ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

Διπλωματική Εργασία

Τεχνικές και Εφαρμογές Συστημάτων Επικοινωνίας 5G

Συγγραφέας: Δημήτριος Δημητρίου

ΑΜ: 71446632

Επιβλέπων Καθηγητής: Μιχαήλ Παπουτσιδάκης

Συνεπιβλέπουσα: Ελένη Συμεωνάκη

Αθήνα, Μάρτιος 2023

UNIVERSITY OF WEST ATTICA SCHOOL

SCHOOL OF ENGINEERING

DEPARTMENT OF INDUSTRIAL DESIGN & PRODUCTION ENGINEERING

Diploma Thesis

Techniques and Applications of 5G Communication Systems

Student: Dimitrios Dimitriou

Registration Number: 71446632

Supervisor: Michail Papoutsidakis

Co-supervisor: Eleni Symeonaki

Athens, March 202

ΤΕΧΝΙΚΕΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΥΣΤΗΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ 5G

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	ΜΙΧΑΗΛ ΠΑΠΟΥΤΣΙΔΑΚΗΣ	ΚΑΘΗΓΗΤΗΣ	Michail Papoutsidakis Digitally signed by Michail Papoutsidakis Date: 2023.05.15 20:15:26 +03'00'
2	ΑΒΡΑΑΜ ΧΑΤΖΟΠΟΥΛΟΣ	ΛΕΚΤΟΡΑΣ	AVRAAM CHATZOPOULOS Digitally signed by AVRAAM CHATZOPOULOS Date: 2023.05.16 09:41:47 +03'00'
3	ΕΛΕΝΗ ΣΥΜΕΩΝΑΚΗ	ΕΔΙΠ Α΄	Eleni Symeonaki Digitally signed by Eleni Symeonaki Date: 2023.05.15 15:41:10 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ/ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Δημητρίου Δημήτριος του Κωνσταντίνου , με αριθμό μητρώου 71446632 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Βιομηχανικής Σχεδίασης και Παραγωγής , δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Δημητρίου Δημήτριος

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία πραγματεύεται τις τεχνικές και τις εφαρμογές των συστημάτων επικοινωνίας 5G. Αρχικά επιχειρείται η εισαγωγή στα ασύρματα δίκτυα και συγκρίνονται οι τεχνολογίες από το 1G έως το 5G.

Στο 2ο Κεφάλαιο, περιγράφονται οι τεχνικές μετάδοσης των συστημάτων 5G και αναλύεται η αρχιτεκτονική τους, το Δίκτυο πυρήνα καθώς επίσης και ο κατακερματισμός του. Επιπλέον, αναλύονται οι τεχνολογίες IOT, Cloud και Fog, οι οποίες συνδυάζονται με την τεχνολογία 5G, ενώ γίνεται διεξοδική περιγραφή των τύπων των επιθέσεων στα συστήματα 5G και τα μέτρα ασφάλειας.

Τέλος, στο 3ο Κεφάλαιο περιέχει τα σενάρια χρήσης και τις κυριότερες εφαρμογές των συστημάτων 5G και η εργασία ολοκληρώνεται με χρήσιμα συμπεράσματα.

Λέξεις Κλειδιά: *Ασύρματα δίκτυα, αρχιτεκτονική, ασφάλεια, εφαρμογές, 5G, IOT, Cloud, Fog*

ABSTRACT

This dissertation deals with the techniques and applications of 5G communication systems. Initially, is attempted an introduction of wireless networks and a comparation of technologies from 1G to 5G.

Chapter 2 describes the transmission techniques of 5G systems and analyzes their architecture, the Core Network as well as its fragmentation. In addition, are analyzed the IoT, Cloud and Fog technologies, which are combined with 5G technology, while the types of attacks on 5G systems and security measures are described in detail.

Finally, Chapter 3 contains the usage scenarios and the main applications of 5G systems. The dissertation is completed with useful conclusions.

Keywords: *Wireless networks, architecture, security, applications, 5G, IoT, Cloud*

ΑΝΑΓΝΩΡΙΣΕΙΣ

Αρχικά, θα ήθελα να εκφράσω τις ειλικρινείς ευχαριστίες μου στον επιβλέποντα καθηγητή κ. Μιχαήλ Παπουτσιδάκη και στη συνεπιβλέπουσα κ. Ελένη Συμεωνάκη για τη συνεχή υποστήριξη της πτυχιακής μου διατριβής και για την υπομονή καθώς και για τα κίνητρα που μου έδωσαν. Με τις διαρκείς συζητήσεις μας με βοήθησαν να καταλάβω ποια βήματα έπρεπε να ακολουθήσω για να ολοκληρώσω με επιτυχία τη διατριβή μου, όπου με τα διορατικά σχόλια και τις δύσκολες ερωτήσεις τους με βοήθησαν να διευρύνω την έρευνά μου από διάφορες οπτικές γωνίες.

Θα ήθελα επίσης να εκφράσω τη βαθύτατη εκτίμηση στους συναδέλφους μου που διάβασαν και σχολίασαν τη διατριβή μου.

Ευχαριστώ τους γονείς μου που με στήριξαν για την ολοκλήρωση της πτυχιακής μου διατριβής. Επίσης για την υπομονή, την ενθάρρυνση και την υποστήριξη.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ ΚΑΙ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Στο 1ο Κεφάλαιο της εργασίας γίνεται μια εισαγωγή στην εξέλιξη των ασύρματων δικτύων. Περιγράφονται οι Ευρυζωνικές Συνδέσεις, οι Αρχιτεκτονικές και γίνεται μια σύντομη σύγκριση των τεχνολογιών κινητής τηλεφωνίας, ξεκινώντας από το 1G και φθάνοντας στο 5G.

Εν συνεχεία, το 2ο Κεφάλαιο, περιλαμβάνει τις τεχνικές μετάδοσης των συστημάτων 5G. Συγκεκριμένα, αναλύεται η αρχιτεκτονική του συστήματος 3GPP 5G, το Δίκτυο πυρήνα (Core Network), καθώς επίσης και ο κατακερματισμός (slicing) του Δικτύου 5G. Επιπλέον, γίνεται εκτενής αναφορά στις υπηρεσίες των δεδομένων στην Αρχιτεκτονική 5G και στα εφαρμοζόμενα πρότυπα.

Ταυτόχρονα, δεδομένου ότι η τεχνολογία 5G δύναται να συνδυαστεί με τις τεχνολογίες IOT, Cloud και Fog, κρίθηκε σκόπιμη η περιγραφή των εν λόγω τεχνολογιών. Πιο αναλυτικά, ορίζονται και περιγράφονται οι ανωτέρω τεχνολογίες και ορισμένα βασικά χαρακτηριστικά τους, ενώ γίνεται αναφορά στην έννοια της ετερογενούς σύνθεσης δεδομένων, στους αισθητήρες και τους ενεργοποιητές που τοποθετούνται σε αυτά τα συστήματα, καθώς στις απαιτήσεις ασφάλειας. Τέλος, στο 2ο Κεφάλαιο περιγράφονται αναλυτικά οι τύποι επιθέσεων σε συστήματα 5G και τα αντίστοιχα αντίμετρα.

Το 3ο Κεφάλαιο έχει σχέση με τις εφαρμογές της κινητής επικοινωνίας 5G. Περιλαμβάνει τα σενάρια χρήσης και τις εφαρμογές σε συστήματα 5G, όπως είναι οι έξυπνοι μετρητές, η εφαρμογή στη βιομηχανία, η επαυξημένη και εικονική πραγματικότητα, η ρομποτική, το Έξυπνο γραφείο (Smart office), το διάχυτο βίντεο, η μαζική συγκέντρωση, το βίντεο υψηλής ευκρίνειας, οι φαρμογές στην καταναλωτική αγορά, το Gaming Media on Demand, η έξυπνη υγεία και τα οχήματα.

Η εργασία ολοκληρώνεται με την εξαγωγή χρήσιμων συμπερασμάτων για την νέα τεχνολογία 5G που έχει εισέλθει στη ζωή μας.

ΚΕΦΑΛΑΙΟ 1ο: Εισαγωγή στην εξέλιξη των ασύρματων δικτύων

1.1 Η πορεία εξέλιξης των ασύρματων δικτύων

Η ραγδαία ανάπτυξη της τεχνολογίας κυρίως τις τελευταίες δεκαετίες έχει επηρεάσει τις περισσότερες εκφάνσεις της καθημερινότητας των ανθρώπων τόσο με θετικό όσο και με αρνητικό τρόπο. Οι αυξημένες ανάγκες ζωής των σύγχρονων κοινωνιών αυξάνουν διαρκώς τις απαιτήσεις για τη δημιουργία νέων καινοτόμων εφαρμογών και τεχνολογικών επιτευγμάτων.

Στο πλαίσιο αυτό αποτελεί κοινή διαπίστωση ότι οι νέοι είναι ιδιαίτερα ευεπίτευκτοι στη χρήση νέων τεχνολογιών και μπορούν να χειρίζονται από νεαρή ηλικία έξυπνες συσκευές όπως τα smartphones καθώς και κάθε είδους ηλεκτρονικές εφαρμογές. Θα πρέπει ωστόσο να αναγνωρίσουμε ότι στην αλματώδη εξέλιξη της τεχνολογίας συνέβαλαν καθοριστικά οι τηλεπικοινωνίες με τα προηγμένα συστήματα μετάδοσης της πληροφορίας. Ειδικότερα, οι ανάπτυξη των έξυπνων συσκευών, σε συνδυασμό με τις εφαρμογές και τις υπηρεσίες των ευρυζωνικών τηλεπικοινωνιακών δημιούργησε ένα πεδίο αλληλεπίδρασης των χρηστών σε παγκόσμια κλίμακα.

Μέσα στο παραπάνω πλαίσιο αναπτύσσονται διαρκώς στα τηλεπικοινωνιακά συστήματα νέες τεχνολογίες καθιστώντας απλούστερη, αποδοτικότερη και με μεγαλύτερη ποιότητα τη δικτύωση ανάμεσα στους χρήστες ανά τον κόσμο.

Η πρώτη ασύρματη δικτύωση έγινε το 1901 με την κατασκευή του ασύρματου τηλέγραφου του Marconi με χρήση του κώδικα μορς, θέτοντας τον θεμελιώδη στην ανάπτυξη των ψηφιακών συστημάτων μέσω της άλγεβρας Boole.

Το 1960 δημιουργήθηκαν τα πρώτα ασύρματα δίκτυα, τα RF δίκτυα με την τεχνολογία TCP/IP. Η πρώτη περιγραφή του όρου πακέτο δεδομένων, έγινε από τον D. Davies ενώ λίγο αργότερα έλαβαν χώρα οι πρώτες δοκιμές μεταγωγής πακέτων.

Ακολούθησε η μετάδοση πακέτων με την τεχνολογία των ασυρμάτων δικτύων. Η εισαγωγή των μικροϋπολογιστών στο τέλος της δεκαετίας του 80 προοιωνίζει την ραγδαία εξάπλωση των ασύρματων ζεύξεων με την ανάπτυξη των πρώτων ολοκληρωμένων τοπικών ασύρματων δικτύων LAN (Local Area Network) με την ονομασία ALOHA στο Πανεπιστήμιο της Χαβάης.

Από την δεκαετία του 90 και έπειτα, ξεκίνησε η κορύφωση των ασύρματων τεχνολογιών

μέσω της εισαγωγής νέων καινοτόμων συσκευών και προϊόντων ασύρματης επικοινωνίας στην παγκόσμια αγορά.

Πλέον η πλειοψηφία των χρηστών κατέχει νέου τύπου κινητά τηλέφωνα - smartphones, καθώς και φορητές ηλεκτρονικές συσκευές laptop, tablet κ.τ.λ τα οποία μπορούν να προμηθευτούν με χαμηλό ή υψηλό κόστος ανάλογα τα χαρακτηριστικά τους και τα οποία παρέχουν μεγάλη υπολογιστική ισχύ και ποιότητα υπηρεσιών ανάλογη με των σταθερών ηλεκτρονικών υπολογιστών.

Οι εταιρείες τεχνολογικού εξοπλισμού επικέντρωσαν το ερευνητικό τους ενδιαφέρον στην ανάπτυξη νέων προτύπων των ασύρματων επικοινωνιών για την υποστήριξη νέων προϊόντων τύπου έξυπνων συσκευών. Ωστόσο η εκτεταμένη χρήση των συσκευών αυτών δημιούργησε απαιτήσεις από την πλευρά των χρηστών για την εξασφάλιση υψηλών ταχυτήτων στην ανταλλαγή των δεδομένων. Παράλληλα δημιουργήθηκε η απαίτηση για την ανάπτυξη νέων υπηρεσιών, προϊόντων και εφαρμογών σε διάφορους τομείς δραστηριοτήτων.

Όλα τα παραπάνω είχαν ως αποτέλεσμα την ουσιαστική βελτίωση των ασύρματων δικτύων σε επίπεδο ταχύτητας οι οποίες πλέον δύνανται να ξεπεράσουν τις αντίστοιχες των ενσύρματων δικτύων (Wicks & Kemerling, 2003).

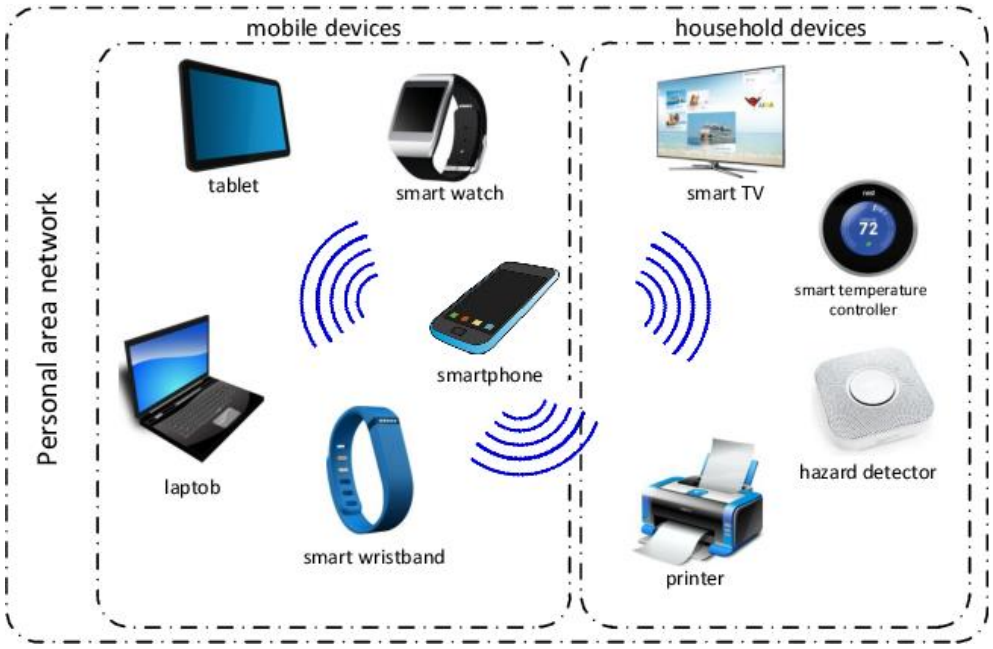
Με τα πρώτα συστήματα κυψελωτών δικτύων κινητής τηλεφωνίας 1G και 2G επακολούθησε η ανάπτυξη του Bluetooth, του GPRS (General Packet Radio Service), του HI.P.E.R.LAN του Ευρωπαϊκού Οργανισμού Τηλεπικοινωνιών ETSI καθώς και η δημιουργία των προτύπων 802.11 WLAN και 802.16 του οργανισμού IEEE.

Εν συνεχεία, αναπτύχθηκαν τα δίκτυα τρίτης και τέταρτης γενιάς 3G και 4G τα οποία σε συνδυασμό με το UMTS (Universal Mobile Telecommunication System) και το LTE (Long Term Evolution) παρείχαν υψηλούς ρυθμούς ασύρματης μετάδοσης δεδομένων.

Τα ασύρματα δίκτυα μπορούν να ταξινομηθούν βάσει της περιοχής κάλυψης σε (Rappaport, 2016):

i. Δίκτυα προσωπικής περιοχής – PAN (Personal Area Network).
ii. Δίκτυα τοπικής περιοχής – LAN (Local Area Network).
iii. Δίκτυα ευρείας περιοχής – WAN (Wide Area Network).

Τα προσωπικά δίκτυα PAN ή WPAN, είναι περιστασιακά δίκτυα κλειστής εμβέλεια τα οποία λειτουργούν χωριστά από το ενσύρματο ή ασύρματο δίκτυο δημιουργώντας ένα προσωρινό δίκτυο μέσω του πρωτοκόλλου Bluetooth. Πρακτικά πρόκειται για δίκτυα μικρής εμβέλειας που απευθύνονται σε ένα άτομο για τη διασύνδεση προσωπικών συσκευών (Shen et al., 2016).



Εικόνα 1.1: Διασύνδεση συστήματος PAN

(Πηγή: Shen et al., 2016).

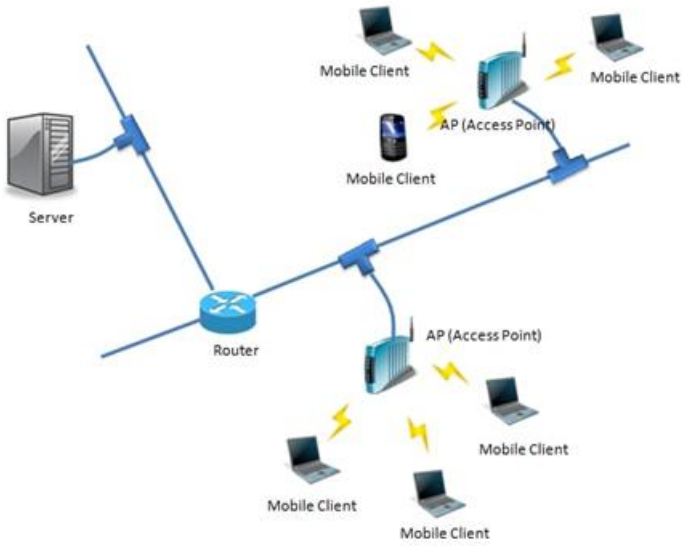
Τα εν λόγω δίκτυα προσφέρουν ένα ικανοποιητικό πεδίο εφαρμογών σε συσκέψεις, συνέδρια, στην τηλεϊατρική, στην ψυχαγωγία κ.α.

Στα ασύρματα δίκτυα WLAN κάθε συσκευή διαθέτει ασύρματο router και κεραία ώστε να επικοινωνεί με τα υπόλοιπα συστήματα. Ένα WLAN δύναται να συνδεθεί με ένα ενσύρματο LAN ή να δημιουργήσει ένα νέο δίκτυο. Ανάλογα με την ισχύ, τα χαρακτηριστικά της περιοχής του δικτύου και τα εμπόδια που παρεμβάλλονται, η εμβέλεια μπορεί να μεταβάλλεται παρέχοντας μεγαλύτερες ή μικρότερες περιοχές κάλυψης. Οι συσκευές που συνδέονται σε ένα WLAN είναι φορητούς υπολογιστές, smartphone, tablet, έξυπνες τηλεοράσεις, αποκωδικοποιητές, κονσόλες παιχνιδιών, εκτυπωτές Wi-Fi και άλλα (Salman, 2020).

Για την δικτύωση υπολογιστών μπορεί να χρησιμοποιηθεί ένα σημείο ασύρματης πρόσβασης (WAP, Wireless Access Point) ή γενικότερα ένα σημείο πρόσβασης (AP). Πρακτικά πρόκειται για συσκευή που επιτρέπει τη σύνδεση ασύρματων συσκευών σε ένα ενσύρματο δίκτυο. Ένα σημείο πρόσβασης AP διαφέρει από ένα hotspot το οποίο αναφέρεται στη φυσική τοποθεσία όπου διατίθεται πρόσβαση WiFi σε ένα WLAN. Ένα AP συνδέεται απευθείας σε ένα ενσύρματο τοπικό δίκτυο, π.χ. Ethernet, και μπορεί να υποστηρίξει τη σύνδεση πολλαπλών ασύρματων συσκευών μέσω της ενσύρματης σύνδεσης τους. Συναντάται μάλιστα σχεδόν παντού από οικίες μέχρι εμπορικά κέντρα (Soewito et al., 2017).

Είναι προφανές ότι η δυνατότητα ασύρματης πρόσβασης στο Internet αποτελεί πλέον απαίτηση των καταναλωτών καθώς υπάρχουν αυξημένες ανάγκες δραστηριοτήτων που προϋποθέτουν την ασύρματη πρόσβαση στο διαδίκτυο. είναι πλέον μία ανάγκη.

Όπως προαναφέραμε, το Access Point έχει τη δυνατότητα σύνδεσης των κυψελών του WLAN με ένα ενσύρματο LAN όπως φαίνεται στην Εικόνα 1.2.

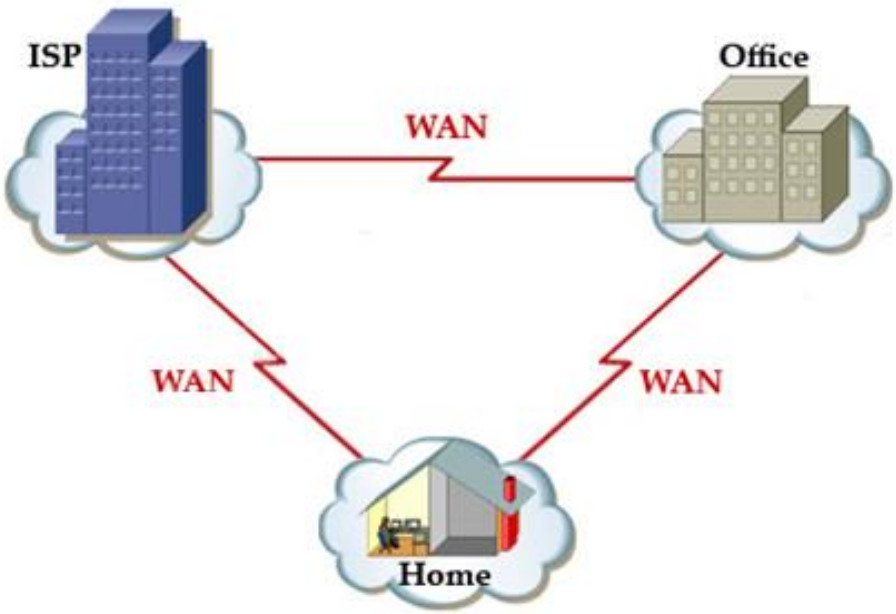


Εικόνα 1.2: Τοπολογία WLAN

(Πηγή: https://www.itrelease.com/2020/10/what-is-wlan)

Παράλληλα, τα access points χρησιμοποιούν κατάλληλο λογισμικό το οποίο επιτρέπει τη συμβατότητα επικοινωνίας μεταξύ διαφορετικών τεχνολογιών δικτύωσης όπως για παράδειγμα WLAN με 3G και 4G.

Ακόμα, ένα άλλο ασύρματο δίκτυο είναι το WAN. Το WAN είναι δίκτυο υπολογιστών το οποίο εκτείνεται σε μια μεγάλη γεωγραφική περιοχή και συχνά κατασκευάζεται από μισθωμένα τηλεπικοινωνιακά κυκλώματα (Soewito et al., 2017).



Εικόνα 1.3: Τοπολογία WAN

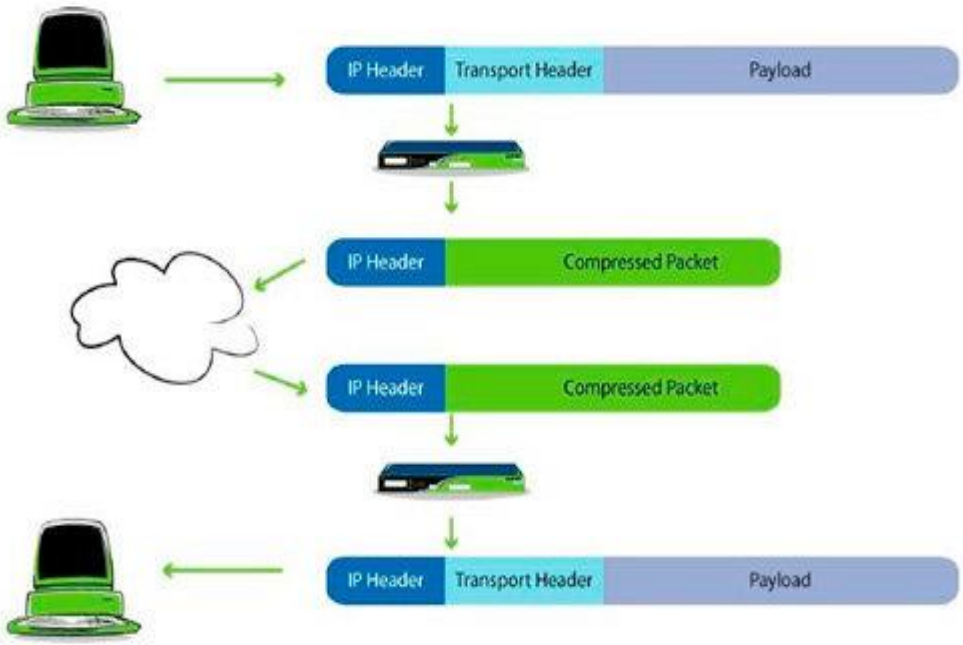
(Πηγή: https://www.9tut.com/wan-tutorial)

Το WAN συνδέει υπολογιστές μεταξύ υποκαταστημάτων και κεντρικών γραφείων σε διαφορετικές πόλεις ή χώρες. Κάθε υπολογιστής σε κάθε γραφείο έχει εφαρμογές για τον χρήστη και αποτελεί τον κεντρικό υπολογιστή. Το δίκτυο που συνδέει τους κεντρικούς υπολογιστές ονομάζεται υποδίκτυο. Το υποδίκτυο αναλαμβάνει να μεταφέρει τις πληροφορίες μεταξύ των κεντρικών υπολογιστών. Παράλληλα δίνεται έμφαση στην βελτιστοποίηση των WAN ώστε να αυξήσουν την απόδοση μεταφοράς των δεδομένων στα δίκτυα της ευρείας περιοχής (Soewito et al., 2017).

Προς αυτή την κατεύθυνση χρησιμοποιούνται διάφορες τεχνικές όπως οι ακόλουθες:

i. Συμπίεση – Compression. Η μέθοδος δέχεται ροές δεδομένων και αποδίδει μια συρρικνωμένη έκδοση τους, εξοικονομώντας εύρος ζώνης (bandwidth) (Εικόνα 1.4).

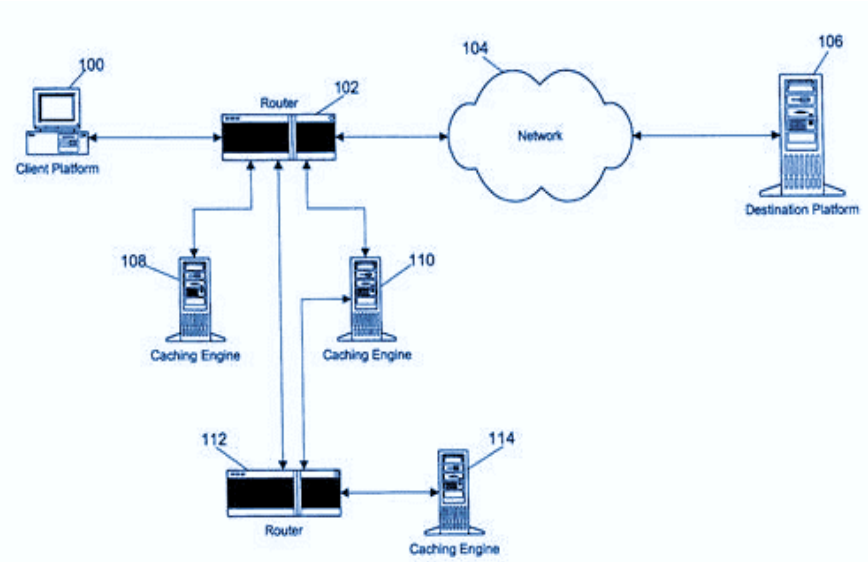
ii. Deduplication: Με την τεχνική αυτή μειώνονται τα δεδομένα καθώς αναγνωρίζονται οι επικαλύψεις-επαναλήψεις των bytes.



Εικόνα 1.4: Βελτιστοποίηση WAN με τη μέθοδο της Συμπίεσης

(Πηγή: Soewito et al., 2017)

iii. Web Caching - προσωρινή αποθήκευση. Με την εν λόγω τεχνική μειώνονται τα δεδομένα καθώς αποθηκεύεται μια πρόσφατη έκδοσή τους στη μνήμη cache. Σε περίπτωση που απαιτηθούν σε επόμενη φορά και βρίσκονται στην cache, αποστέλλεται αντίγραφό τους παρακάμπτοντας την ανάγκη επαναποστολής.



Εικόνα 1.5: Βελτιστοποίηση WAN με τη μέθοδο Cashing

(Πηγή: Soewito et al., 2017)

Αναμφισβήτητα, τα δίκτυα κινητής τηλεφωνίας παρέχουν πλέον μεγάλες ταχύτητες μετάδοσης των δεδομένων οι οποίες φτάνουν τις ταχύτητες των σταθερών δικτύων Ethernet LAN.

Τα τηλεπικοινωνιακά συστήματα παρέχουν ευρυζωνικές υπηρεσίες οι οποίες καλούνται να καλύψουν υψηλές απαιτήσεις εφαρμογών σε ρυθμούς μετάδοσης όπως το video on demand, το live streaming, τα ηλεκτρονικά παιχνίδια κ.α., με μικρή καθυστέρηση και υψηλό QOS (Quality of Service).

Το Cloud, ως εργαλείο της ψηφιακής τεχνολογίας παρέχει τη δυνατότητα αποθήκευσης δεδομένων διαδικτυακά σε κάποιο server παρέχοντας τις απαιτούμενες εγγυήσεις για την ασφάλεια των πληροφοριών. Για να εξασφαλιστεί η μεγάλη ταχύτητα μετάδοσης των δεδομένων με υψηλό QOS, η επεξεργασία από τις εφαρμογές οφείλει να πραγματοποιείτε πλησίον των τελικών χρηστών. Καθώς τα κέντρα δεδομένων των Cloud αποθηκεύουν τα δεδομένα μας κάπου κεντρικά μέσα στο διαδίκτυο, μας δίνεται η δυνατότητα πρόσβασης σε αυτά από οπουδήποτε, ανεξαρτήτως της συσκευής που χρησιμοποιούμε. Απολαμβάνουμε δηλαδή την πρόσβαση στα δεδομένα μας μέσω tablet, laptop, smartphone κλπ. στη δουλειά, στις διακοπές, στον δρόμο και εν γένει οπουδήποτε.

Στο πλαίσιο αυτό το Fog Computing παρέχει αυξημένη αποδοτικότητα στις εφαρμογές. Η Fog παρέχει υπηρεσίες δεδομένων, υπολογισμού, αποθήκευσης αλλά και εφαρμογών με εγγύτητα και υψηλή ποιότητα, προσφέροντας στους τελικούς χρήστες μια ανώτερη εμπειρία υπηρεσιών.

Επιπρόσθετα, με το Fog Computing αντισταθμίζονται πολλές τεχνικές δυσκολίες όπως είναι η μικρή ισχύς των ασύρματων δικτύων των αισθητήρων, το περιορισμένο εύρος ζώνης, η μικρή ικανότητα επεξεργασίας των κατανεμημένων κόμβων κ.α.

Ένα ιδιαίτερο ζήτημα που χρήσει μεγάλης ανάλυσης είναι η ασφάλεια και η ακεραιότητα των δεδομένων που αποθηκεύονται ή ανταλλάσσονται καθώς η απόσταση της διαδρομής που διανύουν καθορίζει το κατά πόσο γίνονται ευάλωτα σε επιθέσεις. Μικρές διαδρομές δεδομένων από τους χρήστες στους servers συνεπάγονται μειωμένο κίνδυνο επιθέσεων. Το Fog computing έχει την ικανότητα εντοπισμού της ελάχιστης απόστασης διαδρομής των δεδομένων συγκριτικά με το Cloud computing.

Επίσης, ανάμεσα στα πλεονεκτήματα του fog computing είναι ότι οι κόμβοι ομίχλης είναι κατανεμημένοι πλησίον των άκρων των δικτύων των χρηστών με αποτέλεσμα οι

επιθέσεις που μπορούν δυνητικά να πραγματοποιηθούν να είναι δύσκολα επιτυχείς. Αυτό οφείλεται στο ότι οι hackers θα πρέπει να διαθέσουν εκτεταμένους πόρους για την υλοποίηση του σκοπού τους, γεγονός που δρα αποτρεπτικά στην εξαπόλυση επιθέσεων.

Η επιλογή ανάμεσα στο Fog και το Cloud computing εξαρτάται κυρίως από τις ανάγκες, τους σκοπούς και το κόστος υλοποίησης των διάφορων λειτουργιών που καλούνται να εκτελέσουν. Για τον λόγο αυτό τα δυο συστήματα συνυπάρχουν και λειτουργούν εναλλακτικά ως ξεχωριστές τεχνολογίες, που εξυπηρετούν διαφορετικές ανάγκες και απαιτήσεις (Firdhous et al., 2014).

Βάσει των ως άνω αναφερόμενων, προκύπτει το συμπέρασμα ότι για την αύξηση της ποιότητας εξυπηρέτησης απαιτούνται υψηλοί ρυθμοί μετάδοσης των δεδομένων για τα οποία η εξέλιξη της τεχνολογίας πραγματοποιεί διαρκώς μελέτες και δοκιμές προς τη βελτιστοποίηση των παρεχόμενων υπηρεσιών. Η διατήρηση του ρυθμού ανάμεσα στο σημείο πρόσβασης και την εκάστοτε συσκευή χρήστη καθώς και η αδιάλειπτη παροχή υπηρεσιών αποτελεί δέσμευση των παρόχων στο πλαίσιο μιας εξόχως ανταγωνιστικής αγοράς.

1.2 Ευρυζωνικές Συνδέσεις και έξυπνα Τηλέφωνα

Είναι γνωστό ότι οι πρώτες ευρυζωνικές συνδέσεις έγιναν στα δίκτυα κινητής τηλεφωνίας τρίτης γενιάς. Οι ανάγκες για υπηρεσίες υψηλότερου ρυθμού μετάδοσης δεδομένων και αυξημένης φασματικής απόδοσης οδήγησε στη δημιουργία του προτύπου UMTS. Το πρότυπο IMT-2000 είχε ως στόχο ανάμεσα στα υπόλοιπα, την ομοιομορφία στη σχεδίαση των συστημάτων, τη συμβατότητα μεταξύ των υπηρεσιών, την παροχή υψηλής ποιότητας υπηρεσιών και τη δυνατότητα περιαγωγής σε παγκόσμια κλίμακα (Grossglauser & Tse, 2002).

Επίσης, καθορίστηκαν οι προϋποθέσεις για την επίτευξη των παραπάνω στόχων και ειδικότερα η μερική κάλυψη και κινητικότητα για κινητά τερματικά με ρυθμό μέχρι 2Mb/s και η πλήρης κάλυψη και κινητικότητα για κινητά τερματικά με ρυθμό μέχρι 384Kb/s. Ως τεχνική πολλαπλής πρόσβασης επιλέχθηκε η ευρυζωνική CDMA (πολλαπλή πρόσβαση διαίρεσης κώδικα). Η τεχνική αυτή επιτρέπει σε πολλά άτομα σε διαφορετικά κινητά τηλέφωνα να πολυπλέκονται μέσω του ίδιου καναλιού ώστε να μοιράζονται ένα εύρος ζώνης συχνοτήτων. Η πολυπλεξία των υπηρεσιών συνδυάζει διαφορετικές

απαιτήσεις αναφορικά με την καθυστέρηση και την ποιότητα και επιτρέπει τη συνύπαρξη μεταξύ συστημάτων διαφορετικών γενιών. Βασικό πλεονέκτημα της CDMA είναι η ανταπόκριση στις μεταβαλλόμενες απαιτήσεις ποιότητας ανάλογα της παρεχόμενης υπηρεσίας, η υποστήριξη της ασύμμετρης τηλεπικοινωνιακής κίνησης και η μεγάλη φασματική απόδοση (Grossglauser & Tse, 2002; Rappaport, 2006).

Η ευρυζωνικότητα διαμορφώνει ένα εξελιγμένο τεχνολογικό περιβάλλον εντός του οποίου εκτελούνται γρήγορες διαδικτυακές συνδέσεις μέσω των κατάλληλων υποδομών για την παροχή ευρυζωνικών εφαρμογών και υπηρεσιών (Albert, & Indra, 2000).

Πιο συγκεκριμένα, ένα ευρυζωνικό περιβάλλον (Rappaport, 2006):

i. παρέχει γρήγορες συνδέσεις στο διαδίκτυο σε μεγάλο τμήμα του πληθυσμού σε τιμές ανταγωνιστικές
ii. υποστηρίζει τις υπάρχουσες και τις μελλοντικές δικτυακές εφαρμογές
iii. παρέχει αδιάλειπτη σύνδεση στους χρήστες
iv. ικανοποιεί δυναμικά τις τρέχουσες ανάγκες των εφαρμογών σε εύρος ζώνης
v. διαθέτει ικανότητα αναβάθμισης, με μικρό πρόσθετο κόστος, στο πλαίσιο των τεχνολογικών εξελίξεων και ανάλογα τις απαιτήσεις και τις ανάγκες των χρηστών
vi. παρέχει στους χρήστες τη δυνατότητα επιλογής ανάμεσα σε πακέτα προσφορών σύνδεσης ανάλογα τις ανάγκες τους
vii. υπόκειται σε κανονιστικό πλαίσιο πολιτικών και στρατηγικών για την ενίσχυση της καινοτομίας και τη διατήρηση του ανταγωνισμού στην αγορά

Στα δίκτυα τέταρτης γενιάς 4G, επικράτησε η τεχνολογία LTE (Long Term Evolution), για την υλοποίηση της ασύρματης επικοινωνίας και δικτύωσης των κινητών συσκευών με υψηλές ταχύτητες. Η τεχνολογία αποτέλεσε φυσική μετεξέλιξη των ήδη υφιστάμενων δικτύων GSM και UMTS, ωστόσο μέσω νέων τεχνικών διαμόρφωσης κατάφερε να αυξήσει τη χωρητικότητα και την ταχύτητα του δικτύου.

Το LTE δύναται να λειτουργεί σε διάφορες συχνότητες. Ενδεικτικά στην Ευρώπη οι συχνότητες λειτουργίας είναι 800MHz, 1.8 και 2.6 GHz, στη Βόρεια Αμερική 700MHz και 1.7GHz, στην Ασία οι 1.8 και 2.6 GHz κ.τ.λ. Η πρόοδος που επέφερε η τεχνολογία LTE, οφείλεται στο γεγονός ότι εισήγαγε την πολυπλεξία διαίρεσης ορθογώνιων

συχνοτήτων OFDM (Orthogonal Frequency Division Multiplexing) και την χρήση πολλαπλών κεραιών στους πομποδέκτες MIMO (Multiple-Input Multiple-Output).

Ανάμεσα στα πλεονεκτήματα του LTE είναι ο διαχωρισμός των χρηστών ανά κυψέλη, στο πεδίο του χρόνου και της συχνότητας και η δυνατότητα επαναχρησιμοποίησης των πόρων σε γειτονικές κυψέλες (Rappaport, 2006).

1.3 Περιγραφή Αρχιτεκτονικών

Αναμφίβολα, ο συνδυασμός των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών διαμόρφωσε ένα πεδίο εξαιρετικά υψηλών προσδοκιών οι οποίες δρομολογήθηκαν να υλοποιηθούν από μέσω της τεχνολογία 5G. Προς αυτή την κατεύθυνση η Ευρωπαϊκή Ένωση, επικέντρωσε το ενδιαφέρον της στην δημιουργία κατάλληλων υποδομών οι οποίες να χαρακτηρίζονται από ευελιξία και επεκτασιμότητα. Τα δίκτυα 5G υπόσχονται να ενσωματώσουν τους τηλεπικοινωνιακούς, υπολογιστικούς και αποθηκευτικούς πόρους εντός μιας κοινής υποδομής ώστε να οι κατανεμημένοι πόροι να αξιοποιούνται με βέλτιστο τρόπο. Η Ευρωπαϊκή Επιτροπή έχει θέσει ως στόχο την εξασφάλιση μέχρι το 2025 της αδιάλειπτης κάλυψης των αστικών περιοχών με δίκτυα 5G. Τον Μάρτιο του 2021, ο ως άνω στόχος διευρύνθηκε καθώς αποφασίστηκε η επέκταση κάλυψης σε όλες τις κατοικημένες περιοχές με δίκτυα 5G μέχρι το τέλος του 2030 (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2022).

Για να γίνει αντιληπτή η αναγκαιότητα της παραπάνω στοχοθεσίας της ΕΕ παραθέτουμε τα ακόλουθα βασικά συγκριτικά χαρακτηριστικά της τεχνολογίας 5G, σε σχέση με τις προγενέστερες και συγκεκριμένα (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2022):

- ✓ Προσφέρει μακράν μεγαλύτερη χωρητικότητα δεδομένων και υψηλότερες ταχύτητες μετάδοσης.
- ✓ Οι ανάδοχοι δεν είναι πλέον αποκλειστικά πάροχοι τηλεπικοινωνιών αλλά πλήθος ετερόκλητων ενδιαφερομένων.
- ✓ Παρέχει υπερταχεία ευρυζωνικότητα και συνδεσιμότητα μικρού λανθάνοντα χρόνου σε μεμονωμένους χρήστες και συνδεδεμένες συσκευές.
- ✓ Το μέσο παροχής bits μετασχηματίζεται σε πλατφόρμα προηγμένων δυνατοτήτων

- ✓ Η τεχνολογία 5G δεν αφορά μόνο σε κινητά αλλά σε μία ποικιλία πραγμάτων/αντικειμένων IOT
- ✓ Κάθε διαδικασία που πραγματοποιείται αντιμετωπίζεται ως υπηρεσία.
- ✓ Οι υπηρεσίες 5G αναμένεται να υποστηρίξουν πλήθος καινοτόμων εφαρμογών οι οποίες θα βελτιώσουν τις υπηρεσίες σε πολλούς τομείς των σύγχρονων κοινωνιών (π.χ μεταφορές, ενέργεια, υγεία κ.α.).

Μέσω της διαδικασίας network virtualization, κατά την οποία συνενώνονται οι πόροι του δικτύου σε ένα εικονικό δίκτυο, δύνανται να δημιουργηθούν διαφορετικές εικονικές δικτυακές φέτες. Κάθε εικονική φέτα έχει την δυνατότητα να εκτελέσει μια συγκεκριμένη απαίτηση υπηρεσίας η οποία να απαιτεί ένα καθορισμένο βαθμό ασφάλειας. Στο πεδίο σχεδιασμού της ασφάλειας των δικτύων 5G, θα πρέπει να λαμβάνεται μέριμνα για την απομόνωση, την εγκατάσταση και τη διαχείριση των εικονικών φετών δικτύου καθώς και για την ετερογένεια των δικτύων που υφίσταται εξαιτίας των διαφόρων τεχνολογιών πρόσβασης π.χ WiFi, LTE.

Ανάμεσα στα πλεονεκτήματα του network virtualization είναι η παρεχόμενη δυνατότητα στους χρήστες, εξαιτίας της επεκτασιμότητάς του, να μεταβάλλουν τις δυνατότητές του ανάλογα με τις ανάγκες τους. Οι λειτουργίες των δικτύων 5G αποτελούν πρακτικά στιγμιότυπα λογισμικού, τα οποία υλοποιούνται σε κέντρα δεδομένων που είναι διαμορφωμένα με εικονικό τρόπο και στηρίζονται στη λογική του Cloud.

Εικόνα 1.6: Η Ευρώπη χαράσσει την πορεία προς το 5G

(Πηγή: https://ati.ec.europa.eu/news/europe-shaping-5g-vision)

Οι λεγόμενες φέτες του δικτύου (network slices) προσφέρουν διαφοροποιημένες υπηρεσίες εφαρμογών. Τα slices αποτελούν ένα εικονικό δίκτυο κατ'απαίτηση (on demand) με παραμέτρους που περιστασιακά μεταβάλλονται βάσει της εφαρμογής ή της υπηρεσίας που εξυπηρετεί.

Ωστόσο πρέπει να τονίσουμε ότι παρά τις προκλήσεις και τις ευκαιρίες ανάπτυξης που δημιουργεί το 5G, διατυπώνονται φόβοι σχετικά με κινδύνους για την ασφάλεια των δικτύων από επικείμενες επιθέσεις και απειλές. Είναι σαφές ότι προκειμένου να διασφαλίζεται η ασφάλεια, η συνολική υποδομή του δικτύου θα πρέπει να είναι ισχυρή. Στο πλαίσιο αυτό, απαιτείται συλλογική προσέγγιση και αυστηρή αξιολόγηση των πιθανών κινδύνων για την ασφάλεια, που σχετίζονται με την ανάπτυξη δικτύων επικοινωνιών 5G. Βάσει σχετικών συστάσεων και Οδηγιών, τα κράτη - μέλη της ΕΕ έχουν δρομολογήσει διαδικασίες επανεξέτασης και ενίσχυσης των μέτρων ασφαλείας για τα δίκτυα 5G (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2022).

Ειδικότερα οι συστάσεις της Ευρωπαϊκής Επιτροπής για τα 5G περιλαμβάνουν (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2022):

- Προώθηση ομοιόμορφης και έγκαιρης ανάπτυξης δικτύων 5G εντός της Ε.Ε.
- Από κοινού προώθηση εναρμονισμένων προσεγγίσεων και πολιτικών για την ασφάλεια των δικτύων 5G
- Έλεγχος και παρακολούθηση των εφαρμοζόμενων πρακτικών των κρατών μελών της ΕΕ σε ζητήματα ασφάλειας και αξιολόγηση των επιπτώσεων από τις αποκλίσεις στην αποτελεσματική λειτουργία της ενιαίας αγοράς.

Τα πιθανά ζητήματα ασφάλειας σχετικά με το 5G προκαλούν μεγάλη ανησυχία καθώς το 5G προσφέρει ένα ευρύτερο πεδίο επιθέσεων συγκριτικά με το δίκτυα 3G και 4G. Ενδεικτικό παράδειγμα για την ύπαρξη ζητήματος ασφάλειας στα δίκτυα πέμπτης γενιάς είναι η κοινή χρήση των υποδομών από πολλούς φορείς εικονικών δικτύων καθώς και το γεγονός ότι συχνά οι τηλεπικοινωνιακοί φορείς αναθέτουν σε εξωτερικούς συνεργάτες τα δεδομένα τους. Τα δίκτυα 5G αποτελούν πλατφόρμες ανοικτού δικτύου, με αποτέλεσμα να υφίσταται κίνδυνος διαρροής προσωπικών δεδομένων. Έτσι, προκειμένου να εξασφαλίζεται η μέγιστη δυνατή ασφάλεια θα πρέπει να είναι εφικτή η απομόνωση σε πολλαπλά επίπεδα.

Πιο συγκεκριμένα απαιτείται να μελετάτε στο στάδιο του σχεδιασμού η δυνατότητα απομόνωσης των κόμβων ελέγχου και προώθησης του δικτύου. Αυτό θα ήταν ιδιαίτερα χρήσιμο σε αρχιτεκτονικές δικτύων που στηρίζονται σε λογισμικό. Για παράδειγμα, σε ένα SDN οι δρομολογητές, οι διακόπτες και κάθε άλλη συσκευή του δικτύου έχει δύο επίπεδα. Το επίπεδο 1 αναφέρεται στο επίπεδο προώθησης στο οποίο η διαβίβαση των δεδομένων δύναται να ανακληθεί και λέγεται επίπεδο δεδομένων ή μεταφοράς. Το επίπεδο 2 αναφέρεται στο επίπεδο ελέγχου, το οποίο ορίζει τις πληροφορίες του δικτύου και λαμβάνει αποφάσεις για την κατεύθυνση της κυκλοφορίας. Σκοπός του SDN είναι η δυνατότητα απομόνωσης των δύο επιπέδων και η μετατροπή του στατικού δικτύου σε ένα έξυπνό, κεντρικά ελεγχόμενο δίκτυο.

Όπως προαναφέραμε, το LTE αποτελεί βασική τεχνολογία ανάπτυξης των ευρυζωνικών συστημάτων επόμενης γενιάς. Το 3GPP, όπως θα αναλυθεί σε επόμενη ενότητα, προωθεί τρόπους βελτιστοποίησης των ισχυόντων προτύπων ώστε το σύστημα LTE / EPC να συμβάλει στην επίτευξη αυτού του σκοπού.

Η αρχιτεκτονική του 5G αποτελεί βάση για τα συστήματα πολλαπλής πρόσβασης. Οι τεχνολογίες NFV και SDN, διαχωρίζουν τον έλεγχο του δικτύου από το χειρισμό των πακέτων δεδομένων επιτρέποντας στα δίκτυα 5G τη δυνατότητα αξιοποίησης των εν λόγω τεχνολογιών.

Η δημιουργία πυκνών και μικρών κυψελών καθώς και η αξιοποίηση τεχνολογιών όπως το MIMO, SDN, NFV και το MEC/caching, αποτελούν πολύτιμα εργαλεία για τη δυναμική ανάπτυξη και την κλιμάκωση των λειτουργιών του δικτύου 5G. Το μοντέλο αρχιτεκτονικής του 5G παρέχει ομοιόμορφες υπηρεσίες σε χρήστες ανεξαρτήτως του συστήματος πρόσβασης, σταθερού ή το ασύρματου δικτύου.

Τα 5G παρέχουν δυνατότητα επικοινωνίας ανάμεσα σε άνθρωπο με άνθρωπο, άνθρωπο και μηχανή και μηχανή με μηχανή M2M (Machine-2-Machine) (Eridy, 2015).

Η αρχιτεκτονική του 5G στηρίζεται στο πρωτόκολλο του διαδικτύου IP και περιλαμβάνει τους εξής κόμβους (Kumari et al., 2018):

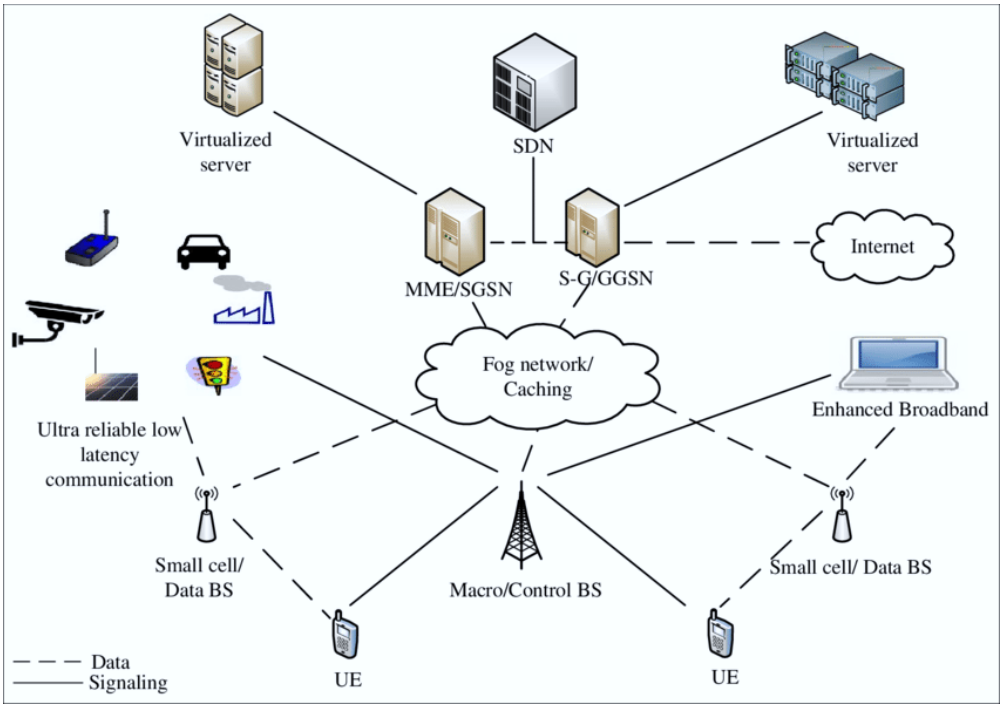
- Κόμβοι πρόσβασης (Access node): αποτελούν το σημείο έναρξης της σύνδεσης που καταλήγει στο χρήστη. Κάθε κόμβος περιλαμβάνει τον ενεργό εξοπλισμό μετάδοσης και αναλαμβάνει τη διευκόλυνση και τον τερματισμό της σύνδεσης.

- Κόμβοι νέφους (Cloud node): συμπεριφέρονται ως μέσο αποθήκευσης μεγάλου όγκου πληροφορίας.

- Κόμβοι δικτύου (Networking node): αναλαμβάνουν τη διαχείριση σύνδεσης μεταξύ των κόμβων πρόσβασης και νέφους καθώς και τη σύνδεση με το εξωτερικό δίκτυο.

Ο συνδυασμός της ετερογένειας του περιβάλλοντος με τα νέα πρότυπα δικτύωσης καθιστούν το 5G ευάλωτο σε απειλές ασφαλείας με αποτέλεσμα να απαιτείται η ανάπτυξη ενός νέου και αξιόπιστου μηχανισμού ασφαλείας. Η προστασία δεδομένων από άκρο σε άκρο (E2E) παρέχει αφενός μεγαλύτερο βαθμό ασφάλειας συνολικά και αφετέρου παρακάμπτει άσκοπές επαναλαμβανόμενες λειτουργίες ασφαλείας όπως είναι η κρυπτογράφηση και η αποκρυπτογράφηση. Παράλληλα προσφέρει τη δυνατότητα παροχής διαβαθμισμένης ασφάλειας με βάση τις υπηρεσίες (Kumari et al., 2018).

Μεταξύ των ζητημάτων ασφάλειας, το E2E ασχολείται με τον έλεγχο ταυτότητας, την ακεραιότητα, τη διαχείριση κλειδιών και την εμπιστευτικότητα. Όπως προαναφέραμε, τα συστήματα 5G παρέχουν μεγαλύτερη επιφάνεια για την εξαπόλυση επιθέσεων και ως εκ τούτου θα πρέπει να λαμβάνεται μέριμνα των τρόπων αποτροπής και αντιμετώπισης των επιθέσεων κατά τον καθορισμό νέων πρωτοκόλλων 5G (Kumari et al., 2018).



Εικόνα 1.7: A candidate architecture for 5G cellular network

(Πηγή: Parvez et al., 2018)

Η ως άνω αξιολόγηση θα πρέπει να πραγματοποιείται βάσει της πολυπλοκότητας υπολογισμού και επικοινωνίας, του βαθμού αντίστασης σε πιθανές επιθέσεις και του αμυντικού ρυθμού ασφάλειας (Kumari et al., 2018).

1.4 Αρχιτεκτονική συστήματος 3GPP 5G βασισμένη στην υπηρεσία

Στο πλαίσιο της εξέλιξης των τηλεπικοινωνιακών συστημάτων και της συμβολής τους στην ανάπτυξη εφαρμογών οι οποίες θα επηρεάσουν πολλούς τομείς και θα ενισχύσουν τις οικονομίες των κρατών μελών της ΕΕ, η αρχιτεκτονική του συστήματος 5G είναι στρατηγικής σημασίας για την ενιαία αγορά συγκριτικά με τεχνολογίες παλαιότερων γενιών καθώς είναι βασισμένη στην υπηρεσία. Ειδικότερα, τα στοιχεία αρχιτεκτονικής ορίζονται ως ξεχωριστές λειτουργίες δικτύου και συνδέονται με άλλες λειτουργίες δικτύου σε ένα κοινό πλαίσιο παρέχοντας μια καθορισμένη υπηρεσία.

Το NRF (Network repository functions) είναι μια από τις λειτουργίες του δικτύου 5G, όπου υποστηρίζει τη δυνατότητα εντοπισμού της υπηρεσίας η οποία λαμβάνει αιτήματα ανακάλυψης NF. Αποτελεί στοιχείο της αρχιτεκτονικής δικτύων πέμπτης γενιάς και διατηρεί ένα ενημερωμένο αποθετήριο του συνόλου των λειτουργιών δικτύου (NF). Με λίγα λόγια, το NRF υποστηρίζει τους μηχανισμούς ανακάλυψης υπηρεσίας καθώς παρέχει τη δυνατότητα στις λειτουργίες του δικτύου να ανακαλύπτουν υπηρεσίες άλλων λειτουργιών. Παράλληλα, επιτρέπει στις οντότητες NF να εγγραφούν λαμβάνοντας ειδοποιήσεις για την εγγραφή νέων παρουσιών NF στο δίκτυο NRF. Η λειτουργία ανακάλυψης υπηρεσίας έγκειται στη λήψη αιτημάτων ανακάλυψης NF από τα άλλα NF και στη παροχή πληροφοριών λειτουργίας για την υποστήριξη μιας καθορισμένης υπηρεσίας.

Τα στοιχεία αρχιτεκτονικής του 5G επιτρέπουν την αλληλεπίδραση των διάφορων λειτουργιών του δικτύου με αποτέλεσμα να εξασφαλίζεται η λειτουργικότητα στο επίπεδο του συστήματος και του δημοσίου δικτύου κινητής τηλεφωνίας (Public Land Mobile Network - PLMN) (ETSI, 2017).

Το PLMN αποτελεί προϊόν συνδυασμού του MCC και του MNC και έχει μοναδική αξία παγκοσμίως καθώς προσδιορίζει το δίκτυο κινητής τηλεφωνίας στο οποίο είναι εγγεγραμμένος κάθε χρήστης.

Στα συστήματα 5G κάθε λειτουργία του δικτύου αποθηκεύει το περιεχόμενο της στην λειτουργία αποθήκευσης δεδομένων (DSF). Αποτελεί ιδιαίτερα χρήσιμη λειτουργία για τη διαχείριση της κινητικότητας του χρήστη όταν απαιτείται μετάβαση από ένα δίκτυο πρόσβασης σε ένα άλλο, καθιστώντας ευκολότερη την αλλαγή κόμβου εξυπηρέτησης του χρήστη (ETSI, 2020).

1.5 Σύγκριση των 1G, 2G, 3G, 4G και 5G

Σε μια σύντομη χρονολογική επισκόπηση των δικτύων 1G, 2G, 3G, 4G μπορούμε να αναφέρουμε συνοπτικά τα εξής (Hussain et al., 2016):

- *Δίκτυο πρώτης γενιάς 1G:* Αναπτύχθηκε το 1981 και στηρίχτηκε στην αναλογική επικοινωνία. Η ταχύτητα και ο ρυθμός μετάδοσης των δεδομένων ήταν μικρής απόδοσης καθώς εξυπηρετούνταν μόνο μία κλήση ανά κανάλι. Επίσης, η ποιότητα φωνής ήταν κακή και υπήρχαν σοβαρά ζητήματα ασφάλειας καθώς τα δεδομένα δεν υπόκεινταν σε κρυπτογράφηση.

- *Δίκτυο δεύτερης γενιάς 2G:* Αναπτύχθηκε το 1991και βασίστηκε στην ψηφιακή επικοινωνία με διαφορετικά πρότυπα, ανάμεσα στα οποία το GSM, το CDMA, το PDC και άλλα. Το GSM ήταν το σπουδαιότερο και χρησιμοποιείται μέχρι και σήμερα. Το GSM λειτουργούσε σε ζώνη συχνοτήτων 900 MHz και 1800 MHz. Παράλληλα, σημαντική ήταν η ανάπτυξη της τεχνολογίας SIM, για τον έλεγχο της ταυτότητας του χρήστη για σκοπούς αναγνώρισης και χρέωσης, και η κρυπτογράφηση των δεδομένων (Temple, 2010).

- *Δίκτυο μεταξύ δεύτερης και τρίτης γενιάς 2.5G:* Αναπτύχθηκε το 2000 και τα βασικότερα χαρακτηριστικά του ήταν ότι στα δεδομένα προστέθηκε η φωνή και ότι εισήχθη η υπηρεσία GPRS (General Packet Radio Service). Μέσω αυτής, έγινε εφικτή η παροχή υπηρεσιών αποστολής και λήψης e-mail και εικονομηνυμάτων. Η ταχύτητα μετάδοσης δεδομένων έφτασε στα 115 kbps, η οποία με τη χρήση του EDGE (Enhanced Data Rates for Global Evolution) αυξήθηκε στα 384 Kbps (Temple, 2010).

- *Δίκτυο τρίτης γενιάς 3G:* Αναπτύχθηκε το 2003 χρησιμοποιώντας ζώνες υψηλότερης συχνότητας και CDMA για τη μετάδοση δεδομένων με ταχύτητες που φτάνουν τα 2

Mbps. Μέσω αυτών κατέστη εφικτή η δυνατότητα παροχής υπηρεσιών πολυμέσων όπως τα MMS. Παράλληλα, το Πρότυπο WCDMA (Wideband Code Division Multiple Access) συνέβαλε στην επίτευξη ταχυτήτων μεταξύ 384 και 2048Kbps. Στο δίκτυο 3G εξακολούθησε η χρήση ελέγχου ταυτότητας SIM για συστήματα χρέωσης και για κρυπτογράφηση δεδομένων.

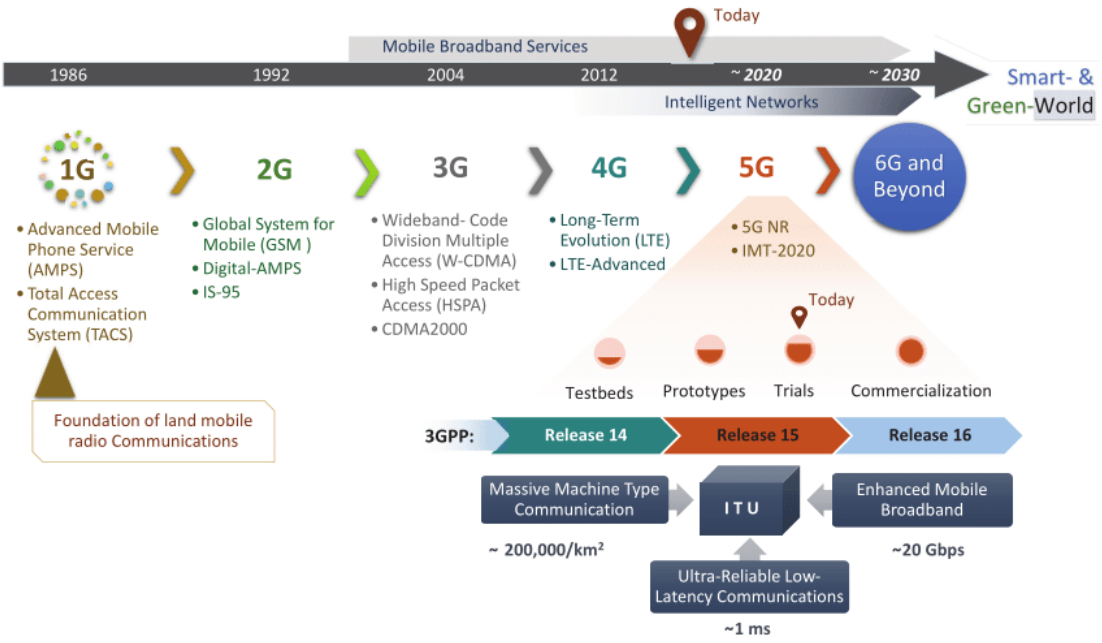
- *Δίκτυο τέταρτης γενιάς 4G:* Αναπτύχθηκε το 2007 με δυνατότητες παροχής ταχυτήτων μέχρι 150Mbps σε περιοχές διπλών συνδέσεων LTE και 300Mbps για συνδέσεις LTE-A. Επίσης ως μοντέλο δικτύωσης το 4G χρησιμοποιεί ευρέως τα ad hoc δίκτυα όπου δεν απαιτείται σταθερή υποδομή. Στα δίκτυα τέταρτης γενιάς η καθυστέρηση κυμαίνεται μεταξύ (40-60)ms. Ανάμεσα στα πρότυπα που χρησιμοποιεί είναι το LTE-A (LongTerm Evolution- Advance) και το Wimax.

- *Δίκτυο πέμπτης γενιάς 5G:* Αναπτύχθηκαν από το 2010 μέχρι το 2015 και ο ρυθμός μετάδοσης δεδομένων κυμαίνεται από (10-100)Gbps. Η παροχή ρεύματος σε απομακρυσμένες περιοχές καλύπτεται ενεργειακά από μεγάλα ηλιακά πάνελ. Το 5G μείωσε κατά πολύ την καθυστέρηση απόκρισης της συσκευής γεγονός που αποτελεί σημαντική παράμετρο για την επίτευξη εξελιγμένων υπηρεσιών όπως οι υψηλότεροι ρυθμοί δεδομένων και ο υψηλός χρόνος απόκρισης. Η υψηλή διαθεσιμότητα και αξιοπιστία αποτελούν χαρακτηριστικά του δικτύου πέμπτης γενιάς. Η υψηλή αξιοπιστία περιλαμβάνει τις υπηρεσίες συστήματος και την αρχιτεκτονική του υλικού και η διαθεσιμότητα περιλαμβάνει το εύρος ζώνης του καναλιού. Η κυκλοφορία στα συστήματα κυψελωτών επικοινωνιών είναι αυξανόμενη (Keenan, 2020).

- Προκειμένου για την διαχείριση της κυκλοφορίας απαιτείται το σύστημα να έχει πολύ μεγάλη χωρητικότητα. Τα δίκτυα 5ης γενιάς πρέπει να μεταφέρουν μεγάλο όγκο δεδομένων με χαμηλότερο κόστος και υψηλό ρυθμό μετάδοσης. Επίσης πρέπει να έχουν την ικανότητα να υποστηρίζουν ένα τεράστιο αριθμό συσκευών μέσω της αποτελεσματικής χρήσης των πρωτοκόλλων.

Βάσει των ανωτέρω, συνάγεται το συμπέρασμα ότι τα κυψελωτά δίκτυα έχουν συνεισφέρει ουσιαστικά στην αύξηση της χωρητικότητας του δικτύου και σε συνδυασμό με τις ευρυζωνικές υπηρεσίες παρέχουν μεγάλη ακτίνα κάλυψης (Holma, & Toskala, 2010; Chan, 2018; Munir, 2005).

Η εξέλιξη των δικτύων κινητής τηλεφωνίας επισφραγίστηκε με την ανάπτυξη των δικτύων 5G ενώ αξίζει να σημειωθεί ότι σε επίπεδο έρευνας η τεχνολογία βρίσκεται ήδη στο 6G. Στην Εικόνα 1.9 αποτυπώνεται χρονολογικά η εξέλιξη των δικτύων κινητής τηλεφωνίας από τα δίκτυα πρώτης γενιάς στο 5G.



Εικόνα 1.8: Εξέλιξη των δικτύων κινητής τηλεφωνίας στις αντίστοιχες γενιές

(Πηγή: Nawaz et al., 2019)

Η ανάγκη ανάπτυξης δικτύων 5G προέκυψε από το απαιτούμενο εύρος ζώνης και το γεγονός ότι οι αναδυόμενες εφαρμογές προϋποθέτουν υψηλότερες ταχύτητες με μικρότερες καθυστερήσεις. Επίσης, παρατηρείτε εκθετική αύξηση του αριθμού συσκευών IoT αυξάνοντας τον ζητούμενο αριθμό συνδέσεων σε πάνω από 29 δισεκατομμύρια έως το 2022. Καθώς τα δίκτυα 4G/LTE πλησιάζουν στον κόρο σε χωρητικότητα, η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) καθόρισε τις νέες προδιαγραφές απαιτήσεων στο δίκτυο 5G.

Τα δίκτυα 5G ξεκίνησαν στις αρχές του 2019 στην Νότια Κορέα με αφορμή τους χειμερινούς Ολυμπιακούς Αγώνες και από το 2020 εφαρμόζεται πιλοτικά σε διάφορες ευρωπαϊκές πόλεις (Moskowitz, 2019).

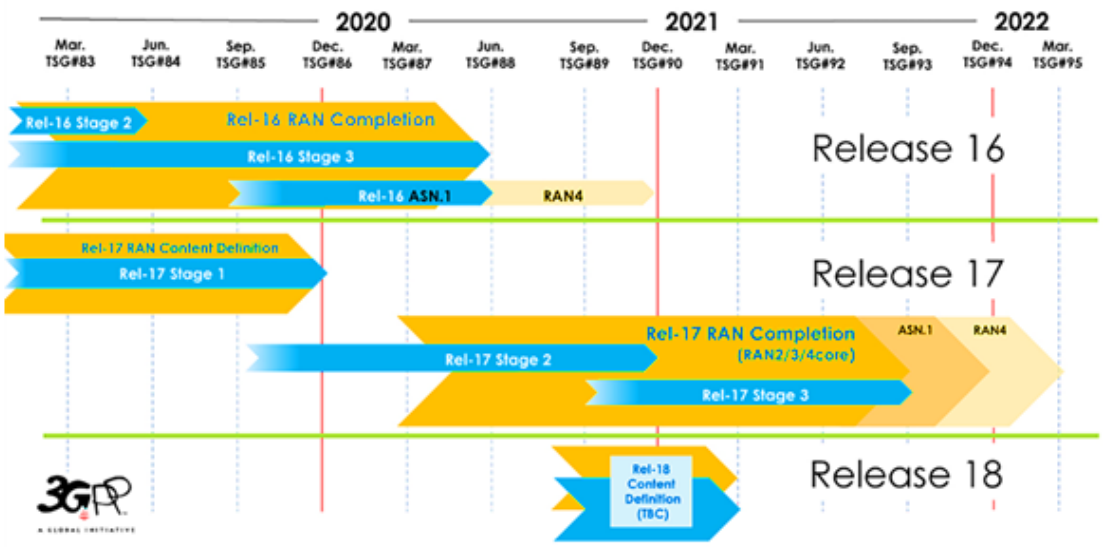
Οι προδιαγραφές της ITU για το 5G καθορίζονται στο ITU-R IMT-2020 (5G) τα βασικά σημεία του οποίου συνοψίζονται στην Εικόνα 1.10 και περιλαμβάνουν (Carugi, 2018):

i. Διαδρομές έως και 10Gbps δηλαδή μέχρι 100 φορές γρηγορότερα από τα δίκτυα 4G, στοχεύουν στην ικανοποίηση της αυξανόμενης απαίτησης για μεγάλο εύρος ζώνης
ii. Καθυστερήσεις της τάξης του 1 ms, έναντι 30 - 50 ms για 4G, θα επιτρέψουν την απόκριση σε σχεδόν πραγματικό χρόνο
iii. Πυκνότητα σύνδεσης κατά προσέγγιση 1.000 συσκευών ανά τετραγωνικό χιλιόμετρο, ήτοι 100 φορές περισσότερο από 4G, απαραίτητη για την τεχνολογία IoT.
iv. Διαθεσιμότητα δικτύου στο 99,999% του χρόνου.
v. Ασφάλεια δικτύου που προστατεύει την ιδιωτικότητα και τα προσωπικά δεδομένα των χρηστών.

Η ITU εισηγήθηκε τον καθορισμό των τεχνικών προδιαγραφών του 5G στον παγκόσμιο οργανισμό τυποποίησης 3GPP - 3rd Generation Partnership Project ο οποίος αποτέλεσε προϊόν συνεργασίας ανεξάρτητων επιτροπών τυποποίησης παγκοσμίου βεληνεκούς. Ο εν λόγω Οργανισμός έχει αρμοδιότητα και την ευθύνη για τον ορισμό των τεχνικών προδιαγραφών των προτύπων ασύρματης επικοινωνίας. Οι προδιαγραφές 5G έχουν ενσωματωθεί στις εκδόσεις 3GPP 15 και 16.

Το 3GPP Release 17 αποτελεί την τρίτη δόση του παγκόσμιου προτύπου 5G. Η έκδοση 17 ολοκληρώθηκε εν μέσω της πανδημίας του COVID 19. Το 3GPP έχει λειτουργεί σε επίπεδο τηλεδιασκέψεων από τον Ιανουαρίου του 2020 χωρίς ωστόσο να μπορούν να υλοποιηθούν δια ζώσης συναντήσεις για αλληλεπιδράσεις. Η ολοκλήρωση της κυκλοφορίας του 3GPP 17 ανάβει το πράσινο φως στην πρώτη φάση της εξέλιξης του 5G και προμηνύει την περεταίρω επικράτηση και επέκτασή του σε νέες συσκευές, εφαρμογές και υπηρεσίες.

Αξίζει να σημειωθεί ότι περάτωση των εν λόγω προδιαγραφών διασφάλισε την αξιοπιστία της τεχνολογίας 5G με αποτέλεσμα την ανάπτυξη εμπιστοσύνης από πλευράς των κατασκευαστών για την υλοποίηση δράσεων και επενδύσεων σε δίκτυα 5ης γενιάς.



Εικόνα 1.9: Πρόγραμμα 3GPP 16 και 17

(Πηγή: https://5g.security/5g-edge-miot-technology/5g-3gpp-releases-15-16-17/)

Η πλήρης ανάπτυξη των δυνατοτήτων 5G όπως ορίζονται στο IMT-2020G προϋποθέτει την υλοποίηση νέων δικτύων και την επένδυση μεγάλων κεφαλαίων για την πλήρη ανάπτυξη και επικράτησή τους. Στο πλαίσιο αυτό καθορίστηκε η έκδοση 15 5G NR Non-Stand Alone (NSA).

Το 5G NSA επιτρέπει την παροχή υπηρεσιών 5G αξιοποιώντας την υπάρχουσα υποδομή LTE. Η απόδοση των υφιστάμενων μακροκυψελών δύναται να μεγαλώσει με την προσθήκη επιπλέον επιπέδων MIMO. Επίσης υπάρχει η δυνατότητα χρησιμοποίησης από τους χειριστές του φάσματος των 3,5GHz για παροχή υπηρεσιών που απαιτούν υψηλότερες ταχύτητες.

Η έκδοση 15 περιλαμβάνει επίσης τις προδιαγραφές για την τεχνολογία 5G NR Stand-Alone (SA). Η 16η έκδοση ολοκληρώθηκε στις αρχές του ΄20 και περιλαμβάνει τις προδιαγραφές της τεχνολογίας σημάτων MMW, σύμφωνα με τις σχετικές αποφάσεις κατανομής φάσματος.

Όπως προαναφέραμε, η ραγδαία αύξηση του αριθμού των χρηστών επέφερε αναπόφευκτα περισσότερες διακοπές στη ζώνη συχνοτήτων του 4G με αποτέλεσμα η μετάβαση στο 5G να είναι απαραίτητη καθώς χρησιμοποιεί ζώνη συχνοτήτων των 5GHz. Με τον τρόπο αυτό παρατηρείται μείωση των παρεμβολών και καλύτερη διαχείριση της

κυκλοφορίας καθώς ο συνωστισμός από την χρήση εφαρμογών οι οποίες προϋποθέτουν μεγαλύτερη χωρητικότητα γίνεται με αποτελεσματικότερο τρόπο.

Οι στοιχειώδεις διαφορές ανάμεσα στο 5G και το 4G περιγράφονται παρακάτω (Sivalingam, 2019):

- Υψηλότερες ταχύτητες

Είναι ταχύτερο και έχει πιο μεγάλο εύρος από το ασύρματο 4G. Με το 5G θα γίνεται πιο γρήγορα η λήψη των βίντεο, δεδομένου ότι θα υπάρχουν λιγότερες λεγόμενες νεκρές ζώνες. Ακόμα, η πλήρης ταχύτητα και τα πλεονεκτήματα του 5G απαιτούν δρομολογητή οικιακού δικτύου, ο οποίος να υποστηρίζει το 5G.

- Αλλαγή συχνοτήτων

Λειτουργώντας το 5G, στη ζώνη των 5GHz, η ζώνη των 2,4GHz του 4G παρουσιάζει συνωστισμό, αφού χρησιμοποιείται από μια πληθώρα συσκευών σε κάθε σπίτι ή στις επιχειρήσεις.

- Μείωση των παρεμβολών

Το 5G θα δεν επηρεάζεται από παρεμβολές. Η ζώνη των 5GHz παρέχει περισσότερο χώρο για τη μετάδοση των δεδομένων. Αυτό έχει ως συνέπεια τη χρήση υψηλότερης ποιότητας, εξαλείφοντας τις προβληματικές συνδέσεις. Επιπλέον, το 5G εξαλείφει τα λεγόμενα νεκρά σημεία, με αποτέλεσμα να χρησιμοποιείται το τηλέφωνο σε περιοχές του δικτύου, εκεί όπου τώρα είναι αδύνατο να χρησιμοποιηθεί έως τώρα με το 4G.

- Υψηλότερο κόστος

Το κόστος της υποδομής στην Νότια Κορέα κυμάνθηκε περίπου στα 1,5 δισεκατομμύρια δολάρια. Επομένως, το ποσό δεν είναι μικρό και για τις υπόλοιπες χώρες, ανάλογα φυσικά και με το μέγεθός τους, την πληθυσμιακή κάλυψη και τις απαιτήσεις των χρηστών. Είναι φανερό, λοιπόν, ότι δεν είναι εύκολο να αντληθούν και να δαπανηθούν, ειδικά αυτήν την περίοδο, που η οικονομική κρίση και λόγω της πανδημίας μαστίζει όλον τον πλανήτη.

- Απρόσκοπτες τηλεδιασκέψεις χωρίς κωλύματα

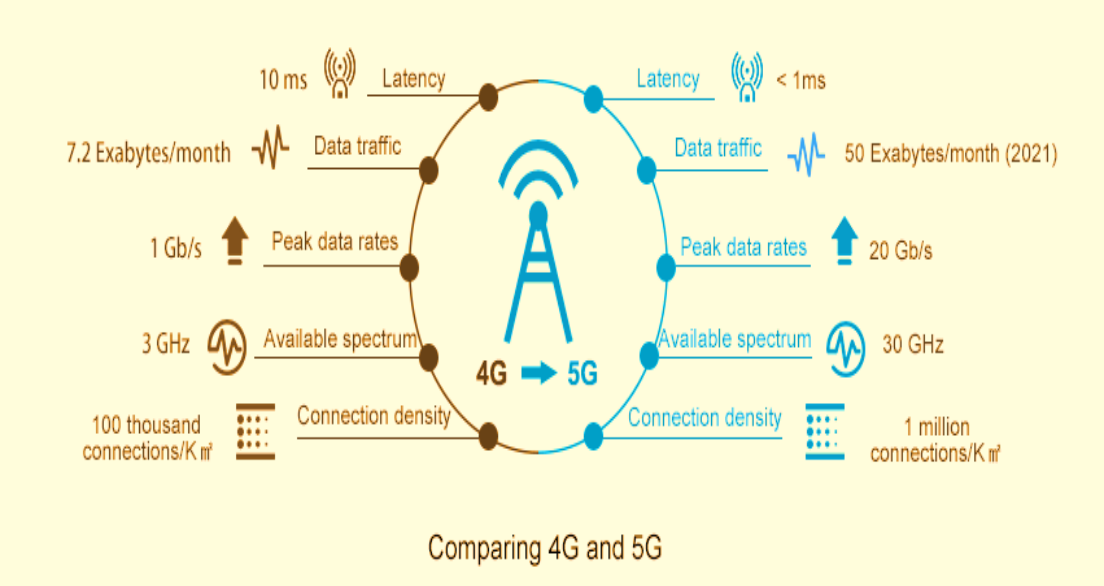
Είναι γνωστό ότι η ροή του βίντεο έχει απαίτηση για μεγάλο εύρος ζώνης συχνοτήτων. Γι' αυτό, η παρακολούθηση βίντεο στα ασύρματα δίκτυα προκαλεί αρκετά προβλήματα.

Το πάγωμα της εικόνας είναι σύνηθες λόγω του ότι το ασύρματο δίκτυο δεν δύναται να μεταδίδει με απόλυτη ακρίβεια τα δεδομένα εικόνας και ήχου. Ωστόσο, το 5G μειώνει τις προβληματικές εικόνες κατά την αποθήκευση βίντεο στην προσωρινή μνήμη buffer.

- Αμεσότερη χρονικά δημιουργία αντιγράφου ασφαλείας

Η δημιουργία αντιγράφων ασφαλείας κινητών συσκευών γίνεται εξαιρετικά γρήγορα. Με άλλα λόγια είναι ζήτημα δευτερολέπτων.

Τέλος, η τεχνολογία 5G θεωρείται πράσινη τεχνολογία και φιλική στο περιβάλλον.



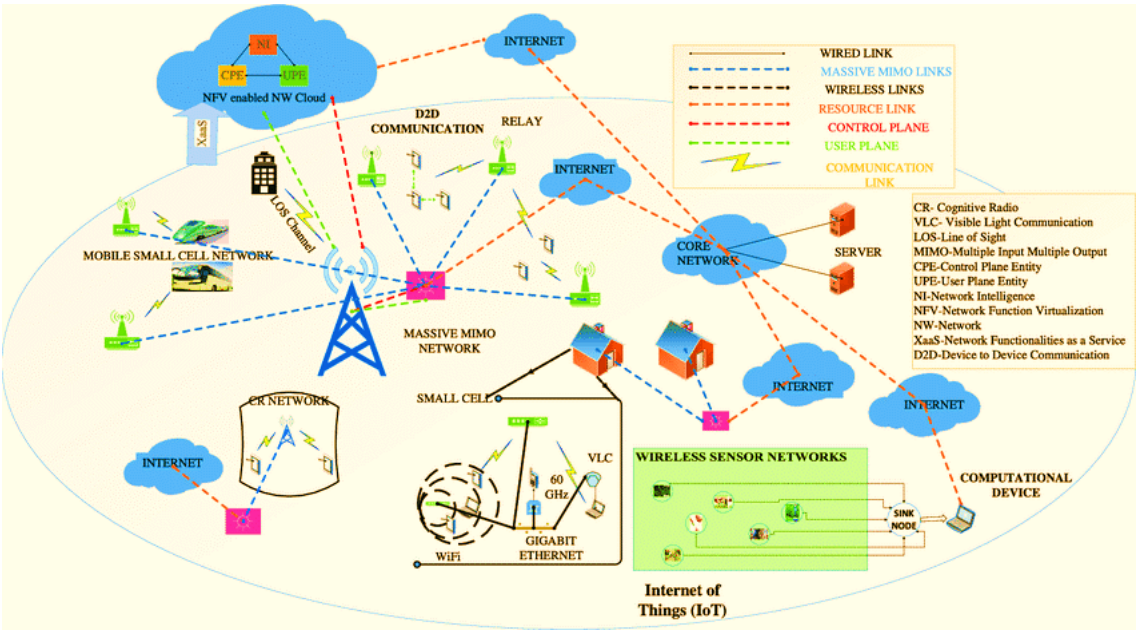
Εικόνα 1.10: Σύγκριση 4G και 5G

(Πηγή: Sivalingam, 2019)

ΚΕΦΑΛΑΙΟ 2ο: Τεχνικές μετάδοσης στα συστήματα 5G

2.1 Αρχιτεκτονική συστήματος 3GPP 5G

Όπως αναφέραμε στο προηγούμενο κεφάλαιο η αρχιτεκτονική του συστήματος 3GPP 5G σε αντίθεση με τις προγενέστερες τεχνολογίες είναι βασισμένη στην υπηρεσία. Αυτό σημαίνει ότι τα στοιχεία αρχιτεκτονικής δύνανται να θεωρούνται ως αυτόνομες λειτουργίες του δικτύου οι οποίες μπορούν να συνδυάζονται και συνδέονται με άλλες λειτουργίες εντός ενός κοινού πλαισίου παρέχοντας μια καθορισμένη υπηρεσία (Gupta & Jha, 2015).



Εικόνα 2.1: Αρχιτεκτονική και Αναδυόμενες Τεχνολογίες 5G

(Πηγή: Gupta & Jha, 2015)

Οι πολλαπλές και ποικίλες απαιτήσεις των χρηστών και η δυνατότητα πολλαπλής πρόσβασης στο δίκτυο απαιτούν την ανάπτυξη μιας εφαρμογής στο βασικό-κεντρικό δίκτυο η οποία θα να εξυπηρετεί τα ανωτέρω. Στο πλαίσιο ανάπτυξης του δικτύου 5G η τεχνολογία MIMO εφαρμόζει την τοποθέτηση διάσπαρτων τοπολογικά σειρών από κεραίες όπου η καθεμία περιλαμβάνει δεκάδες ή εκατοντάδες μονάδες κεραιών. Η αρχιτεκτονική δικτύου βάσει του cloud RAN (C-RAN) και του λογισμικού καθορισμένης

δικτύωσης SDN δημιουργεί ένα πεδίο ανάπτυξης πλήθους υπηρεσιών όπως είναι η διαχείριση δικτύου και η παρακολούθηση των επιδόσεων (Zheng et al., 2015). Πιο συγκεκριμένα ο SDN ελεγκτής νέφους μετατρέπει τεχνικές του cloud παρέχοντας υπηρεσίες κεντρικού ελέγχου. Επίσης το δίκτυο μεταφοράς με βάση το SDN διαχειρίζεται δυναμικά και ευέλικτα τα δίκτυα backhaul προσαρμόζοντας κατάλληλα το εύρος ζώνης μεταφοράς για κάθε σύνδεση RAN στο βασικό δίκτυο Core Network και την επιλογή βέλτιστης διαδρομής.

2.2 Δίκτυο πυρήνα (Core Network)

Το βασικό δίκτυο (core network) βάσει του SDN αποτελείται από μια ενιαία μονάδα ελέγχου (UCE) και μια ενοποιημένη πύλη δεδομένων (UDW). Η μονάδα ελέγχου (UCE) εκτελεί ενιαίο έλεγχο που περιλαμβάνει τη διαχείριση της κινητής μονάδας MME, το επίπεδο ελέγχου της υπηρεσίας εισόδου (SGW-C) και το επίπεδο ελέγχου του πακέτου δεδομένων της πύλης εισόδου (PGW-C). Η ενιαία μονάδα ελέγχου (UCE) μαζί με τον ελεγκτή SDN διαχειρίζονται το πρωτόκολλο GPRS σε επίπεδο χρήστη GTP-U. Παράλληλα η ενοποιημένη πύλη δεδομένων (UDW) πραγματοποιεί τη λειτουργική προώθηση δεδομένων η οποία ενσωματώνει το επίπεδο υπηρεσιών δεδομένων εισόδου SGW-D και το επίπεδο δεδομένων. (Zheng et al., 2015).

Στην αρχιτεκτονική του 5G χρησιμοποιείται η τεχνική νέφους από τον διακομιστή εφαρμογών, τον ελεγκτή, το RAN και το δίκτυο πυρήνα. Η λειτουργία άμεσης ανταπόκρισης του SDN στις συσκευές του δικτύου οι οποίες διαρκώς μεταβάλλονται καθώς και στις μεταβαλλόμενες απαιτήσεις των χρηστών και των επιχειρήσεων προσφέρει βασικό πλεονέκτημα στα δίκτυα πέμπτης γενιάς.

Καθώς η αρχιτεκτονική του SDN περιλαμβάνει (Zheng et al., 2015):

-το επίπεδο εφαρμογής

-το επίπεδο ελέγχου

- το επίπεδο υποδομής.

Η διεπαφή μεταξύ των επιπέδων εφαρμογής και ελέγχου αφορά σε διεπαφές προγραμματισμού API ενώ αντιστοίχως υπάρχει και διεπαφή μεταξύ των επιπέδων ελέγχου και υποδομής. Μέσω της νέας διεπαφής πρόσβασης δικτύου – πυρήνα δικτύου

προσφέρεται η δυνατότητα στο core network να μπορεί να λειτουργεί με διαφορετικά δίκτυα πρόσβασης, όπως το ασύρματο δίκτυο πρόσβασης (NG-RAN) και τα WLAN.

Η αρχιτεκτονική του συστήματος 5G εξασφαλίζει την ομαλή κινητικότητα προσβάσεων δικτύων 3GPP και άλλων. Η διαδικασία ελέγχου της ταυτότητας του χρήστη σε συνθήκες διαφορετικών σεναρίων χρήσης εξασφαλίζεται από την λειτουργία πιστοποίησης βάσει ενός ενιαίου πλαισίου πιστοποίησης.

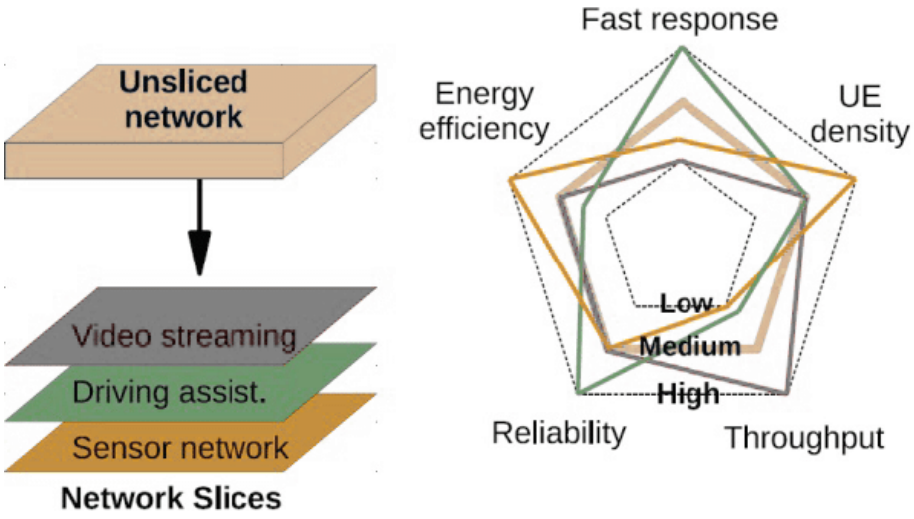
Ωστόσο θα πρέπει να αναφέρουμε, ότι εξαιτίας των ιδιαιτεροτήτων που παρουσιάζουν τα κυψελωτά δίκτυα, ενδέχεται κατά την υλοποίηση των τεχνικών Cloud και SDN να ανακύψουν ζητήματα τεχνικής φύσεως. Για τον λόγο αυτό οι σχεδιαστές δικτύων θα πρέπει να λαμβάνουν μέριμνα για κάθε πιθανό σενάριο που θα προκαλούσε δυσλειτουργία στο δίκτυο (Zheng et al., 2015; Erunkulu et al., 2021).

2.3 Η έννοια του κατακερματισμού (slicing) του Δικτύου 5G

Με τον όρο 5G Network Slicing εννοούμε εν γένει την αρχιτεκτονική του δικτύου που επιτρέπει την πολυπλεξία εικονικοποιημένων και ανεξάρτητων δικτύων στην ίδια φυσική δικτυακή τοπολογία. Τα τελευταία χρόνια, ο διαχωρισμός δικτύου αποτελεί βασικό εργαλείο του 5G προκειμένου να προσδιοριστούν αποτελεσματικότερα οι υπηρεσίες του δικτύου σύμφωνα ανάλογα με τις ποικίλες απαιτήσεις ποιότητας και λειτουργικότητας κοινόχρηστων πόρων. Οι φέτες του δικτύου (network slices) είναι πολλαπλά δίκτυα τα οποία έχουν δική τους διαχείριση, απαιτήσεις και χαρακτηριστικά, τοποθετημένα στο ίδιο φυσικό δίκτυο. Με τον τρόπο αυτό δημιουργούνται πολλαπλά ανεξάρτητα δίκτυα από άκρο σε άκρο του δικτύου 5G χρησιμοποιώντας παράλληλο τεμαχισμό δικτύου (Kumar & Anwar, 2022).

Όπως προαναφέραμε η βελτιωμένη ευρυζωνική κινητή τηλεφωνία (eMBB), παρέχει εξαιρετικά αξιόπιστη επικοινωνία με ιδιαίτερα χαμηλή καθυστέρηση (uRLLC). Οι υπηρεσίες mMTC στο 5G χαρακτηρίζονται από ένα πλήθος συσκευών οι οποίες μεταδίδουν δεδομένα χαμηλού όγκου τα οποία δεν είναι ευαίσθητα σε καθυστερήσεις. Το γεγονός αυτό προϋποθέτει την ύπαρξη πολλών υπολογιστικών πόρων με χαμηλό ρυθμό συμφόρησης. Στην περίπτωση τέτοιων υπηρεσιών, το NS απαιτεί μεγιστοποίηση του υπολειπόμενου εύρους ζώνης των φυσικών συνδέσεων. Οι υπηρεσίες uRLLC παρουσιάζουν υψηλό βαθμό απόδοσης και διαθεσιμότητας και ταυτόχρονα ιδιαίτερα

χαμηλό λανθάνοντα χρόνο. Ως εκ τούτου καθίσταται εφικτός ο στόχος ελαχιστοποίησης της καθυστέρησης NS που μεταφράζεται σε ελαχιστοποίηση κάθε μήκους φυσικής διαδρομής (Kumar & Anwar, 2022).



Εικόνα 2.2: Απεικόνιση τεμαχισμού του φυσικού δικτύου βασισμένο σε υπηρεσίες

(Πηγή: Kumar & Anwar, 2022)

Ο κατακερματισμός δικτύου ως βασικό χαρακτηριστικό των δικτύων πέμπτης γενιάς προσδίδει προβάδισμα συγκριτικά με τις προηγούμενες τεχνολογίες καθώς περιλαμβάνει ολόκληρο το δημόσιο κινητό δίκτυο (PLMN). Όπως αναφέραμε, κάθε τεμάχιο δικτύου (φέτα), έχει τα πλήρη χαρακτηριστικά για την υλοποίηση μιας καθορισμένης υπηρεσίας του δικτύου. Πρακτικά, το σύνολο των χαρακτηριστικών και των λειτουργιών που ορίζονται από το 3GPP και περιλαμβάνονται σε κάθε φέτα δικτύου, δημιουργούν ένα δημόσιο κινητό δίκτυο (PLMN), παρέχοντας υπηρεσίες σε συσκευές χρηστών (UE) βάσει των χρήσεων για τις οποίες προορίζονται. Μέσω του κατακερματισμού δικτύου κάθε φορέας εκμετάλλευσης δικτύου έχει την δυνατότητα να δημιουργήσει μία σειρά ανεξάρτητων δημόσιων κινητών δικτύων (PLMN) όπου καθένα από αυτά είναι προσαρμοσμένο να ικανοποιεί ένα υποσύνολο εξυπηρετούμενων χρηστών (Erunkulu et al., 2021).

Η καινοτομία που εισάγει ο κατακερματισμός δικτύου έγκειται στο γεγονός ότι ο χειριστής μπορεί να διαχειριστεί τμήματα του δικτύου ώστε να εξυπηρετήσει ποικίλες ανάγκες των πελατών. Στο πλαίσιο αυτό, η βέλτιστη διαχείριση των πόρων και των τοπολογιών του δικτύου επιτρέπει την ικανοποίηση καθορισμένων απαιτήσεων συνδεσιμότητας, ταχύτητας κοκ για κάθε εφαρμογή. Ταυτόχρονα ο χειριστής δύναται να ανταποκρίνεται με αμεσότητα και ταχύτητα στις ανάγκες των πελατών (Erunkulu et al., 2021).

Στο σημείο αυτό οφείλουμε να σημειώσουμε ότι παρά τα πλεονεκτήματα που προσφέρει ο τεμαχισμός δικτύου υπάρχει πάντα το ενδεχόμενο η κίνηση σε ένα κομμάτι να επηρεάσει την κίνηση κάποιου άλλου. Για την αποτροπή αυτού του ενδεχόμενου, οι ερευνητές προτείνουν ένα μοντέλο τεμαχισμού και κατανομής το οποίο να βασίζεται στα δεδομένα, ώστε να παρέχει υπηρεσίες υψηλής ποιότητας (QoS) και αποτελεσματική διαχείριση της κυκλοφορίας. Τέλος με τον τρόπο αυτό οι πόροι θα εκχωρούνται έξυπνα και θα ανακατανέμονται μεταξύ τμημάτων δικτύου ανάλογα με τις τρέχουσες διακυμάνσεις των απαιτήσεων των χρηστών (Kumar & Anwar, 2022).

2.4 Υπηρεσίες δεδομένων στην Αρχιτεκτονική 5G

Στην αρχιτεκτονική του 5G οι υπηρεσίες δεδομένων υποστηρίζουν εφαρμογές με μεγαλύτερη ευελιξία προσαρμογής σε σχέση με τις προηγούμενες γενιές. Το νέο μοντέλο έχει σχεδιαστεί ώστε να υποστηρίζει διαφορετικά δίκτυα πρόσβασης ενώ παράλληλα υπάρχει σήμανση πακέτων η οποία καθορίζει την ποιότητας της υπηρεσίας (QoS) που απαιτείται.

Πιο συγκεκριμένα η σήμανση των πακέτων γνωστοποιεί στην εφαρμογή το απαιτούμενο QoS γεγονός το οποίο καθιστά το σύστημα ευέλικτο και εν τέλει αποτελεσματικό. Η συμμετρική διαφοροποίηση του QoS της άνω και κάτω ζεύξης, προϋποθέτει ελάχιστη σηματοδότηση ελέγχου του Reflective QoS (Kumar & Anwar, 2022).

Η ευέλικτη ανάπτυξη λειτουργιών εφαρμογής στην τοπολογία του δικτύου, σύμφωνα με τις υψηλές απαιτήσεις του 5G, υποστηρίζεται, μέσω τριών διαφορετικών τρόπων συνόδου και υπηρεσίας συνέχειας (Session and Service Continuity-SSC) ή μέσω ταξινομητών uplink και σημείων διακλάδωσης. Συγκεκριμένα, οι λειτουργίες υπηρεσίας συνέχειας SSC περιλαμβάνουν την πιο παραδοσιακή λειτουργία (SSC 1), όπου η άγκυρα

IP παραμένει σταθερή για να παρέχει συνεχή υποστήριξη εφαρμογών και συντήρηση της διαδρομής με τον χρήστη καθώς ενημερώνεται η θέση της.

Επίσης, υπάρχουν δύο επιλογές, make-before-break (λειτουργία SSC 3) όπου δεν χάνεται η σύνδεση και έτσι δεν χάνεται η συνέχεια της υπηρεσίας και break-before-make (SSC 2) όπου η σύνδεση χάνεται και επιλέγεται μία καινούρια. Η αρχιτεκτονική συμβάλλει στην κατάλληλη για την ορθή επιλογή της υπηρεσίας των δεδομένων και για τη λειτουργία SSC (Mademann, 2018).

Τέλος, καθώς οι εφαρμογές του δικτύου 5G αναμένεται να εξυπηρετήσουν τεράστιες ποσότητες κίνησης δεδομένων είναι απαραίτητη η αποτελεσματική διαχείριση της διαδρομής του χρήστη. Ακόμη, οι λειτουργίες της κάθε εφαρμογής συντονίζονται με το δίκτυο. Ο σκοπός τους είναι η παροχή πληροφοριών, ώστε να βελτιστοποιούνται οι διαδρομές (paths) της κυκλοφορίας (ETSI, 2019).

2.5 Εφαρμοζόμενα πρότυπα

- 3GPP

Τα συστήματα 3G βασίστηκαν σε μια νέα ευρεία ζώνη η οποία επιτρέπει την πολυλειτουργικότητα και την ευέλικτη ραδιοπρόσβαση. Αυτή η προσέγγιση εξασφαλίζει ότι τα συστήματα που βασίζονται σε προδιαγραφές 3GPP θα προωθούν την ταχεία ανάπτυξη και την ανάπτυξη ανταγωνιστικών προσφορών σε επίπεδο υπηρεσιών επιτρέποντας την παγκόσμια περιαγωγή. Το TSG Radio Access Network (TSG RAN) είναι υπεύθυνο για τον καθορισμό των λειτουργιών, των απαιτήσεων και των διεπαφών του δικτύου UTRA/E-UTRA στους δύο τρόπους λειτουργίας του, ήτοι του FDD και TDD (3GPP, χ.η.).

Το 3ο Πρόγραμμα Σύμπραξης 3ης γενιάς (3GPP) αποτέλεσε προϊόν σύμπραξης διάφορων οργανισμών τυποποίησης των τηλεπικοινωνιών όπως των: ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC κ.α. Μέσω αυτού, αναπτύχθηκε ένα σταθερό πλαίσιο καθορισμένων προδιαγραφών τεχνολογίας 3GPP. Τα εν λόγω πρότυπα οδήγησαν στην επικράτηση του LTE ως μιας ταχέως αναπτυσσόμενης τεχνολογίας. Η 3GPP τυποποίησε το 5G με τη ονομασία New Radio-NR και εισήγαγε τον όρο δίκτυο πυρήνα (Core Network). Παράλληλα ενέκρινε το πρότυπο για το μη αυτόνομο 5G (Non Standalone-

NSA) το οποίο χρησιμοποιεί την υπάρχουσα υποδομή του 4G LTE ως μέσο σύνδεσης με το 5G.

Το TSG RAN, αποτελεί ομάδα εργασίας για τον καθορισμό των λειτουργιών, των απαιτήσεων και των εξελίξεων εν γένει της ασύρματης πρόσβασης.

Οι Ομάδες Τεχνικών Προδιαγραφών (TSG) RAN και TSG SA έχουν προχωρήσει προς τον στόχο της δορυφορικής συμπερίληψης στις τεχνικές προδιαγραφές 3GPP μέσω του Rel-17 NTN. Η ομάδα τεχνικών προδιαγραφών TSG-SA συντονίζει την γενικότερη αρχιτεκτονική, μελετά τις δυνατότητες εξυπηρέτησης των συστημάτων που στηρίζονται στις προδιαγραφές 3GPP και συντονίζει όλες τις τεχνικές ομάδες σε παγκόσμιο επίπεδο.

Η Ομάδα Τεχνικών προδιαγραφών του 3GPP για θέματα υπηρεσιών και συστήματος είναι η SA, η οποία απαρτίζεται από υποομάδες καθεμία από τις οποίες εργάζεται σε διαφορετικά αντικείμενα ως ακολούθως:

- ✓ SA1: Υπηρεσίες
- ✓ SA2: Αρχιτεκτονική
- ✓ SA3: Ασφάλεια
- ✓ SA4: Κωδικοποιητής
- ✓ SA5: Διαχείριση Τηλεπικοινωνιών
- ✓ SA6: κρίσιμες Εφαρμογές αποστολής

Πιο συγκεκριμένα η:

- SA1 έθεσε τις προδιαγραφές και τις απαιτήσεις υπηρεσίας του 5G.

- SA2 ολοκλήρωσε τη μελέτη για το δίκτυο πυρήνα επόμενης γενιάς (NGCore) καθορίζοντας τις προδιαγραφές για την αρχιτεκτονική και τις διαδικασίες του συστήματος 5G. Το κεντρικό δίκτυο διαθέτει υπηρεσίες διαμοιρασμού και απομόνωσης διαφόρων λειτουργιών του δικτύου. Παράλληλα υποστηρίζει υπηρεσίες διαχείρισης της κινητικότητας και της ποιότητας QoS.

- SA3 διεξήγαγε μελέτες σε ζητήματα ασφάλειας.

-SA5 πραγματοποιεί διαδικασίες ελέγχου του δικτύου για αποτελεσματικότερη διαχείριση των υποδομών.

- IETF (Internet Engineering Task Force)

Αντικείμενο του IETF είναι ο σχεδιασμός προτύπων υψηλής αξιοπιστίας του Internet, κυρίως TCP/IP. Τα παραγόμενα πρότυπα καθορίζουν το πλαίσιο λειτουργίας και διαχείρισης του διαδικτύου (Alvestrand, 2004). Στο πλαίσιο της ανάπτυξης της τεχνολογίας του 5G, η 3GPP υιοθέτησε πλήθος πρωτοκόλλων της IETF γεγονός που επικύρωσε την αγαστή συνεργασία τους σε ζητήματα τεχνικής φύσεως (Hoffman, χ.η.).

Η πέμπτη γενιά αρχιτεκτονικής του 3GPP προωθεί την επικράτηση ενός κοινού και ενιαίου συστήματος πρωτοκόλλου του διαδικτύου (all over Internet Protocol-All IP).

Οι ομάδες εργασίας που σχετίζονται με τον IETF και την ανάπτυξη του 5G εργάζονται στα παρακάτω αντικείμενα (Hoffman, χ.η.):

- Δρομολόγηση. Στο επίπεδο αυτό αναπτύσσονται πρωτόκολλα δρομολόγησης και τεχνολογιών που αφορούν σε δίκτυα μεταφορών, κέντρα δεδομένων και εικονικά δίκτυα.

- Διαδίκτυο. Το πρωτόκολλο του διαδικτύου εκτελεί λειτουργίες οι οποίες συνδέονται με την προτυποποίηση του 5G. Μέσω του IPv6 προσφέρεται πλήθος IP και δυνατότητα πολλαπλής πρόσβασης στους χρήστες για τη σύνδεση πολλών συσκευών.

- Εφαρμογές real time (σε πραγματικό χρόνο). Πρόκειται για εφαρμογές φωνής και πολυμέσων οι οποίες με την επικράτηση του 5G αναμένεται να εξελιχθούν μέσω του IoT.

- Επίπεδο Μεταφοράς. Το πρωτόκολλο μεταφοράς εξυπηρετεί στην προσφορά μιας καλύτερης εμπειρίας στον τελικό χρήστη κατά την πρόσβαση σε υπηρεσίες μέσω διαδικτύου.

- Επίπεδο Ασφάλειας: Αποτελεί πρόκληση για κάθε σχεδιαστή και απαίτηση των χρηστών. Η προστασία έναντι επιθέσεων οποιαδήποτε σκοπιμότητας είναι ύψιστης σημασίας για τον IETF.

- NIST (National Institute of Standards and Technology)

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ιδρύθηκε στην Αμερική και αποτελεί σήμερα μέλος του Υπουργείου Εμπορίου των Ηνωμένων Πολιτειών.

Το NIST έχει σχεδιάσει το πρόγραμμα "5G και Beyond", το οποίο επικεντρώνεται σε νέες τεχνολογίες ασύρματης επικοινωνίας. Στο πλαίσιο αυτό διεξάγει μελέτες

συμπεριφοράς και επεξεργασίας καναλιών σε διαφορετικά περιβάλλοντα υψηλής κινητικότητας όπως είναι το 5G, καταγράφοντας έγκυρες μετρήσεις και εκδίδοντας αποτέλεσμα υψηλής ακρίβειας (Gentile et al., 2018).

Ανάμεσα στις δοκιμές που διεξάγονται περιλαμβάνονται δοκιμές πολλαπλών MIMO και μετρήσεις διάφορων μοντέλων κεραίας και καναλιών.

- Οργανισμός 5G AMERICAS

Το 5G Americas είναι ένας εμπορικός οργανισμός βιομηχανιών, παρόχων και κατασκευαστών τηλεπικοινωνιακών υπηρεσιών. Η αποστολή του οργανισμού είναι να υποστηρίξει και να προωθήσει την πρόοδο και τις πλήρεις δυνατότητες των ασύρματων τεχνολογιών LTE και την εξέλιξή τους σε 5G, σε όλα τα δίκτυα, τις υπηρεσίες, τις εφαρμογές και τις συνδεδεμένες συσκευές του οικοσυστήματος στην Αμερική.

Συνέταξε μνημόνιο συνεργασίας με τις ITU, 3GPP, NGMN, ATIS κ.α και συνεργασίες με κορυφαίες εθνικές και περιφερειακές ενώσεις παγκόσμιας κλίμακας.

- IMT 2020 (5G)

Η Chinese Evaluation Group IMT-2020 είναι υπεύθυνη για την οργάνωση και τον συντονισμό καθηκόντων τεχνικής αξιολόγησης. Καταρτίζει το τακτικό πρόγραμμα τεχνικής συζήτησης και αξιολόγησης ενώ παράλληλα συνεργάζεται και αλληλεπιδρά με ομάδες αξιολόγησης άλλων φορέων όπως εταιρείες εξοπλισμού, πανεπιστήμια, ερευνητικά ιδρύματα κ.α. Περιλαμβάνει διάφορες ομάδες εργασίας για την προώθηση της 5G τεχνολογίας και διοργανώνει απολογιστικές ετήσιες συναντήσεις για την αξιολόγηση και τον έλεγχο της πρόοδο του 5G (ITU, 2019).

- 5GPP

Η σύμπραξη δημόσιου και ιδιωτικού τομέα 5G (5G Public Private Partnership) αποτελεί το μεγαλύτερο ερευνητικό πρόγραμμα μεταξύ της Ευρωπαϊκής Επιτροπής και της Ευρωπαϊκής βιομηχανίας. Το 5G - PPP αποσκοπεί να προάγει λύσεις, αρχιτεκτονικές, τεχνολογίες και πρότυπα για την εμπορική ανάπτυξη του 5G στην Ευρώπη. Η 5G PPP έχει ως όραμα την ηγετική και ανταγωνιστική επικράτηση της Ευρώπης στην παγκόσμια αγορά, μέσω της δημιουργίας νέων αγορών (π.χ. έξυπνες πόλεις), της ηλεκτρονικής/ψηφιακής υγείας και των έξυπνων μεταφορών (European Commission, χ.η.).

- NGMN (Next Generation Mobile Networks)

Η Συμμαχία Νέων Γενιών Κινητών Δικτύων (NGMN), αποτέλεσε αναμφίβολα τον εγγυητή για τη αποτελεσματική μετάβαση της αγοράς στα δίκτυα 4G και στην καθοδήγηση για το 5G.

Στοχεύει στην προσφορά προσιτών τις ευρυζωνικών υπηρεσιών στον τελικό χρήστη βάσει των LTE και LTE-Advanced. Το NGMN προωθεί την τυποποίηση της τεχνολογίας 5G ώστε να περιοριστούν τα ζητήματα ασυμβατότητας και να απλουστευθούν οι σχετικές διαδικασίες. Το εγχείρημα τυποποίησης του 5G υποστηρίζεται από διάφορους οργανισμούς προκειμένου να εξαλειφθούν οι αντιθέσεις και τα διαφορετικά πρότυπα τα οποία δημιουργούν ασυμβατότητες. Τέλος δίνεται έμφαση στο να πληρούνται οι προϋποθέσεις προστασίας του οικοσυστήματος από τα δίκτυα και τους παρόχους και ταυτόχρονα να εξυπηρετούνται οι ανάγκες των πελατών (European Commission, χ.η.).

- Τεχνική Συμβουλευτική Ομάδα της Ομοσπονδιακής Επιτροπής - FCC TAC ACTIVITIES

Το Τεχνολογικό Γνωμοδοτικό Συμβούλιο (Technical Advise Council - T.A.C.), παρέχει τεχνικές συμβουλές στην ομοσπονδιακή επιτροπή επικοινωνιών FCC. Απαρτίζεται από πλήθος κορυφαίων επιστημόνων και εμπειρογνωμόνων οι οποίοι εργάζονται σε σημαντικούς τομείς καινοτομίας αναπτύσσοντας πολιτικές και δράσεις που προάγουν την ανταγωνιστικότητα.

Ιδιαίτερα σημαντική είναι η συμβολή του TAC για την Κυβερνοασφάλεια (Cybersecurity) καθώς αξιοποιεί τις πληροφορίες της Cyber WG αναφορικά με την ασφάλεια του διαδικτύου. Μέσω των πληροφοριών αυτών προτείνει στην Ομοσπονδιακή Επιτροπή Επικοινωνιών - FCC τη στρατηγική, τις διαδικασίες και τα δράσεις που απαιτούνται για την ενσωμάτωση των μεθόδων ασφάλειας στο σχεδιασμό της τεχνολογίας 5G. Τέλος συμβάλει στη δημιουργία νέων θέσεων εργασίας παγκοσμίως μέσω των προγραμμάτων αναδυόμενων καινοτόμων τεχνολογιών (Federal Communications Commission, 2017).

2.5.1 Βασικά πρότυπα για το 5G

Εκτός των κύριων προτύπων της οικογένειας IEEE 802, το IEEE έχει προβεί στην έκδοση προτύπων που εμπίπτουν στο ευρύτερο πεδίο εφαρμογής του 5G. Τα κυριότερα είναι τα ακόλουθα (IEEE future networks Enabling 5G and beyond, χ.η.):

- IEEE P1900.1

Η ομάδα εργασίας IEEE 1900.1, εργάζεται για την τυποποίηση των όρων και των ορισμών στον τομέα δυναμικής πρόσβασης στο φάσμα εγγενών τεχνολογιών. Αντικείμενο της ομάδας είναι να καταστήσει στα ενδιαφερόμενα μέρη κατανοητές τις έννοιες των σχετικών τεχνολογιών για την αποτελεσματικότερη συνεργασία τους στο πλαίσιο προώθησης νέων προοπτικών και ανάπτυξης προϊόντων καινοτομίας και έρευνας.

- IEEE P1900.2.

Η ομάδα εργασίας IEEE P1900.2, έχει ως αντικείμενο την ανάλυση των παρεμβολών εντός της ζώνης και των παρακείμενων αυτής, καθώς επίσης της ομαλής συνύπαρξης των ραδιοφωνικών συστημάτων. Οι μελέτες και οι δράσεις της ομάδας στοχεύουν στον εντοπισμό νέων προοπτικών της τεχνολογίας αναφορικά με τη φασματική διαχείριση, τις πολιτικές της ασύρματης επικοινωνίας, την συμβατότητα και το λογισμικό προκειμένου για τη βελτίωση της απόδοσης του φάσματος. Τέλος θα πρέπει να αναφέρουμε ότι η συγκεκριμένη ομάδα εργασίας εξετάζει τη δυνατότητα συνύπαρξης των ραδιοσυστημάτων καθώς και σχετικών με αυτά παραμέτρους ανάμεσα στις οποίες οι παρεμβολές στην ίδια ή σε διαφορετική ζώνη συχνοτήτων.

- IEEE P1903-NGSON.

Ο IEEE στο πλαίσιο διερεύνησης της λειτουργικότητας της αρχιτεκτονικής του δικτύου επικαλυπτόμενων υπηρεσιών επόμενης γενιάς (Next Generation Service Overlay Networks - NGSON), δημιούργησε την ομάδα εργασίας IEEE P1903-NGSON επενδύοντας το ανάλογο χρηματικό ποσό για την υποστήριξη του έργου της ομάδας. Το συγκεκριμένο πρότυπο, καθορίζει το πλαίσιο υπηρεσιών βάσει του πρωτόκολλου (IP) και προσδιορίζει τον τύπο των δεδομένων, το είδος των παρεχόμενων υπηρεσιών, τα τερματικά και τα δυναμικά προσαρμοσμένα δίκτυα τα οποία λειτουργούν ανεξάρτητα από τα υποκείμενα δίκτυα.

- IEEE P1903.2.

Βάσει του προτύπου αυτού καθορίζονται τα πρωτόκολλα διασύνδεσης μεταξύ των διάφορων οντοτήτων στα επικαλυπτόμενα δίκτυα νέας γενιάς. Το πρότυπο έχει την ιδιότητα παροχής στους φορείς εκμετάλλευσης δικτύων, στους παρόχους υπηρεσιών και στους τελικούς χρήστες να χρησιμοποιούν υπηρεσίες από τη σύνθεση υπηρεσιών του NGSON. Με βάσει τα παραπάνω, εξασφαλίζει την ομαλή λειτουργία μεταξύ σύνθετων υπηρεσιών των φορέων εκμετάλλευσης δικτύων και των παρόχων υπηρεσιών.

- IEEE P1901.3.

Βάσει του προτύπου αυτού, ορίζονται τα πρωτόκολλα διαχείρισης του συνόλου των κόμβων NGSON. Ανάμεσα στις λειτουργίες που υποστηρίζει είναι η επιλογή ενεργοποίησης/απενεργοποίησης, προσθήκης, διαγραφής, μετακίνησης και αντιγραφής κόμβων NGSON. Τέλος πρέπει να αναφέρουμε ότι η συμβολή του στην αύξηση της απόδοσης δρομολόγησης είναι σημαντική.

- IEEE P1912.

Πρόκειται για ένα πρότυπο ιδιαίτερης σημασίας καθώς σχετίζεται με την αρχιτεκτονική προστασίας των προσωπικών δεδομένων και την τήρηση της ασφάλειας των ασύρματων συσκευών. Στο πλαίσιο αυτό βασικό μέλημα αποτελεί η ανάπτυξη και η επικράτηση μιας κοινού τύπου αρχιτεκτονικής σε θέματα ασφάλειας τόσο σε οικιακά δίκτυα όσο και επαγγελματικούς χώρους.

- IEEE P1914.1.

Αφορά στην αρχιτεκτονική μεταφοράς των δεδομένων χρήστη, της διαχείρισης της κίνησης και των λειτουργιών ελέγχου. Τέλος καθορίζει τις απαιτήσεις ως προς το ρυθμό δεδομένων, το χρονισμό και συγχρονισμό καθώς και την ποιότητα των υπηρεσιών (QOS).

VIII. IEEE P1915.1.

Σχετίζεται με την ασφάλεια της δικτύωσης, η οποία καθορίζεται από το λογισμικό για τις εικονικές λειτουργίες ασφάλειας του δικτύου.

- IEEE P1916.1.

Σχετίζεται με τη δικτύωση SDN και την απόδοση του NFV. Παράλληλα, θέτει το πλαίσιο των απαιτούμενων και επιθυμητών επιδόσεων, καθορίζει τις μετρήσεις και τις απαιτήσεις, καθορίζει τα μοντέλα για τη δικτύωση βάσει του λογισμικού και της λειτουργίας SDN / NFV.

- IEEE P1917.1.

Παρέχει τις υπηρεσίες SDN / NFV διασφαλίζοντας την αξιοπιστία των υπηρεσιών των δικτύων και παράλληλα βελτιώνει τις λειτουργίες του συστήματος συνολικά.

- IEEE P1930.1.

Καθορίζει το λογισμικό για τη διαχείριση των ασύρματων δικτύων και διαχειρίζεται τον έλεγχο των σημείων πρόσβασης στα ασύρματα δίκτυα τοπικής εμβέλειας (WLAN) βάσει των IEEE 802.11 και IEEE 802.22.

- IEEE P1931.1.

Υλοποιεί το αρχιτεκτονικό πλαίσιο, τα πρωτόκολλα και τις διεπαφές προγραμματισμού των εφαρμογών (APIs) για την παροχή real time υπηρεσιών. Συμβάλει στη διαλειτουργικότητα και την αυτόνομη λειτουργία των δικτύων IOT καθιστώντας τα ευέλικτα και δυναμικά.

- IEEE P2413.

Καθορίζει το πλαίσιο της αρχιτεκτονικής της τεχνολογίας IOT.

2.6 Συνδυασμός 5G με τεχνολογίες IOT, Cloud και Fog

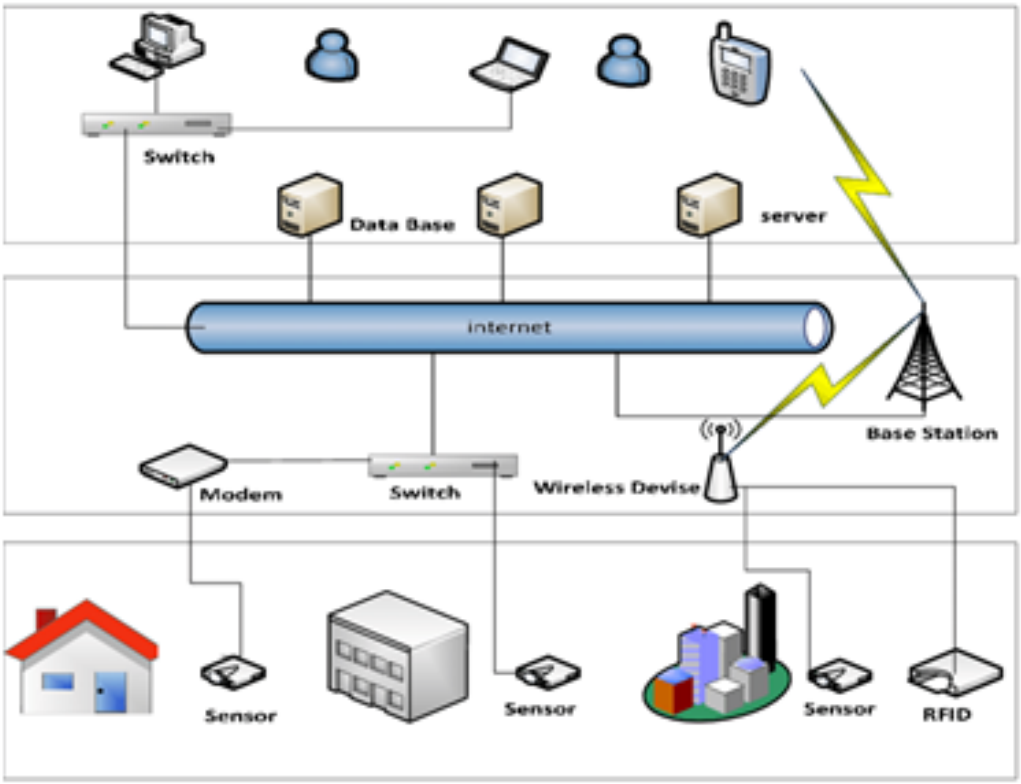
Βάσει των στοιχείων που παρουσιάσαμε στο Κεφ.1 συνάγεται το συμπέρασμα ότι οι υψηλοί ρυθμοί μετάδοσης μπορούν να υποστηρίξουν ένα μεγάλο αριθμό παρεχόμενων υπηρεσιών. Προς αυτή την κατεύθυνση, εφαρμογές για επικοινωνίες Machine-to-Machine (M2M) και IOT δύνανται να υποστηριχθούν αποτελεσματικά από τα δίκτυα 5G.

Η έννοια της τεχνολογίας “Internet of Things” (IoT) αναφέρεται σε αντικείμενα της καθημερινότητας, όπως wearable συσκευές, βιομηχανικές μηχανές, συσκευές με ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και την εντολοδότη συγκεκριμένων αποφάσεων του δικτύου κ.α.

Η βασική ιδέα πίσω από το IoT, είναι η διασύνδεση των ηλεκτρονικών συσκευών μέσω του διαδικτύου ώστε να είναι εφικτός ο έλεγχος και η διαχείριση των διαδικασιών και εργασιών ανάλογα με τις ανάγκες και τις απαιτήσεις κάθε χρήστη.

Η ονοματοδοσία και η απόδοση του όρου IOT έγινε το 2000 από τον επιχειρηματία Kevin Ashton, ενός από τους ιδρυτές του Auto-ID Center στο MIT. Οι ερευνητές ανακάλυψαν έναν νέο, επαναστατικό τρόπο διασύνδεσης αντικειμένων με το διαδίκτυο μέσω μιας ετικέτας RFID χωρίς να είναι απαραίτητη η απευθείας πρόσβαση των συσκευών σε αυτό.

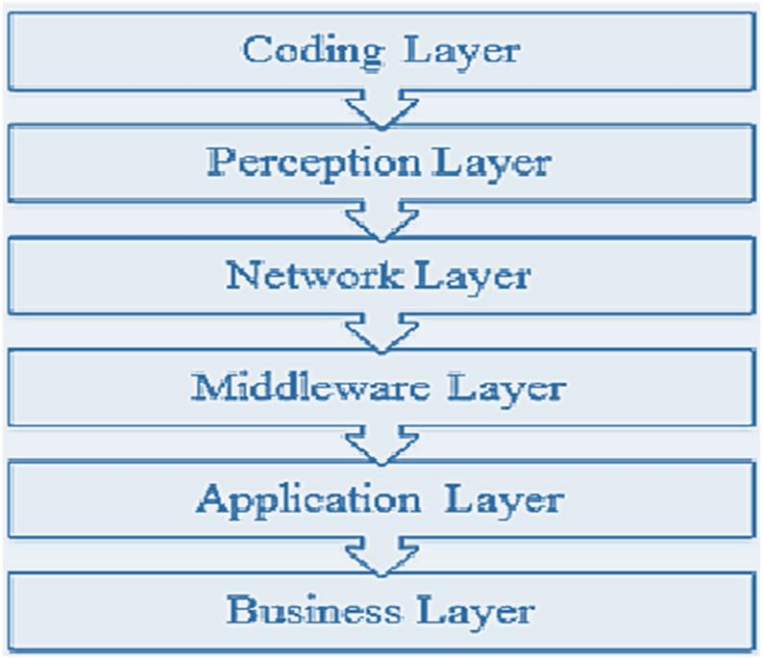
Πρακτικά λοιπόν θα λέγαμε ότι IOT είναι ένα περιβάλλον, στο οποίο γίνεται συλλογή δεδομένων διάφορων ηλεκτρονικών συσκευών ή αισθητήρων που είναι συνδεδεμένοι μεταξύ τους. Για παράδειγμα μια εταιρία ή ένα κτίριο που θα μπορούσε με τη βοήθεια αισθητήρων, να εκτελεί κάποιες λειτουργίες όπως την αυτόνομη ρύθμιση της θέρμανσης, του κλιματισμού, του φωτισμού την ενεργοποίηση/απενεργοποίηση των ρολών ασφαλείας κ.α.



Εικόνα 2.3: Τυπική Αρχιτεκτονική IOT

(Πηγή: Lasloum & Al-Mogren, 2016)

Είναι γεγονός ότι μετά το 2020 οι οντότητες που συνδέονται στο Διαδίκτυο ξεπερνά τα 25 δισεκατομμύρια που είναι ένας τεράστιος αριθμός για να μπορέσει η υπάρχουσα αρχιτεκτονική του Διαδικτύου με τα πρωτόκολλα TCP/IP να τον διαχειριστεί. Το γεγονός αυτό ανέδειξε την αναγκαιότητα για την ανάπτυξη μιας νέας αρχιτεκτονικής η οποία πέρα από δυνατότητα σύνδεσης ενός τεράστιου αριθμού πραγμάτων στο διαδίκτυο θα μπορούσε να αντιμετωπίσει διάφορα θέματα ασφάλειας και ποιότητας υπηρεσίας (QoS) και παράλληλα να υποστηρίξει τις υπάρχουσες εφαρμογές δικτύου χρησιμοποιώντας ανοιχτά πρωτόκολλα. Για την περαιτέρω ανάπτυξη του IoT, προτείνεται μια σειρά πολυεπίπεδης αρχιτεκτονικής ασφάλειας. Στο πλαίσιο αυτό έχουν προταθεί αρχιτεκτονικές τριών, τεσσάρων, πέντε ακόμα και έξι επιπέδων όπως φαίνεται στην παρακάτω Εικόνα 2.4.



Εικόνα 2.4: Αρχιτεκτονική IOT έξι επιπέδων

(Πηγή: Farooq et al., 2015)

Σύμφωνα με τους Farooq et al. (2015), για κάθε επίπεδο ισχύει:

1. Επίπεδο Κωδικοποίησης

Το επίπεδο κωδικοποίησης είναι το θεμέλιο του IoT καθώς παρέχει αναγνώριση στα αντικείμενα ενδιαφέροντος. Σε κάθε αντικείμενο αυτού του επιπέδου εκχωρείται ένα

μοναδικό αναγνωριστικό που διευκολύνει τη διάκρισή του.

2. Επίπεδο Αντίληψης

Το επίπεδο αυτό προσφέρει φυσική σημασία σε κάθε αντικείμενο. Αποτελείται από διάφορους τύπους αισθητήρων δεδομένων όπως ετικέτες RFID, αισθητήρες υπέρυθρων, αισθητήρες ανίχνευσης της θερμοκρασίας, της υγρασίας, της ταχύτητας, της θέσεως των αντικειμένων κ.α. Στο στρώμα του επιπέδου συλλέγονται χρήσιμες πληροφορίες των αντικειμένων που συνδέονται με τις συσκευές αισθητήρων και στην συνέχεια οι πληροφορίες αυτές μετατρέπονται σε ψηφιακά σήματα τα οποία διαβιβάζονται στο επόμενο επίπεδο ήτοι το επίπεδο δικτύου.

3. Επίπεδο δικτύου.

Ο σκοπός αυτού του επιπέδου είναι να λάβει τις χρήσιμες πληροφορίες σε μορφή ψηφιακών σημάτων από το Επίπεδο Αντίληψης και να τις μεταδώσει στα συστήματα επεξεργασίας του επόμενου ενδιάμεσου επιπέδου χρησιμοποιώντας διάφορα μέσα αποστολής όπως WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G με πρωτόκολλα IPv4, IPv6, MQTT, DDS κ.τ.λ.

4. Middlware Επίπεδο

Στο επίπεδο αυτό υλοποιείται η επεξεργασία των πληροφοριών που λαμβάνονται από τους αισθητήρες. Περιλαμβάνει τεχνολογίες όπως το Cloud computing, ώστε να εξασφαλίζει άμεση πρόσβαση στις πληροφορίες που είναι αποθηκευμένες στη βάση δεδομένων. Στη συνέχεια οι πληροφορίες υφίστανται επεξεργασία.

5. Επίπεδο Εφαρμογής

Αυτό το επίπεδο υλοποιεί τις εφαρμογές του IoT για όλα τα είδη βιομηχανίας, με βάση τα επεξεργασμένα δεδομένα. Επειδή οι εφαρμογές αυτές προωθούνται από την ανάπτυξη του IoT, συμπεραίνουμε ότι το επίπεδο αυτό είναι ιδιαίτερα χρήσιμο για την ανάπτυξη του δικτύου IoT σε ευρεία κλίμακα. Παραδείγματα τέτοιων εφαρμογών θα μπορούσαν να είναι έξυπνα σπίτια, έξυπνες μεταφορές, έξυπνες πόλεις, έξυπνος πλανήτης κ.α.

6. Επιχειρησιακό Επίπεδο.

Το επίπεδο αυτό αναλαμβάνει την διαχείριση των εφαρμογών και των υπηρεσιών του IoT και γενικότερα θεωρείται υπεύθυνο για όλη την έρευνα που σχετίζεται με το IoT. Τέλος,

συμβάλει στη δημιουργία διάφορων επιχειρηματικών μοντέλων για την υιοθέτηση και την υλοποίηση αποτελεσματικών επιχειρηματικών στρατηγικών.

Συμπερασματικά, η τεχνολογία IOT αποτελεί το πιο ελπιδοφόρο τεχνολογικό μέλλον στην καθημερινότητά μας, φιλοδοξώντας να απλουστεύσει ακόμα περισσότερο την ζωή μας. Ωστόσο παρά τις μεγάλες προκλήσεις και ευκαιρίες που δημιουργεί η τεχνολογία του IoT αποτελεί ζητούμενο η προστασία των προσωπικών δεδομένων και η διασφάλιση της ιδιωτικότητας των χρηστών.

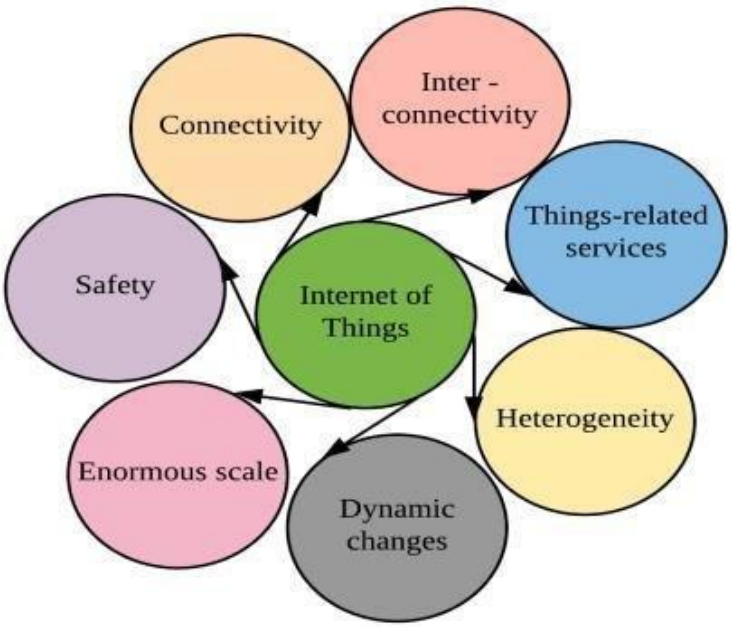
2.7 Ορισμός και βασικές εφαρμογές IOT

Ως τεχνολογία Internet of Things (IOT) ορίζεται το δίκτυο των αντικειμένων που περιλαμβάνουν συστήματα, λογισμικά, αισθητήρες κλπ., με δυνατότητα διαδικτυακής σύνδεσης ώστε να συλλέγουν και να ανταλλάσσουν δεδομένα αναμεταξύ τους.

Σύμφωνα με την αρχή λειτουργίας της τεχνολογίας IOT οι συσκευές που είναι συνδεδεμένες στο διαδίκτυο ελέγχονται από απόσταση μέσω της υπάρχουσας δικτυακής υποδομής. Αυτό συνεπάγεται τη βελτίωση της αποτελεσματικότητας, της ακρίβειας και τη μείωση του κόστους, δεδομένου ότι υφίσταται ενσωμάτωση στα υπολογιστικά συστήματα.

Κάθε συσκευή που συμμετέχει στην τεχνολογία IOT, όπως για παράδειγμα οι αισθητήρες και οι ενεργοποιητές, αναγνωρίζεται ως μονοσήμαντη οντότητα από το ενσωματωμένο υπολογιστικό σύστημα. Ταυτόχρονα, συνδυάζουν την ικανότητα να μπορούν να λειτουργούν αυτόνομα αλλά και σε απόλυτη συνεργασία με την υπάρχουσα διαδικτυακή υποδομή.

Ο όρος Internet of Things εισήχθη στην πληροφορική τη δεκαετία του ’90 από το Auto-ID Center του Πανεπιστημίου MIT, λόγω του ότι προέκυψε η ανάγκη για την ταυτοποίηση και προτυποποίηση των ραδιοσυχνοτήτων (RFID) η οποία αποτελούσε προαπαιτούμενο για την υλοποίηση της τεχνολογίας IOT. Η έννοια Internet of Things πέρα από το ότι δηλώνει τη συνδεσιμότητα μεταξύ συσκευών, συστημάτων και υπηρεσιών, αναφέρεται και σε ένα μεγάλο φάσμα πρωτοκόλλων, προτυποποίησης και εφαρμογών.



Εικόνα. 2.5: Χαρακτηριστικά IoT

(Πηγή: Pradeepa & Parveen, 2020)

Τέλος, τα κυριότερα χαρακτηριστικά που διέπουν την τεχνολογία IOT είναι τα εξής (Pradeepa & Parveen, 2020):

i. Επικοινωνία: Οι συσκευές με τη χρήση δεδομένων και υπηρεσιών, δικτυώνονται με τους πόρους του διαδικτύου. Στην επικοινωνία αυτή συντελούν οι τεχνολογίες ασύρματων ζεύξεων, όπως το UMTS, το Wi-Fi και το Bluetooth.

ii. Διευθυνσιοδότηση: Σε ένα σύστημα όπου εφαρμόζεται η τεχνολογία IOT, οι συσκευές διευθυνσιοδοτούνται μέσω της διαδικασίας ανεύρεσης. Επίσης δύνανται να προσδιορίζονται από το όνομα της παρεχόμενης υπηρεσίας και ρυθμίζονται από απόσταση.

iii. Ταυτοποίηση: Οι συσκευές αναγνωρίζονται και ταυτοποιούνται μονοσήμαντα με τη βοήθεια των τεχνολογιών RFID, NFC (Near Field Communication) και των οπτικά αναγνώσιμων κωδίκων (optical bar codes).

iv. Ανίχνευση: Οι αισθητήρες συμμετέχουν στην ανίχνευση των συσκευών. Ειδικότερα, αναλαμβάνουν τη συλλογή, την καταγραφή και τη διαβίβαση των

πληροφοριών.

v. Ενεργοποίηση: Οι ενεργοποιητές μετατρέπουν τα ηλεκτρικά σήματα που λαμβάνουν προκειμένου να συμβάλλουν σε διαδικασίες ελέγχου και παρακολούθησης διάφορων διεργασιών οι οποίες υλοποιούνται μέσω του διαδικτύου.

vi. Επεξεργασία και αποθήκευση των πληροφοριών: Τα δεδομένα επεξεργάζονται βάσει των πληροφοριών που προέρχονται από τους αισθητήρες. Η αποθήκευση των δεδομένων γίνεται από τις έξυπνες συσκευές που διαθέτουν επεξεργαστή ή μικροελεγκτή.

vii. Εντοπισμός: Οι έξυπνες συσκευές έχουν την ικανότητα να μπορούν να εντοπίζονται ως προς τη θέση τους με τη βοήθεια τεχνολογιών GPS, GSM,UMTS.

viii. Διεπαφή: Αναφέρεται στην επικοινωνία ανάμεσα στο χρήστη και τις έξυπνες συσκευές. Η επικοινωνία δύναται να πραγματοποιηθεί. μέσω ενός έξυπνου κινητού τηλεφώνου.

ix. Διασυνδεσιμότητα: Με την τεχνολογία IoT η έννοια της διασυνδεσιμότητας αφορά σε κάθε αντικείμενο που μπορεί να συνδεθεί με την υποδομή δεδομένων και επικοινωνίας σε παγκόσμιο επίπεδο.

x. Ετερογένεια: Οι κόμβοι στο IoT είναι ετερογενείς καθώς στηρίζονται σε διάφορες πλατφόρμες και δίκτυα υλικού. Επιτρέπουν την επικοινωνία με άλλες συσκευές ή πλατφόρμες υπηρεσιών μέσω διαφορετικών δικτύων.

xi. Δυναμικές αλλαγές: Η κατάσταση των κόμβων δύναται να τροποποιείται ευέλικτα και δυναμικά ανάλογα με τον αριθμό συνδεδεμένων και αποσυνδεδεμένων χρηστών, τη φύση των συσκευών, την ταχύτητα και την τοποθεσία.

xii. Ευρεία κλίμακα: Ο αριθμός των κόμβων που απαιτείται για τη διαχείριση της κίνησης του δικτύου είναι μια τάξη μεγέθους καλύτερη από τις συσκευές που συνδέονται με το Διαδίκτυο. Η διαχείριση των δεδομένων που δημιουργούνται και η ερμηνεία τους ανάλογα με το είδος κάθε εφαρμογής αποτελεί κρίσιμη παράμετρο για τη λειτουργία του δικτύου. Πρακτικά, σχετίζεται με τη σημασιολογία των πληροφοριών καθώς και τον άρτιο χειρισμό αυτών.

xiii. Ασφάλεια: Τα πλεονεκτήματα που παρέχει η τεχνολογία του IoT, θα πρέπει συνδυάζονται με την ασφάλεια. Οι σχεδιαστές του IoT, πρέπει να λαμβάνουν

υπόψη κατά τον σχεδιασμό όλες τις παραμέτρους που σχετίζονται με ζητήματα για την ασφάλεια και την προστασία των προσωπικών δεδομένων των χρηστών. Προς αυτή την κατεύθυνση, η προστασία των τελικών σημείων, των δικτύων και των δεδομένων που διακινούνται θα πρέπει να προστατεύονται από ένα δυναμικό και κλιμακούμενο μοντέλο ασφαλείας.

xiv. Συνδεσιμότητα: Επιτρέπει τη συμβατότητα και την προσβασιμότητα του δικτύου. Η προσβασιμότητα λαμβάνεται σε ένα δίκτυο, ενώ η συμβατότητα προσφέρει τη γενική δυνατότητα κατανάλωσης και δημιουργίας πληροφοριών.

Τέλος, το IoT περιλαμβάνει γενικά συσκευές IoT με ισχύ μπαταρίας που επικοινωνούν μεταξύ τους για να μεταδώσουν ένα μήνυμα από μια συσκευή αποστολέα σε έναν σταθμό βάσης IoT. Λόγω του περιορισμού στο εύρος μετάδοσης του σήματος απαιτείται η δρομολόγηση. Στο IoT, η δρομολόγηση αναφέρεται στις συσκευές που επικοινωνούν με το σταθμό βάσης, μεταδίδοντας μηνύματα προσφέροντας τη δυνατότητα αναγνώρισης και επιλογής της βέλτιστης διαδρομής από τη συσκευή προς το σταθμό βάσης. Ωστόσο πρέπει να επισημάνουμε ότι οι συσκευές IoT είναι ευαίσθητες στις απειλές ασφαλείας από επιθέσεις υποκλοπής, άρνησης υπηρεσίας και δρομολόγησης. Για την αποφυγή και τον περιορισμό αυτών, προτείνεται η χρήση κρυπτογραφικών πρωτοκόλλων.

2.7.1 Η έννοια της ετερογενούς σύνθεσης δεδομένων

Ετερογενής σύνθεση (ή σύντηξη) δεδομένων (heterogeneous data fusion) ονομάζεται η διαδικασία ενσωμάτωσης διαφορετικών δεδομένων από πολλαπλές πηγές για την παραγωγή ακριβέστερων και χρησιμότερων πληροφοριών συγκριτικά με τις πληροφορίες που προέρχονται από μεμονωμένες πηγές δεδομένων.

Ως ετερογενή σύνθεση δεδομένων εννοούμε την άντληση δεδομένων από πολλαπλές πηγές, με αποτέλεσμα την απόκτηση πληροφοριών υψηλότερης ποιότητας σε σχέση με τα αρχικά μεμονωμένα δεδομένα.

Η τεχνολογία της ετερογενούς σύνθεσης δεδομένων, χρησιμοποιεί την υπολογιστική ισχύ των ηλεκτρονικών υπολογιστών λαμβάνοντας χρονικές ακολουθίες των δεδομένων. Στην συνέχεια πραγματοποιείται αυτόματη συλλογή δεδομένων τα οποία μπορούν να υποστούν επεξεργασία, απεικόνιση, ανάλυση και στατιστική επεξεργασία στο πλαίσιο της αξιολόγησης και της λήψης αποφάσεων.

Η επεξεργασία για την απόκτηση των δεδομένων και τη διανομή τους, γίνεται σε συνάρτηση με τη δομή του συστήματος με τη χρήση διάφορων τρόπων. Μπορεί δηλαδή να γίνει με συγκεντρωτικό, κατανεμημένο ή μεικτό τρόπο.

Η σύνθεση των δεδομένων αφορά στη συσχέτισή τους, στην εκτίμηση βάσει στόχου, σε τεχνικά χαρακτηριστικά λειτουργιών, στην ανίχνευση συμπεριφοράς, στην εκτίμηση ταυτότητας, στην πρόβλεψη συμπεριφοράς, στην αξιολόγηση της κατάστασης κ.λπ.

Η συγχώνευση των δεδομένων ακολουθεί μια ιεραρχική σειρά των παρακάτω σταδίων:

- ✓ Επεξεργασία της σύνθεσης δεδομένων σε σχέση με τα αρχικά δεδομένα
- ✓ Σύνθεση ανά επίπεδο με τις αρχικές πληροφορίες, ανάλυση και επεξεργασία
- ✓ Σύνθεση της λήψης των αποφάσεων.

Οι εφαρμογές της IOT περιλαμβάνουν κατά βάση ετερογενείς έξυπνες συσκευές που συνδέονται και επικοινωνούν μεταξύ τους διαθέτοντας ξεχωριστά αναγνωριστικά ID. Ιδιαίτερα συχνή είναι και η χρήση εφαρμογών IOT οι οποίες χρησιμοποιούν δεδομένα από έξυπνες συσκευές που διαθέτουν αισθητήρες.

Είναι σαφές ότι η τεχνολογία IoT αποτελείται από ένα μεγάλο πλήθος συστημάτων που είναι διασυνδεδεμένα στο διαδίκτυο. Χρησιμοποιούν τις IPv6 διευθύνσεις προκειμένου να εξυπηρετήσουν την απόδοση μεγάλου αριθμού διευθύνσεων. Να σημειωθεί ότι κάθε αντικείμενο λαμβάνει μια διεύθυνση IP ή Uniform Resource Identifier (URI).

Η εν λόγω τεχνολογία χαρακτηρίζεται από μεγάλο βαθμό αξιοπιστίας και λειτουργικότητας ενώ συγχρόνως συνεισφέρει ουσιαστικά στην μείωση του κόστους και της κατανάλωσης της ενέργειας.

Ανάμεσα στο πλήθος των εφαρμογών του IOT αναφέρουμε ενδεικτικά τις παρακάτω:

- Smart Mobility

- Έξυπνα σπίτια (Smart Home)

- Υπηρεσία Οικογενειακής ασφάλειας

- Υπηρεσία ιατρικής εξ αποστάσεως παρακολούθησης

- Υπηρεσία οικογενειακών δεδομένων, ψυχαγωγίας και ποικίλων δραστηριοτήτων

- Έξυπνες πόλεις

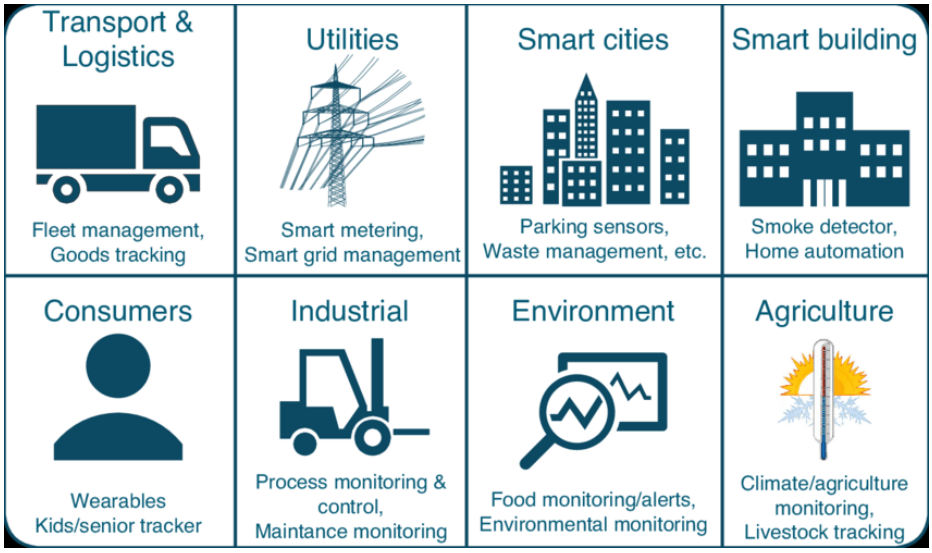
- Έξυπνη βιομηχανία

- Έξυπνο περιβάλλον

- Έξυπνη Γεωργία και κτηνοτροφία

-Υπηρεσίες Μεταφορών και ρύθμισης της κυκλοφορίας

Επίσης, με την τεχνολογία IOT ενσωματώνεται η επικοινωνία των παθητικών αισθητήρων με τις ενσωματωμένες συσκευές και το διαδίκτυο.



Εικόνα 2.6: Ποικίλες εφαρμογές IOT

(Πηγή: https://vizah.ch/en/developing-iot-applications-best-technologies-and-tools-for-iot-developers/)

Οι κύριες τεχνολογίες του IOT είναι οι κάτωθι (Baoan & Jianjun 2011; Miorandi et al., 2012):

1. Πρωτόκολλο IPv6

2. RFID (Radio Frequency Identification)

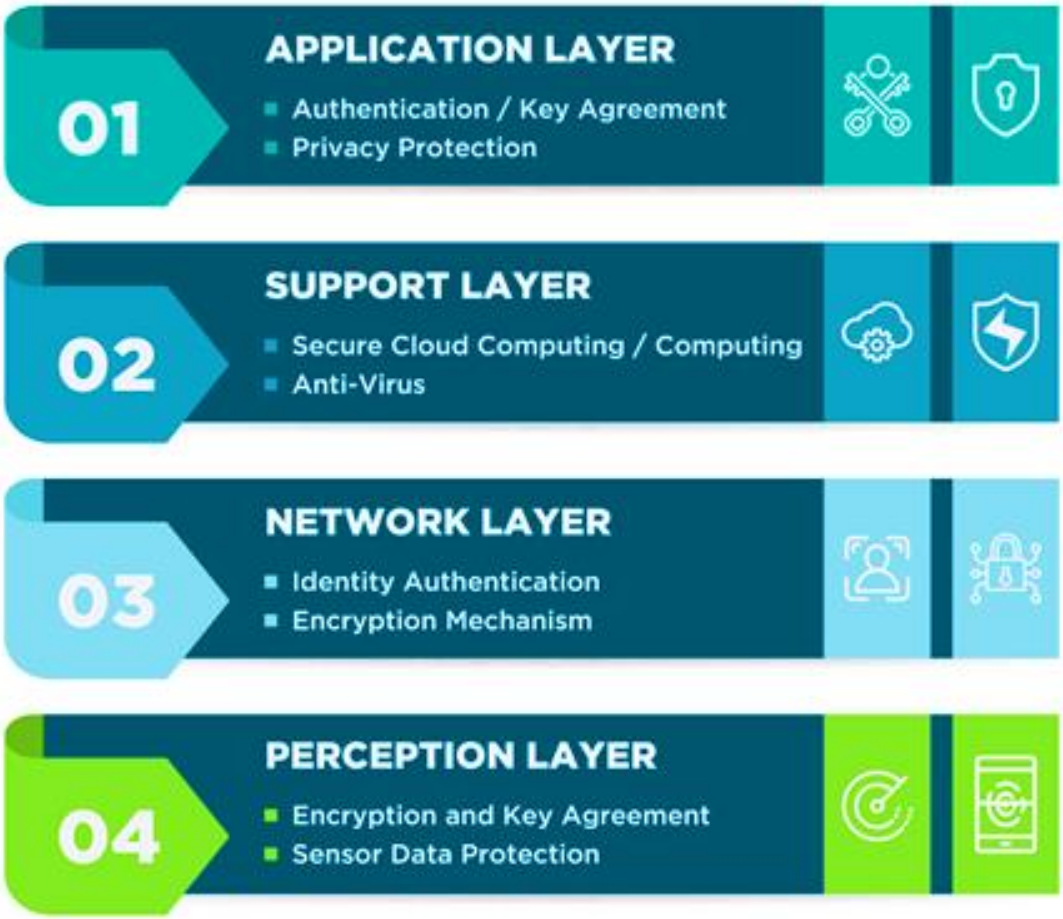
3. WSN (Wireless Sensor Network)

4. NFC (Near-Field Communication)

Όπως προαναφέραμε η αρχιτεκτονική IOT μπορεί να περιλαμβάνει τρία, τέσσερα ή και περισσότερα επίπεδα. Η βασική δομή περιλαμβάνει τέσσερα επίπεδα και ανάλογα με τις

υπολογιστικές δυνατότητες των συσκευών μπορούν να ενσωματώνονται στο σύνολο σχεδόν των βιομηχανικών προϊόντων. Μια τυπική δομή αρχιτεκτονικής τεσσάρων επιπέδων περιλαμβάνει τα ακόλουθα στρώματα:

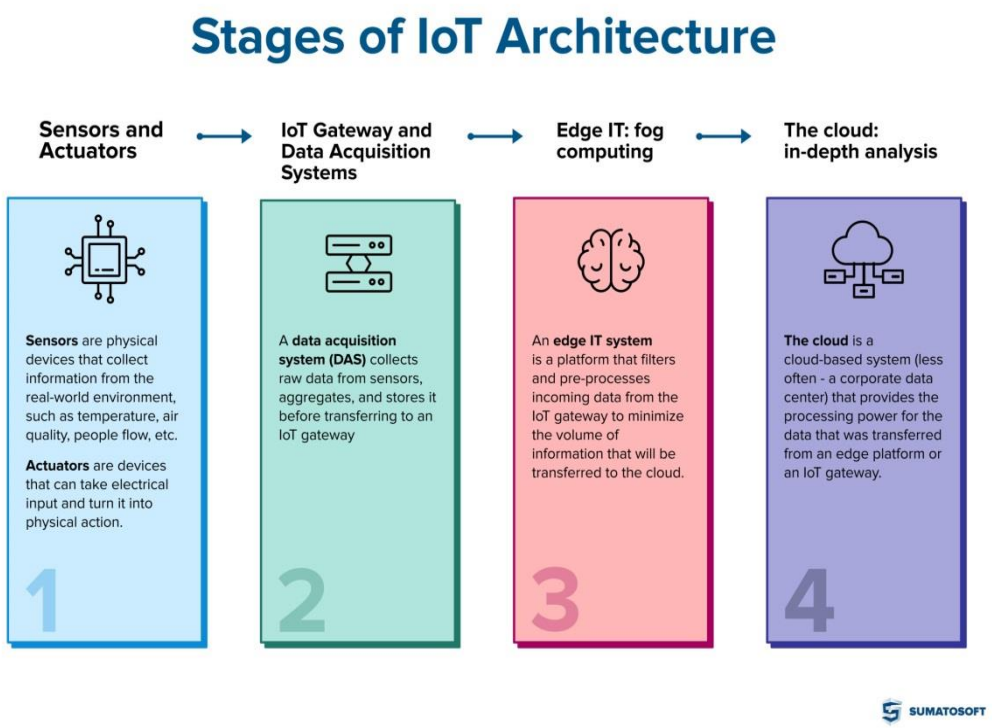
- Application Layer - Εφαρμογής
- Support /Service Layer - Υποστήριξης /Υπηρεσιών
- Network Layer -Δικτύου
- Perception Layer – Αντίληψης



Εικόνα 2.7: Αρχιτεκτονική τεσσάρων επιπέδων IOT

(Πηγή: https://jelvix.com/blog/iot-architecture-layers)

Το IOT λειτουργεί σε τέσσερις (4) βασικές φάσεις ήτοι οι ακόλουθες (Sumatosoft, 2022):



Εικόνα: 2.8 Στάδια αρχιτεκτονικής IOT

(Πηγή: Sumatosoft, 2022)

2.7.2 Αισθητήρες και ενεργοποιητές

Οι αισθητήρες και οι ενεργοποιητές αποτελούν βασικά στοιχεία της αρχιτεκτονικής του IoT. Οι αισθητήρες είναι φυσικές συσκευές που αντλούν πληροφορίες από το πραγματικό, φυσικό περιβάλλον. Τέτοιες πληροφορίες μπορεί να είναι η υγρασία, η θερμοκρασία, ο καπνός, το φυσικό φως, η πίεση του αίματος, η ροή των ανθρώπων ή των οχημάτων, η κίνηση εντός κλειστού χώρου κ.λπ. Γενικά οι αισθητήρες μετατρέπουν κάποιο φυσικό φαινόμενο σε ψηφιακή μορφή.

Οι ενεργοποιητές είναι συσκευές που δέχονται ηλεκτρική είσοδο και τη μετατρέπουν σε φυσική δράση. Συνήθως αλληλεπιδρούν με τους αισθητήρες για να εκτελέσουν μια λειτουργία όπως για παράδειγμα η απενεργοποίηση του φωτισμού όταν δεν ανιχνεύεται κίνηση σε μια έξυπνη κατοικία. Παρά το γεγονός ότι οι κλασικού τύπου ηλεκτρικοί αισθητήρες και ενεργοποιητές κυκλοφορούν στην αγορά εδώ και χρόνια η ανάπτυξη των

δικτύων 4G και 5G επέφερε των εκσυγχρονισμό τους σύμφωνα με τις τρέχουσες ανάγκες των καταναλωτών (Rayes & Salam, 2017).

2.7.3 IoT Gateway και Συστήματα Απόκτησης Δεδομένων

Ένα σύστημα απόκτησης δεδομένων (DAS) συλλέγει ακατέργαστα δεδομένα από αισθητήρες, τα οποία συγκεντρώνει και αποθηκεύει πριν τη μεταφορά τους σε μια πύλη IoT. Η ύπαρξη ποικίλων πρωτοκόλλων αισθητήρων συνδεσιμότητας και η ανάπτυξη ενός συστήματος DAS που θα είναι λειτουργικό για το σύστημα αποτελεί πρακτικό ζητούμενο (Posey, 2022).

Η πύλη IoT είναι ο ενδιάμεσος σταθμός ανάμεσα στις συνδεδεμένες συσκευές και το Cloud. Πρακτικά πρόκειται για μια συσκευή ή μια πλατφόρμα η οποία δέχεται τα δεδομένα από το DAS, τα συμπιέζει και τα ενσωματώνει στο Cloud. Η πύλη IoT και το DAS είναι ιδιαίτερα χρήσιμα καθώς (Posey, 2022):

- ✓ Εξασφαλίζουν τη μεταφορά δεδομένων από τις συσκευές στο Cloud
- ✓ Η μεταφορά των δεδομένων από τις συσκευές στο Cloud πραγματοποιείται με ασφαλή τρόπο
- ✓ Επιτρέπουν τη μετάδοση εντολών ελέγχου από το Cloud στα αντικείμενα.

Συμπερασματικά μια πύλη IOT και το DAS υλοποιούν τη συλλογή και την συμπίεση μεγάλου όγκου δεδομένων πριν μεταφερθούν στην πλατφόρμα Cloud για περαιτέρω ανάλυση.

2.7.4 Edge IT: υπολογισμός ομίχλης

Ένα σύστημα αιχμής αποτελείται από μια πλατφόρμα η οποία προεπεξεργάζεται και φιλτράρει τα δεδομένα εισόδου της πύλης IoT προκειμένου να μειώσει τον όγκο των πληροφοριών που θα μεταφερθούν στο cloud. Ονομάζεται επίσης υπολογισμός ομίχλης ή δίκτυο ομίχλης (Fog Computing).

Η αρχιτεκτονική ομίχλης βρίσκεται πλησίον της πηγής δεδομένων και υλοποιεί το φιλτράρισμα και την ανάλυση δεδομένων των αισθητήρων μέσω τοπικά τοποθετημένων κόμβων ομίχλης πριν τα δεδομένα μεταβούν στο σύννεφο.

Παρόλο που η αρχιτεκτονική IoT δύναται να λειτουργεί και χωρίς την πλατφόρμα Edge IT είναι προτιμότερη η ύπαρξή της καθώς προσφέρει ουσιαστικά πλεονεκτήματα στις λειτουργίες του IoT και συγκεκριμένα:

- ✓ μειώνει το φόρτο του δικτύου cloud
- ✓ περιορίζει το κόστος μετάδοσης των δεδομένων
- ✓ έχει άμεση ανταπόκριση (real time) στα πράγματα
- ✓ παρέχει παρακολούθηση των συσκευών IoT και των δραστηριοτήτων τους

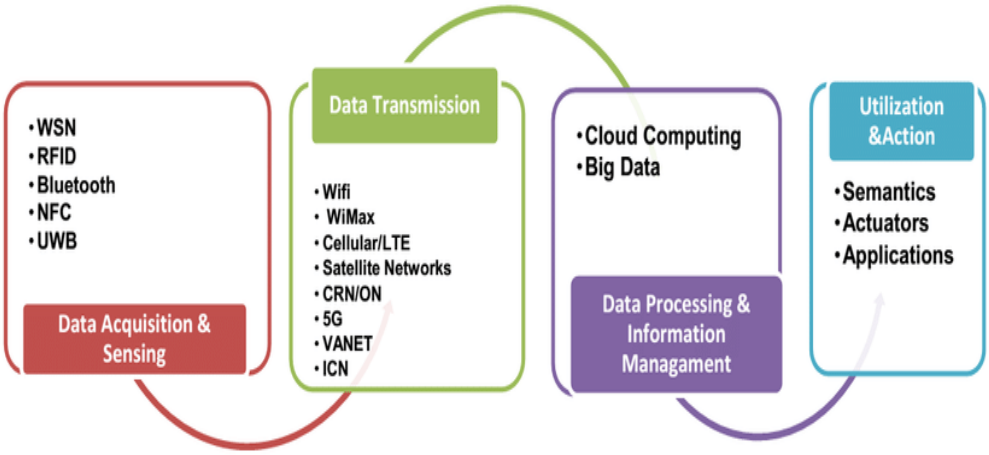
Σε μια βαθύτερη ανάλυση, το Cloud computing είναι ένα ευέλικτο μοντέλο, το οποίο επιτρέπει την δικτυακή πρόσβαση σε ένα κοινόχρηστο πλήθος υπολογιστικών πόρων. Στους πόρους αυτούς συγκαταλέγονται δίκτυα, εξυπηρετητές, εφαρμογές και υπηρεσίες και το κόστος διαχείρισης είναι σχετικά μικρό. Με λίγα λόγια, Cloud computing ονομάζεται εν γένει η παροχή υπολογιστικών υπηρεσιών μέσω του διαδικτύου (Mell & Grance, 2011).

Συνιστά σύστημα με ιδιαίτερα μεγάλη επεξεργαστική ικανότητα των δεδομένων που μεταφέρθηκαν από μια πλατφόρμα αιχμής ή μια πύλη IoT. Το cloud computing παρέχει υπηρεσίες μέσω του Διαδικτύου. Αυτοί οι πόροι περιλαμβάνουν εργαλεία και εφαρμογές όπως αποθήκευση δεδομένων, διακομιστές, βάσεις δεδομένων, δικτύωση και λογισμικό. Επιτρέπει στους χρήστες να την αποθήκευση δεδομένων τους, σε μια απομακρυσμένη βάση δεδομένων. Αποτελεί πλέον μια δημοφιλή και χρήσιμη επιλογή για ανθρώπους και επιχειρήσεις προσφέροντας παράλληλα εξοικονόμηση κόστους, αυξημένη παραγωγικότητα, ταχύτητα και αποδοτικότητα, απόδοση και ασφάλεια. Το cloud μπορεί να τροφοδοτηθεί με λογισμικό αναλυτικών στοιχείων, εργαλεία οπτικοποίησης, τεχνητή νοημοσύνη κ.α. προσφέροντας βαθύτερη ανάλυση και επεξεργασία των δεδομένων. Οι πληροφορίες που συλλέγονται αποτελούν χρήσιμα στοιχεία για τη λήψη κρίσιμων αποφάσεων.

Το cloud computing επωμίζεται όλη τη φόρτιση που προκαλείται από τη συμπίεση και την επεξεργασία των δεδομένων από τις συσκευές εντός ενός τεράστιου συμπλέγματος υπολογιστών στο διαδίκτυο. Το Διαδίκτυο γίνεται το cloud όπου τα δεδομένα, οι υπηρεσίες και οι εφαρμογές είναι διαθέσιμες από οποιαδήποτε συσκευή συνδεδεμένη στο διαδίκτυο, οπουδήποτε στον κόσμο.

Τέλος θα πρέπει να αναφέρουμε ότι το cloud computing δύναται να είναι δημόσιο ή

ιδιωτικό. Οι δημόσιες υπηρεσίες cloud παρέχουν τις υπηρεσίες τους μέσω Διαδικτύου έναντι χρέωσης. Οι ιδιωτικές υπηρεσίες cloud παρέχουν υπηρεσίες μόνο σε συγκεκριμένο αριθμό ατόμων. Υπάρχει επίσης η δυνατότητα επιλογής ενός υβριδικού μοντέλου που συνδυάζει στοιχεία τόσο των δημόσιων όσο και των ιδιωτικών υπηρεσιών.



Εικόνα: 2.9: Φάσεις και αντίστοιχες τεχνολογίες IoT

(Πηγή: Arshad et al., 2018)

Η ανάπτυξη της τεχνολογίας IOT όπως είπαμε και παραπάνω είναι βασισμένη στην υπηρεσία SOA (Service Oriented Architecture), η οποία προτάθηκε ως ιδέα το 1996 από την Gartner Group, μια κορυφαία εταιρεία έρευνας και συμβουλευτικής.

Η εν λόγω αρχιτεκτονική αποσκοπεί στην δημιουργία λογισμικών παροχής υπηρεσιών τα οποία να είναι διαθέσιμα στα δίκτυα.

Η αρχιτεκτονική SOA παρουσιάζει ένα ιδιαίτερα χρήσιμο πλεονέκτημα, αυτό της δυνατότητας επαναχρησιμοποίησης μιας υπηρεσίας. Οι χρήστες δύνανται να επαναχρησιμοποιήσουν εφαρμογές που αναφέρονται σε ετερογενείς τεχνολογίες.

Η λειτουργία αυτή υποστηρίζεται κυρίως από την WSDL -Web Services Description Language.

Πιο συγκεκριμένα, οι πάροχοι υποχρεούνται να παρέχουν απρόσκοπτα κάθε σχετική λεπτομέρεια και πληροφορία αναφορικά με τις παρεχόμενες υπηρεσίες προκειμένου οι χρήστες έχοντας λάβει γνώση αυτών να μπορούν τις χρησιμοποιήσουν με βέλτιστο

τρόπο.

Αντιστοίχως οι χρήστες, οφείλουν να ξέρουν που και πως μπορούν να βρουν τις διαθέσιμες υπηρεσίες προκειμένου να τις προσαρμόσουν στις ανάγκες τους. Για την ορθή λειτουργία των παραπάνω έχει τεθεί το σχετικό πλαίσιο ως προς τις διαδικασίες δημοσίευσης, δέσμευσης και εύρεσης μιας υπηρεσίας, βάσει συγκεκριμένων προτύπων που θα δούμε στην συνέχεια. Παράλληλα με την τεχνολογία IOT, υπάρχει ενδιαφέρον για την ανάπτυξη και την ανάλυση των Κοινωνικών Δικτύων και του Cloud Computing (Alabdulatif et al., 2018).

Τα βασικά χαρακτηριστικά του Cloud Computing είναι (Mell & Grance, 2011):

- Υπηρεσίες κατ' απαίτηση (Services on demand)
- Ευρεία δικτυακή πρόσβαση
- Διαχείριση, εξοικονόμηση πόρων
- Αποκλειστική αποθήκευση
- Ελαστικό και εύχρηστο
- Υπηρεσία βελτιστοποίησης του συστήματος

Το NIST (National Institute of Standards and Tecnology) ορίζει τρία μοντέλα υπηρεσιών του Cloud (Mell & Grance, 2011):

i. **SaaS** - Λογισμικό ως υπηρεσία (Software as a Service).

Αναφέρεται στη δυνατότητα να χρησιμοποιούνται εφαρμογές που προσφέρει ο πάροχος και εκτελούνται σε μια υποδομή του υπολογιστικού νέφους. Οι εν λόγω εφαρμογές είναι προσβάσιμες από διάφορες συσκευές των χρηστών μέσω μιας απλής διεπαφής χρήστη.

ii. ***PaaS*** *- Πλατφόρμα ως υπηρεσία (Platform as a Service).*

Αναφέρεται στη δυνατότητα του χρήστη να αναπτύσσει πάνω στη δομή του υπολογιστικού νέφους εφαρμογές που κατασκευάστηκαν από τον ίδιο με χρήση εργαλείων που υποστηρίζονται από τον πάροχο.

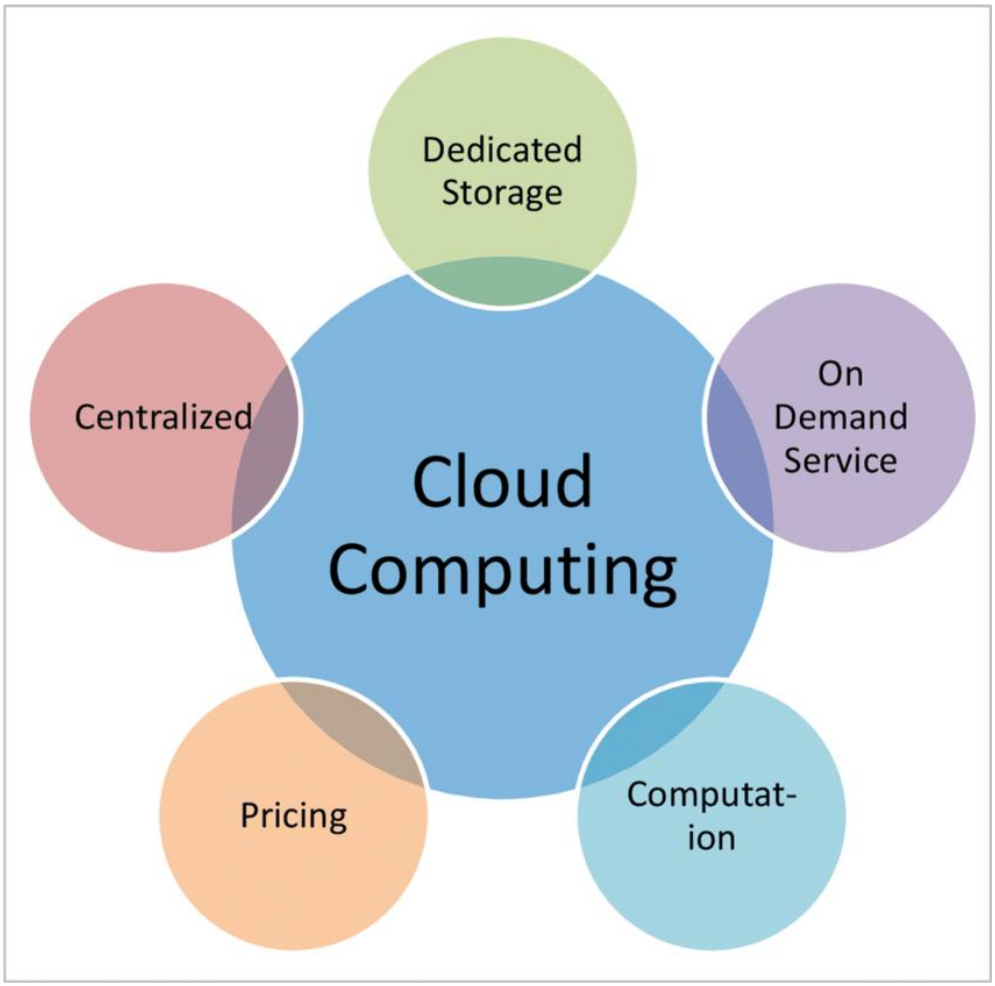
iii. ***IaaS*** *- Υποδομή ως υπηρεσία (Infrastructure as a Service).*

Επιτρέπει τη δέσμευση επεξεργαστικής ισχύος, αποθηκευτικού χώρου, δικτύων και άλλων υπολογιστικών πόρων. Παράλληλα, επιτρέπει στον χρήστη να αναπτύξει και να

εκτελέσει δικό του λογισμικό π.χ λειτουργικά συστήματα και εφαρμογές.

Το κύρια μοντέλα ανάπτυξης ενός Cloud είναι τα κάτωθι (Mell & Grance, 2011; Naeem et al., 2019):

- Ιδιωτικό cloud (Private cloud)
- Δημόσιο cloud (Public cloud)
- Cloud κοινότητας (Community cloud)
- Υβριδικό cloud (Hybrid cloud)



Εικόνα: 2.10: Βασικά χαρακτηριστικά του Cloud Computing

(Πηγή: Naeem et al., 2019)

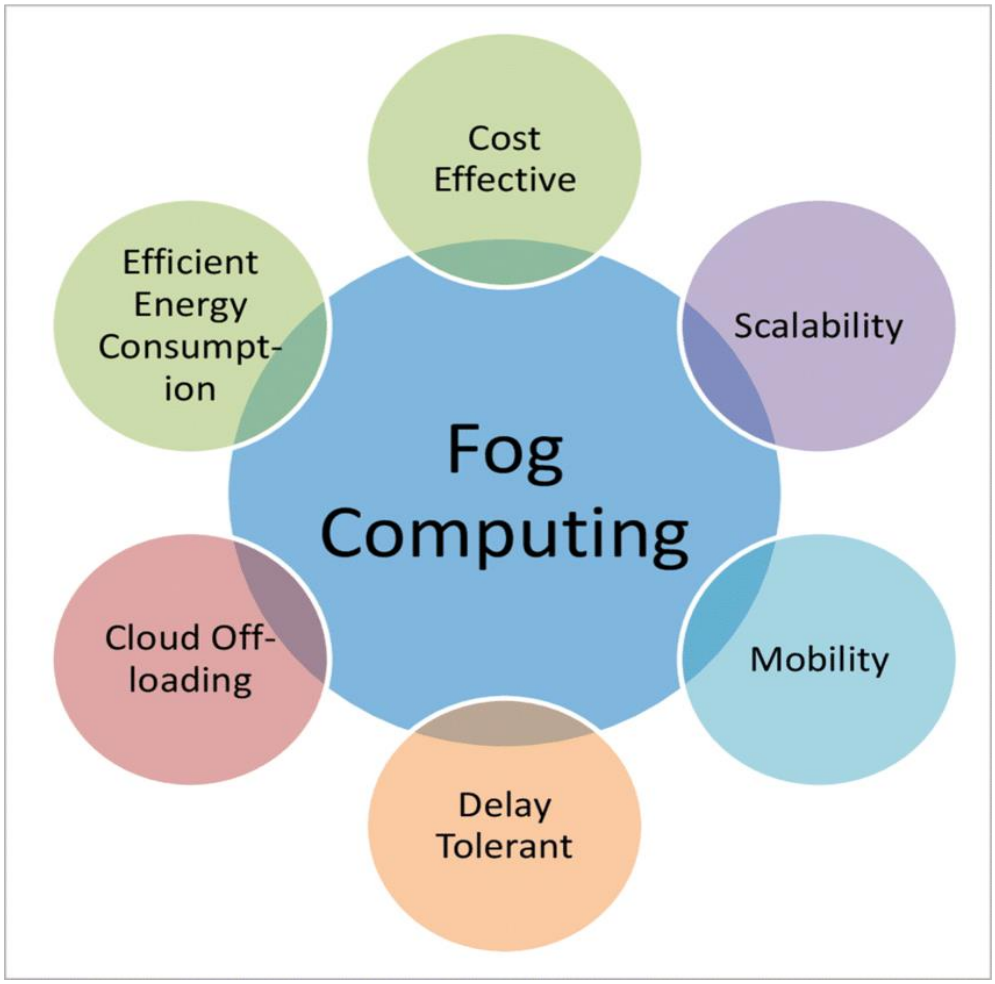
2.8 Χαρακτηριστικά του Fog Computing

Τα βασικά χαρακτηριστικά του Fog computing είναι τα εξής (Naeem et al., 2019; Iorga et al., 2018):

- Επεκτασιμότητα
- Αποδοτικότητα - υψηλοί ρυθμοί μετάδοσης των δεδομένων
- Μεγάλο πλήθος απαιτούμενων κόμβων
- Κινητικότητα (mobility)
- Real time αλληλεπίδραση με Cloud
- Μικρή καθυστέρηση
- Δυνατότητα ενσύρματης/ασύρματης πρόσβασης
- Ετερογένεια, διαλειτουργικότητα, συμβατότητα

Το κύρια μοντέλα ανάπτυξης Fog Computing είναι τα ακόλουθα (Naeem et al., 2019):

a) SaaS - Λογισμικό ως υπηρεσία (Software as a Service)
b) PaaS - Πλατφόρμα ως υπηρεσία (Platfom as a Service)
c) IaaS - Υπηρεσία ως υποδομή (Infrastructure as a Service)
d) Ιδιωτικός κόμβος fog (Private fog node)
e) Κόμβος Fog κοινότητας (Community fog node)
f) Δημόσιος κόμβος Fog (Public fog node)
g) Υβριδικός κόμβος Fog (Hybrid fog node)



Εικόνα: 2.11: Βασικά χαρακτηριστικά του Fog Computing

(Πηγή: Naeem et al., 2019)

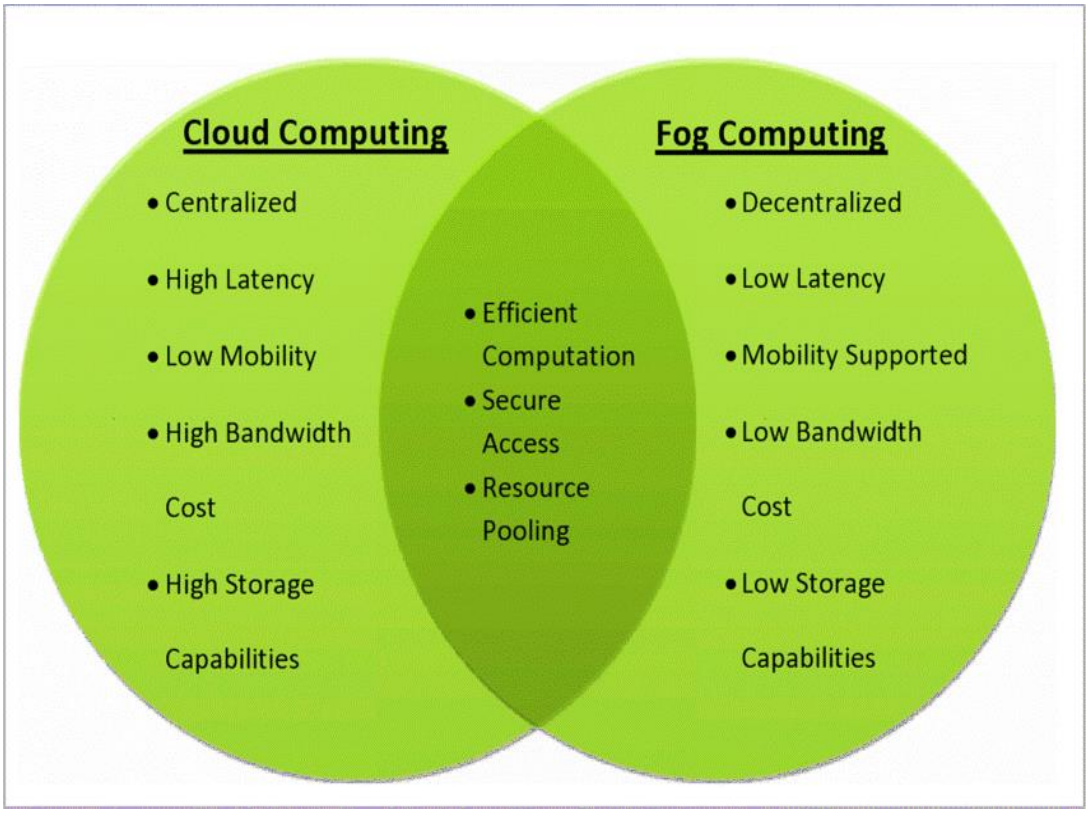
2.9 Σύγκριση μεταξύ Cloud και Fog Computing

Από την σύγκριση των τεχνολογιών Cloud Computing και Fog Computing προκύπτουν οι ακόλουθες διαφορές (Naeem et al., 2019):

1. Συγκεντρωτική κατανομή στο Cloud Computing – Κατανεμημένη στο Fog Computing.
2. Υψηλή καθυστέρηση στο Cloud Computing - χαμηλή στο Fog Computing.
3. Μικρή υποστήριξη της κινητικότητας στο Cloud Computing - μεγάλη στο Fog Computing.
4. Μικρό κόστος εύρους ζώνης στο Cloud Computing - μεγάλο στο Fog Computing.
5. Υψηλές δυνατότητες αποθήκευσης στο Cloud - περιορισμένες στο Fog Computing.

Επίσης υφίστανται οι εξής ομοιότητες (Naeem et al., 2019):

1. Αποτελεσματικός υπολογισμός
2. Ασφαλής πρόσβαση
3. Συγκέντρωση πόρων



Εικόνα 2.12: Σύγκριση Cloud και Fog Computing

(Πηγή: Naeem et al., 2019)

Γενικότερα σε εφαρμογές που απαιτούνται υψηλοί ρυθμοί μετάδοσης με χαμηλή καθυστέρηση και υψηλό QOS (Quality Of Service) η επεξεργασία θα πρέπει να πραγματοποιείται όσο το δυνατόν πλησιέστερα στους τελικούς χρήστες. Καθώς τα κέντρα δεδομένων που διαθέτει το Cloud βρίσκονται εντός του διαδικτύου, η διαχείριση των παραπάνω είναι δύσκολή. Ως αντιστάθμιση μπορεί να χρησιμοποιηθεί η τεχνολογία Fog Computing η οποία υπερτερεί ως προς την ισχύ, το εύρος ζώνης (Bandwidth) και άλλες παραμέτρους, όπως η ασφάλεια από επιθέσεις. Καθώς το μέγεθος της διαδρομής

που διανύουν τα δεδομένα τα καθιστά ευάλωτα σε επιθέσεις, είναι προτιμότερη η επιλογή μικρότερων διαδρομών των δεδομένων από τους clients στους servers. Το Fog computing έχει την ικανότητα αναγνώρισης της ελάχιστης διαδρομής δεδομένων για αυτό και υπερτερεί έναντι του Cloud computing.

Επίσης, οι κόμβοι Fog, είναι κατανεμημένοι προς τα άκρα των δικτύων των χρηστών με αποτέλεσμα κάθε επίδοξος hacker να πρέπει να διαθέσει εκτεταμένους πόρους για να εξαπολύσει μια επίθεση γεγονός που δρα αποτρεπτικά για κάτι τέτοιο (Firdhous et al., 2014).

Τέλος, αξίζει να σημειωθεί ότι υπάρχουν περιπτώσεις στις οποίες είναι περισσότερο δόκιμη η χρήση του Cloud computing όπως για παράδειγμα η υψηλής ποιότητας εργασίες batch processing οι οποίες απαιτούν μεγάλη ποσότητα πόρων. Εν κατακλείδι συνάγεται το συμπέρασμα ότι οι δύο τεχνολογίες θα συνυπάρχουν καθώς κατά περίπτωση, εξυπηρετούν διαφορετικές ανάγκες και απαιτήσεις των χρηστών.

2.10 Ενοποίηση IOT με Cloud και οφέλη

Όπως αναφέρθηκε στο 1ο Κεφάλαιο, η τεχνολογία IOT διαθέτει συσκευές κατανεμημένες σε μεγάλη κλίμακα. Ωστόσο οι συσκευές αυτές, διαθέτουν μικρό χώρο αποθήκευσης και μικρές επεξεργαστικές δυνατότητες. Παράλληλα δε, αντιμετωπίζουν προβλήματα που αφορούν στην απόδοση, την αξιοπιστία, την ιδιωτικότητα και την ασφάλεια.

Στα ως άνω τεχνικά ζητήματα το Cloud μπορεί να διαδραματίσει σημαντικό ρόλο καθώς αποτελείται από ένα τεράστιο δίκτυο εξαιρετικά μεγάλων δυνατοτήτων αποθήκευσης δεδομένων, μεγάλης υπολογιστικής ισχύος. Κατ' αυτόν τον τρόπο παρέχεται ένα ισχυρό και αρκετά ευέλικτο περιβάλλον στους χρήστες. Το περιβάλλον αυτό προωθεί την ενσωμάτωση των δεδομένων από πολλές πηγές.

Έτσι, ο συνδυασμός και εν τέλει η ενοποίηση των τεχνολογιών IOT και Cloud, συνθέτει μια πλατφόρμα η οποία προωθεί τη χρήση εφαρμογών, την ανταλλαγή πληροφοριών και τη βέλτιστη αξιοποίηση των υποδομών με αποδοτικό τρόπο. Πρακτικά οι δύο τεχνολογίες αλληλοσυμπληρώνονται ανάλογα με τα χαρακτηριστικά τους και τις αντίστοιχες απαιτήσεις.

Τα σημαντικότερα πλεονεκτήματα που προκύπτουν από την ενοποίηση των δύο τεχνολογιών αφορούν κυρίως στα ακόλουθα χαρακτηριστικά (Salesforce UK, 2020):

1. Επικοινωνία εφαρμογών και ανταλλαγή δεδομένων
2. Χώρος αποθήκευσης
3. Υψηλές επεξεργαστικές δυνατότητες
4. Νέες δυνατότητες & μοντέλα

Η ανάπτυξη του δικτύου πέμπτης γενιάς, το Cloud computing, το Fog computing και φυσικά το IOT. Χωρίς την ύπαρξη του 5G θα ήταν αδύνατη η υλοποίηση των εφαρμογών αυτών, δεδομένου ότι απαιτούνται τεράστιες ταχύτητες.

2.11 Απαιτήσεις Ασφάλειας IOT

Τα ζητήματα ασφάλειας στην τεχνολογία IOT σχετίζονται με ορισμένους μηχανισμούς ελέγχου της ταυτότητας, και της εμπιστευτικότητας των δεδομένων. Η ασφάλεια των πληροφοριών και του δικτύου είναι συνυφασμένη εν γένει με έννοιες της αυθεντικοποίησης, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Όπως περιγράψαμε παραπάνω το IoT βρίσκει εφαρμογή σε κρίσιμους τομείς της εθνικής οικονομίας, όπως στις υγειονομικές υπηρεσίες, στις ευφυείς μεταφορές, στη βιομηχανία κ.α. Ως εκ τούτου οπότε οι απαιτήσεις ασφάλειας στο διαδίκτυο είναι υψηλότερες όσον αφορά τη διαθεσιμότητα και την αξιοπιστία. Το λεγόμενο τρίπτυχο CIA , όπως συνηθίζεται να λέγεται, εμπιστευτικότητα – ακεραιότητα – διαθεσιμότητα (Confidentiality - Integrity - Availability), αποτελεί πρότυπο που καθοδηγεί πολιτικές για την ασφάλεια των πληροφοριών. Το μοντέλο αυτό μπορεί επίσης να αναφέρεται ως τριάδα AIC (διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα). Τα τρία στοιχεία της τριάδας θεωρούνται κρίσιμα για την ασφάλεια και απασχολούν τους ειδικούς της επιστήμης των υπολογιστών. Γενικά, η εμπιστευτικότητα είναι ένα σύνολο κανόνων που παρέχουν πρόσβαση στις πληροφορίες μόνο σε εξουσιοδοτημένα άτομα. Η ακεραιότητα εξασφαλίζει ότι οι πληροφορίες είναι αξιόπιστες, ακριβείς και χωρίς να έχουν παραποιηθεί. Τέλος η διαθεσιμότητα αποτελεί εγγύηση για αξιόπιστη πρόσβαση των εξουσιοδοτημένων ατόμων στις πληροφορίες (Burhan et al., 2018).

2.11.1 Εμπιστευτικότητα των δεδομένων

Ο όρος της εμπιστευτικότητας των δεδομένων αναφέρεται στην προστασία του απορρήτου ευαίσθητων πληροφοριών. Η εμπιστευτικότητα επιτυγχάνεται με χρήση μηχανισμών που εμποδίζουν τη μη εξουσιοδοτημένη πρόσβαση ή παραβίαση καθώς τα δεδομένα που συλλέγονται από τους αισθητήρες και τους κόμβους δεν θα πρέπει να μεταδίδονται σε μη εξουσιοδοτημένες οντότητες. Τέτοιοι μηχανισμοί είναι η κρυπτογράφηση των δεδομένων και η επαλήθευση δύο δοκιμών με την οποία οι χρήστες αποκτούν πρόσβαση στα δεδομένα, κατόπιν δύο εξαρτημένων δοκιμών ελέγχου της ταυτότητας (Burhan et al., 2018).

2.11.2 Ακεραιότητα δεδομένων

Με την ακεραιότητα των δεδομένων προστατεύονται οι χρήσιμες πληροφορίες και αποτρέπεται η απόπειρα κλοπής τους από hackers. Υφίστανται διάφορες περιπτώσεις επιθέσεων, οι οποίες θα περιγραφούν αναλυτικά παρακάτω. Η πιο διαδεδομένη μέθοδος για την εξασφάλιση της ακεραιότητας των δεδομένων είναι ο λεγόμενος έλεγχος του κυκλικού πλεονασμού (CRC). Με τον έλεγχο αυτό, παρέχεται η δυνατότητα ανίχνευσης σφαλμάτων με την προσθήκη μιας τιμής σταθερού μήκους. Έτσι η ακεραιότητα των δεδομένων δύναται να διασφαλιστεί με την παρακολούθηση της τιμής αυτής η οποία καλείται τιμή ελέγχου.

Μια άλλη μέθοδος για την εξασφάλιση της ακεραιότητας των δεδομένων είναι ο έλεγχος έκδοσης. Με την μέθοδο αυτή δημιουργούνται συγχρονισμένα αντίγραφα ασφαλείας των δεδομένων. Έτσι διατηρούνται όλες οι μεταβολές των αρχείων στο σύστημα IOT και διασφαλίζεται η ακεραιότητα των δεδομένων σε πιθανό ενδεχόμενο διαγραφής ή απώλειάς τους (Burhan et al., 2018; Miorandi et al., 2012).

2.11.3 Διαθεσιμότητα δεδομένων

Η διαθεσιμότητα των δεδομένων συνδέεται με την ασφάλεια του διαδικτύου. Πρακτικά εξασφαλίζει την πρόσβαση των χρηστών σε όλες της πηγές της πληροφόρησης υπό φυσιολογικές, αλλά και μη φυσιολογικές συνθήκες (π.χ. σε φυσικές καταστροφές).

Ο όρος της διαθεσιμότητας των δεδομένων αναφέρεται επίσης στη συνεχή και

απρόσκοπτη ροή των πληροφοριών. Για την επίτευξη αυτής, χρησιμοποιούνται τεχνικές εφεδρείας (backup) και πλεονασμού (redundancy). Η αντιγραφή σημαντικών πληροφοριών εξασφαλίζει ότι σε ενδεχόμενη βλάβη του συστήματος δεν θα προκύψει απώλεια δεδομένων (Burhan et al., 2018).

2.12 Τύποι επιθέσεων και ασφάλεια στα συστήματα 5G

- Επιθέσεις από hackers

Ο όρος Hackers αναφέρεται στα φυσικά πρόσωπα που δρουν κατά μόνας ή κατά ομάδες με σκοπό την εισβολή σε υπολογιστικά συστήματα για διάφορες σκοπιμότητες. Είναι άτομα που διαθέτουν γνώσεις υψηλού επιπέδου προγραμματισμού συνήθως προγραμματιστές και σχεδιαστές συστημάτων. Εντούτοις έχουν καταγραφεί επιθέσεις από άτομα που ασχολούνται ερασιτεχνικά με το αντικείμενο αυτό έχοντας αποκτήσει ιδιαίτερες δεξιότητες κυρίως με εμπειρικό τρόπο. Οι hackers δύνανται να δρουν είτε σε ομάδες, τα λεγόμενα hacking-groups, είτε κατά μόνας. Οι δράσεις και οι τρόποι που απεργάζονται είναι κατά κύριο λόγο κακόβουλες και στην περίπτωση αυτή ονομάζονται crackers ή black hats. Ο όρος crackers χρησιμοποιείτε για να δηλώσει τα πρόσωπα που αποκτούν αυθαίρετη - μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα με σκοπό να προξενήσουν φθορές ή να υποκλέψουν πληροφορίες.

Ανάλογα με τις σκοπιμότητες και τις αρχές που διέπουν τις ομάδες των hackers έχουν επικρατήσει διάφοροι όροι όπως black , white ή gray hats.Ο όρος black hats αναφέρεται στα άτομα που διακρίνονται για την υψηλή τους τεχνογνωσία στο πεδίο των υπολογιστικών συστημάτων και εισβάλλουν σε αυτά με κακόβουλες προθέσεις προξενώντας μεγάλες φθορές.

Το 1960, σπουδαστές του MIT ανέπτυξαν δεξιότητες για τη δημιουργία προγραμμάτων με σκοπό την εκτέλεση μαθηματικών υπολογισμών σε σύντομο χρόνο και την αύξηση της ταχύτητας των υπολογιστών. Το πρώτο hack με όλα τα ανωτέρω χαρακτηριστικά ήταν το γνωστό λειτουργικό σύστημα με την ονομασία UNIX.

Καθώς με την πάροδο του χρόνου άρχισαν να πληθαίνουν οι hackers και να αυξάνεται η συχνότητα και η πυκνότητα οργανωμένων επιθέσεων στα υπολογιστικά συστήματα, δημιουργήθηκε επιτακτικά η ανάγκη δημιουργίας θεσμοθετημένου νομικού πλαισίου για

την αντιμετώπιση και τον περιορισμό φαινομένων απάτης και δολιοφθορών σε προγράμματα υπολογιστικών συστημάτων.

Η αλματώδης ανάπτυξη της τεχνολογίας τις τελευταίες δεκαετίες και η εκτεταμένη χρήση των υπολογιστών και του διαδικτύου στο σύνολο του πληθυσμού, των δημόσιων υπηρεσιών και των ιδιωτικών εταιρειών απαιτεί περισσότερο από ποτέ τη νομική θωράκιση και προστασία έναντι των hackers.

Οι τρόποι δράσης των hackers ποικίλουν ανάλογα το στόχο και την σκοπιμότητα εντούτοις ακολουθούν συνήθως τα ίδια βήματα για να υλοποιήσουν μια επίθεση. Πρωτίστως επικεντρώνονται στη διερεύνηση και στη συλλογή των κατάλληλων πληροφοριών σχετικά με το στόχο που θέλουν να προσβάλουν καθώς και το σύστημα που θέλουν να πλήξουν. Στο στάδιο αυτό οι hackers, επιδιώκουν την απόκτηση κωδικών εισόδου προκειμένου να αποκτήσουν πρόσβαση νόμιμου χρήστη στο σύστημα. Στη συνέχεια ακολουθεί η κύρια φάση δράσης εκτελώντας κατάλληλες ενέργειες ανάλογα με τους στόχους της επίθεσης. Όταν ολοκληρωθεί η επίθεση αποχωρούν σβήνοντας τα ίχνη τους από το σύστημα ώστε να αποκρύψουν την ταυτότητά τους. Ωστόσο έχοντας ανακτήσει τους κωδικούς πρόσβασης κατέχουν τα δικαιώματα του χρήστη και μπορούν να εισέρχονται στο σύστημα οποιαδήποτε στιγμή.

Αξίζει να σημειωθεί ότι η συλλογή δεδομένων είναι καίριας σημασίας στο hacking. Δεδομένα υψηλής χρησιμότητας, εμπιστευτικά αρχεία, κρατικές πληροφορίες, ευαίσθητα προσωπικά δεδομένα κ.α. είναι δυνατόν να υποκλαπούν, να αλλοιωθούν, να καταστραφούν ακόμα και να διαβιβαστούν σε τρίτα μέρη.

Ειδική περίπτωση αποτελούν οι λεγόμενοι white hats hackers, οι οποίοι προβάλλουν ως ιδεολογία την ελεύθερη πρόσβαση ως ένα είδος ιδιότυπου δικαιώματος μάθησης και απόκτησης δεξιοτήτων στον τομέα της πληροφορικής. Είθισται επίσης να προβαίνουν σε επιθέσεις παντός τύπου ως ένδειξη διαμαρτυρίας έναντι σε πολιτικές δράσεις και κρατικούς μηχανισμούς.

Στον αντίποδα, οι black hats hackers ή crackers, δρουν αποκλειστικά με ιδιοτελείς σκοπούς κυρίως για λόγους οικονομικού κέρδους υφαρπάζοντας προσωπικά δεδομένα και επιχειρώντας να καταστρέψουν το σύστημα στο οποίο εισέβαλαν (1ο ΓΕΛ Αγ. Αναργύρων, 2014).

Όπως προαναφέραμε τα κίνητρα των επιθέσεων ποικίλουν ωστόσο μπορούμε να τα

ταξινομήσουμε ως ακολούθως (1ο ΓΕΛ Αγ. Αναργύρων, 2014):

- Διανοητικές προκλήσεις. Εκπορεύονται από την ανάγκη αναγνώρισης των προσώπων αυτών ως αυθεντίες ανώτερων δυνατοτήτων.

- Ανάγκη για προσωπική προβολή, θαυμασμό και κοινωνική αποδοχή.

- Λόγοι προσωπικής αντιδικίας/εκδίκησης.

- Λόγοι ανταγωνισμού σε επιχειρηματικό – οικονομικό επίπεδο.

Επίσης κίνητρα τεχνικής σημασίας όπως είναι (1ο ΓΕΛ Αγ. Αναργύρων, 2014):

- επιθέσεις άρνησης εξυπηρέτησης

- απόκρυψη ταυτότητας

- απόκτηση δικαιωμάτων διαχειριστή στο IRC

- απόκτηση δικαιωμάτων δημοσίευσης και προβολής

Τέλος, για την προστασία κάθε υπολογιστικού συστήματος από κακόβουλα λογισμικά είναι αναγκαία η εγκατάσταση ενός προγραμμάτων antivirus και firewall τα οποία οφείλουν να υπόκεινται σε τακτικές ενημερώσεις για νέους ιούς και κακόβουλες δράσεις.

- Επιθέσεις Dos και DDos

Στα έξυπνα δίκτυα έχει παρατηρηθεί ότι οι συνηθέστερες απειλές προέρχονται από επιθέσεις άρνησης υπηρεσίας κοινώς γνωστές ως επιθέσεις DoS. Στις αρχές της δεκαετίας του 90 καταγράφηκαν οι πρώτες επιθέσεις DoS λόγω των κενών και των αδυναμιών που εμφάνιζαν τα τότε λογισμικά συστήματα και με σκοπό να τεθούν εκτός λειτουργίας οι εξυπηρετητές και οι υπηρεσίες των δικτύων.

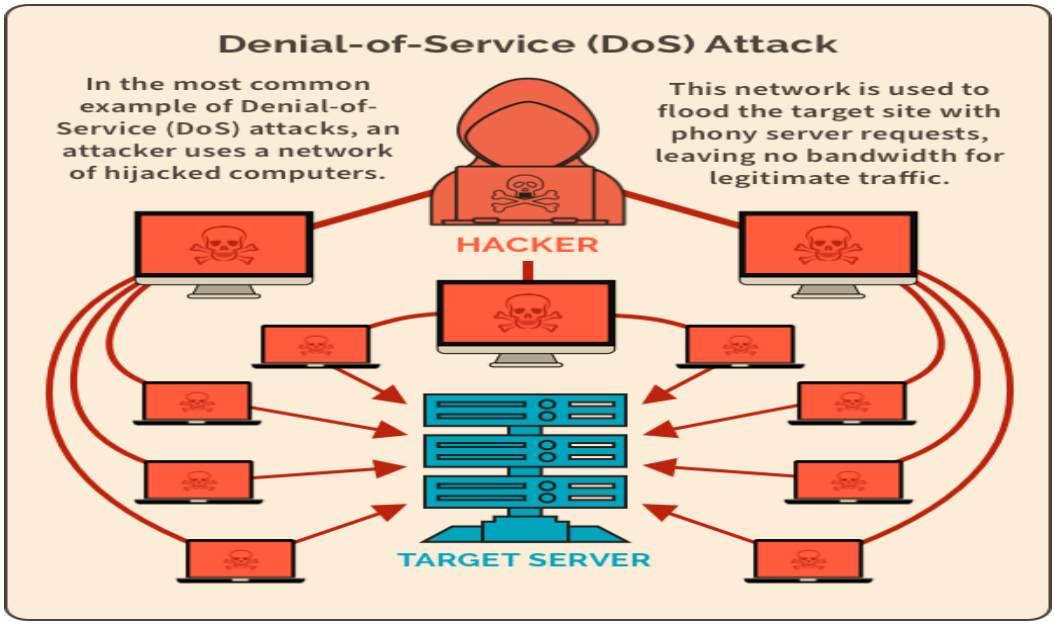
Με την πάροδο των χρόνων οι επιθέσεις DOS έχουν εξελιχθεί σημαντικά με αποτέλεσμα πολλές εταιρείες, δημόσιες υπηρεσίες και οργανισμοί να τίθενται διαρκώς στο στόχαστρο αυτού του είδους των επιθέσεων.

Η βασική επιδίωξη στις επιθέσεις DoS, είναι η διακοπή των υπηρεσιών μέσω του περιορισμού πρόσβασης σε μία συσκευή ή μία υπηρεσία χωρίς ωστόσο να αλλοιώνονται ή να καταστρέφονται τα χαρακτηριστικά των υπηρεσιών.

Παρά την απλότητα που διακρίνει τις επιθέσεις αυτές μέσω δηλαδή κατακλυσμικής ροής αποστολής πακέτων στο δίκτυο οι δυσλειτουργίες που προκαλούνται είναι μεγάλες

καθώς τα πακέτα καταλαμβάνουν μεγάλο μέρος της διαθέσιμης χωρητικότητας. Μια επίθεση άρνησης υπηρεσίας (DoS) έχει πρακτικά ως αποτέλεσμα οι νόμιμοι χρήστες να μην μπορούν να έχουν πρόσβαση στο δίκτυο που χρησιμοποιούν, καθώς και σε ιστότοπους, μηνύματα ηλεκτρονικού ταχυδρομείου και άλλες υπηρεσίες που βασίζονται στο δίκτυο. Η επίθεση εκτοξεύεται χρησιμοποιώντας έναν μόνο υπολογιστή, συνήθως πλημμυρίζοντας το δίκτυο με κίνηση, έως ότου το δίκτυο να μην μπορεί να ανταποκριθεί. Ωστόσο στις εν λόγω επιθέσεις δεν παρατηρούνται αλλοιώσεις στα δεδομένα.

Οι επιθέσεις DoS δύσκολα μπορούν να ανιχνευθούν και γι' αυτό κρίνονται ιδιαιτέρως επικίνδυνες καθώς οι ροές των πακέτων έχουν ανομοιογενή χαρακτηριστικά σε σχέση με τα νόμιμα πακέτα.



Εικόνα 2.13: Επίθεση DoS

(Πηγή: Oza, 2020)

Οι hackers που εξαπολύουν επιθέσεις DoS χρησιμοποιούν παραποιημένες διευθύνσεις IP για να καλύπτουν την ταυτότητά τους.

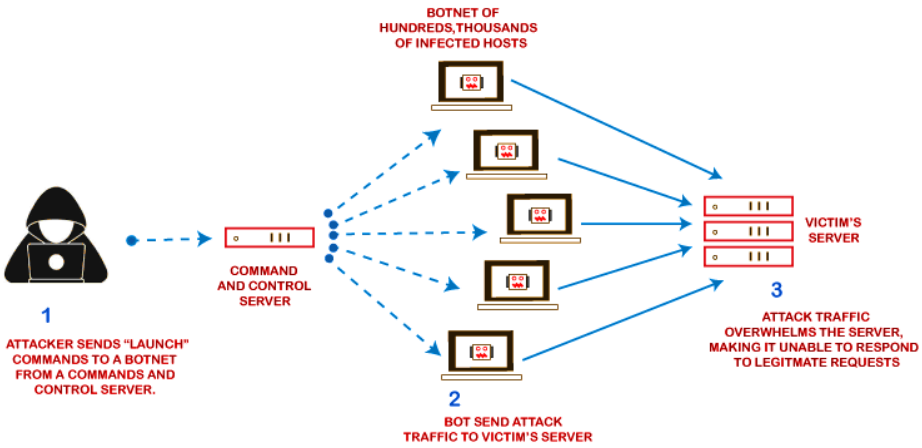
Τα συμπτώματα από μια επίθεση άρνησης υπηρεσίας περιλαμβάνουν:

- Αδυναμία πρόσβασης των χρηστών στον ιστότοπο

- Αργή απόδοση του δικτύου
- Αποτυχία φόρτωσης σελίδων ιστότοπου
- Απώλεια συνδεσιμότητας μεταξύ συσκευών στο ίδιο δίκτυο

Παράλληλα με τις επιθέσεις DoS συπάρχουν και οι DDoS κατανεμημένες επιθέσεις άρνησης υπηρεσίας (Distributed Denial of Service Attacks). Μια επίθεση DDoS χρησιμοποιεί πολλά συστήματα για να επιτεθεί σε μια υπηρεσία Cloud. Σε μια επίθεση DDoS, ο εισβολέας αναλαμβάνει τον έλεγχο πολλών συστημάτων θυμάτων, γνωστά ως ζόμπι ή σκλάβοι, διαδίδοντας διαφορετικά είδη κακόβουλου λογισμικού. Το σύνολο των σκλάβων είναι γνωστό ως botnet. Με τον τρόπο αυτό ο εισβολέας μπορεί να καταργήσει μια υπηρεσία cloud διατάζοντας τους σκλάβους στο botnet να στείλουν ψεύτικη κίνηση που κατασκευάζει δεδομένα ή εφαρμογές ή άλλους πόρους στο cloud που δεν είναι διαθέσιμοι σε νόμιμους χρήστες. Οι εν λόγω επιθέσεις έχουν τη δυνατότητα να εξαντλήσουν τους υπολογιστικούς και επικοινωνιακούς πόρους των θυμάτων σε σύντομο χρονικό διάστημα. Μια επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS) επιχειρεί να καταστήσει μη διαθέσιμη μια διαδικτυακή υπηρεσία ή έναν ιστότοπο υπερφορτώνοντάς την με τεράστιες πλημμύρες κίνησης στο Διαδίκτυο που δημιουργούνται από πολλές πηγές. Χρησιμοποιώντας την τεχνολογία client/server, οι hackers ενισχύουν σημαντικά την αποτελεσματικότητα των επιθέσεων DoS θέτοντας υπό τον έλεγχό τους, τους πόρους πολλαπλών υπολογιστών οι οποίοι πρακτικά λειτουργούν ως πλατφόρμες επίθεσης. Η κατανεμημένη κίνηση που προκύπτει είναι δύσκολα διαχειρίσιμη και έχει ως αποτέλεσμα την πλήρη απόφραξη μιας υπηρεσίας (Suryateja, 2018).

Στη Εικόνα 2.14 απεικονίζεται ο τρόπος με τον οποίο επιτυγχάνεται μία DDoS επίθεση. Σε μία τέτοια επίθεση ο hacker παραβιάζει έναν πλήθος κόμβων ''τρέχοντας'' ένα ειδικό πρόγραμμα. Χρησιμοποιεί δίκτυα μηχανημάτων συνδεδεμένων στο Διαδίκτυο. Τα δίκτυα αυτά αποτελούνται από υπολογιστές και άλλες συσκευές, όπως συσκευές IoT που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται εξ αποστάσεως από τον εισβολέα. Αυτές οι μεμονωμένες συσκευές αναφέρονται ως bot ή ζόμπι και ένα σύνολο αυτών ονομάζεται botnet.



Εικόνα 2.14: Επίθεση DDoS

(Πηγή: https://www.javatpoint.com/what-is-ddos-attack)

Οι χειριστές και τα ζόμπι αποτελούν στην ουσία τον μηχανισμό των hackers για επιθέσεις DDoS καθώς μπορούν να πετύχουν στόχους μεγάλης εμβέλειας πλήττοντας ολόκληρα κέντρα δεδομένων πολλαπλών server.

Το γεγονός ότι ένα έξυπνο δίκτυο υπόκειται σε αυστηρό χρονικό πλαίσιο έχει να κάνει με την εξασφάλιση της αξιοπιστίας παρακολούθησης και ελέγχου των επιμέρους συσκευών που είναι εγκατεστημένες σε αυτό. Συμπερασματικά ότι οι επιθέσεις DoS και DDoS καθιστούν τα έξυπνα δίκτυα ευάλωτα (Lu et al., 2010).

- Επιθέσεις Man-in-the-middle

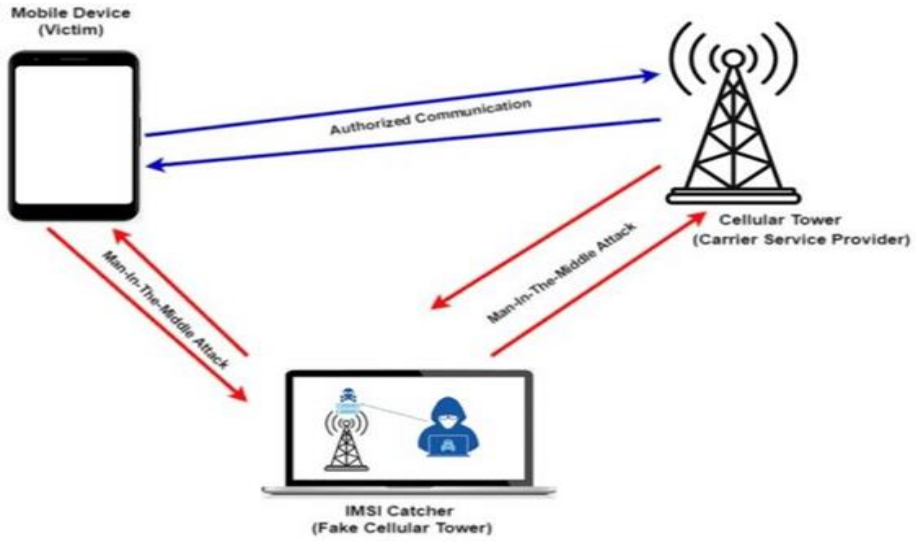
Το δίκτυο κινητής τηλεφωνίας επέφερε αναμφίβολα πολλά οφέλη ωστόσο παρουσιάζει πολλές προκλήσεις σε ζητήματα ασφάλειας. Η έλευση των προηγμένων δικτύων που λειτουργούν με μεταγωγή πακέτων και συνδέονται με εξωτερικά δίκτυα όπως το Διαδίκτυο, σε συνδυασμό με την ανάπτυξη της τεχνολογίας 5G καθιστούν το δίκτυο ευάλωτο σε διάφορους τύπους επιθέσεων, ανάμεσα στις οποίες η επίθεση Man-in-the-Middle.

Η επίθεση Man-in-the-Middle αποτελεί πραγματική απειλή για την ασφάλεια του ασύρματου δικτύου και ειδικότερα για το δίκτυο της κινητής τηλεφωνίας. Η διαδικασία κατά την οποία ένας εισβολέας παρεμβαίνει στις επικοινωνίες μεταξύ δύο μερών για να κλέψει διαπιστευτήρια σύνδεσης ή προσωπικές πληροφορίες, να κατασκοπεύσει το θύμα

ή να κλέψει συνεδρίες επικοινωνίας, ονομάζεται επίθεση Man-in-the-Middle όπως φαίνεται στην Εικόνα 2.15.

Στην επίθεση Man-in-the-middle, ο επιτιθέμενος αποτρέπει την επικοινωνία μεταξύ δύο μερών τα οποία κατέχουν τα νόμιμα δικαιώματα. Ουσιαστικά ο επιτιθέμενος καταλαμβάνει τον έλεγχο της ροής επικοινωνίας και αποκτά την ικανότητα να αποκομίζει πληροφορίες και να τις αλλοιώνει ανάλογα τους σκοπούς της επίθεσης (Kalalas et al., 2016).

Ο επιτιθέμενος προσποιούμενος το νόμιμο μέρος δύναται να καταλάβει τη θέση του σε μια επικοινωνία λαμβάνοντας τα μηνύματα του άλλου μέρους. Στην συνέχεια αλλοιώνει το περιεχόμενό τους στέλνοντας ψευδή μηνύματα και στους δύο παραλήπτες (Bakare & Ekolama, 2021).



Εικόνα 2.15: Επίθεση Man-in-The-Middle

(Πηγή: Bakare & Ekolama, 2021)

Για να κατανοήσουμε μία man-in-the-middle επίθεση σε περιβάλλον έξυπνου δικτύου ας υποθέσουμε ότι ο παραλήπτης είναι ο χειριστής στο κέντρο ελέγχου της εταιρίας ενέργειας. Από την άλλη πλευρά ο hacker στέλνει ψευδή δεδομένα, ώστε να τον αναγκάσει να εκτελέσει ενέργειες ή να τον αποπροσανατολίσει ως προς τη λειτουργία του δικτύου εξυπηρετώντας εν αγνοία του τον σκοπό της επίθεσης (Bakare & Ekolama, 2021).

- Επιθέσεις Eavesdropping

Οι επιθέσεις αυτές είναι επιθέσεις υποκλοπών γνωστές και ως sniffing ή snooping. Σε αυτές πραγματοποιείται υποκλοπή πληροφορίων καθώς μεταδίδονται μέσω του δικτύου από ένα υπολογιστή, ένα smartphone ή κάποια άλλη συνδεδεμένη συσκευή. Η επίθεση εκμεταλλεύεται κενά και αδυναμίες της ασφάλειας των επικοινωνιών του δικτύου για πρόσβαση σε δεδομένα που αποστέλλονται ή λαμβάνονται από τον χρήστη. Η επίθεση πραγματοποιείται με τη βοήθεια εργαλείων (sniffers) τα οποία ανιχνεύουν και συλλέγουν τα πακέτα που διακινούνται στο δίκτυο. Συχνά οι εισβολείς παρακολουθούν ευαίσθητες οικονομικές και εμπορικές πληροφορίες οι οποίες μπορούν να δοθούν σε τρίτους για απόκτηση οικονομικού οφέλους, λόγους ανταγωνισμού και εγκληματικές ενέργειες. Ο εντοπισμός μιας Eavesdropping επίθεσης συνιστά σύνθετη διαδικασία καθώς φαινομενικά οι μεταδόσεις του δικτύου λειτουργούν κανονικά.

Μια επίθεση υποκλοπής εκμεταλλεύεται μια εξασθενημένη σύνδεση ανάμεσα στον πελάτη και τον διακομιστή για να ανακατευθύνει την κίνηση του δικτύου. Ο εισβολέας εγκαθιστά λογισμικό παρακολούθησης δικτύου, το "sniffer", σε υπολογιστή ή διακομιστή για να παρακολουθεί τη μετάδοση των δεδομένων. Πρακτικά, το δίκτυο λαμβάνει πακέτα, τα οποία διαβιβάζονται μέσω υπολογιστών, και στην συνέχεια καθώς διαβάζεται το περιεχόμενό τους, ανιχνεύονται οι ευαίσθητες πληροφορίες.

Η διαφορά ανάμεσα στην επίθεση Evesdropping και την επίθεση Man in the middle είναι ότι στην πρώτη ο παραλήπτης λαμβάνει όλα τα μηνύματα που στέλνονται από τον αποστολέα ακέραια και χωρίς να έχουν υποστεί παραποίηση για αυτό είναι δύσκολο να γίνει αντιληπτή.

Στον αντίποδα στις επιθέσεις Man in the middle, ο εισβολέας προσποιούμενος τον τελικό παραλήπτη λαμβάνει όλα τα μηνύματα του αποστολέα έχοντας την δυνατότητα να τα αλλοιώσει (Ozhelvaci & Ma, 2020).

- Επιθέσεις Spoofing

Μία άλλη διαδικτυακή επίθεση είναι η spoofing η οποία υλοποιείται υπό διάφορες μορφές. Η πιο συνηθισμένη είναι η πλαστογράφηση μιας IP. Έτσι ο εισβολέας αποκρύπτει την πραγματική του ταυτότητα και εμφανίζεται ως κάποιος άλλος με σκοπό την πρόσβαση σε ένα σύστημα ώστε να περιοριστούν οι πόροι ή να υποκλαπούν δεδομένα.

Ο Spoofer στέλνει πακέτα (δεδομένα) με τυπικά νόμιμη IP σε συστήματα και στη συνέχεια πολλαπλοί διακομιστές πακέτων υποκινούν σφάλματα και επιθέσεις DoS.

Μία άλλη μορφή επίθεσης spoofing είναι η αποστολή παραπλανητικών email από τον hacker δημιουργώντας ψεύτικες ιστοσελίδες. Με αυτόν τον τρόπο μπορεί να κλέψει τα ονόματα και τους κωδικούς πρόσβασης των χρηστών κλπ. Επίσης συχνή είναι η δημιουργία ψεύτικου σημείου ασύρματης πρόσβασης εξαπατώντας τα θύματα σε παράνομη ασύρματη σύνδεση.

Η επίθεση spoofing στα έξυπνα ηλεκτρικά δίκτυα είναι ιδιαίτερα αποτελεσματική καθώς τα δεδομένα των τερματικών μονάδων, των αισθητήρων και των έξυπνων μετρητών μεταδίδονται στο κέντρο ελέγχου προς επεξεργασία. Όταν ο hacker παρέμβει σε μία συσκευή και αλλοιώσει τα δεδομένα που συλλέγονται και προέρχονται από αυτήν, δεν θα γίνει αντιληπτός από τον νόμιμο χρήστη ο οποίος θα θεωρεί εσφαλμένα ότι το δίκτυο λειτουργεί ορθά. Με τον τρόπο αυτό ο hacker θα μπορεί να συνεχίσει να στέλνει εντολές στις συσκευές ή στον ελεγκτή χωρίς ο χειριστής να μπορεί να επέμβει για να ανακόψει τις ενέργειες της επίθεσης (Li et al., 2021).

- Επιθέσεις σε δίκτυα 5G που περιέχουν αισθητήρες

Τα ασύρματα δίκτυα αισθητήρων είναι τρωτά απέναντι σε διάφορους τύπους επιθέσεων και θα όπως θα δούμε αναλυτικά παρακάτω. Είναι γνωστό ότι οι επιθέσεις δύνανται να λάβουν χώρα σε οποιοδήποτε επίπεδο του πρωτοκόλλου στρωμάτων.

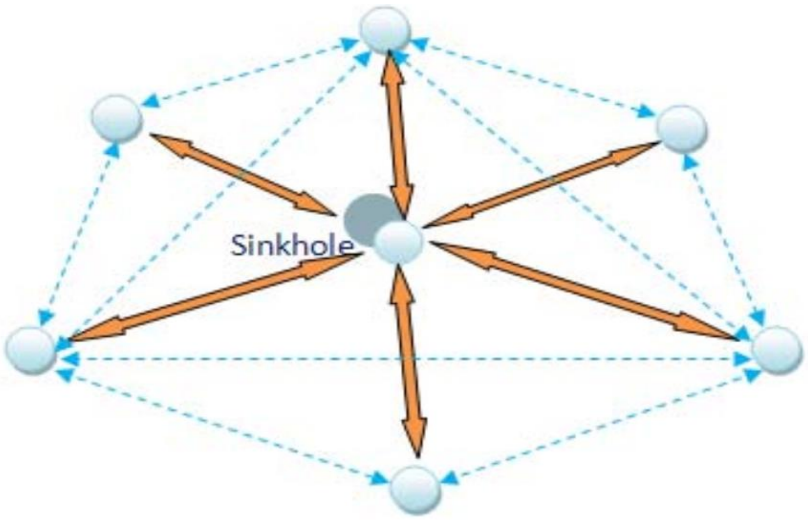
Κάθε επίπεδο στρώματος εκτελεί τις δικές του λειτουργίες ωστόσο υπάρχουν επιθέσεις που πλήττουν καθένα από αυτά ξεχωριστά και άλλες που είναι κοινές όπως οι επιθέσεις εξάντλησης πόρων και μεροληψίας. Η λειτουργία του φυσικού στρώματος είναι η μετάδοση ροών δεδομένων, η ανίχνευση σημάτων και η κρυπτογράφηση δεδομένων και συνήθως οι επιθέσεις που αντιμετωπίζει στοχεύουν στην παρεμβολή και την αλλοίωση των δεδομένων. Το στρώμα ζεύξης δεδομένων είναι υπεύθυνο για την πολυπλεξία των ροών δεδομένων, για την ανίχνευση πακέτων δεδομένων και για τη διασφάλιση συνδέσεων σημείου-σε-σημείο ή σημείου-σε-πολλαπλά-σημεία (Karlof & Wagner, 2003; Park et al., 2021).

- Επιθέσεις Sinkhole

Η επίθεση sinkhole αποτελεί μία από τις σοβαρές επιθέσεις στο ασύρματο ad hoc δίκτυο.

Κατά την επίθεση βύθισης ή καταβόθρας ο επιτιθέμενος επιχειρεί να κατευθύνει όλη την κίνηση μιας συγκεκριμένης περιοχής του δικτύου μέσα από έναν εκτεθειμένο, παραβιασμένο κόμβο, ανακτώντας τον πλήρη έλεγχο αυτής και καταλαμβάνοντας ολόκληρη την κίνηση του δικτύου. Στη συνέχεια τροποποιεί τις μυστικές πληροφορίες ή τις απορρίπτει για να κάνει το δίκτυο πολύπλοκο. Ένας κακόβουλος κόμβος προσπαθεί να προσελκύσει τα ασφαλή δεδομένα από όλους τους γειτονικούς κόμβους. Ο παραβιασμένος κόμβος επιλέγεται να είναι ελκυστικός στους γειτονικούς του κόμβους ως προς τον αλγόριθμο δρομολόγησης. Με τον τρόπο αυτό εξασφαλίζεται ότι οι υπόλοιποι κόμβοι θα χρησιμοποιήσουν τον παραβιασμένο κόμβο για να προωθούν τα πακέτα που υποτίθεται ότι φτάνουν στον σταθμό βάσης. Οι επιθέσεις Sinkhole επηρεάζουν την απόδοση των πρωτοκόλλων Ad hoc δικτύων, όπως το AODV, χρησιμοποιώντας ελαττώματα όπως μεγιστοποιώντας τον αριθμό ακολουθίας ή ελαχιστοποιώντας τον αριθμό hop. Με αυτόν τον τρόπο η διαδρομή που παρουσιάζεται μέσω του κακόβουλου κόμβου φαίνεται να είναι η καλύτερη διαθέσιμη διαδρομή για την επικοινωνία των κόμβων. Στο πρωτόκολλο DSR, η επίθεση με καταβόθρα τροποποιεί την αριθμιτική ακολουθία στο RREQ (Gagandeep & Kataria, 2012).

Χρησιμοποιώντας αυτήν την επίθεση, οι hackers μπορούν εύκολα να καταστείλουν ή να τροποποιήσουν τα πακέτα δεδομένων καθιστώντας ευαίσθητο το δίκτυο στο να δεχθεί και άλλες επιθέσεις όπως για παράδειγμα αυτή της επιλεκτικής προώθησης (Karlof & Wagner, 2003).



Εικόνα 2.16: Επίθεση Sinkhole

(Πηγή: Gagandeep & Kataria, 2012)

Είναι γνωστό ότι τα πρωτόκολλα δρομολόγησης χρησιμοποιούνται κάθε φορά που ένα πακέτο δεδομένων μεταδίδεται από τον κόμβο πηγής στον κόμβο προορισμού επικοινωνώντας με έναν αριθμό ενδιάμεσων κόμβων. Διάφορα πρωτόκολλα δρομολόγησης έχουν προταθεί για τέτοιου είδους ad hoc δίκτυα. Τα εν λόγω πρωτόκολλα είναι χρήσιμα για την εύρεση μιας συγκεκριμένης διαδρομής για την παράδοση πακέτων στον σωστό προορισμό (Mehta & Gupta, 2013).

Για την αποτροπή των επιθέσεων επιλεκτικής προώθησης και βύθισης από κάποιο εξωτερικό παρεμβολέα, χρησιμοποιείται η τεχνική κρυπτογράφησης των κοινόχρηστων κλειδιών. Έτσι ο επιτιθέμενος δεν μπορεί πλέον να ενταχθεί στα WSN. Ωστόσο να σημειωθεί ότι η τεχνική αυτή είναι ακατάλληλη για επιθέσεις που πραγματοποιούνται από εσωτερικούς εισβολείς (Karlof & Wagner, 2003).

- Επιθέσεις Jamming

Οι επιθέσεις παρεμβολής καλούνται και ράδιο-παρεμβολές. Πρόκειται για μέθοδο εκούσιας, από πλευράς εισβολέα παραγόμενης παρεμβολής, για τον αποπροσανατολισμό των radars (π.χ. σε περιπτώσεις πολεμικών αεροσκαφών). Η επίθεση πραγματοποιείται σε ασύρματα δίκτυα με παρεμβολή στις ραδιοσυχνότητες του δικτύου. Οι επιτιθέμενοι που διαθέτουν μεγάλη πηγή ενέργειας και την οποία διαθέτουν για να εκτελέσουν επιθέσεις παρεμβολής, δύνανται να προκαλέσουν εκτροπή της ορθής λειτουργίας του δικτύου με σοβαρές συνέπειες σε αυτό.

Για την αντιμετώπιση επιθέσεων ράδιο-παρεμβολής, υφίστανται οι ακόλουθοι αποτελεσματικοί μηχανισμοί:

- Η αναπήδηση συχνότητας (frequency hopping)και

- Η διάδοση κώδικα (code spreading)

Στην μέθοδο αναπήδησης συχνότητας πραγματοποιούνται γρήγορες μεταβολές της συχνότητας κατά τη μετάδοση των σημάτων, με αποτέλεσμα κάθε επίδοξος εισβολέας να αδυνατεί να παρέμβει στην άγνωστη συχνότητα.

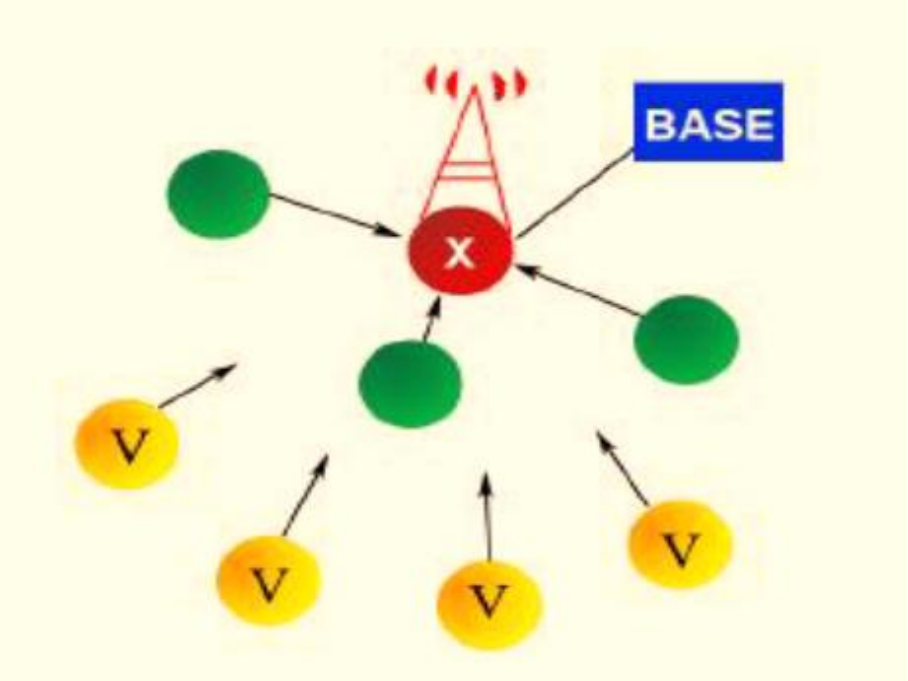
Στη μέθοδο διάδοσης κώδικα πραγματοποιείται επέκταση της συχνότητας ωστόσο η πρακτική αυτή απαιτεί μεγαλύτερη ποσότητα ενέργειας. Βασικό μειονέκτημα της μεθόδου αποτελούν αφενός το υψηλό κόστος των WSN και αφετέρου ο περιορισμένος αριθμός ενεργειακών πόρων, οπότε το εν λόγω μέτρο αντιστάθμισης εμφανίζει

περιορισμούς στην εφαρμογή (Wang et al., 2006; Al Ameen et al., 2012).

- Επιθέσεις Hello Flood

Σε μια επίθεση πλημμύρας (flooding attack), ένας κακόβουλος κόμβος εισέρχεται στο δίκτυο και αποστέλλει διαρκώς πακέτα, πολύ περισσότερα από όσα μπορεί να διαχειριστεί στους υπόλοιπους κόμβους του δικτύου. Αυτό έχει ως αποτέλεσμα το δίκτυο να πλημμυρίζει από πακέτα. Η επίθεση αυτή αποσκοπεί στο να εξαντλήσει τους πόρους, τη μνήμη και την ενέργεια του κόμβου.

Στην Εικόνα 2.17 φαίνεται ένα παράδειγμα επίθεσης τύπου Hello flood. Συγκεκριμένα ένας φορητός υπολογιστής αναμεταδίδει μια ενημέρωση δρομολόγησης με αρκετή ισχύ, ώστε να ληφθεί από ολόκληρο το δίκτυο αφήνοντας πολλούς κόμβους σε λανθάνουσα κατάσταση.



Εικόνα 2.17: Επίθεση Hello flood

(Πηγή: Maleh, & Ezzati, 2014)

Όπως παρατηρούμε, σε μια επίθεση πλημμύρας HELLO ο επιτιθέμενος εκμεταλλεύεται το γεγονός ότι οι κόμβοι πρωτόκολλων δρομολόγησης χρησιμοποιούν τα πακέτα 'HELLO' προκειμένου να συστήνονται στους γειτονικούς κόμβους με την παραδοχή ότι

οι κόμβοι αυτοί βρίσκονται εντός της κανονικής τους εμβέλειας. Οι επιτιθέμενοι που στέλνουν τα πακέτα HELLO, παρά το ότι βρίσκονται σε κανονική εμβέλεια, ξεγελούν τους άλλους κόμβους κάνοντάς τους να θεωρούν ότι είναι οι γειτονικοί κόμβοι αποστολής. Ως εκ τούτου οι γειτονικοί κόμβοι θα μεταδώσουν τα πακέτα δεδομένων τους στον κόμβο HELLO αλλά καθώς βρίσκονται εκτός εμβέλειας, τα πακέτα δεν θα φτάσουν ποτέ στον προορισμό τους διαταράσσοντας την λειτουργία του δικτύου (Karlof & Wagner, 2003).

Προς την κατεύθυνση αποτροπής ή αντιμετώπισης των επιθέσεων πλημμύρας HELLO, συστήνεται η χρήση ενός πρωτοκόλλου το οποίο θα εκτελεί έλεγχο της ταυτότητας μεταξύ των γειτονικών κόμβων. Η επαλήθευση των ταυτοτήτων των κόμβων θα γίνεται χρησιμοποιώντας τον σταθμό βάσης. Συμπερασματικά, στην επίθεση πλημμύρας HELLO, ο επιτιθέμενος θα πρέπει να ταυτοποιηθεί με όλους τους γειτονικούς κόμβους για να καταφέρει να υλοποιήσει την επίθεση. Ωστόσο αν ο αριθμός των γειτονικών κόμβων υπερβεί ένα προκαθορισμένο όριο, ο σταθμός βάσης θα μπορούσε δυνητικά να ανιχνεύσει τον εισβολέα (Karlof & Wagner, 2003).

- Επιθέσεις Tampering

Οι επιθέσεις αλλοίωσης (tampering) βρίσκουν πρόσφορο έδαφος στα δίκτυα αισθητήρων κυρίως εξ' αιτίας του χαμηλού κόστους των κόμβων αισθητήρων. Στοχεύουν στη φυσική καταστροφή των κόμβων και στην υποκλοπή ευαίσθητων δεδομένων, όπως κρυπτογραφικών κλειδιών, με σκοπό την ανάκτηση του ελέγχου του κόμβου που δέχεται τη κακόβουλη ενέργεια. Η επίθεση αλλοίωσης μπορεί να περιλαμβάνει την τροποποίηση, την αντικατάσταση, ή την αναπαραγωγή του κόμβου. Οι επιτιθέμενοι δύνανται να αποκτούν φυσική πρόσβαση σε έναν κόμβο, να εξάγουν τις πληροφορίες και εν τέλει να αποκτούν τον πλήρη έλεγχο αυτού. Ωστόσο υπάρχουν κόμβοι οι οποίοι έχουν την ικανότητα να συμβάλουν στον εντοπισμό τέτοιων παραβιάσεων αλλά εμφανίζουν υψηλό κόστος με αποτέλεσμα τα περισσότερα συστήματα ασφαλείας να διαθέτουν κόμβους μη ανθεκτικούς σε αλλοιώσεις (Wang et al., 2006; Ramotsoela et al., 2018).

Οι επιθέσεις αλλοίωσης παρόμοια με τις επιθέσεις παρεμβολής, πραγματοποιούνται στο φυσικό επίπεδο. Οι περιορισμοί στο κόστος των WSNs, έχουν ως απότοκο την απουσία αποτελεσματικού μέτρου αντιμετώπισης το οποίο θα μπορούσε να συμπεριληφθεί και

να εφαρμοστεί στο στάδιο του σχεδιασμού των WSNs. Κατά τον σχεδιασμό των συστημάτων ασφαλείας θα πρέπει οι σχεδιαστές να λαμβάνουν μέριμνα για πιθανές επιθέσεις στα WSNs στο επίπεδο φυσικού στρώματος (Ramotsoela et al., 2018).

Ωστόσο μια απλή και τεχνική που ενδέχεται να περιορίσει το πρόβλημα είναι η χρήση μικρού μεγέθους κόμβων οι οποίοι θα μπορούν ευκολότερα να αποκρύπτουν τη φυσική τους ταυτότητα.

- Επιθέσεις Sybil

Στην επίθεση Sybil ένας κακόβουλος κόμβος παρουσιάζεται με πολλαπλές ταυτότητες στους άλλους κόμβους του δικτύου. Αυτό ενέχει σημαντικό κίνδυνο για τα πρωτόκολλα δρομολόγησης καθώς θα προκαλέσει κορεσμό στους πίνακες δρομολόγησης των κόμβων με λανθασμένες πληροφορίες.

Γενικά, οι επιθέσεις Sybil εκμεταλλεύονται την αδυναμία απόδοσης έγκυρων ταυτοτήτων στους συμμετέχοντες ενός δικτύου. Οι επιθέσεις αυτές αναφέρονται σε επιθέσεις ταυτοποίησης όπου ο επιτιθέμενος φέρει ψεύτικες ταυτότητες και ταυτόχρονα δημιουργεί ψεύτικους κόμβους τους οποίους τοποθετεί μεταξύ των έμπιστων κόμβων. Με αυτόν τον τρόπο, αποκτά τον έλεγχο σε ένα μεγάλο τμήμα του δικτύου.

Η επίθεση αυτή δύναται να εμφανιστεί σε όλα τα δίκτυα που προϋποθέτουν αυτή τη σχέση ανάμεσα στην οντότητα και την ταυτότητα. Σκοπός της επίθεσης είναι να πλήξει την απόδοση του συστήματος λήψης εφεδρικών αντιγράφων που διαθέτουν τα δίκτυα για να προστατέψουν την ακεραιότητα και την ιδιωτικότητά τους. Γενικά, η επίθεση Sybil βρίσκει συχνά εφαρμογή σε περιπτώσεις γεωγραφικής δρομολόγησης όπου οι κόμβοι μεταβάλλουν τις συντεταγμένες τους με τους γειτονικούς κόμβους προκειμένου να κατευθύνουν γεωγραφικά τις πληροφορίες. Με τον τρόπο αυτό ο επιτιθέμενος εμφανίζεται ότι βρίσκεται σε πολλαπλά σημεία κάθε στιγμή (Karlof & Wagner, 2003).

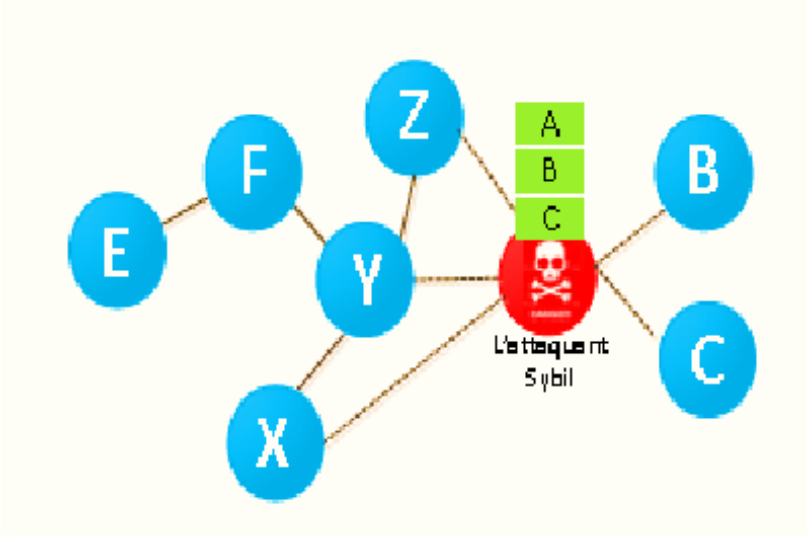
Γενικά το γεγονός ότι οι επιθέσεις προέρχονται από το εσωτερικό του WSN καθιστά σχεδόν αδύνατη την αποτροπή τους. Έτσι, η επαλήθευση των ταυτοτήτων των κόμβων αποτελεί γεγονός κρίσιμης σημασίας για την ανίχνευση της μεταμφίεσης.

Αντισταθμιστικό μέτρο στην επίθεση Sibyl αποτελεί η διαδικασία εγγραφής. Σε κάθε νέο κόμβο, με βάση την IP διεύθυνση και του port, αποδίδεται η ταυτότητά του. Εν συνεχεία πραγματοποιείται η εγγραφή του και αιτείται τη συμμετοχή του στο δίκτυο. Την ευθύνη

και τη δυνατότητα της πιστοποίησης της ταυτότητας του νέου χρήστη την έχουν οι υπόλοιποι εγγεγραμμένοι κόμβοι του συστήματος, οι οποίοι είναι ήδη εγγεγραμμένοι στο δίκτυο. Η εγγραφή του νέου κόμβου γίνεται εφόσον, η πλειοψηφία των άλλων κόμβων εγκρίνει τη συμμετοχή του στο δίκτυο, μέσω του ελέγχου της ταυτότητάς του. Εάν από τη διαδικασία αυτή προκύψει ότι ο νέος κόμβος δεν είναι ψεύτικος τότε γίνει δεκτός.

Μειονέκτημα της μεθόδου self-registration είναι το γεγονός πως το κόστος της απόκτησης μιας IP διεύθυνσης συνεχώς φθίνει. Επιπλέον, οι επιτιθέμενοι έχουν την δυνατότητα να διαθέτουν ένα μεγάλο αριθμό διευθύνσεων IP έχοντας υπό τον έλεγχό τους ένα μεγάλο αριθμό υπολογιστών.

Μια άλλη τεχνική που χρησιμοποιείται είναι το σύστημα ελέγχου πρόσβασης, το οποίο βασίζεται στην ιδέα ενός κρυπτογραφικού παζλ το οποίο κάθε νέος κόμβος πρέπει να επιλύσει ώστε να γίνει δεκτός στο δίκτυο. Έχει γενικώς παρατηρηθεί ότι ο χρόνος που απαιτείται για να μπορέσει ο επιτιθέμενος να αποκτήσει ένα μικρό ποσοστό κόμβων σε ένα δίκτυο είναι από 2 μέχρι 14 ημέρες.



Εικόνα 2.18: Επίθεση Hello flood

(Πηγή: Maleh, & Ezzati, 2014)

Μια άλλη λύση είναι η εφαρμογή μοναδικών συμμετρικών κλειδιών που μοιράζονται μεταξύ τους οι κόμβοι και ο σταθμός βάσης. Τα κλειδιά επιτρέπουν στους γειτονικούς κόμβους να επαληθεύσουν την ταυτότητά τους δημιουργώντας ένα κοινό κλειδί που ελέγχει την επικοινωνία τους με τους γειτονικούς κόμβους που έχουν ήδη επαληθεύσει την ταυτότητα τους. Ωστόσο, ο αριθμός των κλειδιών ανά κόμβο πρέπει να περιορίζεται

από τον σταθμό βάσης για να εμποδίσει τους επιτιθέμενους να δημιουργήσουν ένα κοινόχρηστο κλειδί με κάθε κόμβο. Έτσι όταν ένας κόμβος ξεπεράσει ένα συγκεκριμένο πλήθος κοινόχρηστων κλειδιών με τους γειτονικούς του κόμβους, στέλνει μήνυμα σφάλματος αναγγέλλοντας την ύπαρξη προβλήματος (Karlof & Wagner, 2003).

Στον Πίνακα 1 μπορούμε να δούμε το είδος των επιθέσεων που εξαπολύονται σε κάθε στρώμα της δομής του δικτύου καθώς και τα μέτρα αντιστάθμισης για κάθε μία από αυτές.

Πίνακας 1: Είδη επιθέσεων που εξαπολύονται σε κάθε στρώμα της δομής του δικτύου

Στρώμα - Layer	**Επιθέσεις - Attacks**	**Μέτρα αντιστάθμισης - Defense**
Φυσικό	Jamming- Ραδιοπαρεμβολές	Διάδοση φάσματος, μηνύματα προτεραιότητας, μικρός κύκλος λειτουργίας, χαρτογράφηση περιοχής, αλλαγή τρόπου λειτουργίας
Ζεύξης	Σύγκρουσης	Κώδικας διόρθωσης σφαλμάτων
	Εξάντλησης	Rate limitation
	unfairness	Μικρά frame
Δικτύου	Παραποίησης δεδομένων δρομολόγησης	Φίλτρα εξόδου, αυθεντικοποίηση, παρακολούθηση
	Sinkhole	Έλεγχος πλεονασμού
	Sibyl	αυθεντικοποίηση, παρακολούθηση,
	Wormhole	αυθεντικοποίηση, διερεύνηση
	Hello flood	αυθεντικοποίηση,
Μεταφοράς	Session Hijacking	Συνάθροιση δεδομένων
	SYN Flooding	Αυθεντικοποίηση πακέτων
Εφαρμογής	Αλλοίωσης Δεδομένων Άρνησης Συμμόρφωσης	Αυθεντικοποίηση

(Πηγή: Maleh, & Ezzati, 2014)

Κεφάλαιο 3ο: Εφαρμογές κινητής επικοινωνίας 5G: Μελέτη και σύγκριση περιπτώσεων χρήσης

3.1 Εισαγωγή

Το 5G ως το νεότερο δίκτυο κινητής τηλεφωνίας αναπτύσσεται με γρήγορους ρυθμούς παγκοσμίως, καθώς υπόσχεται να προσφέρει σημαντική μεταμόρφωση στα επιχειρηματικά μοντέλα για την ανάπτυξη καινοτόμων λύσεων, προϊόντων και υπηρεσιών μέσω της συνδεσιμότητας με το 5G.

Η ανάπτυξη των δικτύων 5G θα συμβάλλει στην βελτίωση της εμπειρίας των χρηστών και στον σχεδιασμό όλο και περισσότερων εφαρμογών. Όπως ήδη αναφέραμε οι απαιτήσεις των χρηστών για ασύρματες ευρυζωνικές υπηρεσίες και η ανάγκη μαζικής συνδεσιμότητας συσκευών στο Διαδικτύου των πραγμάτων (IoT) προϋποθέτουν την ύπαρξη δικτύων μεγάλης ταχύτητας και δυναμικής. Προς αυτή την κατεύθυνση η τεχνολογία 5G υπόσχεται απίστευτα υψηλές ταχύτητες, δυνατότητα ταυτόχρονης σύνδεσης μέσω τεχνολογίας IoT και δυνατότητα άμεσης απόκρισης με μικρές καθυστερήσεις. [50].

Στο κεφάλαιο αυτό επιχειρείται μια ολοκληρωμένη παρουσίαση των χρήσεων και των εφαρμογών που στηρίζονται στην τεχνολογία των δικτύων 5G.

Με την διαθεσιμότητα των δικτύων 5G οι εφαρμογές 5G θα είναι ικανές να υποστηρίξουν ένα μεγάλο αριθμό χρήσεων προσαρμοσμένες στις κατά περίπτωση ανάγκες των διάφορων τομέων. Ωστόσο προκύπτει η απαίτηση σωστής και κατάλληλης ταξινόμησης των χαρακτηριστικών και των αναγκών που καλούνται να εξυπηρετήσουν προκειμένου να καταστεί αποτελεσματική η χρήση τους (SDxCentral Studios, 2017; Xiang et al., 2017).

Στο πεδίο της ευρυζωνικότητας, επιθυμούμε διαρκή σύνδεση στο διαδίκτυο, υψηλές ταχύτητες για νέες εφαρμογές και υπηρεσίες και αξιόπιστες συνδέσεις υψηλής αποδοτικότητας, ώστε ο κάθε χρήστης να απολαμβάνει στο έπακρο τα οφέλη του δικτύου. Η κατακόρυφη αύξηση του όγκου δεδομένων που ανταλλάσσονται προϋποθέτει υψηλούς ρυθμούς μετάδοσης, άμεση απόκριση χωρίς καθυστερήσεις και υψηλά ποσοστά κάλυψης.

Ανάμεσα στους χρήστες και τις υπηρεσίες που θα επωφεληθούν από τις εφαρμογές και

τις παροχές της 5G τεχνολογίας είναι οι ραδιοτηλεοπτικοί σταθμοί, οι συνδρομητές τηλεόρασης, οι συνδρομητές υπηρεσιών Over the Top (OTT), οι τεχνολογίες 4K UHD, 8K UHD και 3D κ.α. Οι προκλήσεις για την ανάπτυξη και την χρήση νέων υπηρεσιών, βασισμένων στην τεχνολογία 5G, αναμένονται με μεγάλο ενδιαφέρον τόσο από τους χρήστες, όσο και τους παρόχους. Σε πρώτο στάδιο απευθύνονται και θα διαδοθούν στις μεγάλες αστικές περιοχές με μελλοντική δυνατότητα επέκτασης και κάλυψης και των περιφερειακών περιοχών. Ανάμεσα στις αστικές εφαρμογές είναι η παροχή πληροφοριών που αφορούν στο περιβάλλον (όπως για παράδειγμα μετρήσεις επιπέδων ρύπανσης, θορύβου, θερμοκρασίας), μετρήσεις φωτισμού (σε δρόμους, λεωφόρους και κτίρια), μετρήσεις ελέγχου και διαχείρισης της κυκλοφορίας κ.α. Για την υλοποίηση των προαναφερθέντων γίνεται εύκολα αντιληπτό ότι απαιτείται η συμμετοχή μεγάλου αριθμού συσκευών με πιθανώς ετερόκλητα χαρακτηριστικά που οφείλουν να αλληλοεπιδράσουν για την επίτευξη του κοινού τους σκοπού. Στο ακόλουθο σχήμα μπορούμε να διακρίνουμε την αλληλεπίδραση ανθρώπου και μηχανής στο πλαίσιο ενός ευρέως φάσματος εφαρμογών και υπηρεσιών (Theiotintegrator, χ.η.).

Όπως ήδη αναφέραμε, τα είδη των δικτυωμένων συσκευών πέρα από τις κλασικές συσκευές (προσωπικοί υπολογιστές, smartphones, tablets) περιλαμβάνουν αισθητήρες, μετρητές, οικοσκευές, βιομηχανικά μηχανήματα και εργαλεία, αυτοκίνητα, ιατρικό εξοπλισμό κ.α συνθέτοντας το λεγόμενο «διαδίκτυο των πραγμάτων» (IoT). Στο πλαίσιο λειτουργίας του IoT ο μεγάλος αριθμός των συσκευών που είναι συνδεδεμένες χαρακτηρίζεται από διαφορετικές απαιτήσεις λειτουργίας οι οποίες δύνανται να διαφέρουν σημαντικά από τις υπάρχουσες μορφές επικοινωνίας. Η νέα μορφή επικοινωνίας που προκύπτει από τα παραπάνω ονομάζεται επικοινωνία μηχανής προς μηχανή (Machine to Machine-M2M) ή επικοινωνία τύπου μηχανής (Machine Type Communication-MTC) και οι αντίστοιχες συσκευές καλούνται συσκευές M2M ή MTC (Elvitigala & Sudantha, 2017).

Ενδεικτικά παραδείγματα αυτών των περιπτώσεων είναι η δυνατότητα απομακρυσμένου ελέγχου (π.χ. σε μία μονάδα βιομηχανικής παραγωγής), συσκευές τηλεϊατρικής (π.χ για εξ' αποστάσεως ιατρική επέμβαση), συσκευές ασφάλειας κτιρίων (π.χ. κάμερες παρακολούθησης θυρών) κ.α. (NGMN, 2015).

Ειδικότερα στον τομέα της υγείας, τα δίκτυα 5G αναμένεται να συμβάλουν σημαντικά

στην βελτίωση των υπαρχουσών υποδομών καθώς και στον σχεδιασμό νέων εφαρμογών τηλεϊατρικής και ρομποτικής. Επιπλέον, μέσω των ασύρματων δικτύων αισθητήρων μπορεί να σχεδιαστούν συσκευές απομακρυσμένης παρακολούθησης ασθενών, συσκευές διάγνωσης και παρακολούθησης χρόνιων πασχόντων, ιατρικές συσκευές άμεσης προειδοποίησης περιπτώσεων εκτάκτου ανάγκης κ.α. (NGMN, 2015).

Με την βοήθεια της ρομποτικής και της τηλεϊατρικής θα μπορούν να πραγματοποιηθούν χειρουργικές επεμβάσεις εξ΄ αποστάσεως με μεγάλη ακρίβεια λόγω της υψηλής ταχύτητας και των εξαιρετικά μικρών καθυστερήσεων που προσφέρει η τεχνολογία του δικτύου 5G. Ταυτόχρονα, παρέχεται η δυνατότητα απομακρυσμένης υγειονομικής περίθαλψης κυρίως σε απομακρυσμένες και δυσπρόσιτες περιοχές όπου παρατηρείται μεγάλη έλλειψη ιατρο-νοσηλευτικού προσωπικού και υγειονομικών μονάδων (West, 2016).

Ιδιαίτερα σημαντική προβλέπεται να είναι η συμβολή των εφαρμογών 5G στην μηχανοργάνωση νοσοκομείων, στην καταχώριση ψηφιακών ιατρικών εξετάσεων καθώς και σε πάσης φύσεως ιατρικά δεδομένα, σε μία ενιαία πλατφόρμα πρόσβασης, ώστε να μπορούν ανακληθούν ανά πάσα στιγμή και οπουδήποτε απαιτηθούν (NOKIA, 2016).

Η ανάπτυξη των δικτύων 5G θα επηρεάσει σημαντικά την βιομηχανία αυτοκινήτου και των μεταφορών με την χρήση εφαρμογών πλοήγησης, αυτοματοποιημένης οδήγησης, εξ' αποστάσεως οδήγησης, παροχής υπηρεσιών οδικής ασφάλειας, παροχής πληροφοριών και ελέγχου της κυκλοφορίας.

Όπως αναφέραμε παραπάνω στα αμέσως επόμενα χρόνια η ανάπτυξη των δικτύων 5G, θα μπορεί να προσφέρει μια σειρά προηγμένων εφαρμογών που θα μειώνουν τα τροχαία ατυχήματα, θα διαχειρίζονται αποτελεσματικά την κυκλοφορία και θα διευκολύνουν την κίνηση των οχημάτων έκτακτης ανάγκης όπως ασθενοφόρα, πυροσβεστικά και αστυνομικά οχήματα.

Για την υλοποίηση των παραπάνω θα υπάρχουν εφαρμογές που θα υποστηρίζουν την επικοινωνία μεταξύ των οχημάτων (όχημα με όχημα), του οχήματος με την υποδομή καθώς και την επικοινωνία με τους ευάλωτους χρήστες όπως πεζοί και ποδηλάτες (NGMN, 2015).

Ως προς το πλαίσιο αυτό, θα αναπτυχθούν συνεταιριστικά ευφυή συστήματα μεταφορών (Cooperative Intelligent Transport Systems (C-ITS) τα οποία θα ανταλλάσσουν

αξιόπιστες πληροφορίες σε πραγματικό χρόνο μέσω των δικτύων 5G. Η αυτοματοποιημένη οδήγηση των οχημάτων και των μέσων μαζικής μεταφοράς θα έχει ως αποτέλεσμα την μείωση της διάρκειας των διαδρομών, την εξοικονόμηση κατανάλωσης καυσίμου, την μείωση εκπομπών καυσαερίων, την αύξηση της οδικής ασφάλειας και την καλύτερη κυκλοφορία εν γένει (Sorbara et al., 2015).

Τα εν λόγω συνεταιριστικά συστήματα ενεργητικής ασφάλειας θα προειδοποιούν τους οδηγούς ενόψει επικίνδυνων καταστάσεων ώστε μέσω της αυτόματης πέδησης να επιτυγχάνεται η αποφυγή ατυχημάτων (5GPPP Architecture Working Group, 2017).

Παράλληλα η συνδεσιμότητα των οχημάτων με τα δίκτυα 5G σε συνδυασμό με το γρήγορο ρυθμό μετάδοσης δεδομένων θα επιτρέπουν στους χρήστες να απολαμβάνουν υπηρεσίες Διαδικτύου ανάλογων επιδόσεων με του σπιτιού τους.

Τα δεδομένα των αισθητήρων μεταφέρονται σε «πραγματικό χρόνο», παρέχοντας πληροφορίες ζωτικής σημασίας για την ασφαλή μεταφορά εμπορευμάτων. Επίσης ένα διασυνδεδεμένο όχημα θα μπορεί να προειδοποιεί τα επόμενα για τυχόν εμπόδια ώστε να επιλέγουν εναλλακτική διαδρομή και να αποφεύγεται το κυκλοφοριακό μπλοκάρισμα (5GPPP Architecture Working Group, 2017).

Οι νέες προκλήσεις που προκύπτουν από το δίκτυο 5G μπορούν να συνδυαστούν με άλλες σύγχρονες τεχνολογίες που αφορούν στην κατανάλωση και τη διανομή της ηλεκτρικής ενέργειας, μέσω της αξιοποίησης των ανανεώσιμων πηγών ενέργειας συμβάλλοντας στην γρηγορότερη και αποτελεσματικότερη υλοποίησή τους (Dieudonne et al., 2016).

Ομοίως, τα έξυπνα δίκτυα (Smart grids) θα μπορούν να διασυνδέουν ένα μεγάλο αριθμό αισθητήρων, χρησιμοποιώντας την ψηφιακή τεχνολογία της πληροφορίας και των επικοινωνιών ώστε να συγκεντρώνουν χρήσιμα δεδομένα για την λειτουργία τους. Τέτοιες πληροφορίες μπορεί να περιέχουν καταναλωτικές συνήθειες και συμπεριφορές που θα επιτρέπουν στο έξυπνο δίκτυο την σωστή διαχείριση των πόρων του, τη βελτίωση της αποτελεσματικότητας και της αξιοπιστίας τους καθιστώντας τα ευέλικτα και δυναμικά. (NGMN, 2015).

Οι κυριότερες λειτουργίες του 5G που βρίσκουν εφαρμογή στα έξυπνα δίκτυα παραγωγής και διανομής της ενέργειας περιγράφονται παρακάτω:

- Τα συστήματα ελέγχου και εντοπισμού σφαλμάτων των έξυπνων δικτύων απαιτούν άμεση επικοινωνία μεταξύ τους και με το δίκτυο, ώστε να ενεργοποιούνται έγκαιρα οι εντολές διακοπής λειτουργίας σε περιπτώσεις ανίχνευσης λάθους. Ως προς αυτή την κατεύθυνση οι γρήγορες ταχύτητες του 5G και η άμεση απόκριση με εξαιρετικά μικρές καθυστερήσεις αποτελούν σημαντικό εργαλείο αποτελεσματικότητας.
- Η μεγάλη ταχύτητα ανταλλαγής δεδομένων του 5G επιτρέπει την αυτόματη ενεργοποίηση διακοπής της παραγωγής σε περιπτώσεις που απαιτείται με αποτέλεσμα την εξοικονόμηση ρεύματος και τον περιορισμό της μηχανικής καταπόνησης των συστημάτων.
- Η καλωδίωση για τον έλεγχο των έξυπνων δικτύων θα αντικατασταθεί από τα δίκτυα 5G από τα μηνύματα ελέγχου μετάδοσης. Έτσι οι διαδικασίες διακοπής της λειτουργίας θα εκτελούνται κατανεμημένα και αξιόπιστα.
- Σε ενδεχόμενες βλάβες, κατά την ανίχνευση τους, το δίκτυο θα δύναται να αναδιαρθρωθεί άμεσα με αποτέλεσμα να μειώνεται σημαντικά ο χρόνος αποκατάστασης και το δίκτυο να διατηρεί την αξιοπιστία του.

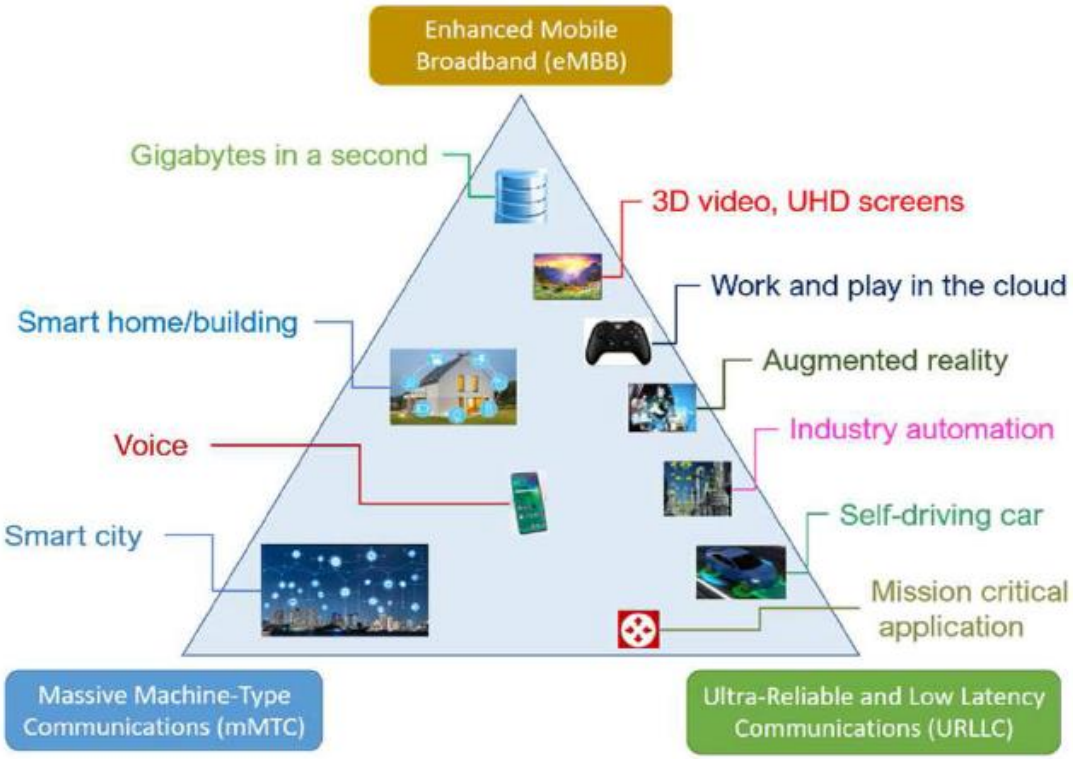
3.2 Σενάρια χρήσης

Τα σενάρια χρήσης του IMT για το έτος 2020 και μετά φαίνονται στην Εικόνα 3.1. Οι περισσότερες εφαρμογές θα αναλυθούν στις επόμενες ενότητες του 3ου Κεφαλαίου.

Βάσει της ταξινόμησης της Διεθνούς Ένωσης Τηλεπικοινωνιών, το υφιστάμενο σχήμα του 5G μπορεί να κατηγοριοποιηθεί σε τρία βασικά σενάρια:

- ✓ βελτιωμένη κινητή ευρυζωνική σύνδεση ***eMBB -Enhanced Mobile Broadband***: Προσφέρει ταχύτητες 10-20 φορές πιο γρήγορα σε σχέση με το 4G,
- ✓ μαζικές επικοινωνίες τύπου μηχανής ***mMTC - Massive Machine Type Communications***:

  Μπορούν να συνδεθούν έως και 1 εκατομμύριο συσκευές ανά τετραγωνικό χιλιόμετρο και
- ✓ Επικοινωνίες εξαιρετικά αξιόπιστες και με χαμηλή καθυστέρηση ***URLLC***: Εγγυημένες καθυστερήσεις κάτω των 10 msμε uRLLC.



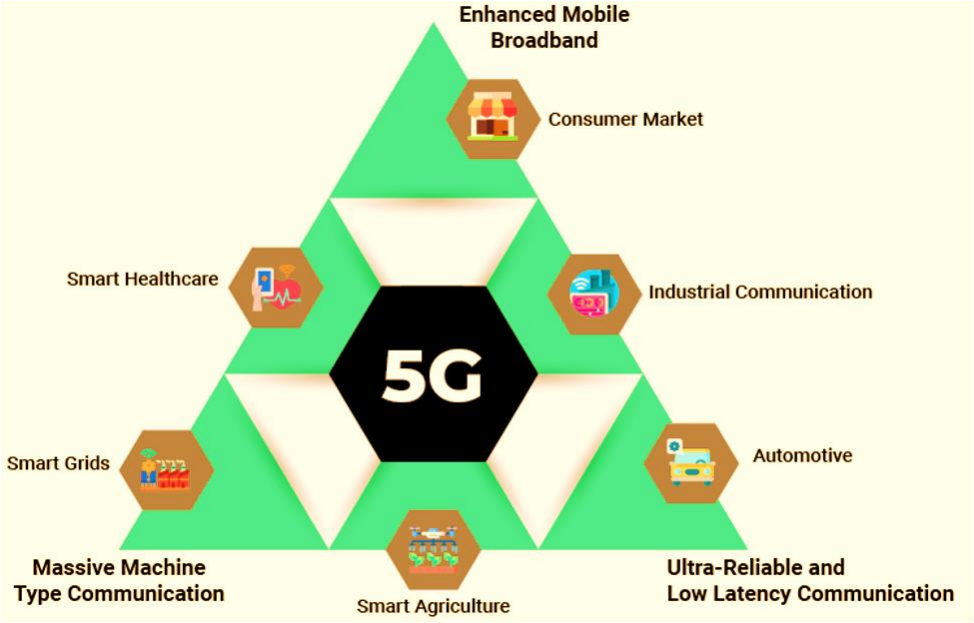
Εικόνα 3.1: Σενάρια χρήσης του IMT (2020+)

(Πηγή: Erunkulu et al., 2021)

Η ως άνω ευρύτερη διχοτόμηση των εφαρμογών τεχνολογίας 5G αναφέρεται σε τρεις διαφορετικές κατηγορίες περιπτώσεων χρήσης που προσφέρουν βελτίωση στις βασικές παραμέτρους απόδοσης της ταχύτητας και του εύρους ζώνης, της κάλυψης και της διαθεσιμότητας και της καθυστέρησης. Η διάταξη αυτή είναι γνωστή και ως το τρίγωνο 5G (Yanjun et al., 2019).

Στο πρώτο σενάριο embb, δίνεται έμφαση σε ανθρωποκεντρικούς δείκτες αξιολόγησης της απόδοσης επικοινωνίας όπως το ποσοστό εμπειρίας χρήστη. Το σενάριο mMTC αναφέρεται στα τεράστια ασύρματα δίκτυα αισθητήρων. Οι βασικοί στόχοι του σεναρίου mMTC σχετίζονται με την υψηλή πυκνότητα σύνδεσης, τη μεγάλη διάρκεια ζωής της μπαταρίας και το χαμηλό κόστος. Αντίστοιχα υπάρχουν πολλές τυπικές περιπτώσεις χρήσης που σχετίζονται με το uRLLC. Ανάμεσα σε αυτές είναι τα τηλεχειριζόμενα μηχανήματα και τα έξυπνα συστήματα μεταφοράς. Ωστόσο σχετικά με το σενάριο uRLLC υπάρχουν δύο κρίσιμες απαιτήσεις οι οποίες θα πρέπει να ικανοποιούνται ήτοι η μικρή καθυστέρηση και ο υψηλός βαθμός αξιοπιστίας. Αποδεικνύεται ότι οι παραπάνω

δείκτες δύνανται να σχετίζονται με πολλά διαφορετικά σενάρια αποδίδοντας χρήσιμες πληροφορίες κάτω από συγκεκριμένες συνθήκες (Yanjun et al., 2019).



Εικόνα 3.2: Τρίγωνο 5G

(Πηγή: https://embeddedcomputing.com/application/networking-5g)

3.3 Εφαρμογές

3.3.1 Έξυπνοι μετρητές

Οι έξυπνοι μετρητές κατέχουν σημαντικό ρόλο στην λειτουργία των έξυπνων δικτύων καθώς πραγματοποιούν μετρήσεις που μεταφέρουν πληροφορίες κατανάλωσης ενέργειας από τους χρήστες χωρίς να απαιτείται η φυσική παρουσία προσωπικού των παρόχων. Η λειτουργία τους στηρίζεται στην παρακολούθηση και τον έλεγχο της ηλεκτρικής ενέργειας που καταναλώνεται, καθώς επίσης και τον real time υπολογισμό του κόστους λειτουργίας των ηλεκτρικών συσκευών. Κατ' αυτόν τον τρόπο μέσω της άμεσης ενημέρωσης του καταναλωτικού κοινού, επιτυγχάνεται η ορθότερη χρήση και διαχείριση όλων των συσκευών, με αποτέλεσμα την επιθυμητή μείωση της κατανάλωσης ενέργειας. Με άλλα λόγια, με έναν έξυπνο μετρητή ενέργειας παρέχονται οι πληροφορίες για το σύνολο ή τις μεμονωμένες βαθμίδες του εξοπλισμού και αποφεύγονται ενδεχόμενες διαρροές ή υπερκαταναλώσεις ενέργειας. Οι πληροφορίες αυτές παρέχονται με κάθε λεπτομέρεια ακόμα και όταν οι χρήστες απουσιάζουν μέσω κινητού ή tablet σε ένα

ασύρματο δίκτυο.

Η εφαρμογή έξυπνων μετρητών στο δίκτυο διανομής ενέργειας, με την ανάπτυξη των δικτύων 5G, θα συμβάλει στην γρήγορη μετάδοση και επεξεργασία των δεδομένων που ανταλλάσσονται. Επιπρόσθετα, η real time μετάδοση θα βελτιστοποιήσει τα τμήματα υποδομών χαμηλής και μέσης τάσης. Αντίστοιχες υποδομές δύναται να χρησιμοποιηθούν σε δίκτυα ύδρευσης και φυσικού αερίου (Dieudonne et al., 2016; NES, 2022).

3.3.2 Εφαρμογή στη βιομηχανία

Το 5G υποστηρίζει την επικοινωνία με πρωτοφανή αξιοπιστία, ιδιαίτερα χαμηλές καθυστερήσεις και τεράστια συνδεσιμότητα IoT. Το γεγονός αυτό σηματοδοτεί πρακτικά την επόμενη εποχή στη βιομηχανική παραγωγή, γνωστή ως τέταρτη βιομηχανική επανάσταση - Industry 4.0. Μέσω αυτής αναμένεται ουσιαστική βελτίωση στην ευελιξία, τη χρηστικότητα και την αποτελεσματικότητα των αναπτυσσόμενων έξυπνων εργοστασίων και βιομηχανικών εγκαταστάσεων (Brettel et al., 2018).

Το Industry 4.0 ενσωματώνει το IoT και τις σχετικές υπηρεσίες στη βιομηχανική κατασκευή και παρέχει ουσιαστική και απρόσκοπτη ενοποίηση στο σύνολο της αλυσίδας αξίας και σε όλα τα επίπεδα του αυτοματισμού (Brettel et al., 2018).

Η συνδεσιμότητα είναι βασικό στοιχείο του Industry 4.0 και θα υποστηρίξει τις συνεχιζόμενες εξελίξεις παρέχοντας ισχυρή και διάχυτη συνδεσιμότητα μεταξύ μηχανών, ανθρώπων και αντικειμένων. Αναμφίβολα, οι βιομηχανικές επαναστάσεις πυροδοτήθηκαν από τεχνικές καινοτομίες όπως η εισαγωγή των προγραμματιζόμενων λογικών ελεγκτών - PLC που επέτρεψε την αυτοματοποίηση των κατασκευών στη δεκαετία του ’70. Αντίστοιχα, με την ανάπτυξη του 5G εξασφαλίζεται η επικοινωνία μεταξύ ανθρώπου και μηχανής (Cyber Physical Systems - CPS) σε μεγάλα δίκτυα (Brettel et al., 2018).

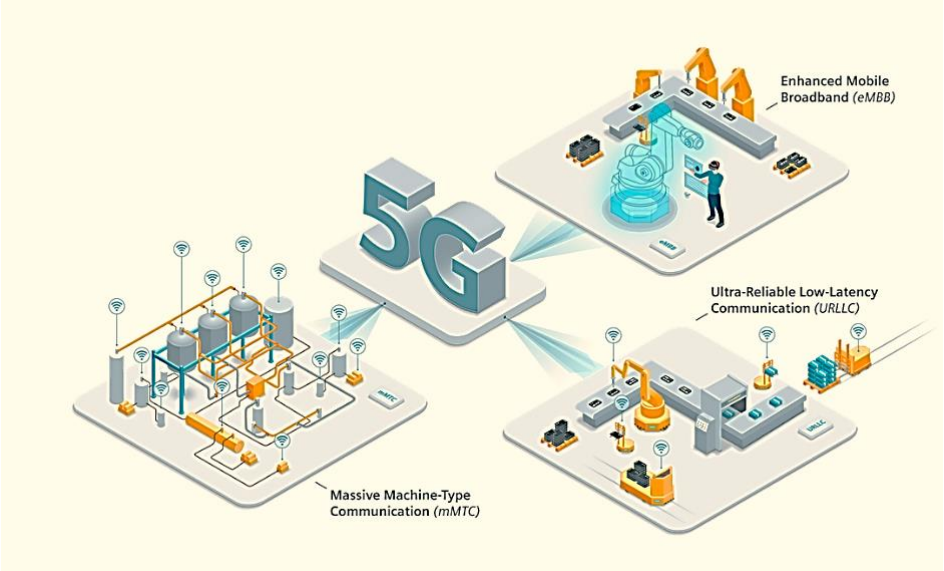
Στον τομέα της βιομηχανίας οι απαιτήσεις για την εισαγωγή και τη λειτουργία σύγχρονων μηχανημάτων στα εργοστάσια των βιομηχανιών αυξάνονται διαρκώς. Η τεχνολογία 5G στον τομέα της βιομηχανίας υπόσχεται να συμβάλει στην αύξηση της παραγωγικότητας, της αποδοτικότητας, της ταχύτητας και της ποιότητας της παραγωγής. Το 5G έχει τη δυνατότητα να παρέχει (ασύρματη) συνδεσιμότητα για ένα ευρύ φάσμα διαφορετικών

περιπτώσεων χρήσης και εφαρμογών στη βιομηχανία. Παράλληλα δύναται να οδηγήσει σε σύγκλιση των διαφορετικών τεχνολογιών επικοινωνίας που χρησιμοποιούνται σήμερα, μειώνοντας τα πρόσθετα κόστη της βιομηχανικής συνδεσιμότητας (Presher, 2019).

Οι εφαρμογές του 5G στον τομέα της βιομηχανίας σχετίζονται με τη χρήση αυτοματισμού και μπορούν να διακριθούν σε πέντε τομείς εφαρμογής ήτοι:

1. εργοστασιακή αυτοματοποίηση
2. αυτοματοποίηση για την απλούστευση των διαδικασιών
3. διεπαφές ανθρώπου-μηχανής (HMIs) και ΤΠ παραγωγής
4. απλούστευση εργασιών μηχανογράφησης
5. παρακολούθηση και προγνωστική συντήρηση.

Με λίγα λόγια, ο βιομηχανικός αυτοματισμός προσανατολίζεται στην αυτοματοποίηση των διαδικασιών της γραμμής παραγωγής, στην υιοθέτηση συστημάτων παρακολούθησης και ελέγχου υψηλών προδιαγραφών, στην ψηφιοποίηση των διαδικασιών επεξεργασίας των προϊόντων κ.α. Παράλληλα θα επέλθει βελτίωση των υπηρεσιών της αλυσίδας εφοδιασμού και διανομής μέσω της παρακολούθησης και του συντονισμού των οχημάτων σε πραγματικό χρόνο real time παρέχοντας αξιόπιστες υπηρεσίες στο στάδιο εφοδιασμού και διανομής.



Εικόνα 3.3: 5G και βιομηχανία

(Πηγή: Presher, 2019)

Τέλος, τα δίκτυα 5G αναμένεται να εξασφαλίσουν ένα πεδίο λύσεων ως προς τα ζητήματα συνδεσιμότητας και τις μεταβαλλόμενες απαιτήσεις σε ταχύτητα και αξιοπιστία μεταξύ των εγκαταστάσεων παραγωγής της βιομηχανικής αλυσίδας (Qi, 2020).

3.3.3 Επαυξημένη και εικονική πραγματικότητα

Με την ανάπτυξη συσκευών επαυξημένης πραγματικότητας (AR), παρέχονται δυνατότητες για υλοποίηση εξ' αποστάσεως υπηρεσιών. Οι εφαρμογές αυτές δύναται να βελτιώνουν την λειτουργική απόδοση ενός μεγάλου φάσματος υπηρεσιών καθώς επιτρέπουν στους χειριστές να προβάλλουν σε υπέρθεση τρέχοντα δεδομένα και αντικείμενα ενός απομακρυσμένου περιβάλλοντος. Τα πλεονεκτήματα που προσφέρουν οι εν λόγω εφαρμογές είναι πολλά όπως για παράδειγμα η μείωση του χρόνου για την εύρεση πληροφοριών, η επιτόπου πρόσβαση σε απομακρυσμένα δεδομένα, η επιτάχυνση της λειτουργίας υπηρεσιών συντήρησης, η μείωση σφαλμάτων που υπεισέρχονται εξ' αιτίας του ανθρώπινου παράγοντα κ.α. (METIS, 2014).

Στο πλαίσιο αυτό οι εταιρείες συστήνουν ομάδες εργασίας και υποστήριξης (back office), στις οποίες παρέχεται η δυνατότητα να χρησιμοποιούν δεδομένα που προέρχονται από έξυπνες συσκευές επαυξημένης πραγματικότητας, ώστε να εκτελούν ελέγχους, να αποκτούν άμεση πρόσβαση σε λειτουργίες συστημάτων απομακρυσμένης τοποθεσίας, να προβαίνουν σε λειτουργίες απομακρυσμένης συντήρησης και επισκευής μηχανημάτων κ.α.

Επιπροσθέτως, μεγάλη αναμένεται να είναι η απήχηση των δικτύων 5G και στα ηλεκτρονικά παιχνίδια εικονικής πραγματικότητας καθώς η εξέλιξη τους δημιουργεί διαρκώς αυξημένες απαιτήσεις. Ανάμεσα σε αυτές είναι ότι αυξάνεται η χωρητικότητά τους και απαιτούν μεγαλύτερο χρόνο εγκατάστασης. Οι κάμερες, τα GPS, τα επιταχυνσιόμετρα αποτελούν μερικά μόνο από τα στοιχεία τους. Μέσω της ανάπτυξης του 5G θα υλοποιηθεί η εισαγωγή εφαρμογών AR/VR στους τομείς ψυχαγωγίας και διασκέδασης ικανοποιώντας σύγχρονες τάσεις των καταναλωτών (π.χ. δημιουργία «έξυπνων» γηπέδων, smart stadiums). Η χαμηλή λανθάνουσα κατάσταση και η απόδοση του δικτύου αποτελούν κυρίαρχα χαρακτηριστικά που θα βελτιωθούν μέσω των δικτύων 5G με ταχύτητες μετάδοσης 50Mbit/s και καθυστέρηση 50 ms (NOKIA, 2016; Stone, χ.η.).

3.3.4 Έξυπνα δίκτυα

Η τεχνολογία 5G βρίσκει εφαρμογή στα δίκτυα παραγωγής και διανομής ενέργειας (smart grids). Συγκεκριμένα, τα συστήματα αυτομάτου ελέγχου για τον εντοπισμό βλαβών και σφαλμάτων θέτουν ως τεχνική προϋπόθεση για τη λειτουργία τους την άμεση επικοινωνία ανάμεσά τους εντός του δικτύου (Zhuo et al., 2010).

Έτσι, επιτυγχάνεται η έγκαιρη ενεργοποίηση των εντολών διακοπής λειτουργίας σε ενδεχόμενα ανίχνευσης σφαλμάτων. Με αυτόν τον τρόπο, οι γρήγορες ταχύτητες στο 5G και η άμεση απόκριση με εξαιρετικά μικρές καθυστερήσεις αποτελούν σημαντικό εργαλείο για την εξασφάλιση μεγάλη αποτελεσματικότητας.

Παράλληλα, η μεγάλη ταχύτητα ανταλλαγής των δεδομένων στην τεχνολογία 5G διευκολύνει την αυτόματη ενεργοποίηση για τη διακοπή της παραγωγής όταν αυτό απαιτείται. Αυτό έχει ως αποτέλεσμα την εξοικονόμηση στην κατανάλωση της ενέργειας και τον περιορισμό της μηχανικής καταπόνησης των συστημάτων.

Ακόμη, η καλωδίωση που υπάρχει για τον έλεγχο των έξυπνων δικτύων θα αντικατασταθεί σύμφωνα με την τεχνολογία των δικτύων 5G από ταχύτατα μηνύματα ελέγχου μετάδοσης. Κατ' αυτόν τον τρόπο, η διακοπή της λειτουργίας των έξυπνων δικτύων γίνονται με τρόπο κατανεμημένο και αξιόπιστο.

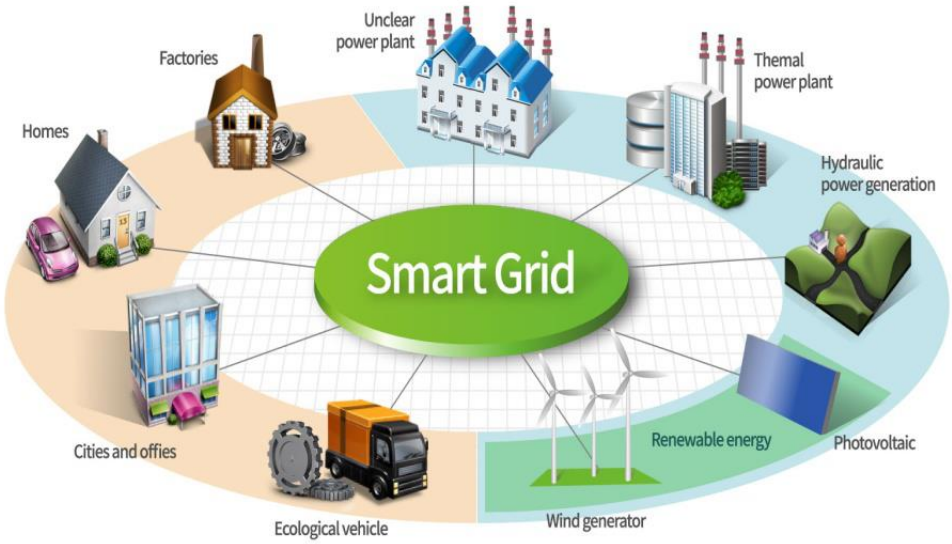
Σε ενδεχόμενες βλάβες, κατά την ανίχνευση τους, το δίκτυο θα δύναται να αναδιαρθρωθεί άμεσα με αποτέλεσμα να μειώνεται σημαντικά ο χρόνος αποκατάστασης και το δίκτυο να διατηρεί την αξιοπιστία του (Michom, 2018).

Επιπροσθέτως, στα έξυπνα δίκτυα χρησιμοποιούνται οι έξυπνοι μετρητές, οι οποίοι έχουν το ρόλο της πραγματοποίησης μετρήσεων αναφορικά με την κατανάλωση ενέργειας χωρίς την απαίτηση φυσικής παρουσίας του προσωπικού του κάθε παρόχου. Η λειτουργία των έξυπνων μετρητών βασίζεται στον έλεγχο της κατανάλωσης της ηλεκτρικής ενέργειας σε πραγματικό χρόνο και στον υπολογισμό του κόστους που προκύπτει από τη λειτουργία των ηλεκτρικών συσκευών.

Έτσι, οι έξυπνοι μετρητές συμβάλλουν στην βέλτιστη χρήση και διαχείριση των συσκευών, ώστε τελικώς να μειώνεται η κατανάλωσης της ενέργειας, ενώ ταυτόχρονα παρέχονται οι απαιτούμενες πληροφορίες για όλες τις βαθμίδες του εξοπλισμού, ώστε να αποφεύγονται διαρροές ή υπερκαταναλώσεις ενέργειας. Οι εν λόγω πληροφορίες

μπορούν να μεταδοθούν με τη χρήση ενός κινητού ή ενός tablet συνδεδεμένα σε ένα δίκτυο 5G.

Συνεπώς, οι έξυπνοι μετρητές στα δίκτυα διανομής ενέργειας, με την παράλληλα υλοποίηση των δικτύων 5G, δύναται να συμβάλει στην περαιτέρω ταχεία μετάδοση και επεξεργασία των δεδομένων, βελτιώνοντας την απόδοση της υφιστάμενης υποδομής παροχής Χαμηλής Τάσης (ΧΤ) και Μέσης Τάσης (ΜΤ) (Dieudonne et al., 2016).



Εικόνα 3.4: Δίκτυο smart grid

(Πηγή: https://www.e-mc2.gr/el/vivliothiki/eidikes-tehnologies-kai-efarmoges-special-technologies-and-innovative-applications-3)

3.3.5 Ρομποτική

Στο πλαίσιο της αύξησης της παραγωγικότητας και της αποδοτικότητας των γραμμών παραγωγής, προκύπτει η ανάγκη βελτιστοποίησης των επιδόσεων των επιμέρους λειτουργιών σε πραγματικό χρόνο, των διακυμάνσεων της ποιότητας των παραγόμενων προϊόντων, των παρεμβάσεων που απαιτούνται από τους χειριστές καθώς και όλων των μεταβλητών παραγόντων του βιομηχανικού περιβάλλοντος εν γένει. Η σύγκριση των κινητών ρομπότ με τους αισθητήρες έγκειται στο γεγονός ότι τα πρώτα απαιτούν υψηλό ρυθμό μετάδοσης, προκειμένου για αξιόπιστη επικοινωνία, ενώ οι δεύτεροι επικοινωνούν

με χαμηλότερο ρυθμό μετάδοσης αλλά με εξαιρετικά χαμηλή καθυστέρηση. Η απαίτηση για άμεση, χαμηλής καθυστέρησης επικοινωνία μεταξύ των μηχανών, οδηγεί σε καινούριες λειτουργίες της νέας γενιάς ρομπότ, όπως είναι η εισαγωγή φορετών συσκευών ελέγχου (wearables) και συσκευών επαυξημένης πραγματικότητας. Η ανάγκη για γρήγορη μετάδοση μεγάλου όγκου δεδομένων οδηγεί στων σχεδιασμό περισσότερων ασύρματων ή κινητών συσκευών στο μέλλον. Τόσο η ταχύτητα όσο και ο όγκος των πληροφοριών που πρέπει να μεταδοθούν και να επεξεργαστούν ώστε να διασφαλιστεί η έγκαιρη λήψη κατάλληλων αποφάσεων αποτελούν στοιχεία μείζονος σημασίας.

Ως προς αυτή την κατεύθυνση η ύπαρξη συνεργατικών ρομπότ θα βελτιώσει περαιτέρω την αυτοματοποίηση, την απόδοση και την ποιότητα της παραγωγής. Τα δίκτυα 5G αναμένεται να διαδραματίσουν καθοριστικό ρόλο, στα παραπάνω παρέχοντας εξαιρετικά γρήγορη και αξιόπιστη πρόσβαση (Stone, χ.η.; METIS, 2014).

3.3.6 Το Έξυπνο γραφείο

Η συγκεκριμένη περίπτωση χρήσης χαρακτηρίζεται από τις εσωτερικές επικοινωνίες στα διαμερίσματα και σε κτίρια γραφείων με μεγάλη πυκνότητα συσκευών. Βραχυπρόθεσμα εκτιμάται ότι οι περισσότερες συσκευές θα συνδέονται ασύρματα και οι χρήστες θα αλληλεπιδρούν μέσω αυτών. Αυτό υποδηλώνει ένα σενάριο στο οποίο εκατοντάδες χρήστες θα είναι συνδεδεμένοι και θα εκτελούν εφαρμογές οι οποίες απαιτούν εξαιρετικά υψηλό εύρος ζώνης, υψηλό ρυθμό μετάδοσης δεδομένων, άμεση επεξεργασία μεγάλου όγκου δεδομένων στο νέφος, και real time επικοινωνία μέσω βίντεο. Η διακίνηση μεγάλου όγκου πληροφορίας με υψηλό ρυθμό δεδομένων αποτελεί βασική επιδίωξη του 5G. Η εκτίμηση είναι ότι ο ρυθμός ασύρματης μετάδοσης των δεδομένων θα ξεπεράσει το 1 Gbps (cosmote, χ.η.).

Και στην περίπτωση του έξυπνου γραφείου, η τεχνολογία IoT μπορεί να παράσχει ένα ιδιαίτερα έξυπνο μοντέλο γραφείου, συμβάλλοντας στην δημιουργία ενός αποτελεσματικού εργασιακού περιβάλλοντος και εστιάζοντας στις εξής πτυχές (Alhajri et al., 2021):

- στον απομακρυσμένο έλεγχο όλων των συσκευών στο γραφείο μέσω ενός smartphone
- στην αυξημένη ασφάλεια.

Συγκεκριμένα, οι Alhajri et al. (2021) πρότειναν το μοντέλο προσομοίωσης με την χρήση του Cisco Packet Tracer που περιλαμβάνει ποικίλες δυνατότητες και λειτουργίες IoT. Σύμφωνα με την προσομοίωση, η εφαρμογές έξυπνων γραφείων προσφέρουν ένα ιδιαίτερα αποτελεσματικό περιβάλλον εργασίας.

3.3.7 Το διάχυτο βίντεο

Στην εποχή μας και ιδιαίτερα τα τελευταία χρόνια με την εξάπλωση του Covid19 προέκυψε η ανάγκη επικοινωνίας μεταξύ των χρηστών με χρήση βίντεο υψηλής ανάλυσης. Το γεγονός αυτό εντείνει την ανάγκη για γρήγορο και αξιόπιστο δίκτυο χωρίς χρονικές καθυστερήσεις. Στο πλαίσιο αυτό ολοένα και περισσότερες εταιρείες χρησιμοποιούν ευρέως τις βιντεοκλήσεις ως αναπόσπαστο μέσω επικοινωνίας μεταξύ των στελεχών και των εργαζομένων. Οι προηγμένες δυνατότητες που παρέχει η τεχνολογία 5G για μετάδοση δεδομένων οπτικής απεικόνισης θέτουν νέες προοπτικές στον επαγγελματικό τομέα. Ενδεικτικά παραδείγματα αποτελούν:

- Η παροχή απομακρυσμένης εργασίας - τηλεργασία π.χ. μέσω της εφαρμογής απομακρυσμένης πρόσβασης στην επιφάνεια εργασίας του χρήστη
- Η πραγματοποίηση εξ' αποστάσεως συνεδριάσεων μέσω 3D απεικόνισης
- Η υποστήριξη πελατών μέσω υπηρεσιών ολογράμματος
- Η παροχή απομακρυσμένης εκπαίδευσης - τηλεκπαίδευση μέσω εγγραφής και εισόδου σε ειδική πλατφόρμα.

Όπως συνάγεται από τα παραπάνω, διαρκώς σχεδιάζονται εφαρμογές και προγράμματα τα οποία θα παρέχουν σε όλους τους χρήστες πρόσβαση και διαθεσιμότητα, ανεξαρτήτως φυσικής τοποθεσίας, δικτύου και συσκευής. Τέλος, τα δίκτυα τεχνολογίας 5G μπορούν να πραγματοποιήσουν επιτυχώς μεγάλο αριθμό ταυτόχρονων ενεργών συνδέσεων, χωρίς να μειώνεται ο απαιτούμενος ρυθμός απόδοσης (Stone, χ.η.; METIS, 2014).

3.3.8 Μαζική συγκέντρωση

Έχει παρατηρηθεί ότι σε περιοχές, όπου λαμβάνουν χώρα μαζικές εκδηλώσεις (π.χ. ένα στάδιο ή ένας μεγάλος συναυλιακός χώρος), ανταλλάσσεται μεγάλος όγκος δεδομένων

από τους χρήστες που βρίσκονται συγκεντρωμένοι εκεί. Επομένως την χρονική περίοδο που πραγματοποιείται η συγκέντρωση, οι απαιτήσεις για μεταφορά δεδομένων αυξάνονται κατακόρυφα με αποτέλεσμα οι πάροχοι, να πρέπει να έχουν εξασφαλισμένο εύρος ζώνης, προκειμένου να καλύψουν τις τρέχουσες και πρόσκαιρες ανάγκες.

Στο πλαίσιο αυτό, η τεχνολογία 5G παρέχει εξαιρετικά μεγάλες ταχύτητες σε σχέση με το 4G (ακόμα και αν οι απαιτήσεις είναι υψηλού ρυθμού δεδομένων) και με καλύτερο GoS (qualcomm, χ.η.).

3.3.9 Βίντεο υψηλής ευκρίνειας

Η επικράτηση της τάσης των χρηστών να καταγράφουν ολοένα και συχνότερα, μέσω κινητών συσκευών περιεχόμενο όπως βίντεο 4k, αποτελεί πεδίο εφαρμογής του δίκτυο 5G. Το δίκτυο πέμπτης γενιάς μπορεί να υποστηρίξει την υψηλή ζήτηση εύρους ζώνης και την συνεχή ροή από διάφορες συσκευές με σκοπό την βελτίωση της εμπειρίας των χρηστών (ΑΠΘ, 2022).

3.3.10 Εφαρμογές στην καταναλωτική αγορά, Gaming Media on Demand

Αδιαμφισβήτητα, το eMBB αναμένεται διαδραματίσει βασικό ρόλο στις αρχικές φάσεις της διάθεσης του 5G, καθώς η ασύρματη ευρυζωνική σύνδεση για φορητές συσκευές χειρός και σταθερούς χρήστες σε απομακρυσμένες περιοχές (FWA) αποτελεί βασικό κίνητρο για την εξέλιξη αυτής της τεχνολογίας. Με πρόσθετη υποστήριξη mmWave, το 5G CPE δύναται να προσφέρει ταχύτητα και αξιοπιστία συγκρίσιμη με των οπτικών ινών. Η ζήτηση για μεγαλύτερο εύρος ζώνης, υψηλό ρυθμό μετάδοσης δεδομένων για ροή βίντεο (HD, SOHO κ.α) διαρκώς αυξάνεται στο πλαίσιο υπηρεσιών και εφαρμογών που απαιτούν υψηλή κίνηση δεδομένων όπως το τρισδιάστατο παιχνίδι και η επαυξημένη πραγματικότητα, καθιστά επιβεβλημένη την ανάπτυξη και τη διάδοση της τεχνολογίας 5G (Alimi et al., 2021).

3.3.11 Εφαρμογή 5G IoT στην Έξυπνη Υγεία

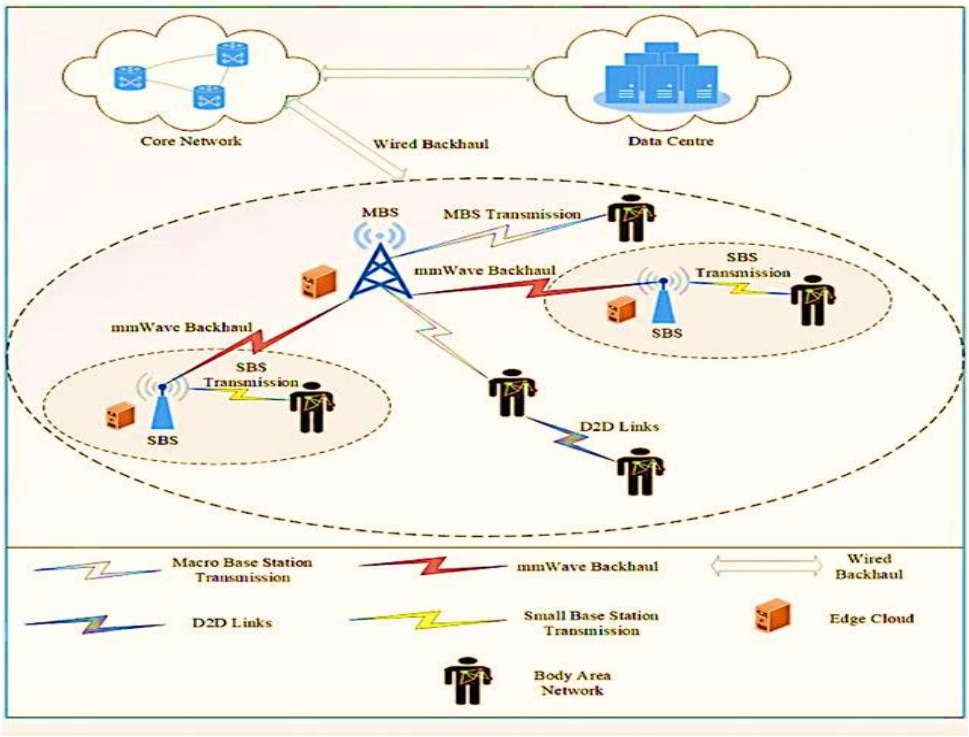
Το eMBB και το URLLC που υποσχέθηκε το 5G έδωσε πρακτικές λύσεις στον κλάδο της υγειονομικής περίθαλψης. Με το δίκτυο πέμπτης γενιάς οι φορητές συσκευές παρακολούθησης και οι κάμερες HD θα μπορούν πλέον να πληρούν απόλυτες, σε πραγματικό χρόνο προδιαγραφές, επιτρέποντας απομακρυσμένες διαβουλεύσεις ροής και την αντιμετώπιση έκτακτων αναγκών χωρίς καθυστέρηση. Τα δίκτυα 5G παρέχουν εφικτές λύσεις και υλοποιήσιμες πρακτικές υψηλών απαιτήσεων όπως για παράδειγμα η τηλεχειρουργική με τη βοήθεια ρομποτικών βραχιόνων. Η αδιάλειπτη διαθεσιμότητα του δικτύου 5G παρέχει το πλεονέκτημα παροχής πρόσθετων υγειονομικών υπηρεσιών όπως υγειονομική φροντίδα στο σπίτι κυρίως για άτομα με αναπηρίες και ηλικιωμένους. Το 5G τροποποιεί το υπάρχον περιβάλλον IoMT ενισχύοντας το εύρος ζώνης δεδομένων και περιορίζοντας την καθυστέρηση προσφέροντας εμπειρίες υψηλότερης αξιοπιστίας στις φορητές συσκευές και στη ροή βίντεο.

Το σύστημα ηλεκτρονικής υγειονομικής περίθαλψης (e-health) συγκεντρώνει ολοένα και περισσότερο το ερευνητικό ενδιαφέρον, καθώς επιτρέπει στους χρήστες της ηλεκτρονικής υγείας να αποθηκεύουν και να μοιράζονται δεδομένα με ευκολία. Βάσει της τεχνολογίας 5G, τα δεδομένα υγειονομικής περίθαλψης που παράγονται από κόμβους αισθητήρων μεταφέρονται στο σύστημα ηλεκτρονικής υγείας με υψηλή απόδοση και αξιοπιστία. Το γεγονός αυτό συμβάλει στη μείωση του κόστους θεραπείας, στην βελτίωση των παρεχόμενων υπηρεσιών, στην αποτελεσματικότερη ανάλυση των δεδομένων και στην ταχύτερη πρόσβαση στη θεραπεία. Ωστόσο, θα πρέπει να τονίσουμε ότι καθώς αυξάνεται ο αριθμός των αισθητήρων και των φορητών συσκευών προκύπτουν ζητήματα ασφάλειας και διαφύλαξης του απορρήτου. Επίσης, η υπάρχουσα αρχιτεκτονική του διακομιστή απαιτεί την αποθήκευση ενός υπέρογκου αριθμού ταυτοτήτων και κωδικών πρόσβασης, με αποτέλεσμα να αυξάνεται το κόστος της βάσης δεδομένων. Προς αυτή την κατεύθυνση, προτείνεται ένα σύστημα γρήγορου ελέγχου ταυτότητας τριών παραγόντων, με χρονικό περιορισμό και ανωνυμία χρήστη για συστήματα ηλεκτρονικής υγείας πολλών διακομιστών σε ασύρματα δίκτυα αισθητήρων που βασίζονται στο 5G (Wong et al., 2020).

Το σύστημα ελέγχου ταυτότητας τριών παραγόντων ενσωματώνει βιομετρικά στοιχεία, κωδικό πρόσβασης και έξυπνη κάρτα μέσω των οποίων διασφαλίζει σε μεγάλο βαθμό η

ασφάλεια. Η ανωνυμία του χρήστη διατηρείται κατά τη διαδικασία επικοινωνίας. Ταυτόχρονα, ο έλεγχος ταυτότητας με χρονική δέσμευση είναι εφαρμόσιμος σε διάφορα σενάρια υγειονομικής περίθαλψης για τη βελτίωση της ασφάλειας. Το εν λόγω προτεινόμενο πρωτόκολλο περιλαμβάνει γρήγορο έλεγχο ταυτότητας, ο οποίος μπορεί να παρέχει γρήγορη επικοινωνία των συμμετεχόντων μερών. Το πρωτόκολλο είναι σχεδιασμένο με αρχιτεκτονική πολλών διακομιστών προκειμένου να διαχειριστεί το φόρτο του δικτύου και να μειώσει το κόστος της βάσης δεδομένων (Wong et al., 2020).

Όπως φαίνεται στην παρακάτω εικόνα, (Εικόνα 3.5) οι macro σταθμοί βάσης (MBS) του 5G παρέχουν backhaul κυμάτων mm στους σταθμούς βάσης μικρών κυψελών (SBS). Οι συσκευές μπορούν να έχουν πρόσβαση τόσο στο MBS όσο και στα SBS.



Εικόνα 3.5: Έξυπνη αρχιτεκτονική υγειονομικής περίθαλψης βασισμένη στο 5G

(Πηγή: Wong et al., 2020)

Η χρήση του IoT σε συστήματα ηλεκτρονικής διαχείρισης υγειονομικής περίθαλψης (e-health) προσφέρει εύκολη αποθήκευση και διαμοιρασμό των δεδομένων υγειονομικής περίθαλψης μεταξύ των συμμετεχόντων. Ένα τέτοιο σύστημα ονομάζεται IoMT (Internet of Medical Things) και αποτελείται από διάφορες οντότητες, ανάμεσα στις οποίες κέντρα

υγειονομικής περίθαλψης, κέντρα έκτακτης ανάγκης, ιατρικές συσκευές και χρήστες ηλεκτρονικής υγείας π.χ. ασθενείς, γιατροί, φαρμακοποιοί, κ.τ.λ.

3.3.12 Εφαρμογές για τα οχήματα

Τα ηλεκτρικά οχήματα καταλαμβάνουν ολοένα και περισσότερο χώρο στα σχεδιαστικά προγράμματα των αυτοκινητοβιομηχανιών. Η ενεργειακή κρίση, η ρύπανση του περιβάλλοντος, η ανάπτυξη ηλεκτρονικών ισχύος καθώς και η κατασκευή νέων συσσωρευτών αυξημένης πυκνότητας ενέργειας οδήγησαν στην ενσωμάτωση των ηλεκτρικών οχημάτων στα ενεργειακά συστήματα. Η ανάπτυξη της τεχνολογίας 5G θα ενισχύσει σημαντικά τον τομέα της ενέργειας μέσω των ηλεκτρικών οχημάτων σε όλες τις χώρες. Ενδεικτικό παράδειγμα αποτελεί η Ιρλανδία όπου εξαιτίας της μεγάλης αιολικής ενέργειας που διαθέτει ανακοίνωσε ότι θα απαγορεύσει την πώληση βενζινοκίνητων και πετρελαιοκίνητων αυτοκινήτων ως το 2030, καθώς θα κυκλοφορούν μόνο ηλεκτρικά οχήματα. Η πρακτική αυτή θα αποτελέσει ένα από τα μέτρα που θα υιοθετήσει με σκοπό την προστασία του περιβάλλοντος. Η φόρτιση των ηλεκτρικών οχημάτων με χρήση ανανεώσιμων πηγών ενέργειας θα μειώσει δραστικά της επιπτώσεις παραγωγής CO_2. Η συμβολή των δικτύων 5G έγκειται στο γεγονός ότι για τον προσδιορισμό των αναγκών φόρτισης των ηλεκτρικών οχημάτων, απαιτείται επικοινωνία μεταξύ των σταθμών φόρτισης με τα ηλεκτρικά οχήματα.

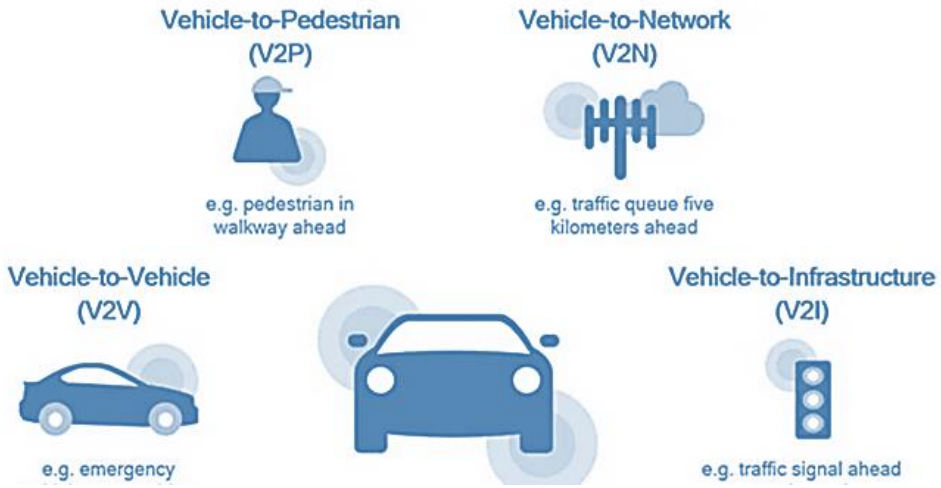
Τα δίκτυα 5G θα συνδράμουν στην αξιόπιστη επικοινωνία των παραπάνω μερών και στην εξαιρετικά μικρή καθυστέρηση επικοινωνίας παρέχοντας ένα μεγάλο φάσμα επιλογών για την παροχή νέων υπηρεσιών και τη βελτιστοποίηση της ενεργειακής υποδομής.

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι λόγω του ότι η τεχνολογία IOT εισάγει μία διεύθυνση IPv6 ανά κάθε συσκευή συνδέοντάς την στο διαδίκτυο. Για παράδειγμα στα δίκτυα (smart grid) οχημάτων, για τη μεταφορά των πληροφοριών, η επικοινωνία διεξάγεται μεταξύ των οχημάτων και των σημείων πρόσβασης, καθώς επίσης και μεταξύ των σημείων πρόσβασης. Οι απαιτήσεις της επικοινωνίας είναι μεγάλες:

- επίγνωση τοποθεσίας,
- ασύρματη σύνδεση,
- ταχύτατη επεξεργασία των δεδομένων,

- real time αλληλεπίδραση μεταξύ των οχημάτων και
- ανταπόκριση στην κινητικότητα των οχημάτων.

Επίσης, τα διασυνδεδεμένα οχήματα συγκεντρώνουν μεγάλο τεχνολογικό ενδιαφέρον και προκύπτει από την διαθεσιμότητα του 5G δικτύου, είναι τα συνδεδεμένα οχήματα, δηλαδή τα αυτοκίνητα που είναι διαρκώς συνδεδεμένα τόσο μεταξύ τους όσο και με τις υποδομές. Μέσω του δικτύου 5G θα παρέχονται άμεσα όλες οι απαραίτητες πληροφορίες, ώστε ο οδηγός ή ο αυτόματος πιλότος να λαμβάνει τη σωστή ανά περίσταση απόφαση (Thrybom & Kapovits, 2015; Smart Cities World news team, 2017).



Εικόνα 3.6: Αυτόνομη οδήγηση

(Πηγή: https://enterpriseiotinsights.com/20160609/5g/qualcomm-autonomous-driving-5g-tag17)

Μέσα από μελέτες που πραγματοποιήθηκαν, αποδείχθηκε ότι μέσα από την παραπάνω εφαρμογή αυξάνεται σημαντικά η ασφάλεια των οδηγών και μειώνεται κατά πολύ η πιθανότητα πρόκλησης τροχαίων ατυχημάτων. Παράλληλα, επιτυγχάνεται αποτελεσματικότερη ρύθμιση της κυκλοφορίας επιτρέποντας την απρόσκοπτη κυκλοφορία οχημάτων έκτακτης ανάγκης όταν απαιτείται. Ωστόσο είναι ιδιαίτερα κρίσιμο να πούμε ότι οι εν λόγω εφαρμογές προϋποθέτουν μεγάλη αξιοπιστία, υψηλούς ρυθμούς μετάδοσης και εξαιρετικά χαμηλές καθυστερήσεις καθώς αφορούν σήματα προειδοποίησης, ανταλλαγή πληροφοριών αισθητήρων καθώς και πληροφοριών ανάμεσα σε οχήματα και υποδομές. Αναφορικά με τα μέρη που μπορούν να επικοινωνούν

με το όχημα, το στο 3GPP ορίζει τις κάτωθι περιπτώσεις (rgbsi, χ.η.):

- όχημα προς όχημα (Vehicle to vehicle-V2V)
- όχημα προς υποδομή (Vehicle to Infrastructure-V2I)
- όχημα προς δίκτυο (Vehicle to Network-V2N)
- όχημα προς το πεζοδρόμιο (Vehicle to Pedestrian-V2P)

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΣΥΖΗΤΗΣΗ

Είναι σαφές ότι η τεχνολογία 5G διαφοροποιείται δυναμικά ως προς τις επιδόσεις και τα χαρακτηριστικά της σε σχέση με τις παλαιότερες τεχνολογίες (ακόμη και το 4G). Δεν είναι υπερβολή αν ειπωθεί ότι τα δίκτυα τεχνολογίας 5G αποτελούν μια κολοσσιαία τεχνολογική επανάσταση.

Στη σύγχρονη εποχή που οι απαιτήσεις για ταχύτητα στη διαχείριση μεγάλου όγκου δεδομένων είναι τεράστιες, το 5G είναι ικανό να παρέχει πολλαπλές υπηρεσίες, καταφέρνοντας να ικανοποιήσει κάθε ανάγκη.

Ταυτόχρονα, να σημειωθεί ότι η επιστημονική κοινότητα σε συνεργασία με τις μεγάλες εταιρίες τηλεπικοινωνιακών συστημάτων, ήδη βρίσκονται σε στάδιο πιλοτικής εφαρμογής του 6G και ετοιμάζονται να κάνουν ένα ακόμη εντυπωσιακό άλμα, δίνοντας ώθηση σε κάθε ανθρώπινη δραστηριότητα.

Επιπλέον, θα πρέπει να σημειωθεί ότι διαρκώς βρίσκεται όλο και πιο κοντά η ανάπτυξη και υλοποίηση της τεχνητής νοημοσύνης σε συνδυασμό με το 5G. Βάσει των σημερινών δεδομένων, θα αποτελέσει καταλυτικό παράγοντα στη διαμόρφωση των σύγχρονων ασύρματων τηλεπικοινωνιών. Επομένως, το 5G είναι η κινητήριος δύναμη για μια σειρά εφαρμογών που αφορούν στην νοημοσύνη της μηχανής (machine intelligence).

Καθίσταται, λοιπόν, προφανές ότι η τεχνολογία των ασύρματων επικοινωνιών καλπάζει, με το 5G να μην αποτελεί απλώς την εξέλιξη του 4G, αλλά μια τεχνολογία μοναδική που ξεφεύγει από τα προγενέστερα μοντέλα. Τα νούμερα είναι πλέον δυσθεώρητα και οι επιδόσεις ασύλληπτες. Ενδεικτικά, κάθε σταθμός τεχνολογίας 5G είναι σχεδιασμένος για να διαχειρίζεται έως και 1 εκ. συνδέσεις. Αρκεί να αναλογιστεί κανείς ότι ένας σταθμός

4G μπορεί να διαχειριστεί έως περίπου 4.000 συνδέσεις ταυτόχρονα. Η ταχύτητα στο μέλλον, εκτιμάται ότι θα προσεγγίσει το 1 Tbps!!!

Ακριβώς, γι' αυτό το λόγο, τα συστήματα 5G αναμένεται να αλλάξουν ριζικά το τοπίο στην τεχνολογία και την καθημερινότητα, δίνοντας ώθηση σε τεχνολογίες, όπως η IoT.

Επιπρόσθετα, στα συστήματα 5G ο χρόνος καθυστέρησης είναι 50 φορές μικρότερος σε σχέση με των συστημάτων 4G. Με άλλα λόγια είναι 50 φορές γρηγορότερα.

Ταυτόχρονα, οι παρεχόμενες υπηρεσίες απαιτούν περίπου 10 φορές μικρότερη κατανάλωση ενέργειας. Το γεγονός αυτό καθιστά την τεχνολογία 5G φιλική προς το περιβάλλον, ιδανική για την πράσινη και βιώσιμη ανάπτυξη και την προστασία του πλανήτη. Επιπλέον, η διάρκεια ζωής των μπαταριών των συσκευών είναι περίπου 10 φορές μεγαλύτερη.

Εντούτοις, τίθενται και νέα σοβαρά ζητήματα, όπως η ασφάλεια των δικτύων και η ανάπτυξη αντίμετρων στις διαρκώς αυξανόμενες κι επικίνδυνες επιθέσεις.

Είναι γεγονός ότι εφόσον ο σκοπός είναι το κέρδος σε αύξηση εύρους ζώνης και ταχύτητας, τότε συνήθως υφίσταται αντίκτυπο στην ασφάλεια. Αυτό σημαίνει ότι οι ειδικοί θα πρέπει να δώσουν έμφαση στον εν λόγω τομέα, ώστε να βελτιστοποιήσουν την ασφάλεια και την ακεραιότητα των δεδομένων που διακινούνται.

Κι επειδή, όπως αναφέρθηκε, εμπλέκονται πολλά συστήματα σε συνδυασμό με το 5G, θα πρέπει να εξασφαλίζεται η ορθή λειτουργία τους. Με άλλα λόγια, θα πρέπει να εξεταστούν σε βάθος όλοι οι περιορισμοί που περιέχει η τεχνολογία 5G και να υπάρξει σχετική μέριμνα, αντιμετώπισης κάθε τεχνητού ζητήματος.

Συμπερασματικά, η τεχνολογία 5G, πραγματικά, εντυπωσιάζει. Ωστόσο, οι ασφαλείς αλληλεπιδράσεις μεταξύ των συσκευών σε τόσο μεγάλες κλίμακες εξελιγμένων δικτύων, όπως είναι το δίκτυο 5G, είναι άκρως απαραίτητες, προκειμένου να διασφαλίζεται η ομαλή λειτουργία των ιδιαίτερα μεγάλων και πολύπλοκων συστημάτων. Ακριβώς αυτό το σημείο, φαίνεται ότι χρήζει περαιτέρω διερεύνησης για τη μελλοντική βελτιστοποίηση του 5G.

ΚΑΤΑΛΟΓΟΣ ΑΝΑΦΟΡΩΝ

1. Wicks, A. & Kemerling, J. (2003). *A brief early history of wireless technology.* Experimental Techniques - EXP TECH. 27. 57 – 58. DOI: 10.1111/j.1747-1567.2003.tb00140.x

2. Shen, W., Yin, B., Liu, L., Cao, X., Cheng, Y., Li, Q. & Wang, W. (2016). *Secure In-Band Bootstrapping for Wireless Personal Area Networks*. IEEE Internet of Things Journal. Vol. 3. No. 6. pp. 1385-1394. doi: 10.1109/JIOT.2016.2604221.

3. Salman, A. (2020). *What is a LAN, WLAN? Definition, Types, Pros and Cons*. Διαθέσιμο στο: https://www.techloversahmad.com/what-is-lan-wlan-definition-types/ [Τελευταία πρόσβαση στις 01.04.22]

4. Soewito, A.B., Gunawan, F.E. & Mansuan, M.S. (2017). *WAN Optimization to Speed up Data Transfer*. Procedia Computer Science. 116. 45-53., Elsevier. https://doi.org/10.1016/j.procs.2017.10.007.

5. Firdhous, M., Ghazali, O., Hassan, S. (2014). *Fog Computing: Will it be the Future of Cloud Computing?* Proceedings of the Third International Conference on Informatics & Applications, Kuala Terengganu, Malaysia. Διαθέσιμο στο: https://www.researchgate.net/publication/266477246_Fog_Computing_Will_it_be_the_Future_of_Cloud_Computing [Ανακτήθηκε στις 28.03.22]

6. Grossglauser, M. & Tse, D.N.C. (2002). *Mobility increases the capacity of ad hoc wireless networks*. IEEE/ACM Transactions on Networking. 10(4). 477-486. DOI: 10.1109/TNET.2002.801403

7. Rappaport, T. (2006). *Ασύρματες επικοινωνίες - Αρχές και πρακτική*. 2η Έκδοση. Αθήνα: Γκιούρδας

8. Albert, L. & Indra, W. (2000). Communication Networks. *McGraw-Hill Higher Education*.

9. Ευρωπαϊκό Ελεγκτικό Συνέδριο (2022). *Ειδική Έκθεση Ευρωπαϊκού Ελεγκτικού Συνεδρίου, Τεχνολογία 5G στην ΕΕ*. Διαθέσιμο στο: https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EL.pdf [Ανακτήθηκε στις 02.04.22]

10. Eridy, L. (2015). *5G Cellular Network for Machine to Machine Communication*. DOI: 10.13140/RG.2.1.4193.3520. Διαθέσιμο στο: https://www.researchgate.net/profile/Eridy-Lukau-2/publication/273956487_5G_Cellular_Network_for_Machine_to_Machine_Communication/links/551164930cf21209d5286e73/5G-Cellular-Network-for-Machine-to-Machine-Communication.pdf?origin=publication_detail [Ανακτήθηκε στις 02.04.22]

11. Kumari, K.A., Sadasivam, G.S., Gowri, S.S., Akash, S.A. & Radhika, E.G. (2018). *An Approach for End-to-End (E2E) Security of 5G Applications*. IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity). IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS). 133-138, doi: 10.1109/BDS/HPSC/IDS18.2018.00038.

12. Parvez, I., Rahmati, A., Guvenc, I., Sarwat, A.I & Dai, H. (2018). *A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions*. IEEE Communications. Surveys & Tutorials. 20. 4. 3098 - 3130. https://doi.org/10.1109/COMST.2018.2841349

13. ETSI (2017). *5G: Study on new radio access technology (3GPP TR 38.912 version 14.1.0 Release 14) TR 38.804, Study on New Radio Access Technology; Radio Interface Protocol Aspects, Rel-14*. Διαθέσιμο στο: https://www.etsi.org/deliver/etsi_tr/138900_138999/138912/14.01.00_60/tr_138912v140100p.pdf [Ανακτήθηκε στις 05.04.22]

14. ETSI (2020). *ETSI TS 123 501 V16.6.0 (2020-10), 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16)*. Διαθέσιμο στο: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf [Ανακτήθηκε στις 03.04.22]

15. Keenan, M. (2020). *The evolution of cellular networks*. Διαθέσιμο στο: https://www.avnet.com/wps/portal/abacus/resources/article/the-evolution-of-cellular-networks/ [Τελευταία πρόσβαση στις 23.04.21]

16. Chan, A. S. (2018). *A brief history of 1G mobile communication technology*. https://blog.xoxzo.com/en/2018/07/24/history-of-1g/.

17. Munir, M. W. (2005). *Different Generations of Cellular Networks System*. Διαθέσιμο στο: https://www.researchgate.net/publication/276319644_Different_Generations_of_Cellular_Networks_System/references [Ανακτήθηκε στις 15.04.22]

18. Temple, S. (2010). *Inside the Mobile Revolution: a Political History of GSM*. Διαθέσιμο στο: http://www.gsmhistory.com/wp-content/uploads/2013/01/Inside-a-Mobile-Revolution-Temple-20101.pdf [Ανακτήθηκε στις 10.04.22]

19. Hussain, S.S., Yaseen, S.M. & Barman, K. (2016). *An overview of massive mimo system in 5G*. JCTA - International Science Press. 9(11). 4957 - 4968

20. Holma, H. & Toskala, A. (2010). *LTE for UMTS: Evolution to LTE-Advanced*. 2nd Edition, John Wiley & Sons Ltd.

21. Nawaz, S.J., Sharma, S.K., Wyne, S., Patwary, M.N. & Asaduzzaman, M. (2019). *Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future*. IEEE Access. 7. 46317-46350. doi: 10.1109/ACCESS.2019.2909490.

22. Moskowitz, J. (2019). *5G Wireless Technology: Millimeter Wave Health Effects*. Center for Family and Community Health School of Public Health University of California, Berkeley.

23. Carugi, M. (2018). *Key features and requirements of 5G/IMT-2020 networks*. ITU Arab Forum on Emerging Technologies. Algeria. Διαθέσιμο στο: https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2018/RDF/Workshop%20Presentations/Session1/5G-%20IMT2020-presentation-Marco-Carugi-final-reduced.pdf [Ανακτήθηκε στις 09.04.22]

24. Sivalingam, T., Kapuruhamy Badalge, S., Dissanayake, M. & Rajatheva, N. (2019). *Positioning of Multiple Unmanned Aerial Vehicle Base Stations in future Wireless Network.* DOI: 10.13140/RG.2.2.20596.50568. Διαθέσιμο στο: https://www.researchgate.net/profile/Thushan-Sivalingam/publication/335826943_Positioning_of_Multiple_Unmanned_Aerial_Vehicle_Base_Stations_in_future_Wireless_Network/links/5d7dffc34585155f1e4deb

cb/Positioning-of-Multiple-Unmanned-Aerial-Vehicle-Base-Stations-in-future-Wireless-Network.pdf?origin=publication_detail [Ανακτήθηκε στις 15.04.22]

25. Gupta, A. & Jha, R.K. (2015). *A Survey of 5G Network: Architecture and Emerging Technologies*. IEEE Access, 3, 1206-1232, doi: 10.1109/ACCESS.2015.2461602.

26. Zheng, M., Zhengquan, Z., Zhiguo, D., Pingzhi, F., HengChao, L. (2015). *Key techniques for 5G wireless communications: Network architecture, physical layer, and MAC layer perspectives.* China Information Sciences. 58, 1-20. DOI: 10.1007/s11432-015-5293-y.

27. Kumar, N. & Anwar, A. (2022). *Machine learning-based QoS and traffic-aware prediction-assisted dynamic network slicing*. Int. J. Commun. Netw. Distrib. Syst. 28(1). 27–42. https://doi.org/10.1504/ijcnds.2022.120298

28. Erunkulu, O.O., Zungeru, A.M., Lebekwe, C.K., Mosalaosi, M. & Chuma, J.M. (2021). *5G Mobile Communication Applications: A Survey and Comparison of Use Cases*. IEEE Access. 9, 97251-97295. doi: 10.1109/ACCESS.2021.3093213.

29. Mademann, F. (2018). *The 5G System Architecture*. Journal of ICT Standardization, 6(1), 77-86.

30. ETSI (2019) *5G: Policy and charging control framework for the 5G System (5GS)*. ETSI TS 123 503 V15.5.0 (2019-04) Stage 2 (3GPP TS 23.503 version 15.5.0 Release 15). Διαθέσιμο στο: https://www.etsi.org/deliver/etsi_ts/123500_123599/123503/15.05.00_60/ts_123503v150500p.pdf [Ανακτήθηκε στις 20.04.22]

31. 3GPP (χ.η.). *Ran plenary*. Διαθέσιμο στο: https://www.3gpp.org/specifications-groups/ran-plenary. Τελευταία πρόσβαση στις 20.04.22]

32. Alvestrand, H. (2004). *A Mission Statement for the IETF - RFC3935*. Cisco. Διαθέσιμο στο: https://datatracker.ietf.org/doc/html/rfc3935 [Τελευταία πρόσβαση στις 22.04.22]

33. Hoffman, P. (χ.η.). *The Tao of IETF - A Novice's Guide to the Internet Engineering Task Force*. IETF. Διαθέσιμο στο: https://www.ietf.org/about/participate/tao/ [Τελευταία πρόσβαση στις 23.04.22]

34. Gentile, C.A., Papazian, P.B., Golmie, N.T., Remley, C.A., Vouras, P.G., Senic, J., Wang, J., Chuang, J. & Sun, R. (2018). *Millimeter-Wave Channel Measurement and Modeling: A NIST Perspective.* NIST. Διαθέσιμο στο: https://www.nist.gov/publications/millimeter-wave-channel-measurement-and-modeling-nist-perspective [Τελευταία πρόσβαση στις 25.04.22]

35. ITU (2019). *Evaluation Report received from Chinese Evaluation Group (CHEG) on the candidate IMT-2020 radio interface technology proposals*. Διαθέσιμο στο: https://www.itu.int/md/R15-IMT.2020-C-0010/en [Τελευταία πρόσβαση στις 28.04.22]

36. European Commission (χ.η.). *5G PPP Phase1 Security Landscape - Produced by the 5G PPP Security WG*. Διαθέσιμο στο: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf [Ανακτήθηκε στις 23.04.22]

37. Federal Communications Commission (2017). *Fifth Generation Wireless Network and Device Security*. Washington. 82(13). 7825 – 7830. Διαθέσιμο στο: https://www.govinfo.gov/content/pkg/FR-2017-01-23/pdf/2017-01325.pdf [Ανακτήθηκε στις 01.05.22]

38. IEEE future networks Enabling 5G and beyond (χ.η.) *Standards*. Διαθέσιμο στο: https://futurenetworks.ieee.org/standards [Τελευταία πρόσβαση στις 02.05.22]

39. Lasloum, T. & Al-Mogren, A.S. (2016) Optimizing Smart Things Addressing through the Zigbee-Based Internet of Things. International journal of Computer Networks & Communications. 8. 113 – 122. DOI: 10.5121/ijcnc.2016.8210. Διαθέσιμο στο: https://www.researchgate.net/publication/300083846_Optimizing_Smart_Things_Addressing_through_the_Zigbee-Based_Internet_of_Things [Ανακτήθηκε στις 03.05.22]

40. Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., Kamal, T. (2015). *A Review on Internet of Things (IoT).* International Journal of Computer Applications (0975 8887). 113(1). Διαθέσιμο στο: https://research.ijcaonline.org/volume113/number1/pxc3901571.pdf [Ανακτήθηκε στις 03.05.22]

41. Pradeepa, K. & Parveen, M. (2020). *Solid State Technology 8060 A Survey on Routing Protocols With Security in Internet of Things.* 63(4). Διαθέσιμο στο: https://www.researchgate.net/profile/Pradeepa-Kanagaraj-2/publication/352678798_Solid_State_Technology_8060_A_Survey_on_Routing_Protocols_With_Security_in_Internet_of_Things/links/60d2da0392851c34e07cf406/Solid-State-Technology-8060-A-Survey-on-Routing-Protocols-With-Security-in-Internet-of-Things.pdf?origin=publication_detail [Ανακτήθηκε στις 05.05.22]

42. Baoan, L. & Jianjun, Y. (2011). *Research and application on the smart home based on component technologies and Internet of Things*. Procedia Engineering 15, 2087 - 2092, Elsevier.

43. Miorandi, D., Sicari, S., Pellegrini, F.D. & Chlamtac, I. (2012). *Internet of things: Vision, applications and research challenges*. Ad Hoc Networks. 10(7). 1497-1516, https://doi.org/10.1016/j.adhoc.2012.02.016, Elsevier.

44. Sumatosoft (2022) *What is IoT Architecture: 4 stages of IoT Architecture*. Διαθέσιμο στο: https://sumatosoft.com/blog/what-is-iot-architecture-4-stages-of-iot-architecture [Τελευταία πρόσβαση στις 10.03.22]

45. Rayes, A. & Salam, S. (2017). *The Things in IoT: Sensors and Actuators. In: Internet of Things From Hype to Reality*. Springer, Cham. https://doi.org/10.1007/978-3-319-44860-2_3.

46. Posey, B. (2022). *IoT gateway*. Διαθέσιμο στο: https://www.techtarget.com/iotagenda/definition/IoT-gateway [Τελευταία πρόσβαση στις 29.05.22]

47. Arshad, S., Azam, M.A., Rehmani, M.H. & Loo, J. (2018). *Recent Advances in Information-Centric Networking based Internet of Things (ICN-IoT)*. IEEE Internet Of Things Journal, 14(8). Διαθέσιμο στο: https://arxiv.org/pdf/1710.03473.pdf [Ανακτήθηκε στις 01.06.22]

48. Alabdulatif, A., Khalil, I., Ahmed, S. H. (2018). *Integration of Internet of Things (IoT) and Cloud Computing: Privacy Concerns and Possible Solutions*. IEEE Internet Policy Newsletter. Διαθέσιμο στο: https://internetinitiative.ieee.org/newsletter/september-2018/integration-of-internet-of-things-iot-and-cloud-computing-privacy-concerns-and-possible-solutions [Τελευταία πρόσβαση στις 15.09.21]

49. Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145. Computer Security Division. Information Technology Laboratory. National Institute of Standards and Technology. Διαθέσιμο στο: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Ανακτήθηκε στις 02.06.22]

50. Naeem, R.Z., Bashir, S., Amjad, M.F., Abbas, H., & Afzal, H. (2019). *Fog computing in internet of things: Practical applications and future directions*. Peer-to-Peer Networking and Applications, 1-27, Spinger

51. Iorga, M., Feldman, L., Barton, R., Martin, M.J., Goren, N. & Mahmoudi, C. (2018). *Fog Computing Conceptual Model. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication (SP) 500-325. https://doi.org/10.6028/NIST.SP.500-325. Διαθέσιμο στο: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf [Ανακτήθηκε στις 02.06.22]

52. Salesforce UK (2020). *What are the Advantages of Cloud Computing?* 10 Reasons to Move to the Cloud. Διαθέσιμο στο: https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html [Τελευταία πρόσβαση στις 20.05.22]

53. Burhan, M., Rehman, R. A., Bilal, K., Kim, B.-S. (2018) *IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey*. Sensor Networks 18, No. 9:2796, DOI: 10.3390/s18092796. Διαθέσιμο στο: https://www.mdpi.com/1424-8220/18/9/2796/htm [Ανακτήθηκε στις 21.05.21]

54. 1ο ΓΕΛ Αγ. Αναργύρων (2014) *Project με θέμα: Ασφάλεια στο Διαδίκτυο*. Διαθέσιμο στο: http://1ogelasaferinternet.weebly.com/hackers.html [Τελευταία πρόσβαση στις 21.05.22]

55. Oza, S. (2020). *Denial-of-Service (DoS) Attacks — Web-based Application Security, Part 7*. Διαθέσιμο στο: https://spanning.com/blog/denial-of-service-attacks-web-based-application-security-part-7/ [Τελευταία πρόσβαση στις 26.05.22]

56. Suryateja, P.S. (2018). *Threats and Vulnerabilities of Cloud Computing A Review*. International Journal of Computer Sciences and Engineering. 6(3). 297-302. DOI: 10.26438/ijcse/v6i3.297302. Διαθέσιμο στο: https://www.researchgate.net/profile/Pericherla-

Suryateja/publication/325779181_Threats_and_Vulnerabilities_of_Cloud_Computing_A_Review/links/5cb31638299bf1209764be26/Threats-and-Vulnerabilities-of-Cloud-Computing-A-Review.pdf?origin=publication_detail [Ανακτήθηκε στις 29.04.22]

57. Lu, Z., Lu, X., Wang, W. & Wang, C. (2010). *Review and evaluation of security threats on the communication networks in the smart grid*. MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, 1830-1835, doi: 10.1109/MILCOM.2010.5679551.

58. Kalalas, C., Thrybom, L. & Alonso-Zarate, J. (2016). *Cellular Communications for Smart Grid Neighborhood Area Networks: A Survey*. IEEE Access, 4, 1469-1493. doi: 10.1109/ACCESS.2016.2551978.

59. Bakare, B.I. & Ekolama, S.M. (2021). *Preventing Man-in-The-Middle (MiTM) Attack of GSM Calls*. European Journal of Electrical Engineering and Computer Science. 5(4). https://doi.org/10.24018/ejece.2021.5.4.336.

60. Ozhelvaci, A. & Ma, M. (2020). *Security for Handover and D2D Communication in 5G HetNets*. 1-35. DOI: 10.1002/9781119471509.w5gref262. Διαθέσιμο στο: https://www.researchgate.net/profile/Alican-Ozhelvaci-2/publication/341436014_Security_for_Handover_and_D2D_Communication_in_5G_HetNets/links/5f34fc62299bf13404be8480/Security-for-Handover-and-D2D-Communication-in-5G-HetNets.pdf?origin=publication_detail [Ανακτήθηκε στις 20.05.22]

61. Li, W., Wang, N. Jiao, L. & Zeng, K. (2021). *Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks. IEEE Access*. 9. 60419-60432. doi: 10.1109/ACCESS.2021.3073115.

62. Park S, Kim D, Park Y, Cho H, Kim D, Kwon S. (2021). *5G Security Threat Assessment in Real Networks. Sensors*. 21(16). 5524. https://doi.org/10.3390/s21165524

63. Gagandeep, L. & Kataria, A. (2012). *Study on Sinkhole Attacks in Wireless Ad hoc Networks*. International Journal on Computer Science and Engineering. 4(6). 1078-1084. Διαθέσιμο στο: https://www.researchgate.net/publication/303009441_Study_on_Sinkhole_Attacks_in_Wireless_Ad_hoc_Networks/fulltext/57ab0da408ae7a6420bf3813/Study-on-

Sinkhole-Attacks-in-Wireless-Ad-hoc-Networks.pdf?origin=publication_detail [Ανακτήθηκε στις 01.05.22]

64. Mehta, A. & Gupta, A. (2013). *Survey On Secure Routing In Ad-Hoc Networks. Global Journal of Advanced Engineering Technologies*. 2(4). 171-175. Διαθέσιμο στο: https://www.researchgate.net/publication/257990998_SURVEY_ON_SECURE_ROUTING_IN_AD-HOC_NETWORKS [Ανακτήθηκε στις 20.05.22]

65. Karlof, C. & Wagner, D. (2003) *Secure routing in wireless sensor networks: attacks and countermeasures*. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, doi: 10.1109/SNPA.2003.1203362.

66. Al Ameen, M., Liu, J., & Kwak, K. (2012). *Security and privacy issues in wireless sensor networks for healthcare applications*. Journal of medical systems. *36*(1). 93–101. https://doi.org/10.1007/s10916-010-9449-4

67. Wang, Y., Garhan, A. & Ramamurthy, B. (2006). *A Survey of Security Issues In Wireless Sensor Networks.* CSE Journal Articles. 8(2). 2-23. Διαθέσιμο στο: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1087&context=csearticles [Ανακτήθηκε στις 10.05.22]

68. Maleh, Y. & Ezzati, A. (2014). *A Review of Security Attacks and Intrusion Detection Schemes in Wireless Sensor Network*. International Journal of Wireless & Mobile Networks. https://doi.org/10.48550/arXiv.1401.1982

69. Ramotsoela, D., Abu-Mahfouz, A., & Hancke, G. (2018). *A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study*. Sensors (Basel, Switzerland), 18(8), 2491. https://doi.org/10.3390/s18082491

70. SDxCentral Studios (2017). *The Top 5G Use Cases*. Διαθέσιμο στο: https://www.sdxcentral.com/5g/definitions/top-5g-use-cases/ [Τελευταία πρόσβαση στις 03.06.22]

71. Xiang, W., Zheng, K. & Shen, X. (2017). *5G Mobile Communications*. Springer

72. Theiotintegrator (χ.η.). *IoT Integrator - Powering the business behind the Internet of Things*. Διαθέσιμο στο: https://www.theiotintegrator.com/industrial/connect-the-

dots-massive-5g-readies-to-take-low-latency-iot-mainstream [Τελευταία πρόσβαση στις 04.06.22]

73. Elvitigala, C. & Sudantha, Bh. (2017). *Machine Learning Capable, IoT Air Pollution Monitoring System with Upgradable Sensor Array*. Conference: ISIS, Daegu, South Korea. Διαθέσιμο στο: https://www.researchgate.net/publication/323868781_Machine_Learning_Capable_IoT_Air_Pollution_Monitoring_System_with_Upgradable_Sensor_Array [Ανακτήθηκε στις 25.03.22]

74. NGMN (2015). *5G White Paper*. Διαθέσιμο στο: https://www.ngmn.org/work-programme/5g-white-paper.html [Τελευταία πρόσβαση στις 05.06.22]

75. West, D.M. (2016). *How 5G technology enables the health internet of things*. Center for Technology Innovation at Brookings. Διαθέσιμο στο: https://www.brookings.edu/wp-content/uploads/2016/07/how-5g-tech-enables-health-iot-west.pdf [Ανακτήθηκε στις 02.06.22]

76. NOKIA (2016). *5G use cases and requirements.* Διαθέσιμο στο: https://www.ramonmillan.com/documentos/bibliografia/5GUseCases_Nokia.pdf [Ανακτήθηκε στις 02.06.22]

77. Sorbara, D., Schubert, M. & Georgakopoulos, A. (2015). *Flexible Air iNTerfAce for Scalable service delivery wiThin wIreless Communication networks of the 5th Generation (FANTASTIC-5G)*. Internal Report IR2.1 Use cases, KPIs and requirements. Project reference: 671660. Διαθέσιμο στο: http://fantastic5g.com/wp-content/uploads/2016/01/FANTASTIC-5G_IR2-1_final.pdf [Ανακτήθηκε στις 03.06.22]

78. 5GPPP Architecture Working Group (2017). *View on 5G Architecture*. Version 2.0. Διαθέσιμο στο: https://5g-ppp.eu/wp-content/uploads/2018/01/5G-PPP-5G-Architecture-White-Paper-Jan-2018-v2.0.pdf [Ανακτήθηκε στις 05.06.22]

79. Dieudonne, M., Cattoni, A., Madueño, C., Salmerón, A., Díaz, A., Merino, P., Morris, D., Cárdenas, C., Baños, J., Mora, J.C. & Castañeda, O. (2016). *5G Applications and Devices Benchmarking (TRIANGLE)*. Project: H2020-ICT-688712. Deliverable D2.1. Initial report on the testing scenarios, requirements and use cases. Διαθέσιμο

στο: https://ec.europa.eu/research/participants/documents/downloadPublic/SW9rRHF1NDJMMi9oMHFuN2NYZDF6OWZjVitLOHJaeWxWdWFaWC9QWGg2YTU1Sm40VWlycVBBPT0=/attachment/VFEyQTQ4M3ptUWRHWXZYZmUrNmVXVHo3eSthTVNLNnI= [Ανακτήθηκε στις 05.06.22]

80. Yanjun S., Qiaomei H., Weiming S. & Hui Z. (2019). *Potential applications of 5G communication technologies in collaborative intelligent manufacturing*. IET Collaborative Intelligent Manufacturing Research Article. Διαθέσιμο στο: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-cim.2019.0007 [Τελευταία πρόσβαση στις 03.06.22]

81. Networked Energy Services Corporation (2022). *Smart meters: Which next-gen cellular and why*. Διαθέσιμο στο: https://www.smart-energy.com/digitalisation/smart-meters-which-next-gen-cellular-and-why/ [Τελευταία πρόσβαση στις 01.06.22]

82. Presher, A. (2019). *Industrial 5G: Impact on Factory Automation*. Διαθέσιμο στο: https://www.designnews.com/automation-motion-control/industrial-5g-impact-factory-automation [Τελευταία πρόσβαση στις 28.05.21]

83. Brettel, M., Friederichsen, N., Keller, M., Rosenberg, M. (2018). *How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective*. Διαθέσιμο στο: http://waset.org/publication/How-Virtualization,-Decentralization-and-Network-Building-Change-the-Manufacturing-Landscape:--An-Industry-4.0-Perspective/9997144 [Τελευταία πρόσβαση στις 30.05.22]

84. Qi, B. (2020). *Progress and Challenges in the Cellular Industry and 5G*. China Telecom, IEEE Future Networks Tech Focus, Volume 4, Issue 1. Διαθέσιμο στο: https://futurenetworks.ieee.org/tech-focus/november-2020/progress-and-challenges-in-the-cellular-industry-and-5g [Τελευταία πρόσβαση στις 22.08.21]

85. Zhuo, L., Xiang L., Wenye W., Cliff, W. (2010). *Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid*. Conference: Military Communications Conference. MILCOM. IEEE Xplore, DOI: 10.1109/MILCOM.2010.5679551

86. Michmon, J. (2018). *Forbes: Smart Grid Dreams Fading Without Congressional*

Support, Technocracy News. Διαθέσιμο στο: https://www.technocracy.news/smart-grid-dreams-fading-without-congressional-support/ [Τελευταία πρόσβαση στις 05.06.22]

87. Stone, M. (χ.η.). *The 5G evolution: Exploring the journey from 2G to 5G*. Διαθέσιμο στο: https://enterprise.verizon.com/resources/articles/s/5g-evolution-exploring-journey-from-2g-to-5g/ [Τελευταία πρόσβαση στις 17.05.22]

88. METIS (2014). *Scenarios, requirements and KPIs for 5G mobile and wireless system*. Document Number: ICT-317669-METIS/D1.1, Project Name: Mobile and wireless communications Enablers for the Twenty-twenty Information Society (METIS). Διαθέσιμο στο: https://cordis.europa.eu/docs/projects/cnect/9/317669/080/deliverables/001-METISD11v1pdf.pdf [Ανακτήθηκε στις 22.05.22]

89. cosmote (χ.η.) *5G*. Διαθέσιμο στο: https://www.cosmote.gr/cs/cosmote/gr/5g.html [Τελευταία πρόσβαση στις 02.06.22]

90. Alhajri, K., AlGhamdi, M., Alrashidi, M., Balharith, T., Tabeidi, R. (2021). *Smart Office Model Based on Internet of Things*. Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021). 174 – 183. DOI: 10.1007/978-3-030-76346-6_16

91. Qualcomm (χ.η.). *What is 5G?* Διαθέσιμο στο: https://www.qualcomm.com/5g/what-is-5g [Τελευταία πρόσβαση στις 05.06.22]

92. ΑΠΘ (2022). *Το ΑΠΘ πρωτοπορεί στις τεχνολογίες της μετά-5G εποχής*. Διαθέσιμο στο: https://www.auth.gr/press/to-apth-protoporei-stis-technologies-ti/ [Τελευταία πρόσβαση στις 04.05.22]

93. Alimi, I., Patel, R., Muga, N., Pinto, A., Teixeira, A. & Monteiro, P. (2021). *Towards Enhanced Mobile Broadband Communications: A Tutorial on Enabling Technologies, Design Considerations, and Prospects of 5G and beyond Fixed Wireless Access Networks*. Applied Sciences. 11. 10427. DOI: 10.3390/app112110427

94. Wong, A., Hsu, C-L., Le, T-V., Hsieh, M-C. & Lin, T.W. (2020). *Three-Factor Fast Authentication Scheme with Time Bound and User Anonymity for Multi-Server E-Health Systems in 5G-Based Wireless Sensor Networks*. Sensors. 20(9). 2511. DOI: 10.3390/s20092511

95. Thrybom, L. & Kapovits, A. (2015). *5G and energy*. 5G Infrastructure Association, Version 1.0. Διαθέσιμο στο: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White_Paper-on-Energy-Vertical-Sector.pdf [Ανακτήθηκε στις 08.06.21]

96. Smart Cities World news team (2017). *Huawei set to accelerate the smart grid*. Διαθέσιμο στο: https://www.smartcitiesworld.net/news/news/huawei-set-to-accelerate-the-smart-grid-1613 [Τελευταία πρόσβαση στις 09.06.21]

97. rgbsi (χ.η.). *7 Types of Vehicle Connectivity*. Διαθέσιμο στο: https://blog.rgbsi.com/7-types-of-vehicle-connectivity [Τελευταία πρόσβαση στις 01.06.22]