Πανεπιστήμιο Πειραιώς

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

[Π.Μ.Σ. ΤΔΑΨΣ] - ΚΑΤ. ΑΣΦΑΛΕΙΑΣ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

5TH Generation Networks Security

Μουρούκος Δημήτρης
Α.Μ.:MTE1524

Διδάσκων
Χ. Ξενάκης
Αναπληρωτής Καθηγητής

Αθήνα, Ιούνιος 2017

Περίληψη

Αντικείμενο της παρούσας εργασίας υπήρξε, η μελέτη και η ανάλυση αρχιτεκτονικών προτάσεων για τα δίκτυα 5η γενιάς. Ωστόσο, η εργασία εστίασε το μελετητικό της ενδιαφέρον σε ζητήματα ασφαλείας των αρχιτεκτονικών 5G. Για τις ανάγκες υλοποίησης της παρούσας βιβλιογραφικής μελέτης, πραγματοποιήθηκε εκτεταμένη και σε βάθος αναζήτηση επιστημονικών δημοσιεύσεων, κυρίως της τελευταίας τριετίας, σε διεθνώς αναγνωρισμένες βάσεις δεδομένων με τη χρήση λέξεων κλειδιά. Μέσω της έρευνας συμπερασματικά διαπιστώθηκε ότι, η ασφάλεια αποτελεί το μεγάλο ζητούμενο των δικτύων της επόμενης γενιάς, προκειμένου να αποφευχθούν σημαντικές βλάβες, οι οποίες θέτουν σε κίνδυνο της ιδιωτικότητα. Παράλληλα, διαπιστώθηκε ότι, τα 5G αποτελούν ένα ολοκληρωμένο δίκτυο πολυεθνικών και πολυτελών τεχνολογιών, το οποίο καλείται να καλύψει τις μελλοντικές ανάγκες ενός ευρέος φάσματος μεγάλων δεδομένων και την ταχεία ανάπτυξη πολλών επιχειρήσεων και βελτιώνει την εμπειρία των χρηστών, παρέχοντας έξυπνες και προσαρμοσμένες υπηρεσίες. Συνεπώς, κρίνεται αναγκαία η ανάπτυξη μεθοδολογιών οι οποίες θα εστιάζουν στις απαιτήσεις ελέγχου ταυτότητας (authentication), στην εξουσιοδότηση (authorization) και στη λογοδοσία (accounting).

Λέξεις-Κλειδιά: δίκτυα 5ης γενιάς, αρχιτεκτονικές δικτύων 5ης γενιάς, ασφάλεια δικτύων 5ης γενιάς, 5G-PPP,5G-Ensure, AAA, mmWave, Multi-RAN, VNF, SDN, Fronthaul, Backhaul, C-RAN, Cloud, WDM, PON, METIS II.

Abstract

The subject of this thesis was the study and the analysis of architectural proposals for the 5th generation networks. However, the study mainly focused its interest in security issues of 5G architectures. Extensive and in-depth search was made for the purpose of implementing of this scientific publication, mainly over the last three years, through internationally recognized databases with the use of keywords. Through the current research, it has been concluded that security is the major challenge of next-generation networks in order to avoid significant damage that compromises privacy. At the same time, it was found that 5G is an integrated network of multinationals and luxury technologies, which is designed to meet the future needs of a wide range of large data and the rapid growth of many businesses and improves user experience by providing smart and customized services. Therefore, it is necessary to develop methodologies that focus on authentication, authorization and accountability requirements.

Key – Words: 5^{th} generation networks, 5^{th} generation network security, 5^{th} network architecture, 5G-PPP,5G-Ensure, AAA, mmWave, Multi-RAN, VNF, SDN, Fronthaul, Backhaul, C-RAN, Cloud, WDM, PON, METIS II.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

API - Interface Protocol Interface

AKA – Authentication and Key Agreement

BBU - Baseband Unit

CAPEX -Capital expenditure

CDMA – Code-division multiple access

CPRI - Common Public Radio Interface

CPU – Central Processing Unit

CSRF - Cross-site Request Forgery

CWDM - Coarse Wavelength Division Multiplexing

DFB - Distributed Feedback

DTwC - Digital Trustworthiness Certificate

DWDM - Dense Wavelength Division Multiplexing

EDGE – Enhanced Data rates for GSM Evolution

ETSI - European Telecommunications Standards Institute

FEC - Forward Error Correction

FSO - Free Space Optics

2G – 2nd Generation

3G – 3rd Generation

4G – 4th Generation

5G – 5th Generation

GGSN –Gateway GPRS support node

GPON - Gigabit-capable Passive Optical Networks

GPRS - General Packet Radio Service

GUI - Graphic User Interface

ICT - Information and communication technology

IoT- Internet of Things

IMS - Multimedia Subsystem

IMSI - International Mobile Subscriber Identity

IMPI - IP Multimedia Private Identity

ITU – International Telecommunication Union

IMSI Catcher - International Mobile Subscriber Identity Catcher

KPIs – Key performance indicator

LED - Light Emitting Diode

LOS - Line-of-Sight

LoWPAN – Low-Power Wireless Personal Area Network

LRAP - Leucine-Rich Amelogenin Protein

LTE – Long Term Evolution

MIT – Massachusetts Institute of Technology

MIMO - Multiple-Input and Multiple-Output

MOST - Ministry of Science and Technology

mMTC – Massive Machine Type Communications

MME – Mobility Management Entity

mmWave - Millimeter wave

MSISDN – Mobile Station International Subscriber Directory Number

OAM - Operations Administration and Maintenance

OPEX - Operating expenses

OWC - Optical Wireless Communications

PEA - Privacy Enhanced Attachment

PON - Passive Optical Networks

PS – CN - Packet Switched Network

QoE - Quality of Experience

RAM – Random Access Memory

RAN – Radio Access Network

RAP – radio access point

RAT - radio access technologies

RCD – Resource Constraint Devices

RCS - Reconfigurable Add-Drop Multiplexers

RNC – Radio Network Controller

ROADM – Reconfigurable optical add-drop multiplexer

RoF - Radio-over-fiber

RPL – Recurrent pregnancy loss

PWG – PDN Gateway

SDN - Software Defined Networking

SGW - Signaling gateway

SIM - Subscriber Identity Module

SGSN – Serving GPRS Support Node

TDM - Time Division Multiplexing

TWDM - Time and Wavelength Division Multiplexing

UCE - User Capability Exchange

UDW- Universal data warehouse

UICCs - Universal Integrated Circuit Cards

VLC - Visible Light Communications

VMNO - Virtual Mobile Operator Network

VNF - Virtualized Network Functions

VoLTE – Voice over LTE

WAN - Wide Area Network

WDM - Wavelength Division Multiplexing

Εισαγωγή

Διαφαίνεται ότι η ζήτηση για ασύρματη μετάδοση δεδομένων δεν ικανοποιείται ποτέ. Μετά από περισσότερα από 30 χρόνια ταχείας ανάπτυξης, τα συστήματα κινητής επικοινωνίας έχουν ξεπεράσει την τεχνολογία 3G και έχουν ασπαστεί την 4G. Μολονότι, ο ρυθμός μετάδοσης δεδομένων έχει αυξηθεί κατά περίπου 1000 φορές, από την πρώτη γενιά κυψελοειδών συστημάτων κινητής επικοινωνίας, εντούτοις οι εκρηκτικές απαιτήσεις ζήτησης σε επίπεδο μετάδοσης δεδομένων και υπηρεσιών, εξακολουθεί να αντιμετωπίζει μεγάλες προκλήσεις. Ενώ, η προηγμένη έκδοση του Διεθνούς Συστήματος Κινητής Επικοινωνίας (IMT- Advanced) βρίσκεται καθοδόν, καθώς το IMT-2020 το οποίο είναι αφιερωμένο στην τεχνολογία 5^{ης} γενιάς (5G) ξεκίνησε από το 2013 (Zheng et al., 2015).

Μολονότι, είναι δύσκολος ακόμα ο ακριβής προσδιορισμός των χαρακτηριστικών του 5G, εντούτοις σε σχέση με τα υφιστάμενα συστήματα κινητής επικοινωνίας, εκτιμάται ότι θα πρέπει να είναι σε θέση να παράσχει 1000 φορές υψηλότερο όγκο δεδομένων κινητής ανά περιοχή, 10 έως 100 φορές υψηλότερο τυπικό ρυθμό δεδομένων χρήστη και συνδεδεμένων συσκευών, καθώς και 10 φορές μεγαλύτερη διάρκεια ζωής της μπαταρίας για συσκευής χαμηλής κατανάλωσης ενέργειας και χρόνο αναμονής από άκρο σε άκρο (Li et al., 2014).

Σε επίπεδο έρευνας, πλήθος κρατών έχει καταβάλει τεράστιες προσπάθειες και έχει δαπανήσει σημαντικούς πόρους σχετικά με την τεχνολογία 5G, όπως για παράδειγμα το Υπουργείο Επιστήμης και Τεχνολογίας της Κίνας (Ministry of Science and Technology - MOST) το οποίο έχει εκκινήσει το έργο 863 σε εθνικό επίπεδο στα 5G, η Ευρωπαϊκή Ένωση με το έργο «METIS 2020», το Ηνωμένο Βασίλειο και η Κίνα χρηματοδότησαν το έργο διεθνούς συνεργασίας «4G Wireless Mobile Communications», καθώς και η Ιαπωνία με την εκκίνηση του έργου «2020 and Beyond Ad Hoc» για 5G. Αντίστοιχα και ο τομέα της βιομηχανίας έχουν καταδείξει έναν ιδιαίτερο ενθουσιασμό για τα 5G, εστιάζοντας στην ικανότητα παράδοσης τεράστιας χωρητικότητα και μαζικής συνδεσιμότητας (Li et al., 2014).

Η τεχνολογία 5G καλείται να αντιμετωπίσει τις απαιτήσεις του 2020 και μετέπειτα, ενώ αναμένεται να ενεργοποιήσει μία πλήρως κινητή και συνδεδεμένη κοινωνία,

αλλά και να ενισχύσει τους κοινωνικοοικονομικούς σχηματισμούς μέσω ποικίλων διαδικασιών. Για το λόγο αυτό καθίσταται αναγκαία η εδραίωση νέων επιπέδων απόδοσης όσον αφορά τη διαθεσιμότητα, το χρόνο αναμονής και την πυκνότητα της συνδεσιμότητας.

Αντικείμενο της παρούσας εργασίας είναι, η μελέτη και η ανάλυση αρχιτεκτονικών προτάσεων για τα δίκτυα 5^{η} γενιάς. Ωστόσο, η εργασία εστιάζει κυρίως το μελετητικό της ενδιαφέρον σε ζητήματα ασφαλείας των αρχιτεκτονικών 5G.

Κεφάλαιο 1 – Εφαρμογές μέτρων ασφαλείας στα δίκτυα 3ης και 4ης γενιάς

1.1 Ζητήματα Ασφαλείας στα 3G και 4G δίκτυα

Οι ασύρματες επικοινωνίες 3η γενιάς παρέχουν υπηρεσίες κυκλώματος εναλλαγής και πακέτου δεδομένων υψηλής ταχύτητας, για κινητές συσκευές 3G. Αυτά τα δίκτυα εξελίχτηκαν από απομονωμένα 1G και 2G δίκτυα ενσωματωμένα με το διαδίκτυο. Ωστόσο, αυτή η ενοποίηση εισήγαγε τις εγγενείς αδυναμίες του διαδικτύου στα δίκτυα 3G και παρέχοντας στον τελικό συνδρομητή άμεση πρόσβαση στην υποδομή ελέγχου του δικτύου 3G (Fischer-Hibner et al., 2006).

Οι επιθέσεις στο δίκτυο 3G είναι μοναδικές διότι η αλλοίωση διαδίδεται λόγω της κανονικής λειτουργίας από άκρο σε άκρο. Αυτή η δυνατότητα είναι γνωστή ως επικαλυπτική επίδραση και συμβαίνει λόγω της ανταλλαγής των διεφθαρμένων στοιχείων δεδομένων στα μηνύματα σηματοδότησης μεταξύ των διακομιστών 3G. Ως εκ τούτου, ο στόχος της εκτίμησης της ευπάθειας δικτύου 3G δεν είναι μόνο η αναγνώριση της προέλευσης της επίθεσης, αλλά και η κλιμακωτή επίπτωση που προκαλείται λόγω του επιπέδου ευπάθειας και των αλληλεπιδράσεων του συστήματος από σημείο προς σημείο (Fischer-Hibner et al., 2006).

Η χειρονακτική – μη αυτόματη αφαίρεση των τρωτών σημείων και των επιθέσεων στα δίκτυα 3G δεν είναι εφικτή, καθώς η αφαίρεση των τρωτών σημείων απαιτεί εκτεταμένη γνώση χιλιάδων πελατειακών μηχανών, καθώς και της δικτύωσης από σημείο-προς-σημείο των τηλεπικοινωνιακών συστημάτων. Επιπλέον, τα τυποποιημένα εργαλεία εκτίμησης ευπάθειας που βασίζονται στο διαδίκτυο χαρακτηρίζονται ως ανεπαρκή για τα δίκτυα 3G, καθώς παρουσιάζουν φυσικά τρωτά σημεία τα οποία δεν αποτελούν στόχο της αξιολόγησης ευπάθειας του δικτύου 3G. Σκοπός είναι η αναγνώριση των ευπαθειών και αλληλεπιδράσεων σε επίπεδο συστήματος από σημείο-προς σημείο τα οποία διέπουν τις κλιμακωτές επιπτώσεις (Fischer-Hibner et al., 2006).

Σύμφωνα με τον ερευνητή ασφαλείας Lindh (2014)[1], πλήθος ευπαθειών εντοπίστηκαν σε modem 3ης και 4ης γενιάς modem USB, καθώς άφηναν στόχους

[1] https://www.tripwire.com/state-of-security/latest-security-news/csrf-vulnerabilities-found-many-3g-4g-modems/

ευάλωτους σε επιθέσεις παραβίασης μεταξύ ιστοτόπων (CSRF), οι οποίες θα μπορούσαν να χρησιμοποιηθούν για την κλοπή διαπιστευτηρίων σύνδεσης ή να διαπράξουν απάτη με την εκτέλεση μικρο-εφαρμογών (applications) στο λειτουργικό του τηλεφώνου. Ο ίδιος υποστηρίζει ότι τα τρωτά σημεία – ευπάθειες, θα μπορούσαν να επιτρέψουν στους επιτεθείς να κάνουν χρήση ψεύτικων ιστοτόπων σχεδιασμένων με τρόπο που να μοιάζουν νόμιμοι, ως μία προσπάθεια υποκλοπής ονομάτων χρηστών και κωδικών πρόσβασης, με τη μέθοδο της αποστολής άμεσων μηνυμάτων πίσω στον αποστολέα, ή με την αποστολή πολυδάπανων κειμένων σε αριθμούς οι οποίοι ελέγχονται από τον χρήστη. Για παράδειγμα, ο ίδιος ο Lindh εντόπισε μία ευπάθεια CSRF που θα μπορούσε να του δώσει πρόσβαση σε ένα μόντεμ, προκειμένου να μπορέσει να στείλει ένα μήνυμα κειμένου σε οποιονδήποτε αριθμό της επιλογής του. Μοναδική απαίτηση ήταν η προσέλκυση του ίδιου του χρήστη σε μια ιστοσελίδα υπό τον έλεγχό του. Αντίθετα στους δρομολογητές Wi-Fi, δεν εντοπίζεται λειτουργία σύνδεσης για μόντεμ USB, οπότε δεν θα πρέπει να υπάρχει ανησυχία για την παράκαμψη της αυθεντικότητας.

Εκτός από την απάτη μέσω SMS, η τεχνική η οποία είναι εξαιρετικά χρήσιμη σε επιθέσεις είναι η επίθεση spear-phishing (δόλιου ψαρέματος). Σύμφωνα με τον Grooten, δεν είναι δύσκολο να διαπιστωθεί με ποιο τρόπο ένας επιτιθέμενος θα μπορούσε να μετατρέψει αυτού του είδους την επίθεση (hack) σε ένα σχέδιο λήψης χρημάτων, αναγκάζοντας το Modem στην αποστολή μηνυμάτων SMS, προς έναν αριθμό υψηλής χρέωσης της κατοχής του. Παράλληλα, ο Rogers δήλωσε ότι αυτού του είδους η ευπάθεια είναι παρόμοια με αυτή των δρομολογητών BrightBox της E.E, όπως αυτή αποκαλύφθηκε από τον ερευνητή Helme Scott και η οποία θα μπορούσε να επιτρέψει στους επιδρομείς την πρόσβαση σε απομακρυσμένες συσκευές, εκθέτοντας δυνητικά ευαίσθητες πληροφορίες.

1.1.1. Συλλέκτης Ταυτοτήτων IMSI στα δίκτυα 3ης γενιάς

Ο συλλέκτης ταυτοτήτων IMSI ή IMSI Catcher, γνωστός και ως Stingray (Σαλάχι), είναι ένα σύστημα το οποίο μιμείται τη λειτουργία των σταθμών βάσης της κινητής τηλεφωνίας με στόχο να «ξεγελάσει» τις κινητές συσκευές ώστε να συνδεθούν μαζί του εκμεταλλευόμενο τις ευπάθειες του δικτύου. Στην συνέχεια κάθε κινητή συσκευή που εισέρχεται στην εμβέλεια του συστήματος αυτού, και συνδεθεί φυσικά, είναι ευάλωτη σε υποκλοπές των επικοινωνιών της. Στην Εικόνα 1.1. φαίνεται η

δράση ενός IMSI Catcher στην προσπάθεια του να υποκλέψει πληροφορίες από μια τηλεφωνική συσκευή[2].

Εικόνα 1.1. IMSI Catcher

Ο συλλέκτης ταυτοτήτων προκειμένου να ξεγελάσει τις τηλεφωνικές συσκευές οι οποίες βρίσκονται στην εμβέλεια του, χρησιμοποίει διάφορες μεθόδους και ευπάθειες που έχουν τα συστήματα 3ης γενιάς. Μερικές από αυτές τις τεχνικές είναι:

α) Το κινητό αυθεντικοποιείται στην κεραία, ενώ η κεραία δεν αυθεντικοποιείται στην τηλεφωνική συσκευή. Με αυτών τον τρόπο και εφόσον συνδεθεί η συσκευή στην κάλπικη κεραία (IMSI Catcher), τότε η κάλπικη κεραία μπορεί να απενεργοποιήσει την κρυπτογράφηση (Αλγόριθμος A5/0).

β) Κατά την διαδικασία αυθεντικοποίησης αρχικά η κινητή συσκευή δεν έχει αποθηκευμένη την προσωρινή ταυτότητα TMSI, οπότε αναγκάζεται να στείλει στον κάλπικο σταθμό την ταυτότητα IMSI, που όπως γνωρίζουμε μεταδίδεται χωρίς κρυπτογράφηση.

γ) Ο πλαστός σταθμός να στείλει ψευδώς μια «κλήση» ότι μετακινήθηκε σε νέα κυψέλη η κινητή συσκευή με αποτέλεσμα το χάσιμο της αντιστοιχίας TMSI-IMSI από την VLR. Το αποτέλεσμα θα είναι για άλλη μια φορά η αποστολή της ταυτότητας IMSI.

δ) Η κάλπικη κεραία έχει την δυνατότητα να μιμηθεί το CID (Cell ID) και το LAC (Local area codes) από μια κεραία ενός φορεί (Provider)[3].

Πολλές φορές χωρίς την χρήση ειδικών εφαρμογών είναι δύσκολο έως ακατόρθωτο να καταλάβεις κανείς ότι έχει συνδεθεί άθελα του σε μια κάλπικη κεραία. Συνεπώς, για την ανίχνευση τέτοιου είδους επιθέσεων, έχουν αναπτυχθεί εφαρμογές όπως το

[2] http://imsicatcher.org/imsi-explained/
[3] https://opensource.srlabs.de/projects/snoopsnitch/wiki/IMSI_Catcher_Score

snoopsnitch όπου υπό προϋποθέσεις η εφαρμογή αυτή έχει την ικανότητα να εντοπίζει πότε η κινητή συσκευή, είναι σε σύνδεση μέσω νόμιμης κεραίας κινητής τηλεφωνίας ή όχι. Επιπλέον σε ειδοποιεί πότε ακριβώς συνέβη αυτό αλλά και επιπλέον για σιωπηλά SMS (ή silent SMS) και γενικότερα για επιθέσεις που έχουνε προέλθει από την εκμετάλλευση του πρωτοκόλλου SS7 (Signaling System 7)[4].

1.1.2 Fraud (Απάτη)

Οι φορείς εκμετάλλευσης όπως και η πρόσβαση στο SS7, καθίσταται ολοένα και πιο προσιτή σε μη αξιόπιστα μέρη, γεγονός το οποίο προσδίδει πλήθος ευκαιριών για την εκκίνηση δόλιων συναλλαγών εκ μέρους του συνδρομητή. Εντός αυτού του πλαισίου, δύο πιθανές απάτες που εξετάζονται είναι η «Fraud-USSD-processUnstructuredSS» και η «Premium rate Fraud – Call forwarding».

Πιο συγκεκριμένα, το USSD αποτελεί ένα πρωτόκολλο το οποίο παραδοσιακά χρησιμοποιείται στο εσωτερικό του δικτύου του διαχειριστή για την παροχή διαφορετικών υπηρεσιών όπως, οι ερωτήσεις τηλεφωνικής κλήσης, η μεταφορά πιστώσεων, οι πληρωμές μέσω κινητού τηλεφώνου, καθώς και πλήθος άλλων υπηρεσιών. Σε αυτή την περίπτωση, ο συνδρομητής τυπικά αποστέλλει κάποιους κωδικούς USSD (#100#), με σκοπό την εκτέλεση κάποιων συναλλαγών. Όπως, διαφαίνεται στην Εικόνα 1.2, με τη χρήση ενός μηνύματος «processUnstructuredSS» ο εισβολέας μπορεί να στείλει κωδικούς USSD εξ ονόματος του πελάτη, επιτρέποντας με αυτόν τον τρόπο μια πιθανή συναλλαγή - μεταφορά πίστωσης ή μεταφοράς χρημάτων από τον στόχο του (Engel, 2014).

Δυστυχώς σε πολλές περιπτώσεις ο φορέας εκμετάλλευσης επιτρέπει τη λήψη αυτού του μηνύματος από εξωτερικά δίκτυα, σε περίπτωση που οι διαχειριστές περιαγωγής τους χρειαστεί να έχουν πρόσβαση σε αυτές τις υπηρεσίες, κατά την επίσκεψη σε άλλη χώρα. Το γεγονός αυτό κάνει το φιλτράρισμα αυτών των μηνυμάτων στα σύνορα πολύ δύσκολο (Engel, 2014).

[4] https://opensource.srlabs.de/projects/snoopsnitch

Εικόνα 1.2. Κατάχρηση της USSD για απάτη

Αναφορικά με την Premium rate Fraud – Call forwarding, όπως συμβαίνει και στα περιστατικά υποκλοπής κλήσεων, το μήνυμα registerSS μπορεί να χρησιμοποιηθεί προκειμένου να ρυθμίσει τη δυνατότητα προώθησης κλήσεων για τον συνδρομητή, σε έναν υπερτιμημένο (Premium) αριθμό αντί του αριθμού παρακολούθησης (Engel, 2014).

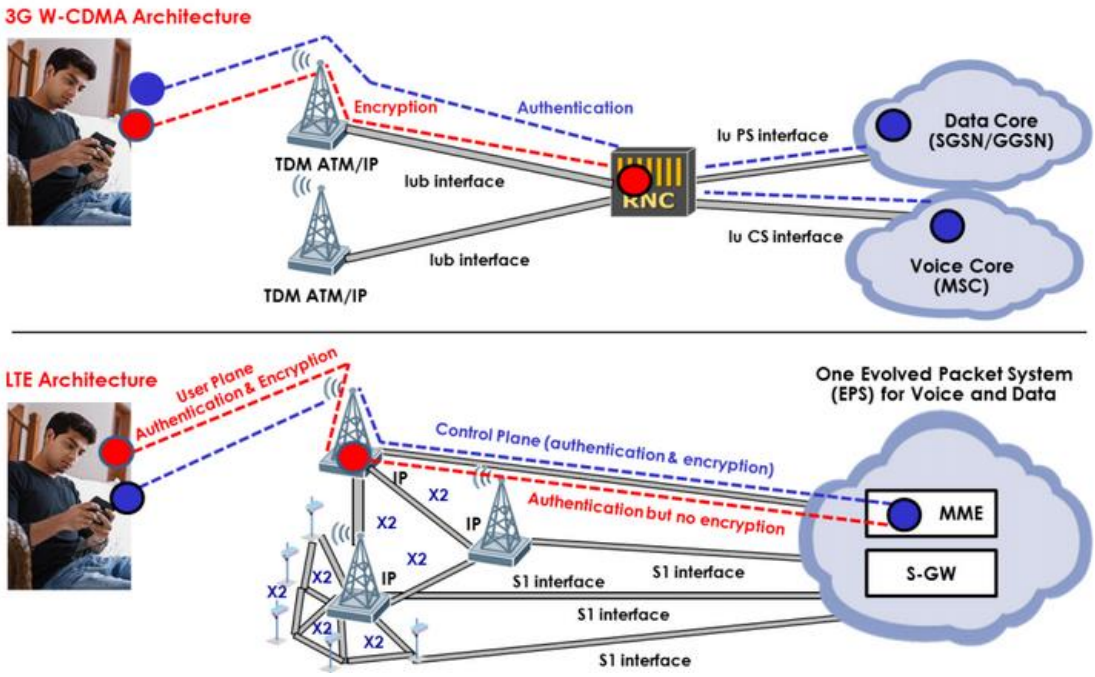
1.1.3. Ασφάλεια δικτύων 4G

Όσον αφορά τα δίκτυα 4ης γενιάς (4G), πλήθος φορέων εκμετάλλευσης κινητών δικτύων υιοθέτησαν την τεχνολογία 4G LTE και προσέφεραν αυτή την τεχνολογία στους πελάτες. Το LTE (Long Term Evolution) εξασφαλίζει υψηλότερη ταχύτητα, χαμηλότερο κόστος και καλύτερη ποιότητα. Ωστόσο, εντοπίζεται ένα ζήτημα ευπάθειας ασφαλείας στο δίκτυο LTE, το οποίο μπορεί να θέσει σε κίνδυνο την ασφάλεια, το οποίο δεν είχε εντοπιστεί στα δίκτυα 2G και 3G. Στα δίκτυα WCDMA 2G GSM και 3G, η κυκλοφορία κρυπτογραφείται μεταξύ του εξοπλισμού χρήστη και του ελεγκτή δικτύου ραδιοσυχνοτήτων (RNC), ωστόσο το LTE κρυπτογραφεί μόνο την κυκλοφορία μεταξύ του εξοπλισμού χρήστη και του σταθμού βάσης (eNodeB)[5].

Το LTE αναφέρεται σε μια επίπεδη αρχιτεκτονική βασισμένη στην τεχνολογία IP, η οποία σχεδιάστηκε προκειμένου να απλοποιήσει τη λειτουργία και τη συντήρηση, αλλά και να επιτύχει τη μείωση των χρόνων απόκρισης. Με την εξάλειψη του RNC στο δίκτυο LTE, η διαδρομή μεταξύ του εξοπλισμού χρήστη και του κεντρικού δικτύου είναι περισσότερο ευάλωτη σε επίθεση. Οι φορείς εκμετάλλευσης συχνά αναπτύσσουν eNodeBs σε δημόσιους χώρους, προκειμένου να αυξήσουν την χωρητικότητα του δικτύου, όπως για παράδειγμα στα αεροδρόμια και στα εμπορικά

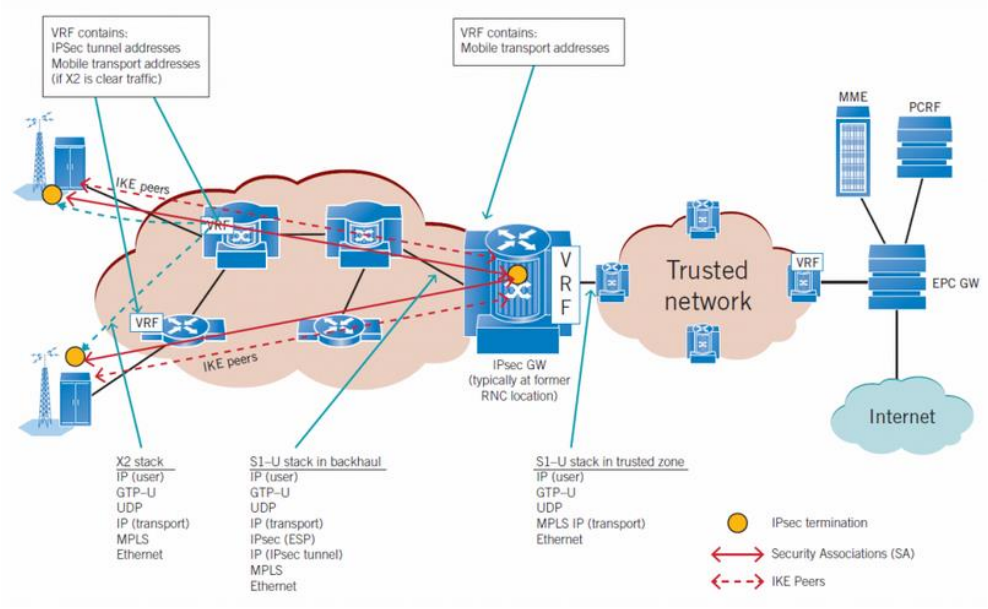
[5] http://www.royabubakar.com/blog/2013/11/05/security-vulnerabilities-in-4g-lte/

κέντρα. Το γεγονός αυτό έχει ως αποτέλεσμα να μην υπάρχει προστασία μεταξύ της κυκλοφορίας των eNodeB και του πυρήνα (Εικόνα 1.3.).



Εικόνα 1.3. Κρυπτογράφηση στα δίκτυα 3G & LTE

Το αντίμετρα για το μετριασμό αυτής της ευπάθειας είναι η εφαρμογή του IPsec πίσω από το eNodeB στο δίκτυο. Το IPsec αποτελεί μια σουίτα πρωτοκόλλων που παρέχουν κρυπτογραφικό στρώμα τόσο στο IPv4 όσο και στο IPv6. Πρόκειται για μια από τις μεθόδους που χρησιμοποιούνται για τη δημιουργία εικονικών ιδιωτικών δικτύων (VPN), τα οποία επιτρέπουν την αποστολή ιδιωτικών δεδομένων μέσω ενός μη ασφαλούς δικτύου. Οι σήραγγες IPsec μπορούν να αναπτυχθούν προκειμένου να εξασφαλίσουν τη προστασία των διασυνδέσεων backhaul, της διασύνδεσης S1-U και S1-C από το eNodeB στην πύλη πυρήνα και την οντότητα διαχείρισης κινητικότητας (MME) αντίστοιχα, καθώς και τη διεπαφή X2 μεταξύ eNodeBs. Ο διακόπτης άκρων μπορεί να αναπτυχθεί στην προηγούμενη θέση RNC για να τερματίσει τις διεπαφές S1 και η πύλη της προηγμένης πλατφόρμας μπορεί να αναπτυχθεί για να τερματίσει τις διεπαφές X2 (Εικόνα 1.4.).



Εικόνα 1.4. Backhaul συνδεσιμότητα με IP VPN full-mesh

1.1.4 Παρακολούθηση τοποθεσίας (Location Tacking)

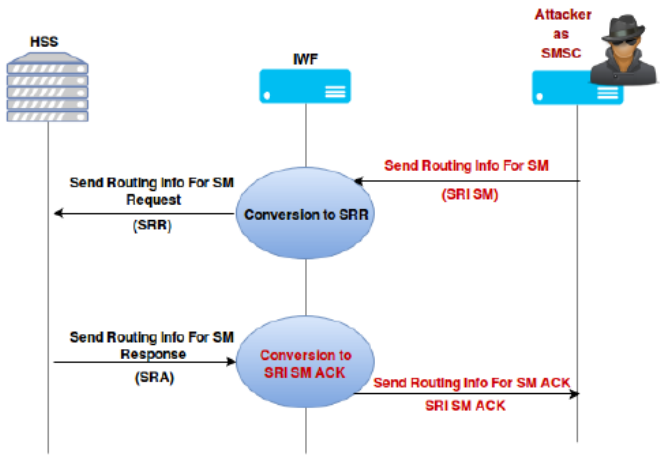
Οι τεχνολογίες κυψελοειδούς δικτύου απαιτούν κάποιον βαθμό παρακολούθησης της θέσης του χρήστη - συγκεκριμένα, τον εντοπισμό του εξοπλισμού των χρηστών, ως μέρος του θεμελιώδους μηχανισμού εργασίας τους. Χωρίς αυτή τη βασική λειτουργία, τα χαρακτηριστικά όπως η μετάβαση μεταξύ των κελιών δεν θα λειτουργούσε και δεν θα ήταν δυνατό να παρέχεται απρόσκοπτη εμπειρία χρήστη (δηλ., Καμία διακοπή κλήσεων ή σύνδεσης) όταν ο χρήστης κινείται. Επιπλέον, η προαναφερόμενη παρακολούθηση χρηστών από τους φορείς εκμετάλλευσης κινητών δικτύων (MNOs) βοηθά στην παροχή υπηρεσιών στους συνδρομητές των συνεργαζόμενων παρόχων υπηρεσιών κινητής τηλεφωνίας, πράγμα που είναι το γενικό σενάριο της "περιαγωγής". Σε τέτοια σενάρια, η σύνδεση δικτύου διαλειτουργικότητας που χρησιμοποιείται για την ανταλλαγή πληροφοριών συχνά ονομάζεται διασύνδεση. Πρόσφατα, αυτές οι διασυνδέσεις έχουν αξιοποιηθεί για την παρακολούθηση των ατόμων από hackers, ειδικά όταν οι διασυνδέσεις γίνονται από το πρωτόκολλο Signaling System No.7 (SS7).

Το πρώτο βήμα για έναν εισβολέα είναι να αποκτήσει το IMSI του θύματος, καθώς το IMSI είναι ένα από τα κύρια αναγνωριστικά χρήστη που απαιτείται για την πλειονότητα της επικοινωνίας εντός του δικτύου διασύνδεσης. Υπάρχουν διάφοροι τρόποι για να αποκτηθεί το IMSI, αλλά στην παρούσα επίθεση χρησιμοποιείται ένα

διάνυσμα προσβολής το IWF (interworking function) και η αναζήτηση του χρήστη γίνεται με βάση MSISDN.

Ο επιτιθέμενος ξεκινά την επίθεσή του ερωτώντας το δίκτυο του στοχευόμενου θύματος χρησιμοποιώντας την εντολή MAP SRI SM. Το IWF του στοχευόμενου δικτύου μεταφράζει το MAP SRI SM σε πληροφορίες δρομολόγησης όπως απεικονίζεται στο Εικόνα 1.4.

Ο εισβολέας εμφανίζεται ως συνεργάτη του SMSC ή IWF (για το σενάριο των δύο IWF) στο δίκτυο αναζήτησης και απαιτεί μόνο να υποστηρίζει παλαιό SSAP MAP αποστέλλοντας το αίτημα MAP SRI SM μέσω του δικτύου διασύνδεσης (Holtmanns-Prakash Rao et al., 2016).



Εικόνα 1.5. Επίθεση αποκάλυψης IMSI χρησιμοποιώντας SRI SM

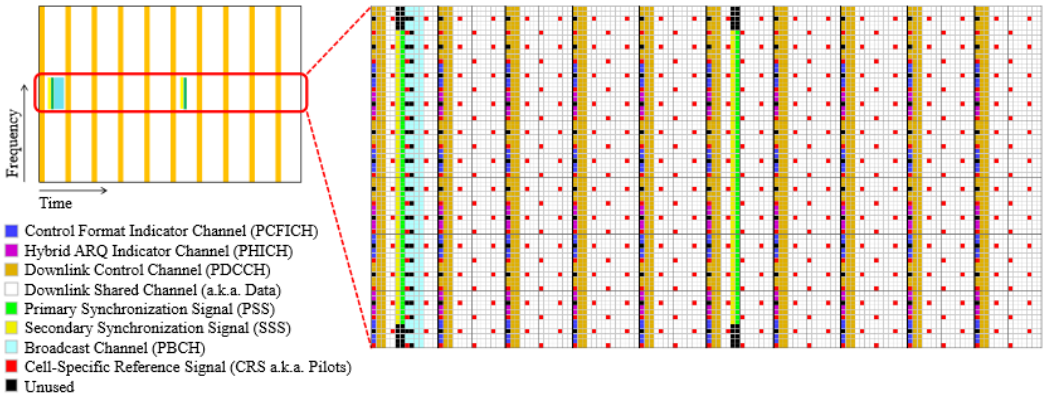
1.1.5 Signal Jamming (Σφάλμα σήματος)

Η Μακροπρόθεσμη Εξέλιξη (LTE) έχει τυποποιηθεί από το Σχέδιο Σύμπραξης 3ης Γενιάς (3GPP) για την κάλυψη της αυξανόμενης ζήτησης στην κυτταρική κίνηση δεδομένων. Το LTE προσφέρει καλύτερη κάλυψη, βελτιωμένη χωρητικότητα συστήματος, υψηλότερη φασματική απόδοση, χαμηλότερη καθυστέρηση και υψηλότερα ποσοστά δεδομένων από τους προκατόχους της με οικονομικά αποδοτικό τρόπο.Η αλήθεια είναι ότι το LTE είναι σε θέση να συμβαδίσει με την ταχεία εξέλιξη της τεχνολογίας, εισάγοντας το LTE-Advanced (LTE-A) για ακόμα υψηλότερα ποσοστά και χωρητικότητα δεδομένων, πιο αξιόπιστη κάλυψη και υψηλότερη φασματική απόδοση. Δυστυχώς, όπως και για οποιαδήποτε ασύρματη τεχνολογία, το πρόβλημα των παρεμβολών (interference), και των εσκεμμένων ασύρματων

διακοπών (Jamming) είναι πιθανά. Ο τρόπος με τον οποίο πραγματοποιείται μια τέτοιου είδους επίθεση περιγράφετε παρακάτω.

Το πρωτεύον σήμα συγχρονισμού (PSS) είναι ένα σήμα συγχρονισμού downstream ζεύξης, το οποίο λαμβάνεται από το UE (Συσκευή χρήστη) προκειμένου να εντοπιστεί και να συγχρονιστεί με ένα κύτταρο (οι σταθμοί βάσης μακροκυττάρων έχουν συνήθως τρία στοιχεία, γνωστά και ως τομείς). Με την ανίχνευση του PSS, το UE καθορίζει την ταυτότητα του φυσικού στρώματος του κυττάρου και αποκτά συγχρονισμό χρόνου και συχνότητας. Το δευτερεύον σήμα συγχρονισμού (SSS) παρέχει στο UE τη φυσική ομάδα ταυτότητας κυττάρων. Η ομάδα φυσικής ταυτότητας κυττάρων μαζί με την ταυτότητα φυσικής στρώσης παρέχει την πλήρη φυσική κυτταρική ταυτότητα (PCI). Μέσω του SSS, το UE μαθαίνει επίσης για τον τύπο του κυκλικού προθέματος (CP) και τη λειτουργία duplexing που χρησιμοποιείται από το κελί.

Η παρεμπόδιση (Jamming) του PSS ή του SSS απαιτεί αρκετά υψηλή ισχύ, επειδή τα δυο σήματα έχουν σχεδιαστεί ώστε να είναι ανιχνεύσιμα με χαμηλό λόγο σήματος προς θόρυβο (SNR). Έχει αποδειχθεί ότι μια πιο αποτελεσματική μέθοδος για την επίθεση στο PSS είναι η χρήση της RF spoofing, για να εμποδιστεί η UE να ανιχνεύσει το πραγματικό PSS ενός δεδομένου κυττάρου. Η PSS spoofing ουσιαστικά σημαίνει ότι ο εισβολέας μεταδίδει ένα ψεύτικο PSS, ασύγχρονο στο πλαίσιο του LTE (δηλαδή, όχι επικάλυψη στο χρόνο που μεταδίδεται το πραγματικό PSS) και με υψηλότερη ισχύ (Εικόνα 1.6.) (Lichtman-Piqueras et al., 2013).



Εικόνα 1.6. Το σήμα LTE Downlink, που δείχνει μια πλήρης εικόνα των 10 χιλιοστών του δευτερολέπτου (αριστερά).

Κεφάλαιο 2- Δίκτυα 5ης γενιάς και η τεχνολογική εξέλιξη τους

2.1 Δυνατότητες ασύρματου δικτύου 4ης γενιάς (LTE και LTE Advanced)

Τα ασύρματα δίκτυα 4ης γενιάς σε σχέση με τα ασύρματα δίκτυα προηγουμένων τεχνολογιών όπως 3ης , 2ης γενιάς, παρέχουν υψηλότερους ρυθμούς μετάδοσης, καθώς επίσης δίνουν μεγάλη έμφαση στην επαρκή ποιότητα υπηρεσιών εφαρμόζοντας τεχνικές QoS. Οι ρυθμοί μετάδοσης δεδομένων κυμαίνονται στα 300 Mbps στην καθοδική ζεύξη (downlink) και 75Mbps για την ανοδική ζεύξη (uplink), δίνοντας την δυνατότητα για παροχή υπηρεσιών με χαμηλότερο κόστος. Μερικές επιπρόσθετες δυνατότητες των δικτύων 4ης γενιάς προγράφονται παρακάτω:

- *Μεγαλύτερη ασφάλεια κλήσεων με την χρήση των δικτύων 4ης γενιάς:* Στα δίκτυα 3ης γενιάς οι κλήσεις πραγματοποιούνται μέσω του συστήματος σηματοδοσίας ss7, το οποίο έχει αποδειχθεί ότι είναι πολύ ευπαθές στις υποκλοπές των κλήσεων. Στα δίκτυα 4ης γενιάς, το σύστημα σηματοδοσίας ss7 παύει να έχει πρωταρχικό ρόλο (χρησιμοποιείται ως fall back σενάριο), και αντικαθιστάτε με το Voice over LTE (VoLTE). Το VoLTE το οποίο είναι βασισμένο στο IMS (IP Multimedia Subsystem) παρέχει νέες τεχνικές ασφάλειας, όπου κάνουν την υποκλοπή των κλήσεων σχεδόν αδύνατη.

- *Βελτιωμένη συνδεσιμότητα*: Η διασύνδεση του χρήση με το δίκτυο πρόσβασης είναι συνεχομένη, εξασφαλίζοντας με αυτόν τον τρόπο την ζητούμενη ποιότητα της υπηρεσίας (QoS) καθώς επίσης και απαιτήσεις κινητικότητας (Ζαχαριά, 2016).

- *Συνεχή σύνδεση:* Ο χρήστης βρίσκεται σε συνεχόμενη σύνδεση με το ετερογενή δίκτυο του όσο χρονικό διάστημα η συσκευή του είναι ενεργοποιημένη. Με αυτό τον τρόπο, μειώνεται η καθυστέρηση της συσκευής στην πρόσβαση του internet. Αυτό είναι ένα μεγάλο πλεονέκτημα των δικτύων 4ης γενιάς, διότι τα δίκτυα 3ης γενιάς δεν ήταν σε θέση να παρέχουν στον πελάτη συνεχόμενη σύνδεση διότι αντιμετώπιζαν θέματα κορεσμού (Ζαχαριά, 2016).

- *Ευρεία Κάλυψη υπηρεσιών:* Ο χρηστής έχει την δυνατότητα να χρησιμοποίει υπηρεσίες χωρίς τον περιορισμό χρόνου και χώρου, αδυναμία που υπήρχε στην προηγούμενη τεχνολογία 3G. Αυτή η κάλυψη μπορεί να μετρηθεί από την διαθεσιμότητα της σε μια περιοχή για έναν ελάχιστο αριθμό χρηστών. Επίσης στα δίκτυα $4^{ης}$ γενιάς μπορεί ο πάροχος να προσφέρει πρόσβαση σε ειδικές υπηρεσίες, προσαρμόζοντας το δίκτυο του έτσι ώστε να μην τίθεται θέμα κάλυψης της υπηρεσίας αυτής ((Ζαχαριά, 2016),).

- *Υποστήριξη νέας γενιάς πρωτοκόλλου IPv6, και πολυμετάδοσης (multicast):* Λόγο του μεγάλου αριθμού συσκευών που συνδέονται στο διαδίκτυο, και με την ταυτόχρονη εξάντληση των IPv4 διευθύνσεων (2^{32}), ένα σημαντικό χαρακτηριστικό που προστίθεται με την τεχνολογία $4^{ης}$ γενιάς είναι το πρωτόκολλο IPv6. Το IPv6 πρωτόκολλο έχει υλοποιηθεί να παρέχει ένα σχεδόν ανεξάντλητο αριθμό IPv6 διευθύνσεων ($3.4*10^{38}$), προκειμένου κάθε συσκευή να μπορεί να αποκτήσει μια πραγματική δημόσια IP address.

Ο ερχομός της τεχνολογία $4^{ης}$ γενιάς εκτός από τα παραπάνω χαρακτηριστικά, έχει διευκολύνει και πάρα πολύ την καθημερινότητα μας σε διάφορους τομείς. Οι ηλεκτρονικές συναλλαγές (Μεταφορά χρημάτων μέσω paypal,ebay), η εκπαίδευση εξ' αποστάσεως (με χρήση πολυμεσικού υλικού από χρήστες που είναι εν' κινήσει), η τηλεϊατρική (γρήγορη μετάδοση δεδομένων ιστορικού ασθενών), η ηλεκτρονική ψυχαγωγία Δικτυακές ταινίες-Video) είναι από τους τομείς που εξελίχτηκαν και αναπτύχτηκαν σε μεγάλο βαθμό με την άφιξη της $4^{ης}$ γενιάς δικτύων (Ζαχαριά, 2016).

2.2 Τρέχουσα κατάσταση δικτύων 5ης γενιάς

Η τρέχουσα κατάσταση της τεχνολογίας $5^{ης}$ γενιάς για τα κυψελοειδή συστήματα βρίσκεται σε μεγάλο βαθμό στα αρχικά στάδια ανάπτυξης. Πολλές εταιρείες εξετάζουν τις τεχνολογίες που θα μπορούσαν να χρησιμοποιηθούν για να γίνουν μέρος του συστήματος. Επιπλέον, πολλά πανεπιστήμια έχουν δημιουργήσει ερευνητικές μονάδες 5G με επίκεντρο την ανάπτυξη των τεχνολογιών για το 5G. Εκτός αυτού, οι φορείς τυποποίησης, ιδιαίτερα το 3GPP, γνωρίζουν την εξέλιξη αλλά δεν σχεδιάζουν ενεργά τα συστήματα $5^{ης}$ γενιάς ακόμη. Πολλές από τις τεχνολογίες

που θα χρησιμοποιηθούν για τα δίκτυα 5ης γενιάς, θα αρχίσουν να εμφανίζονται στα συστήματα που χρησιμοποιούνται για τα δίκτυα 4ης γενιάς. Στη συνέχεια καθώς το νέο κυψελοειδές σύστημα 5ης γενιάς θα αρχίζει να διαμορφώνει με πιο συγκεκριμένο τρόπο, τότε θα ενσωματωθούν στα νέα δίκτυα 5ης γενιάς αποκλειστικά. Το κυριότερο ζήτημα με την τεχνολογία 5ης γενιάς είναι ότι υπάρχει μια τόσο μεγάλη ποικιλία στις απαιτήσεις. Για παράδειγμα το πολύ γρήγορο «κατέβασμα δεδομένων» (superfast downloads) σε μικρές απαιτήσεις δεδομένων όπως είναι τα «Internet of thinks (IoT)» από οποιοδήποτε σύστημα δεν θα είναι σε θέση να καλύψει αυτές τις ανάγκες. Συνεπώς, είναι πιθανό να υιοθετηθεί μια προσέγγιση στρώματος[6].

2.2.1 Προδιαγραφές δικτύων 5ης γενιάς

Παρόλο που οι οργανισμοί τυποποίησης δεν έχουν καθορίσει ακόμη τις παραμέτρους που απαιτούνται για την επίτευξη των δικτύων 5ης γενιάς, άλλοι οργανισμοί έχουν θέσει τους δικούς τους στόχους, οι οποίοι ενδέχεται τελικά να επηρεάσουν τις τελικές προδιαγραφές και αποφάσεις που θα παρθούν. Μια τυπική εικόνα για τις παραμέτρους που μπορεί να περιλαμβάνουν τα δίκτυα 5ης γενιάς είναι η παρακάτω:

SUGGESTED 5G WIRELESS PERFORMANCE	
PARAMETER	SUGGESTED PERFORMANCE
Network capacity	10 000 times capacity of current network
Peak data rate	10 Gbps
Cell edge data rate	100 Mbps
Latency	< 1 ms

Εικόνα 2.1. Τυπικές παράμετροι για τα δίκτυα 5ης γενιάς

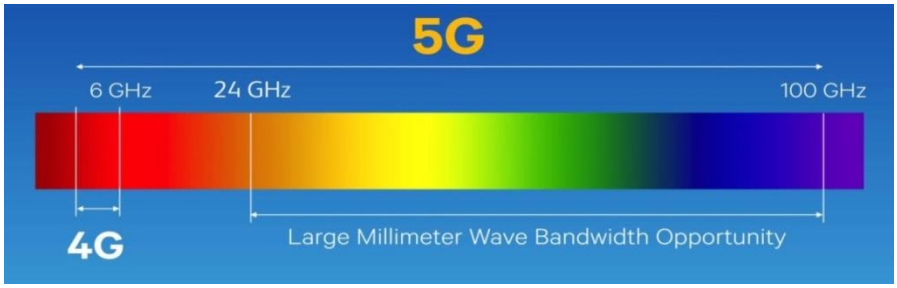
Εκτός από τους στόχους οι οποίο έχουν τεθεί από διαφόρους οργανισμούς, παράλληλα διάφοροι ερευνητικοί οργανισμοί πραγματοποιούν έρευνες για βασικούς τομείς που πιθανόν θα έχουν τα κυψελοειδή συστήματα 5ης γενιάς. Μερικοί από αυτούς τους τομείς αναλύονται παρακάτω.

- ***Millimetre-Wave technologies:*** Χρησιμοποιώντας πολύ υψηλότερες συχνότητες από φάσμα συχνοτήτων (Φάσμα που κυμαίνεται μεταξύ των 30GHz-300GHz) ανοίγει δρόμος για την χρήση περισσότερων καναλιών. Ωστόσο, αυτό δημιουργεί νέες προκλήσεις για την ανάπτυξη φορητών

[6]http://www.radio-electronics.com/info/cellulartelecomms/5g-mobile-cellular/technology-basics.php

ακουστικών, όπου χρησιμοποιούνται σήμερα μέγιστες συχνότητες περίπου 2 GHz και εύρη ζώνης 10-20 MHz. Για τα δίκτυα 5ης γενιάς, εξετάζονται συχνότητες άνω των 50GHz και αυτό θα παρουσιάσει μερικές πραγματικές προκλήσεις όσον αφορά τον σχεδιασμό του κυκλώματος, την τεχνολογία και τον τρόπο που χρησιμοποιείται το σύστημα, καθώς αυτές οι συχνότητες δεν ταξιδεύουν ως τώρα και απορροφώνται σχεδόν εξ ολοκλήρου από τα εμπόδια.

.



Εικόνα 2.2. Millimeter-Wave Bandwidth

- ***Future PHY / MAC:*** Το νέο φυσικό στρώμα (Physical layer) και το MAC παρουσιάζουν πολλές νέες ενδιαφέρουσες δυνατότητες σε διάφορους τομείς όπως:
    - ***Waveforms:*** Ένα βασικό πεδίο ενδιαφέροντος είναι αυτό των νέων κυματομορφών που μπορεί να δει κανείς. Το OFDM (Ορθογώνια πολυπλεξία διαίρεσης συχνότητας) χρησιμοποιήθηκε με μεγάλη επιτυχία στο 4G LTE καθώς και σε πολλά άλλα συστήματα υψηλής ταχύτητας δεδομένων, αλλά έχει κάποιες περιορισμένες ιδιότητες σε ορισμένες περιπτώσεις. Οι μορφές κυματογράφων που προτείνονται είναι: GFDM (γενικευμένη πολυπλεξία διαίρεσης συχνοτήτων), η FBMC (φίλτρο πολλαπλών μεταφορέων), καθώς επίσης και η UFMC (καθολική φιλτραρισμένη πολλαπλή διακίνηση). Κάθε μια από αυτές τις κυματομορφές έχει τα δικά της πλεονεκτήματα και περιορισμούς και είναι πιθανό να μπορούν να χρησιμοποιηθούν συνδυαστικά για μπορέσουν να καλύψου τις απαιτήσεις των νέων δικτύων 5ης γενιάς[7].

    - ***Multiple Access Schemes:*** Και σε αυτή την περίπτωση υπάρχει μια ποικιλία νέων συστημάτων πρόσβασης τα οποία διερευνούνται για την

[7]http://www.radio-electronics.com/info/cellulartelecomms/5g-mobile-cellular/technology-basics.php

τεχνολογία των νέων δικτύων 5ης γενιάς. Οι τεχνικές που έχουν προταθεί είναι οι OFDMA, SCMA, NOMA, PDMA, MUSA και IDMA.

- ***Modulation:*** Ενώ τα PSK (διαμόρφωση μετατόπισης φάσης) και QAM (Διαμόρφωση πλάτους τετραγωνικής διατομής) παρείχαν άριστες επιδόσεις όσον αφορά τη φασματική απόδοση, την ανθεκτικότητα και την ικανότητα, το κύριο μειονέκτημα είναι ο υψηλός λόγος κορυφής προς μέση ισχύ. Τα συστήματα διαμόρφωσης όπως είναι το APSK (Κλειδί μεγέθους πλάτους και φάσης) θα μπορούσαν να παράσχουν πλεονεκτήματα σε ορισμένες περιπτώσεις αν εφαρμοστούς στα δίκτυα 5ης γενιάς.

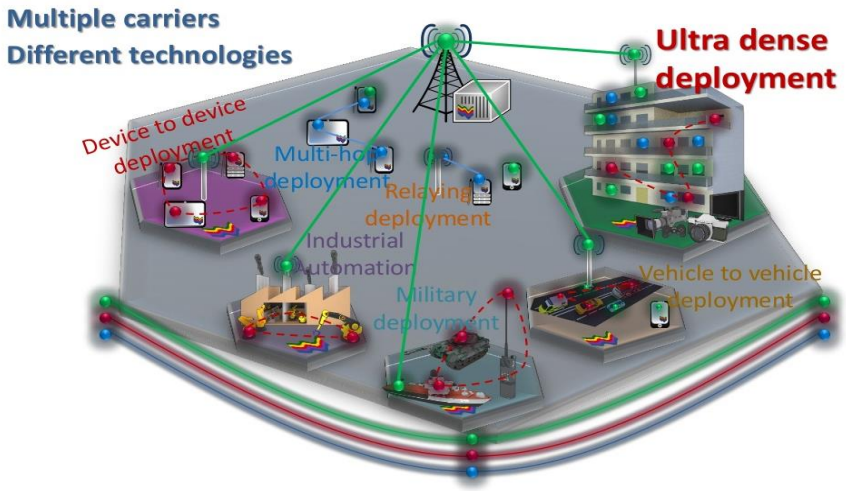
- ***Duplex methods:*** Υπάρχουν διάφορες υποψήφιες μορφές διπλής όψης (Duplex) που εξετάζονται. Σήμερα, τα συστήματα χρησιμοποιούν αμφίπλευρο διαχωρισμό συχνότητας, FDD ή διαχωρισμό χρόνου, TDD. Νέες δυνατότητες δημιουργούνται για τα δίκτυα 5ης γενιάς συμπεριλαμβανομένου του flexible duplex (Ευέλικτο αμφίδρομο), όπου ο χρόνος ή οι συχνότητες που διανέμονται μεταβάλλονται ανάλογα με το φορτίο προς οποιαδήποτε κατεύθυνση ή ένα νέο σχήμα που ονομάζεται division free duplex (Διπλής διαίρεσης) ή single channel full duplex (Μονοφωνικό πλήρες αμφίδρομο κανάλι). Αυτό το σχέδιο για τα δίκτυα 5ης γενιάς θα επέτρεπε την ταυτόχρονη μετάδοση και λήψη στο ίδιο κανάλι.

- ***Massive MIMO:*** Παρόλο που το MIMO χρησιμοποιείται σε πολλές εφαρμογές από LTE σε Wi-Fi, κ.λπ., ο αριθμός των κεραιών είναι αρκετά περιορισμένος. Χρησιμοποιώντας τις συχνότητες μικροκυμάτων ανοίγει ο δρόμος για χρήσης πολλών δεκάδων κεραιών σε ένα μόνο εξοπλισμό, δυνατότητα η οποία είναι εφικτή λόγω των μεγεθών της κεραίας και των αποστάσεων από την άποψη ενός μήκους κύματος[8].

[8] http://www.radio-electronics.com/info/cellulartelecomms/5g-mobile-cellular/technology-basics.php

Εικόνα 2.3. Τρέχουσα υλοποίηση κεραιών για την 4G τεχνολογία και Massive MIMO κεραίες.

- ***Ultra-dense networks (UDN):*** Μεγάλες εταιρίες τηλεπικοινωνιών, αναμένουν ότι έως το 2020, τα δίκτυα θα πρέπει να παρέχουν 1GB εξατομικευμένων δεδομένων ανά χρήστη την ημέρα. Επιπλέον, η κυκλοφορία έως το 2030 προβλέπεται να είναι έως και 10.000 φορές μεγαλύτερη από ό, τι το 2010 και θα πρέπει να υποστηριχθούν υπηρεσίες τελικού χρήστη των 100 Mbps. Για να μπορέσουμε να υποστηρίξουμε μια τέτοια ζήτηση, τα μελλοντικά δίκτυα θα πρέπει να είναι πολύ πυκνά και πολυεπίπεδα. Έτσι στα δίκτυα 5ης γενιάς εξετάζονται τεχνικές προκειμένου τα δίκτυα να είναι πολύ πυκνά για να παρέχουν στον χρήση πολύ καλές ταχύτητες[9].

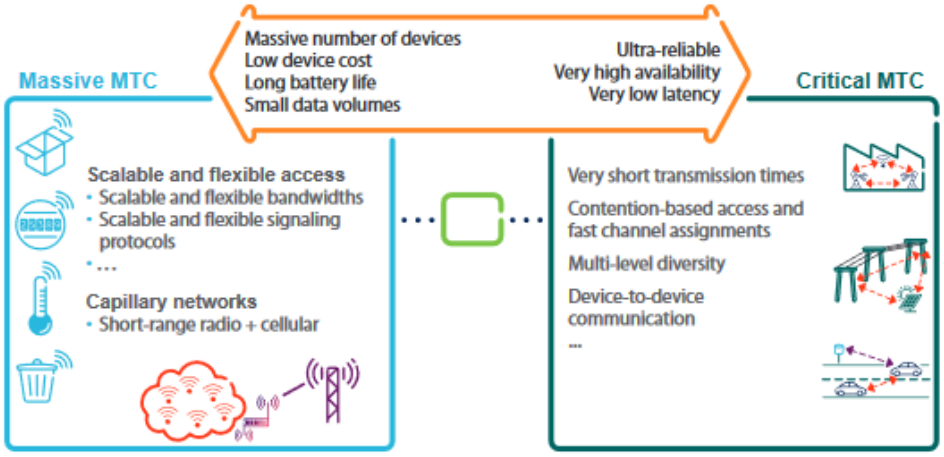


Εικόνα 2.4. Ultra dense networks

[9] https://tools.ext.nokia.com/asset/200295

2.3 Νέα χαρακτηριστικά και απαιτήσεις που αναμένεται να εφαρμοστούς στα δίκτυα 5ης γενιάς.

Βασικές εφαρμογές όπως η κινητή τηλεφωνία, η κινητή ευρυζωνική σύνδεση (broadband internet), και η παροχή μέσων ενημέρωσης αφορούν πληροφορίες οι οποίες απευθύνονται στον άνθρωπο. Υπάρχουν όμως πολλές εφαρμογές και περιπτώσεις που οδηγούν τις απαιτήσεις και τις δυνατότητες των δικτύων 5ης γενιάς να αφορούν επικοινωνίες από άκρο σε άκρο (end to end επικοινωνία) μεταξύ μηχανών. Για να τα διαχωρίσουμε τις ανθρώπινες περιπτώσεις (human-centric), συνήθως τέτοιου είδους εφαρμογές της ονομάζουμε συχνά επικοινωνία τύπου μηχανής (MTC). Παρόλο που καλύπτουν ένα ευρύ φάσμα εφαρμογών, οι εφαρμογές MTC (machine type communications) μπορούν να χωριστούν σε δύο βασικές κατηγορίες - μαζική MTC και κρίσιμη MTC - ανάλογα με τα χαρακτηριστικά και τις απαιτήσεις τους[10].



Εικόνα 2.5. Μαζικά MTC, και Κρίσιμα MTC

Το **μαζικό MTC (Massive MTC)** αναφέρεται σε υπηρεσίες που συνήθως καλύπτουν ένα πολύ μεγάλο αριθμό συσκευών, συνήθως αισθητήρων και ενεργοποιητών και δεν υπάρχει τόσο μεγάλη κρισιμότητα στην απώλεια της επικοινωνίας τους. Οι αισθητήρες έχουν εξαιρετικά χαμηλό κόστος και καταναλώνουν πολύ χαμηλές ποσότητες ενέργειας για να διατηρήσουν την ζωή της μπαταρίας τους για μεγάλο χρονικό διάστημα. Σαφώς, η ποσότητα των δεδομένων που παράγονται από κάθε αισθητήρα είναι συνήθως πολύ μικρή και η πολύ χαμηλή λανθάνουσα κατάσταση δεν αποτελεί κρίσιμη απαίτηση. Οι ενεργοποιητές έχουν και αυτοί χαμηλό κόστος, αλλά

[10] https://www.ericsson.com/assets/local/publications/white-papers/wp-5g.pdf

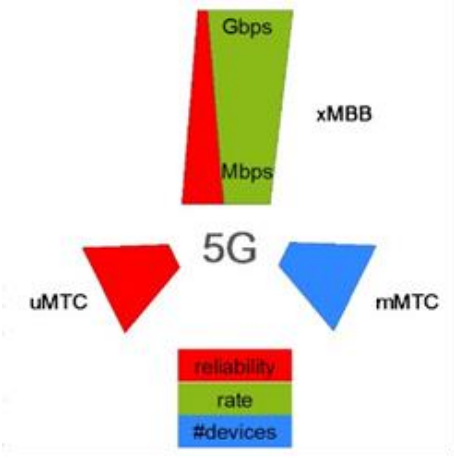
η κατανάλωση ενέργειας κυμαίνονται από πολύ χαμηλή έως μέτρια κατανάλωση (Tullberg-Popovski et al., 2015).

Το **κρίσιμο MTC (Critical MTC)** αναφέρεται σε εφαρμογές όπως η ασφάλεια / έλεγχος της κυκλοφορίας, ο έλεγχος της υποδομής ζωτικής σημασίας και η ασύρματη συνδεσιμότητα για βιομηχανικές διεργασίες. Τέτοιες εφαρμογές απαιτούν πολύ υψηλή αξιοπιστία και διαθεσιμότητα όσον αφορά την ασύρματη συνδεσιμότητα, καθώς και πολύ χαμηλή λανθάνουσα κατάσταση. Από την άλλη πλευρά, το χαμηλό κόστος συσκευών και η κατανάλωση ενέργειας δεν είναι τόσο κρίσιμα όσο για τις τεράστιες εφαρμογές MTC. Ενώ ο μέσος όγκος δεδομένων που μεταφέρονται προς και από τις συσκευές μπορεί να μην είναι μεγάλος, η ύπαρξη μεγάλου εύρου ζώνης είναι απαραίτητη για να ανταποκριθούν οι απαιτήσεις χωρητικότητας και καθυστέρησης.

Ένα από τα έργα (project) του 5G-PPP και συγκεκριμένα το METIS, οραματίζεται τρείς γενικές υπηρεσίες:

- Extreme Mobile BroadBand (xMBB)
- Ultrareliable MTC (uMTC)
- Massive MTC (mMTC)

Συγκεκριμένα, για την υπηρεσία xMBB δίνεται μεγάλη βαρύτητα στους υψηλούς ρυθμούς μεταφοράς και στην αύξηση της αξιοπιστίας καθώς ο ρυθμός μεταφοράς μειώνεται. Στην υπηρεσία uMTC δίνεται έμφαση στην πολύ υψηλή αξιοπιστία και τέλος στη υπηρεσία mMTC δίνεται έμφαση στο μεγάλο αριθμό των συσκευών (Tullberg-Popovski et al., 2015).



Εικόνα 2.6. Τρεις γενικές υπηρεσίες του 5G

Το **xMBB (Extreme Mobile BroadBand)** παρέχει αυξημένους ρυθμούς δεδομένων, αλλά και βελτιωμένη ποιότητα εμπειρίας (QoE- Quality of Experience) μέσω αξιόπιστων προβλέψεων μεταβαλλόμενων (μέτριων) ρυθμών. Τα μεγαλύτερα ποσοστά δεδομένων απαιτούνται από εφαρμογές όπως η διευρυμένη πραγματικότητα (σύνθεση εικονικής πραγματικότητας και φυσικού κόσμου) και η απομακρυσμένη παρουσία. Η βελτιωμένη ποιότητα υπηρεσιών αρχικοποιείται μέσω της απαίτησης παροχής αξιόπιστων μεταβαλλόμενων ποσοστών (μεγαλύτερο του 99%) οπουδήποτε και οποτεδήποτε και της υποβάθμισης της απόδοσης όσον αφορά την ταχύτητα δεδομένων και την καθυστέρηση, καθώς αυξάνεται ο αριθμός των χρηστών. Όπως φαίνεται στην Εικόνα 2.6, το xMBB εκτείνεται από τα μέγιστα ποσοστά της τάξης των Gbps σε μέτρια ποσοστά - με τη σειρά δεκάδων Mbps, όπου τα τελευταία προσφέρονται με πολύ υψηλή αξιοπιστία (Tullberg-Popovski et al., 2015).

Το **mMTC (Massive MTC)** παρέχει συνδεσιμότητα για μεγάλο αριθμό συσκευών, εξοικονόμησης ενέργειας και κόστους. Οι εφαρμογές των αισθητήρων και των ενεργοποιητών μπορούν να βρίσκονται σε ευρεία περιοχή για μετρήσεις επιτήρησης και μετρήσεις των περιοχών που καλύπτουν, αλλά επίσης να συστεγάζεται με ανθρώπους. Το κύριο χαρακτηριστικό αυτής της υπηρεσίας είναι ο τεράστιος αριθμός συνδεδεμένων συσκευών, όπως υπογραμμίζεται στην Εικόνα 2.6, όπου οι απαιτούμενες τιμές μειώνονται όσο αυξάνεται σημαντικά ο αριθμός των συσκευών (Tullberg-Popovski et al., 2015).

Το **uMTC (Ultrareliable MTC)** καλύπτει τις ανάγκες για εξαιρετικά αξιόπιστες υπηρεσίες κρίσιμης σημασίας και χρονικά κρίσιμες εφαρμογές, π.χ. εφαρμογές V2X (οχήματα προς οχήματα / υποδομές) και εφαρμογές βιομηχανικού ελέγχου. Και τα δύο παραδείγματα απαιτούν αξιόπιστη επικοινωνία και συγκεκριμένα το V2X επιπλέον απαιτεί γρήγορη αποκατάσταση της επικοινωνίας. Το κύριο χαρακτηριστικό είναι η υψηλή αξιοπιστία, ενώ ο αριθμός των συσκευών και οι απαιτούμενες ταχύτητες δεδομένων είναι σχετικά χαμηλές.

Αυτές οι υπηρεσίες έχουν πολύ διαφορετικές απαιτήσεις όσον αφορά τα ελάχιστα ποσοστά δεδομένων, την καθυστέρηση, τη διάρκεια ζωής της μπαταρίας, την κάλυψη, το μέγεθος του πακέτου δεδομένων κ.λπ. Θα εξακολουθούν να μοιράζονται δυναμικά τους ίδιους πόρους χρόνου συχνότητας, επιτυγχάνοντας αποδοτική χρήση του ραδιοφάσματος. Κατά την εισαγωγή μιας νέας υπηρεσίας, ένας φορέας εκμετάλλευσης δεν θα χρειαστεί να αγοράσει μια νέα ζώνη φάσματος και να

αναπτύξει μια συγκεκριμένη τεχνολογία ασύρματης πρόσβασης για το σκοπό αυτό. Αντ 'αυτού, στην έννοια 5G θα μπορούσε να εισαχθεί μια νέα υπηρεσία επαναχρησιμοποιώντας τα κοινά στοιχεία, για παράδειγμα τη λειτουργικότητα της διαχείρισης της κινητικότητας και τα ανώτερα στρώματα, και να επεκταθούν δυναμικά οι ραδιοφωνικοί πόροι με την πάροδο του χρόνου καθώς η υπηρεσία γίνεται όλο και πιο δημοφιλής (Tullberg-Popovski et al., 2015).

2.4 Μηχανισμοί των δικτύων 5ης γενιάς

Τα σημερινά δίκτυα ενσωματώνουν διαφορετικές ασύρματες γενεές και άλλες ασύρματες τεχνολογίες χωρίς άδεια χρήσης στα υψηλότερα επίπεδα της στοίβας πρωτοκόλλων. Από την άλλη πλευρά, η ετερογένεια μεταξύ των τριών γενικών υπηρεσιών συνεπάγεται ότι τα συστήματα 5^{ης} γενιάς θα ενσωματώσουν στενά διάφορες υπηρεσίες πιο κοντά στο τερματικό, πράγμα που απαιτεί τα εξής:

- Κοινές λειτουργίες ελέγχου που επιτρέπουν την ενσωμάτωση μεταξύ διαφορετικών παραλλαγών της διασύνδεσης.
- Λειτουργίες ελέγχους και δεδομένα (metadata) προσαρμοσμένα για τα xMBB, mMTC ή uMTC.
- Ενοποιημένη διασύνδεση ραδιοσυχνοτήτων από την οποία τα xMBB, mMTC και uMTC φαίνονται ως στιγμιότυπα.

Τα βασικά στοιχεία που επιτρέπουν τη δημιουργία ενός ευέλικτου συστήματος 5^{ης} γενιάς είναι τα εξής:

Λεπτό Επίπεδο Ελέγχου Συστήματος (Lean System Control Plane): Παρέχει αποτελεσματικά νέες πληροφορίες σηματοδότησης/ελέγχου που είναι αναγκαίες για να εξασφαλίσουν αξιοπιστία, υποστήριξη ευελιξίας φάσματος και μεγάλη ποικιλία συσκευών με πολύ διαφορετικές ικανότητες και διασφάλιση ενεργειακής απόδοσης.

Δυναμικά RAN (Dynamic RAN): Πρόκειται για αναθεώρηση της παραδοσιακής υποδομής ασύρματης πρόσβασης προκειμένου να συμπεριληφθούν δυναμικά στοιχεία, όπως ταχεία και πυκνή ανάπτυξη σημείων πρόσβασης. Στη δυναμική προσπέλαση του RAN, μια ασύρματη συσκευή μπορεί να παρουσιάζει δυαδικότητα,

με την έννοια ότι είναι σε θέση να λειτουργεί τόσο ως τερματικό όσο και ως κόμβος υποδομής. Υποστηρίζει υπερ-πυκνά δίκτυα (Ultra- Dense Networks - UDN) και επικοινωνία συσκευή προς συσκευή (D2D).

Περιεχόμενα / κυκλοφοριακές ροές (Localized Contents/Traffic Flows): Επιτρέπει την εκφόρτωση, τη συγκέντρωση και τη διανομή περιεχομένου σε πραγματικό χρόνο των αποθηκευμένων περιεχομένων.
Εργαλειοθήκη φάσματος (Spectrum Toolbox): Πρόκειται για ένα σύνολο δεικτών (εργαλείων) που επιτρέπουν στα συστήματα 5ης γενιάς να λειτουργούν με άνευ προηγουμένου ευελιξία φάσματος σε υπάρχουσες και νέες ζώνες, υπό διαφορετικά σενάρια ρύθμισης και ανταλλαγής φάσματος (Tullberg-Popovski et al., 2015).

2.4.1 Διπλός ρόλος των κινητών ασύρματων συσκευών

Παραδοσιακά, τα ασύρματα δίκτυα κινητής τηλεφωνίας διαθέτουν δύο τύπους κόμβων: κόμβους υποδομής (σημεία πρόσβασης, σταθμούς βάσης) και τερματικούς κόμβους (κινητές συσκευές). Υπήρξε μια σαφής, προκαθορισμένη ιεραρχία των κύριων κόμβων (master nodes) και των υποτελών κόμβων (slaves nodes) που χαρακτηρίζει κάθε πρωτόκολλο που σχετίζεται με την εγκατάσταση, τη χρήση και τη συντήρηση ενός ασύρματου συνδέσμου. Καθώς αυξάνεται η ικανότητα επεξεργασίας των ασύρματων συσκευών, τα δίκτυα 5ης γενιάς θα διαθέτουν κινητές ασύρματες συσκευές που θα είναι στην περιοχή μεταξύ καθαρής υποδομής και καθαρών τερματικών κόμβων. Ο βασικός κόμβος είναι η άμεση επικοινωνία D2D, όπου ορισμένες λειτουργίες ελέγχου ασύρματου δικτύου μεταφέρονται στη συσκευή. Μια συσκευή εξοπλισμένη με D2D μπορεί να έχει έναν διπλό ρόλο, που απεικονίζεται στην εικόνα 2.7. Επίσης η συγκεκριμένη εικόνα εμφανίζονται μεταξύ άλλων και τα εξής:

Εικόνα 2.7. Διπλός ρόλος

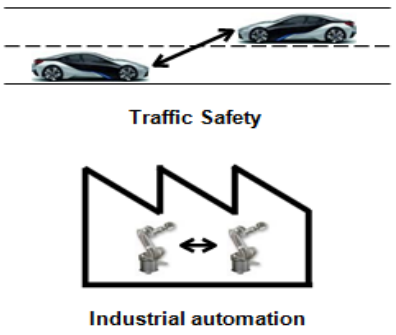
- Ένα όχημα που λειτουργεί ως τερματικό, αλλά και ως κόμβος πρόσβασης μιας ομάδας κυττάρων.
- Αναμετάδοση D2D για επέκταση εμβέλειας, βελτιωμένη χωρητικότητα, μεγαλύτερη διάρκεια ζωής της μπαταρίας και περιορισμό της κυκλοφορίας στην τοπική περιοχή αντί για χρήση πόρων σε μια ευρεία περιοχή.

- Η προσωρινή αποθήκευση του δημοφιλέστερου περιεχομένου σε κινητές συσκευές. Αυτό θα επιτρέψει αργότερα να λειτουργήσουν ως κόμβοι πρόσβασης για την ασύρματη διανομή περιεχομένου.

Ο διπλός ρόλος μιας ασύρματης συσκευής είναι παράλληλος με την αναδυόμενη έννοια του παραγωγού-καταναλωτή (prosumer) στα έξυπνα ενεργειακά δίκτυα, όπου ο χρήστης μπορεί να ενεργεί τόσο ως καταναλωτής όσο και ως παραγωγός ενέργειας. Ο διπλός ρόλος αποδίδεται κυρίως σε συσκευές που υποστηρίζουν πολύ μεγάλους ή πολύ αξιόπιστους μέτριους ρυθμούς, όπως στο xMBB, καθώς θα έχουν παρόμοιο μέγεθος και πολυπλοκότητα με τους κόμβους υποδομής. Από την άλλη πλευρά, οι συσκευές MTC θα είναι σημαντικά πιο απλές και φθηνότερες από τις συσκευές υψηλής ταχύτητας. Ως εκ τούτου, στα δίκτυα 5ης γενιάς η διαφορά μεταξύ ορισμένων κόμβων υποδομής και ορισμένων τύπων συσκευών θα είναι πολύ μικρότερη από τη διαφορά μεταξύ διαφόρων τύπων συσκευών (Tullberg-Popovski et al., 2015).

2.4.2 Εξαιρετικά αξιόπιστες συνδέσεις με χαμηλή καθυστέρηση

Τα συστήματα 5ης γενιάς θα πρέπει να ικανοποιούν τις απαιτήσεις που δεν υποστηρίζονται επί του παρόντος όσον αφορά την αξιοπιστία (reliability) και τη διαθεσιμότητα (availability), και να επιτρέπουν σε εφαρμογές οι οποίες εξυπηρετούν κρίσιμης σημασίας ζητήματα όπως η ασφάλεια της κυκλοφορίας, τα συστήματα αυτόματου ελέγχου αμαξοστοιχιών, ο βιομηχανικός αυτοματισμός και οι υπηρεσίες ηλεκτρονικής υγείας. Δύο παραδείγματα τέτοιου είδους εφαρμογών απεικονίζονται στην εικόνα 2.8.



Εικόνα 2.8. Αξιόπιστες συνδέσεις

Για παράδειγμα, ορισμένες εφαρμογές οδικής ασφάλειας απαιτούν την επιτυχή παράδοση των πακέτων πληροφοριών με πολύ μεγάλη πιθανότητα, εντός συγκεκριμένης προθεσμίας. Η μη επίτευξη αυτού του στόχου μπορεί να επηρεάσει σοβαρά την υγεία των χρηστών που βασίζονται στην υπηρεσία οδικής ασφάλειας. Επομένως, είναι απαραίτητο να σχεδιαστεί προσεκτικά το επίπεδο εφαρμογής της ασύρματης σύνδεσης για να διασφαλίσει την ασφάλεια, και χαμηλό κόστος.

Μια άλλη εφαρμογή η οποία απαιτεί αξιοπιστία και μεγάλη διαθεσιμότητα είναι ο βιομηχανικός έλεγχος. Σε αυτή την περίπτωση ένα δίκτυο θα πρέπει να είναι σε θέση να χειριστεί διαφορετικά είδη κίνησης που περιλαμβάνουν περιοδικά δεδομένα, σποραδικά δεδομένα και μηνύματα διαμόρφωσης. Τα περιοδικά δεδομένα σχετίζονται με τις εισόδους και τις εξόδους των αλγορίθμων ελέγχου και πρέπει να παραδίδονται με υψηλή αξιοπιστία εντός προθεσμίας. Σε γενικές γραμμές, ένα τέτοιο τυπικό πακέτο δεδομένων είναι μικρό και το εύρος ζώνης ανά κόμβο είναι χαμηλό. Σποραδικά δεδομένα, π.χ. που σχετίζονται με συναγερμούς, πρέπει να παραδίδονται με περιορισμένη καθυστέρηση, η οποία μπορεί να διαφέρει ανάλογα με την κρισιμότητα του συναγερμού. Τα μηνύματα διαμόρφωσης είναι συνήθως μη πραγματικού χρόνου, αλλά απαιτούν εξαιρετικά υψηλή αξιοπιστία της παράδοσης.

Προκειμένου να υποστηριχθούν αξιόπιστες συνδέσεις χαμηλής καθυστέρησης (<10ms) σε σχετικά μικρό εύρος, θα πρέπει στα ασύρματα συστήματα 5ης γενιάς η επικοινωνία D2D να είναι ελεγχόμενη από το δίκτυο. Η χρήση δικτύων σύνδεσης ευρείας περιοχής (WAN) καθιστά αυτή τη λειτουργία επικοινωνίας D2D θεμελιωδώς διαφορετική από τις άλλες λειτουργίες για συνδεσιμότητα μικρής εμβέλειας, όπως σύνδεση D2D σε μη εξουσιοδοτημένες ζώνες (Tullberg-Popovski et al., 2015).

2.4.3 Εγγυημένοι μεταβαλλόμενοι ρυθμοί και εξαιρετικά υψηλά ποσοστά

Το χαρακτηριστικό που συνδέεται συχνότερα με τα δίκτυα 5ης γενιάς είναι η παροχή εξαιρετικά υψηλών ποσοστών σε κάθε χρήστη, που κυμαίνονται στην τάξη των Gbps. Ωστόσο, από την πλευρά του χρήστη, η αξιόπιστη παροχή μεταβαλλόμενων ρυθμών (50-100 Mbps) είναι τουλάχιστον εξίσου σημαντική με τη μεγιστοποίηση των υψηλών ποσοστών. Αυτό συχνά εκφράζεται ως παροχή ένα ορισμένο ελάχιστο ποσοστό δεδομένων «παντού». Ένα τέτοιο χαρακτηριστικό έχει τη δυνατότητα να εισάγει μια νέα κατηγορία υπηρεσιών, οι οποίες σχεδιάζονται με την υπόθεση ότι η ασύρματη σύνδεση είναι «πάντα εκεί».

Η αξιόπιστη υποστήριξη για μεταβαλλόμενα ποσοστά είναι διαφορετική από την σημερινή προέκταση διεπαφών αέρα σε υψηλότερες ταχύτητες δεδομένων, αφού π.χ. η τεχνολογία 4ης γενιάς μπορεί να θεωρηθεί ως τεχνολογία βελτιστοποιημένη για υψηλούς ρυθμούς αιχμής. Οι νέες τεχνολογίες μετάδοσης, όπως το Massive MIMO (Multiple Input Multiple Output), και η ιδέα των υπερ-πυκνών δικτύων (UDN) είναι

καθοριστικής σημασίας για την παροχή ισχυρού ραδιοσήματος και τη διατήρηση του επιθυμητής αναλογίας σήματος προς παρεμβολές και θόρυβο (SINR). Η υψηλή αξιοπιστία σημαίνει ότι οι μεταβαλλόμενοι ρυθμοί θα πρέπει να διατηρούνται όταν αμφισβητείται το ασύρματο δίκτυο, όπως σε συχνά σενάρια ή κάτω από υψηλή κινητικότητα. Για παράδειγμα, σε πολυσύχναστα σενάρια, αξιόπιστοι μεταβαλλόμενοι ρυθμοί σημαίνει ότι το σύστημα είναι ικανό να υποβαθμίσει ικανοποιητικά την απόδοση του κάθε χρήστη, αντί να αρνείται υπηρεσίες σε ορισμένους από τους χρήστες (Tullberg-Popovski et al., 2015).

2.4.4 Ανθεκτική ασύρματη σύνδεση ως αντιστάθμισμα στην έλλειψη υποδομών

Η έλλειψη υποστήριξης υποδομής γενικά συμβαίνει λόγω: (1) της κινητικότητας των χρηστών προς χώρους με ανύπαρκτη κάλυψη δικτύου, (2) βλάβη εξοπλισμού ή ζημιές σε υποδομές που οφείλονται σε λόγους οι όπως φυσικές καταστροφές. Τα συστήματα 5^{ης} γενιάς θα πρέπει να ενσωματώσουν τη συμπληρωματική χρήση των ελεγχόμενων δικτύων καθώς και καθαρή D2D ad-hoc επικοινωνία, προκειμένου να προσφέρουν ελάχιστη συνδεσιμότητα σε σενάρια έκτακτης ανάγκης/καταστροφών και να ικανοποιήσει με αποτελεσματικό τρόπο τις απαιτήσεις διαθεσιμότητας και αξιοπιστίας για κρίσιμες εφαρμογές (uMTC), όπως η οδική ασφάλεια και η δημόσια ασφάλεια.

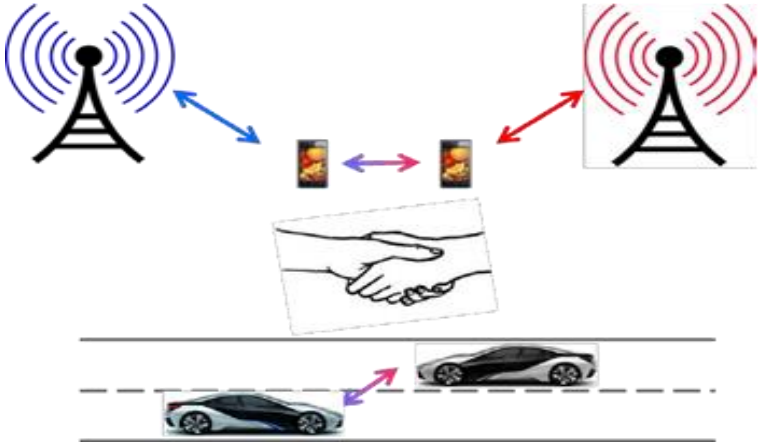
Η επικοινωνία D2D ελεγχόμενη από το δίκτυο παρέχει μια σημαντικά καλύτερη απόδοση από την καθαρή επικοινωνία D2D ad-hoc ως αποτέλεσμα της ανώτερης κατανομής πόρων και της διαχείρισης παρεμβολών που μπορεί να επιτευχθεί με τη συμμετοχή μιας κεντρικής οντότητας (δηλαδή του σταθμού βάσης). Εντούτοις, οι κρίσιμες εφαρμογές πρέπει να λειτουργούν σε κάποιο βαθμό κατά μήκος ολόκληρου του τομέα των υπηρεσιών (π.χ. το οδικό δίκτυο στην περίπτωση εφαρμογών οδικής ασφάλειας) και όχι μόνο με την κάλυψη του δικτύου. Επομένως, η χρήση ad-hoc επικοινωνίας D2D είναι ουσιώδης για την ενεργοποίηση της επικοινωνίας μεταξύ συσκευών, ακόμη και σε περιπτώσεις εκτός κάλυψης. Τα δίκτυα 5^{ης} γενιάς αναμένεται να διαθέτουν προγράμματα επιλογής τρόπου λειτουργίας που διαχειρίζονται την εναλλαγή μεταξύ διαφορετικών τρόπων επικοινωνίας, όπως η λειτουργία D2D ελεγχόμενη από το ad hoc και μέσω δικτύου. Το μελλοντικό δίκτυο

5ης γενιάς θα λειτουργεί επίσης σε περίπτωση μερικής βλάβης δικτύου που προκαλείται, για παράδειγμα, από φυσική καταστροφή. Με αυτόν τον τρόπο, οι σταθμοί βάσης ή ακόμη και οι συσκευές μπορούν να σχηματίζουν δίκτυα ad-hoc, και επομένως να επιτρέψουν την τοπική επικοινωνία ακόμη και αν η σύνδεση με το κεντρικό δίκτυο διακοπεί. Για το σκοπό αυτό, οι περιορισμένες λειτουργίες του κεντρικού δικτύου θα μπορούσαν να προκαθοριστούν στο δίκτυο ασύρματης πρόσβασης (Tullberg-Popovski et al., 2015).

2.4.5 Αυξημένη συνεργασία μεταξύ των φορέων εκμετάλλευσης

Τα δίκτυα 5ης γενιάς απαιτούν νέο και πιο πολύπλοκο τρόπο αλληλεπίδρασης και συνεργασίας μεταξύ των φορέων εκμετάλλευσης υπηρεσιών κινητής τηλεφωνίας. Ας εξετάσουμε, για παράδειγμα, τις νέες υπηρεσίες που σχετίζονται με την επικοινωνία V2X, οι οποίες υποστηρίζονται από την επικοινωνία D2D ελεγχόμενη από το δίκτυο. Σε σύγκριση με μια κανονική κυψελοειδής λειτουργία, το D2D απαιτεί αλλαγές στις λειτουργικές διαδικασίες, ιδιαίτερα λαμβάνοντας υπόψη την επικοινωνία μεταξύ συσκευών από διαφορετικούς χειριστές. Μόνο όταν οι φορείς μπορούν να συνεργάζονται πιο στενά και οι συσκευές από αυτούς μπορούν να δημιουργήσουν άμεση επικοινωνία μεταξύ τους τότε, η λύση D2D μπορεί να προσφέρει ικανοποιητικές επιδόσεις, όπως φαίνεται στην εικόνα 2.9. Ένα άλλο παράδειγμα για την συνεργασία μεταξύ διαφορετικών φορέων εκμετάλλευσης είναι η περίπτωση κοινής χρήσης του ραδιοφάσματος για την βελτίωση της διαχείρισης των παρεμβολών.

Υπάρχουν διάφοροι τρόποι για την αύξηση της συνεργασίας μεταξύ των φορέων εκμετάλλευσης. Ένας τρόπος για την επίλυση του προβλήματος είναι μία μονάδα δικτύου που λειτουργεί ανεξάρτητα με σκοπό την διαχείριση των θεμάτων μεταξύ των φορέων εκμετάλλευσης, συμπεριλαμβανομένου του ελέγχου ταυτότητας, της εξουσιοδότησης μεταξύ διαχειριστών κ.λπ. Ένα άλλο παράδειγμα θα μπορούσε να είναι η συνύπαρξη όπου ένας φορέας μπορεί να λάβει μια απόφαση με βάση την έκθεση μέτρησης μιας συσκευής, όπου η μέτρηση αυτή έχει γίνει από άλλο φορέα (Tullberg-Popovski et al., 2015).



2.9. Αυξημένη συνεργασία

2.4.6 Ενεργειακή απόδοση

Η ενεργειακή απόδοση μπορεί να ληφθεί υπόψη τόσο για την συσκευή όσο για το δίκτυο συνολικά. Ωστόσο, εξαιτίας του διπλού ρόλου των κινητών ασύρματων συσκευών της τεχνολογίας 5ης γενιάς, η διάκριση μεταξύ των δύο παραπάνω περιπτώσεων θα είναι πολύπλοκη. Καθώς τα δίκτυα περιλαμβάνουν όλο και περισσότερες συσκευές, καθίσταται ολοένα και πιο σημαντικό δυνατότητα ενεργοποίησης και απενεργοποίησης των κόμβων του δικτύου ανάλογα με το φορτίο κυκλοφορίας ή εναλλακτικά η απενεργοποίηση μερικών από τους κόμβους του δικτύου σε καταστάσεις χαμηλής φόρτισης.

Η κατανάλωση ενέργειας στα σημερινά δίκτυα κυριαρχείται από την μετάδοση των εναέριων σημάτων όταν δεν μεταδίδεται κανένα δεδομένο χρήστη. Βελτιώσεις στην ενεργειακή απόδοση των δικτύων μπορούν να επιτευχθούν μέσω νέων διαδικασιών σηματοδότησης, ενεργοποίησης/ απενεργοποίησης κόμβων του δικτύου και νέου σχεδιασμού διεπαφής αέρα. Ένα σύστημα 5ης γενιάς θα ενσωματώσει κόμβους με μεγάλες και μικρές περιοχές κάλυψης που λειτουργούν σε διαφορετικές συχνότητες (Tullberg-Popovski et al., 2015).

Κεφάλαιο 3ο 5G-PPP (Public Private Partnership)

Τα δίκτυα επικοινωνιών 5ης γενιάς (5G communication and services) και τα περιβάλλοντα υπηρεσιών το 2020, αναμένεται να είναι απείρως πλουσιότερα αλλά και ιδιαίτερα περίπλοκα από ότι τα υφιστάμενα. Η εμπειρία του χρήστη όχι μόνο θεωρείται επιβεβλημένη αλλά ο ίδιος θα έχει πλήρη εμπλοκή υποστηρίζοντας όλες τις πτυχές της κοινωνικής αλληλεπίδρασης, της εργασιακής επικοινωνίας, της παρακολούθησης της υγείας και της διαχείρισης του περιβάλλοντος, καθώς και της οικονομικής ευημερίας του καθενός. Ωστόσο, την υφιστάμενη χρονική στιγμή αποτελεί σημαντική πρόκληση η προσφορά μίας υποδομής 5η γενιάς, η οποία να έχει την εγγενή χωρητικότητα, ικανότητα, διαθεσιμότητα, αξιοπιστία και ασφάλεια προκειμένου να μπορεί να παράσχει μία απρόσκοπτα έγκαιρη υποστήριξη με βιώσιμο τρόπο (European Commission, 2015).

Αυτή η νέα δικτυακή υποδομή θα πρέπει να είναι ικανή να συνδέει ανθρώπους, διαδικασίες, κέντρα υπολογιστών, περιεχόμενο, γνώση, πληροφορία, αγαθά καθώς και άλλα πράγματα με μεγάλη ταχύτητα, σύμφωνα με μια πολλαπλότητα συγκεκριμένων απαιτήσεων που θέτουν οι ίδιες οι εφαρμογές. Μολονότι, αναμένεται μία δραματική αύξηση της επικοινωνιακής ποσότητας κάθε ατόμου, εντούτοις ο αριθμός των συνδεδεμένων πραγμάτων που επικοινωνούν μεταξύ τους, αναμένεται να είναι δέκα φορές υψηλότερος από τον αριθμό των συνδεδεμένων συνολικά χρηστών. Συνεπώς, η 5η γενιά δικτύων δεν αποτελεί μόνο μία εξέλιξη αλλά ουσιαστικά μία επανάσταση και ως εκ τούτου θα πρέπει να σχεδιαστεί με τρόπο ο οποίος να επιτρέπει το χειρισμό αυτής της δραματικής αύξησης των επικοινωνιών ακόμα από το αρχικό στάδιο (European Commission, 2015).

Λόγω της υφιστάμενης οικονομικής ύφεσης και του έντονου ανταγωνισμού σε παγκόσμιο επίπεδο, η Ευρωπαϊκή Ένωση δεσμεύεται να συνεχίσει να ενισχύει το ρόλο τον οποίο διαδραματίζει στον τομέα των επικοινωνιών, συνεχίζοντας να αναπτύσσει τις υφιστάμενες ευρωπαϊκές υποδομές και υπηρεσίες διαδικτύου. Ζητήματα όπως αυτά της υποστήριξης δέκα έως εκατό φορές περισσότερο της επισκεψιμότητας ανά τελικό χρήστη χωρίς την αύξηση του κόστους των πόρων ή της ενεργειακής χρήσης και του τρόπου παροχής υψηλότερης ποιότητας υπηρεσιών και ασφάλειας, θα πρέπει να απαντηθούν σε ευρωπαϊκό επίπεδο. Προκειμένου να επιτευχθούν αυτοί οι στόχοι, η Ευρωπαϊκή Επιτροπή σε συνεργασία με τους βιομηχανικούς κατασκευαστές, του τηλεπικοινωνιακούς φορείς, τους παρόχους

υπηρεσιών και την ερευνητική κοινότητα, εισήγαγε την 5η γενιάς Υποδομή Συνεργασίας Δημοσίου και Ιδιωτικού τομέα (5G Infrastructure Public Private Partnership) (European Commission, 2015).

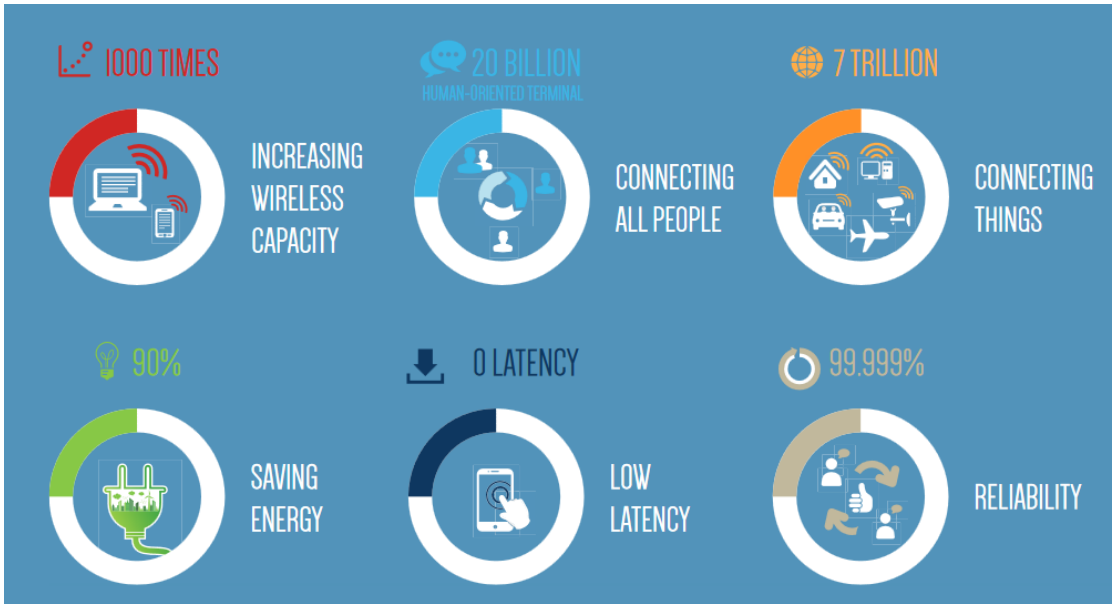
3.1. Υποδομή 5G-PPP

Η Υποδομή 5G – PPP - εν συντομία «5G PPP», αποτελεί μία κοινή πρωτοβουλία μεταξύ της Ευρωπαϊκής Ένωσης (ΕΕ.) και της Ευρωπαϊκής βιομηχανίας Τεχνολογιών Πληροφορικής και Επικοινωνιών (European ICT Industry). Εντός αυτού του πλαισίου, η Ευρωπαϊκή Επιτροπή προτίθεται - σχεδιάζει να επενδύσει 700 εκατομμύρια ευρώ και η βιομηχανία να αξιοποιήσει αυτή την επένδυση με συντελεστή 5, προκειμένου η συνολική επένδυση για τα 5G-PPP να υπερβεί τα 4 δισεκατομμύρια ευρώ, επανεξετάζοντας την υφιστάμενη υποδομή και δημιουργώντας τη νέα γενιά επικοινωνιών και υπηρεσιών.

Επιπρόσθετα, η 5G-PPP αποβλέπει στη διασφάλιση της ηγετικής θέσης της Ευρώπης στην ευρύτερη ευρωπαϊκή περιοχή της ισχύς της ή όπου υπάρχει η δυνατότητα δημιουργίας νέων αγορών όπως οι έξυπνες πόλεις, η ηλεκτρονική υγεία, οι ευφυείς μεταφορές, εκπαίδευση ή ψυχαγωγία και μέσα ενημέρωσης. Η πρωτοβουλία 5G-PPP προβλέπεται να ενισχύσει την ανταγωνιστική θέση της ευρωπαϊκής βιομηχανίας στις παγκόσμιες αγορές και να δημιουργήσει νέες καινοτόμες ευκαιρίες. Ενώ η 5G-PPP, προβλέπεται να προσφέρει λύσεις, αρχιτεκτονικές, τεχνολογίες και πρότυπα για τις ευρύτερες υποδομές της επόμενης γενιάς επικοινωνιών της επόμενης δεκαετίας.

Οι βασικοί στόχοι τους οποίους θέτει η 5G-PPP, όπως διαφαίνεται στην Εικόνα 3.1. είναι:

- Η αύξηση της ασύρματης χωρητικότητας κατά 1000 φορές περισσότερο
- Η εξοικονόμηση ενέργειας
- Διασύνδεση του συνόλου των χρηστών
- Ταχύτερη προσπέλαση
- Υποστήριξη μεγάλου εύρους εφαρμογών
- Χαμηλή χρονική καθυστέρηση (αναμονή)
- Αξιοπιστία
- Διασύνδεση πραγμάτων (European Commission, 2015).



Εικόνα 3.1. Βασικοί στόχοι 5G-PPP

3.2. Οργάνωση 5G-PPP

Η **5G-PPP** σχεδιάζεται να οργανωθεί σε δύο με τρείς φάσεις, περικλείοντας στο τρέχον στάδιο την έρευνα, τη βελτιστοποίηση τη χρονική περίοδο 2016-2017 και την πραγματοποίηση μεγάλης κλίμακας δοκιμές κατά τη χρονική περίοδο 2019-2020. Στοχεύει στην ανάπτυξη της 5G από το 2020, η οποία προηγουμένως θα απαιτήσει την ανάπτυξη μιας σειράς πρωτοποριακών τεχνολογιών και παγκόσμιων προτύπων, καθώς και την ύπαρξη συμφωνίας για τις σχετικές ζώνες ραδιοσυχνοτήτων (European Commission, 2015).

Την 1^{η} Ιουλίου του 2015, τα έργα της πρώτης φάσης ξεκίνησαν μετά από κοινή συνάντηση στο Παρίσι της Γαλλίας. Στιγμή ορόσημο για την επικέντρωση της έρευνας στις επενδύσεις, με πολύ συνεκτικό τρόπο στις προκλήσεις οι οποίες σχετίζονται με την ύπαρξη κατάλληλων επικοινωνιακών υποδομών ικανών να ανταπεξέλθουν στις μελλοντικές απαιτήσεις του 2020 (European Commission, 2015).

Το πρώτο κάλεσμα για έργα οδήγησε στην επιλογή 19 έργων, διευθύνοντας μία πλούσια τομή ερευνητικών προκλήσεων, οδηγώντας προς μία υποδομή 5^{ης} γενιάς έως το 2020. Κοινή πεποίθηση αποτελεί ότι η πλειοψηφία των επικοινωνιών του μέλλοντος θα έχει πρόσβαση σε ασύρματες τεχνολογίες. Ωστόσο, αυτό θέτει τεραστίων διαστάσεων απαιτήσεις στα προκείμενα έργα, για την εξεύρεση τρόπων

μεγιστοποίησης της αποδοτικότητας της ασύρματης διασύνδεσης, τη βελτιστοποίηση της χρήσης των περιορισμένων πόρων – όπως το ενεργειακό φάσμα και τη δραματική αύξηση της δυναμικής απόδοσης της υφιστάμενης υποδομής. Επιπρόσθετα, η υποδομή της 5ης γενιάς καλείται να αντιμετωπίσει από μία πληθώρα πραγμάτων μέσω δισεκατομμυρίων μικρών συσκευών στο Δίκτυο των Πραγμάτων (Internet of Things), έως τα βαριά δεδομένα δισεκατομμυρίων καταναλωτών τα οποία βελτιώνουν τις ζωές και τις δραστηριότητες τους, με το περιεχόμενο πολυμέσων σε πραγματικό χρόνο (European Commission, 2015).

3.3. Έργα 5G-PPP

3.3.1. 5G – Ensure

Η αναγκαιότητα για μία νέα αρχιτεκτονική ασφαλείας υποκινείται από το γεγονός ότι, η 5η γενιά αποτελεί μία πλατφόρμα η οποία ξεπερνάει τις τηλεπικοινωνίες και η οποία θα διαχωρίζεται αρκετά από το συγκεκριμένο τεχνικό και φυσικό έλεγχο του δικτύου. Το έργο 5G-ENSURE, αποβλέπει στην παροχή αναφοράς αρχιτεκτονικής ασφάλειας για τα 5G, τα οποία θα μπορούν να χρησιμοποιηθούν από το σύνολο των έργων 5G και παράλληλα να υποστηρίξουν τη χρήση του, παρέχοντας ένα σύνολο αρχικών ωφέλιμων και λειτουργικών παραγόντων διευκόλυνσης ασφαλείας, για την αντιμετώπιση βασικών προβλημάτων. Καθοριστικοί παράγοντες για την ασφάλεια των παραγόντων διευκόλυνσης στο έργο 5G-ENSURE υπολογίζεται ότι είναι:

- → Ο έλεγχος ταυτότητας, η εξουσιοδότηση και η λογιστική
- → Ιδιωτικότητα
- → Εμπιστοσύνη
- → Παρακολούθηση ασφαλείας
- → Διαχείριση Δικτύου και Απομόνωση της Εικονοποίησης

Ωστόσο, ευρύτερος στόχος του 5G-ENSURE είναι να αποτελέσει το έργο αναφοράς για όλα όσα σχετίζονται με την ασφάλεια στην 5G, ενώ ταυτόχρονα να συμβάλλει στην ανθεκτικότητα των 5G. Συνεπώς, το έργο 5G-ENSURE εστιάζει στην αρχιτεκτονικής ασφαλείας, η οποία είναι ικανή να δημιουργήσει την αναγκαία εμπιστοσύνη και αξιοπιστία για τα 5G, προκειμένου αυτά να υιοθετηθούν ευρέως και να διατυπώσουν τις υποσχέσεις τους, μέσω της ενεργοποίησης των εφαρμογών.

Προκειμένου να επιτευχθεί αυτό το φιλόδοξο εγχείρημα, θα πρέπει να τεθούν στόχοι όπως:

- → η συλλογή, η ανάλυση και παροχή προτεραιότητας στις απαιτήσεις ασφαλείας των 5G
- → ο πλήρης καθορισμός της αρχιτεκτονικής των 5G
- → ο καθορισμός, η ανάπτυξη και ο έλεγχος ενός συνόλου αρχικών παραγόντων διευκόλυνσης ασφαλείας των 5G
- → η κατάδειξη των δυνατοτήτων των παραγόντων διευκόλυνσης ασφαλείας των 5G, η οποίες αναπτύχθηκαν εντός του πλαισίου των αντιπροσωπευτικών μέσων παρουσίασης.
- → η διαφήμιση και η αξιοποίηση των αποτελεσμάτων του Έργου, καθώς και η προσφορά στην κοινότητα των 5G-PPP, αλλά και πέραν αυτής.
- → η προώθηση του Οράματος Ασφαλείας 5G, μέσω της παροχής ενός Χάρτη Ασφαλείας
- → η λειτουργία ως επικρατέστερου κατασκευαστή προ-τυποποίησης

Σε επίπεδο εφαρμογών, το έργο με την επωνυμία 5G-ENSURE θα επιδιώξει να συγκεντρώσει περιπτώσεις χρήσης από εξωτερικές πηγές και εάν καταστεί δυνατό τη δημιουργία συνδέσμων με ένα ή περισσότερα εξωτερικά, σχετικά με 5G, έργα ή δραστηριότητες (άλλα τρέχοντα έργα με Υποδομή Συνεργασίας Δημοσίου και Ιδιωτικού τομέα - PPP). Δεδομένου ότι οι εισροές από εξωτερικές πηγές θα κατευθύνονται κυρίως από τις επιχειρήσεις και την τεχνολογία, το έργο 5G-ENSURE θα μπορέσει να ορίσει νέες πρόσθετες περιπτώσεις ρεαλιστικής χρήσης, οι οποίες θα δίνουν έμφαση σε ζητήματα σχετικά με την ασφάλεια και την ιδιωτικότητα (European Commission, 2015).

Επιπρόσθετα, το έργο 5G-ENSURE αναμένεται να έχει στρατηγικό αντίκτυπο στο σύνολο του τεχνολογικού τομέα, στην επιχειρηματικότητα, στην τυποποίηση, όπως και στο όραμα για ένα ασφαλές ανθεκτικό και βιώσιμο δίκτυο 5ης γενιάς. Επίσης, αναμένεται να παράσχει την επιθυμητή αρχιτεκτονική ασφάλειας και τους μηχανισμούς για την επέκταση του κινητού οικοσυστήματος σε μία πλήρως δικτυωμένη κοινωνία, προσελκύοντας με αυτό τον τρόπο νέες κατηγορίες χρηστών και εφοδιάζοντας τους χειριστές με μία πλατφόρμα για νέες καινοτόμες επιχειρηματικές ευκαιρίες (European Commission, 2015).

Συντονιστής του έργου 5G-ENSURE είναι το Φιλανδικό Τεχνικό Κέντρο Ερευνών VVT, σε συνεργασία με πλήθος συνεργατών.

3.3.2. 5G – Exchange (5GEX)

Ο υφιστάμενος κατακερματισμός της αγοράς απορρέει από την ύπαρξη πλήθους τηλεπικοινωνιακών δικτύων και χειριστών νέφους (cloud operators), κάθε ένας από τους οποίου με το αποτύπωμα του εστιασμένο σε μία συγκεκριμένη περιοχή, ενώ στερούνται της σύμπραξης μεταφορέων επιχειρηματικών μοντέλων, υπηρεσιών και υποστηρικτικών εργαλείων. Αυτό καθιστά ανέφικτη τόσο την ανάπτυξη όσο και την προσφορά οικονομικά προσιτών υπηρεσιών υποδομής, για την κάλυψη πλήθους χωρών. Επιπλέον, οι υφιστάμενες υπηρεσίες και τα εργαλεία συνεργασίας μεταξύ των μεταφορέων εμφανίζονται αρκετά περιορισμένα και πολύπλοκα. Οι προκλήσεις στις οποίες καλείτε να ανταπεξέλθει το έργο «**5G Exchange (5GEX)»** είναι η επινόηση τεχνικών και επιχειρηματικών λύσεων για την αυτόνομη ενορχήστρωση των υπηρεσιών, σε περιβάλλοντα πολλαπλών πεδίων και τεχνολογιών.

Βασική επιδίωξη του έργου «5G Exchange (5GEX)» είναι να καταστήσει ικανή την αποτελεσματική επιχειρηματική και τεχνική διεπιχειρησιακή οργάνωση των υπηρεσιών, καθώς και την οργάνωση μέσω αυτόνομων διαχειριστών. Αυτή η οργάνωση θα επιτρέψει τη δημιουργία διατερματικών δικτύων και υπηρεσιών, εντός πολλαπλών πωλητών και σε ετερογενή περιβάλλοντα τεχνολογικών πόρων. Προκειμένου να ξεπεραστεί ο παραδοσιακός διαχωρισμός των δικτυακών πόρων από τον υπολογισμό και την αποθήκευση, η 5GEx προτίθεται να υλοποιήσει σύνθετες υπηρεσίες συνδυάζοντας απρόσκοπτα τη δικτύωση με τον υπολογισμό και την αποθήκευση δια μέσου των πεδίων ορισμού. Η ανάπτυξη, η ενεργοποίηση και η περαιτέρω διαχείριση της υπηρεσίας μπορεί να θεωρηθεί ως η αποτελεσματική χαρτογράφηση των στοιχείων της υπηρεσίας, εντός ενός περισσότερο απλοποιημένου μοντέλου που βασίζεται σε ένα εικονικά διαμορφωμένο υπόστρωμα, το οποίο ανήκει σε πολλαπλούς χειριστές.

Συνεπώς, στόχος του έργου 5GEx είναι η αυτοματοποιημένη εκχώρηση και η χαρτογράφηση των στοιχείων εικονικής υπηρεσίας, οι οποίες αντιπροσωπεύουν τις

υπηρεσίες και τις δικτυακές λειτουργίες, καθώς και τα στοιχεία στους υποκείμενους πόρους όλων των τομέων. Τα διατομεακά επιχειρηματικά μοντέλα 5GEx και η ενορχήστρωση, θα πρέπει να συμβάλλουν στη βελτιστοποίηση των επιχειρησιακών και λειτουργικά των κατάλληλων ευκαιριών για τους φορείς για την πραγματοποίηση αγορών, πωλήσεων και την ενοποίηση των υπηρεσιών υποδομής, εντός ενός αυτοματοποιημένου και οικονομικά αποδοτικού πλαισίου. Επιπλέον, τα 5GEx μοντέλα θα προβούν στην κατασκευή ενός διαλειτουργικού δικτύου και στην ανάπτυξη ενός καλά τεκμηριωμένου προτύπου, το οποίο θα περιλαμβάνει την έννοια του «Sandox Exchange». Το Sandox Exchange θα ενεργοποιήσει νέες τρόπους πειραματισμού, αλλά και τη νομιμοποίηση περιπτώσεων χρήσης εντός ενός λειτουργικού περιβάλλοντος το οποίο θα διευκολύνει τη μετάβαση από τον πειραματισμό προς μια πιλοτική λειτουργία και κατ' επέκταση στη λειτουργία σε πραγματικές συνθήκες.

Σε επίπεδο εφαρμογών, το έργο 5GEx θα εστιάσει σε έναν αριθμό περιπτώσεων χρήσης, για την κατάδειξη του συνόλου των λειτουργικών χαρακτηριστικών τα οποία απαιτούνται για τις προοπτικές σε πολλαπλά περιβάλλοντα και για την τεχνολογία πολλαπλών χρήσεων, αντικατοπτρίζοντας μελλοντικά ρεαλιστικά σενάρια τα οποία θα είναι εφικτά μέσω του 5GEx. Οι περιπτώσεις ταξινομούνται ανάλογα με το στόχο που τίθεται σε επίπεδο υπηρεσίας όπως, το ζήτημα της συνδεσιμότητας, το Δίκτυο ως υπηρεσία ζήτησης και το Δίκτυο – Αποθήκευση – Υπολογισμός ως αίτημα για υπηρεσία.

Το έργο 5GEx, αναμένεται να κινηθεί πέρα από την υφιστάμενη τεχνολογική ανάπτυξη με την επίτευξη, της εγκατάστασης υπηρεσιών εντός 90 λεπτών, την ενσωμάτωση περιπτώσεων παρακολούθησης σε αρχιτεκτονική πολλαπλών χρηστών και τη βέλτιστη ενσωμάτωση – αναφορικά με τη χρήση των πόρων και των εσόδων - απαίτηση υπηρεσιών εντός ενός συνόλου εικονικών πόρων που αντιστοιχούν σε πολλαπλούς φορείς εκμετάλλευσης, αντίστοιχα με τις ανάγκες κάθε υπηρεσίας και τον καθορισμό καινοτόμων επιχειρήσεων, μοντέλα συντονισμού και πληροφόρησης, εμπορικούς μηχανισμούς και συστήματα τιμολόγησης.

Τέλος το έργο 5GEx, αποβλέπει στη δοκιμή και στην επικύρωση των σχεδιαζόμενων μηχανισμών και της αρχιτεκτονικής της ενορχήστρωση σε πολλαπλά περιβάλλοντα εντός του «Sandbox Exchange», το οποίο θα ενσωματωθεί στις δοκιμαστικές μονάδες του 5GEx.

3.3.3 5G NORMA

Novel Radio Multiservice adaptive network Architecture for 5G networks (NORMA) – Καινοτόμος αρχιτεκτονική ασύρματου προσαρμοζόμενου δικτύου πολλαπλών υπηρεσιών, για δίκτυα 5G. Η τεχνολογική προσέγγιση η οποία ακολουθείτε από το 5G NORMA, βασίζεται στην καινοτόμο έννοια – ιδέα της προσαρμοστικής αποσύνθεσης και κατανομής των λειτουργιών του δικτύου κινητής τηλεφωνίας, η οποία μέσω απλοποιημένων διαδικασιών απενεργοποιεί τις λειτουργίες του δικτύου κινητής τηλεφωνίας και ενεργοποιεί τις προκύπτουσες λειτουργίες εντός της κατάλληλης τοποθεσίας. Με αυτό τον τρόπο, οι βασικές λειτουργίες καθώς και πρόσβαση αναγκαστικά δεν υφίσταται σε διαφορετικές τοποθεσίες, οι οποίες εκμεταλλεύονται για να βελτιστοποιήσουν από κοινού τη λειτουργία τους όποτε είναι δυνατόν. Επιπλέον, η ικανότητα προσαρμογής της αρχιτεκτονικής ενισχύεται περεταίρω μέσω του καινοτόμου λογισμικού, το οποίο καθορίζεται από τον έλεγχο του δικτύου κινητής τηλεφωνίας και τις έννοιες της πολλαπλής μίσθωσης και υποστηρίζεται από την επίδειξη αποδεικτικών στοιχείων.

Μέσω του προγράμματος 5G NORMA, οι έχοντες ηγετικό ρόλο στο κινητό οικοσύστημα αποβλέπουν στην υποστήριξη της ανταγωνιστικής θέσης της Ευρώπης στο 5G.

Βασικός στόχος του έργου αποτελεί η ανάπτυξη μίας πρωτοποριακής εννοιολογικά , ευπροσάρμοστης και μελλοντικά βιώσιμης αρχιτεκτονικής δικτύου κινητής τηλεφωνίας. Η αρχιτεκτονική θα επιτρέψει πρωτοφανή επίπεδα προσαρμοστικότητας του δικτύου, διασφαλίζοντας τις αναγκαίες σε επίπεδο απόδοσης, ασφάλειας, κόστους και ενέργεια απαιτήσεις οι οποίες θα πρέπει να πληρούνται.

Παράλληλα, προκειμένου να αναδειχθεί η αξία της αρχιτεκτονικής τόσο στον κλάδος της ασύρματης επικοινωνίας όσο και σε επίπεδο χρηστών στο ευρύτερο κοινωνικό σύνολο, θα διεξαχθεί μία κοινωνικοοικονομική ανάλυση - σε στενή αλληλεπίδραση με την ανάλυση των περιπτώσεων χρήσης, προκειμένου να αξιολογηθούν και να προσδιοριστούν ποσοτικά τα οφέλη από τις καινοτομίες του έργου 5G NORMA.

Σε επίπεδο εφαρμογών, η αρχιτεκτονική 5G NORMA, θα παράσχει την αναγκαία προσαρμοστικότητα, με σκοπό την αποτελεσματική διαχείριση των ποικίλων απαιτήσεων και τις διακυμάνσεις στις απαιτήσεις κίνησης, οι οποίες προκύπτουν από τις ετερογενείς και μεταβαλλόμενες υπηρεσίες χαρτοφυλακίων. Ξεπερνώντας το

παράδειγμα των υφιστάμενων αρχιτεκτονικών «ένα σύστημα που ταιριάζει σε όλες τις υπηρεσίες», το έργο 5G NORMA θα επιτρέψει την προσαρμογή των μηχανισμών που εκτελούνται για συγκεκριμένες υπηρεσίες, στις απαιτήσεις της συγκεκριμένης υπηρεσίας, ως αποτέλεσμα ενός καινοτόμου παραδείγματος υπηρεσίας και την εξάρτηση από

Επίσης, το έργο 5G NORMA προτίθεται να εξασφαλίσει την οικονομική βιωσιμότητα της λειτουργίας του δικτύου και τις ανοικτές ευκαιρίες για νέους παίκτες, αξιοποιώντας παράλληλα την αποτελεσματικότητα της αρχιτεκτονικής, με τον πλέον οικονομικό και ενεργειακό τρόπο. Ενώ, αποβλέπει στην προώθηση της προ-τυποποίησης με τη δημιουργία συναίνεσης για συγκεκριμένες πτυχές του δικτύου κινητής τηλεφωνίας 5G.

3.3.4 5G – XHAUL

Το έργο 5G – XHAUL, προτείνει μία οπτικά συγκλίνουσα και ασύρματης μεταφοράς λύση, ικανή να συνδέει με εύκολο τρόπο Μικρές Κυψέλες (Small Cells) στο κεντρικό δίκτυο. Αξιοποιώντας την κινητικότητα των χρηστών, η προτεινόμενη λύση επιτρέπει τη δυναμική κατανομή των διαθέσιμων πόρων σε σημεία πρόσβασης (hotspots). Για την υποστήριξη αυτών των καινοτόμων εννοιών, η κύρια τεχνικές και ερευνητικές προκλήσεις είναι η ανάπτυξη:

- Δυναμικά προγραμματιζόμενων, υψηλής χωρητικότητας, χαμηλής χρονικής καθυστέρησης, σημείο-προς-πολλαπλά σημεία πομποδεκτών mm-Wave, σε συνεργασία με ραδιοκύματα sub-6-GHz.
- Κοινού συστήματος χρονικού καταμερισμού με προσφερόμενη ελαστική κατανομή εύρους ζώνης, σε συνεργασία με προηγμένα παθητικά οπτικά δίκτυα.
- Σχέδια γνωστικού ελέγχου μέσω λογισμικού, ικανά να προβλέψουν την κυκλοφοριακή ζήτηση σε χώρο και χρόνο, και κατ’ επέκταση, να αναδιαμορφώσει τις συνιστώσες του δικτύου.

Οι μικρές κυψέλες, τα δίκτυα πρόσβασης Cloud-Radio (C-RAN), τα δίκτυα Λογισμικού Καθορισμού (SDN), και η Εικονοποίηση Λειτουργιών Δικτύου (Network Function Virtualization – NVF), αποτελούν του παράγοντες κλειδί για τη

διευθυνσιοδότηση της ζήτησης για ευρυζωνικής σύνδεσης χαμηλού κόστους και ευέλικτων εφαρμογών.

Ο σχεδιασμός σεναρίου δικτύου μεταφορών για τα πυκνά αστικά, με ογκώδης ανάπτυξη μικρών κυψελών, αποτελεί βασική περίπτωση χρήσης για το 5G – XHAUL. Προβλέπεται ένα πυκνό στρώμα – επίπεδο Μικρών Κυψελών (Small Cells), που βρίσκεται σε απόσταση 50-200 μέτρα απόσταση και 2-6 μέτρα πάνω από το επίπεδο του δρόμου, για παράδειγμα, τοποθετημένο πάνα σε στύλους λαμπτήρων, τοίχους κτιρίων, ή στάσεις λεωφορείων.

Οι Μικρές Κυψέλες μπορεί να είναι ασύρματα οπισθοζευκτικά (backhaul) στην περιοχή της κυψέλη μακροεντολής ή συνδεδεμένα σε ένα κεντρικό κόμβο συστημάτων γραφείου μέσω παθητικών οπτικών δικτύων.

Τα οπτικά δίκτυα επιμερισμού χρόνου (TSON) παρέχουν μεγάλη ταχύτητα και ευέλικτη συνδεσιμότητα σε μητροπολιτικό ή κεντρικό δίκτυο. Ενώ, οι τεχνολογίες 5G – XHaul θα ενσωματωθούν και θα αξιολογηθούν σε μία αίθουσα δοκιμών ένα κατά μήκος της πόλης του Bristol στο Ηνωμένο Βασίλειο.

Προκειμένου να παράσχει ένα αποτελεσματικό οπισθοζευκτικό για τα μελλοντικά δίκτυα κινητής τηλεφωνίας, η βιομηχανία αναγνώρισε το mm-Wave ως μία από τις πιο ελπιδοφόρες τεχνολογίες. Μία σημαντική τεχνολογική επίδραση του 5G – XHaul, αποτελεί η διαμόρφωση του σχεδιασμού των μελλοντικών συστημάτων mm-Wave, μέσω πρωτοποριακών αρχιτεκτονικών πομποδεκτών και πειραματικών επικυρώσεων. Στον τομέα των οπτικών πεδίων, είναι αναγκαία η εξεύρεση καινοτόμων λύσεων για την αύξηση της ευελιξίας της παροχής συνδεσιμότητας, της παρακολούθησης και της αντιμετώπισης προβλημάτων στο δίκτυο. Τέλος, το έργο 5G – XHaul, έχει άμεσο αντίκτυπο στην υιοθέτηση των τεχνικών SDN τόσο στο οπτικό όσο και στον ασύρματο τομέα.

3.3.5 CHARISMA

Συγκέντρωση ετερογενούς προηγμένης αρχιτεκτονικής 5G Cloud-RAN, για Έξυπνα και Ασφαλή Media AccessProject name. Η CHARISMA συγκεντρώνει ασύρματη πρόσβαση – 10G (μέσω mm-wave/60-GHz και οπτικά ελεύθερου χώρου, FSO) και 100G σταθερές οπτικές λύσεις (OFDM-PON), μέσω έξυπνου δικτύου cloud radioaccess (C-RAN) και μίας έξυπνης πλατφόρμας αναμετάδοσης πορείας με δρομολόγηση IPv6

Trust Node, διαθέτοντας πολύ χαμηλή διαχείριση κυκλοφορίας. Το χαμηλού κόστους Ethernet, χρησιμοποιείται σε όλο το μπροστινό και στο πίσω μέρος του δικτύου (Front and backhaul), με εικονικοποιημένο εξοπλισμό τελικών χρηστών (vCPE), κατανεμημένα σε όλες τις μεταφορές δεδομένων. Οι διασυνδέσεις ad-hoc για κινητές συσκευές (D2D, D2I, C2C etc.) δίκτυο παροχής περιεχομένου (CDN) και η διανεμημένη προσωρινή αποθήκευση μέσω κινητού τηλεφώνου (MDC) προσφέρουν μια αρχιτεκτονική δικτύου που βασίζεται στην πληροφορία (ICN). Επιπλέον, η προσωρινή αποθήκευση παρέχει αποτελεσματική χρήση των σπάνιων πόρων μέσω της χαμηλότερης κοινής συνάθροισης δεδομένων ή / και τοπικής εκτέλεσης επικοινωνιών. Επίσης, η CHARISMA θα εκμεταλλευτεί τεχνολογίες προγραμματισμού και εικονικοποίησης δικτύων για την επίτευξη πολλαπλών μισθώσεων και θα επιτρέψει την ταχεία υιοθέτηση αναδυόμενων εφαρμογών δικτύου.

Σε επίπεδο εφαρμογών, η λύση του έργου CHARISMA συμβάλλει στην ανάπτυξη πολλών εφαρμογών που απαιτούν τη μετάδοση ευαίσθητων προσωπικών δεδομένων όπως: ηλεκτρονική υγεία, απομακρυσμένη ιατρική, παρακολούθηση ευεξίας κλπ., που βασίζονται σε συνδέσεις χαμηλής λανθάνοντος χρόνου και χαμηλού κινδύνου, χρησιμοποιώντας υψηλής ταχύτητας και υψηλού εύρους ζώνης επικοινωνιών. Έτσι, πέρα από την ανάπτυξη 5G για τις παραδοσιακές κινητές επικοινωνίες, νέες εφαρμογές για έξυπνα σπίτια (smart homes) και IoT / everything, μελετώνται δίνοντας ιδιαίτερη έμφαση στην ασφάλεια από άκρο σε άκρο.

3.3.6. COGNET

ΓΝΩΣΤΙΚΆ ΔΙΚΤΥΑ (COGNITIVE NETWORKS)

- Συλλογή και επεξεργασία «Μεγάλων Δεδομένων» (Big Data) από τα δίκτυα 5G σε πραγματικό χρόνο.
- Ανάπτυξη νέων αλγορίθμων χρησιμοποιώντας μηχανή μάθησης για τη μάθηση μέσω των δεδομένων που συλλέχθηκαν και για την εφαρμογή στη διαχείριση δικτύου.
- Βελτίωση της επεκτασιμότητας (scalability), της ανθεκτικότητας και της ασφάλειας των δικτύων 5G.
- Πραγματοποίηση μετρίσιμων βελτιώσεων στα δίκτυα όπως αναγνωρίζονται μέσω των KPLs.

Το έργο «CogNet» στοχεύει στην έρευνα και στην ανάπτυξη μιας πλατφόρμας διαχείρισης δικτύου σε πραγματικό χρόνο, με τη δυνατότητα κλιμάκωσης για την αντιμετώπιση των απαιτήσεων, του μελλοντικού δικτύου 5G.

Πιο συγκεκριμένα:

- Για τη συλλογή και την επεξεργασία μεγάλων δεδομένων από το δίκτυο
- Ανάπτυξη, ενός συστήματος για αυτοδιαχείριση των δικτυακών κόμβων, κατά την διαχειριστική υποστήριξη του ενοποιημένου δικτύου.
- Εφαρμογή του αλγόριθμου Μηχανής Μάθησης για διευθυνσιοδότηση
    a. Πρόβλεψη ζήτησης και τροφοδοσίας επιτρέποντας στο δίκτυο την αλλαγή μεγέθους με τη χρήση εικονικής διαμόρφωσης.
    b. Θέματα προσαρμοστικότητας δικτύου συμπεριλαμβανομένου του εντοπισμού σφαλμάτων δικτύου, σφαλμάτων ή καταστάσεων όπως συμφόρηση ή υποβάθμιση της απόδοσης.
- Αναγνώριση σημαντικών ζητημάτων ασφάλειας όπως η μη εξουσιοδοτημένη παρέμβαση ή συμβιβασμένα στοιχεία του δικτύου και συνεργασία με αυτόνομο δίκτυο διαχείρισης για τη διατύπωση και την λήψη της κατάλληλης

3.3.7. COHERENT

Η ραγδαία ανάπτυξη της κινητής κυκλοφορίας (mobile traffic), η δραστική αύξηση της πολυπλοκότητας του δικτύου και η έντονη ανάγκη συντονισμού μεταξύ των δια-δικτύων των πόρων του ασύρματου δικτύου, απαιτούν πρόοδο – τομές σε επίπεδο ελέγχου και συντονισμού, αλλά και ευέλικτη διαχείριση του δικτυακού φάσματος 5G. Το έργο με την ονομασία «Coherent» ασχολείται με τις προκλήσεις οι οποίες έχουν προκύψει σε επίπεδο συντονισμού των δια-δικτύων 5G, των ετερογενών δικτύων RAN (radio access networks), με την εισαγωγή αρχών δικτυακού σχεδιασμού λογισμικά καθορισμένου εντός των RAN. Επιπρόσθετα, προβλέπεται να ασχοληθεί με την ανάπτυξη κοινών διεπαφών ελέγχου και λογισμικού εξοπλισμού ο οποίος θα επιτρέπει τον προγραμματιστικό έλεγχο και το συντονισμό μεταξύ ετερογενών κινητών δικτύων. Ο έλεγχος προγραμματισμού σε δίκτυα 5G-RAN θα προσφέρει στους φορείς εκμετάλλευσης ένα ευέλικτο και οικονομικά αποδοτικό τρόπο για την υλοποίηση νέων λειτουργιών χαμηλού επιπέδου, την παροχή ασύρματων πόρων, τη

διαχείριση διαφορετικών τύπων RAN και επίσης υποστήριξη στην ανοικτή καινοτομία στα δίκτυα κινητής τηλεφωνίας 5ης γενιάς (5G).

3.3.7. EURO – 5G

Υποστήριξη της Ευρωπαϊκής Πρωτοβουλίας 5G

Ως βασικός οργανωτής των διαδικασιών διακυβέρνησης των 5G-PPP, το έργο **EURO – 5G** θα αναλάβει δράσεις προκειμένου να διασφαλιστεί η ειλικρίνεια, η δικαιοσύνη και η διαφάνεια μέσω όλων των δραστηριοτήτων του 5G PPP. Ενώ, θα δρομολογήσει ένα πρόγραμμα εντατικής επικοινωνίας και διάδοσης, προκειμένου να τονιστούν τα αποτελέσματα των 5G-PPP.

Πρωταρχικός στόχος του έργου **Euro – 5g**, αποτελεί η διευκόλυνση της αποτελεσματικής και αποδοτικής συνεργασίας, καθώς και η συνεργασία μεταξύ όλων των έργων των 5G-PPP, της Ευρωπαϊκής Επιτροπής, της Ένωσης Υποδομών 5G, του Networld2020 ETP, όλων των σχετικών έργων με το EUREKA, και σχετικές εθνικές πρωτοβουλίες με σκοπό τη μεγιστοποίηση της ευρωπαϊκής δυναμικής προς τα μελλοντικά ολοκληρωμένα δίκτυα υψηλής χωρητικότητας.

Το έργο **Euro – 5g** προβλέπετε να διευκολύνει τις ομάδες εργασίας οι οποίες καλύπτουν τα έργα 5G-PPP και τη Networld2020 κοινότητα για την ανάπτυξη ενημερωτικών θέσεων σε προ-πρότυπα και φάσμα, τα οποία θα τροφοδοτήσουν τις ευρωπαϊκές και παγκόσμιες συζητήσεις προς αυτές τις περιοχές. Η φιλοδοξία είναι να διασφαλιστεί ότι, τα πρότυπα 5G που θα προκύψουν θα είναι χρήσιμα και αποτελεσματικά, για την τόνωση της αφομοίωσης, ότι θα υπάρχει διαθέσιμο επαρκές φάσμα και ότι η χρήση τους θα βελτιστοποιηθεί έως το 2020 για τις επικοινωνίες.

Παράλληλα, το έργο θα παρακολουθεί και θα αναλύει τις διεθνείς 5G δραστηριότητες – ενέργειες, ενώ προβλέπετε να διευκολύνει σχετικές δραστηριότητες (συναντήσεις, εργαστήρια) και την κοινή συνεργασία μεταξύ της Ένωσης Υποδομών 5G και της Ευρωπαϊκής Επιτροπής, προκειμένου να εδραιωθούν καλές διεθνείς σχέσεις με αυτές τις παγκόσμιες πρωτοβουλίες, με γνώμονα τη διασφάλιση της παγκόσμιας διαλειτουργικότητας. Παράλληλα, ειδικοί υψηλής εξειδίκευσης θα ασχοληθούν με την κατάρτιση χαρτών καινοτομίας και την κάλυψη των πειραματικών απαιτήσεων των επόμενων φάσεων των 5G-PPP.

3.3.8. FANTASTIC – 5G

Η κύρια πρόκληση για το έργο FANTASTIC-5G είναι, η ανάπτυξη ενός πολλαπλού συστήματος διασύνδεσης το οποίο θα είναι σε θέση να υποστηρίξει όλες τις προσδοκώμενες περιπτώσεις χρήσης, με την υψηλότερη απόδοση και επεκτασιμότητα, χωρίς να καταστεί περίπλοκη από πλευράς δικτύου. Για το σκοπό αυτό, το έργο θα αναπτύξει τα τεχνικά στοιχεία AI (ευέλικτη κυματομορφή και σχεδιασμός πλαισίου, κλιμακούμενες διαδικασίες πολλαπλής πρόσβασης, προσαρμοστικά προγράμματα αναμετάδοσης, ενισχυμένα συστήματα πολλαπλών κεραιών με ή χωρίς συνεργασία, προηγμένη ανίχνευση πολλαπλών χρηστών, συντονισμό παρεμβολών, υποστήριξη υπερ-πυκνών διατάξεων κυψελών, διαχείριση πολλαπλών κυψελών ραδιοσυχνοτήτων) και ενσωμάτωση τους σε ένα ευρύτερο πλαίσιο AI, όπου η προσαρμογή στον υψηλότερο βαθμό ετερογένειας 5G που θα κληθεί να αντιμετωπίσει θα επιτευχθεί.

Αντικείμενο το έργου FANTASTIC-5G είναι:

- η ανάπτυξη μίας ευέλικτη και κλιμακούμενης διεπαφής αέρος πολλαπλών υπηρεσιών.
- Η πλήρη κάλυψη και υψηλή χωρητικότητα όπου απαιτείται
- Η αποτελεσματικότητα σε επίπεδο κατανάλωσης ενέργειας και πόρων
- Να παράσχει μελλοντική προστασία και να επιτρέψει τη βιώσιμη παροχή ασύρματων υπηρεσιών και μετά το 2020.
- Η επικύρωση και η αξιολόγηση των ανεπτυγμένων εννοιών
- Η ανάπτυξη κοινής συναίνεσης σε λογικές επιλογές για την τυποποίηση των 5G.

Το έργο πραγματεύεται αποκλειστικά με χαμηλότερη φέρουσα συχνότητα (<6GHz), ενώ φιλοδοξεί να ανταποκριθεί στην ισχυρή ανάπτυξη των απαιτούμενων ρυθμών δεδομένων (εξελικτική επίδραση) και στη διερεύνηση του επιχειρηματικού μοντέλου των φορέων εκμετάλλευσης με τη διεύρυνση των υπηρεσιών.

Η βασική διαφοροποίηση μεταξύ αυτών των βασικών υπηρεσιών είναι η σχετική υπηρεσία καθορισμού των δεικτών KPIs:

- Mobile Broadband (MBB) Κινητή Τεχνολογία Ευρείας Ζώνης
- Mission Critical Communications (MCC):
- Massive Machine Communications (MMC):
- Broad- and Multicast Services (MBS):
- Vehicle –to-Vehicle and Vehicle-to-Infrastructure Services (V2X): Υψηλή κινητικότητα.

3.3.9. METIS – II

Κινητές και Ασύρματες Επικοινωνίες

Το έργο METIS-II θα παράσχει έναν ευρύτερο σχεδιασμό 5G RAN, περιγράφοντας μια συνολική αρχιτεκτονική στοίβας πρωτοκόλλων με όλες τις λειτουργικότητες και τις διεπαφές οι οποίες απαιτούνται, για την επίτευξη του οράματος των 5G. Ο συνολικός σχεδιασμός των 5G θα δομηθεί πάνω στους ακόλουθους βασικούς πυλώνες καινοτομίας που αναπτύχθηκαν στο έργο METIS-II**:**

- Ολιστική αρχιτεκτονική διαχείρισης ραδιοφάσματος
- Ολιστικό πλαίσιο εναρμόνισης της διεπαφής αέρος
- Ευέλικτο πλαίσιο διαχείρισης πόρων (PM)
- Διασυνδεδεμένο και cross-air-interface περιβάλλον πρόσβασης και πλαίσιο κινητικότητας
- Κοινό πλαίσιο ελέγχου και πλαισίου χρηστών

Παράλληλα, το έργο METIS-II θέτει τους παρακάτω στόχους:

- Τη συνολική ανάπτυξη του σχεδίου 5G RAN, εστιάζοντας ιδιαίτερα στο σχεδιασμό της τεχνολογίας για την αποτελεσματική ενσωμάτωση των εννοιών του κληροδοτημένου και καινοτόμου δικτύου ασύρματης πρόσβασης (RAN), εντός ενός ολιστικού συστήματος .
- Παρέχει το 5G πλαίσιο συνεργασίας εντός του 5G-PPP για το σχεδιασμό του 5G RAN και μία κοινή αξιολόγηση των 5G RAN εννοιών τόσο από πλευράς απόδοσης όσο και από τεχνο-οικονομικής πλευράς. Ειδικότερα, το έργο METIS-II θα βελτιώσει περαιτέρω τα σενάρια, τις απαιτήσεις και τους βασικούς δείκτες απόδοσης (KPIs), θα αναπτύξει ένα πλαίσιο απόδοσης και

τεχνικο-οικονομικής αξιολόγησης και ένα εργαλείο αξιολόγησης και απεικόνισης ανοικτού κώδικα, για την υλοποίηση των βασικών περιπτώσεων χρήσης 5G και σχεδιαστικές λύσεις RAN. Επιπρόσθετα, το έργο METIS-II επιδιώκει να διευκολύνει την οικοδόμηση κοινής συμφωνίας εντός του 5G-PPP, για παράδειγμα μέσω της οργάνωσης μίας σειράς παράλληλων εργαστηρίων για 5G-PPP.

- Την προετοιμασία μιας συντονισμένης προσπάθειας προς τους ρυθμιστικούς και φορείς και τους φορείς πιστοποίησης για την αποτελεσματική τυποποίηση, ανάπτυξη και οικονομικά ελκυστική παρουσίαση των 5G.

Μέχρι το τέλος του 2015, το έργο METIS-II απέβλεπε στον καθορισμό ενός σημαντικού συνόλου υποθέσεων χρήσης των 5G, αξιοποιώντας τις περιπτώσεις χρήσης του METIS, άλλων έργων σε επίπεδο Ευρωπαϊκής Ένωσης και οργανισμών όπως τα έργα Μέχρι τα τέλη Σεπτεμβρίου 2015, το METIS-II θα καθορίσει ένα ουσιαστικό σύνολο υποθέσεων χρήσης 5G, αξιοποιώντας τις περιπτώσεις χρήσης του METIS, άλλων σχεδίων και οργανισμών της ΕΕ όπως το NGMN και το ITU-R.

3.3.10. mmMAGIC

Τεχνικές και Ερευνητικές Προκλήσεις

Η χρήση πολύ υψηλών συχνοτήτων για τις κινητές επικοινωνίες αποτελούν μία δύσκολη πρόκληση, ωστόσο είναι αναγκαίες για την υποστήριξη της ακραίας κινητής ευρυζωνικής υπηρεσίας της 5G, η οποία απαιτεί πολύ υψηλή ρυθμό δεδομένων (πάνω από 10Gbps) και σε κάποιες περιπτώσεις, επίσης πολύ χαμηλές end-to-end χρόνους αναμονής (μικρότερες από 5 ms).

Στο έργο, η κυματομορφή, η δομή πλαισίου και η αριθμολογία, θα αναπτυχθούν και θα σχεδιαστούν όπως ακριβώς οι νέες προσαρμοστικές και συνεργατικές τεχνικές σχηματισμού δέσμης και παρακολούθησης για την αντιμετώπιση των συγκεκριμένων προκλήσεων των χιλιοστομετρικών κυμάτων των κινητών επικοινωνιών. Παράλληλα, θα εκτελέσει εκτεταμένες μετρήσεις ραδιοφωνικών καναλιών στα 6-100Ghz και θα αναπτύξει προηγμένα μοντέλα καναλιών την πραγματοποίηση αυστηρής επικύρωσης και ανάλυσης σκοπιμότητας στις προτεινόμενες έννοιες, καθώς και για χρήση από ρυθμιστικά και πρότυπα φόρουμ. Η απρόσκοπτη και ευέλικτη ενσωμάτωση με άλλες

5G και παλαιού τύπου διεπαφές, θα πραγματοποιηθεί μέσω του σχεδιασμού και της επικύρωσης των νέων διαδικτυακών λειτουργιών και των αρχιτεκτονικών στοιχείων.

Βασικός στόχος στο έργο mmMAGIC είναι η ανάπτυξη εννοιών και βασικών εξαρτημάτων για μία νέα 5G τεχνολογία κινητής ραδιοεπικοινωνίας, η οποία αναμένεται να λειτουργεί σε ένα εύρος ζωνών συχνότητας μεταξύ 6 και 100Ghz, που εδώ αναφέρεται ως συχνότητες χιλιοστομετρικών κυμάτων. Περιοχές συχνοτήτων κατάλληλες για την υποστήριξη των αναγνωρισμένων περιπτώσεων χρήσης 5G, θα αναγνωρίζονται και θα αξιολογούνται. Αυτό το νέο RAT προβλέπεται ότι θα αποτελέσει βασικό συστατικό του συνολικού οικοσυστήματος 5G-RAT. Επίσης το έργο αποβλέπει στο να επιταχυνθεί η τυποποίηση των mm-wave τεχνολογιών για 5G, έτσι ώστε η βιομηχανία και οι πολίτες να ωφεληθούν από την εμπορευματοποίηση του περίπου το 2020.

Σε επίπεδο εφαρμογών, οι mmMAGIC τεχνολογίες θα επιτρέψουν ένα εύρος ακραίων κινητών ευριζωνικών υπηρεσιών και εφαρμογών για τους χρήστες κινητής, όπως το UHD TV video streaming, εικονική πραγματικότητα και εξαιρετικά ευέλικτες εφαρμογές οι οποίες βασίζονται σε νέφη (cloud). Οι δυνατότητες auto-backhauling επίσης προβλέπονται, πέρας της πρόσβασης, δημιουργώντας ως εκ τούτου μία ολιστική, κλιμακούμενη και οικονομικά βιώσιμη ολοκληρωμένη λύση 5G, με σκοπό την κάλυψη μελλοντικών αναγκών των φορέων εκμετάλλευσης και των χρηστών.

3.3.11. SELFNET

Πλαίσιο για την Αυτό-Οργανωμένη Διαχείριση Δικτύου σε Virtualized και Δίκτυα Καθορισμένα από Λογισμικό.

Το έργο SELFNET αναμένεται να ενεργοποιήσει και να βελτιστοποιήσει την ολιστική χρήση των SDN (Software Defined Networking), των NFV (Network Function Virtualization), cloud-computing, AI και άλλες σχετικές τεχνολογίες για την επίτευξη νέων οικονομικά αποδοτικών πραγματικού χρόνου αυτόνομη 5G διαχείριση δικτύου. Επίσης θα συμβάλει στο σχεδιασμό υψηλής απόδοσης μετρήσεων HoN, τα οποία θα αντικατοπτρίζουν με ακρίβεια την υφιστάμενες συνθήκες λειτουργίας του δικτύου και των υπηρεσιών, σε σχέση με τις απαιτήσεις του 5G Key Performance Indicator (KPI). Στην επινόηση καινοτόμων, αποδοτικών και με δυνατότητα

επέκτασης αλγορίθμων για την επίλυση ή το μετριασμό των πιθανών προβλημάτων διαχείρισης του δικτύου.

3.3.12 SESAME

Συντονισμός μικρών κυψελών για υπηρεσίες πολλαπλών μισθώσεων και άκρων

Βασικό στοιχείο του έργου με την ονομασία SESAME θα αποτελέσει η εικονοποίηση των Μικρών Κυψελών και η αξιοποίηση τους, καθώς και ο διαχωρισμός τους σε λογικά μεμονωμένα τμήματα που προσφέρονται σε πολλαπλούς χειριστές/κατόχους. Βασική πτυχή αυτής της καινοτομίας θα αποτελέσει η δυνατότητα φιλοξενίας πολλαπλών φορέων εκμετάλλευση κάτω από την ίδια δομή, ικανοποιώντας το προφίλ και τις απαιτήσεις κάθε φορέα ξεχωριστά.

Η πλατφόρμα εκτέλεσης Light DC θα χρησιμοποιηθεί για την υποστήριξη των απαιτούμενων VNF, τα οποία υλοποιούν τα διαφορετικά χαρακτηριστικά/δυνατότητες των Μικρών Κυψελών. Λύσεις για την ομαδοποίηση των δεδομένων, την κωδικοποίηση του περιεχομένου βίντεο με βελτιστοποιημένη παράδοση σε edge networks και cashing στο άκρο του δικτύου, θα επιτρέψει τη μείωση του χρόνου παράδοσης και ως εκ τούτου θα παράσχουν μία αυστηρή διαδρομή για την επιτυχή μείωση χρόνιου σε επίπεδο υπηρεσιών.

Το έργο με την ονομασία SESAME, στοχεύει σε καινοτομίες γύρω από τρία κεντρικά στοιχεία του 5G, την τοποθέτηση πληροφοριών και εφαρμογών στην άκρη του δικτύου μέσω Λειτουργιών Εικονοποίησης Δικτύου (NFV) και Edge Cloud Computing, την ουσιώδη εξέλιξη της ιδέα των Μικρών Κυψελών, η οποία έχει ήδη ενσωματωθεί στα 4G, αλλά αναμένεται να διανείμει το πλήρη δυναμικό της στα απαιτητικά υψηλής πυκνότητας σενάρια 5G, και την ενοποίηση της πολλαπλής μίσθωσης στις υποδομές επικοινωνιών, επιτρέποντας σε αρκετούς φορείς εκμετάλλευσης / παρόχους υπηρεσιών να συμμετάσχουν σε νέα μοντέλα κοινής χρήσης, τόσο της ικανότητας πρόσβασης όσο και των δυνατοτήτων υπολογιστικής άκρης.

Το έργο SESAME, προτείνει την έννοια Cloud-Enabled Small Cell (CESC), ένα νέο πολύ-διαχειριστή Μικρών Κυψελών που ενσωματώνει μία εικονοποιημένη πλατφόρμα εκτέλεσης για την ανάπτυξη Virtual Network Functions (VNFs),

υποστηρίζοντας τη δυναμική διαχείριση Self-x και την εκτέλεση νέων εφαρμογών και υπηρεσιών εντός της υποδομής του δικτύου πρόσβασης.

3.3.13 SONATA

Το Software Defined Networking (SDN) και το Network Function Virtualization (NFV), αναδύονται ως μείζων τεχνολογίες μετασχηματισμού, αναπτύσσοντας τον τομέα των τηλεπικοινωνιών με νέες δυνατότητες δικτύου και επιχειρηματικές ευκαιρίες. Το έργο SONATA, διευθύνει σημαντικές προκλήσεις οι οποίες σχετίζονται τόσο με την ανάπτυξη όσο και με το άνοιγμα των πολύπλοκων υπηρεσιών που προβλέπονται για τα δίκτυα 5G και εξουσιοδοτούνται από αυτές τις τεχνολογίες:

- Μοντέλα, μεθόδους και εργαλεία προγραμματισμού εικονοποιημένων υπηρεσιών.
- Μεθόδους, χειριστές και αλγόριθμους για την ομοειδή και ενοποιημένη ενορχήστρωση των υπηρεσιών δικτύου, πάνω από μία υποδομή η οποία παρέχει συνδεσιμότητα, υπολογισμό και αποθηκευτικούς πόρους.
- Εργαλεία για την αποτελεσματική και αξιόπιστη ανάπτυξη και διαχείριση των ανεπτυγμένων δικτύων, εντός ενός δυναμικού και επιδεκτικού τρόπου διερεύνησης.
- Αποτελεσματική ενσωμάτωση της ανάπτυξης και των διαδικασιών των υπηρεσιών, μεταξύ ποικίλων παραγόντων.

Το έργο SONATA στοχεύει στον ευέλικτο προγραμματισμό των δικτύων λογισμικού, υποστηρίζοντας την αλυσιδωτή λειτουργία του δικτύου και την ενορχήστρωση. Οι καινοτομίες θα καταστήσουν τις πλατφόρμες υπηρεσιών ευκολότερα προσπελάσιμες για την κάλυψη των αναγκών των διαφόρων παρόχων υπηρεσιών και την εισαγωγή ενός εξειδικευμένου μοντέλου υποστήριξης υπευθύνων ανάπτυξης. Ειδικοί στόχοι αποβλέπουν:

- Στη μείωση του χρόνου αγοράς των δικτυακών υπηρεσιών με α) την απλοποίηση της ανάπτυξης με αφαιρούμενα μοντέλα προγραμματισμού και β) την εφαρμογή ενός μοντέλου DevOps το οποίο ενοποιεί – ενσωματώνει

τους φορείς εκμετάλλευσης, τους κατασκευαστές και τους τρίτους προγραμματιστές.

- Στη βελτιστοποίηση των χρησιμοποιούμενων πόρων μέσω ενορχήστρωσης και στη μείωση του κόστους ανάπτυξης και λειτουργίας των υπηρεσιών με α) τη χαρτογράφηση πολύπλοκων υπηρεσιών σε επίπεδο συνδεσιμότητας, υπολογισμού και αποθηκευτικών πόρων, και β) με αυτόματη εκτέλεση αναδιαμόρφωσης / ανταγωνιστικές υπηρεσίες.

Επιτάχυνση της υιοθέτηση των δικτύων λογισμικού από τη βιομηχανία με α) την υποστήριξη του κύκλου ζωής πλήρους υπηρεσίας: ανάπτυξη, δοκιμή, ενορχήστρωση, διαχείριση και λειτουργία και β) τον καθορισμό ενός οδικού χάρτη για την αξιοποίηση των αποτελεσμάτων, προς τη μεγαλύτερη μετάβαση στο SDN/NFV.

3.3.14 SPEED –5G

Ο κύριος στόχος του έργου SPEED – 5G είναι, να πετύχει μία σημαντικά καλύτερη εκμετάλλευση των ετερογενών ασύρματων τεχνολογιών, παρέχοντας μεγαλύτερη χωρητικότητα σε συνάρτηση με την υπερ-πυκνότητα της κυψελοειδούς τεχνολογίας, και την αποτελεσματική υποστήριξη των απαιτήσεων της νέας 5G Quality of Experience (QoE).

Στα πλαίσια του έργου SPEED – 5G θα αναπτυχθούν νέες τεχνολογίες για τη βελτιστοποίηση της χρήσης του φάσματος, με βάση τρείς κύριες διαστάσεις:

- Υπερ-συμπύκνωση μέσω μικρών κυψελών
- Πρόσθετο φάσμα
- Εκμετάλλευση των πόρων σε όλες τις τεχνολογίες

Στο έργο SPEED – 5G, αυτό το τρισδιάστατο μοντέλο αναφέρεται ως εκτεταμένη Δυναμική Κατανομή Φάσματος (DSA – Dynamic Spectrum Allocation), όπου πολλές ζώνες φάσματος, κυψέλες και τεχνολογίες διοικούνται από κοινού ώστε να προσφέρουν βελτιωμένη QoE και τρομακτική αύξηση της χωρητικότητας, εντός ενός οικονομικά αποδοτικού πλαισίου.

3.3.15 SUPERFLUIDITY

Πλήθος αδυναμιών επηρεάζουν σήμερα τα δίκτυα, υπερβολικά μακρά χρονικά περιθώρια παροχής, εξάρτηση από την ιδιοκτησία, δυσκολία στην τροποποίηση, οικονομικά-αναποτελεσματικές συσκευές υλικού και πολυπλοκότητα, η οποία προκύπτει από ένα ευρύ φάσμα τεχνολογιών ετερογενούς πρόσβασης.

Βασικός στόχος του έργου **SUPERFLUIDITY** είναι, η εικονική λειτουργία δικτύου επεξεργασίας, on-demand, σε υποδομή τρίτων που εντοπίζεται σε όλο το δίκτυο και την ανάπτυξη τεχνολογιών οι οποίες επιτρέπουν τέτοιες υπηρεσίες να είναι «υπερρευστές».

- Γρήγοροι χρόνοι Instantiation (σε χιλιοστά του δευτερολέπτου)
- Γρήγορη μετάβαση (σε εκατοντάδες χιλιοστά του δευτερολέπτου)
- Γρήγορη ενοποίηση (εκτέλεση χιλιάδων σε ένα μόνο διακομιστή)
- Υψηλή απόδοση (10Gb/s και υψηλότερη)

Το έργο **SUPERFLUIDITY** αντιμετωπίζει αυτές τις προκλήσεις με μία ολοκληρωμένη στρατηγική πολλαπλών κατευθύνσεων:

Ευελιξία, μέσω αρχιτεκτονικής αποσύνθεσης των στοιχείων του δικτύου και των υπηρεσιών δικτύου σε στοιχειώδη, αρχέγονα πολλαπλών χρήσεων.

Απλότητα, μέσω μίας cloud-based αρχιτεκτονικής.

Ευκινησία, μέσω της εικονοποίησης των radio και των δικτύων επεξεργασίας εργασιών.

Φορητότητα και βιωσιμότητα, μέσω αφαίρεσης ανεξάρτητα από την πλατφόρμα, επιτρέποντας την επαναχρησιμοποίηση των λειτουργιών δικτύου σε πολλαπλές ετερογενείς πλατφόρμες υλικού.

Υψηλές επιδόσεις, μέσω επιτάχυνσης λογισμικού, ειδίκευση και προσαρμογή σε επιταχυντές υλικού.

3.3.16 VIRTUWIND

Εικονικό και προγραμματιζόμενο πρότυπο βιομηχανικού δικτύου που αναπτύσσεται στο επιχειρησιακό Αιολικό πάρκο

Ο κύριος στόχος του έργου VIRTUWIND είναι να αναπτύξει ένα SDN & NFV οικοσύστημα για βιομηχανικούς τομείς, βασισμένο σε ένα ασφαλές πλαίσιο επικοινωνίας, που θα οδηγήσει σε μία πρωτότυπη επίδειξη για intra-domain και inter-domain σενάρια σε πραγματικά αιολικά πάρκα, ως μία αντιπροσωπευτική περίπτωση χρήσης σε βιομηχανικά δίκτυα και να ποσοτικοποίηση τα οικονομικά οφέλη της λύσης. Οι βασικοί στόχοι που τίθενται είναι οι ακόλουθοι:

- Κατανόηση της βιομηχανικής – τάξης της QoS για τη λύση SDN ανά τομέα.
- Εγγύηση μεταξύ inter-domain QoS για πολυεπίπεδο οικοσύστημα με βάση το SDN.
- Μείωση του χρόνου και τους κόστους για την παροχή υπηρεσιών και συντήρησης δικτύου.
- Εξασφαλίζει security-by-design για SDN και NFV οικοσυστήματα.
- Διεξαγωγή δοκιμής πεδίου για πρότυπο για intra- και inter-domain SDN και NFV.

Σε επίπεδο εφαρμογών, το έργο VirtuWind θα προσαρμόσει το SDN σύμφωνα με τις απαιτήσεις στα βιομηχανικά δίκτυα, με την ανάπτυξη νέων SDN-based μηχανισμών για την υλοποίηση industrial-grade QoS και τη μείωση CAPEX και OPEX, στο δίκτυο ελέγχου του αιολικού πάρκου.

3.3.17 Crosshaul

Η ενσωμάτωση 5G fronthaul/backhaul

Το έργο Crosshaul έχει αναλάβει το σχεδιασμό των νέων 5G backhauling/fronthauling δικτύου για 5G και αναμένεται να δώσει λύση στο θεμελιώδες κόστος, τη δικτυακή αποτελεσματικότητα και ζητήματα κλιμάκωσης του δικτύου μεταφοράς 5G στις ακόλουθες πτυχές:

- Θα σχεδιάσει τη σύγκλιση συσκευών δικτύωσης (XFE) εκτελώντας ένα ενοποιημένο επίπεδο δεδομένων ικανό να μεταφέρει όλα τα είδη κίνησης Crosshaul. Αυτό θα μειώσει σημαντικά το κόστος δικτύου αξιοποιώντας τον ολοκληρωμένο σχεδιασμό δικτύου και θα βελτιώσει τη χρήση του δικτύου.

- Θα διευκολύνει την ποιότητα του δικτύου. Στο Crosshaul, νέες τεχνολογίες και λύσεις φυσικού στρώματος (μόχλευση οπτικής ίνας, οπτικά συστήματα ελεύθερου χώρου και χάλκινες υποδομές χαμηλού κόστους κ.α.) θα διερευνηθούν, προκειμένου να μειωθεί σημαντικά το κόστος ανάπτυξης και εγκατάστασης.

- Θα σχεδιάσει ένα συγκεντρωτικό επίπεδο ελέγχου το οποίο θα ακολουθεί το πρότυπο SDN, παρέχοντας υψηλή ευελιξία και δυνατότητα κλιμάκωσης (XCI).

Το έργο Crosshaul, στοχεύει στην ανάπτυξη μίας προσαρμοστικής, αξιόπιστης και οικονομικά αποδοτικής λύσης δικτύου μεταφορών 5G, η οποία θα ενσωματώνει τα τμήματα fronthaul και backhaul του δικτύου. Αυτό το δίκτυο μεταφοράς με ευελιξία θα διασυνδέσει διανεμημένες λειτουργίες δικτύου ραδιοπρόσβασης, καθώς και τις λειτουργίες του κεντρικού δικτύου, που φιλοξενείται στους κόμβους cloud-δικτύου, μέσω της υλοποίησης δύο νέων δομικών στοιχείων:

- Μία υποδομή ελέγχου που χρησιμοποιεί ένα ενοποιημένο, μοντέλο αφηρημένου δικτύου, για την ενοποίηση του επιπέδου ελέγχου (Xhaul/ Crosshaul Control Infrastructure, XCI).
- Ένα ενοποιημένο data plane το οποίο περικλείει καινοτόμες υψηλής-χωρητικότητας τεχνολογίες μετάδοσης και νέες καθοριστικές αρχιτεκτονικές latency switch (Xhaul/ Crosshaul Packet Forwarding Element, XFE).

Τέλος το έργο Crosshaul αποβλέπει να απλοποιήσει σημαντικά τις λειτουργίες δικτύου, παρά το αυξημένο τεχνολογικό εύρος. Έτσι θα καταστεί δυνατή η βελτιστοποίηση της QoS και της ενεργειακής χρήσης, καθώς και η ανάπτυξη εφαρμογών network-aware.

Κεφάλαιο 4- Αρχιτεκτονικές προτάσεις δικτύων 5ης γενιάς

4.1 Προτεινόμενη αρχιτεκτονική- backhaul και fronthaul

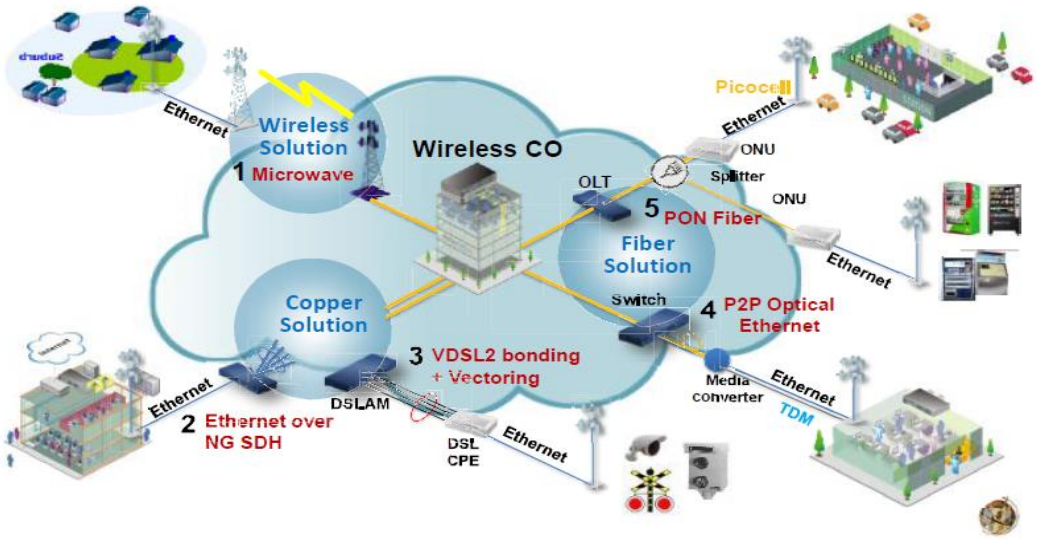
Η κίνηση των δεδομένων της κινητής τηλεφωνίας προβλέπεται να αυξηθεί 11 φορές περισσότερο μέχρι το τέλος του 2018. Τα δίκτυα 5ης γενιάς που πρόκειται να εξυπηρετήσουν αυτό τον μεγάλο όγκο δεδομένων, απαιτούν λύσεις μεταφοράς μεταξύ των ασύρματων δικτύων πρόσβασης (RAN) και των δικτύων κορμού (packet Core) προκειμένου να αντιμετωπίσουν το αυξημένο φορτίο δεδομένων, και παράλληλα να πληρούν τις απαιτήσεις των δικτύων 5ης γενιάς με οικονομικά αποδοτικό τρόπο. Σε αυτό το κεφάλαιο γίνεται μια ποιοτική επισκόπηση των διαφόρων προτεινόμενων τεχνολογιών που πληρούν τις απαιτήσεις μεταφοράς των δικτύων 5ης γενιάς. Η ποικιλία των απαιτήσεων και των σεναρίων ανάπτυξης καθιστά αδύνατη μια προσέγγιση που θα παραδώσει λύσεις backhaul, και fronthaul σε όλα τα δίκτυα, και για αυτό, απαιτείται ο συνδυασμός των διαφόρων τεχνολογιών για τη σύσταση του δικτύου μεταφορών 5ης γενιάς.

Οι παραπάνω τεχνολογίες διαχωρίζονται σε τρεις ομάδες. Αρχικά σε ασύρματες τεχνολογίες (microwave, mmWave, και optical wireless), οι οποίες χρησιμοποιούνται όταν δεν είναι εφικτές οι ενσύρματες επιλογές, ή σε περιπτώσεις όπου η ανάπτυξη και η δυνατότητα ασύρματων δικτύων απαιτείται (Έρευνα η οποία διεξάγεται από το έργο 5G Crosshaul). Ως δεύτερη τεχνολογία εκμετάλλευσης είναι η δυνατότητα της επαναχρησιμοποίησης της τρέχουσας εγκατεστημένης βάσης των υποδομών ινών (GPON,WDM) και χαλκού (G.FAST,VDSL bonding,VDSL bonding 35B) στο δίκτυο πρόσβασης, καθώς επίσης και η αναβάθμιση της (Έρευνα η οποία διεξάγεται από το έργο 5G Crosshaul). Τέλος, επανεξετάζονται σενάρια μεγάλης χωρητικότητας με την χρήση οπτικών ινών (WDM 100 Gbit/s transceivers and low-cost silicon photonic optical switches) προκειμένου να αναβαθμιστούν οι δυνατότητες του δικτύου και παράλληλα επιτευχθεί μείωση του υφιστάμενου κόστους ανά Gbit/s (Έρευνα η οποία διεξάγεται από το έργο 5G Crosshaul και XHaul)[11].

Για την εφαρμογή κάθε μιας από αυτές τις τεχνολογίες, πραγματοποιείται μελέτη με σκοπό την εκτίμηση της καταλληλότητας τους, για την ανάπτυξη του project 5G – Crosshaul και XHaul, αλλά και άλλων παρόμοιων έργων τα οποία χρηματοδοτούνται στα πλαίσια του προγράμματος HORIZON 2020. Αυτές οι

[11] http://5g-crosshaul.eu/

παράμετροι αναφέρονται στην πυκνότητα του δικτύου, την ενεργειακή του απόδοση, την απόσταση επιτεύξιμης σύνδεσης και στον προϋπολογισμό, στο συγχρονισμό και στην καθυστέρηση, στις εκτιμήσεις κόστους, σε πλήθος άλλων λειτουργικών πτυχών (π.χ. αξιοπιστία, αντιμετώπιση προβλημάτων, αυτόματη αναδιάρθρωση), καθώς και σε θέματα ανάπτυξης. Στην Εικόνα 4.1. διαφαίνεται ο τεχνολογικός χάρτης του δικτύου, με την χρήση των τριών τεχνολογικών σεναρίων που μελετούνται στα πλαίσια των έργων 5G Crosshaul και XHaul[12].



Εικόνα 4.1. Συνδυασμός των διαφόρων τεχνολογιών για τη σύσταση του δικτύου μεταφορών 5ης γενιάς.

4.1.1 Ασύρματα δίκτυα 5ης γενιάς

Όπως παρουσιάζεται στο τεχνολογικό χάρτη (Εικόνα 4.2.) του έργου 5G – Crosshaul, ο ρόλος των ασύρματων λύσεων είναι να καλύψουν εκείνες τις περιπτώσεις όπου οι ενσύρματες τεχνολογίες δεν μπορούν να αναπτυχθούν ή η ανάπτυξή τους είναι πάρα πολύ ακριβή. Οι συνδέσεις σταθερού σημείου-προς- σημείο ασύρματου backhaul και fronthaul με χρήση του φάσματος μέχρι τις ζώνες συχνοτήτων millimeter-wave, έχουν χρησιμοποιηθεί για την υποστήριξη της τρέχουσας γενιάς (4G/3G/2G) της κινητής τηλεφωνίας των δικτύων υψηλής χωρητικότητας. Ωστόσο, δεδομένου ότι οι τεχνολογικές απαιτήσεις της 5ης γενιάς αυξάνονται, οι ασύρματες backhaul και fronthaul τεχνολογίες αντιμετωπίζουν νέες προκλήσεις: μια αύξηση της

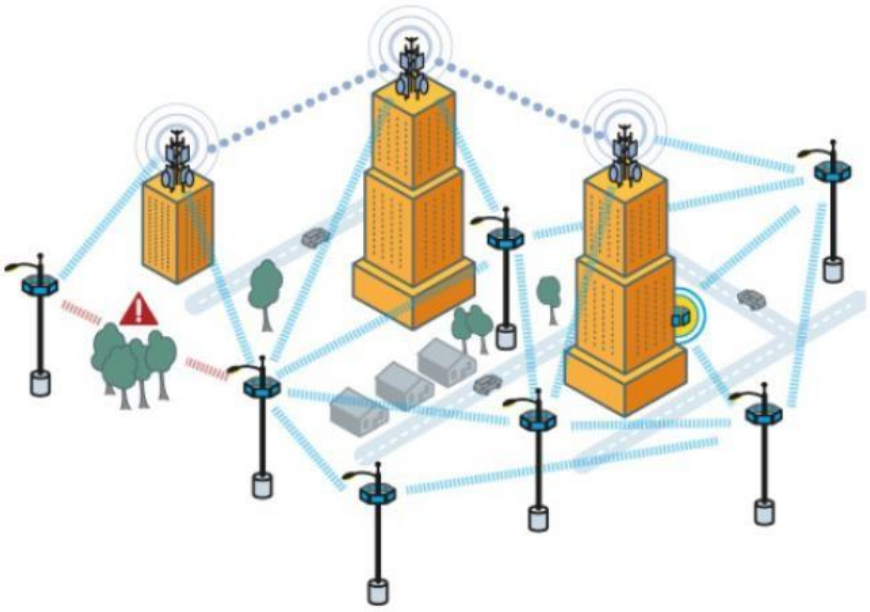
[12] http://5g-crosshaul.eu/

δυναμικότητας κατά 1000 φορές, την πύκνωση των small cells και μια σημαντική μείωση της επιτρεπόμενης καθυστέρησης μέχρι 1 ms από άκρο σε άκρο για ορισμένα σενάρια.

Οι συχνότητες κάτω από τα 50GHz είναι ήδη πολύ κατακερματισμένες με συνέπεια, η σημερινή τάση στη βιομηχανία είναι να επικεντρωθεί στις υψηλότερες ζώνες συχνοτήτων, 50 έως 90 GHz, όπου υπάρχουν μεγάλες αχρησιμοποίητες συνεχείς ζώνες. Κατά μήκος αυτής της γραμμής, το ίδρυμα European Telecommunications Standards Institute (ETSI) έχει πρόσφατα εγκαθιδρύσει μια ομάδα προδιαγραφών με έμφαση στην μετάδοση mmWave στο V-band (57-66 GHz) και E- band (71-76 GHz και 81-86 GHz), κατάλληλο για πυκνή ανάπτυξη των backhaul και fronthaul δικτύων ((Ζαχαριά, 2016),).

Από την άλλη πλευρά, με μια δωρεάν άδεια ελεύθερου φάσματος και ασυλία από ηλεκτρομαγνητικές παρεμβολές, οι οπτικές ασύρματες επικοινωνίες (OWC - Optical Wireless Communications) έχουν προσελκύσει πρόσφατα μεγάλο ενδιαφέρον. Δεδομένου ότι οι αποστάσεις σύνδεσης στα backhaul/fronthaul δίκτυα θα είναι μικρότερες, αυξάνεται η πιθανότητα του οπτικού πεδίου (LOS - Line-of-Sight) και η κακή ορατότητα θεωρείται ακίνδυνη. Ο όρος OWC περιλαμβάνει επικοινωνίες ελεύθερου χώρου οπτικής (FSO - Free Space Optics), όπου χρησιμοποιούνται laser πομποί για οικοδόμηση οπτικών ασύρματων συνδέσεων υψηλής χωρητικότητας καθώς και η νέα τεχνολογία (VLC - Visible Light Communications) που χρησιμοποιεί συστήματα εξοπλισμένα με χαμηλού κόστους LED υψηλής ισχύος για την εσωτερική επικοινωνία ((Ζαχαριά, 2016)).

Μια πολλά υποσχόμενη τεχνολογία για small cells είναι ένα backhaul που χρησιμοποιεί ηλεκτρικά κατευθυνόμενες κεραίες για μετάδοση point-to-multipoint σε ένα φάσμα mmWave που - όπως προαναφέρθηκε- ορίζεται στη ζώνη συχνοτήτων 30 - 300 GHz. Ωστόσο, στη συνέχεια, επικεντρωνόμαστε στις ζώνες συχνοτήτων μεταξύ 50 - 90 GHz που είναι ευθυγραμμισμένες με το ίδρυμα ETSI. Η Εικόνα 4.2. παρουσιάζει το backhaul πλέγμα για small cells στο φάσμα mmWave ((Ζαχαριά, 2016)).



Εικόνα 4.2. Backhaul πλέγμα για small cells στο φάσμα mmWave

Το επιτεύξιμο peak του ρυθμού δεδομένων κορυφή ενός συνδέσμου mmWave εξαρτάται σε μεγάλο βαθμό από την επιλεγμένη συχνότητα. Για παράδειγμα, στη ζώνη E-ζώνη πολλά εμπορικά προϊόντα είναι ικανά να πετύχουν ρυθμούς μεταφοράς δεδομένων της τάξης 1-1.25 Gbit / s. Στη V- ζώνη, τα ποσοστά αυτά κυμαίνονται από 450 Mbit/s σε 1 Gbit/s, ενώ στο project 5G-Crosshaul φτάνει έως 4 Gbit/s ανά κόμβο ((Ζαχαριά, 2016)).

Η πυκνότητα του δικτύου εξαρτάται από την απόσταση μεταξύ των κυψελών (ονομάζεται αλλιώς και ακτίνα κυψελών) και την τοπολογία. Σε γενικές γραμμές, σε μια ανάπτυξη πλέγματος με μια τυπική απόσταση μεταξύ των κυψελών περίπου 150 μέτρα, η χωρητικότητα της περιοχής κυκλοφορίας μπορεί να είναι της τάξης των μερικών δεκάδων Gbit/s/km2, η οποία δίνει μια πυκνότητα χρηστών της τάξης των μερικών χιλιάδων ανά km2 ((Ζαχαριά, 2016)).

Η απόσταση μεταξύ των συνδέσμων του mmWave εξαρτάται επίσης από τη ζώνη συχνοτήτων. Στη ζώνη E-band οι αποστάσεις κυμαίνονται από εκατοντάδες μέτρων έως και πολλά χιλιόμετρα. Στη ζώνη V-band οι αποστάσεις αυτές είναι πολύ μικρότερες και κυμαίνονται από 50 m έως 1000 m. Οι αποστάσεις των συνδέσμων που κυμαίνονται από 50 m έως 600 m εξαρτώνται από την τεχνολογία της κεραίας.

Οι οπτικές ασύρματες συνδέσεις επιτρέπουν τη σύνδεση σε διαφορετικές αποστάσεις που κυμαίνονται από τη ζώνη ultra - short (που χρησιμοποιείται για διασυνδέσεις

εντός του ολοκληρωμένου) έως τη ζώνη ultra - long (που χρησιμοποιείται για επικοινωνία μεταξύ δορυφόρων). Σε γενικές γραμμές, όσο μεγαλύτερη είναι η απόσταση μεταξύ των συνδέσμων, τόσο λιγότερο απαραίτητη είναι μια αποκλίνουσα δέσμη φωτός προκειμένου να διατηρηθεί η ισχύς έναντι στην ατμοσφαιρική εξασθένιση και να επιτευχθεί επαρκής πυκνότητα ισχύος στην πλευρά του δέκτη. Με τον έλεγχο της οπτικής δέσμης, οι οπτικές ασύρματες συνδέσεις που βασίζονται σε LED είναι εφικτές έως και αρκετές εκατοντάδες μέτρα, ενώ για μεγαλύτερες αποστάσεις (πάνω από 200 μέτρα) απαιτούνται συνδέσεις με lazer ((Ζαχαριά, 2016)).

4.1.2 Δίκτυα 5ης γενιάς ενσύρματης πρόσβασης

Στο πλαίσιο του 5G-Crosshaul, η επικάλυψη των συνδέσμων backhaul και fronthaul πάνω από Παθητικά Οπτικά Δίκτυα (PONs - Passive Optical Networks) ενός – προς - πολλά σημεία (point-to-multipoint) και μπορεί να προσφέρει ένα οικονομικά αποδοτικό τρόπο για την πραγματοποίηση μια σταθερής - κινητής υποδομής οπτικού δικτύου πρόσβασης. Επί του παρόντος, υπάρχουν αρκετές υποψήφιες τεχνολογίες, όπως GPON, XG-PON, XGS-PON, NG PON2. Ωστόσο, οι τεχνολογίες PON εξελίσσονται και αναμένεται ότι η επόμενη γενιά των παθητικών δικτύων PON πρόκειται να βασίζεται σε πολυπλεξία διαίρεσης μήκους κύματος (WDM - Wavelength Division Multiplexing).

Η τεχνολογία GPON χρησιμοποιείται αυτή τη στιγμή για οικιακή πρόσβαση και προσφέρει μια συνολική χωρητικότητα της τάξης των 2.5/1.25 Gbit/s για συνδέσεις downstream/upstream αντίστοιχα, που μοιράζεται μεταξύ διαφορετικών χρηστών συνήθως 32/64. Αυτά τα στοιχεία παραγωγικής ικανότητας δεν είναι επαρκή για συνδέσεις fronthaul με βάση την κοινή δημόσια ασύρματη διεπαφή (CPRI - Common Public Radio Interface). Πάντως, το GPON θα μπορούσε να θεωρηθεί ως κατάλληλη τεχνολογία για την επόμενη γενιά fronthaul διεπαφών π.χ. του 5G - Crosshaul σε πυκνοκατοικημένες αστικές περιοχές και ιδιαίτερα για συγκεκριμένες περιπτώσεις, στις οποίες απαιτούνται χαμηλές τιμές fronthaul κάτω του 1 Gb/s. Ο κύριος λόγος για αυτό είναι η ικανότητα των διαφόρων μεθόδων εκχώρησης εύρους ζώνης (σταθερή, εξασφαλισμένη και μη εξασφαλισμένη) του επιπέδου MAC των τεχνολογιών PON που βασίζονται στην πολυπλεξία διαίρεσης χρόνου (TDM - Time Division Multiplexing). Ωστόσο, αυτό είναι δύσκολο να επιτευχθεί λόγω της αναμενόμενης καθυστέρησης για αυτούς τους fronthaul συνδέσμους, που μπορεί να υποδηλώνουν επίσης την ανάγκη για χαμηλότερους λόγους διάσπασης στην ανάπτυξη οπτικών

ινών. Αυτό δεν είναι πολύ εφικτό για τις επιχειρήσεις που έχουν ήδη αναπτύξει την τεχνολογία GPON.

Η τεχνολογία XG-PON προσφέρει 2.5 Gbit/s για upstream και 10 Gbit/s για downstream. Σε αυτή την περίπτωση χρήσης η χωρητικότητα των 2.5G για upstream καθιστά το XG-PON μια πιο κατάλληλη τεχνολογία για την επόμενη γενιά fronthaul διασυνδέσεων του 5G-Crosshaul από το GPON. Ωστόσο, η πρόσφατη έγκριση για ένα νέο συμμετρικό πρότυπο 10G PON (XGS-PON) θα περιορίσει τις απαιτήσεις για τα συστήματα XG-PON. Συνοψίζοντας, οι τεχνολογίες GPON και XGPON δεν αποδείχτηκαν να είναι μακροπρόθεσμα κατάλληλες επιλογές για το δίκτυο 5G-Crosshaul, κυρίως λόγω της σχετικά περιορισμένης χωρητικότητάς τους .

Μια περισσότερο κατάλληλη τεχνολογία για την επόμενη γενιά fronthaul διασύνδεσης των 5G- Crosshaul, από την άποψη της χωρητικότητας, είναι το NG-PON2. Η τυπική NG-PON2 διαμόρφωση τεχνολογίας περιλαμβάνει 4-8 ζεύγη καναλιών χρησιμοποιώντας πολυπλεξία τόσο στο χρόνο όσο και στο μήκος κύματος (TWDM – Time and Wavelength Division Multiplexing). Ανά ζεύγος καναλιών οι ρυθμοί bit για TWDM είναι 10 Gbit/s για downstream και 10 Gbit/s για upstream, 10 Gbit/s για downstream και 2.5 Gbit/s για upstream ή 2.5 Gbit/s για downstream και 2.5 Gbit/s για upstream, αντίστοιχα. Για την ολοκλήρωση της αξιολόγησης των τεχνολογιών PON, αξίζει να αναφερθεί μια σειρά σημαντικών λειτουργικών χαρακτηριστικών και χαρακτηριστικών συντήρησης, για τους σκοπούς του 5G-Crosshaul, και συγκεκριμένα:

- Οι μηχανισμοί για την ανίχνευση και διόρθωση σφαλμάτων, συμπεριλαμβανομένης της κρυπτογράφησης και της υβριδικής αποκωδικοποίησης διόρθωσης σφάλματος, καθώς και τους προς τα εμπρός μηχανισμούς διόρθωσης σφάλματος (FEC - Forward Error Correction) που υλοποιούνται με ισχυρούς κώδικες Reed-Solomon.
- Η ασφάλεια Δικτύων, συμπεριλαμβανομένων των μηχανισμών για τον έλεγχο ταυτότητας, τη διαχείριση κλειδιών και την κρυπτογράφηση δεδομένων.
- Η παρακολούθηση των επιδόσεων και συνεχή επίβλεψη των παραμέτρων του φυσικού επιπέδου και του επιπέδου διασύνδεσης για τη διευκόλυνση της αντιμετώπισης προβλημάτων και τη συντήρηση των δικτύων PON.

Η τεχνολογία WDM-PON θα αποτελέσει μία κάπως καλύτερη επιλογή, λαμβάνοντας ως κριτήριο την καθυστέρηση, σε σύγκριση με την τεχνολογία TDM και TWDM για του σκοπούς του fronthaul στο 5G – Crosshaul. Ωστόσο, η τρέχουσα εμπορική τεχνολογία WDM-PON προσφέρει μόνο συμμετρικές συνδέσεις της τάξης του 1 Gbit/s στις περισσότερες περιπτώσεις, λόγω των περιορισμών των συνιστωσών. Είναι όμως δυνατόν να επιτευχθούν υψηλότεροι ρυθμοί bit, χρησιμοποιώντας ένα ρυθμιζόμενο laser κατανεμημένης ανάδρασης (DFB - distributed feedback) αντί για ανακλαστικά οπτικά εξαρτήματα. Υπό αυτό το πρίσμα, το ρυθμιζόμενο WDM-PON έχει προσελκύσει πρόσφατα την προσοχή των πωλητών και των επενδυτών για την ανάπτυξη της ρυθμιζόμενης υψηλής χωρητικότητας WDM-PON συστημάτων επόμενης γενιάς, τα οποία είναι πολύ κατάλληλα για το 5G-Crosshaul ((Ζαχαριά, 2016)).

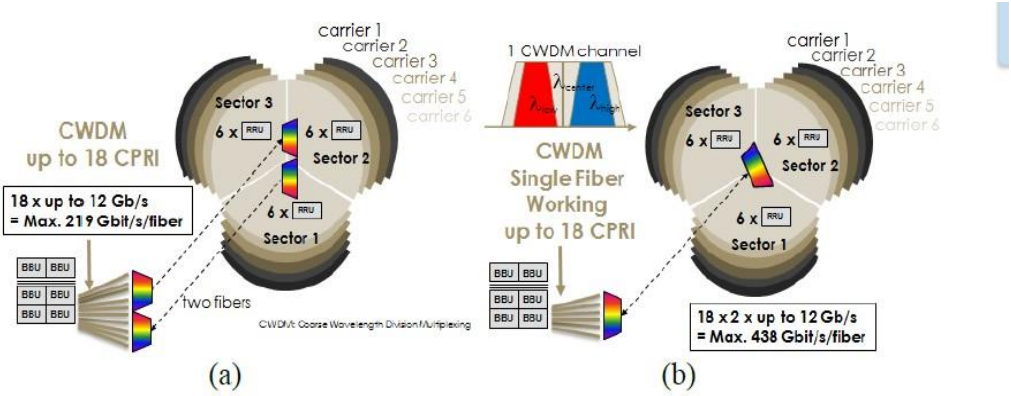
	GPON	XG-PON	NG-PON2 (TWDM) SHARED SPECTRUM	XGS-PON	WDM-PON (SEEDED VARIANT)
ITU-T Recommendation	G.984	G.987	G.989	G.9807	G.698.3
Availability	In market	In market	In market	ITU-T approved	In market
Aggregate Rate	2.5G/1.25G	10G/2.5G coming 10/10	40G/10G 40G/40G	10G/10G	32G/32G
Access Peak Rate	2.5G/1.25G	10G/2.5G	10G/2.5G	10G/10G	1G/1G
MAC	TDM	TDM	TWDM and PtP WDM	TDM	WDM
Multipoint device	Splitter	Splitter	Splitter (but use of Wavelength filters allowed)	Splitter	Wavelength filter (AWG)
ODN Type	WS	WS	WS/WR	WS	WR
Split ratio	1:32/1:64	1:64(128)	1:64(254)	1:128	1:32
Physical reach	20 Km	40 Km	20 Km (for 1:64)	20 Km	20 Km
Price	Low	Medium	High	Medium	Very High
Max. budget	28 dB	35 dB	38.5 dB	35 dB	15 dB
Trasmission Capacity for Degital RoF transport	Little	Medium	High	Medium	High

Πίνακας 4.1. Βασικά χαρακτηριστικά των τεχνολογιών PON

4.1.3 Δίκτυα οπτικών ινών 5ης γενιάς

Εγκαταλείποντας τα παραδοσιακά δίκτυα και οδεύοντας προς την πράσινη ανάπτυξη, τα οπτικά δίκτυα γίνονται ολοένα και πιο ελκυστικά, λόγω της συνολικής τους χωρητικότητας, της υψηλής απόστασης μεταξύ των συνδέσμων και της χαμηλής καθυστέρησης. Παθητικές λύσεις που βασίζονται στην τεχνολογία CWDM (Coarse Wavelength Division Multiplexing) είναι ιδιαίτερα κατάλληλες για την οικονομικά αποδοτική εγκατάσταση σε εξωτερικούς χώρους με μέτρια συνολική χωρητικότητα. Η τεχνολογία DWDM (Dense Wavelength Division Multiplexing) παρέχει αντ' αυτού μια μελλοντική πλατφόρμα για την επέκταση της χωρητικότητας προς το συγκεντρωτισμό. Οι δύο τεχνολογίες παρατίθενται στη συνέχεια .

Η παθητική WDM αποτελείται από μια προσέγγιση πολυπλεξίας και αποπολυπλεξίας του μήκους κύματος και μπορεί να είναι τόσο CWDM όσο και DWDM, αναφορικά με τον αριθμό των μηκών κύματος που χρησιμοποιούνται και την απόσταση μεταξύ τους. Η τεχνολογία CWDM αποτελεί μια καλή επιλογή για εγκαταστάσεις με χαμηλή ή μέτρια συνολική χωρητικότητα καθώς είναι απλή στην εγκατάσταση και ιδιαίτερα αξιόπιστη. Από τη στιγμή που οι πομποδέκτες της τεχνολογίας αυτής σε συνεργασία με την CPRI επιλογή (option) 9 (12.16512 Gbit/s) είναι όλο και πιο κοινή στις μέρες μας, η συνολική χωρητικότητα της σύνδεσης μπορεί να ανέλθει περίπου στα 219 Gbit/s ανά ίνα με 18 CWDM κανάλια. Θα πρέπει να γίνει αντιληπτό ότι οι κανονικές συσκευές CWDM χρειάζονται δύο ίνες, μία για upstream και μια για downstream, όπως φαίνεται στην Εικόνα 4.3. Η μετάδοση σε μια ενιαία ίνα χρησιμοποιώντας αμφίδρομους πομποδέκτες είναι επίσης δυνατή και βοηθά την απλοποίηση της λειτουργίας, αποφεύγοντας λανθασμένους τρόπους σύνδεσης. Οι πρόσφατες λύσεις οπτικών ινών βασίζονται σε μήκος κύματος που προκύπτει από υπο-πολυπλεξία πάνω από το πλέγμα CWDM, η οποία συνίσταται στη διαίρεση του πλάτους της υποδοχής του CWDM (+/- 6.5nm) σε δύο υπο-κανάλια, ένα για κάθε κατεύθυνση. Έτσι, ο συνολικός ρυθμός μετάδοσης bit ανά ίνα μπορεί να διπλασιαστεί και να φτάσει έως και 438 Gbit/s (Εικόνα 4.3.).



Εικόνα 4.3. Τεχνολογία 5G - Crosshaul κεντρικού δικτύου με (a) CWDM δύο οπτικών ινών και (b) CWDM μιας οπτικής ίνας

Η CWDM είναι η φθηνότερη τεχνολογία WDM και για τις δύο παθητικές συσκευές του πολυπλέκτη/αποπολυπλέκτη και των πομποδεκτών. Η δυνατότητα *πληρωμής με την ανάπτυξη* ("pay as you grow") αποτελεί ένα άλλο πλεονέκτημα για τον πομποδέκτη, κάτι που σημαίνει ότι μόνο ο αριθμός των παθητικών θυρών του πολυπλέκτη/αποπολυπλέκτη πρέπει να προγραμματιστεί εκ των προτέρων. Ένα βασικό πλεονέκτημα της CWDM είναι ότι αποτελεί μία από τις λίγες λύσεις συμβατές με συνθήκες εξωτερικού χώρου λειτουργίας (-40 / + 70 ° C) για ρυθμούς μετάδοσης έως 10 Gbit/s.

Μία άλλη ενδιαφέρουσα πτυχή αποτελεί το γεγονός ότι οι παθητικές συσκευές CWDM μπορούν να είναι plug & play, τόσο στον τρέχοντα όσο και στο μελλοντικό RAN εξοπλισμό και επίσης να είναι συμβατές με Ethernet διασυνδέσεις. Ωστόσο, η καθαρά παθητική οπτική μεταφορά δεν παρέχει διαχείριση οπτικών ινών και καναλιών και στερείται βασικών λειτουργιών Διαχείρισης και Συντήρησης (OAM - Operations Administration and Maintenance), όπως είναι η παρακολούθηση και η απομακρυσμένη διαμόρφωση και διαχείριση σφαλμάτων. Αυτός είναι ο λόγος για τον οποίο σχεδόν όλες οι παθητικές λύσεις έχουν προταθεί με οπτικούς αναμεταδότες, που θα είναι σε θέση να διαχειριστούν και να αναφέρουν την κατάσταση του μήκους κύματος του κάθε ζεύγους καναλιού και της υποδομής οπτικών ινών.

Αναφορικά με την τεχνολογία DWDM, ο αριθμός των οπτικών καναλιών για εμπορικά συστήματα DWDM λειτουργεί πάνω από το CBand (1530-1565 nm) είναι 48, με 100 GHz απόσταση. Αυτό οδηγεί σε τεράστια συνολική χωρητικότητα πάνω

από μία μόνο οπτική ίνα, που μπορεί να φτάσει σε 960 Gbit/s με κανάλια 100 Gbit/s σε απόσταση 50 GHz. Περαιτέρω αύξηση θα είναι δυνατή με την εισαγωγή καναλιών 1 Tbit/s. Στην ακραία περίπτωση μετάδοσης της τάξης των Tbit/s τόσο μέσω της ζώνης συχνοτήτων C όσο και της L, η συνολική χωρητικότητα μπορεί να φτάσει σε 67.2 Tbit/s σε μια ενιαία οπτική ίνα. Η υψηλή συνολική χωρητικότητα καθιστά την DWDM ιδιαίτερα κατάλληλη για την υποστήριξη ευρυζωνικών υπηρεσιών και πυκνοκατοικημένων περιοχών που πρέπει να υποστηρίξει το 5G.

Αποτελεί κοινή αντίληψη και ταυτόχρονα πεποίθηση το γεγονός ότι το κόστος αποτελεί το κύριο μειονέκτημα της τεχνολογίας DWDM. Οι προσπάθειες για να μειωθεί το κόστος των πομποδεκτών είναι σε εξέλιξη, με την εισαγωγή νέων τεχνολογιών όπως οι ποδοτικές μορφές διαμόρφωσης, τα ρυθμιζόμενα laser χαμηλού κόστους και οι νέες λύσεις για επαναδιαμορφώσιμους add-drop πολυπλέκτες (ROADMs - Reconfigurable Add-Drop Multiplexers) που υπόσχονται να μειώσουν το κόστος κατά δύο τάξεις μεγέθους. Το υψηλότερο κόστος της τεχνολογίας DWDM οπτικών συσκευών αντισταθμίζεται ούτως ή άλλως από την ευκαιρία που προσφέρει για την αποθήκευση του κόστους του εξοπλισμού συνολικά. Όσον αφορά τις λειτουργικές πτυχές, η ικανότητα να υποστηρίζει πολλαπλές φυσικές τοπολογίες όπως linear, ring, point-to-multipoint κ.λ.π. χρησιμοποιώντας την ίδια τεχνολογία και κρατώντας μια λογική συνδεσιμότητα σημείο-προς-σημείο, αποτελεί είναι ένα από τα μεγαλύτερα πλεονεκτήματα της τεχνολογίας DWDM. Μια τέτοια ευελιξία αυξάνεται με τη διαθεσιμότητα των αναδιαρθρώσιμων συσκευών όπως το ρυθμιζόμενο laser και οι επαναδιαμορφώσιμοι add-drop πολυπλέκτες, που προσφέρουν επίσης την ευκαιρία να μειώσουν το κόστος του εξοπλισμού (H2020 5G-Crosshaul project Grant No. 671598).

4.2 Softwarization στα 5G

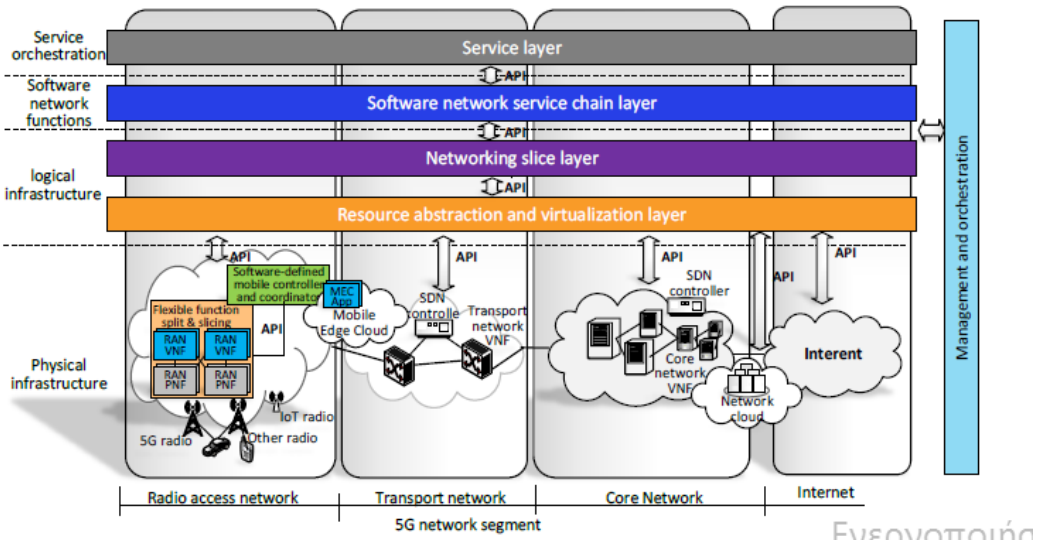
Οι τεχνολογίες δικτύων λογισμικού οι οποίες εισάγονται ως θεμελιώδεις παράγοντες, οι οποίοι επιτρέπουν την υλοποίηση των απαιτήσεων σε επίπεδο προγραμματισμού, ευελιξίας (επαναπροσδιορισμός, επαναχρησιμοποίηση και διαμοιρασμός υποδομών), προσαρμοστικότητας (αυτό-προστασία, αυτό-βελτιστοποίηση) και δυνατοτήτων (υπολογιστικά πλεονεκτήματα για κινητά, κατακερματισμός δικτύου, αυτόνομη διαχείριση δικτύου), αναμένεται να είναι εγγενείς στα δίκτυα 5G (EuCNC, 2016).

Το softwarization των δικτύων περιλαμβάνει την υλοποίηση των λειτουργιών δικτύου στο λογισμικό, την εικονοποίηση αυτών των λειτουργιών και την δυνατότητα προγραμματισμού, μέσω της εγκατάστασης των κατάλληλων διεπαφών. Στην αρχιτεκτονική συστήματος 5G, αναμένεται ένα νέο πλαίσιο προγραμματισμού και softwarization, με σκοπό τη διαχείριση των δικτύων 5G. Αυτή η απαίτηση softwarization, επίσης αναγνωρίζεται από την ομάδα μελέτης ITU-T Study Groyp 13, η οποία σχετικά πρόσφατα παρουσίασε το IMT-2020 Focus Group σε επίπεδο δικτύου, προκειμένου να αναλυθεί ο τρόπος αλληλεπίδρασης των αναδυόμενων τεχνολογιών 5G με τα μελλοντικά δίκτυα (ITU-T, 2013)[13].

Το softwarization δικτύων αποτελεί μία προσέγγιση αναφορικά με τη χρήση του προγραμματισμού λογισμικού για το σχεδιασμό, την υλοποίηση, την ανάπτυξη, τη διαχείριση και τη συντήρηση του εξοπλισμού / συστατικών στοιχείων / υπηρεσιών δικτύου. Επωφελείται από την δυνατότητα προγραμματισμού, την ευελιξία και την επαναχρησιμοποίηση του λογισμικού για γρήγορο επανασχεδιασμό των αρχιτεκτονικών δικτύων και υπηρεσιών. Ο στόχος του softwarization δικτύου είναι η βελτιστοποίηση των διαδικασιών στα δίκτυα, η μείωση του κόστους τους και η προσθήκη προστιθέμενης αξίας στις δικτυακές υποδομές (ITU-T, 2013).

Αξιοποιώντας τις τεχνολογίες εικονικοποίησης, το softwarization αποτελεί ένα από τα βασικά στοιχεία τα οποία επιτρέπουν την ενοποίηση της πλατφόρμας υπηρεσιών 5G end-to-end και την υλοποίηση του τεμαχισμού του δικτύου με τη μορφή υπηρεσίας. Επιπλέον, το softwarization εξελίσσει τα δίκτυα σε επίπεδο διαχείρισης και ενορχήστρωση σύνθετων συστημάτων λογισμικού, τα οποία περιλαμβάνουν και εναρμονίζουν ότι μέχρι πρότινος θεωρούνταν ως αδιάρρηκτα πεδία, λειτουργίες προσανατολισμένες σε δίκτυο και πόρους και λειτουργίες προσανατολισμένες στην εφαρμογή. Αυτό επιτρέπει στους προγραμματιστές και τους φορείς εκμετάλλευσης να ταιριάζουν καλύτερα στις ανάγκες και τις δυνατότητες, να δημιουργούν δίκτυα που να μπορούν να γνωρίζουν τις εφαρμογές, καθώς και εφαρμογές να γνωρίζουν το δίκτυο. Αυτή η κοινή εκφραστική ισχύς θα αποτελέσει έναν από τους κύριους κινητήριους μοχλούς των καινοτομιών που επιτρέπονται από το 5G (Εικόνα 4.4.) (EuCNC, 2016).

[13] Study Group 13, ITU-T, http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/default.aspx



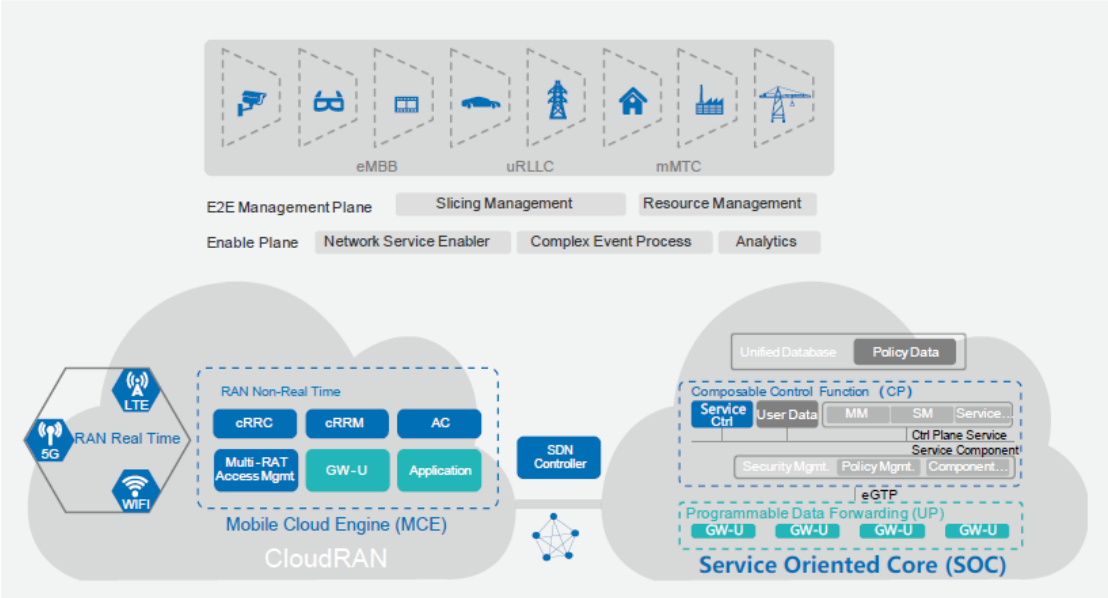
Εικόνα 4.4. Τεχνολογίες δικτύων λογισμικού σε συνολική αρχιτεκτονική 5G

4.3. Cloud RAN

Η καθοδηγούμενη υπηρεσία αρχιτεκτονικής δικτύου 5G, στοχεύει στην ευέλικτη και συνάμα στην αποτελεσματική κάλυψη των απαιτήσεων των διαφοροποιημένων κινητών υπηρεσιών. Με το Λογισμικό Καθορισμένης Δικτύωσης (SDN) και το Δίκτυο Λειτουργιών Εικονοποίησης (NFV) τα οποία υποστηρίζουν τη βασική φυσική υποδομή, η 5G συγκεντρώνει συνολικά δίκτυα πρόσβασης, μεταφοράς και πυρήνα (core networks). Η υιοθέτηση της τεχνολογίας cloud (σύννεφων), παρέχει καλύτερη υποστήριξη στις ποικίλες 5G υπηρεσίες και παράλληλα επιτρέπει την τμηματοποίηση των βασικών τεχνολογιών E2E (End-to-End), την ανάπτυξη κεντρικών υπηρεσιών κατ' απαίτηση και στις λειτουργίες δικτύου βάσει στοιχείων.

Το CloudRAN αποτελείται από ιστοτόπους και cloud μηχανές, όπως διαφαίνεται στην εικόνα Εικόνα 4.5. Αυτή η λειτουργία οργανώνει πολλαπλές υπηρεσίες, και λειτουργεί σε διαφορετικά πρότυπα, αλλά και σε διαφορετικούς ιστοτόπους για πραγματικού χρόνου πόρους RAN, οι οποίοι απαιτούν έναν αριθμό υπολογιστικών πόρων. Η πολλαπλή συνδεσιμότητα εισάγεται για να επιτρέψει την ανάπτυξη δικτύου κατ' απαίτηση για μη πραγματικού χρόνου πόρους RAN. Επιπλέον, τα δίκτυα εφαρμόζουν πολιτική ελέγχου με τη χρήση δυναμικής τακτικής, ημι-στατικού χρήστη και στατικά δεδομένα δικτύου τα οποία είναι αποθηκευμένα στην ενοποιημένη βάση δεδομένων στην πλευρά του κεντρικού δικτύου (core network). Ο έλεγχος επιπέδων με βάσει τα στοιχεία και τα προγραμματιζόμενα επίπεδα χρήστη, επιτρέπουν την

ενορχήστρωση της λειτουργίας δικτύου, ώστε να εγγυώνται ότι τα δίκτυα είναι σε θέση να επιλέξουν αντίστοιχες λειτουργίες επιπέδου ελέγχου ή επιπέδου χρήστη, σύμφωνα με τις απαιτήσεις των διαφορετικών υπηρεσιών.



Εικόνα 4.5. Cloud RAN

Αντίστοιχα, το δίκτυο μεταφοράς αποτελείται από ελεγκτές SDN και βασικούς κόμβους προώθησης. Οι ελεγκτές SDN παράγουν μία σειρά συγκεκριμένων διαδρομών προώθησης δεδομένων, οι οποίες βασίζονται στην τοπολογία δικτύου και στις απαιτήσεις της υπηρεσίας. Το επίπεδο ενεργοποίησης περιγράφει και συνάμα αναλύει τις δυνατότητες δικτύου, για την υλοποίηση της βελτιστοποίησης δικτύου ή τις δυνατότητες ανοικτού δικτύου με τη μορφή API. Το ανώτερο στρώμα – επίπεδο της αρχιτεκτονικής δικτύου, υλοποιεί αυτόματη τμηματοποίηση E2E και διαχείριση πόρων δικτύου.

4.3.1. Αρχιτεκτονική δικτύου

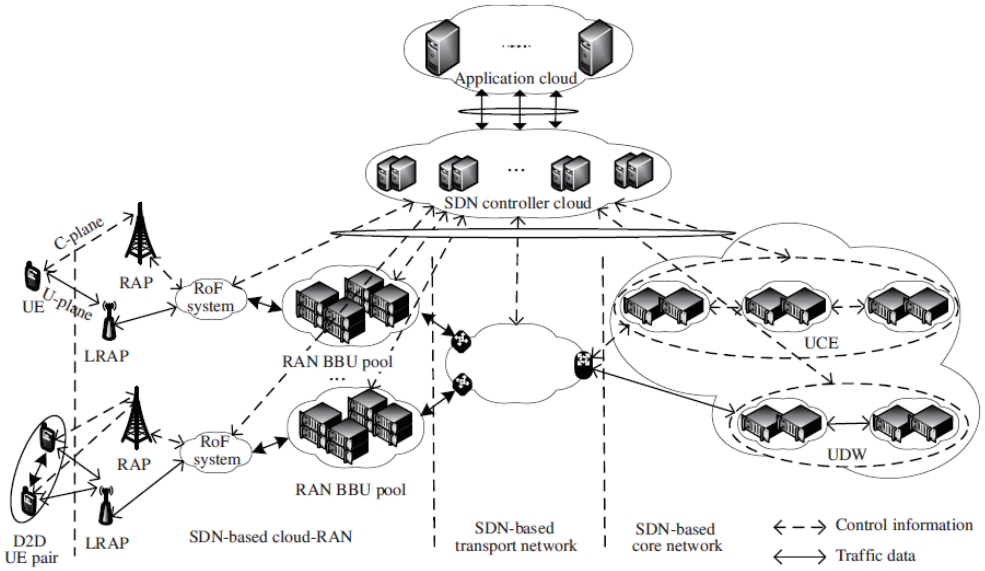
Η αρχιτεκτονική δικτύου με βάσει το cloud RAN (νέφος) (C-RAN) και το SDN, έχει προσελκύσει το ενδιαφέρον τόσο της ακαδημαϊκής κοινότητας όσο και του τομέα της βιομηχανίας. Πλήθος ερευνητών (Chang et al., 2013 ·Sabella et al., 2013 · Wang & Zhang, 2014 · Costa – Reguena, 2014), παρουσίασαν μία καινοτόμο αρχιτεκτονική δικτύου (Εικόνα 4.6.), η οποία αποτελείται από εφαρμογές cloud (νέφους), SDN ελεγκτές νέφους, C-RAN βάσει του Λογισμικό Καθορισμένης Δικτύωσης (SDN) και

του SDN core network. Όπως διαφαίνεται, η εφαρμογή cloud παρέχει πλήθος υπηρεσιών, όπως η διαχείριση δικτύου και η παρακολούθηση επιδόσεων.

Πιο συγκεκριμένα, ο SDN ελεγκτής νέφους (cloud) μετατρέπει τακτικές από την εφαρμογή cloud και παρέχει υπηρεσίες κεντρικού ελέγχου για τα αντικειμενικά στοιχεία του δικτύου μέσω αυτών των τακτικών – πολιτικών, όπως είναι το C-RAN, το δίκτυο μεταφορών (transport network) και το βασικό δίκτυο (core network). Το C-RAN βάσει του SDN, απαρτίζεται από μεγάλης κλίμακας μονάδα δεξαμενών βασικής ζώνης (BBU – Baseband Unit), ασύρματα συστήματα μέσω ινών (radio-over-fiber – RoF), σημεία διαμοιρασμού ραδιοπρόσβασης (RAP) και ελαφρά σημεία ραδιοπρόσβασης (LRAPs). Οι δεξαμενές BBU παρέχουν κεντρική επεξεργασία σημάτων ζώνης βάσης, αρκετά μακριά από ένα σταθμό βάσης. Επίσης, τα RAP επιτυγχάνουν κάλυψη σηματοδότησης όπως η μικροκυψέλη, ενώ τα LRAP επιτυγχάνουν τη μετάδοση δεδομένων όπως οι μικροκυψέλη (Wang & Zhang, 2014).

Στη συνέχεια, τα RAP και LRAP συνδέουν το BBU μέσω του συστήματος RoF. Το σύστημα RoF επιτυγχάνει έξυπνες συνδέσεις μεταξύ των RAPs/ LRAPs και BBU, ενώ ο SDN ελεγκτής παρέχει δυναμική προσαρμογή εύρους ζώνης για κάθε μία σύνδεση RAPs/ LRAPs με σύνδεση BBU και διαχείριση δεξαμενών, συμπεριλαμβανομένου του δικτύου RAT. Παράλληλα, το δίκτυο μεταφοράς βάσει SDN επιτυγχάνει ευέλικτη επιλογή και διαχείριση των δικτύων backhaul, δυναμική προσαρμογή του εύρους ζώνης μεταφοράς για κάθε σύνδεση RAN στο βασικό δίκτυο (core network) και την επιλογή διαδρομής (Zheng et al., 2015).

Από την άλλη πλευρά, το βασικό δίκτυο (core netowork) βάσει του SDN αποτελείται από ενιαία μονάδα ελέγχου (UCE) και από ενοποιημένη πύλη δεδομένων (UDW). Η ενιαία μονάδα ελέγχου (UCE) επιτυγχάνει μία ενοποιημένη λειτουργία ελέγχου, η οποία ενσωματώνει τη διαχείριση της κινητής μονάδας (MME), το επίπεδο ελέγχου της υπηρεσίας εισόδου (SGW-C) και το επίπεδο ελέγχου του πακέτου δεδομένων της πύλης εισόδου του δικτύου (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) επιτυγχάνει τη λειτουργική προώθηση δεδομένων, η οποία ενσωματώνει το επίπεδο υπηρεσιών δεδομένων εισόδου SGW-D και το επίπεδο δεδομένων (Zheng et al., 2015).



Εικόνα 4.6. Αρχιτεκτονική δικτύου

Η τεχνική νέφους (cloud technique) παρουσιάζει πλήθος πλεονεκτημάτων όπως: 1) η ευρεία κεντρική ανάπτυξη η οποία παρέχει χωρητικότητα επεξεργασίας, πέρα από την απλή ανάπτυξη, 2) η εικονοποίηση η οποία επιτρέπει το λογικό διαχωρισμό του υλικού και του λογισμικού, γεγονός το οποίο μειώνει την πολυπλοκότητα της επεξεργασίας και επεκτείνει τη χωρητικότητα του υλικού, 3) ενώ προσφέρει νέες λύσεις υπηρεσιών για πυκνή ανάπτυξη δικτύου, όπως το δίκτυο ασύρματης πρόσβασης ως υπηρεσία (RANaaS) (Zheng et al., 2015).

Σε επίπεδο αρχιτεκτονικής, ο διακομιστής εφαρμογών (application server), ο ελεγκτής SDN, το RAN και το core δίκτυο υιοθετούν την ανάπτυξη νέφους (cloud deployment). Πιο συγκεκριμένα, το SDN διαχωρίζει τον έλεγχο δικτύου από τις μεμονωμένες συσκευές δικτύου και τον μετακινεί σε προσβάσιμες υπολογιστικές συσκευές, γεγονός το οποίο επιτρέπει στην βασική υποδομή να διαχωρίζεται για τις εφαρμογές και τις δικτυακές υπηρεσίες – το δίκτυο αντιμετωπίζεται ως λογική ή εικονική οντότητα. Ωστόσο, το SDN μπορεί να ανταποκριθεί άμεσα στις μεταβαλλόμενες συσκευές δικτύου, στις ανάγκες των επιχειρήσεων και στις απαιτήσεις των χρηστών. Σε επίπεδο αρχιτεκτονικής το SDN αποτελείται από το επίπεδο εφαρμογής, από το επίπεδο ελέγχου και το επίπεδο υποδομής και η διεπαφή μεταξύ του επιπέδου εφαρμογής και του επιπέδου ελέγχου αναφέρεται σε ανοικτές διεπαφές προγραμματισμού εφαρμογών (API), ενώ υπάρχει ένα επίπεδο διεπαφής

ελέγχου/δεδομένων μεταξύ του επιπέδου ελέγχου και του επιπέδου υποδομής (Zheng et al., 2015).

Στην αρχιτεκτονική, τα επίπεδα ελέγχου και δεδομένων του RAN και του κεντρικού δικτύου διαχωρίζονται. Για το RAN, τα RAPs επιτυγχάνουν κάλυψη σηματοδότησης προκειμένου να διατηρήσουν τη σύνδεση του χρήση όπως οι μικροκυψέλες, ενώ τα LRAPs επιτυγχάνουν τη μετάδοση δεδομένων όπως οι μικροκυψέλες. Τα RAPs εφοδιασμένα με ογκώδη MIMO μπορούν να παρέχουν μετάδοση δεδομένων. Δεδομένου ότι τα LRAPs είναι περισσότερο κοντά στους χρήστες, βελτιώνουν την κατάσταση του καναλιού προκειμένου να επιτύχουν καλύτερη απόδοση. Όσον αφορά το βασικό δίκτυο (core network), η λειτουργία διαχείρισης του ανοίγματος GTP-U διαχωρίζεται από τα SGW και PWG. Ωστόσο, δεδομένων των ιδιαίτερων χαρακτηριστικών των κυψελοειδών δικτύων, προκύπτουν ορισμένα τεχνικά προβλήματα κατά τη διαδικασία της εφαρμογής των τεχνικών σύννεφου (cloud) και οι τεχνικές SDN θα πρέπει να μελετηθούν περεταίρω (Zheng et al., 2015).

4.4. Δίκτυο Διαμόρφωσης

Οι τεχνολογίες δικτύων λογισμικού, εισάγονται ως θεμελιώδεις παράγοντες προκειμένου να κατανοηθούν οι απαιτήσεις σε επίπεδο προγραμματισμού, ευελιξίας (επαναδιαμόρφωση, επαναχρησιμοποίηση, διαμοιρασμός υποδομών), ικανότητας προσαρμογής (αυτοδιαμόρφωση, αυτοπροστασία, αυτοβελτιστοποίηση, αυτοθεραπεία) και ικανοτήτων (διαχείριση αυτόνομου δικτύου, mobile edge computing[14], network slicing), οι οποίες αναμένεται να συνυπάρχουν στα δίκτυα 5G.

Μεταξύ των πλεονεκτημάτων του softwarization τα οποία αναγνωρίζονται στα 5G, περιλαμβάνεται η μείωση της λειτουργικής δαπάνης (OPEX) και των κεφαλαιουχικών δαπανών (CAPEX), η ταχεία δημιουργία και ανάπτυξη υπηρεσιών, η αποτελεσματική διαχείριση του κύκλου ζωής, η μείωση τα κατανάλωσης ενέργειας και η βελτίωση της ποιότητας εμπειρίας του χρήστη. Παράλληλα, το softwarization αναγνωρίζεται ως ένα από τα βασικά χαρακτηριστικά των δικτύων 5G, δεδομένου ότι αποτελεί πρότυπο καθώς ηγείται της αλλαγής του σχεδιασμού και της υλοποίησης του δικτύου κινητής τηλεφωνίας.

[14] αρχιτεκτονική έννοια δικτύου η οποία επιτρέπει τις δυνατότητες υπολογιστικού νέφους και ένα περιβάλλον πληροφορικής

Επί του παρόντος, πλήθος μελετών καταδεικνύουν ως μία σημαντική πρόκληση την οικοδόμηση των ασύρματων δικτύων επόμενης γενιάς, τα οποία μπορούν να επαναπροσδιορίσουν μία αρχιτεκτονική δικτύου, προκειμένου να αυξηθεί η ευελιξία του δικτύου (Demestichas et al., 2013; Rost et al., 2014; Chin et al., 2014).Μεταξύ αυτών, ο πυρήνας καθώς και η πιο βασική έννοια και τεχνική, είναι αναμφισβήτητα το **Λογισμικό Καθορισμένης Δικτύωσης (SDN) και οι Λειτουργίες Δικτύου Εικονοποίησης (NFV)** (Jain and Paul, 2013). Πλήθος επαγγελματιών στον τομέα της πληροφορικής, καταδεικνύουν την αποκλειστικότητα των δύο παραπάνω τεχνολογιών. Στην πραγματικότητα και οι δύο παρουσιάζουν συμπληρωματικά πλεονεκτήματα, ως μια προσπάθεια να προωθηθεί η ανάπτυξη διαμορφωμένων δικτύων (Chen et al., 2015).

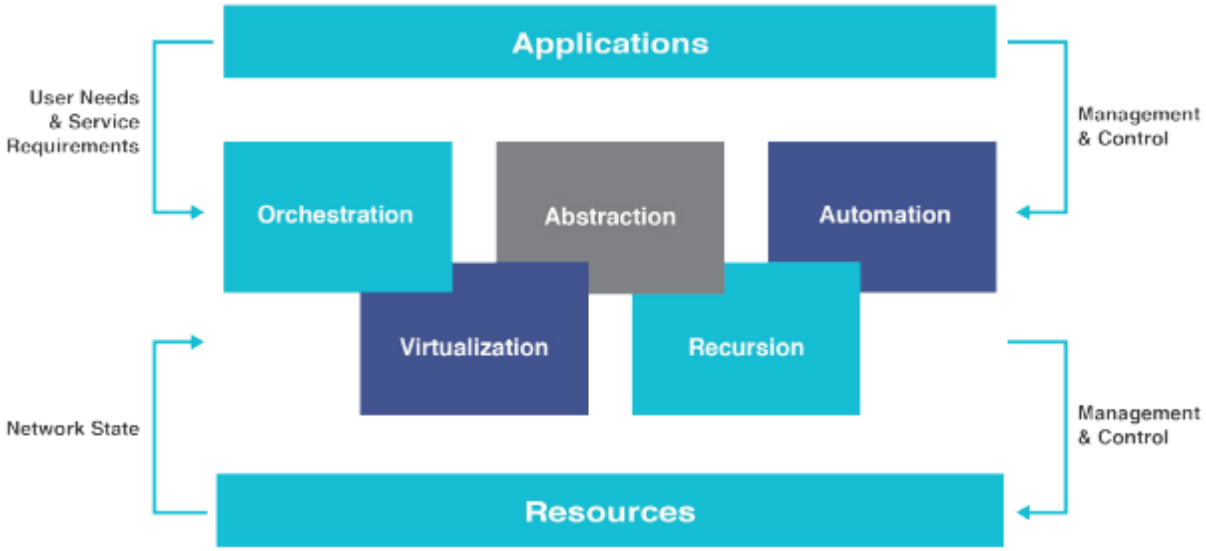
4.4.1. SDN

Το SDN αποτελεί προϊόν του δικτυακού έργου με την ονομασία OpenFlow του Πανεπιστημίου του Stanford, όταν κατά την πραγματοποίηση επιστημονικών ερευνών διαπιστώθηκε ότι κατά την ανάπτυξη κάθε νέας συμφωνίας, είναι αναγκαία η αλλαγή του λογισμικού της δικτυακής συσκευής. Εντός αυτού του πλαισίου, εξετάστηκε το ενδεχόμενο της δημιουργίας ενός δικτύου με προγραμματιζόμενες συσκευές υλικού και κεντρικό έλεγχο και διαχείριση (McKeown et al., 2008). Το νέο αυτό εγχείρημα ανέδειξε το **Λογισμικό Καθορισμένης Δικτύωσης (SDN),** βασικά χαρακτηριστικά του οποίου είναι: ο διαχωρισμός των λειτουργιών ελέγχου και αποστολής, ο κεντρικός έλεγχος και η χρήση ενός ευρέος αποδεκτού ορισμού της διεπαφής λογισμικού (Chen et al., 2015).

Στο **Λογισμικό Καθορισμένης Δικτύωσης (SDN),** ο έλεγχος και η διαχείριση δικτύου λαμβάνει κατά κάποιο τρόπο κεντρική θέση και λαμβάνει τη μορφή λογισμικού (Chen et al., 2015).

Σύμφωνα με την Ανοικτή Υποδομή Δικτύου (Open Network Foundation), το **Λογισμικό Καθορισμένης Δικτύωσης (SDN)** αποτελεί ένα πλαίσιο το οποίο έχει την ικανότητα να μεταφέρει τη λογική ελέγχου στη βασική υποδομή, η οποία μπορεί να διαχωριστεί από τις εξειδικευμένες υπολογιστικές συσκευές που χρησιμοποιούνται για την πρόσβαση σε εφαρμογές και δικτυακές υπηρεσίες, καθώς και να εκλαμβάνουν το δίκτυο ως ένα σύνολο λογικά ανεξάρτητων εικονικών οντοτήτων (Chen et al., 2015).

Επί της ουσίας, αυτό σημαίνει ότι ο έλεγχος του **Λογισμικού Καθορισμένης Δικτύωσης (SDN) που** εγκαθίσταται στην κορυφή – ανώτερο τμήμα του δικτυακού εξοπλισμού, αποτελείται από ένα επίπεδο φυσικής υποδομής (υποδομή υλικού), προκειμένου να επιτευχθεί τάχιστα η επικοινωνία μέσω του OpenFlow επιπέδου ελέγχου διεπαφής. Η γενική αυτή ιδέα, επιτρέπει στο δίκτυο να λάβει τη μορφή πλατφόρμας με την ευελιξία και τον προγραμματισιμότητα της χρήσης των διαθέσιμων πόρων με το πλέον βέλτιστο τρόπο και την επίτευξη εξοικονόμησης κόστους και κλιμακοθτησιμότητα (scalability). Επιπρόσθετα, με την παροχή ενός API για εμπορικές εφαρμογές και υπηρεσίες, το **Λογισμικό Καθορισμένης Δικτύωσης (SDN) ενοποιεί τις υπηρεσίες νέφους (cloud services) με χαρακτηριστικά και τα δίκτυα υψηλής ταχύτητας ως αρχιτεκτονική υπολογιστών, αναδιαμορφώνοντας ουσιαστικά την τεχνολογίας της πληροφορικής** (Chen et al., 2015).

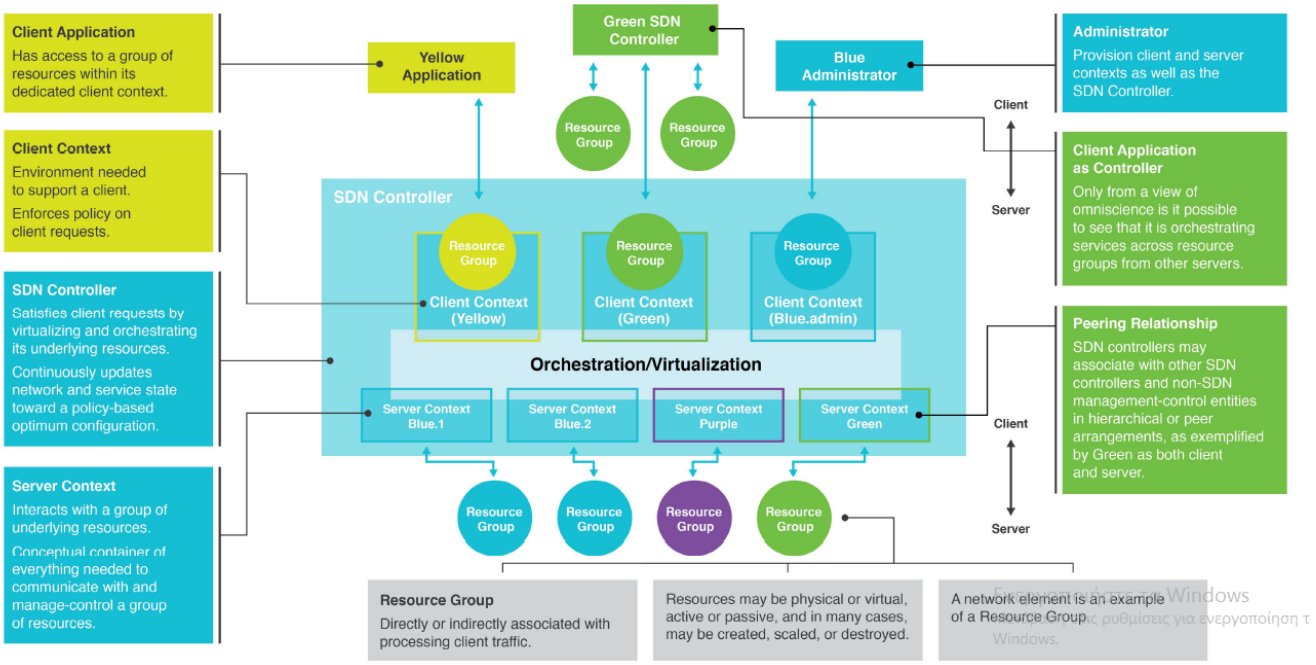


Εικόνα 4.7. Αρχιτεκτονική SDN

Στην πραγματικότητα, ο SDN ελεγκτής αποτελεί την ικανότητα του για έλεγχο ανατροφοδότησης σε πραγματικό χρόνο, η οποία εκφράζεται στις λειτουργίες ενορχήστρωσης και εικονοποίησης. Η αρχιτεκτονική στην Εικόνα 4.8., συνήθως απεικονίζει τον πελάτη και τον διακομιστή ως υφιστάμενους σε διαφορετικούς επιχειρηματικούς τομείς με τη χρήση διαφορετικών χρωματισμών.

Η Εικονοποίηση (Virtualization) αναφέρεται στη διαδικασία του διαχωρισμού, του διαμοιρασμού και της ενοποίησης των πόρων εντός εικονικών πόρων, κάθε ένας από τους οποίους είναι αφιερωμένος σε κάποιον συγκεκριμένο πελάτη.

Παράλληλα, η ενορχήστρωση (Orchestration) αναφέρεται στη διαδικασία της χρήση των πόρων του ελεγκτή, με σκοπό την ταυτόχρονη ικανοποίηση των κατ' απαίτηση υπηρεσιών από το σύνολο των πελατών του, σύμφωνα με την πολιτική της βελτιστοποίησης.



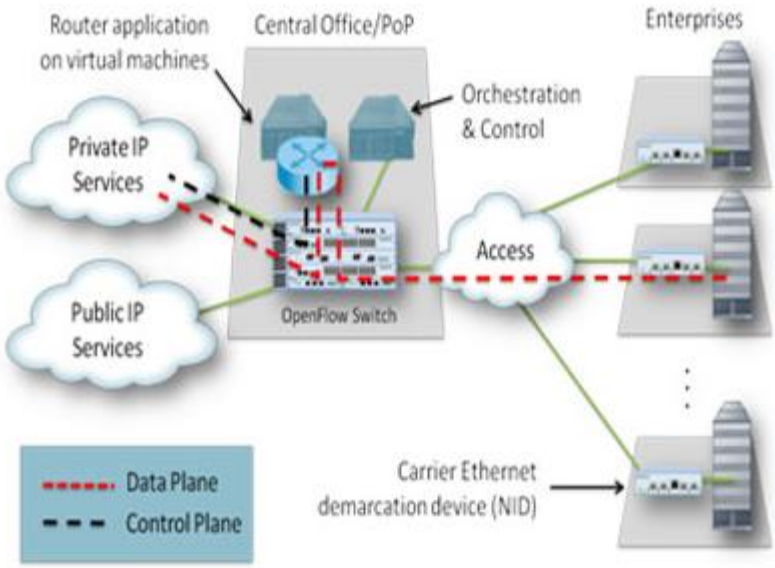
Εικόνα 4.8. Αρχιτεκτονική SDN

4.4.2. NFV

Οι Λειτουργίες Δικτύου Εικονοποίησης (NFV) προέρχονται από τηλεπικοινωνιακούς παρόχους οι οποίοι ευελπιστούν στη δημιουργία κατάλληλης υποδομής δικτύου εικονοποίησης (Virtualization) καθώς και εργαλείων, πολύ περισσότερο από την αύξηση των φυσικών συσκευών για την πραγματοποίηση των λειτουργιών όσον αφορά τη δρομολόγηση, τη διανομή, το φιλτράρισμα περιεχομένου, το φιλτράρισμα ανεπιθύμητων μηνυμάτων, του φορτίου εξισορρόπησης, την επιτάχυνση του WAN (Wide Area Network), τη βελτιστοποίηση και την ενοποίηση της διαχείρισης απειλών, καθώς και την ανάπτυξη νέων υπηρεσιών δικτύου. Οι παραπάνω συμμετοχές καθιέρωσαν το Ινστιτούτο Ευρωπαϊκών Τηλεπικοινωνιών Προτύπων (ETSI) της ομάδας NFV (των Λειτουργιών Δικτύου Εικονοποίησης), μεταξύ των μελών του οποίου συγκαταλέγεται η πλειοψηφία μεγάλων διεθνών επιχειρήσεων και παρόχων (Network Functions Virtualisation, 2012).

Σκοπός του οργανισμού είναι ο καθορισμός των απαιτήσεων και της αρχιτεκτονικής για τις καθορισμένες απαιτήσεις για την εικονοποίηση των λειτουργιών δικτύου και της αρχιτεκτονικής. Μακροπρόθεσμος στόχος είναι η παροχή βοήθειας προς τους πελάτες, προκειμένου αυτοί να μειώσουν το λειτουργικό κόστος του δικτύου, επιτυγχάνοντας ταυτόχρονα την προώθηση των υπηρεσιών λογισμικού για βασικά εξαρτήματα υλικού διακομιστή βιομηχανικού προτύπου, παρέχοντας μία ευέλικτη και επιδέξια λύση (Chen et al., 2015).

Απώτερος στόχος των **Λειτουργιών Δικτύου Εικονοποίησης (NFV)** είναι, η εικονοποίηση των πόρων των Τεχνολογιών Πληροφορικής μέσω μίας εύκολης σχετικά διαδικασίας, με σκοπό την ανάπτυξη της εικονοποίησης, παρέχοντας σημαντικές λειτουργίες δικτύου, περισσότερο από τις φυσικές απαιτήσεις για επαγγελματικό εξοπλισμό. Αυτές οι εικονικές συσκευές εντός του δικτύου λειτουργούν με τη μορφή φυσικής συσκευής και μπορούν να επιτύχουν ένα εύρος εξειδικευμένων λειτουργιών χωρίς την ύπαρξη συγκεκριμένης συσκευής (Taleb et al., 2015).



Εικόνα 4.9. Δειγματοληπτικές Δικτύου Εικονοποίησης (NFV)

Επί του παρόντος, οι **Λειτουργίες Δικτύου Εικονοποίησης (NFV)** εστιάζουν κυρίως σε θέματα όπως:

- Η εικονική ανταλλαγή ή οι φυσικές εικονικές θύρες στο συνδεδεμένο εικονικό διακομιστή (virtual server). Εδώ οι εικονικός δρομολογητής μπορεί να χρησιμοποιήσει την εικονική πύλη IPsec και SSL VPN.
- Τα εικονικά εργαλεία δικτύου. Αυτό καθιστά αναγκαία την ανάπτυξη ειδικών λειτουργιών για τις συσκευές δικτύου, οι οποίες δύναται να αναπτυχθούν με εικονικά εργαλεία τα οποία είναι ικανά να επιτύχουν ένα εύρος εξειδικευμένων λειτουργιών.
- Οι εικονικές συσκευές δικτύου. Μπορεί να παρέχει ανάλυση κίνησης, παρακολούθηση δικτύου και ειδοποίηση, εξισορρόπηση φορτίου, ποιότητα υπηρεσιών ή επιπέδου, συμπεριλαμβανομένης της παρακολούθησης δικτύου βάσει λογισμικού και της διαχείρισης συσκευών.
- Εικονική εφαρμογή: Μπορεί να παράσχει ένα πλαίσιο για τη βελτιστοποίηση του δικτύου και API για εφαρμογές νέφους (cloud), για την υποστήριξη του αυξανόμενου αριθμού κινητών τηλεφώνων (Chen et al., 2015).

4.5. mmWAVE Τεχνολογία

Η πυκνότητα των μικρών κυψελών, προξενεί μεγάλη backhaul κυκλοφορία στο βασικό δίκτυο (core network), η οποία αναπόφευκτα προκαλεί μία σημαντική αλλά κατά κάποιο τρόπο λιγότερο αντιμετωπίσιμο κώλυμα στο σύστημα. Η χρήση ινών ή καλωδίων στα πυκνά μικρά κυψελωτά backhaul θα μπορούσε να οδηγήσει σε ένα απαγορευτικά υψηλό κόστος και πρακτικές δυσκολίες σε επίπεδο υλοποίησης (Ge et al., 2014).

Σε αυτή την περίπτωση το ασύρματο backhaul μπορεί να προσφέρει μία κλιμακούμενη και οικονομικά αποδοτική λύση. Ωστόσο, οι παραδοσιακές μικροκυματικές συχνότητες που υπάρχουν ενδέχεται να αντιμετωπίσουν περιορισμούς στην επίτευξη του επιθυμητού κέρδους, εξαιτίας της υφιστάμενης συρρίκνωσης φάσματος. Παρά τους αναδυόμενους μηχανισμούς για την ενίσχυση της απόδοσης του ραδιοφάσματος, εξακολουθεί να παραμένει δύσκολη η επίτευξη ρυθμών δεδομένων άνω του 1 Gbps ή ακόμα και του 10 Gbps. Επομένως, είναι δύσκολο να αντιμετωπιστεί η ταχεία αύξηση των απαιτήσεων σε επίπεδο κυκλοφορίας 5G σε τέτοιες ζώνες σχετικά χαμηλής συχνότητας (Feng et al., 2016).

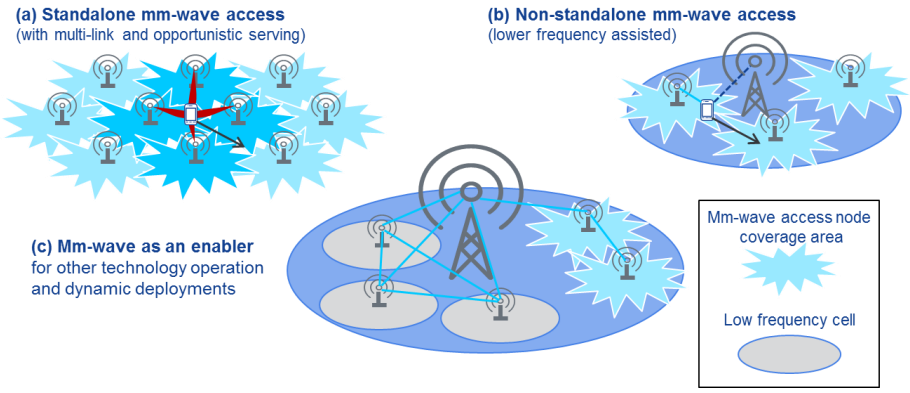
Οι τεχνικές χιλιοστομετρικού κύματος (mm-wave) που κυμαίνονται από 30 έως 300GHz, έχουν καταστεί εφικτές και πολλά υποσχόμενα μέσα για την υπερπήδηση των προαναφερθέντων ζητημάτων (Yong et al., 2011). Επί του παρόντος, οι τρείς περισσότερες πιθανές ζώνες κυματομορφών mm περιλαμβάνουν τα 28 GHz, 60 GHz και η E-band (71-76 και 81-86GHz), οι οποίες κυρίως δεν διαθέτουν άδεια. Με ένα τεράστιο διαθέσιμο εύρος ζώνης ο ρυθμός δεδομένων gigabit είναι πρακτικά εφικτός, καθώς επιλύει τα ζητήματα χωρητικότητας τα οποία συνεχίζουν να υπάρχουν στα συστήματα backhaul χαμηλότερης συχνότητας. Στα μικροκυματικά δίκτυα (mmWave) οι κατευθυντήριοι σύνδεσμοι συνήθως καθιερώνονται προκειμένου να αντισταθμίσουν την υψηλή απώλεια διαδρομής. Η χρήση υψηλών περιστρεφόμενων κεραιών μειώνει σημαντικά τις παρεμβολές και τις απώλειες διείσδυσης, οι οποίες αποδίδονται σε τοίχους και άλλους είδους εμπόδια, ενώ μετριάζουν πολλά σήματα τα οποία παρεμβάλλονται. Πρόσφατα, η μετάδοση των mmWabe κατέστη εφικτή εντός ενός εύρους μερικών εκατοντάδων μέτρων, η οποία υποδεικνύεται μέσω συστηματικών μετρήσεων, τα οποία προσφέρουν επαρκή κάλυψη για μικροκυψέλες backhaul (Nie et al., 2014).

Μολονότι, τα backhaul mmWave αποτελούν μία πολλά υποσχόμενη λύση, εντούτοις οι συνεχώς αυξανόμενες απαιτήσεις για επικοινωνία 5G φέρνει νέες προκλήσεις, οι οποίες θα πρέπει να ξεπεραστούν προκειμένου η τεχνολογία backhaul mmVawe να καταστεί εφαρμόσιμη σε διάφορα σενάρια. Οι παραδοσιακές τεχνολογίες mmWave εστιάζουν κυρίως στον άμεσο σύνδεσμο ενός χρήστη, αλλά υποστηρίζοντας τα σενάρια πολλαπλής ροής πολλαπλών χρηστών είναι πιθανό να αποτελέσουν μελλοντικά μία τάση για 5G backhaul με αυξανόμενες κυκλοφοριακές απαιτήσεις. Επίσης, η κατευθυνόμενη επικοινωνία ανοίγει το δρόμο για τη χωρική επαναχρησιμοποίηση, η οποία θα πρέπει να αξιοποιηθεί πλήρως για την προαγωγή της συνολικής απόδοσης του backhaul. Επιπρόσθετα, η απώλεια μεγάλων αποστάσεων και η παρεμπόδιση επηρεάζουν σοβαρά τη χωρητικότητα του δικτύου mmWave, η οποία απαιτεί κατάλληλα σχέδια δρομολόγησης, με σκοπό τη δημιουργία δυναμικών συνδέσεων αναμετάδοσης (Feng et al., 2016).

Στη μελέτης τους ο Feng και οι συνεργάτες (2016) καθιέρωσαν ένα καινοτόμο πλαίσιο για 5G mmWave backhaul, με βάσει μίας γενικής και ιδιαίτερα ελκυστικής αρχιτεκτονικής. Το προτεινόμενο πλαίσιο συνδυάζει πολλά υποσχόμενες τεχνικές φυσικού επιπέδου όπως η υβριδική διαμόρφωση και η πλήρως αμφίδρομη μετάδοση,

με τη χρήση συστημάτων δρομολόγησης και χρονοδρομολόγησης σε υψηλότερα επίπεδα.

Για την μελέτη της αρχιτεκτονικής mmWave θα χρησιμοποιηθούν δυο λειτουργικές εφαρμογές: α) αυτόνομη (standalone) και β) μη αυτόματη (non- standalone). Επιπλέον, η τεχνολογία mm-wave εξετάζεται και έναν παράγοντα, ο οποίος θα επιτρέπει τη λειτουργία άλλων τεχνολογιών και τη δυναμική ανάπτυξη, παρέχοντας τεχνολογίες και λύσεις για το ασύρματο backhaul και το fronthaul - σενάριο (c) (Εικόνα 4.10)[15].



Εικόνα 4.10. Αυτόνομη και μη αυτόνομη πρόσβαση.

4.6. UDN – Ultra Dense Cellular Network

Με την ανάπτυξη των μαζικών τεχνολογιών επικοινωνίας MIMO και mmWave στα συστήματα κινητής τηλεφωνίας 5ης γενιάς, ένας μεγάλο αριθμός μικρών κυψελών προβλέπεται να αναπτυχθεί για την κατασκευή των 5G πολύ πικών κυψελοειδών δικτύων. Συνεπώς, ο σχεδιασμός της αρχιτεκτονικής των 5G πολύ πυκνών κυψελοειδών δικτύων αποτελεί την πρώτη πρόκληση (Xiaohu et al., 2015).

4.6.1. Conventional Cellular Network Architecture

Η συμβατική αρχιτεκτονική κυψελοειδούς δικτύου, αναφέρεται σε έναν τύπο δενδροειδούς δικτύου στον οποίο κάθε δομικό μακροστοιχείο (macrocell base station – BSs) ελέγχεται από τους BS διαχειριστές ενός του βασικού δικτύου και όλη η κυκλοφορία backhaul προωθείτε στο κεντρικό δίκτυο μέσω της δεδομένης εισόδου. Προκειμένου να υποστηριχθεί η ανάπτυξη μικροκυψελίδων, μία υβριδική αρχιτεκτονική παρουσιάζεται για τα συμβατικά κυψελοειδή δίκτυα με ανάπτυξη

[15] https://5g-mmmagic.eu/project/

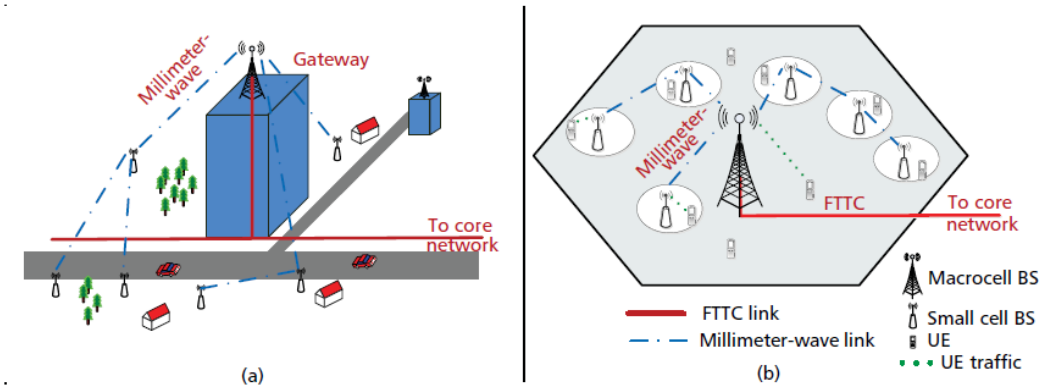
μικροκυττάρων. Σε αυτή την υβριδική αρχιτεκτονική, το δίκτυο μικροκυψέλων επίσης διαμορφώνεται ως ένας τύπος αρχιτεκτονικής δικτύου δένδρων, στο οποίο κάθε μικροκυψέλη BS ελέγχεται από τους BS διαχειριστές στο κεντρικό δίκτυο και η κυκλοφορία backhaul των BS μικροκυψέλων διαβιβάζεται προς το κεντρικό δίκτυο από το ευρυζωνικό διαδίκτυο ή τις συνδέσεις ινών. Παράλληλα, η κάλυψη μικροκυψέλων υπερκαλύπτεται με την κάλυψη των μικροκυττάρων (Xiaohu et al., 2015).

Σε σύγκριση με τα macrocell BSs, τα microcell BSs είναι σε θέση να παράσχουν υψηλής ταχύτητας ασύρματη μετάδοση τόσο σε εωτερικά σενάρια ή σημεία πρόσβασης (hotspot). Τόσο τα macrocell BSs όσο και τα microcell BSs, μπορούν ανεξάρτητα να διαβιβάσουν τα δεδομένα χρήστη και τα δεδομένα διαχείρισης σε συναφείς χρήστες. Οι χρήστες με τη σειρά τους μπορούν να παραδίδουν προς τις macrocells και microcells σύμφωνα με τις απαιτήσεις τους. Επιπλέον, η διαδικασία της παράδοσης ελέγχεται από διαχειριστές macrocells και microcells στο κεντρικό δίκτυο. Σε αυτή την αρχιτεκτονική δικτύου, το δίκτυο μικροκυψελών αποτελεί συμπλήρωμα για το συμβατικό δίκτυο macrocell, προκειμένου να ικανοποιήσει την ασύρματη μετάδοση υψηλής ταχύτητας σε μερικές περιοχές όπως οι εσωτερικοί χώροι και τα σημεία πρόσβασης (hotspots) (Xiaohu et al., 2015).

4.6.2. Αρχιτεκτονική Διανομής των UDN

Υποστηριζόμενο από την massive MIMO (Τεχνολογία πολλαπλών κεραιών) και από τις τεχνολογίες mmWave, η ανάπτυξη των μικρών κυψέλων αναδύεται μέσω των 5G κυψελοειδών δικτύων. Ωστόσο, είναι δύσκολη η προώθηση της κυκλοφορίας backhaul κάθε μικροκυψέλης BS από το ευρυζωνικό Διαδίκτυο ή το σύνδεσμο των ινών, σύμφωνα με τις προκλήσεις αύξησης του κόστους και της γεωγραφικής ανάπτυξης στα αστικά περιβάλλοντα. Επιπλέον, η μικρο κυψέλη BS συνήθως δεν μπορεί να μεταδώσει απευθείας την ασύρματη κίνηση backhaul στη δοθείσα πύλη εφόσον τα μικρά κυψελωτά BS που υιοθετούν την τεχνολογία χιλιομετρικού κύματος περιορίζουν την απόσταση της ασύρματης μετάδοσης. Σε αυτή την περίπτωση, η ασύρματη κίνηση backhaul θα πρέπει να μεταβιβαστεί στη δοθείσα πύλη με συνδέσμους multi-hop. Συνεπώς, η αρχιτεκτονική του δικτύου διανομής αποτελεί μια λογική λύση για τα πολύ πυκνά κυψελοειδή δίκτυα 5G. Στα 5G εξαιρετικά πυκνά κυψελοειδή σενάρια, για την επίλυση συχνών προβλημάτων μεταβίβασης του

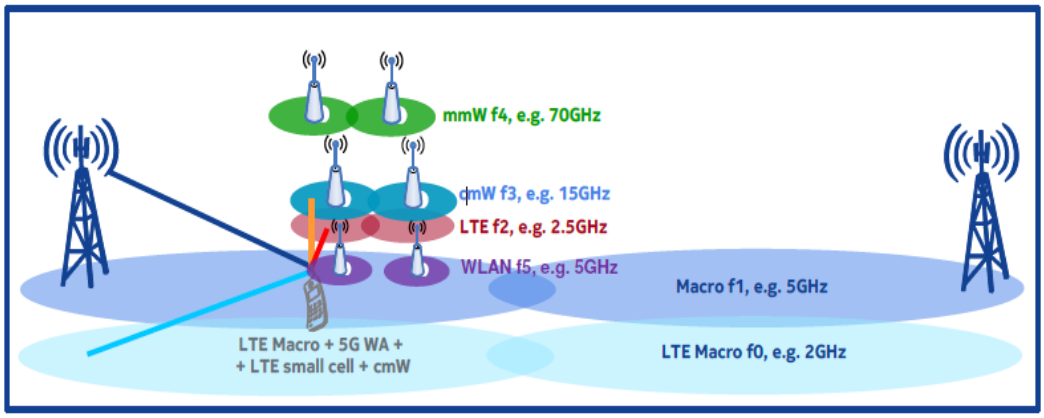
κινητού χρήστη σε μικρά κελιά, το macrocell BS διαμορφώνεται μόνο για να μεταδώσει τα δεδομένα διαχείρισης για τον έλεγχο της παράδοσης του χρήστη σε μικρά κελιά και το μικρό κύτταρο BS αναλαμβάνει τη μετάδοση δεδομένων χρήστη. Επομένως, το δίκτυο μικρών κυψελών δεν αποτελεί συμπλήρωμα του δικτύου macrocell. Τα 5G υπερ-πυκνά κυψελοειδή δίκτυα αποτελούνται από μικρά κύτταρα και macrocells (Xiaohu et al., 2015).



Εικόνα 4.11. Κατανομή υπερσύγχρονων κυψελοειδών δικτύων με ενιαία πύλη

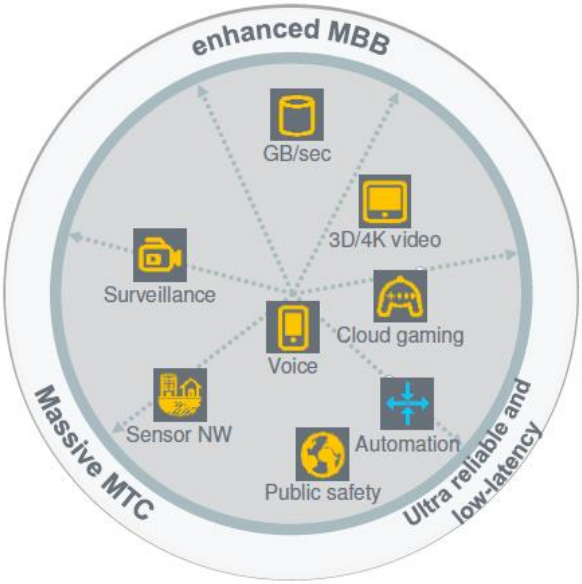
4.7 Αρχιτεκτονική βασισμένη στην χρήση πολλαπλών ασύρματων τεχνολογιών (Multi-RAT)

Τα δίκτυα 5^{ης} γενιάς, προβλέπουν την ενοποίηση διαφορετικών τύπων ασύρματης πρόσβασης υπό την εποπτεία ενός συστήματος, προκειμένου να καταστεί δυνατή και αποτελεσματική η αποδοτική λειτουργία της. Με την μέθοδο αυτή, πολλές ασύρματες τεχνολογίες που είναι ικανές να αποδώσουν υψηλές ρυθμαποδόσεις όπως LAN 802.11 family, LTE small cell, mmW 70GHz κ.λ.π, ενοποιούνται παρέχοντας στον τελικό χρήστη ευκολίες όπως καθοδήγηση κυκλοφορίας (traffic steering), επιλογή συνδέσμου (link selection), και ομαδοποίηση της δικτυακής κίνησης από διαφορετικές πηγές. Αυτό επιτρέπει στην αρχιτεκτονική αυτή να υποστηρίζει καλύτερη απόδοση και αυξημένη αξιοπιστία με διαφορετικά επίπεδα κινητικότητας. Μια τυπική απεικόνιση της αρχιτεκτονικής αυτής φαίνεται στην παρακάτω 4.12.



Εικόνα 4.12. Τυπικό multi-RAT σενάριο

Η προτεινόμενη αρχιτεκτονική Multi-RAT, εκτός από το πλεονέκτημα της ενοποίησης των διαφορετικών τύπων ασύρματων δικτύων, θα πρέπει να είναι σε θέση να υποστηρίζει και να διαχωρίζει περιπτώσεις οι οποίες διαφέρουν ανά χρήση/υπηρεσία. Αυτές οι κύριες τρεις περιπτώσει (Εικόνα 4.13) είναι ο υψηλός ρυθμός ασύρματης μετάδοσης (enhanced mobile broadband eMBB), η μαζική επικοινωνία μηχανών (MTC), και οι εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (ULC).

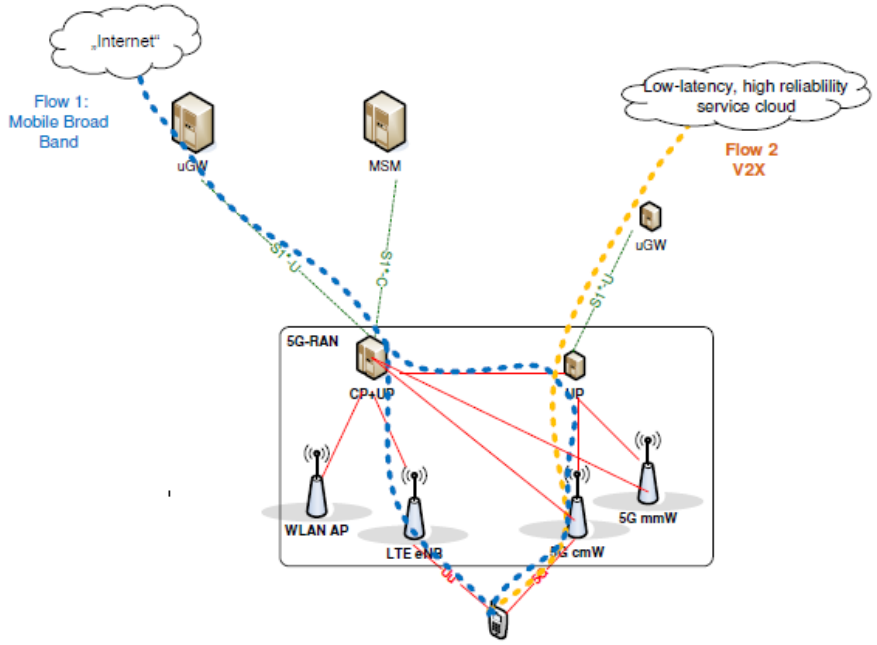


Εικόνα 4.13. Περιπτώσεις χρήσης κρίσιμης σημασίας

Οι απαιτήσεις αυτών των περιπτώσεων χρήσης είναι πολύ διαφορετικές όσον αφορά τις επιδόσεις του δικτύου, καθώς επίσης και στις κατηγορίες κόστους-απόδοσης. Για παράδειγμα, στην μαζική επικοινωνία μηχανών (MTC) ο παράγοντας κόστους είναι ο

πιο σημαντικός λόγω του μεγάλου αριθμού των συσκευών οι οποίες μπορεί να τεθούν εκτός λειτουργία για ένα μεγάλο χρονικό διάστημα. Από την άλλη πλευρά, οι κινητές ευρυζωνικές υπηρεσίες διαφοροποιούνται σε περιπτώσεις χαμηλής και υψηλής χρήσης. Επιπλέον, οι υπηρεσίες όπως το απλό διαδίκτυο, η εικονική πραγματικότητα είναι εξαιρετικά ευαίσθητες στην καθυστέρηση και υπηρεσίες όπως η ηλεκτρονική υγεία και ο αυτοματοποιημένος έλεγχος της κυκλοφορίας απαιτούν εξαιρετικά αξιόπιστες επικοινωνιακές συνδέσεις.

Για την διευκόλυνση των απαιτήσεων που θέτουν οι διάφορες υπηρεσίες, η ανάπτυξη των Multi-RAT δικτύων προβλέπει σχεδιασμό όπου κόμβοι οι οποίοι εξυπηρετούν εξαιρετικά αξιόπιστες υπηρεσίες (π.χ Low latency), θα βρίσκονται πιο κοντά σε σταθμούς βάσης (Base stations). Με αυτό τον τρόπο χρήστες οι οποίοι χρησιμοποιούν υπηρεσίες όπως εικονική πραγματικότητα ή ηλεκτρονική υγεία, θα καθοδηγούνται από το δίκτυο στο κόμβο ο όποιος βρίσκεται κοντινότερα στο σταθμό βάσης με αποτέλεσμα να επιτυχαίνεται χαμηλή καθυστέρηση (Low latency). Στην Εικόνα 4.14. διαφαίνονται οι περίπτωσης χρήσης κρίσης σημασίας (Chandrashekar-Meader et al., 2016).



Εικόνα 4.14. Κόμβος ο όποιος βρίσκεται κοντινότερα στο σταθμό βάσης.

Κεφάλαιο 5- Νέες απαιτήσεις ασφαλείας στα δίκτυα 5ης γενιάς

5.1 Εισαγωγή για θέματα Security

Στο κεφάλαιο αυτό περιγράφονται οι νέοι μηχανισμοί ασφαλείας που έχουν σχεδιαστεί από διάφορα ερευνητικά έργα του 5G-PPP. Ο γενικός στόχος είναι να προσφέρουν στρατηγικό αντίκτυπο σε τεχνολογικές και επιχειρηματικές δραστηριότητες, τυποποίηση και όραμα για ένα ασφαλές, ανθεκτικό και βιώσιμο δίκτυο 5ης γενιάς. Το κεφάλαιο καλύπτει την έρευνα και την καινοτομία - από τεχνικές λύσεις (αρχιτεκτονική ασφαλείας 5G και δοκιμαστικές μονάδες με δυνατότητα επέκτασης ασφαλείας 5G) στην επικύρωση της αγοράς και τη δέσμευση των ενδιαφερομένων - που καλύπτουν διάφορους τομείς εφαρμογών (Hiltunen et al., 2016).

5.2 Μεθοδολογίες ασφαλείας AAA για τα δίκτυα 5ης γενιάς

Στην παρούσα ενότητα, αναπτύσσονται τέσσερις μεθοδολογίες αναφορικά με τα δίκτυα 5ης γενιάς, οι οποίες θα είναι σε θέση να χειριστούν απαιτήσεις ελέγχου ταυτότητας (authentication), εξουσιοδότησης (authorization) και λογοδοσίας (accounting). Οι συγκεκριμένες τρεις απαιτήσεις είναι γνωστές και ως «AAA». Η συμβολή των παραγόντων AAA υπερβαίνει τις αυξημένες βελτιώσεις σε επίπεδο ασφάλειας όπως θα περίμενε κανείς σε ένα δίκτυο επόμενης γενιάς. Όμως, το εξελισσόμενο δίκτυο 5ης γενιάς πρόκειται να υποστηρίξει έναν απρόβλεπτο αριθμό συσκευών εξαιτίας της έκρηξης των δικτυακών μικροσυσκευών (IoT), το οποίο σε επίπεδο ανασφάλειας αναμένεται να κληθεί να αντιμετωπίσει πλήθος προκλήσεων. Επιπλέον, αυτές οι μεθοδολογίες στοχεύουν στην ενσωμάτωση λειτουργιών επαλήθευσης ταυτότητας και εξουσιοδότησης, μεταξύ δορυφορικών και επίγειων συστημάτων. Οι προτεινόμενοι μηχανισμοί δεν ανταποκρίνονται μόνο στις ανάγκες που σχετίζονται με την AAA, αλλά και σε προκαθορισμένες ασφαλείς λειτουργίες για τη στήριξη του νέου συνόλου περιπτώσεων χρήσης 5G (Hiltunen et al., 2016).

5.2.1 Βασικός AAA μηχανισμός ασφαλείας

Για τον βασικό έλεγχο ταυτότητας πρόσβασης στα δίκτυα 5ης γενιάς, θα μπορούσε να χρησιμοποιηθεί και αυτός που ήδη εφαρμόζεται στα δίκτυα προηγούμενης γενιάς 2G, 3G και 4G. Ωστόσο, οι διαδικασίες ελέγχου ταυτότητας κλειδιού (Authentication and Key-Agreement ή AKA) για αυτά τα συστήματα θα πρέπει να πληρούν ως επί το πλείστον τις υφιστάμενες απαιτήσεις για κάθε μία από αυτές τις γενιές. Τα δίκτυα 5ης

γενιάς θέτουν νέες απαιτήσεις στη διαδικασία AKA και ορισμένες νέες πτυχές που πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό του συστήματος 5G. Παραδείγματα τέτοιων νέων πτυχών είναι:

- ***Προηγμένη μυστικότητα των κλειδιών που παράγονται από τη διαδικασία AKA***: Στα δίκτυα προηγούμενης γενιάς (2G,3G,4G) έχουν γίνει αναφορές ότι τα κλειδιά των UICCs καρτών (Universal Integrated Circuit Cards) κρατούνται για μεγάλο χρονικό διάστημα (long-term keys), με αποτέλεσμα η ασφάλεια να μειώνεται σημαντικά. Τα δίκτυα $5^{ης}$ γενιάς αποσκοπούν στην προσέκλυση κρίσιμων υπηρεσιών και για αυτό το λόγο παρέχονται επιπρόσθετοι μηχανισμοί ασφαλείας. Τέτοιου είδους μηχανισμοί ασφαλείας είναι : α) Η τέλεια προσθήκη μυστικότητας (perfect forward secrecy), β) Ο περιορισμός μακροπρόθεσμου κλειδιού χρήσης σε χρονικές και / ή χωρικές διαστάσεις, γ) Η δυσκολότερη εκμετάλλευση συμβιβασμένων κλειδιών και δ) Οι μηχανισμοί επαναφοράς κλειδιών όταν έχουν διαρρεύσει.

- ***Μικρό-τμηματοποίηση δικτύων $5^{ης}$ γενιάς, υπό την εποπτεία AAA μηχανισμών:*** Η μικρό-τμηματοποίηση (Micro-segmentation) αναφέρεται σε μια πιο λεπτή προσέγγιση από την παραδοσιακή αρχιτεκτονική του δικτύου. Σε αυτή την περίπτωση, το δίκτυο χωρίζεται σε μικρότερα τμήματα, τα οποία μπορούν να βασίζονται σε πληροφορίες ταυτότητας του υπολογιστή, του χρήστη, της εφαρμογής ή του δικτύου. Για κάθε ένα τμήμα, ορίζονται έλεγχοι ασφάλειας. Μόνο οι πιστοποιημένες συσκευές και οι υπηρεσίες δικτύου μπορούν να ενταχθούν στο τμήμα, και επιπλέον, η κυκλοφορία εντός του τμήματος θα πρέπει να παρακολουθείται. Η κάθε εργασία που θα πραγματοποιείται σε κάθε τμήμα θα καθορίζεται από τις AAA λειτουργίες. Μέσω της παραπάνω διαδικασίας επιτυγχάνεται η ευκολότερη παρακολούθηση της συμπεριφοράς του δικτύου και τυχών απειλών που μπορεί αυτό να υποστεί.

- ***Αξιόπιστη διασύνδεση και εξουσιοδότηση:*** Ένα πρόβλημα που έχει αναπτυχθεί τα τελευταία χρόνια και είναι πιθανό να αποτελέσει σημαντικό ζήτημα για τα δίκτυα $5^{ης}$ γενιάς, είναι η πιστοποίηση ταυτότητας

(authentication) και η εξουσιοδότηση (authorization) μεταξύ των δικτύων κορμού του φορέα εκμετάλλευσης (operator). Προκειμένου να αποτραπεί μια μη εξουσιοδοτημένη οντότητα (π.χ. τρίτο μέρος (3rd parties)) ή ένας συμβεβλημένος φορέας εκμετάλλευσης (compromised operator) από τη λήψη φορέων επαλήθευσης ταυτότητας, ή την αποστολή πλαστών μηνυμάτων (Spoofed SMS) κλπ., η εισερχόμενη αίτηση προς έναν φορέα εκμετάλλευσης από άλλο φορέα πρέπει να πιστοποιηθεί και να εξουσιοδοτηθεί πριν γίνει αποδεκτή. Αυτό είναι ιδιαίτερα σημαντικό στην περίπτωση που προσφέρονται περισσότερο δυναμικές ευκαιρίες αλληλεπίδρασης, π.χ. με τη μορφή δυναμικής περιαγωγής (dynamic roaming), όπου μπορεί να μην είναι τόσο σαφές ποιοι είναι οι αλληλεπιδρώντες. Για τον λόγο αυτό θα πρέπει να υπάρχει επαρκής βεβαιότητα ότι η αλληλεπίδραση αναφέρεται σε αυθεντικές οντότητες, ακόμη και αν η εν λόγω οντότητα δεν αποτελεί ρητά συμβαλλόμενο μέλος στην επικοινωνία. Έτσι, για την πιστοποίηση και την εξουσιοδότηση του φορέα εκμετάλλευσης με το δίκτυο κορμού, προτείνεται το πρωτόκολλο AAA, με την διασφάλιση ότι δεν θα εισαχθούν νέα ζητήματα προστασίας της ιδιωτικής ζωής (Hiltunen et al., 2016).

5.2.2 Μηχανισμοί ασφαλείας για τα “Internet of Things - IoT”

Ο αριθμός των συνδεδεμένων συσκευών (ή " πράγματα"), που συνήθως αναφέρονται ως Internet of Things ή IoT, είναι πιθανό να αυξηθεί σημαντικά μέσα στα επόμενα χρόνια, με τα δίκτυα 5^{ης} γενιάς να επωμίζονται το βάρος αυτό υποστηρίζοντας πλήρως την λειτουργία τους . Δεδομένου ότι το δίκτυο 5^{ης} γενιάς επιδιώκει να είναι το καταλληλότερο για τις IoT συσκευές, θα πρέπει να παρέχει επαρκές επίπεδο ασφάλειας, χωρίς να εκθέτει άλλες υπηρεσίες και νομικές υποχρεώσεις, γεγονός που με τη σειρά του εισάγει νέες προκλήσεις ασφαλείας, για την εξακρίβωση της ταυτότητας των συσκευών IoT στο 5G.

Η χρήση της UICC (Universal Integrated Circuit Card) φαίνεται να αποτελεί έναν ιδιαίτερα σημαντικό παράγοντα ασφαλείας πρόσβασης στα συστήματα 5^{ης} γενιάς. Όμως η ισχυρή προστασία κλειδιών επιβάλλει εμπόδια χρήσης σε ορισμένες περιπτώσεις όπως, η μαζική ανάπτυξη επικοινωνιών τύπου μηχανής. Επίσης σε πολλές περιπτώσεις θα πρέπει να προστεθούν και φυσικές διασυνδέσεις (USB

dongles κ.λ.π.), όπου η πολυπλοκότητα της διανομής τους, το κόστος, και η διαχείριση τους θα περιόριζε την ελκυστικότητα του 5G.

Με την εμφάνιση ομαδικής επικοινωνίας σε μαζικά σενάρια ανάπτυξης, υπάρχει ένας μεγάλος αριθμός συσκευών με τις ίδιες ιδιότητες σε ένα δίκτυο, π.χ. επικοινωνία μηχανή με μηχανή (M2M). Αυτά τα είδη συσκευών μπορούν να σχηματίσουν δυναμικές ομάδες ανάλογα με την ομοιότητά τους, την περιοχή που βρίσκονται, την εφαρμογή στην οποία ανήκουν ή εάν είναι ο ίδιος τύπος συσκευής. Στην περίπτωση που ένας μεγάλος αριθμός συσκευών σε μια ομάδα χρειάζεται να έχουν πρόσβαση στο δίκτυο διαδοχικά σε σύντομο χρονικό διάστημα, οι υπάρχουσες μέθοδοι επαλήθευσης θα «υποφέρουν» από μεγάλη καθυστέρηση πρόσβασης στο δίκτυο μέχρι να ολοκληρωθούν οι διαδικασίες ελέγχου ταυτότητας όλων των συσκευών της ίδιας ομάδας. Ο λόγος είναι ότι κάθε συσκευή πρέπει να εκτελέσει πλήρη διαδικασία AKA (Authentication and Key-agreement) με τον διακομιστή ελέγχου ταυτότητας, οπότε η σηματοδότηση ελέγχου ταυτότητας στο δίκτυο θα αυξηθεί.

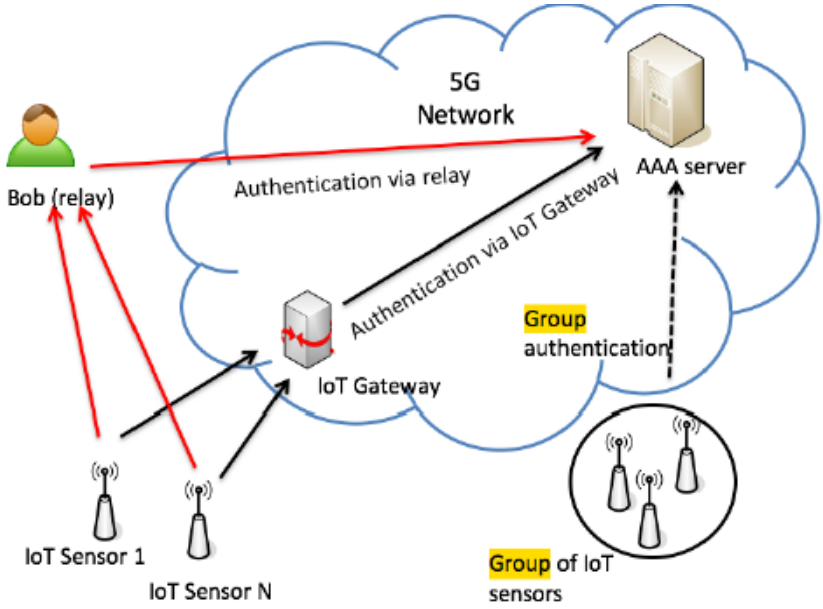
Οι προκλήσεις για την εξακρίβωση της αυθεντικότητας των συσκευών IoT χωρίς UICC και η μεγάλη καθυστέρηση που μπορεί να προκληθεί σε περίπτωση σε μαζική επαλήθευση ταυτότητας των συσκευών, φαίνεται να είναι ένα πολύ σημαντικό πρόβλημα. Για το λόγο αυτό θα πρέπει να μελετηθούν λύσεις οι οποίες θα αντιμετωπίσουν αυτά τα προβλήματα. Κάποιες από τις λύσεις οι οποίες μελετώνται στο έργο Ensure είναι:

- Προδιαγραφές ενός ή περισσοτέρων συσκευών βασισμένων στο hardware ή / και software για τη διαχείριση διαπιστευτηρίων με επαρκή επίπεδα ασφαλείας ως συμπλήρωμα του UICC, και διαχείριση χαμηλού κόστους ταυτότητας και διαπιστευτηρίων για τέτοιες συσκευές χωρίς UICC (Εικόνα 5.1.).

- Η χρήση διαφόρων τεχνικών κρυπτογραφικών, όπως τα αρχικά κλειδιά (pre-shared keys), ή τα πιστοποιητικά (certificates) κλπ. Επιπλέον, οι λύσεις αυτές θα πρέπει να υποστηρίζει τον έλεγχο ταυτότητας με βάση αυτά τα διαπιστευτήρια χωρίς UICC (Εικόνα 5.1.).

- Έλεγχος ταυτότητας βασισμένη σε κάποια τρίτη οντότητα, η οποία θα φέρει τη δική σας ταυτότητα (Εικόνα 5.1).

- Αποτελεσματικός έλεγχος ταυτότητας σε τεράστια σενάρια ανάπτυξης, με την υποστήριξη πιστοποίησης συσκευών που είναι σε ομάδες, είτε μέσω άμεσης επικοινωνίας από μια συσκευή IoT είτε μέσω μιας IoT πύλης (IoT gateway) με πιστοποιήσεις 5G (Εικόνα 5.1.) (Hiltunen et al., 2016).



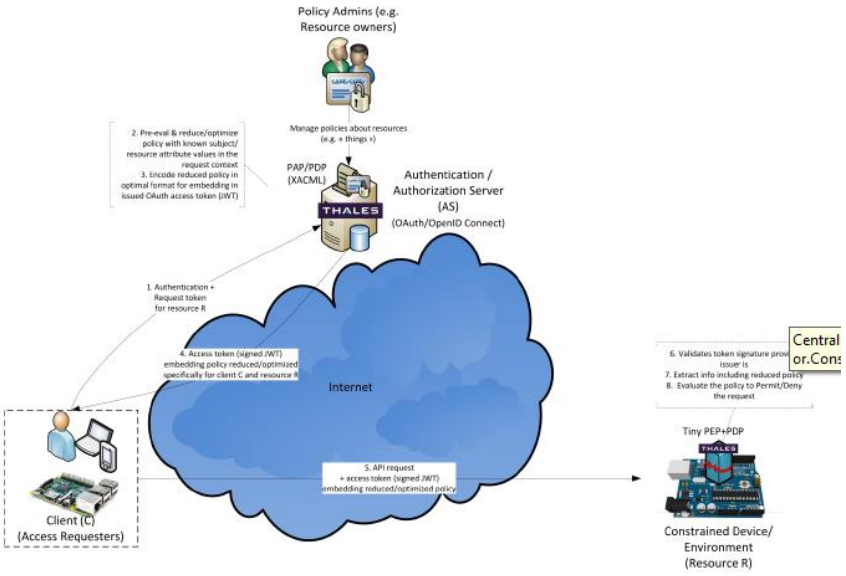
Εικόνα 5.1. Πιστοποίηση συσκευών IoT/M2M στο δίκτυο 5G

5.2.3 Κατανεμημένη αρχιτεκτονική εξουσιοδότησης για RCD (resource-constraint devices)

Ο ρόλος των διασυνδεδεμένων πόρων, όπως οι υπηρεσίες και οι συσκευές περιορισμού πόρων RCD (resource-constraint devices) τα επόμενα χρόνια θα εστιάζουν κυρίως στις δυνατότητες που προσφέρουν τα συστήματα. Σήμερα, πολλά RCD όπως οι αισθητήρες, οι ενεργοποιητές, τα δορυφορικά μόντεμ και οι συσκευές IoT ευρύτερα, υπάρχουν ήδη αλλά δεν είναι ασφαλείς. Ορισμένα πρότυπα έχουν καθοριστεί και εφαρμοστεί (π.χ. LoWPAN - Ασύρματα δίκτυα προσωπικών περιοχών χαμηλής κατανάλωσης, Πρωτόκολλο δρομολόγησης RPL για δίκτυα χαμηλής κατανάλωσης και απώλειες), αλλά με επίκεντρο το επίπεδο επικοινωνίας και όχι το επίπεδο εφαρμογής.

Για την θωράκιση αυτών των συσκευών που μέχρι σήμερα δεν υπάρχουν επίσημες προδιαγραφές για την αφέλεια τους, το έργο Ensure προτείνει κάποιες μεθοδολογίες οι οποίες μπορούν να εφαρμοστούν αξιόπιστα. Αυτές είναι:

- Πολλαπλοί χρήστες με διαφορετικά δικαιώματα.
- Απόφαση ανά χρήστη, πόρους και δράση.
- Η πρόσβαση θα βασίζεται σε δυναμικά μεταβαλλόμενες παραμέτρους.
- Πρόσβαση βασισμένη σε υπογεγραμμένο διακριτικό (Signed token) που περιέχει τα χαρακτηριστικά ταυτότητας του χρήστη και πολιτική προσαρμοσμένη για τον χρήστη και τον πόρο στον οποίο πρέπει να αποκτήσετε πρόσβαση.
- Έλεγχος πρόσβασης απευθείας ενσωματωμένο στη συσκευή (δηλ. Χωρίς σύνδεση με οποιονδήποτε εξωτερικό διακομιστή ελέγχου ταυτότητας).
- Ενσωμάτωση διαφόρων διακομιστών ελέγχου ταυτότητας (Hiltunen et al., 2016).



Εικόνα 5.2. Κατανεμημένη αρχιτεκτονική εξουσιοδότησης για RCD.

5.2.4 Έλεγχος ταυτότητας και αναγνώρισης (Federative authentication and identification)

Ο στόχος του είναι να διαδώσει, στο εσωτερικό των γραμμών παραγωγής, (i) κάποιο επίπεδο δέσμευσης και ευθύνης και (ii) την αξιολόγηση της εμπιστοσύνης των ειδικών λειτουργικών μπλοκ που χρησιμοποιούνται για την παροχή μιας

υπηρεσίας ή ενός περιεχομένου. Για να υπάρχει από άκρο σε άκρο αξιολόγηση εμπιστοσύνης, οι πληροφορίες που ενοποιούνται για τις διάφορες λειτουργικά τμήματα είναι συνδυαστούν και να χρησιμοποιηθούν από διαφορετικούς κόμβους (π.χ. τελικός χρήστης ή κόμβος του δικτύου) (Hiltunen et al., 2016).

5.3. Μηχανισμοί απορρήτου

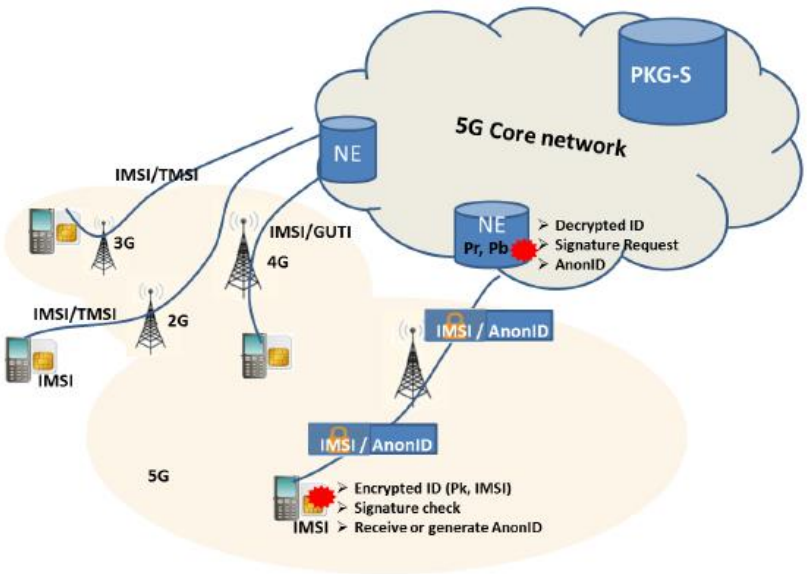
Το απόρρητο αποτελεί μία ιδιαίτερα σημαντική παράμετρο των δικτύων 5ης γενιάς, καθώς έχει υψηλό κοινωνικό αντίκτυπο και μπορεί να είναι μία από τις θεμελιώδεις απαιτήσεις που μπορούν να επιτρέψουν τη δημιουργία νέων υπηρεσιών και νέων επιχειρηματικών μοντέλων πάνω από δίκτυα 5G. Στην περίπτωση που υπάρξει σωστή αντιμετώπιση - προσέγγιση, το απόρρητο δύναται να αυξήσει το βαθμό διαβεβαίωσης και εμπιστοσύνη των χρηστών προς τα δίκτυα 5G.

Ο κύριος στόχος των μηχανισμών «5G-Ensure Privacy» είναι, ο εντοπισμός των απαιτήσεων προστασίας προσωπικών δεδομένων των 5G εκ των προτέρων και η παροχή μηχανισμών ασφαλείας, οι οποίοι θα μπορούν να αποτρέψουν παραβιάσεις της ιδιωτικής ζωής, υιοθετώντας μια προληπτική προσέγγιση. Επομένως, αυτή η ενότητα προσδιορίζει ορισμένους μηχανισμούς απορρήτου που σχετίζονται με το 5G. Αυτοί οι μηχανισμοί θα πρέπει να ενσωματωθούν στο συνολικό σχεδιασμό αρχιτεκτονικής ασφάλειας 5G έτσι ώστε να υποστηριχθούν εγγενώς στα συστήματα 5G, τις υπηρεσίες και τις επιχειρηματικές πρακτικές.

Οι δυνατότητες απορρήτου απορρέουν από την ανάλυση των περιπτώσεων χρήσης 5G και από τις αναμενόμενες απαιτήσεις απορρήτου για την εξαγωγή του σχεδιασμού τους. Για κάθε περίπτωση χρήσης, ερευνήθηκε επίσης η τεχνολογία μετριασμού της ιδιωτικής ζωής (π.χ. ανωνυμία με χρήση προσωρινής ταυτότητας, μηχανισμοί ελέγχου πρόσβασης, νέο σύστημα και διαδικασίες κρυπτογράφησης κ.λπ.), έτσι ώστε να ικανοποιούνται οι απαιτήσεις απορρήτου. Επιπλέον, οι μηχανισμοί απορρήτου αποσκοπούν στην ενίσχυση της προστασίας των δεδομένων των χρηστών, προτείνοντας λύσεις σε διάφορα επίπεδα, όπως σε επίπεδο δικτύου, καθώς και σε επίπεδο εφαρμογής (Hiltunen et al., 2016).

5.3.1 Αυξημένη προστασία προσωπικών δεδομένων.

Αυτός ο μηχανισμός στοχεύει στην παροχή προστασίας έναντι της αποκάλυψης ταυτότητας και της μη εξουσιοδοτημένης παρακολούθησης χρηστών, αποτρέποντας ή υπερασπιζόμενος τους διάφορους τύπους επιθέσεων αλίευσης IMSI (International Mobile Subscriber Identity), επιθέσεις τηλεειδοποίησης (Paging attacks) και επιθέσεις διαρροής θέσης (location leak attacks). Ο κύριος στόχος είναι να προσφέρει ισχυρότερη προστασία της ταυτότητας των χρηστών απ 'ό, τι στα τρέχοντα δίκτυα 3G και 4G. Η θεμελιώδης ιδέα πίσω από αυτόν τον παράγοντα μπορεί να συνοψιστεί σε διάφορες απλές έννοιες. Οι πραγματικές ταυτότητες των συσκευών που συνδέονται σε ένα δίκτυο 5^{ης} γενιάς, δεν θα πρέπει να μεταφέρονται μέσω του δικτύου, αλλά θα πρέπει να χρησιμοποιούνται μόνο δυναμικά τυχαία ψευδώνυμα (pseudo) κατά τη διάρκεια όλων των κανονικών λειτουργιών. Σε εξαιρετικές περιπτώσεις, εάν μια πραγματική ταυτότητα πρέπει να αποσταλεί από το UE (Εξοπλισμός Χρήστη) στο δίκτυο, θα πρέπει να αποστέλλεται κρυπτογραφημένη με το δημόσιο κλειδί του δικτύου και, ενδεχομένως, ένα αίτημα για μεταφορά ταυτότητας θα πρέπει να λαμβάνεται μόνο από στοιχεία ταυτότητας του δικτύου.



Εικόνα 5.3. Αρχιτεκτονική υψηλού επιπέδου προστασίας ιδιωτικού απορρήτου.

Πηγή:

Το σύνολο των προηγούμενων γενιών κινητών συσκευών, όπως αυτές τυποποιήθηκαν από το 3GPP, απέτυχαν να παράσχουν την κατάλληλη προστασία της ιδιωτικής ζωής όσον αφορά την προστασία των συσκευών και το αναγνωριστικό του

συνδρομητή (subscriber ID). Δηλαδή τα τρέχοντα πρωτόκολλα δεν κατάφεραν να αποτρέψουν την παρακολούθηση της θέσης των συσκευών και των χρηστών. Οι κινητές συσκευές «συμπλέκονται» με διάφορα πρωτοκόλλα αλληλεπίδρασης πρωτοκόλλου AAA, που εξαρτώνται από την πρόσβασή τους στο δίκτυο. Στην περίπτωση σύνδεσης στην κεραία της κινητής, ο Εξοπλισμός Χρήστη (UE) θα χρησιμοποιεί το πρωτόκολλο 5K AKA κατά την απόκτηση της προσωρινής ταυτότητάς του (π.χ. S-TMSI, GUTI). Εάν ο εξοπλισμός χρήστη (UE) προσπαθήσει να συνδεθεί με το WiFi τότε μπορεί να χρησιμοποιήσει το πρωτόκολλο EAP-SIM ή EAP-AKA για να επιτρέψει τη σύνδεση στο τοπικό δίκτυο ή στον εξελιγμένο πυρήνα πακέτων (EPC). Υπάρχουν επίσης, νέα πρωτόκολλα που αναπτύσσονται για περιορισμένες συσκευές. Ένας από τους στόχους αυτής της δυνατότητας είναι η χρήση διαφόρων τεχνικών, όπως η ανάλυση πρωτοκόλλου και η επαλήθευση, ώστε να παρέχεται μια λύση που προσφέρει αυξημένη προστασία της ιδιωτικής ζωής σε τέτοιες αλληλεπιδράσεις (Hiltunen et al., 2016). Επομένως, ο υπεύθυνος ασφαλείας πρέπει να υποστηρίξει:

- Αυξημένη ιδιωτικότητα σε αλληλεπιδράσεις πρωτοκόλλου.
- Ενισχυμένες ιδιότητες ανωνυμίας.
- Βελτιωμένη αδυναμία σύνδεσης.

5.3.2 Κρυπτογράφηση από άκρο σε άκρο

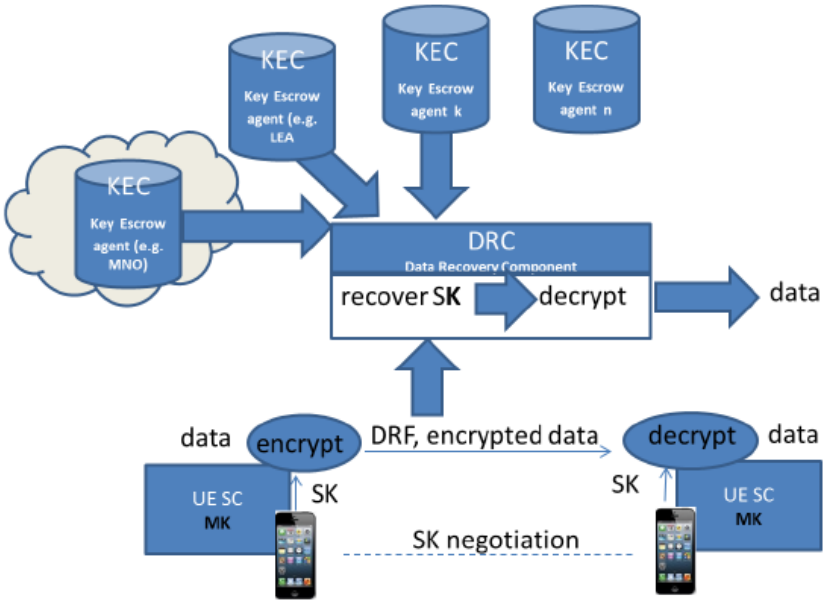
Αυτός ο μηχανισμός έχει ως στόχο την παροχή υποστήριξης κρυπτογράφησης από άκρο σε άκρο σε δίκτυα 5^{ης} γενιάς για την προστασία εμπιστευτικών δεδομένων / πληροφοριών χρηστών και την αποτροπή επιθέσεων υποκλοπής σε όλες τις πιθανές διαδρομές που μεταδίδεται η ροή δεδομένων του χρήστη μέσω του δικτύου κινητής τηλεφωνίας. Ο κύριος στόχος είναι να προσφέρει ισχυρότερη προστασία των δεδομένων του χρήστη και των πληροφοριών που σχετίζονται με τους χρήστες καθώς επίσης και σε περιπτώσεις όπου ένας χρήστης επισκέπτεται σημεία που δεν έχει εμπιστοσύνη στο δίκτυο (μη εφαρμοσμένου μηχανισμού ασφαλείας).

Η έλλειψη ασφάλειας από άκρο σε άκρο κάνει την επικοινωνία ευάλωτη και επιτρέπει την διείσδυση ψεύτικων ή κακόβουλα στοιχείων στο δίκτυο (malicious network). Ενώ παρέχοντας ασφάλεια από άκρο σε άκρο, όπου τα κλειδιά διοικούνται από τις ίδιες τις υπηρεσίες / συσκευές, αφενός αποτρέπει τη νόμιμη παρακολούθηση,

και αφετέρου οι φορείς εκμετάλλευσης μπορούν να εξασφαλίσουν την επικοινωνία βασικού δικτύου με τους δικούς τους μηχανισμούς.

Οι λύσεις διαχείρισης κλειδιών που γίνονται από τους παρόχους του δικτύου 5ης γενιάς, είναι κατάλληλες για περιπτώσεις όπου τα τελικά σημεία (End points) εμπιστεύονται τις δυνατότητες του παρόχου / παρόχων (π.χ., για να δημιουργούν πραγματικά τυχαία κλειδιά που δεν διαρρέουν στους ανταγωνιστές). Σε εξαιρετικά κρίσιμες εφαρμογές αυτές οι υποθέσεις εμπιστοσύνης ενδέχεται να μην είναι πάντοτε δικαιολογημένες. Η διαθεσιμότητα των συνδέσεων από άκρο σε άκρο μπορεί σε αυτές τις περιπτώσεις να επιτευχθεί αντικαθιστώντας τη διαχείριση κλειδιών που παρέχεται από τον πάροχο του δικτύου 5ης γενιάς μόνο με μια πιο αξιόπιστη εναλλακτική λύση.

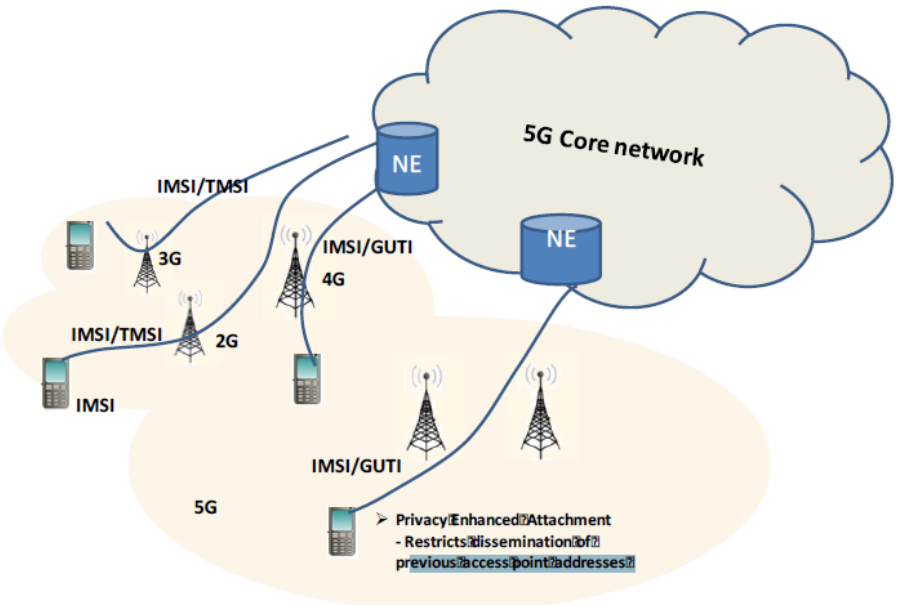
Επιπρόσθετα, εντοπίζονται αναπόφευκτες καταστάσεις κατά τις οποίες τα δεδομένα (ή τουλάχιστον τα μέρη τους) πρέπει να εκτίθενται, όπως και η νόμιμη παρακολούθηση. Ως εκ τούτου, μια λύση η οποία μπορεί να παράσχει υψηλό βαθμό προστασίας της ιδιωτικής ζωής, ακόμη και υπό αυτές τις συνθήκες είναι προκλητική. Αυτό μπορεί να επιτευχθεί με τα αποκαλούμενα βασικά συστήματα εγγύησης (key escrow systems), όπου τα κλειδιά σύντομων συνδέσεων (short-term session) παράγονται τοπικά και μοιράζονται μόνο μεταξύ των τελικών σημείων επικοινωνίας (long-term master keys), αλλά κρυπτογραφούνται από μακροπρόθεσμα βασικά κλειδιά ειδικά για τους χρήστες τελικών σημείων. Προκειμένου να αποφευχθούν τα μεμονωμένα σημεία εμπιστοσύνης, τα οποία συχνά αποτελούν ενιαία σημεία αποτυχίας, τα βασικά κλειδιά μοιράζονται μεταξύ ορισμένων ανεξάρτητων συστήματα εγγύησης (κυβερνητικά υποκαταστήματα, φορείς κινητής τηλεφωνίας κ.λπ.). Ένα κατώτατο (k, n) σχήμα μοιραζόμενης μυστικότητας θα επιτρέψει την ιδιωτικότητα, με μια έννοια ότι λιγότεροι από k χρήστες (agents) δεν λαμβάνουν καμία πληροφορία σχετικά με το κύριο κλειδί και ότι κάθε k ή περισσότεροι χρήστες (ίσως μικρότεροι από όλους τους n χρήστες) μπορούν να ανακτήσουν το κύριο κλειδί (Hiltunen et al., 2016).



Εικόνα 5.4. Αρχιτεκτονική υψηλού επιπέδου κρυπτογράφησης από το σημείο σε σημείο.

5.3.3 Απόρρητη ταυτότητα συσκευής (Device identifier(s) privacy)

Ένας άλλος μηχανισμός των δικτύων 5ης γενιάς, αποβλέπει στην εφαρμογή από σημείο σε σημείο (end-to-end) τεχνικών ανωνυμίας στις συσκευές των χρηστών, προσφέροντας με αυτό τον τρόπο προστιθέμενη προστασία ιδιωτικού απορρήτου (Privacy Enhanced Attachment - PEA), καθώς επίσης και προστασία έναντι της ταυτότητας των συσκευών (και ενδεχομένως και της ταυτότητας των χρηστών). Εστιάζει κυρίως στην προσφορά ισχυρότερης προστασίας ταυτότητας της συσκευής (και των σχετικών χρηστών) από ότι τα υφιστάμενα δίκτυα, σε σύγκριση με τον μηχανισμό Προστασίας Προσωπικών Δεδομένων (Privacy Enhanced Identity Protection), ο οποίος στοχεύει πρωτίστως στη διαφύλαξη της ταυτότητας των συνδρομητών. Επιπλέον, η πολιτική απορρήτου θα πρέπει να ελέγχεται άμεσα από τον χρήστη, ο οποίος θα διαθέτει κατάλληλα εργαλεία για τη διαχείριση της πολιτικής. Ο μηχανισμός καλύπτει και τις δύο συσκευές με και χωρίς UICC / SIM που συνδέονται μέσω διαφόρων τεχνολογιών δικτύων (Hiltunen et al., 2016).

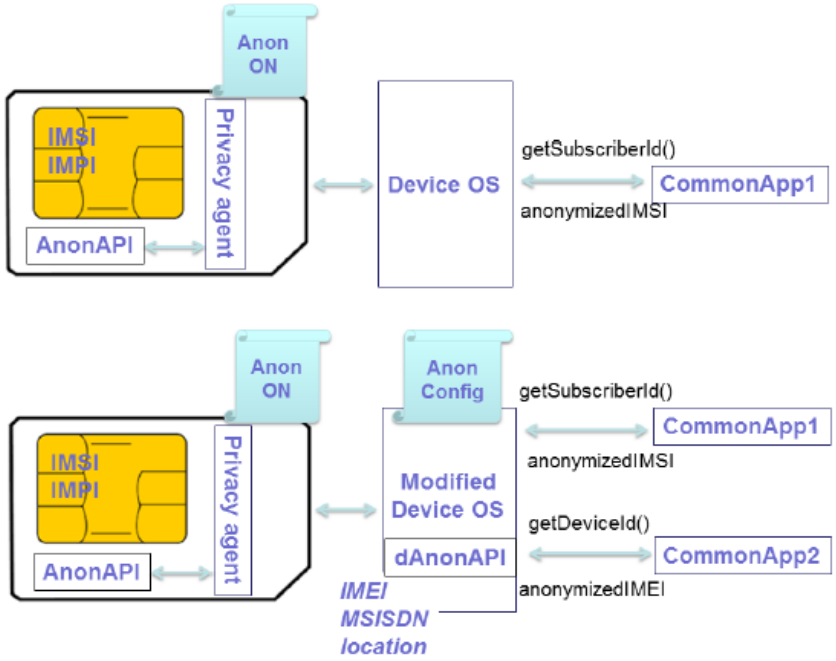


Εικόνα 5.5. Προστασία ιδιωτικού απορρήτου

5.3.4 Ανωνυμοποίηση βασισμένη στην SIM

Ο σκοπός του συγκεκριμένου μηχανισμού είναι, η παροχή τεχνικών ανωνυμοποίησης στο UICC (SIM) του χρήστη, προσφέροντας προστασία έναντι της αποκάλυψης ευαίσθητων πληροφοριών που αποθηκεύονται κυρίως στην κάρτα SIM. Η διαμόρφωση απορρήτου / ανωνυμοποίησης (ή το προφίλ) πρέπει να ελέγχεται άμεσα από το χρήστη, ο οποίος θα είναι σε θέση να ενεργοποιήσει διαφορετικά προφίλ ανωνυμοποίησης, τα οποία θα είναι αποθηκευμένα στην κάρτα SIM. Η κάρτα SIM του χρήστη θα φιλοξενήσει μια εφαρμογή απορρήτου, ανεξάρτητα από τη συσκευή του χρήστη που χρησιμοποιεί την κάρτα SIM, η εφαρμογή θα βοηθήσει στην προστασία του απορρήτου του χρήστη, σύμφωνα με το διαμορφωμένο προφίλ προστασίας προσωπικών δεδομένων. Η κάρτα SIM εφαρμόζει τους αλγόριθμους ανωνυμοποίησης και προσφέρει πρόσβαση στις υλοποιήσεις τους μέσω ενός API (Interface Protocol Interface). Ο εφαρμογή προστασίας προσωπικών δεδομένων μπορεί να ρυθμιστεί ώστε να ενεργοποιεί και να απενεργοποιεί την ανωνυμοποίηση και να εφαρμόζει διαφορετικούς αλγόριθμους στα αποθηκευμένα ευαίσθητα δεδομένα, όπως IMSI, IMPI (IP Multimedia Private Identity), MSISDN κλπ. Όταν μια εφαρμογή που έχει εγκατασταθεί στην συσκευή απαιτεί πρόσβαση στα δεδομένα της SIM που είναι προστατευμένα, τότε καλείται ο μηχανισμός απορρήτου προκειμένου να μετατρέψει αυτά τα δεδομένα σε ανώνυμα (Μη ορατά στην

εφαρμογή που είναι εγκατεστημένη στην συσκευή) με τον αλγόριθμο ρύθμισης ανωνυμοποίησης (Εικόνα 5.6.) (Hiltunen et al., 2016).



Εικόνα 5.6. Αρχιτεκτονική υψηλού επιπέδου για την ανωνυμοποίηση της SIM

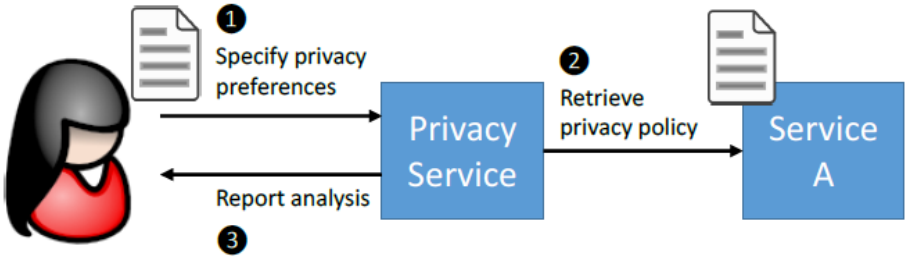
5.3.5 Ανάλυση της πολιτικής απορρήτου (Privacy policy analysis)

Σήμερα, οι χρήστες δικτυακών υπηρεσιών αντιμετωπίζουν πληθώρα εφαρμογών που ενδέχεται να θέσουν σε κίνδυνο το απόρρητο του. Επί του παρόντος, είναι δύσκολο για τον χρήστη να κατανοήσει τις συνέπειες της ιδιωτικής χρήσης μιας υπηρεσίας κινητής τηλεφωνίας ή μιας εφαρμογής. Οι πολιτικές απορρήτου (όπου υπάρχουν) συχνά δεν είναι εύκολο για τους χρήστες να διαβάζουν και συνήθως δεν παρουσιάζονται εκ των προτέρων στον χρήστη.

Η βασική υποστήριξη για τα δίκτυα SDN και NFV στο 5G αυξάνει την προσδοκία ότι τα νέα εικονικά MNO (Virtual mobile network operator) θα μπορούν εύκολα να εισέλθουν στην αγορά και να φέρουν νέα καινοτόμα επιχειρηματικά μοντέλα. Για παράδειγμα, θα μπορούσε ένας VMNO να επιλέξει να χρεώσει πολύ λιγότερο τις υπηρεσίες του στο πελάτη, με την προϋπόθεση της εκμετάλλευσης των προσωπικών του πληροφοριών (όπως τα πρότυπα τοποθεσίας και χρήσης). Ωστόσο, οι χρήστες πρέπει να είναι σε θέση να κάνουν μια τεκμηριωμένη επιλογή σχετικά με ένα τέτοιο συμβιβασμό.

Αυτός ο μηχανισμός έχει ως στόχο να παρέχει στον χρήστη έναν τρόπο να αναλύσει την πολιτική απορρήτου μιας υπηρεσίας ή ενός (V) MNO και να την συγκρίνει με τις προκαθορισμένες προτιμήσεις. Επίσης, θα είναι σε θέση καθορίζει τις προτιμήσεις απορρήτου, συμπεριλαμβανομένου του τύπου των δεδομένων που είναι πρόθυμοι να μοιραστούν, για ποιο σκοπό και για ποια περίοδο. Στην ιδανική περίπτωση, η ανάλυση θα πραγματοποιηθεί πριν από τη χρήση της υπηρεσίας, για παράδειγμα, στον χρόνο εγκατάστασης της εφαρμογής του πελάτη ή στο σημείο σύνδεσης με ένα δίκτυο 5ης γενιάς (Εικόνα 5.7.).

Ο μηχανισμός πολιτικής απορρήτου θα μπορούσε να ενσωματωθεί στην εφαρμογή ανωνυμοποίησης που βασίζεται στην κάρτα SIM για τον καθορισμό των προτιμήσεων πολιτικής απορρήτου του χρήστη, οι οποίες στη συνέχεια μεταφράζονται στη μορφή που απαιτείται για το αρχείο ρυθμίσεων παραμέτρων του παραλήπτη της SIM (Hiltunen et al., 2016).



Εικόνα 5.7. Αρχιτεκτονική υψηλού επιπέδου του Εργαλείου Ανάλυσης Πολιτικής Απορρήτου

5.4 Ασφάλεια εμπιστοσύνης

Το έργο «5G-ENSURE» αναμένεται να προσφέρει ένα νέο μοντέλο εμπιστοσύνης το οποίο, θα μπορεί να αντιμετωπίσει τις περίπλοκες σχέσεις μεταξύ των πολλών παραγόντων των δικτύων 5ης γενιάς, συμπεριλαμβανομένων των αλληλεπιδράσεων μηχανή-μηχανή (M2M), που χαρακτηρίζουν τα δίκτυα επόμενης γενιάς. Το μοντέλο εμπιστοσύνης πρέπει να αντιμετωπίσει διάφορες πτυχές όπως (Hiltunen et al., 2016).:

- Η εμπιστοσύνη μεταξύ των αυτοματοποιημένων συστημάτων (π.χ. μέσω προηγμένων μεθόδων πιστοποιητικών και συμβολοσειρών-token): δηλαδή M2M.

- Η εμπιστοσύνη μεταξύ ανθρώπινων φορέων που έχουν ευθύνες για διαφορετικά τμήματα δικτύων 5ης γενιάς, μεταξύ χρηστών και φορέων δικτύου, και μεταξύ χρηστών του δικτύου (U2Ut).
- Η εμπιστοσύνη ενός ανθρώπινου - φορέα έναντι ενός συστήματος (U2Mt).
- Η εμπιστοσύνη που έχει ένας χρήστης με ένα αυτόματο σύστημα (μηχανή) με τον οποίο αλληλεπιδρά, (M2Ut).

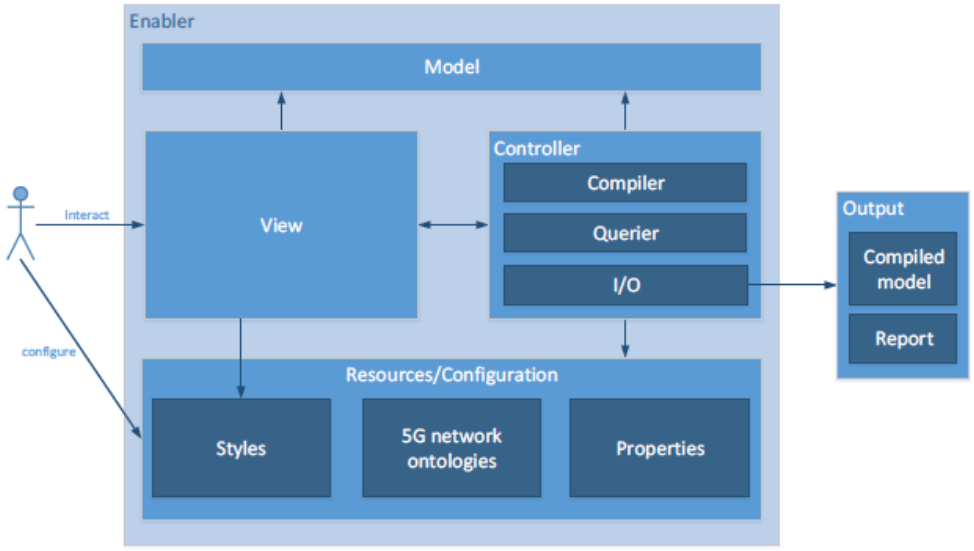
5.4.1 Έμπιστος κατασκευαστής (Trust builder)

Τα δίκτυα 5ης γενιάς αναμένεται να εισαγάγουν νέους φορείς και ρόλους. Η εκτεταμένη έννοια του "φορέα (operator)" θα μπορούσε να περιλαμβάνει π.χ. κατασκευαστές αυτοκινήτων που ενσωματώνουν συσκευές 5G στα αυτοκίνητά τους κατά το χρόνο παραγωγής. Αυτός ο νέος τύπος φορέα εκμετάλλευσης μπορεί να χρειαστεί συμφωνίες περιαγωγής (roaming), με παραδοσιακά δίκτυα MNO (mobile network operator) για τους σκοπούς της απομακρυσμένης διαχείρισης των προϊόντων τους, αφού εγκαταλείψουν τη γραμμή παραγωγής. Τα νέα σενάρια χρήσης θα μπορούσαν να επιφέρουν αλλαγές στις βασικές ευθύνες όπως είναι, η εξακρίβωση της ταυτότητας, ζήτημα που σημαίνει ότι οι παραδοσιακοί φορείς εκμετάλλευσης θα πρέπει να μπορούν να αξιολογούν την αξιοπιστία των ισχυρισμών που διατυπώνονται από τους διάφορους νέους φορείς.

Η αυξανόμενη εικονικοποίηση δημιουργεί περαιτέρω περιπλοκές με φέτες (Slices) και υπο-φέτες (Sub-slices) που περιπλέκουν περαιτέρω τις σχέσεις εμπιστοσύνης. Ένας φορέας εκμετάλλευσης ενδέχεται να επιθυμεί να αναθέσει τις ανάγκες του σε υλικό εξοπλισμού ICT (Information and communication technology) σε έναν τρίτο προμηθευτή Cloud ως λογισμικό πάνω από τα πρότυπα υπηρεσιών cloud της IaaS (infrastructure as a service) ή PaaS (platfore as a service). Αντίστροφα, ένας φορέας εκμετάλλευσης που εξακολουθεί να διαθέτει εξειδικευμένο υλικό (dedicated hardware could) θα μπορούσε να χρησιμοποιήσει αυτό για την δημιουργία ενός εικονικού (virtual) MNOs. Αυτός ο μηχανισμός θα πρέπει να παρέχει στους σχεδιαστές συστημάτων έναν τρόπο να μοντελοποιούν και να αναλύουν τα συστήματά τους, εντοπίζοντας αυτομάτως τις σχετικές απειλές και απαριθμώντας στρατηγικές για τη διαχείρισή τους.

Το μοντέλο εμπιστοσύνης θα υλοποιηθεί ως οντολογία που θα κωδικοποιεί τα αναγνωρισμένα περιουσιακά στοιχεία, τις απειλές και τους ελέγχους σε ένα γνωστικό πεδίο. Ο μηχανισμός θα παρέχει επίσης ένα GUI (Graphic User Interface) για το σχεδιασμό μοντέλων συστημάτων που καθορίζουν τις σχέσεις μεταξύ των κοινωνικοτεχνικών (socio-technical) αγαθών του συστήματος. Με βάση το μοντέλο οντολογίας και συστήματος, αυτός ο παράγοντας θα είναι σε θέση να εντοπίσει τις σχετικές απειλές για την διαμορφωμένη αρχιτεκτονική του συστήματος, εμπλουτίζοντας το σχεδιασμένο μοντέλο συστήματος με τις πληροφορίες απειλής. Θα επιτρέψει επίσης στον σχεδιαστή να επιλέξει μια στρατηγική διαχείρισης βασισμένη σε ελέγχους που εντοπίζονται αυτόματα για συγκεκριμένη απειλή.

Επιπρόσθετα, το σύνολο αυτών των αποφάσεων κωδικοποιούνται στο μοντέλο του συστήματος και μπορούν να αναζητηθούν, να αναλυθούν και να ενημερωθούν όπως απαιτείται. Εκτός από το εμπλουτισμένο σημασιολογικό μοντέλο, ο μηχανισμός μπορεί να παράσχει μια αναφορά κειμένου η οποία δύναται να χρησιμοποιηθεί από διαφορετικά ενδιαφερόμενα μέρη, όπως από σχεδιαστές συστημάτων, κατασκευαστές εξαρτημάτων ή διαχειριστές κινδύνου, με σκοπό τη διαχείριση των εντοπισμένων απειλών (Hiltunen et al., 2016).



Εικόνα 5.9. Αρχιτεκτονική του συστήματος «**Trust builder**»

5.4.2 Πιστοποίηση VNF (VNF Certification)

Η μετατόπιση των λειτουργιών του δικτύου προς ένα κέντρο δεδομένων (Virtualized Network Functions - VNF) και οι νέες μέθοδοι ελέγχου δικτύου (Software Defined

Networking - SDN) οδηγούν σε κινδύνους τα Στοιχεία Δικτύου (NE) από τυχόν επιθέσεις. Η εικονικοποίηση (Virtualization) των λειτουργιών του δικτύου επιτρέπει την γρήγορη αποκατάσταση βλαβών και επιθέσεων μέσω της δυναμικής αναδιάταξης των λειτουργιών του δικτύου. Η πρόκληση είναι να σχεδιαστούν οι δυσλειτουργικές υπηρεσίες VNF, οι οποίες κατασκευάζονται μέσω του SDN, προκειμένου να διασφαλιστούν οι κρίσιμες υπηρεσίες που πρέπει να παραμείνουν λειτουργικές ακόμη και μετά από τεράστιες καταστροφές (π.χ. σεισμό) ή σοβαρές επιθέσεις ασφάλειας.

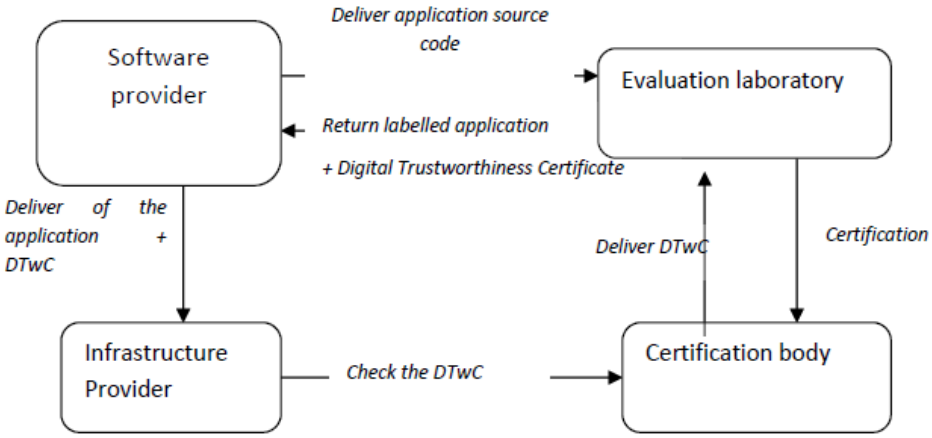
Η εικονικοποίηση των λειτουργιών του δικτύου και του εξοπλισμού, επιτρέπει την εμφάνιση αυτών σε ένα βασικό στοιχείο (Element), με αποτέλεσμα το διαμοιρασμό φυσικών πόρων (CPU, RAM, μνήμη και δίκτυο) με άλλες φιλοξενούμενες εικονικές μηχανές. Επί του παρόντος, ο πάροχος υποδομής διαχειρίζεται το δικό του VNF στη δική του υποδομή. Αντίθετα, στην αρχιτεκτονική 5G αναμένεται ότι οι φορείς VMNO (Virtual Mobile Operator Network) θα έχουν τη δυνατότητα να διαχειριστούν απευθείας το δικό τους VNF. Ο πάροχος υποδομής θα μπορεί να παρακολουθεί αυτά τα VNF και θα εγγυάται τη χρήση αυτού του εξοπλισμού.

Στην περίπτωση που το VMNO που επιθυμεί να χρησιμοποιήσει ένα ιδιόκτητο VNF (που αναπτύχθηκε από τον ίδιο για παράδειγμα), τίθεται το ερώτημα του πώς θα μπορούσε ένας φορέας VMNO να παρέχει εγγυήσεις αξιοπιστίας προς τον πάροχο υποδομής; Έτσι η ιδέα της συγκεκριμένης είναι να παρέχει, μέσω μιας διαδικασίας πιστοποίησης, «Πιστοποιητικό ψηφιακής αξιοπιστίας» (Digital Trustworthiness Certificate-DTwC). Αυτή η διαδικασία πιστοποίησης θα είναι ελαφρύτερη από την υφιστάμενη διαδικασία πιστοποίησης που προβλέπει ακόμη και αυτοπιστοποίηση. Οι πληροφορίες του πιστοποιητικού ψηφιακής αξιοπιστίας θα είναι:

- VNF περιβάλλον
- Απειλές και έλεγχοι για το VNF
- Αξιόπιστα χαρακτηριστικά του VNF

Η 5G-ENSURE θα παρέχει, μέσω των διαφορετικών περιπτώσεων χρήσης, ένα νέο μοντέλο εμπιστοσύνης που θα προσπαθεί να αντιμετωπίσει την πληθώρα των παραγόντων και επίσης θα εξετάσει την αλληλεπίδραση M2M που χαρακτηρίζει δίκτυα νέας γενιάς. Με βάση αυτό το μοντέλο εμπιστοσύνης, το 5G-ENSURE θα παρέχει τα κατάλληλα στοιχεία αξιοπιστίας ώστε να μπορεί να λαμβάνει υπόψη τις ανησυχίες περί εμπιστοσύνης και να προσφέρει (ή να προσδιορίζει) νέα εργαλεία ή

απαιτήσεις. Αυτός ο μηχανισμός θα παρέχει διαβεβαιώσεις για τα αξιόπιστα στοιχεία ειδικά για το VNF (Εικόνα 5.8.) (Hiltunen et al., 2016) .



Εικόνα 5.8. Επισκόπηση του σεναρίου διαδικασίας πιστοποίησης

5.5 Διαχείριση Δικτύου και Ασφάλεια Απομόνωσης Εικονικοποίησης

Η διαχείριση των δικτύων 5G αναμένεται να επιφέρει θεμελιώδεις αλλαγές, μέσω της εφαρμογής της λογικής του software-defined networking (SDN). Ενώ τα δίκτυα 4G έχουν ήδη ξεκάθαρη διάσταση μεταξύ του πλάνου δεδομένων και διαχείρισης, η υιοθέτηση του SDN στα δίκτυα 5G αναμένεται να αναπτύξει περαιτέρω τη διαχείριση του δικτύου με μια πιο συγκεντρωτική προσέγγιση. Ο κεντρικός έλεγχος της συνολικής υποδομής δικτύου έχει τεράστιες δυνατότητες απλοποίησης της διαχείρισης του δικτύου και προσφοράς νέων, πλουσιότερων και πιο ευέλικτων υπηρεσιών δικτύου. Το δυναμικό αυτό συμπληρώνεται από τον προγραμματιζόμενο χαρακτήρα των δικτύων SDN, ο οποίος με τη σειρά του διευκολύνει την εικονικοποίηση των δικτύων. Ωστόσο, ο κεντρικός έλεγχος αποτελεί έναν πολύτιμο στόχο για επιθέσεις και ένα μόνο σημείο αποτυχίας.

Ο στόχος των μέσων ασφαλείας που παρέχονται σε αυτό το τμήμα είναι διττός. Πρωτίστως, μερικοί από τους μηχανισμούς επιδιώκουν να εξασφαλίσουν το πλάνο ελέγχου του δικτύου και τα εικονικά δίκτυα πάνω από αυτό. Δεύτερον, ορισμένα αποσκοπούν στην εξασφάλιση υπηρεσιών δικτύου και την παροχή νέων υπηρεσιών ασφαλείας. Για το σκοπό αυτό, προτείνονται οι ακόλουθοι μηχανισμοί ασφαλείας:

- Μη αποδεκτή αποτύπωσης δακτυλικών αποτυπωμάτων μεταξύ των switches και του ελεγκτή δικτύου.

- Μηχανισμοί ελέγχου πρόσβασης για το επίπεδο ελέγχου του δικτύου.
- Έλεγχος των αλληλεπιδράσεων μεταξύ των στοιχείων του δικτύου.
- Ενίσχυση της εμπιστοσύνης στα εικονικά περιβάλλοντα δικτύου μεταξύ των τελικών σημείων δικτύου και επίσης μεταξύ των στοιχείων του δικτύου (SDN).
- Μηχανισμοί διαχείρισης δικτύου (χρησιμοποιώντας την αρχιτεκτονική SDN) που διευκολύνει την μικροκατανομή (micro-segmentation). Δημιουργία ασφαλούς τμήματος δικτύου για λεπτομερείς πολιτικές ροής δικτύου (Hiltunen et al., 2016).

Συμπεράσματα και Μελλοντικές εξελίξεις

Αναμφίβολα, ο τομέας της ασφάλειας συνιστά ένα συνεχώς αναπτυσσόμενο πεδίο, καθώς αυτό που σήμερα θεωρείται ως ασφαλές αύριο παύει να είναι. Πάντα θα υπάρχουν κακόβουλοι χρήστες οι οποίοι θα επιδιώκουν να εκμεταλλευτούν τα τρωτά σημεία των δικτύων. Ως εκ τούτου, το θέμα της ασφάλεια αποτελεί το μεγάλο ζητούμενο των δικτύων της επόμενης γενιάς, προκειμένου να αποφευχθούν σημαντικές βλάβες, οι οποίες θέτουν σε κίνδυνο της ιδιωτικότητα. Ωστόσο, η ασφάλεια δεν αφορά μόνο στην τοποθέτηση «μεγάλων κλειδαριών στην μπροστινή πόρτα», αλλά αναφέρεται και στην ασφάλιση του συνόλου των παραθύρων, καθώς ο καθένας μπορεί να εξαπατήσει. Ωστόσο, η σύγκριση καθιστά το σύστημα περισσότερο ασφαλές στην ολότητα του.

Τα τελευταία χρόνια, οι τεχνολογίες επικοινωνίας και υπολογισμών πληροφόρησης είναι βαθιά συγκλίνουσες, ενώ πλήθος τεχνολογιών ασύρματης πρόσβασης έχουν συμβάλλει στη συνεχή ανάπτυξη. Μπορεί να προβλεφθεί ότι η επερχόμενη τεχνολογία κινητής επικοινωνίας 5ης γενιάς (5G) δεν μπορεί πλέον να οριστεί από ένα ενιαίο επιχειρηματικό μοντέλο ή ένα τυπικό τεχνικό χαρακτηριστικό. Τα 5G αποτελούν ένα ολοκληρωμένο δίκτυο πολυεθνικών και πολυτελών τεχνολογιών, το οποίο καλείται να καλύψει τις μελλοντικές ανάγκες ενός ευρέος φάσματος μεγάλων δεδομένων και την ταχεία ανάπτυξη πολλών επιχειρήσεων και βελτιώνει την εμπειρία των χρηστών, παρέχοντας έξυπνες και προσαρμοσμένες υπηρεσίες.

Όπως έχει αναφερθεί και αναλυθεί εκτεταμένα στην παρούσα μελέτη, πλήθος πιθανών τεχνικών εισάγονται για τα μελλοντικά συστήματα 5G. Μολονότι, οι τεχνικές αυτές αποτελούν μόνο ένα μικρό μέρος - τμήμα αυτών που τελικά θα χρησιμοποιηθούν στα συστήματα 5G, εντούτοις διαφωτίζουν εν μέρει αυτή την ελπιδοφόρα τάση τεχνολογικής ανάπτυξης. Προκειμένου να επιτευχθεί ο στόχος του IMT-2020 και έπειτα, πιστεύεται ότι θα υπάρξουν εξαιρετικά μεγάλες πρόοδοι στην τεχνολογία των ασύρματων επικοινωνιών, καθώς πλήθος ερευνών έχει εστιάσει στην τεχνολογία 5G σε επίπεδο αρχιτεκτονικής, αλλά κυρίως στον τομέα της ασφάλειας. Ενώ, αναμένεται ότι η νέα αρχιτεκτονική και οι τεχνικές δικτύου θα αναδυθούν στην προσπάθεια προώθησης των υφιστάμενων κυψελοειδών δικτύων.

Πιο συγκεκριμένα, οι προτεινόμενες αρχιτεκτονικές της 5G δικτύωσης οι οποίες έχουν διερευνηθεί εκτεταμένα είναι η fronthaul και η backhaul δικτύωση, η δικτύωση η NFV η οποία αναφέρεται στην εικονοποίηση των λειτουργιών δικτύου, η SDN η οποία βασίζεται στο λογισμικό και η mmWave η οποία χρησιμοποιεί την αρχιτεκτονική της μικροκυματικής ζώνης.

Η παρούσα βιβλιογραφική μελέτη, εστίασε το ερευνητικό της ενδιαφέρον κυρίως στο κομμάτι της ασφάλειας. Εντός αυτού του πλαισίου, διαπιστώθηκε ότι οι νέοι μηχανισμοί ασφαλείας που σχεδιάστηκαν από πλήθος ερευνητικών κέντρων στα πλαίσια των έργων 5G-PPP, αποβλέπουν στη συγκρότηση ενός ασφαλούς, ανθεκτικού και βιώσιμου δικτύου 5^{ης} γενιάς. Οι μεθοδολογίες πάνω στις οποίες αναπτύσσονται τα δίκτυα 5^{ης} γενιάς, εστιάζουν στις απαιτήσεις ελέγχου ταυτότητας (authentication), στην εξουσιοδότηση (authorization) και στη λογοδοσία (accounting), καθώς το αναπτυσσόμενο δίκτυο αναμένεται να παράσχει κάλυψη σε πλήθος δικτυακών μικροσυσκευών (IoT).

Αναφορικά με τους μηχανισμούς ασφαλείας, τα δίκτυα 5^{ης} γενιάς θέτουν νέες απαιτήσεις σε επίπεδο ελέγχου ταυτότητας κλειδιού (AKA) και συνεπακόλουθα νέες πτυχές που πρέπει να λειφθούν υπόψη κατά το στάδιο του σχεδιασμού, όπως η μυστικότητα των κλειδιών και η μικρο-τμηματοποίηση των δικτύων 5^{ης} γενιάς. Παράλληλα, οι μηχανισμοί απορρήτου φαίνεται να αποτελούν μία ιδιαίτερα σημαντική παράμετρο των δικτύων 5^{ης} γενιάς, καθώς αναμένεται να συμβάλλουν στη δημιουργία νέων υπηρεσιών και νέων επιχειρηματικών μοντέλων πάνω στα δίκτυα 5G, στην περίπτωση που υπάρξει σωστή αντιμετώπιση – προσέγγιση, αυξάνοντας το βαθμό αξιοπιστίας των χρηστών.

Βιβλιογραφία

Chang G, K., Liu, C. & Zhang, L. (2013) Architecture and applications of a versatile small-cell, multi-service cloud radio access network using radio-over-fiber technologies. In: Proceedings of IEEE International Conference on Communications Workshops, Budapest, 879–883.

Chen, M., Hu, L., Taleb, T. & Sheng, Z. (2015). Cloud-based Wireless Network: Virtualized, Reconfigurable, Smart Wireless Network to Enable 5G Technologies. *Mobile Networks Applications, 10.*

Chin, W.H. Fan, Z. & Hainer, R. (2014) Emerging technologies and research challenges for 5G wireless networks. *IEEE Wireless Communications, 21,* 106-112.

Costa – Reguena, J. (2014) SDN integration in LTE mobile backhaul networks. In: Proceedings of International Conference on Information Networking, Phuket, 264–269

Demestichas, P., Georgakopoulos, A., Karvounas, D. et al (2013) 5G on the horizon: Key challenges for the radio-access network. *IEEE Vehicular Technology Magazine, 8, 47-53.*

Deliverable D3.1 (2016) 5G-PPP security enablers technical roadmap (early vision).

EuCNC (2016) 5G – Architecture Contributions. EuCNC Conference

Feng, W., Li, Y., Jin, D., Su, L. & Chen, S. (2016). Millimetre-Wave Backhaul for 5G Networks: Challenges and Solutions. *Sensors, 16,* 2-17.

Fischer-Hibner, S., Rannenberg, K., Yngstrom, L. & Lindskog, S. (2006) *Security and Privacy in Dynamic Environments.* USA: Springer.

Ge, X., Cheng, H., Guizani, M. & Han, T. (2014). 5G wireless backhaul networks: Challenges and research advances. IEEE Netw. 2014, 28, 6–11.

Hiltunen et al. (2016) 5G Enablers for Network and System Security and Resilience

Hugo, Tullberg., Petar, Popovski., et al., (2015). METIS System Concept: The Shape of 5G to Come. *IEEE International Conference on Communications (ICC),*2015,*1-9*

H2020 5G-Crosshaul project Grant No. 671598. Detailed analysis of the technologies to be integrated in the XFE based on previous internal reports from WP2/3.2015.30-50.

Jain, R. & Paul, S. (2013) Network virtualization and software defined networking for cloud computing: a survey. *IEEE, Communications Magazine, 51, 24-31.*

McKeown et al., (2008) OpenFlow: Enabling Innovation in Campus Networks. Computer Communication Review, *38,* 69-73.

Marc, Lichtman., Roger, Piqueras, Jover., Mina, Labib., et al., (2013). Threat Assessment and Mitigation. Virginia Tech, Blacksburg, VA, USA. 2Bloomberg LP, New York, NY, USA, 1-4.

Nie , S., MacCartney, GR., Sun, S. & Rappaport, T.S. (2014) 28 GHz and 73 GHz signal outage study for millimeter wave cellular and backhaul communications. In Proceedings of 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014; pp. 4856–4861

Rost, P. et al (2014) Cloud technologies for flexible 5G radio access networks. *IEEE Communication Magazine, 52*, 68–76

Sabella, D., Rost, P., Sheng, Y.L, et al. (2013) RAN as a service: challenges of designing a flexible RAN architecture in a cloud-based heterogeneous mobile network. In: Proceedings of Future Network and Mobile Summit, Lisboa.

Sike, H., Siddhard, P, R., Lan, Oliver., (2016) User Location Tracking Attacks for LTE Networks Using the Interworking Functionality, *ISBN 978-3-901882-83-8 c_ 2016 IFIP*, 1-6.

Subramanya, Chandrashekar., Andreas, Maeder., et al.(2016). 5G Multi-RAT Multi-Connectivity Architecture, *IEEE ICC2016-Workshops, 2016,1-2.*

Taleb, F., et al. (2015).

Wang, Z.X. & Zhang, W. (2014) A separation architecture for achieving energy-efficient cellular networking. *IEEE Trans Wireless Communications, 13*, 3113–3123

Xiaohu, Ge., et al. (2015) 5G Ultra-Dense Cellular Networks. *IEEE,*

Zheng, M.A., ZhengQuan, Z., ZhiGuo, D., PingZhi, F. & HengChao, L.I. (2015). Key techniques for 5G wireless communications: network architecture, physical layer and MAC layer perspectives. *Science China – Information Sciences, 58,*

Ζαχαριά Αθανασία, Μελέτη και αξιολόγηση των προτεινόμενων τεχνολογιών στα δίκτυα 5G, Διπλωματική εργασία, 2016.