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

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Τεχνολογίες Πρωτοκόλλων ασύρματων Τοπικών Δικτύων Υπολογιστών

Του φοιτητή

Θεοδουλίδη Στέφανου

Αρ. Μητρώου: 113719

Επιβλέπων καθηγητής

Βίτσας Βασίλειος

Θεσσαλονίκη 2018

ΠΡΟΛΟΓΟΣ

Τα ασύρματα LAN, που έχουν πλέον διεισδύσει στον χώρο εργασίας, στο σπίτι, στα εκπαιδευτικά ιδρύματα, στις καφετέριες, στα αεροδρόμια και στις γωνίες των δρόμων, είναι η σημαντικότερη τεχνολογία δικτύων προσπέλασης στο Διαδίκτυο σήμερα. Αν και έχουν αναπτυχθεί πολλές τεχνολογίες και πρότυπα για ασύρματα LAN, κατά τη δεκαετία του ’90, μια συγκεκριμένη κατηγορία πρότυπων είχε σαφώς κυριαρχήσει: το ασύρματο LAN IEEE 802.11 (IEEE 802.11 wireless LAN), επίσης γνωστό ως WiFi. Παρότι το WLAN χρησιμοποιεί ραδιοκύματα και όχι καλώδια, εφαρμόζεται κυρίως σε switched network περιβάλλοντα και η μορφή του πακέτου του είναι παρόμοιο με εκείνου που χρησιμοποιείται από το Ethernet.

Τα WLANs χρησιμοποιούνται καθημερινά από τους ανθρώπους για πολλές και διαφορετικές χρήσεις, όμως απαιτείται πολύ περισσότερη προσοχή και ασφάλεια καθώς είναι πιο ευάλωτα σε σχέση με τα παραδοσιακά LAN δίκτυα.

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας πτυχιακής εργασίας είναι η παρουσίαση της WLAN τεχνολογίας και των πρωτοκόλλων που χρησιμοποιούνται στα ασύρματα δίκτυα. Συγκεκριμένα, γίνεται αναφορά στη δημιουργία και στη χρήση των WLANs όπως επίσης και στις διάφορες που παρουσιάζονται ανάμεσα στα WLANs και στα LANs. Παρουσιάζονται αναλυτικά τα πρωτόκολλα των ασυρμάτων δικτύων της οικογενείας IEEE 802.11 και δίνεται ιδιαίτερη έμφαση στην αρχιτεκτονική και τους μηχανισμούς που χρησιμοποιούνται στο φυσικό επίπεδο καθώς και στο MAC επίπεδο. Τέλος, παρουσιάζονται οι απειλές που είναι δυνατό να δεχθεί ένα ασύρματο δίκτυο καθώς και οι τεχνικές άμυνας που χρησιμοποιούνται είτε για να αντιμετωπίσουν είτε για να προλαμβάνουν τις παραπάνω απειλές.

ABSTRACT

The purpose of this thesis is to present of the WLAN technology and the protocols which used in wireless networks. In particular, we make an introduction to the creation and the use of the WLANs as well in differences which exist between WLANs and LANs. We present analytically the IEEE 802.11 and all protocols of the same family and particular emphasis is placed in architectonic and the mechanism which used on physical layer and MAC layer. Finally, we refer to the threats which are use to received by a wireless network and the countermeasures which used to face or to prevent these threats.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευρετήριο σχημάτων

Ευρετήριο πινάκων

ΕΙΣΑΓΩΓΗ

Ο στόχος αυτής της πτυχιακής εργασίας είναι να περιγράψει τα ασύρματα τοπικά δίκτυα και τους μηχανισμούς αλλά και τα πρωτοκολλά που δημιουργήθηκαν για να τα υποστηρίξουν με σκοπό την βέλτιστη δυνατή ποιότητα στην επικοινωνία.

Στο πρώτο κεφάλαιο πραγματοποιείται η γενική παρουσίαση των WLANs για το πώς δημιουργήθηκαν, για το πώς και που χρησιμοποιούνται και τέλος πραγματοποιείται μια σύγκριση ανάμεσα στα WLANS και στα LANs.

Στο δεύτερο κεφάλαιο παρουσιάζονται όλα τα πρωτοκολλά που δημιουργήθηκαν για να υποστηρίξουν τα WLANs.

Στο τρίτο κεφάλαιο αναλύονται τα διαφορετικά φυσικά επίπεδα των WLANs και τους μηχανισμούς που χρησιμοποιούνται σε αυτά.

Στο τέταρτο κεφάλαιο αναφερόμαστε στο MAC επίπεδο και τους μηχανισμούς που χρησιμοποιούνται

Τέλος, στο πέμπτο κεφάλαιο γίνεται μια παρουσίαση των κινδύνων που υπάρχουν στα WLANs δίκτυα καθώς και τους μηχανισμούς που χρησιμοποιούνται για την αντιμετώπιση αλλά και της πρόληψης που θα πρέπει να υπάρχει.

ΚΕΦΑΛΑΙΟ 1
ΤΕΧΝΟΛΟΓΙΑ WLAN

ΕΙΣΑΓΩΓΗ

Τα ασύρματα δίκτυα μπορούν να προσφέρουν στους χρήστες την κινητικότητα, δηλαδή την ικανότητα να συνδέονται από οποιαδήποτε τοποθεσία και όποτε το

επιθυμούν καθώς και την ικανότητα να παραμένουν συνδεδεμένοι ενώ μετακινούνται. Το WLAN είναι ένα ασύρματο δίκτυο που χρησιμοποιείται συνήθως σε σπίτια, γραφεία και σε πανεπιστήμια. Μολονότι, χρησιμοποιούνται ραδιοκύματα αντί για καλώδια, το WLAN εφαρμόζεται σε switched network περιβάλλοντα και η μορφή του πακέτου του είναι παρόμοια με εκείνη του Ethernet.

Σε αυτό το κεφάλαιο αυτό θα πραγματοποιήσουμε μια ιστορική αναδρομή στα WLANs, θα εμβαθύνουμε στη χρήση τους καθώς και θα συγκρίνουμε τα WLANs με τα LANs.

1.1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Στις αρχές του 21ου αιώνα, τα ασύρματα τοπικά δίκτυα (WLAN) προσέλκυσαν ένα τεράστιο μέρος της προσοχής της βιομηχανίας της κινητής τηλεφωνίας και πολλοί θεωρήσαν ότι θα είναι μια τεχνολογία που θα μπορούσε να ανταγωνιστεί και να απειλήσει το ήδη υπάρχον λειτουργικό μοντέλο που βασίζονταν σε δίκτυα κινητής τηλεφωνίας και πίστευαν ότι θα βλάψει ιδιαίτερα τις 3G επενδύσεις.

Την ίδια στιγμή κάποιοι άλλοι ειδικοί δεν υποστήριζαν αυτήν την άποψη τονίζοντας ότι τα WLANs είχαν διαφορετικές λειτουργείες από τα δίκτυα κινητής τηλεφωνίας (διαφορετικό εύρος, throughput και ο τύπος των συσκευών που χρησιμοποιούν για να έχουν πρόσβαση στο δίκτυο) και θα μπορούσαν να χρησιμοποιηθούν από τους φορείς εκμετάλλευσης ως συμπλήρωμα, παρά ως μια εναλλακτική λύση, στα δίκτυα κινητής τηλεφωνίας.

Η προέλευση των WLANs πηγαίνει πίσω στο 1990 όπου η IEEE προσπαθούσε να δημιουργήσει ένα WLAN πρότυπο. Ωστόσο, η ζήτηση ήταν αρχικά στάσιμη λόγω των υψηλών τιμών του εξοπλισμού, των χαμηλών επιδόσεων και τις ανησυχίες για προβλήματα ασφάλειας και για έλλειψη διαλειτουργικότητας, κάτι το οποίο άλλαξε με το πρότυπο 802.11 όπου επιτεύχθηκε η διαλειτουργηκοτητα ανάμεσα σε συσκευές διαφορετικών κατασκευαστών και ειδικότερα με το πρότυπο 802.11b το 1999 στο οποίο βελτιώθηκε ακόμα περισσότερο η απόδοση, όπως επίσης και η πιστοποίηση διαλειτουργικότητας που παρείχε η WECA (μετονομάστηκε σε Wi-Fi alliance το 2002). Η βελτιωμένη απόδοση και η διαλειτουργικότητα των προϊόντων οδήγησε στην ευρύτερη χρήση τους και κατά συνέπεια άρχισε η ραγδαία μείωση των τιμών κάτι το οποίο κατέστησε δυνατή την ραγδαία αύξηση στην δημιουργία των private WLAN από τις επιχειρήσεις και τους οικιακούς καταναλωτές ως μια επέκταση ή αντικατάσταση των παραδοσιακών LANs.

Παράλληλα, η διάχυση του WLAN διευρύνεται σε συμβατικές συσκευές όπως τα κινητά τηλέφωνα και τα tablets, δημιουργώντας μια ευκαιρία να προσφέρουν WLAN access σε νομαδικούς χρήστες σε δημόσιες περιοχές. Συγκεκριμένα, τα τρία τελευταία χρόνια παρατηρήθηκε μια αρχική ασάφεια στη λειτουργεία των δημόσιων δικτύων WLAN από διάφορους τύπους παροχών όπως της κινητής τηλεφωνίας και παραδοσιακούς φορείς εκμετάλλευσης δικτύων, Internet Service Providers και ασύρματες κοινότητες.

1.2 ΧΡΗΣΗ ΚΑΙ ΛΕΙΤΟΥΡΓΕΙΑ ΤΩΝ WLANs

Όσο η ασύρματη δικτύωση κερδίζει πόντους και παράλληλα οπαδούς σε σχέση με την ενσύρματη, τόσο το ασύρματο LAN (local area network) έχει γίνει ένα από τα πιο δημοφιλή περιβάλλοντα δικτύου.

Οι εταιρίες και οι ιδιώτες έχουν υπολογιστές που συνδέονται με local area networks (LANs). Ο LAN χρήστης έχει στη διάθεση του πολλές περισσότερες πληροφορίες, δεδομένα και εφαρμογές σε αντίθεση με αυτά που θα μπορούσε να αποθηκεύσει μόνος του. Η ασύρματη τεχνολογία βοήθησε στο να απλοποιηθεί η δικτύωση επιτρέποντας πολλαπλούς υπολογιστικούς χρήστες να μοιράζονται ταυτόχρονα τους πόρους σε ένα σπίτι ή μια επιχείρηση χωρίς την χρήση επιπλέον καλωδίωσης. Η αυξανόμενη ζήτηση για φορητότητα στην καθημερινότητα μας είναι το ζήτημα που οδήγησε στην ανάπτυξη των ασύρματων δικτύων.

Σύμφωνα με την αναφορά της CISCO το 2000 τα ασύρματα τοπικά δίκτυα (WLAN) κάνουν ακριβώς αυτό που δηλώνει το όνομα τους: προσφέρουν όλα τα χαρακτηριστικά και τα οφέλη των παραδοσιακών LAN τεχνολογιών όπως το Ethernet και το Token Ring χωρίς τον περιορισμό των καλωδίων. Προφανώς, εξ ορισμού το WLAN είναι το ίδιο με το LAN αλλά χωρίς την έννοια του καλωδίου.

Η WLAN τεχνολογία ενώνει δυο ή περισσότερες συσκευές χρησιμοποιώντας την ασύρματη μέθοδο επικοινωνίας. Συνήθως προσφέρει μια σύνδεση μέσω ενός Access Point (AP) στο ευρύτερο internet.

Αυτό προσφέρει στους χρήστες την ικανότητα να μετακινούνται μέσα σε μια τοπική περιοχή κάλυψης του σήματος που προσφέρει ένα access point ενώ εξακολουθούν να είναι συνδεδεμένοι στο δίκτυο, αν όμως σε περίπτωση που εξέλθουν από την περιοχή κάλυψης του access point τότε είτε χάνουν την σύνδεση στο διαδίκτυο είτε εισέρχονται στην περιοχή κάλυψης ενός άλλου access point άμα είναι διαθέσιμο.

Η υποδομή δεν χρειάζεται να είναι θαμμένη στο έδαφος ή κρυμμένη πίσω από τοίχους (καλώδια), άρα οι χρήστες μπορούν να μετακινηθούν πολύ πιο εύκολα

μέσα στην περιοχή κάλυψης από ότι σε περίπτωση που χρησιμοποιούσαν ενσύρματη επικοινωνία.

Οι τρεις βασικοί λόγοι που χρησιμοποιούνται τα wireless LANs είναι:

- Ο αυξανόμενος αριθμός των LAN χρηστών που γίνεται κινητός, για παράδειγμα οι χρήστες που χρησιμοποιούν tablet, smartphone και laptops. Αυτοί οι κινητοί χρήστες απαιτούν να είναι συνδεδεμένοι στο δίκτυο ανεξάρτητα με το που βρίσκονται επειδή θέλουν ταυτόχρονη πρόσβαση στο δίκτυο. Αυτό κάνει την χρήση των καλωδίων ή τον ενσύρματων LAN μη πρακτική αν όχι αδύνατη.
- Η εγκατάσταση των ασύρματων LANs είναι πολύ εύκολη. Δεν απαιτείται δικτύωση σε κάθε σταθμό και σε κάθε δωμάτιο. Αυτή η ευκολία στην εγκατάσταση καθιστά τα ασύρματα LANs εκ φύσεως ευέλικτα. Αν ένας σταθμός πρέπει να μεταφερθεί, μπορεί να πραγματοποιηθεί η μετακίνηση εύκολα και χωρίς επιπλέον καλωδίωση και χωρίς επιπλέον ρύθμιση στο δίκτυο.

Ένα ακόμα λόγος για την χρησιμοποίηση του WLAN είναι η φορητότητα του. Αν μια εταιρία μετακινηθεί σε νέα περιοχή, το ασύρματο σύστημα είναι πολύ πιο εύκολο να μετακινηθεί σε αντίθεση με το να ξηλωθούν όλα τα καλώδια.

1.3 ΣΥΓΚΡΙΣΗ ΤΗΣ WIRED ΜΕ ΤΗΝ WIRELESS ΤΕΧΝΟΛΟΓΙΑ

Τα WLANs έχουν παρόμοια προέλευση με τα Ethernet LANs. Τα δύο κυρίαρχα 802 working groups είναι το 802.3 Ethernet και το 802.11 WLAN. Υπάρχουν πολλές και σημαντικές διαφορές ανάμεσα σε αυτά τα δυο.

Τα WLANs χρησιμοποιούν ραδιοκύματα (με εξαίρεση την τεχνολογία των υπέρυθρων- infrared) και όχι καλώδια στο physical layer. Τα ραδιοκύματα έχουν τα εξής χαρακτηριστικά:

- Έχουν όρια, όπως και το καλώδιο, δηλαδή ο χρήστης που λαμβάνει τα πακέτα πρέπει να βρίσκεται μέσα στην περιοχή κάλυψης του access point.
- Τα ραδιοκύματα είναι απροστάτευτα στα εξωτερικά σήματα, σε αντίθεση με τα καλώδια που έχουν ένα μονωτικό περίβλημα. Άρα

χρησιμοποιώντας την ίδια ή παρόμοια ραδιοσυχνότητα μπορεί να προκληθούν παρεμβολές στην επικοινωνία.

- Τα WLANs συνδέουν τον client στο δίκτυο μέσο ενός ασύρματου access point, σε αντίθεση με τα LANs που χρησιμοποιούν ένα Ethernet switch.

Τα WLANs επίσης διαφέρουν από τα LANs στα παρακάτω:

- Τα WLANs συνδέουν κινητές συσκευές που συνήθως λειτουργούν με μπαταρία, σε αντίθεση με τα LANs που συνδέουν συσκευές οι οποίες είναι συνδεδεμένες στο ρεύμα. Οι ασύρματες κάρτες δικτύου τείνουν να μειώνουν την ζωή της μπαταρίας μιας ασύρματης συσκευής.
- Τα WLANs όπως και τα ενσύρματα LANs υποστηρίζουν σταθμούς που αγωνίζονται για να έχουν πρόσβαση στο μέσο μετάδοσης. Το 802.11 όμως προβλέπει έναν μηχανισμό αποφυγής συγκρούσεων (CSMA/CA) σε αντίθεση με το μηχανισμό ανίχνευσης συγκρούσεων που υπάρχει στα LANs (CSMA/CD) για να επιτρέπει την πιο ασφαλή πρόσβαση στο μέσο μειώνοντας την πιθανότητα να υπάρξει σύγκρουση.
- Τα WLANs χρησιμοποιούν διαφορετική μορφή στα πακέτα σε σχέση με τα ενσύρματα Ethernet LANs. Τα WLANs απαιτούν επιπλέον πληροφορία στη κεφαλίδα του πακέτου στο layer 2, καθώς εμπεριέχονται τέσσερα πεδία διευθύνσεων σε σχέση με τον Ethernet Lan header που περιέχει δυο πεδία διευθύνσεων.
- Τα WLANs αυξάνουν τα θέματα ιδιωτικότητας επειδή τα ραδιοκύματα μπορούν να φτάσουν και εκτός των εγκαταστάσεων.

Πίνακας 1 "WLANs versus LANs"

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential

ΕΠΙΛΟΓΟΣ

Στο προηγούμενο κεφάλαιο αναφερθήκαμε στη δημιουργία καθώς και την εξέλιξη των WLANs και τις δυσκολίες που παρατηρήθηκαν, δώσαμε έμφαση στην χρήση και στη καίρια χρησιμότητα που έχουν τα WLANs στα στην καθημερινότητα και τις διάφορες που έχουν τα WLANS με τα LANs όπως επίσης τονίσαμε τα χαρακτηρίστηκα των ραδιοκυμάτων.

Στο επόμενο κεφάλαιο θα υπάρξει μια εκτενή απεικόνιση των χαρακτηριστικών και της χρήσης που έχουν πολλά ασύρματα πρότυπα.

ΚΕΦΑΛΑΙΟ 2

Πρότυπα ασύρματων δικτύων

ΕΙΣΑΓΩΓΗ

Τα IEEE 802.11 WLAN πρότυπα καθορίζουν πως χρησιμοποιούνται τα ραδιοκύματα σε κάθε συχνότητα για το φυσικό επίπεδο και για το MAC υπό-επίπεδο των ασυρμάτων δικτυών. Στο παρακάτω κεφάλαιο θα κάνουμε μια χρονολογική αναδρομή στα ασύρματα πρότυπα δικτύων και θα γίνει μια εκτενής αναφορά στη χρήση τους και τις καινοτομίες του καθενός.

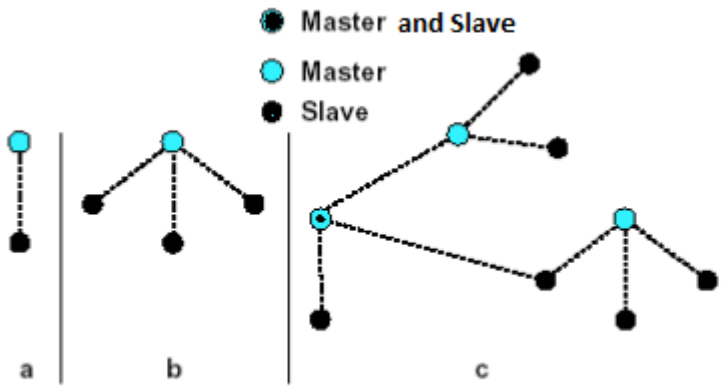
2.1 Bluetooth (1990)

Το όνομα Bluetooth προήλθε από τον Δανό βασιλιά Harald Blåtand(Bluetooth). Ο βασιλιάς Bluetooth πιστώθηκε την ένωση των Σκανδιναβικών χωρών κατά τον 10ό αιώνα. Όμοια το Bluetooth στοχεύει στην ένωση των προσωπικών συσκευών. Αυτό το όνομα αρχικά επιλέχθηκε προσωρινά ,ωστόσο η αναζήτηση ενός νέου ονόματος δεν ήταν επιτυχής.

Η ανάπτυξη του βιομηχανικού προτύπου Bluetooth ξεκίνησε τον χειμώνα του 1998 όταν η Ericson, IBM, Intel, Nokia και η Toshiba σχημάτισαν το Bluetooth Special Industrial Group (SIG)με σκοπό την σχεδίαση και την διάδοση μιας παγκόσμιας low cost λύσης για short-range ασύρματη επικοινωνία που λειτουργεί στα 2,4GHz με σκοπό την αποφυγή των καλωδίων ανάμεσα σε προσωπικές συσκευές.

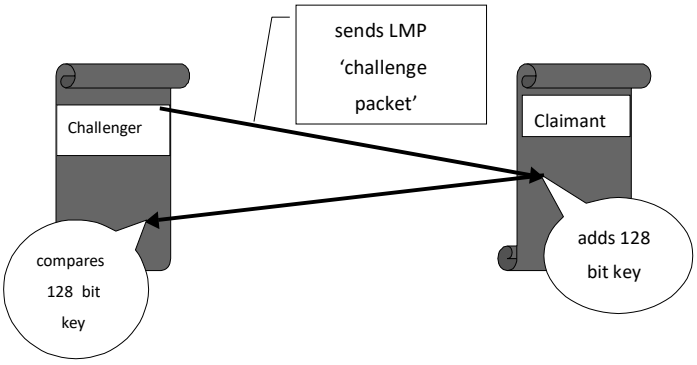
Για να διευκολυνθεί η ευρεία αποδοχή αυτής της νέας τεχνολογίας ,η SIG αποφάσισε να προσφέρει όλη την πνευματική ιδιοκτησία συμπεριλαμβανόμενων και των προδιαγραφών του Bluetooth σε όλα τα μέλη της τεχνολογίας είτε συμμετείχαν στην SIG είτε όχι, με σκοπό την εισαγωγή Bluetooth προϊόντων στην αγορά.

Το Bluetooth χρησιμοποιεί την 2.4GHz ISM (industrial,scientific,medical) μπάντα επειδή είναι αδήλωτη δηλαδή μπορεί να χρησιμοποιηθεί στις περισσότερες χώρες για οποιαδήποτε χρήση χωρίς να χρειάζεται κάποια άδεια. Σε αυτήν την συχνότητα, μια πολύ μικρή κεραία είναι ικανοποιητική. Το Bluetooth παρέχει point-to-point και point-to-multipoint συνδέσεις. Αρκετές συσκευές που χρησιμοποιούν Bluetooth μοιράζονται το ίδιο κανάλι επικοινωνίας. Η συσκευή η οποία αρχίζει την σύνδεση λειτουργεί σαν master και μπορεί να έχει μέχρι και 7 ενεργούς slaves και 256 ανενεργούς. Σαν συσκευές ο master και ο slave είναι ίδιες. Ένας master και ένας slave μπορεί κάποιες φορές να αλλάξουν ρόλους, επίσης ένας master μιας σύνδεσης μπορεί να είναι slave σε μια άλλη σύνδεση. Το Bluetooth παρέχει την δυνατότητα δημιουργίας ad-hoc δικτύων, δηλαδή δικτύων στα οποία κάθε συσκευή Bluetooth μπορεί να συνδεθεί με μια άλλη χωρίς τη ν ανάγκη για οποιαδήποτε υποστηρικτική υποδομή. Οι slaves δεν μπορούν να επικοινωνήσουν απευθείας μεταξύ τους, αν το θέλουν μπορούν να δημιουργήσουν μια δικιά τους ξεχωριστή σύνδεση master- slave. Κάθε Bluetooth συσκευή έχει μια μοναδική 48-bit Bluetooth Device Address, η οποία περιέχει τρία διαφορετικά μέρη: Lower address part (24 bits), Upper address part (8 bits) και Nonsignificant address part (16 bits). Κάθε Bluetooth κανάλι έχει περίπου 1 Mbps data rate.Στο μέλλον είναι πολύ πιθανόν το data rate να φτάσει στα 10 Mbps για να παρέχεται επίσης και η υπηρεσία του real time video.



Σχήμα 2 "Bluetooth Network Topology"

Το Bluetooth προσφέρει κάποιες λειτουργείες ασφάλειας. Δεν χρησιμοποιεί κρυπτογράφηση με δημόσιο κλειδί, αλλά χρησιμοποιεί κοινόχρηστο μυστικό κλειδί. Για την αυθεντικοποίηση το κλειδί είναι 128 bits, η συσκευή που ξεκινάει την δοκιμασία(challenger), στέλνει την δοκιμασία στην άλλη συσκευή(claimant) η οποία προσθέτει το 128 bit κλειδί και επιστρέφει το πακέτο.Ο challenger κάνει το ίδιο τοπικά και συγκρίνει τις δυο εκδοχές(αυτήν που δημιούργησε ο ίδιος και αυτή που δημιούργησε ο claimant).Αν και οι δυο χρησιμοποιούν το ίδιο κλειδί αύτη η διαδικασία θα πιστοποιήσει την δοκιμαζομένη συσκευή.



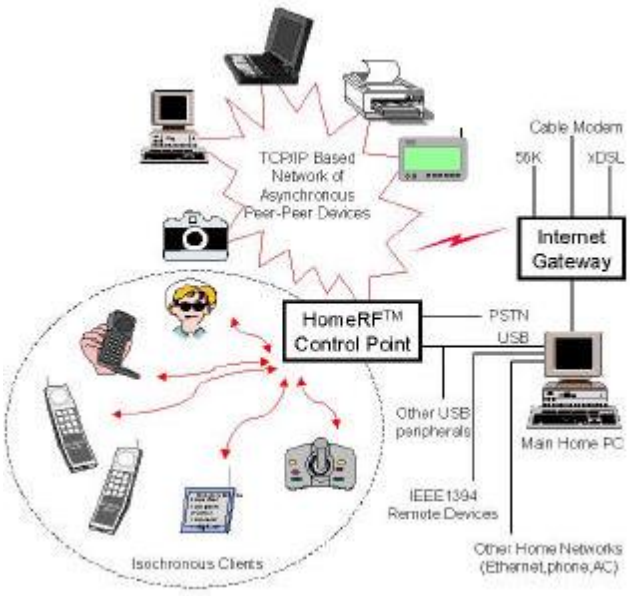
Σχήμα 2 "Authentication (LMP=Link)"

Μετά την επιτυχή αυθεντικοποίηση, θα ακολουθήσει η κρυπτογράφηση της σύνδεσης. Η κρυπτογράφηση χρησιμοποιεί ένα κλειδί όχι μεγαλύτερο από 128 bits.Το ανώτερο όριο ελέγχεται σε πολλές χώρες από τους νόμους του κράτους, Το κλειδί της κρυπτογράφησης αλλάζει σε κάθε πακέτο που μεταδίδεται. Η ασφάλεια που παρέχεται φέρεται να είναι επαρκής για οικονομικές συναλλαγές.

2.2 Home RF (1998-2003)

Το HomeRF Working group είναι μια κοινοπραξία με πάνω από 100 εταιρίες από τη βιομηχανία της πληροφορικής και επικοινωνίας. Αυτή η ομάδα δημιούργησε μια ανοιχτή προδιαγραφή με το όνομα Shared Wireless Access Protocol- Cordless Access(SWAP-CA),η οποία επιτρέπει την ασύρματη επικοινωνία με ραδιοκύματα ανάμεσα σε διαφορετικές συσκευές και στον υπολογιστή που βρίσκονται σε ένα σπίτι. Χτισμένο γύρω από ένα φάσμα ραδιοκυμάτων που είναι παγκοσμίως

διαθέσιμο, το SWAP-CA περιλαμβάνει επιχειρησιακή υποστήριξη και για managed αλλά και για ad-hoc δίκτυα. Συνδυάζει και επεκτείνει την ασύρματη δικτύωση και την ασύρματη τηλεφωνία σε ένα ενιαίο ενοποιημένο πρωτόκολλο που επιτρέπει τις κινητές συσκευές να επικοινωνούν με φωνή αλλά και με δεδομένα ταυτόχρονα μέσω του internet. Για τις συσκευές που λειτουργούν με μπαταρία η προδιαγραφή περιλαμβάνει και μηχανισμό για διαχείριση της ενέργειας, ο οποίος διασφαλίζει την μακρόχρονη σύνδεση.



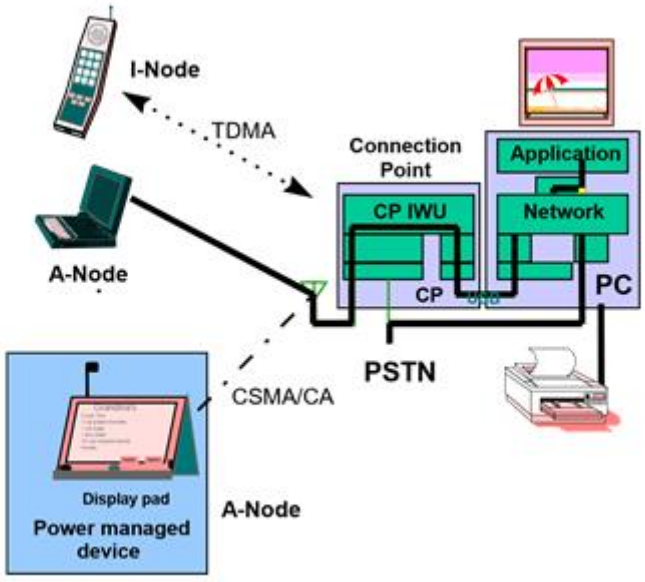
Σχήμα 3 "SWAP vision for Home Networking"

Η αρχιτεκτονική SWAP είναι ένας μοναδικός συνδυασμός ενός managed δικτύου, που προσφέρει ισόχρονες υπηρεσίες όπως η διαδραστική φωνή και ενός ad-hoc δικτύου, που προσφέρει ένα παραδοσιακό δίκτυο δεδομένων. Το πρωτόκολλο έχει βελτιωθεί ώστε να παρέχει τα είδη των υπηρεσιών, οι οποίες απαιτούνται πιο πολύ από τις συνδεδεμένες συσκευές. Τρία είδη συσκευών μπορεί να υπάρχουν σε ένα SWAP δίκτυο:

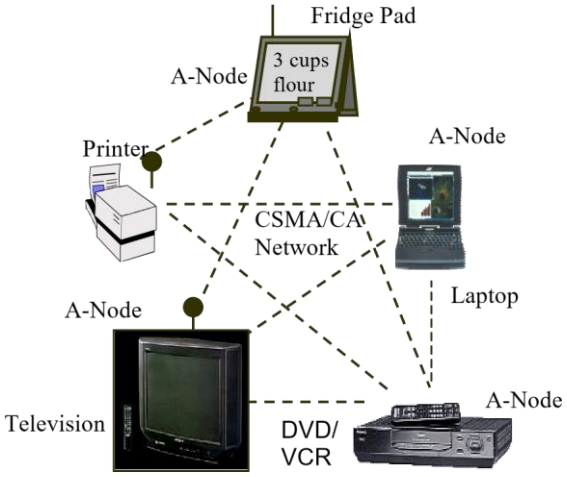
- Ένα Connection Point(CP), το οποίο λειτουργεί ως gateway αναμεσά στον προσωπικό υπολογιστή και, το PSTN και τις συμβατές με το SWAP συσκευές.
- Συσκευές φωνής(I-nodes)
- Ασύγχρονες συσκευές δεδομένων οι οποίες ονομάζονται A-nodes

Το Control Point είναι συνήθως συνδεμένο με τον κύριο οικιακό υπολογιστή, συνήθως μέσω usb. Μπορεί επίσης να είναι συνδεδεμένο και στο PSTN. Είναι ικανό να πραγματοποιεί μεταφορές δεδομένων από και προς άλλες συσκευές χρησιμοποιώντας ένα ασύγχρονο πρωτόκολλο.

Επιπλέον το SWAP πρωτόκολλο είναι υβριδικό με διάφορους τρόπους, είναι τύπου client-server αναμεσά στο Control Point και τις άλλες συσκευές, αλλά είναι peer to peer(ομότιμο) ανάμεσα στις συσκευές δεδομένων. Οι δια δραστικές συναλλαγές φωνής είναι τύπου circuit switched και χρησιμοποιούν time division multiple access, αλλά οι ασύγχρονες συναλλαγές είναι τύπου packet switched και χρησιμοποιούν carrier sense multiple access.Αυτός είναι ο πλούτος που επιτρέπει το SWAP να χρησιμοποιείται ευρέως στο σπίτι, αλλά δεν είναι σχεδιασμένο για να υποστηρίζει χιλιάδες χρήστες όπως σε μια επιχείρηση.



Σχήμα 4 "Managed Network"



Σχήμα 5 "Peer-to-Peer Ad hoc Network"

Όταν ένας SWAP-CA κόμβος λειτουργεί για πρώτη φορά αμέσως μπαίνει στη φάση αναζήτησης δικτύου και προσπαθεί να καθορίσει αν υπάρχει κάποιος άλλος κόμβος ή CP μέσα στην εμβέλεια του και αν υπάρχει κάποιο δίκτυο στο οποίο μπορεί να συμμετέχει. Ο κόμβος επιτυγχάνει την διαδικασία της αναζήτησης πραγματοποιώντας μια παθητική αναζήτηση(passive scanning).Στην παθητική αναζήτηση ο κόμβος “ακούει” κάθε κανάλι για μια συγκεκριμένη χρονική περίοδο. Κατά τη διάρκεια της αναζήτησης ο κόμβος λαμβάνει όλα τα πακέτα του δικτύου ανεξάρτητα της διεύθυνσης προορισμού. Η διαδικασία της αναζήτησης τερματίζεται όταν βρεθεί το πρώτο δίκτυο ή όταν το αποφασίσει ο μηχανισμός διαχείρισης του κόμβου.

2.3 HiperLAN2 (2000)

Η ανάγκη για μεγαλύτερο εύρος ζώνης(bandwidth) στα ιδιωτικά δίκτυα έχει αυξηθεί σημαντικά κατά τη διάρκεια των τελευταίων χρόνων. Μια ακόμα σημαντική τάση είναι η κάλυψη της επικοινωνίας των δεδομένων και της φωνής.

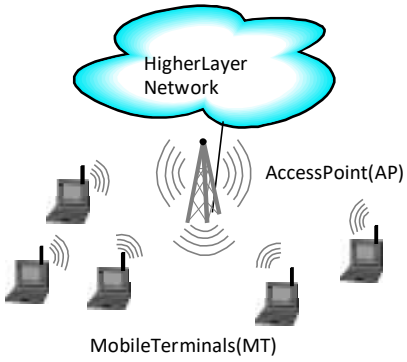
Το HiperLAN2 λειτουργεί στη μπάντα των 5 GHz και προσφέρει μέχρι και 54Mbit/s ρυθμό δεδομένων με την υποστήριξη της κινητικότητας και του QoS (Quality of Service).Το HiperLAN2 υποστηρίζει διάφορες βασικές δικτυακές τεχνολογίες. Ένας σημαντικός στόχος του πρωτοκόλλου είναι η πλήρης διαλειτουργεία με συσκευές από διαφορετικούς κατασκευαστές.

Το HiperLAN2 είναι ένα LAN δίκτυο βασισμένο σε ραδιοκύματα. Ένα access point(AP) καλύπτει μια σημαντική γεωγραφική περιοχή με ασύρματες λειτουργείς στη μπάντα των 5GHz. Αυτές οι λειτουργείες χρησιμοποιούνται από κινητά τερματικά, μέσα στο εύρος κάλυψης του access point.

Το HiperLAN2 μπορεί να χρησιμοποιηθεί με διάφορα βασικά δίκτυα. Αυτό επιτυγχάνεται λόγω:

- Της ευέλικτης αρχιτεκτονικής που ορίζει στα βασικά δίκτυα ανεξάρτητο φυσικό και data-link-control επίπεδο
- Μιας ομάδας από στρώματα που εξυπηρετούν την πρόσβαση σε διαφορά βασικά δίκτυα

  Διαφορά στρώματα έχουν οριστεί για διασυνεργασία με:
- IP πρωτόκολλα μεταφοράς(Ethernet και point-to-point πρωτόκολλα,PPP)
- Ασύγχρονα mode-baser δίκτυα μεταφοράς(ATM)
- Τρίτης γενιάς βασικά δίκτυα
- Δίκτυα τα οποία χρησιμοποιούν IEEE 1394(Firewire) πρωτόκολλα και εφαρμογές



Σχήμα 6 “Basic system architecture"

Το πρωτόκολλο HiperLAN2,υποστηριζει την κινητικότητα στο τερματικό με ταχύτητα μέχρι και τα 10m/s.Επιπλέον, προσφέρει τα μέσα για το χειρισμό των τερματικών σε διαφορετικά περιβάλλοντα παρεμβολών και διάδοσης, με στόχο την

- Διατήρηση του συνδέσμου της επικοινωνίας σε υψηλές αναλογίες σήματος-προς-παρεμβολές.
- Διατήρηση της ποιότητας της λειτουργείας
- Εύρεση μιας κατάλληλης ισορροπίας μεταξύ στο εύρος της επικοινωνίας και του ρυθμού μετάδοσης των δεδομένων

Η ασύρματη διεπαφή (interface) του πρωτοκόλλου HiperLAN2 βασίζεται στους μηχανισμούς dynamic time-division duplex (TDD) και στο dynamic time-division multiple access(TDMA). Το HiperLAN2 είναι μια ευέλικτη πλατφόρμα στην οποία μπορούν να βασιστούν διάφορες επαγγελματικές και οικιακές εφαρμογές πολυμέσων με ρυθμούς μετάδοσης μέχρι και τα 54Mbit/s.

Το HiperLAN2 βασίζεται σε κυψελοειδές (cellular) δικτυακή τοπολογία συνδυασμένη με ad hoc δυνατότητες δικτύωσης. Υποστηρίζει δυο βασικούς τρόπους λειτουργείας: την centralized mode (CM) και την direct mode (DM).

Η λειτουργεία centralized mode εφαρμόζεται σε κυτταρική(cellular) τοπολογία δικτύου όπου κάθε κυψέλη (radio cell) ελέγχεται από ένα access point το οποίο καλύπτει μια συγκεκριμένη γεωγραφική περιοχή. Σε αυτή τη λειτουργεία, τα κινητά τερματικά επικοινωνούν μεταξύ τους ή με ένα βασικό δίκτυο μέσω του access point. Η centralized mode λειτουργεία χρησιμοποιείται κυρίως σε εσωτερικές και εξωτερικές επιχειρησιακές εφαρμογές όπου η περιοχή που καλύπτεται είναι μεγαλύτερη από μια κυψέλη.

Η λειτουργεία direct mode εφαρμόζεται σε ad hoc τοπολογία δικτύου των ιδιωτικών οικιακών περιβαλλόντων και εκεί όπου ολόκληρη η περιοχή εξυπηρέτησης καλύπτεται από μια κυψέλη. Σε αυτή τη λειτουργεία, τα κινητά τερματικά μπορούν να επικοινωνούν κατευθείαν μεταξύ τους. Τα Access points ελέγχουν την εκχώρηση των πόρων στα κινητά τερματικά.

2.4 IEEE 802.11 (1997)

Η αρχική έκδοση του πρωτοκόλλου 802.11 δημοσιεύτηκε το 1997 και είναι ουσιαστικά παρωχημένη σήμερα. Το 802.11 καθορίζει έναν ρυθμό μετάδοσης στο 1 Mbit/s ή 2 Mbit/s και καθορίζει τρεις εναλλακτικές τεχνολογίες για το physical layer :

- Μια υπέρυθρη (infrared) λειτουργεία στο 1 Mbit/s
- Μια frequency- hopping spread spectrum (FSSS) λειτουργεία στο 1 Mbit/s ή στα 2 Mbit/s
- Μια direct- sequence spread spectrum (DSSS) λειτουργεία στο 1 Mbit/s ή στα 2 Mbit/s

Οι τελευταίες δυο τεχνολογίες χρησιμοποιούν μικροκύματα στην ISM μπάντα στα 2.4 GHz. Μια αδυναμία του αρχικού προτύπου ήταν ότι πρόσφερε πάρα πολλές επιλογές κάτι το οποίο δεν βοηθούσε στην διαλειτουργικότητα.

Η DSSS εκδοχή του 802.11 βελτιώθηκε και έγινε πιο δημοφιλής από το 802.11b το 1999, το οποίο αύξησε το ρυθμό μετάδοσης στα 11Mbit/s. Η ευρεία κλίμακας υιοθέτηση των 802.11 δικτυών επιτεύχθηκε μετά την δημοσίευση του 802.11b.

2.4.1 IEEE 802.11a (1999)

Το 802.11a δημοσιεύτηκε το 1999, εκείνη την περίοδο η μόνη Wi-Fi τεχνολογία που ετοιμαζόταν για την αγορά ήταν το 802.11b. (Το 802.11 δεν είχε εξαπλωθεί λόγο του χαμηλού ρυθμού μετάδοσης.) Το 802.11a και τα πρωτόκολλα 802.11 και 802.11b δεν ήταν διαλειτουργηκα μεταξύ τους, δηλαδή οι συσκευές που χρησιμοποιούσαν το πρωτόκολλο 802.11a δεν μπορούσαν να επικοινωνήσουν με άλλες συσκευές που χρησιμοποιούσαν τα πρωτόκολλα 802.11 και 802.11b.

Ένα 802.11a ασύρματο δίκτυο υποστηρίζει ένα θεωρητικό μέγιστο ρυθμό μετάδοσης έως 54 Mb/s. Οι επιδόσεις του 802.11a το έθεσαν ως μια ελκυστική τεχνολογία, αλλά ένα σημαντικό μειονέκτημα ήταν ότι για να επιτευχθεί αυτή η υψηλή απόδοση χρησιμοποιούνταν υλικά υψηλού κόστους και για αυτόν τον λόγο δεν χρησιμοποιήθηκε όσο το 802.11b.

Το 802.11a λειτουργεί στην συχνότητα των 5GHz, η οποία δεν είναι τόσο συνωστισμένη όσο η συχνότητα των 2.4GHz. Επειδή το πρωτόκολλο λειτουργεί σε υψηλότερες συχνότητες σε σχέση με το 802.11 και το 802.11b, προσφέρει μικρότερο εύρος κάλυψης και για αυτό το λόγο η χρήση του δεν είναι τόσο αποτελεσματική σε μεγάλα κτήρια.

2.4.2 IEEE 802.11b (2000)

Το 802.11b έχει μέγιστο ρυθμό μετάδοσης τα 11 Mbit/s και χρησιμοποιεί την ίδια μέθοδο πρόσβασης στο μέσο που ορίστηκε στο αρχικό 802.11. Τα 802.11b προϊόντα εμφανίστηκαν στην αγορά στις αρχές του 2000 και είναι μια επέκταση της τεχνικής που υπήρχε στο 802.11. Η δραματική αύξηση του throughput του 802.11b, σε σύγκριση με το αρχικό 802.11, μαζί με την ουσιώδη μείωση των τιμών οδήγησε στην ταχύτατη αποδοχή του 802.11b ως την οριστική wireless LAN τεχνολογία.

Ένα μειονέκτημα των 802.11b συσκευών ήταν τα πιθανά προβλήματα παρεμβολών με αλλά προϊόντα που λειτουργούσαν στα 2.4 GHz. Οι φούρνοι μικροκυμάτων, τα ασύρματα τηλεφωνά και οι Bluetooth συσκευές λειτουργούν τα 2.4 GHz. Τα προβλήματα με τις παρεμβολές καθώς και η αύξηση του πλήθους των χρηστών

μέσα στα 2.4 GHz μετατράπηκε σε σημαντικό ζήτημα καθώς η δημοτικότητα του Wi-Fi αυξανόταν.

2.4.3 IEEE 802.11g (2003)

Το 802.11g λειτουργεί στην 2.4GHz μπάντα συχνότητας και προσφέρει data rate έως 54Mb/s. Επιγραμματικά, τα νέα χαρακτηριστικά του πρωτοκόλλου IEEE 802.11g σε σχέση με τα παλαιοτέρα πρωτόκολλα είναι:

- Ο εφοδιασμός του με τέσσερα διαφορετικά φυσικά επίπεδα
- Υποστήριξη short preamble

Ο εφοδιασμός του με τέσσερα διαφορετικά φυσικά επίπεδα

Το IEEE 802.11g χρησιμοποιεί DSSS ή OFDM ή και τα δυο στα 2.4GHz και με αυτόν τον τρόπο προσφέρει υψηλές ταχύτητες μεταφοράς δεδομένων που φτάνουν μέχρι και τα 54Mb/s.Η συνδυασμένη χρήση του DSSS και του OFDM επιτυγχάνεται με τον εφοδιασμό με τέσσερα διαφορετικά φυσικά επίπεδα. Αυτά τα επίπεδα που ορίζονται στο πρωτόκολλο ως extended rate physicals(ERP) συνυπάρχουν κατά τη διάρκεια της ανταλλαγής πακέτων, έτσι ώστε ο αποστολέας και ο παραλήπτης να έχει την επιλογή να χρησιμοποιήσει ένα από τα τέσσερα φυσικά επίπεδα αρκεί και οι δυο να το υποστηρίζουν. Τα τέσσερα διαφορετικά φυσικά επίπεδα είναι:

- ERP-DSSS/CCK: Αυτό είναι το παλιό φυσικό επίπεδο που χρησιμοποιούνταν από το IEEE 802.11b.
- ERP-OFDM: Αυτό είναι το νέο φυσικό επίπεδο που εισάγεται με το πρωτόκολλο IEEE 802.11g.Το OFDM χρησιμοποιείται για να προσφέρει τους ρυθμούς μετάδοσης των δεδομένων που έχει το IEEE 802.11a στα 2.4GHz δηλαδή 54 Mbit/s.
- ERP-DSSS/PBCC (προαιρετικό): Αυτό το φυσικό επίπεδο υπήρχε στο 802.11b και προσφέρει τους ιδίους ρυθμούς μετάδοσης με το DSSS/CCK φυσικό επίπεδο. Χρησιμοποιεί την DSSS τεχνολογία με τον PBCC αλγόριθμο.
- DSSS-OFDM (προαιρετικό): Αυτό είναι το νέο φυσικό επίπεδο που χρησιμοποιεί τον υβριδικό συνδυασμό των DSSS και OFDM. Η φυσική κεφαλίδα του πακέτου μεταδίδεται χρησιμοποιώντας το DSSS, ενώ το φορτίο του πακέτου μεταδίδεται χρησιμοποιώντας το OFDM. Ο σκοπός

αυτού του υβριδικού επιπέδου είναι η κάλυψη των προβλημάτων διαλειτουργηκότητας.

Υποστήριξη μικρού preamble

Στο IEEE 802.11b διαπιστώθηκε ότι το preamble ήταν αρκετά μεγάλο και πρόσθετε αρκετό overhead στο WLAN σύστημα. Ως εκ τούτου, μια επιλογή να υποστηριχτεί ένας μικρότερος τύπος preamble εισάχθηκε με σκοπό την μείωση του overhead των πακέτων και τη βελτίωση την απόδοση του δικτύου. Αν και ο αποστολέας και ο παραλήπτης υποστηρίζουν αυτήν την επιλογή ,τότε η επικοινωνία πραγματοποιείται χρησιμοποιώντας short preamble.

2.4.4 IEEE 802.11n (2009)

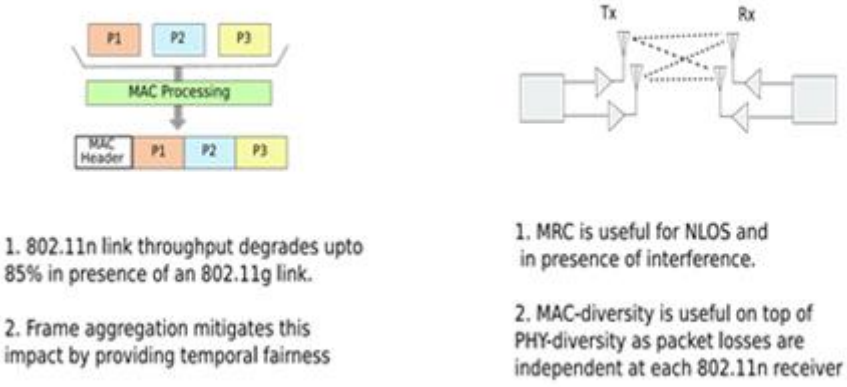
Το 2002 ξεκίνησε η συζήτηση στο IEEE 802.11 Working Group(WG) για την επέκταση του ρυθμού μετάδοσης των δεδομένων στο φυσικό επίπεδο σε σχέση με τους ρυθμούς μετάδοσης που υπήρχαν στα πρωτόκολλα IEEE 802.11a/g,προκειμένου να αντιμετωπίσουν την υψηλότερη απόδοση των ενσύρματων δικτύων και να επωφεληθούν από την ευελιξία της ασύρματης επικοινωνίας. Το WG προχώρησε μέσω τον τυπικών βημάτων στην δημιουργία ενός πρωτοκόλλου. Το WG εισήγαγε μια νέα τεχνολογία κεραίας, όπως η multiple-input-multiple-output(MIMO).

Ακολούθως το IEEE 802.11n Task Group (TGn) ξεκίνησε να αναπτύσσει μια νέα τροπολογία για το πρωτόκολλο IEEE 802.11.Το 802.11n λειτουργεί στη μπάντα των 2,4GHz και στη μπάντα των 5GHz και χρησιμοποιεί τα κανάλια των 20 MHz και 40 MHz. Το τυπικό εύρος του ρυθμού μετάδοσης είναι από 150Mb/s έως και 600Mb/s με ένα εύρος απόστασης μέχρι και 70m. Οι νέοι μηχανισμοί που χρησιμοποιούνται για το πρωτόκολλο IEEE 802.11n είναι:

- PHY-diversity (MIMO): Το IEEE 802.11n χρησιμοποιεί μια ποικιλία από μηχανισμούς διαχωρισμού των φυσικών επίπεδων για να επιτυγχάνει μεγαλύτερη απόδοση και βελτιωμένες δυνατότητες λήψης πακέτων. Η MIMO τεχνική εκμεταλλεύεται την παρουσία πολλαπλών κεραιών και στον πομπό και στον δέκτη για να βελτιώσει και την χωρητικότητα αλλά και την αξιοπιστία της μετάδοσης. Οι τεχνικές για την μετάδοση που χρησιμοποιούνται στο IEEE 802.11n συμπεριλαμβάνουν την Space Time Block Coding (STBC) και Cyclic

Shift Diversity (CSD). Αυτές οι τεχνικές βελτιώνουν την λήψη σήματος απλώνοντας το πάνω σε πολλαπλές κεραίες χρησιμοποιώντας το STBC ή το CSD.

- Συνδυασμός(aggregation) πακέτων: Το IEEE 802.11n προσφέρει την επιλογή του συνδυασμού πολλαπλών πακέτων δεδομένων που είναι έτοιμα για μετάδοση, μέσα σε ένα συνδυαστικό πακέτο. Ο συνδυασμός των πακέτων βοηθάει στην μέγιστη αξιοποίηση της σύνδεσης του καναλιού και στη μείωση της καθυστέρησης λόγω της μετάδοσης των συνδυαστικών πακέτων σε μια μόνο εύκαιρα μετάδοσης στο κανάλι.



Σχήμα 7 “Frame aggregation and PHY- diversity"

2.4.5 IEEE 802.11ac (2013)

Το πρωτόκολλο IEEE 802.11ac λειτουργεί στη μπάντα των 5GHz και προσφέρει ένα εύρος ρυθμού απόδοσης από 450Mb/s μέχρι και 6.77Gb/s. Αυτό σημαίνει την αύξηση ως και πέντε φορές από την μέγιστη απόδοση που προβλέπετε από το πρότυπο 802.11n. Το IEEE 802.11ac, έχει ως σκοπό την περεταίρω βελτίωση της συνολικής απόδοσης του δικτύου και ταυτόχρονα να βελτιώσει ακόμα περισσότερο την απόδοση της κάθε σύνδεσης ξεχωριστά. Λόγω αυτής της σημαντικής αύξησης της απόδοσης που επιτυγχάνεται από το IEEE 802.11ac, ο ορός very high troughput (VHT) χρησιμοποιείται για να περιγράψει αυτό το πρότυπο.

Οι δυο βασικοί λόγοι που επιτρέπουν το 802.11ac να επιτυγχάνει μεταδόσεις με gigabit ρυθμούς είναι:

- Η δυνατότητα στατικής και δυναμικής ένωσης καναλιών
- Ο μηχανισμός Multi-user multiple-input multiple-output (MU-MIMO)

Για να ενεργοποιηθούν αυτά τα δυο χαρακτηριστικά χρειάζονται ουσιώδεις τροποποιήσεις στο PHY επίπεδο. Για τις περισσότερες αλλαγές στο MAC επίπεδο θα πρέπει να ελέγχεται άμα είναι συμβατές με το τροποποιημένο PHY επίπεδο.

Μια από τις αλλαγές που πραγματοποιούνται είναι η χρήση επιπλέον καναλιών μετάδοσης, στο 802.11n χρησιμοποιούνται τα κανάλια των 20 και 40 MHz, ενώ στο 802.11ac χρησιμοποιούνται δυο επιπλέον κανάλια, αυτά των 80 και 160 MHz στη συχνότητα των 5 GHz.

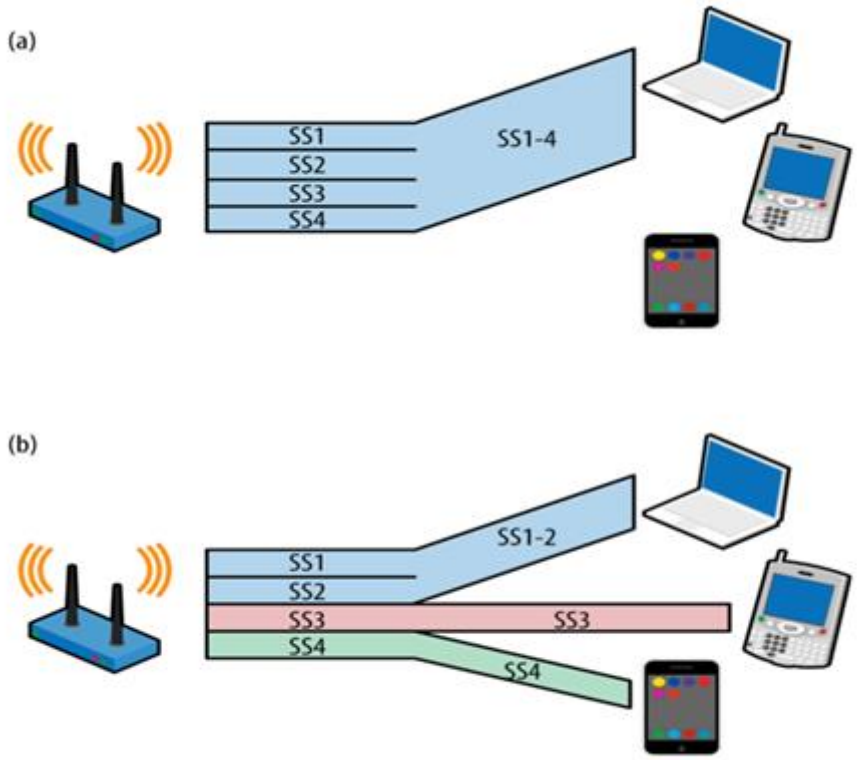
Το 802.11ac αναπτύχθηκε και αυτό για να εξυπηρετεί διαφορετικούς τύπους μοντέλων χρήσης. Οι κυρίες κατηγορίες είναι η ασύρματη παρουσίαση, οικιακή διανομή της HDTV, οι γρήγορες ταχύτητες upload και download για μεγάλα αρχεία από και προς τους servers.

Η τεχνική MIMO παρουσιάστηκε για πρώτη φορά στο πρωτόκολλο 802.11n. Αυτή η τεχνική αποτελείται από ένα physical layer στο οποίο και πομπός και ο δέκτης χρησιμοποιούν πολλαπλές κεραίες. Το 802.11n υποστηρίζει μέχρι και 4 MIMO ρεύματα (streams) που μπορούν να εξυπηρετούν έναν χρήστη κάθε φορά (single-user MIMO, SU- MIMO). Σε αντίθεσή το 802.11ac είναι το πρώτο πρότυπο της 802.11 οικογενείας προτύπων που εισάγει τη τεχνική multi- user MIMO για να εξυπηρετεί πολλαπλούς σταθμούς ταυτόχρονα. Επιπλέον, αυξάνει τον αριθμό των ρευμάτων (streams) από τέσσερα σε οχτώ.

Η τεχνική MU-MIMO ορίζεται από το πρωτόκολλο ως μια τεχνική όπου πολλαπλοί σταθμοί, όπου ο καθένας υπάρχει περίπτωση να διαθέτει πολλαπλές κεραίες, μεταδίδουν και/ή δέχονται ανεξάρτητα ρεύματα δεδομένων ταυτόχρονα. Το MU-MIMO επιτρέπει τους σταθμούς να έχουν πολλαπλές κεραίες για να μεταδίδουν αρκετά ρεύματα δεδομένων σε πολλαπλούς χρήστες ταυτόχρονα στο ίδιο κανάλι συχνότητας. Αυτή η λειτουργεία επιτρέπεται μόνο στην μετάδοση από το access point προς τους ασύρματους σταθμούς. Το 802.11ac υποστηρίζει μέχρι και τέσσερα ρεύματα εξυπηρετώντας έτσι τέσσερεις διαφορετικούς χρήστες ταυτόχρονα ή μέχρι και τέσσερα ρεύματα για κάθε χρήστη.

Το IEEE 802.11ac προσδιορίζει μια μοναδική μέθοδο μετάδοσης beamforming που βασίζεται στην ανατροφοδότηση για να επιτρέψει και την SU (single-user) αλλά και την MU(multi-user)-MIMO. Συγκεκριμένα, το beamforming επιτρέπει έναν σταθμό να μεταδίδει ταυτόχρονα σε πολλαπλά ρεύματα δεδομένων σε ένα μοναδικό χρήστη ή σε πολλαπλούς χρήστες. Το 802.11ac ορίζει ένα μοναδικό ανατροφοδοτούμενο

πρωτόκολλο για να εγγυηθεί την διαλειτουργηκότητα ανάμεσα σε διαφορετικές beamforming υλοποιήσεις από διαφορετικούς κατασκευαστές.



Σχήμα 8"Single- user MIMO (a) and Multi- user MIMO (b) "

2.4.6 IEEE 802.11ah (2016)

Το 802.11ah είναι σχεδιασμένο για την υποστήριξη των εφαρμογών με τις εξής απαιτήσεις: μέχρι και 8191 συσκευές πρέπει να σχετίζονται σε ένα access point, να υιοθετούν την στρατηγική της χαμηλής κατανάλωσης ενέργειας, να έχουν ελάχιστο ρυθμό δεδομένων δικτύου 100kbps, να λειτουργούν σε συχνότητες γύρω στα 900 MHz, να καλύπτουν αποστάσεις μέχρι και 1 km σε εξωτερικούς χώρους, να είναι μέρος τεχνολογίας δικτύου μίας αναπήδησης (one-hop network) και να υποστηρίζουν σύντομες μεταδόσεις δεδομένων.

Ένας από τους στόχους της ομάδας σχεδίασης του πρωτοκόλλου IEEE 802.11ah είναι να προσφέρει ένα πρότυπο το οποίο, εκτός από το να ικανοποιεί τις παραπάνω απαιτήσεις, να ελαχιστοποιεί τις αλλαγές του ευρέως αποδεκτού 802.11. Με αυτή την έννοια τα προτεινόμενα PHY και MAC layers είναι βασισμένα στο πρότυπο 802.11ac που προσπαθεί να πετύχει μια αύξηση της αποδοτικότητας με τη μείωση κάποιων πλαισίων ελέγχου/διαχείρισης όπως και το μήκος του MAC header. Τεχνολογίες όπως η Orthogonal Frequency Division Multiplexing (OFDM), Multi Input Multi Output (MIMO) και Downlink Multi-User MIMO (DL MU-MIMO),οι οποίες πρωτοεμφανίστηκαν στο πρότυπο IEEE 802.11ac, χρησιμοποιούνται από το πρωτόκολλο 802.11ah.

Το IEEE 802.11ah προσφέρει μια πληθώρα πλεονεκτημάτων, όπως η απλή χρήση σε εξωτερικούς χώρους και τα άριστα χαρακτηριστικά διάδοσης σε χαμηλές συχνότητες. Επίσης αναπόσπαστο κομμάτι του IEEE 802.11ah θα είναι οι στρατηγικές που αποσκοπούν στην μεγάλη διάρκεια της μπαταρίας και στην οικονομία της ενέργειας. Παρακάτω παραθέτουμε τα κύρια πλεονεκτήματα του 802.11ah:

- Βέλτιστα χαρακτηριστικά μετάδοσης σε συχνότητες κάτω του 1GHz.
- Χρήση της ζώνης συχνότητας ISM.
- Εύκολο να κατανοηθεί και να εφαρμοστή από τους κατασκευαστές δικτυακών συσκευών.
- Μεγαλύτερη εμβέλεια και μικρότερη κατανάλωση ενέργειας λόγω χαρακτηριστικών της συχνότητας(κάτω του 1GHz).
- Εμπλουτισμός των ασύρματων συσκευών επικοινωνίας.

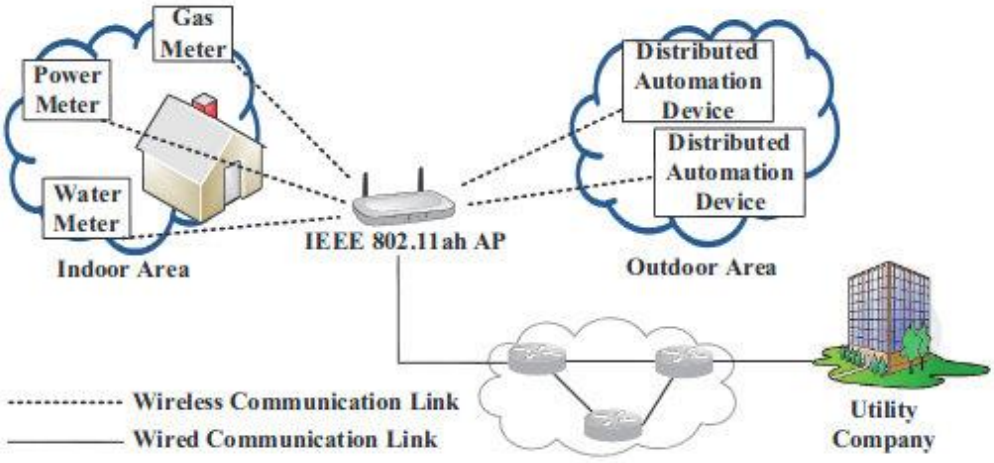
Το IEEE 802.11ah μπορεί να χρησιμοποιηθεί για:

- Δίκτυα αισθητήρων: Η ανίχνευση μπορεί να εκτελεστεί με βραχυπρόθεσμες μεταδόσεις δεδομένων και συνήθως αφορούν έξυπνες μετρήσεις όπως του φυσικού αερίου, του νερού και ασύρματου ελέγχου των συστημάτων διανομής ενέργειας. Λόγω τις αυξανόμενης εισχώρησης σε χαμηλότερες συχνότητες, ένας μεγάλος αριθμός αισθητήρων μπορεί να καλυφθεί από την τεχνική one-hop.
- Εκτεταμένη εμβέλεια Wi-Fi: Είναι σημαντικό οι τεχνολογίες που χρησιμοποιούνται για εκφόρτωση (off-loading) να έχουν τουλάχιστον συγκρίσιμες επιδόσεις στο κυψελοειδές σύστημα που ξεφορτώνουν από τον χρήστη. Επομένως είναι σημαντικό να σκεφτούμε τι είδους φασματική απόδοση, ρυθμοαπόδοση και φορτίο του συστήματος μπορούμε να έχουμε στα τωρινά και

στο μελλοντικά κυψελοειδή δίκτυα και βάση αυτού να σκεφτούμε τις απαιτήσεις του IEEE 802.11ah.

Παρόλο που μπορεί εύκολα να κατανοηθεί ότι η μεγάλη κάλυψη μπορεί να χρησιμοποιηθεί για την εκφόρτωση, κάποιοι θα υποστηρίξουν ότι οι απαιτήσεις του χρήστη μπορούν να εξυπηρετηθούν από τα υπάρχουσα ασύρματα πρότυπα. Αν η απόδοση δεν είναι επαρκής ή προσφέρει μόνο οριακά κέρδη και όχι πραγματική επιπλέον αξία για τον τελικό χρήστη, τότε η εκφόρτωση μπορεί να μην είναι επιτυχής και έτσι και οι τελικοί χρήστες και οι φορείς μπορεί να προτιμήσουν κάποια υπάρχουσα λύση.

- Machine to Machine επικοινωνία: Το πρότυπο IEEE 802.11ah έχει αναγνωριστεί ως ιδανικός υποψήφιος για συστήματα ασύρματης επικοινωνίας για Machine-to- Machine επικοινωνίες. Οι ασύρματες Machine- to- Machine επικοινωνίες επιτρέπουν την μεταφορά δεδομένων σε απευθείας επικοινωνία με λίγη ή καθόλου ανθρώπινη εμπλοκή. Επειδή τα τωρινά συστήματα είναι σχεδιασμένα περισσότερο για επικοινωνία από άνθρωπο σε άνθρωπο, το IEEE 802.11ah πρότυπο θα επικεντρωθεί κυρίως σε εφαρμογές ανίχνευσης. Λόγω όλων των διαφορετικών ενεργειών των M2M προτύπων που συμβαίνουν σε διάφορους οργανισμούς προτυποποίησης, το IEEE 802.11ah θα μπορούσε να παίξει ένα σημαντικό ρόλο στην παροχή μιας βάσης για ένα παγκόσμιο M2M ασύρματο πρότυπο, το οποίο ορισμένοι φορείς θεωρούν ως πρόδρομο του cloud. Αυτό συμπεριλαμβάνει έξυπνες μετρήσεις και αισθητήρες ασφαλείας .Το IEEE 802.11ah θα πρέπει να αντιμετωπίσει κάποιες απαιτήσεις όπως η χαμηλή κατανάλωση ενέργειας, ο μεγάλος αριθμός των συσκευών και μεγάλες σε έκταση επικοινωνίες.
- Αγροτικές επικοινωνίες: Οι ασύρματες επικοινωνίες σε αγροτικές περιοχές έχουν οδηγήσει σε μια προσπάθεια γνωστή ως connect to unconnect. Το φάσμα του 1GHz προσφέρει μεγάλη προοπτική λόγω της ευρύτερης έκτασης του. Το E-health και το E- learning είναι κύριες εφαρμογές σε τέτοια περιβάλλοντα και έχει υποστηριχθεί ότι μία θετική επίδραση στην κοινωνική οικονομία μπορεί να επιτευχθεί μέσω των εφαρμογών.



Σχήμα 9"IEEE 802.11ah smart grid "

Μια άλλη πηγή του υπερβολικού overhead είναι τα beacons. Τα beacons στέλνονται περιοδικά από το access pont, το περιεχόμενο τους εξαρτάται από τον τρόπο με τον οποίο το access point λειτουργεί και συνήθως στα δίκτυα 802.11g/n το μέγεθος τους μπορεί να υπερβαίνει τα 100 bytes. Για να ληφθεί από μακρινούς σταθμούς, τα beacons θα πρέπει να αποστέλλονται με την χαμηλότερη τιμή, η οποία είναι λιγότερο του 1Mbps στην περίπτωση του 802.11ah. Σε τόσο μικρές τιμές, ακόμα και δεκάδες από bytes που στέλνονται αρκετές φορές ανά δευτερόλεπτο καταλαμβάνουν σημαντικό ποσοστό του χρόνου του καναλιού.

Για την μείωση της μέσης πληρότητας και της κατανάλωσης ενέργειας τόσο για τη μετάδοση του beacon από το access point όσο και για την παραλαβή του από τους σταθμούς, η ομάδα υλοποίησης του πρωτοκόλλου χρησιμοποιεί δύο τύπους beacons: πλήρη και σύντομο. Τα σύντομα beacons στέλνονται πιο συχνά από ότι τα πλήρη και δεν περιέχουν μη ουσιώδη, ή μη επείγουσες πληροφορίες, οι οποίες μπορούν να αποκτηθούν από κανονικά beacons ή με αίτηση. Έτσι σε αντίθεση με τα πλήρη beacons, τα σύντομα δεν περιέχουν

- Διευθύνσεις προορισμού, αφού τα beacons μεταδίδονται με broadcast
- Sequence control, αφού δεν είναι χρήσιμο
- Timestamp από 8 σε 4 bytes, αφού είναι αρκετά για να διατηρούν τον συγχρονισμό

Σχεδόν αναλλοίωτα στοιχεία πληροφορίας μπορούν να εξαχθούν από τα σύντομα beacons. Για την ενημέρωση των σταθμών για τυχόν αναβαθμίσεις, τα σύντομα beacons περιέχουν ένα πεδίο Check – Sequence μήκους 1 byte που αυξάνεται σε κάθε κρίσιμη αναβάθμιση. Έχοντας παραλάβει ένα σύντομο beacon με μία νέα τιμή

σε αυτό το πεδίο, ο σταθμός περιμένει για ένα πλήρη beacon για να παραλάβει τις πληροφορίες που αναβαθμίστηκαν.

Η εκφόρτωση είναι μία σημαντική περίπτωση χρήσης της 802.11ah τεχνολογίας, η ανακάλυψη των πυλών στο διαδίκτυο είναι ένα σημαντικό χαρακτηριστικό. Αυτός είναι ο λόγος τα σύντομα beacons περιέχουν ένα προαιρετικό πεδίο Access Network Options μήκους 1 byte που έχει τροποποιηθεί στο 802.11u και το πεδίο αυτό αναφέρει αν η πρόσβαση είναι δημόσια, εάν είναι ελεύθερη και εάν έχει σύνδεση στο διαδίκτυο. Έχοντας λάβει ένα σύντομο beacon, οι σταθμοί μπορούν να αποφασίσουν εάν η πρόσβαση στον δίκτυο είναι κατάλληλη ή όχι χωρίς να χρειάζεται να περιμένει για ένα πλήρη beacon.

2.4.7 IEEE 802.11ax (2019)

Το πρωτόκολλο 802.11ax θα υλοποιεί νέες βελτιώσεις για τα PHY και MAC επίπεδα με σκοπό την επιπλέον βελτίωση της επίδοσης του WLAN δικτύου, με εστίαση στην απόδοση και διάρκεια ζωής της μπαταρίας. Η συνδυασμένη χρήση των CSMA/CA, CCA (Clear Channel Assessment) και το υψηλό επίπεδο μετάδοσης ενέργειας μπορεί να έχει αποτέλεσμα σε σενάρια με περιορισμένη χωρική επαναχρησιμοποίηση. Ο συνδυασμός αυτών των στοιχείων οδηγεί στην ελαχιστοποίηση της παρεμβολής σε WLAN δίκτυα, το οποίο βοηθάει στην μετάδοση με υψηλοτέρους ρυθμούς, ωστόσο μειώθηκε ο αριθμός των ταυτόχρονων μεταδόσεων. Οι εναλλακτικές που μπορούν να χρησιμοποιηθούν για να πέτυχουμε την συνύπαρξη μεταξύ του ρυθμού των ατομικών μεταδόσεων και τον αριθμό των ταυτόχρονων μεταδόσεων συμπεριλαμβάνουν την δυναμική προσαρμογή του επιπέδου της ισχύς μετάδοσης, του CCA επιπέδου και της κατευθυνόμενης μετάδοσης που βασίζεται στη παρατηρούμενη απόδοση του δικτύου.

Μειώνοντας την χρησιμοποιουμένη ισχύ μετάδοσης σε ένα WLAN μειώνουμε την ζώνη επιρροής, το οποίο βελτιώνει την χωρική επαναχρησιμοποίηση. Ωστόσο, αυτό μπορεί να οδηγήσει σε μεγαλύτερο αριθμό πακέτων με σφάλματα και σε μικρότερο ρυθμό μετάδοσης, όπως επίσης να αυξήσει τον αριθμό των κρυμμένων σταθμών(hidden nodes).

Εναλλακτικά, για να μειώσουμε την ζώνη επιρροής των γειτονικών WLANs και να αυξήσουμε τις πιθανότητες κάθε WLANs να μεταδώσει, οι σταθμοί των WLAN μπορεί να αυξήσουν το επίπεδο του CCA,ως εκ τούτου απαιτείται υψηλότερο επίπεδο ενέργειας για να θεωρηθεί κατειλημμένο και να σταματήσει το back off countdown.

Οι Omnidirectional μεταδόσεις διαδίδουν ομοιογενώς την μεταδιδόμενη ενέργεια σε όλες τις κατευθύνσεις, κάτι το οποίο γεμίζει το κανάλι με ενέργεια σε περιοχές που δεν χρειάζεται. Συγκεντρώνοντας την ενέργεια προς τους επιθυμητούς

7σταθμούς βελτιώνουμε την χωρική επαναχρησιμοποίηση επειδή οι συσκευές οι οποίες είναι τοποθετούμενες σε άλλες κατευθύνσεις θα ανιχνεύουν το κανάλι σαν διαθέσιμο και θα αρχίζουν τις δίκες τους μεταδόσεις ταυτόχρονα, ωστόσο αυτοί οι σταθμοί μπορεί να μετατραπούν σε κρυφούς.

Πίνακας 2 "Χαρακτηρίστηκα ασύρματων προτύπων"

Standard	Maximum Speed	Frequency	Release date
802.11	1 Mb/s – 2 Mb/s	2.4 .GHz	1997
802.11a	54 Mb/s	5 GHz	1999
802.11b	11 Mb/s	2.4 GHz	2000
802.11g	54 Mb/s	2.4 GHz	2003
802.11n	600 Mb/s	2.4 GHz,5 GHz	2009
802.11ac	6.77 Gb/s	5 GHz	2013
802.11ah	100 kb/s	<1 GHz	2016
802.11ax	unknown	2.4 GHz,5 GHz	2019

ΕΠΙΛΟΓΟΣ

Στο παραπάνω κεφάλαιο πραγματοποιήθηκε μια εκτενής αναφορά στα ασύρματα WLAN πρότυπα και τη χρήση τους η οποία αναγκάζει τους δημιουργούς τους να καινοτομούν σε κάθε πρότυπο με σκοπό την εξέλιξη του και την βελτίωση της ποιότητας της επικοινωνίας που προσφέρει το κάθε πρότυπο. Επίσης έγινε αντιληπτό ότι η επιλογή προτύπου γίνεται με βάση το περιβάλλον στο οποίο θα χρησιμοποιηθεί και για την χρήση που τα θέλουμε.

Στο επόμενο κεφάλαιο θα αναφερθούμε στο φυσικό επίπεδο και τις τεχνολογίες και τους μηχανισμούς που χρησιμοποιούνται για την βελτίωση της ποιότητας της επικοινωνίας.

ΚΕΦΑΛΑΙΟ 3

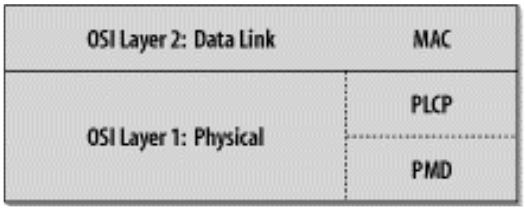
PHY LAYER

ΕΙΣΑΓΩΓΗ

Ο διαχωρισμός των προτύπων σε επίπεδα επιτρέπει την ερευνά, τον πειραματισμό και τη βελτίωση ολοκλήρου του προτύπου. Το σημαντικό στοιχείο της 802.11 αρχιτεκτονικής είναι το φυσικό επίπεδο, το οποίο συχνά το αναφέρουμε ως PHY. Αυτό το κεφάλαιο εισαγάγει τα κοινά θέματα και τις τεχνικές που εμφανίζονται και εφαρμόζονται σε κάθε ένα από φυσικά επίπεδα που έχουν ως βάση τα ραδιοκύματα και επίσης περιγράφει τα κοινά τους προβλήματα.

3.1 Physical-Layer Architecture

Το physical layer διαιρείτε σε δυο sublayer: το Physical Layer Convergence Procedure (PLCP) sublayer και το Physical Medium Dependent (PMD) sublayer. Το PLCP είναι ο σύνδεσμος αναμεσά στα πακέτα στο MAC layer και την ασύρματη μετάδοση στον αέρα και προσθέτει ένα δικό του header στο πακέτο. Κανονικά, τα πακέτα διαθέτουν ένα preamble που βοηθάει στον συγχρονισμό των εισερχομένων μεταδόσεων. Το PMD είναι υπεύθυνο για την μετάδοση των bits που λαμβάνει από το PLCP στον αέρα μέσο της κεραίας. Το physical layer επίσης ενσωματώνει και τη μέθοδο clear channel assessment (CCA) για να υποδεικνύει στο MAC layer άμα ανιχνεύεται άλλο σήμα στο μέσο επικοινωνίας



Σχήμα 10"Physical layer logical architecture "

3.2 Spread Spectrum

Η spread spectrum τεχνολογία είναι το θεμέλιο που χρησιμοποιείται για την καλύτερη χρήση των ISM (industrial, Scientific and medical) bands για τη μετάδοση δεδομένων. Η παραδοσιακή ασύρματη επικοινωνία έχει ως στόχο να “γεμίσει” όσο περισσότερο σήμα μπορεί σε όσο στενότερη μπάντα γίνεται. Το spread spectrum λειτουργεί χρησιμοποιώντας μαθηματικές λειτουργείες για τη διάχυση του σήματος σε ένα μεγάλο φάσμα συχνοτήτων. Όταν ο παραλήπτης πραγματοποιεί την αντιστροφή διαδικασία, το σήμα ανασυγκροτείται ως σήμα στενής ζώνης (narrow band) και κυρίως οποιασδήποτε θόρυβος της στενής ζώνης ελαχιστοποιείται έτσι ώστε το σήμα να είναι καθαρό.

Η χρήση των spread spectrum τεχνολογιών είναι απαιτούμενη για τις unlicensed συσκευές με σκοπό την μείωση της πιθανότητας να υπάρξουν παρεμβολές. Σε κάποιες περιπτώσεις, είναι ένα απαιτούμενο που επιβάλλεται από τις ρυθμιστικές αρχές, ενώ σε άλλες περιπτώσεις είναι ο μονός πρακτικός τρόπος για την εκπλήρωση των κανονιστικών απαιτήσεων. Για παράδειγμα, η FFC (Federal Communications Commission) απαιτεί οι συσκευές στη ζώνη ISM να χρησιμοποιούν spread spectrum μετάδοση και να επιβάλουν αποδεκτά εύρη σε διάφορες παραμέτρους.

Η διάδοση της μετάδοσης σε μια ευρεία μπάντα κάνει τις μεταδόσεις να μοιάζουν με θόρυβο σε έναν παραδοσιακό δεκτή στενής ζώνης (narrow band). Οποιοδήποτε τυποποιημένος spread spectrum δέκτης μπορεί να χρησιμοποιηθεί με ευκολία, ωστόσο, τα προσθετά μέτρα ασφαλείας είναι υποχρεωτικά σε όλα σχεδόν τα περιβάλλοντα.

Τα πλεονεκτήματα της χρησιμοποίησης του spread spectrum είναι η προσπάθεια αποφυγής των σκόπιμων και μη παρεμβολών και μπορεί επίσης ο χρήστης να μοιράζεται την ίδια μπάντα επικοινωνίας με άλλους χρήστες.

Αυτό δεν σημαίνει ότι το spread spectrum είναι μια “μαγική σφαίρα” που εξαλείφει το πρόβλημα της παρεμβολής. Οι spread spectrum συσκευές μπορεί να συγκρούονται με αλλά συστήματα επικοινωνίας, όπως επίσης και μεταξύ τους και οι παραδοσιακές συσκευές RF στενού φάσματος μπορούν να παρεμβαίνουν με τις spread spectrum συσκευές. Παρόλο που το spread spectrum κάνει καλύτερη δουλειά στην αντιμετώπιση του προβλήματος των παρεμβολών σε σύγκριση με άλλες τεχνικές διαμόρφωσης, δεν εξαλείφει το πρόβλημα. Όσο περισσότερες RF συσκευές λειτουργούν στην περιοχή που το δικό μας ασύρματο δίκτυο καλύπτει, θα παρατηρήσουμε ότι τα επίπεδα του θορύβου αυξάνονται, η αναλογία του σήματος με τον θόρυβο μειώνεται και το εύρος στο οποίο μπορείτε να επικοινωνήσετε αξιόπιστα μειώνεται. Για να μειωθούν οι παρεμβολές ανάμεσα στις συσκευές, η FFC επιβάλει περιορισμούς στην ισχύ της spread spectrum μετάδοσης.

3.2.1 Types of spread spectrum

Τα ασύρματα φυσικά επίπεδα στο 802.11 χρησιμοποιούν τρεις διαφορετικές spread spectrum τεχνικές:

- Frequency hopping (FH ή FHSS)- Τα Frequency- hopping συστήματα μεταπηδούν από την μια συχνότητα στην άλλη σε ένα τυχαίο μοτίβο, μεταδίδοντας μια σύντομη μετάδοση σε κάθε δευτερεύον κανάλι.
- Direct sequence (DS ή DSSS)- Τα Direct-sequence συστήματα διαδίδουν την ισχύ σε ένα πιο εύρη φάσμα συχνοτήτων χρησιμοποιώντας μαθηματικές λειτουργίες κωδικοποίησης
- Orthogonal Frequency Division Multiplexing (OFDM)- Το OFDM διαιρεί ένα διαθέσιμο κανάλι σε πολλά δευτερεύοντα κανάλια και κωδικοποιεί ένα τμήμα του σήματος σε κάθε παράλληλο δευτερεύον κανάλι.

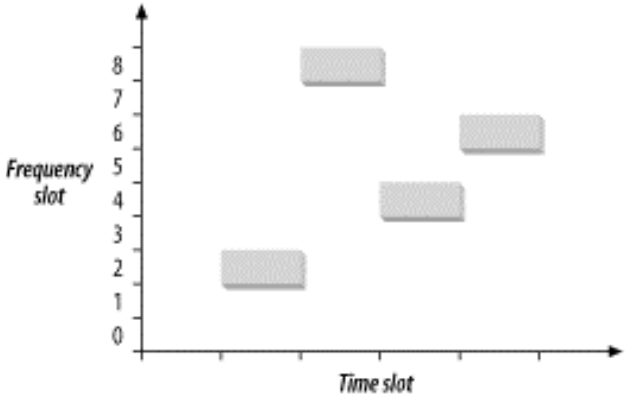
Τα Frequency- hopping συστήματα είναι τα πιο φτηνά στην κατασκευή. Η ακρίβεια στον χρόνο είναι αναγκαία για τον έλεγχο των μεταπηδήσεων στις συχνότητες, αλλά δεν απαιτείται εκλεπτυσμένη επεξεργασία του σήματος για την εξαγωγή της ροής bit από το ασύρματο σήμα. Τα Direct- sequence συστήματα απαιτούν πιο εκλεπτυσμένη επεξεργασία του σήματος, η οποία μεταφράζεται σε μεγαλύτερη ανάγκη για εξειδικευμένο hardware και υψηλότερη κατανάλωση ηλεκτρικής ισχύς. Η Direct- sequence τεχνική επιτρέπει επίσης μεγαλύτερο ρυθμό δεδομένων σε σχέση με τα Frequency- hopping συστήματα.

3.2.2 802.11 FH PHY

Από όλα τα φυσικά στρωματά που τυποποιήθηκαν στο πρώτο σχέδιο του 802.11 το 1977, το frequency- hopping spread spectrum (FHSS) ήταν το πρώτο που αναπτύχθηκε εκτεταμένα. Τα ηλεκτρονικά που χρησιμοποιούνται για τη στήριξη της διαφοροποίησης των συχνοτήτων είναι σχετικά φτηνά και δεν έχουν υψηλές απαιτήσεις ισχύος. Πρώτον, το κύριο πλεονέκτημα στην χρήση των frequency- hopping δικτύων ήταν ο μεγαλύτερος αριθμός των δικτύων που μπορούσαν να συνυπάρξουν και επίσης η υψηλή συνολική απόδοση όλων των δικτύων σε μια προκαθορισμένη περιοχή. Με την έλευση των συστημάτων υψηλοτέρων αποδόσεων direct- sequence, το πλεονέκτημα της συνολικής απόδοσης των frequency- hopping συστημάτων έχει εξαλειφθεί.

3.2.2.1 Frequency- hopping transmission

Το frequency- hopping εξαρτάται από την ταχεία αλλαγή της συχνότητας της μετάδοσης σε ένα, τυχαίο μοτίβο, όπως φαίνεται στο διάγραμμα. Ο κατακόρυφος άξονας του γραφήματος διαίρει τις διαθέσιμες συχνότητες σε έναν αριθμό από υποδοχές. Παρομοίως, ο χρόνος διαιρείται σε μια σειρά από υποδοχές και ένα μοτίβο ελέγχει πως θα χρησιμοποιηθούν οι υποδοχές. Στην εικόνα το μοτίβο είναι {2,8,4,7}. Ο συγχρονισμός των αλμάτων (hops) από την μια συχνότητα στην άλλη είναι το κλειδί για την επιτυχία και ο αποστολέας αλλά και ο παραλήπτης θα πρέπει να συγχρονιστούν έτσι ώστε ο παραλήπτης να ακούει πάντα στην συχνότητα του αποστολέα.

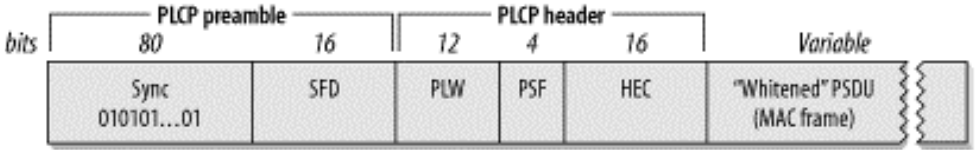


Σχήμα 11"Frequency hopping "

Το frequency- hopping είναι παρόμοιο με το frequency division multiple access (FDMA) αλλά με μια σημαντική διαφορά. Στα FDMA συστήματα, κάθε συσκευή κατανέμεται σε μια προκαθορισμένη συχνότητα. Πολλές συσκευές μοιράζονται το διαθέσιμο ασύρματο φάσμα χρησιμοποιώντας διαφορετικές συχνότητες. Στα frequency- hopping συστήματα, η συχνότητα είναι εξαρτώμενη με τον χρόνο και όχι προκαθορισμένη. Κάθε συχνότητα χρησιμοποιείται για μικρό χρονικό διάστημα που ονομάζεται dwell time.

3.2.2.2 FH PHY Convergence Procedure (PLCP)

Πριν οποιοδήποτε πακέτο διαμορφωθεί για να μεταδοθεί με τα ραδιοκύματα, πρέπει να προετοιμαστεί από το Physical Layer Convergence Procedure (PLCP). Το PLCP προσθέτει μια κεφαλίδα πέντε πεδίων στο πακέτο. Το PLCP βρίσκεται ανάμεσα στο mac layer και στο φυσικό μέσο.



Σχήμα 12"PLCP framing in the FH PHY "

- **Sync-** Το sync πεδίο έχει μέγεθος 80 bits και απαρτίζεται από μια σειρά από 0 και 1. Οι σταθμοί ψάχνουν για ένα μοτίβο συγχρονισμού με σκοπό την προετοιμασία για την παραλαβή των δεδομένων. Εκτός από τον συγχρονισμό του αποστολέα και του παραλήπτη, το Sync πεδίο εξυπηρετεί άλλους τρεις σκοπούς. Πρώτον, η παρουσία του sync σήματος υποδεικνύει ότι ένα πακέτο βρίσκεται στο μέσο επικοινωνίας. Δεύτερον, οι σταθμοί που έχουν πολλαπλές κεραίες μπορούν να διαλέξουν αυτήν με το ισχυρότερο σήμα. Τέλος, ο παραλήπτης μπορεί να μετρήσει τη συχνότητα των εισερχομένων σημάτων σε σχέση με τις αρχικές εκτιμήσεις και να προβεί στις απαραίτητες διορθώσεις.
- **Start Frame Delimiter (SFD)-** Όπως συμβαίνει και στο ethernet, το SFD σηματοδοτεί το τέλος του preamble και σηματοδοτεί την αρχή του πακέτου. Το FH PHY χρησιμοποιεί ένα 16-bit SFD.
- **Header-** Στο PLCP header τρία πεδία περιλαμβάνονται στη κεφαλίδα: το length field, το speed field και το frame check sequence.ακολουθεί του preamble
- **PSDU Length Word (PLW)-** Το πρώτο πεδίο στο PLCP είναι το PLW. Το φορτίο ενός PLCP πακέτου είναι ένα MAC πακέτο το οποίο μπορεί να έχει μέγεθος μέχρι και 4095 bytes. Το πεδίο με μέγεθος 12 bit πληροφορεί τον παραλήπτη για το μέγεθος του MAC πακέτου που ακολουθεί το PLCP header.
- **PLCP Signaling (PSF)-** Το πρώτο Bit είναι κατοχυρωμένο και είναι πάντα 0. Τα bits 1- 3 κωδικοποιούν τη ταχύτητα με την οποία το MAC πακέτο μεταδίδεται.

Πίνακας 3 "PSF meaning"

Bits (1-2-3)	Data Speed
000	1.0 Mbps
001	1.5 Mbps
010	2.0 Mbps
011	2.5 Mbps
100	3.0 Mbps
101	3.5 Mbps
110	4.0 Mbps
111	4.5 Mbps

- **Header Error Check (HEC)-** Για να προστατευτεί από τα λάθη το PLCP header, υπολογίζει από τα περιεχόμενα του header ένα CRC μεγέθους 16 bit. Το header δεν προστατεύεται από τα λάθη σε άλλο σημείο του πακέτου.

3.2.2.3 Frequency- Hopping PMD sublayer

Παρόλο, που το PLCP header έχει ένα πεδίο που αφορά την ταχύτητα με την οποία μεταδίδεται ένα MAC πακέτο, μόνο δυο από αυτές τις τιμές (1.0 Mbps και 2.0 Mbps) έχουν αντίστοιχο τυποποιημένο PMD layer.

Πίνακας 4"FH PHY parameters"

Parameter	**Value**	**Notes**
Slot time	50μs	
Contention Windows Size	15- 1023 slots	
Preamble Duration	96μs	Τα σύμβολα του preamble μεταδίδονται στο 1 MHz, άρα ένα σύμβουλο χρειάζεται 1 sec για να μεταδοθεί, άρα 96 bits απαιτούν 96 symbol times.

PLCP header duration	32μs	Η PLCP κεφαλίδα είναι 2 Bits, άρα απαιτούνται 32 symbol times
Maximum MAC frame	4095 bytes	Το 802.11 προτείνει ένα μέγιστο όριο των 400 symbols (400 bytes στο 1 Mbps, 800 bytes στα 2 Mbps) για να διατηρηθεί η απόδοση σε διαφορετικά περιβάλλοντα

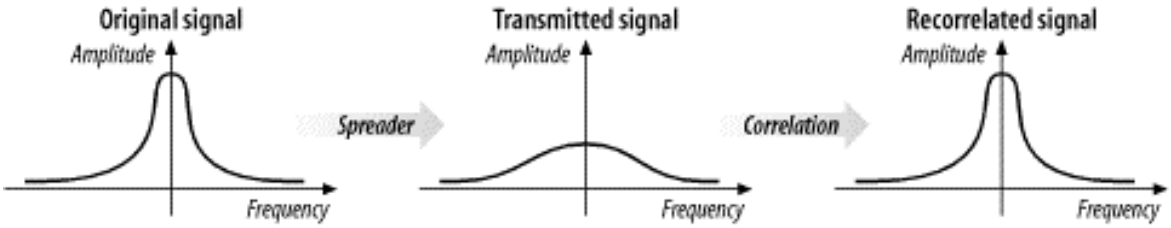
3.2.3 802.11 DS PHY

Η διαμόρφωση Direct- sequence υπήρξε η πιο επιτυχημένη τεχνική διαμόρφωσης που χρησιμοποιήθηκε από το 802.11. Ο αρχικός προσδιορισμός του 802.11 περιγράφει είναι physical layer που βασίζεται σε χαμηλές ταχύτητες και στην τεχνική direct- sequence spread spectrum (DS ή DSSS). Ο direct- sequence εξοπλισμός απαιτεί περισσότερη ισχύ για να επιτύχει την ιδιά απόδοση με τα frequency- hopping συστήματα. Μια διεπαφή (interface) direct- sequence των 2 Mbps θα εξαντλήσει πιο γρηγορά τη μπαταρία από μια διεπαφή frequency- hopping των 2 Mbps. Το αληθινό πλεονέκτημα της direct-sequence μετάδοσης είναι ότι η τεχνική προσαρμόζεται πολύ πιο γρηγορά σε υψηλότερες ταχύτητες σε σχέσης με τα frequency- hopping δίκτυα.

3.2.3.1 Direct- Sequence- Transmission

Η Direct- Sequence μετάδοση είναι μια εναλλακτική τεχνική spread spectrum η οποία μπορεί να χρησιμοποιηθεί για να μεταδώσει το σήμα σε ένα πολύ μεγαλύτερο φάσμα συχνοτήτων. Η βασική προσέγγιση της direct- sequence τεχνικής είναι να παραλειφει την ενέργεια της ραδιοσυχνότητας σε ένα μεγάλο φάσμα συχνοτήτων με έναν προσεκτικό και ελεγχόμενο τρόπο. Οι αλλαγές στον φορέα των ραδιοκυμάτων είναι φανερές σε όλο το μήκος του φάσματος και οι παραλήπτες μπορούν να πραγματοποιήσουν διαδικασίες διόρθωσης για να βρουν τυχόν αλλαγές. Η DSSS τεχνική έχει δυο κύρια πλεονεκτήματα. Προσφέρει το όφελος της εξάπλωσης του σήματος έναντι των narrowband (στενής ζώνης) σημάτων παρεμβολής και εξαπλώνει το μεταδιδόμενο σήμα σε ένα πλατύ εύρος έτσι ώστε η

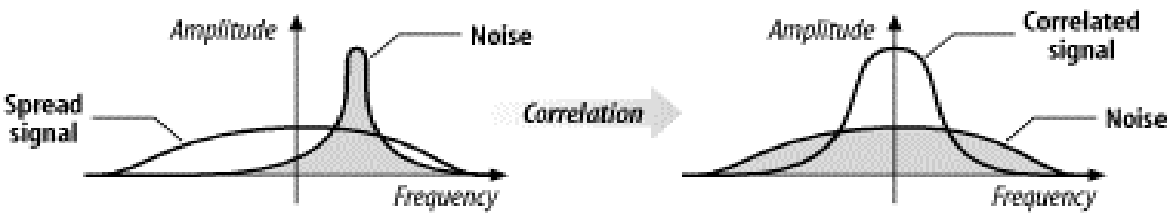
μετάδοση να μοιάζει με θόρυβο σε έναν narrowband δέκτη. Αυτά τα δυο χαρακτηρίστηκα είναι ο λόγος που το DSSS αρχικά χρησιμοποιούνταν από τον στρατό επειδή είναι δύσκολο να πραγματοποιηθεί κάποια σύγκρουση στη μετάδοση και είναι δύσκολο να εντοπιστεί από narrowband ασυρμάτους. Αυτά τα δυο χαρακτηρίστηκα κάνουν, επίσης, τη DSSS τεχνική ιδανική για την συνύπαρξη με άλλους narrowband χρήστες.



Σχήμα 13"Basic DSSS technique "

Στα αριστερά είναι το παραδοσιακό ασύρματο σήμα, το οποίο επεξεργάζεται από έναν spreader, ο οποίος εφαρμόζει έναν μαθηματικό μετασχηματισμό , για να πάρει το σήμα μιας στενής ζώνης(narrowband) εισόδου και να ισοπεδώσει το εύρος σε μια σχετικά ευρεία ζώνη συχνοτήτων. Σε έναν δέκτη στενής ζώνης, το σήμα που μεταδίδεται μοιάζει με χαμηλό θόρυβο επειδή η ενέργεια των ραδιοκυμάτων απλώνεται σε ένα πολύ πλατύ φάσμα. Το κλειδί για τη direct- sequence μετάδοση είναι ότι οποιαδήποτε διαμόρφωση του φορέα των ραδιοκυμάτων απλώνεται επίσης σε όλο το φάσμα της συχνότητας. Οι δέκτες μπορούν να παρατηρήσουν ένα ευρύ φάσμα συχνοτήτων και να ψάχνουν για αλλαγές που συμβαίνουν σε ολόκληρο το φάσμα. Το αρχικό σήμα μπορεί να ανακτηθεί με έναν correlator (συσχετιστής), ο οποίος αντιστρέφει την spreading διαδικασία.

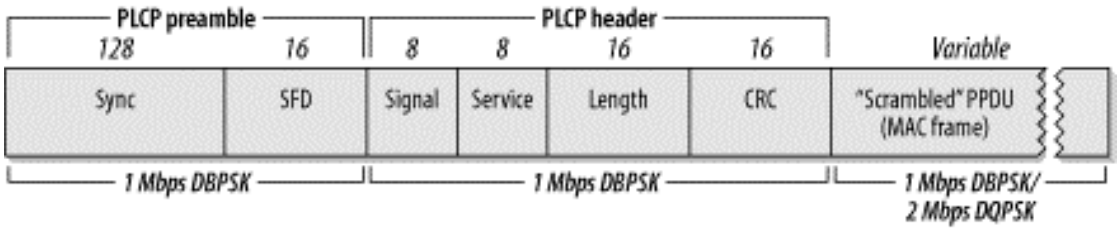
Σε υψηλό επίπεδο, ο correlator απλά ψάχνει για αλλαγές στο σήμα των ραδιοκυμάτων που συμβαίνουν σε ολόκληρο το εύρος του φάσματος. Η συσχέτιση (correlation) δίνει στη direct- sequence μετάδοση μια μεγάλη προστασία από τις παρεμβολές. Ο θόρυβος τείνει να πάρει τη μορφή σχετικά στενών παλμών, οι οποίοι, εξ ορισμού, δεν παράγουν συνεκτικά αποτελέσματα σε ολόκληρη την μπάντα συχνοτήτων. Επομένως, η διαδικασία της συσχέτισης απλώνει τον θόρυβο και το συσχετισμένο σήμα γίνεται πιο εύκολα αντιληπτό.



Σχήμα 14"Spreading of noise by correlation process "

3.2.3.2 DS Physical- Layer Convergence (PLCP)

Όπως στο FH PHY τα πακέτα πρέπει να επεξεργαστούν από το PLCP πριν αρχίσει η μετάδοση τους. Το ίδιο συμβαίνει και στο DS PHY. Το PLCP για το DS PHY προσθέτει μια κεφαλίδα 6 πεδίων στο πακέτο που λαμβάνει από το MAC Layer.



Σχήμα 15"DS PLCP framing "

Preamble- Το preamble συγχρονίζει τον αποστολέα και τον παραλήπτη. Αποτελείται από το Sync πεδίο και το Start Frame Delimiter πεδίο. Πριν την μετάδοση, το preamble κρυπτογραφείται χρησιμοποιώντας τη direct- sequence λειτουργεία κρυπτογράφησης.

Sync-Το Sync πεδίο έχει μέγεθος 128 bits και αποτελείται εξολοκλήρου από bit με τιμή 1. Σε αντίθεση με το FH PHY, το Sync πεδίο κωδικοποιείται πριν την μετάδοση.

Start Frame Delimiter (SFD)- Το SFD επιτρέπει τον παραλήπτη να αναγνωρίσει την αρχή του πακέτου, ακόμη και αν κάποια από τα bits του πεδίου sync έχουν χαθεί κατά τη διάρκεια της μετάδοσης. Το πεδίο έχει την τιμή 0000 0101 1100 1111, η οποία είναι διαφορετική από την τιμή που έχει το SFD που χρησιμοποιείται από το FH PHY.

Header- Η PLCP κεφαλίδα ακολουθεί του preamble. Η κεφαλίδα αποτελείται από το signaling πεδίο, το service identification πεδίο, το length πεδίο, το signal πεδίο που χρησιμεύει στην κωδικοποίηση της ταχύτητας και το frame check sequence.

Signal- Το Signal πεδίο χρησιμοποιείται από τον παραλήπτη για να αναγνωρίσει τον ρυθμό μετάδοσης του ενθυλακωμένου MAC πακέτου. Είναι ορισμένο είτε με την τιμή 0000 1010 για την λειτουργεία στο 1 Mbps είτε 0001 0100 για την λειτουργεία στα 2 Mbps.

Service- Αυτό το πεδίο είναι κατοχυρωμένο για μελλοντική χρήση.

Length- Αυτό το πεδίο έχει οριστεί ως ένας αριθμός από microseconds που απαιτούνται για να μεταδοθεί το πακέτο ως ένας ακέραιος αριθμός 16 bit.

CRC- Για την προστασία της κεφαλίδας εναντίον της αλλοίωσης στο ασύρματο μέσο, ο αποστολέας υπολογίζει ένα CRC 16 bit συνυπολογίζοντάς και τα τέσσερα πεδία της κεφαλίδας. Ο παραλήπτης επαληθεύει το CRC πριν επεξεργαστεί περεταίρω το πακέτο.

Πίνακας 5"DS PHY parameters"

Parameter	**Value**	**Notes**
Slot time	20μs	
Contention window size	31 to 1023 slots	
Preamble duration	144μs	Τα σύμβολα του preamble μεταδίδονται στο 1 MHz, άρα ένα σύμβολο παίρνει 1 s για να μεταδοθεί, άρα και τα 144 bits απαιτούν 144 symbol times
PLCP Header	48μs	Η PLCP κεφαλίδα έχει μέγεθος 48 bits, άρα απαιτεί 48 symbol times
Maximum MAC frame	4- 8191 bytes	

3.2.4 Orthogonal Frequency Division Multiplexing (OFDM)

Το 802.11a είναι βασισμένο στο orthogonal frequency division multiplexing. Το OFDM δεν είναι μια καινούργια τεχνική. Το μεγαλύτερο μέρος της θεμελιώδους εργασίας πραγματοποιήθηκε στα τέλη του 1960. Η πρόσφατη DSL εργασία (HDSL, VDSL και ADSL) έχει αναζωπυρώσει το ενδιαφέρον για το OFDM, ειδικά τώρα όπου υπάρχουν καλύτερες τεχνικές επεξεργασίας του σήματος και καθιστούν το OFDM πιο πρακτικό. Το OFDM, ωστόσο, διαφέρει από τις άλλες αναδυόμενες τεχνικές κωδικοποίησης όπως η code division multiple access (CDMA) στη προσέγγιση του. Η CDMA χρησιμοποιεί περίπλοκες μαθηματικές εφαρμογές για να τοποθετήσει τις πολλαπλές μεταδόσεις σε ένα μόνο φορέα μετάδοσης. Το OFDM κωδικοποιεί μια μετάδοση σε πολλαπλούς φορείς μετάδοσης. Τα μαθηματικά που χρησιμοποιούνται στη CDMA είναι πολύ πιο περίπλοκα από αυτά που χρησιμοποιούνται στο OFDM. Οι OFDM συσκευές χρησιμοποιούν ένα μόνο κανάλι συχνότητας “σπάζοντας” το σε πολλά υποκανάλια. Κάθε υποκανάλι χρησιμοποιείται για τη μετάδοση των δεδομένων. Όλα τα “αργά” υποκανάλια κατά τη μετάδοση πολυπλέκονται σε ένα “γρήγορο” συνδυασμένο κανάλι.

3.2.4.1 Carrier Multiplexing

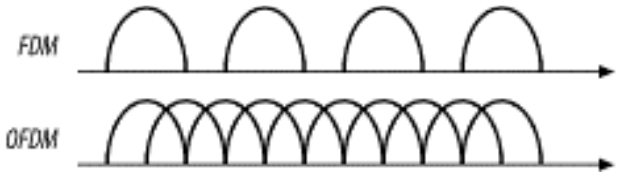
Η ανάγκη για την αύξηση της ταχύτητας των μεταδόσεων των δεδομένων οδήγησε στη δημιουργία πλήθους τεχνολογιών που είχαν ως στόχο να αυξήσουν την ταχύτητα. Το OFDM έχει παρόμοια προσέγγιση με το Multilink PPP, δηλαδή όταν ο ένα σύνδεσμος (link) δεν είναι αρκετός, τότε χρησιμοποιούνται αρκετοί σύνδεσμοι παράλληλα.

Το OFDM είναι στενά συνδεδεμένο με το παλιό frequency division multiplexing (FDM). Και τα δυο διαιρούν το διαθέσιμο bandwidth σε κομμάτια που ονομάζονται carriers ή subcarriers και χρησιμοποιούν τα διαθέσιμα carriers ως ξεχωριστά κανάλια για την μετάδοση των δεδομένων. Το OFDM αυξάνει το throughput χρησιμοποιώντας παράλληλα αρκετά subcarriers και πολυπλεκοντας τα δεδομένα πάνω από ένα σύνολο subcarriers.

Το παραδοσιακό FDM χρησιμοποιούνταν ευρέως από τα κινητά τηλεφωνά της πρώτης γενιάς ως μια μέθοδος για τη διανομή ασυρμάτων καναλιών. Σε κάθε χρήστη δίνονταν ένα αποκλειστικό κανάλι και ένα guard band, που χρησιμοποιούνταν για να διασφαλιστεί ότι η φασματική διαρροή από τον έναν χρήστη δεν θα προκαλέσει προβλήματα σε άλλους χρήστες των γειτονικών καναλιών.

Σχήμα 16"Traditional FDM "

Το μειονέκτημα του παραδοσιακού FDM είναι ότι οι guard bands ξοδεύουν το διαθέσιμο bandwidth και επίσης μειώνουν τη χωρητικότητα. Για το πρόβλημα της σπάταλης της χωρητικότητας της μετάδοσης, το OFDM επιλέγει τα κανάλια να επικαλύπτονται αλλά να μην παρεμβάλλονται μεταξύ τους.

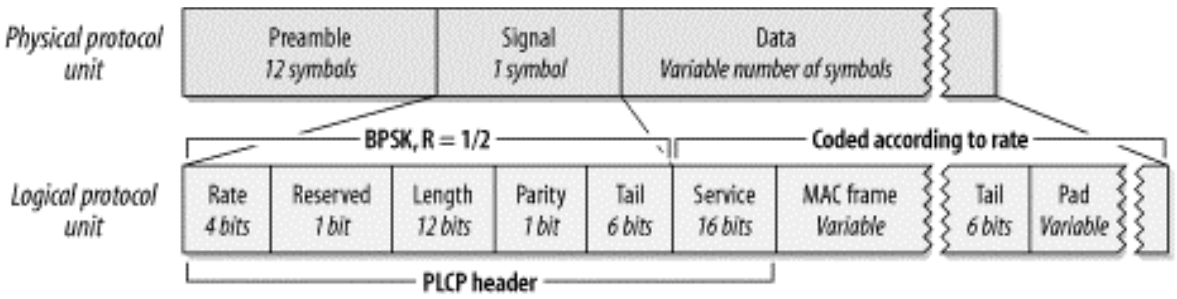


Σχήμα 17"FDM versus OFDM "

Οι επικαλύψεις των carriers επιτρέπονται επειδή τα subcarriers ορίζονται έτσι ώστε να διακρίνονται εύκολα το ένα από το άλλο. Η ικανότητα να ξεχωρίζονται τα subcarriers βασίζεται σε μια περιπλοκή μαθηματική σχέση που ονομάζεται orthogonally.

3.2.4.2 Framing

Το OFDM PHY προσθέτει ένα preamble και μια PLCP κεφαλίδα στο πακέτο. Επίσης προσθέτει κάποια bits στο τέλος που βοηθούν στην κωδικοποίηση.



Σχήμα 18"OFDM PLCP framing format "

Το preamble διαρκεί 16 μs, μετά το preamble ένα OFDM σύμβολο περιέχει το πεδίο Signal, στη συνέχεια ένας μεταβλητός αριθμός από δεδομένα περιέχει το τέλος της PLCP κεφαλίδας, το MAC φορτίο και το trailer.

Preamble- Όπως με όλα τα αλλά 802 δίκτυα, και κυρίως με όλα τα 802.11 physical layers, το OFDM ξεκινάει με ένα preamble. Αποτελείται από 12 OFDM σύμβολα που συγχρονίζουν διάφορους χρόνους ανάμεσα στον αποστολέα και στο δέκτη. Τα πρώτα 10 σύμβολα χρησιμοποιούνται από το δέκτη για να εντοπίσει το σήμα και να επιλέξει την κατάλληλη κεραία αν οκ δέκτης χρησιμοποιεί πολλές κεραίες.

Rate (4 bits)- Αποτελείται από 4 bits που χρησιμοποιούνται για να κωδικοποιούν τον ρυθμό μετάδοσης.

Πίνακας 6"Rate bits"

Data rate (Mbps)	**Bits**
6	1101
9	1111
12	0101
18	0111
24	1001
36	1011
48	0001
54	0011

Length (12 bits)- Δώδεκα bits κωδικοποιούν τον αριθμός των bytes που βρίσκονται στο ενσωματωμένο MAC frame. Όπως συμβαίνει με τα περισσότερα πεδία, έτσι και αυτό μεταδίδεται από το λιγότερο σημαντικό στο περισσότερο σημαντικό bit.

Parity (1 bit) και Reserved (1 bit)- Το 4ο bit είναι κατοχυρωμένο για μελλοντική χρήση και θα πρέπει να είναι ίσο με το 0. Το 17ο bit είναι ένα parity bit για τα πρώτα 16 Signal bit που τα προστατεύει από την αλλοίωση των δεδομένων.

Tail (6 bits)- Το Signal πεδίο τελειώνει με έξι tail bits με τιμή 0.

Service (16 bits)- Το τελευταίο πεδίο της PLCP κεφαλίδας είναι το πεδίο Service με μέγεθος 16 bit. Αντίθετα από τα άλλα πεδία της PLCP κεφαλίδας, μεταδίδεται στο Data πεδίο του φυσικού πρωτοκόλλου με το ρυθμό μετάδοσης του MAC frame. Τα πρώτα 8 bits έχουν τιμή 0.

Trailer Tail (6 bits) – Όπως και με το tail στη PLCP κεφαλίδα, τα tail bits είναι προσαρτημένα στο τέλος του MAC frame για να φέρει ομαλά το τέλος του κώδικα.

3.2.4.3 OFDM PMD

Το OFDM PHY χρησιμοποιεί ένα μίγμα από διαφορετικά σχήματα διαμόρφωσης με σκοπό να επιτύχει έναν ρυθμό απόδοσης ανάμεσα στα 6 Mbps και στα 54 Mbps. Σε όλες τις περιπτώσεις, το physical layer χρησιμοποιεί έναν συμβολικό ρυθμό απόδοσης της τάξεως των 250.000 συμβολών ανά δευτερόλεπτο δια μέσου των 48 subchannels. Ο αριθμός των bits που περιέχουν δεδομένα ανά σύμβολο διαφέρει. Ένα OFDM σύμβολο καλύπτει και τα 48 subchannels.

Πίνακας 7"OFDM PHY parameters"

Parameter	**Value**
Maximum MAC frame length	4095 bytes
Slot time	9 μs
Contention window size	15 to 1023 slots
Preamble duration	20 μs
PCLP header	4 μs

ΕΠΙΛΟΓΟΣ

Στο προηγούμενο κεφάλαιο αναφερθήκαμε στο φυσικό επίπεδο και ιδιαίτερα τις spread spectrum τεχνικές οι οποίες χρησιμοποιούνται για να βελτιώσουν την ασύρματη επικοινωνία, καθώς σχεδιάστηκαν με σκοπό να διαδίδουν το σήμα σε μια μεγαλύτερη συχνότητα με σκοπό να την αποτροπή των παρεμβολών.

Στο επόμενο κεφάλαιο θα μιλήσουμε για το MAC επίπεδο και τα πρωτοκολλά που χρησιμοποιούνται σε αυτό το επίπεδο για να μοιράζεται σωστά το μέσο επικοινωνίας στους ασύρματους σταθμούς, καθώς και για κάποια προβλήματα που παρατηρούνται.

ΚΕΦΑΛΑΙΟ 4

802.11 MAC

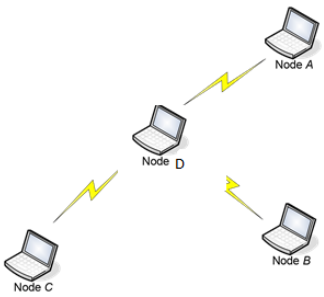
ΕΙΣΑΓΩΓΗ

Το κλειδί στο πρωτόκολλο 802.11 είναι το MAC επίπεδο, βρίσκεται πάνω από το PHY επίπεδο και ελέγχει την μετάδοση των δεδομένων του χρήστη στον αέρα. Διαφορετικά φυσικά επίπεδα μπορεί να προσφέρουν διαφορετικές ταχύτητες μετάδοσης και όλες αυτές θα πρέπει να διαλειτουργούν μεταξύ τους. Το 802.11 δεν παρεκκλίνει ριζικά από τα προηγούμενα IEEE 802 πρωτόκολλα. Το πρωτόκολλο υιοθετεί επιτυχώς τον Ethernet τρόπο δικτύωσης αλλά με ασύρματες συνδέσεις. Όπως στο Ethernet, το 802.11 χρησιμοποιεί έναν μηχανισμό carrier sense multiple access (CSMA) για να ελέγχει τη πρόσβαση στο μέσο μετάδοσης. Σε αντίθεση με το πρωτόκολλο 802.3 Ethernet, το πρωτόκολλο MAC 802.11 δεν υλοποιεί την ανίχνευση σύγκρουσης. Ο σημαντικότερος λόγος είναι ότι η δυνατότητα ανίχνευσης συγκρούσεων απαιτεί να υπάρχει η δυνατότητα αποστολής και λήψης ταυτόχρονα. Επειδή η ισχύς του λαμβανομένου σήματος είναι τυπικά πολύ μικρή σε σύγκριση με την ισχύ του μεταδιδόμενου σήματος στον 802.11 adaptor, είναι αδύνατον να κατασκευαστεί κάποιο υλικό που να μπορεί να ανιχνεύσει μια σύγκρουση.
Επίσης όπως στο Ethernet, το 802.11 χρησιμοποιεί ένα σχήμα κατανεμημένης πρόσβασης χωρίς κεντρική διαχείριση. Κάθε 802.11 σταθμός χρησιμοποιεί την ίδια μέθοδο για να αποκτήσει πρόσβαση στο μέσο.

4.1 Hidden node problem

Ο εντοπισμός των συγκρούσεων στα WLANs είναι αρκετά δύσκολος από την στιγμή που όλοι οι ασύρματοι σταθμοί μπορεί να μην έχουν την δυνατότητα να ακούνε ο ένας τον άλλον κάθε στιγμή. Ένας σταθμός μπορεί να μην είναι μέσα στην εμβέλεια των άλλων σταθμών. Στην παρακάτω εικόνα, οι σταθμοί A, B και C βρίσκονται μέσα στην εμβέλεια του σταθμού D, αλλά δεν βρίσκονται μέσα στην εμβέλεια του καθενός. Ο σταθμός A μπορεί να εντοπίσει μια μετάδοση που προέρχεται από τον σταθμό B, αλλά δεν μπορεί να εντοπίσει μια μετάδοση που προέρχεται από τον σταθμό C (εκτός εμβέλειας). Αν ο σταθμός A ακούσει το ασύρματο μέσο και δεν ακούσει τίποτα, τότε θα το θεωρήσει αδρανές και ότι είναι ελεύθερο για να αρχίσει την μετάδοση του, ενώ την ίδια στιγμή ο σταθμός C μεταδίδει. Αυτό το πρόβλημα είναι γνωστό ως το πρόβλημα του κρυμμένου κόμβου (hidden node). Σε αυτή την περίπτωση αν ο σταθμός A αρχίσει τη μετάδοση του τότε θα υπάρξει σύγκρουση. Ως αποτέλεσμα αυτής της σύγκρουσης και ο σταθμός A αλλά και ο σταθμός C θα

πρέπει να μεταδώσουν ξανά τα πακέτα δεδομένων τους, κάτι το οποίο θα έχει ως αποτέλεσμα την αύξηση του overhead.

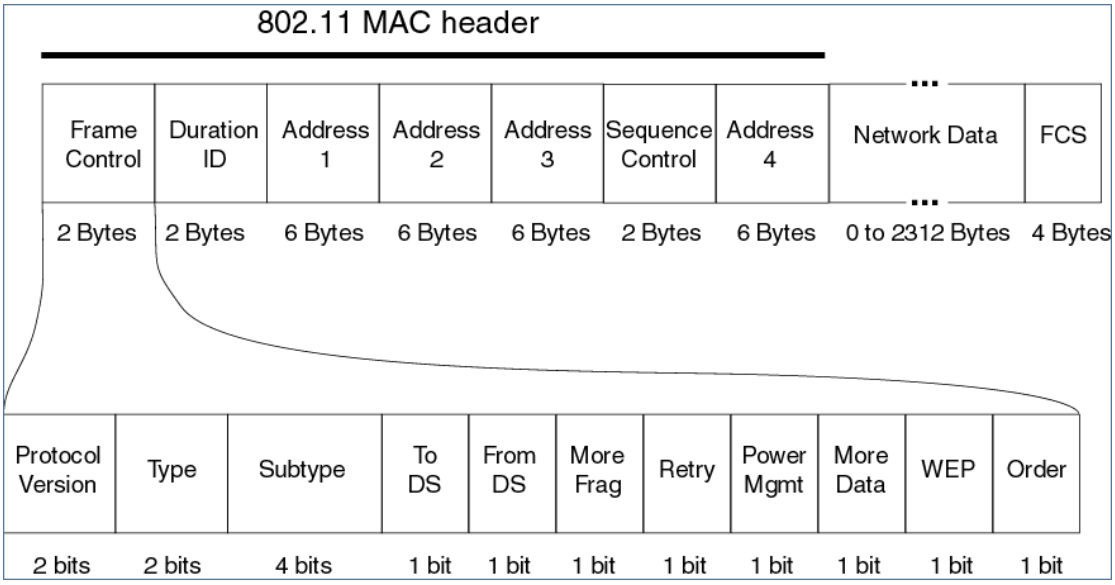


Σχήμα 19"Hidden Terminal Problem "

Το IEEE 802.11 πρωτόκολλο συμπεριλαμβάνει έναν προαιρετικό χαρακτηριστικό του RTS/ CTS (Request To Send/ Clear To Send) μηχανισμού για να ελέγχει την πρόσβαση του σταθμού στο ασύρματο μέσο όταν συμβαίνουν συγκρούσεις λόγω του προβλήματος του κρυμμένου κόμβου. Αυτό το χαρακτηριστικό ονομάζεται virtual carrier sensing (αναλύεται στο παρακάτω υποκεφάλαιο).

4.2 Το IEEE 802.11 frame

Αν και το 802.11 frame έχει πολλές ομοιότητες με ένα Ethernet frame, περιέχει επίσης και αρκετά πεδία, που αφορούν ειδικά στη χρήση του για ασύρματες ζεύξεις. Το 802.11 frame φαίνεται στην παρακάτω εικόνα. Οι αριθμοί κάτω από κάθε πεδίο μέσα στο frame παριστάνουν το μήκος των πεδίων σε byte. Οι αριθμοί κάτω από κάθε υποπεδίο μέσα στο πεδίο frame control παριστάνουν τα μήκη των υποπεδίων σε bit. Παρακάτω εξετάζουμε μερικά από τα πιο σημαντικά πεδία του frame καθώς και κάποια σημαντικά υποπεδία μέσα στο πεδίο frame control του 802.11 frame.



Σχήμα 20"802.11 frame "

Network Data και FCS

Στο πυρήνα του frame βρίσκεται το Network Data (ωφέλιμο φορτίο), που τυπικά αποτελείται από ένα IP πακέτο ή ένα ARP πακέτο. Αν και το πεδίο επιτρέπεται να έχει μήκος μέχρι 2.312 bytes, συνήθως περιέχει λιγότερα από 1500 bytes , που περιέχουν ένα IP πακέτο ή ένα ARP πακέτο (κανονικά το IP πακέτο μπορεί να έχει μέγεθος και περισσότερο από 1500 bytes, όμως επειδή τις περισσότερες φορές μεταδίδεται μέσω ethernet τεχνολογίας αναγκάστηκα η μέγιστη μονάδα μετάδοσης (MTU) είναι 1500bytes). Όπως με ένα Ethernet frame, ένα 802.11 frame περιλαμβάνει ένα πεδίο ελέγχου σφαλμάτων FCS (Frame Check Sequence) με μήκος 32 bit, έτσι ώστε ο δέκτης να μπορεί να ανιχνεύει τα σφάλματα bit στο λαμβανόμενο frame.

ADDRESS FIELDS

Η εμφανέστερη ίσως διαφορά στο 802.11 frame είναι ότι περιέχει τέσσερα πεδία διευθύνσεων, όπου το κάθε ένα μπορεί να περιέχει μια διεύθυνση MAC με μήκος 6 bytes.

- Address 1: είναι η διεύθυνση MAC του ασύρματου σταθμού, που πρόκειται να λάβει το frame. Έτσι, εάν ένας κινητός ασύρματος σταθμός μεταδίδει το

frame, η address 1 περιέχει τη διεύθυνση MAC του access point προορισμού. Παρόμοια, εάν ένα access point μεταδίδει το frame, η address 1 περιέχει την διεύθυνση MAC του ασύρματου σταθμού προορισμού.

- Address 2: είναι η διεύθυνση MAC του ασύρματου σταθμού, που μεταδίδει το frame. Έτσι, εάν ένας ασύρματος σταθμός μεταδίδει το frame, η διεύθυνση MAC του σταθμού εισάγεται στο πεδίο address 2. Παρόμοια, εάν το access point μεταδίδει το πλαίσιο, η διεύθυνση MAC του access point εισάγεται στο πεδίο address 2.
- Address 3: περιέχει την MAC διεύθυνση του interface του router.

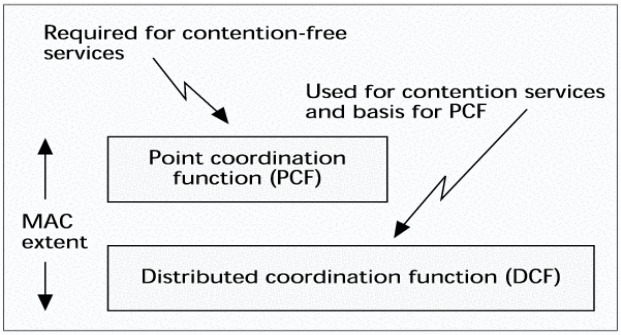
Πεδία Sequence Control και Frame Control

Στο 802.11, οποτεδήποτε ένας σταθμός λαμβάνει σωστά ένα frame από έναν άλλον σταθμό, στέλνει πίσω μια επιβεβαίωση. Επειδή οι επιβεβαιώσεις μπορεί να χαθούν, ο σταθμός αποστολής μπορεί να στείλει πολλαπλά αντίγραφα ενός data frame. Η χρήση αριθμών ακολουθίας επιτρέπει στον παραλήπτη να διακρίνει ανάμεσα σε ένα νέο μεταδιδόμενο frame και στην αναμετάδοση ενός προηγούμενου frame.
Το πρωτόκολλο 802.11 επιτρέπει σε έναν σταθμό που κάνει μετάδοση, να δεσμεύει το κανάλι για ένα χρονικό διάστημα, που περιλαμβάνει το χρόνο που απαιτείται για τη μετάδοση του data frame και του χρόνου που απαιτείται για τη μετάδοση μιας επιβεβαίωσης. Αυτή η τιμή διάρκειας περιλαμβάνεται στο πεδίο duration.
Όπως απεικονίζεται στην παραπάνω εικόνα, το πεδίο frame control περιλαμβάνει πολλά υποπεδία. Τα πεδία type και subtype χρησιμοποιούνται για τη διάκριση των frame συσχέτισης, του RTS, του CTS και των data frame. Τα πεδία to DS και from DS χρησιμοποιούνται προκειμένου να ορίσουν τις σημασίες των διάφορων πεδίων διευθύνσεων. Τέλος, το πεδίο WEP δηλώνει εάν χρησιμοποιείται κρυπτογράφηση ή όχι.

4.3 Distribution Coordination Function

Το βασικό MAC πρωτόκολλο που χρησιμοποιείται είναι το DCF, το οποίο επιτρέπει τους σταθμούς να μοιράζονται αυτόματα το μέσο επικοινωνίας μέσω της χρήσης του CSMA/CA και ενός τυχαίου αλγορίθμου οπισθοχώρησης. Το DCF θα πρέπει να

εφαρμοστεί σε όλους τους σταθμούς για την χρήση του μεταξύ των ad hoc δικτυών και των δικτυών με υποδομή (infrastructure network). Το DCF λειτουργεί μόνο του στα ad hoc δίκτυα, ενώ στα δίκτυα με υποδομή είτε λειτουργεί μόνο του είτε λειτουργεί με την συνύπαρξη του με το PCF (Point Coordination Function). Η MAC αρχιτεκτονική που απεικονίζεται στην παρακάτω εικόνα, στην οποία το DCF βρίσκεται ακριβώς πάνω από το φυσικό επίπεδο και υποστηρίζει τις λειτουργίες για την αποφυγή των συγκρούσεων. Αυτές οι λειτουργίες υπονοούν ότι κάθε σταθμός με ένα MSDU (media access control service data unit) ,που βρίσκεται στην ουρά για μετάδοση, θα πρέπει να «αγωνιστεί» για να έχει πρόσβαση στο κανάλι επικοινωνίας και ότι, όταν το MSDU μεταδίδεται, θα πρέπει να προσπαθήσει ξανά για να έχει πρόσβαση στο κανάλι επικοινωνίας για όλα τα μεταγενέστερα πακέτα. Οι λειτουργίες για την αποφυγή συγκρούσεων υποστηρίζουν την δίκαιη πρόσβαση στο κανάλι επικοινωνίας για όλους τους σταθμούς.



Σχήμα 21“MAC Architecture "

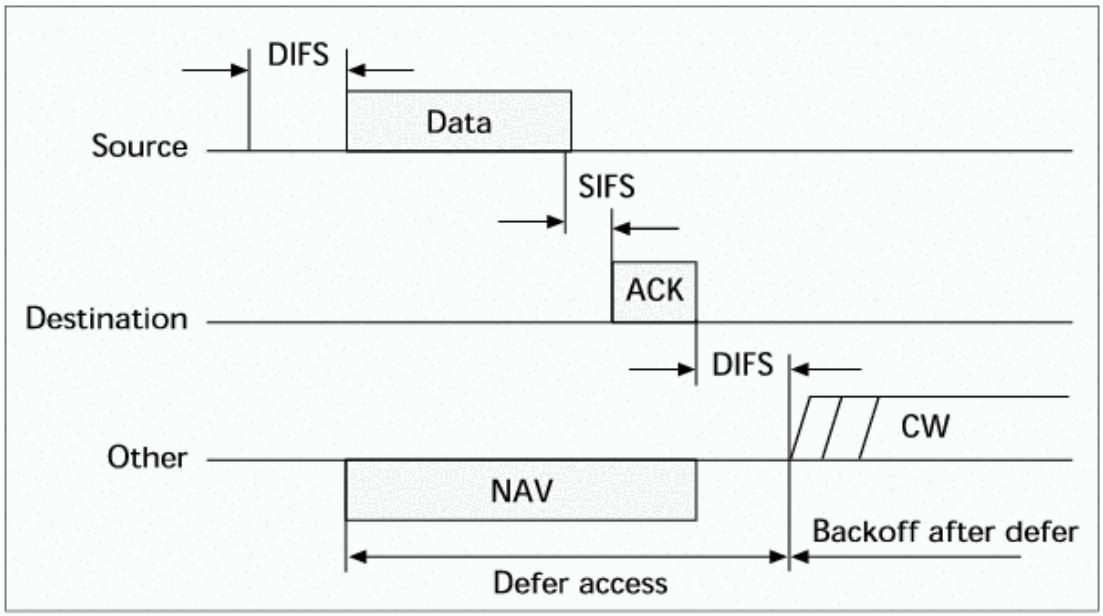
Το CSMA/CA πρωτόκολλο σχεδιάστηκε για την μείωση της πιθανότητας σύγκρουσης αναμεσά σε πολλούς σταθμούς που έχουν πρόσβαση στο μέσο επικοινωνία. Αμέσως μόλις το μέσο επικοινωνίας γίνει αδρανές έπειτα από μεγάλη χρήση, τότε είναι η στιγμή όπου υπάρχει η μεγαλύτερη πιθανότητα να υπάρξει σύγκρουση. Αυτό συμβαίνει επειδή πολλοί σταθμοί μπορεί να ανέμεναν να γίνει ξανά διαθέσιμο το μέσο επικοινωνίας. Αυτή είναι η κατάσταση, η οποία απαιτεί μια τυχαία διαδικασία οπισθοχώρησης από τους σταθμούς για να επιλυθεί το πρόβλημα των συγκρούσεων.

Οι σταθμοί, οι οποίοι χρειάζονται να μεταδώσουν δεδομένα, πρώτα “ακούν” το μέσο επικοινωνίας. Στο IEEE 802.11, το άκουσμα του μέσου επικοινωνίας διενεργείται και στη διεπαφή του αέρα, που ονομάζεται physical carrier sensing και στο MAC υποεπίπεδο, που ονομάζεται virtual carrier sensing. Το physical carrier sensing εντοπίζει την παρουσία άλλων IEEE 802.11 WLAN χρηστών αναλύοντας όλα τα

πακέτα που εντοπίζει. Επίσης εντοπίζει την δραστηριότητα που υπάρχει σε ένα κανάλι μέσω της σχετικής ισχύος του σήματος από άλλες πηγές.

Ένας μηχανισμός virtual carrier- sense θα πρέπει να προσφέρεται από το MAC. Αυτός ο μηχανισμός αναφέρεται ως network allocation vector (NAV). Το NAV διατηρεί μια μελλοντική γνώση για την κίνηση στο μέσο επικοινωνίας με βάση τις πληροφορίες για τη διάρκεια της μετάδοσης, οι οποίες ανακοινώνονται στα RTS/CTS πακέτα πριν από την ανταλλαγή δεδομένων. Η διάρκεια είναι επίσης διαθέσιμη στις MAC κεφαλίδες των πακέτων κατά τη διάρκεια της contention period (CP). Το πεδίο duration/ID καθορίζει την χρονική περίοδο όπου το μέσο έχει οριστεί να μεταδίδει τα πακέτα δεδομένων καθώς και τα ACK πακέτα. Οι σταθμοί χρησιμοποιούν αυτή τη πληροφορία που υπάρχει στο πεδίο duration για να προσαρμόζουν το network allocation vector (NAV), το οποίο υποδεικνύει τον χρόνο που πρέπει να παρέλθει μέχρι η τρέχουσα μετάδοση να ολοκληρωθεί και το κανάλι να ξαναγίνει αδρανές. Το κανάλι ορίζεται ως απασχολημένο αν το physical ή ο virtual sensing mechanism υποδείξει ότι το κανάλι χρησιμοποιείται.

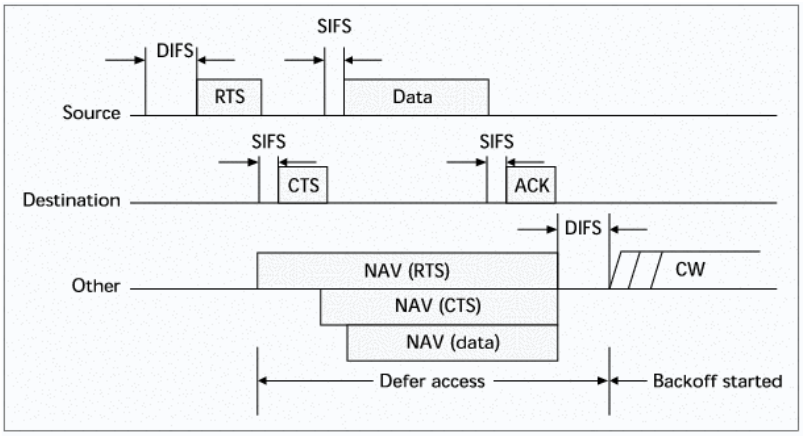
Η προτεραιότητα για την πρόσβαση στο ασύρματο μέσο ελέγχεται με την χρήση των interframe space (IFS) χρονικών διαστημάτων ανάμεσα στις μεταδόσεις των πακέτων. Τα IFS χρονικά διαστήματα είναι υποχρεωτικές περίοδοι που το μέσο επικοινωνίας βρίσκεται σε αδράνεια. Τρία είδη χρονικών διαστημάτων καθορίζονται στο πρωτόκολλο: τα short IFS (SIFS), τα point coordination function IFS (PIFS) και τα DCF- IFS (DIFS). Τα χρονικά διαστήματα SIFS είναι τα μικρότερα IFS, ακολουθούμενα από τα PIFS και τα DIFS, αντίστοιχα. Οι σταθμοί που απαιτείται να περιμένουν ένα SIFS έχουν προτεραιότητα στην πρόσβαση στο μέσο επικοινωνίας σε σχέση με τους σταθμούς που απαιτείται να περιμένουν ένα PIFS ή ένα DIFS πριν αρχίσουν να μεταδίδουν. Επομένως, οι σταθμοί που περιμένουν τα SIFS έχουν την υψηλότερη προτεραιότητα στην πρόσβαση στο μέσο επικοινωνίας. Για την βασική μέθοδο πρόσβασης, όταν ένας σταθμός εντοπίζει ότι το μέσο επικοινωνίας είναι αδρανές, τότε ο σταθμός περιμένει για μια DIFS περίοδο ελέγχοντας το κανάλι και αν αυτό παραμείνει αδρανές τότε ξεκινάει την μετάδοση,. Ο σταθμός- δέκτης υπολογίζει το checksum και αποφασίζει αν το πακέτο που παραλείφθηκε είναι σωστό. Αν το πακέτο που έλαβε ο σταθμός- δέκτης είναι σωστό, τότε ο σταθμός- δέκτης περιμένει ένα SIFS διάστημα μέχρι να μεταδώσει ένα ACK frame στον σταθμό που μετάδωσε το αρχικό πακέτο, υποδεικνύοντας την επιτυχημένη μετάδοση του πακέτου. Η παρακάτω εικόνα είναι ένα χρονικό διάγραμμά που απεικονίζει την επιτυχημένη μετάδοση ενός πακέτου. Όταν το πακέτο με τα δεδομένα μεταδίδεται, το duration πεδίο του πακέτου χρησιμοποιείται για να ενημερώσει όλους τους άλλους σταθμούς για ποσό χρονικό διάστημα το μέσο επικοινωνίας θα είναι απασχολημένο. Όλοι οι σταθμοί που “ακούν” το πακέτο προσαρμόζουν το NAV (network allocation vector) βασιζόμενοι στη τιμή που βρίσκεται duration πεδίο, η οποία εμπεριέχει την SIFS περίοδο και το ACK που ακολουθεί το πακέτο με τα δεδομένα.



Σχήμα 22"Transmission of an MPDU without RTS/CTS "

Από την στιγμή που ο σταθμός- πομπός δεν μπορεί να ακούσει τις δίκες του μεταδόσεις, όταν συμβαίνει μια σύγκρουση (μια σύγκρουση μπορεί να συμβεί αν δυο σταθμοί αρχίζουν να μεταδίδουν ταυτόχρονα), ο σταθμός- πομπός συνεχίζει να μεταδίδει. Αν το πακέτο έχει μεγάλο μέγεθος, ένα μεγάλο μέρος του bandwidth του καναλιού χρησιμοποιείται άσκοπα λόγο του κατεστραμμένου πακέτου. Τα RTS και CTS πακέτα μπορούν να χρησιμοποιηθούν από ένα σταθμό για να εξασφαλίσουν το bandwidth του καναλιού, πριν αρχίσει η μετάδοση των δεδομένων και να μειώσουν το χαμένο bandwidth του καναλιού όταν συμβαίνει μια σύγκρουση. Τα RTS και CTS πακέτα είναι σχετικά μικρά (το RTS έχει μέγεθος 20 bytes και το CTS 14 bytes) σε σχέση με το μέγιστο μέγεθος του πακέτου των δεδομένων (2346 bytes). Το RTS πακέτο μεταδίδεται πρώτο από τον σταθμό- πηγή με πακέτα δεδομένων να περιμένουν στην ουρά για μετάδοση σε ένα συγκεκριμένο σταθμό- προορισμό. Όλοι οι σταθμοί που ακούνε το RTS πακέτο, ελέγχουν το duration πεδίο και ρυθμίζουν κατάλληλα το NAV τους. Στη συνέχεια ο σταθμός- προορισμός απαντά στο RTS πακέτο με ένα CTS πακέτο μετά από μια SIFS χρονική περίοδο. Οι σταθμοί που ακούν το CTS πακέτο ελέγχουν το duration πεδίο και αναβαθμίζουν ξανά το NAV (η τιμή του καθορίζεται από το duration πεδίο του αμέσως προηγούμενου RTS πακέτου αφαιρώντας τον χρόνο που χρειάζεται για να μεταδώσει το CTS πακέτο και το SIFS χρονικό διάστημα). Μετά την επιτυχή λήψη του CTS, ο αποστολέας είναι σχεδόν εξασφαλισμένος ότι το μέσο είναι σταθερό για την επιτυχή μετάδοση των πακέτων. Να σημειωθεί ότι οι σταθμοί είναι ικανοί να αναβαθμίσουν το NAV τους με βάση το RTS πακέτο του αποστολέα και το CTS πακέτο του δεκτή, το οποίο βοηθάει στην καταπολέμηση του hidden node. Η παρακάτω εικόνα αποτυπώνει την μετάδοση ενός πακέτου δεδομένων με τη χρήση του RTS/CTS μηχανισμού. Οι σταθμοί μπορούν να επιλέξουν να μην χρησιμοποιούν το RTS/CTS ή να

χρησιμοποιούν το RTS/CTS , αυτό επιτυγχάνεται με την ρύθμιση της παραμέτρου RTS threshold και όταν το μέγεθος του πακέτου είναι μικρότερο από την τιμή του threshold τότε το RTS/CTS δεν χρησιμοποιείται. Αν συμβεί κάποια σύγκρουση με ένα RTS ή CTS πακέτο, το bandwidth που χρησιμοποιείται άσκοπα, είναι πολύ μικρότερο σε σχέση με μια σύγκρουση που συμβαίνει με ένα μεγάλο πακέτο δεδομένων. Ωστόσο, με τη χρήση του RTS/CTS μηχανισμού προστίθεται επιπλέον overhead.



Σχήμα 23"Transmission of an MPDU using RTS/CTS"

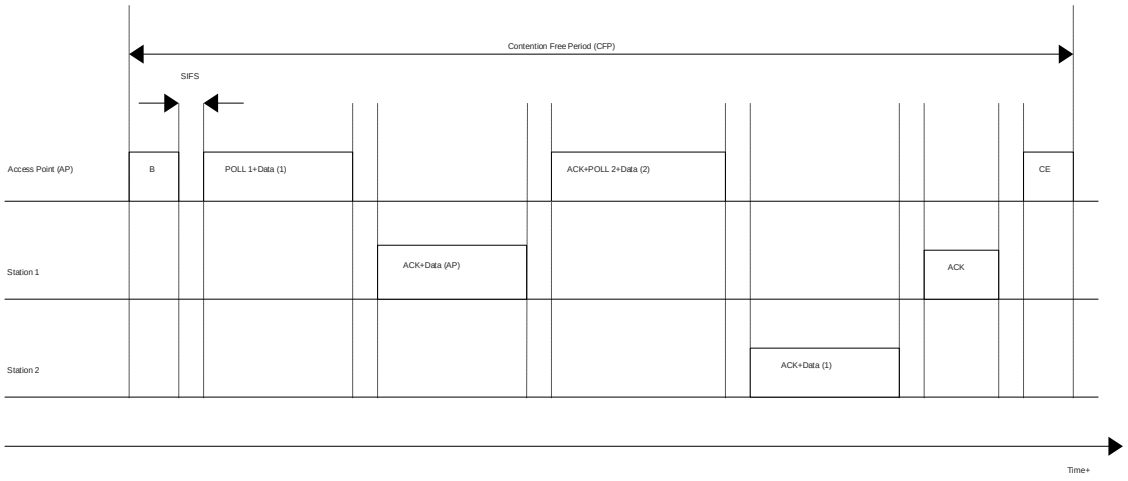
4.4 Point Coordination Function

Το PCF είναι μια προαιρετική λειτουργία συντονισμού του πρωτοκόλλου IEEE 802.11. Λειτουργεί μόνο σε δίκτυα με υποδομή (infrastructure- based networks). Ο χρόνος διαιρείται σε δύο περιόδους: την contention free periods (CFP), όπου το AP στέλνει μηνύματα στους σταθμούς για να τους δώσει την ευκαιρία να μεταδώσουν πακέτα και σε contention periods (CP), όπου το DCF εκτελείται. Από τη στιγμή που το PCF είναι μια προαιρετική λειτουργία συντονισμού, οι DCF περίοδοι είναι υποχρεωτικοί για να διασφαλιστεί η πρόσβαση στους DCF σταθμούς.

Ένα CFP δημιουργείται και διατηρείται από το AP, το οποίο περιοδικά μεταδίδει ένα beacon. Τα περιοδικά μεταδιδόμενα beacons εμπεριέχουν πληροφορίες που αφορούν τη διάρκεια του CFP αλλά και του CP και επιτρέπουν έναν νέο σταθμό να συσχετιστεί με το AP κατά τη διάρκεια ενός CFP. Το CFP ολοκληρώνεται όταν το AP μεταδίδει ένα CF End (CE) πακέτο.

Κατά τη διάρκεια του CFP, ο μόνος σταθμός που επιτρέπεται να μεταδίδει είναι αυτός που έχει εκλεγεί από το AP. Σε κάθε περίπτωση, η πρόσβαση στο μέσο επικοινωνίας δίνεται μετά από ένα SIFS αφού γίνει η παραλαβή είτε του πακέτου εκλογής είτε του πακέτου με τα δεδομένα. Αν ένας εκλεγμένος σταθμός δεν έχει δεδομένα προς μετάδοση, απαντάει με ένα NULL πακέτο.

Ένα παράδειγμα της λειτουργείας του PCF αποτυπώνεται στη παρακάτω εικόνα. Το AP δημιουργεί ένα CFP μεταδίδοντας ένα beacon. Υστέρα από ένα SIFS, το AP συνδυάζει ένα πακέτο εκλογής με δεδομένα και το μεταδίδει στο σταθμό 1. Όταν ληφθεί αυτό το συνδυαστικό πακέτο, ο σταθμός 1 επιβεβαιώνει την παραλαβή του πακέτου με τα δεδομένα και απαντά στην εκλογή μεταδίδοντας ένα πακέτο με δεδομένα στο AP. Στη συνέχεια, το AP επιβεβαιώνει την παραλαβή του πακέτου με τα δεδομένα από το σταθμό 1 και συνδυάζει ένα πακέτο εκλογής με δεδομένα για τον σταθμό 2. Όταν ληφθεί το πακέτο, ο σταθμός 2 επιβεβαιώνει την λήψη του στο AP και μεταδίδει δεδομένα στο σταθμό 1. Αφού λάβει το πακέτο ο σταθμός 1 επιβεβαιώνει την παραλαβή του πακέτου. Το CFP ολοκληρώνεται με τη μετάδοση ενός CE πακέτου. Η τεχνική του συνδυασμού των πακέτων που χρησιμοποιείται από το PCF επιτρέπει την αύξηση της αποδοτικότητας του πρωτοκόλλου ελαχιστοποιώντας το πλήθος των MAC και PHY κεφαλίδων που χρησιμοποιούνται.



Σχήμα 24"PCF Example of operation"

ΕΠΙΛΟΓΟΣ

Στο προηγούμενο κεφάλαιο μιλήσαμε για το MAC επίπεδο και πιο ειδικά για τις ομοιότητες και τις διαφορές που παρουσιάζει το 802.11 frame με το Ethernet frame, αναλύσαμε το πρόβλημα του κρυμμένου κόμβου και τέλος αναφερθήκαμε στις τεχνικές που χρησιμοποιούνται με σκοπό τη σωστή διαχείριση του μέσου επικοινωνίας από τους ασύρματους σταθμούς με σκοπό την αποφυγή των συγκρούσεων.

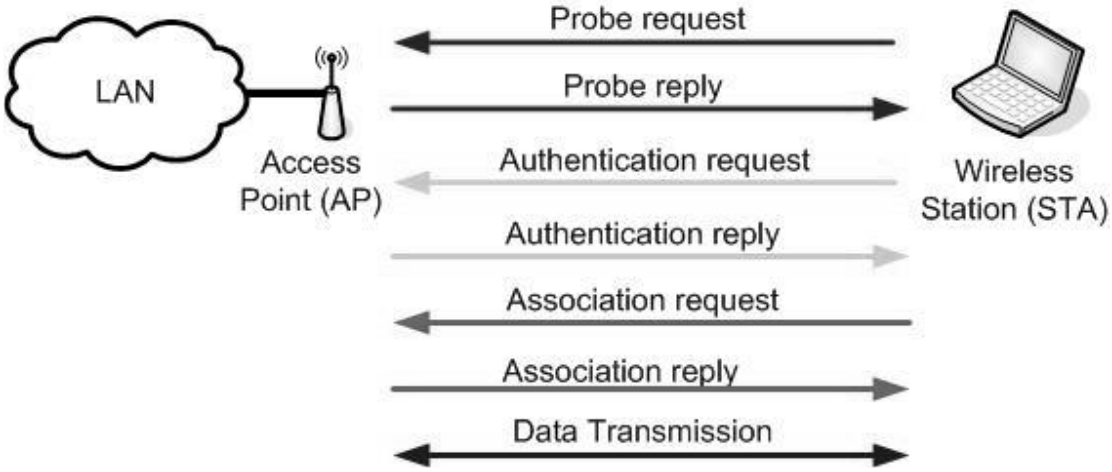
Στο επόμενο κεφάλαιο θα μιλήσουμε για τις μεθόδους που χρησιμοποιούνται με σκοπό την διασφάλιση της ασύρματης επικοινωνίας καθώς και τους πιθανούς κινδύνους που μπορούν να υπάρξουν σε μια ασύρματη επικοινωνία.

ΚΕΦΑΛΑΙΟ 5

WLAN Security

ΕΙΣΑΓΩΓΗ

Τα ασύρματα τοπικά δίκτυα έχουν καταφέρει να προσφέρουν μία ασύρματη δικτυακή πρόσβαση με έναν αποδεκτό ρυθμό μετάδοσης. Τα WLANs έχουν αναπτυχθεί ως μια επέκταση για τα ήδη υπάρχοντα ενσύρματα τοπικά δίκτυα. Λόγω του γεγονότος ότι τα WLANs είναι διαφορετικά σε σχέση με τα ενσύρματα δίκτυα, είναι σημαντικό να αναπτυχθεί η ασφάλεια για τα WLANs κοντά ή ακόμα και στο ίδιο επίπεδο που βρίσκονται τα LANs. Γενικά το IEEE 802.11 μπορεί να λειτουργεί σε δυο δικτυακές τοπολογίες, τις ad hoc αλλά και τις infrastructure. Οι ασύρματοι σταθμοί επικοινωνούν ασύρματα με το δικτυακό access point το οποίο είναι συνδεδεμένο στο ενσύρματο δίκτυο. Η εγκατάσταση της σύνδεσης ανάμεσα στον σταθμό και το access point περνάει από τρεις φάσεις: probing, authentication και association. Στην probing φάση, ο σταθμός μπορεί είτε να ακούει παθητικά τα σήματα του access point και να προσπαθεί αυτόματα τα συμμετάσχει στο access point ή μπορεί ενεργητικά να ζητήσει την συμμετοχή του στο access point. Στη συνέχεια στην φάση της authentication, ορίζεται η αυθεντικότητα του σταθμού από το access point χρησιμοποιώντας τους ανάλογους μηχανισμούς. Στη τρίτη και τελευταία φάση, ο σταθμός θα στείλει ένα association αίτημα στο access point και όταν αυτό εγκριθεί το access point θα προσθέσει τον σταθμό στο πίνακα των associated ασύρματων συσκευών. Κάθε access point μπορεί να έχει πολλούς associated σταθμούς αλλά κάθε σταθμός μπορεί να σχετίζεται με μόνο ένα access point κάθε φορά.



Σχήμα 25"The three phases undergone through WLAN for the establishment of connections between STAs and AP. These are probing, authentication and association"

Οι τρεις βασικές υπηρεσίες ασφάλειας που ορίζονται από την IEEE για τα WLANs είναι οι εξής:

- Authentication: κύριος στόχος της είναι η επαλήθευση των σταθμών που επικοινωνούν. Αυτό προσφέρει τον έλεγχο της πρόσβασης στο δίκτυο απορρίπτοντας την πρόσβαση στους σταθμούς που δεν μπορούν να αυθεντικοποιηθούν σωστά.
- Εμπιστευτικότητα: έχει αναπτυχθεί για να αποτρέπει την έκθεση της πληροφορίας στους επιτιθέμενους.
- Ακεραιότητα: αναπτύχθηκε για να διασφαλίσει ότι τα μηνύματα δεν έχουν μεταβληθεί κατά τη διάρκεια της μετάδοσης ανάμεσα σε δυο ασύρματους σταθμούς.

5.1 Bluetooth Security

Ο μηχανισμός της ασφάλειας ξεκινάει με τη διαδικασία της επιλογής από τον χρηστή του τρόπου με τον οποίο η συσκευή που χρησιμοποιεί το Bluetooth θα εφαρμόσει τις επιλογές της συνδεσιμότητας και του εντοπισμού. Οι διαφορετικοί συνδυασμοί των διαφορετικών δυνατοτήτων της συνδεσιμότητας και του εντοπισμού μπορούν να χωριστούν σε τρεις κατηγορίες ή αλλιώς σε επίπεδα ασφάλειας:

- Silent: Η συσκευή δεν θα δέχεται ποτέ καμία σύνδεση. Η συσκευή απλά θα εντοπίζει την κίνηση.

- Private: Η συσκευή δεν μπορεί να ανιχνευτεί. Θα δέχεται συνδέσεις μόνο από συσκευές των οποίων το αναγνωριστικό είναι γνωστό εκ τον προτέρων.
- Public: Η συσκευή μπορεί και να ανιχνευθεί αλλά και να συνδεθεί.

Υπάρχουν επίσης τρία διαφορετικές λειτουργείες ασφαλείας τις οποίες μια συσκευή μπορεί να χρησιμοποιήσει. Κάθε συσκευή μπορεί να χρησιμοποιεί μόνο μια λειτουργεία κάθε φορά:

- NonSecure: Οι Bluetooth συσκευές δεν χρησιμοποιούν καμία λειτουργία ασφαλείας.
- Security-level enforced security mode: Δυο Bluetooth συσκευές μπορούν να καθιερώσουν μια μη ασφαλή Asynchronous Connection- Less (ACL) σύνδεση. Οι διαδικασίες ασφαλείας, η authentication , η εξουσιοδότηση και η επιλεκτική κρυπτογράφηση ξεκινούν όταν ζητηθεί να δημιουργηθεί ένα L2CAP (Logical Link Control and Adaption Protocol) κανάλι.
- Link-level enforced security mode: Οι διαδικασίες ασφαλείας ξεκινούν όταν καθιερώνεται μια ACL σύνδεση.

Η ασφάλεια στην Bluetooth τεχνολογία καλύπτει τρεις σημαντικούς τομείς: την αυθεντικοποίηση, την εξουσιοδότηση και την κρυπτογραφία. Η αυθεντικοποίηση χρησιμοποιείται για να αποδεικνύεται η ταυτότητα του ενός μέλους της σύνδεσης στο άλλο. Τα αποτελέσματα της αυθεντικοποίησης χρησιμοποιούνται για να αποφασίζεται το επίπεδο εξουσιοδότησης του πελάτη. Η κρυπτογραφία χρησιμοποιείται για να κωδικοποιεί την πληροφορία η οποία ανταλλάσσεται ανάμεσα σε Bluetooth συσκευές. Η ασφάλεια του Bluetooth βασίζεται σε μια αλυσίδα από γεγονότα. Όλα τα γεγονότα θα πρέπει να συμβαίνουν με μια συγκεκριμένη σειρά για να υπάρχει επιτυχημένη ασφάλεια. Δυο Bluetooth συσκευές ξεκινούν την επικοινωνία με το ίδιο PIN (Personal Identification Number) κωδικό ο οποίος χρησιμοποιείται για την δημιουργία αρκετών 128-bit κλειδιών. Κάθε ζευγάρι master-slave μπορεί να έχει διαφορετικό PIN κωδικό για να παρέχει έμπιστες σχέσεις μεταξύ των συσκευών. Υπάρχουν τέσσερα βασικά κλειδιά που χρησιμοποιούνται στις διαδικασίες ασφαλείας του Bluetooth:

- Initialization Key
- Unit Key
- Combination Key
- Master Key

Initialization Key

Το επίπεδο ασφαλείας χρησιμοποιεί το initialization κλειδί με σκοπό να δημιουργήσει ένα ασφαλές κανάλι επικοινωνίας για να ανταλλάξει άλλα link-layer κλειδιά. Δημιουργεί το initialization κλειδί χρησιμοποιώντας έναν συνδυασμό του PIN κωδικού.

Unit Key

Δημιουργείται κατά τη διάρκεια της εγκατάστασης της συσκευής και αποθηκεύεται στη μη διαγραφομένη μνήμη.

Combination Key

Το Combination key δημιουργείται κατά τη διάρκεια της δημιουργία της σύνδεσης, εφόσον οι συσκευές έχουν αποφασίσει να χρησιμοποιήσουν αυτό το κλειδί. Δημιουργείται και από τις δυο συσκευές την ίδια στιγμή. Αρχικά, και οι δυο συσκευές δημιουργούν έναν τυχαίο αριθμό. Με έναν αλγόριθμο δημιουργίας κλειδιών και οι δυο συσκευές δημιουργούν ένα κλειδί συνδυάζοντας τον τυχαίο αριθμό και την Bluetooth διεύθυνση τους. Τέλος, οι συσκευές ανταλλάσσουν με ασφάλεια τους τυχαίους αριθμούς τους και υπολογίζουν το Combination Key για να χρησιμοποιείται στη μεταξύ τους επικοινωνία.

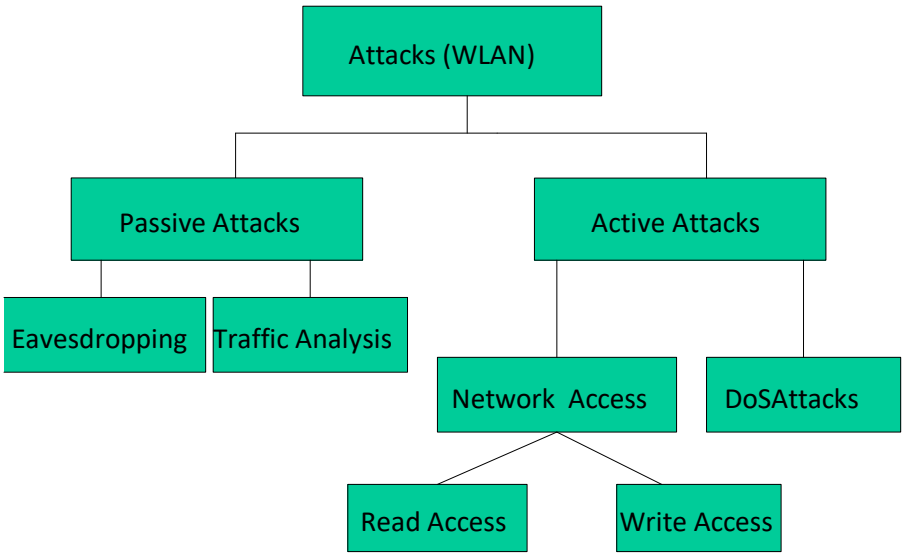
Master Key

Το Master Key είναι το μοναδικό προσωρινό κλειδί και δημιουργείται από την master συσκευή χρησιμοποιώντας έναν αλγόριθμο δημιουργίας κλειδιού και δυο 128-bit τυχαίους αριθμούς. Ο λόγος που χρησιμοποιείται ο αλγόριθμος είναι για να διασφαλιστεί ότι θα υπάρξει τυχαίος αριθμός. Ένας τρίτος τυχαίος αριθμός μεταδίδεται στον slave και μαζί με τον αλγόριθμο και με τρέχων κλειδί υπολογίζεται ένα συμπέρασμα και από τον master και από τον slave.

5.2 WLAN Security Attacks

Οι επιθέσεις στα ασύρματα τοπικά δίκτυα στοχεύουν στην εμπιστοσύνη και στην ακεραιότητα της πληροφορίας και στην διαθεσιμότητα του δικτύου. Οι επιθέσεις αυτές χωρίζονται σε δυο κατηγορίες τις passive attacks και τις active attacks.

- Οι passive attacks έχουν ως σκοπό την μη εξουσιοδοτημένη πρόσβαση στο δίκτυο για την υποκλοπή ή την ανάλυση της κίνησης, αλλά δεν στοχεύουν στην μετατροπή του περιεχομένου. Αυτές οι επιθέσεις είναι δύσκολο να εντοπιστούν επειδή δεν μεταβάλλεται το περιεχόμενο της επικοινωνίας. Για αυτό πρέπει να δίνετε έμφαση στην κωδικοποίηση της πληροφορίας και όχι στον εντοπισμό των επιθέσεων.
- Οι active attacks έχουν ως σκοπό την μη εξουσιοδοτημένη πρόσβαση στο δίκτυο με στόχο είτε να μεταβάλουν τα μηνύματα, τα δεδομένα, τα αρχεία είτε να διαταράξουν την λειτουργεία του δικτύου.



Σχήμα 26“General Taxonomy of WLAN security attacks"

5.2.1 Passive Attacks

Στις passive attacks υπάρχουν δυο φάσεις. Η πρώτη φάση αναφέρεται σαν μια φάση αναγνώρισης. Κατά τη διάρκεια της φάσης αναγνώρισης, ο στόχος του επιτιθέμενου είναι να ανακαλύψει ένα δίκτυο- στόχο και στη συνέχεια να συλλέξει πληροφορίες για αυτό το δίκτυο. Ο επιτιθέμενος ενεργεί με τέτοιο τρόπο ώστε να μην τον παρατηρήσει κάνεις. Ωστόσο, κάποια μέσα για την αναγνώριση του δικτύου μπορούν να εντοπιστούν από τα συστήματα ασφάλειας.

Υπάρχουν δυο μέθοδοι που χρησιμοποιούνται με σκοπό την μη ανιχνεύσιμη passive attack:

- Υποκλοπή: είναι η ικανότητα της καταγραφής των μεταδόσεων για το περιεχόμενο των μηνυμάτων. Ο επιτιθέμενος ακούει και ανακόπτει το ασύρματο σήμα ανάμεσα στο access point και τον ασύρματο σταθμό.
- Ανάλυση της κίνησης: είναι η ικανότητα να αποκτήσει περισσότερη γνώση με την παρακολούθηση της μετάδοσης για τα πρότυπα της επικοινωνίας ή για τα πακέτα που μεταδίδονται. Αυτό μπορεί να πραγματοποιηθεί ακόμα και όταν τα μηνύματα είναι κρυπτογραφημένα και δεν μπορούν να αποκρυπτογραφηθούν.

Υπάρχουν πολλά εργαλεία για υποκλοπή που μπορούν να βοηθήσουν τον επιτιθέμενο να επιτύχει τον σκοπό του. Τα εργαλεία υποκλοπής είναι τα πιο αποτελεσματικά μέσα για την παρατήρηση του δικτύου. Η μη ανιχνεύσιμη υποκλοπή μπορεί να πραγματοποιήσει δυο βασικές λειτουργείες: την συλλογή πακέτων και την ανάλυση, και την εμφάνιση των πακέτων. Αναλύοντας ένα πακέτο, ένας επιτιθέμενος πληροφορείται για τις ικανότητες ενός δικτύου και μπορεί να συλλέξει όλα τα είδη των εμπιστευτικών πληροφοριών με σκοπό την εκμετάλλευση ενός οργανισμού. Η συλλογή πακέτων δίνει την δυνατότητα στον επιτιθέμενο να ανάκτηση τα WEP κλειδιά σε λίγα μόλις λεπτά, ως εκ τούτου του παρέχεται η δυνατότητα να διαβάσει όλα δεδομένα που μεταδίδονται ανάμεσα στο access point και τον ασύρματο σταθμό.

5.2.2 Active Attacks

Η active attack είναι μια επίθεση με τη οποία γίνεται μια προσπάθεια να πραγματοποιηθεί μια μη εξουσιοδοτημένη αλλαγή στο σύστημα. Αυτό μπορεί να συμπεριλάβει για παράδειγμα, την μεταβολή των μεταδιδόμενων ή αποθηκευμένων δεδομένων, την δημιουργία νέων δεδομένων ή τη μείωση της διαθεσιμότητας του δικτύου ενός οργανισμού.

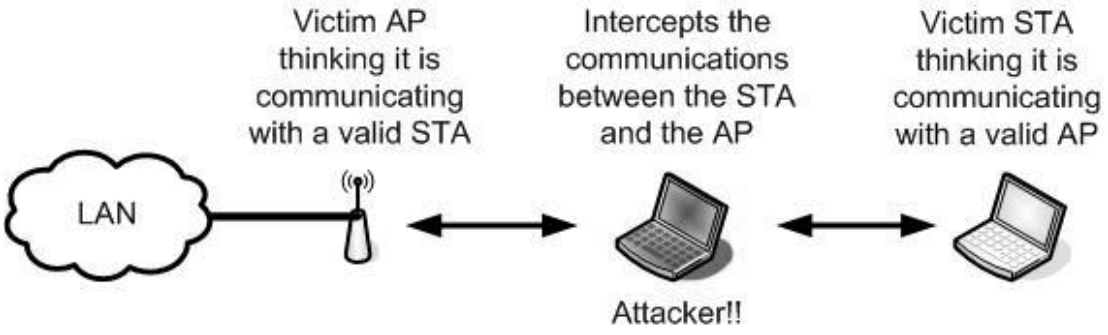
Πλαστοπροσωπία

Μια active attack είναι αυτή στην οποία ο επιτιθέμενος πλαστοπροσωπεί έναν εξουσιοδοτημένο χρήστη και με αυτόν τον τρόπο αποκτά μη εξουσιοδοτημένα δικαιώματα. Αυτή η επίθεση μπορεί να επιτύχει με την χρήση κλεμμένων logon IDs και κωδικών, με την εύρεση κενών ασφάλειας στα προγράμματα ή παρακάμπτοντας τον μηχανισμό γνησιότητας. Η προσπάθεια αυτή μπορεί να πραγματοποιηθεί από έναν εσωτερικό χρήστη, έναν υπάλληλο για παράδειγμα, ή από έναν ξένο χρήστη μέσω του δημοσίου δικτύου. Μόλις επιτύχει η είσοδος και μόλις αποκτηθούν τα σημαντικά δεδομένα ενός οργανισμού, ο επιτιθέμενος είναι ικανός να μεταβάλει και

να διαγράψει λογισμικό και δεδομένα, όπως επίσης να πραγματοποιήσει αλλαγές στις ρυθμίσεις του δικτύου και στις πληροφορίες δρομολόγησης.

MAN-IN-THE-MIDDLE ATTACK

Αυτή είναι μια διάσημη επίθεση και για τα ενσύρματα αλλά και για τα ασύρματα δίκτυα. Ένας παράνομος σταθμός ανακόπτει την επικοινωνία ανάμεσα σε έναν νόμιμο σταθμό και το access point. Ο παράνομος σταθμός εξαπατάει το access point και παριστάνει τον νόμιμο σταθμό και την ίδια στιγμή εξαπατάει και τον νόμιμο σταθμό παριστάνοντας το access point.



Σχήμα 27"Representation of the famous Man- in- the- middle attack for both wired and wireless network"

ΠΑΡΑΠΟΙΗΣΗ ΜΗΝΥΜΑΤΟΣ

Ο επιτιθέμενος μεταβάλει ένα νόμιμο μήνυμα είτε διαγράφοντας το μήνυμα είτε προσθέτοντας σε αυτό δεδομένα είτε καταγράφοντας το.

DENIAL-OF-SERVICES

Οι ασύρματες DoS επιθέσεις μπορεί να είναι αποτέλεσμα:

- Εσφαλμένης ρύθμισης των συσκευών- Λάθη στις ρυθμίσεις μπορούν να απενεργοποιήσουν το WLAN
- Ενός κακόβουλου χρήστη που μπορεί επίτηδες να παρεμβαίνει στην ασύρματη επικοινωνία- Ο σκοπός του είναι να απενεργοποιήσει ολόκληρο το ασύρματο δίκτυο ή σε ένα σημείο όπου οι μη νόμιμες συσκευές μπορούν να έχουν πρόσβαση στο δίκτυο.
- Τυχαία παρεμβολή- Τα WLANs λειτουργούν σε ελεύθερες συχνότητες, άρα, όλα τα ασύρματα δίκτυα, ανεξάρτητα των λειτουργειών ασφάλειας είναι

επιρρεπή στην αλλοίωση του σήματος τους από άλλες ασύρματες συσκευές (φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα).

Ο επιτιθέμενος αποτρέπει ή απαγορεύει την φυσιολογική χρήση ή τη διαχείριση των λειτουργιών της επικοινωνίας. Τα αποτελέσματα των DoS επιθέσεων μπορεί να κυμαίνονται από φυσική καταστροφή του εξοπλισμού, την καταστροφή μιας συγκεκριμένης δικτυακής λειτουργείας από ένα άτομο ή από ένα σύστημα, εκ τούτου αποτρέπει την νόμιμη δικτυακή κίνηση.

Για να επιτύχει μια active attack,ο επιτιθέμενος θα πρέπει να έχει πρόσβαση στο στοχευμένο δίκτυο με δικαιώματα διαβάσματος και γραψίματος. Ο τελικός στόχος είναι να έχει πρόσβαση στους πόρους του δικτύου ή να αποσπάσει και να αποκρυπτογραφήσει τα δεδομένα, εφόσον αυτά έχουν κρυπτογραφηθεί. Το δικαίωμα διαβάσματος επιτρέπει στον επιτιθέμενο να ανακόπτει και να διαβάζει την κίνηση από ένα δίκτυο, ως εκ τούτου του δίνει την μελλοντική δυνατότητα να πραγματοποιήσει επιθέσεις στις μεθόδους κρυπτογραφίας και αυθεντικοποίησης. Έχοντας ανακαλύψει ένα δίκτυο- στόχο μέσω της αναγνωριστικής φάσης της επίθεσης και έχοντας αποσπάσει και κρυπτογραφημένη αλλά και αποκρυπτογραφημένη κίνηση, ο επιτιθέμενος έχει τη δυνατότητα να αποκτήσει τα βασικά υλικά αλλά και τα ίδια τα κλειδιά κρυπτογράφησης. Η απόκτηση των κλειδιών αποκρυπτογράφησης δίνει την δυνατότητα στον επιτιθέμενο να έχει πλήρη πρόσβαση στο δίκτυο- στόχο και με το δικαίωμα γραφής έχει την δυνατότητα να στέλνει δεδομένα. Τα ακόλουθα είναι μερικοί από τους στόχους που έχει ένας επιτιθέμενος:

- Να ανακτήσει τα κλειδιά κρυπτογράφησης
- Να προσθέσει πακέτα δεδομένων στη κίνηση
- Να εγκαταστήσει λογισμικό παρακολούθησης
- Να ρυθμίσει ένα παράνομο access point και να ελέγχει τις παραμέτρους του δικτύου.

Για να μειωθεί ο κίνδυνος μιας DoS επίθεσης λόγω μη σωστής ρύθμισης των συσκευών και κακόβουλων προγραμμάτων, θα πρέπει να παραμένουν ασφαλείς οι κωδικοί και να δημιουργούνται backups.

5.3 Βασική Ασφάλεια για το 802.11

SSID

Ο Service Set Identifier είναι ένας μηχανισμός ο οποίος μπορεί να χωρίσει το ασύρματο δίκτυο σε πολλά δίκτυα που εξυπηρετούνται από πολλά access points. Κάθε access point είναι προγραμματισμένο με ένα SSID το οποίο αντιστοιχεί σε ένα συγκεκριμένο κομμάτι του ασύρματου δικτύου. Αυτή η διαμόρφωση είναι παρόμοια

με την ιδέα του subnetting που χρησιμοποιείται στα ενσύρματα δίκτυα. Για να είναι ικανός ένας σταθμός να έχει πρόσβαση σε ένα συγκεκριμένο ασύρματο δίκτυο θα πρέπει να έχει ρυθμιστεί με το κατάλληλο SSID. Ένα WLAN μπορεί να χωριστεί σε πολλά WLAN με βάση τον όροφο ή το τμήμα στο οποίο λειτουργεί. Ένας σταθμός μπορεί να ρυθμιστεί με πολλά SSID για τους χρήστες που απαιτούν πρόσβαση στο δίκτυο από πολλά διαφορετικά σημεία.

Ένας σταθμός θα πρέπει να παρουσιάσει το σωστό SSID για να έχει πρόσβαση στο access point. Το SSID λειτουργεί σαν κωδικός και σαν ένα μέτρο ασφαλείας. Η ελάχιστη ασφάλεια μπορεί να εκτεθεί αν το access point έχει ρυθμιστεί να μεταδίδει το SSID broadcast. Αν η λειτουργεία broadcast είναι ενεργοποιημένη, κάθε σταθμός που δεν έχει ρυθμιστεί με SSID θα λάβει το SSID και στη συνέχεια θα είναι ικανός να έχει πρόσβαση στο access point. Πιο συχνά, οι χρήστες ρυθμίζουν τα δικά τους συστήματα με τα κατάλληλα SSIDs. Ως αποτέλεσμα αυτά τα SSID είναι ευρέως γνωστά και μπορούν να μοιράζονται εύκολα. Επιπλέον, ένα access point μπορεί να ρυθμιστεί χωρίς SSID και να επιτρέπει μια ανοιχτή πρόσβαση σε κάθε ασύρματη συσκευή να σχετίζεται με το access point.

MAC ADDRESS FILTERING

Ένας σταθμός μπορεί να αναγνωριστεί από την μοναδική MAC διεύθυνση της κάρτας δικτύου του. Για να ενισχυθεί ο έλεγχος του access point κάθε access point μπορεί να προγραμματιστεί με μια λίστα από MAC διευθύνσεις που σχετίζονται με τους ασύρματους σταθμούς που επιτρέπονται να έχουν πρόσβαση στο access point. Αν η MAC διεύθυνση του σταθμού δεν εμπεριέχεται στη λίστα, τότε ο σταθμός δεν επιτρέπεται να έχει πρόσβαση στο access point, ακόμα και αν το SSID που παρουσιάζει ταιριάζει με το SSID του access point.

Αυτός ο μηχανισμός προσφέρει βελτιωμένη ασφάλεια η οποία ταιριάζει περισσότερο σε μικρά δίκτυα, όπου η λίστα με τις MAC διευθύνσεις μπορεί να διαχειριστεί αποτελεσματικά. Η διαχείριση απαιτεί από κάθε access point να είναι προγραμματισμένο χειροκίνητα με μια λίστα από MAC διευθύνσεις. Επιπλέον, αυτή λίστα θα πρέπει να μένει ενημερωμένη. Αυτός ο επιπλέον φόρτος μπορεί να έχει ως αποτέλεσμα την μείωση του WLAN στο πλήθος των access point και των σταθμών.

5.4 WEP (legacy)

Το Wired Equivalent Privacy (WEP) είναι ένα πρωτόκολλο ασφαλείας το οποίο είναι μέρος του προτύπου IEEE 802.11 για τα ασύρματα δίκτυα. Το WEP χρησιμοποιείται ακόμα ευρέως στον κόσμο λόγω του γεγονότος, ότι οι παλαιότερες κάρτες δικτύου

δεν μπορούν να ταιριάξουν με τις απαιτήσεις των νέων πρωτοκόλλων ασφαλείας. Το WEP χρησιμοποιεί ένα κοινόχρηστο κλειδί για κρυπτογράφηση και για την επαλήθευση της αυθεντικότητας του χρήστη. Το WEP δημιουργήθηκε για να προστατεύσει τα δεδομένα κατά τη διάρκεια της ασύρματης μετάδοσης και έχει τρεις κύριους στόχους ασφαλείας:

- Εμπιστευτικότητα
- Πρόσβαση στο μέσο επικοινωνίας
- Ακεραιότητα δεδομένων

Το WEP χρησιμοποιεί ένα 40- bit κλειδί, το οποίο είναι πολύ μικρό και αυτό έχει ως συνέπεια οι brute force επιθέσεις, δηλαδή οι επιθέσεις στις οποίες δοκιμάζονται όλοι οι πιθανοί συνδυασμοί μέχρι να βρεθεί ο σωστός, να είναι πολύ αποτελεσματικές. Άρα, καθένας που έχει τις βασικές γνώσεις υπολογιστή μπορεί να σπάσει το κλειδί. Η προστασία της ασύρματης δικτυακής υποδομής υλοποιείται μέσω του προτύπου IEEE 802.11 το οποίο συμπεριλαμβάνει ένα προαιρετικό χαρακτηριστικό το οποίο απορρίπτει όλα τα πακέτα τα οποία δεν έχουν κρυπτογραφηθεί σωστά χρησιμοποιώντας το WEP. Η προστασία από την παραποίηση των μεταδιδόμενων μηνυμάτων επιτυγχάνεται με την χρήση του πεδίου checksum (CRC32), το οποίο υποδεικνύει αν τα δεδομένα έχουν μεταβληθεί ή όχι. Το CRC32 εμπεριέχεται στο σώμα του πακέτου του μηνύματος και κρυπτογραφείται με αυτό.

Το WEP έχει δυο αδυναμίες, πρώτον, το WEP είναι προαιρετικό στα προγράμματα εγκατάστασης έχοντας ως αποτέλεσμα στις περισσότερες περιπτώσεις το WEP να μην είναι ενεργοποιημένο μετά την εγκατάσταση και δεύτερον, η απουσία βασικών πρωτοκόλλων διαχείρισης στο WEP ώθησε τους χρήστες να βασίζονται σε ένα μοναδικό κοινόχρηστο κλειδί. Αν το κλειδί εκτεθεί, τότε η ασφάλεια του ασυρμάτου δικτύου μπορεί να διακυβεύεται.

5.5 WPA

Το Wi-Fi Protected Access (WPA), διάδοχος του WEP, είναι ένα πρωτόκολλο ασφαλείας το οποίο συμπεριλαμβάνει πολλά από τα πρότυπα της οικογένειας IEEE 802.11i. Το WPA δημιουργήθηκε ως μια προσωρινή λύση για την αντικατάσταση του WEP πριν το IEEE 802.11i ολοκληρωθεί. Το WPA βελτίωσε αρκετά την διαδικασία της κρυπτογράφησης που είχε το WEP και πρόσθεσε πολύ ασφαλές μηχανισμό αυθεντικοποίησης του χρήστη. Στο WPA οι χρήστες μπορούν να αυθεντικοποίηθουν είτε μέσω ενός IEEE 802.11X server αυθεντικοποίησης είτε μέσω ενός access point με μια συνθηματική φράση. Το WPA επίσης προσφέρει

αναβαθμίσεις του λογισμικού για να επιτευχθεί η διαλειτουργηκότητα με παλαιότερες κάρτες δικτύου και access point.

Το WPA παρουσιάζει ένα νέο πρωτόκολλο ασφαλείας, το Temporal Key Integrity Protocol (TKIP), το οποίο δυναμικά αλλάζει τα κλειδιά κατά της διάρκεια επικοινωνίας, ως αποτέλεσμα η επανάληψή των ίδιων κλειδιών αποτρέπεται.

Το TKIP επίσης ενισχύει την ακεραιότητα των πακέτων προσθέτοντας ένα Message Integration Check (MIC) πεδίο για να προστατεύεται από τις επιθέσεις. Η τιμή του MIC πεδίου υπολογίζεται με έναν κρυπτογραφικό αλγόριθμο, ο οποίος χρησιμοποιεί ένα κλειδί 64-bit και διαιρεί τα πακέτα σε block των 32-bit.

Όπως αναφέρθηκε και πριν, υπάρχουν δυο επιλογές για την αυθεντικοποίηση του χρήστη στο WPA. Η πρώτη επιλογή, ο server αυθεντικοποίησης, ονομάζεται WPA-Enterprise. Το WPA-Enterprise χρησιμοποιεί το Extensible Authentication Protocol (EAP) μαζί με μια αμοιβαία αυθεντικοποίηση έτσι ώστε ο ασύρματος χρήστης να μην συμμετέχει κατά λάθος σε κάποιο ξένο δίκτυο. Ο server αυθεντικοποίησης λειτουργεί με την παρακάτω διαδικασία:

1. Ο server αυθεντικοποίησης δέχεται τα διαπιστευτήρια του χρήστη.
2. Ο server αυθεντικοποίησης χρησιμοποιεί την 802.11X δομή και το EAP για να δημιουργήσει ένα μοναδικό master κλειδί
3. Το 802.11X διανέμει το master κλειδί στα AP και στους ασύρματους σταθμούς
4. Το TKIP θέτει ένα ιεραρχικό και διαχειριστικό σύστημα χρησιμοποιώντας το master κλειδί, δηλαδή δημιουργεί μοναδικά κλειδιά κρυπτογράφησης των πακέτων δεδομένων με τη βοήθεια του master κλειδιού.

Η δεύτερη επιλογή ονομάζεται WPA-Personal,το οποίο έχει σχεδιαστεί για το σπίτι και για μικρά επαγγελματικά δίκτυα, τα οποία δεν μπορούν να αντέξουν την πολυτέλεια του server αυθεντικοποίησης. Στο WPA-Personal οι χρήστες αυθεντικοποιούνται στο Access Point με ένα συνθηματικό. Το συνθηματικό μπορεί να αποθηκευτεί και να χρησιμοποιηθεί αυτόματα στα περισσότερα λειτουργικά συστήματα.Το σπάσιμο του συνθηματικού μπορεί να αποφευχθεί με τη χρήση τουλάχιστον δεκατεσσάρων ,αλλά ιδανικά προτείνετε η χρήση 22 τυχαίων χαρακτήρων ως συνθηματικό.

5.6 WPA2

Το WPA2 που είναι βασισμένο πάνω στο IEEE 802.11i πρότυπο προσφέρει έναν νέο αλγόριθμο CCMP που βασίζεται στον AES (Advanced Encryption Standard). Το WPA2 χρησιμοποιεί ένα AES κλειδί για να προστατεύσει την εμπιστευτικότητα και την ακεραιότητα του μηνύματος. Στο WPA2, ο AES υποστηρίζει το Independent Basic Service Set (IBSS), το οποίο ενεργοποιεί την ασφάλεια ανάμεσα στους ασύρματους σταθμούς που λειτουργούν σε add-hoc δίκτυα. Το WPA2 επίσης προσφέρει διαλειτουργικότητα ανάμεσα σε WPA και WPA2 ασύρματους σταθμούς, η οποία επιτρέπει την ομαλή μεταβολή από το WPA σε WPA2 χωρίς να τεθεί σε κίνδυνο η ασφάλεια του δικτύου. Άλλες νέες λειτουργείες του WPA2 είναι η μείωση του overhead στην διαδικασία δημιουργίας του κλειδιού κατά τη ανταλλαγή που γίνεται στη διάρκεια της αυθεντικοποίησης.

Αν και τα WPA και WPA2 είναι δυνατά σχήματα ασφαλείας, οι επιθέσεις εναντίων αυτών έχουν ήδη υλοποιηθεί. Αυτές οι επιθέσεις βασίζονται στη τάση των χρηστών να διαλέγουν αδύναμους κωδικούς οι οποίο παραβιάζονται εύκολα. Η πηγή αυτή του προβλήματος βρίσκεται στην έλλειψη χρηστικότητας. Για αυτό, όταν δημιουργείται ένα ασύρματο δίκτυο, οι χρήστες θα πρέπει να εισάγουν χειροκίνητα τα κλειδιά, κάτι το οποίο καταναλώνει χρόνο και μπορεί να είναι δύσκολο για τους αρχάριους.

Πίνακας 8"Comparison of WEP, WPA and WPA2"

	WEP	WPA	WPA2
Encryption cip.	RC4	TKIP	AES
Key sizes	40/104 bit	128 bit	128 bit
IV size	24 bit	48 bit	48 bit
Per-packet key	Key + IV	TKIP mix.fc.	CCMP
Data integrity	CRC-32	MIC	CCMP
Replay detection	None	IV seq.	IV seq.
Key mng.	None	802.1X	802.1X
Security	Weak	Strong	Stronger

5.7 Μέθοδοι Κρυπτογράφησης

Η κρυπτογράφηση χρησιμοποιείται για να προστατέψει τα δεδομένα. Αν ένας επιτιθέμενος έχει αποσπάσει κρυπτογραφημένα δεδομένα, δεν θα μπορεί να τα αποκρυπτογραφήσει μέσα σε ένα λογικό χρονικό περιθώριο. Τα σημαντικότερα πρωτόκολλα κρυπτογράφησης είναι:

- Temporal Key Integrity Protocol (TKIP): Το TKIP είναι το πρωτόκολλο που χρησιμοποιείται από το WPA. Υποστηρίζει παλαιότερες WLAN συσκευές αντιμετωπίζοντας τις αρχικές ατέλειες που σχετίζονται με τη 802.11 WEP μέθοδο κρυπτογράφησης. Το WPA κάνει χρήση του WEP, αλλά κρυπτογραφεί τα δεδομένα χρησιμοποιώντας το TKIP και πραγματοποιεί έναν έλεγχο της ακεραιότητας του μηνύματος (Message Integrity Check-MIC) στα κρυπτογραφημένα πακέτα για να διασφαλίσει ότι το μήνυμα δεν έχει αλλοιωθεί κατά τη μετάδοση.
- Advanced Encryption Standard (AES): Το AES είναι μια μέθοδος κρυπτογράφησης που χρησιμοποιείται από το WPA2. Το AES πραγματοποιεί τις ιδίες λειτουργίες με το TKIP, αλλά είναι κατά πολύ ισχυρότερη μέθοδος κρυπτογράφησης. Χρησιμοποιεί το Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) που επιτρέπει στον σταθμό- προορισμό να μπορεί να αναγνωρίσει αν τα κρυπτογραφημένα ή μη- κρυπτογραφημένα bits έχουν μεταβληθεί.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό αναφερθήκαμε στα προβλήματα ασφαλείας που παρουσιάζουν οι ασύρματες επικοινωνίες, καθώς στα WLAN μπορεί ο καθένας που βρίσκεται εντός της εμβέλειας ενός access point να ακούσει την επικοινωνία. Επίσης έγινε αναφορά και στους τρόπους καταπολέμησης αλλά και πρόληψης κάθε απειλής της ασύρματης επικοινωνίας.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως είναι εμφανές, τα WLANs δίκτυα βρίσκονται παντού σήμερα και χρησιμοποιούνται καθημερινά από τους ανθρώπους με κύριο σκοπό την επικοινωνία. Τα WLANs προσφέρουν τη ικανότητα της μετακίνησης του χρήστη εντός του ορίου της εμβέλειας της μετάδοσης που προσφέρεται και αυτό είναι το κύριο πλεονέκτημα του σε σχέση με τα LANs.

Για να επιτευχθεί η επικοινωνία των χρηστών μέσο των WLANs έχουν αναπτυχθεί και συνεχίζονται να αναπτύσσονται τα ασύρματα πρωτόκολλα επικοινωνίας, με πιο σημαντικά εκείνα της οικογένειας της IEEE 802.11. Τα ασύρματα πρωτόκολλα επικοινωνίας σχεδιάζονται με τέτοιο τρόπο έτσι ώστε να βελτιωθεί η ποιότητα της επικοινωνίας των χρηστών, με βάση το ρυθμό μετάδοσης που προσφέρουν και το εύρος της επικοινωνίας ανάλογα με το αρχικό σενάριο με βάση το οποίο δημιουργήθηκαν.

Για να επιτευχθούν οι παραπάνω στόχοι τα ασύρματα πρωτόκολλα επικοινωνίας χρησιμοποιούν πολλούς διαφορετικούς μηχανισμούς μετάδοσης του σήματος στο φυσικό επίπεδο και επίσης αρκετές διαφορετικές τεχνικές στο MAC επίπεδο.

Θα πρέπει να τονιστεί και η ανάγκη να αυξηθούν τα μέτρα ασφαλείας και πρόληψης για τις ασύρματες επικοινωνίες, το σήμα των οποίων διαδίδεται στον αέρα ο οποίος είναι ένα κοινό μέσο επικοινωνίας και έτσι αυτές τις μεταδόσεις μπορούν ευκολά να τις λαμβάνουν και κακόβουλοι χρήστες. Για αυτό το λόγο έχουν αναπτυχθεί συγκεκριμένοι μέθοδοι ασφαλείας (κρυπτογράφηση, mac filtering, SSID) για τις ασύρματες επικοινωνίες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Vassis D., Kormentzas G., Rouskas A. and Maglogiannis I. (2005), The IEEE 802.11g Standard for High Data Rate WLANs, Published in: IEEE Network Magazine

Al Shourbaji I. (2013), An Overview of Wireless Local Area Networks (WLAN), Jizan University, Jizan, Saudi Arabia

Bejarano O. and Knightly E. (2013), IEEE 802.11ac: From Channelization to Multi-User MIMO, Published in: IEEE Communications Magazine

Bellalta B. (2016), IEEE 802.11ax: High-Efficiency WLANs, Published in: IEEE Wireless Communications Magazine

Bisdikian C. (2001), An Overview of the Bluetooth Wireless Technology, Published in: IEEE Communications Magazine

Boncella R. (2002), Wireless security: an overview, Washburn University, Kansas, USA

Brida P. and Machaj J. (2015), IEEE 802.11a as a Part of Seamless Positioning, Presented in: International Conference on Indoor Positioning and Indoor Navigation (IPIN)

Camponovo G., Cerutti D. (2005), WLAN Communities and Internet Access Sharing: a Regulatory Overview, Published in: International Conference on Mobile Business

Davies A. (2002), An overview of Bluetooth Wireless Technology™ and some competing LAN Standards, School of Computing and Information Systems, Surrey, England

Gast M. (2002), 802.11 Wireless Networks: The Definitive Guide, pp. 170-193

Hassinen T. (2006), Overview of WLAN security, Presented in: Seminar on Network Security

Heusse M., Rousseau F., Berger- Sabbatel G. and Duda A. (2003), Performance Anomaly of 802.11b, Published in: IEEE INFOCOM

Hongfeng Wang (2001), Overview of Bluetooth Technology, Penn state, Pennsylvania, USA

Kurose J. and Ross K. (2013), Computer Networking A top-Down Approach, Vol 6, pp 531- 533

Lansford J., Bahl P. (2000), The Design and Implementation of HomeRF: A Radio Frequency Wireless Networking Standard for the Connected Home, Published in: Proceedings of the IEEE magazine

Naamany A., Shidhani A. and Bourdoucen H. (2006), IEEE 802.11 Wireless LAN Security Overview, Published in: IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No.5B

Radimirsch M., Vollmer V. (1999), HIPERLAN Type 2 Standardization - An Overview, Robert Bosch GmbH, Hildesheim, Germany

Shrivastava V., Rayanchu S., Yoon J. and Banerjee S. (2008), 802.11n Under the Microscope, Presented in: Internet Measurement Conference (IMC)

Wendell O. (2016), CCNA Routing and Switching 200-125 Official Cert Guide Library, Vol 1