ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασύρματα Τοπικά Δίκτυα

Του φοιτητή
Ηλιάδη Φίλιππου
Αρ. Μητρώου: 134010

Επιβλέπων
Ονοματεπώνυμο Βίτσας Βασίλειος
Βαθμίδα ……

Ημερομηνία ……

Τίτλος Δ.Ε. Ασύρματα Τοπικά Δίκτυα
Κωδικός Δ.Ε. …
Ονοματεπώνυμο φοιτητή Φίλιππος Ηλιάδης
Ονοματεπώνυμο εισηγητή …
Ημερομηνία ανάληψης Δ.Ε. …
Ημερομηνία περάτωσης Δ.Ε. …

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.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

«Αφιέρωση»

Πρόλογος

Η παρούσα Διπλωματική εργασία εκπονήθηκε με την επίβλεψη του κ. Βασίλειου Βίτσα καθηγητή του Τμήματος Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε κατά την εαρινή περίοδο του Ακαδημαϊκού Έτους 2022 – 2023. Εντάσσεται στα πλαίσια του Προγράμματος Προπτυχιακών Σπουδών "Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων" του Διεθνούς Πανεπιστημίου Ελλάδος. Πραγματοποιήθηκε με αφορμή την ραγδαία ανάπτυξη των Ασύρματων δικτύων καθώς η ανάγκη για συνεχή χρήση των smartphones και των ηλεκτρονικών υπολογιστών ασχέτως της θέσης που βρίσκεται κάποιος, αυξάνεται διαρκώς. Σκοπός της είναι η κατανόηση του τρόπου λειτουργίας τους, η μελέτη και η ανάλυση των ποικίλων μορφών τους, καθώς και η αναφορά στα πλεονεκτήματα που παρέχουν, σύμφωνα με τις ανάγκες που υπάρχουν σε ένα σπίτι, ένα γραφείο, μια μικρομεσαία επιχείρηση ακόμα και σε μια μεγάλη πόλη ή χώρα. Επίσης, αναλύεται ο τρόπος με τον οποίον υλοποιούνται και οι λύσεις που προσφέρουν εκεί που τα ενσύρματα παραδοσιακά δίκτυα αδυνατούν. Στην συνέχεια, αναφέρεται η ιστορική εξέλιξη των τεχνολογιών αυτών και ο ρόλος που έπαιξαν στην ανάπτυξη των δικτύων που υπάρχουν σήμερα.

Περίληψη

Είναι σχεδόν αδύνατο να κατονομαστούν όλοι οι τομείς της κοινωνίας που μετασχηματίστηκαν σε μεγάλο βαθμό από την ευρεία εξάπλωση του Διαδικτύου. Το μόνο σίγουρο είναι ότι αυτή η επιρροή του Διαδικτύου, αναμένεται να αυξάνεται με σταθερά ανοδικούς ρυθμούς. Βασικός παράγοντας μιας τέτοιας αύξησης αποτελεί η χρήση των τεχνολογιών ασύρματης σύνδεσης και πιο συγκεκριμένα τα ασύρματα τοπικά δίκτυα. Η ανάπτυξη των ασύρματων τοπικών δικτύων αποτελεί πλέον μια πραγματικότητα του σύγχρονου κόσμου σε παγκόσμιο επίπεδο, λόγω των πολλών δυνατοτήτων τους, όπως είναι η υποστήριξη της κινητικότητας των χρηστών και η εύκολη προσαρμογή στις διάφορες απαιτήσεις τους για επικοινωνία. Μια τέτοια ανάπτυξη καθιστά κάτι παραπάνω από επιτακτική την κατανόηση των διαφορετικών τεχνολογιών ασύρματης επικοινωνίας, ώστε σε κάθε περίπτωση να επιλέγεται η καταλληλότερη. Καθώς, η ασύρματη επικοινωνία είναι ένα διαρκώς αναπτυσσόμενο πεδίο, το μέλλον της βασίζεται σε δύο πολύ σημαντικούς παράγοντες, όπως είναι η μεγαλύτερη ασφάλεια και η δυνατότητα υποστήριξης υψηλότερων ρυθμών μετάδοσης δεδομένων.

Λόγω της φύσης της μετάδοσης των ραδιοκυμάτων, η ασύρματη διεπαφή αέρα των ασύρματων τοπικών δικτύων είναι προσβάσιμη στον καθένα. Το συγκεκριμένο ζήτημα καθιστά τις ασύρματες μεταδόσεις πιο ευάλωτες από τις ενσύρματες επικοινωνίες σε κακόβουλες επιθέσεις, όπως η υποκλοπή δεδομένων ή η σκόπιμη παρεμβολή για τη διακοπή των μεταδόσεων. Ως εκ τούτου, για τη βελτίωση της ασφάλειας των ασύρματων τοπικών δικτύων απαιτείται ο σχεδιασμός και η χρήση αποτελεσματικών μηχανισμών προστασίας των δικτύων από κακόβουλες συμπεριφορές. Μερικές φορές όμως, η χρήση τέτοιων μηχανισμών μπορεί να επηρεάσει αισθητά την αποτελεσματικότητα και την απόδοση των ασύρματων τοπικών δικτύων.

Η σταθερά συνεχιζόμενη αύξηση του όγκου των δεδομένων που μεταφέρονται από τα ασύρματα τοπικά δίκτυα σημαίνει ότι τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται θα πρέπει να είναι αποτελεσματικά και παρέχουν καλή απόδοση. Ωστόσο, δεδομένης της κατανεμημένης φύσης της κοινής χρήσης πόρων στα πρωτόκολλα επικοινωνίας IEEE 802.11, που αποτελούν τη βάση ανάπτυξης των διαφόρων τύπων ασύρματων τοπικών δικτύων, οι όποιες λύσεις μεγαλύτερης κάλυψης και χωρητικότητας των συγκεκριμένων δικτύων θα πρέπει να βασίζονται στη σωστότερη διαμόρφωση και ανάπτυξή τους, παρά στη χρήση μεγαλύτερου αριθμού πόρων.

Σκοπός της παρούσας εργασίας, είναι η παρουσίαση μιας όσο το δυνατόν πιο ολοκληρωμένης βιβλιογραφικής ανασκόπησης των ασύρματων τοπικών δικτύων, εστιάζοντας σε δύο βασικούς παράγοντες που επηρεάζουν τη συνολική εξελικτική τους πορεία, όπως είναι η ασφάλεια και η απόδοσή τους. Για το λόγο αυτό είναι ουσιαστικά διαρθρωμένη σε δύο μέρη. Στο πρώτο μέρος θα γίνει μια παρουσίαση των ασύρματων τοπικών δικτύων, η οποία θα αναπτυχθεί σε τρία κεφάλαια. Στο πρώτο, εισαγωγικό κεφάλαιο, θα δοθεί ο ορισμός των ασύρματων τοπικών δικτύων, καθώς και μια ιστορική αναδρομή των ασύρματων δικτύων γενικότερα. Στο δεύτερο κεφάλαιο, θα παρουσιαστούν και θα αναλυθούν τα γενικά χαρακτηριστικά των ασύρματων τοπικών δικτύων, οι τύποι και οι τεχνολογίες τους, τα πλεονεκτήματα και τα μειονεκτήματα που παρουσιάζουν, καθώς και η τρέχουσα κατάσταση των τεχνολογιών ασύρματης δικτύωσης και των προτύπων που χρησιμοποιούνται στα δίκτυα αυτά. Τέλος, στο τρίτο κεφάλαιο θα αναπτυχθούν οι τρόποι μετάδοσης που χρησιμοποιούνται στα ασύρματα τοπικά δίκτυα. Το δεύτερο μέρος της εργασίας ασχολείται με τα ζητήματα της ασφάλειας και της απόδοσης των ασύρματων τοπικών δικτύων. Αρχικά, όσον αφορά την ασφάλεια, θα αναφερθούν τα τρωτά σημεία των ασύρματων τοπικών δικτύων και ο τρόπος εκμετάλλευσής τους για την πραγματοποίηση των απειλών κατά της ασφάλειάς τους. Στη συνέχεια θα παρουσιαστούν τα

πρωτόκολλα κρυπτογράφησης και ελέγχου ταυτότητας, αλλά και κάποιες άλλες πρακτικές, που χρησιμοποιούνται ως τρόποι βέλτιστης προστασίας της ασφάλειας των συγκεκριμένων δικτύων. Όσον αφορά την απόδοση των ασύρματων τοπικών δικτύων, αρχικά θα παρουσιαστούν και θα αναλυθούν οι παράγοντες που την επηρεάζουν, δίνοντας μεγαλύτερη έμφαση στο ζήτημα των παρεμβολών και τον αντίκτυπό του. Στη συνέχεια, θα παρουσιαστούν κάποιες τεχνικές βελτιστοποίησης της απόδοσης των ασύρματων τοπικών δικτύων. Η εργασία ολοκληρώνεται με κάποια συμπεράσματα που προκύπτουν από την ανάλυση όλων των παραπάνω θεμάτων, επισημαίνοντας κάποιες μελλοντικές ερευνητικές κατευθύνσεις που μπορούν να χρησιμοποιηθούν ως βάση αξιοποίησης κάποιων καινοτόμων ιδεών πάνω στον τομέα των ασύρματων τοπικών δικτύων.

Λέξεις κλειδιά: Απόδοση, ασύρματα τοπικά δίκτυα, ασφάλεια, εφαρμογές, πρωτόκολλα επικοινωνίας, τεχνολογίες πληροφοριών και επικοινωνίας.

Ασύρματα Τοπικά Δίκτυα

Wireless Local Networks

Φίλιππος Ηλιάδης

Filippos Iliadis

Abstract

It is almost impossible to name all the sectors of society that have been greatly transformed by the widespread spread of the Internet. The only thing that is certain is that this influence of the Internet is expected to grow at a steadily increasing rate. A key factor in such an increase is the use of wireless technologies, and more specifically wireless local networks. The development of wireless local area networks is now a reality of the modern world at a global level, due to their many capabilities, such as supporting the mobility of users and easily adapting to their various communication requirements. Such a development makes it more than imperative to understand the different wireless communication technologies, so that the most suitable one can be chosen in each case. As wireless communication is a constantly developing field, its future is based on two very important factors, such as greater security and the ability to support higher data rates.

Due to the nature of radio wave transmission, the wireless air interface of wireless LANs is accessible to anyone. This issue makes wireless transmissions more vulnerable than wired communications to malicious attacks, such as data interception or deliberate interference to disrupt transmissions. Therefore, to improve the security of wireless local area networks, the design and use of effective mechanisms to protect networks from malicious behavior is required. Sometimes, however, the use of such mechanisms can significantly affect the efficiency and performance of wireless LANs.

The steadily continuing increase in the volume of data transferred by wireless LANs means that the communication protocols used should be efficient and provide good performance. However, given the distributed nature of resource sharing in the IEEE 802.11 communication protocols, which are the basis of development of the various types of wireless local area networks, any solutions for greater coverage and capacity of these networks should be based on their correct configuration and deployment, rather than in the use of a greater number of resources.

The purpose of this thesis is to present a literature review of wireless local networks as comprehensive as possible, focusing on two main factors that influence their overall evolution, such as security and performance. For this reason, the thesis is essentially structured in two parts. In the first part, we present the concept of wireless local area networks, in three chapters. In the first, introductory chapter, we give the definition of wireless local area networks, as well as a historical overview of wireless networks in general. In the second chapter, we present and analyze the general characteristics of wireless local area networks, their types and technologies, their advantages and disadvantages, as well as the current state of wireless networking technologies and standards. Finally, in the third chapter, we

present the transmission methods used in wireless local networks. The second part of the thesis deals with the security and performance issues of wireless local area networks. First, in terms of security, we discuss the vulnerabilities of wireless local area networks and how they can be exploited in order to achieve security threats. Next, we present the encryption and authentication protocols, as well as some other practices, which are used as ways to optimally protect the security of the specific networks. Regarding the performance of wireless local area networks, we will present and analyze the factors affecting it, giving a greater emphasis on the issue of interference and its impact. Next, we present some techniques for optimizing the performance of wireless local area networks. The thesis concludes with some thoughts about some future research directions that can be used as a basis for exploiting some innovative ideas in the field of wireless local networks.

Keywords: Applications, communication protocols, information and communication technologies, performance, security, wireless local area networks.

Ευχαριστίες

Σε αυτήν την ενότητα ο φοιτητής/ φοιτήτρια προαιρετικά μπορεί να ευχαριστήσει όσους αισθάνεται ότι συνέβαλαν (επιστημονικά, ηθικά, οικονομικά κτλ) στην ολοκλήρωση της διπλωματικής εργασίας.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

ACI	Adjacent Channel Interference
AES	Advanced Encryption Standard
AM	Amplitude Modulation
AMPS	Advanced Mobile Phone System
AP	Access Point
ASK	Amplitude Shift Keying
BFA	Brute Force Attacks
BPSK	Binary Phase Shift Keying
BS	Buffer Size
CA	Certificate Authorities
CBC-MAC	Cipher Block Chaining Message Authentication
CCA	Chosen Cipher Attacks
CCI	Co-Channel Interference
CCK	Complementary Code Keying
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CDMA	Code Division Multiple Access
CHAP	Challenge Handshake Protocol
CIA	Confidentiality, Integrity, Availability
COA	Ciphertext Only Attacks
CRC	Cyclic Redundancy Code
CSI	Channel State Information
CTR	Counter mode
CW	Contention Window
DFS	Dynamic Frequency Selection
DoS	Denial of Service
DQPSK	Differential Quaternary Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
DVB	Digital Video Broadcasting
EAP	Extensible Authentication Protocol
EAP-AKA	EAP with Authentication and Key Agreement
EAP-FAST	EAP with Flexible Authentication via Secure Tunneling

EAP-MD5	EAP with Message Digest 5
EAP-SIM	EAP for GSM Subscriber Identity Modules
EAP-SRP	EAP with Secure Remote Password
EAP-TLS	EAP with Transport Layer Security
EAP-TTLS	EAP with Tunneled TLS
EDGE	Enhanced Data Rate for GSM Evolution
EMI	ElectroMagnetic Interference
EVDO	Evolution-Data Optimized
FCC	Federal Communications Commission
FDD	Frequency Division Multiplexing
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
FSK	Frequency Shift Keying
FTV	Fragmentation Threshold Value
GFSK	Gaussian Frequency Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HSUPA/HSDPA	High Speed Uplink/Downlink Packet Access
ICI	Inter Carrier Interference
ICV	Integrity Check Value
IDPS	Intrusion Detection and Prevention Systems
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IFS	Interframe Space
IMTS	Improved Mobile Telecommunications Systems
IoT	Internet of Things
ISI	Inter Symbol Interference
ISM	International, Scientific, and Medical
ITU	International Telecommunication Union
KPA	Known Plaintext Attacks

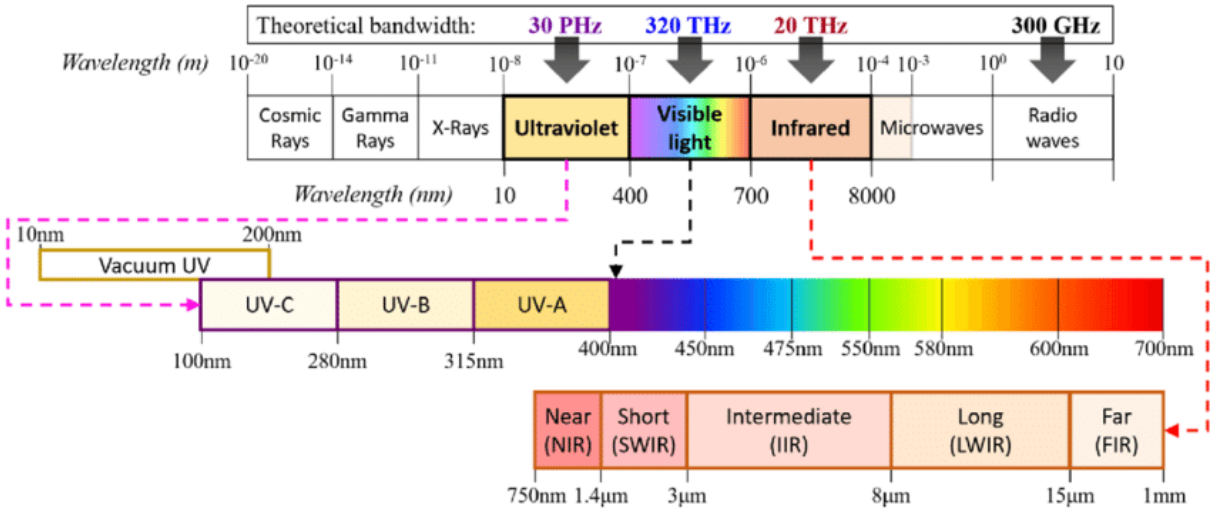
LBS	Location-Based Services
LEAP	Lightweight Extensible Authentication Protocol
MIC	Message Integrity Code
MIMO	Multiple Input Multiple Output
MISO	Multi Input Single Output
MMS	Multimedia Messaging Service
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NMT	Nordic Mobile Telephone system
OFDM	Orthogonal Frequency Division Multiplexing
OSA	Open System Authentication
PAC	Per Antenna Coding
PAPR	Peak to Average Power Ratio
PCS	Personal Communications System
PEAP	Protected EAP
PSK	Phase Shift Keying
QAM	Quadrature amplitude modulation
RADIUS	Remote Authentication Dial-In User Service
RFI	Radio Frequency Interference
RMCAT	Real-Time Media Congestion Avoidance
RSTV	Request to Send Threshold Value
SDM	Space Division Multiplexing
SGI	Short Guard Interval
SS	Spread Spectrum
SSID	Service Set Identifier
STBC	Space Time Block Coding
TACS	Total Access Communication System
TDMA	Time Division Multiplexing
TKIP	Temporal Key Integrity Protocol
TPS	Transmit Power Control
USDC	US Digital Cellular
UMTS	Universal Mobile Telecommunications Systems
VoIP	Voice over Internet Protocol

VPN	Virtual Private Network
WBAN	Wireless Body Area Networks
WCDMA	Wideband Code Division Multiple Access
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan Area Networks
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Networks
WWAN	Wireless Wide Area Networks

Κεφάλαιο 1ο: Εισαγωγή

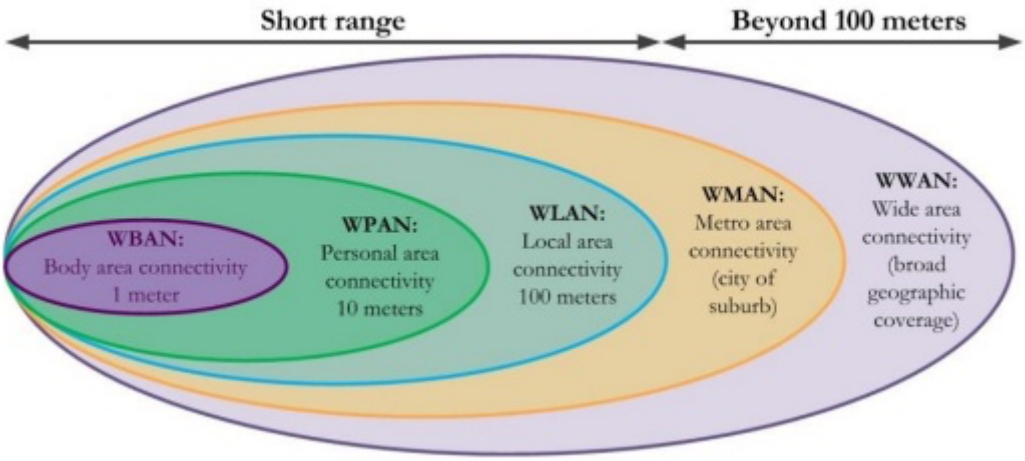
1.1 Τι είναι τα ασύρματα τοπικά δίκτυα

Η ασύρματη επικοινωνία είναι ένας από τους πιο επιθυμητούς τρόπους επικοινωνίας μεταξύ δύο ή περισσότερων συσκευών. Σε αντίθεση με τα ενσύρματα συστήματα επικοινωνίας, όπου η μεταφορά των δεδομένων μεταξύ των συσκευών πραγματοποιείται με χρήση καλωδίων, τα ασύρματα δίκτυα αποτελούν τον ευκολότερο τρόπο επικοινωνίας, καθώς η μετάδοση των πληροφοριών πραγματοποιείται μέσω της χρήσης ηλεκτρομαγνητικών κυμάτων, όπως ραδιοσυχνοτήτων ή υπέρυθρων [1]. Στην περίπτωση της χρήσης ραδιοσυχνοτήτων, ένα ασύρματο δίκτυο επικοινωνίας λειτουργεί σε συγκεκριμένη ζώνη του ηλεκτρομαγνητικού φάσματος, η οποία αναφέρεται ως ζώνη ραδιοκυμάτων (από 3Hz έως 300GHz) (Εικ. 1.1) [2].



Εικόνα 1.1: Το ηλεκτρομαγνητικό φάσμα [2]

Οι συνεχιζόμενες εξελίξεις στις Τεχνολογίες της Πληροφορίας και των Επικοινωνιών (ΤΠΕ) έχουν οδηγήσει σε μια συνεχώς αυξανόμενη τάση της χρήσης των ασύρματων επικοινωνιών. Με τον τρόπο αυτό, τα ασύρματα δίκτυα έχουν καταστεί μέσα ραγδαίου μετασχηματισμού πολλών τομέων της σύγχρονης ζωής και της οικονομίας, από την περιβαλλοντική παρακολούθηση έως τη διαχείριση των εταιρειών και από τον αυτοματισμό της βιομηχανίας έως την βελτιστοποίηση της υγειονομικής περίθαλψης. Η ταυτόχρονη λειτουργία τεράστιου αριθμού ασύρματων συνδέσεων και ζεύξεων έχει δημιουργήσει τη δυνατότητα της υιοθέτησης των ασύρματων επικοινωνιών, σε μια τεράστια γκάμα ποικίλων εφαρμογών, με διαφορετικές απαιτήσεις όσον αφορά την κάλυψη καθώς και τη χωρητικότητα [3]. Λόγω της δυναμικής φύσης των απαιτήσεων αυτών των διαφόρων εμπορικά καθοδηγούμενων εφαρμογών, έχουν αναπτυχθεί διαφορετικές μέθοδοι και πρότυπα ασύρματης επικοινωνίας, τα οποία μπορούν να ταξινομηθούν με βάση την εμβέλεια κάλυψης της μετάδοσης των δεδομένων. Μια τέτοια ταξινόμηση των ασύρματων δικτύων επικοινωνίας δημιουργεί σε γενικές γραμμές πέντε επιμέρους κατηγορίες (Εικ. 1.2) [4]: (α) τα δίκτυα WBAN, (β) τα δίκτυα WPAN, (γ) τα δίκτυα WLAN, (δ) τα δίκτυα WMAN και (ε) τα δίκτυα WWAN. Εκτός από την εμβέλεια κάλυψης, αυτές οι κατηγορίες ασύρματων δικτύων επικοινωνίας παρουσιάζουν διαφορές και ως προς τον ρυθμό μετάδοσης των δεδομένων.



Εικόνα 1.2: Ταξινόμηση ασύρματων δικτύων επικοινωνίας [4]

Τα ασύρματα δίκτυα περιοχής σώματος WBAN (Wireless Body Area Networks) αποτελούν δίκτυα που χαρακτηρίζονται από κάλυψη μόνο λίγων μέτρων. Τα δίκτυα WBAN αποτελούνται από συσκευές wearable, οι οποίες σχηματίζοντας μια ad hoc τοπολογία, μπορούν να κατανεμηθούν πάνω και/ή κοντά στο ανθρώπινο σώμα για παρακολούθηση των φυσικών (βιομετρικών) παραμέτρων της κατάστασης της υγείας του ατόμου [3].

Τα ασύρματα δίκτυα προσωπικής περιοχής WPAN (Wireless Personal Area Networks) χρησιμοποιούνται για επικοινωνία μεταξύ συσκευών που είναι σχετικά κοντά, συνήθως εντός του χώρου εργασίας ενός ατόμου. Οι ραδιοζεύξεις των δικτύων WPAN θεωρητικά έχουν εμβέλεια λιγότερη από 10m, αν και κάποιες τεχνολογίες, όπως οι Bluetooth και Zigbee, παρουσιάζουν πολύ ευρύτερες περιοχές κάλυψης [3]. Σε αρκετές ταξινομήσεις των ασύρματων δικτύων, στα δίκτυα WPAN συμπεριλαμβάνονται και τα WBAN [5].

Τα ασύρματα τοπικά δίκτυα WLAN (Wireless Local Area Networks) αποτελούν δίκτυα επικοινωνίας που έχουν σχεδιαστεί για να παρέχουν ασύρματη πρόσβαση σε συσκευές εντός μιας περιορισμένης περιοχής τυπικής έκτασης 100m (π.χ. σπίτια, σχολεία, κτίρια, κλπ.). Ένας τέτοιος σχεδιασμός έχει αυξήσει τη δημοτικότητα των δικτύων WLAN, καθώς μπορούν να παρέχουν όλες τις υπηρεσίες ενός ενσύρματου τοπικού δικτύου με το πρόσθετο πλεονέκτημα της φορητότητας της συσκευής πελάτη, αποφεύγοντας παράλληλα το κόστος που σχετίζεται με την καλωδίωση εντός της περιοχής κάλυψης του δικτύου. Ταυτόχρονα, μέσω ενός σημείου πρόσβασης (Access Point – AP), ένα δίκτυο WLAN μπορεί επίσης να παρέχει σύνδεση σε συσκευές, όπως laptop, smartphone και tablet, στο ευρύτερο Διαδίκτυο [6]. Το 1997, θεωρείται έτος ορόσημο για τα δίκτυα WLAN, όταν ο οργανισμός IEEE (Institute of Electrical and Electronics Engineers) κυκλοφόρησε την πρώτη έκδοση του προτύπου IEEE 802.11, το οποίο όριζε το φυσικό επίπεδο και το επίπεδο της ζεύξης δεδομένων της ασύρματης δικτύωσης. Το 1999, δημιουργήθηκε η Wi-Fi Alliance ως εμπορικός σύλλογος για την κατοχύρωση του εμπορικού σήματος Wi-Fi, υπό το οποίο πωλούνται τα περισσότερα προϊόντα που ακολουθούν το πρότυπο IEEE 802.11. Σκοπό της ήταν να παρέχει στους χρήστες την ελευθερία να συνδέονται στο Διαδίκτυο από οποιοδήποτε μέρος. Αν και αυτή η υπηρεσία ήταν αρκετά ακριβή μέχρι το 2002, η τροποποίηση IEEE 802.11g του βασικού προτύπου έδωσε τη δυνατότητα δημιουργίας φθηνών συσκευών με δυνατότητα Wi-Fi, με αποτέλεσμα σήμερα ένας δρομολογητής Wi-Fi να αποτελεί πλέον ένα βασικό εξοπλισμό πρόσβασης στο Διαδίκτυο για τα περισσότερα σύγχρονα σπίτια [4].

Τα ασύρματα δίκτυα μητροπολιτικής περιοχής WMAN (Wireless Metropolitan Area Networks) παρέχουν συνδεσιμότητα σε μια περιοχή πολλών χιλιομέτρων, υποστηρίζοντας την επικοινωνία

μεταξύ διαφορετικών κτιρίων μιας μεγάλης πανεπιστημιούπολης ή μιας πόλης. Παράδειγμα δικτύων WMAN αποτελούν τα δίκτυα WiMAX, η λειτουργία των οποίων βασίζεται στο πρότυπο IEEE 802.16-2004 και μπορούν να αποτελέσουν λύση κάλυψης των αυξανόμενων αναγκών των χρηστών για πρόσβαση σε υπηρεσίες ασύρματης ευρυζωνικής σύνδεσης BWA (Broadband Wireless Access) [3].

Τα ασύρματα δίκτυα ευρείας περιοχής WWAN (Wireless Wide Area Networks) παρουσιάζουν ευρύτερες περιοχές κάλυψης από τα δίκτυα WMAN (μεγαλουπόλεις ή ακόμη και χώρες). Παράδειγμα δικτύων WWAN αποτελούν όλα τα κυψελοειδή δίκτυα (GSM, UMTS, LTE, 4G, 5G) [3].

1.2 Ιστορική αναδρομή των ασύρματων δικτύων

Η δυνατότητα της μετάδοσης πληροφοριών χωρίς τη χρήση καλωδίων φαινόταν να είναι κάτι αδιανόητο τον 19ο αιώνα. Ως κομβικό σημείο της εμφάνισης των ασύρματων δικτύων και της ανάπτυξης της τεχνολογίας των ραδιοεπικοινωνιών, μπορεί να θεωρηθεί το 1896, όταν ο Ιταλός φυσικός και εφευρέτης G. Marconi μετέδωσε με επιτυχία το πρώτο ασύρματο ραδιοφωνικό σήμα, αποδεικνύοντας τη δυνατότητα για ασύρματη επικοινωνία. Έκτοτε, τα τελευταία 100 και πλέον χρόνια, νέες μέθοδοι και τεχνολογίες ασύρματης επικοινωνίας έχουν εμφανιστεί και εξελιχθεί [7]. Το 1901, ο Marconi πραγματοποίησε την πρώτη πετυχημένη ασύρματη τηλεγραφική μετάδοση αποστολής και λήψης σήματος Morse χρησιμοποιώντας πομπούς υψηλής ισχύος και ραδιοκύματα μεγάλου μήκους κύματος. Το 1907, ξεκίνησε η πρώτη εμπορική υπερατλαντική ασύρματη υπηρεσία, χρησιμοποιώντας τεράστιους επίγειους σταθμούς και ιστούς κεραιών 30m x 100m. Κατά τη διάρκεια του Πρώτου Παγκοσμίου Πολέμου παρουσιάστηκε μια σχετικά ταχεία ανάπτυξη της ευφυΐας των επικοινωνιών, της τεχνολογίας της κρυπτογραφίας και των υποκλοπών και γενικά τεχνολογιών που αργότερα αποτέλεσαν βασικά συστατικά του σχεδιασμού των σύγχρονων ασύρματων συστημάτων [8].

Το 1915, επιτεύχθηκε ασύρματη φωνητική μετάδοση μεταξύ της Νέας Υόρκης και του Σαν Φρανσίσκο και το 1920, πραγματοποιήθηκε η πρώτη εκπομπή ραδιοφωνικού σταθμού στο Πίτσμπουργκ της Πενσυλβάνια. Το 1921, τα περιπολικά της αστυνομίας στο Ντιτρόιτ του Μίσιγκαν εξοπλίστηκαν με ασύρματες συσκευές επικοινωνίας (dispatch radios). Κατά τη διάρκεια του Δεύτερου Παγκοσμίου Πολέμου, παρουσιάστηκε μια σημαντική ανάπτυξη των ασύρματων συστημάτων επικοινωνίας με χρήση ραδιοσυχνοτήτων για την υποστήριξη των πολεμικών επιχειρήσεων [9].

Μετά το τέλος του πολέμου, το 1946 ξεκίνησε η πρώτη ασύρματη δημόσια τηλεφωνική υπηρεσία σε 25 μεγάλες πόλεις των ΗΠΑ. Το σύστημα που δημιουργήθηκε χρησιμοποιούσε εύρος ζώνης ραδιοσυχνοτήτων 120kHz και λειτουργούσε με ημιαμφίδρομη επικοινωνίας. Στη συνέχεια, το 1950, ο οργανισμός FCC (Federal Communications Commission) στις ΗΠΑ διπλασίασε τον αριθμό των χρησιμοποιούμενων καναλιών επικοινωνίας, μειώνοντας το εύρος ζώνης στα 60kHz. Το 1960, στο πλαίσιο της δημιουργίας των συστημάτων IMTS (Improved Mobile Telecommunications Systems), το εύρος ζώνης μειώθηκε ξανά (στα 30kHz), ενώ τα συστήματα μπορούσαν να προσφέρουν πλήρως αμφίδρομη επικοινωνία και δυνατότητες αυτόματης κλήσης. Την ίδια περίοδο, το 1958, στην Γερμανία παρουσιάστηκε το αναλογικό σύστημα A-Netz, το οποίο λειτουργούσε στα 160Mhz και παρουσίαζε δυνατότητες κάλυψης της τάξης του 80%. Οι κλήσεις στο σύστημα μπορούσαν να πραγματοποιηθούν μόνο μέσω κινητών τερματικών και μέχρι το 1971, οι χρήστες του συστήματος έφτασαν τους 11.000 [7].

Το 1968, η αμερικανική εταιρεία AT&T πρότεινε την ιδέα της κυψελοειδούς επικοινωνίας στον οργανισμό FCC. Μέχρι το 1976, το σύστημα Bell Mobile μπορούσε να υποστηρίξει την επικοινωνία

543 πελατών στην ευρύτερη μητροπολιτική περιοχή της νέας Υόρκης, χρησιμοποιώντας 12 κανάλια. Εν τω μεταξύ στη Γερμανία, το 1972, παρουσιάστηκε το σύστημα B-Netz, το οποίο είχε τα ίδια χαρακτηριστικά με το A-Netz, αλλά παρουσίαζε τη δυνατότητα πραγματοποίησης κλήσεων από το σταθερό δίκτυο, εάν η θέση του κινητού τερματικού ήταν γνωστή εκ των προτέρων. Το σύστημα χρησιμοποιήθηκε από 13.000 χρήστες στη Γερμανία, αλλά και από μεγάλο αριθμό χρηστών στην Αυστρία, το Λουξεμβούργο και την Ολλανδία [10].

Αν και η έννοια της κινητής τηλεφωνίας είχε αναπτυχθεί ήδη από την αμερικανική εταιρεία Bell Labs το 1947, το πρώτο κυψελοειδές κινητό σύστημα ξεκίνησε τη λειτουργία του τον Αύγουστο του 1981 στη Σουηδία, με την ονομασία NMT (Nordic Mobile Telephone) system. Το σύστημα NMT ακολούθησαν το σύστημα TACS (Total Access Communication System) στην Αυστρία (το 1984), στην Ιταλία και στο Ηνωμένο Βασίλειο (το 1985), το C-450 στην Γερμανία, καθώς και το Radiocom2000 στη Γαλλία. Αυτά τα διαφορετικά ευρωπαϊκά συστήματα ανήκουν στην πρώτη γενιά κυψελοειδών δικτύων (1G) και ήταν εντελώς ασύμβατα μεταξύ τους [11].

Το 1983, στις ΗΠΑ έγινε η πρώτη παροχή υπηρεσιών μέσω κυψελοειδών δικτύων, όταν έκανε την εμφάνισή του το σύστημα AMPS (Advanced Mobile Phone System). Το AMPS διέθετε συνολικά 666 κανάλια αμφίδρομης επικοινωνίας, με το καθένα να αποτελείται από ένα ζευγάρι μονόδρομων καναλιών. Τα κανάλια καταλάμβαναν 40MHz στη ζώνη συχνοτήτων των 800MHz (τα κανάλια μετάδοσης στις συχνότητες 824 - 849MHz και τα κανάλια λήψης στις συχνότητες 869 - 894MHz) και είχαν εύρος ζώνης 30kHz, εξυπηρετώντας μόνο έναν χρήστη τη φορά [12].

Το 1985, ο οργανισμός FCC όρισε τις μη αδειοδοτημένες μπάντες συχνοτήτων ISM (International, Scientific, and Medical), μια πράξη που έμελλε να αποτελέσει κομβικό σημείο για την ανάπτυξη των δικτύων WLAN, καθώς αποτελεί μια μη αδειοδοτημένη ζώνη συχνοτήτων που χρησιμοποιείται από τα περισσότερα σύγχρονα ασύρματα δίκτυα. Την ίδια περίοδο στην Ευρώπη αναπτύχθηκε ένα ενιαίο ψηφιακό πανευρωπαϊκό πρότυπο, το GSM (Global System for Mobile communications), το οποίο άρχισε να σχεδιάζεται το 1982 και τελικά ανακοινώθηκε επίσημα για πρώτη φορά το 1990. Το 1989, ο οργανισμός FCC χορήγησε επιπλέον 166 κανάλια (10MHz) στο σύστημα AMPS. Το 1991, κυκλοφόρησε το σύστημα USDC (US Digital Cellular) ή IS-54 στις ΗΠΑ, το οποίο αρχικά υποστήριζε τρεις χρήστες σε κάθε κανάλι των 30kHz και αργότερα βελτιώθηκε για να φιλοξενήσει έξι χρήστες ανά κανάλι [13].

Όλα τα πρότυπα που αναπτύχθηκαν τη δεκαετία του 1980 υποστήριζαν μόνο φωνητική επικοινωνία και χρησιμοποιούσαν διάφορους τύπους διαμόρφωσης, όπως FM (Frequency Modulation) για ομιλία, FSK (Frequency Shift Keying) για σηματοδότηση και FDMA (Frequency Division Multiple Access) για πρόσβαση στο μέσο. Μόνο αργότερα, στη δεκαετία του 1990, τα πρότυπα GSM και IS-95 εξελίχθηκαν για να συμπεριλάβουν ασύρματη μετάδοση δεδομένων ως αναπόσπαστο μέρος του συνόλου των υπηρεσιών τους. Τα πρότυπα που αναπτύχθηκαν αργότερα στη δεκαετία του 1990 βασίστηκαν σε μεθόδους πρόσβασης όπως οι FDMA, TDMA (Time Division Multiplexing), CDMA (Code Division Multiple Access) και FDD (Frequency Division Multiplexing) [7].

Τη διετία 1993-94, η μπάντα των 1,8GHz χρησιμοποιήθηκε από τα συστήματα PCS (Personal Communications System), IS-95 CDMA και GPRS (General Packet Radio Service). Με την έλευση των νέων ψηφιακών προτύπων, η ασύρματη επικοινωνία δεδομένων έγινε πιο διαδεδομένη. Αυτά τα πρότυπα υποστήριζαν ταχύτητες μετάδοσης δεδομένων από 9,6 έως 14,4kbps και ονομάστηκαν κινητά συστήματα δεύτερης γενιάς (2G). Βασικά, τα δίκτυα 2G χρησιμοποιούσαν μεταγωγή κυκλώματος, κάτι που αποδείχθηκε βέλτιστο για τις φωνητικές επικοινωνίες, οι οποίες απαιτούν μικρή καθυστέρηση (latency). Ταυτόχρονα όμως αποδείχθηκαν σχετικά αναποτελεσματικά για τις

επικοινωνίες δεδομένων, γεγονός που οδήγησε σε ερευνητικές προσπάθειες προς την κατεύθυνση της μεταγωγής πακέτων [7].

Παρά τις όποιες βελτιώσεις έγιναν στα δίκτυα 2G, τα συστήματα δεν μπορούσαν να υποστηρίξουν ποιότητα υπηρεσιών (QoS) και ταυτόχρονη επικοινωνία πολλών μερών. Τα δίκτυα 2.5G ουσιαστικά είναι μια ασύρματη τεχνολογία που γεφυρώνει τα 2G και 3G και συνήθως προσυπογράφει ένα κυψελοειδές σύστημα δεύτερης γενιάς που ενσωματώνει υπηρεσίες GPRS και εξελιγμένες τεχνολογίες που δεν προσφέρονται στα δίκτυα 2G ή 1G. Ενώ τα 2G και 3G έχουν επίσημα οριστεί ως ασύρματα πρότυπα από τη διεθνή ένωση ITU (International Telecommunication Union), το 2.5G δεν θεωρείται ως πρότυπο και δημιουργήθηκε μόνο για σκοπούς μάρκετινγκ. Ως ενδιάμεσο βήμα των δικτύων 2G και 3G, ένα σύστημα 2.5G χρησιμοποιεί γενικά πλαίσια συστήματος 2G με ενσωμάτωση κάποιων από τις τεχνολογικές εξελίξεις που υιοθετήθηκαν αργότερα από τα δίκτυα 3G, όπως είναι ο συνδυασμός της μεταγωγής πακέτων με τη μεταγωγή κυκλώματος. Η τεχνική μεταγωγής πακέτων επιτρέπει στα δίκτυα 2.5G να παρέχει και υπηρεσίες μεταφοράς δεδομένων επιπρόσθετα των υπηρεσιών μεταφοράς ηχητικού σήματος. Η εξέλιξη από 2G σε 3G εισήγαγε ταχύτερη και μεγαλύτερη χωρητικότητα μετάδοσης δεδομένων, υποστηρίζοντας ρυθμό μετάδοσης δεδομένων μέχρι 144Kbps και παρέχοντας καλύτερες και ποιοτικότερες υπηρεσίες στους χρήστες. Πολλές τεχνολογίες που θεωρήθηκαν ως βήματα εξέλιξης προς το 3G περιλαμβάνουν το EDGE (Enhanced Data Rate for GSM Evolution) (μέρος της οικογένειας GSM) και το CDMA 2000. Μερικές φορές οι τεχνολογίες αυτές θεωρούνται 3G δεδομένου ότι πληρούν ορισμένες από τις απαιτήσεις της ITU για τα πρότυπα 3G [14].

Η τρίτη γενιά κινητής τηλεφωνίας (3G) δημιουργήθηκε στα τέλη του 2000 βασιζόμενη σε ένα σύνολο διεθνών προτύπων, το IMT-2000 της ITU. Οι τεχνολογίες 3G έχουν δυνατότητα μετάδοσης δεδομένων μεγαλύτερης ταχύτητας, που φτάνει τα 2Mbps, μεγαλύτερη χωρητικότητα δικτύου και πιο προηγμένες υπηρεσίες. Τα συστήματα τρίτης γενιάς συγχωνεύουν κινητή πρόσβαση υψηλής ταχύτητας σε υπηρεσίες με βάση το πρωτόκολλο Internet (IP). Με αυτόν τον τρόπο υποστηρίζουν υπηρεσίες που δεν ήταν διαθέσιμες σε παλαιότερες γενιές ασύρματων δικτύων κινητής τηλεφωνίας, όπως ταυτόχρονη χρήση υπηρεσιών ομιλίας και δεδομένων, βιντεοκλήσεις (video calling), τηλεδιάσκεψη (video conference), κινητή τηλεόραση (mobile TV), κινητό Διαδίκτυο (mobile Internet), downloading, υπηρεσίες βασιζόμενες στην τοποθεσία LBS (Location-Based Services), καθώς και υπηρεσίες τηλεϊατρικής (telemedicine). Εκτός από τις παραπάνω βελτιώσεις, πραγματοποιήθηκε αναβάθμιση της ποιότητας υπηρεσιών (QoS) με βάση τις αυξανόμενες απαιτήσεις των χρηστών. Πρόσθετες παροχές όπως η παγκόσμια περιαγωγή (roaming) και η βελτιωμένη ποιότητα φωνής καθιστούν την 3G ως μια αξιόλογη γενιά, αν και η επιτυχία του 2G είναι δύσκολο να επαναληφθεί. Το κύριο μειονέκτημα των κινητών τηλεφώνων 3G είναι ότι χρειάζονται μεγαλύτερη ισχύ από τα περισσότερα μοντέλα 2G. Επιπρόσθετα, ο σχεδιασμός ενός δικτύου 3G είναι πιο δαπανηρός σε σύγκριση με τον αντίστοιχο σχεδιασμό ενός δικτύου 2G. Τα δίκτυα τρίτης γενιάς περιλαμβάνουν μια πλειάδα τεχνολογιών, όπως οι WCDMA (Wideband Code Division Multiple Access), UMTS (Universal Mobile Telecommunications Systems) και CDMA 2000. Η προσθήκη ακόμα πιο εξελιγμένων τεχνολογιών όπως οι HSUPA/HSDPA (High Speed Uplink/Downlink Packet Access) και EVDO (Evolution-Data Optimized) δημιούργησε μια ενδιάμεση ασύρματη γενιά δικτύων μεταξύ των 3G και 4G, την επονομασμένη 3.5G, με βελτιωμένη ταχύτητα μεταφοράς δεδομένων που κυμαίνεται από 5 έως 30 Mbps [14].

Τα δίκτυα κινητής τηλεφωνίας τέταρτης γενιάς (4G), παρουσιάστηκαν στις αρχές της δεκαετίας του 2010. Το 2008, η οργάνωση ITU-R καθόρισε τις IMT-Advanced απαιτήσεις για τα πρότυπα 4G, καθορίζοντας τη μέγιστη ταχύτητα των υπηρεσιών 4G στα 100Mbps για επικοινωνία υψηλής

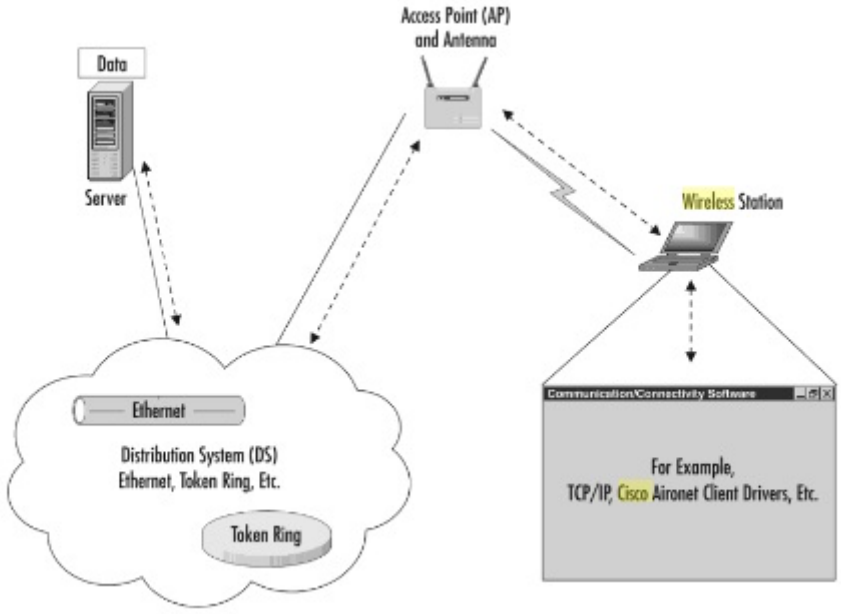
κινητικότητας (όπως για παράδειγμα η επικοινωνία που πραγματοποιείται μέσω κινούμενων οχημάτων) και στο 1Gbps για επικοινωνία χαμηλής κινητικότητας (όπως για παράδειγμα η επικοινωνία πεζών ή σταθερών χρηστών). Ένα σύστημα 4G βελτιώνει τα υπάρχοντα δίκτυα επικοινωνιών, προσδίδοντας μια ολοκληρωμένη, αξιόπιστη και ασφαλή λύση ευρυζωνικής σύνδεσης που βασίζεται στο πρωτόκολλο IP. Με τον τρόπο αυτό ευρυζωνική σύνδεση μπορεί να έχουν laptop με ασύρματα modem, smartphone καθώς και κάθε άλλου είδους φορητές συσκευές. Παροχές και υπηρεσίες φωνής, δεδομένων και πολυμέσων μπορούν έτσι να αξιοποιηθούν από τους χρήστες οποτεδήποτε και από παντού και μάλιστα σε πολύ υψηλότερες ταχύτητες σε σχέση με προηγούμενες γενιές. Εφαρμογές που δημιουργήθηκαν για χρήση ενός δικτύου 4G είναι η ευρυζωνική πρόσβαση στο Internet, η τηλεφωνία IP, η υπηρεσία MMS (Multimedia Messaging Service), η ψηφιακή μετάδοση DVB (Digital Video Broadcasting), η συνομιλία μέσω βίντεο (video chat) και το mobile TV. Η τρίτη γενιά εταιρικής σχέσης έργου (third generation partnership project - 3GPP) προώθησε τεχνολογίες που προϋπήρξαν του 4G, όπως το LTE, που κυκλοφόρησε το 2009, και το WIMAX, που βγήκε στην αγορά το 2006, ως πρότυπα 4G, παρά το γεγονός ότι οι εκδόσεις των τεχνολογιών αυτών δεν πληρούσαν τις αρχικές απαιτήσεις της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU-R) όσον αφορά το ρυθμό μετάδοσης δεδομένων. Η πληρότητα των απαιτήσεων ταχύτητας εξασφαλίστηκε το 2011, όταν η 3GPP καθιέρωσε ως πρότυπο το LTE-A (LTE Advanced), μια αναβάθμιση του LTE [14].

Με την εκθετική αύξηση που παρουσιάζουν οι απαιτήσεις των χρηστών, η αντικατάσταση του 4G με μια προηγμένη τεχνολογία, όπως το 5G, είναι επιτακτική. Τα κινητά και ασύρματα δίκτυα πέμπτης γενιάς (5G) μπορεί να θεωρηθούν ως μια πλήρη ασύρματη επικοινωνία χωρίς περιορισμούς, που οδηγεί προς τον τέλειο κόσμο του ασύρματου World Wide Wireless Web (WWWW). Τα δίκτυα 5G, που πρωτοεμφανίστηκαν το 2019, παρουσιάζουν σημαντικά μεγαλύτερες ταχύτητες λήψης και μεταφόρτωσης από τα δίκτυα 4G, καθώς και μικρότερη καθυστέρηση. Τα δίκτυα 5G δίνουν τη δυνατότητα στους ανθρώπους να απολαμβάνουν ακόμη περισσότερες εφαρμογές που απαιτούν υψηλό εύρος ζώνης, όπως η επαυξημένη και εικονική πραγματικότητα. Ακόμη, έχουν τη δυνατότητα να υποστηρίζουν συσκευές Internet of Things (IoT) σε μεγαλύτερη κλίμακα. Η ανάπτυξη των δικτύων 5G βρίσκεται σε εξέλιξη [15].

Κεφάλαιο 2ο: Ασύρματα τοπικά δίκτυα

2.1 Γενικά χαρακτηριστικά ασύρματων τοπικών δικτύων

Ένας καλός τρόπος απεικόνισης των λειτουργιών ενός δικτύου είναι η παρουσίαση της αρχιτεκτονικής δομής του. Αυτή η δομή περιγράφει τα πρωτόκολλα, τον βασικό εξοπλισμό και το κομμάτι του λογισμικού που το αποτελούν. Η γενική αρχιτεκτονική δομή ενός δικτύου WLAN περιλαμβάνει διάφορες συσκευές και δομές, οι οποίες δεν καθορίζονται στο σύνολό τους από τα πρότυπα IEEE 802.11, αλλά εξαρτώνται από τις εκάστοτε απαιτήσεις των χρηστών [16]. Παρόλα αυτά, ένα τυπικό δίκτυο WLAN αποτελείται από τέσσερα βασικά στοιχεία (Εικ. 2.1) [17]: (α) το σύστημα διανομής, (β) τα σημεία AP, (γ) το ασύρματο μέσο μετάδοσης και (δ) τους σταθμούς.



Εικόνα 2.1: Βασικά στοιχεία δικτύων WLAN [17]

Όταν σε ένα δίκτυο WLAN απαιτείται η σύνδεση πολλών σημείων AP με σκοπό την επέκταση της περιοχής κάλυψης, τα σημεία αυτά θα πρέπει να επικοινωνούν μεταξύ τους για να παρακολουθούν τις κινήσεις των κινητών σταθμών. Σε μια τέτοια περίπτωση τα πρωτόκολλα ασύρματης επικοινωνίας (π.χ. IEEE 802.11) περιλαμβάνουν ένα σύστημα διανομής (Distribution System - DS), το οποίο αφορά ένα λογικό στοιχείο που χρησιμοποιείται για προώθηση των πλαισίων δεδομένων, που μεταφέρονται εντός του δικτύου, προς τον προορισμό τους. Καθώς στα πρωτόκολλα ασύρματης επικοινωνίας δεν καθορίζεται κάποια συγκεκριμένη τεχνολογία για το σύστημα διανομής, στο πλείστο των περιπτώσεων, ένα τέτοιο σύστημα υλοποιείται ως το δίκτυο κορμού (backbone network) (π.χ. Ethernet), που χρησιμοποιείται για τη μετάδοση των πλαισίων δεδομένων μεταξύ των σημείων AP. Τα σημεία AP ενός δικτύου WLAN ουσιαστικά είναι συσκευές του δικτύου, που πραγματοποιούν μια σειρά από λειτουργίες δικτύωσης, η σημαντικότερη από τις οποίες είναι γεφύρωση μεταξύ του ασύρματου και του ενσύρματου μέρους ενός δικτύου. Η μετάδοση των πλαισίων δεδομένων μεταξύ των σημείων AP και των σταθμών σε ένα δίκτυο WLAN πραγματοποιείται μέσω της χρήσης κάποιου ασύρματου μέσου (wireless medium). Στα δίκτυα WLAN αυτό το μέσο μετάδοσης καθορίζεται από το φυσικό επίπεδο (Physical Layer – PHY) του μοντέλου αναφοράς OSI (Open Systems Interconnection) και μπορεί να είναι ραδιοκύματα ή υπέρυθρες συχνότητες, με τη χρήση των ραδιοκυμάτων να αποτελεί τη δημοφιλέστερη λύση στις πρακτικές υλοποιήσεις των δικτύων. Ο

εξοπλισμός ενός δικτύου WLAN περιλαμβάνει, εκτός από τα σημεία AP, και υπολογιστικές συσκευές με διεπαφές ασύρματου δικτύου, οι οποίες είναι γνωστές ως σταθμοί (Stations - STA). Συνήθως, οι σταθμοί STA σε ένα δίκτυο WLAN είναι συσκευές που λειτουργούν με μπαταρία, όπως laptop, smartphone, tablet και ψηφιακές φωτογραφικές μηχανές, και δεν είναι απαραίτητο να είναι κινητές, αφού ως σταθμοί μπορούν να θεωρηθούν και σταθερές συσκευές, όπως σταθεροί υπολογιστές, σαρωτές και εκτυπωτές, αρκεί να είναι εφοδιασμένες με κατάλληλες κάρτες ασύρματης σύνδεσης [17].

Ο σχεδιασμός ενός αξιόπιστου, ασφαλούς και πάντα διαθέσιμου δικτύου WLAN απαιτεί την εξέταση πολλών παραγόντων. Ο ορθολογικός σχεδιασμός και υλοποίηση, με βάση μια ενδελεχή προκαταρκτική αξιολόγηση, μπορούν να διασφαλίσουν ότι ένα δίκτυο WLAN θα λειτουργήσει την πρώτη φορά και θα μπορεί εύκολα να επεκταθεί χωρίς απολύτως κανένα πρόβλημα [18]. Επομένως, για την ικανοποίηση όλων των απαιτήσεων σχεδιασμού του, ένα δίκτυο WLAN θα πρέπει να παρουσιάζει κάποια βασικά χαρακτηριστικά, τα οποία είναι καθολικά ανεξάρτητα από την εκάστοτε περίπτωση χρήσης του δικτύου. Τα χαρακτηριστικά αυτά αφορούν τα εξής στοιχεία [19 - 23]:

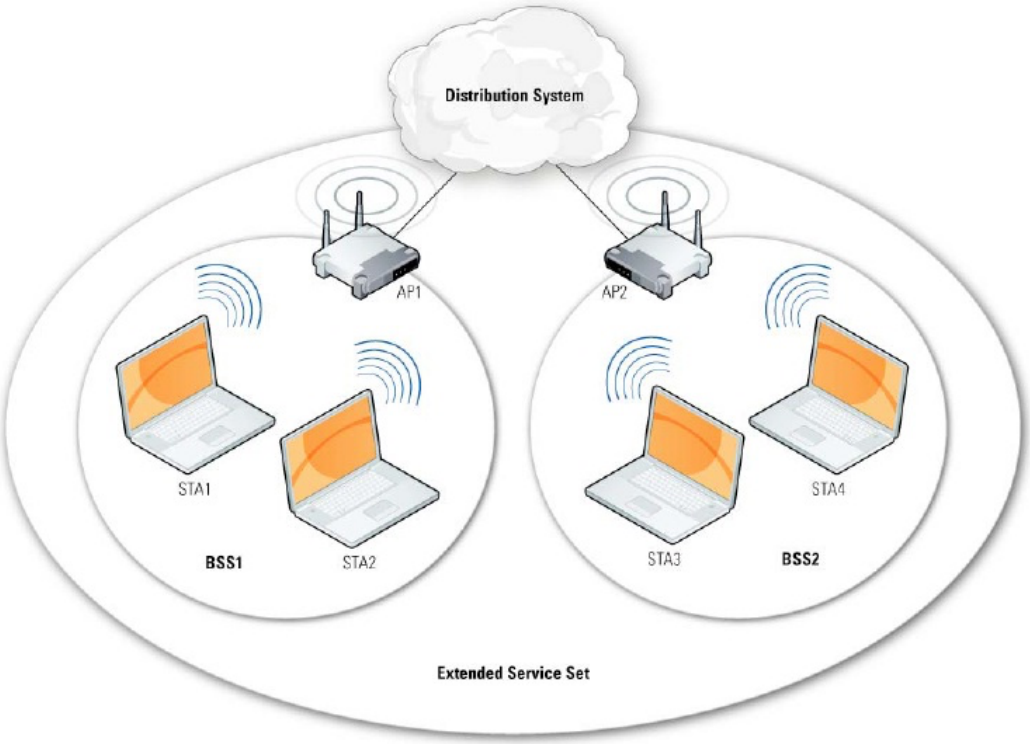
- ***Κινητικότητα (mobility):*** Επιτρέπει τη σύνδεση και αποσύνδεση των σταθμών στο και από το δίκτυο χωρίς να δημιουργούν προβλήματα στην εύρυθμη λειτουργία του. Το χαρακτηριστικό της κινητικότητας θα πρέπει να λαμβάνεται σοβαρά υπόψη κατά την επιλογή των μηχανισμών δρομολόγησης των πακέτων δεδομένων σε ένα δίκτυο WLAN. Το ποσό (amount) και η δομή (structure) της κινητικότητας είναι δύο βασικά στοιχεία της, τα οποία καθορίζουν σε μέγιστο βαθμό τον μηχανισμό δρομολόγησης που επιλέγεται σε κάθε περίπτωση χρήσης του δικτύου
- ***Ασφάλεια (security):*** Αφορά τα μέσα και τις μεθόδους που χρησιμοποιούνται για να προστατεύσουν το δίκτυο και τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις. Ως μέθοδοι και τεχνικές ασφάλειας θεωρούνται οι μηχανισμοί κρυπτογράφησης και οι μέθοδοι παροχής εξουσιοδότησης στους νόμιμους χρήστες του δικτύου
- ***Επεκτασιμότητα (scalability):*** Αφορά την ικανότητα ενός δικτύου να μπορεί να εξυπηρετεί μεγαλύτερο αριθμό σταθμών και χρηστών, χωρίς να επηρεάζεται η συνολική του απόδοση ή αποτελεσματικότητα
- ***Ευελιξία (flexibility):*** Αφορά την ικανότητα ενός δικτύου να μπορεί να προσαρμόζεται στη διαφορετικότητα των αναγκών και των απαιτήσεων που παρουσιάζουν τα εκάστοτε σενάρια και περιβάλλοντα χρήσης του
- ***Περιοχή κάλυψης (coverage):*** Η περιοχή κάλυψης ενός δικτύου WLAN εξαρτάται από τον αριθμό και την υποδομή των σημείων AP και του δικτύου κορμού του. Η περιοχή κάλυψης είναι ιδιαίτερα συνδεδεμένη με την ευαισθησία (sensitivity) των δεκτών των συσκευών του δικτύου, ένα χαρακτηριστικό που εκφράζει την ικανότητα της κεραίας των σημείων AP και των σταθμών του δικτύου να λαμβάνουν σήματα από μακρινές αποστάσεις
- ***Ταχύτητα ή ρυθμός μετάδοσης δεδομένων (speed / data rate):*** Καθορίζει τον ρυθμό των δεδομένων που μεταδίδονται μεταξύ του εξοπλισμού των δικτύων και εκφράζεται ως bit per second (bps). Ο μέγιστος ρυθμός μετάδοσης δεδομένων ενός καναλιού ασύρματης επικοινωνίας εξαρτάται από το εύρος ζώνης του καναλιού, τον αριθμό των διακριτών επιπέδων του ψηφιακού σήματος και το επίπεδο θορύβου που υπάρχει κατά τη διαδικασία της μετάδοσης
- ***Χωρητικότητα (capacity):*** Περιγράφει λεπτομερώς τον αριθμό των συσκευών που μπορούν να υποστηριχθούν ταυτόχρονα σε ένα δίκτυο WLAN με βάση τις εφαρμογές που χρησιμοποιούνται και το εύρος ζώνης που καταναλώνεται. Σε συνδυασμό με την κάλυψη και τη χρήση καναλιών, η κατανόηση των αναγκών χωρητικότητας ενός ασύρματου δικτύου είναι καθοριστικής σημασίας για το σχεδιασμό του, καθώς υποδεικνύει τα σημεία που αναμένεται να υπάρχει μεγαλύτερη πυκνότητα χρηστών
- ***Συμβατότητα (compatibility):*** Αφορά τη δυνατότητα που παρουσιάζει ένα δίκτυο WLAN να λειτουργεί με διάφορα πρότυπα και πρωτόκολλα ασύρματης επικοινωνίας. Βασική προϋπόθεση αυτής της συμβατότητας είναι τα ίδια τα πρότυπα και πρωτόκολλα ασύρματης

επικοινωνίας να παρουσιάζουν συμβατότητα με προηγούμενες εκδόσεις τους ή με αντίστοιχα πρότυπα και πρωτόκολλα άλλων τεχνολογιών

2.2 Τύποι και τεχνολογίες ασύρματων τοπικών δικτύων

Στο πρότυπο IEEE 802.11 καθορίζονται δύο βασικοί τύποι δικτύων WLAN [24]: (α) τα δίκτυα υποδομής WLAN και (β) τα ad hoc δίκτυα WLAN.

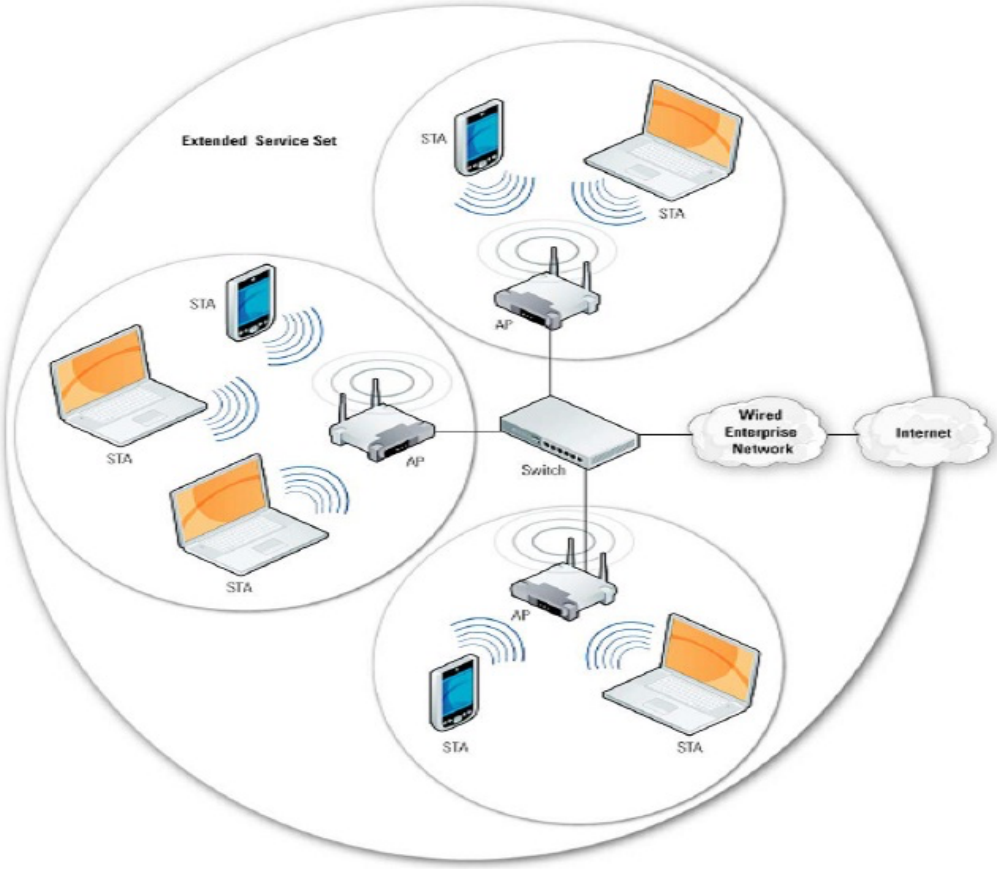
Τα δίκτυα IEEE 802.11 WLAN υποδομής (infrastructure WLAN) περιλαμβάνουν ένα ή περισσότερα βασικά σύνολα υπηρεσιών BSS (Basic Service Sets), τα οποία αποτελούν βασικά δομικά στοιχεία ενός WLAN. Ένα BSS περιλαμβάνει τουλάχιστον ένα σημείο AP και έναν ή περισσότερους σταθμούς STA. Η λειτουργία του σημείου AP ενός BSS στα δίκτυα WLAN υποδομής είναι να συνδέει τους σταθμούς STA με το σύστημα DS. Όπως αναφέρθηκε στην προηγούμενη ενότητα, το σύστημα DS είναι το μέσο με το οποίο οι σταθμοί STA μπορούν να επικοινωνούν με τα ενσύρματα LAN και τα εξωτερικά δίκτυα, όπως το Διαδίκτυο. Στην εικόνα 2.2 παρουσιάζεται η λειτουργία ενός δικτύου IEEE 802.11 WLAN υποδομής, όπου δύο BSS συνδέονται σε ένα σύστημα DS. Ο κύκλος στην εικόνα 2.2 αντιπροσωπεύει την εμβέλεια του σήματος των συσκευών, η οποία είναι σημαντική να ληφθεί υπόψη επειδή καθορίζει την περιοχή κάλυψης εντός της οποίας οι σταθμοί STA μπορούν να παραμείνουν σε επικοινωνία [24].



Εικόνα 2.2: Παράδειγμα δικτύου IEEE 802.11 WLAN υποδομής [24]

Η σύνδεση πολλών σημείων AP σε ένα μόνο σύστημα DS επιτρέπει τη δημιουργία ασύρματων δικτύων αυθαίρετου μεγέθους και πολυπλοκότητας. Στην προδιαγραφή IEEE 802.11, ένα δίκτυο πολλαπλών BSS αναφέρεται ως εκτεταμένο σύνολο υπηρεσιών ESS (Extended Service Set). Στην εικόνα 2.3 παρουσιάζεται ένα παράδειγμα δικτύου με ενσύρματες και ασύρματες δυνατότητες, παρόμοιο με αυτό που θα αναπτυσσόταν γενικά σε μια εταιρεία. Στο παράδειγμα παρουσιάζεται η ανάπτυξη ενός ESS που αποτελείται από τρία BSS, καθένα από τα οποία περιλαμβάνει ένα σημείο AP. Το ESS συνδέεται στο ενσύρματο εταιρικό δίκτυο ή στο σύστημα DS, το οποίο, με τη σειρά του,

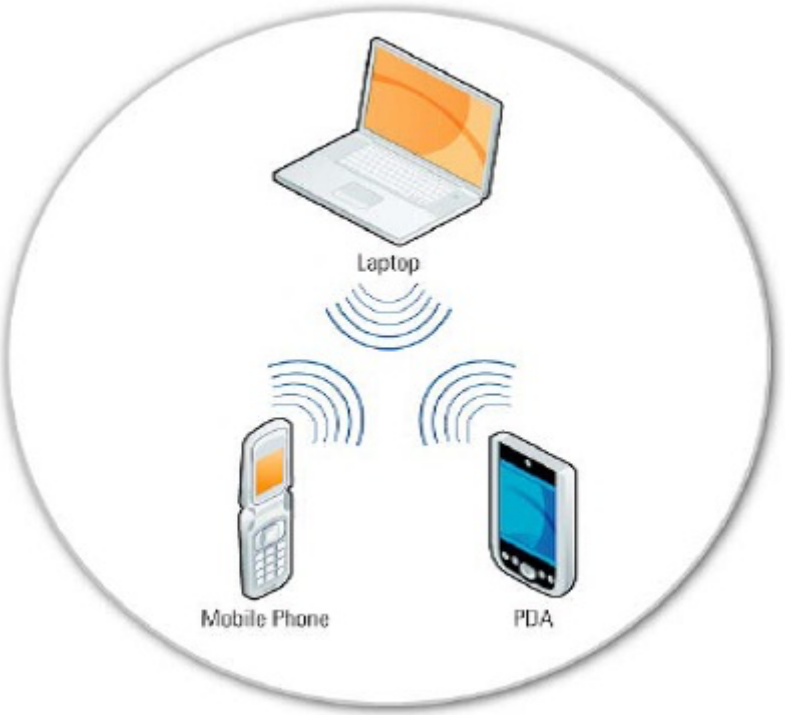
συνδέεται στο Διαδίκτυο και σε άλλα εξωτερικά δίκτυα. Μια τέτοια αρχιτεκτονική θα μπορούσε να επιτρέψει σε διάφορους σταθμούς STA, όπως φορητούς υπολογιστές και PDA, να έχουν πρόσβαση σε δικτυακούς πόρους και στο Διαδίκτυο. Επιπλέον, η χρήση ενός ESS παρέχει την ευκαιρία στους σταθμούς STA των δικτύων IEEE 802.11 WLAN υποδομής να πραγματοποιούν περιαγωγή μεταξύ των σημείων AP, διατηρώντας παράλληλα τη συνδεσιμότητά τους με το δίκτυο [24].



Εικόνα 2.3: Παράδειγμα ανάπτυξης ESS δικτύου IEEE 802.11 WLAN υποδομής [24]

Στην εικόνα 2.4 παρουσιάζεται η λειτουργία ενός ad hoc δικτύου IEEE 802.11 WLAN. Στα ad hoc δίκτυα WLAN, γνωστά και ως peer-to-peer (P2P) δίκτυα WLAN, δύο ή περισσότεροι σταθμοί STA μπορούν να επικοινωνούν απευθείας μεταξύ τους. Στην εικόνα 2.4 παρουσιάζεται παράδειγμα ad hoc δικτύου WLAN, όπου τρεις συσκευές επικοινωνούν μεταξύ τους με τρόπο P2P χωρίς καμία ασύρματη υποδομή ή ενσύρματες συνδέσεις. Ένα σύνολο σταθμών STA που έχει ρυθμιστεί να λειτουργεί με αυτόν τον ad hoc τρόπο είναι γνωστό ως ανεξάρτητο βασικό σύνολο υπηρεσιών IBSS (Independent Basic Service Set). Μια θεμελιώδης ιδιότητα του IBSS είναι ότι δεν ορίζει καμία δρομολόγηση ή προώθηση, επομένως όλες οι συσκευές πρέπει να βρίσκονται εντός εμβέλειας επικοινωνίας μεταξύ τους [24].

Ένα από τα βασικά πλεονεκτήματα των ad hoc δικτύων WLAN είναι ότι μπορούν να διαμορφωθούν οποτεδήποτε και οπουδήποτε, επιτρέποντας σε πολλούς χρήστες να δημιουργούν ασύρματες συνδέσεις φθηνά, γρήγορα και εύκολα. Ένα ad hoc δίκτυο μπορεί να δημιουργηθεί για διάφορους λόγους, όπως η υποστήριξη δραστηριοτήτων κοινής χρήσης αρχείων μεταξύ δύο συσκευών. Ωστόσο, οι συσκευές που λειτουργούν αποκλειστικά σε λειτουργία ad hoc δεν μπορούν να επικοινωνήσουν με εξωτερικά ασύρματα δίκτυα. Μια περαιτέρω περιπλοκή είναι ότι ένα ad hoc δίκτυο μπορεί να επηρεάσει τη λειτουργία ενός δικτύου WLAN υποδομής που υπάρχει στον ίδιο χώρο [24].



Εικόνα 2.4: Παράδειγμα ad hoc δικτύου IEEE 802.11 WLAN [24]

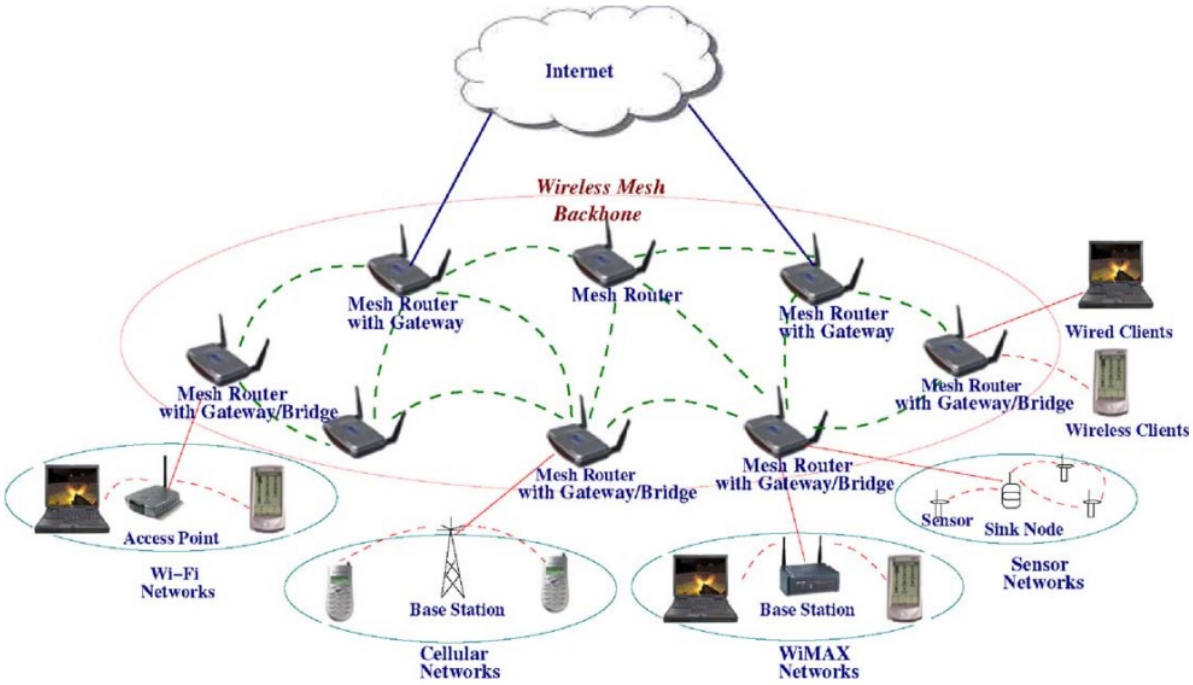
Η ταχεία διάδοση των δικτύων IEEE 802.11 WLAN και η αυξανόμενη ζήτηση για μεγαλύτερη περιοχή κάλυψης, οδήγησε σε αναπτύγματα δικτύων με πολύ μεγάλο αριθμό σημείων AP. Παρόλο που το κόστος των σημείων AP δεν είναι παραδοσιακά πολύ υψηλό, ιδίως σε σύγκριση με το κόστος του εξοπλισμού των κυψελοειδών δικτύων, η ανάπτυξη ενός μεγάλου αριθμού τέτοιων σημείων στα δίκτυα WLAN, αυξάνει την πολυπλοκότητα αλλά και το κόστος υλοποίησής τους. Επίσης, λόγω των περιορισμών που παρουσιάζει το εύρος κάλυψης των δικτύων IEEE 802.11, απαιτείται συνεχή προσθήκη νέων σημείων AP ώστε να καλυφθούν οι αυξανόμενες απαιτήσεις μεταφοράς δεδομένων σε αυτά. Όλα αυτά τα στοιχεία, οδήγησαν στη δημιουργία ενός νέου τύπου δικτύων WLAN, όπως είναι τα δίκτυα πλέγματος (mesh WLANs), τα οποία αποδείχθηκαν ιδιαίτερα χρήσιμα σε περιοχές μεγάλης έκτασης ή σε περιοχές όπου είναι αδύνατη η ανάπτυξη κάποιου ενσύρματου δικτύου LAN. Τα δίκτυα πλέγματος έχουν γίνει μια απαραίτητη τεχνική δικτύωσης για την ανάπτυξη ασύρματων δικτύων επόμενης γενιάς, καθώς υποστηρίζουν μεγαλύτερη κάλυψη και πλεονασμό (redundancy) [25].

Τα δίκτυα WLAN πλέγματος αποτελούνται από δύο τύπους κόμβων [26]: (α) τους δρομολογητές πλέγματος και (β) τους πελάτες πλέγματος. Εκτός από τη δυνατότητα δρομολόγησης, κάτι που αντιστοιχεί στη λειτουργία πύλης/επαναλήπτη των συμβατικών ασύρματων δρομολογητών, οι ασύρματοι δρομολογητές πλέγματος (wireless mesh routers) περιλαμβάνουν πρόσθετες λειτουργίες για την υποστήριξη της δικτύωσης πλέγματος. Για περαιτέρω βελτίωση της ευελιξίας της δικτύωσης, ένας δρομολογητής πλέγματος είναι συνήθως εξοπλισμένος με πολλαπλές ασύρματες διεπαφές της ίδιας ή διαφορετικών τεχνολογιών ασύρματης πρόσβασης. Σε σύγκριση με έναν συμβατικό ασύρματο δρομολογητή, ένας ασύρματος δρομολογητής πλέγματος μπορεί να πετύχει ίδια κάλυψη με πολύ μικρότερη ισχύ μετάδοσης μέσω της χρήσης τεχνικών δρομολόγησης πολλαπλών αλμάτων (multi hop). Οι πελάτες πλέγματος (mesh clients) περιλαμβάνουν επίσης όλες τις απαραίτητες λειτουργίες για την υποστήριξη δικτύωσης πλέγματος, και ως εκ τούτου, μπορούν να λειτουργήσουν και ως δρομολογητές, αλλά όχι ως πύλες ή γέφυρες. Επιπλέον, περιλαμβάνουν συνήθως μόνο μία ασύρματη

διεπαφή. Κατά συνέπεια, οι πελάτες πλέγματος είναι πιο απλής αρχιτεκτονικής από τους δρομολογητές πλέγματος και μπορεί να είναι συσκευές, όπως φορητοί υπολογιστές, συσκευές PDA, συσκευές ανάγνωσης RFID, κλπ. [25].

Η αρχιτεκτονική δομή των δικτύων WLAN πλέγματος μπορεί να ταξινομηθεί σε τρεις βασικούς τύπους με βάση τη λειτουργικότητα των κόμβων τους [25]: (α) τα δίκτυα WLAN πλέγματος υποδομής, (β) τα δίκτυα WLAN πλέγματος πελατών και (γ) τα δίκτυα WLAN υβριδικού πλέγματος.

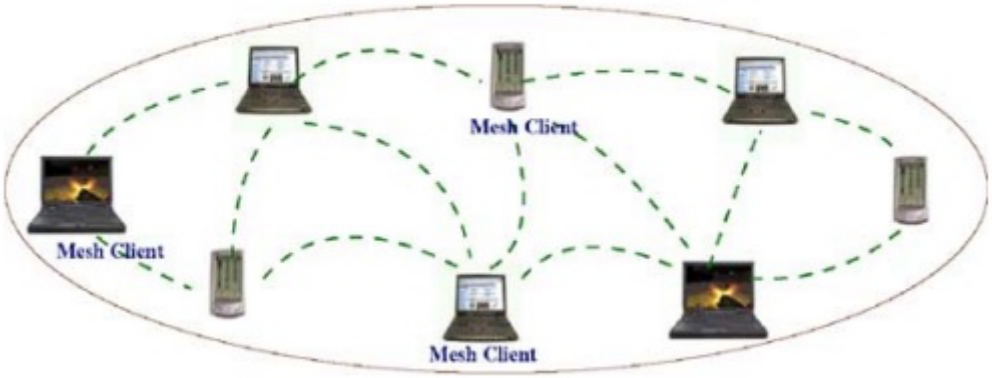
Τα δίκτυα WLAN πλέγματος υποδομής (Infrastructure mesh WLANs) περιλαμβάνουν δρομολογητές πλέγματος που σχηματίζουν μια υποδομή για πελάτες που μπορούν να συνδεθούν σε αυτούς (Εικ. 2.5). Μια τέτοια υποδομή δικτύου μπορεί να κατασκευαστεί χρησιμοποιώντας διάφορους τύπους τεχνολογιών επικοινωνίας, εκτός από τις πλέον χρησιμοποιούμενες IEEE 802.11. Το ασύρματο δίκτυο πλέγματος που δημιουργούν σε αυτή την περίπτωση οι δρομολογητές πλέγματος χαρακτηρίζεται από δυνατότητες αυτο-διαμόρφωσης και αυτο-θεραπείας. Λειτουργώντας ως πύλες, οι δρομολογητές πλέγματος μπορούν να συνδεθούν στο Διαδίκτυο. Αυτή η προσέγγιση λειτουργεί ως δίκτυο κορμού για τους συμβατικούς πελάτες και επιτρέπει την ενσωμάτωση του δικτύου WLAN πλέγματος υποδομής με άλλα ασύρματα δίκτυα. Ταυτόχρονα, οι συμβατικοί πελάτες έχουν τη δυνατότητα να συνδεθούν με τους δρομολογητές πλέγματος είτε μέσω ενσύρματης σύνδεσης (Ethernet) είτε μέσω ασύρματης επικοινωνίας (αν χρησιμοποιούν το ίδιο πρωτόκολλο). Στην περίπτωση χρήσης διαφορετικών πρωτοκόλλων ασύρματης επικοινωνίας, δίνεται η δυνατότητα σύνδεσης των πελατών με τους σταθμούς βάσης, οι οποίοι μπορούν να συνδέονται ενσύρματα με τους δρομολογητές πλέγματος [25].



Εικόνα 2.5: Παράδειγμα δικτύου WLAN πλέγματος υποδομής [25]

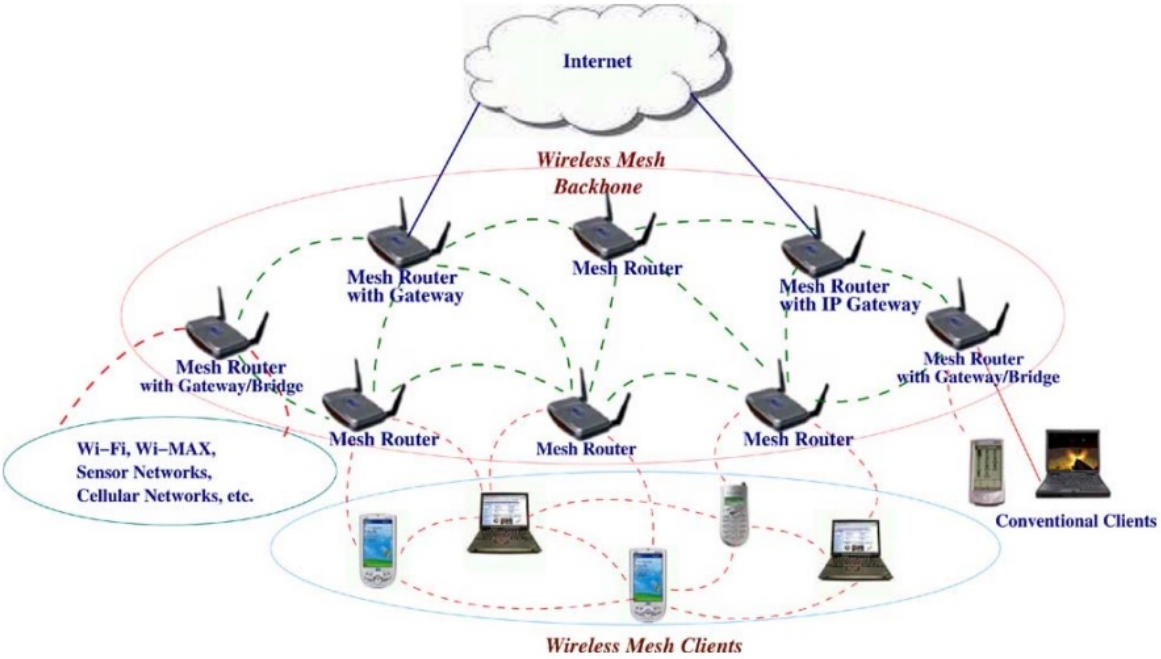
Τα δίκτυα WLAN πλέγματος πελατών παρέχουν στις συσκευές τη δυνατότητα μεταξύ τους σύνδεσης P2P. Σε αυτόν τον τύπο αρχιτεκτονικής, οι κόμβοι πελάτη αποτελούν το πραγματικό δίκτυο για την εκτέλεση λειτουργιών δρομολόγησης και διαμόρφωσης, καθώς και παροχής εφαρμογών τελικού χρήστη στους πελάτες. Ως εκ τούτου, ένα δίκτυο WLAN πλέγματος πελατών ουσιαστικά λειτουργεί όπως ένα ad hoc δίκτυο WLAN, με μόνη διαφορά ότι αποτελείται από συσκευές πλέγματος και όχι

συμβατικές συσκευές, οι οποίες εκτελούν πρόσθετες λειτουργίες, όπως δρομολόγηση και αυτό-διαμόρφωση (Εικ. 2.6) [25].



Εικόνα 2.6: Παράδειγμα δικτύου WLAN πλέγματος πελατών [25]

Τέλος, τα δίκτυα WLAN υβριδικού πλέγματος παρουσιάζουν μια αρχιτεκτονική, η οποία είναι ο συνδυασμός των άλλων δύο τύπων δικτύων πλέγματος (Εικ. 2.7). Οι πελάτες πλέγματος μπορούν να έχουν πρόσβαση στο δίκτυο μέσω δρομολογητών πλέγματος καθώς και απευθείας σύνδεση με άλλους πελάτες πλέγματος. Σε αυτήν την περίπτωση, ενώ η υποδομή παρέχει συνδεσιμότητα με άλλα δίκτυα, όπως το Διαδίκτυο, δίκτυα WiMAX, κυψελοειδή δίκτυα και δίκτυα αισθητήρων, οι δυνατότητες δρομολόγησης των πελατών παρέχουν βελτιωμένη συνδεσιμότητα και κάλυψη εντός του δικτύου WLAN υβριδικού πλέγματος, κάτι που αποτελεί το μεγαλύτερο πλεονέκτημα της αρχιτεκτονικής [25].



Εικόνα 2.7: Παράδειγμα δικτύου WLAN υβριδικού πλέγματος [25]

2.3 Πλεονεκτήματα και μειονεκτήματα των WLAN

Η ανάπτυξη των δικτύων WLAN έχει απλοποιήσει τη διαδικασία της ασύρματης δικτύωσης καθώς επιτρέπει στους χρήστες των κινητών συσκευών να μοιράζονται δικτυακούς πόρους και να λαμβάνουν πληροφορίες με βάση τις απαιτήσεις των καθημερινών τους δραστηριοτήτων. Σε ανώτερο επίπεδο, όπως το επιχειρηματικό, η ανάπτυξη δικτύων WLAN έχει αποδειχθεί ιδιαίτερα χρήσιμη για τις μικρομεσαίες επιχειρήσεις, όπου θεωρείται εργαλείο ενίσχυσης της παραγωγικότητας [27].

Σε γενικότερες γραμμές, τα δίκτυα WLAN παρουσιάζουν πολλά πλεονεκτήματα, μερικά από τα οποία αφορούν την υποστήριξη της κινητικότητας, τη δυνατότητα παροχής ασύρματης πρόσβασης σε περιοχές που είναι δύσκολο να αναπτυχθούν ενσύρματα δίκτυα, την ταχύτητα ανάπτυξης, την επεκτασιμότητα, το κόστος υλοποίησης και την ευελιξία [24].

Η δυνατότητα υποστήριξης της κινητικότητας αποτελεί ένα από τα σημαντικότερα πλεονεκτήματα των δικτύων WLAN, καθώς δίνεται η δυνατότητα στους χρήστες να μετακινούνται εντός της περιοχής κάλυψης του δικτύου διατηρώντας τη συνδεσιμότητά τους με το Διαδίκτυο ή με άλλους δικτυακούς πόρους. Αυτό το πλεονέκτημα θεωρείται ιδιαίτερα σημαντικό στην σύγχρονη εποχή όπου μια τεράστια γκάμα θέσεων εργασίας απαιτούν από τον εργαζόμενο να βρίσκεται σε συνεχή κινητικότητα και παράλληλα να μπορεί να έχει πρόσβαση στο Διαδίκτυο, χωρίς όμως να είναι σε θέση δημιουργίας κάποιου είδους φυσικής σύνδεσης [17].

Ο σύγχρονος τρόπος ζωής καθορίζεται σε μεγάλο βαθμό από την πανταχού παρουσία δικτύων. Ωστόσο υπάρχουν σημεία ή ακόμα και περιοχές, όπως ιστορικά ή παλαιότερα κτίρια, κλπ., όπου η δημιουργία ενσύρματων δικτύων LAN μπορεί να είναι αδύνατο ή ιδιαίτερα δαπανηρό να υλοποιηθεί. Σε τέτοιου είδους καταστάσεις, τα δίκτυα WLAN θεωρούνται μια λύση που μπορεί να αποδειχθεί ιδιαίτερα οικονομική. Επίσης, μπορεί να αποδειχθεί ιδιαίτερα αποτελεσματική σε περιπτώσεις όπου δεν υπάρχουν ή είναι δύσκολο να υλοποιηθούν καλωδιώσεις σύνδεσης δικτύων LAN, όπως για παράδειγμα σε πολυσύχναστους δρόμους ή σε συνδέσεις μεταξύ κτιριακών υποδομών [27].

Καθώς η ανάπτυξη δικτύων WLAN μειώνει σε μέγιστο βαθμό την ανάγκη για εγκατάσταση καλωδίων, ο χρόνος που απαιτείται για την υλοποίησή τους είναι συγκριτικά πολύ λιγότερος σε σύγκριση με τα δίκτυα LAN. Αυτό σημαίνει ότι ένα δίκτυο WLAN είναι διαθέσιμο για χρήση πολύ γρηγορότερα σε σύγκριση με ένα δίκτυο LAN. Επομένως η ταχύτητα ανάπτυξης ενός δικτύου WLAN αποτελεί ένα ακόμα πλεονέκτημά του [28].

Τα δίκτυα WLAN χαρακτηρίζονται από δυναμικά διαφορετικούς τύπους τοπολογιών, οι οποίες μπορούν να σχεδιαστούν και εύκολα να τροποποιηθούν, όταν αυτό απαιτείται, ανάλογα με τις εκάστοτε ανάγκες των εφαρμογών. Αυτό σημαίνει ότι είναι ιδιαίτερα επεκτάσιμα και ευέλικτα ώστε να μπορούν να ικανοποιούν τις εκάστοτε ανάγκες υποστήριξης ενός δυναμικά μεταβαλλόμενου αριθμού συσκευών και χρηστών. Κάτι τέτοιο τα καθιστά ιδιαίτερα χρήσιμα σε περιβάλλοντα που βιώνουν συχνές μεταβολές στον αριθμό των χρηστών, πράγμα το οποίο είναι σαφώς αδιανόητο για τα ενσύρματα δίκτυα [27].

Τα δίκτυα WLAN είναι γενικά λιγότερο δαπανηρά ως προς την εγκατάσταση και συντήρησή τους σε σύγκριση με τα ενσύρματα δίκτυα, καθώς δεν απαιτούνται επιπλέον έξοδα καλωδίωσης. Ταυτόχρονα τα έξοδα αναβάθμισης και επέκτασης των δικτύων WLAN είναι επίσης μικρότερα σε σύγκριση με τα δίκτυα LAN. Επομένως τα δίκτυα WLAN παρουσιάζουν μια οικονομική αποτελεσματικότητα [29].

Τέλος, τα δίκτυα WLAN είναι σχετικά εύκολο να εγκατασταθούν και να ρυθμιστούν, καθιστώντας τα μια δημοφιλή επιλογή για μικρές επιχειρήσεις και οικιακούς χρήστες. Μπορούν να τοποθετηθούν γρήγορα και εύκολα, χωρίς να χρειάζονται εξειδικευμένες δεξιότητες ή εξοπλισμό [27].

Παρά τα παραπάνω πλεονεκτήματα των δικτύων WLAN, σε σύγκριση με τα ενσύρματα δίκτυα LAN, παρουσιάζουν και ορισμένα συγκεκριμένα μειονεκτήματα που αφορούν την ασφάλεια, το ρυθμό μετάδοσης δεδομένων και τις παρεμβολές [30]. Γενικότερα, τα ασύρματα δίκτυα είναι λιγότερο ασφαλή από τα ενσύρματα δίκτυα. Βασική αιτία αποτελεί η χρήση των ηλεκτρομαγνητικών κυμάτων (ραδιοσυχνοτήτων ή υπέρυθρων) για την μετάδοση των σημάτων επικοινωνίας, με αποτέλεσμα να είναι εύκολη η υποκλοπή τους για κακόβουλους σκοπούς. Τρόποι προστασίας για την αύξηση της ασφάλειας των ασύρματων δικτύων υπάρχουν (τεχνολογίες κρυπτογράφησης, τείχη προστασίας, και πολλά άλλα μέτρα ασφαλείας), όμως είναι δύσκολο να εγγυηθεί κανείς για την πλήρη ασφάλεια ενός ασύρματου δικτύου [31].

Οι ρυθμοί μετάδοσης δεδομένων που επιτυγχάνονται ακόμα και στα ασύρματα δίκτυα είναι κατά πολύ μικρότεροι των ταχυτήτων μεταφοράς δεδομένων που παρατηρούνται στα ενσύρματα δίκτυα. Αυτό μπορεί εύκολα να αποδειχθεί από το γεγονός ότι καθώς ο αριθμός των συσκευών που χρησιμοποιούν ένα ασύρματο δίκτυο αυξάνεται, ο ρυθμός μετάδοσης δεδομένων σε κάθε συσκευή μειώνεται, πράγμα που δεν παρατηρείται στα ενσύρματα δίκτυα, όπου η μείωση του ρυθμού μεταφοράς δεδομένων είναι πολύ μικρότερη στην περίπτωση αύξησης του αριθμού των χρηστών. Επίσης, οι ταχύτητες μετάδοσης δεδομένων σε ένα ασύρματο δίκτυο μειώνονται όσο ο χρήστης απομακρύνεται περισσότερο από το σημείο AP, καθώς οι ασύρματες συσκευές λειτουργούν ικανοποιητικά μόνο σε περιορισμένη απόσταση από αυτό το σημείο, με την απόσταση να καθορίζεται σε μεγάλο βαθμό από το πρότυπο που χρησιμοποιείται. Εμπόδια μεταξύ του σημείου AP και του χρήστη, όπως τοίχοι, γυαλί, νερό, φυλλώματα δέντρων, κλπ., μπορούν επίσης να καθορίσουν την απόσταση λειτουργίας των ασύρματων συσκευών. Ιδιαίτερα γύρω από κτίρια με οπλισμένο σκυρόδερμα (μπετόν) παρατηρείται κακή λήψη σήματος. Το ζήτημα των παρεμβολών είναι έντονο και στις περιπτώσεις χρήσης του ίδιου φάσματος ραδιοσυχνοτήτων για τη λειτουργία ενός δικτύου WLAN. Ιδιαίτερα στη ζώνη συχνοτήτων 2,4GHz, το ζήτημα των παρεμβολών αποτελεί πραγματική πρόκληση, καθώς ο αριθμός των ατόμων που χρησιμοποιούν ασύρματες συσκευές αυτής της μπάντας αυξάνει συνεχώς, γεγονός που δημιουργεί αύξηση της συμφόρησής της. Οι τρόποι αντιμετώπισης των συγκεκριμένων ζητημάτων μείωσης του ρυθμού μεταφοράς δεδομένων και εμφάνισης παρεμβολών (όπως για παράδειγμα η χρήση μεγαλύτερου αριθμού σημείων AP και η επιλογή εξελιγμένων μηχανισμών πρόσβασης, αντίστοιχα), μπορούν να οδηγήσουν στην εμφάνιση νέων προκλήσεων, όπως είναι η αύξηση του συνολικού κόστους υλοποίησης του δικτύου WLAN [31].

Στην πράξη, ένα δίκτυο WLAN από μόνο του δεν αποτελεί μια πλήρη λύση ασύρματης δικτύωσης, καθώς απαιτεί την ύπαρξη ενός ενσύρματου LAN που παίζει το ρόλο της ραχοκοκαλιάς δικτύου. Η ραγδαία εξέλιξη των προτύπων ασύρματης σύνδεσης, πέρα από τα όποια πλεονεκτήματα, οδηγεί και σε μια απαραίτητη, ή τουλάχιστον επιθυμητή, αναβάθμιση ενός δικτύου WLAN σε υψηλότερες προδιαγραφές, γεγονός που σημαίνει την αντικατάσταση του ασύρματου εξοπλισμού (ασύρματες κάρτες δικτύωσης, σημεία πρόσβασης, κλπ.). Έτσι, καθώς τα πρότυπα ασύρματης σύνδεσης αλλάζουν πιο γρήγορα από ότι τα ενσύρματα, είναι γενικά ευκολότερη η υλοποίηση ενός ενσύρματου δικτύου που να καλύπτει μεγαλύτερο μέρος των μελλοντικών απαιτήσεων [31].

2.4 Τρέχουσα κατάσταση της τεχνολογίας και των προτύπων WLAN

Οι οργανισμοί τυποποίησης είναι ομάδες που ενδιαφέρονται να προωθήσουν και να συντονίσουν κανόνες για το βάρος, την έκταση, την αξία ή την ποιότητα μιας δεδομένης τεχνολογίας, με σκοπό την μοντελοποίησή της. Κάτι τέτοιο δίνει τη δυνατότητα σε άλλους οργανισμούς να αξιοποιήσουν αυτή τη μοντελοποίηση της τεχνολογίας, βελτιώνοντάς την ή σε ορισμένες περιπτώσεις, προωθώντας νέες τεχνολογίες. Στον τομέα της ασύρματης δικτύωσης, τα τελευταία 25 χρόνια, ένα μεγάλο πλήθος νέων

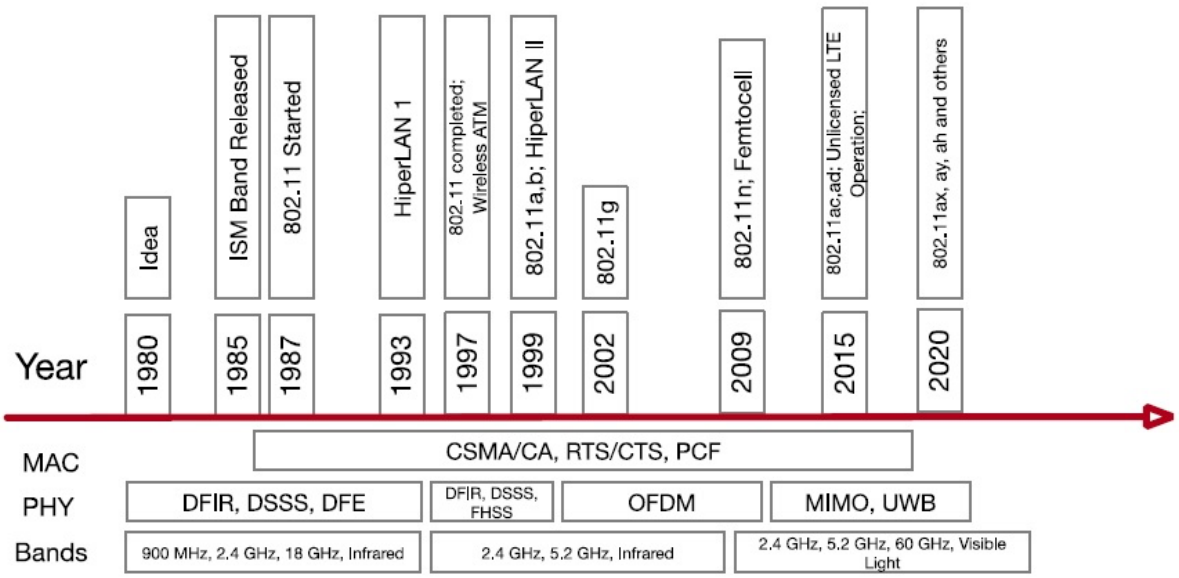
τεχνολογιών έχουν μοντελοποιηθεί, έχοντας περάσει από το στάδιο της σύλληψης της ιδέας στο στάδιο της εμπορευματοποίησης με απίστευτα γρήγορους ρυθμούς. Με τον τρόπο αυτό, τα πρότυπα, που χρησιμοποιούνται ως βάση για τις ασύρματες τεχνολογίες, έχουν δώσει και εξακολουθούν να δίνουν τη δυνατότητα στους τελικούς χρήστες να αποκομίζουν τα οφέλη της εκμετάλλευσης διαλειτουργικών, αξιόπιστων και αποτελεσματικών τεχνολογιών [27].

Η ανάπτυξη των προτύπων ασύρματης σύνδεσης έχει οδηγήσει σε τεχνολογικές εξελίξεις, οι οποίες διαμορφώνουν συνεχώς τη βιομηχανία ασύρματης επικοινωνίας. Επομένως, για την πλήρη κατανόηση της κατάστασης της τεχνολογίας των δικτύων WLAN απαιτείται πρώτα η απόκτηση γνώσης σχετικά με την ιστορική εξέλιξη των προτύπων πάνω στα οποία βασίζεται η λειτουργία τους. Τα πρότυπα ασύρματης σύνδεσης τέθηκαν σε εφαρμογή από τον οργανισμό IEEE, ο οποίος ασχολείται με τη διασφάλιση ότι οι κατασκευαστές ασύρματων συσκευών ακολουθούν την ίδια μοντελοποίηση της τεχνολογίας των ασύρματων επικοινωνιών και επομένως όλες οι ασύρματες συσκευές είναι συμβατές μεταξύ τους. Ο οργανισμός IEEE αναπτύσσει γενικότερα πρότυπα που δεν αφορούν μόνο τον τομέα της υπολογιστικής αλλά καλύπτουν οποιαδήποτε τεχνική πρακτική που μπορεί να οδηγήσει στην προώθηση της τεχνολογικής προόδου. Η επιτροπή προτύπων IEEE 802 LAN/MAN αναπτύσσει πρότυπα για δίκτυα LAN και MAN [27].

2.5 Πρότυπο IEEE 802.11

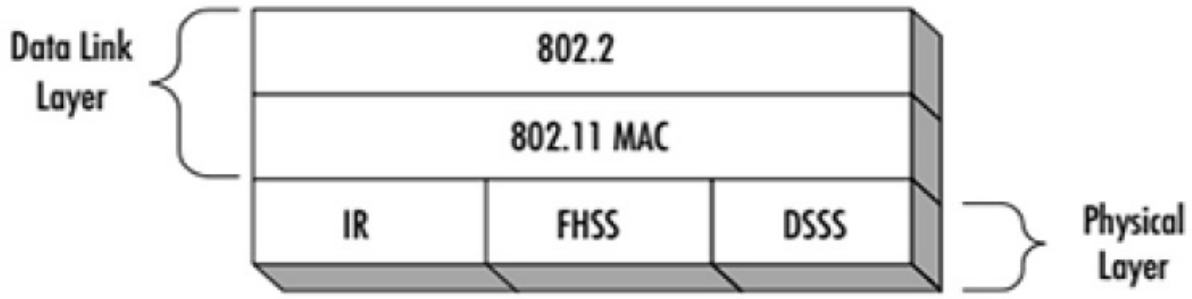
Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, το 1997, θεωρείται έτος ορόσημο για τα δίκτυα WLAN, όταν ο οργανισμός IEEE ανακοίνωσε την επικύρωση του προτύπου IEEE 802.11. Με τα χρόνια, το βασικό πρότυπο IEEE 802.11 εξελίχθηκε σε μια οικογένεια προτύπων, αφού εκδόθηκαν τροποποιήσεις του με βελτιωμένα χαρακτηριστικά, όπως η εμβέλεια, η ταχύτητα, κλπ. Ουσιαστικά, κάθε τροποποίηση αποτελεί βελτίωση του βασικού προτύπου, αλλά και των προηγούμενων τροποποιήσεων, και στην αγορά αντιμετωπίζεται σαν ξεχωριστό πρότυπο. Οι τροποποιήσεις αυτές θα παρουσιαστούν στις επόμενες υποενότητες, στις οποίες θα αναλυθούν οι εξελίξεις του βασικού προτύπου με την πάροδο του χρόνου. Αν και αυτές οι εξελίξεις διατήρησαν την υποδομή, τα χαρακτηριστικά και τις υπηρεσίες του αρχικού προτύπου IEEE 802.11, η διαφορά μεταξύ των ανεπτυγμένων προτύπων αφορά κυρίως αλλαγές στο φυσικό επίπεδο [32]. Στην εικόνα 2.8 παρουσιάζονται αυτές οι αλλαγές στο φυσικό επίπεδο των τροποποιήσεων του βασικού προτύπου IEEE 802.11 [13].

Η τυπική έκδοση του προτύπου και οι τροποποιήσεις του περιέχουν ένα σύνολο προδιαγραφών που καλύπτουν τα επίπεδα ελέγχου πρόσβασης του μέσου (MAC) και το φυσικό επίπεδο (PHY). Όπως φαίνεται στην εικόνα 2.9, το IEEE 802.11 ορίζει ένα υποεπίπεδο MAC, υπηρεσίες και πρωτόκολλα MAC και τρεις τεχνολογίες μετάδοσης δεδομένων για το φυσικό επίπεδο. Οι τρεις τεχνολογίες μετάδοσης είναι οι [27]: (α) η τεχνική FHSS (που υποστηρίζει βασική ταχύτητα μετάδοσης δεδομένων 1Mbps και έναν προαιρετικό ρυθμό μετάδοσης δεδομένων 2Mbps), β) η τεχνική DSSS (που υποστηρίζει ίδιους ρυθμούς μετάδοσης με την τεχνική FHSS) και γ) η τεχνική μετάδοσης μέσω υπερύθρων (IR) (που αν και υποστήριζει ίδιες ταχύτητες μετάδοσης με τις προηγούμενες τεχνικές, εντούτοις, το ζήτημα που παρουσιάζουν τα κύματα υπερύθρων ως προς την ικανότητά τους να διαπερνούν φυσικά εμπόδια, έδωσε ένα προβάδισμα χρήσης στις τεχνικές διαμόρφωσης μέσω ραδιοκυμάτων).



Εικόνα 2.8Εξελικτική πορεία των προτύπων IEEE 802.11 [13]

Ανεξάρτητα από το φυσικό επίπεδο που χρησιμοποιείται, όλοι οι πελάτες ενός δικτύου WLAN χρησιμοποιούν το ίδιο κανάλι για τις μεταδόσεις τους, κάτι που απαιτεί ακριβείς μηχανισμούς πολλαπλής πρόσβασης. Η βασική λειτουργία του επιπέδου MAC ενός δικτύου WLAN που βασίζεται στο πρότυπο IEEE 802.11, είναι να παρέχει ασύγχρονο, περιορισμένου χρόνου και αποφυγή συγκρούσεων, έλεγχο πρόσβασης σε μια ποικιλία φυσικών επιπέδων [33]. Για το λόγο αυτό περιλαμβάνει μια ποικιλία μηχανισμών πρόσβασης στο μέσο και μπορεί να παρέχει ένα σύνολο υπηρεσιών, τα οποία θα αναλυθούν στις επόμενες ενότητες.



Εικόνα 2.9: Τα επίπεδα PHY και MAC του IEEE 802.11 [27]

2.6 Μηχανισμοί πρόσβασης στο μέσο

Το επίπεδο MAC του βασικού προτύπου IEEE 802.11 ορίζει δύο διαφορετικούς τρόπους αποτελεσματικής διαχείρισης των μεταδόσεων μεταξύ των ασύρματων σταθμών, οι οποίοι αφορούν τη χρήση των μηχανισμών DCF (Distributed Coordination Function) και PCF (Point Coordination Function). Από τους μηχανισμούς αυτούς, στα δίκτυα WLAN 802.11 ευρεία εφαρμογή έχει ο μηχανισμός DCF, κυρίως λόγος είναι ότι είναι υποχρεωτικό στοιχείο του προτύπου IEEE 802.11, εξασφαλίζοντας συμβατότητα σε διάφορες ασύρματες συσκευές και δίκτυα. Αντίθετα, το PCF είναι προαιρετικό στοιχείο, και η υποστήριξή του δεν είναι τόσο διαδεδομένη εκτός των δικτύων υποδομής WLAN [27].

2.6.1 Μηχανισμός DCF

Η ασύρματη μεταφορά δεδομένων είναι ουσιαστικά ένας τρόπος μετάδοσης στον οποίο τα μεταδιδόμενα δεδομένα λαμβάνονται από όλα τα στοιχεία του δικτύου. Ο σχεδιασμός και η ανάπτυξη των δικτύων WLAN 802.11 βασίστηκε στη βασική υπόθεση ότι η μετάδοση και η ακρόαση του ασύρματου μέσου δεν είναι δυνατόν να πραγματοποιούνται ταυτόχρονα. Αυτό σημαίνει ότι ο οποιοσδήποτε ασύρματος κόμβος ενός δικτύου WLAN θα πρέπει να μοιράζεται το χρόνο πρόσβασης στο μέσο μετάδοσης με άλλους κόμβους, όπως ακριβώς συμβαίνει στα ενσύρματα δίκτυα που βασίζονται στο πρότυπο Ethernet [34].

Το σκεπτικό αυτό χρησιμοποιήθηκε για τη δημιουργία του μηχανισμού DCF, στον οποίο η χρήση του μηχανισμού πρόσβασης CSMA (Carrier Sense Multiple Access) αποσκοπεί στη διευκόλυνση της ασύρματης μετάδοσης δεδομένων. Βασικό χαρακτηριστικό του μηχανισμού πρόσβασης CSMA είναι η δυνατότητα που δίνεται σε κάθε σταθμό να αντιλαμβάνεται τη μη χρήση του ασύρματου μέσου πριν ξεκινήσει τη διαδικασία μετάδοσης δεδομένων. Στην περίπτωση των ενσύρματων δικτύων και του προτύπου Ethernet, όπου είναι δυνατή η ταυτόχρονη μετάδοση και ακρόαση του μέσου, η εμφάνιση συγκρούσεων (collisions) μπορεί να ανιχνευθεί άμεσα, μέσω του μηχανισμού πρόσβασης CSMA/CD (CSMA with Collision Detection) κατά την πραγματοποίηση της μεταφοράς δεδομένων. Με δεδομένο όμως, ότι η ανίχνευση εμφάνισης συγκρούσεων είναι δύσκολο να πραγματοποιηθεί στα δίκτυα WLAN, ο μηχανισμός DCF απαιτεί την αποστολή σημάτων αναγνώρισης λήψης (ACK) από τον ασύρματο σταθμό λήψης προς τον σταθμό μετάδοσης, μετά την επιτυχημένη λήψη των πλαισίων δεδομένων που έχουν μεταδοθεί. Με τον τρόπο αυτό, εάν ο σταθμός μετάδοσης δεν λάβει κάποιο πλαίσιο ACK από τον σταθμό λήψης, τότε εκτιμά ότι στο μέσο μετάδοσης έχει υπάρξει σύγκρουση. Καθώς, η εμφάνιση πολλών περιπτώσεων σύγκρουσης σε ένα ασύρματο μέσο οδηγεί αναπόφευκτα σε μείωση της συνολικής απόδοσης του δικτύου, η μείωση του αριθμού τους αποτελεί βασικό μέλημα των χρησιμοποιούμενων μηχανισμών πρόσβασης στο μέσο. Για το λόγο αυτό και με σκοπό τη μείωση των πιθανοτήτων εμφάνισης συγκρούσεων, στο μηχανισμό DCF δεν χρησιμοποιείται ο μηχανισμός πρόσβασης CSMA/CD, αλλά ένας μηχανισμός που βασίζεται στην ανίχνευση περιπτώσεων ανταγωνισμού (contentions) και ο οποίος είναι γνωστός ως μηχανισμός πρόσβασης CSMA/CA (CSMA with Collision Avoidance) [35].

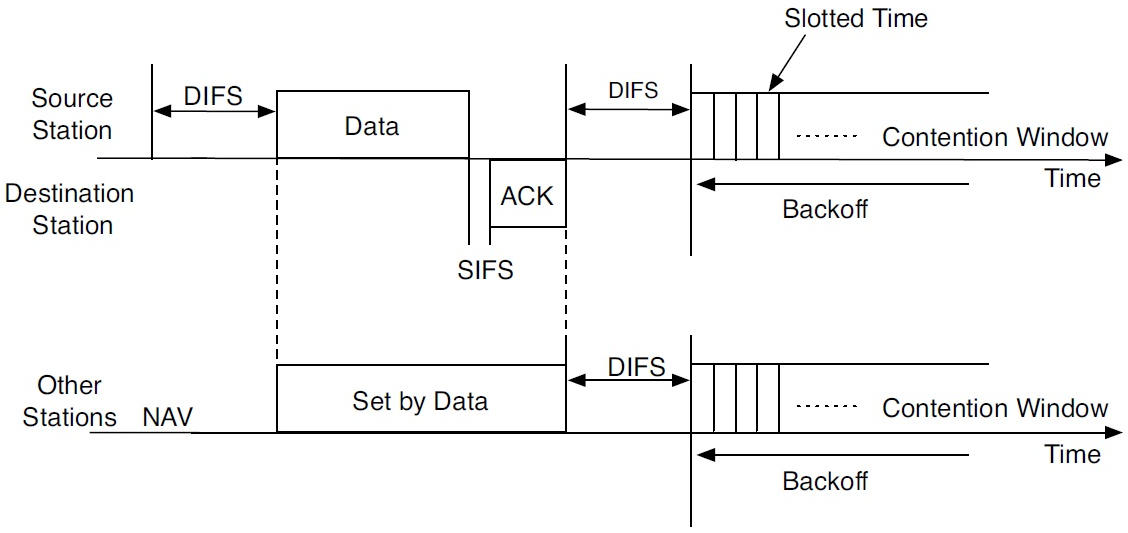
Το βασικό χαρακτηριστικό του μηχανισμού DCF είναι η ανυπαρξία κάποιου κεντρικού ελέγχου, στοιχείο που του δίνει τη δυνατότητα να λειτουργεί ανεξάρτητα σε κάθε ασύρματο σταθμό και σημείο AP του δικτύου για το πότε θα μπορεί να έχει πρόσβαση στο ασύρματο μέσο για τη μετάδοση δεδομένων. Ο μηχανισμός DCF υποστηρίζει δύο διαφορετικούς τρόπους πρόσβασης στο μέσο με βάση την ανίχνευση περιπτώσεων διαμάχης. Στον πρώτο, η κοινή χρήση του ασύρματου μέσου από τους σταθμούς επιτρέπεται μέσω της χρήσης του μηχανισμού CSMA/CA, ενώ στον δεύτερο, μέσω της χρήσης ανταλλαγής πλαισίων RTS (Request to Send) και CTS (Clear to Send) [27].

1) DCF με CSMA/CA

Στον τρόπο πρόσβασης στο μέσο με χρήση του μηχανισμού CSMA/CA, ο μηχανισμός DCF περιλαμβάνει διαδικασίες ανίχνευσης του μέσου μετάδοσης με βάση την εκάστοτε υπάρχουσα κυκλοφορία. Το σύνολο αυτών των διαδικασιών παρουσιάζεται στην εικόνα 2.10. Αρχικά, μέσω του πρωτοκόλλου CSMA/CA, πραγματοποιείται ανίχνευση του μέσου ως προς τη χρήση του από κάποιο ασύρματο σταθμό για μετάδοση δεδομένων. Η ανίχνευση αυτή πραγματοποιείται μέσω της μέτρησης των χρονικών διαστημάτων μεταξύ των μεταδόσεων των πλαισίων δεδομένων, τα οποία είναι γνωστά ως IFS (Inter-Frame Space). Στο επίπεδο MAC του προτύπου IEE 802.11 καθορίζονται τρία χρονικά διαστήματα IFS [34]: (α) το Short IFS (SIFS), (β) το PCF IFS (PIFS) και (γ) το DCF IFS (DIFS), από

τα οποία το SIFS είναι το μικρότερο και το DIFS το μεγαλύτερο. Αν κατά την ανίχνευση αυτή διαπιστωθεί ότι το ασύρματο μέσο έχει παραμείνει σε αδράνεια για χρονικό διάστημα μεγαλύτερο από τη διάρκεια ενός DIFS, τότε ο μηχανισμός DCF επιτρέπει στον ασύρματο σταθμό να αποκτήσει πρόσβαση στο μέσο και να ξεκινήσει άμεσα τη μετάδοση των πακέτων δεδομένων. Μετά την επιτυχημένη λήψη τους, ο σταθμός προορισμού περιμένει για μια χρονική περίοδο SIFS και στη συνέχεια μεταδίδει ένα πλαίσιο ACK προς τον σταθμό που απέστειλε τα πακέτα δεδομένων, υποδεικνύοντας με αυτόν τον τρόπο την επιτυχία της μετάδοσης [34].

Κατά τη διάρκεια της ανταλλαγής πακέτων δεδομένων μεταξύ δύο ασύρματων σταθμών, οι υπόλοιποι σταθμοί του δικτύου θα πρέπει να γνωρίζουν ότι δεν μπορούν να μπουν σε διαδικασία πραγματοποίησης κάποιας προσπάθειας μετάδοσης, ώστε να είναι δυνατός ο περιορισμός των πιθανών συγκρούσεων. Αν και η ανίχνευση της χρήσης του μέσου πραγματοποιείται στο φυσικό επίπεδο μέσω πραγματικών ελέγχων για την ύπαρξη σήματος στο κοινόχρηστο κανάλι, στο επίπεδο MAC ο μηχανισμός DCF χρησιμοποιεί μια διαδικασία εικονικής ανίχνευσης φορέα. Μέσα στην κεφαλίδα MAC του μεταδιδόμενου πλαισίου δεδομένων υπάρχει ένα πεδίο το οποίο αναφέρεται ως πεδίο διάρκειας (duration ID) και αφορά το χρονικό διάστημα στο οποίο το ασύρματο μέσο θα είναι απασχολημένο με τη μετάδοση του πλαισίου δεδομένων και του αντίστοιχου πλαισίου ACK μεταξύ δύο σταθμών. Κάθε σταθμός του δικτύου που δεν εκπέμπει, χρησιμοποιεί την τιμή της καταχώρισης του πεδίου διάρκειας για να προσαρμόσει ανάλογα μια εσωτερική παράμετρο χρονοδιακόπτη DCF που είναι γνωστή ως διάνυσμα NAV (Network Allocation Vector) και η οποία αποτελεί τη διαδικασία εικονικής ανίχνευσης φορέα. Κατά τη διαδικασία αυτή, το διάνυσμα NAV μπορεί να θεωρηθεί ως μετρητής που μετρά αντίστροφα, από μια μέγιστη τιμή μέχρι το μηδέν. Η μέγιστη τιμή του διανύσματος NAV αντιστοιχεί στο χρόνο που απαιτείται για τη μετάδοση του πλαισίου δεδομένων και του αντίστοιχου πλαισίου ACK μεταξύ δύο σταθμών, δηλαδή ο χρόνος για τον οποίο θα είναι απασχολημένο το κανάλι. Κατά την έναρξη της μετάδοσης ενός πλαισίου, η τιμή του NAV παίρνει τη μέγιστη τιμή της. Μια μη μηδενική τιμή υποδηλώνει ότι το κανάλι είναι απασχολημένο και επομένως κανένας σταθμός δεν μπορεί να το χρησιμοποιήσει. Όταν η τιμή NAV μειωθεί στην τιμή 0, υποδηλώνεται ότι το κανάλι είναι ελεύθερο και ότι οι άλλοι σταθμοί μπορούν να διεκδικήσουν τη χρήση του, αφού φυσικά ανιχνεύσουν πρώτα την αδράνεια του μέσου περιμένοντας για χρονικό διάστημα DIFS [34].



Εικόνα 2.10: Λειτουργία μηχανισμού DCF με CSMA/CA [34]

Μετά το τέλος μιας μετάδοσης πακέτων δεδομένων, ο σταθμός που την πραγματοποίησε δεν επιτρέπεται να επιχειρήσει διαδικασία άμεσης απόπειρας μετάδοσης. Κάτι ανάλογο ισχύει και για τους σταθμούς που είχαν προηγουμένως αναβάλει τη μετάδοσή τους λόγω χρήσης του μέσου για άλλες μεταδόσεις. Σε αυτές τις περιπτώσεις, οι σταθμοί θα πρέπει να ξεκινήσουν μια πρόσθετη διαδικασία, η οποία υποδεικνύεται από τον αλγόριθμο BEB (Binary Exponential Back-off). Σύμφωνα με τον αλγόριθμο BEB, ένας ασύρματος σταθμός θα πρέπει να αναβάλλει τη μετάδοσή του για μια τυχαία χρονική διάρκεια, που αναφέρεται ως χρόνος υπαναχώρησης (back-off time), μετά το χρονικό διάστημα DIFS, πριν επιχειρήσει να ξεκινήσει τη διαδικασία μετάδοσης. Με τον τρόπο αυτό, ο σταθμός που επιλέγει μικρότερη τυχαία χρονική περίοδο, αποκτά και την ευκαιρία μετάδοσης. Η τυχαία αυτή χρονική περίοδος δεν επιλέγεται αυθαίρετα, αλλά μέσα από έναν πίνακα του μηχανισμού DCF, που αναφέρεται ως παράθυρο διαμάχης (Contention Window - CW). Ο χρόνος υπαναχώρησης μετριέται μέσω ενός χρονομέτρου υπαναχώρησης, η ένδειξη του οποίου μειώνεται μόνο όταν το μέσο είναι αδρανές, ενώ παραμένει σταθερή όταν το μέσο χρησιμοποιείται για μετάδοση πακέτων δεδομένων. Μετά το τέλος της περιόδου χρήσης του μέσου, η ένδειξη του χρονομέτρου υπαναχώρησης συνεχίζεται μόνο, αν το μέσο παραμείνει ελεύθερο για μεγαλύτερο χρόνο από το χρονικό διάστημα DIFS [34].

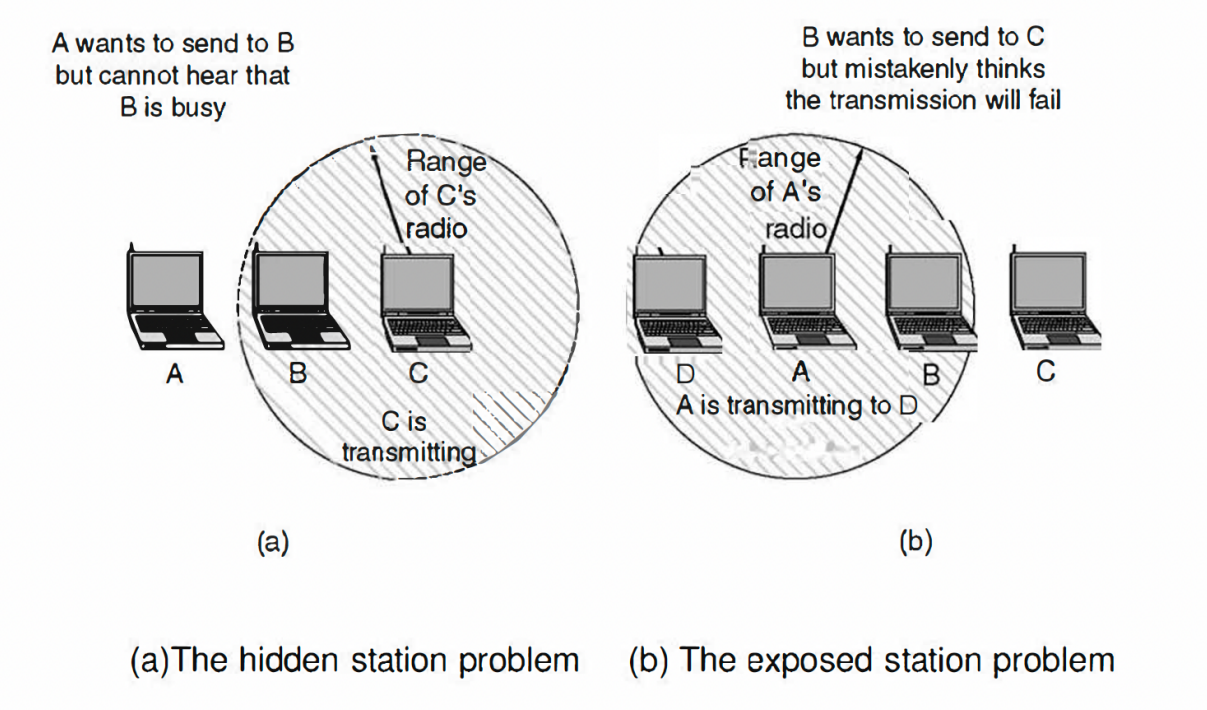
Καθώς το παράθυρο CW χωρίζεται σε μια σειρά χρονοθυρίδων (time slots) ίσου μήκους, με κάθε θυρίδα επομένως να αντιπροσωπεύει την ίδια σταθερή χρονική περίοδο, το τυχαίο χρονικό διάστημα υπαναχώρησης που επιλέγεται από τον εκάστοτε σταθμό αντιστοιχεί σε συγκεκριμένο αριθμό χρονοθυρίδων. Ο αριθμός των χρονοθυρίδων του παραθύρου CW που καθορίζεται από το μηχανισμό DCF παίρνει τιμές από το σύνολο [CWmin, CWmax], με τα CWmin και CWmax να αποτελούν αντίστοιχα τον ελάχιστο και τον μέγιστο αριθμό χρονοθυρίδων. Όταν ένας σταθμός ξεκινά τη διαδικασία υπαναχώρησής του, το CW παίρνει την τιμή CWmin. Μετά από κάθε ανεπιτυχή μετάδοση (π.χ. μετά από την εμφάνιση κάποιου ανταγωνισμού), το παράθυρο CW κάθε εμπλεκόμενου σταθμού διπλασιάζει την τιμή του μέχρι να φτάσει την τιμή CWmax και θα παραμείνει σε αυτή για όλες τις υπόλοιπες απόπειρες μετάδοσης. Ο μέγιστος αριθμός προσπαθειών μετάδοσης που επιτρέπεται για κάθε ασύρματο σταθμό καθορίζεται από μια παράμετρο του μηχανισμού DCF που είναι γνωστή ως όριο προσπαθειών (retry limit). Η προεπιλεγμένη τιμή, όπως καθορίζεται από το πρότυπο IEEE 802.11, είναι 7, με τον μετρητή να ξεκινά από το 0. Μόλις ολοκληρωθεί μια επιτυχημένη μετάδοση, το retry limit επαναφέρεται στο 0, και αντίστοιχα η τιμή του CW επαναφέρεται στο CWmin. [34].

Με τη χρήση του αλγόριθμου BEB και του παραθύρου CW, ανταγωνισμοί μπορούν πλέον να συμβούν μόνο στην περίπτωση που δύο ασύρματοι σταθμοί έχουν επιλέξει τον ίδιο χρόνο υπαναχώρησης ή ξεκινήσουν την αποστολή δεδομένων τους ακριβώς μετά τη λήξη της περιόδου υπαναχώρησης (backoff period). Στην περίπτωση που αυτός ο χρόνος είναι διαφορετικός, τότε ο ασύρματος σταθμός με τον μεγαλύτερο επιλεγμένο χρόνο, σταματά το χρονόμετρο υπαναχώρησης, περιμένει μέχρι το τέλος της μετάδοσης του άλλου σταθμού και συνεχίζει να περιμένει για τη δική του μετάδοση για όσες χρονοθυρίδες του έχουν απομείνει [34].

2) DCF με CSMA/CA και RTS/CTS

Σε ένα δίκτυο WLAN, μπορεί να υπάρχουν περιπτώσεις όπου ορισμένοι ασύρματοι σταθμοί ενδέχεται να μην μπορούν να επικοινωνούν απευθείας με όλους τους άλλους ασύρματους σταθμούς του δικτύου. Οι περιπτώσεις αυτές είναι γνωστές ως ζητήματα του λεγόμενου κρυφού και εκτεθειμένου ασύρματου κόμβου. Το ζήτημα του κρυφού κόμβου παρουσιάζεται όταν δύο ασύρματοι κόμβοι (Α και C της εικόνας 2.11), που βρίσκονται εκτός της εμβέλειας εκπομπής τους και επομένως δεν μπορούν να αισθανθούν την ύπαρξη ο ένας του άλλου, προσπαθούν να εκπέμψουν δεδομένα προς

έναν ενδιάμεσο κόμβο B. Στην περίπτωση αυτή, καθώς οι ασύρματοι κόμβοι A και C δεν μπορούν να ακούσουν ο ένας την εκπομπή του άλλου και αρχίσουν να εκπέμπουν και οι δύο προς τον κόμβο B, τότε θα εμφανιστεί περίπτωση σύγκρουσης μεταξύ των εκπομπών των δύο κόμβων προς τον B. Αντίστοιχα, το ζήτημα του εκτεθειμένου κόμβου παρουσιάζεται όταν ή μετάδοση ενός ασύρματου κόμβου A προς το κόμβο D, παρεμβάλλει τη μετάδοση ενός κοντινού του κόμβου B, παρά το γεγονός ότι ο προβλεπόμενος κόμβος λήψης C της εκπομπής του κόμβου B βρίσκεται εκτός εμβέλειας της μετάδοσης του κόμβου A [36].

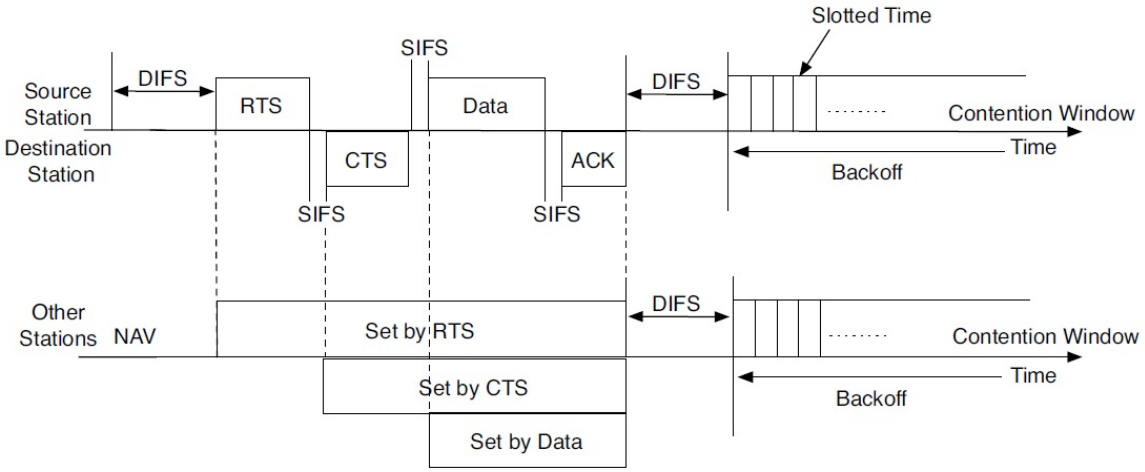


Εικόνα 2.11: Τα ζητήματα του κρυφού και του εκτεθειμένου κόμβου κατά τον έλεγχο της πρόσβασης στο ασύρματο μέσο [36]

Σε μια προσπάθεια να ξεπεραστούν αυτά τα ζητήματα, ο μηχανισμός DCF επιτρέπει την επιλογή χρήσης μιας προαιρετικής διαδικασίας ανταλλαγής πλαισίων ελέγχου μεταξύ δύο ασύρματων σταθμών που θέλουν να επικοινωνήσουν, τα οποία είναι γνωστά ως πλαίσια RTS και CTS. Σύμφωνα με αυτήν τη διαδικασία, η μετάδοση του πλαισίου RTS από έναν σταθμό εξυπηρετεί στη δέσμευση του μέσου μετάδοσης, καθώς και στην ειδοποίηση άλλων σταθμών εντός της εμβέλειάς του ότι θέλει να μεταδώσει ένα πλαίσιο δεδομένων. Με τη λήψη του πλαισίου RTS, ο σταθμός προορισμού αποκρίνεται μεταδίδοντας ένα πλαίσιο CTS, το οποίο εξυπηρετεί στην ενημέρωση του σταθμού προέλευσης ότι μπορεί να ξεκινήσει τη μετάδοση δεδομένων [17].

Στην εικόνα 2.12 παρουσιάζεται η διαδικασία χρονικής ακολουθίας της ανταλλαγής των πλαισίων RTS/CTS. Όπως παρουσιάστηκε και στην προηγούμενη περίπτωση λειτουργίας του μηχανισμού DCF μόνο με CSMA/CA, το πλαίσιο RTS θα αποσταλεί από τον σταθμό που θέλει να ξεκινήσει την μετάδοση προς όλους τους σταθμούς εντός της εμβέλειάς του, μόνο μετά την ανίχνευση ότι το ασύρματο μέσο είναι αδρανές για τουλάχιστον μία χρονική περίοδο DIFS. Στο πλαίσιο RTS ορίζεται η διάρκεια του διανύσματος NAV, η οποία σε αυτήν την περίπτωση αποτελεί το συνολικό χρονικό διάστημα που απαιτείται για τη μετάδοση του ίδιου του πλαισίου RTS, του πλαισίου CTS, του

πλαισίου δεδομένων συν του πλαισίου ACK της επιβεβαίωσης λήψης του. Μετά τη λήψη του πλαισίου RTS, ο σταθμός προορισμού περιμένει να περάσει ένα χρονικό διάστημα SIFS και μετά στέλνει ένα πλαίσιο CTS. Με τη μετάδοση του πλαισίου CTS, η διάρκεια του διανύσματος NAV ρυθμίζεται εκ νέου ώστε να περιλαμβάνει τη χρονική περίοδο που απαιτείται για τη μετάδοση του ίδιου του πλαισίου CTS, του πλαισίου δεδομένων συν του πλαισίου ACK της επιβεβαίωσης λήψης του. Με τη λήψη του πλαισίου CTS, ο σταθμός προέλευσης περιμένει να περάσει ένα χρονικό διάστημα SIFS και μετά ξεκινά τη μετάδοση του πλαισίου δεδομένων. Σε αυτήν την μετάδοση, η διάρκεια του διανύσματος NAV, που ορίζεται από το πλαίσιο δεδομένων, περιλαμβάνει τη χρονική περίοδο που απαιτείται για τη μετάδοση του ίδιου του πλαισίου δεδομένων συν του πλαισίου ACK επιβεβαίωσης λήψης του. Στην περίπτωση που ο σταθμός προέλευσης δεν λάβει πλαίσιο CTS, τότε ξεκινάει πάλι τη διαδικασία από την αρχή μετά από έναν τυχαίο χρόνο υπαναχώρησης. Σε όλη αυτή τη διάρκεια της ανταλλαγής των πλαισίων RTS/CTS μεταξύ δύο σταθμών, οι υπόλοιποι σταθμοί που βρίσκονται εντός της εμβέλειάς τους, ενημερώνουν αντίστοιχα τη διάρκεια των διανυσμάτων NAV τους, έτσι ώστε να είναι σε θέση να γνωρίζουν τη χρονική διάρκεια για την οποία το μέσο θα είναι δεσμευμένο. Σε αυτό το χρονικό διάστημα κανένας από τους υπόλοιπους σταθμούς δεν ξεκινάει κάποια διαδικασία αποστολής δεδομένων. Οι ρυθμίσεις αυτές έχουν ως αποτέλεσμα τη μείωση των πιθανοτήτων εμφάνισης των ζητημάτων του κρυφού ασύρματου κόμβου [34].



Εικόνα 2.12: Λειτουργία μηχανισμού DCF με CSMA/CA και RTS/CTS [34]

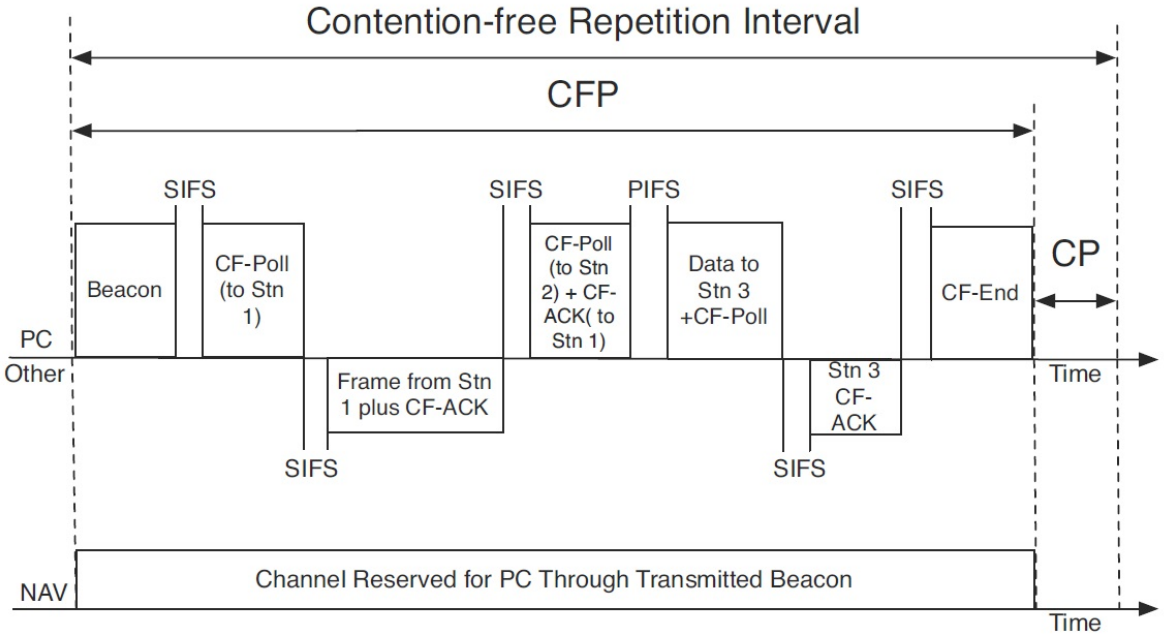
2.6.2 Μηχανισμός PCF

Ο μηχανισμός PCF που ορίζεται στο πρότυπο IEEE 802.11 παρέχει μια εναλλακτική μέθοδο πρόσβασης στο ασύρματο μέσο. Παρά το γεγονός ότι η χρήση του είναι προαιρετική, η διαλειτουργικότητα διατηρείται μεταξύ συσκευών που εφαρμόζουν μόνο τον μηχανισμό DCF και εκείνων που μπορούν να υποστηρίξουν και τους δύο μηχανισμούς πρόσβασης [37].

Σε αντίθεση με τον DCF, ο οποίος όπως αναφέρθηκε στην προηγούμενη υποενότητα είναι ένας μηχανισμός που βασίζεται στην ανίχνευση περιπτώσεων ανταγωνισμού, ο PCF εφαρμόζεται σε περιπτώσεις όπου η διαχείριση και η μετάδοση δεδομένων σε ένα δίκτυο WLAN δεν απαιτεί μια τέτοια ανίχνευση. Μια δεύτερη διαφορά του μηχανισμού PCF σε σύγκριση με τον DCF είναι ότι αποτελεί έναν μηχανισμό κεντρικού ελέγχου πρόσβασης στο μέσο. Αυτή η κεντρικοποιημένη λειτουργία του μηχανισμού PCF εκφράζεται μέσω της χρήσης μιας εξειδικευμένης οντότητας, που

ονομάζεται συντονιστής σημείων (Point Coordinator – PC), ο οποίος είναι υπεύθυνος για την εκχώρηση πρόσβασης στο μέσο. Για το λόγο αυτό, ο ρόλος του συντονιστή PC υλοποιείται σε ένα σημείο AP. Επομένως, ένα συντονιστής PC επιτρέπει την πρόσβαση στο μέσο και τη δυνατότητα μετάδοσης δεδομένων μόνο στους ασύρματους σταθμούς που σχετίζονται με το συγκεκριμένο σημείο AP. Μια τέτοια λειτουργία του μηχανισμού PCF τον καθιστούν κατάλληλο για χρήση μόνο σε σενάρια δικτύων υποδομής WLAN, σε αντίθεση με τον μηχανισμό DCF, ο οποίος μπορεί να εφαρμοστεί σε όλους τους τύπους δικτύων WLAN [34].

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι η πρόσβαση στο μέσο σε ένα δίκτυο WLAN δεν μπορεί να βασιστεί αποκλειστικά και μόνο στην μη ανίχνευση περιπτώσεων ανταγωνισμού. Αντ' αυτού, οι περίοδοι μη ανίχνευσης περιπτώσεων διαμάχης θα πρέπει να εναλλάσσονται τακτικά με περιόδους όπου η πρόσβαση στο μέσω επιτρέπεται μέσω ανίχνευσης περιπτώσεων διαμάχης. αυτό σημαίνει με πιο απλά λόγια, ότι ο μηχανισμός PCF δεν μπορεί να εφαρμοστεί κατά αποκλειστικότητα σε ένα δίκτυο WLAN, αλλά η εφαρμογή του θα πρέπει να αποτελεί συμπλήρωμα του μηχανισμού DCF. Έτσι, σε κάθε δίκτυο WLAN στο οποίο χρησιμοποιείται ο μηχανισμός PCF, ο χρόνος πρόσβασης στο ασύρματο μέσο διαιρείται σε περίοδο μη ανίχνευσης περιπτώσεων ανταγωνισμού (Contention-Free Period - CFP) και σε περίοδο ανίχνευσης περιπτώσεων διαμάχης (Contention Period - CP), στις οποίες η πρόσβαση στο μέσο ελέγχεται από τους μηχανισμούς PCF και DCF, αντίστοιχα. Η διάρκεια της περιόδου CP απαιτείται να είναι τουλάχιστον τέτοια ώστε να μπορούν να μεταδοθούν πλαίσια δεδομένων μέγιστου μεγέθους και το σχετικό πλαίσιο ACK επιβεβαίωσής τους. Η εναλλαγή των δύο περιόδων πρόσβασης CFP και CP πραγματοποιείται σε τακτά χρονικά διαστήματα, τα οποία είναι γνωστά ως διαστήματα επανάληψης CFP (CFP Repetition interval - CFPR). Στην εικόνα 2.13 παρουσιάζεται ένα διάστημα CFPR, στο οποίο απεικονίζεται η διαδικασία μετάδοσης δεδομένων μέσω του μηχανισμού PCF εντός μίας περιόδου CFP [34].



Εικόνα 2.13: Λειτουργία μηχανισμού PCF [34]

Η έναρξη μιας περιόδου CFP ορίζεται από τη μετάδοση ενός πλαισίου Beacon μέσω του σημείου AP και η μέγιστη διάρκειά της ανακοινώνεται μέσω της ρύθμισης του πεδίου CFPMaxDuration του

συγκεκριμένου πεδίου. Οι ασύρματοι σταθμοί που λαμβάνουν το πλαίσιο Beacon θα ορίσουν στη συνέχεια τη διάρκεια του διανύσματος NAV τους σύμφωνα με αυτές τις πληροφορίες, απενεργοποιώντας παράλληλα την πρόσβαση στο μέσο που βασίζεται στο μηχανισμό DCF. Προκειμένου να διασφαλιστεί περαιτέρω ότι ο συντονιστής PC αποκτά πλήρη έλεγχο του ασύρματου μέσου, όλες οι μεταδόσεις εντός μιας περιόδου CFP διαχωρίζονται από ένα διάστημα SIFS και ένα πρόσθετο διάστημα PIFS. Όπως αναφέρθηκε στην προηγούμενη υποενότητα, η διάρκεια του διαστήματος PIFS είναι μικρότερη εκείνης ενός διαστήματος DIFS (το οποίο χρησιμοποιείται στον μηχανισμό DCF) [34].

Καθώς το σημείο AP αποκτά τον έλεγχο του ασύρματου μέσου, ο συντονιστής PC ξεκινάει μια διαδικασία η οποία είναι γνωστή ως polling, με την οποία δημιουργεί μια λίστα ασύρματων σταθμών (polling list) που έχουν δυνατότητα υποστήριξης του μηχανισμού PCF και που επιθυμούν να μπορούν να μεταδίδουν πλαίσια δεδομένων κατά τη διάρκεια της περιόδου CFP, ώστε να τους επιτρέψει μια τέτοια μετάδοση. Οι ασύρματοι σταθμοί μπαίνουν στη λίστα polling μέσω της αρχικής διαδικασίας αιτήματος συσχέτισης με το σημείο AP. Η διαδικασία αιτήματος συσχέτισης επιτρέπει ουσιαστικά στο σημείο AP να προσδιορίσει εάν ένας ασύρματος σταθμός είναι ικανός να ανταποκρίνεται σε πλαίσια polling κατά τη διάρκεια μιας περιόδου CFP [34].

Οι ασύρματοι σταθμοί μπορούν να εκπέμπουν δεδομένα μόνο αφού λάβουν ένα πλαίσιο CF-Poll από τον συντονιστή PC, με κάθε CF-Poll να επιτρέπει μόνο μία μετάδοση πλαισίου δεδομένων. Για παράδειγμα, στην Εικόνα 2.13 ο συντονιστής PC στέλνει ένα πλαίσιο CF-Poll στον σταθμό 1, ο σταθμός 1 έχει ένα πλαίσιο δεδομένων για αποστολή στον σταθμό 3, το οποίο και μεταδίδει μαζί με μια επιβεβαίωση για τη λήψη του CF-Poll (CF-ACK). Μετά την ολοκλήρωση της μετάδοσης του πλαισίου δεδομένων από το σταθμό 1, ο συντονιστής PC μεταδίδει στη συνέχεια ένα πλαίσιο CF-Poll στο σταθμό 2 μετά από ένα διάστημα SIFS. Στο πλαίσιο αυτό περιλαμβάνεται και ένα μήνυμα επιβεβαίωσης CF-ACK, το οποίο δείχνει ότι το πακέτο δεδομένων του σταθμού 1 στάλθηκε με επιτυχία. Δεδομένου ότι ο σταθμός 2 δεν έχει δεδομένα για μετάδοση, ο συντονιστής PC, αφού περιμένει ένα διάστημα PIFS, στέλνει ένα πλαίσιο CF-Poll στον σταθμό 3, μαζί με το πλαίσιο δεδομένων που έχει λάβει από το σταθμό 1 και που προορίζεται για το σταθμό 3. Με τη λήψη του πλαισίου CF-Poll και του πλαισίου δεδομένων, ο σταθμός 3 απλώς στέλνει προς τον συντονιστή PC ένα μήνυμα επιβεβαίωσης CF-ACK, μετά από ένα SIFS. Ο συντονιστής PC δηλώνει το τέλος της περιόδου CFP μέσω ενός πλαισίου εκπομπής CF-End, το οποίο σηματοδοτεί και την έναρξη της περιόδου CP για μεταδόσεις που βασίζονται στον μηχανισμό DCF [34].

Όπως φαίνεται στην εικόνα 2.13, ο μηχανισμός PCF ενσωματώνει τη δυνατότητα συνδυασμού πολλών τύπων πλαισίων σε ένα ενιαίο πλαίσιο μετάδοσης. Αυτή η διαδικασία του επιτρέπει να παρουσιάζει βελτίωση της αποδοτικότητας χρήσης του μέσου [34].

2.7 Υπηρεσίες IEEE 802.11

Ένας τρόπος ορισμού ενός δικτυακού προτύπου είναι μέσω των υπηρεσιών που παρέχει. Οι υπηρεσίες αυτές μπορούν να χρησιμοποιηθούν από τους φορείς εκμετάλλευσης του δικτύου με τον καταλληλότερο τρόπο. Το πρότυπο IEEE 802.11 παρέχει ένα σύνολο υπηρεσιών, οι οποίες χρησιμοποιούνται για την μετάδοση των δεδομένων μεταξύ των οντοτήτων του δικτύου, καθώς και για την διαχείριση του συνολικού δικτύου, ώστε να δίνεται η δυνατότητα παρακολούθησης των ασύρματων σταθμών και μεταφοράς των εκάστοτε πλαισίων σε αυτούς [17]. Στις επόμενες υποενότητες αναλύονται οι σημαντικότερες από τις υπηρεσίες που παρέχει το πρότυπο IEEE 802.11.

2.7.1 Επιβεβαίωση δεδομένων

Κατά τη διάρκεια μια μετάδοσης δεδομένων μεταξύ του αποστολέα και του παραλήπτη, υπάρχει πάντα η πιθανότητα απώλειας πακέτων για διάφορους λόγους, όπως για παράδειγμα η ύπαρξη παρεμβολών. Το πρότυπο IEEE 802.11 περιλαμβάνει μια τεχνική επιβεβαίωσης δεδομένων, η οποία αποτελεί μέρος του μηχανισμού CSMA/CA, για να διασφαλιστεί ότι τα δεδομένα δεν θα χαθούν κατά την επικοινωνία [27].

Η τεχνική της επιβεβαίωσης δεδομένων βασίζεται στην ανταλλαγή πακέτων, κατά την οποία ο δέκτης στέλνει ένα πακέτο στη μονάδα αποστολής ενημερώνοντάς την ότι το πακέτο έχει παραληφθεί. Στην περίπτωση που ο αποστολέας δεν λάβει αυτήν την επιβεβαίωση, θα θεωρήσει το πακέτο έχει χαθεί και θα ενεργοποιηθεί ο μηχανισμός CSMA/CA .Ο αποστολέας περιμένει τυχαία χρονικά διαστήματα υπαναχώρησης προκειμένου να αποφευχθούν πιθανές συγκρούσεις. Στη συνέχεια, προσπαθεί ξανά να μεταδώσει τα δεδομένα, επαναλαμβάνοντας τη διαδικασία αν απαιτείται. Ο στόχος είναι η αποτελεσματική χρήση του καναλιού, αποφυγή συγκρούσεων και διασφάλιση αξιόπιστης επικοινωνίας. Όπως αναφέρθηκε στην προηγούμενη ενότητα, κάθε σταθμός έχει ένα όριο επαναληπτικών προσπαθειών μετάδοσης πακέτων, στην περίπτωση που τα πακέτα έχουν χαθεί για κάποιο λόγο. Εάν αυτό το όριο των ανεπιτυχών προσπαθειών μετάδοσης φτάσει στο μέγιστο, τότε το πακέτο απορρίπτεται. Αυτός ο μηχανισμός επιτρέπει την ανάκτηση των αποστολών από παρεμβολές χωρίς ο τελικός χρήστης να παρατηρήσει ότι παρουσιάστηκε κάποιο σφάλμα επικοινωνίας [34].

2.7.2 Κατακερματισμός

Τα ασύρματα δίκτυα είναι πολύ πιο ευάλωτα σε παρεμβολές από τα ενσύρματα, σε τέτοιο βαθμό που θα μπορούσε να πει κάποιος ότι οι παρεμβολές αποτελούν μια πραγματικότητα και όχι μόνο μια πιθανότητα. Όταν ένα πακέτο αποστέλλεται μέσω ενός ασύρματου περιβάλλοντος, υπάρχει μεγάλη πιθανότητα ένα ή περισσότερα bit του να καταστραφούν, γεγονός που θα οδηγήσει σε εκ νέου αποστολή του, ανεξάρτητα από το μέγεθος των κατεστραμμένων bit [38]. Ένας τρόπος αντιμετώπισης αυτού του προβλήματος στα ασύρματα δίκτυα είναι η μετάδοση πακέτων μικρότερου μήκους σε σύγκριση με αυτά που αποστέλλονται μέσω των ενσύρματων δικτύων. Η τεχνική που χρησιμοποιείται για τη μείωση του μήκους των πακέτων των δεδομένων που αποστέλλονται στα ασύρματα δίκτυα ονομάζεται κατακερματισμός (fragmentation), ένα χαρακτηριστικό του επιπέδου MAC που αποσκοπεί στην αύξηση της αξιοπιστίας της μετάδοσης μέσω ασύρματου μέσου. Για κάθε τμήμα του πακέτου, αποστέλλεται μεμονωμένα ένα μήνυμα επιβεβαίωσης λήψης του. Εάν για κάποιο τμήμα δεν αποσταλεί μήνυμα επιβεβαίωσης λήψης (άρα δεν έχει ληφθεί λόγω σφάλματος ή σύγκρουσης) τότε απαιτείται αναμετάδοση μόνο του συγκεκριμένου τμήματος και όχι ολόκληρου του πλαισίου, γεγονός που αυξάνει την αποτελεσματική απόδοση του μέσου [39].

Ωστόσο, η τεχνική του κατακερματισμού μπορεί να οδηγήσει σε πρόβλημα υπερβολικής επιβάρυνσης του δικτύου, καθώς κάθε τμήμα που αποστέλλεται περιέχει, εκτός από την κεφαλίδα MAC 802.11 και τα δεδομένα, και ένα πλαίσιο επιβεβαίωσης. Για την αντιμετώπιση του συγκεκριμένου ζητήματος, η τεχνική του κατακερματισμού στο πρότυπο IEEE 802.11 περιλαμβάνει δυνατότητα διαμόρφωσης, κάτι που επιτρέπει στον διαχειριστή του δικτύου να ορίζει την αποστολή πακέτων μικρού μήκους σε ορισμένες περιοχές και την αποστολή πακέτων μεγαλύτερου μήκους σε περιοχές που η πιθανότητα παρεμβολών είναι μικρότερη [17].

2.7.3 Σάρωση

Με τον όρο σάρωση (scanning) εννοείται η λειτουργία αναζήτησης ενός σταθμού για το καταλληλότερο σημείο AP με το οποίο απαιτείται να συνδεθεί. Το πρότυπο IEEE 802.11 υποστηρίζει δύο μεθόδους σάρωσης [40]: την ενεργητική και την παθητική σάρωση. Όταν ο σταθμός σαρώνει ενεργά, στέλνει ένα αίτημα ανίχνευσης και περιμένει να λάβει μια απάντηση ανίχνευσης από κάποιο σημείο AP, ενώ κατά τη διάρκεια της παθητικής σάρωσης, ο σταθμός ακούει σε κάθε κανάλι για την εμφάνιση κάποιου beacon που αποστέλλεται περιοδικά από ένα σημείο AP. Και στις δύο περιπτώσεις σάρωσης, όταν ο σταθμός λαμβάνεται μια απόκριση ανίχνευσης από ένα σημείο AP, αποθηκεύσει το αναγνωριστικό του BSS (BSSID) και το χρόνο λήψης της απόκρισης (Timestamp). Σε σύγκριση με την ενεργή σάρωση, η παθητική απαιτεί περισσότερο χρόνο, καθώς ο σταθμός πρέπει να περιμένει την εμφάνιση κάποιου beacon από το σημείο AP. Επί πλέον, εάν ο σταθμός δεν περιμένει αρκετό χρονικό διάστημα για την εμφάνιση του beacon, ενδέχεται να το χάσει [40].

2.7.4 Πιστοποίηση

Κατά τη λειτουργία της πιστοποίησης (authentication), κάθε ασύρματη συσκευή δηλώνει την ταυτότητά της στις υπόλοιπες συσκευές του δικτύου, χωρίς την οποία, η συσκευή δεν μπορεί να έχει πρόσβαση στο ασύρματο δίκτυο. Η ασύρματη συσκευή μπορεί να πιστοποιήσει την ταυτότητά της σε ένα ή περισσότερα σημεία AP ταυτόχρονα. Το πρότυπο IEEE 802.11 υποστηρίζει δύο τρόπους πιστοποίησης [41]: (α) την πιστοποίηση μέσω επαλήθευσης κοινού κλειδιού (SKA) και (β) την πιστοποίηση ανοικτού συστήματος (OSA). Κατά την πιστοποίηση SKA (Shared Key Authentication) ο ασύρματος σταθμός απαιτείται να χρησιμοποιήσει το μηχανισμό WEP (Wired Equivalent Privacy) και να διαθέτει το κλειδί κρυπτογράφησης WEP που να ταιριάζει με το κλειδί που είναι αποθηκευμένο στο ασύρματο σημείο AP. Το κοινόχρηστο μυστικό κλειδί μεταδίδεται και παραδίδεται στους συμμετέχοντες σταθμούς μέσω της χρήσης ενός ασφαλούς καναλιού επικοινωνίας. Η όλη διαδικασία θα αναλυθεί περισσότερο σε επόμενο κεφάλαιο. Η πιστοποίηση OSA (Open System Authentication) αποτελεί έναν μηδενικό αλγόριθμο ελέγχου ταυτότητας που δεν απαιτεί τη χρήση κοινόχρηστου κλειδιού. Στην περίπτωση αυτή, ο σταθμός στέλνει ένα αίτημα πιστοποίησης, το οποίο περιέχει το αναγνωριστικό του (συνήθως τη διεύθυνση MAC). Η πιστοποίηση του σταθμού πραγματοποιείται μόνο αν ο σταθμός λάβει μια ανάλογη απάντηση. Η μόνη απαίτηση για τη χρήση του αλγόριθμου πιστοποίησης OSA είναι, ο σταθμός να έχει ρυθμιστεί ώστε να μπορεί να τον υποστηρίξει [41].

2.7.5 Συσχέτιση

Μετά την ολοκλήρωση της διαδικασίας της πιστοποίησης, κάθε ασύρματος σταθμός μπορεί να συσχετιστεί (συνδεθεί) με το σημείο AP για να αποκτήσει πλήρη πρόσβαση στο δίκτυο. Αυτός η συσχέτιση (association) εγγυάται τη σωστή παράδοση των πλαισίων δεδομένων στις ασύρματες συσκευές, αφού ενεργοποιεί το σημείο AP ώστε να πραγματοποιήσει εγγραφή κάθε συσκευής του BSS. Για το λόγο αυτό, ένας κόμβος δεν μπορεί να συσχετιστεί ταυτόχρονα με περισσότερα από ένα σημείο AP. Η διαδικασία συσχέτισης πραγματοποιείται μόνο στα ασύρματα δίκτυα υποδομής και όχι σε δίκτυα P2P [42].

Εκτός από τη διαδικασία της συσχέτισης, τα δίκτυα IEEE 802.11 μπορούν να υποστηρίξουν και διαδικασίες επανα-συσχέτισης (re-association), οι οποίες επιτρέπουν την απρόσκοπτη κίνηση των ασύρματων συσκευών μεταξύ διάφορων σημείων AP. Στην περίπτωση της επανα-συσχέτισης, παρατηρείται συνδυασμός της διαδικασίας συσχέτισης και μιας ειδοποίησης που υποδεικνύει το

σημείο AP με το οποίο είχε συνδεθεί προηγουμένως η συσκευή. Με τον τρόπο αυτό δίνεται η δυνατότητα στο νέο σημείο AP να αποδεχτεί τη συσχέτιση με τον κόμβο και να στείλει ένα αίτημα ζητώντας να προωθηθούν δεδομένα που έχουν αποθηκευτεί στο buffer του προηγούμενου σημείου AP και αφορούν τον συγκεκριμένο κόμβο [40].

2.7.6 Περιαγωγή

Με τον όρο περιαγωγή (roaming) υποδηλώνεται η δυνατότητα μετακίνησης των ασύρματων σταθμών μεταξύ διάφορων σημείων AP στο ίδιο ή σε διαφορετικό κανάλι, χωρίς να απαιτείται η τροποποίηση των υπηρεσιών δικτύου. Η επιλογή της πραγματοποίησης περιαγωγής ενός ασύρματου σταθμού μεταξύ διαφορετικών σημείων AP εξαρτάται σε μεγάλο βαθμό από την ποιότητα του σήματος ενός σημείου AP. Η περιαγωγή, επομένως, δίνει τη δυνατότητα σε κάθε ασύρματο σταθμό να επιλέγει σύνδεση με σημείο AP με ισχυρότερο σήμα ή με λιγότερο θόρυβο [27].

2.7.7 Διαχείριση ενέργειας

Καθώς η κινητικότητα αποτελεί ένα από τα πιο σημαντικά χαρακτηριστικά των ασύρματων δικτύων, η κατανάλωση των κινητών συσκευών αποτελεί ένα από τα σημαντικότερα ζητήματα που αντιμετωπίζουν. Σε μια προσπάθεια αντιμετώπισης του ζητήματος της εξοικονόμησης ενέργειας, το πρότυπο IEEE 802.11 περιλαμβάνει έναν μηχανισμό που επιτρέπει στους σταθμούς να μπαίνουν σε αδράνεια, ώστε να μπορούν να εξοικονομούν ενέργεια, για μεγάλα χρονικά διαστήματα, χωρίς να υπάρχει κίνδυνος απώλειας επικοινωνίας με το δίκτυο ή οποιασδήποτε πληροφορίας [43].

Η βασική φιλοσοφία αυτού του μηχανισμού είναι ότι το σημείο AP ενημερώνει συνεχώς μια καταγραφή των σταθμών που βρίσκονται σε λειτουργία εξοικονόμησης ενέργειας. Πριν την εισαγωγή σε αυτόν τον τρόπο λειτουργίας, κάθε ασύρματη συσκευή στέλνει ένα μήνυμα στο σημείο AP με το οποίο συσχετίζεται ότι πρόκειται να μεταβεί σε λειτουργία εξοικονόμησης ενέργειας, χρησιμοποιώντας ένα πλαίσιο PS-Poll (Power Save Poll) των 20 byte. Το σημείο AP αποθηκεύει προσωρινά όλα τα πακέτα που αφορούν τις συσκευές που υπάρχουν στη λίστα των συσκευών με λειτουργία εξοικονόμησης ενέργειας και τους τα στέλνει, μόνο μετά από δικό τους αίτημα ή μετά την αλλαγή του τρόπου λειτουργίας τους. Επίσης, αποστέλλει περιοδικά beacon προς τις συσκευές που βρίσκονται σε λειτουργία εξοικονόμησης ενέργειας, ενημερώνοντάς τους ότι έχει αποθηκευμένα προσωρινά πακέτα που τα αφορούν, έτσι ώστε αυτές οι συσκευές να ενεργοποιηθούν. Σε αυτήν την περίπτωση, οι συσκευές αποστέλλουν μήνυμα PS-Poll προς το σημείο AP για να λάβουν αυτά τα πακέτα [44].

2.8 Τροποποιήσεις προτύπου IEEE 802.11

Οι μηχανισμοί που περιλαμβάνει το πρότυπο IEEE 802.11 και το σύνολο των υπηρεσιών που μπορεί να παρέχει, δεν θεωρήθηκαν επαρκή για τη ευρεία αποδοχή του, λόγω διαφόρων ζητημάτων που παρουσίαζε, όπως το ζήτημα της διαλειτουργικότητας, του υψηλού κόστους και της ανεπαρκούς απόδοσης. Για τους λόγους αυτούς, ο οργανισμός IEEE μπήκε σε μια διαδικασία σταδιακής εξέλιξης του βασικού προτύπου, κάτι που τελικά έχει οδηγήσει στην κατά καιρούς δημιουργία τροποποιήσεών του με ολοένα και καλύτερα χαρακτηριστικά και υποστηριζόμενες υπηρεσίες.

Στον πίνακα 2.1 παρουσιάζονται τα διαφορετικά πρότυπα, το έτος κυκλοφορίας, οι ζώνες συχνοτήτων, το εύρος ζώνης και οι μέγιστοι θεωρητικοί ρυθμοί μετάδοσης δεδομένων που επιτεύχθηκαν. Οι πραγματικοί ρυθμοί μεταφοράς δεδομένων είναι χαμηλότεροι από τους θεωρητικούς λόγω της συμβολής πολλών παραγόντων, όπως η υποβάθμιση του σήματος με την απόσταση, ο

ρυθμός διαμόρφωσης, ο μηχανισμός κωδικοποίησης FEC, το εύρος ζώνης καναλιού, η τεχνολογία MIMO, τα διαστήματα προστασίας και τα ποσοστά σφάλματος. Η οικογένεια προτύπων IEEE 802.11 αποτελείται από μια σειρά τεχνικών ημι-αμφίδρομης διαμόρφωσης OTA (over-the-air) που χρησιμοποιούν το ίδιο βασικό πρωτόκολλο για ασύρματη επικοινωνία [45].

2.8.1 IEEE 802.11a

Τον Ιούνιο του 1997, ανακοινώθηκε μια από τις επεκτάσεις φυσικού επιπέδου του προτύπου IEEE 802.11, η οποία αφορούσε το πρότυπο IEEE 802.11a το οποίο εγκατέλειψε τη χρήση της τεχνολογίας του φάσματος διασποράς (spread spectrum) και χρησιμοποίησε μια τεχνική κωδικοποίησης που ονομάζεται OFDM (Orthogonal Frequency Division Multiplexing). Οι συσκευές IEEE 802.11a λειτουργούν στην περιοχή συχνοτήτων 5 - 6GHz και υποστηρίζουν υψηλές ταχύτητες μεταφοράς δεδομένων έως και 6, 12, 24 και 54Mbps [27].

Πίνακας 2.1: Εξέλιξη πρωτοκόλλων IEEE 802.11 [45]

Πρωτόκολλα IEEE 802.11	**Έτος έκδοσης**	**Συχνότητα λειτουργίας (GHz)**	**Εύρος ζώνης καναλιού (MHz)**	**Μέγιστη ταχύτητα μεταφοράς δεδομένων**
Βασικό πρότυπο IEEE 802.11	1997	2,4	22	2Mbps
IEEE 802.11b	1999	2,4	22	11Mbps
IEEE 802.11a	1999	5	20	54Mbps
IEEE 802.11g	2003	2,4	20	54Mbps
IEEE 802.11n (Wi-Fi 4)	2009	2,4 / 5	20 / 40	600Mbps
IEEE 802.11ac (Wi-Fi 5)	2013	5	20 / 40 / 80/ 160	6,8Gbps
IEEE 802.11ax (Wi-Fi 6)	2019	2,5 / 5	20 / 40 / 80/ 160	9,6Gbps
IEEE 802.11ax (Wi-Fi 6E)	2020	2,5 / 5 / 6	20 / 40 / 80/ 160	9,6Gbps

Καθώς το συγκεκριμένο πρότυπο λειτουργεί σε διαφορετική περιοχή συχνοτήτων από ότι το πρότυπο IEEE 802.11b, που δημοσιεύτηκε την ίδια σχεδόν περίοδο, τα προϊόντα 802.11a δεν είναι συμβατά με τα 802.11b καθώς η μεταξύ τους διαλειτουργικότητα είναι αδύνατη. Αυτό αποτελεί έναν από τους περιορισμούς του προτύπου IEEE 802.11a. Παρόλα αυτά, τα προϊόντα των δύο προτύπων μπορούν να συνυπάρχουν στο ίδιο περιβάλλον αφού δεν παρουσιάζουν παρεμβολές στα σήματά τους. Το δεύτερο μειονέκτημα του προτύπου είναι η μικρότερη εμβέλεια λειτουργίας των συσκευών IEEE 802.11a σε σύγκριση με εκείνη των 802.11b [46].

Η μετάδοση στη ζώνη συχνοτήτων των 5GHz δίνει στο IEEE 802.11a το πλεονέκτημα της αντιμετώπισης λιγότερων παρεμβολών σε σύγκριση με το IEEE 802.11b, που λειτουργεί στην πιο πολυσύχναστη ζώνη ISM των 2,4GHz. Ταυτόχρονα όμως, αλλά η υψηλότερη συχνότητα φορέα παρουσιάζει και ένα πολύ σημαντικό μειονέκτημα, καθώς περιορίζει το IEEE 802.11a να χρησιμοποιηθεί σε εφαρμογές όχι πλήρους οπτικής επαφής. Ο συνδυασμός αυτού του μειονεκτήματος με το γεγονός της μικρότερης διείσδυσης των ραδιοκυμάτων που παρουσιάζεται στα 5GHz, οδηγεί

στο συμπέρασμα, ότι για τη χρήση του IEEE 802.11a σε εσωτερικούς χώρους απαιτείται μεγαλύτερος αριθμός σημείων AP ώστε να καλυφθεί πλήρως μια δεδομένη περιοχή λειτουργίας [46].

2.8.2 IEEE 802.11b

Το Σεπτέμβριο του 1999, παρουσιάστηκε η βασική αναθεώρηση του προτύπου IEEE 802.11, με την εμφάνιση του λεγόμενου IEEE 802.11 High Rate (HR/DSSS) ή IEEE 802.11b. Το IEEE 802.11b εισήγαγε δύο νέες ταχύτητες μεταφοράς δεδομένων, 5 και 11Mbps, και τυποποίησε το φυσικό επίπεδο για να τις υποστηρίξει. Για να μπορεί να επιτευχθεί αυτή η υποστήριξη, το DSSS έπρεπε να επιλεγεί ως η μόνη μέθοδος μετάδοσης δεδομένων φυσικού επιπέδου του προτύπου, με αποτέλεσμα το πρότυπο IEEE 802.11b να μην περιλαμβάνει και να υποστηρίζει καθόλου την τεχνική FHSS. Η επίτευξη μιας ταχύτητας μεταφοράς δεδομένων των 11Mbps που υποστηρίζει η τεχνική DSSS του IEEE 802.11b σε σύγκριση με τα 2Mbps που μπορούσε να υποστηρίξει το DSSS του IEEE 802.11 ήταν πολύ εύκολη, καθώς το βασικό σχήμα διαμόρφωσης ήταν πολύ παρόμοιο. Με τον τρόπο αυτό μπορούσε να επιτευχθεί επίσης συνύπαρξη των συστημάτων IEEE 802.11 με τα συστήματα IEEE 802.11b, κάτι που επέτρεπε την ομαλή μετάβαση σε τεχνολογία Wi-Fi υψηλότερου ρυθμού μετάδοσης δεδομένων, αλλά και τη σημαντική βελτίωση της απόδοσής τους, διατηρώντας παράλληλα το ίδιο πρωτόκολλο [27].

Το πρότυπο IEEE 802.11b μπορεί επίσης να υποστηρίξει δυναμικά προσαρμόσιμο ρυθμό μετάδοσης δεδομένων, με σκοπό την αντιμετώπιση των παρεμβολών. Αυτό σημαίνει ότι οι συσκευές IEEE 802.11b μπορούν να προσαρμόσουν το ρυθμό μεταφοράς δεδομένων και να λειτουργήσουν αυτόματα σε χαμηλές ταχύτητες εάν υπάρχουν σημαντικές παρεμβολές, πέφτοντας στα 5,5Mbps, 2Mbps και 1Mbps [46].

2.8.3 IEEE 802.11g

Τον Νοέμβριο του 2001 ο οργανισμός IEEE ανακοίνωσε την έκδοση ενός νέου προτύπου, του IEEE 802.11g. Το νέο πρότυπο χρησιμοποιεί το σχήμα μετάδοσης OFDM (όπως το IEEE 802.11a) και λειτουργεί στη ζώνη των 2,4GHz (όπως το IEEE 802.11b). Αν και το πρότυπο IEEE 802.11g είναι σε θέση να υποστηρίξει μέγιστο ρυθμό μεταφοράς δεδομένων 54Mbps (με τεχνική διόρθωσης λαθών FEC (Forward Error Correction)), στην πραγματικότητα μπόρεσε να υποστηρίξει μέση απόδοση της τάξης των 22Mbps (λόγω της μικρής ανθεκτικότητάς του στις παρεμβολές της ζώνης των 2,4GHz) [27].

Το IEEE 802.11g παρουσίασε δύο διαφορετικές τεχνικές διαμόρφωσης που υποστηρίζουν διαφορετικούς ρυθμούς μετάδοσης δεδομένων [46]: (α) τεχνική OFDM, που υποστηρίζει ταχύτητα μετάδοσης δεδομένων με ρυθμό της τάξης των 54Mbps και (β) τεχνική PBCC (Packet Binary Convolution Code), που υποστηρίζει ταχύτητες μεταφοράς δεδομένων με ρυθμούς 22 και 33Mbps. Τέλος, το πρότυπο κατάφερε να παρουσιάσει συμβατότητα μεταξύ των προϊόντων IEEE 802.11g και IEEE 802.11b, κάτι που οδήγησε στην γρήγορη υιοθέτησή του από τους κατασκευαστές. Κάτι τέτοιο είχε ως αποτέλεσμα την τελική οριστικοποίηση του προτύπου IEEE 802.11g από τον οργανισμό IEEE στις 13 Ιουνίου 2003 [46].

2.8.4 IEEE 802.11n

Το πρότυπο IEEE 802.11n παρουσιάστηκε από τον οργανισμό IEEE με στόχο την περαιτέρω βελτίωση των προηγούμενων τροποποιήσεων του βασικού προτύπου IEEE 802.11, αυξάνοντας την εμβέλεια και την ταχύτητα μετάδοσης δεδομένων για τα δίκτυα WLAN έως και τα 600Mbps. Αυτή η

βελτίωση πραγματοποιήθηκε με την προσθήκη κεραιών πολλαπλής εισόδου πολλαπλής εξόδου MIMO (Multiple Input Multiple Output). Το πρότυπο μπορεί να λειτουργήσει τόσο στη ζώνη συχνοτήτων 2,4GHz, όπου μπορεί να υποστηρίξει ταχύτητες μεταφοράς δεδομένων της τάξης των 100Mbps, όσο και στα 5GHz με ρυθμό μετάδοσης δεδομένων έως 600Mbps [27].

Ο οργανισμός IEEE ενέκρινε και δημοσίευσε τελικά την τροποποίηση τον Οκτώβριο του 2009. Πριν από την τελική επικύρωση, πολλές επιχειρήσεις είχαν ήδη τροποποιήσει τα δίκτυά τους με βάση την πιστοποίηση προϊόντων της Wi-Fi Alliance που συμμορφώνονταν με το προσχέδιο του IEEE 802.11n του 2007 [46]. Με το IEEE 802.11n, τα δίκτυα Wi-Fi έγιναν ακόμα πιο γρήγορα και πιο αξιόπιστα, διατηρώντας παράλληλα τη συμβατότητα με τις προηγούμενες τροποποιήσεις. Τα χαρακτηριστικά αυτά, το κατέστησαν σύντομα ένα ευρέως διαδεδομένο και δημοφιλές πρότυπο. Αυτό επιτεύχθηκε με την προσθήκη της τεχνολογίας MIMO και της δυνατότητας χρήσης ενός διπλάσιου μεγέθους εύρους ζώνης (40MHz) στο επίπεδο PHY, καθώς και της μεθόδου συνάθροισης πλαισίων στο επίπεδο MAC, όπου πολλαπλές μονάδες MSDU (MAC Service Data Units) ή μονάδες MPDU (MAC Protocol Data Units) συνενώνονται για να μειώσουν την επιβάρυνση (overhead) του πρωτοκόλλου και να την ισομοιράσουν σε πολλά πλαίσια, αυξάνοντας έτσι τον ρυθμό μετάδοσης δεδομένων σε επίπεδο χρήστη [45].

2.8.5 IEEE 802.11ac

Το IEEE 802.11ac είναι ένα πρότυπο ασύρματης δικτύωσης που λειτουργεί στη ζώνη των 5GHz και που έχει επισημανθεί αναδρομικά από τη Wi-Fi Alliance ως Wi-Fi 5. Η προδιαγραφή είναι σε θέση να παρουσιάσει απόδοση πολλαπλών σταθμών έως και 1,1Gbps, ενώ στην περίπτωση υποστήριξης μονής σύνδεσης, ο ρυθμός μεταφοράς δεδομένων μπορεί να φτάσει τα 0,5Gbps. Αυτές οι ταχύτητες μεταφοράς δεδομένων είναι εφικτές στο IEEE 802.11ac λόγω της επέκτασης των δυνατοτήτων της διεπαφής αέρα που υποστηρίζεται από το IEEE 802.11n. Οι επεκτάσεις αυτές αφορούν τη χρήση μεγαλύτερου εύρους ζώνης (έως 160MHz), την υποστήριξη μεγαλύτερου αριθμού χωρικών ροών MIMO (έως 8), τη δυνατότητα υποστήριξης κατερχόμενης σύνδεσης πολλαπλών χρηστών MIMO (έως 4 πελάτες) και τη διαμόρφωση υψηλής πυκνότητας (έως 256QAM) [45].

Το IEEE 802.11ac υποστηρίζει τη συμβατότητα με άλλες τεχνολογίες IEEE 802.11 που λειτουργούν στην ίδια συχνότητα των 5GHz. Η εμπορευματοποίηση των προϊόντων του προτύπου έγινε σε δύο φάσεις, που ονομάστηκαν "Wave 1" και "Wave 2". Από τα μέσα του 2013, η Wi-Fi Alliance άρχισε να πιστοποιεί προϊόντα Wave 1 802.11ac που υποστηρίζουν μόνο κανάλια εύρους 80MHz και έως και 3 χωρικές ροές, χαρακτηριστικά που οδηγούν στην επίτευξη ρυθμού μεταφοράς δεδομένων έως και 1,3Gbps. Στη συνέχεια, το 2016, η Wi-Fi Alliance εισήγαγε την πιστοποίηση Wave 2, η οποία περιλαμβάνει πρόσθετες λειτουργίες, όπως τεχνική MIMO πολλαπλών χρηστών (MU-MIMO), υποστήριξη καναλιών εύρους 160MHz και τέσσερις χωρικές ροές. Η προσθήκη αυτών των λειτουργιών σήμαινε ότι τα προϊόντα Wave 2 μπορούσαν να παρουσιάσουν υψηλότερο εύρος ζώνης και χωρητικότητα από τα προϊόντα Wave 1 (παρουσιάζοντας πολύ μεγαλύτερες ταχύτητες μεταφοράς δεδομένων έως και 2,34Gbps) [46].

2.8.6 IEEE 802.11ax

Το IEEE 802.11ax κυκλοφόρησε ως διάδοχος του IEEE 802.11ac και είναι γνωστό ως Wi-Fi 6 (λειτουργώντας στις ζώνες συχνοτήτων 2,4GHz και 5GHz), αλλά και ως Wi-Fi 6E (λειτουργώντας στη ζώνη συχνοτήτων των 6GHz). Είναι επίσης γνωστό ως Wi-Fi υψηλής απόδοσης, λόγω των συνολικών βελτιώσεων στην απόδοση των πελατών Wi-Fi σε πυκνά περιβάλλοντα. Το πρότυπο

μπορεί επίσης να λειτουργήσει στη μη αδειοδοτημένη μπάντα συχνοτήτων μεταξύ 1GHz και 7,125GHz. Ο κύριος στόχος του σχεδιασμού του προτύπου είναι η ενίσχυση της απόδοσης ανά περιοχή σε σενάρια υψηλής πυκνότητας, όπως εταιρικά γραφεία, εμπορικά κέντρα και πυκνά συγκροτήματα κατοικιών. Ενώ η βελτίωση του ονομαστικού ρυθμού μετάδοσης δεδομένων έναντι του IEEE 802.11ac είναι μόνο 37%, η συνολική αύξηση της απόδοσης (σε ολόκληρο το δίκτυο) είναι της τάξης του 400% (δηλαδή μέγιστη ταχύτητα μετάδοσης δεδομένων της τάξης των 9,6Gbps), κάτι που μεταφράζεται επίσης σε 75% χαμηλότερη λανθάνουσα κατάσταση [47].

Ο τετραπλασιασμός της συνολικής απόδοσης καθίσταται δυνατός χάρη στην υψηλότερη φασματική απόδοση. Το βασικό χαρακτηριστικό στο οποίο βασίζεται το IEEE 802.11ax είναι η χρήση της τεχνικής OFDMA (Orthogonal Frequency Division Multiple Access), η οποία είναι ισοδύναμη με την εφαρμογή της κυψελοειδούς τεχνολογίας σε δίκτυα Wi-Fi. Άλλες βελτιώσεις στη χρήση του φάσματος αποτελούν οι καλύτερες μέθοδοι ελέγχου ισχύος για την αποφυγή των παρεμβολών από γειτονικά δίκτυα, η χρήση υψηλότερης τάξης σχήματος διαμόρφωσης (1024-QAM), η υποστήριξη της τεχνικής MU-MIMO και στα δύο κανάλια ζεύξης (ανερχόμενη και κατερχόμενη) για περαιτέρω αύξηση της απόδοσης, καθώς και βελτιώσεις αξιοπιστίας της κατανάλωσης ενέργειας και των πρωτοκόλλων ασφαλείας, όπως τα Target Wake Time και WPA3 [45]. Το πρότυπο IEEE 802.11ax οριστικοποιήθηκε την 1η Σεπτεμβρίου 2020 και έλαβε την τελική έγκριση από το Συμβούλιο Προτύπων IEEE την 1η Φεβρουαρίου 2021 [48].

Κεφάλαιο 3ο: Τρόποι μετάδοσης WLAN

3.1 Τεχνικές μετάδοσης

Στα δίκτυα WLAN, τα δεδομένα μεταδίδονται μεταξύ συσκευών χρησιμοποιώντας διαφορετικές μεθόδους ασύρματης επικοινωνίας. Σε αυτές τις μεθόδους χρησιμοποιούνται διάφορες τεχνικές μετάδοσης οι οποίες καθορίζουν τον τρόπο αποστολής και λήψης των δεδομένων μέσω του μέσου που χρησιμοποιείται, δηλαδή των ραδιοκυμάτων. Αν και όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, το πρότυπο IEEE 802.11 ορίζει στο φυσικό του επίπεδο τεχνικές μετάδοσης μέσω ραδιοκυμάτων και μέσω υπερύθρων, η χρήση των τεχνικών μετάδοσης μέσω ραδιοσυχνοτήτων είναι η πλέον χρησιμοποιούμενη μέθοδος μετάδοσης, κυρίως λόγω της μικρότερης εμβέλειας επικοινωνίας που μπορεί να επιτευχθεί με τη χρήση υπερύθρων [49].

Παρόλα αυτά, η χρήση μετάδοσης μέσω ραδιοσυχνοτήτων θέτει μια σειρά από προκλήσεις, όπως είναι η ασφάλεια, της αξιοπιστία της ζεύξης μετάδοσης των δεδομένων και ο έλεγχος πρόσβασης στο μέσο [36]. Η ασφάλεια αποτελεί τη σημαντικότερη ανησυχία των μεταδόσεων μέσω ραδιοσυχνοτήτων, καθώς τα κανάλια ζεύξης επικοινωνίας μεταξύ του αποστολέα και του παραλήπτη των δεδομένων είναι εύκολο να αποτελέσουν αντικείμενο παραβίασης και υποκλοπών. Τα θέματα της ασφάλειας των δικτύων WLAN θα αναλυθούν λεπτομερώς στο επόμενο κεφάλαιο. Καθώς η μετάδοση μέσω ραδιοσυχνοτήτων είναι επιρρεπής σε παρεμβολές, αλλά παρουσιάζει και άλλα ζητήματα διάδοσης σήματος, η αξιοπιστία της ζεύξης μετάδοσης των δεδομένων αποτελεί τη δεύτερη σημαντική πρόκληση για τα δίκτυα WLAN. Τέλος, ο έλεγχος της πρόσβασης στο μέσο μετάδοσης δεδομένων από πολλούς ασύρματους πελάτες (συσκευές ή σταθμούς) αποτελεί επίσης μια σημαντική πρόκληση για ένα ασύρματο μέσο, καθώς, σε αντίθεση με ένα ενσύρματο δίκτυο, δεν είναι δυνατή η ταυτόχρονη μετάδοση και λήψη των δεδομένων.

Δύο βασικές περιπτώσεις που έχουν τη δυνατότητα να υποβαθμίζουν την απόδοση ενός δικτύου WLAN είναι τα ζητήματα του λεγόμενου κρυφού και εκτεθειμένου ασύρματου κόμβου, που παρουσιάστηκαν στο προηγούμενο κεφάλαιο. Εκτός από τα ζητήματα του κρυφού και του εκτεθειμένου κόμβου, η απόδοση της ασύρματης μετάδοσης μειώνεται επίσης από τις παρεμβολές συν-καναλιού (co-channel interference), καθώς η μπάντα των ραδιοσυχνοτήτων χαρακτηρίζεται από μεγάλο συνωστισμό. Πράγματι, η χρήση πολλών περιοχών συχνοτήτων, όπως οι μπάντες των 902MHz και των 2,4GHz, από διάφορων ειδών ασύρματων συσκευών για τη λειτουργία τους, δημιουργεί πολλά ζητήματα θορύβου και παρεμβολών, με αποτέλεσμα ο ρυθμός μεταφοράς των δεδομένων να μειώνεται [49].

Όλα αυτά τα ζητήματα της χρήση των ραδιοσυχνοτήτων ως μέσο μετάδοσης των δεδομένων στα δίκτυα WLAN, οδήγησαν στην ανεύρεση τεχνικών μετάδοσης, οι οποίες θα είναι σε θέση να τα ελαχιστοποιήσουν, αν όχι να τα εξαλείψουν [43]. Έτσι, αποσκοπώντας σε αυτή την τουλάχιστον ελαχιστοποίηση των ζητημάτων της χρήσης των ραδιοσυχνοτήτων, το βασικό πρότυπο IEEE 802.11 και οι τροποποιήσεις τους περιλαμβάνουν τέτοιες τεχνικές μετάδοσης στο φυσικό επίπεδο της αρχιτεκτονικής δομής τους. Όπως έχει ήδη αναφερθεί στο προηγούμενο κεφάλαιο, η πρώτη έκδοση του προτύπου IEEE 802.11 WLAN παρείχε ταχύτητες σύνδεσης 1 - 2Mbps με χρήση των τεχνικών μετάδοσης FHSS (Frequency Hopping Spread Spectrum) και DSSS (Direct Sequence Spread Spectrum), λειτουργώντας στην μπάντα των 2,4GHz και χρησιμοποιώντας κανάλια επικοινωνίας εύρους ζώνης 22MHz. Η τροποποίηση IEEE 802.11b παρείχε περίπου 11Mbps ρυθμό μετάδοσης δεδομένων, λειτουργώντας επίσης στην μπάντα των 2,4GHz, χρησιμοποιώντας κανάλια επικοινωνίας

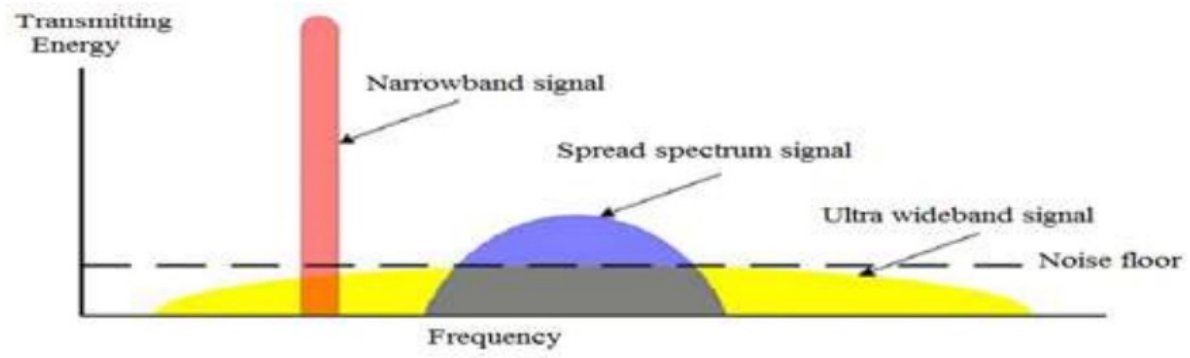
εύρους ζώνης 20MHz και συνδυάζοντας την τεχνική μετάδοσης DSSS με κωδικοποίηση CCK (Complementary Code Keying). Αντίθετα, το πρότυπο IEEE 802.11a ήταν το πρώτο που χρησιμοποίησε τη ζώνη ISM των 5GHz και την τεχνική μετάδοσης OFDM (Orthogonal Frequency Division Multiplexing), με 64 υποφέρουσες συχνότητες (με 312,5kHz μεταξύ τους απόσταση), ώστε να πετύχει μέγιστο ρυθμό μετάδοσης δεδομένων 54Mbps. Μεγαλύτερη περιοχή κάλυψης σε σύγκριση με τις προηγούμενες εκδόσεις, επιτεύχθηκαν στο πρότυπο IEEE 802.11g, το οποίο, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, μπορούσε να υποστηρίξει δύο διαφορετικές τεχνικές μετάδοσης με διαφορετικούς ρυθμούς μετάδοσης δεδομένων (την τεχνική OFDM με ρυθμό μετάδοσης δεδομένων της τάξης των 54Mbps και την τεχνική PBCC με ταχύτητες μεταφοράς δεδομένων 22 και 33Mbps). Η τροποποίηση IEEE 802.11n πέτυχε σημαντική βελτίωση στην ταχύτητα σύνδεσης, με την εισαγωγή των χαρακτηριστικών μετάδοσης MIMO στην τεχνική OFDM, κάτι που επέτρεψε την αύξηση του ρυθμού μετάδοσης δεδομένων και την επίτευξη ταχυτήτων έως και 600Mbps. Η τροποποίηση IEEE 802.11ac, λειτουργώντας στη μπάντα συχνοτήτων των 5GHz, επέκτεινε τις δυνατότητες της διεπαφής αέρα που υποστηρίζεται από το IEEE 802.11n, με μεγαλύτερο εύρος ζώνης καναλιού, πρόσθετες χωρικές ροές MIMO και πρόσθετες λειτουργίες, όπως η τεχνική MU-MIMO, έτσι ώστε να μπορεί να υποστηρίξει ταυτόχρονη μετάδοση πολλαπλών πλαισίων δεδομένων σε διαφορετικούς χρήστες. Τέλος, το βασικό χαρακτηριστικό στο οποίο βασίζεται το IEEE 802.11ax είναι η χρήση της τεχνικής μετάδοσης OFDMA, η οποία είναι ισοδύναμη με την εφαρμογή της κυψελοειδούς τεχνολογίας σε δίκτυα Wi-Fi, μια τεχνική που επιτρέπει την υψηλότερη φασματική απόδοση και επομένως τον τετραπλασιασμό της συνολικής απόδοσης του δικτύου [50].

Λαμβάνοντας υπόψη τα παραπάνω χαρακτηριστικά των τεχνολογιών IEEE 802.11, μπορεί να ειπωθεί ότι τα δίκτυα WLAN βασίζονται σε τέσσερις τεχνικές μετάδοσης (FHSS, DSSS, OFDM και MIMO), καθώς και σε κάποιες παραλλαγές τους. Οι πρώτες εκδόσεις του προτύπου χρησιμοποίησαν τις τεχνικές μετάδοσης FHSS και DSSS. Η λειτουργία αυτών των τεχνικών μετάδοσης βασίζεται στη φιλοσοφία της διασποράς φάσματος (Spread Spectrum – SS), σύμφωνα με την οποία η συχνότητα του εκπεμπόμενου σήματος τροποποιείται εσκεμμένα, ώστε ένα σήμα στενής ζώνης να εκπέμπεται σε μεγαλύτερο εύρος ζώνης. Λόγω όμως της αδυναμίας επίτευξης αρκετά μεγάλων ταχυτήτων μεταφοράς δεδομένων, το μεγαλύτερο μέρος των προτύπων της οικογένειας IEEE 802.11 βασίζεται στη χρήση της τεχνικής OFDM. Η OFDM, αν και στη βιβλιογραφία θεωρείται ως μία μορφή τεχνικής SS, ουσιαστικά είναι μια τεχνική διαμόρφωσης και πολυπλεξίας στην οποία τα ψηφιακά δεδομένα κωδικοποιούνται σε πολλαπλές φέρουσες συχνότητες. Τέλος, οι πιο πρόσφατες τροποποιήσεις του προτύπου IEEE 802.11 ξεκίνησαν να υποστηρίζουν και να εισάγουν την τεχνολογία MIMO, η οποία αποτελεί μια αποτελεσματική τεχνολογία μετάδοσης δεδομένων σε ασύρματες επικοινωνίες που χρησιμοποιεί έναν μεγάλο αριθμό κεραιών για εκπομπή και λήψη, με σκοπό το συνδυασμό πολλαπλών πηγών μετάδοσης για την επίτευξη υψηλότερου ρυθμού μετάδοσης δεδομένων και αύξηση της αποτελεσματικότητας του ασύρματου δικτύου [51]. Περισσότερες λεπτομέρειες θα δοθούν στις επόμενες ενότητες του κεφαλαίου.

3.2 Τεχνική μετάδοσης SS

Η διασπορά φάσματος αποτελεί μια τεχνική μετάδοσης δεδομένων μέσω ραδιοσυχνοτήτων, η οποία αρχικά είχε αναπτυχθεί για στρατιωτικές εφαρμογές στον Β' Παγκόσμιο Πόλεμο με σκοπό την προστασία των ασύρματων μεταδόσεων από υποκλοπές και παρεμβολές (με τη μορφή σήματος jamming). Η τεχνική μετάδοσης SS άρχισε να χρησιμοποιείται για εμπορικούς σκοπούς στις αρχές της δεκαετίας του 1980. Σε σύγκριση με τις πιο οικείες τεχνικές μετάδοσης διαμόρφωσης πλάτους AM (Amplitude Modulation) και συχνότητας FM (Frequency Modulation), η τεχνική SS παρουσιάζει το

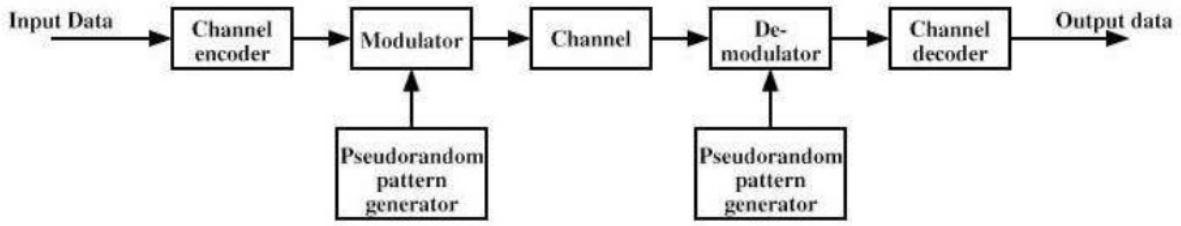
κύριο πλεονέκτημα της μείωσης ή ακόμα και της εξάλειψης των παρεμβολών που πηγάζουν από εκπομπές σημάτων στενής ζώνης στην ίδια περιοχή συχνοτήτων, βελτιώνοντας έτσι σημαντικά την αξιοπιστία της ζεύξης μετάδοσης των δεδομένων μέσω ραδιοσυχνοτήτων [36].



Εικόνα 3.1: Λειτουργία τεχνικής μετάδοσης SS [51]

Όπως υποδηλώνει και το όνομά της, η τεχνική μετάδοσης SS δίνει τη δυνατότητα εκπομπής ενός σήματος στενής ζώνης σε μια ευρεία περιοχή του φάσματος. Αυτό σημαίνει ότι ένα σήμα στενής ζώνης (narrowband), με την τεχνική μετάδοσης SS τροποποιείται κατάλληλα, ώστε να καταλαμβάνει μεγαλύτερο εύρος φάσματος (Εικ. 3.1). Τα σήματα στενής ζώνης μπλοκάρονται εύκολα από οποιοδήποτε άλλο σήμα της ίδιας ζώνης, αλλά μπορούν επίσης εύκολα να εντοπιστούν και να υποκλαπούν, καθώς η ζώνη συχνοτήτων που χρησιμοποιούν είναι σταθερή και στενή. Η βασική φιλοσοφία της τεχνικής SS είναι να χρησιμοποιείται μεγαλύτερο εύρος ζώνης από το αρχικό μήνυμα διατηρώντας την ίδια ισχύ. Ένα σήμα που προκύπτει μέσω της τεχνικής SS δεν παρουσιάζει κάποια ξεκάθαρη και διακριτή κορυφή στο φάσμα, γεγονός που το καθιστά πιο δύσκολο να ξεχωρίσει από το θόρυβο και επομένως πιο δύσκολο να μπλοκαριστεί ή να υποκλαπεί [51].

Στην τεχνική SS, η τροποποίηση του αρχικού σήματος πραγματοποιείται μέσω της χρήσης ενός συστήματος, όπως αυτό που φαίνεται στην εικόνα 3.2. Η δυαδική ακολουθία πληροφοριών (input data) εισάγεται στον κωδικοποιητή καναλιού (channel encoder) στην πλευρά του πομπού. Ο κωδικοποιητής καναλιού κωδικοποιεί αυτήν την ακολουθία εισόδου σύμφωνα με κάποια τεχνική κωδικοποίησης ελέγχου σφαλμάτων. Η κωδικοποιημένη ακολουθία οδηγείται στη συνέχεια στον διαμορφωτή (modulator), ο οποίος λαμβάνει και ως είσοδο μια ακολουθία ψευδοτυχαίων αριθμών, γνωστή και ως ακολουθία ή κώδικας διασποράς, που παράγεται από μια γεννήτρια ψευδοτυχαίου μοτίβου (pseudorandom pattern generator). Η παραγωγή της συγκεκριμένης ακολουθίας βασίζεται στη χρήση μιας αρχικής τιμής (γνωστής ως seed) με αποτέλεσμα, οι αριθμοί της σειράς να μην είναι ουσιαστικά τυχαίοι, από τη στιγμή που μια δεδομένη αρχική τιμή παράγει πάντα την ίδια σειρά αριθμών. Η έξοδος του διαμορφωτή αποτελεί το διαμορφωμένο σήμα SS, το οποίο παρουσιάζει σημαντική αύξηση εύρους ζώνης σε σύγκριση με την στενή ζώνη του αρχικού σήματος. Αυτό το σήμα στη συνέχεια μεταδίδεται μέσω κάποιου καναλιού (channel). Στον δέκτη, ο αποδιαμορφωτής (demodulator) λαμβάνει το σήμα SS, για την αποκωδικοποίηση του οποίου απαιτείται η ίδια ακολουθία ψευδοτυχαίων αριθμών που χρησιμοποιήθηκε στο άκρο εκπομπής. Ως εκ τούτου, οι γεννήτριες ψευδοτυχαίων μοτίβων στην πλευρά του πομπού και του δέκτη λειτουργούν σε συγχρονισμό μεταξύ τους. Μετά την αποδιαμόρφωση του σήματος SS, το προκύπτον σήμα οδηγείται στον αποκωδικοποιητή καναλιών (channel decoder) για την ανάκτηση της αρχικής δυαδικής ακολουθίας πληροφοριών (output data) [52].

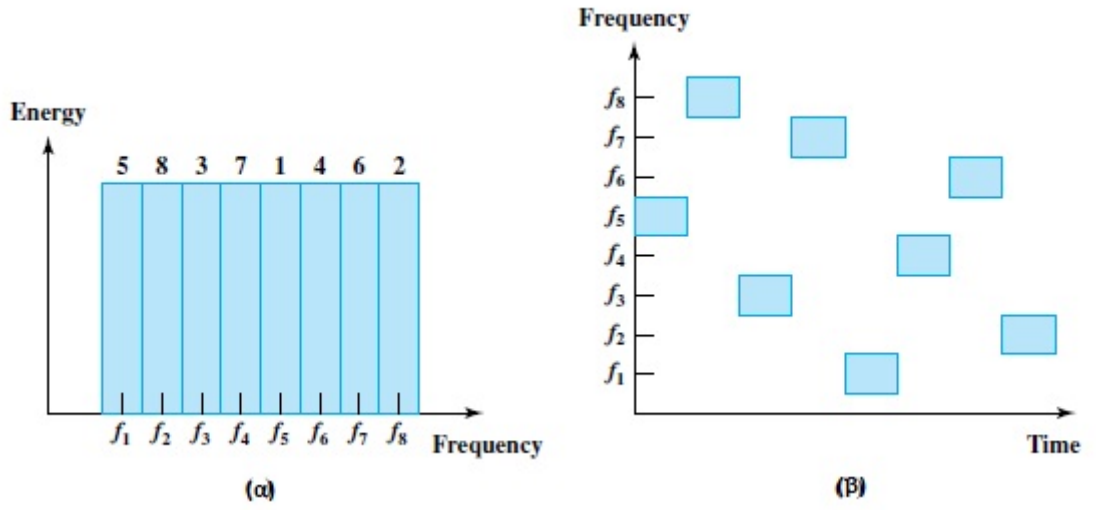


Εικόνα 3.2: Γενικό μοντέλο λειτουργίας τεχνικής μετάδοσης SS [52]

Η τεχνική SS παρουσιάζει πολλά πλεονεκτήματα με βασικότερα την αξιοπιστία της ζεύξης μετάδοσης των δεδομένων μέσω ραδιοσυχνοτήτων (καθώς όπως αναφέρθηκε παραπάνω μειώνει ή ακόμα και εξαλείφει τις παρεμβολές που πηγάζουν από εκπομπές σημάτων στενής ζώνης στην ίδια περιοχή συχνοτήτων), καθώς και την εξάλειψη του φαινομένου του cross-talk, την μείωση της επίδρασης του φαινομένου της εξασθένισης που μπορεί να παρατηρηθεί κατά τη μετάδοση σημάτων μέσω πολλαπλών διαδρομών (multipath fading) και την επίτευξη μεγαλύτερης απόδοσης ως προς την ακεραιότητα των δεδομένων που μεταδίδονται. Όλα αυτά τα πλεονεκτήματα την κατέστησαν ως μία από τις βασικότερες τεχνικές μετάδοσης στα πρώτα πρωτόκολλα της οικογένειας προτύπων IEEE 802.11, στα οποία χρησιμοποιήθηκαν δύο από τους έξι διαφορετικούς τύπους της. Πρόκειται για τις τεχνικές μετάδοσης FHSS και DSSS, οι οποίες διαφέρουν στον τρόπο με τον οποίο ο κώδικας διασποράς διαμορφώνει τα αρχικά δεδομένα, αλλά και στο σημείο που εισάγεται αυτός ο κώδικας στο σύστημα [51], [53]. Η χρήση του κώδικα διασποράς αποτελεί το βασικότερο χαρακτηριστικό της τεχνικής SS, αλλά και των διαφορετικών τύπων της, καθώς είναι ανεξάρτητη από τα δεδομένα που μεταδίδονται. Η τεχνική της διαμόρφωσης του μεταδιδόμενου σήματος μέσω του της χρήσης του κώδικα διασποράς έχει ως αποτέλεσμα το εύρος ζώνης του σήματος που τελικά μεταδίδεται να είναι τυπικά 20 έως αρκετές 100άδες φορές του αντίστοιχου εύρους ζώνης του αρχικού σήματος πληροφοριών, σε εμπορικές εφαρμογές, ή 1000 έως 1 εκατομμύριο φορές στα στρατιωτικά συστήματα [49].

3.3 Τεχνική μετάδοσης FHSS

Η μεταπήδηση συχνότητας (frequency hopping) αποτελεί έναν τύπο τεχνικής μετάδοσης SS που βασίζεται στην κατάτμηση της ζώνης συχνοτήτων, η οποία πρόκειται να χρησιμοποιηθεί για τη μετάδοση του αρχικού σήματος, σε ένα μεγάλο αριθμό μικρότερων υποζωνών (καναλιών) συχνότητας. Με τον τρόπο αυτό, στην τεχνική μετάδοσης FHSS, η μετάδοση του αρχικού σήματος πραγματοποιείται μέσω της εκπομπής σύντομων ριπών (bursts) του σήματος χρησιμοποιώντας διαφορετικό κανάλι κάθε φορά και μεταπηδώντας από κανάλι σε κανάλι με ψευδοτυχαίο τρόπο, σε σταθερά χρονικά διαστήματα, μετά την ολοκλήρωση της εκπομπής κάθε ριπής. Στην εικόνα 3.3(α) παρουσιάζεται ένα παράδειγμα του τρόπου με τον οποίο ένα εύρος ζώνης χωρίζεται σε 8 κανάλια στενού εύρους, καθένα από τα οποία έχει μία διαφορετική κεντρική συχνότητα (f1 έως f8). Για κάθε εκπομπή ριπής του αρχικού σήματος, το σύστημα χρησιμοποιεί διαφορετικό κανάλι, για συγκεκριμένη χρονική διάρκεια (γνωστή ως dwell time), πριν μεταπηδήσει σε άλλο (Εικ. 3.3(β)). Με αυτόν τον τρόπο, όλα τα κανάλια χρησιμοποιούνται περίπου για ίσο χρονικό διάστημα, αλλά κανένα δεν χρησιμοποιείται συνεχώς [27], [54].

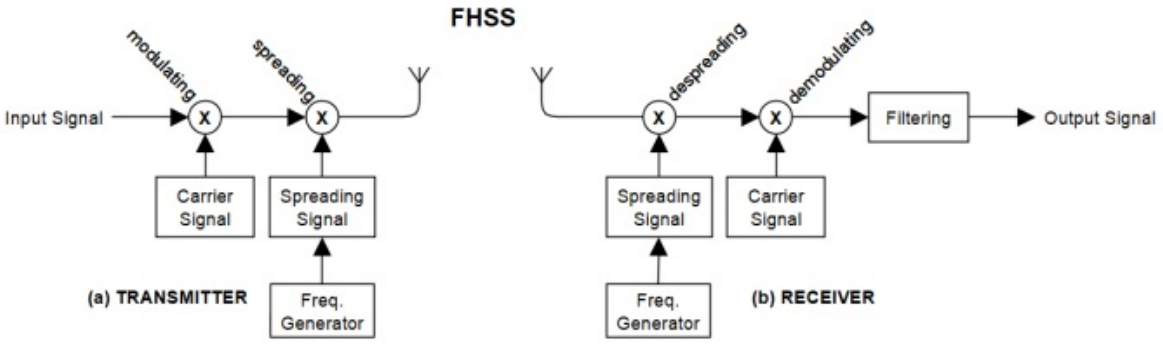


Εικόνα 3.3: Παράδειγμα λειτουργίας τεχνικής FHSS (α) κατάτμηση ζώνης συχνοτήτων σε κανάλια, (β) χρήση καναλιών [54]

Ο ρυθμός μεταπήδησης (hop rate) από κανάλι σε κανάλι μπορεί να κατηγοριοποιήσει τα συστήματα FHSS σε γρήγορης ή αργής μεταπήδησης. Εάν αυτός ο ρυθμός είναι μεγαλύτερος από τον χρόνο μετάδοσης ενός bit του σήματος, τότε το σύστημα χαρακτηρίζεται ως γρήγορης μεταπήδησης. Σε αυτήν την περίπτωση, κάθε μεταδιδόμενο bit του σήματος απαιτεί τη χρήση πολλών καναλιών. Αντίθετα, στα συστήματα αργής μεταπήδησης, ο ρυθμός μεταπήδησης είναι μικρότερος ή ίσος με τον χρόνο μετάδοσης ενός bit του σήματος, με αποτέλεσμα μέσω του ίδιου καναλιού να μπορούν να μεταδοθούν ένα ή περισσότερα bit δεδομένων, πριν από κάθε μεταπήδηση [55].

Η σειρά με την οποία πραγματοποιείται η μεταπήδηση της μετάδοσης από κανάλι σε κανάλι είναι γνωστή ως μοτίβο μεταπήδησης (hopping pattern). Όπως συμβαίνει και στην τεχνική SS, αυτή η ακολουθία δημιουργείται από μια ασφαλή γεννήτρια ψευδοτυχαίου κώδικα στην πλευρά του πομπού. Το συγκεκριμένο μοτίβο μεταπήδησης θα πρέπει επίσης να είναι γνωστό και από τον δέκτη για τον οποίο προορίζεται η εκπομπή του σήματος, έτσι ώστε να μπορεί εύκολα να το λάβει, χωρίς όμως άλλοι δέκτες, που δεν το γνωρίζουν, να είναι σε θέση να το ανιχνεύσουν. Με τον τρόπο αυτό, επιτυγχάνεται προστασία από ανεπιθύμητες περιπτώσεις υποκλοπής σήματος, ενώ παράλληλα το σκόπιμο μπλοκάρισμά του καθίσταται πιο δύσκολο. Για τους ίδιους λόγους, το μοτίβο αναπήδησης θα πρέπει να είναι μια τυχαία ακολουθία μεγάλης περιόδου [56].

Στην εικόνα 3.4 παρουσιάζεται το απλοποιημένο μπλοκ διάγραμμα ενός συστήματος FHSS [57]. Στον πομπό του συστήματος (Εικ. 3.4(α)), το ψηφιακό σήμα εισάγεται σε έναν διαμορφωτή (modulator), στον οποίο διαμορφώνεται (modulating) σε σήμα ενδιάμεσης συχνότητας (IF) με χρήση ενός φέροντος σήματος (carrier signal). Για τη διαμόρφωση αυτή θεωρητικά θα μπορούσε να χρησιμοποιηθεί οποιοδήποτε βασικό σχήμα διαμόρφωσης, όπως PSK (Phase Shift Keying), ASK (Amplitude Shift Keying), FSK (Frequency Shift Keying), κλπ., αλλά το πρότυπο IEEE 802.11 χρησιμοποιεί διαμόρφωση GFSK (Gaussian Frequency Shift Keying) [42]. Στη συνέχεια, το σήμα IF αναμειγνύεται (spreading) με την έξοδο μιας γεννήτριας συχνοτήτων (frequency generator) με σκοπό την παραγωγή του μεταδιδόμενου σήματος ραδιοσυχνότητας RF. Η έξοδος της γεννήτριας συχνοτήτων βασίζεται στο σήμα διασποράς (spreading signal) το οποίο δημιουργείται με τη ίδια λογική με αυτήν της τεχνικής SS (δημιουργίας του κώδικα διασποράς). Η μεταβολή του σήματος διασποράς, δημιουργεί αντίστοιχη μεταβολή της εξόδου της γεννήτριας συχνοτήτων, με αποτέλεσμα να επιτυγχάνεται η μεταπήδηση συχνότητας του μεταδιδόμενου σήματος RF [56].



Εικόνα 3.4: Απλοποιημένο μπλοκ διάγραμμα συστήματος FHSS (α) πομπού και (β) δέκτη [57]

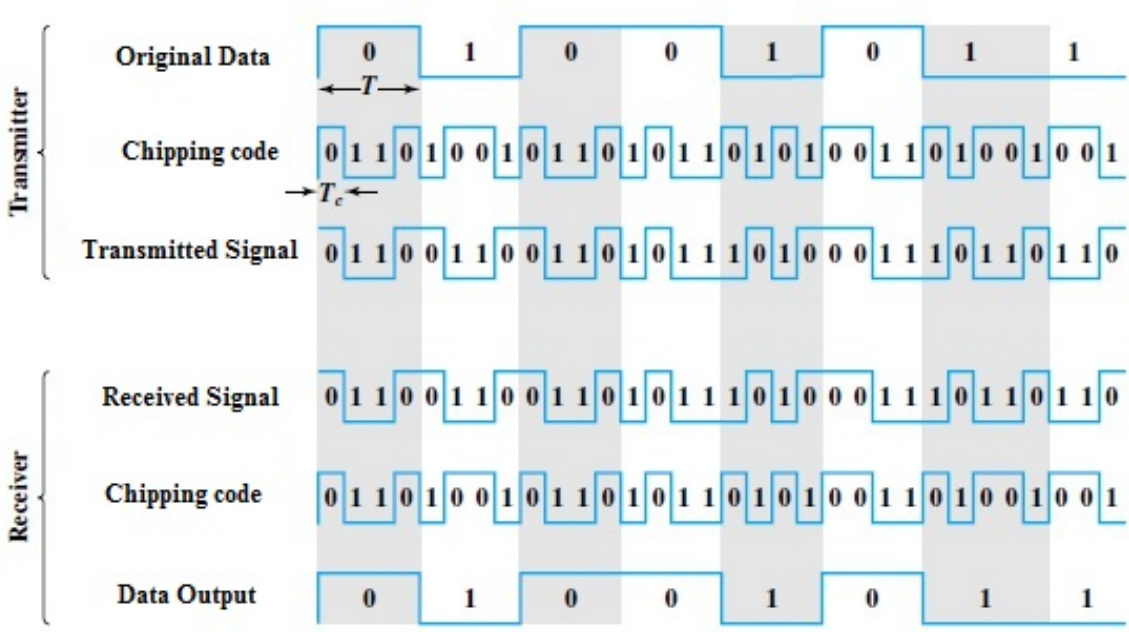
Στον δέκτη του συστήματος (Εικ. 3.4(β)), το λαμβανόμενο σήμα RF μετατρέπεται (dispreading) σε σήμα IF μέσω της χρήσης της εξόδου μιας γεννήτριας συχνοτήτων. Η διαδικασία αυτής της μετατροπής είναι αντίστοιχη με αυτήν της διαδικασίας spreading στην πλευρά του πομπού. Οι μονάδες που συμμετέχουν στις δύο διαδικασίες, στον πομπό και στο δέκτη, θα πρέπει να παρουσιάζουν χρονικό συγχρονισμό, έτσι ώστε η μεταπήδηση συχνότητας να συμβαίνει ταυτόχρονα με το λαμβανόμενο σήμα και επομένως να επιτυγχάνεται ορθή λήψη των μεταδιδόμενων δεδομένων. Σε αντίθετη περίπτωση, είναι πολύ πιθανό να παρουσιαστεί μερική λήψη του μεταδιδόμενου σήματος. Στη συνέχεια, το σήμα IF αποδιαμορφώνεται (demodulation) και φιλτράρεται (filtering) από ένα φίλτρο Gaussian εύρους ζώνης για την ανάκτηση αρχικών δεδομένων [56].

Στα δίκτυα WLAN 802.11, οι μεταδόσεις μέσω της τεχνικής FHSS πραγματοποιούνται σε κανάλια που χρησιμοποιούνται περιοδικά με ψευδοτυχαία σειρά, καλύπτοντας σχεδόν όλο το εύρος της ζώνης ISM 2,4GHz. Πιο συγκεκριμένα, με την τεχνική FHSS δημιουργούνται 79 διαφορετικά κανάλια στις συχνότητες από 2,402GHz έως 2,480GHz. Ο χρόνος παραμονής (dwell time) σε κάθε συχνότητα αποτελεί μια καθορισμένη παράμετρο για κάθε σύστημα και συνιστάται να είναι της τάξης των 20ms, μια τιμή που ισοδυναμεί με έναν ρυθμό μεταπήδησης 50 άλματα ανά δευτερόλεπτο. Ο συγχρονισμός μεταξύ των μονάδων που συμμετέχουν στις διαδικασίες spreading και dispreading, σε πομπό και δέκτη αντίστοιχα, επιτυγχάνεται στο IEEE 802.11 με την αποστολή των βασικών παραμέτρων (χρόνος παραμονής, αριθμός ακολουθίας συχνότητας και αριθμός χρησιμοποιούμενου καναλιού) στο πεδίο συνόλου παραμέτρων συχνότητας που αποτελεί μέρος της μετάδοσης beacon που αποστέλλεται περιοδικά στο κανάλι επικοινωνίας. Ένας ασύρματος σταθμός που επιθυμεί να ενταχθεί στο δίκτυο θα πρέπει να ακούσει αυτά τα beacon και να συγχρονίσει το μοτίβο μεταπήδησης, ως μέρος της διαδικασίας συσχέτισής του με το δίκτυο. Όπως αναφέρθηκε παραπάνω, η μετάδοση των δεδομένων στα δίκτυα IEEE 802.11 γίνεται με τη βοήθεια της διαμόρφωσης GFSK, με το εύρος του καναλιού να περιορίζεται στο 1MHz σε ένα επίπεδο της τάξης των 20dB κάτω από το μέγιστο πλάτος του φέροντος κύματος. Αυτό το εύρος ζώνης ισχύει για ταχύτητες δεδομένων 1Mbps και 2Mbps. Για ταχύτητα δεδομένων 1Mbps, η ονομαστική απόκλιση συχνότητας κάθε καναλιού είναι της τάξης των ±160kHz. Για να είναι εφικτή η υποστήριξη του ρυθμού μετάδοσης δεδομένων 2Mbps, το IEEE 802.11 είναι σε θέση να υποστηρίξει ένα συνδυασμό διαμόρφωσης GFSK με διαμόρφωση FSK τεσσάρων επιπέδων. Σε αυτήν την περίπτωση, τα bit δεδομένων ομαδοποιούνται σε σύμβολα των δύο bit, έτσι ώστε κάθε σύμβολο να μπορεί να καταλάβει ένα από τα τέσσερα επίπεδα. Οι ονομαστικές αποκλίσεις συχνότητας των τεσσάρων επιπέδων είναι της τάξης των ±72kHz και ±216kHz. Και στις δύο περιπτώσεις ρυθμών μετάδοσης, οι δέκτες IEEE 802.11 περιλαμβάνουν φίλτρο Gaussian εύρους ζώνης 500kHz, ενώ η ελάχιστη απαιτούμενη ευαισθησία τους είναι της τάξης των -75dBm [42].

Αν και η ανάπτυξη του Wi-Fi για σημαντικά αυξημένες ταχύτητες μετάδοσης δεδομένων έχει βασιστεί στη χρήση της τεχνικής DSSS, η FHSS παρουσιάζει ορισμένα πλεονεκτήματα που αφορούν τη μεγάλη ανθεκτικότητα σε ζητήματα όπως οι παρεμβολές, το εσκεμμένο μπλοκάρισμα της εκπομπής, η επιλεκτική εξασθένηση συχνότητας (frequency selective fading) και το πρόβλημα near-far effect. Επίσης, η ανάπτυξη πομπών και δεκτών σε ένα ασύρματο δίκτυο, που να την υποστηρίζουν, είναι οικονομικά φθηνή και ενεργειακά αποδοτική [58]. Το μεγάλο μειονέκτημα της τεχνικής FHSS είναι ότι δεν μπορεί να υποστηρίξει ρυθμούς μετάδοσης δεδομένων μεγαλύτερες των 2Mbps, ένα στοιχείο για το οποίο δεν χρησιμοποιήθηκε από τις τροποποιήσεις του βασικού προτύπου IEEE 802.11 [42].

3.4 Τεχνική μετάδοσης DSSS

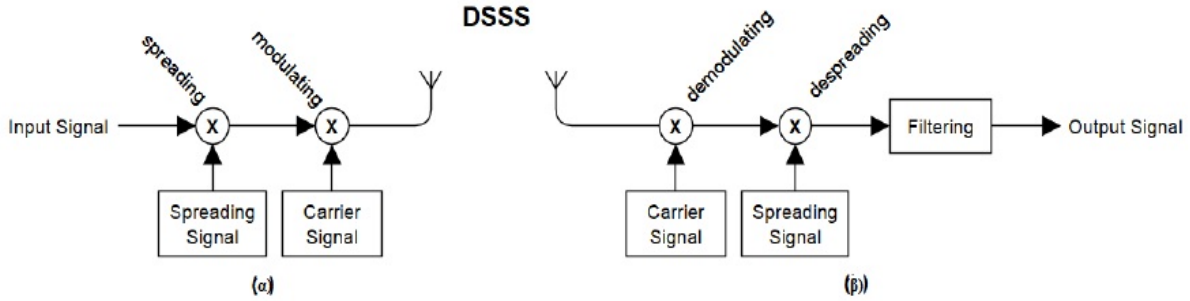
Η DSSS αποτελεί ένα τύπο τεχνικής μετάδοσης SS που διαφέρει στη φιλοσοφία διασποράς του φάσματος του αρχικού σήματος. Η βασική λογική της τεχνικής DSSS αφορά την προσθήκη επιπρόσθετων bit δεδομένων, γνωστών ως chip, στην ακολουθία δεδομένων του αρχικού σήματος. Με αυτήν την προσθήκη, κάθε bit του αρχικού σήματος αντιπροσωπεύεται από έναν μεγάλο αριθμό bit στο σήμα που τελικά εκπέμπεται, χρησιμοποιώντας μια ψευδοτυχαία ακολουθία bit υψηλότερου ρυθμού, γνωστή ως spreading code ή chipping code. Η χρήση της ψευδοτυχαίας ακολουθίας bit έχει ως σκοπό τη διασπορά του φάσματος του αρχικού σήματος, η οποία εξαρτάται από τον αριθμό των επιπρόσθετων bit που χρησιμοποιούνται. Συνήθως ο αριθμός των bit της ψευδοτυχαίας ακολουθίας είναι μεγαλύτερος του 10 και η διασπορά του φάσματος που επιτυγχάνεται με αυτόν τον τρόπο είναι τουλάχιστον 10πλάσια του εύρους ζώνης του αρχικού σήματος [27], [54].



Εικόνα 3.5: Γραφική αναπαράσταση λειτουργίας τεχνικής DSSS [54]

Ένας τρόπος συνδυασμού του αρχικού ψηφιακού σήματος με την ψευδοτυχαία ακολουθία bit, που ακολουθείται πιο συχνά στην τεχνική DSSS, είναι μέσω της πραγματοποίησης ενός δυαδικού πολλαπλασιασμού (XOR). Στην εικόνα 3.5 παρουσιάζεται η γραφική απεικόνιση της λειτουργίας αυτής της τεχνικής, σύμφωνα με την οποία το αρχικό ψηφιακό σήμα (original data) πολλαπλασιάζεται με την ψευδοτυχαία ακολουθία bit (chipping code) υψηλότερου ρυθμού, ώστε να επιτευχθεί διασπορά φάσματος του αρχικού σήματος. Σύμφωνα με την λογική του δυαδικού πολλαπλασιασμού (XOR),

κάθε bit “1” του αρχικού ψηφιακού σήματος αντιστρέφει τα bit της ακολουθίας διασποράς φάσματος κατά το συνδυασμό τους, ενώ τα bit “0” του αρχικού σήματος επιτρέπουν τη μετάδοση των bit της ακολουθίας χωρίς αντιστροφή [54].

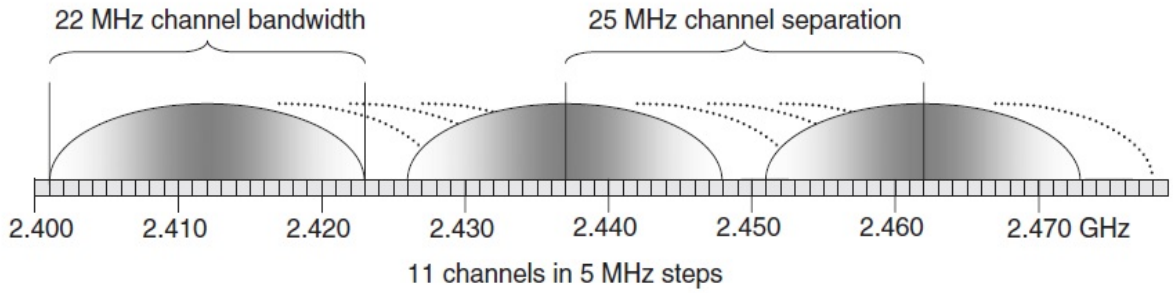


Εικόνα 3.6: Σύστημα DSSS (α) πομπός, (β) δέκτης [57]

Το ψηφιακό σήμα που προκύπτει από αυτόν τον δυαδικό πολλαπλασιασμό (XOR) διατηρεί το ρυθμό της ακολουθίας διασποράς φάσματος, επομένως καλύπτει μεγαλύτερο εύρος ζώνης από αυτό του αρχικού σήματος. Στην πλευρά του πομπού, το ψηφιακό σήμα, που προκύπτει από αυτόν τον πολλαπλασιασμό, οδηγείται σε έναν διαμορφωτή (συνήθως διαμόρφωσης BPSK), ο οποίος το μετατρέπει σε αναλογική μορφή για να μεταδοθεί (Εικ. 3.6(α)). Στον δέκτη ακολουθείται η ακριβώς αντίθετη διαδικασία, με την προϋπόθεση ότι η ψευδοτυχαία ακολουθία που χρησιμοποιείται στον πομπό για τη διασπορά του φάσματος του αρχικού σήματος, χρησιμοποιείται και εδώ με σκοπό την ανάκτηση του αρχικού σήματος που μεταδόθηκε, αφού πρώτα υποστεί διαδικασία φιλτραρίσματος (Εικ. 3.6(β)) [54], [57].

Όπως φαίνεται στην γραφική αναπαράσταση της λειτουργίας της τεχνικής DSSS της εικόνας 3.6, κάθε bit της ψευδοτυχαίας ακολουθίας διασποράς φάσματος έχει πολύ μικρότερη διάρκεια από τα bit του αρχικού ψηφιακού σήματος. Η διάρκεια αυτή των bit της ψευδοτυχαίας ακολουθίας διασποράς φάσματος παίζει μεγάλο ρόλο στο εύρος ζώνης του σήματος που προκύπτει μέσω της χρήσης του δυαδικού πολλαπλασιασμού (XOR). Όσο μικρότερη είναι αυτή η διάρκεια, τόσο μεγαλύτερο είναι το εύρος ζώνης του σήματος που πρόκειται να μεταδοθεί, κάτι που δίνει στην τεχνική DSSS το πλεονέκτημα να παρουσιάζει μεγαλύτερη ανθεκτικότητα στις παρεμβολές, από τη στιγμή που το αρχικό σήμα μεταδίδεται σε μεγαλύτερο εύρος ζώνης. Στην περίπτωση όμως που η διάρκεια κάθε bit της ψευδοτυχαίας ακολουθίας διασποράς φάσματος είναι μεγαλύτερη, τόσο μεγαλώνει η πιθανότητα ανάκτησης του αρχικού ψηφιακού σήματος στο δέκτη [59].

Στα δίκτυα WLAN 802.11, οι μεταδόσεις μέσω της τεχνικής DSSS πραγματοποιούνται σε κανάλια εύρους ζώνης 22MHz, καλύπτοντας σχεδόν όλο το εύρος της ζώνης ISM 2,4GHz (Εικ. 3.7). Η ψευδοτυχαία ακολουθία διασποράς που χρησιμοποιήθηκε ήταν ο κώδικας διασποράς Barker μήκους 11bit, ο οποίος σε συνδυασμό με τις τεχνικές διαμόρφωσης BPSK και QPSK έδινε τη δυνατότητα επίτευξης ρυθμού μετάδοσης δεδομένων 1 και 2Mbps αντίστοιχα. Γενικότερα, οι κώδικες Barker αποτελούν δυαδικές ακολουθίες μήκους από 2bit έως 13bit, που παρουσιάζουν χαμηλή αυτοσυσχέτιση, δηλαδή δεν συσχετίζονται με μια χρονικά μετατοπισμένη εκδοχή του εαυτού τους [49].



Εικόνα 3.7: Κανάλια DSSS των δικτύων WLAN 802.11 [49]

Στα δίκτυα WLAN 802.11b, αντί του κώδικα διασποράς Barker, επιλέχθηκε η χρήση της τεχνικής κωδικοποίησης CCK, μήκους 8bit, η οποία σε συνδυασμό με την τεχνική διαμόρφωσης DQPSK (Differential Quaternary Phase Shift Keying) έδινε τη δυνατότητα επίτευξης ταχύτητας μεταφοράς δεδομένων 5,5 και 11Mbps. Το κύριο πλεονέκτημα της τεχνικής κωδικοποίησης CCK είναι η φασματική απόδοση, αφού κάθε chip του κώδικα διασποράς αντιπροσωπεύει μέχρι 8bit δεδομένων εισόδου αντί για ένα που αντιπροσωπεύεται από τον κώδικα Barker. Η επίτευξη της μέγιστης ταχύτητας μεταφοράς δεδομένων των 11Mbps μέσω της χρήσης της κωδικοποίησης CCK πραγματοποιείται χρησιμοποιώντας το ίδιο εύρος ζώνης των 22MHz που χρησιμοποιείται για τη μετάδοση ρυθμού 1Mbps με τον κώδικα Barker. Ωστόσο, κάτι τέτοιο αυξάνει την πολυπλοκότητα των δεκτών. Στον πίνακα 3.1 παρουσιάζεται μια σύγκριση των μεθόδων κωδικοποίησης, διαμόρφωσης και ρυθμών μεταφοράς δεδομένων που επιτυγχάνονται με τη χρήση της τεχνικής μετάδοσης DSSS στα πρότυπα IEEE 802.11 και IEEE802.11b [49].

Πίνακας 3.1: Μέθοδοι διαμόρφωσης, κωδικοποίησης και ρυθμών μεταφοράς δεδομένων τεχνικής μετάδοσης DSSS στα πρότυπα IEEE 802.11 και IEEE802.11b [49]

Διαμόρφωση	**Μήκος κώδικα (chips)**	**Είδος κώδικα**	**Ρυθμός συμβόλου (Msps)**	**Αριθμός bit ανά σύμβολο**	**Ρυθμός μεταφοράς δεδομένων (Mbps)**
BPSK	11	Barker	1	1	1
QPSK	11	Barker	1	2	2
DQPSK	8	CCK	1,375	4	5,5
DQPSK	8	CCK	1,375	8	11

Σε σύγκριση με την τεχνική FHSS, η DSSS παρουσιάζει τα εξής πλεονεκτήματα [60]:

- δυνατότητα εξαγωγής των σημάτων μέσα από περιβάλλοντα παρεμβολών και θορύβου στενής ζώνης, κάτι που έχει ως αποτέλεσμα τη μείωση των μεταδόσεων και την αύξηση της συνολικής απόδοσης του συστήματος
- μεγαλύτερη ανθεκτικότητα στις παρεμβολές, αλλά και ασφάλεια στις υποκλοπές, λόγω του μηχανισμού διασποράς που χρησιμοποιεί
- σε περίπτωση αλλοίωσης κατά τη μετάδοση, λόγω θορύβου, ενός ή περισσοτέρων bit της ακολουθίας διασποράς φάσματος, ενσωματωμένες στατιστικές τεχνικές μπορούν να βοηθήσουν στην ανάκτηση του αρχικού σήματος, χωρίς να απαιτείται αναμετάδοσή του
- σε έναν ακούσιο δέκτη, το σήμα που εκπέμπεται μέσω της τεχνικής DSSS λαμβάνεται ως θόρυβος ευρείας ζώνης χαμηλής ισχύος και απορρίπτεται από τους περισσότερους δέκτες στενής ζώνης
- ο χρόνος μετάδοσης του σήματος είναι μικρότερος σε σύγκριση με τον αντίστοιχο χρόνο της τεχνικής FHSS, αφού δεν μεσολαβεί καθυστέρηση εναλλαγής της συχνότητας

- παρουσιάζει πολύ μεγαλύτερη προσαρμοστικότητα σε πολύ υψηλότερους ρυθμούς μετάδοσης δεδομένων

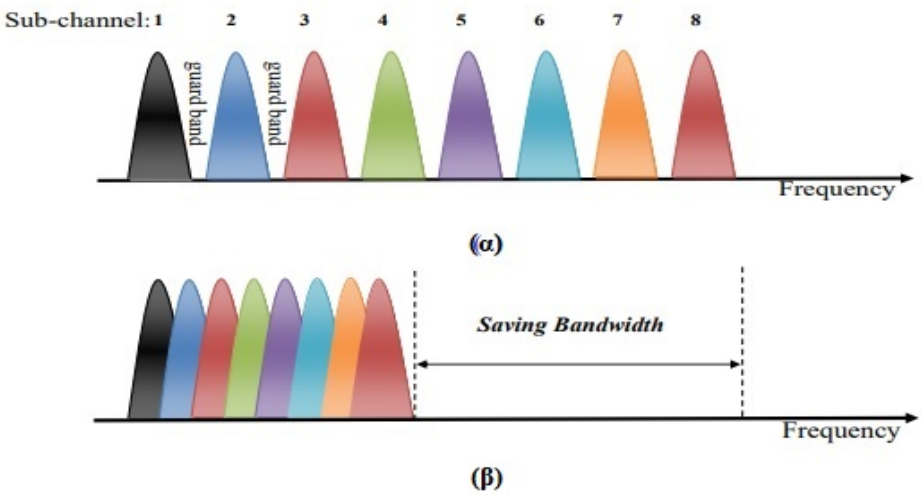
Παρόλα αυτά, υστερεί ως προς την τεχνική FHSS, στα εξής σημεία [60]:

- απαιτεί μεγαλύτερο εύρος ζώνης
- ο εξοπλισμός ενός συστήματος DSSS καταναλώνει περισσότερη ενέργεια για να πετύχει την ίδια ταχύτητα μετάδοσης ενός σήματος, λόγω της μεγαλύτερης πολυπλοκότητας που παρουσιάζει
- επιτρέπει την ταυτόχρονη λειτουργία περιορισμένου αριθμού διαφορετικών ασύρματων δικτύων στην ίδια γεωγραφική περιοχή, λόγω των περιορισμένων ελεύθερων διαθέσιμων καναλιών που μπορούν να μοιραστούν

3.5 Τεχνική μετάδοσης OFDM

Η τεχνική OFDM βασίζεται στη χρήση πολλαπλών φερουσών συχνοτήτων για τη μετάδοση των δεδομένων (multicarrier transmission), μια φιλοσοφία μετάδοσης η οποία είναι γνωστή και ως παράλληλη μετάδοση. Στα συστήματα OFDM, το εύρος ζώνης συχνοτήτων χωρίζεται σε κανάλια, καθένα από τα οποία περιέχει μια ροή δεδομένων χαμηλού ρυθμού, και μεταδίδει αυτά τα δεδομένα παράλληλα. Παρά το γεγονός, ότι τα κανάλια αυτά παρουσιάζουν επικάλυψη εύρους ζώνης, η μεταξύ τους απόσταση είναι τόσο ακριβής που παρουσιάζει μια ορθογωνικότητα. Με τον τρόπο αυτό, η τεχνική OFDM ελαχιστοποιεί τις παρεμβολές μεταξύ των καναλιών μετάδοσης και μειώνει την επίδραση της διάδοσης μέσω πολλαπλών διαδρομών [61].

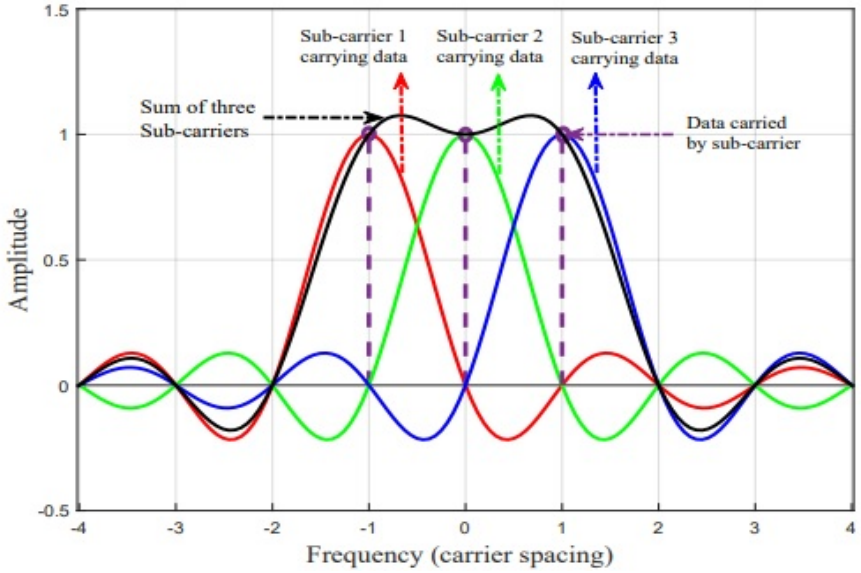
Η βασική ιδέα της τεχνικής μετάδοσης OFDM ακολουθεί αυτή της τεχνικής FDM (Frequency Division Multiplexing), ενσωματώνοντας κάποιες διαφορές. Στην τεχνική FDM, το εύρος ζώνης χωρίζεται σε μη επικαλυπτόμενα κανάλια, κάτι που ελαχιστοποιεί τις μεταξύ τους παρεμβολές ICI (Inter Carrier Interference), αλλά ταυτόχρονα συνεπάγεται και μια αναποτελεσματική χρήση του εύρους ζώνης. Στην τεχνική OFDM, παρά το γεγονός ότι τα κανάλια είναι επικαλυπτόμενα, η χρήση της ορθογωνικότητας αφαιρεί τις όποιες παρεμβολές μεταξύ των καναλιών. Στην εικόνα 3.8 παρουσιάζεται αυτή η διαφορά των τεχνικών FDM και OFDM. Με τη χρήση της τεχνικής OFDM αποσοβείται η κατασπατάληση σχεδόν του 50% του εύρους ζώνης που παρατηρείται με την τεχνική FDM [62].



Εικόνα 3.8: Σύγκριση τεχνικών FDM (α) και OFDM (β) [62]

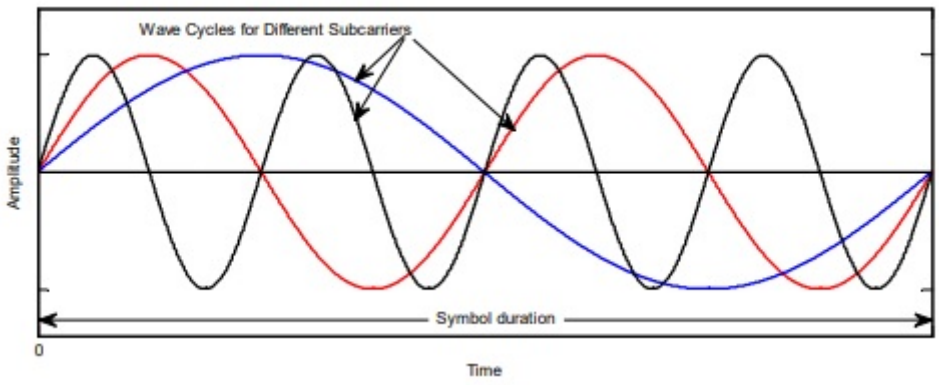
Από τα παραπάνω προκύπτει το συμπέρασμα ότι το βασικό χαρακτηριστικό της τεχνικής OFDM είναι η ορθογωνικότητα, η οποία επιτρέπει τη μετάδοση και την ανίχνευση πολλών σημάτων μέσω ενός

κοινού καναλιού, χωρίς καμία παρεμβολή [28]. Για την επίτευξη της ορθογωνικότητας μεταξύ των φερουσών συχνοτήτων σε ένα σύστημα OFDM θα πρέπει να πληρούνται δύο συνθήκες. Η πρώτη συνθήκη αφορά το πεδίο της συχνότητας, όπου για να επιτευχθεί η ορθογωνικότητα θα πρέπει η κορυφή του σήματος στην μια φέρουσα να συγχρονίζεται με το μηδέν του σήματος των παρακείμενων φερουσών, όπως φαίνεται στην εικόνα 3.9. Κάτι τέτοιο οδηγεί σε ένα πλήρως ευθυγραμμισμένο, και σε απόσταση με τα παρακείμενα, σήμα φέρουσας [63].



Εικόνα 3.9: Ορθογωνικότητα σημάτων φερουσών OFDM στο πεδίο της συχνότητας [63]

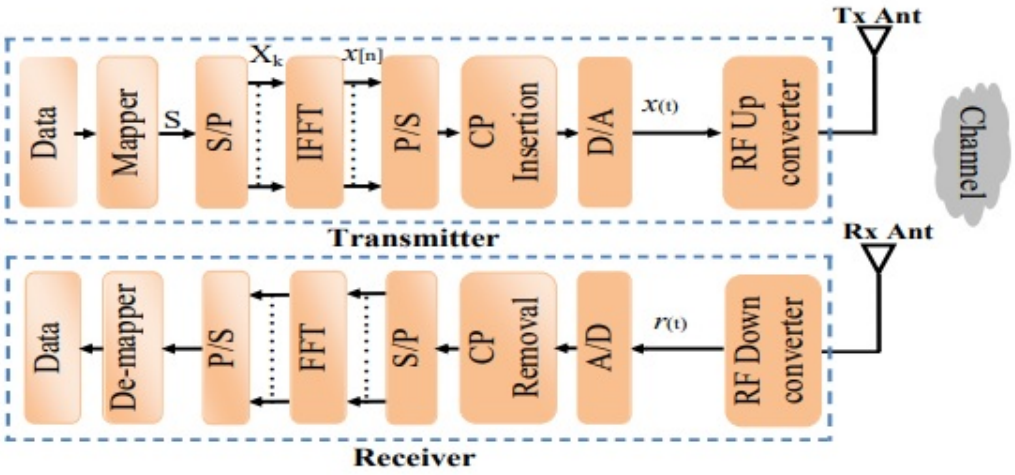
Η δεύτερη συνθήκη αφορά το πεδίο του χρόνου και τη διάρκεια του συμβόλου OFDM (T). Καθώς κάθε φέρουσα έχει έναν ακέραιο αριθμό κύκλων, μεταξύ δύο γειτονικών φερουσών η διαφορά μεταξύ του αριθμού κύκλων θα πρέπει να είναι ίση με έναν, όπως φαίνεται στην εικόνα 3.10 [63]. Με την προϋπόθεση ότι ισχύουν και οι δύο παραπάνω συνθήκες, δύο σήματα λέγονται ορθογώνια εάν είναι αμοιβαία ανεξάρτητα μεταξύ τους. Με άλλα λόγια, για να επιτευχθεί ορθογωνικότητα, το γινόμενο δύο σημάτων πρέπει να ισούται με μηδέν [61].



Εικόνα 3.10: Ορθογωνικότητα σημάτων φερουσών OFDM στο πεδίο του χρόνου [63]

Στην εικόνα 3.11 παρουσιάζεται το τυπικό μπλοκ διάγραμμα ενός συστήματος OFDM. Στον πομπό, τα δεδομένα εισόδου χαρτογραφούνται χρησιμοποιώντας διάφορα σχήματα χαρτογράφησης, όπως τις τεχνικές BPSK (Binary Phase Shift Keying) και QAM (Quadrature Amplitude Modulation). Τα διαμορφωμένα δεδομένα μετατρέπονται από σειριακές σε παράλληλες ροές (S/P) και στη συνέχεια

υποβάλλονται σε επεξεργασία από έναν αντίστροφο μετασχηματισμό Fourier (IFFT). Στα σύμβολα στον τομέα του χρόνου που προκύπτουν εφαρμόζεται μετατροπή παράλληλης σε σειριακή ροή (P/S). Μεταξύ των συμβόλων παρεμβάλλονται διαστήματα προστασίας, με σκοπό την ελαχιστοποίηση της διασυμβολικής παρεμβολής (Inter Symbol Interference - ISI) που προκαλείται από το φαινόμενο της εξασθένισης πολλαπλών διαδρομών και τέλος το σήμα μεταδίδεται, μετά μετασχηματισμό D/A και ενίσχυση στο επιθυμητό επίπεδο ισχύος. Στην πλευρά του δέκτη, τα βήματα επεξεργασίας που παρουσιάστηκαν για τον πομπό αντιστρέφονται με την αντίστοιχη σειρά, ώστε να προκύψει η μορφή της αρχικής δυαδικής ακολουθίας πληροφοριών [62].



Εικόνα 3.11: Μπλοκ διάγραμμα λειτουργίας συστήματος OFDM [62]

Τα πρότυπα IEEE 802.11a/g χρησιμοποιούν την τεχνική μετάδοσης OFDM στις μη αδειοδοτημένες μπάντες ISM των 5GHz και 2,4GHz αντίστοιχα για παροχή ρυθμών μετάδοσης δεδομένων έως 54Mbps. Στα αντίστοιχα δίκτυα WLAN, κάθε ένα από τα κανάλια εύρους 20MHz διαμοιράζεται σε 52 OFDM υποφέρουσες συχνότητες, με απόσταση 312,5kHz μεταξύ των κεντρικών συχνοτήτων. Από αυτές, οι 48 χρησιμοποιούνται για τη μεταφορά δεδομένων και διαμορφώνονται χρησιμοποιώντας τεχνικές BPSK, QPSK, 16-QAM ή 64-QAM. Οι υπόλοιπες τέσσερις υποφέρουσες χρησιμοποιούνται ως πιλοτικοί τόνοι, παρέχοντας ένα είδος αναφοράς για τις περιπτώσεις αντιστάθμισης των μετατοπίσεων φάσης και συχνότητας [49].

Στον πίνακα 3.2 παρουσιάζονται οι συνδυασμοί χρήσης διαφορετικών μεθόδων διαμόρφωσης και κωδικοποίησης, για την επίτευξη ρυθμών μεταφοράς δεδομένων από 6Mbps έως 54Mbps στα πρότυπα IEEE 802.11a/g [49].

Ο ρυθμός κωδικοποίησης υποδεικνύει την επιβάρυνση διόρθωσης σφάλματος που προστίθεται στη ροή δεδομένων εισόδου και ισούται με m / (m+n), όπου n είναι ο αριθμός των bit διόρθωσης σφαλμάτων που εφαρμόζονται σε ένα μπλοκ δεδομένων μήκους m bit. Για παράδειγμα, με ρυθμό κωδικοποίησης 3/4, σε κάθε 8 μεταδιδόμενα bit περιλαμβάνονται 6 bit δεδομένων χρήστη και 2 bit διόρθωσης σφαλμάτων [49].

Στο IEEE 802.11a, οι ρυθμοί μετάδοσης δεδομένων 6Mbps, 12Mbps και 24Mbps έχουν καθοριστεί ως υποχρεωτικοί και αντιστοιχούν σε συνδυασμό ρυθμού κωδικοποίησης 1/2 με τεχνικές διαμόρφωσης BPSK, QPSK και 16-QAM. Στο IEEE 802.11g, η χρήση της τεχνικής μετάδοσης OFDM προσθέτει ρυθμούς δεδομένων από 12Mbps έως 54Mbps, με τις τεχνικές διαμόρφωσης και κωδικοποίησης να είναι πανομοιότυπες με αυτές που εφαρμόζονται στο πρότυπο IEEE 802.11a [49].

Πίνακας 3.2: Μέθοδοι διαμόρφωσης, κωδικοποίησης και ρυθμών μεταφοράς δεδομένων τεχνικής μετάδοσης OFDM στα πρότυπα IEEE 802.11a/g [49]

Διαμόρφωση	**Αριθμός bit κώδικα ανά υποφέρουσα**	**Αριθμός bit κώδικα ανά σύμβολο OFDM**	**Ρυθμός κωδικοποίηση**	**Αριθμός bit δεδομένων ανά σύμβολο OFDM**	**Ρυθμός μεταφοράς δεδομένων (Mbps)**
BPSK	1	48	1/2	24	6
BPSK	1	48	3/4	36	9
QPSK	2	96	1/2	48	12
QPSK	2	96	3/4	72	18
16-QAM	4	192	1/2	96	24
16-QAM	4	192	3/4	144	36
64-QAM	6	288	2/3	192	48
64-QAM	6	288	3/4	216	54

Η χρήση της τεχνικής μεταφοράς OFDM έναντι των τεχνικών FHSS και DSSS επιλέχθηκε για αυτές τις τροποποιήσεις του προτύπου IEEE 802.11, λόγω των πολλών πλεονεκτημάτων που παρουσιάζει, μερικά από τα οποία είναι τα εξής [64]:

- ***Ανοσία στην επιλεκτική εξασθένιση***: Ένα από τα κύρια πλεονεκτήματα της τεχνικής OFDM είναι η ικανότητά της να αντιστέκεται στην επιλεκτική εξασθένιση συχνότητας περισσότερο από άλλες τεχνικές που χρησιμοποιούν μια φέρουσα για μετάδοση, επειδή διαμοιράζει το εύρος ζώνης σε πολλά κανάλια στενής ζώνης. Καθώς, κάθε κανάλι στενής ζώνης παρουσιάζει μεμονωμένο ζήτημα εξασθένισης, αυτός ο διαμοιρασμός του φάσματος σε επιμέρους κανάλια μετάδοσης, οδηγεί στη δημιουργία ενός συστήματος πιο ανθεκτικό στη συνολική εξασθένιση
- ***Ευελιξία στις παρεμβολές***: Σε ένα σύστημα μεμονωμένου φορέα, η εμφάνιση κάποιας παρεμβολής θα δημιουργήσει ζήτημα στο σύνολο των δεδομένων. Αντίθετα με την τεχνική OFDM, κάτι τέτοιο δεν συμβαίνει, αφού η εμφάνιση κάποιας παρεμβολής θα επηρεάσει μόνο τις υποφέρουσες στις οποίες εμφανίστηκε
- ***Αποδοτικότητα φάσματος***: Η τεχνική OFDM είναι πιο αποδοτική σε εύρος ζώνης σε σύγκριση με την FDM, καθώς οι υποφέρουσες συχνότητες που χρησιμοποιούνται για τη μετάδοση μπορούν να επικαλύπτονται λόγω του χαρακτηριστικού της ορθογωνικότητας. Με τον τρόπο αυτό, η χρήση του εύρους ζώνης μειώνεται δραστικά και κατά συνέπεια η αξιοποίηση του διαθέσιμου φάσματος γίνεται πιο αποτελεσματικά
- ***Προστασία από παρεμβολές μεταξύ συμβόλων (ISI)***: Λόγω της επέκτασης του του χρόνου του συμβόλου, η τεχνική OFDM προστατεύεται περισσότερο από παρεμβολές ISI σε σύγκριση με τις τεχνικές μεμονωμένου φορέα. Με την τεχνική OFDM, το εύρος ζώνης χωρίζεται σε πολλά επιμέρους εύρη ζώνης και ως εκ τούτου δημιουργεί έναν μεγάλο χρόνο συμβόλων, με αποτέλεσμα το σήμα να καθίσταται λιγότερο ευαίσθητο στην επίδραση της μετάδοσης πολλαπλών διαδρομών που εισάγει μια παρεμβολή ISI
- ***Εύκολη εφαρμογή διαμόρφωσης και αποδιαμόρφωσης***: Τα συστήματα διαμόρφωσης πολλαπλών φορέων είναι συνήθως πολύπλοκα, λόγω του μεγάλου αριθμού διαμορφωτών και αποδιαμορφωτών που απαιτούνται. Αυτή η πολυπλοκότητα στα συστήματα OFDM δεν υφίσταται, καθώς η χρήση μονάδων IFFT στον πομπό και FFT στον δέκτη απλουστεύει τη χρησιμοποιούμενη κυκλωματική διάταξη του συστήματος

Παρά τα πολλά της πλεονεκτήματα, η τεχνική μετάδοσης OFDM παρουσιάζει επίσης και δύο σημαντικά προβλήματα [62]:

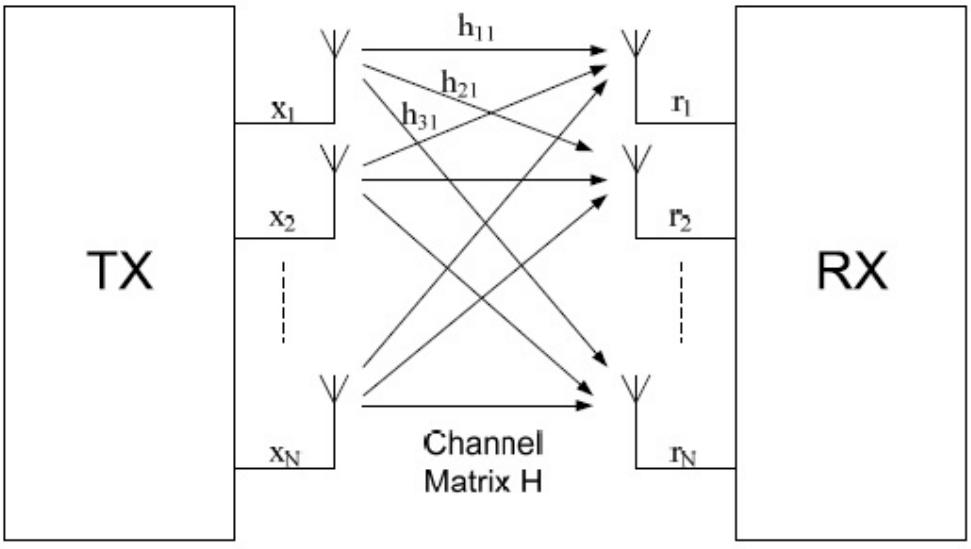
- ***Υψηλή ευαισθησία σε μετατοπίσεις συχνότητας φορέα και θόρυβο φάσης***: Μετατόπιση συχνότητας φορέα συμβαίνει όταν ο τοπικός ταλαντωτής στον δέκτη δεν είναι συγχρονισμένος με το σήμα του φορέα που περιέχεται στο λαμβανόμενο σήμα. Σε αυτήν την

περίπτωση, το λαμβανόμενο σήμα δεν θα δειγματοληφθεί στην κορυφή και στην ορθογωνικότητα μεταξύ των υποφερουσών, κάτι που προκαλεί παρεμβολή ICI

- ***Υψηλός λόγος PAPR (Peak to Average Power Ratio)***: Ο υψηλός λόγος PAPR των σημάτων μετάδοσης είναι ένα από πιο βασικά ζητήματα των συστημάτων OFDM. Για ένα σήμα OFDM, που αποτελείται από N μεμονωμένα και ανεξάρτητα σύμβολα δεδομένων, όταν τα σήματα N αθροίζονται στην ίδια φάση, παρατηρείται σημαντική αύξηση στο λόγο PAPR. Η παρατηρούμενη στιγμιαία τιμής του λόγου PAPR μπορεί να φτάσει τόσο υψηλές τιμές όσο N φορές το μέσο πλάτος των συμβόλων OFDM

3.6 Τεχνολογία MIMO

Στα συμβατικά ασύρματα συστήματα, η χρήση μίας μόνο κεραίας στον πομπό και στον δέκτη συνήθως οδηγεί στο πρόβλημα της υποβάθμισης της ισχύος του μεταδιδόμενου σήματος λόγω του φαινομένου της εξασθένισης πολλαπλών διαδρομών. Το συγκεκριμένο ζήτημα πηγάζει από τη λήψη του μεταδιδόμενου σήματος σε διάφορες χρονικές στιγμές, λόγω της ανάκλασης που προκαλείται από διάφορα εμπόδια, όπως λόφους, κτίρια, δέντρα, κλπ., και επηρεάζει την ποιότητα και την αξιοπιστία της λήψης [65]. Στην προσπάθειά της να ελαχιστοποιήσει το συγκεκριμένο ζήτημα, η ερευνητική και ακαδημαϊκή κοινότητα μπήκε στη διαδικασία ερευνών χρήσης πολλαπλών κεραιών, τόσο στην πλευρά του πομπού όσο και στην πλευρά του δέκτη. Αποτέλεσμα αυτών των ερευνών ήταν η ανάπτυξη της τεχνολογίας MIMO, η οποία εκμεταλλεύεται το χαρακτηριστικό της διάδοσης των ραδιοκυμάτων, μέσω της ταυτόχρονης αποστολής πολλαπλών ροών δεδομένων από πολλές κεραίες στον πομπό και τη λήψη των πολλαπλών διαδρομών μετάδοσης από πολλές κεραίες στο δέκτη (Εικ. 3.12) [49]. Με τον τρόπο αυτό, επιτυγχάνει τη βελτίωση της χωρητικότητας μιας ραδιοζεύξης. Με τον όρο χωρητικότητα (capacity) εννοείται ο μέγιστος δυνατός όγκος πληροφοριών που μπορεί να μεταδοθεί με το διαθέσιμο εύρος ζώνης και την εκπεμπόμενη ισχύ [65].



Εικόνα 3.12: Μοντέλο συστήματος MIMO [65]

Αυτά τα σχήματα θεωρείται ότι βελτιώνουν το εύρος και την απόδοση ενός συνολικού συστήματος. Το MIMO επιτρέπει υψηλότερη απόδοση, κέρδος ποικιλομορφίας (diversity) και μείωση παρεμβολών. Εκπληρώνει επίσης την απαίτηση υψηλού ρυθμού μετάδοσης δεδομένων μέσω απολαβής χωρικής πολυπλεξίας και βελτιωμένης αξιοπιστίας ζεύξης λόγω του κέρδους ποικιλομορφίας των χρησιμοποιούμενων κεραιών μετάδοσης και λήψης [65]. Η μαθηματική μοντελοποίηση των διαδρομών διάδοσης, με χρήση της περιόδου βαθμονόμησης του καναλιού κατά

τη διάρκεια κάθε μεταδιδόμενου πακέτου δεδομένων, επιτρέπει την αναγνώριση και την ορθή ανασύσταση στον δέκτη των διαφορετικών διαδρομών σήματος και των ροών δεδομένων που μεταδίδονται [49].

Στα συστήματα MIMO ευρέως διαδεδομένη είναι η χρήση της τεχνικής πολυπλεξίας SDM (Space Division Multiplexing), η οποία είναι ανάλογη της τεχνικής FDM ως προς το πεδίο της συχνότητας, αλλά αντί για διαφορετικές συχνότητες που μεταφέρουν δεδομένα παράλληλα, η παράλληλη μεταφορά δεδομένων πραγματοποιείται μέσω διαφορετικών χωρικών διαδρομών. Με τον τρόπο αυτό χρησιμοποιείται ουσιαστικά ταυτόχρονα το ίδιο εύρος ζώνης για τη δημιουργία πολλαπλών διαδρομών επικοινωνίας μεταξύ του πομπού και του δέκτη. Σε ένα σύστημα με M πομπούς και N δέκτες, ο αριθμός των ανεξάρτητων διαδρομών που μπορούν να δημιουργηθούν είναι ο μικρότερος από τις τιμές των M και N. Εάν αυτές οι διαδρομές είναι εξίσου ανθεκτικές σε παρεμβολές ή σε εξασθενίσεις και μπορούν να διαχωριστούν τέλεια, η συνολική χωρητικότητα του καναλιού επικοινωνίας αυξάνεται γραμμικά με τον αριθμό των ανεξάρτητων διαδρομών που χρησιμοποιούνται. Στην πράξη, όμως, όλες οι διαδρομές δεν παρουσιάζουν την ίδια ανθεκτικότητα στις παρεμβολές ή τις εξασθενίσεις, αλλά ούτε και μπορούν να διαχωριστούν τέλεια, με αποτέλεσμα, η απόδοση του συστήματος να μπορεί να καθοριστεί από συντελεστές, γνωστούς ως μοναδικές τιμές, που χαρακτηρίζουν κάθε διαδρομή μεταξύ των κεραιών εκπομπής και λήψης. Αυτές οι μοναδικές τιμές καθορίζονται μέσω μιας σύντομης "περιόδου εκπαίδευσης", που συμπεριλαμβάνεται στην αρχή κάθε μεταδιδόμενου πακέτου δεδομένων, κατά τη διάρκεια της οποίας, γνωστά και διαφορετικά σήματα μεταδίδονται από κάθε κεραία. Αυτά τα σήματα παρέχουν πληροφορίες CSI (Channel State Information) για το κανάλι μετάδοσης, μέσω των οποίων ο δέκτης μπορεί να υπολογίσει τις μοναδικές τιμές που χρησιμοποιούνται για την αποκωδικοποίηση του υπόλοιπο του πακέτου δεδομένων [49].

Μια άλλη τεχνική που χρησιμοποιείται στα συστήματα MIMO είναι η τεχνική κωδικοποίησης STBC (Space Time Block Coding), η οποία συνδυάζει χωρική και χρονική ποικιλομορφία με σκοπό την αύξηση της ανθεκτικότητας σε παρεμβολές και της εμβέλειας μιας σύνδεσης ραδιοσυχνοτήτων. Η τεχνική STBC τμηματοποιεί τα μεταδιδόμενα δεδομένα σε μπλοκ και μεταδίδει πολλαπλές χρονικές μετατοπίσεις του αντίγραφου κάθε μπλοκ δεδομένων από κάθε κεραία εκπομπής σε κάθε κεραία λήψης. Παρά το γεγονός, ότι η τεχνική κωδικοποίησης STBC χρησιμοποιήθηκε για πρώτη φορά σε συστήματα MISO (Multi Input Single Output), η χρήση της στα συστήματα MIMO μπορεί να βελτιώσει ακόμη περαιτέρω την απόδοσής τους [49].

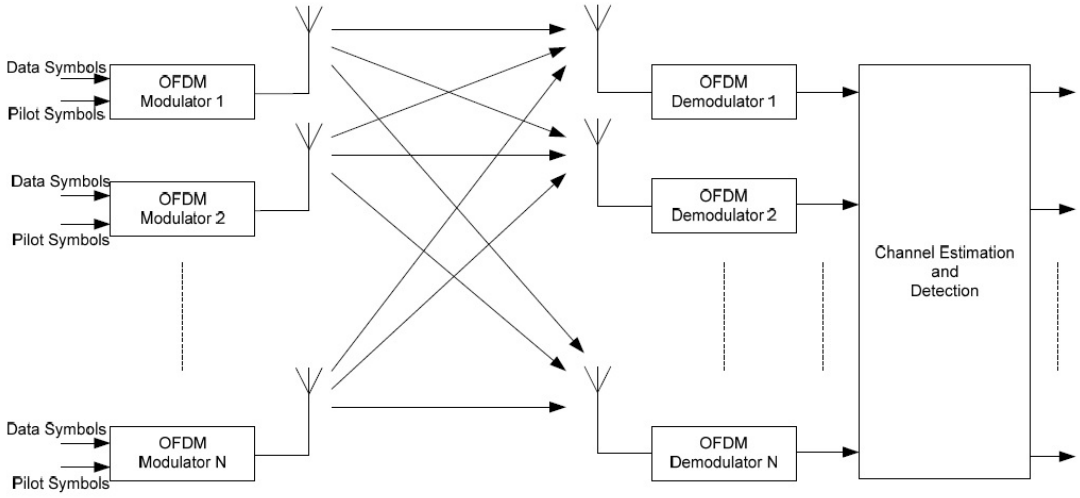
Τα πλεονεκτήματα της τεχνολογίας MIMO είναι πολλά και μπορούν να επιτευχθούν χωρίς να απαιτείται καμία επέκταση στο χρησιμοποιούμενο εύρος ζώνης ή αύξηση της ισχύος μετάδοσης [66]:

- ***Μεγάλη απολαβή συστοιχίας κεραιών***: Η αύξηση της απολαβής της συστοιχίας κεραιών οδηγεί σε αύξηση του μέσου όρου του λόγου SNR (Signal to Noise Ratio) και ως εκ τούτου βελτιώνει την περιοχή κάλυψης και την εμβέλεια του δικτύου
- ***Κέρδος ποικιλομορφίας***: Η τεχνολογία MIMO αυξάνει το κέρδος ποικιλομορφίας, καθώς με τη μετάδοση μεγάλου αριθμού ανεξάρτητων αντιγράφων των μπλοκ δεδομένων οι πιθανότητες απώλειας πληροφοριών κατά τη μετάδοση ελαχιστοποιούνται
- ***Απολαβή πολυπλεξίας***: Το σύστημα MIMO αυξάνει σημαντικά τη χωρητικότητα του καναλιού που μεταφράζεται αμέσως σε υψηλότερο ρυθμό μεταφοράς δεδομένων μέσω της χωρικής πολυπλεξίας
- ***Μείωση παρεμβολών***: Οι παρεμβολές ελαχιστοποιούνται στο σύστημα MIMO λόγω της εκμετάλλευσης της χωρικής πολυπλεξίας, η οποία αυξάνει την απόσταση μεταξύ των χρηστών

Όλα αυτά τα πλεονεκτήματα της τεχνολογίας MIMO, αλλά ιδιαίτερα η αυξημένη χωρητικότητα μιας ραδιοζεύξης, μπορούν να χρησιμοποιηθούν στα δίκτυα WLAN για την επίτευξη υψηλότερων ρυθμών

μετάδοσης δεδομένων ή για να αυξηθεί η ανθεκτικότητα στις παρεμβολές ή η εμβέλεια για έναν δεδομένο ρυθμό μετάδοσης δεδομένων. Κάτι τέτοιο πραγματοποιήθηκε στην προδιαγραφή IEEE 802.11n, στην οποία η τεχνολογία MIMO σε συνδυασμό με την τεχνική μετάδοσης OFDM οδήγησε στην αύξηση του ρυθμού μεταφοράς δεδομένων των τροπολογιών IEEE 802.11a/g, από τα 54Mbps στα 540Mbps [49].

Η ποιότητα της ασύρματης σύνδεσης εξαρτάται βασικά από τρεις παράγοντες [67]: (α) τον ρυθμό μετάδοσης δεδομένων, (β) την εμβέλεια μετάδοσης και (γ) την αξιοπιστία μετάδοσης. Με το συνδυασμό της τεχνικής μετάδοσης OFDM και της τεχνολογίας MIMO, για τη δημιουργία των λεγόμενων συστημάτων OFDM MIMO, οι παραπάνω παράγοντες μπορούν να βελτιωθούν ταυτόχρονα. Σε ένα τέτοιο σύστημα, οι μεμονωμένες λειτουργίες της τεχνικής OFDM μπορούν να εφαρμοστούν σε κάθε κεραία εκπομπής και λήψης, ενώ ταυτόχρονα σε ολόκληρο το σύστημα μπορεί να εφαρμοστεί η χωροχρονική τεχνική επεξεργασίας του σήματος που μεταδίδεται και υποστηρίζεται από την τεχνολογία MIMO. Η κωδικοποίηση μπορεί να πραγματοποιηθεί συλλογικά στις πολλαπλές κεραίες ή σε κάθε μεμονωμένη κεραία ξεχωριστά του πομπού. Η κωδικοποίηση που γίνεται σε κάθε μεμονωμένη κεραία του πομπού ονομάζεται κωδικοποίηση ανά κεραία PAC (Per Antenna Coding) (Εικ. 3.13) [68]. Οι διαδικασίες εκπομπής και λήψης των δυαδικών δεδομένων είναι οι ίδιες με αυτές που περιγράφηκαν στην προηγούμενη ενότητα για την τεχνική μετάδοσης OFDM με μόνη διαφορά ότι στο σύστημα OFDM MIMO πραγματοποιούνται σε κάθε μεμονωμένη κεραία του πομπού και του δέκτη αντίστοιχα.



Εικόνα 3.13: Σύστημα OFDM MIMO [68]

Εκτός από τη χρήση των συστημάτων OFDM MIMO, στο πρότυπο IEEE 802.11n διπλασιάστηκε το εύρος ζώνης του κάθε καναλιού (δηλαδή από 20MHz που χρησιμοποιήθηκαν στις προηγούμενες γενιές των προτύπων Wi-Fi τα κανάλια του IEEE 802.11n λειτουργούν με εύρος ζώνης 40MHz), με αποτέλεσμα να αυξάνεται ακόμα περισσότερο η χωρητικότητα των αντίστοιχων δικτύων WLAN, από τη στιγμή που διπλασιάστηκε ο αριθμός των διαθέσιμων πιλοτικών τόνων OFDM. Η μεγιστοποίηση της απόδοσης των δικτύων WLAN 802.11n εξαρτάται επίσης και από τη χρήση έξυπνων μηχανισμών για τη συνεχή προσαρμογή παραμέτρων, όπως το εύρος ζώνης και η επιλογή καναλιού, η διαμόρφωση κεραίας, το σχήμα διαμόρφωσης και ο ρυθμός κωδικοποίησης, σε διαφορετικές συνθήκες ασύρματου καναλιού. Στον πίνακα 3.3 παρουσιάζονται οι συνδυασμοί χρήσης διαφορετικών μεθόδων διαμόρφωσης και κωδικοποίησης, για την επίτευξη ρυθμών μεταφοράς δεδομένων από 54Mbps έως 540Mbps στο πρότυπο IEEE 802.11n [49].

Πίνακας 3.3: Μέθοδοι διαμόρφωσης, κωδικοποίησης και ρυθμών μεταφοράς δεδομένων τεχνικής μετάδοσης OFDM στο πρότυπο IEEE 802.11n [49]

Διαμόρφωση	**Αριθμός bit κώδικα ανά υποφέρουσα (ανά ροή δεδομένων)**	**Αριθμός bit κώδικα ανά σύμβολο OFDM (σε όλες τις ροές δεδομένων)**	**Ρυθμός κωδικοποίηση**	**Αριθμός bit δεδομένων ανά σύμβολο OFDM (σε όλες τις ροές δεδομένων)**	**Ρυθμός μεταφοράς δεδομένων (Mbps)**
BPSK	1	432	1/2	216	54
QPSK	2	864	1/2	432	108
QPSK	2	864	3/4	648	162
16-QAM	4	1728	1/2	864	216
16-QAM	4	1728	3/4	1296	324
64-QAM	4	2592	2/3	1728	432
64-QAM	6	2592	3/4	1944	486
64-QAM	6	2592	5/6	2160	540

Κεφάλαιο 4ο: Ασφάλεια ασύρματων τοπικών δικτύων

4.1 Απειλές και τρωτά σημεία στα WLAN

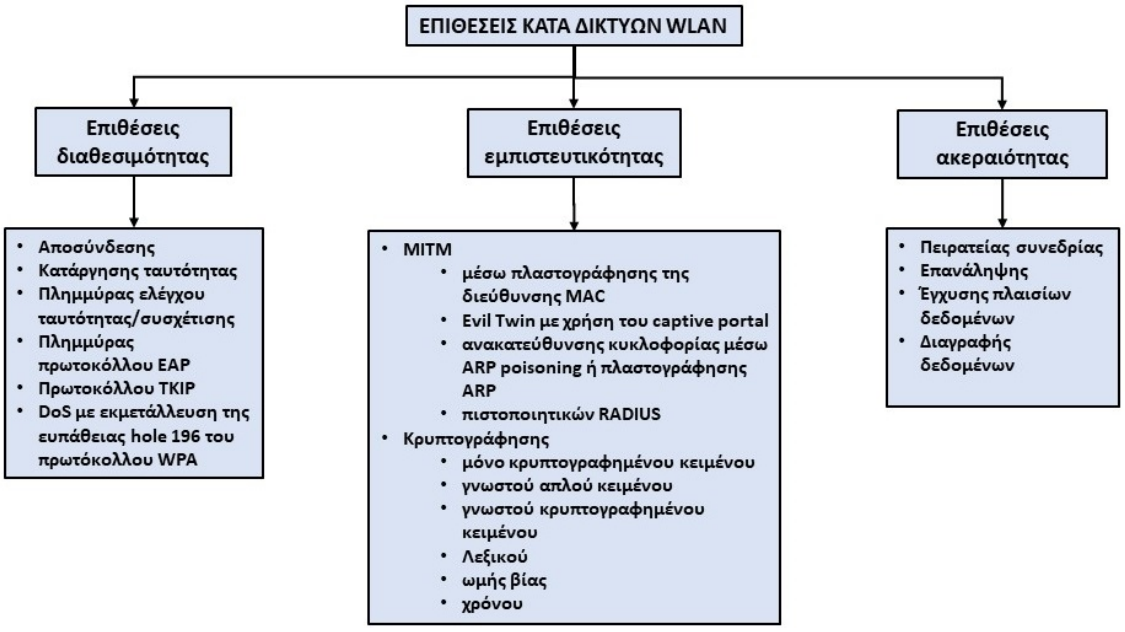
Σε προηγούμενο κεφάλαιο αναφέρθηκε ότι λόγω της φύσης της μετάδοσης των ραδιοκυμάτων, η ασύρματη διεπαφή αέρα των δικτύων WLAN είναι προσβάσιμη στον καθένα. Το συγκεκριμένο ζήτημα καθιστά τις ασύρματες μεταδόσεις πιο ευάλωτες από τις ενσύρματες επικοινωνίες σε κακόβουλες επιθέσεις, όπως η υποκλοπή δεδομένων ή η σκόπιμη παρεμβολή για τη διακοπή των μεταδόσεων. Με την σταθερά αυξανόμενη χρήση των δικτύων WLAN, η ασφάλεια των ασύρματων υποδομών τους καθίσταται ένα σοβαρό και κρίσιμο ζήτημα, η παραβίαση της οποίας μπορεί να επηρεάσει άμεσα ή έμμεσα τους χρήστες τους [27].

Η έννοια της ασφάλειας των δικτύων WLAN δεν περιορίζεται στην προστασία της ασύρματης υποδομής τους από μη εξουσιοδοτημένη πρόσβαση, αλλά περιλαμβάνει και τα ασύρματα κανάλια επικοινωνίας, μέσω των οποίων μεταφέρονται δεδομένα μεταξύ των διάφορων κόμβων των δικτύων. Το σύνολο ενός δικτύου WLAN μπορεί να παρουσιάζει αρκετά ευάλωτα σημεία που μπορούν να δεχτούν κάποιου είδους επίθεση για κακόβουλους σκοπούς. Ένας κλασικός ορισμός της ασφάλειας, που προκύπτει από την ανάδειξη των βασικών χαρακτηριστικών της, αφορά το ακρωνύμιο CIA (Confidentiality, Integrity, Availability). Ο συγκεκριμένος τρόπος ερμηνείας της ασφάλειας αναδεικνύει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα, ως τις τρεις βασικές απαιτήσεις που θα πρέπει να πληροί ένα οποιοδήποτε σύστημα για να θεωρηθεί ασφαλές. Παρόλα αυτά, τα ζητήματα ασφάλειας και προστασίας των δεδομένων που μεταφέρονται εντός των δικτύων WLAN δεν μπορούν να περιορίζονται μόνο στην τήρηση του μοντέλου ασφάλειας CIA. Ο έλεγχος πρόσβασης και ο έλεγχος ταυτότητας αποτελούν επίσης σημαντικούς παράγοντες επίτευξης ασφάλειας σε ένα δίκτυο WLAN [6], [27], [69].

Η εμπιστευτικότητα διασφαλίζει ότι όλα τα πλαίσια δεδομένων πριν και μετά τον έλεγχο ταυτότητας δεν διαβάζονται από μη εξουσιοδοτημένες οντότητες, ενώ η ακεραιότητα διασφαλίζει ότι δεν γίνονται τροποποιήσεις στα πλαίσια δεδομένων από μη εξουσιοδοτημένες οντότητες. Η διαθεσιμότητα διασφαλίζει ότι κάθε φορά που οι νόμιμες ασύρματες συσκευές ή μεμονωμένοι χρήστες χρειάζονται πρόσβαση σε έναν πόρο WLAN, μπορούν να το κάνουν χωρίς διακοπή [6], [27]. Στη βιβλιογραφία, σε πάρα πολλές μελέτες έχει προσδιοριστεί ότι η διακοπή (interruption), η υποκλοπή (interception), η τροποποίηση (modification) και η πλαστογραφία (fabrication) αποτελούν τις βασικές απειλές του μοντέλου ασφάλειας CIA ενός ασύρματου δικτύου [70].

Ο έλεγχος πρόσβασης περιορίζει τα δικαιώματα των ασύρματων συσκευών ή των μεμονωμένων χρηστών να έχουν πρόσβαση σε έναν πόρο WLAN έως ότου επαληθευτούν δεόντως. Τέλος, ο έλεγχος ταυτότητας είναι η διαδικασία απόδειξης ότι μια συσκευή ή ένα άτομο είναι αυτό που ισχυρίζεται ότι είναι [6], [27]. Σε αντίθεση με ένα ενσύρματο τοπικό δίκτυο όπου ένας εισβολέας πρέπει είτε να αποκτήσει φυσική πρόσβαση στο LAN είτε να υπονομεύσει τους κεντρικούς υπολογιστές του δικτύου από απόσταση, στην περίπτωση των WLAN οι επίδοξοι επιτιθέμενοι χρειάζεται μόνο να βρίσκονται εντός της εμβέλειας της κάλυψης του σημείου AP. Για το λόγο αυτό και για την προστασία του ασύρματου δικτύου, η σύνδεση μιας συσκευής ή ενός χρήστη σε ένα WLAN θα πρέπει να πραγματοποιείται μετά τον έλεγχο των δικαιωμάτων πρόσβασης και την πραγματοποίηση ενός ορθού και ασφαλούς ελέγχου ταυτότητας [71]. Η έννοια του ασφαλούς ελέγχου ταυτότητας προϋποθέτει την εκ των προτέρων διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων που μεταφέρονται στο ασύρματο δίκτυο [72].

Οι απειλές και τα τρωτά σημεία των δικτύων WLAN έχουν αποτελέσει θέμα μεγάλου όγκου ερευνών και μελετών της βιβλιογραφίας. Στις μελέτες αυτές έχουν παρουσιαστεί τα είδη των επιθέσεων κατά των δικτύων WLAN λαμβάνοντας υπόψη την εκμετάλλευση των αδυναμιών που παρουσιάζουν οι χρησιμοποιούμενοι μηχανισμοί ελέγχου ταυτότητας, οι μηχανισμοί εμπιστευτικότητας και ακεραιότητας που χρησιμοποιούνται για την προστασία των πληροφοριών ελέγχου ταυτότητας, αλλά και οι εσφαλμένες διαμορφώσεις των ασύρματων δικτύων. Οι επιθέσεις αυτές, που θα παρουσιαστούν στη συνέχεια, θέτουν γενικότερα σε κίνδυνο τη διαθεσιμότητα ενός δικτύου WLAN, την εμπιστευτικότητα ή/και την ακεραιότητα των δεδομένων που μεταδίδονται μέσω αυτού, καθώς και την ορθή και ασφαλή λειτουργία των διαδικασιών ελέγχου ταυτότητας και ελέγχου πρόσβασης. Στο πλαίσιο της παρούσας εργασίας, οι επιθέσεις αυτές ταξινομούνται με βάση το ποιο από τα χαρακτηριστικά του μοντέλου ασφάλειας CIA στοχεύουν σε μεγαλύτερο βαθμό. Έτσι, θα παρουσιαστούν τύποι επιθέσεων κατά της διαθεσιμότητας ενός δικτύου WLAN, καθώς και της εμπιστευτικότητας και της ακεραιότητας των δεδομένων που μεταδίδονται μέσω αυτού (Εικ. 4.1).



Εικόνα 4.1: Κατηγοριοποίηση επιθέσεων κατά δικτύων WLAN[75]

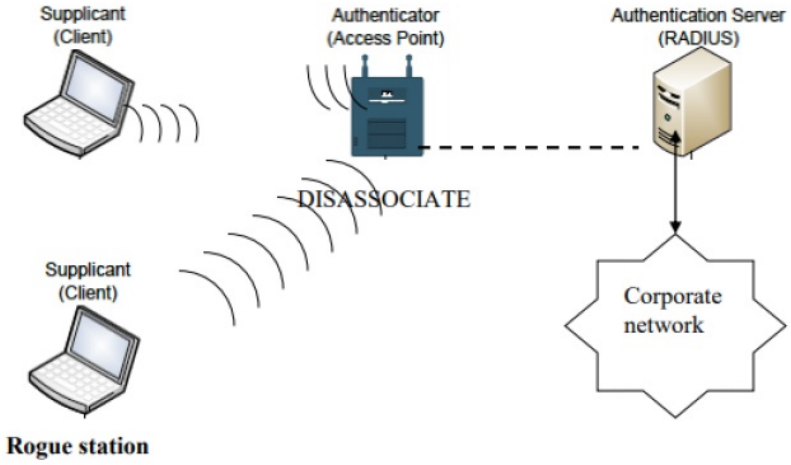
4.1.1 Επιθέσεις κατά της διαθεσιμότητας δικτύου WLAN

Οι επιθέσεις κατά της διαθεσιμότητας ενός δικτύου WLAN αφορούν εκείνο το είδος των επιθέσεων που αποσκοπούν στην αδυναμία εξυπηρέτησης των νόμιμων χρηστών από τις υπηρεσίες που μπορεί αυτό να παρέχει. Για το λόγο αυτό είναι γνωστές και ως επιθέσεις άρνησης υπηρεσίας DoS (Denial of Service) [73]. Όπως φαίνεται στην εικόνα 4.1, σημαντικότερες από τις επιθέσεις αυτές αποτελούν οι [6], [74], [75]: (α) επιθέσεις αποσύνδεσης, (β) επιθέσεις κατάργησης ταυτότητας, (γ) επιθέσεις πλημμύρας ελέγχου ταυτότητας/συσχέτισης, (δ) επιθέσεις πλημμύρας πρωτοκόλλου EAP, (ε) επιθέσεις κατά του πρωτοκόλλου TKIP και (στ) επιθέσεις DoS με εκμετάλλευση της ευπάθειας hole 196 του πρωτόκολλου WPA.

1) Επιθέσεις αποσύνδεσης

Μια επίθεση αποσύνδεσης (disassociation attack) έχει ως στόχο την δημιουργία περίπτωσης άρνησης υπηρεσίας σε μια νόμιμη συσκευή ενός δικτύου WLAN, αναγκάζοντάς την να αποσυνδεθεί από ένα

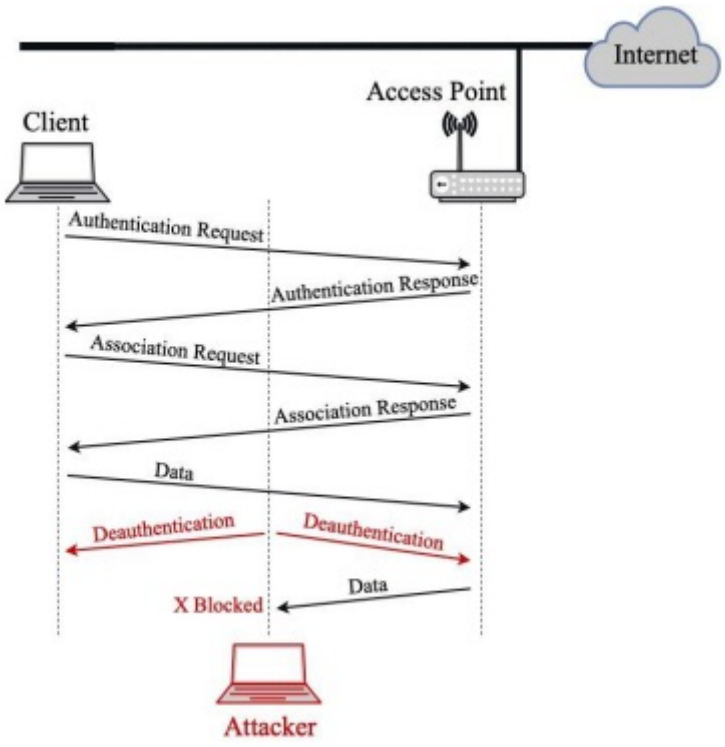
σημείο AP, κάτι που περατώνει τη μεταξύ τους μετάδοση ροών πλαισίων δεδομένων. Για την πραγματοποίηση μιας τέτοιας επίθεσης DoS απαιτείται η αναπαραγωγή ενός μηνύματος DISASSOCIATE, που κανονικά αποστέλλεται από το σημείο AP προς την νόμιμη συσκευή, από έναν κακόβουλο σταθμό. Μια τέτοια αναπαραγωγή είναι δυνατή από τη στιγμή που ο κακόβουλος σταθμός έχει υποκλέψει προηγουμένως παρόμοια μηνύματα DISASSOCIATE. Στην εικόνα 4.2 παρουσιάζεται η γραφική αναπαράσταση μιας επίθεσης αποσύνδεσης. Η επιτυχία της επίθεσης βασίζεται στην ανυπαρξία κάποιου μηχανισμού προστασίας της ακεραιότητας και απόδειξης της αυθεντικότητας των μηνυμάτων που αποστέλλονται μεταξύ των σημείων AP και των νόμιμων συσκευών ενός δικτύου WLAN [6], [75].



Εικόνα 4.2: Παράδειγμα επίθεσης αποσύνδεσης [75]

2) Επιθέσεις κατάργησης ταυτότητας

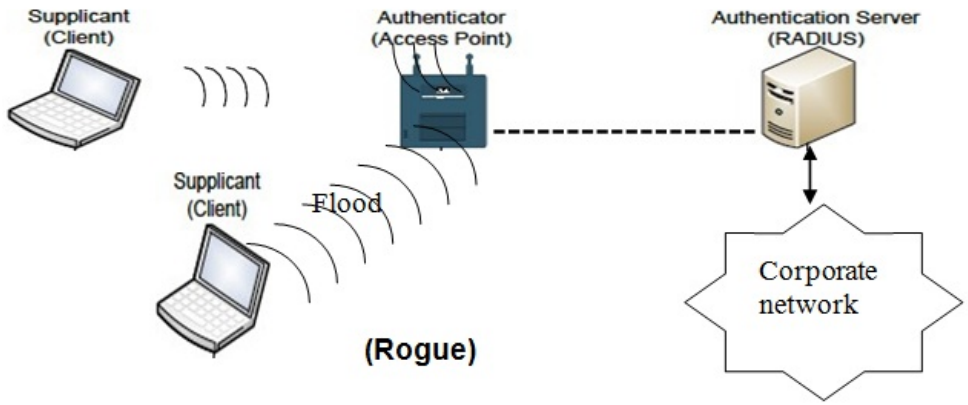
Μια επίθεση κατάργησης ταυτότητας (de-authentication attack) έχει ως στόχο την επικοινωνία μεταξύ μιας νόμιμης συσκευής και του σημείου AP με το οποίο είναι συνδεδεμένη. Πριν ξεκινήσει η επικοινωνία μεταξύ μιας νόμιμης ασύρματης συσκευής και ενός σημείο AP του δικτύου WLAN, το πρότυπο IEEE 802.11 απαιτεί την πραγματοποίηση δύο υποχρεωτικών διαδικασιών: του ελέγχου ταυτότητας και της συσχέτισης (σύνδεσης). Για την πραγματοποίηση αυτών των διαδικασιών, μεταξύ της συσκευής και του σημείου AP ανταλλάσσονται τα μηνύματα που φαίνονται στην εικόνα 4.3. Μετά το πέρας της ανταλλαγής των πλαισίων δεδομένων, οποιαδήποτε συσκευή μπορεί να στείλει ένα πλαίσιο DE-ATHENTICATION στο σημείο AP, ενημερώνοντάς το για την αφαίρεσή του από τον πίνακα συσκευών που εξυπηρετεί. Καθώς το συγκεκριμένο πλαίσιο κατάργησης ταυτότητας αποτελεί ειδοποίηση και όχι αίτημα, το σημείο AP δεν μπορεί να αρνηθεί να το εκτελέσει. Όλα αυτά τα μηνύματα που ανταλλάσσονται μεταξύ ενός σημείου AP και των συσκευών που εξυπηρετεί δεν είναι προστατευμένα, κάτι που μπορεί να εκμεταλλευτεί ένας επίδοξος επιτιθέμενος και να τα πλαστογραφήσει ώστε να διακόψει την επικοινωνία οποιασδήποτε ασύρματης συσκευής και του σημείου AP της. Αυτή η έλλειψη αμοιβαίας επαλήθευσης ταυτότητας μεταξύ της συσκευής και του σημείου AP δημιουργεί ένα κενό ασφάλειας, δίνοντας τη δυνατότητα για δημιουργία κακόβουλων σημείων AP, τα οποία μπορούν να τερματίσουν την επικοινωνία σε οποιαδήποτε νόμιμη ασύρματης συσκευής [74], [76].



Εικόνα 4.3: Σενάριο επίθεσης κατάργησης ταυτότητας [76]

3) Επιθέσεις πλημμύρας ελέγχου ταυτότητας/συσχέτισης

Οι επιθέσεις πλημμύρας ελέγχου ταυτότητας/συσχέτισης (authentication/association flood attacks) έχουν ως στόχο τη μείωση της δυνατότητας των νόμιμων χρηστών να συνδεθούν με ένα σημείο AP του δικτύου WLAN. Όπως φαίνεται στην εικόνα 4.4, σε μια τέτοιου είδους επίθεση DoS, ο επιτιθέμενος χρησιμοποιεί πλαστές διευθύνσεις MAC συσκευών, με σκοπό τη δημιουργία περίπτωσης κατά την οποία μεγάλος αριθμός συσκευών προσπαθεί ταυτόχρονα να πραγματοποιήσει διαδικασίες σύνδεσης με το σημείο AP. Σε μια τέτοια περίπτωση, μηνύματα ελέγχου ταυτότητας ή συσχέτισης αποστέλλονται επαναλαμβανόμενα, χρησιμοποιώντας διαφορετική διεύθυνση MAC κάθε φορά, με αποτέλεσμα η μνήμη και η ικανότητα επεξεργασίας του σημείου AP να εξαντλούνται στη προσπάθεια εξυπηρέτησης όλων αυτών των αιτημάτων. Αυτό που επιτυγχάνει τελικά ο επιτιθέμενος είναι να μην μπορούν οι νόμιμοι πελάτες να έχουν πρόσβαση στο σημείο AP του δικτύου [6], [74], [75].



Εικόνα 4.4: Παράδειγμα επίθεσης πλημμύρας ελέγχου ταυτότητας/συσχέτισης [75]

4) Επιθέσεις πλημμύρας πρωτοκόλλου EAP

Οι επιθέσεις πλημμύρας πρωτοκόλλου EAP (Extensible Authentication Protocol) στοχεύουν και πάλι στη δημιουργία συνθηκών δυσλειτουργίας ενός σημείου AP του δικτύου WLAN, όπως ακριβώς και οι επιθέσεις πλημμύρας ελέγχου ταυτότητας/συσχέτισης. Η μόνη διαφορά εδώ είναι ότι η κακόβουλη συσκευή πλημμυρίζει το δίκτυο με αιτήματα ελέγχου ταυτότητας EAP. Όπως θα αναλυθεί σε επόμενη ενότητα, το EAP αποτελεί ένα εκτεταμένο πρωτόκολλο ελέγχου ταυτότητας, το οποίο παρέχει διαφορετικές μεθόδους για την πραγματοποίησή της. Στόχος επομένως αυτών των επιθέσεων DoS είναι να κατακλυστεί αποτελεσματικά ο διακομιστής RADIUS, που χρησιμοποιείται από το πρωτόκολλο EAP, με μεγάλο αριθμό αιτημάτων ελέγχου ταυτότητας, προκαλώντας άρνηση υπηρεσίας στις νόμιμες συσκευές που θέλουν να συνδεθούν με κάποιο σημείο AP. Ένας από τους βασικότερους τρόπους πραγματοποίησης μιας επίθεσης πλημμύρας πρωτοκόλλου EAP είναι μέσω της χρήσης ενός εργαλείου επίθεσης για την αποστολή αιτημάτων ελέγχου ταυτότητας EAP, έτσι ώστε να γεμίσει όλος ο αναγνωριστικός χώρος του EAP (EAP Identifier space), κάτι που προκαλεί την "κατάρρευση" του σημείου AP, από τη στιγμή που δεν μπορεί να εξυπηρετήσει περισσότερες συνδέσεις. Ένας δεύτερος πολύ διαδεδομένος τρόπος κατάρρευσης του σημείου AP είναι μέσω κατάκλισής του με πλαίσια EAPOL-Start frames [6], [75].

5) Επιθέσεις κατά του πρωτοκόλλου TKIP

Το TKIP (Temporal Key Integrity Protocol) είναι ένα πρωτόκολλο, το οποίο περιλαμβάνει αντίμετρα για τον εντοπισμό και την απόκριση σε μια ενεργή επίθεση, τερματίζοντας το δίκτυο και ανανεώνοντας τα κλειδιά που χρησιμοποιούνται. Οι επιθέσεις κατά του πρωτοκόλλου TKIP εκμεταλλεύονται τον μηχανισμό ελέγχου MIC (Message Integrity Check) που περιλαμβάνει, σύμφωνα με τον οποίο, το πρωτόκολλο διακόπτει κάθε δραστηριότητα για ένα λεπτό και στη συνέχεια ανανεώνει τα κλειδιά μιας επικοινωνίας μετά τη λήψη δύο πλαισίων MIC. Οι επίδοξοι επιτιθέμενοι καταφέρνουν να δημιουργήσουν περίπτωση DoS στο σημείο AP μέσω της αποστολής ενός μεγάλου αριθμού μη έγκυρων πλαισίων MIC. Ο συγκεκριμένος τρόπος επίθεσης μπορεί να χρησιμοποιηθεί σε δίκτυα WLAN που χρησιμοποιούν μόνο το πρωτόλολο TKIP για κρυπτογράφηση ή σε εκείνα που χρησιμοποιούν συνδυασμό των πρωτοκόλλων TKIP και CCMP (Counter Mode with Cipher Block Chaining-MAC Protocol), ακόμα και όταν χρησιμοποιείται ο πιο ασφαλής μηχανισμός ελέγχου ταυτότητας και ελέγχου πρόσβασης των ασύρματων συσκευών από το σημείο AP του δικτύου. Αυτό συμβαίνει επειδή η ύπαρξη οποιασδήποτε συσκευής TKIP σε ένα δίκτυο WLAN θα αναγκάσει το σημείο AP να χρησιμοποιήσει κλειδί TKIP ακόμη και σε συσκευές CCMP [6], [75].

6) Επιθέσεις DoS με εκμετάλλευση της ευπάθειας hole 196 του πρωτόκολλου WPA

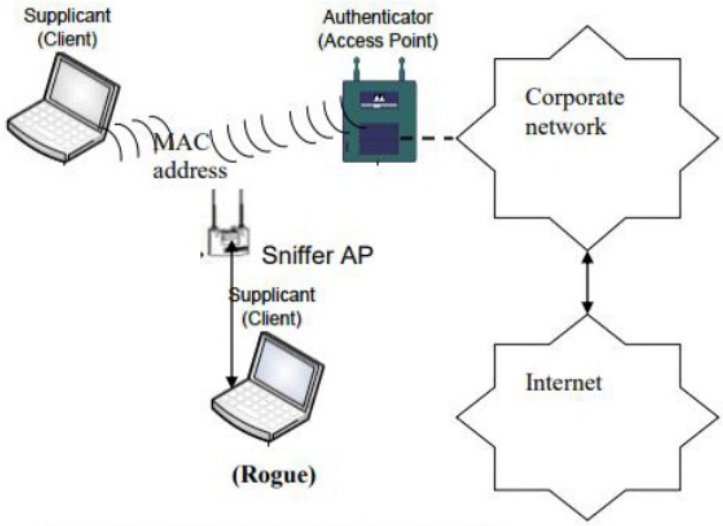
Η ευπάθεια hole 196 εκθέτει την ασφάλεια των εξουσιοδοτημένων συσκευών ενός δικτύου WLAN, που προστατεύεται από το πρωτόκολλο WPA (Wi-Fi Protected Access), σε κακόβουλους χρήστες. Σε μια τέτοια επίθεση DoS, οι επιτιθέμενοι εκμεταλλεύονται τη χρήση του κλειδιού GTK (Group Transient Key) στο πρωτόκολλο WPA και χρησιμοποιούν μια κακόβουλη συσκευή για την εκπομπή πλαστών πλαισίων δεδομένων μεγάλου αριθμού πακέτων. Μετά από μια τέτοια εκπομπή, οι συσκευές (θύματα της επίθεσης) του δικτύου WLAN αγνοούν τα νόμιμα πλαίσια με αριθμούς πακέτων που είναι μικρότεροι από τον αριθμό των πακέτων που εκπέμπονται από την κακόβουλη συσκευή. Για την πραγματοποίηση μιας τέτοιου είδους επίθεσης, η κακόβουλη συσκευή θα πρέπει πρώτα να έχει πιστοποιηθεί σωστά στο δίκτυο WLAN. Υπάρχουν όμως περιπτώσεις, που ο επιτιθέμενος μπορεί να παρακάμψει τους ορθούς τρόπους ελέγχου ταυτότητας, χρησιμοποιώντας εικονικό σημείο AP [6], [75], [77].

4.1.2 Επιθέσεις κατά της εμπιστευτικότητας των δεδομένων δικτύου WLAN

Οι επιθέσεις κατά της εμπιστευτικότητας των δεδομένων που μεταδίδονται εντός ενός δικτύου WLAN αφορούν εκείνο το είδος των επιθέσεων που αποσκοπούν στην υποκλοπή των πληροφοριών που ανταλλάσσονται μεταξύ δύο μερών που επικοινωνούν στο ασύρματο δίκτυο. Οι επιθέσεις εμπιστευτικότητας είναι κρυφές επιθέσεις που πραγματοποιούνται σε πραγματικό χρόνο και έχουν ως στόχο την παρακολούθηση, την αποκρυπτογράφηση και την ανάλυση των πληροφοριών που μεταδίδονται ασύρματα εντός του δικτύου WLAN, χωρίς να υπάρχει η ανάγκη απόκτησης πρόσβασης σε αυτό μέσω των διαδικασιών ελέγχου ταυτότητας και συσχέτισης. Για το λόγο αυτό, η φιλοσοφία τους είναι τελείως διαφορετική αυτής των επιθέσεων κατά της διαθεσιμότητας των δικτύων WLAN [77]. Όπως φαίνεται στην εικόνα 4.1, οι επιθέσεις αυτές μπορούν να επιτευχθούν με δύο τρόπους [6], [75], [77]: (α) ο επιτιθέμενος μπορεί να παίξει το ρόλο του MITM (Man-In-The-Middle) (ευρισκόμενος στη διαδρομή επικοινωνίας των χρηστών στο δίκτυο WLAN) και (β) ο επιτιθέμενος είναι σε θέση να σπάσει τον μηχανισμό του πρωτοκόλλου εμπιστευτικότητας της σουίτας κρυπτογράφησης που χρησιμοποιείται στο δίκτυο WLAN.

1) Επιθέσεις MITM

Στην κατηγορία των επιθέσεων MITM περιλαμβάνονται εκείνες που βασίζονται στο γεγονός ότι ο επιτιθέμενος βρίσκεται στη διαδρομή επικοινωνίας μεταξύ των χρηστών του δικτύου WLAN, με αποτέλεσμα να του δίνεται η δυνατότητα να υποκλέπτει τις πληροφορίες που μεταδίδονται, χωρίς να γίνεται αντιληπτός. Επιθέσεις MITM μπορούν να θεωρηθούν οι [6], [75], [78]: (α) επιθέσεις μέσω πλαστογράφησης της διεύθυνσης MAC, (β) επιθέσεις Evil Twin με χρήση του captive portal, (γ) επιθέσεις ανακατεύθυνσης κυκλοφορίας μέσω ARP poisoning ή πλαστογράφησης ARP και (δ) επιθέσεις πιστοποιητικών RADIUS.

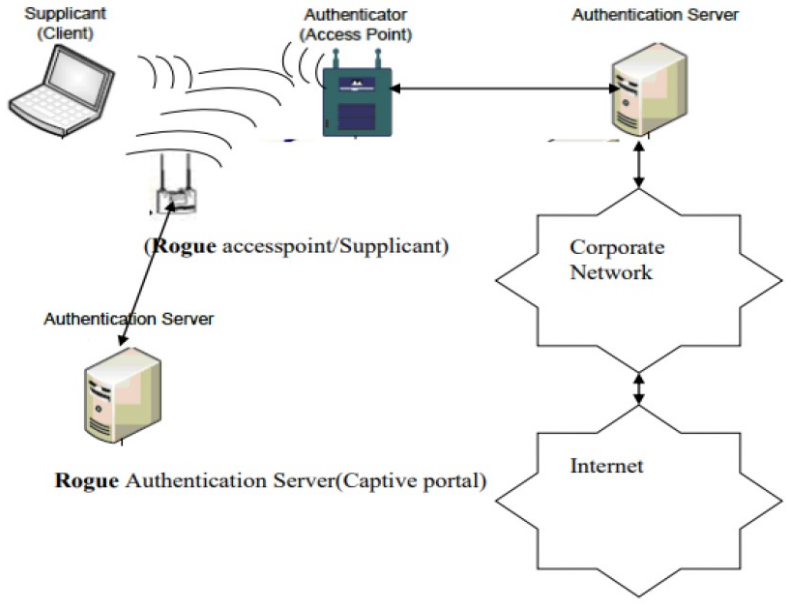


Εικόνα 4.5: Παράδειγμα επίθεσης πλαστογράφησης της διεύθυνσης MAC [75]

Η πλαστογράφηση της διεύθυνσης MAC (MAC address spoofing) αποτελεί συνηθισμένη μορφή επίθεσης στην οποία ο επιτιθέμενος εμφανίζεται ως νόμιμος χρήστης του δικτύου WLAN, χρησιμοποιώντας ασύρματη συσκευή στην οποία αλλάζει τη διεύθυνση MAC για να προσποιηθεί ότι είναι νόμιμη (Εικ. 4.5). Παρά το γεγονός ότι από μόνη της η πλαστογράφηση της διεύθυνσης MAC δεν αποτελεί σοβαρή απειλή, μπορεί να αξιοποιηθεί για την πραγματοποίηση άλλων πολύ σοβαρών επιθέσεων, όπως οι επιθέσεις DoS που αναφέρθηκαν στην προηγούμενη ενότητα, δημιουργώντας

προβλήματα στην ακεραιότητα και στη διαθεσιμότητα του δικτύου. Για την πραγματοποίηση της συγκεκριμένης επίθεσης, ο επιτιθέμενος εκμεταλλεύεται διάφορα τρωτά σημεία ενός δικτύου WLAN, όπως η έλλειψη προστασίας του πλαισίου διαχείρισης, η έλλειψη αμοιβαίας επαλήθευσης ταυτότητας μεταξύ σημείου AP και των ασύρματων συσκευών, κλπ. Σε μια τέτοια επίθεση, η κακόβουλη συσκευή περιμένει έως ότου η νόμιμη συσκευή, της οποίας έχει πλαστογραφήσει τη διεύθυνση MAC, να αποσυνδεθεί από το σημείο AP του δικτύου WLAN και, στη συνέχεια, επιχειρεί να συσχετιστεί με το σημείο AP. Εάν αυτή η προσπάθεια είναι πετυχημένη, θα έχει αποκτήσει παράνομη πρόσβαση στο δίκτυο WLAN, με αποτέλεσμα να μπορεί να υποκλέψει την κυκλοφορία που μεταδίδεται εντός του δικτύου για ανάλυση εκτός σύνδεσης ή να χρησιμοποιήσει το δίκτυο WLAN για να αποκτήσει πρόσβαση στους πόρους του, όπως θα έκανε ένας νόμιμος πελάτης WLAN [6], [75], [78].

Η επίθεση Evil Twin με χρήση του captive portal πραγματοποιείται μέσω της δημιουργίας ενός κακόβουλου διακομιστή ελέγχου ταυτότητας, με πανομοιότυπη σελίδα σύνδεσης (captive portal) με την νόμιμη, ο οποίος χρησιμοποιείται για τη συλλογή/αποτύπωση των διαπιστευτηρίων των νόμιμων χρηστών κατά τη διαδικασία σύνδεσής τους στο δίκτυο WLAN (Εικ. 4.6). Τα τρωτά σημεία του δικτύου WLAN που εκμεταλλεύεται ένας επιτιθέμενος για την πραγματοποίηση μιας τέτοιας επίθεσης αφορούν την έλλειψη αμοιβαίου ελέγχου ταυτότητας μεταξύ του χρήστη και του captive portal του διακομιστή ελέγχου ταυτότητας και την έλλειψη επικύρωσης του πιστοποιητικού που παρέχεται από τον διακομιστή ελέγχου ταυτότητας. Για την πραγματοποίηση της επίθεσης, ο επιτιθέμενος αρχικά χρησιμοποιεί ένα κακόβουλο σημείο AP για να πλαστογραφήσει το έγκυρο αναγνωριστικό SSID (Service Set IDentifier), με το οποίο οι χρήστες συνδέονται στο hotspot του δικτύου. Στη συνέχεια, το κακόβουλο σημείο AP εκπέμπει το έγκυρο αναγνωριστικό SSID για να ξεγελάσει του ανυποψίαστους χρήστες ώστε να συνδεθούν με αυτό. Μετά τη σύνδεση, ο χρήστης ανακατευθύνεται στον κακόβουλο διακομιστή ελέγχου ταυτότητας, που περιέχει ένα captive portal, το οποίο δημιουργήθηκε έτσι ώστε να φαίνεται αυθεντικό. Καθώς ο χρήστης του hotspot εισάγει τον κωδικό πρόσβασής του ή δημιουργεί νέες πληροφορίες ταυτότητας, τα στοιχεία του καταγράφονται στο κακόβουλο captive portal, με αποτέλεσμα ο επιτιθέμενος να έχει αποκτήσει έγκυρα διακριτικά (όνομα χρήστη και κωδικό πρόσβασης) για να συνδεθεί στο δίκτυο WLAN. Κάτι τέτοιο του επιτρέπει την υποκλοπή κρίσιμων πληροφοριών ή/και τη χρήση του δικτύου για να εξαπολύσει άλλου είδους επιθέσεις [6], [75].



Εικόνα 4.6: Παράδειγμα επίθεσης Evil Twin με χρήση captive portal [75]

Οι επιθέσεις ανακατεύθυνσης κυκλοφορίας μέσω ARP poisoning ή πλαστογράφησης ARP πραγματοποιούνται με τη χρήση μιας κακόβουλης συσκευής που λειτουργεί ως MITM μεταξύ του σημείου AP και ενός switch του δικτύου, με σκοπό την απόκτηση πρόσβασης στους πίνακες ARP (Address Resolution Protocol) του switch. Με την επιτυχημένη πραγματοποίηση της επίθεσης, τα πλαίσια δεδομένων που κατευθύνονται προς διάφορους προορισμούς του δικτύου, ανακατευθύνονται προς την κακόβουλη συσκευή, κάτι που της δίνει τη δυνατότητα να τα υποκλέψει για μεταγενέστερη ανάλυση ή να τα χρησιμοποιήσει για την πραγματοποίηση άλλων επιθέσεων MITM. Από την ανάλυση του τρόπου πραγματοποίησης της επίθεσης, προκύπτει το συμπέρασμα ότι μπορεί να θέσει σε κίνδυνο ακόμη και συσκευές του ενσύρματου δικτύου και θα μπορούσαν να συνδεθούν στο ασύρματο μέσω του switch. Μια άλλη πιθανή προσέγγιση πραγματοποίησης της επίθεσης ανακατεύθυνσης της κυκλοφορίας είναι μέσω της πλαστογράφησης των πινάκων ARP με εκμετάλλευση της ευπάθειας hole 196 του πρωτόκολλου WPA. Σε αυτήν την περίπτωση η κακόβουλη συσκευή μεταμφιέζεται ως σημείο AP και χρησιμοποιεί το κλειδί GTK για τη μετάδοση πλαισίων δεδομένων απευθείας σε άλλους ασύρματους πελάτες του δικτύου WLAN. Έτσι, οι συσκευές-θύματα, αναγνωρίζοντας το κακόβουλο σημείο AP ως τον προεπιλεγμένο δρομολογητή του δικτύου, θα διοχετεύουν όλη την κίνηση μέσω αυτού [6], [75], [79].

Τέλος, οι επιθέσεις πιστοποιητικών RADIUS πραγματοποιούνται μέσω της εκμετάλλευσης των ευπαθειών που σχετίζονται με τη χρήση ψηφιακών πιστοποιητικών από τις ασύρματες συσκευές για την επαλήθευση του διακομιστή RADIUS (Remote Authentication Dial-In User Service). Πολλές ασύρματες συσκευές ενός δικτύου WLAN ρυθμίζονται ώστε να μην απορρίπτουν πιστοποιητικά που παρέχονται από τον διακομιστή RADIUS, με αποτέλεσμα να δέχονται ψηφιακά πιστοποιητικά που μπορεί να έχουν υπογραφεί από εσφαλμένη αρχή έκδοσης πιστοποιητικών. Αυτό το στοιχείο, επομένως, μπορεί να αποτελέσει σημείο εκμετάλλευσης από έναν επιτιθέμενο και να χρησιμοποιήσει έναν κακόβουλο διακομιστής RADIUS με σκοπό την παροχή τέτοιων ψηφιακών πιστοποιητικών σε ασύρματες συσκευές, οι οποίες θα τα αποδεχθούν αυτόματα, επιτρέποντας τη μεταξύ τους σύνδεσης. Με την ολοκλήρωση της σύνδεσης, ο κακόβουλος διακομιστής RADIUS μπορεί να υποκλέψει τα διαπιστευτήρια της ασύρματης συσκευής [80].

2) Επιθέσεις κρυπτογράφησης

Πρόκειται για επιθέσεις που στοχεύουν τους κρυπτογραφικούς αλγόριθμους και τα πρωτόκολλα ασφάλειας του δικτύου (WEP, WPA, WPA2, κλπ.) που χρησιμοποιούνται κατά τον έλεγχο ταυτότητας και οδηγούν στην αποκρυπτογράφηση των κρυπτογραφημένων πακέτων που μεταδίδονται εντός του δικτύου WLAN ή στην ανάκτηση του κλειδιού. Επομένως, η βασική πρόθεση του επιτιθέμενου σε αυτές τις επιθέσεις είναι να σπάσει το σύστημα κρυπτογράφησης που χρησιμοποιείται στα συστήματα WLAN για να εξάγει τις πληροφορίες που βρίσκονται εντός των κρυπτογραφημένων πλαισίων που μεταδίδονται σε αυτά. Η πρόθεση αυτή μπορεί να πραγματοποιηθεί μέσω της ανακάλυψης του μυστικού κλειδιού που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης των πλαισίων δεδομένων. Ανάλογα με τη μέθοδο που χρησιμοποιείται σε κάθε επίθεση κρυπτογράφησης, οι επιθέσεις αυτές μπορούν να ταξινομηθούν ως εξής [6], [75], [81]: (α) επιθέσεις μόνο κρυπτογραφημένου κειμένου, (β) επιθέσεις γνωστού απλού κειμένου, (γ) επιθέσεις γνωστού κρυπτογραφημένου κειμένου, (δ) επιθέσεις λεξικού, (ε) επιθέσεις ωμής βίας και στ) επιθέσεις χρόνου.

Στις επιθέσεις μόνο κρυπτογραφημένου κειμένου (Ciphertext Only Attacks – COA), γνωστές και ως επιθέσεις γνωστού κρυπτογραφημένου κειμένου, ο επιτιθέμενος παρακολουθεί τα κανάλια επικοινωνίας του δικτύου WLAN και συλλέγει με παθητικό τρόπο κρυπτογραφημένα κείμενα. Με τον τρόπο αυτό έχει στην κατοχή του ένα σύνολο κρυπτογραφημένων κειμένων, μέσα από το οποίο

προσπαθεί να εντοπίσει τα αντίστοιχα απλά κείμενα ή να ανακαλύψει το κλειδί κρυπτογράφησής τους [82].

Στις επιθέσεις γνωστού απλού κειμένου (Known Plaintext Attacks - KPA), ο επιτιθέμενος γνωρίζει τα απλά κείμενα που αντιστοιχούν σε ορισμένα μέρη των κρυπτογραφημένων κειμένων. Στόχος του είναι να ανακαλύψει το κλειδί κρυπτογράφησης ώστε να μπορέσει να αποκρυπτογραφήσει και τα υπόλοιπα κρυπτογραφημένα κείμενα [83].

Στις επιθέσεις επιλεγμένου κρυπτογραφημένου κειμένου (Chosen Cipher Attacks – CCA), ο επιτιθέμενος προσπαθεί να συλλέξει συγκεκριμένα μέρη των απλών κειμένων που αντιστοιχούν σε συγκεκριμένα μέρη κρυπτογραφημένων κειμένων, ώστε να μπορέσει να ανακαλύψει το κλειδί κρυπτογράφησης και να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο της επιλογής του [83].

Στις επιθέσεις λεξικού (dictionary attacks), ο επιτιθέμενος συντάσσει ένα λεξικό με όλα τα κρυπτογραφημένα κείμενα και τα αντίστοιχα απλά κείμενα που του έγιναν γνωστά σε μια χρονική περίοδο. Με τον τρόπο αυτό του δίνεται η δυνατότητα, οποτεδήποτε συλλαμβάνει κάποιο κρυπτογραφημένο κείμενο, να ανατρέξει στο λεξικό για να βρει το αντίστοιχο απλό κείμενο [84]. Παραδείγματα επιθέσεων λεξικού, αποτελούν οι επιθέσεις λεξικού WPA-PSK και οι επιθέσεις λεξικού LEAP. Στις επιθέσεις λεξικού WPA-PSK (Pre-Shared Key), οι επιτιθέμενοι εκμεταλλεύονται τις αδυναμίες που παρουσιάζει η επιλογή του ήδη κοινόχρηστου κλειδιού. Τις περισσότερες φορές τα ήδη κοινόχρηστα κλειδιά είναι σύντομες λέξεις που υπάρχουν σε λεξικό, με αποτέλεσμα, ο επιτιθέμενος να μπορεί να τα αποκτήσει εύκολα [6]. Κατά τις επιθέσεις λεξικού LEAP (Lightweight EAP), οι επιτιθέμενοι στοχεύουν τα δίκτυα WLAN που εφαρμόζουν το πρωτόκολλο LEAP ως μηχανισμό ελέγχου ταυτότητας, καθώς η συγκεκριμένη μέθοδος ελέγχου ταυτότητας παρουσιάζει αδύναμα διαπιστευτήρια. Κάτι τέτοιο, επιτρέπει την υποκλοπή πακέτων και την ανάλυσή τους εκτός σύνδεσης, για την απόκτηση των διαπιστευτηρίων του χρήστη [6].

Στις επιθέσεις ωμής βίας (Brute Force Attacks - BFA), ο επιτιθέμενος προσπαθεί να προσδιορίσει το κλειδί κρυπτογράφησης μέσω εξαντλητικής δοκιμής όλων των πιθανών κλειδιών που θα μπορούσαν να έχουν χρησιμοποιηθεί κατά τη διαδικασία της κρυπτογράφησης. Ο συγκεκριμένος τρόπος επίθεσης είναι ιδιαίτερα χρονοβόρος καθώς η εύρεση του κλειδιού κρυπτογράφησης θα πρέπει να εντοπιστεί μέσα από τη δοκιμή όλων των αριθμών των πιθανών τιμών του κλειδιού. Ο αριθμός αυτός μεγαλώνει όσο μεγαλύτερο είναι το μήκος του κλειδιού κρυπτογράφησης [84].

Κατά τις διαδικασίες που εκτελούνται από τον αλγόριθμο κρυπτογράφησης, ο χρόνος υπολογισμού για την εξαγωγή του κλειδιού, αλλά και την κρυπτογράφηση ή την αποκρυπτογράφηση ενός μηνύματος, ποικίλει. Βασιζόμενος σε αυτή τη γνώση, και για να πραγματοποιήσει μια επίθεση χρόνου (timing attack), ο επιτιθέμενος συλλέγει μια σειρά από μετρήσεις χρόνου του δικτύου και στη συνέχεια εκτελεί στατιστική ανάλυση για να αποκαλύψει τις διαφορές στο χρόνο εκτέλεσης της εκάστοτε διαδικασίας. Με τη μέτρηση τέτοιων χρόνων, επομένως, δίνεται η δυνατότητα στον επιτιθέμενο να κατανοήσει τον εκάστοτε υπολογισμό που πραγματοποιήθηκε [85].

Όλες οι επιθέσεις κρυπτογράφησης βασίζονται στην εκμετάλλευση των τρωτών σημείων που παρουσιάζουν οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται στα δίκτυα WLAN, όπως οι WEP, WPA, WPA2, κλπ. Η ανάλυσή τους θα πραγματοποιηθεί σε επόμενη υποενότητα.

4.1.3 Επιθέσεις κατά της ακεραιότητας των δεδομένων δικτύου WLAN

Η ακεραιότητα των δεδομένων διασφαλίζει ότι δεν πραγματοποιείται καμία αλλαγή των μεταδιδόμενων δεδομένων μεταξύ της πηγής και του προορισμού. Επομένως, οι επιθέσεις κατά της

ακεραιότητας των δεδομένων έχουν ως σκοπό την τροποποίηση των δεδομένων που μεταδίδονται εντός του δικτύου WLAN, έτσι ώστε αυτό που φτάνει στον προορισμό να μην είναι αυτό που στάλθηκε από την πηγή. Μια τέτοια τροποποίηση των δεδομένων μπορεί να αφορά τη διαγραφή ή προσθήκη πλαισίων διαχείρισης ή δεδομένων ή τη δημιουργία πλαστών πακέτων ελέγχου. Όλες αυτές οι τροποποιήσεις των δεδομένων σε ένα δίκτυο WLAN μπορούν να έχουν στόχο ακόμα και την πραγματοποίηση άλλου είδους επιθέσεων, η επιτυχία των οποίων μπορεί να εξαρτάται από τις επιθέσεις κατά της ακεραιότητας των μεταδιδόμενων πλαισίων εντός του δικτύου WLAN. Εκτός από τις επιθέσεις DoS και MITM, που περιγράφηκαν στις προηγούμενες υποενότητες, που μπορούν να χρησιμοποιηθούν και ως επιθέσεις κατά της ακεραιότητας των δεδομένων στα δίκτυα WLAN, άλλες γνωστές επιθέσεις που μπορούν να προκαλέσουν τροποποίηση των πλαισίων δεδομένων, είναι οι [6], [86]: (α) επιθέσεις πειρατείας συνεδρίας, (β) επιθέσεις επανάληψης, (γ) επιθέσεις έγχυσης πλαισίων δεδομένων και (δ) επιθέσεις διαγραφής δεδομένων.

1) Επιθέσεις πειρατείας συνεδρίας

Στις επιθέσεις πειρατείας συνεδρίας (session hijacking), ο επιτιθέμενος έχει ως σκοπό το κλέψιμο μιας εξουσιοδοτημένης και πιστοποιημένης συνεδρίας από έναν νόμιμο χρήστη του δικτύου. Σε αυτήν την περίπτωση, ο νόμιμος χρήστης πιστεύει ότι η απώλεια συνεδρίας μπορεί να αποτελεί μια κάποια δυσλειτουργία του δικτύου WLAN και επομένως, δεν αντιλαμβάνεται του τι πραγματικά έχει συμβεί. Οι επιθέσεις πειρατείας συνεδρίας πραγματοποιούνται σε πραγματικό χρόνο και ο επιτιθέμενος μπορεί να χρησιμοποιήσει τη συνεδρία για όποιον σκοπό θέλει, διατηρώντας την για μεγάλο χρονικό διάστημα. Η πραγματοποίηση της επίθεσης γίνεται σε δύο στάδια. Στο πρώτο, ο επιτιθέμενος μεταμφιέζεται ως η νόμιμη συσκευή που αποτελεί στόχο του. Με τον τρόπο αυτό είναι σε θέση να υποκλέψει την επικοινωνία της συσκευής που στοχεύει και να συγκεντρώσει τις απαραίτητες πληροφορίες. Στο δεύτερο στάδιο, ο επιτιθέμενος αποστέλλει μια μεγάλη ακολουθία πλαστών πακέτων αποσύνδεσης, για να κρατήσει την νόμιμη συσκευή εκτός της συνεδρίας [86].

2) Επιθέσεις επανάληψης

Οι επιθέσεις επανάληψης (replay attacks) δεν αποτελούν επιθέσεις σε πραγματικό χρόνο και χρησιμοποιούν τις νόμιμες περιόδους ελέγχου ταυτότητας για πρόσβαση στο δίκτυο WLAN. Ο επιτιθέμενος αρχικά υποκλέπτει τη συνεδρία της διαδικασίας ελέγχου ταυτότητας ενός νόμιμου χρήστη. Αργότερα, όποτε εκείνος το κρίνει σκόπιμο, επαναλαμβάνει τη συνεδρία ελέγχου ταυτότητας που έχει υποκλέψει για να αποκτήσει πρόσβαση στο δίκτυο, χωρίς να την τροποποιήσει [86].

3) Επιθέσεις έγχυσης πλαισίων δεδομένων

Στις επιθέσεις έγχυσης πλαισίων δεδομένων (frame injection attacks) ο επιτιθέμενος αποστέλλει πλαστά ή τροποποιημένα πλαίσια δεδομένων κατά τη διάρκεια μιας μετάδοσης. Για παράδειγμα, ο επιτιθέμενος θα μπορούσε να εγχύσει πλαίσια δεδομένων κατά τη διάρκεια σύνδεσης ενός χρήστη σε έναν ιστότοπο μέσω ασύρματης σύνδεσης, προσπαθώντας να τροποποιήσει την νομιμότητα του ιστότοπου. Με αυτόν τον τρόπο, όλες οι πληροφορίες σύνδεσης θα καταγραφούν από τον επιτιθέμενο [86].

4) Επιθέσεις διαγραφής δεδομένων

Σε αυτές τις επιθέσεις, ο επιτιθέμενος διαγράφει τα δεδομένα που μεταδίδονται. Κάτι τέτοιο θα μπορούσε να πραγματοποιηθεί μέσω μπλοκαρίσματος (jamming) του σήματος που μεταδίδεται προς τον προορισμό και την αποστολή μηνυμάτων επιβεβαίωσης λήψης (ACK) προς την πηγή. Με αυτό τον τρόπο, τα δεδομένα δεν φτάνουν ποτέ στον προορισμό τους, κάτι που δεν γίνεται αντιληπτό από την πηγή, από τη στιγμή που έλαβε μήνυμα ACK [86].

4.1.4 Ανάλυση τρωτών σημείων που αξιοποιούνται κατά τις επιθέσεις

Όπως αναλύθηκε στις προηγούμενες υποενότητες, οι επιθέσεις κατά των δικτύων WLAN θέτουν σε κίνδυνο τη διαθεσιμότητα του ίδιου του δικτύου, αλλά και την εμπιστευτικότητα και την ακεραιότητα των δεδομένων που μεταδίδονται σε αυτά. Όλες αυτές οι επιθέσεις εκμεταλλεύονται διάφορες ευπάθειες και τρωτά σημεία των δικτύων WLAN.

Οι επιθέσεις κατά της διαθεσιμότητας του δικτύου, που όπως αναφέρθηκε είναι γνωστές και ως επιθέσεις DoS, εκμεταλλεύονται κυρίως την έλλειψη μηχανισμών προστασίας των πλαισίων διαχείρισης που μεταδίδονται εντός των δικτύων WLAN. Λόγω αυτής της έλλειψης, η επιτυχία επιθέσεων, όπως οι επιθέσεις αποσύνδεσης και οι επιθέσεις κατάργησης ταυτότητας είναι μάλλον δεδομένη [87]. Οι σωστές διαμορφώσεις του λειτουργικού συστήματος και των προγραμμάτων οδήγησης (driver) των ασύρματων συσκευών, αλλά και του υλικολογισμικού (firmware) του σημείου AP, αποτελούν καθοριστικούς παράγοντες αντιμετώπισης της ικανότητας των επιτιθέμενων να εκμεταλλεύονται αυτά τα τρωτά σημεία των δικτύων WLAN [88]. Για παράδειγμα, η δυνατότητα των λειτουργικών συστημάτων των ασύρματων συσκευών να υποστηρίζουν διάφορες λειτουργίες, όπως τα εικονικά WLAN, δημιουργεί μια ευπάθεια που μπορεί να αξιοποιηθεί για να διευκολυνθεί η πραγματοποίηση επιθέσεων DoS με εκμετάλλευση της ευπάθειας hole 196 του πρωτόκολλου WPA [6]. Επίσης, η μη σωστή διαμόρφωση των προγραμμάτων οδήγησης αποτελεί μία ευπάθεια η οποία μπορεί να οδηγήσει στην πραγματοποίηση επιθέσεων δακτυλικών αποτυπωμάτων (fingerprinting attacks) [89]. Η αδυναμία των πρωτοκόλλων IEEE 802.11 να υποστηρίξουν μηχανισμούς συνδυασμού του πρωτοκόλλου EAP με σουίτες κρυπτογράφησης οδηγεί σε επιλογές κρυπτογράφησης που μπορούν να αξιοποιηθούν από τους επιτιθέμενους για την εξαπόλυση επιθέσεων πλημμύρας πρωτοκόλλου EAP και επιθέσεων κατά του πρωτοκόλλου TKIP [6]. Τέλος, η θέση της βάσης δεδομένων των χρηστών παίζει σημαντικό ρόλο στον καθορισμό του πόσο εύκολο είναι για τους επιτιθέμενους να την εκμεταλλευτούν για την πραγματοποίηση επιθέσεων. Όταν αυτή η βάση δεδομένων δεν βρίσκεται στη συσκευή του χρήστη, αλλά είναι ενσωματωμένη στο σημείο AP ή σε κάποια κεντρική βάση δεδομένων, τότε είναι εύκολη η πραγματοποίηση κάποιου είδους επίθεσης DoS, όπως οι επιθέσεις πλημμύρας πρωτοκόλλου EAP [6].

Για την πραγματοποίηση επιθέσεων κατά της εμπιστευτικότητας των δεδομένων, οι επιτιθέμενοι εκμεταλλεύονται διάφορα τρωτά σημεία των δικτύων WLAN, όπως [6], [90], [91]: (α) τους υφιστάμενους μηχανισμούς ελέγχου ταυτότητας, που δεν υποστηρίζουν ασφαλείς αμοιβαίους ελέγχους ταυτότητας μεταξύ των σημείων AP και των ασύρματων συσκευών, (β) τις διαμορφώσεις του υλικολογισμικού (firmware) των ασύρματων συσκευών και των σημείων AP, που δεν διαθέτουν μηχανισμούς προστασίας των πλαισίων διαχείρισης κατά τις διαδικασίες ελέγχου ταυτότητας, (γ) τη ρύθμιση των παραμέτρων των ασύρματων συσκευών για παράβλεψη επικύρωσης του ψηφιακού πιστοποιητικού που δημιουργείται από το captive portal του διακομιστή ελέγχου ταυτότητας, (δ) τη χρήση εικονικών σημείων AP και (ε) την εσφαλμένη διαμόρφωση των ασύρματων συσκευών για την αποδοχή ψηφιακών πιστοποιητικών που έχουν επικυρωθεί από άλλες ασύρματες συσκευές. Για παράδειγμα, η αδυναμία των ασύρματων συσκευών να επικυρώσουν σωστά τα πιστοποιητικά που δημιουργούνται από το διακομιστή ελέγχου ταυτότητας οδηγεί σε επιθέσεις MITM, όπως επιθέσεις Evil Twin με χρήση του captive portal και επιθέσεις πιστοποιητικών RADIUS [92].

Πολλές από τις επιθέσεις κρυπτογράφησης πραγματοποιούνται μέσω εκμετάλλευσης των τρωτών σημείων που παρουσιάζουν τα πρωτόκολλα ασφάλειας των δικτύων WLAN και οι διάφορες χρησιμοποιούμενες τεχνικές κρυπτογράφησης. Για παράδειγμα, το πρωτόκολλο WEP αποτελεί έναν εύκολο στόχο για την πραγματοποίηση πολλών επιθέσεων κατά της εμπιστευτικότητας των

δεδομένων, στις οποίες επιτυγχάνεται αποκρυπτογράφηση των προστατευμένων πλαισίων δεδομένων ή ανάκτηση του κλειδιού WEP [86]. Η μη ορθή ρύθμιση των παραμέτρων της φράσης πρόσβασης (passphrase) κατά τη διαδικασία υλοποίησης του πρωτοκόλλου WPA οδηγεί στη δημιουργία αδύναμων ήδη κοινόχρηστων κλειδιών (Pre-Shared Key - PSK), κάτι το οποίο μπορούν να εκμεταλλευτούν οι επιτιθέμενοι για την πραγματοποίηση επιθέσεων λεξικού, όπως οι επιθέσεις WPA-PSK [92]. Η χρήση του πρωτοκόλλου LEAP ως μηχανισμού ελέγχου ταυτότητας ανώτερου επιπέδου μπορεί επίσης να αξιοποιηθεί για να προκαλέσει επιθέσεις λεξικού LEAP [90].

Συνοψίζοντας, μπορεί να αναφερθεί ότι, σε γενικές γραμμές οι επιθέσεις κατά των δικτύων WLAN στοχεύουν τους μηχανισμούς ελέγχου ταυτότητας, τον διακομιστή ελέγχου ταυτότητας, τα διαπιστευτήρια ελέγχου ταυτότητας, τη βάση δεδομένων του χρήστη, το λειτουργικό σύστημα και τα προγράμματα οδήγησης των ασύρματων συσκευών, το υλικολογισμικό του σημείου AP, τα πρωτόκολλα ασφάλειας και τις τεχνικές κρυπτογράφησης. Από την ανάλυση της βιβλιογραφίας, προκύπτει το συμπέρασμα ότι, ενώ οι διάφορες μελέτες και έρευνες πάνω στα θέματα ασφάλειας των δικτύων WLAN μπόρεσαν να αποκαλύψουν τα τρωτά τους σημεία που οδηγούν στην πραγματοποίηση επιθέσεων, και παρά τις διάφορες λύσεις που έχουν παρουσιαστεί κατά καιρούς πάνω στην αντιμετώπιση αυτών των επιθέσεων, δεν έχουν πραγματοποιηθεί εις βάθος προτάσεις που να αφορούν τη λήψη καθολικών αποφάσεων ως προς την επιλογή των κατάλληλων χαρακτηριστικών ασφαλείας των δικτύων WLAN [6].

4.2 Πρωτόκολλα κρυπτογράφησης δικτύων WLAN

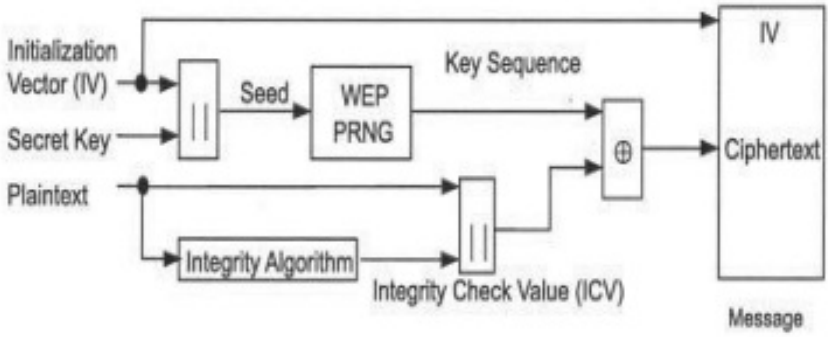
Η κρυπτογράφηση και ο έλεγχος ταυτότητας αποτελούν δύο πολύ σημαντικά μέτρα ασφαλείας που μπορούν να χρησιμοποιηθούν για την προστασία των δικτύων WLAN. Η κρυπτογράφηση χρησιμοποιείται για την προστασία του απορρήτου των δεδομένων, ενώ ο έλεγχος ταυτότητας χρησιμοποιείται για την επαλήθευση της ταυτότητας των χρηστών και των συσκευών [93]. Σε αυτήν την ενότητα, θα παρουσιαστούν οι πιο κοινοί μηχανισμοί και τα πιο σημαντικά πρωτόκολλα κρυπτογράφησης που χρησιμοποιούνται στα WLAN, καθώς και τα πλεονεκτήματα και τα μειονεκτήματά τους. Οι αντίστοιχοι μηχανισμοί και πρωτόκολλα ελέγχου ταυτότητας θα παρουσιαστούν στην επόμενη ενότητα.

Τα πρωτόκολλα κρυπτογράφησης των δικτύων WLAN αναφέρονται στη βιβλιογραφία και ως πρωτόκολλα εμπιστευτικότητας και ακεραιότητας [6], [93], [94]. Τα πρωτόκολλα αυτά αποτελούν την πολιτική ασφάλειας των δικτύων WLAN, χρησιμοποιούμενα κατά τη διαδικασία συσχέτισης μεταξύ της ασύρματης συσκευής και του σημείου AP και πιο συγκεκριμένα κατά την περίοδο επικοινωνίας των δύο μονάδων, όταν ο έλεγχος ταυτότητας της ασύρματης συσκευής είναι επιτυχημένη. Σύμφωνα με την πολιτική ασφάλειας των δικτύων WLAN, τα πρωτόκολλα κρυπτογράφησης είναι υπεύθυνα για τη δημιουργία και τη διαχείριση κλειδιών δυναμικής κρυπτογράφησης, τα οποία είναι διαφορετικά για κάθε περίπτωση συσχέτισης, αλλά και για την παροχή μηχανισμών κρυπτογράφησης και προστασίας της ακεραιότητας των δεδομένων [95], [96]. Η κρυπτογράφηση αποτελεί μια διαδικασία μετατροπής των δεδομένων απλού κειμένου σε κωδικοποιημένη μορφή, τέτοιας μορφής που να μην μπορεί να διαβαστεί από μη εξουσιοδοτημένους χρήστες. Στα διάφορα πρότυπα επικοινωνίας WLAN έχουν χρησιμοποιηθεί διάφορες λύσεις και πρωτόκολλα κρυπτογράφησης, όπως τα WEP, WPA, WPA2 και WPA2 με διαφορετικούς διακομιστές 802.1x RADIUS. Κάθε μία από τις λύσεις αυτές περιλαμβάνει διαφορετικές απαιτήσεις ασφαλείας με στόχο τη δημιουργία ενός ασφαλούς WLAN [93].

4.2.1 Πρωτόκολλο WEP

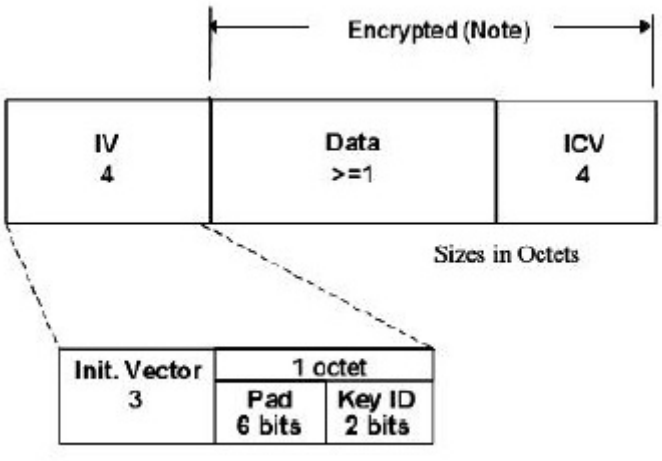
Το WEP (Wired Equivalent Privacy) αποτελεί ένα πρωτόκολλο κρυπτογράφησης που σχεδιάστηκε για το πρότυπο IEEE 802.11 με σκοπό να παρέχει εμπιστευτικότητα στα δεδομένα, που μεταδίδονται εντός ενός δικτύου WLAN, τέτοιου επιπέδου ώστε να είναι συγκρίσιμη με αυτή των ενσύρματων δικτύων LAN [91], [96].

Τα βασικά χαρακτηριστικά του πρωτοκόλλου WEP είναι η χρήση ενός μυστικού κλειδιού PSK μήκους 40bit, το οποίο ονομάζεται βασικό κλειδί ή προεπιλεγμένο κλειδί, ενός αλγόριθμου αθροίσματος ελέγχου (checksum) CRC-32 (Cyclic Redundancy Code), που χρησιμοποιείται ως μηχανισμός ακεραιότητας δεδομένων και του αλγόριθμου κρυπτογράφησης RC4. Το πρωτόκολλο υποστηρίζει έως και τέσσερα διαφορετικά βασικά κλειδιά, με αναγνωριστικά (Key ID) από 0 έως 3. Κάθε ένα από αυτά τα βασικά κλειδιά αποτελούν ομαδικά κλειδιά, δηλαδή μοιράζονται μεταξύ όλων των μελών ενός συγκεκριμένου ασύρματου δικτύου. Αυτό ήταν λιγότερο συνηθισμένο στα προϊόντα πρώτης γενιάς, καθώς συνεπάγεται την ύπαρξη μιας βασικής μονάδας διαχείρισης, την οποία το WEP δεν ορίζει [96].



Εικόνα 4.7: Διαδικασία κρυπτογράφησης πρωτοκόλλου WEP [97]

Η λειτουργία του πρωτοκόλλου είναι πολύ απλή, προσπαθώντας να ασφαλίσει τις μονάδες MPDU του πρωτοκόλλου MAC, οι οποίες αποτελούν τμήματα πακέτων 802.11 (Εικ. 4.7) [97]. Πριν την μετάδοση των πακέτων και για την προστασία τους μέσω κρυπτογράφησης, ο μηχανισμός CRC-32 του πρωτοκόλλου WEP υπολογίζει πρώτα μια τιμή αθροίσματος ελέγχου, την τιμή ICV (Integrity Check Value) των δεδομένων κάθε μονάδας MPDU. Στη συνέχεια, όπως φαίνεται στην εικόνα 4.8, η τιμή ICV προσαρτιέται στο τέλος των δεδομένων, αυξάνοντας το μήκος τους κατά τέσσερα byte. Η τιμή ICV επιτρέπει στον δέκτη να ανιχνεύσει εάν τα δεδομένα έχουν αλλοιωθεί κατά τη διάρκεια της μετάδοσης ή εάν το πακέτο που λαμβάνεται είναι πλαστό. Για την κρυπτογράφηση των δεδομένων, το πρωτόκολλο επιλέγει ένα βασικό κλειδί και ένα διάνυσμα IV (Initialization Vector), μήκους 24bit. Για κάθε πακέτο χρησιμοποιείται διαφορετικό κλειδί RC4, η δημιουργία του οποίου πραγματοποιείται μέσω της συνένωσης της τιμής IV και του επιλεγμένου κοινού βασικού κλειδιού. Η διαδικασία της κρυπτογράφησης αφορά τόσο τα πακέτα όσο και την τιμή ICV. Τελικά, το πλαίσιο που μεταδίδεται μέσω του πρωτοκόλλου WEP έχει τη μορφή της εικόνας 4.8. Όπως φαίνεται στην εικόνα, το διάνυσμα IV και το αναγνωριστικό κλειδιού (ID), που προσδιορίζουν το επιλεγμένο κλειδί, κωδικοποιούνται ως συμβολοσειρά τεσσάρων byte και προσαρτώνται στην αρχή των δεδομένων που μεταδίδονται [96]. Κατά τη λήψη, το εκάστοτε πλαίσιο αποκρυπτογραφείται, η τιμή του αθροίσματος ελέγχου επανυπολογίζεται και, στη συνέχεια, το αποτέλεσμα συγκρίνεται με την τιμή αθροίσματος ελέγχου που ελήφθη (ICV). Εάν οι δύο τιμές δεν είναι ίδιες, τότε, όπως αναφέρθηκε παραπάνω, το πλαίσιο που ελήφθη απορρίπτεται, επειδή θεωρείται ότι έχει τροποποιηθεί κατά τη μετάδοση [6].



Εικόνα 4.8: Διαμόρφωση μονάδας MPDU με χρήση πρωτοκόλλου WEP [96]

Το πρωτόκολλο WEP παρουσιάζει μια σειρά από αδυναμίες, όπως [97]:

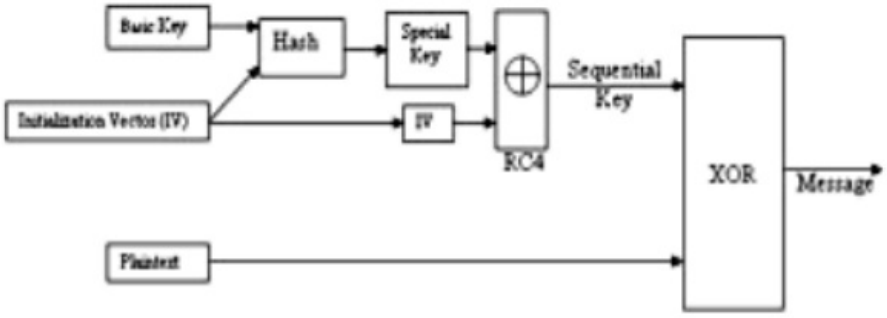
- χρησιμοποιεί αδύναμο αλγόριθμο κρυπτογράφησης (RC4) και μάλιστα χωρίς να τον εκμεταλλεύεται πλήρως
- χρησιμοποιεί κλειδιά κρυπτογράφησης μικρού μήκους
- δεν κρυπτογραφεί το διάνυσμα IV
- παρουσιάζει αδυναμία προσδιορισμού του τρόπου ρύθμισης ή αλλαγής του διανύσματος IV
- ο μηχανισμός ακεραιότητας CRC-32 του πρωτοκόλλου είναι επιρρεπής σε επιθέσεις αναστροφής bit και εντοπίζει μόνο τυχαία σφάλματα κατά τη μετάδοση των δεδομένων και όχι σκόπιμες τροποποιήσεις τους

Η εκμετάλλευση όλων αυτών των αδυναμιών του πρωτοκόλλου από κακόβουλες οντότητες δημιουργούν τις κατάλληλες βάσεις για την πραγματοποίηση απειλών κατά των δικτύων WLAN, όπως την ανίχνευση των κρυπτοκαλυμμένων πλαισίων δεδομένων για ανάλυση εκτός σύνδεσης με σκοπό την ανάκτηση του κλειδιού κρυπτογράφησης (κάτι που τελικά οδηγεί στην υποκλοπή των αρχικών απλών κειμένων), την ανακάλυψη των μερών επικοινωνίας και τους χρόνους στους οποίους επικοινωνούν, τον προσδιορισμό του περιεχομένου των επικοινωνιών, τον προσδιορισμό των λειτουργικών συστημάτων που χρησιμοποιούνται από τις ασύρματες συσκευές, καθώς επίσης και την επανάληψη των πλαισίων που είχαν καταγραφεί στο παρελθόν [6]. Σε μια προσπάθεια ενίσχυσης της ισχύος κρυπτογράφησης του πρωτοκόλλου WEP, σε πολλές περιπτώσεις πρακτικής εφαρμογής του, χρησιμοποιήθηκαν κλειδιά μεγέθους 128 και 256bit, κάτι που την βελτίωσε σε κάποιο βαθμό, όμως περιόρισε τη διαλειτουργικότητα των συσκευών [98].

4.2.2 Πρωτόκολλο TKIP

Με σκοπό την αντιμετώπιση των αδυναμιών που παρουσιάζει το πρωτόκολλο WEP, στην τροποποίηση IEEE 802.11i συμπεριλήφθηκε ένα νέο πρωτόκολλο ασφάλειας των δικτύων WLAN, το οποίο αφορούσε την προστασία της πρόσβασης στα δίκτυα Wi-Fi, ένας στόχος που έδωσε και το όνομα στο νέο αυτό πρωτόκολλο WPA (Wi-Fi Protected Access) [96]. Η δυνατότητα αντιμετώπισης των αδυναμιών του πρωτοκόλλου WEP από το WPA, βασίστηκε στο πρωτόκολλο κρυπτογράφησης TKIP (Temporal Key Integrity Protocol) που περιλαμβάνει. Τα χαρακτηριστικά του πρωτοκόλλου TKIP, όπως η λειτουργία ανάμιξης (ή κατακερματισμού) κλειδιών, ο έλεγχος ακεραιότητας μηνύματος, η υποστήριξη εκτεταμένου διανύσματος IV, ο μηχανισμός επαναφοράς κλειδιών, κλπ. δίνουν τη δυνατότητα στο WPA να βελτιώσει την ασφάλεια των υλοποιήσεων του πρωτοκόλλου

WEP χωρίς να προκαλεί σημαντική υποβάθμιση της απόδοσης των δικτύων WLAN, διατηρώντας παράλληλα τη διαλειτουργικότητα των ασύρματων συστημάτων, χωρίς να απαιτείται η προσθήκη ή τροποποίηση του υφιστάμενου εξοπλισμού των δικτύων, αλλά μόνο ενημερώσεις του λογισμικού τους [6], [96], [97].



Εικόνα 4.9: Διαδικασία κρυπτογράφησης πρωτοκόλλου TKIP [97]

Όπως φαίνεται στην εικόνα 4.9, όπου παρουσιάζεται η λειτουργία του πρωτοκόλλου TKIP, το πρωτόκολλο χρησιμοποιεί τον ίδιο αλγόριθμο κρυπτογράφησης RC4 με το WEP, με μόνη διαφορά ότι πριν τη χρήση του προηγείται μια λειτουργία ανάμιξης (ή κατακερματισμού) κλειδιών (mixing ή hushing function), με αποτέλεσμα τη δημιουργία ενός επαυξημένου αλγόριθμου RC4. Σε αυτή τη λειτουργία πραγματοποιείται μια ανάμιξη (κατακερματισμός) του βασικού κλειδιού και ένα αντίγραφο του διανύσματος IV. Το αποτέλεσμα αυτής της λειτουργίας δημιουργεί ένα ειδικό κλειδί ανά πακέτο, το οποίο στη συνέχεια ενώνεται με το κανονικό διάνυσμα IV, ο συνδυασμός των οποίων χρησιμοποιείται στον επαυξημένο αλγόριθμο RC4. Το διαδοχικό κλειδί (sequential key) που δημιουργείται με αυτόν τον τρόπο, χρησιμοποιείται για την κρυπτογράφηση του προς μετάδοση απλού κειμένου [99].

Η λειτουργία του πρωτοκόλλου TKIP βασίζεται στη χρήση του αλγόριθμου RC4 για την κρυπτογράφηση και στη χρήση του αλγόριθμου Michael, στον οποίο η εφαρμογή του κώδικα MIC (Message Integrity Code) αποσκοπεί στην προστασία της ακεραιότητας των μηνυμάτων. Μερικές από τις απειλές που προστατεύει ο συνδυασμός αυτών των δύο αλγορίθμων είναι η τροποποίηση της διεύθυνσης προορισμού σε επιθέσεις αναστροφής bit, η τροποποίηση της διεύθυνσης πηγής στις επιθέσεις πλαστοπροσωπίας, ο κατακερματισμό2 και η εικασία επαναληπτικού κλειδιού. Επίσης, η δυνατότητα του πρωτοκόλλου να δημιουργεί διαφορετικό κλειδί κρυπτογράφησης ανά πακέτο και η αντιστοίχιση κάθε πλαισίου με διαφορετικό διαδοχικό αριθμό σειράς, παρέχουν προστασία από επιθέσεις επανάληψης που είναι κοινές σε δίκτυα WLAN που βασίζονται στη χρήση του πρωτοκόλλου WEP. Το πρωτόκολλο TKIP εφαρμόζει επίσης ορισμένα αντίμετρα κάθε φορά που μια ασύρματη συσκευή ή ένα σημείο AP αντιμετωπίζει τη λήψη ενός πλαισίου με σφάλμα κωδικού MIC, για να αποτρέψει πιθανή ενεργή επίθεση. Παρά το γεγονός, ότι το πρωτόκολλο TKIP σχεδιάστηκε για να αντιμετωπίσει τις αδυναμίες του WEP, η χρήση του αλγόριθμου κρυπτογράφησης RC4, δεν το καθιστά και την καλύτερη λύση για συστήματα με μεγάλες ανάγκες ασφαλείας [100].

4.2.3 Πρωτόκολλο CCMP

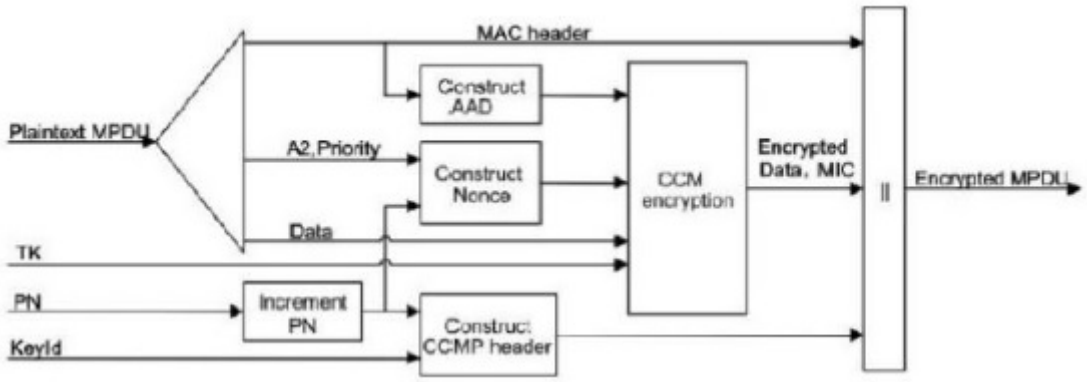
Το CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) αποτελεί ένα πρωτόκολλο κρυπτογράφησης που σχεδιάστηκε για να βελτιώνει την απόδοση ασφάλειας των δικτύων WLAN αντιμετωπίζοντας τις ανεπάρκειες των WEP και TKIP. Το πρωτόκολλο αποτελεί

επίσης την καρδιά του πρωτοκόλλου WAP2, που όπως υποδεικνύεται και από το όνομά του είναι η δεύτερη, πιο καινούργια, έκδοση του WAP [96]. Ωστόσο, σε αντίθεση με το πρωτόκολλο TKIP, το CCMP δεν υποστήριζε τη διαλειτουργικότητα, με αποτέλεσμα να απαιτεί τροποποίηση της υλοποίησης των δικτύων που βασίζονταν στα WEP ή TKIP [101].

Η ισχυρή προστασία κρυπτογράφησης που παρουσιάζει το πρωτόκολλο CCMP βασίζεται στο πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard), το οποίο θεωρείται μια από τις καλύτερες προδιαγραφές κρυπτογράφησης δεδομένων, και πιο συγκεκριμένα σε δύο βασικές του λειτουργίες [96]:

- τη λειτουργία CTR (Counter mode), για την κρυπτογράφηση των δεδομένων, και
- τη λειτουργία CBC-MAC (Cipher Block Chaining Message Authentication), τόσο για έλεγχο ταυτότητας όσο και προστασία της ακεραιότητας των δεδομένων

Βασιζόμενο σε αυτές τις δύο λειτουργίες, το CCMP προστατεύει την ακεραιότητα τόσο των δεδομένων πλαισίου όσο και των τμημάτων της κεφαλίδας πλαισίου IEEE 802.11. Η επιτυχία του πρωτοκόλλου στην αντιμετώπιση των επιθέσεων επανάληψης, οφείλεται στη χρήση κλειδιών μεγέθους 128bit για κρυπτογράφηση και ενός αριθμού πακέτου (PN) των 48bit, μέσω των οποίων δημιουργεί nonce. Στην κρυπτογραφία, ένα nonce είναι ένας αυθαίρετος αριθμός που μπορεί να χρησιμοποιηθεί μόνο μία φορά σε μια κρυπτογραφική επικοινωνία. Ως εκ τούτου, η κατασκευή του nonce επιτρέπει τη χρήση ενός μόνο κλειδιού για την προστασία της ακεραιότητας, αλλά και της εμπιστευτικότητας των δεδομένων χωρίς να υπάρχει ο φόβος παραβίασής του [6]. Για πολλούς ερευνητές, η χρήση του πρωτοκόλλου CCMP παρουσιάζει τόσο μεγάλη ασφάλεια για τα δίκτυα WLAN, που μπορεί να χρησιμοποιηθεί ακόμη και σε περιπτώσεις προστασίας κυβερνητικών δεδομένων [96]. Η λειτουργία του πρωτοκόλλου παρουσιάζεται στην εικόνα 4.10 [97].



Εικόνα 4.10: Διαδικασία κρυπτογράφησης πρωτοκόλλου CCMP [97]

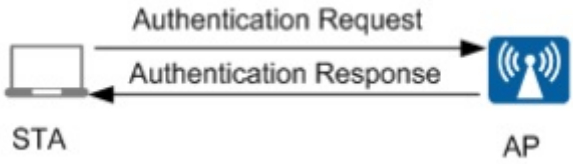
4.3 Πρωτόκολλα και μηχανισμοί ελέγχου ταυτότητας δικτύων WLAN

Η ανάπτυξη ενός ασφαλούς μηχανισμού ελέγχου ταυτότητας που να πληροί όλες τις απαιτήσεις ασφαλείας των δικτύων WLAN είναι μεγάλης ζωτικής σημασίας. Το αρχικό πρότυπο IEEE 802.11 περιλάμβανε μόνο δύο μηχανισμούς ελέγχου της ταυτότητας των συσκευών που προσπαθούσαν να αποκτήσουν πρόσβαση στο δίκτυο WLAN. Ο πρώτος μηχανισμός ήταν ο έλεγχος ταυτότητας OSA και ο έλεγχος ταυτότητας PSK, με τον δεύτερο να είναι προαιρετικός [24]. Με τη βελτίωση της ασφάλειας που παρουσιάστηκε σε επόμενες τροποποιήσεις του IEEE 802.11, πιο ασφαλείς προσεγγίσεις ελέγχου ταυτότητας και ελέγχου πρόσβασης ενσωματώθηκαν ως εναλλακτικές λύσεις σε αυτούς τους δύο μηχανισμούς. Οι λύσεις αυτές αφορούν το πρωτόκολλο ελέγχου ταυτότητας EAP, τα

captive portal και τα διαπιστευτήρια ελέγχου ταυτότητας και ελέγχου πρόσβασης [6], [75]. Όλοι αυτοί οι μηχανισμοί ελέγχου ταυτότητας των δικτύων WLAN θα αποτελέσουν το αντικείμενο της παρούσας ενότητας.

4.3.1 Έλεγχος ταυτότητας OSA

Ο μηχανισμός ελέγχου ταυτότητας OSA (Open System Authentication) χρησιμοποιείται πριν από τη διαδικασία σύνδεσης μιας ασύρματης συσκευής με ένα σημείο AP και πραγματοποιείται με σκοπό την απόκτηση πρόσβασης της συσκευής σε ένα δίκτυο WLAN που χρησιμοποιεί το πρωτόκολλο κρυπτογράφησης WEP. Μέσω του μηχανισμού OSA, οποιαδήποτε ασύρματη συσκευή μπορεί να αποκτήσει πρόσβαση στο δίκτυο WLAN WEP και να ανταλλάξει αρχεία, τα οποία δεν είναι κρυπτογραφημένα. Η πραγματοποίηση της ασφαλούς σύνδεσης στην περίπτωση του μηχανισμού OSA επιτυγχάνεται μέσω της χρήσης του αναγνωριστικού SSID (Service Set Identifier) του σημείου AP και της διεύθυνσης MAC της συσκευής [102]. Από τη στιγμή, όμως, που τα σημεία AP εκπέμπουν τα αναγνωριστικά SSID τους σε απλό κείμενο, η καταγραφή τους μπορεί να πραγματοποιηθεί από οποιαδήποτε ασύρματη συσκευή, κάτι που σημαίνει ότι ο μηχανισμός δεν περιλαμβάνει κάποιο ουσιαστικό στοιχείο απόδειξης της ταυτότητας της συσκευής. Επομένως, κατά τον μηχανισμό OSA δεν πραγματοποιείται κάποιος ουσιαστικός έλεγχος ταυτότητας της συσκευής και οποιαδήποτε συσκευή μπορεί να συνδεθεί σε οποιοδήποτε σημείο AP του δικτύου, ανταλλάσσοντας δεδομένα, αρκεί να βρίσκεται εντός της εμβέλειας του σημείου AP (Εικ. 4.11). Ο μηχανισμός OSA χρησιμοποιήθηκε επομένως σε συστήματα που δεν περιλάμβαναν κάποιο μηχανισμό διαχείρισης της ασφάλειας του δικτύου, όπως για παράδειγμα τα δημόσια δίκτυα Wi-Fi [103], [104].



Εικόνα 4.11: Μηχανισμός ελέγχου ταυτότητας OSA [104]

Από τα παραπάνω προκύπτει το συμπέρασμα ότι τελικά ο μηχανισμός ελέγχου ταυτότητας που χρησιμοποιήθηκε στο πρότυπο IEEE 802.11 μέσω της υλοποίησης του OSA, αφορούσε τον έλεγχο πρόσβασης των ασύρματων συσκευών μόνο μέσω των διευθύνσεων MAC τους. Σε αυτό τον έλεγχο, οι διαχειριστές του δικτύου πρόσθεταν στη μνήμη του εκάστοτε σημείου AP μια λίστα με τις εξουσιοδοτημένες διευθύνσεις MAC, έτσι ώστε το σημείο AP να επιτρέπει την πρόσβαση στους πόρους του δικτύου WLAN μόνο στις συσκευές των οποίων οι διευθύνσεις MAC υπάρχουν σε αυτή τη λίστα [104], [105].

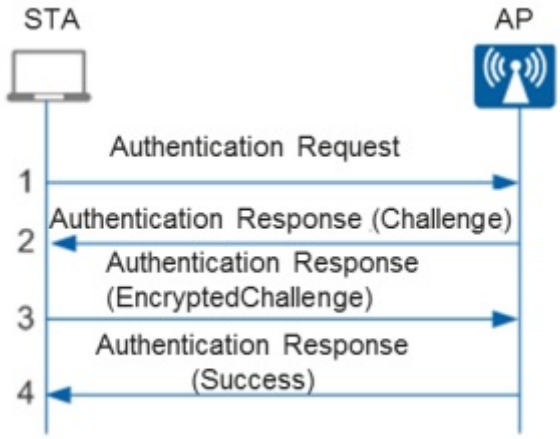
Μια σημαντική αδυναμία αυτής της μεθόδου είναι ότι οι διευθύνσεις MAC των συσκευών δεν ήταν κρυπτογραφημένες. Με τον τρόπο αυτό, οποιοσδήποτε επιτιθέμενος θα μπορούσε να ρυθμίσει μια κακόβουλη ασύρματη συσκευή σε λειτουργία παρακολούθησης για να υποκλέψει την κυκλοφορία δεδομένων των νόμιμων συσκευών που συνδέονται στο δίκτυο WLAN και κατά συνέπεια να είναι σε θέση να δημιουργήσει μια διεύθυνση MAC που να μπορεί να γίνει αποδεχτή από το σημείο AP. Έτσι, μόλις οι διαχειριστές του δικτύου καθορίσουν τις επιτρεπόμενες διευθύνσεις MAC, ο επιτιθέμενος είναι σε θέση να δώσει στην κακόβουλη συσκευή μία από αυτές, ώστε να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο δίκτυο. Εφόσον ο μηχανισμός OSA δεν επαληθεύει με άλλο τρόπο

την ταυτότητα της συσκευής, της δίνεται η δυνατότητα συσχέτισης με ένα κακόβουλο σημείο που έχει οριστεί στο αναγνωριστικό SSID του νόμιμου σημείου AP [105].

4.3.2 Έλεγχος ταυτότητας PSK

Ο μηχανισμός ελέγχου ταυτότητας PSK βασίζεται σε κρυπτογραφικές προσεγγίσεις μυστικού κλειδιού, όπου ένα μυστικό κλειδί μοιράζεται μεταξύ των νόμιμων ασύρματων συσκευών και του σημείου AP. Ο μηχανισμός εφαρμόζει ένα σχήμα πρόκλησης-απόκρισης που έχει σκοπό να αποδείξει ότι η συσκευή που προσπαθεί να αποκτήσει πρόσβαση σε ένα συγκεκριμένο δίκτυο WLAN γνωρίζει το μυστικό κλειδί [106].

Η διαδικασία ξεκινάει από τη συσκευή με την αποστολή ενός αιτήματος ελέγχου ταυτότητας προς το σημείο AP (Εικ. 4.12). Το σημείο AP δημιουργεί μια τυχαία λέξη μήκους 128bit, που ονομάζεται πρόκληση, και τη στέλνει στη συσκευή. Σε περίπτωση που η συσκευή είναι νόμιμη, είναι σε θέση να κρυπτογραφήσει αυτήν την πρόκληση χρησιμοποιώντας το κλειδί PSK, το οποίο γνωρίζει εκ των προτέρων. Μετά την κρυπτογράφηση της λέξης, η συσκευή επιστρέφει το αποτέλεσμα της κρυπτογράφησης στο σημείο AP ως απόκριση. Κατά τη λήψη της απόκρισης από τη συσκευή, το σημείο AP την αποκρυπτογραφεί χρησιμοποιώντας το ίδιο κλειδί με αυτό που αναμένεται να έχει χρησιμοποιηθεί από τη συσκευή. Η απόκτηση πρόσβασης στο δίκτυο WLAN επιτρέπεται μόνο εάν η τιμή της διαδικασίας της αποκρυπτογράφησης είναι ίδια με την πρόκληση που στάλθηκε από το σημείο AP [104].



Εικόνα 4.12: Μηχανισμός ελέγχου ταυτότητας PSK [104]

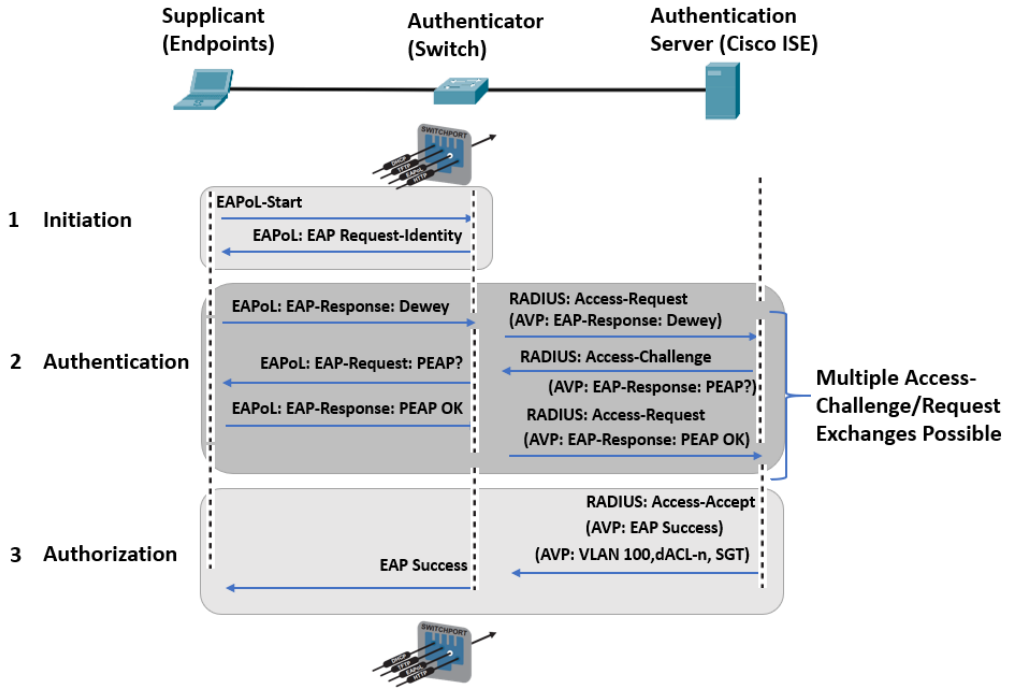
Στα περισσότερα αναπτύγματα μεγάλων δημόσιων δικτύων WLAN, όπως αυτά των πανεπιστημίων, ο μηχανισμός PSK δεν προτιμάται, λόγω της δυσκολίας διαχείρισης της ασφάλειας των μη αυτόματα κατανεμημένων κλειδιών PSK σε μεγάλο αριθμό συσκευών [75].

Παρά το γεγονός ότι ο σχεδιασμός του μηχανισμού ελέγχου ταυτότητας PSK θεωρείται πιο ισχυρός από τον OSA, όπως έχει ήδη αναφερθεί σε προηγούμενη ενότητα, παρουσιάζει διάφορα τρωτά σημεία, τα οποία μπορούν να χρησιμοποιηθούν σε επιθέσεις κατά της ασφάλειας των δικτύων WLAN. Καθώς ο μηχανισμός υποστηρίζει μόνο την επαλήθευση της ταυτότητας της συσκευής από το σημείο AP, αλλά όχι το αντίστροφο, ο επιτιθέμενος μπορεί να δημιουργήσει ένα κακόβουλο σημείο AP που να προσποιείται ότι ο έλεγχος ταυτότητας ήταν επιτυχής ακόμη και χωρίς να γνωρίζει το μυστικό κλειδί [108]. Επίσης επειδή τα σημεία AP δεν μπορούν να αναγνωρίσουν τα άτομα που χρησιμοποιούν το δίκτυο WLAN, οι χρήστες των ασύρματων συσκευών, που ταυτοποιήθηκαν μέσω

του μηχανισμού PSK, παραμένουν ουσιαστικά ανώνυμοι [6]. Τέλος, το πρωτόκολλο CHAP (Challenge Handshake Protocol) που χρησιμοποιείται για την κρυπτογράφηση της πρόκλησης παρουσιάζει τρωτά σημεία τα οποία είναι γνωστά από τους επιτιθέμενους. Τα σημεία αυτά μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους με σκοπό την ανάκτηση των αδύναμων PSK κλειδιών. Για το λόγο αυτό, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν εργαλεία ανάκτησης κωδικού πρόσβασης, cracker και sniffer, όπως τα Cain και Abel [75].

4.3.3 Πρωτόκολλο ελέγχου ταυτότητας EAP

Έχοντας ως στόχο να καλύψει τις οποίες ευπάθειες παρουσιάζουν τα δίκτυα WLAN, ο οργανισμός IEEE αποφάσισε να δημιουργήσει ένα πρότυπο, το IEEE 802.1i, που να ορίζει την αρχιτεκτονική ασφαλείας των συγκεκριμένων δικτύων. Το πρότυπο IEEE 802.1i περιγράφει την ευέλικτη ιεραρχία των κλειδιών, αλλά και τον τρόπο ανταλλαγής τους μεταξύ των πελατών (ασύρματων συσκευών) και ενός διακομιστή, που ονομάζεται διακομιστής ελέγχου ταυτότητας. Στο πρότυπο IEEE 802.1i καθορίστηκε επίσης η χρήση της αρχιτεκτονικής IEEE 802.1x, στην οποία περιγράφεται ένα αξιόπιστο και ασφαλές πλαίσιο ελέγχου ταυτότητας, το οποίο είναι σε θέση να υποστηρίξει την ασφαλής σύνδεση μεταξύ των πελατών και του διακομιστή ελέγχου ταυτότητας. Σύμφωνα με την αρχιτεκτονική IEEE 802.1x, σε ένα περιβάλλον WLAN IEEE 802.11, η σύνδεση μεταξύ των πελατών και του διακομιστή ελέγχου ταυτότητας μπορεί να είναι απευθείας ή μέσω ενός σημείου AP, το οποίο παίζει το ρόλο του authenticator [109].



Εικόνα 4.13: Παράδειγμα ανταλλαγής μηνυμάτων διαδικασίας ελέγχου ταυτότητας σύμφωνα με την αρχιτεκτονική IEEE 802.1x και τη χρήση του πρωτοκόλλου EAP [109]

Ο ρόλος του πρωτοκόλλου EAP στη διαδικασία που ορίζεται από την αρχιτεκτονική IEEE 802.1x είναι να παρέχει μια ευέλικτη και αξιόπιστη βάση πάνω στην οποία διάφοροι μηχανισμοί ελέγχου ταυτότητας μπορούν να εκτελεστούν. Στην εικόνα 4.13 παρουσιάζεται ένα παράδειγμα ανταλλαγής μηνυμάτων μεταξύ των συμμετεχόντων στη διαδικασία ελέγχου ταυτότητας, με βάση τη χρήση του πρωτοκόλλου EAP [109]. Σε αυτήν την περίπτωση, μία ασύρματη συσκευή (πελάτης) θέλει να αποκτήσει πρόσβαση στο δίκτυο WLAN. Αν και αυτή η πρόσβαση μπορεί να ενεργοποιηθεί μόνο από

το σημείο AP (authenticator), η αποδοχή του αιτήματος του πελάτη δεν μπορεί να πραγματοποιηθεί αν δεν γίνει πρώτα έλεγχος της ταυτότητάς του. Για το λόγο αυτό, το σημείο AP προωθεί τα μηνύματα πρωτοκόλλου EAP του αιτούντος την πρόσβαση προς τον διακομιστή ελέγχου ταυτότητας. Μετά την ολοκλήρωση της διαδικασίας του ελέγχου ταυτότητας, ο διακομιστής ενημερώνει τον authenticator σχετικά με το αποτέλεσμα. Εάν ο έλεγχος ταυτότητας είναι επιτυχής, ο authenticator δίνει στον πελάτη πρόσβαση στο δίκτυο WLAN [81].

Με τη χρήση του EAP ένα σημείο AP προωθεί μηνύματα ελέγχου ταυτότητας μεταξύ του πελάτη και του διακομιστή ελέγχου ταυτότητας. Το EAP χρησιμοποιείται επίσης για να επιτρέψει τόσο στη συσκευή όσο και στον διακομιστή ελέγχου ταυτότητας να συμφωνήσουν και να διανείμουν μεταξύ τους υλικό κρυπτογράφησης το οποίο μπορεί να δημιουργηθεί από τον διακομιστή ελέγχου ταυτότητας. Το πρωτόκολλο RADIUS συνεργάζεται με το EAP για τη μεταφορά των μηνυμάτων ελέγχου ταυτότητας και διανομής κλειδιών [6].

Επομένως, το πρωτόκολλο EAP αποτελεί ένα πλαίσιο, παρά έναν μηχανισμό, ελέγχου ταυτότητας, το οποίο παρέχει ορισμένες κοινές λειτουργίες και τρόπους διαπραγμάτευσης σε μεθόδους ελέγχου ταυτότητας, που ονομάζονται μέθοδοι EAP [110]. Το EAP είναι σε θέση να υποστηρίζει μια μεγάλη ποικιλία μεθόδων ελέγχου ταυτότητας, οι οποίοι βασίζονται σε διάφορα κριτήρια, όπως διαπιστευτήρια (credentials), μόνιμους κωδικούς πρόσβασης, πιστοποιητικά, μυστικά κλειδιά, κωδικούς πρόσβασης μιας χρήσης, κλπ., ή συνδυασμό τους. Το πλαίσιο EAP που αναπτύσσεται σε μια υλοποίηση δικτύου WLAN επηρεάζει την ασφάλειά του, καθώς, εκτός από τον έλεγχο ταυτότητας, οι μέθοδοι EAP δημιουργούν επίσης το βασικό υλικό που χρησιμοποιείται για την προστασία των επόμενων επικοινωνιών [6]. Επί του παρόντος, 40 περίπου διαφορετικές μέθοδοι EAP έχουν οριστεί σε αναφορές RFC του οργανισμού IETF [110]. Πιο συγκεκριμένα, για τα δίκτυα WLAN οι μέθοδοι EAP που χρησιμοποιούνται για έλεγχο ταυτότητας περιγράφονται στην αναφορά RFC 4017 [109]. Στη συνέχεια αναφέρονται οι πιο συνηθισμένες σύγχρονες μέθοδοι EAP που μπορούν να λειτουργήσουν σε δίκτυα WLAN [6], [109], [111]:

- ***Μέθοδος LEAP***: Είναι ένα πρωτόκολλο ελέγχου ταυτότητας που αναπτύχθηκε από τη Cisco και ενσωματώθηκε σε πολλές συσκευές WLAN για τον έλεγχο ταυτότητας μόνο των ασύρματων συσκευών της συγκεκριμένης εταιρίας. Η μέθοδος προσφέρει υποστήριξη για αμοιβαίο έλεγχο ταυτότητας και αλλάζει δυναμικά τα κλειδιά κάθε φορά που υπάρχει ανάγκη για εκ νέου έλεγχο ταυτότητας με σκοπό την ενίσχυση της ασφάλειάς της. Στην ουσία, η μέθοδος LEAP αποτελεί μια τροποποιημένη έκδοση του MS-CHAP και δεν θα πρέπει πλέον να χρησιμοποιείται λόγω γνωστών ελαττωμάτων ασφαλείας
- ***Μέθοδος EAP-TLS (EAP with Transport Layer Security)***: Είναι ένας αμοιβαίος μηχανισμός ελέγχου ταυτότητας που χρησιμοποιεί ψηφιακά πιστοποιητικά πελάτη και διακομιστή X.509, ως διαπιστευτήρια ελέγχου ταυτότητας. Παρά το γεγονός, ότι το EAP-TLS απαιτεί περισσότερη προσπάθεια διαμόρφωσης από την πλευρά του πελάτη σε σύγκριση με άλλες μεθόδους EAP, θεωρείται η μέθοδος EAP που παρέχει την μεγαλύτερη ασφάλεια στα δίκτυα WLAN, τα οποία μπορεί να προστατέψει από επιθέσεις DoS, MITM και λεξικού. Η ασφάλεια που παρέχει έχει φυσικά και το κόστος της καθώς απαιτείται ανταλλαγή μεγάλου αριθμού μηνυμάτων, στα οποία η επιβάρυνση είναι αρκετά υψηλή
- ***Μέθοδος EAP-TTLS (EAP with Tunneled TLS)***: Πρόκειται για μια παραλλαγή της μεθόδου EAP-TLS που μπορεί να εφαρμοστεί στην αρχιτεκτονική IEEE 802.1x, στην οποία η έννοια της σήραγγας (tunnel) χρησιμοποιείται για να δείξει την κρυπτογραφημένη σύνδεση μεταξύ του πελάτη και του διακομιστή, την οποία εκμεταλλεύεται ο πελάτης για να επαληθεύσει την ταυτότητά του, στέλνοντας τον κωδικό πρόσβασης του. Σε αντίθεση με τη μέθοδο EAP-TLS,

ενώ η χρήση πιστοποιητικών διακομιστή είναι υποχρεωτική, αυτή των πιστοποιητικών πελάτη είναι προαιρετική, με αποτέλεσμα οι πελάτες να μπορούν να χρησιμοποιούν παλαιότερες μεθόδους ελέγχου ταυτότητας, όπως τα διαπιστευτήρια. Έτσι, καθώς στη μέθοδο EAP TTLS ο έλεγχος της ταυτότητας του πελάτη δεν πραγματοποιείται μέσω χρήσης κάποιου πιστοποιητικού, το δίκτυο WLAN δεν είναι αναγκασμένο να παρουσιάζει πολύπλοκες υποδομές δημιουργίας κάποιου δημόσιου κλειδιού. Παρόλα αυτά, παρέχει αρκετά ισχυρή ασφάλεια, η οποία προστατεύει από επιθέσεις DoS και λεξικού, αλλά όχι από επιθέσεις MITM. Επίσης, για την υλοποίηση της μεθόδου απαιτείται ανταλλαγή μεγάλου αριθμού μηνυμάτων

- ***Μέθοδος EAP-FAST (EAP with Flexible Authentication via Secure Tunneling)***: Αποτελεί μια μέθοδο EAP, η οποία αναπτύχθηκε από τη Cisco ως διάδοχο της μεθόδου LEAP, με στόχο τη δημιουργία μιας μεθόδου που να βασίζεται στο TLS. Η μέθοδος αποτελείται από δύο φάσεις. Στην πρώτη πραγματοποιείται επικοινωνία TLS μεταξύ πελάτη και διακομιστή ελέγχου ταυτότητας με αμφίδρομη ταυτοποίηση, ενώ στη δεύτερη πραγματοποιείται έλεγχος ταυτότητας EAP με χρήση της μεταξύ τους κρυπτογραφημένης σύνδεσης TLS (tunnel)
- ***Μέθοδος EAP-MD5 (EAP with Message Digest 5)***: Αποτελεί μια μέθοδο EAP στην οποία το πρωτόκολλο CHAP συνδυάζεται με τη συνάρτηση κατακερματισμού MD5 για τον έλεγχο ταυτότητας του πελάτη. Ωστόσο, η ασφάλεια ασύρματου δικτύου που παρέχεται από αυτή τη μέθοδο EAP στις περισσότερες περιπτώσεις είναι ακατάλληλη
- ***Μέθοδος PEAP (Protected EAP)***: Είναι μέθοδος η οποία χρησιμοποιεί επίσης μόνο πιστοποιητικά διακομιστή για τον έλεγχο της ταυτότητάς του, ενώ ο έλεγχος της ταυτότητας του πελάτη αφήνεται να πραγματοποιηθεί από άλλες μεθόδους, όπως το EAP-TTLS. Η συγκεκριμένη μέθοδος δεν είναι συμβατή με μεθόδους και πλατφόρμες παλαιού τύπου με τις οποίες είναι συμβατή η EAP-TTLS
- ***Μέθοδος EAP-SIM (EAP for GSM Subscriber Identity Modules)***: Είναι μια μέθοδος EAP που υλοποιείται με χρήση της κάρτας SIM δικτύου 2G GSM. Σε αυτή τη μέθοδο, το ρόλο του διακομιστή ελέγχου ταυτότητας παίζει το κέντρο ελέγχου ταυτότητας GSM AuC (Authentication Center), ενώ ο πελάτης θα πρέπει να είναι εφοδιασμένος απαιτεί με κάρτα SIM εξοπλισμένη με αλγόριθμους A3 και A8. Το EAP-SIM αντιμετωπίζει δύο αδυναμίες των προδιαγραφών GSM, όπως είναι το μικρός μήκος κλειδιού κρυπτογράφησης (μόνο 64bit) και το γεγονός ότι το δίκτυο GSM δεν πιστοποιείται στον πελάτη
- ***Μέθοδος EAP-AKA (EAP with Authentication and Key Agreement)***: Αποτελεί μια παρόμοια μέθοδο με την EAP-SIM με μόνη διαφορά ότι το δίκτυο που χρησιμοποιείται εδώ είναι το 3G UMTS, πράγμα που σημαίνει και χρήση από τους πελάτης διαφορετικής κάρτας (USIM). Καθώς, το δίκτυο UMTS δεν παρουσιάζει τις αδυναμίες του GSM, η συγκεκριμένη μέθοδος δεν απαιτεί ιδιαίτερη τροποποίηση της βασικής μεθόδου EAP

Σε γενικές γραμμές, οι μέθοδοι EAP μπορούν να ταξινομηθούν σε τρεις διαφορετικές βασικές κατηγορίες με βάση τις προσεγγίσεις ελέγχου ταυτότητας που ακολουθούν [6], [109]: (α) βασικές μέθοδοι EAP, (β) μέθοδοι EAP που βασίζονται στη χρήση πιστοποιητικού και (γ) μέθοδοι EAP που βασίζονται στη χρήση κρυπτογραφημένης σύνδεσης. Οι μέθοδοι EAP που ανήκουν στη βασική κατηγορία βασίζονται σε προσεγγίσεις ελέγχου ταυτότητας παλαιού τύπου, όπως είναι η χρήση διαπιστευτηρίων (όνομα χρήστη και κωδικός πρόσβασης) ή η χρήση κάποιου κρυφού κλειδιού. Αυτές οι μέθοδοι ορίζονται από τις αναφορές RFC 3748 και RFC 1994 και η απόδειξη της νομιμότητας του διακομιστή ελέγχου ταυτότητας και της ασύρματης συσκευής πραγματοποιείται μέσω της δημιουργίας μεταξύ τους αμοιβαίας εμπιστοσύνης. Μια τέτοια εμπιστοσύνη προκύπτει από το γεγονός ότι και τα δύο μέρη γνωρίζουν ένα κοινό μυστικό (τα διαπιστευτήρια του χρήστη ή το κρυφό κλειδί) [6], [109]. Σε αυτήν την κατηγορία περιλαμβάνονται μέθοδοι όπως οι LEAP και EAP-SRP (EAP with

Secure Remote Password). Παρά την ευρεία χρήση της μεθόδου LEAP, η απόδειξη της εμφάνισης ευπαθειών και τρωτών σημείων που το εκθέτουν σε επιθέσεις λεξικού, οδήγησε στην ανάπτυξη της μεθόδου EAP-SRP, η λειτουργία της οποίας βασίζεται στη χρήση προσωρινών ασύμμετρων κλειδιών που δημιουργούνται από ένα κοινό συμμετρικό κλειδί [6].

Στη δεύτερη κατηγορία ανήκουν μέθοδοι EAP όπου ο διακομιστής ελέγχου ταυτότητας και η συσκευή δημιουργούν αμοιβαία εμπιστοσύνη μέσω της χρήσης πιστοποιητικών. Τα πιστοποιητικά αυτά, υπογράφονται από αρχές έκδοσης πιστοποιητικών CA (Certificate Authorities) χρησιμοποιώντας δικό τους (ιδιωτικό) κλειδί, έτσι ώστε μια συσκευή να μπορεί να επαληθεύσει την εγκυρότητα του πιστοποιητικού χρησιμοποιώντας το δημόσιο κλειδί της. Στην περίπτωση αυτή, κάθε συσκευή θεωρείται ότι διαθέτει, εκ των προτέρων, ένα αντίγραφο του δημόσιου κλειδιού της αρχής CA, το οποίο μπορεί να χρησιμοποιήσει για την επικύρωση των πιστοποιητικών. Οι μέθοδοι EAP που βασίζονται στη χρήση πιστοποιητικού είναι δύσκολο να εφαρμοστούν λόγω των απαιτήσεων των αρχών CA. Η μέθοδος EAP-TLS θεωρείται ως μία από τις πλέον δημοφιλείς μεθόδους αυτής της κατηγορίας [6], [112].

Στην τρίτη κατηγορία μεθόδων EAP, που βασίζονται στη χρήση κρυπτογραφημένης σύνδεσης, ανήκουν μέθοδοι των οποίων η διαδικασία ελέγχου ταυτότητας πραγματοποιείται σε δύο φάσεις. Στην πρώτη φάση, ο πελάτης αρχικά επαληθεύει την ταυτότητα του διακομιστή ελέγχου ταυτότητας χρησιμοποιώντας διαπιστευτήρια πιστοποιητικού που παρέχονται από τον διακομιστή και στη συνέχεια δημιουργεί ένα κλειδί συνεδρίας που χρησιμοποιείται για τη δημιουργία της κρυπτογραφημένης σύνδεσης και επικοινωνίας με τον διακομιστή. Στη δεύτερη φάση, ο διακομιστής ελέγχου ταυτότητας επαληθεύει τον πελάτη μέσω αυτής της κρυπτογραφημένης σύνδεσης [113]. Οι σημαντικότερες μέθοδοι EAP αυτής της κατηγορίας είναι οι PEAP και EAP-TTLS, οι οποίες παρά την ασφάλεια που παρέχουν, παρουσιάζουν τρωτά σημεία τα οποία μπορούν να χρησιμοποιηθούν σε επιθέσεις MITM. Οι ευπάθειες αυτές αφορούν περισσότερο τις συσκευές που χρησιμοποιούν λειτουργικό σύστημα και λογισμικό παλαιότερων εκδόσεων, τα οποία ενδέχεται να μην μπορούν να εκτελέσουν έλεγχο ταυτότητας EAP-TLS, με αποτέλεσμα η μέθοδος EAP-TTLS να τους επιτρέπει τη μη δημιουργία κρυπτογραφημένης σύνδεσης. Αυτή η ευπάθεια μπορεί να γίνει αντικείμενο εκμετάλλευσης από τους επιτιθέμενος για την πραγματοποίηση επίθεσης MITM μέσω της οποίας μπορεί να υποκλέψει τη συνεδρία της νόμιμης συσκευής [6]. Παρόλα αυτά, μελέτες έχουν δείξει ότι οι μέθοδοι EAP-TTLS και PEAP προσφέρουν ασφάλεια παρόμοια με αυτή της μεθόδου EAP-TLS, ξεπερνώντας παράλληλα τη δυσκολία που παρουσιάζει αυτή ως προς την απαίτηση κατοχής από τον πελάτη πιστοποιητικών που έχουν εκδοθεί από αρχή CA που εμπιστεύεται ο διακομιστής ελέγχου ταυτότητας. Επιπλέον, η μέθοδος EAP-TTLS παρέχει υποστήριξη για υπάρχοντες διακομιστές RADIUS παλαιού τύπου για τον έλεγχο ταυτότητας των συσκευών. Αυτό επιτυγχάνεται με την εισαγωγή ενός διακομιστή RADIUS/EAP-TTLS μεταξύ των σημείων AP και του διακομιστή RADIUS [114]. Τέλος, ενώ οι περισσότερες από τις μεθόδους EAP υποστηρίζουν μόνο έναν συγκεκριμένο τρόπο ελέγχου ταυτότητας για προστασία από ορισμένους τύπους επιθέσεων, οι μέθοδοι που ανήκουν σε αυτήν την τρίτη κατηγορία μπορούν να υποστηρίξουν συνδυασμό τρόπων ελέγχου ταυτότητας ώστε να είναι σε θέση να αντιμετωπίζουν μεγαλύτερη γκάμα τύπων επιθέσεων [6].

Οι μέθοδοι EAP επίσης είναι σε θέση να υποστηρίξουν μια μεγάλη ποικιλία διαφορετικών τύπων διαμόρφωσης των μονάδων που εμπλέκονται σε μια διαδικασία ελέγχου ταυτότητας. Για παράδειγμα, μπορεί να υπάρξει περίπτωση ο έλεγχος ταυτότητας μεταξύ της συσκευής και του διακομιστή ελέγχου ταυτότητας να είναι αμοιβαίος, αλλά όχι απαραίτητα συμμετρικός. Σε μια τέτοια περίπτωση, ο διακομιστής ελέγχου ταυτότητας μπορεί να ταυτοποιηθεί από τη συσκευή μέσω χρήσης

πιστοποιητικού, ενώ η ταυτοποίησης της συσκευής από το διακομιστή ελέγχου ταυτότητας να πραγματοποιηθεί μέσω χρήση βιομετρικών πληροφοριών. Σε όλες αυτές τις περιπτώσεις, η φύση του ελέγχου ταυτότητας εξαρτάται από τη μέθοδο EAP που χρησιμοποιείται. Επίσης, ορισμένες μέθοδοι EAP υποστηρίζουν αμοιβαίο έλεγχο ταυτότητας, ενώ άλλες όχι [6].

Όπως αναφέρθηκε στην αρχή της ενότητας, μια τυπική υλοποίηση του πλαισίου EAP απαιτεί την ύπαρξη τριών ξεχωριστών οντοτήτων, δηλαδή την ασύρματη συσκευή (πελάτη), το σημείο AP (authenticator) και τον διακομιστή ελέγχου ταυτότητας. Ωστόσο, το πλαίσιο EAP υποστηρίζεται επίσης μια άλλη προσέγγιση όπου οι οντότητες του authenticator και του διακομιστή ελέγχου ταυτότητας ενσωματώνονται σε μία. Για να υποστηριχθεί μια τέτοια προσέγγιση, ο κόμβος που λειτουργεί ως διακομιστής ελέγχου ταυτότητας, αλλά και ως authenticator, θα πρέπει να έχει παρουσιάζει υψηλές υπολογιστικές δυνατότητες. Μια τέτοια προσέγγιση όμως αντιμετωπίζει το ζήτημα της αδυναμίας λειτουργίας του συνόλου της επεξεργαστικής δυνατότητας του κόμβου, με αποτέλεσμα την πιθανή εμφάνιση περιπτώσεων επιθέσεων DoS [6].

4.3.4 Captive portal

Ένα captive portal αποτελεί μια ιστοσελίδα η οποία εμφανίζεται σε νέους χρήστες ενός δικτύου Wi-Fi, πριν τους παραχωρηθεί ευρύτερη πρόσβαση στους πόρους του, και συνήθως είναι αποθηκευμένο σε κάποιον διακομιστή ιστού. Ένα captive portal ελέγχει την ταυτότητα των χρηστών χρησιμοποιώντας μια διεπαφή ιστού που συνδέεται με έναν διακομιστή ελέγχου ταυτότητας, ο οποίος περιέχει μια βάση δεδομένων έγκυρων χρηστών. Κάθε φορά που ένας μη ταυτοποιημένος χρήστης προσπαθεί να αποκτήσει πρόσβαση στο Διαδίκτυο, το πρόγραμμα περιήγησής του ανακατευθύνεται στη σελίδα σύνδεσης, όπου πρέπει να εισαγάγει τα διαπιστευτήριά του (όνομα χρήστη και κωδικό πρόσβασης). Αν και τα δύο ταιριάζουν με αυτά που είναι αποθηκευμένα στη βάση δεδομένων χρήστη, ο διακομιστής ελέγχου ταυτότητας δίνει στον χρήστη πρόσβαση στο Διαδίκτυο μέσω του δικτύου WLAN [115].

Με τη χρήση του captive portal δεν απαιτείται η εγκατάσταση κάποιου πρόσθετου λογισμικού στην ασύρματη συσκευή του χρήστη, πέρα από κάποιο πρόγραμμα περιήγησης Ιστού. Αυτή είναι η ευκολία που κάνει πολλά δημόσια δίκτυα WLAN να χρησιμοποιούν ιστοσελίδες captive portal για έλεγχο ταυτότητας χρήστη [116].

Έρευνες έχουν δείξει ότι όταν τα captive portal δεν είναι σωστά διαμορφωμένα, για παράδειγμα, δεν περιλαμβάνουν κρυπτογράφηση SSL ή όταν αυτή δεν έχει ρυθμιστεί σωστά, τότε παρουσιάζουν τρωτά σημεία τα οποία μπορούν να χρησιμοποιηθούν για την πραγματοποίηση MITM. Παράδειγμα αυτού του ζητήματος είναι η πραγματοποίηση επίθεσης με χρήση πλαστογράφησης ARP. Το συγκεκριμένο ζήτημα προκύπτει από το γεγονός ότι τα captive portal ελέγχουν την ταυτότητα μόνο της συσκευής του χρήστη αλλά όχι τον διακομιστή (χωρίς αμοιβαίο έλεγχο ταυτότητας) [6], [117].

Ένα δεύτερο ζήτημα των captive portal είναι ότι δεν παρέχουν κρυπτογράφηση επιπέδου MAC και επομένως, η εμπιστευτικότητα και η ακεραιότητα των πλαισίων δεδομένων σε αυτό το επίπεδο μπορούν να επιτευχθούν μόνο με βάση το σκεπτικό των σχεδιαστών τους [118]. Η αποτυχία παροχής πρόσθετης προστασίας μπορεί να οδηγήσει στην υποκλοπή πληροφοριών, όπως η διεύθυνση MAC των ασύρματων συσκευών που χρησιμοποιούν το captive portal, και η χρησιμοποίησή τους σε μεταγενέστερο χρόνο για τη διαμόρφωση κακόβουλων συσκευών, οι οποίες θα είναι σε θέση με τον τρόπο αυτό να αποκτήσουν παράνομη πρόσβαση στο δίκτυο WLAN. Αυτό σημαίνει ότι, εκτός εάν συνδυαστεί με άλλες μεθόδους ελέγχου ταυτότητας που περιγράφονται σε αυτήν την ενότητα, ο

έλεγχος ταυτότητας που παρέχεται από τα captive portal αποτελεί ένα τρωτό σημείο των δικτύων WLAN, η εκμετάλλευση του οποίου μπορεί να οδηγήσει σε επιθέσεις αποσύνδεσης ή evil twin [6].

4.3.5 Διαπιστευτήρια ελέγχου ταυτότητας και ελέγχου πρόσβασης

Ως διαπιστευτήρια ελέγχου ταυτότητας θεωρούνται όλες οι πληροφορίες που αποστέλλονται στον διακομιστή ελέγχου ταυτότητας από μια ασύρματη συσκευή ή το αντίθετο και χρησιμοποιούνται για την επαλήθευση μιας αξίωσης από μια οντότητα (πελάτη ή διακομιστή ελέγχου ταυτότητας) ότι είναι εξουσιοδοτημένη να ενεργεί για λογαριασμό μιας γνωστής οντότητας (χρήστη) [6]. Τα διαπιστευτήρια που χρησιμοποιούνται κατά τον έλεγχο ταυτότητας μπορούν να υποκλαπούν και να χρησιμοποιηθούν για την απόκτηση μη νόμιμης πρόσβασης σε ένα δίκτυο WLAN. Επιθέσεις που έχουν ως στόχο την υποκλοπή αυτών των διαπιστευτηρίων είναι οι επιθέσεις λεξικού, brute force, phishing και sniffing [86].

Η ανάλυση διαφόρων μεθόδων ελέγχου ταυτότητας δείχνει ότι τα διαπιστευτήρια ελέγχου ταυτότητας που χρησιμοποιούνται πιο κοινά από τους διάφορους μηχανισμούς ελέγχου ταυτότητας είναι οι κωδικοί πρόσβασης, τα μυστικά κλειδιά, τα κλειδιά PSK, τα αναγνωριστικά SSID, οι διευθύνσεις MAC, οι κωδικοί πρόσβασης μίας χρήσης και τα πιστοποιητικά (πελάτη και διακομιστή). Κάθε ένα από αυτά τα διαπιστευτήρια έχει τα δικά του τρωτά σημεία όταν χρησιμοποιούνται για έλεγχο ταυτότητας, τα περισσότερα από τα οποία οφείλονται σε εσφαλμένες διαμορφώσεις. Για παράδειγμα, πολλά hotspot δικτύων WLAN λειτουργούν ανοιχτά (χωρίς κάποιο είδος προστασίας), κάτι που επιτρέπει σε οποιαδήποτε ασύρματη συσκευή να συνδεθεί σε αυτά χωρίς διαπιστευτήρια, μέσω προεπιλεγμένων κωδικών πρόσβασης ή μέσω της διεύθυνσης MAC [86], [90]. Ωστόσο, υπάρχουν πολλά διαθέσιμα εργαλεία επίθεσης ανοιχτού κώδικα, όπως για παράδειγμα το Kismet, τα οποία μπορούν να υποκλέψουν αυτά τα διακριτικά των εξουσιοδοτημένων ασύρματων συσκευών και να αποκτήσουν, με τον τρόπο αυτό, μη εξουσιοδοτημένη πρόσβαση στο δίκτυο WLAN [86], [102].

4.4 Βέλτιστες πρακτικές για την ασφάλεια των WLAN

Παρά το γεγονός ότι τα πρωτόκολλα κρυπτογράφησης και ελέγχου ταυτότητας, που παρουσιάστηκαν στις προηγούμενες ενότητες, σχεδιάστηκαν με σκοπό την παροχή λύσεων ως προς την ασφάλεια των δικτύων WLAN, στην πραγματικότητα η υλοποίηση ενός πλήρως ασφαλούς δικτύου WLAN είναι κάτι παραπάνω από αδύνατο [119]. Ένας τεράστιος όγκος μελετών και ερευνών που υπάρχουν στη βιβλιογραφία έχει αποδείξει ότι τα πρωτόκολλα αυτά δεν μπορούν να παρέχουν πλήρη ασφάλεια στα δίκτυα WLAN και ότι ακόμα και τα ίδια αποτελούν στόχους πολλών ειδών επιθέσεων κατά των δικτύων WLAN. Αυτό σημαίνει ότι η αξιολόγηση της ασφάλειας των δικτύων WLAN αποκτά μεγάλη σημασία, καθώς μέσω αυτής μπορούν να διαπιστωθούν όλα τα τρωτά σημεία και οι πηγές ευπαθειών που παρουσιάζουν τα ασύρματα δίκτυα, αλλά και να σχεδιαστούν διάφορες πρακτικές ασφαλείας για τον μετριασμό τους [88].

Για την αξιολόγηση της ασφάλειας των δικτύων WLAN θα πρέπει να γίνει μια ανάλυση της λειτουργίας τους που να αναδεικνύει τις όποιες προκλήσεις ασφαλείας παρουσιάζουν. Η ορθή κατανόηση αυτών των προκλήσεων μπορεί να οδηγήσει στην εξαγωγή χρήσιμων συμπερασμάτων ως προς το ποια μέτρα και μηχανισμοί ασφάλειας μπορούν να βελτιώσουν, στο μέτρο του δυνατού, την ασφάλεια της υποδομής ενός δικτύου WLAN, αλλά και τον τρόπο με τον οποίο κάτι τέτοιο είναι εφικτό. Με τον τρόπο αυτό είναι δυνατή η ανάπτυξη μιας πολιτικής ασφάλειας των δικτύων WLAN, στην οποία θα περιλαμβάνονται οι βέλτιστες πρακτικές που πρέπει να ακολουθηθούν, ώστε μια τέτοια ασφάλεια να είναι υλοποιήσιμη [120].

Στη βιβλιογραφία, ως βέλτιστες πρακτικές ασφάλειας των δικτύων WLAN θεωρούνται όλες εκείνες οι ενέργειες που πρέπει να ακολουθηθούν ως προς τη ρύθμιση και τη διαχείριση όλων των μονάδων που περιλαμβάνονται στα δίκτυα αυτά. Σε γενικές γραμμές οι πρακτικές αυτές αφορούν τους μηχανισμούς κρυπτογράφησης και ελέγχου ταυτότητας, τα υλικολογισμικά των μονάδων, τις υπηρεσίες που παρέχονται από το δίκτυο, καθώς και την εισαγωγή νέων στοιχείων σε αυτό, όπως η χρήση τειχών προστασίας, συστημάτων IDPS και δικτύων VPN. Ακολουθώντας αυτές τις βέλτιστες πρακτικές, στο πλαίσιο πολιτικών ασφάλειας, είναι δυνατή η πραγματοποίηση μιας όσο το δυνατόν μεγαλύτερης ασφάλειας των ασύρματων δικτύων και αποτελεσματικής προστασίας των ευαίσθητων δεδομένων που μεταφέρονται σε αυτά [121].

4.4.1 Τροποποίηση προεπιλεγμένων κωδικών πρόσβασης

Μια πρώτη βέλτιστη πρακτική αφορά την τροποποίηση των προεπιλεγμένων κωδικών πρόσβασης. Ένας προεπιλεγμένος κωδικός πρόσβασης μπορεί να θεωρηθεί ως μία από τις απλούστερες μεθόδους ασφαλείας, αλλά, ταυτόχρονα, μπορεί να αποτελέσει πηγή σημαντικών ζητημάτων ασφαλείας [122]. Σχεδόν όλος ο εξοπλισμός ενός δικτύου WLAN, όπως οι ασύρματες συσκευές των χρηστών και τα σημεία AP, διαθέτουν βασικούς και προεπιλεγμένους κωδικούς πρόσβασης, οι οποίοι, λόγω της απλότητάς τους, παρέχουν ένα ελάχιστο επίπεδο προστασίας [88]. Οι προεπιλεγμένοι κωδικοί πρόσβασης των συσκευών WLAN εκχωρούνται από τον εκάστοτε κατασκευαστή και μπορούν εύκολα να βρεθούν από τους επιτιθέμενους με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο δίκτυο [123].

Οι Benqdara και Mahmoud (2019) μελέτησαν την κατάσταση ασφάλειας των δικτύων Wi-Fi που παρέχονται στους επισκέπτες χώρων, όπως οι καφετέριες. Στόχος της μελέτης ήταν η αξιολόγηση των τρωτών σημείων που παρουσιάζει μια τέτοια χρήση των δικτύων WLAN. Τα δεδομένα που συλλέχθηκαν, αναλύθηκαν κατάλληλα ώστε να προκύψουν τα κατάλληλα συμπεράσματα για την ασφάλεια των ασύρματων τοπικών δικτύων σε τέτοιους χώρους. Τα αποτελέσματα της μελέτης των συγγραφέων απέδειξαν ότι η κατάσταση της ασφάλειας των δικτύων WLAN σε δημόσιους χώρους χρειάζεται βελτίωση, η οποία θα μπορούσε να επιτευχθεί μέσω εφαρμογής εξελιγμένων κωδικών πρόσβασης και κατάλληλης διαμόρφωσης της κρυπτογράφησης του πρωτοκόλλου WPA2 [124].

Ο M. Maráczi (2019) μελέτησε την ευκολία με την οποία τα δίκτυα WLAN μπορούν να εκτεθούν σε κίνδυνο ως αποτέλεσμα των συσκευών στις οποίες χρησιμοποιούνται οι προεπιλεγμένοι κωδικοί πρόσβασης από τους χρήστες τους. Ο συγγραφέας υποστήριξε ότι κάτι ανάλογο ισχύει και για τα δίκτυα WLAN στα οποία δεν χρησιμοποιείται κανενός είδους κωδικός πρόσβασης, κάτι αρκετά συνηθισμένο σε εκείνες τις ομάδες χρηστών που είναι λιγότερο εξοικειωμένες με τη χρήση του Διαδικτύου και εκείνες που αγνοούν την ύπαρξη απειλών στα δίκτυα WLAN με τα οποία συνδέονται. Η βέλτιστη πρακτική σε αυτές τις περιπτώσεις είναι η δημιουργία από τους χρήστες ισχυρών κωδικών πρόσβασης, οι οποίοι μπορούν να χρησιμοποιηθούν ως πρόσθετο στοιχείο αμυντικού μηχανισμού από επιθέσεις κατά των δικτύων WLAN κοινής χρήσης [125].

Στην περίπτωση που κάποιος επιτιθέμενος αποκτήσει με κάποιον τρόπο έναν έγκυρο κωδικό πρόσβασης, τα περισσότερα συστήματα του επιτρέπουν να συνεχίσει την πρόσβαση μέχρι να εντοπιστεί η εισβολή [126]. Η τροποποίηση αυτών των κωδικών πρόσβασης, σε τακτά χρονικά διαστήματα, με επιλογή πιο σύνθετων, είναι σε θέση να αυξήσουν το επίπεδο ασφάλειας της υποδομής του δικτύου WLAN [84]. Για το λόγο αυτό, όλα τα στοιχεία ενός δικτύου WLAN πρέπει να είναι εξοπλισμένα με μια επιλογή, η οποία θα δίνει τη δυνατότητα τροποποίησης του προεπιλεγμένου κωδικού πρόσβασης, μετά την πρώτη χρήση τους [88], [122].

Σύμφωνα με τους Carballal και συν. (2020), οι πιο δημοφιλείς στρατηγικές για τη δημιουργία ισχυρών κωδικών πρόσβασης, με σκοπό τη μείωση των αδυναμιών ασφάλειας που είναι εγγενείς με τη χρήση των προεπιλεγμένων, είναι οι εξής [126]:

- ***Μήκη κωδικού πρόσβασης τουλάχιστον οκτώ χαρακτήρων***: Οι μεγαλύτεροι κωδικοί πρόσβασης αυξάνουν τον χρόνο που απαιτείται από τα λογισμικά που χρησιμοποιούνται από τους επιτιθέμενους για την αποκρυπτογράφηση τους
- ***Τυχαίος συνδυασμός κεφαλαίων και πεζών γραμμάτων με ειδικά σύμβολα***: Η χρήση στους κωδικούς πρόσβασης χαρακτήρων κεφαλαίων, πεζών και συμβόλων (!£$%, κ.λπ.) αυξάνει την πολυπλοκότητά τους και αυξάνει γεωμετρικά τον αριθμό των προσπαθειών που πρέπει να πραγματοποιηθούν από τους επιτιθέμενους για την αποκωδικοποίησή τους. Ένας προτεινόμενος τρόπος προσέγγισης αυτής της στρατηγικής είναι η χρήση μνημονικών κανόνων (π.χ., το "Θέλω να δημιουργήσω έναν ασφαλή κωδικό πρόσβασης ενάντια στο λογισμικό αποκωδικοποίησης" δημιουργεί τον κωδικό πρόσβασης "IwtgaspacS" παίρνοντας το πρώτο γράμμα κάθε λέξης της φράσης στα αγγλικά)
- ***Μη χρήση λέξεων λεξικού***: Η δημιουργία κωδικών πρόσβασης με λέξεις που δεν μπορούν να βρεθούν στο λεξικό μιας οποιαδήποτε γλώσσας ελαχιστοποιεί την αποτελεσματικότητα των επιθέσεων λεξικού

4.4.2 Χρήση ισχυρών μεθόδων ελέγχου ταυτότητας

Μια δεύτερη βέλτιστη πρακτική για την ασφάλεια των δικτύων WLAN είναι η χρήση ισχυρών μεθόδων ελέγχου ταυτότητας. Πολλές από τις μεθόδους EAP, όπως αναφέρθηκε σε προηγούμενη ενότητα, είναι σε θέση να παρέχουν μεγάλη ασφάλεια κατά τη διαδικασία των ελέγχων ταυτότητας. Σε ένα δίκτυο WLAN, είναι σημαντικό όλες οι ασύρματες συσκευές του να έχουν ρυθμιστεί ώστε να χρησιμοποιούν την ίδια μέθοδο ελέγχου ταυτότητας [88]. Επίσης, τα κλειδιά ελέγχου ταυτότητας που χρησιμοποιούνται σε αυτές τις διαδικασίες θα πρέπει να αλλάζουν τακτικά. Με τον τρόπο αυτό, μπορεί να επιτευχθεί μεγαλύτερη ασφάλεια ως προς την πρόσβαση στους πόρους του δικτύου μόνο από τους εξουσιοδοτημένους χρήστες και την απαγόρευση πρόσβασης στους μη εξουσιοδοτημένους [127]. Ως πιο προηγμένες μέθοδοι ελέγχου ταυτότητας, θεωρούνται οι μηχανισμοί ελέγχου ταυτότητας δύο παραγόντων ή οι αντίστοιχοι πολλαπλών παραγόντων, οι οποίοι είναι σε θέση να παρέχουν πρόσθετα επίπεδα ασφάλειας [121].

Οι μηχανισμοί ελέγχου ταυτότητας δύο παραγόντων προτάθηκαν από πολλούς μελετητές με σκοπό τον συνδυασμό των διαπιστευτηρίων των χρηστών (συνδυασμό όνομα χρήστη και κωδικού πρόσβασης) με έναν δεύτερο παράγοντα, όπως της προσωπικής ιδιοκτησίας (ownership), της γνώσης (knowledge) και των βιομετρικών στοιχείων (biometrics) [128], [129]. Η εφαρμογή αυτού του μηχανισμού ελέγχου ταυτότητας απαιτεί έναν πρόσθετο μηχανισμό ταυτοποίησης της ασύρματης συσκευής του χρήστη. Μετά την ολοκλήρωση του πρώτου σταδίου ελέγχου ταυτότητας, ακολουθεί ο δεύτερος μηχανισμός όπου ο χρήστης καλείται να παρουσιάσει έναν φυσικό μηχανισμό ή έναν κωδικό πρόσβασης μίας χρήσης, που αποστέλλεται μέσω email, SMS ή άλλης συσκευής [130].

Καθώς οι επιθέσεις γίνονται πιο στοχευμένες και οι συνέπειες της μη εξουσιοδοτημένης πρόσβασης είναι πλέον πιο σοβαρές, δημιουργήθηκε η ανάγκη δημιουργίας μηχανισμών ελέγχου ταυτότητας περισσότερων επιπέδων που θα μεγιστοποιήσουν την ασφάλεια των δικτύων WLAN. Επομένως, οι μηχανισμοί ελέγχου ταυτότητας πολλαπλών παραγόντων προτάθηκαν από πολλούς μελετητές για την παροχή ακόμα υψηλότερου επιπέδου ασφάλειας και τη διευκόλυνση της συνεχούς προστασίας των συσκευών καθώς και άλλων κρίσιμων υπηρεσιών από μη εξουσιοδοτημένη πρόσβαση. Ως επί το πλείστον, οι μηχανισμοί αυτοί βασίζονται στη χρήση βιομετρικών στοιχείων, τα οποία αποτελούν ένα είδος αυτοματοποιημένης αναγνώρισης των ατόμων με βάση τη συμπεριφορά και τα μοναδικά βιολογικά χαρακτηριστικά τους, όπως τα δακτυλικά αποτυπώματα ή η ίριδα [128], [129].

4.4.3 Χρήση ισχυρών μεθόδων κρυπτογράφησης

Η προστασία των δεδομένων με χρήση ισχυρών μεθόδων κρυπτογράφησης αποτελεί μια ακόμα περίπτωση βέλτιστης πρακτικής ασφάλειας των δικτύων WLAN. Με την κρυπτογράφηση των δεδομένων που μεταδίδονται σε ένα δίκτυο WLAN μεταξύ των ασύρματων συσκευών και των σημείων AP, η υποκλοπή τους για κακόβουλους σκοπούς καθίσταται πιο δύσκολη. Όπως αναφέρθηκε σε προηγούμενη ενότητα, αυτή η κρυπτογράφηση μπορεί να γίνει με τεχνικές και μεθόδους που υποστηρίζονται από τα πρωτόκολλα κρυπτογράφησης WPA, WPA2 και WPA3. Αν και τα WPA και WPA2 εξακολουθούν να είναι διαθέσιμα, συνιστάται η χρήση του πρωτοκόλλου WPA3, τουλάχιστον από τον εξοπλισμό του δικτύου που το υποστηρίζει, καθώς τα πρωτόκολλα αυτά παρουσιάζουν ευπάθειες οι οποίες μπορούν να οδηγήσουν στην παραβίαση του δικτύου WLAN. Αυτή τη στιγμή, το πρωτόκολλο κρυπτογράφησης WPA3 θεωρείται το πλέον ασφαλές [131].

Οι Bhattacharjee και Senapati (2023) παρουσίασαν μια μελέτη με σκοπό τον εντοπισμό των κενών ασφαλείας που παρουσιάζουν τα υφιστάμενα πρωτόκολλα κρυπτογράφησης Wi-Fi. Οι διαδικασίες εντοπισμού αυτών των κενών ασφαλείας πραγματοποιήθηκαν σε ελεγχόμενο εργαστηριακό περιβάλλον. Οι συγγραφείς απέδειξαν ότι παρά την κρυπτογράφηση που παρουσιάζουν τα διάφορα πρωτόκολλα κρυπτογράφησης, τα πακέτα δεδομένων των ασύρματων δικτύων μπορούσαν εύκολα να υποκλαπούν χρησιμοποιώντας την σουίτα λογισμικών aircrack-ng (ένα πρόγραμμα που μπορεί να ανιχνεύσει τη διαδικασία χειραψίας μεταξύ των σημείων AP και των ασύρματων συσκευών του δικτύου WLAN), ενώ το σπάσιμο του κωδικού πρόσβασης μπορούσε να πραγματοποιηθεί μέσω χρήσης τεράστιων λιστών λέξεων. Βρέθηκε επίσης, ότι η διαδικασία σπασίματος του κωδικού πρόσβασης θα μπορούσε να επιταχυνθεί μέσω χρήσης μιας μονάδας επεξεργασίας γραφικών GPU (Graphics Processing Unit) για την εκτέλεση επαναλαμβανόμενων συνόλων διαδικασιών εξαγωγής των κωδικών πρόσβασης. Οι συγγραφείς κατέληξαν στο συμπέρασμα, ότι για την ελαχιστοποίηση αυτών των κενών ασφαλείας θα πρέπει [132]:

- να γίνεται πάντα χρήση του πρωτοκόλλου WPA2 σε παλαιότερες συσκευές και του μοντέλου ασφαλείας WPA3 στις πιο σύγχρονες
- να γίνεται χρήση κλειδιών κρυπτογράφησης μεγαλύτερου μήκους με σκοπό τη μείωση των πιθανοτήτων επιτυχίας των επιθέσεων brute force
- να γίνεται χρήση του διακομιστή RADIUS τόσο σε επαγγελματικά όσο και σε οικιακά δίκτυα WLAN

Η χρήση του πρωτοκόλλου κρυπτογράφησης WPA3 έχει προταθεί από μια μεγάλη πλειάδα μελετητών ως την ιδανικότερη λύση κρυπτογράφησης των επικοινωνιών WLAN, καθώς παρέχει πολλές βελτιώσεις που μπορούν να συνοψιστούν ως εξής [133], [134], [135]:

- ***Πολύ πιο δύσκολο σπάσιμο των κωδικών πρόσβασης***: Με τη χρήση του πρωτοκόλλου WPA2, οι επιτιθέμενοι μπορούν να εξάγουν τους κωδικούς πρόσβασης χρησιμοποιώντας επιθέσεις λεξικού. Αντίθετα με το WPA3 κάτι τέτοιο δεν είναι δυνατό, καθώς οι επιτιθέμενοι θα πρέπει να είναι online και να αλληλεπιδρούν με το Wi-Fi σε όλη τη διαδικασία εξαγωγής των κωδικών πρόσβασης. Ως εκ τούτου, το WPA3 κάνει το σπάσιμο των κωδικών πρόσβασης μια πολύ πιο δύσκολη και χρονοβόρα διαδικασία
- ***Επιβολή συχνής τροποποίησης των κωδικών πρόσβασης***: Το WPA3 περιλαμβάνει μηχανισμούς που επιβάλουν στους χρήστες τη συχνή τροποποίηση των κωδικών τους πρόσβασης για μεγαλύτερη ασφάλεια
- ***Μεγαλύτερη ασφάλεια σε δημόσια δίκτυα Wi-Fi***: Το WPA3 κρυπτογραφεί την κυκλοφορία δεδομένων του χρήστη στα δημόσια και ανοιχτά δίκτυα Wi-Fi, ώστε να είναι πολύ πιο ασφαλής η χρήση τους

4.4.4 Τροποποίηση χρήσης αναγνωριστικών SSID

Η αποτροπή πρόσβασης στο δίκτυο WLAN των μη εξουσιοδοτημένων χρηστών θα μπορούσε να ενισχυθεί και μέσω της μη δημοσίευσης των αναγνωριστικών SSID. Ακόμα και στην περίπτωση που κάτι τέτοιο είναι δύσκολο, η αλλαγή αυτού του αναγνωριστικού θα μπορούσε να αποτελέσει μια κάποια λύση, καθώς αν διατηρηθεί η προεπιλεγμένη επιλογή του αναγνωριστικού SSID, κάθε επίδοξος επιτιθέμενος είναι εύκολο να προσδιορίσει το είδος των router που χρησιμοποιούνται σε ένα δίκτυο WLAN για να εκμεταλλευτεί οποιοδήποτε γνωστό τρωτό σημείο του. Επίσης, από την πλευρά των χρηστών του δικτύου, η προστασία του αναγνωριστικού SSID της συσκευής τους σε όλους τους δρομολογητές Wi-Fi, θα καταστήσει πιο δύσκολο για τους εισβολείς να εντοπίσουν ένα δίκτυο WLAN [136].

Οι Lindroos, Hakkala και Virtanen (2021), στη μελέτη τους πάνω στην αξιολόγηση της ασφάλειας των δικτύων Wi-Fi, κατάληξαν στο συμπέρασμα ότι το αναγνωριστικό SSID και οι κωδικοί πρόσβασης των σημείων AP των δικτύων Wi-Fi θα πρέπει να τροποποιούνται συχνά και να μην διατηρούνται σε αυτά οι εργοστασιακές προεπιλογές. Στην περίπτωση που κάτι τέτοιο δεν πραγματοποιείται, το προεπιλεγμένο αναγνωριστικό SSID του δικτύου, άρα και ο προεπιλεγμένος κωδικός πρόσβασης που δίνεται από τον κατασκευαστή, είναι ήδη γνωστά στοιχεία του δικτύου ακόμα και στους επιτιθέμενους. Σύμφωνα με τους συγγραφείς, ένα τέτοιο σημείο AP μπορεί να αποτελέσει πιθανό σημείο εισβολής στο δίκτυο, καθώς στο αναγνωριστικό SSID περιλαμβάνονται σημαντικές πληροφορίες, όπως το μοντέλο και ο κατασκευαστής της συσκευής, με αποτέλεσμα ο επιτιθέμενος να μπορεί να τις χρησιμοποιήσει για να εξαπολύσει επίθεση στο ασύρματο δίκτυο. Οι συγγραφείς τονίζουν επίσης ότι παρά το γεγονός ότι υπάρχουν προγράμματα τα οποία μπορούν να σαρώσουν ένα ασύρματο δίκτυο για την άντληση των παραπάνω πληροφοριών, κάτι που μπορεί να παρακάμψει τα οφέλη της τροποποίησης του αναγνωριστικού SSID, η προτεινόμενη διαδικασία μπορεί να αποθαρρύνει την πραγματοποίηση επιθέσεων από μια μεγάλα μερίδα επίδοξων επιτιθέμενων, δίνοντας στο δίκτυο WLAN ένα επιπλέον στρώμα προστασίας [137]. Σε αντίστοιχα συμπεράσματα κατάληξαν και οι μελέτες των Lu και Yu (2021) [138], αλλά και των Etta και συν. (2022) [88].

4.4.5 Τακτική ενημέρωση λογισμικών προστασίας

Η τακτική ενημέρωση των λογισμικών προστασίας από ιούς και των υλικολογισμικών των σημείων AP και των router των δικτύων WLAN αποτελεί μια ακόμα βέλτιστη πρακτική της ασφάλειάς τους. Η διατήρηση αυτών των ενημερώσεων διασφαλίζει την προστασία των συσκευών από γνωστές ευπάθειες, καθώς τα συγκεκριμένα λογισμικά ενημερώνονται ανά τακτά χρονικά διαστήματα από τις εταιρείες ανάπτυξής τους, με σκοπό τη συνεχή βελτίωση της λειτουργίας τους [139]. Η ορθή λειτουργία των λογισμικών προστασίας από ιούς εξαρτάται βέβαια σε μεγάλο βαθμό και από τον τρόπο χρήσης των συσκευών σε ένα δίκτυο WLAN. Για παράδειγμα, για την ενίσχυση της λειτουργίας των εν λόγω λογισμικών, συνιστάται η απενεργοποίηση των επιλογών της κοινής χρήσης των αρχείων δικτύου και συσκευών [140].

Ο J. P. Patra (2021) αναφέρει ότι παρόλο που τα περισσότερα πρωτόκολλα κρυπτογράφησης παρουσιάζουν ευπάθειες ως προς την ασφάλεια των δικτύων WLAN, η χρήση τους μπορεί να παρέχει ένα μεγάλο ποσοστό ασφάλειας. Ο συγγραφέας συνιστά κάποιες πρακτικές για την αντιμετώπιση αυτών των απειλών ασφαλείας και την ελαχιστοποίηση των όποιων επακόλουθων κινδύνων, οι περισσότερες από τις οποίες αναφέρονται σε αυτήν την ενότητα. Ανάμεσα σε αυτές τις πρακτικές αναφέρεται ότι για μεγαλύτερη ασφάλεια, συνιστάται η εγκατάσταση και η τακτική ενημέρωση

λογισμικών προστασίας από ιούς, καθώς και η χρήση τειχών προστασίας με τακτική ενημέρωση του υλικολογισμικού τους [141].

Οι Aslan και συν. (2023) στη μελέτη τους πάνω στα τρωτά σημεία, στις απειλές και στις επιθέσεις που παρουσιάζονται στον κυβερνοχώρο και ως προς τις προτάσεις που κάνουν όσον αφορά την ασφάλεια των δικτύων WLAN, αναφέρουν ότι παρά το γεγονός ότι η κρυπτογράφηση είναι ένας από τους πιο αποτελεσματικούς τρόπους προστασίας των ασύρματων δικτύων, η χρήση λογισμικών προστασίας από ιούς, τειχών προστασίας και λογισμικών προστασίας από κατασκοπεία, αλλά και η συχνή ενημέρωση τους, μπορεί να θεωρηθεί εξίσου απαραίτητη για τη βελτιστοποίηση της ασφάλειάς τους [142].

Οι Le και συν. (2022) αναφέρουν ότι από μόνη της, η τακτική ενημέρωση των λογισμικών προστασίας από τους ιούς δεν είναι αρκετή για την αντιμετώπιση των επιθέσεων κακόβουλου λογισμικού κατά των δικτύων Wi-Fi, αλλά απαιτείται και μια ανάλυση του αντίκτυπού τους, ιδιαίτερα στα δίκτυα μεγάλης εμβέλειας. Για το λόγο αυτό πρότειναν ένα μοντέλο εξάπλωσης του εκάστοτε κακόβουλου λογισμικού στα δίκτυα αυτά, το οποίο λαμβάνει υπόψη του τα χαρακτηριστικά των μεθόδων κρυπτογράφησης και την πολυπλοκότητα των κωδικών πρόσβασης που χρησιμοποιούνται από τους δρομολογητές του δικτύου. Επιπλέον, είναι επίσης απαραίτητο να λαμβάνει υπόψη του τα συγκεκριμένα χαρακτηριστικά που παρουσιάζει η εκάστοτε επίθεση κακόβουλου λογισμικού σε κάθε στάδιο της. Οι συγγραφείς κατέληξαν στο συμπέρασμα, ότι μέσω ενός τέτοιου μοντέλου είναι δυνατή η βελτιστοποίηση της ασφάλειας των δικτύων Wi-Fi, με την προϋπόθεση ότι οι δρομολογητές του δικτύου περιλαμβάνουν ισχυρές μεθόδους κρυπτογράφησης (π.χ. WPA3 και WPS), χρησιμοποιούν ισχυρούς και πολύπλοκους κωδικούς πρόσβασης, αλλά και το υλικολογισμικό τους ενημερώνεται σε τακτά χρονικά διαστήματα [143].

4.4.6 Χρήση τειχών προστασίας

Το τείχος προστασίας (firewall) αποτελεί μια συσκευή ασφαλείας δικτύου που παρακολουθεί την εισερχόμενη και την εξερχόμενη κυκλοφορία του δικτύου και αποφασίζει εάν θα επιτρέψει ή θα αποκλείσει συγκεκριμένη κυκλοφορία με βάση ένα προκαθορισμένο σύνολο κανόνων ασφαλείας [84]. Η χρήση τειχών προστασίας, σε συνδυασμό με τη σωστή ρύθμισή τους και την τακτική ενημέρωση του υλικολογισμικού τους, μπορεί να ενισχύσει την προστασία των δικτύων WLAN από περιπτώσεις μη εξουσιοδοτημένης πρόσβασης. Η μη σωστή ρύθμιση των firewall ή η μη τακτική ενημέρωση του υλικολογισμικού τους μπορεί να αποτελέσει τρωτό σημείο ενός δικτύου WLAN, το οποίο μπορεί να εκμεταλλευτεί ένας επιτιθέμενος και να παρακάμψει το τείχος προστασίας, αποκτώντας έτσι άμεση πρόσβαση στο ασύρματο δίκτυο [88].

Οι Saini, Gupta και Gupta (2021) έδωσαν ιδιαίτερη έμφαση στη σωστή ρύθμιση των τειχών προστασίας, ώστε να μπορεί να επιτευχθεί μεγαλύτερη ασφάλεια ενός δικτύου WLAN [144]. Οι Pebrianti, Kanedi και Arliando (2021) αναφέρουν ότι η σωστή ρύθμιση των τειχών προστασίας σε συνδυασμό με captive portal είναι σε θέση, όχι μόνο να αυξήσει την ασφάλεια ενός Internet-based δικτύου WLAN, αλλά και να αυξήσει την αποδοτικότητά του, καθώς το τείχος προστασίας μπορεί με τον τρόπο αυτό να λειτουργήσει ως φίλτρο πρόσβασης σε ιστότοπους, κάτι που διευκολύνει την ισοκατανομή των δικτυακών πόρων στους χρήστες του δικτύου, ανάλογης των αναγκών πρόσβασης σε αυτό [145].

Ιδιαίτερα η χρήση host-based τειχών προστασίας μπορεί να αποτελέσει ένα επιπρόσθετο επίπεδο ασφάλειας των δικτύων WLAN. Οι Susmita και Kailas (2021) αναφέρουν ότι με την εξέλιξη των δικτυακών τεχνολογιών, οι απαιτήσεις από τα τείχη προστασίας έχουν αυξηθεί ως προς την παροχή

ασφάλειας από προηγμένες απειλές στην υποδομή και τις συνδεδεμένες συσκευές στα δίκτυα WLAN. Κατά συνέπεια, οι "παραδοσιακές" συσκευές τείχους προστασίας θα πρέπει να παρουσιάζονται ως ένα μείγμα φυσικών και εικονικών συσκευών. Με άλλα λόγια τα ασύρματα δίκτυα θα πρέπει να περιλαμβάνουν φυσικές συσκευές τειχών προστασίας, αλλά και εικονικές οι οποίες θα μπορούσαν να παρέχονται ως υπηρεσία από δημόσια περιβάλλοντα cloud. Με τον τρόπο αυτό θα είναι καλύτερη η προστασία όλων των συσκευών του δικτύου που παρουσιάζουν κλιμακούμενες απαιτήσεις κυκλοφορίας, των λογισμικών που λειτουργούν στις προσωπικές συσκευές των χρηστών, των δρομολογητών SD-WAN και των πυλών του δικτύου με το Διαδίκτυο. Οι συγγραφείς αναφέρουν ότι μια τέτοια χρήση των τειχών προστασίας δημιουργεί πολλά στρατηγικά σημεία ασφάλειας σε ολόκληρο τον ιστό του δικτύου, τα οποία βρίσκονται πιο κοντά στις πληροφορίες και τις εφαρμογές που πρέπει να προστατεύονται. Συνοψίζοντας, αναφέρεται ότι η χρήση host-based τειχών προστασίας θα έχει μεγαλύτερα αποτελέσματα ασφάλειας και προστασίας στην περίπτωση που αυτά συνδυάζονται με συστήματα IDPS [146].

4.4.7 Χρήση συστημάτων IDPS

Τα συστήματα IDPS (Intrusion Detection and Prevention Systems) μπορούν να χρησιμοποιηθούν για τον εντοπισμό και την πρόληψη παραβιάσεων ασφάλειας των δικτύων WLAN. Η ορθή λειτουργία τους είναι άρρηκτα συνδεδεμένη με την σωστή ρύθμισή τους και την τακτική ενημέρωση του λογισμικού και του υλικολογισμικού τους [147].

Σύμφωνα με τους Satam και Hariri (2020), τα συστήματα IDPS που έχουν χρησιμοποιηθεί κατά καιρούς στα δίκτυα Wi-Fi, μπορούν να ταξινομηθούν σε τρεις τύπους, με βάση το επίπεδο στο οποίο πραγματοποιούν την ανάλυσής τους [148]: (α) τα συστήματα IDPS φυσικού επιπέδου, (β) τα συστήματα IDPS επιπέδου MAC και (γ) τα συστήματα IDPS φυσικού επιπέδου και επιπέδου σύνδεσης δεδομένων. Τα συστήματα IDPS που ανιχνεύουν επιθέσεις στο φυσικό επίπεδο χρησιμοποιούν πολλαπλές κεραίες και μετρούν την ισχύ των σημάτων που μεταδίδονται εντός των δικτύων Wi-Fi. Με τον τρόπο αυτό είναι σε θέση να ανιχνεύουν διάφορα είδη επιθέσεων, όπως επιθέσεις παρεμβολής δικτύου και επιθέσεις πλαστογράφησης διεύθυνσης MAC. Ο σχεδιασμός και η ανάπτυξή τους είναι πολύπλοκες, καθώς θα πρέπει να λαμβάνουν υπόψη τους πολλούς παραμέτρους και παράγοντες, όπως η εξασθένηση του σήματος, ο θόρυβος, οι αλλαγές στο μέσο και η συνεχή κινητικότητα των χρηστών [149], [150]. Τα συστήματα IDPS που χρησιμοποιούνται για να ασφαλίζουν το επίπεδο σύνδεσης δεδομένων των δικτύων Wi-Fi, εντοπίζουν την ύπαρξη επιθέσεων μέσω χρήσης των δεδομένων που λαμβάνονται από το πλαίσιο Wi-Fi [151]. Σύμφωνα με τους συγγραφείς, εκτός από αυτά τα συστήματα που έχουν παρουσιαστεί σε μελέτες των αρχών της δεκαετίας του 2010, σε πραγματικές υλοποιήσεις δικτύων Wi-Fi χρησιμοποιούνται συστήματα ανίχνευσης εισβολής ανοιχτού κώδικα (π.χ. Snort), εμπορικά συστήματα ανίχνευσης εισβολής (π.χ. AirMagnet), καθώς και κάποιες μηχανές ανίχνευσης (π.χ. Air Defense). Όλα αυτά τα συστήματα χρησιμοποιούν τεχνικές εντοπισμού επιθέσεων που βασίζονται στην υπογραφή (signature based), κάτι που σημαίνει ότι δεν μπορούν να εντοπίσουν άλλα είδη επιθέσεων, όπως επιθέσεις zero-day [148].

Οι Usha και Kavitha (2017) παρουσίασαν ένα σύστημα IDPS που βασίζεται στη χρήση τεχνικών εντοπισμού ανωμαλιών (anomaly based), το οποίο είναι σε θέση να εντοπίζει επιθέσεις κατά του επιπέδου MAC στα δίκτυα 802.11. Πειραματική αξιολόγηση αυτής της προσέγγισης έδειξε ποσοστό επιτυχημένων ανιχνεύσεων εισβολών της τάξης του 99%, με ποσοστό ψευδών συναγερμών 0,1%. Το πρόβλημα του προτεινόμενου συστήματος είναι ότι δεν είναι σε θέση να ανιχνεύσει τροποποιημένες επιθέσεις, όπως για παράδειγμα επιθέσεις κατάργησης ταυτότητας [152]. Αντίστοιχο σύστημα που παρουσίασαν οι Satam και Hariri (2020), είναι σε θέση να εντοπίζει σχεδόν όλα τα είδη επιθέσεων

κατά των δικτύων Wi-Fi, μέσω μοντελοποίησης της συνολικής συμπεριφοράς του, αλλά η αξιολόγησή του έδειξε μέσο όρο ποσοστών επιτυχημένων ανιχνεύσεων της τάξης του 98,8% και μέσο ποσοστό ψευδών συναγερμών της τάξης του 1,74% για διάφορα είδη επιθέσεων [148].

4.4.8 Χρήση δικτύων VPN

Μια τελευταία βέλτιστη πρακτική που μπορεί να αυξήσει την προστασία και την ασφάλεια των δικτύων WLAN είναι η χρήση δικτύων VPN (Virtual Private Network). Τα περισσότερα πρωτόκολλα WAP επιτρέπουν τη χρήση δικτύων VPN. Σε μια τέτοια περίπτωση, το ασύρματο δίκτυο διαχωρίζεται από το υπόλοιπο δίκτυο και όλη η πρόσβαση γίνεται μέσω του διακομιστή VPN. Στην ιδανική περίπτωση, ένα δίκτυο WLAN μπορεί να χωριστεί σε πολλά μέρη, καθένα από τα οποία λειτουργεί με χρήση σημείων AP και διακομιστών VPN. Σε μια τέτοια περίπτωση, πρόσβαση στο δίκτυο αποκτούν μόνο οι ασύρματες συσκευές που χρησιμοποιούν λογισμικό VPN και παρουσιάζουν τα σωστά διαπιστευτήρια. Με αυτόν τον τρόπο, οι συνδέσεις εντός του δικτύου WLAN δεν μπορούν να υποκλαπούν, από τη στιγμή που όλη η κυκλοφορία είναι κρυπτογραφημένη [88]. Λόγω των πολλών πλεονεκτημάτων τους, δύο είδη δικτύων VPN, όπως τα IPSec VPN και SSL VPN είναι ευρέως διαδεδομένα στη χρήση τους στα δίκτυα WLAN [153].

Κεφάλαιο 5ο: Απόδοση Ασύρματων τοπικών δικτύων

5.1 Η έννοια της απόδοσης στα δίκτυα WLAN

Οι διάφορες ασύρματες τεχνολογίες που υπάρχουν αποσκοπούν στην κάλυψη όσο το δυνατόν περισσότερων από τις διαφορετικές ανάγκες των χρηστών. Σε αυτήν την προσπάθεια, κάθε τεχνολογία παρουσιάζει τα δικά της χαρακτηριστικά απόδοσης και έχει σχεδιαστεί ώστε να παρουσιάζει τη βέλτιστη απόδοση για συγκεκριμένες εφαρμογές και πλαίσια. Ωστόσο, οι περισσότερες από αυτές τις τεχνολογίες λειτουργούν βάσει κοινών κανόνων, παρουσιάζουν κοινούς συμβιβασμούς και υπόκεινται σε κοινά κριτήρια απόδοσης και περιορισμούς, η κατανόηση των οποίων είναι πολύ σημαντική για την ορθή εκτίμηση της συνολικής απόδοσης των ασύρματων συστημάτων και των όποιων βελτιώσεων μπορούν να γίνουν [27].

Γενικότερα, το ασύρματο μέσο μετάδοσης αποτελεί ένα πολύ δυναμικό κοινόχρηστο περιβάλλον που επηρεάζεται από διάφορους παράγοντες, οι οποίοι τις περισσότερες φορές αλληλοεπιδρούν μεταξύ τους. Μερικοί από αυτούς τους παράγοντες μπορούν να ελεγχθούν, ενώ άλλοι αποτελούν θεμελιώδεις περιορισμούς του ασύρματου μέσου που πρέπει να αναγνωρίζονται και να λαμβάνονται υπόψη κατά τον σχεδιασμό ενός δικτύου WLAN [124].

Παρά τα οφέλη των δικτύων WLAN, όπως αυτά αναφέρθηκαν και αναλύθηκαν σε προηγούμενο κεφάλαιο, μία από τις προκλήσεις που αντιμετωπίζουν οι μηχανικοί και οι σχεδιαστές τους είναι η αύξηση της απόδοσης ανά χρήστη που μπορεί να παρουσιάσει ένα τυπικό δίκτυο WLAN με μεσαίο έως μεγάλο αριθμό χρηστών. Η οπτική αυτή είναι γνωστή ως εμπειρία του χρήστη (user experience) και αφορά τον τρόπο που βιώνουν οι τελικοί χρήστες την ποιότητα QoS των υπηρεσιών που παρέχονται από ένα δίκτυο [154]. Έτσι σε ένα δίκτυο WLAN το οποίο παρουσιάζει χαμηλή συνολική απόδοση, οι χρήστες βιώνουν προβλήματα που εμφανίζονται, για παράδειγμα, με τη μορφή της αργής περιήγησης στο Διαδίκτυο, της αργής λήψης αρχείων και γενικότερα της αργής επικοινωνίας με άλλες συσκευές του δικτύου [155].

Η συνεχώς αυξανόμενη χρήση των δικτύων WLAN οδήγησε τους οργανισμούς τυποποίησης, τις κατασκευάστριες εταιρείες και του σχεδιαστές δικτύων στην ανεύρεση λύσεων για μεγαλύτερη κάλυψη και χωρητικότητα των συγκεκριμένων δικτύων. Δεδομένης της κατανεμημένης φύσης της κοινής χρήσης των πόρων των δικτύων WLAN 802.11, αυτές οι λύσεις μπορεί να καταστούν αναποτελεσματικές όταν ισοδυναμούν με απλό σχεδιασμό και ανάπτυξη δικτύων μεγαλύτερου αριθμού πόρων. Αντίθετα, οι λύσεις αυτές μπορούν να αποδειχθούν ιδιαίτερα σημαντικές, αν συνδυαστούν με σωστή διαμόρφωση του εξοπλισμού των δικτύων WLAN, ένα στοιχείο ζωτικής σημασίας για την απόδοσή τους [156].

Οι συνεχώς αυξανόμενες απαιτήσεις για μεγαλύτερη χωρητικότητα και μεγαλύτερο εύρος κάλυψης είχαν ως αποτέλεσμα τη δημιουργία μεγάλου αριθμού τροποποιήσεων του προτύπου IEEE 802.11 και τον σχεδιασμό δικτύων WLAN με δυνατότητα υποστήριξης ολοένα και μεγαλύτερου αριθμού σημείων AP. Τα στοιχεία όμως αυτά, της ανάπτυξης νέων (και πιο πολύπλοκων) προτύπων και της αύξησης της πυκνότητας των δικτύων WLAN, οδηγούν σε μια σειρά ζητημάτων απόδοσης. Δεδομένης της συνεχιζόμενα αυξανόμενης δημοτικότητας των ασύρματων επικοινωνιών, η αξιολόγηση της απόδοσης των δικτύων WLAN παραμένει ένα από τα πλέον δημοφιλή ζητήματα προς διερεύνηση και μελέτη [156].

Για την βελτιστοποίηση της απόδοσης που θεωρητικά μπορούν να παρουσιάσουν όλα τα πρότυπα των δικτύων WLAN, απαιτείται ο εντοπισμός και η ποσοτικοποίηση όλων των βασικών παραγόντων που μπορούν να συμβάλουν περιοριστικά σε αυτή, καθώς και προσεκτικός σχεδιασμός και ανάπτυξη του δικτύου. Μόνο με αυτόν τον τρόπο είναι δυνατή η εκπλήρωση όλων των σύγχρονων απαιτήσεων για υψηλή διαθεσιμότητα και απόδοση των δικτύων WLAN [155].

5.2 Παράγοντες που επηρεάζουν την απόδοση των δικτύων WLAN

Καθώς το ζήτημα της απόδοσης των δικτύων WLAN είναι ιδιαίτερα σημαντικό για την εύρυθμη λειτουργία τους, η ακαδημαϊκή και ερευνητική κοινότητα έχει προχωρήσει στη μελέτη του συγκεκριμένου ζητήματος, με τεράστιο πλήθος μελετών να έχουν ασχοληθεί με την ανεύρεση των παραγόντων που επηρεάζουν τις ασύρματες μεταδόσεις σε αυτά τα δίκτυα. Παρά όμως το τεράστιο αυτό πλήθος μελετών, τουλάχιστον επί του παρόντος, δεν υφίσταται κάποια συγκεκριμένη μεθοδολογία προσδιορισμού αυτών των παραγόντων, κάτι που τελικά μπορεί να προκαλέσει σύγχυση σε οποιονδήποτε θελήσει να ασχοληθεί με το συγκεκριμένο ζήτημα [157].

Στο πλαίσιο της παρούσας εργασίας, στόχος είναι η ανεύρεση των βασικών παραγόντων που επηρεάζουν την απόδοση των δικτύων WLAN, αλλά και των τρόπων με τους οποίους μπορεί αυτή να βελτιωθεί. Η επίτευξη αυτού του στόχου θα βασιστεί στην παρουσίαση κάποιων μελετών που έχουν παρουσιαστεί στη βιβλιογραφία και ασχολούνται με τα ζητήματα αυτά. Στις μελέτες αυτές, οι μετρήσεις της παρεχόμενης ποιότητας QoS από ένα δίκτυο WLAN αφορούν διάφορους δείκτες, οι οποίοι, όπως έχει διαπιστωθεί, επηρεάζουν άμεσα ή έμμεσα την απόδοσή του [158], [159]. Η επιλογή του σωστού δείκτη μέτρησης της απόδοσης ή συνδυασμού τους, εξαρτάται σε μεγάλο βαθμό από την επιθυμητή συμπεριφορά του εκάστοτε δικτύου και ο προσδιορισμός του σε ένα συγκεκριμένο σενάριο χρήσης του δικτύου, πριν από την ανάπτυξη, είναι σαφώς ένα ζήτημα σημαντικής πρακτικής σημασίας [156]. Η σωστή κατανόηση των χαρακτηριστικών απόδοσης των ασύρματων δικτύων είναι ζωτικής σημασίας προκειμένου να επιτευχθούν αποτελεσματικές αναπτύξεις [158].

Η απόδοση των δικτύων WLAN έχει μελετηθεί στη βιβλιογραφία χρησιμοποιώντας διαφορετικές μεθόδους, λαμβάνοντας διαφορετικές μετρήσεις και κάνοντας διαφορετικές υποθέσεις. Για την ανάλυση της απόδοσης ενός δικτύου WLAN, σε μεγάλο πλήθος μελετών, ιδιαίτερα παλαιότερων, χρησιμοποιούνται πολλές τεχνικές και πακέτα προσομοίωσης που αποσκοπούν στην εξέταση μοντέλων των δικτύων αυτών. Παρά το γεγονός, ότι με τον τρόπο αυτό μπορεί να δημιουργηθούν συνθήκες λεπτομερούς αναπαράστασης της λειτουργίας των δικτύων, οι συγκεκριμένες προσεγγίσεις ενδέχεται να παρουσιάζουν υπερβολικά μεγάλους χρόνους εκτέλεσης, καθιστώντας τη βελτιστοποίηση των παραμέτρων των δικτύων γενικά ανέφικτη [158].

Στην περίπτωση μελέτης της απόδοσης των δικτύων με βάση τα χρησιμοποιούμενα πρωτόκολλα, η διαφορετικότητα των χαρακτηριστικών των προτύπων IEEE 802.11 έχει ως συνέπεια την εμφάνιση μιας ποικιλίας μελετών απόδοσης οι οποίες βασίζονται στην εξέταση τελείως διαφορετικών ιδιοτήτων και θεμάτων [160]. Παρά αυτή τη διαφορετικότητα, η μοντελοποίηση της απόδοσης των δικτύων WLAN έχει εφαρμοστεί με επιτυχία για την αξιολόγηση της απόδοσής τους για πολλές δεκαετίες. Για το λόγο αυτό, σε αρκετές, νεότερες μελέτες, χρησιμοποιούνται τεχνικές μοντελοποίησης, οι οποίες αποσκοπούν στη δημιουργία μιας αφηρημένης αναπαράστασης του συστήματος. Με τον τρόπο αυτό, τα διάφορα μεγέθη του δικτύου επαληθεύονται μέσω προσομοίωσης, η οποία μπορεί να χρησιμοποιηθεί για την ανάλυση της συμπεριφοράς του μοντέλου και να εξαχθούν αριθμητικές λύσεις για την πρόβλεψη της απόδοσής του [158].

Στα δίκτυα επικοινωνίας, οι μετρήσεις που σχετίζονται με την απόδοσή τους χρησιμοποιούνται για την ποσοτικοποίηση των χαρακτηριστικών τους, που επιτρέπουν την εξαγωγή πολύτιμων συμπερασμάτων από τους παρόχους του δικτύου και αφορούν άμεσα τους χρήστες του [156]. Στα δίκτυα WLAN, τέτοιες μετρήσεις αντιστοιχούν σε μεγέθη όπως η διαμεταγωγή (throughput), η καθυστέρηση (delay) της μετάδοσης των πακέτων καθώς και η διακύμανσή της (jitter), η αναλογία απώλειας πακέτων, η δικαιοσύνη των ασύρματων συσκευών ως προς την πρόσβαση στο κανάλι επικοινωνίας, η παρουσία ηλεκτρομαγνητικού θορύβου, η παρουσία παρεμβολών, κλπ. [161]. Στη βιβλιογραφία, έχουν παρουσιαστεί και άλλα μεγέθη τα οποία μπορούν να θεωρηθούν ως βασικοί παράγοντες που περιορίζουν την απόδοση των δικτύων WLAN, όπως τα πρωτόκολλα MAC των προτύπων, τα περιβάλλοντα διάδοσης των σημάτων ραδιοσυχνότητας, τα πρωτόκολλα δρομολόγησης, ο τύπος της κυκλοφορίας, κλπ. [162]. Ένας μεγάλος αριθμός μελετών έχει εστιάσει επίσης στη διερεύνηση της επίδρασης που έχει η χρήση πρωτοκόλλων ασφάλειας στα δίκτυα WLAN ως προς την απόδοσή τους. Στις μελέτες αυτές διαπιστώθηκε ότι παρατηρείται πάντα μια αντιστάθμιση μεταξύ της ασφάλειας που παρέχεται από αυτά τα πρωτόκολλα και της σχετικής απόδοσης που παρουσιάζει το εκάστοτε δίκτυο WLAN. Για το λόγο αυτό, η επιλογή του καταλληλότερου πρωτοκόλλου ασφάλειας ενός δικτύου WLAN εξαρτάται σε μεγάλο βαθμό και από το ποσοστό επίδρασής του πάνω στην απόδοση του δικτύου [163]. Τέλος, η απόδοση ενός δικτύου WLAN μπορεί να επηρεαστεί από την αλληλεπίδραση πολλών από τους παράγοντες που αναφέρθηκαν παραπάνω [164]. Από τους παραπάνω παράγοντες, λόγω της ιδιαίτερης σημασίας που παρουσιάζουν τα ζητήματα των παρεμβολών και των θορύβων, καθώς και των πρωτοκόλλων ασφάλειας στην απόδοση των δικτύων WLAN, θα αναλυθούν σε επόμενες ενότητες του κεφαλαίου.

Εκτός από τις παραπάνω μελέτες, που εστιάζουν στην εξέταση κάποιου ή κάποιων από τους προαναφερθέντες παράγοντες επίδρασης στην απόδοση των δικτύων WLAN, στη βιβλιογραφία έχουν εμφανιστεί και κάποιες που συγκρίνουν την συνολική απόδοση των δικτύων WLAN διαφορετικών προτύπων 802.11. Για παράδειγμα, η μελέτη των Lopez-Aguilera, Garcia-Villegas και Casademont (2019) παρουσιάζει μια διεξοδική ανάλυση διαφόρων τροποποιήσεων του βασικού πρωτοκόλλου IEEE 802.11, συγκρίνοντάς τες ως προς το εύρος κάλυψης και την διαμεταγωγή. Με βάση την εμβέλεια κάλυψης, το είδος του σχήματος διαμόρφωσης και κωδικοποίησης και τις τιμές ευαισθησίας του δέκτη, οι συγγραφείς συμπέραναν ότι το πρότυπο IEEE 802.11n παρουσιάζει καλύτερη απόδοση σε σύγκριση με το βασικό πρωτόκολλο IEEE 802.11, ενώ ορισμένες διαμορφώσεις του προτύπου IEEE 802.11ac παρουσιάζουν χειρότερη απόδοση από το IEEE 802.11n, για τον ίδιο ονομαστικό ρυθμό μετάδοσης δεδομένων [165].

Στις επόμενες υποενότητες θα παρουσιαστούν κάποιες από τις μελέτες που έχουν παρουσιαστεί στη βιβλιογραφία και ασχολούνται με την ανάλυση και διερεύνηση των παραγόντων που έχουν αντίκτυπο στην απόδοση των δικτύων WLAN. Η ταξινόμηση των μελετών αυτών είναι καθαρά ενδεικτική, καθώς οι περισσότερες από τις μελέτες αυτές εστιάζουν στην ανάλυση και διερεύνηση περισσότερων του ενός παράγοντα ή συνδυασμού τους.

5.2.1 Διαμεταγωγή

Σε γενικές γραμμές, ο όρος της διαμεταγωγής αφορά τον μέσο όρο του ρυθμού μεταφοράς δεδομένων σε ένα δίκτυο και εξαρτάται σε μεγάλο βαθμό από τον αριθμό των ενεργών χρηστών του δικτύου. Στην περίπτωση, για παράδειγμα, που ένα σημείο AP είναι κοινόχρηστο από πολλούς χρήστες, μπορεί να διαπιστωθεί μειωμένη διαμεταγωγή του δικτύου WLAN από την αναμενόμενη [166], [167]. Σύμφωνα με τους Memon, Nisar και Ahmad (2019), η διαμεταγωγή των δικτύων WLAN επηρεάζεται σε μεγάλο βαθμό από τον μεγάλο αριθμό των χρηστών που εξυπηρετούν, καθώς η αύξηση του

απαιτούμενου αριθμού σημείων AP μειώνει τη συνολική απόδοση του δικτύου. Ταυτόχρονα, όμως, μεγάλο ρόλο σε αυτή τη μείωση της απόδοσης παίζει και το γεγονός ότι στα δίκτυα WLAN, οι κόμβοι χρησιμοποιούν συνήθως πανκατευθυντικές κεραίες για επικοινωνία με το σημείο AP, η αποτελεσματικότητα των οποίων μετριάζεται από την ίδια τη λειτουργία τους, αφού η μετάδοση των πακέτων δεδομένων πραγματοποιείται προς όλες τις κατευθύνσεις. Για το λόγο αυτό, οι συγγραφείς πραγματοποίησαν μια διεξοδική σύγκριση της χρήσης πανκατευθυντικών και κατευθυντικών κεραιών. Τα πειραματικά αποτελέσματα απέδειξαν μικρότερα ποσοστά καθυστέρησης, απόρριψης δεδομένων και προσπαθειών αναμετάδοσης για τις κατευθυντικές κεραίες, ανεξάρτητα από τον αριθμό των σημείων AP και για μέγεθος πακέτου 250byte, το οποίο θεωρείται ιδανικό μέγεθος πακέτου σε σενάρια χρήσης των δικτύων WLAN εξαιρετικά μεγάλης πυκνότητας [168].

Μεγάλο ρόλο στην απόδοση των δικτύων WLAN παίζει και ο κυκλοφοριακός φόρτος που παρατηρείται κατά τη λειτουργία τους. Για παράδειγμα, στον πίνακα 5.1 παρουσιάζεται η απόδοση τριών δικτύων WLAN διαφορετικών προτύπων IEEE 802.11, από τον οποίο αποδεικνύεται η σημαντική επίδραση της αύξησης του κυκλοφοριακού φόρτου στην απόδοση των δικτύων WLAN [161]. Η αύξηση του κυκλοφορικού φόρτου γενικότερα στον τομέα της δικτύωσης είναι γνωστή ως υπερφόρτωση δικτύου και η ύπαρξή της παρουσιάζει μεγάλο αντίκτυπο στα δίκτυα WLAN ως προς την αύξηση των καθυστερήσεων, την απώλεια πακέτων και γενικότερα οδηγεί σε μια υποβάθμιση του δικτύου [154].

Πίνακας 5.1: Παράδειγμα ρυθμού μετάδοσης δεδομένων ανά χρήστη σε δίκτυα WLAN 802.11 [161]

Πρότυπο IEEE 802.11	**Μέγιστος ρυθμός μετάδοσης δεδομένων (Mbps)**	**Συνθήκες λειτουργίας**	**Ρυθμός μετάδοσης δεδομένων ανά χρήστη**		
			Μικρή κίνηση (2 ενεργοί χρήστες) (Mbps)	**Μεσαία κίνηση (5 ενεργοί χρήστες) (Mbps)**	**Υψηλή κίνηση (10 ενεργοί χρήστες) (Mbps)**
IEEE 802.11a (OFDM)	54	Ιδανικές	17	7	3
		Κανονικές	11	5	2
IEEE 802.11b (DSSS)	11	Ιδανικές	5	2	1
		Κανονικές	3	1	0,5
IEEE 802.11g (CCK, OFDM)	54	Ιδανικές	17	7	3
		Κανονικές	11	5	2

Οι Obelovska, Panova και Karovič Jr (2021) αναφέρουν ότι η διαμεταγωγή ενός δικτύου WLAN εξαρτάται σε μεγάλο βαθμό από τις διεργασίες που υλοποιούνται στο επίπεδο MAC της εκάστοτε τροποποίησης του προτύπου IEEE 802.11. Ταυτόχρονα όμως, αυτές οι διεργασίες του επιπέδου MAC εξαρτώνται σε μεγάλο βαθμό από διάφορες παραμέτρους, όπως είναι ο αριθμός των σταθμών στο δίκτυο και το φορτίο. Με την μαζική ανάπτυξη της κυκλοφορίας που προέρχεται από τις εφαρμογές πολυμέσων, η διαμεταγωγή του δικτύου δείχνει να επηρεάζεται σε μεγάλο βαθμό και από τους τύπους της κυκλοφορίας. Θέλοντας λοιπόν να εξετάσουν όλα αυτά τα στοιχεία, οι συγγραφείς μελέτησαν τον αντίκτυπο που μπορεί να παρουσιάσει η αναλογία κίνησης υψηλής/χαμηλής προτεραιότητας στη διαμεταγωγή ενός δικτύου WLAN με διαφορετικούς αριθμούς κατηγοριών πρόσβασης. Τα αποτελέσματα της προσομοίωσης που πραγματοποιήθηκε γι' αυτό το σκοπό έδειξαν διαφορετική επίδραση της αναλογίας κίνησης υψηλής/χαμηλής προτεραιότητας στην απόδοση του επιπέδου MAC

του δικτύου, ανάλογα με τα διαφορετικά μεγέθη και τις συνθήκες του δικτύου. Πιο συγκεκριμένα, η διαμεταγωγή ενός μεγάλου δικτύου WLAN με δύο κατηγορίες πρόσβασης και με επικρατούσα την κίνηση υψηλής προτεραιότητας είναι σημαντικά υψηλότερη από την περίπτωση χρήσης του δικτύου με τέσσερις κατηγορίες πρόσβασης στο επίπεδο MAC [169].

5.2.2 Καθυστέρηση και διακύμανσή της

Η καθυστέρηση περιγράφει τον χρόνο που απαιτείται για τη μετάδοση ενός πακέτου δεδομένων μεταξύ των κόμβων ενός δικτύου, ενώ η διακύμανσή της περιγράφει τους διαφορετικούς χρόνους μετάδοσης που παρατηρούνται σε μια ροή δεδομένων και είναι ένα μέγεθος χαρακτηριστικό της σταθερότητας ενός δικτύου. Οι μικρότερες τιμές της καθυστέρησης και της διακύμανσής της αυξάνουν την απόδοση του δικτύου [170].

Οι Lopez-Aguilera, Garcia-Villegas και Casademont (2019) μελέτησαν την υποβάθμιση της απόδοσης που παρουσιάζουν τα δίκτυα WLAN με βάση την καθυστέρηση πρόσβασης που μπορεί να παρουσιάσουν ανόμοιοι κόμβοι, λαμβάνοντας υπόψη την πιθανότητα σύγκρουσης και την καθυστέρηση πρόσβασης στο κανάλι [165].

5.2.3 Απώλεια πακέτων

Απώλεια πακέτων σε ένα δίκτυο WLAN ονομάζεται η περίπτωση κατά την οποία τα πακέτα δεδομένων αποτυγχάνουν να φτάσουν στον προορισμό τους για διάφορους λόγους, όπως για παράδειγμα η ύπαρξη παρεμβολών. Σε αυτήν την περίπτωση η απώλεια μετριέται ως αναλογία του αριθμού των πακέτων δεδομένων που λήφθηκαν προς τον αριθμό των πακέτων που στάλθηκαν (αναλογία επιτυχημένης μετάδοσης) και θα πρέπει να είμαι μεγάλη για να παρουσιάζει το δίκτυο μεγάλη απόδοση. Τα δίκτυα WLAN παρουσιάζουν μεγαλύτερη αναλογία απώλειας πακέτων και ποσοστών σφάλματος μετάδοσης δεδομένων σε σύγκριση με τα δίκτυα LAN, παράγοντες που μειώνουν περαιτέρω την απόδοσή τους [171].

5.2.4 Πρωτόκολλα MAC

Σχεδόν κάθε νέα τροποποίηση του αρχικού προτύπου IEEE 802.11 παρουσιάζει νέο πρωτόκολλο MAC με σκοπό την εξάλειψη της πιθανότητας της σπατάλης του εύρους ζώνης στην κατάσταση backoff, αλλά και τη σημαντική βελτίωση της απόδοσης του συνολικού δικτύου [172], [173]. Για την αξιολόγηση των πρωτοκόλλων MAC καθώς και των αλγορίθμων που χρησιμοποιούν αυτά, κάποιοι μελετητές χρησιμοποίησαν τεχνικές αλυσίδας Markov [174], [175]. Πολλοί ερευνητές ασχολήθηκαν μάλιστα μόνο με τους βασικούς αλγόριθμους πρόσβασης που χρησιμοποιούν διάφορα πρωτόκολλα MAC (π.χ., αλγόριθμος DCF με RTS/CTS και αλγόριθμος PCF) [176], [177].

Οι Hassan και συν. (2018) ασχολήθηκαν με την μελέτη της επίδρασης της διαδικασίας BEB, που χρησιμοποιείται στον αλγόριθμο DCF του πρωτοκόλλου MAC, στην απόδοση των δικτύων WLAN. Οι συγγραφείς κατέληξαν στο συμπέρασμα ότι καθώς ο αριθμός των ανταγωνιστικών κόμβων για την πρόσβαση στο μέσο αυξάνεται, η επιμήκυνση του χρόνου backoff είχε ως αποτέλεσμα την υποβάθμιση της διαμεταγωγής του δικτύου. Ένα τέτοιο συμπέρασμα έρχεται σε συμφωνία με παλαιότερες μελέτες, οι οποίες απέδειξαν ότι η διαδικασία BEB αποτελεί βασικό παράγοντα υποβάθμισης της συνολικής απόδοσης των δικτύων WLAN [178].

Οι Gopinath και Nithya (2018) παρουσίασαν μια αναλυτική μελέτη σχετικά με την αξιολόγηση των επιδόσεων του μηχανισμού επίλυσης διενέξεων (contention) σε δίκτυα WLAN 802.11ah, εξετάζοντας

την απόδοση του αλγόριθμου DCF και της διαδικασίας backoff ως προς τη διαμεταγωγή και την καθυστέρηση που παρουσιάζουν τα συγκεκριμένα δίκτυα [179].

Οι Kocak και Karakurt (2019) χρησιμοποίησαν ένα μοντέλο OPNET για την αξιολόγηση της απόδοσης του πρωτοκόλλου MAC σε δίκτυα WLAN 802.11e. Σύμφωνα με τους συγγραφείς, υπάρχουν παράμετροι των πρωτοκόλλων MAC που επηρεάζουν την ποιότητα των υπηρεσιών που παρέχονται από ένα δίκτυο WLAN, όπως οι RSTV (Request to Send Threshold Value), FTV (Fragmentation Threshold Value) και BS (Buffer Size), οι οποίες επηρεάζουν άμεσα την απόδοση του δικτύου. Η παράμετρος RSTV χρησιμοποιείται στον μηχανισμό RTS/CTS του πρωτοκόλλου CSMA/CA για την πρόληψη συγκρούσεων και καθορίζει το κατώφλι ενεργοποίησής του. Η παράμετρος FTV χρησιμοποιείται για την αποστολή πακέτων μεγάλου μεγέθους διαιρώντας τα σε κατάλληλα τμήματα κατά τη μετάδοση CSMA/CA, μειώνοντας την απώλεια πακέτων σε ένα δίκτυο WLAN. Η παράμετρος BS χρησιμοποιείται επίσης στο πρωτόκολλο CSMA/CA και επηρεάζει άμεσα την απόδοση του δικτύου [180].

Οι Mukta και Gupta (2020) μελέτησαν την επίδραση του μηχανισμού περιορισμένης προσωρινής αποθήκευσης (buffering) στην απόδοση του μηχανισμού DCF των δικτύων WLAN 802.11. Σε αυτή τους τη μελέτη χρησιμοποίησαν ένα μοντέλο για την πρόβλεψη της διαμεταγωγής και της καθυστέρησης του δικτύου για διαφορετικά μεγέθη buffering, καθώς μοντέλο NS-2 για την προσομοίωση του δικτύου. Τα αποτελέσματα της προσομοίωσης έδειξαν ότι το μεγαλύτερο μέγεθος του buffer αύξανε τη διαμεταγωγή του δικτύου, αλλά προκαλούσε ταυτόχρονα σοβαρή αύξηση της καθυστέρησης. Επομένως, δεν ήταν κατάλληλο για εφαρμογές σε πραγματικό χρόνο, όπως το VoIP [181].

Οι Bedi, Sharma και Gupta (2020) αξιολόγησαν την απόδοση των δικτύων WLAN 802.11e εξετάζοντας τους μηχανισμούς DCF και PCF ως προς την επίδραση που έχουν πάνω στην παρεχόμενη ποιότητα QoS των υπηρεσιών πραγματικού χρόνου. Η αξιολόγηση αυτή έγινε χρησιμοποιώντας μια μεγάλη ποικιλία μεθόδων [182].

Οι Eyadeh, Jarrah και Aljumaili (2019) μελέτησαν τα όρια απόδοσης των δικτύων WLAN 802.11n βασιζόμενοι στην ανάλυση του αλγορίθμου PCF του πρωτοκόλλου MAC και χρησιμοποιώντας ένα αναλυτικό μοντέλο υπολογισμού της θεωρητικής μέγιστης διαμεταγωγής και του χρόνου καθυστέρησης που παρουσιάζονται. Οι συγγραφείς ανέπτυξαν επίσης, ένα μοντέλο προσομοίωσης για τη μελέτη αυτών των ορίων απόδοσης με χρήση μοντελοποίησης OPNET, με σκοπό την εξέταση των επιπτώσεων που έχουν το μέγεθος των πακέτων και ο αριθμός των σταθμών στη θεωρητική μέγιστη διαμεταγωγή και το χρόνο καθυστέρησης. Τα αποτελέσματα της μελέτης έδειξαν αύξηση του χρόνου καθυστέρησης τόσο με την αύξηση του μεγέθους των πακέτων όσο και με την αύξηση του αριθμού των σταθμών, ενώ ως προς τη θεωρητική μέγιστη μεταγωγή έδειξαν αύξηση με την αύξηση του μεγέθους των πακέτων και μείωση με την αύξηση του αριθμού των σταθμών [183].

5.2.5 Περιβάλλοντα διάδοσης σημάτων ραδιοσυχνότητας

Η επίδραση των διαφόρων περιβαλλόντων διάδοσης των σημάτων ραδιοσυχνότητας ως προς την απόδοση των δικτύων WLAN έχει εξεταστεί σε πολλές μελέτες, στις οποίες έχουν χρησιμοποιηθεί πολλά διαφορετικά σενάρια μετρήσεών της, όπως σε χώρους γραφείων [184], σε κατοικίες αστικών περιοχών [185], σε βιομηχανικά περιβάλλοντα [186], κλπ. Στις μελέτες αυτές σχεδιάστηκαν πλαίσια που συνδυάζουν τα επίπεδα PHY και MAC, με σκοπό την επίτευξη μεγαλύτερης απόδοσης, μέσω μείωσης της καθυστέρησης μετάδοσης των δεδομένων στα δίκτυα WLAN. Στις μελέτες αυτές εξετάστηκε επίσης, η επίδραση της διαμόρφωσης και της θέσης εγκατάστασης των σημείων AP των

δικτύων WLAN, στοιχεία τα οποία επίσης βρέθηκε ότι επηρεάζουν την απόδοση τους [184] - [189]. Σύμφωνα με τον A. Aijaz (2020), τα δίκτυα WLAN δεν θεωρούνται κατάλληλα σε βιομηχανικά περιβάλλοντα με σκοπό την εξυπηρέτηση εφαρμογών ελέγχου, λόγω της ανεπαρκούς αξιοπιστίας και του μη ντετερμινιστικού λανθάνοντος χρόνου που παρουσιάζουν [190].

5.2.6 Πρωτόκολλα δρομολόγησης και μετάδοσης

Σε άλλες μελέτες έχει εξεταστεί και διερευνηθεί μέσω προσομοίωσης η επίδραση των πρωτοκόλλων δρομολόγησης στην απόδοση ενός τυπικού δικτύου WLAN 802.11 [191]. Οι Rezaei, Gharib και Movaghar (2018) αναφέρουν ότι η διαμεταγωγή από άκρο σε άκρο της επικοινωνίας πολλαπλών αλμάτων σε ad hoc δίκτυα WLAN επηρεάζεται σε μεγάλο βαθμό από την ύπαρξη συγκρούσεων μεταξύ των κόμβων προώθησης. Οι συγγραφείς εστιάζουν το συγκεκριμένο ζήτημα στο γεγονός ότι η αποστολή περισσότερων πακέτων από το μέγιστο όριο που μπορεί να υποστηρίξει η επιτεύξιμη διαμεταγωγή έχει ως αποτέλεσμα την υποβάθμιση της διαμεταγωγής αυτής λόγω δημιουργίας μεγάλου αριθμού διαμαχών για την πρόσβαση στο μέσο από τους κόμβους προώθησης. Για την αποφυγή αυτού του ζητήματος, οι κόμβοι αποστολής των πακέτων δεδομένων θα πρέπει να γνωρίζουν τη μέγιστη διαμεταγωγή που παρουσιάζει το δίκτυο από άκρο σε άκρο, η οποία εξαρτάται από πολλούς παράγοντες, όπως οι περιορισμοί του φυσικού επιπέδου, οι ιδιότητες του χρησιμοποιούμενου πρωτοκόλλου MAC, η πολιτική δρομολόγησης και η διανομή των κόμβων [192].

Οι Raza και συν. (2020) μελέτησαν και αξιολόγησαν την απόδοση διαφόρων πρωτοκόλλων δρομολόγησης, λαμβάνοντας ως παράγοντες απόδοσης την διαμεταγωγή και την καθυστέρηση που παρουσίαζαν σε σχέση με την αύξηση της πυκνότητας των χρηστών του δικτύου [193]. Ανάλογη μελέτη πραγματοποιήθηκε και από τους Nisar και συν. (2020), με τους συγγραφείς να εστιάζουν στο τρόπο με τον οποίο τα διαφορετικά χαρακτηριστικά των πρωτοκόλλων δρομολόγησης μπορούν να επιδράσουν στην ποιότητα των παρεχόμενων υπηρεσιών από το δίκτυο [194].

Κάτι αντίστοιχο έχει πραγματοποιηθεί και για τα πρωτόκολλα μετάδοσης [195]. Ο A. Z. Yonis (2019) μελέτησε και αξιολόγησε της απόδοση της τεχνικής μετάδοσης OFDM σε δίκτυα WLAN 802.11ac σε διαφορετικά σενάρια εφαρμογής, εξετάζοντας την καθυστέρηση που παρουσιάζεται σε καθένα από αυτά [196].

5.2.7 Ισχύς σημάτων ραδιοσυχνοτήτων και τύπος κυκλοφορίας

Υπάρχουν επίσης διάφορες μελέτες στις οποίες έχει αναλυθεί η επίδραση που προκαλεί ο συνδυασμός της ισχύος των σημάτων ραδιοσυχνοτήτων και του τύπου της κυκλοφορίας (π.χ. δεδομένα ήχου ή εικόνας) στην απόδοση των δικτύων WLAN [197]. Η απόδοση ενός δικτύου WLAN εξαρτάται άμεσα από την ισχύ του σήματος ραδιοσυχνοτήτων και ποικίλλει από τοπολογία σε τοπολογία, η οποία συμβάλει σε μεγάλο βαθμό στην επίτευξη ευελιξίας ως προς την κινητικότητα των κόμβων. Επίσης, η χρήση πολύτιμων πόρων που καταναλώνονται για την εξυπηρέτηση υπηρεσιών που βασίζονται στο Διαδίκτυο, όπως η πρόσβαση σε ιστότοπους, η αποστολή email και η μεταφορά αρχείων, επηρεάζει σε μεγάλο βαθμό την απόδοση των δικτύων WLAN, με αποτέλεσμα την υποβάθμιση της ικανότητας ταυτόχρονης εξυπηρέτησης εφαρμογών μεταφοράς δεδομένων φωνής μέσω των ασύρματων δικτύων. Για το λόγο αυτό, η παροχή υψηλής ποιότητας QoS από τα δίκτυα WLAN σε εφαρμογές πολυμέσων πραγματικού χρόνου, όπως VoIP (Voice over Internet Protocol), βίντεο μέσω IP και διαδικτυακών παιχνιδιών αποτελεί ένα ζήτημα [198].

Η ισχύς του σήματος είναι αντιστρόφως ανάλογη της απόστασης που έχουν οι ασύρματες συσκευές από τα σημεία AP του δικτύου. Η απόσταση των ασύρματων συσκευών έχει μεγάλη σημασία για την

αδιάλειπτη λήψη των δεδομένων, λόγω του γεγονότος ότι κάθε σημείο AP του δικτύου έχει μία συγκεκριμένη περιοχή στην οποία η ισχύς του σήματος που εκπέμπεται είναι στο μέγιστο. Η απόσταση στην οποία κάποια ασύρματη συσκευή μπορεί να συνδεθεί σε ένα σημείο AP ποικίλλει ανάλογα με τον προσανατολισμό της κεραίας. Οι χρήστες smartphone, ειδικότερα, μπορεί να δουν την ισχύ της σύνδεσής τους να αυξάνεται ή να μειώνεται απλώς περιστρέφοντας τη συσκευή σε διαφορετικές γωνίες. Επιπλέον, ορισμένα σημεία AP χρησιμοποιούν κατευθυντικές κεραίες που επιτρέπουν μεγαλύτερη εμβέλεια σε κάποιες περιοχές, αλλά μικρότερη σε άλλες περιοχές, ανάλογα με το διάγραμμα εκπομπής των κεραιών [154].

Η επίδραση που έχει αυτή η εξάρτηση της απόστασης των ασύρματων συσκευών από τα σημεία AP στην απόδοση των δικτύων WLAN μελετήθηκε τα τελευταία χρόνια από μια σειρά ερευνών που στόχευσαν στον εντοπισμό της εύρεσης της ποιότητας QoS που παρουσιάζουν διαφορετικοί τύποι κυκλοφορίας. Στις μελέτες αυτές βρέθηκε ότι τα δεδομένα ήχου παρουσίαζαν μικρότερες αλλοιώσεις σε σύγκριση με τα δεδομένα εικόνας και βίντεο [199], [200].

Η μελέτη του A. Chhabra (2020) βασίστηκε σε παλαιότερες μελέτες που αφορούσαν τη δυνατότητα υποστήριξης των εφαρμογών VoIP από τα δίκτυα WLAN και τη σχέση μεταξύ της χρήσης των πόρων στα συγκεκριμένα δίκτυα, αλλά και της ποιότητας των κλήσεων VoIP που μεταδίδονται μέσω του ασύρματου μέσου. Ο συγγραφέας αναφέρει ότι το φορτίο του δικτύου επηρεάζει την απόδοση των κλήσεων και μάλιστα ότι η ύπαρξη μεγάλου φορτίου μπορεί να έχει ως αποτέλεσμα κακή ποιότητα φωνητικών κλήσεων. Ο συγγραφέας τονίζει επίσης ότι η μελέτη της αύξησης της ποιότητας το QoS είναι απαραίτητη για τη δυνατότητα υποστήριξης των εφαρμογών πραγματικού χρόνου, γενικότερα, από τα δίκτυα WLAN [201]. Οι Ali, Dhimish και Alsmadi (2020) αναφέρουν ότι η εύρυθμη λειτουργία της εφαρμογής VoIP στα δίκτυα WLAN απαιτεί την επίτευξη βέλτιστης απόδοσής τους, κάτι το οποίο θα οδηγήσει στην εκπλήρωση όλων των απαιτούμενων χαρακτηριστικών και παραμέτρων των ποιότητας QoS [198].

Οι Govindarajan και Mohanapriya (2019) ανέλυσαν τη δυνατότητα εκπομπής δεδομένων βίντεο μέσω δικτύου WLAN, λαμβάνοντας υπόψη τη χρήση του αλγόριθμου RMCAT (Real-Time Media Congestion Avoidance) και την απόδοσή του σε διάφορες συνθήκες δικτύου και καναλιού. Τα αποτελέσματα της μελέτης έδειξαν ότι η απόδοση της μετάδοσης βίντεο επηρεάζεται από την απόσταση των χρηστών από το σημείο AP, αλλά και από τις εκάστοτε συνθήκες καναλιού, καθώς ο έλεγχος συμφόρησης του αλγόριθμου RMCAT λαμβάνει υπόψη του τις απώλειες πακέτων, λόγω αυτών των συνθηκών, ως συμφόρηση [202].

5.3 Αντίκτυπος παρεμβολών και θορύβων στην απόδοση των δικτύων WLAN

Τα ζητήματα των παρεμβολών στα δίκτυα WLAN προκαλούνται από δύο μεγάλες ομάδες σημάτων όπως είναι οι παρεμβολές ραδιοσυχνοτήτων RFI (Radio Frequency Interference) και οι ηλεκτρομαγνητικές παρεμβολές EMI (ElectroMagnetic Interference), γνωστές και ως ηλεκτρομαγνητικός θόρυβος [203].

5.3.1 Παρεμβολές RFI

Τα σήματα RFI είναι παρεμβολές στενής ζώνης από τη φύση τους, που εμφανίζονται στη μη αδειοδοτημένη ζώνη ISM των 2,4GHz. Οι οικιακές συσκευές που λειτουργούν σε αυτήν την ζώνη συχνοτήτων μπορούν να αποτελέσουν πιθανές πηγές παρεμβολών RFI για τα σημεία AP των δικτύων WLAN της ίδιας ζώνης λειτουργίας. Αντίθετα, η λειτουργία των δικτύων WLAN στη ζώνη συχνοτήτων των 5GHz τους δίνει το πλεονέκτημα της αντιμετώπισης λιγότερων παρεμβολών σε

σύγκριση αυτά που λειτουργούν στην πιο πολυσύχναστη ζώνη ISM των 2,4GHz. Τα δίκτυα WLAN που λειτουργούν στη ζώνη συχνοτήτων των 5GHz μπορεί να επηρεαστούν, για παράδειγμα, από παρακείμενα συστήματα ραντάρ, τα οποία χρησιμοποιούν την ίδια ζώνη συχνοτήτων για τη λειτουργία τους [204]. Για τον μετριασμό των παρεμβολών στα 5GHz, τα σημεία AP των δικτύων WLAN χρησιμοποιούν ενσωματωμένες λειτουργίες, όπως αλγόριθμους DFS (Dynamic Frequency Selection) και TPS (Transmit Power Control) [205], [206].

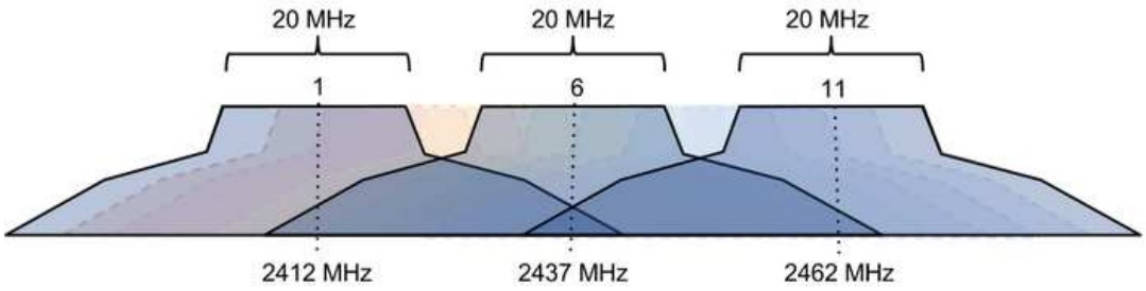
Οι παρεμβολές RFI συνδέονται σε μεγάλο βαθμό με την υποβάθμιση της απόδοσης και της ποιότητας QoS των υπηρεσιών που παρέχονται από ένα δίκτυο WLAN, καθώς η ύπαρξή τους επηρεάζει ένα σύστημα ή μια συσκευή σε τέτοιο βαθμό που να λειτουργεί εκτός των κανονικών τεχνικών παραμέτρων του [203]. Σύμφωνα με τους Haider, Saleem και Jamal (2018), το επίπεδο της υποβάθμισης της απόδοσης των ασύρματων δικτύων που προκαλείται από την ύπαρξη παρεμβολών εξαρτάται σε μεγάλο βαθμό από ένα μέγεθος το οποίο είναι γνωστό ως εμβέλεια παρεμβολών (interference range). Οι συγγραφείς αναφέρουν ότι ως εμβέλεια παρεμβολών ονομάζεται η περιοχή στην οποία η μετάδοση ενός κόμβου μπορεί να διακοπεί από την παρεμβολή που δημιουργεί ένας άλλος κόμβος, και μπορεί να επηρεάσει έντονα την απόδοση των δικτύων WLAN, λόγω της αύξησης του αριθμού των συγκρούσεων που εμφανίζονται σε αυτή την περιοχή, κάτι που μπορεί να οδηγήσει ακόμη και σε διακοπή λειτουργίας των κόμβων της περιοχής ή ακόμα και ολόκληρου του δικτύου. Σύμφωνα με τους συγγραφείς, το εύρος της εμβέλειας παρεμβολών μπορεί να μοντελοποιηθεί ως συνάρτηση της απόστασης μεταξύ των κόμβων του δικτύου που παρεμβάλλονται και των χαρακτηριστικών του φυσικού επιπέδου του δικτύου [207].

Στη βιβλιογραφία έχουν παρουσιαστεί μελέτες για διάφορους τύπους παρεμβολών RFI, οι οποίοι μπορούν να προκαλέσουν υποβάθμιση της απόδοσης των δικτύων WLAN. Οι βασικότεροι από αυτούς τους τύπους είναι [203], [207] – [209]: (α) οι παρεμβολές παρακείμενου καναλιού, (β) οι παρεμβολές συν-καναλιού, (γ) οι παρεμβολές ομογενών τεχνολογιών και (δ) οι παρεμβολές ετερογενών τεχνολογιών.

1) Παρεμβολές παρακείμενου καναλιού

Οι παρεμβολές παρακείμενου καναλιού ACI (Adjacent Channel Interference) προκαλούνται στις περιπτώσεις που τα σήματα των εκπομπών δύο παρακείμενων καναλιών έχουν διαφορετική ισχύ. Σε αυτές τις περιπτώσεις, το σήμα με την μεγαλύτερη ισχύ θα δημιουργήσει παρεμβολές στην εκπομπή του παρακείμενου καναλιού με την μικρότερη ισχύ [209]. Οι λόγοι για τους οποίους μπορεί να εμφανιστεί παρεμβολή ACI είναι αρκετές, όπως το ανεπαρκές φιλτράρισμα των προϊόντων διαμόρφωσης παρεμβολής σε ασύρματα συστήματα, ο κακός συντονισμός εκπομπής ή ο κακός έλεγχος της συχνότητας εκπομπής των παρακείμενων καναλιών [203]. Ιδιαίτερα ο τελευταίος λόγος είναι η σοβαρότερη αιτία εμφάνισης παρεμβολών ACI στην περίπτωση των δικτύων WLAN που λειτουργούν στη ζώνη των 2,4GHz. Τα δίκτυα WLAN που λειτουργούν σε επικαλυπτόμενα παρακείμενα κανάλια προκαλούν αναβολή ή ακόμη και καταστροφή της μετάδοσης των συσκευών, λόγω παρεμβολών ACI που οδηγούν σε περιττές διαμάχες πρόσβασης στο μέσο μεταξύ των συσκευών, αναμεταδόσεις πλαισίων δεδομένων και χαμηλούς ρυθμούς μετάδοσης δεδομένων, στοιχεία που τελικά έχουν ως αποτέλεσμα την υποβάθμιση της απόδοσης και της ποιότητας QoS του δικτύου [209]. Αντίθετα, στα δίκτυα WLAN που λειτουργούν στη ζώνη των 5GHz, οι παρεμβολές ACI δεν αποτελούν ζήτημα, καθώς οι κεντρικές συχνότητες των καναλιών της συγκεκριμένης ζώνης έχουν μεγάλη απόσταση μεταξύ τους, με αποτέλεσμα να μην μπορεί να υπάρξει ζήτημα επικάλυψής τους, ακόμα και στην περίπτωση εφαρμογής της τεχνικής channel bonding για αύξηση της χωρητικότητας και του εύρους ζώνης [210].

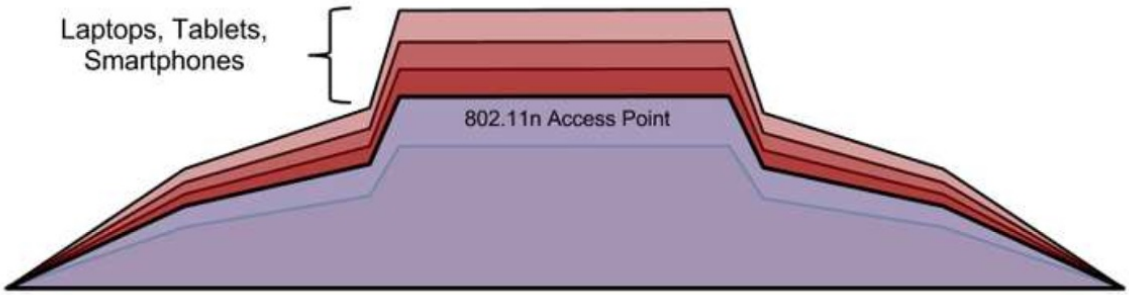
Ένας απλός τρόπος ελαχιστοποίησης του ζητήματος των παρεμβολών ACI στα δίκτυα WLAN που λειτουργούν στη ζώνη συχνοτήτων των 2,4GHz είναι η επιλογή καναλιών εκπομπής που να μην παρουσιάζουν επικάλυψη. Αν και η μπάντα των 2,4GHz υποστηρίζει 11 κανάλια, μόνο τα τρία από αυτά έχουν κεντρικές συχνότητες που δεν επικαλύπτονται (Εικ. 5.1). Έτσι, η επιλογή μόνο των καναλιών 1, 6 και 11 για εκπομπή δίνει τη δυνατότητα ελαχιστοποίησης της εμφάνισης παρεμβολών ACI, αφού όπως φαίνεται στην εικόνα 5.1, σε αυτήν την περίπτωση οι ασύρματες συσκευές που τις χρησιμοποιούν θα μπορούσαν να μεταδίδουν δεδομένα ταυτόχρονα, χωρίς κανένα πρόβλημα [203], [209].



Εικόνα 5.1: Χρήση μη επικαλυπτόμενων παρακείμενων καναλιών για ελαχιστοποίηση του ζητήματος των παρεμβολών ACI [203]

2) Παρεμβολές συν-καναλιού

Οι παρεμβολές συν-καναλιού CCI (Co-Channel Interference) εμφανίζονται στις περιπτώσεις που οι ασύρματες συσκευές ενός δικτύου WLAN χρησιμοποιούν το ίδιο κανάλι, όπως φαίνεται στην εικόνα 5.2. Οι παρεμβολές CCI μπορεί να δημιουργηθούν στις περιπτώσεις κακού προγραμματισμού της χρήσης των συχνοτήτων από τις ασύρματες συσκευές των δικτύων ή στις περιπτώσεις δικτύων WLAN με εξαιρετικά μεγάλη πυκνότητα συσκευών [203].



Εικόνα 5.2: Φαινόμενο παρεμβολών CCI [203]

Όπως φαίνεται στην εικόνα 5.2, ασύρματες συσκευές, όπως φορητοί υπολογιστές, tablet και έξυπνα τηλέφωνα, παρουσιάζουν διαφορετικά επίπεδα ισχύος των σημάτων που εκπέμπουν. Λειτουργώντας στην ίδια συχνότητα (άρα και στο ίδιο κανάλι), ο χρόνος λειτουργίας τους θα πρέπει να διαχειρίζεται με τέτοιο τρόπο ώστε να εναλλάσσεται η εκπομπή τους. Μια τέτοια διαχείριση μπορεί να πραγματοποιηθεί μόνο αν οι συσκευές που θέλουν να εκπέμψουν, καθυστερήσουν τη μετάδοσή τους, αν το μέσο χρησιμοποιείται από κάποια άλλη συσκευή [209]. Κάτι τέτοιο όμως συνήθως έχει ως αποτέλεσμα την υποβάθμιση της ποιότητας QoS τους [203]. Σε περίπτωση όμως που μια τέτοια διαχείριση δεν έχει πραγματοποιηθεί, η ρύθμιση των συσκευών αυτών για λειτουργία στο ίδιο κανάλι,

οδηγεί σε περιττές διαμάχες πρόσβασης στο μέσο. Παρόλο που οι συσκευές αυτές, λειτουργούν όπως υπαγορεύονται από τους μηχανισμούς CSMA/CA, η ύπαρξη αυξημένων διαμαχών πρόσβασης στο μέσο, μπορεί να υποβαθμίσει σοβαρά τη συνολική απόδοση του δικτύου [209].

Αν και ο αντίκτυπος των παρεμβολών CCI θα μπορούσαν να μειωθούν με σωστό συντονισμό και προγραμματισμό καναλιών, οι συγκεκριμένες παρεμβολές είναι απλά αναπόφευκτες σε δίκτυα WLAN μεγάλης πυκνότητας χρηστών, που λειτουργούν στη ζώνη των 2,4GHz. Οι παρεμβολές που προκαλούνται από το συνδυασμό του μεγάλου αριθμού των χρηστών και του περιορισμένου αριθμού συχνοτήτων στη ζώνη των 2,4GHz, είναι μία από τις κύριες αιτίες χαμηλής απόδοσης των δικτύων WLAN. Όταν ένα μεγάλο πλήθος συσκευών λειτουργούν σε έναν περιορισμένο αριθμό συχνοτήτων, η πιθανότητα για ύπαρξη συγκρούσεων και καταστροφής του μεταδιδόμενου σήματος αυξάνεται, δημιουργώντας την ανάγκη για μεγάλο αριθμό αναμεταδόσεων πλαισίου επιπέδου MAC, που υποβαθμίζουν τη διαμεταγωγή του δικτύου. Επιπλέον, σε ένα περιβάλλον υψηλής συμφόρησης, απαιτείται περισσότερος χρόνος σε μια μεμονωμένη συσκευή για να ολοκληρώσει τη μετάδοσή της, λόγω των διαδικασιών πρόσβασης μέσου CSMA/CA, κάτι που οδηγεί σε περαιτέρω μείωση της απόδοσης του δικτύου. Κάτι τέτοιο είναι ιδιαίτερα εμφανές στα αστικά περιβάλλοντα, όπου τεράστιοι αριθμοί σημείων AP των δικτύων WLAN και ασύρματων συσκευών λειτουργούν σε κοντινές αποστάσεις [209].

3) Παρεμβολές ομογενών τεχνολογιών

Οι παρεμβολές ομογενών τεχνολογιών εμφανίζονται όταν οι παρεμβολές που υπάρχουν σε ένα δίκτυο προέρχονται από σήματα της ίδιας τεχνολογίας και μπορούν να είναι παρεμβολές CCI ή ACI. Σε ορισμένες περιπτώσεις, ο αριθμός των σημάτων παρεμβολής μπορεί να είναι μεγαλύτερος από ένα, ανάλογα με τον τύπο της ζώνης συχνότητας που χρησιμοποιεί το σήμα με την μεγαλύτερη ισχύ [210]. Τέτοιες παρεμβολές εμφανίζονται συχνά σε δίκτυα WLAN που μπορούν να υποστηρίξουν τη λειτουργία συσκευών διαφόρων τροποποιήσεων του βασικού προτύπου IEEE 802.11, όπως το ζήτημα της διαχείρισης της συνύπαρξης των διαφορετικών προτύπων, όπως για παράδειγμα των IEEE 802.11b και IEEE 802.11g, είναι εμφανές [211].

4) Παρεμβολές ετερογενών τεχνολογιών

Η κατανόηση των παρεμβολών ετερογενών τεχνολογιών είναι ζωτικής σημασίας για την εύρυθμη λειτουργία και συνύπαρξη δικτύων που χρησιμοποιούν διαφορετικές ασύρματες τεχνολογίες και μοιράζονται παρόμοιες μη αδειοδοτημένες ζώνες συχνοτήτων [210], [211]. Όσον αφορά τα δίκτυα WLAN οι παρεμβολές αυτές εμφανίζονται όταν λειτουργούν στον ίδιο χώρο με άλλα ασύρματα δίκτυα, όπως δίκτυα LTE στην μπάντα των 2,4GHz [212], δίκτυα LTE στην μπάντα των 5GHz [213], συστημάτων ραντάρ [214], κλπ.

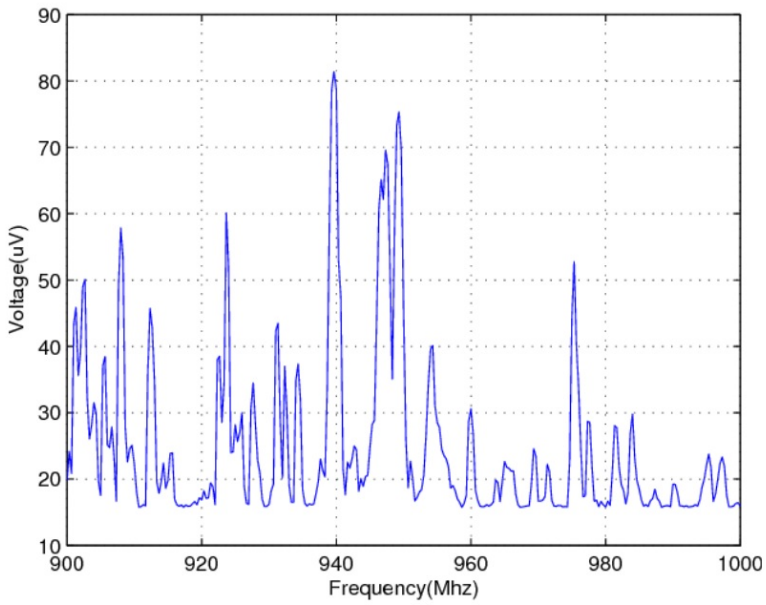
Λόγω των ζητημάτων συνύπαρξης που μπορεί να οδηγήσουν σε παρεμβολές ετερογενών τεχνολογιών, αρκετές μελέτες έχουν αξιολογήσει την μείωση της απόδοσης των δικτύων WLAN που προκαλείται από αυτές και έχουν προτείνει διάφορες τεχνικές καταστολής αυτών των παρεμβολών [215] – [217]. Από τις μελέτες αυτές προκύπτει ένα σημαντικό συμπέρασμα. Τα δίκτυα WLAN υπόκεινται ολοένα και περισσότερο σε παρεμβολές ετερογενών τεχνολογιών, λόγω της αυξημένης χρήσης της μη αδειοδοτημένης ζώνης των 2,4GHz από λύσεις επικοινωνίας IoT και κυψελοειδών δικτύων. Λόγω της διαφορετικότητας που παρουσιάζουν αυτές οι πηγές παρεμβολών, η διατήρηση της απόδοσης των δικτύων WLAN σε υψηλά επίπεδα γίνεται όλο και πιο δύσκολη [216].

5.3.2 Θόρυβος EMI

Οι παρεμβολές ή θόρυβος EMI είναι ευρείας ζώνης από τη φύση τους και μπορούν να εμφανιστούν στις ζώνες συχνοτήτων 2,4GHz και 5GHz, προκαλώντας πολύ μεγαλύτερα ζητήματα στους χρήστες των δικτύων WLAN σε σύγκριση με τις παρεμβολές RFI [204]. Η δημιουργία των προβλημάτων που παρουσιάζουν οι παρεμβολές EMI στα δίκτυα WLAN είναι τόσο σημαντικές, αφού η ύπαρξή τους μπορεί να οδηγήσει ακόμη και στην απενεργοποίηση ενός ολόκληρου δικτύου, κάτι το οποίο δεν είναι τόσο αποτελεσματικό ούτε με τη χρήση ενός παρεμβολέα ασύρματου δικτύου (wireless network jammer) συντονισμένου στη συχνότητα λειτουργίας του WLAN [203]. Οι παρεμβολές EMI μπορεί να προέρχονται από πολλές διαφορετικές πηγές και, αν και συχνά τα ζητήματα που δημιουργούν μπορούν να περιοριστούν μέσω ενός καλά σχεδιασμένου δικτύου WLAN, ουσιαστικά δεν μπορούν να εξαλειφθούν πλήρως [204].

Στην περίπτωση που κοντά στην ανάπτυξη ενός δικτύου WLAN υπάρχουν συσκευές όπως, φούρνοι μικροκυμάτων, συσκευές Bluetooth, ασύρματα τηλέφωνα, κλπ., σε χρήση, παρατηρείται η εμφάνιση θορύβου EMI, αλλά και παρεμβολών ετερογενών τεχνολογιών, στα μεταδιδόμενα ασύρματα σήματα Wi-Fi. Πολλές φορές, αυτά τα σήματα παρεμβολών ή θορύβου μπορεί να είναι αρκετά ισχυρά ώστε να αποτρέπεται σε έναν ασύρματο πελάτη να έχει πρόσβαση στο δίκτυο WLAN για αόριστο χρονικό διάστημα [218].

Ο παλμικός θόρυβος αποτελεί ένα από τα παραδείγματα των παρεμβολών EMI και μπορεί να δημιουργηθεί κάθε φορά που η λειτουργία μιας ηλεκτρικής συσκευής ξεκινά ή διακόπτεται απότομα. Ηλεκτρικές συσκευές που μπορούν να δημιουργήσουν παλμικό θόρυβο είναι οι ηλεκτρικοί κινητήρες, οι ηλεκτρικοί φούρνοι, ο εξοπλισμός συγκόλλησης, οι ροοστάτες φωτός, καθώς και τα καλώδια ρεύματος στις περιπτώσεις εμφάνισης ηλεκτρικού τόξου και ηλεκτρικού σπινθήρα [219].



Εικόνα 5.3: Το φάσμα συχνοτήτων του παλμικού θορύβου [203]

Στην εικόνα 5.3 φαίνεται ένα παράδειγμα μέτρησης του ηλεκτρομαγνητικού πεδίου όπως αυτό διαμορφώνεται από τις παρεμβολές που δημιουργεί ο παλμικός θόρυβος των οικιακών συσκευών. Όπως μπορεί εύκολα να διαπιστωθεί από την ανάγνωση της εικόνας 5.3, τα σήματα παρεμβολής που προέρχονται από οικιακές συσκευές λόγω της δημιουργίας παλμικού θορύβου περιλαμβάνουν μια

ευρεία ζώνη συχνοτήτων [203]. Το πλάτος του θορύβου που παρατηρείται στις διάφορες συχνότητες μπορεί εύκολα να επηρεάσει τη λειτουργία των δικτύων WLAN που λειτουργούν σε αυτές τις συχνότητες [220].

5.4 Αντίκτυπος χρήσης πρωτοκόλλων ασφάλειας στην απόδοση των δικτύων WLAN

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, τα θέματα ασφάλειας που παρουσίαζαν κατά καιρούς τα δίκτυα WLAN αύξησαν την ανάγκη εφαρμογής ισχυρών μηχανισμών ασφαλείας με σκοπό την προστασία των πληροφοριών που μεταφέρονταν σε αυτά. Κατά συνέπεια, κατά καιρούς, αναπτύχθηκαν διάφορα πρωτόκολλα και μηχανισμοί ασφαλείας για την ενίσχυση της ασφάλειας των δικτύων WLAN. Η εφαρμογή των πρωτοκόλλων ασφαλείας και των μηχανισμών κρυπτογράφησης που περιλαμβάνουν αυξάνει, όμως, την γενική επιβάρυνση των πακέτων που μεταφέρονται εντός των δικτύων, κάτι που τελικά αποτελεί σοβαρό εμπόδιο στην επίτευξη της θεμιτής ποιότητας QoS για τις υπηρεσίες που παρέχονται από τα δίκτυα WLAN [163]. Εκτός από την υποβάθμιση της παρεχόμενης ποιότητας QoS, μελέτες απέδειξαν ότι οι μηχανισμοί ασφαλείας επηρεάζουν και την απόδοση των δικτύων WLAN ως προς την προκύπτουσα διαμεταγωγή, την απώλεια πακέτων, τον χρόνο απόκριση, την διακύμανση της καθυστέρησης, το κόστος κρυπτογράφησης και τον χρόνο πραγματοποίησης των διαδικασιών ελέγχου ταυτότητας [221] – [225].

Οι Kolahi και Almatrook (2017) μελέτησαν και ανέλυσαν τις επιπτώσεις των πρωτοκόλλων ασφαλείας στην απόδοση των ροών κυκλοφορίας TCP και UDP και διαπίστωσαν ότι την επηρεάζουν αρνητικά. Πιο συγκεκριμένα, ερεύνησαν την απόδοση ενός δικτύου WLAN 802.11ac χωρίς ασφάλεια και με το πρωτόκολλο ασφάλειας WPA2. Τα αποτελέσματα έδειξαν ότι, με την εφαρμογή του πρωτοκόλλου ασφάλειας WPA2, η διαμεταγωγή του πρωτοκόλλου μεταφοράς TCP σε συνδυασμό με πρωτόκολλα δικτύου IPv4 και IPv6 μειώθηκε κατά μέσο όρο κατά 16,79% και 10,22%, αντίστοιχα, ενώ εκείνη του UDP με IPv4 και IPv6 κατά 18,07% και 12,99%, αντίστοιχα. Και για τις δύο ροές κυκλοφορίας παρατηρήθηκε επίσης αύξηση της καθυστέρησης μεταφοράς τους [226]. Σε ανάλογα συμπεράσματα κατέληξε και η μελέτη των Tsetse και συν. (2018), οι οποίοι εξέτασαν τον αντίκτυπο της χρήσης πρωτοκόλλων ασφαλείας σε δίκτυα WLAN 802.11ac, με τη μόνη διαφορά ότι τα ποσοστά της μείωσης στην απόδοση των ροών κυκλοφορίας TCP και UDP που βρέθηκαν ήταν σαφώς μικρότερα. Οι συγγραφείς μάλιστα διαπιστώνοντας ότι τα ποσοστά μείωσης και σε άλλες παραμέτρους (καθυστέρηση και διακύμανσή της, αναλογία απώλειας πακέτων και χρόνος σύνδεσης των ασύρματων συσκευών στο δίκτυο) ήταν αντίστοιχα μικρά, θεώρησαν ότι αυτός ο αντίκτυπος των μηχανισμών ασφαλείας στην απόδοση των δικτύων WLAN 802.11ac θα μπορούσε να οφείλεται και σε άλλους παράγοντες, όπως η ύπαρξη συγκρούσεων πρόσβασης καναλιού, η ύπαρξη παρεμβολών, κλπ. [227].

Στην ίδια μελέτη, οι Kolahi και Almatrook (2017) μελέτησαν τον αντίκτυπο που έχει η χρήση του πρωτόκολλου ασφάλειας WPA2 στο εύρος ζώνης ενός δικτύου WLAN 802.11ac για πρωτόκολλα δικτύου IPv4 και IPv6 με χρήση λειτουργικού συστήματος Windows 8.1. Τα αποτελέσματα των αναλύσεων απέδειξαν μείωση του εύρους ζώνης του δικτύου (της τάξης των 850Mbps για ροή UDP και 700Mbps για ροή TCP σε σύγκριση με το θεωρητικό εύρος ζώνης του 1Gbps των δικτύων WLAN 802.11ac), κάτι που αποδεικνύει μείωση της διαμεταγωγής του, στην περίπτωση χρήσης του πρωτοκόλλου WPA2. Σε αντίστοιχα αποτελέσματα και συμπεράσματα είχαν καταλήξει οι ίδιοι συγγραφείς σε παλαιότερες μελέτες τους, όπου είχαν μελετήσει τον αντίκτυπο της χρήσης του πρωτοκόλλου ασφαλείας WAP2 στο εύρος ζώνης ενός δικτύου WLAN 802.11n για πρωτόκολλα δικτύου IPv4 και IPv6 με χρήση διαφορετικών λειτουργικών συστημάτων (Windows XP και Windows 7) [226].

Οι Jindal και Singh (2017) μελέτησαν την επίδραση που έχουν οι μηχανισμοί ασφαλείας στην απόδοση των δικτύων WLAN 802.11b/g/n σε πειραματική πλατφόρμα δοκιμών σε περιβάλλοντα πολλαπλών πελατών και σε περιπτώσεις ύπαρξης και μη κυκλοφοριακής συμφόρησης. Τα πειραματικά αποτελέσματα είχαν ως στόχο την αξιολόγηση της απόδοσης των δικτύων στα οποία εφαρμόστηκε ένα πολυεπίπεδο μοντέλο ασφαλείας που περιελάμβανε εννέα διαφορετικά πρωτόκολλα ασφαλείας, ως προς τη διαμεταγωγή, τον χρόνο απόκρισης και την επιβάρυνση της κρυπτογράφησης. Οι συγγραφείς διαπίστωσαν ότι η υποβάθμιση της απόδοσης των δικτύων ήταν ανάλογη της μεγαλύτερης ασφάλειας που επιτυγχανόταν από τον εφαρμοζόμενο μηχανισμό ασφαλείας [224].

Μια πιο λεπτομερής ανάλυση για τη μελέτη της επίδρασης των πρωτοκόλλων ασφάλειας στην απόδοση των δικτύων WLAN 802.11 διαφόρων προτύπων, με εφαρμογή ενός πολυεπίπεδου μοντέλου ασφάλειας το οποίο να μπορεί να υποστηρίξει ενσωμάτωση των χρησιμοποιούμενων πρωτοκόλλων ασφάλειας, παρουσιάστηκε από τον M. K. Ray (2022). Ο συγγραφέας αναφέρει ότι η χρήση ανεξάρτητων λύσεων ασφάλειας σε κάθε επίπεδο μιας στοίβας πρωτοκόλλου ασύρματου δικτύου για την αντιμετώπιση των επιθέσεων που μπορεί να δεχθεί, ενδέχεται να οδηγήσει σε επιδείνωση της απόδοσης του δικτύου. Ως λύση του συγκεκριμένου ζητήματος, για την επίτευξη όσο το δυνατό μεγαλύτερης ασφάλειας σε συνδυασμό με τη διατήρηση της σταθερότητας του δικτύου, ο συγγραφέας πρότεινε τη σωστή αλληλεπίδραση και συντονισμό μεταξύ των πρωτοκόλλων που εφαρμόζονται στα πολλαπλά επίπεδα του δικτύου [228].

Ο U. Singh (2018) ανέλυσε τον αντίκτυπο που παρουσιάζει η χρήση των κρυπτογραφικών πρωτοκόλλων στη διαμεταγωγή και στη καθυστέρηση που παρουσιάζουν τα δίκτυα WLAN 802.11. Ο συγγραφέας ανέφερε ότι η χρήση κρυπτογραφικών πρωτοκόλλων αυξάνει την πολυπλοκότητα στην επικοινωνία, η οποία αυξάνει περαιτέρω την κατανάλωση των πόρων του συστήματος και μειώνει την συνολική του απόδοση. Η αύξηση της κατανάλωσης των πόρων του συστήματος είναι ανάλογη της ασφάλειας που παρέχουν οι κρυπτογραφικοί αλγόριθμοι. Ο συγγραφέας κατέληξε στο συμπέρασμα ο σχεδιασμός των δικτύων WLAN θα πρέπει να παρουσιάζει μια αντιστάθμιση μεταξύ της ασφάλειας και της παρεχόμενης ποιότητας QoS ως προς τη διαμεταγωγή, τον χρόνο απόκρισης, τον λανθάνοντα χρόνο, την καθυστέρηση ή τη διακύμανσή της, την επιβάρυνση των μεθόδων κρυπτογράφησης, τη χρήση, την αξιοπιστία, την αναλογία κόστους/απόδοσης, τον χρόνο πραγματοποίησης των διαδικασιών επαλήθευσης ταυτότητας για διάφορους μηχανισμούς ασφάλειας [229].

Οι Caldas-Calle και συν. (2017) εξέτασαν τον αντίκτυπο στην απόδοση των δικτύων WLAN που παρουσιάζει η αύξηση της ασφάλειάς τους με χρήση δικτύων VPN. Οι συγγραφείς κατέληξαν στο συμπέρασμα, ότι από τη στιγμή που η χρήση δικτύου VPN προσθέτει ένα επιπλέον επίπεδο στην μετάδοση των δεδομένων στα δίκτυα WLAN, μια τέτοια χρήση έχει αντίκτυπο στη διαμεταγωγή, τον λανθάνοντα χρόνο και την αναλογία απώλειας πακέτων, στοιχεία που επηρεάζουν την παρεχόμενη ποιότητα QoS του δικτύου [230].

Οι Aziz, Abd Razak και Ghani (2017) πραγματοποίησαν πειράματα σε ασύρματη πλατφόρμα δοκιμών για την ανάλυση της απόδοσης των δικτύων WLAN ως προς την υποστήριξη εφαρμογών πραγματικού χρόνου και μεταφοράς δεδομένων σε πραγματικό χρόνο. Η ανάλυση βασίστηκε στην εξέταση παραμέτρων, όπως η ισχύς του σήματος, η διαμεταγωγή, η καθυστέρηση και η διακύμανσή της, καθώς και η αναλογία απώλειας πακέτων, χρησιμοποιώντας τέσσερις διαφορετικές ρυθμίσεις ασφαλείας: απενεργοποιημένη ασφάλεια, WEP, WPA και WAP2. Τα αποτελέσματα της ανάλυσης έδειξαν ότι η χρήση των πρωτοκόλλων ασφάλειας υποβαθμίζει τη συνολική απόδοση των δικτύων WLAN. Τα πειραματικά αποτελέσματα μάλιστα της ανάλυσης της απόδοσης των δικτύων WLAN ως προς την εφαρμογή μεταφοράς φωνητικών δεδομένων έδειξαν ότι αυτή η υποβάθμιση είναι

μεγαλύτερη για τα δίκτυα WLAN που λειτουργούν στην μπάντα συχνοτήτων των 2,4GHz, σε σύγκριση με εκείνα των 5GHz [223].

Ο P. K. Pant (2020) εξέτασε τον αντίκτυπο που παρουσιάζει το διάστημα προστασίας SGI (Short Guard Interval) και η ενεργοποίηση/απενεργοποίηση του μηχανισμού RTS/CTS στη διαμεταγωγή ενός δικτύου WLAN 802.11n σε διαφορετικά σενάρια χρήσης μηχανισμών ασφάλειας. Η ανάλυση του αντίκτυπου έγινε μόνο για τη διαμεταγωγή του δικτύου με ροή δεδομένων TCP και με χρήση προσομοιωτή NS-3. Από την ανάλυση των αποτελεσμάτων ο συγγραφέας βρήκε ότι το διάστημα προστασίας SGI από μόνο του υποβαθμίζει τη διαμεταγωγή του δικτύου κατά 5-7%, ενώ με την ενεργοποίηση του μηχανισμού RTS/CTS, η διαμεταγωγή υποβαθμίζεται σημαντικά. Η υψηλότερη διαμεταγωγή του δικτύου μπορεί να επιτευχθεί απενεργοποιώντας τον μηχανισμό ασφάλειας. Ο συγγραφές επίσης αναφέρει ότι το χρησιμοποιούμενο πρωτόκολλο ασφάλειας επίσης επηρεάζει την διαμεταγωγή του δικτύου. Η κρυπτογράφηση RC4 του WEP παρουσιάζει την χαμηλότερη διαμεταγωγή, ενώ υψηλότερη διαμεταγωγή μπορεί να επιτευχθεί μέσω της χρήσης της κρυπτογράφησης AES του WPA2 [225].

Από την παρουσίαση της παραπάνω βιβλιογραφίας προκύπτει το συμπέρασμα ότι αρκετοί μελετητές έχουν πραγματοποιήσει πειράματα για την ποσοτικοποίηση του αντίκτυπου της χρήσης των πρωτοκόλλων ασφάλειας στην απόδοση των δικτύων WLAN, αλλά οι μελέτες αυτές παρουσιάζουν κάποιες ελλείψεις. Πρώτον, το μεγαλύτερο μέρος των μελετών δεν είναι της τελευταίας πενταετίας. Δεύτερον, οι μελέτες αυτές έχουν επικεντρωθεί στον αντίκτυπο των μεθόδων κρυπτογράφησης των πρωτοκόλλων ασφάλειας πάνω στην απόδοση των δικτύων WLAN, αλλά σε ένα μικρό εύρος σεναρίων χρήσης των δικτύων. Τρίτον, το μεγαλύτερο μέρος των μελετών έχει επικεντρωθεί στην έρευνα πάνω στον αντίκτυπο των πρωτοκόλλων ασφάλειας πάνω στους βασικότερους παράγοντες που μπορούν να επηρεάσουν τη συνολική απόδοση των δικτύων WLAN, χωρίς να ασχολούνται με την μελέτη του αντίκτυπου αυτού σε μια ποικιλία σεναρίων χρήσης των δικτύων ή σε διαφορετικά μήκη πακέτων δεδομένων.

5.5 Τεχνικές βελτιστοποίησης της απόδοσης

Μετά την ανεύρεση των βασικών παραγόντων που επηρεάζουν την απόδοση των δικτύων WLAN, ο επόμενος στόχος είναι η παρουσίαση των τρόπων με τους οποίους μπορεί αυτή να βελτιωθεί. Η παρουσίαση αυτών των τρόπων θα γίνει μέσα από την αναφορά μελετών που έχουν εμφανιστεί στη βιβλιογραφία και έχουν ασχοληθεί με το συγκεκριμένο ζήτημα. Οι περισσότερες από αυτές τις μελέτες είναι οι ίδιες με αυτές που αναφέρθηκαν στην παρουσίαση των βασικών παραγόντων που επηρεάζουν την απόδοση των δικτύων WLAN. Επομένως, οι τρόποι βελτίωσης της απόδοσης έχουν ως απώτερο σκοπό την αντιμετώπιση των ζητημάτων που επηρεάζουν τους παράγοντες που την υποβιβάζουν, όπως αυτοί αναφέρθηκαν στις προηγούμενες ενότητες του κεφαλαίου. Η ταξινόμηση των μελετών αυτών είναι καθαρά ενδεικτική, καθώς οι περισσότερες από τις μελέτες αυτές εστιάζουν στην ανάλυση και διερεύνηση τεχνικών βελτιστοποίησης περισσότερων του ενός παράγοντα υποβιβασμού της απόδοσης του δικτύου ή συνδυασμού τους. Επίσης, κάποιοι από τους τρόπους βελτίωσης της απόδοσης των δικτύων WLAN έχουν ήδη αναφερθεί κατά τη διάρκεια ανάλυσης των μελετών ως προς την παρουσίαση των βασικών παραγόντων επίδρασης πάνω στην απόδοση αυτή.

1) Διαμεταγωγή

Ο A. Franco (2017) παρουσίασε μια μελέτη βελτίωσης της διαμεταγωγής των δικτύων WLAN μεγάλης πυκνότητας βασιζόμενος στη χρήση τεχνικών συνεργασίας (cooperative techniques), όπως ο προγραμματισμός συνεργασίας (cooperative scheduling), η αναμετάδοση συνεργασίας (cooperative

relaying) και η συνάθροιση πλαισίων (frame aggregation), στο πλαίσιο τροποποίησης του πρωτοκόλλου MAC των δικτύων WLAN 802.11. Το προτεινόμενο πρωτόκολλο MAC, το OMAC (Opportunistic MAC), περιλαμβάνει έναν μηχανισμό προγραμματισμού που βασίζεται στον τρόπο λειτουργίας του ήδη υπάρχοντα αλγόριθμου DCF, αλλά χρησιμοποιεί διαφορετικές ουρές και μηχανισμούς πρόσβασης προτεραιότητας προκειμένου να αυξηθεί η διαμεταγωγή των δικτύων WLAN. Προσομοιώσεις της προτεινόμενης μεθόδου έδειξαν σημαντική βελτίωση της διαμεταγωγής σε σύγκριση με τα υφιστάμενα σχήματα IEEE 802.11 MAC. Το πρωτόκολλο OMAC εξαλείφει την ανάγκη για ρητή ανταλλαγή πληροφοριών βασιζόμενο μόνο στην ικανότητα των συσκευών για μέτρηση της ισχύος του σήματος RSSI, κάτι που μειώνει την γενική επιβάρυνση λόγω της δυνατότητας συνεργασίας μεταξύ των κόμβων για ανταλλαγή πλαισίων. Η χρήση μόνο του RSSI μιας συσκευής, δεν απαιτεί αποκωδικοποίηση του σήματος, επομένως, το προτεινόμενο σχήμα είναι ανθεκτικό σε διάφορες συνθήκες καναλιού, καθώς μπορεί να προσαρμόζεται στις εκάστοτε συνθήκες καναλιού [173].

Οι Obelovska, Panova και Karovič Jr (2021), στη μελέτη τους πάνω στον αντίκτυπο που μπορεί να παρουσιάσει η αναλογία κίνησης υψηλής/χαμηλής προτεραιότητας στη διαμεταγωγή ενός δικτύου WLAN με διαφορετικούς αριθμούς κατηγοριών πρόσβασης, αναφέρουν ότι για τη βελτίωση της διαμεταγωγής ενός μεγάλου δικτύου WLAN με επικρατούσα την κυκλοφορία υψηλής προτεραιότητας απαιτείται μια προσαρμοστική προσέγγιση του αριθμού των κατηγοριών πρόσβασης στο επίπεδο MAC [170].

2) Πρωτόκολλα MAC

Οι Hassan και συν. (2018) παρουσίασαν μια μελέτη η οποία αποτελεί μια περιεκτική ανασκόπηση των τεχνικών βελτίωσης της διαδικασίας BEB, που χρησιμοποιείται στον αλγόριθμο DCF του πρωτοκόλλου MAC, ο οποίος όπως αναφέρουν αποτελεί βασικό παράγοντα υποβάθμισης της συνολικής απόδοσης των δικτύων WLAN. Ανάμεσα στις λύσεις που αναφέρονται ιδιαίτερο ενδιαφέρον παρουσιάζουν ο έλεγχος του μεγέθους του παραθύρου CW (Contention Window), η μείωση της περιόδου του διαστήματος IFS (Interframe Space) και η ρύθμιση του ορίου της εκπομπής TXOP (Transmission Opportunity) [178].

Οι Gopinath και Nithya (2018) παρουσίασαν έναν αποτελεσματικό μηχανισμό επίλυσης διενέξεων σε δίκτυα WLAN 802.11ah, σε μια προσπάθεια αντιμετώπισης των ζητημάτων που παρουσιάζει η διαδικασία BEB ως προς την υποβάθμιση της απόδοσης του δικτύου. Ο προτεινόμενος αλγόριθμος χρησιμοποιεί αποτελεσματικό μηχανισμό ρύθμισης του παραθύρου CW χρησιμοποιώντας κατάλληλη ακολουθία κατά τη διάρκεια των συγκρούσεων. Ο αλγόριθμος περιλαμβάνει επίσης έναν τροποποιημένο μηχανισμό επαναφοράς του παραθύρου CW, ο οποίος ενεργοποιείται μετά από κάθε επιτυχημένη μετάδοση, με σκοπό τον έλεγχο των συγκρούσεων και τη βελτίωση της απόδοσης του δικτύου. Η εκτίμηση της διαμεταγωγής που επιτυγχάνεται με αυτόν τον τρόπο πραγματοποιήθηκε μέσω χρήσης ενός μοντέλο ακριβείας 2D Markov, ενώ τα αποτελέσματα της προσομοίωσης NS3 του αλγόριθμου έδειξαν βελτίωση της συνολικής απόδοσης του δικτύου ως προς τον λόγο παράδοσης πακέτων, την διαμεταγωγή, την απώλεια πακέτων και την καθυστέρηση, σε σύγκριση με τις αντίστοιχες παραμέτρους της διαδικασίας BEB [179].

Οι Kocak και Karakurt (2019) χρησιμοποίησαν μια μέθοδο βελτίωσης της απόδοσης του πρωτοκόλλου MAC σε δίκτυα WLAN 802.11e, η οποία βασίζεται στη χρήση τεχνικών fuzzy logic. Η χρήση του μοντέλου OPNET για την αξιολόγηση της απόδοσης του δικτύου ως προς την εξέταση των παραμέτρων της διαμεταγωγής και της καθυστέρησης, και πιο συγκεκριμένα των τιμών

συγκεκριμένων παραμέτρων των πρωτοκόλλων MAC, όπως οι RSTV, FTV και BS, έδειξε μείωση της καθυστέρησης κατά 36-38% και αύξηση της διαμεταγωγής κατά 25-44% [180].

3) Περιβάλλοντα διάδοσης σημάτων ραδιοσυχνότητας

Στη μελέτη τους ως προς την ανάλυση ισχύος του σήματος σε οικιακά δίκτυα WLAN, οι Dhere και συν. (2018) αναφέρουν ότι η χρήση επαναληπτών μπορεί να αυξήσει την απόδοση των δικτύων σε μεγάλο βαθμό. Καθώς οι συγγραφείς παρατήρησαν στις αναλύσεις τους, ότι η ταχύτητα της ανερχόμενης και κατερχόμενης ζεύξης επηρεάζεται σε μεγάλο βαθμό από την ισχύ του σήματος Wi-Fi, το οποίο μειώνεται σημαντικά με την αύξηση της απόστασης της ασύρματης συσκευής από το πλησιέστερο σημείο AP, πρότειναν τη χρήση επαναλήπτων ή επεκτατών εύρους σε κατάλληλα σημεία που να ενισχύουν αυτό το σήμα. Οι συγγραφείς προτείνουν επίσης την αντικατάσταση στους επαναλήπτες και στους δρομολογητές, των πανκατευθυντικών κεραιών με κατευθυντικές, με σκοπό την ενίσχυση του σήματος στις περιοχές που παρουσιάζουν σήμα ασθενούς ισχύος [199].

Οι Tramarin, Mok και Han (2019) παρουσίασαν μια μελέτη ως προς τη χρήση των δικτύων WLAN για υποστήριξη εφαρμογών πραγματικού χρόνου σε βιομηχανικά περιβάλλοντα. Οι συγγραφείς πρότειναν τον σχεδιασμό αλγορίθμων αποτελεσματικής επιλογής ρυθμού μετάδοσης δεδομένων ως τρόπο αύξησης της αξιοπιστίας της παράδοσης δεδομένων σε τέτοιου είδους εφαρμογές. Επιπρόσθετα, παρουσίασαν ένα νέο πρωτόκολλο επιπέδου σύνδεσης δεδομένων το οποίο βασίζεται στη χρήση της μεθόδου πρόσβασης TDMA και επιτρέπει υψηλή παραμετροποίηση για την αύξηση της ταχύτητας ανταλλαγής δεδομένων σε πραγματικό χρόνο σε δίκτυα WLAN 802.11 [205].

Ο A. Aijaz (2020) προτείνει μια λύση για την αύξηση της αξιοπιστίας των επικοινωνιών Wi-Fi σε βιομηχανικά περιβάλλοντα. Η προτεινόμενη λύση περιλαμβάνει υβριδικούς μηχανισμούς πρόσβασης καναλιού για την επίτευξη ντετερμινιστικής επικοινωνίας. Κάτι τέτοιο επιτυγχάνεται μέσω τροποποίησης του πρωτοκόλλου MAC, ώστε να περιλαμβάνει μηχανισμούς με προκαθορισμένο (φυσικό) χρονοδιάγραμμα και με εικονικό χρονοδιάγραμμα. Η αξιολόγηση της απόδοσης, με βάση ανάλυση και προσομοιώσεις σε επίπεδο συστήματος, έδειξε τη βιωσιμότητα της προτεινόμενης λύσης σε βιομηχανικές εφαρμογές ελέγχου, καθώς ελαχιστοποιεί τον λανθάνοντα χρόνο και αυξάνει την αξιοπιστία του δικτύου Wi-Fi [190].

4) Ισχύς σημάτων ραδιοσυχνοτήτων και τύπος κυκλοφορίας

Στις μελέτες τους, οι Ali, Dhimish και Mather (2019) και Ali, Dhimish και Alsmadi (2020) αναφέρουν ότι για τη δυνατότητα υποστήριξης εφαρμογών πραγματικού χρόνου, όπως VoIP και τηλεδιασκέψεων, από τα δίκτυα WLAN, απαιτείται ο σχεδιασμός δικτύων βέλτιστης αρχιτεκτονικής και χρήσης του καταλληλότερου πρωτοκόλλου ανά περίσταση, κάτι που θα μπορεί να εγγυηθεί τη βέλτιστη επίτευξη συνολικής απόδοσης του δικτύου, ως προς τις παραμέτρους της καθυστέρησης, της διακύμανσής της και της αναλογίας απώλειας πακέτων, αλλά και την παροχή βέλτιστης ποιότητας QoS στις εφαρμογές. Για το λόγο αυτό, οι συγγραφείς πρότειναν μια αρχιτεκτονική σχεδιασμού δικτύων WLAN, η οποία να βασίζεται σε επιλογή πρόσβασης καναλιού πολλαπλών κριτηρίων, όπως η χωρική κατανομή και ο αριθμός των χρηστών που εξυπηρετούνται από ένα σημείο AP του δικτύου [198], [231].

Για τη βελτίωση της απόδοσης των δικτύων WLAN ως προς τη δυνατότητα υποστήριξης μεταφοράς δεδομένων βίντεο με χρήση του αλγόριθμου RMCAT, οι Govindarajan και Mohanapriya πρότειναν τον επανασχεδιασμό της διαδικασίας ελέγχου συμφόρησης που περιλαμβάνει ο αλγόριθμος, λαμβάνοντας υπόψη τις εκάστοτε παραμέτρους της κατάστασης των καναλιών επικοινωνίας του δικτύου [202].

5) Παρεμβολές και θόρυβος

Οι Oyedare και συν. (2022) παρουσίασαν μια μελέτη στην οποία εξετάζεται η χρήση τεχνικών βαθιάς μάθησης με σκοπό την καταστολή των παρεμβολών στα δίκτυα WLAN. Οι συγγραφείς εστίασαν τη μελέτη τους σε τέσσερις τεχνικές βαθιάς μάθησης, όπως τα συνελικτικά νευρωνικά δίκτυα CNN (Convolutional Neural Networks), τα τεχνητά νευρωνικά δίκτυα autoencoders, τα επαναλαμβανόμενα νευρωνικά δίκτυα RNN (Recurrent Neural Neyworks) και τα βαθιά νευρωνικά δίκτυα DNN (Deep Neural Networks). Τα συμπεράσματα στα οποία κατέληξαν αποδεικνύουν την ανωτερότητα των τεχνικών βαθιάς μάθησης στην καταστολή των παρεμβολών στα δίκτυα WLAN σε σύγκριση με τις παραδοσιακές τεχνικές καταστολής. Οι συγγραφείς μάλιστα ανέφεραν ότι από τις εξεταζόμενες τεχνικές βαθιάς μάθησης, οι autoencoders και τα δίκτυα RNN παρουσιάζουν τα μεγαλύτερα ποσοστά καταστολής των παρεμβολών [209].

Κεφάλαιο 6ο: Συμπεράσματα

Η ανάπτυξη των δικτύων WLAN αποτελεί πλέον μια πραγματικότητα του σύγχρονου κόσμου σε παγκόσμιο επίπεδο, λόγω των πολλών δυνατοτήτων τους, όπως είναι η υποστήριξη της κινητικότητας των χρηστών και η εύκολη προσαρμογή στις διάφορες απαιτήσεις τους για επικοινωνία. Μια τέτοια ανάπτυξη καθιστά κάτι παραπάνω από επιτακτική την κατανόηση των διαφορετικών τεχνολογιών ασύρματης επικοινωνίας, ώστε σε κάθε περίπτωση να επιλέγεται η καταλληλότερη. Αρωγός σε αυτήν την εξέλιξη των δικτύων WLAN ήταν ο οργανισμός IEEE, ο οποίος, από το 1997 που κυκλοφόρησε την πρώτη έκδοση του προτύπου IEEE 802.11, ορίζοντας το φυσικό επίπεδο και το επίπεδο της ζεύξης δεδομένων της ασύρματης δικτύωσης, εξακολουθεί ακόμα και σήμερα να κυκλοφορεί νέα πρότυπα ως τροποποιήσεις του βασικού. Χαρακτηριστικό γνώρισμα σχεδόν κάθε νέας τροποποίησης που παρουσιάζεται είναι να παρέχει υψηλότερες ταχύτητες επικοινωνίας και μεγαλύτερη εμβέλεια, διατηρώντας ταυτόχρονα συμβατότητα με τις προηγούμενες. Καθώς επομένως, η ασύρματη επικοινωνία αποτελεί ένα διαρκώς αναπτυσσόμενο πεδίο, το μέλλον της βασίζεται σε δύο πολύ σημαντικούς παράγοντες, όπως είναι η μεγαλύτερη ασφάλεια και η δυνατότητα υποστήριξης υψηλότερων ρυθμών μετάδοσης δεδομένων.

Σκοπός της παρούσας εργασίας, ήταν η παρουσίαση μιας όσο το δυνατόν πιο ολοκληρωμένης βιβλιογραφικής ανασκόπησης των δικτύων WLAN, εστιάζοντας σε δύο βασικούς παράγοντες που επηρεάζουν τη συνολική εξελικτική τους πορεία, όπως είναι η ασφάλεια και η απόδοσή τους.

Για το λόγο αυτό, διαρθρώθηκε ουσιαστικά σε δύο μέρη. Στο πρώτο μέρος έγινε μια παρουσίαση των δικτύων WLAN, η οποία αναπτύχθηκε σε τρία κεφάλαια. Στο πρώτο, εισαγωγικό κεφάλαιο, δόθηκε ο ορισμός των δικτύων WLAN, καθώς και μια ιστορική αναδρομή των ασύρματων δικτύων γενικότερα.

Στο δεύτερο κεφάλαιο, αρχικά παρουσιάστηκαν και αναλύθηκαν τα γενικά χαρακτηριστικά των δικτύων WLAN, όπως η κινητικότητα, η ασφάλεια, η επεκτασιμότητα, η ευελιξία, η περιοχή κάλυψης, η ταχύτητα ή ρυθμός μετάδοσης δεδομένων, η χωρητικότητα και η συμβατότητα. Στη συνέχεια, παρουσιάστηκαν οι τύποι και οι τεχνολογίες των τεχνολογιών WLAN, με ιδιαίτερη έμφαση στα δίκτυα υποδομής, τα ad-hoc δίκτυα, τα δίκτυα πλέγματος και τα υβριδικά δίκτυα WLAN. Κατόπιν παρουσιάστηκαν τα πλεονεκτήματα και τα μειονεκτήματα των δικτύων WLAN, κυρίως με γνώμονα τη σύγκρισή τους με τα ενσύρματα δίκτυα. Μια τέτοια σύγκριση αναδεικνύει την υποστήριξη της κινητικότητας, τη δυνατότητα παροχής ασύρματης πρόσβασης σε περιοχές που είναι δύσκολο να αναπτυχθούν ενσύρματα δίκτυα, την ταχύτητα ανάπτυξης, την επεκτασιμότητα, το κόστος υλοποίησης, την αξιοπιστία και την ευελιξία, ως πλεονεκτήματα των δικτύων WLAN και την ασφάλεια, το ρυθμό μετάδοσης δεδομένων και τις παρεμβολές ως τα κυριότερα μειονεκτήματά τους. Το δεύτερο κεφάλαιο ολοκληρώθηκε με μια παρουσίαση της τρέχουσας κατάσταση των τεχνολογιών ασύρματης δικτύωσης και των προτύπων που χρησιμοποιούνται στα δίκτυα WLAN. Σε αυτό το πλαίσιο παρουσιάστηκαν τα κυριότερα χαρακτηριστικά του βασικού προτύπου IEEE 802.11, καθώς και των βασικότερων τροποποιήσεών του, όπως οι IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac και IEEE 802.11ax.

Το πρώτο μέρος της εργασίας ολοκληρώθηκε με το τρίτο κεφάλαιο στο οποίο αναπτύχθηκαν οι τρόποι μετάδοσης που χρησιμοποιούνται στα δίκτυα WLAN. Για το λόγο αυτό παρουσιάστηκαν οι τεχνικές μετάδοσης SS, FHSS, DSSS, OFDM, καθώς και η τεχνολογία MIMO.

Το δεύτερο μέρος της εργασίας ασχολήθηκε με τα ζητήματα της ασφάλειας και της απόδοσης των δικτύων WLAN. Όσον αφορά την ασφάλεια, αρχικά πραγματοποιήθηκε μια αναφορά στις απειλές και

τα τρωτά σημεία των δικτύων WLAN και ο τρόπος εκμετάλλευσής τους για την πραγματοποίηση των επιθέσεων κατά της ασφάλειάς τους. Σε αυτό το πλαίσιο, οι επιθέσεις που παρουσιάστηκαν επιλέχθηκαν με γνώμονα τον κίνδυνο που παρουσιάζουν για τη διαθεσιμότητα ενός δικτύου WLAN, την εμπιστευτικότητα ή/και την ακεραιότητα των δεδομένων που μεταδίδονται μέσω αυτού, καθώς και την ορθή και ασφαλή λειτουργία των διαδικασιών ελέγχου ταυτότητας και ελέγχου πρόσβασης. Για το λόγο αυτό ταξινομήθηκαν με βάση το ποιο από τα χαρακτηριστικά του μοντέλου ασφάλειας CIA στοχεύουν σε μεγαλύτερο βαθμό. Έτσι, παρουσιάστηκαν τύποι επιθέσεων κατά της διαθεσιμότητας ενός δικτύου WLAN, καθώς και της εμπιστευτικότητας και της ακεραιότητας των δεδομένων που μεταδίδονται μέσω αυτού.

Στη συνέχεια παρουσιάστηκαν τα πρωτόκολλα κρυπτογράφησης, όπως τα WEP, TKIP και CCMP, καθώς και οι μηχανισμοί ελέγχου ταυτότητας OSA και PSK, το πρωτόκολλο ελέγχου ταυτότητας EAP, η έννοια του captive portal και τα διαπιστευτήρια ελέγχου ταυτότητας και ελέγχου πρόσβασης. Το κεφάλαιο της ασφάλειας ολοκληρώθηκε με την παρουσίαση κάποιων άλλων πρακτικών, που χρησιμοποιούνται ως τρόποι βέλτιστης προστασίας της ασφάλειας των δικτύων WLAN.

Όσον αφορά την απόδοση των δικτύων WLAN, αρχικά αναλύθηκε η έννοια της απόδοσης στα δίκτυα αυτά και στη συνέχεια έγινε μια προσπάθεια εντοπισμού και παρουσίασης των βασικότερων παραγόντων που την επηρεάζουν. Ο εντοπισμός και η παρουσίαση αυτή έγινε μέσω της αναφοράς κάποιων από τις σχετικές μελέτες που εμφανίστηκαν στη βιβλιογραφία. Μεγαλύτερη έμφαση δόθηκε στο ζήτημα των παρεμβολών και τον αντίκτυπό του, αλλά και της επίδρασης των πρωτοκόλλων ασφάλειας στην συνολική απόδοση των δικτύων WLAN. Το κεφάλαιο ολοκληρώθηκε με μια παρουσίαση κάποιων τεχνικών βελτιστοποίησης της απόδοσης των δικτύων WLAN, πάντα με βάση κάποιων σχετικών μελετών που εμφανίστηκαν στη βιβλιογραφία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] E. O. E. Elmahdi. *Secure data integrity in wireless ad hoc networks*. Dissertation. The University of Alabama in Huntsville. 2021.

[2] W. A. Cahyadi, Y. H. Chung, Z. Ghassemlooy, and N. B. Hassan. *Optical camera communications: Principles, modulations, potential and challenges*. Electronics, 9(9), 1339, 2020.

[3] S. A. Alomari, P. Sumari, and A. Taghizadeh. *A comprehensive study of wireless communication technology for the future mobile devices*. European Journal of Scientific Research, 60(4), 583-591, 2011.

[4] L. Azpilicueta Fernández de las Heras. *Characterization of wireless propagation in complex indoor environments*. Doctoral thesis submitted for the degree of Doctor of Philosophy in Telecommunication Engineering. Universidad Publica de Navarra. Pamplona, 2015.

[5] M. A. El-Bendary. *Wireless Networks*. Developing security tools of WSN and WBAN networks applications. Springer Japan. Chapter 3, pp: 43-55, 2015.

[6] D. G. Mwathi. *A model based approach for implementing authentication and access control in public WLANs: A case of Universities in Kenya*. Doctoral dissertation. Computer Science in the School of Computing and Informatics. University Of Nairobi, 2018.

[7] R. Prasad, and F. J. Velez. *The Evolution Towards WiMAX*. WiMAX networks: techno-economic vision and challenges. Springer Science & Business Media. Chapter 1, pp: 1-62, 2010.

[8] U. H. Rao, and U. Nayak. *History of Computer Security*. The InfoSec handbook: An introduction to information security. Springer Nature. Chapter 2, pp: 13-26, 2014.

[9] S. Gagliarducci, M. G. Onorato, F. Sobbrio, and G. Tabellini. *War of the waves: Radio and resistance during World War II*. American Economic Journal: Applied Economics, 12(4), 1-38, 2020.

[10] R. Raj, and V. Raheja. *Mobile technology: a study on its evolution*. International Journal of Management, IT and Engineering, 4(10), 222-230, 2014.

[11] V. Kumar. Mobile and Wireless Communication. Fundamentals of pervasive information management systems. John Wiley & Sons. Chapter 2, pp: 7-43, 2013.

[12] M. M. R. K. Mamun, A. S. M. Abdullah, and S. Mahmud. *Application of Duplication Strategy In 4g For Better Accessibility To Network*. International Journal of scientific research and management (IJSRM), 1(6), 308-311, 2013.

[13] K. Pahlavan, and P. Krishnamurthy. *Evolution and impact of Wi-Fi technology and applications: A historical perspective*. International Journal of Wireless Information Networks, 28, 3-19, 2021.

[14] S. Jaiswal, A. Kumar, and N. Kumari. *Development of Wireless Communication Networks: From 1G to 5G*. International Journal Of Engineering And Computer Science, 3(5), 6053-6056, 2014.

[15] A. A. Salih, S. R. Zeebaree, A. S. Abdulraheem, R. R. Zebari, M. A. Sadeeq, and O. M. Ahmed. *Evolution of mobile wireless communication to 5G revolution*. Technology Reports of Kansai University, 62(5), 2139-2151, 2020.

[16] E. Ouellet, R. Padjen, A. Pfund, R. Fuller, and T. Blankenship. *Wireless LAN Overview*. Building a Cisco Wireless LAN. Syngress. Chapter 2, pp: 31-91, 2002.

[17] M. Gast. *Overview of 802.11 Networks*. 802.11 wireless networks: The definitive guide. O'Reilly. Chapter 2, pp: 12-31, 2006.

[18] K. J. Negus, and A. Petrick. History of wireless local area networks (WLANs) in the unlicensed bands. info, 11(5), 36-56, 2009.

[19] D. E. Capano. *WLAN design basics and wireless network considerations*. Control Engineering. 2015, August. [Online]. Available: https://www.controleng.com/articles/wlan-design-basics-and-wireless-network-considerations/

[20] T. Spyropoulos, R. N. B. Rais, T. Turletti, K. Obraczka, and A. Vasilakos. *Routing for disruption tolerant networks: taxonomy and design*. Wireless networks, 16, 2349-2370, 2010.

[21] A. ElShafee, and K. A. Hamed. Design and implementation of a WIFI based home automation system. International Journal of Computer and Information Engineering, 6(8), 1074-1080, 2012.

[22] C. Beard, and W. Stallings. *Long Range Communications*. Wireless Communication, Networks and Systems, Pearson Higher Education, Inc., 1st Edition, Chapter 16, pp: 544-587, 2016.

[23] D. Antonenko. *Understanding Wireless Networks: A simple guide for business*. Business Tech Weekly. 2021, June. [Online]. Available: https://www.businesstechweekly.com/operational-efficiency/wireless-networks/wireless-networks/

[24] K. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs. *Guide to securing legacy IEEE 802.11 wireless networks*. NIST Special Publication, 800, 48, 2008.

[25] A. Yarali, B. Ahsant, and S. Rahman. *Wireless mesh networking: A key solution for emergency & rural applications*. IEEE 2009 Second International Conference on Advances in Mesh Networks. pp. 143-149, 2009, June.

[26] I. F. Akyildiz, X. Wang, and W. Wang. *Wireless mesh networks: a survey*. Computer networks, 47(4), 445-487, 2005.

[27] K. E. Faraj. *Security technologies for wireless access to local area networks*. Doctoral dissertation, Universidade do Algarve (Portugal). 2019.

[28] J. T. Geier. *The Wireless World: An Introduction to Concepts*. Wireless Networks first-step. Cisco Press. Chapter 1, pp: 3-31, 2005.

[29] J. Salazar Soler. *Wireless networks*. Faculty of electrical engineering. Czech Technical University of Prague. 2017.

[30] A. Mellouk. *Principles and Mechanisms for Quality of Service in Networks*. End-to-end quality of service: engineering in next generation heterogenous networks. John Wiley & Sons. Chapter 2, 2013.

[31] J. S. Cheema. *Study of Wireless Local Area Networks*. International Journal of Creative Research Thoughts (IJCRT), 6(1), 963-967, 2018, February.

[32] S. Cirani, G. Ferrari, M. Picone, and L. Veltri. *Standards*. Internet of things: architectures, protocols and standards. John Wiley & Sons. Chapter 2, pp: 9-78, 2018.

[33] P. S Patheja, A. A. Waoo, and V. Tiwari. *Improving Performance of 802.11 MAC by Optimizing DCF in Mobile ad-hoc Network*. Computer Science. 2012.

[34] S. Karim. Throughput Management for CSMA/CA Networks: IEEE 802.11 e Wireless LAN. Doctor of Philosophy in Electrical and Electronic Engineering. The University of Adelaide (Faculty of Engineering, Computer and Mathematical Sciences). 2012, November.

[35] I. A. Meer, W. H. Lee, M. Ozger, C. Cavdar, and K. W. Sung, K. W. *Low-Latency MAC Design for Pairwise Random Networks*. In 2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring) (pp. 1-6). 2022, June.

[36] S. Rackley. *Radio Communication Basics*. Wireless Networking Technology - From Principles to Successful Implementation. Elsevier. Chapter 4, pp: 71-128, 2007.

[37] E. Guérin, T. Begin, and I. G. Lassous. *An overview of MAC energy-saving mechanisms in Wi-Fi*. Computer Communications. 2023.

[38] G. H. Koepke, J. Coder, J. M. Ladbury, and W. Young. *Complexities of testing interference and coexistence of wireless systems in critical infrastructure*. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology. 2015.

[39] P. Mafole, and M. Aritsugi. *Analysis and performance assessment of a fragment retransmission scheme for energy efficient IEEE 802.11 WLAN*s. SpringerPlus, 5, 1-24. 2016.

[40] D. Singh. *Channel Scanning and Access Point Selection Mechanisms for 802.11 Handoff: A Survey*. Engineering Master's Thesis. Department of Computer Engineering, Santa Clara University, 2020.

[41] K. Lounis. *Wi-Fi Security: Do We Still Have to Look Back?*. Cryptology ePrint Archive. 2022.

[42] G. Chatzisofroniou, and P. Kotzanikolaou. *Association attacks in IEEE 802.11: Exploiting WiFi usability features*. In Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers 9 (pp. 107-123). Springer International Publishing. 2021.

[43] A. Bensky. *Wireless local area networks*. Short-range wireless communication. Newnes. Chapter 11, pp: 273-315, 2019.

[44] I. G. Lee, K. Go, and J. H. Lee. *Battery draining attack and defense against power saving wireless LAN devices*. Sensors, 20(7), 2043. 2020.

[45] A. H. Abdelmajid. *The Wi-Fi Evolution*. White Paper. Qorvo. 2019.

[46] R. Bhoyar, M. Ghonge, and S. Gupta. *Comparative Study on IEEE Standard of Wireless LAN/Wi-Fi 802.11 a/b/g/n*. International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 2(7), 687-691. 2013.

[47] T. Gotsis. *Wi-Fi evolution: the IEEE 802.11 ax standard for dense wireless local area networks*. Master's thesis, University of Piraeus, 2017.

[48] R. G. Rathor, and R. D. Joshi. *Performance Analysis of IEEE802. 11ax (Wi-Fi 6) Technology using Multi-user MIMO and Up-Link OFDMA for Dense Environment*. In 2021 IEEE 2nd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC) (pp. 1-7). IEEE. 2021, November.

[49] P. W. Fink. *Wireless Network Communications Overview for Space Mission Operations*. Organization and Processes for the Consultative Committee for Space Data Systems (CCSDS A02.1-Y-4). Informational Report, Issue 3. Washington, DC, USA. 2017.

[50] A. G. H. Mohamed. *Enabling Technologies for Next Generation Wireless Local Area Networks (WLANs)*. Doctoral dissertation. Faculty of Philosophy in Electrical Engineering. The University of Texas at Dallas. 2017, May.

[51] A. K. Jassim. *Design and Analysis of UWB Microstrip Antenna for Wireless Communication Systems*. MSc. in Electronics and Communication Engineering. Electrical Engineering Department, College of Engineering, Mustansiriyah University. 2019.

[52] M. P. Sren. *Spread spectrum analysis for CDMA system*. Doctoral dissertation. Technology in Electronics & Communication Engineering. National Institute of Technology, Rourkela. 2010.

[53] S. Indriani Lestariningati. *Week 9 Spread Spectrum*. Unikom Indonesia Computer University, 2017. [Online]. Available: https://repository.unikom.ac.id/51396/1/Week%209%20Spread%20Spectrum.pdf

[54] W. Stallings. *Spread Spectrum*. Data and computer communications. 8th Ed., Pearson Education India. Chapter 9, pp: 274-294, 2007.

[55] D. J. Torrieri. *Frequency Hopping Systems*. Principles of Spread-Spectrum Communication Systems. 5th Ed., Springer Nature. Chapter3, pp: 151-204, 2022.

[56] W. M. S. A. Atta. *Improved jamming-resistant frequency hopping spread spectrum systems*. Doctoral dissertation. Institute for Electrical and Computer Engineering, Department of Systems and Computer Engineering. Carleton University, Ottawa, Ontario. 2014, January.

[57] F. G. A. K. Bawahab, E. Kurniawan, E. Yuniarti, B. Widiyatmoko, and D. Bayuwati. *Performance evaluation and mathematical analysis of direct sequence and frequency hopping spread spectrum systems under wideband interference*. International Journal of Advances in Intelligent Informatics, 4(3), 180-191. 2018, November.

[58] D. Torrieri. *Frequency-Hopping Systems*. Principles of Spread-Spectrum Communication Systems, Springer New York, NY. Chapter 3, pp: 159–212. 2011.

[59] L. S. Gordon. *Spread Spectrum Techniques*. Principles of mobile communication. 4th Ed., Spinger. Chapter 9, pp: 449-500, 2017.

[60] R. K. Ghosh and R. K. Ghosh. *Wireless Local Area Network*. Wireless Networking and Mobile Data Management. Springer. Chapter 4, pp: 95-124, 2017.

[61] A. Mohammed, T. Ismail, A. Nassar, and H. Mostafa. *A novel companding technique to reduce high peak to average power ratio in OFDM systems*. IEEE Access, 9, 35217-35228, 2021.

[62] E. Hassan. Orthogonal Frequency Division Multiplexing. Multi-carrier communication systems with examples in MATLAB: A new perspective. CRC Press. Chapter 1, pp: 3-16, 2016.

[63] Y. T. Bozkurt, and N. Taspinar. *PAPR Reduction in OFDM Systems using Partial Transmit Sequence combined with Cuckoo Search Optimization Algorithm*. International Journal of Intelligent Systems and Applications in Engineering, 4(Special Issue-1), 260-263. 2016.

[64] P. K. Pradhan. *On efficient signal processing algorithms for signal detection and PAPR reduction in OFDM systems*. Doctoral dissertation. Department of Electronics and Communication Engineering, National Institute of Technology Rourkela, India. 2016.

[65] M. A. Gulzar, R. Nawaz, and D. Thapa. *Implementation of MIMO-OFDM System for WiMAX*. Doctoral dissertation. School of Computer Science, Physics and Mathematics, Linnaeus University, 2011, June.

[66] E. Biglieri, R. Calderbank and A. Constantinides. *Introduction*. MIMO Wireless Communications, New York, USA: Cambridge Univ. press. Chapter 1, pp: 1-23, 2007.

[67] M. J. Jiang and L. Hanzo. *Multiuser MIMO-OFDM for Next-Generation Wireless Systems*. Proceedings of the IEEE, 95(7), 1430-1469. 2007, June.

[68] S. J. Vaughan-Nichols. *Mobile WiMAX: The next wireless battle ground*. Computer, 41(6), 16-18. 2008, June.

[69] S. Kumar. *Wireless LAN-802.11*. International Research Journal of Computer Science (IRJCS), 7(7). 2020.

[70] M. N. Riaz, A. Buriro, and A. Mahboob. *Classification of attacks on wireless sensor networks: A survey*. International Journal of Wireless and Microwave Technologies, 8(6), 15-39. 2018.

[71] A. Gupta, and R. K. Jha. *Security threats of wireless networks: A survey*. In IEEE International Conference on Computing, Communication & Automation. pp. 389-395. 2015, May.

[72] M. M. Hamdi, Y. A. Yussen, and A. S. Mustafa. *Integrity and Authentications for service security in vehicular ad hoc networks (VANETs): A Review*. In IEEE 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). pp. 1-7. 2021, June.

[73] T. Jamal, P. Amaral, A. Khan, A. Zameer, K. Ullah, and S. A. Butt. *Denial of service attack in wireless LAN*. ICDS 2018, 51. 2018.

[74] M. Tyagi, S. Narvare, and C. Agrawal. *A Survey of Different Dos Attacks on Wireless Network*. Computer Engineering and Intelligent Systems, 9 (5), 23-32. 2018.

[75] R.Njeru. *An APN Authentication Model for a Secure Enterprise Wireless Local Area Network*. Doctoral dissertation. Faculty of computing and Information Mangement, KCA University. 2021, October.

[76] R. Korolkov, S. Kutsak, and V. Voskoboinyk. *Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection*. Bulletin of V.N. Karazin Kharkiv National University. Series Mathematical modeling. Information technology. Automated control systems, 50, 58-70, 2021.

[77] M. Agarwal, S. Biswas, and S. Nandi. *Advanced stealth man-in-the-middle attack in WPA2 encrypted Wi-Fi networks*. IEEE Communications Letters, 19(4), 581-584. 2015.

[78] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain. *Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey*. IEEE Open Journal of the Communications Society. 2022.

[79] P. Arote, and K. V. Arya. *Detection and prevention against ARP poisoning attack using modified ICMP and voting*. In IEEE 2015 International Conference on Computational Intelligence and Networks (pp. 136-141). 2015, January.

[80] D. G. Mwathi, W. Okello-Odongo, and E. Opiyo. *Selection of EAP Authentication Method for use in a Public WLAN: Implementation Environment Based Approach*. International Research Journal of Computer Science, 3(5), 47-52. 2016.

[81] J. Schwenk. *Wireless LAN (WLAN)*. Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications. Cham: Springer International Publishing. Chapter 6, pp: 99-119. 2022.

[82] M. Mohan, M. K. Devi, and V. J. Prakash. *Security analysis and modification of classical encryption scheme*. Indian journal of science and technology, 8(8), 542-548. 2015.

[83] W. Li, D. Mclernon, J. Lei, M. Ghogho, S. A. R. Zaidi, and H. Hui. *Cryptographic primitives and design frameworks of physical layer encryption for wireless communications*. IEEE Access, 7, 63660-63673. 2019.

[84] S. Suroto. *WLAN security: threats and countermeasures*. JOIV: International Journal on Informatics Visualization, 2(4), 232-238. 2018.

[85] T. Van Goethem, C. Pöpper, W. Joosen, and M. Vanhoef. *Timeless timing attacks: Exploiting concurrency to leak secrets over remote connections*. In Proceedings of the 29th USENIX Conference on Security Symposium (pp. 1985-2002). 2020, August.

[86] M. Waliullah, and D. Gan. *Wireless LAN security threats & vulnerabilities*. International Journal of Advanced Computer Science and Applications, 5(1). 2014.

[87] A. E. Abdallah, M. Hamdan, M. S. Gismalla, A. O. Ibrahim, N. S. Aljurayban, W. Nagmeldin, and M. H. Khairi. *Detection of Management-Frames-Based Denial-of-Service Attack in Wireless LAN Network Using Artificial Neural Network*. Sensors, 23(5), 2663. 2023.

[88] V. O. Etta, A. Sari, A. L. Imoize, P. K. Shukla, and M. Alhassan. *Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique*. Mobile Information Systems, 2022.

[89] M. Vanhoef, D. Schepers, and F. Piessens. *Discovering logical vulnerabilities in the Wi-Fi handshake using model-based testing*. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 360-371). 2017, April.

[90] D. G. Mwathi, W. Okello-Odongo, and E. Opiyo. *Vulnerability Analysis of 802.11 Authentications and Encryption Protocols: CVSS Based Approach*. International Research Journal of Computer Science, IV, 16-23. 2017.

[91] D. G. Mwathi, D. M. Nchunge, M. Sakwa, W. Mwangi, A. M. Ngereki, A. M. Kahonge, ..., and E. Opiyo. *WLAN Security: A Trusted Computing Base Approach*. Research Journal of Computer Science, 6, 15-20. 2019.

[92] M. K. Qabalin, Z. A. Arida, O. A. Saraereh, F. Wu, I. Khan, P. Uthansakul, and M. Alsafasfeh. *An Improved Dictionary Cracking Scheme Based on Multiple GPUs for Wi-Fi Network*. CMC-COMPUTERS MATERIALS & CONTINUA, 66(3), 2957-2972. 2021.

[93] P. Nalajala, R. V. Krishnaiah, B. Annapurna, and B. Godavarthi. *Security for wireless local area network with pre share key authentication using wi-fi protected access*. International Journal of Civil Engineering and Technology (IJCIET). 8 (8), pp. 841–851. 2017, August.

[94] M. E. Rana, M. Abdulla, and K. C. Arun. *Common security protocols for wireless networks: A comparative analysis*. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 632-638). Atlantis Press. 2021, September.

[95] S. Ciornei, I. Bogdan, and L. Scripcariu. *On 802.11 standard and the WiFi network security*. In Third European Conference on the Use of Modern Information and Communication Technologies ECUMICT Gent, Belgium (pp. 89-98). 2008, January.

[96] A. M. Al Naamany, A. Al Shidhani, and H. Bourdoucen. *IEEE 802.11 wireless LAN security overview*. Ijcsns, 6(5B), 138. 2006.

[97] B. I. Reddy, and V. Srikanth. *Review on wireless security protocols (WEP, WPA, WPA2 & WPA3)*. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(4). 2019.

[98] S. Sindhu, and D. Sindhu. *Cryptographic algorithms: applications in network security*. International Journal of New Innovations in Engineering and Technology, 7(1), 11. 2017.

[99] A. H. Lashkari, A. Saba, S. Alizadeh, and M. Khazaei. *A Survey on Wireless Security protocols Wi-Fi (802.11) and WiMAX (802.16)*. Conference: International Conference on Communication and Broadband Networking (ICCBN 2011). 2011, January.

[100] M. Vanhoef. *A Security Analysis of the WPA-TKIP and TLS Security Protocols*. Doctoral thesis submitted for the degree of Doctor in Engineering Science and Computer Science. KU Leuven – Faculty of Engineering Science, 2016.

[101] K. K. Singh, and L. Liu. *Security Issues in Wireless Networks*. Research Gate, 1-5. 2014.

[102] R. Budhrani, and R. Sridaran. *Wireless Local Area Networks: Threats and Their Discovery Using WLANs Scanning Tools*. International Journal Of Advanced Networking & Applications, 137-150. 2015.

[103] I. Ullah. *A study and analysis of Public WiFi*. Doctoral thesis. Institutionen för datavetenskap, Department of Computer and Information Science. 2012, October.

[104] Huawei. *CloudCampus WLAN Authentication and Encryption*. Technology White Paper. Issue 01. 2019, March.

[105] J. Kolárik. *IEEE 802.11 wireless networking for HelenOS*. Doctoral thesis. Charles University in Prague. Faculty of Mathematics and Physics. Department of Distributed and Dependable Systems. 2015, July.

[106] M. Beck, and E. Tews. *Practical Attacks against WEP and WPA*. TU-Dresden, Germany, TU-Darmstadt, Germany. 2008, January.

[107] O. P. Sarmiento, F. G. Guerrero, and D. Rey Argote. *Basic security measures for IEEE 802.11 wireless networks*. Ingenieria E Investigación, 28(2), 89-96. 2008.

[108] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis. *Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset*. IEEE Communications Surveys & Tutorials, 18(1), 184-208. 2015.

[109] A. K. Yadav, M. Misra, M. Liyanage, and G. Varshney. *Secure and user efficient eap-based authentication protocol for ieee 802.11 wireless lans*. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 576-584). 2020, December.

[110] F. P. Miller, A. F. Vandome, and J. McBrewster. *Extensible Authentication Protocol: Authentication, Wireless LAN, Point-to-Point Protocol, Wi-Fi Protected Access, Internet Engineering Task Force, EAP-SIM,... Protected Extensible Authentication Protocol*. Alpha Press. 2009, November.

[111] J. Schwenk. *Point-to-Point Security*. Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications. Cham: Springer International Publishing. Chapter 5, pp: 85-98. 2022.

[112] B. Shojaie, I. Saberi, and M. Salleh. *Enhancing EAP-TLS authentication protocol for IEEE 802.11 i*. Wireless Networks, 23, 1491-1508. 2017.

[113] S. Boire, T. Akgün, P. Ginzboorg, P. Laitinen, S. Tamrakar, and T. Aura. *Credential Provisioning and Device Configuration with EAP*. In Proceedings of the 19th ACM International Symposium on Mobility Management and Wireless Access (pp. 87-96). 2021, November.

[114] P. Kumar, and D. Kumar. *DoMT: An Evaluation Framework for WLAN Mutual Authentication Methods*. In Mobile Radio Communications and 5G Networks: Proceedings of Second MRCN 2021 (pp. 345-363). Singapore: Springer Nature Singapore. 2022.

[115] V. Bolgouras. *Combination of the PEAP Protocol with EAP-OpenID Connect.* MSc Dissertation. University of Piraeus, Department of Digital Systems. 2018, March.

[116] S. Ali, T. Osman, M. Mannan, and A. Youssef. *On privacy risks of public wifi captive portals*. In Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26–27, 2019, Proceedings 14 (pp. 80-98). Springer International Publishing. 2019.

[117] N. Marques, A. Zúquete, and J. P. Barraca. *Integration of the Captive Portal paradigm with the 802.1 X architecture*. arXiv preprint arXiv:1908.09927. 2019.

[118] O. Nakhila. *Masquerading techniques in IEEE 802.11 wireless local area networks*. Doctoral Dissertation. Doctor of Philosophy, Department of Electrical and Computer Engineering. College of Engineering and Computer Science. University of Central Florida, Orlando, Florida. 2018.

[119] J. Gierszewski, and M. M. Matuśkiewicz. *Assessment of the effectiveness of the security features of personal wireless networks*. Security and Defence Quarterly, 32. 2020.

[120] R. Guo. *Survey on wifi infrastructure attacks*. International Journal of Wireless and Mobile Computing, 16(2), 97-101. 2019.

[121] A. A. Mughal. *Well-Architected Wireless Network Security*. Journal of Humanities and Applied Science Research, 5(1), 32-42. 2022.

[122] H. A. Abdul-Ghani, and D. Konstantas. *A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective*. Journal of Sensor and Actuator Networks, 8(2), 22. 2019.

[123] M. Dahiya. *Security Issues and Solutions in Wi-Fi*. International Journal of Electronics Engineering Research, 9(5), 773-777. 2017.

[124] S. Benqdara and A. Mahmoud. Wireless security in Libya: a survey paper. International Journal of Computer Applications, 181(35), 26-31. 2019.

[125] M. Maráczi. *Wardriving in eger*. In 2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI) (pp. 000127-000130). 2019, May.

[126] A. Carballal, J. P. Galego-Carro, N. Rodriguez-Fernandez, and C. Fernandez-Lozano. *Wi-Fi Handshake: analysis of password patterns in Wi-Fi networks*. PeerJ Computer Science, 8, e1185. 2020.

[127] J. K. Kim, W. J. Lee, C. B. Chae, and J. H. Kim. *Performance analysis of fair medium access control protocol for asymmetric full duplex in WLAN*. IEEE Access, 8, 140546-140557. 2020.

[128] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy. *Multi-factor authentication: A survey*. Cryptography, 2(1), 1. 2018.

[129] M. Papathanasaki, L. Maglaras, and N. Ayres. *Modern Authentication Methods: A Comprehensive Survey*. AI, Computer Science and Robotics Technology. 2022.

[130] P. Wang, and R. Baskerville. *The Case for Two-Factor Authentication-Evidence from a Systematic Literature Review*. PACIS 2019 Proceedings. 179. 2019.

[131] E. Baray, and N. K. Ojha. *WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique*. In 2021 IEEE 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 23-30). 2021, April.

[132] S. Bhattacharjee, and K. K. Senapati. *Performance Evaluation and Analysis of Wi-Fi Security Protocols*. Intelligent Sustainable Systems: Selected Papers of WorldS4 2022, Volume 1 (pp. 327-338). Singapore: Springer Nature Singapore. 2023.

[133] I. S. Al-Mejibli, and N. R. Alharbe. *Analyzing and evaluating the security standards in wireless network: A review study*. Iraqi Journal for Computers and Informatics, 46(1), 32-39. 2020.

[134] M. Alhamry, and A. Alomary. Exploring Wi-Fi WPA2-PSK protocol weaknesses. In 2022 IEEE International Conference on Data Analytics for Business and Industry (ICDABI) (pp. 190-195). 2022, October.

[135] D. S. M. Narayana, S. B. Nookala, S. Chopra, and U. Shanmugam. *An Adaptive Threat Defence Mechanism Through Self Defending Network to Prevent Hijacking in WiFi Network*. In 2023 IEEE International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS) (pp. 133-138). 2023, April.

[136] K. Juhász, V. Póser, M. Kozlovszky, and A. Bánáti. *WiFi vulnerability caused by SSID forgery in the IEEE 802.11 protocol*. In 2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI) (pp. 333-338). 2019, January.

[137] S. Lindroos, A. Hakkala, and S. Virtanen. *A systematic methodology for continuous WLAN abundance and security analysis*. Computer Networks, 197, 108359. 2021.

[138] H. J. Lu, and Y. Yu. *Research on WiFi penetration testing with Kali Linux*. Complexity, 2021, 1-8. 2021.

[139] A. Imoize, B. Ben-Adeola, and J. Adebisi. *Development of a multifactor-security-protocol system using ambient noise synthesis*. EAI Endorsed Transactions on Security and Safety, 6(22). 2020.

[140] S. M. Jwad, A. J. Alabbasy, and H. A. Hussein. *Review on Network Control and Protection Systems*. Journal of Controller and Converters, 6(03), 34-40. 2021.

[141] J. P. Patra. *Wireless Network Security Threats and Best Method to Warn*. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(12), 4147-4155. 2021.

[142] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin. *A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions*. Electronics, 12(6), 1333. 2023.

[143] D. T. Le, T. T. Tran, K. Q. Dang, R. Alkanhel, and A. Muthanna. *Malware spreading model for routers in Wi-Fi networks.* IEEE Access, 10, 61873-61891. 2022.

[144] A. S. Saini, P. Gupta, and H. Gupta. *Implementation of Secured Wired and WLAN Network Using eNSP*. In Advances in Smart Communication and Imaging Systems: Select Proceedings of MedCom 2020 (pp. 577-590). Springer Singapore. 2021.

[145] P. Pebrianti, I. Kanedi, and Y. Arliando. *The Design and Implementation of Internet-Based Wireless Lan (WLAN) at Rawa Makmur Permai Urban Village Office*. Jurnal Komputer, Informasi dan Teknologi (JKOMITEK), 1(2), 397-406. 2021.

[146] K. S. V. Susmita, and D. P. Kailas. *Portable firewall for data security toward secured communication*. East African Scholars Journal of Engineering and Computer Sciences, 4 (4), 41-45. 2021, May.

[147] I. Al-Shourbaji, and S. Al-Janabi. *Intrusion Detection and Prevention Systems in Wireless Networks*. Kurdistan Journal of Applied Research, 2(3), 267-272. 2017.

[148] P. Satam, and S. Hariri. *WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol*. IEEE Transactions on Network and Service Management, 18(1), 1077-1091. 2020.

[149] J. Lv, D. Man, W. Yang, L. Gong, X. Du, and M. Yu. *Robust device-free intrusion detection using physical layer information of WiFi signals*. Applied Sciences, 9(1), 175. 2019.

[150] W. Yan, S. Hylamia, T. Voigt, and C. Rohner. *PHY-IDS: A physical-layer spoofing attack detection system for wearable devices*. In Proceedings of the 6th ACM Workshop on Wearable Systems and Applications (pp. 1-6). 2020, June.

[151] S. Almjamai. *A Comprehensive Taxonomy of Attacks and Mitigations in IoT Wi-Fi Networks: physical and data-link layer*. Doctoral Thesis. Faculty of Technology, Department of computer science and media technology (CM). Linnaeus University, 2022.

[152] M. Usha, and P. J. W. N. Kavitha. *Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier*. Wireless Networks, 23, 2431-2446. 2017.

[153] K. Kaur and A. Kaur. A Survey of Working on Virtual Private Networks. International Research Journal of Engineering and Technology (IRJET), 6(9), 1340-1343. 2019, September.

[154] U. S. Adekunle. *Factors Affecting Wireless Network Performance in the ICT University, Cameroon Campus*. Doctoral Dissertation. Degree in Information and Communication Technology, Department of Information and Communication Technology. ICT University of Cameroon. 2017, August.

[155] G. Cañizares, and B. Bellalta. *Improving User's Experience through Simultaneous Multi-WLAN Connections*. arXiv preprint arXiv:1712.07738. 2017.

[156] M. Stojanova. *Performance Modeling of IEEE 802.11 WLANs*. Doctoral dissertation, Spécialité de doctorat Informatique. l'Université Claude Bernard Lyon. 2019, December.

[157] O. I. Ikem, J. Eke, and E. C. Kalu. *Modeling Throughput Performance in 802.11 Wireless Local Area Network*. Iconic Research and Engineering (IRE) Journals, 5(10), 121-130. 2022, April.

[158] C. O. Abdullah. *Performance modelling of fairness in IEEE 802.11 wireless LAN protocols*. Doctoral dissertation. School of Computing Newcastle upon Tyne, Newcastle University, United Kingdom. 2019. January.

[159] G. Min, Y. Wu, K. Li, and A. Y. Al-Dubai. *Performance modelling and optimization of integrated wireless LANs and multi-hop mesh networks*. International Journal of Communication Systems, 23(9-10), 1111-1126. 2010.

[160] P. Rathee, R. Singh, and S. Kumar. *Performance Analysis of IEEE 802.11 p in the Presence of Hidden Terminals*. Wireless Personal Communications, 89, 61-78. 2016.

[161] N. Sarkar. *Introduction*. Improving the performance of wireless LANs: A practical guide. Taylor & Francis. Chapter 1, pp: 3-16, 2014.

[162] A. M. Ali, M. R. Hassan, A. Al-Qerem, A. Hamarsheh, K. Al-Qawasmi, M. Aljaidi, ... & J. Lloret. *Towards a Smart Environment: Optimization of WLAN Technologies to Enable Concurrent Smart Services*. Sensors, 23(5), 2432. 2023.

[163] P. Jindal, and B. Singh. *Quantitative analysis of the security performance in wireless LANs*. Journal of King Saud University-Computer and Information Sciences, 29(3), 246-268. 2017.

[164] D. Hoglund, and V. Varga. *Building a Reliable Wireless Medical Device Network*. Global Clinical Engineering Journal, (1), 42-49. 2018.

[165] E. Lopez-Aguilera, E. Garcia-Villegas, and J. Casademont. *Evaluation of IEEE 802.11 coexistence in WLAN deployments*. Wireless Networks, 25(1), 87-104. 2019.

[166] R. Khanduri, S. Rattan, and A. Uniyal. *Understanding the features of IEEE 802. 11g in high data rate wireless LANs*. International Journal of Computer Applications, 64(8), 1-5. 2013.

[167] C. Othman Abdullah, and N. Thomas. *Performance Modelling of IEEE 802.11 g Wireless LAN*. In Proceedings of the 9th EAI International Conference on Performance Evaluation Methodologies and Tools (pp. 71-78). 2016, February.

[168] S. K. Memon, K. Nisar, and W. Ahmad. *Performance evaluation of densely deployed WLANs using directional and omni-directional antennas*. In Computational Science and Technology: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018 (pp. 369-378). Springer Singapore. 2019.

[169] K. Obelovska, O. Panova, and V. Karovič Jr. *Performance analysis of wireless local area network for a high-/low-priority traffic ratio at different numbers of access categories*. Symmetry, 13(4), 693. 2021.

[170] A. Croitoru, D. Niculescu, and C. Raiciu. *Towards wifi mobility without fast handover*. In 12th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 15) (pp. 219-234). 2015.

[171] S. Lan, L. Ma, and J. Huang. *Research and Practice of TCP Protocol Optimization in Mobile Internet*. Cyber Security: 19th China Annual Conference, CNCERT 2022, Beijing, China, August 16–17, 2022, Revised Selected Papers (pp. 187-196). Singapore: Springer Nature Singapore. 2022, December.

[172] N. Sarkar. *Improving WLAN Performance by Modifying MAC Protocols*. Improving the performance of wireless LANs: A practical guide. Taylor & Francis. Chapter 9, pp: 151-182, 2014.

[173] A. Franco. *Improving Throughput and Minimizing Age of Information in dense WLANs, Using Cooperative Techniques*. Licentiate Thesis, Lund University. 2017, December.

[174] C. E. Weng, and H. C. Chen. *The performance evaluation of IEEE 802.11 DCF using Markov chain model for wireless LANs*. Computer Standards & Interfaces, 44, 144-149. 2016.

[175] M. A. Hossain, N. I. Sarkar, J. Gutierrez, and W. Liu. *Performance study of block ACK and reverse direction in IEEE 802.11 n using a Markov chain model*. Journal of Network and Computer Applications, 78, 170-179. 2017.

[176] A. S. Dhaliwal. *Analyzing the Impact of DCF and PCF on WLAN Network Standards 802.11 a, 802.11 b and 802.11 g.* International Journal of Computer and Information Engineering, 7(12), 1594-1598. 2013.

[177] J. Singh, and J. Singh. *Comparative analysis of PCF, DCF, and EDCF over IEEE 802.11 WLANs*. International Journal of Advance research, Ideas and Innovations in Technology, 2. 2016.

[178] W. H. W. Hassan, H. King, S. Ahmed, and M. Faulkner. *Enhancement techniques of IEEE 802.11 wireless local area network distributed coordination function: A review*. ARPN Journal of Engineering and Applied Sciences, 13(3), 1053-1062. 2018.

[179] A. J. Gopinath, and B. Nithya. *Mathematical and simulation analysis of contention resolution mechanism for IEEE 802.11 ah networks*. Computer Communications, 124, 87-100. 2018.

[180] C. Kocak, and H. B. Karakurt. *Fuzzy logic-based performance improvement on MAC layer in wireless local area networks*. Neural Computing and Applications, 31, 6113-6128. 2019.

[181] Mukta, and N. Gupta. *Transform free modeling of finite buffer non-saturated IEEE 802.11 DCF in Ad Hoc networks*. International Journal of Wireless Information Networks, 27(1), 197-206. 2020.

[182] H.S. Bedi, K. K. Sharma, and R. Gupta. *A review paper on performance analysis of IEEE 802.11 e*. In Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019) (pp. 47-56). Springer Singapore. 2020.

[183] A. Eyadeh, M. Jarrah, and A. Aljumaili. *Modeling and simulation of performance limits in IEEE 802.11 point-coordination function*. International Journal of Recent Tech-nology and Engineering, 8(4), 5575-5580. 2019.

[184] N. Sarkar. *Effect of Radio Propagation Environments on WLAN Performance*. Improving the performance of wireless LANs: A practical guide. Taylor & Francis. Chapter 7, pp: 107-134, 2014.

[185] N. I. Sarkar, O. Mussa, and S. Gul. *Impact of People's Movement on Wi-Fi Link Throughput in Indoor Propagation Environments: An Empirical Study*. Electronics, 10(7), 856. 2021.

[186] M. Maadani, and S. A. Motamedi. *A simple and closed-form access delay model for reliable IEEE 802.11-based wireless industrial networks*. Wireless personal communications, 75(4), 2243-2268. 2014.

[187] N. Sarkar. *Effect of AP Configuration and Placement on WLAN Performance*. Improving the performance of wireless LANs: A practical guide. Taylor & Francis. Chapter 10 pp: 183-202, 2014.

[188] N. Sarkar. *Improving WLAN Performance Using CLD Optimization*. Improving the performance of wireless LANs: A practical guide. Taylor & Francis. Chapter 12, pp: 249-272, 2014.

[189] A. Triwinarko, S. Cherkaoui, and I. Dayoub. *Performance of PHY/MAC Cross-Layer Design for Next-Generation V2X Applications*. In 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) (pp. 98-104). 2022, November.

[190] A. Aijaz. *High-performance industrial wireless: Achieving reliable and deterministic connectivity over IEEE 802.11 WLANs*. IEEE Open Journal of the Industrial Electronics Society, 1, 28-37. 2020.

[191] N. Sarkar. *Effect of Routing Protocols on WLAN Performance*. Improving the performance of wireless LANs: A practical guide. Taylor & Francis. Chapter 11, pp: 203-248, 2014.

[192] S. Rezaei, M. Gharib, and A. Movaghar. *Throughput analysis of IEEE 802.11 multi-hop wireless networks with routing consideration: A general framework*. IEEE Transactions on Communications, 66(11), 5430-5443. 2018.

[193] N. Raza, A. Amin, H. Ur, and M. Tariq. *Effect of Node Density over the performance of DSR, TORA, and OLSR Routing Protocols of MANET*. International Journal of Computer Applications, 177(39), 34-41. 2020.

[194] K. Nisar, I. A. Lawal, U. I.Abdulmalik, A. A. Mu'azu, B. S.Chowdhry, S. Khan, and S. Memon. *QoS Analysis of the MANET routing protocols with Respect to Delay, Throughput, & Network load: Challenges and Open Issues*. In 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT) (pp. 1-8). 2020, October.

[195] M. Maadani, and M. Baseri. *Performance evaluation of the OFDM modulation in IEEE 802.11-based wireless industrial networks*. In IEEE 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI) (pp. 451-456). 2015, November.

[196] A. Z. Yonis. *Performance analysis of IEEE 802.11 ac based WLAN in wireless communication systems*. International Journal of Electrical and Computer Engineering, 9(2), 1131. 2019.

[197] N. Sarkar. *Combined Effect of Signal Strength and Traffic Type on WLAN Performance*. Improving the performance of wireless LANs: A practical guide. Taylor & Francis. Chapter 14, pp: 293-317, 2014.

[198] A. M. Ali, M. Dhimish, and M. Alsmadi. *Optimum WLAN Protocol and Network Architecture Identification for VOIP Application*. Journal of Theoretical and Applied Information Technology, 3237-3248. 2020.

[199] P. Dhere, P. Chilveri, R. Vatti, V. Iyer, and K. Jagdale. *Wireless signal strength analysis in a home network.* In IEEE 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT) (pp. 1-5). 2018, March.

[200] T. A. Darsono, and I. H. Wayangkau. *Analysis of WiFi Network Performance Using FDMI Method*. In Journal of Physics: Conference Series (Vol. 1569, No. 4, p. 042005). IOP Publishing. 2020, July.

[201] A. Chhabra. *VoIP QoS Prediction over Wireless Mesh Network Scenario*. International Journal of Computer Science & Communication, 11(2), 52-55. 2020.

[202] J. Govindarajan, and C. Mohanapriya. *Study on real-time media congestion avoidance technique for video streaming over wireless local area network*. Indonesian Journal of Electrical Engineering and Computer Science, 15(3), 1535-1543. 2019.

[203] P. Suhonen. *Radio Frequency Interference Measurements in WLAN Networks*. Master's Thesis in Engineering Information Technology. Helsinki Metropolia University of Applied Sciences. 2019, March.

[204] J. Geier. *Wireless LAN Implications, Problems, and Solutions*. Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications, 2nd Edition. Chapter 4. 2015.

[205] F. Tramarin, A.K. Mok, and S. Han. *Real-time and reliable industrial control over wireless lans: Algorithms, protocols, and future directions*. Proceedings of the IEEE, 107(6), 1027-1052. 2019.

[206] J. Saldana, J. Ruiz-Mas, J. Fernández-Navajas, J. L. S. Riaño, J. P. Javaudin, J. M. Bonnamy, and M. Le Dizes. *Attention to Wi-Fi diversity: Resource management in WLANs with heterogeneous APs*. IEEE Access, 9, 6961-6980. 2021.

[207] Z. Haider, M. Saleem, and T. Jamal. *Analysis of interference in wireless networks*. arXiv preprint arXiv:1810.13164. 2018.

[208] S.Lindroos, A.Hakkala, and S. Virtanen. *Battle of the Bands: A Long-Term Analysis of Frequency Band and Channel Distribution Development in WLANs*. IEEE Access, 10, 61463-61471. 2022.

[209] T. Oyedare, V. K. Shah, D. J. Jakubisin, and J. H. Reed. *Interference suppression using deep learning: Current approaches and open challenges*. IEEE Access. 2022.

[210] D. Kandar, P. Chyne, S. Nath Sur, and S. Nandi. *A study on the channel bonding in IoT networks: Requirements, applications, and challenges*. International Journal of Communication Systems, 36(6), e5443. 2023.

[211] S. Grunau, D. Block, and U. Meier. *Multi-label wireless interference identification with convolutional neural networks*. arXiv preprint arXiv:1804.04395. 2018.

[212] S. Bayhan, A. Zubow, and A. Wolisz. *Coexistence gaps in space: Cross-technology interference-nulling for improving LTE-U/WiFi coexistence*. arXiv preprint arXiv:1710.07927. 2017.

[213] G. Naik, J. Liu, and J. M. J. Park. *Coexistence of wireless technologies in the 5 GHz bands: A survey of existing solutions and a roadmap for future research*. IEEE Communications Surveys & Tutorials, 20(3), 1777-1798. 2018.

[214] E. Saltikoff, J. Y. Cho, P. Tristant, A. Huuskonen, L. Allmon, R. Cook, ... , and P. Joe. *The threat to weather radars by wireless technology*. Bulletin of the American Meteorological Society, 97(7), 1159-1167. 2016.

[215] T. Pulkkinen, J. K. Nurminen, and P. Nurmi. *Understanding wifi cross-technology interference detection in the real world*. In 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS) (pp. 954-964). 2020, November.

[216] W. Liu, Y. Xia, M. Xu, J. Xie, R. Luo, and D. Huang. *Distributed and accurate packet reception rate estimation under cross-technology interference*. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-6). 2020, December.

[217] W. Wang, D. He, W. Jia, X. Chen, T. Gu, H. Liu, ... , and F. Wu. *PRComm: Anti-interference cross-technology communication based on pseudo-random sequence*. In Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021) (pp. 163-175). 2021, May.

[218] S. N. Arinze, G. N. Onoh, and D. O. Abonyi. *Performance of Light Fidelity and Wireless Fidelity Networks in a Wlan.* Int. J. Res. Eng. Sci., 4(1), 10-20. 2020.

[219] O. Z. Batur, M. Koca, and G. Dundar. *Measurements of impulsive noise in broad-band wireless communication channels*. In IEEE 2008 Ph. D. Research in Microelectronics and Electronics (pp. 233-236). 2008, June.

[220] K. A. Saaifan, and W. Henkel. *Measurements and modeling of impulse noise at the 2.4 GHz wireless LAN band*. In 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP) (pp. 86-90). 2017, November.

[221] A. H. Adnan, M. Abdirazak, A. S. Sadi, T. Anam, S. Z. Khan, M. M. Rahman, and M. M. Omar. *A comparative study of WLAN security protocols: WPA, WPA2*. In IEEE 2015 International Conference on Advances in Electrical Engineering (ICAEE) (pp. 165-169). 2015, December.

[222] T. Hayajneh, S. Ullah, B. J. Mohd, and K. S. Balagani. *An enhanced WLAN security system with FPGA implementation for multimedia applications*. IEEE Systems Journal, 11(4), 2536-2545. 2015.

[223] T. A. T. Aziz, M. R. Abd Razak, and N. E. A. Ghani. *The performance of different IEEE802. 11 security protocol standard on 2.4 GHz and 5GHz WLAN networks*. In IEEE 2017 International Conference on Engineering Technology and Technopreneurship (ICE2T) (pp. 1-7). 2017, September.

[224] P. Jindal, and B. Singh. *Security-performance tradeoffs in a class of wireless network scenarios*. Journal of Network and Systems Management, 25, 83-121. 2017.

[225] P. K. Pant. *The impact of sgi and rts/cts in wlan throughput*. In IEEE 2020 International Conference on Intelligent Engineering and Management (ICIEM) (pp. 207-211). 2020, July.

[226] S. S. Kolahi, and A. A. Almatrook. *Impact of security on bandwidth and latency in IEEE 802.11 ac client-to-server WLAN*. In IEEE 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 893-897). 2017, July.

[227] A. Tsetse, E. Bonniord, P. Appiah-Kubi, and S. Tweneboah-Kodua. *Performance Study of the Impact of Security on 802.11 ac Networks*. In Information Technology-New Generations: 15th International Conference on Information Technology (pp. 11-17). Springer International Publishing. 2018.

[228] M. K. Ray. *Cross Layer Design in Wireless Local Area Networks (WLANs): Issues and Possible Solutions*. Carleton University. 2022, May.

[229] U. Singh. *Impact of Transmission Power on the Performance of Secure Wireless Network*. Master Thesis. Department of Electronics & Communication Engineering, National Institute of Technology, Kurukshetra, Haryana. 2018.

[230] L. Caldas-Calle, J. Jara, M. Huerta, and P. Gallegos. *QoS evaluation of VPN in a Raspberry Pi devices over wireless network.* In IEEE 2017 International Caribbean Conference on Devices, Circuits and Systems (ICCDCS) (pp. 125-128). 2017, June.

[231] A. Ali, M. Dhimish, and P. Mather. *WLAN protocol and network architecture selection for real-time applications*. International Journal of Advance Computational Engineering and Networking (IJACEN). 2019.