβασης στο μέσο. Όλοι οι σταθμοί έχουν ίδιες ευκαιρίες για πρόσβαση στο μέσο λόγο της σχεδίασής του για ασύγχρονη μετάδοση δεδομένων. Η μέθοδος αυτή βασίζεται στο μηχανισμό CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) και μπορεί να χρησιμοποιηθεί με το μηχανισμό RTS/CTS για την καλύτερη αντιμετώπιση του προβλήματος του «κρυμμένου» κόμβου. [5][7][8]

### 5.7.1.1 CSMA/CA ΧΩΡΙΣ ΤΗ ΧΡΗΣΗ ΤΟΥ ΜΗΧΑΝΙΣΜΟΥ RTS/CTS

Ο μηχανισμός πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA) είναι παρόμοιος με το μηχανισμό πολλαπλής πρόσβασης με ανίχνευση φέροντος και ανίχνευση συγκρούσεων (Carrier Sense Multiple Access with Collision Detection - CSMA/CD). Στα ασύρματα δίκτυα έχει επιλεχθεί να χρησιμοποιείται ο μηχανισμός αποφυγής συγκρούσεων αντί για το μηχανισμό ανίχνευσης ώστε να αποφευχθούν όσο το δυνατόν περισσότερο οι συγκρούσεις. Αιτία για την επιλογή αυτή είναι η αδυναμία του δέκτη να αντιλαμβάνεται την κατάσταση του ασύρματου μέσου τη χρονική στιγμή που μεταδίδει κάποια

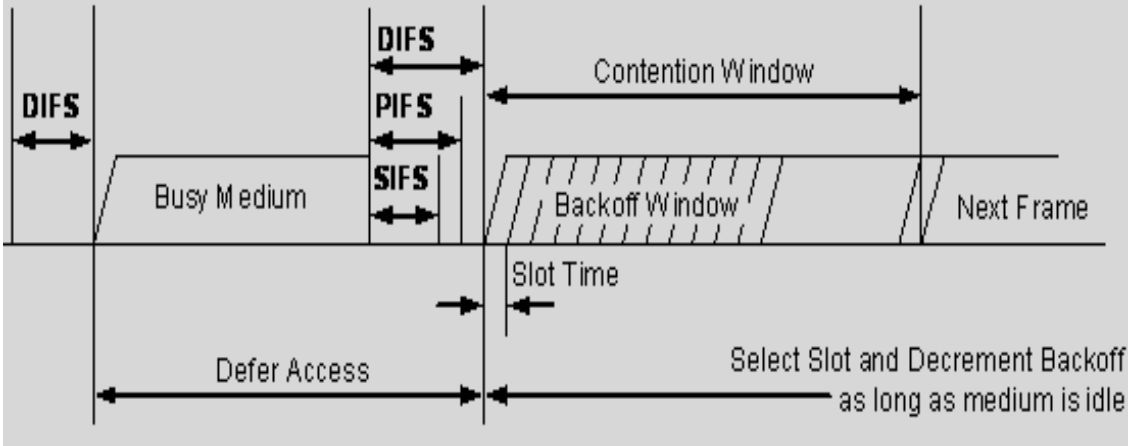
πληροφορία. Επομένως, μία σύγκρουση γίνεται αντιληπτή από τους σταθμούς μόνο εκ του αποτελέσματος που είναι φυσικά η μη παράδοση των πακέτων της πληροφορίας. Επιπλέον, στα ασύρματα δίκτυα συναντάμε προβλήματα τα οποία δεν υπάρχουν στα ενσύρματα, όπως η κακή ποιότητα της ασύρματης ζεύξης λόγω θορύβου ή παρεμβολών, το πρόβλημα του «κρυμμένου κόμβου» ακόμα και η πιθανότητα κάποιος σταθμός να βρίσκεται προσωρινά εκτός της περιοχής κάλυψης του δικτύου [1]

Ο μηχανισμός αυτός βασίζεται στον ανταγωνισμό για την κατάκτηση του μέσου. Κάθε σταθμός πριν αρχίσει τη μετάδοση κάποιου πλαισίου «ακούει», ελέγχει το μέσο ώστε να βεβαιωθεί ότι είναι ελεύθερο. Ο έλεγχος γίνεται και σε φυσικό επίπεδο και μέσω εικονικής ανίχνευσης φέροντος. Αν το μέσον είναι ελεύθερο για περισσότερο από χρόνο DIFS, ο σταθμός μεταδίδει τα δεδομένα που επιθυμεί. Αν το μέσο μετάδοσης είναι δεσμευμένο, τότε ο σταθμός συνεχίζει να ελέγχει το ασύρματο μέσο περιοδικά μέχρι αυτό να ελευθερωθεί. Συγκεκριμένα, ένας σταθμός όταν μεταδίδει ένα πλαίσιο, ενημερώνει το πεδίο ID/DURATION του πλαισίου με την ποσότητα του χρόνου κατά την οποίο θα απασχολήσει το μέσο για μία επιτυχημένη μετάδοση. Οι υπόλοιποι σταθμοί διαβάζουν το ID/DURATION πεδίο και ενημερώνουν το Network Allocation Vector (NAV) τους. Ο NAV λειτουργεί ως μετρητής, μετρώντας αντίστροφα και υπολογίζει τη διάρκεια που χρειάζεται το πλαίσιο που ανιχνεύθηκε για να μεταδοθεί. Όταν ο NAV μηδενιστεί, τότε ένας σταθμός μπορεί να εκπέμψει. Στο διπλανό σχήμα φαίνεται ένα παράδειγμα λειτουργίας του NAV.




Μόλις τελειώσει η τρέχουσα μετάδοση, ο σταθμός ο οποίος θέλει να μεταδώσει περιμένει για χρόνο DIFS. Αν το μέσο παραμείνει ελεύθερο κατά αυτόν το χρόνο, τότε οπισθοχωρεί για ένα τυχαίο χρόνο, δηλαδή για back – off time. Κατά τη διάρκεια του back – off time ο σταθμός συνεχίζει να ακούει το μέσο. Με το πέρας του back – off time, εάν το μέσον είναι ακόμα ελεύθερο, τότε μεταδίδει τα πλαίσια

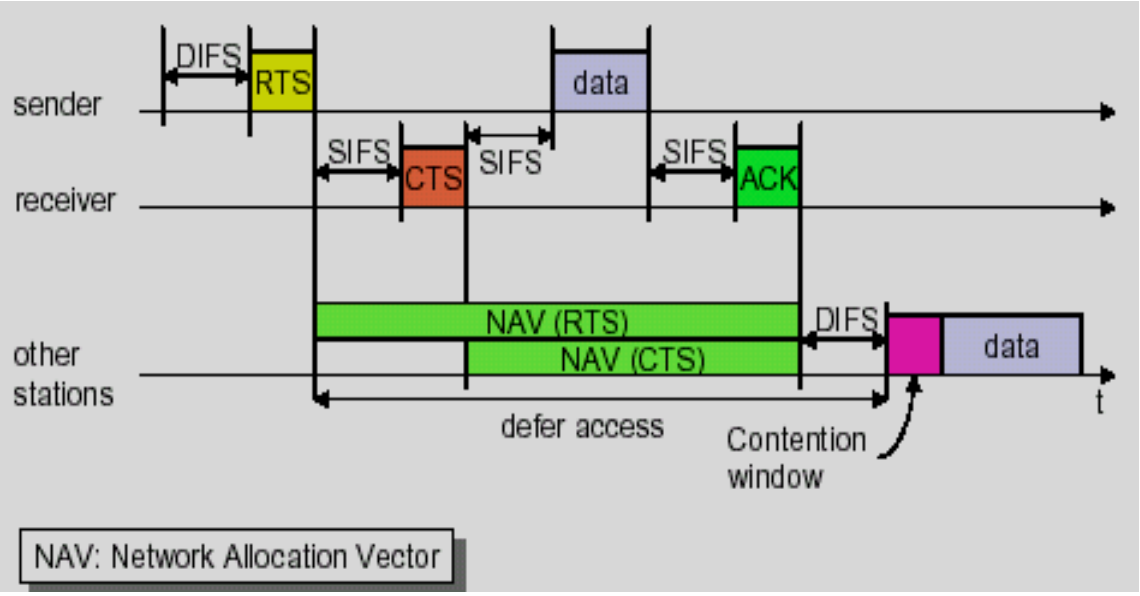
που έχει προς μετάδοση. Αν κατά τη διάρκεια αυτήν εκπέμψει κάποιος άλλος σταθμός, τότε ο back – off time σταματάει και ξανά ξεκινάει όταν ελευθερωθεί το μέσο. [6][7]




**ΕΙΚΟΝΑ 77: ΜΗΧΑΝΙΣΜΟΣ CSMA/CA ΧΩΡΙΣ ΤΗ ΧΡΗΣΗ ΤΟΥ ΜΗΧΑΝΙΣΜΟΥ RTS/CTS [8]**

### 5.7.1.2 CSMA/CA ΜΕ ΧΡΗΣΗ ΤΟΥ ΜΗΧΑΝΙΣΜΟΥ RTS/CTS

Όπως έχει ήδη αναφερθεί, σε ένα ασύρματο δίκτυο είναι πολύ πιθανόν να συμβούν συγκρούσεις, με αποτέλεσμα να αυξάνονται οι καθυστερήσεις. Το πρόβλημα του «κρυμμένου κόμβου» μεγαλώνει τις πιθανότητες να συμβεί κάποια σύγκρουση. Έτσι, ο μηχανισμός CSMA/CA, όπως φαίνεται στο επόμενο σχήμα, ενισχύθηκε με τα πλαίσια RTS/CTS, με τα οποία δεσμεύεται το μέσον ώστε να πραγματοποιηθεί η μετάδοση των πακέτων. Αυτό έχει ως σκοπό να μειωθούν οι συγκρούσεις και φυσικά να μειωθεί ο χρόνος που σπαταλιέται στις αναμεταδόσεις λόγω μη λήψης του ACK. Η μείωση του χρόνου συμβαίνει επειδή με το μηχανισμό CSMA/CA με τα πλαίσια RTS/CTS, αν συμβεί μία σύγκρουση αναμεταδίδεται μόνο το πλαίσιο RTS, το οποίο είναι πολύ μικρό σε μέγεθος, σε αντίθεση με το μηχανισμό CSMA/CA χωρίς τα πλαίσια RTS/CTS, όπου στέλνονται ξανά όλα τα δεδομένα.



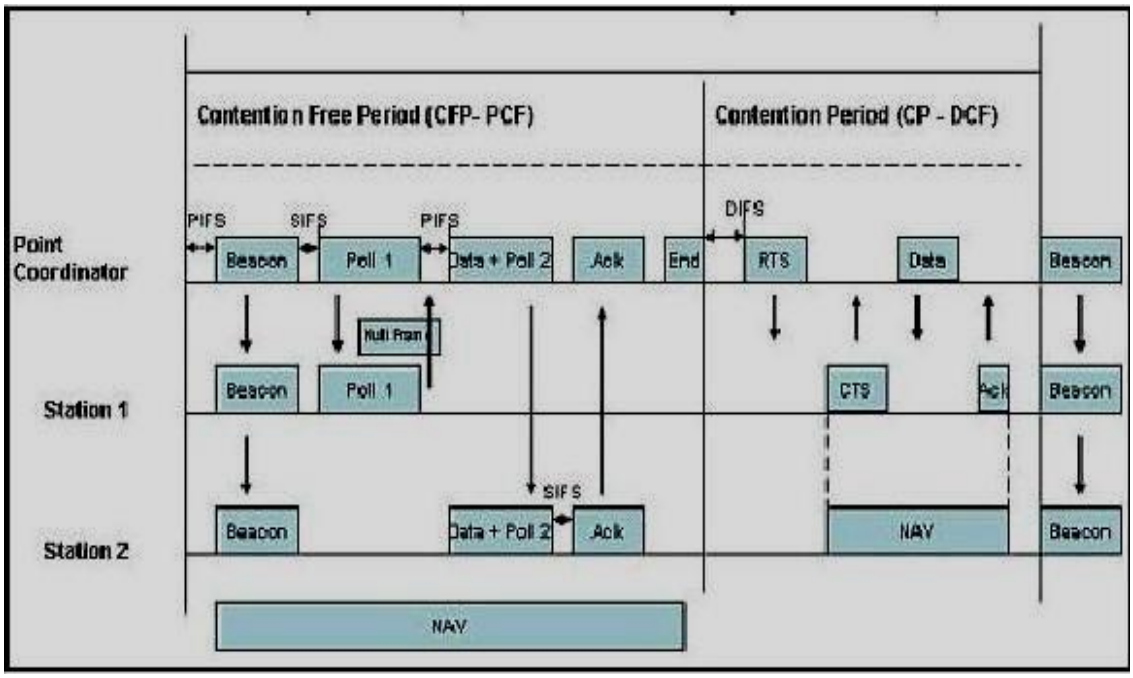

**ΕΙΚΟΝΑ 78: ΜΗΧΑΝΙΣΜΟΣ CSMA/CA ΜΕ ΧΡΗΣΗ ΤΟΥ ΜΗΧΑΝΙΣΜΟΥ RTS/CTS**

Στο μηχανισμό αυτό, ο σταθμός μόλις καταφέρει να αποκτήσει πρόσβαση στο μέσο, στέλνει ένα πλαίσιο RTS στο σταθμό που τον ενδιαφέρει. Οι υπόλοιποι σταθμοί που βρίσκονται στο ίδιο δίκτυο, λαμβάνουν το RTS και αφού διαβάσουν το πεδίο ID/DURATION, ενημερώνουν το NAV τους. Ο παραλήπτης του πλαισίου RTS, απαντάει με ένα πλαίσιο CTS αφού πρώτα περάσει SIFS χρόνος και οι υπόλοιποι σταθμοί ξανά ενημερώνουν το NAV τους. Αφού ο αποστολέας λάβει το CTS, είναι πλέον σίγουρος ότι το δίκτυο έχει δεσμευτεί για την αποστολή των δεδομένων του. Μόλις ολοκληρωθεί επιτυχώς η αποστολή του πλαισίου, ο παραλήπτης στέλνει ένα ACK για να βεβαιώσει τον αποστολέα για την ορθή λήψη των δεδομένων.

Τα πλαίσια τα οποία είναι μεγάλα σε μέγεθος, διαιρούνται σε μικρότερα πλαίσια (fragment). Το μέσο μετάδοσης παραμένει δεσμευμένο μέχρι την ολοκλήρωση όλων των τμημάτων του πλαισίου. Ο παραλήπτης για κάθε fragment που λαμβάνει στέλνει και το αντίστοιχο ACK. Ο αποστολέας μόλις λαμβάνει ένα ACK περιμένει SIFS χρόνο και μετά στέλνει το επόμενο fragment. Αν κάποια ACK δεν ληφθούν, τότε αποτυγχάνει η αποστολή και ο αποστολέας χάνει την πρόσβαση στο μέσο. Τέλος, θα πρέπει να σημειωθεί ότι όταν ένα πλαίσιο διαιρείται, μόνο στο πρώτο fragment στέλνονται RTS και CTS πλαίσια. [7]

## 5.7.2 PCF (POINT COORDINATION FUNCTION)

Η λειτουργία του μηχανισμού αυτού μοιάζει αρκετά με το σχήμα ελέγχου πρόσβασης με σκυτάλη (token based). Ο μηχανισμός αυτός δε χρησιμοποιείται ιδιαίτερα στα προϊόντα που κυκλοφορούν στην αγορά, εξαιτίας του ότι είναι προαιρετικός. Επιπλέον, ο μηχανισμός αυτός απαιτεί έναν κεντρικό έλεγχο από κάποιο AP, ο οποίος χωρίζει τους σταθμούς σε υψηλής και χαμηλής προτεραιότητας. Χρησιμοποιείται μόνο σε δομημένα (infrastructure) δίκτυα και προσφέρει πρόσβαση στο μέσον χωρίς ανταγωνισμό μεταξύ των σταθμών. Στο παρακάτω σχήμα περιγράφεται ο τρόπος λειτουργίας του μηχανισμού PCF.




**ΕΙΚΟΝΑ 79: ΜΗΧΑΝΙΣΜΟΣ PCF**

Σε αντίθεση με τα απλά δεδομένα, τα δεδομένα πραγματικού χρόνου, όπως είναι η φωνή ή το video, απαιτούν μετάδοση μέσα σε ένα συγκεκριμένο χρονικό διάστημα, ώστε να μην χαθεί η σημασία τους. Ο μηχανισμός CSMA/CA δεν ξεχωρίζει τα δεδομένα σε υψηλής ή χαμηλής προτεραιότητας γι' αυτούς τους λόγους χρειάζεται ο μηχανισμός PCF ο οποίος δίνει προτεραιότητες. Για την ακρίβεια, το PCF συνυπάρχει με το DCF στα δομημένα δίκτυα, μιας και το DCF είναι υποχρεωτικό.

Ο μηχανισμός αυτός χρησιμοποιεί σε κάθε δίκτυο έναν ελεγκτή, ο οποίος ονομάζεται Point Coordination (PC – Σημειακός Συγχρονιστής). Η χρήση του

μηχανισμού αυτού συνεπάγεται τη δημιουργία χρονικών περιόδων χωρίς ανταγωνισμό (contention – free periods), ενώ κατά τον υπόλοιπο χρόνο γίνετε χρήση του μηχανισμού DCF, όπου έχουμε ανταγωνισμό (contention periods). Οι περίοδοι με ανταγωνισμό και χωρίς ανταγωνισμό επαναλαμβάνονται διαδοχικά και η διάρκειά τους ονομάζεται contention – free repetition interval. [7]

Κατά τη διάρκεια του contention – free period τον έλεγχο για την πρόσβαση στο μέσον τον έχει ο PC. Για να καταλάβει το PC την πρόσβαση στο μέσον περιμένει για χρόνο PIFS από τη στιγμή που ελευθερώνεται το μέσον, και λόγο της μικρότερης διάρκειάς του από το DIFS, καταφέρνει και εκπέμπει πρώτο. Αρχικά, το PC εκπέμπει ένα πλαίσιο Beacon με το οποίο ενημερώνονται οι υπόλοιποι σταθμοί ότι έχουν περάσει σε περίοδο μη ανταγωνισμού και από το τμήμα Duration του πλαισίου βλέπουν πόσο θα διαρκέσει και το αποθηκεύουν στο NAV.

Στη συνέχεια, το PC περιμένει για SIFS χρόνο και στέλνει ένα πλαίσιο CF – Poll, επιλέγοντας έτσι το σταθμό που έχει προτεραιότητα να εκπέμψει. Μόλις ο παραλήπτης λάβει το CF – Poll, περιμένει για SIFS χρόνο και απαντάει με ένα πλαίσιο CF – ACK – data, όπου data τα δεδομένα που θέλει να στείλει. Αν ο παραλήπτης δεν έχει δεδομένα για αποστολή στέλνει μόνο επιβεβαίωση, ενώ αν δεν διαθέτει ούτε πλαίσιο επιβεβαίωσης στέλνει ένα κενό πλαίσιο (null frame). Κάθε σταθμός θα πρέπει πριν εκπέμψει να ελέγξει το NAV για να σιγουρευτεί ότι προλαβαίνει να στείλει τα δεδομένα και να λάβει το ACK πριν τελειώσει ο χρόνος της περιόδου μη ανταγωνισμού. Διαφορετικά στέλνει κενό πλαίσιο. Πρέπει να επισημάνουμε ότι κάθε σταθμός έχει δικαίωμα να στείλει ένα μόνο πλαίσιο και οι χρόνοι οι οποίοι χρησιμοποιούνται είναι είτε PIFS είτε SIFS. [8]

Η περίοδος χωρίς ανταγωνισμό ολοκληρώνεται όταν περάσει ο χρόνος που ορίστηκε στο πλαίσιο Beacon στην αρχή ή όταν έχουν μεταδώσει όλοι οι σταθμοί. Και στις δύο περιπτώσεις το PC στέλνει ένα πλαίσιο CF – End ή CF – End + CF – ACK στην περίπτωση που χρειάζεται να επιβεβαιωθεί η λήψη κάποιου πλαισίου δεδομένων. Οι σταθμοί μόλις λάβουν ένα από αυτά τα πλαίσια, ενημερώνουν το NAV ώστε να είναι έτοιμοι για την περίοδο ανταγωνισμού. Τέλος, είναι πρέπον να αναφερθεί ότι το πρότυπο δεν ορίζει τη μέγιστη διάρκεια της περιόδου χωρίς ανταγωνισμό, με μόνο περιορισμό ότι πρέπει να έχει ελάχιστο χρόνο τόσο ώστε να

προλαβαίνουν να μεταδοθούν δύο πλαίσια μεγίστου μεγέθους μαζί με τα πλαίσια ελέγχου και διαχείρισης.

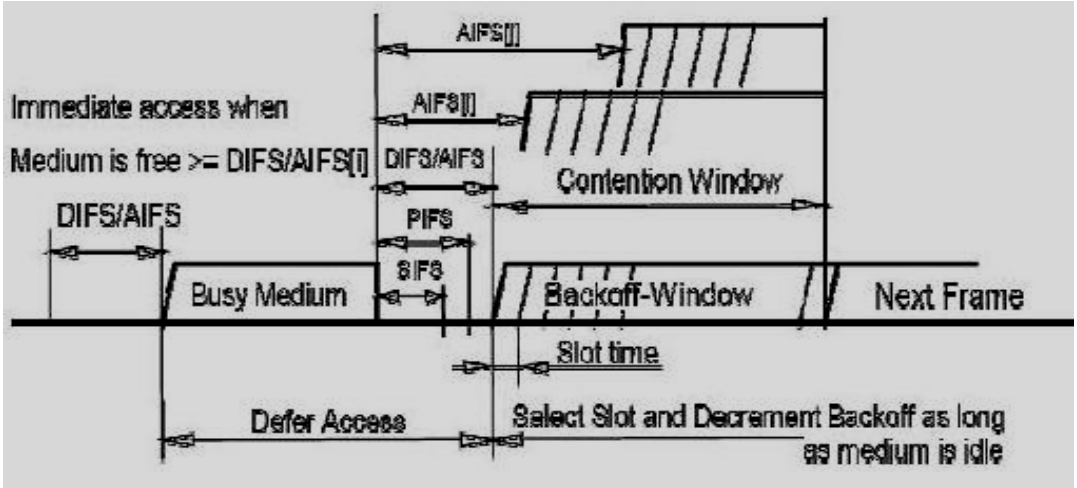
### 5.7.3 EDCF (ENHANCED COORDINATION FUNCTION)

Ο μηχανισμός EDCF, όπως και ο HCF, ο οποίος θα αναλυθεί στη συνέχεια, υποστηρίζονται από το πρωτόκολλο IEEE 802.11e. Είναι επέκταση του μηχανισμού DCF. Υποστηρίζει εφαρμογές που απαιτούν QoS (Quality of Service) και αυτό το καταφέρνει εισάγοντας τέσσερις κατηγορίες πρόσβασης (Access Categories - ACs). Ανάλογα την κατηγορία στην οποία ανήκει ένας σταθμός, ο χρόνος αναμονής του για την πρόσβαση στο μέσον διαφέρει. Για να αυξηθεί ακόμα περισσότερο η διαφοροποίηση, εισάγονται οχτώ προτεραιότητες χρήστη (User Priority – UP), με σκοπό να διαφοροποιηθούν οι σταθμοί οι οποίοι ανήκουν στην ίδια κατηγορία πρόσβασης. Στον επόμενο πίνακα παρουσιάζονται οι κατηγορίες πρόσβασης και οι προτεραιότητες χρήστη.

**ΠΙΝΑΚΑΣ 28: ΚΑΤΗΓΟΡΙΕΣ ΠΡΟΣΒΑΣΗΣ ΚΑΙ ΠΡΟΤΕΡΑΙΟΤΗΤΕΣ ΧΡΗΣΤΗ**

| USER PRIORITIES | ACCESS CATEGORY | DESIGNATION |
|---|---|---|
| 0 | 0 | Best effort |
| 1 | 0 | Best effort |
| 2 | 0 | Best effort |
| 3 | 1 | Video Probe |
| 4 | 2 | Video |
| 5 | 2 | Video |
| 6 | 3 | Voice |
| 7 | 3 | Voice |

Κάθε σταθμός ανήκει σε μία κατηγορία και έχει μία προτεραιότητα χρήστη, όμως μία ή περισσότερες προτεραιότητες μπορούν να ανήκουν στην ίδια κατηγορία πρόσβασης. Υψηλότερη προτεραιότητα έχουν οι σταθμοί με AC ίσο με 3. Στο επόμενο σχήμα παρουσιάζεται η μετάδοση δεδομένων με το μηχανισμό EDCF.




**ΕΙΚΟΝΑ 80: ΜΗΧΑΝΙΣΜΟΣ EDCF**

## 5.7.4 HCF (HYBRID COORDINATION FUNCTION)

Το HCF είναι επέκταση του PCF. Κατά τη διάρκεια της περιόδου με ανταγωνισμό, ορίζεται ένας HC (Hybrid Coordinator) ο οποίος στέλνει ένα πλαίσιο QoS CF – Poll στο σταθμό που έχει μεγαλύτερη προτεραιότητα. Οι υπόλοιποι σταθμοί διαβάζουν το πεδίο DURATION / ID και ενημερώνουν το NAV, σταματούν τις προσπάθειες για απόκτηση του μέσου και ο σταθμός ξεκινάει να μεταδίδει τα δεδομένα του. Ο μηχανισμός αυτός προσφέρει αποκλειστική χρήση του καναλιού για τον HC και για το σταθμό που μεταδίδει, με αποτέλεσμα να μη μπορεί κανένας άλλος σταθμός να έχει πρόσβαση στο κανάλι, μέχρι να περάσει DIFS χρόνος μετά την επιτυχημένη αποστολή των δεδομένων, έτσι ώστε να μειώνονται οι πιθανότητες να συμβεί κάποια σύγκρουση.

## 5.8 ΣΥΝΟΨΗ

Ανακεφαλαιώνοντας, στην αρχή του κεφαλαίου έγινε μία μικρή αναφορά στις υπηρεσίες των ασύρματων δικτύων και στη συνέχεια περιγραφή του υποστρώματος MAC. Αναλύθηκαν οι χρόνοι αναμονής, το παράθυρο ανταγωνισμού και φυσικά το πρόβλημα του «κρυμμένου κόμβου». Τέλος, περιγράφηκαν οι μέθοδοι πρόσβασης στο μέσο, με βασικότερους το PCF και το DCF. Πέρα όμως από την ολοκληρωμένη περιγραφή του προτύπου IEEE 802.11, υπάρχουν και άλλα πρότυπα τα οποία είναι χρήσιμο να τα γνωρίζετε. Τα πρότυπα που θα αναλυθούν στο επόμενο κεφάλαιο είναι το HomeRF, το IrDa, το Hiperlan και το Bluetooth.

# 6. ΑΛΛΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

## 6.1 ΕΙΣΑΓΩΓΗ

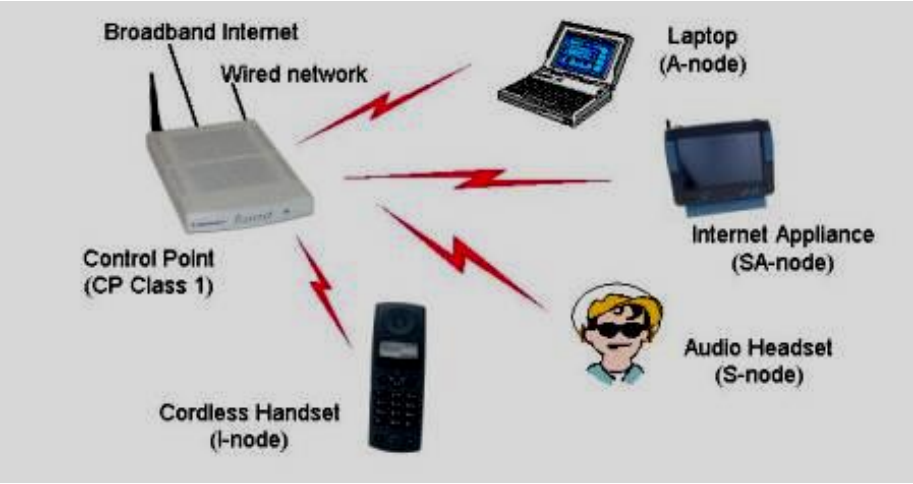
Εκτός από το πρότυπο IEEE 802.11 υπάρχουν και άλλες τεχνολογίες για την ασύρματη δικτύωση. Οι τεχνολογίες που παρατίθενται παρακάτω χρησιμοποιούνται σε ασύρματα προσωπικά δίκτυα (PAN) και σε ασύρματα τοπικά δίκτυα (LAN). Για την ασύρματη δικτύωση σε ασύρματα προσωπικά δίκτυα παρατίθενται οι τεχνολογίες HomeRF, IrDA και το γνωστό σε όλους, δια μέσου των κινητών τηλεφώνων, Bluetooth. Τέλος, για τα ασύρματα τοπικά δίκτυα το πανευρωπαϊκό πρότυπο HIPERLAN.

## 6.2 HOMERF

Η ομάδα εργασίας του προτύπου HomeRF (for Home Radio Frequency) δημιουργήθηκε το 1998 και διαλύθηκε το 2003. Η ομάδα εργασίας του προτύπου HomeRF ήταν ένας μη κερδοσκοπικός οργανισμός, ο οποίος υπαγόταν στη Διεθνή Ένωση Τηλεπικοινωνιών (ITU) και συνεργαζόταν με 100 εταιρείες για την ασύρματη δικτύωση.

Η ομάδα εργασίας HomeRF είχε ως στόχο την ανάπτυξη ενός προτύπου που θα αφορά την οικιακή δικτύωση, θα έχει χαμηλό κόστος και ευκολία χρήσης. Η ομάδα εργασίας HomeRF το 2001, ανέπτυξε το πρωτόκολλο SWAP (Shared Wireless Access Protocol), που έπειτα το μετονόμασαν σε HomeRF.

Το πρότυπο HomeRF χρησιμοποιείται για την δικτύωση των οικιακών συσκευών όπως των υπολογιστών (σταθερών ή laptop), τους εκτυπωτές, ασύρματα τηλέφωνα και άλλα για την μεταφορά φωνής και δεδομένων μέσω του internet και του Δημόσιου Δικτύου Μεταγωγής Τηλεφωνίας (Public Switched Telephone Network, PSTN)[5] .




**ΕΙΚΟΝΑ 81: ΕΙΔΗ ΣΥΣΚΕΥΩΝ ΓΙΑ ΤΗΝ ΔΙΚΤΥΩΣΗ HOMERF**

Το πρότυπο HomeRF (ή SWAP) περιέχει ένα συνδυασμό της τεχνολογίας Wireless LAN και του Ευρωπαϊκού προτύπου DECT (Digital Enhanced Cordless Telecommunications) για ασύρματα τηλέφωνα. Το πρότυπο HomeRF έχει δύο εκδόσεις, τη HomeRF1.2 και τη HomeRF2.0[5]. Το πρότυπο HomeRF1.2 υποστηρίζει ρυθμούς μετάδοσης ως 1.6 Mbps και η εμβέλεια του εκτείνεται στα 50 μέτρα[7]. Το πρότυπο HomeRF2.0 υποστηρίζει ρυθμούς μετάδοσης ως 10 Mbps και είναι συμβατό με το προηγούμενο πρότυπο. Οι κυριότερες διαφορές των δύο εκδόσεων προβάλλονται στον παρακάτω πίνακα (Nicopolitidis et all,2006). Παρακάτω αναπτύσσεται η τοπολογία του προτύπου HomeRF και τα επίπεδα του HomeRF.

**ΠΙΝΑΚΑΣ 29: ΔΙΑΦΟΡΕΣ ΤΩΝ ΔΥΟ ΕΚΔΟΣΕΩΝ ΠΡΟΤΥΠΩΝ HOMERF**

| | HomeRF 1. 2 | HomeRF 2.0 |
|---|---|---|
| **ΣΥΧΝΟΤΗΤΑ** | 2.4 GHz ISM | 2.4 GHz ISM |
| **ΔΙΑΜΟΡΦΩΣΗ** | FHSS, κανάλια 1 MHz | FHSS, κανάλια 1 και 5 MHz |
| **ΜΕΓΙΣΤΗ ΤΑΧΥΤΗΤΑ** | 1.6 Mbps | 10 Mbps |
| **ΡΥΘΜΟΣ ΜΕΤΑΠΗΔΗΣΗΣ** | 50 hops/sec | 50 hops/sec, 100 hops/sec |

| | HomeRF 1. 2 | HomeRF 2.0 |
|---|---|---|
| **ΙΣΧΥΣ ΕΚΠΟΜΠΗΣ** | 100mW | 100mW, 500mW |
| **ΠΕΡΙΑΓΩΓΗ** | ΟΧΙ | ΝΑΙ |

### 6.2.1 Η ΤΟΠΟΛΟΓΙΑ ΤΟΥ ΠΡΟΤΥΠΟΥ HOMERF

Οι προδιαγραφές του προτύπου HomeRF συνδυάζουν μηχανισμούς για την μεταφορά των δεδομένων όπως την βέλτιστη προσπάθεια των ασύγχρονων δεδομένων, την προτεραιότητα της ροής των ασύγχρονων δεδομένων (ήχου και βίντεο) και τις υπηρεσίες της ισόχρονης αλληλεπιδραστικής φωνής. Το δίκτυο HomeRF περιλαμβάνει κόμβους ανάλογα με τις ιδιότητες των συσκευών που παρουσιάζονται παρακάτω[5][11]:

- Το σημείο σύνδεσης (Connection Points, CP), το οποίο είναι μια συσκευή που ενεργεί ως πύλη και συνδέει τον υπολογιστή με το δίκτυο HomeRF, το δημόσιο τηλεφωνικό δίκτυο μεταγωγής και με άλλες συσκευές.
- Ο ασύγχρονος κόμβος (Asynchronous nodes) που είναι μια συσκευή για την μετάδοση ασύγχρονων δεδομένων, όπως το laptop και το PDA(Personal Digital Assistance).
- Ο ισόχρονος κόμβος (Isochronous nodes) που είναι μια συσκευή για την μετάδοση ισοχρόνων δεδομένων, όπως το ασύρματο τηλέφωνο.
- Ο συνδυασμός ασύγχρονων και ισόχρονων κόμβων (AI nodes).

Όταν το σημείο σύνδεσης δεν υπάρχει, το δίκτυο HomeRF λειτουργεί σαν ένα ad-hoc δίκτυο και μεταφέρει μόνο ασύγχρονα δεδομένα. Ο συγχρονισμός των ασύγχρονων κόμβων πραγματοποιείται ισότιμα από όλους τους ασύγχρονους κόμβους. Για την αποφυγή των συγκρούσεων, κατά την έναρξη του υπερπλαισίου δομής, οι ασύγχρονοι κόμβοι υποχωρούν με διάρκεια ίση με την διάρκεια του beacon πλαισίου, όπως στο πρότυπο 802.11.

Όταν το σημείο σύνδεσης υπάρχει, είναι υπεύθυνο για την διαχείριση του δικτύου. Το σημείο σύνδεσης υποστηρίζει ισόχρονη μεταφορά δεδομένων χωρίς

ανταγωνισμό, όπως η μέθοδος PCF (Point Coordination Function) στο 802.11 με διαφορά το ότι εδώ υπάρχει μεταφορά ισόχρονων δεδομένων. Το σημείο σύνδεσης χρησιμοποιεί την πολλαπλή πρόσβαση με διαίρεση χρόνου (TDMA) για την ανάθεση του εύρους ζώνης για την μεταφορά ισόχρονων δεδομένων μεταξύ των κόμβων του δικτύου HomeRF.

Το σημείο σύνδεσης είναι υπεύθυνο να παρέχει πληροφορίες συγχρονισμού με τη μετάδοση πλαισίων beacon στους ισόχρονους και στους ασύγχρονους κόμβους. Το πλαίσιο beacon περιέχει το μήκος του υπερπλαισίου δομής και την ακολουθία μεταπήδησης του χρησιμοποιούμενου δικτύου HomeRF.

Όταν τα σημεία σύνδεσης είναι περισσότερα από ένα, ένα μόνο σημείο σύνδεσης αναλαμβάνει για μία χρονική διάρκεια να είναι σε ενεργή κατάσταση και τα υπόλοιπα σημεία σύνδεσης αναλαμβάνουν την παθητική κατάσταση. Όταν ένα σημείο σύνδεσης έχει αποτυχία λήψης 50 συνεχόμενων πλαισίων beacon που μετέδωσε το σημείο σύνδεσης με ενεργή κατάσταση, τότε το σημείο σύνδεσης πιστεύει ότι το σημείο σύνδεσης με ενεργή κατάσταση είτε είναι εκτός εμβέλειας είτε δυσλειτουργεί. Τότε ένα σημείο παθητικής κατάστασης μετατρέπεται σε σημείο ενεργής κατάστασης.

Στην περίπτωση που οι ασύγχρονοι κόμβοι έχουν αποτυχία λήψης 100 συνεχόμενων πλαισίων beacon από το μοναδικό σημείο σύνδεσης υποθέτουν ότι αυτό το σημείο σύνδεσης είναι εκτός εμβέλειας ή δυσλειτουργεί, και σχηματίζουν δικό τους ad hoc δίκτυο.

Ένα σημείο σύνδεσης του δικτύου HomeRF ρυθμίζεται ώστε να αναλάβει την διαχείριση ισχύος είτε σε κόμβους εξοικονόμησης ενέργειας (Power Saving, PS) είτε σε κόμβους μη εξοικονόμησης ενέργειας. Η εξοικονόμηση ενέργειας περιλαμβάνει κόμβους που παραμένουν ανενεργοί για συγκεκριμένα διαστήματα και καταναλώνουν χαμηλή ισχύ.

Οι ισόχρονοι κόμβοι ενεργοποιούνται όταν περάσει κάποιος αριθμός υπερπλαισίων για να λάβουν το πλαίσιο σηματοδοσίας που περιλαμβάνει τις πληροφορίες για την ανάθεση των χρονικών σχισμών και την λίστα των ισόχρονων κόμβων που είναι σε αναμονή για μετάδοση φωνής κατά τις περιόδους

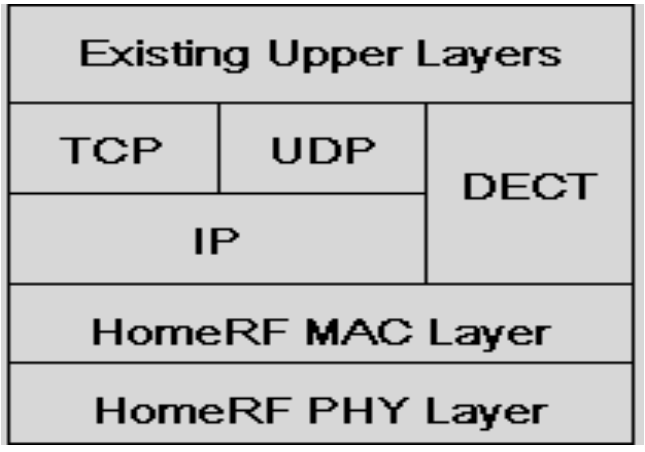
άνευ ανταγωνισμού. Αφού λάβουν τις πληροφορίες παραμένουν ανενεργοί μέχρι να έρθει η χρονική στιγμή να λάβουν ή να μεταδώσουν δεδομένα.

Οι ασύγχρονοι κόμβοι ενεργοποιούνται κατά διαστήματα για να ελέγξουν στο πλαίσιο σηματοδοσίας αν υπάρχουν πακέτα για λήψη unicast εκπομπής. Αν δεν υπάρχουν μένουν ανενεργοί μέχρι να αντιληφθούν ότι υπάρχουν πακέτα για λήψη ή για αποστολή μονής κατεύθυνσης και παραμένουν ενεργοί ώσπου η διάρκεια του υπερπλαισίου να τελειώσει.

Τα δεδομένα broadcast εκπομπής αποθηκεύονται στο σημείο σύνδεσης μέχρι να ενεργοποιηθούν οι ασύγχρονοι κόμβοι. Το σημείο πρόσβασης στέλνει μια παράμετρο Β μέσα στο πλαίσιο σηματοδοσίας που περιλαμβάνει τα Β χρονικά υπερπλαίσια που πρέπει να περάσουν για να ενεργοποιηθούν οι κόμβοι και να λάβουν δεδομένα broadcast εκπομπής[5].

### 6.2.2 ΕΠΙΠΕΔΑ ΤΟΥ ΠΡΟΤΥΠΟΥ HOMERF

Το πρότυπο ακολουθεί το μοντέλο του OSI με τροποποιήσεις του φυσικού και του υποστρώματος MAC και με τη χρησιμοποίηση των πρωτοκόλλων TCP, IP και UDP για τη μεταφορά δεδομένων στο Internet και το πρότυπο DECT για καλύτερη ποιότητα μετάδοσης φωνής και την αποφυγή παρεμβολών.




**ΕΙΚΟΝΑ 82: ΕΠΙΠΕΔΑ ΤΟΥ ΠΡΟΤΥΠΟΥ HOMERF**

#### 6.2.2.1 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΤΟΥ ΠΡΟΤΥΠΟΥ HOMERF

Το πρότυπο HomeRF χρησιμοποιεί την τεχνική FHSS και λειτουργεί στη μη αδειοδοτημένη ISM ζώνη συχνοτήτων των 2.4 GHz με 79 διαφορετικά κανάλια για την Αμερική και 23 διαφορετικά για την Ευρώπη. Το πρότυπο HomeRF1.2

χρησιμοποιεί διαμόρφωση FSK level 2 για τον ρυθμό μετάδοσης δεδομένων του 1 Mbps και τη διαμόρφωση FSK level 4 για τον ρυθμό μετάδοσης δεδομένων των 2 Mbps στα κανάλια με εύρος 1 MHz. Στην έκδοση αυτή, ο ρυθμός μεταπήδησης είναι 50 hops/sec με διάρκεια χρόνου εκπομπής υπερπλαισίου (dwell time) των 20 msec και η ισχύ μετάδοσης είναι 100 mW.

Το πρότυπο HomeRF 2.0 χρησιμοποιεί διαμόρφωση FSK level 2 και τη διαμόρφωση FSK level 4 όπως στην προηγούμενη έκδοση για να υπάρχει συμβατότητα. Το πρότυπο HomeRF2.0 για να επιτύχει τις ταχύτητες 5 Mbps και 10 Mbps διαχωρίζει το χρησιμοποιούμενο φάσμα σε 15 κανάλια με εύρος 5MHz. Η ισχύ μετάδοσης είναι ως 500 mW, ο ρυθμός μεταπήδησης είναι 50 hops/sec ή 100 hops/sec με διάρκεια χρόνου εκπομπής υπερπλαισίου (dwell time) των 10 msec για ισόχρονη μετάδοση με ρυθμό μετάδοσης ως 1.6 Mbps και των 20 msec για ασύγχρονη μετάδοση ως 10 Mbps[5].

#### 6.2.2.2 ΤΟ ΥΠΟΣΤΡΩΜΑ MAC ΤΟΥ ΠΡΟΤΥΠΟΥ HOMERF

Για την πρόσβαση στο μέσο από την ασύγχρονη και την ισόχρονη μετάδοση έχει δημιουργηθεί ένα υπερπλαίσιο. Κατά την ασύγχρονη μετάδοση το υπερπλαίσιο έχει διάρκεια 20 msec, χρησιμοποιεί την μέθοδο CSMA/CA και έχει μηδενική τιμή στην διάρκεια της περιόδου άνευ ανταγωνισμού (CFP). Αυτό οφείλεται στο γεγονός ότι χρησιμοποιεί την λειτουργία της περιόδου ανταγωνισμού όπως στο πρότυπο IEEE 802.11, με εξαίρεση του προτύπου HomeRF2.0, που περιλαμβάνεται ο μηχανισμός προτεραιοτήτων για ασύγχρονα δεδομένα. Ο μηχανισμός προτεραιότητας για ασύγχρονα δεδομένα χρησιμοποιεί έναν αριθμό πρόσβασης, ο οποίος λαμβάνεται μόλις ιδρυθεί η σύνοδος της ροής πολυμέσων. Ο αριθμός πρόσβασης με την μικρότερη τιμή παρέχει μεγαλύτερη προτεραιότητα στην ροή αυτή. Όταν οι ασύγχρονοι κόμβοι υποχωρήσουν, η μέθοδος CSMA/CA με την λειτουργία ανταγωνισμού είναι υπεύθυνη να αλλάξει τους αριθμούς πρόσβασης που είχαν.

**ΠΙΝΑΚΑΣ 30: ΤΙΜΕΣ ΤΩΝ ΠΑΡΑΜΕΤΡΩΝ CSMA/CA ΣΤΟ ΠΡΟΤΥΠΟ HOMERF**

| ΠΑΡΑΜΕΤΡΟΣ | ΤΙΜΗ |
|---|---|
| Μέγεθος SIFS | 142 μsec |
| Μέγεθος DIFS | 309 μsec |
| Μέγεθος σχισμής | 167 μsec |
| Ελάχιστο μέγεθος παραθύρου ανταγωνισμού | 8 σχισμές |
| Μέγιστο μέγεθος παραθύρου ανταγωνισμού | 64 σχισμές |

Στην ισόχρονη μετάδοση το υπερπλαίσιο περιέχει δύο περιόδους άνευ ανταγωνισμού (CFP). Στο πρότυπο HomeRF 2.0 το υπερπλαίσιο αλλάζει την διάρκεια του από 20 msec σε 10 msec για καλύτερη ποιότητα, χαμηλότερες καθυστερήσεις και αντοχή σε παρεμβολές. Το σημείο σύνδεσης έχει την ίδια λειτουργία με το σημείο συντονιστή (Point Coordination, PC) του δικτύου 802.11 κατά την λειτουργία της περιόδου CFP. Οι διαφορές μεταξύ της λειτουργίας της περιόδου CFP του δικτύου 802.11 με την λειτουργία της περιόδου CFP του δικτύου HomeR είναι[5]:

- Η σύνδεση της φωνής είναι full duplex και χρησιμοποιεί τον διπλό διαχωρισμό του χρόνου (time division duplex, TDD) με δύο χρονικές σχισμές που περιλαμβάνουν μία upload για την αποστολή και μία download για την λήψη πακέτων φωνής.
- Το σημείο σύνδεσης χορηγεί άδεια μετάδοσης πακέτων φωνής στους ισόχρονους κόμβους με ενεργή κατάσταση χρησιμοποιώντας την διαιτησία TDMA.
- Οι αρχικές μεταδόσεις πακέτων φωνής γίνονται πάντα κατά την διάρκεια CFP2 του υπερπλαισίου, ενώ κατά την διάρκεια CFP1 του υπερπλαισίου γίνεται μία αναμετάδοση δεδομένων, αν το προηγούμενο υπερπλαίσιο με διάρκεια CFP2 δεν είχε επιτυχή μετάδοση.

## 6.3 IrDA

Ο οργανισμός Infrared Data Association (IrDA) ανέπτυξε ένα πρότυπο που απευθύνεται στις ασύρματες συνδέσεις δεδομένων με υπέρυθρες. Ο Infrared Data Association είναι ένας μη κερδοσκοπικός οργανισμός που είναι υπεύθυνος για τη δημιουργία και την ανάπτυξη προτύπων ώστε να διασφαλίζει την διαλειτουργικότητα του υλικού και του λογισμικού διάφορων συσκευών που χρησιμοποιούν ασύρματη επικοινωνία με υπέρυθρες[2].

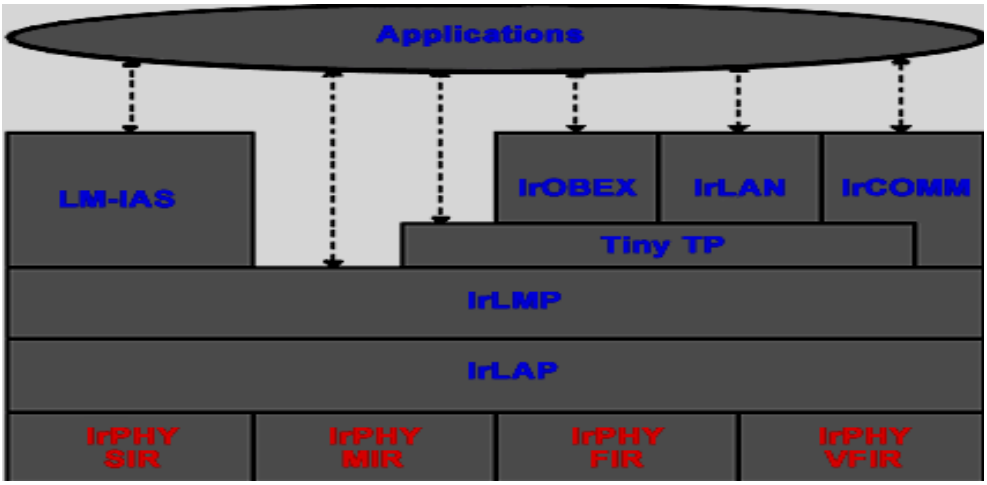
Το πρότυπο IrDA παρέχει χαμηλό κόστος, χαμηλή ισχύ, σειριακές συνδέσεις δεδομένων που υποστηρίζουν half-duplex επικοινωνία σε απόσταση έως 1 μέτρο και ρυθμό μετάδοσης έως 4 Mbps. Το πρότυπο IrDA χρησιμοποιείται για την μετάδοση δεδομένων από πολλές συσκευές όπως υπολογιστές, PDA, εκτυπωτές, ιατρικούς και βιομηχανικούς εξοπλισμούς, κάμερες, τηλέφωνα και άλλες.

Το πρότυπο IrDA έχει δύο πρότυπα, το IrDA Sir και το AIr. Το πρότυπο IrDA Sir (Serial Infrared) απευθύνεται για σειριακές συνδέσεις, έχει μικρή εμβέλεια και οι ρυθμοί μετάδοσής του ξεκινούν από 9.6 Kbps έως 4 Mbps.

Το πρότυπο IrDA AIr χρησιμοποιεί την τεχνική διαμόρφωσης 4PPM και δεν χρειάζεται οπτική επαφή. Η εμβέλεια του φτάνει τα 3.8 μέτρα με ρυθμό μετάδοσης 4 Mbps και πάνω από 7.6 μέτρα με ρυθμό μετάδοσης 250 Kbps. Και τα δύο πρότυπα περιλαμβάνουν τη διαστρωμάτωση του προτύπου IrDA με τις διαφορές που προαναφέρθηκαν[6].


**ΕΙΚΟΝΑ 83: ΣΥΣΚΕΥΕΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝ ΤΟ ΠΡΟΤΥΠΟ IrDA**

Οι προδιαγραφές της διαστρωμάτωσης του προτύπου IrDA περιλαμβάνουν το φυσικό επίπεδο, το επίπεδο ζεύξης δεδομένων και τα υπόλοιπα στρώματα που περιλαμβάνονται στα προαιρετικά πρωτοκόλλα, τα οποία θα αναλυθούν στην συνέχεια.




**ΕΙΚΟΝΑ 84: ΕΠΙΠΕΔΑ ΤΟΥ ΠΡΟΤΥΠΟΥ IrDA**

## 6.3.1 ΤΟ ΦΥΣΙΚΟ ΣΤΡΩΜΑ ΤΟΥ ΠΡΟΤΥΠΟΥ IrDA

Τα σημαντικότερα χαρακτηριστικά του προτύπου IrDA για το φυσικό στρώμα IrPHY αναφέρονται παρακάτω[2][6][7]:

- Η ισχύς εκπομπής δεν πρέπει να ξεπερνά τα 500 mW/sr (milliwatts per steradian), επίσης χωρίζεται σε δύο τύπους: α) στην κανονική ισχύ που περιλαμβάνει την μέγιστη ισχύ και β) στην χαμηλή ισχύ που περιλαμβάνει ισχύ εκπομπής 28.2 mW/sr.
- Η απόσταση φτάνει μέχρι το 1 μέτρο με την κανονική ισχύ και τα 0.2 μέτρα με τη χαμηλή ισχύ.
- Το μήκος κύματος των υπερύθρων που είναι στα 800nm ως τα 900nm.
- Η γωνία εκπομπής με ελάχιστου κώνου είναι +30 ή -30 μοίρες.
- Ο ρυθμός μετάδοσης ξεκινάει από 9.6 Kbps έως 16 Mbps.

Οι προδιαγραφές του προτύπου περιλαμβάνουν τους παρακάτω τύπους μετάδοσης[2][6][7]:

- Τη σειριακή με υπέρυθρες (Serial infrared, SIR) που είναι για την ασύγχρονη μετάδοση και περιλαμβανόταν στο πρώτο πρότυπο με διαμόρφωση UART και ρυθμούς μετάδοσης 2.400 Kbps ως 115 Kbps. Τώρα χρησιμοποιείται με διαμόρφωση RZI και έχει ρυθμούς μετάδοσης από 9.6 Kbps ως 115.2 Kbps.
- Την γρήγορη με υπέρυθρες (Fast infrared,FIR) που είναι για την σύγχρονη μετάδοση με διαμόρφωση RZI με ρυθμούς μετάδοσης από 0.576 Mbps έως 1.152 Mbps και τη διαμόρφωση 4-PPM με ρυθμό μετάδοσης 4 Mbps.
- Την πολύ γρήγορη με υπέρυθρες (Very Fast infrared,VFIR) που είναι για την σύγχρονη μετάδοση με διαμόρφωση HHH και έχει ρυθμούς μετάδοσης από 9.6 Kbps ως 16 Mbps.

Οι ρυθμοί μετάδοσης ξεκινούν από 9.6 Kbps για να υποστηρίζουν την διαλειτουργικότητα.

Υπάρχουν και αυτοί οι εναλλακτικοί τύποι μετάδοσης, οι οποίοι είναι[2]:

- Η ultra-fast με υπέρυθρες (UFIR) με ρυθμό μετάδοσης έως 96 Mbps.
- Η Giga-IR με υπέρυθρες που χρησιμοποιεί τη διαμόρφωση 2 ASK για ρυθμό μετάδοσης 512 Mbps και τη διαμόρφωση 4 ASK για ρυθμό μετάδοσης 1 Gbps.

### 6.3.2 ΕΠΙΠΕΔΟ ΖΕΥΞΗΣ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΤΟ ΠΡΟΤΥΠΟ IrDA

Το επίπεδο Ζεύξης Δεδομένων του IrDA περιλαμβάνει δύο πρωτόκολλα, το IrLAP για την πρόσβαση σύνδεσης και το IrLMP για τη διαχείριση της σύνδεσης. Το πρωτόκολλο IrLAP είναι υπεύθυνο για την σύνδεση των διαφορετικών συσκευών, εγκαθιστά τον ρυθμό μετάδοσης των δεδομένων για την καλύτερη ποιότητα υπηρεσιών (QoS) των συνδεδεμένων συσκευών, ελέγχει την υπηρεσία ανίχνευσης που γίνεται με τυχαίο τρόπο και ελέγχει την διευθυνσιοδότηση των συσκευών που ανταλλάσουν κατά την ανίχνευση. Το πρωτόκολλο αυτό κατανέμει τους ρόλους που θα έχουν οι συσκευές, χρησιμοποιώντας την σχέση master-slave. Ο ρόλος του master περιλαμβάνει την αποστολή πλαισίων command, την αρχικοποίηση των συνδέσεων και των μεταδόσεων, τον έλεγχο και την οργάνωση της ροής των δεδομένων και την διαχείριση των λαθών κατά την σύνδεση. Ο

ρόλος του slave περιλαμβάνει την αποστολή πλαισίων απάντησης για τις εντολές και τις απαιτήσεις του master.

Το πρωτόκολλο IrLMP είναι πάνω από το επίπεδο του IrLAP και χωρίζεται στο LM-MUX και στο LM-IAS .Ο πολυπλέκτης της διαχείρισης των συνδέσεων(LM-MUX) είναι υπεύθυνος για την πολύπλεξη των υπηρεσιών και των εφαρμογών των συνδέσεων του πρωτοκόλλου IrLAP, παρέχει πολλαπλά λογικά κανάλια που είναι ανεξάρτητα μεταξύ τους και χρησιμοποιούνται από εφαρμογές των υψηλότερων επιπέδων. Επίσης το LM-MUX επιτρέπει την αλλαγή ρόλων των συσκευών (master-slave).Η υπηρεσία πληροφοριών πρόσβασης της διαχείρισης συνδέσεων LM-IAS παρέχει μία βάση δεδομένων για τις πληροφορίες σχετικά με τις συσκευές, την ανίχνευση των συσκευών και την διαθεσιμότητα των εφαρμογών που υπάρχουν σε κάθε συσκευή. Η υπηρεσία αυτή βρίσκεται πάνω από το LM-MUX[2][6][7].

### 6.3.3 ΠΡΟΑΙΡΕΤΙΚΑ ΠΡΩΤΟΚΟΛΛΑ

Tiny-TP

Το πρωτόκολλο Tiny-TP είναι στο ενδιάμεσο επίπεδο του IrLMP και παρέχει μεταφορά μεγάλων μηνυμάτων από το SAR (Segmentation and Reassembly). Ελέγχει τη ροή προσθέτοντας ένα επιπλέον byte σε κάθε πλαίσιο για την υπερχείλιση.

IrCOMM

Το πρωτόκολλο IrCOMM (Infrared Communication Protocol) επιτρέπει στην συσκευή να συμπεριφέρεται σαν παράλληλη ή σαν σειριακή θύρα σύνδεσης όπως για την εφαρμογή εκτύπωσης.

IrOBEX

Το πρωτόκολλο IrOBEX ανήκει στο επίπεδο εφαρμογών και επιτρέπει στις εφαρμογές να ανταλλάσουν αυθαίρετα πολλά διαφορετικά δεδομένα όπως αρχεία, ηλεκτρονικές επαγγελματικές κάρτες και ψηφιακές εικόνες. Για την χρήση του πρωτοκόλλου αυτού πρέπει να χρησιμοποιηθεί το πρωτόκολλο Tiny-TP.

IrLAN

Το πρωτόκολλο IrLAN επιτρέπει την πρόσβαση στα τοπικά δίκτυα προσομοιώνοντας την σύνδεση Ethernet χαμηλότερου επιπέδου περιλαμβάνοντας το TCP/IP με τις μεθόδους peer-to-peer, access point με την χρήση ενός IrLAN adapter και hosted μέσω άλλου υπολογιστή που σχετίζεται με το LAN. Το πρωτόκολλο Tiny-TP πρέπει να εφαρμοστεί ώστε να λειτουργήσει το πρωτόκολλο IrLAN.

IrTran-P

Το πρωτόκολλο IrTran-P επιτρέπει την μετάδοση εικόνων από ψηφιακές φωτογραφικές συσκευές[2][6][7].

### 6.3.4 ΑΛΛΑ ΠΡΟΤΥΠΑ IrDA

IrSimple

Το νέο πρότυπο IrSimple παρέχει ρυθμούς μετάδοσης 4 έως 10 φορές γρηγορότερους από το πρότυπο IrDA, βελτιώνοντας με αυτόν τον τρόπο την αποτελεσματικότητα του. Το μόνο που χρειάζεται για την επίτευξη αυτών των ταχυτήτων είναι αναβάθμιση στο λειτουργικό των συσκευών. Ένα κινητό τηλέφωνο που χρησιμοποιεί αυτό το πρότυπο μπορεί να μεταδώσει μια εικόνα σε ένα δευτερόλεπτο[2].

**Comparison of IrDA protocols**
Transfer times when transferring a 2-megapixel image (approximately 500KB)

| **Protocol:** | IrSimple-4M protocol | IrDA-4M protocol | IrDA-115K protocol |
|---|---|---|---|
| **Physical layer:** | FIR (Fast IrDA) (4 Mbit/s) | FIR (Fast IrDA) (4 Mbit/s) | SIR (serial infrared) (115.2 Kbit/s) |
| **Transfer time (approx.):** | 1 second | 4 to 11 seconds | 50 to 100 seconds |
| (Based on a table from NTT DoCoMo) | | | |

**ΕΙΚΟΝΑ 85: ΠΡΟΤΥΠΟ IrDA**

Το νέο πρότυπο έχει επιτύχει πολύ γρήγορη σύνδεση με υπέρυθρες (Very Fast infrared,VFIR) που φτάνουν ρυθμούς μετάδοσης 16 Mbps και με την σύνδεση ultra fast infrared (UFIR) ρυθμούς μετάδοσης ως 96 Mbps. Αυτοί οι τύποι μετάδοσης δεν υποστηρίζονται από τις συσκευές που έχουν άλλο τύπο μετάδοσης λόγω των περιορισμών του υλικού[2].

IrDA Lite Minimal Protocol

Το IrDA Lite Minimal Protocol Implementation περιλαμβάνει την βελτίωση του IrDA μειώνοντας την πολυπλοκότητα και το μέγεθος του κώδικα.

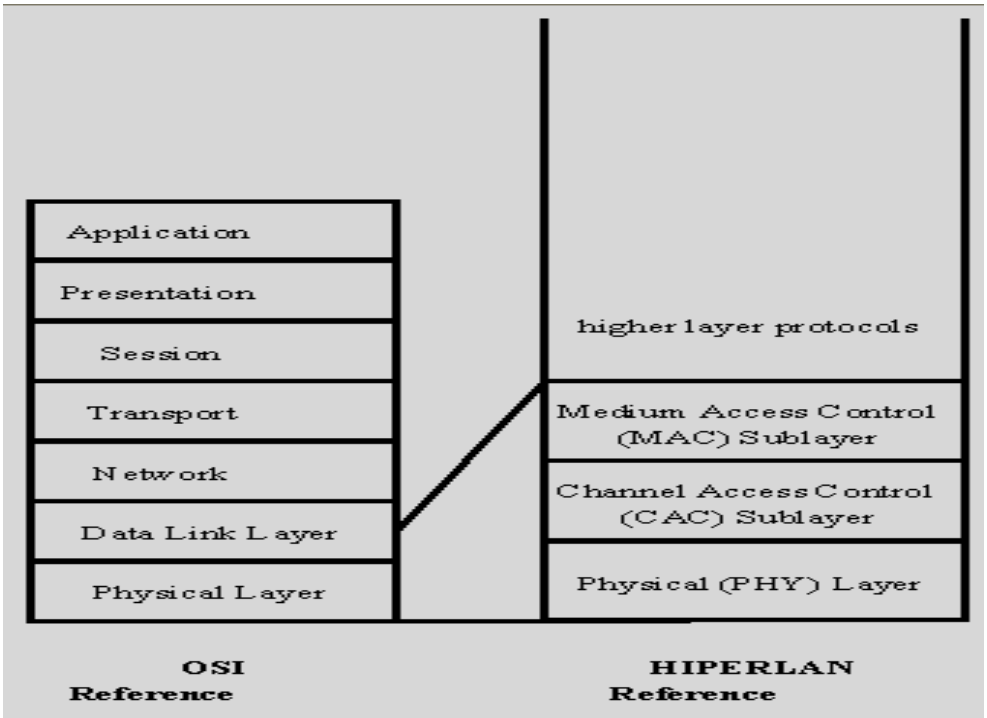
Το IrDA έχει ευρεία χρήση και το έχουν αποδεχτεί παγκοσμίως με αποτέλεσμα να δημιουργούνται νέες προδιαγραφές. Όμως η δημοτικότητα του έχει μειωθεί και οφείλεται στα πρότυπα Bluetooth και wi-fi που είναι πιο βελτιωμένα και δεν χρειάζονται οπτική επαφή[2].

## 6.4 HIPERLAN

Το ασύρματο τοπικό δίκτυο υψηλής απόδοσης (High Performance Radio LAN, HIPERLAN) είναι ένα πρότυπο που δημιουργήθηκε από το Ινστιτούτο Τυποποίησης Ευρωπαϊκών Τηλεπικοινωνιών (ETSI) για την ασύρματη δικτύωση με υψηλές ταχύτητες. Το 1993, το CEPT διακήρυξε τη χρήση των ζωνών 5.15-5.30 GHz και 17.1-17.3 GHz από το πρότυπο HIPERLAN. Με την ολοκλήρωση του προτύπου HIPERLAN 1, το ETSI συγχώνευσε στο πρόγραμμα για τα ευρυζωνικά ραδιοδίκτυα πρόσβασης (BRAN), τις εργασίες για τον ασύρματο βρόχο (Radio Local Loop) και τα ασύρματα δίκτυα, για την δημιουργία προτύπων ενός ασύρματου ATM. Με το πρόγραμμα για τα ευρυζωνικά ραδιοδίκτυα πρόσβασης δημιουργήθηκαν τα πρότυπα HIPERLAN 2, HIPERLAN 3 και HIPERLAN 4 για το ασύρματο ATM[5].

### 6.4.1 ΕΠΙΠΕΔΑ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 1

Το πρότυπο HIPERLAN 1 δημιουργήθηκε για να έχει καλή απόδοση όπως τα ενσύρματα δίκτυα και να υποστηρίζει ισόχρονες υπηρεσίες. Το πρότυπο HIPERLAN 1 δημοσιεύτηκε το 1995, απευθύνεται στο φυσικό επίπεδο και στο υπόστρωμα MAC του μοντέλου OSI, τα οποία περιγράφονται παρακάτω .




**ΕΙΚΟΝΑ 86: ΤΑ ΕΠΙΠΕΔΑ ΤΟΥ ΠΡΟΤΥΠΟΥ OSI ΚΑΙ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 1**

### 6.4.1.1 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 1

Το πρότυπο HIPERLAN 1 λειτουργεί στην ζώνη συχνοτήτων των 5.15-5.3 GHz, ο ρυθμός μετάδοσης των δεδομένων φτάνει τα 23.5 Mbps και η τελική απόσταση είναι στα 50 μέτρα. Χρησιμοποιεί τη διαμόρφωση στενής ζώνης (narrowband) για να επιτύχει μεγαλύτερους ρυθμούς σε σχέση με τις τεχνικές FHSS και DSSS.

Το πρότυπο HIPERLAN 1 χωρίζει το εύρος ζώνης σε πέντε κανάλια. Ο χαμηλότερος ρυθμός μετάδοσης δεδομένων του προτύπου είναι στα 1.47 Mbps, αφορά την μετάδοση πληροφοριών ελέγχου και χρησιμοποιεί τη διαμόρφωση μετατόπιση συχνότητας (FSK). Ο υψηλότερος ρυθμός μετάδοσης δεδομένων είναι στα 23.4 Mbps και χρησιμοποιεί την γκαουσιανή διαμόρφωση ελάχιστης μετατόπισης (Gaussian Minimum Shift Keying) με bandwidth-time, BT=0.3. Τα δεδομένα της βασικής ζώνης φιλτράρονται με ένα φίλτρο Gaussian και το εύρος ζώνης του φίλτρου Gaussian συσχετίζεται με την περίοδο του bit[3][5].

Το φυσικό επίπεδο προσθέτει στη μονάδα MPDU την κεφαλίδα χαμηλού ρυθμού μετάδοσης, 450 bit training υψηλού ρυθμού μετάδοσης που χρησιμοποιούνται για την ισοστάθμιση των καναλιών, 496*n bit υψηλού ρυθμού μετάδοσης που αντιστοιχούν στο ωφέλιμο φορτίο και ένα μεταβλητό πλήθος bit padding. Τα bit

ισοστάθμισης είναι απαραίτητα προκειμένου να υποστηριχθεί ο υψηλός ρυθμός μετάδοσης όταν υπάρχουν διασυμβολικές παρεμβολές. Το πρότυπο δεν καθορίζει την τεχνική ισοστάθμισης, αφήνοντάς τη στην ευχέρεια της εκάστοτε υλοποίησης [5].

### 6.4.1.2 ΤΟ ΥΠΟΣΤΡΩΜΑ MAC ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 1

Στο πρότυπο HIPERLAN 1 οι λειτουργίες ελέγχου πρόσβασης στο μέσο χωρίζονται σε δύο μέρη στο υποεπίπεδο πρόσβασης και ελέγχου του καναλιού (Channel Access and Control,CAC) και στο υποεπίπεδο MAC. Το υποεπίπεδο CAC ελέγχει τη διαθεσιμότητα και την προτεραιότητα του καναλιού για την πρόσβασή του. Το υποεπίπεδο MAC παρέχει τον μηχανισμό δρομολόγησης πολλαπλών διαδρομών, τη μεταφορά δεδομένων στα πρωτόκολλα των υψηλότερων επιπέδων.

Μηχανισμός προτεραιοτήτων και υποστήριξη

Στο πρότυπο HIPERLAN 1 η ανάθεση προτεραιοτήτων πρόσβασης στο κανάλι γίνεται δυναμικά ανάλογα με την διάρκεια ζωής και την προτεραιότητα του MAC πακέτου. Κατά την δημιουργία του πακέτου MAC η διάρκεια ζωής του έχει τιμή από 0 ως 32767 msec και προκαθορισμένη τιμή είναι στα 500 msec. Αν περάσει η διάρκεια ζωής του πακέτου και δεν έχει παραδοθεί τότε το πακέτο απορρίπτεται. Η προτεραιότητα ενός πακέτου MAC περιλαμβάνει τις τιμές από 1 έως 5, όπου στην υψηλότερη προτεραιότητα αντιστοιχεί η τιμή 1 και στην χαμηλότερη η τιμή 5. Η προτεραιότητα πρόσβασης στο κανάλι εξαρτάται από την διάρκεια ζωής που απομένει στο πακέτο και στην προτεραιότητα του.

Το πρωτόκολλο MAC παρέχει τον μηχανισμό EY-NPMA (Elimination Yield-Non-Preemptive Priority Multiple Access). Ο μηχανισμός αυτός περιέχει τρείς φάσεις[5]:

- Την φάση καθορισμού προτεραιοτήτων.
- Την φάση μετάδοσης.
- Την φάση ανταγωνισμού που χωρίζεται στην φάση απαλοιφής και στην φάση υποχώρησης.

Αν ένας σταθμός ανιχνεύσει ότι το μέσο είναι αδρανές για το διάστημα που χρειάζεται για την αποστολή 1700 bit, τότε ο μηχανισμός EY-NPMA επιτρέπει αμέσως στον σταθμό να ξεκινήσει την μετάδοση δεδομένων. Αν το μέσο δεν είναι αδρανές τότε κάθε σταθμός αναμένει μέχρι να γίνει αδρανές. Οι σταθμοί περιμένουν για χρόνο ίσο με την σχισμή συγχρονισμού και έπειτα ξεκινούν οι φάσεις καθορισμού προτεραιοτήτων και την φάση ανταγωνισμού.

Η φάση καθορισμού προτεραιοτήτων περιλαμβάνει από μια ως πέντε χρονικές σχισμές που κάθε μία έχει διάρκεια ίση με την διάρκεια αποστολής 256 bit. Ο σταθμός με αριθμό προτεραιότητας p που θέλει να μεταδώσει, εκπέμπει μια ριπή (burst) στην χρονική σχισμή p+1 αν ήδη δεν έχει ανιχνευτεί ριπή με υψηλότερη προτεραιότητα από άλλο σταθμό. Αν ανιχνευτεί ριπή με υψηλότερη προτεραιότητα απορρίπτονται οι σταθμοί από την διεκδίκηση και περιμένουν την επόμενη σχισμή συγχρονισμού ή μια ελεύθερη χρονική σχισμή διάρκειας 1700 bit (P.Nicopolitidis et all,2005).

Η φάση απαλοιφής έχει ως στόχο την μείωση των ανταγωνιζόμενων σταθμών. Περιέχει από 1 έως 13 σχισμές που κάθε μία έχει διάρκεια ίση με την διάρκεια αποστολής 256 bit. Οι σταθμοί που εκπέμψανε ριπή, στην φάση καθορισμού προτεραιοτήτων, ανταγωνίζονται για την διεκδίκηση του μέσου. Έπειτα εκπέμπουν μια ριπή για ένα γεωμετρικό κατανεμημένο πλήθος σχισμών και «ακούν» το μέσο για μία ακόμα σχισμή. Αν ανιχνεύσουν κάποια άλλη ριπή κατά την διάρκεια της σχισμής αποσύρονται διαφορετικά συνεχίζουν στην φάση υποχώρησης.

Η φάση υποχώρησης περιλαμβάνει έναν σταθμό που απέκτησε πρόσβαση στο μέσο. Η φάση αυτή περιλαμβάνει από 1 έως 15 σχισμές. Κάθε σχισμή έχει διάρκεια όση η διάρκεια αποστολής 64 bit. Οι σταθμοί που απέμειναν περιμένουν για ένα γεωμετρικό κατανεμημένο πλήθος σχισμών ανιχνεύοντας το κανάλι. Ο σταθμός με τον λιγότερο χρόνο αναμονής καταλαμβάνει το μέσο και μεταδίδει. Οι υπόλοιποι περιμένουν την επόμενη σχισμή. Ο μηχανισμός αυτός δεν λύνει το πρόβλημα των «κρυμμένων» κόμβων.

#### 6.4.1.3 ΔΡΟΜΟΛΟΓΗΣΗ ΠΟΛΛΑΠΛΩΝ ΔΙΑΔΡΟΜΩΝ

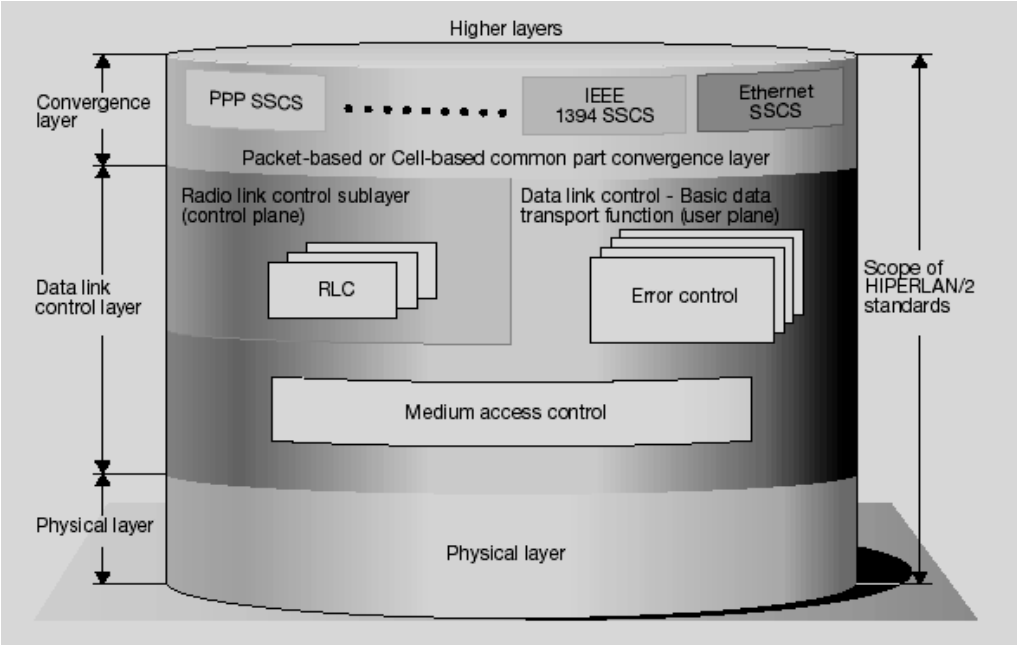
Το πρότυπο HIPERLAN 1 υποστηρίζει τις τοπολογίες υποδομής και τις αδόμητες τοπολογίες, υποστηρίζει την προώθηση πακέτων από ενδιάμεσους

σταθμούς εκτός εμβέλειας. Ένας σταθμός στέλνει τα πακέτα για τον προορισμένο σταθμό εκτός εμβέλειας, σε έναν γειτονικό του σταθμό. Ο σταθμός που παρέλαβε αυτά τα πακέτα τα αναμεταδίδει στον γειτονικό του μέχρι τα πακέτα να φτάσουν στον τελικό προορισμό τους. Υπάρχει η δυνατότητα ένας σταθμός να μην είναι διαμεσολαβητής αλλά θα πρέπει να γνωρίζει τους γειτονικούς σταθμούς. Οι διαμεσολαβητές πρέπει να γνωρίζουν την τοπολογία του δικτύου και να έχουν μια δυναμική βάση δεδομένων δρομολόγησης.

### 6.4.2 ΕΠΙΠΕΔΑ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 2

Το πρότυπο HIPERLAN 2 χρησιμοποιείται για τα ασύρματα δίκτυα και αλληλεπιδρά με πολλά διαφορετικά είδη δικτύων όπως το ATM, το Ethernet και το UMTS. Το πρότυπο χρησιμοποιεί την τεχνική OFDM στην ζώνη συχνοτήτων 5 GHz και οι ρυθμοί μετάδοσής του φτάνουν τα 54 Mbps. Το εύρος ζώνης, του προτύπου αυτού, χωρίζεται σε 19 κανάλια των 20 MHz. Επίσης, το σημείο πρόσβασης χρησιμοποιεί την TDMA/TDD. Επιπλέον, το πρότυπο HIPERLAN 2 χρησιμοποιεί την DFS (Dynamic Frequency Selection) για την αποφυγή παρεμβολών και τον εύκολο διαμοιρασμό συχνοτήτων. Υποστηρίζει την κινητικότητα των σταθμών μεταξύ διαφορετικών κυψελών χωρίς να χάνεται η σύνδεση.

Το πρότυπο HIPERLAN 2 είναι connection-oriented για την υποστήριξη QoS υπηρεσιών. Το connection-oriented σημαίνει ότι πρώτα εγκαθιδρύονται οι συνδέσεις των Access Point και μετά γίνονται οι μεταδόσεις. Το πρότυπο αυτό λειτουργεί σε δύο τύπους δικτύων, το bi-directional με point-to-point συνδέσεις και το unidirectional με point-to-multipoint συνδέσεις. Η διαστρωμάτωση του προτύπου αυτού περιλαμβάνει το φυσικό επίπεδο, το επίπεδο ζεύξης δεδομένων, το επίπεδο σύγκλισης και τα υπόλοιπα υψηλότερα επίπεδα του μοντέλου OSI. Το επίπεδο ζεύξης χωρίζεται στο υπόστρωμα MAC, το υποεπίπεδο Data Control Link και το υποεπίπεδο Radio Link Control. Το επίπεδο σύγκλισης περιλαμβάνει την υποστήριξη πολλών ενσύρματων δικτύων που κάθε ένα έχει διαφορετικό επίπεδο σύγκλισης.




**ΕΙΚΟΝΑ 87: ΔΙΑΣΤΡΩΜΑΤΩΣΗ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 2**

## 6.4.2.1 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 2

Το πρότυπο HIPERLAN 2 χρησιμοποιεί την τεχνική OFDM όπως προαναφέρθηκε με διαφορετικές διαμορφώσεις ανάλογα με τους ρυθμούς μετάδοσης.

Transmission rates for various modulation/coding modes

| MODULATION FORMAT | CODING RATE, R | NOMINAL BIT RATE (Mb/s) |
|---|---|---|
| BPSK | 1/2 | 6 |
| BPSK | 3/4 | 9 |
| QPSK | 1/2 | 12 |
| QPSK | 3/4 | 18 |
| 16QAM | 9/16 | 27 |
| 16QAM | 3/4 | 36 |
| 64QAM | 3/4 | 54 (optional) |

**ΕΙΚΟΝΑ 88: ΤΥΠΟΙ ΔΙΑΜΟΡΦΩΣΗΣ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 2**

## 6.4.2.2 ΤΟ ΣΤΡΩΜΑ ΖΕΥΞΗΣ ΚΑΙ ΔΕΔΟΜΕΝΩΝ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 2

Το πρότυπο HIPERLAN 2 περιέχει το πρωτόκολλο MAC χρησιμοποιώντας την τεχνική TDMA και την TDD για την πρόσβαση στο μέσο, το πρωτόκολλο Error Control που ευθύνεται για την αξιόπιστη μετάδοση και το πρωτόκολλο Radio Link Control που περιέχει τρεις βασικές λειτουργίες. Οι λειτουργίες αυτές είναι η Radio

Resource Control που διαχειρίζεται τις διαθέσιμες συχνότητες, η Association Control που ελέγχει την διανομή των σταθμών στα Access Points και η DLC Connection Control (DCC) που ελέγχει την εγκαθίδρυση και τον τερματισμό της σύνδεσης[11].

#### 6.4.2.3 ΤΟ ΕΠΙΠΕΔΟ ΣΥΓΚΛΙΣΗΣ ΤΟΥ ΠΡΟΤΥΠΟΥ HIPERLAN 2

Το επίπεδο σύγκλισης του προτύπου HIPERLAN 2 προσαρμόζει τις λειτουργίες των υψηλότερων επιπέδων για την μεταφορά στο υποεπίπεδο Ελέγχου Σύνδεσης δεδομένων και την τροποποίηση των πακέτων από τα υψηλότερα επίπεδα σε σταθερού μεγέθους πακέτα για το υποεπίπεδο Ελέγχου Σύνδεσης δεδομένων. Το επίπεδο σύγκλισης διαιρείται σε δύο μέρη, στο packet-based που χρησιμοποιούν πακέτα άλλων δικτύων και στο cell-based που χρησιμοποιούν τα πακέτα του ATM cell[11]. Τα HIPERLAN 3 και HIPERLAN 4 είναι βελτιώσεις του HIPERLAN 2

### 6.4.3 HIPERLAN 3

Το πρότυπο HIPERLAN 3 που ονομάζεται και αλλιώς HIPERACCESS χρησιμοποιεί συνδέσεις για απομακρυσμένη πρόσβαση. Η μέγιστη απόστασή του φτάνει τα 5 Km, χρησιμοποιεί την ζώνη συχνοτήτων των 5 GHz και φτάνει ρυθμούς μετάδοσης έως 25 Mbps[3][5].

### 6.4.4 HIPERLAN 4

Το πρότυπο HIPERLAN 4 που ονομάζεται και HIPERLINK παρέχει την σύνδεση μεταξύ του HIPERLAN 2 και του HIPERACCESS για την δημιουργία ενός Broadband Δικτύου. Το πρότυπο HIPERLINK λειτουργεί στη ζώνη συχνοτήτων των 17 GHz, ο ρυθμός μετάδοσης του φτάνει τα 155 Mbps στα 150 μέτρα και χρησιμοποιεί point-to-point διασυνδέσεις[3][5].

## 6.5 BLUETOOTH

Η τεχνολογία Bluetooth δημιουργήθηκε από την Ομάδα Ειδικών Ενδιαφερόντων (Special Interest Group,SIG) για την ασύρματη διασύνδεση πολλών υπολογιστικών και επικοινωνιακών συσκευών μικρής εμβέλειας, με χαμηλό κόστος και χαμηλή ισχύ[10]. Το 1999 η Ομάδα Ειδικών Ενδιαφερόντων δημοσίευσε τη προδιαγραφή για την έκδοση 1.0 της τεχνολογίας Bluetooth[9]. Η τεχνολογία αυτή αφορά την ασύρματη δικτύωση του Δικτύου Προσωπικής Περιοχής, το οποίο

σχετίζεται με ένα ολοκληρωμένο σύστημα από το φυσικό επίπεδο έως το επίπεδο εφαρμογών.

Η ομάδα εργασίας IEEE 802.15 ενδιαφερόταν για τη δημιουργία προτύπων για τα Ασύρματα Προσωπικά Δίκτυα και υιοθέτησε την προδιαγραφή της τεχνολογίας Bluetooth και άρχισε να την τροποποιεί για να δημιουργήσει ένα κοινό πρότυπο. Το πρότυπο που τυποποίησε η ομάδα εργασίας IEEE 802.15 περιλαμβάνει μόνο το φυσικό επίπεδο και το επίπεδο Ζεύξης Δεδομένων και τα υπόλοιπα επίπεδα περιλαμβάνονται από το μοντέλο OSI. Το 2002 η ομάδα εργασίας δημοσίευσε το πρώτο πρότυπο IEEE 802.15.1 για τα Ασύρματα Προσωπικά Δίκτυα που αφορούσε την τεχνολογία Bluetooth. Παρακάτω παρουσιάζεται το λογότυπο του προτύπου αυτού.

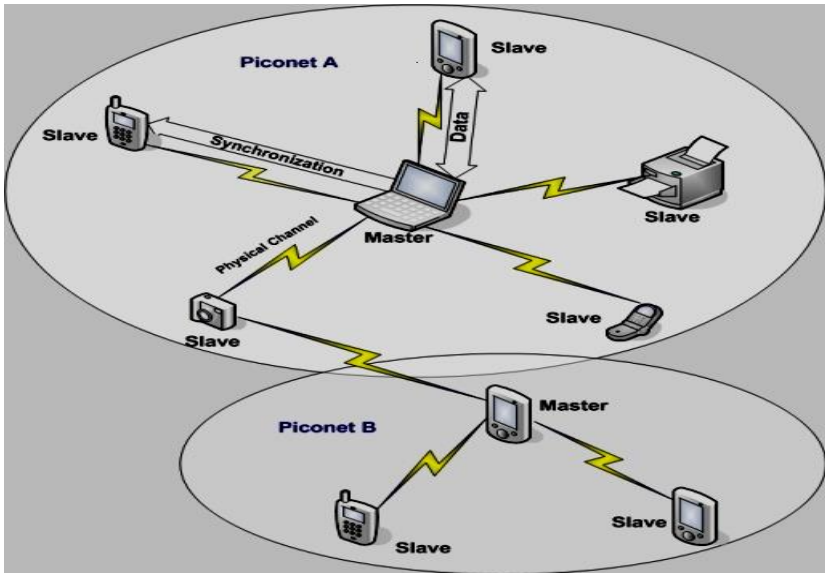

**ΕΙΚΟΝΑ 89: ΛΟΓΟΤΥΠΟ BLUETOOTH**

Το Bluetooth χρησιμοποιεί την ISM ζώνη συχνοτήτων των 2.4 GHz, ο ρυθμός μετάδοσης δεδομένων αγγίζει τα 3 Mbps (έκδοση 2.0 EDR). Στην έκδοση Bluetooth 1.2 χρησιμοποιεί την διαμόρφωση GFSK για ρυθμό μετάδοσης δεδομένων των 1 Mbps, για την έκδοση Bluetooth 2.0 χρησιμοποιεί την διαμόρφωση π/4-DQPSK για ρυθμό μετάδοσης δεδομένων των 2 Mbps και την διαμόρφωση 8-DPSK για ρυθμό μετάδοσης δεδομένων των 3 Mbps. Η εμβέλεια κυμαίνεται στα 91,44 μέτρα με μέγιστη ισχύ 100 mW, στα 10 μέτρα με μέγιστη ισχύ 2.5 mW και στο 1 μέτρο με μέγιστη ισχύ 1 mW[6].

Το εύρος ζώνης, που χρησιμοποιεί το πρότυπο αυτό, περιέχει 79 κανάλια με εύρος 1 MHz το καθένα. Κάθε μεταπήδηση συχνότητας αντιστοιχεί μια σχισμή με μήκος 0.625 msec. Το Bluetooth χρησιμοποιεί FHSS με αλλαγή συχνότητας 1600hops/sec για την αποφυγή παρεμβολών. Οι προδιαγραφές του προτύπου περιλαμβάνουν την στοίβα πρωτοκόλλων, η οποία παρουσιάζεται μετά την τοπολογία[3][8].

### 6.5.1 ΤΟΠΟΛΟΓΙΑ BLUETOOTH

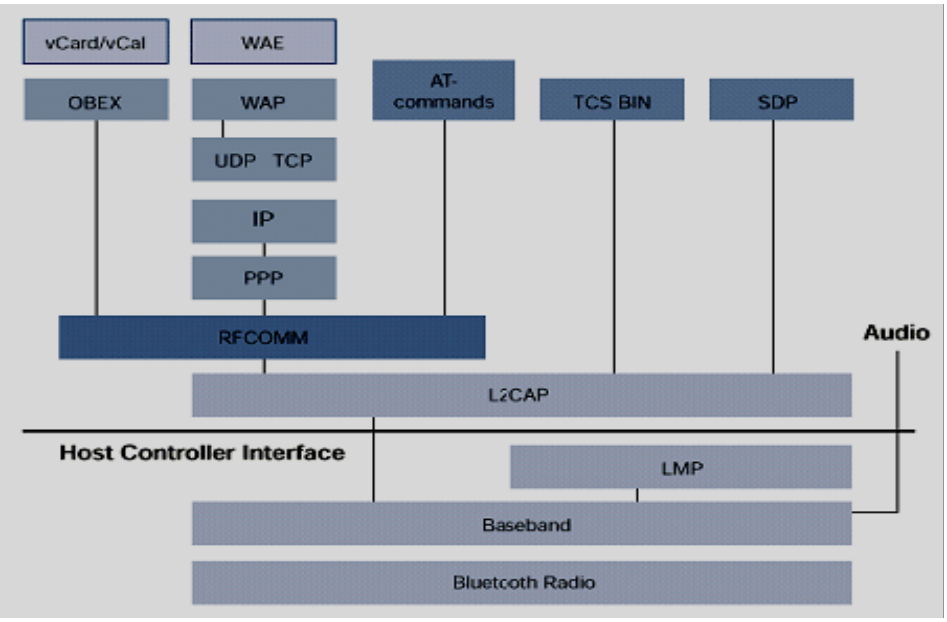
Η επικοινωνία βασίζεται στα ad-hoc δίκτυα και έχει ως αποτέλεσμα το πρωτόκολλο να ορίζει μηχανισμούς και μηνύματα ώστε οι συσκευές Bluetooth να ανακαλύπτουν η μία την άλλη και να εγκαθιδρύονται οι συνδέσεις. Στο Bluetooth χρησιμοποιείται ένα μικροσκοπικό δίκτυο (piconet), το οποίο περιέχει μία συσκευή master και μέχρι εφτά slave συσκευές Bluetooth σε κοντινή απόσταση. Μία συσκευή μπορεί να είναι slave σε ένα μικροσκοπικό δίκτυο και master σε ένα άλλο μικροσκοπικό δίκτυο. Οι συσκευές μπορούν να παίρνουν είτε τον ένα ρόλο (master) είτε τον άλλο ρόλο (slave). Το διάσπαρτο δίκτυο (scatternet) περιλαμβάνει πολλά μικροσκοπικά δίκτυα.




**ΕΙΚΟΝΑ 90: BLUETOOTH SCATTERNET**

Στο δίκτυο, εκτός από τις εφτά ενεργές συσκευές slaves μπορούν να υπάρχουν κι άλλες συσκευές οι οποίες είναι σταθμευμένες (parked). Ο master για να έχει εξοικονόμηση ισχύς μετατρέπει τις συσκευές από ενεργές σε σταθμευμένες. Οι σταθμευμένες συσκευές απλά «κοιμούνται». Υπάρχουν και άλλες δύο καταστάσεις η hold και η sniff. Στην κατάσταση hold οι συσκευές «ακούν» και περιμένουν από τον master ένα σήμα ενεργοποίησης. Στη sniff κατάσταση οι συσκευές slave αποδέχονται τα μηνύματα του master μόνο σε συγκεκριμένες χρονικές στιγμές και την υπόλοιπη διάρκεια «κοιμούνται»[3][8].

## 6.5.2 ΤΑ ΕΠΙΠΕΔΑ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ BLUETOOTH




ΕΙΚΟΝΑ 91: ΣΤΟΙΒΑ ΠΡΟΤΩΚΟΛΛΩΝ ΤΟΥ BLUETOOTH

Τα επίπεδα των πρωτοκόλλων του Bluetooth παρουσιάζονται παρακάτω[3][5][6]:

Επίπεδο ραδιοεκπομπής

Το επίπεδο ραδιοεκπομπής περιλαμβάνει όλα τα χαρακτηριστικά και τη χρήση τους για την φυσική ασύρματη σύνδεση.

Επίπεδο βασικής ζώνης

Το επίπεδο ζώνης περιλαμβάνει τις αρμοδιότητες για τη λειτουργία των συνδέσεων, τη διαμόρφωση των πλαισίων, τον έλεγχο ροής, την πραγματοποίηση ζεύξης και τις διαδικασίες συγχρονισμού.

Επίπεδο διαχείρισης ζεύξης

Στο επίπεδο διαχείρισης ζεύξης χρησιμοποιείται το πρωτόκολλο διαχείρισης σύνδεσης (Link Management Protocol, LMP), το οποίο διαχειρίζεται τις καταστάσεις συνδέσεων και την διαχείριση ισχύος.

Επίπεδο λογικής ζεύξης και προσαρμογής

Το επίπεδο λογικής ζεύξης και προσαρμογής (Logical Link And Adaptation Layer, L2CAP) μετατρέπει τα δεδομένα που έχουν ληφθεί από τα παραπάνω

επίπεδα και παρέχει connection-oriented, connectionless υπηρεσίες, λειτουργίες πολύπλεξης πρωτοκόλλων, λειτουργίες κατάτμησης και επανασυναρμολόγησης των πακέτων δεδομένων. Η μεταφορά δεδομένων ήχου δεν υποστηρίζονται από το L2CAP και έτσι μεταβιβάζονται στο επίπεδο βασικής ζώνης. Το L2CAP υποστηρίζει μόνο μεταφορά δεδομένων.

Επίπεδο εντοπισμού υπηρεσιών

Στο επίπεδο εντοπισμού υπηρεσιών χρησιμοποιείται το πρωτόκολλο ανακάλυψης υπηρεσιών (Service Discovery Protocol,). Το SDP χρησιμοποιείται για την ενημέρωση συσκευών για τις προσφερόμενες υπηρεσίες και την πληροφόρηση των γειτονικών συσκευών.

Επίπεδο RFCOMM

Στο επίπεδο RFCOMM χρησιμοποιείται το πρωτόκολλο προσομοίωσης ελέγχου σειριακής γραμμής RS-232 και σηματοδοσίας δεδομένων που εξομοιώνει την σειριακή θύρα των υπολογιστών για την σύνδεση ασύρματων πληκτρολογίων και άλλα.

Επίπεδο TCS

Το επίπεδο TCS παρέχει την κατάλληλη σηματοδοσία για την εγκαθίδρυση και τον τερματισμό μιας σύνδεσης κλήσεων έλεγχο των συνδέσεων.

Διάφορα επίπεδα

Στα επόμενα επίπεδα περιέχονται πρωτόκολλα που δεν καθορίζονται για το Bluetooth αλλά χρησιμοποιούνται για την λειτουργία των εφαρμογών των υψηλών επιπέδων.

Η διασύνδεση ελεγκτή υπολογιστή υπηρεσίας

Η διασύνδεση ελεγκτή υπολογιστή υπηρεσίας (Host Controller, HCI) παρέχει την διασύνδεση του λογισμικού και του υλικού του Bluetooth και δεν αποτελεί επίπεδο στη στοίβα.

## 6.5.3 ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΡΟΦΙΛ ΤΟΥ BLUETOOTH

Οι εφαρμογές του Bluetooth χωρίζονται σε 13 προφίλ (Bluetooth 1.1) στα οποία χρησιμοποιούνται συγκεκριμένα πρωτόκολλα. Τα προφίλ υποστηρίζονται μεταξύ τους και για τη δημιουργία κάποιων προφίλ υλοποιούνται κάποια άλλα. Η ύπαρξη των προφίλ εφαρμογών στοχεύει στη διαλειτουργικότητα των συσκευών Bluetooth. Τα προφίλ των εφαρμογών παρουσιάζονται παρακάτω[4][8]:

Προφίλ γενικής πρόσβασης

Το προφίλ γενικής χρήσης είναι προφίλ συστήματος και είναι υποχρεωτικό για κάθε συσκευή γιατί περιλαμβάνει λειτουργίες που χρειάζονται τα άλλα προφίλ. Το προφίλ αυτό είναι υπεύθυνο για τη διαχείριση των συνδέσεων.

Προφίλ εφαρμογής ανακάλυψης υπηρεσιών

Το προφίλ εφαρμογής ανακάλυψης υπηρεσιών είναι και αυτό προφίλ συστήματος, παρέχει στους χρήστες την πρόσβαση στο πρωτόκολλο ανακάλυψης υπηρεσιών για την πληροφόρηση των υποστηριζόμενων εφαρμογών μιας συσκευής. Το προφίλ αυτό είναι προαιρετικό και αν δεν χρησιμοποιείται η πρόσβαση στο πρωτόκολλο γίνεται μόνο από εφαρμογές.


**ΕΙΚΟΝΑ 92: ΣΥΣΚΕΥΕΣ ΜΕ BLUETOOTH**

Προφίλ σειριακής θύρας

Το προφίλ σειριακής θύρας είναι προφίλ συστήματος και χρησιμοποιεί το πρωτόκολλο RFCOMM.

Προφίλ ενδοεπικοινωνίας

Στο προφίλ ενδοεπικοινωνίας υποστηρίζονται οι μεταδόσεις φωνής μεταξύ των συσκευών Bluetooth που είναι εντός εμβέλειας.

Προφίλ ασύρματης τηλεφωνίας

Το προφίλ ασύρματης τηλεφωνίας υποστηρίζει την ενδοεπικοινωνία ενός τηλεφώνου συμβατού με το Bluetooth ως ασύρματου ή ως κινητού τηλεφώνου.

Προφίλ ακουστικών και μικροφώνων

Το προφίλ ακουστικών και μικροφώνων χρησιμοποιεί το προφίλ σειριακής θύρας για την υποστήριξη συνδέσεων μεταξύ κινητών τηλεφώνων και ασύρματων ακουστικών και μικροφώνων.

Προφίλ φαξ

Το προφίλ φαξ χρησιμοποιεί το προφίλ σειριακής θύρας και επιτρέπει την αποστολή φαξ από τους υπολογιστές μέσω του κινητού τηλεφώνου.

Προφίλ δικτύωσης μέσω τηλεφώνου

Το προφίλ δικτύωσης μέσω τηλεφώνου χρησιμοποιεί το προφίλ σειριακής θύρας για την υποστήριξη τηλεφωνικών συνδέσεων από ένα φορητό υπολογιστή μέσω κινητών τηλεφώνων.

Προφίλ πρόσβασης σε τοπικό δίκτυο

Το προφίλ πρόσβασης σε τοπικό δίκτυο επιτρέπει στις συσκευές Bluetooth να συνδέονται με τοπικά δίκτυα μέσω των σημείων πρόσβασης.

Προφίλ μεταφοράς αρχείων

Το προφίλ μεταφοράς αρχείων υποστηρίζει μεταφορά αρχείων μεταξύ των συσκευών Bluetooth.

Προφίλ γενικής ανταλλαγής αντικειμένων

Το προφίλ γενικής ανταλλαγής αντικειμένων είναι προφίλ συστήματος και καθορίζει τις λειτουργίες ώστε να μπορούν οι συσκευές Bluetooth να υποστηρίζουν ανταλλαγή αντικειμένων.

Προφίλ προώθησης αντικειμένων

Το προφίλ προώθησης αντικειμένων είναι υπεύθυνο για την προώθηση αντικειμένων. Για παράδειγμα η διανομή διαφημίσεων.

Προφίλ συγχρονισμού

Το προφίλ συγχρονισμού παρέχει τον αυτόματο συγχρονισμό δεδομένων μεταξύ των συσκευών. Για παράδειγμα μια συσκευή PDA επιτρέπεται να συγχρονίζεται με έναν άλλον υπολογιστή.

## 6.6 ΣΥΝΟΨΗ

Σε αυτό το κεφάλαιο παρουσιάστηκαν οι τεχνολογίες HomeRF, IrDA, Bluetooth και HIPERLAN για την ασύρματη δικτύωση. Στο επόμενο κεφάλαιο παρουσιάζεται η τεχνολογία WiMAX.

# 7. ΤΕΧΝΟΛΟΓΙΑ WiMAX

## 7.1 ΕΙΣΑΓΩΓΗ

Στο προηγούμενο κεφάλαιο αναπτύχθηκαν οι τεχνολογίες των ασύρματων προσωπικών και τοπικών δικτύων. Σε αυτό το κεφάλαιο θα αναπτυχθεί η τεχνολογία WiMAX που αφορά τα ασύρματα μητροπολιτικά δίκτυα. Το WiMAX (World Interoperability for Microwave Access) δεν είναι πρότυπο αλλά ένα εμπορικό όνομα που αναφέρεται στα πιστοποιημένα προϊόντα του WiMAX Forum, όπως είναι τα πιστοποιημένα προϊόντα Wi-Fi της Wi-Fi Alliance. Το WiMAX Forum είναι ένας μη κερδοσκοπικός οργανισμός που πιστοποιεί κάθε σύστημα και κάθε εφαρμογή που χρησιμοποιεί το πρότυπο 802.16[5].

ΕΙΚΟΝΑ 93: ΛΟΓΟΤΥΠΟ ΤΟΥ WiMAX FOROUM

Το πρότυπο IEEE 802.16 δημιουργήθηκε από την ομάδα εργασίας IEEE και αφορά την ασύρματη πρόσβαση ευρείας ζώνης. Το πρότυπο IEEE 802.16 είχε ως στόχο την ασύρματη πρόσβαση ευρείας ζώνης για σταθερά συστήματα (Fixed WiMAX). Μετά τη δημιουργία και άλλων προτύπων IEEE 802.16, το πρότυπο IEEE 802.16 παρέχει ασύρματη πρόσβαση ευρείας ζώνης και για κινητά συστήματα (Mobile WiMAX). Τα πρότυπα IEEE 802.16 θα παρουσιαστούν παρακάτω αφού πρώτα περιγραφεί το πρότυπο για την ασύρματη πρόσβαση ευρείας ζώνης για σταθερά συστήματα.

Το πρότυπο IEEE 802.16 εκτείνεται στη ζώνη συχνοτήτων των 2-66 GHz και οι αποστάσεις που προσφέρει πλησιάζουν τα 50 Km. Το πρότυπο IEEE 802.16 χρησιμοποιεί κυρίως point-to-multipoint συνδέσεις και λιγότερο point-to-point. Επίσης, χρησιμοποιεί τη διαμόρφωση OFDM. Ο ρυθμός μετάδοσης πλησιάζει τα

72 Mbps στον αέρα, ενώ ο πραγματικός ρυθμός μετάδοσης στο Ethernet πλησιάζει τα 50 Mbps, ικανοποιώντας τους απαιτητικούς χρήστες και παρέχοντας μια εναλλακτική λύση για τους συνδρομητές.

Χρήσεις WiMAX

Η τεχνολογία WiMAX με τις μεγάλες αποστάσεις που καλύπτει και τους μεγάλους ρυθμούς μετάδοσης που παρέχει, έχει τις παρακάτω βασικές χρήσεις:

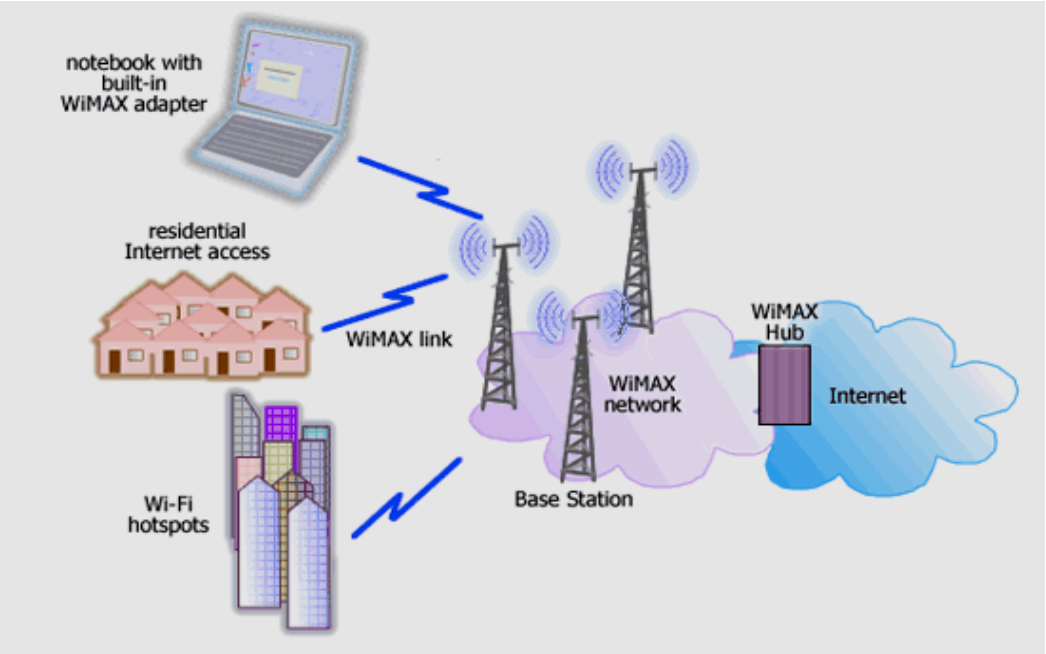
- **Broadband on Demand**: Χρησιμοποιείται στην τεχνολογία αυτή για εφαρμογές πραγματικού χρόνου, παρέχοντας υψηλούς ρυθμούς μετάδοσης σε μεγάλες αποστάσεις.
- **Δίκτυο κορμού στα κυψελωτά συστήματα κινητής τηλεφωνίας**: Παρέχει καλύτερη αξιοπιστία και υψηλούς ρυθμούς μετάδοσης για τα δίκτυα κορμού των κινητών δικτύων επικοινωνιών. Επίσης, μειώνει σημαντικά το κόστος διάδοσης των δικτύων κινητής τηλεφωνίας από την χρήση της οπτικής ίνας και
- **Παρέχει κάλυψη σε απομακρυσμένες περιοχές**: Χρησιμοποιείται σαν εναλλακτική λύση για την αντικατάσταση ή την μερική αντικατάσταση της οπτικής ίνας, της οποίας το κόστος εγκατάστασης είναι πολύ υψηλό.

## 7.2 ΤΟΠΟΛΟΓΙΑ WiMAX

Στην τοπολογία των σταθερών συστημάτων για την ασύρματη πρόσβαση ευρείας ζώνης υπάρχουν δύο βασικά δομικά στοιχεία ο σταθμός βάσης (Base Station,BS) WiMAX και ο σταθμός συνδρομητή (Subscriber Station, SS). Ο σταθμός βάσης αποτελείται από ηλεκτρονικές συσκευές (αναμεταδότη, δρομολογητή) και πύργους WiMAX, που είναι οι κεραίες. Ο σταθμός βάσης είναι υπεύθυνος για τη διανομή του σήματος στην εκάστοτε περιοχή που καλύπτει. Ο σταθμός βάσης διαχειρίζεται τις αιτήσεις πρόσβασης των σταθμών συνδρομητών και τη δρομολόγηση των δεδομένων στον σταθμό βάσης ή στο δίκτυο του παροχέα (backbone).

Ο σταθμός συνδρομητή που υποστηρίζει το WiMAX εξυπηρετεί είτε έναν χρήστη είτε πολλούς χρήστες. Οι χρήστες πρέπει να διαθέτουν τον κατάλληλο εξοπλισμό, όπως μια κάρτα PCMCIA για τον σταθερό υπολογιστή ή να είναι ενσωματωμένο στον φορητό υπολογιστή και ένα δρομολογητή για τους χρήστες που βρίσκονται

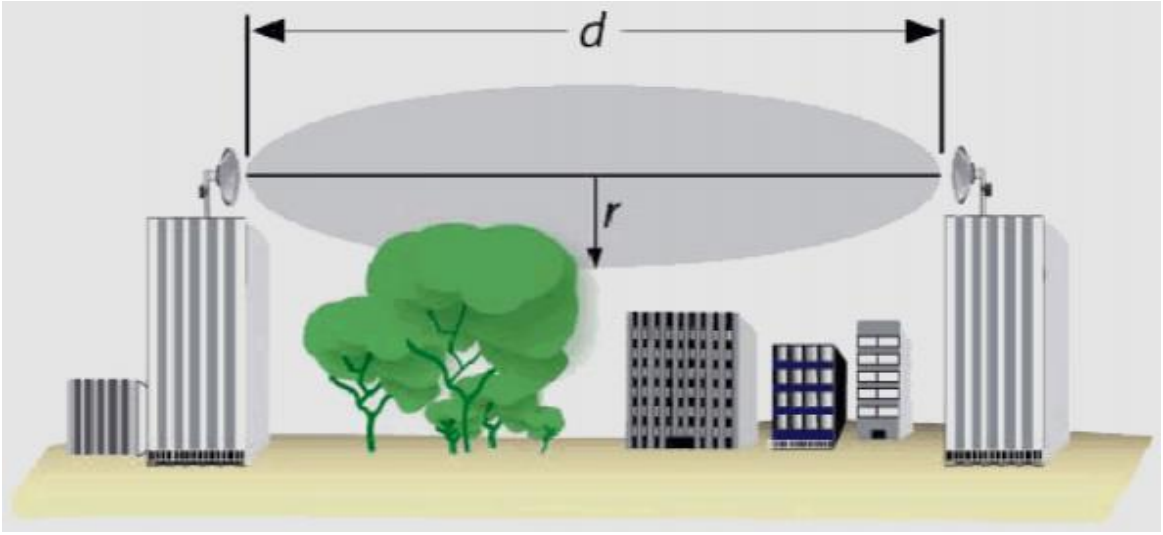
στον ίδιο χώρο. Για μεγαλύτερη κάλυψη χρησιμοποιείται στο μέρος του συνδρομητή μια κατευθυντική κεραία.




**ΕΙΚΟΝΑ 94: FIXED WiMAX**

Οι συνδέσεις μεταξύ του σταθμού βάσης και του σταθμού συνδρομητή είναι είτε point-to-multipoint είτε point-to-point με οπτική επαφή αν υπάρχει μόνο ένας σταθμός συνδρομητή. Ο σταθμός βάσης που συνδέεται point-to-point με τον σταθμό συνδρομητή χρησιμοποιεί κεραία στενότερης δέσμης για την κάλυψη μεγαλύτερων αποστάσεων των 50 Km και ρυθμό μετάδοσης 72 Mbps.

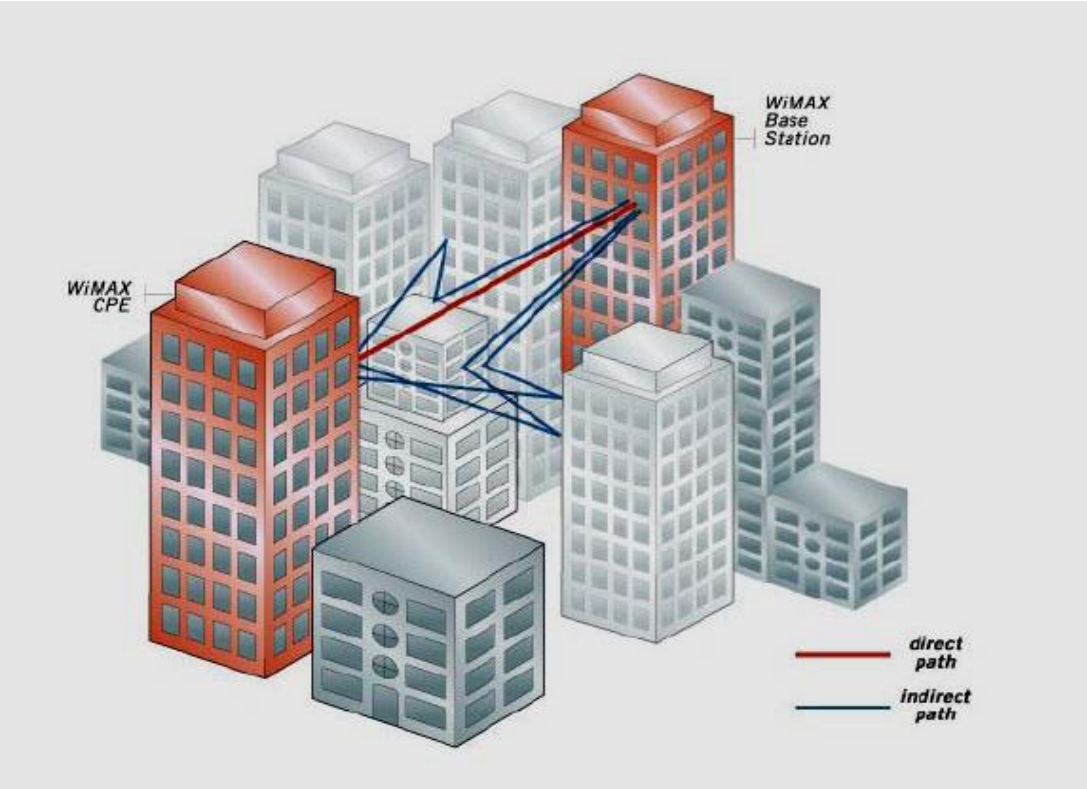
Υπάρχουν δύο τρόποι υπηρεσίας για την ζεύξη σημείων, η οπτική επαφή (Line of Site, LOS) και η μη-οπτική επαφή (Non Light of Site). Στον τύπο υπηρεσίας με οπτική επαφή υπάρχει μία σταθερή κατευθυντική κεραία σε ένα ύψωμα στον σταθμό συνδρομητή, ο οποίος κοιτάζει άμεσα έναν πύργο WiMAX με την προϋπόθεση ότι δε θα υπάρχουν εμπόδια μεταξύ τους όπως κτίρια, δέντρα και λόφοι ώστε το σήμα να μη δέχεται ανακλάσεις.




**ΕΙΚΟΝΑ 95: FRESNEL ZONE CLEARANCE (ΟΠΤΙΚΗ ΕΠΑΦΗ)**

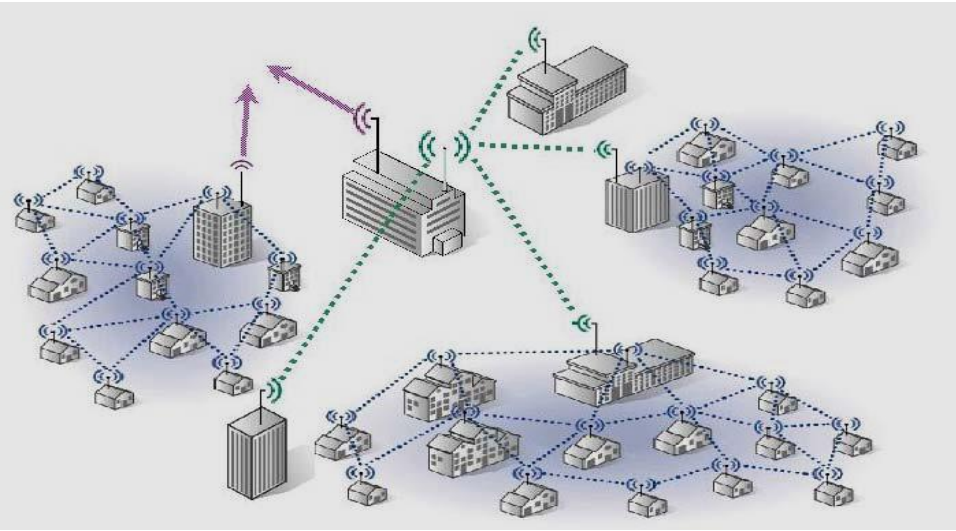
Η ζώνη Fresnel η οποία δεν πρέπει να περιέχει εμπόδια (Fresnel Clearance), καλύπτει τη ζώνη μεταξύ της κεραίας του σταθμού συνδρομητή και του πύργου WiMAX και εξαρτάται από τη συχνότητα του σήματος και τη διάμετρο της απόστασης των δύο κεραιών. Η εκπομπή οπτικής επαφής χρησιμοποιεί συχνότητες έως 66 GHz και επειδή η σύνδεση είναι σταθερή μεταδίδονται περισσότερα δεδομένα χωρίς να υπάρχουν λάθη.

Στον τύπο υπηρεσίας με μη-οπτική επαφή υπάρχει μια κεραία στον υπολογιστή που συνδέεται με τον πύργο WiMAX, σε συχνότητες από 2 έως 11 GHz όπου με τη χρήση της κυψελωτής ακτίνας φτάνει τα 8 Km. Το κόστος της υπηρεσίας αυτής είναι χαμηλότερο από την υπηρεσία οπτικής επαφής γιατί δεν χρειάζονται αυστηρές σχεδιαστικές απαιτήσεις ούτε περιορισμοί του ύψους της κεραίας. Στην υπηρεσία αυτή, οι εκπομπές με μικρότερο μήκος κύματος, δεν διακόπτονται εύκολα από φυσικά εμπόδια όπως δέντρα και μικρά κτίρια, αφού μπορούν να διαθλαστούν και να παρακάμψουν τα εμπόδια.




**ΕΙΚΟΝΑ 96: ΔΙΑΔΟΣΗ ΜΗ - ΟΠΤΙΚΗΣ ΕΠΑΦΗΣ**

Εκτός από την τοπολογία των συνδέσεων point-to-multipoint χρησιμοποιείται και η τοπολογία πολυγωνικής δικτύωσης ή πλεγματική (mesh topology). Στην τοπολογία πολυγωνικής δικτύωσης, όταν δεν υπάρχει άμεση επικοινωνία για την αναμετάδοση του πακέτου ή όταν η αναμετάδοση του πακέτου είναι αποδοτικότερη, οι σταθμοί συνδρομητή μπορούν να έχουν είτε τον ρόλο του αποστολέα είτε τον ρόλο του παραλήπτη.



**ΕΙΚΟΝΑ 97: ΠΟΛΥΓΩΝΙΚΗ ΔΙΚΤΥΩΣΗ**

Στην πολυγωνική δικτύωση υπάρχουν κόμβοι, όπου ένας από αυτούς γίνεται ο Mesh σταθμός βάσης και οι άλλοι Mesh σταθμοί συνδρομητή, στην περίπτωση όπου η πολυγωνική δικτύωση έχει άμεση σύνδεση με ένα backhaul δίκτυο. Όλοι οι κόμβοι της πολυγωνικής δικτύωσης πρέπει να συντονίσουν την εκπομπή τους στους hop-to-hop γείτονές τους και να εκπέμπουν broadcast πληροφορίες σε όλους τους γειτονικούς κόμβους[3].

## 7.3 ΠΡΟΤΥΠΑ IEEE 802.16

### 7.3.1 Αρχικό IEEE 802.16

Το αρχικό πρότυπο IEEE 802.16 εγκρίθηκε το 2001. Λειτουργούσε στη ζώνη συχνοτήτων από 10 έως 66 GHz και οι σταθμοί έπρεπε να βρίσκονται σε οπτική επαφή.

### 7.3.2 IEEE 802.16 a

Η ομάδα εργασίας αποφάσισε να στραφεί στη ζώνη συχνοτήτων από 2 έως 11 GHz, όπου οι σταθμοί δε θα χρειαζόταν να έχουν οπτική επαφή. Το πρότυπο IEEE 802.16a είχε το πλεονέκτημα του χαμηλότερου κόστους υλοποίησης και απευθυνόταν στην ασύρματη πρόσβαση σταθερών συστημάτων .

### 7.3.3 IEEE 802.16 b

Το πρότυπο IEEE 802.16 b αφορά τις μη-αδειοδοτημένες ζώνες συχνοτήτων των 5 GHz και παρέχει υπηρεσίες ποιότητας (QoS), ώστε να υπάρχει προτεραιότητα στη μετάβαση πραγματικού χρόνου εικόνας και ήχου. Επίσης, παρέχει διαφορετικά επίπεδα υπηρεσίας σε διαφορετικού τύπου μετάδοση δεδομένων.

### 7.3.4 IEEE 802.16 c

Το πρότυπο IEEE 802.16 c είναι η αναβάθμιση του αρχικού προτύπου IEEE 802.16 και δημιουργήθηκε για να παρέχει τις προδιαγραφές για τη διαλειτουργικότητα μεταξύ των συστημάτων που χρησιμοποιούν οπτική επαφή.

### 7.3.5 IEEE 802.16 d

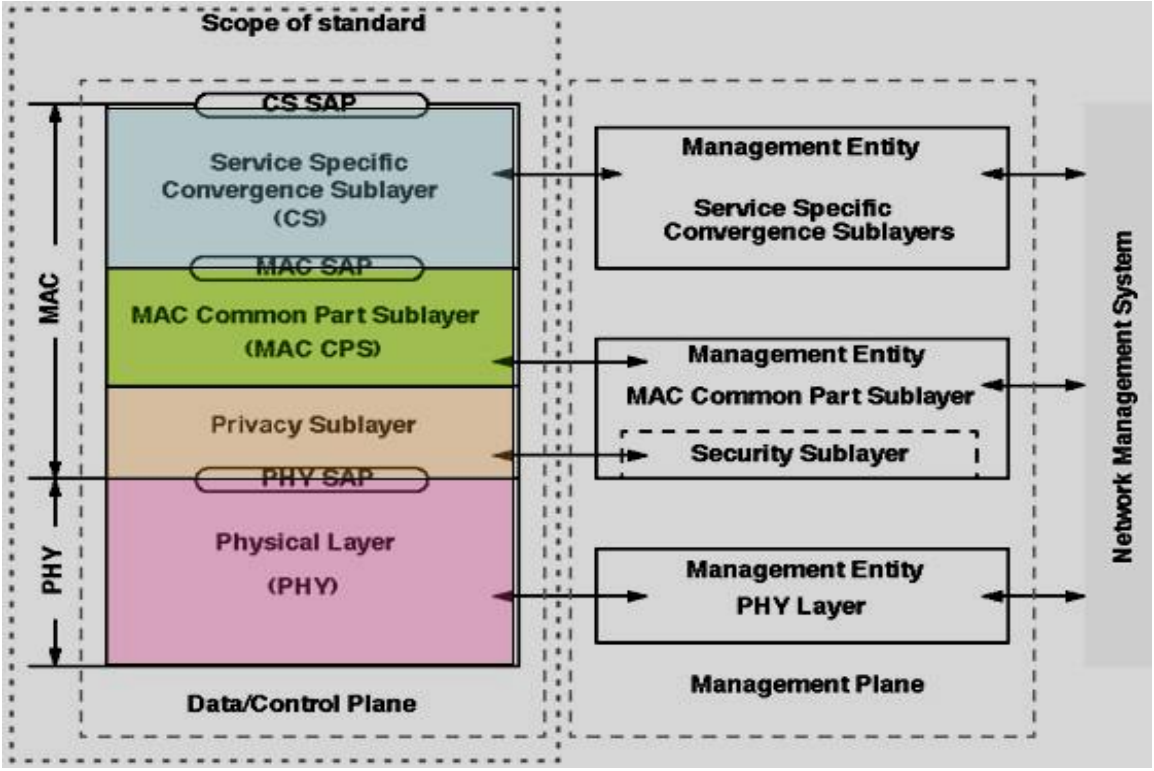
Η ομάδα εργασίας IEEE 802.16 αρχικά ξεκίνησε την αναθεώρηση των προτύπων IEEE 802.16, IEEE 802.16 a, IEEE 802.16 c αλλά στο τέλος αποφάσισε την τροποποίηση των προτύπων αυτών. Μετά την τροποποίηση, η ομάδα εργασίας κατέληξε στην αντικατάσταση των προτύπων αυτών με το πρότυπο 802.16 d. Το πρότυπο 802.16 d δημοσιεύτηκε το 2004 και μετονομάστηκε σε IEEE 802.16-2004 και περιλαμβάνει όλες τις λειτουργίες των προτύπων που αντικατέστησε και αφορούν την ασύρματη πρόσβαση σταθερών συστημάτων WiMAX για συχνότητες από 2 έως 66 GHz.

### 7.3.6 IEEE 802.16 e

Το πρότυπο IEEE 802.16e υποστηρίζει ασύρματη πρόσβαση για σταθερά, νομαδικά και κινητά συστήματα. Σε αυτό το πρότυπο ο χρήστης επιτρέπεται να κινείται από ένα σταθμό βάσης σε έναν άλλο, χωρίς να χάνεται η σύνδεση. Θεωρητικά, στο πρότυπο αυτό, ο χρήστης μπορεί να κινείται με ταχύτητα 120 Km / h. Βέβαια, πρακτικά δεν υπάρχει κάποιο πιστοποιημένο προϊόν που να είναι συμβατό με αυτό το πρότυπο και να έχει επιτύχει αυτήν την ταχύτητα. Αυτό το πρότυπο που δημοσιεύτηκε το 2005 και ονομάστηκε IEEE 802.16e-2005 αφορά την ασύρματη πρόσβαση κινητών συστημάτων WiMAX (Mobile WiMAX) και θα παρουσιαστεί σε επόμενη ενότητα.

## 7.4 ΑΝΑΛΥΣΗ ΕΠΙΠΕΔΩΝ WiMAX

Το πρότυπο IEEE 802.16 απευθύνεται στα δύο χαμηλότερα επίπεδα, όπως και τα περισσότερα πρότυπα του οργανισμού IEEE.Τα χαμηλότερα επίπεδα που υλοποιούνται είναι το φυσικό επίπεδο και το επίπεδο ζεύξης δεδομένων.



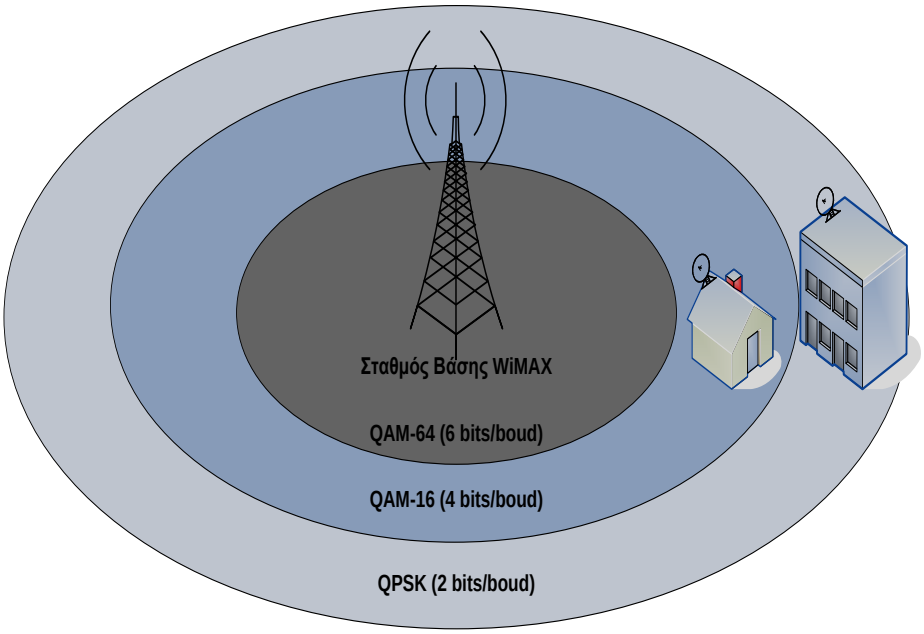

ΕΙΚΟΝΑ 98: ΕΠΙΠΕΔΑ ΤΟΥ ΠΡΟΤΥΠΟΥ 802.16

## 7.4.1 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΤΟΥ ΠΡΟΤΥΠΟΥ WiMaX

Το φυσικό στρώμα του 802.16 συνδυάζει την αμφιδρόμηση με διαίρεση χρόνου (Time Division Duplexing, TDD) και την αμφιδρόμηση με διαίρεση συχνότητας (Frequency Division Duplexing, FDD). Στην ανερχόμενη ζεύξη συνδυάζεται η τεχνική πολλαπλής πρόσβασης διαίρεσης χρόνου (Time Division Multiple Access, TDMA) και η πολλαπλή πρόσβαση αίτησης εκχώρησης (Demand Assignment Multiple Access, DAMA). Η πολλαπλή πρόσβασης αίτησης εκχώρησης DAMA είναι μια τεχνική ανάθεσης χωρητικότητας που προσαρμόζεται ανάλογα με την ζήτηση των σταθμών. Στην DAMA-TDMA η ανάθεση των χρονικών σχισμών είναι δυναμική.

Το κανάλι της ανερχόμενης ζεύξης διαιρείται σε έναν αριθμό χρονικών σχισμών. Το υπόστρωμα MAC στο σταθμό βάσης ελέγχει τον αριθμό των χρονικών σχισμών που καθορίζονται για διάφορες χρήσεις όπως την καταχώρηση (registration), την αναμέτρηση (contention), την φύλαξη (guard) και την κίνηση του χρήστη. Κάθε burst πληροφορίας μεταφέρει μεταβλητού μήκους MAC PDU (Packet Data Units). Η κωδικοποίηση των δεδομένων γίνεται με τον αλγόριθμο FEC (Forward Error Correction) και η διαμόρφωση των δεδομένων με QPSK

(Quadrature Phase Shift Keying) ή με 16 QAM (Quadrature Amplitude Modulation) ή με 64 QAM, ανάλογα με τη θέση του σταθμού συνδρομητή όπως φαίνεται στο παρακάτω σχήμα[1][2][3]:




**ΕΙΚΟΝΑ 99: ΚΩΔΙΚΟΠΟΙΗΣΗ ΣΤΟ ΠΕΡΙΒΑΛΛΟΝ ΜΕΤΑΔΟΣΗΣ**

Στο μοντέλο αυτό, ο σταθμός βάσης ελέγχει το σύστημα, προγραμματίζει τον χρόνο για τα κατερχόμενα κανάλια, δηλαδή τα κανάλια από το σταθμό βάσης προς το σταθμό συνδρομητή, ενώ είναι αρμόδιος για τη διαχείριση των ανερχόμενων καναλιών, δηλαδή των καναλιών από το σταθμό συνδρομητή προς το σταθμό βάσης.

Στην κατερχόμενη ζεύξη χρησιμοποιείται η τεχνική πολύπλεξης διαίρεσης χρόνου (Time Division Multiplexing, TDM), όπου τα δεδομένα για κάθε σταθμό συνδρομητή πολυπλέκονται σε μια ομοιόμορφη ροή δεδομένων και λαμβάνονται από τους σταθμούς συνδρομητή που βρίσκονται στον ίδιο τομέα (sector). Στο φυσικό στρώμα, στην κατερχόμενη ζεύξη, υπάρχει το υπόστρωμα σύγκλισης της μετάδοσης (Transmission Convergence), το οποίο τοποθετεί ένα δείκτη σε byte στην αρχή της μετάδοσης, για να βοηθήσει το δέκτη να καταλάβει την αρχή ενός MAC PDU. Τα bits των δεδομένων που έρχονται από αυτό το υπόστρωμα κωδικοποιούνται και πάλι με το FEC και η διαμόρφωσή τους γίνεται με μια από τις τεχνικές QPSK, 16 QAM και 64 QAM[1][2][3].

### 7.4.1.1 AIR INTERFACES WiMAX

Το WiMAX διαθέτει πέντε παραλλαγές που ορίζονται από το φυσικό τους στρώμα. Οι παραλλαγές χωρίζονται ανάλογα με το αν είναι μονού φέροντος (Single Carrier) ή χρησιμοποιούν OFDM. Χωρίζονται σε κατηγορίες ανάλογα με τη ζώνη συχνοτήτων που καλύπτουν 2-11 GHz και 10-66 GHz. Στη συνέχεια παρουσιάζονται οι παραλλαγές αυτές[2].

ΠΙΝΑΚΑΣ 31: ΠΑΡΑΛΛΑΓΕΣ

| ΟΝΟΜΑΣΙΑ | ΛΕΙΤΟΥΡΓΙΑ | LOS/NLOS | ΣΥΧΝΟΤΗΤΑ | DUPLEXING |
|---|---|---|---|---|
| WirelessMAN-SC | Point-to-Multipoint | LOS | 10-66 GHz | TDD, FDD |
| WirelessMAN-SCa | Point-to-Point | NLOS | 2-11 GHz | TDD, FDD |
| WirelessMAN-OFDM | Point-to-Multipoint | NLOS | 2-11 GHz | TDD, FDD |
| WirelessMAN-OFDMA | Point-to-Multipoint | NLOS | 2-11 GHz | TDD, FDD |
| WirelessHUMAN | Point-to-Multipoint | NLOS | 2-11 GHz | TDD |

### 7.4.1.2 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ WiMAX 10-66 GHz

Στην ζώνη συχνοτήτων 10-66 GHz με χρήση οπτικής επαφής, ο σταθμός βάσης μεταδίδει το σήμα στο κατωφερές κανάλι με τη TDM. Επίσης, χρησιμοποιούνται οι TDD και η FDD για την ευέλικτη χρήση του φάσματος. Το φυσικό επίπεδο της ανερχόμενη ζεύξης χρησιμοποιεί την TDMA και την DAMA. Το φυσικό επίπεδο της κατωφερούς ζεύξης με το υπόστρωμα σύγκλισης της μετάδοσης (Transmission Convergence) καθώς και τα δεδομένα, κωδικοποιούνται με το FEC και διαμορφώνονται με τις τεχνικές QPSK, 16 QAM και 64 QAM. Όλες αυτές οι

λειτουργίες που αναφέρθηκαν περιλαμβάνονται στην παραλλαγή WirelessMAN-SC. Το μέγεθος του καναλιού στο πρώτο πρότυπο, ήταν 20 ή 25MHz για τις ΗΠΑ και 28MHz για την Ευρώπη.

### 7.4.1.3 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ WiMAX 2-11 GHz

Το φυσικό επίπεδο των 2-11 GHz χρησιμοποιεί τις παραλλαγές WirelessMAN-SCa, την WirelessMAN-OFDM, την WirelessMAN-OFDMA και την WirelessHUMAN, με χρήση μη-οπτικής επαφής. Η παραλλαγή WirelessMAN-SCa βασίζεται στην τεχνολογία μονού φέροντος και σχεδιάστηκε για NLOS λειτουργία σε ζώνες συχνοτήτων μικρότερες των 11GHz. Το φυσικό επίπεδο των 2-11 GHz χρησιμοποιούν είτε την TDD είτε την FDD. Για την ανερχόμενη ζεύξη χρησιμοποιεί την TDMA ενώ για την κατερχόμενη ζεύξη είτε την TDM είτε την TDMA. Για την κωδικοποίηση των δεδομένων, χρησιμοποιείται το FEC και για τις ανερχόμενες αλλά και για τις κατερχόμενες ζεύξεις.

Η παραλλαγή WirelessMAN-OFDM χρησιμοποιεί την διαμόρφωση 256–FFT OFDM, που όπως δηλώνει το όνομα της, είναι υποχρεωτική στις μη-αδειοδοτημένες ζώνες και η πρόσβαση γίνεται με την TDMA. Χρησιμοποιείται κυρίως για ασύρματη πρόσβαση σταθερού σημείου, όπου οι πύλες των συνδρομητικών σταθμών αποτελούνται από σπίτια και επιχειρήσεις. Επίσης, υποστηρίζει υπό-καναλοποίηση με 16 υποκανάλια στην κατερχόμενη ζεύξη και χρησιμοποιεί πολλές διαμορφώσεις όπως Binary Phase Shift Keying (BPSK), QPSK, 16-QAM και 64-QAM. Επιπλέον, υποστηρίζει διαφορετικές εκπομπές στην κατερχόμενη ζεύξη χρησιμοποιώντας το Space Time Coding (STC) και το σύστημα προσαρμόσιμων κεραιών με Spatial Division Multiple Access (SDMA). Για τις διαφορετικές εκπομπές χρησιμοποιούνται δύο κεραίες στο σταθμό βάσης για να εκπέμψουν ένα σήμα κωδικοποιημένο με το STC.

Η παραλλαγή WirelessMAN-OFDMA χρησιμοποιεί την διαμόρφωση 2048 – FFT OFDMA η οποία παρέχει πολλαπλή πρόσβαση.

Η παραλλαγή WirelessHUMAN αφορά τις συχνότητες των μη-αδειοδοτημένων ζωνών και η δομή της είναι παρόμοια με τις δομές των παραλλαγών που χρησιμοποιούν την OFDM.

Το WiMAX χρησιμοποιεί παγκοσμίως τη μη-αδειοδοτημένη ζώνη συχνοτήτων των 5 GHz και την αδειοδοτημένη ζώνη συχνοτήτων των 2.3 GHz, των 2.5 GHz, των 3.3 GHz και των 3.5 GHz. Στον πίνακα που ακολουθεί παρουσιάζονται οι παγκόσμιες ζώνες συχνοτήτων στις οποίες λειτουργεί το WiMAX.

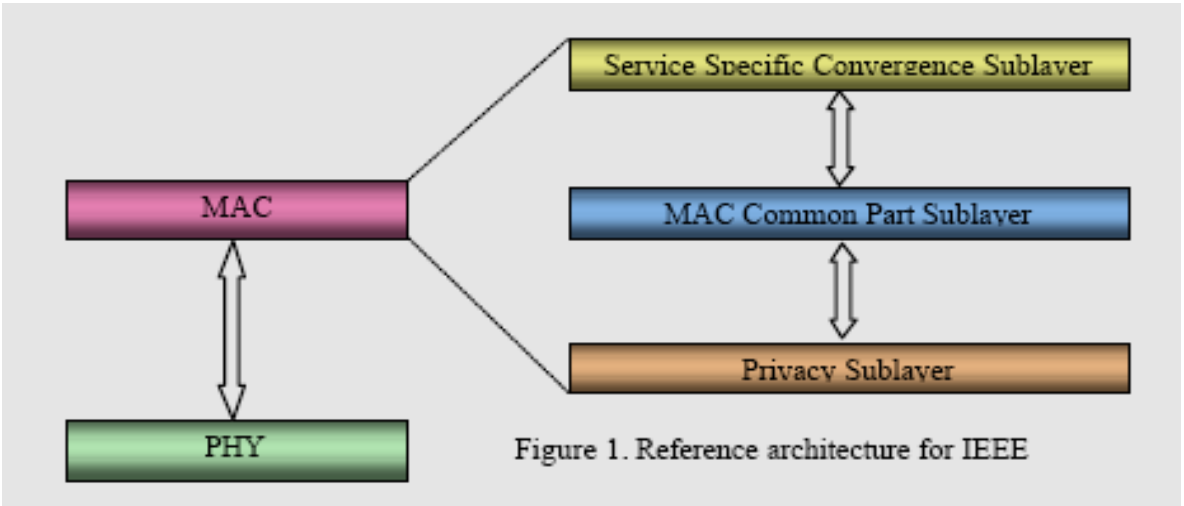
**ΠΙΝΑΚΑΣ 32: ΖΩΝΕΣ ΣΥΧΝΟΤΗΤΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΕΙ ΤΟ WiMAX ΠΑΓΚΟΣΜΙΩΣ**

| Region or country | Reported WiMAX frequency bands |
|---|---|
| USA | 2.3, 2.5 and 5.8GHz |
| Central and South America | 2.5, 3.5 and 5.8GHz |
| Europe | 3.5 and 5.8GHz; possible: 2.5GHz |
| South-East Asia | 2.3, 2.5, 3.3, 3.5 and 5.8GHz |
| Middle East and Africa | 3.5 and 5.8GHz |

## 7.4.2 ΤΟ ΥΠΟΣΤΡΩΜΑ MAC ΤΟΥ ΠΡΟΤΥΠΟΥ WiMaX

Το υπόστρωμα MAC χωρίζεται σε πολλά υποεπίπεδα όπως[1][2][3]:

- Το υποεπίπεδο privacy.
- Το υποεπίπεδο κοινού μέρους.
- Το υποεπίπεδο Σύγκλισης Ειδικών υπηρεσιών.




**ΕΙΚΟΝΑ 100: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ MAC ΚΑΙ ΤΟΥ PHY ΕΠΙΠΕΔΩΝ ΤΟΥ ΠΡΟΤΥΠΟΥ IEEE 802.16**

### 7.4.2.1 ΥΠΟΕΠΙΠΕΔΟ ΑΣΦΑΛΕΙΑΣ

Το υποεπίπεδο Ασφαλείας (privacy) παρέχει την ασφάλεια στο πρότυπο IEEE 802.16 και περιλαμβάνει την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων από το φυσικό επίπεδο. Το WiMAX χρησιμοποιεί το πρότυπο X.509 για την κρυπτογράφηση της σύνδεσης κατά την δημιουργία της. Επίσης, κάνει χρήση του αλγόριθμου 56-bit DES για την προστασία των δεδομένων κατά την μετάδοση.

### 7.4.2.2 ΚΟΙΝΟ ΤΜΗΜΑ ΥΠΟΣΤΡΩΜΑΤΟΣ MAC

Το κοινό τμήμα του υποστρώματος MAC περιέχει τα βασικά πρωτόκολλα για την διαχείριση των συνδέσεων . Το κοινό τμήμα του υποστρώματος MAC είναι αρμόδιο για την αναμετάδοση των πακέτων σε περιπτώσεις λαθών και για την εξασφάλιση της ποιότητας των υπηρεσιών.

Πρόσβαση στο μέσο

Στο πρότυπο IEEE 802.16, το υπόστρωμα MAC ορίζει ότι για την αρχική είσοδο του σταθμού συνδρομητή μέσα στο δίκτυο, θα χρειαστεί μία προσπάθεια και έπειτα ο σταθμός βάσης θα διαθέσει στον σταθμό συνδρομητή μία χρονική θυρίδα. Οι άλλοι σταθμοί δεν μπορούν να χρησιμοποιήσουν αυτήν την χρονική θυρίδα με αποτέλεσμα να περιμένουν την σειρά τους. Όπως έχει αναφερθεί, για την εισερχόμενη ζεύξη χρησιμοποιείται η TDMA και για την κατερχόμενη ζεύξη η TDM. Η χρήση της TDM για την πρόσβαση στο μέσο, επιτρέπει σε πολλούς χρήστες να συνδεθούν με χαμηλό κόστος υλοποίησης. Η πρόσβαση στο μέσο παραμένει σταθερή, δεν επηρεάζεται από συνθήκες υπερφόρτωσης ούτε από τον αριθμό των σταθμών.

Ποιότητα υπηρεσίας

Το πρότυπο IEEE 802.16 παρέχει υψηλή ποιότητα υπηρεσίας, καθώς το υπόστρωμα MAC έχει σχεδιαστεί με σκοπό να παρέχει τον καλύτερο δυνατό ρυθμό μετάδοσης και τη βέλτιστη προσπάθεια πρόσβασης σε όλους τους χρήστες που καλύπτει ένας βασικός σταθμός. Αν ένας σταθμός βάσης καλύπτει δύο σταθμούς συνδρομητή, τότε ο ένας θα έχει υψηλή ποιότητα υπηρεσίας και ο άλλος

θα έχει την απλή IP κίνηση μέγιστης προσπάθειας για τη μετάδοση των δεδομένων.

Για τις απαιτήσεις των χρηστών, η κατανομή του εύρους ζώνης διαχειρίζεται από μηχανισμούς τεσσάρων τύπων υπηρεσιών. Οι τύποι υπηρεσίας είναι η υπηρεσία αυτόκλητης αίτησης, η υπηρεσία σταθμοσκόπησης πραγματικού χρόνου, η υπηρεσία σταθμοσκόπισης μη πραγματικού χρόνου και η υπηρεσία καλύτερης προσπάθειας[1][2].

Υπηρεσία αυτόκλητης αίτησης (Unsolicited Grand Services, UGS)

Η υπηρεσία αυτόκλητης αίτησης παρέχει μέγιστο συνεχή ρυθμό μετάδοσης, μέγιστη αντοχή στην καθυστέρηση και στην διακύμανση της καθυστέρησης, όπως στο VoIP χωρίς σιωπή.

Υπηρεσία σταθμοσκόπησης πραγματικού χρόνου (Real-Time Polling Services, rtPS)

Η υπηρεσία σταθμοσκόπησης πραγματικού χρόνου υποστηρίζει υπηρεσίες πραγματικού χρόνου που παράγουν μεταβλητό μέγεθος πακέτων δεδομένων, όπως βίντεο ή VoIP και παρέχει τον ελάχιστο απαιτούμενο ρυθμό, τον μέγιστο συνεχή ρυθμό, μεγάλη αντοχή στην καθυστέρηση και προτεραιότητα στην κίνηση.

Υπηρεσία Polling μη πραγματικού χρόνου (Non-Real-Time Polling Services, nrtPS)

Η υπηρεσία Polling μη πραγματικού χρόνου, υποστηρίζει υπηρεσίες μη πραγματικού χρόνου που περιέχουν μεταβλητό μέγεθος δεδομένων, οι οποίες χρειάζονται προτεραιότητα κίνησης και τον ελάχιστο απαιτούμενο ρυθμό, όπως το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol).

Υπηρεσία καλύτερης προσπάθειας (Best Effort Services)

Η υπηρεσία καλύτερης προσπάθειας παρέχει μέγιστο ρυθμό και προτεραιότητα κίνησης για την μεταφορά των δεδομένων, το Web και την πλοήγηση στο διαδίκτυο.

### 7.4.2.3 ΥΠΟΕΠΙΠΕΔΟ ΣΥΓΚΛΙΣΗΣ ΣΧΕΤΙΚΟ ΜΕ ΤΙΣ ΥΠΗΡΕΣΙΕΣ

Το υποεπίπεδο σύγκλισης σχετικό με τις υπηρεσίες (Service Specific Convergence Sublayer, CS) παρέχει την διασύνδεση με το επίπεδο δικτύου. Το υποεπίπεδο αυτό τροποποιεί σε MAC SDU (Service Data Unit), τα εξωτερικά δεδομένα του δικτύου που λαμβάνονται μέσω του CS service access point (SAP), για να ληφθούν από το υποεπίπεδο κοινού τμήματος. Επίσης, οι μονάδες δεδομένων υπηρεσίας SDU ταξινομούνται σε κατηγορίες και συσχετίζονται με το αντίστοιχο αναγνωριστικό Σύνδεσης (Connection Identifier, CID) και τη ροή των υπηρεσιών.

Στην αντιστοίχιση υπηρεσιών, το CS συμπιέζει τις κεφαλίδες εφόσον είναι ενεργοποιημένη η λειτουργία PHS (payload header suppression) και τροποποιεί τα εξωτερικά δεδομένα που προήλθαν από υψηλότερο επίπεδο σε MAC SDUs, αφού πρώτα έχει γίνει η προετοιμασία των εξωτερικών δεδομένων για την μεταβίβαση στο υποεπίπεδο κοινού τμήματος.

Αν η λειτουργία PHS είναι ενεργοποιημένη, με τη συμπίεση της κεφαλίδας μειώνεται το overhead και έχουμε κέρδος στο bandwidth. Αυτή η λειτουργία εφαρμόζεται σε επίπεδο δικτύου ATM και packet-switched. Το υπόστρωμα CS είναι αρμόδιο[1][2][3]: 1) για την παραλαβή των πακέτων PDU από τα ανώτερα επίπεδα, 2) για την ταξινόμηση των πακέτων PDU ώστε να παραδοθούν στην κατάλληλη σύνδεση προς μετάδοση, 3) για την προαιρετική επεξεργασία των PDU με βάση την ταξινόμηση τους, 4) για την παράδοση των επεξεργασμένων PDU στο κατάλληλο interface του MAC SAP και την παραλαβή των CS SDU από το CPS και 5) για την μετάδοση προς τα ανώτερα επίπεδα. Το υπόστρωμα αυτό παρέχει δύο προδιαγραφές το CS πακέτο για υπηρεσίες πακέτων δεδομένων όπως IP και Ethernet και τον ασύγχρονο τύπο μετάδοσης CS (Asynchronous transfer mode, ATM CS) για υπηρεσίες ATM.

Το CS πακέτο χρησιμοποιείται για την μεταφορά όλων των πακέτων με βάση τα πρωτόκολλα όπως το IP και το Ethernet. Επίσης, στο πακέτο CS καθορίζεται η ταξινόμηση και η ενεργοποίηση της λειτουργίας PHS (αν είναι ενεργοποιημένη).

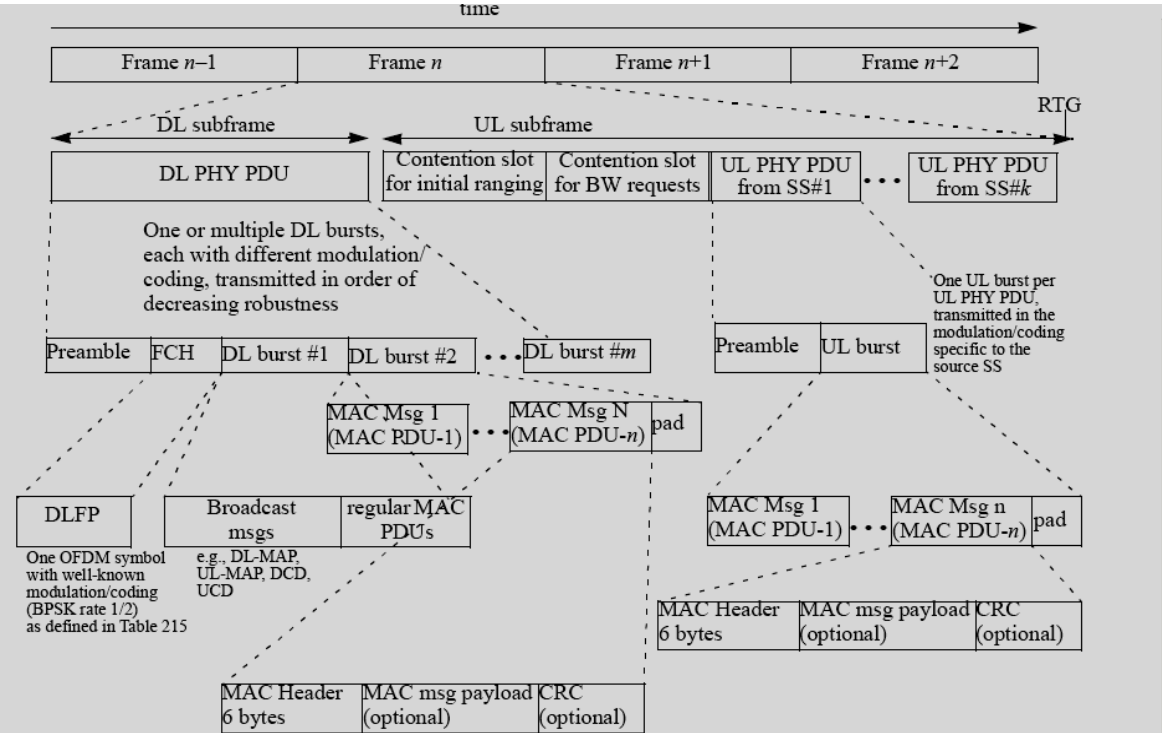
Το ATM CS είναι μία διεπαφή που συνδέει τις υπηρεσίες ATM με το MAC CPS SAP. Το ATM CS δέχεται ATM cells από το ATM επίπεδο, εκτελεί την ταξινόμηση

αν η PHS είναι ενεργοποιημένη. Το ATM CS αποδέχεται τα cell του ATM από το επίπεδο ATM, τα ταξινομεί, τα επεξεργάζεται και τα παραδίδει ως CS PDU στο κατάλληλο MAC CP SAP.

### 7.4.3 ΔΟΜΗ ΠΛΑΙΣΙΟΥ

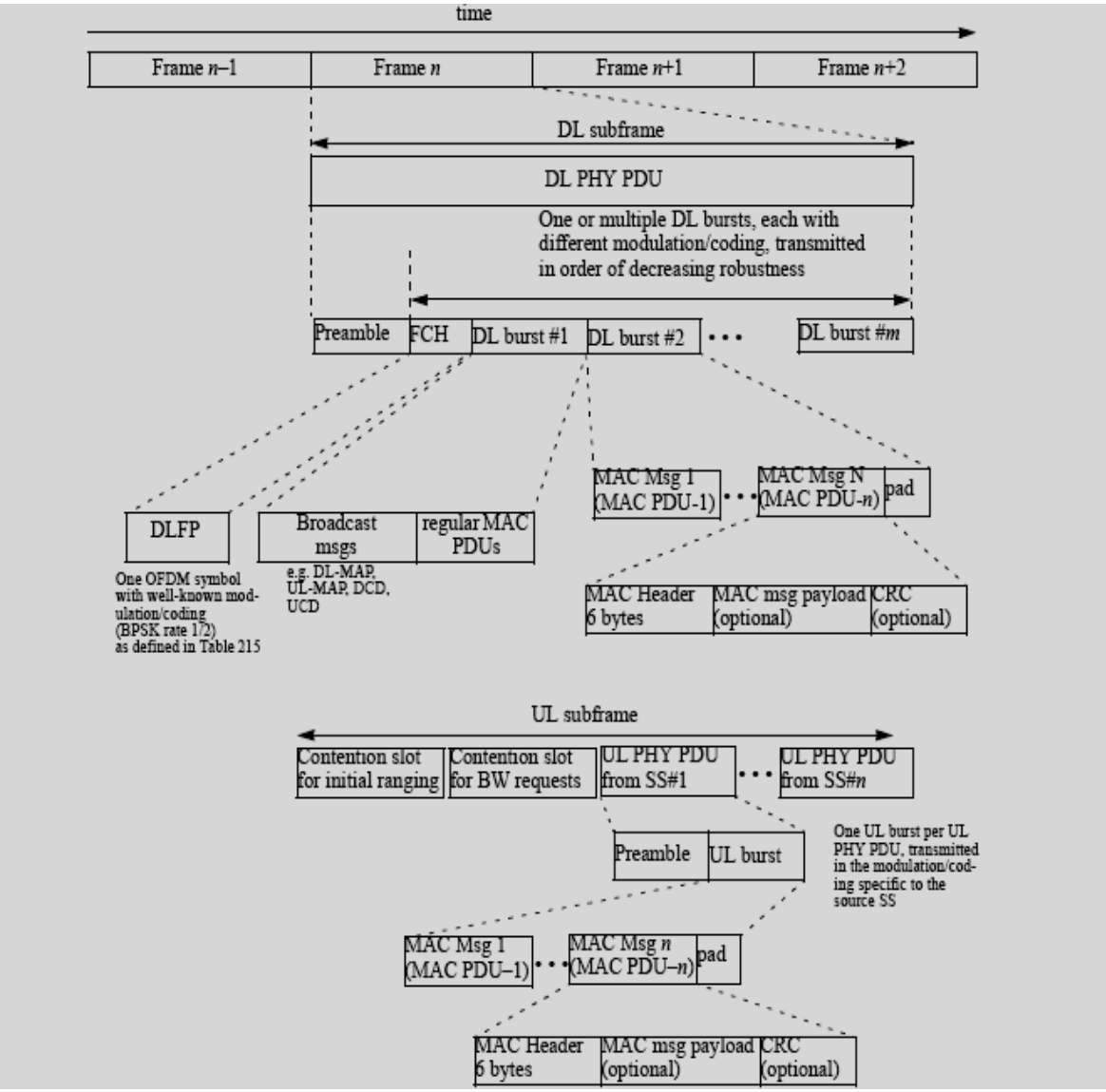
Παρακάτω περιγράφεται η δομή πλαισίων με την διαμόρφωση φυσικού επιπέδου OFDM. Η διαμόρφωση OFDM αποτελείται από ένα ανερχόμενο υπο-πλαίσιο και από ένα κατερχόμενο υπο-πλαίσιο. Ένα κατερχόμενο υπο-πλαίσιο περιλαμβάνει ένα κατερχόμενο PDU και ένα ανερχόμενο υπο-πλαίσιο περιλαμβάνει ένα ή πολλά ανερχόμενα PDU που εκπέμπονται από διαφορετικούς σταθμούς συνδρομητή. Επίσης, το ανερχόμενο υπο-πλαίσιο περιλαμβάνει διαστήματα για την αρχικοποίηση και την απαίτηση εύρους.

Ένα κατερχόμενο PDU ξεκινά με ένα long preamble που χρησιμοποιείται για τον συγχρονισμό. Μετά το preamble ακολουθεί ένα FCH (Frame Control Header) burst με διάρκεια ενός συμβόλου OFDM και χρησιμοποιεί διαμόρφωση QPSK. Το DLFP (Downlink frame prefix) περιέχεται στο FCH, το οποίο καθορίζει το προφίλ burst και το μέγεθος ενός ή περισσοτέρων downlink burst ακολουθούμενα από το FCH. Το DLFP περιλαμβάνει τέσσερα στοιχεία πληροφορίας (Information Elements) που κάθε ένα ορίζει ένα DL burst. Τα πεδία των στοιχείων πληροφορίας περιέχουν τις πληροφορίες για το μήκος και το προφίλ burst και ένα προαιρετικό preamble για το συγχρονισμό. Όταν υπάρχουν παραπάνω από ένα DL burst, καθορίζονται από ένα DL-MAP, το οποίο ακολουθεί το FCH. Το DL-MAP περιέχει τους δείκτες των στοιχείων πληροφορίας των επόμενων DL burst που βρίσκονται σε επόμενα πλαίσια. Το προφίλ καθορίζεται από το DIUC (Downlink Interval Usage Code) και από ένα Rate-ID που έχει μέγεθος τεσσάρων bit του πρώτου DL burst. Το DIUC καθορίζεται στα μηνύματα DCD (Downlink Channel Descriptor).




**ΕΙΚΟΝΑ 101: ΔΟΜΗ ΠΛΑΙΣΙΩΝ ΜΕ TDD**

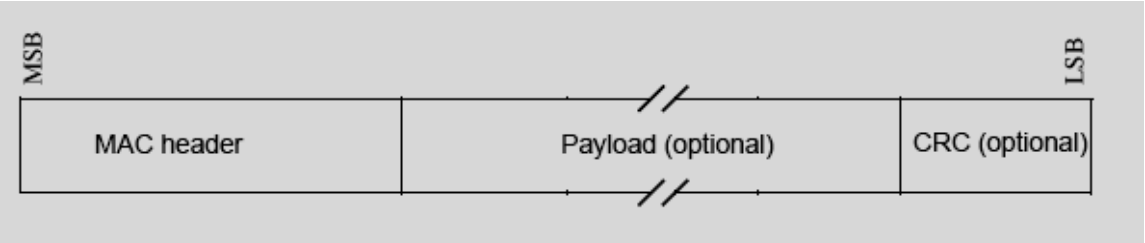
Ένα ανερχόμενο PDU αποτελείται από ένα UL burst και ένα short preamble. Το προφίλ καθορίζεται από το UIUC (Uplink Interval Usage Code) τεσσάρων bit. Το UL-MAP μήνυμα πρέπει να ακολουθεί το DL-MAP ή το DLFP και μετά ακολουθούν τα μηνύματα UCD (Uplink Channel Descriptor). Στην αμφίδρομη διαίρεση χρόνου υπάρχει το πεδίο TTG (Transmit transition gap) και το πεδίο RTG (Receive Transition gap) που εκφράζουν το κενό μετάδοσης μεταξύ της εκπομπής και της λήψης. Μόλις τελειώσει το υποπλαίσιο downlink ακολουθεί το πεδίο TTG και έπειτα το ανερχόμενο υποπλαίσιο. Στο τέλος του ανερχόμενου υποπλαισίου υπάρχει το πεδίο RTG. Στην αμφιδρόμηση με διαίρεση συχνότητας τα υποπλαίσια DL και UL συμπίπτουν χρονικά αλλά είναι σε διαφορετικές συχνότητες[1][2].




**ΕΙΚΟΝΑ 102: ΔΟΜΗ ΠΛΑΙΣΙΩΝ ΜΕ FDD**

## 7.4.3.1 ΔΟΜΗ MAC PACKET DATA UNIT

Η συντακτική δομή της MAC Packet Data Unit περιλαμβάνει την κεφαλίδα MAC, το προαιρετικό πεδίο Payload και το προαιρετικό πεδίο CRC. Το πεδίο CRC είναι προαιρετικό σε πλαίσια δεδομένων και υποχρεωτικό σε πλαίσια διαχείρισης. Το πεδίο CRC καθορίζεται κατά τη σηματοδοσία ανάλογα με την ποιότητα υπηρεσιών. Το πεδίο Payload PDU περιέχει την μεταφερόμενη πληροφορία.




**ΕΙΚΟΝΑ 103: ΔΟΜΗ MAC PACKET DATA UNIT**

Το uplink περιέχει δύο τύπους κεφαλίδων τη γενική επικεφαλίδα MAC (Generic MAC Header) και την επικεφαλίδα Bandwidth Request Header. Όταν το πλαίσιο περιέχει την επικεφαλίδα Bandwidth Request Header, το πλαίσιο δεν περιέχει payload και CRC. Το downlink περιέχει τον τύπο της γενικής επικεφαλίδας MAC (Generic MAC Header) που περιέχει μηνύματα διαχείρισης MAC ή δεδομένα του υποεπιπέδου σύγκλισης.

Η επικεφαλίδα MAC έχει μέγεθος 6 οκτάδες και υπάρχει κατά την μεταφορά των δεδομένων διαχείρισης και ελέγχου. Η επικεφαλίδα MAC περιέχει τα παρακάτω πεδία[1]:

- **Header Type.** Όταν το πεδίο Header Type έχει την τιμή 0 αφορά τον τύπο της γενικής επικεφαλίδας MAC (Generic MAC Header), ενώ όταν έχει την τιμή 1 αφορά την επικεφαλίδα Bandwidth Request Header (χωρίς payload και CRC) και έχει μέγεθος ενός bit.
- **Encryption Control.** Το πεδίο Encryption Control (EC) περιέχει την τιμή 0 στην περίπτωση που δεν υπάρχει payload ή όταν υπάρχει το payload και δεν είναι κρυπτογραφημένο. Επίσης περιέχει την τιμή 1 όταν το payload είναι κρυπτογραφημένο και έχει μέγεθος ένα bit. Στην περίπτωση της επικεφαλίδας Bandwidth Request Header, το EC έχει την τιμή 0.
- **Type.** Το πεδίο Type για την επικεφαλίδα Generic MAC έχει μέγεθος έξι bits και υποδεικνύει την παρουσία ή την απουσία των υποκεφαλίδων και των ειδικών τύπων του payload, τα οποία παρουσιάζονται παρακάτω. Το πεδίο Type για την επικεφαλίδα Bandwidth Request Header, έχει μέγεθος τρία bits και περιλαμβάνει τις τιμές “000” για την προσαύξηση (incremental) της ποσότητας του bandwidth που χρειάζεται μία σύνδεση με το bandwidth που ζητήθηκε και “001” για τη συνολική αντικατάσταση της ποσότητας του bandwidth που χρειάζεται μία σύνδεση με το bandwidth που ζητήθηκε.

- **CRC Indicator.** Το πεδίο CRC Indicator (CI) έχει μέγεθος ένα bit και υποδεικνύει την χρήση ή τη μη χρήση του CRC. Έχει την τιμή 0 όταν δεν περιλαμβάνεται και την τιμή 1 όταν περιλαμβάνεται στο PDU και μετά την κρυπτογράφηση επισυνάπτεται στο PDU payload. Το πεδίο αυτό δεν περιέχεται στην επικεφαλίδα Bandwidth Request Header.
- **Encryption key sequence.** Το πεδίο Encryption key sequence (EKS) έχει μέγεθος δύο bits, εξαρτάται από την ύπαρξη της κρυπτογράφησης. Για την κρυπτογράφηση του payload χρησιμοποιείται το διάνυσμα αρχικοποίησης (Initialization Vector,IV) και ο δείκτης του traffic encryption key (TEK), που περιλαμβάνονται στο πεδίο EKS. Το πεδίο αυτό δεν περιέχεται στην επικεφαλίδα Bandwidth Request Header.
- **Length.** Το πεδίο Length έχει μέγεθος έντεκα bits και δείχνει το μέγεθος σε bytes του MAC PDU μαζί με την επικεφαλίδα Generic MAC και το CRC (αν υπάρχει). Το πεδίο αυτό δεν περιέχεται στην επικεφαλίδα Bandwidth Request Header.
- **Connection ID.** Το πεδίο Connection ID (CID) έχει μέγεθος δεκαέξι bits και περιέχει το αναγνωριστικό της σύνδεσης CID που προσδιορίζει το πλαίσιο.
- **Extended Subheader field.** Το πεδίο Extended Subheader (ESF) έχει μέγεθος ένα bit, παίρνει την τιμή 0 όταν δεν υπάρχουν επιπλέον Subheaders και την τιμή 1 όταν υπάρχουν επιπλέον Subheaders. Όταν υπάρχουν Subheaders πρέπει να ακολουθούν την επικεφαλίδα του Generic MAC, ισχύουν για downlink και για uplink. Το πεδίο αυτό δεν περιέχεται στην επικεφαλίδα Bandwidth Request Header.
- **Header Check Sequence.** Το πεδίο Header Check Sequence (HCS) έχει μέγεθος οκτώ bits και εντοπίζει τα λάθη που γίνονται στην κεφαλίδα.
- Οι τιμές που παίρνει το πεδίο Type, στην επικεφαλίδα Generic MAC, σε κάθε bit ξεκινώντας από το πιο σημαντικό bit (Most Significant bit, MSB) και καταλήγοντας στο λιγότερο σημαντικό bit (Least Significant bit, LSB) είναι:
  - **#5 bit:** Subheader Mesh. Η υποκεφαλίδα Mesh δείχνει αν χρησιμοποιείται ή όχι η τοπολογία Mesh. Αν χρησιμοποιείται η τοπολογία αυτή, τότε η υποκεφαλίδα Mesh προηγείται από τις υπόλοιπες υποκεφαλίδες. Η υποκεφαλίδα Mesh παίρνει την τιμή 1, αν χρησιμοποιείται και την τιμή 0, αν δεν χρησιμοποιείται.

- **#4 bit:** ARQ Feedback Payload. Η υποκεφαλίδα αυτή παίρνει την τιμή 1, αν χρησιμοποιείται και την τιμή 0 αν δεν χρησιμοποιείται. Όταν χρησιμοποιείται, το ARQ Feedback Payload μεταδίδεται ως αυτόνομο μήνυμα διαχείρισης MAC στη βασική σύνδεση διαχείρισης. Το ARQ Feedback Payload μεταδίδεται σε συνδέσεις ARQ και μη-ARQ. Όταν χρησιμοποιείται επανασυναρμολόγηση, το ARQ Feedback Payload μεταδίδεται πρώτο από το επανασυναρμολογούμενο payload και μόνο ένα ARQ Feedback Payload ενσωματώνεται σε ένα ενιαίο MAC PDU. Αν χρησιμοποιείται η κατάτμηση, ο πομπός χωρίζει σε ένα σύνολο από blocks κάθε SDU με μέγεθος ανάλογο με την τιμή της παραμέτρου του ARQ_BLOCK_SIZE για ξεχωριστή μετάδοση. Κάθε block ARQ έχει ακολουθιακή αρίθμηση (Block Sequence Number, BSN) μέσα στο πλαίσιο PDU. Η εφαρμογή του μηχανισμού ARQ (Automatic Repeat ReQuest) είναι προαιρετική και ο μηχανισμός ARQ καθορίζεται κατά τη δημιουργία κάθε σύνδεσης. Κάθε σύνδεση είναι μιας κατεύθυνσης και μεταδίδονται είτε δεδομένα ARQ είτε μη- ARQ δεδομένα. Ο μηχανισμός ARQ χρησιμοποιεί μηνύματα acknowledgement (ACK) ή non acknowledgement (NACK), που μεταδίδονται από τον παραλήπτη στον αποστολέα για την θετική ή την αρνητική επιβεβαίωση των block που λήφθηκαν. Αν ο παραλήπτης μεταδώσει αρνητική επιβεβαίωση ενός block στον αποστολέα, ο αποστολέας αναμεταδίδει το συγκεκριμένο block. Τα πακέτα ARQ έχουν μικρό μήκος και για αυτό δεν διαχωρίζονται σε επιπλέον τμήματα. Τα είδη των πακέτων ARQ είνα[1]:
  - Η επιλεκτική επιβεβαίωση (Selective ACK), στην οποία αποστέλλονται θετικές ή αρνητικές επιβεβαιώσεις για κάθε λαμβανόμενο block.
  - Η σωρευτική επιβεβαίωση (Cumulative ACK) χρησιμοποιεί τον μηχανισμό του κινούμενο παραθύρου. Σε αυτή την περίπτωση χρησιμοποιείται ο BSN, αν το BSN=2 σημαίνει ότι από όλα τα λαμβανόμενα block, μόνο τα πρώτα δύο block έχουν ληφθεί σωστά.
  - Η σωρευτική με επιλεκτική επιβεβαίωση (Cumulative with Selective ACK), στην οποία χρησιμοποιείται πάλι το BSN και η επιβεβαίωση αρχίζει με την σωρευτική. Αν το BSN=2, τότε τα υπόλοιπα λαμβανόμενα

block (μετά τα δύο πρώτα σωστά λαμβανόμενα block), ακολουθούν την επιλεκτική επιβεβαίωση.

- Η σωρευτική επιβεβαίωση με block ακολουθίας (Cumulative ACK with Block Sequence), στην οποία ορίζονται ακολουθίες με κάποιο αριθμό block.

- **#3 bit:** Extended Type. Το Extended Type παίρνει την τιμή 1 όταν σε συνδέσεις που χρησιμοποιούν τον μηχανισμό ARQ, χρησιμοποιούνται οι subheaders Packing ή Fragmentation και την τιμή 0 όταν χρησιμοποιούνται οι subheaders Packing ή Fragmentation αλλά σε συνδέσεις που δεν χρησιμοποιούν τον μηχανισμό ARQ.
- **#2 bit:** Subheader Fragmentation. Η υποκεφαλίδα κατάτμησης (Fragmentation Subheader, FSH) περιλαμβάνει την λειτουργία κατάτμησης. Η λειτουργία κατάτμησης, διαχωρίζει το MAC SDU σε περισσότερα MAC PDU, αν το μέγεθος του MAC SDU είναι μεγαλύτερο από το όριο της μέγιστης μονάδας μεταφοράς (MTU) του πρωτοκόλλου. Η υποκεφαλίδα κατάτμησης περιέχει το αναγνωριστικό αριθμό (fragment sequence number, FSN) κάθε πλαισίου για την ορθή σειρά των πακέτων κατά την επανασυναρμολόγηση και τον δείκτη ελέγχου κατάτμησης (Fragmentation Control, FC). Ο δείκτης ελέγχου κατάτμησης παίρνει τις ακόλουθες τιμές:
  a) 00 = No fragmentation
  b) 01 = Last fragment
  c) 10 = First fragment
  d) 11 = Continuing (middle) fragment.

- **#1 bit:** Subheader Packing. Η υποκεφαλίδα επανασυναρμολόγησης (Packing Subheader, PSH) περιλαμβάνει την λειτουργία επανασυναρμολόγησης. Η επανασυναρμολόγηση είναι η αντίθετη λειτουργία της κατάτμησης. Η επανασυναρμολόγηση, συναρμολογεί όλα τα MAC SDU σε ένα MAC PDU. Η λειτουργία αυτή πραγματοποιείται στον δέκτη. Στο MAC PDU θα υπάρχει είτε η υποκεφαλίδα κατάτμησης είτε η υποκεφαλίδα επανασυναρμολόγησης. Η υποκεφαλίδα επανασυναρμολόγησης παίρνει την τιμή 1 αν χρησιμοποιείται η λειτουργία

επανασυναρμολόγησης ή την τιμή 0 αν δεν χρησιμοποιείται η λειτουργία επανασυναρμολόγησης.

- **#0 bit:** Για το uplink χρησιμοποιείται το Grant Management subheader, που παίρνει την τιμή 1 αν χρησιμοποιείται και την τιμή 0 αν δεν χρησιμοποιείται. Για το downlink χρησιμοποιείται το FAST-FEEDBACK Allocation subheader, που παίρνει την τιμή 1 αν χρησιμοποιείται και την τιμή 0 αν δεν χρησιμοποιείται [3].

## 7.5 ΔΙΑΔΙΚΑΣΙΑ ΑΡΧΙΚΟΠΟΙΗΣΗΣ ΔΙΚΤΥΟΥ ΚΑΙ ΕΙΣΟΔΟΥ ΣΤΟ ΔΙΚΤΥΟ

Η διαχείριση σύνδεσης, μεταξύ του σταθμού συνδρομητή και του σταθμού βάσης, περιέχει τρία είδη συνδέσεων. Τα τρία είδη συνδέσεων είναι η βασική σύνδεση διαχείρισης, η πρωτεύουσα σύνδεση διαχείρισης και η δευτερεύουσα σύνδεσης διαχείρισης. Στη βασική σύνδεση διαχείρισης μεταδίδονται σύντομα και επείγοντα (MAC, radio link control) μηνύματα, παρέχοντας καλύτερο επίπεδο ποιότητας για τη γρήγορη και ασφαλή μεταφορά.

Στην πρωτεύουσα σύνδεση διαχείρισης μεταδίδονται μεγαλύτερα μηνύματα, τα οποία έχουν μεγάλη αντοχή στην καθυστέρηση, όπως μηνύματα για την αυθεντικοποίηση και την εγκατάσταση συνδέσεων. Στην δευτερεύουσα σύνδεση διαχείρισης μεταδίδονται μηνύματα για την διαχείριση των UDP υπηρεσιών όπως μηνύματα DHCP, RIP ή SNMP. Οι συνδέσεις διαχείρισης περιέχουν ένα αναγνωριστικό αριθμό (Connection ID, CID) 16 bit. Το υπόστρωμα MAC υποστηρίζει αρκετές συνδέσεις για γενικές λειτουργίες όπως αρχικοποίηση του δικτύου, broadcast και multicast εκπομπές.

Ο σταθμός συνδρομητή για να αποκτήσει πρόσβαση στο δίκτυο ακολουθεί κάποιες διαδικασίες. Ο σταθμός συνδρομητή ανιχνεύει το κατωφερές σήμα του βασικού σταθμού και συγχρονίζεται με αυτό. Αν δεν έχει χρησιμοποιηθεί πρόσφατα κάποιο κατωφερές κανάλι, ο σταθμός συνδρομητή ανιχνεύει όλα τα κανάλια της κατωφερούς ζώνης συχνοτήτων. Μόλις ανιχνευτεί και επιλεγεί ένα κανάλι, ο σταθμός συνδρομητή συγχρονίζεται με αυτό το κανάλι και ανιχνεύει κατά περιόδους τα preamble πλαίσια. Αν έχει χρησιμοποιηθεί πρόσφατα ένα κατωφερές κανάλι, ο σταθμός συνδρομητή συγχρονίζεται πρώτα με αυτό, με τις ίδιες παραμέτρους.

Μετά τον συγχρονισμό του σήματος του σταθμού συνδρομητή με το σταθμό βάσης, γίνεται αναζήτηση των μηνυμάτων Descriptor του ανερχόμενου και του κατερχόμενου καναλιού (Uplink/Downlink Channel Descriptor, UCD/DCD), που εκπέμπει ο σταθμός βάσης. Τα μηνύματα αυτά, περιέχουν πληροφορίες για τα φυσικά χαρακτηριστικά των καναλιών, όπως τον τύπο διαμόρφωσης και τον αλγόριθμο διόρθωσης σφαλμάτων.

Με τη διαδικασία ranging ένας σταθμός συνδρομητή μπορεί να συγχρονιστεί με το σήμα και να αποδεχτεί τα αναγνωριστικά της σύνδεσης (CID). Μόλις ολοκληρωθεί η διαδικασία ranging, ο σταθμός συνδρομητή αποστέλλει τις παραμέτρους των δυνατοτήτων που διαθέτει και υποστηρίζει, όπως τον τύπο διαμόρφωσης και τον αλγόριθμο διόρθωσης σφαλμάτων για την αποδοχή ή την απόρριψη τους από τον σταθμό βάσης.

Έπειτα, ακολουθεί η διαδικασία πιστοποίησης της ταυτότητας και εξουσιοδότησης του σταθμού συνδρομητή. Ο σταθμός βάσης παρέχει ένα αναγνωριστικό πελάτη και ένα κλειδί στο σταθμό συνδρομητή για να τα χρησιμοποιεί κατά την πραγματοποίηση της σύνδεσης.

Μόλις ολοκληρωθεί η διαδικασία αυθεντικοποίησης και εξουσιοδότησης, ο σταθμός συνδρομητή ακολουθεί την διαδικασία εγγραφής (registration). Η διαδικασία εγγραφής περιλαμβάνει την αποστολή αίτησης εγγραφής (registration request) από τον σταθμό συνδρομητή στον σταθμό βάσης. Ο σταθμός βάσης αποστέλλει ένα μήνυμα απάντησης εγγραφής (registration response). Ο σταθμός συνδρομητή αποκτά την διεύθυνση IP μέσω του πρωτοκόλλου DHCP και τις παραμέτρους σύνδεσης από τον σταθμό βάσης[1][3].

## 7.6 MOBILE WiMAX

Το Mobile WiMAX, δηλαδή το πρότυπο 802.16e, βασίζεται στο πρότυπο IEEE 802.16-2004 με κάποιες τροποποιήσεις. Οι τροποποιήσεις αυτές έχουν στόχο την άμεση ασύρματη κινητή πρόσβαση των πελατών σε ένα δίκτυο WiMAX. Το πρότυπο IEEE 802.16e χρησιμοποιεί την τεχνική διαμόρφωσης Scalable OFDMA, η οποία περιέχει πολλαπλά φέροντα και χρησιμοποιεί sub-channelization.

Η Scalable OFDMA παρέχει διαφορετική κατανομή του φάσματος ανάλογα με τις ανάγκες του συστήματος Mobile WiMAX. Η Scalable OFDMA ρυθμίζει το μέγεθος

του FFT και καθορίζει την απόσταση των subcarriers. Η Scalable OFDMA χρησιμοποιεί ένα σταθερό εύρος ζώνης του subcarrier στα 11.2 KHz και ο αριθμός των subcarriers εξαρτάται από το εύρος του καναλιού που είναι από 1.25 MHz ως 20 MHz. Για το εύρος 1.25 MHz του καναλιού υπάρχουν 128 subcarriers και για το εύρος 20 MHz του καναλιού υπάρχουν 2048 subcarriers.

Το πρότυπο IEEE 802.16e χρησιμοποιεί τις συχνότητες από 2 έως 11 GHz, με χρήση μη-οπτικής επαφής. Το πρότυπο αυτό χρησιμοποιεί τη TDD και κεραίες MIMO. Η πρώτη έκδοση Realease 1 Profile χρησιμοποιεί μόνο την TDD, ενώ σε μελλοντικές εκδόσεις θα συμπεριληφθεί και η FDD. Επίσης, για κάθε τομέα με εύρος καναλιού 10 MHz, προσφέρει μέγιστο ρυθμό μετάδοσης δεδομένων 63 Mbps για την κατωφερή ζεύξη και μέγιστο ρυθμό μετάδοσης δεδομένων 28 Mbps για την ανωφερή ζεύξη.

Το Mobile WiMAX για την ελαχιστοποίηση της κατανάλωσης ισχύος περιλαμβάνει τις λειτουργίες Sleep Mode και Idle Mode. Στη λειτουργία Sleep Mode, το κινητό τερματικό για συγκεκριμένους χρόνους δεν παράγει κίνηση, ούτε στην ανωφερή ζεύξη ούτε στην κατωφερή ζεύξη, με το σταθμό βάσης που έχει επικοινωνία. Με αυτήν την λειτουργία μειώνεται η κατανάλωση ισχύος του τερματικού και οι καταναλώσιμοι πόροι του σταθμού βάσης.

Στη λειτουργία Idle Mode το κινητό τερματικό κατά διαστήματα γίνεται διαθέσιμο, ώστε να γίνει μετάδοση δεδομένων κάτω ζεύξης χωρίς να γίνεται εγγραφή (register) σε κάποιο σταθμό βάσης[6].

## 7.7 ΣΥΓΚΡΙΣΗ ΠΡΟΤΥΠΩΝ IEEE 802.16 ΚΑΙ IEEE 802.11

Τα πρότυπα IEEE 802.16 και IEEE 802.11 δημιουργήθηκαν από τον ίδιο οργανισμό (IEEE) και σχεδιάστηκαν για την ασύρματη δικτύωση υψηλού εύρους. Το πρότυπο IEEE 802.16 παρέχει εύρος μετάδοσης από 8 έως 50 χιλιομέτρων ενώ το πρότυπο IEEE 802.11 παρέχει εύρος μετάδοσης μερικών εκατοντάδων μέτρων (802.11n: 250 μέτρα). Το πρότυπο IEEE 802.11 χρησιμοποιεί τις μη-αδειοδοτημένες ζώνες συχνοτήτων, ενώ το πρότυπο IEEE 802.16 χρησιμοποιεί ένα μεγάλο εύρος συχνοτήτων που περιλαμβάνει αδειοδοτημένες, αλλά και μη-αδειοδοτημένες ζώνες συχνοτήτων.

Το πρότυπο IEEE 802.16 παρέχει κυρίως υπηρεσίες σε κτίρια, στα οποία απαιτούνται υψηλότερου κόστους επικοινωνιακοί εξοπλισμοί, ενώ δεν χρησιμοποιείται συνήθως από οικιακούς χρήστες καθώς οι ίδιοι δεν είναι διατεθειμένοι να δαπανήσουν χρήματα για υψηλού κόστους επικοινωνιακό εξοπλισμό. Οι χρήστες μιας κυψέλης 802.16 μπορεί να είναι περισσότεροι και να χρησιμοποιούν περισσότερο εύρος ζώνης από έναν χρήστη μιας τυπικής κυψέλης 802.11.

Τα συστήματα του 802.16 μπορούν να χρησιμοποιούν είτε οπτική επαφή είτε μη οπτική επαφή με χαμηλότερο ρυθμό μετάδοσης 50 Mbps, ενώ τα συστήματα 802.11 χρησιμοποιούν μη οπτική επαφή. Επίσης, το πρότυπο IEEE 802.16 παρέχει υψηλότερη ποιότητα υπηρεσίας από το πρότυπο IEEE 802.11. Το πρότυπο IEEE 802.16 (στο επίπεδο MAC) παρέχει στους χρήστες, εφόσον το επιθυμούν, εγγυημένο ρυθμό μετάδοσης και υπηρεσία best-effort σε χρήστες που βρίσκονται στον ίδιο σταθμό βάσης. Αν στον ίδιο σταθμό βάσης καλύπτονται δύο χρήστες, ο ένας χρήστης μπορεί να έχει εξασφαλισμένη και σταθερή ποιότητα υπηρεσίας και ο άλλος χρήστης να χρησιμοποιεί απλή IP κίνηση best-effort για την αποστολή και τη λήψη μηνυμάτων. Ενώ, στο πρότυπο IEEE 802.11 οι χρήστες έχουν την ίδια ποιότητα υπηρεσίας όταν καλύπτονται από το ίδιο Access Point.

Το IEEE 802.16 σχεδιάστηκε για να παρέχει ευρυζωνική ασύρματη πρόσβαση, ενώ το IEEE 802.11 σχεδιάστηκε για την κινητικότητα των ενσύρματων τοπικών δικτύων[3][4] .

## 7.8 ΣΥΝΟΨΗ

Σε αυτό το κεφάλαιο παρουσιάστηκε η τεχνολογία WiMAX, η οποία είναι καινούρια τεχνολογία και ακόμα βρίσκεται σε πιλοτικό στάδιο. Η τεχνολογία WiMAX έχει ως στόχο την ασύρματη πρόσβαση ευρείας ζώνης για σταθερά και για κινητά συστήματα, καλύπτοντας μεγάλες αποστάσεις. Η τεχνολογία αυτή χρησιμοποιείται με δύο τρόπους υπηρεσίας, με χρήση οπτικής επαφής και με χρήση μη-οπτικής επαφής. Στο επόμενο κεφάλαιο αναφέρονται οι αλγόριθμοι και οι μέθοδοι που χρησιμοποιούνται για την ασφάλεια των τεχνολογιών που περιγράφηκαν στα προηγούμενα κεφάλαια αλλά και σε αυτό.

# 8. ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

## 8.1 ΕΙΣΑΓΩΓΗ

Τα ασύρματα δίκτυα είναι περισσότερο επιρρεπή στην προσβολή της ασφάλειας, επειδή οι μεταδόσεις των πληροφοριών γίνονται μέσω του αέρα. Ο έλεγχος πρόσβασης σε ένα ασύρματο δίκτυο μπορεί να είναι ελλιπής ή ακόμα και να απουσιάζει, με αποτέλεσμα να προσβάλλεται η ασφάλεια των δεδομένων. Όταν δεν υπάρχει ο έλεγχος πρόσβασης, τότε οποιοσδήποτε μπορεί να επιτεθεί στο δίκτυο με αποτέλεσμα να βρεθούν εκτεθειμένα τα δεδομένα. Παρακάτω περιγράφονται οι βασικές έννοιες της ασφάλειας, οι εισβολείς, οι επιθέσεις και οι μηχανισμοί που προστατεύουν τα δεδομένα που μεταδίδονται.

## 8.2 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Οι βασικές έννοιες της ασφάλειας των ασύρματων δικτύων είναι η Εμπιστευτικότητα, η Ακεραιότητα, η Διαθεσιμότητα, η Εξουσιοδοτημένη χρήση και η Αυθεντικοποίηση [1][3][4], οι οποίες περιγράφονται αναλυτικά στη συνέχεια.

### Εμπιστευτικότητα ή εξασφάλιση απορρήτου

Η εμπιστευτικότητα (confidentiality) είναι η πρόληψη για ανάγνωση και αντιγραφή των δεδομένων από μη εξουσιοδοτημένους χρήστες. Η εμπιστευτικότητα περιλαμβάνει την ιδιωτικότητα (privacy) που αφορά την προστασία των προσωπικών δεδομένων και τη μυστικότητα (secrecy) που αφορά την προστασία των δεδομένων του χρήστη, ο οποίος μπορεί να είναι ένα άτομο ή ακόμα και ένας οργανισμός.

### Ακεραιότητα

Η ακεραιότητα (integrity) είναι η πρόληψη μεταβολής πληροφοριών από μη εξουσιοδοτημένους χρήστες. Η δημιουργία, η τροποποίηση και η διαγραφή των δεδομένων γίνεται μόνο από τους εξουσιοδοτημένους χρήστες.

### Διαθεσιμότητα

Η διαθεσιμότητα (availability) είναι η ιδιότητα προσπέλασης πληροφοριών, πόρων και υπηρεσιών σε εξουσιοδοτημένους χρήστες, χωρίς αδικαιολόγητη

καθυστέρηση προσπέλασης υπηρεσιών και η αποφυγή επιθέσεων άρνησης παροχής υπηρεσιών.

Αυθεντικοποίηση

Η αυθεντικοποίηση χρηστών (authentication user) περιλαμβάνει την πιστοποίηση των χρηστών που επιθυμούν να επικοινωνήσουν μεταξύ τους. Η πιστοποίηση παρέχει στον αποστολέα τη διαβεβαίωση ότι ο χρήστης που θέλει να επικοινωνήσει, είναι ο πραγματικός αποδέκτης. Η αυθεντικοποίηση μηνυμάτων προσφέρει στον παραλήπτη τη διαβεβαίωση ότι ο αποστολέας, έχει εξουσιοδοτημένη χρήση του συστήματος και το σημαντικότερο ότι αυτός είναι ο πραγματικός αποστολέας.

Εξουσιοδοτημένη χρήση

Η εξουσιοδοτημένη χρήση (authorization) είναι η βεβαίωση ότι οι χρήστες μπορούν να προσπελάσουν ένα υπολογιστικό σύστημα και να το χρησιμοποιούν με προκαθορισμένους τρόπους. Η εξουσιοδοτημένη χρήση ακολουθείται μετά από τη διαδικασία της αυθεντικοποίησης των χρηστών.

## 8.3 ΕΠΙΘΕΣΕΙΣ

Οι επιθέσεις σε ένα σύστημα ασύρματου δικτύου, αλλά και σε συστήματα υπολογιστών, συμβαίνουν από κακόβουλους χρήστες, οι οποίοι επιτίθενται ανάλογα με τα κίνητρά τους. Παρακάτω αναφέρονται οι κατηγορίες των εισβολέων καθώς και τα κίνητρά τους. Επιπλέον, περιγράφονται και οι επιθέσεις που πραγματοποιούνται από τους εισβολείς.

### 8.3.1 ΚΑΤΗΓΟΡΙΕΣ ΕΙΣΒΟΛΕΩΝ

Οι κακόβουλοι χρήστες που επιτίθενται στα ασύρματα δίκτυα ονομάζονται hackers και χωρίζονται σε τέσσερις κατηγορίες, στους accidental users, στους script kiddies, στους casual hackers και στους skilled hackers[3].

Οι accidental users είναι οι χρήστες που παραβιάζουν ένα ελεύθερο ασύρματο δίκτυο, το οποίο ανιχνεύεται τυχαία.

Οι script kiddies είναι οι επίδοξοι hackers, οι οποίοι θεωρούν την επίθεση ως παιχνίδι ή ως πρόκληση. Οι script kiddies προμηθεύονται από το διαδίκτυο κάποια

ειδικά προγράμματα για να εισβάλλουν σε ένα δίκτυο με χαμηλό επίπεδο προστασίας. Οι εισβολείς αυτοί γνωρίζουν πως θα χρησιμοποιήσουν τα προγράμματα αυτά αλλά δεν γνωρίζουν πως ακριβώς λειτουργούν.

Οι casual hackers είναι πολύ καλοί γνώστες της τεχνολογίας. Γνωρίζουν πως να αποκωδικοποιούν τα πακέτα καταγραφής και να συλλέγουν χρήσιμες για αυτούς πληροφορίες. Συνήθως, οι casual hackers μπαίνουν σε ένα σύστημα από πρόκληση.

Οι skilled hackers διαθέτουν τεχνογνωσία και άφθονο χρόνο για να αποκαλύψουν τις αδυναμίες της κρυπτογραφίας. Οι skilled hackers μπορεί να εισβάλλουν σε ένα σύστημα από πρόκληση ή από οικονομικό όφελος.

Οι περισσότερες επιθέσεις πραγματοποιούνται με συγκεκριμένα κίνητρα τα οποία χωρίζονται στις παρακάτω κατηγορίες[4]. Η πρώτη κατηγορία περιλαμβάνει τους εισβολείς που έχουν ως κίνητρο το οικονομικό όφελος ή την εκδίκηση. Οι κακόβουλοι χρήστες που εισβάλουν σε ένα σύστημα ενός οργανισμού από εκδίκηση, συνήθως είναι δυσαρεστημένοι υπάλληλοι ή πρώην υπάλληλοι, που αναζητούν κατάλληλα εργαλεία για να επιτεθούν στις αδυναμίες του οργανισμού που εργαζόντουσαν ή συνεχίζουν να εργάζονται. Οι κακόβουλοι χρήστες που έχουν οικονομικό όφελος εισβάλουν είτε σε βάσεις δεδομένων πιστωτικών καρτών, είτε σε μη δημοσιευμένα χρηματοοικονομικά στοιχεία του οργανισμού, κλέβοντας πληροφορίες προς όφελος τους, αγοράζοντας μετοχές ή πουλώντας τις πληροφορίες αυτές.

Η δεύτερη κατηγορία περιλαμβάνει τους εγώ-εισβολείς, οι οποίοι εισβάλλουν σε ξένα συστήματα μόνο και μόνο για προσωπική τους ευχαρίστηση και επιδεικνύοντας τις ικανότητές τους, δηλαδή τη δυνατότητα να εισβάλλουν παντού εύκολα και γρήγορα. Αυτοί οι κακόβουλοι χρήστες είναι γνώστες των μεθόδων επίθεσης της ασφάλειας, των αδυναμιών της ασφάλειας και δημιουργούν καινούριες μεθόδους που θα έχουν επιτυχή επίθεση, όπως η κρυπτανάλυση.

### 8.3.2 ΚΑΤΗΓΟΡΙΕΣ ΕΠΙΘΕΣΕΩΝ

Οι επιθέσεις των ασύρματων δικτύων χωρίζονται σε δύο τύπους, στις ενεργές και στις παθητικές επιθέσεις. Οι ενεργές επιθέσεις των εισβολέων έχουν ως κύριο στόχο την τροποποίηση ή τη δημιουργία απατηλών δεδομένων και περιεχομένων

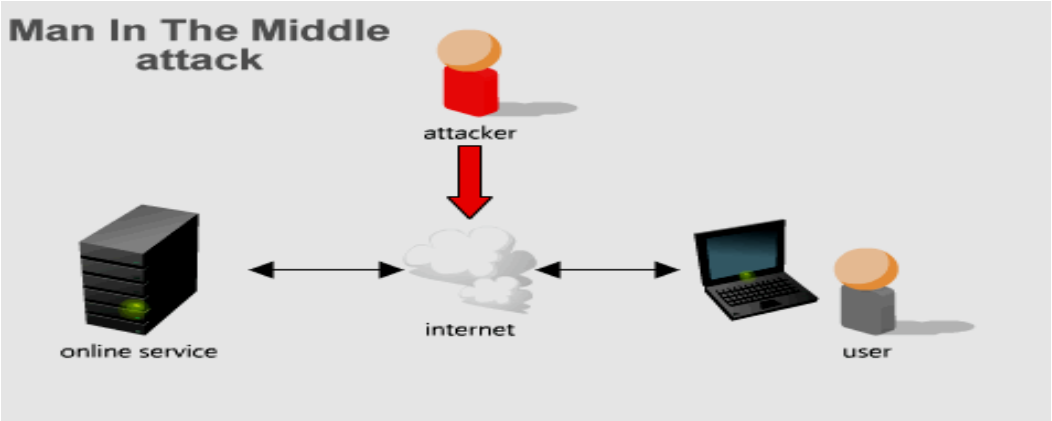
των πληροφοριών μέσω του διαδικτύου. Στις ενεργές επιθέσεις περιλαμβάνονται η διακοπή εξυπηρέτησης, η μεταμφίεση, η επανεκπομπή (replay), η πλαστογραφία και η τροποποίηση των δεδομένων. Οι παθητικές επιθέσεις έχουν ως στόχο την υποκλοπή των δεδομένων κατά την μετάδοση και την καταμέτρηση των ιδιοτήτων της ασύρματης μετάδοσης όπως το μήκος, το χρόνο και την συχνότητα για την αναζήτηση χρήσιμων πληροφοριών. Στις παθητικές επιθέσεις περιλαμβάνονται η ανάλυση της κυκλοφορίας των σταθμών και η υποκλοπή.

Αναλυτικότερα οι κατηγορίες των επιθέσεων διακρίνονται [1][3][4]:

- **Ανάλυση της κίνησης των σταθμών (traffic analysis).** Οι εισβολείς πριν προβούν στην ενεργητική επίθεση, λαμβάνουν τις κατάλληλες πληροφορίες του δικτύου, όπως τα πρωτόκολλα που χρησιμοποιεί, την δραστηριότητά του, τα ενεργά Access Points του δικτύου και τις τοποθεσίες τους. Οι εισβολείς συλλέγουν τα πεδία του πλαισίου beacon (beacon frames) που στέλνονται κατά χρονικά διαστήματα από τα Access Points και τα χρησιμοποιούν για διάφορους σκοπούς όπως για την μεταμφίεση, την υποκλοπή και την επίθεση ενδιάμεσου. Τα πλαίσια beacon (beacon frames) περιέχουν πληροφορίες για τα Access Points όπως το SSID, τους υποστηριζόμενους ρυθμούς μετάδοσης και άλλα. Το SSID (Service Set Identifier) είναι μία ακολουθία χαρακτήρων όπου δίνει ένα και μοναδικό όνομα σε ένα ασύρματο δίκτυο, πολλές φορές αναφέρεται και ως όνομα δικτύου.
- **Άρνηση Εξυπηρέτησης (Denial of Service).** Η επίθεση Άρνησης Εξυπηρέτησης πραγματοποιείται όταν ο εισβολέας πλημμυρίζει (flooding) το ασύρματο δίκτυο με παράνομη κυκλοφορία πακέτων, αποτρέπει την πρόσβαση του εξουσιοδοτημένου χρήστη σε αυτό ή επιβραδύνει την κυκλοφορία στο ασύρματο δίκτυο που χρησιμοποιεί ο εξουσιοδοτημένος χρήστης. Επίσης προσβάλει τη διαθεσιμότητα του δικτύου.
- **Εμπλοκή (jamming).** Οι επιθέσεις Εμπλοκής οδηγούν στην Άρνηση Εξυπηρέτησης και πραγματοποιείται όταν δημιουργούνται παρεμβολές και θόρυβοι στη ζώνη συχνοτήτων. Η Άρνηση εξυπηρέτησης με χρήση παρεμβολών μπορεί να δημιουργηθεί αθέλητα από φούρνους μικροκυμάτων, ενδοεπικοινωνία και άλλες παρόμοιες μικροσυσκευές.
- **Υποκλοπή (interception ή eavesdropping).** Η παθητική υποκλοπή πραγματοποιείται για την παρακολούθηση των πληροφοριών που

μεταφέρονται μέσω του δικτύου καθώς επίσης και τα χαρακτηριστικά των πακέτων που μεταδίδονται και οδηγεί στην προσβολή της ιδιωτικότητας των δεδομένων. Μετά την παθητική υποκλοπή ακολουθεί η ενεργητική υποκλοπή, στην οποία γίνεται η καταγραφή και ενδεχομένως η τροποποίηση των δεδομένων του αποστολέα ή του παραλήπτη χωρίς να αντιληφθούν το παραμικρό. Επίσης, με την υποκλοπή γνωστοποιούνται στον εισβολέα, ο κωδικός και το όνομα πρόσβασης του πρόσφατα συνδεδεμένου χρήστη, με αποτέλεσμα την μετέπειτα χρησιμοποίησή τους από τον εισβολέα για την πρόσβαση του στο δίκτυο (επίθεση επανεκπομπής).

- **Masquerading/spoofing.** Η μεταμφίεση/προσποίηση γίνεται όταν μια συσκευή διαδικτύου του εισβολέα προσπαθήσει να προσποιηθεί μια εξουσιοδοτημένη συσκευή και ξεγελώντας το δίκτυο-στόχο, ο εισβολέας λαμβάνει όλα τα δικαιώματα πρόσβασης.
- **ARP Spoofing ή ARP poisoning.** Μετά την επίθεση με υποκλοπή, ο εισβολέας, αφού αποκτήσει πρόσβαση στο δίκτυο, απαντάει με τη δική του MAC διεύθυνση στις ARP αιτήσεις άλλων σταθμών, με αποτέλεσμα να μάθει τις IP διευθύνσεις τους και να τροποποιεί τον πίνακα ARP. Επίσης ο εισβολέας λαμβάνει ευαίσθητες πληροφορίες που απευθύνονται στους επιτιθέμενους σταθμούς.
- **Ενδιάμεσο άτομο (man-in-the-middle).** Η επίθεση του ενδιάμεσου ατόμου προσβάλει την ακεραιότητα και την εμπιστευτικότητα της συνόδου. Η επίθεση αυτή πραγματοποιείται ως εξής: ο εισβολέας εγκαθιστά ένα ψεύτικο (μη-εξουσιοδοτημένο) Access Point, το οποίο αναγνωρίζεται ως αληθινό. Στην συνέχεια, όταν μια κινητή συσκευή αντιληφθεί το ψεύτικο Access Point προσπαθεί να συνδεθεί μαζί του. Το ψεύτικο Access Point αντιγράφει όλα τα ληφθέντα μηνύματα από το αληθινό, ανταλλάσσοντας την MAC διεύθυνση με τη δική του και τα προωθεί στο νόμιμο Access Point, και αντίστροφα. Αυτό έχει ως αποτέλεσμα το ψεύτικο Access Point να παρεμβάλει ως ενδιάμεσος στην επικοινωνία μεταξύ της συσκευής και του νόμιμου Access Point.




ΕΙΚΟΝΑ 104: ΕΠΙΘΕΣΗ ΕΝΔΙΑΜΕΣΟΥ ΑΤΟΜΟΥ

Σε αυτή την επίθεση, ο εισβολέας τροποποιεί τα δεδομένα. Η τροποποίηση των δεδομένων γίνεται με την τακτική store-and-forward, το οποίο σημαίνει ότι πρώτα ο εισβολέας αποθηκεύει τα δεδομένα, τα τροποποιεί και κάποια άλλη χρονική στιγμή τα προωθεί. Μία ακόμα τακτική για τη τροποποίηση των δεδομένων είναι με άμεση τροποποίηση των δεδομένων.

- **Session Hijacking.** Η επίθεση Session Hijacking είναι παρόμοια με την επίθεση ενδιάμεσου ατόμου με την διαφορά ότι ο εισβολέας με το ψεύτικο Access Point στέλνει μήνυμα διακοπής της συσχέτισης στο θύμα. Το θύμα πιστεύει ότι έχει γίνει διακοπή της συσχέτισης, ενώ το αληθινό Access Point λειτουργεί κανονικά και ο εισβολέας έχει τον έλεγχο της συνόδου.
- **Rogue access point.** Η επίθεση Rogue access point είναι μία παραλλαγή της επίθεσης ενδιάμεσου ατόμου. Το ψεύτικο Access Point εγκαθίσταται με ένα έγκυρο SSID ενός δικτύου. Το ψεύτικο Access Point έχει ισχυρότερο σήμα, με αποτέλεσμα η συσκευή πελάτη να ανιχνεύει και να συνδέεται με αυτό το Access Point. Ο εισβολέας, αφού συνδεθεί με τη συσκευή πελάτη, μπορεί να καταγράψει σημαντικές πληροφορίες όπως αιτήσεις αυθεντικοποίησης και μυστικά κλειδιά.
- **Εξουθενωτικές επιθέσεις (brute force attacks) κατά των κωδικών των σημείων πρόσβασης.** Οι εισβολείς δοκιμάζουν όλους τους δυνατούς συνδυασμούς για να προσβάλλουν τους κωδικούς ή τα κλειδιά που χρησιμοποιούν τα σημεία πρόσβασης για να συνδεθούν με τους ασύρματους σταθμούς-πελάτες.

- **Επιθέσεις λεξικού (dictionary attacks).** Οι επιθέσεις λεξικού περιλαμβάνουν μια βάση δεδομένων που περιέχει όλες τις λέξεις κάθε γλώσσας όπως κύρια ονόματα, γεωγραφικά ονόματα, ονόματα ζώων και άλλα, που να μοιάζουν με τους εύκολα απομνημονευμένους κωδικούς που χρησιμοποιούν οι απλοί χρήστες. Με αυτή τη βάση δεδομένων είναι πολύ εύκολο να σπάσουν αυτούς τους κωδικούς για αυτό όταν χρησιμοποιούνται λέξεις για κωδικούς καλό θα είναι τα γράμματα να εναλλάσσονται με κεφαλαία γράμματα, μικρά γράμματα και αριθμητικά ώστε η ασφάλεια να είναι ισχυρή.
- **Αλγοριθμικές επιθέσεις (algorithmic attacks).** Οι εισβολείς για να χρησιμοποιήσουν την αλγοριθμική επίθεση, θα πρέπει να γνωρίζουν πολύ καλά τη λειτουργία, τους μηχανισμούς όλων των αλγορίθμων κρυπτογράφησης, επειδή αν ένα ψηφίο διαρρεύσει κάποια στιγμή τότε είναι εύκολος ο συνδυασμός του κλειδιού. Ο χρόνος για να ανακαλύψει κανείς το κλειδί είναι ανάλογος με το μήκος του κλειδιού. Είναι πιο εύκολο να «σπάσει» κανείς έναν αλγόριθμο με μήκος κλειδιού 40-bit από έναν αλγόριθμο με μήκος κλειδιού 128-bit.

## 8.4 Η ΑΣΦΑΛΕΙΑ ΣΤΟ ΑΡΧΙΚΟ ΠΡΟΤΥΠΟ IEEE 802.11 ΜΕ ΤΗ ΜΕΘΟΔΟ WEP

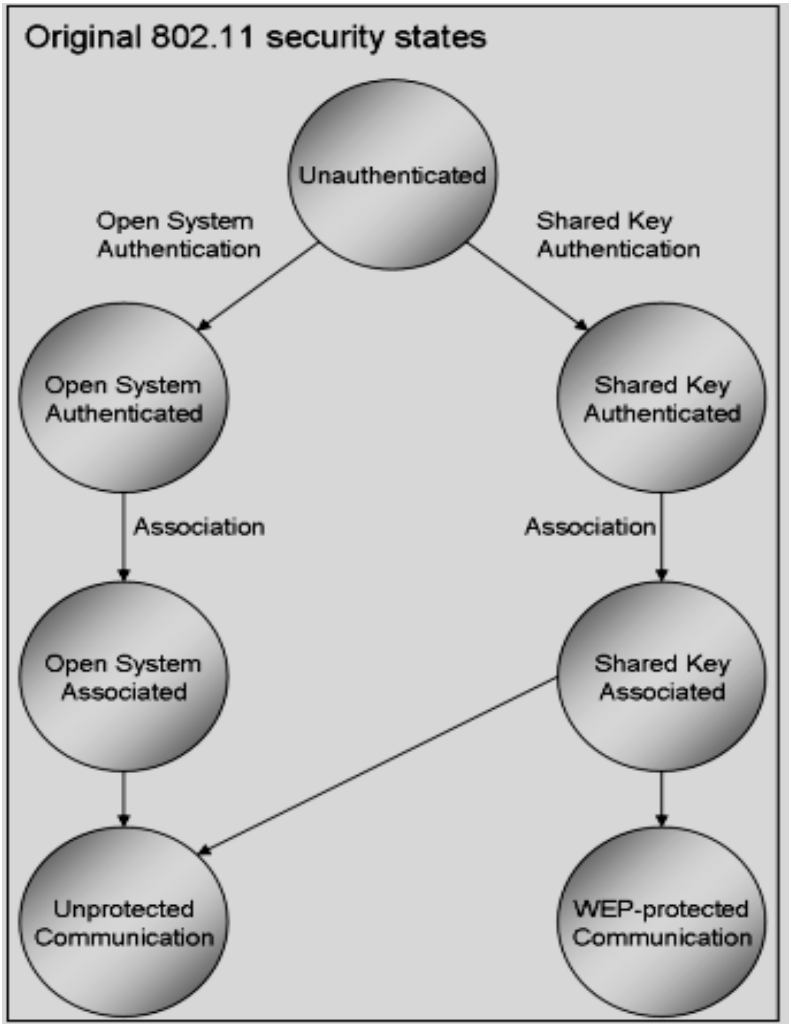
Το αρχικό πρότυπο IEEE 802.11, χρησιμοποιούσε για την ασφάλεια τη μέθοδο WEP (Wired Equivalent Privacy), που την χρησιμοποιούν τα ενσύρματα δίκτυα. Η μέθοδος WEP χρησιμοποιείται για την προστασία κατά της υποκλοπής και εξασφαλίζει τη πιστοποίηση ότι τα μηνύματα προέρχονται από αυθεντική πηγή.

Η μέθοδος WEP χρησιμοποιεί την κρυπτογράφηση των πλαισίων του υποστρώματος MAC κατά την μετάδοση τους για την εμπιστευτικότητα των δεδομένων.

Η μέθοδος WEP έχει τις παρακάτω ιδιότητες[4]:

- **Είναι αρκετά ισχυρή.** Κατά την μετάδοση των πλαισίων, κάθε πλαίσιο μεταδίδεται με ένα διάνυσμα ανάθεσης (Initialization Vector) αρχικών τιμών και τη χρήση ενός μυστικού κλειδιού (secret key), με τη χρήση μιας γεννήτριας ψευδοτυχαίων αριθμών που δυσκολεύει την εξουθενωτική επίθεση.
- **Είναι αυτό-συγχρονιζόμενη.** Η μέθοδος WEP συγχρονίζεται ξανά σε περίπτωση απώλειας πακέτων από την διανομή βέλτιστης προσπάθειας.

- **Είναι αποτελεσματική.** Η μέθοδος WEP είναι αποτελεσματική και περιλαμβάνεται είτε στο υλικό είτε στο λογισμικό.




**ΕΙΚΟΝΑ 105: ΚΑΤΑΣΤΑΣΕΙΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΑΡΧΙΚΟΥ ΠΡΟΤΥΠΟΥ**

Το IEEE 802.11 χρησιμοποιεί τη μέθοδο πιστοποίησης ανοικτού συστήματος (Open system) και τη μέθοδο πιστοποίησης κοινού κλειδιού (shared-key). Η μέθοδος ανοικτού συστήματος επιτρέπει την πιστοποίηση σε οποιονδήποτε σταθμό. Απλά ο σταθμός στέλνει μία αίτηση στο Access Point και το Access Point στέλνει μια απάντηση επιτυχίας. Η μέθοδος πιστοποίησης κοινού κλειδιού βασίζεται στο προεπιλεγμένο σύνολο κλειδιών, που διανέμονται μεταξύ των ασύρματων συσκευών και των ασύρματων Access Points. Η επικοινωνία μεταξύ του σταθμού-πελάτη και του Access Point γίνεται μόνο με τη χρήση του σωστού κλειδιού, αλλιώς απορρίπτεται το αίτημα για επικοινωνία. Τα δεδομένα κρυπτογραφούνται πριν τη μετάδοση και ελέγχονται για την ακεραιότητα τους. Η αποκρυπτογράφηση των δεδομένων πραγματοποιείται με την χρήση του σωστού

κλειδιού για την αποφυγή της απόκτησης πρόσβασης από μη εξουσιοδοτημένα άτομα. Κάθε δίκτυο περιέχει μια λίστα πρόσβασης των διευθύνσεων MAC όλων των επιτρεπόμενων σταθμών που επιθυμούν να συνδεθούν με το δίκτυο.

### 8.4.1 ΠΙΣΤΟΠΟΙΗΣΗ ΣΤΟ WEP

Η πιστοποίηση με χρήση κοινού κλειδιού λαμβάνεται από ένα σταθμό, έπειτα από αίτηση που έστειλε ο σταθμός σε μορφή πλαισίου διαχείρισης σε ένα σταθμό πιστοποίησης.

Ο σταθμός πιστοποίησης στέλνει ένα μήνυμα απάντησης για την επιτυχημένη πιστοποίηση, με περιεχόμενο το κείμενο πρόκλησης που αποτελεί το πλαίσιο διαχείρισης πιστοποίησης. Το κείμενο πρόκλησης δημιουργείται από την γεννήτρια ψευδοτυχαίων αριθμών χρησιμοποιώντας το κοινό μυστικό κλειδί και το τυχαίο διάνυσμα ανάθεσης αρχικών τιμών.

Μόλις λάβει ο σταθμός το πλαίσιο διαχείρισης πρόκλησης, κρυπτογραφεί το αντιγραμμένο περιεχόμενο του κειμένου με το κοινό μυστικό κλειδί και με το διάνυσμα ανάθεσης αρχικών τιμών, το τοποθετεί στο σώμα ενός πλαισίου διαχείρισης και το στέλνει στον σταθμό πιστοποίησης. Ο σταθμός πιστοποίησης αποκρυπτογραφεί το πλαίσιο, έπειτα ελέγχει την τιμή ελέγχου ακεραιότητας (Integrity Check Value) CRC, το οποίο έχουμε αναλύσει σε προηγούμενο κεφάλαιο, και αν αντιστοιχεί με το κείμενο πρόκλησης του αρχικού μηνύματος που στάλθηκε, τότε η πιστοποίηση είναι επιτυχής. Σε αυτή τη μέθοδο δεν διασφαλίζεται ότι ο σταθμός πιστοποίησης γνωρίζει το μυστικό κλειδί, με αποτέλεσμα να υπάρχει η δυνατότητα για επίθεση rogue access point. Επίσης, μπορεί να υπάρξει επίθεση παθητικής υποκλοπής, στην οποία ο εισβολέας αποκτά το κείμενο πρόκλησης και το κρυπτογραφημένο κείμενο πρόκλησης και με μια κατάλληλη ανάλυση να βρει το μυστικό κλειδί.

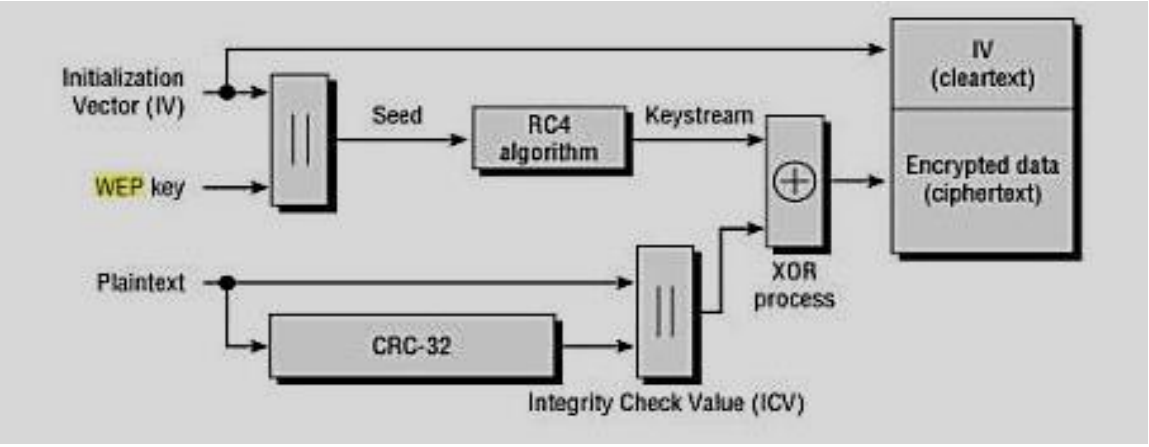
Η πιστοποίηση με χρήση ανοιχτού συστήματος πραγματοποιείται ως εξής: ο σταθμός στέλνει αίτηση αυθεντικοποίησης περιέχοντας την διεύθυνση MAC του. Ο σταθμός πιστοποίησης ελέγχει αν η διεύθυνση αυτή περιέχεται στην προκαθορισμένη λίστα με τις διευθύνσεις MAC, που έχει καθοριστεί από τον διαχειριστή δικτύου. Αν η διεύθυνση MAC δεν περιέχεται στην προκαθορισμένη λίστα ή αυτή η μέθοδος δεν χρησιμοποιείται, ο σταθμός πιστοποίησης αποστέλλει

μήνυμα αποτυχίας στον σταθμό, ενώ στην αντίθετη περίπτωση στέλνει μήνυμα επιτυχίας.

### 8.4.2 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΣΤΟ WEP

Η μέθοδος WEP χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4 (κρυπτογράφηση ροής) για την εμπιστευτικότητα και παίρνει την ακολουθία των δεδομένων του αρχικού κειμένου και τη μετατρέπει σε μια ακολουθία δεδομένων ενός κρυπτογραφημένου κειμένου. Ο κρυπτογραφικός αλγόριθμος RC4 αναπτύχθηκε από το Ron Rivest της εταιρίας RSA Security. Επίσης, η μέθοδος WEP χρησιμοποιεί τον αλγόριθμο CRC (Cyclic Redundancy Code) για την ακεραιότητα των δεδομένων.

Η κρυπτογράφηση ενός πλαισίου με την μέθοδο WEP πραγματοποιείται ως εξής: χρησιμοποιείται ο CRC στο αρχικό κείμενο και η τιμή ελέγχου ακεραιότητας (Integrity Check Value) επισυνάπτεται στο τέλος του αρχικού κειμένου. Έπειτα, με τον συνδυασμό του μυστικού κλειδιού και του διανύσματος ανάθεσης αρχικών (IV) τιμών δημιουργείται μία κλειδοροή (με την γεννήτρια ψευδοτυχαίων αριθμών, pseudorandom number Generator) του RC4. Η κλειδοροή προστίθεται με το αρχικό κείμενο, χρησιμοποιώντας την δυαδική πράξη XOR και έπειτα δημιουργείται το κρυπτογραφημένο κείμενο (ciphertext). Τέλος, το κρυπτογραφημένο κείμενο συνδυάζεται με το διάνυσμα ανάθεσης αρχικών τιμών. Η διαδικασία αυτή παρουσιάζεται στην παρακάτω εικόνα .




**ΕΙΚΟΝΑ 106: ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΕΝΟΣ ΠΛΑΙΣΙΟΥ ΜΕ ΤΗΝ ΜΕΘΟΔΟ WEP**

**Διάνυσμα ανάθεσης αρχικών τιμών (IV, Initialization Vector):** Το τυχαίο διάνυσμα ανάθεσης αρχικών τιμών είναι ένας τυχαίος αριθμός 24-bit που αλλάζει

για κάθε πακέτο. Αυτός ο αριθμός συνδυάζεται με το μυστικό κλειδί για να δημιουργηθεί ένα μεταβλητό κλειδί κρυπτογράφησης.

### 8.4.3 WEP ΚΛΕΙΔΙΑ

Η αποθήκευση και η εισαγωγή των κλειδιών γίνεται χειροκίνητα με δύο μεθόδους χρήσης. Η μια μέθοδος χρησιμοποιεί ένα σύνολο τεσσάρων κλειδιών (default keys), επιλέγοντας ένα από αυτά για κρυπτογράφηση από τον σταθμό και ένα για αποκρυπτογράφηση των δεδομένων από ένα Access Point και αντίστροφα. Η άλλη μέθοδος περιλαμβάνει έναν πίνακα αντιστοίχισης κλειδιών (mapping keys), όπου κάθε διεύθυνση MAC περιέχει διαφορετικά κλειδιά, τα οποία αποθηκεύονται χειροκίνητα σε κάθε συσκευή ή σε κάθε Access Point.

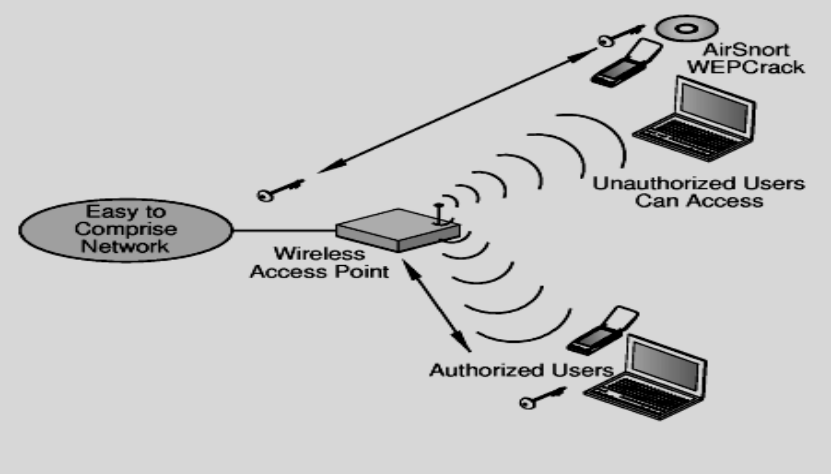
### 8.4.4 ΑΔΥΝΑΜΙΕΣ ΤΗΣ ΜΕΘΟΔΟΥ WEP

Οι αδυναμίες της μεθόδου WEP είναι [1][4][5][11][13]:

- **Η διαχείριση των κλειδιών και το μέγεθος του κλειδιού.** Η μέθοδος WEP δεν καθορίζει μία Διαχείριση κλειδιών, με αποτέλεσμα ο συγχρονισμός αλλαγής κλειδιών από ένα Access Point σε ένα σταθμό-πελάτη να γίνεται σπάνια, επειδή αυτή είναι δύσκολη διαδικασία. Επίσης, τα κλειδιά έχουν χαμηλή ποιότητα αν παραμένουν ίδια για μεγάλο χρονικό διάστημα. Κατά την δημιουργία του αρχικού προτύπου IEEE 802.11, το μήκος του κλειδιού ήταν 40 bit και δεχόταν εύκολα εξουθενωτικές επιθέσεις.
- **Το διάνυσμα ανάθεσης αρχικών τιμών είναι πολύ μικρό.** Το τυχαίο διάνυσμα ανάθεσης αρχικών τιμών στέλνεται ίδιο σε κάθε πακέτο που μεταδίδεται και αν ο εισβολέας το βρει από ένα πακέτο τότε θα μπορεί να αποκρυπτογραφήσει και τα επόμενα ή να πλαστογραφήσει νέα πακέτα. Στη μέθοδο WEP δεν καθορίζεται πως επιλέγεται ή κάθε πότε αλλάζει το διάνυσμα ανάθεσης τιμών. Άλλοτε το διάνυσμα ανάθεσης τιμών χρησιμοποιείται από το μηδέν και αυξάνεται σε κάθε πακέτο και άλλοτε χρησιμοποιείται το τυχαίο διάνυσμα ανάθεσης τιμών, όπου μετά από κάποια πακέτα υπάρχει επαναχρησιμοποίηση των αριθμών.
- **Ο RC4 που χρησιμοποιείται από την μέθοδο WEP έχει αδύναμα κλειδιά.** Η αδυναμία των κλειδιών προέρχεται από τη συσχέτιση των κλειδιών και των κρυπτογραφημένων κειμένων. Εξάλλου τα πρώτα τρία bytes κάθε πακέτου

περιέχουν το διάνυσμα ανάθεσης αρχικών τιμών, το οποίο δεν κρυπτογραφείται.

- **Η αυθεντικοποίηση των δεδομένων μπορεί εύκολα να πλαστογραφηθεί.** Με τη χρήση κοινών μυστικών κλειδιών, όπως αναφέρθηκε παραπάνω, είναι πιο εύκολο να αναγνωριστεί το κλειδί WEP. Αν ο εισβολέας παρακολουθεί το κείμενο πρόκλησης και την κρυπτογραφημένη απάντηση, μπορεί να καθορίσει την ροή του RC4 που χρησιμοποιείται για την κρυπτογράφηση της απάντησης και να κρυπτογραφήσει κάθε κείμενο πρόκλησης που λαμβάνει.




**ΕΙΚΟΝΑ 107: ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΜΗΧΑΝΙΣΜΟΥ WEP**

Υπήρξαν τροποποιήσεις του μήκους του κλειδιού WEP σε 64 bit, σε 128 bit και 256 bit αλλά η αδυναμία του WEP για το διάνυσμα ανάθεσης αρχικών τιμών παρέμεινε. Στο διαδίκτυο υπάρχουν τα εργαλεία WEPCrack και AirSnort, με τα οποία παραβιάστηκε η ασφάλεια του μηχανισμού WEP το 2001. Αυτά τα εργαλεία είναι λογισμικό το οποίο διατίθεται στο διαδίκτυο δωρεάν (freeware). Η παραβίαση της ασφάλειας πραγματοποιήθηκε με την επίθεση - ανάλυση της κίνησης, την καταγραφή των πληροφοριών που συλλέχθηκαν καθώς και με την αποκρυπτογράφηση του κλειδιού με τα εργαλεία WEPCrack και AirSnort[5][10][14].

## 8.5 Η ΑΣΦΑΛΕΙΑ ΤΟΥ 802.11 ΜΕ WPA

Η Wi-Fi Alliance αποφάσισε την αντικατάσταση της μεθόδου WEP, που είχε αρκετές αδυναμίες, με μία μέθοδο πιο ισχυρή για την ασφάλεια των ασύρματων δικτύων. Το μοντέλο που αναπτύχθηκε ήταν το WPA (Wi-Fi Protected Access) για την συμμόρφωση των πρωτοκόλλων ασφάλειας, που είχε αναπτύξει η Wi-Fi

Alliance. Το μοντέλο WPA χρησιμοποιεί τον αλγόριθμο RC4 με κλειδί μήκους 128 bit και με το διάνυσμα ανάθεσης αρχικών τιμών μήκους 40 bit .

Το μοντέλο περιλαμβάνει το πρωτόκολλο ακεραιότητας προσωρινών κλειδιών (Temporal Integrity Key Protocol, TKIP) που παρέχει εμπιστευτικότητα. Το πρωτόκολλο αυτό παρέχει τη δυναμική αλλαγή των κλειδιών και τη χρήση τους για συγκεκριμένο χρονικό διάστημα (δηλαδή, όσο διαρκεί μια σύνδεση ενός σταθμού-πελάτη και ενός Access Point). Με την αύξηση του μήκους του διανύσματος ανάθεσης αρχικών τιμών και με τη δυναμική αλλαγή των κλειδιών, ο αλγόριθμος RC4 δημιουργεί μεγαλύτερη κλειδοροή, ώστε να αποφευχθεί η επίθεση ανάκτησης κλειδιού.

Στην επίθεση ανάκτησης κλειδιού, ο εισβολέας παρακολουθεί τα κρυπτογραφημένα πακέτα ώσπου να βρει δύο πακέτα με την ίδια σειρά κλειδιού και με αυτό τον τρόπο ανακτά το κλειδί και το χρησιμοποιεί για πλαστογραφία.

Επίσης, το μοντέλο WPA περιλαμβάνει και τον κωδικό Ακεραιότητας του μηνύματος (Message Integrity Code, MIC) για την εξασφάλιση της ακεραιότητας. Ο κωδικός Ακεραιότητας του μηνύματος χρησιμοποιεί κλειδί μήκους 64 bit, το οποίο δημιουργείται από τον αλγόριθμο Michael και είναι ένας αυθεντικοποιημένος κωδικός, που περιλαμβάνεται σε κάθε μήνυμα μαζί με έναν μετρητή για να παρέχει προστασία από επιθέσεις replay.

Το μοντέλο WPA χωρίζεται σε δύο κατηγορίες σχεδιασμού, στον προσωπικό και στον επιχειρηματικό. Στον προσωπικό σχεδιασμό του WPA περιλαμβάνονται τα μικρά γραφεία, τους οικιακούς χρήστες και η καταναλωτική χρήση (μικρά δίκτυα). Στον επιχειρηματικό σχεδιασμό του WPA περιλαμβάνονται οι επιχειρήσεις, οι κυβερνήσεις και οι εκπαιδευτικοί οργανισμοί (μεγάλα δίκτυα).

Στον προσωπικό σχεδιασμό χρησιμοποιείται ο μηχανισμός Pre-Shared Key (PSK) mode αυθεντικοποίησης, ο οποίος χρησιμοποιεί ένα passphrace (password) για να δημιουργήσει το μυστικό κλειδί της κρυπτογράφησης. Το μυστικό κλειδί της κρυπτογράφησης εισάγεται από τις συσκευές και από το Access Point πριν αρχίσει η μεταξύ τους επικοινωνία.

Στον επιχειρηματικό σχεδιασμό, το WPA χρησιμοποιείται με το πρότυπο IEEE 802.1X που παρέχει αυθεντικοποίηση των χρηστών. Το 802.1X δημιουργεί δύο

ειδών δυναμικά κλειδιά, το ζεύγος κλειδιών και την ομάδα κλειδιών και διανέμει διαφορετικά κλειδιά σε κάθε χρήστη. Το πρότυπο 802.1X χρησιμοποιεί τον μηχανισμό αυθεντικοποίησης port-based, του ελέγχου πρόσβασης διαδικτύου, στις συσκευές που επιθυμούν να σχετιστούν με το LAN και ιδρύει μια point – to - point σύνδεση.

Αυθεντικοποίηση χρηστών με το 802.1X και το EAP

Η αυθεντικοποίηση του προτύπου 802.1X περιλαμβάνει τα χαρακτηριστικά με τη σειρά που διέπονται: την αρχικοποίηση, την εισαγωγή, την διαπραγμάτευση και τέλος την αυθεντικοποίηση, χρησιμοποιώντας το πρωτόκολλο Extensible Authentication Protocol (EAP) για να παρέχει πιστοποιημένη μεταφορά [1].

i. **Αρχικοποίηση.** Κατά την εμφάνιση ενός νέου σταθμού η θύρα του αυθεντικοποιητή ενεργοποιείται και ρυθμίζεται σε μη-εξουσιοδοτημένη κατάσταση που επιτρέπει μόνο την κίνηση του προτύπου IEEE 802.1X , απορρίπτοντας την κίνηση από το HTTP και το DHCP.
ii. **Εισαγωγή.** Ο σταθμός ακούει την διεύθυνση του τμήματος του τοπικού δικτύου, όπου ο αυθεντικοποιητής μεταδίδει πλαίσια ταυτοποίησης EAP-Request Identity, και ο σταθμός αποκρίνεται στέλνοντας ένα πακέτο ταυτοποίησης EAP-Response Identity μαζί με ένα αναγνωριστικό του (όπως την ταυτότητα χρήστη). Ο αυθεντικοποιητής ενθυλακώνει το πακέτο που έστειλε ο σταθμός σε ένα πακέτο RADIUS Access-Request και το προωθεί στον σταθμό πιστοποίησης.
iii. **Διαπραγμάτευση.** Χρησιμοποιεί την τεχνική του EAP για διαπραγμάτευση. Ο σταθμός πιστοποίησης στέλνει μία απάντηση ενθυλακώνοντας ένα πακέτο RADIUS Access-Challenge με μία αίτηση EAP που καθορίζει την μέθοδο EAP στον αυθεντικοποιητή. Ο αυθεντικοποιητής ενθυλακώνει σε ένα πακέτο την αίτηση EAP και ένα πλαίσιο EAPOL και το στέλνει στον σταθμό. Ο σταθμός μπορεί να αρχίσει την μέθοδο EAP που καθορίστηκε ή να αρνηθεί τις προκαθορισμένες μεθόδους EAP και να προσθέσει αυτές που επιθυμεί.
iv. **Αυθεντικοποίηση.** Αν ο αυθεντικοποιητής σταθμός συμφωνήσει με τον σταθμό για την μέθοδο EAP, ο αυθεντικοποιητής σταθμός στέλνει ένα επιτυχές μήνυμα EAP-Success, ενθυλακώνοντάς το στο πακέτο RADIUS Access - Accept. Έπειτα, η θύρα ρυθμίζεται σε εξουσιοδοτημένη κατάσταση και

επιτρέπει την κανονική κυκλοφορία. Αν δεν υπάρξει συμφωνία, ο αυθεντικοποιητής στέλνει ένα ενθυλακωμένο μήνυμα αποτυχίας στο πακέτο RADIUS Access-Reject και η θύρα παραμένει στη μη-εξουσιοδοτημένη κατάσταση.

Αν ο σταθμός αποσυνδεθεί, στέλνει ένα μήνυμα EAPOL - logoff στον αυθεντικοποιητή κι αυτός ρυθμίζει τη θύρα στη μη-εξουσιοδοτημένη κατάσταση.

Το πρότυπο 802.1X και το πρωτόκολλο Extensible Authentication Protocol παρέχουν το κλειδί, κατά τη διάρκεια της σύνδεσης, σε ένα κινητό σταθμό και σε ένα Access Point. Το Access Point σταματά τη σύνδεση στο δίκτυο, μέχρι ο κινητός σταθμός να αυθεντικοποιηθεί από τον RADIUS server. Μόλις αυθεντικοποιηθεί ο σταθμός, ο RADIUS server στέλνει το μυστικό κλειδί ζεύγους που θα χρησιμοποιηθεί από το Access Point για να δημιουργήσει προσωρινά κλειδιά και κλειδιά για την κρυπτογράφηση. Το AP στέλνει το μυστικό κλειδί ζεύγους στο σταθμό για να το εγκαταστήσει και να αρχίσει τη μετάδοση των πλαισίων. Για την πιστοποίηση χρησιμοποιούνται οι EAP οι ακόλουθοι μέθοδοι: η EAP - TLS, η PEAP και η EAP - TTLS, οι οποίες χρησιμοποιούν εξωτερικές βάσεις δεδομένων για την αποφυγή επιθέσεων λεξικού.

Η μέθοδος EAP - TLS χρησιμοποιείται για την αμοιβαία πιστοποίηση χρησιμοποιώντας ψηφιακά πιστοποιητικά. Για να πιστοποιηθούν ο σταθμός και ο RADIUS server θα πρέπει να έχουν ο καθένας από ένα πιστοποιητικό.

Οι μέθοδοι PEAP και EAP - TTLS χρησιμοποιούνται για την πιστοποίηση του αυθεντικοποιητή, όπου μόνο αυτός χρειάζεται να διαθέτει ψηφιακό πιστοποιητικό. Ο σταθμός όταν επιβεβαιώσει το ψηφιακό πιστοποιητικό του αυθεντικοποιητή, πιστοποιεί και την ταυτότητα του RADIUS server. Τα δεδομένα πιστοποίησης του σταθμού που ενθυλακώνονται ως μηνύματα TLS, αποστέλλονται με ασφάλεια μέσω ενός μονόδρομου tunnel στον αυθεντικοποιητή.

## 8.6 Η ΑΣΦΑΛΕΙΑ ΤΟΥ IEEE 802.11i

Το πρότυπο IEEE 802.11i έχει ως στόχο τη δημιουργία μιας κλιμακωτής λύσης της ασφάλειας και την παροχή μιας αποτελεσματικής προστασίας από τις ενεργές και παθητικές επιθέσεις. Το πρότυπο IEEE 802.11i χρησιμοποιεί το Transitional

Security Network (TSN) για την συνύπαρξη της Αυτοδύναμης Αρχιτεκτονικής Προστασίας Δικτύου και του WEP μέσω του ίδιου ασύρματου LAN. Το TKIP, του μοντέλου WPA, μπορεί να υλοποιηθεί με το υλικό του WEP, ενώ ο κρυπτογραφικός αλγόριθμος δέσμης AES δεν μπορεί να υλοποιηθεί στο ίδιο υλικό του μοντέλου WPA. Το πρότυπο IEEE 802.11i περιλαμβάνει ένα μέρος του μοντέλου WPA και ένα μέρος του μοντέλου WPA2 και χρησιμοποιεί την 4-way handshake [1].

Το μοντέλο WPA2 ονομάζεται και Αυτοδύναμη Αρχιτεκτονική Προστασία Δικτύου (Robust Security Network Architecture,RSNA) και είναι η δεύτερη έκδοση του WPA. Το μοντέλο WPA2 βασίζεται στον ισχυρό κρυπτογραφικό αλγόριθμο δέσμης AES (Advance Encryption Standard) και στον μηχανισμό κρυπτογράφησης CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), που πρότεινε το Εθνικό Ινστιτούτο των Προτύπων και των Τεχνολογιών (National Institute of Standards and Technology, NIST) και παρέχουν ολοκληρωμένη προστασία. Ο κρυπτογραφικός αλγόριθμος δέσμης AES Counter Mode κρυπτογραφεί 128 bit δέσμες των δεδομένων με κλειδί μήκους 128 bit,192 bit και 256 bit.

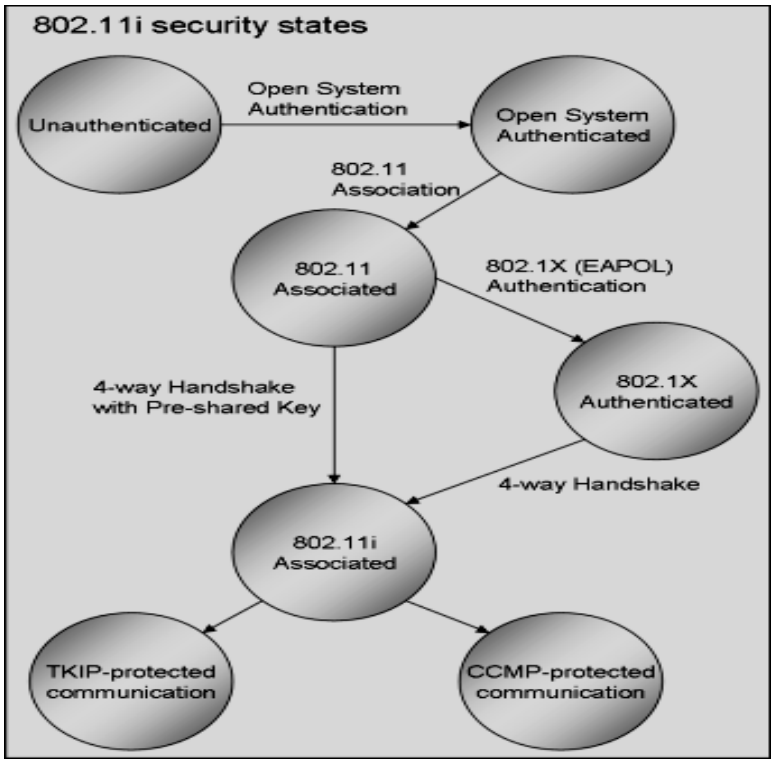
Εμπιστευτικότητα και ακεραιότητα

Με το Counter Mode παρέχεται εμπιστευτικότητα στα δεδομένα και με το Cipher Block Chaining Message Authentication Code (CBC-MAC) παρέχεται ακεραιότητα στα δεδομένα. Ο αλγόριθμος CBC-MAC παράγει έναν κωδικό Ακεραιότητας του μηνύματος με τον αλγορίθμου Michael, που παρέχει την αυθεντικοποίηση και την ακεραιότητα των δεδομένων του πακέτου. Στο προστατευμένο WPA2 πλαίσιο περιέχεται ένα πεδίο με τον Αριθμό του Πακέτου, όπου υπάρχει ένας μετρητής και ενσωματώνεται με τους υπολογισμούς του κωδικού Ακεραιότητας του μηνύματος του αλγορίθμου Michael κατά την κρυπτογράφηση, για να αποφεύγονται οι επιθέσεις replay.

Το μοντέλο WPA2 υποστηρίζει γρήγορη περιαγωγή των ασύρματων σταθμών πελάτη για την μετακίνηση μεταξύ των Access Points. Επίσης, το μοντέλο επιτρέπει την αποθήκευση του ζεύγους μυστικού κλειδιού, που χρησιμοποιείται για την σύνοδο μεταξύ ενός Access Point και ενός σταθμού πελάτη, ούτως ώστε να μπορεί να συνδεθεί με ένα πρόσφατα χρησιμοποιήσιμο Access Point χωρίς να

χρειάζεται να αυθεντικοποιηθεί ξανά. Επίσης, το μοντέλο επιτρέπει να αυθεντικοποιηθεί ένας σταθμός πελάτη σε ένα κινούμενο Access Point, εφόσον διατηρεί τη σύνδεση με το υπάρχον Access Point. Με αυτόν τον τρόπο μειώνεται ο χρόνος που χρειάζεται για να μετακινηθεί ένας σταθμός πελάτη από το ένα Access Point σε ένα άλλο.

Το μοντέλο WPA2 χρησιμοποιεί για την αυθεντικοποίηση και τη διανομή των κλειδιών, το πρότυπο 802.1X, υπολογίζοντας τα προσωρινά ζεύγη κλειδιών (Pairwise Transient Keys, PTK) μέσω της 4-way handshake (όπως στο μοντέλο WPA).




**ΕΙΚΟΝΑ 108: ΚΑΤΑΣΤΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ 802.11i**

Τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση προέρχονται από το μοιραζόμενο μυστικό κλειδί ζεύγους που διατηρεί όλη την σύνδεση και προέρχεται από την αυθεντικοποίηση του πρωτοκόλλου Extensible Authentication Protocol (EAP), το οποίο περιέχεται στο επιτυχές μήνυμα EAP και στέλνεται στον αυθεντικοποιητή. Ο σταθμός πελάτη (STA) έχει πάρει το αντίγραφο του κλειδιού, με αποτέλεσμα να μη χρειάζεται να προωθηθεί. Η ψευδοτυχαία μέθοδος παράγει τα προσωρινά ζεύγη κλειδιών με τις εξής παραμέτρους: την MAC διεύθυνση του σταθμού πελάτη, την MAC διεύθυνση του αυθεντικοποιητή (Access Point), ένα

nonce από τον σταθμό πελάτη και ένα nonce από τον αυθεντικοποιητή. Αυτή η διαδικασία δεν φαίνεται στο σχήμα, γιατί η 4 - way handshake στέλνει τέσσερα πακέτα (EAPOL - key frames) που ανταλλάσσονται μεταξύ του αυθεντικοποιητή και του σταθμού πελάτη, από όπου έχει πάρει και την ονομασία του.

Προσωρινό ζεύγος κλειδιών

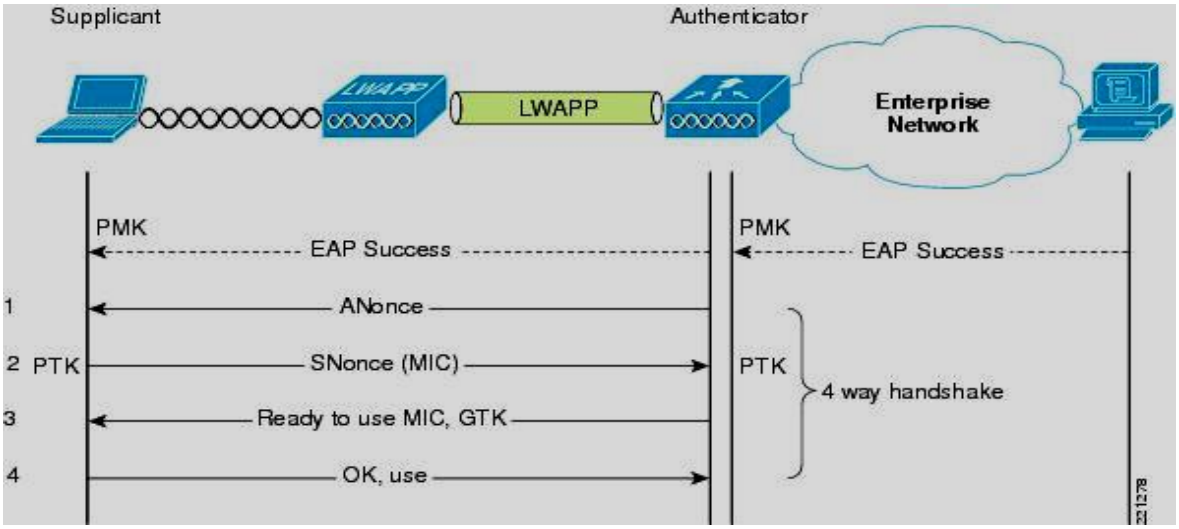
Το προσωρινό ζεύγος κλειδιών 64 bytes διαιρείται σε πέντε κλειδιά:

- Το προσωρινό κλειδί για την εμπιστευτικότητα των δεδομένων των πρωτοκόλλων.
- Το EAPOL-key confirmation key (KCK) για την αυθεντικοποίηση των δεδομένων.
- Το EAPOL-key encryption key (KEK) για την εμπιστευτικότητα.
- Το κλειδί μετάδοσης.
- Το κλειδί λήψης (το κλειδί μετάδοσης και το κλειδί λήψης χρησιμοποιούνται μόνο στο TKIP).

Το EAPOL - key encryption key περιέχει 16 bytes και χρησιμοποιείται για την κρυπτογράφηση των επιπλέον απεσταλμένων δεδομένων. Το EAPOL - key confirmation key (KCK) περιέχει 16 bytes και χρησιμοποιείται για τον υπολογισμό του κωδικού Ακεραιότητας του μηνύματος από το μήνυμα του WPA EAPOL Key. Το προσωρινό κλειδί που περιέχει 16 bytes χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση των unicast πακέτων δεδομένων. Τα unicast πακέτα, είναι τα πακέτα που αποστέλλονται από έναν αποστολέα σε έναν παραλήπτη. Το κλειδί μετάδοσης που περιέχει 8 bytes του κωδικού Ακεραιότητας του μηνύματος χρησιμοποιείται για unicast πακέτα δεδομένων του αυθεντικοποιητή. Επίσης, το κλειδί λήψης που περιέχει 8 bytes του κωδικού Ακεραιότητας του μηνύματος, χρησιμοποιείται για unicast πακέτα δεδομένων του σταθμού. Το KCK και το KEK χρησιμοποιούνται από το EAPOL-key exchanges.

4-way handshake

Στο πρώτο μήνυμα ANonce, ο αυθεντικοποιητής στέλνει ένα Nonce (ψευδοτυχαίος αριθμός μιας χρήσης) στον σταθμό πελάτη. Ο σταθμός πελάτη δημιουργεί ένα Nonce, το SNonce και πληκτρολογεί το προσωρινό ζεύγος κλειδιού. Στο δεύτερο μήνυμα, ο σταθμός πελάτη στέλνει το SNonce και τις παραμέτρους ασφάλειας που χρησιμοποιούνται κατά τη διάρκεια της σύνδεσης στον αυθεντικοποιητή και τον κωδικό Ακεραιότητας του μηνύματος. Χρησιμοποιώντας το KCK, ελέγχεται η αυθεντικοποίηση του μηνύματος κι έτσι ο αυθεντικοποιητής θα αποφασίσει αν οι πληροφορίες είναι έγκυρες ή όχι.




**ΕΙΚΟΝΑ 109: 4-WAY HANDSHAKE ΜΕ ΤΟ 802.1X**

Στο τρίτο μήνυμα, ο αυθεντικοποιητής στέλνει τις δικές του παραμέτρους ασφάλειας που αφορούν το δικό του beacon, τη συστηματική έρευνα των αποκρίσεων και επιπλέον στέλνει το κρυπτογραφημένο από το KEK, ομαδικό προσωρινό κλειδί (Group Temporal Key,GTK ) για την multicast και την broadcast κρυπτογράφηση, για να ελεγχθεί η εγκυρότητα των παραμέτρων ασφαλείας από το σταθμό πελάτη.

Στο τέταρτο μήνυμα δηλώνεται ότι τα προσωρινά κλειδιά μπορούν να χρησιμοποιηθούν από τα πρωτόκολλα εμπιστευτικότητας των δεδομένων.

Με αυτόν τον τρόπο, ο σταθμός πελάτη και ο αυθεντικοποιητής έχουν επιβεβαιώσει την εγκυρότητα του μυστικού κλειδιού, την κοινή χρησιμοποίηση των προσωρινών κλειδιών και του ομαδικού προσωρινού κλειδιού.

The Group Key Handshake

Το ομαδικό προσωρινό κλειδί ενημερώνεται κάθε φορά που μια συσκευή φεύγει από το δίκτυο ώστε να εμποδίζεται η συσκευή να λαμβάνει multicast ή broadcast μηνύματα. Το πρότυπο IEEE 802.11i καθορίζει το Group Key Handshake με δύο τρόπους handshake:

- αυθεντικοποιητής στέλνει ένα καινούριο ομαδικό προσωρινό κλειδί (32 bytes) που είναι κρυπτογραφημένο με το KEK για κάθε σταθμό στο δίκτυο.
- Ο σταθμός αναγνωρίζει το καινούριο ομαδικό προσωρινό κλειδί και απαντά στο Access Point.

Το ομαδικό προσωρινό κλειδί περιέχει το ομαδικό προσωρινό κλειδί κρυπτογράφησης που είναι 16 bytes και χρησιμοποιείται για τα multicast πακέτα δεδομένων, το κλειδί μετάδοσης που περιέχει 8 bytes του κωδικού Ακεραιότητας του μηνύματος για multicast πακέτα δεδομένων του αυθεντικοποιητή και το κλειδί λήψης που περιέχει 8 bytes του κωδικού Ακεραιότητας του μηνύματος [1][4][5][12].

Το μοντέλο WPA έχει μία αδυναμία στον αλγόριθμο TKIP. Η αδυναμία αυτή αφορά την εισαγωγή από ψεύτικα ARP πακέτα και οδηγεί το θύμα να στέλνει πακέτα στο ανοιχτό διαδίκτυο. Αυτή η αδυναμία δημιουργείται από την ανακάλυψη της κλειδοροής που είναι κρυπτογραφημένη σε ένα πακέτο, με αποτέλεσμα την επαναχρησιμοποίηση της κλειδοροής με στόχο την αποστολή πλαστών δεδομένων του ίδιου μήκους πακέτων σε ένα ασύρματο σταθμό πελάτη. Το είδος αυτής της αδυναμίας του αλγόριθμου TKIP, αποτρέπεται από την χρησιμοποίηση του μηχανισμού CCMP. Ο μηχανισμός CCMP είναι ισχυρός και δεν επηρεάζεται από αυτήν την αδυναμία, με αποτέλεσμα να παρέχεται ισχυρή προστασία στο πρότυπο IEEE 802.11i.


## 8.7 Wi-Fi PROTECTED SETUP ΠΡΟΤΥΠΟ

Η Wi-Fi Alliance έχει προτείνει ένα πρόγραμμα εγκατάστασης για προστατευμένα Wi-Fi (Wi-Fi protected Setup)[15]. Η Wi-Fi Alliance πιστοποιεί τη συμμόρφωση με τα πρότυπα WPA και WPA2 και τυποποιεί μεθόδους για την εξάλειψη της αδύναμης επιλογής της passphrase, για τη δημιουργία και διανομή

ισχυρών κλειδιών και για την νέα προσθήκη μιας συσκευής στο δίκτυο. Το Wi-Fi protected Setup προσφέρει εύκολη εγκατάσταση και ασφάλεια.

Για να προστεθεί μία καινούρια συσκευή σε ένα δίκτυο για οικιακή χρήση, χρησιμοποιούνται δύο μέθοδοι[16]:

- Την PBC μέθοδο, στην οποία ο χρήστης πιέζει ένα κουμπί για ένα Access Point, που είναι υπεύθυνο για τις νέες εγγραφές και για ένα καινούριο σταθμό πελάτη. Συνήθως χρησιμοποιείται υποχρεωτικά για το Access Point και προαιρετικά για τον σταθμό.
- Την μέθοδο PIN, στην οποία ο κωδικός PIN (Personal Identification Number) περιέχεται στο αυτοκόλλητο της ασύρματης συσκευής ή παρέχεται από το Access Point. Αυτή η μέθοδος είναι υποχρεωτική για όλες τις Wi-Fi συσκευές.

Υπάρχουν δύο ακόμα μέθοδοι, που αναφέρονται ως μέθοδοι εκτός ζώνης (out – of - band) όταν μεταδίδονται πληροφορίες από ένα κανάλι διαφορετικό από το Wi-Fi. Η μία μέθοδος είναι η NFC, η οποία είναι προαιρετική και ο χρήστης με τον καινούριο σταθμό πελάτη πρέπει να είναι κοντά στο Access Point για να επιτραπεί η επικοινωνία κοντινής περιοχής (Near Field Communication). Η άλλη μέθοδος είναι η USB μέθοδος, η οποία δεν έχει πιστοποιηθεί από την Wi-Fi protected Setup, και χρησιμοποιείται με USB stick για την μεταφορά δεδομένων του νέου σταθμού και του Access Point.

Το πρότυπο Wi-Fi protected Setup καθορίζεται από τους παρακάτω τύπους συσκευών στο δίκτυο: α) ο υπεύθυνος εγγραφών (registrar), είναι μια συσκευή, η οποία εκδίδει και ανακαλεί τα πιστοποιητικά που στέλνονται από τους χρήστες στο δίκτυο, β) η συσκευή (enrollee) που θέλει να εγγραφεί για να συνδεθεί σε ένα ασύρματο τοπικό δίκτυο και γ) ο αυθεντικοποιητής η οποία είναι μια λειτουργία ανάμεσα στον υπεύθυνο εγγραφών και στη συσκευή που θέλει να εγγραφεί.

Το πρότυπο Wi-Fi protected Setup προτείνει τρεις τρόπους που περιλαμβάνουν τους τύπους που ακολουθούν:

- Ένα Access Point, που μπορεί να έχει τον ρόλο του υπεύθυνου εγγραφών και να διαμορφώνει τον σταθμό enrollee. Η σύνδεση αυτή πραγματοποιείται στο ασύρματο μέσο με μηνύματα αίτησης και απόκρισης του EAP. Ώσπου ο

σταθμός να συνδεθεί με τις καινούριες διαμορφώσεις, το Access Point τερματίζει τη σύνδεση,

- Ένας σταθμός παίρνει τον ρόλο του υπεύθυνου εγγραφών και διαμορφώνει το Access Point enrollee. Μία περίπτωση είναι να μπορεί μια σύνδεση να συμβαίνει σε ενσύρματο ή σε ασύρματο μέσο και η άλλη περίπτωση το Access Point να είχε ήδη ρυθμιστεί κατά την εύρεση του υπεύθυνου εγγραφών. Στην ενσύρματη σύνδεση, το πρότυπο χρησιμοποιεί το Universal Plug and Play, το οποίο πρέπει να είναι υποστηριζόμενο από τις συσκευές και δεν χρειάζεται η αυθεντικοποίηση. Στην ασύρματη σύνδεση, ο υπεύθυνος εγγραφών ρωτά τον χρήστη αν θα αναδιαμορφώσει το Access Point ή θα παραμείνουν οι ρυθμίσεις.
- ένας σταθμός παίρνει τον ρόλο του υπεύθυνου εγγραφών και διαμορφώνει ένα άλλο σταθμό enrollee. Το Access Point κατέχει τον ρόλο του αυθεντικοποιητή και είναι αρμόδιος για την αποστολή μηνυμάτων από την μία πλευρά στην άλλη.

Πλεονεκτήματα του προτύπου Wi-Fi protected Setup

Το πρότυπο παρέχει αυτόματα την διαμόρφωση του ονόματος δικτύου (SSID) και του κλειδιού WPA για την προστασία του Access Point και των συσκευών που συμμετέχουν στο δίκτυο. Δεν χρειάζεται η γνώση του ονόματος, των κλειδιών ή των passphrace για την σύνδεση σε ένα ασύρματο δίκτυο. Τα προστατευτικά κλειδιά και τα passphrace δημιουργούνται τυχαία. Το πρότυπο Wi - Fi protected Setup παρέχει ισχυρή αυθεντικοποίηση επειδή χρησιμοποιεί το πρωτόκολλο EAP.

Μειονεκτήματα του προτύπου Wi-Fi protected Setup

Το πρότυπο Wi - Fi protected Setup δεν υποστηρίζει Ad - Hoc mode, γιατί δεν χρησιμοποιεί Access Point. Εάν η ασύρματη συσκευή του χρήστη δεν υποστηρίζει το πρότυπο Wi - Fi protected Setup και το δίκτυο που θέλει να συνδεθεί το χρησιμοποιεί, ο χρήστης δεν θα μπορεί να συνδεθεί [15][16].

## 8.8 Η ΑΣΦΑΛΕΙΑ ΤΩΝ ΑΛΛΩΝ ΑΣΥΡΜΑΤΩΝ ΤΕΧΝΟΛΟΓΙΩΝ

Στις προηγούμενες ενότητες παρουσιάστηκαν οι μηχανισμοί για την προστασία των ασύρματων τοπικών δικτύων που ακολουθούν το πρότυπο 802.11. Σε αυτήν

την ενότητα θα περιγραφούν οι μηχανισμοί για τις ασύρματες τεχνολογίες IrDA, Bluetooth, HiperLAN, HomeRF και WiMAX.

### 8.8.1 Η ΑΣΦΑΛΕΙΑ ΜΕ ΤΟ ΠΡΟΤΥΠΟ IrDA

Το πρότυπο IrDA δεν παρέχει υψηλό επίπεδο ασφαλείας, επιτρέποντας τη μη-εξουσιοδοτημένη πρόσβαση στο επίπεδο ζεύξης. Στο επίπεδο εφαρμογών για την αυθεντικοποίηση περιλαμβάνεται ο μηχανισμός αυθεντικοποίησης IrDA OBEX. Οι χρήστες που θέλουν να επικοινωνήσουν, πρέπει να εισάγουν τον κωδικό OBEX και να αποθηκευτεί στη συσκευή τους, ώστε να πιστοποιηθούν. Αν δεν εισάγουν αυτόν τον κωδικό, οι χρήστες δεν μπορούν να επικοινωνήσουν.

### 8.8.2 Η ΑΣΦΑΛΕΙΑ ΜΕ ΤΟ ΠΡΟΤΥΠΟ HomeRF

Όταν αρχίσει η αρχικοποίηση της σύνδεσης των κόμβων, οι κόμβοι ενημερώνουν ο ένας τον άλλον αν υποστηρίζουν την κρυπτογράφηση. Αν κάποιοι κόμβοι δεν υποστηρίζουν την κρυπτογράφηση, τότε είτε τα δεδομένα αποστέλλονται χωρίς να κρυπτογραφηθούν είτε η σύνδεση ακυρώνεται. Αν οι κόμβοι υποστηρίζουν την κρυπτογράφηση, πραγματοποιείται η ανταλλαγή του κοινού μυστικού κλειδιού που έχει μήκος 56 bit. Ο μηχανισμός κρυπτογράφησης για κάθε πακέτο λειτουργεί ως εξής:

- υπολογίζεται το διάνυσμα αρχικών τιμών (IV των 32 bit) από τον αύξοντα αριθμό του πακέτου,
- δημιουργείται μία hash function με μήκος 48 bit από την διεύθυνση MAC του αποστολέα και
- κρυπτογραφούνται τα δεδομένα με το μυστικό κλειδί και το διάνυσμα αρχικών τιμών.

Η αποκρυπτογράφηση του πακέτου πραγματοποιείται με το μυστικό κλειδί και τον αύξοντα αριθμό του πακέτου.

### 8.8.3 Η ΑΣΦΑΛΕΙΑ ΜΕ ΤΟ ΠΡΟΤΥΠΟ HIPERLAN

Το πρότυπο HIPERLAN περιέχει ένα σύνολο από τρία κλειδιά και χρησιμοποιεί ένα από αυτά για την κρυπτογράφηση των δεδομένων. Το κλειδί και τα δεδομένα περιέχονται στο πακέτο που θα αποσταλεί. Ο αλγόριθμος κρυπτογράφησης προσθέτει με τη δυαδική πράξη XOR το κλειδί και μια τυχαία ακολουθία από bit.

Το κλειδί και η ακολουθία έχουν το ίδιο μήκος. Το αποτέλεσμα της πράξης XOR χρησιμοποιείται ως γεννήτρια τυχαίων αριθμών και παράγει ένα bitstream. Οι δύο ροές προστίθενται πάλι με τη δυαδική πράξη XOR για να κρυπτογραφηθούν τα δεδομένα.

### 8.8.4 Η ΑΣΦΑΛΕΙΑ ΜΕ ΤΗΝ ΤΕΧΝΟΛΟΓΙΑ BLUETOOTH

Η τεχνολογία Bluetooth περιέχει δύο επίπεδα ασφαλείας, που χαρακτηρίζουν τις συσκευές Bluetooth, trusted και untrusted. Όταν οι συσκευές Bluetooth εισέρχονται σε ένα piconet, το piconet καθορίζει ποιο από τα δύο επίπεδα ασφαλείας θα παρέχεται σε κάθε συσκευή. Οι untrusted συσκευές δεν έχουν πρόσβαση σε άλλες συσκευές και σε υπηρεσίες και αφορά τις νέες συσκευές που εισέρχονται στο δίκτυο. Μετά την αυθεντικοποίηση, οι συσκευές χαρακτηρίζονται ως trusted. Οι trusted συσκευές έχουν πρόσβαση σε όλες τις συσκευές και υπηρεσίες [6][7].

Το Bluetooth παρέχει τρεις τύπους ασφάλειας[6][7]. Ο πρώτος τύπος δεν παρέχει καμία ασφάλεια, ο δεύτερος παρέχει ασφάλεια μετά το επίπεδο L2CAP (Logical Link And Adaptation Layer) και ο τρίτος τύπος παρέχει ασφάλεια στο επίπεδο LMP (Link Management Protocol). Το Bluetooth επικεντρώνεται στον τρίτο τύπο ασφάλειας.

Το Bluetooth περιέχει τις εξής παραμέτρους: την διεύθυνση συσκευής, το PIN, τα κλειδιά ζεύξης (link key) και τα μυστικά κλειδιά. Η διεύθυνση συσκευής είναι δημόσια και μοναδική σαν το ID για κάθε συσκευή. Το PIN (Personal Identification Number) χρησιμοποιείται για την σύνδεση με την συσκευή και ορίζεται ως το πρώτο μυστικό κλειδί, ώστε να δημιουργηθούν τα άλλα κλειδιά. Το PIN, η διεύθυνση και το προκαθορισμένο μέγεθος του μυστικού κλειδιού κρυπτογράφησης καθορίζονται από τον κατασκευαστή της συσκευής. Τα μυστικά κλειδιά είναι το στατικό μυστικό κλειδί για την ταυτοποίηση και το μυστικό κλειδί κρυπτογράφησης, το οποίο παράγεται από το μυστικό κλειδί ταυτοποίησης για κάθε κρυπτογραφημένη σύνδεση. Το στατικό μυστικό κλειδί για την ταυτοποίηση παράγεται κατά την αρχικοποίηση και έχει συχνή χρήση χωρίς να υπάρξουν αλλαγές.

Όταν η συσκευή τίθεται για πρώτη φορά σε λειτουργία, η διεύθυνση συσκευής κι ένας τυχαίος αριθμός (RAND), μαζί με τον αλγόριθμο $E_{21,}$ δημιουργούν το κλειδί

unit (μονάδας), το οποίο είναι ένα από τα κλειδιά ζεύξης και αποθηκεύεται στη συσκευή.

Όταν η συσκευή εισέρχεται στο piconet, ο χρήστης ορίζει το PIN και η συσκευή αυθεντικοποίησης στέλνει ένα τυχαίο αριθμό RAND. Το PIN, το μήκος του PIN και το RAND μαζί με τον αλγόριθμο $E_{22}$, δημιουργούν ένα προσωρινό κλειδί link, το κλειδί αρχικοποίησης (initialization key).

Στην αυθεντικοποίηση χρησιμοποιείται η διεύθυνση της συσκευής και το μοιρασμένο κλειδί συνδέσμου ( link key ) ή το μυστικό κλειδί ταυτοποίησης, το οποίο είναι είτε το συνδυασμένο κλειδί είτε το κλειδί μονάδας της συσκευής με την λιγότερη μνήμη, το οποίο χρησιμοποιείται για την επικοινωνία. Το συνδυασμένο κλειδί παράγεται όταν και οι δύο συσκευές έχουν αρκετή μνήμη. Το κλειδί παράγεται από την ακόλουθη διαδικασία: η πρώτη συσκευή υπολογίζει το κλειδί μονάδας της δεύτερης, αφού πρώτα η δεύτερη της έχει στείλει ένα τυχαίο αριθμό και την διεύθυνσης της και αντίστροφα, η δεύτερη της πρώτης. Έπειτα, τα δύο κλειδιά προσθέτονται με την δυαδική πράξη XOR και το αποτέλεσμα που παράγεται είναι το συνδυασμένο κλειδί. Αν μία συσκευή δεν έχει αρκετή μνήμη, τότε ορίζεται το κλειδί μονάδας αυτής της συσκευής.

Η διαδικασία της αυθεντικοποίησης έχει ως εξής: ο αυθεντικοποιητής στέλνει ως πρόκληση ένα τυχαίο αριθμό, η αιτούσα συσκευή στέλνει ως απάντηση το αποτέλεσμα SRES. Το αποτέλεσμα SRES δημιουργείται από την κρυπτογράφηση του μυστικού κλειδιού ταυτοποίησης, από την διεύθυνση της συσκευής και από το ληφθέντα τυχαίο αριθμό με την μέθοδο αυθεντικοποίησης $E_1$. Ο αυθεντικοποιητής χρησιμοποιεί τα ίδια στοιχεία, δηλαδή το μυστικό κλειδί, την διεύθυνση και το τυχαίο αριθμό, για να παράγει το αποτέλεσμα και έπειτα ελέγχει το αποτέλεσμα με το SRES που έστειλε η αιτούσα συσκευή. Αν είναι ίδιο το αποτέλεσμα, πιστοποιείται η αιτούσα συσκευή. Αν δεν είναι ίδιο, δεν πιστοποιείται. Αν για πρώτη φορά πιστοποιούνται οι δύο συσκευές, τότε η πιστοποίηση ονομάζεται pairing. Εκτός από το αποτέλεσμα SRES παράγεται και το αποτέλεσμα ACO (Authenticated Cipher Offset). Το ACO χρησιμοποιείται για τη δημιουργία του κλειδιού κρυπτογράφησης.

Για την κρυπτογράφηση της σύνδεσης χρησιμοποιείται το κλειδί κρυπτογράφησης του αλγόριθμου. Το κλειδί του φορτίου (payload key)

υπολογίζεται από μία ποσότητα CLOCK που παρέχεται από το master του piconet για τη δημιουργία των ανατροφοδοτούμενων κλειδιών, τη διεύθυνση της συσκευής, το κλειδί κρυπτογράφησης και έναν τυχαίο αριθμό χρησιμοποιώντας τη μέθοδο κρυπτογράφησης $E_0$. Έπειτα, το αποτέλεσμα από τα προηγούμενα προστίθεται με τα δεδομένα χρησιμοποιώντας τη δυαδική πράξη XOR. Το κλειδί κρυπτογράφησης του αλγόριθμου παράγεται από το κλειδί συνδέσμου, τον αριθμό COF (το αποτέλεσμα ACO) και την διεύθυνση της συσκευής με τη μέθοδο κρυπτογράφησης $E_3$. Αν χρειάζεται, χρησιμοποιείται η συνάρτηση μείωσης του μεγέθους RED για τη μείωση του κλειδιού. Ο αλγόριθμος κρυπτογράφησης είναι ο SAFER+ και είναι αλγόριθμος κρυπτογράφησης δέσμης (block cipher). Παραπάνω αναφέρθηκαν οι μέθοδοι $E_0$,$E_1$,$E_3$,$E_{21}$,$E_{22}$ του αλγόριθμου SAFER+. Για περισσότερες πληροφορίες για τον αλγόριθμο SAFER+ και τις μεθόδους του δείτε στην αναφορά [9].

### 8.8.5 Η ΑΣΦΑΛΕΙΑ ΣΤΟ WiMAX

Οι υπηρεσίες ασφάλειας που παρέχονται στα πλαίσια MAC, προσφέρονται από το υποεπίπεδο ασφαλείας MAC του WiMAX. Το υποεπίπεδο αυτό προσφέρει εμπιστευτικότητα των δεδομένων και αυθεντικοποίηση των χρηστών. Τα πρωτόκολλα που χρησιμοποιούνται είναι το πρωτόκολλο ενθυλάκωσης και το πρωτόκολλο διαχείρισης κλειδιών. Το πρωτόκολλο ενθυλάκωσης ορίζει κρυπτογραφικές σουίτες για την εμπιστευτικότητα των δύο σταθμών (BS και SS) και περιλαμβάνουν πληροφορίες και κανόνες για τους αλγόριθμους που θα χρησιμοποιηθούν. Το πρωτόκολλο διαχείρισης κλειδιού PKM (Privacy Key Management) καθορίζει τη διαχείριση και τη διανομή των κλειδιών.

Το υποεπίπεδο ασφαλείας ορίζει τρεις συσχετισμούς ασφαλείας (SA, Security Association) για ακεραιότητα και για εμπιστευτικότητα των πληροφοριών που ανταλλάσσουν οι δύο σταθμοί: την κύρια, τη στατική και τη δυναμική. Η κύρια SA εγκαθίσταται και στους δύο σταθμούς στην διαδικασία αρχικοποίησης του SS (Subscriber Station - σταθμός συνδρομητή) και έχει ως ταυτότητα (SAID, Security Association Identifier) τη βασική ταυτότητα σύνδεσης (Basic Connection ID, BID) του SS. Η στατική AS δημιουργείται από το BS (Basic Station - βασικός σταθμός) κατά την αρχικοποίηση του SS και χρησιμοποιείται από το BS. Αν το SS έχει εγγραφεί σε πολλές υπηρεσίες, τότε ο αριθμός των στατικών AS θα είναι ο ίδιος με

των αριθμό των υπηρεσιών. Η δυναμική AS δημιουργείται και καταστρέφεται όταν ξεκινάει μια υπηρεσία και όταν τερματίζεται αντίστοιχα.

Η διαχείριση και η ανανέωση των κλειδιών πραγματοποιείται από το BS και τα κλειδιά έχουν συγκεκριμένη διάρκεια ζωής. Για να ανανεωθεί η διάρκεια ενός κλειδιού, ο SS πρέπει να ζητήσει την ανανέωσή τους από τον BS, όμως πριν από την λήξη τους.

#### 8.8.5.1 ΠΙΣΤΟΠΟΙΗΣΗ ΜΕ ΤΟ PKM ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η πιστοποίηση του SS πραγματοποιείται με το πρωτόκολλο PKM και ο SS πρέπει να διαθέτει το ψηφιακό πιστοποιητικό X.509 από τον κατασκευαστή του ή από μια αρχή πιστοποίησης για την εξασφάλιση της ακεραιότητας και της αυθεντικότητας του. Το ψηφιακό πιστοποιητικό περιέχει το όνομα, το δημόσιο κλειδί RSA για τη πιστοποίηση της ταυτότητας, την ημερομηνία έναρξης και λήξης, το σειριακό αριθμό, τη διεύθυνση MAC και το όνομα της αρχής πιστοποίησης. Ο τρόπος που αποθηκεύεται το ιδιωτικό κλειδί στη συσκευή, αποτρέπει την προσπέλαση και την αντιγραφή του κλειδιού. Ο BS δεν υποχρεούται να πιστοποιηθεί.

Η διαδικασία πιστοποίησης είναι η εξής: ο SS στέλνει μία αίτηση πιστοποίησης (Authorization request) στο BS, η οποία περιέχει το πιστοποιητικό, την ταυτότητα της SA (SAID) και τους αλγόριθμους που υποστηρίζει. Ο BS ελέγχει τα πιστοποιητικά του SS και καθορίζει τις παραμέτρους της ασφάλειας. Αν τα πιστοποιητικά είναι έγκυρα, ο BS απαντά με μια αίτηση έγκρισης (Authorization Response), η οποία περιέχει το κλειδί εξουσιοδότησης (AK, Authentication Key) που κρυπτογραφείται με το δημόσιο κλειδί του SS, μία ακολουθία αριθμών με μέγεθος 4 bit AK, την ημερομηνία λήξης του κλειδιού και τα στοιχεία της SA (ταυτότητα και ιδιότητες). Το AK ανανεώνεται, όταν ο SS ξαναστείλει αίτηση πιστοποίησης, χωρίς να στείλει ξανά τις πληροφορίες αυθεντικοποίησης στον BS. Το AK παράγει το κλειδί κρυπτογράφησης (KEK, key encryption key) και τα δύο κλειδιά πιστοποίησης μηνυμάτων (HMAC). Το KEK χρησιμοποιείται για την κρυπτογράφηση του κλειδιού TEK (Traffic Encryption Key) παρέχοντας εμπιστευτικότητα. Το κλειδί TEK είναι τυχαία επιλεγμένο από το BS, έχει μικρή διάρκεια ζωής και κρυπτογραφεί τα δεδομένα.

Ο SS αποστέλλει ένα μήνυμα Key request για την ανανέωση των κλειδιών TEK (για την συγκεκριμένη SA) στο BS. Το μήνυμα περιέχει το AK για να καθορίσει το κλειδί HMAC του SS και να δημιουργήσει την ψηφιακή υπογραφή HMAC του μηνύματος, την ταυτότητα της SA και την ψηφιακή υπογραφή HMAC του μηνύματος, που δημιουργήθηκε με το κλειδί HMAC της ανερχόμενης ζεύξης. Ο BS απαντά με το μήνυμα Key Reply. Το μήνυμα αυτό περιέχει την ακολουθία αριθμών AK, την ταυτότητα της SA, τα στοιχεία του παλιού και του καινούριου TEK και την ψηφιακή υπογραφή HMAC.

Τα στοιχεία του κλειδιού είναι το καινούριο TEK κρυπτογραφημένο με το KEK και τον αλγόριθμο κρυπτογράφησης, τη διάρκεια ζωής του TEK, την ακολουθία αριθμών TEK και το IV με μήκος 64 bit.

Η κρυπτογράφηση πραγματοποιείται με τον αλγόριθμο κρυπτογράφησης DES με CBC mode με κλειδί 56-bits ή τον AES με CCM mode και κλειδί 128-bits. Ο αλγόριθμος DES χωρίζει τα δεδομένα σε block και κρυπτογραφείται το ένα από αυτά με το κλειδί. Η λειτουργία του αλγόριθμου κρυπτογράφησης AES έχει περιγραφεί στο 802.11i [1][2][12].

## 8.9 ΣΥΝΟΨΗ

Οι μεταδόσεις δεδομένων στα ασύρματα δίκτυα πρέπει να προστατευτούν, επειδή είναι πολύ πιο εύκολο να εκτεθούν σε κάποια προσβολή από ότι τα ενσύρματα δίκτυα. Πρέπει να υπάρχουν μηχανισμοί, οι οποίοι να προλαμβάνουν τις επιθέσεις και να εξασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα, την αυθεντικοποίηση, την πρόσβαση των δεδομένων από μη-εξουσιοδοτημένους χρήστες και τη διαθεσιμότητα του δικτύου. Χρησιμοποιούνται διαφορετικοί μηχανισμοί σε κάθε ασύρματη επικοινωνία. Στα ασύρματα τοπικά δίκτυα που χρησιμοποιούν το πρότυπο 802.11, αρχικά χρησιμοποιήθηκε το WEP, το οποίο παρότι πρόσφερε πιστοποίηση, ακεραιότητα και εμπιστευτικότητα, οι μέθοδοι που εφαρμόζει, εμφάνισαν αρκετές αδυναμίες. Το WEP αποδείχθηκε αναποτελεσματικό στα ασύρματα δίκτυα, για αυτό το λόγο δημιουργήθηκε το WPA.

Το WPA είναι ο ενδιάμεσος μηχανισμός από το WEP στο WPA2 (802.11i). Προσφέρει διαλειτουργικότητα με το υλικό του WEP και ισχυρότερες μεθόδους για

την προστασία των δεδομένων. Το WPA, όμως, αποδείχθηκε και αυτό επιρρεπή σε υποκλοπές. Μετά την ανακάλυψη της αδυναμίας του, δημιουργήθηκε το WPA2 (802.11i), το οποίο παρέχει ισχυρή προστασία, όπου μέχρι στιγμής δεν έχει παρουσιάσει κάποια δείγματα εισβολών.

Για την προστασία των δεδομένων, εκτός από τους μηχανισμούς που προσφέρονται σε κάθε ασύρματη επικοινωνία, θα πρέπει να ακολουθούνται ένα σύνολο καλών πρακτικών, όπως να αλλάζουμε τις προκαθορισμένες ρυθμίσεις για την ασύρματη επικοινωνία και να χρησιμοποιούμε ισχυρούς κωδικούς. Επιπλέον, όλος ο σχεδιασμός να διέπεται από ένα σχέδιο ασφαλείας που θα προστατεύει την ακεραιότητα και την εμπιστευτικότητα των προσωπικών δεδομένων.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## ΚΕΦΑΛΑΙΟ 1

[1] Αλεξόπουλος Άρης, Γιώργος Λαγογιάννης. (2003). Τηλεπικοινωνίες και Δίκτυα Υπολογιστών. 6η Έκδοση. ΑΦΟΙ ΡΟΗ Α.Ε.. Αθήνα.

[2] Abbate Janet. (2000). Inventing The Internet. THE MIT PRE.

[3] Campolo Domenico. (2010). Wireless Body Area Network (WBAN) For Medical Applications. INTECH.

[4] CLARK P. Martin. (2003). Data Networks, IP And The Internet. Protocols, Design And Operation. John Wiley & Sons, Ltd..

[5] Garg K. Vijay. (2007). Wireless Communications And Networking. Elsevier, Inc..

[6] Gast Matthew. (2002). 802.11 Wireless Networks: The Define Guide. O' Reilly & Associates, Inc..

[7] Halsall Fred. (2005). Computer Networking And The Internet. 5TH Edition. Addison – Wesley.

[8] Molish F. Andreas. (2011). Wireless Communications. 2ND Edition. John Wiley & Sons, Ltd..

[9] (2007-12-12). The Brief History Of Internet

URL: http://www.webhostingsearch.com/articles/history-of-internet.php

[10] Gromov Gregory. (2011). Roads And Crossroads Of The Internet History.

URL: http://www.netvalley.com/cgi-bin/intval/net_history.pl?chapter=1

[11] Internet Society. (2011) A Brief History Of The Internet

URL: http://www.isoc.org/internet/history/brief.shtml

[12] Investintech.com. (2011). A Brief Guide To The History Of The Internet.

URL: http://www.investintech.com/content/historyinternet/

[13] Netvalley. (27-10-2011). History Of The Internet: Timeline.

URL: http://www.netvalley.com/archives/mirrors/davemarsh-timeline-1.htm

[14] SRI International. (2009). The Computer History Museum, SRI International, And BBN Celebrate The 40TH Anniversary Of First ARPANET Transmission, Precursor To Today's Internet.

URL: http://www.sri.com/news/releases/102709.html

## ΚΕΦΑΛΑΙΟ 2

[1] Αλεξόπουλος Άρης, Γιώργος Λαγογιάννης. (2003). Τηλεπικοινωνίες και Δίκτυα Υπολογιστών. 6η Έκδοση. ΑΦΟΙ ΡΟΗ Α.Ε.. Αθήνα.

[2] Stallings William. (2007). Ασύρματες Επικοινωνίες Και Δίκτυα. Εκδόσεις Τζιόλας.

[3] Fazel K., Kaiser S.. (2008). Multi – Carrier And Spread Spectrum Systems. From OFDM And MC-CDMA To LTE And WiMAX. 2ND Edition. John Wiley & Sons, Ltd..

[4] Garg K. Vijay. (2007). Wireless Communications And Networking. Elsevier, Inc..

[5] Halsall Fred. (2005). Computer Networking And The Internet. 5TH Edition. Addison – Wesley.

[6] Mohammad Ilyas, Syed Ahson. (2005). Handbook Of Wireless Local Area Networks. Applications, Technology, Security And Standards. Taylor & Francis Group.

[7] Molish F. Andreas. (2011). Wireless Communications. 2ND Edition. John Wiley & Sons, Ltd..

[8] Poole Ian. (2006). Cellular Communications Explained. From Basics To 3G. Newnes.

## ΚΕΦΑΛΑΙΟ 3

[1] Αλεξόπουλος Άρης, Γιώργος Λαγογιάννης. (2003). Τηλεπικοινωνίες και Δίκτυα Υπολογιστών. 6η Έκδοση. ΑΦΟΙ ΡΟΗ Α.Ε.. Αθήνα.

[2] Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) (2010).

URL: http://www.eett.gr.

[3] Carpenter Tom, Barrett Joel. (2008). CWNA® Certified Wireless Network

Administrator, Official Study Guide(Exam PW0-100). 4η Έκδοση. USA: McGraw-Hill Companies.

[4] Coleman David D., Westsott David A.v.(2006). CWNA® Certified Wireless Network Administrator, Official Study Guide(Exam PW0-100). Indiana: Wiley Publishing, Inc.

[5] Conference of European Postal and Telecommunications Administrations. Homepage: http://www.cept.org.

[6] European Telecommunications Standards Institute.

Homepage: http://www.etsi.org.

[7] Federal Communications Committee.

Homepage: http://www.fcc.gov.

[8] Finneran F. Michael. (2008). Voice Over WLAN: the Complete Guide. Elsevier Inc..USA.

[9] Gast Matthew. (2005). 802.11 Wireless Networks: The Definitive Guide. 2η Έκδοση. USA: O'Reilly Media.

[10] International Telecommunications Union.

Homepage: http://www.itu.int

[11] Institute of Electrical and Electronics Engineers.

Homepage: www.ieee.org

[12] Institute of Electrical and Electronics Standards Status Report for 802.11: http://standards.ieee.org/cgi-bin/status.

[13] Kartalopoulos V. Stamatios. (2009). Security of Information and Communication Networks. John Wiley & Sons Inc. Canada.

[14] Nikopolitidis P. , Obaidat M.S., Papadimitriou G.I. , Pomportsis A.S.. (2006). Ασύρματα Δίκτυα. 1η Έκδοση. Κλειδάριθμος. Αθήνα

[15] Rackley Steve. ( 2007). Wireless Networking Technology:From Principles to Successful Implementation. Oxford: Elsevier.

[16] Sobh Tarek, Elleithy Khaled, Mahmood Ausif. (2008). Novel Algorithms and Techniques in Telecommunications : Automation and Industrial Electronics. Springer Science+Business Media B.V.. USA.

[17 ]Tanenbaum, S. Andrew. (2003). Δίκτυα Υπολογιστών. 4η έκδ. Μετάφρ. Γ. Ξυλωμένος.Αθήνα: Κλειδάριθμος.

[18] Wang Haojin Henry. (2003). Packet broadband network handbook. The McGraw-Hill Companies. USA.

[19] Wi-Fi Alliance.

Homepage: http://www.wi-fi.org.

## ΚΕΦΑΛΑΙΟ 4

[1] Αλεξόπουλος Άρης, Γιώργος Λαγογιάννης. (2003). Τηλεπικοινωνίες και Δίκτυα Υπολογιστών. 6η Έκδοση. ΑΦΟΙ ΡΟΗ Α.Ε.. Αθήνα.

[2] Garg K. Vijay. (2007). Wireless Communications And Networking. Elsevier, Inc..

[3] Gast Matthew. (2002). 802.11 Wireless Networks: The Define Guide. O' Reilly & Associates, Inc..

[4] Minoli Daniel. (2002). Hotspot Networks: Wi-Fi For Public Acess Locations. 1ST Edition. McGraw – Hill.

[5] Molish F. Andreas. (2011). Wireless Communications. 2ND Edition. John Wiley & Sons, Ltd..

[6] Poole Ian. (2006). Cellular Communications Explained. From Basics To 3G. Newnes.

[7] URL:
http://www.iphelp.ru/doc/3/Cisco.Press.802.11.Wireless.LAN.Fundamentals.eBook-LiB/1587050773_ch03lev1sec2.html

[8] Couey Anna. (1997). About CDMA Spread Spectrum.

URL:
http://people.seas.harvard.edu/~jones/cscie129/nu_lectures/lecture7/hedy/lemarr.htm

[9] DATA COMMUNICATIONS. (2008). LECTURE#22 – WIRELESS NETWORKING.

URL: http://ironbark.bendigo.latrobe.edu.au/subjects/DC/lectures/22/

[10] MAXIM. (18-2-2003). An Introduction To Spread – Spectrum Communications.

URL: http://www.maxim-ic.com/app-notes/index.mvp/id/1890

## ΚΕΦΑΛΑΙΟ 5

[1] Αλεξόπουλος Άρης, Γιώργος Λαγογιάννης. (2003). Τηλεπικοινωνίες και Δίκτυα Υπολογιστών. 6η Έκδοση. ΑΦΟΙ ΡΟΗ Α.Ε.. Αθήνα.

[2] Stallings William. (2007). Ασύρματες Επικοινωνίες Και Δίκτυα. Εκδόσεις Τζιόλας.

[3] Brenner Pablo. (1997). A Technical Tutorial On The IEEE 802.11 Protocol. BreezeCOM Wireless Communications.

[4] Coleman David, Westcott David. (2006). CWNA: Certified Wireless Network Administrator Study Guide. Wiley Publishing,Inc., Indianapolis, Indiana.

[5] Garg K. Vijay. (2007). Wireless Communications And Networking. Elsevier, Inc..

[6] ] Gast Matthew. (2002). 802.11 Wireless Networks: The Define Guide. O' Reilly & Associates, Inc..

[7] Halsall Fred. (2005). Computer Networking And The Internet. 5TH Edition. Addison – Wesley.

[8] Molish F. Andreas. (2011). Wireless Communications. 2ND Edition. John Wiley & Sons, Ltd..

[9] Sarinnapakorn Kanoksri. (15-3-2001). "High Rate" Wireless Local Area Networks.

URL:http://www.cs.uccs.edu/~gsc/pub/master/pjfong/UCCS%20Project/Articles/IEEE%20802_11b%20High%20Rate%20Wireless%20LANs.htm

## ΚΕΦΑΛΑΙΟ 6

[1] Hardy Daniel, Malleus Guy, Mereur Jean-Noel. (2002). Networks: Internet,Telephony, Multimedia Convergences and complementarities. translation Horne Michael. De Boeck Supérieur. Paris.

[2] Infrared Data Association.

Homepage: http://www.irda.org

[3] Gehrmann Christian, Person Joakim, Smeets Ben. (2004). Bluetooth security. Artech House,INC.. London.

[4]Kartalopoulos V. Stamatios. (2009). Security of Information and Communication Networks. John Wiley & Sons Inc. Canada.

[5] Nikopolitidis P. , Obaidat M.S., Papadimitriou G.I. , Pomportsis A.S.. (2006). Ασύρματα Δίκτυα. 1η Έκδοση. Κλειδάριθμος. Αθήνα.

[6] Rackley Steve. (2007). Wireless Networking Technology: From Principles to Successful Implementation. Oxford: Elsevier.

[7] Santamaría Asunción, López-Hernández J. Francisco. (2001). Wireless LAN Standards and Applications Artech House. Inc,London.

[8] Tanenbaum S. Andrew. (2003). Δίκτυα Υπολογιστών. 4η Έκδοση. Μετάφρ. Γ. Ξυλωμένος. Αθήνα: Κλειδάριθμος.

[9] The Official Bluetooth SIG Member.

Web Site: https://www.bluetooth.org/apps/content/.

[10] The Official Bluetooth® Technology.

Web Site: http://www.bluetooth.com.

[11] Wang Haojin Henry. (2003.) Packet broadband network handbook. The McGraw-Hill Companies. USA.

ΚΕΦΑΛΑΙΟ 7

[1] IEEE Standard for Local and metropolitan area networks IEEE Std 802.16™-2009, Part 16: Air Interface for Broadband Wireless Access Systems.

URL: http://standards.ieee.org/cgi-bin/status.

[2] IEEE Standard for Local and metropolitan area networks IEEE Std 802.16™-2004, Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

URL: http://standards.ieee.org/cgi-bin/status.

[3] Nuaym Loutfi. (2007). WiMAX Technology for Broadband Wireless Access. John Wiley and Sons Ltd. England.

[4] Tanenbaum S. Andrew. (2003). Δίκτυα Υπολογιστών. 4η Έκδοση. Μετάφρ. Γ. Ξυλωμένος.Αθήνα: Κλειδάριθμος.

[5] WiMAX Forum.

Homepage: http://www.wimaxforum.org/.

[6] WiMAX Forum. (2006). Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation. August 2006.

ΚΕΦΑΛΑΙΟ 8

[1] Καμπουράκης Γ., Γκρίτζαλης Σ., Κάτσικας Σ.. (2006). Ασφάλεια Ασύρματων και Κινητών Δικτύων Επικοινωνιών. εκδόσεις Παπασωτηρίου. Αθήνα.

[2] Ahson Syed, Ilyas Mohammmad. (2008). WiMAX Standards and Security. Taylor & Francis Group. USA.

[3] Bigdoli Hossein. (2004). Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection and Management Volume 3. California State University Bakersfield. California: John Wiley & Sons.

[4] Edney Jon and Arbaugh William A.. (2003). Real 802.11 Security: Wi-Fi Protected Access and 802.11i. USA: Addison Wesley.

[5] Gast S. Matthew. (2002). 802.11 Wireless Networks: The Definitive Guide. O'Reilly & Associates Inc.. USA .

[6] Gehrmann Christian, Person Joakim, Smeets Ben. (2004). Bluetooth security, Artech House, Inc.. London.

[7] Joshi B.D. James. (2008). Network Security: Know it all. Elsevier Inc.. USA.

[8] Kartalopoulos V. Stamatios. (2009). Security of Information and Communication Networks. John Wiley & Sons Inc. Canada.

[9] Knudsen, L. R.. (2000). "A Detailed Analysis of Safer k." *J. Cryptology*, Vol. 13. No. 4

[10] Praphul Chandra, Bensky Alan, Olexa Ron, Dobkins Daniel Mark, Lide David. (2008). Wireless Networking: Know it all. Elsevier Inc.. USA.

[11] Sobh Tarek, Elleithy Khaled, Mahmood Ausif. (2008). Novel Algorithms and Techniques in Telecommunications: Automation and Industrial Electronics. Springer Science+Business Media B.V.. USA.

[12] Tang Yee Seok, Muler Peter, Sharif Hamid R.. (2010). WiMAX Security and Quality of Service: An End-to-End Perspective. John Wiley & Sons. UK.

[13] Vacca John A. (2010). Network and System Security. Elsevier Inc.. USA.

[14] Vacca, John R.. (2009). Computer and Information Security Handbook. Elsevier Ink.. USA.

[15] Wi-Fi Alliance, Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup.

URL: http://www.wi-fi.org/wifi-protected-setup.

[16] Wi-Fi Alliance, Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup™: Easing the User Experience for Home and Small Office Wi-Fi® Networks.

URL: http://www.wi-fi.org/files/kc/20090123_Wi-Fi__Protected_Setup.pdf.

# ΠΑΡΑΡΤΗΜΑ

## A

***Amplitude Shift Keying (*ASK)**

Η ψηφιακή διαμόρφωση πλάτους ASK είναι η πιο απλή μορφή ψηφιακής διαμόρφωσης. Το πλάτος του ημιτονικού σήματος-φέροντος μεταβάλλεται αναλογικά με την τιμή του ψηφιακού σήματος πληροφορίας.

**Asynchronous Transfer Mode (ATM)**

Η κατάσταση Ασύγχρονης μετάδοσης είναι μία τεχνολογία δικτύου υψηλής ταχύτητας, στην οποία το δίκτυο αποτελείται από έναν ή περισσότερους μεταγωγείς που είναι συνδεδεμένοι μεταξύ τους ώστε να δημιουργούν μία ίνα μεταγωγής. Το ATM είναι συνδεσμοστρεφής τεχνολογία δικτύου που χρησιμοποιεί στο χαμηλότερο επίπεδο μικρά κελιά σταθερού μεγέθους. Στη τεχνολογία αυτή οι υπολογιστές για να μεταφέρουν δεδομένα πρέπει να δημιουργήσουν ένα εικονικό κύκλωμα στο δίκτυο. Η τεχνολογία υποστηρίζει τη μετάδοση φωνής, βίντεο και δεδομένων.

**Auto Rate Fallback (ARF)**

Το ARF καθορίζει σταθερά κατώτερα όρια για την αύξηση ή την μείωση του ρυθμού μετάδοσης των απεσταλμένων δεδομένων ανάλογα με τον αριθμό των επιτυχιών ή των αποτυχιών των συνεχόμενων προσπαθειών μετάδοσης. Ο ρυθμός μετάδοσης μειώνεται όταν έχουμε δύο συνεχόμενες αποτυχημένες προσπάθειες μετάδοσης και αυξάνεται όταν έχουμε δέκα συνεχόμενες προσπάθειες επιτυχούς μετάδοσης. Αν ο ρυθμός μετάδοσης αυξηθεί και υπάρξει αποτυχία στην προσπάθεια μετάδοσης, τότε μειώνεται αμέσως ο ρυθμός μετάδοσης. Με αυτό τον τρόπο γίνεται εκμετάλλευση του αποτελεσματικότερου υψηλού ρυθμού μετάδοσης τη κάθε στιγμή. Δεν συνίσταται σε περιπτώσεις πολλών χρηστών επειδή δε διακρίνονται οι αποτυχίες εξαιτίας λαθών που δημιουργούνται κατά την προσπάθεια δέσμευσης του καναλιού.

## B

## C

**Connection ID (CID)**

Το αναγνωριστικό σύνδεσης είναι ένας μοναδικός ακέραιος που έχει εκχωρηθεί σε κάθε σύνδεση και διατηρείται στο κατάλογο του εξυπηρετητή. Χρησιμοποιείται κυρίως για την είσοδο σε μία σύνδεση, έτσι ώστε να εκτελούνται οι διάφορες εργασίες που έχουν ρυθμιστεί στη συγκεκριμένη σύνδεση.

Το αναγνωριστικό σύνδεσης έχει έναν μετρητή, ο οποίος ξεκινά από το μηδέν για την πρώτη σύνδεση που λαμβάνεται από το διακομιστή και αυξάνεται κατά ένα για κάθε επιπλέον σύνδεση. Ο μετρητής μηδενίζεται κάθε φορά που ο διακομιστής κάνει επανεκκίνηση. Αρνητικές τιμές ορίζονται στις εσωτερικές συνδέσεις, οι οποίες χρησιμοποιούνται για την επεξεργασία των εσωτερικών λειτουργιών, έτσι ώστε να ξεχωρίζουν από τις εξωτερικές συνδέσεις.

**Complementary Code Keying (CCK)**

Η συμπληρωματική μεταλλαγή κωδικών διαιρεί την chip ακολουθία σε κωδικοσύμβολα των 8 bit. Η μέθοδος αυτή χρησιμοποιεί 64 κωδικολέξεις των 8 bit, οι οποίες παράγονται μερικώς από τα δεδομένα και χρησιμοποιούνται τόσο για να εξαπλώσουν το σήμα αλλά και για να μεταφέρουν πληροφορία. Αυτές οι ακολουθίες των 8 bit, με τη χρήση κατάλληλων μαθηματικών μετασχηματισμών, μπορούν να κωδικοποιήσουν 4 ή ακόμα και 8 bit πετυχαίνοντας τα 5.5 και 11 Mbps αντίστοιχα.

**Cyclic Redundancy Check (CRC)**

Ο Κωδικός Κυκλικού Πλεονασμού είναι μία μέθοδος που υπολογίζει μία μικρή ακέραια τιμή**.** Η ακέραια αυτή τιμή υπολογίζεται από μία ακολουθία οκτάδων, η οποία χρησιμοποιείται για τον εντοπισμό σφαλμάτων και η οποία προκύπτει όταν η ακολουθία οκτάδων μεταδίδεται από ένα μηχάνημα σε άλλο. Το υλικό δικτύου μεταγωγής πακέτων υπολογίζει έναν κωδικό κυκλικού πλεονασμού και τον προσαρτά στο πακέτο κατά τη μετάδοση. Με τη λήψη, το υλικό επαληθεύει τα περιεχόμενα του πακέτου υπολογίζοντας πάλι τον κωδικό κυκλικού πλεονασμού και συγκρίνοντας το με τη τιμή που στάλθηκε.

## D

**Differencial PSK (DPSK)**

Η ψηφιακή διαμόρφωση διαφορικής διαμόρφωσης φάσης είναι παραλλαγή της PSK (δείτε παρακάτω) και έχουμε DPSK των δύο, τεσσάρων και οχτώ φάσεων. Στη διαμόρφωση

αυτή, η πληροφορία είναι κωδικοποιημένη στη διαφορά φάσης μεταξύ δύο διαδοχικών συμβόλων (**baud**:ρυθμός μετάδοσης διαμορφωμένου σήματος) και όχι στην απόλυτη τιμή φάσης του κάθε συμβόλου (όπως στην PSK).

**Dynamic Host Configuration Protocol (DHCP)**

Το Πρωτόκολλο Δυναμικής Διευθέτησης Υπολογιστών Υπηρεσίας παρέχει δυναμική εκχώρηση διευθύνσεων, επιτρέπει σε έναν υπολογιστή να αποκτά όλες τις πληροφορίες διευθέτησης που χρειάζεται σε ένα μόνο μήνυμα. Για να χρησιμοποιηθεί το DHCP πρέπει ο διαχειριστής να διευθετήσει ένα διακομιστή DHCP, παρέχοντας του ένα σύνολο διευθύνσεων. Το DHCP επιτρέπει στο διαχειριστή την αυτόματη διευθέτηση, τη μη αυτόματη διευθέτηση και τη δυναμική διευθέτηση. Η αυτόματη διευθέτηση παρέχει την εκχώρηση μιας μόνιμης διεύθυνσης σε έναν υπολογιστή που εισέρχεται πρώτη φορά στο δίκτυο. Η μη αυτόματη διευθέτηση παρέχει στον διαχειριστή να επεξεργαστεί/ορίσει/διευθετήσει μία συγκεκριμένη διεύθυνση για έναν συγκεκριμένο υπολογιστή. Η δυναμική εκχώρηση περιλαμβάνει μια προσωρινή διεύθυνση στον υπολογιστή για ορισμένο χρονικό διάστημα.

# E

# F

**Forward error correction (FEC)**

Το FEC είναι μία κωδικοποίηση Αυτόματης διόρθωσης λαθών. Η πληροφορία διέρχεται μέσα από το module κωδικοποίησης, όπου με κατάλληλες πράξεις δημιουργείται μια καινούρια λέξη. Κατά κανόνα, η λέξη αυτή είναι μικρότερη ή ίση με την λέξη της πληροφορίας. Τα bits της λέξης που προκύπτει ονομάζονται και πλεονάζοντα ή bit ισοτιμίας (parity bits), λόγω της προσθήκης τους στο τέλος της λέξης της πληροφορίας. Η λέξη πληροφορίας με την λέξη που δημιουργήθηκε από την κωδικοποίηση ονομάζεται κωδική λέξη και, όπως είναι φυσικό, έχει μήκος μεγαλύτερο από τη λέξη πληροφορίας.

**Frequency Division Duplexing (FDD)**

Η τεχνική αμφιδρόμησης με διαίρεση συχνότητας διαιρεί το διαθέσιμο εύρος ζώνης σε δυο υπο-κανάλια μονού δρόμου διαχωρίζοντας με αυτό τον τρόπο την ανερχόμενη και την κατερχόμενη ζεύξη.

**Frequency Division Multiplexing (FDM)**

Η Πολύπλεξη με Διαίρεση Συχνότητας είναι μία μέθοδος για την μεταβίβαση πολλών ανεξάρτητων σημάτων σε ένα μόνο μέσο, εκχωρώντας στο κάθε σήμα μία μοναδική συχνότητα φορέα.

***Frequency Shift Keying (FSK)***

Στη ψηφιακή διαμόρφωση συχνότητας, η συχνότητα του ημιτονικού φέροντος σήματος μεταβάλλεται με διακριτό τρόπο ανάλογα με την τιμή του ψηφιακού σήματος πληροφορίας. Στην πιο απλή περίπτωση, αντιστοιχεί μία τιμή συχνότητας για την δυαδική τιμή «0» και μία άλλη τιμή συχνότητας για τη δυαδική τιμή «1».

**File Transfer Protocol (FTP)**

Το πρωτόκολλο Μεταφοράς Αρχείων είναι το πρωτόκολλο υψηλού επιπέδου που χρησιμοποιείται για την μεταφορά αρχείων από ένα μηχάνημα σε ένα άλλο.

## G

**(Gaussian) Minimum Shift Keying – (G) MSK**

Η ελάχιστη ολίσθηση κωδικοποίησης (**MSK**) είναι ένας ειδικός τύπος συνεχούς φάσης κωδικοποίησης ολίσθησης συχνότητας (Continuous Phase Frequency Shift Keying CPFSK). Είναι δηλαδή μια τεχνική όπου δεν μεταβάλλεται η φάση του φέροντος ανάλογα με το σήμα πληροφορίας, αλλά η συχνότητά του. Η GMSK είναι μια μορφή της MSK όπου το απαιτούμενο εύρος ζώνης μειώνεται ακόμα περισσότερο με το πέρασμα της διαμορφωμένης κυματομορφής από ειδικό χαμηλοπερατό φίλτρο (Gaussian filter).

Είναι διαμόρφωση συνεχούς φάσης και σταθερού πλάτους. Αυξάνει τη φασματική απόδοση και έχει εξαιρετική απόδοση ισχύος επειδή δεν έχει απότομες αλλαγές στη φάση. Επίσης μετατρέπει το δυαδικό σήμα σε αναλογικό στην κατάλληλη συχνότητα και την κατάλληλη χρονική στιγμή, συμβιβάζοντας την απόδοση φάσματος και την πολυπλοκότητα αποδιαμόρφωσης με χαμηλό επίπεδο παρεμβολών γειτονικών διαύλων.

# H

**HHH**

Ο κώδικας HHH είναι ένας Run Length Limited κώδικας που παρέχει απόδοση ισχύος και απόδοση του εύρου ζώνης για τον υψηλό ρυθμό μετάδοσης δεδομένων. Ο κώδικας HHH (1,13) εγγυάται ότι θα υπάρχει τουλάχιστον ένα και το μέγιστο 13 κενά ανάμεσα σε κάθε παλμό.

**Hypertext Transfer Protocol (HTTP)**

Το πρωτόκολλο μεταφοράς Υπερκειμένου χρησιμοποιείται για τη μεταφορά εγγράφων Ιστού από ένα διακομιστή σε ένα φυλλομετρητή.

# I

**Internet Protocol (IP)**

Το Internet Protocol αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση αυτοδύναμων πακέτων (datagrams). Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους, και αποτελεί το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το διαδίκτυο.

**IP Security (IPSec)**

Η IPSec είναι ένα πρωτόκολλο ανοιχτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών. Είναι βασισμένο στις προδιαγραφές που ανέπτυξε η ομάδα εργασίας του Internet. Η IPSec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο. Η IPSec παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφάλειας σε ένα δίκτυο.

# J

# K

# L

**Light Emitting Diode (LED)**

Δίοδος Εκπομπής Φωτός αποκαλείται ένας ημιαγωγός ο οποίος εκπέμπει φωτεινή ακτινοβολία στενού φάσματος, όταν του παρέχεται μία ηλεκτρική τάση κατά τη φορά ορθής πόλωσης. Το χρώμα του φωτός που εκπέμπεται εξαρτάται από τη χημική σύσταση του ημιαγώγιμου υλικού που χρησιμοποιείται και μπορεί να είναι υπεριώδες, ορατό ή υπέρυθρο.

# M

**Multiple Input Multiple Output (MIMO)**

Το σύστημα Πολλαπλής Εισόδου Πολλαπλής Εξόδου χρησιμοποιεί πολλαπλές κεραίες, οι οποίες τοποθετούνται για την μετάδοση και την λήψη των σημάτων, έτσι ώστε να βελτιωθεί η απόδοση της επικοινωνίας. Ο χωρικός διαχωρισμός των κεραιών επιτρέπει καλύτερη διάκριση και επωφελείται από το όφελος των πολλαπλών διαδρομών. Το σύστημα MIMO ρυθμισμένο να χρησιμοποιεί το όφελος των πολλαπλών διαδρομών, δεν επιτρέπει στο εισερχόμενο σήμα να υποβαθμιστεί από τα εμπόδια, τις αντανακλάσεις, τις αναπηδήσεις και τον διαχωρισμό του σε τμήματα.

# N

# O

# P

**Packet Binary Convolutional Coding (PBCC)**

Η δυαδική συνελικτική κωδικοποίηση πακέτου, χρησιμοποιεί την 8-PSK και είναι προαιρετική τεχνική διαμόρφωσης για το 802.11g. Η κωδικοποίηση PBCC προσφέρει υψηλό ρυθμό μετάδοσης για συγκεκριμένο μήκος chip κωδικών. Επίσης, προσφέρει υψηλή αποδοτικότητα για συγκεκριμένο ρυθμό μετάδοσης χρησιμοποιώντας μεγαλύτερο μήκος chip κωδικών.

***Phase Shift Keying (PSK, Ψηφιακή Διαμόρφωση Φάσης)***

Στην περίπτωση αυτή είναι η φάση του ημιτονικού φέροντος που μεταβάλλεται συναρτήσει του σήματος πληροφορίας. Η πιο απλή μορφή της είναι η ***δυαδική PSK (Binary Phase Shift Keying – BPSK)*** όπου χρησιμοποιείται μία από τις δυο φάσεις για την κωδικοποίηση ενός bit. Χρησιμοποιείται η φάση 180° για την κωδικοποίηση του «0» και η φάση 0° για την κωδικοποίηση του «1».

Η ψηφιακή διαμόρφωση **QPSK (Quaternary Phase Shift Keying** ή **4-PSK)** έχει την ιδιότητα της ορθογωνικότητας χρησιμοποιώντας μία από τις τέσσερις φάσεις για την κωδικοποίηση από ένα ως τέσσερα σύμβολα των δύο bit. Η κάθε φάση έχει διαφορά 90° η μία από την άλλη. Η μέθοδος μπορεί να χρησιμοποιηθεί για την αποστολή πληροφορίας με ταχύτητα διπλάσια από αυτήν της BPSK στο ίδιο εύρος ζώνης, χωρίς να υποβαθμιστεί η απόδοση της ανίχνευσης ως προς την BPSK. Στη ψηφιακή διαμόρφωση **8PSK** χρησιμοποιούνται μία από τις οχτώ φάσεις για την κωδικοποίηση από ένα ως οχτώ συμβόλων των τριών bit.

# Q

***Quadrature Amplitude Modulation (QAM)***

Η διαμόρφωση QAM είναι ένας συνδυασμός PSK και διαμόρφωσης πλάτους. Το QAM σήμα έχει τόσες καταστάσεις όσοι είναι οι πιθανοί συνδυασμοί πλάτους και φάσης των φερόντων σημάτων. Για την **4-QAM** έχουμε μία τιμή πλάτους και τέσσερις διαφορετικές καταστάσεις κωδικοποιώντας δύο bits τη φορά. Για τη διαμόρφωση **8-QAM** έχουμε δύο διαφορετικές τιμές πλάτους και τέσσερις διαφορετικές φάσεις έχουμε 2 x 4 = 8 διαφορετικές καταστάσεις κωδικοποιώντας τρία bit τη φορά. Για την 16-QAM έχουμε

τέσσερις διαφορετικές τιμές πλάτους και τέσσερις διαφορετικές φάσεις κωδικοποιώντας τέσσερα bits τη φορά.

# R

**Routing Information Protocol (RIP)**

Το πρωτόκολλο RIP αποτελεί άμεση υλοποίηση της δρομολόγησης διανύσματος απόστασης για τοπικά δίκτυα. Διαχωρίζει τις συμμετέχουσες μηχανές σε ενεργητικές και παθητικές. Οι ενεργητικές μηχανές κοινοποιούν τις διαδρομές τους στις υπόλοιπες, ενώ οι παθητικές δέχονται τα μηνύματα RIP και τα χρησιμοποιούν για να ενημερώσουν τον πίνακα δρομολόγησης που διαθέτουν, δεν κάνουν όμως κοινοποιήσεις. Μόνο ο δρομολογητής μπορεί να εκτελέσει το πρωτόκολλο RIP σε ενεργητική κατάσταση. Οι υπολογιστές υπηρεσίας πρέπει να εκτελέσουν τη παθητική.

**Return-to-zero, inverted**

Η RZI είναι μία μέθοδος της χαρτογράφησης για την μετάδοση. Το 2-level RZI σήμα έχει ένα παλμό αν το δυαδικό σήμα είναι 0 και κανένα παλμό αν το δυαδικό σήμα είναι 1.

# S

**Simple Network Management Protocol (SNMP)**

Το Πρωτόκολλο Διαχείρισης Απλού Δικτύου χρησιμοποιείται για τη διαχείριση συσκευών όπως υπολογιστές υπηρεσίας, δρομολογητές και εκτυπωτές.

**Space/Spatial Division Multiple Access (SDMA)**

Στην Πολυπλεξία Διαίρεσης χώρου γίνεται χωρικός διαχωρισμός των χρηστών από το σταθμό βάσης ανάλογα με τη θέση που κατέχει την κάθε στιγμή ο κινητός χρήστης. Ο σταθμός λαμβάνει όλα τα σήματα και με βάση την ακτινοβολούμενη ισχύ των κινητών τερματικών μπορεί και απομονώνει το χρήστη με τον οποίο θέλει να επικοινωνήσει .Όλοι οι χρήστες του συστήματος μπορούν και επικοινωνούν την ίδια χρονική στιγμή κάνοντας χρήση στον ίδιο ραδιοδίαυλο. Τα ιδανικά αποτελέσματα της μεθόδου αυτής μπορούν να υλοποιηθούν με την χρησιμοποίηση προσαρμοστικών κεραιών, οι οποίες θα μπορούν να

συλλέγουν τις διάφορες συνιστώσες, από πολλαπλές διαδρομές για όλα τα τερματικά και να τις συνδυάζουν με τον αποδοτικότερο δυνατό τρόπο για την συλλογή όλης της διαθέσιμης ενέργειας των σημάτων.

**Space Time Coding (STC)**

Η χωροχρονική κωδικοποίηση είναι μία τεχνική κωδικοποίησης των συμβόλων της πληροφορίας στο χώρο και στο χρόνο, όπως είναι και η ονομασία της. Η τεχνική αυτή παρέχει πολλαπλά αντίγραφα των δεδομένων στο δέκτη για την βελτίωση της αξιοπιστίας του συστήματος σε συνθήκες εξασθένισης χωρίς να αυξάνεται το εύρος ζώνης. Κατά τη διαδικασία της μετάδοσης ο κωδικοποιητής επεξεργάζεται τα δεδομένα και σε κάθε περίοδο μετάδοσης παράγει σύμβολα κώδικα. Ο αριθμός των συμβόλων ισούται με το πλήθος των κεραιών μετάδοσης. Κάθε σύμβολο αποστέλλεται από διαφορετική κεραία κατά την ίδια χρονική στιγμή. Για την αποκωδικοποίηση γίνεται η ίδια διαδικασία στον δέκτη.

## T

**Time Division Duplexing (TDD)**

Η τεχνική αμφιδρόμησης με διαίρεση χρόνου ορίζει χρονοθυρίδες για την εκπομπή και τη λήψη. Η ανερχόμενη και η κατερχόμενη ζεύξη διαχωρίζονται στο χρόνο αλλά στην ίδια συχνότητα.

**Time Division Multiplexing (TDM)**

Η Πολύπλεξη Χρονικής Διαίρεσης είναι μία τεχνική που χρησιμοποιείται για την πολύπλεξη πολλών σημάτων σε ένα μόνο κανάλι μετάδοσης υλικού και επιτρέπει σε κάθε σήμα να χρησιμοποιεί το κανάλι για σύντομο χρονικό διάστημα, πριν προχωρήσει στο επόμενο σήμα.

**Transmission Control Protocol (TCP)**

Το πρωτόκολλο Ελέγχου Μετάδοσης παρέχει αξιόπιστη και πλήρως αμφίδρομη υπηρεσία ρεύματος δεδομένων στην οποία βασίζονται πολλά πρωτόκολλα εφαρμογών. Το TCP επιτρέπει σε μία διεργασία ενός μηχανήματος να στείλει ένα ρεύμα δεδομένων σε μία διεργασία ενός άλλου μηχανήματος.

# U

**Unshielded Twisted Pair (UTP)**

Το καλώδιο UTP είναι το πιο συνηθισμένο μέσω δικτύωσης. Αποτελείται από τέσσερα ζεύγη λεπτών, χάλκινων καλωδίων εκ των οποίων το κάθε ένα είναι καλυμμένο με χρωματιστή πλαστική επένδυση. Όλα μαζί είναι καλυμμένα με μια πλαστική εξωτερική επένδυση. Ονομάζεται αθωράκιστο γιατί απλούστατα δεν περιέχει καμία θωράκιση από εξωτερικές παρεμβολές. Ο τύπος βύσματος που χρησιμοποιείται για το UTP είναι το RJ-45.

**User Datagram Protocol (UDP)**

Το Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη επιτρέπει σε ένα πρόγραμμα Εφαρμογής ενός μηχανήματος να στείλει ένα αυτοδύναμο πακέτο σε ένα πρόγραμμα Εφαρμογής ενός άλλου μηχανήματος. Το UDP χρησιμοποιεί το IP(Internet Protocol) για την παράδοση αυτοδύναμων πακέτων.

# V

# W

**Wireless Internet Service Provider (WISP)**

Ο WISP είναι ο Φορέας Παροχής Υπηρεσιών Internet των ασύρματων δικτύων.

# X

# Y

# Ζ

**Ομοαξονικά καλώδια**

Τα ομοαξονικά καλώδια είναι πιο δύσκαμπτα από τα υπόλοιπα καλώδια και επιπλέον τα πιο ακριβά. Το πλεονέκτημά τους είναι ότι έχουν μεγαλύτερο εύρος ζώνης, δεν είναι ευαίσθητα και επιτυγχάνουν μεγάλες ταχύτητες. Τα ομοαξονικά καλώδια αποτελούνται από δύο αγωγούς. Ο ένας βρίσκεται κεντρικά στο καλώδιο και περιβάλλεται από μονωτικό υλικό και ο εξωτερικός αγωγός είναι σε μορφή πλέγματος το οποίο και αυτό το περιβάλει μονωτικό υλικό. Με αυτόν τον τρόπο αποκτά αντοχή και το κάνει χρήσιμο σε περιοχές όπου υπάρχουν ηλεκτρικές παρεμβολές.