ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ

ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΟΥ ΦΟΙΤΗΤΗ ΣΙΑΝΚΟ ΙΝΤΡΙΤ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ Κ.ΛΙΟΔΑΚΗΣ ΓΕΩΡΓΙΟΣ

<u>ΤΙΤΛΟΣ:</u> Αξιολόγηση απόδοσης ενός Wi-Fi δικτύου μέσω λήψης μετρήσεων.

ΧΑΝΙΑ, Ιανουάριος 2013

ΠΡΟΛΟΓΟΣ

Μετά από περίπου πέντε χρόνια στο ΤΕΙ ηλεκτρονικής Χανίων τα ασύρματα δίκτυα ήταν ένα κεφάλαιο που βοήθησε στην περεταίρω ανάπτυξη μου στα ηλεκτρονικά. Σήμερα ασχολούμαι ακόμα με την επίτευξη διαμοιρασμού και άρτιας λειτουργίας των ασύρματων δικτύων στη περιοχή μου(Σαντορίνη) καθώς η τουριστική ανάπτυξη της φέρει τη φιλοδοξία για ολική κάλυψη του νησιού από wifi ακόμα και στις πιο απόμακρες γωνίες. Αυτή η εργασία ήταν μια πρωτοβουλία του κ. Λιοδάκη Γεώργιου που μας κατεύθυνε στην μελέτη αυτή και σε συνεργασία με την υλοποίηση της από τον κ.Ζερβουδάκη Αντώνιο και δυο Γάλλους συμφοιτητές στα πλαίσια του προγράμματος ανταλλαγής φοιτητών Erasmus φτάσαμε στο επιθυμητό αποτέλεσμα, δηλαδή στην άρτια μελέτη και υλοποίηση του ασύρματου δικτύου της σχολής μας μέσω της εύρεσης των κατάλληλων σημείων (hotspots) και την τοποθέτηση των αναμεταδοτών(access points-repeaters).Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τους καθηγητές μου για την υπομονή και την διάθεση μετάδοσης αυτής τους της γνώσης για την επίτευξη του στόχου μας.

ΠΕΡΙΛΗΨΗ

Πολλές έρευνες και δημοσιεύσεις έχουν γίνει αναφορικά με την απόδοση των ασύρματων δικτύων. Κοινό συμπέρασμα μεταξύ των ερευνητών είναι ότι αυτή εξαρτάται κατά πολύ από τα χαρακτηριστικά του καναλιού ραδιοσυχνοτήτων. Πιο συγκεκριμένα, στα ασύρματα τοπικά δίκτυα, τα οποία καθορίζονται από τα πρότυπα 802.11 της IEEE, οι μετρήσεις διαφόρων μεγεθών του φυσικού στρώματος, βοηθούν τους ειδικούς να εντοπίσουν δυσλειτουργίες και προβλήματα στην ασύρματη υποδομή και να αξιολογήσουν εναλλακτικούς τρόπους σχεδίασης αυτής σε πραγματικό χρόνο και σε πραγματικές συνθήκες αντίστοιχα.

Μέσα σε αυτό το πλαίσιο, στο κεφάλαιο 2 της παρούσης εργασίας παρουσιάζεται το θεωρητικό υπόβαθρο των ραδιοσυχνοτήτων και του ραδιοφάσματος. Το φυσικό στρώμα και το στρώμα πρόσβασης στο μέσο, καθώς και τα χαρακτηριστικά αυτών αναλύονται στα κεφάλαια 3 και 4. Στο κεφάλαιο 5 παρουσιάζονται τα σχετικά κάποια θέματα ασφάλειας. Ο σκοπός αυτής της εργασίας είναι να παρουσιάσει τα παραπάνω χαρακτηριστικά των ασύρματων τοπικών δικτύων με τη βοήθεια του λογισμικού παρακολούθησης και αξιολόγησης ασύρματων τοπικών δικτύων Air Magnet Wi-Fi Analyzer της εταιρείας Fluke Networks. Για τις μετρήσεις και τα δεδομένα που συλλέχθηκαν, χρησιμοποιήθηκε η υπάρχουσα ασύρματη δικτυακή υποδομή του Τεχνολογικού Εκπαιδευτικού Ινστιτούτου Κρήτης,παράρτημα Χανίων. Η ανάλυση και η αξιολόγηση των αποτελεσμάτων παρουσιάζονται στο κεφάλαιο 6.

ABSTRACT

It is well known that the performance of wireless networks depends heavily on the physical layer details of the RF channel. In particular, as it concerns IEEE 802.11 WLANs, physical layer measurements are useful in many ways, such as to diagnose network problems in a real setting or to evaluate alternative wireless designs. In such a framework, the purpose of this thesis is to present various issues of IEEE 802.11 WLANs (physical and MAC layer issues, etc.) as well as to exhibit these issues through a commercial measurement tool. Measurements are taken at the IEEE 802.11 WLAN campus network of TEI of Crete / Branch of Chania. More specifically, the measurement tool used is the Air Magnet Wi-Fi Analyzer, an industry standard tool for mobile auditing and troubleshooting enterprise Wi-Fi networks.

Κάποιες Συσκευές οι οποίες συνδέονται σε ασύρματο δίκτυο στις μέρες μας και που συνεχώς πληθαίνουν διευκολύνοντας τη ζωή μας, απεικονίζονται κάποιες από αυτές.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

1.1 ΓΕΝΙΚΑ

Τα τηλεπικοινωνιακά συστήματα που βασίζονται σε καλώδια είναι από τη φύση τους πιο γρήγορα, πιο αξιόπιστα και πιο ασφαλή από τα αντίστοιχα ασύρματα. Όμως η εγκατάσταση μιας υποδομής καλωδίωσης μπορεί να έχει μεγάλο κόστος. Επιπλέον, αν η υποδομή διασχίζει δημόσιους χώρους, η εγκατάστασή της υπόκειται σε κάποιους περιορισμούς και ρυθμίσεις. Αντίθετα, η ασύρματη επικοινωνία έχει το πλεονέκτημα της "ευκινησίας", η υλοποίηση μιας ασύρματης υποδομής συχνά είναι πιο φθηνή, ενώ οι αυστηροί περιορισμοί που συναντώνται αφορούν το φάσμα συχνοτήτων. Παρόλα αυτά η εκχώρηση μη αδειοδοτημένων τμημάτων του φάσματος βοήθησε τη γρήγορη υιοθέτηση και ανάπτυξη των ασύρματων τοπικών δικτύων.

Το Ευρωπαϊκό Ινστιτούτο Τυποποίησης των Τηλεπικοινωνιών (European Telecommunications Standards Institute, ETSI) εξέδωσε το πρώτο πρότυπο ασύρματου τοπικού δικτύου, το HiperLAN/1, το 1995 και ακολούθησε το HiperLAN/2 το 2000. Στην πράξη όμως το πιο διαδεδομένο και κοινά αποδεκτό πρότυπο είναι το 802.11 του IEEE. Είναι γνωστό ότι κινητές συσκευές όπως οι φορητοί υπολογιστές, οι προσωπικοί ψηφιακοί οδηγοί (Personal Digital Assistant, PDA), αλλά και τα κινητά τηλέφωνα ενσωματώνουν ολοκληρωμένα κυκλώματα που υποστηρίζουν το πρότυπο 802.11. Αρκετά φτηνα΄και ευρέως χρησιμοποιούμενα είναι τα ασύρματα σημεία πρόσβασης (Access Points, APs), δομικά στοιχεία μιας

ασύρματης δικτυακής υποδομής. Στον Πίνακα 1 απεικονίζονται πρότυπα δικτύωσης τηλεπικοινωνιακών συστημάτων της IEEE.

802.x	ΕΦΑΡΜΟΓΗ	ΟΝΟΜΑΣΙΑ
802.1	Bridging	
802.2	Logic Link Control (LLC)	
802.3	CSMA/CD	Ethernet
802.4	Token bus	
802.5	Token ring	
802.11	WLAN	Wi-Fi
802.15	WPAN	Bluetooth
802.16	WMAN	WiMAX

Πίνακας 1. Μερικά πρότυπα της IEEE

Το αρχικό πρότυπο της οικογένειας IEEE 802.11 (συχνά αναφέρεται και ως 802.11-1997) υποστήριζε ρυθμούς μετάδοσης δεδομένων έως 2Mbps. Αυτός ο ρυθμός πλέον έχει φτάσει τα 54 Mbps, ενώ συσκευές που χρησιμοποιούν τεχνολογία πολλαπλής εισόδου/ πολλαπλής εξόδου (Multiple Input Multiple Output, MIMO) μπορούν να υποστηρίξουν ρυθμούς που αγγίζουν τα 300 Mbps και γίνονται ολοένα και πιο δημοφιλής. Το βασικότερο πλεονέκτημα της οικογένειας προτύπων IEEE 802.11 είναι ότι εμπεριέχουν προηγμένες τεχνικές διαμόρφωσης και ταυτόχρονα υποστηρίζουν διασυνδεσιμότητα με παρωχημένες τεχνολογίες. Οι νέες τεχνικές διαμόρφωσης δεν αντικαθιστούν τις παλαιότερες. Έτσι δύναται να επιλεγεί οποιοδήποτε σχήμα διαμόρφωσης με σκοπό την βέλτιστη μετάδοση των πλαισίων δεδομένων. Με αυτό τον τρόπο οι ασύρματες συσκευές προσαρμόζουν το ρυθμό μετάδοσης της ζεύξης ανάλογα με τις συνθήκες του καναλιού.

Ξέχωρα από τα παραπάνω, δε θα μπορούσε κανείς να παραβλέψει κάποια σοβαρά μειονεκτήματα της οικογένειας 802.11 και ειδικότερα αυτά που αφορούν την ασφάλεια. Πιο συγκεκριμένα, τα ασύρματα τοπικά δίκτυα είναι ευάλωτα σε υποκλοπές, μη εξουσιοδοτημένη πρόσβαση και άρνηση υπηρεσίας (Denial of Service, DoS), κυρίως λόγο της φύσης τους. (όποιος έχει μια κεραία μπορεί να

εκπέμπει σήμα και αντίστοιχα όποιος έχει μια κεραία μπορεί να λαμβάνει σήμα). Το αρχικό πρότυπο 802.11-1997 δεν παρείχε απολύτως καμία ασφάλεια οποιουδήποτε επιπέδου, αναφορικά με την επικύρωση, την κρυπτογράφηση ή την ακεραιότητα των δεδομένων. Μεμονωμένα, κάποιοι κατασκευαστές ασύρματων σημείων πρόσβασης πρόσφεραν επικύρωση της φυσικής διεύθυνσης του πελάτη (client). Το πρότυπο επανεξετάστηκε το 1999 για να υποστηρίξει ένα μηχανισμό βασικής προστασίας, το Wired Equivalent Privacy (WEP), το οποίο χρησιμοποιεί κρυπτογραφικές μεθόδους για επικύρωση [15].

Τα σοβαρά κενά ασφάλειας στο WEP οδήγησαν στην ανάπτυξη ενός ξεχωριστού ερευνητικού πεδίου, αυτό της ασφάλειας στα ασύρματα δίκτυα. Το 2001, οι Fluhrer, Mantin και Shamir [1] έδειξαν ότι το κλειδί WEP μπορούσε να ανακτηθεί μέσα σε λίγες ώρες χρησιμοποιώντας απλώς έναν κοινό υπολογιστή οικιακής χρήσης. Επεσήμαναν μια αδυναμία του αλγόριθμου RC4, ο οποίος παράγει το κλειδί και απέδειξαν ότι είναι δυνατή η ανακάλυψη του κλειδιού με μια απλή συγκέντρωση των κρυπτογραφημένων πλαισίων δεδομένο και ανάλυσης αυτών.

Από αυτό το χρονικό σημείο, η εξέλιξη του υλικού, η αύξηση της υπολογιστικής ισχύος είχαν σαν αποτέλεσμα οι επιθέσεις στο WEP κλειδί να γίνουν αρκετά τόσο "αποδοτικές", ώστε να επιτρέπουν την ανάκτησή του σε μερικά μόλις δευτερόλεπτα. Μια επιπλέον αδυναμία του κλειδιού WEP είναι ότι το προδιαμοιραζόμενο κλειδί είναι κοινό σε όλους τους χρήστες που είναι συνδεδεμένοι στο ίδιο Service Set Identifier (SSID). Με αυτόν τον τρόπο οποιοσδήποτε χρήστης μπορεί να αποκρυπτογραφεί τα πακέτα άλλων χρηστών, όταν όλοι αυτοί βρίσκονται στο ίδιο SSID.

Πάντως τα παραπάνω προβλήματα έχουν ξεπεραστεί με την υιοθέτηση καλύτερων τεχνικών ασφάλειας. Οι σύγχρονες αυτές τεχνικές είναι διαθέσιμες μόνο σε καινούριες συσκευές. Αυτό σε συνδυασμό με νέες τεχνικές διαμόρφωσης εγείρει θέμα διασυνδεσιμότητας, καθώς οι παλαιότερες συσκευές θα πρέπει να χρησιμοποιήσουν ενδιάμεσες λύσεις για να μπορέσουν να επικοινωνήσουν.

1.2 ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Το πρότυπο IEEE 802.11 έχει τις "ρίζες" του στο WaveLAN, το οποίο ήταν το ιδιόκτητο ασύρματο τοπικό δίκτυο της εταιρείας NCR. Η NCR κατέθεσε το σχεδιασμό του WaveLAN [36] στην αρμόδια επιτροπή του IEEE για το 802.11 πρότυπο.

802.11x	ΕΤΟΣ	ΣΥΧΝΟΤΗΤΑ	ΕΥΡΟΣ ΖΩΝΗΣ	ΡΥΘΜΟΣ ΜΕΤΑΔΟΣΗΣ	ΚΑΝΑΛΙΑ ΜΙΜΟ	ΔΙΑΜΟΡΦΩΣΗ	ΚΑΛΥΨΗ
	1997	2,4GHz	20MHz	2Mbps	1	DSSS, FHSS	100m
a	1999	5GHz	20MHz	54 Mbps	1	OFDM	120m
		3,7GHz [802.11y]					5000m
b	1999	2,4GHz	20MHz	11 Mbps	1	DSSS	140m
g	2003	2,4GHz	20MHz	54Mbps	1	OFDM, DSSS	140m
n	2009	2,4GHz/5GHz	20MHz	65Mbps	4	OFDM	250m
			40MHz	135Mbps			

Πίνακας 2. Η οικογένεια προτύπων IEEE 802.11

Το IEEE 802.11 πρότυπο εκδόθηκε το 1997 και επικυρώθηκε το 1999. Ήταν ικανό να υποστηρίξει ρυθμούς μετάδοσης 1 ή 2 Mbps. Λειτουργούσε σε μη αδειοδοτημένη ζώνη ραδιοσυχνοτήτων. Η Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών (Federal Communications Commission, FCC) εκχώρησε τη ζώνη των 2,4GHz ISM (Industrial, Scientific, Medical) για τα ασύρματα δίκτυα το 1985. Τα προγενέστερα του 802.11 πρότυπα των ασύρματων δικτύων καθώς και τα πρώτα πρότυπα της οικογένειας 802.11 χρησιμοποιούσαν επίσης τη ζώνη των 900MHz ISM. Το αρχικό πρότυπο 802.11 έχει αντικατασταθεί από ένα πλήθος τροποποιήσεων που εκδόθηκαν από την IEEE (βλ. Πίνακα 2) [25].

Ένας "ανταγωνιστής" του IEEE 802.11 είναι το HiperLAN/1 που εκδόθηκε από το ETSI, το οποίο χρησιμοποιεί μέθοδο πολλαπλής πρόσβασης με ακρόαση φέροντος αποφυγής συγκρούσεων (Carrier Sence Multiple Access with Collision Avoidance, CSMA/CA), παρόμοια με αυτή στο 802.11. Το HiperLAN/2 είναι παρόμοιο με το 802.11a, αλλά αντί της χρήσης του CSMA/CA, η πρόσβαση στο μέσο γίνεται με βάση την πολλαπλή πρόσβαση διαίρεσης χρόνου (Time Division Multiple

Access, TDMA). Όταν εκδόθηκε το HiperLAN/2 το 2000, υπερείχε κατά πολύ του 802.11. Παρά το γεγονός αυτό, οι συσκευές που βασίζονται στο 802.11 κυριάρχησαν γρήγορα στην αγορά.

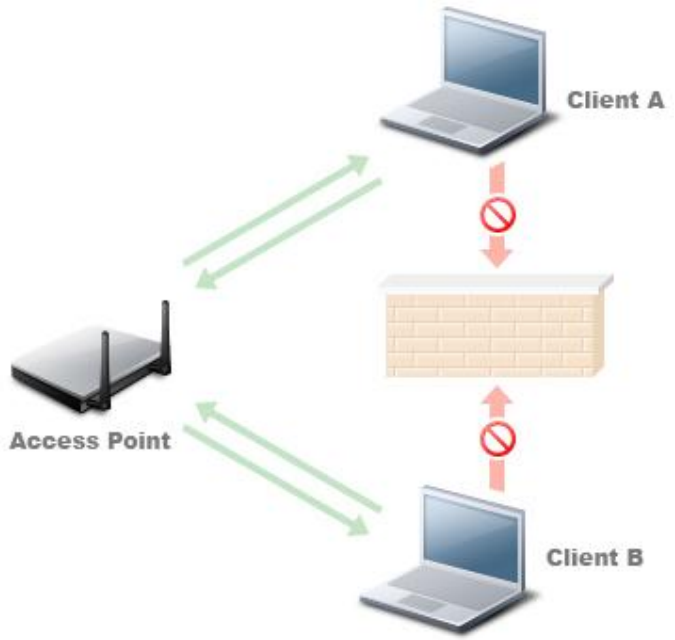
Το 802.11 είναι ένα από τα διάφορα πρότυπα πολλαπλής πρόσβασης. Η λεπτομερή ανάλυση των διάφορων τεχνικών πολλαπλής πρόσβασης ξεφεύγει από τους σκοπούς της παρούσας εργασίας. Γενικά, μπορούμε να σημειώσουμε ότι τα πρωτόκολλα πολλαπλής πρόσβασης εμπίπτουν σε δύο κατηγορίες: active και passive. Τα active συστήματα επιτρέπουν στους χρήστες να μεταδίδουν όποτε αυτοί έχουν να στείλουν δεδομένα. Σε αυτό το σημείο, χρησιμοποιούνται διάφοροι τρόποι για να αποφευχθούν οι συγκρούσεις, οι οποίοι διαφέρουν στο σχεδιασμό, στην πολυπλοκότητα και στην αποτελεσματικότητα.

Τα passive συστήματα βασίζονται σε ένα κεντρικό ελεγκτή ο οποίος επιτρέπει την πρόσβαση στο κανάλι επικοινωνίας μέσω ενός κουπονιού που διανέμεται και κατακρατείται από τους χρήστες εκ περιτροπής. Το πρότυπο 802.11 ελέγχει την πρόσβαση στο κανάλι μέσω ενός πλήθους λειτουργιών συγχρονισμού και καθορίζει active τεχνικές πρόσβασης όσο και passive. Η active πρόσβαση συμβαίνει εξαιτίας ενός αλγορίθμου, της λειτουργίας κατανεμημένου συντονισμού (Distributed Coordination Function, DCF), ο οποίος είναι υποχρεωτικό δομικό στοιχείο του προτύπου 802.11. Ο αλγόριθμος της λειτουργίας συντονισμού σημείου (Point Coordination Function, PCF) υποστηρίζει passive πρόσβαση και είναι προαιρετικό στοιχείο του προτύπου. Η τροποποίηση 802.11e υποστηρίζει διαφοροποιημένες υπηρεσίες τόσο για active όσο και για passive μεθόδους πρόσβασης [30].

Ένα από τα πρώτα ασύρματα συστήματα πολλαπλής πρόσβασης ήταν το Aloha [37]. Το 1970 ο Abramson σκέφτηκε και σχεδίασε ένα ασύρματο δίκτυο για μεταφορά πακέτων δεδομένων στο Πανεπιστήμιο Hawaii, το Aloha. Τα τερματικά επικοινωνούν πάνω από μια κοινή ζώνη συχνοτήτων χρησιμοποιώντας μια μέθοδο τυχαίας πρόσβασης. Το Aloha στην πρώτη του υλοποίηση (pure Aloha) λειτουργούσε ως εξής: ένα τερματικό μεταδίδει όταν έχει δεδομένα προς μετάδοση. Επιβεβαιώνει την επιτυχημένη ή μη αποστολή πακέτου παρακολουθώντας το κανάλι κατά τη διάρκεια της μετάδοσης. Αν συμβεί μια σύγκρουση τότε το πακέτο επαναμεταδίδεται. Συνεχόμενες συγκρούσεις αποφεύγονται εφαρμόζοντας έναν

αλγόριθμο εκθετικής υποχώρησης (exponential back-off), ενώ οι επαναμεταδόσεις αναβάλλονται για ένα τυχαίο χρονικό διάστημα. Αυτό το σχήμα δεν είναι αποδοτικό αναφορικά με το βαθμό χρήσης του καναλιού.

Η ανίχνευση συγκρούσεων δεν είναι εγγενές χαρακτηριστικό των ασύρματων δικτύων. Αφενός η εκπομπή ενός πακέτου και η παρακολούθηση για συγκρούσεις θα απαιτούσε δύο "ζεύξεις" γεγονός που θα καθιστούσε τις ασύρματες συσκευές ακριβές. Αφετέρου, τα σήματα υποκύπτουν σε μεγαλύτερη εξασθένηση στον αέρα από όταν μεταδίδονται μέσω καλωδίου. Ενώ η ισχύς της παρεμβολής είναι ικανή να καταστρέψει ένα πακέτο στο δέκτη, αυτή μπορεί να έχει εξασθενήσει τόσο πολύ ώστε να μην μπορεί να ανιχνευθεί τη στιγμή που φτάνει σε αυτόν. Αυτό είναι το πρόβλημα του κρυμμένου τερματικού [3] (hidden node) (βλ. Σχήμα 1). Στο παρακάτω σχήμα ο Α και ο Β θέλουν να μεταδώσουν, όμως για διάφορους λόγους (υψηλά επίπεδα θορύβου, απόσταση) ο καθένας αγνοεί την ύπαρξη του άλλου. Άρα αν π.χ. ο Α στέλνει πλαίσια και ο Β αποφασίσει να μεταδώσει τότε η σύγκρουση είναι αναπόφευκτη, αφού αγνοεί ότι την συγκεκριμένη χρονική στιγμή μεταδίδει ο Α.



Σχήμα 1. Το πρόβλημα του κρυμμένου κόμβου

Ένα άλλο σχετικό πρόβλημα είναι η περίπτωση του εκτιθέμενου τερματικού (exposed node). Μια εκτιθέμενη συσκευή πρέπει να αναβάλει τη μετάδοση διότι

μια γειτονική συσκευή μεταδίδει σε κάποια τρίτη, η οποία είναι εκτός εμβέλειας της εκτιθέμενης. Η εκτιθέμενη συσκευή αν και δε δημιουργεί παρεμβολές στο σήμα του δέκτη (αφού είναι εκτός εμβέλειας), εντούτοις δεν της επιτρέπεται η εκπομπή. Για τους παραπάνω λόγους λοιπόν, το πρότυπο 802.11 δε δύναται να χρησιμοποιήσει CSMA/CD. Αντ' αυτού χρησιμοποιεί CSMA/CA για active πρόσβαση στο κανάλι.

1.3 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ - ΕΞΕΛΙΞΗ

Το 1985, η Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών FCC εκχώρησε τη ζώνη συχνοτήτων ISM στα ασύρματα δίκτυα [2]. Οι πρώτες ασύρματες υλοποιήσεις εμφανίστηκαν το 1990 και λειτουργούσαν στη ζώνη των 900MHz με ταχύτητες του 1Mbps. Την ίδια περίοδο τα ενσύρματα τοπικά δίκτυα υποστήριζαν ταχύτητες των 10Mbps. Οι υλοποιήσεις αυτές δεν βασίζονταν σε κάποιο πρότυπο. Το 1992 κάνουν την εμφάνισή τους οι πρώτες υλοποιήσεις στη ζώνη των 2,4GHz ISM. Και σε αυτές τις περιπτώσεις παρατηρούνται χαμηλοί ρυθμοί μεταφοράς δεδομένων. Η ανάγκη λοιπόν για την δημιουργία ενός γενικού πλαισίου λειτουργίας των ασύρματων δικτύων είναι επιβεβλημένη και η πρωτοβουλία για το IEEE 802.11 έχοντας ξεκινήσει ήδη από το 1990 εγκρίνεται το 1997. Ο σκοπός του ήταν να αναπτύξει έλεγχο πρόσβασης στο μέσο (Medium Access Control, MAC) και πρότυπα φυσικού επιπέδου (PHY) για σταθερές και κινητές ασύρματες συσκευές.

Οι βασικές προδιαγραφές του αρχικού 802.11 είναι θεμελιώδεις και δεν υπάρχουν πλέον συσκευές που τις υλοποιούν. Η ομάδα εργασίας του 802.11 έκτοτε έχει παρουσιάσει αρκετές βελτιώσεις και επεκτάσεις που επικεντρώνονται κυρίως σε θέματα απόδοσης και ασφάλειας. Από τις πιο αξιοσημείωτες τροποποιήσεις είναι τα 802.11a και 802.11b, οι οποίες εμφανίστηκαν το 1999 και καθορίζουν βελτιωμένες τεχνικές διαμόρφωσης που επιτρέπουν μεγαλύτερους ρυθμούς μετάδοσης. Οι εμπορικές υλοποιήσεις του 802.11b είναι ευρέως διαδεδομένες. Οι συσκευές 802.11b λειτουργούν στην ίδια ζώνη συχνοτήτων με αυτές του πρώτου 802.11, ενώ επιτυγχάνει ρυθμούς μετάδοσης από 5,5Mbps έως 11 Mbps.

Συγχρόνως εισάγει το WEP, την πρώτη μορφή ασφάλειας για ασύρματα δίκτυα, βασισμένη σε κρυπτογραφία.

Η τροποποίηση 802.11a ολοκληρώθηκε το 1999. Το 802.11a λειτουργεί στη ζώνη των 5GHz και χρησιμοποιεί ορθογώνια πολυπλεξία με διαίρεση συχνότητας (Orthogonal Frequency Division Multiplexing, OFDM). Υποστηρίζει ρυθμούς έως 54Mbps, οι οποίοι μπορούν να προσαρμοστούν σε τιμές των 48, 36, 24, 18, 12, 9 ή 6Mbps ανάλογα με τις συνθήκες και τους περιορισμούς του καναλιού. Η FCC επέτρεψε τη χρήση του OFDM το 2001. Αυτό συνέβαλε στην έκδοση της τροποποίησης

802.11g το 2003. Παρόμοια με το προηγούμενο 802.11a, το 802.11g υποστηρίζει ρυθμούς έως 54Mbps (με προσαρμογή στις ίδιες χαμηλότερες τιμές με αυτές του 802.11a). Δεδομένου ότι το 802.11g χρησιμοποιεί το ίδιο φάσμα συχνοτήτων με τα 802.11b, 802.11g, οι αντίστοιχες συσκευές είναι συμβατές με αυτές που βασίζονται στο 802.11b. Επίσης, το 802.11g υλοποιεί μηχανισμούς προστασίας που βρίσκονται στο 802.11b.

Το 802.11n επικυρώθηκε το 2009. Το PHY του 802.11n βασίζεται σε μεγάλο βαθμό σε τεχνολογία MIMO, γεγονός που προσφέρει αυξημένη ταχύτητα και εμβέλεια συγκριτικά με τα προηγούμενα πρότυπα. Οι συσκευές που υλοποιούν το 802.11n μπορούν να λειτουργούν είτε στη ζώνη των 2,4GHz είτε των 5GHz. Εξασφαλίζεται η συμβατότητα με όλα τα προηγούμενα πρότυπα.

Οι πρώτες συσκευές 802.11 των διάφορων κατασκευαστών είχαν αρκετά προβλήματα διασυνδεσιμότητας. Αυτό σε συνδυασμό με την εμφάνιση του 802.11b συνετέλεσε στο σχηματισμό του Wi-Fi Alliance [38] από εταιρείες όπως 3Com, Cisco, Intersil, Lucent, Motorola και άλλε, οι οποίες ελέγχουν τη συμβατότητα των συσκευών που βασίζονται στο 802.11.

Όπως αναφέρθηκε και προηγουμένως, το 802.11b παρουσιάζει ένα μηχανισμό επικύρωσης και κρυπτογράφησης, το WEP, που όμως στην πράξη αποδεικνύεται ανεπαρκής. Το 2004, το 802.11i αναπτύσσεται από την IEEE για να αντιμετωπίσει τα μειονεκτήματα του WEP και να το αντικαταστήσει. Το Wi-Fi Alliance έχει ήδη εισάγει το Wi-Fi Protected Access (WPA), ως μέθοδο προστασίας καλύτερης του WEP, το οποίο βασίζεται σε μια draft έκδοση του 802.11i [32]. Όταν το 802.11i επικυρώνεται, το Wi-Fi Alliance προτείνει το WPA2.

1.4 ΤΟ ΠΕΡΙΒΑΛΛΟΝ ΡΑΔΙΟΣΥΧΝΟΤΗΤΩΝ (RF)

Οι συσκευές 802.11 λειτουργούν σε μη αδειοδοτημένες ζώνες ραδιοσυχνοτήτων, οι οποίες κατά συνέπεια δεν υπόκεινται σε καμία ρύθμιση. Οι συσκευές Wi-Fi θα πρέπει να υπακούν σε αυστηρά όρια ισχύος (ανάλογα την περιοχή και τη ζώνη συχνοτήτων) και μεθόδους διαμόρφωσης. Αυτό γιατί οι ελεύθερες συχνότητες του φάσματος είναι διαμοιραζόμενες στον οποιοδήποτε.

Γενικά, οι συσκευές που λειτουργούν σε αυτές τις συχνότητες δε θα πρέπει να δημιουργούν παρεμβολές σε γειτονικές συσκευές. Η συμφόρηση είναι ένα από τα ανεπιθύμητα συμπτώματα που προκάλεσε η ευρεία χρήση του 802.11. Αυτές οι ζώνες δεν φυλάσσονται αποκλειστικά για συσκευές 802.11. Η ζώνη των 2,4GHz (ISM) είναι ανοιχτή και για ασύρματα τηλέφωνα ή συσκευές Bluetooth. Η εμβέλεια, η απόδοση και η αξιοπιστία των ασύρματων επικοινωνιών εξαρτάται κυρίως από την ισχύ του σήματος και το επίπεδο θορύβου. Το θεώρημα του Shannon μας δίνει ένα άνω φράγμα της χωρητικότητας του καναλιού

$$C = B \cdot log_2(1 + SNR)$$

όπου C η χωρητικότητα του καναλιού (σε bps), B το εύρος ζώνης του καναλιού (σε Hz) και SNR ο σηματοθορυβικός λόγος. Η φασματική πυκνότητα των ραδιοσημάτων εξασθενεί όσο αυξάνει η απόσταση από τον δέκτη. Εμπόδια στο ενδιάμεσο πομπού-δέκτη προκαλούν απορρόφηση ή σκέδαση του σήματος. Τα σήματα που ανακλώνται ή διαθλώνται φτάνουν στον δέκτη εκτός φάσης σε σχέση με αυτά που ακολούθησαν τη διαδρομή άμεσης οπτικής επαφής (Line of Sight, LoS) και κατά συνέπεια "μπερδεύονται". Αυτό προκαλεί τη λεγόμενη εξασθένιση πολλαπλής διόδευσης (multipath fading). Στο επόμενο κεφάλαιο παρουσιάζονται οι βασικές αρχές των ραδιοσυχνοτήτων που απαντώνται στα ασύρματα τοπικά δίκτυα [19][20].

2. ΡΑΔΙΟΣΥΧΝΟΤΗΤΕΣ

2.1 ΜΙΚΡΟΚΥΜΑΤΑ

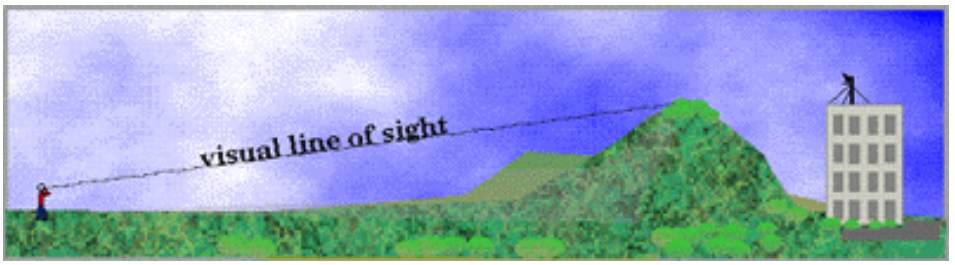
Το αρχικό πρότυπο 802.11 καθορίζει ένα φυσικό επίπεδο PHY που βασίζεται στο φάσμα των υπερύθρων. Επειδή δεν υπήρξε αρκετή εμπορική ανταπόκριση, η παρούσα εργασία θα επικεντρωθεί στο φάσμα των ραδιοκυμάτων. Το φάσμα των ραδιοκυμάτων εκτείνεται από μερικά Hz έως 300GHz. Τα WLANs λειτουργούν εντός ενός εύρους συχνοτήτων, γνωστών ως μικροκύματα.

Όλα τα ηλεκτρονικά κυκλώματα εκπέμπουν τέτοια κύματα. Η ενέργεια στον πομπό μεταφέρεται στο χώρο με τη μορφή ηλεκτρομαγνητικών κυμάτων [19][22]. Τον πρώτο λόγο στη διάδοση αυτών των κυμάτων έχει η συχνότητα. Για παράδειγμα, στην περιοχή συχνοτήτων 2-30MHz τα κύματα διαδίδονται στην ατμόσφαιρα και διαθλώνται στην ιονόσφαιρα. Συγκεκριμένα για τα WLANs ενδιαφερόμαστε για συχνότητες πάνω από 30MHz. Σε αυτή την περιοχή τα σήματα διαδίνονται μεταξύ πομπού και δέκτη ακολουθώντας τη διαδρομή LoS (βλ. Σχήμα 2). Η εμβέλεια αυτών των κυμάτων περιορίζεται από την κυρτότητα της Γης και άλλες παραμέτρους. Τα ραδιοκύματα σε αυτές τις συχνότητες υπόκεινται σε πολύ μικρή διάθλαση από την ιονόσφαιρα και τείνουν να διαδοθούν μέσα από αυτή. Για αυτό και είναι ιδανικά για δορυφορικές επικοινωνίες [21]. Έτσι λοιπόν οι μικροκυματικές συχνότητες είναι αυτές στις οποίες λειτουργούν τα WLANs βασισμένα στο 802.11 πρότυπο. Η διάδοση αυτών των κυμάτων εξαρτάται από το περιβάλλον και τα αντικείμενα μέσα σε αυτό. Οι παράμετροι που καθορίζουν το τρόπο με τον οποίο αυτή λαμβάνει χώρα είναι οι παρακάτω:

- Διαδρομή άμεσης οπτικής επαφής (LoS path)
- Απορρόφηση
- Διάθλαση
- Περίθλαση
- Αντανάκλαση
- Σκέδαση
- Εξασθένιση Πολλαπλής Διόδευσης

ΔΙΑΔΡΟΜΗ LoS

Όταν υπάρχει LoS μεταξύ πομπού και δέκτη τότε τα σήματα ακολουθούν αυτή την άμεση διαδρομή προς το δέκτη. Κατά την εκπομπή του σήματος, η ενέργειά του διαχέεται στην γύρω περιοχή καθώς αυτό διαδίδεται στον αέρα. Ο τρόπος και το μέγεθος αυτής της διάχυσης εξαρτάται από τον τύπο της κεραίας (ισοτροπική, κατευθυντική, κλπ.). ένα μικρό ποσοστό του σήματος φτάνει στην κεραία του δέκτη. Η περιοχή λήψης ή αλλιώς το ενεργό άνοιγμα (effective aperture) της κεραίας καθορίζει το ποσό της ενέργειας του σήματος που φτάνει στο δέκτη.



Σχήμα 2. Η Line of Sight διαδρομή

ΑΠΟΡΡΟΦΗΣΗ

Όταν τα μικροκύματα συναντούν κάποιο φυσικό εμπόδιο, ένα τμήμα από την ενέργεια που μεταφέρουν απορροφάται. Ως εκ τούτου το σήμα που θα ληφθεί στο δέκτη είναι εξασθενημένο. Ο βαθμός της εξασθένισης του σήματος εξαρτάται από το υλικό του φυσικού εμποδίου.

ΔΙΑΘΛΑΣΗ

Όταν το κύμα διαπερνά ένα εμπόδιο με διαφορετική ταχύτητα διάδοσης τότε το κύμα κάμπτεται. Η ανακατεύθυνση του κύματος ονομάζεται διάθλαση.

ΠΕΡΙΘΛΑΣΗ

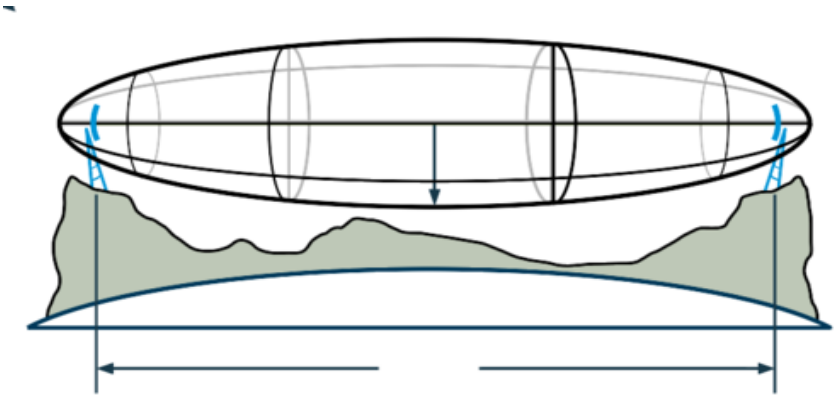
Η περίθλαση λαμβάνει χώρα όταν τα μικροκύματα συναντούν την ακμή ενός αντικειμένου αρκετά μεγάλου συγκριτικά με το μήκος κύματος. Ένα τμήμα της ενέργειας του κύματος κάμπτεται, προκαλώντας αλλαγή διεύθυνσης. Τερματικά που είναι σχεδόν LoS και βρίσκονται στη σκιά ενός αντικειμένου λαμβάνουν εξασθενημένα σήματα.

ΑΝΤΑΝΑΚΛΑΣΗ

Τα μικροκύματα αντανακλώνται στις επιφάνειες αντικειμένων το υλικό των οποίων σχετίζεται με το μήκος κύματος. Τα εμπόδια που βρίσκονται σχεδόν LoS (near Line of Sight) αντανακλούν τα κύματα προκαλώντας τη διπλή λήψη τους στο δέκτη. Αυτές οι αντανακλάσεις μπορεί να αποβούν καταστρεπτικές ή ενισχυτικές αναφορικά με τη λήψη του σήματος στο δέκτη. Αυτό εξαρτάται από το αν η φάση τους συμβαδίζει με τη φάση του σήματος που λαμβάνεται από τη LoS.

Οι ζώνες Fresnel παρέχουν έναν τρόπο ανάλυσης της παρεμβολής λόγω φυσικών εμποδίων σχεδόν LoS (βλ. Σχήμα 3). Αν το αντανακλώμενο κύμα φτάσει στο δέκτη με ολίσθηση φάσης κατά π, τότε το εμπόδιο βρίσκεται εντός της ακτίνας της πρώτης ζώνης Fresnel. Η ακτίνα της δεύτερης ζώνης Fresnel σχηματίζεται από τα σημεία εκείνα όπου τα αντανακλώμενα κύματα φτάνουν με συμφωνία φάσης στο δέκτη.

μπόδια που περιέχονται στην πρώτη ζώνη "καταστρέφουν" το σήμα, ενώ εμπόδια στην δεύτερη ζώνη επιδρούν θετικά. Θεωρητικά υπάρχει άπειρο πλήθος ζωνών Fresnel, αυτές περιττού αριθμού έχουν αρνητική επίδραση, ενώ αυτές άρτιου αριθμού έχουν θετική.



Σχήμα 3. Ζώνες Fresnel

ΣΚΕΔΑΣΗ

Ένα κύμα υφίσταται σκέδαση όταν συναντά ένα αντικείμενο και τότε η κατανομή ενέργειάς του υπόκειται σε αλλαγές στη διεύθυνση, τη φάση και την πόλωση.

ΕΞΑΣΘΕΝΙΣΗ ΠΟΛΛΑΠΛΗΣ ΔΙΟΔΕΥΣΗΣ

Η εξασθένιση πολλαπλής διόδευσης μπορεί να μοντελοποιηθεί με χρήση στατιστικών μοντέλων. Τα πιο γνωστά μοντέλα είναι η κατανομή Rayleigh και η κατανομή Rice. Η διάδοση του σήματος μέσω της τροπόσφαιρας και της ιονόσφαιρας εμπίπτει στην εξασθένιση Rayleigh. Η ίδια κατανομή είναι επίσης κατάλληλη για αστικές περιοχές όπου τα σήματα σπάνια είναι LoS. Στην αντίθετη περίπτωση, θα προτιμήσουμε την κατανομή Rice [20].

2.2 ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΡΑΔΙΟΣΥΧΝΟΤΗΤΩΝ

Το ραδιοφάσμα είναι ένα δημόσιο αγαθό και υπόκειται σε αυστηρούς περιορισμούς. Οι ρυθμιστικές αρχές είναι υπεύθυνες για τον έλεγχο των συχνοτήτων που χρησιμοποιούνται. Στην Αγγλία η ρυθμιστική αρχή είναι η Office of Communications (OFCOM). Στις Ηνωμένες Πολιτείες υπάρχουν δύο ρυθμιστικές αρχές, η Federal Communications Commission (FCC) και η National Telecommunications Information Administration (NTIA) που ασχολούνται για εμπορικά και κυβερνητικά ζητήματα αντίστοιχα [39].

Το ραδιοφάσμα διαιρείται σε ζώνες και εκχωρείται για παροχή μιας συγκεκριμένης υπηρεσίας. Υπάρχουν τρεις τύποι εκχώρησης του φάσματος:

- Αδειοδοτημένο
- Ανοιχτό
- Μη αδειοδοτημένο

Για τις αδειοδοτημένες ζώνες, οι ρυθμιστικές αρχές εκδίδουν άδειες προς τους οργανισμούς, οι οποίοι αποκτούν αποκλειστικά δικαιώματα χρήσης της συγκεκριμένης ζώνης. Το ποιος θα αποκτήσει αυτές τις άδειες καθορίζεται από τη ρυθμιστική αρχή, η οποία για αυτό το σκοπό χρησιμοποιεί τους παρακάτω τρόπους:

- στρατηγική first come first served
- κληρωση
- δημοπρασία
- εσωτερική διοικητική διαδικασία

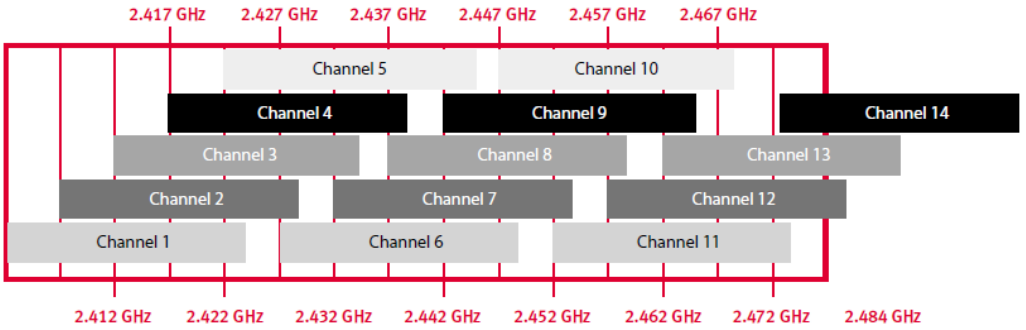
Ο πρώτος και ο δεύτερο τρόπος χρησιμοποιούνται σπάνια έως καθόλου. Πιο συνηθισμένη τακτική είναι αυτή της δημοπρασίας. Για παράδειγμα, στην Αγγλία η εκχώρηση φάσματος για υπηρεσίες 3G έγινε με αυτό τον τρόπο. Ας σημειωθεί ότι δεν είναι όλες οι αδειοδοτημένες ζώνες του φάσματος για αποκλειστική χρήση από κάποιο οργανισμό, κάποιες ζώνες εκχωρούνται για χρήση από συγκεκριμένες τεχνολογίες. Για τη χρήση των ανοιχτών ζωνών δεν απαιτείται κάποια σχετική άδεια.

Κανάλι #	Συχνότητα GHz		Αμερική	Ευρώπη	Ιαπωνία
	Min	Max			
1	2,401	2,423	✓	✓	✓
2	2,406	2,428	✓	✓	✓
3	2,411	2,433	✓	✓	✓
4	2,416	2,438	✓	✓	✓
5	2,421	2,443	✓	✓	✓
6	2,426	2,448	✓	✓	✓
7	2,431	2,453	✓	✓	✓
8	2,436	2,458	✓	✓	✓
9	2,441	2,463	✓	✓	✓
10	2,446	2,468	✓	✓	✓
11	2,451	2,473	✓	✓	✓
12	2,456	2,478	×	✓	✓
13	2,461	2,483	×	✓	✓
14	2,466	2,488	×	×	✓

Πίνακας 3. Κανάλια και συχνότητες ανά περιοχή

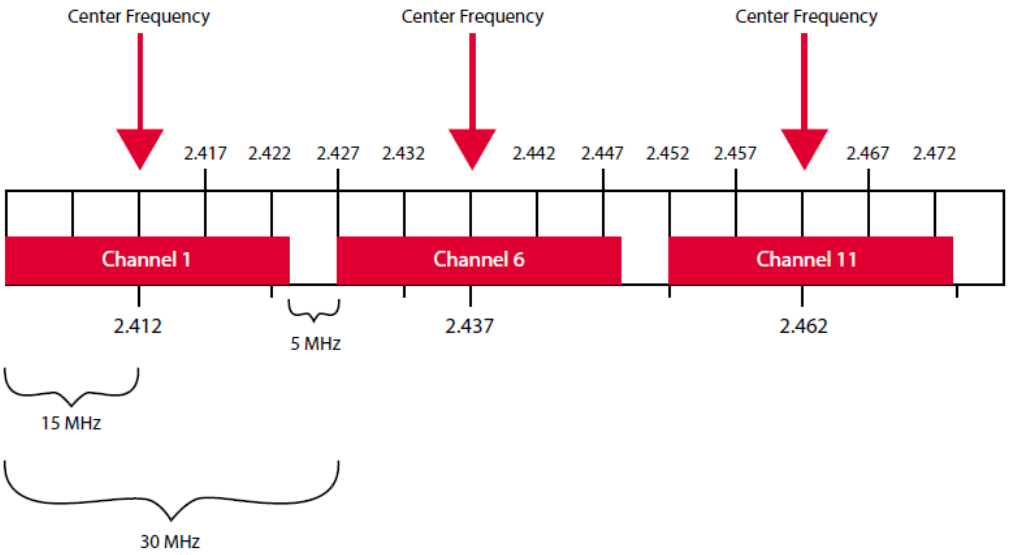
Το μόνο που απαιτείται είναι κάποιες ελάχιστες προϋποθέσεις και κανόνες χρήσης που επιβάλλονται ώστε η πρόσβαση και χρήση αυτών των ζωνών να μην είναι ανεξέλεγκτη, αφού αυτό θα είχε ως αποτέλεσμα η ζώνη να μην μπορεί να χρησιμοποιηθεί από όλους τους χρήστες.

Ούτε οι μη αδειοδοτημένες ζώνες απαιτούν κάποια άδεια. Η διαφορά είναι ότι οι αντίστοιχοι περιορισμοί στην πρόσβαση και χρήση είναι πιο αυστηροί. Σε αυτή την κατηγορία είναι οι ζώνες ISM [40]. Οι συσκευές που χρησιμοποιούν το 802.11 λειτουργούν σε κάποιες ζώνες ISM. Η πρώτη ISM ζώνη που χρησιμοποιήθηκε ήταν αυτή των 900MHz. Οι συσκευές 802.11b και 802.11g χρησιμοποιούν τις ζώνες 2,4GHz. Η ζώνη διαιρείται σε ένα πλήθος από επικαλυπτόμενα κανάλια (βλ. Σχήμα 4). Στην Αμερική ορίζονται 11 κανάλια, το ETSI ορίζει 13 κανάλια για την Ευρώπη, ενώ στην Ιαπωνία χρησιμοποιούνται και τα 14 κανάλια (βλ. Πίνακα 3) [18].



Σχήμα 4. Επικαλυπτόμενες συχνότητες και κανάλια

Το εύρος ζώνης κάθε καναλιού είναι 22MHz με μια διαφορά 5MHz μεταξύ των κεντρικών συχνοτήτων του κάθε καναλιού (βλ. Σχήμα 5). Κάθε κανάλι μπορεί να έχει μέχρι τέσσερα γειτονικά κανάλια που επικαλύπτονται. Στο 802.11 και για την ζώνη των 2,4GHz, τα τρία μη επικαλυπτόμενα κανάλια είναι τα 1, 6 και 11. Οι συσκευές 802.11a λειτουργούν στη μη αδειοδοτημένη ζώνη των 5GHz. Η εκχώρηση του φάσματος ποικίλει ανά περιοχή [6].



Σχήμα 5. Εύρος ζώνης που απαιτείται σε κάθε κανάλι.

2.3 ΔΙΑΧΕΙΡΙΣΗ ΦΑΣΜΑΤΟΣ

Σε μη αδειοδοτημένες ζώνες οι συσκευές WLAN θα πρέπει να τηρούν κάποιους περιορισμούς αναφορικά με τη χρήση του φάσματος, όπως π.χ. η ισχύς εκπομπής. Πιο συγκεκριμένα, οι συσκευές που λειτουργούν στο εύρος των 5GHz θα πρέπει να κάνουν έλεγχο εκπεμπόμενης ισχύος (Transmit Power Control, TPC) και δυναμική επιλογή συχνότητας (Dynamic Frequency Selection, DFS) [7]. Η περιοχή των 5GHz είναι κατειλημμένη από τα ραντάρ και δορυφορικές υπηρεσίες. Επιπρόσθετα, θα πρέπει να κάνουν χρήση τεχνικών διασποράς φάσματος.

Η διασπορά φάσματος (Spread Spectrum, SS) είναι η μέθοδος διασποράς ενός σήματος στενής ζώνης σε μια ευρύτερη ζώνη συχνοτήτων. Αυτό είναι χρήσιμο γιατί έτσι τα σήματα που υπόκεινται σε τέτοιες τεχνικές γίνονται πιο "ανθεκτικά" σε παρεμβολές, παράσιτα και υποκλοπές, για αυτό και είναι ευρεία η στρατιωτική της χρήση. Οι τεχνικές λοιπόν αυτές υλοποιούν δύο φάσεις διαμόρφωσης:

- διαμόρφωση του κώδικα διασποράς
- διαμόρφωση του μηνύματος διασποράς

Το αρχικό πρότυπο 802.11 [25] καθόριζε δύο τεχνικές διασποράς φάσματος: τη διασπορά φάσματος με εναλλαγή συχνοτήτων (Frequency Hopping Spread Spectrum, FHSS) και τη διασπορά φάσματος συνεχούς ακολουθίας (Direct Sequence Spread Spectrum, DSSS).

Στη FHSS, ο πομπός και ο δέκτης "μεταπηδούν" από κανάλι σε κανάλι ακολουθώντας μια ψευδοτυχαία ακολουθία. Τέτοια ακολουθία είναι διαφορετική ανά διαφορετικό ζευγάρι πομπού/δέκτη έτσι ώστε να ελαχιστοποιηθούν οι συγκρούσεις κατά την επικοινωνία στο ίδιο κανάλι.

Στη DSSS, ο πομπός και ο δέκτης χρησιμοποιούν την ίδια κεντρική συχνότητα. Η ενέργεια του αρχικού σήματος διευρύνεται σε μια ευρύτερη ζώνη, πολλαπλασιάζοντάς αυτήν με μια ψευδοτυχαία ακολουθία. Το σήμα DSSS στο δέκτη υφίσταται αποδιεύρυνση (despreading).

Από τότε που επικυρώθηκε το αρχικό πρότυπο 802.11 έχουν παρουσιαστεί διάφορες τεχνικές διαμόρφωσης. Η DSSS υψηλού ρυθμού (High Rate DSSS, HR/DSSS) παρουσιάστηκε στην τροποποίηση 802.11b και η ορθογώνια πολυπλεξία διαίρεσης συχνότητας (Orthogonal Frequency Division Multiplexing, OFDM) παρουσιάστηκε αρχικά στο 802.11a και μετέπειτα χρησιμοποιήθηκε στα 802.11g και 802.11n. Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, οι συσκευές 802.11 προσαρμόζουν την τεχνική διαμόρφωσης, και κατά συνέπεια την ταχύτητα της ζεύξης, σύμφωνα με το περιβάλλον. Το πρότυπο 802.11 δεν καθορίζει τον τρόπο με τον οποίο θα πρέπει να γίνει αυτή η προσαρμογή. Αφήνεται στον κατασκευαστή να επιλέξει πώς αυτή θα υλοποιηθεί.

Η τροποποίηση 802.11k [33]παρουσιάστηκε για να παρέχει ένα πλαίσιο μετρικών για τη διαχείριση και συντήρηση των WLANs. Η τροποποίηση 802.11r έχει κι αυτή τον ίδιο σκοπό με τη διαφορά ότι επικεντρώνεται κυρίως στο VOIP (Voice Over IP).

Αυτό το πλαίσιο μετρικών επιτρέπει στις συσκευές να συλλέγουν πληροφορίες που σχετίζονται με την απόδοση της ραδιοζεύξης και μπορούν είτε να υπολογίσουν τοπικές τιμές είτε να ζητήσουν πληροφορία από γειτονικές συσκευές. Για παράδειγμα, ας υποθέσουμε ένα ασύρματο δίκτυο με διάφορα access points, τα οποία υποστηρίζουν το αρχικό 802.11. Οι συσκευές θα συνδεθούν με τα access points βασισμένες στην καλύτερη ποιότητα σήματος. Αυτό θα έχει ως συνέπεια μια

ανισοκατανομή τερματικών και access points, αφού κάποια access points ενδέχεται να υπερφορτωθούν από τερματικά και κάποια άλλα να υπολειτουργούν. Επομένως, είναι πολύ σημαντική μια πληροφορία αναφορικά με την τοπολογία των τερματικών ώστε να γίνεται καλύτερος διαμοιρασμός του συνολικού εύρους ζώνης.

Η τροποποίηση 802.11h [31] παρουσιάστηκε για να συμπεριλάβει τις ευρωπαϊκές ρυθμιστικές απαιτήσεις των WLANs που λειτουργούν στη ζώνη των 5GHz (π.χ. συσκευές με το 802.11a). Το πρότυπο αυτό αποτελεί μια επέκταση του MAC για το TPC και DFS. Ο σκοπός του TPC είναι να ελαχιστοποιήσει την παρεμβολή μεταξύ δύο διπλανών ασύρματων δικτύων και ταυτόχρονα βελτιστοποιεί την αξιοπιστία κατά τη μετάδοση των πλαισίων. Το 802.11h είναι υπεύθυνο για την επιβολή της μέγιστης τοπικής τιμής στην εκπεμπόμενη ισχύ, με γνώμονα την ικανότητα μετάδοσης των συσκευών και τα επίπεδα παρεμβολής. Αυτή η μέγιστη τιμή δε θα πρέπει να ξεπερνά την τιμή που καθορίζεται από τη ρυθμιστική αρχή. Οι συσκευές συνδέονται με τα access points βασιζόμενα στην ισχύ τους. Η μέγιστη τιμή ισχύος καθορίζεται από το access point και γνωστοποιείται στα τερματικά χρησιμοποιώντας κάποια κατάλληλα πλαίσια ελέγχου. Αυτή η τιμή ενημερώνεται δυναμικά σύμφωνα με τις αλλαγές στο κανάλι επικοινωνίας.

Ο σκοπός του DFS είναι να ελαχιστοποιεί τις παρεμβολές σε άλλες ασύρματες συσκευές στη συγκεκριμένη περιοχή. Οι ασύρματες συσκευές συλλέγουν πληροφορία για την κατάσταση του καναλιού και ενημερώνουν το access point. Βασισμένο σε αυτή την πληροφορία, το access point ακολούθως καθορίζει αν απαιτείται η εναλλαγή σε άλλο κανάλι. Με το DFS, το access point ελέγχει την επικοινωνία μέσα στο βασικό σύνολο υπηρεσιών (Basic Service Set, BSS). Οι συσκευές μπορεί να μην έχουν πρόσβαση στο κανάλι χωρίς εξουσιοδότηση από το access point. Πριν από την εξουσιοδότηση οποιασδήποτε επικοινωνίας το access point επιλέγει ένα κανάλι και παρακολουθεί για σήματα. Αν εντοπίσει παρεμβολή τότε επιλέγει άλλο κανάλι. Όταν βρεθεί κανάλι χωρίς παρεμβολές τότε τις άλλες συσκευές στο BSS να συντονιστούν σε αυτό. Ελλείψει access point, απαιτείται από τις συσκευές να ανιχνεύσουν οι ίδιες τις παρεμβολές. Το access point καθορίζει ποιες χρονικές περιόδους οι συσκευές μπορούν να σκανάρουν το κανάλι [20].

3. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΜΕΣΟ (MAC)

Οι συσκευές που λειτουργούν σε ένα ασύρματο περιβάλλον αντιμετωπίζουν καταστάσεις που δεν υφίσταται στα ενσύρματα τοπικά δίκτυα. Όμως, για το επίπεδο πρωτοκόλλου θα πρέπει να εμφανίζονται σαν αυτά. Το 802.11 καθορίζει τον έλεγχο πρόσβασης στο μέσο (Medium Access Control, MAC) ως ένα υπόστρωμα του επιπέδου ζεύξης δεδομένων. Το MAC παρέχει υπηρεσίες σε ένα δεύτερο υπόστρωμα, τον έλεγχο λογικών συνδέσεων (Logical Link Control, LLC). Κατω από το υπόστρωμα MAC είναι το φυσικό επίπεδο, το οποίο αποτελείται από δύο υποστρώματα: το πρωτόκολλο σύγκλισης φυσικού επιπέδου (Physical Layer Convergence Protocol, PLCP) και το εξαρτώμενο από το φυσικό μέσο (Physical Medium Dependent, PMD).

Τα πλαίσια LLC περνούν στο στρώμα MAC και ενθυλακώνονται MAC Service DataUnits (MSDUs) προσθέτοντας ένα πεδίο ελέγχου σειράς, το frame check sequence (FCS). Ένα MSDU αντιστοιχεί σε ένα ή περισσότερα MAC Protocol Data Units (MPDUs). Τα MPDUs περνούν στο φυσικό επίπεδο για μετάδοση.

Το 802.11 MAC ελέγχει την πρόσβαση το κανάλι ραδιοσυχνοτήτων μέσω ενός αριθμού λογικών λειτουργιών που ονομάζονται λειτουργίες συντονισμού. Αυτές οι λειτουργίες καθορίζουν πότε μια συσκευή μπορεί να μεταδίδει πλαίσια. Η λειτουργία κατανεμημένου συντονισμού (Distributed Coordination Function, DCF) και η λειτουργία συντονισμού σημείου (Point Coordination Function, PCF) καθορίστηκαν στο αρχικό πρότυπο.

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο, η DCF είναι απαραίτητο στοιχείο του 802.11. Η παράδοση των πλαισίων με τη DCF ακολουθεί τη λογική best-effort. Η είναι ένα προαιρετικό στοιχείο του 802.11, το οποίο υποστηρίζει παράδοση πλαισίων χρονικά περιορισμένη. Η PCF διαιρεί το ασύρματο μέσο σε περιόδους που εναλλάσσονται μεταξύ περιόδων χωρίς ανταγωνισμό (Contention-

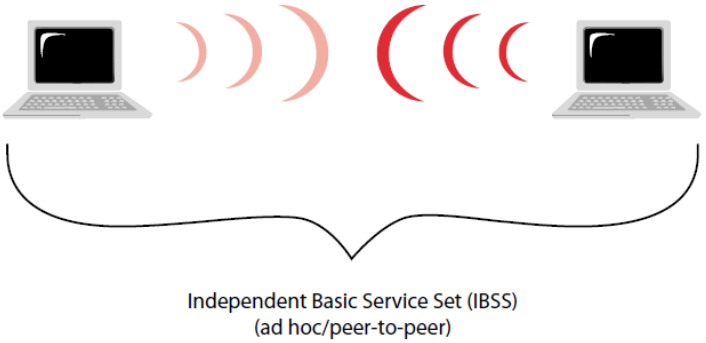
Free Periods, CFP) και σε περιόδους ανταγωνισμού (Contention Periods, CP). Κατά τη διάρκεια των CFPs, η πρόσβαση στο κανάλι ελέγχεται από έναν κυρίαρχο κόμβο (τυπικά μπορεί να είναι ένα access point) χρησιμοποιώντας ένα μηχανισμό ψηφοφορίας. Η DCF χρησιμοποιείται για τις CPs [21].

Η τροποποίηση 802.11e [30] παρουσιάστηκε για να υποστηρίξει ποιότητα υπηρεσίας (Quality of Service, QoS). Η λειτουργία υβριδικού συντονισμού (Hybrid Coordination Function, HCF) είναι συμβατή με το MAC του αρχικού 802.11. Στις επόμενες γραμμές θα αναλυθούν οι τρεις αυτές λειτουργίες.

3.1 ΥΠΗΡΕΣΙΕΣ 802.11

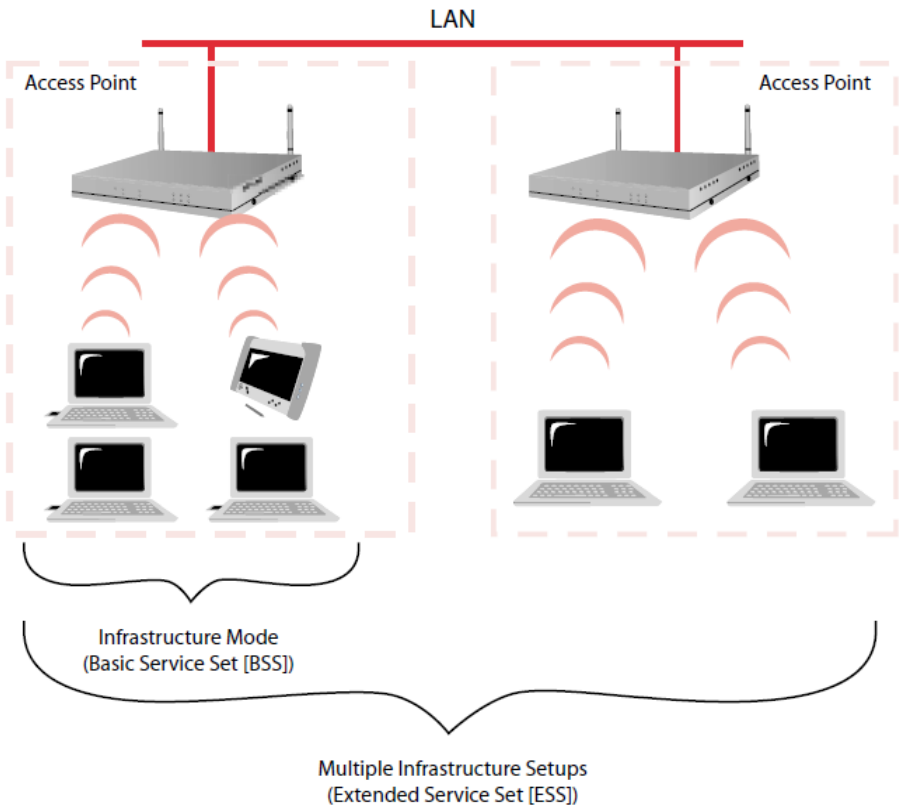
Το 802.11 καθορίζει ένα πλήθος από αρχιτεκτονικές: το βασικό σύνολο υπηρεσιών (Basic Service Set, BSS), το ανεξάρτητο σύνολο βασικών υπηρεσιών (Independent Basic Service Set, IBSS) και το επεκταμένο σύνολο υπηρεσιών (Extended Service Set, ESS). Το BSS αποτελείται από διάφορες ασύρματες συσκευές και ένα access point. Οι συσκευές επικοινωνούν μέσω του access point. Το BSS και το ESS είναι επίσης γνωστά ως υποδομές (infrastructure mode). Στο IBSS οι συσκευές συνδέονται η μια με την άλλη με adhoc τρόπο (adhoc mode) και επικοινωνούν απευθείας χωρίς την ύπαρξη κάποιου access point (βλ. Σχήμα 6). Ένας αριθμός από BSS μπορούν να διασυνδεθούν διαμέσου ενός συστήματος κατανομής (Distribution System, DS) για να σχηματίσουν ένα ESS (βλ. Σχήμα 7). Το DS είναι τυπικά ένα ενσύρματο τοπικό δίκτυο. Τα ασύρματα συστήματα κατανομής (Wireless Distribution Systems, WDS) μπορούν επίσης να χρησιμοποιηθούν [17].

Το 802.11 παρέχει διάφορες υπηρεσίες. Πέρα από την παράδοση των πλαισίων προσφέρει λειτουργίες πιστοποίησης, εξουσιοδότησης και ιδιωτικότητας. Αυτές οι υπηρεσίες προσφέρονται και στα δύο modes (infrastructure και adhoc). Στο infrastructure mode παρέχονται κάποιες επιπλέον υπηρεσίες όπως η σύνδεση, η αποσύνδεση και η επανασύνδεση.



Σχήμα 6. Adhoc mode και IBSS.

Έως ότου μια συσκευή μπορέσει να στέλνει και να λαμβάνει πλαίσια σε ένα BSS/ESS WLAN, πρέπει πρώτα να γνωστοποιήσει το εαυτό της στο access point με το να συνδεθεί με αυτό. Όταν μια συσκευή μετακινείται από ένα BSS σε ένα άλλο, πρέπει να επανασυνδεθεί με το νέο access point. Μια συσκευή αποσυνδέεται από το BSS στέλνοντας μια αίτηση αποσύνδεσης στο access point.



Σχήμα 7. Infrastructure mode (BSS και ESS)

Μια συσκευή θα πρέπει να πιστοποιήσει τον εαυτό της πριν συνδεθεί. Το 802.11 έχει ένα πλήθος από μεθόδους πιστοποίησης, η απλούστερη των οποίων είναι η ανοιχτή πιστοποίηση (open authentication). Κατά την ανοιχτή πιστοποίηση, μια συσκευή στέλνει μια αίτηση πιστοποίησης στο access point και αυτό με τη σειρά του στέλνει στη συσκευή μια απόκριση πιστοποίησης (χωρίς επικύρωση της αυθεντικότητας της συσκευής). Κάποια σχήματα αυθεντικότητας βασισμένα στην κρυπτογραφία παρέχονται από το 802.11.

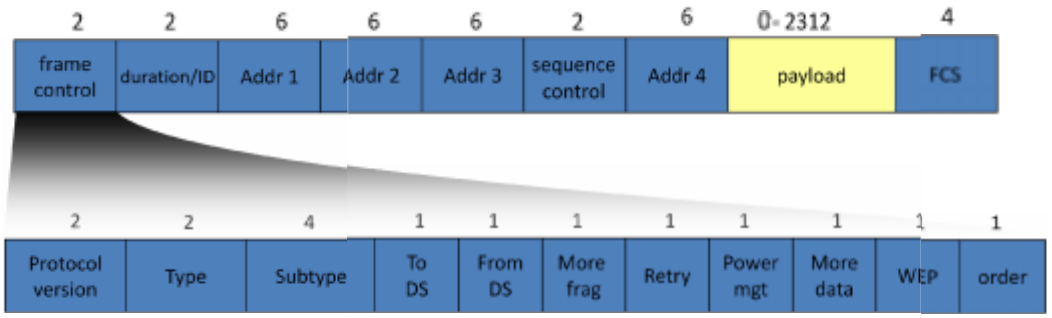
Πριν από την πιστοποίηση και σύνδεση των συσκευών, αυτές θα πρέπει να ενημερώσουν το access point ότι βρίσκονται εντός εμβέλειας. Δύο μέθοδοι ανίχνευσης χρησιμοποιούνται, η παθητική (passive) και η ενεργός (active). Στην παθητική ανίχνευση, η συσκευή παρακολουθεί κάθε κανάλι για αναγνωριστικά πλαίσια το οποία ονομάζονται beacons. Αυτά εκπέμπονται από τα access points. Κατά την ενεργό ανίχνευση, η συσκευή στέλνει μια αίτηση ελέγχου. Τα access points που είναι εντός εμβέλειας ανταποκρίνονται με μια απόκριση ελέγχου. Η συσκευή αποθηκεύει προσωρινά οποιαδήποτε BSSIDs που απέκτησε κατά τη διάρκεια της ενεργούς ή παθητικής ανίχνευσης. Τα beacons δεν χρησιμεύουν μόνο για να ανακοινώνουν ασύρματα δίκτυα, αλλά επίσης χρησιμοποιούνται για να συγχρονίσουν τα ρολόγια σε όλες τις συσκευές που είναι στο ίδιο BSS. Το beacon μεταφέρει ένα target beacon transmission time (TBTT) που είναι το χρονικό διάστημα μεταξύ δύο διαδοχικών beacons. Οι συσκευές στο BSS διακόπτουν οποιαδήποτε μετάδοση πλαισίων κατά το TBTT [17].

3.2 ΔΟΜΗ ΠΛΑΙΣΙΟΥ MAC

Στο σχήμα 8 φαίνεται η δομή ενός πλαισίου MAC. Τα πεδία που αυτό περιέχει είναι τα εξής:

- Frame control: το πεδίο αυτό αποτελείται από κάποια υποπεδία. Η δομή του φαίνεται επίσης στο σχήμα 10, ενώ τα πεδία αυτά είναι:
  - Protocol version: η έκδοση του MAC. Υπάρχει μόνο ένα πρότυπο για το MAC και παίρνει την τιμή 0.

- ❖ Type: περιγράφει τον τύπο πλαισίου, δηλαδή αν αυτό αφορά δεδομένα, έλεγχο ή διαχείριση
- ❖ Subtype: οι τιμές αυτού του πεδίου εξαρτώνται από το προηγούμενο πεδίο
- ❖ To DS: παίρνει τιμή 1 αν το πλαίσιο είναι για το DS
- ❖ From DS: παίρνει τιμή 1 αν το πλαίσιο είναι από το DS
- ❖ More frag: αν ένα πλαίσιο είναι κατατετμημένο τότε όλα εκτός από το τελευταίο έχουν σε αυτό το πεδίο τιμή 1
- ❖ Retry: αν το πλαίσιο είναι επαναμετάδοση τότε παίρνει τιμή 1, διαφορετικά παίρνει τιμή 0
- ❖ Power Mgt: αν ο πομπός είναι σε κατάσταση εξοικονόμησης ενέργειας παίρνει τιμή 1, αλλιώς τιμή 0
- ❖ More data: όταν μια συσκευή είναι σε κατάσταση εξοικονόμησης ενέργειας, το access point φυλάσσει τα πλαίσια που προορίζονται για αυτή. Παίρνει τιμή 1 για να δείξει ότι το access point έχει ένα ή περισσότερα πακέτα για συσκευή που είναι σε κατάσταση sleep
- ❖ WEP: παίρνει τιμή 1 υποδεικνύοντας ότι το πλαίσιο είναι κρυπτογραφημένο με WEP
- ❖ Order: παίρνει τιμή 1 για να δείξει ότι η επεξεργασία των ληφθέντων πλαισίων θα γίνει με τη σειρά



Σχήμα 8. Το πλαίσιο MAC και τα πεδία από τα οποία αποτελείται.

- ➢ Duration/ID: καθορίζει το χρόνο μεταξύ της αποστολής πλαισίου και της λήψης της επιβεβαίωσής του.

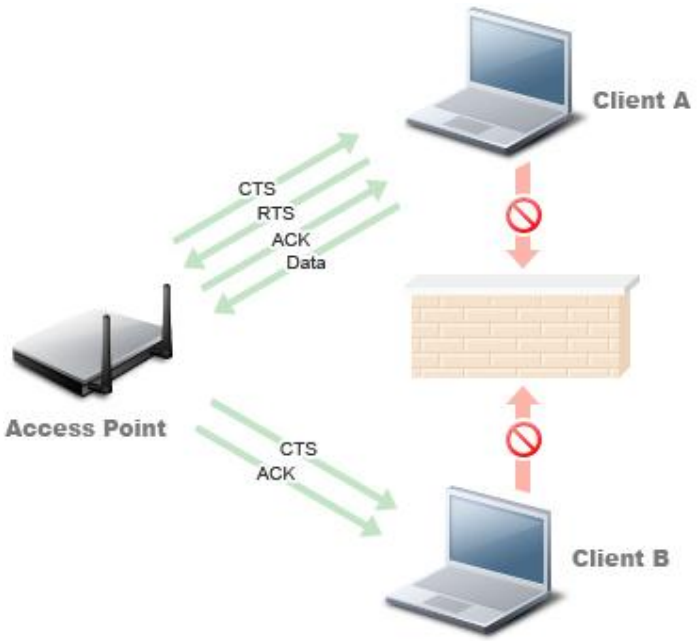
- Addr 1-4: περιέχουν διευθύνσεις 48-bit. Οι διευθύνσεις αυτές εξαρτώνται από τα υποπεδία from DS και to DS του πεδίου frame control και συζητούνται παρακάτω
- Sequence control: είναι ένας αριθμός σειράς των 12-bit συν ένα αριθμό τμήματος των 4-bit και χρησιμοποιείται για να αναγνωριστούν και να ταξινομηθούν τα τμήματα των MSDU (MPDUs).
- Frame body: περιέχει το payload και το FCS (32-bit CRC)

Η σημασία των διευθύνσεων στο πλαίσιο MAC είναι η εξής. Στο adhoc mode (IBSS) η διευθυνσιοδότηση είναι άμεση. Έτσι το Addr1 είναι η MAC διεύθυνση του προορισμού και η Addr2 είναι η διεύθυνση του πομπού. Το Addr3 καθορίζεται στο BSSID και το Addr4 δε χρησιμοποιείται. Στο πεδίο frame control, τόσο το To Ds όσο και το From DS είναι 0. Στο infrastructure mode, η διευθυνσιοδότηση είναι διαφορετική. Έστω ότι μια συσκευή στέλνει πλαίσια σε μια άλλη. Ακόμα κι αν η μια είναι στην εμβέλεια της άλλης τα πλαίσια κυκλοφορούν μέσω του access point. Για τα πλαίσια από τη συσκευή προς το access point το To DS είναι 1 και το From DS είναι 0. Το Addr1 παίρνει την τιμή του BSSID, το Addr 2 είναι η διεύθυνση του πομπού και το Addr3 είναι η διεύθυνση του δέκτη. Για τα πλαίσια που στέλνονται από το access point σε μια συσκευή το To DS είναι 0 και το From DS είναι 1. Το Addr1 είναι η διεύθυνση προορισμού, το Addr2 είναι η διεύθυνση του πομπού και το Addr3 είναι το BSSID. Το Addr4 δεν χρησιμοποιείται.

Έστω τώρα μια συσκευή στέλνει ένα πλαίσιο σε μια άλλη που είναι όμως σε άλλο BSS. Και οι δύο συσκευές είναι συνδεδεμένες σε διαφορετικά access points. Το To DS είναι 1 και το From DS είναι 1 όταν τα πλαίσια μεταδίδονται μεταξύ των access-points. Το Addr1 είναι η διεύθυνση MAC του access point που λαμβάνει και το Addr2 είναι η διεύθυνση MAC του access point που στέλνει. Τα Addr 3 και Addr4 είναι οι διευθύνσεις δέκτη και πομπού αντίστοιχα [4][5][13].

3.3 ΛΕΙΤΟΥΡΓΙΑ ΚΑΤΑΝΕΜΗΜΕΝΟΥ ΣΥΝΤΟΝΙΣΜΟΥ (DCF) [30]

Η DCF βασίζεται στο πρωτόκολλο πολλαπλής πρόσβασης με ακρόαση φέροντος (Carrier Sense Multiple Access, CSMA). Η DCF μπορεί επίσης να υποστηρίξει ένα μηχανισμό αποφυγής συγκρούσεων, ο οποίος χρησιμοποιεί ένα handshake μηνυμάτων ready-to-send/clear-to-send (RTS/CTS) πριν από την αποστολή ενός πλαισίου. Ο σκοπός αυτού του μηχανισμού είναι να αντιμετωπιστεί το πρόβλημα του κρυμμένου τερματικού (hidden terminal) που περιγράφηκε στο κεφάλαιο 1. Έτσι λοιπόν στο παρακάτω σχήμα οι Α και Β δεν ξέρουν ο ένας για την ύπαρξη του άλλου και έστω ότι ο Α έχει πρόσβαση αρχικά στο κανάλι, αφού με τα RTS/CTS ενημερώθηκε από το access point ότι το κανάλι είναι ελεύθερο και ότι μπορεί να μεταδώσει. Ο Β επιθυμεί να μεταδώσει αλλά δε θα του επιτραπεί η πρόσβαση, άρα δε θα γίνει σύγκρουση.



Σχήμα 9. Λύση στο πρόβλημα του κρυμμένου κόμβου μέσω μηνυμάτων RTS/CTS

ΑΚΡΟΑΣΗ ΦΕΡΟΝΤΟΣ

Μια συσκευή πρέπει να ακροάσει το κανάλι προτού εκκινήσει μια μετάδοση. Το 802.11 καθορίζει δύο μεθόδους ακρόασης φέροντος:

- Ακρόαση φυσικού φέροντος (Physical Carrier Sensing, PCS)
- Ακρόαση εικονικού φέροντος (Virtual Carrier Sensing, VCS)

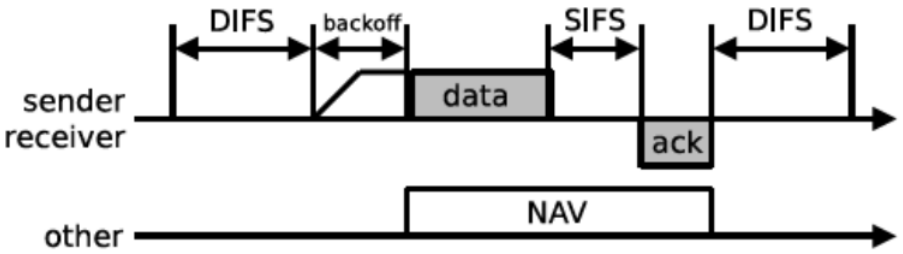
Με το PCS, η ακρόαση φέροντος γίνεται στο φυσικό επίπεδο χρησιμοποιώντας τη λειτουργία αξιολόγησης μη κατειλημμένου καναλιού (Clear Channel Assessment, CCA). Το CCA μπορεί να χρησιμοποιήσει είτε σύμφωνες είτε ασύμφωνες μεθόδους ανίχνευσης σήματος. Η σύμφωνη ανίχνευση σήματος έγκειται στην ανίχνευση προοιμίου (preamble), όπου ο κόμβος συγχρονίζεται με το προοίμιο του πλαισίου. Με αυτή τη μέθοδο το CCA εκτελείται συνεχώς ώστε να μπορεί να ανιχνεύσει το προοίμιο στο κανάλι. Κατά την ασύμφωνη μέθοδο, η ένδειξη ισχύος ληφθέντος σήματος (Received Signal Strength Indicator, RSSI) συγκρίνεται με κάποιο κατώφλι. Αντίθετα με την σύμφωνη μέθοδο, δεν απαιτείται κάποιος συγχρονισμός εξαρχής και μπορεί να εκκινηθεί εν μέσω μετάδοσης πλαισίου, άρα είναι πιο αποδοτική από πλευράς κατανάλωσης ενέργειας.

Το VCS χρησιμοποιεί έναν χρονομετρητή ο οποίος ονομάζεται διάνυσμα εκχώρησης δικτύου (Network Allocation Vector, NAV) για τη δέσμευση το καναλιού. Η τιμή του NAV καθορίζεται στο πεδίο διάρκειας στην επικεφαλίδα του MAC. Κάθε συσκευή παρακολουθεί το NAV και "αφουγκράζεται" το κανάλι παρακολουθώντας την τιμή του. Αν αυτή η τιμή είναι διάφορη του μηδενός, τότε κάποια άλλη συσκευή μεταδίδει. Μια συσκευή ακούει το κανάλι πριν μεταδώσει ένα πλαίσιο για μια χρονική περίοδο που καθορίζεται από το κατανεμημένο διάστημα μεταξύ των πλαισίων (Distributed Inter-Frame Space, DIFS). Αν το κανάλι είναι ελεύθερο για αυτή την περίοδο, η συσκευή μεταδίδει το πλαίσιο. Αν η συσκευή καταλάβει ότι το κανάλι χρησιμοποιείται από άλλη τότε αναβάλει τη μετάδοση και συνεχίζει να ακούει το κανάλι. Μόλις το κανάλι ελευθερωθεί, η συσκευή εξακολουθεί να το ακούει για το υπόλοιπο του διαστήματος DIFS και έπειτα μπαίνει σε μια περίοδο οπισθοχώρησης (backoff), κατά την οποία περιμένει έναν χρονομετρητή που μετρά αντίστροφα να λήξει. Ο χρονομετρητής παγώνει όταν το κανάλι γίνει απασχολημένο και συνεχίζει ότι ελευθερωθεί ξανά. Η συσκευή μεταδίδει ότι ο μετρητής γίνει μηδέν.

ΜΕΘΟΔΟΙ ΜΕΤΑΔΟΣΗΣ ΠΛΑΙΣΙΩΝ

Η DCF υποστηρίζει δύο μεθόδους μετάδοσης, τη βασική και την RTS/CTS. Η δεύτερη μέθοδος υποστηρίζει αποφυγή συγκρούσεων. Με τη βασική μέθοδο (βλ. Σχήμα 10), αν η συσκευή διαπιστώσει ότι το κανάλι είναι ελεύθερο τότε στέλνει τα

πλαίσια δεδομένων. Όλες οι γειτονικές συσκευές που ανιχνεύουν το πλαίσιο θέτουν στο NAV τους τιμή σύμφωνα με την τιμή του πεδίου duration της επικεφαλίδας του πλαισίου δεδομένων. Η τιμή του πεδίου duration ορίζεται από το χρόνο μετάδοσης πλαισίου, το χρόνο αποστολής της επιβεβαίωσης (ACK) και το μικρό διάστημα μεταξύ των πλαισίων (Short Inter-Frame Space, SIFS). Αν το πλαίσιο δεδομένων ληφθεί σωστά, ο δέκτης, αφού περιμένει για ένα SIFS, απαντά με ένα ACK πριν λήξει το NAV.



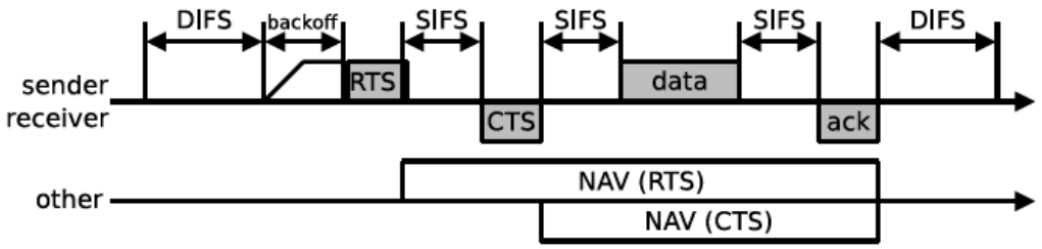
Σχήμα 10. Πρόσβαση στο κανάλι με τη βασική DCF μέθοδο μετάδοσης

Με τη μέθοδο της αποφυγής συγκρούσεων (βλ. Σχήμα 11), έχουμε επιπλέον δύο μεταδόσεις πλαισίων πέραν των δεδομένων και ACK. Αφού λοιπόν ανιχνεύσει το κανάλι ως ελεύθερο, ο αποστολέας εκκινεί την επικοινωνία με τον δέκτη στέλνοντας ένα πλαίσιο RTS. Μόλις ληφθεί από το δέκτη, αυτός με τη σειρά του περιμένει για ένα SIFS και στέλνει ένα πλαίσιο CTS. Οι γείτονες πομπού και δέκτη ανιχνεύουν τις μεταδόσεις κάποιων εκ των RTS και CTS και ρυθμίζουν κατάλληλα τις τιμές των NAVs τους. Τα αντίστοιχα πεδία duration στα RTS και CTS αντίστοιχα, υπολογίζονται από τις εξισώσεις:

$$\text{duration\_field} = t_{CTS} + t_{DATA} + t_{ACK} + 3 \cdot SIFS$$

$$\text{duration\_field} = t_{DATA} + t_{ACK} + 2 \cdot SIFS$$

Αφού η ανταλλαγή των μηνυμάτων RTS/CTS γίνει επιτυχημένα, μεταδίδονται τα πλαίσια δεδομένων και τα ACKs όπως ακριβώς και στη βασική μέθοδο.



Σχήμα 11. Πρόσβαση στο κανάλι με χρήση RTS/CTS και ρύθμιση των NAV.

ΔΙΑΣΤΗΜΑ ΜΕΤΑΞΥ ΤΩΝ ΠΛΑΙΣΙΩΝ (INTER-FRAME SPACING)

Οι συσκευές θα πρέπει να περιμένουν για μια χρονική περίοδο πριν μεταδώσουν ένα πλαίσιο, η οποία ονομάζεται Inter-Frame Space (IFS). Η διάρκεια του IFS εξαρτάται από τον τύπο του πλαισίου. Ως εκ τούτου το MAC του 802.11 αναθέτει διαφορετική προτεραιότητα μεταξύ των πλαισίων με τη χρήση IFS διαφορετικού μεγέθους. Οι χρόνοι IFS που ορίζονται από το αρχικό πρότυπο είναι οι εξής:

- Short IFS (SIFS)
- PCF IFS (PIFS)
- DCF IFS (DIFS)
- Extended IFS (EIFS)

Ισχύει ότι SIFS<PIFS<DIFS<EIFS, οπότε με αυτόν τον τρόπο καθορίζονται και οι προτεραιότητες. Οι χρόνοι SIFS προηγούνται πλαισίων υψηλής προτεραιότητας, δηλαδή των ACK, CTS (βλ. Πίνακα 4). Στο DCF προηγείται πάντα χρόνος DIFS οποιασδήποτε μετάδοσης δεδομένων. Αντίστοιχα στο PCF προηγείται πάντα χρόνος PIFS οποιασδήποτε μετάδοσης δεδομένων. Αφού ισχύει ότι DIFS>PIFS, οι μεταδόσεις PCF έχουν μεγαλύτερη προτεραιότητα. Το EIFS χρησιμοποιείται στο DCF αντί του DIFS στην περίπτωση που οι μεταδόσεις πλαισίων δε γίνουν με τη σωστή σειρά. Οι χρόνοι PIFS και DIFS αντίστοιχα υπολογίζονται από τις σχέσεις:

$$PIFS = aSIFSTime + aSlotTime$$
$$DIFS = SIFS + 2 \cdot aSlotTime$$

Το SIFS εξαρτάται από το PHY και υπολογίζεται ως εξής:

$$SIFS = RxRFDelay + RxPLCPDelay + MacProcessingDelay + RxTxTurnaroundTime$$

ενώ το aSlotTime είναι:

$$aSlotTime = CCATime + RxTxTurnaroundTime + AirPropagationTime + MacProcessingDelay$$

Για τους χρόνους SIFS και aSlotTime ορίζονται οι παρακάτω παράμετροι ως εξής:

RxRFDelay: ο χρόνος που χρειάζεται το PHY για να παραδώσει ένα σύμβολο στο PLCP

RxPLCPDelay: ο χρόνος που χρειάζεται το PLCP για να παραδώσει ένα σύμβολο στο MAC

MacProcessingDelay: ο χρόνος επεξεργασίας ενός πλαισίου από το MAC

RxTxTurnaroundTime: ο μέγιστος χρόνος που χρειάζεται το PHY για να εναλλαχθεί μεταξύ λήψης και αποστολής

CCATime: ο ελάχιστος χρόνος που χρειάζεται το PHY για να καθορίσει την κατάσταση του καναλιού

AirPropagationTime: η καθυστέρηση διάδοσης διαμέσου του ασύρματου καναλιού

PHY	aSlotTime	SIFS
FHSS	50μs	28μs
DSSS	20μs	10μs
OFDM	9μs	16μs

Πίνακας 4. Οι τιμές των aSlotTime και SIFS για κάθε PHY.

ΑΛΓΟΡΙΘΜΟΣ ΤΥΧΑΙΑΣ ΟΠΙΣΘΟΧΩΡΗΣΗΣ

Αν δύο ή περισσότερες συσκευές ανιχνεύσουν ότι το κανάλι είναι κατειλημμένο, τότε αναβάλλουν τις μεταδόσεις τους μέχρι αυτό να ελευθερωθεί. Στην περίπτωση που και οι δύο μεταδώσουν όταν το κανάλι είναι διαθέσιμο και αφού έχουν περιμένει για χρόνο DIFS, τότε γίνεται σύγκρουση. Για να αποφευχθούν αυτές οι συγκρούσεις, το πότε θα γίνουν οι μεταδόσεις καθορίζεται από έναν αλγόριθμο τυχαίας οπισθοχώρησης (random backoff). Κάθε συσκευή περιμένει για ένα τυχαίο πλήθος χρονοθυρίδων πριν μεταδώσει. Η συσκευή με τη μικρότερη τιμή χρονομετρητή θα χρησιμοποιήσει πρώτη το κανάλι. Τότε οι χρονομετρητές των άλλων συσκευών σταματούν να μετρούν, ενώ θα συνεχίσουν την αντίστροφη μέτρηση τους όταν το κανάλι γίνει ξανά ελεύθερο, με τη διαδικασία αυτή να επαναλαμβάνεται συνεχώς. Το μήκος του μετρητή σε χρονοθυρίδες καθορίζεται από τον αλγόριθμο δυαδικής εκθετικής οπισθοχώρησης (Binary Exponential Backoff,

BEB). Ο αριθμός των χρονικών σχισμών επιλέγεται ομοιόμορφα τυχαία από το διάστημα [0,CW − 1], όπου CW είναι το τρέχον μέγεθος του παραθύρου ανταγωνισμού (Contention Window, CW). Ο μετρητής υπολογίζεται σύμφωνα με τη σχέση:

$$backoff = \lfloor CW \cdot U(0,1) \rfloor \cdot aSlotTime$$

όπου U(0,1) είναι ένας τυχαίος αριθμός μεταξύ 0 και 1 που επιλέγεται ομοιόμορφα. Η τιμή του CW εξαρτάται από τον αριθμό των συγκρούσεων και των προηγούμενων επιτυχημένων μεταδόσεων. Το CW στην i-οστή αποτυχημένη μετάδοση, δηλαδή το CW_i, δίνεται από:

$$CW_i = 2^i \cdot (CW_{min} + 1) - 1, \quad 0 \le i \le m$$

όπου $m = \log_2 CW_{max} / CW_{min}$

Στην πρώτη προσπάθεια μετάδοσης, είναι $CW_0 = CW_{min}$. Μετά από κάθε σύγκρουση το CW διπλασιάζεται. Το CW_i ποτέ δεν ξεπερνά το CW_{max}, όπου $CW_{max} = 2^m \cdot (CW_{min} + 1) - 1$. Το CW επανέρχεται στην τιμή CW_{min} όταν το πλαίσιο μεταδίδεται επιτυχώς. Οι παράμετροι του αλγορίθμου BEB διαφέρουν ανάλογα με το PHY. Οι μέγιστες και ελάχιστες τιμές του CW φαίνονται στον παρακάτω πίνακα:

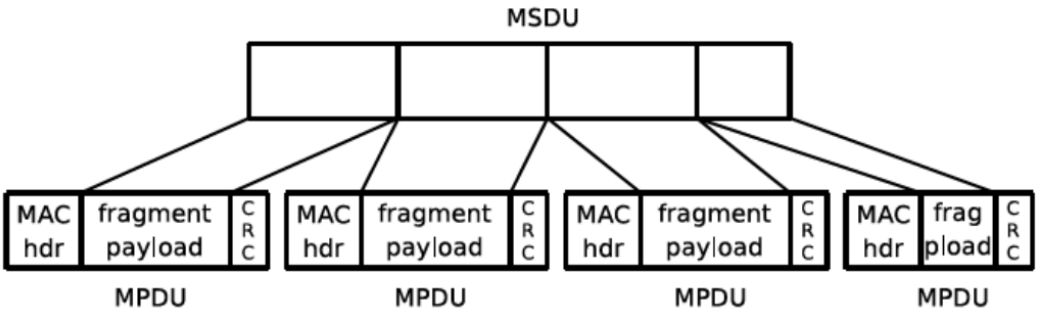
PHY	CW_{min}	CW_{max}
FHSS	15	1023
DSSS	31	1023
OFDM	15	1023

Πίνακας 5. Οι τιμές των CW ανάλογα με κάθε PHY

ΚΑΤΑΤΜΗΣΗ (FRAGMENTATION)

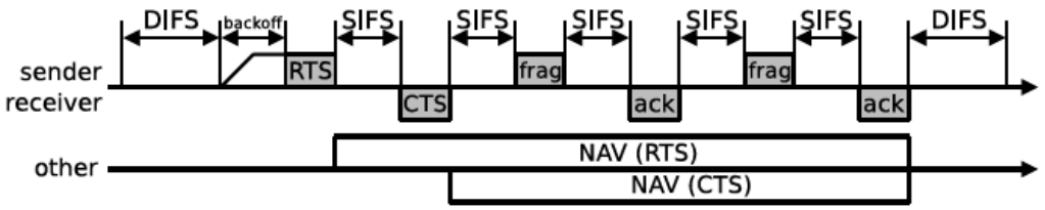
Καθότι τα ασύρματα κανάλια είναι από τη φύση τους αναξιόπιστα, τα MSDUs με μέγεθος μεγαλύτερο ενός συγκεκριμένου μπορεί να είναι κατατετμημένα και να σταλούν ως μια ακολουθία μικρότερων MPDUs (βλ. Σχήμα 12). Ο δέκτης είναι υπεύθυνος να ανασυνθέσει το MSDU από τα MPDUs. Αυτή η διαδικασία ονομάζεται αποκατάτμηση. Κάθε MPDU αποστέλλεται ανεξάρτητα και επιβεβαιώνεται επίσης ανεξάρτητα. Ως εκ τούτου οποιαδήποτε σφάλματα κατά τη

μετάδοσή τους επιφέρουν επανεκπομπή μόνο των συγκεκριμένων MPDUs κι όχι ολόκληρου του MSDU. Η μετάδοση ενός MSDU θα θεωρείται επιτυχημένη μόνο όταν η μετάδοση όλων των MPDUs γίνει με επιτυχία.



Σχήμα 12. Κατάτμηση ενός MSDU σε MPDUs.

Ένας μηχανισμός αυτόματης επανεκπομπής (Automatic Repeat reQuest, ARQ) χρησιμοποιείται για έλεγχο των σφαλμάτων. Το 802.11 υλοποιεί για κάθε MPDU το πρωτόκολλο παύσης-και-αναμονής (stop-and-wait) με θετικές επιβεβαιώσεις (positive ACK)(βλ. Σχήμα 13). Επίσης, ορίζεται ένας χρόνος προθεσμίας (timeout) για τα ACK. Το MPDU επαναμεταδίδεται όταν λήξει αυτή η προθεσμία. Όταν επιτευχθεί ο μέγιστος αριθμός επαναμεταδόσεων ενός MPDU, η μετάδοση ολόκληρου του MSDU αναβάλλεται (τα υπόλοιπα MPDUs στην ακολουθία απορρίπτονται).



Σχήμα 13. Μετάδοση ενός κατατετμημένου MSDU με τη μέθοδο RTS/CTS

ΔΙΚΑΙΟΣΥΝΗ

Το DCF παρουσιάζει ορισμένα προβλήματα δικαιοσύνης. Με τον όρο δικαιοσύνη εννοούμε το εξής. Όπως προαναφέραμε, οι συσκευές προσαρμόζουν το ρυθμό μετάδοσης ανάλογα με τις συνθήκες του καναλιού. Ο ρυθμός σφαλμάτων αυξάνεται όσο οι συνθήκες του καναλιού χειροτερεύουν, προκαλώντας έτσι ολοένα και περισσότερες αναμεταδόσεις. Κάτω από κακές λοιπόν συνθήκες, η ελάττωση

του ρυθμού μετάδοσης μπορεί να μετριάσει το ρυθμό σφαλμάτων (άρα και τις επανεκπομπές). Οι συσκευές που μεταδίδουν με χαμηλούς ρυθμούς θα χρησιμοποιούν το κανάλι για μεγαλύτερα χρονικά διαστήματα από ότι αυτές που μεταδίδουν με υψηλότερους ρυθμούς. Αυτό στο 802.11 ονομάζεται ανωμαλία επίδοσης (performance anomaly). Αναφορικά με την πρόσβαση στο κανάλι, το 802.11 επιτυγχάνει μακροπρόθεσμη δικαιοσύνη. Για μικρό πλήθος τερματικών το 802.11 επιτυγχάνει βραχυπρόθεσμη δικαιοσύνη. Ένα τερματικό με μεγάλο CW τελικά θα αποκτήσει πρόσβαση στο κανάλι αφού το χρονικό διάστημα οπισθοχώρησης κάποια στιγμή θα λήξει. Η βραχυπρόθεσμη δικαιοσύνη όμως εξαλείφεται όσο αυξάνεται το πλήθος των συσκευών. Αυτές των οποίων οι μεταδόσεις υφίστανται συγκρούσεις θα έχουν μεγάλα διαστήματα αναμονής. Οι συσκευές που μόλις έχουν αναβάλλει τη μετάδοσή τους για ακρόαση το κανάλι με το NAV τους, απολαμβάνουν μεγαλύτερης προτίμησης για μετάδοση, από ότι αυτές που είχαν υποστεί σύγκρουση.

Επιπρόσθετα, το DCF δεν είναι δίκαιο όσον αφορά τη σχέση μεταξύ ανερχόμενης και κατερχόμενης ζεύξης (upstream/downstream). Έστω ότι N−1 συσκευές είναι συνδεδεμένες με ένα access point, τότε μαζί με αυτό έχουν η καθεμιά 1/N της συνολικής χωρητικότητας του καναλιού. Δεδομένου ότι το DCF δεν υποστηρίζει QoS, το access point έχει την ίδια προτεραιότητα με οποιαδήποτε άλλη συσκευή, ακόμα και όταν αυτό εκκινεί όλες τις κατερχόμενες ζεύξεις στο WLAN. Σε κάθε περίπτωση η συνολική λειτουργία του DCF θεωρείται δίκαιη αν και δε μπορεί να διαχωρίσει τις υπηρεσίες. Οι λειτουργίες που περιγράφονται στις επόμενες γραμμές υλοποιούν καθορισμό προτεραιοτήτων και μια πιο ντετερμινιστική παράδοση πλαισίων.

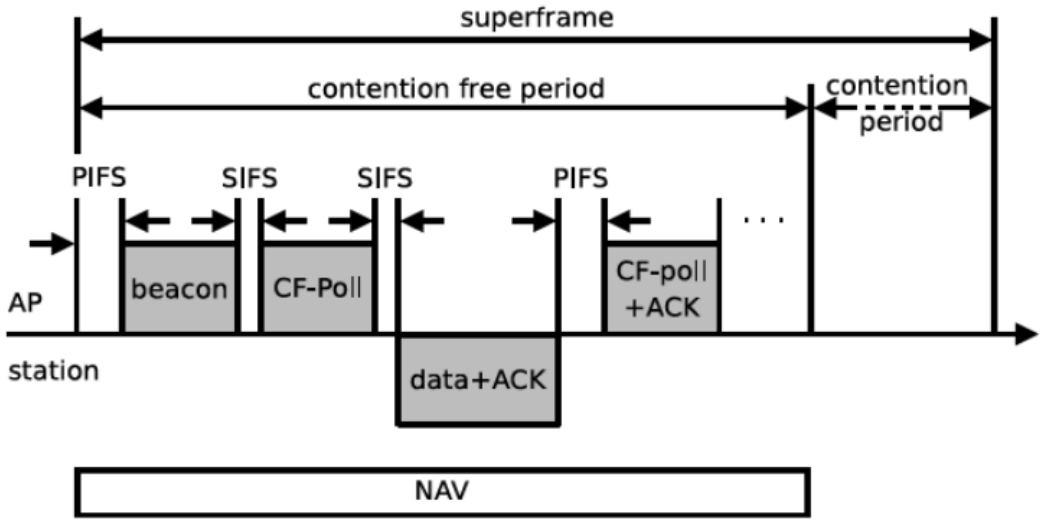
3.4 ΛΕΙΤΟΥΡΓΙΑ ΣΥΝΤΟΝΙΣΜΟΥ ΣΗΜΕΙΟΥ (PCF) [30]

Το DCF υποστηρίζει μόνο μια υπηρεσία παράδοσης πλαισίων "καλύτερης προσπάθειας" (best-effort), γεγονός που το κάνει αναξιόπιστο. Το PCF δημιουργήθηκε για να παρέχει υποστήριξη στην παράδοση πλαισίων όταν αυτή

είναι χρονικά εξαρτώμενη. Το PCF δουλεύει μόνο σε infrastructure mode. Ένας συντονιστής σημείου ή σημειακός συντονιστής (Point Coordinator, PC) "τρέχει" σε ένα access point και περιοδικά στέλνει beacons. Αυτό διαιρεί το κανάλι σε μια ακολουθία από "υπερπλαίσια" (superframes) αποτελούμενα από CFPs ακολουθούμενα από CPs.

Το PC εκκινεί ένα CFP με το παίρνει τον έλεγχο του καναλιού στέλνοντας ένα beacon μετά από χρόνο PIFS. Το beacon ανακοινώνει τη διάρκεια του CFP και όλες οι συσκευές που το λαμβάνουν αναθέτουν στο NAV τους τιμή ίση με τη διάρκεια του CFP, αποτρέποντας έτσι πρόσβαση με DCF. Η πρόσβαση με DCF επανεκκινείται όταν το NAV γίνει μηδέν. Τα τερματικά αποκτούν πρόσβαση στο κανάλι από το PC.

Το PC διατηρεί μια λίστα από συσκευές που δύνανται να μεταδώσουν κατά τη διάρκεια του CFP και αναθέτει την πρόσβαση μέσω ψηφοφορίας (polling) μεταξύ των συσκευών της λίστας του. Το PC περιμένει ένα χρονικό διάστημα ίσο με SIFS μετά από το beacon και έπειτα στέλνει ένα πλαίσιο CF-Poll στην πρώτη συσκευή. Η συσκευή απαντά με ένα ACK αν δεν έχει πλαίσια να μεταδώσει, αλλιώς στέλνει ένα πλαίσιο CF-ACK μαζί με τα δεδομένα. Στην τελευταία περίπτωση, το PC απαντά με ένα πλαίσιο CF-ACK μαζί με ένα CF-Poll. Είναι προφανές λοιπόν ότι το PC μπορεί ταυτόχρονα να κάνει polling στην επόμενη συσκευή της λίστας και να επιβεβαιώνει δεδομένα από την προηγούμενη. Στο τέλος του CFP, το CP επανεκκινείται και οι συσκευές χρησιμοποιούν τη μέθοδο μετάδοσης DCF για να αποκτήσουν πρόσβαση στο κανάλι.



Σχήμα 14. Πρόσβαση καναλιού με τη μέθοδο PCF

3.5 ΛΕΙΤΟΥΡΓΙΑ ΥΒΡΙΔΙΚΟΥ ΣΥΝΤΟΝΙΣΜΟΥ (HCF) [30]

Ενώ το PCF δημιουργήθηκε για μεταδόσεις πακέτων χρονικά εξαρτώμενες, κάποια προβλήματα είναι ορατά. Ο χρόνος μεταξύ των beacons δεν είναι προβλέψιμος. Το PC χρονοπρογραμματίζει τα beacons στο TBTT, αλλά η μετάδοση θα πρέπει να περιμένει έως ότου το κανάλι παραμένει ανενεργό για χρόνο PIFS. Αν το κανάλι είναι κατειλημμένο στο τέλος ενός superframe, το beacon καθυστερεί. Κι επειδή τα πλαίσια δεδομένων στέλνονται κατά το CFP, καθυστερούν και αυτά.

Άλλο ένα πρόβλημα είναι το μεταβλητό μήκος των πλαισίων δεδομένων. Αυτό ποικίλει λόγω των payloads και τις τεχνικές διαμόρφωσης του φυσικού επιπέδου. Για να ξεπεραστούν τα προβλήματα του PCF, η IEEE παρουσίασε την HCF μέθοδο στην τροποποίηση 802.11e για να υποστηρίξει QoS στα WLANs.

Η HCF καθορίζει δύο μεθόδους πρόσβασης: την επεκταμένη κατανεμημένη πρόσβαση στο κανάλι (Enhanced Distributed Channel Access, EDCA) και την HCF ελεγχόμενη πρόσβαση στο κανάλι (HCF Controlled Channel Access, HCCA). Η υπηρεσία (που βασίζεται σε ανταγωνισμό) του HCF βασίζεται στο DCF, ενώ υποστηρίζεται και το PCF για να υποστηριχθούν παλαιότερες συσκευές. Η συσκευή που λειτουργεί με HCF μεταδίδει ένα πλαίσιο κατά τη διάρκεια της ευκαιρίας μετάδοσης (Transmit Opportunity, TXOP). Ένα TXOP εκχωρείται σε μια συσκευή όταν αυτή αποκτά πρόσβαση στο κανάλι. Ο τύπος του TXOP εξαρτάται από τη μέθοδο πρόσβασης στο κανάλι. Ανάλογα με την περίοδο, κατά τη διάρκεια της οποίας λαμβάνονται τα TXOP, αυτά λέγονται αντίστοιχα EDCA-TXOP και HCCA-TXOP.

ΕΠΕΚΤΑΜΕΝΗ ΚΑΤΑΝΕΜΗΜΕΝΗ ΠΡΟΣΒΑΣΗ ΣΤΟ ΚΑΝΑΛΙ (EDCA)

Το EDCA είναι μια βελτίωση στο παρωχημένο DCF παρέχοντας κατά προτεραιότητα best-effort παράδοση των πλαισίων στο ασύρματο κανάλι. Η διαβάθμιση προτεραιοτήτων επιτυγχάνεται με τη χρήση παραμέτρων συντονισμού. Αυτές οι

παράμετροι ελέγχουν την περίοδο ακρόασης του καναλιού από τις συσκευές, το μέγεθος του CW καθώς και τη χρονική διάρκεια κατά την οποία θα μεταδώσουν πλαίσια, αφού έχουν αποκτήσει πρόσβαση στο κανάλι.

Η παράδοση πλαισίων με EDCA βασίζεται στη διαφοροποίηση των προτεραιοτήτων του χρήστη (User Priorities, UPs). Τα UPs είναι ακέραιες τιμές μεταξύ 0 και 7 και αντιστοιχούν στις ετικέτες προτεραιότητας του 802.1D [14][34] (βλ. Πίνακα 6). Το 802.11e αντιστοιχεί τα UPs σε τέσσερις κατηγορίες πρόσβασης (Access Categories, ACs). Τέσσερις διακριτές οντότητες οπισθοχώρησης, μια για κάθε AC λειτουργούν σε κάθε συσκευή. Η προτεραιότητα ενός MSDU καθορίζεται από τις παραμέτρους AC που σχετίζονται με την οντότητα που είναι υπεύθυνη για την παράδοση του MSDU. Κάθε οντότητα υποστηρίζει ανεξάρτητα ένα TXOP. Η ακρόαση του καναλιού γίνεται για χρονική διάρκεια που ονομάζεται Arbitration Inter-Frame Space (AIFS) (βλ. Σχήμα 15). Το AIFS που σχετίζεται ένα συγκεκριμένο AC, το AIFS[AC], υπολογίζεται ως εξής:

$$AIFS[AC] = SIFS + AIFSN[AC] \cdot aSlotTime$$

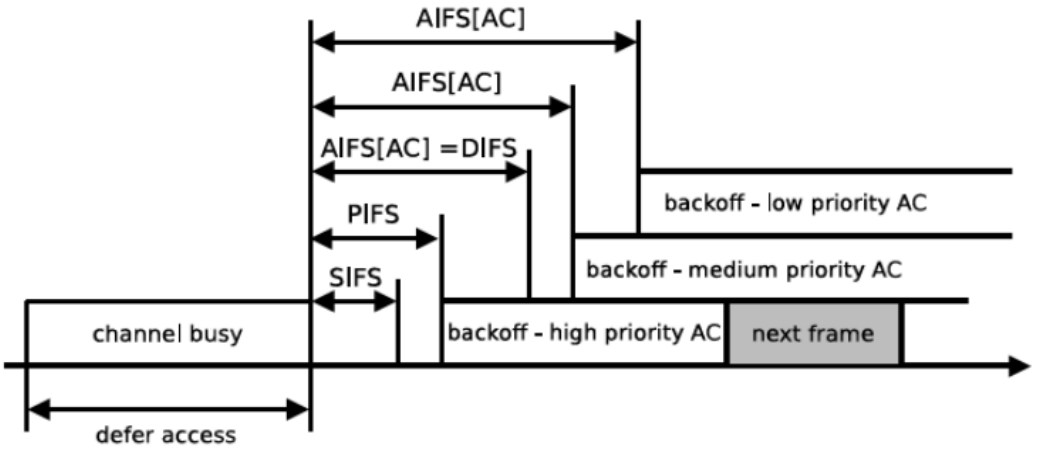
Η ελάχιστη τιμή του AIFS[AC] είναι ίση με το DIFS στο αρχικό πρότυπο 802.11. ο αριθμός AISF (AIFSN) αρχικά έχει τιμή 2 από το HC. Παρόλα αυτά η οντότητα οπισθοχώρησης μπορεί να αυξήσει κατά προτίμηση την τιμή του AIFS[AC] με το να αυξήσει το AIFSN[AC]. Αύξηση στο AISFN[AC] έχει σαν αποτέλεσμα να μειωθεί η προτεραιότητα των MSDUs που στέλνονται από αυτή την οντότητα. Η ελάχιστη και μέγιστη τιμή των CW (CW_{min} και CW_{max} αντίστοιχα) επίσης καθορίζονται από το AC.

Προτεραιότητα	UP	AC	Κατηγορία δικτυακής κίνησης
Χαμηλοτερη	1	AC_BK	background
-	2	AC_BK	Background
-	0	AC_BE	Best-effort
-	3	AC_BE	Best-effort
-	4	AC_VI	Video
-	5	AC_VI	Video
-	6	AC_VO	Voice
υψηλότερη	7	AC_VO	voice

Πίνακας 6. Αντιστοίχιση προτεραιότητας χρήστη σε κατηγορία πρόσβασης

Όσο μικρότερες είναι αυτές οι τιμές, τόσο μεγαλύτερη είναι η προτεραιότητα πρόσβασης στο κανάλι. Το μέγεθος του CW στην i-οστη οπισθοχώρηση είναι:

$$CW_i[AC]=min(2^i\cdot(CW_{min}[AC]+1)-1,CW_{max}[AC])$$



Σχήμα 15. Καθορισμός προτεραιοτήτων στο EDCA

Στο παραπάνω σχήμα, ανατίθενται προτεραιότητες στα πλαίσια σύμφωνα με το AIFS. Μόλις η οντότητα οπισθοχώρησης αποκτά πρόσβαση στο κανάλι, μεταδίδει για χρόνο όσο είναι το TXOP. Τα όρια του TXOP καθορίζονται για κάθε AC και το TXOPlimit[AC] καθορίζει το μέρος της χωρητικότητας του καναλιού που θα έχει η οντότητα. Επιπλέον, το 802.11e επιτρέπει σε μια οντότητα οπισθοχώρησης να μεταδίδει πολλαπλά MSDUs, υπό τον όρο ότι δε θα υπερβει το όριο TXOPlimit[AC].

Τέλος, οι συσκευές 802.11e δύο μετρητές επανάληψης για κάθε AC, το QSRC[AC] και το QLRC[AC], μικρής και μεγάλης διάρκειας αντίστοιχα. Το ποιος μετρητής θα χρησιμοποιηθεί εξαρτάται από το μήκος του MSDU. Για τα AC_VO και AC_VI, οι τιμές των μετρητών επανάληψης είναι χαμηλές γιατί η κίνηση που ανατίθεται σε αυτά τα ACs δε μπορεί να υποστεί μεγάλες καθυστερήσεις. Για τα AC_BK και AC_BE, τα οποία δεν επηρεάζονται στον ίδιο μεγάλο βαθμό από τις καθυστερήσεις, οι τιμές των μετρητών ειναι υψηλότερες.

ΕΛΕΓΧΟΜΕΝΗ ΠΡΟΣΒΑΣΗ ΣΤΟ ΚΑΝΑΛΙ (HCCA)

Η πρόσβαση στο κανάλι με το HCCA ελέγχεται από έναν υβριδικό συντονιστή (Hybrid Coordinator, HC), ο οποίος τρέχει στο access point. Το HCCA είναι παρόμοιο με το PCF υπό την έννοια ότι μοιράζει το κανάλι σε CFP και CP χρονικές περιόδους. Κατά τη CFP χρησιμοποιεί ένα μηχανισμό polling (όπως και το PCF). Η διαφορά είναι ότι η συσκευή που επιλέγεται να μεταδώσει, μεταδίδει για χρονικό διάστημα όσο και το HCCA-TXOP. Το HCCA εκκινεί το CFP ανακοινώνοντας ένα beacon, αφού περιμένει για PIFS. Το HC εκχωρεί χρόνο HCCA-TXOP στις συσκευές από την λίστα που διατηρεί χρησιμοποιώντας ένα πλαίσιο CF-Poll.

Μια συσκευή θα πρέπει να στείλει μια αίτηση κράτησης QoS στο HC ώστε να καταχωρηθεί στη λίστα. Αυτό δημιουργεί μια ροή κίνησης (Traffic Stream, TS) στο HC. Οι παράμετροι προδιαγραφών κίνησης (TSPEC) συμπεριλαμβάνονται στο πλαίσιο διαχείρισης QoS από τη συσκευή. Αυτοί είναι ο μέσος ρυθμός μετάδοσης ρ, το μέγεθος του MSDU σ για την εφαρμογή ([AC]). Αν A είναι η συνάρτηση συνολικής κίνησης, η κίνηση που στέλνεται κατά την περίοδο t−s, όπου t>s, φράζεται από:

$$A(t) - A(s) \leq \rho \cdot (t - s) + \sigma$$

Ο χρονοπρογραμματισμός HC υπολογίζει μια συνάρτηση αποδοχής ελέγχου για να καθορίσει αν είναι διαθέσιμοι αρκετοί πόροι ώστε να διεκπεραιωθεί η αίτηση TSPEC. Για οποιαδήποτε ροή κίνησης k, η συνάρτηση υπολογίζει το πλήθος των MSDUs που φθάνουν σε ένα συγκεκριμένο διάστημα υπηρεσίας (Service Interval, SI) με μέσο ρυθμό:

$$N_k = \left\lceil \frac{SI \cdot \rho_k}{\sigma_k} \right\rceil$$

Το SI έχει την ελάχιστη τιμή των μέγιστων SI όλων των ροών. Η ευκαιρία μετάδοσης $TXOP_k$ δίνεται από:

$$TXOP_k = max\left[\frac{N_k \cdot \sigma_k}{R_k} + O, \frac{\sigma_{max}}{R_i} + O \right]$$

Όπου R_k είναι ο ελάχιστος ρυθμός μετάδοσης για το PHY, σ_{max} το μέγιστο μέγεθος MSDU και O η επιβάρυνση. Το TS είναι αποδεκτό αν:

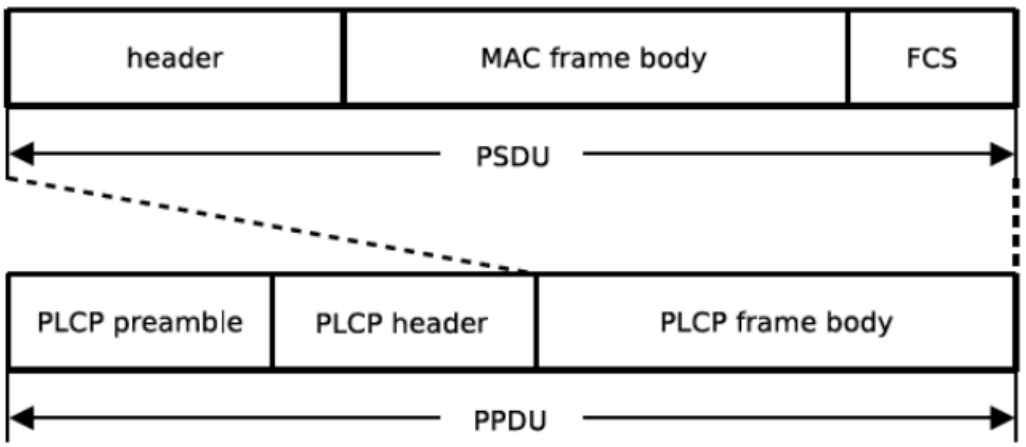
$$\frac{TXOP_{n+1}}{SI} + \sum_{k=1}^{n} \frac{TXOP_k}{SI} \leq \frac{B - T_{CP}}{B}$$

όπου B είναι το διάστημα του beacon και T_{CP} ο χρόνος που αντιστοιχεί σε μετάδοση κατά το CP. Το TXOP εκχωρείται σε μεμονωμένο AC (που αντιστοιχεί σε κάποια

συσκευή) παρά στην ίδια τη συσκευή. Το AC μεταδίδει έως ότου στείλει όλα τα πλαίσια ή λήξει το TXOP. Στο τέλος του CFP ή αν όλες οι συσκευές δεν έχουν άλλα πλαίσια να μεταδώσουν, το HC μεταδίδει ένα πλαίσιο CF-End. Αυτό το πλαίσιο σηματοδοτεί την αρχή του CP.

4. ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ

Το φυσικό επίπεδο του 802.11 διαιρείται σε δύο υποστρώματα: το υπόστρωμα διαδικασίας σύγκλισης φυσικού επιπέδου (Physical Layer Convergence Procedure, PLCP) και το υπόστρωμα εξαρτώμενου φυσικού μέσου (Physical Medium Dependent, PMD). Το PLCP είναι υπεύθυνο για την ενθυλάκωση των MPDUs από το επίπεδο MAC στα πλαίσια, τα οποία μεταδίδονται από μια οντότητα PMD. Το υπόστρωμα PMD είναι υπεύθυνο για την υλοποίηση ενός σχήματος κωδικοποίησης της μετάδοσης. Τα MPDUs αντιστοιχούνται σε δεδομένα υπηρεσίας PLCP (Plcp Service Data Units, PSDUs) τα οποία ενθυλακώνονται στα δεδομένα πρωτοκόλλου PLCP (Plcp Protocol Data Units, PPDUs)(βλ. Σχήμα 16). Το PMD καθορίζει ένα πλήθος από PHYs ώστε να υποστηρίξει πολλαπλά σχήματα διαμόρφωσης. Η δομή των PPDUs ποικίλει ανάλογα με το PHY. Το αρχικό πρότυπο 802.11 καθορίζει τρία PHYs; το FHSS, το



Σχήμα 16. Ενθυλάκωση στο πλαίσιο PPDU

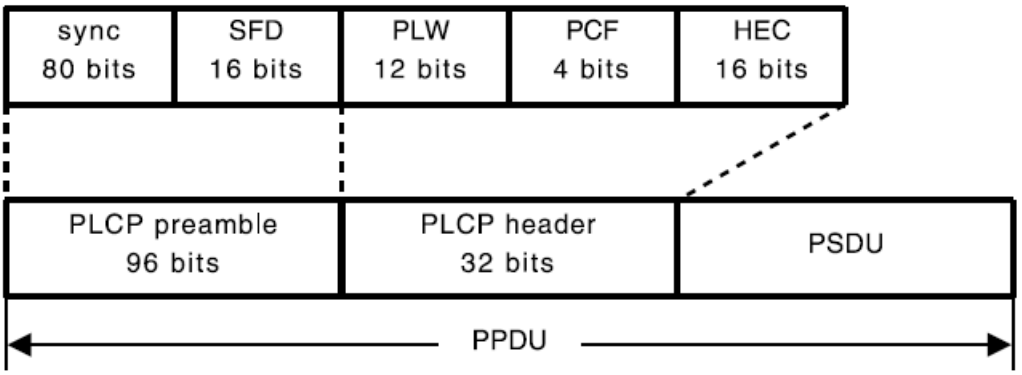
DSSS και το υπέρυθρο (InfraRed, IR) (το οποίο εμπορικά απέτυχε). Το FHSS και το DSSS υποστηρίζουν ρυθμούς μετάδοσης 1 και 2 Mbps. Στην τροποποίηση 802.11b παρουσιάστηκεένα DSSS υψηλού ρυθμού (High Rate DSSS, HR/DSSS), υποστηρίζοντας ταύχητες έως 11 Mbps. Αντί για διασπορά φάσματος, οι τροποποιήσεις 802.11a και 802.11g χρησιμοποιούν οορθογώνια πολυπλεξία με διαίρεση συχνότητας (Orthogonal Frequency Division Multiplexing, OFDM) και υποστηρίζουν ταχύτητες έως 54 Mbps [26][27][28].

Η τροποποίηση 802.11n συνδυάζει μια βελτιωμένη μέθοδο OFDM με τεχνολογία πολλαπλής εισόδου-πολλαπλής εξόδου (Multiple Input-Multiple Output, MIMO) και επιτυγχάνει ρυθμούς έως 600 Mbps [29].

4.1 Frequency Hoping Spread Spectrum (FHSS)

Το FHSS χρησιμοποιεί κλείδωμα μεταλλαγής συχνότητας (Frequency Shift Keying, FSK) για τη διαμόρφωση. Οι συσκευές εκπέμπουν και λαμβάνουν σε μια κοινή συχνότητα για μια μικρή χρονική περίοδο, πριν "μεταπηδήσουν" σε άλλο κανάλι. Αυτή η εναλλαγή από κανάλι σε κανάλι λαμβάνει χώρα με ψευδοτυχαία ακολουθία. Διαφορετικά ζεύγη πομπού/δέκτη χρησιμοποιούν διαφορετική ψευδοτυχαία ακολουθία για να ελαχιστοποιήσουν τον αριθμό των συγκρούσεων στη ζώνη του ίδιου καναλιού. Για να αποφευχθεί η παρεμβολή στενής ζώνης που επηρεάζει μια συγκεκριμένη εναλλαγή αλλά και την επόμενη, οι διαδοχικές εναλλαγές διαχωρίζονται φασματικά κατά 6MHz.

Το Gaussian FSK (GFSK) χρησιμοποιείται για να κωδικοποιήσει την προκύπτουσα διασπορά φάσματος προς μετάδοση. Τα πλεονεκτήματα είναι ότι η κωδικοποίηση αυτή είναι αρκετά ανθεκτική στο θόρυβο, αφού συνήθως ο θόρυβος επηρεάζει το πλάτος του σήματος. Το GFSK δεν είναι όμως φασματικά αποδοτικό για αυτό και οι ρυθμοί μετάδοσης παραμένουν χαμηλοί [16]. Στο παρακάτω σχήμα φαίνεται η δομή του πλαισίου PLCP και περιγράφονται τα πεδία του.



Σχήμα 17. Δομή πλαισίου PLCP για το FHSS

Τα πεδία του πλαισίου είναι τα εξής:

- sync: η ακολουθία εναλλασσόμενων 0 και 1
- SFD (Start Frane Delimiter): δείχνει την αρχή του PSDU χρησιμοποιώντας τη 16-bit δυαδική ακολουθία 0000.1100.1011.1101
- PLW (PSDU Length Word): το μήκος του PSDU σε οκτάδες (bytes)
- PSF (PLCP Signalling Field): καθορίζει τον ρυθμό μετάδοσης του PSDU
- HEC (Header Error Check): τιμή CRC του πλαισίου μήκους 16-bit

4.2 Direct Sequence Spread Spectrum (DSSS)

Το DSSS χρησιμοποιεί κλείδωμα μεταλλαγής φάσης (Phase Shift Keying, PSK) τόσο για τον κώδικα διασποράς όσο και για τη διαμόρφωση του μηνύματος. Ο κώδικας διασποράς είναι μια ψευδοτυχαία ακολουθία θορύβου, η οποία ονομάζεται chip sequence. Επί της ουσίας η chip sequence είναι ένα τραίνο τετραγωνικών παλμών πλάτους +1 ή -1. Μεταξύ της chip sequence και του κάθε bit δεδομένων πριν από τη μετάδοση εφαρμόζεται η λογική πράξη XOR. Το 802.11 χρησιμοποιεί ως κώδικα διασποράς τον κώδικα Barker 11-bit:

$$\{+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1\}$$

όπου το +1 αντιπροσωπεύεται με 1 και το -1 με 0. Καθώς τα σύμβολα στο chip παράγονται με πολύ μεγαλύτερο ρυθμό από ότι τα bits των δεδομένων, η ενέργεια του αρχικού σήματος απλώνεται σε μια ευρύτερη ζώνη συχνοτήτων. Το σήμα που

προκύπτει διαμορφώνεται προς μετάδοση, με χρήση τεχνικών PSK. Κατά το δυαδικό PSK (Binary PSK, BPSK), που είναι η απλούστερη μορφή PSK, ο διαμορφωτής αλλάζει τη φάση του φέροντος f_c ώστε να αντιστοιχίσει το δυαδικό 0 ή 1.

$$s(t)=\begin{cases} A\cos(2\pi f_c t) & 0 \\ A\cos(2\pi f_c t+\pi) & 1 \end{cases}$$

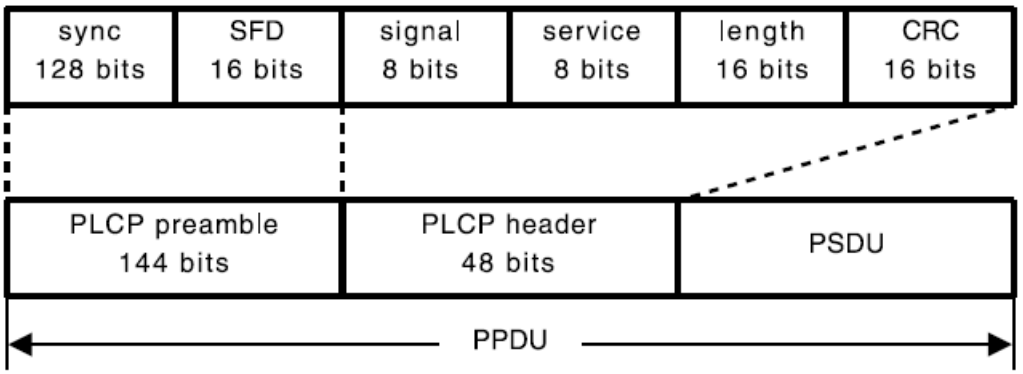
Ένα τετραδικό PSK (Quadratur PSK, QPSK) εκμεταλλεύεται το εύρος ζώνης του καναλιού πιο αποδοτικά. Λαμβάνουν χώρα τέσσερις εναλλαγές φάσεων κι έτσι θα έχουμε:

$$s(t)=\begin{cases} A\cos(2\pi f_c t+\pi/4) & 11 \\ A\cos(2\pi f_c t+3\pi/4) & 01 \\ A\cos(2\pi f_c t-3\pi/4) & 00 \\ A\cos(2\pi f_c t-\pi/4) & 10 \end{cases}$$

Το 802.11b χρησιμοποιεί μεθόδους διαφορικού PSK (Differential PSK, DPSK) και πιο συγκεκριμένα το διαφορικό BPSK (Differential BPSK, DBPSK) και το διαφορικό QPSK (Differential QPSK, DQPSK). Στο PSK η φάση ορίζεται σύμφωνα με την είσοδο. Στο DPSK οι εναλλαγές στη φάση σχετίζονται με την τελευταία τιμή εισόδου [16].

Το πλαίσιο PPDU του DSSS αποτελείται από ένα PLCP preamble, ένα PLCP header ακολουθούμενο από το payload του πλαισίου κι ένα MPDU. Οι μεταγενέστερες του 802.11b τροποποιήσεις αναφέρουν τα DSSS PLCP preamble και header ως long για να ξεχωρίζουν από αυτά του 802.11b (βλ. Σχήμα 18). Τα πεδία είναι τα εξής:

- sync: η ακολουθία εναλλασσόμενων 0 και 1
- SFD (Start Frane Delimiter): δείχνει την αρχή των παραμέτρων PHY μέσα στο preamble
- signal: καθορίζει την τεχνική διαμόρφωσης που χρησιμοποιείται. Για ένα DBPSK 1Mbps, το πεδίο έχει τιμή 10, για DQPSK 2Mbps είναι 20. Στο 802.11b, όπου υποστηρίζονται μεγαλύτεροι ρυθμοί το πεδίο παίρνει τιμή 55 ή 110 για 5,5 και 11 Mbps αντίστοιχα
- service: φυλάσσεται
- length: ο χρόνος μετάδοσης του MPDU σε μsec
- CRC: τιμή του CRC 16bit για έλεγχο σφαλμάτων



Σχήμα 18. Δομή πλαισίου DSSS PPDU Long preamble

4.3 High Rate DSSS (HR/DSSS) [27]

Η τροποποίηση 802.11b παρουσίασε μια επέκταση φυσικού στρώματος υψηλότερης ταχύτητας στη ζώνη των 2,4GHz. Η τεχνική HR/DSSS παρήγαγε πολυ πιο βελτιωμένους ρυθμούς μετάδοσης. Αντί του Barker έχουν τους ακόλουθους κώδικες:

- Συμπληρωματική μεταλλαγή κώδικα (Complementary Code Keying, CCK)
- Συνελικτικη κωδικοποίηση δυαδικών πακέτων (Packet Binary Convolution Coding, PBCC)

Οι CCK και PBCC επιτυγχάνουν ρυθμούς δεδομένων των 5,5 και 11 Mbps. Ο CCK ειναι ένας κώδικας block, όπου τα σύμβολα χωρίζονται σε καθορισμένα blocks και χρησιμοποιούνται σαν κώδικες λέξεις. Η διαμόρφωση CCK βασίζεται στη χρήση των πολυφασικών συμπληρωματικών κωδίκων οι οποίοι είναι αρκετά πολύπλοκοι.

Το υποσύνολο των επιτρεπόμενων κωδικών λέξεων είναι μικρότερο από το σύνολο όλων των πιθανών λέξεων. Οι συμπληρωματικοί κώδικες είναι σύμβολα με επιθυμητά στοιχεία συσχετισμού. Η ληφθείσα κωδική λέξη συγκρίνεται με το σύνολο των έγκυρων κωδικών λέξεων. Αν είναι πολύ κοντά σε κάποια έγκυρη λέξη τότε αυτή επιλέγεται για να αποσταλεί. Με αυτό τον τρόπο μια κωδική λέξη με σφάλματα μπορεί να ανακτηθεί στο δέκτη. Ο CCK χρησιμοποιεί μήκος συμβόλου από 8 πολύπλοκα chips και η κωδική λέξη C υπολογίζεται από τη σχέση [8]:

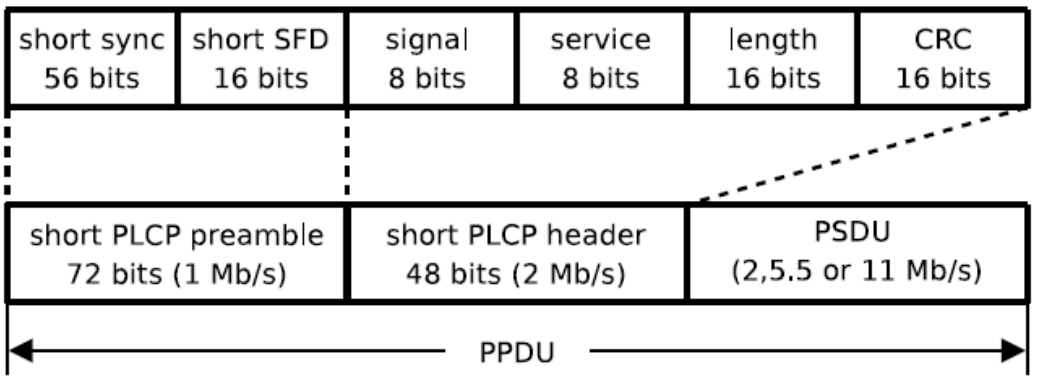
$$C = \begin{cases} e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, \\ e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, e^{j(\varphi_1+\varphi_3)}, e^{j(\varphi_1+\varphi_2)}, e^{j(\varphi_1)} \end{cases}$$

Οι όροι ϕ_1, ϕ_2, ϕ_3 και ϕ_4 επιλέγονται σύμφωνα με το ρυθμό μετάδοσης (5,5 ή 11Mbps). Έξι bits από τα 8 χρησιμοποιούνται για να κωδικοποιήσουν τον πολυφασικό συμπληρωματικό κώδικα κλειδί. Η κωδική λέξη ύστερα περιστρέφεται κατά 0, π/2, π ή 3π/4 σύμφωνα με τα εναπομείναντα δύο two bits.

Αν το κανάλι λόγω συνθηκών δε μπορεί να υποστηρίξει υψηλούς ρυθμούς μετάδοσης τότε μια συσκευή μπορεί να ελαττώσει την ταχύτητα μετάδοσης σε 1 ή 2Mbps χρησιμοποιώντας το DSSS PHY του αρχικού προτύπου 802.11 [9].

Το PBCC βασίζεται σε συνελικτικούς κώδικες. Κάθε bit εισόδου υπόκειται σε επεξεργασία από μια σειρά από καταχωρητές ολίσθησης και προσθέσεις modulo-2. Ο κωδικοποιητής παράγει δύο ψηφία στην έξοδο τα οποία αποθηκεύονται στους καταχωρητές.

Όπως προαναφέραμε. στο 802.11b υποστηρίζονται δύο τύποι preamble/header, ο long και ο short (βλ. Σχήμα 19). Τα long preamble/header είναι ίδια για το DSSS των 1 και 2 Mbps, όπως αυτά καθορίζονται από το αρχικό πρότυπο.



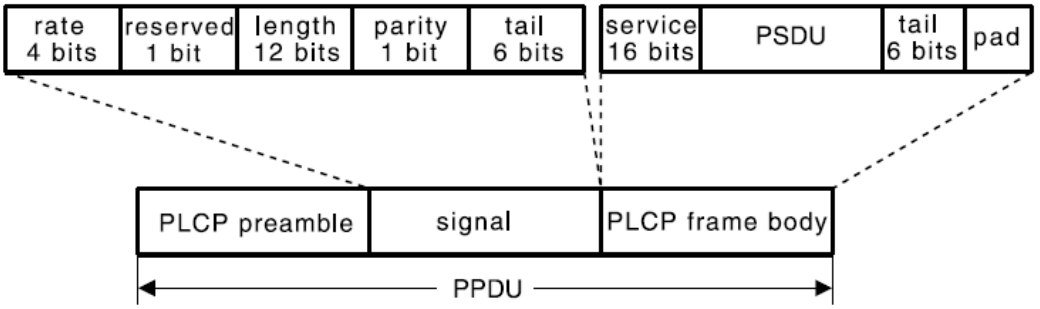
Σχήμα 19. Δομή πλαισίου DSSS PPDU Short preamble

4.4 Orthogonal Frequency Division Multiplexing (OFDM)

Το 802.11a PHY ορίζει το OFDM ως το σχήμα διαμόρφωσης που χρησιμοποιεί [10][11][12]. Το OFDM χρησιμοποιείται και σε άλλες ασύρματες τεχνολογίες όπως το HiperLAN/2 ή το IEEE 802.16 (WiMAX). Επίσης χρησιμοποιείται

στην ψηφιακή μετάδοση ήχου (Digital Audio Broadcasting, DAB), στην ψηφιακή μετάδοση βίντεο (Digital Video Broadcasting, DVB) και στην ασύμμετρη ψηφιακή συνδρομητική γραμμή (Asynchronous Digital Subscriber Line, ADSL).

Το OFDM μεταδίδει δυαδικό σήμα με υψηλό ρυθμό πάνω από χαμηλού ρυθμού υποφέροντα. Στο 802.11a υπάρχουν συνολικά 52 υποφέροντα, 48 από τα οποία είναι για δεδομένα ενώ τα υπόλοιπα 4 είναι οδηγοί. Η δομή του πλαισίου PLCP για το 802.11a φαίνεται στο παρακάτω σχήμα.



Σχήμα 20. Δομή πλαισίου PLCP για το OFDM στο 802.11a

Τα bits του PPDU είναι κωδικοποιημένα με ένα συνελικτικό κώδικα. Αυτά είναι αναδιατεταγμένα και παρεμβαλλόμενα και έπειτα μοιράζονται ανάμεσα στα υποφέροντα. Στα υποφέροντα εφαρμόζεται ένας αντίστροφος ταχύς μετασχηματισμός Fourier και μεταδίδονται. Η διαμόρφωση των σημάτων των υποφερόντων γίνεται χρησιμοποιώντας μία από τις τέσσερις μεθόδους διαμόρφωσης: BPSK, QPSK, 16-QAM ή 64-QAM. Οι ανελικτικοί κώδικες χρησιμοποιούνται για να εξαλείψουν τα σφάλματα. Οι συσκευές 802.11a μπορούν να μεταδίδουν με ταχύτητες των 6, 9, 12, 18, 24, 36, 48 ή 54 Mbps, ανάλογα με το σχήμα διαμόρφωσης και τον ανελικτικό κώδικα.

Παραδοσιακά, η πολυπλεξία διαίρεσης συχνότητας χρησιμοποιεί ζώνες φύλαξης μεταξύ των καναλιών για να καταπολεμήσει την διακαναλική παρεμβολή. Παρόλα αυτά, με το OFDM τα υποφέροντα επικαλύπτονται. Όμως, είναι η ορθογώνια ιδιότητα των διαμορφωμένων υποφερόντων αυτή που εξασφαλίζει ότι τα διπλανά σήματα δεν θα παρεμβληθούν το ένα στο άλλο. Τα υποφέροντα, που συχνά λέγονται και τόνοι, είναι ημιτονοειδής μορφές και αποτελούν ιδιοσυναρτήσεις ενός γραμμικού καναλιού. Αυτή η ιδιότητα δεν χάνεται λόγω της

φύσης ενός καναλιού να προκαλεί διασπορά. Προκαλεί όμως διαφεροντική παρεμβολή (Inter-Carrier Interference, ICI). Επιπρόσθετα, μπορεί να προκαλέσει διασυμβολική παρεμβολή (Inter-Symbol Interference, ISI) μεταξύ διαδοχικών συμβόλων του OFDM. Το ISI αποφεύγεται με την εισαγωγή διαστημάτων φύλαξης (Guard Interval, GI) ανάμεσα στα διαδοχικά σύμβολα. Από την άλλη πλευρά, αυτά τα διαστήματα προκαλούν απώλεια της ορθογωνιότητας. Η προσθήκη ενός κυκλικού προθέματος διατηρεί την ορθογωνιότητα των υποφερόντων και αποτρέπει το ISI. Για να δημιουργηθεί το κενό μεταξύ των συμβόλων, μέρος του σήματος αντιγράφεται στην αρχή των συμβόλων OFDM [16].

4.5 Extended Rate PHY (ERP) [28]

Το 802.11g, παρόμοια με το 802.11a, υποστηρίζει ρυθμούς έως 54Mbps χρησιμοποιώντας PHY εκτεταμένου ρυθμού (Extended Rate PHY, ERP). Όμως, διαφορετικά από το 802.11a, το 802.11g λειτουργεί στη ζώνη των 2,4GHz όπως και το 802.11b. Για να υπάρχει συμβατότητα μεταξύ των συσκευών 802.11g και εκείνων που λειτουργούν σε παλαιότερα πρότυπα, το 802.11g καθορίζει ένα πλήθος από PHYs, τα οποία φαίνονται στον παρακάτω πίνακα.

PHY	Ρυθμός δεδομένων	χρήση
ERP-OFDM	≤54Mbps	Υποχρεωτική
ERP-DSSS/CCK	1, 2, 5.5, 11Mbps	Υποχρεωτική
DSSS-OFDM	≤54Mbps	Προαιρετική
ERP-PBCC	22, 33Mbps	Προαιρετική

Πίνακας 7. Τα PHYs του 802.11g

Το ERP-CCK/DSSS χρησιμοποιείται όταν μια συσκευή 802.11g επικοινωνεί με μια 802.11b. Χρησιμοποιεί DSSS για 1 και 2Mbps και CCK για 5,5 και 11Mbps, ουσιαστικά δηλαδή "μετατρέπεται" σε μια 802.11b συσκευη. Το ERP-OFDM είναι το ίδιο με το OFDM στο 802.11a, αλλά προσαρμοσμένο για τη ζώνη των 2,4GHz. Η δομή του PPDU είναι ίδια με του 802.11a. Όταν δύο συσκευές 802.11g

επικοινωνούν, χρησιμοποιούν το ERP-OFDM. Όμως όταν υπάρχουν άλλες συσκευές 802.11b, αυτές δε μπορούν να ανιχνεύσουν τα σήματα ERP-OFDM και δε μπορούν να καταλάβουν αν το κανάλι είναι δεσμευμένο. Για αυτό το λόγο όταν το 802.11g χρησιμοποιεί το ERP-OFDM, ενημερώνει το NAV για συσκευές που δεν υποστηρίζουν το ERP στέλνοντας RTS/CTS πλαίσια χρησιμοποιώντας DSSS ή CCK διαμόρφωση.

Το 802.11g καθορίζει δύο προαιρετικά PHYs: το DSSS-OFDM και ERP-PBCC. Το DSSS-OFDM είναι ένα υβριδικό σχήμα διαμόρφωσης κατά το οποίο το DSSS διαμορφώνει τα preamble/header του πλαισίου και το OFDM το payload. Το DSSS-OFDM δεν έχει ανάγκη να υλοποιήσει κάποιο μηχανισμό προστασίας, για αυτό και δεν προηγούνται των πλαισίων δεδομένων RTS/CTS πλαίσια. Το ERP-PBCC είναι σχήμα διαμόρφωσης ενός φέροντος που κωδικοποιεί το payload με έναν 256αδικό PBCC. Επιτυγχάνει ρυθμούς των 22 και 33Mbps [28].

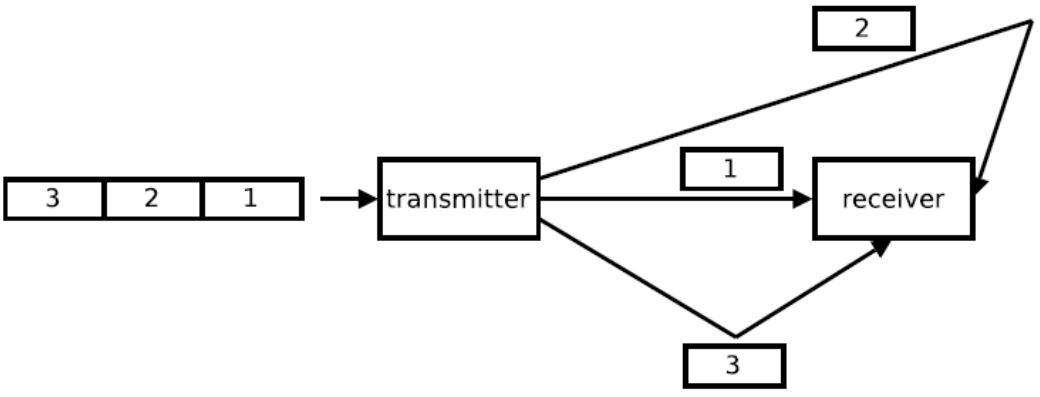
4.6 MIMO-OFDM [29]

Το 802.11n χρησιμοποιεί το PHY MIMO-OFDM και υποστηρίζει ρυθμούς δεδομένων έως 300Mbps. Εκτός από το PHY, υπάρχουν βελτιώσεις αποδοτικότητας στο MAC, όπως η συνάθροιση πλαισίου (frame aggregation) και επιβεβαιώσεις block. Το PHY του 802.11n βασίζεται πολύ στην τεχνολογία MIMO για να επιτύχει τους γνωστούς υψηλούς ρυθμούς μεταφοράς δεδομένων. Τα συστήματα MIMO αποτελούνται από πολλαπλές κεραίες και ζεύξεις στον πομπό και στο δέκτη. Το πλήθος των κεραιών/ζεύξεων στον πομπό (n_T) δεν απαιτείται να είναι το ίδιο με αυτό του δέκτη (n_R). Η τεχνολογία MIMO είναι συμβαλλόμενη στα OFDM συστήματα, τα οποία μεταδίδουν σήαμτα σε πολλαπλά κανάλια στενής ζώνης. Ως εκ τούτου το MIMO-OFDM είναι ένας πολλά υποσχόμενος τομέας έρευνας για παροχή υψηλών ταχυτήτων σε ασύρματες υποδομές.

Τα συστήματα MIMO προσφέρουν αυτούς τους ρυθμούς γιατί υλοποιούν χωρική διαφορετικότητα και χωρική πολυπλεξία. Η χωρική διαφορετικότητα υπάρχει τόσο από την πλευρά του πομπού όσο και του δέκτη. Κατά τη λήψη, δύο ή

περισσότερες κεραίες διαχωρίζονται χωρικά, έτσι ώστε να λαμβάνουν μη-συσχετισμένα σήματα, τα οποία έχουν ακολουθήσει ανεξάρτητα μονοπάτια. Η κεραία με το καλύτερο σήμα επιλέγεται για επεξεργασία από τη ζεύξη. Αυτό ονομάζεται switched diversity. Ο συνδυαστής μεγίστου λόγου (Maximal Ratio Combining, MRC) είναι μια πιο ανώτερη μέθοδος διαφορισμού στη λήψη. Με το MRC, χρησιμοποιούνται ανώτερες μέθοδοι ψηφιακής επεξεργασίας σήματος για να συνδυάσουν τα ξεχωριστά σήματα σε ένα ενιαίο, υψηλότερης ποιότητας σήμα για καλύτερη απολαβή. Για αυτή τη μέθοδο απαιτούνται πολλαπλές RF ζεύξεις.

Μέθοδοι διαφορισμού στη λήψη χρησιμοποιούνται εδώ και καιρό από συσκευές που λειτουργούν σε πρότυπα προγενέστερα του 802.11n (802.11a/b/g). Αντίθετα, η εφαρμογή του διαφορισμού στην εκπομπή είναι πιο πρόσφατη. Μια απλή προσέγγιση είναι να μεταδίδει η κεραία που έχει το καλύτερο σήμα προς το δέκτη. Αυτό εμπεριέχει γνώση από το δέκτη του περιβάλλοντος του καναλιού. Μια πιο περίπλοκη μέθοδος διαφορισμού εκπομπής είναι ο περιορισμός της εξασθένισης μέσω της αποστολής πολλαπλών σημάτων. Η εκπεμπόμενη ροή bit κωδικοποιείται στο χωρικά και χρονικά. Οι κώδικες χώρου-χρόνου (Space-Time Codes, STC) χρησιμοποιούνται για την αποστολή αντιγράφων των σημάτων, τα οποία μπορούν να επανασυνδυαστούν στο δέκτη. Η πολυπλεξία χώρου εκμεταλλεύεται συνθήκες πολλαπλών μονοπατιών για την αποστολή παράλληλων ροών δεδομένων (βλ. Σχήμα 21). Ένα σήμα υψηλού ρυθμού διαιρείται σε ροές σημάτων δεδομένων χαμηλότερου ρυθμού, τα οποία μεταδίδονται ταυτόχρονα στην ίδια ζώνη συχνοτήτων. Ο δέκτης μπορεί να αποκωδικοποιήσει αυτές τις ροές υπό την προϋπόθεση ότι φτάνουν στην διάταξη κεραιών με επαρκή χωρικό διαχωρισμό.



Σχήμα 21. Χωρική πολυπλεξία

Ενώ το MIMO υπόσχεται βελτιωμένη κάλυψη, εμβέλεια και απόδοση, επιφέρει και αντίστοιχη αύξηση πολυπλοκότητας και κόστους. Οι κεραίες μπορεί να είναι φθηνές και το κόστος για DSP να μειώνεται, αλλά ο νόμος του Moore δεν εφαρμόζεται σε συσκευές που σχετίζονται με ραδιοσυχνότητες. Για αυτό το λόγο, έχει γίνει σημαντική έρευνα σε σχήματα υβριδικής επιλογής. Με την υβριδική επιλογή επιλέγονται L από K κεραίες για επεξεργασία. Παρόλο που υπάρχει μείωση της απόδοσης συγκριτικά με τα συστήματα K×K, είναι σημαντική και η μείωση του κόστους.

Το 802.11n καθορίζει ένα πλήθος από βελτιώσεις στο OFDM. Ο αριθμός των υποφερόντων αυξήθηκε στα 56, εκ των οποίων τα 4 χρησιμοποιούνται για σηματοδοσία. Αυτό από μόνο του επιφέρει μια αύξηση του ρυθμού μετάδοσης κατά 20% σε σχέση με τα 802.11a/g (χρησιμοποιούν 52 υποφέροντα μείον 4 για σηματοδοσία). Όταν έχουμε συνδυασμό καναλιών (channel bonding), χρησιμοποιούνται 114 υποφέροντα (6 για σηματοδοσία). Όπως προαναφέραμε, το OFDM χρησιμοποιεί GI για να προστατευτεί από το ISI. Στα 802.11a/g, το GI είναι 800 nsec, ενώ στο 802.11n είναι 400 nsec. Αυτό επιφέρει αύξηση του ρυθμού συμβόλων κατά 10%. Το 802.11n μπορεί να μεταδίδει σε ένα κανάλι εύρους ζώνης είτε 20MHz είτε 40MHz. Αυτό το χαρακτηριστικό που επιτρέπει κανάλια των 40MHz ονομάζεται συνδυασμός καναλιών (channel bonding). Το τίμημα είναι στον αριθμό των επικαλυπτόμενων καναλιών που μπορούν να συνυπάρχουν. Στη ζώνη των 2,4GHz, υπάρχει μόνο μια χωρητικότητα για ένα μη επικαλυπτόμενο κανάλι των 40MHz (συν ένα των 20MHz). Η ζώνη των 5GHz είναι ευρύτερη μπορεί να υποστηρίξει πολλαπλά κανάλια των 40MHz. Έτσι το channel bonding χρησιμοποιείται σε αυτή τη ζώνη συνήθως.

Όπως και με τις προηγούμενες τροποποιήσεις, έτσι και το 802.11n θα πρέπει να υποστηρίξει επικοινωνία με συσκευές παλαιότερων πρωτοκόλλων. Δεδομένου ότι λειτουργεί και στα 2,4GHz και στα 5GHz, μπορεί να επικοινωνεί με συσκευές 802.11b/g και 802.11a. χρησιμοποιούνται τα preambles/headers που ορίζονται από τα παλαιότερα πρότυπα ώστε οι συσκευές 802.11a/b/g να μπορούν να ανιχνεύσουν τα πλαίσια του 802.11n. Κάτω από ορισμένες συνθήκες αυτό μπορεί να αποτελέσει

πρόβλημα. Όταν μεταδίδεται ένα 802.11n payload, η αλλαγή της ισχύος λόγω του MIMO και του beamforming ενδέχεται να προκαλέσει επαναφορά της τιμής του NAV στις παλαιότερες συσκευές. Για αυτό το λόγο τα τερματικά 802.11n συνήθως χρησιμοποιούν το μηχανισμό RTS/CTS.

4.7 BEAMFORMING

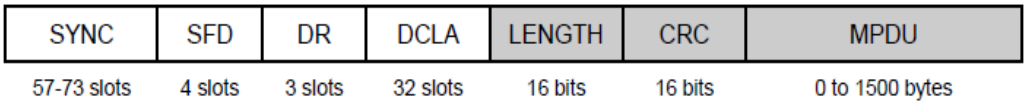
Το beamforming είναι μια μέθοδος για την δημιουργία κατευθυντικής αποστολής/λήψης σήματος χρησιμοποιώντας τεχνικές επεξεργασίας σήματος και διατάξεις αισθητήρων. Η κατευθυντικότητα λήψης μιας συστοιχίας μπορεί να αλλαχθεί με ανάλυση των παρεμβολών που δημιουργούνται από την άφιξη πολλαπλών σημάτων στη συστοιχία. η φάση και το πλάτος του σήματος ελέγχεται από τον beamformer έτσι ώστε το πρότυπο του σήματος να παρεμβάλλεται θετικά προς την κατεύθυνση του δέκτη και αρνητικά προς όλες τις άλλες κατευθύνσεις. Το beamforming είναι προαιρετικό στοιχείο του 802.11n.

Το beamforming δε μπορεί να χρησιμοποιηθεί σε συνδυασμό με τις τεχνικές MIMO. Για παράδειγμα, η χωρική πολυπλεξία βασίζεται στο "πλούσιο" από σήματα περιβάλλον, ενώ στην περίπτωση του beamforming παράγεται ένα και μοναδικό σύμφωνο RF σήμα προς την κατεύθυνση του δέκτη [41].

4.8 INFRARED (IR) [25]

Το υπέρυθρο (InfraRed, IR) PHY στρώμα χρησιμοποιεί για μετάδοση οπτικό σήμα μήκους κύματος 850nm και 950 nm. Η διαφορά του 802.11 IR με το IrDA είναι ότι πομπός και δέκτης δε χρειάζεται να βρίσκονται σε LoS (η λεγόμενη και diffused infrared). Το IR έχει σημαντικούς περιορισμούς όσον αφορά τη χρήση του. Ένας από αυτούς είναι ότι η απόσταση επικοινωνίας μεταξύ πομπού και δέκτη δεν πρέπει ξεπερνάει θεωρητικά τα 20 μέτρα, πρακτικά να είναι το πολύ 10 μέτρα, ενώ μπορεί

να μειωθεί κι άλλο αν δεν υπάρχουν επιφάνειες ανάκλασης. Ένας άλλος περιορισμός είναι ότι η χρήση του γίνεται στα όρια του εσωτερικού χώρου, αφού τα υπέρυθρα σήματα δε μπορούν να διαπεράσουν τους τοίχους. Η δομή του πλαισίου PLCP φαίνεται στο παρακάτω σχήμα.



Σχήμα 22. Δομή πλαισίου IR PPDU

Το PLCP Preamble επιτρέπει σε πομπό και δέκτη να συγχρονιστούν έως ότου φτάσει το υπόλοιπο πλαίσιο με τα δεδομένα. Αποτελείται από τα παρακάτω πεδία:

- SYNC: χρησιμοποιείται για το συγχρονισμό του δέκτη. Αντίθετα με τα PHY που περιγράφθηκαν στις προηγούμενες παραγράφους, είναι μεταβλητό με μήκος που κυμαίνεται μεταξύ 57 και 73 χρονοσχισμών.
- SFD: σηματοδοτεί την έναρξη του πλαισίου. Η τιμή αυτού του πεδίου είναι πάντα 1001 (μοναδική τιμή για το IR PLCP). Το 1 αντιστοιχεί σε παλμό και το 0 σε απουσία παλμού.

Η επικεφαλίδα παρέχει πληροφορίες για το πλαίσιο που ακολουθεί και αποτελείται από τα παρακάτω πεδία:

- DR (Data Rate): ο ρυθμός μετάδοσης του πλαισίου. Το IR προσφέρει 1 και 2Mbps και το πεδίο παίρνει αντίστοιχα τις τιμές 000 και 001. (το preamble και το header στέλνονται πάντα με ρυθμό 1Mbps)
- DCLA (DC Level Adjustment): δίνεται η δυνατότητα στο δέκτη να σταθεροποιήσει το επίπεδο DC του ληφθέντος σήματος. Για ρυθμό 1Mbps έχει τιμή 00000000100000000000000010000000, ενώ για ρυθμό 2Mbps έχει τιμή 00100010001000100010001000100010
- Length: το μήκος του πλαισίου σε bytes
- CRC: ο κώδικας ανίχνευσης σφαλμάτων είναι ο CRC-16

Η ευθύνη του PMD είναι να μετατρέψει τα bits του PPDU σε ηλεκτρικό σήμα κατάλληλο για μετάδοση. Όπως προαναφέρθηκε, το 802.11 IR λειτουργεί χωρίς να υπάρχει απαίτηση LoS μεταξύ πομπού και δέκτη. Αυτό είναι εφικτό διότι το σήμα φτάνει στο δέκτη ύστερα από ανακλάσεις. Αυτός ο τρόπος μετάδοσης ονομάζεται μετάδοση διαχεόμενου υπέρυθρου φωτός (Diffused Infrared Transmission).

Η μέγιστη τιμή ισχύος για το μεταδιδόμενο σήμα δεν ξεπερνά τα 2Watt που αγγίζει η ισχύς του μεταδιδόμενου σήματος δεν ξεπερνάει τα δύο watt, ενώ η συχνότητα του εκπεμπόμενου σήματος δεν υπόκειται σε κάποιο περιορισμό.

Το 802.11 IR μεταδίδει δεδομένα με ρυθμούς 1 ή 2Mbps και χρησιμοποιεί ξεχωριστό τύπο διαμόρφωσης για το καθένα. Χρησιμοποιείται η διαμόρφωση θέσης παλμού (Pulse Position Modulation, PPM). Είναι γνωστό ότι ο θόρυβος επιδρά στο πλάτος του σήματος κι όχι στη φάση του. Άρα είναι εύκολα κατανοητό ότι η διαμόρφωση PPM περιορίζει τις παρεμβολές που προκαλεί ο θόρυβος. Η λογική λειτουργίας του PPM είναι να αλλάζει την θέση του παλμού και με αυτό τον τρόπο να αντιπροσωπεύει τα διαφορετικά δυαδικά σύμβολα.

Για ρυθμό μετάδοσης 1Mbps υλοποιείται η διαμόρφωση PPM 16 συμβόλων (16-PPM) αντιστοιχίζει κάθε 4-bit ακολουθία σε μία αναπαράσταση των 16 bit (16 PPM Symbol), η οποία περιέχει δεκαπέντε μηδενικά και μοναδικό ένα και απεικονίζεται στον παρακάτω πίνακα.

bits δεδομένων	Σύμβολα 16-PPM
0000	0000000000000001
0001	0000000000000010
0011	0000000000000100
0010	0000000000001000
0110	0000000000010000
0111	0000000000100000
0101	0000000001000000
0100	0000000010000000
1100	0000000100000000
1101	0000001000000000
1111	0000010000000000
1110	0000100000000000
1010	0001000000000000
1011	0010000000000000
1001	0100000000000000
1000	1000000000000000

Πίνακας 8. Η διαμόρφωση 16-PPM

Για ρυθμό μετάδοσης 2Mbps χρησιμοποιείται η διαμόρφωση 4-PPM, αντιστοιχίζοντας κάθε ζεύγος bit σε τετράδες που έχουν τρία μηδενικά και μοναδικό ένα, όπως φαίνεται στον παρακάτω πίνακα.

Bits δεδομένων	Σύμβολα 4-PPM
00	0001
01	0010
11	0100
10	1000

Πίνακας 9. Η διαμόρφωση 4-PPM

5. ΑΣΦΑΛΕΙΑ [23]

Το αρχικό 802.11 δεν καθορίζει κάποιες μεθόδους ασφάλειας. Κάποιοι κατασκευαστές παρείχαν πιστοποίηση βασισμένη στις διευθύνσεις MAC, κατά την οποία τα access points διατηρούσαν λίστες από διευθύνσεις MAC των συσκευών

που επιτρέπονταν να συνδεθούν με αυτά. Αυτή η μέθοδος όμως υστερεί σε επεκτασιμότητα, αφού η διατήρηση και ενημέρωση αυτών των λιστών είναι επίπονη διαδικασία, ειδικά όταν τα τερματικά είναι πολλά. Επιπλέον, οι διευθύνσεις MAC μπορούν εύκολα να εξαπατηθούν. Το WEP παρουσιάστηκε στην τροποποίηση 802.11b, αλλά έδειξε κι αυτό αρκετές σοβαρές αδυναμίες.

Για να ξεπεραστούν όλα αυτά τα μειονεκτήματα παρουσιάστηκε η τροποποίηση 802.11i [32] (βλ. Σχήμα 22). Ο σκοπός του 802.11i ήταν να υλοποιήσει ένα Robust Security Network Association (RSNA) σχεδιασμένο να βελτιώσει τα παρακάτω χαρακτηριστικά:

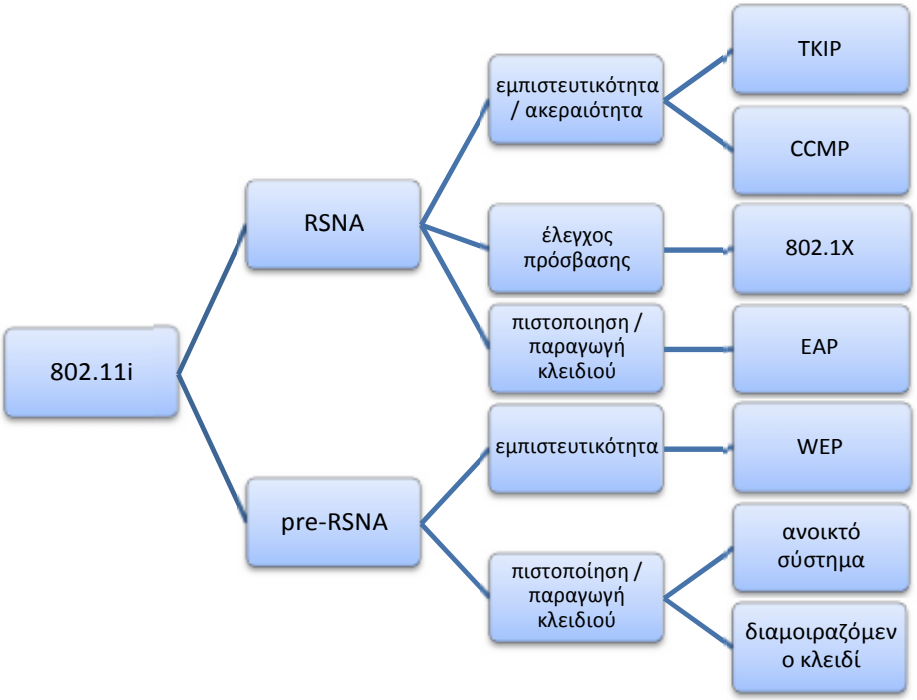
- Πιστοποίηση (authentication)
- Διαχείριση κλειδιού (key management)
- Εμπιστευτικότητα και ακεραιότητα (confidentiality, integrity)

Το WiFi Alliance παρουσίασε μια ενδιάμεση λύση ως προς το WEP, το WiFi Protected Access (WPA). Ο στόχος του WPA ήταν να αντιμετωπίσει κάποιες αδυναμίες του WEP, ενώσο το 802.11i ετοιμαζόταν να επικυρωθεί (το WPA παρουσιάστηκε σε draft έκδοση του 802.11i). Το πρότυπο 802.11i περιλαμβάνει αλγόριθμους προγενέστερους του RSNA (pre-RSNA). Όταν επικυρώθηκε το 802.11i, το WiFi Alliance εξέδωσε το WPA2.

5.1 Pre-RSNA [27]

Οι αλγόριθμοι pre-RSNA πηγάζουν από το WEP, το οποίο αρχικά παρουσιάστηκε στο 802.11b. Το WEP είχε σκοπό να παράσχει εμπιστευτικότητα, ακεραιότητα και πιστοποίηση. Όσον αφορά την εμπιστευτικότητα, αυτή θα υποστηριζόταν από τη χρήση του RC4 για την κωδικοποίηση. Όσον αφορά την ακεραιότητα των δεδομένων, αυτή θα βασιζόταν στη χρήση 32bit ελέγχου κυκλικού πλεονασμού (Cyclic Redundancy Check, CRC). Αναφορικά με την πιστοποίηση, αυτή στηρίχθηκε σε δύο μεθόδους: ανοικτό σύστημα (Open System) και διαμοιραζόμενο κλειδι (shared key). Όλοι οι pre-RSNA αλγόριθμοι δεν έτυχαν και της καλύτερης

υποδοχής, με εξαίρεση την πιστοποίηση ανοικτού συστήματος. Το "¨παράδοξο" είναι ότι το WEP και το διαμοιραζόμενο κλειδί ακόμα έχουν ευρεία χρήση.



Σχήμα 22. Η ασφάλεια του 802.11i

ΠΙΣΤΟΠΟΙΗΣΗ

Με το ανοικτό σύστημα, η πιστοποίηση λαμβάνει χώρα κατά την μετάδοση δύο μηνυμάτων. Έστω δύο ασύρματα τερματικά, το Α και το Β. Το Α βεβαιώνει την ταυτότητά του στο Β στέλνοντάς του μια αίτηση πιστοποίησης. Το Β απαντά με μήνυμα "επιτυχία" ή "αποτυχία". Αν οι αίτηση είναι επιτυχής τότε τα Α, Β πιστοποιούνται αμοιβαία. Μιας και δεν υπάρχουν όμως κάποια κριτήρια αυθεντικότητας τότε η απάντηση θα είναι "επιτυχία". Θα μπορούσε να χρησιμοποιηθεί πιστοποίηση βασισμένη στη διεύθυνση MAC, δηλαδή αν η διεύθυνση MAC του τερματικού δεν συμπεριλαμβάνεται στη λίστα πρόσβασης του access point, τότε η απάντηση στην αίτηση θα είναι αποτυχία. Παρόλα αυτά, στο πρότυπο δεν περιγράφεται μια τέτοιου είδους πιστοποίηση και υλοποιείται μόνο από κατασκευαστές υλικού.

Με την πιστοποίηση διαμοιραζόμενου κλειδιού, πιστοποιούνται επιτυχώς μόνο οι συσκευές που έχουν το διαμοιραζόμενο κλειδί. Τα διαμοιραζόμενα κλειδιά

διανέμονται μεταξύ των συσκευών μέσω κάποιας διαδικασίας που δεν καθορίζεται από το πρότυπο, π.χ. ο διαχειριστής δικτύου μπορεί να είναι ένας υπεύθυνος για αυτή τη διανομή. Η πιστοποίηση λοιπόν ολοκληρώνεται έπειτα από μια διαδικασία (χειραψία) τεσσάρων βημάτων. Για το παραπάνω σενάριο, το Α στέλνει μια αίτηση πιστοποίησης στο Β (1ο βήμα). Το Β παράγει ένα 1024bit ψευδοτυχαίο αριθμό και τον στέλνει στον Α (2ο βήμα). Το Α κωδικοποιεί αυτόν τον αριθμό με τον RC4 με τρόπο παρόμοιο με αυτόν που κωδικοποιεί και τα πλαίσια δεδομένων και στέλνει το αποτέλεσμα στο Β (3ο βήμα). Όταν το Β το λάβει, ελέγχει την τιμή ελέγχου ακεραιότητας (Integrity Check Value, ICV). Αν το ICV είναι σωστό, τότε ενημερώνει το Α για αυτή την επαλήθευση με ένα μήνυμα "επιτυχία" (4ο βήμα). Αλλιώς, το Β απαντά με μήνυμα "αποτυχία".

Το ίδιο διαμοιραζόμενο κλειδί χρησιμοποιείται και για την κωδικοποίηση του μηνύματος. Το κλειδί Κ μπορεί να ανακτηθεί αν τα bits του αρχικού κειμένου γίνουν XOR με αυτά του κρυπτογραφημένου. Προφανώς, το διαμοιραζόμενο κλειδί είναι περισσότερο εκτεθειμένο κατά τη φάση της πιστοποίησης γιατί το κείμενο και η κρυπτογραφημένη απάντηση μεταδίδονται στο δίκτυο. Οπότε η εμπιστευτικότητα τίθεται σε κίνδυνο. Διαισθητικά θα σκεφτόταν κανείς ότι η μέθοδος διαμοιραζόμενου κλειδιού θα είναι ασφαλέστερη, όμως ισχύει το αντίθετο. Το αδύνατο σημείο είναι ότι το κλειδί ειναι συνήθως το ίδιο αφού για την αλλαγή του, υπεύθυνος είναι κάποιος χρήστης ο οποίος συνήθως αδιαφορεί. Το διάνυσμα αρχικοποίησης (Initialisation Vector, IV) έχει μήκος μόλις 24bits, κάτι το οποίο θεωρείται πολύ μικρό. Σε ένα αρκετά φορτωμένο με κίνηση δίκτυο, το πλαίσια με το ίδιο IV θα συγκρούονται πολύ συχνά. Η πιθανότητα εικασίας του κλειδιού αυξάνει με το ρυθμό συγκρούσεων των IV. Το πρόβλημα λοιπόν επικεντρώνεται στο γεγονός ότι η προδιαγραφή 802.11 δεν ορίζει επακριβώς την παραγωγή του IV, ενώ πολλές κάρτες ασύρματου δικτύου δεν κάνουν συχνές αλλαγές του IV ανά πακέτο.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΑΚΕΡΑΙΟΤΗΤΑ

Το ICV υπολογίζεται για κάθε πλαίσιο και είναι ένα CRC των 32bit. Οπότε για το ICV ενός πλαισίου Μ μπορούμε να γράψουμε ότι:

$$ICV = CRC_{32}(M)$$

Το ICV προστίθεται στο M για να σχηματίσει πακέτο P:

$$P = M|ICV$$

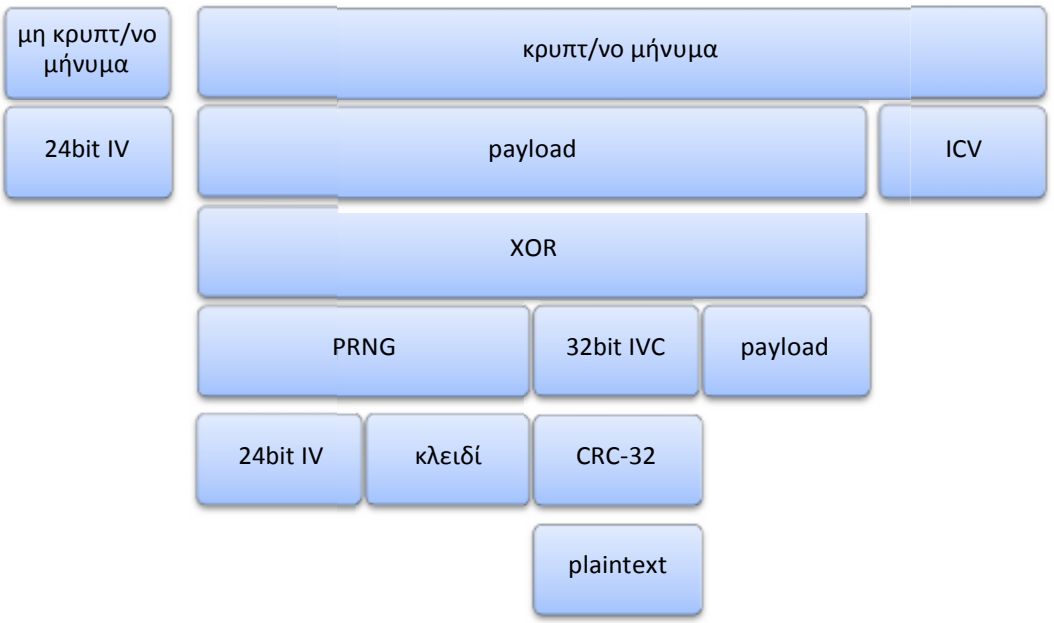
Το κλειδί παράγει το PRNG από το κλειδί WEP (K_{WEP}) και ένα IV των 24bits. Ένα νέο IV χρησιμοποιείται για κάθε πλαίσιο, ενώ το ίδιο IV επαναχρησιμοποιείται κάθε 242 πλαίσια. Το IV προστίθεται στην αρχή του K_{WEP} για να σχηματίσει ένα κλειδί K για κάθε πλαίσιο:

$$K = IV|K_{WEP}$$

Το P κρυπτογραφείται με τον κρυπταλγόριθμο RC4. Το κρυπτογραφημένο κείμενο C προκύπτει από την πράξη XOR μεταξύ του P και του K:

$$C = P \oplus K$$

Αρχικά το κλειδί WEP είχε μήκος 40bits (WEP-40) το οποίο προφανώς είναι πολύ μικρό για να παρέχει έστω και τη στοιχειώδη ασφάλεια. Το μήκος αυξήθηκε στα 104bits (WEP-104), γεγονός που πρακτικά δε βελτίωσε και πολλά πράγματα όσον αφορά την ασφάλεια. Η επικεφαλίδα στο πλαίσιο MAC του 802.11 είναι plaintext και προστίθεται πριν το payload. Ένα πεδίο της επικεφαλίδας του πλαισίου MAC είναι το IV, οπότε αυτό μεταδίδεται μη κρυπτογραφημένο, δηλαδή ως plaintext.



Σχήμα 23. Τα στάδια σχηματισμού του κλειδιού (πλαισίου) WEP από το αρχικό κείμενο (plaintext)

5.2 RSNA [32]

Η τροποποίηση του 802.11i παρουσίασε το RSNA για να εξαλείψει τις ελλείψεις στην ασφάλεια του αρχικού 802.11. Οι αλγόριθμοι του RSNA παρέχουν βελτιώσεις στην εμπιστευτικότητα, στην ακεραιότητα, στην πιστοποίηση και στη διαχείριση των κλειδιών.

ΠΙΣΤΟΠΟΙΗΣΗ (AUTHENTICATION)

Στο 802.11i παρουσιάζονται δύο RSNA μηχανισμοί πιστοποίησης:

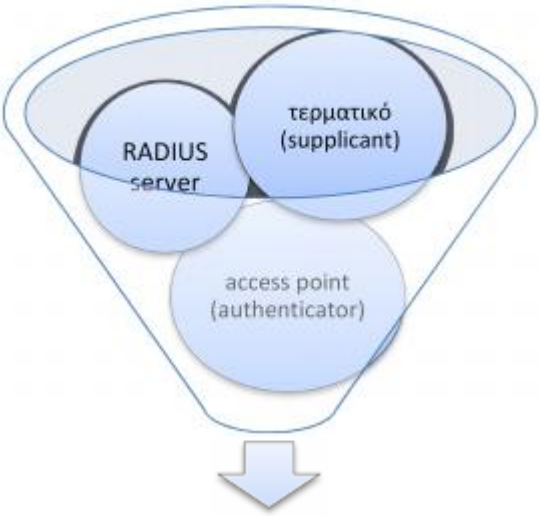
- Προδιαμοιραζόμενο κλειδί (Pre-Shared Key, PSK)
- 802.1X

Στον πρώτο μηχανισμό, ένα κοινό μυστικό κλειδί εγκαθίσταται στο τερματικό και στο access point. Η αμοιβαία πιστοποίηση γίνεται σε τέσσερα στάδια. Η διανομή του PSK γίνεται εκτός του 802.11i. Επειδή το διαχειριστικό κόστος είναι αρκετά υψηλό για τη διανομή κλειδιών σε μεγάλης έκτασης δίκτυα με πολλά τερματικά, συνήθως προτιμάται το 802.1X.

Το 802.1X [35] είναι ένα πρωτόκολλο layer 2 το οποίο υποστηρίζει έλεγχο πρόσβασης δικτύου που βασίζεται σε θύρες (ports). Η επικοινωνία σε μια θύρα που ελέγχεται από το 802.1X μπλοκάρεται από το access point έως ότου αυτή πιστοποιηθεί επιτυχώς. Το 802.1X αρχικά είχε σχεδιαστεί για ενσύρματα τοπικά δίκτυα, αλλά έχει τροποποιηθεί για τα ασύρματα δίκτυα 802.11. Το εκτεταμένο πρωτόκολλο πιστοποίησης (Extensible Authentication Protocol, EAP) επιτελεί τη διαδικασία πιστοποίησης. Το 802.1X καθορίζει πως τα πακέτα EAP ενθυλακώνονται σε πλαίσια layer 2 (βλ. Σχήμα 25). Αυτό ονομάζεται EAP Over Lan (EAPOL). Το 802.1X ορίζει τρεις οντότητες που συμμετέχουν στη διαδικασία πιστοποίησης (βλ. Σχήμα 24):

- Supplicant
- Authenticator
- Authentication server

Το supplicant είναι ένα κομμάτι λογισμικού που τρέχει στην πλευρά του ασύρματου τερματικού. Ο authenticator τρέχει στον εξυπηρέτη πιστοποίησης δικτύου (Network Authentication Server, NAS). Σε ένα 802.11 δίκτυο το ρόλο του NAS παίζει το access point. Ο εξυπηρέτης πιστοποίησης είναι συνήθως ένας RADIUS server. Το NAS είναι απαραίτητο να υπάρχει γιατί ο authentication server μπορεί να μη βρίσκεται στο ίδιο layer 2 δίκτυο με το τερματικό και το NAS μπλοκάρει τα πακέτα layer 3 από το τερματικό έως ότου αυτό πιστοποιηθεί. Το NAS έχει παραμετροποιηθεί από την IP διεύθυνση ή το domain του authentication server και προωθεί τα πακέτα EAP που προέρχονται από το τερματικό.



Σχήμα 24. Δομικά στοιχεία του 802.1X

Το access point ανακοινώνει τις δυνατότητες του σχετικά με την ασφάλεια με πλαίσια beacons ή με αποκρίσεις σε κατάλληλες αιτήσεις. Επομένως ένα ασύρματο τερματικό, ενημερώνεται για τα επίπεδα ασφάλειας είτε άμεσα είτε έμμεσα. Το ασύρματο τερματικό έπειτα επιλέγει ένα access point και πιστοποιείται χρησιμοποιώντας τη μέθοδο ανοικτού συστήματος. Η πιστοποίηση σε αυτό το σημείο είναι αρκετά αδύναμη και απλώς επιτρέπει στη συσκευή να συνδεθεί με το access point ώστε να αρχίσει να στέλνει πακέτα EAP. Οποιαδήποτε άλλη επικοινωνία μπλοκάρεται.

Το supplicant και το RADIUS διεκπεραιώνουν την πιστοποίηση χρησιμοποιώντας το authenticator ως ένα μεσάζοντα. Η πιστοποίηση μπορεί να γίνει είτε μόνο από τη μεριά του τερματικού ή αμοιβαία και εξαρτάται από τη μέθοδο EARP.

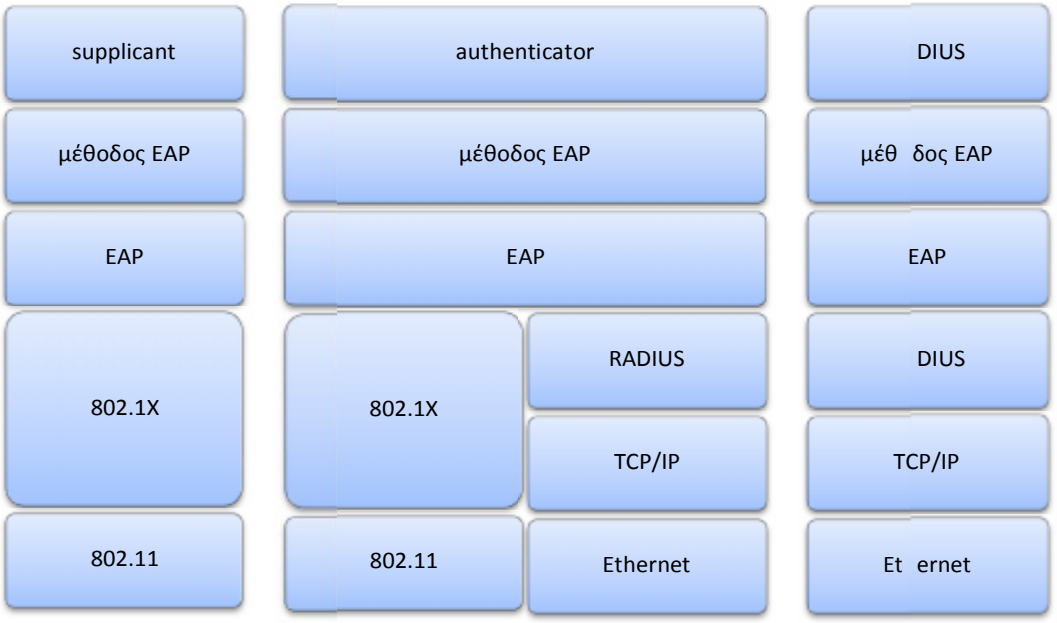
Δεδομένης μιας επιτυχημένης πιστοποίησης, το τερματικό και ο authentication server παράγουν ένα κοινό μυστικό κλειδί που ονομάζεται Master Session Key (MSK). Το supplicant δημιουργεί το Pairwise Master Key (PMK) από το MSK. Ο authentication server μεταδίδει τα κλειδιά στο authenticator, δίνοντάς του τη δυνατότητα να υπολογίσει κι αυτός το PMK. Τα supplicant και authenticator εκτελούν μια χειραψία (handshake) 4 σταδίων η οποία ορίζει τη μέθοδο κρυπτογράφησης για το Pairwise Transient Key (PTK). Σε επόμενες γραμμές θα περιγραφούν τα άλλα κλειδιά που παράγονται από το PTK. Σε αυτό το σημείο το 802.1X ξεμπλοκάρει τη θύρα και δέχεται τα πακέτα δεδομένων στο δίκτυο. Σε αυτό το σημείο το supplicant και το authenticator μπορούν να ανταλλάξουν πλαίσια με ασφάλεια.

Το EAP είναι ένα πρότυπο διαδικτύου για πιστοποίηση ενός πελάτη δικτύου (netowrk client). Το EAP αρχικά ήταν μια επέκταση στο πρωτόκολλο απο σημείο-σε-σημείο (Point-to-Point Protocol, PPP). Αναπτύχθηκε σαν ένα πλαίσιο για να αποφασίζουν οι τερματικές συσκευές ποιο μηχανισμό πιστοποίησης να χρησιμοποιήσουν. Αυτό σημαίνει ότι νέοι μηχανισμοί πιστοποίησης μπορούν να υιοθετηθούν χωρίς να πρέπει να επεκταθεί το PPP.

Όταν το supplicant συνδέεται, το authenticator στέλνει ένα πακέτο EAP-στο supplicant ρωτώντας για την ταυτότητά του. Το supplicant απαντά στο authenticator με ένα πακέτο EAP που υποδεικνύει την ταυτότητά του. Ο authentication server στέλνει στο supplicant μια δοκιμασία. Το supplicant αποκρίνεται και αν τα διαπιστευτήρια του client είναι έγκυρα, ο authentication server στέλνει μήνυμα επιτυχίας. Ο authenticator προωθεί τα μηνύματα EAP μεταξύ του supplicant και του authentication server. Τα μηνύματα που κυκλοφορούν στο δίκτυο ενθυλακώνονται σε πακέτα EAPOL. Αντίστοιχα τα μηνύματα που κυκλοφορούν στο ενσύρματο δίκτυο ενθυλακώνονται σε RADIUS πακέτα (over TCP/IP). Ο authenticator είναι υπεύθυνος για την ενθυλάκωση των πακέτων EAPOL και RADIUS.

Μερικές από τις υπάρχουσες μεθόδους EAP είναι οι εξής:

- EAP-PSK: Πιστοποίηση βασισμένη στο PSK
- EAP-MD5: Η στοιχειώδης μέθοδος πιστοποίησης βασισμένη σε συνάρτηση κατακερματισμού MD5. Η πιστοποίηση δεν είναι αμοιβαία. Λαμβάνει χώρα στη μεριά του client. Είναι ευπαθής σε επιθέσεις λεξικού (dictionary attack) και επιθέσεις man-in-the-middle. Επίσης είναι ακατάλληλη για παραγωγή κλειδιών.
- EAP-MSCHAPv2: Η έκδοση 2 του Microsoft CHAP, είναι ένα πρωτόκολλο πιστοποίησης που βασίζεται σε χειραψία. Ενώ η έκδοση 1 ήταν μηχανισμός μόνο στη μεριά του client, η έκδοση 2 επιτρέπει και στη μεριά του εξυπηρέτη.
- EAP-LEAP: είναι ένα EAP πρωτόκολλο της Cisco και παρέχει αμοιβαία πιστοποίηση που βασίζεται σε συνθηματικά.
- EAP-PEAP: πρωτόκολλο EAP που αναπτύχθηκε από κοινού από τη Microsoft, τη Cisco και την RSA Security. Επίσης παρέχει αμοιβαία πιστοποίηση από τη μεριά του client και του server.
- EAP-TLS: Η ασφάλεια επιπέδου μεταφοράς (Transport Layer Security, TLS) βασίζεται σε αμοιβαία πιστοποίηση με χρήση πιστοποιητικών, τα οποία ανταλλάσουν οι client και server.
- EAP-TTLS: Είναι επέκταση του TLS (Tunneled Transport Layer Security, TTLS). Οι clients πιστοποιούνται με συνθηματικό, ενώ η πιστοποίηση του server γίνεται με πιστοποιητικό.



Σχήμα 25. Σχέση μεταξύ EAP και 802.1X. (EAP Over Lan, EAPOL)

ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΟΥ

Η διανομή των κλειδιών είναι στενά συνδεδεμένη με τη διαδικασία πιστοποίησης. Το 802.11i χρησιμοποιεί διαφορετικά κλειδιά για διαφορετικούς σκοπούς. Αυτά τα κλειδιά σχηματίζουν μια ιεραρχία. Στην κορυφή βρίσκεται το PMK, από το οποίο προκύπτουν άλλα κλειδιά. Αν χρησιμοποιείται το 802.1X για πιστοποίηση, το PMK εγκαθιδρύεται κατά τη φάση της αμοιβαίας πιστοποίησης μεταξύ του supplicant και του authentication server. Αν χρησιμοποιείται η μέθοδος του προ-διαμοιρασμένου κλειδιού, τότε αυτό χρησιμοποιείται για το PMK. Το PTK εγκαθιδρύεται και στο supplicant και στο authenticator (access point). Από το PTK προκύπτουν άλλα τρία κλειδιά:

- Το EAPOL Key Confirmation Key (KCK)
- EAPOL Key Encryption Key (KEK)
- Temporal Key (TK)

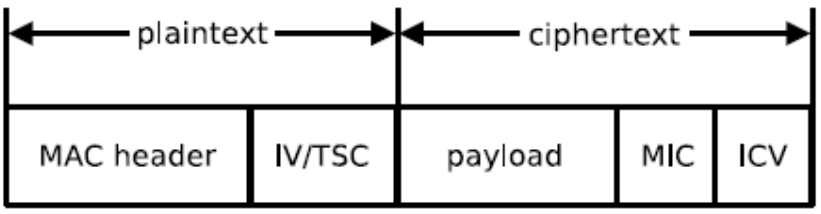
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΑΚΕΡΑΙΟΤΗΤΑ

Το RSNA καθορίζει δύο πρωτόκολλα για κρυπτογράφηση (εμπιστευτικότητα) και ακεραιότητα: το πρωτόκολλο αξιοπιστίας προσωρινού κλειδιού (Temporal Key

Integrity Protocol, TKIP) και το Counter Mode με Cipher Block Chaining Message Authentication Code (CBC-MAC) πρωτόκολλο (CCMP). Το TKIP χρησιμοποιεί RC4 για κρυπτογράφηση, αλλά είναι μια πολύ πιο ανθεκτική υλοποίηση σε σχέση με το WEP. Εκτός των άλλων, το TKIP χρησιμοποιεί ένα πιο πολύπλοκο σύστημα κλειδιών το οποίο αντιπαρέρχεται πολλών αδυναμιών του WEP. Ο αλγόριθμος Michael χρησιμοποιείται για τους κώδικες ακεραιότητας των μηνυμάτων. Το CCMP χρησιμοποιεί το προηγμένο πρότυπο κρυπτογράφησης (Advanced Encryption Standard, AES) στο Counter Mode για κρυπτογράφηση και το CBC-MAC για την ακεραιότητα μηνύματος. Το CBC-MAC υποστηρίζει επίσης προστασία εμπιστευτικότητας.

TKIP

Παρά τη βελτιωμένη ασφάλεια που θα εξασφάλιζε το 802.11i, ήταν κοινά αποδεκτό ότι η χρήση παρωχημένου υλικού βασισμένο στο 802.11 θα συνεχιζόταν. Οι παλιές συσκευές χρησιμοποιούσαν WEP άρα και τον κρυπταλγόριθμο RC4. Επίσης, κατά τη χρήση του WEP συμβαίνουν ανεπιθύμητες καταστάσεις, όπως για παράδειγμα παραγωγή αδύναμων κλειδιών, συγκρούσεις των IV και παραποίηση πακέτων. Για να αποτραπούν τα παραπάνω, η τροποποίηση 802.11i καθορίζει ένα υποπρωτόκολλο, το TKIP. Το TKIP πρακτικά "τυλίγει" την κρυπτογράφηση του WEP, παρέχοντας έτσι μια πιο πολύπλοκη λειτουργία στο ανακάτεμα των κλειδιών (βλ. Σχήμα 26). Το 128μπιτο κλειδί κωδικοποίησης ανά πλαίσιο που βασίζεται στο RC4, προκύπτει από το TK, από τη διεύθυνση MAC του client και από ένα IV. Το IV στο TKIP επίσης λειτουργεί ως ένας μετρητής σειράς για να προστατεύσει από επιθέσεις απλής επανάληψης.



Σχήμα 26. Δομή πλαισίου TKIP

Η συνάρτηση ανακατέματος του TKIP λειτουργεί σε δύο φάσεις. Στην πρώτη φάση, υπολογίζεται ένα κλειδί εκπομπής διεύθυνσης (TKIPmixed Transmit Address Key, TTAK) από το TK, η διεύθυνση MAC (TA) και ο μετρητής σειράς (TKIP Sequence Counter, TSC). Ένα κλειδί ανά πλαίσιο που ονομάζεται WEP-seed παράγεται στη δεύτερη φάση χρησιμοποιώντας τα TTAK, TA και TSC.

Το WEP-seed περνά από τη διαδικασία ενθυλάκωσης του WEP μαζί με το πλαίσιο του αρχικού μηνύματος M. Από το WEP-seed, το WEP παίρνει ένα RC4 κλειδί και ένα IV. . όπως φαίνεται το WEP-seed χρησιμοποιείται στη θέση του κλειδιού WEP και του WEP IV. Το WEP υπολογίζει το ICV και κρυπτογραφεί το M, οπότε και δημιουργεί το πλαίσιο του κρυπτογραφημένου μηνύματος.

Το TKIP περιλαμβάνει έναν έλεγχο ακεραιότητας μηνύματος των 64bits (Message Integrity Check, MIC) για κάθε πλαίσιο. Ο αλγόριθμος που χρησιμοποιείται για να υπολογιστεί το MIC ονομάζεται Michael. Σκοπός του είναι να αποτρέψει τους τύπους επιθέσεων στους οποίους ήταν ευάλωτο το WEP εξαιτίας του αδύναμου ελέγχου ακεραιότητας CRC. Το MIC υπολογίζεται με βάση τη διεύθυνση του πομπού (Source Address, SA), τη διεύθυνση προορισμού (Destination Address, DA), το πεδίο προτεραιότητας (Priority field, Pr), τρεις φυλασσόμενες οκτάδες Rsvd και τα δεδομένα payload M του πλαισίου MAC:

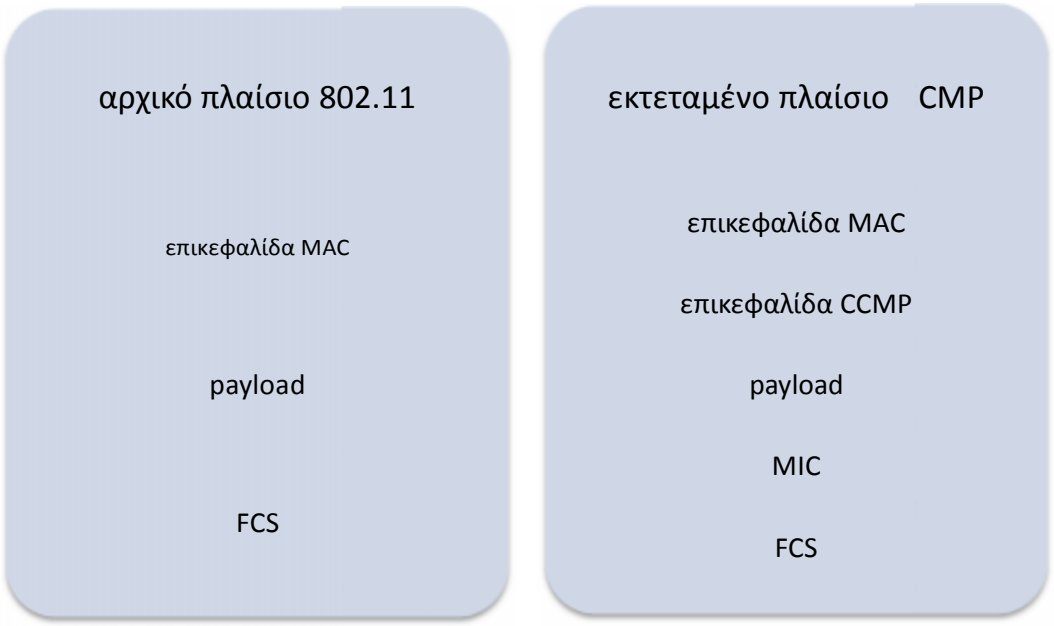
$$MIC = Michael(SA|DA|\Pr|Rsvd|M)$$

Ένα TSC για κάθε πλαίσιο χρησιμοποιείται για προστασία από απλές επιθέσεις επανάληψης. Τα πλαίσια που δεν έχουν αυξανόμενους αριθμούς σειράς απορρίπτονται από το δέκτη. Παρόλο που ο Michael είναι μια βελτίωση του CRC που χρησιμοποιείται στο WEP, έχει κι αυτός αδυναμίες σχετικά με την ακεραιότητα του μηνύματος. Αυτό οφείλεται στους σχεδιαστικούς περιορισμούς που επέβαλε η απαίτηση για υποστήριξη παλαιότερων συσκευών. Έτσι το TKIP υλοποιεί αντίμετρα για να μειώσει την πιθανότητα παραποιήσεων και να περιορίσει την εξάπλωση οποιασδήποτε πληροφορίας σχετικής με το κλειδί. Αν μια επίθεση γίνει αντιληπτή οι λειτουργίες του TKIP αναστέλλονται για 60 δευτερόλεπτα. Τα κλειδιά αναδιανέμονται και λαμβάνονται μέτρα αν δύο πλαίσια φτάσουν με διαφορά ενός λεπτού το ένα από το άλλο με λανθασμένα MICs. Το κλειδί RC4 και το IV χρησιμοποιούνται ως το WEP-seed, το οποίο περνά στη διαδικασία ενθυλάκωσης του WEP. Το WEP το χρησιμοποιεί για να παράγει ένα ICV και να κρυπτογραφήσει

το MPDU και το MIC. Ενώ αποτελεί μια βελτίωση στο WEP, το MIC του TKIP παραμένει σχετικά αδύναμο μπροστά στην παραποίηση μηνύματος. Παρόλα αυτά, αντιπροσωπεύει ότι καλύτερο μπορεί να εφαρμοστεί σε παλαιά τερματικά.

CCMP

Το CCMP είναι ένα πρωτόκολλο βασισμένο στο counter mode του AES με CBC-MAC. Ο AES είναι πολύ πιο ισχυρός από τον RC4 που χρησιμοποιείται στο WEP και στο TKIP. Παρόλα αυτά δε μπορεί να "τρέξει" σε παλιές συσκευές. Τα πλαίσια του 802.11 MAC περνούν για επεξεργασία από το CCMP (βλ. Σχήμα 27). Τα πλαίσια 802.11 αποτελούνται από μια επικεφαλίδα MAC, τα δεδομένα και το FCS. Το MIC κρυπτογραφείται μαζί με το payload του 802.11 πλαισίου. Η επικεφαλίδα CCMP και τα κρυπτογραφημένα δεδομένα προστίθενται στην αρχική επικεφαλίδα MAC, καθώς και το FCS. Η επικεφαλίδα CCMP αποτελείται από το ExtIV, το KeyID και τον αριθμό πακέτου (Packet Number, PN). Το PN0 είναι το λιγότερο σημαντικό byte του PN. Το CCMP παράγει ένα νέο TK για κάθε σύνοδο και μια μοναδική τιμή για κάθε πλαίσιο. Η τιμή αυτή είναι ένα PN των 48bits κωδικοποιημένο με το TK. Το πρότυπο 802.11i [13] επισημαίνει ότι η ασφάλεια μπορεί να τεθεί σε κίνδυνο αν το PN ξαναχρησιμοποιηθεί με το ίδιο TK. Επομένως, το PN αυξάνει για κάθε πλαίσιο.

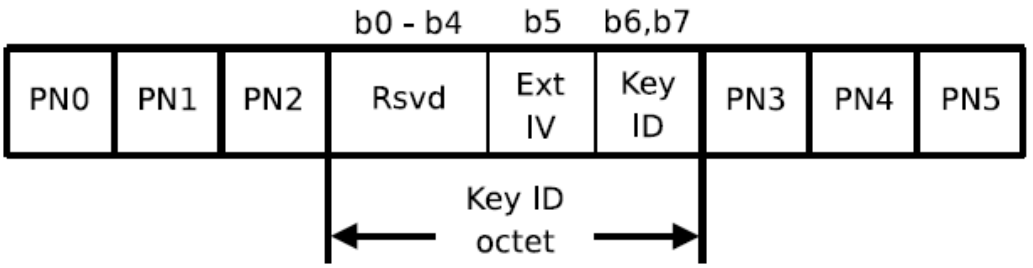


Σχήμα 27. Επεκταμένο πλαίσιο CCMP

Η διαδικασία ενθυλάκωσης του CCMP έχει ως εξής. Τα δεδομένα πρόσθετης πιστοποίησης (Additional Authentication Data, AAD) κατασκευάζονται από πεδία στην επικεφαλίδα του MPDU. Το PN, το πεδίο της δεύτερης διεύθυνσης (A2) και το πεδίο προτεραιότητας της επικεφαλίδας MAC χρησιμοποιούνται για να πράξουν τη μοναδική τιμή του block CCM:

$$CCM\ block = Priority|A2|PN$$

Το PN και το key identifier τοποθετούνται μέσα στην επικεφαλίδα CCMP (βλ. Σχήμα 28). Η συνένωση του payload από το πλαίσιο MAC και το MIC κρυπτογραφούνται με το AES χρησιμοποιώντας το TK, το AAD και τη μοναδική τιμή. Το κρυπτογραφημένο πλαίσιο σχηματίζεται από την επικεφαλίδα MAC, την επικεφαλίδα CCMP και τα κρυπτογραφημένα δεδομένα. Η αποκρυπτογράφηση έχει ως εξής. Πεδία από τις επικεφαλίδες MAC και CCMP εξάγονται για να κατασκευαστεί το AAD και η μοναδική τιμή. Η αποκρυπτογράφηση των δεδομένων δίνει τα αρχικά δεδομένα και το MIC. Το αρχικό πλαίσιο ανακατασκευάζεται προσθέτοντας τα αρχικά δεδομένα στην επικεφαλίδα MAC.



Σχήμα 28. Η επικεφαλίδα CCMP

5.3 ΣΥΓΚΡΙΣΗ WEP, WPA ΚΑΙ WPA2

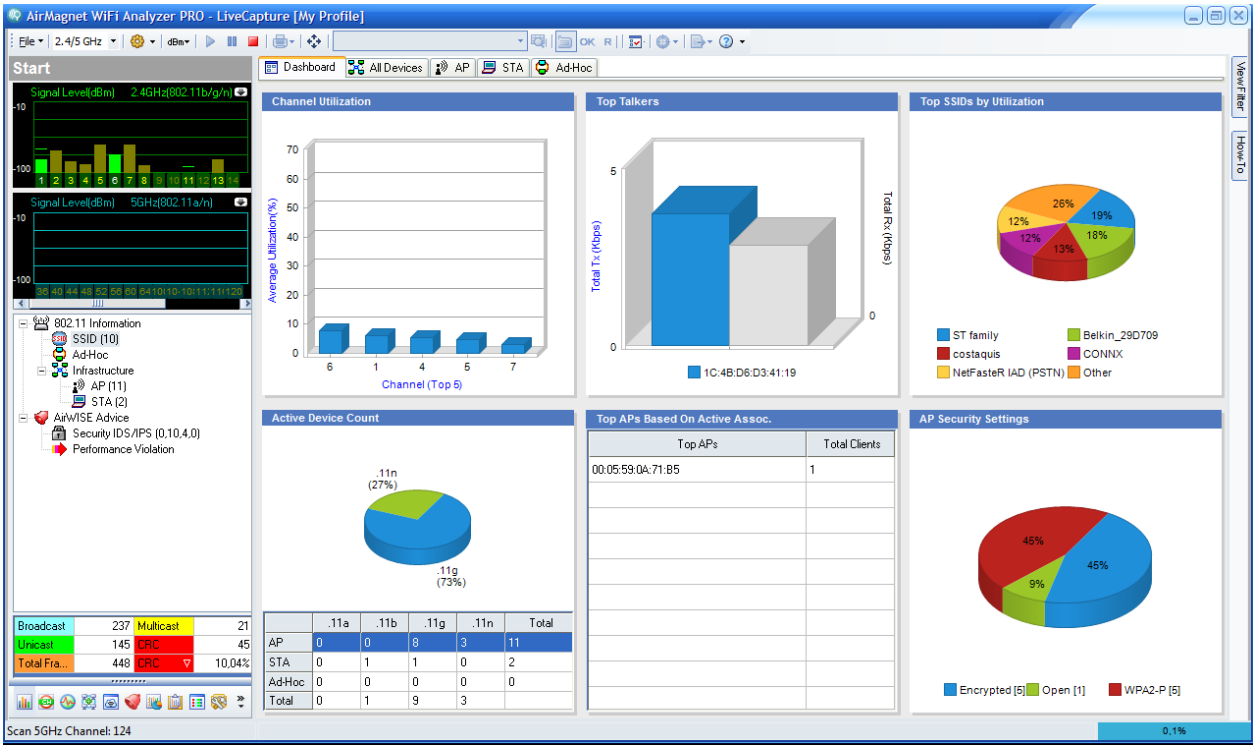
Όπως επισημάνθηκε στην αρχή του κεφαλαίου, το Wi-Fi Alliance παρουσίασε το WPA και εν συνεχεία το WPA2 ως μια βελτίωση στην ανεπάρκεια του WEP να προσφέρει μια στοιχειώδη ασφάλεια. Οι διάφορες και οι βελτιώσεις παρουσιάζονται συνοπτικά στον παρακάτω πίνακα.

WEP	WPA	WPA2
Προδιαμοιραζόμενο κλειδί το οποίο εγκαθίσταται χειροκίνητα στα τερματικά και στο BSS/ESS	802.1X για πιστοποίηση και διανομή κλειδιών. Υποστηρίζει και προδιαμοιρασμένα κλειδιά όπως το WEP	το ίδιο με το WPA
Χρησιμοποιεί σύγχρονο κρυπταλγόριθμο ροής (RC4) που είναι ακατάλληλος για ασύρματες ζεύξεις	Το ίδιο με το WEP	Αντικαθιστά τον RC4 με κρυπταλγόριθμο block, τον AES
Παράγει ένα κλειδί ανά πακέτο με το να προσθέτει απευθείας το IV στο master κλειδί, το οποίο πλέον είναι εκτεθειμένο σε επιθέσεις τύπου FMS	Εισάγει την έννοια του PTK στην ιεραρχία κλειδιών. Χρησιμοποιεί μια συνάρτηση αναδιανομής κλειδιών.	Το ίδιο με το WPA
Πολύ περιορισμένο εύρος κλειδιών λόγω στατικού master κλειδιού, μικρού IV και παραγωγής κλειδιού ανά πακέτο.	Αυξάνει το IV σε 56bits φυλάσσοντας τα 8bits για να απορρίπτει αδύναμα κλειδιά. Μεγαλύτερο σύνολο κλειδιών λογω καινούριου PTK για κάθε σύνοδο	Το ίδιο με το WPA
Πολύ πιθανή η επαναχρησιμοποίηση κλειδιών λόγω προαιρετικής αλλαγής του IV	Καθορίζει αυστηρά ότι πομπός και δέκτης αρχικοποιούν το IV σε 0 για κάθε καινούριο PTK και το αλλάζουν μετά από κάθε αποστολή πακέτου	Το ίδιο με το WPA
Ελλείπεις προστασία ακεραιότητας με το CRC-32	Michael αντί για CRC. Επίσης καθορίζει εναλλακτικές στην περίπτωση που ο Michael παραβιαστεί	Πιο ισχυρή προστασία ακεραιότητας με χρήση AES CCMP
Ευάλωτο σε επιθέσεις ανακατεύθυνσης γιατί το ICV δε προστατεύει την ακεραιότητα της επικεφαλίδας του 802.11	Διευρύνει τον υπολογισμό του ICV περιλαμβάνοντας τις MAC διευθύνσεις πομπού και δέκτη	Το ίδιο με το WPA
Καμιά προστασία απέναντι σε επιθέσεις επανάληψης	Η χρήση του IV ως αύξοντα αριθμού σειράς παρέχει ασφάλεια σε τέτοιες επιθέσεις	Το ίδιο με το WPA
Καμιά υποστήριξη ώστε τα τερματικά να πιστοποιήσουν το δίκτυο	Το 802.1X θα μπορούσε να χρησιμοποιηθεί από τις συσκευές για την πιστοποίηση του δικτύου	Το ίδιο με το WPA

Πίνακας 10. Σύγκριση αρχιτεκτονικών ασφάλειας WEP, WPA και WPA2

6. ΜΕΤΡΗΣΕΙΣ ΜΕ ΤΟ AIRMAGNET Wi-Fi ANALYZER

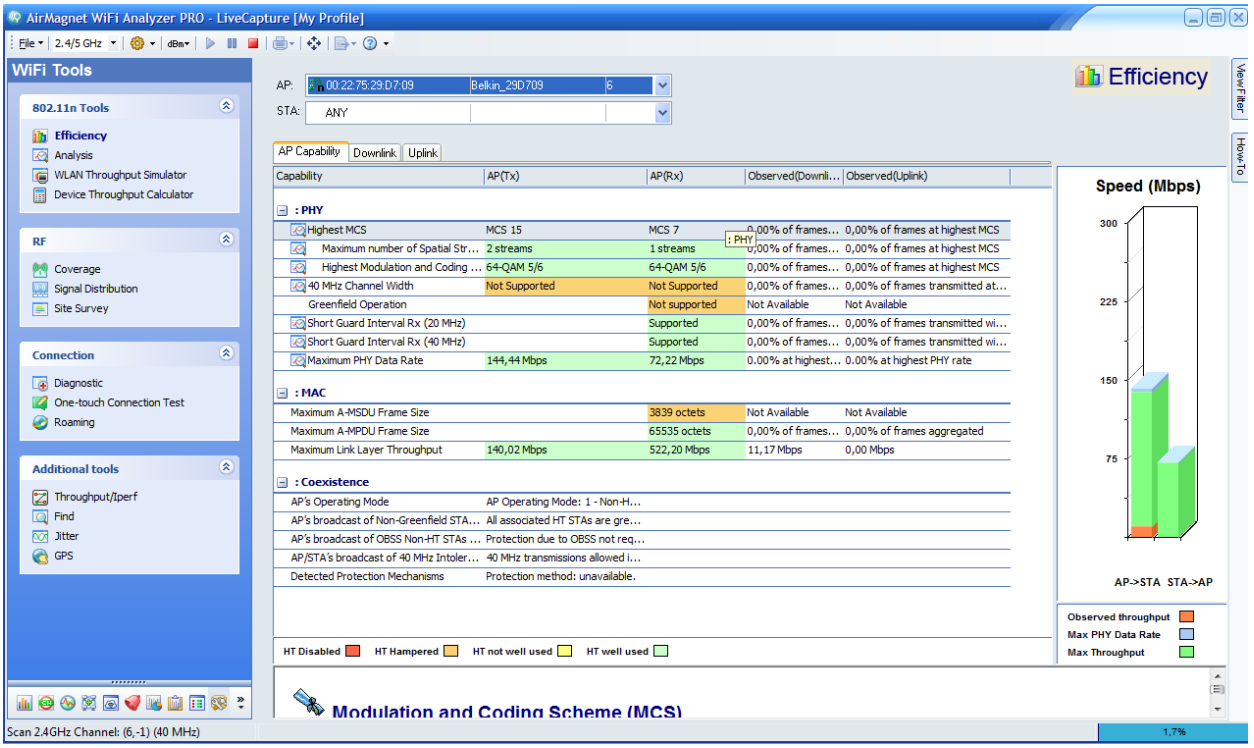
Χρησιμοποιήθηκε το πρόγραμμα AirMagnet Wi-Fi Analyzer. Ξεκινώντας την επισκόπηση του δικτύου, βλέπουμε τα γενικά χαρακτηριστικά όσον αφορά τα access points (AP) και τους σταθμούς-πελάτες (client stations, STAs). Στη συγκεκριμένη περιοχή βρέθηκαν 11 APs και 2 τερματικά. Κάποια πιο λεπτομερή στοιχεία που αναφέρονται από το πρόγραμμα είναι το πλήθος συσκευών ανά πρωτόκολλο (802.11b/g/n). Παρατηρούμε λοιπόν ότι ένα τερματικό δουλεύει στο 802.11b κι ένα στο 802.11g. Από τα APs οκτώ δουλεύουν στο 802.11g και 3 στο 802.11n. Εκτός από τα στατιστικά χρήσης ανά SSID βλέπουμε και τις ρυθμίσεις ασφάλειας σε ποσοστό επί του συνόλου των APs. Έτσι 5 χρησιμοποιούν κλειδιά WEP, 5 WPA2 και 1 είναι ανοικτό (βλ. Σχήμα 29). Το ότι αναφέρεται ως ανοικτή η πρόσβαση στο συγκεκριμένο AP δεν σημαίνει ότι δεν έχει καθόλου κάποιο επίπεδο ασφάλειας. Πιθανότατα κάποια λίστα πρόσβασης διευθύνσεων MAC. Τέλος, πάνω αριστερά στο παράθυρο φαίνονται οι ζώνες συχνοτήτων και τα κανάλια ανάλογα με το πρωτόκολλο που χρησιμοποιούν οι συσκευές.



Σχήμα 29. Γενικά στατιστικά τερματικών και AP στην περιοχή κάλυψης.

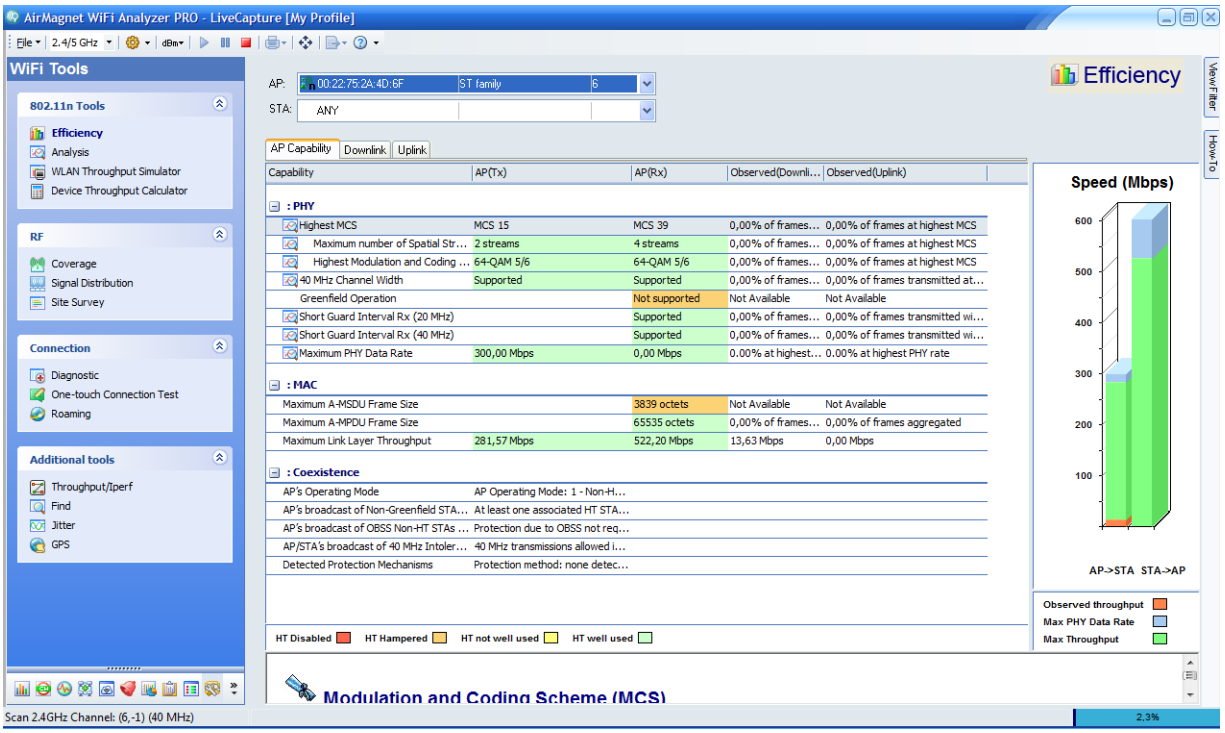
Έπειτα βλέπουμε πιο λεπτομερή χαρακτηριστικά για συγκεκριμένο AP της επιλογής μας. Στην προκειμένη περίπτωση ελέγχθηκαν τα APs Belkin_29D709, ST Family και costaquis, τα οποία υποστηρίζουν το 802.11n, αλλά όπως θα δούμε στις παρακάτω εικόνες μόνο 1 AP το χρησιμοποιεί (το ST Family).

Στο σχήμα 30 βλέπουμε τα στοιχεία του Belkin_29D709. Πιο αναλυτικά, βλέπουμε τη διαμόρφωση και κωδικοποίηση (64 QAM και 5/6). Το 5/6 είναι ο ρυθμός κωδικοποίησης. Να σημειώσουμε ότι το MCS είναι το Modulation and Coding Scheme που χρησιμοποιείται και για το 802.11n υποχρεωτικά είναι τα MCS 0-15 όσον αφορά τα APs, ενώ για τα τερματικά 802.11n είναι υποχρεωτικά τα MCS 0-7, τα οποία στο σχήμα φαίνονται στις αντίστοιχες στήλες. Επίσης παρατηρούμε ότι υποστηρίζονται short GIs στη λήψη (Rx) και στα 20 αλλά και στα 40MHz. Τα streams είναι 2 και 1 για MCS 0-15 και MCS 0-7 αντίστοιχα. Ο μέγιστος ρυθμός δεδομένων που μπορεί να υποστηριχθεί από το PHY είναι 144Mbps και 72,22Mbps. Η ζώνη των 40Mhz δεν υποστηρίζεται.



Σχήμα 30. Χαρακτηριστικά του Belkin_29D709.

Αντίθετα στο ST Family (βλ. Σχήμα 31), έχουμε 4 streams ενώ υποστηρίζεται η ζώνη των 40MHz, γεγονός που υποδεικνύει ότι η λειτουργία του AP είναι στο 802.11n. Γι' αυτό και τελικά βλέπουμε ότι ο μέγιστος ρυθμός δεδομένων που μπορεί να υποστηρίξει το PHY είναι 300Mbps. Επίσης υποστηρίζονται short GIs στις ζώνες των 20 και 40MHz. Και τα 2 APs χρησιμοποιούν το κανάλι 6. Το AP costaquis χρησιμοποιεί το κανάλι 1 και παρατηρούμε παρόμοια χαρακτηριστικά με αυτά του Belkin_29D709. Αυτά τα APs χρησιμοποιούν το 802.11g.



Σχήμα 31. Χαρακτηριστικά του ST Family.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΑΝΑΦΟΡΕΣ

1. Scott R. Fluhrer, Itsik Mantin, Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. In SAC ’01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, p. 1–24. Springer, London, 2001
2. Bruce Tuch. Development of waveLAN an ISM band wireless WAN. In AT&T Technical Journal, vol. 72, p. 27–37, 1993
3. Saikat Ray, Jeffrey B. Carruthers, and David Starobinski. RTS/CTS-induced congestion in ad hoc wireless LANs. Wireless Communications and Networking, p. 1516–1521, 2003
4. IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 1: Radio Resource Measurement of Wireless LANs, 6 2008. IEEE Std 802.11k-2008
5. IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe, 10 2003. IEEE Std 802.11h-2003
6. P. Fuxjager, D. Valerio, and F. Ricciato. The myth of non-overlapping channels: interference measurements in IEEE 802.11. In Wireless on Demand Network Systems and Services Conference, 2007, p. 1–8, 2007

7. B. Boskovic and M. Markovic. On spread spectrum modulation techniques applied in IEEE 802.11 wireless LAN standard. In EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security, p. 238–241, 2000
8. S. Salam Shumona, Sabrina Islam, Sabrina Ralman, Fakhrul Alam, and Forruk Almed. Performance of IEEE 802.11b wireless local area network. In ICECE 2004, 3rd International Conference on Electrical & Computer Engineering, p. 283–286, 2004
9. K. Halford, S. Halford, M. Webster & C. Andren. Complementary code keying for rakebased indoor wireless communication. In ISCAS 99. Proceedings of the 1999 IEEE International Symposium on Circuits & Systems, vol. 4, p. 427–430, 1999
10. Jishu DasGupta, Karla Ziri-Castro, and Hajime Suzuki. Capacity analysis of MIMO-OFDM broadband channels in populated indoor environments. In ISCIT '07. International Symposium on Communications and Information Technologies, p. 273–278, 2007
11. Mourad Melliti, Salem Hasnaoui, and Ridha Bouallegue. Analysis of frequency offsets and phase noise effects on an OFDM 802.11g transceiver. International Journal of Computer Science and Network Security, p. 87–91, 2007
12. Zelst. Per-Antenna-Coded Schemes for MIMO OFDM, vol. 4, p. 2032–2836, 2003
13. IEEE 802.11 WG. IEEE 802.11i Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements, 07 2004. Reference number ISO/IEC 8802-11-2004
14. IEEE 802.1D, http://standards.ieee.org/getieee802/download/802.1D-2004.pdf

ΒΙΒΛΙΑ

15. Andrew S. Tanenbaum. Computer Networks. 4th Edition, Prentice Hall, 2003
16. J.G. Proakis, Masoud Salehi, Communication Systems Engineering, 2nd Ed., Prentice Hall, 2002
17. C. E. Perkins, Ad Hoc Networking. Addison-Wesley, 2001.

18. Bernhard H. Walke, Stefan Mangold and Lars Berlemann, IEEE 802 Wireless Systems: Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence, Wiley, 2006
19. Καραγιαννίδης Γ., Τηλεπικοινωνιακά Συστήματα, εκδόσεις Τζιόλα, 2009
20. Κωττής Π., Ασύρματες Επικοινωνίες, εκδόσεις Τζιόλα, 2010
21. Θεολόγου Μ.Ε., Δίκτυα Κινητών & Προσωπικών Επικοινωνιών, εκδόσεις Τζιόλα, 2008
22. Νικοπολιτίδης Π., Obaidat M., Παπαδημητρίου Γ., Πομπόρτσης Α., Ασύρματα Δίκτυα, εκδόσεις Κλειδάριθμος, 2003
23. Καμπουράκης Γ., Γκρίτζαλης Σ., Κάτσικας Σ., Ασφάλεια Ασύρματων και Κινητών Δικτύων Επικοινωνιών, εκδόσεις Παπασωτηρίου, 2006

ΔΙΑΔΙΚΤΥΑΚΟΙ ΣΥΝΔΕΣΜΟΙ

24. http://en.wikipedia.org/wiki/802.11
25. http://en.wikipedia.org/wiki/IEEE_802.11_(legacy_mode)
26. http://en.wikipedia.org/wiki/IEEE_802.11a-1999
27. http://en.wikipedia.org/wiki/IEEE_802.11b-1999
28. http://en.wikipedia.org/wiki/IEEE_802.11g-2003
29. http://en.wikipedia.org/wiki/IEEE_802.11n-2009
30. http://en.wikipedia.org/wiki/IEEE_802.11e
31. http://en.wikipedia.org/wiki/IEEE_802.11h
32. http://en.wikipedia.org/wiki/IEEE_802.11i
33. http://en.wikipedia.org/wiki/IEEE_802.11k
34. http://en.wikipedia.org/wiki/IEEE_802.1D [802.11c]
35. http://en.wikipedia.org/wiki/802.1X
36. http://en.wikipedia.org/wiki/WaveLAN
37. http://en.wikipedia.org/wiki/ALOHA
38. http://en.wikipedia.org/wiki/Wi-Fi_Alliance
39. http://en.wikipedia.org/wiki/List_of_telecommunications_regulatory_bodies
40. http://en.wikipedia.org/wiki/ISM_band
41. http://en.wikipedia.org/wiki/Beamforming