ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σκουλίκης Αθανάσιος

ΑΜ:9090

E-mail:Thanasis.1988@windowslive.com

ΤΙΤΛΟΣ: «ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ Wi-Fi»

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

κ.ΡΙΖΟΣ ΓΕΩΡΓΙΟΣ

ΑΡΤΑ ΙΟΥΝΙΟΣ 2014

ΕΥΧΑΡΙΣΤΙΕΣ

Τελικά ήρθε ο καιρός να τελειώσει και η τελευταία εργασία των σπουδών μου στο τμήμα Μηχανικών και Πληροφορικής.Ομολογώ ότι από το ξεκίνημα των σπουδών μου στο τμήμα αυτό δεν σκέφτηκα ότι θα έρθει αυτή η στιγμή.Βέβαια,το ότι τελειώνουν οι σπουδές αυτές δεν σημαίνει ότι πρέπει να σταματήσει η αναζήτηση της γνώσης,τόσο στους υπολογιστές όσο και γενικότερα. Θα ήθελα να ευχαριστήσω όσους με βοήθησαν στην πραγματοποίηση αυτής της διπλωματικής εργασίας:Τον επιβλέποντα αυτής της διπλωματικής εργασίας Καθηγητή κ. Ρίζο Γεώργιο για την καθοδήγηση του στην πραγματοποίηση αυτής της εργασίας.Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου που μου στάθηκαν στην διάρκεια των σπουδών μου.

ΔΗΛΩΣΗ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Η παρούσα εργασία αποτελεί προϊόν αποκλειστικά δικής μου προσπάθειας.Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας.Όλες οι πηγές που χρησιμοποιήθηκαν περιλαμβάνονται στη βιβλιογραφία.

ΠΡΟΛΟΓΟΣ

Η μεγάλη ανάγκη του ανθρώπου για επικοινωνία και ενημέρωση άμεσα και γρήγορα, οδήγησε στην εξέλιξη της τεχνολογίας με μεγάλα βήματα. Η ιστορία των ασύρματων δικτύων ξεκινάει από πολύ παλιά και συγκεκριμένα από το 1896 όταν ο Guglielmo Marconi ανακάλυψε τον ασύρματο τηλέγραφο. Τα πρώτα ασύρματα δίκτυα εμφανίστηκαν το 1964 ήταν Data και ήταν τεχνολογίαςTCP/IP.Στην εποχή μας η μετάδοση της πληροφορίας, η ανταλλαγή δεδομένων και η επικοινωνία βασίζεται αποκλειστικά στα δίκτυα (ιντερνέτ, τηλεφωνία).Η κινητή τηλεφωνία και η τεχνολογία του Internet, όταν βγήκαν στην αγορά συνάντησαν την ευρεία αποδοχή του κοινού σαν απάντηση στο πλήθος των υπηρεσιών και των δυνατοτήτων που του προσφέρθηκαν. Κάθε τεχνολογία από τη πλευρά της υποστήριξε την επικοινωνία, την ενημέρωση, την διασκέδαση σύμφωνα με τις προδιαγραφές και τις δυνατότητές της. Η τεχνολογία Wi-Fi χρησιμοποιείται για να συνδέει ασύρματες συσκευές μεγάλης ισχύος και υψηλής ταχύτητας όπως είναι οι σταθεροί και οι φορητοί υπολογιστές, δημιουργώντας έτσι ένα μεγάλο και γρήγορο δίκτυο τοπικού εύρους ζώνης (Local Area Network-LAN).Σε αυτό το δίκτυο μπορούν να συνδεθούν υπολογιστές PDAsκαι άλλες συσκευές όπου με την χρήση των σημείων πρόσβασης (Access Points) συνδέονται στο διαδίκτυο μεταφέρουν δεδομένα μεταξύ τους καθώς και άλλες εφαρμογές.Εφαρμογές οι οποίες με την χρήση της ασύρματης τεχνολογίας είναι σε θέση να εντοπίζουν την θέση των συσκευών των χρηστών με σκοπό την εκμετάλλευση της ίδιας πληροφορίας της θέσης και την αποστολή στους χρήστες διάφορων δεδομένων-πληροφοριών μια τέτοια τεχνολογία είναι το γνωστό GPS(GlobalPositioningSystem).Σήμερα τα ασύρματα συστήματα γνωρίζουν μια τεράστια άνθιση και χρησιμοποιούνται σε πάρα πολλές εφαρμογές.Σε αυτό βασικό ρόλο παίζουν τα πλεονεκτήματα που έχουν τα ασύρματα δίκτυα σε σχέση με τα ενσύρματα.Η φύση των ασύρματων δικτύων επιτρέπει την πρόσβαση στους δικτυακούς πόρους και την παροχή υπηρεσιών χωρίς καλωδίωση.Η ιδιαιτερότητα αυτή όμως πέρα από τα πλεονεκτήματα που παρουσιάζει, εμφανίζει αδυναμίες και πιο συγκεκριμένα αδυναμίες ασφάλειας. Στην διπλωματική αυτή εργασία παρουσιάζονται οι γνωστές αδυναμίες ασφάλειας καθώς και οι τρόποι αντιμετώπισής αυτών. Πιο συγκεκριμένα γίνεται μελέτη της ασύρματης τεχνολογίας Wi-Fi τα πλεονεκτήματα της, τα μειονεκτήματα της, οι εφαρμογές της, παρουσίαση του πρωτοκόλλου IEEE 802.11 και τα υποπρότυπα του καθώς και που μπορεί να εξελιχθεί μελλοντικά η συγκεκριμένη τεχνολογία. Αρχικά γίνεται μια ανάλυση των ειδικών δικτύων και δικτυακών τοπολογιών.

Λέξειςκλειδιά: Ασύρματα Τοπικά Δίκτυα,802.11,OSI,Τεχνολογία Wi-Fi, Τεχνολογία WiMAX(IEEE802.16), κρυπτογράφηση, παραβίαση, ασφάλεια, Υποπρότυπα 802.11WLAN, WWAN, WMAN, WPAN, WEP, WPA. Access Point, Ad-hoc.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1^{Ο}:ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

1.1 ΤΙ ΕΙΝΑΙ ΤΟ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ

Ως ασύρματο δίκτυο(Wireless Network) χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο το οποίο συνήθως είναι τηλεφωνικό ή δίκτυο υπολογιστών όπου με την χρήση ραδιοκυμάτων επιτυγχάνεται η μετάδοση δεδομένων.Μέσω των ηλεκτρομαγνητικών κυμάτων τα δεδομένα μεταφέρονται με συχνότητα η οποία κάθε φορά εξαρτάται από τον ρυθμό μετάδοσης των δεδομένων που απαιτεί το δίκτυο για να υποστηρίζεται.Τα χαμηλότερα συχνοτήτων ραδιοκύματα γενικά εξασθενούν σχετικά γρήγορα,διότι συγκριτικά μεταφέρουν λίγη ενέργεια,όμως έχουν την ικανότητα να διαπερνούν φυσικά εμπόδια.Αντίθετα τα ραδιοκύματα υψηλών συχνοτήτων αν και διαδίδονται σε μεγαλύτερες αποστάσεις ανακλώνται εύκολα από φυσικά εμπόδια.Σε αντίθεση με την ενσύρματη επικοινωνία,η ασύρματη επικοινωνία δεν χρησιμοποιεί ως μέσο μετάδοσης της πληροφορίας κάποιο τύπο καλωδίου.Σε παλαιότερες εποχές τα τηλεφωνικά δίκτυα ήταν αναλογικά,όμως σήμερα όλα τα ασύρματα δίκτυα βασίζονται στην ψηφιακή τεχνολογία,επομένως κατά μια έννοια είναι ουσιαστικώς δίκτυα υπολογιστών.Η υλοποίηση του ασύρματου δικτύου βασίζεται σε κάποια πρότυπα που θεσπίζει το Ινστιτούτο Ηλεκτρολόγων Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers – IEEE) και για αυτό είναι της μορφής IEEE 802.X (όπου X ένας αριθμός).Τα πρότυπα αυτά διαφέρουν ως προς την διαμόρφωση που χρησιμοποιούν και την ταχύτητα μετάδοσης.Στα ασύρματα δίκτυα εντάσσονται τα δίκτυα κινητής τηλεφωνίας,οι δορυφορικές επικοινωνίες,τα ασύρματα δίκτυα ευρείας περιοχής (WWAN),τα ασύρματα μητροπολιτικά δίκτυα (WMAN), τα ασύρματα τοπικά δίκτυα (WLAN) καθώς και τα ασύρματα προσωπικά δίκτυα (WPAN).Τα τελευταία χρόνια η εξέλιξη των ασύρματων επικοινωνιών δείχνει ότι ένα σύστημα που να μπορεί να ικανοποιήσει όλες τις ανάγκες του χρήστη και να προσαρμοστεί στις ιδιαιτερότητες του κάθε περιβάλλοντος είναι πολύ δύσκολο να υπάρξει.Έτσι για το λόγο αυτό τα ασύρματα δίκτυα τις επόμενες γενιές θα αποτελούνται από την ενοποίηση ενός συνόλου τεχνολογιών που κάθε μια από αυτές θα ειδικεύεται σε ένα συγκεκριμένο περιβάλλον.Αν και η τηλεόραση και το ραδιόφωνο,αν και ως τηλεπικοινωνιακά μέσα είναι εκ φύσεως ασύρματα στις περισσότερες περιπτώσεις,δεν συμπεριλαμβάνονται στα ασύρματα δίκτυα, καθώς η μετάδοση γίνεται προς πάσα κατεύθυνση χωρίς να υπάρχει κάποιο δομημένο δίκτυο.

Εικόνα: Παράδειγμα ενός ασύρματου (τοπικού) δικτύου.

1.2 ΚΑΤΗΓΟΡΙΕΣ ΔΙΚΤΥΩΝ

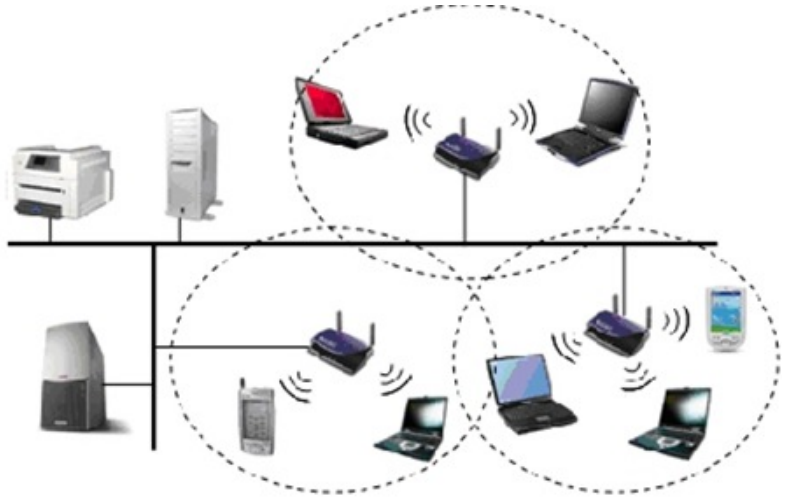
Τα ασύρματα δίκτυα ανάλογα με την κλίμακα τους χωρίζονται στις εξής κατηγορίες:

- WLAN (Wireless Local Area Network) ασύρματα δίκτυα τοπικής εμβέλειας.
- WWAN (Wireless Wide Area Network) ασύρματα δίκτυα ευρείας περιοχής.
- WMAN (Wireless Metropolitan Area Network) ασύρματα μητροπολιτικά δίκτυα.

Τα WLAN ασύρματα δίκτυα τοπικής εμβέλειας αποτελούν επέκταση ή ανταγωνιστική τεχνολογία των σταθερών τοπικών δικτύων σε κτήρια ή περιοχές μικρού εύρους μέχρι 100 μέτρα.Με το WLAN γίνεται δυνατή η ανταλλαγή δεδομένων μεταξύ υπολογιστών, έξυπνων τηλεφώνων, εκτυπωτών και άλλων περιφερειακών συσκευών με δυνατότητα σύνδεσης.Χρησιμοποιούν κυρίως την τεχνολογία της ραδιοεπικοινωνίας(spread-spectrum ή OFDM ραδιόφωνο).Άλλες τεχνικές που χρησιμοποιούν είναι υπέρυθρων ακτινών(Infra-Red) και μικροκυμάτων στενής ζώνης(Narrowband Microwave).Το WLAN βασίζεται σε έναν ασύρματο μεταγωγέα ο οποίος είναι πολλές φορές ενσωματωμένος σε κάποιο δρομολογητή (router) οοποίος ρυθμίζει την ανταλλαγή δεδομένων και επιτρέπει την σύνδεση μεταξύ του ενσύρματου και ασύρματου μέρους του δικτύου.Οι δρομολογητές προκειμένου να αποκρυπτογραφήσουν τα κωδικοποιημένα (κρυπτογραφημένα) δεδομένα διαθέτουν συχνά και κάποιο ενσύρματο ADSLμόντεμ. Υπάρχουν διάφορα πρότυπα ασύρματων συνδέσεων WLAN, τα οποία διαφέρουν ως προς την ταχύτητα μεταφοράς δεδομένων,τη μέθοδο κρυπτογράφησης και την εμβέλεια.Υπάρχουν τρεις βασικές κατηγορίες προτύπων για Ασύρματα Τοπικά Δίκτυα**:** το ETSI (European Telecommunications Standards Institute) High Performance European Radio LAN (HIPERLAN), τοIEEE (Institute of Electronic and Electrical Engineers) 802.11 WLANκαι τοBluetooth.Τα δύο γνωστότερα πρότυπα WLAN είναι το IEEE 802.11g με 54 Mbps (Megabit ανά δευτερόλεπτο) και το πιο σύγχρονο IEEE 208.11n με ταχύτητα μεταφοράς που ξεπερνά τα 300 Mbps.Υπάρχουν τέσσερις περιοχές εφαρμογών για τα ασύρματα δίκτυα LANs**:**προέκταση LAN,διασύνδεση των κτηρίων,νομαδική πρόσβαση και δίκτυα ad hoc.Τα ασύρματα δίκτυα WLAN σήμερα λειτουργούν σε ανεπίσημες ζώνες συχνοτήτων,όπου οι κανονισμοί είναι χαλαροί και δεν υπάρχει χρέωση ή χρόνος αναμονής για την κατάληψη της ζώνης.Τέλος η εμβέλεια των WLAN δικτύων εξαρτάται από διάφορους παράγοντες όπως**:**

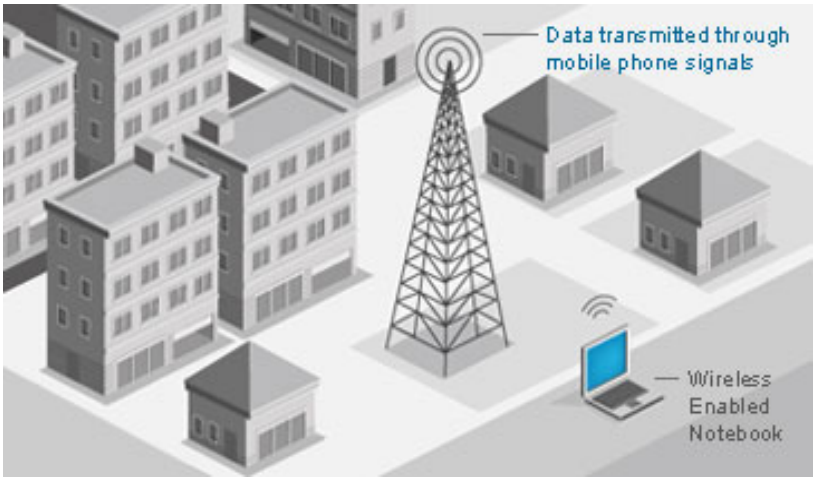
- Το περιβάλλον**:** Σε ανοιχτό χώρο η εμβέλεια μπορεί να φτάσει μέχρι και 12 μέτρα ενώ σε κλειστό χώρο για παράδειγμα στο εσωτερικό ενός κτηρίου να περιοριστεί σε λίγα μέτρα εξαιτίας παραγόντων που δημιουργού εμπόδια όπως το τοίχωμα του κτηρίου.
- Το είδος του δρομολογητή**:** Ένας απλό μοντέλο δρομολογητή διαθέτει συνήθως μια κεραία ενώ κάποιος ακριβότερο δύο ή περισσότερες κεραίες.
- Το είδος της κάρτας ασύρματού δικτύου ενός φορητού υπολογιστή ή οποιασδήποτε άλλης συσκευής Wi-Fiπου σε αυτή την περίπτωση παίζει πολύ σημαντικό ρόλο η ποιότητα της κεραίας.

- Το ασύρματο πρότυπο 802.11n παρέχει εμβέλεια μέχρι και 108Mbps με την χρήση της τεχνολογίας MIMO(Multiple Inputs Multiple Outputs).



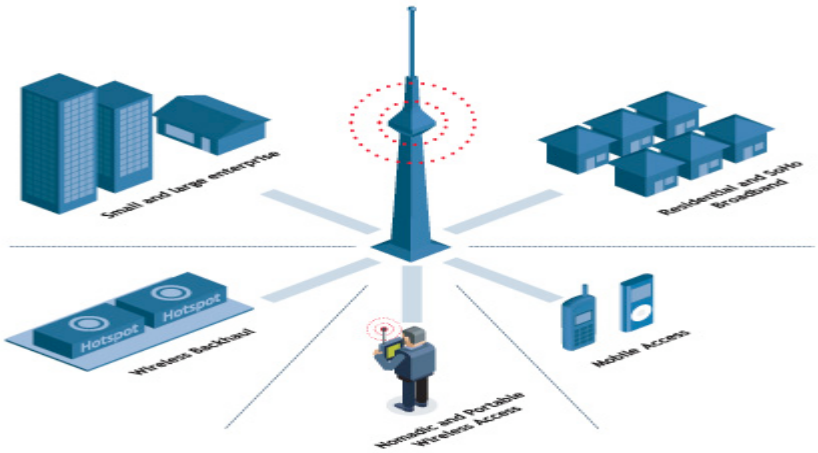
Εικόνα: WLAN(Wireless Local Area Network).

Τα WWAN ασύρματα δίκτυα ευρείας περιοχής είναι δίκτυα τα οποία καλύπτουν μια μεγάλη περιοχή όπως μια χώρα ή μια ήπειρο.Το καλύτερο παράδειγμα ενός δικτύου ευρείας περιοχής είναι το Διαδίκτυο (internet).Σε σύγκριση με το ασύρματο τοπικό δίκτυο WLAN το δίκτυο ευρείας περιοχής παρέχουν προσδεμένα απομακρυσμένη πρόσβαση στο δίκτυο μέσω της χρήσης των κινητών ή κυψελοειδή δίκτυα δεδομένων κινητής τηλεφωνίας κυψελοειδές τεχνολογίες δικτύου όπως:η LTE,WIMAX,GSM,UMTS,CDMA2000,CDPD και Mobitex για την μεταφορά δεδομένων ή με την χρήση μικροκυμάτων ή μέσω δορυφόρου.Για την πρόσβαση στο διαδίκτυο (internet) χρησιμοποιούν την Τοπική Multipoint Υπηρεσία Διανομής (LMDS) ή την τεχνολογία Wi-Fi.Οι τεχνολογίες αυτές προσφέρονται από τον φορέα παροχής ασύρματου δικτύου υπηρεσιών τόσο σε εθνικό αλλά και σε παγκόσμιο επίπεδο.Μπορούν να καλύψουν απόσταση μέχρι και 30 χιλιομέτρων.Το WWAN δίκτυο επιτρέπει σε ένα χρήστη με φορητό υπολογιστή (laptop) και μιας κάρταςUSB δικτύου που θα έχει αγοράσει να ελέγξει τα e-mailτου,να σερφάρει στο διαδίκτυο ή ακόμη να συνδεθεί σε ένα εικονικό ιδιωτικό δίκτυο(VPN).Πολλά νέα μοντέλα φορητών υπολογιστών διαθέτουν ενσωματωμένη κάρτα ασύρματού δικτύου.Η απόδοση των WWAN δικτύων είναι μέχρι 10Gbps και εξαρτάται από τον τύπο κυκλοφορίας που διαχειρίζεται το δίκτυο**:** φωνή μόνο ή φωνή, βίντεο και δεδομένα.Τα WWANδίκτυα δεδομένου ότι τα συστήματα ραδιοεπικοινωνιών δεν παρέχουν φυσικά ασφαλή διαδρομή σύνδεσης ενσωματώνουν μεθόδους κρυπτογράφησης και ελέγχου ταυτότητας για να γίνουν πιο ασφαλές.Το συγκεκριμένο υλικό χρησιμοποιείται για την παροχή αυτής της υπηρεσίας ονομάζεται ένα ασύρματο μόντεμ.Οι WWAN συσκευές που υποστηρίζουν επίσης Wi-Fi μπορεί μερικές φορές να χρησιμοποιηθούν ως Hot-spot παροχή router,όπως για τις υπηρεσίες Wi-Fi μόνο συσκευές με δυνατότητα ώστε να μπορούν να χρησιμοποιούν το Διαδίκτυο.



Εικόνα: WWAN(Wireless Wide Area Network).

Τα WMAN ασύρματα μητροπολιτικά δίκτυα. είναι τα δίκτυα που ολοκληρώνουν τα LAN και καλύπτουν τυπικά τις περιοχές μέχρι 10km είναι ανοιχτά δίκτυα προς όλους χωρίς να πουλούν internet ή άλλες υπηρεσίες.Και τα δύο, το WiMAX και οι επιχαλκωμένες συνδεμένες με καλώδιο τεχνολογίες (όπως το καλώδιο DSL και DOCSIS) χρησιμοποιούνται σε αυτό το δίκτυο.Τα WMAN δίκτυα είναι συχνά υλοποιημένα από οργανισμούς και είναι ιδιωτικά.Με βάση το πρότυπο IEEE 802.16 μπορούν να φτάσουν σε ταχύτητές μέχρι και 10 Mbps.Το πιο γνωστό ασύρματο δίκτυο μητροπολιτικής περιοχής είναι το WiMAX,το οποίο μπορεί να φτάσει ταχύτητες της τάξης των 70 Mbps σε ακτίνα αρκετών χιλιομέτρων. Τέλος τα WMAN δίκτυα αναπτύσσονται στην ζώνη των 2.4 και 5GHz.



Εικόνα: WMAN(Wireless Metropolitan Area Network).

Πέρα από τις βασικές κατηγορίες δικτύων υπάρχουν και κάποιες άλλες κατηγορίες μια τέτοια μορφή είναι το WPAN(Wireless Personal Area Network) το οποίο χρησιμοποίει τεχνολογίες όπως Bluetooth,ασύρματο USB και της υπέρυθρης σύνδεσης δεδομένων(IrDA) για να συνδέσει διάφορές συσκευές υπολογιστών όπως κινητά τηλέφωνα,laptop,πληκτρολόγιο και εκτυπωτή χωρίς καλωδίωση και ευκολία εγκατάστασης μέσω ραδιοκυμάτων μικρής εμβέλειας.Η εμβέλεια αυτού του δικτύου κυμαίνεται από μερικά εκατοστά σε απόσταση 10 μέτρων με ταχύτητες έως 1Mbps σε συχνότητα 2.4 GHz.

1.3 ΤΟ ΜΟΝΤΕΛΟ OSI

Το μοντέλο OSI μοντέλο Διασύνδεσης Ανοικτών Συστημάτων(Open System Interconnection) αναπτύχθηκε από τον διεθνή Οργανισμό Τυποποίησης ISO (International Organization for Standardization) το 1977 ως μοντέλο αρχιτεκτονικής πρωτοκόλλων υπολογιστών και ως πλαίσιο ανάπτυξης πρότυπων πρωτοκόλλων.Το μοντέλο OSI αποτελεί το πλαίσιο για την επίλυση επιμέρους προβλημάτων που εμφανίζονται στην επικοινωνία μεταξύ των υπολογιστών διαφόρων κατασκευαστών μέσα στο οποίο κινούνται οι λεπτομερείς πλέον τυποποιήσεις.Όλες οι απαιτούμενες λειτουργίες για την επικοινωνία ομαδοποιούνται σε επτά επίπεδά,είναι ανεξάρτητες μεταξύ τους,έτσι ώστε οι αλλαγές που γίνονται σε ένα επίπεδο να μην έχουν επίδραση στα άλλα επίπεδα.Σκοπός του μοντέλου OSI είναι να αναπτυχθούν πρωτόκολλα τα οποία να εκτελούν τις λειτουργίες του κάθε στρώματος.Το μοντέλο OSI σχεδιάστηκε έτσι ώστε να κυριαρχήσει στις επικοινωνίες υπολογιστών μαζί με τα πρωτόκολλα που θα αναπτύσσονταν μέσα σε αυτό, αντικαθιστώντας έτσι τις υλοποιήσεις ιδιόκτητων πρωτοκόλλων και ανταγωνιστικά μοντέλα όπως το TCP/IP χωρίς αυτό να συμβεί και να κυριαρχήσει η αρχιτεκτονικήTCP/IP.Αν και έχουν αναπτυχθεί πολλά χρήσιμα πρωτόκολλα σε περιβάλλον OSI,ολόκληρο το μοντέλο των επτά στρωμάτων δεν έχει αναπτυχθεί.Υπάρχουν αρκετοί λόγοι γι’ αυτό,ο πιο σημαντικός είναι ότι ενώ τα πιο σημαντικά πρωτόκολλα του TCP/IP ήταν πλήρως αναπτυγμένα και πολύ καλά δοκιμασμένα,όταν τα αντίστοιχα του OSI βρίσκονταν στο στάδιο της ανάπτυξης. Επίσης ένας ακόμη λόγος είναι ότι το μοντέλο OSI είναι πιο πολύπλοκο χωρίς λόγο και πραγματοποιεί με τα επτά στρώματα το ίδιο που κάνει το TCP/IP με λιγότερα στρώματα.

1.4 ΕΠΙΠΕΔΑ ΤΟΥ OSI

Το πρότυπο OSIπεριλαμβάνει τα εξής 7 επίπεδα**:**

Εικόνα: Επίπεδα του OSI.

Σε γενικές γραμμές κάθε επίπεδο χρησιμοποιεί υπηρεσίες από το επόμενο επίπεδο και προσφέρει υπηρεσίες στο προηγούμενο επίπεδο.

Τα επίπεδα του OSI περιγράφονται ως εξής:

<u>Επίπεδο 1:</u> Φυσικό επίπεδο (Physical Layer).

Το φυσικό επίπεδο αναλαμβάνει την εκπομπή των ακατέργαστων δυαδικών ψηφίων bits στο μέσο μετάδοσής (κανάλι επικοινωνίας) και το αντίστροφο δηλαδή την λήψη από ένα μέσο μεταφοράς.Ασχολείται με τα λειτουργικά,ηλεκτρικά και μηχανικά χαρακτηριστικά των διασυνδέσεων δύο υπολογιστικών συστημάτων.Στο επίπεδο αυτό καθορίζεται ακόμη ο συγχρονισμός των συσκευών,δηλαδή με ποια τάση θα παριστάνεται το 1 και με ποια το 0 (μηδέν),πόσο χρόνο διαρκεί η εκπομπή ενός δυαδικού ψηφίου ποια σηματοδοσία θα χρησιμοποιείται κλπ.Στο επίπεδο αυτό λειτουργούν οι παράλληλοί δίαυλοι SCSIκαι μαζί με το 2 επίπεδο αφορούν προδιαγραφές των πρωτοκόλλων Ethernet,Token Ring,FDDI και IEEE 802.11.

<u>Επίπεδο 2:</u> Επίπεδο ζεύξης δεδομένων (Data Link Layer).

Το επίπεδο ζεύξης δεδομένων αναλαμβάνει την παροχή αξιόπιστης γραμμής δεδομένων χωρίς σφάλματα,αφού πάρει τα δεδομένα από το φυσικό επίπεδο και μέσα από την εκτέλεση διάφορων ουσιώδη λειτουργιών,όπως έλεγχος ροής των πληροφοριών και την ανίχνευση και διόρθωση σφαλμάτων μετάδοσής τα αποδώσει στο ανώτερο επίπεδο του.Επίσης το επίπεδο αυτό εκτελεί και το αντίστροφο,δηλαδή δέχεται δεδομένα από το ανώτερο επίπεδο του (Network Layer) και τα αποδίδει στο Physical Layer.Τα δεδομένα bit που λαμβάνονται και εκπέμπονται ομαδοποιούνται σε πλαίσια.Τα πλαίσια αυτά κατανέμονται σε επίπεδα που το κάθε ένα έχει διαφορετική λειτουργία π.χ.

- Το επίπεδο διεύθυνσης (address) περιέχει τις διευθύνσεις του κόμβου αποστολής και παραλαβής αντίστοιχα.
- Το πεδίου ελέγχου (Flow Control) δηλώνει το είδος των πλαισίων δεδομένων του καναλιού σύνδεσης δηλαδή αν τα πλαίσια είναι πλαίσια δεδομένων ή διαχείρισης.
- Το πεδίο δεδομένων(Data) περιέχει τα πραγματικά δεδομένα που μεταδίδονται.
- Το πεδίο ελέγχου λαθών στο οποίο γίνεται ανίχνευση στο πλαίσιο των δεδομένων τυχόν λαθών.

Παράδειγμα πρωτοκόλλων ζεύξης δεδομένων αποτελούν το HDLC και ADCCP για την σύνδεση από-σημείο-σε-σημείο.

<u>Επίπεδο 3:</u> Επίπεδο Δικτύου (Network Layer).

Το επίπεδο δικτύου παρέχει τα στοιχεία που είναι απαραίτητα για την δημιουργία, υποστήριξη και τερματισμό συνδέσεων μεταξύ συνδρομητών ενός δικτύου.Αναλαμβάνει τις βασικές λειτουργίες οι οποίες είναι η δρομολόγηση των

μυνημάτων,η οργάνωσή τους σε πακέτα,η απαρίθμηση και η ταξινόμησή τους προσφέρει υπηρεσίες οι οποίες είναι**:**

- Μεταξύ διάφορων ακραίων σημείων του δικτύου δημιουργία και τερματισμό συνδέσεων.
- Χρήση της διεύθυνσης για προσδιορισμό των ακραίων σημείων σύνδεσης.
- Η μεταφορά των δεδομένων.
- Έλεγχος σφαλμάτων και απαρίθμηση των πακέτων.
- Έλεγχος της ροής δεδομένων.

Το πιο γνωστό παράδειγμα πρωτοκόλλου είναι το πρωτόκολλο Διαδικτύου IP.

Επίπεδο 4: Επίπεδο Μεταφοράς (Transport Layer).

Το επίπεδο μεταφοράς παρέχει αξιόπιστη παράδοση δεδομένων και βελτιώνει τις υπηρεσίες των επιπέδων δικτύου.Για την εξασφάλιση της ακεραιότητας δεδομένων βασίζεται στους μηχανισμούς ελέγχου των λαθών χαμηλότερων επιπέδων. Ουσιαστικά είναι ένα Software Interface μεταξύ των τριών χαμηλότερων και των υψηλότερων επιπέδων του προτύπου OSI που σχετίζονται με εφαρμογές που αυτοί εξυπηρετούν.Παρέχει υπηρεσίες οι οποίες είναι**:**

- Σε επίπεδο μεταφοράς αποκατάσταση και τερματισμό σύνδεσης.
- Σύμφωνα με τον απαιτούμενο βαθμό αξιοπιστίας από τον χρήστη την μετάδοση των δεδομένων με επιβεβαίωση δηλαδή ή όχι παραλαβή πακέτου.
- Καθορισμό και επιλογή από τον χρήστη της ποιότητας εξυπηρέτησης της σύνδεσης (όταν αυτό υπάρχει).
- Έλεγχος της ροής και δυνατότητα πολύπλεξης μέσω της ίδιας ζεύξης.

Το πιο γνωστό παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP.Επίσης άλλα πρωτόκολλα μεταφοράς είναι το UDP (User Datagram Protocol),το SCTP (Stream Control Transmission Protocol) κλπ.

Επίπεδο 5: Επίπεδο Συνόδου (Session Layer).

Το επίπεδο συνόδου ελέγχει τις συνόδους δηλαδή τις ανταλλαγές δεδομένων όπως είναι η σύνδεση ενός χρήστη με έναν κεντρικό σταθμό χρησιμοποιώντας το Επίπεδο Μεταφοράς.Επιτρέπει την ταυτόχρονη αμφίδρομή επικοινωνία μεταξύ δυο άκρων μιας σύνδεσης με επιλογή των δυο τύπων επικοινωνίας FDXκαι HDX.Οι υπηρεσίες που προσφέρει είναι**:**

- Μεταξύ ενός η περισσότερων σταθμών ταυτόχρονα την έναρξη και συντήρηση συνόδου.
- Έλεγχο και διαχείριση προσπέλασης της κάθε συνόδου.
- Σε περίπτωση προβλήματος επανορθωτικές διαδικασίες αποθήκευσης κατάστασης(checkpoint),αναβολής(adjournment),τερματισμού(termination) και επανεκκίνησης (restart).

Σημαντικό στοιχείο στην ανάπτυξη μιας συνόδου είναι ο αριθμός και η χρήση των portsτα οποία προσδιορίζουν το είδος της υπηρεσίας που θα δημιουργηθεί κάθε φορά.

Επίπεδο 6: Επίπεδο παρουσίασης (Presentation Layer).

Το επίπεδο παρουσίασης ασχολείται με την δομή των δεδομένων και την παράσταση της πληροφορίας από εφαρμογή σε εφαρμογή.Τα δεδομένα στο επίπεδο αυτό υφίστανται διαδικασίες κρυπτογράφησης,συμπίεσης, κωδικοποίησης καθώς και την μετατροπή και προσαρμογή τους σε χαρακτηριστικά συγκεκριμένου τερματικού ώστε να παρουσιαστούν σε τελική ανάλυση σωστά στον χρήστη.Παράδειγμα αποτελούν η μετατροπή αρχείων από κώδικα EBCDIC σε κώδικα ASCII και η μετατροπή της δομής των δεδομένων σε μορφή XML ή αντίστροφα).Το επίπεδο αυτό επίσης επιτρέπει σε μια εφαρμογή την μετάφραση της σημασίας της μεταφερόμενης πληροφορίας όταν αυτό απαιτείται.

Επίπεδο 7: Επίπεδο εφαρμογών (Application Layer).

Το επίπεδο εφαρμογών είναι το πλησιέστερο επίπεδο στον χρήστη δίνοντας την δυνατότητα μέσω μιας εφαρμογής να προσπελάσει τις πληροφορίες ενός δικτύου.Η μια εφαρμογή είναι σε θέση να συνομιλεί με την άλλη.Αποτελεί το interfaceμεταξύ της εφαρμογής και των υπόλοιπών επίπεδων αφού είναι το υψηλότερο επίπεδο.Οι λειτουργίες του επιπέδου καθορίζονται σε μεγάλο βαθμό από τον χρήστη του δικτύου.Το επίπεδο αυτό παρέχει υπηρεσίες οι οποίες είναι**:**

- Όταν οι εφαρμογές θέλουν να επικοινωνήσουν παρέχει την εξακρίβωση της ταυτότητας τους και την επιβεβαίωση της διαθεσιμότητας για συνομιλία.
- Τον έλεγχο στο δικαίωμα της συνομιλίας.
- Τον καθορισμό αρμοδιοτήτων.
- Για τον έλεγχο της ροής τν συνόδων και την αξιοπιστία της πληροφορίας τον καθορισμό των διαδικασιών.

1.5 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

Η αρχιτεκτονική ενός ασύρματου δικτύου μπορεί να προσεγγιστεί από δύο τρόπους**:** λογικά και φυσικά.Στην λογική αρχιτεκτονική ανήκουν οι λειτουργίες και τα υποσυστήματα που απαιτούνται για να πραγματοποιηθεί δικτύωση σε ένα ασύρματο σύστημα και είναι βασισμένες σε λογισμικό.Δεν πρέπει να ξεχνάμε ότι τα ασύρματα συστήματα πρέπει να συμφωνούν με τις προδιαγραφές των ενσύρματων ώστε να μπορούν να ενοποιούνται με αυτά.Έτσι στην λογική αρχιτεκτονική έχουμε**:**

- **Σύστημα διανομής (Distribution System):** Συνδέει πολλά σημεία πρόσβασης μεταξύ τους,καθώς και με το υπόλοιπο ενσύρματο δίκτυο και το internet.Είναι απαραίτητο όταν πράγματα όπως βάσεις δεδομένων ανήκουν σε συστήματα προσβάσιμα μόνο μέσω ενσύρματου δικτύου.Δεν ορίζεται μορφή για το DSκαι έτσι δίνει στον κατασκευαστή την δυνατότητα να επιλέξει τα προϊόντα που θα

το απαρτίζουν καθώς και αν απαιτούνται πολλαπλά σημεία πρόσβασης για την επέκταση εμβέλειας ενός πλήρους ασύρματου συστήματος.

- **Τεχνική πολλαπλής πρόσβασης (Multiple Access Technique):** Η τεχνική πολλαπλής πρόσβασης διευκολύνουν τη διανομή του κοινού μέσου.Υπάρχουν 3 ειδών τεχνικές Πολλαπλή Πρόσβαση με Διαίρεση στη Συχνότητα(Frequency Division Multiple Access - FDMA),Πολλαπλή Πρόσβαση με διαίρεση στο Χρόνο(Time Division Multiple Access - TDMA)και Πολλαπλή Πρόσβαση με Διαίρεση Κώδικα(Code Division Multiple Access - CDMA).Αυτό το συστατικό προσδιορίζεται στις προδιαγραφές IEEE 802.11.
- **Συγχρονισμός και έλεγχος λαθών (Synchronization and error control):** Εξασφαλίζει ότι τα δεδομένα μεταφέρονται άθικτα από κάθε ζεύξη και πρόκειται για το 2 επίπεδο(Data Link Layer) του μοντέλου OSI.Οι προδιαγραφές του IEEE 802.11 καθορίζουν το MAC που πρέπει να χρησιμοποιηθεί για τα ασύρματα δίκτυα.
- **Μηχανισμοί δρομολόγησης (Routing Mechanisms):** Οι μηχανισμοί αυτοί μετακινούν τα δεδομένα από την πηγή προέλευσης στο μελλοντικό προορισμό.Αυτοί οι μηχανισμοί λειτουργούν στο 3 επίπεδο(Network Layer) του μοντέλου αναφοράς OSI.
- **Διεπαφή εφαρμογής (Application interface):** Συνδέει μια συσκευή όπως το laptop με λογισμικό εφαρμογών που βρίσκεται σε έναν server.Ένα τέτοιο παράδειγμα αποτελεί ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου σε ασύρματο laptop.Τέλος μπορεί να περιλαμβάνεται λογισμικό επικοινωνίας και συνδεσιμότητας όπως το TCP/IP και οι driversγια ασύρματους χρήστες.

Στην φυσική αρχιτεκτονική έχουμε τα φυσικά συστατικά που απαρτίζουν ένα ασύρματο δίκτυο και είναι**:**

- **Το μέσο:** Αποτελεί τμήμα του DS ασύρματού συστήματος και φυσικό συστατικό του ενσύρματου LAN.Παραδείγματα μέσου αποτελούν τα καλώδια χαλκού,ομοαξονικά καλώδια και οι οπτικές ίνες.
- **Σημείο πρόσβασης (Access Point):** Είναι οι συσκευές(π.χ.switches) που λειτουργεί ως γέφυρα μεταξύ του ασύρματού και ενσύρματου δικτύου.Η εγκατάσταση πολλών τέτοιων συσκευών προσφέρει την δυνατότητα σε χρήστες που διαθέτουν ασύρματούς adapters να έχουν πρόσβαση στο δίκτυο καθώς κινούνται ελεύθερα σε εκτεταμένη περιοχή.
- **Κεραία:** Πρόκειται για μια συσκευή η οποία εκπέμπει και λαμβάνει σήματα με την βοήθεια του αέρα.Τα είδη της κεραίας ποικίλουν ανάλογα με τον τύπο διασποράς τους,το κέρδος και την ισχύ εκπομπή τους.Οι κεραίες διακρίνονται σε μονοκατευθυντικές χρησιμοποιούνται για σύνδεση μεταξύ κτηρίων(point-to–point) και μη κατευθυντικές που χρησιμοποιούνται για την κάλυψη μεγάλων περιοχών όπως η κεραία Vertical.
- **Κάρτα δικτύου NIC (Network Interface Card):** Πρόκειται για το υλικό το οποίο ενσωματώνεται στην κάρτα επέκτασης της μητρικής του σταθερού Η/Υ ή εισάγεται στο δίαυλο επικοινωνίας (bus) και σκοπό έχει την σύνδεση του

υπολογιστή μας με το διαδίκτυο ασύρματα μέσω switchesκαι ασύρματων routers.Επίσης μπορεί να είναι εσωτερικοί αντάπτορες δικτύου πάνω σε PCI κάρτα για επιτραπέζιους υπολογιστές.Εξωτερικοί αντάπτορεςUSB.Εσωτερικοί ασύρματοι αντάπτορες που είναι ενσωματωμένοι σε laptops.Οι κεραίες τους είναι συνήθως κρυμμένες μέσα στην οθόνη.

- **Ασύρματός σταθμός:** Πρόκειται για συσκευές οι οποίες έχουν εγκαταστημένη μια ασύρματη κάρτα δικτύου και μπορούν να επικοινωνούν μεταξύ τους.Παραδείγματα τέτοιων σταθμών είναι τα laptops,,τα ασύρματα PDAs,τα ασύρματα USB.
- **Δρομολογητής (router):** Είναι συσκευές που μπορούν να ανακατευθύνουν την πληροφορία και να ανιχνεύσουν αν μέρος του δικτύου δεν λειτουργεί ή βρίσκεται σε συμφόρηση.Επίσης επιτρέπουν την διασύνδεση δικτύων με διαφορετικά πρωτόκολλα επικοινωνίας.Διασφαλίζει ότι η πληροφορία θα φτάσει στον προορισμό της αφού βλέπει κάθε μήνυμα που αποστέλλεται και από τις δύο πλευρές του δικτύου απαγορεύοντας τη πρόσβαση από το ένα δίκτυο στο άλλο καθώς και την μεταφορά μη αναγκαίας πληροφορίας.

Εικόνα:.USB wireless adapter.

Εικόνα: Ασύρματο modem(Access Point).

1.6 ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΑΣΥΡΜΑΤΟΥΔΙΚΤΥΟΥ.

Τα ασύρματα δίκτυα προσφέρουν πληθώρα δυνατοτήτων πέρα από σταθερά δίκτυα και έτσι συνέβαλαν στην έκρηξη της χρήσης τους.Οι λόγοι αυτοί είναι οι εξής**:**

- Τα ασύρματα δίκτυα δεν περιορίζονται σε μια σταθερή και αμετάβλητη εγκατάσταση,δίνοντας στον χρήστη παροχή υπηρεσιών δικτύου και ευκολία μετακίνησης, αφού δεν υπάρχει η απαραίτητη υποδομή.
- Η χρήση του δικτύου είναι δυνατή ακόμη και σε χώρους όπου η τοποθέτηση καλωδίων είναι ανεπιθύμητη ή δύσκολο να πραγματοποιηθεί π.χ. σε κάποιο διατηρητέο κτίριο σε κάποιο περιορισμένο χώρο γραφείου κλπ.
- Επιτρέπει σε χρήστες να έχουν πρόσβαση σε real-timeπληροφορία από όπου και αν βρίσκονται σε διαφορετική χρονική στιγμή ακόμη και αν εκείνοι βρίσκονται εν κινήσει.

- Τα ασύρματα δίκτυα μπορούν να επεκταθούν πιο εύκολα ακόμη και σε σύγχρονες εγκαταστάσεις καθώς η διαδικασία της καλωδίωσης είναι ακριβή και χρονοβόρα.
- Ένα ασύρματο δίκτυο μπορεί να αλλάξει την τοποθεσία που βρίσκεται αφοί οι ασύρματα συνδεδεμένες συσκευές μπορούν να μεταφέρονται πιο εύκολα.
- Τα ασύρματα δίκτυα μπορούν εύκολα να συνδεθούν με ένα άλλο δίκτυο ακόμη και ενσύρματο.
- Το συνολικό κόστος εγκατάστασης και χρήσης ενός ασύρματου δικτύου είναι σημαντικά μικρότερο από αυτό του ενσύρματού δικτύου.Προσφέρουν έτσι μακροπρόθεσμα οφέλη σε χώρους εργασίας όπου η μετακίνηση και οι αλλαγές είναι συχνές.
- Μπορεί εύκολα να φανταστεί κανείς το χρόνο που κερδίζει κάποιος να έχει δυνατότητα πρόσβασης στο e-mailtου και σε άλλες εφαρμογές ακόμη και όταν βρίσκεται σε καφετέρια.
- Με τα ασύρματα δίκτυα είναι εξαιρετικά εύκολα να μοιράζεσαι σύνδεση στο internet ή και άλλους πόρους.

ΚΕΦΑΛΑΙΟ 2^{Ο}: Η ΤΕΧΝΟΛΟΓΙΑ Wi-Fi

2.1 ΤΙ ΕΙΝΑΙ ΤΟ Wi-Fi ΔΗΜΙΟΥΡΓΙΑ ΕΞΕΛΙΞΗ.

Με τον όρο Wi-Fi ή Wi-Fi (Wireless Fidelity) εννοούμε την επαναστατική τεχνολογία η οποία βασίζεται στο πρότυπο 802.11 του IEEE (Institute of Electrical and Electronics, Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών) και επιτρέπει σε διάφορες συσκευές όπως**:**laptop,tablet,κονσόλες παιχνιδιών,Smartphones κλπ,με την χρήση ραδιοκυμάτων να επικοινωνούν μεταξύ τους,ανταλλάσοντας δεδομένα και να έχουν πρόσβαση στο internet ασύρματα.Πολλές συσκευές μπορούν να χρησιμοποιούσουν το Wi-Fi για να συνδεθούν στο διαδίκτυο χρησιμοποιώντας ένα ασύρματο σημείο πρόσβασης (AP) εκπέμποντας σε συχνότητες των 2,4GHz και 5GHz.Ένα τέτοιο σημείο πρόσβασης (ή hotspot) έχει εμβέλεια περίπου 20 μέτρα σε εσωτερικούς χώρους και μεγαλύτερη εμβέλεια σε ανοικτούς χώρους.Η κάλυψη με Hotspot μπορεί να περιλαμβάνει ένα χώρο τόσο μικρό όσο ένα μονόκλινο δωμάτιο με τοίχους που μπλοκάρουν ραδιοκύματα,ή μεγάλης απόστασης με πολλά τετραγωνικά μέτρα που επιτυγχάνεται με τη χρήση πολλαπλών επικαλυπτόμενων σημείων πρόσβασης.Η ταχύτητα πρόσβασης στο διαδίκτυο της συμβατής συσκευής με Wi-Fi σχετίζεται με το πρωτόκολλο ασύρματης επικοινωνίας που χρησιμοποιείται από τις συμβατές συσκευές Wi-Fi. Να σημειωθεί, ότι για να επιτευχθεί ο συγκεκριμένος τρόπος ασύρματης επικοινωνίας, θα πρέπει η συμβατή συσκευή Wi-Fi (laptop,tablet,PDA,κλπ) να βρίσκεται στην προαπαιτούμενη απόσταση από το σταθμό Wi-Fi (hotspot).Η πρώτη έκδοση του Wi-Fi έγινε το 1997 με ζώνη μετάδοσης 2.4GHz η οποία περιλάμβανε δυο μεθόδους διασποράς φάσματος (Spread spectrum) την FHSS (Frequency Hopping Spread spectrum) με ρυθμό μετάδοσης 1Mbps και την

DSSS (Direct Sequence Spread spectrum) με ρυθμό μετάδοσης 1-2Mbps.Επίσης περιελάμβανε και μια υπέρυθρη ακτινοβολία (IR).Το 1999 η ταχύτητα του φτάνει τα 11Mbps χρησιμοποιώντας την DSSS τεχνική και με την έκδοση του πρότυπου 802.11b και χρησιμοποιούνται και εξαπλώνονται ευρέως ασύρματες κάρτες δικτύου.Η ταχύτητα φτάνει τα 54Mbps με τα δυο νέα πρότυπα 802.1a/g και με την μέθοδο OFDM (Orthogonal Frequency Division Multiplexing) σε ζώνη συχνότητας 5GHz.Κατά τις αρχές της δεκαετίας του 2000 εμφανίζονται συσκευές(π.χ.PDA) με ενσωματωμένη κάρτα ασύρματης δικτύωσης παρέχοντας σύνδεση στο διαδίκτυο μέχρι και σήμερα. Έτσι μια συσκευή όπως ένα laptop μπορεί να συνδεθεί οπουδήποτε υπάρχει σημείο πρόσβασης (π.χ. σε πάρκα ή πλατείες μεγάλων πόλεων, καφετέριες, βιβλιοθήκες κλπ).

Εικόνα: Σήμα κατατεθέν του Wi-Fi.

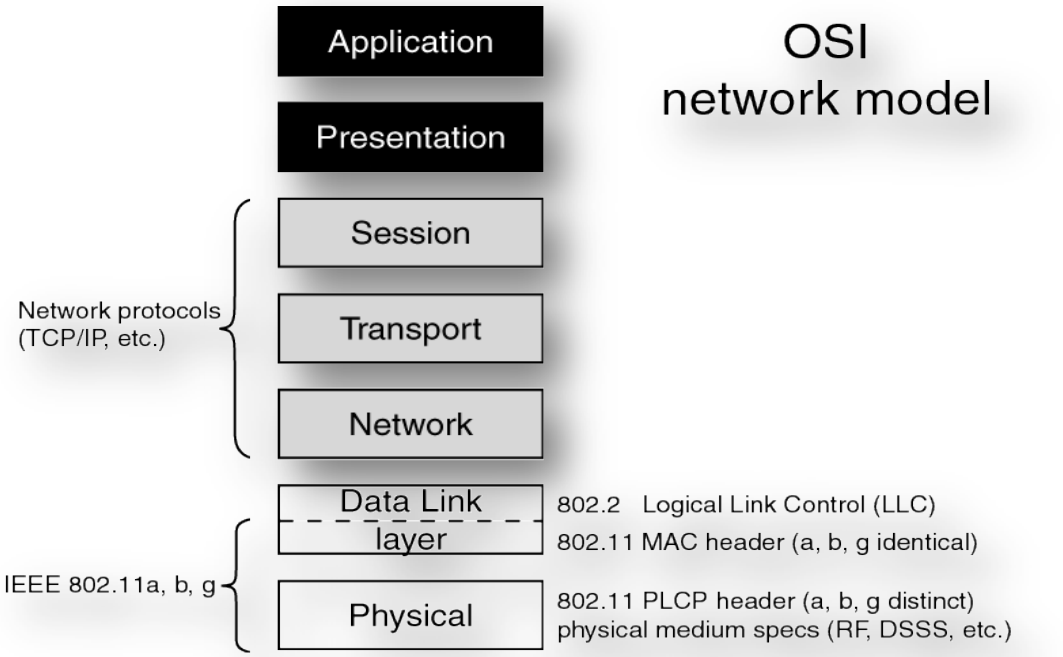
2.2 *ΠΡΟΤΥΠΟ 802.11(Wi-Fi)*

Το 802.11 γνωστό ως Wi-Fi είναι ένα πρότυπο (πρωτόκολλο) του IEEE για την υλοποίηση ασύρματου τοπικού δικτύου (WLAN) το οποίο αναπτύχθηκε το 1997 με σκοπό την επέκταση του 802.3 (Ethernet) πρωτόκολλο ενσύρματης μετάδοσης στην ασύρματη περιοχή,με ταχύτητα 2Mbps και ακολουθείται από τα περισσότερα ασύρματα δίκτυα μέχρι και σήμερα.Στην συνέχεια δημιουργήθηκαν υποπρότυπα του όπως:τοIEEE802.11a,IEEE802.11b,IEEE802.11e,IEEE802.11f,IEEE802.11g,IEEE802.11i,IEEE802.11h,IEEE802.11n.Όλα τα ασύρματα δίκτυα σήμερα βασίζονται σε αυτήν την οικογένεια προτύπων είναι πλέον διαδεδομένα,ενώ κυκλοφορεί μεγάλη γκάμα σχετικών προϊόντων στην αγορά.Το 802.11 όπως και όλα τα πρότυπα του 802 της IEEE επικεντρώνεται στα δυο χαμηλότερα στρώματα του μοντέλου διαστρωμάτωσης OSI (Open System Interconnection),δηλαδή στο φυσικό στρώμα (Physical Layer) και στο υπόστρωμα MAC (Medium Access Control) του στρώματος ζεύξης δεδομένων (Data Link Layer).Το άλλο υπόστρωμα ελέγχου λογικής ζεύξης LLC(Logical Link Control) έχει προτυποποιηθεί ως IEEE 802.2 και χρησιμοποιείται

σε συνδυασμό με όλα τα MACτης σειράς IEEE802.Σκοπός του είναι να κρύβει τις διαφορές ανάμεσα στις διάφορες παραλλαγές του 802.11 ώστε να τις κάνει ορατές όσον αφορά το επόμενο επίπεδο δικτύου (Network Layer).Το φυσικό επίπεδο του 802.11 καθορίζει 3 τεχνικές μετάδοσης των υπέρυθρων της FHSSκαι DSSS στα 2.4GHz καθώς και την OFDM με ταχύτητες 54 και 11Mbps σε 5GHz συχνότητα.Η φιλοσοφία του πρότυπου 802.11 είναι η ύπαρξη ενός μόνο MAC που όμως υποστηρίζει περισσότερα από ένα φυσικά στρώματα.

Το υπόστρωμα MAC έχει 2 τρόπους λειτουργίας**:**

- Μία κατανεμημένη (distributed) λειτουργία (CSMA/CA)
- Μια συντονισμένη (coordinated) λειτουργία (polling mode)



Εικόνα:Διαστρωμάτωση του 802.11(Έμφαση στο επίπεδο συνδέσμου δεδομένων).

2.3 ΒΑΣΙΚΕΣ ΜΟΝΑΔΕΣ ΤΩΝ ΔΙΚΤΥΩΝ WI-FI (802.11)

Τα ασύρματα δίκτυα Wi-Fi αποτελούνται από τέσσερες βασικές μονάδες οι οποίες είναι**:**

- **Σημείο πρόσβασης (Access Point –AP):** Το AP είναι η μονάδα που παίζει το ρόλο γέφυρας μεταξύ του ενσύρματού και του ασύρματου δικτύου,μετατρέποντας τα πλαίσια που ανταλλάσσονται μεταξύ αυτών κατάλληλα.
- **Σύστημα διανομής (Distribution System):** Το σύστημα διανομής ενώνει τα διάφορα AP του ίδιου δικτύου,επιτρέποντας να ανταλλάσουν τα πλαίσια.Το 802.11 δεν προσδιορίζει τον τρόπο που γίνεται αυτό.

- **Ασύρματο μέσο μετάδοσης (Wireless Medium):** Για την μετάδοση των πλαισίων μεταξύ των σταθμών του ασύρματού δικτύου έχουν οριστεί διάφορα φυσικά στρώματα που κάνουν χρήση των ραδιοσυχνοτήτων ή των υπέρυθρων ακτινών.
- **Σταθμοί (Station):** Συνήθως οι σταθμοί που ανταλλάσουν πληροφορία μέσω του ασύρματου δικτύου είναι φορητές συσκευές (π.χ. Laptops) χωρίς αυτό να είναι απαραίτητο.

2.4 ΑΡΧΙΤΕΚΤΟΝΙΚΗ-ΤΟΠΟΛΟΓΙΑ

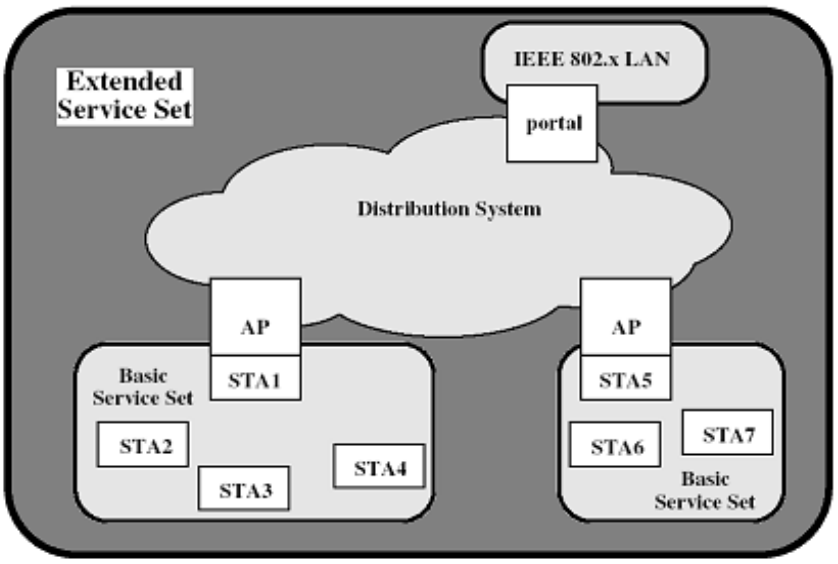
Το 1987 η ομάδα IEEE 802.4 ξεκίνησε εργασία για τα ασύρματα δίκτυα μέσα στην κοινότητα IEEE 802.11 με σκοπό την ανάπτυξη ενός ασύρματου δικτύου LAN βασισμένο στην μπάντα ISM,χρησιμοποιώντας το token bustou MAC πρωτοκόλλου που αποδείχθηκε στην συνέχεια ακατάλληλο για τον έλεγχο του ραδιομέσου,χωρίς να δημιουργείται αναποτελεσματική χρήση του φάσματος ραδιοσυχνοτήτων.Έτσι το 1990 δημιουργήθηκε μια νέα ομάδα εργασίας ,IEEE 802.11 για τα σύρματα με σύμβαση να αναπτυχθεί ένα MACπρωτόκολλο και οι προδιαγραφές για το φυσικό μέσο.Ο παρακάτω πίνακας ορίζει τους βασικούς όρους που χρησιμοποιούνται στις προδιαγραφές IEEE 802.11.

AccessPoint (AP):	Κάθε οντότητα που έχει λειτουργικότητα σταθμού και παρέχει ασύρματη πρόσβαση στο σύστημα διανομής, για επικοινωνούντες σταθμούς.
Basic Service Set (BSS):	Ένα σύνολο σταθμών που ελέγχεται από μια απλή λειτουργία συντονισμού.
Coordination Function:	Η λογική λειτουργία που καθορίζει πότε ένας σταθμός που λειτουργεί σε ένα BSS επιτρέπεται αν στείλει και είναι σε θέση να λάβει PDUs.
Distribution System (DS):	Ένα σύστημα που χρησιμοποιείται για να διασυνδέει ένα σύνολο από BSS και ολοκληρωμένα LAN για τη δημιουργία ενός ESS.
Extended Service Set (ESS):	Ένα σύνολο ενός ή περισσοτέρων διασυνδεδεμένων BSS και ολοκληρωμένων LAN που εμφανίζεται ως ένα απλό BSS στο επίπεδο LLS σε οποιοδήποτε σταθμό που επικοινωνεί με ένα από αυτά τα BSS.
MAC protocol data unit: (MPDU)	Η μονάδα της ανταλλαγής δεδομένων, ανάμεσα σε δύο ομότιμες οντότητες MAC χρησιμοποιώντας τις υπηρεσίες του φυσικού επιπέδου.
MAC Service Data Unit: (MSDU)	Η πληροφορία που παραδίδεται ως μια μονάδα ανάμεσα σε χρήστες MAC.

Station:	Κάθε συσκευή που περιέχει επίπεδα MAC και φυσικό, σύμφωνα με το 802.11.

Πίνακας: Ορολογία IEEE 802.11

Το μικρότερο δομικό στοιχείο ενός ασύρματου δικτύου είναι το BSS που περιλαμβάνει ένα αριθμό σταθμών που εκτελούν το ίδιο MAC πρωτόκολλο και συναγωνίζονται στο ίδιο μοιραζόμενο ασύρματο μέσο. Ένα BSS μπορεί να απομονωθεί ή να συνδεθεί σε ένα backbone DS μέσω ενός AP.Το σημείο πρόσβασης λειτούργει ως γέφυρα.Το πρωτόκολλο MACμπορεί να διανεμηθεί ολοκληρωτικά ή να ελεγχθεί από μια κεντρική λειτουργία συντονισμού που εδρεύει στο σημείο πρόσβασης. Το BSS γενικά αντιστοιχεί σε αυτό που καλείται κελί.Το DSμπορεί να είναι μεταγωγός,ενσύρματο ή ασύρματο δίκτυο.Ο πιο απλός σχεδιασμός φαίνεται στο σχήμα Α,όπου κάθε σταθμός ανήκει σε ένα BSSκαι κάθε σταθμός είναι μέσα στην ασύρματη εμβέλεια μόνον όσων βρίσκονται στο ίδιο BSS.Είναι επίσης πιθανό για δύο BSS να επικαλύπτεται γεωγραφικά,έτσι ώστε κάθε σταθμός να μπορεί να συμμετέχει σε πάνω από ένα BSS.Επίσης η σύνδεση του σταθμού με το BSSείναι δυναμική.Οι σταθμοί μπορεί να αποσυνδεθούν,να μπουν εντός της εμβέλειας και να βγουν έξω από αυτήν. Ένα ESS περιλαμβάνει δύο ή περισσότερα BSS διασυνδεδεμένα μέσω ενός DS.Συνήθως το DS είναι ένα κεντρικό ενσύρματο LAN αλλά μπορεί να είναι οποιοδήποτε δίκτυο επικοινωνιών.Το ESS εμφανίζεται ως ένα μόνο λογικό δίκτυο LAN στο στρώμα ελέγχου λογικής σύνδεσης (LLC).Το σχήμα Α δείχνει ότι ένα σημείο πρόσβασης AP υλοποιείται ως μέρος ενός σταθμού.Δηλαδή το AP έχει τη λογική ενός σταθμού (Station) παρέχοντας επιπλέον πρόσβαση στο DS.Για να υλοποιηθεί η αρχιτεκτονική IEEE 802.11 σε συνδυασμό με ένα παραδοσιακό ενσύρματο δίκτυο LAN,χρειάζεται μια πύλη η οποία είναι μια συσκευή όπως μια γέφυρα ή ένας δρομολογητής που είναι μέρος του ενσύρματού δικτύου και συνδέεται με το DS.



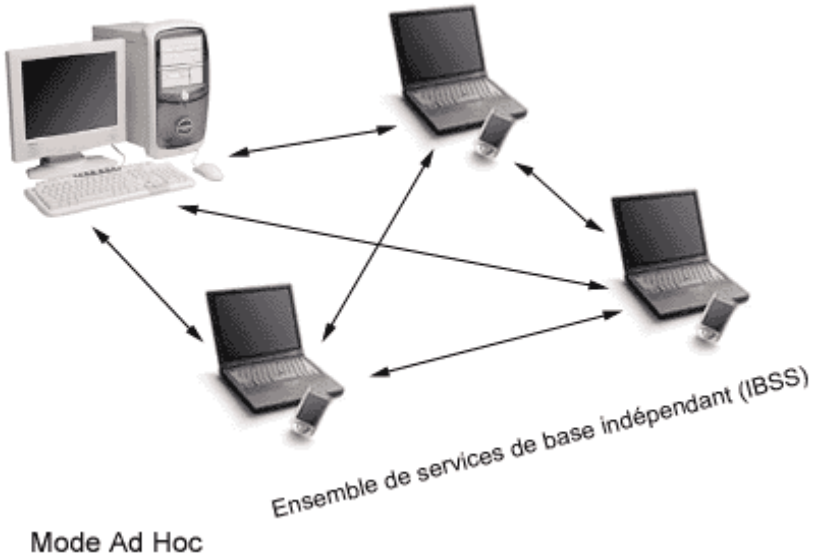
Εικόνα: IEEE 802.11 Αρχιτεκτονική.

Όσον αφορά την τοπολογία η αρχιτεκτονική του συστήματος διακρίνει δυο τοπολογίες**:** την δομημένη (infrastructure) και την ανεξάρτητη-αδόμητη (ad-hoc).Στην δομημένη τοπολογία οι κινητοί σταθμοί επικοινωνούν μέσω ενός σημείου πρόσβασης (Access Point,AP)με το δίκτυο κορμού. Το AP αποτελεί γέφυρα που συνδέει το ασύρματο δίκτυο (802.11) με την υποδομή του ενσύρματου δικτύου κορμού.Ηπεριοχή η οποία καλύπτεται από ένα AP ονομάζεται βασική περιοχή εξυπηρέτησης (Basic Service Area,BSA) και είναι ανάλογη της κυψέλης των κυψελωδών συστημάτων.Για να συμμετέχει ένας σταθμός στο BSSπρέπει να ακολουθήσει την διαδικασία του association(θα δούμε πιο κάτω)με το AP.Η διαδικασία αυτή ξεκινάει πάντα με πρωτοβουλία του σταθμού και είναι απόφαση του AP αν ο σταθμός θα γίνει δεκτός στοBasic Service Set(BSS).Το 802.11 δεν ορίζει μέγιστο αριθμό σταθμών που μπορούν να συμμετάσχουν σε ένα BSS,αλλά τίθενται περιορισμοί στις διάφορες υλοποιήσεις του AP.Πολλές BSSσυνδεόμενες με κοινό δίκτυο κορμού σχηματίζουν μια ενιαία υποδομή Extended Service Set (ESS).Ένα κινητό τερματικό μπορεί να περιφέρεται σε διαφορετικές BSS μιας ESS χωρίς να χάνει την σύνδεση του με το δίκτυο κορμού.Τυπική εφαρμογή αυτής της τοπολογίας μια ομάδα από φορητούς υπολογιστές (laptops) συνδέονται μέσω ενός WLANσε ενσύρματο LAN κορμού.

Εικόνα: Δομημένη τοπολογία (infrastructure networks).

Στην ανεξάρτητη ad-hoc τοπολογία οι κινητοί σταθμοί επικοινωνούν μεταξύ τους σε ανεξάρτητη BSS χωρίς σύνδεση στο ενσύρματο δίκτυο κορμού.Για το σχηματισμό και την διατήρηση μιας BSS,χρειάζονται μερικές από τις λειτουργίες του AP οι οποίες στην περίπτωση αυτή παρέχονται από ένα κινητό τερματικό.Εκτός από την μέθοδο πολλαπλής πρόσβασης CSMA/CA,που είναι κατάλληλη για ασύγχρονες μεταδόσεις,το IEEE 802.11 παρέχει και έναν μηχανισμό με προτεραιότητες,χωρίς ανταγωνισμό,ελεγχόμενο από ένα σημείο για την υποστήριξη ισόχωρων εφαρμογών με χρονικούς περιορισμούς.Το πρωτόκολλο MAC για την αντιμετώπιση του προβλήματος των κρυμμένων τερματικών,διαθέτει μηχανισμό με μηνύματα request-to-sent/clear-to-sent (RTS/CTS).Ο μηχανισμός αυτός παρέχει μικρή εξασφάλιση για

την ποιότητα υπηρεσίας.Οι υπηρεσίες του στρώματος MACστο IEEE 802.11 υποστηρίζουν μηχανισμούς για τον έλεγχο αυθεντικότητας, απόκρυψη, διαχείριση συχνοτήτων και εξοικονόμηση ενέργειας.Η τοπολογία αυτή ονομάζεται και IBSS (Independent BSS) και αποτελείται το λιγότερο από δυο σταθμούς και συνήθως είναι προσωρινό,δηλαδή δημιουργείται για κάποιον σκοπό και μετά διαλύεται.Είναι ο απλούστερος τύπος ασύρματου δικτύου.



Εικόνα: Ανεξάρτητη τοπολογία Ad-hoc.

2.5 ΥΠΗΡΕΣΙΕΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ Wi-Fi (802.11)

Το ασύρματο δίκτυο IEEE 802.11 παρέχει εννέα υπηρεσίες,όπου ο παροχέας υπηρεσίας μπορεί να είναι ή ο σταθμός ή το σύστημα διανομής.Οι υπηρεσίες σταθμού υλοποιούνται σε κάθε σταθμό 802.11 και στους σταθμούς σημείων πρόσβασης φυσικά.Οι υπηρεσίες DSπαρέχονται μεταξύ των BSS,όπου μπορούν να υλοποιούνται σε ένα σημείο πρόσβασης ή σε κάποια άλλη συσκευή η οποία είναι συνδεδεμένη στο σύστημα διανομής.Από τις εννέα υπηρεσίες να επισημάνουμε ότι τρεις από αυτές σχετίζονται με την πρόσβαση, τη μεταφορά δεδομένων και της εμπιστευτικότητας του IEEE 802.11 και υπόλοιπες έξι σχετίζονται με την διαχείριση. Οι υπηρεσίες αυτές είναι οι εξής**:**

- **Distribution (Διανομή):** Είναι η κύρια υπηρεσία που είναι απαραίτητη για την ανταλλαγή πλαισίων MAC η οποία χρησιμοποιείται από τους σταθμούς. Η παράδοση ενός πλαισίου από το AP στον τελικό προορισμό του συνιστά τον εντοπισμό του παραλήπτη ώστε να είναι επιτυχής.Έτσι λαμβάνεται απόφαση αν ένα πλαίσιο πρέπει να σταλεί από τον έναν σταθμό μιας BSS σε έναν άλλο της ίδιας BSSή να σταλεί στο DS προς παράδοση σε σταθμό συσχετιζόμενο με άλλο AP.
- **Integration (Ενοποίηση):** Η υπηρεσία αυτή παρέχεται από το σύστημα διανομής DS.Δίνει την δυνατότητα μεταφοράς δεδομένων μεταξύ ενός

δικτύου διαφορετικού του 802.11,που είναι διασυνδεδεμένο με το DS.Ηυπηρεσία ενοποίησης αναλαμβάνει την λογική της όποιας μετάφρασης διεύθυνσης και όποιας μετατροπής των πλαισίων από τον ένα τύπο στον άλλο για την ανταλλαγή δεδομένων.

- **MSDU Delivery:** Η MSDUείναι το μπλοκ δεδομένων που μεταβιβάζεται προς τα κάτω από το χρήστη MACστο στρώμα MAC και είναι συνήθως μια PDULLC.Αν η MSDU είναι πολύ μεγάλη για να μεταδοθεί σε ένα μόνο πλαίσιο MAC μπορεί να διασπαστεί και να μεταδοθεί σε περισσότερα MAC πλαίσια.
- **Association (Συσχέτιση):** Για να μπορέσει ένας σταθμός να εκπέμψει ή να λάβει πλαίσια σε ένα ασύρματο δίκτυο πρέπει να είναι γνωστά η διεύθυνση και η ταυτότητα του.Για το λόγο είναι απαραίτητη η διαδικασία συσχετισμού ενός σταθμού με το σημείο πρόσβασης AP μιας συγκεκριμένης BSS.Μόλις γίνει αυτό,το σημείο πρόσβασης μπορεί να μεταδώσει αυτές τις πληροφορίες και στα άλλα σημεία πρόσβασης που βρίσκονται μέσα στην ίδια ESS για την διευκόλυνση της δρομολόγησης και της αναζήτησης πλαισίων.
- **Reassociation (Επανασυχέτιση):** Η λειτουργία αυτή δίνει την δυνατότητα σε μια συσχέτιση που είναι ήδη αποκατεστημένη να μεταφερθεί από ένα σημείο πρόσβασης σε ένα άλλο, επιτρέποντας σε ένα κινητό σταθμό να μετακινηθεί από μία BSS σε μια άλλη.
- **Disassociation (Αποσυσχέτιση):** Είναι μια ειδοποίηση ότι μια υπάρχουσα συσχέτιση τερματίζεται.Η ειδοποίηση αυτή προέρχεται είτε από ένα σταθμό (πριν βγει από μια ESSή απενεργοποιηθεί)είτε από ένα σημείο πρόσβασης.Η λειτουργία διαχείρισης MACπροστατεύει τον εαυτό της από σταθμούς που εξαφανίζονται χωρίς ειδοποίηση.
- **Authentication (Πιστοποίηση):** Η υπηρεσία αυτή χρησιμοποιείται από τους σταθμούς που θέλουν να επικοινωνήσουν με άλλους σταθμούς για την επαλήθευση της ταυτότητας τους.Το IEE 802.11 υποστηρίζει κάποιες μεθόδους πιστοποίησης όπως κρυπτογράφηση με χρήση δημοσίων κλειδιών κι επιτρέπει την επέκταση της λειτουργικότητας αυτών των μεθόδων.Ωστόσο απαιτεί αμοιβαία αποδεχτή,επιτυχημένη πιστοποίηση πριν προχωρήσει στην διαδικασία της συσχέτισης (Association).
- **Deauthentication (Αποπιστοπίηση):** Η υπηρεσία αυτή χρησιμοποιείται για μια υπάρχουσα πιστοποίηση (Authentication) που πρόκειται να τερματιστεί.Τερματίζει επίσης και το Association εφόσον το Authentication είναι προαπαιτούμενο αυτού.
- **Privacy (Ιδιωτικότητα):** Η λειτουργία αυτή χρησιμοποιείται για να αποτρέψει την ανάγνωση των περιεχομένων των μηνυμάτων από σταθμούς άλλους από τον προοριζόμενο αποδέκτη.Λόγω του ασύρματού περιβάλλοντος μετάδοσης το 802.11 επιτρέπει την προαιρετική χρήση κρυπτογράφησης για την εξασφάλιση προστασίας χρησιμοποιώντας τον αλγόριθμό WEP.

2.6 ΥΠΟΣΤΡΟΜΑ MAC ΤΟΥ 802.11

Το υπόστρωμα MAC του 802.11(Wi-Fi) αποτελεί ίσως το πιο σημαντικό κομμάτι προτυποποίησης.Υποστηρίζει όλα τα φυσικά στρώματα και προσφέρει υπηρεσίες αξιόπιστης παράδοσης δεδομένων,πρόσβασης στο μέσο,ασφάλεια και πιστοποίηση στα ανώτερα στρώματα.οι υπηρεσίες αυτές περιγράφονται παρακάτω**:**

- **Πρόσβαση στο μέσο:** Χρησιμοποιεί δυο μεθόδους πρόσβασης την DCF(Distributed Coordination Function) και την PCF(Point Coordination Function) χρησιμοποιώντας ως μηχανισμό πρόσβασης την τεχνική πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance).Η επιλογή αυτή έχει ως αποτέλεσμα την μείωση της πιθανότητας να συμβεί σύγκρουση όταν δυο ή περισσότεροι σταθμοί μεταδίδουν δεδομένα την ίδια χρονική στιγμή,ως αποτέλεσμα τη μη παράδοση των πακέτων πληροφορίας.Έτσι κάθε σταθμός που θέλει να κάνει εκπομπή, πρέπει πρώτα να βεβαιωθεί ότι το μέσο μετάδοσης είναι ελεύθερο.Αν το μέσο δεν είναι ελεύθερο,τότε η εκπομπή αναβάλλεται μέχρι να τελειώσει η προηγούμενη εκπομπή.Μετά τον χρόνο αναμονής όμως και πριν προσπαθήσει να ξανακάνει εκπομπή ο σταθμός,πρέπει να περιμένει ένα τυχαίο χρονικό διάστημα. επίσης το ίδιο συμβαίνει και πριν ένας σταθμός κάνει εκπομπή ξανά, μετά από μια επιτυχημένη προηγούμενη εκπομπή.Μια παραλλαγή του μηχανισμού επίσης ορίζει επιπλέον την ανταλλαγή μηνυμάτων RTS/CTS (Request toSend/Clear to Send) μεταξύ αποστολέα και παραλήπτη ανταλλαγή γίνεται μετά τον έλεγχο διαθεσιμότητας του μέσου και ακριβώς πριν την αποστολή των δεδομένων.Η μέθοδος DCF είναι η βασική μέθοδος που χρησιμοποιείται στα ασύρματα δίκτυα 802.11,ενώ η μέθοδος PCF είναι προαιρετική βασίζεται σε σύστημα pollingκαι απαιτεί την ύπαρξη ενός Point Coordinator (PC) σταθμού, δηλαδή ενός σταθμού που αναλαμβάνει την κεντρική διαχείριση των εκπομπών των υπολοίπων σταθμών.Τα Access Point έχουν το ρόλο του Point Coordinator γι' αυτό και αυτή η μέθοδος χρησιμοποιείται μόνο στα Infrastructure δίκτυα.Η μέθοδος PCF λειτουργεί ένα επίπεδο πιο πάνω από την μέθοδο DCF, γιατί η μέθοδος πρόσβασης εναλλάσσεται: για κάποιο χρονικό διάστημα χρησιμοποιείται η PCF και για το υπόλοιπο χρησιμοποιείται η DCF.Ο Point Coordinator κατά το διάστημα χρήσης της PCF ρωτάει κυκλικά όλους τους σταθμούς, αν έχουν δεδομένα προς αποστολή. Οι σταθμοί μπορούν να εκπέμψουν μόνο αν τους το επιτρέψει ο Point Coordinator.
- **Αξιόπιστη παράδοση δεδομένων:** Η αξιόπιστη παράδοση δεδομένων μεταξύ διάφορων σταθμών μπορεί να δυσχερανθεί από το ασύρματο φυσικό μέσο,τον θόρυβο,τις παραβολές,κάποιος κόμβος να έχει βγει προσωρινά εκτός περιοχής κάλυψης δικτύου,το πρόβλημα ύπαρξης κρυμμένου κόμβου και άλλα φαινόμενα διάδοσης οδηγώντας έτσι στην απώλεια σημαντικού αριθμού πλαισίου.Ένας αριθμός πλαισίων MAC ακόμη και με κώδικες διόρθωσης σφάλματος υπάρχει πιθανότητα να μην ληφθεί επιτυχώς.Για να

αντιμετωπιστούν τα παραπάνω το 802.11 MAC χρησιμοποιεί τους κατάλληλους μηχανισμούς όπως την βεβαίωση λήψης κάθε πλαισίου (ACK)στο σταθμό πηγής,τον RTS(request to send) και τον CTS(clear to send) για την ανταλλαγή πλαισίων.ORTS ειδοποιεί ότι μια ανταλλαγή βρίσκεται σε εξέλιξη και έτσι όλοι οι σταθμοί που βρίσκονται μέσα στην εμβέλεια λήψης της πηγής δεν επιχειρούν καμία εκπομπή αποφεύγοντας έτσι την σύγκρουση μεταξύ δυο πλαισίων που εκπέμπονται την ίδια στιγμή.Το CTS αντίστοιχα ειδοποιεί ότι μια ανταλλαγή βρίσκεται σε εξέλιξη όλους τους σταθμούς που βρίσκονται μέσα στην εμβέλεια λήψης του προορισμού.Το τμήμα RTS/CTS της ανταλλαγής είναι μια απαιτούμενη λειτουργία του MAC η οποία μπορεί να απενεργοποιηθεί.

- **Ασφάλεια:** Το 802.11 παρέχει μηχανισμούς τόσο ασφάλειας όσο και πιστοποίησης.Σαν παράδειγμα ασφάλειας αναφέρεται ο αλγόριθμος WEP (Wired Equivalent Privacy) ο οποίος παρέχει προστασία ισοδύναμη με αυτή των ενσύρματων LAN.Το WEP χρησιμοποιεί ένα αλγόριθμό κρυπτογράφησης RCA για την παροχή ακυρότητας και προστασίας των δεδομένων.Για την κρυπτογράφηση ένα κρυφό κλειδί 40 bit διαμοιράζεται από τα δύο συμμετέχοντα μέρη της ανταλλαγής.Με το κρυφό κλειδί συνενώνεται ένα διάνυσμα εκκίνησης IV (Initialization Vector).Το μπλοκ που προκύπτει αποτελεί τον πυρήνα που είναι είσοδος στη γεννήτρια ψευδοτυχαίων αριθμών (pseudorandom number generator) PRNG που ορίζεται στον αλγόριθμο RC4.Το κρυπτογράφημα δημιουργείται από την ακολουθία bit ίδιου μήκους με το μήκος πλαισίου MAC συν τον CRC 32 bit αλγόριθμο ακεραιότητας που προστίθεται στο τέλος του πλαισίου.Το IV προστίθενται στο κρυπτογράφημα και το μπλοκ που προκύπτει εκπέμπεται.Το IV αλλάζει περιοδικά (τόσο συχνά όσο κάθε εκπομπή) και κάθε φορά που αλλάζει το IV,αλλάζει και η PRNG ακολουθία,γεγονός που κάνει πολύπλοκο το έργο της υποκλοπής.Το 802.11 παρέχει δυο τύπους πιστοποίησης**:** ανοιχτού συστήματός (open system) και κοινόχρηστού κλειδιού (shared key).Η πιστοποίηση ανοιχτού συστήματος δεν παρέχει κανενός είδους ασφάλεια και παρέχει ένα τρόπο συμφωνίας ανάμεσα σε δυο πλευρές για να συμφωνήσουν και να ανταλλάξουν δεδομένα.Η μια πλευρά στέλνει στην άλλη ένα πλαίσιο ελέγχου MAC που λέγεται πλαίσιο πιστοποίησης,η άλλη πλευρά απαντά με το δικό της πλαίσιο πιστοποίησης και η διαδικασία ολοκληρώνεται.Η πιστοποίηση αυτή συνιστάται απλά στην ανταλλαγή των ταυτοτήτων μεταξύ των δυο πλευρών.Η πιστοποίηση κοινόχρηστού κλειδιού απαιτεί οι δυο πλευρές που επικοινωνούν να μοιράζονται ένα κρυφό κλειδί που δεν μοιράζεται από κανέναν άλλο.Το κλειδί αυτό χρησιμοποιείται για να εξασφαλίσει ότι και οι δυο πλευρές είναι πιστοποιημένες η μια από την άλλη.Η πιστοποίηση αυτή μεταξύ δυο πλευρών Α και Β έχει ως εξής**:**

1. Η Α στέλνει με την ένδειξη ‘’Shared Key’’ ένα πλαίσιο πιστοποίησης MAC για τον αλγόριθμο πιστοποίησης και με ένα αναγνωριστικό σταθμού που προσδιορίζει το σταθμό αποστολής.

2. Η Β απαντά με ένα πλαίσιο πιστοποίησης το οποίο περιλαμβάνει ένα συνθηματικό κείμενο (challenge text) μήκους 128 οκτάδων το οποίο προκύπτει από την γεννήτρια ψευδοτυχαίων αριθμώνPRNG του WEP το κλειδί και το IV.
3. Η Α εκπέμπει ένα πλαίσιο πιστοποίησης που περιλαμβάνει το challenge text το οποίο έχει λάβει από την Β,το οποίο κρυπτογραφείται ολόκληρο χρησιμοποιώντας το πρωτόκολλο WEP.
4. Το κρυπτογραφημένο πλαίσιο που λαμβάνει η Β το αποκρυπτογραφεί χρησιμοποιώντας τον WEP και το κρυφό κλειδί που μοιράζεται με την Α.Αν η κρυπτογράφηση είναι επιτυχημένη δηλαδή ταιριάζουν οι CRC τότε η Β συγκρίνει το εισερχόμενο challenge textμε το challenge text που έστειλε στη Α.Τότε η Β στέλνει στην Α ένα πλαίσιο πιστοποίησης με ένα κωδικό κατάστασης που υποδηλώνει επιτυχία ή αποτυχία.

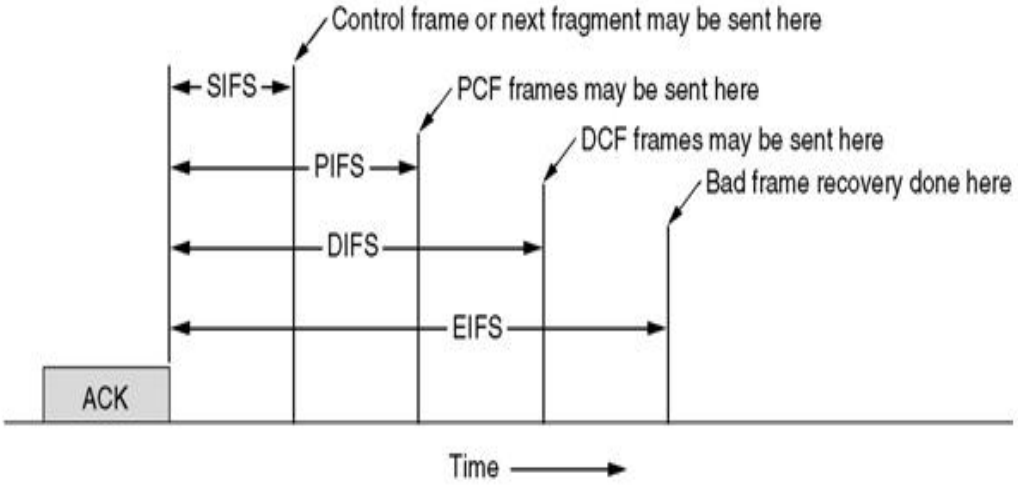
2.7 ΧΡΟΝΟΙ ΑΝΑΜΟΝΗΣ (Interframe Spacing)

Όπως είχε αναφερθεί για την πρόσβαση στο μέσο χρησιμοποιούνται δυο τεχνικές πρόσβασης η DCF(Distributed Coordination Function) και η PCF(Point Coordination Function).Για να είναι δυνατή η λειτουργία πρόσβασης με διάφορούς τρόπους, προδιαγράφονται τέσσερις τύποι περιόδων σιγής μεταξύ των μεταδιδόμενων πλαισίων IFS (inter-frames pacing).Γενικά,κάθε σταθμός ο οποίος θέλει να μεταδώσει κάποιο πλαίσιο πρέπει πρώτα να περιμένει ένα ορισμένο χρονικό διάστημα ίσο με ένα από τα τέσσαρα διαθέσιμα είδη IFS,ανάλογα με το βαθμό προτεραιότητας του πλαισίου προς αποστολή και αν δεν ανιχνεύσει άλλη μετάδοση προχωρεί στην απόκτηση πρόσβασης στο μέσο ,που διαφέρει ανάλογα με την τεχνική που χρησιμοποιείται (DCF ή PCF).Τα χρονικά διαστήματα αυτά ποικίλουν ανάλογα με το τύπο πλαισίου που πρόκειται να μεταδοθεί και είναι τα ακόλουθα**:**

- **Short Interframe Space (SIFS):** Πρόκειται για το μικρότερο χρόνο αναμονής και χρησιμοποιείται για μεταδόσεις μέγιστης προτεραιότητας όπως είναι τα πλαίσια RTS/CTSκαι ACK.
- **PCF Interframe Space (PIFS):** Χρησιμοποιείται με τον αλγόριθμό PCF έχει μεγαλύτερη χρονική διάρκεια από τον SIFS.Επιτρέπει σε έναν σταθμό να στείλει ένα πλαίσιο δεδομένων χωρίς να υπάρχει άλλος που να τον εμποδίζει και δίνει την ευκαιρία στο σταθμό βάσης να καταλάβει τον δίαυλο όταν τελειώσει η προηγούμενη αποστολή,χωρίς να περιμένει τους σταθμούς που είναι έτοιμοι να στείλουν
- **DCF Interframe Space (DIFS):** Πρόκειται για το μεγαλύτερο σε διάρκεια χρόνο από τους δυο προηγούμενους, διότι προορίζεται για δεδομένα με χαμηλότερη προτεραιότητα.Αν κάποιος σταθμός βάσης δεν έχει τίποτε άλλο να στείλει, οποιοσδήποτε άλλος σταθμός μπορεί να προσπαθήσει να καταλάβει το δίαυλο και να στείλει ένα νέο πλαίσιο.Ισχύουν οι συνήθεις κανόνες ανταγωνισμού.

- **Extended Interframe Space (EIFS):** Ο τελευταίος χρόνος και μεγάλος σε διάρκεια δεν έχει κάποια συγκεκριμένη τιμή και χρησιμοποιείται για να αναφερθεί σε κάποιο σφάλμα ή άγνωστο πλαίσιο που μόλις έχει λάβει ένας σταθμός.Σε αυτό το γεγονός η ιδέα του να δίνεται χαμηλότερη προτεραιότητα είναι ότι ο δέκτης μπορεί να μην γνωρίζει τι συμβαίνει και να πρέπει να περιμένει αρκετό διάστημα ώστε να μην παρεμβληθεί σε κάποιον εξελισσόμενο διάλογο μεταξύ δυο άλλων σταθμών.

Από τα παραπάνω γίνεται προφανές ότι κάθε σταθμός πρέπει να έχει την δυνατότητα να ανιχνεύσει αν υπάρχει σε εξέλιξη κάποια άλλη μετάδοση πριν αρχίσει να μεταδίδει αυτός.Για το σκοπό αυτό χρησιμοποιείται ο μηχανισμός ανίχνευσης φέροντος ο οποίος παρουσιάζεται πιο κάτω.

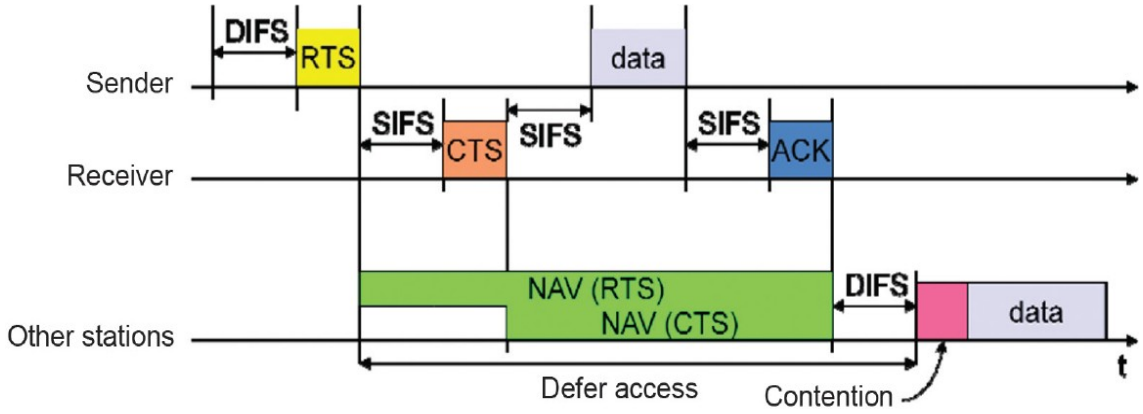


Εικόνα: Interframe Spacing.

2.8 ΜΗΧΑΝΙΣΜΟΣ ΑΝΙΧΝΕΥΣΗΣ ΦΕΡΟΝΤΟΣ

Ο συγκεκριμένος μηχανισμός σχετίζεται με τους σταθμούς που παρακολουθούν το μέσο μετάδοσης και αν εντοπίσουν σήμα συγκεκριμένης ισχύος καταλαβαίνουν ότι κάποια μετάδοση πλαισίου βρίσκεται σε εξέλιξη.Λόγων των αποστάσεων μεταξύ των σταθμών και στο μεγάλο αριθμό των σχημάτων διαμόρφωσης που χρησιμοποιούνται αλλά και το πρόβλημα των κρυμμένων κόμβων (hidden nodes) είναι δύσκολο να δημιουργηθεί αξιόπιστός μηχανισμός ανίχνευσης φέροντός ο οποίος θα λειτουργεί αποκλειστικά στο φυσικό επίπεδο.Ο μηχανισμός ανίχνευσης φέροντος επιτυγχάνεται με δυο τρόπους,τόσο με φυσικό όσο και με εικονικό.Ο φυσικός τρόπος βασίζεται στην συχνότητα που λειτουργεί στο σύστημα μας και στην ανίχνευση μέσω της κεραίας στο φυσικό επίπεδο φέροντος.Ο εικονικός μηχανισμός παρέχεται από το MAC και χρησιμοποιεί έναν μετρητή χρόνου που ονομάζεται NAV(Network Allocation Vector)ο οποίος βασιζόμενος στις πληροφορίες για την διάρκεια των πακέτων πλαισίων από τους μηχανισμούς RTS/CTS/ACKκαθένα από τα οποία

περιλαμβάνουν την διάρκεια μιας επερχόμενης μετάδοσης πετυχαίνει μια πρόβλεψη της μμελλοντικής κίνησης στο μέσο.Ο μετρητής NAV περιλαμβάνεται στα περισσότερα πλαίσια που ανταλλάσσονται.Ο κάθε σταθμός όταν αποκτήσει το δικαίωμα θέτει το πεδίο αυτό ίσο με το χρόνο που θέλει να κρατήσει δεσμευμένο το μέσο μετάδοσης.Το NAV μπορεί να θεωρηθεί ως ένας μετρητής που μετράει το χρόνο αντίστροφα μέχρι το κανάλι να ελευθερωθεί, βασισμένος στη γνώση που έχει για την κίνηση στο κανάλι.Όταν είναι μη μηδενικός το κανάλι θεωρείται κατειλημμένο ενώ όταν μηδενιστεί το κανάλι θεωρείται ελεύθερο.Οι σταθμοί μπορούν με την χρήση του NAV να εκτελέσουν συγκεκριμένες ενέργειες χωρίς να χάσουν τον έλεγχο του μέσου μετάδοσης.Πρέπει όμως για να ολοκληρωθεί αυτή η ενέργεια να ανταλλάξουν οι δυο σταθμοί που επικοινωνούν μεταξύ τους 4 πλαίσια συνολικά,χωρίς να διακοπούν από άλλη μετάδοση.

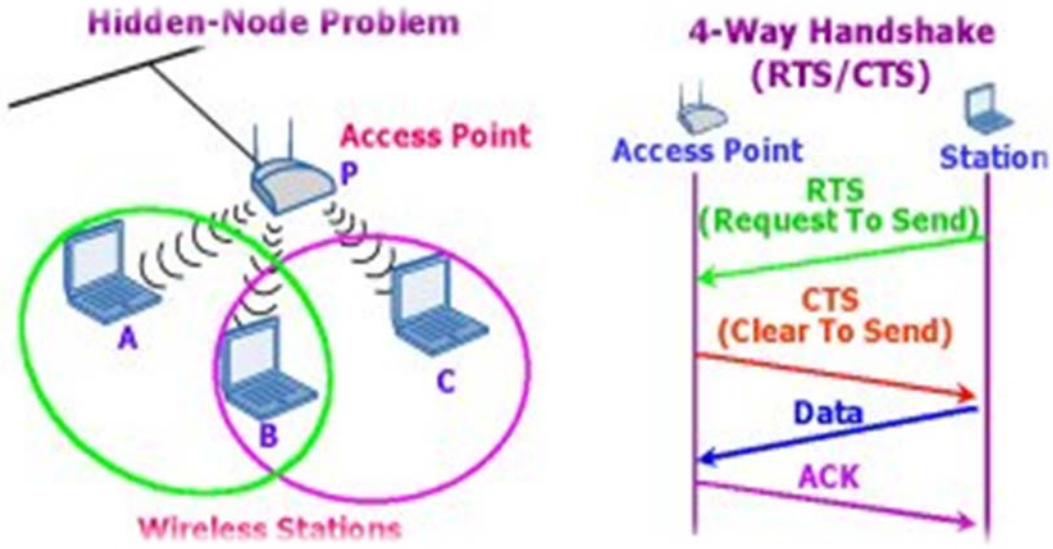


Εικόνα: Παράδειγμα ενεργοποίησης NAVσημάτων.

2.9 ΜΗΧΑΝΙΣΜΟΣ RTS/CTS

Το πρότυπο 802.11 για να διασφαλίσει ότι μια συγκεκριμένη ανταλλαγή πλαισίων θα γίνει χωρίς διακοπή από μετάδοση τρίτου σταθμού, υποστηρίζει το μηχανισμό RTS/CTS.Η διαδικασία αποστολής πλαισίου διαφοροποιείται καθώς εισάγονται δυο επιπλέον πλαίσια,τα RTS (request to send) και CTS (clear to send).Ο μηχανισμός RTS/CTS προστατεύοντας την ανταλλαγή πλαισίων βελτιώνει την απόδοση της χρήσης του ασύρματου δικτύου σε περιπτώσεις μεγάλου φόρτου εξαιτίας της ύπαρξης πολλών τερματικών και αντιμετωπίζει το πρόβλημα του κρυμμένου κόμβου (hidden node).Η χρησιμοποίηση του μηχανισμού αυτού χωρίς λόγο επιφέρει αντίθετο αποτέλεσμα στο ασύρματο δίκτυο καθώς προσθέτει επιπλέον φορτίο. Το πρόβλημα των κρυμμένου κόμβου δημιουργείται όταν ένας σταθμός δεν μπορεί να ¨δει¨ τον άλλον που εκπέμπει ενώ βλέπουν και οι δύο το σημείο πρόσβασης. Το πρόβλημα αυτό συμβαίνει λόγω της απόστασης, λόγω εμποδίου, ή λόγω της χρήσης κατευθυντικών κεραιών από τους σταθμούς .Στην παρακάτω εικόνα ο σταθμός Α δεν μπορεί να ανιχνεύσει την εκπομπή του C με αποτέλεσμα να αρχίζουν να εκπέμπουν και οι δυο μαζί έτσι ώστε να υπάρξει σύγκρουση και ο Β να μην μπορεί να ¨δει¨ κανέναν. Έτσι στην περίπτωση αυτή ο σταθμός μη ανιχνεύοντας την εκπομπή του

άλλου θα δοκιμάζει να εκπέμψει με αποτέλεσμα να συμβεί σύγκρουση στα πακέτα όπως αυτά λαμβάνονται από το AP. Πιο αναλυτικά όταν ένας σταθμός θέλει να μεταδώσει ένα πλαίσιο (framework) περιμένει μέχρι το κανάλι ανιχνευθεί αδρανή-ελεύθερο για ένα DIFS.Ο αποστολέας σταθμός στέλνει αρχικά ένα πλαίσιο RTS στον παραλήπτη το οποίο δεν περιέχει δεδομένα. Το πλαίσιο αυτό έχει ως σκοπό να δεσμεύσει το μέσο μετάδοσης ο αποστολέας σταθμός για όσο χρόνο υπολογίζει ότι θα διαρκέσει η αποστολή του πλαισίου δεδομένων και να το ανακοινώσει και στους υπόλοιπους σταθμούς μέσω του μετρητή NAV.Όταν ο σταθμός παραλήπτης ανιχνεύσει ένα RTS frame,ανταποκρίνεται στέλνοντας, μετά από ένα SIFS,το CTS frame.Ο σταθμός αποστολέας επιτρέπεται να μεταδώσει το πακέτο του μόνο εάν το CTS frame έχει παραληφθεί σωστά. Υπενθυμίζεται ότι η αποστολή πλαισίου CTSγίνεται με τον συντομότερο χρόνο αναμονής SIFS.Τα frame των RTS και CTS περιλαμβάνουν πληροφορίες για το μήκος του μεταδιδόμενου πακέτου, όπου μπορούν να διαβαστούν από οποιονδήποτε σταθμό ο οποίος ¨ακούει¨ το μέσο. Έτσι για τη χρονική περίοδο στην οποία το κανάλι θα παραμείνει απασχολημένο μπορεί να ενημερώσει το NAV



Εικόνα: Το πρόβλημα του κρυμμένου κόμβου και ο μηχανισμός RTS/CTS.

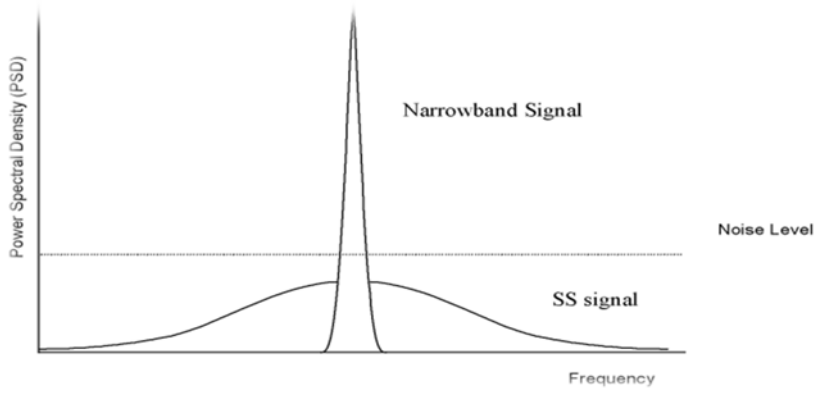
του σταθμού,το οποίο περιέχει τις πληροφορίες της.Το κανάλι αποδεσμεύεται με την λήψη από τον αποστολέα του τελευταίου πλαισίου ACK από τον παραλήπτη.Ο αποστολέας στέλνει το πλαίσιο δεδομένων και περιμένει την επιβεβαίωση λήψης του παραλήπτη.Έτσι η διαδικασία αποστολής του πλαισίου απαιτεί την ανταλλαγή τεσσάρων πλαισίων για να ολοκληρωθεί σωστά.Όταν ένας σταθμός είναι “hidden” από τον αποστολέα σταθμό, με την ανίχνευση μόνο ενός πλαισίου μεταξύ των πλαισίων RTS και CTS, μπορεί να καθυστερήσει την περαιτέρω μετάδοση και έτσι να αποφύγει τη σύγκρουση.Ο μηχανισμός RTS/ CTS επιτρέπει την αύξηση της απόδοσης ενός συστήματος αφού μειώνει τη διάρκεια μίας σύγκρουσης,όταν διαβιβάζονται μεγάλα μηνύματα δεδομένου ότι μειώνεται το μήκος των frames που περιλαμβάνονται στη σύγκρουση. Αν υποθέσουμε ότι έχουμε το τέλειο κανάλι το

οποίο ανιχνεύεται από κάθε σταθμό, σύγκρουση μπορεί να συμβεί μόνο όταν δύο ή περισσότερα πακέτα μεταδίδονται μέσα στο ίδιο slot time (χρονική θυρίδα).Εάν και οι δύο σταθμοί οι οποίοι επιχειρούν να μεταδώσουν τα πακέτα τους, χρησιμοποιούν το μηχανισμό RTS/CTS, σύγκρουση μπορεί να συμβεί μόνο στο RTS frame, η οποία ανιχνεύεται αρκετά νωρίς από τον σταθμό αποστολέα λόγω της έλλειψης του CTS frame από τον σταθμό προορισμού.

2.10 ΦΥΣΙΚΟ ΣΤΡΩΜΑ ΤΟΥ 802.11 (Wi-Fi)

Το φυσικό στρώμα του 802.11 έχει εκδοθεί σε τρία στάδια.Το πρώτο εκδόθηκε το 1997 και τα άλλα δυο το 1999.Το πρώτο στάδιο γνωστό ως 802.11 περιλαμβάνει το στρώμα MAC(αναφέρθηκε πιο πάνω) και τρείς προδιαγραφές φυσικού στρώματος, δύο για την ζώνη των 2.4 GHZ και μια για τις υπέρυθρες στα 1 και 2 Mbps.Τα άλλα στάδια περιλαμβάνουν,το 802.11a το οποίο λειτουργεί στην ζώνη των 5 GHz και σε ρυθμούς μετάδοσης δεδομένων μέχρι 54 Mbps και το 802.11b το οποίο λειτουργεί στην ζώνη 2.4 και 5.5 GHz και σε ρυθμούς μετάδοσης δεδομένων έως 11 Mbps.Τα δυο αυτά θα τα αναλύσουμε στην συνέχεια.Έτσι στο φυσικό στρώμα του 802.11 προδιαγράφονται οι παρακάτω τρεις τεχνικές διαμόρφωσής**:**

- **Direct Sequence Spread Spectrum (DSSS):** Διασπορά φάσματος άμεσης ακολουθίας η οποία λειτουργεί στην ζώνη των 2.4 GHz και σε ρυθμούς μετάδοσης 1 και 2 Mbps.
- **Frequency Hopping Spread Spectrum (FHSS):** Διασπορά φάσματος αναπήδησης συχνότητας η οποία λειτουργεί στην ζώνη των 2.4 GHz και σε ρυθμούς μετάδοσης 1 και 2 Mbps.
- **Infrared (IR):** Υπέρυθρες ακτίνες οι οποίες λειτουργούν σε μήκη κύματος 850 και 950 nmμε ρυθμούς μετάδοσης 1 και 2 Mbps.

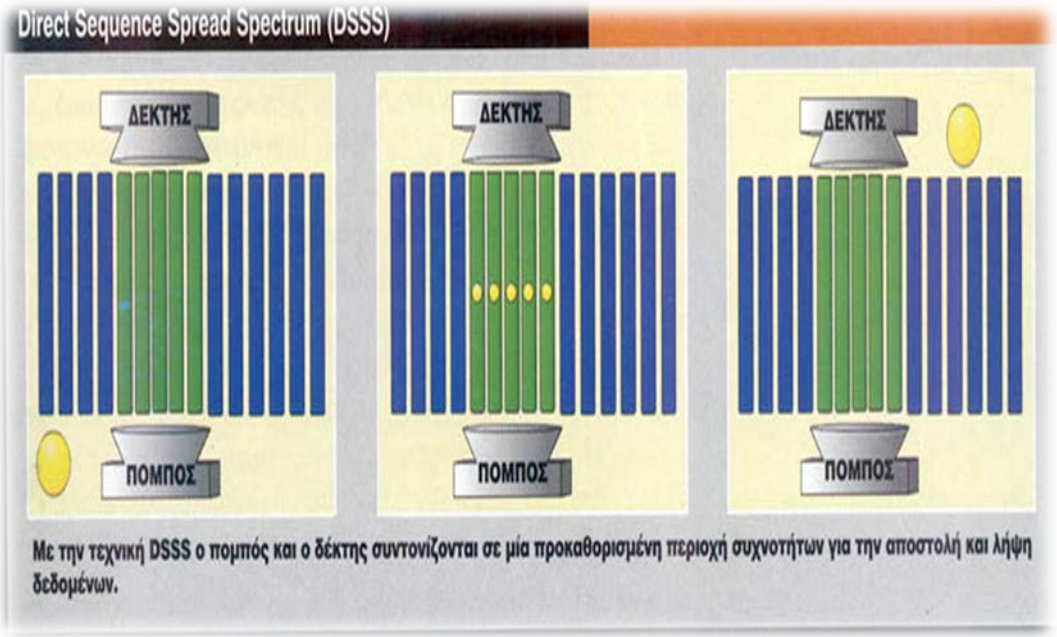


Εικόνα: Spread Spectrum.

Αξίζει να σημειωθεί ότι οι δυο πρώτες είναι τεχνικές εξάπλωσης φάσματος (Spread Spectrum),στις οποίες αφού διαμορφωθεί το σήμα πληροφορίας στην συνέχεια

εξαπλώνουν την ισχύ του σήματος σε μια ευρεία περιοχή συχνοτήτων,όπως φαίνεται στο παρακάτω σχήμα.Παρακάτω αναλύονται οι παραπάνω τεχνικές.

Direct Sequence Spread Spectrum (DSSS): Η τεχνική DSSS είναι μια επιτυχημένη τεχνική η οποία χρησιμοποιείται σε συνδυασμό με τα ασύρματα δίκτυα.Στην τεχνική αυτή δίνεται η δυνατότητα να χρησιμοποιηθούν μέχρι και 7 κανάλια,όπου το καθένα έχει ρυθμό μετάδοσης δεδομένων 1 και 2 Mbps.Ο αριθμός αυτών των καναλιών εξαρτάται από το εύρος ζώνης το οποίο εκχωρείται από διάφορούς εθνικούς οργανισμούς.Ο αριθμός των καναλιών αυτών κυμαίνεται σε 14 διαθέσιμα κανάλια από τα οποία τα 13 υπάρχουν στις περισσότερες χώρες της Ευρώπης και 1 μόνο διαθέσιμο κανάλι στην Ιαπωνία, όπου κάθε κανάλι έχει εύρος ζώνης ίσο με 5 GHz.Για τον ρυθμό μετάδοσης των 1 Mbps χρησιμοποιείται η μέθοδος κωδικοποίησης DBPSK και για ρυθμό μετάδοσης 2 Mbps την DQPSK μέθοδο κωδικοποίησης.Για την διασπορά του ρυθμού μετάδοσης δεδομένων και του εύρους του σήματος επομένως η τεχνική DSSS χρησιμοποιεί ένα κώδικα τεμαχισμού ή ακολουθία ψευδοθορύβου όπου κάθε bit πληροφορίας αντικαθιστάται από πολλά bitχρησιμοποιώντας ένα κώδικα διασποράς.Ο κώδικας αυτός διασκορπίζει το σήμα σε μια μεγαλύτερη ζώνη συχνότητας σε ευθεία αναλογία προς τον αριθμό bitπου χρησιμοποιούνται.Τα bit του κώδικα αυτού κατά σύμβαση ονομάζονται chips.Έτσι



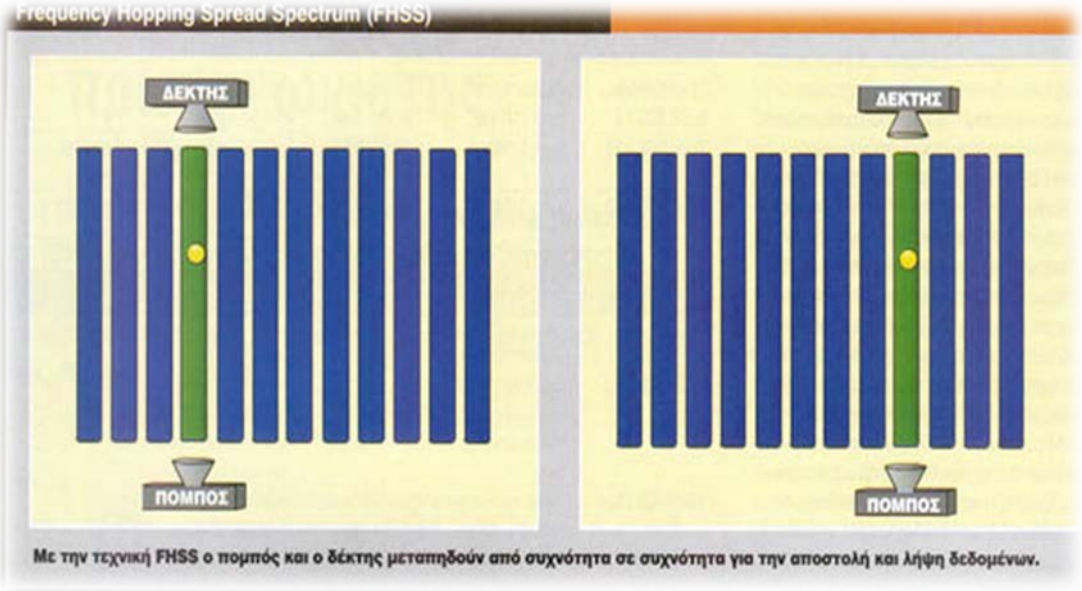
Εικόνα: Direct Sequence Spread Spectrum (DSSS).

για παράδειγμα αν ένα bit αντικαθίσταται από μια ακολουθία 10 chipstότε το σήμα το τελικό διαχέεται σε μια ζώνη συχνότητας η οποία είναι 10 φορές μεγαλύτερη από το αρχικό 1 bit.Υποθέτουμε πάντα ότι ο χρόνος μετάδοσης των bits είναι ίδιος και στις δυο περιπτώσεις δηλαδή ότι τα 10 chips πρέπει να μεταδοθούν στον ίδιο χρόνο

με το αρχικό bit.Έτσι με αυτήν την τεχνική διευρύνεται το φάσμα του μεταδιδόμενου σήματος μειώνοντας το πλάτος του ταυτόχρονα,δηλαδή απλώνεται η ισχύς του σε μεγαλύτερο φασματικό εύρος.Για το 802.11 χρησιμοποιείται μια ακολουθία Barkerη οποία είναι μια δυαδική ακολουθία {-1,+1} {s(t)}μήκους nόπου ότι οι τιμές αυτοσυσχέτισης της R(τ) ικανοποιούν την σχέση | R(τ)| <=1 για όλα τα |τ|<=(n-1).Έτσι στην DSSS τεχνική χρησιμοποιείται μια ακολουθία Barker11 τεμαχίων και συγκεκριμένα η λέξη «10110111000» όπου κάθε δυαδικό 1 αντιστοιχίζεται στην {+-++-+++- - -} ακολουθία και κάθε δυαδικό 0 στην ακολουθία {-+- -+- - -+++}.Να σημειωθεί ότι σημαντικό χαρακτηριστικό των ακολουθιών Barker αυθεντικότητα τους στις παρεμβολές και στην διάδοση πολλαπλών διαδρομών.

Frequency Hopping Spread Spectrum (FHSS): Η τεχνική FHSS χρησιμοποιεί πολλαπλά κανάλια ώστε το σήμα εκπέμπεται σε μια φαινομενικά τυχαία σειρά ραδιοσυχνοτήτων, αναπηδώντας από συχνότητα σε συχνότητα σε σταθερά χρονικά διαστήματα με βάσει μιας ακολουθίας ψευδοθορύβου.Το εύρος κάθε καναλιού και η απόσταση μεταξύ των φερουσών συχνοτήτων αντιστοιχεί συνήθως στο εύρος ζώνης του σήματος εισόδου.Για ένα σταθερό χρονικό διάστημα ο πομπός λειτουργεί σε ένα κανάλι τη φορά.Το 802.11 χρησιμοποιεί διάστημα 300 ms.Στην διάρκεια αυτή του διαστήματος αυτού,εκπέμπεται ένας αριθμός bit χρησιμοποιώντας κάποια μέθοδο κωδικοποίησης όπως την διαμόρφωση μετατόπισης συχνότητας (FSK) ή την δυαδική διαμόρφωση μετατόπισης φάσης (BPSK).Η ακολουθία των καναλιών που χρησιμοποιείται υπαγορεύεται από ένα κώδικα διασποράς.Για να συντονιστούν στην ακολουθία των καναλιών σε συγχρονισμό και ο πομπός και ο δέκτης χρησιμοποιούν τον ίδιο κώδικα διασποράς.Το σήμα που προκύπτει τοποθετείται με κέντρο κάποιας συχνότητας βάσης.Μια πηγή ψευδοθορύβου ή ψευδοτυχαίων αριθμών χρησιμεύει ως δείκτης σε ένα πίνακα συχνοτήτων.Αυτός είναι ο κώδικάς διασποράς που αναφέρθηκε προηγουμένως.Η κάθε ομάδα k-bit της πηγής ψευδοθορύβου καθορίζει μια από τις 2^{κ} συχνότητες.Έτσι σε κάθε διαδοχικό διάστημα δηλαδή σε κάθε ομάδα k-bit της πηγής ψευδοθορύβου επιλέγεται μια νέα φέρουσα συχνότητα.Στην συνέχεια η συχνότητα αυτή διαμορφώνεται από το σήμα που διαμορφώθηκε από τον αρχικό διαμορφωτή για να δώσει ένα νέο σήμα με την ίδια μορφή όπου έχει ως κέντρο την επιλεγμένη φέρουσα συχνότητα.Το 802.11 χρησιμοποιεί κανάλια του 1 MHz.Ο αριθμός των καναλιών κυμαίνεται από 23 στην Ιαπωνία, 20 στην Ευρώπη και μέχρι 70 στις ΗΠΑ.Το σχήμα αναπήδησης και τα στοιχεία του είναι ρυθμιζόμενα.Ο ελάχιστός ρυθμός αναπήδησης στις ΗΠΑ για παράδειγμα είναι 2,5 αναπηδήσεις ανά δευτερόλεπτό.Ενώ η ελάχιστη απόσταση αναπήδησης σε συχνότητα στην Βόρειο Αμερική και στο μεγαλύτερο τμήμα της Ευρώπης είναι 6MHz και στην Ιαπωνία είναι 5 MHz.Η FSSSγια την διαμόρφωση χρησιμοποιεί για το ρυθμό μετάδοσης 1 Mbpsτην Gaussian FSK δυο επιπέδων και για 2 Mbps την GFSK τεσσάρων επιπέδων, όπου από την κεντρική συχνότητα τις τέσσερις διαφορετικές αποκλίσεις τις ορίζουν τέσσερις συνδυασμοί των 2 bit.Τα bit0 και 1 κωδικοποιούνται από την τρέχουσα φέρουσα συχνότητα.Χαρακτηριστικά πλεονεκτήματα αυτής της τεχνικής σε σχέση με την DSSS είναι**:**

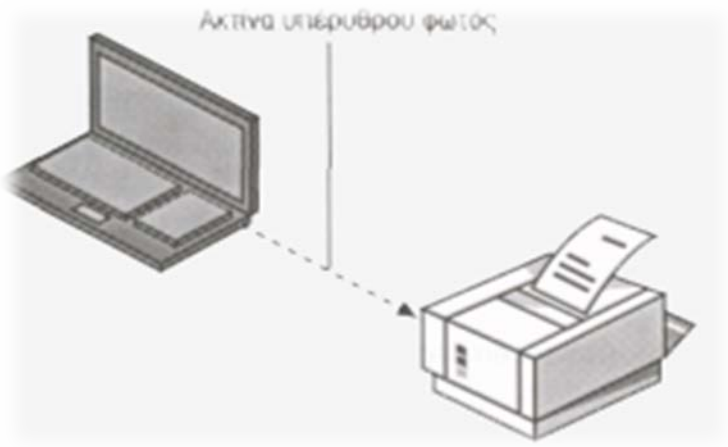
- Η χαμηλότερη κατανάλωση ενέργειας και η συνύπαρξη πολλών τέτοιων δικτύων χωρίς να επηρεάζεται η συνολική διέλευση δηλαδή σε κάθε χρονική στιγμή μεταδίδεται διαφορετική φέρουσα μεγιστοποιώντας έτσι την συνολική διέλευση.
- Τα ηλεκτρονικά τα οποία χρησιμοποιούνται για την υλοποίηση ανάλογων συσκευών είναι φθηνά και απλούστερα.
- Η δυνατότητα συνύπαρξης χρηστών οι οποίοι εκπέμπουν σήματα στενής ζώνης.Αν από ένα σύστημα αναπήδησης συχνότητας η εκπομπή γίνεται με μεγάλη ισχύ οι παρεμβολή που έχουν οι χρήστες,εφόσον μπλοκάρουν μια φέρουσα από όσες αυτό χρησιμοποιεί είναι αμελητέα.



Εικόνα: Frequency Hopping Spread Spectrum (FHSS).

Υπέρυθρες ακτίνες(IR): Στο 802.11 ένα σύστημα υπέρυθρων είναι πανκατευθυντκό με εμβέλεια μέχρι και 20m,όπου περιλαμβάνει ένα μοναδικό σταθμό ο οποίος λειτουργεί σαν επαναλήπτης πολλών θυρών,εκπέμποντας ένα σήμα προς όλες τις κατευθύνσεις προς όλες τις κατευθύνσεις το οποίο μπορεί να ληφθεί από όλους πομποδέκτες IR οι οποίοι βρίσκονται μέσα στον ίδιο χώρο δηλαδή μέσα στην ευθεία της οπτικής του επαφής.Ο σταθμός βάσης βρίσκεται στην κορυφή από όπου οι πομποδέκτες επικοινωνούν με αυτόν στέλνοντας μια κατευθυντική δέσμη.Για την μετάδοσή των δεδομένων χρησιμοποιείται η τεχνική διαμόρφωσης παλμών PPM (pulse position modulation) όπου η εκπομπή των παλμών είναι 250 nsec και παράγονται από τα LEDs (Light Emitting Diode) εμπόδια δεν χρησιμοποιείται ιδιαίτερα.Χρησιμοποιεί για τον ρυθμό μετάδοσης 1Mbps την μέθοδο διαμόρφωσης 16-PPM (pulse position modulation) διαμόρφωσή θέσης παλμού, όπου κάθε ομάδα 4 bitδεδομένων αντιστοιχίζεται σε ένα από τα 16-PPM σύμβολα,όπου η διάρκεια του κάθε bitείναι 250 nsecκαι ένα από αυτά είναι ίσο με 1 και τα υπόλοιπα με 0.Ενώ για τον ρυθμό μετάδοσης 2 Mbps,την 4-PPM όπου κάθε ομάδα 2 bit αντιστοιχίζεται σε

μία από τις τέσσερις ακολουθίες των 4 bit όπου η κάθε μια αποτελείται από τρία 0 και ένα 1 όπου με την μέθοδο ισχύος οπτικού παλμού το δυαδικό 1 αντιστοιχεί στην παρουσία το σήματος ενώ το 0 στην απουσία του.Να υπενθυμισθεί ότι η μετάδοσή των δεδομένων γίνεται σε μήκη κύματος 850 και 950 nm για τους ρυθμούς μετάδοσης 1 έως 2 Mbpsμε όριο 2 Wattκαι με μέση τιμή ίση με 125 ή 250 mWatt.Τέλος λόγω του ότι η τεχνική αυτή δεν μπορεί να διαπεράσει τα εμπόδια δεν χρησιμοποιείται ιδιαίτερα.



Εικόνα: Υπέρυθρη επικοινωνία.

2.11 ΥΠΟΤΡΟΠΑ IEEE 802.11

Τα υπότροπα του 802.11 προέρχονται από την ομάδα εργασίας του IEEE(Institute of Electrical and Electronics, Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών),από έρευνες των μελών της. Στην ουσία αποτελούν τα μέλη της οικογένειας του προτύπου IEEE 802.11.Στην συνέχεια αναλύονται αυτά τα υπότροπα ανά κωδικό ομάδας εργασίας.

2.12 ΥΠΟΤΡΟΠΟ 802.11a

Το υπότροπο 802.11a εκδόθηκε το 1999 από το IEEE με τίτλο**:** "Higher-Speed Physical Layer Extension in the 5 GHz Band".Πρόκειται για ένα πρωτόκολλο ενός ασύρματου τοπικού δικτύου το οποίο λειτουργεί στην μπάντα των 5 GHz. Το 802.11 χρησιμοποιεί την διαμόρφωση διαίρεσης συχνότητας ή αλλιώς διαμόρφωση πολλών φερουσών, Orthogonal Frequency Division Multiplexing (OFDM).Η διαμόρφωση αυτή προσφέρει στο 802.11 ρυθμούς μετάδοσης μέχρι και 54 Mbps.Η λειτουργία του στην μπάντα των 5 GHzπροσφέρει το πλεονέκτημα μείωσης των παρεμβολών και των προβλημάτων που προκαλούν προσφέροντας καλύτερες επιδόσεις σε σχέση με το 802.11 και το 802.11b. Λόγω της μειωμένης πιθανότητας παρεμβολών και της

υψηλής ταχύτητάς του, το συγκεκριμένο πρωτόκολλο θεωρείται ιδανικό για την υποστήριξη multimedia εφαρμογών, καλύπτοντας στο ακέραιο τόσο τις σημερινές όσο και τις μελλοντικές απαιτήσεις διαμεταγωγής.Ορισμένα προϊόντα ασύρματης δικτύωσης με chipset από την εταιρεία Atheros υποστηρίζουν ακόμη μεγαλύτερες ταχύτητες,που φθάνουν τα 72Mbps,ενώ σε ορισμένες περιπτώσεις ξεπερνούν ακόμη και τα 108Mbps.Η αύξηση των επιδόσεων στην πράξη δεν είναι ιδιαίτερα εντυπωσιακή, ενώ πραγματοποιείται σε βάρος της εμβέλειας του ασύρματου δικτύου.Το 802.11 χρησιμοποιεί μέχρι 52 φέρουσες που διαμορφώνονται ανάλογα με το ρυθμό που απαιτείται κατά διαμόρφωσηBRSK,QPSK,16-QAM ή 64-QAM.Ο διαχωρισμός των συχνοτήτων υποφερουσών είναι 0.3125 MHz.Επίσης ένας συναλλακτικός κώδικας με ρυθμό 1/2,2/3 ή 3/4 παρέχει αυτοδύναμη διόρθωση σφαλμάτων.Το πρότυπο 802.11 ωστόσο δεν επικράτησε και ένα λόγος είναι ότι δεν είναι συμβατό με το 802.11b.

2.13 ΥΠΟΤΡΟΠΟ 802.11b

Το υπότροπο 802.11b εκδόθηκε και αυτό το 1999 από το IEEE με τίτλο**:** "Higher-Speed Physical Layer Extension in the 2.4 GHz Band".Πρόκειται για ένα πρωτόκολλο το οποίο επεκτείνει το φυσικό επίπεδο των ασύρματων δικτύων του 802.11 και επέκταση του τρόπου κωδικοποίησης εξάπλωσης φάσματος ευθείας ακολουθίας DSSS,παρέχοντας ρυθμούς μετάδοσης 5,5 και 11Mbpsτο οποίο λειτουργεί στην μπάντα των 2,4 GHz.Για την επίτευξη μεγαλύτερου ρυθμού δεδομένων στο ίδιο εύρος ζώνης,με τον ίδιο αριθμό τεμαχισμού ο οποίος είναι ίδιος με την DSSS 11MHz χρησιμοποιεί την συμπληρωματική διαμόρφωση κώδικα CCK (complementary code keying).Η διαμόρφωση CCK προσφέρει και δυο νέα χαρακτηριστικά τα οποία είναι:

- Δυνατότητα επιλογής μικρότερου προοιμίου (short preamble) των 72 bits στο επίπεδο 2 (OSI) σε αντίθεση με το μεγάλο προοίμιο (long preamble) των 144 bits του αρχικού 802.11. Η δυνατότητα αυτή αποσκοπεί στον ταχύτερο συγχρονισμό των συσκευών. Φυσικά για λόγους συμβατότητας με το αρχικό πρότυπο, ως προεπιλογή χρησιμοποιείται το μεγάλο προοίμιο.
- Δυνατότητα επιλογής καναλιών, σε αντίθεση με την στατική κατανομή καναλιού στο 802.11.

Στην διαμόρφωση CCK τα δεδομένα εισόδου λαμβάνονται σε μπλοκ των 8 bitμε ρυθμό 1.375MHz (8 bit/σύμβολο x 1.375 MHz=11Mbps).Τα έξι από αυτά τα 8 bit αντιστοιχίζονται σε έναν από 64 σύνθετους κωδικούς βάσει ενός πίνακα Walsh 8 x 8 όπου ή έξοδος αντιστοίχησης μαζί με τα δυο επιπλέον bitαποτελούν την είσοδο προς έναν διαμορφωτή QPSK.Για την διατήρηση της συμβατότητας με το 802.11 και για τους ρυθμούς μετάδοσης των 1 και 2 Mbpsχρησιμοποιεί την διαμόρφωση BPSKκαι QPSK αντίστοιχα.Τέλος για την βελτίωση της συνολικής απόδοσης στους ρυθμούς 5,5 και 11Mbps χρησιμοποιήθηκε ο δυαδικός κώδικάς συνέλιξης πακέτου PBCC (Packet Binary Convolution Code) με κέρδος κωδικοποίησης 3db.Σήμερα οι περισσότερες εγκαταστάσεις ασύρματων δικτύων,ακολουθούν το συγκεκριμένο πρότυπο, ενώ ο οργανισμός WECA (Wireless Ethernet Certitication Alliance), μέλη

του οποίου είναι όλοι οι μεγάλοι κατασκευαστές προϊόντων ασύρματης δικτύωσης, αναλαμβάνει την πιστοποίηση της συμβατότητας όλων των συσκευών που κυκλοφορούν στην αγορά με το συγκεκριμένο πρωτόκολλο.

2.14 ΥΠΟΤΡΟΠΟ 802.11c

Το πρωτόκολλο αυτό χρησιμοποιείται διότι παρέχει όλες τις απαραίτητες πληροφορίες για τη διασφάλιση των σωστών λειτουργιών των γεφυρών (bridges).Οι πληροφορίες αυτές χρησιμοποιούνται από τους κατασκευαστές σημείων πρόσβασης κυρίως για την διασφάλιση της διαλειτουργικότητας με τις αντίστοιχες συσκευές άλλων κατασκευαστών.

2.15 ΥΠΟΤΡΟΠΟ 802.11g

Το υπότροπο 802.11g εκδόθηκε το 2003 από το IEEE με τίτλο**:** "Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band".Πρόκειται για ένα πρωτόκολλο το οποίο διατηρώντας συμβατότητα με το 802.11b προσφέρει ρυθμούς μετάδοσης 54 Mbps όπως το 802.11a χρησιμοποιώντας την διαμόρφωση OFDM λειτουργώντας στην μπάντα των 2,4 GHz και για υψηλούς ρυθμούς μετάδοσης εμπρόσθια διόρθωση λαθών.Επίσης υποστηρίζει την συμπληρωματική διαμόρφωση κώδικα CCK για συμβατότητα με το 802.11b.Χρησιμοποιεί δυαδικό κώδικά συνέλιξης πακέτου PBCC προσφέροντας έτσι ταχύτητες 22 Mbps.Τέλος το βασικό πλεονέκτημα του 802.11g είναι ότι είναι συμβατό με το 802.11b,οπότε συσκευές 802.11b και 802.11g μπορούν να συνυπάρχουν σε ένα δίκτυο.

2.16 ΥΠΟΤΡΟΠΟ 802.11e

Το υπότροπο 802.11e είναι ένα συμπληρωματικό πρωτόκολλο του επιπέδου πολλαπλής πρόσβασης του 802.11 το οποίο παρέχει εγγυήσεις για βελτιωμένη ποιότητα υπηρεσίας QoS(Quality of Service) τις οποίες δεν παρείχε το αρχικό πρότυπο 802.11.Η έλλειψη δυνατότητας παροχής διαφοροποιημένης μεταχείρισης σε διαφορετικές κατηγορίες κίνησης,είναι μια από τις βασικές αδυναμίες του 802.11 πρωτοκόλλου τις οποίες στοχεύει το 802.11e.Η βελτίωση επετεύχθηκε με την τροποποίηση του επιπέδου MAC.

2.17 ΥΠΟΤΡΟΠΟ 802.11f

Η επικοινωνία των σημείων πρόσβασης με σκοπό την άμεση υποστήριξη υπηρεσίας περιαγωγής (roaming) μεταξύ των χρηστών από ένα σημείο πρόσβασης σε ένα άλλο δεν προσδιορίστηκε από την ομάδα εργασίας του 802.11 σκόπιμα.Έτσι το πρόβλημα που προκύπτει είναι ότι τα σημεία πρόσβασης AP τα οποία προέρχονται από διαφορετικούς κατασκευαστές όταν υποστηρίζουν λειτουργίες περιαγωγής να μην λειτουργούν ομαλά μεταξύ τους.Έτσι το πρωτόκολλο 802.11f έχει σκοπό την

δημιουργία των προδιαγραφών που θα περιγράφουν όλες τις απαραίτητες πληροφορίες ρητά που απαιτούνται από τα σημεία πρόσβασης για την εξασφάλιση μιας επιτυχής περιαγωγής και ομαλής διαλειτουργικότητας.

2.18 ΥΠΟΤΡΟΠΟ 802.11i

Το υπότροπο 802.11 ιεκδόθηκε το 2004 από το IEEE με τίτλο**:** "Amendment 6: Medium Access Control (MAC) Security Enhancements".Πρόκειται για ένα συμπληρωματικό πρότυπο για την βελτίωση της ασφάλειας συστήματος καθώς καλύπτει τα κενά που εντοπίστηκαν στο πρωτόκολλο ασφάλειας WEPτου 802.11 ο οποίος θα αναλυθεί στο επόμενο κεφάλαιο. Η χρήση του αλγορίθμου RC4 αποδείχτηκε ανεπαρκής με παραλήψεις και αρκετά σφάλματα κάνοντας τα ασύρματα δίκτυα εύκολο στόχο σε διάφορα είδη κακόβουλων επιθέσεων.Έτσι με το πρωτόκολλο 802.11i καθορίζονται πρωτόκολλα για τα κλειδιά κρυπτογράφησης όπως τα 802.1X,TKIP, CCMP,AES και άλλα.

2.19 ΥΠΟΤΡΟΠΟ 802.11h

Το υπότροπο 802.11h αποτελεί ένα συμπληρωματικό πρότυπο για το υποεπίπεδο MAC και λειτουργεί στην ζώνη των 5 GHz.Παρόλο που το 802.11h πρωτόκολλο είναι αμερικάνικής προελεύσεως εντούτοις έχει ευρεία χρήση στην Ευρώπη.Συγκεκριμένα για τις συσκευές οι οποίες λειτουργούν στην ζώνη των 5 GHzοι ευρωπαϊκοί κανονισμοί απαιτούν να έχουν δυνατότητες ελέγχου της εκπεμπόμενης ισχύος TCP (Transmission Power Control) και δυναμικής επιλογής συχνότητας DFS (Dynamic Frequency Selection),απαιτήσεις οι οποίες προδιαγράφονται στο συγκεκριμένο πρωτόκολλο.

2.20 ΥΠΟΤΡΟΠΟ 802.11n

Στις αρχές του 2004 η νέα ομάδα εργασίας TaskGroup ή TGn του IEEE ανέλαβε σκοπό να δημιουργήσει μια τροποποίηση του 802.11 η οποία θα είχε ως επίτευξη του πραγματικού ρυθμού μεταφοράς σε 100 Mbpstουλάχιστον ενώ ο θεωρητικός αριθμός φτάνει τα 200 Mbpstουλάχιστον. Για την επίτευξή αυτών των ταχυτήτων χρειάζεται η μετάβαση σε νέες τεχνολογίες ασύρματης μετάδοσης και πιο συγκεκριμένα στην τεχνολογία MIMO (Multiple Input – Multiple Output).Η τεχνολογία MIMO κάνει χρήση πολλαπλών κεραιών για την μετάδοση δεδομένων όπου η κάθε μια λειτουργεί ταυτόχρονα και ανεξάρτητα.Σύμφωνα με τον οργανισμό Wi-Fi (Wi-Fi Alliance) η δημοσίευση της τροποποίησης δηλαδή το 802.11n εκδόθηκε μετά το δεύτερο εξάμηνο του 2006.

Παρακάτω στην εικόνα παραθέτονται μερικά από τα υπότροπα του 802.11.

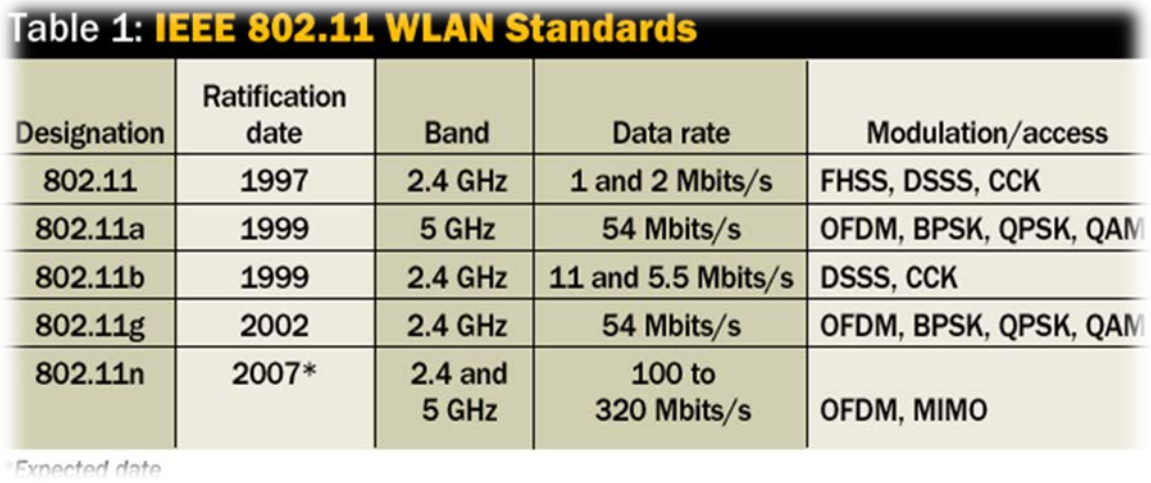


Table 1: IEEE 802.11 WLAN Standards

Designation	Ratification date	Band	Data rate	Modulation/access
802.11	1997	2.4 GHz	1 and 2 Mbits/s	FHSS, DSSS, CCK
802.11a	1999	5 GHz	54 Mbits/s	OFDM, BPSK, QPSK, QAM
802.11b	1999	2.4 GHz	11 and 5.5 Mbits/s	DSSS, CCK
802.11g	2002	2.4 GHz	54 Mbits/s	OFDM, BPSK, QPSK, QAM
802.11n	2007*	2.4 and 5 GHz	100 to 320 Mbits/s	OFDM, MIMO

*Expected date

Εικόνα: Υπότροπα του 802.11.

ΚΕΦΑΛΑΙΟ 3^{Ο}: Η "ΑΣΦΑΛΕΙΑ" ΣΤΑ Wi-FiΔΙΚΤΥΑ

3.1 ΤΡΟΠΟΙ ΕΠΙΘΕΣΗΣ ΣΤΑ ΑΣΥΡΜΑΤΑ Wi-Fi ΔΙΚΤΥΑ

Πέρα από το ότι η δυνατότητα σύνδεσης σε δίκτυο εν κινήσει αποτελεί ένα ισχυρό πλεονέκτημα του ασύρματου δικτύου εν του τοις φανερώνει και ένα βασικό μειονέκτημα το οποίο είναι το ζήτημα ασφαλείας του ασύρματου δικτύου.Στην αρχή της εμφάνισης της ασύρματης τεχνολογίας υπήρχαν λιγότεροι κίνδυνοι από ότι σήμερα διότι τα ασύρματα δίκτυα ήταν λιγοστά και έτσι οι επικείμενοι εισβολείς δεν είχαν ούτε καν την προσπάθεια εξουσιοδοτημένης εισόδου.Προβλήματα δημιουργούνται από τις υπάρχουσες τεχνολογίες κρυπτογράφησης και πιστοποίησης χρήστη που χρησιμοποιούνται σήμερα.Επίσης η ευρεία χρήση των ασύρματωνDSL routerκαθώς και η άγνοια που έχουν πολλοί χρήστες όσο αφορά τους κινδύνους ασφάλειας του ασύρματου δικτύου κάνουν τα ασύρματα οικιακά κυρίως δίκτυα μη ασφαλή.Έτσι η ευρεία χρήση των ασύρματων δικτύων καθώς και ότι διάφοροι crackers έχουν δημιουργήσει εργαλεία πρόσβασης δικτύων κάνουν την δυνατότητα πρόσβασης στα ασύρματα δίκτυα πιο εύκολη από ποτέ ακόμη και για έναν απλό χρήστη.Χωρίς λοιπόν καμία γνώση προγραμματισμού και δικτύων μπορεί κάποιος χρησιμοποιώντας τα εργαλεία αυτά να έχει πρόσβαση σε ασύρματο δίκτυο που υπάρχει στο περιβάλλον του.Οι εισβολείς σε ένα ασύρματο δίκτυο έχουν ευκολία πρόσβασης επίσης κυρίως λόγω της ασύρματης φύσης του δικτύου.Αν για παράδειγμα ένας εργαζόμενος μια εταιρίας χρησιμοποιήσει κάποια από τα συστήματα της εταιρίας του όπως π.χ. ασύρματο routertότε σε περίπτωση επίθεσης από κάποιον εισβολέα και υποκλοπής των κρυπτογραφικών δεδομένων εκτίθεται αυτομάτως όλα τα συστήματα της εταιρίας.

3.2 ΜΗ ΗΘΕΛΗΜΕΝΗ ΣΥΣΧΕΤΙΣΗ

Η μη εξουσιοδοτημένη πρόσβαση στο ασύρματο δίκτυο μιας εταιρίας για παράδειγμα μπορεί να συμβεί μέσω αρκετών τεχνικών και προθέσεων.Έτσι η μη ηθελημένη πρόσβαση μπορεί να γίνει όταν ένας χρήστης μια εταιρίας για παράδειγμα, χρησιμοποιήσει τον υπολογιστή του (laptop) για να συνδεθεί στο ασύρματο δίκτυο της εταιρίας του για διάφορες εργασίες άλλα όμως ο υπολογιστής του συνδέεται με το ασύρματο δίκτυο που παρέχει η διπλανή εταιρία.Η διαδικασία αυτή μπορεί να συμβεί χωρίς τουλάχιστον αρχικά ο χρήστης να το αντιληφθεί ότι έχει συνδεθεί σε κάποιο άλλο ασύρματο δίκτυο.Η μη ηθελημένη συσχέτισή γίνεται λόγω κυρίως του ότι έχει προστεθεί σε αρκετά λογισμικά διαχείρισης συνδέσεων ασύρματου δικτύου η δυνατότητα αυτόματης σύνδεσης σε δίκτυα στα οποία η στάθμη σήματος είναι ισχυρή εφόσον στο παρελθόν έχει προηγηθεί συσχέτιση με αυτό το δίκτυο.

3.3 ΗΘΕΛΗΜΕΝΗ ΣΥΣΧΕΤΙΣΗ

Η ηθελημένη συσχέτιση μπορεί να συμβεί ως εξής**:** Ο εισβολέας-υποκλοπέας χρησιμοποιεί ως σημείο πρόσβασης AP κάποιο δικό του υπολογιστικό σύστημα όπως ένας υπολογιστής με ασύρματη κάρτα δικτύου.Έτσι το σημείο πρόσβασης του υποκλοπέα φαίνεται ότι είναι το αυθεντικό σημείο πρόσβασης που χρησιμοποιεί η εταιρία με αποτέλεσμα οι εξουσιοδοτημένοι χρήστες της εταιρίας εν αγνοία να συνδέονται σε αυτό.Η λειτουργικότητα του ¨αληθινού¨ σημείου πρόσβασης επιτυγχάνεται με την χρήση λογισμικού όπως είναι για παράδειγμα οι HostAPστο λειτουργικό σύστημα Linux,το οποίο επιτρέπει την ασύρματη κάρτα δικτύου του να μοιάζει με νόμιμο σημείο πρόσβασης.Έτσι ο υποκλοπέας μπορεί να συνδεθεί νόμιμα πλέον στο σημείο πρόσβασης εφόσον γνωρίζει τους κωδικούς χρηστών και του ασύρματού δικτύου καθώς όλα τα δεδομένα περνάνε από το δικό του υπολογιστικό σύστημα.Έτσι μπορεί να διεξάγει επίθεση και υποκλοπή δεδομένων καθώς και να εισάγει κακόβουλο λογισμικό όπως Trojan,worm,κλπ σε υπολογιστικά συστήματα χρηστών.Προστασίες όπως ο έλεγχος ταυτότητας δικτύου και εικονικά ιδιωτικά δίκτυα (VPN) δεν προσφέρουν εμπόδιο καθώς τα ασύρματα δίκτυα όπως γνωρίζουμε λειτουργούν στο επίπεδο 1 και 2 του μοντέλου OSI.

Εικόνα: Ηθελημένη συσχέτιση ο χρήστης εν αγνοία συνδέεται στο AP του υποκλοπέα και διαβιβάζει σε αυτό προσωπικά δεδομένα.

3.4 ΟΜΟΤΙΜΑ (ad-hoc) ΔΙΚΤΥΑ

Τα ομότιμα (Ad-hoc) δίκτυα μπορούν να δημιουργήσουν μια απειλή σε θέμα ασφάλειας,καθώς στα δίκτυα αυτά μεταξύ των ασύρματων υπολογιστών δεν υπάρχει ένα σημείο πρόσβασης μεταξύ τους και λόγω του ότι χρησιμοποιούνται συνήθως προσωρινά δεν δίνεται απαραίτητη σημασία από τους διαχειριστές τους για την ασφάλεια τους.Χρησιμοποιούνται ωστόσο μέθοδοι κρυπτογράφησης για να παρέχουν ασφάλεια αλλά η προστασία των δικτύων αυτών είναι συνήθως μικρή.Η απειλή στην ασφάλεια δεν δημιουργείται από το ίδιο το Ad-hoc δίκτυο αλλά από τη γέφυρα που παρέχει σε άλλα δίκτυα και την προεπιλογή τοποθέτησης στις περισσότερες εκδόσεις του MicrosoftWindowsνα έχει ανοιχτή αυτήν την λειτουργία.Κατά συνέπεια ο χρήστης μπορεί ούτε καν να γνωρίζει ότι ο υπολογιστής του έχει ένα ακάλυπτο Ad-hoc δίκτυο σε λειτουργία.Αν οι χρήστες χρησιμοποιούν συγχρόνως επίσης ένα συνδεδεμένο με καλώδιο ή ασύρματο δίκτυο υποδομής,παρέχουν μια γέφυρα στο εξασφαλισμένο οργανωτικό δίκτυο μέσω της ακάλυπτηςAd-hoc σύνδεσης.Η γέφυρα που δημιουργείται είναι δυο ειδών**:** Μια άμεση γέφυρα, που απαιτεί το χρήστη να διαμορφώνει μια γέφυρα μεταξύ των δύο συνδέσεων και είναι έτσι απίθανο να αρχίσει εκτός αν είναι επιθυμητό και μια έμμεση γέφυρα που είναι οι κοινοί πόροι στον υπολογιστή του χρήστη.Στην έμμεση γέφυρα διακρίνονται δυο κίνδυνοί ασφαλείας. Στον πρώτο τα σημαντικά οργανωτικά στοιχεία που λαμβάνονται μέσω του εξασφαλισμένου δικτύου μπορεί να είναι στην τελικό κόμβο του σκληρού του υπολογιστή του χρήστη και έτσι να είναι εκτεθειμένος και να ανακαλυφθεί μέσω του ακάλυπτου Ad-hoc δικτύου.

Εικόνα: ομότιμο Ad-hoc δίκτυο.

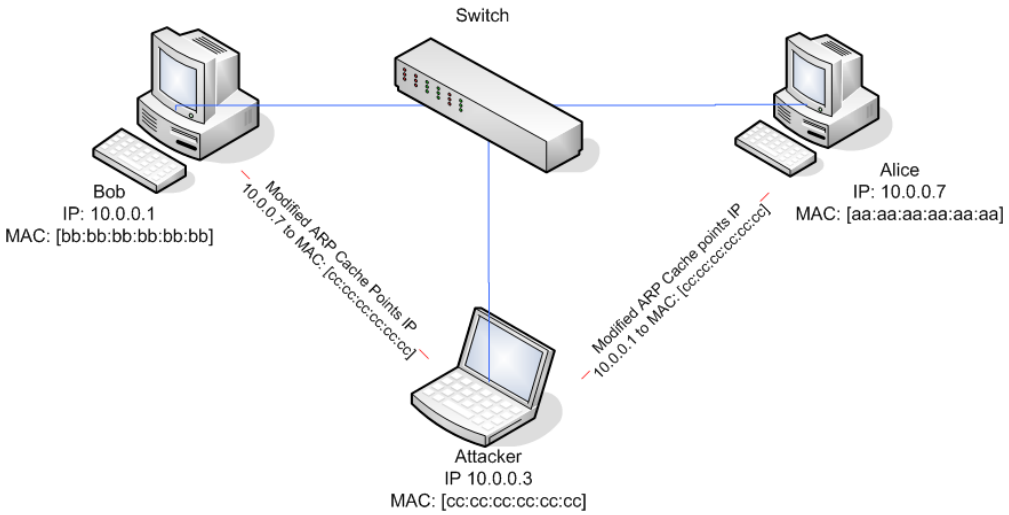
Ο δεύτερος είναι ότι ένας ιός υπολογιστών ή ένας ανεπιθύμητος κώδικαςμπορεί να τοποθετηθεί στον υπολογιστή του χρήστη μέσω της ακάλυπτης Ad-hoc σύνδεσης και έτσι θα διαρρεύσει μέσα στο οργανωτικό εξασφαλισμένο δίκτυο,όπου σε αυτήν την περίπτωση,το πρόσωπο που τοποθετεί τον κακόβουλο κώδικα δεν χρειάζεται να

«σπάσει» τους κωδικούς πρόσβασης στο οργανωτικό δίκτυο,ο νόμιμος χρήστης του παρέχει την πρόσβαση μέσω της κανονικής σύνδεσης του.Έτσι απλά ο εισβολέας πρέπει να τοποθετήσει τον κακόβουλο κώδικα στο τελικό κόμβο του συστήματος του ανυποψίαστου χρήστη μέσω των ανοικτών (ακάλυπτων) Ad-hoc δικτύων. Παρόλα αυτά τα ομότιμα (Ad-hoc) λόγω της μικρής διάρκειας ζωής τους μιας και είναι συνήθως ¨μια χρήσης¨ δεν κρίνονται ιδιαιτέρως επικίνδυνα.Τα δίκτυα αυτά φυσικά είναι ανασφαλή χωρίς την χρήση των υποτυπωδών διαδικασιών ασφαλείας.

3.5 ΥΠΟΚΛΟΠΗΤΑΥΤΟΤΗΤΑΣ (MAC spoofing)

Η υποκλοπή ταυτότητας (ή MAC spoofing) συμβαίνει όταν ο εισβολέας είναι σε θέση να παρακολουθήσει την κίνηση του δικτύου και να εντοπίσει την διεύθυνση MAC ενός υπολογιστικού συστήματός το οποίο παρέχει αυξημένα δικτυακά δικαιώματα.Μια διεύθυνση MAC (Media Access Control) είναι ένας δεκαεξαδικός σειριακός αριθμός και είναι μοναδικός για κάθε δικτυακή συσκευή σε όλο το πλανήτη με την μορφή xx:xx:xx:xx:xx:xx,για παράδειγμα 0B:23:45:C5:B4:89.Η διεύθυνση αυτή είναι μοναδική για κάθε ελεγκτή διασύνδεσης δικτύου (NIC) από τον κατασκευαστή.Η διεύθυνση MAC χρησιμεύει στην ανταλλαγή μηνυμάτων μεταξύ δικτυακών συσκευών (π.χ.laptop) και ο αριθμός αυτός αποκαλύπτεται κατά την διάρκεια επικοινωνίας μεταξύ του αποστολέα και του παραλήπτη.Έτσι η υποκλοπή ταυτότητας είναι μια τεχνική αλλοίωσης της προκαθορισμένης φυσικής διεύθυνσης MAC μιας κάρτας δικτύου.Ο εισβολέας σε αυτήν την περίπτωση,υποκρίνεται κάποιον νόμιμο χρήστη του διαδικτύου και έτσι αποκτάει τα δικαιώματα πρόσβασης σε υπηρεσίες που αυτός επιθυμεί χρησιμοποιώντας ουσιαστικά τα στοιχεία πρόσβασης ενός νόμιμού χρήστη.Τα στοιχεία αυτά μπορούν να βρεθούν στα χέρια ενός εισβολέα όταν δεν χρησιμοποιείται κρυπτογράφηση στο δίκτυο,όταν χρησιμοποιούνται εύκολοι κωδικοί και όταν δεν ακολουθούνται οι κανόνες προστασίας κωδικών πρόσβασης.Η μέθοδος αυτή είναι ιδανική όταν ο υποκλοπέας θέλει να μην αποκαλυφθεί.Έτσι αν η συσκευή καταφέρει να ξεγελάσει το δίκτυο ως εξουσιοδοτημένη συσκευή τότε όλα τα δικαιώματα πρόσβασης περιέρχονται σε αυτόν.Τα περισσότερα ασύρματα συστήματα διαθέτουν κάποιο είδος φιλτραρίσματος MAC διευθύνσεων έτσι ώστε να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες (με συγκεκριμένη προ δηλωμένη MAC διεύθυνση) να αποκτήσουν πρόσβαση στο δίκτυο και να το χρησιμοποιήσουν.Ωστόσο υπάρχει μεγάλος αριθμός προγραμμάτων τα οποία έχουν την δυνατότητα σε συνδυασμό με άλλο λογισμικό να παρουσιάζουν στο ασύρματο δίκτυο την διεύθυνση MAC που είναι επιθυμητή για την πρόσβαση στο δίκτυο για τον εισβολέα.Μερικά από τα εργαλεία (software) που χρησιμοποιούνται για την υποκλοπή ταυτότητας MACspoofing είναι**:**

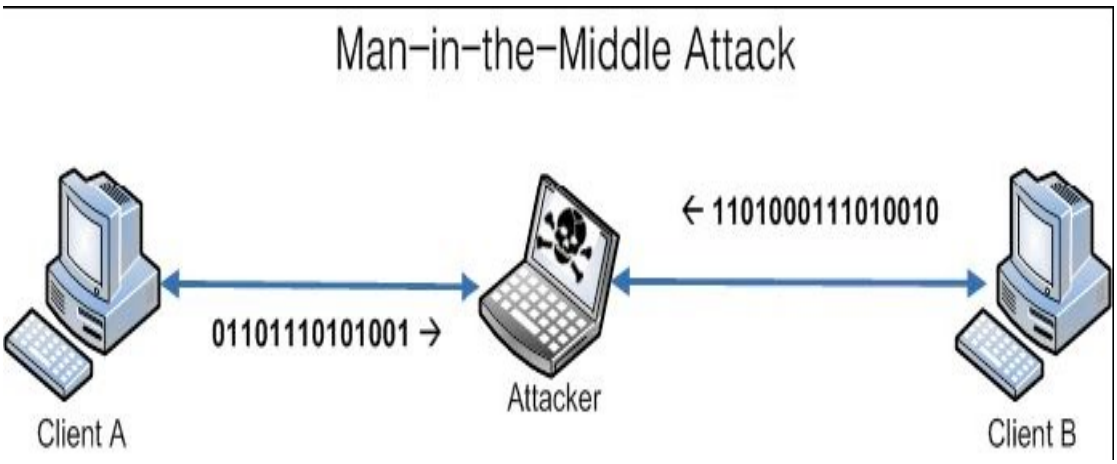
- Ifconfig
- Technetium Mac Address Changer (Windows)
- iproute2



Εικόνα: Υποκλοπή Ταυτότητας (MAC spoofing).

3.6 Man-in-the-middle ΕΠΙΘΕΣΕΙΣ

Πρόκειται για μια από τα συχνά είδη επιθέσεων στα ασύρματα τοπικά δίκτυα.Σε μια επίθεση Man-in-the-middle ο εισβολέας-επιτιθέμενος με την χρήση λογισμικού δημιουργεί-στήνει ένα δικό του σημείο πρόσβασης και συνδέεται επίσης σε ένα άλλο σημείο πρόσβασης με διαφορετική κάρτα δικτύου.Έτσι το υπολογιστικό σύστημα του υποκλοπέα επιτελεί τον ρόλο του ενδιάμεσου κόμβου με αποτέλεσμα η όλη ροή των συνδεδεμένων χρηστών σε αυτόν τον κόμβο να παρακολουθείται και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες.Το υπολογιστικό σύστημα του υποκλοπέα στην περίπτωση αυτή δεν φαίνεται στο χρήστη ο οποίος νομίζει ότι έχει συνδεθεί με το αρχικό σημείο πρόσβασης.Μια μορφή επίθεσης Man-in-the-middle βασίζεται σε σφάλματα και έλλειψη συγχρονισμού σε πρωτόκολλα χειραψίας που χρησιμοποιούνται στο δίκτυο όπως το πρωτόκολλο Diffie-Hellman,όταν η συμφωνία ανταλλαγής κλειδιών γίνεται χωρίς επικύρωση (authentication).

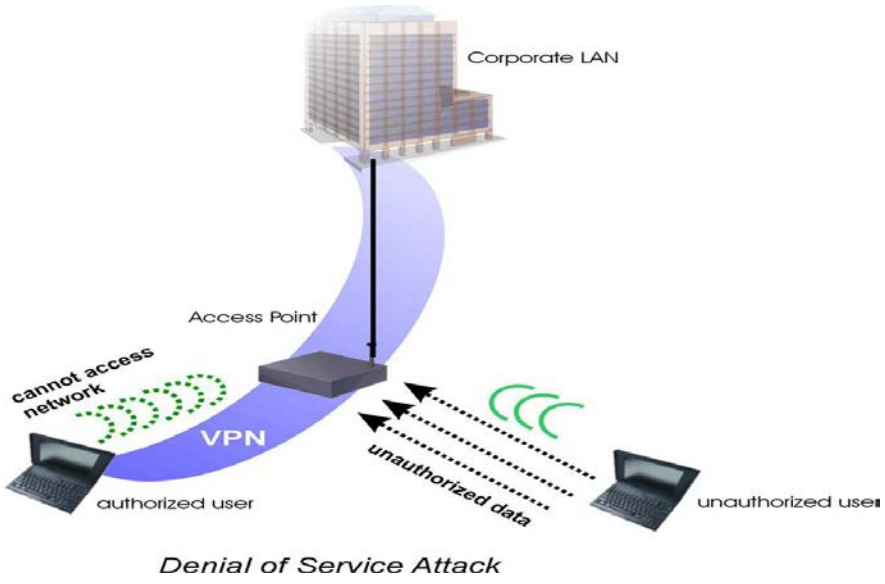


Εικόνα: Man-in-the-middle επίθεση.

Συγκεκριμένα η επίθεση αυτή οδηγεί το αληθές σημείο πρόσβασης να εγκαταλείψει τις συνδέσεις με τους χρήστες του και να επανασυνδέσει τους χρήστες με το ψεύτικό σημείο πρόσβασης AP.Στο διαδίκτυο υπάρχει αρκετό λογισμικό για την ενίσχυση των Man-in-the-middle επιθέσεων όπως το LANjack και το Airjacktα οποία αυτοματοποιούν και κατ' επέκταση διευκολύνουν πολλά βήματα της διαδικασίας.

3.7 ΆρνησηΥπηρεσίας (Denial of Service DoS attack).

Η άρνηση υπηρεσίας ή επίθεση DoS (Denial of Service) συμβαίνει όταν υποκλοπέας ή αλλιώς εισβολέας με συνεχείς αιτήσεις σύνδεσής, μηνύματα λάθους ή/και εντολές έλεγχου βομβαρδίζει συνεχώς ένα συγκεκριμένο σημείο πρόσβασης AP(Access Point) ή το δίκτυο.Ως αποτέλεσμα αυτής της επίθεσης είναι η υπερφόρτωση της λειτουργικότητας δικτύωσης του σημείου πρόσβασης AP.Έτσι δημιουργείται σημείο συμφόρησης στο AP και οι εξουσιοδοτημένοι (νόμιμοι) χρήστες δεν μπορούν να συνδεθούν στο δίκτυο και το αποτέλεσμα της επίθεσης είναι η κατάρρευση του δικτύου.Η επίθεση DoS δεν συμβάλει η ίδια σημαντικά στο να διαρρεύσουν οργανωτικά δεδομένα στον εισβολέα-επιτιθέμενο καθώς η κατάρρευση του διαδικτύου εμποδίζει τα δεδομένα να διαρρεύσουν και συμβάλλοντας στην πραγματικότητα έμμεσα προστατεύοντας τα από τα να μεταδοθούν.Ο συνήθης λόγος εκτέλεσης μιας επίθεσής DoS είναι να παρατηρήσουμε την ανάκτηση του ασύρματου δικτύου,όπου το σύνολο όλων των αρχικών κωδικών πρόσβασης χειραψίας αναμεταδίδονται από όλες τις συσκευές παρέχοντας έτσι στον κακόβουλο εισβολέα να τους καταγράψει και χρησιμοποιώντας διάφορα εργαλεία παραβίασης αναλύοντας την αδυναμίες ασφάλειας να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα.



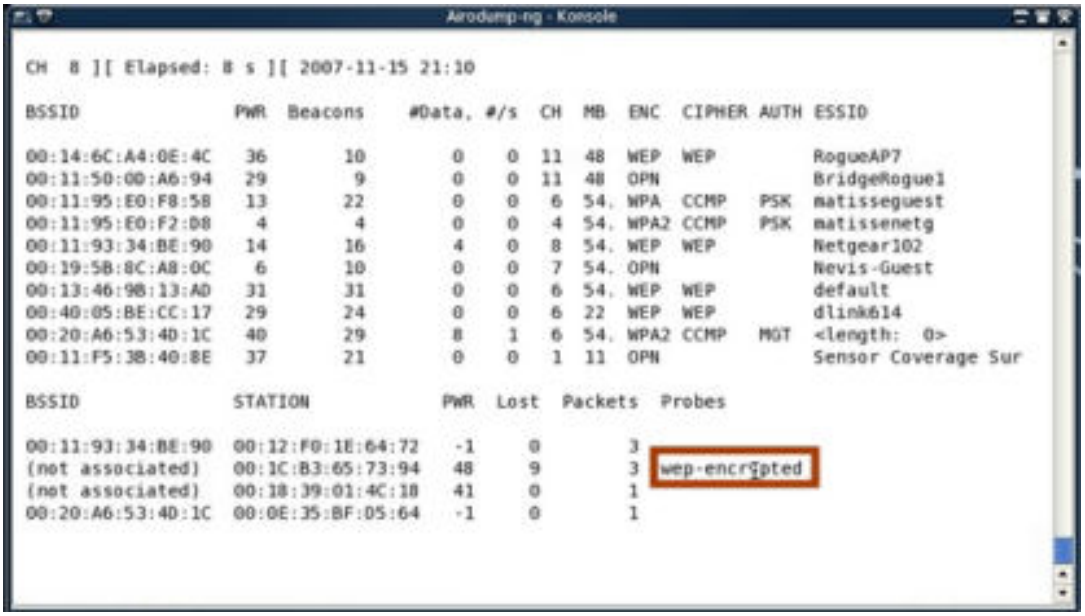
Εικόνα: Denial of Service DoS attack.

Η επίθεση αυτή λειτουργεί καλύτερα στην ασθενή κρυπτογράφηση των συστημάτων κρυπτογράφησης όπως το WEP που θα δούμε στην συνέχεια όπου ο εισβολέας

κάνοντας χρήση λογισμικού το οποίο παραβιάζει την κρυπτογράφηση καταφέρνει και αποκομίζει το κλειδί που χρησιμοποιείται από τους χρήστες του δικτύου κατά τη διάρκεια αποκατάστασης του δικτύου.Επίσης οι επιθέσεις αυτές βασίζονται στην κατάχρηση πρωτοκόλλων όπως το πρωτόκολλο ελέγχου ταυτότητας EAP (Extensible Authentication Protocol).Υπάρχουν δύο βασικές μορφές των επιθέσεωνDoS**:** οι υπηρεσίες συντριβή και ότι οι υπηρεσίες των πλημμυρών.

3.8 ΕΠΙΘΕΣΗCaffe-Latte

Η επίθεση Caffe-Latte είναι μια διαφορετική επίθεση η οποία μπορεί να νικήσει την κρυπτογράφηση WEP.Ο εισβολέας με την συγκεκριμένη επίθεση καταφέρνει να υποκλέψει το WEP κλειδί του δικτύου χωρίς όμως να βρίσκεται καν στο χώρο κάλυψης του δικτύου.Η επίθεση αυτή πραγματοποιείται με την χρήση λογισμικού το οποίο στοχεύει στο σύνολο των διαχειριστών ασύρματων δικτύων των λειτουργικών Windows.Έτσι με την χρήση της υπάρχουσας δικτύωσης το λογισμικό αυτό υποκλέπτει το κλειδί του WEP και παράλληλα το στέλνει στον υποκλοπέα.Ο υποκλοπέας στέλνοντας μια μεγάλη ροή κρυπτογραφημένων αιτήσεων ARP χρησιμοποιεί την ταυτότητα κοινόχρηστού κλειδιού (shared key authentication) καθώς και τα σφάλματα των μηνυμάτων ρύθμισης του WEP.Με την χρήση απόκρισης στις ARP αιτήσεις αποκτά σε πολύ λίγα λεπτά το κλειδί WEP.



Εικόνα: Επίθεση Caffe-Latte.

3.9 ΤΡΟΠΟΙ ΘΩΡΑΚΙΣΗΣ ΤΟΥ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

Για την θωράκιση ενός ασύρματου δικτύου υπάρχουν πολλές τεχνολογίες και τεχνικές οι οποίες μπορούν να χρησιμοποιηθούν για το σκοπό αυτό.Όμως παρόλα

αυτά δεν μπορεί καμία από αυτές τις τεχνολογίες και τις τεχνικές να παρέχει απόλυτη ασφάλεια.Έτσι η καλύτερη λύση είναι ο συνδυασμός αυτών των τεχνολογιών και των τεχνικών.Η ασφάλεια ενός ασύρματου δικτύου αποτελεί βασική παράμετρο που πρέπει να λάβει υπόψη του ο σχεδιαστής ενός ασύρματου δικτύου.Έτσι ο στόχος είναι η ασφάλιση του με διάφορους τρόπους σε διάφορα επίπεδα έτσι ώστε να είναι ιδιαίτερα δύσκολο έως ακατόρθωτο να προκληθεί βλάβη στο δίκτυο ή αν προκληθεί αυτή να είναι πολύ περιορισμένη.Η ασφάλεια παρέχεται από τον ολοκληρωμένο σχεδιασμό του δικτύου και του κάθε υπολογιστή ξεχωριστά υπολογίζοντας τα υπέρ και τα κατά σε κάθε επιλογή.Στην ασύρματη μετάδοση η πιο σοβαρή αδυναμία που την χαρακτηρίζει είναι ότι δεν μπορεί να παρεμποδιστεί εύκολα η φυσική πρόσβαση στο μέσο,λόγω της ασύρματης φύσης του ασύρματου δικτύου.Αποτέλεσμα αυτού είναι κάποιος ο οποίος είναι εφοδιασμένος με το κατάλληλο υλικό και λογισμικό να έχει την δυνατότητα να συλλέξει ικανό αριθμό πακέτων που μεταδίδονται ανάμεσα στους σταθμούς του ασύρματου δικτύου κατά την διάρκεια της ασύρματης επικοινωνίας μεταξύ τους.Επίσης με τον τρόπο αυτό μπορεί να υποκλέψει την πληροφορία που μεταδίδεται ακόμη και όταν αυτή είναι κρυπτογραφημένη με κάποιο αδύναμο αλγόριθμό.Ακόμη μπορεί να επιχειρήσει να συνδεθεί ο ίδιος στο ασύρματο δίκτυο με σκοπό την υποκλοπή πληροφορίας ή την κακόβουλη χρήση.Παρακάτω παρατίθενται διάφορες μέθοδοι θωράκισης του ασύρματου δικτύου.

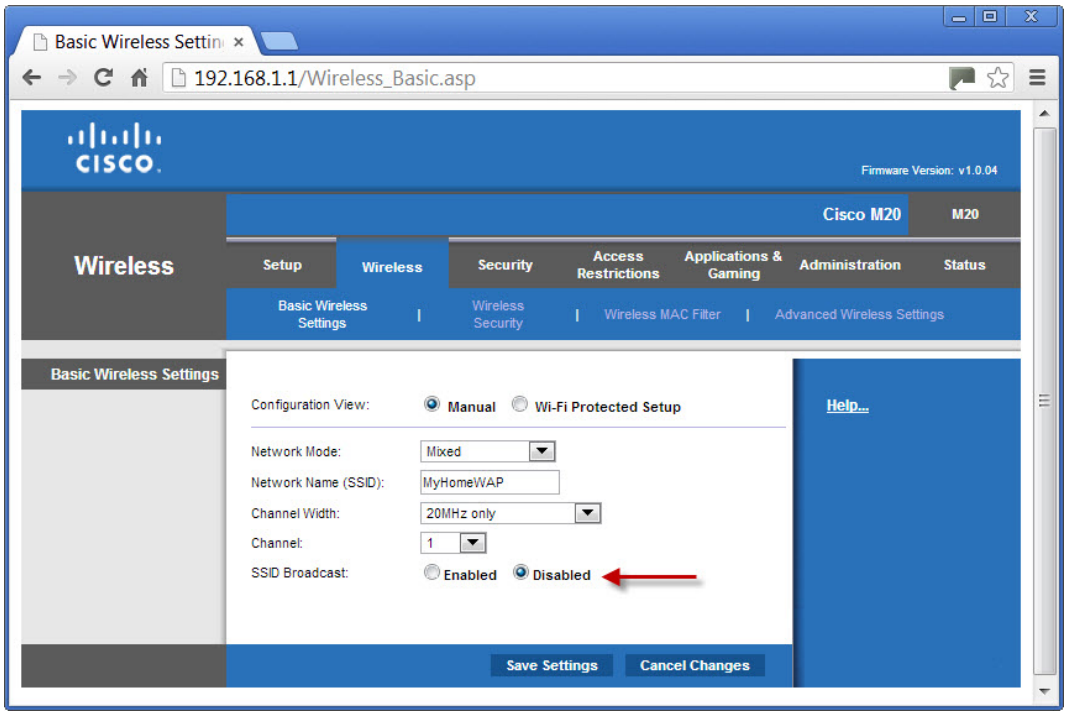
3.9.1 Η ΣΗΜΑΣΊΑ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Το λειτουργικό σύστημα των υπολογιστικών συστημάτων τα οποία χρησιμοποιούνται σε μια ασύρματη δικτύωση αποτελεί βασική παράμετρο ασφάλειας του ασύρματου δικτύου.Τα MicrosoftWindows λόγω της μεγάλης διάδοσής τους και του κλειστού κώδικα τους καθίστανται ιδιαίτερα ευάλωτα σε επιθέσεις και διαπιστώνονται κενά ασφαλείας.Έτσι για την αντιμετώπιση των επιθέσεων θα πρέπει να γίνεται διαρκής ενημέρωση του λειτουργικού συστήματος,ο περιορισμός των υπηρεσιών που μόνο πραγματικά χρησιμοποιούνται και εγκατάσταση κάποιου προγράμματος προστασίας από ιούς antivirus (για την περίπτωση εγκατάστασης κακόβουλου λογισμικού).Τέλος η χρήση κάποιου firewall τείχους προστασίας το οποίο μπορεί να απορρίψει δεδομένα που προέρχονται από άγνωστη πηγή ή αρχεία που αντιστοιχούν σε μία συγκεκριμένη πηγή,όπως ιούς ή μπορεί επίσης να επιτρέπει τη διέλευση όλων των δεδομένων προς το διαδίκτυο και να επιτρέπει τη διέλευση μόνο ορισμένων δεδομένων από το διαδίκτυο.Η πιο συνηθισμένη χρήση ενός firewall είναι στην πύλη μεταξύ των ασύρματων σημείων πρόσβασης και του ενσύρματου δικτύου.Έτσι απομονώνει το ασύρματο κομμάτι από το ενσύρματο κομμάτι του LAN,έτσι ώστε εισβολείς που έχουν συνδέσει τον υπολογιστή τους στο δίκτυο χωρίς άδεια να μην μπορούν να χρησιμοποιήσουν την ασύρματη σύνδεση για να μπουν στο διαδίκτυο ή στο ενσύρματο κομμάτι του LAN,δίνοντας έτσι κάποια ικανοποιητική ασφάλεια.Στο περιβάλλον Linux ή BSD τα οποία είναι βασισμένα στο Unix,λόγω της σχεδίασης τους η ασφάλεια μπορεί να φτάσει στο καλύτερο δυνατό επίπεδο.Το ίδιο ισχύει και για το λειτουργικό σύστημα Mac OSX.

3.9.2 SSID ΚΑΙ ΑΠΟΚΡΥΨΗ

Κάθε ασύρματο δίκτυο έχει ένα όνομα.Σε ένα δίκτυο με ένα μόνο σημείο πρόσβασης, το όνομα είναι το βασικό σύνολο υπηρεσιών ID (BSSID).Σε περίπτωση που το δίκτυο έχει περισσότερα σημεία πρόσβασης, το όνομα γίνεται επεκταμένο σύνολο υπηρεσιών ID (ESSID).Για όλα τα ονόματα δικτύων το αρχικό καθορισμένο όνομα είναι το SSID και είναι ο πιο συχνά συναντημένος όρος σε προγράμματα ρύθμισης σημείων πρόσβασης.Όταν ρυθμίζεται το σημείο πρόσβασης ενός δικτύου πρέπει να καθοριστεί το SSID για αυτό το συγκεκριμένο δίκτυο.Κάθε σημείο πρόσβασης και πελάτης δικτύου πρέπει να χρησιμοποιούν το ίδιο SSID.Όταν οι υπολογιστές χρησιμοποιούν το λειτουργικό σύστημα Windowsπρέπει το SSID να είναι το ίδιο και με το όνομα της ομάδας εργασίας στην οποία ανήκει αυτός ο υπολογιστής.Όταν δυο η περισσότερα σημεία πρόσβασης με το ίδιο SSID ανιχνευτούν από ένα δίκτυο τότε υποθέτει ότι είναι και τα δύο μέρος του ίδιου δικτύου (ακόμη και αν τα σημεία πρόσβασης λειτουργούν σε διαφορετικά κανάλια) και πραγματοποιεί σύνδεση με το σημείο πρόσβασης που παρέχει το δυνατότερο ή καθαρότερο σήμα.Αν λόγω παρεμβολών το σήμα αυτό εξασθενήσει,ο πελάτης θα προσπαθήσει να συνδεθεί σε άλλο σημείο πρόσβασης του δικτύου αυτού.Αν τώρα δύο διαφορετικά δίκτυα με επικαλυπτόμενα σήματα έχουν το ίδιο όνομα,ένα πελάτης θα υποθέσει ότι ανήκουν στο ίδιο δίκτυο, και ίσως προσπαθήσει να πραγματοποιήσει ένα handoff από το ένα δίκτυο στο άλλο με αποτέλεσμα από την πλευρά του χρήστη αυτό το λανθασμένο handoff θα φανεί σαν ¨πέσιμο¨ της σύνδεσης.Γι’ αυτό, κάθε ασύρματο δίκτυο που θα μπορούσε να επικαλύπτεται από ένα άλλο πρέπει να έχει μοναδικό SSID.Τα δημόσια και κοινοτικά δίκτυα αποτελούν ένα κανόνα εξαίρεση του μοναδικού SSID παρέχουν πρόσβαση μόνο στο διαδίκτυο,αλλά όχι σε άλλους υπολογιστές ή συσκευές σε ένα LAN.Αυτά τα δίκτυα συχνά έχουν ένα κοινό SSID,έτσι ώστε οι συνδρομητές να μπορούν να τα ανιχνεύουν και να συνδέονται σε αυτά από διάφορες τοποθεσίες. Κάποια σημεία πρόσβασης προσφέρουν την επιλογή μεταξύ ανοιχτής και κλειστής πρόσβασης.Όταν το σημείο πρόσβασης είναι σε λειτουργία ανοιχτής πρόσβασης,θα δεχτεί τη σύνδεση με ένα πελάτη που το SSID του είναι ¨ANY¨,αλλά και με συσκευές ρυθμισμένες στο SSID του σημείου πρόσβασης.Όταν είναι ρυθμισμένο σε λειτουργία κλειστής πρόσβασης,δέχεται συνδέσεις μόνο με συσκευές που το SSID τους είναι το ίδιο με το δικό του SSID.Αυτός είναι ένας καλός τρόπος για να κρατήσει κανείς κάποιους εισβολείς εκτός του δικτύου του,αλλά λειτουργεί μόνο αν κάθε συσκευή του δικτύου χρησιμοποιεί έναν αντάπτορα Orinoco.Το SSID ενός δικτύου προσφέρει μια πολύ περιορισμένη μορφή ελέγχου πρόσβασης, γιατί είναι απαραίτητος ο προσδιορισμός του SSID όταν στήνουμε μια ασύρματη σύνδεση.Η επιλογή SSID σε ένα σημείο πρόσβασης δέχεται οποιοδήποτε όνομα θελήσουμε να ορίσουμε,αλλά πολλά προγράμματα ρύθμισης δικτύου ανιχνεύουν αυτόματα τα SSID όλων των δικτύων της περιοχής τους.Οπότε δεν είναι απαραίτητο συνήθως να ξέρουμε το SSID ενός δικτύου εκ των προτέρων για να προσπαθήσουμε να συνδεθούμε σε αυτό.Κάθε σημείο πρόσβασης έχει εξαρχής ένα SSID το οποίο είναι συνήθως το ίδιο και γνωστό στα σημεία πρόσβασης που παράγει μια εταιρεία π.χ. Cosmote.Οπότε ποτέ δε θα πρέπει να χρησιμοποιείται το εργοστασιακό SSID μιας συσκευής δικτύου.Πολλά

σημεία πρόσβασης έχουν την επιλογή το SSID να είναι κρυφό.Έτσι εμποδίζει πολλούς να ανιχνεύσουν το δίκτυο,αλλά και πάλι κάθε φορά που ένας νέος πελάτης συνδέεται στο δίκτυο εκπέμπεται το SSID του δικτύου με ασθενές σήμα το οποίο ανιχνεύεται όμως από λογισμικό όπως το Kismet.Έτσι η απόκρυψη του SSID μπορεί να δημιουργήσει μεγαλύτερη δυσκολία σε κάποιον που θέλει να μπει στο δίκτυο αλλά δεν προσφέρει τελικά ουσιαστική προστασία.



Εικόνα: Απόκρυψη SSIDτου δικτύου.

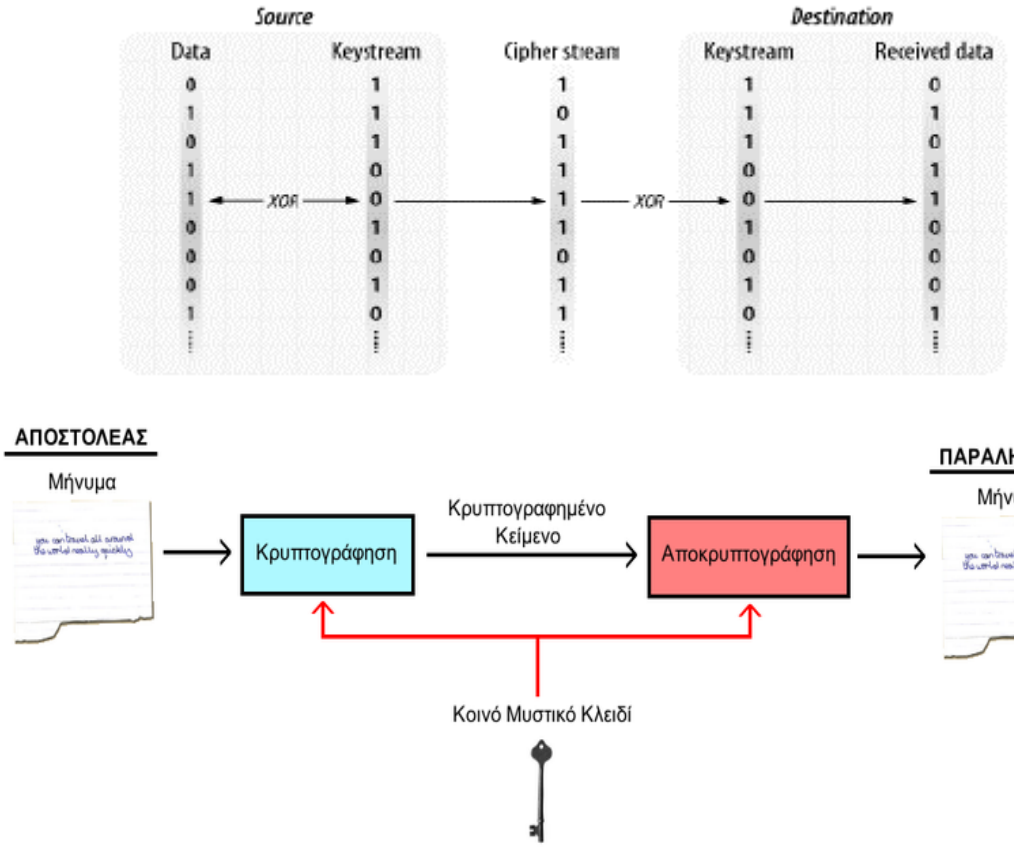
3.9.3 ΧΡΗΣΗ ΣΤΑΤΙΚΗΣ ΔΙΕΥΘΥΝΣΙΟΔΟΤΗΣΗΣ

Η απενεργοποίηση του DHCP (Dynamic Host Configuration Protocol) server του δρομολογητή του ασύρματου δικτύου παρέχει μια σχετική υποτυπώδη ασφάλεια.Σε καμία περίπτωση όμως η ασφάλεια αυτή δεν είναι η θωράκιση του δικτύου όμως καταφέρνει να αντιμετωπίσει σε πολλές περιπτώσεις απλούς εισβολείς ή κατά λάθος εισβολείς από την είσοδο τους στο δίκτυο μας.

3.9.4 ΧΡΗΣΗ ΤΟΥ WEP (Wired Equivalent Privacy)

Το πρωτόκολλοWEP (Wired Equivalent Privacy) δημιουργήθηκε από την επιτροπή IEEE 802.11 για λόγους ασφάλειας των χρηστών από διάφορές επιθέσεις κακόβουλων εισβολέων και πιστοποίησης (authentication) των χρηστών με σκοπό την εμπιστευτικότητα των πακέτων των δεδομένων από λαθροακρόαση-υποκλοπές eavesdroppingπου είναι ένα γνωστό πρόβλημα στους χρήστες όλων των τύπων ασύρματων τεχνολογιών για την επίτευξη ασφάλειας παρόμοιας με το ασύρματο

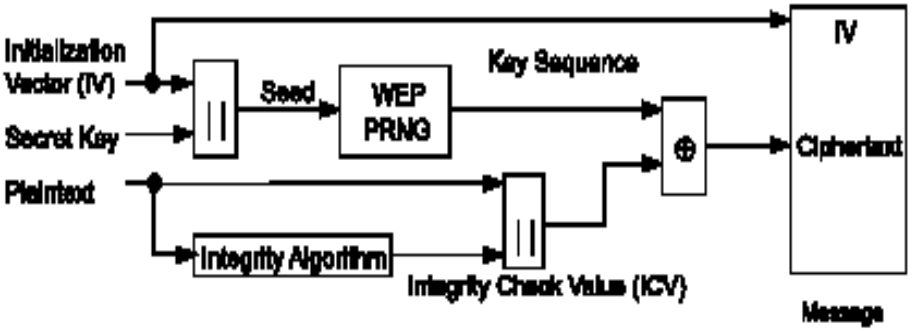
δίκτυο.Η εμπιστευτικότητα των δεδομένων εξαρτάται από μια εξωτερική υπηρεσία διαχείρισης κλειδιού η οποία διανέμει τα κλειδιά κρυπτογράφησης-αποκρυπτογράφησης των δεδομένων.Για την προστασία των δεδομένων το WEP χρησιμοποιεί τον αλγόριθμό κρυπτογράφησης RC4 (RC4 cipher) ο οποίος είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας ¨μυστικού κλειδιού¨ χρησιμοποιώντας μια ακολουθία από bitsπαράγει μια ακολουθία bit κλειδιού keystream.Από το συνδυασμό του keystream με το μήνυμα παράγεται το κρυπτογράφημα (ciphertext) και για τον συνδυασμό μεταξύ των δύο ο RC4 χρησιμοποιεί το αποκλειστικό Η (XOR).Για την ανάκτηση του αρχικού μνήματος ο δέκτης θα πρέπει να επεξεργαστεί το κρυπτογράφημα με το ίδιο keystream.Το keystream παράγεται από ένα μικρό σχετικά μυστικό κλειδί (secret key) το οποίο επεκτείνεται με μήκος ίδιο με του μηνύματος. Την λειτουργία αυτή την αναλαμβάνει η ψευδοτυχαία γεννήτρια αριθμού (PRNG) η οποία είναι ένα σύνολο κανόνων που χρησιμοποιούνται για να επεκταθεί το μυστικό κλειδί σε keystream.Έτσι για να ανακτήσουν τα δεδομένα θα πρέπει να μοιραστούν το ίδιο μυστικό κλειδί και οι δυο πλευρές αποστολέας-δέκτης και να χρησιμοποιούν τον ίδιο αλγόριθμο για να επεκτείνουν το κλειδί σε μια ψευδοτυχαία ακολουθία.Το πιο σημαντικό στοιχείο της κρυπτογράφησης είναι η παραγωγή του keystream από το secret key.Η διαδικασία πρέπει να παράγει όσο τον δυνατόν πιο τυχαίες ακολουθίες keystream.Το τυχαίο keystream ονομάζεται on-timepand.Παρακάτω στην εικόνα φαίνεται η διαδικασία αυτή.



Εικόνα: Λειτουργία κρυπτογράφησης-αποκρυπτογράφησης.

Το WEP για την προστασία από ισχυρές επιθέσεις αποκρυπτογράφησης χρησιμοποιεί ένα σύνολο μέχρι τεσσάρων προεπιλεγμένων κλειδιών και όταν επιτρέπεται μπορεί επίσης να χρησιμοποιήσει κλειδιά ζευγών (pairwise),αποκαλούμενα χαρτογραφημένα κλειδιά.Τα προεπιλεγμένα κλειδιά μοιράζονται μεταξύ όλων των σταθμών σε ένα σύνολο υπηρεσιών.Έτσι ένας σταθμός μόλις λάβει τα κλειδιά προεπιλογής για το σύνολο υπηρεσιών του μπορεί να επικοινωνήσει με τη χρησιμοποίηση WEP.Η επαναχρησιμοποίηση κλειδιών είναι συχνά μια αδυναμία των κρυπτογραφικών πρωτοκόλλων.Το WEP για αυτόν τον λόγο έχει μια δεύτερη κατηγορία κλειδιών που χρησιμοποιούνται για pairwise επικοινωνίες.Τα κλειδιά μοιράζονται μόνο μεταξύ της επικοινωνίας δύο σταθμών.Έτσι οι δύο σταθμοί που μοιράζονται ένα κλειδί έχουν μια σχέση χαρτογράφησης κλειδιού.Το μήκος των κλειδιών κρυπτογράφησης που χρησιμοποιούνται στην κρυπτογράφηση WEPείναι 40 ή 104 bitsστα Access Pointsκαι στους σταθμούς για αμοιβαία επικύρωση ωστόσο συχνά αναφέρονται για 64 ή 128 bitsδιότι παραλείπεται να αναφερθούν τα 24 επιπλέον bitsπου χρησιμοποιούνται από το διάνυσμα αρχικοποίησης IV (Initialization Vector).ToIV για κάθε πακέτο ουσιαστικά αλλάζει και συνδυάζεται με το μυστικό κλειδί και το αποτέλεσμα αυτών των δυο κρυπτογραφείται.Ετσι αν και τα αρχικά δεδομένα είναι ίδια η κρυπτογραφημένη μορφή τους είναι διαφορετική.Επίσης το IV δεν είναι μυστικό,ενώ σε κάθε μετάδοση στέλνεται σε μη κρυπτογραφημένη μορφή ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή IV.Στην επικύρωση θα πρέπει η συσκευή να αποδείξει στο σημείο πρόσβαση AccessPoint ότι γνωρίζει τον μυστικό κλειδί της κρυπτογράφησης.Αρχικά στέλνεται αίτηση επαλήθευσης ταυτότητας προς το σημείο πρόσβασης από την ασύρματη συσκευή (π.χ.laptop,κινητό τηλέφωνο).Στην συνέχεια το σημείο πρόσβασης στέλνει έναν τυχαίο αριθμό μήκους 128 bit προς κρυπτογράφηση στην ασύρματη συσκευή.Ο αριθμός κρυπτογραφείται από τη συσκευή με το μυστικό κλειδί WEP και αποστέλλεται πίσω.Ωστόσο η μέθοδος αυτή αποτελεί πολύ μεγάλο πρόβλημα για την ασφάλεια της κρυπτογράφησης καθώς παρέχει πληροφορίες σε κακόβουλους χρήστες, που παρακολουθούν την επικοινωνία τόσο της κρυπτογραφημένης αλλά και της μη κρυπτογραφημένης πληροφορίας.Η λύση στο πρόβλημα αυτό δόθηκε με την χρήση και υιοθέτηση τωνVPN (Virtual Private Network) και των RADIUS server (Remote Authentication Dial-in User Services),που αρχικά σχεδιάστηκαν για να επικυρώνουν συνδέσεις dial-upμεταξύ modems.Τέλος το σημείο πρόσβασης ελέγχει εάν η κρυπτογράφηση έγινε με το σωστό κλειδί. Οι πιο κοινές εφαρμογές WEP χρησιμοποιούν κοινά κλειδιά RC4 64bit,όπου τα 40 από τα 64 είναι ένα δημόσιο μυστικό.Το όνομα του τυποποιημένου WEP είναι γνωστό ως ¨40 bit WEP¨ή και ακόμα ¨64 bit WEP¨.Το μεγαλύτερο μέρος της βιομηχανίας έχει κινηθεί στο 128-bitδημόσιο RC4 κλειδί όπου τα 24 από τα 128 bitείναι ένα δημόσιο μυστικό.Ακόμα κι αν μόνο 104 bit είναι μυστικά,οι προμηθευτές αναφέρονται σε αυτό ως ¨128-bit WEP¨.Κατά την διαδικασία της κρυπτογράφησης πρώτα από όλα το μυστικό κλειδί συνδέεται με ένα διάνυσμα έναρξής (IV) και το αποτέλεσμα στέλνεται σε ένα PRNG. Ο PRNG παράγει μια ακολουθία κλειδιού keystreamαπό ψευδοτυχαίαbitsίσα στο μήκος με τον αριθμό των bitsτων δεδομένων που πρέπει να διαβιβαστούν συν 4(δεδομένου ότι η ακολουθία κλειδιού χρησιμοποιείται για να προστατεύσει την τιμή ελέγχου ακεραιότητας (Integrity Check Value ICV) καθώς επίσης και τα δεδομένα).Έπειτα για προστασία από αναρμόδια τροποποίηση των δεδομένων χρησιμοποιείται ένας αλγόριθμός ακεραιότητας επάνω στα δεδομένα που δεν κρυπτογραφούνται και παράγεται το ICV.Έτσι το προϊόν της διαδικασίας είναι ένα μήνυμα που περιέχει το IV και το κρυπτογράφημα (ciphertext).Ο PRNG δεδομένου ότι μετασχηματίζει ένα σχετικά σύντομο μυστικό

κλειδί σε μια αυθαίρετα μακροχρόνια ακολουθία κλειδιού είναι το κρίσιμο συστατικό αυτής της διαδικασίας.Αυτή η μέθοδος απλοποιεί πολύ την διαδικασία διανομής κλειδιού,καθώς μόνο το μυστικό κλειδί πρέπει να μεταδοθεί μεταξύ των σταθμών STAs.Το διάνυσμα IV επεκτείνει την διάρκεια ζωής του μυστικού κλειδιού και παρέχει την ιδιότητα αυτοσυγχρονισμού του αλγορίθμου,ενώ οι IV αλλάζουν περιοδικά το μυστικό κλειδί παραμένει σταθερό.Κάθε νέο IV καταλήγει σε μια νέα ακολουθία κλειδιού.Δεδομένου ότι το IV ταξιδεύει με το μήνυμα,μπορεί να αλλάξει τόσο συχνά όσο κάθε MPDU(Mac Protocol Data Unit) και ο δέκτης θα είναι σε θέση πάντα να αποκρυπτογραφήσει οποιοδήποτε μήνυμα.Το IV διαβιβάζεται χωρίς ασφάλεια αφού δεν παρέχει σε έναν επιτιθέμενο οποιεσδήποτε πληροφορίες για το μυστικό κλειδί και δεδομένου ότι η τιμή του πρέπει να μαθευτεί από τον παραλήπτη προκειμένου να εκτελεσθεί η αποκρυπτογράφηση.Για την αποκρυπτογράφηση θα πρέπει να σταλεί μήνυμα το οποίο θα περιέχει το διάνυσμα αρχικοποίησης IV μαζί με το κρυπτογραφημένο πακέτο.Ο IV του εισερχόμενου μηνύματος θα χρησιμοποιηθεί για να παράγει τη ακολουθία κλειδιού που είναι απαραίτητη για να αποκρυπτογραφηθεί το εισερχόμενο πακέτο.Στην συνέχεια συνδυάζοντας την κατάλληλη ακολουθία κλειδιού με το κρυπτογραφημένο κείμενο παράγεται το αρχικό κείμενο(plaintext) και ο ICV.Με την χρήση του αλγορίθμου CRC-32 ελέγχου ακεραιότητας θα ελεγχθεί το ανακτημένο πακέτο συγκρίνοντας το παραγόμενο ICV΄ με το ICV που διαβιβάζεται με το μήνυμα.Εάν το ICV΄ είναι ίδιο με το ICV,τότε το πακέτο είναι έγκυρο και ο σταθμός μεταφέρει το MACστο LLC.Εάν το ICV’ δεν είναι ίδιο με το ICV, η λαμβανόμενη MPDU είναι λάθος και μια ένδειξη λάθους στέλνεται στη διαχείριση MAC.MSDUs με λανθασμένες MPDUs(λόγω της ανικανότητας αποκρυπτογράφησης) δεν θα περάσουν στο LLC (επίπεδο 2 του OSI).



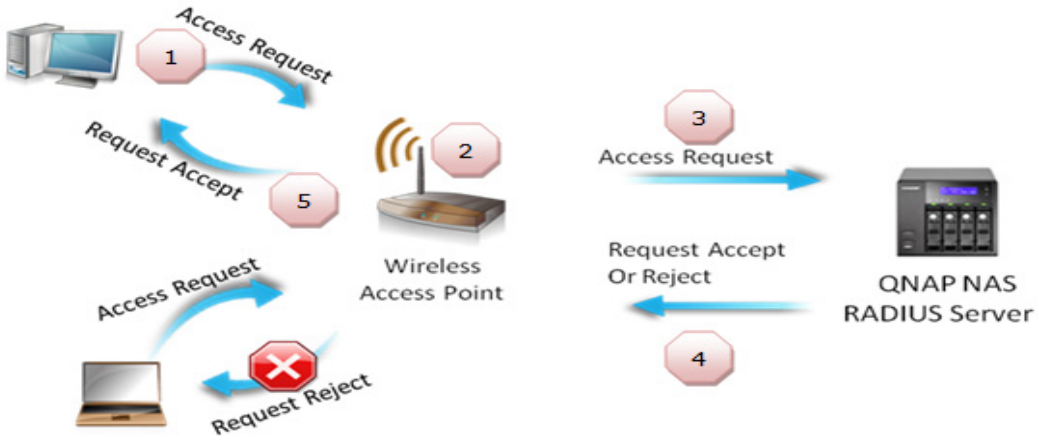
Εικόνα: Μπλοκ διάγραμμα WEP κρυπτογράφησης.

3.9.5 ΧΡΗΣΗ ΤΟΥ WPA (Wi-Fi Protected Access)

Το πρωτόκολλο Wi-Fi Protected Access (WPA) δημιουργήθηκε από την Wi-Fi Alliance με σκοπό να καλύψει το κενό ασφάλειας που άφηνε η WEP κρυπτογράφηση.Το WPA προέρχεται από το IEEE 802.11 και είναι σχεδιασμένο για να εξασφαλίσει όλες τις εκδόσεις 802.11 συσκευών,καθώς και υποσύνολο του 802.11i γνωστό ως WAP2 που θα δούμε πιο κάτω.Ο WPA προσφέρει ευελιξία και ευκολία μεταξύ των χρηστών καθώς και να εργάζονται ασύρματα και ασφαλές χωρίς την ανάπτυξή πρόσθετων λύσεων ασφάλειας όπως VPNs.Το WPAγια την κρυπτογράφηση χρησιμοποιεί τονRC4 όπως και τοWEP,καθώς και το πρωτόκολλο ακεραιότητας προσωρινού κλειδιού TKIP (Temporal Key Integrity Protocol),το οποίο

αυξάνει το μέγεθός του κλειδιού από 40 σε 128 bit αντικαθιστώντας έτσι το ενιαίο στατικό κλειδί WEP με κλειδιά τα οποία παράγονται δυναμικά και διανέμονται από τον κεντρικό υπολογιστή επικύρωσης (RADIUS),κάνοντας έτσι πλέον σχεδόν αδύνατη την εύρεση του.Το χαρακτηριστικό αυτό σε συνδυασμό με το ότι το IVείναι διπλάσιο σε μήκος δηλαδή 48 bit προσφέρει μια βελτιωμένη ασφάλεια κυρίως από επιθέσεις ανάκτησης κλειδιών brute-forceαπό τις οποίες οWEPυπέφερε λόγω του μικρού μήκους 24 bitτου IVτου.Έτσι αρχικοποιεί τον αποστολέα και τον παραλήπτη με κάθε νέο κλειδί και ένας νέος χώρος καταλαμβάνεται για την χρήση το κλειδιού που έχει δοθεί.Το TKIP χρησιμοποιεί για την επικύρωση το πρότυπο 802.1X το οποίο περιέχει μηχανισμούς πιστοποίησης ταυτότητας και εξουσιοδότησης των κόμβων του δικτύου,μαζί με την χρήση ενός πρωτοκόλλου ελέγχου ταυτότητας γνωστό ως EAP (Extensible Authentication Protocol).Με το 802.1X ουσιαστικά παρέχεται έλεγχος ταυτότητας μεταξύ του πελάτη και ενός διακομιστή RADIUS (Remote Authentication Dial-In User Service) που είναι συνδεδεμένος στο σημείο πρόσβασης. Έτσι στην επικύρωση όταν ένας χρήστης ζητήσει πρόσβαση στο δίκτυο τα πιστοποιητικά του χρήστη στέλνονται στον κεντρικό υπολογιστή επικύρωσης μέσω του AP.Αν ο κεντρικός υπολογιστής δεχτεί τα πιστοποιητικά του χρήστη,το κύριο κλειδί TKIP στέλνεται στο χρήστη και στο AP.Έτσι με την διαδικασία χειραψίας four-way στην οποία ο χρήστης και το AP αναγνωρίζουν ο ένας το άλλο και εγκαθιστούν τα κλειδιά ολοκληρώνοντας την διαδικασία.Το WPA επιπλέον χρησιμοποιεί αντί του CRC που χρησιμοποιούνταν στο WEP χρησιμοποιεί έναν μηχανισμό ακεραιότητας μηνυμάτων MIC (Message Integrity Check) γνωστό και ως Michaelμε σκοπό να βελτιώσει την ακεραιότητα των στοιχείων προστατεύοντας από τις παραποιήσεις πακέτων χρησιμοποιώντας τους αλγορίθμους Hash. Επιπλέον το MIC παρέχει έναν μετρητή πλαισίου έτσι ώστε να αντιμετωπίζονται οι επιθέσεις επαναλαμβανόμενης προσπάθειας εισβολής.Όσον αφορά τους οικιακούς χρήστες το WPA παρέχει έναν μηχανισμό προ-μοιρασμένου κλειδιού τον PSK (Pre-Shared Key).Αυτός ο μηχανισμός αυθεντικότητας είναι για οικιακή και μικρές επιχειρήσεις χρήση.Δεν απαιτείται η χρήση ενός διακομιστή αυθεντικότητας.Στον μηχανισμό αυτόν εισάγεται μια λέξη κωδικός και στο σημείο πρόσβασης(AP)και στο σταθμό(STA).Η λέξη κωδικός χρησιμοποιείται για να επικυρώνει οποιονδήποτε σταθμό προσπαθεί να συνδεθεί στο συγκεκριμένο δίκτυο και θα πρέπει να αποτελείται από 8 έως 63 χαρακτήρες σε ASCII.Ακολούθως το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα.Το256 bit κλειδί υπολογίζεται χρησιμοποιώντας τη hash συνάρτηση PBKDF2 χρησιμοποιώντας τον αρχικό κωδικό ως κλειδί.Για την προστασία από μια επίθεση ένας αληθινά τυχαίος κωδικός 13 χαρακτήρων είναι πιθανώς αρκετός.Τα προϊόντα που γράφουν ότι έχουν ¨WPA-Personal¨ σημαίνει ότι υποστηρίζουν τον PSK μηχανισμό επικύρωσης. Επίσης το WPA ορίζει τη χρήση του προτύπου AES (Advanced Encryption Standard) ως επιπλέον αντικατάσταση για την κρυπτογράφηση WEP.Επειδή ίσως να μην είναι δυνατή η προσθήκη υποστήριξης AES μέσα από ενημερωμένη έκδοση υλικού του λογισμικού σε υπάρχον ασύρματο εξοπλισμό,η υποστήριξη προτύπου AES είναι προαιρετική και εξαρτάται από την υποστήριξη που παρέχει ο προμηθευτής (π.χ. η Microsoft,η Cisco κλπ),όσον αφορά προγράμματα

οδήγησης.Κατά την διάρκεια της κρυπτογράφησης το TKIP χρησιμοποιεί μια μεθοδολογία ιεραρχίας κλειδιού και διαχείρισης κλειδιών δυναμώνοντας το πλαίσιο 802.1X/EAP δυσκολεύοντας έτσι τους εισβολείς να εκμεταλλευτούν το κλειδί.Έπειτα ο κεντρικός υπολογιστής ο οποίος θα δεχτεί τα πιστοποιητικά ενός χρήστη θα χρησιμοποιήσει το 802.1X για να παράγει ένα μοναδικό κύριο κλειδί master key ή ένα ζεύγος κλειδιών pair-wise.Το κλειδί αυτό ο TKIP το διανέμει στο χρήστη και στο AP.Παράγει δυναμικά τα μοναδικά κλειδιά κρυπτογράφησης δεδομένων χρησιμοποιώντας topair-wise κλειδί,για την κρυπτογράφηση κάθε πακέτου δεδομένων που επικοινωνούν ασύρματα κατά την διάρκεια της συνόδου του χρήστη.Το ενιαίο στατικό κλειδί του WEPανταλλάσσεται από την ιεραρχία κλειδιού TKIP για 300 τρισεκατομμύρια περίπου κλειδιά τα οποία μπορούν να χρησιμοποιηθούν σε ένα δεδομένο πακέτο δεδομένων.Έπειτα ο έλεγχός ακεραιότητας μηνυμάτων MICπαρέχει στον δέκτη και στον αποστολέα να υπολογίζουν και να συγκρίνουν ο καθένας μέσω του κρυπτογραφικού αλγορίθμου Michael την τιμή των MIC.Με τον αλγόριθμο αυτό προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και παραλήπτη.Έτσι αν οι τιμές ταιριάζουν συνεχίζεται η ανταλλαγή πακέτων και οι μεταξύ τους επικοινωνία,αλλιώς αν οι τιμές δεν ταιριάζουν,τότε υποτίθεται ότι τα δεδομένα έχουν τροποποιηθεί και έτσι το πακέτο διαγράφεται.Έτσι ο TKIP με τον μηχανισμό MIC την μεγάλη επέκταση στο μέγεθός των κλειδιών όπως προαναφέρθηκε πιο πάνω από 40 σε 128 και τον αριθμό των κλειδιών αυτών σε χρήση καθιστά πολύπλοκή και δύσκολη την αποκωδικοποίηση των δεδομένων σε ένα Wi-Fiδίκτυο.Έτσι η πολυπλοκότητα της ασύρματης δικτύωσης καθιστά πολύ δύσκολη εάν όχι αδύνατη την είσοδο για έναν κακόβουλο εισβολέα σε ένα δίκτυο Wi-Fi.



Εικόνα: Η κρυπτογράφηση WAP με χρήση RADIUS εξυπηρετητή για προστασία ασφάλειας δικτύου.

3.9.6 ΦΙΛΤΡΟ MAC ΔΙΕΥΘΥΝΣΕΩΝ

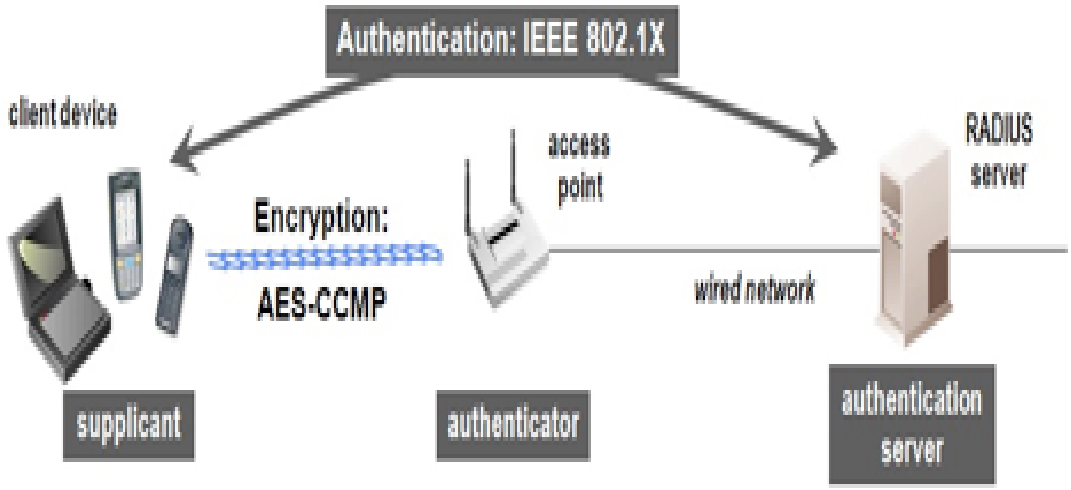
Όπως προαναφέρθηκε η λειτουργία του πρωτοκόλλου WEP πιστοποιεί τον χρήστη στο AP και όχι την συσκευή. Έτσι για την πιστοποίηση της προστίθενται στο AP

φίλτρα σχετικά με τις MAC διευθύνσεις των συσκευών οι οποίες καθορίζουν ποιες συσκευές επιτρέπεται να συνδεθούν και ποιες όχι.Η διαλειτουργικότητα αυτή παρέχεται από τις περισσότερες συσκευές οι οποίες κυκλοφορούν στο εμπόριο.Μια MAC διεύθυνση όπως έχει προαναφερθεί είναι ένας μοναδικός δεκαεξαδικός αριθμός ο οποίος βρίσκεται αναγραφόμενος στο υλικό κάθε δικτυακής συσκευής π.χ. ένα ασύρματο router.Έτσι δίνεται η δυνατότητα στο χρήστη να δηλώσει ρητά τις συσκευές στις οποίες επιτρέπει την συνδεσιμότητα και τις συσκευές στις οποίες δεν την επιτρέπει.Το Access Point εμπεριέχει μια λίστα με όλες τις διευθύνσειςMAC τις οποίες ο διαχειριστής του δικτύου επιτρέπει να συνδεθούν.Έτσι αν η MAC διεύθυνση μιας clientσυσκευής δεν ανήκει σε αυτή την λίστα,η συσκευή αυτή δεν θα μπορέσει να συνδεθεί στο AP.Παρόλα αυτά η μέθοδος αυτή είναι ανεπαρκής καθώς κάποιος εισβολέας με χρήση ενός κατάλληλού λογισμικού το οποίο πολλές φορές είναι δωρεάν,με ένα laptopκαι μια απλή κάρτα Wi-Fi να φτιάξει μια λίστα με τις MAC διευθύνσεις οι οποίες βλέπει ότι συνδέονται επιτυχώς με το AP.Με αυτό τον τρόπο αλλάζοντας την MAC διεύθυνση του σε οποιαδήποτε από αυτές,καταφέρνει να συνδεθεί επιτυχώς στο δίκτυο χωρίς έτσι κανείς να καταλάβει την διαφορά.Μια τέτοια επίθεση ονομάζεται MAC spoofing attacks η οποία περιγράφτηκε πιο πάνω.Τέλος την δυνατότητα χρησιμοποίησης οποιασδήποτε MAC διεύθυνσης ο κάθε χρήστης επιθυμεί παρέχουν και αρκετές εταιρίες παραγωγής υλικού δικτύων πλέον στα προϊόντα τους.

3.9.7 ΧΡΗΣΗ ΤΟΥ WAP2 (Wi-Fi Protected Access 2)

Το πρωτόκολλοWAP2-Wi-Fi Protected Access2 αναπτύχθηκε από την Wi-Fi alliance για την ενίσχυση της ασφάλειας του δικτύου Wi-Fi και αποτελεί μαζί με το πρότυπο 802.11i διάδοχο του WAP,ενισχύοντας δυναμικά την ασφάλεια των προτύπων 802.11b,802.11a και 802.11g.Το WAPόπως και το WEP παρουσιάζει και αυτό κάποια σημαντικά κενά ασφαλείας.Το γεγονός αυτό οφείλεται κυρίως στο ότι και τα δυο πρωτόκολλα χρησιμοποιούν τον ίδιο αλγόριθμο κρυπτογράφησης.Το WAP2 διαθέτει συμβατότητα με το WAP,όπως και με την κρυπτογράφηση TKIP,την 802.1X/EAP επικύρωση και τον μηχανισμό RSK.Έτσι όπως ο WAP ο WAP2 για την επικύρωση θα χρησιμοποιήσει το 802.1X/EAP πλαίσιο το οποίο την συγκεντρωμένη αμοιβαία επικύρωση και την διαχείριση δυναμικών κλειδιών καθώς και ενός φορέα πιστοποίησης.Η μεταφορά αυθεντικότητας μεταξύ του σταθμού (STA) και του διακομιστή αυθεντικότητας (AS) παρέχεται από το υψηλότερο επίπεδο του εκτεταμένου πρωτοκόλλου αυθεντικότητας και του επιπέδου ασφαλείας μεταφοράς (EAP-TLS).Αυτό που κάνει το IEEE 802.1X για τα ασύρματα LANδίκτυα είναι παρόμοιο με αυτό που κάνει το RADIUSδηλαδή να παρέχει μεταφορά στο EAP. Επίσης για τους οικιακούς χρήστες το WPA2 παρέχει έναν μηχανισμό προ-μοιρασμένου κλειδιού τον PSK (Pre-Shared Key).Επίσης όπως και ο WAP έτσι και ο WAP2 είναι σχεδιασμένο για να εξασφαλίσει όλες τις εκδόσεις 802.11 συσκευών,συμπεριλαμβανομένου του 802.11b,802.11aκαι 802.11g.Όσον αφορά την κρυπτογράφηση το WAP2 χρησιμοποιεί τον αλγόριθμο CCMP(Counter Mode with

Cipher Block Chaining Message Authentication Code Protocol),ο οποίος για την ανάπτυξη του βασίστηκε στο CCM του αλγορίθμου AES καθώς επίσης και τον μηχανισμό AES,ο οποίος χρησιμοποιεί ένα μαθηματικό αλγόριθμο κρυπτογράφησης ο οποίος υιοθετεί μεταβλητά μεγέθη κλειδιών μήκους 128bit,192 bit,ή 256bit.Έτσι ο αλγόριθμος RC4 αντικαταστάθηκε.Όπως το TKIP έτσι και το CCMP χρησιμοποιεί διπλάσιο IVδηλαδή 48 bitαλλά αντί για την ακολουθία αριθμών ανά πακέτο χρησιμοποιεί AES κλειδιά για την εξασφάλιση της εμπιστευτικότητας,ακεραιότητας και προστασίας του πακέτου.Επίσης χρησιμοποιεί κλειδί κρυπτογράφησης 128 bitτο οποίο ελαχιστοποιεί την ευπάθεια σε επαναλαμβανόμενες επιθέσεις.Το χαρακτηριστικό του κλειδιού κρυπτογράφησης είναι ότι επιτρέπει σε ένα σημείο πρόσβασης να κρατήσει τις πληροφορίες για τα κλειδιά των σταθμών που αποσυνδέθηκαν πρόσφατα.Έτσι αν ένας σταθμός προσπαθήσει να επανασυνδεθεί ενώ η καταχώρηση για την προηγούμενη σύνδεση ισχύει ακόμη μπορεί γρήγορα να αυθεντικοποιηθεί και να συνδεθεί.Η ενισχυμένη προστασία που προσφέρει το CCMP σε σύγκριση με το TKIP απαιτεί μεγαλύτερη επεξεργαστική ισχύ καθώς επίσης χρειάζεται και συχνά νέο ή αναβαθμισμένο hardware.Οι συσκευές και τα ασύρματα δίκτυα που υποστηρίζουν την μικτή λειτουργία WPA και WPA2 κάνουν πιο εύκολη την μεταφορά των δεδομένων ανάμεσα στα πρότυπα.



Εικόνα: Λειτουργία WAP2 με την χρήση του AES-CCMP αλγόριθμου κρυπτογράφησης.

3.9.8 ΧΡΗΣΗ ΤΟΥ EAP

Το EAP (Extensible Authentication Protocol) είναι ένα πρωτόκολλο-πλαίσιο ταυτότητας δηλαδή πιστοποίησης το οποίο περιλαμβάνει ένα σύνολο μηνυμάτων που χρησιμοποιείται στα ασύρματα δίκτυα και στις point-to-point συνδέσεις,κατά την έναρξή και το τέλος των διαπραγματεύσεων που πραγματοποιούνται από όλες τις μεθόδους πιστοποίησης των ανώτερων στρωμάτων και όχι ένας συγκεκριμένος μηχανισμός.Το EAP ορίζεται από το RFC 2284 και 3748 και παρέχει κάποιες συναρτήσεις για την επικοινωνία και την χρήση τους σε μηχανισμό

πιστοποίησης.Επίσης το EAP επιτρέπει την ανταλλαγή πληροφοριών ανάμεσα σε δυο πλευρές οι οποίες αφορούν την συγκεκριμένη μέθοδο πιστοποίησης που επιθυμούν να εφαρμόσουν.Το περιεχόμενο αυτών των μεθόδων δεν ορίζεται στο EAP.Η δυνατότητα αυτή του EAP να διεκπεραιώνει μέρος της επικοινωνίας με προτυποποιημένο τρόπο κατ το υπόλοιπο με ειδικό τρόπο για κάθε μέθοδο οφείλεται στο κλειδί επεκτασιμότητας του πρωτοκόλλου.Το EAP υποστηρίζει πολλές μεθόδους πιστοποίησης καθώς διαχειρίζεται την πιστοποίηση αλλά η χρησιμοποιούμενη παραλλαγή του ανάλογα με τις ανάγκες τις κάθε μιας υλοποίησης υπαγορεύει πώς οι πελάτες πιστοποιούνται και επιτρέπει έτσι στο EAP διαφορετικούς τύπους πιστοποίησης.Μερικές από τις μεθόδους επικύρωσης είναι**:**

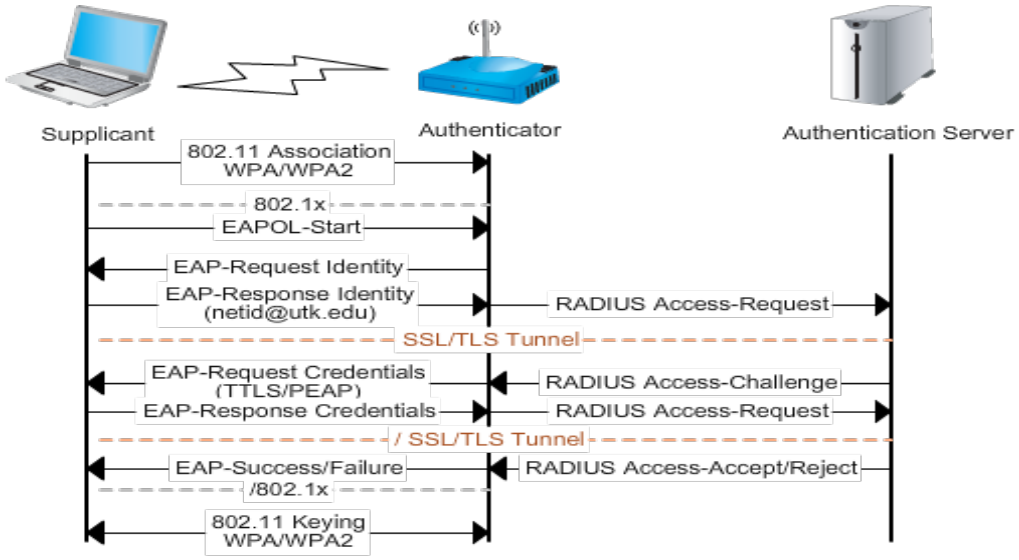
- Επικύρωση δημόσιου κλειδιού,
- Πιστοποιητικά,
- Έξυπνες κάρτες (smart cards),
- Συνθηματικό μιας χρήσης (One time pass words OTP)

Υπάρχουν πολλά είδη πλαισίων EAP πιστοποίησης όπως τα LEAP,EAP-TLS,EAP-MD5,EAP-PSK,EAP-TTLS, EAP-POTP, EAP-GTC, EAP-SIM, EAP-AKA και EAP-AKA.Κάθε πρωτόκολλο που χρησιμοποιεί EAP ορίζει τον τρόπο να ενσωματώσουν τα μηνύματα EAP μηνύματα εντός του εν λόγω πρωτοκόλλου.Τα μηνύματα αυτά είναι ενδιάμεσα και είναι ειδικά,επειδή παρουσιάζονται μετά την έναρξή και πριν τον τερματισμό της πιστοποίησης ταυτότητας.Ο αριθμός των ενδιάμεσων αυτών μηνυμάτων που μπορούν να ανταλλαχτούν μέχρι να ολοκληρωθεί η επαλήθευση της ταυτότητας είναι μεγάλος.Το EAP ορίζει τέσσερις τύπους μηνυμάτων που μπορούν να σταλούν αυτοί είναι**:**

- **Αίτηση(Request):** Χρησιμοποιείται από τον πάροχο πιστοποίησης για την αποστολή μηνυμάτων στον αιτούμενο supplicant.
- **Απάντηση(Response):** Χρησιμοποιείται από τον αιτούντα (supplicant) για την αποστολή μηνυμάτων στον πάροχο πιστοποίησης-authenticator.
- **Επιτυχία(Success):** Αποστέλλεται από τον πάροχο πιστοποίησης ως ένδειξή για την παροχή πρόσβασης.
- **Αποτυχία(Failure):** Αποστέλλεται από τον πάροχο πιστοποίησης ως ένδειξή για την άρνηση πρόσβασης.

Τα μηνύματα αυτά ορίζονται σε σχέση με τον πάροχο πιστοποίησης,όμως στο IEEE 802.1X ο πάροχος πιστοποίησης τα μηνύματα αυτά τα προωθεί στο εξυπηρετητή πιστοποίησης που χρησιμοποιεί το RADIUS.Έτσι τα παραπάνω μηνύματα παράγονται από τον RADIUS και ο πάροχος πιστοποίησης απλά τα αναμεταδίδει στην οντότητα του αιτούμενου.Τα μηνύματα EAP έχουν όλα την ίδια βασική μορφή.Το πρώτο πεδίο είναι ο κωδικός ο οποίος υποδεικνύει τον τύπο του μηνύματός δηλαδή (01) αν είναιRequest,(02) αν είναι Response,(03) αν είναι Success και (04) αν είναι Failure.Το δεύτερο πεδίο του αναγνωριστικού το οποίο παίρνει τιμές από 0-255 και το 802.1X ορίζει ότι πρέπει να αυξάνεται το εύρος αυτό σε κάθε μήνυμα που αποστέλλεται. Το πεδίο τύπος είναι το συνολικό μέγεθος του μηνύματος EAP.Το

πεδίο δεδομένα το οποίο περιέχει τα πραγματικά δεδομένα αίτησης ή απόκρισης που στέλνονται. Επίσης τα μηνύματα αίτησης και απάντησης υποδιαιρούνται επιπλέον με βάση το πεδίο τύπου του EAP όπου υποδεικνύει το είδος της πληροφορίας που μεταφέρεται στο μήνυμα για τις μεθόδους πιστοποίησης ταυτότητας.Ο πιο σημαντικός από τους βασικούς τύπος είναι η ταυτότητα IDπου χρησιμοποιείται στην φάση έναρξής του EAP και έχει τιμή 1.Το μήνυμα EAP-Request/Identityαποστέλλεται από τον πάροχο πιστοποίησης σε ένα αιτούμενο όπου με την σειρά του αυτός απάντα με το μήνυμα EAP-Response/Identity που περιέχει το όνομα χρήστη ή κάποιο άλλο χαρακτηριστικό κατάλληλο για τον εξυπηρετητή πιστοποίησης ταυτότητας.Τα μηνύματαsuccessκαι failureείναι σύντομα και δεν περιέχουν δεδομένα.Επίσης το κάθε ένα από αυτά χρησιμοποιούνται κάθε φορά για να σηματοδοτήσει το αποτέλεσμα της διαδικασίας επαλήθευσης ταυτότητας,είναι κοινά για όλες τις μεθόδους πιστοποίησης ταυτότητας και για τις ενδιάμεσες συσκευές όπως είναι το σημείο πρόσβασης,επιτυγχάνοντας έτσι την ολοκλήρωση πιστοποίησης ταυτότητας χωρίς την απαίτηση σχετικών λεπτομερειών. Το σημείο πρόσβασης πρέπει να περιμένει μήνυμα RADIUS access-accept τύπου όπως θα δούμε πιο κάτω πριν πάρει οποιαδήποτε απόφαση που αφορά δικαιώματα πρόσβασης.Το EAP είναι σε ευρύ σε χρήση,για παράδειγμα στο IEEE 802.11 (Wi-Fi),το WPA και WPA2 αυτά τα πρωτόκολλα έχουν υιοθετήσει το πρότυπο 802.1X με πέντε τύπους EAP τους επίσημους μηχανισμούς πιστοποίησης.



Εικόνα: Διαδικασία πιστοποίησης EAP.

3.9.9 ΑΛΛΟΙ ΤΡΟΠΟΙ ΘΩΡΑΚΙΣΗΣ ΤΟΥ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ

Πέρα από τις προαναφερθείσες τεχνικές που αναλύθηκαν πιο πάνω οι οποίες μπορούν να προσφέρουν ένα ικανοποιητικό επίπεδο ασφαλείας όμως σε περιβάλλοντα,όπου η ασφάλεια αποτελεί μείζονος σημασία (π.χ.επιχείρηση),απλά δεν αρκούν.Σε τέτοιες περιπτώσεις για να γίνει το δίκτυο ασφαλέστερο θα πρέπει να χρησιμοποιηθεί επίσης επιπλέον hardware ή software.Παρακάτω αναλύονται μερικές επιπλέον μέθοδοι ασφαλείας ασύρματού δικτύου.

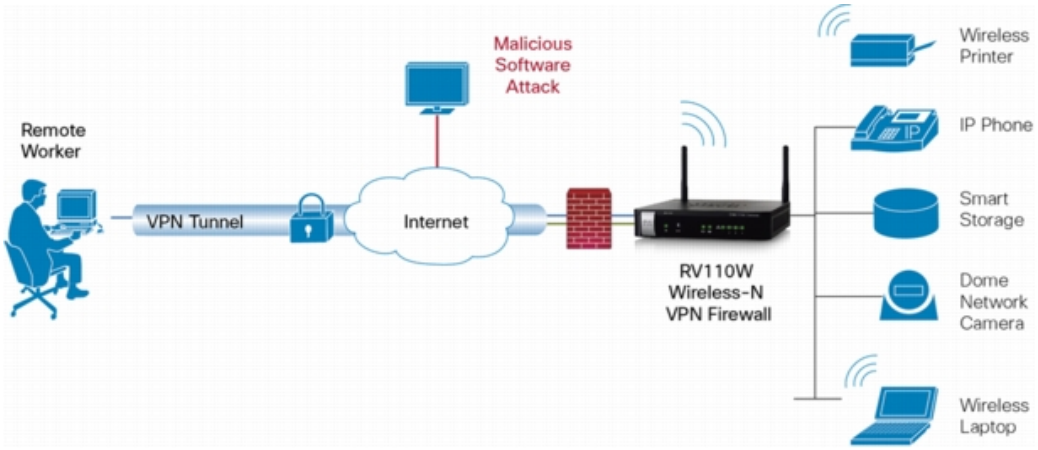
- **Τείχος προστασίας-Firewalls:** Επειδή το ασύρματο δίκτυο θεωρείται οπωσδήποτε ανασφαλές και μέρος του διαδικτύου για το λόγο αυτό ένα Firewall (τοίχος προστασίας) μπορεί να βοηθήσει στην εξάλειψη των κινδύνων ασφαλείας που διατρέχει το δίκτυο.Το Firewall είναι ένας εξυπηρετητής μεσολάβησης (proxy server) ο οποίος με βάση ένα σύνολο κανόνων που καθορίζονται από τον διαχειριστή του δικτύου,φιλτράρει όλα τα δεδομένα που περνάν μέσα από αυτόν στην πορεία από και προς ένα δίκτυο.Ένα Firewall ανάλογα με το είδος της πολιτικής που ακολουθείται από μια επιχείρηση ή εταιρία και με την εγκατάσταση μπορεί να αποτρέψει τις μη εξουσιοδοτημένες αιτήσεις.Έτσι για τους εισβολείς οι οποίοι μπορεί να έχουν τον έλεγχο του ασύρματου δικτύου και να προσπαθούν να διεισδύσουν στο εσωτερικό δίκτυο,το Firewall δημιουργεί ένα φυσικό εμπόδιο.Ένα Firewall για παράδειγμα μπορεί να απορρίψει τα δεδομένα που προέρχονται από άγνωστη πηγή ή αρχεία που αντιστοιχούν σε μία συγκεκριμένη πηγή, όπως ιούς-virus ή μπορεί να επιτρέπει τη διέλευση όλων των δεδομένων προς το διαδίκτυο και να επιτρέπει τη διέλευση μόνο ορισμένων δεδομένων από το διαδίκτυο.Τα Firewalls μπορεί να είναι είτε software είτε hardware.Η ιδανική λύση είναι η χρήση και των δυο.Ενα Firewall μπορεί να τοποθετηθεί στην πύλη μεταξύ των ασύρματων σημείων πρόσβασης και του ενσύρματου δικτύου.Με αυτό τον τρόπο απομονώνεται το ασύρματο κομμάτι από το ενσύρματο κομμάτι του LAN,ούτως ώστε οι εισβολείς που έχουν συνδέσει τον υπολογιστή τους στο δίκτυο χωρίς άδεια να μην μπορούν να χρησιμοποιήσουν την ασύρματη σύνδεση για να μπουν στο διαδίκτυο ή στο ενσύρματο κομμάτι του LAN.Σήμερα οι routers περιέχουν ενσωματωμένο Firewall και παρέχουν την δυνατότητα ενεργοποίησης/απενεργοποίησης του.Εκτός από την ασφάλεια που παρέχουν τα Firewalls όσο αφορά τον περιορισμό της πρόσβασης στο δίκτυο και τον προσωπικό υπολογιστή, επιτρέπει και την ασφαλή απομακρυσμένη πρόσβαση (remote access) μέσα από μηχανισμούς αυθεντικοποίησης.

Εικόνα: Firewall απομόνωσης ασύρματου και ενσύρματου LAN.

- **Virtual Private Networks-VPNS:** Το εικονικό ιδιωτικό δίκτυο(κανάλι)VPN μπορεί να παρέχει μια άλλη μορφή αποτελεσματικής προστασίας στα δεδομένα

από κακόβουλη επίθεση.Το VPN βρίσκεται πάνω σε ένα ήδη υπάρχον δίκτυο και χρησιμοποιεί ένα ¨τούνελ δεδομένων¨ για να συνδέσει δύο σημεία σε ένα δίκτυο μέσω ενός κωδικοποιημένου καναλιού.Τα σημεία αυτά μπορεί να είναι ένας πελάτης δικτύου και ένας server ή ένα ζεύγος πελατών κλπ.Στα πακέτα των δεδομένων ο πελάτης του VPN προσθέτει μια νέα επικεφαλίδα με πληροφορίες καθοδήγησης που λέει στα πακέτα πως θα φτάσουν στο τέλος του VPN.Στην άλλη άκρη του τούνελ,ο VPN Server αφαιρεί την επικεφαλίδα καθοδήγησης και προωθεί τα δεδομένα στον προορισμό που καθορίζεται από το επόμενο στρώμα επικεφαλίδων.Τα δεδομένα αντιμετωπίζουν το τούνελ σαν μια σύνδεση poin-to-point και έτσι η ακριβής μορφή του τούνελ δεν παίζει ρόλο για τα δεδομένα.Οι επικεφαλίδες τούνελ μπορούν να πάρουν διάφορες μορφές.Οι μέθοδοι που χρησιμοποιούνται ευρέως στα VPNs είναι**:** Πρωτόκολλο τούνελ σημείου-σημείου (PPTP),Πρωτόκολλο τούνελ δεύτερου στρώματος (L2TP) και IP Security (IPSec) mode.Ο πελάτης και ο server πρέπει να χρησιμοποιούν το ίδιο πρωτόκολλο.Το VPN υποστηρίζει υπηρεσίες κρυπτογράφησης,πιστοποίησης και διαχείρισης κλειδιών μέσω κωδικού και ονόματος χρήστη κάνοντας έτσι τα δεδομένα ακατανόητα στους εισβολείς,καθώς επίσης διατηρεί την πιστότητα κάθε πακέτου δεδομένων εξασφαλίζοντας έτσι ότι όλα τα δεδομένα προέρχονται από αξιόπιστους πελάτες δικτύου.Επίσης στο σημείο πρόσβασης ο VPN server δεν δέχεται συνδέσμους δεδομένων από ασύρματους πελάτες που δεν χρησιμοποιούν τους σωστούς οδηγούς και κωδικούς VPN.Έτσι οι μη εξουσιοδοτημένοι χρήστες δεν μπορούν να εισβάλουν στο δίκτυο και στο μονοπάτι των δεδομένων καθώς αυτό είναι απομονωμένο.Έτσι τα απομονωμένα και κρυπτογραφημένα δεδομένα μπορούν να κινούνται σε κοντινή απόσταση και όχι σε εκατοντάδες ή χιλιάδες χιλιόμετρα.Το σημείο πρόσβασης ωστόσο μπορεί να μεταφέρει δεδομένα κωδικοποιημένα κατά VPN μέσω του διαδικτύου σε άλλη τοποθεσία. Το VPN συχνά ενσωματώνεται σε εργαλεία ή λογισμικά πακέτα.Έτσι σε ένα Firewall μπορούν να δοθούν ρυθμίσεις,οι οποίες θα αποκλείουν εντελώς όλες τις εισερχόμενες αιτήσεις,με εξαίρεση αυτές των πιστοποιημένων VPN σταθμών.Αυτό παρέχει μια δικλείδα ασφαλείας όχι μόνο για το ασύρματο σημείο πρόσβασης αλλά και για τους χρήστες και των δεδομένων τους.Όπως είδαμε πιο πάνω η κρυπτογράφηση WEP είναι ανασφαλής,καθώς ένας επιδέξιος επιτιθέμενος με τα κατάλληλα εργαλεία μπορεί να βρεθεί στην ζώνη εκπομπής του δικτύου και να συλλάβει αρκετά πακέτα για να ανακτήσει τον μυστικό κωδικό WEP.Στη συνέχεια με τη βοήθεια αυτού του κωδικού μπορεί να παγιδέψει και όλη την πληροφορία που μετακινείται στον αέρα και να την αποκωδικοποιήσει.Έτσι για την αποφυγή αυτής της επίθεσης χρησιμοποιείται η VPN κρυπτογράφηση σε συνδυασμό με την WEP, αναγκάζοντας έτσι τον επιτιθέμενο να αποκρυπτογραφήσει σε δυο επίπεδα. Στο πρώτο επίπεδο θα πρέπει να βρεθεί ο μυστικός κωδικός της WEP κρυπτογράφησης και στο δεύτερο επίπεδο θα πρέπει να αντιμετωπίσει το ισχυρό τοίχος της VPN κρυπτογράφησης.Έτσι επειδή ακόμα και ένα έμπειρος επιτιθέμενος δε μπορεί με ευκολία να αναπαράγει τον κωδικό της

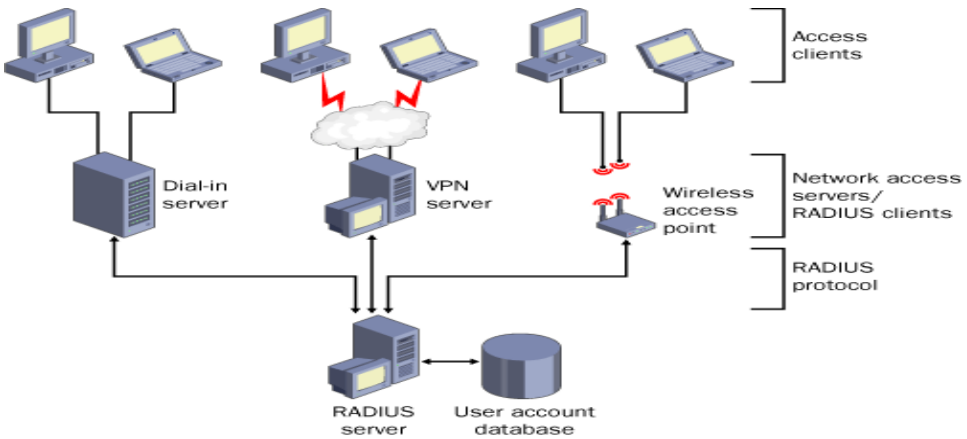
κρυπτογράφησης,να προσπεράσει την πιστοποίηση ή τον έλεγχο πρόσβασης,το ποσοστό επιτυχίας μιας τέτοιας επίθεσης είναι πολύ χαμηλό.Παρόλα αυτά η χρήση του συνδυασμού των δυο κρυπτογραφήσεων έχει ένα μεγάλο μειονέκτημα.Εμφανίζεται η ανάγκη για διπλάσια επεξεργαστική ισχύ.η οποία προκαλείται από την κρυπτογράφηση και αποκρυπτογράφηση σε δύο επίπεδα. Έτσι η χρήση του WEP σε συνδυασμό με το VPN σε ένα σωστά ρυθμισμένο ασύρματο μέσο πρόσβασης μπορεί να ελαττώσει την ταχύτητα της μετάδοσης κατά μεγάλο ποσοστό έως και 80%.Τέλος η χρήση ενός VPN δικτύου προϋποθέτει την εγκατάσταση ενός λογισμικού σε κάθε σταθμό που πρόκειται να συνδεθεί στο δίκτυο.Όμως επειδή τα περισσότερα λογισμικά VPN προορίζονται για Windows λειτουργικό αυτό σημαίνει ότι σταθμοί με λειτουργικά συστήματα όπως MACOS,Linux και υπολογιστές παλάμης (palmtop) μπορεί να μην μπορούν να συνδεθούν στο δίκτυο.



Εικόνα: VPN δικτύωση.

- **Remote Authentication Dial-In User Service-RADIUS:** Το RADIUS είναι ένα πρωτόκολλο το οποίο αναπτύχθηκε από την Livingston Enterprise ως διακομιστής πρόσβασης,πιστοποίησης και παρακολούθησης,Το πρωτόκολλο αυτό αν και αρχικά χρησιμοποιήθηκε για dial-up απομακρυσμένη πρόσβαση σήμερα χρησιμοποιείται από VPNs server,802.11 APs,Ethernet Switches πιστοποίησης για DSL πρόσβαση,WLANs δίκτυα για την απόκτηση ελέγχου κάθε παραμέτρου της σύνδεσης και άλλους τύπους δικτυακής πρόσβασης, ενώ μπορεί να πιστοποιήσει και άλλους τύπους υπηρεσιών. ToRADIUS πρωτόκολλο είναι ένα πρωτόκολλο πελάτη/διακομιστή το οποίο εκτελείται στο επίπεδο εφαρμογών του μοντέλου OSI χρησιμοποιώντας το UDP πρωτόκολλο για την επικοινωνία μεταξύ ενός σημείου πρόσβασης και του εξυπηρετητή πιστοποίησης ταυτότητας. Ο εξυπηρετητής πιστοποίησης ταυτότητας είναι συνήθως ενσωματωμένος στο σημείο πρόσβασης με σκοπό να προσφέρει μια κεντρικοποιημένη πιστοποίηση, εξουσιοδότηση και λογιστική καταγραφή χρηστών για δικτυακή πρόσβαση. Συναντάται κυρίως σε εταιρικά και ευρείας κλίμακας δίκτυα και σπάνια σε οικιακές εγκαταστάσεις. Στις μικρές εγκαταστάσεις είναι απίθανο σχεδόν να χρησιμοποιηθεί το RADIUS διότι η επικύρωση γίνεται συνήθως μέσα στο σημείο πρόσβασης. Οι εξυπηρετητές

πρόσβασης δικτύου NAS (Network Access Server) λειτουργούν σαν clients του RADIUS.Ο client είναι υπεύθυνος για να προωθήσει την πληροφορία του χρήστη στον αρμόδιο RADIUS Server και εκτελεί τις εντολές που θα του σταλούν πίσω από το Server. Ο RADIUS Server λειτουργεί ως εξυπηρετητής πιστοποίησης ταυτότητας AS (Authentication Server) και είναι υπεύθυνος για τις υπηρεσίες πιστοποίησης και παρακολούθησης σε περισσότερους από έναν RADIUS client δηλαδή στις συσκευές NAS.Επίσης για να δοθούν οι απαιτούμενες υπηρεσίες στους χρήστες λαμβάνει τις αιτήσεις σύνδεσης των χρηστών, τις πιστοποιεί και τέλος επιστρέφει όλη τη πληροφορία με τις απαιτούμενες ρυθμίσεις για τους clients.Ο RADIUS Server είναι συνήθως ένας αφιερωμένος σταθμός εργασίας συνδεδεμένος με το δίκτυο. Για να χρησιμοποιήσει το δίκτυο για παράδειγμα μιας εταιρίας ή ενός οργανισμού κάποιος χρήστης θα πρέπει πρώτα να εισαγάγει τα στοιχεία του,username και password τα οποία διασταυρώνονται με τον RADIUS Server. Έτσι όταν ο RADIUS Server λαμβάνει μια αίτηση από κάποιον NAS αναζητά σε μια βάση δεδομένων το username που υπάρχει στην αίτηση, εάν το username δεν υπάρχει στην βάση δεδομένων τότε ο RADIUS Server στέλνει μήνυμα απόρριψης (Access-Reject) το οποίο μπορεί να συνοδεύεται και από κάποιο επεξηγηματικό μήνυμα του λόγου απόρριψης. Εάν όμως το username βρεθεί και το password είναι σωστό ο RADIUS Server επιστρέφει μία Access-Accept αποδοχή απάντησης η οποία περιλαμβάνει μια λίστα των χαρακτηριστικών των ρυθμίσεων που πρέπει να χρησιμοποιηθούν από τη μεριά του NAS για τη σύνδεση.Ο RADIUS Server όπως είδαμε και πιο πάνω χρησιμοποιείται στην κρυπτογράφηση WEP για την αποφυγή υποκλοπής του κλειδιού WEP καθώς και στην WAP κρυπτογράφηση κάνοντας έτσι πλέον σχεδόν αδύνατη την εύρεση του κλειδιού από τους εισβολείς. Τέλος επειδή η πιστοποίηση αποτελεί την πιο απαιτητική πλευρά της ασφάλισης απομακρυσμένων χρηστών λόγω της δυσκολίας που σχετίζεται με τη σίγουρη αναγνώριση του χρήστη, για την διασφάλιση ταυτότητας ενός απομακρυσμένου χρήστη το πρωτόκολλο RADIUS υποστηρίζει πολλές μεθόδους πιστοποίησης περιλαμβανομένων των Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) ή Extensible Authentication Protocol (EAP).



Εικόνα: Ο RADIUS Server και το δίκτυο.

ΚΕΦΑΛΑΙΟ 4^{Ο}: ΜΕΛΛΟΝΤΙΚΗ ΕΞΕΛΙΞΗ

4.1 ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ Η ΤΕΧΝΟΛΟΓΙΑ Wi-Fi ΣΗΜΕΡΑ

Η εποχή στην οποία ζούμε χαρακτηρίζεται από την μεγάλη διακίνηση όγκων πληροφορίας και την ραγδαία ανάπτυξη πληροφορίας,έτσι η υλοποίηση των ασύρματων δικτύων συμβάλλει δραματικά στην απλούστευση του τρόπου επικοινωνίας και σύνδεσης των οντοτήτων του δικτύου καθώς και στην ταχύτερη μετάδοση των πληροφοριών.Οι εφαρμογές των ασύρματων δικτύων όπως του Wi-Fi βρίσκουν χώρο σε πολλούς τομείς οι οποίοι αναφέρονται ενδεικτικά παρακάτω**:**

- Πρόσβαση σε πολυσύχναστα και κεντρικά σημεία (HotSpots),όπως αεροδρόμια,εμπορικά καταστήματα, εστιατόρια, καφετέριες, ξενοδοχεία κλπ.Προφέροντας έτσι στους ανθρώπους ενημέρωση, διαφήμιση, ψυχαγωγία και ασφαλή και γρήγορη πρόσβαση στο ιντερνέτ και κυρίως σε εκείνους που ξοδεύουν πολύ χρόνο εκτός γραφείου όπως επαγγελματίες και στελέχη επιχειρήσεων.
- Στο περιβάλλον μιας επιχείρησης όπου προσφέρει στους εργαζόμενους ευελιξία καθώς μπορούν να επικοινωνούν μεταξύ τους,να εργάζονται και να κινούνται ελεύθερα με τους φορητούς υπολογιστές χωρίς να χάνουν λεπτό από την σύνδεση τους στο δίκτυο της εταιρίας και το διαδίκτυο. Έτσι αυξάνεται η παραγωγικότητα τους καθώς μπορούν να συνεργάζονται ευκολότερα και να έχουν συνεχή πρόσβαση σε κρίσιμές πληροφορίες.
- Στην εκπαίδευση σε πανεπιστήμια,σχολεία επιτρέποντας την πρόσβαση των φοιτητών/μαθητών σε βιβλιοθήκες,εκπαιδευτικό υλικό το οποίο υπάρχει αναρτημένο σε κάποιο σχετικό Link,βάσεις δεδομένων κλπ.,καθώς και την υλοποίηση μαθήματος τηλεκπαίδευσης,προσφέροντας έτσι νέους τρόπους μάθησης.
- Στην επίβλεψη χώρων όπως π.χ. σε έναν αρχαιολογικό χώρο όπου με χρήση ασύρματων καμερών μπορούν να μεταφέρουν ασύρματα εικόνα ιδιωτική ή δημόσια στο ιντερνέτ. Η παρακολούθηση χώρων γίνεται καλώντας την ασύρματη δικτυωμένη κάμερα.
- Στο σπίτι όπου δίνεται η δυνατότητα με χρήση μιας wi-fi συσκευής περιήγηση στο διαδίκτυο, παίζοντας παιχνίδια στο ιντερνέτ,παρακολούθηση μιας ταινίας αποφεύγοντας έτσι την χρήση καλωδίων και άλλων δικτυακών συσκευών με την τοποθέτηση ενός ή περισσότερων Access Points.
- Στην τηλεφωνία όπου με χρήση ασύρματων τηλεφωνικών συσκευών όπως τα κινητά μέσα στο ήδη υπάρχον ασύρματο δίκτυο Wi-Fi επιτρέπει την επικοινωνία μεταξύ πολλών ανθρώπων εξοικονομώντας χρήματα κάνοντας χρήση μιας υπηρεσίας βασισμένη στο ιντερνέτ όπως π.χ. η Viber.
- Δημιουργία σύνδεσης για κάποια συγκεκριμένη χρονική περίοδο,όπως για παράδειγμα η ανάγκη χρήσης του ιντερνέτ ή η πρόσβαση στο δίκτυο μιας

εταιρίας σε μια έκθεση από μια ομάδα εργασίας σε ένα συγκεκριμένο projectπου βρίσκεται σε απομακρυσμένο σημείο κάνοντας χρήση του Wi-Fi.

4.2 ΤΟ Wi-Fi ΣΤΗΝ ΕΛΛΑΔΑ

Στην Ελλάδα η ευρυζωνικότητα και το δίκτυο Wi-Fiαναπτύσσονται με το πέρασμα του χρόνου όλο και περισσότερο. Βέβαια σε σχέση με άλλες ευρωπαϊκές χώρες η Ελλάδα βρίσκεται σε δυσμενή σχέση καθώς βρίσκεται στα αρχικά στάδια ανάπτυξής του Wi-Fi.Δεδομένου του καθορισμού των ζωνών Σταθερής Ασύρματης Πρόσβασης (ΣΑΠ) με Υπουργική Απόφαση στα 3,6 και 26GHz και της χορήγησης των σχετικών αδειών με τη διαδικασία της δημοπρασίας το Δεκέμβριο του 2000,δεν έχει επιτραπεί μέχρι σήμερα η χρήση των 2,4GHz για την παροχή υπηρεσιών ΣΑΠ.Στον Κάτοχο της Άδειας,δίδεται το δικαίωμα παροχής Δημόσιων Κινητών Τηλεπικοινωνιακών Υπηρεσιών Ασύρματων Τοπικών Δικτύων σε δημόσιους χώρους (hotspots), με χρήση ραδιοεξοπλισμού συμβατού με το πρότυπο EN 300 328 του ETSI,που χρησιμοποιεί ραδιοσυχνότητες που βρίσκονται στη ζώνη 2.400-2.483,5MHz.Ο κάτοχος της άδειας αποδέχεται ότι στους σταθμούς ραδιοεπικοινωνιών που εγκαθίστανται και οι οποίοι λειτουργούν στη ζώνη 2.400-2.483,5MHz για την παροχή Δημόσιων Κινητών Τηλεπικοινωνιακών Υπηρεσιών Ασύρματων Τοπικών Δικτύων,δεν παρέχεται προστασία από τυχόν παρεμβολές,ούτε επιτρέπεται οι σταθμοί αυτοί να προκαλούν επιζήμιες παρεμβολές σε άλλους σταθμούς ραδιοεπικοινωνίας.Τέλος, ο κάτοχος της Άδειας δεν επιτρέπεται να παρέχει υπηρεσίες Σταθερής Ασύρματης Πρόσβασης (δεν επιτρέπεται η ζεύξη σημείου προς σημείο) και δεν επιτρέπεται να αναπτύξει Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κορμού,κάνοντας χρήση ραδιοσυχνοτήτων,που βρίσκονται στη ζώνη 2.400-2.483,5MHz.Για τις περιοχές 5.150-5.250, 5.250-5.350,5.470-5.725MHzκαι17,1-17,3GHz, (ΦΕΚ 979/Β11672003, παρ. 3/ιδ) επιτρέπεται χωρίς άδεια,η λειτουργία συσκευών μικρής εμβέλειας, οι οποίες είναι σύμφωνες με το Προεδρικό Διάταγμα 44/2002,τη Σύσταση ERC/REC 7003 και τα Πρότυπα ΕΝ 3008361, 2, 3 και 4, για την υλοποίηση τοπικών ασύρματων δικτύων με πρωτόκολλο HIPERLAN,σε 16 εσωτερικούς μόνο χώρους.Η δημιουργία τέτοιων δικτύων σε εξωτερικούς χώρους, επιτρέπεται μόνο μετά από άδεια της ΕΕΤΤ,η οποία χορηγείται ύστερα από σύμφωνη γνώμη του Υπουργείου Εθνικής Αμύνης.Παρομοίως,με την περιοχή των 2,4GHz,δεν επιτρέπονται ζεύξεις σημείου προς σημείο.Δοθέντος του γεγονότος ότι η εγκατάσταση δικτύων σε εξωτερικούς χώρους απαιτεί τη σύμφωνη γνώμη του ΓΕΕΘΑ,καθίσταται πολύ δύσκολη έως αδύνατη,η χορήγηση αδειών για παροχή υπηρεσιών στο κοινό, λόγω του ότι θα πρέπει οι παροχείς να καθορίζουν εκ των προτέρων και με την αίτηση τους, τους χώρους στους οποίους επιθυμούν να εγκαταστήσουν δίκτυα για την παροχή υπηρεσιών.Έτσι στόχος της χώρας είναι η δημιουργία και η εξάπλωση ανοικτών δημόσιών κεντρικών σημείων ασύρματων δικτύων Wi-Fiμε δωρεάν πρόσβαση στο δίκτυο σε όλη την Ελλάδα.Στην χώρα μας λειτουργούν κάποιες ασύρματες κοινότητες οι οποίες έχουν δικό τους ανεξάρτητό δίκτυο Wi-Fi,εξασφαλίζοντας φθηνή και απρόσκοπτη επικοινωνία. Έτσι σε πολλές ελληνικές πόλεις (Αθήνα,

Θεσσαλονίκη, Πάτρα, Γιάννενα, Σέρρες, Ξάνθη, κ.ά.)υπάρχουν τέτοια δίκτυα.Οι επίσημοι κόμβοι Wi-Fi στη χώρα μας έχουν πλέον αυξηθεί κατά πολύ (κυρίως στα αστικά κέντρα),ενώ πληθαίνουν τα hotspots σε ξενοδοχεία,καφετέριες και κάθε είδους επιχειρήσεις.Δυστυχώς,τα ελληνικά ασύρματα δίκτυα παραμένουν ακόμη στην πρώτη εποχή του Wi-Fi, δηλαδή του τοπικού δικτύου,αλλά αυτό δεν μειώνει καθόλου το ενδιαφέρον.Μερικές από τις ασύρματες είναι το Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών (AWMN) το οποίο είναι ένας μη κερδοσκοπικός σύλλογος που καλύπτει τις περισσότερες περιοχές της Αθήνας. Το Salonica Wireless Network (SWN),η ασυρμάτως δικτυωμένη κοινότητα της Θεσσαλονίκης, αυτοπροσδιορίζεται στην ιστοσελίδα της ως εξής: ¨7ο SWN¨ είναι μια ομάδα ατόμων,η οποία επεκτείνεται μέρα με τη μέρα,που ασχολούνται με τη δημιουργία ενός νόμιμου,ψηφιακού, ασύρματου δικτύου υψηλών ταχυτήτων,ελεύθερης πρόσβασης,στην ευρύτερη περιοχή της Θεσσαλονίκης.Κύριος σκοπός είναι να δημιουργηθεί ένα αξιοπρεπές, ελεύθερο δίκτυο,με υψηλό bandwidth ανάμεσα στους κόμβους κάθε ενδιαφερόμενου, μέσω ενός κοινοτικού ασύρματου δικτύου.Το Ακαδημαϊκό Ασύρματο Δίκτυο Ηρακλείου, είναι άλλο ένα community network, που έχει δημιουργηθεί εξ ολοκλήρου από την ακαδημαϊκή κοινότητα του Πανεπιστημίου Ηρακλείου και παρουσιάζει σοβαρή ανάπτυξη.Στο Βόλο,το Πανεπιστήμιο Θεσσαλίας έχει υλοποιήσει ένα ασύρματο δίκτυο,το οποίο συνδέει ευζωνικά όλα τα σχολεία της περιοχής, στο πλαίσιο του Πανελλήνιου Σχολικού Δικτύου.Αξίζει να σημειωθεί ότι όλα τα Ασύρματα Δίκτυα της Ελλάδας,δεν έχουν εμπορική διάσταση,αλλά αυστηρά συνεργατική.Με βάση το ισχύον κανονιστικό πλαίσιο, τα community networks εντάσσονται στο "καθεστώς ιδίας χρήσης",υπό την προϋπόθεση ότι δεν παρέχουν εμπορικές υπηρεσίες σε τρίτους, δεν κάνουν δηλαδή εμπορική εκμετάλλευση του δικτύου,αλλά χρήση μόνο από τα μέλη τους.Σύμφωνα με ανακοινώσεις του υπουργού Μεταφορών και Δικτύων Μιχάλη Χρυσοχοΐδη και του γενικού γραμματέα Τηλεπικοινωνιών Μενέλαου Δασκαλάκη δωρεάν πρόσβαση στο Internet από δημόσια σημεία θα μπορούν να έχουν οι πολίτες από τον Νοέμβριο του 2014,υλοποιώντας έτσι την εξαγγελία του πρωθυπουργού Αντώνη Σαμαρά (Νοέμβριος 2013) για ενεργοποίηση της υπηρεσίας σε όλη την Ελλάδα σε έναν χρόνο.Η πρώτη φάση του έργου,αφορά δωρεάν ασύρματη πρόσβαση σε 4.000 κλειστούς και ανοικτούς δημόσιους χώρους σε όλη την Ελλάδα.Η δεύτερη φάση θα επεκταθεί σε χώρους μεγάλης έκτασης,ειδικού ενδιαφέροντος και ειδικών τεχνικών και λειτουργικών απαιτήσεων δικτύου και εξοπλισμού και η τρίτη φάση αφορά πανεπιστήμια, νοσοκομεία και μέσα μαζικής μεταφοράς.Η πλήρης λειτουργία του δικτύου αναμένεται τέλος του 2014.Για την πρώτη φάση του έργου,η επιλογή των σημείων (wi-fi hotspots) αφορά χώρους από 302 δήμους της χώρας (σε σύνολο 325) που υπέδειξαν οι ίδιοι,100 αρχαιολογικούς χώρους και μουσεία και 200 χώρους λιμένων και μαρινών.Αυτό που πρέπει να επισημανθεί είναι πως είναι ήδη λειτουργεί ένα δίκτυο από δημόσια Wi-Fi hotspots,το οποίο αποτελεί το αποτέλεσμα του έργου «Ανάπτυξη Δημόσιων Σημείων Ασύρματης Ευρυζωνικής Πρόσβασης στο Διαδίκτυο (Public Hotspots)» που ξεκίνησε να υλοποιείται πριν από 5 χρόνια. Μέσω του συγκεκριμένου έργου,όπως αναφέρεται στην ηλεκτρονική διεύθυνση www.publichotspots.gov.gr,έχει δημιουργηθεί ένα δίκτυο από 195 σημεία ασύρματης

πρόσβασης σε ολόκληρη την Ελλάδα όπου η πρόσβαση είναι δωρεάν.Συγκεκριμένα, τα σημεία παρουσίας του δικτύου βρίσκονται σε**:**

- 126 κεντρικές πλατείες - πεζόδρομους
- 34 λιμάνια - μαρίνες
- 8 αεροδρόμια
- άλλους σταθμούς μεταφοράς
- 13 μουσεία - αρχαιολογικούς χώρους και
- 12 πάρκα.

Όμως, πολλά από αυτά τα σημεία δεν λειτουργούν ουσιαστικά και γι' αυτό αναμένεται να υπάρξει παρέμβαση από την πλευρά του ελληνικού Δημοσίου ώστε να «ξαναζωντανέψουν» με το πλάνο να περιλαμβάνει και την επέκταση αυτού του δικτύου.Επίσης,αρκετοί δήμοι αξιοποίησαν τα κονδύλια του συγκεκριμένου έργου προκειμένου να αποκτήσουν δημόσια Wi-Fi hotspots,παράλληλα,όμως,υπάρχουν αρκετοί ακόμη οργανισμοί τοπικής αυτοδιοίκησης που προχώρησαν σε αυτόνομες κινήσεις και επέκτειναν τα ήδη υπάρχοντα ασύρματα δίκτυα τους.Ακόμη το Γ' ΚΠΣ είχε επιδοτηθεί και η δημιουργία περίπου 560 Wi-Fi hotspots από επιχειρήσεις που κινούνταν στους χώρους της εστίασης και της ψυχαγωγίας.Στα πλάνα της κυβέρνησης είναι η δημιουργία Wi-Fi hotspots στα δημόσια νοσοκομεία με τις πρώτες εγκαταστάσεις να έχουν ήδη ξεκινήσει αλλά και στα δημόσια σχολεία.Αντίστοιχο πλάνο υπάρχει και για τα πανεπιστημιακά ιδρύματα,όπου λειτουργεί μεν ήδη ασύρματο δίκτυο αλλά η πρόσβαση σε αυτό επιτρέπεται μόνο στους φοιτητές και το προσωπικό των ιδρυμάτων.Ρόλο κλειδί σε αυτή την προσπάθεια αναμένεται να παίξει το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ) που έχει τη διαχείριση των ακαδημαϊκών δικτύων.Παράλληλα,ήδη έχουν αρχίσει να υπάρχουν κινήσεις για την παροχή Wi-Fi πρόσβασης στο Διαδίκτυο από την ΤΡΑΙΝΟΣΕ,ενώ πρόσφατα ξεκίνησε και η λειτουργία ασύρματων σημείων πρόσβασης σε σταθμούς του Μετρό της Αθήνας.Πιο συγκεκριμένα η εταιρία ΣΤΑΣΥ(ΣΤΑΘΕΡΕΣ ΣΥΓΚΟΙΝΩΝΙΕΣ Α.Ε.),σε συνεργασία με την Hellas online οργάνωσε την εγκατάσταση δικτύου προηγμένης τεχνολογίας Wi-Fi στο αθηναϊκό μετρό.Το δίκτυο εξασφαλίζει γρήγορη πρόσβαση στο ιντερνέτ σε επτά σταθμούς των γραμμών 1, 2 και 3 του μετρό και του ηλεκτρικού σιδηροδρόμου.Οι σταθμοί που θα «αποκτήσουν» το ελεύθερο Wi-Fi είναι οι εξής: Σύνταγμα, Πανεπιστήμιο, Ακρόπολη, Ομόνοια,Πειραιάς,Νερατζιώτισσα και Δούκισσας Πλακεντίας.Για τους υπόλοιπους σταθμούς στα μέσα Ιουλίου προγραμματίζεται η σταδιακή επέκταση του δικτύου σε όλους τους σταθμούς των γραμμών 2 και 3,του ΗΣΑΠ καθώς και σε στάσεις του τραμ.

4.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ Wi-Fi ΤΕΧΝΟΛΟΓΙΑΣ

Η τεχνολογία Wi-Fiπαρουσιάζει ορισμένα θετικά στοιχεία τα οποία αναφέρονται στην συνέχεια πιο κάτω**:**

- Ευκολία πρόσβασης στο ιντερνέτ ή στο e-mailαπό σχεδόν οποιαδήποτε τοποθεσία και αν βρίσκεται χωρίς να χρειάζεται να βρίσκεται στο σπίτι ή στο γραφείο,ιδίως στην περίπτωση δημόσιου Wi-Fi hotspot,με την αύξηση της χρήσης φορητών υπολογιστών laptop, κινητών τηλέφωνων,PDA κλπ.,αυτό είναι ιδιαίτερα σημαντικό. Αλλά ακόμη και αν βρίσκεται στους χώρους αυτούς η πρόσβαση είναι εφικτή σε οποιαδήποτε σημείο τους.
- Η σύνδεση του χρήστη στο διαδίκτυο γίνεται χωρίς την χρήση καλωδίων καθώς και συσκευών διασύνδεσης (modem,router)απελευθερώνοντας τον έτσι από αυτά.Επίσης του δίνει τη δυνατότητα στους χρήστες για πρόσβαση σε πληροφορίες όπως μια βάση δεδομένων όταν βρίσκονται σε κίνηση.Αυτή η ευχέρεια στην κίνηση υποστηρίζει την παραγωγικότητα και τις ευκαιρίες για εξυπηρέτηση οι οποίες δεν είναι δυνατές με ενσύρματα δίκτυα.
- Η ταχύτητα και η ευελιξία εγκατάστασης των δικτύων αυτών,καθώς δεν υπάρχει ο περιορισμός των καλωδίων.Μάλιστα σε ιστορικά κτίρια ή σε εξωτερικούς χώρους (πλατείες κ.α.),όπου δεν παρέχεται η δυνατότητα ανάπτυξης ενσύρματων δικτύων,τα δίκτυα Wi-Fi μπορούν πολύ εύκολα να υλοποιηθούν.
- Τα ασύρματα δίκτυα αποτελούν μια πολύτιμη λύση για ομάδες εργαζομένων οι οποίοι χρειάζονται να επικοινωνούν και να συνεργάζονται από διαφορετικό τόπο σε διαφορετική χρονική στιγμή.
- Το κόστος για την υλοποίηση αυτών το δικτύων είναι μειωμένο.Παρότι η αρχική επένδυση για την υλοποίηση ενός ασύρματου δικτύου (αγορά και εγκατάσταση συσκευών και εξοπλισμού) να είναι υψηλότερη από το αντίστοιχο ενός ενσύρματου δικτύου,το συνολικό κόστος χρήσης και λειτουργίας είναι αρκετά μικρότερο.Τα οφέλη είναι ακόμα μεγαλύτερα σε μακροπρόθεσμο επίπεδο, ιδιαίτερα στις περιπτώσεις δυναμικών χώρων εργασίας, οι οποίοι μπορεί να απαιτούν συχνές μετακινήσεις του προσωπικού και αλλαγές στη δομή και τη διάταξή τους.
- Τα ασύρματα δίκτυα Wi-Fi έχουν τη δυνατότητα επέκτασης,ώστε να υποστηρίξουν ποικιλία τοπολογιών και να ανταποκριθούν στις ανάγκες συγκεκριμένων εφαρμογών.Η γεωγραφική έκταση ενός Wi-Fi hotspot μπορεί να επεκταθεί χρησιμοποιώντας περισσότερα από ένα (διασυνδεδεμένα μεταξύ τους) σημεία πρόσβασης.
- Πολλά σημεία πρόσβασης καθώς και διεπαφές δικτύων υποστηρίζουν διάφορα επίπεδα κρυπτογράφησης για να προστατεύουν τα δεδομένα από υποκλοπή.

4.4 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΗΣ Wi-Fi ΤΕΧΝΟΛΟΓΙΑΣ

Όπως κάθε τεχνολογία παρουσιάζει θετικά και αρνητικά στοιχεία έτσι και η τεχνολογία Wi-Fi παρουσιάζει κάποια μειονεκτήματα τα οποία αναφέρονται παρακάτω**:**

- Η ταχύτητα του ασύρματου δικτύου είναι συνήθως είναι εξασθενισμένη και πιο ασταθής από ότι στο ενσύρματο δίκτυο διότι το ασύρματο δίκτυο έχει εγγενώς έναν περιορισμό όσον αφορά το φάσμα συχνότητάς του.Οι πιο σύγχρονοι δρομολογητές προσφέρουν μέχρι 100 Mbps, κι αυτό αν βρίσκεστε πολύ κοντά του και τα παλιότερα δίκτυα των 10Mbps θα μπορούν να χρησιμοποιηθούν παράλληλα.Κατά την κίνηση,το φάσμα συχνότητας πέφτει στα 80 Mbps και μειώνεται ακόμα περισσότερο καθώς απομακρύνεστε από το σημείο πρόσβασης.Για τις περισσότερες επιχειρήσεις τα δίκτυα των 10Mbps και 54Mbps είναι επαρκεί εκτός κι αν χρειάζεται να μεταφέρονται μεγάλα αρχεία μεταξύ των υπολογιστών.
- Το κόστος είναι συνήθως φθηνό αλλά αυτό μπορεί να κοστίσει έως και τέσσερις φορές περισσότερο για να δημιουργήσει ένα ασύρματο δίκτυο από το να δημιουργήσει ένα ενσύρματο δίκτυο σε ορισμένες περιπτώσεις.Για παράδειγμα μία κάρτα δικτύου μπορεί να στοιχίζει και 20Ευρώ ενώ ένα αντίστοιχο σύστημα μπορεί να στοιχίσει ακόμα και δύο με τρεις φορές περισσότερο.Έτσι παρόλο που οι τιμές τα τελευταία χρόνια έχουν πέσει αρκετά και οι συσκευές είναι πιο προσιτές στους καταναλωτές παραμένουν να είναι αρκετά πιο ακριβές.
- Ένα άλλο μειονέκτημα του ασύρματου δικτύου είναι οι παρεμβολές,τόσο αυτές που δέχεται, όσο και αυτές που προκαλεί.Τα ασύρματα δίκτυα είναι εξαιρετικά ευαίσθητα σε παρεμβολές από ραδιοσήματα και κάθε άλλο παρόμοιο τύπο παρεμβολή η οποία μπορεί να προκαλέσει σε ένα ασύρματο δίκτυο δυσλειτουργία. Έτσι κλειστά σημεία πρόσβασης μπορούν να παρεμβάλλονται από ανοιχτά σημεία πρόσβασης σωστά ρυθμισμένα στην ίδια συχνότητα,εμποδίζοντας έτσι την λειτουργία ανοιχτών σημείων πρόσβασης από άλλους.
- Το φαινόμενο του κρυμμένου κόμβο το οποίο παρατηρείται όταν υπάρχει ένας σταθμός που δεν μπορεί να ανιχνεύσει την δραστηριότητα ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται.
- Η ασφάλεια αποτελεί και αυτή ένα σημαντικό μέρος του Wi-Fi δικτύου. Μη σωστά εγκατεστημένα δίκτυα ή δίκτυα με χαμηλή ασφάλεια μπορούν πολύ εύκολα να παραβιαστούν από άτομα ειδικευμένα στις παραβιάσεις (hackers).
- Το ασύρματο δίκτυο καταναλώνει περισσότερη ενέργεια κάνοντας την διάρκεια ζωής της μπαταρίας και την εκπεμπόμενη θερμότητα πρόβλημα.Ωστόσο η ανάπτυξή της τεχνολογίας παρέχει συσκευές που είναι ειδικά σχεδιασμένες για την εξοικονόμηση ενέργειας, όπως είναι οι συσκευές Bluetooth για παράδειγμα,χωρίς αυτό να σημαίνει ότι δεν απαιτούν περισσότερη ενέργεια για τη μετάδοση του ασύρματου σήματος,σε αντίθεση με το ενσύρματο δίκτυο,που καταναλώνει ελάχιστη ηλεκτρική ενέργεια για τον ίδιο σκοπό.
- Η υγεία των ανθρώπων μπορεί να επηρεαστεί λόγω της καθημερινής έκθεσης ακτινοβολίας καθώς η τεχνολογία αυτή λειτουργεί σε αρκετά υψηλές συχνότητες.

4.5 ΜΕΛΛΟΝΤΙΚΗ ΕΞΕΛΙΞΗ

Η εξέλιξη της τεχνολογίας Wi-Fi και η βελτίωση της αρχίζει να παίρνει ραγδαίες διαστάσεις καθώς η τεχνολογία στην εποχή μας αναπτύσσεται με ταχύτερούς ρυθμούς. Πιο συγκεκριμένα η ομάδα του IEEE ανακοίνωσε το Wi-Fi IEEE 802.22, μια τεχνολογία που αυξάνει τη σημερινή εμβέλεια στα 100 χιλιόμετρα και προσφέρει ταχύτητα μέχρι 22Mbps. Η νέα τεχνολογία μετά από αρκετές δοκιμές θα κάνει χρήση τηλεοπτικών συχνοτήτων,των VHF και UHFTVσυχνοτήτων χωρίς όμως να επηρεάζει τη λήψη των τηλεοπτικών δεκτών.Επίσης η νέα αυτή τεχνολογία θα είναι ιδιαίτερα χρήσιμη σε όχι και τόσο πυκνοκατοικημένες περιοχές,σε αναπτυσσόμενες χώρες και γενικότερα περιοχές όπου μπορεί να υπάρχει "κενός χώρος" ανάμεσα στα τηλεοπτικά κανάλια.Επίσης η νέα τεχνολογία θα προσφέρει ελευθερία κινήσεων η οποία είναι εξωπραγματική για τα σημερινά στάνταρ όπου και είμαστε δέσμιοι των κοστολόγων3G προγραμμάτων συμβολαίου.Το παραπάνω γεγονός, όχι και άδικα, κάνει ορισμένους να είναι απαισιόδοξοι με την πορεία της νέας τεχνολογίας με ότι αυτό συνεπάγεται για τις τσέπες μας.Νέα μελέτη της Ευρωπαϊκής Επιτροπής έδειξε ότι υπάρχει σήμερα μεγάλο ενδιαφέρον για τη χρήση ασύρματου διαδικτύου (Wi-Fi) και η τάση αυτή πρόκειται να συνεχιστεί.Το 2012 το 71% του συνόλου της ασύρματης κυκλοφορίας δεδομένων στην Ε.Ε. έγινε με έξυπνα τηλέφωνα και tablets που χρησιμοποιούν Wi-Fi,σε ποσοστό που ενδέχεται να αυξηθεί σε 78% έως το 2016.Τα εντυπωσιακά αυτά αποτελέσματα της μελέτης δείχνουν πώς το χαμηλότερο κόστος για τους καταναλωτές από τη χρήση ζωνών ασύρματης πρόσβασης αλλάζει τις συνήθειες,και προτείνεται η διάθεση επιπλέον ραδιοφάσματος σε ολόκληρη τν Ε.Ε. για την ικανοποίηση της αυξανόμενης αυτής ζήτησης.Σύμφωνα με την αντιπρόεδρο της Ευρωπαϊκής Επιτροπής, κυρία Neelie Kroes η συμφόρηση στα δίκτυα 3G/4G,με την ελαχιστοποίηση του κόστους τόσο για τους φορείς εκμετάλλευσης όσο και για τους χρήστες των δικτύων,μπορεί να αντιμετωπιστεί με τη συνδυασμένη χρήση Wi-Fi και άλλων υποδομών μικρών κυψελών (που συμπληρώνουν τους παραδοσιακούς σταθμούς βάσης κινητών επικοινωνιών μεγάλων κυψελών). Έτσι οι φορείς εκμετάλλευσης θα μπορούν να εξοικονομούν δεκάδες δισεκατομμύρια ευρώ όταν αναβαθμίζουν τα δίκτυα για να καλύψουν τη ζήτηση των πελατών.όπως επίσης και καταναλωτές θα εξοικονομούν χρήματα χρησιμοποιώντας Wi-Fi όταν βρίσκονται κοντά σε ζώνη ασύρματης πρόσβασης αντί να πληρώνουν κινητές υπηρεσίες δεδομένων.Επίσης η Ευρωπαϊκή Επιτροπή ανήγγειλε κάποιες προτάσεις για την υλοποίηση όλων αυτών**:**

- Να καταστεί ευρέως διαθέσιμο ραδιοφάσμα από 5150 MHz έως 5925 MHz για ασύρματη πρόσβαση στο διαδίκτυο (Wi Fi).
- Να συνεχιστεί η διάθεση των ζωνών συχνοτήτων 2,6 GHz και 3,5 GHz για χρήση στην κινητή τηλεφωνία και να εξεταστεί η δυνατότητα για μελλοντικές αδειοδοτήσεις3,5 GHz και άλλες πιθανές νέες αδειοδοτημένες ζώνες συχνοτήτων κινητών επικοινωνιών.
- Να μειωθεί ο διοικητικός φόρτος που συνεπάγεται η εγκατάσταση δικτύων και υπηρεσιών σε δημόσιους χώρους.

Μια σημαντική εξέλιξη για το Wi-Fiεπίσης αποτελεί η ανακάλυψη από επιστήμονες του πανεπιστημίου Φουντάν της Σαγκάης λαμπτήρα,ο οποίος εκπέμπει σήμα Wi-Fi με την χρήση του φωτός σύμφωνα με το κινέζικό πρακτορείο ειδήσεων.Η τεχνολογία ονομάζεται Li-Fi και ο πρωτότυπος λαμπτήρας εκπέμπει καλύτερο σήμα Wi-Fi συγκριτικά με τις κοινές διαδικτυακές συνδέσεις στην Κίνα.Συμφωνά με αυτό τέσσερις υπολογιστές τοποθετημένοι σε κοντινή απόσταση από τον λαμπτήρα μπορούν να συνδεθούν ταυτόχρονα στο διαδίκτυο.Για την εκπομπή σήματος Wi-Fi μέθοδος που χρησιμοποιείται αξιοποιεί τις συχνότητες του φωτός σε αντίθεση με τις κοινές ασύρματες συνδέσεις που αξιοποιούν ραδιοκύματα.Ο λαμπτήρας διαθέτει ενσωματωμένο ένα ειδικό μικροτσίπ,το οποίο εκπέμπει το σήμα,πιάνοντας ταχύτητες έως και 150 Mbps.Τον επόμενο μήνα,οι ερευνητές ανακοίνωσαν ότι θα πραγματοποιήσουν επίδειξη με 10 τέτοιους λαμπτήρες σε εμπορική έκθεση στην Κίνα. Ένα άλλο σημαντικό γεγονός στην εξέλιξη του Wi-Fi η τεχνολογία MU-MIMO (Multi User – Multiple Input Multiple Output) η οποία ανακοινώθηκε επίσημα από την εταιρία Qualcomm από 7 χρόνια έρευνας και ανάπτυξης χάριν στην οποία οι ταχύτητες μεταφοράς δεδομένων μέσω των δικτύων Wi-Fi γίνονται 2 με 3 φορές μεγαλύτερες.Η τεχνολογία MU-MIMO επιτρέπει τη διανομή δεδομένων σε πολλαπλές ομάδες χρηστών ταυτόχρονα με τη βοήθεια ειδικού αλγορίθμου που ξεχωρίζει τι πρέπει να σταλεί στον καθένα.Σύμφωνα με την εταιρεία,τα πρώτα MU-MIMO chips θα δοθούν στους κατασκευαστές μέσα στο 2014 (για smartphones, tablets, routers και άλλες ηλεκτρονικές συσκευές που χρησιμοποιούν Wi-Fi) και οι τελικοί χρήστες θα δουν τα οφέλη τους από το 2015.Σημαντικό γεγονός στην εξέλιξη του Wi-Fiαποτελεί και η για πρώτη φορά σε υπερατλαντικές πτήσεις, πρόσβαση στο Wi-Fi δίκτυο της DeutscheTelekom, κάτι που γίνεται εφικτό με τη δορυφορική τεχνολογία της Panasonic που προσφέρει η γερμανική αεροπορική εταιρία Lufthansa η οποία αποτελεί τη μεγαλύτερη αεροπορική εταιρία της Ευρώπης. Έτσι οι επιβάτες θα μπορούν να έχουν 24ωρη πρόσβαση στο δίκτυο,με τις ταχύτητες οι οποίες θα αγγίζουν τα 5Mbps για download και 1Mbps για upload,ενώ αυτοί που θέλουν απλά να τσεκάρουν τα mails τους,),τους παρέχει πρόσβαση μονάχα για μία ώρα πληρώνοντας €19.95 (7.500 μίλια) και €10.95 (3.500 μίλια, αντιστοίχως).Αργότερα όλο και περισσότερες διαδρομές θα υποστηρίζουν την FlyNet υπηρεσία,ενώ δίνεται η δυνατότητα κατόχων smartphones και tablets να συνδεθούν επίσης, σε περίπτωση που κάποιος δεν κουβαλά το laptop του μαζί. Ένα άλλο σημαντικό γεγονός στην εξέλιξη του Wi-Fiαποτελεί το πρώτο υποθαλάσσιο Wi-Fiδίκτυο το οποίο ανέπτυξαν και δοκίμασαν με επιτυχία στην λίμνη ερευνητές από το Πανεπιστήμιο του Μπάφαλο.Στην έρευνα αυτή οι επιστήμονες βύθισαν στη λίμνη δυο γιγάντιους αισθητήρες, βάρους 18 κιλών ο καθένας, ενώ χρησιμοποίησαν ακουστικά κύματα για να δημιουργήσουν το ασύρματο δίκτυο,τα οποία στη συνέχεια μετέτρεψαν σε ραδιοκύματα.Το υποθαλάσσιο ασύρματο δίκτυο Wi-Fi θα χρησιμοποιηθεί για την παρακολούθηση της θαλάσσιας ζωής και την έγκαιρη πρόβλεψη ακραίων φαινομένων όπως τα τσουνάμι καθώς όπως δήλωσε ο Δρ. Tommaso Melodia, ηλεκτρολόγος μηχανικός στο πανεπιστήμιο του Μπάφαλο**:** «Το υποθαλάσσιο ασύρματο δίκτυο θα μας δώσει για πρώτη φορά τη δυνατότητα να συλλέγουμε και να αναλύουμε δεδομένα για τους ωκεανούς μας σε ζωντανό χρόνο» και πρόσθεσε ότι «Η

διάδοση αυτών των πληροφοριών μέσω έξυπνων τηλεφώνων ή ηλεκτρονικού υπολογιστή, ειδικά στην περίπτωση τσουνάμι ή κάποιας άλλης καταστροφής, θα μπορούσε να σώσει ζωές". Αξίζει να σημειωθεί ότι στο πλαίσιο της έρευνας αυτής συνεργάζονται και δυο Έλληνες καθηγητές ηλεκτρολογίας μηχανικής του University at Buffalo Στέλλα Μπαταλαμά και Δημήτρης Πάδος,απόφοιτοι του Πανεπιστημίου Πατρών. Στόχος της εφαρμογής του υποθαλασσίου ασύρματού Wi-Fiδικτύου είναι η καλύτερη συλλογή ωκεανογραφικών δεδομένων (επιτρέποντας καλύτερη συνεργασία μεταξύ ερευνητών και μειώνοντας την ανάγκη για χρήση πολλών αισθητήρων και εξοπλισμού γενικότερα). Επίσης, θα μπορούσε να φανεί πάρα πολύ χρήσιμο και στη βιομηχανία ενέργειας,καθώς ένα δίκτυο διασυνδεδεμένων συσκευών θα βοηθούσε σημαντικά για έρευνες για αέριο και πετρέλαιο. Τέλος στην Ελλάδα ο ΟΤΕ σε συνεργασία με το παγκόσμιο Wi-Fi δίκτυο της Fon φέρνει την δυνατότητα στους συνδρομητές του ΟΤΕ Double Play να συνδέονται δωρεάν στο Internet και έξω από το σπίτι τους,χρησιμοποιώντας απλά τη σύνδεσή τους.Έτσι με το ΟΤΕ My Wi-Fi δημιουργείται ένα δίκτυο φτιαγμένο από τους ίδιους τους χρήστες, οι οποίοι παρέχουν ένα μικρό μέρος της σύνδεσής τους στο παγκόσμιο δίκτυο των Wi-Fi FonSpots,με αντάλλαγμα την πρόσβαση σε αυτό εντελώς δωρεάν,σε περισσότερα από 12.000.000 σημεία σε όλον τον κόσμο.Ο εξοπλισμός του ΟΤΕ Double Play, θα εκπέμπει 2 διαφορετικά σήματα Wi-Fi. Ένα ιδιωτικό, για χρήση από τον κάτοχο της τηλεφωνικής γραμμής και μόνο και ένα δημόσιο,προσβάσιμο από άλλους συνδρομητές ΟΤΕ Double Play. Έτσι επιτρέπει με απόλυτη ασφάλεια ένα μικρό μέρος του Wi-Fi να μοιράζεται μεταξύ των συνδρομητών ΟΤΕ. Όλοι μαζί, δημιουργούν ένα δίκτυο στο οποίο όποιος συνεισφέρει,συνδέεται δωρεάν στο Internet όταν βρίσκεται εκτός σπιτιού.Το μόνο που χρειάζεσαι είναι η ΟΤΕ Double Play σύνδεσή στο Internet και ο εξοπλισμός που τη συνοδεύει.

Εικόνα: Υποθαλάσσιο Wi-Fi δίκτυο από ερευνητές του Πανεπιστήμιο του Μπάφαλο.

4.6 ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΣΤΟΝ ΑΝΘΡΩΠΟ

Όσον αφορά την επίπτωση της τεχνολογίας Wi-Fiστην ανθρώπινη υγεία το εύρος συχνοτήτων των 2,4 GHz στο οποίο λειτουργεί η τεχνολογία Wi-Fi αποτελούν μικροκύματα. Ο καθηγητής Pat Troop, της αναγνωρισμένης από την κυβέρνηση των ΗΠΑ,Υπηρεσίας Προστασίας της Υγείας (ΥΠΥ),το 2007 είχε δηλώσει**:** ¨Δεν υπάρχει καμία επιστημονική απόδειξη που να τεκμηριώνει ότι η χρήση του Wi-Fi και του WLANs επηρεάζει δυσμενώς την υγεία του πληθυσμού.Το σήμα που εκπέμπεται είναι πολύ χαμηλό, μόλις 0.1 βατ.Δεδομένου αυτού δεν υπάρχει κάποιος λόγος για τον οποίο τα σχολεία και άλλες υπηρεσίες να μην πρέπει να χρησιμοποιούν το Wi-Fi οι άλλες ασύρματες τεχνολογίες¨. Επίσης δήλωσε**:** ΄Έχουμε πολλούς επιστημονικούς λόγους για να περιμένουμε τα αποτελέσματα μιας έρευνας να είναι καθησυχαστικά και φυσικά εμείς θα δημοσιεύσουμε ό,τι κι αν μάθουμε.Τα αποτελέσματα της έρευνας θα αποτελέσουν τη βάση για μια πιο ευρεία μελέτη στις επιπτώσεις των ραδιοσημάτων στην υγεία¨.Όμως το γερμανικό υπουργείο Περιβάλλοντος πρότεινε στους πολίτες να αποφεύγουν την έκθεσή τους στην ακτινοβολία του WLAN και να επιλέγουν τις ενσύρματες συνδέσεις Διαδικτύου και ενημέρωσε ότι δραστηριοποιείται στην ενεργητική ενημέρωση των ανθρώπων για τις δυνατότητες μείωσης της ατομικής έκθεσης στις ακτινοβολίες του WLAN». Μάλιστα, στις 23-07-2007 εξέδωσε οδηγία για τη λήψη συμπληρωματικών μέτρων προφύλαξης.Επίσης ο δήμαρχος του Παρισιού, Μπερτράν Ντελανοέ, απαγόρευε από το 2007 τη χρήση του WLAN στις δημοτικές βιβλιοθήκες, γιατί ¨η συνεχής λειτουργία του εκθέτει μακροχρόνια στην ακτινοβολία του επισκέπτες και εργαζόμενους στους χώρους αυτούς¨.Η ομάδα εργασίας BioInitiative το 2007 είχε με χρονικό δείγμα 30 ετών προχωρήσει σε ανασκόπηση επιστημονικών οι οποίες τεκμηριώνουν τις βίο-επιδράσεις και τα ανεπιθύμητα αποτελέσματα στην υγεία από την έκθεση του ανθρώπου στα συγκεκριμένα ηλεκτρομαγνητικά πεδία (electromagnetic field – EMF) και συμπέρανε ότι ¨τα υφιστάμενα όρια δημόσιας ασφαλείας είναι ανεπαρκή¨.Ωστόσο όμως η πρόσφατα δημοσιευμένη έκθεση της Bioinitiative (έτος έκδοσης 2012) η οποία συγγράφηκε από 29 ανεξάρτητους επιστήμονες από ολόκληρο τον κόσμο αναφέρει ότι πλέον η κατάσταση είναι πολύ χειρότερη από αυτή που η ομάδα εργασίας είχε ¨βρει¨ για το 2007.Ο Παγκόσμιος Οργανισμός Υγείας – World Health Organization (WHO),στις αρχές του έτους 2011κατηγοριοποίησε τη ραδιενέργεια που εκπέμπεται από συσκευές όπως τα κινητά τηλέφωνα και τα ασύρματα μόντεμ Wi-Fi ως "Πιθανά Ένοχη για Καρκινογένεση στον Άνθρωπο – 'Possible Human Carcinogen' (Class 2B).Ωστόσο όμως το 99% τοις εκατό του πληθυσμού (σ.σ. pentapostagma.gr στατιστικά που αφορούν κυρίως τις Η.Π.Α) συνεχίζει να χρησιμοποιεί ασύρματα μόντεμ Wi-Fi και έτερες συσκευές ασύρματων δικτύων δίχως δεύτερη σκέψη.Πάντως, ένας ολοένα αυξανόμενος αριθμός ατόμων εγείρει έντονες ανησυχίες σχετικά με τους κινδύνους που εγκυμονεί για την υγεία η χρήση αντίστοιχων τεχνολογιών.Ανάμεσα στην ομάδα αυτών των ανθρώπων συγκαταλέγεται ο Didier Bellens ως πρόεδρος της Belgacom της μεγαλύτερης εταιρίας τηλεπικοινωνιών στο Βέλγιο.Οι ενστάσεις και οι ανησυχίες του είναι τόσο μεγάλες,ώστε δεν διστάζει να ενημερώνει με πυγμή τους συναδέλφους και οικείους

του σχετικά με τα εν λόγω ζητήματα και ειδικότερα τη νεολαία.Ο ίδιος επίσης έχει επιλέξει να εργάζεται δίχως την εγκατάσταση ασύρματου δικτύου στο γραφείο του, ενώ έχει αποκλείσει την χρησιμοποίηση κινητού τηλεφώνου – λαμβάνοντας κλήσεις μονάχα στην εταιρική τηλεφωνική γραμμή.Όπως εξηγεί ο ίδιος ο Bellens: ¨κατά τη διάρκεια της ημέρας είναι προτιμότερο να χρησιμοποιούνται ακουστικά αντί για GSM¨. Τα ραδιοκύματα είναι επικίνδυνα.Τη νύχτα είναι προτιμότερο,να απενεργοποιείται το ασύρματο μόντεμ¨.Ωστόσο σύμφωνα με την μελέτη του Δόκτορος Michael Clark της Health Protection Agency δεν υπάρχει άμεσος κίνδυνος από αυτήν την ακτινοβολία.Υποστηρίζει ότι όλες οι μελέτες που έχουν γίνει δεν έχουν αποδείξει ότι ενέχονται βλάβες για την ανθρώπινη υγεία,ενώ όσες μελέτες έχουν δείξει το αντίθετο δεν είναι καταληκτικές.Το πραγματικό πρόβλημα είναι ποιά όρια πρέπει να θεσπιστούν έτσι ώστε να ληφθούν τα κατάλληλα προληπτικά μέτρα και όρια.Επίσης με βάση τις μετρήσεις που έχουν γίνει είδαν ότι η (σχετικά) κοντινή έκθεση για διάστημα ενός έτους σε σχολεία που είχαν ασύρματα δίκτυα στις αίθουσες αποτελούσε τα 20 εκατομμυριοστά της διεθνούς προτεινόμενης οριοθέτησης (τα οποία δεν αναφέρουν ποια είναι).Για την κατανόηση του μεγέθους αυτού λέμε ότι ένα παιδί που μιλάει σε κινητό λαμβάνει,σε αντίστοιχο χρονικό διάστημα,το 50% της ίδιας οριοθέτησης.Δηλαδή ένα έτος σε τάξη με ασύρματο δίκτυο ισοδυναμεί με 20 λεπτά ομιλίας στο κινητό.Επίσης προσθέτουν,ότι αν απομακρυνθούν τα ασύρματα δίκτυα από τα σχολεία θα πρέπει να κλείσουμε και τα δίκτυα κινητής τηλεφωνίας όπως επίσης τους τηλεοπτικούς και ραδιοφωνικούς σταθμούς των οποίων οι ακτινοβολίες είναι ίσης έντασης με τα ασύρματα δίκτυα στις σχολικές αίθουσες.Ωστόσο τα επίπεδα ραδιενέργειας που εκπέμπονται από τα ασύρματα μόντεμ τεχνολογίας Wi-Fi είναι πράγματι χαμηλά.Όμως το πρόβλημα έγκειται στην φύση των συγκεκριμένων ηλεκτρομαγνητικών πεδίων.Σχετικά με την χρησιμοποίηση τεχνολογίας Wi-Fi προκύπτουν οι ανησυχίες και ο προβληματισμός που έχουν ως επίκεντρο τις ανακαλύψεις που πραγματοποίησε η Δρ. Magda Havas από το Πανεπιστήμιο Tren.Η Δρ. Havas ανακάλυψε ότι όσοι βρίσκονται σε περιβάλλον όπου χρησιμοποιούνται τεχνολογίες ασύρματων δικτύων υποφέρουν από:

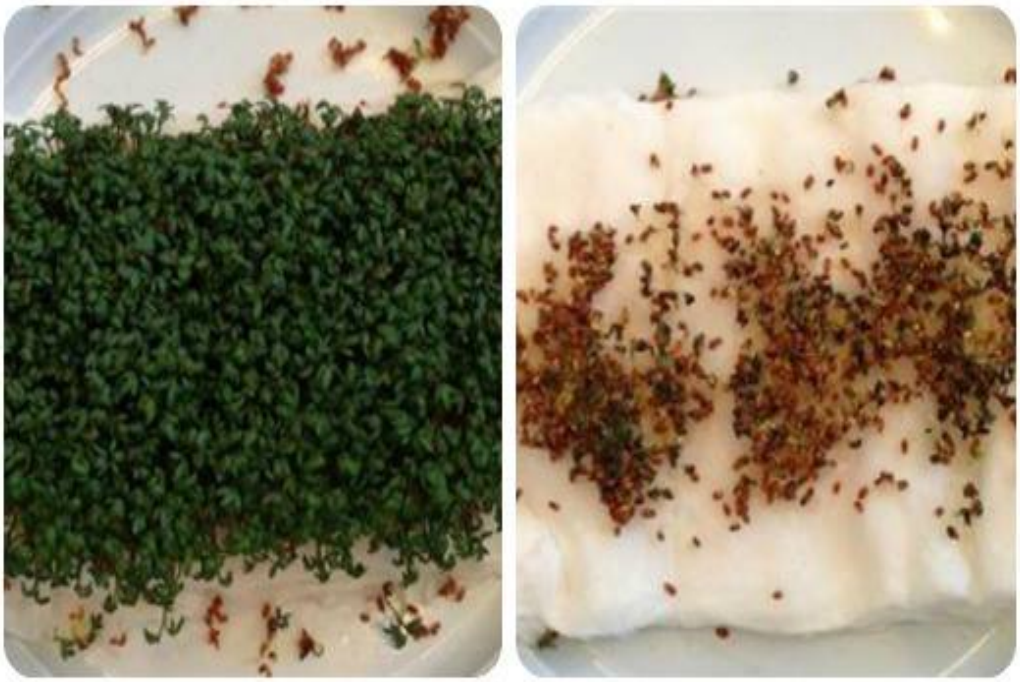
- Πονοκεφάλους,
- Ζάλη Αίσθημα αποσυντονισμού,
- Μεγάλη αύξηση των καρδιακών παλμών,
- Καρδιακή Αρρυθμία,
- Κόπωση, ναυτία και μούδιασμα.

Επίσης έρευνες έχουν δείξει ότι η έκθεση σε τεχνολογία Wi-Fi ενοχοποιείται για:

- Όξυνση της καρκινικής ανάπτυξης,
- Πρόκληση μόνιμων βλαβών στο DNA,
- Θέτει σε κίνδυνο την ομαλή λειτουργία του ανοσοποιητικού συστήματος,
- Επιδρά αρνητικά στην ανδρική γονιμότητα επηρεάζοντας τα σπερματοζωάρια.

Επίσης αποκαλυπτική είναι η πρόσφατη έρευνα του καθηγητή Βιοχημείας του Πανεπιστημίου Πατρών Χρήστου Γεωργίου (www.biology.upatras.gr/cgeorgiou), όπου καταγράφει τις συνέπειες στην υγεία από τη χρήση του WLAN,του γνωστού τηλεπικοινωνιακού συστήματος ασύρματης σύνδεσης.Παραθέτει επίσης πρωτοβουλίες και νομικές ρυθμίσεις, για την προστασία της δημόσιας υγείας,από τη διεθνή εμπειρία.Οι κεραίες του WLAN εκπέμπουν μη ιονίζουσες ηλεκτρομαγνητικές ακτινοβολίες (ΜΙΗΜΑ) με σημαντικές επιπτώσεις στην υγεία.Όπως μας εξηγεί ο καθηγητής Χρ. Γεωργίου**:** ¨οι μη θερμικές επιδράσεις οφείλονται στο γεγονός ότι ο άνθρωπος εξελίχθηκε,ως είδος, χωρίς να εκτίθεται σε παρόμοιες ακτινοβολίες (τις πρώτο-δημιούργησε τη δεκαετία του 1940) και ως εκ τούτου ο μεταβολισμός του δεν προσαρμόστηκε σε αυτές, ούτε ανέπτυξε μηχανισμό αντιμετώπισής τους: ¨Ευθύνονται για ένα μεγάλο εύρος βιολογικών βλαβών όπως καταστροφή του DNA, καρκινογενέσεις (μέσος χρόνος εμφάνισης τα 10 χρόνια, εν αντιθέσει π.χ. με τα 20 χρόνια για τον καρκίνο του πνεύμονα εξαιτίας του καπνίσματος),σκλήρυνση κατά πλάκας Αλτσχάιμερ,μείωση προσοχής,μαθησιακής ικανότητας και μνήμης, αποδυνάμωση του ανοσοποιητικού,ίλιγγοι,πονοκέφαλοι,αναπαραγωγικές δυσλειτουργίες, κ.ά.¨.Στην Ελλάδα ο ΟΤΕ αναφέρει ότι το ασύρματο δίκτυο λειτουργεί σε όρια ιδιαίτερα χαμηλά, και πιο αυστηρά από αυτά που ισχύουν διεθνώς κείμενο του γραφείου τύπου του επισημαίνει**:** ¨Τα ασύρματα δίκτυα WLAN-Wi-Fi λειτουργούν στις ζώνες συχνοτήτων(2,4 και 5,4 GHz),οι οποίες έχουν χαρακτηρισθεί παγκοσμίως ως ζώνες ελεύθερης εκπομπής για ιδιώτες ή εταιρείες.Ενδεικτικά αναφέρουμε ότι στη ζώνη αυτή λειτουργούν συσκευές μικρής εμβέλειας (π.χ. φορητοί υπολογιστές, εκτυπωτές, ακουστικά Bluetooth κ.ά.), των οποίων η χρήση καθορίζεται από το Προεδρικό Διάταγμα (ΠΔ) 44/2002 (ΦΕΚ 44/Α/7-3-2002).Στις φασματικές αυτές περιοχές συχνοτήτων ισχύουν ειδικά όρια εκπομπής ισοδύναμης ισοτροπικής ακτινοβολούμενης ισχύος (EIRP).Συγκεκριμένα στη ζώνη των 2,4 Ghz η μέση μέγιστη επιτρεπόμενη τιμή EIRP είναι 100 mW και στη ζώνη των 5,4 Ghz είναι 1W, τιμές ιδιαίτερα χαμηλές που ισχύουν διεθνώς. ¨Σχετικά με τα ζητήματα για τα όρια ασφαλούς έκθεσης σε ηλεκτρομαγνητική ακτινοβολία εξετάζονται στο ΦΕΚ 1.105/Β/6-9-2000, καθώς και στις παραγράφους 9 και 10, του άρθρου 31 του Νόμου 3.431 (ΦΕΚ 13/Α/3-2-2006) με θέμα "Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις".¨Στην Ελλάδα (Νόμος 3.431) τα όρια ασφαλούς έκθεσης του κοινού που έχουν θεσπιστεί είναι αυστηρότερα από αυτά της Ε.Ε. (αντιστοιχούν στο 70% των τιμών της Ε.Ε.), εισάγοντας έτσι έναν πρόσθετο συντελεστή ασφαλείας.Σε περίπτωση εγκατάστασης κατασκευής κεραίας επίσης η απόσταση είναι μέχρι 300 μέτρα από την περίμετρο κτιριακών εγκαταστάσεων βρεφονηπιακών σταθμών,σχολείων,γηροκομείων και νοσοκομείων,προβλέπεται περαιτέρω μείωση των ορίων ασφαλούς έκθεσης του κοινού (παράγ. 10 του άρθρου 31 του Νόμου 3.431)¨. ¨Αυτό που προκύπτει από τα παραπάνω είναι ότι στην Ελλάδα ισχύουν αυστηρότερα όρια έκθεσης από τα αντίστοιχα ευρωπαϊκά σε όλες τις ζώνες συχνοτήτων.Ο ΟΤΕ Σε κάθε περίπτωση, τηρεί τα θεσμοθετημένα όρια εκπομπής στις ζώνες λειτουργίας WLAN-Wi-Fi, ενώ παράλληλα ενημερώνεται για τα πορίσματα της επιστημονικής έρευνας που αφορούν βιολογικές επιδράσεις της ηλεκτρομαγνητικής ακτινοβολίας στον άνθρωπο και συμμορφώνεται με το ισχύον

νομικό πλαίσιο και τις εκάστοτε υποδείξεις της πολιτείας¨.Τέλος το σχολικό πείραμα στην Δανία έδειξε ότι το ασύρματου Ιντερνέτ Wi-Fiεπηρεάζει και τα φυτά που τοποθετούνται κοντά στον ρούτερ του ασύρματου Ιντερνέτ τα οποία κινδυνεύουν λόγω αυξημένης ακτινοβολίας.Στο πείραμα χρησιμοποιήθηκαν σπόροι κάρδαμου,τους οποίους οι μαθήτριες μοίρασαν σε 12 δίσκους.Τους έξι τους τοποθέτησαν δίπλα σε δύο ρούτερ Wi-Fi, και τους άλλους έξι σε ένα δωμάτιο χωρίς ακτινοβολία και τους άφησαν εκεί για ένα διάστημα 12 ημερών.Μετά το πέρας αυτού του χρονικού διαστήματος οι μαθήτριες παρατήρησαν ότι οι σπόροι που είχαν τοποθετηθεί κοντά στα ρούτερ δεν είχαν εμφανίσει κανένα απολύτως σημάδι ανάπτυξης σε αντίθεση με εκείνους που είχαν τοποθετηθεί στο «καθαρό» από πλευράς ακτινοβολίας δωμάτιο,οι οποίοι είχαν αναπτυχθεί σε υγιή φυτά.Ειδικοί ωστόσο επισημαίνουν ότι οι σπόροι που τοποθετήθηκαν κοντά στα ρούτερ ενδεχομένως να πέθαναν εξαιτίας της υψηλής θερμοκρασίας των συσκευών.Ωστόσο από την πλευρά της η δασκάλα Βιολογίας Κιμ Χόρσβαντ,στο σχολείο Hjallerup αναφέρει**:**¨Το πείραμά μας,οδήγησε στο ξέσπασμα μια ολόκληρης συζήτησης στη Δανία γύρω από τις πιθανές επιπτώσεις που θα μπορούσαν να έχουν στην υγεία μας οι συσκευές Wi-Fi ή οι συσκευές κινητών τηλεφώνων¨.Επίσης σύμφωνα με την ίδια,ένας καθηγητής νευροεπιστήμης από το Ινστιτούτο Καρολίνσκα στη Σουηδία εκδήλωσε το μεγάλο ενδιαφέρον του για τα ευρήματα του σχολικού πειράματος λέγοντας ότι θα ήθελε να το επαναλάβει, αυτή τη φορά σε ελεγχόμενο περιβάλλον εργαστηρίου.



Εικόνα: Το κάρδαμο που είχε τοποθετηθεί στο απομονωμένο από ακτινοβολία δωμάτιο στα αριστερά, και το κάρδαμο που είχε τοποθετηθεί δίπλα στους ρούτερ στα δεξιά στο σχολικό πείραμα της Δανίας.

ΕΠΙΛΟΓΟΣ

Η τεχνολογία Wi-Fi μπορεί πριν μερικά χρόνια να φάνταζε εξωπραγματική,ωστόσο πλέον σήμερα είναι γεγονός και αποτελεί την καθημερινότητα όλων και περισσότερων ανθρώπων και είναι αναμφισβήτητη σε κάθε είδους οικιακό ή εργασιακό περιβάλλον.Αναμφίβολα ο κόπος και το κόστος για το στήσιμο ενός ασύρματου δικτύου αξίζει και με το παραπάνω.Η συνεχής ανάπτυξη της εξαιτίας ορισμένων πλεονεκτημάτων της όπως η ευκολία εγκατάστασης και διαχείρισης,μεγάλη ευελιξία στη χρήση οδηγούν επίσης στη συνεχή ανάπτυξη τεχνολογιών ανταγωνιστικών μεταξύ τους.Τα ασύρματα δίκτυα λοιπόν θα παίξουν και θα παίζουν σημαντικό ρόλο στον τομέα των δικτύων με τις ταχύτητες και τις εμβέλειες να αυξάνονται συνέχεια καθώς και τα αντίστοιχα μηχανήματα να γίνονται πιο καλύτερα ποιοτικά.Ωστόσο,τα κενά της ασφάλειας σε ένα τέτοιο είδος επικοινωνίας φαίνεται να μεγαλώνουν όλο και πιο πολύ χρόνο με το χρόνο όπου η προστασία των δεδομένων έχει εξέχοντα ρόλο καθιστώντας βάσεις πάνω στις οποίες θα αναπτυχθούν οι τεχνολογίες του μέλλοντος.Παρόλο που η Ελλάδα βρίσκεται στα αρχικά στάδια ανάπτυξής του Wi-Fi,το δίκτυο Wi-Fi αναπτύσσεται με το πέρασμα του χρόνου όλο και περισσότερο.Επίσης σε όσον αφορά την συμβατότητα των διάφορων συσκευών το οποίο αποτελεί ένα ενδιαφέρον σημείο ο μη κερδοσκοπικός οργανισμός Wi-Fi Alliance και υιοθέτηση του logo γνωστοποιούν στους αγοραστές αν το προϊόν που σκοπεύει να αγοράσει είναι συμβατό με την Wi-Fi τεχνολογία και δεν θα υπάρξει πρόβλημα με συσκευές διαφορετικών συσκευαστών από την δική του. Τέλος θα πρέπει όσον αφορά τις επιπτώσεις στην υγεία και στο περιβάλλον να γίνουν πιο πολλές έρευνες και να βρεθούν με την ιλιγγιώδη ανάπτυξη της τεχνολογίας τρόποι μείωσης των κινδύνων αυτών.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ:

16-PPM (Pulse Position Modulation) Διαμόρφωση θέσης παλμών.
AP (Access Point) Σημείο πρόσβασης.Μια συσκευή ενός Wi-Fi δικτύου η οποία συνδέει τους πελάτες του δικτύου αυτού μεταξύ τους.
Ad Hoc Η λειτουργία κατά την οποία ένας υπολογιστής μπορεί να συνδεθεί σε έναν άλλον απευθείας σχηματίζοντας δίκτυο, χωρίς την παρεμβολή ενός AP.
AES (Advanced Encryption Standard) Προηγμένο πρότυπο κρυπτογραφίας.
ACK (Acknowledgment)
BPSK (Binary Phase-Shift Keying) Δυαδική μεταλλαγή μετατόπισης φάσης.
BSS (Base Service Set) Συνόλου υπηρεσιών βάσης.
CDMA (Code Division Multiple Access) Πολλαπλή προσπέλαση διαίρεσης κώδικα.
CRC (Cyclic Redundancy Code) Κώδικας ελέγχου κυκλικής πλειονότητας.
CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance) Πρωτόκολλο πολλαπλής προσπέλασης με ανίχνευση φέροντος με αποφυγή συγκρούσεων.
CTS (Clear to Send).
CCK (Complementary Code Keying) Συμπληρωματική διαμόρφωση κώδικα.
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) Πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στο WAP2 βασισμένο στονAES block chipper.
DCF (Distributed Coordination Function) Λειτουργία κατανεμημένου συντονισμού.
DFT (Discrete Fourier Transform).
DQPSK (Differential Quadric Phase-Shift Keying) Διπλή ορθογωνική μεταλλαγή μετατόπισης φάσης.
DS (Distribution Service) Υπηρεσία κατανομής.
DSSS (Direct Sequence Spread Spectrum) Εξαπλωμένο φάσμα ευθείας σκόπευσης.
DHCP (Dynamic Host Configuration Protocol).
ESS (Extended Service Set) Εκτεταμένο σύνολο υπηρεσιών.
EAP (Extensible Authentication Protocol).
ΕΔΕΤ (Εθνικό Δίκτυο Έρευνας και Τεχνολογίας).
FDM (Frequency Division Multiplexing) Πολυπλεξία διαίρεσης συχνότητας.
FHSS (Frequency Hopping Spread Spectrum) Εξαπλωμένο φάσμα αναπήδησης συχνότητας.
FSK (Frequency Shift Keying) Μεταλλαγή μετατόπισης συχνότητας.
GFSK (Gaussian Frequency Shft Keying) Γκαουσιανή μεταλλαγή μετατόπισης συχνότητας.
GPS (Global Positioning System) Παγκόσμιο σύστημα εντοπισμού.
IEEE (Institute of Electrical and Electronic Engineering) Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών.
IFS (Interframe Space) Διάστημα interframe.
IP (Internet Protocol) Πρωτόκολλο διαδικτύου.
IR (InfraRed) Υπέρυθρες.
ISO (International Standards Organization) Διεθνής Οργανισμός Προτύπων.
IV (Initialization Vector) Διάνυσμα εκκίνησης.
LLC (Logical Link Control) Έλεγχος λογικής ζεύξης.
MAC (Medium Access Control sub layer) Υπόστρωμα ελέγχου πρόσβασης στο μέσο μετάδοσης.
Mbps (Megabits per second).
MPDU (MAC Protocol Data Unit) Μονάδα δεδομένων πρωτοκόλλου MAC.
MU-MIMO (Multi User – Multiple Input Multiple Output).

MIC (Message Integrity Code) Παράγεται από τον αλγόριθμο Michael και προσαρτάται στηνplaintextγια έλεγχο της ακεραιότητας της.
ΜΙΗΜΑ Μη ιονίζουσες ηλεκτρομαγνητικές ακτινοβολίες.
NIC (Network Interface Card) Κάρτα δικτύου.
NAV (Network Allocation Vector).
OFDM (Orthogonal Frequency Division Method) Μέθοδος ορθογώνιας διαίρεσης συχνότητας.
OSI (Open Systems Interconnection-reference model) Πρότυπο αναφοράς για τη διασύνδεση ανοιχτών συστημάτων.
PDA (Personal Digital Assistant) Προσωπικός ψηφιακός βοηθός.
PRNG (Pseudo-Random Number Generator) Γεννήτρια ψευδοτυχαίων αριθμών.
PSK (Pre-Shared Key).
QoS (Quality of Service) Ποιότητα υπηρεσίας.
QPSK (Quadric Phase-Shift Keying) Ορθογωνική μεταλλαγή μετατόπισης φάσης.
ΟΤΕ (Οργανισμός Τηλεπικοινωνιών Ελλάδας).
RF (Radio Frequency) Ραδιοσυχνότητα.
RTS (Ready to Send).
ΣΑΠ (Σταθερής Ασύρματης Πρόσβασης).
ΣΤΑΣΥ(ΣΤΑΘΕΡΕΣ ΣΥΓΚΟΙΝΩΝΙΕΣ Α.Ε.).
TDM (Time Division Multiplex) Πολυπλεξία διαίρεσης χρόνου.
TDMA (Time-Division Multiple Access) Πολλαπλή πρόσβαση διαίρεσης χρόνου.
TKIP (Temporal Key Integrity Protocol) Πρωτόκολλο προσωρινής ακεραιότητας κλειδιού.
TCP/IP (Transport Control Protocol/ Internet Protocol) Πρωτόκολλο ελέγχου μεταφοράς/ Πρωτόκολλο διαδικτύου.
VPN (Virtual Private Network).
WEP (WiredEquivalentPrivacy).
WPA (Wi-Fi Protected Access).
WAP2 (Wi-Fi Protected Access 2).
WIFI (Wireless Fidelity) Ασύρματη αξιοπιστία.
WLAN (WirelessLocalAreaNetwork) Ασύρματο τοπικό δίκτυο.
WMAN (Metropolitan Area Network) Ασύρματο Μητροπολιτικό δίκτυο.
WWAN (Wireless Wide Area Network) Ασύρματο Δίκτυο ευρείας περιοχής.
WHO (World Health Organization**)** Παγκόσμιος Οργανισμός Υγείας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Tanenbaum, Andrews 2004 Fourth Edition. «Δίκτυα Υπολογιστών», Εκδόσεις «Κλειδάριθμος».

Χρήστος Ι. Μπούρας 2004 «Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων» Πανεπιστημιακές Σημειώσεις.

ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ WilliamStallingsΕκδόσεις «Τζιόλα».

Ασύρματα Δίκτυα Υπολογιστών Ασφάλεια και Απόδοση των Πρωτοκόλλων TCP/IP Νικόλαος Πρέβες Εκδόσεις «Νέων Τεχνολογιών».

Wireless Communication Standards A study of IEEE 802.11, 802.15 and 802.16 Todor Cooklev.

Wireless and Mobile Data Network Aftab Ahmad.

ΤΟΠΙΚΑ ΚΑΙ ΑΣΤΙΚΑ ΔΙΚΤΥΑ (LAN-MAN) Σπυριδούλα Μαργαρίτη-Ελευθέριος Στεργίου Εκδόσεις «Νέων Τεχνολογιών».

ΙΣΤΟΣΕΛΙΔΕΣ:

http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

http://www.smarteck.gr/info_wlan.html

http://www.mediamarkt.gr/mp/article/WLAN,970024.html

http://en.wikipedia.org/wiki/Wireless_LAN#Peer-to-peer

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

http://searchenterprisewan.techtarget.com/definition/wireless-WAN

http://www.wisegeek.com/what-is-a-wwan.htm

http://en.kioskea.net/contents/833-wireless-metropolitan-area-networks

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

http://el.wikipedia.org/wiki/%CE%9C%CE%BF%CE%BD%CF%84%CE%AD%CE%BB%CE%BF_%CE%B1%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82_OSI

http://www.aic.gr/%CE%B1%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%B1-%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%B1/

http://users.sch.gr/pepoudi/site/pages/page12.html

http://el.wikipedia.org/wiki/Wi-Fi

http://www.epaggelmaties.com/writer/2001-2003/teyxos222.html

http://www.news4tech.com/product_info.php?products_id=67

http://www.plusnet.gr/article.php?id=94

http://www.dalailaptop.gr/%CE%B2%CE%B1%CF%83%CE%B9%CE%BA%CE%AC-%CE%BC%CE%B5%CE%B9%CE%BF%CE%BD%CE%B5%CE%BA%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1-%CF%84%CE%BF%CF%85-%CE%B1%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF%CF%85-%CE%B4/

http://pcex.gr/index.php?option=com_content&task=view&id=37&Itemid=43

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

http://plinet.kas.sch.gr/saferinternet/index.php/asfaleia-se-asyrmata-diktya-wi-fi

http://www.tutorial-reports.com/wireless/wlanwifi/security_wifi.php

http://olagiatopc.blogspot.gr/2011/03/wifi-modems.html

http://www.pentapostagma.gr/2013/11/eseis-gnwrizete-tous-kindynous-gia-thn-ygeia-apo-thn-xrhsh-twn-asyrmatwn-diktywn.html#.U3pobtJ_tPd

http://minotavrs.blogspot.gr/2011/08/wifi-100.html

http://www.dealnews.gr/roi/item/503-%CE%93%CE%B5%CE%B3%CE%BF%CE%BD%CF%8C%CF%82-%CE%BF%CE%B9-%CF%85%CF%80%CE%B5%CF%81%CE%B1%CF%84%CE%BB%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AD%CF%82-%CF%80%CF%84%CE%AE%CF%83%CE%B5%CE%B9%CF%82-%CE%BC%CE%B5-WiFi,-%CE%BA%CE%BF%CE%B9%CF%84%CE%AC%CE%B6%CE%B5%CE%B9-%CF%84%CE%BF-%CE%BC%CE%AD%CE%BB%CE%BB%CE%BF%CE%BD-%CE%B7-Lufthansa

www.ote.gr/web/guest/consumer/products-services/ote-my-wifi?gclid=CNzeir3Rh70CFSsKwwodyBAAFw

http://www.tovima.gr/science/technology-planet/article/?aid=549858

http://www.sepe.gr/default.aspx?pid=34&la=1&artID=4794

http://www.unblogger.gr/2013/10/ypobrixio-wi-fi-gia-thalassio-Internet.html

http://2epal-n-smyrn.att.sch.gr/files/texn_site/texn2.htm

http://www.techgear.gr/qualcomm-mu-mimo-technology-triples-wifi-speeds-87126/

http://www.imerisia.gr/article.asp?catid=27340&subid=2&pubid=129544143

http://news.in.gr/greece/article/?aid=1231306271

http://www.real.gr/DefaultArthro.aspx?page=arthro&id=270267&catID=22

http://www.aic.gr/%CE%B1%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%B1-%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%B1/

http://www.iefimerida.gr/news/128618/%CE%B3%CE%B9%CE%B1-%CF%80%CF%81%CF%8E%CF%84%CE%B7-%CF%86%CE%BF%CF%81%CE%AC-%CE%B1%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF-%CE%AF%CE%BD%CF%84%CE%B5%CF%81%CE%BD%CE%B5%CF%84-%CF%83%CF%84%CE%BF-%CE%B2%CF%85%CE%B8%CF%8C-%CF%84%CE%B7%CF%82-%CE%B8%CE%AC%CE%BB%CE%B1%CF%83%CF%83%CE%B1%CF%82-wi-fi-

%CE%BC%CE%B1%CE%B6%CE%AF-%CE%BC%CE%B5-%CF%84%CE%BF-%CE%BC%CE%B1%CE%B3%CE%B9%CF%8C-%CE%B5%CE%B9%CE%BA%CF%8C%CE%BD%CE%B5%CF%82

http://www.unblogger.gr/2013/10/ypobrixio-wi-fi-gia-thalassio-Internet.html#.U3pn99J_tPc

http://www.alopsis.gr/modules.php?name=News&file=article&sid=1011

http://www.modnet.gr/%CE%B1%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%B1-%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%B1-%CF%87%CF%81%CE%B7%CF%83%CE%B9%CE%BC%CF%8C%CF%84%CE%B7%CF%84%CE%B1/

http://www.in2life.gr/everyday/modernlife/article/334515/elefthero-wi-fi-pleon-kai-sto-metro.html