ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

«Πρωτόκολλα ασύρματων τοπικών δικτύων - WiFi»

Της φοιτήτριας
Δομζαρίδου Ελένης
Αρ. Μητρώου: 05/2782

Επιβλέπων καθηγητής
Βίτσας Βασίλειος

Θεσσαλονίκη 2010

Περίληψη

Η παρούσα πτυχιακή είναι μια προσπάθεια περιγραφής του τρόπου λειτουργίας των ασύρματων τοπικών δικτύων και συγκεκριμένα του προτύπου IEEE 802.11. Ο αναγνώστης εισάγεται στον κόσμο των WLANs μέσα από μια ιστορική αναδρομή στα ασύρματα τοπικά δίκτυα, ξεκινώντας από το πρότυπο OpenAir και καταλήγοντας στο πιο πρόσφατο πρότυπο IEEE 802.11n. Ακολουθούν περισσότερο τεχνικά θέματα όπως οι μέθοδοι λειτουργίας του πρωτοκόλλου IEEE 802.11 στο φυσικό επίπεδο, με αναλυτική περιγραφή των μεθόδων διασποράς φάσματος, FHSS, DSSS και OFDM. Ακολουθεί μια εισαγωγή στο MAC επίπεδο των WLANs όπου περιγράφονται συνοπτικά οι λειτουργίες που επιτελούνται σε αυτό, όπως η ανίχνευση ενός δικτύου από κάποιον σταθμό, η αυθεντικοποίηση ενός σταθμού, η ενσωμάτωσή του στο δίκτυο και η διαδικασία πρόσβασης στο μέσο. Σε επόμενο κεφάλαιο περιγράφεται με περισσότερη λεπτομέρεια η λειτουργία DCF, η λειτουργία PCF, θέματα που σχετίζονται με την εξοικονόμηση ενέργειας στα WLANs, ενώ αναλύονται τα προβλήματα του κρυφού και του εκτεθειμένου σταθμού. Το τελευταίο κεφάλαιο αναφέρεται στην ασφάλεια των WLANs, όπου περιγράφονται τα πρωτόκολλα WEP, WPA, WPA2 (802.11i), καθώς και το πρωτόκολλο EAP (802.1x) που σχετίζεται με μεθόδους αυθεντικοποίησης.

Abstract

This thesis is an effort to describe the way Wireless Local Area Networks, and especially the protocol IEEE 802.11, operate. We introduce the reader into the WLANs' world by a historical retrospection, which begins from the OpenAir protocol, leading to the most recent protocol, the IEEE 802.11n. We offer a presentation of how the IEEE 802.11 operates on a physical level, accompanied by an analytic description of spread spectrum technique, FHSS, DSSS and OFDM methods. Afterwards, an introduction to the MAC level of WLANs follows, where we describe the operations that need to be carried out, as the detection of a network, the authentication process by a station, the station's association in a network and the necessary processes a station needs to implement in order to have access in the channel. On the following chapters, we give an extensive analysis over the DCF and PCF methods, the hidden and exposed station problems and the power save features for WLANs. The last chapter refers to the WLANs' security issues by describing the WEP, WPA, WPA2 (802.11i) protocols, as well as EAP (802.1x) protocol, which is related with authentication methods.

Ευχαριστίες

Η ολοκλήρωση της πτυχιακής μου σηματοδοτεί την έναρξη μιας νέας περιόδου στη ζωή μου, στην οποία θα προσπαθήσω να αξιοποιήσω τις γνώσεις που απέκτησα μέσα σε αυτά τα πέντε έτη από τη σχολή. Πολλές φορές όμως, το τέλος μιας πορείας αποτελεί και το δυσκολότερο κομμάτι της, το οποίο δεν θα μπορούσα να ολοκληρώσω χωρίς τη βοήθεια κάποιων ανθρώπων. Για αυτούς, το ελάχιστο που μπορώ να κάνω είναι να τους ευχαριστήσω.

Έτσι, αρχικά οφείλω ένα μεγάλο ευχαριστώ στον επιβλέποντα καθηγητή μου, κύριο Βίτσα Βασίλειο, γιατί μου έδωσε την ευκαιρία να ασχοληθώ με ένα θέμα που με ενδιαφέρει, για τη στήριξή του σε στιγμές άγχους και αγωνίας μου, και κυρίως για την υπομονή και τη σχολαστική διόρθωση των λαθών και των παραλήψεών μου. Η συμβολή του ήταν πολύ σημαντική στο τελικό αποτέλεσμα της πτυχιακής.

Επίσης θέλω να ευχαριστήσω τον κύριο Ηλιούδη Χρήστο ο οποίος με βοήθησε στο κεφάλαιο που αφορά στην ασφάλεια των WLANs και τα σχόλιά του ήταν χρήσιμα και ενθαρρυντικά.

Τέλος, ένα μεγάλο ευχαριστώ στη μητέρα μου Βασιλική, στον πατέρα μου Φώτη και στους φίλους μου Παναγιώτη και Νατάσσα που ήταν δίπλα μου όλο αυτό το διάστημα και στήριξαν την προσπάθειά μου.

Περιεχόμενα

Ευρετήριο Εικόνων viii

Ευρετήριο Πινάκων x

Εισαγωγή 1

Κεφάλαιο 1 Ασύρματα τοπικά δίκτυα 3

1.1 Εισαγωγή 3

1.2 Η ιστορία των WLANs 3

1.3 WiFi (Wireless Fidelity) – Ασύρματη Πιστότητα 6

1.4 Ραδιοσυχνότητες – το κλειδί για τη λειτουργία των WLANs 7

1.5 Πλεονεκτήματα χρήσης των WLANs 7

1.6 Τα μειονεκτήματα των WLANs 8

1.7 Κινδυνεύουμε από τη χρήση ασύρματων συσκευών; 9

1.8 OpenAir 10

1.9 HomeRF 11

1.10 Το πρότυπο HiperLAN 11

1.10.1 HiperLAN/1 11

1.10.2 HiperLAN/2 12

1.11 Το πρότυπο IEEE 802.11 13

1.11.1 IEEE 802.11 – 1997 14

1.11.2 IEEE 802.11a 14

1.11.3 IEEE 802.11b 15

1.11.4 IEEE 802.11g 15

1.11.5 IEEE 802.11n 16

Επίλογος 16

Κεφάλαιο 2 Το φυσικό επίπεδο του προτύπου IEEE 802.11 17

2.1 Εισαγωγή 17

2.2 Το φυσικό επίπεδο του προτύπου IEEE 802.11 17

2.3 Διασπορά Φάσματος (Spread Spectrum) 20

2.3.1 Διασπορά φάσματος μεταπήδησης συχνότητας (Frequency Hopping Spread Spectrum - FS ή FHSS) 24

2.3.2 Διασπορά φάσματος άμεσης ακολουθίας (Direct Sequence Spread Spectrum – DSSS) 29

2.3.3 Ορθογωνική πολύπλεξη διαίρεσης συχνότητας (Orthogonal Frequency Division Multiplexing - OFDM) 33
2.4 Υπέρυθρες Ακτίνες (Infrared) 34
Επίλογος 35

Κεφάλαιο 3 Εισαγωγή στο MAC επίπεδο του IEEE 802.11 36
3.1 Εισαγωγή 36
3.2 Το επίπεδο ελέγχου πρόσβασης στο μέσο του IEEE 802.11 (MAC Layer) 36
3.2.1 Περιγραφή λειτουργιών του υποεπιπέδου MAC του IEEE 802.11 39
3.3 Στοιχεία αρχιτεκτονικής των ασύρματων δικτύων 40
3.4 Μορφή μηνυμάτων στο IEEE 802.11 41
3.4.1 PLCP (Physical Layer Convergence Protocol) 42
3.4.2 Κεφαλίδα του MAC 42
3.4.2.1 Έλεγχος πλαισίου (Frame Control Field) 42
3.4.2.2 Πεδίο Duration / ID 44
3.4.2.3 Διεύθυνση MAC 45
3.4.2.4 Έλεγχος ακολουθίας 45
3.4.3 Σώμα του πλαισίου (Frame Body) 48
3.4.4 Ακολουθία ελέγχου πλαισίου (Frame Check Sequence) 48
3.5 Οι διαδικασίες ανίχνευσης, ενσωμάτωσης, αυθεντικοποίησης και συσχέτισης 48
3.5.1 Διαδικασία ανίχνευσης δικτύου (Scanning) 49
3.5.2 Διαδικασία ενσωμάτωσης σε ένα δίκτυο (Joining) 50
3.5.3 Αυθεντικοποίηση ενός σταθμού (Authentication) 50
3.5.3.1 Αυθεντικοποίηση ανοιχτού συστήματος 51
3.5.3.2 Αυθεντικοποίηση προμοιρασμένου κλειδιού 52
3.5.4 Συσχέτιση ενός σταθμού με το δίκτυο (Association) 53
Επίλογος 54

Κεφάλαιο 4 Το MAC επίπεδο του IEEE 802.11 55
4.1 Εισαγωγή 55
4.2 Η πρόσβαση στο μέσο 55
4.2.1 Media Access Control Protocol - CSMA/CA 55
4.2.1.1 CSMA/CA Distributed Coordination Function (DCF) 56
4.2.1.2 Χρόνοι αναμονής μετάδοσης πλαισίων 56
4.2.1.3 Παράθυρο υπαναχώρησης / οπισθοχώρησης 59
4.2.1.4 Διάνυσμα δέσμευσης δικτύου (Network Allocation Vector) 61
4.2.1.5 Λειτουργία κατανεμημένου συντονισμού (DCF) 61
4.2.1.6 DCF - όταν το κανάλι είναι ελεύθερο 62
4.2.1.7 DCF - όταν το κανάλι είναι απασχολημένο 63

4.2.1.8 Το πρόβλημα του κρυφού σταθμού (Hidden node problem) 64
4.2.1.9 Το πρόβλημα του εκτεθειμένου σταθμού (Exposed node problem) 68
4.2.1.10 Τρόπος λειτουργίας του μηχανισμού RTS / CTS 70
4.2.1.11 Άλλες λύσεις για το πρόβλημα του κρυφού σταθμού 72
4.2.1.12 Λειτουργία Protection Mode για μικτά δίκτυα 802.11b/g 74
4.2.1.13 Χρήση μόνο CTS μηνυμάτων (CTS only Method) 75
4.2.1.14 Μέθοδος Σημειακού Συντονισμού (PCF) 75
4.2.1.15 Τρόπος λειτουργίας της μεθόδου PCF 76
4.3 Επιπρόσθετα χαρακτηριστικά του πρωτοκόλλου 77
4.3.1 Λειτουργία streaming / burst 77
4.3.2 Μη αποστολή μηνυμάτων επιβεβαίωσης (No Acknoledgement) 78
4.3.3 Λειτουργία κατάτμησης 78
4.4 Εξοικονόμηση ενέργειας 79
4.4.1 Power Save Mode 80
4.4.2 Automatic Power Save Delivery (APSD) 81
Επίλογος 81

Κεφάλαιο 5 Θέματα ασφάλειας στα WLANs 82
5.1 Εισαγωγή 82
5.2 Απαιτήσεις ασφάλειας: αυθεντικοποίηση, ιδιωτικότητα, μη απάρνηση, διαθεσιμότητα 82
5.3 Κενά ασφάλειας στα WLANs 83
5.4 Ανάλυση ευπαθειών στα WLANs 85
5.5 Οι τρεις γενιές ασφάλειας των WLANs 86
5.6 Wired Equivalent Privacy (WEP) 88
5.6.1 Το κρυπτογραφικό background του WEP 89
5.6.2 Κρυπτογραφικές λειτουργίες του WEP 90
5.6.3 Τύποι κλειδιών στο WEP 91
5.6.4 Το πλαίσιο του WEP 92
5.6.5 Πως γίνεται η επεξεργασία των δεδομένων στο WEP 92
5.6.6 Ο κρυπτογραφικός αλγόριθμος RC4 94
5.6.8 Διαμοιρασμός του κλειδιού 96
5.6.9 Ευπάθειες και αδυναμίες του WEP 96
5.7 Τα πρωτόκολλα ασφάλειας 802.11i και 802.1x των WLANs 99
5.7.1 WiFi Protected Access της WiFi Alliance (WPA) 100
5.7.1.1 Τρόπος λειτουργίας του πρωτοκόλλου TKIP 101
5.7.2 802.11i / WPA2: Advanced Encryption Standard (AES) 103
5.7.2.1 Ο αλγόριθμος AES – CCMP 104
5.7.3 Υλοποιήσεις των WPA/WPA2 – Personal ή Enterprise; 104

5.7.4 Extensible Authentication Protocol (EAP): 802.1x _____ 105
5.7.4.1 Η διαδικασία της αυθεντικοποίησης με το 802.1x _____ 106
5.7.4.2 Πρωτόκολλα αυθεντικοποίησης του 802.1x _____ 107

Επίλογος _____ 108

Προτάσεις _____ 109

Βιβλιογραφία _____ 110

Ευρετήριο Εικόνων

Σχήμα 2.1: Το φυσικό επίπεδο του 802.11 και τα δυο υποεπίπεδά του 18
Σχήμα 2.2: Μη επικαλυπτόμενα κανάλια 1, 6 και 11 του προτύπου 802.11b 20
Σχήμα 2.3: Η φασματική πυκνότητα ισχύος (PSD) στην τεχνική διασποράς φάσματος..... 22
Σχήμα 2.4: Εξάπλωση ενός σήματος στενής ζώνης με την τεχνική διασποράς φάσματος..... 23
Σχήμα 2.5: Αναπαράσταση της τεχνικής FHSS 26
Σχήμα 2.6: Επιλογή συχνοτήτων στην τεχνική FHSS 26
Σχήμα 2.7: Κύκλοι μεταπηδήσεων στην τεχνική FHSS..... 27
Σχήμα 2.8: Αναπαράσταση της τεχνικής DSSS 30
Σχήμα 2.9: Διασπορά ακολουθίας bits με την τεχνική DSSS 31
Σχήμα 2.10: Παρουσίαση των δεδομένων του σχήματος 2.9 σε παλμούς από bits 32
Σχήμα 2.11: Ανίχνευση πληροφοριών στην τεχνική OFDM 34
Σχήμα 3.1: Το φυσικό και το MAC επίπεδο του προτύπου 802.11 37
Σχήμα 3.2: Οι μέθοδοι πρόσβασης DCF και PCF..... 40
Σχήμα 3.3: Ad hoc δίκτυο..... 41
Σχήμα 3.4: Δίκτυο υποδομής 41
Σχήμα 3.5: Κεφαλίδα του πλαισίου MAC και τα υποπεδία του πεδίου ελέγχου 44
Σχήμα 3.6: Πεδία της κεφαλίδας MAC 47
Σχήμα 3.7: Αυθεντικοποίηση ανοιχτού συστήματος..... 52
Σχήμα 3.8: Αυθεντικοποίηση προμοιρασμένου κλειδιού 53
Σχήμα 4.1: Διαπλαισιακά διαστήματα αναμονής (IFS) 59
Σχήμα 4.2: Χρόνοι αναμονής μετάδοσης πλαισίων 60
Σχήμα 4.3: Το πρόβλημα του κρυφού σταθμού – δίκτυο υποδομής 65
Σχήμα 4.4: Διαδικασία κατάληψης του μέσου από έναν σταθμό σε δίκτυο υποδομής 66
Σχήμα 4.5: Εμβέλεια σταθμών σε δίκτυο ad hoc 67
Σχήμα 4.6: Χειραψία RTS/CTS σε δίκτυο ad hoc 68

Σχήμα 4.7: Το πρόβλημα του εκτεθειμένου σταθμού 69
Σχήμα 4.8: Το πρόβλημα του εκτεθειμένου σταθμού 70
Σχήμα 4.9: Χειραψία RTS/CTS και το πρόβλημα του εκτεθειμένου σταθμού..... 70
Σχήμα 4.10: Η μορφή των πλαισίων ACK, RTS, CTS και DATA..... 73
Σχήμα 5.1: Λειτουργία ενός stream cipher αλγορίθμου..... 89
Σχήμα 5.2: Το πλαίσιο του WEP 92
Σχήμα 5.3: Αναπαράσταση της διαδικασίας κρυπτογράφησης στο WEP 93
Σχήμα 5.4: Η διαδικασία αποκρυπτογράφησης στο WEP 94
Σχήμα 5.5: Το πρότυπο ασφάλειας 802.11i 100

Ευρετήριο Πινάκων

Πίνακας 2.1: Interfaces συχνοτήτων στο πρότυπο 802.11 19
Πίνακας 2.2: Χρήση καναλιών στην τεχνική FHSS 28
Πίνακας 2.3: Επιτρεπόμενα κανάλια εκπομπής με την τεχνική DSSS 29
Πίνακας 3.1: Τιμές για τα πεδία Type/Subtype του frame control 46
Πίνακας 3.2: Διευθύνσεις του 802.11 47
Πίνακας 4.1: Τιμές των χρόνων αναμονής και της χρονικής 57
σχισμής σε κάθε σύστημα μετάδοσης 57
Πίνακας 4.2: Τιμές του παραθύρου υπαναχώρησης στο IEEE 802.11 61
Πίνακας 5.1: Λύσεις ασφάλειας που παρέχονται από τα WLANs 88
Πίνακας 5.3: Σύγκριση των μεθόδων του WEP και του WPA 102

Εισαγωγή

Σήμερα η εξάπλωση των ασύρματων τοπικών δικτύων έχει πάρει τεράστιες διαστάσεις και η ραγδαία τους εξέλιξη έχει επηρεάσει τον τρόπο ζωής μας. Στόχος της εργασίας είναι η κατανόηση των πλεονεκτημάτων που παρέχουν τα WLANs, αλλά και η εισαγωγή σε τεχνικά θέματα όπως η ανάλυση του τρόπου λειτουργίας τους στο φυσικό και το υποεπίπεδο MAC. Επίσης η κατανόηση των ευπαθειών σε θέματα ασφάλειας θα αποτελέσει μια εισαγωγή για την πλήρη αντίληψη των τεχνολογιών ασφάλειας που έχουν αναπτυχθεί και ενισχύουν το επίπεδο προστασίας μας απέναντι σε επιθέσεις από τρίτους. Η εργασία αποτελείται από τα πέντε ακόλουθα μέρη:

Κεφάλαιο 1: Περιλαμβάνει μια ιστορική αναδρομή των ασύρματων τοπικών δικτύων και περιγράφει την εξέλιξή τους από το 1970 μέχρι σήμερα. Αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης τους και γίνονται σύντομες περιγραφές των προτύπων OpenAir, HomeRF, HiperLAN1/2 και βέβαια του προτύπου IEEE 802.11 και των παραλλαγών του.

Κεφάλαιο 2: Γίνεται περιγραφή του φυσικού επιπέδου των ασύρματων τοπικών δικτύων. Αναλύεται η τεχνική της διασποράς φάσματος και επεξηγείται ο τρόπος λειτουργίας των τεχνικών FHSS, DSSS, OFDM καθώς και των υπέρυθρων ακτινών που χρησιμοποιούνται στα ασύρματα δίκτυα.

Κεφάλαιο 3: Αναφέρονται κάποια εισαγωγικά θέματα για το επίπεδο ελέγχου πρόσβασης στο μέσο. Περιγράφονται οι δυο αρχιτεκτονικές των ασύρματων τοπικών δικτύων, δηλαδή τα δίκτυα υποδομής (Infrastracture) και τα αυτοοργανούμενα δίκτυα (Ad Hoc) και γίνεται περιγραφή της μορφής των πλαισίων που ανταλλάσσονται σε ένα ασύρματο δίκτυο. Το κεφάλαιο ολοκληρώνεται με την περιγραφή των διαδικασιών που λαμβάνουν χώρα μέχρι ένας σταθμός να αποκτήσει πλήρη πρόσβαση στο μέσο μετάδοσης (διαδικασίες ανίχνευσης, ενσωμάτωσης, αυθεντικοποίησης και συσχέτισης με ένα δίκτυο).

Κεφάλαιο 4: Αναλύονται οι λειτουργίες του υποεπιπέδου ελέγχου πρόσβασης στο μέσο (MAC). Επεξηγούνται βασικές έννοιες του υποπεπιπέδου όπως οι χρόνοι αναμονής μέχρι να μεταδοθούν τα πλαίσια, το παράθυρο συμφόρησης και έπειτα περιγράφονται οι δυο μέθοδοι που χρησιμοποιούν τα ασύρματα τοπικά δίκτυα για να επιτευχθεί η πρόσβαση των σταθμών στο μέσο, δηλαδή οι μέθοδοι DCF και σπανιότερα η PCF. Επίσης αναφέρονται μέθοδοι που εξασφαλίζουν εξοικονόμηση ενέργειας, μιας και η κατανάλωση της μπαταρίας στους κινητούς σταθμούς είναι ένα σημαντικό ζήτημα.

Κεφάλαιο 5: Το τελευταίο κεφάλαιο εστιάζει σε θέματα ασφάλειας στα ασύρματα τοπικά δίκτυα. Επεξηγούνται τα κενά ασφάλειας και οι ευπάθειές τους, ενώ ακολουθεί ανάλυση των τρόπων με τους οποίους μπορούμε να προστατευτούμε. Περιγράφεται το πρωτόκολλο WEP, το πρότυπο 802.11i και το πρωτόκολλο αυθεντικοποίησης 802.1x.

Κεφάλαιο 1

Ασύρματα τοπικά δίκτυα

1.1 Εισαγωγή

Το παρόν κεφάλαιο αναφέρεται στα ασύρματα τοπικά δίκτυα. Γίνεται μια ιστορική αναδρομή και περιγράφονται τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης τους. Επίσης περιγράφονται συνοπτικά πρωτόκολλα όπως το OpenAir, το HomeRF και άλλα που αναπτύχθηκαν παράλληλα ή έπειτα από το 802.11, όπως τα HiperLan1, HiperLan2. Φυσικά αναφέρονται τα βασικά χαρακτηριστικά της οικογένειας προτύπων 802.11 που σήμερα χρησιμοποιούνται ευρέως.

1.2 Η ιστορία των WLANs

Το 1970, ο Norman Abramson, καθηγητής στο πανεπιστήμιο της Χαβάη, ανέπτυξε το πρώτο παγκόσμιο δίκτυο υπολογιστών το οποίο ονομάζονταν ALOHAnet, χρησιμοποιώντας χαμηλού κόστους ραδιόφωνα. Με μια αμφίδρομη τοπολογία αστέρα, το σύστημα κατάφερε να διασυνδέσει επτά υπολογιστές σε τέσσερα νησιά ώστε να μπορούν να επικοινωνούν με έναν κεντρικό υπολογιστή στο νησί Oahu χωρίς τη χρήση τηλεφωνικών γραμμών.

Το 1979, οι F.R. Gfeller και U. Bapst δημοσίευσαν στην IEEE[1] μια μελέτη παρουσιάζοντας ένα πειραματικό τοπικό ασύρματο δίκτυο που λειτουργούσε με

1 Institute of Electrical and Electronics Engineers

υπέρυθρες ακτίνες. Σύντομα, το 1980 σε συνέδριο της IEEE, ο P. Ferrert υπέβαλε μια έκθεση σχετικά με μια πειραματική εφαρμογή που χρησιμοποιούσε ένα ενιαίο διεσπαρμένο φάσμα για εκπομπή με ασύρματες επικοινωνίες. Το 1984, δημοσιεύθηκε μια σύγκριση μεταξύ των υπέρυθρων ακτίνων και των CDMA[2] επικοινωνιών διεσπαρμένου φάσματος για τα ασύρματα δίκτυα από τον Kaveh Pahlavan στο συνέδριο δικτύωσης υπολογιστών της IEEE, που αργότερα δημοσιεύθηκε στο περιοδικό της IEEE.

Τον Μάιο του 1985, οι προσπάθειες του Michael Marcus οδήγησαν την Ομοσπονδιακή Επιτροπή Επικοινωνιών των ΗΠΑ (FCC[3]) στην αναγγελία των πειραματικών ISM[4] ζωνών για την εμπορική εφαρμογή της τεχνολογίας διασποράς φάσματος, ενώ λίγο αργότερα, ο M. Kavehrad υπέβαλε μια μελέτη σχετικά με το πειραματικό ασύρματο σύστημα PBX χρησιμοποιώντας την τεχνική CDMA. Αυτές οι προσπάθειες συνέβαλλαν στην πραγματοποίηση σημαντικών βιομηχανικών δραστηριοτήτων για την ανάπτυξη μιας νέας γενιάς ασύρματων τοπικών δικτύων που αναθεώρησε διάφορες παλιές απόψεις σχετικά με τη φορητή ραδιοβιομηχανία.

Η πρώτη γενιά ασύρματων modem αναπτύχθηκε στις αρχές της δεκαετίας του 1980. Αυτό που έγινε ήταν η προσθήκη ενός voice band modem με ρυθμούς μετάδοσης κάτω από 9600bps, σε ένα υπάρχον σύστημα ραδιομεταδόσεων για μικρές αποστάσεις. Η δεύτερη γενιά των ασύρματων modem αναπτύχθηκε αμέσως μετά την ανακοίνωση της FCC για τις ISM ζώνες. Αυτά τα modem παρείχαν ρυθμούς μετάδοσης δεδομένων εκατοντάδων Kbps. Η τρίτη γενιά των ασύρματων modem στόχευσε στη συμβατότητα με τα WLANs της εποχής, παρέχοντας ρυθμούς μετάδοσης της τάξης των Mbps. Διάφορες επιχειρήσεις ανέπτυξαν προϊόντα τρίτης γενιάς με ρυθμούς μετάδοσης πάνω από 1 Mbps και μερικά προϊόντα είχαν αναγγελθεί ήδη μέχρι τη διεξαγωγή του πρώτου συνεδρίου της IEEE για τα WLANs (1991).

Παρόλο που τα ασύρματα δίκτυα είχαν αρχίσει να αναπτύσσονται, η

2 Code Division Multiple Access

3 Federal Communications Commission

4 Industrial Scientific and Medical bands

έλλειψη προτύπων οδήγησε στον διχασμό της αγοράς και στην κατασκευή συσκευών που δεν ήταν πάντα συμβατές μεταξύ τους. Η πρώτη προσπάθεια καθορισμού προτύπων έγινε το 1980 από την IEEE και συγκεκριμένα από την ομάδα εργασίας 802.4, η οποία ήταν υπεύθυνη για την ανάπτυξη της μεθόδου προσπέλασης μέσου με μεταβίβαση σκυτάλης (Token Passing). Η ομάδα αυτή κατέληξε στην ακαταλληλότητα της συγκεκριμένης μεθόδου για τα ασύρματα δίκτυα και πρότεινε την ανάπτυξη νέων προτύπων. Τελικά συστάθηκε η ομάδα εργασίας 802.11 η οποία είναι αρμόδια για την ανάπτυξη προτύπων ασύρματων δικτύων που σχετίζονται με το φυσικό και το MAC επίπεδό τους.

Το πρώτο συνέδριο της IEEE για τα WLANs το 1991 στόχευε στην αξιολόγηση των νέων εναλλακτικών τεχνολογιών. Μέχρι εκείνη τη στιγμή τα ασύρματα προϊόντα για τοπικά ασύρματα δίκτυα μόλις είχαν εμφανιστεί στην αγορά και η επιτροπή IEEE 802.11 είχε αρχίσει την ανάπτυξη προτύπων. Μέχρι το 1996, η τεχνολογία ήταν σχετικά ώριμη, ποικίλες εφαρμογές είχαν αναπτυχθεί και είχαν ελεγχθεί ενώ οι τεχνολογίες που χρησιμοποιήθηκαν είχαν ερευνηθεί αρκετά. Τα chipsets για τα WLANs άρχισαν να αναπτύσσονται ραγδαία και να κατακλύζουν την αγορά, ενώ τα WLANs χρησιμοποιούνταν σε νοσοκομεία, χρηματιστήρια, σε κτίρια επιχειρήσεων καθώς και σε πανεπιστήμια για νομαδική πρόσβαση[5], ή ακόμη και σε point-to-point ασύρματες γέφυρες. Το 1997 οριστικοποιήθηκε το πρώτο πρότυπο στης ομάδας 802.11 ενώ το 1999 ορίστηκαν δυο επιπλέον πρότυπα, το 802.11a και 802.11b. Ακολούθησε το 802.11g το 2003 και το 802.11n το 2009.

Το υλικό WLAN ήταν αρχικά τόσο ακριβό που χρησιμοποιούνταν μόνο ως εναλλακτική λύση του ενσύρματου LAN, σε σημεία όπου η εγκατάσταση καλωδίων ήταν δύσκολη ή αδύνατη. Η σταδιακή εξέλιξή του περιέλαβε λύσεις για επιστημονικές και βιομηχανικές εφαρμογές καθώς και πιστοποίηση για πρωτόκολλα για τα οποία δεν υπήρχε κάποια, ενώ η μαζική παραγωγή οδήγησε σε σημαντική μείωση των τιμών.

Τον Ιούλιο του 2005 υπήρξαν τουλάχιστον 68.643 WiFi σημεία πρόσβασης

5 Έτσι ονομάζουμε τον τρόπο πρόσβασης ο οποίος παρέχει ασύρματη σύνδεση μεταξύ ενός φορητού σταθμού και ενός κομβικού σημείου σε ένα τοπικό δίκτυο.

παγκοσμίως, τα περισσότερα στις ΗΠΑ και ακολουθούσαν η Αγγλία και η Γερμανία. Οι ΗΠΑ και η Δυτική Ευρώπη συγκεντρώνουν περίπου το 80% των παγκόσμιων χρηστών WiFi. Ακόμη και με αυτούς τους αριθμούς και την μεγάλη εξάπλωση των ασύρματων τοπικών δικτύων, η πραγματική χρήση WiFi είναι μικρότερη από την αναμενόμενη.

1.3 WiFi (Wireless Fidelity) – Ασύρματη Πιστότητα

Το WiFi είναι το σήμα κατατεθέν της WiFi Alliance το οποίο χρησιμοποιείται από τους κατασκευαστές σε πιστοποιημένα προϊόντα τα οποία αναπτύχθηκαν για ασύρματα τοπικά δίκτυα και λειτουργούν βάσει του 802.11 προτύπου. Εξαιτίας της στενής του σχέσης με το 802.11, ο όρος WiFi πολλές φορές χρησιμοποιείται σαν συνώνυμο της τεχνολογίας 802.11. Η WiFi Alliance είναι μια ένωση από εταιρίες και η αρμοδιότητά της είναι η πιστοποίηση προϊόντων, εφόσον αυτά πληρούν τις προϋποθέσεις που θέτουν τα πρότυπα. Αυτό όμως δεν σημαίνει ότι όσα προϊόντα δεν έχουν την WiFi πιστοποίηση δεν μπορούν να λειτουργούν σωστά με άλλες WiFi-πιστοποιημένες συσκευές.

Ο όρος WiFi μοιάζει με τον όρο HiFi (High Fidelity) που είχε αναπτυχθεί για συσκευές ήχου. Όμως παρά το γεγονός ότι η WiFi Alliance χρησιμοποιεί τον όρο Wireless Fidelity στα επίσημα έγγραφά της και στον τύπο, στην ουσία ο όρος αναπτύχθηκε αρχικά χωρίς να σημαίνει κάτι. Χρησιμοποιήθηκε για πρώτη φορά τον Αύγουστο του 1999 και ήταν ιδέα της εταιρίας Interbrand Corporation την οποία συμβουλεύθηκε η WiFi Alliance προκειμένου να βρεθεί ένα όνομα πιο ελκυστικό από το “IEEE 802.11b Direct Sequence”. Ο όρος Wireless Fidelity ακολούθησε, ώστε η λέξη WiFi να αντιστοιχεί σε κάτι που θα είχε νόημα. [2], [3]

1.4 Ραδιοσυχνότητες – το κλειδί για τη λειτουργία των WLANs

Οι ασύρματες συσκευές έχουν κατασκευαστεί έτσι ώστε να λειτουργούν σε κάποια συγκεκριμένη ζώνη συχνοτήτων. Κάθε τέτοια ζώνη έχει ένα ορισμένο εύρος ζώνης, δηλαδή ένα ορισμένο εύρος καναλιού. Το bandwidth έχει χρησιμοποιηθεί ως μονάδα μέτρησης του μεγέθους της πληροφορίας που μπορεί να αποστέλλεται από ένα κανάλι και μπορούμε να πούμε πως ένα κανάλι με μεγάλο bandwidth μπορεί να μεταφέρει περισσότερες πληροφορίες.

Η χρήση των ραδιοσυχνοτήτων ελέγχεται αυστηρά από κάποιες αρχές μέσω συγκεκριμένων διαδικασιών. Στις ΗΠΑ αυτός ο έλεγχος πραγματοποιείται από την FCC ενώ πολλοί από τους κανονισμούς της έχουν υιοθετηθεί και από άλλες χώρες της Αμερικής. Ο αντίστοιχος οργανισμός για την Ευρώπη είναι το CEPT's ERO[6] και η ITU[7]. Για να αποφευχθούν οι επικαλύψεις, οι συχνότητες χωρίζονται σε ζώνες, οι οποίες ουσιαστικά είναι σύνολα συχνοτήτων που έχουν οριστεί για συγκεκριμένες εφαρμογές. Η ζώνη στην οποία λειτουργούν οι συσκευές του προτύπου 802.11 είναι η ISM, η χρήση της οποίας δεν απαιτεί χορήγηση άδειας, που σημαίνει ότι δεν χρειαζόμαστε άδεια για την εγκατάσταση κάθε ασύρματου τοπικού δικτύου ενώ συνέπεια αυτού ενδέχεται να είναι η ύπαρξη παρεμβολών.

1.5 Πλεονεκτήματα χρήσης των WLANs

Ένα σημαντικό πλεονέκτημα που προσφέρουν τα ασύρματα δίκτυα είναι η *ευκολία εγκατάστασής τους* καθώς και *η μείωση του κόστους και του χρόνου εγκατάστασης* σε σημεία που η καλωδίωση είναι ακριβή ή αδύνατη όπως διατηρητέα κτίρια, ιστορικά μνημεία ή εξωτερικοί χώροι. Σήμερα, όλοι σχεδόν οι φορητοί υπολογιστές διαθέτουν κάρτες ασύρματης δικτύωσης, ενώ το κόστος αυτών των ηλεκτρονικών κυκλωμάτων μειώνεται συνεχώς. Έτσι κυκλώματα για WiFi ενσωματώνονται σε όλο και περισσότερες συσκευές κάνοντάς το μια ευρέως

6 European Radio-communications Office

7 International Telecommunications Union

διαδεδομένη τεχνολογία.

Τα ασύρματα δίκτυα δίνουν *δυνατότητες κίνησης* στους χρήστες τους και η συνεχής ανάπτυξή τους μπορεί να αποδοθεί στην ανάγκη υποστήριξης δικτυακών εφαρμογών που θα είναι διαθέσιμες εν κινήσει. Αυτό βοήθησε πολύ τους εργαζόμενους σε επιχειρήσεις που η εργασία τους απαιτεί μετακίνηση και χρήση φορητών συσκευών, αύξησε την αποδοτικότητά τους αλλά και την παραγωγικότητα των επιχειρήσεων. Σήμερα μπορούν να έχουν πρόσβαση σε δεδομένα που υπάρχουν σε υπολογιστές άλλων χρηστών ή σε κεντρικούς υπολογιστές σε πραγματικό χρόνο, σε οποιοδήποτε σημείο της επιχείρησης κι αν βρίσκονται, με την προϋπόθεση ότι υπάρχει κάλυψη από το ασύρματο δίκτυο.

Πολλές εφαρμογές απαιτούν *ευελιξία στην αλλαγή τοπολογιών* των δικτύων στα οποία χρησιμοποιούνται. Αυτή η ανάγκη μπορεί να υποστηριχθεί από τα ασύρματα δίκτυα, αφού έχουν τη δυνατότητα να αλλάζουν τοπολογίες έτσι ώστε να περιλαμβάνουν από ισότιμα δίκτυα με μικρό αριθμό χρηστών, μέχρι μεγαλύτερα με δυνατότητες περιαγωγής (roaming)[8] που εξυπηρετούν μεγάλο αριθμό χρηστών σε μεγάλες αποστάσεις.

1.6 Τα μειονεκτήματα των WLANs

Τα WiFi δίκτυα έχουν *περιορισμένη ακτίνα εκπομπής*. Ένας δρομολογητής που χρησιμοποιεί το πρότυπο 802.11b ή το 802.11g μπορεί να εκπέμπει σε απόσταση 32m σε εσωτερικούς χώρους και 95m σε εξωτερικούς, σε αντίθεση με το νέο πρότυπο 802.11n που μπορεί ακόμη και να διπλασιάσει αυτές τις αποστάσεις. Ωστόσο, η μέγιστη απόσταση εκπομπής εξαρτάται και από το εύρος συχνοτήτων που χρησιμοποιείται, έτσι στη ζώνη των 2.4GHz έχουμε καλύτερη κάλυψη από εκείνη στη ζώνη των 5GHz. Επίσης, η κάλυψη σε εξωτερικούς χώρους μπορεί να βελτιωθεί με τη χρήση κατευθυντικών κεραιών που μπορούν να

8 Πρόκειται για έναν όρο που αναφέρεται στην επέκταση κάποιων υπηρεσιών διασύνδεσης σε περιοχή διαφορετική από εκείνη όπου έχει οριστεί η λειτουργία. Επίσης εγγυάται ότι η ασύρματη συσκευή θα παραμείνει συνδεδεμένη στο δίκτυο χωρίς να υπάρξει απώλεια σύνδεσης.

τοποθετηθούν αρκετά χιλιόμετρα μακριά από τη βάση μας.

Προκειμένου να ικανοποιηθούν οι απαιτήσεις των ασύρματων τοπικών εφαρμογών, το *WiFi καταναλώνει μεγάλα ποσά ενέργειας* σε σύγκριση με άλλες τεχνολογίες, γεγονός που σχετίζεται άμεσα με την μπαταρία των φορητών συσκευών. Το Bluetooth το οποίο παρέχει κάλυψη σε πολύ μικρότερες περιοχές (κάτω των 10m) έχει γενικά μικρή ενεργειακή κατανάλωση. Επίσης το πρότυπο ZigBee έχει και αυτό μικρή ενεργειακή κατανάλωση, αλλά παρόλο που μπορεί να εκπέμπει σε μεγαλύτερες αποστάσεις, οι ρυθμοί μετάδοσης δεδομένων είναι χαμηλοί. [3]

Οι *παρεμβολές* από γειτονικά δίκτυα ή οικιακές συσκευές που λειτουργούν στην ίδια ζώνη συχνοτήτων όπως φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα, κάμερες παρακολούθησης, συσκευές των προτύπων ZigBee και Bluetooth, είναι πιθανόν να επηρεάσουν την αποδοτικότητα των WLANs. Επίσης, στην περίπτωση που πολλοί χρήστες στην ίδια περιοχή χρησιμοποιούν ένα ασύρματο δίκτυο (το ίδιο ή ακόμη και διαφορετικό), το κανάλι μετάδοσης δεδομένων μπορεί να υπερφορτωθεί.

1.7 Κινδυνεύουμε από τη χρήση ασύρματων συσκευών;

Ένα σημαντικό ζήτημα για τα WLANs, η απάντηση του οποίου εκκρεμεί, είναι η πιθανότητα εμφάνισης προβλημάτων υγείας που ενδεχομένως προκαλεί η έκθεσή μας στην εκπομπή ραδιοσυχνοτήτων. Η ύπαρξη μη τεκμηριωμένων ενδείξεων έχουν συνδέσει την έκθεση στις ραδιοσυχνότητες με ασθένειες που μπορεί να είναι σοβαρές, όπως η αυξανόμενη εμφάνιση ορισμένων μορφών καρκίνου, αλλά και λιγότερο σοβαρές, όπως πονοκέφαλοι, οξυθυμία και απώλεια συγκέντρωσης.

Αυτή τη στιγμή δεν υπάρχει κάποιο επίσημο στοιχείο που να καθιστά την έκθεση στις ραδιοσυχνότητες υπεύθυνη, ωστόσο η έλλειψη στοιχείων δεν θα πρέπει να μειώνει την ανησυχία μας. Μερικές από τις εκθέσεις που κυκλοφορούν, προσδιορίζουν ασθένειες όπως η οξυθυμία ή η απώλεια συγκέντρωσης που θα ήταν δύσκολο να τεκμηριωθούν. Επιπλέον, μια καλή επιστημονική μελέτη θα

απαιτούσε την απομόνωση κάποιων παραγόντων ώστε να εξεταστεί ο αντίκτυπος της έκθεσης στις διαφορετικές ραδιοσυχνότητες, σε διαφορετικά επίπεδα ενέργειας, σε διαφορετικές διάρκειες έκθεσης και στα διαφορετικά στάδια της ζωής ενός ανθρώπου.

Αυτό που μπορούμε να πούμε όσον αφορά στην ασφάλεια μας είναι ότι πρόκειται για ένα ζήτημα που πρέπει να ερευνηθεί. Η επιστημονική κοινότητα θα πρέπει να παρέχει χρήσιμες πληροφορίες σχετικά με τη φύση και την ένταση των κινδύνων προτού πάρουμε σημαντικά μέτρα προστασίας. Προς το παρόν, οι περισσότεροι χρήστες δεν δείχνουν πρόθυμοι να αρνηθούν την ευκολία που τους προσφέρουν οι ραδιοεπικοινωνίες παρά τις ανησυχίες.

1.8 OpenAir

Το OpenAir είναι ένα πρωτόκολλο που αναπτύχθηκε από την εταιρία Proxim με στόχο την παροχή μιας εναλλακτικής λύσης για το 802.11. Η Proxim είναι ένας από τους μεγαλύτερους κατασκευαστές ασύρματων τοπικών δικτύων και είναι η μόνη που κατέχει όλες τις λεπτομέρειες για το OpenAir, καθώς τα περισσότερα προϊόντα τα οποία το υποστηρίζουν βασίζονται στο πρότυπό της.

Το OpenAir είναι πρωτόκολλο που χρησιμοποιεί διασπορά φάσματος με μεταπήδηση συχνότητας (FHSS) και υποστηρίζει ρυθμούς μετάδοσης δεδομένων 0.8 και 1.6 Mbps. Το πρωτόκολλο του MAC επιπέδου είναι το CSMA/CA με χρήση μηχανισμού επαναποστολών και είναι βασισμένο σε μεγάλο βαθμό στον μηχανισμό RTS/CTS. Ένα σημαντικό χαρακτηριστικό του OpenAir είναι ότι τα σημεία πρόσβασης μπορούν αρχικά να αποστέλλουν όλη την κίνηση χωρίς να χρησιμοποιούν ανταγωνισμό (contention free periods) και έπειτα να αλλάζουν ξανά σε ανταγωνιστικό τον τρόπο πρόσβασης στο κανάλι. Παρά τους χαμηλούς ρυθμούς μετάδοσης, το αναφέρουμε για ιστορικούς λόγους.

1.9 HomeRF

Το HomeRF είναι ένα πρότυπο ασύρματης δικτύωσης συσκευών που αναπτύχθηκε το 1998 από μια ομάδα μεγάλων επιχειρήσεων που αποτελούνταν από τη Siemens, τη Motorola, τη Philips κ.ά., προκειμένου να προωθηθεί η χρήση του ασύρματου τοπικού δικτύου σε χώρους όπως το σπίτι και το γραφείο. Η ομάδα αυτή διαλύθηκε το 2003, έπειτα από τη δυναμική είσοδο του προτύπου 802.11b σε οικίες και εφόσον η Microsoft είχε αρχίσει να συμπεριλαμβάνει την υποστήριξη του Bluetooth στα Windows, πρότυπο με το οποίο το HomeRF ανταγωνίζονταν.

Το HomeRF χρησιμοποιούσε τη διασπορά φάσματος με μεταπήδηση συχνότητας (FHSS), λειτουργούσε στη ζώνη των 2.4GHz και υποστήριζε ρυθμούς μετάδοσης δεδομένων μέχρι και 10Mbps. Κάθε σταθμός μπορούσε να απομακρυνθεί μέχρι και 50m από το σημείο πρόσβασης χωρίς να διακοπεί η σύνδεσή του με αυτό. Επίσης το πρότυπο επιτρέπει την ανταλλαγή δεδομένων και τηλεφωνικών σημάτων, έτσι ένα ασύρματο τηλέφωνο και ένας φορητός υπολογιστής μπορούν να μοιράζονται το ίδιο εύρος συχνοτήτων.

1.10 Το πρότυπο HiperLAN

Το HiperLAN (High Performance Radio LAN) είναι ένα πρότυπο ασύρματης δικτύωσης για τοπικά δίκτυα που αναπτύχθηκε από τον ευρωπαϊκό οργανισμό ETSI[9] σαν μια εναλλακτική λύση για το πρότυπο 802.11 που είχε αρχίσει να αναπτύσσεται εκείνη την εποχή.

1.10.1 HiperLAN/1

Η πρώτη έκδοση του προτύπου άρχισε να αναπτύσσεται το 1991, ονομάστηκε HiperLAN/1 και στόχος της ήταν η υποστήριξη υψηλότερων ρυθμών μετάδοσης δεδομένων από εκείνους του 802.11. Το πρότυπο καλύπτει το φυσικό

9 European Telecommunications Standards Institute

και το επίπεδο ελέγχου πρόσβασης στο μέσο (MAC), ενώ υπάρχει ένα νέο υποεπίπεδο που ονομάζεται CAC (Channel Access and Control) και ασχολείται με τα αιτήματα προσπέλασης του καναλιού. Η ικανοποίηση ενός τέτοιου αιτήματος εξαρτάται από το βαθμό χρήσης του καναλιού τη δεδομένη στιγμή καθώς και από την προτεραιότητα του αιτήματος.

Το υποεπίπεδο CAC παρέχει ιεραρχία με τη βοήθεια του πρωτοκόλλου ελέγχου πρόσβασης στο κανάλι EY-NPMA (Elimination-Yield Non-Preemptive Multiple Access). Αυτό το πρωτόκολλο επιτρέπει στο δίκτυο να λειτουργεί με μικρό αριθμό συγκρούσεων, ακόμη και αν ο αριθμός των χρηστών είναι πολύ μεγάλος. Το HiperLAN επιλέγεται συχνά για υποστήριξη πολυμεσικών εφαρμογών καθώς το πρωτόκολλο EY-NPMA χρησιμοποιεί προτεραιότητες. Στο επίπεδο MAC χρησιμοποιούνται πρωτόκολλα δρομολόγησης, ασφάλειας και εξοικονόμησης ενέργειας.

Στο φυσικό επίπεδο του προτύπου χρησιμοποιούνται οι κωδικοποιήσεις FSK[10] και GMSK[11] και είναι ένα πρότυπο που δεν παρουσιάζει παρεμβολές από μικροκυματικές και άλλες οικιακές συσκευές που λειτουργούν στα 2.4GHz, καθώς λειτουργεί στα 5GHz. Σαν βασικά χαρακτηριστικά του προτύπου μπορούμε να αναφέρουμε τα εξής:

- περιοχή κάλυψης: 50m
- υποστήριξη σύγχρονης και ασύγχρονης κίνησης
- ρυθμός μετάδοσης ήχου: 32Kbps
- ρυθμός μετάδοσης video: 2Mbps
- ρυθμός μετάδοσης δεδομένων: 10Mbps

1.10.2 HiperLAN/2

Το HiperLAN/2 έγινε αποδεκτό τον Φεβρουάριο του 2000. Η δεύτερη έκδοση σχεδιάστηκε για να υποστηρίξει ασύρματες συνδέσεις υψηλών ταχυτήτων

10 Frequency Shift Keying

11 Gaussian Minimum Shift Keying

για διάφορα είδη δικτύων, όπως το UMTS[12], το ATM[13] και τα δίκτυα IP. Επίσης λειτουργεί σε οικιακά δίκτυα όπως και το HiperLAN/1 και χρησιμοποιεί τη ζώνη συχνοτήτων των 5GHz, υποστηρίζοντας ρυθμούς μετάδοσης δεδομένων μέχρι και 54Mbps.

Το φυσικό επίπεδο του προτύπου είναι παρόμοιο με εκείνο του 802.11a και οι κωδικοποιήσεις που χρησιμοποιούνται είναι οι BPSK, QPSK, 16QAM και 64QAM. Ωστόσο το επίπεδο MAC χρησιμοποιεί το πρωτόκολλο Dynamic TDMA. Οι βασικές λειτουργίες που επιτελεί το πρότυπο είναι η μετάδοση δεδομένων, ήχου και video ενώ δίνεται ιδιαίτερη έμφαση στην ποιότητα των παρεχόμενων υπηρεσιών (QoS). Επίσης, το επίπεδο ασφάλειας που παρέχει το πρότυπο είναι αρκετά καλό, καθώς τα δεδομένα προστατεύονται από τους αλγορίθμους DES και 3DES, ενώ τα σημεία πρόσβασης και οι σταθμοί αυθεντικοποιούνται μεταξύ τους.

1.11 Το πρότυπο IEEE 802.11

Το 802.11 είναι ένα σύνολο προτύπων που δημιουργήθηκαν από την IEEE για να υποστηρίζουν επικοινωνίες σε ασύρματα τοπικά δίκτυα σε συχνότητες 2.4 και 5GHz. Οι τεχνικές διαμόρφωσης των σημάτων που μεταδίδονται μέσω του αέρα και χρησιμοποιούνται από το πρότυπο, βασίζονται όλες στη διασπορά φάσματος. Οι γνωστότερες από αυτές χρησιμοποιούνται στα πρότυπα 802.11b/g που είναι τροποποιήσεις του βασικού πρωτοκόλλου 802.11.

Το 1997 ήταν η χρονιά που το 802.11 καθιερώθηκε ως το πρώτο πρότυπο ασύρματης δικτύωσης. Το 802.11b ήταν το πρώτο πρότυπο που έγινε ευρέως αποδεκτό, ενώ ακολούθησαν τα 802.11g και 802.11n. Όσο αφορά στην ασφάλεια των ασύρματων δικτύων, αρχικά ήταν ένα αδύναμο σημείο τους αλλά με την ανάπτυξη του προτύπου 802.11i δεν αποτελεί πλέον μεγάλο πρόβλημα.

Τα πρότυπα 802.11b και 802.11g χρησιμοποιούν την ζώνη συχνοτήτων των 2.4GHz και εξαιτίας αυτής της επιλογής είναι πιθανόν οι συσκευές που βασίζονται

12 Universal Mobile Telecommunications System

13 Asynchronous Transfer Mode

σε αυτά τα πρότυπα να δέχονται περιστασιακά παρεμβολές από φούρνους μικροκυμάτων, ασύρματα τηλέφωνα, συσκευές Bluetooth κ.ά. Όμως το πρότυπο 802.11 μετριάζει τις παρεμβολές χρησιμοποιώντας τεχνικές διασποράς φάσματος όπως θα αναλύσουμε στο επόμενο κεφάλαιο.

1.11.1 IEEE 802.11 – 1997

Η πρώτη έκδοση του προτύπου δημιουργήθηκε το 1997 και σήμερα θεωρείται απαρχαιωμένη. Υποστηρίζει δυο διαφορετικούς ρυθμούς δεδομένων, 1 και 2Mbps με FEC[14]. Ορίζει τρεις διαφορετικές τεχνολογίες φυσικού επιπέδου, τις υπέρυθρες ακτίνες που λειτουργούν στο 1Mbps, την διασπορά φάσματος με μεταπήδηση συχνότητας (FHSS) στο 1 ή στα 2Mbps και τη διασπορά φάσματος άμεσης ακολουθίας (DSSS) επίσης στο 1 ή στα 2Mbps. Οι δυο τελευταίες τεχνολογίες χρησιμοποιούν μικροκύματα στα 2.4GHz της ISM ζώνης.

1.11.2 IEEE 802.11a

Το πρότυπο 802.11a χρησιμοποιεί το ίδιο πρωτόκολλο για το επίπεδο ζεύξης δεδομένων και τα πλαίσια έχουν τη μορφή που έχουν και στο 802.11, αλλά χρησιμοποιεί το OFDM φυσικό επίπεδο. Λειτουργεί στη ζώνη των 5GHz με μέγιστο ρυθμό μετάδοσης δεδομένων τα 54Mbps και χρησιμοποιεί κώδικα διόρθωσης λαθών.

Η χρήση της ζώνης συχνοτήτων των 5GHz κάνει το 802.11a να πλεονεκτεί έναντι των προτύπων που χρησιμοποιούν τη συνωστισμένη ζώνη των 2.4GHz. Ωστόσο αυτό έχει και μειονεκτήματα, καθώς η περιοχή εκπομπής σημάτων σε αυτές τις συχνότητες είναι μικρότερη από εκείνη των προτύπων 802.11b/g. Τα σήματα του 802.11a απορροφόνται πιο εύκολα από τοίχους και άλλα στέρεα υλικά με αποτέλεσμα να μην μπορούν τα φτάσουν τόσο μακριά όσο εκείνα του προτύπου 802.11b. Πρακτικά, το πρότυπο 802.11b έχει μεγαλύτερη εμβέλεια σε

14 Forward Error Correction

χαμηλές ταχύτητες, δηλαδή μπορεί να μειώσει τους ρυθμούς μετάδοσης στα 5Mbps ή ακόμη και στο 1Mbps όταν το σήμα δεν είναι δυνατό. Ωστόσο, σε υψηλότερες ταχύτητες το 802.11a συνήθως έχει την ίδια ή και μεγαλύτερη εμβέλεια εξαιτίας των μικρών παρεμβολών.

1.11.3 IEEE 802.11b

Ο μέγιστος ρυθμός μετάδοσης δεδομένων στο πρότυπο 802.11b είναι τα 11Mbps και χρησιμοποιείται η ίδια μέθοδος πρόσβασης στο μέσο με το 802.11 (CSMA/CA). Τα πρώτα προϊόντα που βασίζονταν σε αυτό το πρότυπο εμφανίστηκαν στην αγορά στις αρχές του 2000. Η μεγάλη αύξηση της ρυθμοαπόδοσης του 802.11b σε συνδυασμό με την πτώση των τιμών του απαιτούμενου εξοπλισμού, κατέστησαν το πρότυπο ευρέως αποδεκτό. Μειονέκτημά του είναι η εμφάνιση παρεμβολών λόγω της λειτουργίας του στα 2.4GHz.

1.11.4 IEEE 802.11g

Το πρότυπο 802.11g εμφανίστηκε το 2003, χρησιμοποιεί και αυτό τη ζώνη των 2.4GHz, αλλά την τεχνική OFDM για τη μετάδοση σημάτων. Μεταδίδει δεδομένα με ταχύτητα 54Mbps με κώδικα διόρθωσης σφαλμάτων ενώ η ρυθμοαπόδοσή του υπολογίζεται περίπου στα 22Mbps κατά μέσο όρο. Το υλικό στο οποίο υλοποιείται το πρότυπο είναι πλήρως συμβατό με το πρότυπο 802.11b.

Από το καλοκαίρι του 2003, τα περισσότερα προϊόντα που υποστήριζαν τα δυο πρότυπα 802.11a/b, υποστήριζαν πλέον και το 802.11g. Ωστόσο, τεχνικά η διαδικασία παράλληλης λειτουργίας δικτύων που είχαν συσκευές με τα πρότυπα 802.11b/g ήταν αρκετά χρονοβόρα. Σε ένα δίκτυο 802.11g, η λειτουργία συσκευών που βασίζονται στο 802.11b μειώνει τον συνολικό ρυθμό μετάδοσης σε όλο το δίκτυο με αποτέλεσμα την επιβάρυνσή του. Τέλος, όπως και οι 802.11b συσκευές, έτσι και οι συσκευές του 802.11g επηρεάζονται από τις παρεμβολές που

δημιουργούνται άλλες συσκευές στα 2.4GHz.

1.11.5 IEEE 802.11n

Πρόκειται για μια πρόσφατη τροποποίηση του 802.11 που βελτιώνει τα προηγούμενα πρότυπα, καθώς χρησιμοποιεί την τεχνική υψηλής ρυθμοαπόδοσης MIMO (multiple-input / multiple-output) και αρκετά άλλα νέα χαρακτηριστικά. Το πρότυπο έγινε αποδεκτό από την IEEE και ανακοινώθηκε τον Οκτώβριο του 2009. Πριν από την τελική επικύρωσή του από την IEEE, χρησιμοποιούνταν ήδη από πολλές εταιρίες, οι οποίες βασίζονταν στην WiFi πιστοποίηση μιας προσωρινής έκδοσής του.

Επίλογος

Το παρόν κεφάλαιο ήταν μια εισαγωγή για τα ασύρματα τοπικά δίκτυα και ουσιαστικά αποτελεί μια ιστορική αναδρομή περιγράφοντας τα διάφορα στάδια που πέρασαν τα WLANs μέχρι τις σημερινές και ευρέως χρησιμοποιούμενες τεχνολογίες τους. Το επόμενο κεφάλαιο αναφέρεται σε περισσότερο τεχνικά θέματα και συγκεκριμένα ασχολείται με το φυσικό επίπεδο των WLANs.

Κεφάλαιο 2

Το Φυσικό Επίπεδο του προτύπου IEEE 802.11

2.1 Εισαγωγή

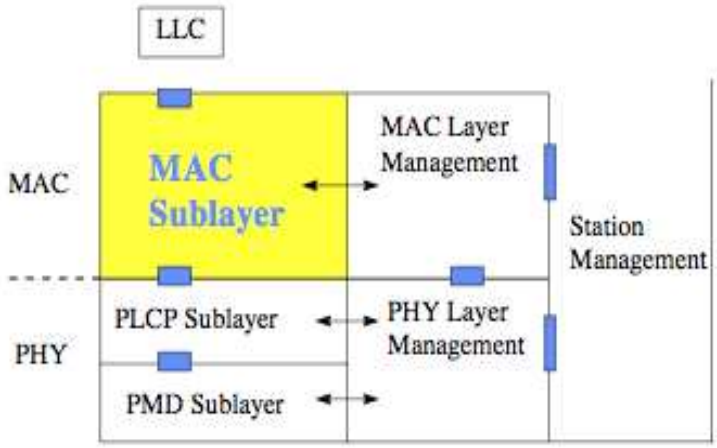
Ένα σημαντικό συστατικό της αρχιτεκτονικής του προτύπου 802.11 είναι το φυσικό επίπεδο. Σε αυτό το κεφάλαιο αναλύονται οι τεχνικές που χρησιμοποιούνται στο φυσικό επίπεδο, καθώς επίσης η διασπορά φάσματος και με περισσότερη λεπτομέρεια οι τεχνικές FHSS, DSSS και OFDM.

2.2 Το φυσικό επίπεδο του προτύπου IEEE 802.11

Το φυσικό επίπεδο του προτύπου χωρίζεται σε δυο τμήματα, το φυσικό επίπεδο σύγκλισης (Physical Layer Convergence Procedure – PLCP) και τα φυσικά υποεπίπεδα που εξαρτώνται από το μέσο (Physical Medium Depent sublayers – PMD). Το PLCP ασχολείται με την προετοιμασία των δεδομένων που προορίζονται για αποστολή ή λήψη χρησιμοποιώντας διάφορες τεχνικές πρόσβασης στο μέσο, ενώ το PMD προετοιμάζει δεδομένα που πρόκειται να αποσταλούν και να παραληφθούν διαμορφώνοντας και αποδιαμορφώνοντας τα πλαίσια που μεταδίδονται, επεμβαίνοντας άμεσα σε αυτά αφού μεταδίδονται στον αέρα, φυσικά μέσω της λήψης οδηγιών από το PLCP. [4]

Επιπλέον, το PLCP βρίσκεται σε συνεχή αλληλεπίδραση με το PMD

προκειμένου τα PSDUs (Physical layer Service Data Unit) να μεταδίδονται μέσω του αέρα. Από μόνο του το PMD επικοινωνεί άμεσα με το μέσο μετάδοσης και αυτό το επιτυγχάνει μέσω μιας SAP διασύνδεσης (Service Access Point) η οποία έχει την ικανότητα να επιτελεί λειτουργίες χαμηλού επιπέδου. Έτσι, τα δεδομένα που λαμβάνονται μορφοποιούνται από το PMD ώστε να μπορούν να αναγνωστούν από το PLCP. [7]



Σχήμα 2.1: Το φυσικό επίπεδο του 802.11 και τα δυο υποεπίπεδά του

Τα φυσικά επίπεδα για το πρότυπο 802.11 ήταν τα εξής τρία [4]:

- Frequency Hopping Spread Spectrum radio (FHSS) PHY
- Direct Sequence Spread Spectrum radio (DSSS) PHY
- Infrared light (IR) PHY

Στη συνέχεια προστέθηκαν τα και τα ακόλουθα:

- 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) PHY
- 802.11b: High Rate Direct Sequence (HR/DS ή HR/DSSS) PHY
- 802.11g: Extended Rate PHY (ERP)
- 802.11n: Υψηλής ρυθμοαπόδοσης MIMO PHY (multiple-input / multiple-output)

Η χρήση συχνοτήτων είναι το κλειδί για τη λειτουργία των ασύρματων δικτύων εφόσον κάθε δεδομένο μεταδίδεται μέσω αυτών. Γενικά, καθένα από τα πέντε πρότυπα που χρησιμοποιούνται στα WLANs χαρακτηρίζεται από κάποιους ρυθμούς μετάδοσης bits (bit rate) καθώς και από ρυθμούς λήψης δεδομένων (fallback rates). Ο πίνακας που ακολουθεί δείχνει αυτούς τους ρυθμούς για τα πρότυπα 802.11, 802.11b, 802.11g, 802.11a και 802.11n. [1]

Πίνακας 2.1: Interfaces συχνοτήτων στο πρότυπο 802.11

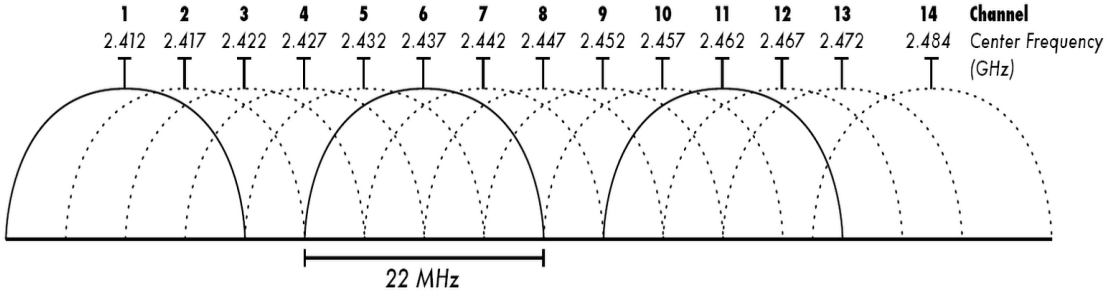
Πρότυπο	Μέγιστος ρυθμός μετάδοσης bit (Mbps)	Ρυθμός λήψης δεδομένων (Mbps)	Χωρητικότητα καναλιού (bandwidth)	Πλήθος μη επικαλυπτόμενων καναλιών	Συχνότητα μετάδοσης
802.11	2	2, 1	20MHz	5	2.4GHz
802.11b	11	5.5, 2, 1	22MHz	3	2.4GHz
802.11g	54	48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1	20MHz	3	2.4GHz
802.11a	54	48, 36, 24, 18, 12, 9, 6	20MHz	23	5GHz
802.11n	≤ 289 στα 20MHz ≤ 600 στα 40MHz	Κάτω από 6.5 στα 20MHz	20MHz 40MHz	2 στα 2.4GHz 11 στα 5GHz	2.4GHz 5GHz

Εάν χρησιμοποιούμε τα πρότυπα 802.11b και 802.11g είναι πολύ πιθανό να έχουμε παρεμβολές από άλλες συσκευές που λειτουργούν και αυτές στη ζώνη των 2.4GHz όπως ασύρματα τηλέφωνα, ηλεκτρονικές συσκευές για το άνοιγμα πορτών, αλλά μπορεί ακόμη να έχουμε επιρροές και από WLANs που χρησιμοποιούν άλλοι χρήστες κοντά στην οικία μας και μπορούν να μειώσουν την αποδοτικότητα του δικού μας δικτύου ή ακόμη να διακόψουν τη σύνδεσή μας. Επίσης υπάρχει περίπτωση η εμβέλεια του δικτύου μας να είναι μειωμένη εξαιτίας τοίχων και ορόφων σε μια πολυκατοικία. Για αυτούς τους λόγους η ζώνη συχνοτήτων των 2.4GHz χωρίζεται σε περαιτέρω ζώνες (κάτι ανάλογο με τα

τηλεοπτικά κανάλια) και έχουμε τη δυνατότητα να επιλέξουμε σε ποιο κανάλι θα δουλεύει το ασύρματο δίκτυό μας ώστε να έχουμε λιγότερες παρεμβολές.

Όπως φαίνεται και στο σχήμα 2.2, στο πρότυπο 802.11b το εύρος κάθε καναλιού είναι στα 22MHz και τα διαθέσιμα κανάλια είναι 13[15]. Τρία όμως από αυτά δεν επικαλύπτονται μεταξύ τους και είναι το 1, το 6 και το 11. Επίσης είναι σημαντικό να αναφέρουμε ότι εάν χρησιμοποιούμε τα πρότυπα 802.11b ή 802.11g, όταν εκπέμπουμε σε κάποιο κανάλι, τα γειτονικά κανάλια που επικαλύπτονται περισσότερο είναι τέσσερα, δηλαδή αν χρησιμοποιούμε το κανάλι 6 τότε θα επικαλύπτουμε τα διπλανά 3, 4, 5 και 7, 8, 9. [7]

Ενώ κάθε κανάλι του προτύπου 802.11g έχει εύρος 20MHz και όχι 22MHz όπως στο 802.11b, η IEEE θα μπορούσε να "συμπιέσει" τα κανάλια του προτύπου g ώστε τα μη επικαλυπτόμενα στη ζώνη των 2.4GHz να είναι τέσσερα αντί για τρία. Ωστόσο, επειδή την περίοδο της εμφάνισης του 802.11g είχαν ήδη αναπτυχθεί ευρέως προϊόντα που βασίζονταν στο 802.11b, τα κανάλια 1, 6 και 11 χρησιμοποιούνται και στο πρότυπο 802.11g. [1]



Σχήμα 2.2: Μη επικαλυπτόμενα κανάλια 1, 6 και 11 του προτύπου 802.11b

2.3 Διασπορά Φάσματος (Spread Spectrum)

Η τεχνολογία διασποράς φάσματος αναπτύχθηκε αρχικά για στρατιωτικές εφαρμογές προκειμένου να γίνει εφικτή η μετάδοση σημάτων σε ζώνες μεγάλου

15 Στη Βόρεια Αμερική τα κανάλια εκπομπής είναι 11, στην Ευρώπη ο ETSI έχει ορίσει 13, ενώ στην Ιαπωνία η TELEC έχει ορίσει 14 κανάλια προς χρήση με 4 μη επικαλυπτόμενα.

εύρους συχνοτήτων, αλλά και να γίνει δυσκολότερη η υποκλοπή και η εσκεμμένη παρεμβολή τρίτων. Αυτή τη στιγμή η τεχνική χρησιμοποιείται στις δορυφορικές επικοινωνίες, σε συστήματα εντοπισμού θέσεως, συστήματα τηλεμετρίας, 3G συστήματα κινητής τηλεφωνίας, στο WiMAX, στο Bluetooth και φυσικά στα τοπικά ασύρματα δίκτυα.

- **ISM μπάντες**

Το 1985 η FCC όρισε τις τρεις ISM μπάντες (Industrial, Scientific and Medical radio bands) που για τη χρήση τους δεν απαιτείται χορήγηση άδειας και το εύρος συχνοτήτων τους είναι 902 έως 928 MHz, 2400 έως 2483.5 MHz και 5725 έως 5850 MHz.

Αυτές οι ζώνες συχνοτήτων αναπτύχθηκαν προκειμένου να ξεπεραστούν κάποια προβλήματα όπως η αναμονή για την χορήγηση άδειας από τις αρμόδιες αρχές, καθώς και η μη ανάθεση του εύρους ζώνης που επιθυμεί κανείς (αυτό συμβαίνει σε περιπτώσεις που ένα προϊόν είναι νέο με αμφίβολη επιτυχία στην αγορά και οι αρχές δεν χορηγούν εύκολα άδεια για κάποιο συγκεκριμένο εύρος ζώνης).

Ωστόσο το μειονέκτημα της μη χορήγησης άδειας χρήσεως είναι ότι καθένας μπορεί να δέχεται παρεμβολές από χρήστες που εκπέμπουν στην ίδια μπάντα. Έτσι για να αποφευχθούν οι υπερβολικές παρεμβολές έχουν οριστεί προδιαγραφές που πρέπει να ακολουθούνται από τα προϊόντα, οι σημαντικότερες εκ των οποίων είναι η χρήση της διασποράς φάσματος και η μετάδοση με χαμηλή ισχύ.

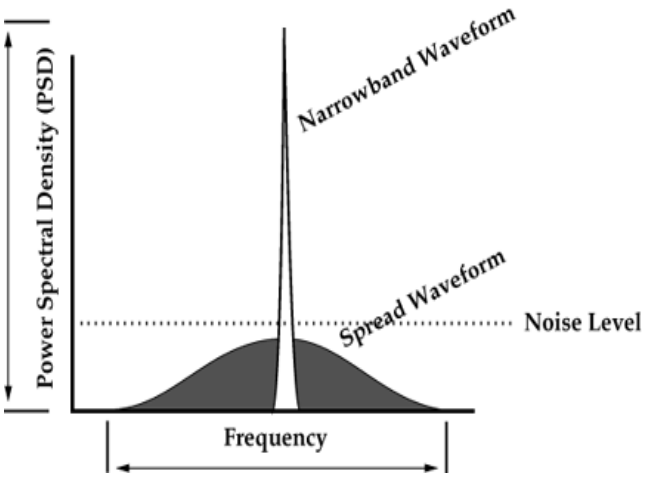
- **Παράγοντας Διασποράς**

Μια παράμετρος-κλειδί για τη διασπορά φάσματος αποτελεί ο παράγοντας διασποράς και ουσιαστικά είναι αναλογία μεταξύ του bandwidth του διεσπαρμένου σήματος και του bandwidth της πληροφορίας και σύμφωνα με τους κανόνες της FCC, η λειτουργία σε αυτές της συχνότητες απαιτεί από τον αποστολέα να

χρησιμοποιεί την διασπορά φάσματος με μεταδιδόμενη ενέργεια κάτω του ενός watt και ο παράγοντας διασποράς να είναι μεγαλύτερος του 10. [9]

$$\textit{παράγοντας διασποράς} = N = \frac{\textit{Bandwidth διεσπαρμένου σήματος}}{\textit{Bandwidth πληροφορίας}} \quad (2.1)$$

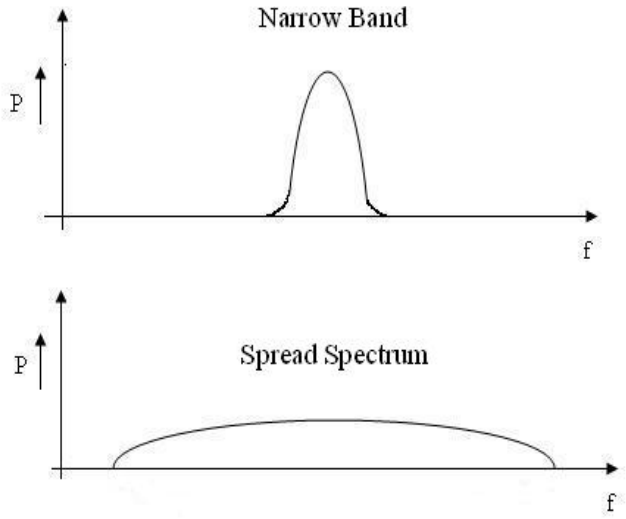
Πρακτικά, ο αριθμός *N* είναι ένας ακέραιος με τιμή $10\log_{10}N = 10$ έως 30dB. Ο παράγοντας διασποράς είναι σημαντικός για τις τεχνικές διασποράς φάσματος διότι δείχνει ότι η μεταδιδόμενη ενέργεια διασπείρεται στο εύρος ζώνης *N* φορές ευρύτερα απ' ότι ο ρυθμός μετάδοσης της πληροφορίας. Όπως φαίνεται και στο παρακάτω σχήμα, χωρίς να μεταβάλλουμε την ενέργεια του σήματος, η φασματική πυκνότητα ισχύος του σήματος (power spectral density -PSD) είναι *N* φορές μικρότερη από εκείνη που θα ήταν αν δεν χρησιμοποιούσαμε την τεχνική διασποράς φάσματος και έτσι το σήμα έχει μικρότερες πιθανότητες ανίχνευσης από τρίτους. [9]



Σχήμα 2.3: Η φασματική πυκνότητα ισχύος (PSD) στην τεχνική διασποράς φάσματος

- **Τρόπος λειτουργίας της διασποράς φάσματος**

Στη διασπορά φάσματος χρησιμοποιείται ένας κωδικοποιητής από τον οποίο περνούν όλα τα δεδομένα που πρόκειται να μεταδοθούν. Ο κωδικοποιητής χρησιμοποιεί ένα φέρον σήμα ώστε να παράγει ένα αναλογικό σήμα στενής ζώνης, που ανήκει σε κάποια συγκεκριμένη συχνότητα. Έπειτα γίνεται εξάπλωση αυτού του σήματος (σχήμα 2.4) από έναν διαμορφωτή ο οποίος για να το πετύχει αυτό, κάνει χρήση μιας ψευδοτυχαίας ακολουθίας αριθμών (pseudorandom noise). Η ακολουθία αυτή παράγεται από μια γεννήτρια τυχαίων αριθμών που χρησιμοποιεί μια αρχική τιμή (φύτρο) ως είσοδο. Ωστόσο οι αριθμοί της ακολουθίας δεν είναι απόλυτα τυχαίοι επειδή ο αλγόριθμος παραγωγής τους είναι ντετερμινιστικός.



Σχήμα 2.4: Εξάπλωση ενός σήματος στενής ζώνης με την τεχνική διασποράς φάσματος

Η ιδέα είναι παρόμοια και για τον παραλήπτη, ο οποίος προκειμένου να ανακτήσει το αρχικό αναλογικό σήμα, εφαρμόζει μια ακολουθία ψευδοτυχαίων αριθμών (την ίδια που χρησιμοποιήθηκε και από τον διαμορφωτή στον αποστολέα) και αποδιαμορφώνει το εξαπλωμένο σήμα ώστε να γίνει ανάκτηση του αρχικού αναλογικού σήματος στενής ζώνης. [5]

Οι υποστηρικτές αυτής της τεχνικής πιστεύουν ότι προσθέτει ασφάλεια στη

μεταφορά δεδομένων, εφόσον κάθε παραλήπτης δεν είναι σε θέση να λάβει το πλήρες σήμα εάν δεν γνωρίζει τον αλγόριθμο παραγωγής των τυχαίων αριθμών, καθώς και τον αρχικό αριθμό που χρησιμοποιήθηκε ως είσοδος στον αλγόριθμο (φύτρο). Επίσης η τεχνολογία αποδείχθηκε ότι έχει αντοχή στην εξασθένηση, καθώς το σήμα δεν είναι μιας συγκεκριμένης συχνότητας αλλά διαχέεται, και συνέπεια αυτού του γεγονότος είναι να επηρεάζεται μόνο ένα μικρό τμήμα του σήματος.

Τα συστήματα που χρησιμοποιούν τη διασπορά φάσματος χωρίζονται στους παρακάτω τύπους ανάλογα με τον τρόπο με τον οποίο ο κώδικας διασποράς (PN) διαμορφώνει τα αρχικά δεδομένα. Έτσι έχουμε [9]:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Υβριδική Direct Sequence και Frequency Hopping Spread Spectrum
- Time Hopping Spread Spectrum
- Chirp Spread Spectrum
- Orthogonal Frequency Division Multiplexing (OFDM)

Από τους έξι παραπάνω τύπους, στα WLANs χρησιμοποιούνται ευρέως οι τεχνικές FHSS, DSSS και OFDM οι οποίες αναλύονται παρακάτω.

2.3.1 Διασπορά φάσματος μεταπήδησης συχνότητας (Frequency Hopping Spread Spectrum - FS ή FHSS)

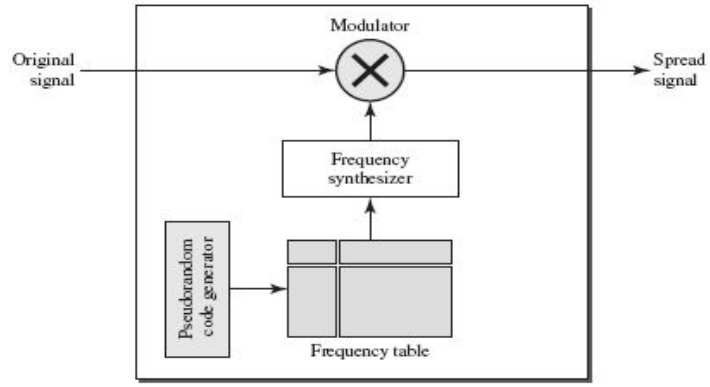
Η τεχνική χρησιμοποιείται στα πρότυπα 802.11b και 802.11g και βασίζεται στην ύπαρξη ενός συστήματος που εναλλάσσεται τυχαία ή ψευδοτυχαία ανάμεσα σε κανάλια συχνοτήτων. Το χρονικό διάστημα παραμονής σε κάθε συχνότητα πρέπει να είναι γνωστό μεταξύ του πομπού και του δέκτη, ενώ αντιστοιχεί πάντα σε 0,4 sec σύμφωνα με τους κανόνες που ορίζει η FCC. Έτσι, σε μια μετάδοση, ο αποστολέας χρησιμοποιεί κάποιο κανάλι για μια σύντομη χρονική περίοδο και έπειτα επιλέγει κάποιο άλλο για να συνεχίσει να μεταδίδει δεδομένα. Ο

παραλήπτης, γνωρίζοντας κάθε πότε ο αποστολέας αλλάζει κανάλι μετάδοσης, μπορεί να λαμβάνει σωστά τα μεταδιδόμενα δεδομένα.

Η μεταπήδηση μεταξύ των καναλιών γίνεται μέσω μιας φαινομενικά τυχαίας ακολουθίας η οποία είναι γνωστή στον αποστολέα και τον παραλήπτη και καθορίζεται από την είσοδο (φύτρο) που δίνεται στη γεννήτρια τυχαίων αριθμών, ενώ ο ρυθμός με τον οποίο γίνεται η μεταπήδηση στα διάφορα κανάλια καθορίζει το σύστημα μεταπήδησης συχνοτήτων που θα χρησιμοποιηθεί, δηλαδή αργή ή γρήγορη μεταπήδηση.

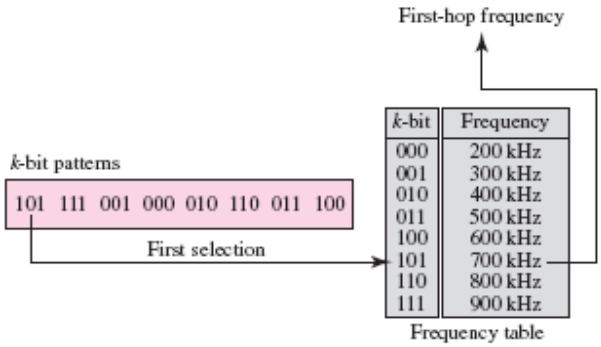
Αν η ταχύτητα μεταπήδησης έχει τιμή μεγαλύτερη από το χρόνο μετάδοσης ενός bit, ένα κανάλι συχνότητας μεταδίδει πολλά bit και τότε έχουμε *αργή μεταπήδηση συχνότητας*. Αν η ταχύτητα μεταπήδησης έχει τιμή μικρότερη από το χρόνο μετάδοσης ενός bit, ένα bit μεταδίδεται σε περισσότερες από μια συχνότητες. Αυτή η τεχνική καλείται *γρήγορη μεταπήδηση συχνότητας*. Και στις δυο περιπτώσεις όταν βρισκόμαστε σε ένα κανάλι, το πραγματικό μεταδιδόμενο σήμα είναι το αποτέλεσμα της διαμόρφωσης της κεντρικής συχνότητας του καναλιού με το αρχικό σήμα. [5]

Η μέθοδος που χρησιμοποιείται για να μεταδοθούν τα δεδομένα στη ζώνη των 2.4GHz με ταχύτητες 1 ή 2 Mbps είναι η γκαουσιανή μετατόπιση συχνότητας (Gaussian Frequency Shift Keying – GFSK). Όπως φαίνεται στο σχήμα 2.5, τα ψηφιακά σήματα εισάγονται σε έναν διαμορφωτή GFSK ο οποίος παράγει αναλογικά σήματα γύρω από μια ορισμένη συχνότητα. Με τη βοήθεια μιας ψευδοτυχαίας ακολουθίας που ονομάζεται PN (pseudorandom noise), κάθε bit της οποίας είναι δείκτης σε έναν πίνακα συχνοτήτων (σχήμα 2.6), από τα αναλογικά σήματα, παράγονται σήματα που είναι περιορισμένα στη συχνότητα που επιλέχθηκε από τον πίνακα. Αυτό επιτυγχάνεται με τη χρήση μιας συσκευής που ονομάζεται *synthesizer* η οποία παρέχει στον διαμορφωτή τις συχνότητες από τον πίνακα συχνοτήτων, ώστε να συνδυαστούν με το αρχικό σήμα και να παραχθεί το τελικό διεσπαρμένο σήμα. Αποτέλεσμα της επανάληψης αυτής της διαδικασίας είναι η παραγωγή του σήματος μεταπήδησης συχνότητας.



Σχήμα 2.5: Αναπαράσταση της τεχνικής FHSS

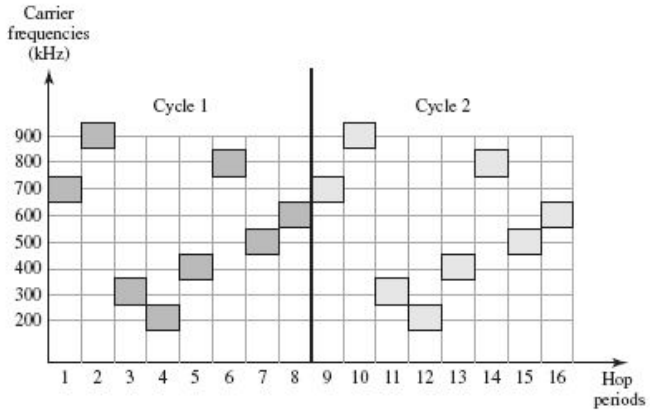
Στο σχήμα 2.6 φαίνεται ο τρόπος επιλογής των συχνοτήτων από τον πίνακα συχνοτήτων. Κάθε δείκτης στον πίνακα συχνοτήτων αποτελείται από τρία bits. Έτσι θα υποθέσουμε ότι έχουμε στη διάθεσή μας μόνο οχτώ συχνότητες μεταπήδησης (2^3), αν και το νούμερο είναι εντελώς υποθετικό, εφόσον στην πράξη οι συχνότητες μεταπήδησης είναι πολύ περισσότερες.



Σχήμα 2.6: Επιλογή συχνοτήτων στην τεχνική FHSS

Η ακολουθία επιλογής συχνοτήτων είναι ψευδοτυχαία και επαναλαμβάνεται μετά από οχτώ αλλαγές συχνοτήτων (ο αριθμός οχτώ είναι ενδεικτικός). Αυτό σημαίνει ότι στην πρώτη περίοδο μεταπήδησης, επιλέγεται ο αριθμός 101. Η

συχνότητα που επιλέγεται αντιστοιχεί σύμφωνα με το σχήμα 2.6 σε 700KHz και το αρχικό σήμα διαμορφώνεται βάσει αυτής της συχνότητας. Αφού αυτή η διαδικασία ολοκληρωθεί και για τις οχτώ συχνότητες, αρχίζουμε και πάλι από τον αριθμό 101 και έτσι έχουμε έναν νέο κύκλο μεταπηδήσεων όπως φαίνεται και στο σχήμα 2.7. [6]



Σχήμα 2.7: Κύκλοι μεταπηδήσεων στην τεχνική FHSS

Γενικά, το πρότυπο 802.11 χωρίζει το κανάλι σε μικρότερες συχνότητες του 1MHz. Τα κανάλια χαρακτηρίζονται από κεντρικές συχνότητες, οι οποίες ξεκινούν από 2.400GHz για το κανάλι 0. Οι συχνότητες των ακόλουθων καναλιών προκύπτουν προσθέτοντας 1MHz, δηλαδή το κανάλι 1 έχει κεντρική συχνότητα 2.401GHz, το κανάλι 2 έχει την 2.402GHz, και συνεχίζονται ομοίως, μέχρι το 95ο κανάλι που λειτουργεί στα 2.495MHz. Διαφορετικές αρχές προτύπων επιτρέπουν τη χρήση διαφορετικών τμημάτων της ISM μπάντας όπως φαίνεται παρακάτω στον πίνακα 2.2.

Πίνακας 2.2: Χρήση καναλιών στην τεχνική FHSS

Τοποθεσία	Πλήθος καναλιών μεταπήδησης	Κανάλια προς χρήση
ΗΠΑ (FCC)	26	2 έως 79 (2.402-2.479 GHz)
Καναδάς (IC)	26	2 έως 79 (2.402-2.479 GHz)
Ευρώπη (εκτός Γαλλίας και Ισπανίας) (ETSI)	26	2 έως 79 (2.402-2.479 GHz)
Γαλλία	27	48 έως 82 (2.448-2.482 GHz)
Ισπανία	35	47 έως 73 (2.447-2.473 GHz)
Ιαπωνία (MKK)	23	73 έως 95 (2.473-2.495 GHz)

Το γεγονός ότι η λήψη των δεδομένων εξαρτάται από το χρονικό διάστημα που ο αποστολέας εναλλάσσεται μεταξύ των καναλιών, καθιστά δύσκολη κάθε μεσολάβηση στην επικοινωνία από τρίτους. Επίσης άλλο ένα πλεονέκτημα αυτής της τεχνικής είναι η μειωμένη ενεργειακή κατανάλωση, εφόσον το κάθε κανάλι χρησιμοποιείται για μικρό χρονικό διάστημα και δεν απασχολείται συνεχώς. Σημαντικό πλεονέκτημα είναι και το χαμηλό κόστος των ηλεκτρονικών συστημάτων που απαιτούνται για την υλοποίηση της τεχνικής.

Η τεχνική FHSS επιτρέπει την συνύπαρξη πολλών δικτύων, που η συνολική τους ρυθμοαπόδοση (throughput) είναι αυξημένη. Εάν ο αριθμός των συχνοτήτων μεταπήδησης είναι *M*, μπορούμε να πολυπλέξουμε τα *M* κανάλια σε ένα. Αυτό είναι δυνατό επειδή ένας σταθμός χρησιμοποιεί μόνο μια συχνότητα σε κάθε περίοδο μεταπήδησης. Οι υπόλοιπες *M-1* συχνότητες μπορούν να χρησιμοποιηθούν από άλλους *M-1* σταθμούς. Αυτό σημαίνει ότι *M* διαφορετικοί σταθμοί μπορούν να έχουν ίδιο bandwidth εάν χρησιμοποιηθεί η κατάλληλη τεχνική διαμόρφωσης (πχ η FSK). [6]

2.3.2 Διασπορά φάσματος άμεσης ακολουθίας (Direct Sequence Spread Spectrum –DSSS)

Πρόκειται για μια τεχνολογία η οποία χρησιμοποιείται στο πρότυπο 802.11b συχνότητας 2.4GHz, στα ασύρματα τηλέφωνα συχνότητας 5GHz, στα τηλεφωνικά δίκτυα κινητής τηλεφωνίας δεύτερης γενιάς που είναι βασισμένα στην τεχνική CDMA (Code Division Multiple Access) καθώς και σε όλες τις υπηρεσίες τρίτης γενιάς.

Η DSSS χρησιμοποιείται για τη μεταφορά σημάτων μέσα από κανάλια υψηλών συχνοτήτων. Ο εξοπλισμός που απαιτείται για τη λειτουργία της χρειάζεται περισσότερη ενέργεια για να πετύχει την ίδια ρυθμοαπόδοση σε σχέση με την FHSS. Όμως το μεγάλο πλεονέκτημα της DSSS είναι η προσαρμοστικότητά της σε πολύ υψηλότερους ρυθμούς μετάδοσης δεδομένων απ' ότι η FHSS. Ο πίνακας 2.3 δείχνει τα επιτρεπόμενα κανάλια εκπομπής για διάφορες χώρες.

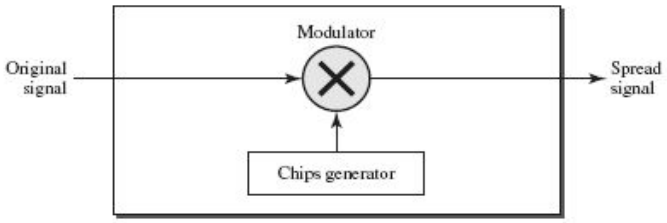
Πίνακας 2.3: Επιτρεπόμενα κανάλια εκπομπής με την τεχνική DSSS

Τοποθεσία	Επιτρεπόμενα κανάλια εκπομπής
ΗΠΑ (FCC) / Καναδάς (IC)	1 έως 11 (2.412 - 2.462 GHz)
Ευρώπη (εκτός Γαλλίας, Ισπανίας) ETSI	1 έως 13 (2.412 - 2.472 GHz)
Γαλλία	10 έως 13 (2.457 - 2.472 GHz)
Ισπανία	10 έως 11 (2.457 - 2.462 GHz)
Ιαπωνία (MKK)	14 (2.484 GHz)

Βασική ιδέα της τεχνολογίας είναι ότι η μετάδοση δεδομένων βασίζεται στα *chips*. Με τον όρο chip, εννοούμε ένα δυαδικό ψηφίο το οποίο όμως διαφέρει από ένα bit. Τα bits είναι δεδομένα υψηλού επιπέδου ενώ τα chips είναι απλοί αριθμοί που χρησιμοποιούνται ως απαραίτητο στοιχείο της κωδικοποίησης.

Σύμφωνα με την DSSS, το bandwidth του αρχικού σήματος εξαπλώνεται αλλά ο τρόπος με τον οποίο γίνεται διαφέρει από εκείνον της FHSS, αφού στην

DSSS τα bits του αρχικού σήματος συνδυάζονται με τα *n* chips της ακολουθίας, μέσω μιας συνάρτησης XOR και αυτό που προκύπτει είναι το τελικό διεσπαρμένο σήμα. Η ακολουθία με τα chips ονομάζεται chipping code ή Barker Code στην περίπτωση που αποτελείται από 11 chips (σχήμα 2.9) ενώ ο ρυθμός των chips του διεσπαρμένου σήματος είναι *n* φορές μεγαλύτερος από εκείνον των bit του αρχικού σήματος.



Σχήμα 2.8: Αναπαράσταση της τεχνικής DSSS

Ο παράγοντας διασποράς είναι σημαντικός διότι το σήμα διασπείρεται ανάλογα με αυτόν γύρω από μια ζώνη συχνοτήτων, το πλάτος της οποίας είναι ανάλογο προς τον παράγοντα διασποράς. Επίσης, όσο ο παράγοντας διασποράς αυξάνεται, ο ρυθμός μετάδοσης των δεδομένων του διεσπαρμένου σήματος μειώνεται. Πρακτικά αυτό σημαίνει ότι αν χρησιμοποιούμε παράγοντα διασποράς ίσο με 10 σε ένα κανάλι το οποίο έχει εύρος X MHz, ο ρυθμός μετάδοσης των δεδομένων θα περιορισθεί στο X/10, τη στιγμή που ένα σύστημα στενής ζώνης μπορεί να φτάσει ρυθμούς μετάδοσης ίσους με X. Ενώ με αυτή την παρατήρηση φαίνεται περιττή η χρήση της τεχνικής DSSS, πλεονεκτεί άλλων τεχνικών εφόσον μπορεί να κάνει εξαγωγή δεδομένων από παρεμβολές και θορύβους στενής ζώνης (δηλαδή ρυθμού μικρότερου ή ίσου με 2Mbps) με αποτέλεσμα τη μείωση των μεταδόσεων και την αύξηση της αποδοτικότητας. Ωστόσο, η περίπτωση εμφάνισης παρεμβολών είναι μικρότερη από εκείνη των συστημάτων μεταπήδησης συχνότητας.

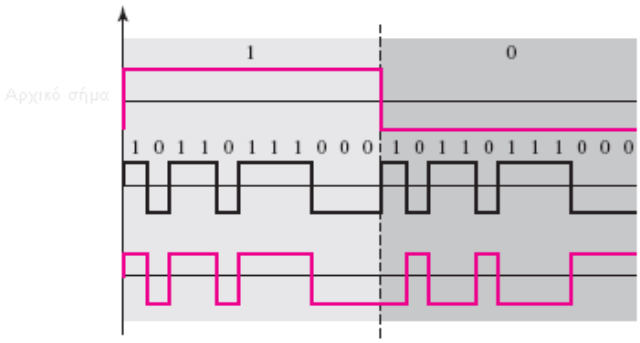
Στο παρακάτω σχήμα φαίνεται ο τρόπος με τον οποίο μια ακολουθία από bits μετατρέπεται σε ένα διεσπαρμένο σήμα μέσω της συνάρτησης XOR.

Αρχική ακολουθία	1											0										
Chipping code	1	0	1	1	0	1	1	1	0	0	0	1	0	1	1	0	1	1	1	0	0	0
Διεσπαρμέ-νο σήμα	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1	1	0	0	0

Σχήμα 2.9: Διασπορά ακολουθίας bits με την τεχνική DSSS

Το σχήμα που ακολουθεί δείχνει το τελικό διεσπαρμένο σήμα (τρίτος παλμός) που είναι αποτέλεσμα της εφαρμογής του chipping code (δεύτερος παλμός) επάνω στον αρχικό παλμό. Ο κώδικας διασποράς αποτελείται από 11 chips που στην περίπτωσή μας είναι η ακολουθία 10110111000. Εάν το αρχικό σήμα έχει ρυθμό *N*, τότε ο ρυθμός του διεσπαρμένου σήματος θα είναι *11N*. Αυτό σημαίνει ότι το bandwidth που απαιτείται για το διεσπαρμένο σήμα είναι κατά 11 φορές μεγαλύτερο από εκείνο που χρειάζεται για το αρχικό σήμα.

Το διεσπαρμένο σήμα παρέχει ασφάλεια στα μεταδιδόμενα δεδομένα αφού ένας εισβολέας πρέπει να γνωρίζει τον κώδικα διασποράς που χρησιμοποιήθηκε για να τα “διαβάσει”. Μπορεί επίσης να προστατέψει από πιθανές παρεμβολές μεταξύ διαφορετικών σταθμών αν ο καθένας από αυτούς χρησιμοποιεί διαφορετικό κώδικα διασποράς.



Σχήμα 2.10: Παρουσίαση των δεδομένων του σχήματος 2.9 σε παλμούς από bits

Γενικά η DSSS λειτουργεί στα 2.4GHz, χωρίζοντας το διαθέσιμο εύρος ζώνης σε κανάλια που το καθένα έχει εύρος ζώνης 11MHz και έχει τη δυνατότητα να μεταδίδει τη διεσπαρμένη ροή δεδομένων με ταχύτητες 1 ή 2Mbps διαμορφώνοντας τη φάση και όχι τη συχνότητα του εκπεμπόμενου σήματος, επειδή ο θόρυβος επηρεάζει συνήθως το εύρος ζώνης και όχι τη φάση. Για μετάδοση με 1Mbps χρησιμοποιείται η δυαδική διαμόρφωση μετατόπισης φάσης (BPSK), η οποία μετατοπίζει τη φάση της συχνότητας του φέροντος σήματος προκειμένου να αναπαραχθούν τα διαφορετικά σύμβολα. Εάν έχουμε μετάδοση με ταχύτητα 2Mbps χρησιμοποιούμε τετραγωνική διαμόρφωση μετατόπισης φάσης (QPSK) όπου μεταδίδουμε ένα ζεύγος από bit με ρυθμό 1Mbps με αποτέλεσμα να πετυχαίνουμε μετάδοση με ταχύτητα 2Mbps.

Το πρότυπο 802.11b υποστηρίζει ρυθμούς μετάδοσης στα 11Mbps, με εναλλακτικούς ρυθμούς μετάδοσης τα 5.5, 2 και 1Mbps στα 2.4GHz. Η τεχνική διαμόρφωσης που χρησιμοποιείται είναι η διαμόρφωση συμπληρωματικού κωδικού (CCK), η οποία είναι και ο υποχρεωτικός τρόπος λειτουργίας που ορίζεται από το πρότυπο.

Η τεχνική μπορεί επίσης να υποστηρίξει την ταυτόχρονη λειτουργία διαφορετικών ασύρματων δικτύων, στην περίπτωση που κάποια δίκτυα δεν χρησιμοποιούν όλο το διαθέσιμο εύρος ζώνης. Έτσι, τα επιπλέον δίκτυα

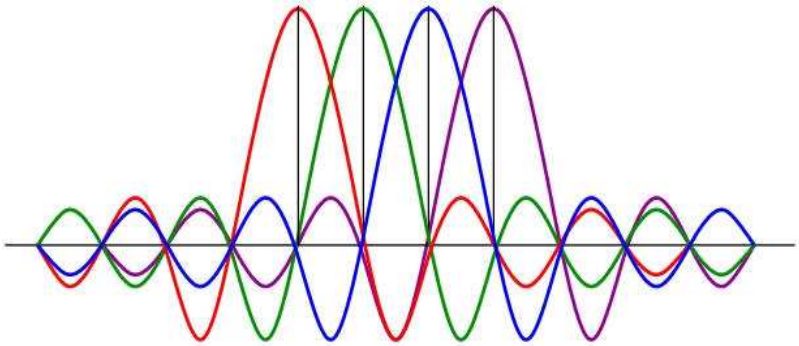
χρησιμοποιούν τα υπόλοιπα ελεύθερα κανάλια και λειτουργούν όλα μαζί στην ίδια γεωγραφική περιοχή. [5]

2.3.3 Ορθογωνική πολύπλεξη διαίρεσης συχνότητας (Orthogonal Frequency Division Multiplexing - OFDM)

Η ορθογωνική πολύπλεξη διαίρεσης συχνότητας είναι μια σχετικά πρόσφατη τεχνική η οποία χρησιμοποιείται στα πρότυπα 802.11a, 802.11g, 802.11n, στο WiMAX καθώς και σε DSL τεχνολογίες όπως οι HDSL, ADSL και VDSL. Η ανάπτυξή της είχε ξεκινήσει πολύ πιο πριν, στις δεκαετίες του '60 και του '70. Υλοποιήθηκε προκειμένου να εξουδετερωθούν οι συνέπειες του multipath, δηλαδή της κατάστασης κατά την οποία το ίδιο σήμα φτάνει στον παραλήπτη πολλές φορές από διαφορετικά κανάλια μετάδοσης και έτσι κάθε επόμενο σήμα ακυρώνει το προηγούμενό του, εφόσον τα σήματα αυτά έχουν ίδια συχνότητα αλλά διαφορετική φάση.

Σύμφωνα με την OFDM, το ψηφιακό σήμα χωρίζεται σε *n* υποκανάλια και η χωρητικότητα του κάθε καναλιού διαιρείται σε *n* ορθογωνικούς τόνους. Αποτέλεσμα αυτών είναι η ταυτόχρονη μετάδοση σημάτων, μικρότερων του αρχικού αλλά ίσων σε μέγεθος, μέσα από πολλά κανάλια που υποστηρίζουν χαμηλούς ρυθμούς μετάδοσης. Έπειτα, όλα αυτά τα κανάλια μετά από πολύπλεξη ενώνονται σε ένα, που υποστηρίζει μεγαλύτερους ρυθμούς μετάδοσης. Τα κανάλια τοποθετούνται κοντά το ένα με το άλλο και με τρόπο τέτοιο ώστε οι φορείς να είναι μεταξύ τους ορθογωνικοί για να μην υπάρχουν παρεμβολές ανάμεσά τους. Όπως φαίνεται στο σχήμα 2.11, παρά το γεγονός ότι υπάρχει επικάλυψη φασμάτων, οι μεταδιδόμενες πληροφορίες είναι εύκολο να ανακτηθούν χάρη στην εφαρμογή της ορθογωνικότητας που χρησιμοποιεί η OFDM. Αυτό σημαίνει ότι η λήψη των ορθών σημάτων πρέπει να γίνεται σε σημείο τέτοιο που όλα τα υπόλοιπα σήματα είναι μηδενικά εκτός από αυτό που γίνεται η μέτρηση (στο σχήμα 2.11 είναι τα σημεία με τις κάθετες γραμμές). Η έλλειψη ορθογωνικότητας θα είχε σαν αποτέλεσμα την

επικάλυψη των σημάτων που περιέχουν πληροφορίες και θα υποβάθμιζαν την ποιότητα της επικοινωνίας.



Σχήμα 2.11: Ανίχνευση πληροφοριών στην τεχνική OFDM

Στο πρότυπο 802.11a υποστηρίζονται διάφοροι ρυθμοί μετάδοσης δεδομένων στο διάστημα από 6 έως 54 Mbps, ενώ πρέπει υποχρεωτικά να υπάρχει υποστήριξη των ρυθμών 6, 12 και 24 Mbps. Επίσης, ανάλογα με τον ρυθμό μετάδοσης που υποστηρίζεται, υπάρχουν μαζί με την OFDM και οι τεχνικές [1]:

- δυαδικής διαμόρφωσης μετατόπισης φάσης
- τετραγωνικής διαμόρφωσης μετατόπισης φάσης
- τετραγωνικής μετατόπισης πλάτους 16 επιπέδων (16-QAM)
- τετραγωνικής μετατόπισης πλάτους 64 επιπέδων (64-QAM)

2.4 Υπέρυθρες Ακτίνες (Infrared)

Οι υπέρυθρες ακτίνες δεν κατάφεραν να γίνουν πλήρως αποδεκτές από το κοινό για μεταδόσεις σε ασύρματα τοπικά δίκτυα και δεν υπάρχει κάποια

επιτυχημένη υλοποίηση για το πρότυπο 802.11 που να βασίζεται στις υπέρυθρες ακτίνες. Για τη μετάδοση δεδομένων χρησιμοποιείται παλμοθεσική διαμόρφωση (Pulse Position Modulation – PPM) για μεταδόσεις της τάξης του 1Mbps και των 2Mbps. Το υπέρυθρο σήμα παράγεται από πηγές λέιζερ ή LED και για τη λειτουργία των υπέρυθρων ακτινών χρησιμοποιούνται τρεις διαφορετικές τεχνικές οι οποίες είναι οι εξής:

- διάχυτη εκπομπή
- ανάκλαση του μεταδιδόμενου σήματος σε οροφή
- εστιασμένη μετάδοση

Τα προϊόντα ασύρματων δικτύων που υπάρχουν σήμερα λειτουργούν σε μήκη κύματος γύρω από τα 850nm και το συγκεκριμένο φάσμα επιτρέπει την επίτευξη υψηλών ρυθμών μετάδοσης δεδομένων που μπορούν να αγγίξουν μέχρι και το 1Gbps, μια ταχύτητα που είναι θεωρητική. Με τη χρήση αρχών της θεωρίας πληροφοριών αποδεικνύεται ότι τα οπτικά κανάλια έχουν πολύ μεγάλες χωρητικότητες Shannon με συνέπεια να είναι εφικτές τέτοιες ταχύτητες.

Επίσης ένα ακόμη πλεονέκτημα των υπέρυθρων ακτινών είναι το γεγονός ότι οι δέκτες που χρησιμοποιούνται έχουν χαμηλό κόστος εφόσον αυτό που κάνουν είναι η αποδιαμόρφωση των σημάτων με βάση την πλάτος και όχι της συχνότητας ή της φάσης του, γεγονός που μειώνει την πολυπλοκότητα των συσκευών και κατ' επέκταση και το κόστος κατασκευής τους. Επιπλέον, οι παρεμβολές από άλλους και ο θόρυβος διατηρούνται σε χαμηλά επίπεδα, αφού το πεδίο λειτουργίας τους περιορίζεται στα πλαίσια ενός σπιτιού ή ενός κτιρίου εφόσον δεν μπορούν να προσπεράσουν τοίχους και αδιαφανή αντικείμενα και αυτό αποτελεί ταυτόχρονα ένα σημαντικό μειονέκτημα.

Επίλογος

Σε αυτό το κεφάλαιο αναλύσαμε το φυσικό επίπεδο του προτύπου 802.11, τα υποεπίπεδά του, καθώς και τις διαφορετικές τεχνικές διασποράς φάσματος που χρησιμοποιεί. Στο κεφάλαιο που ακολουθεί θα αναλύσουμε το MAC επίπεδο του προτύπου.

Κεφάλαιο 3

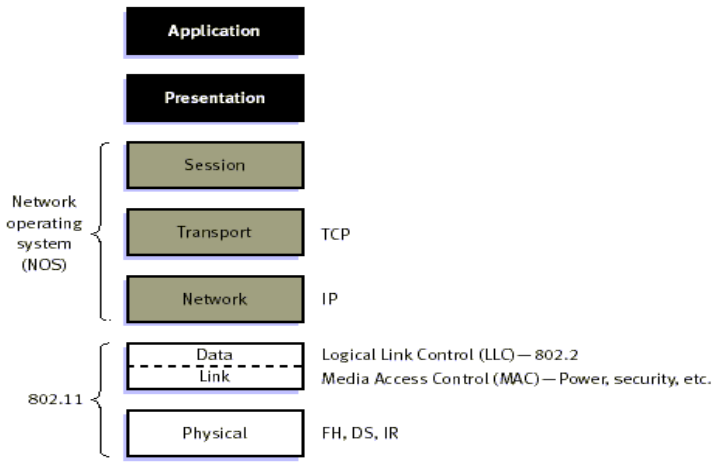
Εισαγωγή στο MAC επίπεδο του IEEE 802.11

3.1 Εισαγωγή

Το κεφάλαιο αυτό αποτελεί μια εισαγωγή στις λειτουργίες του επιπέδου MAC των ασύρματων δικτύων του προτύπου 802.11. Αναφέρονται οι αρχιτεκτονικές των WLANs και επίσης αναλύεται η δομή των πλαισίων. Επίσης περιγράφονται οι διαδικασίες που πραγματοποιούνται μέχρι ένας σταθμός να αποκτήσει πλήρη πρόσβαση στο μέσο, δηλαδή τα στάδια ανίχνευσης, ενσωμάτωσης, αυθεντικοποίησης και συσχέτισης ενός σταθμού με ένα δίκτυο.

3.2 Το επίπεδο ελέγχου πρόσβασης στο μέσο του IEEE 802.11 (MAC Layer)

Στο πρότυπο 802.11 καθορίζονται οι λειτουργίες για το πρώτο επίπεδο του OSI και για το υποεπίπεδο MAC. Στο πρώτο επίπεδο περιγράφονται οι τεχνικές μετάδοσης με ραδιοσυχνότητες ενώ στο υποεπίπεδο MAC περιγράφεται η διαδικασία με την οποία μορφοποιούνται και διευθυνσιοδοτούνται τα πλαίσια, ώστε ο κάθε σταθμός να έχει πρόσβαση στο κανάλι μετάδοσης.



Σχήμα 3.1: Το φυσικό και το MAC επίπεδο του προτύπου 802.11

Το MAC επίπεδο του 802.11 χρησιμοποιεί την τεχνική ανίχνευσης φέροντος πολλαπλής πρόσβασης με αποφυγή συγκρούσεων (CSMA/CA). Παρά την ομοιότητα του ονόματος της μεθόδου CSMA/CA με την μέθοδο CSMA/CD του Ethernet, ο τρόπος λειτουργίας τους είναι εντελώς διαφορετικός εφόσον η CSMA/CD χρειάζονταν τροποποιήσεις προκειμένου να προσαρμοστεί στις ανάγκες των ασύρματων δικτύων.

Ένας βασικός λόγος που θα προκαλούσε πολλές τροποποιήσεις στο πρωτόκολλο του Ethernet προκειμένου να προσαρμοστεί στα ασύρματα δίκτυα είναι το πρόβλημα της ανίχνευσης συγκρούσεων. Στο Ethernet ο σταθμός που μεταδίδει συνεχίζει να “ακούει” το μέσο και κατά τη διάρκεια της μετάδοσής του. Στα ασύρματα δίκτυα, όταν ένας σταθμός αποστέλλει δεδομένα, δεν μπορεί ταυτόχρονα να “ακούει” άλλες μεταδόσεις. Η ανίχνευση συγκρούσεων υλοποιείται εύκολα στα ενσύρματα δίκτυα, καθώς σε αυτά η σύγκρουση μπορεί να ανιχνευτεί εξαιτίας της μικρής διαφοράς στα επίπεδα ισχύος των εκπεμπόμενων και των λαμβανόμενων σημάτων. Στα ασύρματα δίκτυα, η ενέργεια του εκπεμπόμενου σήματος διαχέεται σε όλες τις κατευθύνσεις και αυτό απαιτεί μεγάλη ευαισθησία των δεκτών ώστε να ανιχνεύσουν το σήμα. Ακόμη και στην πιο απλή περίπτωση που τα τερματικά που εκπέμπουν είναι μόνο δυο, η ισχύς του σήματος του ενός

επικαλύπτει την ισχύ του σήματος του άλλου σταθμού και έτσι η ανίχνευση σύγκρουσης γίνεται δύσκολη. Επίσης στα ασύρματα δίκτυα το σήμα εξασθενεί γρήγορα. Τέλος, η ακτίνα εκπομπής και λήψης των σταθμών είναι περιορισμένη και αυτό δυσκολεύει τον σχηματισμό μιας πλήρους εικόνας του δικτύου. [12]

Για την αποφυγή συγκρούσεων, το πρωτόκολλο διαθέτει μηχανισμούς αναμονής που προηγούνται κάθε μετάδοσης, μηνύματα ACKs που επιβεβαιώνουν την παράδοση των δεδομένων και επαναποστολές στην περίπτωση αποτυχίας λόγω σύγκρουσης. Δεν χρησιμοποιούνται αρνητικά ACKs, αλλά ο παραλήπτης απορρίπτει κάθε πλαίσιο με λάθη. Όλες αυτές οι τεχνικές προσθέτουν επιβάρυνση στη ρυθμοαπόδοση του δικτύου εφόσον αυξάνουν το χρόνο που απαιτείται για την αποστολή των πλαισίων. Αξίζει να αναφέρουμε κάποιες ιδιαιτερότητες που υπάρχουν στα WLANs [1]:

- Η ροή των δεδομένων σε σχέση με τα ενσύρματα δίκτυα είναι διαφορετική, εφόσον οι σταθμοί, ακόμη και αν βρίσκονται στο ίδιο BSS/ESS δίκτυο, προκειμένου να ανταλλάξουν δεδομένα πρέπει να επικοινωνήσουν με το σημείο πρόσβασης. Αν οι σταθμοί βρίσκονται σε δίκτυο Ad Hoc, τότε επικοινωνούν απευθείας.
- Ο ρυθμός μετάδοσης δεδομένων εξαρτάται από το πρότυπο που χρησιμοποιείται (802.11a/b/g) καθώς και από την απόσταση που έχει κάθε σταθμός από το σημείο πρόσβασης, από κατασκευαστικές ατέλειες των συσκευών ή από παρεμβολές. Τόσο οι σταθμοί όσο και το σημείο πρόσβασης μοιράζονται το ίδιο half duplex κανάλι με διαφορετικούς ρυθμούς μετάδοσης. Επιπλέον, διαφορετικοί χρήστες μπορούν να πετύχουν διαφορετικούς ρυθμούς μετάδοσης σε αυτό το κανάλι. Όμως, ακόμη και οι σταθμοί που μεταδίδουν με μικρούς ρυθμούς δεδομένων επιβαρύνουν το μέσο επειδή το κανάλι μένει απασχολημένο περισσότερο χρόνο.
- Εφόσον ένας σταθμός δεν μπορεί να “ακούει” άλλες μεταδόσεις κατά το διάστημα που ο ίδιος μεταδίδει, δεν υπάρχει τρόπος να ανιχνεύσει συγκρούσεις. Επίσης, υπάρχει το ενδεχόμενο ένας σταθμός ο οποίος δεν είναι μέσα στο πεδίο εμβέλειας των άλλων σταθμών να προκαλέσει

σύγκρουση αν μεταδώσει δεδομένα επειδή νομίζει πως το κανάλι είναι ελεύθερο (πρόβλημα του κρυφού σταθμού).

3.2.1 Περιγραφή λειτουργιών του υποεπιπέδου MAC του IEEE 802.11

Πέρα από τις βασικές λειτουργίες που επιτελούνται γενικά από το επίπεδο MAC, το υποεπίπεδο MAC του 802.11 έχει κατασκευαστεί για να μπορεί να αλληλεπιδρά με τα φυσικά επίπεδα του προτύπου 802.11 (FH, DS και IR). Οι τέσσερις κύριες λειτουργίες του MAC είναι:

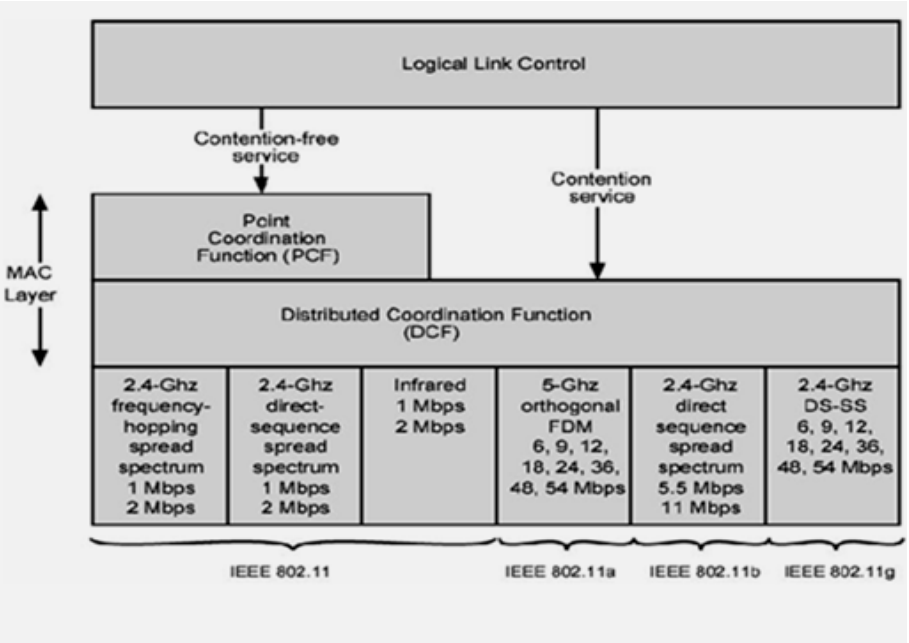
- ανίχνευση του δικτύου
- η αυθεντικοποίηση του σταθμού
- η ενσωμάτωση ενός σταθμού στο δίκτυο
- συσχέτιση με το δίκτυο
- η πρόσβαση στο μέσο
- εξοικονόμηση ενέργειας
- θέματα σχετικά με την ασφάλεια

Είναι επίσης υπεύθυνο και για λειτουργίες που γίνονται σε υψηλότερα επίπεδα όπως η κατάτμηση, η επαναποστολή πακέτων και οι επιβεβαιώσεις λήψης. Το πρωτόκολλο MAC του προτύπου είναι ουσιαστικά ένα πρωτόκολλο CSMA/CA το οποίο ονομάζεται DFWMAC (Distributed Foundation Wireless MAC)16, γνωστό και ως DCF (Distributed Coordination Function). Χρησιμοποιείται για πρόσβαση στο μέσο με τη βοήθεια ενός CSMA/CA αλγορίθμου με χρονικές σχισμές.

Ωστόσο υπάρχει και άλλη μια μέθοδος για πρόσβαση στο μέσο, η χρήση της οποίας είναι προαιρετική και ονομάζεται λειτουργία σημειακού συντονισμού PCF (Point Coordination Function). Είναι “χτισμένη” επάνω από την DCF και υποστηρίζει κυκλοφορία των δεδομένων χωρίς ανταγωνισμό ενώ προσφέρεται μόνο σε δίκτυα υποδομής καθώς οι ειδικές συσκευές που χρησιμοποιούνται

16 Άλλα πρωτόκολλα που χρησιμοποιούνται στα WLANs είναι τα BTMA, SRMA, MACA, MACAW, FAMA, GAMA, EY-NPMA.

(σημειακοί συντονιστές) προκειμένου να εξασφαλιστεί ότι το μέσο χρησιμοποιείται χωρίς ανταγωνισμό, είναι τοποθετημένες στα σημεία πρόσβασης. Οι δυο μέθοδοι πρόσβασης θα αναλυθούν διεξοδικά στο επόμενο κεφάλαιο.



Σχήμα 3.2: Οι μέθοδοι πρόσβασης DCF και PCF

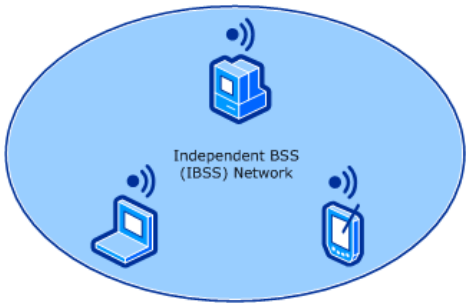
3.3 Στοιχεία αρχιτεκτονικής των ασύρματων δικτύων

Κάθε ασύρματο τοπικό δίκτυο βασίζεται σε μια κυψελωτή αρχιτεκτονική. Αυτό σημαίνει ότι όλο το δίκτυο χωρίζεται σε περιοχές/κυψέλες που η κάθε μια ονομάζεται Basic Service Set (BSS) και ελέγχεται από ένα σημείο πρόσβασης. Αν και ένα ασύρματο δίκτυο μπορεί να “σταθεί” με μια μόνο κυψέλη και ένα σημείο πρόσβασης, οι περισσότερες υλοποιήσεις χρησιμοποιούν πολλές κυψέλες, όπου ένα σημείο πρόσβασης είναι συνδεδεμένο με τους σταθμούς υπό μορφή ραχοκοκαλιάς (backbone) όπως και στο Ethernet και όλο αυτό καλείται σύστημα διαμοιρασμού (Distribution System – DS). Αυτό φαίνεται και στο σχήμα 3.4. [11]

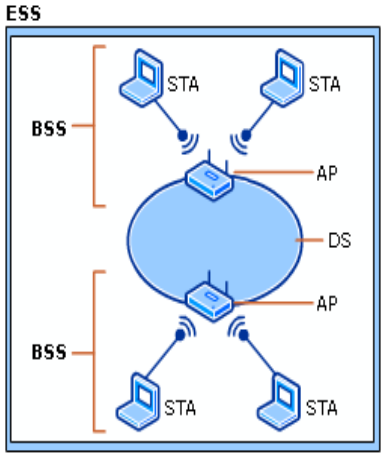
Ένα σύνολο από ασύρματους σταθμούς που επικοινωνούν κάτω από τον έλεγχο της κατανεμημένης συνάρτησης συντονισμού (DCF) ή της σημειακής

συνάρτησης συντονισμού (PCF) αποτελούν το BSS, ενώ η περιοχή η οποία καλύπτουν ονομάζεται Basic Service Area (BSA). Συνολικά όλο το ασύρματο δίκτυο μαζί με τις διαφορετικές κυψέλες, τα σημεία πρόσβασης και τα σημεία διαμοιρασμού ονομάζεται Extended Service Set (ESS). Τα ασύρματα δίκτυα χωρίζονται σε δυο κατηγορίες λειτουργίας: (α) τα αυτοοργανούμενα δίκτυα ή Ad hoc και (β) τα δίκτυα υποδομής ή Infrastructure. [11]

Σε ένα δίκτυο που είναι αυτοοργανούμενο, οι σταθμοί επικοινωνούν μεταξύ τους μέσω ενός IBSS χωρίς να υπάρχουν καλώδια, όπως δείχνει το σχήμα 3.3. Στα δίκτυα υποδομής, όπως φαίνεται στο σχήμα 3.4, οι σταθμοί επικοινωνούν με το υπόλοιπο δίκτυο μέσω των σημείων πρόσβασης που ουσιαστικά παίζουν το ρόλο “γεφυρών” ανάμεσα στα διάφορα BSS.



Σχήμα 3.3: Ad hoc δίκτυο



Σχήμα 3.4: Δίκτυο υποδομής

3.4 Μορφή μηνυμάτων στο IEEE 802.11

Το πρότυπο 802.11 περιλαμβάνει πλαίσια δεδομένων, διαχείρισης και ελέγχου. Κάθε τέτοιο πλαίσιο έχει τα παρακάτω τέσσερα μέρη [1]:

1. PLCP (Physical Layer Convergence Protocol)

2. MAC κεφαλίδα (περιλαμβάνει έως 30Bytes)
3. Σώμα (έως 2.312Bytes στο 802.11b, έως 4.095Bytes στα 802.11a και 802.11g)
4. Ακολουθία ελέγχου (Frame Check Sequence) μήκους έως 4Bytes.

3.4.1 PLCP (Physical Layer Convergence Protocol)

Η PLCP κεφαλίδα είναι τμήμα του φυσικού επιπέδου, και προηγείται κάθε μετάδοσης, περικλείοντας πλαίσια διαχείρισης και πλαίσια ελέγχου. Το συνολικό μέγεθός της εξαρτάται από το πρωτόκολλο ραδιοσυχνοτήτων που χρησιμοποιείται. Πρέπει να διαβάζεται από κάθε σταθμό στο δίκτυο και γι' αυτό αποστέλλεται πάντα με το χαμηλότερο ρυθμό μετάδοσης που μπορεί να υποστηρίξει το κάθε πρότυπο (1Mbps στο 802.11b, 6Mbps στο 802.11a και g).

3.4.2 Κεφαλίδα του MAC

Η κεφαλίδα αποτελείται από τα εξής τέσσερα μέρη:

- Έλεγχος πλαισίου (2Bytes)
- Πεδίο Duration/ID (2Bytes)
- Διεύθυνση MAC (3 πεδία των 6Bytes το καθένα)
- Έλεγχος ακολουθίας (2Bytes)

3.4.2.1 Έλεγχος πλαισίου (Frame Control Field)

Καθώς το πρότυπο 802.11 ορίζει πλαίσια δεδομένων, διαχείρισης και ελέγχου ο τύπος των πλαισίων εμφανίζεται μέσα στο πεδίο *έλεγχος πλαισίου - frame control* της κεφαλίδας. Κάθε πλαίσιο, περιλαμβάνει στην αρχή του ένα πεδίο των 2Bytes που ονομάζεται έλεγχος πλαισίου και έχει τα παρακάτω υποπεδία:

Protocol Version

πεδίο με μέγεθος 2bits, δείχνει ποια έκδοση του 802.11 MAC χρησιμοποιείται, η τρέχουσα είναι η 00.

Type / Subtype

πεδία με μέγεθος 2bits και 4bits αντίστοιχα, δείχνουν τον τύπο του πλαισίου που χρησιμοποιείται (π.χ. αν πρόκειται για πλαίσιο δεδομένων, διαχείρισης ή ελέγχου) και τον υποτύπο αυτού (Πίνακας 3.1).

To DS / From DS

από 1bit το καθένα, πρόκειται για πεδία που δείχνουν σε ένα δίκτυο BSS ή ESS αν ένα πλαίσιο προορίζεται για το σύστημα κατανομής.

More fragments

πεδίο με μέγεθος 1bit που τίθεται στην τιμή 1 εάν το αρχικό πλαίσιο έχει κατακερματιστεί και ακολουθούν άλλα τμήματά του, ενώ παίρνει την τιμή 0 αν το πλαίσιο είναι το τελευταίο πλαίσιο ή είναι μη κατακερματισμένο πλαίσιο.

Retry

πεδίο με μέγεθος 1bit που έχει τιμή 1 εάν πρόκειται για πλαίσιο που αναμεταδόθηκε. Βοηθάει ώστε ο παραλήπτης να απορρίπτει αντίγραφα των πλαισίων.

Power Management

πεδίο με μέγεθος 1bit, εάν έχει την τιμή 1 τότε ο σταθμός είναι σε κατάσταση εξοικονόμησης ενέργειας (power save mode). Ένας σταθμός που βρίσκεται σε αυτή την κατάσταση ή σε κατάσταση sleep, απενεργοποιεί κάποια τμήματα του εξοπλισμού του που αφορούν το δίκτυο. Εάν πρόκειται για το σημείο πρόσβασης, αυτό το bit είναι πάντα 0.

More Data

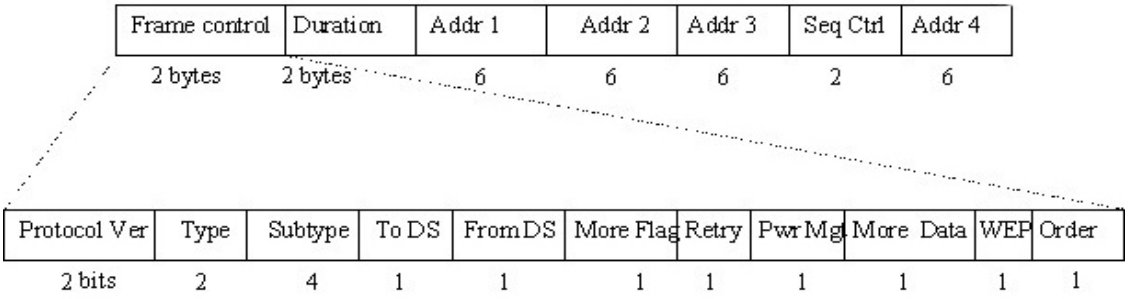
πεδίο με μέγεθος 1 bit που χρησιμοποιείται από το σημείο πρόσβασης κατά την επικοινωνία του με σταθμούς που είναι σε κατάσταση εξοικονόμησης ενέργειας, ώστε να αποφασίσει εάν υπάρχουν επιπλέον πλαίσια στους buffers του για αυτούς. Χρησιμοποιείται επίσης και στην περίπτωση που οι σταθμοί βρίσκονται σε sleep mode.

WEP (ή Protected Frame)

πεδίο με μέγεθος 1bit που δείχνει εάν το πλαίσιο έχει κρυπτογραφηθεί βάσει του WEP.

Order bit

πεδίο με μέγεθος 1bit που δείχνει εάν το πλαίσιο και τα τεμάχιά του μεταδίδονται με τη σειρά (τιμή 1) ή όχι (τιμή 0).



Σχήμα 3.5: Κεφαλίδα του πλαισίου MAC και τα υποπεδία του πεδίου ελέγχου

3.4.2.2 Πεδίο Duration / ID

Το πεδίο έχει τις ακόλουθες χρήσεις:

- Ο σκοπός του είναι να θέτει τον NAV μετρητή κάθε σταθμού ώστε να υπολογίζεται ο χρόνος που θα χρειαστεί η αποστολή κάθε επόμενου προς μετάδοση πλαισίου. Όλοι οι σταθμοί που χρησιμοποιούν τον NAV καταλαβαίνουν εάν το μέσο είναι ελεύθερο ή απασχολημένο ακόμη και αν δεν μπορούν να το “ακούσουν” (ουσιαστικά οι σταθμοί ακούν την αρχή κάθε πλαισίου ενώ ενδέχεται να μην μπορούν να ακούσουν τα δεδομένα που περιέχει το πλαίσιο).
- Σε περίπτωση που ένας σταθμός βρίσκεται σε κατάσταση εξοικονόμησης ενέργειας από την οποία θέλει να επανέρθει και να ανακτήσει από το σημείο πρόσβασης τα πλαίσια που προορίζονταν για αυτόν, αποστέλλει πλαίσια που ονομάζονται PS-Poll, τα 14

πρώτα bits των οποίων δείχνουν το BSS στο οποίο ανήκει ο σταθμός και τα 2 τελευταία bits τίθενται στο 1, επομένως παίζει το ρόλο του ID κάθε σταθμού.

3.4.2.3 Διεύθυνση MAC

Όπως φαίνεται και στο σχήμα 3.6, στο πρότυπο 802.11 τα πλαίσια περιλαμβάνουν 3 ή 4 διευθύνσεις. Κάθε συσκευή στο 802.11 προσδιορίζεται μοναδικά από την 48-bit MAC διεύθυνσή της η οποία αναγράφεται επάνω σε κάθε ασύρματη κάρτα δικτύου. Εάν πρόκειται για σημείο πρόσβασης, η MAC διεύθυνση ονομάζεται Basic Service Set Identifier (BSSID). Το γεγονός ότι οι διευθύνσεις είναι μοναδικές απαλλάσσει τον χρήστη από τον καθορισμό ή τη διαχείριση τους. Η κεφαλίδα κάθε πλαισίου του προτύπου περιέχει τη MAC διεύθυνση της πηγής, του προορισμού καθώς και το BSSID. Ο πίνακας 3.2 δείχνει τους τέσσερις τύπους διευθύνσεων που έχουν οριστεί.

3.4.2.4 Έλεγχος ακολουθίας

Πεδίο που αποτελείται από 2Bytes και χρησιμοποιείται για να επανασυναρμολογήσει πλαίσια που έχουν κατατμηθεί ή να απορρίψει διπλά πλαίσια. Αποτελείται από δυο υποπεδία:

Sequence Number

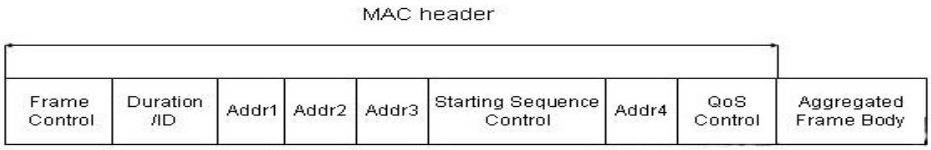
Πεδίο των 12bits που λειτουργεί ως μετρητής των πλαισίων που έχουν αποσταλεί. Ξεκινάει από το 0 και αυξάνει σταδιακά κατά 1 μονάδα για κάθε νέο πλαίσιο που μεταδίδεται. Τα κατακερματισμένα πλαίσια έχουν όλα τον ίδιο αριθμό ακολουθίας.

Fragment Number

Πεδίο των 4bits που χρησιμοποιείται για την αρίθμηση κατακερματισμένων πλαισίων, δίνοντας στο πρώτο τεμάχιο τον αριθμό 0. [10]

Πίνακας 3.1: Τιμές για τα πεδία Type/Subtype του frame control

Τύπος Πλαισίου (Type)	Bits 5-8 (Subtype)	Όνομα Subtype
Management Frames (00)	0000	Association request
	0001	Association response
	0010	Reassociation request
	0011	Reassociation response
	0100	Probe request
	0101	Probe response
	0110–0111	Reserved
	1000	Beacon
	1001	Announcement traffic indication map (ATIM)
	1010	Disassociation
	1011	Authentication
	1100	Deauthentication
	1101–1111	Reserved
Control Frames (01)	0000–1001	Reserved
	1010	Power Save (PS)-Poll
	1011	Request To Send (RTS)
	1100	Clear To Send (CTS)
	1101	Acknowledgment (ACK)
	1110	Contention-Free (CF)-End
	1111	CF-End + CF-Ack
Data Frames (10)	0000	Data
	0001	Data + CF-Ack
	0010	Data + CF-Poll
	0011	Data + CF-Ack + CF-Poll
	0100	Null function (no data)
	0101	CF-Ack (no data)
	0110	CF-Poll (no data)
	0111	CF-Ack + CF-Poll (no data)
	1000–1111	Reserved



Σχήμα 3.6: Πεδία της κεφαλίδας MAC

Πίνακας 3.2: Διευθύνσεις του 802.11

To DS	From DS	Ερμηνεία	Διευθ. 1	Διευθ. 2	Διευθ. 3	Διευθ. 4
0	0	Τα πλαίσια αποστέλλονται άμεσα από τον έναν σταθμό στον άλλο σε ένα δίκτυο Ad Hoc ή BSS	DA17	SA18	BSSID	Δ.Χ.19
0	1	Τα πλαίσια αποστέλλονται από το σημείο πρόσβασης στον σταθμό σε ένα BSS ή ESS δίκτυο	DA	BSSID	SA	Δ.Χ
1	0	Τα πλαίσια αποστέλλονται από τον σταθμό στο σημείο πρόσβασης σε ένα BSS ή ESS δίκτυο	BSSID	SA	DA	Δ.Χ
1	1	Τα πλαίσια αποστέλλονται μεταξύ δυο σημείων πρόσβασης σε μια Point-to-Point σύνδεση	RA20	TA21	DA	SA

17 Destination Address: ο τελικός προορισμός των πλαισίων όπου θα γίνει η επεξεργασία τους

18 Source Address: η πηγή του πλαισίου που αντιστοιχεί στον σταθμό που δημιούργησε το περιεχόμενο του πλαισίου

19 Δ.Χ. : δεν χρησιμοποιείται

20 Receiver Address: ο σταθμός που λαμβάνει το πλαίσιο χωρίς να είναι ο τελικός σταθμός για τον οποίο αυτό προοριζόταν

21 Transmitter Address: η MAC διεύθυνση του σταθμού που προωθεί το πλαίσιο μέσα στο δίκτυο χωρίς να είναι ο αρχικός αποστολέας που το δημιούργησε

3.4.3 Σώμα του πλαισίου (Frame Body)

Το σώμα του πλαισίου μεταφέρει τα προς μετάδοση δεδομένα από τα ανώτερα στρώματα στα κατώτερα και το μέγεθός του ποικίλει ανάλογα με το πρότυπο που χρησιμοποιείται, έτσι στο 802.11b το σώμα μπορεί να είναι μέχρι και 2312Bytes ενώ στο 802.11a και 802.11g φτάνει τα 4095Bytes. Στο σώμα του πλαισίου περιέχεται το IP πακέτο στο οποίο εμπεριέχονται οι IP και TCP κεφαλίδες. [1]

3.4.4 Ακολουθία ελέγχου πλαισίου (Frame Check Sequence)

Είναι ένα πεδίο που αποτελείται από 4Bytes (αναφέρεται και ως CRC). Πρόκειται για τιμή που υπολογίζεται πριν γίνει η αποστολή των πλαισίων ώστε όταν οι δέκτες τα λάβουν να υπολογίσουν και αυτοί το CRC και να το συγκρίνουν με εκείνο που έλαβαν. Για να πλαίσια που λήφθηκαν και δεν υπήρξε λάθος κατά τη μετάδοση, πρέπει να αποσταλεί ένα μήνυμα ACK στον αρχικό αποστολέα. Για τα πλαίσια που δεν λήφθηκαν σωστά, δεν αναμένεται ACK (πρέπει να γίνει επαναποστολή τους) και ο παραλήπτης τα απορρίπτει.

3.5 Οι διαδικασίες ανίχνευσης, ενσωμάτωσης, αυθεντικοποίησης και συσχέτισης

Πρόκειται για διαδικασίες οι οποίες είναι απαραίτητες ώστε ένας σταθμός να αποκτήσει πλήρη πρόσβαση στο μέσο μετάδοσης και να μπορεί να λαμβάνει και να μεταδίδει πλαίσια.

3.5.1 Διαδικασία ανίχνευσης δικτύου (Scanning)

Προτού χρησιμοποιήσουμε οποιοδήποτε δίκτυο, πρέπει προφανώς να το ανιχνεύσουμε. Για τα ενσύρματα δίκτυα η διαδικασία είναι απλή εφόσον αρκεί να βρούμε κάποιο καλώδιο ή κάποια πρίζα στον τοίχο. Στα ασύρματα δίκτυα τα πράγματα είναι διαφορετικά καθώς οι σταθμοί πριν ενσωματωθούν σε ένα δίκτυο θα πρέπει πρώτα να βρουν κάποιο με το οποίο να είναι συμβατοί. Αυτή η διαδικασία ονομάζεται *scanning* και υπάρχουν δυο τρόποι για να επιτευχθεί, το *active* και το *passive scanning* (αν και στο 802.11 όλες οι συσκευές χρησιμοποιούν το active scanning).

- **Passive Scanning**

  Κατά το passive scanning ένας σταθμός σαρώνει κάθε κανάλι μετάδοσης και συλλέγει πληροφορίες από κάθε μήνυμα beacon που λαμβάνει. Τα μηνύματα αυτά είναι σχεδιασμένα με τρόπο τέτοιο ώστε να επιτρέπεται σε κάθε σταθμό η συλλογή των απαραίτητων πληροφοριών για να ξεκινήσει να επικοινωνεί με κάποιο σημείο πρόσβασης σε ένα BSS, όπως η ποιότητα του εκπεμπόμενου σήματος και τα επίπεδα θορύβου. Επειδή δεν υπάρχουν ανταλλαγές δεδομένων και ο σταθμός απλά ανιχνεύει μηνύματα beacon, το passive scanning είναι μια μέθοδος που εξοικονομεί ενέργεια.

- **Active Scanning**

  Στο active scanning ο ρόλος του σταθμού είναι αρκετά διαφορετικός. Χρησιμοποιούνται *probe request* πλαίσια για να ζητήσουν απαντήσεις από ένα δίκτυο, το όνομα του οποίου είναι γνωστό. Οι σταθμοί, αντί να περιμένουν κάθε δίκτυο να κοινοποιήσει την παρουσία του με μηνύματα beacon, το ανακαλύπτουν μόνοι τους. Έτσι, αποστέλλουν probe request πλαίσια σε όλα τα σημεία πρόσβασης που βρίσκονται στο πεδίο εκπομπής τους και όσα από αυτά είναι διαθέσιμα, απαντούν με πλαίσια *probe response*. Από αυτά τα σημεία πρόσβασης ο σταθμός επιλέγει εκείνο που έχει το καλύτερο σήμα. Το μειονέκτημα αυτής της μεθόδου είναι η αυξημένη κίνηση που εισάγει στο δίκτυο και η ενέργεια που καταναλώνεται από τα μηνύματα που κυκλοφορούν.

3.5.2 Διαδικασία ενσωμάτωσης σε ένα δίκτυο (Joining)

Με την ολοκλήρωση του scanning, ο σταθμός μπορεί να επιλέξει κάποιο BSS. Η διαδικασία του joining είναι ο προθάλαμος της συσχέτισης ενός σταθμού με κάποιο δίκτυο και δεν παρέχει πρόσβαση σε αυτό.

Η επιλογή του BSS στο οποίο θα ενσωματωθεί ένας σταθμός είναι μια απόφαση που ενδέχεται να απαιτεί και την επέμβαση των χρηστών. Τα BSSs που είναι μέρη του ίδιου ESS επιτρέπεται να αποφασίσουν με όποιον τρόπο επιθυμούν, είτε ανάλογα με το επίπεδο ενέργειας είτε με τη δύναμη των εκπεμπόμενων σημάτων. Οι σταθμοί που δεν λαμβάνουν μέρος στη διαδικασία δεν γνωρίζουν πότε ένας σταθμός έχει ενσωματωθεί σε ένα δίκτυο, επειδή πρόκειται για μια διαδικασία εσωτερική ως προς τον σταθμό, καθώς περιλαμβάνει το ταίριασμα των τοπικών παραμέτρων με τις παραμέτρους που απαιτούνται από το επιλεγμένο BSS. Ένας από τους σημαντικότερους στόχους που πρέπει να επιτευχθεί είναι ο συγχρονισμός των πληροφοριών χρονισμού μεταξύ του κινητού σταθμού και του υπόλοιπου δικτύου.

Ο σταθμός πρέπει επίσης να ταιριάξει τις παραμέτρους του φυσικού επιπέδου, κάτι το οποίο εγγυάται ότι οποιεσδήποτε ανταλλαγές δεδομένων με το BSS γίνονται στο σωστό κανάλι (πχ η χρήση χρονιστών εγγυάται ότι όταν χρησιμοποιείται η FHSS, οι σταθμοί μεταπηδούν μεταξύ των καναλιών στον σωστό χρόνο). Η χρήση του BSSID εξασφαλίζει ότι οι μεταδόσεις κατευθύνονται στο σωστό σύνολο σταθμών και αγνοούνται από τους σταθμούς που ανήκουν σε ένα άλλο BSS.

3.5.3 Αυθεντικοποίηση ενός σταθμού (Authentication)

Καθώς τα ασύρματα δίκτυα δεν έχουν τη δυνατότητα να προστατεύονται με φυσικούς τρόπους όπως τα ενσύρματα, εφαρμόζουν διαφορετικές διαδικασίες ώστε να παραμένουν ασφαλή και να είμαστε βέβαιοι ότι μόνο εξουσιοδοτημένοι σταθμοί μπορούν να τα προσπελαύνουν.

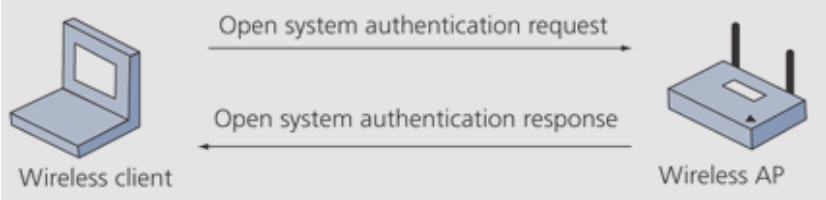
Η αυθεντικοποίηση είναι η διαδικασία που συμβαίνει πριν να ενσωματωθεί ένας σταθμός σε ένα δίκτυο. Το πρότυπο 802.11 ορίζει τρεις καταστάσεις στις οποίες μπορεί να βρίσκεται ένας σταθμός σχετικά με τις διαδικασίες αυθεντικοποίησης και ενσωμάτωσής του στο δίκτυο. Αυτές είναι οι εξής:

- Αρχική κατάσταση κατά την οποία ο σταθμός δεν έχει αυθεντικοποιηθεί και δεν έχει ενσωματωθεί στο δίκτυο
- Έχει γίνει η αυθεντικοποίηση του σταθμού αλλά εκκρεμεί η ενσωμάτωσή του στο δίκτυο
- Ο σταθμός είναι αυθεντικοποιημένος και έχει ενταχθεί στο δίκτυο

Ο μηχανισμός που παρέχεται από το πρότυπο εξουσιοδοτεί το σημείο πρόσβασης να αποφασίζει αν ένας σταθμός μπορεί να ενσωματωθεί στο δίκτυο ή όχι. Για να γίνει αυτό υπάρχουν δυο μέθοδοι, η αυθεντικοποίηση ανοιχτού συστήματος - Open Authentication Process, και η αυθεντικοποίηση μοιραζόμενου κλειδιού - Shared Key Authentication Process.

3.5.3.1 Αυθεντικοποίηση ανοιχτού συστήματος

Σύμφωνα με αυτόν τον τρόπο αυθεντικοποίησης, το σημείο πρόσβασης δέχεται έναν σταθμό χωρίς να επικυρώσει την ταυτότητά του. Απαιτείται η χρήση δυο τύπων πλαισίων, το πλαίσιο από την πλευρά του κινητού σταθμού είναι ένα πλαίσιο διαχείρισης και παρόλο που δεν υπάρχει επίσημη αναφορά του 802.11 σε αυτό το πλαίσιο, ονομάζεται *authentication request πλαίσιο*. Το στοιχείο που κάνει μοναδικό κάθε σταθμό είναι η MAC διεύθυνσή του, επομένως μπορεί να λειτουργήσει ως αναγνωριστικό των σταθμών. Έτσι, τα σημεία πρόσβασης χρησιμοποιούν την διεύθυνση πηγής των πλαισίων ως αναγνωριστικό του αποστολέα. Έπειτα το σημείο πρόσβασης επεξεργάζεται την αίτηση ενός σταθμού και απαντάει. Το πλαίσιο απάντησης είναι και αυτό ένα μήνυμα διαχείρισης όπως και το πρώτο πλαίσιο που αποστέλλεται από τον σταθμό. Η διαδικασία φαίνεται στο ακόλουθο σχήμα.



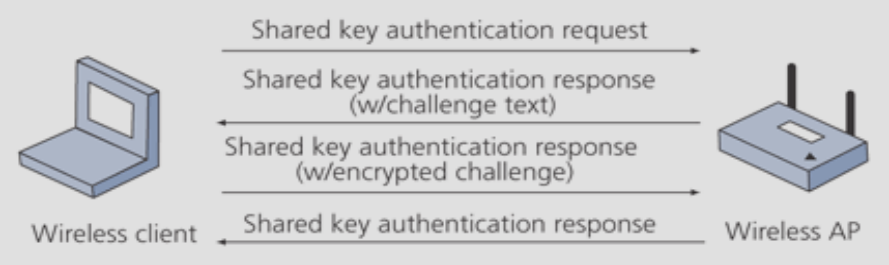
Σχήμα 3.7: Αυθεντικοποίηση ανοιχτού συστήματος

3.5.3.2 Αυθεντικοποίηση προμοιρασμένου κλειδιού

Πρόκειται για μέθοδο αυθεντικοποίησης που εφαρμόζεται σε προϊόντα τα οποία υλοποιούν το WEP. Επίσης, το 802.11 απαιτεί από κάθε σύστημα που χρησιμοποιεί το WEP να υλοποιεί την αυθεντικοποίηση αυτού του τύπου. Πριν την αυθεντικοποίηση, πρέπει να έχει μοιραστεί στους σταθμούς ένα κλειδί, ενώ η αυθεντικοποίηση πραγματοποιείται με τη χρήση τεσσάρων πλαισίων διαχείρισης. Η διαδικασία που ακολουθείται είναι η εξής (σχήμα 3.8):

- Ο σταθμός αποστέλλει ένα πλαίσιο αυθεντικοποίησης στο σημείο πρόσβασης
- Το σημείο πρόσβασης απαντάει με ένα πλαίσιο αυθεντικοποίησης που περιέχει ένα τυχαίο μήνυμα μήκους 128 bits, δηλαδή το *challenge text*
- Το challenge text κρυπτογραφείται από τον σταθμό με το προμοιρασμένο κλειδί κρυπτογράφησης και αποστέλλεται ξανά στο σημείο πρόσβασης
- Το σημείο πρόσβασης θα προσπαθήσει να αποκρυπτογραφήσει το challenge text και εάν το μήνυμα είναι το ίδιο με το αρχικό challenge text που είχε αποστείλει το σημείο πρόσβασης στην προηγούμενη φάση, σημαίνει ότι ο σταθμός έχει το σωστό κλειδί και του δίνεται το δικαίωμα πρόσβασης στο δίκτυο.

Η αυθεντικοποίηση προμοιρασμένου κλειδιού σε συνδυασμό με το κλειδί κρυπτογράφησης του WEP, προσφέρουν μόνο αυθεντικοποίηση ονόματος, κάτι που κάνει αρκετά εύκολη την ανίχνευση του WEP κλειδιού.



Σχήμα 3.8: Αυθεντικοποίηση προμοιρασμένου κλειδιού

3.5.4 Συσχέτιση ενός σταθμού με το δίκτυο (Association)

Από τη στιγμή ολοκλήρωσης της διαδικασίας αυθεντικοποίησης, ένας σταθμός μπορεί να συσχετιστεί με κάποιο σημείο πρόσβασης προκειμένου να έχει πλήρη πρόσβαση στο δίκτυο. Πρόκειται για διαδικασία η οποία επιτρέπει στο σύστημα διαμοιρασμού (DS) να εντοπίσει τη θέση κάθε σταθμού ώστε να προωθεί στα σωστά σημεία πρόσβασης τα πλαίσια που προορίζονται για κάθε σταθμό. Δεν επιτρέπεται η χρήση της σε δίκτυα υποδομής και είναι μια διαδικασία αντίστοιχη με την τοποθέτηση ενός καλωδίου σε ένα ενσύρματο δίκτυο. Το πρότυπο 802.11 απαγορεύει τη συσχέτιση ενός σταθμού με περισσότερα από ένα σημεία πρόσβασης.

Η διαδικασία της συσχέτισης είναι παρόμοια με τη διαδικασία της αυθεντικοποίησης και ολοκληρώνεται σε τρεις φάσεις οι οποίες είναι οι εξής:

- Αφού ο σταθμός αυθεντικοποιηθεί, αποστέλλει ένα πλαίσιο *association request*, ζητώντας να συσχετιστεί με το δίκτυο. Εάν ο σταθμός δεν έχει αυθεντικοποιηθεί ακόμη, το σημείο πρόσβασης αποστέλλει ένα *deauthentication* πλαίσιο ως απάντηση στο αίτημα.
- Έπειτα, το σημείο πρόσβασης επεξεργάζεται το αίτημα του σταθμού. Δεν υπάρχει κάποιος καθορισμένος τρόπος με τον οποίο το 802.11 να αποφασίζει πως πρέπει να γίνει η συσχέτιση του σταθμού με το δίκτυο, αυτό εξαρτάται από την υλοποίηση στην οποία βασίζεται το σημείο πρόσβασης.
  - Όταν το σημείο πρόσβασης αποδέχεται το αίτημα του σταθμού για

συσχέτιση, απαντάει θέτοντας την τιμή 0 στο πεδίο που ονομάζεται *κωδικός κατάστασης* και επίσης θέτει μια τιμή στον *κωδικό συσχέτισης (association ID – AID)*. Ο AID είναι ένα αναγνωριστικό με αριθμητική τιμή που χρησιμοποιείται ώστε να ανιχνεύεται ο σταθμός στον οποίο πρέπει να μεταδοθούν τα δεδομένα που φυλάσσονται στις προσωρινές μνήμες των σημείων πρόσβασης.

  - Η αποτυχία συσχέτισης περιλαμβάνει μόνο την αποστολή του κωδικού κατάστασης προς τον σταθμό και η διαδικασία ολοκληρώνεται.

- Το σημείο πρόσβασης ξεκινάει την επεξεργασία των πλαισίων του σταθμού.

Επίλογος

Το παρόν κεφάλαιο ήταν μια εισαγωγή στις διαδικασίες που συμβαίνουν στο επίπεδο MAC μέχρι να αποκτήσουμε πλήρη πρόσβαση στο μέσο μετάδοσης. Το επόμενο κεφάλαιο αναλύει διεξοδικά τις δυο βασικές μεθόδους πρόσβασης στο μέσο, δηλαδή την DCF και την PCF, τον μηχανισμό RTS/CTS και επίσης περιλαμβάνει ζητήματα που είναι σχετικά με την εξοικονόμηση ενέργειας.

Κεφάλαιο 4

Το MAC επίπεδο του IEEE 802.11

4.1 Εισαγωγή

Το παρόν κεφάλαιο ασχολείται με το MAC επίπεδο του προτύπου 802.11 και αναλύει διεξοδικά τη διαδικασία που ακολουθείται προκειμένου ένας σταθμός να έχει πρόσβαση στο μέσο μετάδοσης. Αναλύονται οι λειτουργίες DCF, PCF και ο μηχανισμός RTS/CTS καθώς και οι καταστάσεις στις οποίες μπορεί να τίθεται ένας σταθμός για να εξοικονομήσει ενέργεια.

4.2 Η πρόσβαση στο μέσο

4.2.1 Media Access Control Protocol - CSMA/CA

Παρά το γεγονός ότι στα ασύρματα δίκτυα υπάρχουν διάφορα interfaces ραδιοσυχνοτήτων και υπέρυθρων ακτινών, όλα χρησιμοποιούν το ίδιο πρωτόκολλο MAC το οποίο είναι ένα CSMA/CA πρωτόκολλο και ονομάζεται DCF (Distributed Coordination Function – DCF) με προαιρετική χρήση του μηχανισμού RTS/CTS (Request to Send / Clear to Send). Ωστόσο η ομάδα εργασίας 802.11 συμπεριέλαβε και την προαιρετική λειτουργία σημειακού συντονισμού (Point Coordination Function – PCF). Η λειτουργία DCF είναι αυτή που χρησιμοποιείται

σήμερα στα περισσότερα ασύρματα τοπικά δίκτυα προκειμένου να μπορούμε να προσπελάσουμε το κανάλι μετάδοσης, ενώ η λειτουργία PCF αναπτύχθηκε για μεταδόσεις δεδομένων που είναι άμεσα εξαρτημένα με τον χρόνο, όπως η μετάδοση video ή φωνής, όμως χρησιμοποιείται σπάνια.

4.2.1.1 CSMA/CA Distributed Coordination Function (DCF)

Εφόσον ένας χρήστης συνδεθεί και γίνει η αυθεντικοποίησή του σε ένα δίκτυο, μπορεί να στέλνει και να λαμβάνει πακέτα. Η μέθοδος DCF είναι αυτή που χρησιμοποιείται περισσότερο και περιγράφει τη διαδικασία με την οποία οι σταθμοί μεταδίδουν πλαίσια σε ένα δίκτυο, προσπαθώντας να αποφύγουν συγκρούσεις. Προκειμένου να καταλάβουμε πως λειτουργεί, πρέπει να εστιάσουμε σε κάποια βασικά σημεία που είναι:

- οι χρόνοι αναμονής
- το παράθυρο ανταγωνισμού/οπισθοχώρησης
- ο NAV (Network Allocation Vector)

4.2.1.2 Χρόνοι αναμονής μετάδοσης πλαισίων

Αναφερόμαστε στα χρονικά διαστήματα που μεσολαβούν ανάμεσα στις μεταδόσεις των πλαισίων από τους σταθμούς (για αυτό τον λόγο είναι γνωστά και ως διαπλαισιακά διαστήματα – Interframe Spaces ή IFS) προκειμένου να αποφευχθούν οι συγκρούσεις. Η DCF χρησιμοποιεί έναν αλγόριθμο CSMA/CA με χρονικές σχισμές. Αυτό σημαίνει ότι μια μετάδοση μπορεί να ξεκινήσει μόνο στην αρχή κάθε σχισμής.

Η πραγματική διάρκεια των χρόνων αναμονής που αναφέρουμε παρακάτω εξαρτάται από τη διάρκεια μιας χρονικής σχισμής, η οποία με τη σειρά της εξαρτάται από το πρωτόκολλο του φυσικού επιπέδου που χρησιμοποιείται (πχ στην μέθοδο FHSS η σχισμή αντιστοιχεί σε 50μsec, ενώ στην DSSS σε 20μsec). Γενικά το φυσικό επίπεδο υπέρυθρης μετάδοσης φαίνεται πιο αποδοτικό από το DSSS, το οποίο ακολούθως είναι πιο αποδοτικό από το FHSS όπως φαίνεται και

στον πίνακα 4.1. [5]

Πίνακας 4.1: Τιμές των χρόνων αναμονής και της χρονικής σχισμής σε κάθε σύστημα μετάδοσης

	FHSS	DSSS	OFDM	IR
σχισμή	50 μsec	20 μsec	9 μsec	8 μsec
SIFS	28 μsec	10 μsec	16 μsec	10 μsec
PIFS	78 μsec	30 μsec	25 μsec	18 μsec
DIFS	128 μsec	50 μsec	34 μsec	26 μsec

Κάθε σταθμός που επιθυμεί να πραγματοποιήσει μια μετάδοση πρέπει σε κάθε περίπτωση να περιμένει διάστημα ίσο με DIFS (ή EIFS αν είχε προηγηθεί κάποιο λάθος στη μετάδοση), είτε το κανάλι είναι ελεύθερο, είτε είναι απασχολημένο. Το πραγματικό μέγεθος της σχισμής καθορίζεται να είναι τουλάχιστον ίσο με το άθροισμα:

- του χρονικού διαστήματος ενεργοποίησης του πομπού
- του χρονικού διαστήματος ανίχνευσης του απασχολημένου μέσου και
- της μέγιστης καθυστέρησης διάδοσης μεταξύ δυο οποιωνδήποτε σταθμών

Αυτή η επιλογή για τη διάρκεια μιας σχισμής εξασφαλίζει ότι οι συγκρούσεις θα λαμβάνουν χώρα μόνο όταν δυο ή περισσότεροι σταθμοί επιλέγουν να μεταδώσουν στην ίδια σχισμή, επειδή η πληροφορία για την ύπαρξη μετάδοσης που ξεκίνησε στη σχισμή k διαδίδεται σε ολόκληρο το δίκτυο πριν την έναρξη της σχισμής k+1. [5]

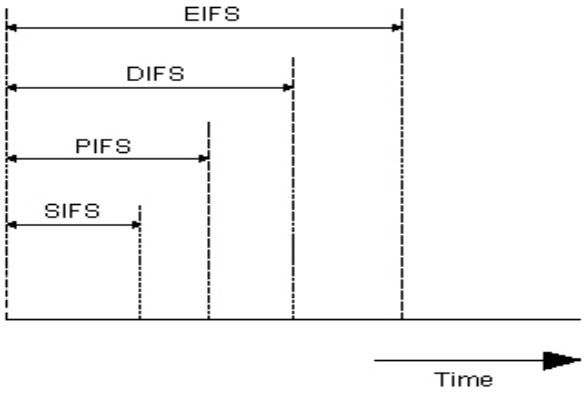
Συνολικά το επίπεδο MAC χρησιμοποιεί τέσσερις διαφορετικούς τύπους χρονικών διαστημάτων αναμονής μέσα σε κάθε πλαίσιο, που ο καθένας εξυπηρετεί διαφορετικούς σκοπούς και ισχύει η σχέση:

SIFS < PIFS < DIFS < EIFS

- ***SIFS - Short Interframe Space:*** πρόκειται για το μικρότερο χρονικό διάστημα και χρησιμοποιείται για μεταδόσεις δεδομένων με υψηλή προτεραιότητα όπως τα CTS πλαίσια και τα ACKs αλλά και για τμήματα

ενός κατακερματισμένου πλαισίου. Τέτοιου είδους μεταδόσεις εκκινούν όταν το χρονικό διάστημα που ορίζει το SIFS πεδίο λήξει.

- ***PIFS - PCF Interframe Space:*** η μέθοδος PCF είναι ένας σπάνια χρησιμοποιούμενος μηχανισμός ο οποίος είναι απαραίτητος για μεταδόσεις που σχετίζονται άμεσα με το χρόνο, όπως η μετάδοση φωνής και το video. Στην PCF το σημείο πρόσβασης παίρνει κατά διαστήματα τον έλεγχο του καναλιού ώστε αυτό να προσπελαύνει το μέσο πριν από οποιονδήποτε άλλο σταθμό. Σε αυτό το χρονικό διάστημα που ονομάζεται CF (contention-free), το σημείο πρόσβασης “ρωτάει” κάθε σταθμό (polling) που αποστέλλει δεδομένα τα οποία εξαρτώνται άμεσα από τον χρόνο αν πρόκειται να μεταδώσει. Το χρονικό διάστημα που απαιτείται για να αποσταλεί το μήνυμα ελέγχου για το σημείο πρόσβασης ονομάζεται PIFS. Στο τέλος του CF διαστήματος το δίκτυο επιστρέφει στην DCF μέθοδο. Το PIFS είναι στην ουσία ίσο με SIFS συν μια χρονική σχισμή.
- ***DIFS - DCF Interframe Space:*** αντιπροσωπεύει τον χρόνο που απαιτείται όταν ένας σταθμός θέλει να ξεκινήσει μια μετάδοση δεδομένων. Είναι ίσος με τον SIFS συν δυο σχισμές.
- ***EIFS - Extended Interframe Space:*** Όλοι οι σταθμοί που χρησιμοποιούν DCF χρησιμοποιούν το EIFS όταν έπειτα από τη μετάδοση ενός πλαισίου εντοπίστηκε από το φυσικό επίπεδο ότι υπήρξε λανθασμένη λήψη αυτού. Έπειτα το φυσικό επίπεδο ενημερώνει το MAC επίπεδο για το λάθος. Το EIFS παράγεται από το SIFS, το DIFS και το χρόνο (σε milliseconds) που απαιτείται για την μετάδοση ενός ACK, μεταδιδόμενο με τον χαμηλότερο ρυθμό μετάδοσης που ορίζεται από το κάθε φυσικό επίπεδο και προκύπτει από τη σχέση *EIFS = aSIFSTime + ACKTxTime + DIFS.* Όπου aSIFSTime ισούται με SIFS σε milliseconds (μs) και ACKTxTime είναι ο χρόνος που απαιτείται για τη μετάδοση ενός πλαισίου ACK, μαζί με το πρόθεμα, την PLCP κεφαλίδα και κάθε επιπρόσθετη πληροφορία του φυσικού επιπέδου. [12], [16]

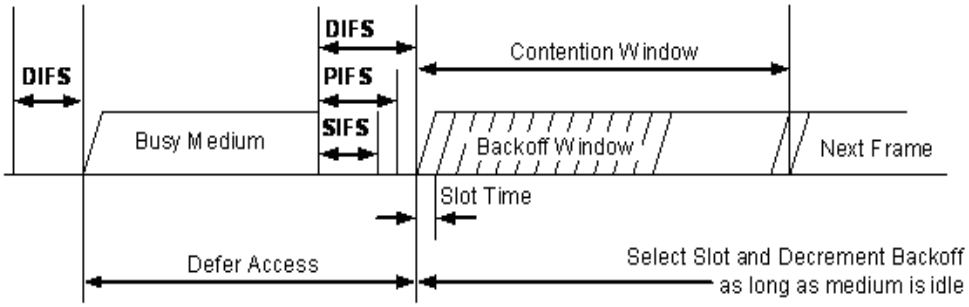


Σχήμα 4.1: Διαπλαισιακά διαστήματα αναμονής (IFS)

4.2.1.3 Παράθυρο υπαναχώρησης / οπισθοχώρησης

Η αποφυγή συγκρούσεων στο πρότυπο 802.11 υλοποιείται με τη βοήθεια του παραθύρου υπαναχώρησης (γνωστό και ως παράθυρο ανταγωνισμού ή Contention Window – CW) το οποίο αναλαμβάνει δράση σε δυο περιπτώσεις, είτε στην περίπτωση που όσο ένας σταθμός προσπαθεί να χρησιμοποιήσει το κανάλι μετάδοσης αυτό είναι απασχολημένο, είτε στην περίπτωση που ένας σταθμός προσπάθησε ανεπιτυχώς να χρησιμοποιήσει το κανάλι.

Ο σταθμός που θέλει να μεταδώσει πλαίσια θέτει αρχικά έναν τυχαίο αριθμό σχισμών σε έναν μετρητή που ονομάζεται μετρητής υπαναχώρησης. Αυτή η τιμή είναι στο διάστημα [0, CW]. Οι τιμές CW είναι της μορφής 2^n-1 για παράδειγμα 31, 63, 127, 255, 511 και 1023 με ελάχιστη τιμή την CW_{min} και μέγιστη την CW_{max}. Έπειτα ο σταθμός αναμένει επί χρονικό διάστημα ίσο με ένα DIFS (ή EIFS σε περίπτωση που το τελευταίο πλαίσιο που ανιχνεύθηκε στο μέσο δεν είχε μεταδοθεί σωστά) και σταδιακά μειώνει την τιμή του μετρητή, έως ότου αυτός μηδενιστεί και ο σταθμός να μπορεί τελικά να μεταδώσει. Όσο ο σταθμός αποτυγχάνει να μεταδώσει, ο μετρητής αυξάνεται εκθετικά σύμφωνα με τον αλγόριθμο backoff και ταυτόχρονα μειώνεται η πιθανότητα συγκρούσεων.



Σχήμα 4.2: Χρόνοι αναμονής μετάδοσης πλαισίων

Το συνολικό χρονικό διάστημα αναμονής ενός σταθμού μέχρι να μεταδώσει υπολογίζεται από τον τύπο:

$$BackoffTime = Random( ) \times aSlotTime$$

Όπου

Random( ) → Ένας ψευδοτυχαίος ακέραιος αριθμός επιλεγμένος από μια ομοιόμορφη κατανομή στο διάστημα [0, CW], όπου ο CW είναι ένας ακέραιος στο διάστημα CW_{min} και CW_{max} (ισχύει η σχέση: $CW_{min} \leq CW \leq CW_{max}$) που εξαρτάται από τα χαρακτηριστικά του φυσικού επιπέδου που χρησιμοποιείται.

aSlotTime → Η χρονική διάρκεια της σχισμής που επίσης εξαρτάται από το φυσικό επίπεδο που χρησιμοποιείται. [8]

Σε περίπτωση που στο κανάλι υπάρχει μετάδοση όσο ο μετρητής υπαναχώρησης μειώνεται, όλοι οι μετρητές υπαναχώρησης “παγώνουν” και ξεκινούν ξανά να μειώνονται - από την τιμή που είχαν όταν σταμάτησαν - έπειτα από χρονικό διάστημα ενός DIFS αφού το κανάλι γίνει και πάλι αδρανές.

Εάν οι μετρητές συνέχιζαν να μειώνονται όσο υπήρχε κίνηση στο κανάλι, θα συνέβαινε σύγκρουση στην περίπτωση που κάποιοι από αυτούς έληγαν ταυτόχρονα και περισσότεροι από έναν σταθμοί αναγκάζονταν να μεταδώσουν. Το πρότυπο ορίζει κάποια συγκεκριμένα διαστήματα τιμών που μπορεί να πάρει κάθε μετρητής οπισθοχώρησης όπως φαίνεται στον πίνακα 4.2. [1]

Πίνακας 4.2: Τιμές του παραθύρου υπαναχώρησης στο IEEE 802.11

Πρότυπο	CW_{min}	CW_{max}
802.11b ή 802.11b/g	31	1023
802.11a ή 802.11g	15	1023

4.2.1.4 Διάνυσμα δέσμευσης δικτύου (Network Allocation Vector)

Πρόκειται για χρονιστή ο οποίος αποθηκεύεται σε κάθε σταθμό και χρησιμοποιείται για εικονική ανίχνευση φέροντος στο μέσο μεταφοράς δεδομένων. Τίθεται από την τιμή *duration* που υπάρχει στην κεφαλίδα κάθε πλαισίου και δίνει τη δυνατότητα στον σταθμό να αποφασίσει αν το κανάλι είναι απασχολημένο ή ελεύθερο, ακόμη και στην περίπτωση που δεν μπορεί να το “ακούσει”. Επίσης χρησιμοποιείται στην μέθοδο DCF και όταν υπάρχει δίκτυο υποδομής όπου το σημείο πρόσβασης δεσμεύει το κανάλι στέλνοντας CTS πλαίσια ώστε να θέσει τους NAV χρονιστές σε κάθε σταθμό του δικτύου. Επίσης ο μετρητής χρησιμοποιείται στην επιλογή RTS/CTS. Όταν η τιμή NAV έχει ορισθεί, ο σταθμός δεν θα προσπαθήσει να μεταδώσει και εάν ο σταθμός τρέχει τον χρονιστή οπισθοχώρησης, ο NAV θα “παγώσει” για αυτό το χρονικό διάστημα.

4.2.1.5 Λειτουργία κατανεμημένου συντονισμού (DCF)

Λειτουργία κατανεμημένου συντονισμού σημαίνει ότι όλοι οι σταθμοί συνεργάζονται ώστε να αποφευχθεί μια σύγκρουση. Χρησιμοποιείται τόσο σε δίκτυα IBSS όσο και σε δίκτυα υποδομής.

Ένας σταθμός που επιθυμεί να μεταδώσει, ακούει το μέσο και αποφασίζει αν υπάρχει μετάδοση από κάποιον άλλο σταθμό. Αν το μέσο είναι είναι ελεύθερο για DIFS, ο σταθμός θα ξεκινήσει να μεταδίδει. Η μέθοδος DCF ορίζει το DIFS ως

ελάχιστο χρονικό διάστημα μεταξύ δυο διαδοχικών πλαισίων. Ο σταθμός-αποστολέας ελέγχει το μέσο για αυτή τη χρονική διάρκεια και αποφασίζει εάν είναι ελεύθερο ή όχι. Σε δίκτυα υποδομής του προτύπου 802.11, το κανάλι που χρησιμοποιείται για μεταφορά δεδομένων προς το σημείο πρόσβασης, αλλά και από αυτό, είναι μόνο ένα και παρά το γεγονός ότι τα σημεία πρόσβασης υπάρχουν κυρίως ως σταθμοί ελέγχου της κυκλοφορίας των δεδομένων σε ένα BSS ή ESS δίκτυο, διεκδικούν και αυτά χρήση του καναλιού μετάδοσης, όπως και κάθε άλλος σταθμός.

Για κάθε πληροφορία που μεταδίδεται σε όλους τους σταθμούς του δικτύου (broadcast) δεν λαμβάνονται πλαίσια επιβεβαίωσης παράδοσης, ενώ ο κάθε σταθμός τοποθετεί την MAC διεύθυνση του προορισμού (δηλαδή τη διεύθυνση broadcast), στο κατάλληλο πεδίο μέσα σε ένα πλαίσιο (δηλαδή στο destination address field).

4.2.1.6 DCF - όταν το κανάλι είναι ελεύθερο

Ο σταθμός που επιθυμεί να μεταδώσει πρέπει αρχικά να ελέγξει αν το κανάλι μετάδοσης είναι ελεύθερο, γι' αυτό ακολουθεί δυο μεθόδους, την φυσική ανίχνευση φέροντος κατά την οποία “ακούει” το κανάλι μέσω του φυσικού επιπέδου, και την εικονική ανίχνευση φέροντος κατά την οποία ελέγχει την τιμή του NAV μέσω του MAC επιπέδου.

- Σταθμός-αποστολέας

Αρχικά ο αποστολέας πρέπει να αποφασίσει αν το κανάλι είναι ελεύθερο ή όχι. Για να το πετύχει αυτό χρησιμοποιεί τις δυο παραπάνω μεθόδους δηλαδή “ακούει” το μέσο και εξετάζει τον μετρητή NAV. Εάν η τιμή του NAV είναι μεγαλύτερη του 0 τότε ο αποστολέας θεωρεί ότι το μέσο είναι απασχολημένο ανεξάρτητα από το γεγονός ότι “ακούγοντας” το μέσο φάνηκε ότι ήταν ελεύθερο. Για να μεταδώσει ένας σταθμός θα πρέπει να ισχύουν τα εξής:

  - ο σταθμός να “ακούσει” το μέσο και αυτό να είναι ελεύθερο και
  - η τιμή του NAV να είναι 0

Στην περίπτωση που ο αποστολέας μετά τους ελέγχους του αποφασίσει ότι

το κανάλι ελεύθερο, αναμένει για διάστημα ίσο με DIFS μέχρι να μεταδώσει. Αν δυο σταθμοί θεωρήσουν ακριβώς την ίδια χρονική στιγμή το κανάλι ελεύθερο τότε θα συμβεί σύγκρουση, ενώ αν κάποιος σταθμός “ακούσει” κάποια μετάδοση κατά τη διάρκεια του DIFS, θα αναβάλλει την μετάδοσή του και θα ακολουθήσει τους κανόνες που ισχύουν όταν το κανάλι είναι απασχολημένο.

- Σταθμός-παραλήπτης

Ο σταθμός-παραλήπτης του πλαισίου λαμβάνοντάς το, θα το αντιγράψει σε μια προσωρινή μνήμη προκειμένου να το ελέγξει για σφάλματα (υπολογισμός του check sequence πεδίου π.χ. 32-bit CRC) και εάν δεν εντοπιστεί κανένα, τότε έπειτα από διάστημα ίσο με ένα SIFS θα αποστείλει ένα μήνυμα ACK των 14bytes στην πηγή.

Εάν εντοπιστούν σφάλματα, τότε το πλαίσιο θα απορριφθεί χωρίς κανένα μήνυμα ειδοποίησης στην πηγή, κάνοντας τον αποστολέα να υποθέσει πως συνέβη σύγκρουση ή κάποια άλλη δυσλειτουργία κατά την μετάδοση ώστε να θέσει σε λειτουργία τον μετρητή οπισθοχώρησής του και μετά την πάροδο ενός διαστήματος να επαναμεταδώσει. Αφού θέσει σε λειτουργία τον μετρητή οπισθοχώρησης, τον αρχικοποιεί έπειτα από ένα DIFS και όταν λήξει μεταδίδει. Σε περίπτωση που ενώ ο μετρητής μειώνεται, κάποιος άλλος σταθμός προλάβει να μεταδώσει, ο μετρητής “παγώνει” μέχρι να αποσταλεί το άλλο μήνυμα και ξεκινάει ξανά εφόσον το κανάλι γίνει αδρανές μετά από DIFS.

Το σύστημα με τους μετρητές διασφαλίζει ότι κάποιες μεταδώσεις θα έχουν προτεραιότητα έναντι κάποιων άλλων. Για παράδειγμα, κάθε σταθμός που επιθυμεί να μεταδώσει θα πρέπει να περιμένει για διάστημα τουλάχιστον ίσο με DIFS ενώ ένας σταθμός που θέλει να μεταδώσει ένα μήνυμα ACK θα περιμένει για ένα SIFS. Έτσι, η μετάδοση ενός μηνύματος ACK πάντα θα προηγείται εκείνης ενός άλλου πλαισίου.

4.2.1.7 DCF - όταν το κανάλι είναι απασχολημένο

Όταν το κανάλι είναι απασχολημένο, οι σταθμοί παίρνουν επιπρόσθετα μέτρα ώστε να αποφεύγεται η σύγκρουση. Έτσι, κάθε σταθμός που θέλει να

μεταδώσει θέτει τον μετρητή οπισθοχώρησής του σε έναν τυχαίο αριθμό μεταξύ του μηδενός και του CW, το οποίο ορίζει τον αριθμό των σχισμών που πρέπει ένας σταθμός να περιμένει προκειμένου να μεταδώσει. Ο μετρητής δεν ξεκινάει να τρέχει μέχρι να περάσει ένα DIFS και το κανάλι να είναι ελεύθερο.

Σε περίπτωση που ξεκινήσει κάποια άλλη μετάδοση όσο ο μετρητής τρέχει, τότε αυτός “παγώνει” όσο υπάρχει μετάδοση για να επανεκκινήσει μετά από ένα DIFS αφού το κανάλι γίνει ελεύθερο. Όταν ο μετρητής λήξει, ο σταθμός στέλνει απευθείας και έπειτα περιμένει για διάστημα ίσο με ένα SIFS για μηνύματα ACKs (σχήμα 4.5). Το διάστημα αναμονής DIFS, εξασφαλίζει ότι τα μηνύματα ACKs θα μπορέσουν να μεταδοθούν με τη μέγιστη προτεραιότητα. Αυτό συμβαίνει καθώς μεταξύ δυο σταθμών όπου ο ένας θέλει να στείλει ένα οποιοδήποτε πλαίσιο και ένας άλλος θέλει να στείλει ένα ACK, προηγείται η μετάδοση του ACK, εφόσον εκείνος ο σταθμός περιμένει διάστημα ίσο με SIFS ενώ ο άλλος περιμένει διάστημα ίσο με με DIFS.

Εάν δεν ληφθεί μήνυμα επιβεβαίωσης σημαίνει ότι συνέβη σύγκρουση ή κάποια άλλη δυσλειτουργία. Τότε ο σταθμός αυξάνει εκθετικά τον μετρητή οπισθοχώρησής του και επαναλαμβάνει τη διαδικασία. Οι αυξήσεις είναι πάντα της μορφής 2^n-1 και κάθε φορά που γίνεται μια αποτυχημένη προσπάθεια μετάδοσης, ο μετρητής αυξάνεται, μέχρι να φτάσει στο υψηλότερο επιτρεπτό όριό του (δηλαδή το CW_{max}).

4.2.1.8 Το πρόβλημα του κρυφού σταθμού (Hidden node problem)

Η αναβολή της μετάδοσης δεδομένων στην περίπτωση που άλλοι σταθμοί μεταδίδουν, προϋποθέτει ότι κάθε σταθμός ενός τοπικού δικτύου μπορεί και “ακούει” τους υπόλοιπους. Ωστόσο αυτό δεν ισχύει πάντα. Παρά το γεγονός ότι σε ένα δίκτυο υποδομής το σημείο πρόσβασης μπορεί να ακούσει κάθε μετάδοση, υπάρχει περίπτωση δυο σταθμοί μεταξύ τους να μην έχουν αυτή τη δυνατότητα λόγω της απόστασης που τους χωρίζει ή εξαιτίας άλλων εμποδίων. Το ίδιο μπορεί να συμβεί και σε δίκτυα ad hoc. Σε δίκτυα υποδομής, η κατάσταση κατά την οποία οι σταθμοί ακούν το σημείο πρόσβασης αλλά δεν μπορούν να ακούσουν την

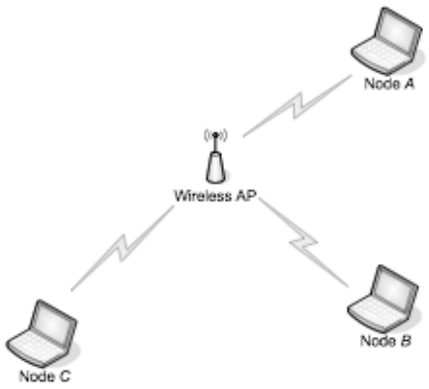
μετάδοση κάποιου άλλου σταθμού, ονομάζεται *πρόβλημα του κρυφού σταθμού*. Το ίδιο πρόβλημα εμφανίζεται και σε δίκτυα ad hoc όταν ένας σταθμός, ακούγοντας το μέσο, δεν ανιχνεύει κάποια μετάδοση, το θεωρεί ελεύθερο και μεταδίδει, ενώ στην πραγματικότητα ισχύει το αντίθετο, εφόσον υπάρχει μετάδοση από άλλον σταθμό.

Το συγκεκριμένο πρόβλημα αυξάνει κατά πολύ την πιθανότητα σύγκρουσης, εφόσον οι κρυφοί σταθμοί μπορεί να μεταδίδουν δεδομένα όσο υπάρχει άλλη μετάδοση την οποία δεν ακούν. Αυτό επιδιώκει να λύσει ο μηχανισμός RTS/CTS, γνωστός και ως *εικονική ανίχνευση φέροντος*, η χρήση του οποίου είναι προαιρετική στο πρότυπο 802.11 και αναλύεται παρακάτω.

- **Κρυφοί σταθμοί σε δίκτυα υποδομής**

Στο παρακάτω σχήμα οι σταθμοί Α, Β και C βρίσκονται μέσα στην περιοχή κάλυψης του σημείου πρόσβασης. Ο σταθμός Α μπορεί να ανιχνεύσει μια μετάδοση από τον σταθμό Β αλλά όχι και από τον σταθμό C. Σε μια τέτοια περίπτωση, εάν ο σταθμός Α αρχίσει να μεταδίδει, θα συμβεί σύγκρουση. Το αποτέλεσμα θα είναι να μην μπορεί να μεταδώσει ούτε ο σταθμός Α ούτε ο C, με συνέπεια την επιβάρυνση του δικτύου και τη μείωση της ρυθμοαπόδοσής του.

Με την ενεργοποίηση του μηχανισμού RTS/CTS σε έναν σταθμό, δεν θα αποστέλλεται κανένα πλαίσιο δεδομένων μέχρι να ολοκληρωθεί η RTS/CTS χειραψία μεταξύ του σταθμού που θέλει να μεταδώσει και του σημείου πρόσβασης.



Σχήμα 4.3: Το πρόβλημα του κρυφού σταθμού – δίκτυο υποδομής

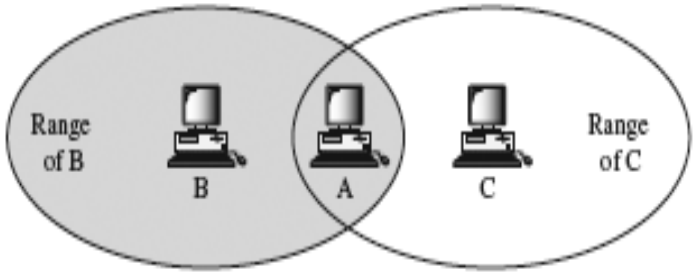
Ο σταθμός ξεκινάει τη διαδικασία στέλνοντας ένα πλαίσιο RTS. Το σημείο πρόσβασης απαντά στο RTS στέλνοντας ένα CTS πλαίσιο. Ο σταθμός πρέπει να λάβει το CTS πλαίσιο πριν στείλει το πλαίσιο δεδομένων. Το CTS πλαίσιο περιέχει μια χρονική τιμή η οποία αποτελεί ειδοποίηση για τους υπόλοιπους σταθμούς ώστε να περιμένουν και να μην επιχειρήσουν μετάδοση στο μέσο, όσο ο σταθμός που έστειλε το RTS πλαίσιο αποστέλλει δεδομένα. Με αυτόν τον τρόπο, ο μηχανισμός RTS/CTS μειώνει τις συγκρούσεις και αυξάνει την απόδοση του δικτύου εφόσον υπάρχουν κρυφοί σταθμοί. Το ακόλουθο σχήμα δείχνει τη διαδικασία κατάληψης του μέσου από έναν σταθμό με τον μηχανισμό RTS/CTS ενώ το σχήμα ... δείχνει τους χρόνους αναμονής στη διαδικασία.

Σχήμα 4.4: Διαδικασία κατάληψης του μέσου από έναν σταθμό σε δίκτυο υποδομής

Εάν το δίκτυο δεν έχει κρυφούς σταθμούς, η χρήση του μηχανισμού θα το επιβαρύνει και θα μειώσει την ρυθμοαπόδοσή του. Σε αυτή την περίπτωση τα επιπλέον πλαίσια RTS/CTS “κοστίζουν” περισσότερο από το κέρδος που έχουμε μειώνοντας τις επαναποστολές με τη χρήση του μηχανισμού. Επιπλέον, η χρήση του μηχανισμού βοηθάει, ειδικά όταν τα πλαίσια δεδομένων είναι πολύ μεγαλύτερα από τα RTS/CTS.

- **Κρυφοί σταθμοί σε δίκτυα Ad Hoc**

Έστω ότι έχουμε τρεις σταθμούς, τους A, B και C όπως δείχνει το παρακάτω σχήμα, όπου η εμβέλεια του σταθμού B σημειώνεται με την αριστερή έλλειψη και κάθε σταθμός μέσα σε αυτή την περιοχή ακούει κάθε σήμα που μεταδίδει ο B. Ο σταθμός C έχει εμβέλεια που σημειώνεται στο σχήμα από τη δεξιά έλλειψη και κάθε σταθμός μέσα σε αυτήν την περιοχή ακούει τις μεταδόσεις του C. Ο σταθμός C βρίσκεται έξω από την εμβέλεια του B και ομοίως ο B έξω από την εμβέλεια του C. Ωστόσο, ο σταθμός A μπορεί να ακούει τις μεταδόσεις και του B και του C εφόσον βρίσκεται εντός της εμβέλειας και των δυο σταθμών.



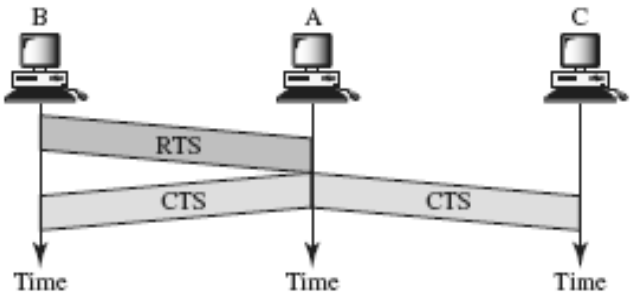
Σχήμα 4.5: Εμβέλεια σταθμών σε δίκτυο ad hoc

Ως *εμβέλεια μετάδοσης* του σταθμού A καθορίζεται η περιοχή στην οποία οι υπόλοιποι σταθμοί μπορούν να λάβουν σωστά τα πακέτα του. Από την άλλη πλευρά, ως *περιοχή ανίχνευσης φέροντος* του A καθορίζεται η περιοχή που περιλαμβάνει τους σταθμούς εκείνους, οι μεταδόσεις των οποίων γίνονται αντιληπτές από τον A, αλλά αυτό δεν συνεπάγεται απαραίτητα ότι ο A είναι σε θέση να λάβει τα μεταδιδόμενα πακέτα. Γενικά δεν μπορούμε να ισχυριστούμε ότι αυτές οι δυο περιοχές ταυτίζονται πάντα (πχ η περιοχή ανίχνευσης φέροντος μπορεί να είναι διπλάσια της περιοχής μετάδοσης δεδομένων). [17]

Ο σταθμός C είναι εκτός της περιοχής μετάδοσης του σταθμού B και έτσι εμφανίζεται ως κρυφός σταθμός ως προς τον σταθμό B. Ωστόσο, εάν η περιοχή ανίχνευσης φέροντος του C είναι μεγαλύτερη από εκείνη του B, ο C παύει να είναι

κρυφός σταθμός επειδή μπορεί να ακούσει τις μεταδόσεις του B και να αποφύγει να μεταδώσει κατά τη διάρκεια μετάδοσης εκείνου. Αυτός ο μηχανισμός μπορεί να περιορίσει το πρόβλημα του κρυφού σταθμού.

Το ακόλουθο σχήμα δείχνει ότι το RTS πλαίσιο από τον σταθμό B φτάνει στον A αλλά όχι στον C. Ωστόσο, επειδή και ο B και ο C είναι στην περιοχή εμβέλειας του A, το CTS πλαίσιο που περιέχει τη διάρκεια της μετάδοσης των δεδομένων από τον B στον A, λαμβάνεται και από τον σταθμό C. Ο σταθμός C αντιλαμβάνεται ότι το κανάλι χρησιμοποιείται από κάποιον κρυφό σταθμό και αποφεύγει να μεταδώσει μέχρι την πάροδο του διαστήματος που ορίζεται στο πεδίο *duration* του CTS πλαισίου.



Σχήμα 4.6: Χειραψία RTS/CTS σε δίκτυο ad hoc

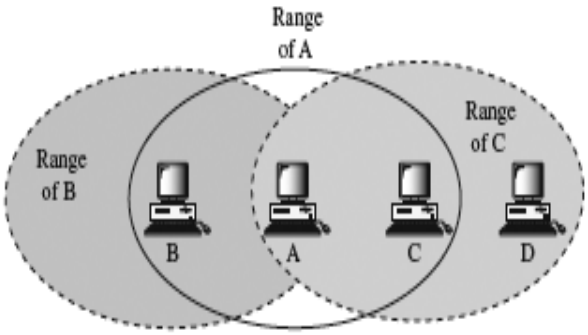
4.2.1.9 Το πρόβλημα του εκτεθειμένου σταθμού (Exposed node problem)

Το πρόβλημα του εκτεθειμένου σταθμού εμφανίζεται όταν ένας σταθμός αποφεύγει να μεταδώσει εξαιτίας της ύπαρξης μετάδοσης από κάποιον γειτονικό σταθμό. Στο ακόλουθο σχήμα που αναπαριστά το πρόβλημα, φαίνονται οι σταθμοί R1, S1, S2 και R2, όπου ο κάθε παραλήπτης (R1, R2) είναι εκτός της εμβέλειας του άλλου, ενώ οι δυο αποστολείς (S1, S2) βρίσκονται ενδιάμεσα. Εάν υπάρξει μετάδοση μεταξύ των S1 και R1, ο σταθμός S2 δεν θα εκπέμψει προς τον R2, επειδή έπειτα από την ανίχνευση του μέσου, θεωρεί ότι θα οδηγηθεί σε σύγκρουση με τον σταθμό S1.

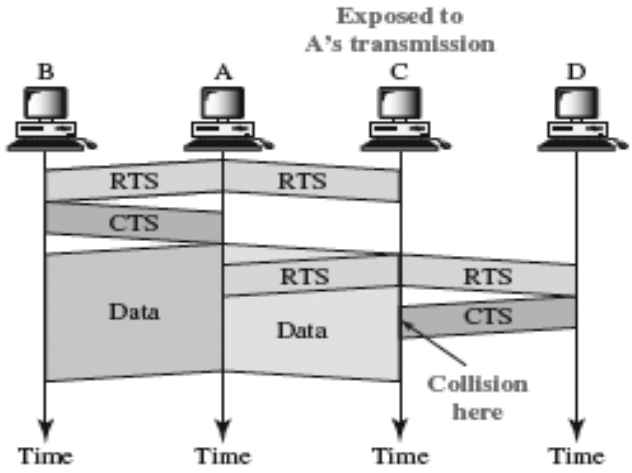
Σχήμα 4.7: Το πρόβλημα του εκτεθειμένου σταθμού

Ο μηχανισμός RTS/CTS του προτύπου 802.11 βοηθάει στη λύση του προβλήματος μόνο εάν υπάρχει *συγχρονισμός* μεταξύ των σταθμών. Όταν ένας σταθμός ακούσει ένα πλαίσιο RTS από κάποιον γειτονικό σταθμό, αλλά δεν ακούσει το αναμενόμενο CTS, αυτός ο σταθμός πρέπει να θεωρηθεί εκτεθειμένος και επιτρέπεται να μεταδώσει σε άλλους, γειτονικούς του σταθμούς. Εάν οι σταθμοί δεν είναι συγχρονισμένοι, το πρόβλημα που πιθανόν μπορεί να συμβεί είναι ο αποστολέας να μην ακούσει το CTS ή το ACK στη διάρκεια μετάδοσης των δεδομένων του δεύτερου αποστολέα (σχήμα 4.8). [17]

Σε μια περίπτωση όπως αυτή του σχήματος 4.8 που ο σταθμός C είναι εκτεθειμένος, η RTS/CTS χειραψία δεν φαίνεται χρήσιμη. Ο σταθμός C ακούει το RTS πλαίσιο από τον σταθμό A αλλά δεν μπορεί να ακούσει το CTS πλαίσιο από τον B. Ο σταθμός C αφού ακούσει το RTS από τον A, περιμένει για ένα χρονικό διάστημα μέχρις ότου το CTS πλαίσιο να φτάσει από τον B στον A. Έπειτα, στέλνει ένα RTS πλαίσιο στον σταθμό D για να διαπιστώσει την διαθεσιμότητά του ώστε να επικοινωνήσουν. Και οι δυο σταθμοί A και B μπορούν να ακούσουν αυτό το RTS, αλλά ο σταθμός A μπορεί να αποστέλλει δεδομένα και όχι να λαμβάνει. Ωστόσο ο σταθμός B απαντάει με ένα CTS πλαίσιο και εδώ εντοπίζεται το πρόβλημα. Εάν ο σταθμός A ξεκινήσει να στέλνει δεδομένα, ο σταθμός C δεν μπορεί να ακούσει τα CTS από τον D εξαιτίας σύγκρουσης και έτσι δεν μπορεί να αποστείλει δεδομένα στον D. Παραμένει εκτεθειμένος μέχρι να ολοκληρωθεί η αποστολή δεδομένων από τον A (σχήμα 4.9).



Σχήμα 4.8: Το πρόβλημα του εκτεθειμένου σταθμού



Σχήμα 4.9: Χειραψία RTS/CTS και το πρόβλημα του εκτεθειμένου σταθμού

4.2.1.10 Τρόπος λειτουργίας του μηχανισμού RTS / CTS

Ο σταθμός που επιθυμεί να μεταδώσει, είτε πρόκειται για το σημείο πρόσβασης είτε για απλούς σταθμούς, έπειτα από χρονικό διάστημα ίσο με ένα DIFS, στέλνει ένα RTS πλαίσιο μεγέθους 20Bytes, εφόσον διαπιστώσει ότι το κανάλι δεν χρησιμοποιείται. Εάν το κανάλι είναι απασχολημένο, το RTS πλαίσιο αποστέλλεται σύμφωνα με τους κανόνες που περιγράψαμε για το απασχολημένο κανάλι.

Το RTS πλαίσιο είναι ουσιαστικά ένα πλαίσιο ελέγχου, το οποίο περιέχει πεδία όπως η διεύθυνση του αποστολέα, η διεύθυνση του παραλήπτη και η χρονική διάρκεια που απαιτείται για την αποστολή των δεδομένων (σχήμα 4.10). Στην περίπτωση που ο σταθμός στείλει ένα RTS πλαίσιο ενώ υπάρχει άλλη μετάδοση, θα συμβεί σύγκρουση με τη διαφορά ότι ο σταθμός, προτού επιχειρήσει να ξαναστείλει το μήνυμα, θα χρησιμοποιήσει τον μηχανισμό οπισθοχώρησης.

Από την πλευρά του παραλήπτη, έπειτα από διάστημα ενός SIFS επιστρέφεται ένα CTS μήνυμα των 16Bytes που περιέχει την διεύθυνση του παραλήπτη και μια τιμή για τη χρονική διάρκεια της μεταφοράς. Το γεγονός ότι το CTS μήνυμα στέλνεται μετά από διάστημα ενός SIFS δίνει προτεραιότητα σε τέτοιου είδους μεταδόσεις (επειδή DIFS > SIFS).

Κάθε σταθμός που “ακούει” το RTS ή το CTS μήνυμα, είτε βρίσκεται σε δίκτυο ad hoc είτε σε δίκτυο υποδομής, θα ξέρει τη διάρκεια κατά την οποία το μέσο θα είναι απασχολημένο. Επίσης όλοι οι σταθμοί χρησιμοποιούν το πεδίο με αυτή τη χρονική διάρκεια για να θέσουν τους NAVs και μέσα σε αυτή την περίοδο δεν θα επιχειρήσουν καμία αποστολή.

Ο σταθμός θα ξεκινήσει να μεταδίδει δεδομένα έπειτα από ένα SIFS από τη στιγμή που παρέλαβε το CTS και αφού αποστείλει τα δεδομένα περιμένει και πάλι διάστημα ίσο με ένα SIFS για να λάβει ACK από τον παραλήπτη.

Το σχήμα 4.10 δείχνει τη μορφή των πλαισίων για τους τέσσερις τύπους μηνυμάτων που χρησιμοποιούνται στη λειτουργία RTS/CTS καθώς και το πλήθος των bytes που καταλαμβάνει κάθε πεδίο μέσα στα πλαίσια. Εκτός από τα bytes που αφιερώνονται για ελέγχους και χρονικά διαστήματα, υπάρχει μια συσχέτιση στα πλαίσια RTS και CTS εφόσον το πρώτο περιέχει πάντα τη διεύθυνση και του παραλήπτη και του αποστολέα ενώ το CTS πλαίσιο περιέχει μόνο τη διεύθυνση του αποστολέα ώστε να είναι ξεκάθαρος ο προορισμός της απάντησης του CTS μηνύματος.

Παρά τα υπέρ της χρήσης RTS/CTS μηνυμάτων υπάρχουν και περιπτώσεις που δεν ενδείκνυται η χρήση του μηχανισμού λόγω επιβάρυνσης του δικτύου. Μια τέτοια περίπτωση είναι η εκπομπή σε ομάδες σταθμών – είτε broadcast είτε multicast. Σε τέτοιες περιπτώσεις δεν γίνεται χρήση του μηχανισμού καθώς οι

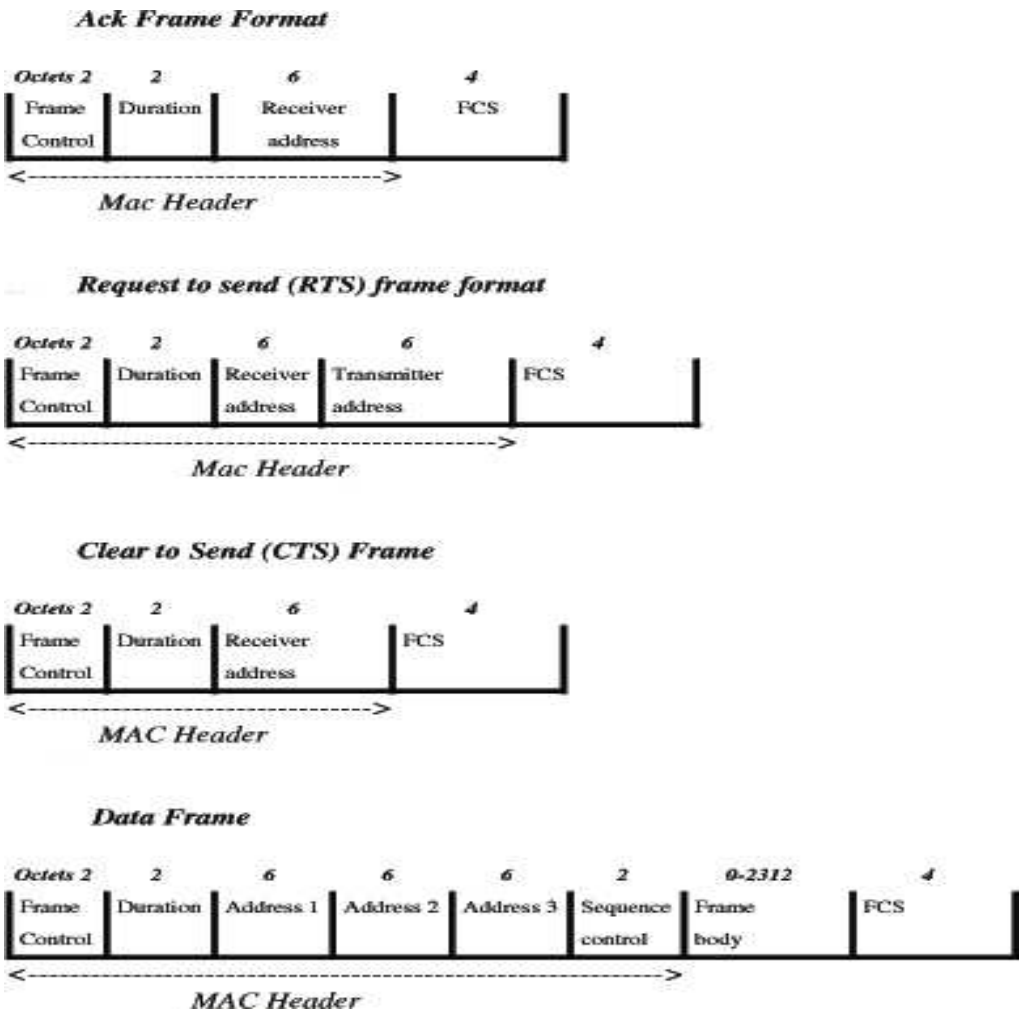
συγκρούσεις μεταξύ των πολλών μηνυμάτων CTS θα ήταν αναπόφευκτες. Μια άλλη περίπτωση κατά την οποία δεν χρησιμοποιείται ο μηχανισμός είναι η περίπτωση αποστολής πλαισίων μικρών σε μέγεθος, όπου δεν υπάρχει λόγος να αποσταλούν RTS/CTS μηνύματα. Το πρότυπο επιτρέπει σε μικρά πλαίσια να αποστέλλονται χωρίς τον μηχανισμό RTS/CTS ενώ μπορεί να χρησιμοποιείται για μεγαλύτερα. Ωστόσο, κάθε σταθμός που δεν χρησιμοποιεί τον μηχανισμό, υποχρεώνεται να ενημερώνει τον NAV όποτε λαμβάνει πλαίσια RTS-CTS και επίσης υποχρεώνεται να απαντά με ένα πλαίσιο CTS σε κάθε RTS. [12]

4.2.1.11 Άλλες λύσεις για το πρόβλημα του κρυφού σταθμού

Εκτός από τον μηχανισμό RTS/CTS υπάρχουν και άλλες λύσεις για το πρόβλημα του κρυφού σταθμού όπως οι ακόλουθες [17]:

1. Αύξηση ισχύς μετάδοσης δεδομένων από τους σταθμούς

Με την αύξηση της ισχύος (σε mWatts) μπορούμε να λύσουμε το πρόβλημα του κρυφού σταθμού, επιτρέποντας στην περιοχή γύρω από αυτόν να αυξηθεί σε μέγεθος, περιλαμβάνοντας όλους τους άλλους σταθμούς. Αυτή η υλοποίηση επιτρέπει στους σταθμούς που δεν είναι κρυφοί να ανιχνεύουν τους κρυφούς και εφόσον επιτευχθεί αυτό παύουν να υπάρχουν κρυφοί σταθμοί.



Σχήμα 4.10: Η μορφή των πλαισίων ACK, RTS, CTS και DATA

2. Χρήση πολυκατευθυντικών κεραιών

Καθώς οι σταθμοί που χρησιμοποιούν κατευθυντικές κεραίες είναι ορατοί μόνο στους κόμβους που είναι τοποθετημένοι στην κατεύθυνση τους σήματος της κεραίας, οι κατευθυντικές κεραίες θα πρέπει να χρησιμοποιούνται μόνο για πολύ μικρά δίκτυα.

3. Μετακίνηση του σταθμού και απομάκρυνση εμποδίων

Το πρόβλημα του κρυφού σταθμού επιλύεται με τη μετακίνησή του ώστε

κάθε σταθμός στο δίκτυο να μπορεί να ακούσει τους υπόλοιπους. Η μετακίνηση των χρηστών επεκτείνει το ασύρματο LAN ώστε να είναι δυνατή η κατάλληλη κάλυψη στην περιοχή, ενώ είναι πιθανή η προσθήκη επιπρόσθετων σημείων πρόσβασης.

4. Χρήση του WiCCP

Το WiCCP είναι μια βελτίωση της μεθόδου DCF σε δίκτυα του προτύπου 802.11b, που παρέχει πρόσβαση στο μέσο με κυκλική παράδοση σκυτάλης και καθορισμένη δέσμευση των διαθέσιμων πόρων του δικτύου, εξαλείφοντας το πρόβλημα του κρυφού σταθμού. Είναι μια μέθοδος που ελέγχει αποτελεσματικά την κυκλοφορία του δικτύου, με αποτέλεσμα την υψηλή αποδοτικότητά του.

4.2.1.12 Λειτουργία Protection Mode για μικτά δίκτυα 802.11b/g

Παρά το γεγονός ότι ο RTS/CTS μηχανισμός κατασκευάστηκε προκειμένου να λυθεί το πρόβλημα του κρυφού σταθμού, ενδέχεται, συσκευές του προτύπου 802.11g να αλλάζουν αυτόματα κατάσταση λειτουργίας και να χρησιμοποιούν τον μηχανισμό, όταν μια άλλη, χαμηλής ταχύτητας συσκευή του προτύπου 802.11b εντάσσεται στο ίδιο τοπικό δίκτυο. Για το πρότυπο 802.11g αυτή η λειτουργία είναι γνωστή ως *λειτουργία Protection Mode*.

Βέβαια προκύπτουν προβλήματα από την συνύπαρξη στο ίδιο δίκτυο, συσκευών που βασίζονται σε διαφορετικά πρότυπα, αφού το πρότυπο 802.11b δεν μπορεί να αναγνωρίσει ως “νόμιμους” χρήστες, τους χρήστες των σταθμών που βασίζονται στο 802.11g, αλλά οι αποστολές τους εκλαμβάνονται από το πρότυπο ως θόρυβος. Επίσης για τον ίδιο λόγο, συσκευές που βασίζονται στο 802.11b μεταφέρουν δεδομένα αγνοώντας την ύπαρξη αποστολών από σταθμούς που λειτουργούν με το 802.11g. Λόγω αυτών των παραμέτρων η διεκπεραιωτική ικανότητα ενός δικτύου 802.11b/g μπορεί να αγγίζει μόλις τα 15Mbps.

Κατά την προστατευόμενη λειτουργία λοιπόν, αν θέλουμε να αποφύγουμε τις παραπάνω δυσκολίες θα πρέπει [1]:

- πριν από την μετάδοση οποιουδήποτε πλαισίου, οι σταθμοί που

λειτουργούν με βάση το 802.11g να στέλνουν RTS/CTS μηνύματα χρησιμοποιώντας ραδιοσυχνότητες του 802.11b στο 1Mbps

- όλα τα προθέματα καθώς και τα πλαίσια ελέγχου να στέλνονται και αυτά στο 1Mbps
- όλοι οι χρονιστές του δικτύου καθώς και οι μετρητές οπισθοχώρησης να χρησιμοποιούν τα μεγαλύτερα χρονικά διαστήματα που προσφέρει το πρότυπο 802.11b

4.2.1.13 Χρήση μόνο CTS μηνυμάτων (CTS only Method)

Πρόκειται για μια μέθοδο η οποία αφορά επίσης τα μικτά δίκτυα 802.11b/g και σχεδιάστηκε με βάση το γεγονός ότι ενώ οι σταθμοί το δικτύου μπορούν να “ακούν” το σημείο πρόσβασης, δεν υπάρχει λόγος αυτό να μεταδίδει σε όλους ένα RTS μήνυμα όταν θέλει να μεταδώσει, περιμένοντας για ένα CTS από κάθε σταθμό. Έτσι όποτε το σημείο πρόσβασης θέλει να ξεκινήσει μια μετάδοση, μπορεί να το κάνει στέλνοντας μόνο ένα CTS μήνυμα.

4.2.1.14 Μέθοδος Σημειακού Συντονισμού (PCF)

Πρόκειται για μια μέθοδο πρόσβασης η οποία δεν είναι “ανταγωνιστική”, αφού εγγυάται ότι μόνο ένας σταθμός μπορεί να εκπέμπει στο κανάλι σε κάποια χρονική περίοδο, ώστε να μη συμβαίνουν συγκρούσεις. Όταν εφαρμόζεται, μπορεί να συνυπάρχει με την μέθοδο DCF και ο χρόνος πρόσβασης στο κοινό μέσο χωρίζεται σε χρονοθυρίδες [14]. Δημιουργήθηκε για να υποστηρίξει μεταδόσεις πραγματικού χρόνου που απαιτούσαν υψηλούς ρυθμούς μετάδοσης όπως το video και η φωνή, σε αντίθεση με τη μέθοδο DCF που είναι αποδοτικότερη σε μεταδόσεις δεδομένων που δεν έχουν χρονικές απαιτήσεις (π.χ. email, ftp). [15]

Η βασική ιδέα της μεθόδου είναι η περιοδική απόκτηση του ελέγχου του δικτύου από το σημείο πρόσβασης και η εφαρμογή της μεθόδου polling από αυτό. Τα χρονικά διαστήματα κατά τα οποία ο έλεγχος της κίνησης αναλαμβάνεται από

το σημείο πρόσβασης καλούνται διαστήματα χωρίς ανταγωνισμό (Contention Free – CF). Κατά τη διάρκεια αυτών των διαστημάτων το σημείο πρόσβασης κάνει polling μεταξύ των σταθμών που είναι “ευαίσθητοι” στην κίνηση, δηλαδή σταθμοί οι οποίοι πρέπει να μεταδώσουν δεδομένα χωρίς καθυστερήσεις. Το χρονικό διάστημα που δεσμεύεται για τις CF περιόδους είναι μεταβλητό και το μέγεθός του αποφασίζεται από το σημείο πρόσβασης ενώ εξαρτάται από το πλήθος των σταθμών που ζητούν CF περιόδους, από τις απαιτήσεις μετάδοσης, και από τους ρυθμούς μετάδοσης των δεδομένων.

4.2.1.15 Τρόπος λειτουργίας της μεθόδου PCF

Αρχικά το σημείο πρόσβασης κάνει broadcast ένα μήνυμα ελέγχου έπειτα από χρονικό διάστημα ίσο με ένα PIFS, υποχρεώνοντας τους σταθμούς να αρχικοποιήσουν τους NAV μετρητές τους, ώστε να μην αποστέλλουν δεδομένα για εκείνη την περίοδο (όπως και στην λειτουργία RTS/CTS). Κατά τη διάρκεια της CF περιόδου, το σημείο πρόσβασης κάνει polling στους σταθμούς του δικτύου, ενώ εκείνοι μπορούν να εκπέμπουν μόνο μηνύματα/απαντήσεις στα αιτήματά του.

Το σημείο πρόσβασης περιλαμβάνει έναν μηχανισμό που ονομάζεται σημειακός συντονιστής (polling coordinator - PC) που του δίνει τη δυνατότητα να λειτουργεί σαν master ενώ οι σταθμοί σαν slaves. Ο PC αποφασίζει κάθε φορά ποιος σταθμός θα ερωτηθεί για να στείλει δεδομένα. Χωρίς την ύπαρξη απροσδιόριστης καθυστέρησης που δημιουργούν οι συγκρούσεις στην DCF, η PCF παρέχει συγκεκριμένη καθυστέρηση που είναι ιδανική για δεδομένα που προέρχονται από εφαρμογές όπως ο ήχος και το video. Παρόλο που η μέθοδος χρησιμοποιείται από το σημείο πρόσβασης, κάθε σταθμός έχει τη δυνατότητα να αποφασίσει εάν θέλει να «ερωτάται» από αυτό ή όχι. Κάθε σταθμός που ενσωματώνεται σε ένα δίκτυο λαμβάνει ένα μήνυμα ελέγχου (αυτό επιτυγχάνεται θέτοντας στο υποπεδίου CP_Pollable του πλαισίου Association Request την τιμή TRUE) σχετικά με το εάν θέλει να περιλαμβάνεται στη λίστα που δημιουργεί το σημείο πρόσβασης με τους σταθμούς στους οποίους θα στέλνει μηνύματα polling. Ένας σταθμός μπορεί να αρνηθεί, να συμφωνήσει, αρχικά να αρνηθεί και έπειτα να συμφωνήσει εφόσον βρίσκεται ακόμη στο δίκτυο, ή να δεχθεί για ένα διάστημα

και έπειτα να αρνηθεί την αποδοχή polling μηνυμάτων. [15]

Στην περίπτωση που η DCF και η PCF συνυπάρχουν, οι σχισμές χωρίζονται σε περιόδους χωρίς ανταγωνισμό όταν χρησιμοποιείται η μέθοδος PCF (Contention Free Period) και περιόδους με ανταγωνισμό όταν χρησιμοποιείται η μέθοδος DCF (Contention Period) [15]. Αυτά τα διαστήματα ονομάζονται χρονοθυρίδες ή superframes. [13]

Στο τέλος της CF περιόδου το δίκτυο τίθεται αυτομάτως και πάλι σε κατάσταση “ανταγωνισμού”. Ο αντίκτυπος που μπορεί να έχει η χρήση της μεθόδου στη ρυθμοαπόδοση των δικτύων είναι μεγάλος και ο λόγος έγκειται στη χρήση των NAV μηνυμάτων, τα οποία θέτουν κατά τη διάρκεια χρήσης τους ολόκληρο το δίκτυο σε κατάσταση αναμονής.

4.3 Επιπρόσθετα χαρακτηριστικά του πρωτοκόλλου

Υπάρχουν επιπρόσθετα χαρακτηριστικά τα οποία σχεδιάστηκαν ώστε να αυξήσουν την αποτελεσματικότητα του πρωτοκόλλου και να μειώσουν την κατανάλωση ενέργειας. Κάποια χαρακτηριστικά δεν συμπεριλαμβάνονταν στο 802.11 ενώ άλλα έχουν προστεθεί στις τελευταίες εκδόσεις του, όπως το 802.11e και 802.11n.

4.3.1 Λειτουργία streaming / burst

Πρόκειται για μια λειτουργία η οποία χρησιμοποιείται στα πρότυπα 802.11e και 802.11n και επιτρέπει σε ένα σταθμό να “κατεβάσει” μια σειρά πλαισίων δεσμεύοντας το κανάλι. Μέσω της λειτουργίας streaming, μια συσκευή μπορεί να έχει πρόσβαση σε ένα κανάλι μετά από την απαιτούμενη DIFS αναμονή (ή EIFS, σε περίπτωση που συνέβη κάποιο σφάλμα), αλλά θα στείλει πλαίσια έπειτα από διάστημα ίσο με ένα SIFS. Εφόσον το SIFS είναι μικρότερο από κάθε άλλο χρονικό

διάστημα, κανείς άλλος σταθμός δεν θα μπορεί να χρησιμοποιήσει το κανάλι μέχρις ότου να σταλούν όλα τα πακέτα από την προσωρινή μνήμη του σταθμού που χρησιμοποιεί αυτή τη μέθοδο. [1]

4.3.2 Μη αποστολή μηνυμάτων επιβεβαίωσης (No Acknoledgement)

Εφόσον ο μηχανισμός των επιβεβαιώσεων είναι ο μόνος που εγγυάται στον αποστολέα την παράδοση των δεδομένων του, είναι πολύ σημαντική η ύπαρξή του. Σε περίπτωση που δεν ληφθεί κανένα μήνυμα επιβεβαίωσης λήψης, ο αποστολέας θεωρεί αποτυχημένη την αποστολή του, ενεργοποιεί τον μετρητή οπισθοχώρησης και επιχειρεί επαναποστολή όταν ο μετρητής εκλείψει. [1]

4.3.3 Λειτουργία κατάτμησης

Γενικά η κατάτμηση είναι η διαδικασία κατά την οποία τα προς αποστολή πλαίσια τεμαχίζονται από τον αποστολέα σε άλλα, μικρότερου μήκους προκειμένου να μεταδοθούν. Τα περισσότερα πρωτόκολλα για τοπικά δίκτυα χρησιμοποιούν χιλιάδες bytes για κάθε πακέτο, όμως στα ασύρματα δίκτυα είναι απαραίτητη η χρήση μικρών πακέτων για συγκεκριμένους λόγους [11]:

- Εξαιτίας του υψηλού ρυθμού εμφάνισης λαθών σε συνδέσεις μέσω ραδιοσυχνοτήτων, η πιθανότητα καταστροφής ενός πακέτου είναι μεγάλη.
- Αν καταστραφεί ένα πακέτο, είτε λόγω σύγκρουσης είτε λόγω θορύβου, όσο μικρότερο είναι, τόσο λιγότερο επιβαρύνεται το μέσο μετάδοσης σε περίπτωση επαναποστολής του.
- Σε ένα σύστημα που βασίζεται στη μέθοδο FHSS, κάθε 20 msec το μέσο αλλάζει κανάλι μετάδοσης, επομένως όσο μικρότερο είναι το πακέτο, τόσο μικρότερη είναι και η πιθανότητα να ακυρωθεί η μετάδοση μετά από αυτό το χρονικό διάστημα.

  Από την άλλη πλευρά, πρακτικά δεν έχει νόημα η δημιουργία ενός

πρωτοκόλλου για τοπικά δίκτυα το οποίο δεν θα μπορεί να χειριστεί πακέτα των 1518Bytes που χρησιμοποιεί το Ethernet. Τη λύση σε αυτό το πρόβλημα δίνουν οι μηχανισμοί κατάτμησης και επανασυναρμολόγησης που ενσωματώθηκαν στο επίπεδο MAC.

Η λειτουργία του μηχανισμού είναι αρκετά απλή. Κάθε πλαίσιο (MSDU – Mac Service Data Unit) υποδιαιρείται σε μικρότερα τμήματα που καλούνται MPDU (Mac Protocol Data Unit). Όταν πρέπει να μεταδοθεί ένα πλαίσιο που έχει κατατμηθεί, ο αποστολέας αναμένει διάστημα ίσο με ένα DIFS πριν να αρχίσει τη μετάδοση. Αφού σταλεί το πρώτο τμήμα του κατακερματισμένου πλαισίου, θα αναμένει για διάστημα ίσο με ένα SIFS μετά από κάθε ACK για να στείλει κάθε επόμενο κομμάτι του αρχικού πλαισίου. Προκειμένου κάποιος άλλος σταθμός να αρχίσει να μεταδίδει, θα πρέπει ο σταθμός ο οποίος αποστέλλει τμήματα ενός πλαισίου που έχει κατατμηθεί, να ολοκληρώσει τη μετάδοσή του αποστέλλοντας και το τελευταίο τμήμα του αρχικού πλαισίου.

Σε περίπτωση που συμβεί κάποιο σφάλμα, μόνο το λάθος πλαίσιο θα ξανασταλθεί. Η λειτουργία της κατάτμησης απαιτεί από τους χρήστες τον ορισμό ενός ανώτατου ορίου στο μέγεθος των πλαισίων, ώστε τα πλαίσια που είναι μεγαλύτερα αυτού να κατατέμνονται.

4.4 Εξοικονόμηση ενέργειας

Ένα από τα προβλήματα που εντοπίζονται στα WLANs είναι η κατανάλωση ενέργειας. Τα σημεία πρόσβασης τροφοδοτούνται με ρεύμα μέσω πρίζας ή μέσω Ethernet καλωδίου, ενώ οι σταθμοί τροφοδοτούνται με μπαταρίες, η διάρκεια ζωής των οποίων παίζει σημαντικό ρόλο στα WLANs. Επίσης, ποσά ενέργειας καταναλώνουν οι χρήστες τους δικτύου, δηλαδή οι αποστολείς και οι παραλήπτες, με πρώτους σε κατανάλωση ενέργειας τους αποστολείς.

Δυο είναι οι μηχανισμοί που χρησιμοποιούνται για εξοικονόμηση ενέργειας στα WLANs και επιμήκυνση της ζωής των μπαταριών, ο μηχανισμός Power Save

Mode και ο μηχανισμός Automatic Power Save Delivery. Παρά αυτούς τους δυο μηχανισμούς, οι κατασκευαστές προσπαθούν συνεχώς να χρησιμοποιούν νέα καινοτόμα χαρακτηριστικά και τεχνολογίες μπαταριών που θα οδηγούν σε ακόμη μεγαλύτερη εξοικονόμηση ενέργειας. [1]

4.4.1 Power Save Mode

Το πρότυπο 802.11 περιλάμβανε πολύ βασικές τεχνικές ώστε να εξοικονομείται ενέργεια από τρόπους που ήταν προσανατολισμένοι στα δεδομένα. Ο αποστολέας μπορεί να ενημερώσει το σημείο πρόσβασης ότι θα αλλάξει την κατάστασή του σε sleep mode, τροποποιώντας την τιμή του bit του πεδίου “power save” του πλαισίου ελέγχου. Το σημείο πρόσβασης παρατηρεί τους σταθμούς που είναι ανενεργοί και αποθηκεύει σε προσωρινές μνήμες τα πακέτα που προορίζονται για αυτούς. Οι σταθμοί πρέπει να επανέρχονται από αυτή την κατάσταση κάθε 100msec, ώστε να λάβουν τα μηνύματα beacon[22], τα οποία μπορεί να ακολουθούνται από μηνύματα ATIM (Announcement Traffic Indication MAP). Σκοπός αυτών των μηνυμάτων είναι να διαπιστώσουν οι σταθμοί αν το σημείο πρόσβασης φυλάσσει δεδομένα για αυτούς.

Οι σταθμοί για τους οποίους υπάρχουν δεδομένα στις προσωρινές μνήμες παραμένουν ενεργοί και στέλνουν ένα μήνυμα στο σημείο πρόσβασης ώστε να ανακτήσουν κάθε πλαίσιο. Αφού τελειώσει η μεταφορά των πλαισίων από το σημείο πρόσβασης προς τον σταθμό, ο σταθμός αλλάζει και πάλι κατάσταση (sleep mode). Επίσης, από το μήνυμα beacon μπορούμε να εκμεταλλευτούμε την ύπαρξη του beacon μετρητή έτσι ώστε οι σταθμοί να γνωρίζουν πότε πρέπει να ενεργοποιηθούν ξανά και να ελέγξουν την εισερχόμενη κίνηση.

Ωστόσο μειονέκτημα της μεθόδου αποτελεί το γεγονός αφύπνισης των σταθμών κάθε 100 msec ώστε να “ακούν” τα μηνύματα beacon και να στέλνουν άλλα μηνύματα. Με αυτή τη διαδικασία καταναλώνουν ενέργεια από την μπαταρία τους. Αυτό το πρόβλημα λύνει η επόμενη μέθοδος εξοικονόμησης ενέργειας. [1]

22 Τα beacons είναι μηνύματα που μεταφέρουν τα σημεία πρόσβασης σε BSS ή ESS δίκτυα προκειμένου να δείξουν τη διαθεσιμότητά τους και άλλες χρήσιμες πληροφορίες προς τους σταθμούς. [1]

4.4.2 Automatic Power Save Delivery (APSD)

Πρόκειται για ένα χαρακτηριστικό που συμπεριλαμβάνεται στο πρότυπο 802.11e. Σύμφωνα με αυτό, οι σταθμοί γίνονται και πάλι ενεργοί βάσει ενός δικού τους προγράμματος αφύπνισης, ώστε να στείλουν ένα πλαίσιο (trigger frame) στο σημείο πρόσβασης ζητώντας να μεταφερθούν όλα τα αποθηκευμένα σε εκείνο πλαίσια που προορίζονταν για τον εκάστοτε σταθμό. Το σημείο πρόσβασης εκτελεί την μεταφορά των δεδομένων και μέσω ενός bit που χρησιμοποιεί για να σηματοδοτήσει το τελευταίο πλαίσιο που μεταφέρθηκε, δίνει τη δυνατότητα στον σταθμό να επιστρέψει σε κατάσταση sleep. [1]

Επίλογος

Σε αυτό το κεφάλαιο περιγράψαμε τις λειτουργίες που επιτελούνται στο επίπεδο MAC του 802.11 και αναλύσαμε τις μεθόδους πρόσβασης στο κανάλι μετάδοσης καθώς και θέματα που σχετίζονται με την εξοικονόμηση ενέργειας στα WLANs. Το κεφάλαιο που ακολουθεί θα εστιάσει σε θέματα σχετικά με την ασφάλεια των WLANs και θα αναλυθούν τα πρωτόκολλα του 802.11 μέσω των οποίων επιτυγχάνεται αυτή.

Κεφάλαιο 5

Θέματα ασφάλειας στα WLANs

5.1 Εισαγωγή

Το κεφάλαιο αυτό εστιάζει σε θέματα ασφάλειας των ασύρματων τοπικών δικτύων. Αναλύονται οι ευπάθειες και τα κενά ασφαλειάς τους ενώ περιγράφεται διεξοδικά το πρωτόκολλο WEP και το πρότυπο 802.11i. Δίνεται βαρύτητα στους αλγορίθμους κρυπτογράφησης που χρησιμοποιούν τα πρότυπα WEP, WPA και WPA2 και επίσης γίνεται μια συνοπτική περιγραφή του πρωτοκόλλου αυθεντικοποίησης 802.1x.

5.2 Απαιτήσεις ασφάλειας: αυθεντικοποίηση, ιδιωτικότητα, μη απάρνηση, διαθεσιμότητα

Η ασφάλεια αποτελεί τον πρώτο λόγο για τον οποίο πολλοί αποφεύγουν τη χρήση ασύρματων τοπικών δικτύων. Ωστόσο με τον όρο “ασφάλεια” στα δίκτυα, αναφερόμαστε σε τέσσερις θεμελιώδεις διαδικασίες:

- ***Αυθεντικοποίηση***: η διαδικασία κατά την οποία η πρόσβαση σε ένα δίκτυο επιτρέπεται μόνο στους νόμιμους χρήστες του.
- ***Ιδιωτικότητα***: η διαδικασία κατά την οποία βεβαιωνόμαστε πως κάθε

πληροφορία κυκλοφορεί στο δίκτυο, μπορεί να ανταλλάσεται μόνο μεταξύ νόμιμων αποστολέων και παραληπτών.

- ***Μη απάρνηση***: η σιγουριά ότι οποιοδήποτε μήνυμα παραλαμβάνουμε, αποστάλθηκε από την αναμενόμενη πηγή, χωρίς να έχει υποστεί καμία τροποποίηση.
- ***Διαθεσιμότητα***: παρέχει προστασία από επιθέσεις τύπου *denial of service*, ιούς, σκουλίκια και γενικά οτιδήποτε θα μπορούσε να θέσει το δίκτυο εκτός χρήσης ή να διαταράξει την κανονική λειτουργία του.

Επίσης τα δίκτυα μπορούν να θέτουν διαφορετικά επίπεδα ασφάλειας ανάλογα με τους χρήστες που τα χρησιμοποιούν. Έτσι, θα μπορούσαμε να θέσουμε κανόνες και να υποθέσουμε π.χ. ότι για τους χρήστες εντός του δικτύου θα λαμβάνουμε επιπλέον προστασία για την πρόσβαση στο διαδίκτυο, ενώ δεν θα λαμβάνουμε ανάλογα μέτρα για τους επισκέπτες του δικτύου.

5.3 Κενά ασφάλειας στα WLANs

Στην πραγματικότητα δεν είναι μόνο τα WLANs που αντιμετωπίζουν προβλήματα ασφάλειας, αλλά γενικότερα κάθε σύστημα που είναι σενδεδεμένο με ένα δίκτυο. Στα ενσύρματα δίκτυα, φροντίζουμε η προστασία να είναι κυρίως φυσική και από τους χρήστες απαιτείται η τήρηση της πολιτικής που έχει θεσπιστεί, καθόλη τη διάρκεια της ύπαρξής τους μέσα στο δίκτυο.

Προκειμένου να αποτρέψουμε την μη εξουσιοδοτημένη πρόσβαση στο διαδίκτυο, εγκαθιστούμε firewalls και αυτά ανιχενύουν/φιλτράρουν την εισερχόμενη και την εξερχόμενη κίνηση σύμφωνα με τους κανόνες που έχουμε αποφασίσει εμείς. Επίσης η χρήση συστημάτων ανίχνευσης εισβολέων και proxies μπορούν να μας προστατέψουν. Καθώς οι επιθέσεις αυξάνονται, το λογισμικό που σχετίζεται με την ασφάλεια πρέπει να ανανεώνεται συνεχώς.

Επειδή στα WLANs οι μεταδόσεις γίνονται μέσω ραδιοσυχνοτήτων, θα αναφέρουμε κάποιες γενικότερες ευπάθειες που σχετίζονται με αυτές [1]:

- *Διάχυση εκπεμπόμενου σήματος:* συνήθως τα WLANs παρέχουν πολύ καλή κάλυψη σε μικρές περιοχές όπως ένα κτίριο και η περιοχή γύρω του.

Κάποιοι οργανισμοί προσπάθησαν να περιορίσουν την εκπομπή του σήματος σε μια συγκεκριμένη περιοχή χρησιμοποιώντας κατευθυντικές κεραίες και προσαρμόζοντας την εκπεμπόμενη ενέργεια των σημείων πρόσβασης. Ωστόσο, έχει αποδειχθεί ότι τα μέτρα που λαμβάνονται για να προστατέψουμε τα ραδιοσήματα δεν είναι απολύτως επαρκή.

- *Απουσία κρυπτογράφησης για τις κεφαλίδες και τα μηνύματα ελέγχου:* παρόλο που το περιεχόμενο ενός WLAN πλαισίου μπορεί να κρυπτογραφηθεί, τα πεδία της κεφαλίδας στέλνονται χωρίς κρυπτογράφηση. Το γεγονός αυτό δίνει στους hackers το έναυσμα να καταστρώνουν επιθέσεις που βασίζονται στο spoofing[23] της MAC κεφαλίδας. Επίσης τα μηνύματα διαχείρισης στέλνονται και αυτά χωρίς κρυπτογράφηση. Μέχρι πρόσφατα οι χρήστες πίστευαν ότι μπορούσαν να κρατήσουν κρυφά τα δίκτυα τους από το ευρύ κοινό, ρυθμίζοντας τα σημεία πρόσβασης να παραλείπουν το SSID από τα μηνύματα beacon. Δυστυχώς, κάθε συσκευή η οποία ενσωματώνεται στο δίκτυο κρατάει το SSID σε ένα μη κρυπτογραφημένο μήνυμα ελέγχου, γεγονός που διευκολύνει έναν hacker να αποφασίσει το όνομα του δικτύου παρακολουθώντας μια απλή διαδικασία association και όσα μηνύματα ανταλλάσσονται σε αυτή.
- *Άρνηση υπηρεσίας:* τα πρωτόκολλα ασύρματων τοπικών δικτύων προσθέτουν νέες επιλογές για τις επιθέσεις τύπου *denial of service (DoS),* η πιο συνηθισμένη από αυτές είναι η επίθεση διακοπής της συσχέτισης ενός σταθμού με το δίκτυο (*disassociation attack)*. Σε αυτή, ο επιτιθέμενος παρακολουθεί τη διαδικασία συσχετισμού (association) ενός σταθμού με το δίκτυο και στέλνει ένα μήνυμα disassociation για να αποσυνδέσει τον σταθμό. Ακολουθεί πλήθος από CTS[24] μηνύματα που κατακλείζουν τους σταθμούς, με αποτέλεσμα αυτοί να νομίζουν πως το δίκτυο είναι μονίμως

23 Επίθεση κατά την οποία ένα άτομο ή πρόγραμμα μεταμφιέζεται και παρουσιάζεται σαν κάτι άλλο, ενώ στοχεύει στην αλλοίωση των δεδομένων.

24 Clear to Send, τύπος μηνύματος που χρησιμοποιείται για έλεγχο της κυκλοφορίας ενός δικτύου. Αποστέλλεται από ένα σημείο πρόσβασης σε έναν σταθμό και εκφράζει τη διαθεσιμότητα του σημείου να δέχεται μηνύματα.

απασχολημένο. Επίσης, σαν επίθεση τύπου DoS μπορούν να θεωρηθούν και οι παρεμβολές *(jamming)*.

- *Μολυσμένοι σταθμοί:* Εάν κάποια συσκευή ενός χρήστη δεν διαθέτει firewall ή κάποιο λογισμικό προστασίας, μπορεί να "κολλήσει" οποιοδήποτε σκουλίκι ή ιό συνδεόμενη με ένα δίκτυο ελεύθερο στο κοινό (public hot spot). Έπειτα η μολυσμένη συσκευή μπορεί να μολύνει και άλλα δίκτυα με τα οποία θα συνδέεται κάθε φορά.

5.4 Ανάλυση ευπαθειών στα WLANs

Υπάρχουν διάφοροι τύποι έκθεσης ασφάλειας στα WLANs [1]:

- *Το να παρακολουθεί/"κρυφακούει" (eavesdropping) κανείς τις μη κρυπτογραφημένες μεταδώσεις στα ασύρματα δίκτυα ή το να σπάσει το κλειδί κρυπτογράφησης ώστε να τις παρακολουθεί:* είναι η πιο διαδεδομένη πρακτική που χρησιμοποιείται από τους hackers, αλλά σήμερα μπορεί να αποφευχθεί εξαιτίας των διαφόρων επιλογών κρυπτογράφησης, όπως εκείνες που περιγράφονται στα πρωτόκολλα 802.11i/WPA2.
- *Το να παρακολουθεί κανείς ή να αποκτήσει πρόσβαση στο δίκτυο μέσω των σημείων πρόσβασης που ο χρήστης τοποθέτησε εξαιτίας της άγνοιάς του ενώ επρόκειτω για συσκευές που προορίζονταν για απάτη:* πρόκειται περισσότερο για πρόβλημα διαχείρησης, αλλά απαιτείται ο συνεχής έλεγχος των ραδιοσυχνοτήτων ώστε να εξασφαλιστεί η νόμιμη χρήση τους.
- *Η εγκατάσταση κακόβουλων σημείων πρόσβασης που επιτρέπουν την παρεμβολή τρίτων όταν ένας σταθμός ανταλλάσσει δεδομένα κατά την διαδικασία της συσχέτισής του με το δίκτυο:* Ένα κακόβουλο σημείο πρόσβασης (πρόκειται για λογισμικό που εγκαθίσταται σε ένα laptop που του επιτρέπει να δρα σαν να επρόκειτω για σημείο πρόσβασης) είναι ένα σημείο πρόσβασης που χρησιμοποιείται από έναν hacker και η ιδέα είναι να συσχετισθούν οι νόμιμες συσκευές του δικτύου ώστε να συνδεθούν με το κακόβουλο σημείο πρόσβασης και τελικά να παρέχουν στον hacker μη εξουσιοδοτημένη πρόσβαση στο δίκτυο. Αυτός ο τύπος επίθεσης καλείται

man-in-the-middle-attack ή *evil twin attack* και στοχεύει στην εξαπάτηση των χρηστών ώστε χωρίς τη θέλησή τους να γίνουν πληροφοριοδότες ονομάτων και κωδικών πρόσβασης. Τέτοιου είδους επιθέσεις μπορούν να αποφευχθούν μέσω ενός συστήματος που το δίκτυο θα απαιτεί την ταυτοποίηση του χρήστη, ενώ από την πλευρά του χρήστη το δίκτυο θα ταυτοποιείται σε αυτόν.

- *Επισκέπτες που θέτουν εκτός λειτουργίας τους μηχανισμούς ασφαλείας στα σημεία πρόσβασης:* τα σημεία πρόσβασης θα πρέπει να εγκαθίστανται σε περιοχές που δεν είναι εύκολα προσβάσιμες, δεδομένου ότι η φυσική πρόσβαση μπορεί να επιτρέψει σε κάποιον να θέσει εκτός λειτουργίας τα μέτρα ασφαλείας που έχουν ληφθεί. Η απλούστερη μέθοδος για να γίνει κάτι τέτοιο είναι να πιεστεί το κουμπί reset ώστε να ανακτηθούν οι εργοστασιακές ρυθμίσεις του σημείου πρόσβασης.
- *Η κλοπή σημείων πρόσβασης, κλειδιών κρυπτογράφησης και λιστών με MAC διευθύνσεις που έχουν αποθηκευτεί σε αυτά.*
- *Πρόσβαση μέσω χαμένων/κλεμμένων συσκευών χρηστών:* οι χρήστες πολλές φορές αποτελούν το αδύνατο σημείο σε ένα σύστημα ασφαλείας, γι' αυτό θα πρέπει να ενημερώνονται σχετικά με τους κινδύνους που αναδύονται όταν μια συσκευή φτάνει στα χέρια ενός hacker.
- *Διακοπή εκπομπής ραδιοσυχνοτήτων:* πολλές φορές οι επιθέσεις DoS στοχεύουν σκόπιμα στις ραδιοσυχνότητες, ή άθελά τους επεμβαίνουν σε μπάντες που η χρήση τους δεν απαιτεί άδεια.

5.5 Οι τρεις γενιές ασφάλειας των WLANs

Σήμερα, οι διαθέσιμοι μηχανισμοί ασφάλειας για τα WLANs είναι πολύ αποτελεσματικοί, παρά το γεγονός ότι η ασφάλεια στα ασύρματα δίκτυα είναι ένα θέμα παρεξηγημένο. Ωστόσο πρέπει να έχουμε υπόψη μας ότι η ασφάλεια ενός ασύρματου δικτύου είναι, σε μεγάλο ποσοστό, ευθύνη του κάθε χρήστη ο οποίος πρέπει να κατανοεί τις ευπάθειες και να λαμβάνει τα κατάλληλα μέτρα. Συνήθως όμως η εγκαθίδρυση του βέλτιστου τρόπου προστασίας ενός δικτύου απαιτεί

αναβαθμίσεις στο υλικό που στοιχίζουν σε χρήματα, καθώς και προσωρινή διακοπή άλλων λειτουργιών για την ολοκλήρωση της εγκατάστασής τους. Επίσης, είναι πιθανή η ύπαρξη περιοριστικών παραγόντων σχετικά με τα μέτρα ασφάλειας που θα χρησιμοποιήσουμε, όπως θέματα συμβατότητας με παλαιότερες συσκευές που δεν μπορούν να αναβαθμιστούν ώστε να υποστηρίζουν νέες μεθόδους προστασίας. Μπορούμε να εξετάσουμε τις λύσεις σε θέματα ασφάλειας, χωρίζοντας τες σε τρεις γενιές (πίνακας 5.1):

- **Πρώιμο στάδιο προστασίας:** τα περιορισμένα και αδύναμα χαρακτηριστικά ασφάλειας του WEP απαιτούσαν την ανάπτυξη τρόπων προστασίας που έκαναν χρήση επιπρόσθετων μέτρων όπως η εγκατάσταση ενός VPN/VLAN.
- **Ανεπτυγμένη πρακτική προστασίας:** το WPA (WiFi Protected Access) είναι ένας ενδιάμεσος τρόπος προστασίας που ανέπτυξε η WiFi Alliance και παρέχει βελτιωμένες πρακτικές ασφάλειας σε σχέση με το WEP. Το βασικό του πλεονέκτημα είναι ότι μπορεί να υλοποιηθεί με αναβαθμίσεις στο λογισμικό και όχι στο υλικό. Για τη λειτουργία του χρησιμοποιείται ένα προμοιρασμένο κλειδί (pre-shared key) το οποίο είτε έχει τοποθετηθεί στη συσκευή από τον χρήστη, είτε μέσω 802.1x αυθεντικοποίησης που παρέχει διαμοιρασμό κλειδιών συνόδου (session-key) αλλά και ανανέωση κλειδιών.
- **Βέλτιστη πρακτική προστασίας:** Η IEEE έχει αναπτύξει μια πιο περιεκτική μέθοδο ασφάλειας που καλείται 802.11i. Η WiFi Alliance αναφέρεται στο 802.11i με την ονομασία WPA2. Αυτή η επιλογή χρησιμοποιεί κρυπτογράφηση που βασίζεται στον αλγόριθμο AES. Η χρήση όμως του 802.11i ενδέχεται να απαιτεί την απόσυρση των παλιών καρτών δικτύου καθώς και την αντικατάσταση των σημείων πρόσβασης με νέα. Όπως το WEP έτσι και το 802.11i μπορεί να υλοποιηθεί χρησιμοποιώντας ένα προμοιρασμένο κλειδί που έχει εισαχθεί στη συσκευή από τον χρήστη είτε μέσω 802.1x αυθεντικοποίησης

Πίνακας 5.1: Λύσεις ασφάλειας που παρέχονται από τα WLANs

	Περιγραφή	Κρυπτογράφηση	Αυθεντικοποίηση
Wired Equivalent Privacy (WEP)	WEP	40 ή 104 bit RC4	Προμοιρασμένο κλειδί
	Dynamic WEP	40 ή 104 bit RC4	802.1x με διαμοιρασμό των κλειδιών συνόδου
	VPN/VLAN	168 bit 3DES	802.1x
WiFi Protected Access (WPA)	Ενδιάμεση λύση από την WiFi Alliance	128 bit RC4 με TKIP	Personal: προμοιρασμένο κλειδί που καθορίστηκε από τον χρήστη
			Enterprise: 802.1x με διαμοιρασμό κλειδιού
802.11i/WPA2	Πρότυπο της IEEE	AES	Personal: προμοιρασμένο κλειδί που καθορίστηκε από τον χρήστη
			Enterprise: 802.1x με διαμοιρασμό κλειδιού

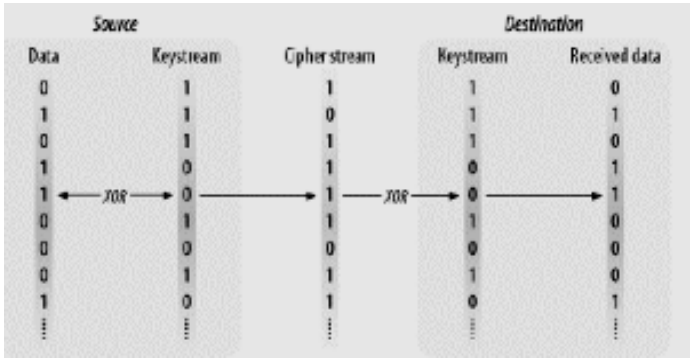
5.6 Wired Equivalent Privacy (WEP)

Το WEP πρωτοεμφανίστηκε το 1997 με σκοπό να προστατέψει τα ασύρματα δίκτυα σε βαθμό ανάλογο με τον βαθμό ασφάλειας των ενσύρματων δικτύων (είναι και ο λόγος του ονόματός του). Βασική του ιδέα ήταν η παροχή ασφάλειας από την κρυφή παρακολούθηση (eavesdropping) και όχι από τις επιθέσεις των hackers. Παρέχει τρία χαρακτηριστικά ασφάλειας: κρυπτογράφηση που βασίζεται στον RC4 με κλειδί των 40 ή των 104 bits (αν συμπεριλάβουμε και

το IV τότε το κλειδί είναι μήκους 68 ή 128 bits αντίστοιχα), αυθεντικοποίηση προμοιρασμένου κλειδιού που κρυπτογραφήθηκε βάσει του WEP και φιλτράρισμα MAC διευθύνσεων.

5.6.1 Το κρυπτογραφικό background του WEP

Προκειμένου το WEP να μπορέσει να προστατέψει αποτελεσματικά τα δεδομένα χρησιμοποιεί έναν αλγόριθμο *συμμετρικής ροής (stream cipher)* που ονομάζεται RC4. Γενικά οι ροές δεδομένων που παράγει ένας αλγόριθμος ονομάζονται *keystreams*, οι οποίες έπειτα συνδυαζόμενες με κάποιο μήνυμα *(plaintext)* παράγουν το κρυπτογράφημα *(cipheretext)*. Από την πλευρά του παραλήπτη, για να ανακτήσουμε και πάλι το αρχικό μήνυμα, αρκεί να εφαρμόσουμε τη συνάρτηση XOR που εφαρμόζει ο RC4 μεταξύ του κρυπτογραφημένου μηνύματος και του keystream που χρησιμοποιήθηκε. Η εικόνα 5.1 δείχνει ένα τέτοιο παράδειγμα.



Σχήμα 5.1: Λειτουργία ενός stream cipher αλγορίθμου

Οι περισσότεροι αλγόριθμοι που χρησιμοποιούν ακολουθίες για κρυπτογράφηση, ουσιαστικά επιμηκύνουν ένα μικρού μήκους κλειδί σε μια ψευδοτυχαία ακολουθία που έχει το ίδιο μέγεθος με το μήνυμα που μεταδίδεται. Μια γεννήτρια ψευδοτυχαίων αριθμών (Pseudoramdon Number Generator - PRNG) βασιζόμενη σε κάποιους κανόνες επιμηκύνει το κλειδί και παράγει μια νέα

ακολουθία, δηλαδή το keystream. Για να ανακτήσουμε τα αρχικά δεδομένα θα πρέπει και ο αποστολέας και ο παραλήπτης να χρησιμοποιούν το ίδιο μυστικό κλειδί και τον ίδιο αλγόριθμο επιμήκυνσης του κλειδιού.

Εξαιτίας του γεγονότος ότι η ασφάλεια του keystream εξαρτάται πλήρως από τον βαθμό τυχαιότητας του keystream, ο σχεδιασμός της μετατροπής ενός κλειδιού σε keystream είναι ένα θέμα πολύ σημαντικό. Όταν έγινε η επιλογή του RC4 από την ομάδα εργασίας του 802.11 φαινόταν πως αλγοριθμικά ήταν μια ασφαλής επιλογή. Από τη στιγμή της επιλογής του όμως ξεκίνησαν έρευνες που το αποτέλεσμα τους ήταν η εξεύρεση μιας αδυναμίας που μπορούσαν να εκμεταλλευτούν για να σπάσουν το WEP. Ουσιαστικά η αδυναμία ήταν ο τρόπος που ο RC4 παράγει το keystream, κάτι το οποίο εξηγείται στη συνέχεια.

5.6.2 Κρυπτογραφικές λειτουργίες του WEP

Κάθε πρωτόκολλο που αναπτύσσεται για να προστατέψει ένα δίκτυο, πρέπει να βοηθάει τον διαχειριστή του να πετυχαίνει τρεις βασικούς στόχους της ασφάλειας των επικοινωνιών:

- ***Εμπιστευτικότητα*:** όρος που χρησιμοποιείται για να δείξει ότι τα δεδομένα προστατεύονται από παρεμβολές μη εξουσιοδοτημένων ατόμων.
- ***Ακεραιότητα*:** δηλαδή ότι τα δεδομένα δεν έχουν υποστεί καμία τροποποίηση.
- ***Αυθεντικοποίηση*:** Οι χρήστες πρέπει να είναι σίγουροι πως η πηγή των δεδομένων είναι πράγματι αυτή που ισχυρίζεται πως είναι.

Το WEP διαθέτει μηχανισμούς που υποστηρίζουν τις παραπάνω απαιτήσεις. Έτσι, η κρυπτογράφηση των πλαισίων παρέχει εμπιστευτικότητα. Οι ICS (Integrity Check Sequense) ακολουθίες προστατεύουν τα δεδομένα κατά τη μεταφορά τους δίνοντας στους παραλήπτες την δυνατότητα να τα ελέγξουν για τυχόν αλλοιώσεις, επομένως παρέχουν ακεραιότητα. Επίσης το WEP παρέχει αυθεντικοποίηση εφόσον η ταυτοποίηση ενός χρήστη προηγείται της πρόσβασής του στο δίκτυο.

Ωστόσο, το WEP υστερεί λόγω των πρακτικών που υιοθετεί. Κρυπτογραφεί

τα πλαίσια όσο αυτά διασχίζουν το ασύρματο μέσο. Επιπλέον, παρόλο που σκοπός του είναι να ασφαλίσει το δίκτυο από εξωτερικούς εισβολείς. Μόλις κάποιος ανακαλύψει το κλειδί κρυπτογράφησης, το ασύρματο μέσο γίνεται απευθείας ισοδύναμο με ένα ενσύρματο δίκτυο.

5.6.3 Τύποι κλειδιών στο WEP

Για να προστατέψουμε την κίνηση του δικτύου από επιθέσεις τύπου brute-force, το WEP χρησιμοποιεί ένα σύνολο από (το πολύ) τέσσερα προεπιλεγμένα κλειδιά *(default keys)* τα οποία είναι πιθανόν να περιέχουν ζεύγη κλειδιών που ονομάζονται *mapped keys.* Τα προεπιλεγμένα κλειδιά είναι ίδια για κάθε σταθμό και από τη στιγμή που μοιράζονται, οι σταθμοί μπορούν να χρησιμοποιήσουν το WEP.

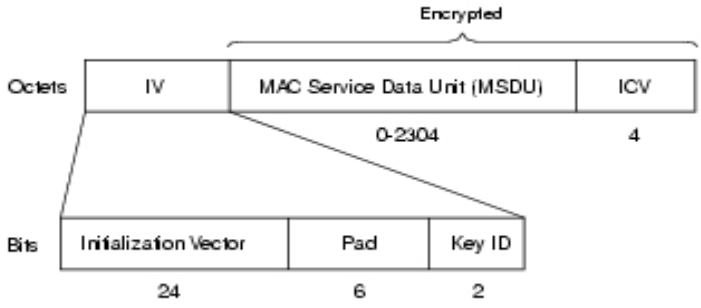
Η επαναχρησιμοποίηση των κλειδιών αποτελεί συχνά μια αδυναμία των πρωτοκόλλων κρυπτογράφησης. Γι' αυτό το WEP διαθέτει μια δεύτερη συλλογή κλειδιών που χρησιμοποιείται σε επικοινωνίες ανά ζεύγη και τα κλειδιά μοιράζονται μόνο στις δυο πλευρές που πρόκειται να επικοινωνήσουν. Αυτές έχουν μια σχέση που ονομάζεται *key mapping σχέση* η οποία, ως διαδικασία αποτελεί τμήμα του 802.11 MIB[25]. Τα mapped keys είναι διαφορετικά κλειδιά για κάθε σταθμό και το σημείο πρόσβασης, για να μπορεί να επικοινωνεί μαζί τους, διατηρεί έναν πίνακα με το κλειδί που χρησιμοποιεί ο κάθε σταθμός. Αυτή η πρακτική βοηθάει στη διατήρηση της μυστικότητας του κλειδιού και επίσης στην ανανέωσή τους, αφού δεν χρειάζεται να τεθεί το δίκτυο εκτός λειτουργίας όταν χρειαστεί να αλλάξουμε κλειδιά.

25 Το 802.11 περιλαμβάνει διάφορες συναρτήσεις διαχείρισης, ώστε το ασύρματο μέσο να μοιάζει με ενσύρματο. Η πολυπλοκότητα αυτών των συναρτήσεων συνεπάγεται την πολυπλοκότητα των οντοτήτων διαχείρισης λόγω της παρουσίας πολλών μεταβλητών. Έτσι, για ευκολία χρήσης, αυτές οι μεταβλητές έχουν οργανωθεί σε μια πληροφοριακή βάση διαχείρισης, την MIB, ώστε οι διαχειριστές του δικτύου να έχουν μια δομημένη οπτική των παραμέτρων του 802.11. [8]

5.6.4 Το πλαίσιο του WEP

Όταν χρησιμοποιούμε το WEP, στο σώμα του πλαισίου προστίθενται οχτώ επιπλέον bytes (σχήμα 5.2).

- ***IV κεφαλίδα (4Bytes):*** χρησιμοποιεί 3 Bytes για το 24bit IV ενώ το τέταρτο byte χρησιμοποιείται για padding και ταυτοποίηση κλειδιών. Όταν χρησιμοποιείται ένα *default κλειδί*, το υποπεδίο *Key ID* το ανιχνεύει. Αν χρησιμοποιείται *key mapping σχέση,* το υποπεδίο Key ID ισούται με 0.
- ***ICV (4Bytes):*** πρόκειται για ένα πεδίο στο σώμα του πλαισίου που προστατεύεται από τον RC4 και ουσιαστικά είναι ένας έλεγχος CRC (Cyclic Redundancy Check).



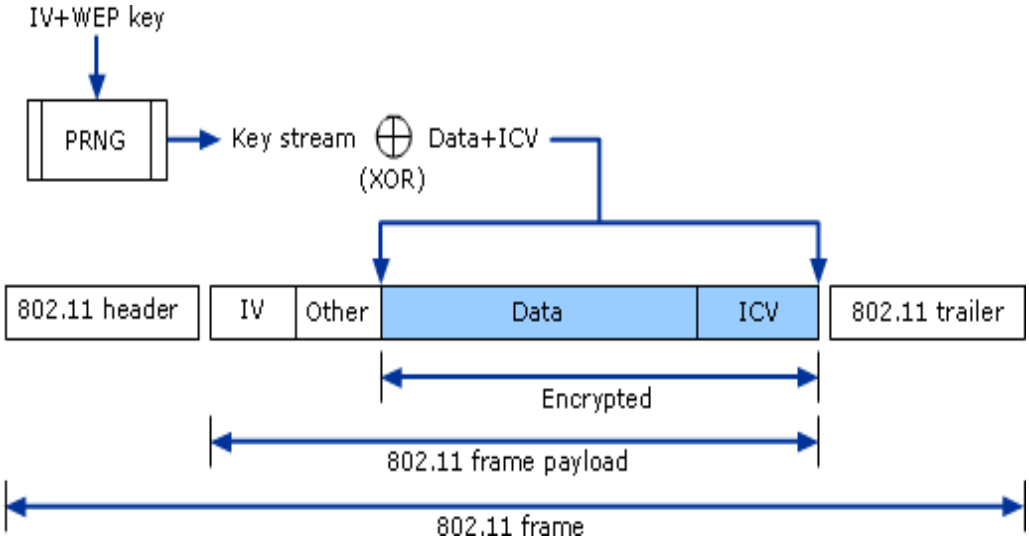
Σχήμα 5.2: Το πλαίσιο του WEP

5.6.5 Πως γίνεται η επεξεργασία των δεδομένων στο WEP

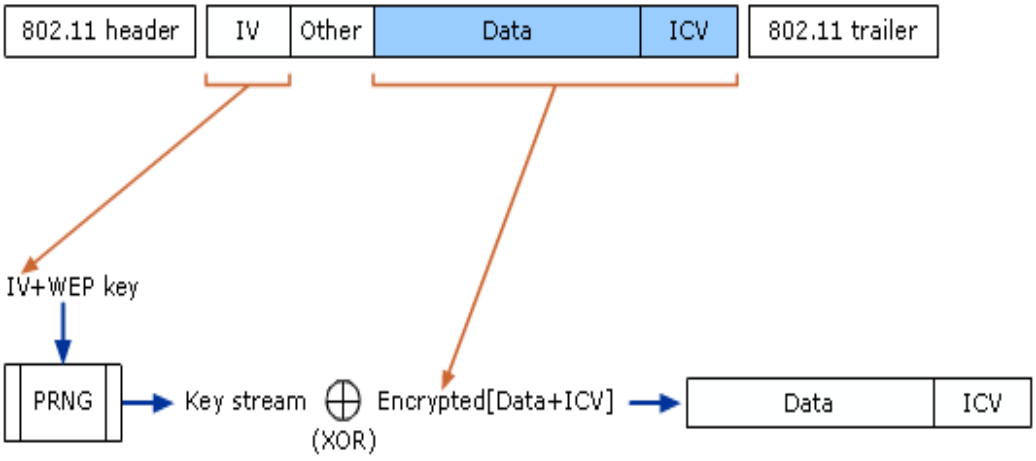
Η εμπιστευτικότητα και η ακεραιότητα είναι δυο διαδικασίες που συμβαίνουν ταυτόχρονα. Πριν από την κρυπτογράφηση, το πλαίσιο ελέγχεται μέσω ενός αλγορίθμου ελέγχου ακεραιότητας, που παράγει μια hash value, γνωστή ως *τιμή ελέγχου ακεραιότητας* (ICV). Η ICV προστατεύει το περιεχόμενο του κάθε πλαισίου από αλλαγές λόγω παρεμβολών και εξασφαλίζει ότι το πλαίσιο δεν έχει αλλάξει κατά τη μεταφορά. Τα δεδομένα και οι ICV κρυπτογραφούνται πάντα.

Το WEP ορίζει τη χρήση ενός μυστικού κλειδιού μήκους 40bits. Αυτό το

κλειδί συνδυάζεται με το διάνυσμα αρχικοποίησης (initialization vector – IV) μήκους 24bits, για να δημιουργήσει ένα κλειδί 64bits μέσω του RC4, τα 24 πρώτα bits του οποίου είναι το IV, ακολουθούμενο από το κλειδί των 40bits. Ο αλγόριθμος RC4 παίρνει αυτά τα 64bits και παράγει μια ακολουθία (keystream) ίση με το μήκος του σώματος των πλαισίων συν το IV. Έπειτα η ακολουθία μαζί με το σώμα πλαισίων και το ICV περνάει από μια συνάρτηση XOR προκειμένου να παράγει το κρυπτογράφημα (Σχήμα 5.3). Για να επιτραπεί στον δέκτη η αποκρυπτογράφηση του πλαισίου, το IV τοποθετείται στην κεφαλίδα του χωρίς να είναι κρυπτογραφημένο (Σχήμα 5.4).



Σχήμα 5.3: Αναπαράσταση της διαδικασίας κρυπτογράφησης στο WEP



Σχήμα 5.4: Η διαδικασία αποκρυπτογράφησης στο WEP

5.6.6 Ο κρυπτογραφικός αλγόριθμος RC4

Κάθε κρυπτογραφικός αλγόριθμος είναι ένα σύνολο από λειτουργίες που εφαρμόζονται σε ένα απλό κείμενο (plaintext) και παράγουν ένα κρυπτογράφημα (ciphertext). Είναι αυτονόητο ότι ένας τέτοιος αλγόριθμος είναι άχρηστος εάν δεν υπάρχει ένας αλγόριθμος αποκρυπτογράφησης. Στην περίπτωση του RC4 όμως, χρησιμοποιείται ο ίδιος αλγόριθμος για κρυπτογράφηση και για αποκρυπτογράφηση. Η ποιότητα ενός κρυπτογραφικού αλγορίθμου εξαρτάται από το πόσο ισχυρός είναι αλλά και από το πόσο εύκολη είναι η υλοποίησή του. Φυσικά, υπάρχουν πιο ισχυροί αλγόριθμοι από τον RC4, ωστόσο χρησιμοποιείται αυτός από το WEP καθώς η υλοποίησή του είναι πολύ απλή και ως λύση είναι ισχυρή όταν γίνεται χρησιμοποιείται σωστά.

Η βασική του ιδέα είναι η παραγωγή μιας ψευδοτυχαίας ακολουθίας από bytes (keystream) η οποία έπειτα συνδυάζεται με τα αρχικά δεδομένα μέσω μιας συνάρτησης XOR. Ένα σημαντικό στοιχείο της εφαρμογής της συνάρτησης XOR είναι ότι εάν εφαρμοστεί δυο φορές, το αποτέλεσμα είναι η λήψη της αρχικής τιμής όπως φαίνεται παρακάτω:

Κρυπτογράφηση: (Αρχικό κείμενο) xor (Τυχαία τιμή) = Κρυπτογράφημα
Αποκρυπτογράφηση: (Κρυπτογράφημα) xor (Τυχαία τιμή) = Αρχικό κείμενο

Η τυχαία τιμή είναι *φαινομενικά τυχαία*, καθώς μοιάζει τυχαία για έναν επιτιθέμενο, ωστόσο και ο αποστολέας και ο παραλήπτης μπορούν να παράγουν αυτήν την "τυχαία τιμή" για κάθε byte που επεξεργάζονται. Αυτός είναι και ο λόγος που αναφερόμαστε σε αυτή την τιμή με τον όρο *ψευδοτυχαία τιμή*.

Η σημαντικότερη ιδιότητα του ψευδοτυχαίου keystream είναι ότι μπορούμε να υπολογίσουμε το επόμενο byte της ακολουθίας μόνο εάν γνωρίζουμε το κλειδί που χρησιμοποιήθηκε για να παραχθεί το keystream, ενώ εάν δεν γνωρίζουμε το κλειδί, η τιμή είναι πραγματικά τυχαία. Επίσης, η συνάρτηση XOR καλύπτει πλήρως το plaintext, έτσι ακόμη και αν αυτό αποτελείται μόνο από μηδενικά το κρυπτογράφημα θα μοιάζει τυχαίο στον επιτιθέμενο.

Επειδή η XOR είναι εύκολα υλοποιήσιμη σε ένα υπολογιστικό σύστημα, η μόνη πρόκληση είναι η παραγωγή μιας ψευδοτυχαίας ακολουθίας. Απαιτείται η παραγωγή ενός ψευδοτυχαίου byte από τον RC4 για κάθε byte του μηνύματος που πρόκειται να κρυπτογραφηθεί.

Ο αλγόριθμος εκτελείται σε δυο διαφορετικές φάσεις. Στην πρώτη φάση δημιουργείται ένας πίνακας των 256 bytes με αριθμούς στο διάστημα 0-255, οι οποίοι υπάρχουν στον πίνακα αναδιατεταγμένοι. Ένας δεύτερος πίνακας των 256bytes (K-box) γεμίζει με το κλειδί και η διαδικασία επαναλαμβάνεται μέχρι να γεμίσει πλήρως ο πίνακας. Έπειτα, οι αριθμοί στο S-box ανακατανέμονται με βάση τις τιμές στο K-box. Έτσι ολοκληρώνεται η πρώτη φάση, κατά την οποία λαμβάνουν μέρος όλες οι αρχικοποιήσεις. Κατά τη δεύτερη φάση έχουμε την παραγωγή της ψευδοτυχαίας ακολουθίας. Το πρώτο ψευδοτυχαίο byte παράγεται από την αναδιάταξη του S-box και την επιλογή ενός byte από αυτό.

Στο WEP και οι δυο φάσεις ενεργούν στο κάθε πακέτο χωριστά και αυτό σημαίνει πως κάθε πακέτο αντιμετωπίζεται σαν μια διαφορετική οντότητα δεδομένων. Έτσι, σε περίπτωση που κάποιο χαθεί, το επόμενο πακέτο μπορεί να αποκρυπτογραφηθεί. [18], [19]

5.6.8 Διαμοιρασμός του κλειδιού

Παρόλο που τα μυστικά WEP κλειδιά πρέπει να διαμοιραστούν σε όλους τους σταθμούς ενός BSS, το 802.11 δεν καθορίζει κάποιον συγκεκριμένο μηχανισμό διαμοίρασής τους. Αυτό είχε σαν αποτέλεσμα να μην καθορίζεται τίποτα από την πλευρά των κατασκευαστών και θα πρέπει ο χρήστης να πληκτρολογεί το κλειδί στις συσκευές του. Η πληκτρολόγηση του κλειδιού από τον χρήστη δημιουργεί τις παρακάτω δυσκολίες:

- Τα κλειδιά δεν μπορούν να θεωρηθούν μυστικά από τη στιγμή που πρέπει να είναι γνωστά σε όλα τα μέλη ενός δικτύου.
- Στο πλαίσιο μιας εταιρίας, κάθε φορά που ένας υπάλληλος αντικαθίσταται από έναν άλλο, τα κλειδιά θα πρέπει να αλλάζουν. Γνωρίζοντας το WEP κλειδί, ένας χρήστης μπορεί να παρακολουθεί και να αποκρυπτογραφεί την κίνηση στο δίκτυο από έναν δικό του σταθμό με μια ασύρματη κάρτα δικτύου. Το WEP μας αφήνει απροστάτευτους ενάντια σε μη εξουσιοδοτημένους εισβολείς οι οποίοι έχουν στα χέρια τους το μυστικό κλειδί.

5.6.9 Ευπάθειες και αδυναμίες του WEP

Όσοι ασχολούνται με την κρυπτανάλυση, έχουν εντοπίσει αρκετά κενά ασφαλείας του WEP. Οι σχεδιαστές εντοπίζουν αδυναμίες σχετικές με τον RC4 ενώ οι hackers δεν στέκονται τόσο στον αλγόριθμο αλλά επιτίθενται ενάντια σε κάθε αδύναμο σημείο ενός κρυπτογραφικού συστήματος. Παρακάτω αναφέρουμε κάποια από τα προβλήματα του WEP. Να σημειώσουμε ότι κανένα από τα προβλήματα που ανακάλυψαν ερευνητές δεν έχει σχέση με το “σπάσιμο” του RC4. [8], [19]

- *Η πληκτρολόγηση του κλειδιού από τον χρήστη: α*ν παραβλέψουμε τα λειτουργικά ζητήματα με τη διανομή των ίδιων κοινών μυστικών κλειδιών στους χρήστες, τα προβλήματα ασφαλείας και πάλι παραμένουν εφιαλτικά. Πρέπει να διανεμηθούν νέα κλειδιά σε όλα τα συστήματα ταυτόχρονα, και

κανονικά με κάθε αποχώρηση κάποιου από το δίκτυο, θα πρέπει να διανέμονται νέα κλειδιά, κάτι το οποίο ίσως να μην είναι εφικτό σε περιπτώσεις που το φορτίο της διαχείρισης δεν το επιτρέπει. Τα ευρέως διαδεδομένα κλειδιά, με την πάροδο του χρόνου τείνουν να γίνονται δημόσια. Οι *sniffing*[26] επιθέσεις απαιτούν μόνο τα κλειδιά WEP, τα οποία είναι πολύ πιθανό να αλλάζουν σπάνια. Μόλις ο επιτιθέμενος λάβει τα κλειδιά WEP, το sniffing είναι εύκολη υπόθεση. Τα προγράμματα που κυκλοφορούν στην αγορά (sniffers) αρχίζουν να ενσωματώνουν αυτήν τη μέθοδο για τους διαχειριστές συστημάτων, καθώς υποστηρίζουν ότι μετά την εισαγωγή των WEP κλειδιών, όλη η κυκλοφορία του δικτύου γίνεται αναγνώσιμη.

- *Παρά τις προσδοκίες των προμηθευτών, η στάνταρ έκδοση του WEP προσφέρει ένα μυστικό κλειδί των 40bits.* Οι ειδικοί σε θέματα ασφάλειας έχουν εξετάσει την επάρκεια των ιδιωτικών κλειδιών αυτού του μήκους και πολλοί συστήνουν ότι τα ευαίσθητα στοιχεία πρέπει να προστατεύονται από κλειδιά με μήκος τουλάχιστον 128 bits. Δυστυχώς, κανένα πρότυπο δεν έχει αναπτυχθεί βασιζόμενο σε μεγαλύτερα κλειδιά και έτσι η διαλειτουργικότητα μεταξύ δικτύων διαφορετικών κατασκευαστών με μεγαλύτερα κλειδιά WEP δεν είναι εγγυημένη καθώς απαιτούνται περεταίρω εργασίες από την IEEE.
- *Οι αλγόριθμοι κρυπτογράφησης που βασίζονται σε ροές (stream ciphers) αποδεικνύονται αδύναμοι όταν χρησιμοποιούν το ίδιο keystream περισσότερες από μια φορές.* Η χρήση του IV μπορεί να δώσει ιδιαίτερες πληροφορίες σε έναν επιτιθέμενο για την επαναχρησιμοποίηση του keystream. Δύο πλαίσια που μοιράζονται το ίδιο IV σχεδόν πάντα χρησιμοποιούν το ίδιο μυστικό κλειδί και το ίδιο keystream. Αυτό το πρόβλημα γίνεται πιο έντονο σε εφαρμογές που η επιλογή του IV μπορεί να μην είναι τυχαία.
- *Η σπάνια μεταβολή των κλειδιών επιτρέπει στους επιτιθεμένους να δημιουργήσουν τα decryption dictionaries, δηλαδή μεγάλες συλλογές από πλαίσια που κρυπτογραφούνται με τα ίδια keystreams (κλειδοροές).* Όσο

26 Η παρακολούθηση των πακέτων που κυκλοφορούν σε ένα δίκτυο.

εμφανίζονται όλο και περισσότερα πλαίσια με το ίδιο IV[27], οι επιτιθέμενοι συγκεντρώνουν περισσότερες πληροφορίες, ακόμα κι αν δεν έχουν αποκτήσει το μυστικό κλειδί. Λαμβάνοντας υπόψη τον βαθμό στον οποίο το προσωπικό μιας εταιρίας ασχολείται με τη διαχείριση συστημάτων και δικτύων της, η σπάνια αλλαγή των κλειδιών αποτελεί κανόνα.

- *Το WEP χρησιμοποιεί έναν CRC για τον έλεγχο της ακεραιότητας.* Αν και η τιμή που παράγεται από τον έλεγχο κρυπτογραφείται μέσω του RC4 keystream, από κρυπτογραφική σκοπιά οι CRC[28] δεν είναι ασφαλείς. Η χρήση ενός αδύναμου ελέγχου ακεραιότητας δεν αποτρέπει τους επιτιθεμένους να τροποποιήσουν τα πλαίσια χωρίς να γίνει αντιληπτό. Τέτοιου είδους αλγόριθμοι μπορούν να συλλάβουν την αλλαγή ενός μόνο bit αλλά δεν είναι ασφαλείς από κρυπτογραφική άποψη. Οι υπολογισμοί που κάνουν είναι απλά μαθηματικά, και είναι εύκολο να προβλεφθεί ο τρόπος με τον οποίο η αλλαγή ενός μόνο bit επηρεάζει το αποτέλεσμα του CRC υπολογισμού. Οι ασφαλείς έλεγχοι ακεραιότητας για την κρυπτογραφία είναι βασισμένοι σε συναρτήσεις κατακερματισμού (hash functions), που η τιμή που παράγουν είναι εντελώς απρόβλεπτη και τυχαία. Με τέτοιου είδους συναρτήσεις, ακόμη να αλλαχθεί και μόνο ένα bit του αρχικού πλαισίου, η τιμή στο πεδίο ελέγχου ακεραιότητας θα αλλάξει απρόβλεπτα και έτσι η πιθανότητα που έχει ένας επιτιθέμενος να βρει ένα τροποποιημένο πλαίσιο

27 Πρόκειται για ένα block από bits που απαιτείται ώστε οι κρυπτογραφικοί αλγόριθμοι να παράγουν ένα μοναδικό ρεύμα, ανεξάρτητο από άλλα ρεύματα που ενδέχεται να παράγονται από το ίδιο κλειδί κρυπτογράφησης, χωρίς να χρειάζεται η παραγωγή νέου κλειδιού κρυπτογράφησης.

28 Ένας CRC κώδικας υπολογίζει μια σύντομη, καθορισμένου μήκους δυαδική ακολουθία, γνωστή επίσης ως CRC, για κάθε block δεδομένων, την οποία αποστέλλει μαζί με τα δεδομένα στον προορισμό. ¨όταν ένα block δεδομένων παραλαμβάνεται, η τιμή CRC υπολογίζεται ξανά και εάν το αποτέλεσμα δεν ταιριάζει με το αρχικό, σημαίνει ότι το block δεδομένων περιέχει κάποιο λάθος. Τότε απαιτείται η διόρθωση του συγκεκριμένου block ή η επαναποστολή του. Διαφορετικά, σε περίπτωση που η τιμή του CRC στον παραλήπτη συμπίπτει με την αρχική, το block θεωρείται σωστό (εν τούτοις, με κάποια μικρή πιθανότητα, οι CRC κώδικες ενδέχεται να αφήνουν μη ανιχνευθέντα λάθη και αυτή είναι η μεγάλη τους αδυναμία).

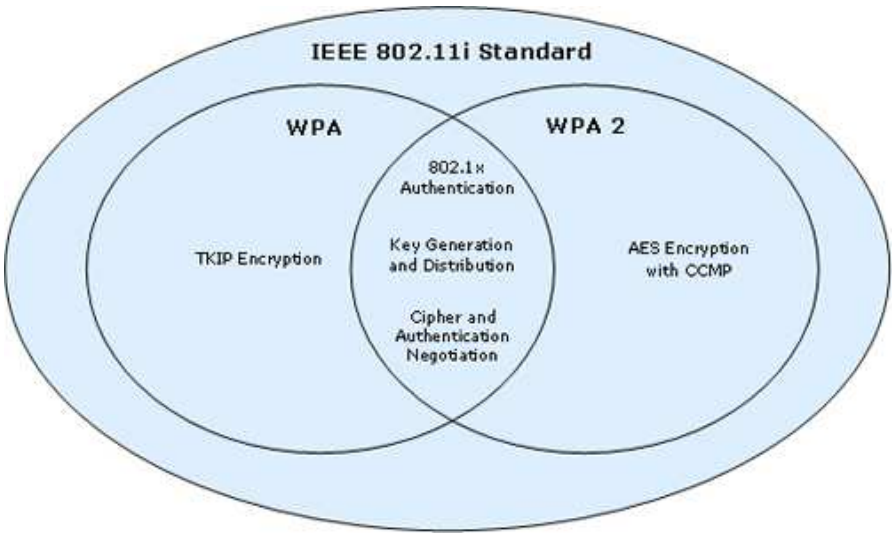
με τον ίδιο έλεγχο ακεραιότητας είναι τόσο μικρή που δεν μπορεί να γίνει σε πραγματικό χρόνο.

- *Η θέση του σημείου πρόσβασης για την αποκρυπτογράφηση των πλαισίων είναι κομβική.* Ουσιαστικά ένας hacker μπορεί να εκμεταλλευτεί αυτό το χαρακτηριστικό για εξαπάτηση του σημείου πρόσβασης ώστε να το αναγκάσει να αναμεταδίδει πλαίσια που κρυπτογραφήθηκαν από το WEP. Τα πλαίσια που παραλαμβάνονται από το σημείο πρόσβασης θα αποκρυπτογραφούνταν και έπειτα θα αναμεταδίδονταν στον σταθμό του επιτιθέμενου. Εάν και αυτός χρησιμοποιεί το WEP, το σημείο πρόσβασης έπειτα θα κρυπτογραφούσε τα πλαίσια χρησιμοποιώντας το κλειδί του.
- *Ο RC4 παράγει αδύναμα κλειδιά.* Το πρόβλημα εμφανίζεται καθώς δεν υπάρχουν πολλοί ανασχηματισμοί μεταξύ του αρχικού πίνακα που περιέχει το κλειδί και του ψευδοτυχαίου byte. Έτσι τα πρώτα bytes του keystream δεν είναι τυχαία, δίνοντας πληροφορίες για το κλειδί.

5.7 Τα πρωτόκολλα ασφάλειας 802.11i και 802.1x των WLANs

Σήμερα υπάρχουν δυο σημαντικές βελτιώσεις οι οποίες αναπτύχθηκαν για να καλύψουν τα κενά ασφάλειας του WEP που ήδη αναφέραμε. Η IEEE έχει ορίσει δυο πρότυπα που καλύπτουν τις απαιτήσεις για ιδιωτικότητα και αυθεντικοποίηση:

- **802.11i:** πρόκειται για πρότυπο ασφάλειας το οποίο εισάγει έναν νέο τύπο ασύρματων δικτύων που ονομάζεται Robust Security Network (RSN) και χρησιμοποιεί τον AES ως αλγόριθμο κρυπτογράφησης ενώ εφαρμόζει 802.1x αυθεντικοποίηση.
- **802.1x:** είναι ένα πρότυπο που χρησιμοποιείται για αυθεντικοποίηση τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα και βασίζεται στο EAP (Extensible Authentication Protocol).



Σχήμα 5.5: Το πρότυπο ασφάλειας 802.11i

5.7.1 WiFi Protected Access της WiFi Alliance (WPA)

Η WiFi Alliance, αναγνωρίζοντας τις ανησυχίες των χρηστών όσο αφορά στην ασφάλεια και στο κόστος της αναβάθμισης για την υποστήριξη του 802.11i, ανέπτυξε ένα σχέδιο προκειμένου να βελτιώσει την ασφάλεια στα WLANs και το ονόμασε WiFi Protected Access. Το πιο σημαντικό σημείο του WPA είναι το γεγονός ότι μπορεί να υλοποιηθεί επάνω στις ήδη υπάρχουσες κάρτες ασύρματης δικτύωσης μόνο με μια αναβάθμιση στο λογισμικό. Οι συσκευές που έχουν ελεγχθεί και λειτουργούν σωστά με το WPA, πιστοποιήθηκαν και ονομάζονται WPA πιστοποιημένες συσκευές (WPA certified). Τα δυο βασικά συστατικά που συμπεριλαμβάνονται στο WPA είναι τα εξής:

- ***Το Temporal Key Integrity Protocol (TKIP):*** προκειμένου να καλυφθούν τα κενά κρυπτογράφησης του WEP, το WPA χρησιμοποιεί το πρωτόκολλο TKIP. Το TKIP χρησιμοποιεί τον ίδιο RC4 αλγόριθμο κρυπτογράφησης όπως και το WEP και έτσι δεν χρειάζονται αλλαγές στο υλικό για τη λειτουργία του WPA. Το πρωτόκολλο ονομάζεται *Temporal Key* διότι σε κάθε

πακέτο το κλειδί κρυπτογράφησης αλλάζει, γεγονός που δυσκολεύει τους επιτιθέμενους στο σπάσιμο του κλειδιού εφόσον η εύρεση πακέτων με το ίδιο κλειδί είναι απίθανη.

- ***Ο έλεγχος της ακεραιότητας των μηνυμάτων - Message Integrity Check (MIC):*** Ο MIC (ονομάζεται και Michael) είναι ουσιαστικά ένας CRC έλεγχος και σκοπός του είναι να διαβεβαιώνει τον παραλήπτη ότι το μήνυμα που έλαβε δεν έχει υποστεί καμία τροποποίηση. Δυστυχώς όμως ο MIC δεν παρέχει τόσο καλό επίπεδο ελέγχου και παρουσιάζει ευπάθειες σε επιθέσεις τύπου *bit-flipping* κατά τις οποίες ο επιτιθέμενος αλλάζει ταυτόχρονα κάποια bits του μηνύματος και έπειτα αλλάζει και την τιμή του MIC.

5.7.1.1 Τρόπος λειτουργίας του πρωτοκόλλου TKIP

Μια συνάρτηση κατακερματισμού ενεργοποιεί το κλειδί κάθε πακέτου και έπειτα συνδυάζει την διεύθυνση MAC του αποστολέα, το IV και αυτό το κλειδί (κλειδί συνόδου). Προκειμένου να διατηρηθούν χαμηλά τα επίπεδα ενεργειακής κατανάλωσης από την παραγωγή του κλειδιού, η διαδικασία αυτή εκτελείται σε δυο φάσεις.

Κατά την πρώτη φάση, η MAC διεύθυνση του αποστολέα, το κλειδί συνόδου και τα πρώτα 32 bits του IV περνούν από τη συνάρτηση κατακερματισμού. Το αποτέλεσμα από αυτή τη φάση παραμένει ίδιο μέχρι να αλλάξει το κλειδί συνόδου ή να αλλάξουν τα υπόλοιπα bits του IV (εκτός από τα 32 που χρησιμοποιήθηκαν).

Η δεύτερη φάση εκτελείται για κάθε πακέτο που λαμβάνεται. Τα υπόλοιπα 16 bits του IV και το αποτέλεσμα της πρώτης φάσης περνούν από τη συνάρτηση κατακερματισμού με αποτέλεσμα ένα κλειδί των 104 bits για κάθε πακέτο.

Μετά από τη δεύτερη φάση, η διαδικασία κρυπτογράφησης είναι παρόμοια με εκείνη του WEP. Οι διαφορές τους είναι οι εξής: Το IV του WEP με μήκος 24 bits αντικαθίσταται από τα 16 τελευταία bits του IV του WPA με ένα *dummy byte* να παρεμβάλλεται στη μέση (για να αποφεύγεται η δημιουργία αδύναμων κλειδιών) και το κλειδί WEP αντικαθίσταται από το κλειδί συνόδου κάθε πακέτου. Οι

διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης εκτελούνται όπως και στο WEP.

Χρησιμοποιώντας το TKIP, το κλειδί κρυπτογράφησης είναι ένα κλειδί των 128 bits, με 24 bits να χρησιμοποιούνται δυναμικά και με στατικό κλειδί 40 ή 104 bits, βελτιώνοντας αποτελεσματικά την ασφάλεια των ασύρματων δικτύων.

Πίνακας 5.3: Σύγκριση των μεθόδων του WEP και του WPA

Σκοπός	**WPA/TKIP**	**WEP**
Επιλογή IV	Άλλαξε τους κανόνες επιλογής του IV και αύξησε το μέγεθός του για να μειωθεί η πιθανότητα επαναχρησιμοποίησής του	Το μέγεθος του IV είναι αρκετά μικρό και οδηγεί σε επαναχρησιμοποίηση
Ακεραιότητα μηνυμάτων	Πρόσθεσε ένα πρωτόκολλο ακεραιότητας των μηνυμάτων για να αποφευχθεί η αλλοίωση των μηνυμάτων	Δεν υπάρχει κάποιος αποτελεσματικός τρόπος ελέγχου της ακεραιότητας
Διαφορετικό κλειδί	Κάθε πακέτο κρυπτογραφείται με διαφορετικό κλειδί	Ο τρόπος που συνδυάζονται τα κλειδιά με το IV οδηγεί σε επιθέσεις που στοχεύουν στην ανάκτηση του κλειδιού
Διαχείριση κλειδιών	Υπάρχει μέθοδος διαμοιρασμού των κλειδιών	Το αρχικό κλειδί (master key) που δίνει ο χρήστης χρησιμοποιείται απευθείας για κρυπτογράφηση. Δεν υπάρχει καθορισμένος τρόπος ανανέωσης των κλειδιών

5.7.2 802.11i / WPA2: Advanced Encryption Standard (AES)

Στο 802.11i περιγράφονται οι ενισχυμένες κρυπτογραφικές δυνατότητες των WLANs. Η WiFi Alliance έχει ορίσει το WPA2 ώστε να υπάρχει συμβατότητα με το 802.11i. Το χαρακτηριστικό του πρωτοκόλλου είναι η χρήση του AES αλγορίθμου για κρυπτογράφηση. Με την πρόοδο της τεχνολογίας και την υπολογιστική δύναμη των νέων συστημάτων, οι επιθέσεις τύπου *brute force* καθιστούν εύκολους στόχους τον RC4 και τους DES και 3DES αλγορίθμους.

Το 1997 το NIST (National Institute of Standards and Technology) παρουσίασε μια μελέτη για την αντικατάσταση του DES. Τελικά η επιτροπή επέλεξε έναν νέο αλγόριθμο, ο οποίος ήταν ο AES. Συγκεκριμένα, η υλοποίηση που χρησιμοποιείται στο 802.11i ονομάζεται *Counter Mode with CBC-MAC Protocol* (ή CCMP). Πρόκειται για έναν συμμετρικό αλγόριθμο που χωρίζει τα δεδομένα σε blocks, δηλαδή χωρίζει τα μη κρυπτογραφημένα δεδομένα και έπειτα εφαρμόζεται σε αυτά. Το γεγονός ότι πρόκειται για συμμετρικό αλγόριθμο σημαίνει ότι το block δεδομένων έχει ίδιο μέγεθος στην είσοδο και στην έξοδο του από τη διαδικασία. Κάθε block συνήθως ισούται με 128 bits και το κλειδί κρυπτογράφησης έχει μήκος 128, 192, ή 256 bits. Η υλοποίηση του 802.11i χρησιμοποιεί κλειδί μήκους 128 bits με τα οποία μπορεί να παράγει 3.4×10^{38} διαφορετικούς συνδυασμούς.

Ένα βασικό πρόβλημα που υπάρχει στο 802.11i είναι ότι τα παλαιότερα σημεία πρόσβασης και οι παλιές κάρτες δικτύου δεν διαθέτουν το κατάλληλο υλικό για να μπορούν να χρησιμοποιήσουν τον AES. Όμως από τα μέσα του 2006, η WiFi Alliance απαίτησε τη συμβατότητα των συσκευών που πιστοποιούσε με το πρωτόκολλο 802.11i, έτσι ώστε όλες οι συσκευές WiFi δεύτερης γενιάς που εισήχθησαν στην αγορά από το 2007 και έπειτα, να συμπεριλαμβάνουν τις δυνατότητες που παρέχει το WPA2. [1]

5.7.2.1 Ο αλγόριθμος AES – CCMP

Ο AES είναι ένας αλγόριθμος κρυπτογράφησης ο οποίος χωρίζει τα δεδομένα σε blocks σταθερού μήκους και έπειτα τα κρυπτογραφεί. Για το 802.11i το μέγεθος των blocks είναι ίσο με το μέγεθος των κλειδιών ανά πακέτο, δηλαδή 128 bits. Αλγόριθμοι όπως ο AES έχουν διάφορους τρόπους λειτουργίας προκειμένου να χωρίσουν τα δεδομένα σε blocks. Η μέθοδος που έχει επιλεχθεί από το 802.11i είναι η *CCMP - Counter mode with Cipher Block Chaining Message Authentication Code*:

- η λειτουργία *Counter mode* παρέχει ιδιωτικότητα χωρίς να κρυπτογραφεί απευθείας τα blocks δεδομένων. Αντί αυτού, κρυπτογραφείται μια τυχαία τιμή και έπειτα συνδυάζεται με ένα block μέσω μιας συνάρτησης XOR. Μετά από κάθε επιτυχώς κρυπτογραφημένο block, η τυχαία τιμή αυξάνεται κατά μια μονάδα.
- *Ο Cipher Block Chaining Message Authentication Code* χρησιμοποιείται για να προστατέψει την ακεραιότητα των δεδομένων καθώς παράγει την τιμή Message Integrity Code – MIC. Για την παραγωγή του MIC, κάθε κρυπτογραφημένο block περνάει από μια συνάρτηση XOR μαζί με το αποτέλεσμα του προηγούμενου MIC. Έπειτα το αποτέλεσμα κρυπτογραφείται από τον AES και η διαδικασία επαναλαμβάνεται για όλα τα blocks. Με αυτόν τον τρόπο τα δεδομένα από όλα τα blocks συνδυάζονται σε ένα και μόνο block των 128 bits. [19]

5.7.3 Υλοποιήσεις των WPA/WPA2 – Personal ή Enterprise;

Οι υλοποιήσεις που υπάρχουν για το WPA και το WPA2 είναι δυο και χρησιμοποιούν διαφορετικούς τρόπους για την παραγωγή του αρχικού κλειδιού κρυπτογράφησης:

- ***Personal:*** πρόκειται για μια έκδοση που χρησιμοποιεί ένα προμοιρασμένο κλειδί (PSK – preshared key) δηλαδή ο χρήστης αναλαμβάνει την τοποθέτηση του αρχικού κλειδιού στο σημείο πρόσβασης και στον σταθμό,

όπως ακριβώς έκανε και κατά τη χρήση του WEP. Χρησιμοποιείται περισσότερο στο WEP και δεν προτείνεται για χρήση με το WPA2.

- ***Enterpise:*** αυτή η υλοποίηση απαιτεί έναν εξυπηρετητή, ο οποίος χρησιμοποιεί κάποιο από τα 802.1x πρωτόκολλα αυθεντικοποίησης. Ο χρήστης εισάγει κάποιες κρίσιμες πληροφορίες στον εξυπηρετητή (όπως το όνομά του και τον κωδικό πρόσβασης), ενώ αυτός κάνει την αυθεντικοποίηση, παρέχοντας στον χρήστη το κλειδί κρυπτογράφησης ως τμήμα αυτής της ανταλλαγής.

Μια πολύ σημαντική αδυναμία της χρήσης του προμοιρασμένου κλειδιού είναι ότι βάση της παραγωγής του αποτελεί το αρχικό κλειδί που επιλέγεται από τον χρήστη. Άμεση συνέπεια αυτού είναι ότι κάθε πιθανός επιτιθέμενος, “μαντεύοντας” το αρχικό κλειδί και γνωρίζοντας τον αλγόριθμο παραγωγής των επόμενων κλειδιών (αφού ο τρόπος λειτουργίας του είναι γνωστός), ουσιαστικά μπορεί να ανακτήσει όλα τα κλειδιά. Επιθέσεις τέτοιου είδους που ο επιτιθέμενος μαντεύει το αρχικό κλειδί χρησιμοποιώντας μια λίστα από συνηθισμένες επιλογές κλειδιών ονομάζονται *επιθέσεις λεξικού* (dictionary attacks).

Από τις αρχές του 2007, το WPA και το WPA2 χρησιμοποιούνταν στον ίδιο βαθμό, παρά το γεγονός ότι τα ποσοστά χρήσης των εικονικών δικτύων (VPN/VLAN) ήταν λίγο μεγαλύτερα. Σιγά σιγά όμως το WPA2 άρχισε να κερδίζει έδαφος. Όσοι χρησιμοποιούν ακόμη και την enterprise υλοποίηση του WPA δεν αισθάνονται απόλυτα ασφαλείς εξαιτίας της χρήσης του αλγορίθμου RC4, εξακολουθούν όμως να το θεωρούν μια καλή λύση για τα τοπικά δίκτυα στο πλαίσιο ενός σπιτιού.

5.7.4 Extensible Authentication Protocol (EAP): 802.1x

Το WPA και το WPA2 προσφέρουν ιδιωτικότητα στα δεδομένα και προστατεύουν από την παράνομη παρακολούθησή τους. Δεν παρέχουν όμως

μηχανισμούς αυθεντικοποίησης και γι' αυτόν το λόγο έχει αναπτυχθεί το πρωτόκολλο 802.1x που χρησιμοποιείται σε ενσύρματα και ασύρματα δίκτυα. Το πρωτόκολλο εφαρμόζει διάφορες μεθόδους αυθεντικοποίησης και βασίζεται στην αυθεντικοποίηση μέσω πορτών (port-based authentication)[29]. Λόγω της φύσης των ασύρματων δικτύων, μπορούμε να διαχωρίσουμε σε τρεις φάσεις την διαδικασία της αυθεντικοποίησης:

- ***1η φάση - Ισχυρή προστασία των ευαίσθητων δεδομένων των χρηστών:*** απαιτείται η προστασία από την παρακολούθηση τρίτων και για να επιτευχθεί, οι περισσότερες υλοποιήσεις χρησιμοποιούν μηχανισμούς ασφάλειας σε επίπεδο μεταφοράς (transport layer security – TLS).
- ***2η φάση - Αμοιβαία αυθεντικοποίηση:*** προκειμένου να αποφευχθούν επιθέσεις τύπου man-in-the-middle, θα πρέπει οι συσκευές των χρηστών να λειτουργούν έτσι ώστε να μην μεταδίδουν σε τρίτους δεδομένα που είναι απαραίτητα για την αυθεντικοποίησή τους.
- ***3η φάση - Διαμοιρασμός κλειδιών:*** η αδυναμία των σταθερών κλειδιών είναι αποδεδειγμένη, επομένως θα πρέπει σε κάθε σύνοδο να χρησιμοποιούνται διαφορετικά κλειδιά. [1]

5.7.4.1 Η διαδικασία της αυθεντικοποίησης με το 802.1x

Κατά τη χρήση του 802.1x, το σημείο πρόσβασης επιτρέπει αρχικά στον σταθμό να επικοινωνήσει μόνο με τον εξυπηρετητή. Όταν η διαδικασία της αυθεντικοποίησης ολοκληρωθεί επιτυχώς, το σημείο πρόσβασης θα επιτρέψει στον σταθμό να επικοινωνήσει και με τις υπόλοιπες οντότητες του δικτύου. Όσο διαρκεί η διαδικασία της αυθεντικοποίησης, ανταλλάσσονται EAP-αιτήματα και EAP-απαντήσεις μεταξύ:

- των σταθμών (supplicants)

29 Στα ασύρματα δίκτυα η “πόρτα” είναι ουσιαστικά η συσχέτιση ενός σταθμού με το σημείο πρόσβασης που είναι κάτι ανάλογο με τη φυσική σύνδεση δυο συσκευών στα ενσύρματα δίκτυα.

- του authenticator, δηλαδή της οντότητας που ελέγχει την είσοδο των σταθμών στο δίκτυο και λειτουργεί ως ενδιάμεσος μεταξύ των σταθμών και του εξυπηρετητή αυθεντικοποίησης
- και του εξυπηρετητή αυθεντικοποίησης (authentication server) που αποφασίζει αν ο σταθμός γίνεται αποδεκτός ή όχι. [18]

5.7.4.2 Πρωτόκολλα αυθεντικοποίησης του 802.1x

Επειδή το 802.1x δεν απαιτεί κάποιο συγκεκριμένο πρωτόκολλο αυθεντικοποίησης, τα πρωτόκολλα που λειτουργούν μαζί του είναι πολλά. Βασίζεται στο EAP που είναι πρωτόκολλο ενθυλάκωσης και γι' αυτό επιτρέπει την χρήση διαφορετικών πρωτοκόλλων αυθεντικοποίησης. Παρακάτω αναφέρονται κάποια από τα σημαντικότερα πρωτόκολλα:

- **LEAP (Lightweight EAP):** πρόκειται για μια ευρέως χρησιμοποιούμενη μέθοδο αυθεντικοποίησης της Cisco, η οποία βασίζεται στο όνομα ενός χρήστη και στον κωδικό πρόσβασης που κατέχει. Το LEAP χρησιμοποιεί το MS-CHAP (Microsoft Challenge Handshake Protocol) για να παρέχει αυθεντικοποίηση. Παρόλο που παρέχει αμοιβαία αυθεντικοποίηση και κρυπτογράφηση των κλειδιών συνόδου, περιέχει κάποια αδύναμα σημεία. Τα βασικά προβλήματα του LEAP είναι η χρήση του απαρχαιωμένου πλέον MS-CHAP, καθώς και η ευπάθειά του απέναντι στις επιθέσεις λεξικού και γενικά σε περιβάλλοντα που δεν μπορούν να εφαρμοστούν ισχυρές πολιτικές ασφάλειας για τους κωδικούς πρόσβασης.
- **EAP FAST (EAP Flexible Authentication via Secure Tunneling):** Το πρωτόκολλο που προτείνει σήμερα η Cisco είναι το PEAP ή το EAP FAST. Το EAP FAST χρησιμοποιεί αλγορίθμους συμμετρικού κλειδιού για να πετύχει αυθεντικοποίηση μέσω σήραγγας (*tunnel*) η οποία βασίζεται σε προστατευμένα στοιχεία σύνδεσης (PAC - Protected Access Credential). Η χρήση σήραγγας καθιστά το πρωτόκολλο ικανό να προστατέψει τους χρήστες ενός δικτύου ενάντια σε επιθέσεις τύπου man-in-the-middle και επιθέσεις λεξικού.

- **EAP-TLS (Transport Layer Security):** Είναι μηχανισμός αυθεντικοποίησης ο οποίος χρησιμοποιεί ένα δημόσιο κλειδί (Public Key Infrastructure) και η αυθεντικοποίηση βασίζεται σε πιστοποιητικά ασφάλειας. Το EAP-TLS είναι αντίστοιχο του πρωτοκόλλου SSL που χρησιμοποιείται για να προστατέψει τις μεταδόσεις δεδομένων στο διαδίκτυο. Από τη στιγμή που ο σταθμός αυθεντικοποιηθεί, το 802.1x ξεκινάει τη διαδικασία παραγωγής κλειδιών. Το μεγάλο μειονέκτημα του TLS είναι ότι για τη λειτουργία του απαιτείται η εγκατάσταση ψηφιακών πιστοποιητικών στις συσκευές όλων των χρηστών.
- **EAP-TTLS (Tunneled TLS) και PEAP (Protected TLS):** το TTLS και το PEAP είναι δυο παρόμοιοι μηχανισμοί και ουσιαστικά πρόκειται για επεκτάσεις του TLS. Μπορούν να χρησιμοποιηθούν μαζί με πρωτόκολλα αυθεντικοποίησης υψηλότερων επιπέδων όπως το MS-CHAPv2 και τα απαιτούμενα πιστοποιητικά αφορούν μόνο την πλευρά των εξυπηρετητών. Σχετικά με τον τρόπο λειτουργίας τους, αρχικά εγκαθιδρύουν μια TLS σήραγγα (outer authentication), ενώ στη δεύτερη φάση τα δεδομένα που απαιτούνται για την αυθεντικοποίηση αποστέλλονται μέσω μιας κρυπτογραφημένης σύνδεσης (inner authentication). [1]

Επίλογος

Στο παρόν κεφάλαιο αναλύθηκαν γενικά οι απαιτήσεις ασφάλειας καθώς και οι ευπάθειες των ασύρματων τοπικών δικτύων. Δόθηκε έμφαση σε πρωτόκολλα ασφάλειας που ήδη χρησιμοποιούνται όπως το WEP, το WPA, το WPA/2 και αναφέρθηκαν οι τρόποι λειτουργίας των αλγορίθμων που αυτά υλοποιούν. Τέλος, περιγράφηκε συνοπτικά το πρωτόκολλο αυθεντικοποίησης 802.11X.

Προτάσεις

Ο τομέας των ασύρματων τοπικών δικτύων εκτός από τη χρησιμότητά του, είναι ιδιαίτερα κερδοφόρος και αποτελεί ένα ενδιαφέρον ερευνητικό κομμάτι των δικτύων, λόγω των δυσκολιών που εισάγει η φύση του ασύρματου μέσου. Σήμερα η αγορά ασύρματων τοπικών δικτύων έχει ενσωματωθεί με την κινητή τηλεφωνία αλλά και με άλλες συσκευές όπως ασύρματα τηλέφωνα, συσκευές αναπαραγωγής ήχου, ακόμη και τηλεοράσεις. Επίσης μεγάλο βάρος δίνεται στην τεχνολογία WiMax η οποία έχει δυνατότητες μεγαλύτερης κάλυψης σε σχέση με το WiFi, αν και τα δυο πρότυπα σχεδιάστηκαν για διαφορετικούς σκοπούς.

Επίσης, έχουν αναπτυχθεί από ερευνητικές ομάδες πρότυπα που αντικαθιστούν το WiFi, και κατασκευάστηκαν για εφαρμογές όπου η παρεχόμενη εμβέλεια του WiFi δεν επαρκεί ενώ η χρήση καλωδίων θα ήταν μια οικονομικά ασύμφορη λύση. Ένα τέτοιο πρότυπο είναι το ITU-T G.hn (τεχνολογία power line) που κατασκευάστηκε για να χρησιμοποιεί τις ήδη υπάρχουσες γραμμές καλωδίων, είτε ηλεκτρικού ρεύματος είτε τηλεφώνου. Παρά το γεγονός ότι το πρότυπο G.hn μπορεί να χρησιμοποιηθεί μόνο εντός ενός χώρου που υπάρχει ρεύμα ή τηλέφωνο, έχει σχεδιαστεί για εφαρμογές όπως η IPTV όπου η εμβέλεια μέσα σε ένα χώρο είναι σημαντικότερη από τη φορητότητα.

Η μελέτη των μειονεκτημάτων και η ανεύρεση νέων τρόπων, που θα οδηγήσουν στην επίλυση προβλημάτων και στην κάλυψη των αδυναμιών της υπάρχουσας τεχνολογίας (όπως νέες μέθοδοι που θα εξασφαλίζουν απόλυτη προστασία των μεταδιδόμενων πληροφοριών από επιθέσεις τρίτων ή τρόποι αύξησης της εμβέλειας των ασύρματων συσκευών, χωρίς αυτό να είναι βλαβερό για την υγεία μας) είναι θέματα που πρέπει να μας απασχολήσουν και ίσως αποτελέσουν το έναυσμα για επέκταση του θέματος με το οποίο καταπιάστηκα στην παρούσα πτυχιακή εργασία.

Βιβλιογραφία

[1] Finneran Michael, “Voice Over WLANs the complete guide”, Newnes, 2008

[2] http://www.boingboing.net/2005/11/08/wifi_isnt_short_for_.html

[3] http://en.wikipedia.org/wiki/Wi-Fi

[4] Denis Bakin, “Evolution of 802.11 (physical layer”, May 2007, https://www.okob.net/texts/mydocuments/80211physlayer/

[5] Π. Νικοπολιτίδης, M. S. Obaidat, Γ. Ι. Παπαδημητρίου, Α. Σ. Πομπόρτσης, “Ασύρματα Δίκτυα”, Κλειδάριθμος, 2006

[6] A. Forouzan, “Data Communications And Networking”, McGraw-Hill, 2007 http://www.globalspec.com/reference/10509/121073/Chapter-6-2-2-Frequency-Hopping-Spread-Spectrum-FHSS

[7] http://www.blahblah.gr/2010/02/wifi.html

[8] Gast Matthew, “Wireless Networks: The Definitive Guide”, O' Reilly, April 2002

[9] Guoliang Li, Thesis “Physical Layer Design for a Spread Spectrum Wireless LAN”, faculty of the Virginia Polytechnic Institute and State University, 1996

[10] Αυγουστίνος Κ. Φιλιππουπολίτης, Διπλωματική εργασία: “Ανάλυση της επίδοσης δικτύων WLAN υπό φορτίο αλληλοδραστικών εφαρμογών”, Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, 2004, http://artemis.cslab.ntua.gr/Dienst/UI/1.0/Display/artemis.ntua.ece/DT2004-0070

[11] Pablo Brenner, “A technical tutorial on the IEEE 802.11 Protocol”, 1996, http://www.sss-mag.com/pdf/802_11tut.pdf

[12] Πανοπούλου Β. Ελένη, πτυχιακή εργασία “Θεωρία και ψηφιακή προσομοίωση ασυρμάτων τοπικών δικτύων υψηλής ταχύτητας: τα πρότυπα IEEE 802.11 και ETSI Hiperlan 2”, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Πολυτεχνική σχολή, 2002

[13] S. Selvakennedy, “Integrated Performance Analysis of PCF and DCF Schemes over IEEE 802.11a Physical Layer”, University of Sydney, School of IT, 2006, http://www.cs.usyd.edu.au/~skennedy/papers/witsp2003.pdf

[14] Imad Aad and Claude Castelluccia, “Differentiation mechanisms for IEEE 802.11”, PLANETE project, INRIA, http://www.inrialpes.fr/planete/people/ccastel/infocom01.ps

[15] Xuanming Dong, Pravin Varaiya, and Anuj Puri, “An Adaptive Polling Algorithm for PCF Mode of 802.11 Wireless LANs”, University of California, Berkeley, Department of Electrical Engineering & Computer Science, http://wwwinst.eecs.berkeley.edu/~ee228a/fa03/228A03/802.11%20wlan/802.11_polling.pdf

[16] http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[17] Viral V. Kapadia, Sudarshan N. Patel and Rutvij H. Jhaveri, “Comparative study of hidden node problem and solution using different techniques and protocols”, Journal of Computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617

[18] John Edney and William A. Arbaugh, “Real 802.11 Security”, Addison Wesley, 2004

[19] Luis Carlos Wong, “An overview of 802.11 Wireless Network Security Standards & Mechanisms”, Sans Institute InfoSec Reading Room, 2004 http://www.sans.org/reading_room/whitepapers/wireless/overview-80211-wireless-network-security-standards-mechanisms_1530