



Πανεπιστήμιο Πελοποννήσου

Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

**«Ασύρματα δίκτυα και οι επιπτώσεις της Η/Μ
ακτινοβολίας τους»**

Πτυχιακή Εργασία

Δημήτριος Φλέγκας Α.Μ. 2993

Επιβλέπων: Λάμπρος Δρόσος Καθηγητής

Χρόνος εκπόνησης : 6 μήνες

Πάτρα 2022

Περιεχόμενα

1.1 Τα οφέλη της ασύρματης δικτύωσης.....	9
1.1.1 Δυνατότητα κίνησης	9
1.1.2 Μείωση κόστους	10
1.1.3 Εγκατάσταση σε περιοχές που καλωδιώνονται δύσκολα.	10
1.1.4 Αυξανόμενη αξιοπιστία	12
1.1.5 Μειωμένος χρόνος εγκατάστασης	12
1.1.6 Μακροπρόθεσμη μείωση κόστους	13
1.2 Αγορές και εφαρμογές ασύρματων δικτύων	14
1.2.1 Γενικά	14
1.2.2 Λιανικές Πωλήσεις	14
1.2.3 Αποθήκες εμπορευμάτων	15
1.2.4 Υγειονομική περίθαλψη	16
1.2.5 Ακίνητη περιουσία	17
1.2.6 Φιλοξενία	18
1.2.7 Οργανισμοί κοινής ωφελείας	18
1.3 Παράγοντες σχεδίασης ασύρματων δικτύων	20
1.3.1 Γενικά	20
1.3.2 Παρεμβολή ραδιοσημάτων	20
1.3.3 Εσωτερική παρέμβαση	20
1.3.4 Εξωτερική παρέμβαση	21
1.3.5 Τεχνικές για την αποφυγή παρεμβολών	22
1.3.6 Διαχείριση ισχύος.....	22

1.3.7 Διαλειτουργικότητα συστημάτων	23
1.4 Ασφάλεια δικτύων	24
1.4.1 Γενικά.....	24
1.4.2 Απειλές ασφάλειας	24
1.4.3 Μέτρα προστασίας ασφάλειας.....	25
1.4.4 Προβλήματα σύνδεσης	26
1.4.5 Ζητήματα εγκατάστασης	27
2.1 Τα συστατικά ενός ασύρματου δικτύου.....	29
2.1.1 Γενικά.....	29
2.1.2 Φυσική αρχιτεκτονική ενός ασύρματου δικτύου	29
2.1.3 Συσκευές τελικών χρηστών	30
2.1.4 Λογισμικό δικτύων	31
2.1.5 Ασύρματη διεπαφή δικτύων	32
2.1.6 Κεραία.....	33
2.1.7 Το κανάλι επικοινωνιών.....	35
2.2 Η ιστορία των ασύρματων δικτύων.....	36
2.3 Το μέλλον των ασύρματων δικτύων.....	38
3.1 Γενικά.....	39
3.2 Κεραίες.....	42
3.2.1 Γενικά.....	42
3.2.2 Omni.....	42
3.2.3 Sector.....	43
3.2.4 Yagi.....	44
3.2.5 Παραβολικό πιάτο (Parabolic dish)	45

3.3 Χαρακτηριστικά καλωδίων και συνδέσμων	47
3.3.1 Σύνδεσμοι.....	47
3.3.2 Καλώδια.....	48
3.4 Κανονιστικό πλαίσιο.....	53
4.1 Προβλήματα ασφάλειας δικτύου.....	54
4.2 802.11 Τα χαρακτηριστικά γνωρίσματα ασφαλείας του 802.11..	56
4.2.1 SSID – Service Set Identifier	56
4.2.2 WEP - Wired Equivalent Privacy	56
4.2.3 Authentication and association στο 802.11	57
4.2.4 802.1X.....	58
4.3 LEAP - Lightweight Extensible Authentication	60
Protocol	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
4.3.1 Distribution of WEP Keys on a Per-session Basis	60
4.3.2 Αρχιτεκτονική LEAP της CISCO	60
4.4 Συστήματα ανίχνευσης εισβολών.....	64
(Intrusion Detection Systems).....	64
4.4.1 Τρέχουσες τεχνικές IDS.....	64
4.4.2 Πλεονεκτήματα και μειονεκτήματα.....	65
4.5 Προστασία της μεταδιδόμενης πληροφορίας στα ψηφιακά συστήματα	66
4.6 Ασφαλίζοντας τα ασύρματα δίκτυα AD HOC	67
4.7 Ανίχνευση εισβολής στα ασύρματα δίκτυα ad hoc	68
4.8 Ασφάλεια του πρωτοκόλλου των δικτύων ad hoc	70

5.1 Εισαγωγή	71
5.2 Ηλεκτρομαγνητικά κύματα.....	72
5.2.1 Τι είναι τα ηλεκτρομαγνητικά κύματα	72
5.2.2 Επιπτώσεις των ηλεκτρομαγνητικών πεδίων στα μόρια	73
5.2.3 Τι συμβαίνει όταν το ανθρώπινο σώμα εκτίθεται σε ηλεκτρομαγνητικά πεδία ραδιοσυχνότητας;	74
5.3.1 Ραδιοκύματα.....	75
5.3.2 Πεδία ραδιοσυχνότητας.....	76
5.3.3 Ποιες είναι οι εφαρμογές των ραδιοκυμάτων;.....	76
5.3.4 Η μη ionίζουσα ακτινοβολία	77
5.3.5 Το ηλεκτρομαγνητικό φάσμα	78
5.4 Τα ασύρματα δίκτυα.....	82
5.4.1 Το εύρος των 2,4GHz.....	82
5.4.2 Επιστημονικές μελέτες και διεθνείς οργανισμοί.....	82
5.4.2.1 Ηλεκτρομαγνητικά κύματα γενικά	83
5.4.2.1.1 National Radiological Protection Board (NRPB)	83
5.4.2.1.2 International Commission on Non-Ionizing Radiation Protection.....	83
5.4.2.1.3 Reflex - Δεκέμβριος του 2004.....	83
5.4.2.1.4 Wiley-Liss Inc.....	84
5.4.2.2 Κινητά τηλέφωνα.....	84
5.4.2.2.1 Σουηδικό Εθνικό Ινστιτούτο Εργασίας	84
5.4.2.2.2 Βρετανοί και Κινέζοι μελετούν τις επιπτώσεις στα παιδιά .	85
5.4.2.2.3 Australian Communications Authority & Radiation.....	85
Protection and Nuclear Safety Agency	85

5.4.2.2.4 National Institute of Environmental Health Sciences	86
5.4.2.2.5 Έρευνα του νοσοκομείου του Birmingham	86
5.4.2.3 Ασύρματα δίκτυα	87
5.4.2.3.1 Federal Communications Commission (FCC)	87
5.4.2.3.2 World Health Organization	87
5.4.2.3.3 National Cancer Institute	87
5.5.1 Πώς ποσοτικοποιείται η ενέργεια των ραδιοκυμάτων;	89
5.5.2 Αποστάσεις Ασφαλείας	89
6.1 Ελληνικό νομοθετικό πλαίσιο για την Η/Μ ακτινοβολία	91
6.2. Ευρωπαϊκή Ένωση - Διεθνώς νομοθετικό πλαίσιο για την Η/Μ ακτινοβολία	93
6.3.1 Πώς έχουν καθοριστεί τα όρια;	94
6.3.2 Πώς διασφαλίζεται η τήρηση των θεσμοθετημένων ορίων;	94
6.3.3 Ποιοι έχουν θέσει τα όρια ασφαλούς έκθεσης; Έχουν επιστημονική βάση;	95

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον Καθηγητή μου κ. Λάμπρο Δρόσο για την εμπιστοσύνη που μου έδειξε δίνοντας μου τη δυνατότητα να εκπονήσω την πτυχιακή μου εργασία στον επιστημονικό τομέα που επιθυμούσα. Επίσης, θα ήθελα να τον ευχαριστήσω για τη διάθεση του να με βοηθήσει και να μου λύσει οποιαδήποτε απορία οποιαδήποτε στιγμή το χρειαζόμουν.

Ένα μεγάλο ευχαριστώ στους φίλους μου, οι οποίοι μου συμπαράσταθηκαν όλο αυτό τον καιρό. Τέλος, θέλω να ευχαριστήσω θερμά την οικογένειά μου για την ηθική και οικονομική συμπαράσταση όχι μόνο κατά τη διάρκεια της εκπόνησης της πτυχιακής μου εργασίας αλλά και καθ' όλη τη διάρκεια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Σε αυτήν την ερευνητική/θεωρητική εργασία παρουσιάζονται τα οφέλη των ασύρματων δικτύων έναντι των ενσύρματων με ενδεικτικά οφέλη την μείωση κόστους και την εγκατάσταση σε περιοχές που η καλωδίωση καθίσταται δύσβατη, η ασφάλεια και οι παράγοντες που πρέπει να ληφθούν υπόψη όσον αφορά τον σχεδιασμό και την εγκατάσταση. Επιπλέον, εμβαθύνεται στην αρχιτεκτονική και το λογισμικό των ασύρματων δικτύων αλλά και της άμεσης συσχέτισης των κεραιών με τα ασύρματα δίκτυα στην μετάδοση του σήματος, όπου και παρουσιάζονται όλοι οι τύποι των κεραιών. Περιγράφονται οι σύνδεσμοι και τα καλώδια που εξυπηρετούν στην επικοινωνία μεταξύ του ασύρματου πομποδέκτη και των κεραιών αλλά και της ιστορίας και της επίδρασης των δικτύων στο εγγύς μέλλον. Εν συνεχεία, σημειώνονται τα θέματα που δημιουργούνται από την ελλειπή ασφάλεια των δικτύων αλλά και η χρησιμότητα του 802.11, WEP και πρωτοκόλλου LEAP στην εμπιστευσιμότητα και την χρήση αλλά και την αμοιβαία επικύρωση μεταξύ του σταθμού και του σημείου πρόσβασης. Επίσης, παρουσιάζονται οι ανιχνευτές εντοπισμού εισβολών και της ασφάλειας των ad hoc δικτύων (δίκτυα που πραγματοποιείται η επικοινωνία μεταξύ κόμβων και σημείων πρόσβασης). Τέλος, περιγράφεται η άμεση επιρροή των ηλεκτομαγνητικών κυμάτων στα μόρια και στον άνθρωπο, τα ραδιοκύματα και η ακτινοβολία, ενώ σημειώνονται έρευνες από ινστιτούτα, οργανισμούς και νοσοκομεία του εξωτερικού. Εν κατακλείδι, αναφέρονται τα νομοθετικά πλαίσια της Ελλάδας και της Ευρωπαϊκής Ένωσης σε σχέση με την ηλεκτρομαγνητική ακτινοβολία καταλήγοντας στο συμπέρασμα ότι η χρησιμότητα των ασύρματων δικτύων είναι κομβική για την ανθρώπινη ζωή με αρκετά οφέλη αλλά και αρνητικές επιρροές στην υγεία του.

In this researched/theoretical diplomatic project are presented the benefits of wireless networks against wired with indicatively benefits the decrease of cost installation and the faciilty that provide in impassable regions that wiring becomes difficult, their security and factors that must be take into account in case of design and establishment.

Furthermore, it deepens in the architecture and the logistics of wireless networks and the direct correlation of the antennas and wireless networks in the transmission of signal whereas all the types of antennas are being presented. A description of links and cables take part that serve the communication between the wireless transceiver and the antennas but also the history and the influence of network in the near futute.

Later, issues that resulted from the deficient security of network are noted but also the usefulness of 802.11, WEP and LEAP protocol in their confidentiality and use, and the mutual validation of station and access point. Also, the detection mode of the intruders and the security of ad hoc network are being presented (network that the communication between the nodes and access points take place). Last but not least, the direct influence of the electormagnetic waves is being described in the molecule and human being, the radiowaves and radiation, researches from instiues, organizations and hospitals of abroad are listed. In conclusion, the legislative framework of Greece and European union are mentioned because of their revelance with the electormagnetic radiance ending up with the conclusion that the usefulness of wireless networks is nodal for humans life with benefits but also negative influence in his healthness.

Κεφάλαιο 1ο

1.1 Τα οφέλη της ασύρματης δικτύωσης

Η εμφάνιση και η συνεχής αύξηση των ασύρματων δικτύων οδηγούνται από την ανάγκη να ελαττωθούν οι δαπάνες που συνδέονται με τις υποδομές δικτύων και να υποστηριχθούν οι κινητές εφαρμογές δικτύωσης που προσφέρουν τα κέρδη στην αποδοτικότητα διαδικασίας, την ακρίβεια, και τις χαμηλότερες επιχειρησιακές δαπάνες. Τα εξής τμήματα εξηγούν την κινητικότητα και τα οφέλη οικονομιών της ασύρματης δικτύωσης.

1.1.1 Δυνατότητα κίνησης

Η ασύρματη δικτύωση παρέχει στους χρήστες τη δυνατότητα επικοινωνίας χρησιμοποιώντας μια συσκευή, όπως ένας φορητός υπολογιστής ή ένας συλλέκτης στοιχείων. Πολλές εργασίες απαιτούν από τους εργαζομένους να κινούνται συνεχώς, όπως οι υπάλληλοι καταλόγων, εργαζόμενοι υγειονομικής περίθαλψης, αστυνομικοί, με ειδική ανάγκη-προσοχής. Φυσικά, τα δίκτυα καλωδιώσεων απαιτούν ένα φυσικό μέσο μεταξύ του τερματικού σταθμού του χρήστη και των πόρων του δικτύου, το οποίο καθιστά την πρόσβαση σε αυτούς τους πόρους αδύνατη αν περιπλανάται ο χρήστης μέσα στο κτήριο ή αλλού.

Οι κινητές εφαρμογές που απαιτούν την ασύρματη δικτύωση περιλαμβάνουν εκείνους που εξαρτώνται από την σε πραγματικό χρόνο πρόσβαση στα στοιχεία που αποθηκεύονται συνήθως στις κεντρικές βάσεις δεδομένων. Εάν η εφαρμογή σας απαιτεί οι κινητοί χρήστες να γνωρίζουν αμέσως τις αλλαγές που γίνονται στα δεδομένα, ή εάν οι πληροφορίες που εισάγονται στο σύστημα πρέπει αμέσως να είναι διαθέσιμες σε άλλα, έχουμε μια καθορισμένη ανάγκη για την ασύρματη δικτύωση. Για ακριβή και αποδοτικά συστήματα αποτύπωσης τιμών, παραδείγματος χάριν, πολλά λιανικά καταστήματα χρησιμοποιούν τα ασύρματα δίκτυα για να διασυνδέσουν τους φορητούς ανιχνευτές και τους εκτυπωτές κώδικα φραγμών στις βάσεις δεδομένων που έχουν τις πληροφορίες τρεχουσών τιμών. Αυτό επιτρέπει την εκτύπωση της σωστής τιμής στα προϊόντα, διαδικασία που καθιστά και τον πελάτη και τον ιδιοκτήτη μιας επιχείρησης πιο ικανοποιημένους.

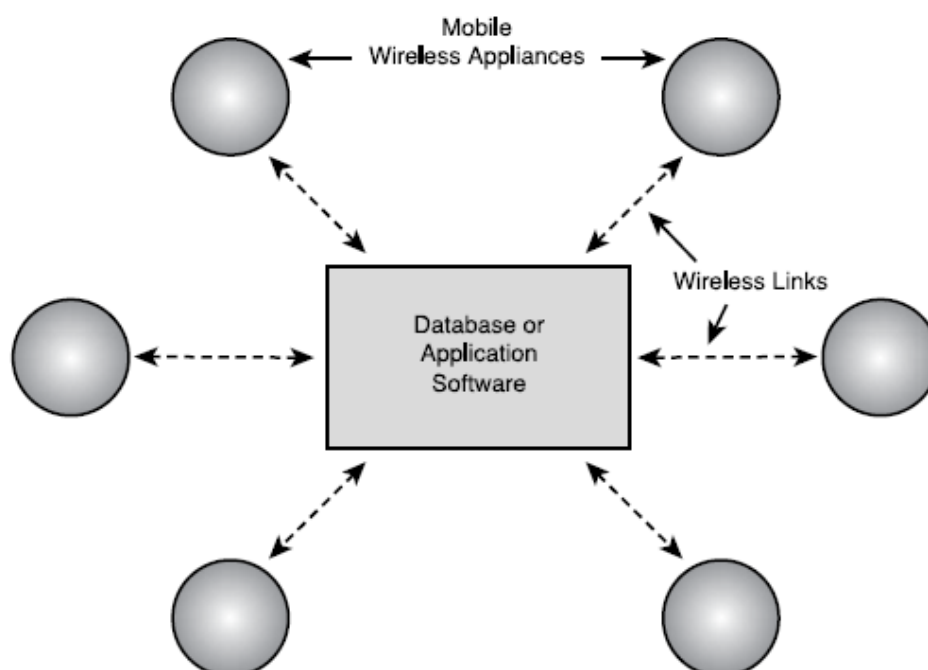
Ένα άλλο παράδειγμα της χρήσης της ασύρματης δικτύωσης είναι στον αγώνα αυτοκινήτων. Στους αγώνες Formula 1 έχουν δημιουργήσει εξελιγμένα συστήματα αποκτήσεων πληροφοριών που ελέγχουν τα διάφορα επί του σκάφους συστήματα στο αυτοκίνητο. Όταν τα αυτοκίνητα έρχονται γύρω από τη διαδρομή και περνούν τις αντίστοιχες ομάδες στο κοίλωμα, αυτές οι πληροφορίες μεταφορτώνονται σε έναν

κεντρικό υπολογιστή, με αυτόν τον τρόπο επιτρέπουν τη σε πραγματικό χρόνο ανάλυση της απόδοσης του αυτοκινήτου (**Σχήμα 1.1**).

Όλες οι κινητές εφαρμογές δεν απαιτούν την ασύρματη δικτύωση. Εντούτοις μερικές φορές δεν υπάρχει άμεση ανάγκη για πρόσβαση σε πραγματικό χρόνο στις πληροφορίες. Εάν τα στοιχεία της εφαρμογής μπορούν να αποθηκευτούν στη συσκευή του χρήστη, και οι αλλαγές στα στοιχεία δεν είναι σημαντικές, το συμπληρωματικό κόστος του ασύρματου υλικού δικτύων μπορεί να μην παρέχει αρκετά οφέλη για να δικαιολογήσει την πρόσθετη δαπάνη. Ας μην ξεχνούμε όμως ότι τα ασύρματα δίκτυα μπορούν να καλύψουν και άλλες ανάγκες που μπορεί να προκύψουν.

1.1.2 Μείωση κόστους

Λόγω της έλλειψης ενός καλωδίου μεταξύ της συσκευής του χρήστη και ενός κεντρικού υπολογιστή, τα ασύρματα δίκτυα χαρακτηρίζονται από μείωση στις δαπάνες δικτύωσης. Τα εξής τμήματα εξηγούν τα οφέλη και τη σχετική μείωση κόστους τους χρησιμοποιήσης των ασύρματων δικτύων.

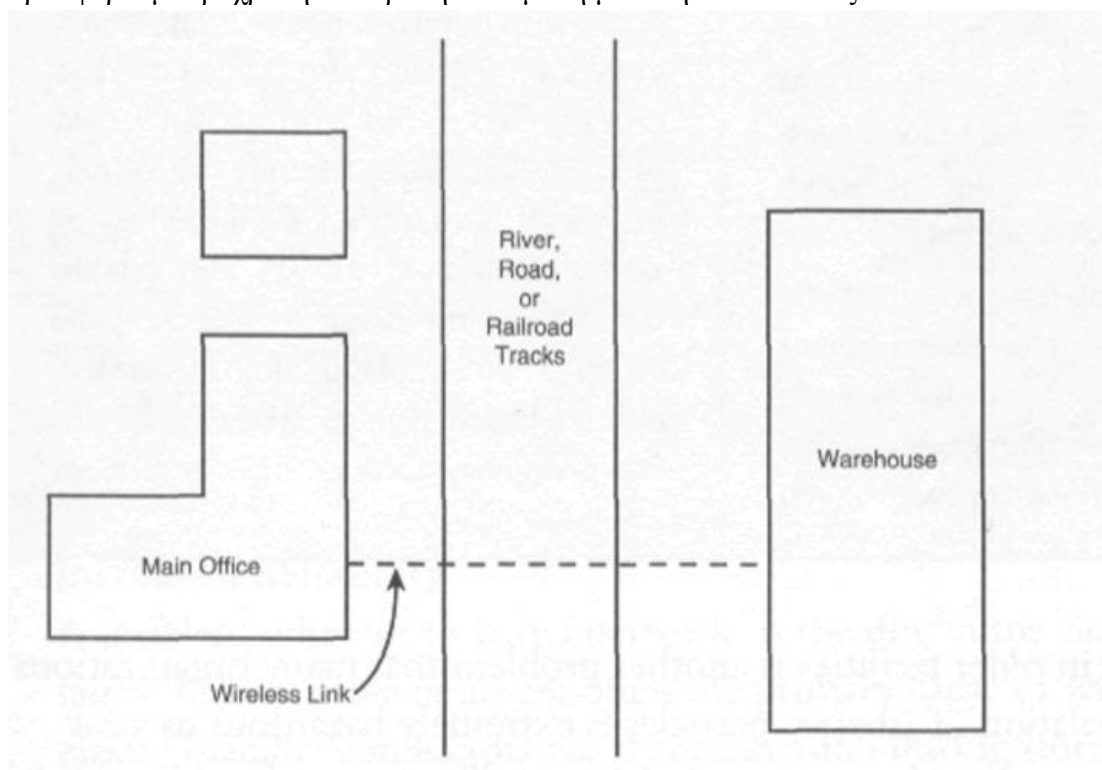


Σχήμα 1.1. Ένα ασύρματο δίκτυο παρέχει πρόσβαση στα δεδομένα σε πραγματικό χρόνο.

1.1.3 Εγκατάσταση σε περιοχές που καλωδιώνονται δύσκολα.

Η εφαρμογή των ασύρματων δικτύων προσφέρει πολλή σημαντική μείωση κόστους κατά την εγκατάσταση του εξοπλισμού στις περιοχές όπου είναι δύσκολο να τοποθετηθούν καλώδια. Εάν οι ποταμοί, οι αυτοκινητόδρομοι, ή άλλα φυσικά εμπόδια αποκόπτουν τη δικτύωση των κτιρίων που επιθυμούμε, μια ασύρματη λύση μπορεί να είναι πιο οικονομική από το να εγκαταστήσουμε το φυσικό καλώδιο ή να μισθώσουμε κυκλώματα επικοινωνίας, όπως υπηρεσία T1 ή γραμμές των 56 Kbps. Αρκετές εταιρείες ξοδεύουν χιλιάδες ή ακόμα και τα εκατομμύρια δολάρια για να εγκαταστήσουν φυσικές συνδέσεις με τις κοντινές εγκαταστάσεις.

Εάν υφίστανται προβλήματα εγκατάστασης αυτού του είδους η ασύρματη δικτύωση μπορεί να θεωρηθεί ως εναλλακτική λύση. Η δημιουργία υποδομής ασύρματης δικτύωσης σε αυτές τις καταστάσεις κοστίζει αρκετές χιλιάδες ευρώ αλλά προσφέρει μακρόχρονη απόσβεση και άμεση μείωση του κόστους.



Σχήμα 1.2. Τα ασύρματα δίκτυα παρέχουν οικονομικές λύσεις σε περιπτώσεις που είναι αδύνατη η καλωδίωση.

Ο αμιάντος που βρίσκεται σε παλαιότερες εγκαταστάσεις είναι ένα άλλο πρόβλημα που πολλές εταιρείες αντιμετωπίζουν. Η εισπνοή των μορίων αμιάντου είναι εξαιρετικά επικίνδυνη και επομένως θα πρέπει να ληφθεί μεγάλη προσοχή κατά την εγκατάσταση των καλωδίων του δικτύου σε αυτές τις περιοχές. Η λήψη των απαραίτητων προφυλάξεων, οι οποίες είναι αναγκαίες κατά την εγκατάσταση των καλωδίων σε αυτά τα κτίρια μπορεί να κάνουν το κόστος απαγορευτικό.

Κάποιοι οργανισμοί αφαιρούν τον αμιάντο, καθιστώντας το ασφαλές να εγκαταστήσει την καλωδίωση. Αυτή η διαδικασία είναι πολύ ακριβή επειδή θα πρέπει να προστατευτούν οι ένοικοι από την εισπνοή μορίων αμιάντου που ταράσσονται κατά τη διάρκεια της αφαίρεσης. Το κόστος αφαίρεσης του αμιάντου που καλύπτει

μικρές επιφάνειες των σκαλοπατιών μπορεί να κοστίζει δεκάδες χιλιάδων δολάρια. Προφανώς, το πλεονέκτημα της ασύρματης δικτύωσης στα κτήρια που έχουν αμιάντο είναι ότι μπορεί να αποφευχθεί η διαδικασία αφαίρεσης αμιάντων, με συνέπεια την τεράστια μείωση του κόστους.

Σε μερικές περιπτώσεις, είναι αδύνατο να εγκατασταθούν καλώδια. Μερικοί δήμοι, παραδείγματος χάριν, έχουν στη διάθεση τους παλαιά και ιστορικά κτίρια. Αυτό θα μπορούσε να περιορίσει τη διάτρηση των τοίχων κατά τη διάρκεια της εγκατάστασης του δικτύου καλωδίων. Σε αυτήν την κατάσταση, ένα ασύρματο δίκτυο μπορεί να είναι η μόνη λύση. Οι περιορισμοί προτεραιότητας μέσα στις πόλεις και τους νομούς μπορούν επίσης να εμποδίσουν το σκάψιμο των τάφρων στο έδαφος για να βάλουν την οπτική ίνα για τη διασύνδεση των δικτυωμένων περιοχών. Πάλι σε αυτήν την κατάσταση, ένα ασύρματο δίκτυο αποτελεί την καλύτερη εναλλακτική λύση.

1.1.4 Αυξανόμενη αξιοπιστία

Ένα πρόβλημα έμφυτο στα συνδεδεμένα με καλώδιο δίκτυα είναι ο χρόνος διακοπής που προκύπτει από τα ελαττώματα καλωδίων. Στην πραγματικότητα, τα ελαττώματα καλωδίων είναι συχνά η κυρίαρχη αιτία του χρόνου διακοπής συστημάτων. Η υγρασία διαβρώνει τους μεταλλικούς αγωγούς μέσω της παρείσφρησης ύδατος κατά τη διάρκεια των θυελλών και της τυχαίας έκχυσης ή της διαρροής των υγρών. Με τα συνδεδεμένα με καλώδιο δίκτυα, οι χρήστες ενδέχεται να σπάσουν τους συνδετήρες δικτύων κατά την προσπάθεια να αποσυνδεθεί το PC τους από το δίκτυο για να το μεταφέρουν σε διαφορετικές θέσεις. Οι ατελείς συναρμογές καλωδίων μπορούν να προκαλέσουν τις αντανάκλασεις σημάτων που οδηγούν σε σφάλματα μετάδοσης. Η τυχαία κοπή καλωδίων μπορεί να θέσει αμέσως ένα δίκτυο εκτός λειτουργίας. Τα καλώδια και οι συνδετήρες μπορούν εύκολα να σπάσουν μέσω της κακής χρήσης και ακόμη και της κανονικής χρήσης. Αυτά τα προβλήματα παρεμποδίζουν τη δυνατότητα των χρηστών να χρησιμοποιήσουν τους πόρους δικτύων, προκαλώντας πονοκέφαλο στους διαχειριστές δικτύων. Ένα πλεονέκτημα της ασύρματης δικτύωσης προκύπτει από τη χρήση λιγότερου καλωδίου. Αυτό μειώνει το χρόνο διακοπής του δικτύου και των δαπανών που συνδέονται με την αντικατάσταση των καλωδίων.

1.1.5 Μειωμένος χρόνος εγκατάστασης

Η εγκατάσταση της καλωδίωσης είναι συχνά μια χρονοβόρα δραστηριότητα. Για την περίπτωση των τοπικών δικτύων, οι τεχνικοί θα πρέπει να εγκαταστήσουν ομοαξονικά καλώδια ή καλώδια UTP μέσω ειδικών διόδων ανάμεσα στους τοίχους. Ακόμη θα πρέπει να τοποθετήσουν τις κατάλληλες εξόδους δικτύων ούτως ώστε να είναι εφικτή η σύνδεση. Αυτοί οι στόχοι μπορούν να πάρουν αρκετές ημέρες ή

εβδομάδες, ανάλογα με το μέγεθος της εγκατάστασης. Η εγκατάσταση της οπτικής ίνας μεταξύ των κτηρίων μέσα στην ίδια γεωγραφική περιοχή περιλαμβάνει το σκάψιμο των τάφρων για την τοποθέτηση της ίνας ή το τράβηγμα της ίνας μέσω ενός υπάρχοντος αγωγού. Θα χρειαστούν εβδομάδες ή ενδεχομένως μήνες για να ληφθούν οι εγκρίσεις εγκατάστασης και να σκαφτεί το έδαφος και η άσφαλτος για την εγκατάσταση των καλωδίων .

Η επέκταση των ασύρματων δικτύων μειώνει πολύ την ανάγκη για την εγκατάσταση καλωδίων, που καθιστά το δίκτυο διαθέσιμο προς χρήση πολύ πιο σύντομα. Επομένως, πολλές χώρες που στερούνται υποδομής δικτύων έχουν στραφεί στην ασύρματη δικτύωση ως μέθοδο για τη διασύνδεση υπολογιστών χωρίς τη δαπάνη και το χρόνο που συνδέονται με την εγκατάσταση των φυσικών μέσων.

1.1.6 Μακροπρόθεσμη μείωση κόστους

Οι επιχειρήσεις αναδιοργανώνονται, με συνέπεια την κυκλοφορία των ατόμων, τα νέα σχέδια ορόφων, τα χωρίσματα γραφείων, και άλλες ανακαινίσεις. Αυτές οι αλλαγές αφορούν συχνά το δίκτυο, αναλαμβάνοντας και την εργασία και τις υλικές δαπάνες. Σε μερικές περιπτώσεις, η επανεγκατάσταση καλωδίωσης απαιτεί πολύ σημαντικές δαπάνες των οργανωτικών αλλαγών, ειδικά με τα μεγάλα επιχειρηματικά δίκτυα. Ένα ποσοστό αναδιοργάνωσης 15 τοις εκατό κάθε έτος μπορεί να οδηγήσει στις ετήσιες δαπάνες επανασχηματισμού τόσο υψηλές όσο €250,000 για τα δίκτυα που έχουν 6.000 διασυνδεδεμένες συσκευές. Το πλεονέκτημα της ασύρματης δικτύωσης είναι πάλι βασισμένο στην έλλειψη καλωδίου: Είναι δυνατό να κινηθεί η σύνδεση δικτύων με την επανεντόπιση του PC ενός υπαλλήλου.

1.2 Αγορές και εφαρμογές ασύρματων δικτύων

1.2.1 Γενικά

Η ασύρματη δικτύωση βρίσκει εφαρμογή σε όλες τις βιομηχανίες. Μπορεί να εφαρμοστεί όταν είναι απαραίτητη η χρήση φορητών υπολογιστών ή όταν δεν είναι εφικτή η εγκατάσταση των φυσικών μέσων. Τέτοια δικτύωση είναι ιδιαίτερα χρήσιμη όταν πρέπει να επεξεργαστούν οι υπάλληλοι τις πληροφορίες επί τόπου, άμεσα μπροστά από τους πελάτες, μέσω των ηλεκτρονικών μορφών και των διαλογικών επιλογών. Η ασύρματη δικτύωση καθιστά πιθανή την τοποθέτηση των φορητών υπολογιστών στα χέρια των κινητών εργαζομένων πρώτης γραμμής όπως οι γιατροί, οι νοσοκόμες, οι υπάλληλοι αποθηκών εμπορευμάτων, οι επιθεωρητές, οι πράκτορες ακίνητων περιουσιών, και ασφαλιστών. Η σύζευξη των φορητών συσκευών με την ασύρματη σύνδεση σε μια κοινή βάση δεδομένων και συγκεκριμένες εφαρμογές, όπως το σχήμα επεξηγεί, ικανοποιεί τις ανάγκες για δυνατότητα μετακίνησης, αποβάλλει τη γραφική εργασία, μειώνει τα λάθη και τις δαπάνες διαδικασίας, και βελτιώνει την αποδοτικότητα. Η εναλλακτική λύση αυτού, που πολλές επιχειρήσεις υιοθετούν ακόμα σήμερα, χρησιμοποιεί τη γραφική εργασία για να ενημερώσει τα αρχεία, τους καταλόγους της παραγωγικής διαδικασίας, και την κοινή χρήση αρχείων. Αυτή η χειρωνακτική μέθοδος επεξεργάζεται τις πληροφορίες αργά, δημιουργεί περιττά στοιχεία, και υπόκειται σε λάθη που προκαλούνται από τη δυσανάγνωστη γραφή. Η ασύρματη προσέγγιση υπολογιστών που χρησιμοποιεί μια κεντρική βάση δεδομένων είναι σαφώς ανώτερη.

1.2.2 Λιανικές Πωλήσεις

Τα καταστήματα λιανικής πρέπει να ορίσουν, τιμή, να πωλήσουν, και να κρατήσουν τους καταλόγους των εμπορευμάτων. Ένα ασύρματο δίκτυο σε ένα λιανικό περιβάλλον επιτρέπει στους υπαλλήλους και το προσωπικό αποθηκών να εκτελέσει τις λειτουργίες τους άμεσα από το τμήμα πωλήσεων.

Οι πωλητές είναι εξοπλισμένοι με light pen που είναι συνδεδεμένο με υπολογιστή ή μια μικρή συσκευή υπολογισμού με την ικανότητα ανάγνωσης και εκτύπωσης bar-codes, με την ασύρματη σύνδεση με τη βάση δεδομένων του καταστήματος. Είναι έπειτα ικανοί να ολοκληρώσουν τις συναλλαγές όπως είναι η τιμολόγηση, η σήμανση της συσκευασίας, ο ορισμός ενεργειών για ομάδες προϊόντων, και η λήψη του καταλόγου από οπουδήποτε μέσα στο κατάστημα.

Κατά την εκτύπωση των ετικετών τιμών που θα επισυναφθούν στο προϊόν ή τα ράφια, οι λιανοπωλητές χρησιμοποιούν συχνά έναν φορητό ανιχνευτή και έναν

εκτυπωτή κώδικα γραμμών για να παράγουν το απαιτούμενο bar-code που κωδικοποιείται ή και τις ανθρώπινες αναγνώσιμες ετικέτες. Μια βάση δεδομένων ή ένα αρχείο περιέχει τις πληροφορίες για τις τιμές είτε τοποθετημένες στη φορητή συσκευή, αποκαλούμενη συχνά μια συσκευή batch, είτε στον κεντρικό υπολογιστή που βρίσκεται κάπου στο κατάστημα. Κατά δεσμίδες, ο υπάλληλος τιμών ανιχνεύει τον bar-code (χαρακτηριστικά το προϊόν κώδικας) τοποθετημένο στο στοιχείο ή την άκρη ραφιών, τα προγράμματα εφαρμογών χρησιμοποιούν τον κώδικα προϊόντων για να ανατρέξουν τη νέα τιμή, και έπειτα ο εκτυπωτής παράγει μια νέα ετικέτα που ο υπάλληλος επισυνάπτει στο στοιχείο.

Σε μερικές περιπτώσεις, ο batch-based scanner ή εκτυπωτής έχει αρκετή μνήμη για να αποθηκεύσει όλες τις πληροφορίες για τις τιμές που απαιτούνται για να εκτελέσουν αποτελεσματικά τη λειτουργία τιμολόγησης καθ' όλη τη διάρκεια μιας τιμολόγησης διαφορετικών προϊόντων ή ακόμη και μιας ολόκληρης ημέρας. Αυτή η κατάσταση έχει νόημα εάν ενημερώνονται οι πληροφορίες για τις τιμές στη βάση δεδομένων μία φορά την ημέρα, κυρίως κατά τη διάρκεια της νύχτας. Οι υπάλληλοι φορτώνουν τα στοιχεία προς την συσκευή στην αρχή της διαδρομής τους. Στη συνέχεια και κατά την διάρκεια της διαδρομής σε όλο το κατάστημα, διενεργεί διατίμηση σε όλα τα προϊόντα του καταστήματος. Εάν η μνήμη στη συσκευή δεν είναι αρκετά μεγάλη να αποθηκεύσει όλα τα στοιχεία, ένα ασύρματο δίκτυο είναι πιθανώς απαραίτητο. Εάν η φορητή μονάδα είναι εξοπλισμένη με μια ασύρματη σύνδεση δικτύων, τα στοιχεία μπορούν να αποθηκευτούν στην μνήμη ενός συγκεντρωτικού υπολογιστή ή του κεντρικού υπολογιστή και να προσπελαστούν κάθε φορά που ανιχνεύεται το bar-code του προϊόντος. Επιπλέον, προστιθέμενη αξία στην ασύρματη δικτύωση προσθέτει το γεγονός ότι δεν καταναλώνεται χρόνος για μεταφόρτωση δεδομένων.

1.2.3 Αποθήκες εμπορευμάτων

Το προσωπικό που είναι υπεύθυνο στην αποθήκη των εμπορευμάτων πρέπει να είναι σε θέση να διαχειριστεί τη λειτουργία της αποθήκης. Η διαδικασία αυτή απαιτεί από τον εργαζόμενο να κινείται συνεχώς στο χώρο εργασίας και να βρίσκεται μακριά από τους καταλόγους των προϊόντων. Η διαδικασία διαχείρισης μιας αποθήκης εμπορευμάτων δημιουργεί συνήθως ένα εντατικό και χρονοβόρο περιβάλλον. Μια εταιρεία μπορεί να αποβάλει την γραφειοκρατία, να ελαττώσει τα λάθη, και να μειώσει τον απαραίτητο χρόνο που απαιτείται για την διακίνηση προϊόντων. Αυτό θα επιτευχθεί με τον εφοδιασμό των υπάλληλων της αποθήκης με μια φορητή συσκευή υπολογισμού και με έναν ανιχνευτή bar-code που διασυνδέεται μέσω ενός ασύρματου δικτύου με τη βάση δεδομένων που περιέχει τους καταλόγους εμπορευμάτων της αποθήκης.

Κατά τη διαδικασία καταχώρησης του κόστους των προϊόντων που εισάγονται στην αποθήκη, ο υπάλληλος ανιχνεύει το bar-code του αγαθού, μπορεί να το

εντοπίζει μέσα στον κατάλογο και να εισάγει επιπρόσθετες πληροφορίες στη βάση δεδομένων με τη βοήθεια ενός μικρού αριθμητικού πληκτρολογίου που είναι ενσωματωμένο στην φορητή συσκευή. Το σύστημα είναι σε θέση να ενημερώσει τον χρήστη σε ποιο σημείο της αποθήκης πρέπει να τοποθετηθούν τα προϊόντα. Ο υπάλληλος είναι σε θέση να εκτυπώσει οτιδήποτε στοιχεία των προϊόντων κρίνει απαραίτητα. Η βάση δεδομένων ενημερώνεται συνεχώς σε πραγματικό χρόνο. Μέσα στους καταλόγους της βάσης δεδομένων αποτυπώνεται με ακρίβεια η κίνηση των προϊόντων στην αποθήκη. Έχοντας στη διάθεση του και την παραμικρή λεπτομέρεια ο υπάλληλος είναι σε θέση να συντάξει ακριβείς καταλόγους.

Με την παραλαβή μιας παραγγελίας προς αποστολή, δημιουργείται αυτόματα ο κατάλογος από τα προϊόντα που την αποτελούν. Ο υπάλληλος μπορεί να δει αυτόν τον κατάλογο μέσω της φορητής συσκευής, να εντοπίζει τα προϊόντα που απαιτούνται καθώς επίσης και τις θέσεις που βρίσκονται μέσα στην αποθήκη ούτως ώστε να ετοιμαστεί η παραγγελία. Για να εκτελεστούν οι παραπάνω λειτουργίες, είναι απαραίτητη η χρήση των ασύρματων δικτύων. Με τη συνδρομή τους καθίσταται δυνατή η, σε πραγματικό χρόνο, πρόσβαση στα στοιχεία της κεντρικής βάσης δεδομένων.

1.2.4 Υγειονομική περίθαλψη

Τα κέντρα υγειονομικής περίθαλψης, όπως τα νοσοκομεία και τα ιδιωτικά ιατρεία, πρέπει να διατηρούν ακριβή αρχεία. Ένα απλό λάθος μπορεί να κοστίσει τη ζωή κάποιου. Κατά συνέπεια, οι γιατροί και οι νοσοκόμες πρέπει προσεκτικά να καταγράψουν τα αποτελέσματα των εξετάσεων, τα στοιχεία των ασθενών, τις φαρμακευτικές αγωγές, και τις χειρουργικές διαδικασίες. Αυτή η γραφική εργασία επιβαρύνει πάρα πολύ το προσωπικό υγειονομικής περίθαλψης, καθώς καταναλώνει το 50-70 τοις εκατό του χρόνου τους.

Οι γιατροί και οι νοσοκόμες είναι επίσης εξαιρετικά δραστήριοι, πηγαίνοντας από δωμάτιο σε δωμάτιο φροντίζοντας τους ασθενείς. Το ιατρικό προσωπικό καταγράφει τα στοιχεία του ασθενή, διαβάζει το ιατρικό του ιστορικό, εισάγει νέα δεδομένα και επιβεβαιώνει την χορήγηση της αγωγής.

Εάν προμηθευθεί ο κάθε γιατρός και νοσοκόμος με μια ασύρματη φορητή συσκευή και ένα light-pen, η οποία θα είναι συνδεδεμένη με τη βάση δεδομένων μέσω ασύρματου δικτύου, τότε η χρήση γραφικής ύλης θα είναι περιττή. Η παραπάνω διαδικασία (προβολή, επεξεργασία, αποθήκευση στοιχείων του ασθενή) θα γίνεται ηλεκτρονικά και η αποθήκευση θα γίνεται με την βοήθεια του ασύρματου δικτύου στη βάση δεδομένων όπου βρίσκονται όλες οι χρήσιμες πληροφορίες για τους ασθενείς. Με αυτό τον τρόπο αυξάνεται η ταχύτητα και η ακρίβεια της υγειονομικής περίθαλψης. Ένας γιατρός που φροντίζει κάποιον στο νοσοκομείο, μπορεί να αποστείλει μια εντολή για μια εξέταση αίματος διαμέσου ενός φορητού υπολογιστή. Το εργαστήριο θα λάβει τη διαταγή ηλεκτρονικά και θα αποστείλει έναν τεχνικό

εργαστηρίων για να πάρει αίμα από τον ασθενή. Το εργαστήριο θα πραγματοποιήσει τις εξετάσεις που ζητούνται από το γιατρό και θα εισαγάγει τα αποτελέσματα στο ηλεκτρονικό ιατρικό αρχείο του ασθενή. Ο γιατρός μπορεί έπειτα να ελέγξει τα αποτελέσματα μέσω της φορητής συσκευής από οπουδήποτε στο νοσοκομείο.

Μια άλλη εφαρμογή για τα ασύρματα δίκτυα στα νοσοκομεία είναι ο εντοπισμός των φαρμακευτικών ειδών. Η χρήση των κινητών φορητών συσκευών εκτύπωσης και ανίχνευσης bar-code αυξάνει εντυπωσιακά την αποδοτικότητα και την ακρίβεια όλων των συναλλαγών φαρμάκων, όπως η λήψη, η επιλογή, η διανομή, ο κατάλογος που παίρνουν, και ο εντοπισμός των ημερομηνιών λήξης φαρμάκων. Επιπλέον εξασφαλίζει ότι το προσωπικό των νοσοκομείων μπορεί να χορηγήσει το σωστό φάρμακο στο σωστό πρόσωπο εγκαίρως. Αυτό δεν θα ήταν δυνατό χωρίς τη δυνατότητα ενός ασύρματου δικτύου να υποστηρίζει μια κεντρική βάση δεδομένων και κινητές συσκευές συλλογής δεδομένων.

1.2.5 Ακίνητη περιουσία

Οι πωλητές ακίνητων περιουσιών εκτελούν ένα σημαντικό τμήμα της εργασίας τους μακριά από το γραφείο, μιλώντας συνήθως με τους πελάτες στην ιδιοκτησία που πωλείται ή που νοικιάζεται. Πριν φύγουν από το γραφείο, οι πωλητές επιλέγουν μερικές περιοχές για να παρουσιάσουν σε έναν πελάτη, τυπώνουν τις πληροφορίες υπηρεσιών λιστών (MLS) που περιγράφουν την ιδιοκτησία, και έπειτα την κίνηση σε κάθε θέση με τον πιθανό αγοραστή. Εάν ο πελάτης είναι ανικανοποίητος με εκείνο τον κύκλο των περιοχών, ο πράκτορας ακίνητων περιουσιών πρέπει να γυρίσει πίσω στο γραφείο και να χρησιμοποιήσει περισσότερες λίστες. Ακόμα κι αν ο πελάτης αποφασίζει να αγοράσει την ιδιοκτησία, πρέπει και οι δύο να επιστρέψουν στο γραφείο ακίνητων περιουσιών για να τελειώσουν τη γραφική εργασία που ολοκληρώνει την πώληση.

Η ασύρματη δικτύωση καθιστά την πώληση της ακίνητης περιουσίας αποδοτικότερη. Ο πράκτορας ακίνητων περιουσιών μπορεί να χρησιμοποιήσει έναν υπολογιστή μακριά από το γραφείο για να έχει πρόσβαση σε ένα ασύρματο αρχείο MLS. Η ομάδα κινητής δικτύωσης της IBM και η συνεργασία λογισμικού της Αμερικής, παραδείγματος χάριν, καθιστούν τις ασύρματες πληροφορίες MLS διαθέσιμες στους πράκτορες ακίνητων περιουσιών που έχουν πρόσβαση στις πληροφορίες για ένα σύνολο στοιχείων, όπως οι περιγραφές, που παρουσιάζουν τις οδηγίες, τα ανεξόφλητα δάνεια και την τιμολόγηση. Ένας πράκτορας μπορεί επίσης να χρησιμοποιήσει έναν φορητό υπολογιστή και έναν εκτυπωτή για να παράγει τις συμβάσεις και τις εφαρμογές δανείου για την υπογραφή στο σημείο της πώλησης.

1.2.6 Φιλοξενία

Η ανάγκη εξυπηρέτησης των πελατών στις ξενοδοχειακές μονάδες τόσο στα δωμάτια όσο και στον περιβάλλοντα χώρο του ξενοδοχείου καθιστά απαραίτητη την εγκατάσταση ενός ασύρματου δικτύου. Τα εστιατόρια πρέπει να γνωρίζουν τα ονόματα και τον αριθμό των ανθρώπων που περιμένουν στην είσοδο, τις διαθέσιμες θέσεις που υπάρχουν στο εστιατόριο, και τις παραγγελίες ποτών και τροφίμων που βρίσκονται σε εξέλιξη. Το προσωπικό εστιατορίων πρέπει να εκτελέσει αυτές τις δραστηριότητες γρήγορα και ακριβώς για να αποφύγει τους δυσαρεστημένους πελάτες. Η ασύρματη δικτύωση ικανοποιεί αυτές τις ανάγκες πολύ καλά.

Οι ασύρματοι υπολογιστές είναι πολύ χρήσιμοι σε καταστάσεις όπου υπάρχει ένας μεγάλος αριθμός πελατών, όπως ένα εστιατόριο. Παραδείγματος χάριν, κάποιος υπεύθυνος στην είσοδο του εστιατορίου μπορεί να χαιρετήσει τους πελάτες που περιμένουν στην πόρτα και παράλληλα να καταχωρήσει τα ονόματά τους, το μέγεθος της παρέας, και αν προτιμούν να καθίσουν σε μέρος καπνιστών ή όχι, σε μια κοινή βάση δεδομένων μέσω μιας ασύρματης συσκευής. Το γκαρσόν μπορεί έπειτα να ρωτήσει τη βάση δεδομένων και να καθορίσει τη διαθεσιμότητα ενός κατάλληλου τραπέζιου. Εκείνοι που επιτηρούν την κίνηση των τραπεζιών επίσης θα χρησιμοποιούσαν μια ασύρματη συσκευή για να ενημερώσουν τη βάση δεδομένων για να παρουσιάσουν εάν το κάθε τραπέζι είναι κατειλημμένο, καθαρισμένο, ή διαθέσιμο. Μετά από την παραγγελία που θα λάβει ο σερβιτόρος από ένα τραπέζι, διαβιβάζει τη διαταγή στην κουζίνα μέσω της ασύρματης συσκευής, που εξαλείφει την ανάγκη της γραφειοκρατίας που συνήθως ισχύει σε τέτοιου είδους επιχείρησης.

1.2.7 Οργανισμοί κοινής ωφελείας

Οι οργανισμοί κοινής ωφελείας ενεργοποιούν και διατηρούν ένα ιδιαίτερα εκτεταμένο σύστημα που παρέχει ηλεκτρικό ρεύμα και φυσικό αέριο στις βιομηχανίες και τις κατοικίες. Οι οργανισμοί κοινής ωφελείας πρέπει συνεχώς να ελέγχουν τη λειτουργία των ηλεκτρικών γραμμών συστημάτων και αερίου διανομής, και τους μετρητές χρήσης τουλάχιστον μια φορά το μήνα για να υπολογίσουν τους λογαριασμούς. Παραδοσιακά, αυτό σημαίνει ότι ένα πρόσωπο πρέπει να μεταφέρεται από θέση σε θέση, να καταγράφει τις κατοικίες και τις εγκαταστάσεις των επιχειρήσεων, και να εισάγει έπειτα τα στοιχεία σε μια υπηρεσία ή ένα υπολογιστικό κέντρο. Σήμερα, οι οργανισμοί κοινής ωφελείας χρησιμοποιούν τα ασύρματα δίκτυα για να υποστηρίξουν την αυτοματοποίηση της ανάγνωσης μετρητών και του ελέγχου συστημάτων, της εξοικονόμησης του χρόνου και της μείωσης των γενικών εξόδων.

Η εταιρεία παροχής ηλεκτρικής ενέργειας των πόλεων του Κάνσας έχει εγκαταστήσει ένα από τα μεγαλύτερα ασύρματα συστήματα μέτρησης, που εξυπηρετεί περισσότερους από 150.000 πελάτες στο ανατολικό Κάνσας και το δυτικό Μισούρι. Αυτό το σύστημα χρησιμοποιεί μια συσκευή ελέγχου, σε κάθε πελάτη, που

μετράει σε περιοδικές χρονικές στιγμές την κατανάλωση και στέλνει τις πληροφορίες πίσω σε μια βάση δεδομένων που ακολουθεί τα επίπεδα χρήσης και παράλληλα υπολογίζει το λογαριασμό που χρεώνει τον κάθε πελάτη, αποφεύγοντας την ανάγκη για πρόσληψη προσωπικού που θα παρακολουθεί την πορεία των μετρητών.

1.3 Παράγοντες σχεδίασης ασύρματων δικτύων

1.3.1 Γενικά

Τα οφέλη ενός ασύρματου δικτύου γίνονται δεκτά από τις επιχειρήσεις και τις οργανώσεις με μεγάλη ευκολία. Οι διευθυντές και οι μηχανικοί δικτύων πρέπει να γνωρίζουν, εντούτοις, τις ακόλουθες παραμέτρους σχεδίασης που σχετίζονται με την εφαρμογή και τη χρήση της ασύρματης δικτύωσης:

- Παρεμβολή ραδιοσημάτων
- Διαχείριση ισχύος
- Διαλειτουργικότητα συστημάτων
- Ασφάλεια δικτύων
- Προβλήματα σύνδεσης
- Ζητήματα εγκατάστασης
- Κίνδυνοι υγείας

1.3.2 Παρεμβολή ραδιοσημάτων

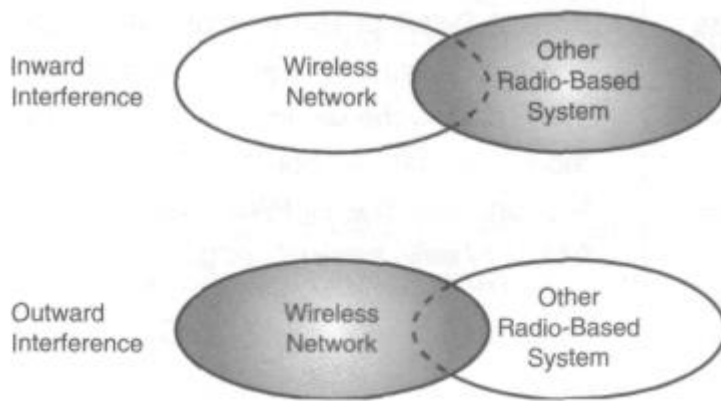
Η λειτουργία και τα σήματα των ραδιοφώνων και συστημάτων εκπομπής laser μέσω του αέρα καθιστά τα ασύρματα συστήματα ευάλωτα στον ατμοσφαιρικό θόρυβο και τις μεταδόσεις από άλλα συστήματα.

Επιπλέον, τα ασύρματα δίκτυα μπορούν να παρεμποδίσουν άλλα κοντινά ασύρματα δίκτυα καθώς επίσης και τον εξοπλισμό ραδιοκυμάτων. Όπως φαίνεται στο **σχήμα 1.3**, η παρέμβαση μπορεί να είναι εσωτερική και εξωτερική.

1.3.3 Εσωτερική παρέμβαση

Ένα ασύρματο τοπικό δίκτυο μπορεί να υποστεί εσωτερική παρέμβαση είτε από τις αρμονικές της μετάδοσης των συστημάτων είτε από άλλα συστήματα που λειτουργούν στην ίδια περιοχή ραδιοσυχνοτήτων. Για παράδειγμα οι φούρνοι μικροκυμάτων λειτουργούν στη ζώνη του S (2,4 GHz) που χρησιμοποιείται από τα ασύρματα LANs για τη μετάδοση δεδομένων.

Αυτά τα σήματα οδηγούν σε καθυστερήσεις μετάδοσης εμποδίζοντας τις μεταδόσεις από τους σταθμούς στο τοπικό LAN. Αυτοί οι τύποι παρεμβάσεων μπορούν να περιορίσουν τις περιοχές στις οποίες μπορεί να επεκταθεί ένα ασύρματο δίκτυο.



Σχήμα 1.3. Οι εσωτερικές και εξωτερικές παρεμβολές εγείρουν πιθανά προβλήματα στα ασύρματα δίκτυα

Η παρέμβαση με τα ασύρματα δίκτυα δεν είναι τόσο κακή όσο αρχικά φαίνεται. Τα συστήματα που χρησιμοποιούν τις δημόσιες ραδιοσυχνότητες ενσωματώνουν τεχνολογικά χαρακτηριστικά τα οποία περιορίζουν σε μεγάλο ποσοστό τα προβλήματα που δημιουργούνται από τις παρεμβολές σημάτων.

Το φάσμα διάδοσης του σήματος λειτουργεί σε ένα μεγάλο εύρος ζώνης και μια πιθανή παρέμβαση θα έχει επιπτώσεις μόνο σε ένα μικρό μέρος του σήματος μετάδοσης πληροφοριών, με συνέπεια την αποφυγή λαθών.

Επομένως οι συσκευές ασύρματης δικτύωσης είναι ιδιαίτερα ανθεκτικές στις παρεμβάσεις. Η παρέμβαση περιορισμένης ζώνης με τις αναλογίες σήματος / παρέμβασης είναι λιγότερο από 10 DB και συνήθως δεν έχει επιπτώσεις σε μια μετάδοση φάσματος διάδοσης. Η παρέμβαση ευρείας ζώνης, μπορεί να έχει καταστρεπτικά αποτελέσματα σε οποιοδήποτε τύπο ασύρματης μετάδοσης. Η αρχική πηγή της ευρείας ζώνης παρέμβασης είναι οι εσωτερικοί φούρνοι μικροκυμάτων που λειτουργούν στη ζώνη 2,4 GHz. Τα κύματα που εκπέμπουν οι φούρνοι μικροκυμάτων αναπτύσσονται στους 2450 MHz. Αυτό έχει σαν αποτέλεσμα να αλλοιώνεται το σήμα των συσκευών ασύρματης δικτύωσης σε απόσταση 25 μέτρων από την πηγή της παρεμβολής. Άλλη παρέμβαση μπορεί να προκύψει από τις μηχανές ανελκυστήρων, τις μηχανές αναπαραγωγής, τον εξοπλισμό προστασίας κλοπής, και τα ασύρματα τηλέφωνα.

1.3.4 Εξωτερική παρέμβαση

Η εσωτερική παρέμβαση αποτελεί μόνο το ήμισυ του προβλήματος. Το άλλο μισό, είναι η εξωτερική παρέμβαση που εμφανίζεται όταν το σήμα ενός ασύρματου δικτύου επηρεάζεται από άλλα συστήματα, όπως παρακείμενα ασύρματα LANs και ο εξοπλισμός ναυσιπλοΐας στα αεροσκάφη. Αυτή η διάσπαση οδηγεί στην απώλεια μερικού ή όλου του συστήματος λειτουργίας. Η παρουσίαση παρεμβολών είναι

σπάνια όταν γίνεται χρήση συσκευών ασύρματου τοπικού LAN που λειτουργούν στις κοινές ζώνες φάσματος. Αυτό συμβαίνει επειδή λειτουργούν με χαμηλή ισχύ (λιγότερο από 1Watt). Τα διαβιβαζόμενα δεδομένα πρέπει να είναι πολύ σύντομα και να λειτουργούν στην ίδια ζώνη.

1.3.5 Τεχνικές για την αποφυγή παρεμβολών

Κατά την εξέταση ύπαρξης παρεμβολών, θα πρέπει να συντονιστεί η λειτουργία των προϊόντων ασύρματης δικτύωσης σε κοινή συχνότητα. Οι κυβερνητικοί οργανισμοί και τα περισσότερα νοσοκομεία απασχολούν τεχνικούς οι οποίοι διαχειρίζονται τις συσκευές διαβίβασης. Ο συντονισμός των συσκευών ασύρματης δικτύωσης συμβάλλει στην αποφυγή πιθανών παρεμβάσεων.

1.3.6 Διαχείριση ισχύος

Εάν γίνεται χρήση φορητού υπολογιστή σε ένα αυτοκίνητο, εκτέλεση και έλεγχος ενός κατάλογου εργασιών σε μια αποθήκη εμπορευμάτων, ή εξέταση ασθενών σε ένα νοσοκομείο, είναι πιθανώς πάρα πολύ δυσλειτουργικό ή ακόμα και αδύνατο να συνδεθεί ο υπολογιστής με μια πρίζα. Επομένως, ο υπολογιστής θα εξαρτάται αποκλειστικά από την μπαταρία του. Το πρόσθετο φορτίο της ασύρματης κάρτας διεπαφών δικτύων (NIC) σε αυτήν την περίπτωση μπορεί να μειώσει σημαντικά το χρονικό διάστημα που μπορεί να είναι διαθέσιμος ενώ υπάρχει περίπτωση να χρειαστεί να ενεργοποιηθεί ο υπολογιστής προτού επαναφορτιστούν οι μπαταρίες. Επομένως ο χρόνος χρήσης του υπολογιστή θα μειωθεί σε λιγότερο από μία ώρα εφ' όσον γίνεται χρήση του δικτύου ή εκτελούνται άλλες λειτουργίες όπως η εκτύπωση.

Για να αντιμετωπίσουν αυτό το πρόβλημα, οι προμηθευτές εφαρμόζουν τις τεχνικές διαχείρισης ισχύος στις ασύρματες κάρτες PCMCIA. Η ασύρματη συσκευή τοπικού LAN του Proxim, RangeLAN2/PCMCIA, παραδείγματος χάριν, μεγιστοποιεί τη συντήρηση ισχύος. Το RangeLAN2 προσαρμόζει γνωρίσματα που βρίσκονται στους περισσότερους φορητούς υπολογιστές. Το Proxim ενσωματώνει δύο τρόπους για να βοηθήσει στη διατήρηση της ισχύος: η μέθοδος της μερικής αδρανοποίησης και η μέθοδος της αδρανοποίησης. Η μέθοδος της μερικής αδρανοποίησης, που είναι η κατάσταση προεπιλογής του προϊόντος, κρατά τη συσκευή ασύρματης δικτύωσης σε κατάσταση αδράνειας και την ενεργοποιεί περιοδικά για να ελέγξει εάν υπάρχουν σε αναμονή οποιαδήποτε μηνύματα σε μια ειδική θυρίδα αποστολής. Αυτός ο τρόπος χρησιμοποιεί μόνο 50 τοις εκατό λιγότερη ενέργεια από τις μπαταρίες. Από την άλλη πλευρά η μέθοδος της αδρανοποίησης αναγκάζει τη συσκευή ασύρματης δικτύωσης να παραμένει σε εφεδρεία. Με άλλα λόγια, η συσκευή ενεργοποιείται μόνο αν είναι απαραίτητο να λάβει ή να αποστείλει δεδομένα.

1.3.7 Διαλειτουργικότητα συστημάτων

Κατά την εγκατάσταση ενός δικτύου ethernet, οι διαχειριστές και οι μηχανικοί του δικτύου μπορούν να χρησιμοποιήσουν NICs από πολλούς προμηθευτές στο ίδιο δίκτυο. Λόγω των IEEE 802,3 προτύπων που διευκρινίζουν τα πρωτόκολλα και τα ηλεκτρονικά χαρακτηριστικά που οι κατασκευαστές πρέπει να ακολουθήσουν για το ethernet, αυτά τα προϊόντα όλα μιλούν ακριβώς την ίδια γλώσσα. Αυτή η ομοιομορφία επιτρέπει την επιλογή των προϊόντων που καλύπτουν σε κάθε περίπτωση τις απαιτήσεις του χρήστη.

Στις μέρες μας, αυτό δεν είναι δυνατό με τα περισσότερα προϊόντα ασύρματης δικτύωσης που κυκλοφορούν στο εμπόριο. Η αγορά προϊόντων ασύρματης δικτύωσης για μια συγκεκριμένη εγκατάσταση, πρέπει να γίνει από ένα μόνο εργοστάσιο παραγωγής. Συμβαίνει συχνά προϊόντα διαφορετικής κατασκευαστικής εταιρείας να μην μπορούν να επικοινωνήσουν μεταξύ τους. Σε αυτή την περίπτωση λέμε ότι έχουμε προβλήματα συμβατότητας μεταξύ συσκευών που προέρχονται από διαφορετικούς προμηθευτές. Μακροπρόθεσμα, τα πρότυπα 802.11 που εγκρίνονται από την IEEE θα αυξήσουν σημαντικά την συμβατότητα.

1.4 Ασφάλεια δικτύων

1.4.1 Γενικά

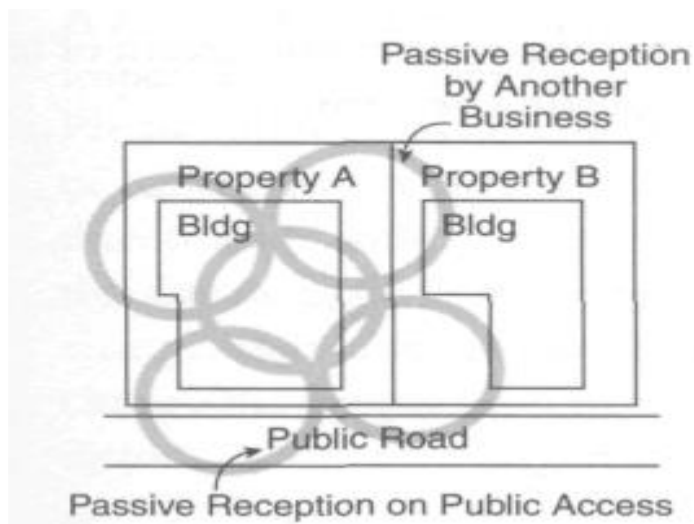
Η ασφάλεια δικτύων αναφέρεται στην προστασία των πληροφοριών και των πόρων από την απώλεια και την ανάρμοστη χρήση. Είναι τα ασύρματα δίκτυα ασφαλή; Μεταξύ των επιχειρήσεων που εξετάζουν την εφαρμογή ενός ασύρματου συστήματος, αυτό είναι μια κοινή και πολύ σημαντική ερώτηση. Για να απαντήσουμε σε αυτήν την ερώτηση, πρέπει να θεωρήσουμε τη λειτουργία ασύρματου δικτύου.

Ένα ασύρματο δίκτυο παρέχει μία δίοδο μετάδοσης δεδομένων, που αποτελείται από ένα μέσο, μια διαδικασία συγχρονισμού, και έναν μηχανισμό έλεγχου λαθών που υποστηρίζει τη ροή των δεδομένων από ένα σημείο σε άλλο. Η λειτουργία ενός ασύρματου δικτύου αντιστοιχεί στα χαμηλότερα επίπεδα της δικτυακής αρχιτεκτονικής και δεν περιλαμβάνει άλλες λειτουργίες, όπως οι υπηρεσίες αποκατάστασης σύνδεσης που τα υψηλότερα στρώματα ικανοποιούν. Επομένως, τα μόνα ζητήματα ασφάλειας σχετικά με τα ασύρματα δίκτυα περιλαμβάνουν τα στρώματα που ασχολούνται με ζητήματα, όπως η κρυπτογράφηση στοιχείων.

1.4.2 Απειλές ασφάλειας

Το κύριο ζήτημα ασφάλειας με τα ασύρματα δίκτυα, είναι ότι διαδίδουν τα στοιχεία πέρα από μια περιοχή που μπορεί να υπερβεί τα όρια της περιοχής επί της οποίας ασκείται ο έλεγχος. Τα εκπεμπόμενα σήματα ενός ασύρματου δικτύου διαπερνούν με σχετική ευκολία τους τοίχους ενός κτηρίου και διαχέονται στο γειτονικό περιβάλλον. Έτσι κάλλιστα κάποιος κακόβουλος χρήστης μπορεί με τη χρήση της ίδιας συσκευής NIC να λάβει τα σήματα αυτά από απόσταση που δεν επιτηρείται από προσωπικό ασφαλείας όπως είναι οι χώροι στάθμευσης (**Σχήμα 1.4**). Αυτό φυσικά απαιτεί ο εισβολέας να γνωρίζει τον κωδικό πρόσβασης του δικτύου ούτως ώστε να συνδεθεί με αυτό.

Αυτό το πρόβλημα υπάρχει επίσης με τα ενσύρματα δίκτυα τύπου ethernet, αλλά σε έναν μικρότερο βαθμό. Η τρέχουσα ροή μέσω των καλωδίων εκπέμπει ηλεκτρομαγνητικά κύματα που κάποιος θα μπορούσε να παραλάβει με τη χρησιμοποίηση του κατάλληλου εξοπλισμού λήψης.



Σχήμα 1.4. Η παθητική λήψη δεδομένων στα ασύρματα δίκτυα είναι πιο εύκολη από ότι στα ενσύρματα.

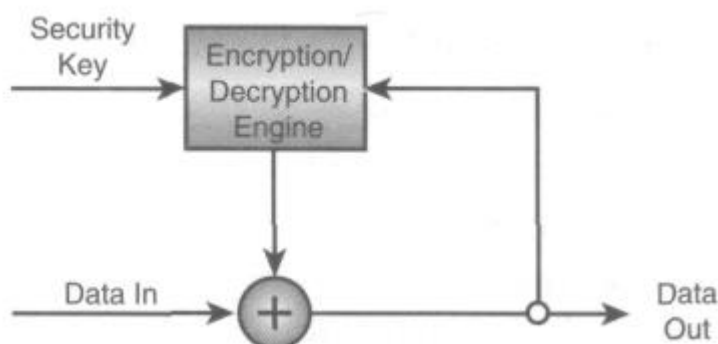
Ένα άλλο πρόβλημα ασφάλειας είναι η δυνατότητα ηλεκτρονικής δολιοφθοράς, στην οποία κάποιος φράζει κακόβουλα το δίκτυο και εμποδίζει τη χρησιμοποίησή του. Όπως είναι γνωστό τα περισσότερα ασύρματα δίκτυα χρησιμοποιούν ένα πρωτόκολλο ανίχνευσης φέροντος σήματος για να μοιραστούν τη χρήση. Επομένως για να ασφαλιστεί το δίκτυο κρίνεται απαραίτητη η χρήση προϊόντων ασύρματης δικτύωσης από μία ίδια εταιρεία κατασκευής. Με τη σύσταση ενός σταθμού πρόσβασης θα ελέγχεται η προέλευση όλων των μεταδόσεων και θα υπάρχει φραγμός για τις μεταδόσεις που θα προέρχονται από αλλότριες συσκευές. Η διάταξη αυτή θα καταστήσει το δίκτυο ασφαλές από περιπτώσεις εξωτερικής επέμβασης.

1.4.3 Μέτρα προστασίας ασφάλειας

Οι προμηθευτές ασύρματων δικτύων λύνουν τα περισσότερα προβλήματα ασφάλειας με τον περιορισμό της πρόσβασης στα στοιχεία τους. Τα περισσότερα προϊόντα απαιτούν τη χρήση ενός κωδικού πρόσβασης. Ένας ασύρματος σταθμός δεν θα επεξεργαστεί τα στοιχεία εκτός αν ο κωδικός του τίθεται στην ίδια τιμή εκείνης με του δικτύου. Μερικοί προμηθευτές προσφέρουν επίσης την κρυπτογράφηση ως επιλογή.

Το WaveLAN, παραδείγματος χάριν, έχει δύο επιλογές για την κρυπτογράφηση. Μια έκδοση κρυπτογραφεί σύμφωνα με τα πρότυπα κρυπτογράφησης στοιχείων (DBS) όπως καθορίζεται από το Αμερικάνικο τμήμα εμπορίου, το εθνικό ίδρυμα προτύπων και την τεχνολογία (NIST), αποκαλούμενα στο παρελθόν εθνικό γραφείο των προτύπων (NBS). Η άλλη έκδοση εφαρμόζει μια ιδιόκτητη μέθοδο που ονομάζεται AES.

Οι αλγόριθμοι DES και AES χρησιμοποιούν ένα 16-δεκαεξαδικό ψηφίο για την κρυπτογράφηση, όπως φαίνεται στο **σχήμα 1.5**. Το κλειδί φορτώνεται στο τσιπ ασφάλειας όταν διαμορφώνεται ο προσαρμοστής κατά την εγκατάσταση. Όταν ένα μήνυμα παραλαμβάνεται ή στέλνεται, το τσιπ ασφάλειας χρησιμοποιεί το κλειδί για να κρυπτογραφήσει ή να αποκρυπτογραφήσει το μήνυμα. Μόνο εκείνοι οι τερματικοί σταθμοί στο δίκτυο με το ίδιο τσιπ και το κλειδί ασφάλειας θα είναι σε θέση να καταλάβουν τα μηνύματα. Άλλοι χρήστες WaveLAN που δεν έχουν το βασικό τσιπ ασφάλειας είναι ανίκανοι να αποκρυπτογραφήσουν οποιαδήποτε μηνύματα. Τα DES και τα AES εκτελούν την κρυπτογράφηση σε ένα συνεχές ρεύμα δεδομένων που περνούν μέσω του διαμορφωτή του συστήματος χωρίς μείωση της απόδοσης.



Σχήμα 1.5. Η κρυπτογράφηση βελτιώνει την ασφάλεια των ασύρματων δικτύων.

Το τμήμα εμπορίου περιορίζει την εξαγωγή συσκευών DES έξω από τις Ηνωμένες Πολιτείες. Ο σκοπός του AES είναι να παρασχεθεί μια εναλλακτική λύση για DES σε εκείνους τους χρήστες WaveLAN που χρειάζονται μια ασφαλή διεπαφή, αλλά που δεν έχουν την άδεια για να χρησιμοποιήσουν DES λόγω των περιορισμών εξαγωγής. Το AES εφαρμόζει έναν ιδιόκτητο αλγόριθμο που έχει εγκριθεί για την εξαγωγή.

1.4.4 Προβλήματα σύνδεσης

Η χρήση των παραδοσιακών συνδέσεων με καλώδια πρωτοκόλλων πέρα από τα ασύρματα δίκτυα εισάγει τα προβλήματα διατήρησης των συνδέσεων μεταξύ της συσκευής του χρήστη και της εφαρμογής που χρησιμοποιείται σε έναν κεντρικό υπολογιστή. Το TCP/IP, παραδείγματος χάριν, παρέχει τις πολύ αξιόπιστες συνδέσεις πέρα από τα συνδεδεμένα με καλώδιο δίκτυα, όπως το ethernet και το token ring. Πέρα από τα ασύρματα δίκτυα, εντούτοις, το TCP/IP είναι ευαίσθητο στην απώλεια των συνδέσεων, ειδικά όταν λειτουργεί η συσκευή σε μια περιοχή με την οριακή ασύρματη κάλυψη δικτύων.

Επιπλέον, η κινητή φύση των ασύρματων δικτύων μπορεί να διευκολύνει την εξέταση των προβλημάτων. Τα περισσότερα δίκτυα απαιτούν τη διεύθυνση IP που φορτώνεται στη συσκευή του χρήστη να είναι μέσα σε μια συγκεκριμένη περιοχή διευθύνσεων για να διατηρήσουν τις κατάλληλες συνδέσεις με τις εφαρμογές. Όταν ένας χρήστης περιπλανάται με μια ασύρματη συσκευή από ένα υποδίκτυο IP σε άλλο, η συσκευή και η εφαρμογή μπορούν να χάσουν την ικανότητα να συνδέουν η μια με την άλλη.

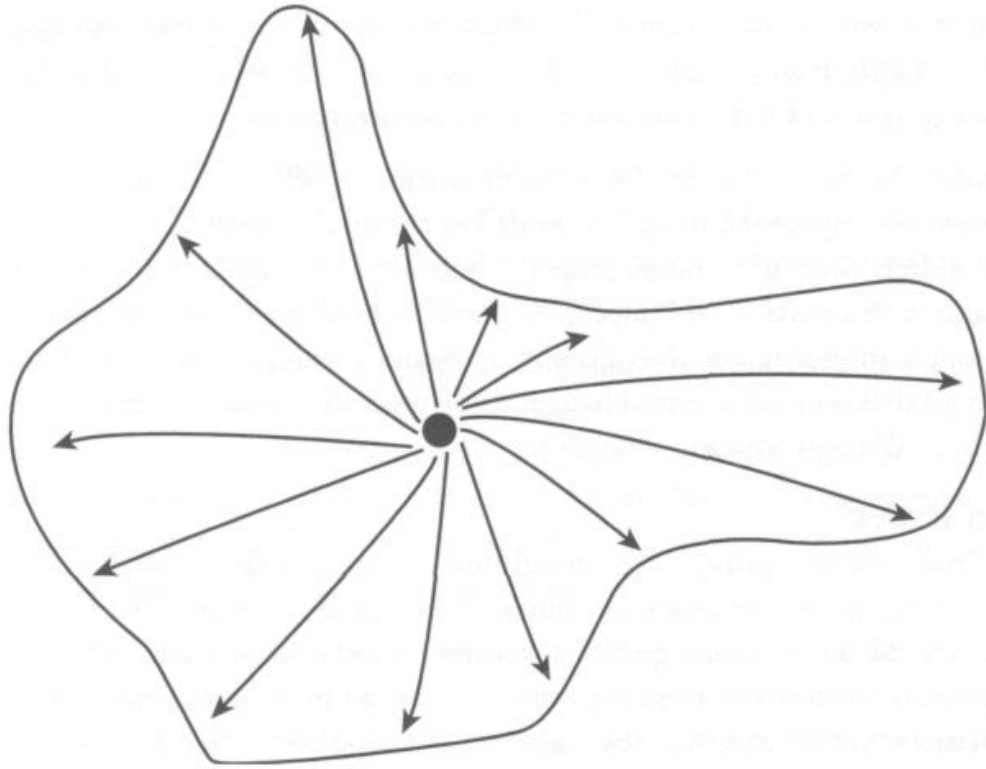
1.4.5 Ζητήματα εγκατάστασης

Ο προγραμματισμός εγκατάστασης ενσύρματων δικτύων είναι μια αρκετά απλή διαδικασία. Αρκεί να γίνει μια σύντομη έρευνα στην περιοχή εγκατάστασης για να αποφασιστεί ποιες διαδρομές θα ακολουθήσουν οι τεχνικοί για να περάσουν τα καλώδια. Για να ελεγχθεί αν η εγκατάσταση των καλωδίων είναι δυνατή, πρέπει να μετρηθούν οι αποστάσεις των διαδρομών που θα ακολουθήσουν τα καλώδια. Εάν κάποιος από τους χρήστες βρίσκεται πάρα πολύ μακριά από το δίκτυο, είναι εφικτή η σχεδίαση μιας μακρινής λύσης δικτύωσης ή η επέκταση του μήκους του καλωδίου με την χρήση επαναληπτών. Αφού ολοκληρωθεί ο σχεδιασμός, οι τεχνικοί θα περάσουν όλη την καλωδίωση και η διαβίβαση των δεδομένων θα γίνει σύμφωνα με τα προγραμματισμένα.

Μια ασύρματη εγκατάσταση του τοπικού LAN δεν είναι όμως προβλέψιμη. Είναι δύσκολο, έως και αδύνατο, να σχεδιαστεί το ασύρματο σύστημα με μόνο εργαλείο την επιθεώρηση της περιοχής. Η πρόβλεψη του τρόπου με τον οποίο το περίγραμμα του κτιρίου έχει επιπτώσεις στη διάδοση των ραδιοκυμάτων είναι δύσκολη. Οι κατευθυντικές κεραίες διαδίδουν τα ράδιο κύματα σε όλες τις κατευθύνσεις. Οι τοίχοι, οι οροφές, και άλλα εμπόδια μειώνουν τα σήματα περισσότερο σε μια κατεύθυνση σε σχέση με μια άλλη, και αναγκάζουν ακόμη και μερικά κύματα να αλλάξουν τις πορείες μετάδοσής τους. Ακόμη και το άνοιγμα μιας πόρτας λουτρών μπορεί να αλλάξει το σχέδιο διάδοσης. Αυτά τα γεγονότα αναγκάζουν το πραγματικό σχέδιο ακτινοβολίας να διαστρεβλώνεται, παίρνοντας μια οδοντωτή εμφάνιση, όπως φαίνεται στο σχήμα 6.

Ασύρματα μητροπολιτικά δίκτυα είναι πολύ δύσκολο να εγκατασταθούν. Βασικό πρόβλημα αποτελεί η έλλειψη οπτικής επαφής μεταξύ των κεραιών λόγω της ύπαρξης πολλών κτιρίων. Επίσης είναι δυνατόν να συναντήσουμε πολλές παρεμβολές από άλλα ασύρματα δίκτυα ή οικιακές συσκευές που παράγουν «θόρυβο».

Για να αποφύγει τα προβλήματα εγκαταστάσεων, μια εταιρεία πρέπει να εκτελέσει τις δοκιμές μετάδοσης για να αξιολογήσει την κάλυψη του δικτύου. Αν παραμεληθεί η παραπάνω διαδικασία τότε είναι πολύ πιθανόν μερικοί από τους χρήστες να μην είναι σε θέση να συνδεθούν με τα σημεία πρόσβασης.



Σχήμα 1.6. Η αναπαράσταση των ραδιοκυμάτων που εκπέμπει μια οmni κεραία μέσα σε ένα γραφείο είναι ακανόνιστη και απρόβλεπτη.

Κεφάλαιο 2ο

2.1 Τα συστατικά ενός ασύρματου δικτύου

2.1.1 Γενικά

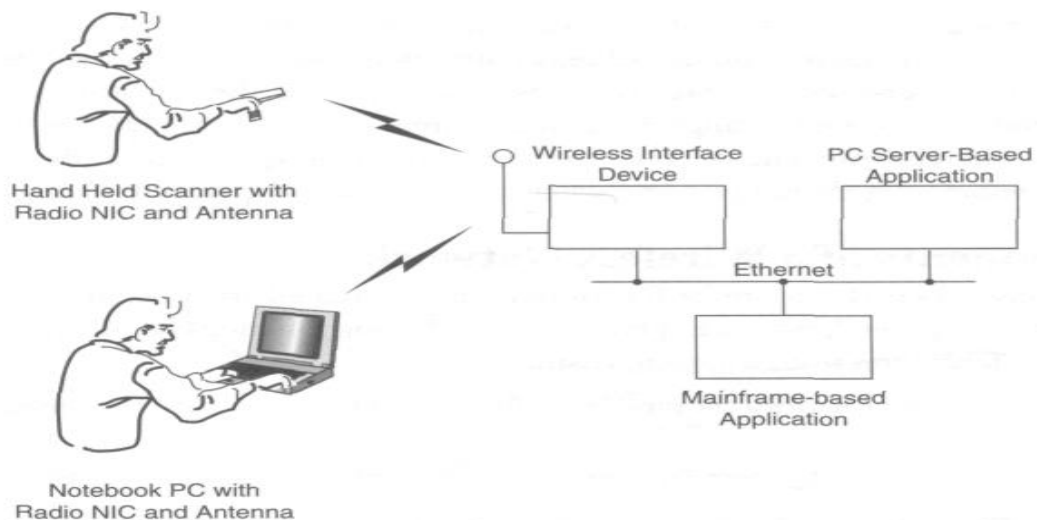
Τα ασύρματα δίκτυα εκτελούν παρόμοιες λειτουργίες με τα ενσύρματα δίκτυα όπως το ethernet και το token ring. Γενικά, τα δίκτυα εκτελούν τις ακόλουθες λειτουργίες για να επιτρέψουν τη μεταφορά των πληροφοριών από την πηγή στον προορισμό:

1. Το μέσο παρέχει ένα δίαυλο διαβίβασης στοιχείων.
2. Οι μέσες τεχνικές πρόσβασης διευκολύνουν τη διανομή ενός κοινού μέσου.
3. Τα δεδομένα παραμένουν αναλλοίωτα.
4. Οι μηχανισμοί δρομολόγησης επιτρέπουν τη μετάδοση των δεδομένων από την πηγή δημιουργίας προς τον αποδέκτη.
5. Το λογισμικό συνδετικότητας διασυνδέει μια συσκευή, όπως ο light pen ανιχνευτής κώδικα υπολογιστών ή φραγμών, στα προγράμματα εφαρμογών που φιλοξενούνται σε έναν κεντρικό υπολογιστή.

Ένας καλός τρόπος να απεικονιστούν αυτές οι λειτουργίες είναι να διευκρινιστεί η δικτυακή αρχιτεκτονική. Αυτή η αρχιτεκτονική περιγράφει τα πρωτόκολλα, το σημαντικό υλικό, και τα στοιχεία λογισμικού που αποτελούν το δίκτυο. Μια δικτυακή αρχιτεκτονική, είτε ασύρματη είτε ενσύρματη, μπορεί να αντιμετωπισθεί με δύο τρόπους, φυσικά και λογικά.

2.1.2 Φυσική αρχιτεκτονική ενός ασύρματου δικτύου

Τα φυσικά συστατικά ενός ασύρματου δικτύου εφαρμόζουν τη φυσική, σύνδεση στοιχείων, και τις λειτουργίες στρώματος δικτύων (**Σχήμα 2.1**) για να ικανοποιήσουν τη λειτουργία που απαιτείται μέσα στις τοπικές, μητροπολιτικές, και ευρείες περιοχές. Τα εξής τμήματα εξηγούν τα διάφορα συστατικά του ασύρματου τοπικού LAN.



Σχήμα 2.1. Τα συστατικά ενός ασύρματου δικτύου επεκτείνουν τις δυνατότητες του ενσύρματου.

2.1.3 Συσκευές τελικών χρηστών

Όπως με οποιοδήποτε σύστημα, πρέπει να υπάρχει ένας τρόπος για τους χρήστες να διασύνδεδουν τις εφαρμογές με τις υπηρεσίες. Εάν το δίκτυο είναι ασύρματο ή ενσύρματο, μια συσκευή τελικών χρηστών είναι μια διεπαφή μεταξύ του χρήστη και του δικτύου. Παρακάτω είναι οι κατηγορίες συσκευών τελικών χρηστών που είναι οι αποτελεσματικότερες ως συσκευές για τα ασύρματα δίκτυα:

- Τερματικοί σταθμοί υπολογιστών γραφείου
- Υπολογιστές laptop
- Υπολογιστές Palmtop
- Φορητό PC
- light pen βασισμένα σε υπολογιστές
- Προσωπικοί ψηφιακοί βοηθοί (PDA)
- Φορητοί ανιχνευτές και συλλέκτες στοιχείων
- Φορητοί εκτυπωτές

Σήμερα, το φορητό PC, που εισάγεται από τη Microsoft (αλλά που αναπτύσσεται και που κατασκευάζεται από άλλες επιχειρήσεις), είναι η αρχική πλατφόρμα υλικού για τα Windows CE, τα οποία λειτουργούν άψογα με τις συσκευές ασύρματης δικτύωσης των φορητών υπολογιστών. Οι βασικοί στόχοι στην ανάπτυξη του φορητού PC περιλαμβάνουν τη μακριά ζωή μπαταριών, την προσιτή τιμή (περίπου €500), την πυκνότητα και το ελάχιστο δυνατό βάρος, τις γνωστές διεπαφές, την εύκολη σύνδεση PC, και την εργονομική διάταξη των πληκτρολογίων.

Τα κοινά χαρακτηριστικά γνωρίσματα φορητού PC περιλαμβάνουν τα εξής:

- Ενσωματωμένο πληκτρολόγιο QWERTY με τα αλφαριθμητικά πλήκτρα, την τυποποιημένη στίξη, ένα κουμπί CTRL, κουμπί ALT, και δύο πλήκτρα Shift. Υπάρχουν και άλλα πλήκτρα που είναι προαιρετικά.

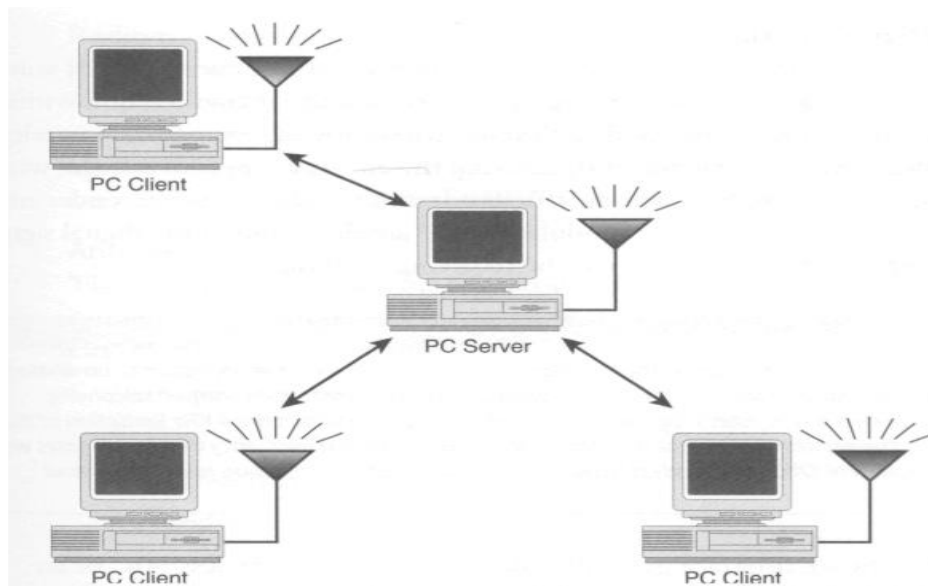
- Ενσωματωμένη οθόνη αφής με ανάλυση 480x240 ή 640x240.
- Διαθέτουν υποδοχές καρτών PC (PCMCIA), υποδοχή για USB, υποδοχή για καλώδιο UTP και αισθητήρας υπέρυθρων (IrDA).
- Τουλάχιστον 512MB RAM.

2.1.4 Λογισμικό δικτύων

Ένα ασύρματο δίκτυο αποτελείται από το λογισμικό που βρίσκεται εγκατεστημένο στα διαφορετικά μέρη του δικτύου. Ένα λειτουργικό σύστημα δικτύων, όπως τα Windows XP, που φιλοξενείται σε ένα high-end PC παρέχει υπηρεσίες εφαρμογής. Πολλά αριθμητικά στοιχεία είναι αποθηκευμένα στον κεντρικό υπολογιστή που προσανατολίζεται, όπως φαίνεται στο σχήμα 8, όπου περιέχονται τα προγράμματα εφαρμογών και οι βάσεις δεδομένων. Στις περισσότερες περιπτώσεις, οι συσκευές θα διασυνδέσουν μέσω του TCP/ IP τα προγράμματα εφαρμογών ή μια βάση δεδομένων που λειτουργεί.

Το λογισμικό πελατών, που βρίσκεται στη συσκευή του τελικού χρήστη, κατευθύνει τις εντολές του χρήστη στο τοπικό λογισμικό των συσκευών, ή τις οδηγεί έξω μέσω του ασύρματου δικτύου. Το λογισμικό που βρίσκεται σε μια ασύρματη συσκευή είναι πολύ παρόμοιο με το λογισμικό που τρέχει σε μια συνδεδεμένη με καλώδιο συσκευή. Η κύρια διαφορά είναι ότι είναι σημαντικό να αναπτυχθεί το ασύρματο λογισμικό για να βελτιστοποιήσει τη χρήση του μικρού ποσού του ασύρματου δικτύου σχετικά εύρους ζώνης.

Το λογισμικό που εκτελεί τις λειτουργίες εφαρμογής μπορεί να τρέξει σε έναν κεντρικό υπολογιστή, όπως είναι ένας υπολογιστής της IBM, (π.χ. IBM AS/400), ή ένας σταθμός Unix. Αυτό κάνει τη συσκευή να ενεργήσει ως κουτό τερματικό, διασυνδέοντας το πληκτρολόγιο, την οθόνη και τον εκτυπωτή, με την εφαρμογή που τρέχει στον κεντρικό υπολογιστή. Με τα συστήματα αυτού του είδους, το λογισμικό στη συσκευή μπορεί να εκτελέσει τη λειτουργία ενός τμήματος ή όλης της εφαρμογής και διασυνδέεται με μια βάση δεδομένων που βρίσκεται σε έναν κεντρικό υπολογιστή, όπως ένας υπολογιστής με Windows NT.



Σχήμα 2.2. Ένα δικτυακό λειτουργικό σύστημα που βασίζεται σε server παρέχει μια συγκεντρωτική πλατφόρμα για την αποθήκευση δεδομένων μέσω εφαρμογών που χρησιμοποιούν οι χρήστες του ασύρματου δικτύου.

Σε μερικές περιπτώσεις, ένας υπολογιστής-πύλη είναι απαραίτητος για να παρέχει μια διεπαφή μεταξύ της συσκευής και των προγραμμάτων εφαρμογών που τρέχουν στον κεντρικό υπολογιστή. Οι συσκευές επικοινωνούν με τον κεντρικό υπολογιστή μέσω της πύλης. Η πύλη ενεργεί ως πληρεξούσιος για τις διάφορες συσκευές. Τα πλεονεκτήματα της χρήσης του υπολογιστή-πύλη είναι τα ακόλουθα:

- Καλύτερη απόδοση: Με την παρουσία μιας πύλης μεταφορών και εφαρμογής, οι συσκευές επικοινωνούν με την πύλη με τη χρησιμοποίηση ενός φιλικού πρωτοκόλλου που είναι πιο απλό σε σχέση με το TCP/IP.
- Αξιοπιστία: Εάν ο υπολογιστής-πύλη είναι αξιόπιστος τότε το δίκτυο δουλεύει απρόσκοπτα.
- Μακρύτερη ζωή μπαταριών: Όταν οι συσκευές βρίσκονται σε κατάσταση μη απασχόλησης, το λογισμικό δικτύων δεν είναι απαραίτητο να στείλει τα keep - alive πακέτα για να τηρήσει τη σύνδεση με τον κεντρικό υπολογιστή.

2.1.5 Ασύρματη διεπαφή δικτύων

Οι υπολογιστές επεξεργάζονται τις πληροφορίες σε ψηφιακή μορφή, με χαμηλή τάση τύπου DC η οποία αναπαριστά τις καταστάσεις 1 και 0. Αυτά τα σήματα είναι κατάλληλα για μετάδοση στο εσωτερικό ενός υπολογιστή, αλλά δεν ενδείκνυνται για μετάδοση δεδομένων μέσω ενός ενσύρματου ή ασύρματου δικτύου. Μια διεπαφή ασύρματου δικτύου, συνδέει το ψηφιακό σήμα τη συσκευή των τελικών χρηστών με το ασύρματο μέσο, που είναι ο αέρας, για να γίνει δυνατή μια αποδοτική μεταφορά των δεδομένων μεταξύ του αποστολέα και του δέκτη. Αυτή η διαδικασία

περιλαμβάνει τη διαμόρφωση και την ενίσχυση του ψηφιακού σήματος σε μια μορφή αποδεκτή για τη διάδοση προς την λαμβάνουσα θέση.

Η διεπαφή ασύρματων δικτύων παίρνει γενικά τη μορφή ενός ασύρματου NIC ή ενός εξωτερικού διαμοδιαμορφωτή (modem) που διευκολύνει το διαμορφωτή και τα πρωτόκολλα επικοινωνιών. Αυτά τα συστατικά διασυνδέουν τη συσκευή χρηστών μέσω ενός διαύλου επικοινωνίας, όπως ISA (τυποποιημένη αρχιτεκτονική βιομηχανίας) ή PCMCIA. Ο δίαυλος ISA χρησιμοποιείται περισσότερο από τους υπολογιστές γραφείου PC. Πολλοί φορητοί υπολογιστές έχουν θύρες PCMCIA που δέχονται κάρτες NICs. Το PCMCIA υποστηρίζει τρία μεγέθη διεπαφών: Τύπος I (3,3 χιλιοστόμετρα), τύπος II (5,0 χιλιοστόμετρα), και τύπος III (10,5 χιλιοστόμετρα). Μερικές επιχειρήσεις παράγουν επίσης τα ασύρματα συστατικά που συνδέουν με τον υπολογιστή μέσω του προτύπου RS-232.

Η διεπαφή μεταξύ της συσκευής του χρήστη και του NIC περιλαμβάνει επίσης έναν οδηγό λογισμικού που συνδέει την εφαρμογή του πελάτη ή το λογισμικό και την κάρτα. Οι πιο σημαντικοί από αυτούς τους οδηγούς είναι οι ακόλουθοι:

- NDIS (Network Driver Interface Specification): Οδηγός που χρησιμοποιείται με τα λειτουργικά συστήματα δικτύων της Microsoft.

- ODI (Open Datalink Interface): Οδηγός που χρησιμοποιείται με τα λειτουργικά συστήματα δικτύων Novell.

- PDS (Packet Driver Specification): Ένας γενικός driver για το DOS που αναπτύχθηκε από την εταιρεία λογισμικού FTP για τη χρήση σε υλοποιήσεις βασισμένες στο TCP/IP.

Οι ασύρματες κάρτες έρχονται παραδοσιακά με δύο συσκευές δηλαδή μια κάρτα PCMCIA που τοποθετείται στο φορητό υπολογιστή και ένα εξωτερικό κουτί πομποδεκτών. Αυτή η οργάνωση είναι ικανοποιητική για μερικές εφαρμογές, όπως οι ενσωματωμένες συσκευές εντούτοις όμως, δεν είναι εργονομική για τις περισσότερες φορητές συσκευές. Μερικοί προμηθευτές, ειδικά με τις νεώτερες ασύρματες κάρτες τους, προσφέρουν τις νέες PCMCIA οι οποίες έχουν ενσωματωμένους τους πομποδέκτες.

2.1.6 Κεραία

Η κεραία ακτινοβολεί το διαμορφωμένο σήμα μέσω του αέρα έτσι ώστε ο προορισμός να μπορεί να το παραλάβει. Οι κεραίες έρχονται σε πολλές μορφές και μεγέθη και έχουν τα ακόλουθα συγκεκριμένα χαρακτηριστικά:

- Πρότυπο διάδοσης
- Κέρδος
- Εύρος ζώνης

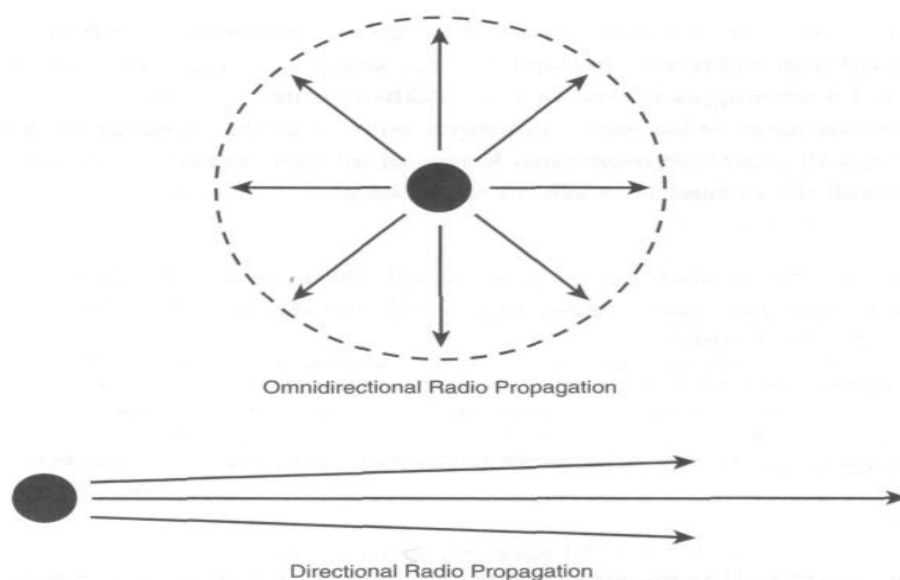
Το πρότυπο διάδοσης μιας κεραίας καθορίζει την κάλυψή του. Μια κατευθυντική κεραία αποστέλλει το μεγαλύτερο μέρος του σήματος της προς μια κατεύθυνση. Το σχήμα 9 επεξηγεί τις διαφορές.

Μια κατευθυντική κεραία έχει μεγαλύτερο βαθμό ενίσχυσης του σήματος σε σχέση με μία πανκατευθυντική. Και είναι σε θέση να διαδώσει μακρύτερα το διαμορφωμένο σήμα επειδή επικεντρώνει την εκπομπή προς μία συγκεκριμένη κατεύθυνση. Οι πανκατευθυντικές κεραίες είναι καλύτερες για τα εσωτερικά ασύρματα δίκτυα λόγω των σχετικά πιο σύντομων απαιτήσεων σειράς και τη λιγότερη ευαισθησία στην εξωτερική παρέμβαση.

Οι κατευθυντικές κεραίες θα ικανοποιήσουν καλύτερα τις ανάγκες για τα κτήρια μέσα στις μητροπολιτικές περιοχές λόγω της μεγαλύτερης σειράς και της επιθυμίας να ελαχιστοποιηθεί η παρέμβαση.

Ο συνδυασμός ισχύος μετάδοσης και κέρδους μιας κεραίας καθορίζει την απόσταση στην οποία θα διαδώσει το σήμα. Οι μεγάλης απόστασης μεταδόσεις απαιτούν υψηλότερη ισχύ και κατευθυντική εκπομπή σήματος.

Από την άλλη πλευρά οι εκπομπές μικρής απόστασης απαιτούν λιγότερη ισχύ και λιγότερο κέρδος. Με τα ασύρματα δίκτυα, η ισχύς μετάδοσης είναι σχετικά χαμηλή, χαρακτηριστικά περίπου ένα Watt ή λιγότερα.



Σχήμα 2.3. Μια πανκατευθυντική κεραία εκπέμπει προς όλες τις κατευθύνσεις ενώ μια κατευθυντική εστιάζει σε μια συγκεκριμένη κατεύθυνση.

Το εύρος ζώνης είναι το επηρεάζων μέρος της συχνότητας φάσματος που διαδίδει το σήμα. Το τηλεφωνικό σύστημα, παραδείγματος χάριν, λειτουργεί σε ένα εύρος ζώνης κατά προσέγγιση από 0 έως 4KHz. Το εύρος ζώνης αυτό είναι αρκετό για να εξυπηρετήσει τις ανάγκες μετάδοσης φωνής.

Τα συστήματα ραδιοκυμάτων έχουν τα μεγαλύτερα ποσά εύρους ζώνης που βρίσκονται στις πολύ υψηλότερες συχνότητες. Ο ρυθμός μετάδοσης πληροφοριών και το εύρος ζώνης είναι άμεσα ανάλογα: όσο υψηλότερος είναι ο ρυθμός μετάδοσης πληροφοριών, τόσο περισσότερο εύρος ζώνης θα χρειαστεί.

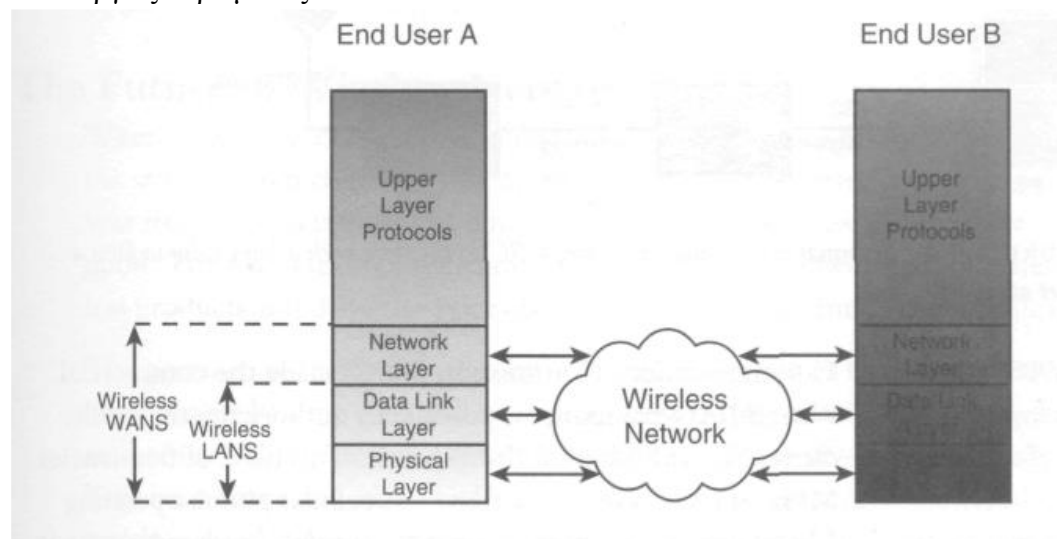
2.1.7 Το κανάλι επικοινωνιών

Όλα τα συστήματα πληροφοριών χρησιμοποιούν ένα κανάλι επικοινωνιών κατά μήκος του οποίου ρέουν πληροφορίες από την πηγή στον προορισμό. Τα δίκτυα Ethernet μπορούν να χρησιμοποιήσουν το UTP ή το ομοαξονικό καλώδιο. Τα ασύρματα δίκτυα χρησιμοποιούν τον αέρα ως μέσο. Στη γήινη επιφάνεια, ως μέσα μετάδοσης χρησιμοποιούνται τα κύματα και το υπέρυθρο φως.

Η βροχή, η ομίχλη, και το χιόνι μπορούν να αυξήσουν το ποσό μορίων ύδατος στον αέρα. Παρόλα αυτά η μετάδοση μπορεί να γίνει πολύ καλά. Εξασθένιση καλείται η μείωση του εύρους του σήματος, η οποία περιορίζει το βεληνεκές της λειτουργίας του συστήματος. Οι τρόποι να καταπολεμηθεί η μείωση είναι είτε να αυξηθεί η ισχύς μετάδοσης των ασύρματων συσκευών, που στις περισσότερες περιπτώσεις περιορίζεται από την FCC, είτε να γίνει χρήση ειδικών ενισχυτών που καλούνται επαναλήπτες οι οποίοι ειδικεύονται στη λήψη αδύναμων σημάτων.

Ένα ασύρματο δίκτυο δεν προσφέρει όλες τις λειτουργίες του OSI αλλά λειτουργεί μόνο στα κατώτερα τρία στρώματα όπως φαίνεται στο σχήμα 10 .

Μόνο τα ασύρματα δίκτυα ευρείας περιοχής, εντούτοις, εκτελούν τις λειτουργίες στρώματος δικτύων.

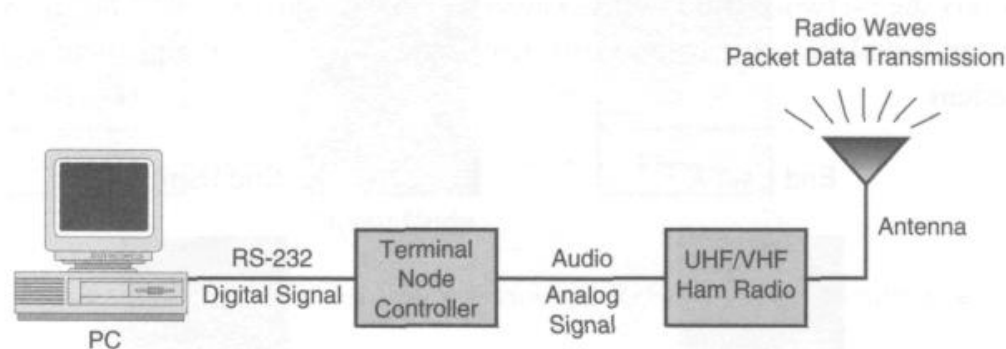


Σχήμα 2.4. Τα ασύρματα δίκτυα μπορούν να συνδέσουν 2 ενσύρματα.

2.2 Η ιστορία των ασύρματων δικτύων

Η τεχνολογία δικτύων και οι ασύρματες επικοινωνίες συνδυάστηκαν για πρώτη φορά το 1971 στο πανεπιστήμιο της Χαβάης χάρις σε ένα ερευνητικό πρόγραμμα που ονομάζονταν ALOHANET. Το σύστημα ALOHANET επέτρεπε την επικοινωνία μεταξύ των υπολογιστών που βρίσκονταν σε επτά πανεπιστημιούπολεις χτισμένες πάνω σε τέσσερα νησιά.

Οι υπολογιστές επικοινωνούσαν με τον κεντρικό υπολογιστή χωρίς τη χρήση των υπάρχουσών αναξιοπίστων και ακριβών τηλεφωνικών γραμμών. Το ALOHANET πρόσφερε τις αμφίδρομες επικοινωνίες, σε μια τοπολογία αστεριών, μεταξύ του κεντρικού υπολογιστή και κάθε ενός από τους χρήστες. Στη δεκαετία του '80, ραδιοερασιτέχνες με την ονομασία « hams », διατήρησαν την ασύρματη δικτύωση ενεργή μέσα στις Ηνωμένες Πολιτείες και τον Καναδά. Σχεδίασαν και υλοποίησαν τα terminal node controllers (TNCs) για να διασυνδέσουν τους υπολογιστές τους μέσω του ραδιοεξοπλισμού τους. (Σχήμα 11). Τα TNC λειτουργούν σαν ένα modem που μετατρέπουν το ψηφιακό σήμα του υπολογιστή σε ένα που το ραδιοερασιτεχνικό δίκτυο « ham » μπορεί να διαμορφώσει και να στείλει μέσω του μέσου μετάδοσης κυμάτων χρησιμοποιώντας μια τεχνική μεταγωγής πακέτων. Στην πραγματικότητα, η American Radio Relay League (ARRL) και η Canadian Radio Relay League (CRRL) έχουν υποστηρίξει τη διάσκεψη δικτύωσης υπολογιστών από την αρχή της δεκαετίας του '80 για να παρέχουν ένα φόρουμ για την ανάπτυξη ασύρματων δικτύων. Κατά συνέπεια, οι ραδιοερασιτέχνες « hams » έχουν χρησιμοποιήσει την ασύρματη δικτύωση για χρόνια, πολύ νωρίτερα από την εμπορική αγορά.



Σχήμα 2.5. Ένας ελεγκτής τερματικός κόμβος μπορεί να κάνει ένα PC να επικοινωνήσει μέσω μιας ραδιοφωνικής μπάντας και να δημιουργήσει ένα δικτύου ασύρματης μετάδοσης πληροφοριών.

Το 1985, η Federal Communications Commission (FCC) κατέστησε δυνατή την εμπορική ανάπτυξη ασύρματων τμημάτων ενός τοπικού LAN με την έγκριση της δημόσιας χρήσης των βιομηχανικών, επιστημονικών, και ιατρικών (ISM) ζωνών. Αυτή η ζώνη συχνοτήτων ανήκει ανάμεσα στους 902MHz και στους 5,85 GHz, ακριβώς επάνω από τις κυψελοειδείς τηλεφωνικές συχνότητες. Η ζώνη ISM αποδείχθηκε πολύ ελκυστική για τους προμηθευτές προϊόντων ασύρματης δικτύωσης

διότι παραχωρείται μέρος του φάσματος στο οποίο θα λειτουργήσουν τα προϊόντα τους, όπου οι τελικοί χρήστες δεν είναι απαραίτητο να λάβουν ειδικές άδειες για να χρησιμοποιήσουν τα προϊόντα. Η κατανομή των ζωνών ISM είχε μια δραματική επίδραση στην ασύρματη βιομηχανία. Συντέλεσε στην έντονη ανάπτυξη των ασύρματων δικτύων. Παρόλα αυτά, δίχως πρότυπα, οι προμηθευτές άρχισαν να υλοποιούν συσκευές ασύρματης δικτύωσης. Προς το τέλος της δεκαετίας του '80, το Institute for Electrical and Electronic Engineers (IEEE), αρμόδιο για την ανάπτυξη των προτύπων του τοπικού LAN, όπως το ethernet και το token ring, άρχισε την ανάπτυξη των προτύπων για τα ασύρματα δίκτυα. Υπό την προεδρία του Vic Hayes, ενός μηχανικού από την NCR, η ομάδα εργασίας του IEEE για το 802.11 ανέπτυξε τις προδιαγραφές Ελέγχου Προσπέλασης Μέσου και Φυσικού Επιπέδου για τα ασύρματα δίκτυα.

Το συμβούλιο προτύπων του IEEE ενέκρινε τα πρότυπα στις 26 Ιουνίου 1997, και το IEEE δημοσίευσε τα πρότυπα στις 18 Νοεμβρίου 1997. Η περάτωση αυτών των προτύπων προτρέπει στους κατασκευαστές να παράγουν συσκευές ασύρματης δικτύωσης συμβατές με το 802.11 από το έτος 1998. Είναι βέβαιο ότι θα εμφανιστούν νέοι κατασκευαστές οι οποίοι θα συμμορφωθούν με τα πρότυπα 802.11. Μια άλλη ευρέως αποδεκτή ασύρματη σύνδεση δικτύων, είναι ασύρματες υπηρεσίες WAN, οι οποίες άρχισαν να υλοποιούνται στις επιχειρήσεις στις αρχές της δεκαετίας του '90. Εταιρείες όπως η ARDIS και η RAM Mobile Data ήταν οι πρώτες που πουλούσαν ασύρματες ζεύξεις μεταξύ φορητών υπολογιστών, εταιρικών δικτύων, και του Διαδικτύου. Οι επιχειρήσεις άρχισαν έπειτα τις υπηρεσίες Κυψελικά Ψηφιακά Πακέτα Δεδομένων (CDPD), οι οποίες επιτρέπουν στους χρήστες να στείλουν και να λάβουν πακέτα δεδομένων μέσω των ψηφιακών υπηρεσιών μετάδοσης. Αυτές οι υπηρεσίες επιτρέπουν στους υπαλλήλους να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο και σε άλλες υπηρεσίες πληροφοριών από τις προσωπικές συσκευές τους χωρίς τη χρήση του τηλεφωνικού συστήματος.

2.3 Το μέλλον των ασύρματων δικτύων

Αναρωτιέται κανείς ποια θα είναι η πορεία της ασύρματης δικτύωσης. Ποια θα είναι η ανάπτυξη της τεχνολογίας καθώς και τα προϊόντα της την επόμενη πενταετία. Η προοπτική για τα ασύρματα δίκτυα είναι ελπιδοφόρα. Η ωρίμανση των προτύπων αποτελεί κίνητρο για τους προμηθευτές ώστε να παράγουν νέα προϊόντα ασύρματης δικτύωσης και να μειώσουν τις τιμές σε επίπεδα πιο προσιτά στο καταναλωτικό κοινό.

Η παρουσία προτύπων θα παρακινήσει τις μικρότερες επιχειρήσεις να κατασκευάσουν τα ασύρματα προϊόντα επειδή δεν θα πρέπει να επενδύσουν μεγάλα χρηματικά ποσά στους τομείς της έρευνας και ανάπτυξης των προϊόντων. Αυτές οι επενδύσεις ήδη θα έχουν γίνει και θα έχουν ενσωματωθεί μέσα στα πρότυπα, τα οποία θα είναι διαθέσιμα σε κάθε ενδιαφερόμενο που επιθυμεί να εγκαταστήσει ασύρματα δίκτυα.

Κεφάλαιο 3ο

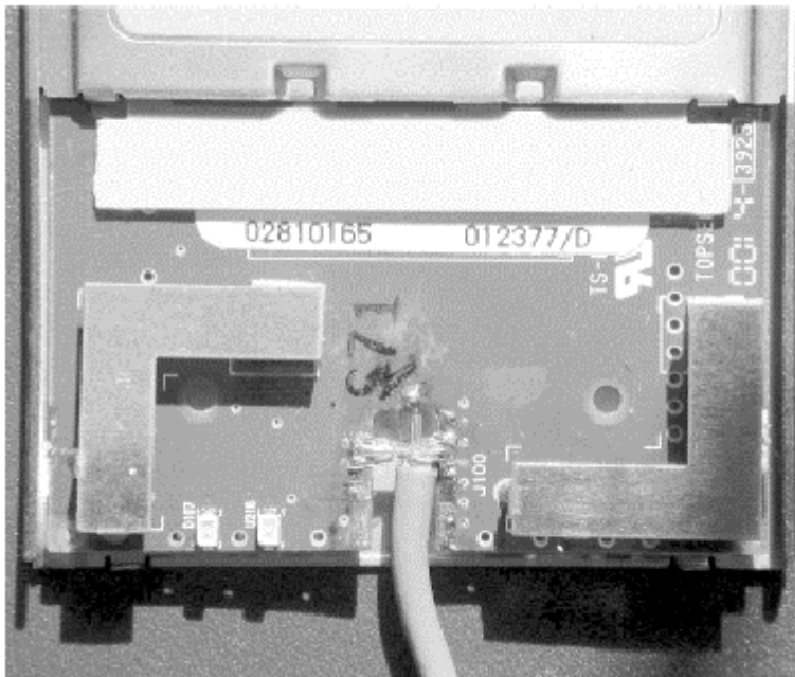
3.1 Γενικά

Η επιλογή κεραιών ασκεί τεράστια επίδραση στο βεληνεκές και στην αξιοπιστία του ασύρματου δικτύου. Η ειρωνεία είναι ότι όλες σχεδόν οι εξωτερικές κάρτες ασύρματης δικτύωσης τοποθετούν την κεραία 802.11b σε λάθος προσανατολισμό: Υπερβολικά λοξά και πολύ κοντά στο laptop. Σε αυτήν την θέση, το πεδίο ακτινοβολίας είναι σχεδόν ευθύ πάνω-κάτω. Δυστυχώς από αυτή τη θέση χάνεται τουλάχιστον το μισό σήμα εκπομπής μειώνοντας έτσι την απόδοση του δικτύου ενώ παράλληλα δημιουργούνται προβλήματα αλληλεπίδρασης της κεραίας με τον υπολογιστή. Αξιοσημείωτη εξαίρεση σε αυτήν την παρούσα κατάσταση είναι η ενσωματωμένη κάρτα AirPort της Apple. Η καινοτομία της συνίσταται στο γεγονός ότι περιλαμβάνεται μια ενσωματωμένη κεραία στην οθόνη LCD. Αυτό το σχέδιο βελτιώνει τις αποδόσεις του δικτύου αλλά δυστυχώς δεν υπάρχει η δυνατότητα προσθήκης μια εξωτερικής κεραίας. Η εταιρεία IBM είναι η πρώτη που μιμείται αυτήν την τεχνολογία ενσωματώνοντας κάρτες ασύρματης δικτύωσης στη σειρά ThinkPad. Μάλιστα με την προσθήκη εξωτερικής κεραίας και τον σωστό προσανατολισμό της επιτυγχάνεται απίστευτη αύξηση της απόδοσης του ασύρματου δικτύου. Ποιος όμως είναι ο κατάλληλος τρόπος προσανατολισμού της κεραίας; Αυτό εξαρτάται από το περιβάλλον στο οποίο θα λειτουργήσει το δίκτυο. Καλό είναι να γίνεται πρώτα μια μέτρηση της ισχύς των σημάτων σε κάθε πιθανή θέση και έπειτα να γίνεται η εγκατάσταση της κεραίας. Ο καλύτερος προσανατολισμός της κεραίας είναι πάντα η θέση στην οποία λαμβάνει το καλύτερο σήμα, έτσι δεν θα πρέπει κανείς να διστάσει να μετακινήσει την κεραία γύρω στο χώρο σε συνάρτηση πάντα με κάποια εφαρμογή μέτρησης σήματος. Οφείλει ο χρήστης να πετύχει το μέγιστο δυνατό σήμα γι' αυτό το λόγο οι δοκιμές είναι απαραίτητες. Προτού ο χρήστης αποφασίσει να αγοράσει εξωτερική κεραία, καλό θα είναι να ελέγξει εάν η κάρτα ασύρματης δικτύωσης έχει υποδοχή για εξωτερική κεραία. Πολλοί κατασκευαστές για να μειώσουν τα κόστη παραγωγής αποφεύγουν να βάλουν το ανάλογο βύσμα. Επίσης υπάρχουν στην αγορά διάφοροι τύποι βυσμάτων με αποτέλεσμα να είναι απαραίτητη η προσεκτική επιλογή των καλωδίων.



Σχήμα 3.1. Pigtail

Για να συνδεθεί η εξωτερική κεραία με την κάρτα ασύρματης δικτύωσης είναι απαραίτητο ένα καλώδιο το οποίο ονομάζεται pigtail. Το καλώδιο φαίνεται στο **Σχήμα 3.1**. Είναι δυνατή η αποφυγή αγοράς αυτού του καλωδίου. Αυτό προϋποθέτει ειδικές γνώσεις ηλεκτρολογίας έτσι ώστε να συνδέσει ο ίδιος ο χρήστης τις υποδοχές όπως φαίνεται στο Σχήμα 3.2.



Σχήμα 3.2. Σύνδεση με τη συσκευή προς αποφυγή χρήσης pigtail.

Η επιλογή του σωστού pigtail είναι σημαντική διαδικασία διότι κάθε κατασκευαστής έχει τις δικές του ιδιαιτερότητες. Άξιο αναφοράς αποτελεί η ιδιαίτερη ευπάθεια του pigtail. Ειδικά όταν χρησιμοποιείται σε laptop όπου οι χώροι είναι πολύ στενοί και είναι πιθανόν να καταστρέφουν οι συνδέσεις του. Σημαντικό στοιχείο στη διασύνδεση 2 σημείων είναι το Line of Sight (LOS). Σε εσωτερικές συνδέσεις μπορεί να μην διαδραματίζει σημαντικό ρόλο, αλλά σε εξωτερικές συνδέσεις και μάλιστα σε μακρινές αποστάσεις, αποτελεί κρίσιμο παράγοντα. Το LOS συνίσταται στο εάν υπάρχει οπτική επαφή μεταξύ του σημείου πρόσβασης και του σταθμού ή 2 σταθμών

εάν έχουμε point to point σύνδεση. Ο ενδεικτικός τρόπος σύνδεσης είναι οι κεραίες να βρίσκονται σε μεγάλο ύψος μακριά από παρεμβολές και φυσικά εμπόδια.

Το μεγαλύτερο πρόβλημα στις εξωτερικές συνδέσεις είναι τα δέντρα και τα ψηλά κτίρια. Για την επιλογή του κατάλληλου σημείου τοποθέτησης της κεραίας πρέπει να ληφθεί υπόψη η ισχύς του σήματος και οι καιρικές συνθήκες. Οι ακατάλληλες καιρικές συνθήκες μπορούν να προκαλέσουν ανεπανόρθωτες βλάβες.

3.2 Κεραίες

3.2.1 Γενικά

Οι κεραίες δεν αυξάνουν την αρχική ισχύ του σήματος. Οι ενισχυτές έχουν αυτή τη δυνατότητα. Εάν τοποθετηθεί σωστά η κεραία είναι εφικτό να επιτευχθεί η μέγιστη δυνατή ισχύ που το σύστημα παρέχει. Το σήμα εκπομπής και λήψης δεν ενισχύεται, απλά η δέσμη των ραδιοκυμάτων γίνεται πιο συμπαγής. Η συγκέντρωση ενός φακού δίνει μια φωτεινότερη ακτίνα που καλύπτει μια μικρότερη συνολικά περιοχή και, επιπλέον, περισσότερες κατευθυντικές κεραίες δίνουν ένα ισχυρότερα αντιληπτό σήμα σε έναν μικρότερο χώρο. Όλες οι κεραίες είναι κάπως κατευθυντικές, και το μέτρο της κατευθυντικότητας τους αναφέρεται ως κέρδος (gain). Χαρακτηριστικά, όσο υψηλότερο είναι το κέρδος, τόσο καλύτερη είναι η σειρά (στην κατεύθυνση που η κεραία ακτινοβολεί καλύτερα).

Υπάρχουν τέσσερις διαφορετικοί γενικοί τύποι κεραίων κατάλληλων για τη χρήση 2.4GHz. Κάθε εργασία απαιτεί ειδικού τύπου κεραία και καμία κεραία δεν είναι κατάλληλη για όλες τις εργασίες. Είναι απαραίτητο να μελετηθούν οι συνθήκες που επικρατούν τοπικά σε συνάρτηση με την επιθυμητή εργασία έτσι ώστε να καταλήξει κανείς στον κατάλληλο τύπο κεραίας. Παρακάτω περιγράφονται οι πιο κοινοί τύποι κεραίας.

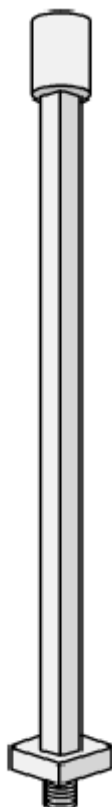
3.2.2 Omni

Οι Omnidirectionals (ή omnis), που παρουσιάζονται στο παρακάτω σχήμα, εκπέμπουν εξωτερικά εξίσου σε όλες τις οριζόντιες κατευθύνσεις κατά προσέγγιση. Για να γίνει αντιληπτό αυτό θα πρέπει κανείς να φανταστεί ένα τεράστιο donut που αναπτύσσεται γύρω από τον κεντρικό πόλο μιας κεραίας τύπου Omni. Με αυτό μοιάζει το σχέδιο εκπομπής του σήματος. Αυτού του τύπου η κεραία είναι καλή για την κάλυψη μιας μεγάλης περιοχής όπου δεν είναι γνωστή η κατεύθυνση που θα προέλθουν οι πελάτες. Το μειονέκτημα της είναι ότι λαμβάνει τον θόρυβο από κάθε κατεύθυνση, έτσι δεν είναι τόσο αποδοτικές όσο οι κατευθυντικές κεραίες. Τέτοιου είδους κεραίες χρησιμοποιούνται όταν απαιτείται να καλυφθούν περιοχές εύρους 360 μοιρών, αυτές έχουν σχετικά μικρό κέρδος (gain) (περίπου 3-10 dBi), όμως στο κατακόρυφο επίπεδο έχουν σχετικά περιορισμένο εύρος (περίπου 5-6 μοίρες).

Μοιάζουν με ψηλούς, λεπτούς πόλους, κυμαίνονται από το ένα έως πέντε πόδια ύψος, και τείνουν να είναι ακριβές. Όσο μακρύτερες είναι, τόσο περισσότερα στοιχεία έχουν (και συνήθως περισσότερο κέρδος και υψηλότερη τιμή). Τοποθετούνται κάθετα, όπως ένα ραβδί που κοιτάει προς τον ουρανό.

Κερδίζουν στον οριζόντιο, εις βάρος της κατακόρυφου. Αυτό σημαίνει ότι η χειρότερη θέση είναι ο σταθμός να είναι τοποθετημένος ακριβώς από κάτω από την

omni. Η κάθετη απόκρυση βελτιώνεται εντυπωσιακά όταν απομακρυνόμαστε από την κεραία.



Σχήμα 3.3. Κεραία Omni

3.2.3 Sector

Η κεραία Sector έχει τη μορφή της omni αρκεί να προστεθεί ένας καθρέφτης από πίσω. Οι τομείς εκπέμπουν προς μια κατεύθυνση, με μια ακτίνα τόσο ευρεία όσο 180 βαθμοί, ή τόσο στενή όσο 60 βαθμοί (ή ακόμα και λιγότερους). Υπερέχουν στις point-to-multipoint εφαρμογές, όπου διάφοροι πελάτες έχουν πρόσβαση στο ασύρματο δίκτυο από την ίδια κατεύθυνση.

Οι κεραίες sector (που παρουσιάζονται στο παρακάτω σχήμα) παρέχονται σε ποικίλες συσκευασίες, από τα ισωμένα omnis (ψηλά, λεπτά, και ορθογώνια) σε μικρά, επίπεδα τετράγωνα ή σε κύκλους. Μερικές έχουν διαγώνιο μόνο οκτώ ίντσες και τοποθετούνται επίπεδα ενάντια σε έναν κάθετο τοίχο ή σε έναν στροφέα. Μπορούν επίσης να τοποθετηθούν πάνω στο ταβάνι μιας αίθουσας συνεδριάσεων ή ενός μεγάλου δωματίου. Όπως με τις omni, το κόστος είναι συνήθως ανάλογο ως προς το κέρδος.

Οι κεραίες τύπου Sector βρίσκουν εφαρμογές στην κάλυψη περιοχών με μεγάλο εύρος, αυτό πραγματοποιείται διαιρώντας τις περιοχές αυτές σε μικρότερου εύρους κυψέλες. Οι κεραίες αυτού του είδους έχουν εύρος στο οριζόντιο επίπεδο που

συνήθως παίρνει μία τιμή, αλλά είναι δυνατόν να πάρουν και περισσότερες (με παρέμβαση στον εξοπλισμό της κεραίας), όπως 30, 45, 60, 90, 120, 180 μοίρες. Στο κατακόρυφο επίπεδο έχουν εύρος εκπομπής 5-6 μοίρες. Γενικά ισχύει ότι όσο μικρότερο είναι το εύρος εκπομπής στο οριζόντιο επίπεδο, τόσο μεγαλύτερο είναι το αντίστοιχο στο κατακόρυφο επίπεδο. Οι κεραίες αυτές βρίσκουν εφαρμογές ως επί το πλείστον σε σταθμούς βάσης, δηλαδή σε κεντρικά σημεία του δικτύου.



Σχήμα 3.4. Κεραία Sector

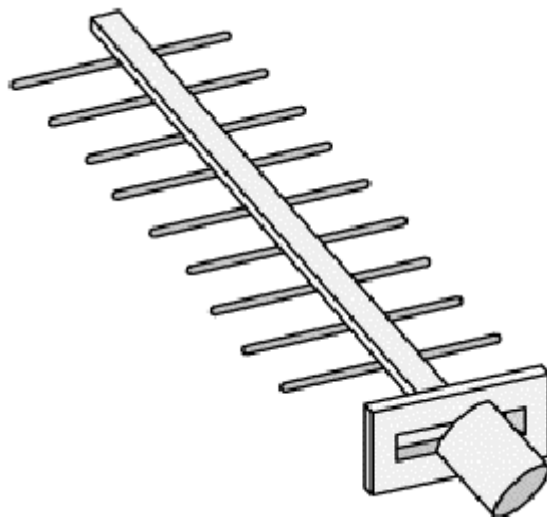
3.2.4 Yagi

Μια κεραία τύπου yagi μοιάζει με μια παλαιά κεραία τηλεόρασης. Αποτελείται από ένα τμήμα μετάλλου με μια δέσμη από οριζόντιες δοκίδες ή είναι ένας μακρύς σωλήνας με μια δέσμη δακτυλίων κατά μήκος του μήκους του. Το χαρακτηριστικό πλάτος των ακτινών μπορεί να ποικίλλει από 15 βαθμούς έως και 60, ανάλογα με τον τύπο της κεραίας. Όπως με τις omnis, όταν προσθέτουν περισσότερα στοιχεία σημαίνει περισσότερο κέρδος, μια μακρύτερη κεραία, και ασφαλώς υψηλότερο κόστος. Αυτές τις χρησιμοποιούμε όταν θέλουμε να καλύψουμε μεσαίες αποστάσεις .

Οι κεραίες αυτού του τύπου έχουν εύρος 25 μοιρών περίπου στο οριζόντιο και στο κατακόρυφο επίπεδο και το κέρδος τους είναι περίπου 10-14 dBi. Ατυχώς οι κεραίες αυτές είναι πολύ ακριβές και αρκετά ευπαθείς στις έντονες

περιβαλλοντολογικές συνθήκες όπως είναι ο πάγος. Λόγω όλων των παραπάνω δεν έχουμε συχνή χρήση αυτών.

Η οριζόντια και η κατακόρυφη πόλωση μπορεί να προκύψει με περιστροφή κατά 90 μοίρες της κεραίας .



Σχήμα 3.5. Κεραία Yagi

Μερικές κεραίες yagis είναι απλά γυμνές, όπως ένα επίπεδο χριστουγεννιάτικο δέντρο που δείχνει αόριστα προς την κατεύθυνση επικοινωνίας. Άλλοι τις τοποθετούν σε μακριά, οριζόντια δοχεία PVC. Μπορούν να λειτουργήσουν καλά σε point-to-point ή point-to-multipoint εφαρμογές, και συνήθως μπορούν να επιτύχουν υψηλότερο κέρδος από τις sector κεραίες.

3.2.5 Παραβολικό πιάτο (Parabolic dish)

Κατά κάποιο τρόπο, ένα πιάτο είναι το αντίθετο μιας omni. Αντί να γίνεται προσπάθεια να καλυφθεί ολόκληρη περιοχή, τα παραβολικά πιάτα εστιάζουν σε ένα πολύ συμπαγές διάστημα. Τα πιάτα έχουν το υψηλότερο κέρδος και την περισσότερη κατευθυντικότητα από οποιαδήποτε κεραία. Είναι ιδανικά για μια point to point σύνδεση και σχεδόν άχρηστα για τίποτ' άλλο.



Σχήμα 3.6. 24 db Parabolic dish

Τα πιάτα μπορούν να είναι στερεά ή από πλέγμα, με ελάχιστο μήκος 18 ίντσες ενώ η μέγιστη διάσταση καθορίζεται από το χρήστη (ένα πιάτο 30- ποδιών είναι δυνατό, αλλά πιθανώς ακατάλληλο). Ένα πιάτο μπορεί να στείλει σήμα σε ένα 802.11b σε απόσταση περισσότερων των 20 μιλίων. Από την άποψη του κέρδους, τα πιάτα είναι πιθανώς ο φτηνότερος τύπος κεραίας. Μερικοί άνθρωποι έχουν επιτύχει τη μετατροπή παλαιών δορυφορικών πιάτων και dss σε πιάτα 2.4GHz. Μια άλλη αξία αναφοράς ιδιότητα των κεραίων είναι η πόλωση. Η πόλωση της κεραίας αναφέρεται στην κατεύθυνση που το ηλεκτρικό μέρος του ηλεκτρομαγνητικού κύματος εκπέμπεται. Και οι οριζόντιες και οι κάθετες πολώσεις είναι κοινές, αλλά σε μερικές σπάνιες και ακριβές κεραίες, κυκλικές (δεξιόστροφα ή αντίθετα προς τη φορά των δεικτών του ρολογιού) η πόλωση είναι δυνατή. Η πόλωση της κεραίας στα άκρα κάθε σύνδεσης πρέπει να ταιριάζει, διαφορετικά οι σταθμοί θα έχουν πρόβλημα. Οι Omni κεραίες και οι sectors είναι κάθετα πολωμένες. Οι Yagis και τα πιάτα μπορούν να τοποθετηθούν κάθετα ή οριζόντια, ανάλογα με την εφαρμογή. Σε μια point to point σύνδεση, πρέπει να δοκιμαστούν και οι δύο εκδοχές ώστε να φανεί σε ποια υφίσταται χαμηλότερος θόρυβος. Η πόλωση ενός πιάτου υποδεικνύεται από τη θέση της λήψης του στοιχείου.

3.3 Χαρακτηριστικά καλωδίων και συνδέσμων

Η σύνδεση του ασύρματου πομποδέκτη με την κεραία γίνεται με ειδικά καλώδια (RF), τα οποία φέρουν κάποια ειδικά χαρακτηριστικά με σκοπό να εξασφαλίσουν την ελάχιστη δυνατή εξασθένηση του σήματος, μέχρι αυτό να φτάσει στην κεραία.

3.3.1 Σύνδεσμοι

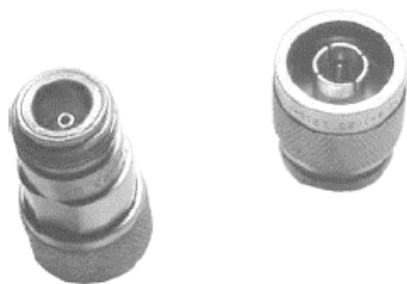
Τα καλώδια αυτά έχουν σαν κύριο χαρακτηριστικό την μείωση της εξασθένησης που υφίσταται το διερχόμενο σήμα για δεδομένη συχνότητα ή για ζώνη συχνοτήτων. Πράγμα που φαίνεται και στον παρακάτω πίνακα.

Τύπος Καλωδίου	Εξασθένηση στα 2,4 Ghz ανά 30 μέτρα (σε dB)
RG8	10
LMR400	6,8
HELIAX 3/8"	5,36
LMR600	5,4
HELIAX 1/2"	3,74
HELIAX 5/8"	2,15

Πίνακας 2: Εξασθένηση σήματος σε καλώδια RF

Όπως μπορεί να παρατηρήσει κανείς και από τον πίνακα η εξασθένηση υπολογίζεται σε dB ανά μέτρα καλωδίου. Εξέχουσας σημασίας είναι και εξαρτήματα τα οποία χρησιμοποιούνται είτε για την σύνδεση των καλωδίων, είτε για σύνδεση εξαρτημάτων μεταξύ τους.

Οι σύνδεσμοι (connectors) εμφανίζουν με την σειρά τους και αυτοί εξασθένηση στο διερχόμενο σήμα. Αυτή η εξασθένηση είναι συνήθως της τάξης των 0,25 - 0,5dB. Στην παρακάτω εικόνα παρουσιάζουμε μερικούς χαρακτηριστικούς τύπους συνδέσμων.



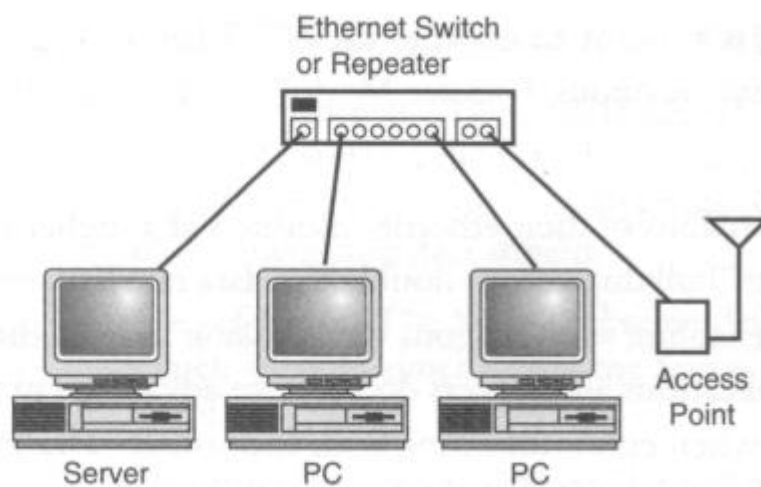
Σχήμα 3.7. Σύνδεσμοι (N-FEMALE, N-MALE).

3.3.2 Καλώδια

Μη Θωρακισμένο Ζεύγος Συννεστραμμένων Καλωδίων (UTP)

Το καλώδιο UTP χρησιμοποιεί τους μεταλλικούς αγωγούς, που παρέχουν μια πορεία για την τρέχουσα ροή που αντιπροσωπεύει τις πληροφορίες. Όπως το όνομα υπονοεί, η καλωδίωση UTP δεν περιλαμβάνει το προστατευτικό κάλυμμα που βρίσκεται με άλλες μορφές καλωδίων συννεστραμμένου ζεύγους. Το καλώδιο είναι στριμμένο ανά ζεύγη για να ελαχιστοποιήσει την ηλεκτρομαγνητική παρέμβαση η οποία είναι αποτέλεσμα των παρακείμενων ζευγαριών καλωδίων και των εξωτερικών πηγών θορύβου. Ένας μεγαλύτερος αριθμός συστροφών ανά πόδι αυξάνει την προστασία από τον θόρυβο.

Το UTP είναι οικονομικό και εύκολο να εγκατασταθεί και συγκαταλέγεται αυτήν την περίοδο στα πρότυπα της βιομηχανίας για την καλωδίωση των LANs. Η χρήση του συννεστραμμένου ζεύγους ενδείκνυται για όλες τις ενσύρματες συνδέσεις μέσα στα κτήρια. Το **Σχήμα 3.8** επεξηγεί χαρακτηριστικά την τοπολογία ενός ethernet τοπικού LAN.



Σχήμα 3.8. Χρήση καλωδίου UTP σε τοπολογία αστέρα

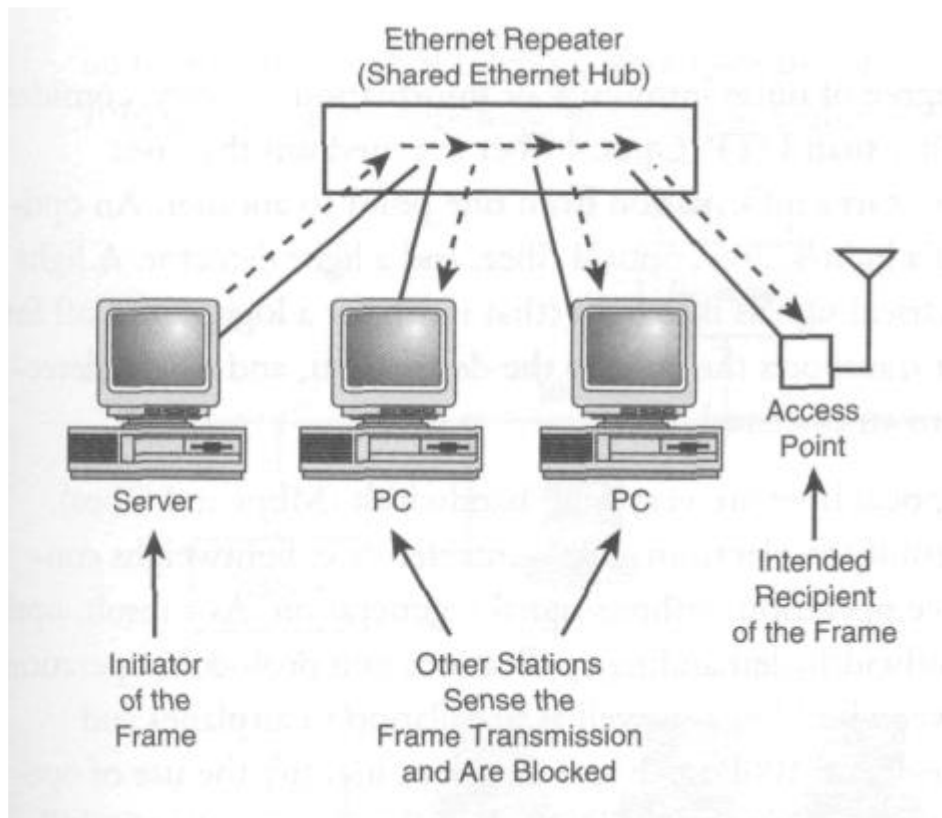
Τα ηλεκτρονικά πρότυπα που ορίζει η Αμερικάνικη Ένωση Βιομηχανικής Οικοδόμησης διευκρινίζουν τις πέντε κατηγορίες του UTP:

- Κατηγορία 1: Παλιό τηλεφωνικό καλώδιο, το οποίο δεν είναι κατάλληλο για τη μετάδοση δεδομένων. Αυτό περιλαμβάνει το μεγαλύτερο μέρος του τηλεφωνικού καλωδίου που εγκαταστάθηκε στις Ηνωμένες Πολιτείες πριν από 1983.
- Κατηγορία 2: Επικυρωμένο για χρήση με την έκδοση IEEE 802.5 των 4 Mbps για δίκτυα token-ring.

- Κατηγορία 3: Επικυρωμένο για 10 Mbps και 100Mbps του IEEE 802.3 των δικτύων ethernet. Πολλές εγκαταστάσεις που έχουν μια αρχική εγκατάσταση ενός ethernet δικτύου 10 Mbps μπορούν με ελάχιστες μετατροπές να αναβαθμιστούν στα 100 Mbps.

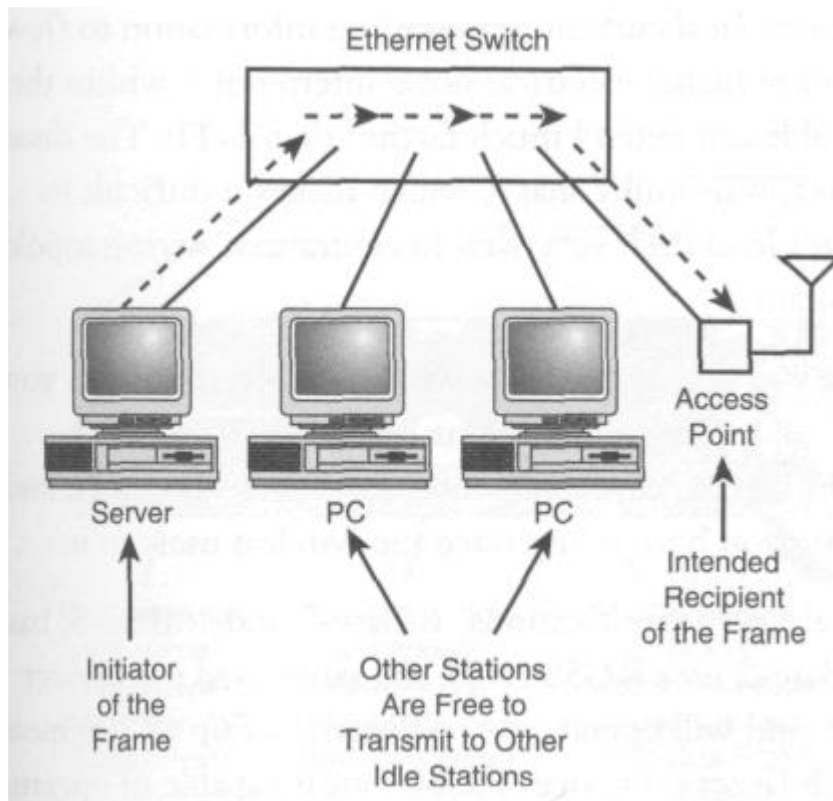
- Κατηγορία 4: Επικυρωμένο για τη χρήση με το IEEE 802.5 στα 16Mbps για δίκτυα token-ring.

- Κατηγορία 5: Επικυρωμένο για χρήση με token-ring Ansi FDDI, καθώς επίσης και σε δίκτυα ethernet IEEE802.5 με ταχύτητες 100 ή 1000Mbps. Η κατηγορία 5 είναι η δημοφιλέστερη μορφή καλωδίωσης για τα ενσύρματα δίκτυα.



Σχήμα 3.9. Χρήση καλωδίου UTP (η χρήση hub στο παραπάνω δίκτυο έχει ως αποτέλεσμα όταν μεταδίδει ένας H/Y να μην μπορούν να μεταδώσουν οι υπόλοιποι).

Ένας μεταγωγέας είναι ευφρόνιστο από ένα hub, διότι συνδέει άμεσα τον υπολογιστή-αποστολέα με τον υπολογιστή-παραλήπτη (Σχήμα 3.9). Αυτό αυξάνει σημαντικά τη ρυθμοαπόδοση. Ένα switch είναι γενικά πιο ακριβό από ένα hub, εντούτοις το switch θεωρείται ενδεδειγμένη λύση σε τοπολογίες όπως αυτή του σχήματος 20.



Σχήμα 3.10. Χρήση καλωδίου UTP (η χρήση switch στο παραπάνω δίκτυο έχει ως αποτέλεσμα όταν μεταδίδει ένας Η/Υ να μπορούν να μεταδώσουν συγχρόνως και οι υπόλοιποι).

Καλώδιο οπτικών ινών

Εάν η παντελής έλλειψη θορύβου και η υψηλή ασφάλεια των πληροφοριών είναι επιβεβλημένη, τότε η χρήση της οπτικής ίνας υπερτερεί του καλωδίου UTP. Η οπτική ίνα είναι ένα μέσο που χρησιμοποιεί τις ελαφριές αλλαγές της έντασης για να μεταδώσει πληροφορίες από ένα σημείο σε ένα άλλο. Ένα σύστημα οπτικών ινών αποτελείται από μια πηγή φωτός, μια οπτική ίνα, και έναν ανιχνευτή ακριβείας. Μια πηγή φωτός αλλάζει τα ψηφιακά ηλεκτρικά σήματα στο φως, οι οπτικές ίνες μεταφέρουν το φως στον προορισμό, και ένας ανιχνευτής ακριβείας μετασχηματίζει το φως σε ηλεκτρικό σήμα.

Τα κύρια πλεονεκτήματα της οπτικής ίνας είναι το υψηλό εύρος ζώνης (Mbps και Gbps), η ασφάλεια των πληροφοριών, η έλλειψη ηλεκτρομαγνητικής παρέμβασης, η ελαφριά κατασκευή, και η λειτουργία σε μεγάλες αποστάσεις δίχως τη ανάγκη χρήσης επαναληπτών (repeaters). Κατά συνέπεια, η οπτική ίνα είναι ανώτερη όταν οι εφαρμογές και τα πρωτόκολλα απαιτούν υψηλό εύρος ζώνης, για τη σύνδεση μεταξύ κτιρίων, καθώς επίσης και σε εγκαταστάσεις στα αεροπλάνα και τα σκάφη. Οι προδιαγραφές του προτύπου IEEE802.3 προσδιορίζουν τη χρήση της οπτικής ίνας ως φυσικό μέσο. Επίσης και το FDDI προσδιορίζει τη χρήση της οπτικής ίνας.

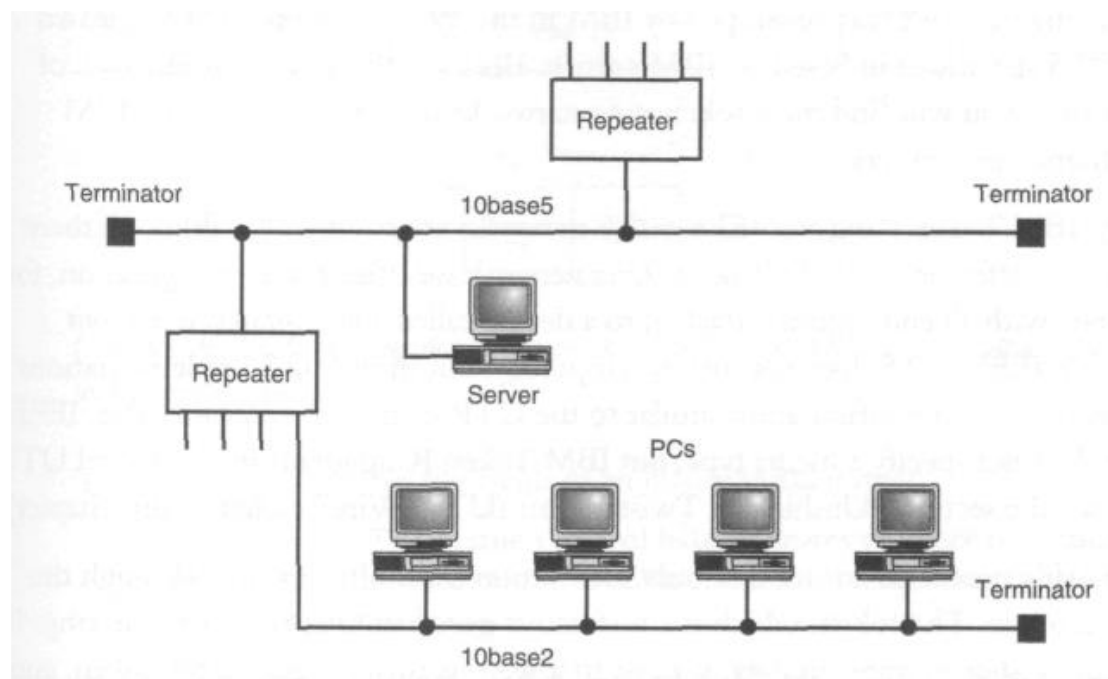
Ομοαξονικό καλώδιο

Η κατασκευή του ομοαξονικού καλωδίου περιλαμβάνει έναν στερεό μεταλλικό πυρήνα με ένα προστατευτικό κάλυμμα ο οποίος λειτουργεί ως πορεία επιστροφής και προσφέρει μια ροή για το ηλεκτρικό ρεύμα που αντιπροσωπεύει τη μετάδοση των πληροφοριών. Το προστατευτικό κάλυμμα μειώνει αποτελεσματικά τις ηλεκτρομαγνητικές παρεμβολές μέσα στον πυρήνα του καλωδίου. Κατά συνέπεια, το ομοαξονικό καλώδιο μπορεί να επεκταθεί πολύ μακρύτερα σε σχέση με το UTP. Το μειονέκτημα του ομοαξονικού καλωδίου, είναι η ογκώδης μορφή του, η οποία το καθιστά δύσκολο στην εγκατάσταση. Επίσης, το ομοαξονικό καλώδιο δεν συνίσταται για συγκεντρωτικές τοπολογίες καλωδίωσης, κάνοντας τη συντήρηση ιδιαίτερα δύσκολη.

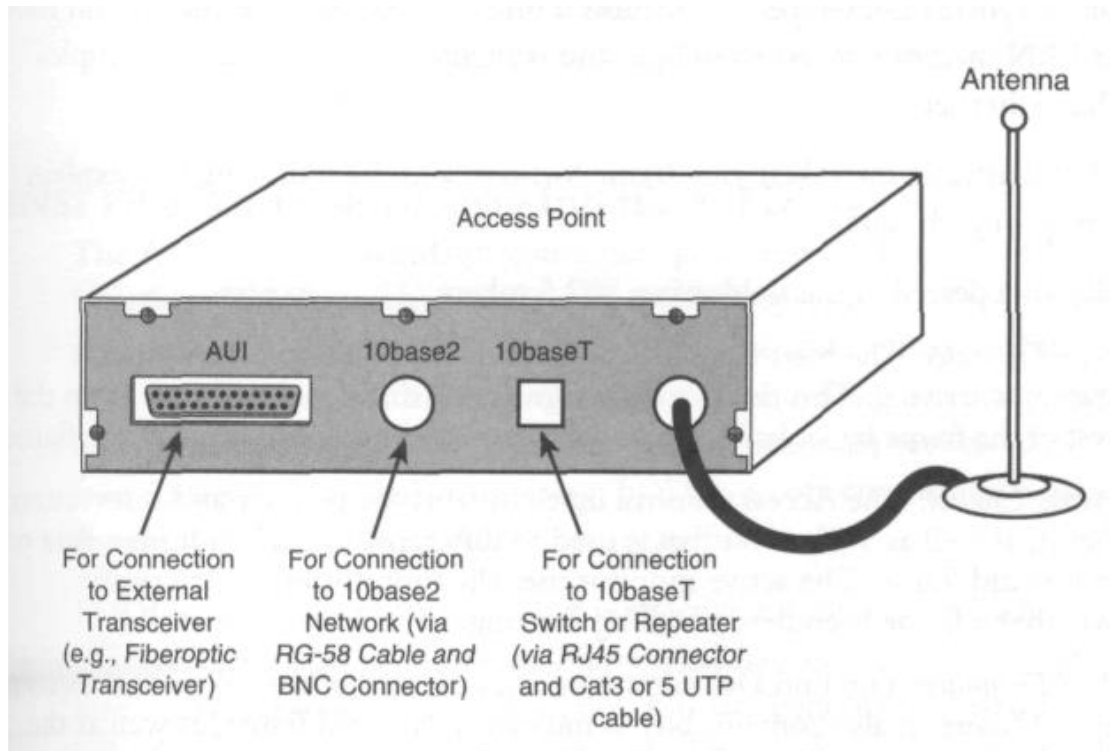
Κατά τη διάρκεια της δεκαετίας του '80, το ομοαξονικό καλώδιο ήταν πολύ δημοφιλές για την καλωδίωση δικτύων, και συναντάται ακόμα στις μέρες μας σε παλαιές εγκαταστάσεις. Ελάχιστες νέες εγκαταστάσεις απαιτούν τη χρήση του ομοαξονικού καλωδίου.

Το IEEE 802.3 καθορίζει δύο προδιαγραφές για το φυσικό επίπεδο, το 10Base-2 και το 10Base-5, τα οποία είναι βασισμένα στη χρήση του ομοαξονικού καλωδίου. Το 10Base-2 χρησιμοποιεί καλώδιο RG58, το ίδιο που χρησιμοποιείται για τη σύνδεση της τηλεόρασης με μια έξοδο καλωδίων, και λειτουργεί για μια απόσταση έως 200 μέτρα.

Το 10Base-5 χρησιμοποιεί ένα πολύ μεγαλύτερο καλώδιο σε σχέση με το RG58, αλλά είναι ικανό να λειτουργεί σε απόσταση έως και 500 μέτρα. Και το 10Base-2 και το 10Base-5 χρησιμοποιούν μια τοπολογία διαύλου, όπως φαίνεται στο σχήμα 21.



Σχήμα 3.11. Ομοαξονικό καλώδιο εάν κοπεί σε κάποιο σημείο τίθεται εκτός λειτουργίας ολόκληρο το δίκτυο.



Σχήμα 3.12. Ένα Access Point μας δίνει τη δυνατότητα να συνδεθούμε μέσω διαφόρων τύπων δικτύων Ethernet.

3.4 Κανονιστικό πλαίσιο

Σύμφωνα με το άρθρο 5 της απόφασης 254/72 της ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων), που περιέχεται στο ΦΕΚ της 16/07/2002 στον Ελλαδικό χώρο επιτρέπεται η χρήση μόνο της ISM ζώνης 2.400-2483.5 Mhz, για χρήση σε συσκευές που χρησιμοποιούν την τεχνολογία της διασποράς φάσματος.

Οι συσκευές πρέπει να είναι πλήρως εναρμονισμένες με το πρότυπο ETSI 300-328, το οποίο μεταξύ άλλων επιβάλλει και την ύπαρξη ενός μεγίστου ορίου στην ισχύ εκπομπής των εν λόγω συσκευών και ορίζει πιο συγκεκριμένα την τιμή των 20 dBm EIRP (Effective Isotropic Radiated Pattern) ως το όριο αυτό.

Στην πράξη, το EIRP αποτιμάται στην έξοδο της κεραίας. Πρόκειται για τον συνδυασμό της ισχύς εξόδου της συσκευής (ERP Effective Radiated Pattern) της ασύρματης γέφυρας, του κέρδους της κεραίας και των απωλειών του ομοαξονικού καλωδίου της σύνδεσής τους. Στην ουσία πρόκειται για το αλγεβρικό άθροισμα της ισχύς του wireless bridge, του κέρδους της κεραίας και της απώλειας του καλωδίου. Δηλαδή ισχύει ο ακόλουθος τύπος:

$$EIRPT = P_{wb} + G_a - L_c$$

όπου P_{wb} είναι η ισχύς εκπομπής της ασύρματης γέφυρας σε dBm, G_a το κέρδος της κεραίας σε dB και L_c η απώλεια του καλωδίου σε dB.

Από την παραπάνω σχέση για το παράδειγμα της προηγούμενης ενότητας προκύπτει ότι οι δύο σταθμοί A και B έχουν $EIRP = 20$ dBm.

Εδώ πρέπει να σημειώσουμε ότι τον σημαντικότερο ρόλο στο θέμα της επίτευξης της μέγιστης δυνατής απόστασης μεταξύ δύο ασύρματων μονάδων παίζει η επιλογή της κεραίας. Όσο πιο κατευθυντική είναι η τελευταία, τόσο μεγαλύτερη είναι και η απόσταση η οποία μπορεί να επιτευχθεί, καθώς και η διαθέσιμη ισχύ εκπομπής συγκεντρώνεται περισσότερο προς μία κατεύθυνση. Από τα παραπάνω βγαίνει το συμπέρασμα ότι για την επίτευξη μεγάλης απόστασης θα πρέπει να γίνει χρήση κεραίας μεγάλης κατευθυντικότητας η οποία έχει μικρό εύρος ζώνης στο οριζόντιο επίπεδο, οπότε και μεγάλο κέρδος.

Ωστόσο πρέπει να τηρηθεί ταυτόχρονα και το όριο των +20 dBm EIRP οπότε πρέπει να επιλεγεί ο σωστός συνδυασμός της ισχύος εκπομπής της ασύρματης γέφυρας και της απώλειας του καλωδίου σύνδεσης που όπως περιγράφηκε παραπάνω εξαρτάται από το μήκος και τον τύπο του.

Κεφάλαιο 4^ο

4.1 Προβλήματα ασφάλειας δικτύου

Η ασφάλεια είναι θεμελιώδες μέρος των επικοινωνιών των ασύρματων δικτύων. Είναι αρκετά ενδιαφέρον ότι αυτά τα συστήματα έχουν σχεδιαστεί, για να εξασφαλίζουν ανοιχτή πρόσβαση δια μέσου τεράστιων δικτυακών περιβαλλόντων. Οι σημερινές τεχνολογίες είναι συνήθως του τύπου παρείσφρησης της διεύθυνσης του δικτύου, συχνά περιορίζουν την συνδεσιμότητα και εμποδίζουν την εύκολη πρόσβαση σε δεδομένα και υπηρεσίες. Με την συνεχή αύξηση του πλήθους των ασύρματων δικτύων, τα ζητήματα ασφαλείας των κινητών χρηστών μπορεί να είναι πολύ πιο σημαντικά από ότι περιμένουμε. Τα αναλογικά, παραδοσιακά τηλέφωνα δεν είναι καθόλου ασφαλή. Οι σειριακοί αριθμοί των 32-bit, ο αριθμός τηλεφώνου των 34-bit και η συζήτηση σε μια τοποθεσία που αντιστοιχεί σε ένα κύτταρο κινητής τηλεφωνίας μπορούν εύκολα να εντοπιστούν από έναν δέκτη πολλαπλών συχνοτήτων. Ένα σημαντικό ζήτημα είναι η αποστολή κάποιου password ή host name μέσω ενός συστήματος. Άλλα ζητήματα ασφαλείας στα ασύρματα δίκτυα τα οποία έχουν μελετηθεί εκτενώς, είναι η ανωνυμία και η μυστικότητα τοποθεσίας στα φορητά δίκτυα, στα οποία και έχει δοθεί ιδιαίτερη σημασία τελευταία. Μια τυπική κατάσταση είναι αυτή κατά την οποία ένας χρήστης που έχει συνδράμει σε μια δεδομένη κυριότητα, ζητά υπηρεσίες όταν βρίσκεται σε μία άλλη ξένη κυριότητα. Μόνο η τοπική κυριότητα κάθε χρήστη πρέπει να ενημερώνεται για την πραγματική του ταυτότητα, δρομολόγηση και το μέρος που πιθανόν να βρίσκεται. Ένα ακόμη σημαντικό ζήτημα είναι η κλωνοποίηση των τηλεφωνικών συσκευών που αυξάνει το πλήθος των υποθέσεων σε πολλές γραμμές μεταφοράς. Μάλιστα πολλές επιχειρήσεις τηλεπικοινωνιών χάνουν πολλά χρήματα από την χρήση των κλωνοποιημένων συσκευών ή των αυθεντικών συσκευών από εισβολείς.

Ωστόσο τα ζητήματα ασφαλείας παραμένουν και είναι απαραίτητο να βρεθούν λύσεις για τις επόμενες γενιές των ασύρματων δικτύων. Συμπερασματικά υπάρχει μεγάλο ενδιαφέρον τελευταία συσκευών που θα χρησιμοποιούν νέες τεχνολογίες. Η αλήθεια όμως είναι ότι μέχρι σήμερα μηδαμινή είναι η δουλειά που έχει γίνει για λογισμικό τέτοιου είδους. Για να καταπολεμήσουμε τη χρήση κλωνοποιημένων πρέπει να ελέγχουμε για ασυνήθιστες αντιγραφές. Προφανώς έχουν γνώση πως μία αυθεντική συσκευή δεν είναι δυνατόν να βρίσκεται σε δύο μέρη ταυτόχρονα. Έτσι αν η συσκευή πραγματοποιεί περισσότερες από μία κλήσεις ταυτόχρονα έχει σίγουρα δημιουργηθεί παράνομα μία συσκευή αντίγραφο. Ακόμη περισσότερο για να διαπιστώσουμε αν μία κλήση είναι εκτός των ορίων του πελάτη που την πραγματοποιεί, το παρόν λογισμικό δεν έχει κάποια αποδοτική αυτόματη διαδικασία, ώστε να προειδοποιήσει τους νόμιμους πελάτες, ότι οι εισβολείς κάνουν χρήση των δικών τους συσκευών. Στα περισσότερα συστήματα συνηθίζεται αυτή η δουλειά να γίνεται από ανθρώπινο προσωπικό. Ακόμη δεν υπάρχουν

αποτελεσματικοί τρόποι για να ελέγξουμε την ταυτότητα των εισβολέων. Τέλος γίνεται πειραματική επανόρθωση της ασφάλειας του πλαισίου εργασίας. Μερικά συστήματα υποστηρίζουν την διαδικασία με την οποία τίθενται ονόματα σε επιγραφές δια μέσω του διαδικτύου. Εντούτοις η ταυτοποίηση ενός κλώνου πραγματοποιείται μόνον στο τέλος του μήνα το οποίο δυστυχώς δεν είναι καθόλου αποδοτικό και μπορεί να οδηγήσει σε μεγάλες απώλειες για τον κομιστή.

Με το ασύρματο δίκτυο ανοίγονται πολλές νέες επιχειρησιακές ευκαιρίες οι πιο σημαντικές από τις οποίες είναι αυτές που κάνουν χρήση της location-based τεχνολογίας. Από την στιγμή που εμφανίστηκε το φορητό δίκτυο, οι εταιρίες με αντιβιοτικά (antivirus) προϊόντα έσπευσαν να προειδοποιήσουν για επιθέσεις. Ο Timemofonica ήταν από τους πρώτους ιούς που έκαναν την εμφάνισή τους μεταξύ άλλων. Ο τελευταίος ιός ήταν προγραμματισμένος, ώστε να στέλνει υβριστικά μηνύματα σε τυχαίους χρήστες κάπου στην Ισπανία. Οι ιοί είναι μία δεδομένη απειλή στις υπολογιστικές πλατφόρμες και στα ασύρματα δίκτυα τα οποία περιλαμβάνουν διεργασίες και μνήμη παρόμοια με αυτήν των μοντέρνων υπολογιστών.

4.2 802.11 τα χαρακτηριστικά γνωρίσματα ασφάλειας του 802.11

Το πρότυπο 802.11 προβλέπει αρχικά δύο χαρακτηριστικά γνωρίσματα ασφάλειας τα οποία δυστυχώς, υπολείπονται μιας αληθινά ασφαλούς λύσης. Και οι δύο λύσεις λειτουργούν με το επίπεδο σύνδεσης δεδομένων ενός δικτύου.

4.2.1 SSID – Service Set Identifier

Το SSID είναι ένα σύνολο πληροφοριών που χρησιμοποιείται για να προσδιορίσει ένα σημείο πρόσβασης στους σταθμούς που επιθυμούν να συνδεθούν προκειμένου να χρησιμοποιήσουν το ασύρματο δίκτυο. Κατά συνέπεια, το SSID δεν είναι τίποτα άλλο παρά ένα συνηθισμένο όνομα θέσης δικτύου το οποίο μοιράζονται το σημείο πρόσβασης και οι χρήστες που συνδέονται πάνω σε αυτό. Το SSID πρέπει είτε να έχει διαμορφωθεί από πριν είτε να προβάλλεται στις ασύρματες μεταδόσεις των αναγνωριστικών σημάτων. Επειδή εξ' ορισμού το SSID διαβιβάζεται με σαφήνεια στα πλαίσια αναγνωριστικών σημάτων, παρέχει πολύ μικρή ασφάλεια. Ένα μη εξουσιοδοτημένο σημείο πρόσβασης θα μπορούσε να διαβάσει το SSID από τα πλαίσια αναγνωριστικών σημάτων και ίσως να υποθέσει την ταυτότητα του νόμιμου σημείου πρόσβασης. Αυτό θα μπορούσε ενδεχομένως να επιτρέψει την υποκλοπή της κυκλοφορίας των δεδομένων των σταθμών.

4.2.2 WEP - Wired Equivalent Privacy

Σύμφωνα με τη τυποποίηση του προτύπου 802.11, το Wired Equivalent Privacy (WEP) δημιουργήθηκε με σκοπό να παρέχει την εμπιστευτικότητα. Η τελευταία είναι θεωρητικά ισοδύναμη με την αντίστοιχη εμπιστευτικότητα ενός ενσύρματου τοπικού δικτύου, το οποίο δεν υιοθετεί τις κατάλληλες εκείνες κρυπτογραφικές τεχνικές που θα ενισχύσουν την μυστικότητά του.

Το WEP στηρίζεται σε ένα μυστικό κλειδί που μοιράζονται ένας κινητός σταθμός και ένα σημείο πρόσβασης (AP). Χρησιμοποιεί την RC4 κρυπτογράφηση δεδομένων που εφευρέθηκε από την RSA Data Security. Το RC4 είναι μια συμμετρικού τύπου κρυπτογράφηση δεδομένων στην οποία χρησιμοποιείται το ίδιο κλειδί μεταβλητού μήκους, τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Με το WEP επιτρέπεται στον αποστολέα να κρυπτογραφεί το ωφέλιμο φορτίο πλαισίων δεδομένων και να το αντικαθιστά με το αντίστοιχο αρχικό ωφέλιμο φορτίο με το κρυπτογραφημένο ωφέλιμο φορτίο. Στην συνέχεια ο αποστολέας προωθεί τα κρυπτογραφημένα πλαίσια στον προορισμό τους. Τέλος τα κρυπτογραφημένα πλαίσια δεδομένων στέλνονται στον προορισμό τους. Το σύνολο

των κομματιών, των επιγραφών WEP της MAC στέλνονται στον παραλήπτη. Στην συνέχεια, ο δέκτης όπως θα περίμενε κανείς χρησιμοποιεί το κοινό κλειδί WEP, για να αποκρυπτογραφήσει το ωφέλιμο φορτίο και να ανακτήσει τα αρχικά πλαίσια δεδομένων. Το παραγόμενο πλαίσιο με το ωφέλιμο φορτίο μπορεί έπειτα να περαστεί σε ένα ανώτερο πρωτόκολλο στρώματος. Το WEP παρέχει δύο κύρια χαρακτηριστικά γνωρίσματα:

- Αρνείται την πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες οι οποίοι δεν φέρουν το κατάλληλο κλειδί WEP.
- Αποτρέπει την αποκωδικοποίηση πληροφοριών που έχουν κρυπτογραφηθεί σε ένα WLAN, χωρίς την κατοχή του κλειδιού WEP.

4.2.3 Authentication and association στο 802.11

Για να είναι σε θέση ένας ασύρματος σταθμός να χρησιμοποιεί το WLAN, πρέπει πρώτα να πιστοποιήσει την αυθεντικότητά του στο σημείο πρόσβασης. Κατά τη διαδικασία της πιστοποίησης, ο σταθμός πρέπει να συνδεθεί με ένα σημείο πρόσβασης. Μόλις εκτελέσει ένας σταθμός αυτά τα δύο βήματα, μπορεί να έχει πρόσβαση στους πόρους του WLAN. Το πρότυπο 802.11 περιγράφει δύο μεθόδους για την επικύρωση των σταθμών.

Ανοικτή επικύρωση

Με την ανοικτή επικύρωση, ο σταθμός κάνει πιστοποίηση εξ ολοκλήρου χρησιμοποιώντας ένα σαφές κείμενο. Αυτό αποτρέπει σε έναν σταθμό να επικυρωθεί και να συνδεθεί χωρίς την κατοχή του σωστού κλειδιού WEP. Με αυτόν τον τρόπο ο σταθμός δεν είναι σε θέση να διαβιβάσει ή να λάβει τα στοιχεία χωρίς το σωστό κλειδί WEP.

Κοινή βασική επικύρωση

Με την μέθοδο της κοινής βασικής επικύρωσης ένα πακέτο πρόκλησης στέλνεται προς επικύρωση στο σταθμό. Ο σταθμός πρέπει να κρυπτογραφήσει τα πακέτα χρησιμοποιώντας το κοινό κλειδί WEP και να τα στείλει μετά πίσω στο σημείο πρόσβασης. Στην περίπτωση που το πακέτο πρόκλησης κρυπτογραφήθηκε σωστά, τότε ο σταθμός επιτρέπει να πραγματοποιηθεί η σύνδεση.

Σύνδεση

Σε αυτή την φάση, μόλις λάβει εξουσιοδότηση ο σταθμός, διαβιβάζει ένα αίτημα σύνδεσης στο σημείο πρόσβασης. Εάν το αίτημα γίνει αποδεκτό, τότε ο σταθμός συνδέεται με το σημείο πρόσβασης. Εν συνεχεία το σημείο πρόσβασης

στέλνει μια απάντηση σύνδεσης πίσω στο σταθμό. Τονίζεται ότι η επικύρωση και η σύνδεση γίνονται απλώς στο στρώμα συνδέσεων δεδομένων, μεταξύ του σταθμού και του σημείου πρόσβασης. Καμία ενέργεια του χρήστη δεν εξετάστηκε στην άδεια της πρόσβασης σταθμών στο WLAN.

Η ανοικτή και κοινή βασική επικύρωση, περιλαμβάνει την επικύρωση των σταθμών σε σημεία πρόσβασης τα οποία χρησιμοποιούν τη διεύθυνση MAC του σταθμού. Αυτός ο τύπος επικύρωσης δεν εξετάζει την ταυτότητα του χρήστη. Κατά συνέπεια η κλοπή ενός laptop ή μιας κάρτας ασύρματης δικτύωσης (NIC) θα σήμαινε και την ταυτόχρονη απόκτηση πρόσβασης στο δίκτυο, αφού είναι αυτόματα και κάτοχος των WEP κλειδιών.

4.2.4 802.1X

Το πρότυπο IEEE 802.1x το οποίο στηρίζεται στο Port Based Network Access Control υιοθετήθηκε για να εξεταστούν μερικές από τις τρέχουσες ανάγκες ασφάλειας του προτύπου 802.11. Το 802.1x μας παρέχει δύο σημαντικούς μηχανισμούς.

User Authentication using EAP

Το Extensible Authentication Protocol (EAP) είναι μια μέθοδος επικύρωσης μεταξύ ενός χρήστη και ενός κεντρικού υπολογιστή επικύρωσης. Ενδιάμεσες συσκευές όπως είναι τα σημεία πρόσβασης και οι κεντρικοί δρομολογητές (routers) δεν συμμετέχουν στη συνομιλία. Εδώ σκοπός είναι η αναμετάδοση πακέτων EAP μεταξύ των συμβαλλόμενων μερών που εκτελούν την επικύρωση. Το πρότυπο 802.1x περιγράφει τον τρόπο με τον οποίο τα πακέτα EAP είναι συμπυκνωμένα και μεταφέρονται σε Ethernet πλαίσια έτσι ώστε οι διαδικασίες επικύρωσης EAP να μπορούν να κατευθυνθούν μέσω Ethernet. Το EAP υποστηρίζει πολλαπλούς μηχανισμούς επικύρωσης όπως τα σημεία πρόσβασης, οι κάρτες, τα πιστοποιητικά, η βιομετρική, η επικύρωση χρηστών κ.λπ. Συσκευές που χρησιμοποιούν το EAP δίνουν λύσεις στην ανάγκη για την ασφάλεια των MAC address.

Η έκδοση κλειδιού WEP χρησιμοποιώντας το EAP-Key Frame

Αυτό το μήνυμα επιτρέπει στο ασύρματο σημείο πρόσβασης να στείλει ένα ή περισσότερα κλειδιά WEP προς το σταθμό. Τα σημεία πρόσβασης μπορούν να στείλουν ένα μήνυμα EAP-Key οποιαδήποτε στιγμή μετά την επικύρωση για την ενημέρωση των κλειδιών WEP στο σταθμό. Αυτό επιτρέπει (αλλά δεν απαιτεί) τη διανομή των κλειδιών στα σημεία και τους σταθμούς πρόσβασης. Είναι σημαντικό να σημειωθεί ότι αυτό παρέχει έναν μηχανισμό για τη διαχείριση των WEP κλειδιών αλλά δεν περιγράφει πώς αντιμετωπίζεται. Η χρησιμοποίηση του EAP-Key Frame για την παραγωγή των κλειδιών WEP μπορεί να βοηθήσει, ώστε να μετριαστούν οι

κυριότεροι κίνδυνοι ασφάλειας στους στατικούς σταθμούς. Η υιοθέτηση του 802.1x και η χρήση του σε WLAN αποτελεί μια βελτίωση στην ασφάλεια των SSID και των στατικών κλειδιών WEP. Προκειμένου να βελτιωθεί περαιτέρω η ασφάλεια στο WLAN, η Cisco έχει αναπτύξει το EAP-Key.

Μονόδρομη εξουσιοδότηση (One Way Authentication)

Η επικύρωση WEP είναι μονόδρομη. Το σημείο πρόσβασης δεν πρέπει να επικυρώσει τον κινητό σταθμό. Αυτό μπορεί να επιτρέψει σε ένα σημείο πρόσβασης μη εξουσιοδοτημένων χρηστών να ξεγελάσει το σύστημα και να επιτύχει επικύρωση σε έναν σταθμό πρόσβασης.

Στατικά κλειδιά WEP (Static WEP Keys)

Κανένας μηχανισμός δεν καθορίζει τη βασική διανομή ή τη βασική διαπραγμάτευση. Αυτό καθιστά απαραίτητο, τα ασύρματα δίκτυα να διαμορφώνονται με τα κλειδιά WEP που ορίζει ο χρήστης. Τα διοικητικά έξοδα από αυτήν την εγγύηση διαμόρφωσης κλειδιών από τον χρήστη ουσιαστικά διασφαλίζουν ότι αυτά τα κλειδιά θα είναι σπάνια.

Αδυναμίες των κλειδιών WEP (WEP Key Vulnerability)

Πρόσφατες καταγραφές περιγράφουν μερικές επιτυχείς επιθέσεις στον αλγόριθμο WEP. Μία από αυτές τις επιθέσεις, της οποίας ο κώδικας πηγής είναι εύκολα διαθέσιμος στο διαδίκτυο, περιγράφει μια επίθεση η οποία είναι σε θέση να ανακτήσει ένα κλειδί 40-bit WEP σε 15 λεπτά με ένα συνηθισμένο laptop. Επειδή οι κλίμακες αυτής της επίθεσης στηρίχθηκαν στο βασικό μέγεθος του κλειδιού, φαίνεται πολύ καθαρά ότι ένα κλειδί των 128-bit μπορεί να ανακτηθεί μέσα σε περίπου 45 λεπτά.

4.3 LEAP - Lightweight extensible authentication protocol

Τα συστήματα της Cisco, έχουν αναπτύξει το Lightweight Extensible Authentication Protocol (LEAP). Το LEAP παρέχει δύο σημαντικά χαρακτηριστικά γνωρίσματα ασφάλειας. Αμοιβαία επικύρωση μεταξύ του σταθμού και του σημείου πρόσβασης.

Το LEAP απαιτεί την αμοιβαία επικύρωση μεταξύ των σταθμών και των σημείων πρόσβασης. Αυτό επιτρέπει σε έναν συνδεδεμένο σταθμό να ελέγξει την ταυτότητα του σημείου πρόσβασης με το οποίο προσπαθεί να συνδεθεί. Παράλληλα, το σημείο πρόσβασης πρέπει να ελέγξει την ταυτότητα του σταθμού. Ο σταθμός πρέπει να παρουσιάσει ένα όνομα χρήστη και έναν κωδικό πρόσβασης που θα πρέπει να έχει ελεγχθεί από έναν κεντρικό υπολογιστή με ενεργοποιημένο το LEAP, όπως είναι τα Interlink Networks RADSeries. Αυτή η αμοιβαία επικύρωση εξασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες επιτρέπεται να έχουν πρόσβαση στο δίκτυο αποτρέποντας την εξαπάτηση του κάθε νόμιμου χρήστη από ψεύτικους σταθμούς πρόσβασης. Η αμοιβαία επικύρωση τελειοποιεί μια μεγάλη βελτίωση στη μονόδρομη επικύρωση που περιγράφεται παραπάνω.

4.3.1 Distribution of WEP Keys on a Per-session Basis

Στην επιτυχή επικύρωση, ο αλγόριθμος LEAP παράγει δυναμικά το μοναδικό κλειδί συνόδου WEP. Η διεπαφή των δικτύων ή ο ασύρματος προσαρμογέας (NIC) του τοπικού LAN Cisco Aironet παράγει ανεξάρτητα αυτό το κλειδί. Αυτό σημαίνει ότι το κλειδί δεν διαβιβάζεται μέσω του αέρα όπου θα μπορούσε να παρεμποδιστεί. Η χρήση των WEP κλειδιών ανά σύνοδο μειώνει πολύ τη δυνατότητα του WEP κλειδιού να αποκαλυφθεί. Στην απίθανη περίπτωση που το κλειδί αποκαλύπτεται, τότε αυτό καθίσταται άχρηστο αφού έχει ολοκληρωθεί η τρέχουσα σύνοδος. Αυτό μειώνει πολύ την ευπάθεια του κλειδιού WEP που περιγράφεται παραπάνω. Η χρήση του LEAP της Cisco καλύπτει δύο αξιοσημείωτα κενά ασφάλειας των WLAN.

4.3.2 Αρχιτεκτονική LEAP της CISCO

Υπάρχουν τρία βασικά συστατικά που απαιτούνται για τη λειτουργία του LEAP.

LEAP Supplicant

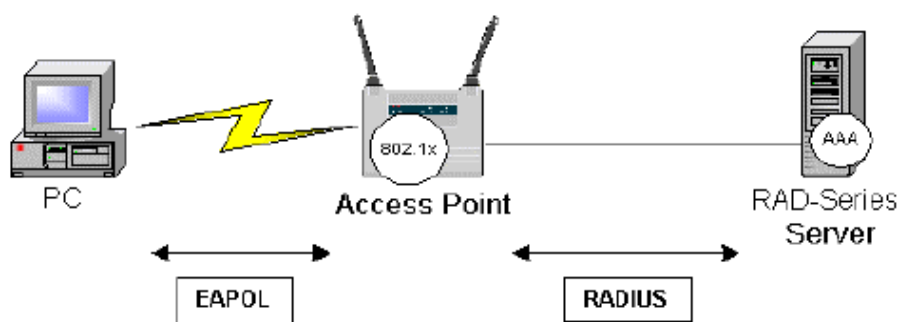
Το Supplicant είναι το λογισμικό και το firmware των πελατών που ζητούν εξουσιοδότηση στο WLAN. Το λογισμικό υπάρχει στη συσκευή των διακομιστών του προσαρμοστή του WLAN. Το Firmware υπάρχει στον προσαρμοστή της Cisco. Το LEAP supplicant μπορεί να διαμορφωθεί ώστε να αποθηκεύει το όνομα χρήστη και τον κωδικό πρόσβασης ή να προτρέπει τα πιστοποιητικά στο χρόνο σύνδεσης. Η αποθήκευση του ονόματος χρήστη και του κωδικού πρόσβασης supplicant μπορεί να είναι ένας κίνδυνος ασφάλειας αφού μια κλεμμένη συσκευή θα επέτρεπε την πρόσβαση στους πόρους των δικτύων.

802.1x Authenticator

Το authenticator είναι το λογισμικό που τρέχει στο σημείο πρόσβασης. Το authenticator ενεργεί ως ηλεκτρονόμος, διαβιβάζοντας τα μηνύματα EAP στον κεντρικό υπολογιστή επικύρωσης.

Κεντρικός υπολογιστής επικύρωσης

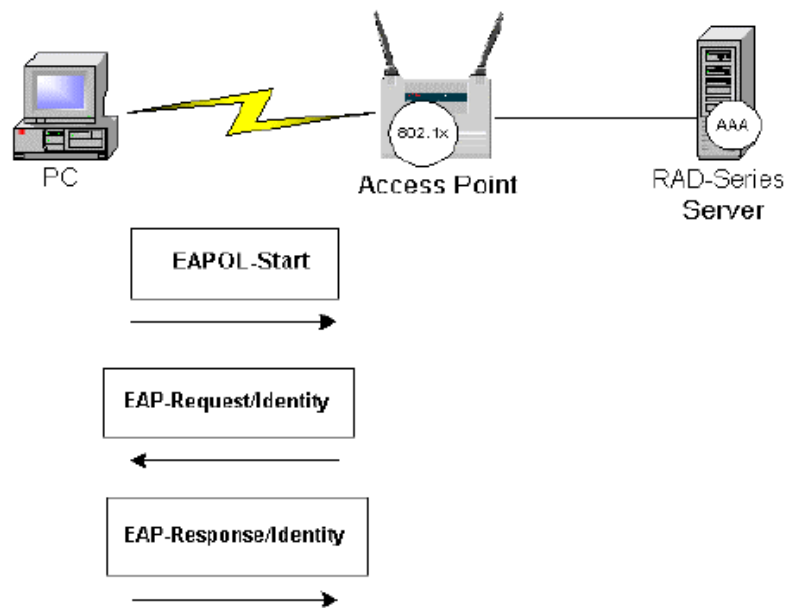
Ο κεντρικός υπολογιστής επικύρωσης είναι ένας κεντρικός υπολογιστής με το LEAP ενεργοποιημένο. Ο κεντρικός υπολογιστής επιτρέπει την επικύρωση των σταθμών βασισμένη στο όνομα χρήστη και τον κωδικό πρόσβασης.



Σχήμα 4.1. Η επικύρωση LEAP της Cisco και η βασική διαδικασία ανταλλαγής εμφανίζονται σε τρεις φάσεις.

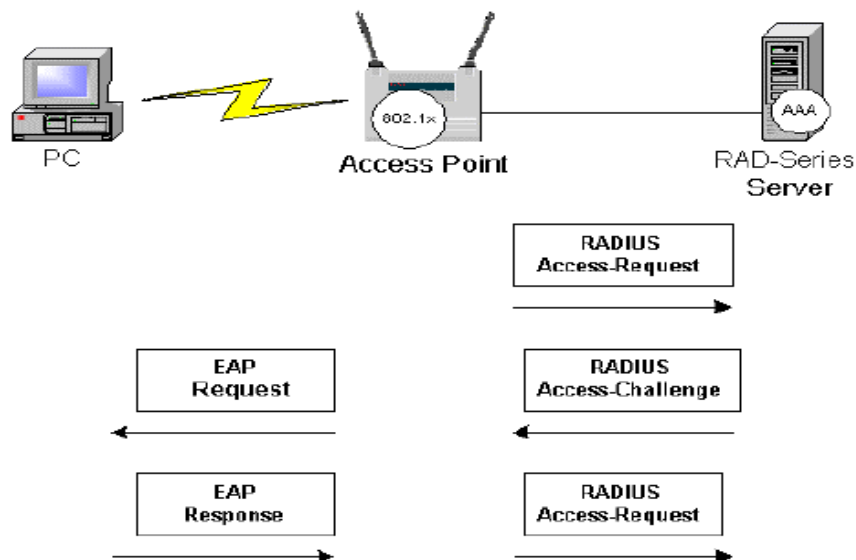
Η φάση της έναρξης

Στη φάση της έναρξης, το supplicant αρχίζει την επικύρωση με την έκδοση ενός μηνύματος EAPOL-Start προς στον authenticator. Ο authenticator αποκρίνεται προς τον supplicant με ένα μήνυμα EAPRequest/ Identity. Ο Supplicant αποκρίνεται με ένα μήνυμα EAP-Response/ Identity και παραδίδει την ταυτότητά του στο authenticator.



Σχήμα 4.2. Η φάση της επικύρωσης

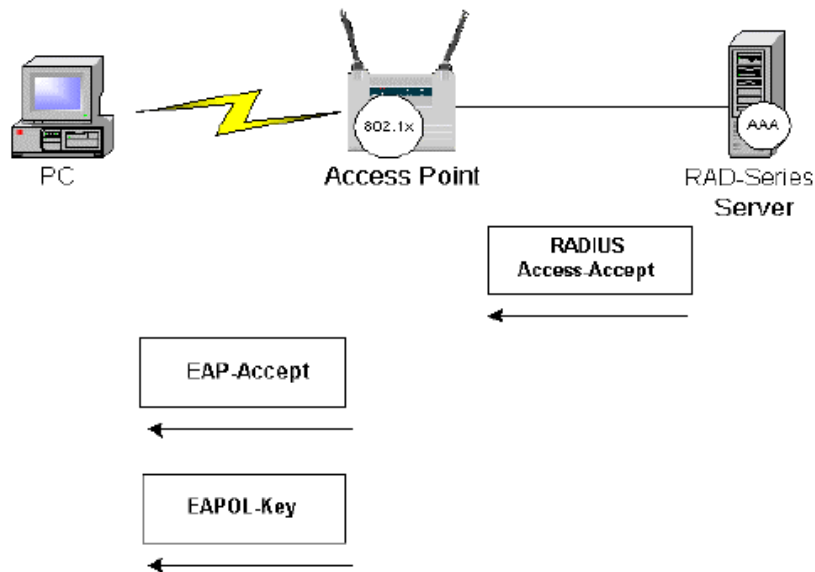
Η επικύρωση του LEAP της Cisco είναι μια αμοιβαία μέθοδος επικύρωσης. Μηνύματα ηλεκτρονόμων του EAP Authenticator αποστέλλονται στον κεντρικό υπολογιστή επικύρωσης χρησιμοποιώντας ένα μήνυμα πρόσβασης. Κατά την επικύρωση ο κεντρικός υπολογιστής αποκρίνεται με ένα μήνυμα πρόσβασης. Ο Authenticator αναμεταδίδει αυτό το μήνυμα στον supplicant ως αίτημα. Έπειτα, ο supplicant αποκρίνεται με ένα μήνυμα απάντησης που διαβιβάζεται στην επικύρωση.



Σχήμα 4.3. Η φάση του τερματισμού

Εάν ο χρήστης δεν είναι έγκυρος, ο κεντρικός υπολογιστής επικύρωσης στέλνει ένα πακέτο RADIUS Deny με ένα μήνυμα αποτυχίας του EAP. Εάν ο χρήστης είναι έγκυρος, ο κεντρικός υπολογιστής επικύρωσης στέλνει ένα πακέτο

αποδοχής RADIUS και ένα μήνυμα επιτυχίας EAP. Ο κεντρικός υπολογιστής επικύρωσης και ο supplicant είναι σε θέση να αντλήσουν ένα κλειδί από τον κωδικό πρόσβασης του χρήστη. Η βασική τεχνική παραγωγής δημιουργεί ένα πιο μακροχρόνιο κλειδί το οποίο θα χρησιμοποιηθεί για τη σύνοδο. Κατά την παραλαβή του κλειδιού από τον κεντρικό υπολογιστή επικύρωσης, ο Authenticator διαβιβάζει ένα βασικό μήνυμα EAPOL-Key στον supplicant. Αυτό το μήνυμα είναι ένα βασικό κλειδί περιεχομένου και μήκους το οποίο ο supplicant μπορεί να χρησιμοποιήσει για να υπολογίσει το κλειδί της συνόδου.



Σχήμα 4.4. Σε αυτό το σημείο, ο supplicant και ο Authenticator έχουν ένα κοινό κλειδί συνόδου που μπορεί να χρησιμοποιηθεί κατά τη διάρκεια της συνόδου.

4.4 Συστήματα ανίχνευσης εισβολών

(Intrusion Detection Systems)

Οι ανεπιθύμητες εισβολές αποτελούν ένα από τα σημαντικότερα ζητήματα των ασύρματων δικτύων, που πρέπει να αντιμετωπίσουμε. Από την φύση τους τα ασύρματα αυτά δίκτυα είναι πολύ ευαίσθητα στις εχθρικές επιθέσεις. Γενικότερα μιλώντας για μία εισβολή, μπορούμε να την προσδιορίσουμε σαν μία ενέργεια, ενός ατόμου ή μίας συνεργαζόμενης ομάδας, με σκοπό να εισέλθουν ή να προσβάλουν το επιτιθέμενο σύστημα με βίαιο και ζημιογόνο τρόπο. Πολύ λίγη είναι μέχρι σήμερα η έρευνα που έχει πραγματοποιηθεί για να καταπολεμήσει τέτοιου είδους θέματα-προβλήματα στα ασύρματα δίκτυα. Θα προσπαθήσουμε να περιγράψουμε γενικά το πρόβλημα των εισβολών. Αποτελεί ελπίδα μας ότι οι ερευνητές θα ασχοληθούν εγκαίρως με το πρόβλημα και θα μας δώσουν επιθυμητές απαντήσεις.

4.4.1 Τρέχουσες τεχνικές IDS

Μιλώντας γενικότερα τις εισβολές αυτές είναι δυνατόν να κατηγοριοποιηθούν ως εξής :

1. Κακόβουλες εισβολές, αυτές είναι καλά προγραμματισμένες επιθέσεις εναντίον επιρρεπών συστημάτων.
2. Οι συχνότερες εισβολές, στις οποίες οι ενέργειες είναι βασισμένες σε εκτροπές των κανονικών συστημάτων συνηθισμένων αντιγράφων.

Τα συστήματα εξιχνίασης εισβολών (IDS) είναι από τα τελευταία εργαλεία ασφαλείας στον αγώνα ενάντια σε αυτές τις επιθέσεις. Όπως είναι γνωστό είναι πολύ δύσκολο να αποτρέψουμε πλήρως τις επιθέσεις αυτές. Αυτού του είδους οι επιθετικές δραστηριότητες αντιμετωπίζονται με τις καλύτερες ενδεικτικές λύσεις. Γι' αυτόν τον λόγο οι ερευνητές έχουν στραφεί στο να χρησιμοποιούν συστήματα βασισμένα στα γνωστά IDS για να εντοπίσουν τις δραστηριότητες που απαιτούν συμπεριφορές εισβολής. Τα κίνητρα για αυτήν την προσέγγιση είναι να αναζητήσουμε εξαιρετικές συμπεριφορές σαν αντιστάθμιση για τις συνηθισμένες. Τα γνωστά σχήματα εξιχνίασης εισβολών απευθύνονται στην γνώση η οποία έχει συγκεντρωθεί για συγκεκριμένες επιθέσεις και στις αδυναμίες των συστημάτων. Κάνοντας χρήση αυτής της βάσης γνώσεων, κάθε ενέργεια που δεν δηλώνει σαφή επίθεση και δεν έχει αναγνωριστεί σαν τέτοια, θεωρείται αποδεκτή. Διαφορετικά ένας συναγερμός θα ενεργοποιηθεί από το σύστημα.

Υπάρχουν διάφορων ειδών συστήματα ανίχνευσης εισβολών που κυκλοφορούν στο εμπόριο . Εξειδικευμένα συστήματα βασίζονται στις ήδη γνωστές τεχνικές ανίχνευσης εισβολών. Κάθε επίθεση συντελείται από ένα σύνολο εντολών και ενεργειών. Οι γλώσσες, οι βασιζόμενες στους κανόνες αυτούς, χρησιμοποιούνται για να σχεδιάσουν ένα πλάνο γνώσεων, που οι ειδικοί έχουν συγκεντρώσει για τις

επιθέσεις. Οι πληροφορίες οι οποίες αναφέρονται σε κάποιους εισβολείς, έχουν επίσης ενσωματωθεί στα συστήματα αυτά.

4.4.2 Πλεονεκτήματα και μειονεκτήματα

Ένα μεγάλο μειονέκτημα των συστημάτων ανίχνευσης εισβολών αποτελεί η δυσκολία της συγκέντρωσης των πληροφοριών, από γνωστές επιθέσεις, για τις οποίες πρέπει να υπάρχει άμεση ενημέρωση, ώστε να αναπτυχθεί ένα περιεκτικό και πλήρες σύστημα καταπολέμησης επιθετικών συμπεριφορών. Ορισμένα συστήματα κάνουν χρήση ενός συνδυασμού, διαφόρων προσεγγίσεων, με σκοπό να καλύψουν τις συνηθισμένες, αλλά και τις εξειδικευμένες επιθέσεις. Αναφερόμαστε σε αυτά τα συστήματα εξιχνίασης, τα βασιζόμενα στις συμπεριφορές . Το βασικό τους χαρακτηριστικό είναι ότι κάθε ενέργεια η οποία δεν ταιριάζει με μία ήδη γνωστή συμπεριφορά, ενεργοποιεί τον συναγερμό. Η ενέργεια λαμβάνεται σαν μία εχθρική εισβολή. Από την άλλη μεριά τα κύρια πλεονεκτήματα των συστημάτων αυτών είναι ότι μπορούν να αντιλαμβάνονται τις νέου τύπου αλλά και τις απρόβλεπτες επιθέσεις και να συνδράμουν αυτομάτως, ενεργοποιώντας τα συστήματα ασφαλείας. Ωστόσο η μεγάλη συχνότητά τους για ψευδείς συναγερμούς αποτελεί ένα από τα βασικά μειονεκτήματα των συστημάτων αυτών, πράγμα το οποίο αποδίδεται βασικά στην ακρίβεια της συμπεριφοράς πληροφόρησης, η οποία συγκεντρώνεται κατά την διαδικασία της εκμάθησης.

4.5 Προστασία της μεταδιδόμενης πληροφορίας στα ψηφιακά κινητά συστήματα .

Όλα τα ψηφιακά κινητά συστήματα προωθούν την ασφάλεια δια μέσου κάποιου είδους απόκρυψης. Η πληροφορία είναι δυνατόν να διασφαλιστεί με πολλούς τρόπους, ωστόσο για την ασφάλιση της μεταδιδόμενης πληροφορίας γίνεται χρήση δύο τρόπων, των συμμετρικών και των ασύμμετρων. Και οι δύο αυτοί τρόποι βασίζονται στην εκτέλεση μαθηματικών διαδικασιών, χρησιμοποιώντας κρυφούς αριθμούς, γνωστούς σε όλους μας σαν κλειδιά (keys). Η δυσκολία με τους συμμετρικούς αυτούς αλγόριθμους είναι πως και τα δύο άκρα πρέπει να έχουν γνώση του εν λόγω κωδικού κλειδιού. Από την άλλη μεριά οι ασύμμετρες τεχνικές κάνουν χρήση δύο επιμέρους κλειδιών για κωδικοποίηση και αποκωδικοποίηση. Συνήθως, το κλειδί της κωδικοποίησης μπορεί να διανέμεται δημοσίως, δεδομένου ότι το κλειδί της αποκωδικοποίησης διαφυλάσσεται ασφαλώς από τον αποδέκτη.

Ο πιο ευρέως χρησιμοποιούμενος συμμετρικός αλγόριθμος ονομάζεται DES (data encryption standard) και αναπτύχθηκε από την IBM στα 1977. Κάνει χρήση ενός κωδικού των 56-bit ο οποίος για τα δεδομένα της εποχής του ήταν αδύνατον να αποκρυπτογραφηθεί. Μία ομάδα χρηστών του διαδικτύου δύναται να χρησιμοποιήσει ένα DES κωδικοποιημένο μήνυμα. Ως εκ τούτου οι περισσότεροι οργανισμοί σήμερα χρησιμοποιούν το triple-DES το οποίο κάνει χρήση ενός αριθμού των 112-bits. Η βασική ιδέα είναι ότι τα μεγαλύτερα κλειδιά, μπορούν να σημαίνουν περισσότερους συνδυασμούς και οπότε καλύτερη κωδικοποίηση. Με GSM κωδικοποιούνται όλα τα δεδομένα μεταξύ των συνδρομητών και του σταθμού χρησιμοποιώντας έναν κώδικα που λέγεται A5. Οι λεπτομέρειες για τον κώδικα αυτό κρατούνταν κρυφές, ώστε να είναι δυσκολότερος στο "σπάσιμο". Δυστυχώς όμως, οι λεπτομέρειες αυτές διέρρευσαν με την πάροδο του χρόνου και κοινοποιήθηκαν από τους hackers και τους crackers στο διαδίκτυο. Για τον λόγο αυτό κρίνεται απαραίτητη η συνεχής δουλειά, μα σκοπό την ασφάλεια και προστασία των δεδομένων.

Διάφοροι ασύμμετροι αλγόριθμοι έχουν αναπτυχθεί, καθένας από αυτούς χρησιμοποιεί και έναν διαφορετικό τύπο μαθηματικής συνάρτησης. Έχει προταθεί ένας αποδοτικός αλγόριθμος που βασίζεται στο γεγονός ότι ο παραγοντισμός είναι καλύτερος από τον πολλαπλασιασμό. Πράγματι το να πολλαπλασιαστούν δύο αριθμοί από έναν υπολογιστή είναι εύκολη υπόθεση, αλλά η ανάκτηση αυτών των αριθμών από το προϊόν δεν είναι. Το μεγάλο μειονέκτημα των ασύμμετρων σχημάτων είναι ότι απαιτούν μεγάλη χρήση της CPU και δεν είναι δυνατόν να χρησιμοποιηθούν για κωδικοποίηση μεγάλων μηνυμάτων. Αντιθέτως με την τεχνική A5 το μήνυμα κωδικοποιείται με συμμετρικό αλγόριθμο και ένα κωδικό που διαλέγεται τυχαία από το δίκτυο και αποστέλλεται στην συσκευή που χρησιμοποιεί τον ασύμμετρο αλγόριθμο.

4.6 Ασφαλίζοντας τα ασύρματα δίκτυα AD HOC

Πολλά LANs που χρησιμοποιούνται σήμερα χρειάζονται εξειδικευμένη δικτυακή υποδομή. Η υποδομή των δικτύων δεν προωθεί μόνο την πρόσβαση σε άλλα δίκτυα, αλλά περιλαμβάνει επίσης τους ενδιάμεσους ελέγχους πρόσβασης κλπ. Σε αυτά τα ασύρματα δίκτυα, τυπικά η επικοινωνία λαμβάνει χώρα μόνο ανάμεσα σε ασύρματους κόμβους και σημεία πρόσβασης, αλλά όχι απ' ευθείας ανάμεσα σε ασύρματους κόμβους (nodes). Ωστόσο τα ad hoc ασύρματα δίκτυα δεν χρειάζονται καμία υποδομή για να τεθούν σε λειτουργία. Ο κάθε κόμβος έχει την δυνατότητα να επικοινωνεί με κάποιον άλλο κόμβο, χωρίς την παρεμβολή κάποιου σημείου πρόσβασης μεταξύ των να είναι απαραίτητη.

Οι κόμβοι μέσω μίας συχνότητας επικοινωνούν απ' ευθείας με ασύρματους συνδέσμους, δεδομένου ότι βρίσκονται μακριά μεταξύ τους βασίζονται σε άλλους κόμβους, οι οποίοι θα αναμεταδώσουν τα μηνύματα, λειτουργώντας σαν δρομολογητές (routers). Η κινητικότητα των κόμβων σε ένα ad hoc δίκτυο προκαλεί πολύ συχνές αλλαγές όσον αφορά την τοπολογία του εν λόγω δικτύου. Αφού ένα ad hoc ασύρματο δίκτυο μπορεί να αναπτυχθεί ραγδαία, με σχετικά μικρό κόστος, αποτελεί μία πολύ ελκυστική επιλογή για εμπορικούς σκοπούς, όπως ευαίσθητα δίκτυα ή εικονικές αίθουσες διδασκαλίας. Ωστόσο πριν ένα ad hoc δίκτυο γίνει εμπορεύσιμο, διάφορα ζητήματα ασφαλείας πρέπει να εξετασθούν και να επιλυθούν. Από την μία μεριά οι ευαίσθητες εφαρμογές ασφαλείας ενός ad hoc δικτύου απαιτούν έναν πολύ υψηλό βαθμό ασφαλείας. Από την άλλη μεριά τα ad hoc δίκτυα είναι εξοπλισμένα με μηχανισμούς που αντιλαμβάνονται τις επιθέσεις κατά τις ασφάλειας του δικτύου. Επομένως οι μηχανισμοί ασφαλείας γίνονται αναγκαία για τα ad hoc δίκτυα και αναπόσπαστα μέρη αυτών.

Όπως σε κάθε ασύρματο και ενσύρματο δίκτυο, η κυκλοφορία σε ένα ad hoc δίκτυο είναι ευαίσθητη σε επιθέσεις που αφορούν την ασφάλεια. Για τον λόγο αυτό, με σκοπό να ασφαλίσουμε ένα ad hoc δίκτυο, πρέπει να λάβουμε υπ' όψιν μας όχι μόνο χαρακτηριστικά που αναφέρονται στην τρίτη ενότητα αυτού του κεφαλαίου όπως είναι η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα, η πιστοποίηση και εξασφάλιση πληρωμής, αλλά και τις απειλές τις οποίες επεκτείνονται ακόμη και στην βασική δομή των δικτύων. Τα αξιοπρόσεκτα χαρακτηριστικά των ad hoc δικτύων προσφέρουν τόσο τις προκλήσεις όσο και τις ευκαιρίες στην επίτευξη αυτών των σκοπών. Από την στιγμή που ένα ad hoc δίκτυο κάνει χρήση ασύρματων συνδέσμων γίνεται επιρρεπές σε επιθέσεις μέσω συνδέσμων.

Υπάρχουν δύο ειδών επιθέσεις. Οι παθητικές επιθέσεις αρκούνται στην υποκλοπή των μηνυμάτων. Από την άλλη μεριά οι ενεργητικές τροποποιούν και καταστρέφουν μηνύματα, δημιουργούν παρεμβολές και προκαλούν κατάρρευση του συστήματος. Σε ακόμα πιο ακραίες περιπτώσεις υποκαθιστούν τους νόμιμους κόμβους δημιουργώντας έτσι τεράστια προβλήματα.

4.7 Ανίχνευση εισβολής στα ασύρματα δίκτυα ad hoc .

Τα περισσότερα από τα συστήματα ανίχνευσης εισβολών (IDS), που αναπτύχθηκαν για ενσύρματα δίκτυα μπορούν επίσης να αναφέρονται και σε ασύρματα δίκτυα. Αυτό συμβαίνει κυρίως λόγω του ότι σήμερα τα συστήματα ανίχνευσης εισβολών βασίζονται σε ανάλυση σε πραγματικό χρόνο και δεν είναι δυνατόν να λειτουργήσουν σε ασύρματα περιβάλλοντα, όπως είναι τα ασύρματα δίκτυα ad hoc. Πραγματοποιώντας μία σύγκριση, μεταξύ των ενσύρματων και των ασύρματων ad hoc δικτύων, στα οποία η κυκλοφορία που παρακολουθείται, συνηθίζεται να γίνεται σε διάφορους μεταγωγούς (switches), δρομολογητές (routers) και ανοίγματα θυρών, συμπεραίνουμε ότι ένα ασύρματο ad hoc δίκτυο δεν έχει σημεία συγκέντρωσης διακίνησης στα οποία ένα σύστημα ανίχνευσης εισβολών να μπορεί να συλλέγει πληροφορίες για ολόκληρο το δίκτυο. Υπενθυμίζοντας ότι σε ένα ασύρματο δίκτυο ad hoc, κάθε κόμβος έχει την δυνατότητα να επικοινωνεί με έναν άλλον κόμβο, χωρίς κανέναν ενδιάμεσο έλεγχο από κάποιο σημείο πρόσβασης (access point) να είναι απαραίτητο. Οι κινητοί κόμβοι βρίσκονται ο καθένας στο πεδίο συχνότητας του άλλου και ως εκ τούτου επικοινωνούν απ' ευθείας, μέσω ασύρματων συνδέσμων (links), δεδομένου ότι μεταξύ αυτών που βρίσκονται μακριά βασίζουν την επικοινωνία τους σε άλλους κόμβους, για την μεταβίβαση μηνυμάτων, οι οποίοι στην προκειμένη περίπτωση παίζουν τον πόλο των δρομολογητών (routers).

Προσφάτως έχουν εξετασθεί οι αδυναμίες και το κατά πόσο είναι ευάλωτο ένα δίκτυο ad hoc. Έχει περιγραφεί ένας μηχανισμός ανίχνευσης και θετικής απόδοσης. Σε αυτήν την προσέγγιση λοιπόν των δύο ερευνητών Zhang και Lee, κάθε κόμβος θεωρείται υπεύθυνος για την αναζήτηση σημάτων για τοπικές εισβολές ανεξαρτήτως, αλλά οι γείτονες κόμβοι έχουν την δυνατότητα της συνεργασίας και εξιχνίασης σε ευρύτερο φάσμα. Ιδιαίτεροι παράγοντες συστημάτων ανίχνευσης εισβολών βρίσκονται σε κάθε κόμβο ξεχωριστά. Κάθε τέτοιος παράγοντας συστήματος υπάρχει ανεξάρτητα και παρακολουθεί τοπικές δραστηριότητες, όπως δραστηριότητες συστήματος-χρηστών, δραστηριότητες επικοινωνίας κλπ. Αυτοί οι παράγοντες των συστημάτων αναπτύσσονται συλλεκτικά από το σύστημα , με σκοπό την προστασία του δικτύου ad hoc από εχθρικές επιθέσεις. Αν ένας παράγοντας ενός συστήματος εξιχνίασης εισβολών, διαπιστώσει μια εισβολή από τοπικά σε αυτόν δεδομένα, τότε οι γειτονικοί παράγοντες θα συνεργαστούν για την ανεύρεση ενεργειών εισβολών στην ευρύτερη, του συγκεκριμένου κόμβου, περιοχή. Οι ανταποκρίσεις ανίχνευσης εισβολών προωθούνται, τόσο από το τοπικό σύστημα ανταπόκρισης του παράγοντα του συγκεκριμένου κόμβου, όσο και από ολόκληρο το συνεργαζόμενο σύστημα ανταπόκρισης. Ο τύπος της αντίδρασης, στις εισβολές, εξαρτάται από τον τύπο των πρωτοκόλλων και των εφαρμογών του δικτύου, αλλά και από την πιστότητα των ενδείξεων. Για παράδειγμα ένας παράγοντας, κάποιου συστήματος ανίχνευσης εισβολών μπορεί να αποστείλει ένα αίτημα άρσης της πιστοποίησης σε όλους τους κόμβους του δικτύου και να ζητήσει από τους πιο πρόσφατους χρήστες να πιστοποιήσουν για ακόμη μία φορά τους εαυτούς τους και

στην συνέχεια τους κόμβους τους οποίους σχετίζονται με αυτούς, κάνοντας χρήση διαφόρων μηχανισμών εκτός των ορίων, όπως είναι η οπτική επαφή. Μόνο οι κόμβοι οι οποίοι έχουν επαναλιστοποιηθεί έχουν την δυνατότητα να διαπραγματεύονται καινούρια κανάλια επικοινωνίας, τα οποία στην συνέχεια αναγνωρίζουν κάθε επόμενο σαν γνήσιο. Για τον λόγο αυτό, οι δεσμευμένοι εχθρικοί κόμβοι μπορούν να αποκλειστούν και να γίνουν ακίνδυνοι. Τέλος οι διαχειριστές χρησιμοποιούν μια υπομονάδα ασφαλούς επικοινωνίας στα δικά τους συστήματα ανίχνευσης εισβολών και προωθούν ένα υψηλής πιστότητας κανάλι επικοινωνίας μεταξύ των παραγόντων του συστήματος. Ωστόσο η δουλειά που έχει πραγματοποιηθεί, είναι για την ώρα στα αρχικά της στάδια και δεν έχει προωθηθεί η έρευνα πάνω σε πειραματικά δεδομένα, προκειμένου να μελετηθεί η αποτελεσματικότητά των σχημάτων τους .

4.8 Ασφάλεια του πρωτοκόλλου των δικτύων ad hoc .

Η ασφάλεια για κάθε πρωτόκολλο αποτελεί ένα πολύ δύσκολο πρόβλημα το οποίο πρέπει να αντιμετωπίσουμε. Με τον τρόπο αυτό μπορούμε να αποκομίσουμε πλεονεκτήματα από τους πλεονασμούς της τοπολογίας του δικτύου. Για παράδειγμα εάν πολλαπλασιαστούν οι πιθανές διαδρομές μεταξύ των κόμβων τότε εξασφαλίζεται η επίτευξη της διαθεσιμότητας σε περίπτωση εισβολής. Η ασφάλεια των πρωτοκόλλων είναι στενά συνδεδεμένη με την πρέπουσα διανομή κάποιων κωδικών κλειδιών τα οποία θα επιτρέψουν την δημιουργία τεράστιας αξιοπιστίας. Για τον λόγο αυτό η σχεδίαση ασφαλών κωδικών κλειδιών στα δίκτυα ad hoc αποτελεί ένα μείζον ζήτημα και πρόβλημα συνάμα. Η ανταλλαγή των απαραίτητων κλειδιών μπορεί πράγματι να βοηθήσει στην ανάπτυξη κάποιας προσωρινής ασφάλειας μεταξύ των επικοινωνούντων σημείων. Ωστόσο είναι ακόμη ευαίσθητα στις ανθρωποκεντρικές (man – in – the middle) επιθέσεις οι οποίες είναι πολύ δύσκολο να καταπολεμηθούν σε ένα δίκτυο ad hoc.

Προσφάτως οι Zhang και Lee ερμήνευσαν τα ευρισκόμενα δεδομένα ώστε να περιγράψουν για τον κάθε κόμβο τις φυσικές ενημερώσεις πληροφόρησης για την δρομολόγηση. Από την στιγμή που μία δικαιολογημένη αλλαγή στα περιδρομολόγησης, μπορεί βασικά να οφείλεται στις φυσικές κινήσεις των κόμβων ή τις αλλαγές των περιεχομένων του δικτύου, κάθε κινητός κόμβος πρέπει να χρησιμοποιείται με αξιοπιστία πληροφορίας. Η τελευταία πρέπει να είναι έμπιστη. Έχει συμφωνηθεί να γίνεται χρήση της πληροφορίας στις φυσικές κινήσεις των κόμβων και στην αλλαγή ανταπόκρισης στο πλάνο δρομολόγησης σαν βάση της ευρισκόμενης πληροφορίας. Ένα φυσικό προφίλ της ευρισκόμενης αυτής πληροφορίας, συντελεί στον αποτελεσματικό καθορισμό της συσχέτισης των φυσικών κινήσεων των κόμβων και εντοπίζει τις αλλαγές στο σχέδιο δρομολόγησης. Ένας αλγόριθμος ταξινόμησης, χρησιμοποιείται για να ταξινομηθεί και να περιγραφεί η εκτίμηση των αλλαγών που προέρχονται από το κέρδος των αλλαγών στην δρομολόγηση και από το κέρδος των αλλαγών στο πλήθος των αναπηδήσεων (hops) όλων των διαδρομών. Δυστυχώς για ακόμη μία φορά δεν έχουν προωθηθεί πειραματικά δεδομένα προκειμένου να μελετηθεί η απόδοση και η αποτελεσματικότητα αυτών των σχεδίων.

Τα πρωτόκολλα δημοσίων κλειδιών και μεθόδων συμμετρικών κλειδιών, είναι επίσης τρομερά δύσκολα και δίχως υποδομή και έτσι είναι πολύ δύσκολο να καταλάβουμε την χρήση των πρωτοκόλλων που βασίζονται στην πιστοποίηση. Η μεγάλη συνάθροιση των διανεμόμενων πληροφοριών σε ένα ad hoc δίκτυο επιφέρει άλλους νέους τύπους προβλημάτων ασφαλείας. Στην πραγματικότητα δεν πρέπει να ξεχνάμε ότι πάντα θα υπάρχουν πολλοί διάφοροι τύποι έμπιστων σχέσεων , οι οποίοι είναι δύσκολο να διατηρηθούν μεταξύ των γειτονικών κόμβων σε μια μεγάλη κοινωνία. Η ποιότητα του ελέγχου των υπηρεσιών, πρέπει να χρησιμοποιείται για να προωθεί μια λογική λύση στην διανομή του μεγάλου πλήθους των πληροφοριών σε ένα ad hoc δίκτυο.

Κεφάλαιο 5^ο

5.1 Εισαγωγή

Στο παρόν κείμενο θα εξετάσουμε κατά πόσο η χρήση ασυρμάτων δικτύων επικοινωνιών (συχνοτήτων 2,4 GHz) επηρεάζουν την δημόσια υγεία. Σκοπός μας είναι να καταγράψουμε έρευνες που αφορούν πιθανές επιπτώσεις και προβλήματα υγείας στον ανθρώπινο οργανισμό από την συστηματική χρήση συσκευών ασύρματων ζεύξεων. Τα αποτελέσματα έχουν προέλθει από αναφορές που βρήκαμε στη διεθνή βιβλιογραφία και δεν είναι σε καμία περίπτωση πλήρη. Επίσης δεν καταλήγουμε σε δικά μας συμπεράσματα αλλά κάνουμε μια απλή αναφορά έτσι ώστε ο κάθε ενδιαφερόμενος να μπορεί να ψάξει περαιτέρω μόνος του. Θα προσπαθήσουμε να εξηγήσουμε την λειτουργία των ηλεκτρομαγνητικών κυμάτων, πως αυτά μπορούν και επιδρούν στα μόρια, καθώς και να τα διαχωρίσουμε ανάλογα με τις ιδιότητες τους. Στη συνέχεια θα αναφερθούμε στα ασύρματα δίκτυα και στην συχνότητα των 2.4GHz και πως αυτά επηρεάζουν τον άνθρωπο. Θα παρουσιάσουμε μελέτες και δείκτες αξιολόγησης που υπάρχουν, θα αναφερθούμε στο νομικό πλαίσιο που διέπει αυτή την συχνότητα και τέλος θα δώσουμε παραδείγματα από ασύρματα δίκτυα από όλο τον κόσμο.

5.2 Ηλεκτρομαγνητικά κύματα

Σε αυτό το κεφάλαιο κάνουμε μια εισαγωγή στα ηλεκτρομαγνητικά κύματα. Προσπαθούμε να εξηγήσουμε την λειτουργία τους και πως δημιουργούνται ενώ δίνουμε παραδείγματα όπου τα συναντάμε καθημερινά στην ζωή μας. Ύστερα εξηγούμε πως αυτά μας μπορούν να επηρεάσουν τα μόρια και διαχωρίζουμε την ακτινοβολία σε ιονίζουσα και μη. Στο τέλος παρουσιάζουμε το ηλεκτρομαγνητικό φάσμα και αναλύουμε της διάφορες κατηγορίες.

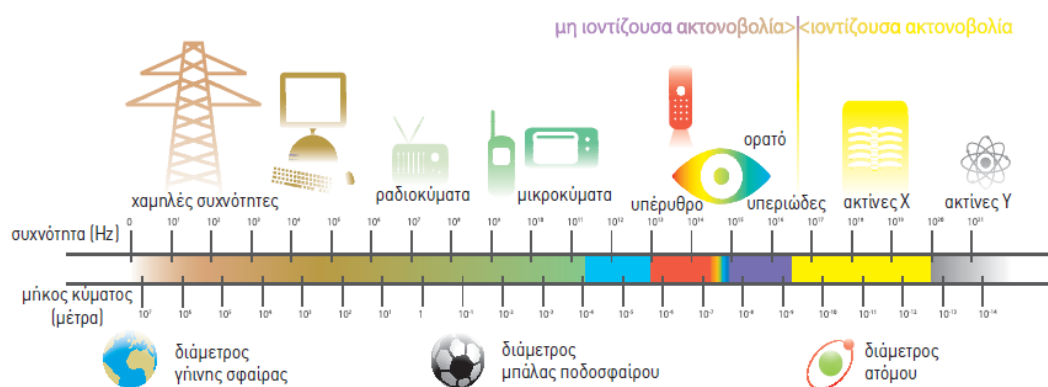
5.2.1 Τι είναι τα ηλεκτρομαγνητικά κύματα

Τα ηλεκτρομαγνητικά κύματα (ακτινοβολία) είναι τα γνωστά σε όλους ραδιοκύματα που χρησιμοποιούνται στο ραδιόφωνο, στην τηλεόραση και σε άλλες τεχνολογικές εφαρμογές της καθημερινής μας ζωής [1]. Πρόκειται για ταλαντώσεις ηλεκτρικών και μαγνητικών πεδίων που διαδίδονται ως κύματα με την ταχύτητα του φωτός. Ποικίλες εφαρμογές τους βρίσκονται στην υπηρεσία του ανθρώπου για περισσότερο από 100 χρόνια, καθώς καθημερινά χρησιμοποιούνται για την λειτουργία οικιακών συσκευών (όπως για παράδειγμα ραδιόφωνο, τηλεόραση, φούρνος μικροκυμάτων), ασύρματων εφαρμογών καθώς και σε ιατρικές εφαρμογές κ.α. Επιπλέον χρησιμοποιούνται στα τηλεπικοινωνιακά συστήματα της Πυροσβεστικής, Αστυνομίας, των ασθενοφόρων αλλά και των ραντάρ. Οι πιο πρόσφατες εφαρμογές των ηλεκτρομαγνητικών κυμάτων πραγματοποιήθηκαν στις δεκαετίες του '80 και '90, όταν έγινε η χρήση τους στην κινητή και δορυφορική επικοινωνία.

Κάθε πηγή ηλεκτρομαγνητικών κυμάτων (π.χ. κεραιές ραδιοφωνίας, τηλεόρασης, κινητής τηλεφωνίας, ραντάρ) παράγει ηλεκτρομαγνητικό πεδίο που διαδίδεται στο χώρο (συνθά χρησιμοποιούμε τον όρο ηλεκτρομαγνητική ακτινοβολία). Τα ηλεκτρομαγνητικά πεδία (ΗΜΠ), υπάρχουν παντού στο περιβάλλον μας. Μπορεί να είναι φυσικής προέλευσης ή μπορεί να έχουν δημιουργηθεί από τον άνθρωπο. Το ηλεκτρικό ρεύμα δημιουργεί ΗΜΠ. Τα ΗΜΠ μπορεί να είναι ψηλής ή χαμηλής έντασης, συνεχή ή μικρής διάρκειας. Τα ηλεκτρικά πεδία δημιουργούνται λόγω διαφοράς ηλεκτρικής τάσης. Όσο πιο μεγάλη είναι η διαφορά, τόσο πιο δυνατό θα είναι το ηλεκτρικό πεδίο που προκύπτει. Η μονάδα μέτρησης των ηλεκτρικών πεδίων είναι βολτ ανά μέτρο (V/m). Τα μαγνητικά πεδία δημιουργούνται όταν υπάρχει ροή ηλεκτρικού ρεύματος. Όσο πιο ψηλή είναι η ένταση του ρεύματος τόσο πιο δυνατό θα είναι το μαγνητικό πεδίο. Όταν διακοπεί το ηλεκτρικό ρεύμα, το μαγνητικό πεδίο μηδενίζεται. Μια συσκευή όπως για παράδειγμα ο στεγνωτήρας μαλλιών, παράγει μαγνητικό πεδίο μόνο όταν το ηλεκτρικό ρεύμα τη θέτει σε λειτουργία. Η διακοπή του ρεύματος, εξαφανίζει άμεσα το μαγνητικό πεδίο.

Τα ΗΜΠ δημιουργούνται μεταξύ άλλων από τα ακόλουθα:

1. Ηλεκτροφόρα καλώδια υψηλής τάσης
2. Ηλεκτροφόρα καλώδια στις γειτονιές
3. Συστήματα γείωσης που προστατεύουν από κεραυνούς ή από ελαττωματικές οικιακές συσκευές
4. Οικιακές συσκευές όπως φούρνοι μικροκυμάτων, στεγνωτήρες μαλλιών, ηλεκτρικοί φούρνοι, ηλεκτρική θέρμανση,
5. Οθόνες ηλεκτρονικών υπολογιστών, ηλεκτρικά ρολόγια, ηλεκτρικές κουβέρτες
6. Κινητά τηλέφωνα, κεραιές σταθμών βάσης, ραντάρ, ραδιοφωνικοί και τηλεοπτικοί σταθμοί
7. Φυσικές πηγές
8. Ακτίνες X
9. Φως του ήλιου
10. Ακτίνες γάμα



5.2.2 Επιπτώσεις των ηλεκτρομαγνητικών πεδίων στα μόρια

Τα ηλεκτρομαγνητικά κύματα μεταφέρονται από τα σωματίδια που ονομάζονται κβάντα. Στην υψηλή συχνότητα (και άρα στα μικρά μήκη κύματος) η κβαντική ενέργεια είναι πολύ μεγάλη και αποτελεί μεταλλαξογόνο παράγοντα [2]. Όταν η μεταφερόμενη ενέργεια είναι μεγάλη, τότε σπάζουν οι δεσμοί μεταξύ των μορίων. Το γεγονός αυτό είναι ιδιαίτερα επικίνδυνο. Προκαλούνται αλλοιώσεις του γενετικού κώδικα του DNA. Το αποτέλεσμα είναι η πρόκληση καρκίνου και άλλων σοβαρών ασθενειών. Ευτυχώς δεν είναι όλα τα είδη ΗΜΠ που μπορούν να προκαλέσουν αλλοιώσεις στο DNA. Μόνο αυτά που χαρακτηρίζονται από υψηλή συχνότητα, μικρό μήκος κύματος και υψηλή ενέργεια μπορούν να προκαλέσουν βλάβες στο DNA. Η ακτινοβολία που έχει αυτή τη δυνατότητα ονομάζεται ionίζουσα ακτινοβολία. Η ηλεκτρομαγνητική ακτινοβολία στην οποία υποβαλλόμαστε συνήθως

και καθημερινά είναι η μη ιονίζουσα ακτινοβολία και δεν έχει τέτοιες δυνατότητες και κινδύνους. Υπάρχει μόνο μια εξαίρεση στην καθημερινή ακτινοβολία που δεχόμαστε. Πρόκειται για την ιονίζουσα ακτινοβολία που προκαλείται από τις υπεριώδεις ακτίνες του ήλιου. Η έκθεση στο ηλιακό φως και κατά συνέπεια στις υπεριώδεις ακτίνες, είναι αιτία καρκίνου του δέρματος (μελανώματος, ακανθοκυτταρικού και βασεοκυτταρικού καρκινώματος) και άλλων αλλοιώσεων και ρυτίδων. Τα διάφορα είδη ηλεκτρομαγνητικής ακτινοβολίας και τα πεδία που προκύπτουν, έχουν διαφορετικές επιδράσεις στον ανθρώπινο οργανισμό.

Οι επιπτώσεις που προκαλούνται από την έκθεση στην ηλεκτρομαγνητική ακτινοβολία εξαρτώνται κυρίως από δύο παράγοντες:

Τη Συχνότητα Εκπομπής: Για συχνότητες που ανήκουν στο ραδιοφάσμα (υπηρεσίες ραδιοφωνίας, τηλεόρασης, κινητής τηλεφωνίας), η εκπεμπόμενη ακτινοβολία ονομάζεται «μη ιονίζουσα», διότι δεν μπορεί να δημιουργήσει ιόντα μέσα στην ύλη, δηλαδή (με επιστημονικούς όρους) το φωτόνιό της δεν έχει αρκετή ενέργεια, ώστε να εκδιώξει ένα ηλεκτρόνιο από ένα άτομο της ύλης. Αντιθέτως, σε πολύ υψηλές συχνότητες (π.χ. ακτίνες X) η ακτινοβολία μπορεί να προκαλέσει ιονισμό, επομένως άμεση βλάβη στη βιολογική ύλη, και ονομάζεται «ιονίζουσα». Στις ραδιοσυχνότητες, έχει διαπιστωθεί ότι οι κύριες επιπτώσεις της ηλεκτρομαγνητικής ακτινοβολίας είναι θερμικές.

Την Ισχύ Εκπομπής: Υπάρχουν διάφορα μεγέθη που ποσοτικοποιούν την ηλεκτρομαγνητική ακτινοβολία, με το πιο ευρέως διαδεδομένο στις ραδιοσυχνότητες την Ένταση του ηλεκτρικού πεδίου (συμβολίζεται με E και μετριέται σε Βολτ ανά μέτρο). Άλλα μεγέθη είναι η Ένταση του μαγνητικού πεδίου (συμβολίζεται με H και μετριέται σε Αμπέρ ανά μέτρο), η Μαγνητική Επαγωγή πεδίου (συμβολίζεται με B και μετριέται σε Τέσλα) και η Πυκνότητα Ροής Ισχύος (συμβολίζεται με S και μετριέται σε Βατ ανά τετραγωνικό μέτρο).

5.2.3 Τι συμβαίνει όταν το ανθρώπινο σώμα εκτίθεται σε ηλεκτρομαγνητικά πεδία ραδιοσυχνότητας;

Ηλεκτρικά ρεύματα υπάρχουν και στο ανθρώπινο σώμα και είναι απαραίτητα για τις φυσιολογικές σωματικές λειτουργίες. Όλες οι δομές του νευρικού συστήματος λειτουργούν μεταδίδοντας παλμικά ηλεκτρικά σήματα. Οι περισσότερες βιοχημικές αντιδράσεις, από εκείνες που σχετίζονται με την πέψη μέχρι εκείνες που σχετίζονται με την εγκεφαλική λειτουργία,

περιλαμβάνουν ηλεκτρικές διεργασίες. Τα βιολογικά αποτελέσματα της έκθεσης του ανθρώπινου σώματος και των κυττάρων του σε εξωτερικά πεδία ΡΣ εξαρτώνται κυρίως από τη συχνότητα και την ένταση των ηλεκτρομαγνητικών πεδίων. Στις

ραδιοσυχνότητες, η ακτινοβολία απορροφάται μερικώς και διεισδύει σε μικρό μόνο βάθος μέσα στο σώμα.

Η ενέργεια αυτών των ηλεκτρομαγνητικών πεδίων απορροφάται και προκαλεί την κίνηση των μορίων. Η τριβή και οι κρούσεις μεταξύ των ταχέως κινουμένων μορίων έχουν ως αποτέλεσμα την αύξηση της θερμοκρασίας. Δύο περιοχές του σώματος, τα μάτια και οι όρχεις, είναι ιδιαίτερος ευπαθείς στη θέρμανση ΡΣ διότι χαρακτηρίζονται από χαμηλή αιματική κυκλοφορία και, συνεπώς, ανεπαρκή απαγωγή της αυξημένης θερμότητας. Τα επίπεδα έντασης των πεδίων ΡΣ στα οποία συνήθως εκτίθεται το κοινό στο καθημερινό περιβάλλον του είναι πολύ ασθενέστερα σε σχέση με αυτά που απαιτούνται για να προκληθεί αξιοσημείωτη τοπική θέρμανση ή αύξηση της θερμοκρασίας του σώματος.

Εκτός, όμως, από τα γνωστά θερμικά αποτελέσματα, υπάρχει σήμερα αυξημένο ενδιαφέρον για τη μελέτη ύπαρξης και άλλων μη θερμικών μηχανισμών αλληλεπίδρασης των ραδιοκυμάτων με τους βιολογικούς ιστούς. Ορισμένες μελέτες έχουν δείξει ότι, υπό συγκεκριμένες συνθήκες, τα ραδιοκύματα μπορούν να προκαλέσουν μη θερμικές βιολογικές επιδράσεις σε καλλιέργειες κυττάρων ή πειραματόζωα, χωρίς, ωστόσο, αυτές οι επιδράσεις να σχετίζονται άμεσα με την πρόκληση κάποιας βλάβης στον ανθρώπινο οργανισμό. Επιπλέον, σε μερικές από τις μελέτες αυτές, τα αποτελέσματα εμφανίζονται αντιφατικά, ενώ σε κάποιες άλλες δεν έγινε δυνατό να επαναληφθούν. Είναι φανερό ότι υπάρχει αβεβαιότητα και ανάγκη για περαιτέρω διερεύνηση των μηχανισμών που σχετίζονται με μη θερμικά φαινόμενα και τη συσχέτισή τους με επιβλαβείς βιολογικές επιδράσεις και ενδεχόμενες επιπτώσεις στην υγεία. Η έρευνα σε παγκόσμιο επίπεδο συνεχίζεται υπό το συντονισμό του Παγκόσμιου Οργανισμού Υγείας.

5.3.1 Ραδιοκύματα

Τα ραδιοκύματα είναι κύματα με συχνότητα από 3 KHz μέχρι 300 GHz. Τα μικροκύματα αποτελούν ένα υποσύνολο των ραδιοκυμάτων με συχνότητες που κυμαίνονται περίπου μεταξύ των 300 MHz και 3 GHz. Το μήκος κύματος των ραδιοκυμάτων ποικίλλει μεταξύ των τιμών 1mm και 10Km. Τα ραδιοκύματα δημιουργούνται από την κίνηση ηλεκτρικών φορτίων επί των κεραιών και αναφέρονται και ως ηλεκτρομαγνητική ακτινοβολία ραδιοσυχνοτήτων (ΡΣ), γιατί ακτινοβολούνται στο χώρο απομακρυνόμενα από την πηγή τους, δηλαδή την κεραία εκπομπής.

Τα ραδιοκύματα ανήκουν στην κατηγορία των μη ιοντιζουσών ακτινοβολιών, καθώς δεν είναι ικανά να διασπάσουν χημικούς δεσμούς ή να αποσπάσουν ηλεκτρόνια από άτομα, προκαλώντας ιοντισμό της ύλης, όπως η ραδιενέργεια (ακτίνες X, ακτίνες γ). Ο ιοντισμός είναι επικίνδυνος γιατί μπορεί να οδηγήσει σε αλλοιώσεις του γενετικού υλικού και να επιφέρει επιβλαβή αποτελέσματα στην υγεία.

Η κυριότερη βιολογική επίδραση των ραδιοκυμάτων είναι η αύξηση της θερμοκρασίας των ιστών που εκτίθενται σε αυτά υπό ορισμένες συνθήκες. Οι μέχρι σήμερα έρευνες δεν έχουν τεκμηριώσει σχέση αιτίου – αιτιατού μεταξύ αυτού του τύπου της ακτινοβολίας και της πρόκλησης επιβλαβών επιπτώσεων στην υγεία (π.χ. καρκινογενέσεις).

Ο διαχωρισμός μεταξύ ιοντίζουσας και μη ιοντίζουσας ακτινοβολίας είναι σημαντικός, γιατί επιτρέπει την καλύτερη αντίληψη των πραγματικών κινδύνων των διαφόρων τύπων της ηλεκτρομαγνητικής ακτινοβολίας.

5.3.2 Πεδία ραδιοσυχνοτήτων

Τα ραδιοκύματα είναι ηλεκτρομαγνητικά πεδία που μπορούν να ακτινοβολούνται προς όλες τις κατευθύνσεις για ευρυεκπομπή, προς συγκεκριμένες περιοχές του χώρου όπου ενδεχομένως βρίσκεται ένας μετακινούμενος δέκτης, ή προς σταθερούς δέκτες που βρίσκονται σε γνωστές θέσεις. Η κεραία είναι διάταξη σχεδιασμένη για να εκπέμπει και να λαμβάνει ραδιοκύματα.

Η ένταση του πεδίου που δημιουργείται εξαρτάται από:

- Τη συνολικά ακτινοβολούμενη ισχύ – μεγαλύτερη ισχύς προκαλεί ισχυρότερα πεδία.
- Την απόσταση από την κεραία – η ένταση του πεδίου μειώνεται σημαντικά με την αύξηση της απόστασης .
- Το διάγραμμα ακτινοβολίας της κεραίας– στενές δέσμες δημιουργούν ισχυρά πεδία στο εσωτερικό τους.

Ως προς την εξάρτηση από την απόσταση, τα ραδιοκύματα εξασθενούν αντιστρόφως ανάλογα προς το τετράγωνο της απόστασης από την πηγή τους. Δηλαδή, η πυκνότητα ισχύος που είναι το μέγεθος που καθορίζει την ποσότητα ισχύος που προσπίπτει σε μια επιφάνεια και μετριέται σε W/m^2 , σε απόσταση 100 μέτρων από την πηγή ακτινοβολίας, εξασθενεί 10.000 φορές σε σχέση με την πυκνότητα ισχύος που δημιουργείται σε απόσταση 1 μέτρου από την πηγή.

Όταν συναντούν αντικείμενα κατά τη διάδοσή τους, τα ραδιοκύματα μπορεί να ανακλαστούν, να απορροφηθούν ή να διαπεράσουν το αντικείμενο μερικώς ή ολικώς κατά τρόπο αντίστοιχο με ό,τι συμβαίνει με το φως.

5.3.3 Ποιες είναι οι εφαρμογές των ραδιοκυμάτων;

Η πλέον σημαντική εφαρμογή των ραδιοκυμάτων είναι οι τηλεπικοινωνίες. Οι ραδιοφωνικές και τηλεοπτικές εκπομπές, τα κινητά τηλέφωνα, τα ασύρματα τηλέφωνα, οι επικοινωνίες της αστυνομίας και της πυροσβεστικής, οι δορυφορικές επικοινωνίες πραγματοποιούνται μεταδίδοντας την ενέργεια ραδιοκυμάτων.

Τα ραδιοκύματα λειτουργούν ως φορείς της πληροφορίας στις τηλεπικοινωνίες, τη ραδιοφωνία και την τηλεόραση.



Σχήμα 5.2 Εκπομπή, μετάδοση και λήψη των ραδιοκυμάτων

Άλλες χρήσεις των ραδιοκυμάτων περιλαμβάνουν τους φούρνους μικροκυμάτων, τα ραντάρ, βιομηχανικά συστήματα θέρμανσης και στεγανοποίησης και τα ιατρικά μηχανήματα.

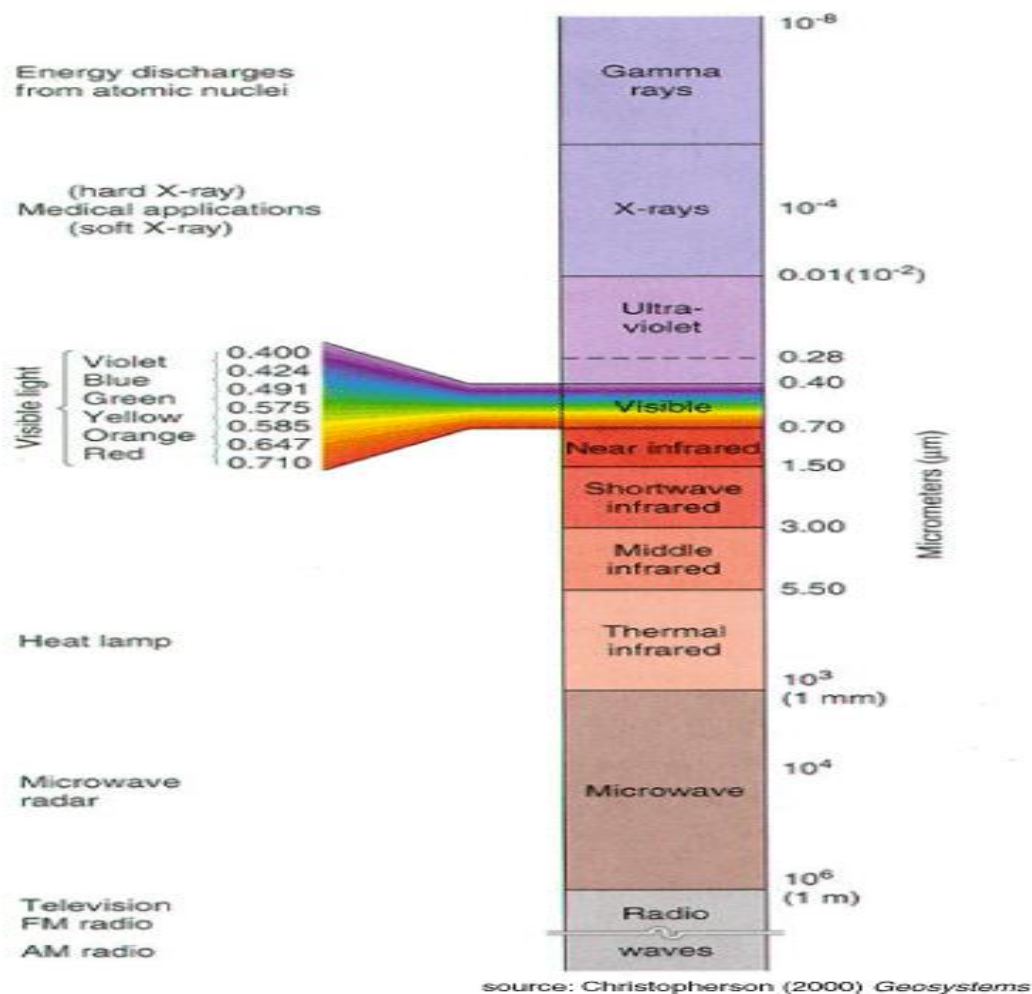
Η ενέργεια των ραδιοκυμάτων, ειδικά αυτή των μικροκυμάτων, έχει τη δυνατότητα να θερμαίνει το νερό. Δεδομένου ότι οι περισσότερες τροφές έχουν υψηλή περιεκτικότητα σε νερό, τα μικροκύματα μπορούν να θερμάνουν το φαγητό αρκετά γρήγορα. Τα ραντάρ χρησιμοποιούν την ενέργεια των ραδιοκυμάτων για τον εντοπισμό αυτοκινήτων και αεροπλάνων καθώς και για στρατιωτικές εφαρμογές. Οι βιομηχανικοί θερμαντήρες και στεγανοποιητές χρησιμοποιούν ραδιοκύματα για τη συγκόλληση παραγώγων ξύλου, τη στεγανοποίηση δερμάτινων αντικειμένων όπως παπουτσιών και για την επεξεργασία φαγητού. Οι ιατρικές χρήσεις της ενέργειας ραδιοκυμάτων περιλαμβάνουν τη μαγνητική τομογραφία, την εποπτεία και τον προγραμματισμό βηματοδοτών, την υπερθερμία για την αντιμετώπιση του καρκίνου.

5.3.4 Η μη ιονίζουσα ακτινοβολία

Η ενέργεια που μεταφέρουν τα κβάντα των ηλεκτρομαγνητικών πεδίων μεγάλου μήκους κύματος και χαμηλής συχνότητας, δεν είναι αρκετή για να προκαλέσει ιονισμό. Οι πηγές των ΗΜΠ που έχει κατασκευάσει ο άνθρωπος, στα οποία υποβαλλόμαστε καθημερινά (ραδιοκύματα, μικροκύματα, ηλεκτρισμός), είναι μεγάλου μήκους κύματος και χαμηλής συχνότητας. Δεν μπορούν να προκαλέσουν ιονισμό διότι η ενέργεια που μεταφέρουν τα κβάντα τους είναι μικρή. Δεν μπορούν να σπάσουν χημικούς δεσμούς στα μόρια των κυττάρων.

5.3.5 Το ηλεκτρομαγνητικό φάσμα

Οι ηλεκτρομαγνητικές πηγές διαφέρουν ως προς τη συχνότητα εκπομπής τους και έτσι προκύπτει μία βασική κατηγοριοποίηση των ηλεκτρομαγνητικών πεδίων. Ο όρος ηλεκτρομαγνητικά πεδία περιλαμβάνει τα στατικά πεδία, τα πεδία ιδιαίτερα χαμηλής συχνότητας (ELF) και τα πεδία ραδιοσυχνοτήτων (RF), συμπεριλαμβανομένων των μικροκυμάτων και καλύπτει τη ζώνη συχνοτήτων από 0 Hz έως 300 GHz. Το σύνολο των συχνοτήτων εκπομπής ονομάζεται φάσμα. Το φάσμα των ηλεκτρομαγνητικών ακτινοβολιών μπορούμε να το δούμε στο **Σχήμα 5.3**. Τα ΗΜΠ που παράγονται από τα καλώδια ηλεκτρικού ρεύματος και τις ηλεκτρικές συσκευές στο σπίτι, είναι εξαιρετικά χαμηλής συχνότητας που φτάνουν μέχρι 300 Hz. Οι κεραιές ραδιοφωνίας, τηλεόρασης και κινητής τηλεφωνίας εκπέμπουν ηλεκτρομαγνητικά πεδία ραδιοσυχνοτήτων και το αντίστοιχο τμήμα του φάσματος ονομάζεται ραδιοφάσμα (RF spectrum).



Σχήμα 5.3

Ας δούμε τώρα τις κατηγορίες πως κατηγοριοποιείται το φάσμα καθώς και τις επιπτώσεις που μπορεί να έχει η κάθε συχνότητα στον άνθρωπο.

Μήκος κύματος (μm – μικρόμετρο)	Ακτινοβολία
10^{-8} - 10^{-6}	Ακτίνες γ
10^{-6} - 10^{-2}	Ακτίνες X
0.28 - 10^{-2}	Υπεριώδης
0.70 - 0.40	Ορατή
0.70 - 10^3	Υπέρυθρη
10^3 - 10^6	Μικροκύματα

Ακτίνες γ: Έχουν τη μεγαλύτερη συχνότητα και τα μικρότερα μήκη κύματος εκπέμπονται από ραδιενεργά υλικά και βρίσκονται και στο διάστημα. Οι ακτίνες αυτές έχουν μια εκπληκτική διατρητική ικανότητα. Μπορούν να διατρήσουν μια επιφάνεια τσιμέντου με πάχος 3 μέτρα! Τα μήκη κύματος αυτής της ακτινοβολίας εκτείνονται από 0.1 έως 0.000001 νανόμετρα.

Ακτίνες X: Η συχνότητά τους βρίσκεται σε τιμές μεταξύ των ακτίνων γ και των υπεριώδων ακτίνων. Έχουν τέτοια διατρητική ικανότητα ώστε να διαπερνούν εύκολα αρκετά υλικά και να καταστρέφουν ιστούς δέρματος πολλών ζώων. Αυτό έχει οδηγήσει τους επιστήμονες στο να χρησιμοποιούν τις ακτίνες X (με αρκετή φειδώ όμως) ώστε να παρατηρούν το ανθρώπινο σώμα (ακτινογραφίες). Τα μήκη κύματος των ακτίνων X έχουν μεγάλη έκταση. Εκτείνονται από ένα μέχρι 0.00001 νανόμετρα.

Υπεριώδης ακτινοβολία: Έχουν συχνότητες λίγο παραπάνω από αυτές του ορατού φωτός. Ωστόσο η έντασή τους είναι τέτοια που μπορεί να καταστρέψει ιστούς και κύτταρα. Ο ήλιος είναι μια πηγή ηλεκτρομαγνητικής ακτινοβολίας και μικρές δόσεις αυτής της ακτινοβολίας βοηθούν στην παραγωγή της βιταμίνης D και προκαλούν το μαύρισμα του ανθρώπινου δέρματος. Φυσικά, μεγαλύτερες δόσεις προκαλούν σοβαρά εγκαύματα. Η ηλεκτρομαγνητική ακτινοβολία χρησιμοποιείται ευρέως στον επιστημονικό χώρο σε διάφορα πειράματα, καθώς και από τους αστρονόμους για την παρατήρηση του ηλιακού συστήματος, του γαλαξία μας και άλλων περιοχών του σύμπαντος. Το μήκος κύματος της υπεριώδους ακτινοβολίας εκτείνεται από 50 μέχρι 350 και 400 νανόμετρα.

Ορατό φως: Τα χρώματα ενός ουράνιου τόξου, δηλαδή η ακτινοβολία που μπορεί να εντοπιστεί από το ανθρώπινο μάτι (από 400 έως 700 νανόμετρα) δεν είναι παρά ένα πολύ μικρό μέρος του ηλεκτρομαγνητικού φάσματος. Εμείς, αν και δεν το αντιλαμβανόμαστε, βρισκόμαστε υπό το συνεχές βομβαρδισμό ηλεκτρομαγνητικής ακτινοβολίας, η οποία εκτείνεται σε πολύ διαφορετικά μήκη κύματος.

Υπέρυθρη ακτινοβολία: Εκτείνεται από εκεί που σταματάει η ορατή ακτινοβολία, δηλαδή περίπου τα 700 νανόμετρα μέχρι περίπου το ένα χιλιοστό. Αυτού του τύπου η ακτινοβολία έχει να κάνει με θερμότητα. Για παράδειγμα, το ανθρώπινο σώμα εκπέμπει θερμότητα όχι στο ορατό φως, αλλά σε περιοχές της υπέρυθρης ακτινοβολίας. Όλα τα σώματα λίγο έως πολύ εκπέμπουν θερμότητα σε αυτά τα μήκη κύματος ανάλογα με τη θερμοκρασία τους. Οι πιο κοινές χρήσεις της υπέρυθρης ακτινοβολίας έχουν να κάνουν με τη νυχτερινή όραση, ανιχνευτές σε δορυφόρους και αεροπλάνα, καθώς και την αστρονομία.

Μικροκύματα: Έχουν ένα μήκος κύματος που εκτείνεται από ένα χιλιοστό μέχρι 30 εκατοστά. Ο άνθρωπος εκμεταλλεύτηκε αυτήν την ακτινοβολία στην κατασκευή φούρνων μικροκυμάτων, οι οποίοι μπορούν να θερμάνουν φαγητά, καθώς η

ακτινοβολία αυτή απορροφάται από τις τροφές και τις θερμαίνει. Τα μικροκύματα είναι ένα μέρος μιας μεγαλύτερης κατηγορίας ακτινοβολίας, τα ραδιοκύματα (radiowaves).

Ραδιοκύματα : Εκπέμπονται από τη Γη, τα κτήρια, τα αυτοκίνητα κι άλλα μεγάλα σε μέγεθος αντικείμενα. Πάνω στα ραδιοκύματα έχει βασιστεί η λειτουργία των ραντάρ τα οποία ανιχνεύουν την παρουσία και την κίνηση σωμάτων που εκπέμπουν αυτού του τύπου την ακτινοβολία. Τα ραδιοκύματα επίσης είναι ευρέως γνωστά για την ικανότητά τους να μεταφέρουν ραδιοφωνικά σήματα και σήματα τηλεόρασης. Τα ραδιοκύματα έχουν μήκος κύματος, που εκτείνεται σε μια αρκετά μεγάλη περιοχή, από ένα εκατοστό έως δεκάδες και εκατοντάδες μέτρα.

5.4 Τα ασύρματα δίκτυα

Έχοντας αναλύσει γενικά τα ηλεκτρομαγνητικά κύματα προχωράμε στην εξέταση των μικροκυμάτων και ποιο συγκεκριμένα των 2,4 GHz που χρησιμοποιούνται από τα ασύρματα δίκτυα. Θα αναφερθούμε σε μελέτες που έχουν γίνει και θα εξηγήσουμε μονάδες μετρήσεων που θεσπίζονται από διεθνείς οργανισμούς. Έπειτα θα αναλύσουμε το νομικό πλαίσιο σε Αμερική και Ελλάδα και θα καταλήξουμε στην παρουσίαση εφαρμογών του Wi-Fi ανά τον κόσμο

5.4.1 Το εύρος των 2,4GHz

Το εύρος των 2,4 GHz είναι η συχνότητα που χρησιμοποιείται στις ασύρματες επικοινωνίες και αποτελούν μικροκύματα. Ανήκουν στην κατηγορία των μη ιονίζουσων ακτινοβολιών, δηλαδή αντίθετα με τις ακτίνες X (χρησιμοποιούνται κυρίως για ακτινογραφίες) και το πλουτόνιο, δεν προκαλούν αλλαγές στο DNA άρα προκαλούνται παθήσεις που σχετίζονται με την μετάλλαξη του (π.χ. καρκίνος). Από την άλλη τα μικροκύματα ασκούν ηλεκτρομαγνητική δύναμη στα μόρια του νερού, με αποτέλεσμα αυτά να ταλαντώνονται τόσο γρήγορα που στο τέλος δεν μπορούν να ακολουθήσουν τον ρυθμό και καθυστερούν. Το αποτέλεσμα είναι να τα μόρια να απορροφούν μέρος της ισχύς του σήματος και να την απελευθερώνουν σε μορφή θερμότητας (Dr. Eleanor R. Adair, ειδική σε έρευνες για τα μικροκύματα, σε συνέντευξη της στην εφημερίδα New York Times) . Αυτός είναι και ο κύριος λόγος που τα μικροκύματα χρησιμοποιούνται από τους φούρνους μικροκυμάτων (πιο συγκεκριμένα αν και όλες οι συχνότητες άνω των 2GHz μπορούν να θερμάνουν το νερό, τα 2,4 επιλέχθηκαν για λόγους σταθερότητας).

Σε αυτό το σημείο αξίζει να κάνουμε μια σημαντική παρατήρηση. Οι φούρνοι μικροκυμάτων, που χρησιμοποιούν την ίδια συχνότητα με τα ασύρματα δίκτυα, συγκεντρώνουν σήματα ισχύος 1kW σε μια μικρή περιοχή, ενώ στα ασύρματα δίκτυα μιλάμε για σήματα ισχύος το πολύ (σύμφωνα με τον ελληνικό νόμο όπως αναλύεται παρακάτω) 100mW.

5.4.2 Επιστημονικές μελέτες και διεθνείς οργανισμοί

Παρακάτω βρίσκονται μελέτες που έχουν γίνει ανά τον κόσμο για τις επιδράσεις που μπορεί να έχει η ηλεκτρομαγνητική ακτινοβολία στον ανθρώπινο οργανισμό. Παρόλα αυτά, όσο αφορά το εύρος των 2,4GHz οι μελέτες που υπάρχουν είναι πολύ λίγες, καθώς η ισχύς που χρησιμοποιούν τα ασύρματα τερματικά είναι πολύ μικρή. Αντίστοιχα, μπορούμε εύκολα να βρούμε έναν μεγάλο αριθμό από μελέτες και έρευνες που έχουν γίνει για την επίδραση των κινητών τηλεφώνων, αφού αυτά χρησιμοποιούν τουλάχιστον την δεκαπλάσια ισχύ σε σχέση με τα ασύρματα τερματικά και είναι πολύ περισσότερο διαδεδομένα.

5.4.2.1 Ηλεκτρομαγνητικά κύματα γενικά

5.4.2.1.1 National Radiological Protection Board (NRPB)

Ο NRPB είναι πλέον μέλος του “Health Protection Agency (HPA)”, ο οποίος είναι ένας οργανισμός ο οποίος έχει ως στόχο την προστασία της υγείας των κατοίκων της Αγγλίας και Ουαλίας.

Σύμφωνα με σχετική έρευνα που δημοσιοποίησε τον Ιανουάριο του 2005, δεν υπάρχει κανένα στοιχείο που να αποδεικνύει πως τα ηλεκτρομαγνητικά κύματα δημιουργούν ή επιταχύνουν την εμφάνιση ασθενειών στον ανθρώπινο οργανισμό. Στην έρευνά τους αναφέρουν πολλά παραδείγματα κατοίκων που είχαν εκτεθεί σε υψηλά επίπεδα ηλεκτρομαγνητικής ακτινοβολίας και δεν παρουσίασαν το παραμικρό σύμπτωμα, το οποίο να είχε σχέση με την έκθεση αυτή.

5.4.2.1.2 International Commission on Non-Ionizing Radiation Protection

Η ICNIRP είναι η Διεθνής Υπηρεσία Προστασίας της Μη-Ιονίζουσας Ακτινοβολίας. Είναι ένα σώμα από ανεξάρτητους επιστημονικούς εμπειρογνώμονες που απαρτίζουν την κύρια Υπηρεσία με 14 μέλη, την Επιστημονική Νομοπαρασκευαστική Επιτροπή η οποία καλύπτει τους τομείς της Επιδημιολογίας, της Βιολογία, της Δοσιμετρίας, της Οπτικής Ακτινοβολίας και από έναν αριθμό από συμβουλευτικά μέλη. Αυτή η σύνθεση έχει ως σκοπό να τονίσει σημαντικά θέματα πιθανών δυσμενών επιπτώσεων στην ανθρώπινη υγεία που θα επιφέρει η έκθεση σε μη-ιονίζουσα ακτινοβολία.

Η επίσημη θέση της υπηρεσίας είναι πως αν και έχουν γίνει εκατοντάδες έρευνες την τελευταία δεκαετία σχετικά με τις επιπτώσεις που επιφέρουν τα ηλεκτρομαγνητικά κύματα στην ανθρώπινη υγεία δεν υπάρχει καμία επιστημονική απόδειξη που να το αποδεικνύει πως τα ηλεκτρομαγνητικά κύματα προκαλούν αρνητικές επιπτώσεις στον άνθρωπο .

5.4.2.1.3 Reflex - Δεκέμβριος του 2004.

Η έρευνα της Reflex διήρκησε 4 χρόνια και διεξήχθη σε συνεργασία με την γερμανική ερευνητική ομάδα Verum και χρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση. Μελέτησε τις επιδράσεις της ακτινοβολίας πάνω σε ζωικά και ανθρώπινα κύτταρα σε συνθήκες εργαστηρίου και, τελικά, διαπιστώθηκε ότι μετά από παρατεταμένη έκθεση σε ηλεκτρομαγνητικά πεδία τα κύτταρα παρουσίασαν αυξανόμενες βλάβες του DNA που δεν ήταν δυνατόν να διορθωθούν σε όλες τις

περιπτώσεις. Επιπλέον, οι βλάβες αυτές παρουσιάστηκαν και στις επόμενες γενιές κυττάρων, ενώ παρουσιάστηκε και πληθώρα άλλων βλαβερών επιδράσεων σε αυτά. Τα συγκεκριμένα μεταλλαγμένα κύτταρα θεωρούνται πιθανή αιτία πρόκλησης καρκίνου. Η ακτινοβολία που χρησιμοποιήθηκε στα πειράματα ανέρχονταν από 0,3 έως και 2 watt ανά χιλιογράμμο ιστού, σύμφωνα με την κλίμακα SAR. Τα αποτελέσματα όμως αυτά θεωρούνται προκαταρκτικά και δεν έχουν ακόμα δημοσιευθεί σε κάποια επιστημονική επιθεώρηση, ούτε έχουν διασταυρωθεί από άλλες ομάδες επιστημόνων.

5.4.2.1.4 Wiley-Liss Inc

Η Wiley-Liss Inc διενέργησε μια έρευνα σχετικά με τις επιπτώσεις που έχει ηλεκτρομαγνητικό πεδίο εντάσεως 0.2mT, το οποίο δημιουργείται από ημιτονοειδές ρεύμα των 50Hz, επάνω στα κύτταρα των ερυθρών αιμοσφαιρίων και στις καρδιακές λειτουργίες 24 αρσενικών λευκοπαθικών (αλβίνων) ποντικών. Τα αποτελέσματα της έρευνας αυτής έδειξαν πως τα ποντίκια που υποβλήθηκαν σε αυτή την έκθεση σημείωσαν μείωση στην ελαστικότητα και περατότητα της μεμβράνης των κυττάρων των ερυθρών αιμοσφαιρίων καθώς και αλλαγές στην μοριακή δομή του hemoglobin. Επίσης, το EGC των εκτιθέμενων ποντικών είχε αλλοιωθεί σε μεγάλο βαθμό.

5.4.2.2 Κινητά τηλέφωνα

5.4.2.2.1 Σουηδικό Εθνικό Ινστιτούτο Εργασίας

Η συγκεκριμένη έρευνα, που κράτησε έναν ολόκληρο χρόνο, πραγματοποιήθηκε υπό την αιγίδα του Σουηδικού Εθνικού Ινστιτούτου Εργασίας, της νορβηγικής SINTEF Unimed και της νορβηγικής υπηρεσίας για την προστασία από την ακτινοβολία (Norwegian Radiation Protection Authority) με σκοπό να ανακαλύψουν αν και κατά πόσο υπάρχουν επιπτώσεις στην υγεία των εργαζομένων από την χρήση κινητών τηλεφώνων. Συνολικά βρέθηκε πως το 25% των ερωτηθέντων εμφανίζει απώλεια μνήμης, το 50% πονοκεφάλους και σχεδόν το 70% νιώθει μια αφύσικη υπνηλία. Σημαντικό είναι επίσης το γεγονός ότι ένας στους τρεις συμμετέχοντες, δήλωσε ότι αντιμετωπίζει πρόβλημα συγκέντρωσης κατά τη διάρκεια, ή αμέσως μετά από ένα τηλεφώνημα. Τα συμπτώματα βρέθηκαν να είναι πιο συχνά στους χρήστες κάτω των 30 ετών και σε αυτούς που χρησιμοποιούν πολύ συχνά το κινητό τους τηλέφωνο. Σχετικά με αυτά τα ευρήματα, ο ερευνητής Dr. Gunnhild Oftedal δήλωσε πως "μπορεί να υπάρχουν πολλοί παράγοντες που να οδηγούν σε αυτά τα συμπτώματα, δεν μπορούμε όμως να αγνοήσουμε και τον παράγοντα της ακτινοβολίας." Μια ανεξάρτητη έρευνα, για παράδειγμα, έφτασε στο συμπέρασμα

πως οι πόνοι στο λαιμό, οφείλονται στην κύρτωση του κεφαλιού που κάνουν οι άνθρωποι, όταν μιλάνε στο τηλέφωνο και το έχουν στερεώσει στον ώμο τους για πολύ ώρα. Ειδικοί, από το πανεπιστήμιο του Surrey βρήκαν πως μιλώντας πολύ ώρα στο τηλέφωνο με αυτόν τον τρόπο, αυξάνεται ο κίνδυνος για σκλήρυνση των μυών, ερεθισμούς στους τένοντες, και δισκοπάθειες. Οπότε, επιβάλλεται η χρήση ακουστικών handsfree, ώστε το κεφάλι να παραμένει σε όρθια στάση και η εκπομπή ακτινοβολίας μακριά από τον εγκέφαλο.

5.4.2.2 Βρετανοί και Κινέζοι μελετούν τις επιπτώσεις στα παιδιά

Έρευνα που πραγματοποιήθηκε από Βρετανούς επιστήμονες δείχνει ότι σε σχέση με τους ενήλικες, τα παιδιά λόγω του ότι έχουν μικρότερα αυτιά και λεπτότερο κρανιακό φλοιό, ενδέχεται να απορροφήσουν 50% περισσότερη ακτινοβολία χρησιμοποιώντας κινητό τηλέφωνο. Σε ένα παιδί πέντε χρονών η ακτινοβολία θα απορροφηθεί στο 50% του εγκεφάλου του, ενώ σε ένα παιδί δέκα χρονών η ακτινοβολία θα επηρεάσει το 30% της φαιάς ουσίας του εγκεφάλου του. Επίσης, Κινέζοι γιατροί υποστηρίζουν ότι η χρήση κινητών τηλεφώνων σε νεαρές ηλικίες μπορεί να επηρεάσει το κρανιακό νεύρο. Αυτό έχει ως αποτέλεσμα ημικρανίες, απώλεια μνήμης, καθώς και διαταραχές ύπνου, αναφέρει ο Liang Xuanmei, γιατρός στο Lanzhou Chinese & Western Medicine Hospital και προσθέτει πως "όσοι παίζουν παιχνίδια στα κινητά τηλέφωνα συχνά νιώθουν ενοχλήσεις. Σε ορισμένους παρουσιάζεται το σύνδρομο του καρπιαίου σωλήνα, ή ακόμα και διαταραχές των ακροδακτύλων από την πίεση που ασκούν στα πλήκτρα, ενώ σε άλλες περιπτώσεις υπάρχουν ακόμα και οφθαλμικές επιπλοκές."

5.4.2.3 Australian Communications Authority & Radiation Protection and Nuclear Safety Agency

Άσφαλή για την υγεία τα 3G δίκτυα έδειξε έρευνα σχετικά με τις επιπτώσεις της εκπομπής των εγκαταστάσεων 3ης γενιάς κινητής τηλεφωνίας που παρουσίασε στο ευρύ κοινό η αυστραλιανή αρχή επικοινωνιών (Australian Communications Authority - ACA) μαζί με την αυστραλιανή αρχή που είναι υπεύθυνη για την προστασία από τις ακτινοβολίες και για την πυρηνική ασφάλεια (Radiation Protection and Nuclear Safety Agency - ARPANSA). Ο αντιπρόεδρος της ACA, δρ Robert Horton εξήγησε τι είναι τελικά γνωστό σχετικά με τις επιπτώσεις της παραγόμενης από 3G πομπής, ηλεκτρομαγνητικής ακτινοβολίας, καθώς και τι προσπάθειες γίνονται ώστε να περιοριστεί αυτή για την προστασία της υγείας των αυστραλών. "Καθώς πλέον τα 3G δίκτυα έχουν κάνει την εμφάνισή τους στην Αυστραλία οι απορίες είναι πολλές. Στόχος αυτής της έρευνας ήταν να κατευνάσουμε τις ανησυχίες του κόσμου σχετικά με το θέμα της εκπεμπόμενης ακτινοβολίας", είπε. "Η ακτινοβολία των 3G πομπών θεωρείται χαμηλή, με μέσο όρο εκπομπής 3 watt ενός σταθμού βάσης, το οποίο

αποτελεί λίγο περισσότερο από το ένα δέκατο εκπομπής ενός ασυρμάτου ταξί, περιπολικού ή ασθενοφόρου", δήλωσε. Εξηγώντας περισσότερο το θέμα, είπε πως οι κεραίες των δικτύων 3G χρειάζονται λιγότερη ενέργεια στις κεραίες τους από τους άλλους πομπούς λόγω του ότι χρησιμοποιούν μικρότερες κυψέλες αλλά και προηγμένες τεχνολογίες για την κωδικοποίηση του σήματος. Ακόμα μέσω ειδικής τεχνολογίας η ενέργεια των 3G κινητών μειώνεται στο κατώτερο αναγκαίο επίπεδο (συνήθως χαμηλότερο κι από τα GSM και CDMA συστήματα), όσο χρειάζεται δηλαδή για να είναι απρόσκοπτη η επικοινωνία. Έτσι παράλληλα μειώνεται κι άλλο εκπομπή η ακτινοβολίας! Κάνοντας ένα βήμα παραπέρα, η ACA πρόσφατα ανακοίνωσε νέα όρια σχετικά με την μέγιστη επιτρεπόμενη ανθρώπινη έκθεση στην ηλεκτρομαγνητική ακτινοβολία, βασισμένα σε επίπεδα που τέθηκαν από την ARPANSA. Τα όρια αυτά είναι αρκετά χαμηλότερα από αυτά που έχουν αποδειχθεί να έχουν επιπτώσεις στον ανθρώπινο οργανισμό, ενώ όλες οι εταιρίες κινητής τηλεφωνίας υποχρεώνονται να θέσουν τους πομπούς τους και τις κεραίες τους εντός αυτών των ορίων, μέσα σε ένα εύλογο χρονικό διάστημα.

5.4.2.2.4 National Institute of Environmental Health Sciences

Στο Πανεπιστήμιο Lund της Σουηδίας τελείωσε τον Ιανουάριο του 2003 μια έρευνα σχετικά με τις επιπτώσεις της έκθεσης σε ηλεκτρομαγνητικά πεδία των 900MHz (αυτά που χρησιμοποιούνται στην κινητή τηλεφωνία). Σε αυτή την έρευνα, υποβλήθηκαν 3 ομάδες των 8 ποντικών σε δίωρη έκθεση ηλεκτρομαγνητικών πεδίων, διαφορετικών εντάσεων, παρόμοιων με αυτών που χρησιμοποιούν τα GSM τηλέφωνα. Τα αποτελέσματα της έρευνα έδειξαν, για πρώτη φορά, στοιχεία που αποδεικνύουν ότι η έκθεση σε ηλεκτρομαγνητικά πεδία κινητών τηλεφώνων μπορούν να προκαλέσουν βλάβες στους νευρώνες του φλοιού, του ιππόκαμπου και της γάγγλιας του εγκεφάλου των ποντικών που εκτέθηκαν σε αυτού του είδους τις ακτινοβολίες. [26]

5.4.2.2.5 Έρευνα του νοσοκομείου του Birmingham

Σε ένα νοσοκομείο του Bristol, πομποί εμφυτεύτηκαν στα κεφάλια εθελοντών για αρκετό χρονικό διάστημα. Αυτοί οι πομποί εξέπεμπαν ηλεκτρομαγνητικά κύματα παρόμοια με αυτά των κινητών τηλεφώνων. Έπειτα από αυτή την έκθεση, ερευνητές στο νοσοκομείο του Birmingham, υπέβαλαν τους εθελοντές αυτούς σε απλά τεστ για να μετρήσουν την λειτουργία του εγκεφάλου τους. Το ένα τρίτο των ανθρώπων που υποβλήθηκαν στην έκθεση των μικροκυμάτων αυτών είχαν σημαντικά χειρότερες επιδόσεις στα τεστ.

5.4.2.3 Ασύρματα δίκτυα

5.4.2.3.1 Federal Communications Commission (FCC)

Σύμφωνα με τον FCC, εάν η χρήση των μικροκυμάτων στις τηλεπικοινωνίες μπορούν να προκαλέσουν προβλήματα υγείας στον άνθρωπο είναι ακόμα υπό αμφισβήτηση. Δεν υπάρχουν ακόμα σοβαρές ενδείξεις που να αποδεικνύουν ότι η χρήση των μικροκυμάτων (και συγκεκριμένα των 2,4GHz) στις τηλεπικοινωνίες μπορούν να βλάψουν τον άνθρωπο. Παρά ταύτα, ο οργανισμός παραδέχεται το γεγονός ότι υψηλή έκθεση σε μικροκυματική ακτινοβολία μπορεί να έχει ως αποτέλεσμα την αύξηση της θερμοκρασίας του δερμάτινου ιστού και κατ' επέκταση την αύξηση της θερμοκρασίας του σώματος. Άλλωστε με αυτόν τον τρόπο λειτουργεί και ο φούρνος μικροκυμάτων.

5.4.2.3.2 World Health Organization

Ο Παγκόσμιος Οργανισμός Υγείας είναι τμήμα του Οργανισμού Ηνωμένων Εθνών εξειδικευμένο πάνω σε θέματα υγείας. Ιδρύθηκε στις 7 Απριλίου του 1948. Αντικείμενό του, σύμφωνα με το καταστατικό του, όλοι οι άνθρωποι να μπορούν να απολαμβάνουν το υψηλότερο δυνατό επίπεδο υγείας.

Η υγεία ενός ανθρώπου είναι ορισμένη στο καταστατικό του, ως η κατάσταση πλήρους φυσικής, πνευματικής, και κοινωνικής ευεξίας. Σύμφωνα με την δημοσίευση υπ' αριθμών 193, που δημοσιεύθηκε τον Ιούνιο του 1993 από τον Οργανισμό, οι περισσότερες έρευνες που έχουν γίνει, είναι αποτελέσματα βραχυπρόθεσμης έκθεσης σε ηλεκτρομαγνητικά πεδία επιπέδου πολύ μεγαλύτερου από αυτά που δεχόμαστε καθημερινά από τις ασύρματες τεχνολογίες. Οι τρέχουσες επιστημονικές μελέτες προς το παρόν δεν έχουν βρει κανένα στοιχείο που να αποδεικνύει πως τα ηλεκτρομαγνητικά κύματα δημιουργούν ή επιταχύνουν την εμφάνιση του καρκίνου ή άλλων παρεμφερών ασθενειών.

Παρά ταύτα, η επίσημη θέση του οργανισμού είναι πως αναγνωρίζει ότι τα ηλεκτρομαγνητικά πεδία μπορεί να είναι αιτία πρόκλησης καρκίνου.

5.4.2.3.3 National Cancer Institute

Γιατροί από το National Cancer Institute των Ηνωμένων Πολιτειών, εξέτασαν τα δεδομένα υγείας για 40 χρόνια από 40.581 βετεράνους στρατιώτες και ναύτες που πολέμησαν στον πόλεμο της Κορέας από το 1950 έως το 1954. Η ιδιαιτερότητα που

χαρακτηρίζει τους βετεράνους αυτούς είναι ότι υποβλήθηκαν κατά τον πόλεμο της Κορέας σε πολύ ψηλές δόσεις ακτινοβολίας μικροκυμάτων από τα ραντάρ(τα ραντάρ χρησιμοποιούν μεγαλύτερες συχνότητες των 2,4GHz). Οι συχνότητες μικροκυμάτων των ραντάρ χρησιμοποιήθηκαν για σκοπούς ανίχνευσης, για τα οπλικά συστήματα και ακόμη για άμεσες βολές. Οι βετεράνοι αυτοί και ιδιαίτερα οι ναυτικοί, υποβλήθηκαν σε πολύ ψηλότερες δόσεις ακτινοβολίας μικροκυμάτων απ' ότι υποβαλλόμαστε εμείς συνήθως σήμερα.

Τα αποτελέσματά της έρευνας έδειξαν ότι η έκθεση σε ψηλά επίπεδα ακτινοβολίας μικροκυμάτων που προερχόταν από τα ραντάρ, δεν προκάλεσε στους βετεράνους αυτούς περισσότερους καρκίνους από ότι στον υπόλοιπο πληθυσμό. Μάλιστα βρέθηκε οι άνδρες αυτοί, είχαν 35% λιγότερες πιθανότητες να πεθάνουν κατά τη διάρκεια των 40 ετών της έρευνας σε σύγκριση με τους υπόλοιπους άνδρες. Το γεγονός αυτό πιστεύουν οι ερευνητές, οφείλεται στο ότι ένα από τα βασικά κριτήρια της επιλογής των ναυτών, είναι η πολύ καλή τους υγεία και υποχρεώνονται να διατηρούνται σε μια πολύ καλή φυσική κατάσταση κατά τη διάρκεια της υπηρεσίας τους. Φαίνεται λοιπόν ότι η έκθεση σε ψηλά επίπεδα ακτινοβολίας μικροκυμάτων από ραντάρ δεν είχε επιπτώσεις με περισσότερους καρκίνους ή αυξημένους θανάτους στη μεγάλη αυτή ομάδα βετεράνων.

5.5.1 Πώς ποσοτικοποιείται η ενέργεια των ραδιοκυμάτων;

Τα κύματα και τα πεδία ΡΣ διαθέτουν ηλεκτρικές και μαγνητικές συνιστώσες. Η ένταση του πεδίου ΡΣ εκφράζεται με βάση την ένταση και των δύο συνιστωσών. Η μονάδα "Volt ανά μέτρο" (V/m) χρησιμοποιείται για τη μέτρηση της έντασης του ηλεκτρικού πεδίου και η μονάδα "Ampere ανά μέτρο" (A/m) χρησιμοποιείται για να εκφράσει την ένταση του μαγνητικού πεδίου. Ένας άλλος συνήθης τρόπος για το χαρακτηρισμό ενός πεδίου ΡΣ είναι μέσω της πυκνότητας ισχύος. Η πυκνότητα ισχύος ορίζεται ως η ισχύς του κύματος που προσπίπτει στη μονάδα επιφάνειας. Η πυκνότητα ισχύος μπορεί να εκφραστεί σε μονάδες Watt ανά τετραγωνικό μέτρο (W/m^2), milliwatts (1 χιλιοστό του Watt) ανά τετραγωνικό εκατοστό (mW/cm^2) ή microwatts (1 εκατομμυριοστό του Watt) ανά τετραγωνικό εκατοστό ($\mu W/cm^2$).

Το μέγεθος που χρησιμοποιείται για τη μέτρηση της ποσότητας της ενέργειας των ραδιοκυμάτων που απορροφάται από το σώμα ονομάζεται **Ρυθμός Ειδικής Απορρόφησης (Specific Absorption Rate-SAR)**. Συνήθως εκφράζεται σε Watts ανά χιλιόγραμμο (W/kg) ή milliwatts ανά γραμμάριο (mW/g).

5.5.2 Αποστάσεις ασφαλείας

Από αυτά τα πειράματα μαζί με άλλα που έχουν γίνει πάνω σε ανθρώπινα ομοιώματα, μετρώντας την άνοδο της θερμοκρασίας που η ακτινοβολία προκαλούσε και συνυπολογίζοντας το Specific Absorption Rate (SAR)(μέτρο που έχει καθορίσει η FCC (Federal Communications Commission [24]) για το ποσοστό απορρόφησης της ακτινοβολίας από το σώμα) βρέθηκαν (όπως αναλύεται και στις διαφάνειες του κ. Νικήτα Γιαννάκου[10]) τα ακόλουθα μεγέθη για την ένταση του πεδίου σε σχέση με τα όρια του ανθρώπινου οργανισμού:

1 μέχρι $10 mW/cm^2$	Είναι επιτρεπτή η έκθεση λίγες ώρες κάθε 24ωρο
Πάνω από $10 mW/cm^2$	ΕΠΙΚΙΝΔΥΝΗ ΑΚΤΙΝΟΒΟΛΙΑ. Το προσωπικό δεν πρέπει να εκτίθεται σε ακτινοβολία αυτού του μεγέθους

Αυτό πρακτικά σημαίνει ότι αν υπερβούμε το $1mW/cm^2$ η άνοδος της θερμοκρασίας θα μας προκαλέσει μη αντιστρεπτή μεταβολή στα κύτταρα μας.

Επίσης άλλες έρευνες, χρησιμοποιώντας τα δεδομένα από την FCC, έχουν καταλήξει ότι μπορούμε να υπολογίσουμε μια απόσταση ασφαλείας για κάθε πηγή σύμφωνα με τον παρακάτω τύπο :

$$R_{\min} = \sqrt{N} 10(G-L)/10 P / \sqrt{4 \pi S}$$

όπου

- G το κέρδος (gain) της κεραίας
- P η ισχύς εισόδου στην κεραία
- L απώλειες (dB) μεταξύ πομπού - κεραίας
- N αριθμός πομπών συνδεδεμένοι με την κεραία
- S μέγιστη επιτρεπόμενη πυκνότητα ισχύος (W/m²)

Συμπέρασμα

Από την εμφάνιση και την έναρξη χρησιμοποίησης των ασύρματων δικτύων και έκτοτε, η επιρροή τους στην ζωή των ανθρώπων είναι κομβική.

Σύμφωνα με τις έρευνες πολλών πανεπιστημίων και οργανισμών του εξωτερικού, παρόλο που δεν απέβησαν απόλυτα ακριβείς με αξιόλογα συμπεράσματα, τα πορίσματα που βγήκαν είναι πως τα κινητά τηλέφωνα είναι αυτά που προκαλούν τις περισσότερες βλάβες στον ανθρώπινο οργανισμό σε αντίθεση με την απλή έκθεση στην ηλεκτρομαγνητική ακτινοβολία και πιο συγκεκριμένα τα μικρότερα σε ηλικία παιδιά είναι αυτά που αποκομίζουν τις μεγαλύτερες επιπτώσεις.

Μέχρι και σήμερα οι έρευνες συνεχίζονται, αλλά είναι ακόμα υπό αμφισβήτηση αν τα μικροκύματα και τα ραδιοκύματα επηρεάζουν σε τεράστιο βαθμό τον άνθρωπο.

Κεφάλαιο 6^ο

6.1 Ελληνικό νομοθετικό πλαίσιο για την Η/Μ ακτινοβολία

Στον τομέα των τηλεπικοινωνιών τα δικαιώματα και οι υποχρεώσεις των συνδρομητών και των εταιρειών προσδιορίζονται από τους ακόλουθους νόμους:

N. 3431/2006	«Περί ηλεκτρονικών επικοινωνιών και άλλων διατάξεων». Δημοσιεύτηκε στο ΦΕΚ 13/A/03-02-2006
N. 3115/2003	«Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών». Δημοσιεύτηκε στο ΦΕΚ 47/A/27-02-2003
N. 2867/2000	«Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις» (κατάργηση του Ν. 2246). Δημοσιεύτηκε στο ΦΕΚ 273/A/19-12-2000
Π.Δ 181/1999	«Προσαρμογή στην Οδηγία 1998/10/ΕΚ για την εφαρμογή της Παροχής Ανοιχτού Δικτύου (ONP) στη φωνητική τηλεφωνία και για την Καθολική Υπηρεσία για τις τηλεπικοινωνίες σε ανταγωνιστικό περιβάλλον». Δημοσιεύτηκε στο ΦΕΚ 170/A/20-08-1999
N. 2774/1999	«Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα». Δημοσιεύτηκε στο ΦΕΚ 287/A/22-12-1999
N. 2578/1998	«Δομή και λειτουργία της τηλεπικοινωνιακής αγοράς». Δημοσιεύτηκε στο ΦΕΚ 30/A/17-02-1998, άρθρο 12
N. 2472/1997	«Προστασία δεδομένων προσωπικού χαρακτήρα». Δημοσιεύτηκε στο ΦΕΚ 50 A/10-04-1997
N. 2251/1994	«Προστασία του καταναλωτή». Δημοσιεύτηκε στο ΦΕΚ 191/A/16-11-1994.

Συγκεκριμένα, τα ελληνικά όρια για χώρους προσπελάσιμους από το γενικό πληθυσμό (για εργαζομένους σε εγκαταστάσεις κινητής τηλεφωνίας βλ. * σε **Σχημα**

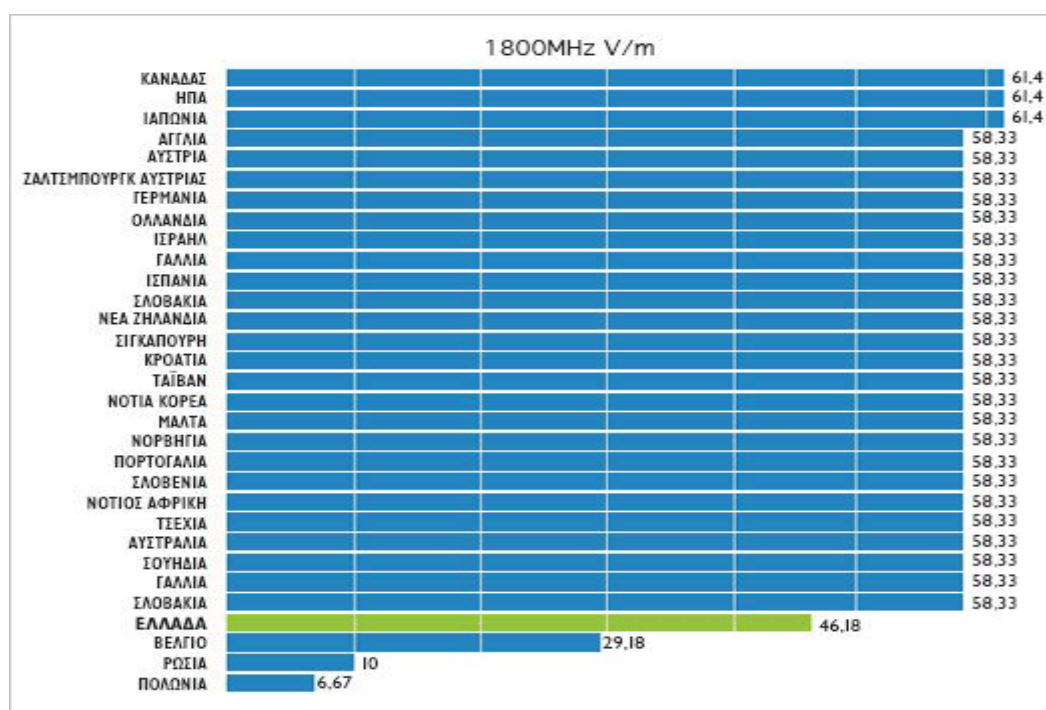
6.1) φαίνονται στον παραπάνω πίνακα και προκύπτουν από τα αντίστοιχα όρια έκθεσης που έχει θεσπίσει η Διεθνής Επιτροπή για την Προστασία από τη Μη-Ιοντίζουσα Ακτινοβολία (ICNIRP) μειωμένα στο 70% αυτών καθώς και στο 60% σε απόσταση μικρότερη των 300μ από σχολεία, νοσοκομεία, κλπ (βλ. ι)Νόμος 3431 / ΦΕΚ 13 Α' 3-2-2006 και ιι)Κοινή Υπ. Απόφαση 53571 / 3839 / [ΦΕΚ 1105 Β' 6-9-2006](#)).

Εφαρμογή	Ένταση Ηλεκτρικού Πεδίου (V/m)	Ένταση Μαγνητικού Πεδίου(A/m)	Πυκνότητα Ισχύος Ισοδύναμου Επίπεδου ΗΜ Κύματος (W/m ²)
Κινητή τηλεφωνία 900 MHz (GSM)	28.7 (24.6)	0.08 (0.066)	3.15 (2.7)
Κινητή τηλεφωνία 1800 MHz (DCS)	40.6 (34.8)	0.11 (0.096)	6.3 (5.4)
Κινητή τηλεφωνία 2100 MHz (UMTS)	42.7 (36.6)	0.11 (0.096)	7 (6)
Ασύρματα δίκτυα 2.4 GHz (WiFi)	42.7 (36.6)	0.11 (0.096)	7 (6)
Ασύρματα δίκτυα 3.5 GHz (WiMax)	42.7 (36.6)	0.11 (0.096)	7 (6)

Σχημα 6.1. Ελληνικά όρια έκθεσης ακτινοβολίας

6.2. Ευρωπαϊκή Ένωση - Διεθνώς νομοθετικό πλαίσιο για την Η/Μ ακτινοβολία

Οι βασικοί περιορισμοί και τα επίπεδα αναφοράς για την ηλεκτρομαγνητική ακτινοβολία των Σταθμών Βάσης κινητής τηλεφωνίας, έχουν θεσπιστεί με τη Σύσταση του Συμβουλίου της Ευρωπαϊκής Ένωσης «Σχετικά με τον περιορισμό της έκθεσης του κοινού σε ηλεκτρομαγνητικά πεδία 0 Hz - 300 GHz » (L199,1999/519/EC).



Σε ότι αφορά συγκριτικά στοιχεία ορίων που ισχύουν σε άλλες χώρες του κόσμου, αναφέρουμε ενδεικτικά:

οι Νορβηγία, Σουηδία, Αγγλία, Αυστρία, Γαλλία, Γερμανία, Ισπανία, Ολλανδία, Πορτογαλία, Μάλτα κ.α. έχουν θεσπίσει ακριβώς τα όρια που ορίζονται στην ICNIRP. Ο Καναδάς, οι ΗΠΑ και η Ιαπωνία έχουν θεσπίσει ελαστικότερα όρια, ενώ το Βέλγιο, η Ρωσία και η Πολωνία έχουν όπως και η Ελλάδα, αυστηρότερα όρια. Ο ΠΟΥ, μέσω του International EMF Project, προσπαθεί για την εναρμόνιση των ορίων μεταξύ των κρατών, για να μην αμφισβητείται η επιστημονική τους εγκυρότητα.

6.3.1 Πώς έχουν καθοριστεί τα όρια;

Για τη διασφάλιση της υγείας των ανθρώπων από τυχόν επιδράσεις της ηλεκτρομαγνητικής ακτινοβολίας έως και την περιοχή του φάσματος των ραδιοσημάτων (0-300 GHz), έχουν τεθεί διεθνή πρότυπα που θεσπίζουν όρια έκθεσης στα ηλεκτρομαγνητικά πεδία. Η πλειονότητα των εθνικών προτύπων και ορίων βασίζονται στις Οδηγίες που ορίζονται από τη **Διεθνή Επιτροπή Προστασίας από τη Μη Ιοντίζουσα Ακτινοβολία (International Commission on Non-Ionizing Radiation Protection, ICNIRP)**. Πρόκειται για ένα μη κυβερνητικό επιστημονικό οργανισμό, επίσημα αναγνωρισμένο από τον Παγκόσμιο Οργανισμό Υγείας. Η ICNIRP μελετά και αξιολογεί τα επιστημονικά αποτελέσματα των ερευνών από ολόκληρο τον κόσμο και εκδίδει οδηγίες με τις οποίες συνιστά συγκεκριμένα όρια για την έκθεση των ανθρώπων στα ηλεκτρομαγνητικά πεδία. Σε τακτά χρονικά διαστήματα, η ICNIRP εξετάζει αναλυτικά τη διεθνή έρευνα και βιβλιογραφία και επαναξιολογεί τις οδηγίες που έχει εκδώσει.

Ο **Παγκόσμιος Οργανισμός Υγείας** αναφέρει ότι τα όρια που προτείνουν οι οδηγίες της ICNIRP, έχουν βασιστεί σε προσεκτική μελέτη του συνόλου της σχετικής επιστημονικής βιβλιογραφίας. Λαμβάνουν υπόψη τους όλες τις γνωστές επιδράσεις και προσφέρουν προστασία απέναντι σε όλους τους εξακριβωμένους κινδύνους από έκθεση στα ηλεκτρομαγνητικά πεδία. Μάλιστα, οι οδηγίες της ICNIRP έχουν εφαρμόσει έναν παράγοντα ασφαλείας 50, χαμηλότερα από την οριακή τιμή κάτω από την οποία δεν έχουν αναφερθεί αρνητικά φαινόμενα στον ανθρώπινο οργανισμό.

6.3.2 Πώς διασφαλίζεται η τήρηση των θεσμοθετημένων ορίων;

Η τήρηση των διεθνών ορίων ασφαλούς έκθεσης αποδεικνύεται για όλες τις εταιρίες κινητής τηλεφωνίας από ξεχωριστή μελέτη για κάθε σταθμό βάσης, η οποία κατατίθεται στην Ελληνική Επιτροπή Ατομικής Ενέργειας (Ε.Ε.Α.Ε.), υπεύθυνο φορέα για την προστασία του πληθυσμού και του περιβάλλοντος από τις μη ιονίζουσες ακτινοβολίες. Κατά τη λειτουργία των σταθμών βάσης, η τήρηση των ορίων ελέγχεται περιοδικά ή οποτεδήποτε αυτό κριθεί απαραίτητο με μετρήσεις που διενεργούνται από συνεργείο της Ε.Ε.Α.Ε. αυτεπάγγελα.

Παράλληλα, υπάρχουν τρία προγράμματα συστηματικών μετρήσεων της Η/Μ ακτινοβολίας στη χώρα μας: [πεδίων 24](#), [ΕΡΜΗΣ](#), [ΦΑΣΜΑ](#). Τα προγράμματα αυτά αποτελούν ερευνητικό έργο των εργαστηρίων ραδιοεπικοινωνιών του Εθνικού Μετσόβιου Πολυτεχνείου (Ε.Μ.Π.), του Αριστοτέλειου Πανεπιστημίου Θεσσαλονίκης (Α.Π.Θ.), του Πανεπιστημίου Αιγαίου και του Πανεπιστημίου/Πολυτεχνείου Κρήτης.

Όλες οι μετρήσεις που έχουν γίνει –τόσο από την ΕΕΑΕ όσο και από τα 3 προγράμματα συστηματικών μετρήσεων-, έχουν δείξει ότι η ισχύς των ραδιοκυμάτων της κινητής τηλεφωνίας είναι από εκατοντάδες έως χιλιάδες φορές κάτω από τα όρια ασφαλούς έκθεσης, ακόμα και σε απόσταση λίγων μέτρων από τις κεραιές.

6.3.3 Ποιοι έχουν θέσει τα όρια ασφαλούς έκθεσης; Έχουν επιστημονική βάση;

Το Συμβούλιο της Ευρωπαϊκής Ένωσης, κατόπιν σχετικής εισήγησης ειδικής επιστημονικής επιτροπής υιοθέτησε τα όρια για την προστασία του κοινού της ICNIRP (International Commission on Non Ionizing Radiation Protection – Διεθνής Επιτροπή για την Προστασία από τις Μη Ιοντίζουσες Ακτινοβολίες), όπως αυτά παρουσιάστηκαν στις σχετικές κατευθυντήριες γραμμές της. Η ICNIRP είναι ανεξάρτητη, μη κυβερνητική επιστημονική οργάνωση, επίσημα αναγνωρισμένη από τον Παγκόσμιο Οργανισμό Υγείας, το Διεθνές Γραφείο Εργασίας και την Ευρωπαϊκή Ένωση που ασχολείται με την προφύλαξη των ανθρώπων από τις μη ιοντίζουσες ακτινοβολίες (όπως είναι αυτές που χρησιμοποιούνται στα συστήματα κινητής τηλεφωνίας). Έχει ως μέλη διεθνώς αναγνωρισμένους επιστήμονες που καλύπτουν τους χώρους της ιατρικής, της βιολογίας, της επιδημιολογίας, της φυσικής και της μηχανικής.

***Υπεύθυνη Δήλωση:** Βεβαιώνω εγώ ο Δημήτριος Φλέγκας με επιβλέπων καθηγητή τον κύριο Λάμπρο Δρόσο είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου.*

ΒΙΒΛΙΟΓΡΑΦΙΑ

- World Health Organization, Electromagnetic fields (WHO EMF Project)
- Non-Ionizing Radiation, Part 1: Static and Extremely Low-Frequency (ELF) Electric and Magnetic Fields, Summary of Data Reported and Evaluation, Monographs, International Agency for Research on Cancer
- Electric Power Research Institute (EPRI)
- How Safe Is Wireless Computer Networking?
- Institute of Informatics and Telecommunication – Τι ακτινοβολούν οι σταθμοί και τα κινητά μας
 - Ασύρματο Δίκτυο Τρίπολης
 - Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών
- Ασύρματο Δίκτυο Θεσσαλονίκης
- Is Wi-Fi Bad for Your Health? – Paul Swider
- The Royal Society of Canada
- Wireless Network Access Point (WNAP) Set Up Guide - Appendix B : Health & Safety - Toronto Wireless Community Network
- Connected Home, Rethinking Microsoft, and Wireless Health Issues – Paul Thurrott
- ETSI - European Telecommunications Standards Institute
- Εγκυκλοπένδια του φωτός – Ηλεκτρομαγνητική ακτινοβολία
- Ηλεκτρομαγνητική ακτινοβολία

- Medlook – Ηλεκτρομαγνητικά πεδία και υγεία
- Evaluation of the effects of electric and magnetic fields in humans
- National Radiological Protection Board (NRPB)
<http://www.nrpb.org/>
- Assessing human exposure to power-frequency electric and magnetic fields
- National Institute of Environmental Health Sciences
- Radio Frequency Safety
- National Institute for Occupational Safety and Health fact sheet on EMF
- International Agency for Research on Cancer (IARC)
- International Commission on Non-Ionizing Radiation Protection (ICNIRP)
- Ελληνική Επιτροπή Ατομικής Ενέργειας
- National Institute for Environmental Health Science (NIEHS) RAPID Program
- Wireless networks. Amsterdam : Baltzer Science Publishers, c1995-
- Wireless information networks / Kaveh Pahlavan, Allen H. Levesque. by Pahlavan, Kaveh, 1951-New York: Wiley, c1995.
- Wireless intelligent networking / Gerry Christensen, Paul G. Florack, Robert Duncan. by Christensen, Gerald Boston, MA: Artech House, c2001.
- Wireless LANs: implementing interoperable networks / Jim

Geier. by Geier, James T. [Indianapolis, Ind.]: Macmillan Technical Publishing, c1999.

- Data over wireless networks: Bluetooth, WAP, and wireless LANS / Gilbert Held. by Held, Gilbert, 1943-New York, NY : McGraw-Hill, c2001.
- Building wireless community networks / Rob Flickenger. by Flickenger, Rob. Sebastopol, CA: O'Reilly, c2002.
- Mobile networks and applications: MONET. Amsterdam, Netherlands Baltzer Science Publishers, 1996.
- Wireless communications and mobile computing Chichester, UK: John Wiley & Sons,
- Handbook of wireless networks and mobile computing / edited by Ivan Stojmenović. New York: Wiley, 2002.
- Maximum wireless security / Cyrus Peikari, Seth Fogie. by Peikari, Cyrus. Indianapolis, IN : Sams Pub., c2003.
- Enhanced wireless networking certification / [written by Max Main]. by Main, Max. Upper Saddle River, N.J: Pearson Education, c2003.
- The handbook of ad hoc wireless networks / edited by Mohammad Ilyas. Boca Raton: CRC Press, c2003.
- Wireless local area networks : the new wireless revolution / edited by Benny Bing. New York: Wiley-Interscience, c2002.
- Wireless communications and networking / William Stallings.
Βιβλιογραφία
Ασύρματα δίκτυα 802.11 175
by Stallings, William Upper Saddle River, N.J: Prentice Hall, c2002.

- Wireless communications and networking / Jon W. Mark and Weihua Zhuang. by Mark, Jon W. Upper Saddle River, N.J.: Prentice Hall, c2003.
- Wireless personal and local area networks / Axel Sikora. by Sikora, Axel Chichester, West Sussex, England: John Wiley, c2003.
- Encyclopedia of wireless telecommunications / Francis Botto. by Botto, Francis New York : McGraw-Hill, 2002.
- 802.11 wireless networks: the definitive guide by Gast, Matthew 2002 O'Reilly
- Home networking technologies and standards / Theodore B. Zahariadis. by Zahariadis, Theodore B. Boston: Artech House, 2003.

Ηλεκτρονικές σελίδες

Geosystems Christopherson

- http://wps.prenhall.com/esm_christopherson_geosystems_5/0,6339,389792-main,00.html

World Health Organization (WHO)

- <http://www.who.int/peh-emf/about/en/>

New York Times

- <http://www.nytimes.com>

National Cancer Institute

- <http://aje.oupjournals.org/cgi/content/abstract/155/9/810>

Royal Society of Canada

- <http://www.rsc.ca/>

Τα αποτελέσματα της έρευνας της RSC:

- http://www.rsc.ca//files/publications/expert_panels/RF//expert_panel_radiofrequency_update2.pdf
- http://www.rsc.ca//files/publications/expert_panels/RF//RFreport-en.pdf

θέση του World Health Organization

- <http://www.who.int/mediacentre/news/statements/statementemf/en/>

International Agency for Research Cancer

- <http://www.iarc.fr/ENG/Units/RCAd.html>

ICNIRP

- <http://www.icnirp.net/activities.htm>

National Cancer Institute

- <http://aje.oupjournals.org/cgi/content/abstract/155/9/810>

ETSI

- <http://www.etsi.org>

Πρότυπο ETSI EN 300 328

- http://webapp.etsi.org/action%5COP/OP20041105/en_300328v010601o.pdf

EETT

- <http://www.eett.gr/>

ΦΕΚ 11/7 2002 αριθμός φύλλου 895, δεύτερο τεύχος

- http://www.eett.gr/gr_pages/telec/kanonistika_keimena/APOF2002/APOF254-72FEK.pdf

παραδείγματα νοσοκομείων

- <http://www.engadget.com/entry/7684782035846660/>
- <http://wifinetnews.com/archives/003876.html>
- http://www.pdacortex.com/WiFi_Patients.htm
- <http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=100216>
- <http://www.proxim.com/about/pressroom/pressrelease/pr2003-07-29.html>
- http://www.cio.com/archive/080103/mobile_sidebar_1.html
- <http://www.cioinsight.com/article2/0,1397,1170383,00.asp>
- <http://www.canadait.com/cfm/index.cfm?It=106&Id=18593&Se=2&Lo=2>

μαιευτήριο στο Σικάγο

- <http://washingtontimes.com/upi-breaking/20040429-101218-5859r.htm>

παιδιατρικά νοσοκομεία

- <http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=100216>

παραδείγματα σχολείων

- <http://www.enterblog.com/200304270630.php>
- http://searchnetworking.techtarget.com/originalContent/0,289142,side7_gci785

343,00.html

- <http://www.psusd.us/>
- <http://www.rm.com/HE/Products/Story.asp?cref=PS95306>

δημόσια πάρκα

- <http://www.wi-fiplanet.com/news/article.php/3087291>

EDUnet

- <http://www.crm2day.gr/news/106795783272998.shtml>

Wireless Devices, Standards, and Microwave Radiation in the Education Environment - Gary Brown, October, 2000

- <http://www.emfacts.com/wlans.html>

Suit Alleges Health Risks of Wi-Fi

- http://www.cio.com/archive/021504/tl_lawsuits.html

Health Protection Agency

- <http://www.hpa.org.uk/>

Federal Communications Commission

- <http://www.fcc.gov>

Έρευνα του National Radiological Protection Board

- http://www.hpa.org.uk/radiation/publications/documents_of_nrpbfdfs/doc_15

Έρευνα του Πανεπιστημίου Lund της Σουηδίας

- <http://www.applelinks.com/p5/index.php?URL=http://www.elektrosmognews.de/salfordjan2003.pdf>

de/salfordjan2003.pdf

Έρευνα του Wiley-Liss Inc

- <http://www3.interscience.wiley.com/cgi-bin/abstract/106561095/ABSTRACT?CRETRY=1>

Έρευνα του νοσοκομείου του Birmingham

- http://www.theregister.co.uk/1999/03/01/mobile_phone_cause_memory_loss/
- <http://broadband.uop.gr/>
- <http://www.broad-band.gr/>
- <http://www.awmn.gr/>
- <http://www.swn.gr/>
- <http://www.wi-fiplanet.com/>
- <http://www.esoterraka.com/>
- <http://www.eekt.gr/>
- http://www.dimotikosantilogos.gr/index.php?option=com_content&view=article&id=27-kiniti-tilefonia-kai-hm-aktinobolia&catid=13&Itemid=113