ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Πρωτόκολλα Ασύρματων Προσωπικών, Τοπικών, Μητροπολιτικών και Δικτύων Ευρείας Περιοχής

Σχήμα 1[1]

Του φοιτητή
Χρηστίδη Αρίσταρχου
Αρ. Μητρώου: 175061

Επιβλέπων
Ονοματεπώνυμο Βίτσας Βασίλης
Βαθμίδα Καθηγητής

Ημερομηνία 23/5/2024

Τίτλος Π.Ε. Πρωτόκολλα Ασύρματων Προσωπικών, Τοπικών, Μητροπολιτικών και Δικτύων Ευρείας Περιοχής

Κωδικός Π.Ε. 24121

Ονοματεπώνυμο φοιτητή Χρηστίδης Αρίσταρχος

Ονοματεπώνυμο εισηγητή Βασίλης Βίτσας

Ημερομηνία ανάληψης Π.Ε.11-02-2024

Ημερομηνία περάτωσης Π.Ε.23-5-2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Πρόλογος

Η παρούσα πτυχιακή εργασία με τίτλο «Πρωτόκολλα Ασύρματων Προσωπικών, Τοπικών, Μητροπολιτικών και Δικτύων Ευρείας Περιοχής» αποτελεί την επισφράγιση της ακαδημαϊκής μου πορείας στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων. Η ενασχόλησή μου με το συγκεκριμένο θέμα προέκυψε από το βαθύ ενδιαφέρον μου για τις ασύρματες τεχνολογίες, οι οποίες αποτελούν αναπόσπαστο κομμάτι της καθημερινότητάς μας και διαδραματίζουν καθοριστικό ρόλο σε πολλούς τομείς της ζωής μας, από την απλή επικοινωνία και την ψυχαγωγία, μέχρι τις επιστήμες, την υγεία και την αυτοματοποίηση. Η πτυχιακή αυτή εργασία μου έδωσε την ευκαιρία να εμβαθύνω στην αιχμή της τεχνολογίας των ασύρματων δικτύων. Πιο συγκεκριμένα, στην παρούσα εργασία αναλύονται οι βασικές αρχές των ασύρματων δικτύων, ο εξοπλισμός που απαιτείται για τις ασύρματες ζεύξεις, οι ασύρματες τεχνολογίες Wi-Fi, Bluetooth, ZigBee & WiMAX, τα δίκτυα κινητών επικοινωνιών καθώς και τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται στις ασύρματες επικοινωνίες. Η εργασία αυτή αποτέλεσε μια πρόκληση η οποία με ώθησε στο να αναπτύξω τις ικανότητές μου στην έρευνα της βιβλιογραφίας, την ανάλυση και την κριτική σκέψη. Η μελέτη των διαφορετικών τεχνολογιών, η ανάλυση των πλεονεκτημάτων και των μειονεκτημάτων τους, καθώς και η αξιολόγηση των εφαρμογών τους, μου έδωσαν μια ολοκληρωμένη εικόνα του τομέα των ασύρματων δικτύων, η οποία αποτελεί πολύτιμη και χρήσιμη γνώση στη μετέπειτα επαγγελματική μου σταδιοδρομία. στον τομέα των ασύρματων δικτύων και των τηλεπικοινωνιών.

Περίληψη

Η παρούσα πτυχιακή εργασία εξετάζει την λειτουργία, την εξέλιξη, τις εφαρμογές και την ασφάλεια των ασύρματων δικτύων. Αρχικά, παρουσιάζονται μία σύντομη ιστορική εξέλιξη των ασύρματων επικοινωνιών, επικεντρωμένη στα δίκτυα Wi-Fi και κινητής τηλεφωνίας, τα μοντέλα OSI (Open Systems Interconnection) και TCP/IP (Transmission Control Protocol/Internet Protocol), καθώς και οι βασικότεροι οργανισμοί τυποποίησης στον τομέα των ασύρματων επικοινωνιών, όπως η Wi-Fi Alliance, η Bluetooth SIG, η Wireless Broadband Alliance, το IEEE (Institute of Electrical and Electronics Engineers) και η Telecommunications Industry Association. Ακολούθως, αναλύονται οι βασικές έννοιες των ασύρματων δικτύων, όπως η συχνότητα ραδιοκυμάτων, τα κανάλια επικοινωνίας και οι τεχνικές διαμόρφωσης του σήματος. Στη συνέχεια, παρατίθενται οι βασικοί τύποι ασύρματων δικτύων: WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network) και WWAN (Wireless Wide Area Network). Για κάθε τύπο δικτύου, περιγράφονται οι τεχνολογίες που χρησιμοποιούνται, οι εφαρμογές τους, τα πλεονεκτήματα και τα μειονεκτήματά τους. Κατόπιν, η πτυχιακή αυτή εργασία αναφέρεται στον εξοπλισμό που απαιτείται για την επίτευξη των ασύρματων ζεύξεων. Παρατίθενται τα χαρακτηριστικά, οι λειτουργίες και τα είδη των κεραιών, των ασύρματων σημείων πρόσβασης (access points) και των δρομολογητών (routers). Επιπλέον, η εργασία εμβαθύνει στα ασύρματα δίκτυα που βασίζονται στη σειρά προτύπων IEEE 802.11 (“Wi-Fi”), αναλύοντας την αρχιτεκτονική, τη λειτουργία, και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν, όπως το CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Επίσης, εξετάζεται σύντομα η αρχιτεκτονική και η λειτουργία των τεχνολογιών Bluetooth, ZigBee και WiMAX. Επίσης παρατίθεται η εξέλιξη των δικτύων κινητών επικοινωνιών ακολουθούμενη από τη δομή και τις βασικές λειτουργίες του δικτύου για τη μετάδοση φωνής και δεδομένων. Τέλος αναλύονται οι απειλές που δοκιμάζουν τα ασύρματα δίκτυα καθώς και οι τεχνικές ασφάλειας που εφαρμόζονται για την προστασία των μεταδιδόμενων δεδομένων, όπως φιλτράρισμα διευθύνσεων MAC (Media Access Control), αυθεντικοποίηση ανοικτού συστήματος ή κλειστού κλειδιού με αλγορίθμους κρυπτογράφησης.

Wireless Personal, Local Area, Metropolitan and Wide Area Network Protocols

Aristarchos Christidis

Abstract

This thesis discusses the operation, the evolution, the applications and the security of the wireless networks. Firstly, a brief history of wireless communications, focusing on Wi-Fi and mobile networks, the OSI (Open Systems Interconnection) model, the TCP/IP (Transmission Control Protocol/Internet Protocol) model, and the wireless communications standardization organizations, such as the Wi-Fi Alliance, the Bluetooth SIG, the Wireless Broadband Alliance, the IEEE (Institute of Electrical and Electronics Engineers) and the Telecommunications Industry Association (TIA), are presented. Next, the basic concepts of wireless networks, such as radio frequency, communication channels and signal modulation techniques are discussed. Next, the main types of wireless networks are listed: WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network) and WWAN (Wireless Wide Area Network). For each type of network, the technologies used, their applications, their advantages and disadvantages are described. Then, this thesis discusses the equipment required to achieve wireless links. The characteristics, the functions and the types of antennas, wireless access points and routers are listed. In addition, this thesis delves into wireless networks based on the IEEE 802.11 standard series ("Wi-Fi"), analyzing the architecture, the operation, and the communication protocols they use, such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It also briefly examines the architecture and operation of Bluetooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4), and WiMAX (IEEE 802.16).The evolution of mobile communication networks is also discussed and is followed by the structure and the basic network functions performed for voice and data transmission. Finally, the threats experienced by wireless networks are analyzed as well as the security techniques used for the protection of the transmitted data, such as MAC (Media Access Control) address filtering, open-system or shared-key authentication with encryption algorithms.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1: Εισαγωγή

1.1 Ορισμός και Σημασία των Ασύρματων δικτύων

Τα ασύρματα δίκτυα αποτελούν έναν θεμελιώδη πυλώνα της σύγχρονης επικοινωνίας και της τεχνολογίας . Η συνεχής ανάπτυξη και εξέλιξη της τεχνολογίας έχει οδηγήσει στην ευρεία διάδοση και χρήση ασύρματων δικτύων σε πολλούς τομείς της καθημερινής μας ζωής. Από τις επικοινωνίες κινητής τηλεφωνίας και τα ασύρματα δίκτυα εντός επιχειρήσεων έως την ασύρματη σύνδεση στο Internet στα σπίτια μας αλλά και τη δυνατότητα σύνδεσης στο διαδίκτυο οποιασδήποτε συσκευής από οποιοδήποτε σημείο μέσω της τεχνολογίας Internet of Things (IoT), οι τεχνολογίες των ασυρμάτων δικτύων έχουν αλλάξει ριζικά τον τρόπο που επικοινωνούμε και αλληλοεπιδρούμε με το περιβάλλον μας. Τα ασύρματα δίκτυα αναφέρονται σε οποιαδήποτε δίκτυα επικοινωνιών χωρίς τη χρήση καλωδίωσης. Αυτό σημαίνει ότι η μετάδοση δεδομένων και η επικοινωνία γίνονται μέσω σημάτων που μεταδίδονται στον αέρα, προσφέροντας μεγάλη ευελιξία ως προς τους χρήστες . Η εξέλιξη αυτών των τεχνολογιών έχει δώσει τη δυνατότητα σε κινητές συσκευές, όπως κινητά τηλέφωνα, φορητούς υπολογιστές και tablet, να συνδεθούν ασύρματα και να επικοινωνήσουν μεταξύ τους στο διαδίκτυο χωρίς την ανάγκη για φυσική σύνδεση. Η επίδραση των ασύρματων δικτύων είναι αναπόσπαστη στην καθημερινότητά μας. Από τα σπίτια μας μέχρι τα καταστήματα, τα γραφεία και τα μεγάλα εταιρικά δίκτυα, η ασύρματη επικοινωνία είναι παντού. Η ευκολία σύνδεσης, η ευελιξία και η φορητότητα που παρέχουν έχουν επιταχύνει την υιοθέτησή τους σε όλους τους τομείς της κοινωνίας.

Η σημασία των ασύρματων δικτύων στον σύγχρονο κόσμο είναι πολύ μεγάλη και πολύπλευρη. Καταρχάς, επιτρέπουν στις συσκευές να συνδέονται στο διαδίκτυο και να επικοινωνούν μεταξύ τους χωρίς την ανάγκη για πολύπλοκες φυσικές υποδομές. Αυτό τα κάνει εύκολα προ βάσιμα και επιτρέπει στους χρήστες να παραμένουν συνδεδεμένοι ακόμα και όταν βρίσκονται εν κίνηση.

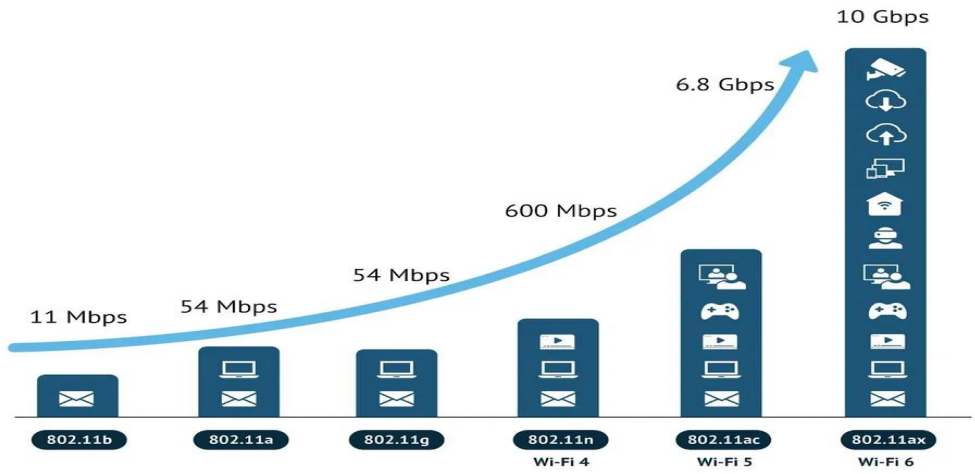
Ένας ακόμα σημαντικός λόγος για τη σημασία των ασύρματων δικτύων είναι η επικοινωνία μεταξύ των έξυπνων συσκευών και των συστημάτων του Internet of Things (IoT). Αυτές οι συσκευές ανταλλάσσουν συνεχώς δεδομένα για να παρέχουν υπηρεσίες και λειτουργίες που καθιστούν τη ζωή μας πιο εύκολη και ευχάριστη, σε διάφορες εφαρμογές της καθημερινότητας (εργασία, εκπαίδευση, ιατρική, γεωργία, βιομηχανία κλπ). Επιπλέον έχουν αλλάξει τον τρόπο εργασίας και τις επιχειρηματικές διαδικασίες. Επιτρέπουν στους εργαζομένους να συνδεθούν στα εταιρικά δίκτυα από οπουδήποτε, βελτιώνοντας την απόδοση και την ευελιξία τους. Αυτό συνεπάγεται σε αύξηση της παραγωγικότητας και μείωση του χρόνου που απαιτείται για την ολοκλήρωση εργασιών .Συνολικά, τα ασύρματα δίκτυα αποτελούν τον θεμέλιο λίθο της σύγχρονης ψηφιακής εποχής, επιτρέποντας τη σύνδεση, την επικοινωνία και την ανταλλαγή δεδομένων μεταξύ συσκευών και ανθρώπων σε όλο τον κόσμο.

1.2 Ιστορική Ανάπτυξη και Εξέλιξη

Η εξέλιξη των ασύρματων δικτύων έχει σημαντική ιστορία και έχει αλλάξει ριζικά τον τρόπο με τον οποίο επικοινωνούμε και συνδεόμαστε στον ψηφιακό κόσμο. Από την ανακάλυψη των ραδιοκυμάτων έως την εποχή του 5G, η ιστορία των ασύρματων δικτύων είναι μια ιστορία προόδου και καινοτομίας. Ιστορικά η μετάδοση δεδομένων με την βοήθεια των ραδιοκυμάτων προέρχεται απ’ τον 19ο αιώνα με την δημιουργία της ραδιοτηλεγραφίας. Παρόλα αυτά οι ρίζες του ασυρμάτου δικτύου χρονολογείται έπειτα από την δημιουργία του ALOHAnet στο Πανεπιστήμιο της Χαβάης το 1971.Τεχνολογικά χρησιμοποιούσε σήματα στην ζώνη συχνοτήτων των 400MHz για την μετάδοση πακέτων. Η τεχνολογία Ethernet άρχισε το 1973 και ολοκληρώθηκε μετά την καθιέρωση του προτύπου Ethernet IEE 802.3.

Η εμπορική δραστηριότητα του προτύπου IEEE 802.11 (Wireless LAN-WiFi) ξεκίνησε νωρίτερα από το 1997 όταν και καθιερώθηκε. Στην ελεύθερη αγορά το ασύρματο δίκτυο ήταν κυρίως ανενεργό μέχρι και το 1985, όταν η επιτροπή ομοσπονδιακών επικοινωνιών (FCC) χαλάρωσε τις απαιτήσεις άδειας

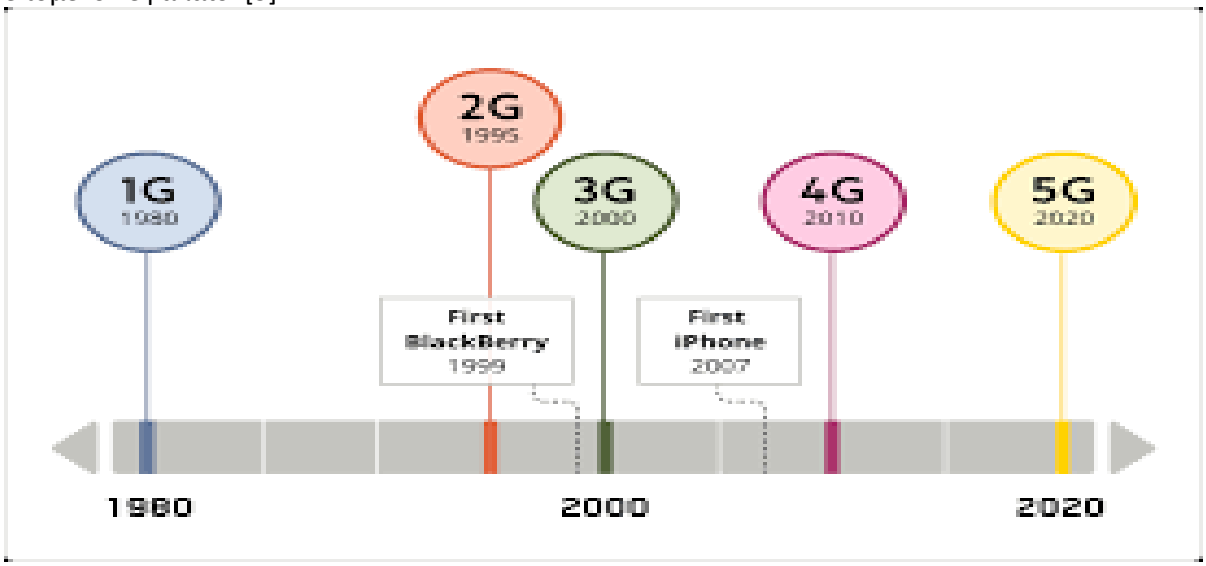
για τις ζώνες 900MHz, 2.4 GHz και 5 GHz. Αρκετές εταιρίες όπως η NCR, η AT&T και η Lucent Technologies έφεραν στην αγορά προϊόντα που εξυπηρετούν διαφορετικούς σκοπούς. Γι' αυτό τον λόγο μια ομάδα του IEEE δημιούργησε την πρώτη έκδοση του πρωτοκόλλου 802.11.
Περίπου μετά από δύο χρόνια, το 1999, κυκλοφόρησαν ενημερωμένες εκδόσεις του προτύπου, το 802.11a και το 802.11b. Μετά από ένα μικρό χρονικό διάστημα, μια ομάδα διαμορφώθηκε και δημιούργησε το Wireless Ethernet Compatibility Alliance (WECA) διότι πολλά προϊόντα δεν μπορούσαν να συνεργαστούν μεταξύ τους. Ο στόχος της ομάδας αυτής ήταν η συμμόρφωση των προϊόντων στα πρότυπα. Η ονομασία Wi-fi έγινε τόσο γρήγορα πασίγνωστη στην ελεύθερη αγορά ακολουθώντας το πρότυπο 802.11b, όπου η ομάδα άλλαξε το όνομα της σε Wi-Fi Alliance. Από το 1999 και έπειτα το IEEE συνεχίζει να εκδίδει καινούργιες ενημερώσεις για το πρότυπο LAN 802.11. Αυτές οι ενημερώσεις είχαν και έχουν στόχο την καλύτερη ασφάλεια, αξιοπιστία , ταχύτητα και μείωση της κατανάλωσης ενέργειας με καλύτερη εκμετάλλευσης της εκάστοτε τεχνολογία της εποχής. Για τις επόμενες δύο δεκαετίες κυκλοφόρησαν τα πρότυπα 802.11g το 2003, 802.11n το 2009, 802.11ac το 2013 και το 802.11ax το 2019. Ο ρυθμός μετάδοσης αυτών των προτύπων σταδιακά βελτιώθηκε όπως φαίνεται στο παρακάτω σχήμα 1. Μία μεγαλύτερη ανάλυση των προτύπων αυτών θα γίνει σε επόμενο κεφάλαιο.



Σχήμα 1-1: IEE Standard speeds[2]

Η αύξηση της απόδοσης, της ταχύτητας μετάδοσης, της ασφάλειας και η γενικότερη βελτίωση της τεχνολογίας των ασυρμάτων δικτύων WLANs διεύρυνε την χρήση τους. Το 2000 άρχισε η μεταβίβαση από χρήση LANs σε WLANs σε μεγάλη κλίμακα στις περισσότερες επιχειρήσεις .
Παράλληλα με την ανάπτυξη του WLAN, εταιρίες όπου πρόσφεραν τηλεπικοινωνιακές παροχές ανέπτυξαν μια τεχνολογία κινητής ευρυζωνικότητας. Ο κύριος σκοπός της τεχνολογίας αυτής είναι η παροχή πρόσβασης σε δεδομένα κυρίως σε κινητά τηλέφωνα (και στη συνέχεια σε άλλες κινητές συσκευές, πχ tablet, ρολόγια κλπ). Το 1990 πραγματοποιήθηκε η μεταβίβαση από τις υπηρεσίες

κινητής τηλεφωνίας πρώτης γενιάς (1G) σε δεύτερης γενιάς (2G). Η υπηρεσία αυτή επέτρεπε την αποστολή μηνυμάτων (SMS) και πρώιμες υπηρεσίες πολυμέσων. Η επιτυχία στο ευρύ κοινό ήταν τόσο μεγάλη όπου λόγο της τεράστιας ζήτησης, οι πάροχοι ξεκίνησαν μία καινούργια γενιά κινητών υπηρεσιών δεδομένων (3G). Ουσιαστικά το 3G πρόσφερε υψηλότερες ταχύτητες μετάδοσης δεδομένων, βελτιωμένες υπηρεσίες επικοινωνίας, αυξημένη κινητικότητα και προσωπικά hotspots. Στις αρχές του 2010 οι πάροχοι έστρεψαν την προσοχή τους προς τις τεχνολογίες 4G και έπειτα στην εξέλιξη του 4G γνωστή ως LTE (Long-Term Evolution). Η τεχνολογία αυτή πρόσφερε ακόμα μεγαλύτερες ταχύτητες και κατά τη δεκαετία του 2010 ήταν πανταχού παρούσα κυρίως στις Ηνωμένες Πολιτείες, επιτρέποντας σε έναν εργαζόμενο μιας επιχείρησης να εργάζεται από οπουδήποτε. Το 2020 κατασκευάστηκε μία καινούργια τεχνολογία, το 5G. Ο στόχος ήταν η υποστήριξη υπηρεσιών δεδομένων για μεγαλύτερος πλήθος συσκευών, μεγαλύτερη αξιοπιστία, χαμηλότερες καθυστερήσεις και υψηλότερες ταχύτητες. Η χρονολογική εξέλιξη των τεχνολογιών αυτών φαίνεται στο παρακάτω σχήμα 2. Η εμβάθυνση των παραπάνω τεχνολογιών θα γίνει σε επόμενο κεφάλαιο. [3]



Σχήμα 1-2: Time line of mobile networks[4]

1.3 Μοντέλο OSI

Το διαδίκτυο είναι ένα αρκετά περίπλοκο σύστημα και γι' αυτό το λόγο χρησιμοποιούμε μοντέλα που το χωρίζουν σε λογικά επίπεδα, ώστε να καταφέρουμε και να οργανώσουμε την αρχιτεκτονική του διαδικτύου. Μια αρχιτεκτονική οργανωμένη σε επίπεδα, μας επιτρέπει να μιλήσουμε για ένα κομμάτι ενός μεγάλου συστήματος, προσεγγίζοντας το ανεξάρτητα από τα υπόλοιπα. Κάθε επίπεδο παρέχει υπηρεσίας στα επίπεδα πάνω από αυτό μέσω διεπαφών (interfaces) και παράγει μηνύματα ώστε να επικοινωνεί απευθείας με το ίδιο επίπεδο στις ενδιάμεσες συσκευές ή στον παραλήπτη. Επίσης, τυχόν αλλαγές στα πρωτόκολλα ενός επιπέδου, δεν επηρεάζουν τα υπόλοιπα επίπεδα. Κάθε επίπεδο περιλαμβάνει κάποια πρωτόκολλα (κανόνες) που ορίζουν τον τύπο, τη μορφή των μηνυμάτων και περιγράφουν λεπτομερώς τις λειτουργίες του επιπέδου για να υπάρχει επιτυχής μετάδοση στο διαδίκτυο.

Το μοντέλο OSI (Open Systems Interconnection), του οργανισμού τυποποίησης ISO, είναι ένα μοντέλο εφτά επιπέδων, όπως φαίνεται στο σχήμα 3. Όσο πιο πάνω βρίσκεται ένα επίπεδο, πλησιάζει περισσότερο προς την εφαρμογή και όσο πιο κάτω, πλησιάζει προς το υλικό.

Ιστορικά στα τέλη του 1970 εμφανίστηκε μεγάλη ζήτηση για την ανάγκη για πρότυπα σχετικά με τον τρόπο επικοινωνίας των συνδεδεμένων πραγμάτων. Μία οργάνωση που εργαζόταν πάνω σε αυτό ήταν η International Organization for Standardization (ISO). Το μοντέλο OSI προοριζόταν να είναι το βιομηχανικό πρότυπο για το διαδίκτυο αλλά δεν κατάφερε να πείσει αρκετές βιομηχανίες να το ακολουθήσουν. Παρόλα αυτά χρησιμοποιείται μέχρι και σήμερα ως αναφορά πάνω σε κάποιο πρωτόκολλο του δικτύου από ανθρώπους του πεδίου.

Σχήμα 1-3: Layers of the Osi model[5]

Επίπεδο 1 : Το φυσικό επίπεδο το οποίο περιλαμβάνει το φυσικό εξοπλισμό που εμπλέκεται στην μεταφορά δεδομένων όπως τα καλώδια και οι διακόπτες, αλλά και τους κανόνες σύμφωνα με τους οποίους τα bit του μηνύματος μετατρέπονται στο σήμα που θα μεταδοθεί στο φυσικό μέσο.
Επίπεδο 2 : Το επίπεδο σύνδεσης δεδομένων παίρνει πακέτα από το επίπεδο δικτύου και τα προσθέτει περισσότερες πληροφορίες δημιουργώντας πλαίσια (frames). Το επίπεδο σύνδεσης δεδομένων είναι υπεύθυνο για τον έλεγχο ροής και τον έλεγχο σφαλμάτων στην εσωτερική επικοινωνία δικτύου και εξασφαλίζει τη μεταγωγή του μηνύματος στον επόμενο κόμβο.
Επίπεδο 3 : Το επίπεδο δικτύου είναι υπεύθυνο για τη δρομολόγηση πακέτων μεταξύ των κόμβων. Τα πρωτόκολλα του επιπέδου δικτύου περιλαμβάνουν διευθύνσεις IP, το Πρωτόκολλο Ελέγχου Διαδικτύου (ICMP), το Πρωτόκολλο Ομαδικών Μηνυμάτων Διαδικτύου (IGMP) και το σύνολο πρωτοκόλλων Ipsec όπως φαίνεται στο παραπάνω σχήμα 3.
Επίπεδο 4 : Το επίπεδο μεταφοράς είναι υπεύθυνο για την επικοινωνία από άκρο σε άκρο μεταξύ των δύο συσκευών και για τον έλεγχο ροής και τον έλεγχο σφαλμάτων. Τα πρωτόκολλα TCP και UDP ανήκουν στο Επίπεδο 4 και επιλέγεται ένα από τα δύο ανάλογα με τον τύπο της εφαρμογής, την ανοχή σε καθυστερήσεις και σφάλματα.
Επίπεδο 5 : Το επίπεδο συνεδρίας είναι υπεύθυνο για το άνοιγμα και το κλείσιμο της επικοινωνίας μεταξύ των δύο συσκευών. Εξασφαλίζει ότι η συνεδρία παραμένει ανοιχτή αρκετά για να μεταφερθούν

όλα τα δεδομένα που ανταλλάσσονται και στη συνέχεια να κλείσει τη συνεδρία άμεσα προκειμένου να αποφευχθεί η σπατάλη πόρων.

Επίπεδο 6 : Το επίπεδο παρουσίασης επιτελεί τη λειτουργία της μετάφρασης μεταξύ διαφορετικών μορφών εφαρμογών. Εδώ πραγματοποιούνται διάφορες εργασίες, όπως η κρυπτογράφηση, η αποσυμπίεση, η συμπίεση, η αποκωδικοποίηση και η κωδικοποίηση.

Επίπεδο 7 : Το επίπεδο εφαρμογής αλληλεπιδρά απευθείας με τα δεδομένα από τον χρήστη. Ποιο συγκεκριμένα παρέχει μια διεπαφή μεταξύ της εφαρμογής και του δικτύου. Περιλαμβάνει αρκετά απ' τα γνωστά πρωτόκολλα όπως HTTP, DNS, SSH και άλλα όπως φαίνεται στο σχήμα 3.

Σημειώνεται ότι πρωτόκολλα των ανώτερων επιπέδων (7,6,5,4) εκτελούνται μόνο στις τερματικές συσκευές, οπότε τα μηνύματα αυτών των επιπέδων αφορούν επικοινωνίας αποστολέα-παραλήπτη ενώ τα πρωτόκολλα των κατώτερων επιπέδων εκτελούνται και στις ενδιάμεσες συσκευές [routers, switch (μόνο επιπέδου 2 ή και 3 αν πρόκειται για L3 switch), συνεπώς τα μηνύματα των επιπέδων αυτών αφορούν επικοινωνία από κόμβο σε κόμβο. [6]

1.4 Μοντέλο TCP/IP

Το μοντέλο Transmission Control Protocol/Internet Protocol Model γνωστό ως TCP/IP σχεδιάστηκε για να ανταποκριθεί στις ανάγκες της επικοινωνίας σε ένα δίκτυο, προσφέροντας μία ελεύθερη από σφάλματα και αποτελεσματική μετάδοση δεδομένων. Το μοντέλο αυτό έχει συνολικά τέσσερα επίπεδα και κάθε επίπεδο εμπεριέχει πρωτόκολλα δικτύου, όπως και στο μοντέλο OSI.

Το TCP/IP δημιουργήθηκε απ΄ το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών στην εποχή του ψυχρού πολέμου. Από τα τέλη της δεκαετίας του '60, το TCP/IP επίσημα εγκρίθηκε από το DARPA και στη συνέχεια επικράτησε ως κοινό πρότυπο δικτύωσης, χρησιμοποιούμενο από κυβερνητικούς οργανισμούς και πανεπιστήμια σε ολόκληρο τον πλανήτη. Το αρχικό όνομα που δόθηκε στο TCP/IP ήταν το ARPANET το 1975 και μετά από λίγα χρόνια το 1983 η ονομασία άλλαξε σε TCP/IP. Επίσης το ίδιο έτος, το μοντέλο αυτό έγινε ένα ανοιχτό πρότυπο που μπορούσε να χρησιμοποιηθεί σε οποιοδήποτε δίκτυο

Το μοντέλο TCP/IP αποτελείται από το επίπεδο πρόσβασης στο δίκτυο, το επίπεδο Internet, το επίπεδο μεταφοράς και το επίπεδο εφαρμογής όπου φαίνεται στο σχήμα 4.

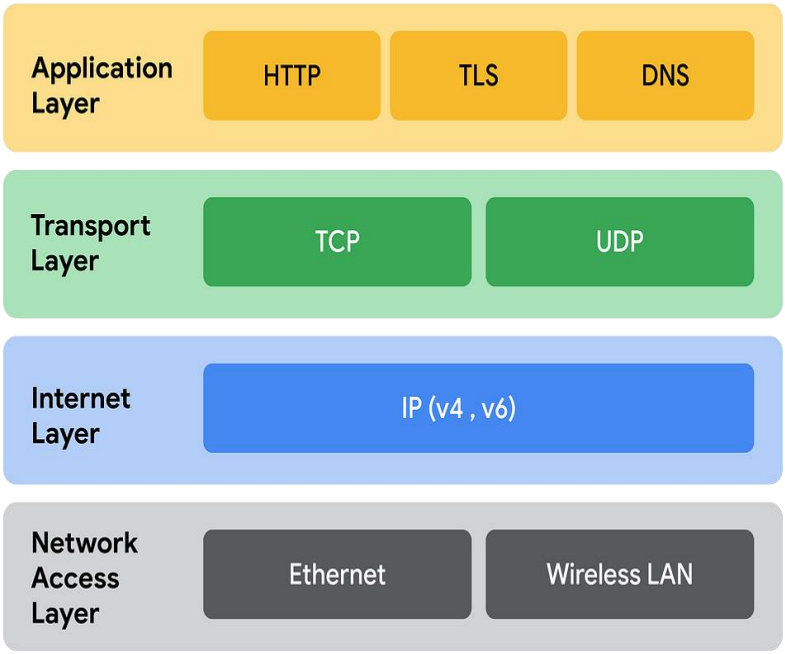
Επίπεδο 1 : Το Επίπεδο Διασύνδεσης Δικτύου ή επίπεδο πρόσβασης στο δίκτυο βοηθά ν προσδιορισμό των λεπτομερειών σχετικά με το πώς πρέπει να μεταδοθούν τα δεδομένα μέσω του δικτύου και ενσωματώνει τις λειτουργίες φυσικού επιπέδου και επιπέδου ζεύξης δεδομένων του OSI. Σε πρόσφατες εκδόσεις του μοντέλου TCP/IP του επίπεδο αυτό χωρίζεται σε δύο υποεπίπεδα για να ξεχωρίζουν οι λειτουργίες φυσικού επιπέδου και Data Link Layer.

Επίπεδο 2 : Στο επίπεδο δικτύου η βασική λειτουργία είναι η μεταφορά πακέτων από οποιοδήποτε δίκτυο και οποιοδήποτε υπολογιστή προς τον προορισμό τους, ανεξαρτήτως της διαδρομής που ακολουθούν. Η παράδοση πακέτων στο επίπεδο δικτύου δεν παρέχει καμία εγγύηση για αξιοπιστία από το πρωτόκολλο του επιπέδου δικτύου. Τα πρωτόκολλα του επιπέδου δικτύου περιλαμβάνουν διευθύνσεις IPV4 και IPV6. Οι λειτουργίες του Internet Layer του μοντέλου TCP/IP ταυτίζονται με το Network Layer του OSI.

Επίπεδο 3 : Το επίπεδο μεταφοράς είναι υπεύθυνο για την παράδοση τμημάτων απ΄τον αποστολέα στον παραλήπτη και για το διαχωρισμό των τμημάτων ανάμεσα στις διάφορες εφαρμογές στην ίδια συσκευή. Επίσης εκτελεί έλεγχο ροής και διαχειρίζεται το πόσα και με ποιο ρυθμό δεδομένα πρέπει να σταλούν. Αυτό το επίπεδο λαμβάνει μηνύματα από το επίπεδο εφαρμογής και επιβεβαιώνει ότι τα δεδομένα

παραδίδονται ακέραια και με τη σειρά που πρέπει. Επιπλέον, το επίπεδο μεταφοράς βοηθάει στον έλεγχο της αξιοπιστίας μιας σύνδεσης μέσω του ρυθμού ροής, του ελέγχου σφαλμάτων και της διακοπής ή αναδιάταξης δεδομένων. Επιπλέον, παρέχει αναγνώριση για την επιτυχή μετάδοση δεδομένων και στέλνει τα επόμενα δεδομένα σε περίπτωση που δεν υπάρχουν σφάλματα. Όπως φαίνεται και στο παρακάτω σχήμα 4, σε αυτό το επίπεδο χρησιμοποιούνται τα πρωτόκολλα TCP και UTP.

Επίπεδο 4 : Το επίπεδο εφαρμογής διασφαλίζει μια άριστη σύνδεση ανάμεσα στην εφαρμογή και τον χρήστη για την ανταλλαγή δεδομένων, ενώ παρέχει επίσης διάφορες λειτουργίες, όπως απομακρυσμένη διαχείριση συστημάτων και υπηρεσίες ηλεκτρονικού ταχυδρομείου. Ορισμένα πρωτόκολλα σε αυτό το επίπεδο είναι το HTTP, TSL και DNS όπως φαίνεται στο σχήμα 4 αλλά και άλλα όπως το FTP και SMTP. Ενσωματώνει τις λειτουργείες των επιπέδων 5,6,7 του μοντέλου OSI. [7]



Σχήμα 1-4: Layers of the TCP/IP model[8]

1.5 Οργανισμοί Τυποποίησης

Τα πρότυπα και οι οργανισμοί τυποποίησης στα ασύρματα δίκτυα επικοινωνιών είναι κρίσιμα για την εξασφάλιση της συμβατότητας, της ασφάλειας και της αποδοτικότητας των συσκευών και των υπηρεσιών. Επιπλέον, τα πρότυπα διασφαλίζουν την ασφάλεια των δεδομένων και την προστασία της ιδιωτικότητας, ενώ ταυτόχρονα προάγουν την καινοτομία και τον ανταγωνισμό στην αγορά, παρέχοντας μια σταθερή βάση για την ανάπτυξη νέων προϊόντων και υπηρεσιών.

1.5.1 Wi-Fi Alliance

Το 1999 μια παγκόσμια μη κερδοσκοπική ομάδα δημιουργήθηκε με στόχο τη βελτίωση της εμπειρίας του χρήστη. Το 2000 η ομάδα αυτή ονομάστηκε επίσημα Wi-Fi Alliance. Η από κοινού επιδίωξή των μελών της ομάδας αυτής να ενώσει την ανθρωπότητα με την τεχνολογία, παγκοσμίως και χωρίς εξαίρεση, συνεχίζεται μέχρι και σήμερα. Εκατοντάδες επιχειρήσεις-μέλη της Ομοσπονδίας Wi-Fi ανά τον κόσμο, εκπροσωπώντας δεκάδες χώρες, ενεργούν εντός του οργανισμού. Προωθώντας νέες

τεχνολογίες και εφαρμογές για την αξιοποίηση του Wi-Fi, πιστοποιώντας πολλές χιλιάδες προϊόντα κάθε έτος.[9]

1.5.2 Bluetooth SIG

Η τεχνολογία Bluetooth ανοίγει το δρόμο για την ανταλλαγή πληροφοριών μεταξύ ασύρματων συσκευών, όπως φορητών υπολογιστών, εκτυπωτών και ψηφιακών καμερών, μέσω ενός ασφαλούς και οικονομικού καναλιού ραδιοσυχνοτήτων. Αρχικά αναπτυγμένη από την Ericsson, η τεχνολογία αυτή έχει επικρατήσει σε πολλά προϊόντα, καθιστώντας την πλέον διαδεδομένη σε χρήση τεχνολογία ασύρματης επικοινωνίας. Οι κατασκευαστές πρέπει να είναι μέλη του Bluetooth SIG για να έχουν πρόσβαση στις προδιαγραφές του Bluetooth. Το Bluetooth SIG είναι υπεύθυνο για τη διαχείριση των εμπορικών σημάτων Bluetooth και του προγράμματος πιστοποίησης Bluetooth SIG. Οι κύριες εργασίες της είναι η δημοσίευση προδιαγραφών Bluetooth και η προώθηση της τεχνολογίας Bluetooth . Το Bluetooth SIG ιδρύθηκε το 1998 και λειτουργούσε με προσωπικό από τις εταιρείες μελών του έως το 2002 όπου και προσλήφθηκε επαγγελματικό προσωπικό. [10]

1.5.3 Wireless Broadband Alliance

Το Wireless Broadband Alliance (WBA) ιδρύθηκε το 2003 με σκοπό να αντιμετωπίσει τόσο τεχνικά όσο και επιχειρησιακά θέματα. Οι δραστηριότητές του καλύπτουν ένα ευρύ φάσμα, από την ανάπτυξη προτύπων και οδηγιών βιομηχανίας έως δοκιμές και πιστοποίησες. Κύρια προγράμματα του είναι το Next Gen Wi-Fi, το OpenRoaming, το 5G και το IoT.[11]

1.5.4 Institute of Electrical and Electronics Engineers (IEEE)

Η IEEE, ένας οργανισμός αφοσιωμένος στην προώθηση της καινοτομίας και της τεχνολογίας προς όφελος της ανθρωπότητας, αποτελεί τη μεγαλύτερη επαγγελματική κοινότητα στον κόσμο στον τεχνικό τομέα. Στόχος της είναι να υποστηρίξει επαγγελματίες που δραστηριοποιούνται σε κάθε πτυχή των ηλεκτρικών, ηλεκτρονικών και υπολογιστικών επιστημών και σε σχετικούς τομείς που αποτελούν τη βάση του σύγχρονου πολιτισμού. Η ιστορία της IEEE ξεκινά από το 1884, όταν η χρήση της ηλεκτρικότητας άρχισε να επηρεάζει σημαντικά την κοινωνία. Εκείνη την εποχή, η ηλεκτρική βιομηχανία ήταν σε ανοδική πορεία, με τον τηλέγραφο να είναι ήδη ένας σημαντικός τρόπος επικοινωνίας που ενώνει τον κόσμο. Οι βιομηχανίες του τηλεφώνου και της ηλεκτρικής ενέργειας και φωτισμού μόλις ξεκινούσαν να αναπτύσσονται, υποδεικνύοντας τον δρόμο για τις μεγάλες τεχνολογικές αλλαγές που θα ακολουθούσαν.[12]

1.5.5 Telecommunications Industry Association (TIA)

Η TIA αναπτύσσει πρότυπα για προϊόντα τεχνολογίας πληροφορικής και τηλεπικοινωνιών σε συνεργασία με πολλές εταιρείες. Διαθέτει δώδεκα επιτροπές που επικεντρώνονται σε διάφορους τομείς, όπως η ασύρματη επικοινωνία και η δομημένη καλωδίωση. Συνεργάζεται με διεθνείς οργανισμούς για την παγκόσμια ενσωμάτωση των προτύπων. Το 2017, ενώθηκε με το Quest Forum, επεκτείνοντας την επιρροή της και συγχωνεύοντας τα διοικητικά συμβούλια. Η έδρα της βρίσκεται στο Arlington, Virginia.[13]

1.5.6 Διεθνής Οργανισμός Τυποποίησης (ISO)

Ο Διεθνής Οργανισμός Τυποποίησης ISO είναι δίκτυο Εθνικών Φορέων Τυποποίησης που επί του παρόντος περιλαμβάνει 147 μέλη, ένα από κάθε χώρα.Η Κεντρική του Γραμματεία εδρεύει στη Γενεύη.

Ο στόχος του ISO είναι να προωθήσει την ανάπτυξη της Τυποποίησης και των σχετικών με αυτή δραστηριοτήτων στον κόσμο, έτσι ώστε να διευκολύνεται η διεθνής ανταλλαγή αγαθών και υπηρεσιών καθώς επίσης και η ανάπτυξη συνεργασίας σε δραστηριότητες πνευματικού, επιστημονικού, τεχνολογικού και οικονομικού ενδιαφέροντος.
Ο ISO ενώνει τα συμφέροντα των παραγωγών, των χρηστών (συμπεριλαμβανομένων των καταναλωτών), των κυβερνήσεων και της Επιστημονικής Κοινότητας κατά την προετοιμασία των Διεθνών Προτύπων. Οι δραστηριότητες του Οργανισμού πραγματοποιούνται σε περιφερειακό επίπεδο από τις Τεχνικές Επιτροπές και τις Υποεπιτροπές, οι οποίες οργανώνονται και υποστηρίζονται από Τεχνικές Γραμματείες που ανατίθενται στις χώρες μέλη. Τα αποτελέσματα του Τεχνικού Έργου του ISO εκδίδονται υπό την μορφή των Διεθνών Προτύπων (International Standards ISO).[14]

1.5.7 Consultative Committee for International Telephony and Telegraphy (CCITT)

Η CCITT είναι μέρος της ITU (Διεθνής Ένωση Τηλεπικοινωνιών), η οποία ιδρύθηκε το 1865 για την τυποποίηση των τηλεγραφικών δικτύων. Με την πάροδο του χρόνου, η ITU επέκτεινε τις δραστηριότητές της για να συμπεριλάβει τη ρύθμιση της τηλεφωνίας, των ασύρματων ραδιοεπικοινωνιών και της ραδιοφωνίας. Το 1934, η ITU μετονομάστηκε για να αντικατοπτρίζει τον ευρύτερο ρόλο της σε όλες τις μορφές επικοινωνίας. Μετά τον Β' Παγκόσμιο Πόλεμο, η ITU έγινε ειδικός οργανισμός του ΟΗΕ και καθιέρωσε τον Πίνακα Κατανομής Συχνοτήτων για να αποφεύγονται οι παρεμβολές μεταξύ διαφόρων ραδιοϋπηρεσιών. Το 1956, οι επιτροπές CCIF και CCIT συγχωνεύθηκαν για να δημιουργήσουν την CCITT, με σκοπό τη βελτίωση της διαχείρισης των τηλεφωνικών και τηλεγραφικών επικοινωνιών. Το 1993, η ITU αναδιοργανώθηκε και η CCITT ενσωματώθηκε στον νέο Τομέα Τυποποίησης Τηλεπικοινωνιών (ITU-T). Παρόλο που η ITU-T είναι υπεύθυνη για τις συστάσεις και τα πρότυπα, οι συστάσεις της CCITT εξακολουθούν να αναφέρονται και πλέον διαχειρίζονται από την ITU. [15]

Κεφάλαιο 2: Θεμελιώδεις Αρχές Ασύρματων Δικτύων

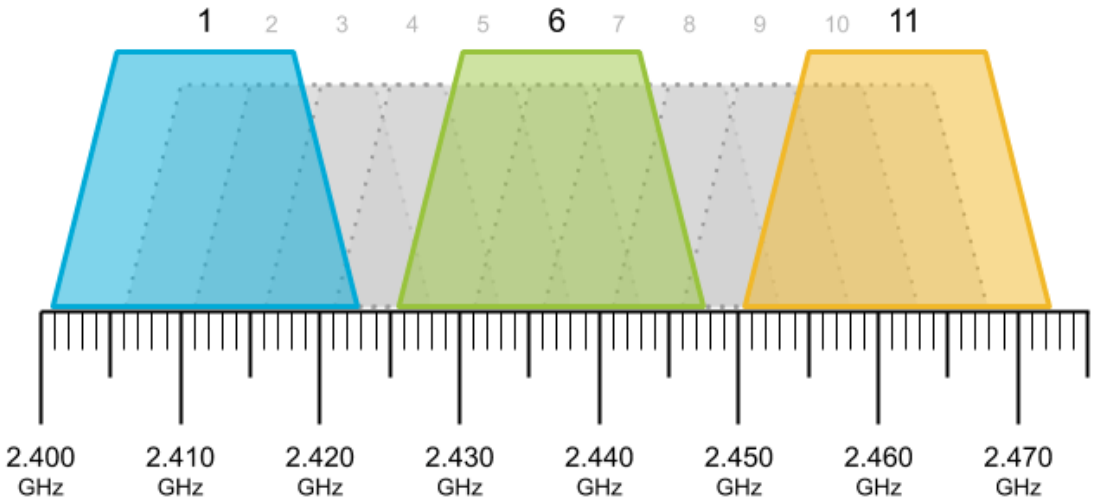
2.1 Συχνότητα Ραδιοκυμάτων

Ένα απ' τα πράγματα που θα μπορούσαμε να αναρωτηθούμε είναι πως τα ασύρματα δίκτυα μεταφέρουν δεδομένα από το σημείο Α στο Β. Το κυριότερο μέσο για την επίτευξη του σκοπού αυτού, είναι τα ραδιοκύματα. Ο Heinrich Hertz ήταν ο πρώτος που ανακάλυψε τις ραδιοκυματικές εκπομπές τον 18ο αιώνα, παρόλα αυτά, ο Hertz ποτέ δεν αντιλήφθηκε πλήρως τη βαρύτητα των ανακαλύψεων του. Το 1894, ωστόσο, ο Marconi ανέπτυξε πρακτικές εφαρμογές για τη μετάδοση μηνυμάτων μέσω ραδιοκυμάτων. Η ανακάλυψή των ραδιοκυμάτων άνοιξε το δρόμο για την ανάπτυξη των ασύρματων τηλεπικοινωνιών. Η χρήση τους είναι καθημερινή στον τομέα των ασύρματων δικτύων, όπως για παράδειγμα το Wi-fi. Συσκευές όπως ασύρματοι δρομολογητές εκπέμπουν ραδιοκύματα για να μπορέσουν να επικοινωνήσουν με υπολογιστές, τηλέφωνα και άλλες συσκευές που το υποστηρίζουν. Τα ραδιοκύματα είναι ηλεκτρομαγνητικά κύματα που χρησιμοποιούμε ώστε να μεταφέρουμε δεδομένα ασύρματα.[16] Η ραδιοσυχνότητα (Radio Frequency - RF) ορίζεται ως ο ρυθμός ταλάντωσης ενός εναλλασσόμενου ηλεκτρομαγνητικού πεδίου στην περιοχή συχνοτήτων από περίπου 3 kHz έως 300 GHz. Αυτό είναι περίπου μεταξύ του ανώτερου ορίου των ακουστικών συχνοτήτων και του κατώτερου ορίου των υπέρυθρων συχνοτήτων.Όταν κύμα συχνότητας f, μήκους κύματος λ, μεταδίδεται στο κενό, προκύπτει ότι ταξιδεύει με την ταχύτητα του φωτός c=3*10^8m/s. Η σχέση που συνδέει τα μεγέθη είναι η εξής: c=λ * f. Η επιλογή της κατάλληλης συχνότητας εξαρτάται από πολλούς παράγοντες, όπως η απόδοση, η εμβέλεια, η αντοχή στις παρεμβολές και η συμβατότητα με άλλες συσκευές. Οι συχνότητες που συναντώνται συχνότερα στα ασύρματα τοπικά δίκτυα είναι τα 2,4 GHz και τα 5 GHz, για το Wi-Fi, το Bluetooth και άλλες ασύρματες τεχνολογίες. Το πρότυπο 802.11a χρησιμοποιεί ραδιοσυχνότητες μεταξύ 5.15 GHz έως 5.875 GHz και τα πρότυπα 802.11b και 802.11g μεταξύ 2.4 GHz έως 2.495 GHz. Οι συχνότητες αυτές εμφανίζουν κάποια συγκριτικά πλεονεκτήματα και μειονεκτήματα. Για παράδειγμα, τα 2,4 GHz χρησιμοποιούνται κατά προτίμηση σε μεγαλύτερες αποστάσεις αλλά συχνά σε αυτή τη συχνότητα συμβαίνουν παρεμβολές διότι τη χρησιμοποιούν πολλές συσκευές. Σε αντίθεση, τα 5 GHz προσφέρουν μεγαλύτερες ταχύτητες, δίχως παρεμβολές, αλλά σε μικρότερη εμβέλεια λόγω μεγαλύτερων εξασθενίσεων.[17]

2.2 Ασύρματα Ραδιοκανάλια

Τα ασύρματα ραδιοκανάλια αποτελούν το μέσο δια των οποίων πραγματοποιείται η ασύρματη επικοινωνία, χρησιμοποιώντας σήματα ραδιοσυχνοτήτων RF για τη μετάδοση δεδομένων ανάμεσα σε συσκευές. Το εύρος ζώνης του καναλιού (Bandwidth) είναι η περιοχή συχνοτήτων που καταλαμβάνει ένα διαμορφωμένο σήμα. Στις ασύρματες τηλεπικοινωνίες τα κανάλια καταλαμβάνουν εύρη καναλιών όπως 20 MHz, 40 MHz, 80 MHz ή 160 MHz, για τα ασύρματα τοπικά δίκτυα και 30 KHz (2G) ως 1 GHz (5G) για τα δίκτυα κινητής τηλεφωνίας. Οι κυβερνητικοί οργανισμοί κατανέμουν το φάσμα RF σε ραδιοκανάλια και οι κατάλληλοι ρυθμιστικοί φορείς καθορίζουν τις τιμές της μέγιστης επιτρεπόμενης ισχύος. Το εύρος ζώνης του καναλιού είναι ανάλογο του μέγιστου ρυθμού μετάδοσης (bit rate) που μπορεί να επιτευχθεί στο συγκεκριμένο κανάλι. Η ποιότητα των ασύρματων ραδιοκαναλιών μπορεί να επηρεαστεί από διάφορους παράγοντες, όπως η απόσταση μεταξύ του πομπού και του δέκτη, η παρεμβολή από άλλες συσκευές, η φυσική διάταξη του περιβάλλοντος και η παρουσία εμποδίων όπως τοίχοι και κτίρια. Η ταχύτητα μετάδοσης των δεδομένων, η σταθερή λειτουργία του δικτύου και η συνολική απόδοσή του επηρεάζεται από την ποιότητα των ραδιοκαναλιών εντός των οποίων λειτουργούν [18]. Τα μη επικαλυπτόμενα κανάλια (σχήμα 1) αναφέρονται στα ασύρματα δίκτυα, όταν ορισμένα κανάλια χρησιμοποιούν διαφορετικές συχνότητες, οι οποίες είναι μη επικαλυπτόμενες μεταξύ τους ώστε να μην προκαλούνται παρεμβολές στην επικοινωνία. Στα ασύρματα δίκτυα Wi-Fi, τα μη επικαλυπτόμενα κανάλια είναι σημαντικά για τη μείωση των παρεμβολών και τη βελτίωση της απόδοσης του δικτύου. Συγκεκριμένα, στο εύρος συχνοτήτων 2,4 GHz που συχνά χρησιμοποιούνται απ' τις περισσότερες IoT συσκευες, υπάρχουν τρία μη επικαλυπτόμενα κανάλια που μπορούν να χρησιμοποιηθούν χωρίς παρεμβολές. Αυτά τα κανάλια είναι τα 1, 6 και 11. Αυτό συμβαίνει διότι η ζώνη

συχνοτήτων των 2,4 GHz που χρησιμοποιείται σε ασύρματα δίκτυα WiFi είναι περιορισμένη σε 100 MHz εύρος. Κάθε κανάλι σε αυτή τη ζώνη είναι πλάτους 20 MHz και οι κεντρικές συχνότητες των καναλιών διαχωρίζονται με απόσταση 5 MHz. Αυτό σημαίνει ότι τα 11 διαθέσιμα κανάλια πρέπει να χωρέσουν σε αυτό το φάσμα, με αποτέλεσμα να επικαλύπτονται μεταξύ τους. Ωστόσο, τα κανάλια 1, 6 και 11 βρίσκονται αρκετά μακριά ο ένας από τον άλλο στη ζώνη 2,4 GHz, επιτρέποντας τη χρήση τους χωρίς να προκαλούνται παρεμβολές μεταξύ τους. [19]



Σχήμα 2-1: Μη επικαλυπτόμενα κανάλια [19]

2.3 Σήμα

Το σήμα σε ένα ασύρματο δίκτυο είναι η ηλεκτρομαγνητική ενέργεια που μεταφέρει πληροφορία από έναν πομπό σε έναν δέκτη. Μέσω του σήματος μπορεί να μεταδίδονται δεδομένα, φωνή, εικόνα, κείμενο ή άλλη μορφή πληροφορίας. Ο δέκτης λαμβάνει την πληροφορία από τις ιδιότητες του ηλεκτρομαγνητικού κύματος που λαμβάνει Η ποιότητα του σήματος αναφέρεται στην ικανότητά του να μεταδώσει τα δεδομένα δίχως παρεμβολές, απώλειες ή παραμορφώσεις. Επομένως είναι η πλέον κρίσιμη παράμετρος για τη σταθερότητα και την ταχύτητα της ασύρματης σύνδεσης. Επηρεάζεται από πλήθος παραγόντων όπως η ισχύς του, η συχνότητα του, η ευαισθησία του δέκτη, η αναλογία σήματος προς θόρυβο (Signal to Noise Ratio - SNR) και η καθυστέρηση (Latency), την απόσταση μεταξύ πομπού και δέκτη, των φυσικών εμποδίων και των παρεμβολών από άλλες συσκευές που λειτουργούν σε κοντινές συχνότητες [20]. Η ισχύς του σήματος αναφέρεται στην ποσότητα της ηλεκτρομαγνητικής ενέργειας που μεταφέρεται από τον πομπό στο δέκτη και μετριέται σε Watt ή dB ή dBm ή dBi. Επηρεάζει την απόδοση και την απόσταση της τηλεπικοινωνιακής ζεύξης καθώς και το λόγο SNR. Η αύξηση της ισχύος μπορεί να βελτιώσει την ποιότητα της επικοινωνίας, ενώ η μείωσή της μπορεί να επιφέρει απώλεια του σήματος και παραμόρφωση των δεδομένων.[21]

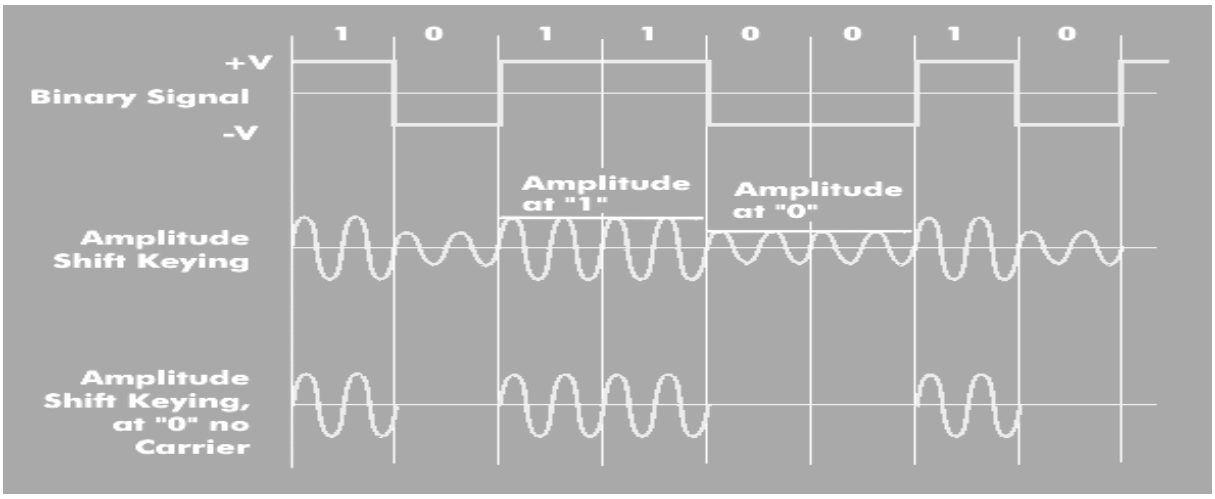
2.4 Διαμόρφωση Σήματος

Η διαμόρφωση σήματος αποτελεί μια τεχνική επεξεργασίας σήματος κατά την οποία τα δεδομένα που θέλουμε να μεταφέρουμε μετατρέπονται σε μια μορφή που μπορεί να μεταδοθεί μέσω ενός μέσου, όπως είναι ο αέρας για τις ασύρματες επικοινωνίες που εξετάζουμε. Η διαδικασία της διαμόρφωσης συνήθως περιλαμβάνει τη μετατροπή αυτών των δεδομένων σε ένα σήμα που μπορεί να μεταδοθεί μέσω του επιλεγμένου μέσου επικοινωνίας. Στα ασύρματα δίκτυα, η διαμόρφωση σήματος περιλαμβάνει την αντιστοίχιση των ψηφιακών δεδομένων σε αναλογικά σήματα που μπορούν να μεταδοθούν μέσω των ραδιοκυμάτων. Οι τεχνικές διαμόρφωσης του σήματος, ιδιαίτερα στις ασύρματες επικοινωνίες που το

ασύρματο μέσο υπόκειται σε μεγαλύτερες απώλειες και θόρυβο, είναι καθοριστικές για την αποτελεσματική μετάδοση και λήψη δεδομένων στα ασύρματα δίκτυα. Η επιλογή της κατάλληλης διαμόρφωσης εξαρτάται από τις απαιτήσεις της εφαρμογής, τις συνθήκες του ραδιοκαναλιού και τους περιορισμούς του συστήματος.[22]

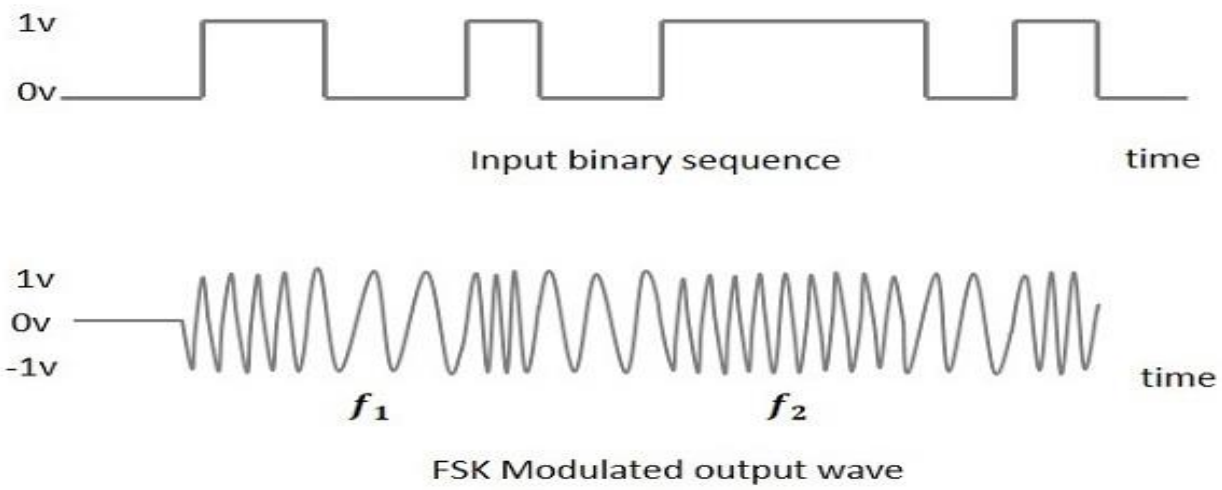
2.5 Τεχνικές Ψηφιακής Διαμόρφωσης Σήματος

Η Διαμόρφωση Μετατόπισης Πλάτους (Amplitude Shift Keying - ASK) είναι μια τεχνική ψηφιακής διαμόρφωσης που χρησιμοποιείται στις ασύρματες επικοινωνίες. Κατά τη μέθοδο αυτή, η πληροφορία κωδικοποιείται μέσω της αλλαγής του πλάτους του φέροντος σήματος. Όταν η τιμή του ψηφιακού σήματος είναι 1, το πλάτος του φορέα αυξάνεται σε ένα υψηλότερο επίπεδο, ενώ όταν η τιμή είναι 0, το πλάτος του φορέα πέφτει σε ένα χαμηλότερο επίπεδο, όπως φαίνεται στο σχήμα 2. Στην ουσία, οι αλλαγές στο πλάτος αντιπροσωπεύουν την ψηφιακή πληροφορία που μεταδίδεται. Το ASK χρησιμοποιείται σε πολλές εφαρμογές, όπως στις ασύρματες μεταφορές δεδομένων και τις ασύρματες επικοινωνίες μεταξύ συσκευών. Ένα από τα κύρια πλεονεκτήματα του ASK είναι η απλότητά στην υλοποίηση και το μικρό οικονομικό κόστος. Ωστόσο, ένα από τα μειονεκτήματά της είναι ότι είναι ευαίσθητο στο θόρυβο και σε παρεμβολές, καθώς ο θόρυβος μπορεί να προκαλέσει σφάλματα στην αναγνώριση των σημάτων.[23]



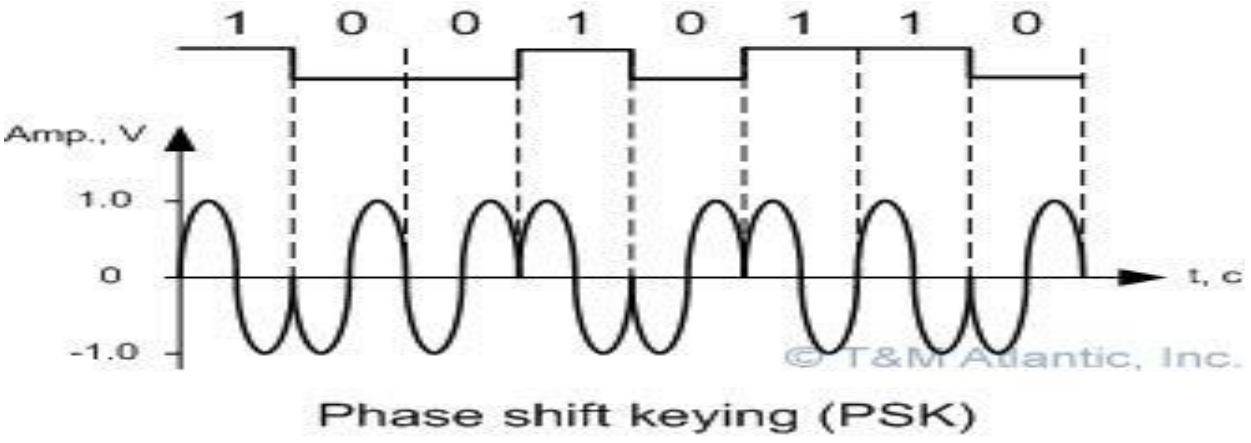
Σχήμα 2-2: Amplitude Shift Keying [24]

Η Διαμόρφωση Μετατόπισης Συχνότητας (Frequency Shift Keying - FSK) είναι μια τεχνική ψηφιακής διαμόρφωσης που χρησιμοποιείται στις ασύρματες επικοινωνίες. Κατά τη διαμόρφωση FSK, η πληροφορία κωδικοποιείται μέσω της αλλαγής της συχνότητας του φέροντος σήματος. Κατά τη μετάδοση, ένας φορέας σήματος μετατοπίζεται σε δύο ή περισσότερες διαφορετικές συχνότητες, ανάλογα με τις τιμές των ψηφιακών δεδομένων που πρέπει να μεταδοθούν. Η πιο συχνά χρησιμοποιούμενη παραλλαγή της είναι η Binary Frequency Shift Keying (BFSK), κατά την οποία μία συχνότητα αντιστοιχεί στη δυαδική τιμή 1, ενώ μία άλλη συχνότητα αντιστοιχεί στην τιμή 0 (σχήμα 3). Χρησιμοποιείται συχνά λόγω της απλότητας υλοποίησης και της ανθεκτικότητάς της στο θόρυβο. Μια άλλη παραλλαγή της είναι η Multiple Frequency Shift Keying (MFSK), κατά την οποία χρησιμοποιούνται περισσότερες από δύο συχνότητες φέροντος κύματος, οι οποίες αντιστοιχούν διαφορετικό σύμβολο η κάθε μία (σειρά bits). Έτσι η MFSK προσφέρει μεγάλο βαθμό αξιοποίησης του φάσματος και καθίσταται κατάλληλη για απαιτητικές σε ταχύτητα μετάδοσης δεδομένων εφαρμογές.[25]



Σχήμα 2-3: Binary Frequency Shift Keying[26]

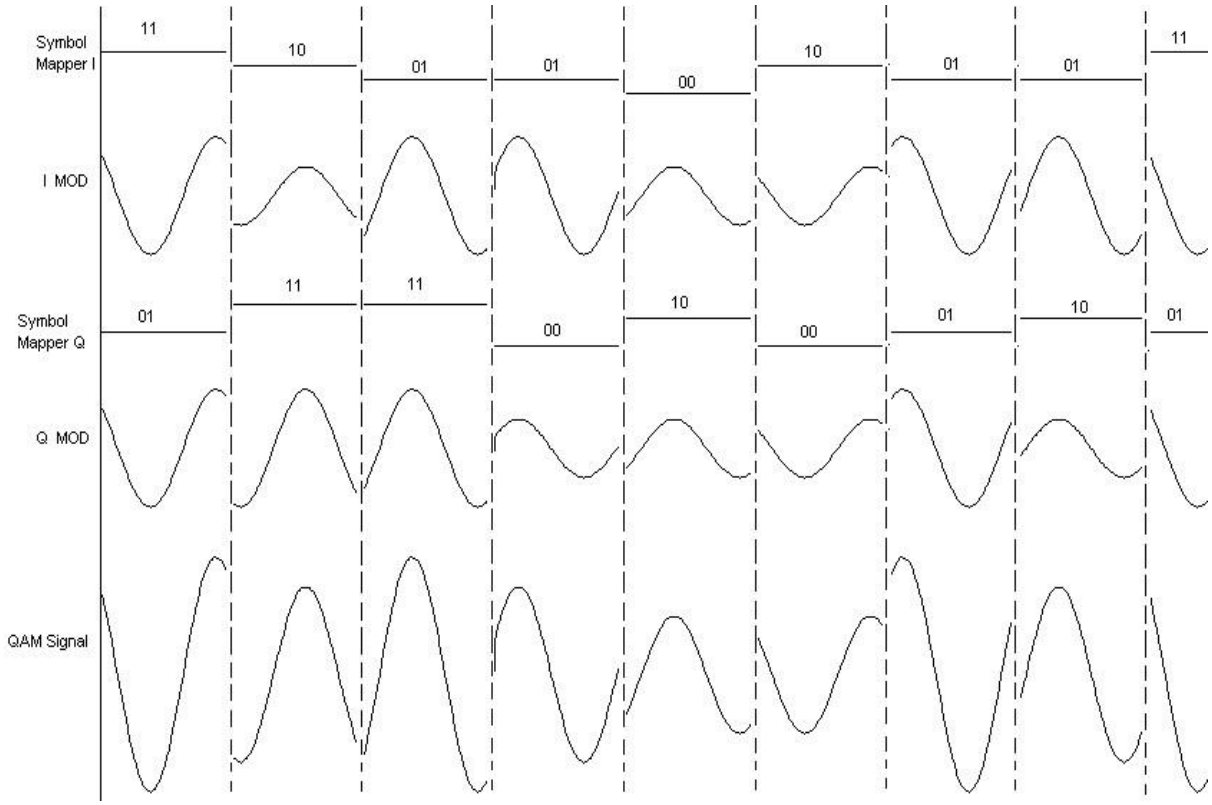
Η Διαμόρφωση Μετατόπισης Φάσης (Phase Shift Keying - PSK) αποτελεί μία από τις βασικές μεθόδους διαμόρφωσης σήματος στην ασύρματη επικοινωνία. Κατά τη διαμόρφωση PSK, η πληροφορία κωδικοποιείται με την αλλαγή της φάσης του φέροντος σήματος, ενώ η συχνότητα και το πλάτος παραμένουν σταθερά. Στην κλασική μορφή του PSK, γνωστή ως Binary Phase Shift Keying (BPSK) ή Phase Reversal Keying (PRK), το ψηφίο "1" αναπαρίσταται με μία φάση του φορέα, ενώ το ψηφίο "0" αναπαρίσταται με την αντίθετη φάση, όπως απεικονίζεται στο παράδειγμα του σχήματος 4. Κατά τη χρήση της παραλλαγής Quadrature Phase Shift Keying (QPSK), τέσσερις διαφορετικές φάσεις χρησιμοποιούνται για την αναπαράσταση των bits ανά δύο. Αυτό επιτρέπει τη μετάδοση διπλάσιας ποσότητας πληροφορίας σε σχέση με τη BPSK, στο ίδιο εύρος ζώνης. Η τεχνική M Phase Shift Keying (M-PSK) επεκτείνει ακόμα περισσότερο την PSK για να χρησιμοποιηθεί M αριθμός φάσεων. Με τη χρήση των τεχνικών διαμόρφωσης PSK, μπορούμε να μεταδώσουμε αξιόπιστα ψηφιακά δεδομένα με ελάχιστα σφάλματα και υψηλή απόδοση, καθιστώντας την μία από τις πιο βασικές μεθόδους διαμόρφωσης σήματος στην ασύρματη επικοινωνία.[27][28]



Σχήμα 2-4: Phase Shift Keying[29]

Η Διαμόρφωση Ορθογώνιου πλάτους (Quadrature Amplitude Modulation - QAM) είναι μια ακόμα τεχνική ψηφιακής διαμόρφωσης σήματος. Κατά την ψηφιακή διαμόρφωση QAM, τα δεδομένα

ψηφιοποιούνται και μεταδίδονται μέσω αλλαγών στο πλάτος δύο φερόντων σημάτων (I MOD, Q MOD), τα οποία έχουν την ίδια συχνότητα και έχουν διαφορά φάσης 90 μοίρες με τη μέθοδο ASK ή AM. (σχήμα 5). Το πλήθος των συνδυασμών πλάτους και φάσης που μπορούν να χρησιμοποιηθούν στην QAM καθορίζει τον αριθμό των bits που μπορούν να μεταδοθούν ανά σύμβολο. Έτσι προκύπτουν οι παραλλαγές QAM-2^n (QAM-4, QAM-8, QAM-16, QAM-32 κ.ο.κ.) στις οποίες ο αριθμός αντιστοιχεί στο πλήθος των διαφορετικών συνδυασμών πλάτους και φάσης. Επιτρέπει τη μετάδοση πολλαπλών bits ανά σύμβολο, καθιστώντας την αποδοτική για εφαρμογές που απαιτούν υψηλές ταχύτητες μετάδοσης δεδομένων, όπως τα σύγχρονα πρότυπα Wi-Fi, για τη μετάδοση ψηφιακών δεδομένων με υψηλές ταχύτητες. Επιπλέον παρουσιάζει ανοχή στο θόρυβο και χαμηλή πιθανότητα σφαλμάτων. Ωστόσο, παρουσιάζει και μειονεκτήματα, όπως η αυξημένη πολυπλοκότητα και επομένως το κόστος του δέκτη και η απαίτηση για σύγχρονη αποκωδικοποίηση με το ίδιο πλάτος και συχνότητα.[30]

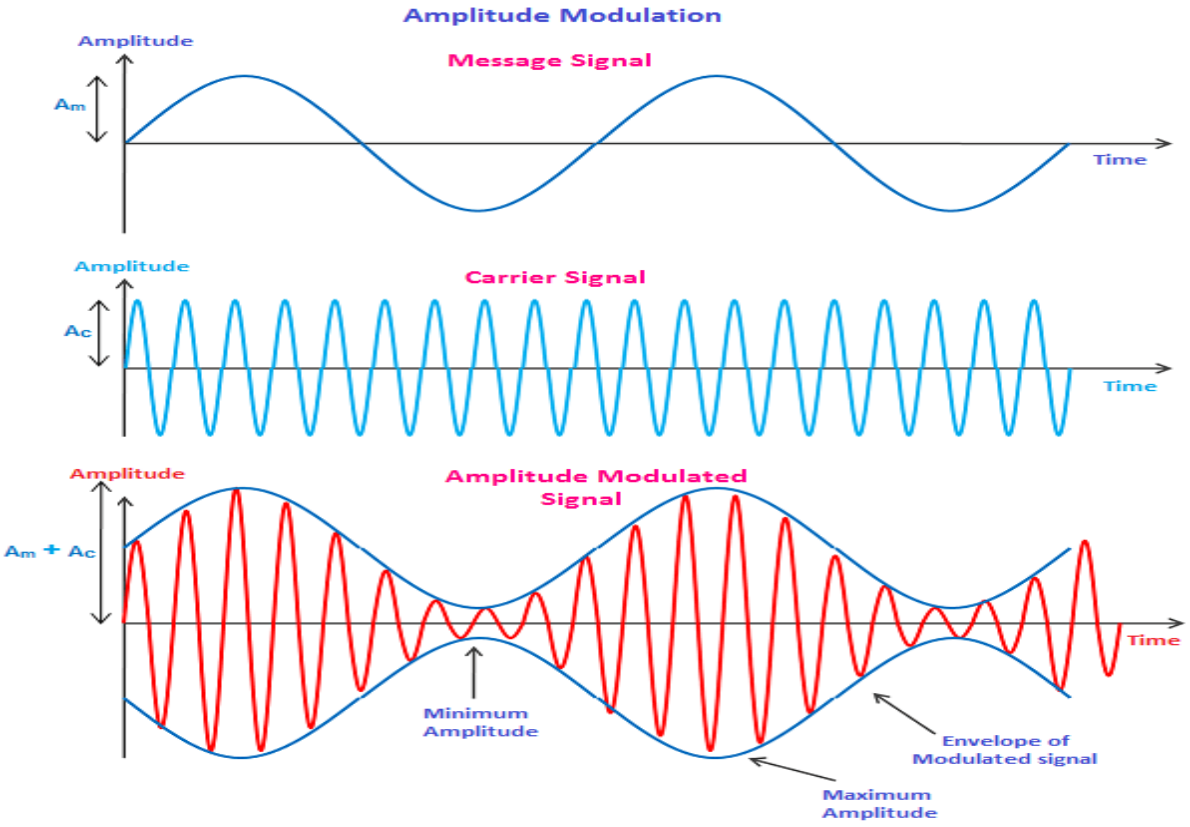


Σχήμα 2-5: Quadrature Amplitude Modulation QAM-4 [31]

2.6 Τεχνικές Αναλογικής Διαμόρφωσης Σήματος

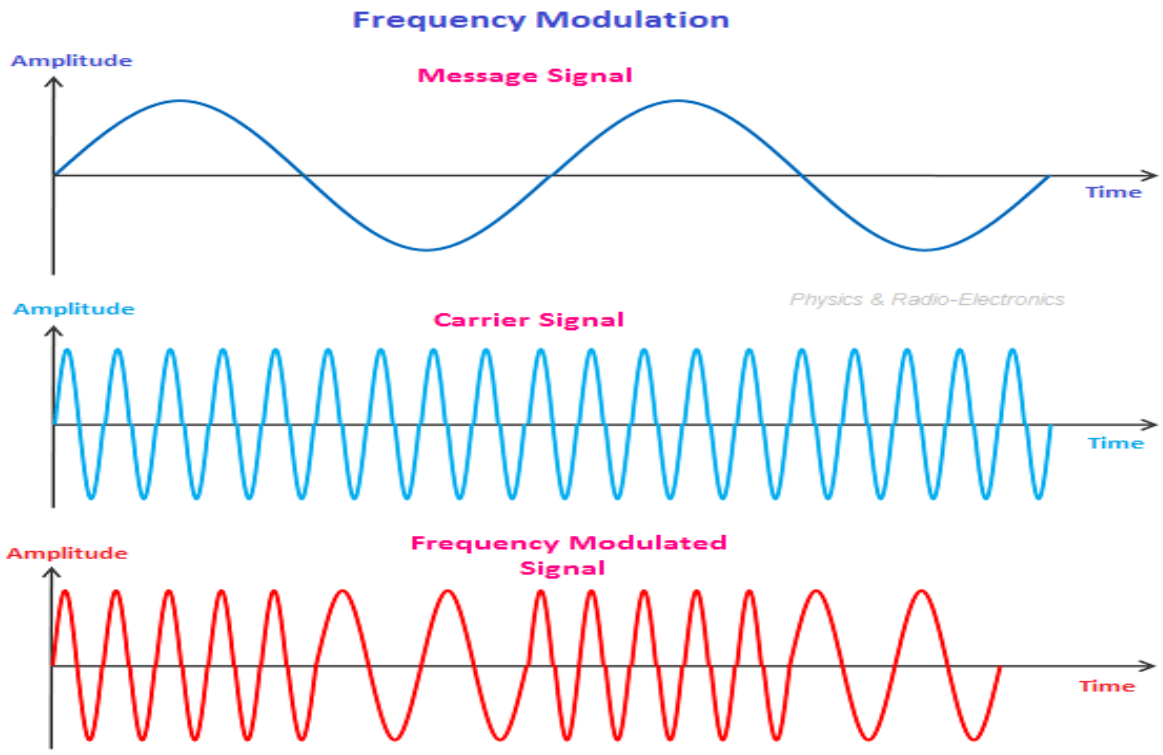
Οι τεχνικές αναλογικής διαμόρφωσης χρησιμοποιούνται για την ασύρματη μετάδοση αναλογικών δεδομένων (π.χ. ραδιόφωνο, τηλεφωνία). Η Διαμόρφωση Πλάτους (AM - Amplitude Modulation) είναι μια μέθοδος αναλογικής διαμόρφωσης σήματος, κατά την οποία, το πλάτος του φέροντος σήματος αλλάζει ανάλογα με το σήμα πληροφορίας που επιθυμούμε να μεταδώσουμε. Αυτό σημαίνει ότι μεταβάλλεται μόνο το πλάτος του φέροντος του σήματος, ενώ η φάση και η συχνότητα παραμένουν σταθερές. Όταν το πλάτος του σήματος πληροφορίας μειώνεται, μειώνεται και το πλάτος του φέροντος, ενώ το αντίθετο συμβαίνει όταν το πλάτος του σήματος πληροφορίας αυξάνεται, όπως απεικονίζεται στο σχήμα 6. Η διαμόρφωση AM χρησιμοποιήθηκε κυρίως στο παρελθόν ευρέως στις ραδιοφωνικές μεταδόσεις, καθώς παρείχε το πλεονέκτημα της απλότητας στην υλοποίηση. Ωστόσο, παρουσιάζει

ευαισθησία στο θόρυβο σε σύγκριση με άλλες μεθόδους διαμόρφωσης, όπως η διαμόρφωση συχνότητας (FM).[32]



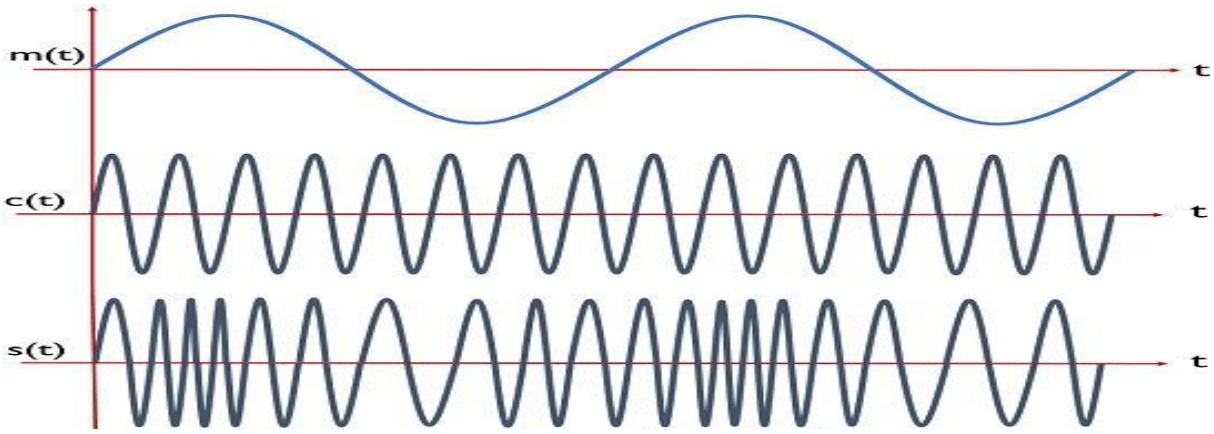
Σχήμα 2-6: Amplitude Modulation [33]

Η Διαμόρφωση Συχνότητας (Frequency Modulation - FM) είναι μια αναλογική τεχνική διαμόρφωσης σήματος, κατά την οποία, η πληροφορία κωδικοποιείται με την αλλαγή της συχνότητας του φέροντος σήματος σύμφωνα με την πληροφορία που πρέπει να μεταδοθεί. Το διαμορφωμένο σήμα που προκύπτει έχει σταθερό πλάτος άλλα μεταβαλλόμενη συχνότητα και παρουσιάζει «πυκνώματα» (αύξηση της συχνότητας του φέροντος) και «αραιώματα» (μείωση της συχνότητας του φέροντος), τα οποία αντιστοιχούν σε μεγάλο και μικρό πλάτος του υπό διαμόρφωση σήματος (σχήμα 7). Η τεχνική FM επιτρέπει τη μετάδοση ηχητικών σημάτων, δεδομένων και άλλων πληροφοριών μέσω ραδιοκυμάτων. Ένα από τα κύρια πλεονεκτήματα της FM είναι η ανθεκτικότητα της στον θόρυβο και η ικανότητά της να μεταδίδει υψηλή ποιότητα ήχου. Συχνά, η διαμόρφωση FM συνοδεύεται από διάφορα πρότυπα και πρωτόκολλα που εξασφαλίζουν την αποτελεσματική μετάδοση και λήψη των σημάτων.[34]



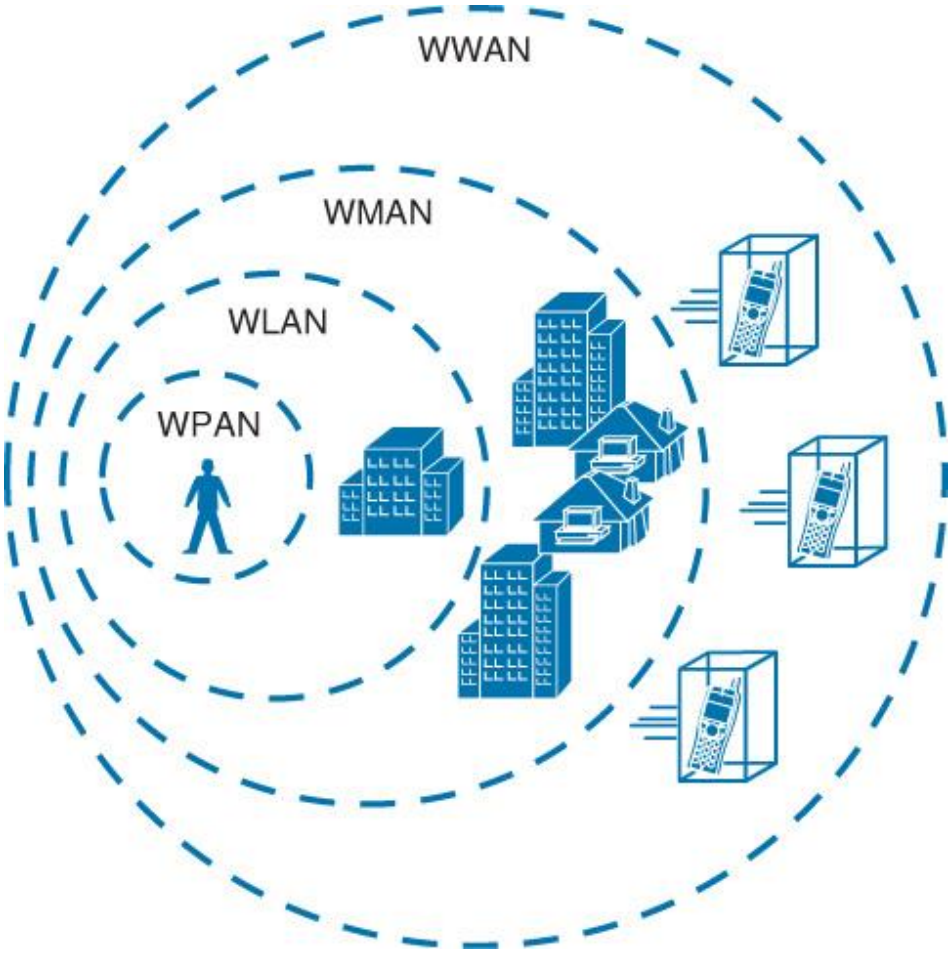
Σχήμα 2-7: Frequemcy Modulation [35]

Η Διαμόρφωση Φάσης (Phase Modulation - PM) είναι μια αναλογική τεχνική διαμόρφωσης σήματος, κατά την οποία η φάση του φέροντος σήματος αλλάζει ανάλογα με την τιμή του σήματος πληροφορίας που επιθυμούμε να μεταδώσουμε. Το μέγιστο πλάτος και η συχνότητα του φέροντος σήματος διατηρούνται σταθερά, αλλά καθώς το πλάτος του σήματος μηνύματος μεταβάλλεται, η φάση του φέροντος μεταβάλλεται αντίστοιχα (σχήμα 8). Χρησιμοποιείται ευρέως στην κινητή τηλεφωνία και στη δορυφορική τηλεόραση. Σε πολλές περιπτώσεις, η PM χρησιμοποιείται σε συνδυασμό με άλλες τεχνικές διαμόρφωσης, όπως η Διαμόρφωση Πλάτους (AM) ή η Διαμόρφωση Συχνότητας (FM), για να επιτύχει συγκεκριμένα χαρακτηριστικά επικοινωνίας ή για να βελτιώσει την απόδοση του συστήματος υπό συγκεκριμένες συνθήκες. Η PM παρουσιάζει ανθεκτικότητα στο θόρυβο σε σύγκριση με την AM, αλλά μπορεί να απαιτεί πιο πολύπλοκη κυκλωματική υλοποίηση. Επίσης, η διαμόρφωση PM μπορεί να παρέχει υψηλότερη ενέργεια εισόδου - εξόδου σε σχέση με τη διαμόρφωση FM.[36]



Σχήμα 2-8: Phase Modulation [35]

2.7 Τύποι Ασύρματων Δικτύων



Σχήμα 2-9: Network Wireless Types [37]

2.7.1 WPAN

Ένα Ασύρματο Προσωπικό Δίκτυο Περιοχής (Wireless Personal Area Network - WPAN) είναι ένας τύπος προσωπικού δικτύου που χρησιμοποιεί ασύρματες τεχνολογίες επικοινωνίας για να συνδέσει συσκευές εντός περιορισμένης εμβέλειας, καλύπτοντας συνήθως μόνο μερικά μέτρα. Επιτρέπει τη συνεχή επικοινωνία και μεταφορά δεδομένων μεταξύ των συνδεδεμένων συσκευών, χωρίς την ανάγκη για σύνδεση μέσω καλωδίου [38]. Η πιο συνηθισμένη συχνότητα που χρησιμοποιεί είναι τα 2.4GHz. Η περιοχή που καλύπτει εξαρτάται από τα χαρακτηριστικά της συσκευής που δημιουργεί το δίκτυο. Ωστόσο, συνήθως περιορίζεται σε μικρούς χώρους όπως μικρά δωμάτια. Τα WPAN δημιουργούνται με τη χρήση πρωτοκόλλων όπως το Bluetooth. Ιστορικά, η πρώτη σημαντική στιγμή στην ιστορία του WPAN ήρθε με την ανάπτυξη του πρωτοκόλλου Bluetooth στα τέλη της δεκαετίας του 1990. Το Bluetooth επέτρεψε για πρώτη φορά την ασύρματη επικοινωνία μεταξύ συσκευών όπως κινητά τηλέφωνα, ακουστικά και υπολογιστές, σε κοντινές αποστάσεις. Στη συνέχεια, η εξέλιξη των WPAN επέτρεψε τη σύνδεση μικρών αισθητήρων οι οποίοι και λειτουργούν με μπαταρίες σε ασύρματα δίκτυα μεγαλύτερης κλίμακας. Πιο συγκεκριμένα, με την εμφάνιση πρωτοκόλλων όπως το ZigBee, το Z-Wave και το Thread, οι εφαρμογές του WPAN επεκτάθηκαν σε τομείς όπως οι έξυπνες οικιακές συσκευές, τα συστήματα αυτοκινήτων, οι ιατρικές συσκευές και πολλά άλλα. Οι χρησιμοποιούμενες τοπολογίες, πάντα εντός μικρής εμβέλειας μπορούν να είναι αστέρα (star), πλέγματος (mesh), δενδροειδής (cluster tree) Τα ασύρματα προσωπικά δίκτυα WPAN παρουσιάζουν θετικά και αρνητικά στοιχεία που πρέπει να λαμβάνονται υπόψη κατά τη σχεδίαση του δικτύου [39]. Ας ξεκινήσουμε με τα θετικά. Τα δίκτυα WPAN προσφέρουν τη δυνατότητα να κινούμαστε ελεύθερα χωρίς καλώδια. Αυτή η ελευθερία κίνησης

είναι πολύ χρήσιμη, ιδίως όταν χρειάζεται να μετακινηθούμε ελεύθερα στο χώρο. Επίσης, μας δίνει τη δυνατότητα να συνδέσουμε και να αποσυνδέσουμε συσκευές εύκολα. Από άποψη κόστους, τα δίκτυα WPAN μπορούν να είναι πιο οικονομικά σε σύγκριση με τα ενσύρματα προσωπικά δίκτυα (PAN), διότι δε χρειάζεται να αγοράσουμε και να εγκαταστήσουμε ακριβά καλώδια. Επιπλέον, τα WPAN είναι εύκολα επεκτάσιμα και μπορούμε να προσθέσουμε νέες συσκευές ή σημεία πρόσβασης χωρίς μεγάλη προσπάθεια. Αυτή η επεκτασιμότητα είναι σημαντική όταν θέλουμε να αυξήσουμε τον αριθμό των συσκευών μας. Επιπλέον, καθώς δε χρησιμοποιείται μεγάλη ισχύ για την επικοινωνία, η κατανάλωση ενέργειας των συνδεδεμένων συσκευών είναι ιδιαίτερα χαμηλή. Από την άλλη πλευρά, τα WPAN έχουν και τα μειονεκτήματα τους [40]. Ένα από αυτά είναι η περιορισμένη εμβέλεια, γεγονός που μπορεί να δημιουργήσει πρόβλημα όταν προσπαθούμε να συνδεθούμε από μεγάλη απόσταση. Επίσης, τα WPAN είναι ευαίσθητα στις παρεμβολές από άλλες ηλεκτρονικές συσκευές που λειτουργούν στην ίδια ή κοντινή συχνότητα, γεγονός που μπορεί να προκαλέσει προβλήματα σύνδεσης. Επίσης η ταχύτητες μεταφοράς αυτών των δικτύων είναι σχετικά χαμηλές. Τέλος, η ασφάλεια μπορεί να είναι ένα πρόβλημα των δικτύων WPAN, καθώς είναι ευαίσθητα σε διάφορα είδη επιθέσεων. Επομένως, είναι σημαντικό να λάβουμε μέτρα για να προστατεύσουμε τα δεδομένα και τις συσκευές μας από τις απειλές αυτές. Κάποιες χαρακτηριστικές εφαρμογές των ασύρματων προσωπικών δικτύων είναι οι εξής:

- Οι ασύρματες ακουστικές συσκευές που χρησιμοποιούν την τεχνολογία Bluetooth (Bluetooth Headsets), για τη σύνδεση με έξυπνα τηλέφωνα (smartphones), φορητούς υπολογιστές (laptops) και άλλες συσκευές αναπαραγωγής μουσικής.
- Τα ασύρματα πληκτρολόγια, ποντίκια και εκτυπωτές που επίσης χρησιμοποιούν την τεχνολογία Bluetooth ή άλλες παρόμοιες τεχνολογίες WPAN για την ασύρματη σύνδεση με τους ηλεκτρονικούς υπολογιστές.
- Οι ασύρματοι αισθητήρες, όπως για παράδειγμα αισθητήρες θερμοκρασίας, υγρασίας και φωτεινότητας μπορούν να συνδεθούν ασύρματα με υπολογιστές ή άλλες συσκευές χρησιμοποιώντας τεχνολογίες WPAN για τη μετάδοση δεδομένων.
- Οι προσωπικές συσκευές παρακολούθησης υγείας, όπως οι παλμογράφοι, χρησιμοποιούν τεχνολογίες WPAN για να συνδεθούν ασύρματα με smartphones ή άλλες συσκευές παρακολούθησης. Οι έξυπνες οικιακές συσκευές, όπως οι έξυπνες λάμπες, οι έξυπνοι θερμοστάτες και οι έξυπνες πρίζες μπορούν να συνδεθούν μεταξύ τους μέσω πρωτοκόλλων επικοινωνίας WPAN, όπως το ZigBee για τον έλεγχο και την αυτοματοποίηση των λειτουργιών τους.[41]

2.7.2 WLAN

Το ασύρματο τοπικό δίκτυο (Wireless Local Area Network - WLAN) επιτρέπει την ασύρματη μετάδοση δεδομένων μεταξύ συσκευών σε ένα τοπικό δίκτυο. Οι πιο κύριες λειτουργίες του περιλαμβάνουν την ασύρματη μετάδοση και λήψη δεδομένων χρησιμοποιώντας τα σημεία πρόσβαση (access points), για τη σύνδεση των χρηστών στο διαδίκτυο. Συναντάμε αυτά τα δίκτυα συνήθως σε σπίτια, γραφεία, καταστήματα, κέντρα δημόσιας συνάντησης και άλλα μέρη όπου απαιτείται ασύρματη πρόσβαση στο διαδίκτυο. Η υλοποίηση των ασύρματων τοπικών δικτύων βασίζεται στη σειρά προτύπων IEEE 802.11. Οι υποστηριζόμενες δομές δικτύου των WLANs είναι η αστερα (star), κατά την οποία οι συσκευές συνδέονται με ένα κεντρικό σημείο πρόσβασης, η πλέγματος (mesh), κατά την οποία οι συσκευές συνδέονται αμοιβαία μεταξύ τους, και η δενδροειδής (cluster tree), που συνδυάζει την αστεροειδή και τη μεσαία τοπολογία για πιο ευέλικτη και αποτελεσματική κάλυψη. Το 1991 ορίστηκαν οι τεχνικές προδιαγραφές του προτύπου Wavelan που αποτέλεσε τον πρόγονο του Wi-Fi. Τότε, οι ταχύτητες μετάδοσης δεν ξεπερνούσαν τα 2 Mbit/s και το κόστος ήταν μεγάλο. Το 1999 άρχισε η τεχνολογία να χρησιμοποιείτε ευρέως [42]. Σήμερα αποτελούν σημαντικό πυλώνα της σύγχρονης τεχνολογίας δικτύων. Επιτρέπουν στους χρήστες να συνδέονται ασύρματα σε ένα δίκτυο επικοινωνιών, παρέχοντας κινητικότητα και ευελιξία σε διάφορα περιβάλλοντα. Χρησιμοποιούν κυρίως τις συχνότητες 2.4GHz και 5GHz. Τα πιο σημαντικά θετικά χαρακτηριστικά των ασύρματων τοπικών δικτύων είναι η σύνδεση του χρήστη στο διαδίκτυο χρησιμοποιώντας τα σημεία πρόσβασης και η αρκετά μεγαλύτερη εμβέλεια συγκριτικά με το WPAN. Έτσι, διευκολύνονται περισσότερο οι χρήστες, χωρίς να περιορίζονται σε ένα δωμάτιο αλλά σε ένα σπίτι ή και σε ακόμα μεγαλύτερες εκτάσεις, ανάλογα τον εξοπλισμό που

χρησιμοποιείται. Αποτελεί μία αξιόπιστη και πιο οικονομική λύση σε σύγκριση με τις ενσύρματες επικοινωνίες [43]. Με τα σύγχρονα πρότυπα IEEE 802.11, παρέχει υψηλές ταχύτητες μετάδοσης δεδομένων. Συνήθως χρησιμοποιούνται πανκατευθυντικές κεραίες, οπότε οι συσκευές μπορούν να βρίσκονται σε οποιαδήποτε κατεύθυνση σε σχέση με το σημείο πρόσβασης. Η εγκατάσταση του δικτύου χαρακτηρίζεται εύκολη και οικονομικότερη σε σύγκριση με τα ενσύρματα τοπικά δίκτυα (LAN). Απ' την άλλη πλευρά του νομίσματος, η εμβέλεια τους σε ορισμένες περιπτώσεις δεν είναι επαρκής και επομένως, σε κάποιες υλοποιήσεις θα πρέπει να χρησιμοποιηθεί άλλος τύπος ασύρματου δικτύου. Επίσης, υπάρχει μεγάλη πιθανότητα παρεμβολών ή απώλειας σήματος λόγω φυσικών ή τεχνητών εμποδίων, φυσικών φαινομένων όπως η βροχή ή λόγω άλλων IoT συσκευών που λειτουργούν στο ίδιο φάσμα συχνοτήτων, με αποτέλεσμα της μειωμένης ταχύτητας ή και των αποσυνδέσεων. Οι ταχύτητες επικοινωνίας μειώνονται με τη σύνδεση περισσότερων συσκευών και συγκριτικά με τα τοπικά δίκτυα που χρησιμοποιούν καλώδια είναι χαμηλότερες. Επιπλέον, η ανάγκη για τη χρήση καλωδίων εξακολουθεί να υφίσταται για την υλοποίηση του δικτύου κορμού (backbone). Τέλος, όπως και σε κάθε άλλο τύπο ασύρματου δικτύου, η ασφάλεια αποτελεί αδυναμία διότι καθιστά την σύνδεση πιο ευάλωτη σε επιθέσεις σε σύγκριση με τις ενσύρματες συνδέσεις [44]. Για το λόγο αυτό συχνά χρησιμοποιούνται πρωτόκολλα κρυπτογράφησης, όπως το Wi-Fi Protected Access 2 (WPA2). Τα ασύρματα δίκτυα WLAN μπορούν να χρησιμοποιηθούν στις κάτωθι εφαρμογές:

- Την αντικατάσταση και την επέκταση των παραδοσιακών ενσύρματων δικτύων LAN. Πλέον, λόγω της εξέλιξης της τεχνολογίας υφίσταται απαίτηση για δικτύωση και πρόσβαση στο Internet. Τα περισσότερα κτίρια στη χώρα μας δε διαθέτουν εγκατεστημένη καλωδίωση ethernet. Τη λύση στο πρόβλημα αυτό δίνουν τα δίκτυα WLAN. Επίσης, σε ιδιαίτερα ανοιχτά δωμάτια, όπως, όπως εργοστάσια παραγωγής, αίθουσες διαπραγμάτευσης χρηματιστηρίων και αποθήκες, ένα ασύρματο τοπικό δίκτυο παρέχει μια πιο αποτελεσματική λύση από τα LANs. Στις περιπτώσεις που αναφέραμε, το δίκτυο δομής (backbone network) υλοποιείται με καλωδίωση ethernet. Υποκατηγορία αυτής της χρήσης μπορεί να θεωρηθεί η χρήση της τεχνολογίας WLAN για τη ζεύξη δικτύων LAN σε γειτονικά κτίρια. Στην περίπτωση αυτή χρησιμοποιείται μία ασύρματη σύνδεση point-to-point μεταξύ των κτιρίων. Οι συσκευές που συνδέονται με αυτόν τον τρόπο είναι συνήθως access points που λειτουργούν ως γέφυρες ή δρομολογητές.
- Τη νομαδική πρόσβαση, η οποία παρέχει μια ασύρματη σύνδεση μεταξύ ενός κόμβου LAN και μιας συσκευής εξοπλισμένης με κεραία, όπως ένας φορητός υπολογιστής. Ένα παράδειγμα της χρησιμότητας μιας τέτοιας σύνδεσης είναι η δυνατότητα ενός εργαζόμενου που επέστρεψε από ταξίδι να μεταφέρει δεδομένα από έναν προσωπικό φορητό υπολογιστή σε έναν διακομιστή της εργασίας του. Η νομαδική πρόσβαση είναι επίσης χρήσιμη σε περιβάλλοντα όπως όπως μια πανεπιστημιούπολη ή μια επιχείρηση που λειτουργεί σε ένα σύμπλεγμα κτιρίων. Και στα δύο αυτές τις περιπτώσεις, οι χρήστες μπορεί να μετακινούνται με τους φορητούς υπολογιστές τους και μπορεί να επιθυμούν πρόσβαση στους διακομιστές ενός ενσύρματου LAN από διάφορες τοποθεσίες.
- Τη δικτύωση Ad Hoc, η οποία αποτελεί ένα δίκτυο peer-to-peer, χωρίς κεντρικό διακομιστή, που δημιουργείται προσωρινά για την κάλυψη κάποιας άμεσης ανάγκης. Για παράδειγμα, μια ομάδα υπαλλήλων, ο καθένας με έναν φορητό υπολογιστή, μπορεί να συγκεντρωθεί σε ένα συνέδριο για μια επαγγελματική συνάντηση και συνδέουν τους υπολογιστές μεταξύ τους, σε ένα προσωρινό δίκτυο, μόνο για τη διάρκεια της συνάντησης [40].

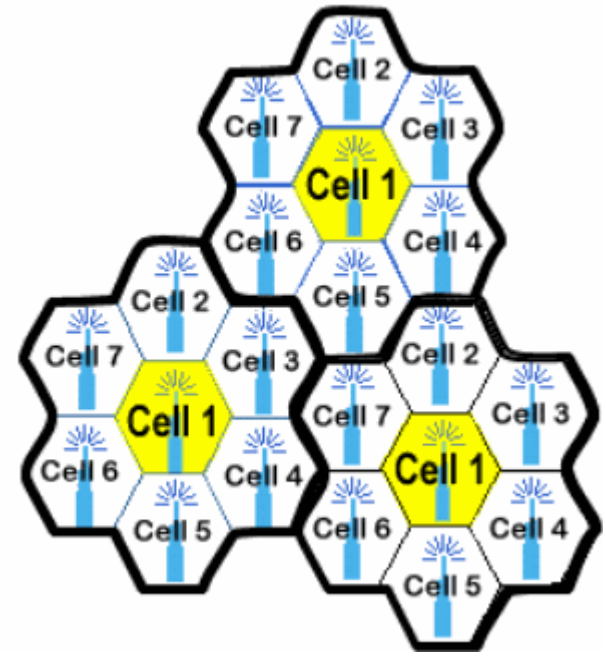
2.7.3 WMAN

Τα ασύρματα δίκτυα μητροπολιτικής περιοχής (Wireless Metropolitan Area Network - WMAN) είναι ασύρματα δίκτυα που παρέχουν ευρυζωνική σύνδεση σε μεγάλες γεωγραφικές περιοχές μητροπολιτικού μεγέθους ακτίνας ως 50 χιλιόμετρα. Οι συνδέσεις που πραγματοποιούνται μπορεί να είναι point-to-point ή point-to-multipoint [40]. Έτσι ένα σημείο πρόσβασης εξυπηρετεί πολλαπλούς κόμβους. Κυρίως χρησιμοποιούνται οι τεχνολογίες Wireless Interoperable Metropolitan Area Exchange (WiMAX), Local Multipoint Distributed Service (LMDS) και Multi-Channel Multipoint Distributed

Service (MMDS) [45]. Τέτοια δίκτυα στο παρελθόν τοποθετήθηκαν σε κάποιες πόλεις ώστε να προσφέρουν πρόσβαση στο διαδίκτυο σε ανθρώπους που βρίσκονται εκτός κτιρίων. Τα δίκτυα αυτά έχουν κοινές λειτουργίες σε σύγκριση με τα WLANs αλλά καλύπτουν αρκετά μεγαλύτερες περιοχές. Τα σημεία πρόσβασης μπαίνουν πάνω σε κολώνες ή πύργους τηλεφωνίας, διάσπαρτα, ώστε να καλύψουν το μεγαλύτερο μέρος ή και όλη την πόλη. Οι χρήστες χρησιμοποιούν το πλησιέστερο σημείο πρόσβασης προκειμένου να έχουν πρόσβαση στο διαδίκτυο. Τα σημεία πρόσβασης συνδέονται στο δίκτυο κορμού μέσω καλωδίων UTP ή fiber optic. Από την πλευρά του χρήστη, η σύνδεση στα δίκτυα WMAN είναι γρήγορη, εύκολη και οικονομική καθώς δεν απαιτείται η εγκατάσταση εξοπλισμού. Επίσης η επέκταση τους είναι χρονικά γρήγορη, δίνοντας την δυνατότητα στους φορείς του δικτύου να προσαρμόζονται στις απαιτήσεις των χρηστών. Επίσης παρέχουν ταχύτητες μετάδοσης που είναι συγκρίσιμες με τις ενσύρματες συνδέσεις, αλλά με την προστιθέμενη ευελιξία της ασύρματης συνδεσιμότητας. Απ΄ την άλλη πλευρά το κόστος εγκατάστασης του απαιτούμενου εξοπλισμού για τους φορείς είναι εξαιρετικά δαπανηρό. Επιπλέον, μέσα στις πόλεις, υπάρχουν ηλεκτρομαγνητικές παρεμβολές ιδιαίτερα λόγω σκεδάσεων και ανακλάσεων από τα κτήρια. Τέλος, απαιτούνται αξιόπιστοι αλγόριθμοι κρυπτογράφησης προκειμένου να μην υποκλέβονται τα δεδομένα, και η συντήρηση και η διαχείριση του δικτύου αυτού απαιτεί συνεχή παρακολούθηση από εξειδικευμένο προσωπικό. [46]

2.7.4 WWAN

Το ασύρματο δίκτυο ευρείας περιοχής (Wireless Wide Area Network - WWAN), είναι ένας τύπος ασύρματου δικτύου που καλύπτει εκτάσεις αρκετά μεγαλύτερες από μία πόλη. Επεκτείνεται πέρα από 50 χιλιόμετρα και τις περισσότερες φορές χρησιμοποιεί “ενοικιαζόμενες συχνότητες” (licensed frequencies). Αυτό γίνεται δυνατό αξιοποιώντας την κινητή τηλεφωνία και τις δορυφορικές τηλεπικοινωνίες. Αναφορικά με τα δίκτυα κινητής τηλεφωνίας, στο κυψελοειδές σύστημα, η περιοχή κάλυψης χωρίζεται σε κυψέλες, όπως φαίνεται στο σχήμα 10. Ένας σταθμός βάσης, στο κέντρο της κυψέλης, εξυπηρετεί μια μεμονωμένη κυψέλη. Οι σταθμοί βάσης μιας περιοχής είναι συνδεδεμένοι με τον ελεγκτή σταθμού βάσης που συνδέει το κυψελωτό και το ενσύρματο δίκτυο κινητής τηλεφωνίας. Το σύστημα επιδιώκει την αποτελεσματική χρήση των διαθέσιμων καναλιών. Με τον χωρικό διαχωρισμό μιας μεγάλης περιοχής σε κυψέλες, οι σταθμοί βάσης εκπέμπουν ακτινοβολία χαμηλότερης ισχύος, σε σύγκριση με την περίπτωση που η περιοχή καλυπτόταν από έναν σταθμό βάσης και οι συχνότητες επαναχρησιμοποιούνται σε πολύ μικρότερες αποστάσεις. Από τις αρχές της δεκαετίας του 1980 έχουν αναπτυχθεί διάφορες γενιές κυψελωτών δικτύων. Η πρώτη γενιά (1G) ήταν αναλογική και σχεδιάστηκε καθαρά για φωνητικές κλήσεις με σχεδόν καθόλου υπηρεσίες δεδομένων. Η ταχύτητα δεδομένων έφτανε έως 2,4 kbps. Η δεύτερη γενιά (2G) βασίστηκε στην ψηφιακή τεχνολογία και υποδομή δικτύου (GSM) επιτρέποντας την αποστολή μηνυμάτων κειμένου. Η ταχύτητα δεδομένων έφτανε έως 64 Kbps. Η γενιά 2.5G βρίσκεται μεταξύ της δεύτερης και της τρίτης γενιάς και μερικές φορές αναφέρεται ως 2G + GPRS. Είναι μια βελτιωμένη έκδοση της 2G, με ταχύτητα δεδομένων έως 144 Kbps. Η τρίτη γενιά (3G) εισήχθη το έτος 2000, με ταχύτητα δεδομένων έως και 2 Mbps. Ακολούθως, η γενιά 3.5G είναι μια βελτιωμένη έκδοση της 3G που χρησιμοποιεί HSDPA για να επιταχύνει τη μεταφορά δεδομένων μέχρι και τα 14 Mbps. Η τέταρτη γενιά (4G) είναι ικανή να παρέχει έως και 1 Gbps ταχύτητα δεδομένων και κάθε είδους υπηρεσία ανά πάσα στιγμή σύμφωνα με τις απαιτήσεις του χρήστη, οπουδήποτε. Τέλος, η γενιά (5G) παρουσιάστηκε στις αρχές της δεκαετίας του 2020 και αποτελεί την ταχύτερη και πιο αξιόπιστη τεχνολογία WWAN μέχρι σήμερα, με ταχύτητες έως και 20 φορές ταχύτερες από το 4G. Το 5G έχει επίσης χαμηλότερη καθυστέρηση και υψηλότερη χωρητικότητα, καθιστώντας το ιδανικό για αναδυόμενες τεχνολογίες όπως το Διαδίκτυο των Πραγμάτων (Internet of Things- IoT). Συμπερασματικά, η εξέλιξη των WWANs καθοδηγείται από την ανάγκη για ταχύτερη και πιο αξιόπιστη συνδεσιμότητα στο διαδίκτυο. [47]



Σχήμα 2-10: Κυψελωτά Συστήματα [48]

Ο βασικός εξοπλισμός των είναι οι τηλεφωνικοί πύργοι, οι οποίοι είναι τα κύρια στοιχεία που επιτρέπουν την ασύρματη επικοινωνία, μεταδίδοντας και λαμβάνοντας δεδομένα σε μεγάλη έκταση, οι δρομολογητές που καθιστούν δυνατή την σύνδεση των χρηστών στο διαδίκτυο, οι κάρτες SIM που είναι απαραίτητες για την ταυτοποίηση και αναγνώριση των χρηστών και τα συστήματα παρακολούθησης της απόδοσης του δικτύου. Η κύρια και πιο εμφανής διαφορά με τους άλλους τύπους δικτύων είναι η απόσταση στην οποία μπορούν τα ασύρματα δίκτυα αυτού του τύπου να χρησιμοποιηθούν. Το WWAN μπορεί να καλύψει από πόλεις έως και χώρες, ενώ το WLAN καλύπτει συνήθως εκτάσεις όσο ένα κτήριο και το WPAN όσο ένα δωμάτιο. Επίσης, το WWAN είναι καταλληλότερο για τηλεφωνικές συσκευές, όπως τα έξυπνα τηλέφωνα, διότι παρέχουν την δυνατότητα σύνδεσης στο διαδίκτυο ενώ αυτές βρίσκονται εν κινήσει και οι ταχύτητες είναι υψηλές. Το πιο σημαντικό πλεονέκτημα των δικτύων WWAN είναι η ευελιξία και η κινητικότητα που παρέχουν στους χρήστες. Το κόστος με το οποίο επιβαρύνονται οι πάροχοι για τον εξοπλισμό και την διατήρηση αυτού είναι χαμηλό. Επίσης σε περιπτώσεις που το τοπικό δίκτυο του χρήστη υπολειτουργεί ή έχει πέσει, αποτελεί μία εναλλακτική δυνατότητα η οποία μπορεί να χρησιμοποιηθεί στις περισσότερες περιπτώσεις. Τα αρνητικά χαρακτηριστικά των WWAN είναι το μεγάλος κόστος που θα πρέπει να πληρώνει ο συνδρομητής σε σύγκριση με άλλες τηλεπικοινωνιακές τεχνολογίες, η περιορισμένη ταχύτητα, ιδιαίτερα σε περιοχές με ασθενές σήμα και η καθυστέρηση που μπορεί να παρουσιαστεί συγκριτικά με τις ενσύρματες συνδέσεις. Αυτά τα χαρακτηριστικά δεν το καθιερώνουν ως ιδανική επιλογή για “ζωντανές” εφαρμογές με ήχο και βίντεο. Τέλος όπως όλοι οι άλλοι τύποι ασύρματων δικτύων, είναι ευάλωτο σε κακόβουλες επιθέσεις. [46]

Κεφάλαιο 3: Εξοπλισμός Ασύρματων Δικτύων

3.1 Κεραίες

Στα ασύρματα δίκτυα, οι κεραίες αποτελούν βασικό τεχνολογικό στοιχείο . Αντιπροσωπεύουν τη γέφυρα μεταξύ των συσκευών και του ασύρματου περιβάλλοντος, επιτρέποντας την ασύρματη μετάδοση και τη λήψη δεδομένων.[49]

3.1.1 Χαρακτηριστικά Κεραιών

Ανάλογα με τη χρήση, πρέπει να χρησιμοποιήσουμε την κατάλληλη κεραία, λαμβάνοντας υπόψη τα χαρακτηριστικά της. Τα βασικότερα χαρακτηριστικά των κεραιών είναι τα εξής:

Το **κέρδος (gain)** εκφράζει την αποδοτικότητα της κεραίας. Το κέρδος μιας κεραίας σε μια δεδομένη κατεύθυνση ορίζεται ως ο λόγος της ηλεκτρομαγνητικής ισχύος, σε μια δεδομένη κατεύθυνση, προς την εκπεμπόμενη ηλεκτρομαγνητική ισχύ της ισοτροπική κεραίας. Μετριέται συχνά σε dBi. Ένα ακόμα χαρακτηριστικό μιας κεραίας συναφές με το κέρδος είναι η κατευθυντικότητα. Ορίζεται ως μέγιστη εκπεμπόμενη ακτινοβολία προς τη μέση εκπεμπόμενη ακτινοβολία. Το μέγεθος αυτό είναι ανεξάρτητο από τις απώλειες της κεραίας και συνεπώς αποτελεί ένα μέγεθος που περιγράφει την ικανότητα της κεραίας να κατευθύνει την ισχύ και, όταν δεν υπάρχουν απώλειες, ταυτίζεται με το κέρδος της κεραίας.

Η **πόλωση (polarization)** εκφράζει την κατεύθυνση των ηλεκτρομαγνητικών κυμάτων που παράγει η κεραία καθώς η ενέργεια ακτινοβολείται. Μπορεί να είναι γραμμική (linear), κυκλική (circular) ή ελλειπτική (elliptical) .

Η **μπάντα συχνοτήτων (frequency band)**. στην οποία λειτουργεί. Για παράδειγμα στις επικοινωνίες Wi-Fi χρησιμοποιούνται οι συχνότητες 2,4 GHz και 5 GHz.

Το **μήκος της κεραίας (antenna length),** όταν αναφερόμαστε σε δίπολα, πρέπει να είναι περίπου το μισό του μήκους κύματος του σήματος που λαμβάνει ή εκπέμπει. Αξιοποιώντας τον τύπο $c = \lambda * f$, μπορούμε, με γνωστή τη συχνότητα, να υπολογίσουμε το μήκος κύματος και συνεπώς το μήκος της κεραίας. Για υψηλότερες συχνότητες, το μήκος κύματος μειώνεται, με αποτέλεσμα το μήκος της κεραίας να μειώνεται επίσης.

Το **διάγραμμα ακτινοβολίας (radiation pattern)** αποτελεί την γραφική απεικόνιση της εκπομπής και λήψης της ηλεκτρομαγνητικής ακτινοβολίας μιας κεραίας σε συνάρτηση με τις γωνίες συντεταγμένων (αζιμούθιο φ και ανύψωση θ).

Ο **κύριος λοβός (main lobe or main beam)** είναι ο λοβός ακτινοβολίας στον οποίο η κεραία παρουσιάζει το μεγαλύτερο κέρδος.[50][51] [52]

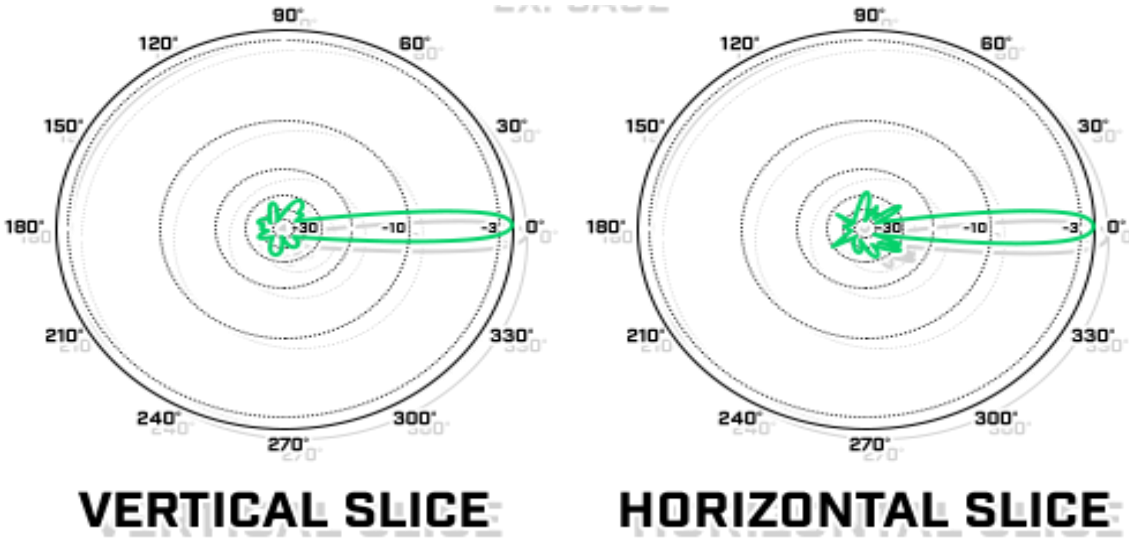
Το **εύρος δέσμης (beamwidth)** είναι ο γωνιακός διαχωρισμός μεταξύ των σημείων του κύριου λοβού που βρίσκονται 3 dB χαμηλότερα από το μέγιστο κέρδος. Η γωνία αυτή ονομάζεται γωνία λοβού. Μια κεραία έχει οριζόντιο και κατακόρυφο εύρος δέσμης, σχηματίζοντας μια γωνία οριζόντιου λοβού και μια γωνία κατακόρυφου λοβού, αντίστοιχα. Το εύρος δέσμης είναι μια βασική παράμετρος για τις κατευθυντικές κεραίες. [53]

3.1.2 Είδη κεραιών

Οι βασικότεροι τύποι κεραιών ως προς την κατευθυντικότητα είναι οι κατευθυντικές (Directional Antennas), οι πανκατευθυντικές (Omni Directional Antennas), οι ημικατευθυντικές κεραίες (Semi Directional Antennas) και οι έξυπνες κεραίες (Smart Antennas). Ο κάθε τύπος έχει τα δικά του

χαρακτηριστικά και συνεπώς η επιλογή του κατάλληλου τύπου εξαρτάται από τις ανάγκες του δικτύου, το περιβάλλον και τις απαιτήσεις κάλυψης.

- Οι κατευθυντικές κεραίες (Directional Antennas) είναι ένα είδος κεραιών, που εστιάζουν την ισχύ τους σε μια συγκεκριμένη κατεύθυνση. Αυτή η ιδιότητα, την καθιστά ιδανική για περιπτώσεις όπου απαιτείται επικοινωνία μεγάλης απόστασης. Οι κεραίες αυτές έχουν ένα στενό διάγραμμα ακτινοβολίας, το οποίο σημαίνει ότι η εκπεμπόμενη ακτινοβολία συγκεντρώνεται σε μια συγκεκριμένη κατεύθυνση, όπως φαίνεται στο σχήμα 1. Αυτό το χαρακτηριστικό, τις καθιστά κατάλληλες για εφαρμογές όπου απαιτείται μακρινή επικοινωνία με σταθερή και αξιόπιστη σύνδεση. Χρησιμοποιούνται κυρίως σε εξωτερικούς χώρους για την επέκταση της κάλυψης ή για τη σύνδεση μεταξύ σταθμών σε μεγάλες αποστάσεις. Τις συναντάμε σε συσκευές όπως τα σημεία πρόσβασης (Access Points) που χρησιμοποιούνται για τη ζεύξη point-to-point σε ασύρματα μητροπολιτικά δίκτυα (σχήμα 2).[49]



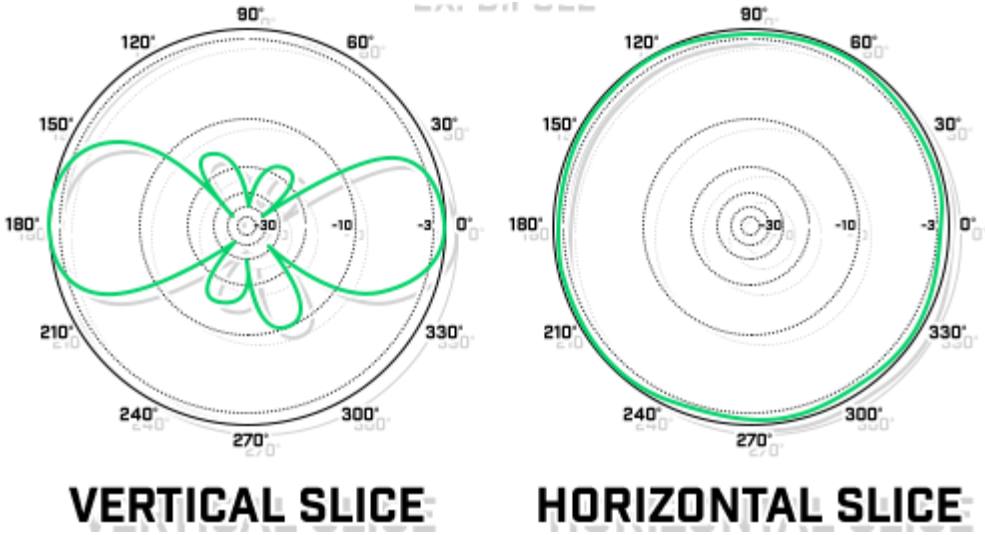
Σχήμα 3-1: Διάγραμμα ακτινοβολίας κατευθυντικής κεραίας [54]

Σχήμα 3-2: Ζεύξη point-to-point με χρήση κατεθυντικών κεραιών [55]

Ο παραβολικός ανακλαστήρας, με τη μορφή πλέγματος ή πιάτου, όπως φαίνεται στο σχήμα 3, χρησιμοποιείται κυρίως στις δορυφορικές και επίγειες μικροκυματικές τηλεπικοινωνίες. Προσφέρει μείωση των δευτερευόντων λοβών και συνεπώς της σπατάλης ισχύος. Η τροφοδοσία μπορεί να τοποθετηθεί σε οποιαδήποτε θέση και γίνεται ρύθμιση της δέσμης (στένωση ή διεύρυνση) ρυθμίζοντας τις ανακλαστικές επιφάνειες. Ωστόσο, λόγω της κατασκευής του, μέρος της ισχύος που ανακλάται από τον παραβολικό ανακλαστήρα παρεμποδίζεται ιδιαίτερα σε ανακλαστήρες μικρών διαστάσεων.[56]

Σχήμα 3-3: Παραβολικοί ανακλαστήρες με τη μορφή πιάτου και πλέγματος[57] [58]

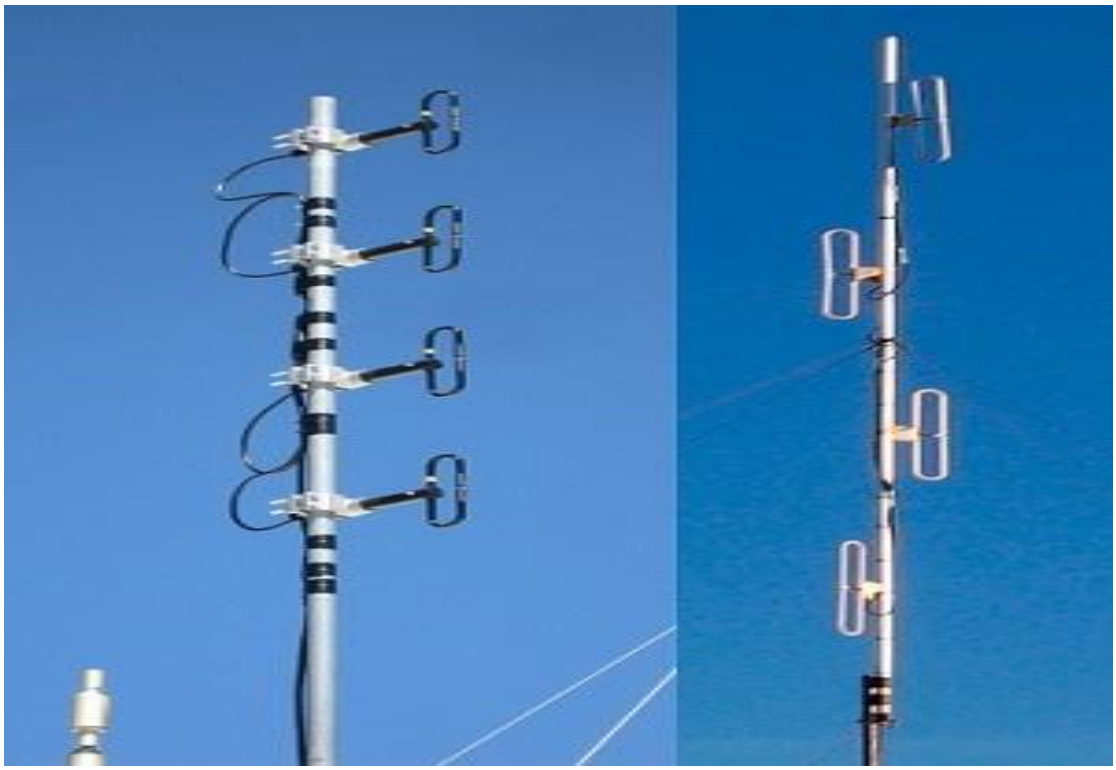
- Οι πανκατευθυντικές κεραίες έχουν απλό σχεδιασμό, εκπέμπουν και λαμβάνουν ισχυρά σήματα σε όλες τις κατευθύνσεις ταυτόχρονα, χωρίς να χρειάζεται να στραφούν προς ένα συγκεκριμένο σημείο. Οι πανκατευθυντικές κεραίες είναι εξαιρετικά χρήσιμες σε περιπτώσεις όπου απαιτείται ευρεία κάλυψη του σήματος σε πολλές κατευθύνσεις, χωρίς την ανάγκη να προσανατολιστούν προς συγκεκριμένα σημεία. Αυτό το χαρακτηριστικό τις καθιστά ιδανικές για χρήση σε περιβάλλοντα όπου οι συνδέσεις πρέπει να είναι γενικής κάλυψης ή όπου οι συσκευές μπορεί να βρίσκονται σε διάφορες κατευθύνσεις. Το διάγραμμα ακτινοβολίας μια πανκατευθυντικής κεραίας φαίνεται στο σχήμα 4. Τις συναντάμε συνήθως σε ασύρματους δρομολογητές (wireless Routers) σε σπίτια, γραφεία, καφετέριες και άλλα μέρη όπου χρειάζεται ευρεία κάλυψη του σήματος. Επιπλέον, χρησιμοποιούνται σε μητροπολιτικά δίκτυα όπου η κάλυψη του σήματος πρέπει να είναι ομοιόμορφη σε όλη την περιοχή.[49]
-
-
-
-



Σχήμα 3-4: Διάγραμμα ακτινοβολίας Πανκατευθυντικής Κεραίας [54]

Η κεραία collinear, η οποία φαίνεται στο σχήμα 5 είναι ένας τύπος κεραίας που είναι συνήθως κατακόρυφος και αποτελείται από έναν αριθμό στοιχείων κεραίας, συχνά δίπολα, τοποθετημένα με τέτοιο τρόπο ώστε να βρίσκονται στον ίδιο άξονα. Συνήθως όλα τα στοιχεία τροφοδοτούνται έτσι ώστε κάθε στοιχείο της κεραίας να εκπέμπει σήμα της ίδιας φάσης, με αποτέλεσμα η μέγιστη ακτινοβολία να είναι κάθετη στον άξονα της κεραίας. Χρησιμοποιείται συχνά για εκπομπές ραδιοφωνικών μεταδόσεων ή ως κεραία ραδιοεπικοινωνιών από σημείο σε σημείο, καθώς είναι σε θέση να επιτύχει ολόπλευρη κάλυψη και με την κύρια δέσμη παράλληλη προς την επιφάνεια της γης. Μικρό τμήμα του σήματος

εκπέμπεται προς τα πάνω, όπου δεν έχει καμία χρησιμότητα.[59]



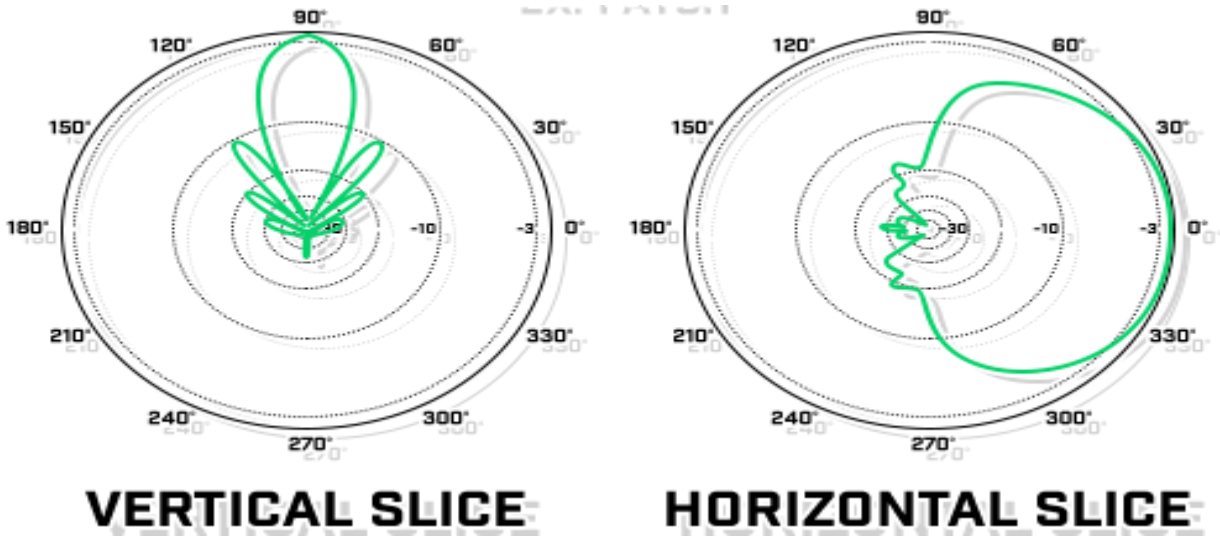
Σχήμα 3-5: Κεραία collinear [60]

Το δίπολο είναι ο απλούστερος τύπος κεραίας από θεωρητική άποψη. Συνήθως αποτελείται από δύο αγωγούς ίσου μήκους προσανατολισμένους συγγραμμικά, με τη γραμμή τροφοδοσίας συνδεδεμένη στο κέντρο μεταξύ τους. Το διάγραμμα ακτινοβολίας του διπόλου μισού μήκους κύματος είναι μέγιστο κάθετα προς τον αγωγό, ενώ μηδενίζεται στην αξονική κατεύθυνση, υλοποιώντας έτσι μια πανκατευθυντική κεραία αν εγκατασταθεί κάθετα, ή (συνηθέστερα) μια ασθενώς κατευθυντική κεραία αν εγκατασταθεί οριζόντια. Αν και μπορούν να χρησιμοποιηθούν ως αυτόνομες κεραίες χαμηλού κέρδους, τα δίπολα χρησιμοποιούνται επίσης ως οδηγούμενα στοιχεία σε πιο σύνθετα σχέδια κεραιών, όπως η κεραία Yagi-Uda και οι οδηγούμενες συστοιχίες (phased arrays).

Στο σχήμα 6, φαίνεται μια πανκατευθυντική κεραία που μπορεί να χρησιμοποιηθεί για την κάλυψη ενός δικτύου WLAN.[61]

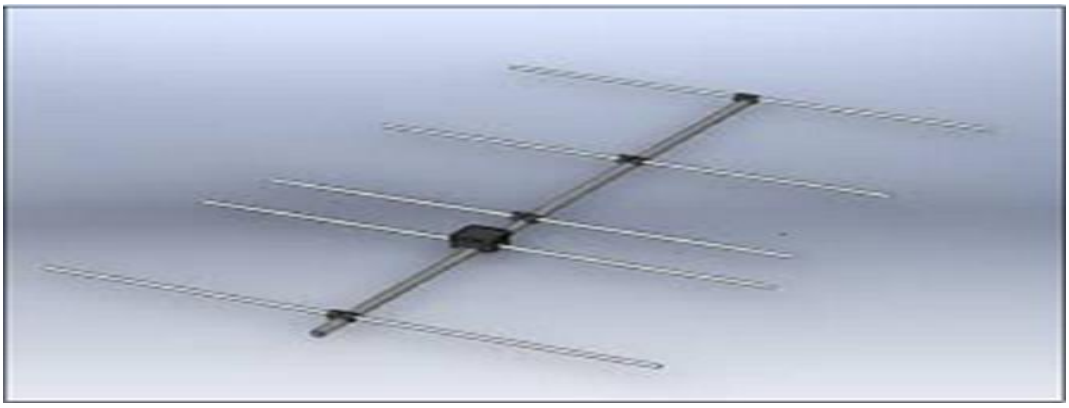
Σχήμα 3-6: Πανκατευθυντική Κεραία για WLAN [62]

- Οι ημικατευθυντικές κεραίες (Semi Directional Antenna) είναι ένα είδος κεραιών που παρέχουν μεσαίου μεγέθους κατευθυντικότητα. Αντίθετα με τις πανκατευθυντικές κεραίες που εκπέμπουν σε όλες τις κατευθύνσεις και τις κατευθυντικές κεραίες που εστιάζουν την ενέργειά τους σε μια συγκεκριμένη κατεύθυνση, οι ημικατευθυντικές κεραίες παρέχουν ένα ενδιάμεσο επίπεδο κατευθυντικότητας, όπως φαίνεται στο σχήμα 7. Συνήθως έχουν ένα πιο στενό πεδίο ακτινοβολίας σε σύγκριση με τις πανκατευθυντικές κεραίες, αλλά εξακολουθούν να καλύπτουν μεγαλύτερη περιοχή από τις κατευθυντικές κεραίες. Οι ημικατευθυντικές κεραίες επιτρέπουν στους χρήστες να επικεντρώνουν τα σήματά τους προς μια συγκεκριμένη κατεύθυνση, ενώ ταυτόχρονα παρέχουν μια σχετικά καλή κάλυψη σε μια ευρύτερη περιοχή σε σύγκριση με τις κατευθυντικές κεραίες. Αυτή η ισορροπία τους τις κάνει κατάλληλες σε περιβάλλοντα όπως στα ασύρματα δίκτυα πόλεων όπου υπάρχουν πολλοί χρήστες που βρίσκονται σε διαφορετικές κατευθύνσεις, αλλά η κάλυψη πρέπει να περιορίζεται σε συγκεκριμένες περιοχές. Χαρακτηριστική είναι η χρήση τους σε εφαρμογές όπως οι ασύρματες κάμερες ασφαλείας όπου είναι σημαντική η επίτευξη κάλυψης σε μια συγκεκριμένη περιοχή αλλά και η δυνατότητα λήψης σήματος από γύρω περιοχές.[49]



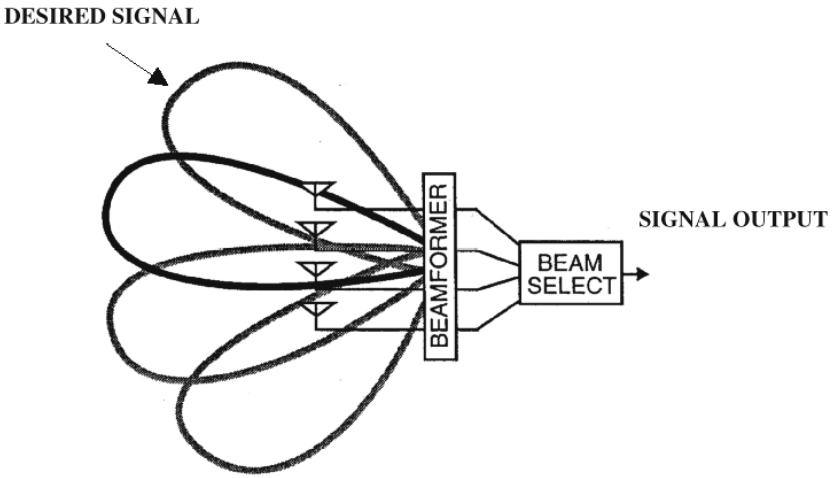
Σχήμα 3-7: Διάγραμμα Ακτινοβολίας Ημικατευθυντικής Κεραίας [54]

Η κεραία Yagi-Uda, η οποία φαίνεται στο σχήμα 8, είναι ο πιο συχνά χρησιμοποιούμενος τύπος ημικατευθυντικής κεραίας για τηλεοπτική λήψη. Είναι ο πιο δημοφιλής και εύχρηστος τύπος κεραίας με καλύτερες επιδόσεις, ο οποίος φημίζεται για το υψηλό κέρδος και την κατευθυντικότητα του.[63]



Σχήμα 3-8: Κεραία Yagi-Uda [64]

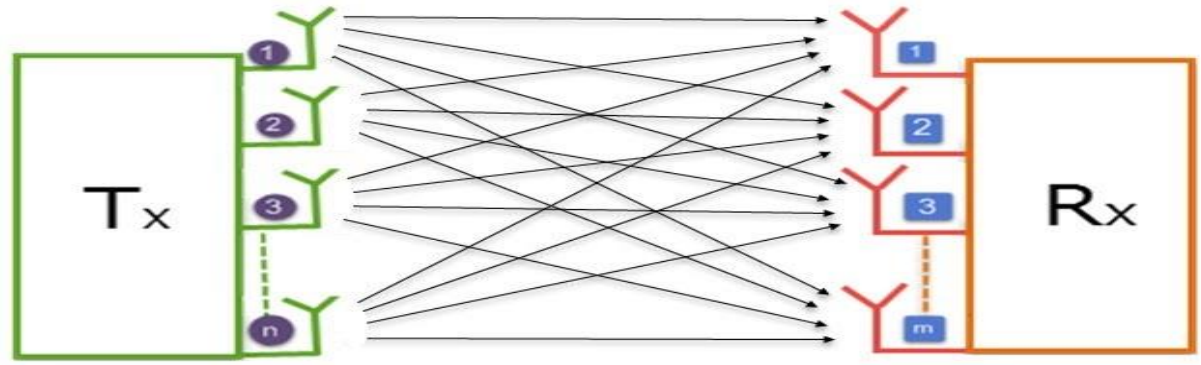
- Οι έξυπνες κεραίες, γνωστές και ως "smart antennas", είναι κεραίες που έχουν τη δυνατότητα να προσαρμόζουν δυναμικά την κατεύθυνση της ακτινοβολίας τους, όπως φαίνεται στο σχήμα 9. Οι έξυπνες κεραίες χρησιμοποιούνται ευρέως σε ασύρματα δίκτυα κινητών τηλεφώνων, ασύρματα δίκτυα LAN και ασύρματα συστήματα αισθητήρων για να βελτιώσουν την απόδοση και την αξιοπιστία της επικοινωνίας. Επιπλέον, οι έξυπνες κεραίες μπορούν να βοηθήσουν στην εξοικονόμηση ενέργειας και στη μείωση της παρεμβολής από άλλα ασύρματα δίκτυα. Για να το πετύχουν αυτό, χρησιμοποιούν τεχνολογίες όπως Active Phased Array, Adaptive Array και Space-Division Multiple Access (SDMA). Οι Active Phased Array Antennas χρησιμοποιούν πολλαπλά στοιχεία κεραίας που μπορούν να ρυθμιστούν ανεξάρτητα για να δημιουργήσουν επιθυμητά μοτίβα ακτινοβολίας, οι Adaptive Antenna Arrays χρησιμοποιούν αισθητήρες για να ανιχνεύσουν την κατεύθυνση του σήματος και να προσαρμόσουν το μοτίβο της ακτινοβολίας τους ανάλογα και οι SDMA χρησιμοποιούν πολύπλοκες τεχνικές επεξεργασίας σήματος για να διαχωρίσουν και να εξυπηρετήσουν πολλαπλά σήματα που προέρχονται από διαφορετικές κατευθύνσεις ταυτόχρονα.[65]



Σχήμα 3-9: Δέσμη Smart Antenna [66]

3.1.3 Πολλαπλή Είσοδος Πολλαπλή Έξοδος (MIMO)

Η τεχνολογία Πολλαπλής Εισόδου Πολλαπλής Εξόδου (Mulitple Input Multiple Output - MIMO) χρησιμοποιεί πολλαπλούς πομποδέκτες για να μεταφέρει δεδομένα ασύρματα. και χρησιμοποιείται ευρέως σε ασύρματα δίκτυα, όπως τα Wi-Fi, WiMAX, 3G και LTE. Ο βασικός στόχος του MIMO είναι η βελτίωση της ασύρματης επικοινωνίας μέσω της χρήσης των πολλαπλών κεραιών για τη μετάδοση και λήψη δεδομένων με μεγαλύτερες ταχύτητες. Η τεχνολογία αυτή εκμεταλλεύεται το φαινόμενο των πολλαπλών διαδρομών (multipath), κατά το οποίο τα ασύρματα σήματα αντανακλώνται από διάφορες επιφάνειες και φτάνουν στο δέκτη μέσω πολλών διαδρομών, όπως φαίνεται στο σχήμα 10. Ένα σημαντικό στοιχείο του MIMO είναι η χρήση έξυπνων αλγορίθμων στον πομποδέκτη που επιτρέπουν την ανίχνευση και τη διαχείριση των διαφορετικών σημάτων που φτάνουν από διάφορες κατευθύνσεις. Αυτό βοηθά στη μείωση των παρεμβολών και στην αύξηση της ταχύτητας και της εμβέλειας της ασύρματης επικοινωνίας. Επιπλέον, η σύγχρονη χρήση MIMO αναφέρεται συχνά σε πολλαπλά σήματα δεδομένων που αποστέλλονται σε διαφορετικούς δέκτες (με μία ή περισσότερες κεραίες λήψης), αν και αυτό είναι πιο ακριβές να ονομάζεται Πολλαπλών Χρηστών Πολλαπλών Εισόδων Μίας Εξόδου (Multi-User Multiple-Input Single-Output - MU-MISO).[67]



Σχήμα 3-10: Συστήματα MIMO [68]

3.1.4 Διαμόρφωση Δέσμης (Beamforming)

Η Beamforming είναι μια τεχνολογία ασύρματης επικοινωνίας που χρησιμοποιείται σε ασύρματα δίκτυα για να βελτιώσει την απόδοση και την εμβέλεια του σήματος. Με τη χρήση της τεχνολογίας Beamforming, μία κεραία μπορεί να εστιάσει το σήμα εκπομπής ή λήψης προς συγκεκριμένες κατευθύνσεις αντί για όλο το χώρο γύρω της, όπως φαίνεται στο σχήμα 11. Αυτό βελτιώνει την ποιότητα του σήματος και αυξάνει την ταχύτητα μεταφοράς δεδομένων, καθώς επίσης και την απόσταση στην οποία μπορεί να φτάσει το σήμα. Το Beamforming είναι ιδιαίτερα χρήσιμο σε μεγάλα δίκτυα ή σε ένα περιβάλλον με πολλά εμπόδια, όπου η ασύρματη επικοινωνία αντιμετωπίζει προκλήσεις κατά τη μετάδοση του σήματος. Χρησιμοποιείται ευρέως σε ασύρματα δίκτυα όπως το Wi-Fi.[69]

Σχήμα 3-11: Διαμόρφωση Δέσμης [70]

3.2 Σημεία πρόσβασης

Καθημερινά οι άνθρωποι χρησιμοποιούν τα σημεία πρόσβασης (access points) για να μπορέσουν να συνδεθούν στο διαδίκτυο. Στην πραγματικότητα, τα σημεία πρόσβασης μας παρέχουν ασύρματη πρόσβαση στο διαδίκτυο, προσφέροντας στους χρήστες ευελιξία σε ότι αφορά τη σύνδεση στο διαδίκτυο σε σύγκριση με τα ενσύρματα δίκτυα. Αυτό γίνεται δυνατό δημιουργώντας τοπικά δίκτυα που χρησιμοποιούνται ως πύλες για την πρόσβαση των χρηστών στο διαδίκτυο. Ο εξοπλισμός, η χρήση και δυνατότητες τους διαφέρουν ανάλογα με τις ανάγκες έκαστου γραφείου, σπιτιού ή εταιρείας. Οι περιοχές κάλυψης τους εξαρτώνται από τον εξοπλισμό που χρησιμοποιείται και την λειτουργία τους. Όταν επιλέγουμε σημείο πρόσβασης, πρέπει να λαμβάνουμε υπόψη διάφορους παράγοντες. Το IEEE 802.11 είναι ένα σύνθετο πρότυπο με πολλά προαιρετικά χαρακτηριστικά. Οι εξωτερικές κεραίες είναι συχνά χρήσιμες για τη δημιουργία ενός πυκνού δικτύου κάλυψης σε μια περιοχή. Δεν μπορούν όλα τα σημεία πρόσβασης να συνδεθούν σε εξωτερικές κεραίες. Εάν οι εξωτερικές κεραίες είναι σημαντικές για τα σχέδια ανάπτυξής του δικτύου, πρέπει να βεβαιωθούμε ότι διατίθενται από τον προμηθευτή. Η ασφάλεια είναι ένας τομέας που πρέπει να αξιολογείται. Ορισμένοι κατασκευαστές προσφέρουν εκδόσεις WEP με μεγαλύτερο μήκος κλειδιού, οι οποίες δεν είναι τυποποιημένες αλλά γενικά δια λειτουργικές [71]. [72]

3.2.1 Είδη Σημείων Πρόσβασης

Υπάρχουν αρκετά είδη σημείων πρόσβασης, το καθένα από αυτά χρησιμοποιείται για διαφορετικούς σκοπούς, ανάλογα με τις ιδιαιτερότητες του περιβάλλοντος και τις υπάρχουσες ανάγκες του χρήστη. Το πιο συνηθισμένο σημείο πρόσβασης που συναντάμε στην καθημερινότητα μας είναι εντός της κατοικίας (εσωτερικού χώρου). Αυτά χρησιμοποιούνται για να καλύψουν μικρές περιοχές όπως ένα γραφείο ή ένα σπίτι, προσφέροντας μεγάλες ταχύτητες και σταθερή σύνδεση. Είναι συνηθισμένο πλέον τα οικιακά σημεία πρόσβασης να κάνουν χρήση πολλαπλών κεραιών και διαφόρων εξελιγμένων τεχνολογιών όπως το Beamforming, προκειμένου να βελτιώσουν το σήμα. Ένα άλλο είδος σημείου πρόσβασης το οποίο επίσης συναντάμε συχνά είναι το εξωτερικό. Είναι κατασκευασμένο για να παρέχει μεγαλύτερη κάλυψη δικτύου προκειμένου να χρησιμοποιηθεί για κάλυψη περιοχών όπως ένα γήπεδο ή ένα σχολείο. Με σκοπό την κάλυψη ευρύτερης περιοχής τα συγκεκριμένα σημεία πρόσβασης περιλαμβάνουν είδη κεραιών όπως οι κατευθυντικές και οι ομοαξονικές. Ένα άλλο είδος σημείου πρόσβασης είναι το ελεγχόμενο (Controller-Based Access Points). Το σημείο πρόσβασης αυτό είναι ένα κομμάτι μια κεντρικής υποδομής του ασύρματου δικτύου. Η συσκευή κεντρικής διαχείρισης που είναι υπεύθυνη για την παραμετροποίηση, παρακολούθηση και τον έλεγχο των ελεγχόμενων ασύρματων σημείων πρόσβασης ονομάζεται Wireless Lan Controller (WLC). Ο τύπος αυτός χρησιμοποιείται κυρίως σε επιχειρήσεις. Αυτή η κεντρική διαχείριση προσφέρει στους χρήστες καλύτερο έλεγχο και επέκταση του ασύρματου δικτύου τους. Τέλος, το διαχειριζόμενο από το cloud σημείο πρόσβασης (Cloud-Managed Access

Points). είναι ένα σημείο πρόσβασης που μπορεί ο διαχειριστής να το διαχειριστεί μέσω του δικτύου διαχείρισης στο cloud. Αυτό κάνει τα Access Points "plug-and-play" και επιτρέπει ευέλικτη επέκταση των Access Points, ανεξάρτητα από τον διαθέσιμο χώρο. Οι χρονικά ευαίσθητες λειτουργίες, όπως η γρήγορη περιαγωγή (roaming), ενσωματώνονται στο Cloud-Managed Access Point, ενώ άλλες λειτουργίες που είναι λιγότερο χρονικά ευαίσθητες, όπως η διαχείριση, η παρακολούθηση και η βελτιστοποίηση, αναπτύσσονται στην πλατφόρμα διαχείρισης του cloud. Αυτό βελτιώνει σημαντικά την αποτελεσματικότητα ολόκληρου του δικτύου, την ασφάλεια και τη σταθερότητα. Η χρήση των σημείων πρόσβασης προσφέρει τα ακόλουθα πλεονεκτήματα:

Ευελιξία στη δικτύωση. Τα APs παρέχουν μεγαλύτερη ευελιξία στην τοποθέτηση συσκευών, καθώς εξαλείφεται η ανάγκη για φυσικά καλώδια. Αυτό διευκολύνει την εύκολη πρόσβαση στο δίκτυο από όλες τις τοποθεσίες εντός της περιοχής κάλυψης.

Απλοποιημένη υποδομή δικτύου. Η μειωμένη ανάγκη για φυσικές συνδέσεις απλοποιεί την υποδομή του δικτύου. Αυτό είναι ιδιαίτερα ωφέλιμο σε χώρους όπου η χρήση καλωδίων είναι ανέφικτη ή αντιαισθητική.

Κινητικότητα και περιαγωγή (roaming). Τα ασύρματα σημεία πρόσβασης υποστηρίζουν την περιαγωγή (roaming), η οποία εξασφαλίζει ομαλές μεταβάσεις μεταξύ περιοχών κάλυψης διαφορετικών σημείων πρόσβασης καθώς οι χρήστες μετακινούνται από περιοχή σε περιοχή. Αυτό επιτρέπει στους χρήστες να κινούνται εντός της περιοχής κάλυψης χωρίς να χάνουν τη συνδεσιμότητα.[73][72]

3.2.2 Λειτουργίες Σημείων Πρόσβασης

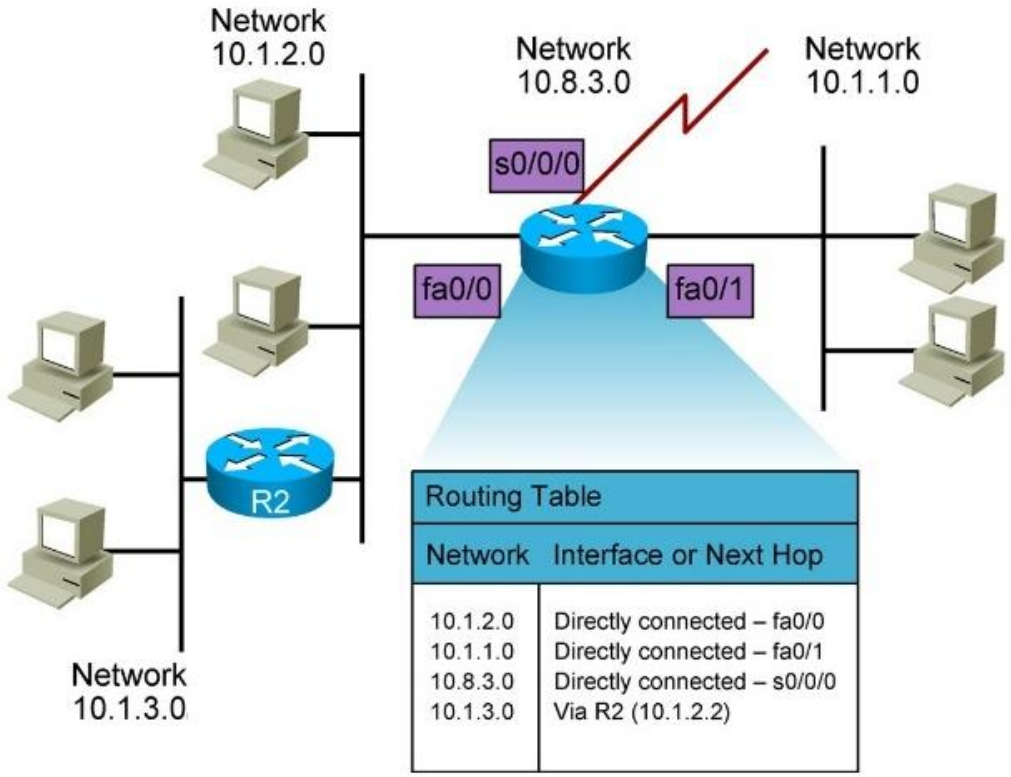
Υπάρχουν τρία βασικά είδη λειτουργιών των σημείων πρόσβασης. Ο βασικότερος από αυτούς είναι το κεντρικό σημείο πρόσβασης (Root access point). Συνδέεται με καλώδιο απευθείας στο ενσύρματο τοπικό δίκτυο (LAN) προσφέροντας ασύρματη πρόσβαση στους χρήστες. Οι ταχύτητες με αυτή την λειτουργία είναι υψηλές και συγκρίσιμες με αυτές της ενσύρματη σύνδεσης. Ανάλογα τις ανάγκες, το πλήθος των root access points μπορεί να διαφέρει. Έχοντας περισσότερα από ένα σημεία πρόσβασης παρέχουμε την δυνατότητα στους χρήστες να κινούνται ελεύθερα μεταξύ περιοχών, χωρίς να χάνουν την πρόσβαση στο διαδίκτυο. Η δεύτερη λειτουργία των σημείων πρόσβασης ονομάζεται επαναλήπτης (Repeater access point). Σε αυτή τη λειτουργία το σημείο πρόσβασης επεκτείνει το ήδη υπάρχων ασύρματο δίκτυο. Η επέκταση του ασύρματου δικτύου και η ταχύτητα εξαρτάται από πολλούς παράγοντες. Η δουλειά του είναι η αποστολή δεδομένων από' τη συσκευή του χρήστη προς το κεντρικό σημείο πρόσβασης ή έναν άλλο επαναλήπτη. Είναι σημαντικό να αναφέρουμε ότι όσους περισσότερους επαναλήπτες χρησιμοποιούμε για την κάλυψη μιας διαδρομής τόσο περισσότερο θα μειώνεται η ταχύτητα, πρόβλημα το οποίο ένα κεντρικό σημείο πρόσβασης δεν παρουσιάζει. Απ’ την άλλη ο επαναλήπτης βοηθά την επεκτασιμότητα του δικτύου χωρίς τη χρήση καλωδίων . Μία άλλη λειτουργία είναι η ασύρματη γέφυρα (Wireless bridge access point). Αυτό το σημείο πρόσβασης χρησιμοποιείται για τη δημιουργία μίας γέφυρας - σύνδεσης μεταξύ δύο δικτύων. Η χρησιμότητα αυτής της λειτουργίας μπορεί να φανεί ιδιαίτερα όταν παραδείγματος χάρη ένα κτήριο χρειάζεται σύνδεση στο διαδίκτυο δίχως να χρησιμοποιεί δομημένη καλωδίωση. Οι ασύρματες γέφυρες αποτελούν ένα σημαντικό κομμάτι για τη δημιουργία ευέλικτων και αξιόπιστων ασύρματων δικτύων.[74].[75]

3.3 Δρομολογητές

Ο δρομολογητής είναι μια φυσική ή εικονική συσκευή που μεταφέρει πληροφορίες μεταξύ δύο ή περισσότερων δικτύων υπολογιστών πραγματοποιώντας μεταγωγή πακέτων. Ο δρομολογητής αποτελεί έναν κοινό τύπο πύλης, ο οποίος τοποθετείται εκεί όπου συναντώνται δύο ή περισσότερα δίκτυα. Εκατοντάδες δρομολογητές ενδέχεται να προωθήσουν ένα και μόνο πακέτο καθώς αυτό κινείται από το δίκτυο που ξεκίνησε μέχρι τον τελικό προορισμό του. Συσκευές δικτύου, όπως τα σημεία ασύρματης πρόσβασης (Access Points) και οι μεταγωγείς (Switches), ενδέχεται να περιλαμβάνουν ενσωματωμένη λειτουργία δρομολογητή.[76]

3.3.1 Ο τρόπος Λειτουργίας του Δρομολογητή

Ένας δρομολογητής εξετάζει τη διεύθυνση IP του προορισμού που βρίσκεται στην επικεφαλίδα ενός πακέτου και τη συγκρίνει με τον πίνακα δρομολόγησης που διαθέτει για να καθορίσει το καλύτερο επόμενο προορισμό του πακέτου, όπως φαίνεται στο σχήμα 12.



Σχήμα 3-12: Λειτουργία Δρομολόγησης [77]

Οι πίνακες δρομολόγησης περιλαμβάνουν κατευθύνσεις για την προώθηση δεδομένων σε συγκεκριμένους προορισμούς δικτύου, μερικές φορές σε συνάρτηση με άλλες μεταβλητές, όπως το κόστος. Ένας πίνακας δρομολόγησης καθορίζει συχνά μια προεπιλεγμένη διαδρομή, την οποία ο δρομολογητής χρησιμοποιεί κάθε φορά που αποτυγχάνει να βρει μια καλύτερη διαδρομή για ένα δεδομένο πακέτο. Για παράδειγμα, ένας τυπικός δρομολογητής οικιακού γραφείου κατευθύνει όλη την εξερχόμενη κυκλοφορία προς μια μόνο προεπιλεγμένη διαδρομή, αυτή προς τον πάροχο Internet του. Οι πίνακες δρομολόγησης είναι είτε στατικοί είτε δυναμικοί. Οι στατικοί δρομολογητές ρυθμίζονται χειροκίνητα, ενώ οι δυναμικοί δρομολογητές ενημερώνουν αυτόματα τους πίνακες δρομολόγησης με βάση τη δραστηριότητα του δικτύου ανταλλάσσοντας πληροφορίες με άλλες συσκευές μέσω πρωτοκόλλων δρομολόγησης.[76]

3.3.2 Λειτουργίες του Δρομολογητή

Η δρομολόγηση πακέτων δεδομένων μεταξύ δικτύων με βάση τις διευθύνσεις IP αποτελεί την πρωταρχική λειτουργία ενός δρομολογητή. Παράλληλα οι δρομολογητές, μπορούν να εκτελούν και άλλες λειτουργίες:

- Το DHCP (Dynamic Host Configuration Protocol) χρησιμοποιείται για τη δυναμική εκχώρηση διευθύνσεων IP σε συσκευές σε ένα δίκτυο. Απλοποιεί τη διαδικασία διαχείρισης διευθύνσεων

IP παρέχοντας αυτόματα στις συσκευές διευθύνσεις IP, μάσκες υποδικτύου, πύλες και πληροφορίες διακομιστή DNS.

- Το Network Address Translation (NAT): επιτρέπει σε πολλές συσκευές εντός ενός ιδιωτικού δικτύου να μοιράζονται μία και μόνη δημόσια διεύθυνση IP. Τροποποιεί τη διεύθυνση IP πηγής ή προορισμού στα πακέτα δεδομένων, επιτρέποντας στις συσκευές ενός ιδιωτικού δικτύου να επικοινωνούν με το διαδίκτυο χρησιμοποιώντας μια ενιαία δημόσια IP.
- Το Virtual Private Network (VPN) χρησιμοποιείται για τη δημιουργία ασφαλών, κρυπτογραφημένων συνδέσεων μέσω του διαδικτύου. Επιτρέπει στους απομακρυσμένους χρήστες να έχουν πρόσβαση σε ιδιωτικά δίκτυα σαν να ήταν απευθείας συνδεδεμένοι στο τοπικό δίκτυο. Το VPN είναι απαραίτητο για την ασφαλή απομακρυσμένη εργασία και την προστασία των δεδομένων κατά τη μετάδοση.
- Το τείχος προστασίας (Firewall) είναι λειτουργία ασφαλείας δικτύου που ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία δικτύου με βάση προκαθορισμένους κανόνες ασφαλείας. Συμβάλλει στην προστασία των δικτύων και των συσκευών από μη εξουσιοδοτημένη πρόσβαση και απειλές στον κυβερνοχώρο.
- Ορισμένοι δρομολογητές υποστηρίζουν μηχανισμούς ποιότητας υπηρεσίας (QoS) ώστε να δίνουν προτεραιότητα σε ορισμένους τύπους κίνησης, όπως φωνή ή βίντεο με σκοπό τη βελτιωμένη απόδοση του δικτύου.[78]

3.3.3 Τύποι Δρομολογητών

Δρομολογητές πυρήνα (Core Routers). Είναι ο ταχύτερος και ισχυρότερος τύπος δρομολογητή και χρησιμοποιείται από τους παρόχους internet. Οι δρομολογητές πυρήνα βρίσκονται στο κέντρο του διαδικτύου και προωθούν τις πληροφορίες κατά μήκος του backbone δικτύου. Οι δρομολογητές επιχειρήσεων συνδέουν τα δίκτυα μεγάλων οργανισμών με τους δρομολογητές πυρήνα.

Δρομολογητές άκρων (Edge Routers). Είναι γνωστοί και ως δρομολογητές πρόσβασης. Είναι μια συσκευή χαμηλότερης χωρητικότητας που βρίσκεται στα όρια ενός τοπικού δικτύου και το συνδέει με το δημόσιο διαδίκτυο, ένα ιδιωτικό WAN ή ένα εξωτερικό τοπικό δίκτυο. Χρησιμοποιούνται ως οικιακοί δρομολογητές και δρομολογητές μικρών γραφείων.

Δρομολογητές κλάδου (Branch Routers). Οι δρομολογητές κλάδου συνδέουν τις απομακρυσμένες τοποθεσίες γραφείων ενός οργανισμού με το ευρύτερο δίκτυο (WAN), συνδεόμενοι με τους δρομολογητές άκρων του πρωτεύοντος δικτύου. Οι δρομολογητές κλάδου παρέχουν συχνά πρόσθετες λειτουργίες, όπως πολυπλεξία διαίρεσης χρόνου, δυνατότητες διαχείρισης WLAN και επιτάχυνση εφαρμογών WAN.

Λογικοί δρομολογητές (Logical Routers). Ένας λογικός δρομολογητής είναι ένα διαμορφωμένο τμήμα ενός παραδοσιακού φυσικού δρομολογητή. Αντιγράφει τη λειτουργικότητα του υλικού, δημιουργώντας πολλαπλούς τομείς δρομολόγησης μέσα σε έναν μόνο δρομολογητή. Οι λογικοί δρομολογητές εκτελούν ένα υποσύνολο των εργασιών που μπορούν να ολοκληρώσουν οι φυσικοί δρομολογητές. Κάθε λογικός δρομολογητής μπορεί να περιέχει πολλές περιπτώσεις δρομολόγησης και πίνακες δρομολόγησης.

Ασύρματοι δρομολογητές (Wireless Routers). Ένας ασύρματος δρομολογητής λειτουργεί με τον ίδιο τρόπο όπως ο δρομολογητής σε ένα ενσύρματο οικιακό ή επαγγελματικό LAN, αλλά επιτρέπει μεγαλύτερη κινητικότητα για τις φορητές συσκευές.[79] [76]

3.3.4 Πρωτόκολλα Δρομολόγησης

Τα πρωτόκολλα δρομολόγησης καθορίζουν τον τρόπο με τον οποίο ένας δρομολογητής αναγνωρίζει άλλους δρομολογητές στο δίκτυο, παρακολουθεί όλους τους πιθανούς προορισμούς και λαμβάνει δυναμικές αποφάσεις για το πού να προωθήσει το κάθε μήνυμα δικτύου. Κάποια εκ των πρωτοκόλλων δρομολόγησης είναι τα εξής:

- Το **Open Shortest Path First (OSPF)** είναι ιεραρχικό πρωτόκολλο δρομολόγησης εσωτερικών πυλών (Interior Gateway Protocol - IGP) με βάση την κατάσταση της σύνδεσης (link-state), για δρομολόγηση σε δίκτυα υπολογιστών. Χρησιμοποιεί το κόστος σαν μέτρο για την δρομολόγηση και χρησιμοποιεί τον αλγόριθμο του Dijkstra για να υπολογιστεί η ελάχιστη διαδρομή,

- Το **Border Gateway Protocol (BGP)** είναι πρωτόκολλο εξωτερικής δρομολόγησης (Exterior Gateway Protocol EGP) που επιτρέπει την δρομολόγηση πακέτων και την ανταλλαγή πληροφοριών προσβασιμότητας μεταξύ μεταξύ των edge routers που ανήκουν σε διαφορετικά αυτόνομα συστήματα (Autonomous Systems - AS) στο διαδίκτυο. Επίσης η λειτουργία του είναι Path Vector, δηλαδή οι αποφάσεις δρομολόγησης βασίζονται στα διαθέσιμα μονοπάτια δρομολόγησης. Το BGP προσφέρει σταθερότητα δικτύου που εγγυάται ότι οι δρομολογητές μπορούν να προσαρμοστούν γρήγορα για να στέλνουν πακέτα μέσω άλλης επανασύνδεσης, εάν ένα μονοπάτι του διαδικτύου πέσει.

- Το **Interior Gateway Routing Protocol (IGRP)** είναι πρωτόκολλο δρομολόγησης εσωτερικών πυλών (Interior Gateway Protocol - IGP) διανύσματος κατάστασης (distance-vector). Για τη δρομολόγηση των πακέτων λαμβάνει υπόψη πολλές παραμέτρους δικτύου όπως το εύρους ζώνης, την καθυστέρηση, το φορτίο και την αξιοπιστία.

- Το **Enhanced Interior Gateway Routing Protocol (EIGRP)** αποτελεί εξέλιξη του πρωτόκολλου IGRP. Εάν ένας δρομολογητής δεν μπορεί να βρει μια διαδρομή προς έναν προορισμό σε έναν από τους πίνακες του, ρωτάει κοντινούς δρομολογητές, οι οποίοι στη συνέχεια ρωτούν τους επόμενους πιο κοντινούς μέχρι να βρεθεί μια διαδρομή. Όταν μια εγγραφή του πίνακα δρομολόγησης αλλάζει σε έναν από τους δρομολογητές, ειδοποιεί τους κοντινούς δρομολογητές για την αλλαγή αντί να στέλνει ολόκληρο τον πίνακα.

- Το **Exterior Gateway Protocol (EGP)** καθορίζει τον τρόπο ανταλλαγής πληροφοριών δρομολόγησης μεταξύ δύο γειτονικών αυτόνομων συστημάτων.

Το **Routing Information Protocol (RIP)** είναι ένα από τα παλαιότερα πρωτόκολλα δρομολόγησης διανύσματος απόστασης, το οποίο χρησιμοποιεί τον αριθμό των αλμάτων ως μέτρο για τη δρομολόγηση. Ο μέγιστος αριθμός αλμάτων που επιτρέπεται για το RIP είναι 15, γεγονός που περιορίζει το μέγεθος των δικτύων που μπορεί να υποστηρίξει. Στα σύγχρονα δίκτυα, το RIP δεν είναι η προτιμώμενη επιλογή πρωτοκόλλου δρομολόγησης, καθώς ο χρόνος σύγκλισης και η επεκτασιμότητά του είναι ανεπαρκείς σε σύγκριση με τα νεώτερα πρωτόκολλα όπως τα EIGRP και OSPF.[79]

Κεφάλαιο 4: Τεχνολογίες Ασύρματων Δικτύων

4.1 Wi-Fi (IEEE 802.11)

Τα ασύρματα τοπικά δίκτυα (WLAN) αποτελούν σήμερα μία από τις πιο σημαντικές τεχνολογίες δικτύων πρόσβασης στο διαδίκτυο. Το Wi-Fi είναι διαδεδομένο σε πολλά μέρη όπως στον εργασιακό χώρο, στο σπίτι, στα εκπαιδευτικά ιδρύματα, στις καφετέριες, στα αεροδρόμια αλλά και σε πολλά άλλα μέρη. Παρόλο που πολλές τεχνολογίες και πρότυπα για δίκτυα WLAN αναπτύχθηκαν τη δεκαετία του 1990, μια συγκεκριμένη σειρά προτύπων έχει επικρεατήσει: η σειρά IEEE 802.11, γνωστή και ως WiFi. Σε αυτό το υποκεφάλαιο θα εξετάσουμε τη δομή, το πρωτόκολλο πολλαπλής πρόσβασης στο μέσο και τη διασύνδεση με ενσύρματα δίκτα των δκτύων WLAN της σειράς προτύπων 802.11. Η σειρά προτύπων IEEE 802.11 (“WiFi”) περιλαμβάνει αριθμό προτύπων 802.11, όπως συνοψίζεται στον πίνακα 1. Τα διάφορά πρότυπα 802.11 μοιράζονται κοινά χαρακτηριστικά. Όλα χρησιμοποιούν βελτιωμένες εκδώσεις της μεθόδου πολλαπλής πρόσβασης στο μέσο, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), το οποίο θα αναλύσουμε παρακάτω. Επίσης, όλα χρησιμοποιούν την ίδια δομή για τα πλαίσια του επιπέδου data link και έχουν τη δυνατότητα να μειώσουν το ρυθμό μετάδοσής τους ώστε να καλύψουν μεγαλύτερες αποστάσεις. Το σημαντικότερο χαρακτηριστικό τους είναι ότι τα πρότυπα 802.11 είναι αναδρομικά συμβατά με προηγούμενες εκδόσεις της σειράς (αφορά πρότυπα που λειτουργούν σε ίδια ζώνη συχνοτήτων). Η δυνατότητα αυτή επιτρέπει, για παράδειγμα, σε μια συσκευή κινητής που είναι ικανή να λειτουργήσει μόνο με το πρότυπο 802.11g να επικοινωνήσει και με έναν νεότερο σταθμό βάσης που λειτουργεί με το πρότυπο 802.11ax. Ωστόσο, όπως φαίνεται στην πίνακα 1, τα πρότυπα 802.11 έχουν κάποιες σημαντικές διαφορές σε ότι αφορά τα χαρακτηριστικά τους. Κάποια πρότυπα λειτουργούν στην περιοχή συχνοτήτων των 2,4 GHz, κάποια στα 5 GHz, και κάποια άλλα υποστηρίζουν και τις δύο συχνότητες. Οι μέγιστοι ρυθμοί μετάδοσης δεδομένων που εμφανίζονται στον Πίνακα 1 αφορούν ένα ιδανικό περιβάλλον (για παράδειγμα, ένας δέκτης τοποθετημένος ένα μέτρο μακριά από το σταθμό βάσης, χωρίς παρεμβολές - σενάριο που είναι απίθανο να συμβεί στην πραγματικότητα).[80]

Standard	Year Launched	Frequency	Maximum Data Rate
Legacy 802.11	1997	2,4 GHz	2 Mbps
802.11b	1999	2,4 GHz	11 Mbps
802.11a	1999	5 GHz	54 Mbps
802.11g	2003	2,4 GHz	54 Mbps
802.11n	2009	2,4 GHz or 5 Ghz	600 Mbps
802.11ac	2013	5 GHz	6.93 Gbps
802.11ax	2019	2,4 GHz or 5 GHz	9.6 Gbps

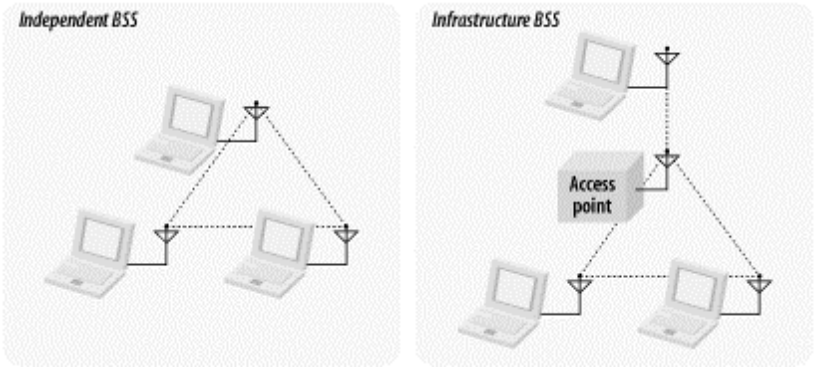
Πίνακας 1: Χαρακτηριστικά των προτύπων της σειράς 802.11 [81][82][83]

Κάποιες τεχνολογίες που ενσωματώνουν τα πρότυπα της σειράς 802.11 είναι οι ακόλουθες:

- **OFDM**. Από το πρότυπο 802.11a και έπειτα χρησιμοποιείται η τεχνική πολυπλεξίας Orthogonal Frequency Division Multiplexing (OFDM), ώστε να επιτευχθεί υψηλότερη ταχύτητα μετάδοσης δεδομένων καθώς υπό διαμόρφωση το σήμα διαιρείται σε τμήματα, τα οποία αποστέλλονται παράλληλα, με τέσσερεις ορθογώνιες φέρουσες (διαφορά φάσης 90^{o}).
- **MIMO**. Τα πρότυπα 802.11n, 802.11ac και 802.11ax χρησιμοποιούν την τεχνολογία πολλαπλών εισόδων πολλαπλών εξόδων.
- **Smart Antennas**. Οι σταθμοί βάσης 802.11ac και 802.11ax μπορούν να μεταδίδουν σε πολλαπλούς σταθμούς ταυτόχρονα και να χρησιμοποιούν "έξυπνες" κεραίες για να διαμορφώνουν τις εκπομπές προς την κατεύθυνση ενός δέκτη, ανάλογα με τις ανάγκες, μειώνοντας έτσι τις παρεμβολές και αυξάνοντας την κάλυψη που επιτυγχάνεται.[80]

4.1.1 Αρχιτεκτονική Wi-Fi (802.11)

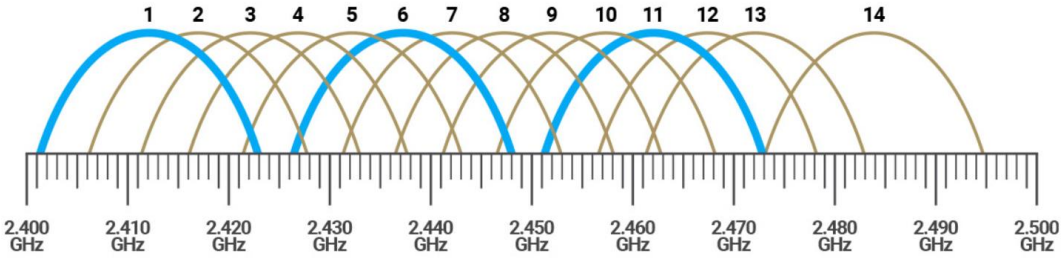
Το βασικό δομικό στοιχείο ενός δικτύου 802.11 είναι το Basic Service Set (BSS), το οποίο αποτελείται από μια ομάδα σταθμών που επικοινωνούν μεταξύ τους. Οι επικοινωνίες λαμβάνουν χώρα εντός μιας περιοχής, που ονομάζεται basic service area, η οποία εξαρτάται από τα χαρακτηριστικά διάδοσης του ασύρματου μέσου και του εξοπλισμού που χρησιμοποιείται. Όταν ένας σταθμός βρίσκεται στην περιοχή βασικής υπηρεσίας, μπορεί να επικοινωνήσει με τα άλλα μέλη του BSS. Τα BSS τα συναντάμε σε δύο εκδοχές, οι οποίες απεικονίζονται στο σχήμα 1.[84][80]



Σχήμα 4-1: Ανεξάρτητο (Independent) και δομημένο (infrastracture) BSS

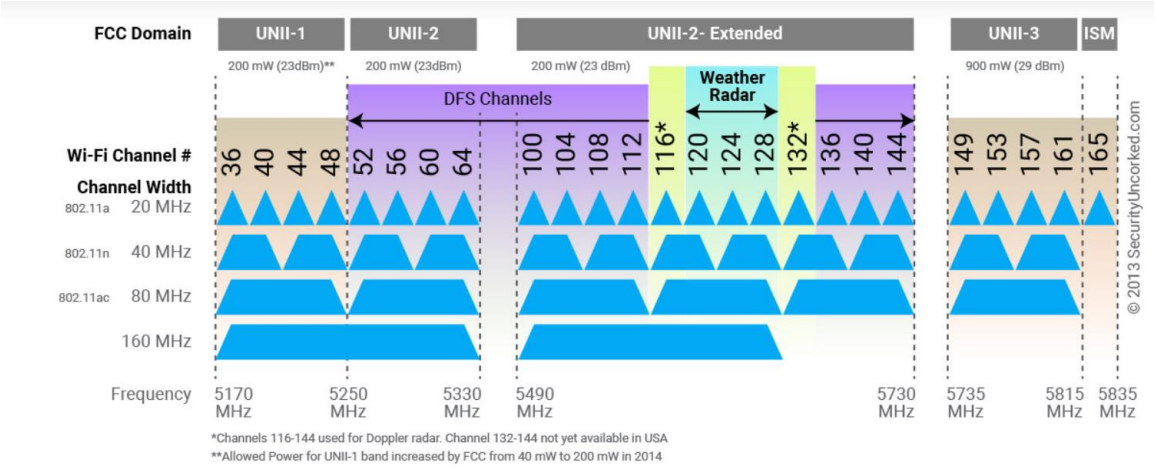
Στο ανεξάρτητο (Independent) BSS (IBSS), οι σταθμοί επικοινωνούν απευθείας μεταξύ τους και, συνεπώς, πρέπει να βρίσκονται σε άμεση εμβέλεια επικοινωνίας. Το μικρότερο δυνατό δίκτυο 802.11 είναι ένα IBSS με δύο σταθμούς. Συνήθως, τα IBSS αποτελούνται από μικρό αριθμό σταθμών που έχουν δημιουργηθεί για συγκεκριμένο σκοπό και για σύντομο χρονικό διάστημα. Για παράδειγμα, μια χρήση του μπορεί να είναι η δημιουργία ενός δικτύου για σύντομη χρονική διάρκεια για την υποστήριξη μιας μόνο συνάντησης σε μια αίθουσα συνεδριάσεων. Με την έναρξη της συνάντησης, οι συμμετέχοντες δημιουργούν ένα IBSS για την ανταλλαγή δεδομένων. Όταν τελειώσει η συνάντηση, το IBSS διαλύεται. Λόγω της σύντομης διάρκειας, του μικρού μεγέθους και του συγκεκριμένου σκοπού τους, τα IBSS αναφέρονται μερικές φορές ως ad hoc BSS ή ad hoc ασύρματα δίκτυα.
Τα δομημένα (Infrastructure) BSS, διακρίνονται από τα ανεξάρτητα (IBSS) λόγω της χρήσης ενός AP, το οποίο χρησιμοποιείται για όλες τις επικοινωνίες, συμπεριλαμβανομένης της επικοινωνίας μεταξύ κινητών σταθμών. Με όλες τις επικοινωνίες να αναμεταδίδονται μέσω ενός AP, η basic service area ενός δομημένου BSS ορίζεται η περιοχή στην οποία μπορούν να ληφθούν μεταδόσεις από το σημείο πρόσβασης. Σε ένα δομημένο BSS, οι σταθμοί πρέπει να συνδεθούν με ένα σημείο πρόσβασης για να λάβουν υπηρεσίες δικτύου Κάθε ασύρματος σταθμός 802.11 έχει μια διεύθυνση Media Access Control (MAC) μήκους 6 byte που είναι αποθηκευμένη στο firmware της κάρτας δικτύου του. Κάθε AP διαθέτει επίσης μια διεύθυνση MAC για την ασύρματη διεπαφή του. Αυτές οι διευθύνσεις MAC διαχειρίζονται από τον οργανισμό IEEE και είναι (θεωρητικά) παγκοσμίως μοναδικές. Όταν ένας διαχειριστής δικτύου εγκαθιστά ένα AP, εκχωρεί στο σημείο πρόσβασης ένα όνομα Service Set Identifier (SSID) μίας ή δύο λέξεων. Ο διαχειριστής πρέπει επίσης να επιλέξει τον αριθμό του καναλιού (ραδιοδιάυλου) λειτουργίας του AP. Το 802.11 λειτουργεί στη ζώνη συχνοτήτων από 2,4 GHz έως

2,4835 GHz. Εντός αυτής της ζώνης των 83,5 MHz, το 802.11 ορίζει 11 μερικώς επικαλυπτόμενα κανάλια των 20 MHz, τα οποία απεικονίζονται στο σχήμα 2 (δύο κανάλια δεν αλληλοεπικαλύπτονται καθόλου εάν και μόνο εάν χωρίζονται από τέσσερα και πλέον κανάλια-ενδεικτικά, τα κανάλια 1, 6 και 11 δεν έχουν καθόλου επικάλυψη μεταξύ τους).[73][84][80]



Σχήμα 4-2: Κανάλια Wi-Fi 2,4 GHz [84]

Σε ότι αφορά την περιοχή των 5 GHz, έχει διατεθεί στο Wi-Fi αρκετά μεγαλύτερο εύρος συχνοτήτων (555 MHz), με αποτέλεσμα να ορίζονται περισσότερα κανάλια και να είναι αρκετά ευκολότερη η επιλογή μη επικαλυπτόμενων καναλιών, μεγαλύτερου εύρους ζώνης το οποίο επιτυγχάνει μεγαλύτερους ρυθμούς μετάδοσης. Όπως φαίνεται στο σχήμα 3, το 802.11a χρησιμοποιεί κανάλια εύρους 20 MHz, το 802.11n 20 ή 40 MHz και το 802.11ac 20 ή 40 ή 80 ή 160 MHz. Επισημαίνεται ότι ένα μέρος αυτής της περιοχής συχνοτήτων χρησιμοποιείται παράλληλα για RADAR καιρού τύπου Doppler και ως εκ τούτου δε θα πρέπει να επιλέγονται σε περίπτωση ύπαρξης συγκεκριμένου εξοπλισμού σε κοντινή απόσταση.[84][80]



Σχήμα 4-3: Κανάλια Wi-Fi 5 GHz [84]

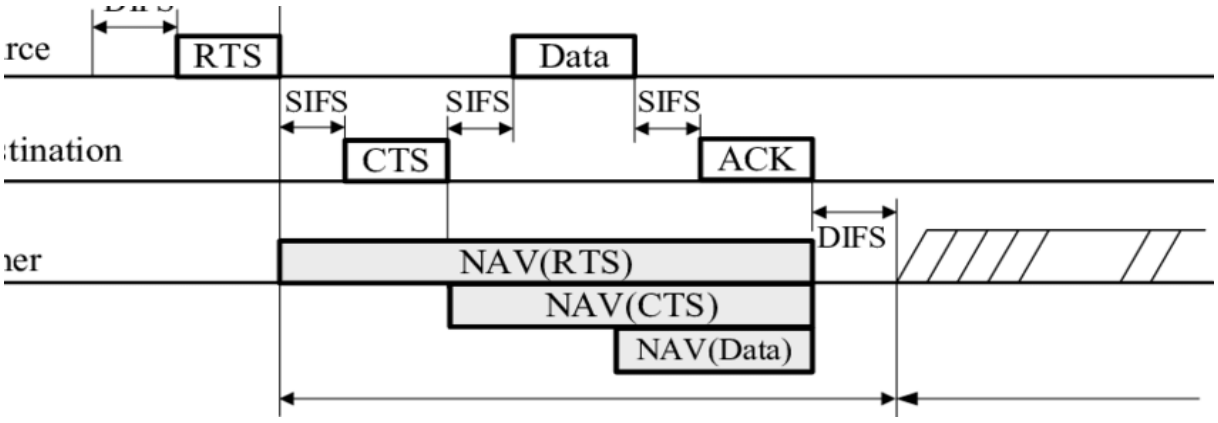
Σύνδεση σε Access Point

Έστω ότι ο ασύρματος σταθμός μας που βρίσκεται σε μια φυσική τοποθεσία λαμβάνει ένα αρκετά ισχυρό σήμα από δύο ή περισσότερα AP. Για να αποκτήσει πρόσβαση στο διαδίκτυο, θα πρέπει να ενταχθεί σε ένα υποδίκτυο κάποιου AP που σημαίνει ότι απαιτείται η ασύρματη σύνδεση του στο AP. Μετά τη σύνδεση, μόνο το συνδεδεμένο AP θα στέλνει δεδομένα στον ασύρματο σταθμό, και ο ασύρματος σταθμός θα στέλνει δεδομένα στο διαδίκτυο μόνο μέσω του συνδεδεμένου AP. Για να γίνει αυτή η μοναδική ζεύξη, τα πρότυπα 802.11 απαιτούν το AP να στέλνει περιοδικά πλαίσια beacon που περιλαμβάνουν το SSID και τη διεύθυνση MAC του AP. Ο ασύρματος σταθμός, γνωρίζοντας ότι τα AP στέλνουν πλαίσια beacon, σαρώνει όλα τα κανάλια, αναζητώντας πλαίσια από οποιαδήποτε AP που μπορεί να υπάρχουν (μερικά από τα οποία μπορεί να εκπέμπουν στο ίδιο κανάλι). Έχοντας μάθει για τα διαθέσιμα AP από τα πλαίσια beacon, υπάρχει η δυνατότητα επιλογής σύνδεσης σε ένα από τα AP. Συνήθως, η συσκευή αυτόματα επιλέγει το AP του οποίου το πλαίσιο beacon λαμβάνεται με την υψηλότερη ισχύ σήματος. Ο αλγόριθμος επιλογής του AP δεν περιλαμβάνεται στο 802.11, αλλά

υλοποιείται από τους κατασκευαστές της κάρτας δικτύου WLAN του ασύρματου σταθμού.[80]

4.1.2 Ανίχνευση Φορέα και Διάνυσμα Εκχώρησης Δικτύου (NAV)

Η μετάδοση μέσω του δικτύου Wi-Fi είναι ημι-αμφίδρομη (Half-Duplex) ως προς την κατεύθυνση, καθώς η ταυτόχρονη διάδοση από παραπάνω από έναν σταθμούς θα επιφέρει συγκρούσεις και αλλοίωση της πληροφορίας. Ως εκ τούτου, απαιτείται η χρήση τεχνικών ανίχνευσης του μέσου μετάδοσης, ώστε να διαπιστωθεί πότε είναι διαθέσιμο για μετάδοση και να μειωθούν σε αριθμό οι συγκρούσεις. Η ανίχνευση φορέα (carrier sensing) χρησιμοποιείται από το 802.11 για να διαπιστωθεί αν το μέσο είναι διαθέσιμο. Περιλαμβάνει δύο λειτουργίες ανίχνευσης φορέα: τη φυσική και την εικονική ανίχνευση. Η λειτουργία φυσικής ανίχνευσης φορέα παρέχεται από το φυσικό επίπεδο (physical layer) και εξαρτάται από τη διαμόρφωση που χρησιμοποιείται. Η εικονική ανίχνευση φορέα παρέχεται από το Διάνυσμα Εκχώρησης Δικτύου (Network Allocation Vector - NAV). Τα περισσότερα πλαίσια 802.11 φέρουν ένα πεδίο διάρκειας, το οποίο μπορεί να χρησιμοποιηθεί για τη δέσμευση του μέσου για μια σταθερή χρονική περίοδο. Το NAV είναι ένα χρονόμετρο που υποδεικνύει το χρονικό διάστημα, για το οποίο το μέσο θα είναι δεσμευμένο. Ο σταθμός που θα επικοινωνήσει παραδείγματος χάρη με ένα σημείο πρόσβασης ορίζει την τιμή του NAV στο χρόνο για τον οποίο αναμένει να χρησιμοποιήσει το μέσο, συμπεριλαμβανομένων όλων των πλαισίων που είναι απαραίτητα για την ολοκλήρωση της επικοινωνίας. Οι άλλοι σταθμοί μετρούν αντίστροφα από το NAV έως το 0. Όταν το NAV δεν είναι πλέον 0, η λειτουργία εικονικής ανίχνευσης φορέα υποδεικνύει ότι το μέσο είναι απασχολημένο και, όταν το NAV φτάσει στο 0, η λειτουργία εικονικής ανίχνευσης φέροντος υποδεικνύει ότι το μέσο είναι ελεύθερο.[73][80]



Σχήμα 4-4: Λειτουργία NAV [85]

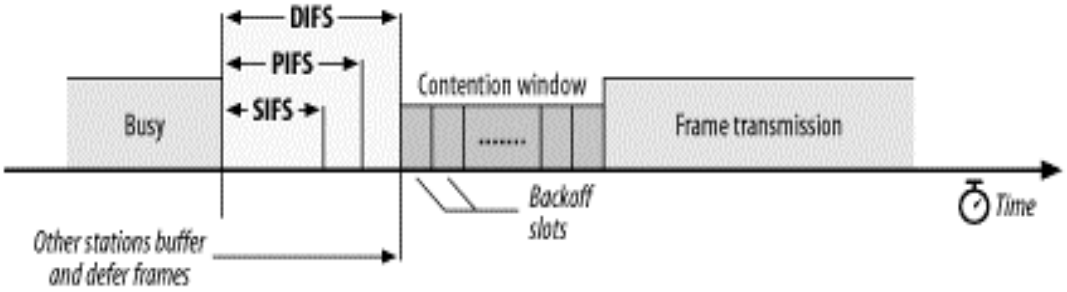
Το σχήμα 4 απεικονίζει μια τυπική ανταλλαγή πλαισίων του 802.11 (RTS και CTS, τα οποία θα αναλυθούν σε επόμενο υποκεφάλαιο). Το NAV μεταφέρεται στις επικεφαλίδες των πλαισίων RTS και CTS. Ο σταθμός Source θέτει το NAV στο πλαίσιο RTS για να εμποδίσει την πρόσβαση στο μέσο καθ όλη τη διάρκεια, απ' την αρχή της μετάδοσης του RTS ως το τέλος της μετάδοσης. Οι άλλοι σταθμοί που ακούνε το RTS αναβάλλουν την πρόσβαση στο μέσο μέχρι να το NAV να μηδενιστεί. Όπως είναι φυσικό, το πλαίσιο RTS δεν ακούγεται απαραίτητα από κάθε σταθμό του δικτύου. Επομένως, ο σταθμός destination για να εμποδίσει την πρόσβαση άλλων σταθμών στο μέσο μέχρι να ολοκληρωθεί η μετάδοση των δεδομένων περιλαμβάνει ένα μικρότερο NAV στο πλαίσιο CTS από αυτό στο πλαίσιο RTS. Τόσο μικρότερη όσο το χρονικό διάστημα του CTS και SIFS όπως φαίνεται και στο σχήμα 4. Όταν ολοκληρωθεί η ακολουθία, το μέσο μπορεί πλέον να χρησιμοποιηθεί από οποιονδήποτε σταθμό.[73][80]

4.1.3 Χρονικά Διαστήματα μεταξύ πλαισίων 802.11

Για την κατανόηση της πρόσβασης στο μέσο είναι επίσης απαραίτητος ο ορισμός των χρόνων που χρησιμοποιούνται στα πρότυπα 802.11. Οι χρόνοι αυτοί δίνουν προτεραιότητα στην μετάδοση δεδομένων ανάλογα με τη σπουδαιότητα τους, μόλις το μέσο είναι ελεύθερο. Επομένως, αν υπάρχει κίνηση υψηλής προτεραιότητας που περιμένει, χρησιμοποιεί το δίκτυο πριν τα πλαίσια χαμηλής

προτεραιότητας έχουν την ευκαιρία να προσπαθήσουν να το απασχολήσουν. Τα χρονικά διαστήματα που ορίζονται στα πρότυπα 802.11 απεικονίζονται στο σχήμα 5 και είναι τα εξής:

- **SIFS (Short Interframe Space)**. Το SIFS χρησιμοποιείται για τις μεταδόσεις υψηλότερης προτεραιότητας, όπως τα πλαίσια RTS/CTS και ACK. Οι μεταδόσεις υψηλής προτεραιότητας μπορούν να ξεκινήσουν μόλις το SIFS έχει παρέλθει. Επομένως, τα πλαίσια που μεταδίδονται μετά την παρέλευση του SIFS έχουν προτεραιότητα έναντι των πλαίσια που μπορούν να μεταδοθούν μόνο μετά τα επόμενα μεγαλύτερα χρονικά διαστήματα.
- **PIFS (PCF InterFrame Space)**. Χρησιμοποιείται από το PCF (υποκεφάλαιο 4.1.4). Οι σταθμοί με δεδομένα προς μετάδοση μπορούν να έχουν πρόσβαση στο ασύρματο μέσο μετά την πάροδο του χρονικού διαστήματος PIFS και προηγούνται της κίνησης που ρυθμίζεται από το DCF.
- **DIFS (DCF Interframe Space)**. Είναι ο ελάχιστος χρόνος αδράνειας του μέσου που χρησιμοποιείται από το DCF (υποκεφάλαιο 4.1.3). Οι σταθμοί μπορούν να έχουν άμεση πρόσβαση στο μέσο, όταν αυτό είναι ελεύθερο για χρονική περίοδο μεγαλύτερη από το DIFS.[73][80]



Σχήμα 4-5: Χρονικά Διαστήματα μεταξύ πλαισίων 802.11 [73]

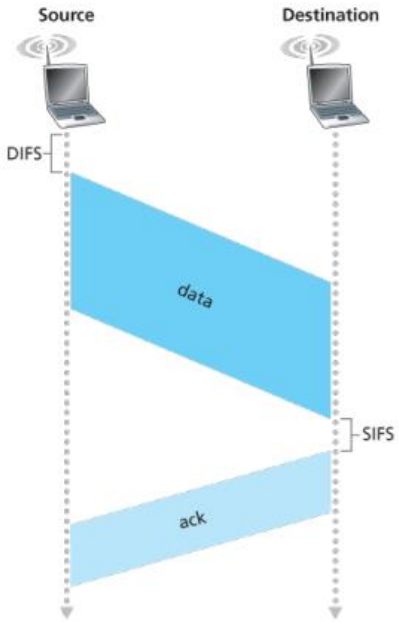
4.1.4 Κατανεμημένη Λειτουργεία Συντονισμού (DCF)

Οι σχεδιαστές του 802.11 επέλεξαν την Κατανεμημένη Λειτουργία Συντονισμού (Distributed Coordination Function - DCF) για τον έλεγχο πρόσβασης στο μέσο. Όλοι οι σταθμοί πρέπει υποστηρίζουν την DCF, είτε ο σταθμός αυτός λειτουργεί σε ad hac δίκτυο είτε σε δίκτυο με υποδομή. Η λειτουργία αυτή υποστηρίζει υπηρεσίες με ανταγωνισμό, δηλαδή κάθε σταθμός που κατέχει δεδομένα προς μετάδοση ανταγωνίζεται για πρόσβαση στον δίαυλο. Όταν τελικά στείλει τα δεδομένα ,σε περίπτωση όπου έχει και άλλα πλαίσια προς μετάδοση θα πρέπει ξεκινήσει την διαδικασία απ' την αρχή. Η διαδικασία αυτή προσφέρει δίκαια πρόσβαση στον δίαυλο για όλους τους σταθμούς. Επιπλέον η DCF χρησιμοποιεί ένα πρωτόκολλο τυχαίας πρόσβασης με ανίχνευση φέροντος που ονομάζεται **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**, δηλαδή κάθε σταθμός ανιχνεύει το κανάλι πριν από τη μετάδοση και αποφεύγει να μεταδώσει όταν το κανάλι ανιχνεύεται απασχολημένο και χρησιμοποιούνται τεχνικές αποφυγής σύγκρουσης.[73] [80]

Επειδή τα δίκτυα WLAN 802.11 δεν χρησιμοποιούν ανίχνευση συγκρούσεων (όπως στο Legace Ethernet), μόλις ένας σταθμός αρχίσει να μεταδίδει ένα πλαίσιο, αυτό αποστέλλεται ολόκληρο. Όταν ένας σταθμός σε ένα ασύρματο τοπικό δίκτυο στέλνει ένα πλαίσιο, το πλαίσιο μπορεί να μη φτάσει στο σταθμό προορισμού άθικτο για διάφορους λόγους. Για να αντιμετωπιστεί αυτή η μη αμελητέα πιθανότητα αποτυχίας, το πρωτόκολλο πρόσβασης στο φυσικό μέσο του 802.11 χρησιμοποιεί τεχνική επιβεβαίωσης σε επίπεδο datalink. Όπως φαίνεται στο σχήμα 6, όταν ο σταθμός προορισμού λάβει ένα πλαίσιο, περιμένει μια σύντομη χρονική περίοδο SIFS και στη συνέχεια στέλνει πίσω ένα πλαίσιο επιβεβαίωσης (ACK). Αν ο σταθμός εκπομπής δε λάβει το πλαίσιο επιβεβαίωσης εντός συγκεκριμένου χρονικού διαστήματος, θεωρεί ότι έχει συμβεί σφάλμα και επανεκπέμπει το πλαίσιο, χρησιμοποιώντας το πρωτόκολλο CSMA/CA για πρόσβαση στο κανάλι. Εάν δεν ληφθεί επιβεβαίωση μετά από κάποιο αριθμό επαναμεταδόσεων, ο σταθμός εκπομπής εγκαταλείπει την προσπάθεια και απορρίπτει το πλαίσιο. Ένας σταθμός (ασύρματη συσκευή ή AP) έχει ένα πλαίσιο προς μετάδοση. Η λειτουργία του

πρωτοκόλλου CSMA/CA είναι η ακόλουθη:[86][73][80]

- Όταν κάποιος σταθμός που κατέχει ένα πλαίσιο προς αποστολή και ανιχνεύσει ότι ο δίαυλος εκείνη την χρονική στιγμή είναι κατειλημμένος, περιμένει μέχρι να ελευθερωθεί.
- Όταν ο δίαυλος παύσει να είναι κατειλημμένος ο σταθμός περιμένει επιπλέον για μία περίοδο DIFS (κατά της οποίας το διάστημα αυτό ο δίαυλος παραμένει ελεύθερος) και στην συνέχεια θα στείλει
- Όταν ο δίαυλος παύσει να είναι κατειλημμένος ο σταθμός περιμένει επιπλέον για μία περίοδο DIFS (κατά της οποίας το διάστημα αυτό ο δίαυλος παραμένει ελεύθερος) και στην συνέχεια θα επιλέξει έναν τυχαίο χρόνο αναμονής (backoff).
- Μετά την απελευθέρωση του μέσου και παρέλευση περιόδου DIFS, οι σταθμοί θα μειώσουν τον μετρητή αναμονής μέχρι το μέσο να καταληφθεί ξανά , είτε ο μετρητής να μηδενιστεί.
- Ο σταθμός θα σταματήσει τον μετρητή του όταν το μέσο καταληφθεί.
- Όταν ο μετρητής μηδενιστεί τότε ο σταθμός θα μεταδώσει και στη συνέχεια θα περιμένει μια επιβεβαίωση. Αν ληφθεί επιβεβαίωση, ο μεταδίδων σταθμός γνωρίζει ότι το πλαίσιό του έχει ληφθεί σωστά από τον σταθμό προορισμού. Αν ο σταθμός έχει άλλο πλαίσιο για αποστολή, ξεκινά την διαδικασία από την αρχή. Αν δεν ληφθεί επιβεβαίωση, ο μεταδίδων σταθμός εισέρχεται ξανά στη φάση υποχώρησης, με την τυχαία τιμή να επιλέγεται μεγαλύτερη (το οποίο αναλύεται πιο κάτω).
- Σε ορισμένες περιπτώσεις υπάρχει η πιθανότητα ο μετρητής να μηδενιστεί την ίδια χρονική στιγμή σε δύο ή περισσότερους σταθμούς. Στην περίπτωση αυτή θα δημιουργηθεί σύγκρουση και οι εμπλεκόμενοι σταθμοί θα πρέπει να παράξουν έναν νέο χρόνο αναμονής.[73]

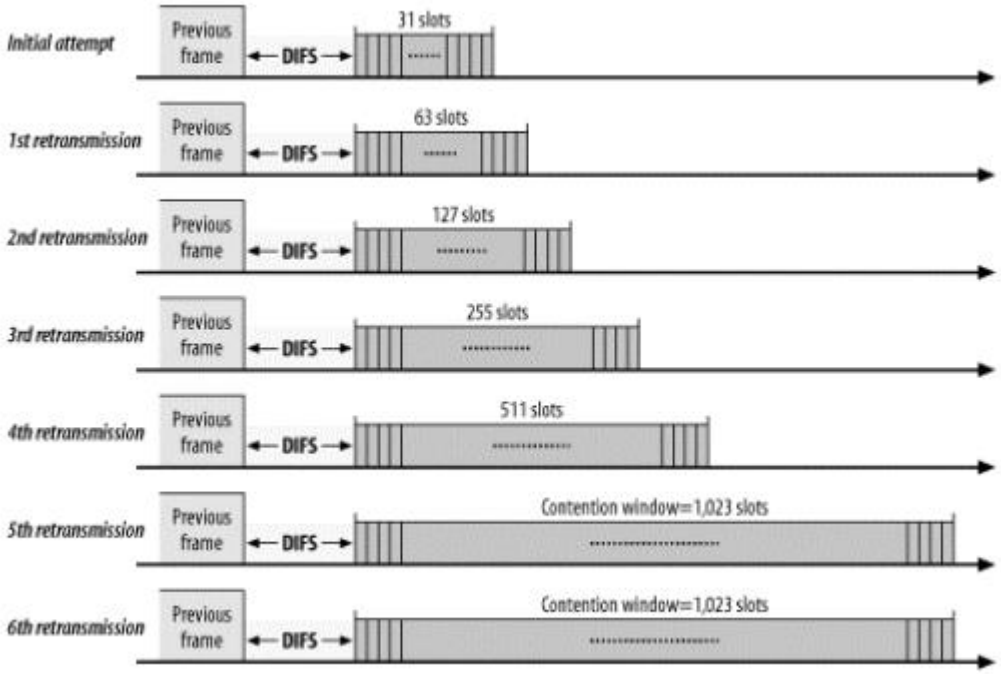


Σχήμα 4-6: Επιβεβαίωση (ACK) σε επίπεδο datalink [80]

Backoff

Αφού η μετάδοση του πλαισίου ολοκληρωθεί και περάσει ο χρόνος DIFS, οι σταθμοί μπορούν να επιχειρήσουν να μεταφέρουν δεδομένα. Ακολουθεί ένα διάστημα που ονομάζεται backoff window (παράθυρο ανταγωνισμού ή οπισθοχώρισης). Το παράθυρο αυτό είναι χωρισμένο σε χρονοσχισμές, Οι σταθμοί διαλέγουν τυχαία μια χρονισχισμή και περιμένουν για αυτό το χρονικό διάστημα πριν προσπαθήσουν να αποκτήσουν ξανά πρόσβαση στο μέσο επικοινωνίας. Όλες οι χρονοσχισμές επιλέγονται με την ίδια πιθανότητα. Ο αριθμός των χρονοσχισμών είναι πάντα μία δύναμη του δύο μείον ένα, όπως φαίνεται στο *σχήμα* 7 (πχ 31, 63, 127 κλπ.). Αυτό συμβαίνει διότι μετριέται και το 0, δηλαδή στην περίπτωση που επιλέξει το 31 στην πραγματικότητα έχει 32

χρονοσχιμές επειδή περιλαμβάνεται και το 0 σε αυτό Σε περιπτώσεις όπου πολλοί σταθμοί επιχειρούν να μεταδώσουν, ο σταθμός που επιλέγει τη χρονοσχισμή με το μικρότερο νούμερο είναι αυτός που κερδίζει την πρόσβαση στο μέσο. Κάθε φορά που μια μετάδοση αποτυγχάνει, το μέγεθος του παραθύρου οπισθοχώρησης διπλασιάζεται (μέχρι να φτάσει στο μέγιστο) με αποτέλεσμα οι σταθμοί που δεν τους στάλθηκε ACK από τον παραλήπτη, να επιλέξουν τυχαία από μεγαλύτερο εύρος χρονοσχισμών και να μειώνεται η πιθανότητα σύγκρουσης, όπως φαίνεται και στο παρακάτω *σχήμα* 7. [73]



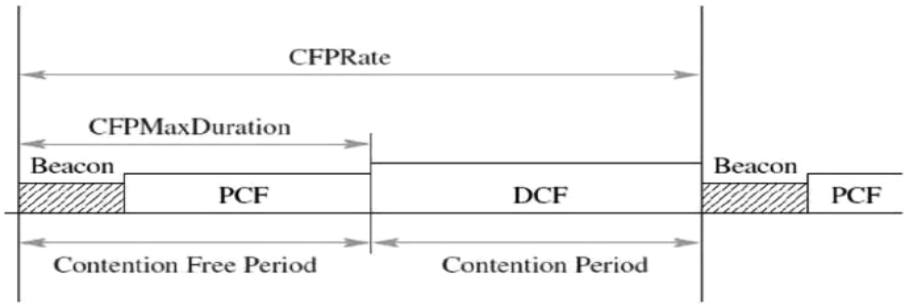
Σχήμα 4-7: Backoff time [73]

Οι αριθμοί στο σχήμα 7 αναφέρονται για το τη μορφή διαμόρφωσης του φυσικού επιπέδου direct-sequence spread-spectrum (DSSS). Διαφορετικές διαμορφώσεις χρησιμοποιούν διαφορετικά μεγέθη παραθύρου οπισθοχώρησης και χρονοσχισμών, αλλά η αρχή είναι ίδια. Κάθε φορά που ο μετρητής επανάληψης αυξάνεται, το μέγεθος του παραθύρου ανταγωνισμού μετακινείται στην επόμενη μεγαλύτερη δύναμη του δύο μέχρι να φτάσει στο μέγιστο όπως φαίνεται στο παραπάνω σχήμα 7. Το μέγεθος του παραθύρου ανταγωνισμού περιορίζεται από τη διαμόρφωση του φυσικού επιπέδου. Το παράθυρο επανέρχεται στο αρχικό μέγεθος του μετά την επιτυχή μετάδοση των πλαισίων ή όταν ο μετρητής επανάληψης φτάσει το όριο του (1,023 slots) και το πλαίσιο απορρίπτεται.[73]

4.1.5 Λειτουργία Σημείου Συντονισμού (PCF)

Η Λειτουργία Σημείου Συντονισμού (Point Coordination Function - PCF) είναι ένα ακόμα πρωτόκολλο που περιλαμβάνεται στα πρότυπα 802.11. Το πρωτόκολλο αυτό παρέχει τη δυνατότητα για μια διαφορετική προσέγγιση στην πρόσβαση στο ασύρματο μέσο σε σχέση με το DCF. Το PCF παρέχει μια διαδικασία πρόσβασης στο μέσο χωρίς ανταγωνισμό (contention-free access) για συγκεκριμένα χρονικά διαστήματα. Αυτό επιτυγχάνεται με την ανάθεση της πρόσβασης στο μέσο σε ένα AP, το οποίο λειτουργεί ως σημείο συντονισμού. Το PCF επιτρέπει στο AP να διαχειρίζεται τη ροή των δεδομένων στο ασύρματο δίκτυο. Οι σταθμοί μπορούν να μεταδίδουν δεδομένα μόνο όταν τους επιτρέπεται από το AP - συντονιστής. Κατά κάποιο τρόπο, η πρόσβαση στο ασύρματο μέσο, στο πλαίσιο του PCF μοιάζει με token-based πρωτόκολλα δικτύωσης, με το AP - συντονιστής να παίρνει τη θέση του token. Οι οδηγίες από το AP προς στους σταθμούς σχετικά με το πότε μπορούν να μεταδώσουν τα δεδομένα τους

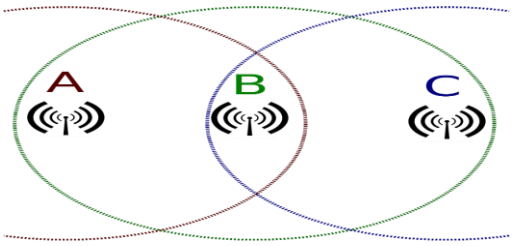
δίνονται με την αποστολή πλαισίων ελέγχου. Όταν χρησιμοποιείται το PCF, ο χρόνος στο μέσο χωρίζεται σε δύο περιόδους: την Contention Free Period (CFP) και την Contention Period. Η πρόσβαση στο μέσο στην πρώτη περίπτωση ελέγχεται από το PCF, ενώ η πρόσβαση στο μέσο στην δεύτερη περίπτωση ελέγχεται από το DCF. Οι προαναφερθείσες περίοδοι εναλάσσονται περιοδικά, όπως φαίνεται στο σχήμα 8.[86][73] [80]



Σχήμα 4-8: Αλληλουχία γεγονότων πρόσβασης στο ασύρματο δίκτυο με λειτουργίες PCF & DCF [87]

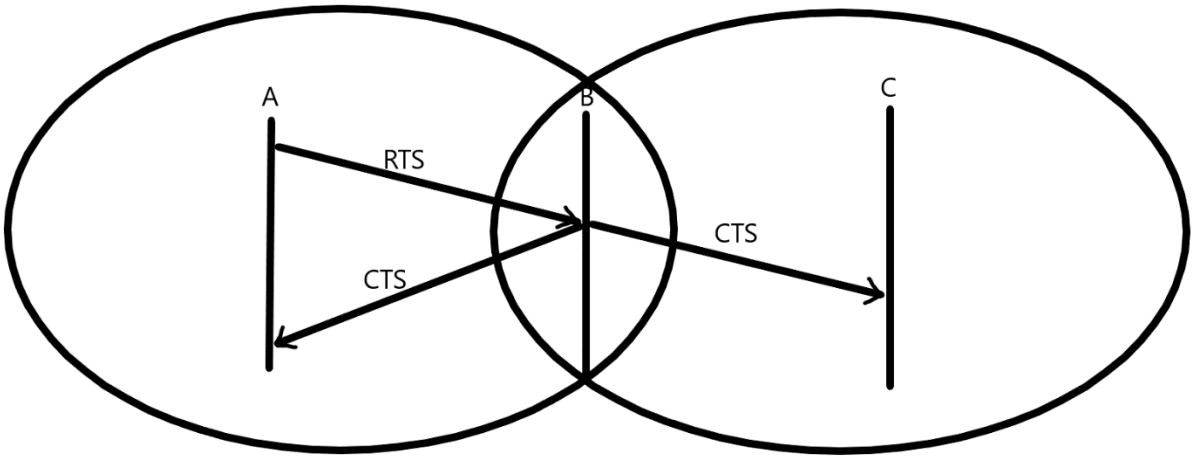
4.1.6 Κρυφοί Κόμβοι

Το πρόβλημα των κρυφών κόμβων παρουσιάζεται στο σχήμα 8 παρακάτω. Ο κόμβος Α μπορεί να επικοινωνήσει μόνο με τον κόμβο Β, ενώ ο κόμβος C μπορεί να επικοινωνήσει μόνο με τον κόμβο Β. Αντίστοιχα, ο κόμβος Β μπορεί να επικοινωνήσει τόσο με τον Α όσο και με τον C. Το πρόβλημα των κρυφών κόμβων προκύπτει όταν οι κόμβοι Α και C εκτελούν ταυτόχρονη μετάδοση προς τον κόμβο Β. Αυτό οδηγεί σε σύγκρουση δεδομένων στον κόμβο Β και συνεπώς σε απώλεια δεδομένων που προέρχονται από τους κόμβους Α και C. Πιο συγκεκριμένα, ο κόμβος Α ξεκινά να στέλνει δεδομένα στον κόμβο Β. Ο κόμβος C δεν λαμβάνει αυτή τη μετάδοση επειδή είναι εκτός της εμβέλειας του Α. Σε κάποια άλλη χρονική στιγμή, ο κόμβος C ξεκινά την αποστολή δεδομένων στον κόμβο Β καθώς θεωρεί ότι ο κανάλι είναι ελεύθερο, περιμένοντας μόνο το χρονικό διάστημα DIFS. Έτσι, ο κόμβος C ξεκινάει επίσης τη μετάδοση προς τον κόμβο Β όπου τα δεδομένα συγκρούονται.



Σχήμα 4-9: Το πρόβλημα των κρυφών κόμβων [88]

Για την αποφυγή αυτού του προβλήματος, η σειρά προτύπων 802.11 χρησιμοποιεί τα σύντομα πλαίσια ελέγχου Request To Send (RTS) και Clear To Send (CTS) για να διαχειριστεί την πρόσβαση στο κανάλι, όπως φαίνεται στο σχήμα 10. Όταν ένας αποστολέας θέλει να στείλει δεδομένα, μπορεί πρώτα να στείλει ένα πλαίσιο RTS στον παραλήπτη (η περιγραφόμενη διαδικασία είναι προαιρετική σύμφωνα με τη σειρά προτύπων 802.11), υποδεικνύοντας το συνολικό χρόνο που απαιτείται για τη μετάδοση του πλαισίου RTS, CTS, DATA και του ACK. Όταν ο παραλήπτης λάβει το πλαίσιο RTS, απαντά με μετάδοση ενός πλαισίου CTS. Αυτό το πλαίσιο CTS εξυπηρετεί δύο σκοπούς. Αφενός δίνει στον αποστολέα ρητή άδεια να ξεκινήσει την αποστολή, αφετέρου, δίνει οδηγίες στους άλλους σταθμούς να μη στείλουν δεδομένα για την κατειλημμένη από τον πρώτο αποστολέα διάρκεια. Όσοι κόμβοι δε λαμβάνουν το CTS επειδή δεν βρίσκονται εντός της εμβέλειας του παραλήπτη , άλλα βλέπουν το RTS επειδή βρίσκονται εντός της εμβέλειας του αποστολέα, διαπιστώνουν ότι δεν μπορούν να μεταδώσουν δεδομένα.[89]

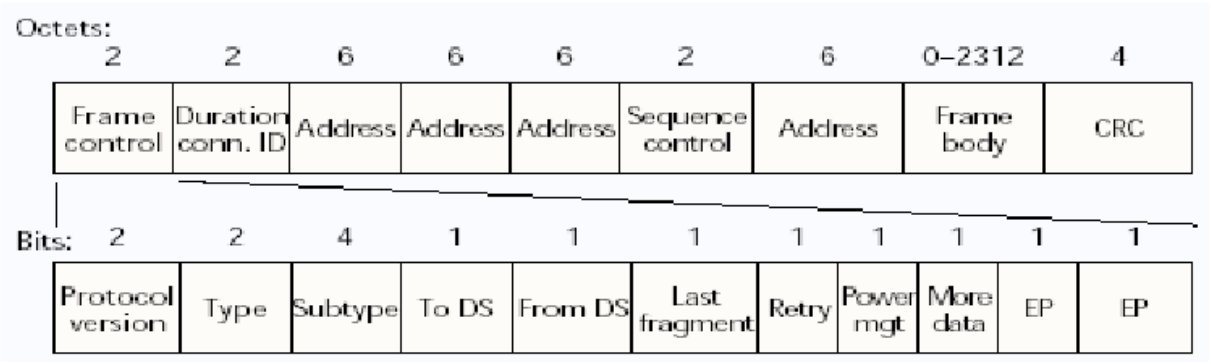


Σχήμα 4-10: Ανταλλαγή πλαισίων CTS & RTS για την αποφυγή προβλήματος κρυφών κόμβων

Αν και η ανταλλαγή των RTS και CTS συμβάλλει στην αντιμετώπιση έως έναν βαθμό του των συγκρούσεων των δεδομένων, εισάγει επίσης καθυστέρηση και καταναλώνει πόρους από το ασύρματο μέσο. Για το λόγο αυτό, η ανταλλαγή RTS και CTS χρησιμοποιείται (προεραιτικά) μόνο για να δεσμεύσει το κανάλι για τη μετάδοση ενός μεγάλου πλαισίου δεδομένων επειδή σε αυτήν την περίπτωση η σύγκρουση θα ήταν πολύ πιο μεγάλη. Στην πράξη, κάθε ασύρματος σταθμός μπορεί να ορίσει ένα κατώφλι RTS έτσι ώστε η διαδικάσία RTS/CTS να χρησιμοποιείται μόνο όταν το πλαίσιο είναι μεγαλύτερο από το κατώφλι αυτό. [90][91]

4.1.7 Πλαίσιο 802.11

Το πλαίσιο (frame) 802.11 φαίνεται στο σχήμα 11. Οι αριθμοί πάνω από κάθε ένα από τα πεδία στο πλαίσιο αντιπροσωπεύουν τα μήκη των πεδίων σε bytes. Οι αριθμοί πάνω από κάθε ένα από τα υποπεδία πλαισίου αντιπροσωπεύουν τα μήκη των υποπεδίων σε bits. Τα σημαντικότερα πεδία του πλαισίου 802.11 είναι τα ακόλουθα:



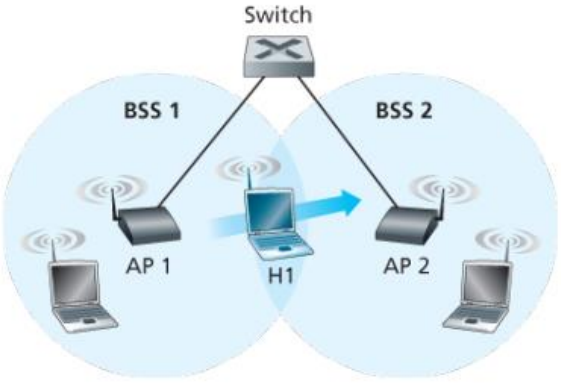
Σχήμα 4-11: Δομή πλαισίου 802.11[92]

- Το πεδίο *Payload* περιέχει συνήθως ένα πακέτο δεδομένων IP. Παρόλο που το πεδίο επιτρέπεται να έχει μήκος έως 2.312 bytes, συνήθως έχει μήκος μικρότερο από 1.500 bytes,.
- Το πεδίο *Cyclic Redundancy Check (CRC)* μήκους 32-bit. Με τη χρήση αυτού του πεδίου ο δέκτης να μπορεί να εντοπίζει σφάλματα bit στο ληφθέν πλαίσιο. Όπως είναι λογικό, τα σφάλματα bit είναι πολύ πιο συνηθισμένα στα δίκτυα WLAN σε σύγκριση με τα δίκτυα LAN.

- Ένα πλαίσιο 802.11 διαθέτει τέσσερα πεδία διευθύνσεων, καθένα από τα οποία μπορεί να περιέχει μια διεύθυνση MAC μήκους 6 bytes. Η Address 1 είναι η διεύθυνση MAC του ασύρματου σταθμού που πρόκειται να λάβει το πλαίσιο. Η Address 2 είναι η διεύθυνση MAC του σταθμού που μεταδίδει το πλαίσιο. Η Address 3 περιέχει τη διεύθυνση MAC της διεπαφής του δρομολογητή μέσω του οποίου δρομολογήθηκε το πλαίσιο προερχόμενο από το διαδίκτυο (ή προς τον οποίο θα δρομολογηθεί για να φτάσει στο διαδίκτυο). Η Address 4 χρησιμοποιείται μόνο όταν τα AP προωθούν πλαίσια απευθείας μεταξύ τους (λειτουργία ad hoc).
- Το πεδίο *Sequence Number* επιτρέπει στο δέκτη να διακρίνει ένα πρόσφατα μεταδιδόμενο πλαίσιο από ένα προηγούμενο πλαίσιο στην περίπτωση που ο σταθμός αποστολής έχει στείλει πολλαπλά αντίγραφα ενός συγκεκριμένου πλαισίου.
- Το πεδίο *Duration* δείχνει την τιμή της χρονικής διάρκειας κατά την οποία ένας σταθμός έχει δεσμεύσει το κανάλι (περιλαμβάνεται ο χρόνος για τη μετάδοση του πλαισίου δεδομένων του και ο χρόνος για τη μετάδοση μιας επιβεβαίωσης).
- Το πεδίο *Frame control* περιλαμβάνονται πολλά υποπεδία ελέγχου, με σημαντικότερα υποπεδία τα *Type* και *Subtype* που χρησιμοποιούνται για τη διάκριση του τύπου των πλαισίων (beacon, RTS, CTS, ACK και δεδομένων). [80]

4.1.8 Κινητικότητα στο ίδιο υποδίκτυο

Προκειμένου να αυξήσουν τη φυσική εμβέλεια ενός ασύρματου τοπικού δικτύου, οι εταιρείες και τα πανεπιστήμια συχνά εγκαθιστούν πολλαπλά BSS. Αυτό εγείρει φυσικά το ζήτημα της κινητικότητας μεταξύ των BSSs. Η κινητικότητα μπορεί να αντιμετωπιστεί με σχετικά απλό τρόπο όταν τα BSS είναι μέρος του ίδιου υποδικτύου IP. Όταν οι σταθμοί μετακινούνται μεταξύ διαφορετικών υποδικτύων, απαιτούνται πιο περίπλοκα πρωτόκολλα διαχείρισης κινητικότητας. Η εικόνα 12 δείχνει δύο διασυνδεδεμένα BSS με ένα switch και έναν υπολογιστή H1, ο οποίος μμετακινείται από το BSS1 στο BSS2. Όλοι οι σταθμοί στα δύο BSS, συμπεριλαμβανομένων των AP, ανήκουν στο ίδιο υποδίκτυο IP. Έτσι, όταν ο H1 μετακινείται από το BSS1 στο BSS2, μπορεί να διατηρήσει τη διεύθυνση IP του. Καθώς ο H1 απομακρύνεται από το AP1, ο H1 ανιχνεύει ένα εξασθενημένο σήμα από το AP1 και αρχίζει να αναζητά ένα ισχυρότερο σήμα. Ο H1 λαμβάνει πλαίσια beacon από το AP2 (το οποίο πολλές φορές έχει το ίδιο SSID με το AP1). Στη συνέχεια, ο H1 αποσυνδέεται από το AP1 και συνδέεται με το AP2, διατηρώντας τη σύνδεση στο διαδίκτυο.[80]



Σχήμα 4-12: Κινητικότητα στο ίδιο υποδίκτυο [93]

4.2 Bluetooth (IEEE 802.15.1)

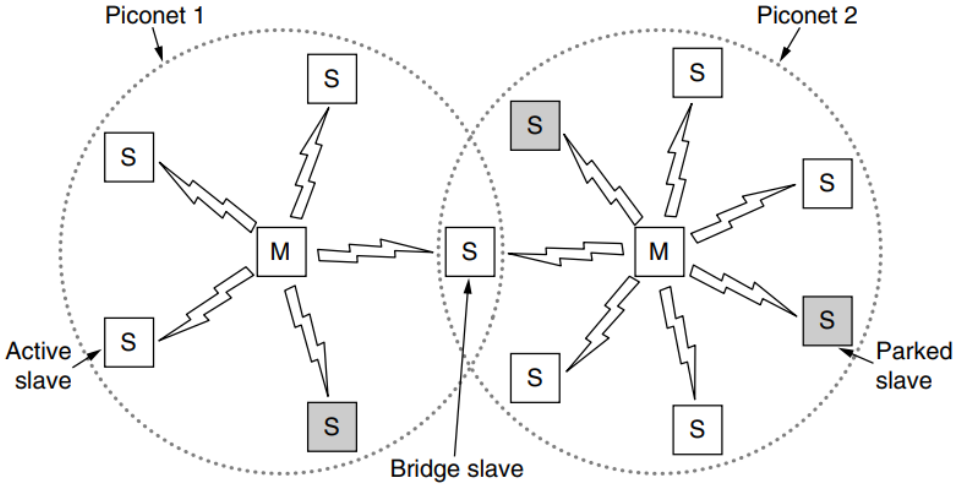
Η τεχνολογία Bluetooth ορίζεται με το πρότυπο IEEE 802.15.1. Το Bluetooth είναι τεχνολογία χαμηλής ισχύος, μικρής εμβέλειας και χαμηλού ρυθμού μετάδοσης σε σχέση με το WiFi και χρησιμοποιείται ουσιαστικά ως μια ασύρματη τεχνολογία "αντικατάστασης καλωδίων" για τη διασύνδεση ενός υπολογιστή με τις περιφερειακές του συσκευές (πληκτρολόγιο, ποντίκι κλπ) ή των κινητών τηλεφώνων με συσκευές φωνής και ήχου καθώς και για διασύνδεση μεταξύ άλλων κινητών συσκευών (εκτυπωτές, ρολόγια, gps κλπ). Το Bluetooth επιτρέπει σε αυτές τις συσκευές να διασυνδεθούν μεταξύ τους, με μια διαδικασία που ονομάζεται σύξευξη (pairing) και να μεταφέρουν δεδομένα με ασφάλεια. Υπάρχουν αρκετές εκδόσεις του πρωτοκόλλου και παρακάτω θα γίνει μία σύντομη αναφορά σε αυτές:Η αρχική έκδοση του Bluetooth (Bluetooth 1 (1999)) παρείχε βασική συνδεσιμότητα για φωνή και δεδομένα. Ακολούθησε η έκδοση Bluetooth 1.1, η οποία περιελάμβανε κυρίως βελτιώσεις ως προς την διόρθωση των σφαλμάτων της μετάδοσης. Το 2003, το Bluetooth 1.2 πρόσθεσε την τεχνολογία προσαρμοστικής αλλαγής συχνοτήτων, αποφεύγοντας κανάλια που εντοπίζονταν παρεμβολές. Στη συνέχεια, το 2005, η δεύτερη έκδοση πρόσθεσε περαιτέρω λειτουργίες όπως τον ενισχυμένο ρυθμό δεδομένων (Enhanced Data Rate - EDR) όπου αύξησε την ταχύτητα εώς 2.1 Mbps, ενώ έκανε ευκολότερο το pairing των συσκευών, χωρίς να απαιτείται η χρήση κωδικών.
Η έκδοση Bluetooth 3, το 2009 αύξησε σημαντικά την απόδοση του πρωτοκόλλου εισάγοντας μια νέα προαιρετική πρόσθετη λειτουργία μεταφοράς δεδομένων υψηλών ρυθμών μετάδοσης έως και 24 Mbps με το όνομα "Bluetooth + HS", η οποία όμως δεν εφαρμόστηκε ποτέ ευρέως - αν και υποστηρίζεται επίσημα ακόμη και σήμερα. Η τέταρτη έκδοση του Bluetooth, το 2010, έφερε τη σημαντικότερη αναβάθμιση, καθώς εισήγαγε μια νέα "χαμηλής κατανάλωσης" λειτουργία γνωστή ως Bluetooth LE (Low Energy), περιορίζοντας όμως τους ρυθμούς μετάδοσης σε μικρότερους του 1 Mbps. Με τη χρήση αυτής της τεχνολογίας στις συμβατικές οικιακές συσκευές (ποντίκια, πληκτρολόγια) μειώθηκε σημαντικά η κατανάλωση ενέργειας, απαλλάσσοντας τους χρήστες από τη συχνή αλλαγή μπαταριών. Επίσης το 2013 έγινε εφικτή η συνδυαστική χρήση του Bluetooth με το IPv6 (με ενσωμάτωση Bluetooth στα router ή με τη χρήση ξεχωριστού hub) με σκοπό να επιτρέψει στις συσκευές Internet of Things (IoT) οι οποίες χρησιμοποιούν παράλληλα την τεχνολογία Bluetooth, να μεταφέρουν δεδομένα μέσω του διαδικτύου. Το 2016, η πέμπτη έκδοση αναβάθμισε τις επιδόσεις του Bluetooth LE, επιτρέποντας ταχύτητες μετάδοσης δεδομένων έως και 2 Mbps, διατηρώντας τη χαμηλή κατανάλωση ενέργειας, Το 2019, η έκδοση Bluetooth 5.1 εστίασε στην αύξηση της εμβέλειας, με μια νέα λειτουργία σύνδεσης πλέγματος που επιτρέπει συνδέσεις multi-hop μέσω αναμετάδοσης μηνυμάτων από κόμβο σε κόμβο. Προστέθηκε επίσης μια νέα λειτουργία εντοπισμού της γωνίας άφιξης του σήματος, η οποία επιτρέπει στις συσκευές Bluetooth να ανιχνεύουν την κατεύθυνση των εισερχόμενων σημάτων και ως εκ τούτου, να εκτελούν βασικό εντοπισμό της θέσης της συζευγμένης συσκευής. Η έκδοση 5.2 του Bluetooth, που εκδόθηκε το ίδιο έτος, παρείχε μια σημαντική αναβάθμιση, εισάγοντας το νέο προφίλ LE Audio που υπόσχεται ροή ήχου υψηλότερης ποιότητας και υψηλότερου ρυθμού μετάδοσης με μικρότερη κατανάλωση ενέργειας. Το LE Audio περιλαμβάνει επίσης το πρωτόκολλο Auracast, το οποίο επιτρέπει σε μια πηγή ήχου Bluetooth να μεταδίδει σε απεριόριστο αριθμό ακουστικών ή ηχείων. Τέλος, η τελευταία έκδοση 5.3 το 2021 επιτρέπει την ταχύτερη μετάβαση μεταξύ των λειτουργιών αναμονής και ενεργοποίησης. Με αυτόν τον τρόπο, οι συσκευές Bluetooth μπορούν να πηγαίνουν σε κατάσταση αναμονής όταν δεν χρησιμοποιούνται και να ενεργοποιούνται σε ελάχιστο χρονικό διάστημα όταν απαιτείται.Στον παρακάτω πίνακα απεικονίζονται οι εκδόσεις Bluetooth και ο μέγιστος ρυθμός μετάδοσης που υποστηρίζει η καθεμία.[94]

Bluetooth Version	Maximum transmission rate
Bluetooth 1.0a and 1.0b	732.2 kbps
Bluetooth 1.1	732.2 kbps
Bluetooth 1.2	1 Mbps
Bluetooth 2.0 and 2.1	2.1 Mbps
Bluetooth 3.0	24 Mbps
Bluetooth 4.0	24 Mbps
Bluetooth 4.1 and 4.2	25 Mbps
Bluetooth 5.0, 5.1, and 5.2	50 Mbps

Πίνακας 2: Εκδόσεις Bluetooth και μέγιστος υποστηριζόμενος ρυθμός μετάδοσης [95]

4.2.1 Αρχιτεκτονική Δικτύου Bluetooth

Τα δίκτυα 802.15.1 είναι δίκτυα ad hoc (κατ'απαίτηση): Δεν απαιτείται σταθερή υποδομή δικτύου (π.χ. σημείο πρόσβασης) για τη διασύνδεση συσκευών μέσω Bluetooth. Έτσι, οι συσκευές που πρόκειται να συνδεθούν μεταξύ τους οργανώνονται μόνες τους και δημιουργούν έναν τύπο μικρού δικτύου που ονομάζεται piconet, στο οποίο μπορούν να ανήκουν μέχρι οκτώ ενεργές συσκευές, όπως φαίνεται στο σχήμα 13. Περισσότερα piconet μπορούν να βρίσκονται στο ίδιο δωμάτιο και να επικοινωνούν μεταξύ τους μέσω ενός κόμβου-γέφυρας (bridge node) ο οποίος θα συμμετέχει σε περισσότερα του ενός piconets. Το σύνολο των διασυνδεδεμένων piconets ονομάζεται scatternet.

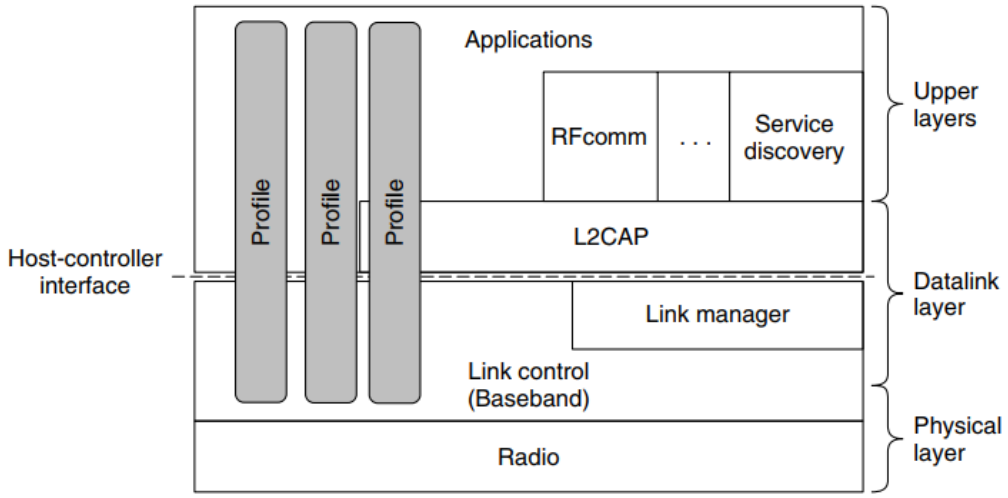


Σχήμα 4-13: Bluetooth scatternet [94]

Μία από τις συσκευές κάθε piconet ορίζεται ως master κόμβος, με τις υπόλοιπες συσκευές να λειτουργούν ως slaves. Ο κόμβος που έχει το ρόλο του master έχει καθοριστικό ρόλο στο piconet καθώς το δικό του ρολόι ρυθμίζει το χρονισμό εντός του δικτύου, ο ίδιος μπορεί να εκπέμψει σε κάθε χρονοθυρίδα με περιττό αριθμό, ενώ ένας slave κόμβος μπορεί να εκπέμψει μόνο αφού ο master έχει επικοινωνήσει μαζί του στο προηγούμενο slot και μπορεί να στείλει πληροφορία μόνο στον master. Εκτός από τους κόμβους που έχουν το ρόλο του slave, μπορούν επίσης να υπάρχουν έως και 255 αδρανείς (parked) συσκευές στο δίκτυο. Αυτές οι συσκευές βρίσκονται σε κατάσταση χαμηλότερης κατανάλωσης ενέργειας για εξοικονόμηση μπαταρίας και δεν μπορούν να επικοινωνήσουν μέχρι να αλλάξει η κατάστασή τους από parked σε ενεργή από τον master.[94]

4.2.2 Στοίβα Πρωτοκόλλων Bluetooth

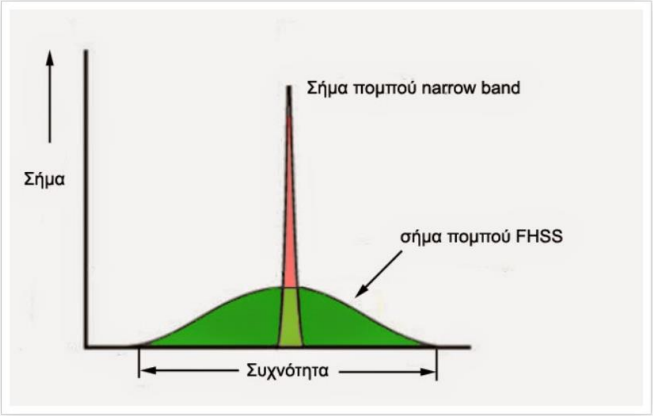
Η τεχνολογία Bluetooth υποστηρίζει πλήθος διαφορετικών εφαρμογών, κάθε μία αντιστοιχεί σε διαφορετικό προφίλ (profiles) και για κάθε προφίλ υπάρχουν διαφοροποιήσεις στην στοίβα πρωτοκόλλων. Ενδεικτικά αναφέρεται το προφίλ intercom που επιτρέπει τη σύνδεση δύο κινητών τηλεφώνων μεταξύ τους, τα προφίλ "headset" και "hands-free" που επιτρέπουν τη σύνδεση ασύρματων ακουστικών σε τηλέφωνο ενώ άλλα προφίλ υποστηρίζουν τη μετάδοση ήχου και βίντεο από κινητή συσκευή σε τηλεόραση. Το προφίλ "human interface device" επιτρέπει τη σύνδεση περιφερειακών συσκευών σε υπολογιστή ενώ άλλα προφίλ υποστηρίζουν υπηρεσίες δικτύωσης όπως το προφίλ "dial-up networking". Η στοίβα πρωτοκόλλων του Bluetooth είναι χωρισμένη στα επίπεδα που φαίνονται στο σχήμα 14 και αναλύονται παρακάτω, όχι με αυστηρό τρόπο, δηλαδή υπάρχει επικάλυψη μεταξύ των επιπέδων για τα διάφορα προφίλ. Η δομή δεν ακολουθεί κάποιο από τα γνωστά μοντέλα (OSI, TCP/IP κλπ) αλλά υπάρχουν ομοιότητες με κάποια από τα επίπεδα του μοντέλου OSI. Όπως και στα υπόλοιπα μοντέλα έτσι και εδώ ισχύει η αρχή ότι κάθε επίπεδο παρέχει υπηρεσίες στο από πάνω επίπεδο και δέχεται υπηρεσίες από το από κάτω επίπεδο.[94]



Σχήμα 4-14: Στοίβα πρωτοκόλλων Bluetooth [94]

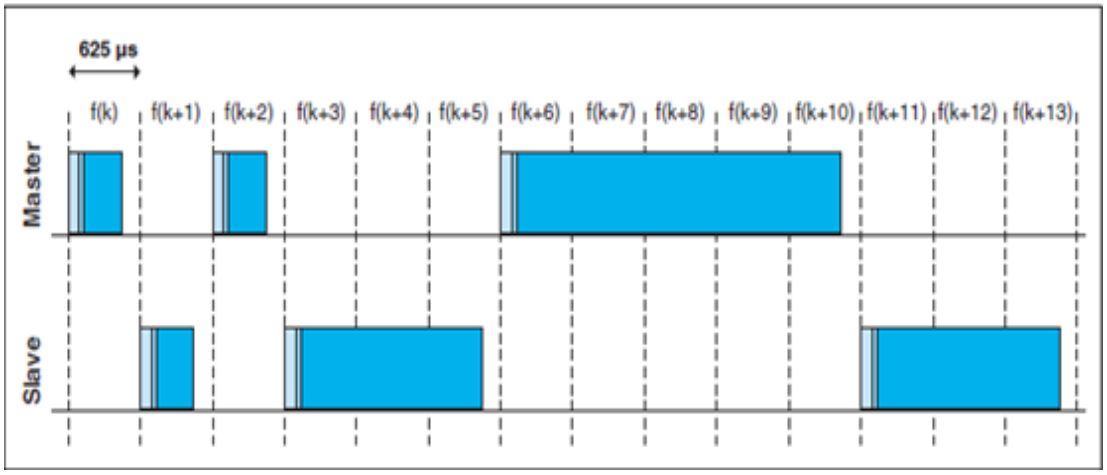
Το κατώτερο επίπεδο Radio layer, αντιστοιχεί σε μεγάλο βαθμό με το φυσικό επίπεδο του μοντέλου OSI. Ασχολείται με ζητήματα διαμόρφωσης του σήματος και μετάδοσης. Το επίπεδο link control ή baseband είναι ανάλογο του MAC sublayer (υποεπίπεδο του datalink layer), αλλά περιλαμβάνει και κάποια στοιχεία του φυσικού επιπέδου. Ανάμεσα στα άλλα, ορίζει πώς ο master κόμβος ελέγχει και κατανέμει τις χρονοθυρίδες και πώς αυτές ομαδοποιούνται σε πλαίσια (frames). Τα επόμενα δύο επίπεδα χρησιμοποιούν τις υπηρεσίες του επιπέδου link control. Αρχικά το επίπεδο link manager είναι υπεύθυνο για τη δημιουργία λογικών καναλιών μεταξύ των συσκευών που πρόκειται να επικοινωνήσουν, ελέγχει τη σύζευξη τους (pairning) καθώς και την κωδικοποίηση των μεταδιδόμενων πληροφοριών, τον έλεγχο της ισχύος και την ποιότητα της υπηρεσίας (Quality of Service - QoS). Όπως φαίνεται στο ανωτέρω σχήμα, το πρωτόκολλο αυτό βρίσκεται ακριβώς κάτω από τη διακεκομμένη γραμμή η οποία διαχωρίζει ποια πρωτόκολλα και υπηρεσίες εκτελούνται στο Bluetooth chip (πρωτόκολλα κάτω από τη γραμμή) και ποια στη συσκευή που περιέχει το chip (πρωτόκολλα πάνω από τη γραμμή). Το επίπεδο που βρίσκεται ακριβώς από πάνω από τη διακεκομμένη γραμμή ονομάζεται L2CAP (Logical Control Adaptation Protocol) και είναι υπεύθυνο για την τοποθέτηση των δεδομένων σε πλαίσια (frames). Οι υπηρεσίες αυτού του επιπέδου χρησιμοποιούνται από αρκετά πρωτόκολλα εφαρμογών, όπως ενδεικτικά το service discovery protocol, που χρησιμοποιείται για τον εντοπισμό υπηρεσιών εντός του δικτύου και το RFcomm (Radio Frequency communication) protocol, το οποίο προσομοιώνει τη σειριακή θύρα για σύνδεση περιφερειακών συσκευών. Στο ανώτερο επίπεδο της στοίβας βρίσκονται οι εφαρμογές. Κάθε προφίλ παρουσιάζεται στη στοίβα σαν ένα κάθετο πλαίσιο, δεδομένου ότι χρησιμοποιεί μόνο τα πρωτόκολλα από κάθε επίπεδο που απαιτούνται για το

συγκεκριμένο προφίλ. Το κατώτερο επίπεδο της στοίβας πρωτοκόλλων Bluetooth, το **radio layer** είναι υπεύθυνο για τη μεταφορά των bits μεταξύ των κόμβων master και slave. Πρόκειται για σύστημα χαμηλής ισχύος που λειτουργεί στην περιοχή συχνοτήτων των 2.4 GHz, ίδια περιοχή με το 802.11 και με εμβέλεια μέχρι 10 μέτρα. Η μπάντα συχνοτήτων χωρίζεται σε 79 κανάλια, εύρους ζώνης 1 MHz το καθένα. Για την αποφυγή παρεμβολών με άλλα δίκτυα που χρησιμοποιούν την ίδια περιοχή συχνοτήτων χρησιμοποιείται η τεχνολογία διασπορά φάσματος με εναλλαγή συχνοτήτων (frequency hoping spread spectrum FHSS). Πρόκειται για μεταπήδηση συχνοτήτων με ψευδοτυχαίο τρόπο, μέχρι 1600 hops/sec. Όλοι οι κόμβοι στο piconet αλλάζουν συχνότητα ταυτόχρονα σύμφωνα με το χρονισμό και τη σειρά συχνοτήτων που τους υποδεικνύει ο master. Με τη χρήση αυτής της τεχνολογίας υπάρχει διασπορά της πληροφορίας σε μεγάλο εύρος συχνοτήτων σε σχέση με ένα σήμα στενής ζώνης, όπως φαίνεται στο σχήμα 15 γεγονός που αυξάνει την αξιοπιστία του συστήματος.[94]



Σχήμα 4-15: FHSS [96]

Κατά τις πρώτες εκδόσεις του Bluetooth παρατηρούνταν παρεμβολές μεταξύ δικτύων Bluetooth και WiFi. Για την επίλυση του προβλήματος, εφαρμόστηκε η τεχνική adaptive frequency hopping, προσαρμόζοντας τη μεταπήδηση συχνοτήτων αποκλείοντας κανάλια που είναι κατειλημμένα από σήματα RF άλλων δικτύων. Για τη διαμόρφωση και την μετάδοση της πληροφορίας, το Bluetooth χρησιμοποιεί κατά κύριο λόγο διαμόρφωση Frequency Shift Keying (FSK) στέλνοντας 1 bit ανά σύμβολο ανά μsec, επιτυγχάνοντας ρυθμό μέχρι 1 Mbps. Από την έκδοση Bluetooth 2 και έπειτα χρησιμοποιήθηκε η διαμόρφωση Phase Shift Keying (PSK) αυξάνοντας τον αριθμό των bits ανά σύμβολο σε 2 ή 3, επιτυγχάνοντας ρυθμούς ως 3 Mbps. Το link control layer προσεγγίζει σε μεγάλο βαθμό τις λειτουργίες του MAC sublayer του OSI. Ουσιαστικά διαχωρίζει τη ροή των bit πληροφορίας σε πλαίσια (frames). Στην απλούστερη μορφή του πρωτοκόλλου, ο master κόμβος του κάθε piconet ορίζει την έναρξη των χρονοθυρίδων διάρκειας 625 μsec η καθεμία, με τον ίδιο τον master να μπορεί να αρχίσει την εκπομπή μηνύματος στις χρονοθυρίδες με ζυγό αριθμό ενώ οι slave κόμβοι σε αυτές με μονό αριθμό, όπως φαίνεται στο σχήμα 16. [94]

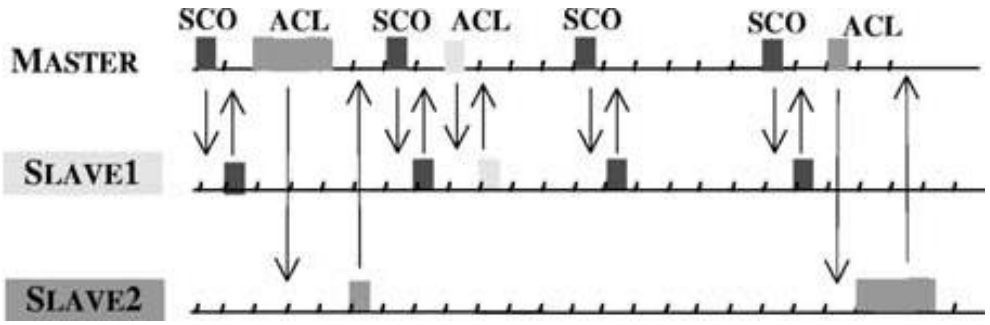


Σχήμα 4-16: Bluetooth time slots [97]

Πρόκειται για παραδοσιακό σχήμα πολυπλεξίας διαίρεσης χρόνου (time division multiplexing) με τον master να εκμεταλλεύεται τις μισές χρονοθυρίδες και τους slave τις άλλες μισές. Τα πλαίσια δεδομένων μπορεί να είναι διάρκειας 1, 3 ή 5 χρονοθυρίδων. Κάθε πλαίσιο πλέον του ωφέλιμου φορτίου, περιλαμβάνει επιβάρυνση (overhead) 126 bits που χρησιμοποιούνται για προσθήκη κωδικού πρόσβασης (access code) και επικεφαλίδας (header) ενώ για κάθε αναπήδηση (hop) συχνότητας υπολογίζεται χρόνος 250-260 μsec/hop για τη σταθεροποίηση των RF κυκλωμάτων. Τα hop πραγματοποιούνται μόνο μεταξύ των frames και όχι κατά τη διάρκεια του frame. Ως εκ τούτου, ένα frame που καταλαμβάνει 5 χρονοθυρίδες θα μεταφέρει περισσότερο ωφέλιμο φορτίο σε σχέση με τα μικρότερα frames καθώς το overhead του frame θα είναι σταθερό.[94] Το link manager protocol δημιουργεί λογικά κανάλια, που ονομάζονται links, για τη μεταφορά frames μεταξύ του master και ενός slave κόμβου. Το συγκεκριμένο πρωτόκολλο είναι υπεύθυνο για τη δημιουργία σύζευξης, το οποίο σε παλιότερες εκδόσεις γινόταν με εισαγωγή κοινού τετραψήφιου PIN (Personal Identification Number) και από τους δύο. Η μέθοδος αυτή αποδείχθηκε μη ασφαλής, λόγω της χρήσης τυποποιημένων PIN, όπως “0000” και “1234”. Η πιο σύγχρονη μέθοδος σύζευξης με το όνομα secure simple pairing, χρησιμοποιεί πιο σύνθετους κωδικούς (passkey) που δεν επιλέγονται από τους χρήστες αλλά δημιουργούνται από τις συσκευές. Η μέθοδος αυτή δεν εφαρμόζεται σε συσκευές που δεν έχουν τη δυνατότητα πληκτρολόγησης χαρακτήρων όπως τα ακουστικά Bluetooth και για τη σύζευξη των οποίων δεν εισάγεται καθόλου κωδικός. Όταν έχει ολοκληρωθεί η σύζευξη δύο συσκευών, το link manager protocol ενεργοποιεί έναν από τους δύο βασικούς τύπους καναλιών:

- SCO (Synchronous Connection Oriented) link: Χρησιμοποείται για real-time δεδομένα όπως οι τηλεφωνικές κλήσεις. Σε κάθε slave κόμβο δίνονται μέχρι τρία SCO link με τον master του, και κάθε link υποστηρίζει μετάδοση ήχου ρυθμού 64.000 bps. Δεν υποστηρίζεται επαναμετάδοση πλαισίων λόγω της χρονικής αμεσότητας που απαιτεί ο συγκεκριμένος τύπος link.
- ACL (Asynchronous ConnectionLess) link. Χρησιμοποιείται για τη μετάδοση πακέτων σε ακανόνιστα χρονικά διαστήματα. Η παράδοση των δεδομένων βασίζεται στο μοντέλο της καλύτερης προσπάθειας (best-effort) και τα χαμένα πλαίσια επανεκπέμπονται. Κάθε slave μπορεί να έχει μόνο ένα ACL link.

Ενδεικτικά στο σχήμα 17 φαίνεται η επικοινωνία του master κόμβου με δύο slaves. Με τον slave1 επικοινωνεί και με τους δύο τύπους καναλιών ενώ με τον slave2 με ACL κανάλια.

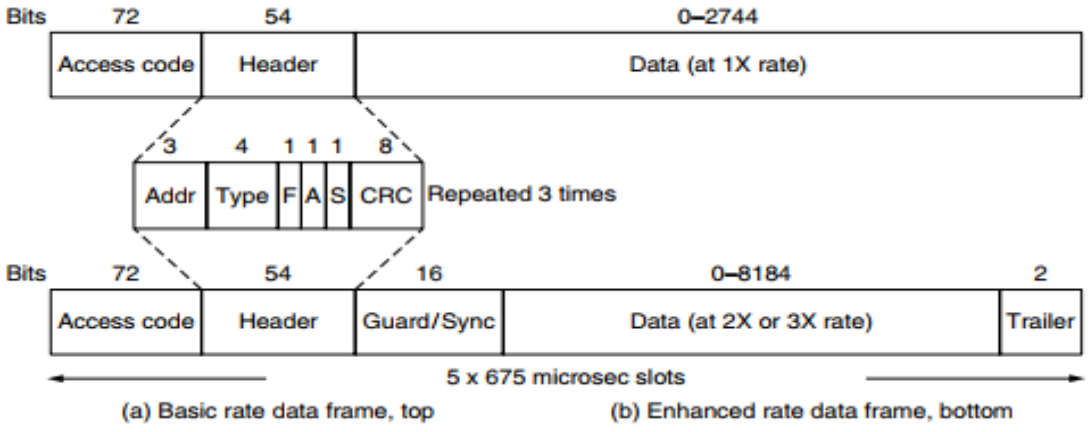


Σχήμα 4-17: SCO και ACL Link [98]

Τα δεδομένα που στέλνονται μέσω των ACL links προέρχονται απ'το επίπεδο **L2CAP** το οποίο έχει 4 κύριες λειτουργίες:

- Λαμβάνει πακέτα μεγέθους έως 64KB από τα ανώτερα επίπεδα και τα διαχωρίζει σε κατάλληλου μεγέθους frames.
- Αναλαμβάνει την πολυπλεξία και αποπολύπλεξία των πακέτων από διαφορετικές πηγές, λειτουργία που μοιάζει με αυτή του επιπέδου μεταφοράς του OSI.
- Εκτελεί έλεγχο σφαλμάτων και επαναμεταδόσεις εάν απαιτείται.
- Εφαρμόζει τις απαιτήσεις QoS μεταξύ των διαφορετικών link.

Η γενική μορφή του Bluetooth frame φαίνεται στο σχήμα 18. Ο κωδικός πρόσβασης (access code) χρησιμοποιείται για την ταυτοποίηση του master κόμβου κάθε μετάδοσης, σε περίπτωση που ένας slave βρίσκεται στην εμβέλεια δύο master. Το header μήκους 54 bit περιλαμβάνει τυπικά πεδία του Mac Sublayer, όπως διευθύνσεις, τύπος ωφέλιμου φορτίου, CRC. Το μέγεθος του πεδίου των δεδομένων ποικίλει ανάλογα με το πόσες χρονοθυρίδες καταλαμβάνει το frame. Σε περίπτωση νεώτερων εκδόσεων όπου αποστέλλονται frame με αυξημένο ρυθμό μετάδοσης, περιλαμβάνεται το πεδίο Guard/Sync.[94]

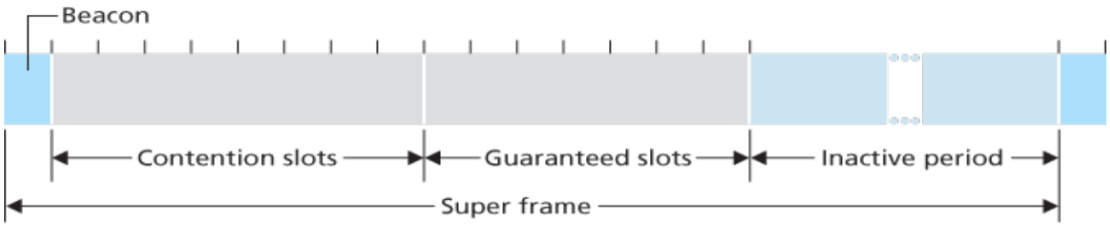


Σχήμα 4-18: Bluetooth frame [94]

4.3 Zigbee (IEEE 802.15.4)

Ένας δεύτερος τύπος δικτύων προσωπικής περιοχής (PAN) που έχει τυποποιηθεί από το IEEE είναι το Zigbee, που ορίζεται με το πρότυπο IEEE 802.15.4. Ενώ τα δίκτυα Bluetooth αναπτύχθηκαν με σκοπό να παρέχουν ρυθμό δεδομένων πάνω από ένα Mbps ώστε να αντικαταστήσουν με επιτυχία την ενσύρματη μετάδοση σε πολλές εφαρμογές, το Zigbee αφορά εφαρμογές που απαιτούν χαμηλότερη ισχύ, χαμηλότερο ρυθμό μετάδοσης και με χαμηλότερο κύκλο λειτουργίας από ό,τι το Bluetooth. Αν και η τάση που επικρατεί είναι ότι "το ταχύτερο είναι καλύτερο", στην πραγματικότητα δεν απαιτούν

όλες οι δικτυακές εφαρμογές υψηλό εύρος ζώνης το οποίο επιφέρει και υψηλό κόστος. Για παράδειγμα, οι έξυπνες οικιακές συσκευές, όπως οικιακοί αισθητήρες θερμοκρασίας και φωτός, συσκευές ασφαλείας και διακόπτες τοίχου είναι πολύ απλές συσκευές χαμηλής ισχύος, χαμηλού κύκλου λειτουργίας και χαμηλού κόστους που για την επιτυχή μετάδοση των δεδομένων τους επαρκούν μερικά Kbps. Το Zigbee είναι επομένως κατάλληλο για αυτές τις συσκευές. Το Zigbee ορίζει κανάλια με ρυθμούς δεδομένων 20, 40, 100 και 250 Kbps, ανάλογα με τη συχνότητα που χρησιμοποιείται.
Το Zigbee λειτουργεί στις βιομηχανικές, επιστημονικές και ιατρικές (Industrial Scientific-Medical - ISM) ζώνες συχνοτήτων, κάτω του ενός GHz, "Sub-GHz", (902-928 MHz στη Βόρεια Αμερική και 868-870 MHz στην Ευρώπη) και στην περιοχή των 2,4 GHz, κυρίως για συσκευές οικιακού αυτοματισμού. Οι ρυθμοί μετάδοσης δεδομένων κυμαίνονται από περίπου 20 Kbps για τις ζώνες κάτω του 1GHz έως περίπου 250 Kbps για τα την περιοχή των 2,4 GHz.
Οι κόμβοι σε ένα δίκτυο Zigbee χωρίζονται σε δύο κατηγορίες. Οι αποκαλούμενες "συσκευές μειωμένης λειτουργίας" (reduced-function devices) λειτουργούν ως slave συσκευές υπό τον έλεγχο μίας μόνο "συσκευής πλήρους λειτουργίας" (full-function device), με παρόμοια λογική με τη λειτουργία των slave κόμβων στα δίκτυα Bluetooth. Μια συσκευή πλήρους λειτουργίας μπορεί να λειτουργήσει ως master κόμβος, όπως στο Bluetooth, ελέγχοντας πολλαπλούς slave κόμβους. ενώ πολλαπλές συσκευές πλήρους λειτουργίας μπορούν επιπλέον να συνδεθούν μεταξύ τους σε ένα δίκτυο πλέγματος και να ανταλλάσσουν δεδομένα μεταξύ τους.
Το Zigbee χρησιμοποιεί πολλούς μηχανισμούς που χρησιμοποιούνται σε άλλα πρωτόκολλα επιπέδου επιπέδου datalink. Για παράδειγμα χρησιμοποιεί πλαίσια beacon και επιβεβαιώσεις (ACK) παρόμοιες με του 802.11 και πρωτόκολλα πολλαπλής πρόσβασης στο μέσο με αλγορίθμους δυαδικής οπισθοχώρησης για την αποφυγή σύγκρουσης, παρόμοια με αυτά που χρησιμοποιούνται στο Ethernet.
Η ρύθμιση ενός δικτύου Zigbee μπορεί να γίνει με πολλούς διαφορετικούς τρόπους. Ενδεικτικά αναφέρεται η απλή περίπτωση μιας συσκευής πλήρους λειτουργίας που ελέγχει πολλαπλές συσκευές μειωμένης λειτουργίας με χρήση χρονοθυρίδων χρησιμοποιώντας πλαίσια beacon. Στο σχήμα 19 απεικονίζεται ο τρόπος λειτουργίας του δικτύου, όπου το δίκτυο Zigbee διαιρεί το χρόνο σε επαναλαμβανόμενα υπερπλαίσια (superframes), καθένα από τα οποία αρχίζει με ένα beacon frame. Κάθε beacon frame διαιρεί το super frame σε μια ενεργό χρονική περίοδο (κατά την οποία συσκευές μπορούν να μεταδίδουν) και σε μια ανενεργή χρονική περίοδο (κατά την οποία όλες οι συσκευές, συμπεριλαμβανομένου του master κόμβου, μπορούν να είναι αδρανείς και έτσι να εξοικονομούν ενέργεια). Η ενεργή περίοδος αποτελείται από 16 χρονοθυρίδες, μερικές από τις οποίες χρησιμοποιούνται από τις συσκευές με τη χρήση του πρωτοκόλλου πολλαπλής πρόσβασης CSMA/CA ενώ οι υπόλοιπες κατανέμονται από τον master σε συγκεκριμένες συσκευές παρέχοντας εγγυημένη πρόσβαση στο κανάλι.[80]



Σχήμα 4-19: Zigbee Superframe [80]

4.4 WiMAX (IEEE 802.16)

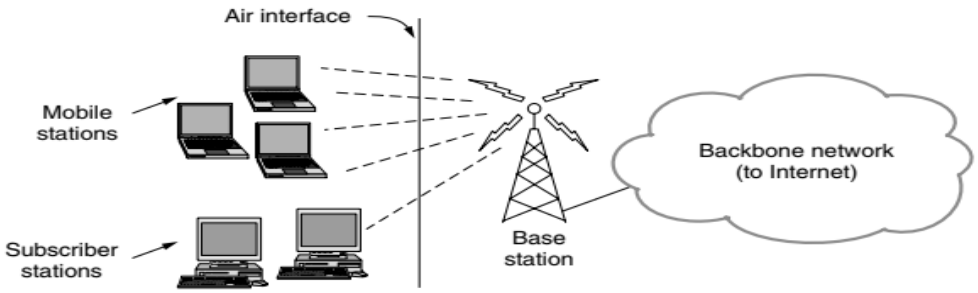
Το WiMAX, ή αλλιώς Worldwide Interoperability for Microwave Access, ορίζεται με το πρότυπο IEEE 802.16. Αρχικά, χρησιμοποιήθηκε για ασύρματες ζεύξεις σταθμών με επαφή line-of-sight. Σύντομα, προσπάθησε να αντικαταστήσει τις καλωδιακές και DSL γραμμές πρόσβασης στο διαδίκτυο και τα πρώτα δίκτυα κινητής τηλεφωνίας που υποστήριζαν μετάδοση δεδομένων, υποστηρίζοντας ζεύξεις non line-of-sight, με χρήση OFDM. Η προσπάθεια αυτή δε στέφθηκε όμως με επιτυχία.

Η συχνότητα λειτουργίας του είναι 2 GHz ως 66 GHz για το "Fixed" WiMAX και 2 GHz ως 6 GHz για το "Mobile" WiMAX. Σε ιδανικές συνθήκες, η εμβέλεια του WiMAX μπορεί να φτάσει μέχρι και 50 χιλιόμετρα (μέγεθος μιας μητροπολιτικής περιοχής), ενώ οι ταχύτητες μετάδοσης δεδομένων μπορούν να είναι αρκετά υψηλές, φτάνοντας μέχρι και 1 Gbps. [94]

4.4.1 Αρχιτεκτονική 802.16

Η αρχιτεκτονική του προτύπου 802.16 παρουσιάζεται στο σχήμα 20. Οι σταθμοί βάσης (base stations) συνδέονται στο ενσύρματο δίτυο του παρόχου Internet και επικοινωνούν με τους ασύρματους σταθμούς (mobile stations) μέσω του ασύρματου μέσου. Υφίστανται δύο είδη σταθμών:

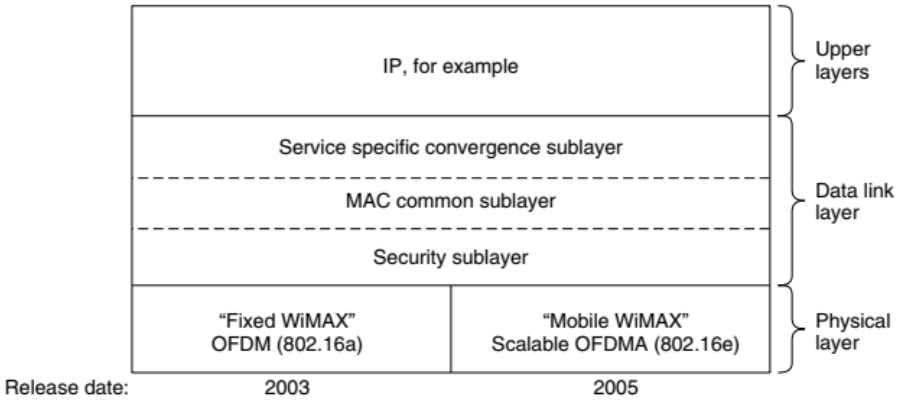
- Οι σταθμοί συνδρομητών (subscriber stations), οι οποίοι παραμένουν σε σταθερή θέση, όπως ένα σπίτι.
- Οι κινητοί σταθμοί (mobile stations), οι οποίοι μπορούν να λαμβάνουν υπηρεσίες ενώ κινούνται, όπως ένα αυτοκίνητο εξοπλισμένο με WiMAX.2 [94]



Σχήμα 4-20: Αρχιτεκτονική 802.16 [94]

4.4.2 Στοίβα πρωτοκόλλων 802.16

Όπως όλα τα πρότυπα της σειράς 802, το 802.16 έχει βασιστεί στο μοντέλο OSI. Η στοίβα πρωτοκόλλων 802.16 παρουσιάζεται στο σχήμα 21. Η γενική δομή είναι παρόμοια με εκείνη των άλλων προτύπων 802, αλλά με περισσότερα υποστρώματα.



Σχήμα 4-21: Στοίβα πρωτοκόλλων 802.16 [94]

Το φυσικό επίπεδο ασχολείται με τη μετάδοση δεδομένων στο ασύρματο μέσο. Στο σχήμα παρουσιάζονται μόνο οι δημοφιλείς εκδόσεις του 802.16, το "Fixed" και "Mobile" WiMAX. Και τα δύο στρώματα λειτουργούν σε αδειοδοτημένο φάσμα κάτω των 11 GHz και χρησιμοποιούν OFDM, αλλά με διαφορετικούς τρόπους.

Πάνω από το φυσικό στρώμα, το στρώμα data link αποτελείται από τρία υποστρώματα:

- Το κατώτερο αφορά στην ασφάλεια δεδομένων και διαχειρίζεται την κρυπτογράφηση, την αποκρυπτογράφηση και τη διαχείριση κλειδιών.
- Ακολουθεί το υποεπίπεδο Media Access Control (MAC) common, στο οποίο βρίσκονται βασικά πρωτόκολλα, όπως η διαχείριση καναλιών. Στο WiMAX ο σταθμός βάσης ελέγχει πλήρως το σύστημα, καθώς μπορεί να προγραμματίσει τα κανάλια downlink (σταθμός βάσης προς συνδρομητή) πολύ αποτελεσματικά και παίζει σημαντικό ρόλο στη διαχείριση του uplink (συνδρομητής προς σταθμό βάσης). Ένα ασυνήθιστο χαρακτηριστικό του υποεπιπέδου MAC είναι ότι, σε αντίθεση με τα άλλα πρωτόκολλα 802, είναι απολύτως προσανατολισμένο στη σύνδεση, προκειμένου να παρέχει εγγυμένη QoS για την τηλεφωνία και την ανταλλαγή πολυμέσων.
- Το υποεπίπεδο service-specific convergence αντικαθιστά το υποεπίπεδο λογικών συνδέσεων άλλων πρωτύπων 802. Η λειτουργία του είναι να παρέχει μια διεπαφή με το επίπεδο δικτύου. Διαφορετικά επίπεδα σύγκλισης ορίζονται για την απρόσκοπτη ενσωμάτωση με διαφορετικά ανώτερα επίπεδα. Το βασικότερο ανώτερο επίπεδο είναι το IP, αν και το πρότυπο ορίζει αντιστοιχίες και για άλλα πρωτόκολλα όπως το Ethernet και το ATM. [94]

Κεφάλαιο 5: Δίκτυα Κινητών Επικοινωνιών

5.1 Εισαγωγή

Τα δίκτυα κινητών επικοινωνιών παρέχουν στους χρήστες πρόσβαση σε ανταλλαγές κλήσεων, μηνυμάτων SMS και πρόσβαση στο δίκτυο. Ειδικά τα δίκτυα τέταρτης (4G) και πέμπτης γενιάς (5G) παρέχουν μεγάλες ταχύτητες μεταφοράς δεδομένων στις περιοχές κάλυψής τους. Συνήθως η κάλυψη του δικτύου είναι πολύ καλή, επεκτείνοντας τη σύνδεση στο διαδίκτυο σε περισσότερες περιοχές. Ωστόσο, σε απομακρυσμένες από τους πύργους κινητής τηλεφωνίας περιοχές οι υπηρεσίες που χρειάζονται υψηλές ταχύτητες υπολειτουργούν με αποτέλεσμα η ταχύτητα να μειώνεται ή ακόμα και να μηδενίζεται. Αυτό επιφέρει σημαντικά περιορισμένες δυνατότητες για τους χρήστες που κατοικούν στις περιοχές αυτές. Επιπλέον, σε μερικές περιπτώσεις η ταχύτητα μπορεί να περιορίζεται λόγω υπερφόρτωσης του δικτύου.

5.2 Εξέλιξη των Κινητών Επικοινωνιών

Οι βασικές αρχές των κυψελωτών συστημάτων τηλεπικοινωνίας ορίστηκαν τη δεκαετία του 1960. Η βασική ιδέα ήταν ο χωρισμός μιας περιοχής κάλυψης σε μικρές κυψέλες, κάθε μία από τις οποίες επαναχρησιμοποιεί συχνότητες με σκοπό την αύξηση της χωρητικότητας. Παρ'όλα αυτά, η τεχνολογία ήταν έτοιμη να υποστηρίξει τα κυψελωτά συστήματα στα τέλη της δεκαετίας του 1970.

- Κυψελωτά Συστήματα 1ης Γενιάς (1G)

Αναπτύχθηκαν μετά το 1979. Χρησιμοποιούσαν αναλογική διαμόρφωση και απαιτούσαν μεγάλη κατανάλωση ισχύος και εμφάνιζαν υψηλό θόρυβο. Παράλληλα, λόγω της αναλογικής διαμόρφωσης που χρησιμοποιούσαν, απαιτούσαν μεγάλο φάσμα συχνοτήτων και υπήρχε απουσία ασφάλειας.

- Κυψελωτά Συστήματα 2ης Γενιάς (2G)

Στηρίζονται στις ψηφιακές τεχνικές διαίρεσης χρόνου (TDM). Έχουν αυξημένη ανοσία στο θόρυβο, προσφέρουν καλύτερη ποιότητα υπηρεσιών σε σύγκριση με τα κυψελωτά δίκτυα 1ης Γενιάς, έχουν δυνατότητα εφαρμογής τεχνικών κρυπτογράφησης για την ασφάλεια της μετάδοσης ενώ δίνουν ευελιξία στην επέκταση των δικτύων. Το πιο γνωστό από τα συστήματα αυτά είναι το σύστημα Global System for Mobile Communications (GSM) το οποίο χρησιμοποιείται ακόμα και σήμερα.

- Κυψελωτά Συστήματα 2,5 Γενιάς (2.5G)

Είναι τα πρώτα συστήματα που προσφέρουν υπηρεσίες μετάδοσης δεδομένων από τις κινητές συσκευές. Τα πιο σημαντικά συστήματα 2,5 Γενιάς είναι το General Packet Radio Service (GPRS) το οποίο υποστηρίζει μετάδοση δεδομένων με ρυθμό έως και 112Kbps και το Enhanced Data for Global Evolution (EDGE) το οποίο υποστηρίζει ρυθμούς έως και 384 Kbps.

- Κυψελωτά Συστήματα 3ης Γενιάς (3G)

Το βασικό χαρακτηριστικό αυτών των συστημάτων είναι η υποστήριξη εφαρμογών πολυμέσων (μουσική, video) και η δυνατότητα πρόσβασης σε πληροφορίες με υψηλούς ρυθμούς μετάδοσης, έως και 7,2 Mbps. Η τεχνολογία που υποστηρίζουν ονομάζεται Πρόσβαση Πακέτων Υψηλής Ταχύτητας (High Speed Packet Access - HSPA).

- Κυψελωτά Συστήματα 4ης Γενιάς (4G)

Η συμφόρηση των δικτύων 2G και 3G μετά το 2010 οδήγησε στην ανάγκη ανάπτυξης των δικτύων 4ης Γενιάς. Βασίζονται στο πρότυπο Long Term Evolution (LTE) και συνδυάζουν τις τεχνικές Orthogonal Frequency Division Multiplexing (OFDM) και Multiple Input-Multiple Output (MIMO). Υποστηρίζονται ταχύτητες μετάδοσης δεδομένων έως και 1Gbps ενώ υποστηρίζονται κινητές συσκευές που κινούνται με ταχύτητα έως και 500 χλμ/ώρα. Έχουν απλή αρχιτεκτονική δικτύου και υποστηρίζουν

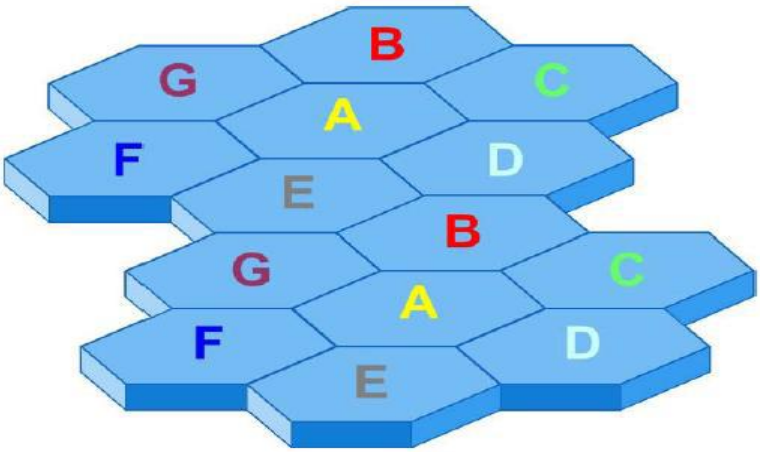
διαλειτουργικότητα με τα συστήματα των παλιότερων γενιών.

- Κυψελωτά Συστήματα 5ης Γενιάς (5G)

Τα συστήματα αυτά αναπτύχθηκαν μετά το 2017 και υποστηρίζουν διασύνδεση σε εξαιρετικά υψηλές ταχύτητες (έως και 20 Gbps) όχι μόνο κινητών τηλεφώνων και συσκευών, αλλά οποιουδήποτε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων (Internet of Things). Έτσι, το πλήθος το συσκευών που εξυπηρετούνται σε μια κυψέλη είναι σημαντικά μεγαλύτερο σε σύγκριση με τις προηγούμενες γενιές. [99]

5.3 Κυψέλες

Το φάσμα των ραδιοσυχνοτήτων αποτελεί έναν περιορισμένο και πολύτιμο πόρο του οποίου πρέπει να γίνει ορθή χρήση και εκμετάλλευση. Οι σχεδιαστές των συστημάτων κινητών επικοινωνιών πρέπει να χρησιμοποιήσουν αποδοτικά το περιορισμένο φάσμα που τους εκχωρείται ώστε να εξυπηρετούν ταυτόχρονα μεγάλο αριθμό χρηστών. Για παράδειγμα, αν σε μια εταιρεία κινητής τηλεφωνίας αποδίδονται οι συχνότητες από 1800 MHz έως 1830 MHz για μία περιοχή, θα πρέπει η εταιρεία να μεριμνήσει ώστε όλοι οι συνδρομητές της που θα βρεθούν στη συγκεκριμένη περιοχή, οποιαδήποτε χρονική στιγμή, να έχουν διαθέσιμο ένα ραδιοκανάλι ώστε να μπορούν να πραγματοποιήσουν μια τηλεφωνική κλήση ή να ανταλλάξουν δεδομένα, εξασφαλίζοντας παράλληλα την καλή ποιότητα της σύνδεσης. Από τα παραπάνω προέκυψαν οι βασικές αρχές της σχεδίασης και η χρήσης των κυψελωτών συστημάτων. Κυψέλη (cell) ονομάζεται μια μικρή γεωγραφική περιοχή στην οποία αποδίδεται προς χρήση μια ομάδα συχνοτήτων (ραδιοδιαύλων), η οποία αποτελεί ένα μέρος του συνόλου που έχει ο πάροχος στη διάθεσή του. Σε κάθε γειτονική κυψέλη αποδίδονται διαφορετικές ομάδες συχνοτήτων ώστε να μην υπάρχει επικάλυψη και παρεμβολή. Οι κεραίες κάθε περιοχής είναι σχεδιασμένες ώστε να επιτυγχάνουν την κάλυψη μέσα στη συγκεκριμένη κυψέλη. Η χρήση των κυψελωτών συστημάτων δίνει τη δυνατότητα στους παρόχους να επαναχρησιμοποιούν την ίδια ομάδα συχνοτήτων σε άλλες κυψέλες που απέχουν μεταξύ τους απόσταση ικανή ώστε να μην υπάρχουν παρεμβολές. Η εξαγωνική κυψέλη (σχήμα 1) είναι θεμελιώδες σχήμα και έχει υιοθετηθεί παγκοσμίως για την ευκολία που παρέχει στην ανάλυση και τη σχεδίαση των συστημάτων. Η πραγματική όμως κάλυψη μιας περιοχής, δε μπορεί να είναι πλήρως κυψελωτή αλλά εξαρτάται από τις κεραίες εκπομπής και το φυσικό ανάγλυφο.



Σχήμα 5-1: Παράδειγμα Κυψελωτού Συστήματος [100]

Οι κυψέλες διαφέρουν ως προς το μέγεθος ανάλογα με τις ανάγκες κάλυψης μιας περιοχής. Μια μεγάλη αγροτική έκταση θα πρέπει να υποστηρίξει μικρό αριθμό χρηστών ενώ σε μια πυκνοκατοικημένη πόλη θα υπάρχουν χιλιάδες χρήστες ανά τετραγωνικό χιλιόμετρο. Συνεπώς υπάρχουν οι κάτωθι τύποι κυψελών:

- Μακροκυψέλες (macrocels)

Έχουν μεγάλη ακτίνα της τάξης δεκάδων χιλιομέτρων. Χρησιμοποιούνται σε αγροτικές ή προαστιακές περιοχές με μικρό αριθμό συνδρομητών και με μικρή παρεμπόδιση της διάδοσης λόγω κτιρίων ή πάνω από εθνικές οδούς ώστε να ικανοποιούν χρήστες με μεγάλη κινητικότητα. Οι κεραίες εκπομπής τοποθετούνται σε ψηλά κτίρια ή πύργους με καλή ορατότητα πάνω από την περιοχή κάλυψης.

- Μικροκυψέλες (microcells)

Είναι μικρότερες σε έκταση με ακτίνα μέχρι τα 2 χλμ αλλά και παρουσιάζεται πιο συχνή επαναχρησιμοποίηση συχνοτήτων μεταξύ των κυψελών. Οι κεραίες εκπομπής τοποθετούνται συνήθως σε στέγες κτιρίων και έχουν σημαντικά μικρότερη ισχύ εκπομπής λόγω της μικρότερης ακτίνας κάλυψης.

- Πικοκυψέλες (picocells)

Χρησιμοποιούνται ιδιαίτερα σε εσωτερικούς χώρους αλλά και σε περιοχές υψηλής πυκνότητας τηλεπικοινωνιακής κίνησης. Έχουν ακτίνα κάλυψης 100-200 μέτρα και οι κεραίες εκπομπής τοποθετούνται σε χαμηλά ύψη (συνήθως κάτω από 4 μέτρα) ή αν πρόκειται για εσωτερικούς χώρους σε διαδρόμους ή ανελκυστήρες.

- Σταθμοί βάσης σπιτιών (femtocells)

Καλύπτουν πολύ μικρές περιοχές, έχουν ακτίνα κάλυψης 10-12 μέτρα. Συνήθως συνδέεται με το δίκτυο του παρόχου υπηρεσιών μέσω του διαδικτύου μέσω ενός ενσύρματου ευρυζωνικού συνδέσμου (όπως DSL ή καλώδιο). Επίσης υποστηρίζουν από 4 μέχρι 8 ενεργές συσκευές ταυτόχρονα. [99]

5.4 Δομή Δικτύου Κινητών Επικοινωνιών

Ένα σύγχρονο κυψελωτό σύστημα κινητών επικοινωνιών έχει αποκεντρωμένη δομή και αποτελείται από τέσσερα κύρια μέρη, τα οποία αναλύονται στη συνέχεια.

5.4.1 Κινητός Σταθμός

Ο Κινητός Σταθμός (Mobile Station - MS) είναι ο φυσικός εξοπλισμός που χρησιμοποιεί ο συνδρομητής ώστε να έχει πρόσβαση στις προσφερόμενες τηλεπικοινωνιακές υπηρεσίες, όπως για παράδειγμα το κινητό τηλέφωνο. Σημαντικό μέγεθος που χαρακτηρίζει κάθε κινητό σταθμό είναι η στάθμη της ισχύος εκπομπής του. Σε κάθε κινητό σταθμό έχουν αποδοθεί διάφοροι αριθμοί αναγνώρισης ή όπως αποκαλούνται, ταυτότητες. Κάθε συσκευή αναγνωρίζεται από μία μοναδική ταυτότητα, την International Mobile Equipment Identity (IMEI). Αυτή αποτελείται από 15 ψηφία, έξι από τα οποία φέρουν τον Type Approval Code (TAC), που υποδεικνύει τον αριθμό έγκρισης τύπου του κινητού σταθμού, δύο φέρουν τον Final Assembly Code (FAC), που υποδεικνύει τον κατασκευαστή και έξι φέρουν τον Serial Number (SN), που προσδιορίζει μοναδικά τον κινητό σταθμό για συγκεκριμένο TAC και FAC. Η ταυτότητα της συσκευής IMEI αποθηκεύεται και σε μια άλλη βάση δεδομένων του δικτύου, η οποία καλείται Equipment Identity Register (EIR) και η οποία θα αναλυθεί παρακάτω. Όταν ο κινητός σταθμός χρησιμοποιείται από ένα συνδρομητή, μεταφέρει άλλη μία ταυτότητα, την International Mobilie Subscriber Identity (IMSI). Η ταυτότητα χρησιμοποιείται για την αναγνώριση του κινητού σταθμού στο δίκτυο. Ουσιαστικά πρόκειται για τον αριθμό τηλεφώνου κάθε συνδρομητή. Αποτελείται από τρεις επιμέρους κωδικούς, τον τριψήφιο Mobile Country Code (MCC), τον διψήφιο Mobile Network Code (MNC) και τον Mobile Subscriber Identification Number (MSIN), ο οποίος μπορεί να φτάσει τα δέκα ψηφία. Η IMSI ενσωματώνεται σε μια κάρτα εντός του κινητού τηλεφώνου, που ονομάζεται Subscriber Identity Module (SIM). Η κάρτα SIM είναι ιδιοκτησία του συνδρομητή και αποτελεί ένα μηχανισμό ταυτοποίησής του, ο οποίος μπορεί να τοποθετηθεί και να χρησιμοποιηθεί σε οποιοδήποτε κινητό τηλέφωνο. Η κάρτα SIM περιέχει επίσης αριθμούς ταυτοποίησης του χρήστη (Personal Identification Number-PIN, Personal Unblocking Key-PUK), μία λίστα των υπηρεσιών στις οποίες ο χρήστης είναι συνδρομητής και μία λίστα των διαθέσιμων δικτύων. Παράλληλα, περιλαμβάνει

εργαλεία απαραίτητα για τις διαδικασίες πιστοποίησης και κρυπτογράφησης. Διαθέτει δε χώρο αποθήκευσης για μηνύματα, τηλεφωνικούς αριθμούς επαφών κλπ. [101]

5.4.2 Υποσύστημα Σταθμών Βάσης

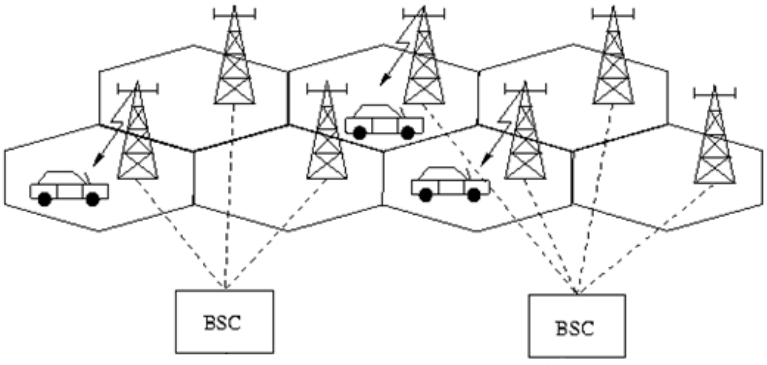
Το Υποσύστημα Σταθμών Βάσης (Base Station System - BSS) παρέχει την απαιτούμενη ραδιοκάλυψη αλλά και τη διαχείρηση πόρων του φάσματος (Radio Resource Management – RRM) του δικτύου κινητής επικοινωνίας. Ουσιαστικά περιέχει το σύστημα κεραιών που σχηματίζει τις κυψέλες και περιλαμβάνει τρεις οντότητες.

- Πομποδέκτης Σταθμού Βάσης

Η βασική υπηρεσία του Πομποδέκτη Σταθμού Βάσης (Base Transceiver Station – BTS) είναι να παρέχει στο Σταθμό Βάσης τις λειτουργίες εκπομπής και λήψης, καθώς αποτελείται από αντίστοιχες διατάξεις συμπεριλαμβανομένων των κεραιών. Επιπλέον, περιλαμβάνει όλες τις ειδικές διατάξεις επεξεργασίας σήματος, όπως διαμόρφωση και κωδικοποίηση. Τέλος είναι υπεύθυνο για τον έλεγχο της ποιότητας των σημάτων. Ένας Σταθμός Βάσης μπορεί να έχει από 1 έως 16 πομποδέκτες, καθένας από τους οποίους αντιπροσωπεύει ένα ξεχωριστό κανάλι εκπομπής και υποστηρίζει την τεχνική πολλαπλής πρόσβασης με διαίρεση συχνότητας (FDMA). Κάθε πομποδέκτης μπορεί να επικοινωνήσει με το πολύ 8 διαφορετικούς κινητούς σταθμούς (MS). Ο αριθμός των πομποδεκτών εξαρτάται από τον αριθμό χρηστών (χωρητικότητα) που απαιτείται να υποστηρίξει κάθε κυψέλη. Οι κεραίες μπορεί να είναι είτε πανκατευθυντικές, είτε κατευθυντικές. Η εκπεμπόμενη ισχύς του BTS είναι αυτή που καθορίζει το μέγεθος της αντίστοιχης κυψέλης.

- Ελεγκτής Σταθμού Βάσης

Ο Ελεγκτής Σταθμού Βάσης (Base Station Controller - BSC) παρακολουθεί και ελέγχει συνεχώς πολλαπλούς Σταθμούς Βάσης (BTS), όπως απεικονίζεται στο σχήμα 2. Κύριος ρόλος του είναι η διαχείρηση των διαθέσιμων συχνοτήτων αποδίδοντας ελεύθερες συχνότητες στους πομποδέκτες για την επικοινωνία με τα κινητά τερματικά, ο έλεγχος των BTS και η διαχείρηση των μεταπομπών, μέσω εντολών προς τους Σταθμούς Βάσης και τα κινητά τερματικά. Ο BSC είναι πλέον υπεύθυνος για την αποσύνδεση μιας ζεύξης, όταν η σύνδεση τερματιστεί. Επιπρόσθετα, μία επιπλέον λειτουργία του είναι ο έλεγχος της ισχύος τόσο των κινητών μονάδων όσο και των Σταθμών Βάσης, με σκοπό τη μείωση των παρεμβολών σε άλλους χρήστες του δικτύου και η μεγιστοποίηση της διάρκειας ζωής της μπαταρίας των κινητών μονάδων. Ο φυσικός εξοπλισμός του BSC μπορεί να τοποθετηθεί είτε στον ίδιο χώρο με το BTS είτε σε δικό του ξεχωριστό χώρο, είτε στο χώρο του κέντρου μεταγωγής MSC.[101]



Σχήμα 5-2: Διασύνδεση BSC-BTS [102]

5.4.3 Υποσύστημα Δικτύου και Διαμεταγωγής

Το Υποσύστημα Δικτύου και Διαμεταγωγής (Network & Switching Subsystem - NSS) είναι υπεύθυνο για τις λειτουργίες μεταγωγής και τη διαχείρηση της επικοινωνίας μεταξύ των κινητών σταθμών και

του σταθερού δικτύου τηλεφωνίας. Εδώ ανήκουν και άλλα κέντρα για παροχή υπηρεσιών όπως τα SMS και ο τηλεφωνητής. Σε αυτό περιλαμβάνονται τα εξής κέντρα:

- Κέντρο Μεταγωγής Κινητών Υπηρεσιών

Το Κέντρο Μεταγωγής Κινητών Υπηρεσιών (Mobile Services Switching Centre - MSC) εκτελεί όλες τις λειτουργίες μεταγωγής κυκλώματος που απαιτούνται για κινητές μονάδες τοποθετημένες στη σχετική MSC περιοχή, δηλαδή την περιοχή για την οποία το συγκεκριμένο κέντρο είναι υπεύθυνο. Από τη μία πλευρά έχει διεπαφή προς τους σταθμούς βάσης (BSS) και από την άλλη προς τα εξωτερικά δίκτυα. Ως φυσική οντότητα, ένα MSC ελέγχει μερικούς BSCs. Προωθεί εισερχόμενες και εξερχόμενες κλήσεις και δεδομένα, συλλέγει δεδομένα και προωθεί μηνύματα σηματοδοσίας σε καταχωρητές καθώς και στο κέντρο χρέωσης (Billing Center). Επίσης, έχει την ευθύνη για τη διαχείριση της κινητικότητας των χρηστών, τη μεταπομπή καθώς και λειτουργίες που σχετίζονται με την ασφάλεια της πληροφορίας. Για την εκτέλεση των παραπάνω λειτουργιών ελέγχου, το MSC πρέπει να διατηρεί συνδέσεις σηματοδοσίας με κάθε κινητό σταθμό, τις διάφορες βάσεις δεδομένων, το τοπικό κέντρο μεταγωγής του σταθερού δικτύου, καθώς και με γειτονικά MSCs.

- Διαβιβαστικό Κέντρο Μεταγωγής Κινητών Υπηρεσιών

Το Διαβιβαστικό Κέντρο Μεταγωγής Κινητών Υπηρεσιών (Gateway Mobile services Centre - GMSC) αποτελεί τη διεπαφή μεταξύ του κυψελωτού δικτύου και του δημόσιου δικτύου σταθερής τηλεφωνίας. Παρέχει τη δυνατότητα δρομολόγησης κλήσεων από το δίκτυο σταθερής τηλεφωνίας προς ένα μεμονωμένο κινητό σταθμό, μέσω του συστήματος σταθμών βάσης (BSS). Το GMSC παρέχει, επίσης, στο δίκτυο συγκεκριμένες πληροφορίες σχετικά με τους κινητούς σταθμούς. Ανάλογα με το μέγεθος του δικτύου μπορούν να χρησιμοποιηθούν ένα ή περισσότερα GMSCs, Σε ένα σύγχρονο δίκτυο κινητών επικοινωνιών, κάθε MSC μπορεί να παίξει το ρόλο του GMSC.

- Οικείος Καταχωρητής Θέσης

Ο Οικείος Καταχωρητής Θέσης (Home Location Register - HLR) είναι η πρωταρχική βάση δεδομένων που χρησιμοποιείται για τη διαχείριση των κινητών συνδρομητών. Κάθε δίκτυο μπορεί να περιέχει έναν ή περισσότερους HLRs ανάλογα το μέγεθός του. Δύο είδη δεδομένων αποθηκεύονται στον HLR:
Τα μόνιμα (στατικά) δεδομένα όλων των συνδρομητών που ανήκουν στη σχετική περιοχή, όπως η IMSI κάθε χρήστη, ο αριθμός τηλεφώνου από το δημόσιο δίκτυο κάθε χρήστη, το κλειδί πιστοποίησης (authentication key), καθώς και οι επιπρόσθετες υπηρεσίες στις οποίες ο συνδρομητής επιτρέπεται να έχει πρόσβαση. Τα προσωρινά (δυναμικά) δεδομένα, όπως ένα μέρος της πληροφορίας θέσης και ειδικότερα η διεύθυνση του τρέχοντος VLR, που αυτή τη στιγμή εξυπηρετεί τον εκάστοτε συνδρομητή που είναι καταχωρημένος στον HLR, ο αριθμός στον οποίο θα πρέπει να προωθούνται οι κλήσεις (εάν ο συνδρομητής έχει επιλέξει προώθηση κλήσεων), καθώς και μερικές προσωρινές παράμετροι για πιστοποίηση και κρυπτογράφηση.

- Καταχωρητής Θέσης Επισκεπτών

Ο Καταχωρητής Θέσης Επισκεπτών (Visitor Location Register - VLR) είναι μία βάση δεδομένων που περιέχει δυναμική πληροφορίας για όλες τις κινητές μονάδες, που είναι επί του παρόντος τοποθετημένες στην περιοχή που καλύπτει ένα συγκεκριμένο MSC. Κάθε MSC έχει έτσι το δικό του VLR.
Μόλις το κινητό μεταφερθεί σε μια νέα MSC περιοχή, ο VLR του νέου MSC θα ζητήσει δεδομένα για το κινητό από τον HLR. Ως μέρος της διαδικασίας, ο HLR θα αποθηκεύσει τη διεύθυνση του VLR, όπου το κινητό θα καταχωρηθεί. Αν αργότερα το κινητό θελήσει να εγκαταστήσει μια κλήση, ο VLR έχει όλα τα απαραίτητα δεδομένα για την εγκατάσταση της κλήσης, χωρίς να είναι απαραίτητη η ενημέρωση από τον HLR, γεγονός που μειώνει την κίνηση δεδομένων στον HLR. Ένας λόγος για τον οποίο αποθηκεύονται σχεδόν πανομοιότυπα δεδομένα σε δύο διαφορετικές βάσεις (HLR και VLR), είναι ότι κάθε μία από τις βάσεις αυτές εξυπηρετεί διαφορετικό σκοπό. Ο HLR παρέχει στο GMSC την απαραίτητη πληροφορία για το συνδρομητή, όταν εισέρχεται μία κλήση από το δημόσιο δίκτυο. Από την άλλη, ο VLR εξυπηρετεί την αντίστροφη διαδικασία, παρέχοντας στον εξυπηρετούντα MSC την απαραίτητη πληροφορία για το συνδρομητή, όταν εισέρχεται μία κλήση από ένα κινητό σταθμό.

- Κέντρο Πιστοποίησης

Το Κέντρο Πιστοποίησης (Authentication Centre - AUC) είναι ένα τμήμα του HLR. Πρόκειται για μια προστατευόμενη βάση δεδομένων που διατηρεί ένα αντίγραφο ενός μυστικού αλγορίθμου πιστοποίησης, ο οποίος είναι αποθηκευμένος και στην κάρτα SIM του κάθε συνδρομητή και χρησιμοποιείται για πιστοποίηση και κρυπτογράφηση πάνω στο ραδιοδίαυλο. Το AUC παρέχει πρόσθετη ασφάλεια ενάντια σε κακόβουλες ενέργειες.

- Καταχωρητής Ταυτότητας Εξοπλισμού

Ο καταχωρητής Ταυτότητας Εξοπλισμού (Equipment Identity Register - EIR) είναι επίσης μια βάση δεδομένων, η χρήση της οποίας αποτελεί ένα ακόμα χαρακτηριστικό ασφάλειας του δικτύου. Στη βάση αυτή καταχωρούνται όλοι οι σειριακοί αριθμοί (serial numbers) των κινητών συσκευών, οι οποίες είτε είναι κλεμμένες είτε, λόγω ελαττωματικού εξοπλισμού, δε χρησιμοποιούνται στο δίκτυο. Η ιδέα είναι να ελέγχεται η ταυτότητα οποιουδήποτε Κινητού Σταθμού σε κάθε εγγραφή του στο δίκτυο και στη συνέχεια, ανάλογα με την IMEI να επιτρέπεται ή όχι η πρόσβαση του κινητού σταθμού στο σύστημα. Ο EIR είναι συνδεδεμένος στο MSC και χρησιμοποιείται από αυτό ώστε να ελέγχει την εγκυρότητα του IMEI της συσκευής που χρησιμοποιεί ένας συνδρομητής, ώστε να μπορεί να γίνει απαγόρευση της εγγραφής του κλεμμένου ή χωρίς άδεια χρήσης κινητού τηλεφώνου.[101]

5.4.4 Κόμβος Υποστήριξης Πύλης GPRS

Ο Κόμβος Υποστήριξης Πύλης GPRS (Gateway GPRS Support Node - GGSN) χρησιμοποιείται στα δίκτυα που υποστηρίζουν υπηρεσίες δεδομένων με μεταγωγή πακέτων. Το GGSN λειτουργεί ως δρομολογητής του κυψελωτού δικτύου και ως πύλη μεταξύ του κυψελωτού δικτύου και του εξωτερικού δικτύου δεδομένων, δηλαδή το διαδίκτυο. Επίσης εκχωρεί διευθύνσεις IP σε κινητές συσκευές, εκτελεί μετάφραση διευθύνσεων IP και διαχειρίζεται τη δρομολόγηση πακέτων δεδομένων μεταξύ του κυψελωτού δικτύου και των εξωτερικών δικτύων.[101]

5.4.5 Κόμβος Υποστήριξης Εξυπηρέτησης GPRS

Ο Κόμβος Υποστήριξης Εξυπηρέτησης GPRS (Serving GPRS Support Node - SGSN) χρησιμοποιείται στα δίκτυα μεταγωγής πακέτων. Το SGSN είναι υπεύθυνο για τη δρομολόγηση και την προώθηση πακέτων δεδομένων από και προς τους κινητούς σταθμούς εντός της περιοχής κάλυψής του. Διατηρεί δεδομένα των συνδέσεων δεδομένων και διαχειρίζεται την κινητικότητα μεταξύ διαφορετικών SGSNs όταν οι κινητές συσκευές μετακινούνται μεταξύ περιοχών κάλυψης (μεταπομπές).[101]

5.4.6 Υποσύστημα Λειτουργείας και Συντήρησης

Το Υποσύστημα Λειτουργίας και Συντήρησης (Operation and Maintenance Subsystem - OMS) πολλές φορές καλείται και Υποσύστημα Υποστήριξης Λειτουργίας (Operation Support Subsystem-OSS) και είναι υπεύθυνο τόσο για τον έλεγχο λειτουργίας και τη συντήρηση του τηλεπικοινωνιακού εξοπλισμού του δικτύου, όσο και τη διαχείριση και τη χρέωση των συνδρομητών. Περιλαμβάνει τα ακόλουθα κέντρα:

- Κέντρο Λειτουργίας και Συντήρησης

Το Κέντρο Λειτουργίας και Συντήρησης (Operation & Maintenance Centre - OMC) είναι ένα σύστημα διαχείρισης που επιβλέπει τη λειτουργία του δικτύου και βοηθάει το χειριστή του δικτύου στη διατήρηση της ικανοποιητικής λειτουργίας του. Το OMC έχει πρόσβαση και στο MSC και στο BSC, χειρίζεται μηνύματα σφάλματος που έρχονται από το δίκτυο και ελέγχει το φορτίο της κίνησης στον BSC και BTS. Μάλιστα, ρυθμίζει τους σταθμούς βάσης BTS μέσω των BSCs και επιτρέπει στο χειριστή του δικτύου να ελέγχει τις διάφορες οντότητες του συστήματος. Συνοπτικά παρέχει το Σύστημα Διαχείρισης Σφαλμάτων, που αναλύει το σήματα συναγερμού, το Σύστημα Διαχείρισης της Διάταξης,

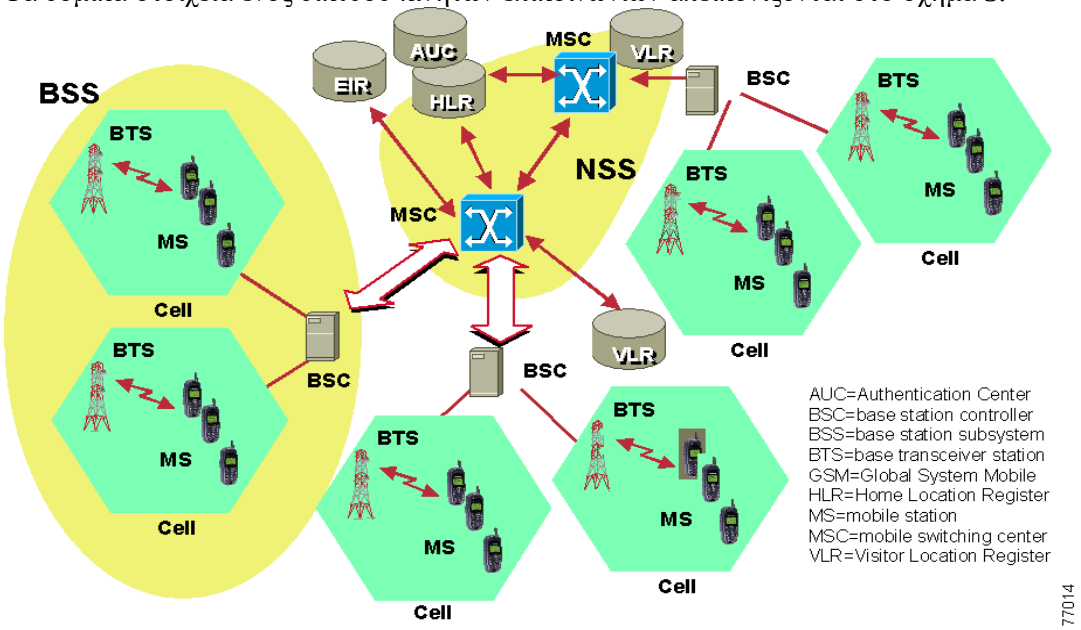
που εγκαθιστά το λογισμικό σε νέα στοιχεία του BSS και το σύστημα Διαχείρισης Λογισμικού, που τροφοδοτεί το σύστημα με νέες εκδόσεις του λογισμικού.

- Κέντρα Διαχείρισης Δικτύου

Τα Κέντρα Διαχείρισης Δικτύου (Network Management Centres - NMC) είναι υπεύθυνα για την αξιολόγηση και τη διαχείριση της επίδοσης του δικτύου, όπου σήματα συναγερμού και σφάλματα αξιολογούνται στατιστικά, γίνεται αναγνώριση κυψελών με μεγάλη τηλεπικοινωνιακή κίνηση ή προβλήματα χωρητικότητας και παρακολουθείται η ποιότητα των προσφερόμενων υπηρεσιών (Quality of Service - QoS).

- Κέντρο Διαχείρισης και Χρέωσης

Το Κέντρο Διαχείρισης και Χρέωσης (Administration & Billing Centre - ABC) είναι υπεύθυνο για τη διαχείριση των συνδρομών, τη συλλογή των στοιχείων κλήσεων και δεδομένων internet καθώς και τη χρέωση των συνδρομητών. [101]
Τα δομικά στοιχεία ενός δικτύου κινητών επικοινωνιών απεικονίζονται στο σχήμα 3.



Σχήμα 5-3: Τα δομικά στοιχεία ενός δικτύου κινητών επικοινωνιών [103]

Κεφάλαιο 6: Ασφάλεια Ασύρματων Δικτύων

6.1 Εισαγωγή

Η ασφάλεια των ασύρματων δικτύων αποτελεί ζητούμενο στον τομέα της πληροφορικής και των τηλεπικοινωνιών. Καθώς οι τεχνολογίες ασύρματων δικτύων εξελίσσονται και επεκτείνονται, το φάσμα των πιθανών κινδύνων και επιθέσεων αυξάνεται επίσης. Από ανεπιθύμητη πρόσβαση σε ευαίσθητα δεδομένα μέχρι και τη διαταραχή ή ακόμη και την καταστροφή του δικτύου, οι απειλές είναι ποικίλες και προσφέρουν πολλά προβλήματα στους διαχειριστές και τους χρήστες των ασύρματων δικτύων. Οι κίνδυνοι στην ασφάλεια των ασύρματων δικτύων προέρχονται από διάφορες πηγές. Οι επιθέσεις μπορούν να προέρχονται από εξωτερικούς εισβολείς, εσωτερικούς χρήστες με κακόβουλες προθέσεις ή ακόμα και από λάθος ενέργειες από τους χρήστες. Η πρόσβαση σε ασύρματα δίκτυα μπορεί να γίνει ακόμη και από απόσταση, χωρίς την ανάγκη φυσικής παρουσίας στο χώρο του δικτύου. Οι απειλές περιλαμβάνουν την παράνομη πρόσβαση σε δεδομένα, την κλοπή ταυτότητας, τη διάρρηξη δικτύου, την εισβολή στο δίκτυο, την καταστροφή δεδομένων και πολλά άλλα. Καθώς οι τεχνολογίες ασύρματων δικτύων γίνονται ολοένα και πιο διαδεδομένες και χρησιμοποιούνται σε πολλούς τομείς της ζωής μας, η ανάγκη για αποτελεσματικές λύσεις ασφάλειας είναι πιο επίκαιρη από ποτέ.

6.2 Υποκλοπή Δεδομένων

Η υποκλοπή των δεδομένων, γνωστή και ως "interception of data", είναι μια από τις κύριες απειλές στην ασφάλεια των ασύρματων δικτύων. Σε αυτήν την επίθεση ο εισβολέας ή κακόβουλος χρήστης παρακολουθεί την ασύρματη επικοινωνία μεταξύ δύο ή περισσότερων συσκευών με σκοπό την παράνομη πρόσβαση σε ευαίσθητα δεδομένα. Η υποκλοπή των δεδομένων μπορεί να γίνει με διάφορους τρόπους. Ένας από τους πιο συνηθισμένους τρόπους είναι η παρακολούθηση της ασύρματης επικοινωνίας μέσω ειδικών λογισμικών όπως το wireshark που επιτρέπουν στον εισβολέα να καταγράφει την κυκλοφορία δεδομένων στο δίκτυο. Αυτό μπορεί να οδηγήσει στην παραβίαση του απορρήτου των πληροφοριών και στην απόκτηση πρόσβασης σε ευαίσθητα δεδομένα, όπως κωδικοί πρόσβασης ή προσωπικές πληροφορίες.

Για την προστασία από την υποκλοπή των δεδομένων, είναι σημαντικό να χρησιμοποιούνται αποτελεσματικά μέτρα ασφαλείας, όπως η κρυπτογράφηση της επικοινωνίας με τη χρήση αξιόπιστων πρωτοκόλλων ασφαλείας όπως το WPA3, η χρήση ενισχυμένων μεθόδων ταυτοποίησης και η τακτική παρακολούθηση της κυκλοφορίας δεδομένων στο δίκτυο για την έγκαιρη ανίχνευση ενδεχόμενων παρεμβάσεων.[104]

6.3 Άρνηση Υπηρεσίας (DOS)

Οι επιθέσεις άρνησης υπηρεσίας (Denial of Service - DoS) αποτελούν μια μορφή επίθεσης στην οποία ο επιτιθέμενος προσπαθεί να καταστήσει μια υπηρεσία ή ένα δίκτυο μη διαθέσιμο για τους νόμιμους χρήστες, εμποδίζοντας την πρόσβασή τους σε αυτήν. Οι επιθέσεις αυτές μπορούν να προκαλέσουν διακοπή της λειτουργίας των υπηρεσιών, υπερφόρτωση των συστημάτων ή των δικτύων, και γενικά να δημιουργήσουν δυσλειτουργίες και προβλήματα στους χρήστες ή στους διαχειριστές. Οι επιθέσεις αυτές μπορούν να πραγματοποιηθούν με διάφορους τρόπους, όπως οι κάτωθι:

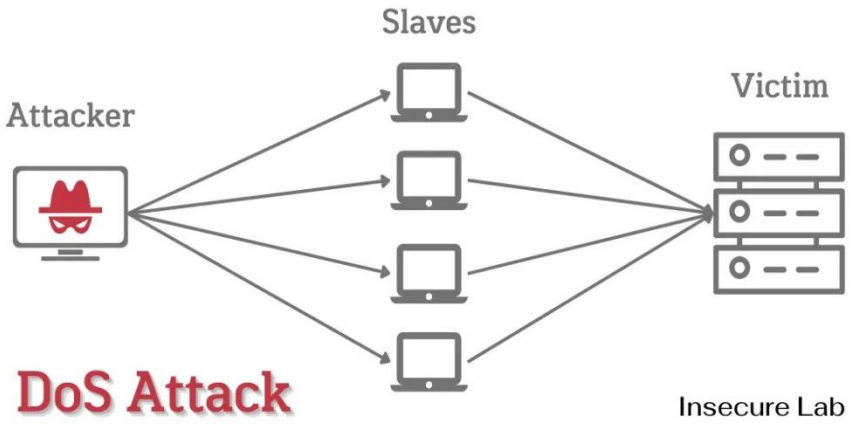
- **Bandwidth Consumption**: Ο επιτιθέμενος μπορεί να αποστέλλει μεγάλους όγκους δεδομένων στο στόχο του δικτύου, καταναλώνοντας το εύρος ζώνης και δυσκολεύοντας ή αποτρέποντας την κανονική λειτουργία του.

- **Ping Flood Attacks**: Ο επιτιθέμενος αξιοποιεί την κακή ρύθμιση των δικτυακών συσκευών, αποστέλλοντας πλαστά πακέτα που κάνουν ping σε κάθε υπολογιστή του στοχευμένου δικτύου,

- **SYN flood**: Ο επιτιθέμενος στέλνει αίτηση σύνδεσης σε ένα διακομιστή, αλλά δεν ολοκληρώνει ποτέ την αλληλεπίδραση. Συνεχίζει μέχρι να κορεστούν όλες οι ανοιχτές θύρες με αιτήσεις και να μην υπάρχει καμία διαθέσιμη για τους νόμιμους χρήστες να συνδεθούν.

Για την προστασία από επιθέσεις DoS, οι διαχειριστές δικτύου μπορούν να χρησιμοποιήσουν διάφορα μέτρα, όπως το φιλτράρισμα της εισερχόμενης κίνησης, η χρήση λύσεων προστασίας DoS σε επίπεδο δικτύου ή εφαρμογής, η ανίχνευση και η απόκριση σε επιθέσεις, και η αναβάθμιση της υποδομής δικτύου για την αντιμετώπιση αυξημένων φόρτων ή επιθέσεων.[105]

Η Distributed Denial-of-Service (DDoS) είναι μια πιο εξελιγμένη μορφή επίθεσης, όπου ο επιτιθέμενος χρησιμοποιεί μια συντονισμένη ομάδα συσκευών μεγάλη σε αριθμό, γνωστή ως botnet, για να εκτελέσει την επίθεση, όπως στο σχήμα 1. Ο κατανεμημένος χαρακτήρας της επίθεσης καθιστά πολύ δυσκολότερο τον εντοπισμό και τον αποκλεισμό του επιτιθέμενου. Σε αυτό το είδος επίθεσης, οι επιτιθέμενοι εκμεταλλεύονται συχνά ευπάθειες σε ευρέως χρησιμοποιούμενα πρωτόκολλα δικτύου ή εφαρμογές, καθώς και την ευρεία διάδοση μηχανισμών επίθεσης με τη χρήση botnets. Οι επιπτώσεις των επιθέσεων DDoS μπορεί να είναι σοβαρές, περιλαμβάνοντας αποκλεισμό των υπηρεσιών, απώλεια εσόδων και ζημίες στη φήμη.[106]



Σχήμα 6-1: Επίθεση Distributed Denial-of-Service (DDoS) [107]

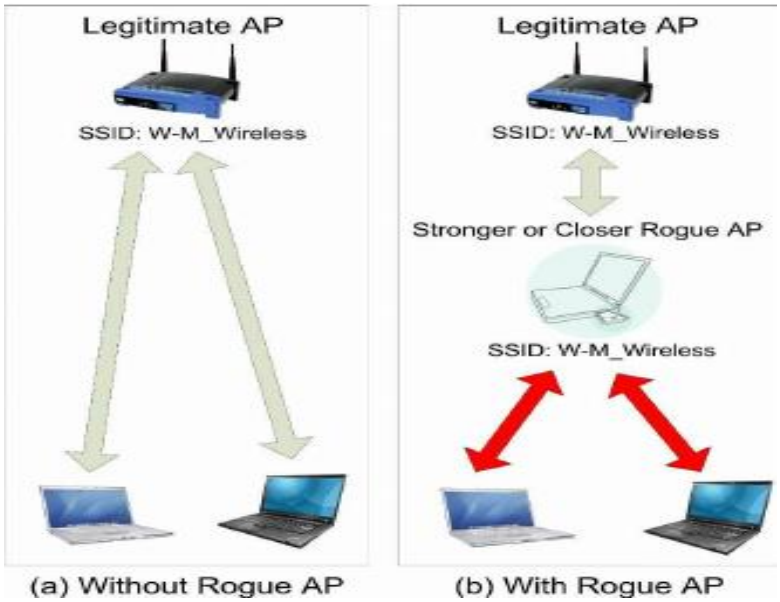
6.4 Κακόβουλα Σημεία Πρόσβασης

Τα Rogue Access Points (Rogue APs) είναι ασύρματα σημεία πρόσβασης που δημιουργούνται από μη εξουσιοδοτημένους χρήστες ή από επιτιθέμενους σε ένα ασύρματο δίκτυο. Αυτά τα APs μπορεί να είναι επικίνδυνα για την ασφάλεια του δικτύου, καθώς μπορούν να δημιουργήσουν ευκαιρίες για επιθέσεις και παραβιάσεις της ασφάλειας. Οι επιτιθέμενοι μπορούν να δημιουργήσουν Rogue APs με διάφορους τρόπους, συμπεριλαμβανομένης της εγκατάστασης ενός δικού τους ασύρματου δρομολογητή ή της δημιουργίας ενός ασύρματου δικτύου από ένα laptop ή ένα κινητό τηλέφωνο που λειτουργεί ως hotspot, όπως στο σχήμα 2. Οι κύριοι κίνδυνοι που συνδέονται με τα Rogue APs είναι οι εξής:

- **Παθητική υποκλοπή (passive interception):** Στην παθητική υποκλοπή, ο επιτιθέμενος μπορεί να διαβάσει τα δεδομένα χωρίς να τα παραποιήσει. Αυτό σημαίνει ότι, αν κάποιος συνδεθεί σε ένα τέτοιο δίκτυο και εισάγει προσωπικές πληροφορίες, όπως κωδικούς πρόσβασης, αυτές μπορούν να διαβαστούν. Επιπλέον, ο επιτιθέμενος έχει τη δυνατότητα να παρακολουθεί την κυκλοφορία στο δίκτυο για να δημιουργήσει προφίλ της συμπεριφοράς στο διαδίκτυο.

- **Ενεργή υποκλοπή (active interception):** Στην ενεργή παρεμβολή, ο επιτιθέμενος όχι μόνο διαβάζει τα δεδομένα του χρήστη, αλλά μπορεί να τα παραποιεί και ακολούθως να τα αποστέλλει στον προορισμό.

Για την αντιμετώπιση των Rogue APs, οι διαχειριστές δικτύου μπορούν να λάβουν μέτρα όπως η ανίχνευση των Rogue APs, η ρύθμιση του δικτύου για να αποφεύγονται οι ανεπιθύμητες συνδέσεις, η χρήση Virtual Private Network (VPN) και η χρήση του πρωτοκόλλου HTTPS. [108]



Σχήμα 6-2: Επίθεση με Rogue AP [109]

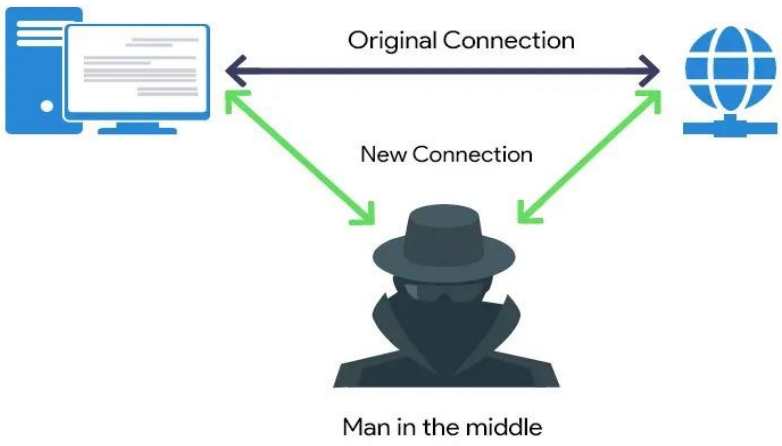
6.5 Επίθεση Man In The Middle (MITM)

Κατά τη διάρκεια μιας Man-In-The-Middle (MITM) επίθεσης, ο επιτιθέμενος εμφανίζεται στο δίκτυο ως ενδιάμεσος κόμβος μεταξύ των δύο ενδιαφερόμενων μερών και μπορεί να παρακολουθήσει, να διαμορφώσει ή ακόμα και να διακόψει την επικοινωνία ανάλογα με τους σκοπούς του, όπως φαίνεται στο σχήμα 3. Οι επιθέσεις MITM είναι συχνές σε ασύρματα δίκτυα, καθώς οι επιτιθέμενοι μπορούν να εκμεταλλευτούν την ασύρματη φύση του δικτύου για να εκτελέσουν αυτές τις επιθέσεις με μεγαλύτερη ευκολία. Μερικοί τρόποι με τους οποίους μπορεί να επιτευχθεί μια MITM επίθεση σε ένα ασύρματο δίκτυο είναι οι εξής:

- **Επίθεση ARP Spoofing**: Ο επιτιθέμενος στέλνει πλαστές αποκρίσεις ARP στο δίκτυο, εκτρέποντας την επικοινωνία από τον αρχικό παραλήπτη στον επιτιθέμενο πριν φτάσει στον προορισμό της.

- **Αντιγραφή SSID**: Ο επιτιθέμενος δημιουργεί ένα πλαστό δίκτυο με το ίδιο SSID όπως ένα αυθεντικό δίκτυο, και επιτρέπει στους χρήστες να συνδεθούν σε αυτό, προκειμένου να καταγράψει ή να παρεμβάλλει την επικοινωνία τους.

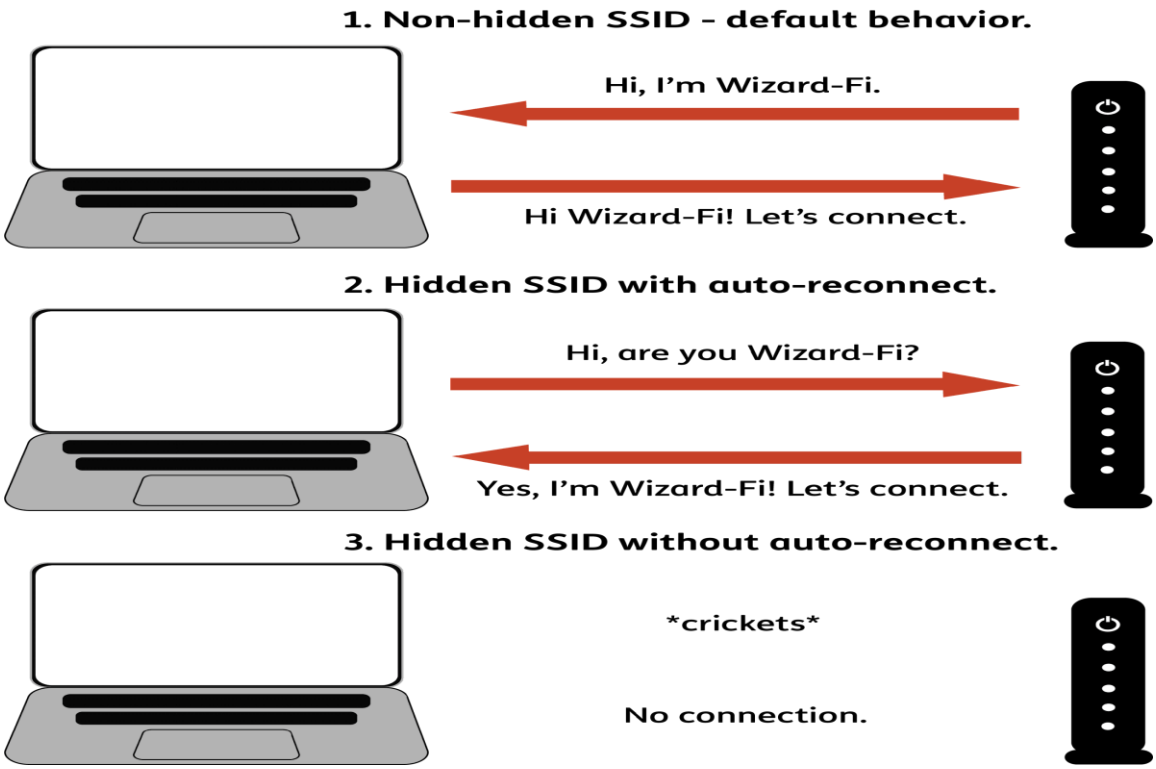
Για να αντιμετωπίσουν τις επιθέσεις MITM, οι χρήστες και οι διαχειριστές δικτύου πρέπει να χρησιμοποιούν ασφαλή πρωτόκολλα επικοινωνίας όπως το HTTPS και να εφαρμόζουν πρακτικές όπως η χρήση δικτύων VPN και η επαλήθευση του πιστοποιητικού ασφαλείας.[104]



Σχήμα 6-3: Επίθεση Man-In-The-Middle [110]

6.6 Απόκρυψη SSID

Ένας τρόπος για να προστατέψουμε το ασύρματο δίκτυο μας είναι η απόκρυψη του Service Set Identifier (SSID), ένα μοναδικό όνομα που χρησιμοποιείται για να αναγνωριστεί ένα ασύρματο δίκτυο από τις συσκευές που αναζητούν σήμα. Η απόκρυψη του SSID, γνωστή και ως "SSID cloaking" ή "SSID hiding", είναι μια εύκολη και απλή τεχνική για την ενίσχυση της ασφάλειας ενός ασύρματου δικτύου. Η βασική ιδέα είναι η απενεργοποίηση του broadcast ώστε να γίνει απόκρυψη του ονόματος του δικτύου από τις αναζητήσεις δικτύων των συσκευών που αναζητούν ασύρματα δίκτυα (σχήμα 4). Αν και η πρακτική αυτή δεν προσφέρει απόλυτη ασφάλεια, καθώς το SSID μπορεί να εντοπιστεί με εξειδικευμένα εργαλεία, παρέχει ένα επιπλέον εμπόδιο για τους επιτιθέμενους. Η χρήση του SSID cloaking προσφέρει κάποια μικρά πλεονεκτήματα για την ασφάλεια του ασύρματου δικτύου. Καταρχάς, αποτρέπει τον εύκολο εντοπισμό του δικτύου από κακόβουλος χρήστες που αναζητούν ασύρματα δίκτυα για πιθανή εισβολή. Επιπλέον, μειώνει την πιθανότητα επιθέσεων κατά του δικτύου, καθώς οι επιτιθέμενοι πρέπει να γνωρίζουν το όνομα του δικτύου προτού μπορέσουν να προβούν σε επίθεση. Τέλος, η απόκρυψη του SSID μπορεί να βοηθήσει στη διατήρηση του απορρήτου, καθώς δεν επιτρέπει εύκολη σύνδεση στο δίκτυο. Παρά τα πλεονεκτήματά του, το SSID cloaking δεν αποτελεί ικανό μέτρο ασφαλείας. Ορισμένες συσκευές μπορούν να αναγνωρίσουν δίκτυα με κρυμμένο SSID και να τα εμφανίσουν στους χρήστες. Επίσης, η απόκρυψη του SSID μπορεί να δυσκολέψει τη διαχείριση του δικτύου, καθώς η σύνδεση νέων συσκευών απαιτεί την εισαγωγή του SSID με το χέρι. Παρά τα μειονεκτήματά του, το SSID cloaking παραμένει ένα χρήσιμο εργαλείο για την ενίσχυση της ασφάλειας του ασύρματου δικτύου.[111]



Σχήμα 6-4: Σύνδεση σε δίκτυο χωρίς και με απόκρυψη SSID [112]

6.7 Φιλτράρισμα MAC Διευθύνσεων

Ο βασικός σκοπός του φιλτραρίσματος των διευθύνσεων MAC είναι η περιορισμένη πρόσβαση συγκεκριμένων συσκευών στο ασύρματο δίκτυο, βασιζόμενη στις μοναδικές τους διευθύνσεις MAC. Κάθε δικτυακή συσκευή διαθέτει μια μοναδική διεύθυνση MAC που την αναγνωρίζει στο δίκτυο. Με τον μηχανισμό αυτό, ο διαχειριστής δικτύου μπορεί να καθορίσει ποιες συσκευές είναι εξουσιοδοτημένες να συνδεθούν στο δίκτυο, ενώ απορρίπτει αυτές που δεν είναι εξουσιοδοτημένες. Το φιλτράρισμα των διευθύνσεων MAC παρέχει αρκετά οφέλη στην ασφάλεια του ασύρματου δικτύου. Αρχικά επιτρέπει στους διαχειριστές να έχουν πλήρη έλεγχο επί των συσκευών που έχουν πρόσβαση στο δίκτυο, αποτρέποντας τυχόν μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, αποτελεί έναν αποτελεσματικό τρόπο να αντιμετωπιστούν οι προσπάθειες εισβολής στο δίκτυο από μη εξουσιοδοτημένες συσκευές. Το φιλτράρισμα των διευθύνσεων MAC βοηθά επίσης στη διατήρηση του απορρήτου των δεδομένων, καθώς περιορίζει την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες. Παρά τα πλεονεκτήματά του, το φιλτράρισμα MAC διευθύνσεων εμφανίζει και ορισμένα μειονεκτήματα. Ένα από τα βασικά μειονεκτήματα είναι η δυσκολία διαχείρισης μεγάλου αριθμού διευθύνσεων MAC σε μεγάλα δίκτυα. Επιπλέον, οι εξειδικευμένοι εισβολείς μπορούν να χρησιμοποιήσουν τεχνικές όπως η πλαστογράφηση διεύθυνσης MAC ή η κλωνοποίηση διεύθυνσης MAC για να αποκτήσουν πρόσβαση στο δίκτυο. Σε κάθε περίπτωση, είναι σημαντικό να συνειδητοποιήσουμε ότι το φιλτράρισμα MAC διευθύνσεων δεν παρέχει απόλυτη ασφάλεια και ότι πρέπει να συνδυάζεται με άλλα μέτρα ασφαλείας για την καλύτερη προστασία του δικτύου.[111]

6.8 Open System Authentication

Η διαδικασία αυθεντικοποίησης ανοικτού συστήματος (Open System Authentication) είναι ένα από τα δύο βασικά πρωτόκολλα αυθεντικοποίησης που χρησιμοποιούνται στα ασύρματα δίκτυα IEEE 802.11 (Wi-Fi). Κατά τη διαδικασία αυτή, οι συσκευές που επιθυμούν να συνδεθούν στο ασύρματο δίκτυο δεν απαιτούν να παρέχουν κωδικό πρόσβασης ή άλλα διαπιστευτήρια. Αντ' αυτού, η διαδικασία αυθεντικοποίησης συνίσταται απλώς στην ανταλλαγή ενός ανοικτού πακέτου ελέγχου πρόσβασης (Authentication Request) και ενός πακέτου αναγνώρισης (Authentication Response) μεταξύ της συσκευής που επιθυμεί να συνδεθεί και του access point. Το Open System Authentication δεν παρέχει πραγματική ασφάλεια καθώς η πρόσβαση στο δίκτυο είναι ανοιχτή σε οποιαδήποτε συσκευή εντός της εμβέλειας του access point. Είναι μια απλή μορφή αυθεντικοποίησης που χρησιμοποιείται συνήθως σε καταστάσεις όπου η ασφάλεια δεν είναι κρίσιμη, όπως σε δίκτυα δημόσιας πρόσβασης ή σε περιβάλλοντα όπου οι περιορισμοί πρόσβασης διαχειρίζονται με άλλα μέσα.[113]

6.9 Shared Key Authentication

Η αυθεντικοποίηση κοινού κλειδιού (Shared Key Authentication) αποτελεί έναν από τους βασικούς μηχανισμούς ασφαλείας που χρησιμοποιούνται στα ασύρματα δίκτυα. Κατά την αυθεντικοποίηση με χρήση κλειδιών, ο πελάτης (client) που επιθυμεί να συνδεθεί σε ένα ασύρματο δίκτυο πρέπει να αποδείξει ότι διαθέτει το σωστό κλειδί πρόσβασης. Η διαδικασία αυτή περιλαμβάνει τα εξής βήματα:

- **Αίτηση σύνδεσης**: Ο πελάτης στέλνει ένα αίτημα σύνδεσης στο σημείο πρόσβασης
- **Challenge**: Το AP στέλνει ένα αίτημα στον πελάτη.
- **Authentication**: Ο πελάτης λαμβάνει την πρόκληση και την κρυπτογραφεί με την χρήση 64 bit ή 128 bit και έπειτα τη στέλνει στο access point.
- **Verification**: Το access point λαμβάνει το κρυπτογραφημένο μήνυμα από τον πελάτη και το επαληθεύει χρησιμοποιώντας το κοινό κλειδί. Εάν το μήνυμα είναι σωστό, ο πελάτης αυθεντικοποιείται και λαμβάνει πρόσβαση στο δίκτυο.

Παρόλο που η αυθεντικοποίηση κοινού κλειδιού είναι ένας απλός μηχανισμός, έχει τις αδυναμίες του. Ένας εξειδικευμένος επιτιθέμενος μπορεί να καταφέρει να αποκτήσει το κλειδί πρόσβασης μέσω καταγραφής της κυκλοφορίας δεδομένων και εκμετάλλευσης των αδύναμων πρωτοκόλλων κρυπτογράφησης.[114]

6.10 Κεντρικός Έλεγχος Ταυτότητας

Η διαδικασία αυθεντικοποίησης χρησιμοποιώντας έναν κεντρικό διακομιστή αυθεντικοποίησης, όπως ο RADIUS (Remote Authenication Dial-In User Service) είναι ένας τρόπος που χρησιμοποιείται για να επιβεβαιωθεί η ταυτότητα ενός χρήστη πριν του επιτραπεί η πρόσβαση σε ένα ασύρματο δίκτυο. Σε αυτό το μοντέλο, ο διακομιστής αυθεντικοποίησης λειτουργεί ως κεντρικός ελεγκτής ταυτότητας και επιβεβαιώνει την ταυτότητα του χρήστη πριν του παραχωρήσει πρόσβαση στο δίκτυο. Η διαδικασία ξεκινά όταν ο χρήστης προσπαθεί να συνδεθεί στο ασύρματο δίκτυο. Η συσκευή του αποστέλλει ένα αίτημα στο διακομιστή αυθεντικοποίησης για να επιβεβαιώσει την ταυτότητά του. Ο διακομιστής αυθεντικοποίησης ελέγχει στη συνέχεια τα διαπιστευτήρια του χρήστη, συνήθως χρησιμοποιώντας μια κεντρική βάση δεδομένων στην οποία αποθηκεύονται τα ονόματα χρηστών και οι κωδικοί πρόσβασης. Εάν οι πληροφορίες πιστοποίησης του χρήστη είναι σωστές, ο διακομιστής αυθεντικοποίησης εκδίδει ένα πιστοποιητικό επιτυχούς αυθεντικοποίησης στη συσκευή του χρήστη. Αυτό το πιστοποιητικό χρησιμοποιείται στη συνέχεια για να επιβεβαιωθεί η ταυτότητα του χρήστη κατά τη σύνδεση στο ασύρματο δίκτυο. Με αυτόν τον τρόπο, η αυθεντικοποίηση με κεντρικό διακομιστή εξασφαλίζει ότι μόνο εγκεκριμένοι χρήστες έχουν πρόσβαση στο ασύρματο δίκτυο, καθιστώντας το πιο ασφαλές και προστατευμένο από ανεπιθύμητους εισβολείς.[115]

6.11 Πρωτόκολλα και Αλγόριθμοι Κρυπτογράφησης

Στην κρυπτογραφία, υπάρχουν δύο κύριες κατηγορίες αλγορίθμων που χρησιμοποιούνται για τη διασφάλιση της εμπιστευτικότητας των δεδομένων. Αυτές οι δύο κατηγορίες είναι οι συμμετρικοί και οι ασύμμετροι αλγόριθμοι κρυπτογράφησης. Μερικοί συμμετρικοί αλγόριθμοι κρυπτογράφησης είναι οι εξής:

- **DES:** Αυτός είναι ένας αλγόριθμος κρυπτογράφησης που παλαιότερα αποτελούσε τυπική επιλογή. Ωστόσο, το μειονέκτημά του είναι το μικρό μήκος του κλειδιού, κάτι που καθιστά το χρήστη ευάλωτο σε σύγχρονες μεθόδους επίθεσης. [116]

- **3DES:** Είναι ίδιος με τον DES με την διαφορά ότι εκτελείται τρεις φορές.[116]

- **AES:** Είναι ένας δημοφιλής και ασφαλής συμμετρικός αλγόριθμος κρυπτογράφησης. Περισσότερα χαρακτηριστικά θα αναφερθούν παρακάτω. [111]

- **SEAL:** Ο αλγόριθμος SEAL αποτελεί μια ταχύτερη εναλλακτική συμμετρική μέθοδος κρυπτογράφησης. Χρησιμοποιεί ένα κλειδί κρυπτογράφησης 160-bit και επιφέρει μικρότερο φορτίο στην κεντρική μονάδα επεξεργασίας σε σύγκριση με άλλους αλγορίθμους [117]

- **RC:** Χρησιμοποιήθηκε για να προστατεύει την κυκλοφορία στο διαδίκτυο, αλλά έχει αποδειχθεί ότι έχει πολλές ευπάθειες που τον καθιστούν μη ασφαλή. [118]

Ορισμένοι μη συμμετρικοί αλγόριθμοι κρυπτογράφησης είναι οι εξής:

- **DH :** Ο αλγόριθμος Diffie-Hellman επιτρέπει σε δύο μέρη να δημιουργήσουν ένα κοινό μυστικό κλειδί, το οποίο μπορούν να χρησιμοποιήσουν για να κρυπτογραφήσουν και να αποκρυπτογραφήσουν τα μηνύματα που ανταλλάσσονται ανάμεσά τους, χωρίς να χρειάζεται να μοιραστούν το κλειδί μέσω ανοιχτής επικοινωνίας. Το μήκος κλειδιού που χρησιμοποιεί είναι 512, 1024 ή 2048 bits.[119]

- **RSA :** Το RSA είναι ένας αλγόριθμος κρυπτογράφησης που βασίζεται στην παραγοντοποίηση πολύ μεγάλων αριθμών. Είναι η πρώτη γνωστή μέθοδος που κατασκευάστηκε ώστε να είναι κατάλληλη για την υπογραφή και την κρυπτογράφηση δεδομένων. Το μήκος κλειδιού που συνηθίζονται είναι 1024 ή 2048 bits.[120]

6.11.1 WEP

Το Wired Equivalent Privacy (WEP) ήταν ένα πρωτόκολλο ασφάλειας που χρησιμοποιούνταν στα ασύρματα δίκτυα για την προστασία των δεδομένων και την αυθεντικοποίηση των συσκευών. Ήταν ο αρχικός αλγόριθμος κρυπτογράφησης του προτύπου 802.11 και αναπτύχθηκε για να παρέχει επίπεδο ασφάλειας παρόμοιο με τα ενσύρματα δίκτυα. Το WEP χρησιμοποιούσε κρυπτογράφηση κλειδιού για την προστασία των δεδομένων που μεταδίδονταν μέσω του ασύρματου δικτύου. Αυτό επιτυγχάνεται με την κρυπτογράφηση δεδομένων μέσω του αλγορίθμου συμμετρικής κρυπτογράφησης RC4. Το κλειδί WEP μπορούσε να έχει μήκος 40-bit ή 104-bit και χρησιμοποιούνταν για την κρυπτογράφηση των δεδομένων πριν από τη μετάδοσή τους. Ωστόσο, η ασφάλεια του πρωτοκόλλου WEP αποδείχθηκε σύντομα ανεπαρκής λόγω πολλαπλών αδυναμιών στον τρόπο λειτουργίας του. Κάποιες από τις βασικές αδυναμίες του WEP ήταν η επαναχρησιμοποίηση των κλειδιών κρυπτογράφησης, καθώς και η αναπόφευκτη πρόβλεψη των κλειδιών λόγω του μικρούς μήκους τους. Λόγω των σοβαρών αδυναμιών του, το WEP τελικά αντικαταστάθηκε από πιο ασφαλή πρωτόκολλα κρυπτογράφησης, όπως το WPA.[111]

6.11.2 WPA

Το Wi-Fi Protected Access (WPA) είναι ένα πρωτόκολλο ασφαλείας που αναπτύχθηκε ως

βελτίωση της ασφάλειας των ασύρματων δικτύων από το προηγούμενο πρότυπο WEP. Η ανάπτυξή του προέκυψε από την ανάγκη για πιο αξιόπιστες μεθόδους κρυπτογράφησης και πιστοποίησης στα ασύρματα δίκτυα Wi-Fi. Το WPA προσφέρει αρκετές βελτιώσεις σε σχέση με το WEP, συμπεριλαμβανομένης της χρήσης πιο ασφαλών αλγορίθμων κρυπτογράφησης, όπως το Temporal Key Integrity Protocol (TKIP). Αυτός ο αλγόριθμος είναι πιο ανθεκτικός σε επιθέσεις σε σύγκριση με το αδύναμο κλειδί WEP. Το WPA έχει εξελιχθεί, με την εισαγωγή διαδοχικών εκδόσεων, όπως το WPA2, το οποίο παρέχει ακόμα μεγαλύτερη ασφάλεια και λειτουργικότητα σε σύγκριση με το αρχικό WPA.[111]

Το Temporal Key Integrity Protocol (TKIP) είναι ένα πρωτόκολλο κρυπτογράφησης που αναπτύχθηκε ως μέρος του WPA (Wi-Fi Protected Access) για να αυξήσει την ασφάλεια των ασύρματων δικτύων. Αντικαθιστά το αρχικό πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στο WEP, το οποίο είχε διαπιστωθεί ότι είναι ευάλωτο σε επιθέσεις.Ο βασικός στόχος του TKIP είναι να προσφέρει μια πιο ασφαλή μέθοδο κρυπτογράφησης και διανομής κλειδιών στα ασύρματα δίκτυα. Χρησιμοποιεί το πρωτόκολλο RC4 για την κρυπτογράφηση των δεδομένων, αλλά εισάγει μια σειρά από βελτιώσεις για την ασφάλεια. Μία από τις κύριες βελτιώσεις που προσφέρει το TKIP είναι η αυτόματη αλλαγή των κλειδιών κρυπτογράφησης. Αυτό γίνεται για να αποτρέψει τις επιθέσεις που βασίζονται στην ανάλυση της επαναλαμβανόμενης χρήσης του ίδιου κλειδιού. Κάθε πακέτο δεδομένων στο TKIP κρυπτογραφείται με ένα νέο κλειδί, το οποίο υπολογίζεται βάσει μιας σειράς παραμέτρων όπως το αρχικό κλειδί και ένας τυχαίος αριθμός.Επιπλέον, το TKIP υιοθετεί μια σειρά μέτρων για την προστασία από άλλες επιθέσεις όπως η αποτροπή επαναλαμβανόμενων πακέτων δεδομένων και η προστασία από Injection Attacks. Αυτές οι βελτιώσεις συνεισφέρουν στη γενική αύξηση της ασφάλειας του ασύρματου δικτύου σε σύγκριση με το αρχικό πρωτόκολλο WEP. Παρόλα αυτά, το TKIP έχει θεωρηθεί ότι παρουσιάζει κάποιες ευπάθειες και έχει αντικατασταθεί από πιο σύγχρονες και ασφαλείς μεθόδους κρυπτογράφησης όπως το AES που χρησιμοποιείται στο WPA2 και WPA3.[121]

6.11.3 WPA2

Το Wi-Fi Protected Access 2 (WPA2) αποτελεί τη δεύτερη γενιά του πρωτοκόλλου ασφαλείας Wi-Fi, αναπτυγμένη για την προστασία ασύρματων δικτύων εναντίον διαφόρων επιθέσεων και απειλών. Είναι η βασική προτεινόμενη επιλογή για την ασφάλεια σύγχρονων ασύρματων δικτύων και αντικαθιστά το προηγούμενο WPA. Το WPA2 χρησιμοποιεί ισχυρότερους αλγορίθμους κρυπτογράφησης σε σύγκριση με το WPA. Αντί για τον προσχεδιασμένο αλγόριθμο TKIP που χρησιμοποιούνταν στο WPA, το WPA2 χρησιμοποιεί το πιο ασφαλές Advanced Encryption Standard (AES) για την κρυπτογράφηση των δεδομένων. Αυτό καθιστά το WPA2 πιο ανθεκτικό σε επιθέσεις και προσφέρει υψηλό επίπεδο ασφάλειας για τα ασύρματα δίκτυα. Μια σημαντική αναβάθμιση που παρέχει το WPA2 είναι η υποστήριξη του πρωτοκόλλου 802.1X για τον έλεγχο πρόσβασης (Access Control), που επιτρέπει στους διαχειριστές των δικτύων να εφαρμόζουν πολύπλοκες μεθόδους πιστοποίησης των χρηστών. Η εισαγωγή του WPA2 έχει συμβάλει σημαντικά στη βελτίωση της ασφάλειας των ασύρματων δικτύων και έχει καταστήσει τη χρήση των ασύρματων δικτύων πιο ασφαλή και αξιόπιστη. Παρά τις βελτιώσεις του WPA2, ενδέχεται να υπάρχουν κενά στην ασφάλεια, και για αυτόν τον λόγο εμφανίστηκε η ανάγκη για την ανάπτυξη του πιο σύγχρονου πρωτοκόλλου WPA3.[111]

Το Advanced Encryption Standard (AES) είναι ένας από τους πιο αξιόπιστους αλγορίθμους κρυπτογράφησης που χρησιμοποιούνται σε ασύρματα δίκτυα και άλλες εφαρμογές ασφαλείας. Ο AES είναι ένας συμμετρικός αλγόριθμος, που σημαίνει ότι χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων (Pre-Shared Key - PSK). Ένα από τα σημαντικά χαρακτηριστικά του AES είναι η δυνατότητά του να λειτουργεί με διάφορα μήκη κλειδιών, περιλαμβανομένων των 128, 192 και 256 bits. Αυτό προσφέρει επιπλέον επίπεδα ασφάλειας και προστασίας από επιθέσεις. Ο AES έχει ενσωματωθεί σε πολλά πρότυπα ασφάλειας, όπως το WPA2 και το WPA3, προσφέροντας έτσι ένα υψηλό επίπεδο προστασίας σε ασύρματα δίκτυα.[111]

6.11.4 WPA3

Το Wi-Fi Protected Access 3 (WPA3) είναι η τρίτη γενιά του πρωτοκόλλου ασφαλείας Wi-Fi, σχεδιασμένη για την προστασία των ασύρματων δικτύων από επιθέσεις και απειλές. Πρόκειται για ένα σημαντικό βήμα προς τη βελτίωση της ασφάλειας στα ασύρματα δίκτυα και την ενίσχυση της προστασίας των δεδομένων και της ιδιωτικότητας των χρηστών. Οι κύριες βελτιώσεις και χαρακτηριστικά του WPA3 περιλαμβάνουν:

- **Ενισχυμένη Ασφάλεια Κρυπτογράφησης:** Το WPA3 χρησιμοποιεί ένα προηγμένο πρωτόκολλο κρυπτογράφησης 128-bit Simultaneous Authentication of Equals (SAE). Αυτό το πρωτόκολλο προσφέρει ακόμη υψηλότερο επίπεδο ασφάλειας από το AES, το οποίο είναι γνωστό για την κρυπτογράφηση με 128 bits.

- **Ανθεκτικότητα σε Επιθέσεις Brute Force:** Το WPA3 παρέχει μεγαλύτερη ανθεκτικότητα σε επιθέσεις brute force επιτρέποντας λιγότερες προσπάθειες για την απόκτηση του κλειδιού πρόσβασης.

- **Βελτιωμένη Προστασία της Ιδιωτικότητας:** Το WPA3 προσφέρει βελτιωμένη προστασία της ιδιωτικότητας μέσω της υποστήριξης του προτύπου Opportunistic Wireless Encryption (OWE), που παρέχει κρυπτογράφηση των δεδομένων ακόμη και για μη-εγγεγραμμένους χρήστες.

- **Ασφαλής Σύνδεση σε Ανοιχτά Δίκτυα:** Με την εισαγωγή του WPA3, η σύνδεση σε ανοιχτά δίκτυα γίνεται πιο ασφαλής μέσω του πρωτοκόλλου Enhanced Open, που προσφέρει κρυπτογράφηση κατά τη διάρκεια της ανταλλαγής δεδομένων.

Συνολικά, το WPA3 αποτελεί μια σημαντική βελτίωση στην ασφάλεια των ασύρματων δικτύων, παρέχοντας πιο ισχυρή και αξιόπιστη προστασία ενάντια σε επιθέσεις και εξασφαλίζοντας την ιδιωτικότητα και την ακεραιότητα των δεδομένων των χρηστών.[122]

Το SAE ορίζεται στο πρότυπο IEEE 802.11-2016. Αποτελεί μια παραλλαγή της λεγόμενης dragonfly-handshake που χρησιμοποιεί κρυπτογραφία για να αποτρέψει τον επιτιθέμενο να μαντέψει έναν κωδικό πρόσβασης και αντικαθιστά τη μέθοδο PSK (Pre-Shared Key) που χρησιμοποιείται από την εισαγωγή του WPA2 το 2004. Μέχρι το 2016, το PSK φαινόταν ασφαλές, μέχρι που ανακαλύφθηκαν οι επιθέσεις επανεγκατάστασης κλειδιού (Key Reinstallation Attacks - KRACK). Ένα KRACK διακόπτει τη σειρά των χειραψιών προσποιούμενο ότι χάνει προσωρινά τη σύνδεση με το δρομολογητή. Στην πραγματικότητα, χρησιμοποιεί τις επαναλαμβανόμενες προσπάθειες σύνδεσης για να αναλύσει τις χειραψίες μέχρι να συνθέσει ποιο πρέπει να είναι το password. Το SAE εμποδίζει αυτό το είδος επίθεσης, καθώς και τις πιο συνηθισμένες επιθέσεις λεξικού εκτός σύνδεσης, κατά τις οποίες ένας υπολογιστής εξετάζει εκατοντάδες, χιλιάδες ή εκατομμύρια κωδικούς πρόσβασης για να προσδιορίσει ποιος κωδικός πρόσβασης ταιριάζει με τις πληροφορίες επαλήθευσης που παρέχονται από τις χειραψίες PSK. Όπως υποδηλώνει και το όνομά του, το SAE λειτουργεί θεωρώντας τις συσκευές ως ισότιμες, αντί να αντιμετωπίζει τη μία πλευρά ως αιτούντα και την άλλη πλευρά ως αυθεντικοποιητή. Οποιοδήποτε από τα δύο μέρη μπορεί να ξεκινήσει τη χειραψία (handshake). Στη συνέχεια προχωρούν στην αποστολή των πληροφοριών αυθεντικοποίησης τους ανεξάρτητα. Χωρίς την αμοιβαία ανταλλαγή χειραψιών, οι επιθέσεις KRACK δεν μπορούν να εισέλθουν στη διαδικασία και οι επιθέσεις λεξικού είναι άχρηστες.[123]

Κεφάλαιο 7: Συμπέρασμα

Η παρούσα πτυχιακή εργασία μελέτησε τεχνολογίες ασύρματων δικτύων με ιδιαίτερη έμφαση στο WiFi (IEEE 802.11) και τα δίκτυα κινητών επικοινωνιών, παρουσιάζοντας τις βασικές αρχές λειτουργίας, κάποιες εκ των πολλών εφαρμογών τους στο σύγχρονο κόσμο, τα μειονεκτήματα και τα πλεονεκτήματά τους. Μετά από την ανάλυση όλων των δεδομένων που συλλέχτηκαν από τη διατιθέμενη βιβλιογραφία, προκύπτουν τα εξής συμπεράσματα:

- Η ιστορική εξέλιξη των ασύρματων δικτύων είναι αξιοσημείωτη, από την ανακάλυψη των ραδιοκυμάτων μέχρι την σημερινή εποχή των δικτύων κινητής 5G.
- Στο σύγχρονο κόσμο τα ασύρματα δίκτυα προσφέρουν φορητότητα και ευελιξία με ικανοποιητικούς ρυθμούς μετάδοσης δεδομένων. Για το λόγο αυτό, η χρήση τους έχει υιοθετηθεί σε πολλούς τομείς, αλλάζοντας ριζικά τον τρόπο που επικοινωνούμε και διασκεδάζουμε.
- Στα ασύρματα δίκτυα δεν απαιτείται η χρήση περίπλοκων υποδομών. Συνεπώς ανταλλάσσονται πιο εύκολα δεδομένα μεταξύ έξυπνων συσκευών και συστημάτων του Internet of Things (IoT) για την παροχή υπηρεσιών και λειτουργιών που απλοποιούν σημαντικά την καθημερινότητά μας.
- Η ασφάλεια αποτελεί κρίσιμο ζήτημα στα ασύρματα δίκτυα, με απειλές όπως η υποκλοπή δεδομένων, οι επιθέσεις άρνησης υπηρεσίας (DoS) και τα κακόβουλα σημεία πρόσβασης. Η χρήση ισχυρών πρωτοκόλλων ασφαλείας, όπως το WPA3, καθώς και η εφαρμογή μέτρων ασφαλείας όπως το φιλτράρισμα MAC διευθύνσεων και η αυθεντικοποίηση με κεντρικό διακομιστή, είναι απαραίτητα για την προστασία των δεδομένων και την ασφάλεια των δικτύων.
- Λαμβάνοντας υπόψη τα συμπεράσματα της παρούσας εργασίας, προτείνεται μελλοντικά η έρευνα στους ακόλουθους τομείς:
- Βελτιστοποίηση των τεχνολογιών MIMO και OFDM, η οποία θα προσφέρει ακόμα μεγαλύτερη αποδοτικότητα των ασύρματων τεχνολογιών δικτύωσης.
- Ενίσχυση των μέτρων ασφάλειας και των αλγορίθμων κρυπτογράφησης που χρησιμοποιούνται στα ασύρματα δίκτυα για την προστασία των δεδομένων και των χρηστών από κακόβουλες ενέργειες.
- Διερεύνηση και εξέλιξη των δυνατοτήτων των δικτύων κινητών επικοινωνιών στο πλαίσιο της επερχόμενης γενιάς 6G για την υποστήριξη έξυπνων πόλεων και περισσότερων εφαρμογών IoT, με στόχο την υλοποίηση πιο βιώσιμων και πιο αποδοτικών αστικών δομών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] "Wireless Networks - DIS." Accessed: May 23, 2024. [Online]. Available: https://disnetwork.co.uk/service/wireless-networks/

[2] "The Evolution of Wi-Fi networks: from IEEE 802.11 to Wi-Fi 6E." Accessed: May 21, 2024. [Online]. Available: https://www.wevolver.com/article/the-evolution-of-wi-fi-networks-from-ieee-80211-to-wi-fi-6e

[3] "A history of wireless for business and a look forward | TechTarget." Accessed: May 21, 2024. [Online]. Available: https://www.techtarget.com/searchnetworking/tip/A-history-of-wireless-for-business-and-a-look-forward

[4] "History of mobile networks, from 1G to 5G | Videotron Forum." Accessed: May 21, 2024. [Online]. Available: https://forum.videotron.com/t5/blog/from-1g-to-5g-a-brief-history-of-mobile-networks/ba-p/43211

[5] "Understanding OSI Model | Indusface." Accessed: May 21, 2024. [Online]. Available: https://www.indusface.com/learning/osi-model/

[6] "The OSI model acronym - How the OSI model began." Accessed: May 21, 2024. [Online]. Available: https://blog.domotz.com/it-security/history-of-the-osi-model/

[7] "Best Guide To Understand What Is TCP/IP Model | Simplilearn." Accessed: May 21, 2024. [Online]. Available: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model

[8] "What is TCP/IP Model. The TCP/IP model serves as a framework… | by Victor Aaron Winnercoz | Medium." Accessed: May 21, 2024. [Online]. Available: https://winnercoz.medium.com/what-is-tcp-ip-model-9410b9a4776b

[9] "History | Wi-Fi Alliance." Accessed: May 21, 2024. [Online]. Available: https://www.wi-fi.org/who-we-are/history

[10] "Bluetooth Special Interest Group - Wikipedia." Accessed: May 21, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Bluetooth_Special_Interest_Group

[11] "Wireless Broadband Alliance - Wikipedia." Accessed: May 21, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Wireless_Broadband_Alliance

[12] "IEEE - History of IEEE." Accessed: May 21, 2024. [Online]. Available: https://www.ieee.org/about/ieee-history.html

[13] "Telecommunications Industry Association - Wikipedia." Accessed: May 21, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Telecommunications_Industry_Association

[14] "Οργανισμοί Τυποποίησης | ΤΕΕ." Accessed: May 21, 2024. [Online]. Available: https://web.tee.gr/d-e-k-a-d/tmima-typopoiisis/organismoi/

[15] "CCITT (Consultative Committee for International Telephony and Telegraphy) (Linktionary term)." Accessed: May 22, 2024. [Online]. Available: https://www.linktionary.com/c/ccitt.html

[16] "The Evolution & History of Radio Wave Technology [Infographic]." Accessed: May 21, 2024. [Online]. Available: https://blog.bliley.com/evolution-of-radio-wave-technology

[17] "Wireless for Beginners Part 1: RF and Waves." Accessed: May 21, 2024. [Online]. Available: https://www.networkcomputing.com/network-infrastructure/wireless-for-beginners-part-1-rf-and-waves

[18] "Wireless for Beginners Part 1: RF and Waves." Accessed: May 21, 2024. [Online]. Available: https://www.networkcomputing.com/network-infrastructure/wireless-for-beginners-part-1-rf-and-waves

[19] "Why Channels 1, 6 and 11? | MetaGeek." Accessed: May 21, 2024. [Online]. Available: https://www.metageek.com/training/resources/why-channels-1-6-11/

[20] "Fundamentals of Wireless Signals and Cellular Networks." Accessed: May 21, 2024. [Online]. Available: https://www.qualcomm.com/developer/blog/2019/10/fundamentals-wireless-

signals-and-cellular-networks
[21] T. S. Rappaport, “Wireless Communications: Principles and Practice (2nd Edition).” [Online]. Available: www.vsofts.net
[22] “Διαμόρφωση σήματος - Βικιπαίδεια.” Accessed: May 21, 2024. [Online]. Available: https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%BC%CF%8C%CF%81%CF%86%CF%89%CF%83%CE%B7_%CF%83%CE%AE%CE%BC%CE%B1%CF%84%CE%BF%CF%82
[23] “Amplitude Shift Keying - GeeksforGeeks.” Accessed: May 21, 2024. [Online]. Available: https://www.geeksforgeeks.org/amplitude-shift-keying/
[24] “Amplitudenumtastung_en.png (592×402).” Accessed: May 21, 2024. [Online]. Available: https://www.itwissen.info/lex-images/Amplitudenumtastung_en.png
[25] “FSK (Frequency Shift Keying).” Accessed: May 21, 2024. [Online]. Available: https://www.telecomtrainer.com/fsk-frequency-shift-keying/
[26] “Frequency Shift Keying.” Accessed: May 21, 2024. [Online]. Available: https://www.tutorialspoint.com/digital_communication/digital_communication_frequency_shift_keying.htm
[27] “2.13: Phase Shift Keying Modulation - Engineering LibreTexts.” Accessed: May 22, 2024. [Online]. Available: https://eng.libretexts.org/Bookshelves/Electrical_Engineering/Electronics/Microwave_and_RF_Design_I_-_Radio_Systems_(Steer)/02%3A_Modulation/2.13%3A_Phase_Shift_Keying_Modulation
[28] “Phase-shift keying - Wikipedia.” Accessed: May 22, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Phase-shift_keying
[29] “PSK – phase shift keying - T&M Atlantic.” Accessed: May 21, 2024. [Online]. Available: https://www.tmatlantic.com/encyclopedia/index.php?ELEMENT_ID=10478
[30] J. G. Proakis and Masoud. Salehi, *Digital communications*. McGraw-Hill, 2008.
[31] “16-QAM Modulation Signal with Variable Data | Download Scientific Diagram.” Accessed: May 21, 2024. [Online]. Available: https://www.researchgate.net/figure/16-QAM-Modulation-Signal-with-Variable-Data_fig5_285535883
[32] “Amplitude modulation - Wikipedia.” Accessed: May 22, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Amplitude_modulation
[33] “Amplitude Modulation – Physics and Radio-Electronics.” Accessed: May 21, 2024. [Online]. Available: https://www.physics-and-radio-electronics.com/blog/amplitude-modulation/
[34] “Frequency modulation - Wikipedia.” Accessed: May 22, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Frequency_modulation
[35] “Frequency Modulation – Physics and Radio-Electronics.” Accessed: May 21, 2024. [Online]. Available: https://www.physics-and-radio-electronics.com/blog/frequency-modulation/
[36] “Phase modulation - Wikipedia.” Accessed: May 22, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Phase_modulation
[37] “Types of Wireless Networks - CCNA Wireless 640-722 Official Cert Guide [Book].” Accessed: May 21, 2024. [Online]. Available: https://www.oreilly.com/library/view/ccna-wireless-640-722/9780133445725/ch05lev2sec1.html
[38] “What is a Wireless Personal Area Network (WPAN)? - Definition from Techopedia.” Accessed: May 21, 2024. [Online]. Available: https://www.techopedia.com/definition/5109/wireless-personal-area-network-wpan
[39] “Everything about WPAN: Wireless Personal Area Network.” Accessed: May 21, 2024. [Online]. Available: https://ccm.net/computing/networks/9763-wpan-wireless-personal-area-network/
[40] “The 4 different types of wireless networks | TechTarget.” Accessed: May 21, 2024. [Online]. Available: https://www.techtarget.com/searchnetworking/tip/The-4-different-types-of-wireless-networks
[41] R. C. Braley, I. C. Gifford, and R. F. Heile, “Wireless Personal Area Networks: An Overview of the IEEE P802.15 Working Group.” [Online]. Available: http://www.bluetooth.com/

[42] "(PDF) Evolution of Wireless LAN in Wireless Networks." Accessed: May 21, 2024. [Online]. Available: https://www.researchgate.net/publication/321864911_Evolution_of_Wireless_LAN_in_Wireless_Networks
[43] "The first wireless LAN /WLAN - Teldat." Accessed: May 21, 2024. [Online]. Available: https://www.teldat.com/blog/the-first-wireless-lan-wlan/
[44] I. Al Shourbaji, "An Overview of Wireless Local Area Networks (WLAN)."
[45] "Overview of Wireless Metropolitan Area Network (WMAN) - GeeksforGeeks." Accessed: May 21, 2024. [Online]. Available: https://www.geeksforgeeks.org/overview-of-wireless-metropolitan-area-network-wman/
[46] J. Salazar, *WIRELESS NETWORKS*. [Online]. Available: http://www.techpedia.eu
[47] "What is WWAN? | Inseego." Accessed: May 21, 2024. [Online]. Available: https://inseego.com/resources/5g-glossary/what-is-wwan/
[48] "Cellular System- Basic Concepts - Open Means." Accessed: May 21, 2024. [Online]. Available: https://openmeans.com/articles/education/19-engineering/4115-cellular-system-basic-concepts.html
[49] "Types of WiFi Antenna in Wireless Networks - GeeksforGeeks." Accessed: May 21, 2024. [Online]. Available: https://www.geeksforgeeks.org/types-of-wifi-antenna-in-wireless-networks/
[50] "What is an Antenna? Different Different Types of Antennas & Characteristics of Antenna | Characteristics." Accessed: May 22, 2024. [Online]. Available: https://www.electronicshub.org/types-of-antennas/
[51] "Antenna Gain - an overview | ScienceDirect Topics." Accessed: May 22, 2024. [Online]. Available: https://www.sciencedirect.com/topics/engineering/antenna-gain
[52] "Intro to Antenna Polarization - JEM Engineering Blog." Accessed: May 22, 2024. [Online]. Available: https://jemengineering.com/blog-intro-to-antenna-polarization/
[53] "Beamwidth - WLAN Antenna Quick Start - Huawei." Accessed: May 21, 2024. [Online]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1000077015/25277461/beamwidth
[54] "WiFi Antenna Types." Accessed: May 21, 2024. [Online]. Available: https://www.accessagility.com/blog/wifi-antenna-types
[55] "Point-to-Point/Multipoint Access Points Singapore." Accessed: May 21, 2024. [Online]. Available: https://www.dlink.com.sg/point-to-point-multipoint-aps/
[56] "Parabolic antenna - Wikipedia." Accessed: May 22, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Parabolic_antenna
[57] "Parabolic-Solid-Dish-Antenna.jpg (300×399)." Accessed: May 22, 2024. [Online]. Available: https://www.sannytelecom.com/wp-content/uploads/2022/03/Parabolic-Solid-Dish-Antenna.jpg
[58] "parabolic-grid-reflector.jpg (300×280)." Accessed: May 22, 2024. [Online]. Available: https://www.sannytelecom.com/wp-content/uploads/2022/03/parabolic-grid-reflector.jpg
[59] "Collinear Antenna » Electronics Notes." Accessed: May 21, 2024. [Online]. Available: https://www.electronics-notes.com/articles/antennas-propagation/phased-array-antennas/collinear-vertical-antenna.php#google_vignette
[60] "What is a Collinear Antenna? - everything RF." Accessed: May 21, 2024. [Online]. Available: https://www.everythingrf.com/community/what-is-a-collinear-antenna
[61] "Dipole antenna - Wikipedia." Accessed: May 22, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Dipole_antenna
[62] "DATAEAGLE Omnidirectional Antenna for 2.4GHz - 2.5 dbi – Grid Connect." Accessed: May 21, 2024. [Online]. Available: https://www.gridconnect.com/products/omnidirectional-antenna-no-10248-for-2-4ghz
[63] "Antenna Theory - Yagi-Uda Antenna." Accessed: May 21, 2024. [Online]. Available: https://www.tutorialspoint.com/antenna_theory/yagi_uda_antenna_theory.htm

[64] “YAGI UDA ANTENNA | SEMT.” Accessed: May 21, 2024. [Online]. Available: https://semtsite.wordpress.com/2016/12/13/yagi-uda-antenna/
[65] “What Are Smart Antennas? Why Do We Need Them? - Huawei.” Accessed: May 21, 2024. [Online]. Available: https://info.support.huawei.com/info-finder/encyclopedia/en/Smart+Antenna.html
[66] “Smart Antenna Systems and Technology.” Accessed: May 21, 2024. [Online]. Available: https://www.circuitstoday.com/smart-antennas
[67] “Learn about Multiple-Input Multiple-Output.” Accessed: May 21, 2024. [Online]. Available: https://www.intel.com/content/www/us/en/support/articles/000005714/wireless/legacy-intel-wireless-products.html
[68] “What is MIMO Technology? - everything RF.” Accessed: May 21, 2024. [Online]. Available: https://www.everythingrf.com/community/what-is-mimo-technology
[69] “What Is Beamforming WiFi. Beamforming WiFi is a type of wireless… | by Arafat Bidyut | Medium.” Accessed: May 21, 2024. [Online]. Available: https://medium.com/@greentechrevolution/what-is-beamforming-wifi-8a241822fe07
[70] “All about beamforming, the faster Wi-Fi you didn’t know you needed | PCWorld.” Accessed: May 21, 2024. [Online]. Available: https://www.pcworld.com/article/448537/all-about-beamforming-the-faster-wi-fi-you-didnt-know-you-needed.html
[71] “Fat, Fit, and Cloud APs in a Nutshell — Huawei Enterprise.” Accessed: May 21, 2024. [Online]. Available: https://e.huawei.com/se/blogs/enterprise-networking/wifi6/201903011058
[72] “What Are Wireless Access Points? A Complete Overview | WiFi Marketing | Beambox | Beambox.” Accessed: May 21, 2024. [Online]. Available: https://beambox.com/townsquare/what-are-wireless-access-points-a-complete-overview-or-wifi-marketing-or
[73] Matthew. Gast, *802.11 wireless networks : the definitive guide*. O’Reilly, 2002.
[74] “Wireless Access Points: Everything You Need To Know | Jones IT.” Accessed: May 21, 2024. [Online]. Available: https://www.itjones.com/blogs/wireless-access-points-everything-you-need-to-know
[75] “What is an Access Point? - Cisco.” Accessed: May 21, 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-access-point.html#~types-of-access-points
[76] “What is a Router? - Definition and Uses - Cisco.” Accessed: May 21, 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-to-choose-small-business-routers
[77] “42-routing-tables.jpg (607×466).” Accessed: May 22, 2024. [Online]. Available: https://www.learncisco.net/wp-content/themes/learncisco/assets/images/icnd1/42-routing-tables.jpg
[78] “How Networks Work: Exploring the Fundamentals of Switches, Routers, DNS, DHCP, NAT, VPN, and More - DEV Community.” Accessed: May 21, 2024. [Online]. Available: https://dev.to/kaushit/how-networks-work-exploring-the-fundamentals-of-switches-routers-dns-dhcp-nat-vpn-and-more-33d1
[79] “What is a router? Definition from SearchNetworking.” Accessed: May 21, 2024. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/router
[80] J. F. Kurose and K. W. Ross, *Computer networking : a top-down approach*.
[81] “The Evolution of IEEE 802 11 standards — BAG NAC - Networks & Security - Medium.” Accessed: May 22, 2024. [Online]. Available: https://medium.com/networks-security/the-evolution-of-ieee-802-11-standards-bag-nac-177a8f71eab2
[82] “What is 802.11ac (Wi-Fi 5)? | Definition from TechTarget.” Accessed: May 22, 2024. [Online]. Available: https://www.techtarget.com/whatis/definition/80211ac
[83] “802.11ax release date: Here’s what has to happen first | TechTarget.” Accessed: May 22, 2024. [Online]. Available: https://www.techtarget.com/searchnetworking/infographic/80211ax-release-date-Heres-

what-has-to-happen-first
[84] “Channel & Transmit Power on Wi-Fi Networks Guide (Part 2) | EnGenius.” Accessed: May 22, 2024. [Online]. Available: https://www.engeniustech.com/go-guide-channel-transmit-power-wi-fi-networks-2/
[85] “ResearchGate.” Accessed: May 22, 2024. [Online]. Available: https://www.researchgate.net/figure/RTS-CTS-and-NAV-Setting_fig2_3044634/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ
[86] “802.11 Medium Access Control DCF and PCF: Performance Comparison | SpringerLink.” Accessed: May 22, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-04927-0_13
[87] “802.11 Medium Access Control DCF and PCF: Performance Comparison | SpringerLink.” Accessed: May 22, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-04927-0_13
[88] “Hidden node problem - Wikipedia.” Accessed: May 22, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Hidden_node_problem
[89] “Hidden Station Problem (HSP) in Wireless LAN - GeeksforGeeks.” Accessed: May 22, 2024. [Online]. Available: https://www.geeksforgeeks.org/hidden-station-problem-hsp-in-wireless-lan/
[90] J. L. Sobrinho, R. De Haan, and J. M. Brázio, “Why RTS-CTS is not your ideal wireless LAN multiple access protocol,” *IEEE Wireless Communications and Networking Conference, WCNC*, vol. 1, pp. 81–87, 2005, doi: 10.1109/WCNC.2005.1424480.
[91] “layer2 - Why is RTS/CTS optional for IEEE 802.11? - Network Engineering Stack Exchange.” Accessed: May 22, 2024. [Online]. Available: https://networkengineering.stackexchange.com/questions/52313/why-is-rts-cts-optional-for-ieee-802-11
[92] “8: Standard IEEE 802.11 Frame Format . | Download Scientific Diagram.” Accessed: May 22, 2024. [Online]. Available: https://www.researchgate.net/figure/Standard-IEEE-80211-Frame-Format_fig7_267375905
[93] “Mobility in the Same IP Subnet.”
[94] “Andrew S. Tanenbaum - Computer Networks”.
[95] “Transmission Rate vs. Bandwidth in Bluetooth Technology | Advanced PCB Design Blog | Cadence.” Accessed: May 22, 2024. [Online]. Available: https://resources.pcb.cadence.com/blog/2022-transmission-rate-vs-bandwidth-in-bluetooth-technology
[96] “greekmodeller - Αερομοντελισμός στην Ελλάδα: Τα συστήματα FHSS και FASST της FUTABA.” Accessed: May 22, 2024. [Online]. Available: https://greekmodeller.blogspot.com/p/4-5-2015-fhss-fasst-futaba-1-fhss-fhss.html
[97] “Part 2 – Bluetooth Physical Layer – Embedded Sense.” Accessed: May 22, 2024. [Online]. Available: https://msreekan.com/2011/09/06/bluetooth-physical-layer/
[98] “Packet transmissions on SCO and ACL links. | Download Scientific Diagram.” Accessed: May 22, 2024. [Online]. Available: https://www.researchgate.net/figure/Packet-transmissions-on-SCO-and-ACL-links_fig3_225131180
[99] “Συστήματα Κινητών Επικοινωνιών, 2η Έκδοση – Εκδόσεις Παπασωτηρίου.” Accessed: May 22, 2024. [Online]. Available: https://ekdoseis-papasotiriou.gr/products/9789604910861-konstantinou-filippos-sustimata-kiniton-epikoinonion-2i-ekdosi
[100] Τ. Μηχανικών Πληροφοριακών and Ε. Συςτημάτων Πανεπιςτήμιο Αιγαίου, “Βαςικζσ Αρχζσ Κυψελωτϊν Συςτημάτων Δημοςθζνησ Βουγιοφκασ (dvouyiou@aegean.gr) Αναπληρωτήσ Καθηγητήσ Κινητζσ και Δορυφορικζσ Επικοινωνίεσ.”
[101] “ΔΙΚΤΥΑ ΚΙΝΗΤΩΝ & ΠΡΟΣΩΠΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ, 2η Έκδοση Βελτιωμένη - Εκδόσεις ΤΖΙΟΛΑ.” Accessed: May 22, 2024. [Online]. Available: https://www.tziola.gr/book/diktya-kiniton-prosopikon-epikinonion/

[102] “Cellular Networks: Past, Present and Future.” Accessed: May 21, 2024. [Online]. Available: https://faculty.kfupm.edu.sa/ics/salah/082/ics343/handouts/mobile/mobileO.html
[103] “(13) GSM Network Architecture | LinkedIn.” Accessed: May 21, 2024. [Online]. Available: https://www.linkedin.com/pulse/gsm-network-architecture-stiven-raid/
[104] “Enterprise Networking, Security, and Automation -Threat Actor Tools.” Accessed: May 21, 2024. [Online]. Available: https://contenthub.netacad.com/ensa/3.3.4
[105] “What is a denial of service attack (DoS) ? - Palo Alto Networks.” Accessed: May 21, 2024. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
[106] “Denial-of-Service (DoS) Attack: Examples and Common Targets.” Accessed: May 21, 2024. [Online]. Available: https://www.investopedia.com/terms/d/denial-service-attack-dos.asp
[107] “Denial of Service (DoS) Attack: Types and Prevention.” Accessed: May 21, 2024. [Online]. Available: https://www.insecure.in/dos-attack
[108] “Rogue access points (article) | Khan Academy.” Accessed: May 21, 2024. [Online]. Available: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks
[109] “This figure shows the setup of a rogue AP. A rogue AP is connected to... | Download Scientific Diagram.” Accessed: May 21, 2024. [Online]. Available: https://www.researchgate.net/figure/This-figure-shows-the-setup-of-a-rogue-AP-A-rogue-AP-is-connected-to-the-wired-network_fig2_224256664
[110] “Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention.” Accessed: May 21, 2024. [Online]. Available: https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html
[111] W. Odom, *CCNA 200-301. Official cert guide, Volume 1*.
[112] “Hiding SSID: Understand the Pros and Cons | Fractional CISO.” Accessed: May 21, 2024. [Online]. Available: https://fractionalciso.com/should-you-hide-your-wi-fi-ssid/
[113] “Open System Authentication, Shared Key Authentication, and Deauthentication – Dot11AP.” Accessed: May 21, 2024. [Online]. Available: https://dot11ap.wordpress.com/open-system-authentication-shared-key-authentication-and-deauthentication/
[114] “What is Shared Key Authentication, and how does it work?” Accessed: May 21, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/Shared-Key-Authentication-SKA
[115] “Central Authentication Service (CAS) Protocol Explained | Okta.” Accessed: May 21, 2024. [Online]. Available: https://www.okta.com/identity-101/central-authentication-service/
[116] “Encryption choices: rsa vs. aes explained | Prey.” Accessed: May 21, 2024. [Online]. Available: https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes
[117] “(PDF) Cryptanalysis of the SEAL Encryption Algorithm.” Accessed: May 21, 2024. [Online]. Available: https://www.researchgate.net/publication/2439273_Cryptanalysis_of_the_SEAL_Encryption_Algorithm
[118] “RC4 Encryption Algorithm - GeeksforGeeks.” Accessed: May 21, 2024. [Online]. Available: https://www.geeksforgeeks.org/rc4-encryption-algorithm/
[119] “How Diffie-Hellman Key Exchange Provides Encrypted Communications | UpGuard.” Accessed: May 21, 2024. [Online]. Available: https://www.upguard.com/blog/diffie-hellman
[120] “RSA Algorithm in Cryptography - GeeksforGeeks.” Accessed: May 21, 2024. [Online]. Available: https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
[121] “Temporal Key Integrity Protocol - an overview | ScienceDirect Topics.” Accessed: May 21, 2024. [Online]. Available: https://www.sciencedirect.com/topics/engineering/temporal-key-integrity-protocol
[122] “What is WPA3? | Definition from TechTarget.” Accessed: May 21, 2024. [Online]. Available:

https://www.techtarget.com/searchsecurity/definition/WPA3
[123] “Wi-Fi Gets More Secure: Everything You Need to Know About WPA3 - IEEE Spectrum.” Accessed: May 21, 2024. [Online]. Available: https://spectrum.ieee.org/everything-you-need-to-know-about-wpa3