



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

**Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΚΑΙ ΕΥΦΥΗ ΠΕΡΙΒΑΛΛΟΝΤΑ»**

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Ανάπτυξη ευέλικτης και ανθεκτικής πύλης δικτύου για
Ασύρματα Δίκτυα Αισθητήρων βασισμένη σε
τεχνολογία SDR για την προστασία
κρίσιμων υποδομών**

Μεταπτυχιακός Φοιτητής / Φοιτήτρια: Σπυρίδων Παπαγιάκουμος, AM msciot20005

Επιβλέπων / Επιβλέπουσα: Διονύσιος Κανδρής, Καθηγητής

ΑΙΓΑΛΕΩ, ΙΟΥΛΙΟΣ 2023



UNIVERSITY OF WEST ATTICA

FACULTY OF ENGINEERING

DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

**Master of Science in
“INTERNET of THINGS AND INTELLIGENT ENVIRONMENTS”**

MSc Thesis

**A flexible and resilient network gateway development
for Wireless Sensor Networks based on SDR technology
for critical infrastructure protection**

Student: Papagiakoumos, Spyridon, Registration Number msciot20005

MSc Thesis Supervisor: Kandris Dionysios, Professor

ATHENS-EGALEO, JULY 2023

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

Διονύσης Κανδρής Καθηγητής (Επιβλέπων)	Γρηγόριος Καλτσάς Καθηγητής (Μέλος)	Γρηγόριος Κουλούρας Αναπληρωτής Καθηγητής (Μέλος)

Copyright © Με επιφύλαξη παντός δικαιώματος. All rights reserved.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ και Σπυρίδων Παπαγιάκουμος, Ιούλιος 2023

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τους συγγραφείς.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον/την συγγραφέα του και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις θέσεις του επιβλέποντος, της επιτροπής εξέτασης ή τις επίσημες θέσεις του Τμήματος και του Ιδρύματος.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Ο κάτωθι υπογεγραμμένος Σπυρίδων Παπαγιάκουμος του Ανδρέα, με αριθμό μητρώου msciot20005, φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

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

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

Ο Δηλών



Σπυρίδων Παπαγιάκουμος

ΠΕΡΙΛΗΨΗ

Η συνεχής ανάπτυξη της τεχνολογίας στις κινητές επικοινωνίες σε συνδυασμό με την ανάγκη για συλλογή δεδομένων από αισθητήρες, για μεγαλύτερη ασφάλεια και σταθερότητα σε κρίσιμες υποδομές, έχουν φέρει στην επιφάνεια την αναγκαιότητα ανάπτυξης λύσεων ανοιχτού κώδικα για την υλοποίηση ιδιωτικών δικτύων άμεσης ανάγκης. Στην εργασία αυτή υλοποιείται ένας ανεξάρτητος σταθμός βάσης κινητής τηλεφωνίας 4G-LTE τεχνολογίας, για την υποστήριξη κρίσιμων δικτύων υποδομών με δυνατότητα πραγματοποίησης κλήσεων πάνω από το δίκτυο (VoLTE). Με χρήση ανοιχτού κώδικα λογισμικού, Open Source Software (OSS), της πλατφόρμας Open Air Interface (OAI) και της τεχνολογίας Software Define Radio (SDR) δημιουργούμε και αναπτύσσουμε ένα ιδιωτικό δίκτυο κινητής τηλεφωνίας 4G-LTE με ενσωμάτωση ελευθέρου ανοιχτού κώδικα σε ένα USRP γενικής χρήσης. Μετά το πέρας της ανάπτυξης πραγματοποιούνται κλήσεις μεταξύ συνδεδεμένων στο δίκτυο κινητών καθώς και περιήγηση στο διαδίκτυο.

ΛΕΞΕΙΣ – ΚΛΕΙΔΙΑ: Open Source Software, Open Air Interface, Software Define Radio, Ubuntu Linux, 4G LTE, Ettus, USRP B210, VoLTE, Asterisk, Κρίσιμες Υποδομές, Internet of Things, WSN

ABSTRACT

Constant technological development in mobile communications combined with the need of data collection from sensors, more security and stability in critical infrastructure, create the necessity for development of solutions based on open source code for the creation of private emergency mobile networks. In this project, we create an independent mobile communication network base station, using 4G-LTE, for critical infrastructure with the ability to make calls over network (VoLTE). Using Open Source Software (OSS), Open Air Interface platform (OAI) and Software Define Radio, we created a private mobile 4G-LTE network, with open source code integration on a general purpose USRP. Calls between connected devices as well as internet use is possible

KEYWORDS: Open Source Software, Open Air Interface, Software Define Radio, 4G LTE, Ettus, USRP B210, VoLTE, Asterisk, Critical Infrastructure, Internet of Things, WSN

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τους καθηγητές μου 1) Κύριο Παπαγέωργα Παναγιώτη και 2) Κύριο Κανδρή Διονύσιο, για την καθοδήγηση και υποστήριξη τους ως προς την υλοποίηση της, την εργασίας. Την παροχή κατάλληλου εξοπλισμού, τις γνώσεις που μου προσέφεραν καθ' όλη την διάρκεια των σπουδών μου και της μελέτης μου διπλωματική αυτή, καθώς και την εμπιστοσύνη τους, στο πρόσωπό μου για την εκπλήρωση της. Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου και την σύζυγό μου για την υποστήριξη σε όλη αυτή την προσπάθεια μου. Τέλος να ευχαριστήσω από καρδιάς τον υποψήφιο διδάκτορα του τμήματος Κύριο Χειμάρα Βασίλειο για την πολύτιμη συνδρομή και βοήθειά του για την επιτυχή ολοκλήρωση και υλοποίηση της εργασίας.

ΠΙΝΑΚΑΣ ΣΥΜΒΟΛΩΝ-ΑΚΡΩΝΥΜΙΩΝ-ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

3GPP:	3rd Generation Partnership Project (3GPP)
AKA:	Authentication and Key Agreement
ADC:	Analog to Digital Converter
AMPS:	Advanced Mobile Phone System
AMR:	Adaptive Multi-Rate
AMR-WB:	Adaptive Multi-Rate Wideband
API:	Application Programming Interface
CBRS:	Citizens Broadband Radio Service
CDMA:	Code Division Multiple Access
CIP:	Critical Infrastructure Protection
DAC:	Digital to Analog Converter
DIY:	Do-It-Yourself
ENB:	Evolved Node B
EPC:	Evolved Packet Core
E-UTRAN:	Evolved Universal Terrestrial Radio Access Network
FCC:	Federal Communications Commission
FDMA:	Frequency-Division Multiple Access
GPRS:	General Radio Packet System
GPS:	Global Positioning System
GSM:	Global System for Mobile Communications
HD:	High-definition
HSS:	Home Subscriber Server
IDC:	International Data Corporation
IETF:	Internet Engineering Task Force
IF:	Intermediate Frequency
IMEI:	International Mobile Equipment Identifier
IMS:	IP Multimedia Subsystem
IMSI:	International Mobile Subscriber Identity
IoT:	Internet of Things
IP:	Internet Protocol
LAS-CDMA:	Large Area Synchronized Code-Division Multiple Access
LNA:	Low Noise Amplifier
LPWAN:	Low Power Wide Area Network
LTE:	Long Term Evolution
LTE:	Long Term Evolution
MBWA:	Mobile Broadband Wireless Access
MCC:	Mobile Country Code

MC-CDMA:	Multi-carrier code division multiple access,
ME:	Mobile equipment
MEMS:	Micro Electro-Mechanical Systems
MGCP:	Media Gateway Control Protocol/Megaco
MME:	Mobility Management Entity)
MMS:	Multimedia Messaging Services
MNC:	Mobile Network Code
Network-LMDS:	Local Multipoint Distribution System Network
NFC:	Near-field communication
NMT:	Nordic Mobile Telephone
OAI:	Open Air Interface
OFDM:	Orthogonal Frequency Division Multiplexing
OSS:	Open-Source Software
PAN:	Personal Area Network
PBX:	Private Branch exchange
PDN:	Packet Data Network
P-GW:	Packet Data Network Gateway
PIN:	Postal Index Code
QoS:	Quality of service
RF:	Radio Frequency
RFID:	Radio Frequency Identification
RTP:	Real-Time Transport Protocol
RTTP:	Real-Time Transport Protocol
SAS:	Spectrum Access System
SDN:	Software Distribution Network
SDR:	Software Define Radio
S-GW:	Serving Gateway
SIM:	Subscriber Identity Module
SIP:	Session Initiation Protocol
SIP:	Session Initiation Protocol
SMS:	Short Message Service.
SOA:	Service-Oriented Architecture
SR:	Software Radio
SRTP:	Secure Real-time Transport Protocol
TDMA:	Time Division Multiple Access
TETRA:	Terrestrial Trunked Radio
UAT:	User Acceptance Test
UE:	User Equipment
UICC:	Universal Integrated Circuit Card

UMTS:	Universal Mobile Telecommunications System
USRP:	Universal Software Radio Peripheral
UUID:	universal unique identifier
VOIP:	Voice over Internet Protocol
VoLTE:	Voice over Long-Term Evolution
Wi-Fi:	Wireless Fidelity
WiMAX:	Wireless Interoperability for Microwave Access
WLAN:	Wireless Local Area Network
WPAN:	Wireless Personal Area Network
WSN:	Wireless Sensor Network
WWW:	Wireless World Wide Web

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΔΙΑΤΡΙΒΗΣ	4
ΠΕΡΙΛΗΨΗ	5
ABSTRACT	6
ΕΥΧΑΡΙΣΤΙΕΣ	7
ΠΙΝΑΚΑΣ ΣΥΜΒΟΛΩΝ-ΑΚΡΩΝΥΜΙΩΝ-ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ	8
ΕΙΣΑΓΩΓΗ Αντικείμενο, ερευνητικά ερωτήματα και διάρθρωση της εργασίας	15
Σκοπός εργασίας	16
Αναγκαιότητα και σπουδαιότητα της εργασίας	16
Βασικά ερευνητικά ερωτήματα	17
Δομή εργασίας και μεθοδολογία.....	17
ΚΕΦΑΛΑΙΟ 1 Διαδίκτυο των Πραγμάτων (IoT), Κρίσιμα Δίκτυα Υποδομής (CI) και τεχνολογίες υποστήριξης	18
1.1 Το διαδίκτυο των πραγμάτων (IoT).....	18
1.2 Η αρχιτεκτονική του διαδικτύου των πραγμάτων (IoT).....	19
1.2.1 Επίπεδο ανίχνευσης	20
1.2.2 Επίπεδο δικτύου.....	21
1.2.3 Επίπεδο Υπηρεσίας	21
1.2.4 Επίπεδο διεπαφής.....	22
1.3 Οι τεχνολογίες του διαδικτύου των πραγμάτων (IoT).....	22
1.3.1 Radio Frequency Identification (RFID)	22
1.3.2 Wi-Fi	23
1.3.3 NFC	23
1.3.4 Internet Protocol (IP)	24
1.3.5 Bluetooth	24
1.3.6 Ασύρματα δίκτυα αισθητήρων (WSN).....	24
1.4 Οι εφαρμογές του διαδικτύου των πραγμάτων (IoT).....	25
1.4.1 Έξυπνο Σύστημα Κυκλοφορίας.	25
1.4.2 Έξυπνο Περιβάλλον.	26
1.4.3 Έξυπνο Σπίτι.	26
1.4.4 Έξυπνα νοσοκομεία (μελλοντική εφαρμογή).....	27
1.4.5 Έξυπνη γεωργία.	28
1.4.6 Έξυπνο Εμπόριο και Διαχείριση Εφοδιαστικής Αλυσίδας.....	28
1.5 Κρίσιμα δίκτυα υποδομών (Critical Infrastructure Networks)	29

1.5.1. Παραδείγματα κρίσιμων δικτύων υποδομής.....	30
1.5.2 Απαιτήσεις δικτύων κρίσιμων υποδομών	31
1.6 Τεχνολογίες υποστήριξης δικτύων κρίσιμων υποδομών.	32
1.6.1 Συστήματα επικοινωνίας.....	32
1.6.2 Ασύρματα συστήματα επικοινωνίας.....	33
1.6.2.1 Κίνδυνοι και προκλήσεις στα ασύρματα συστήματα επικοινωνίας.....	34
ΚΕΦΑΛΑΙΟ 2 Δίκτυα επικοινωνιών, κινητής τηλεφωνίας, ασύρματων αισθητήρων (WSN) και εφαρμογές.....	35
2.1 Δίκτυα επικοινωνιών	35
2.1.1 Δημόσια δίκτυα επικοινωνιών.....	35
2.1.2 Ιδιωτικά δίκτυα επικοινωνιών	35
2.2 Δίκτυα κινητής τηλεφωνίας.....	36
2.2.1 Δίκτυα 1ης γενιάς.....	37
2.2.2 Δίκτυα 2ης γενιάς.....	37
2.2.3 Δίκτυα 3ης γενιάς.....	37
2.2.4 Δίκτυα 4ης γενιάς.....	37
2.2.5 Δίκτυα 5ης Γενιάς	38
2.2.6 Σύγκριση γενναίων κινητής τηλεφωνίας.	38
2.2.7 Υλοποίηση με LTE ή WiMAX;.....	39
2.3 Δίκτυα ασύρματων αισθητήρων	39
2.3.1 Είδη ασύρματων αισθητήρων.....	40
2.3.2 Αισθητήρες επιφάνειας.....	40
2.3.3 Αισθητήρες υπεδάφους.....	41
2.3.4 Κινητοί αισθητήρες	42
2.3.5 Υποθαλάσσιοι αισθητήρες.....	42
2.4 Εφαρμογές στα ασύρματα δίκτυα αισθητήρων	43
2.4.1 The Macroscopic of Redwood	43
2.4.2 Εφαρμογές σε εργοστάσια και πετρελαιοφόρα	43
2.4.3 Εφαρμογές υποθαλάσσιας παρακολούθησης.....	44
2.4.4 Εφαρμογές παρακολούθησης ηφαιστείων.....	44
2.5 Ασύρματα δίκτυα αισθητήρων για προστασία κρίσιμων υποδομών	44
ΚΕΦΑΛΑΙΟ 3 Ιδιωτικά δίκτυα, εφαρμογές, πλατφόρμες ανοιχτού κώδικα και υλοποιήσεις	46
3.1 Ιδιωτικά δίκτυα	46
3.2 Τεχνολογίες σε ιδιωτικά δίκτυα	47
3.2.1 LPWAN.....	47
3.2.2 Αρχιτεκτονική δομή και τοπολογία του LPWAN.....	47

3.2.3 SDN	48
3.3.3 SD_WAN	49
3.3.3.1 Αρχιτεκτονική του SD_WAN	49
3.3.4 LTE	50
3.3.4.1 Αρχιτεκτονική του LTE.....	51
3.3.4.2 Ασφάλεια του LTE	53
3.3.5 CBRS	54
3.4 Εφαρμογές	55
3.4.1 VoIP	55
3.4.2 Αρχιτεκτονική του VoIP	56
3.4.3 Κλήσεις φωνής VoLTE (Voice over LTE)	57
3.4.4 Το Asterisk ως μέσω επικοινωνίας στο VoIP	59
3.4.4.1 Υλοποίηση εγκατάστασης του Asterisk	60
3.5 Πλατφόρμες ανοιχτού κώδικα για υλοποιήσεις	60
3.5.1 Πλατφόρμες ανοιχτού κώδικα για υλοποιήσεις	60
3.5.2 Πλατφόρμες ανοιχτού και ελεύθερου λογισμικού	61
3.5.2.1 OmneT++	61
3.5.2.2 MATLAB	62
3.5.2.3 OAI	62
3.6 Η τεχνολογία SDR για χρήση σε Open Source Platform	63
3.6.1 Η ιστορία του SDR.....	63
3.6.2 Αρχές λειτουργίας του SDR.....	64
3.6.3 Το SDR B210.....	65
3.6.4 Αναλυτικός πίνακας των USRPs SDR	66
ΚΕΦΑΛΑΙΟ 4 Υλοποίηση	68
4.1 Αρχιτεκτονική δομή του ιδιωτικού δικτύου	68
4.2 Εξοπλισμός eNB.....	69
4.2.1 Λειτουργικό eNB	70
4.2.2 Διαχείριση ισχύος και εγκατάσταση Low Latency Kernel στο eNB.....	70
4.3 Παραμετροποίηση του eNB	73
4.4 Εξοπλισμός του EPC	78
4.4.1 Λειτουργικό EPC.....	78
4.4.2 XZ utils.....	79
4.4.3. Εγκατάσταση Generic Kernel, ενεργοποίηση GPRS protocol, ηproc.....	80
4.5 Παραμετροποίηση του EPC.....	82
4.5.1 Ορισμός FQDN εγκατάσταση βάσης δεδομένων.	82

4.6 Προετοιμασία του Asterisk Server	90
4.6.1 Λειτουργικό του Asterisk Server.....	90
4.6.2 Υλοποίηση και παραμετροποίηση του Asterisk.....	92
4.6.3 Εγκατάσταση του Client στα UEs.....	92
4.7 Προγραμματισμός Καρτών UICC	94
4.8 Δοκιμές	96
4.8.1 (1 ^η) Δοκιμή δικτύου, χωρίς UEs	97
4.8.2 (2 ^η) Δοκιμή δικτύου με χρήση 2 UEs	98
4.8.3 (3 ^η) Δοκιμή δικτύου με χρήση 2 UEs και κλήση εντός δικτύου.	102
ΚΕΦΑΛΑΙΟ 5 Σύνοψη Συμπεράσματα – Προβλήματα και αντιμετώπιση– Εφαρμογές– Προτάσεις εξέλιξης	104
Σύνοψη Συμπεράσματα.....	104
Προβλήματα και αντιμετώπιση	104
Εφαρμογές.....	105
Μελλοντικές εξελίξεις	106
ΒΙΒΛΙΟΓΡΑΦΙΑ - ΠΗΓΕΣ	107
ΠΑΡΑΡΤΗΜΑΤΑ.....	114
Παράρτημα Α: Κώδικας eNB.....	114
Παράρτημα Β: Κώδικας EPC.....	116
Παράρτημα Γ: Κώδικας Asterisk.....	118
Παράρτημα Δ: Κώδικας UICC SIM Cards	120
Παράρτημα Ε: Εικόνες.....	121

Με τις κρίσιμες υποδομές να αποτελούν ένα πολύ σημαντικό παράγοντα στην λειτουργία μιας χώρας, υπάρχει μεγάλη ανάγκη για καθημερινή παρακολούθησης τους σε 24ωρη βάση μέσα από κατάλληλα διαμορφωμένα συστήματα, ώστε να προλαμβάνεται ο οποιοσδήποτε κίνδυνος τόσο για την ασφάλεια των πολιτών όσο για την έγκαιρη ενημέρωσή τους. Ένα δίκτυο κρίσιμης υποδομής αποτελούμενο από διάφορους πόρους φυσικούς και μη, κατά την διακοπή υπηρεσιών του μπορεί να προκαλέσει αρκετές και σε πολλές περιπτώσεις σοβαρές επιπτώσεις σε θέματα που άπτονται στην ασφάλεια την δημόσια υγεία ακόμα στην κατάλυση βασικών καθημερινών εργασιών. Με την συνεχόμενη αύξηση του πληθυσμού, οι βασικές και καθημερινές υπηρεσίες όπως παροχή ηλεκτρικής ενέργειας, νερού, φυσικού αερίου και άλλων αγαθών ταξινομούνται σε κατηγορίες και προστίθενται σε λίστες κρίσιμων υποδομών. Για να υπάρξει μια κατηγοριοποίηση σε αυτές τις λίστες έχουν δημιουργηθεί τα κρίσιμα δίκτυα υποδομών (ΚΔΥ). Ενδεικτικά θα μπορούσαμε να αναφέρουμε τα δίκτυα ενέργειας, πληροφορία της τεχνολογίας, νοσοκομείου και δημόσιας υγείας, ακόμα και τα δίκτυα εθνικής άμυνας. Ωστόσο η διακοπή των υπηρεσιών αυτών μπορεί να οφείλεται όχι μόνο από φυσικές καταστροφές αλλά και από τρομοκρατικές επιθέσεις. Η προστασία τους απαιτεί μηχανισμούς παρακολούθησης και πρόβλεψης το συντομότερο δυνατό, με κύριες απαιτήσεις την διαθεσιμότητα, συντήρηση, ανάλυση, και σε περιπτώσεις που χρήζει ανάγκη αναβάθμιση.

Με την έλευση του Industry 4.0 και την “ψηφιοποίηση” των κλασσικών παραδοσιακών πόλεων σε “έξυπνες”, κρίνεται ταυτόχρονα απαραίτητη η δημιουργία και η μεταβίβαση σε ένα σύστημα αδιάληπτης και καθημερινής παρακολούθησης των ΚΔΥ της σε 24ωρη βάση όλο το χρόνο. Το διαδίκτυο των πραγμάτων (IoT) που είναι απόλυτα συνυφασμένο με τις έννοιες του Industry 4.0 και της έξυπνης πόλης μπορεί να δημιουργήσει μέσα από τις κατάλληλες εφαρμογές και τις τεχνολογίες του την δυνατότητα τέτοιων συστημάτων παρακολούθησης στα ΚΔΥ. Αναφορικά να πούμε ότι το δίκτυο ασύρματων αισθητήρων (WSN) είναι ένα σύστημα αποτελούμενο από “έξυπνους” αισθητήρες που μπορούν να προβλέψουν τις αλλαγές στα ΚΔΥ, να αποθηκεύσουν πληροφορίες για ένα χρονικό διάστημα, και να στείλουν δεδομένα σε ένα κεντρικό σύστημα παρακολούθησης και αναφοράς.

Από την άλλη πλευρά τα δίκτυα κινητής τηλεφωνίας με την αλματώδη εξέλιξη τους από την 1^η γενιά στην 5^η δίνουν την δυνατότητα δημιουργίας ιδιωτικών δικτύων κινητής για την διαχείριση των WSN και των ΚΔΥ στις έξυπνες πόλεις. Ακόμα και σε περιπτώσεις όπου το δίκτυο κινητής ή το Internet λόγω κάποιου κρίσιμου γεγονότος, όπως σεισμού πυρκαγιάς ή πλημύρας το σύστημα που είναι εντελώς αυτόνομο μπορεί να λάβει τις πληροφορίες από τους αισθητήρες να τις αποθηκεύσει σε τοπικούς Servers, και δώσει την δυνατότητα κλήσεων εντός του δικτύου σε εγγεγραμμένους χρήστες.

Η εργασία έχει ως σκοπό να δημιουργήσουμε ένα ιδιωτικό δίκτυο κινητής τηλεφωνίας βασισμένο στην τεχνολογία του LTE, εντός του οποίου θα μπορούν να πραγματοποιούνται κλήσεις μεταξύ των εγγεγραμμένων συνδρομητών. Η συγκεκριμένη υλοποίηση θα δώσει την δυνατότητα διαχείρισης κρίσιμων δικτύων υποδομών μέσω ασύρματων δικτύων

Μεταπτυχιακή Διπλωματική Εργασία, Σπυρίδων Παπαγιάκουμος, AM msciot20005 15

αισθητήρων, θα υποστηρίξει κλήσεις φωνής όπου δεν μπορεί να καλυφθεί από τα δημόσια δίκτυα κινητής τηλεφωνίας.

Σκοπός εργασίας

Σύμφωνα με την επιστημονική άποψη του άρθρου [1] η συνεχιζόμενη ανάπτυξη των ευφυών ασυρμάτων δικτύων αισθητήρων στο διαδίκτυο των πραγμάτων IOT για έξυπνες εφαρμογές συλλογής πληροφοριών, την πρόληψη σε ασθενείς με προβλήματα υγείας [2], αλλά και την ανάγκη αδιάληπτης επικοινωνίας σε κρίσιμες υποδομές [3] να δημιουργεί την ανάγκη ανάπτυξης ιδιωτικών LTE δικτύων προς την καλύτερη διαχείριση των παραπάνω αναγκών. Η ανάπτυξη και υλοποίηση τους, είναι απαραίτητη για να παρέχει εξατομικευμένες λύσεις, βελτιωμένης ασφάλειας και αξιοπιστία κάλυψης σε δύσκολα περιβάλλοντα, ενεργοποίηση έξυπνων απομακρυσμένων συσκευών, έλεγχο της υποδομής του δικτύου και συμμόρφωση με τις κανονιστικές απαιτήσεις. Αυτά τα δίκτυα προσφέρουν την ευελιξία, τον έλεγχο και την απόδοση που απαιτούνται για τις συγκεκριμένες εφαρμογές και λειτουργικές ανάγκες τους. Αξίζει να σημειωθεί ότι η δημιουργία ενός ιδιωτικού δικτύου LTE με SDR απαιτεί ειδίκευση στη μηχανική της ραδιοσυχνότητας, την ανάπτυξη λογισμικού και τα ασύρματα δίκτυα. Είναι απαραίτητο να ληφθούν υπόψη παράγοντες όπως η διαθεσιμότητα του φάσματος, η συμμόρφωση με τη νομοθεσία, ο κατάλληλος σχεδιασμός αυτού του δικτύου και η ενσωμάτωση με την υπάρχουσα υποδομή κατά την ανάπτυξη ενός ιδιωτικού δικτύου LTE με χρήση SDR.

Αναγκαιότητα και σπουδαιότητα της εργασίας

Σύμφωνα με την επιστημονική άποψη του άρθρου [1] η συνεχιζόμενη ανάπτυξη των ευφυών ασυρμάτων δικτύων αισθητήρων στο διαδίκτυο των πραγμάτων IOT για έξυπνες εφαρμογές συλλογής πληροφοριών, την πρόληψη σε ασθενείς με προβλήματα υγείας [2], αλλά και την ανάγκη αδιάληπτης επικοινωνίας σε κρίσιμες υποδομές [3] να δημιουργεί την ανάγκη ανάπτυξης ιδιωτικών LTE δικτύων προς την καλύτερη διαχείριση των παραπάνω αναγκών. Η ανάπτυξη και υλοποίηση τους, είναι απαραίτητη για να παρέχει εξατομικευμένες λύσεις, βελτιωμένης ασφάλειας και αξιοπιστία κάλυψης σε δύσκολα περιβάλλοντα, ενεργοποίηση έξυπνων απομακρυσμένων συσκευών, έλεγχο της υποδομής του δικτύου και συμμόρφωση με τις κανονιστικές απαιτήσεις. Αυτά τα δίκτυα προσφέρουν την ευελιξία, τον έλεγχο και την απόδοση που απαιτούνται για τις συγκεκριμένες εφαρμογές και λειτουργικές ανάγκες τους. Αξίζει να σημειωθεί ότι η δημιουργία ενός ιδιωτικού δικτύου LTE με SDR απαιτεί ειδίκευση στη μηχανική της ραδιοσυχνότητας, την ανάπτυξη λογισμικού και τα ασύρματα δίκτυα. Είναι απαραίτητο να ληφθούν υπόψη παράγοντες όπως η διαθεσιμότητα του φάσματος, η συμμόρφωση με τη νομοθεσία, ο κατάλληλος σχεδιασμός αυτού του δικτύου και η ενσωμάτωση με την υπάρχουσα υποδομή κατά την ανάπτυξη ενός ιδιωτικού δικτύου LTE με χρήση SDR.

Βασικά ερευνητικά ερωτήματα

- ❖ Open-Source Code για ιδιωτικά LTE δίκτυα
 - Τι είναι το Open Source Code;
 - Μπορεί να παραμετροποιηθεί για LTE ιδιωτικά δίκτυα;
 - Ποια είναι η Open Air Interface;
- ❖ On premise LTE δίκτυο
 - Τι είναι το SDR;
 - Ποια είδη SDR υπάρχουν;
 - Ποια είναι τα τεχνικά χαρακτηριστικά του B210;
 - Πως μπορεί να υλοποιηθεί ένα On Premise LTE δίκτυο;
 - Πως γίνεται η επικοινωνία μέσω VoIP εντός του On Premise LTE δικτύου;
- ❖ Δίκτυα Έκτακτης ανάγκης
 - Τί είναι οι κρίσιμες υποδομές;
 - Πως διαφυλάσσεται η αδιάληπτη επικοινωνία σε τέτοια δίκτυα;
 - Πώς γίνεται η επικοινωνία εντός των δικτύων έκτακτης ανάγκης;
- ❖ Τεχνολογίες για εφαρμογές IoT στα δίκτυα έκτακτης ανάγκης;
- ❖ Που μπορεί να χρησιμοποιηθεί η συγκεκριμένη υλοποίηση

Δομή εργασίας και μεθοδολογία.

Στο πρώτο κεφάλαιο γίνεται μια ανάλυση του ορισμού Κρίσιμο Δίκτυο Υποδομών και πως μέσα από την τεχνολογία του διαδικτύου των αντικειμένων και των εφαρμογών, να μπορούν αυτά τα δίκτυα να υποστηριχθούν για συνεχή εποπτεία και λειτουργία.

Στο δεύτερο κεφάλαιο γίνεται μια τεχνολογική αναδρομή στα δίκτυα κινητής τηλεφωνίας και την εξέλιξή τους μέσα στα χρόνια λειτουργίας τους, ενώ αναλύουμε πως τα ασύρματα δίκτυα αισθητήρων μπορούν να καλύψουν τις ανάγκες κρίσιμων υποδομών.

Στο τρίτο κεφάλαιο κάνουμε μια πλήρη αναφορά στις δυνατότητες ενός ιδιωτικού δικτύου κινητής τηλεφωνίας τις εφαρμογές που μπορούν να υλοποιηθούν μέσα σε αυτό καθώς και τις πλατφόρμες που υποστηρίζουν μια τέτοια υλοποίηση.

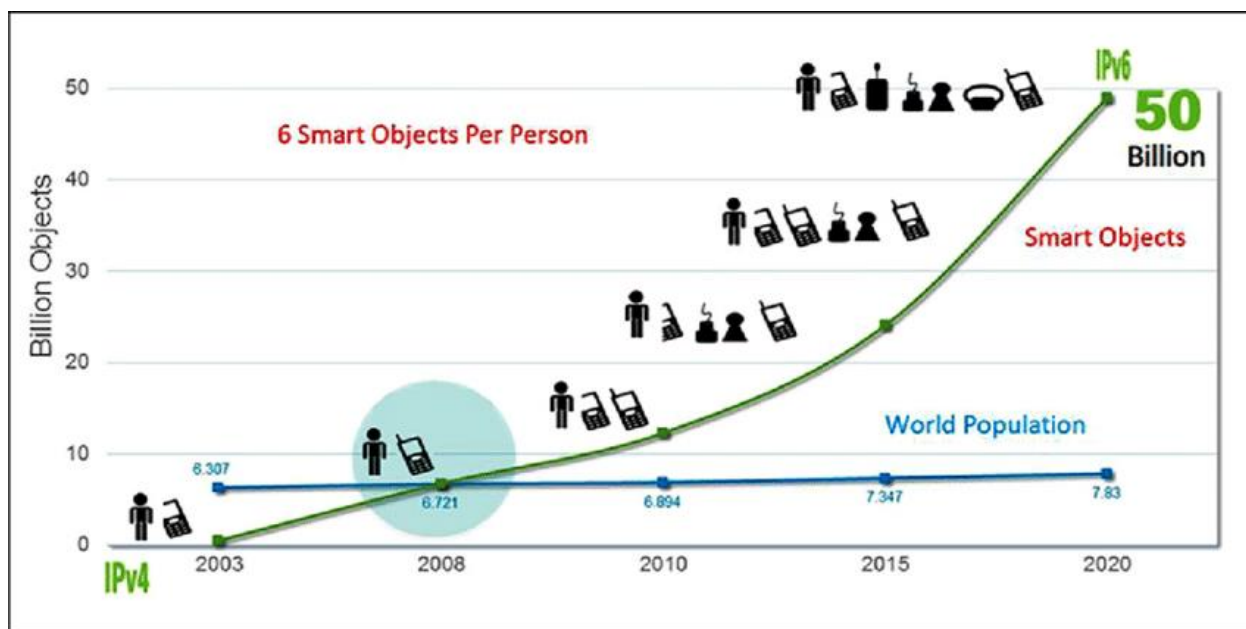
Στο τέταρτο και τελευταίο κεφάλαιο υλοποιούμε το ιδιωτικό δίκτυο LTE με χρήση της τεχνολογίας SDR και του USRP B210, της Ettus Research, το οποίο προγραμματίζουμε κατάλληλα μέσω του ανοιχτού κώδικα και λογισμικού της Open Air Interface. Τέλος χρησιμοποιούμε ένα Raspberry pi 4 με 8GB Ram, ως Server με το ανοιχτό λογισμικό Asterisk ώστε να πραγματοποιήσουμε κλήσεις μεταξύ 2 εγγεγραμμένων συνδρομητών του δικτύου, με χρήση Smart Phone τηλεφώνων και την βοήθεια του ελεύθερου λειτουργικού Mizudroid

ΚΕΦΑΛΑΙΟ 1

Διαδίκτυο των Πραγμάτων (IoT), Κρίσιμα Δίκτυα Υποδομής (CI) και τεχνολογίες υποστήριξης

1.1 Το διαδίκτυο των πραγμάτων (IoT)

Με τη συνεχή πρόοδο της τεχνολογίας, μια καινοτομία που έχει αλλάξει τον κόσμο από το 2012 και κινείται με πολύ γρήγορους ρυθμούς είναι το διαδίκτυο των πραγμάτων IoT, το οποίο έχει αναπτυχθεί ως ένας πανταχού παρών παγκόσμιος δικτυακός υπολογιστής αφού όλοι και τα πάντα μπορούν να συνδεθούν με το Internet [4]. Το IoT εξελίσσεται συνεχώς και αποτελεί ένα ισχυρό και άκρος ενδιαφέρον πεδίο έρευνας με απεριόριστες ευκαιρίες επαγγελματικής εξέλιξης. Υπάρχει αυξανόμενη χρήση των συσκευών που χρησιμοποιούν τις υπηρεσίες του Internet καθημερινά. Από τις αρχές του 2010 μέχρι και το 2020 σε κάθε χρήστη αντιστοιχούν 6 συσκευές, αριθμός οποίος και συνεχώς αλλάζει.

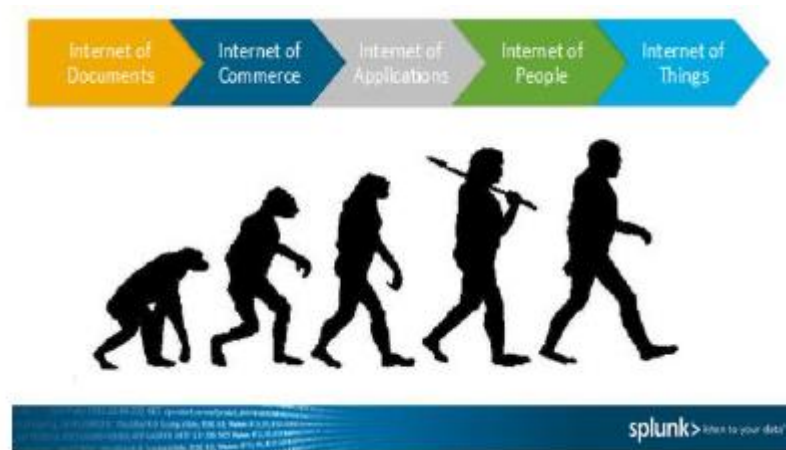


Εικόνα 1. Η αλματώδης εξέλιξης διασύνδεσης συσκευών στο δίκτυο του IoT [F1]

Η έννοια της δυνατότητας αλληλεπίδρασης μεταξύ έξυπνων μηχανών είναι μια πρωτοποριακή τεχνολογία, αλλά οι τεχνολογίες που συνθέτουν το IoT δεν είναι κάτι καινούργιο για εμάς [5]. Η βασική ιδέα του IoT είναι να επιτρέπει την αυτόνομη ανταλλαγή χρήσιμων πληροφοριών διαφορετικών συσκευών του πραγματικού κόσμου γύρω μας, με την

χρήση κορυφαίων τεχνολογιών όπως το Radio Frequency Identification – RFID (η Ταυτοποίηση με Ραδιοσυχνότητα) και τα Wireless Sensor Network (Ασύρματα Δίκτυα Αισθητήρων) [5], τα οποία ανιχνεύονται από τις αισθητήριες συσκευές και επεξεργάζονται περαιτέρω για τη λήψη αποφάσεων, βάσει των οποίων πραγματοποιείται μια αυτοματοποιημένη ενέργεια [4]. Ο Kevin Ashton που ήταν ο πρώτος που πρότεινε την έννοια του IoT το 1999, το ορίζει ως μια παγκόσμια δυναμική υποδομή βασισμένη σε πρότυπα και πρωτόκολλα επικοινωνίας [6]. Μελετώντας την εξέλιξη του διαδικτύου (Internet) στο πέρασμα των χρόνων μπορεί κανείς να διαπιστώσει τις 5 διαφορετικές φάσεις:

1. Διαδίκτυο βασισμένο στα έγγραφα, ηλεκτρονικές βιβλιοθήκες, και ιστοστοχώροι που περιλαμβάνουν έγγραφα.
2. Διαδίκτυο Εμπορίου - ηλεκτρονικό εμπόριο βασισμένο στην ηλεκτρονική τραπεζική και αγοροπωλησίες μετοχών.
3. Διαδίκτυο Εφαρμογών - Διαδίκτυο 2.0
4. Διαδίκτυο Ανθρώπων – πολλά μέσα κοινωνικής δικτύωσης.
5. Διαδίκτυο Πραγμάτων και αντικειμένων - συνδεδεμένες συσκευές και μηχανές που επικοινωνούν μεταξύ τους.



Εικόνα 2. Εξέλιξη του διαδικτύου (Internet) [6]

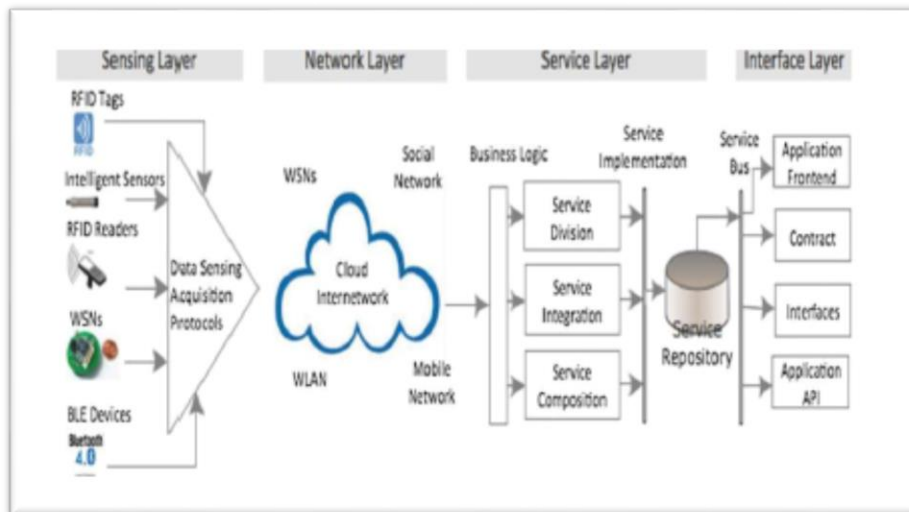
1.2 Η αρχιτεκτονική του διαδικτύου των πραγμάτων (IoT)

Ένα πολύ σημαντικό στοιχείο του Διαδικτύου των Πραγμάτων (IoT) είναι η διασύνδεση των πραγμάτων στο δίκτυο. Η αρχιτεκτονική δομή του συστήματος για IoT εξασφαλίζει τη λειτουργική γέφυρα ανάμεσα στον φυσικό κόσμο και τον εικονικό. Ο σχεδιασμός της αρχιτεκτονικής του είναι πολύ πολύ-παραγοντικός, αφού περιλαμβάνει δίκτυα, επικοινωνία, επιχειρηματικά μοντέλα διαδικασίες, και ασφάλεια. Καθ' όλη την σχεδίαση της αρχιτεκτονικής αυτής, πρέπει να λαμβάνονται υπόψη η επεκτασιμότητα, η κλιμάκωση και η αλληλεπίδραση μεταξύ ασυμβίβαστων συσκευών και μοντέλων. Εξ αιτίας του γεγονότος ότι τα αντικείμενα μπορεί να μετακινούνται με φυσικό τρόπο και να αλληλοεπιδρούν σε πραγματικό χρόνο, η αρχιτεκτονική του IoT πρέπει να είναι προσαρμόσιμη για να καθιστά ικανές τις συσκευές να αλληλοεπιδρούν με άλλα δυναμικά πράγματα και να υποστηρίζει την ορθή επικοινωνία [6]. Το SoA είναι ένα σύστημα ως ένα σύνολο υποσυστημάτων. Αυτά τα υποσυστήματα μπορούν να επαναχρησιμοποιηθούν και διατηρούνται ξεχωριστά. Επομένως, τα λογισμικά και τα υλικά στοιχεία σε ένα Διαδίκτυο των Πραγμάτων (IoT) μπορούν να επαναχρησιμοποιηθούν και να αναβαθμιστούν αποτελεσματικά. Λόγω αυτών των πλεονεκτημάτων, η Αρχιτεκτονική Υπηρεσιών έχει ευρεία εφαρμογή ως κύρια αρχιτεκτονική.

Μεταπτυχιακή Διπλωματική Εργασία, Σπυρίδων Παπαγιάκουμος, AM msciot20005

Η Αρχιτεκτονική Υπηρεσιών αποτελείται από τέσσερα επίπεδα με διακριτές λειτουργίες, και παρέχει τη διαχείριση μεταξύ των συσκευών με πολλούς τρόπους. Αυτά τα επίπεδα είναι:

1. **Επίπεδο ανίχνευσης:** Ενσωματώνεται τα διαθέσιμα αντικείμενα (πράγματα) για να ανιχνεύσει την κατάστασή τους.
2. **Επίπεδο δικτύου:** Είναι η υποδομή που υποστηρίζει τις ασύρματες ή ενσύρματες συνδέσεις μεταξύ των πραγμάτων.
3. **Επίπεδο υπηρεσίας:** Δημιουργεί και διαχειρίζεται τις απαιτούμενες υπηρεσίες των χρηστών ή των εφαρμογών.
4. **Επίπεδο διεπαφής:** Αποτελείται από τις μεθόδους που αλληλοεπιδρούν οι χρήστες ή οι εφαρμογές.



Εικόνα 3. Η αρχιτεκτονική του IoT [6]

1.2.1 Επίπεδο ανίχνευσης

Στο επίπεδο ανίχνευσης, οι αισθητήρες μπορούν να ανιχνεύουν αυτόματα το περιβάλλον και να ανταλλάσσουν δεδομένα μεταξύ των συσκευών.. Κάθε αντικείμενο στο Διαδίκτυο των Πραγμάτων κατέχει μια ψηφιακή ταυτότητα και μπορεί να ανιχνευθεί εύκολα στον ψηφιακό χώρο. Η τεχνική της ανάθεσης μοναδικής ταυτότητας σε ένα αντικείμενο ονομάζεται UUID. Οι ταυτότητες αυτές μπορεί να περιέχουν ονόματα και διευθύνσεις. Ένα UUID είναι ένας 128 bit αριθμός που χρησιμοποιείται για τη μοναδική ταυτοποίηση ενός αντικειμένου ή οντότητας στο Διαδίκτυο. Κατά τον καθορισμό του επιπέδου ανίχνευσης, πρέπει να ληφθούν υπόψη τα παρακάτω στοιχεία:

1. **Μείωση κόστους, ελαχιστοποίηση κατανάλωσης ενέργειας και πόρων:** Τα αντικείμενα είναι εξοπλισμένα με κατάλληλους αισθητήρες. Λόγω του υψηλού αριθμού, σε ποσότητα, αισθητήρων οι εφαρμογές, και οι έξυπνες συσκευές θα πρέπει να είναι σχεδιασμένες κατάλληλα έτσι ώστε να μπορούν να ελαχιστοποιούν το κόστος και τους πόρους.
2. **Ανάπτυξη:** Τα αντικείμενα ανίχνευσης που είναι οι ετικέτες RFID, αισθητήρες και άλλα μπορούν να τοποθετηθούν μια φορά, ή αυξητικά, ή σε τυχαία σειρά αναλόγως των απαιτήσεων.

3. **Επικοινωνία:** Τα αισθητήρια θα πρέπει να μπορούν να ανιχνεύονται ώστε να είναι εύκολη η προσβασιμότητα τους
4. **Δίκτυο:** Τα αντικείμενα οργανώνονται ως κόμβοι με δυνατότητα μετάδοσης δεδομένων προς όλους (mesh) ή αδέσμευτα (ad hoc).

1.2.2 Επίπεδο δικτύου

Το επίπεδο δικτύου στο Διαδίκτυο των Πραγμάτων συνδέει όλα τα αντικείμενα και τους επιτρέπει να γνωρίζουν το περιβάλλον τους. Στο επίπεδο του δικτύου, τα αντικείμενα μοιράζονται μεταξύ τους δεδομένα με τα συνδεδεμένα πράγματα, κάτι που είναι αρκετά κρίσιμο για την έξυπνη επεξεργασία και διαχείριση των γεγονότων στο Διαδίκτυο των Πραγμάτων. Για την κοινή χρήση δεδομένων και την παροχή υπηρεσιών από μια συσκευή, είναι απαραίτητο ένα ισχυρό δίκτυο. Το δίκτυο πρέπει επίσης να ανακαλύπτει και να χαρτογραφεί αυτόματα τα πράγματα. Ανατίθενται ρόλοι αυτόματα για την ανάπτυξη, διαχείριση και προγραμματισμό της συμπεριφοράς των πραγμάτων και πρέπει να είναι σε θέση να μεταβαίνουν σε οποιονδήποτε ρόλο ανά πάσα στιγμή κατά την απαίτηση. Αυτό επιτρέπει στις συσκευές να εκτελούν καθήκοντα συνεργατικά. Στο επίπεδο δικτύου, πρέπει να αντιμετωπιστούν τα εξής θέματα:

1. **Τεχνολογίες διαχείρισης δικτύου:** διαχείριση σταθερών και ασύρματων κινητών δικτύων.
2. Απαιτήσεις ποιότητας υπηρεσιών: (QoS).
3. **Τεχνολογίες αναζήτησης δεδομένων:** επεξεργασία δεδομένων.
4. **Ασφάλεια και ιδιωτικότητα.**

1.2.3 Επίπεδο Υπηρεσίας

Το επίπεδο υπηρεσιών περιέχει υπηρεσίες και του Διαδικτύου των Πραγμάτων και Αποτελεί μια οικονομικά αποδοτική πλατφόρμα, όπου το λογισμικό και το υλικό μπορούν να επαναχρησιμοποιηθούν. Στο επίπεδο αυτό οι υπηρεσίες εκτελούνται απευθείας στο δίκτυο για τον εντοπισμό αποτελεσματικών νέων υπηρεσιών για μια εφαρμογή ώστε να ανακτηθούν δυναμικά τα δεδομένα σχετικά με τις υπηρεσίες. Οι περισσότερες προδιαγραφές υποστηρίζονται από διάφορα πρότυπα που αναπτύχθηκαν από διάφορους οργανισμούς. Ένα παγκοσμίως αποδεκτό και πρακτικό επίπεδο υπηρεσιών αποτελείται από ένα ελάχιστο σύνολο εφαρμογών διεπαφής, προγραμματισμένων εφαρμογών APIs και πρωτοκόλλων απ' όπου εφαρμογές και υπηρεσίες υποστηρίζονται από αυτά. Δραστηριότητες που αφορούν τις ανταλλαγές και αποθήκευση πληροφορίας, δεδομένα διαχείρισης, ή μηχανές αναζήτησης, πραγματοποιούνται σε αυτό το επίπεδο. Οι κύριες εργασίες που εκτελούνται στο επίπεδο υπηρεσιών είναι οι εξής:

1. **Ανακάλυψη υπηρεσιών:** Εντοπίζουν τα αντικείμενα που μπορούν να παρέχουν την απαιτούμενη υπηρεσία και πληροφορίες με αποτελεσματικό τρόπο.
2. **Σύνθεση υπηρεσιών:** Η αλληλεξάρτηση μεταξύ των συνδεδεμένων πραγμάτων περιγράφει τις σχέσεις μεταξύ τους για την επίτευξη της επιθυμητής υπηρεσίας.
3. **Διεπαφές υπηρεσιών (APIs):** Παρέχουν τη διεπαφή μεταξύ των υπηρεσιών κάτω από τις απαιτήσεις των χρηστών.

1.2.4 Επίπεδο διεπαφής

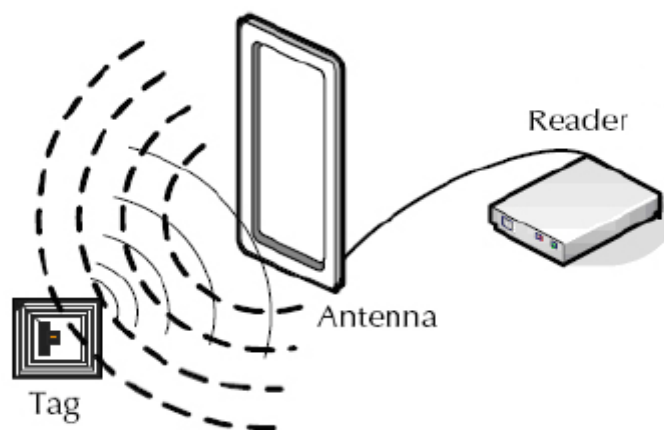
Στο IoT, ένας μεγάλος αριθμός συνδεδεμένων συσκευών, ανήκει σε διάφορα άτομα οπότε δεν έχουν πάντα ίδιας μορφής πρότυπα. Το θέμα της ασυμβατότητας μεταξύ των αντικειμένων θα πρέπει να επιλυθεί για την αλληλεπίδραση μεταξύ των πραγμάτων. Η συμβατότητα συνδέεται με την μεταφορά πληροφοριών, την επικοινωνία και την διαχείριση γεγονότων. Κρίνεται αναγκαίος ένας αποτελεσματικός μηχανισμός διεπαφής για την απλοποίηση της επεξεργασίας και της αλληλεπίδρασης των πραγμάτων. Το επίπεδο διεπαφής λειτουργεί στο frontend των εφαρμογών ή στο API

1.3 Οι τεχνολογίες του διαδικτύου των πραγμάτων (IoT)

Οι κύριες τεχνολογίες του Διαδικτύου των Πραγμάτων περιλαμβάνουν την τεχνολογία RFID, την τεχνολογία αισθητήρων, τη νανοτεχνολογία και την τεχνολογία ενσωματωμένης νοημοσύνης. Ανάμεσά τους, η τεχνολογία RFID αποτελεί τη βάση και τον πυρήνα δικτύωσης για την κατασκευή του IoT, αφού επέτρεψε στους χρήστες να φέρουν φυσικά αντικείμενα στον κόσμο του κυβερνοχώρου. Αυτό έγινε δυνατό μέσω διαφορετικών τεχνολογιών όπως NFC, RFID και 2D barcode που επέτρεψαν την αναγνώριση και αναφορά φυσικών αντικειμένων στο διαδίκτυο. Το IoT, το οποίο είναι συνυφασμένο με την τεχνολογία αισθητήρων και την τεχνολογία ραδιοσυχνοτήτων, είναι το πανταχού παρόν δίκτυο βασισμένο στους ανεξάντλητους υλικούς πόρους του Διαδικτύου και αποτελεί τα αντικείμενα του Διαδικτύου. Αποτελεί επίσης ένα νέο κύμα της βιομηχανικής τεχνολογίας και πληροφορικής, καθώς έχουν εφαρμοστεί τεχνολογίες υπολογιστών, δικτύωσης. Εκτός από τις προηγμένες τεχνολογίες υπολογιστών και δικτύωσης, περιλαμβάνει επίσης πολλές νέες υποστηρικτικές τεχνολογίες του Διαδικτύου των Πραγμάτων, όπως η τεχνολογία συλλογής πληροφοριών (Data Collection), η τεχνολογία απομακρυσμένης επικοινωνίας (Remote Communication), η τεχνολογία απομακρυσμένης μετάδοσης πληροφοριών (Remote Data Transfer) [7].

1.3.1 Radio Frequency Identification (RFID)

Η αναγνώριση με ραδιοσυχνότητα (RFID) είναι ένα σύστημα που μεταδίδει ασύρματα την ταυτότητα ενός αντικειμένου ή προσώπου χρησιμοποιώντας ραδιοκύματα σε μορφή σειριακού αριθμού. Η πρώτη χρήση της συσκευής RFID έγινε κατά τον Β' Παγκόσμιο Πόλεμο στη Βρετανία και χρησιμοποιήθηκε για την αναγνώριση συμμάχου ή εχθρού το 1948.. Η τεχνολογία RFID παίζει σημαντικό ρόλο στο IoT για την επίλυση ζητημάτων αναγνώρισης των αντικειμένων. Η τεχνολογία κατατάσσεται σε τρεις κατηγορίες βάση της μεθόδου παροχής ενέργειας: 1) ενεργή RFID, 2) παθητική RFID και 3) ημι-ενεργή RFID. Οι βασικές συνιστώσες του RFID είναι ο αναγνώστης, η κεραία, ο ελεγκτής πρόσβασης, το λογισμικό και ο διακομιστής. Η τεχνολογία RFID είναι η πιο αξιόπιστη, αποδοτική, ασφαλής, οικονομική και ακριβής αφού έχει μια ευρεία γκάμα ασύρματων εφαρμογών όπως διανομή, παρακολούθηση ασθενών, στρατιωτικές εφαρμογές κ.λπ.



Εικόνα 4. Λειτουργία RFID [4]

1.3.2 Wi-Fi

Το Wi-Fi αποτελεί μια τεχνολογία δικτύωσης τον κόσμο των υπολογιστών αλλά και σε άλλες συσκευές να επικοινωνούν μέσω ενός ασύρματου σήματος. Η αρχή του Wi-Fi ξεκίνησε το 1991 από την εταιρεία NCR Corporation στην περιοχή Nieuwege στην Ολλανδία. Τα πρώτα ασύρματα προϊόντα δόθηκαν στην αγορά υπό την ονομασία WaveLAN με ταχύτητες από 1 Mbps έως 2 Mbps. Σήμερα, υπάρχει σχεδόν διαδεδομένο το WiFi και παρέχει υψηλή ταχύτητα ασύρματης σύνδεσης σε εκατομμύρια γραφεία, σπίτια και δημόσιες τοποθεσίες όπως ξενοδοχεία, καφετέριες και αεροδρόμια. Η ένταξη του WiFi σε φορητούς υπολογιστές, φορητές συσκευές και κινητά έχει επιταχύνει την υιοθέτηση του WiFi μέχρι το σημείο που σχεδόν αποτελεί προεπιλογή σε αυτές τις συσκευές. Η τεχνολογία περιλαμβάνει οποιοδήποτε είδος προϊόντος ασύρματου δικτύου WLAN που υποστηρίζει οποιαδήποτε από τις IEEE 802.11, συμπεριλαμβανομένων των διπλής ζώνης, 802.11a, 802.11b, 802.11g και 802.11n. Σήμερα, ολόκληρες πόλεις μετατρέπονται σε διάδρομους WiFi μέσω ασύρματων σημείων πρόσβασης.

1.3.3 NFC

Είναι ένα σύνολο τεχνολογιών ασύρματης επικοινωνίας σε κοντινή απόσταση στα 13,56 MHz, που συνήθως απαιτεί απόσταση 4 εκατοστών. Η τεχνολογία NFC διευκολύνει τους καταναλωτές σε ολόκληρο τον κόσμο, καθιστώντας απλούστερες τις συναλλαγές, την ανταλλαγή ψηφιακού περιεχομένου και τη σύνδεση ηλεκτρονικών συσκευών με ένα άγγιγμα. Επιτρέπει την εύκολη αρχικοποίηση ασύρματων δικτύων και είναι συμπληρωματική προς το Bluetooth και το 802.11 με τις δυνατότητες μακρινής απόστασης στα περίπου 10 εκατοστά. Δεν απαιτεί οπτική επαφή και προσφέρει μια εύκολη και απλή μέθοδο σύνδεσης. Αρχικά αναπτύχθηκε από τις εταιρείες Philips και Sony. Η ταχύτητα ανταλλαγής δεδομένων σήμερα είναι περίπου 424 kbps. Η κατανάλωση ενέργειας κατά την ανάγνωση δεδομένων στο NFC είναι κάτω από 15mA.



Εικόνα 5. Λειτουργία NFC [F2]

1.3.4 Internet Protocol (IP)

Το Πρωτόκολλο Διαδικτύου IP αποτελεί το κύριο πρωτόκολλο δικτύου που χρησιμοποιείται στο Διαδίκτυο το οποίο και αναπτύχθηκε κατά τη δεκαετία του 1970. Το IP είναι το κύριο πρωτόκολλο επικοινωνίας στη σουίτα πρωτοκόλλων Διαδικτύου για τη μετάδοση διαγραμμάτων δικτύου διασχίζοντας τα όρια του δικτύου. Υπάρχουν δύο εκδόσεις του Πρωτοκόλλου Διαδικτύου (IP) σε χρήση: IPv4 και IPv6. Κάθε έκδοση ορίζει μια διεύθυνση IP διαφορετικά. Λόγω της ευρείας χρήσης του, ο γενικός όρος "διεύθυνση IP" συνήθως αναφέρεται ακόμα στις διευθύνσεις που ορίζονται από το IPv4. Υπάρχουν πέντε κλάσεις διαθέσιμων εύρων IP στο IPv4: Κλάση A, Κλάση B, Κλάση C, Κλάση D και Κλάση E, ενώ μόνο οι κλάσεις A, B και C χρησιμοποιούνται συνήθως. Το πραγματικό πρωτόκολλο προβλέπει 4,3 δισεκατομμύρια διευθύνσεις IPv4, ενώ το IPv6 θα αυξήσει σημαντικά τη διαθεσιμότητα σε 85.000 τρισεκατομμύρια διευθύνσεις. Το IPv6 είναι το πρωτόκολλο Διαδικτύου του 21ου αιώνα. Αυτό υποστηρίζει περίπου 2¹²⁸ διευθύνσεις.

1.3.5 Bluetooth

Η ασύρματη τεχνολογία Bluetooth είναι μια οικονομική, βραχείας εμβέλειας ραδιοτεχνολογία που εξαλείφει την ανάγκη για ειδικά καλώδια μεταξύ συσκευών όπως φορητοί υπολογιστές, PDAs, φωτογραφικές μηχανές και εκτυπωτές, με αποτελεσματική εμβέλεια 10 - 100 μέτρα. Κατά κανόνα, επικοινωνεί μεταξύ των συσκευών σε ταχύτητες μικρότερες του 1 Mbps και χρησιμοποιεί τις προδιαγραφές του προτύπου IEEE 802.15.1. Αρχικά, το 1994, η εταιρεία Ericson Mobile Communication ξεκίνησε το έργο με την ονομασία "Bluetooth". Χρησιμοποιείται για τη δημιουργία Προσωπικών Δικτύων Περιοχής Personal Area Network PAN. Ένα σύνολο συσκευών Bluetooth που μοιράζονται ένα κοινό κανάλι επικοινωνίας ονομάζεται Piconet. Το Piconet αυτό είναι ικανό να συνδέει ταυτόχρονα 2 έως 8 συσκευές για την ανταλλαγή δεδομένων, που μπορεί να είναι κείμενο, εικόνα, βίντεο και ήχος.

1.3.6 Ασύρματα δίκτυα αισθητήρων (WSN)

Ένα WSN είναι ένα ασύρματο δίκτυο που αποτελείται από αυτόνομες, έξυπνες συσκευές. Αποτελείται από εκατοντάδες ή χιλιάδες αισθητήρες που επικοινωνούν μεταξύ τους και μεταφέρουν δεδομένα από τον έναν στον άλλον. Ένα ασύρματο δίκτυο αισθητήρων είναι ένα σημαντικό στοιχείο στην παραδείγματος του IoT. Τα WSN που βασίζονται στο IoT και έχουν

εντυπωσιακή προσοχή σε πολλούς τομείς, όπως τον στρατό, την εθνική ασφάλεια, την υγεία, την παρακολούθηση της ακρίβειας της γεωργίας, την κατασκευή, την παρακολούθηση του φυσικού περιβάλλοντος, την ανίχνευση δασικών πυρκαγιών και πλημμυρών κ.α. Οι αισθητήριои κόμβοι που τοποθετούνται στο σώμα του ασθενούς παρακολουθούν τις αντιδράσεις στα φάρμακα, έτσι ώστε οι γιατροί να μπορούν να μετρήσουν την επίδραση των φαρμάκων.

1.4 Οι εφαρμογές του διαδικτύου των πραγμάτων (IoT)

Στην καθημερινότητα μας πολλές εφαρμογές έχουν έξυπνες λειτουργίες, αλλά δεν μπορούν να επικοινωνήσουν μεταξύ τους. Η δυνατότητα επικοινωνίας και κοινής χρήσης πληροφοριών μεταξύ τους, είναι αυτή που θα δημιουργήσει μια ευρεία γκάμα νέων εφαρμογών. Αυτές οι εξελισσόμενες εφαρμογές με αυτοματοποιημένες δυνατότητες και αυτονομία θα βελτιώνουμε πιο πολύ την ποιότητα της καθημερινής μας ζωής. Μερικές από αυτές τις εφαρμογές ήδη υπάρχουν στην αγορά προς διάθεση. Ας πάρουμε για παράδειγμα το Google Car, που είναι μια πρωτοβουλία για να παρέχει μια εμπειρία αυτόνομης οδήγησης με πραγματικό χρόνο, με πραγματική κίνηση, σε συνθήκες δρόμου, καιρού και ανταλλαγής πληροφοριών. Όλα τα παραπάνω χάρη στην έννοια του Διαδικτύου των Πραγμάτων (IoT). Υπάρχουν πολλές εφαρμογές που έχουν υλοποιηθεί και θα υλοποιηθούν ακόμα περισσότερες για ωφελήσουν τους πωλητές μέσα από τις λειτουργίες τους. Σε αυτήν την ενότητα, παρουσιάζουμε μερικές από αυτές τις εφαρμογές[4].



Εικόνα 6. Εφαρμογές IoT [F3]

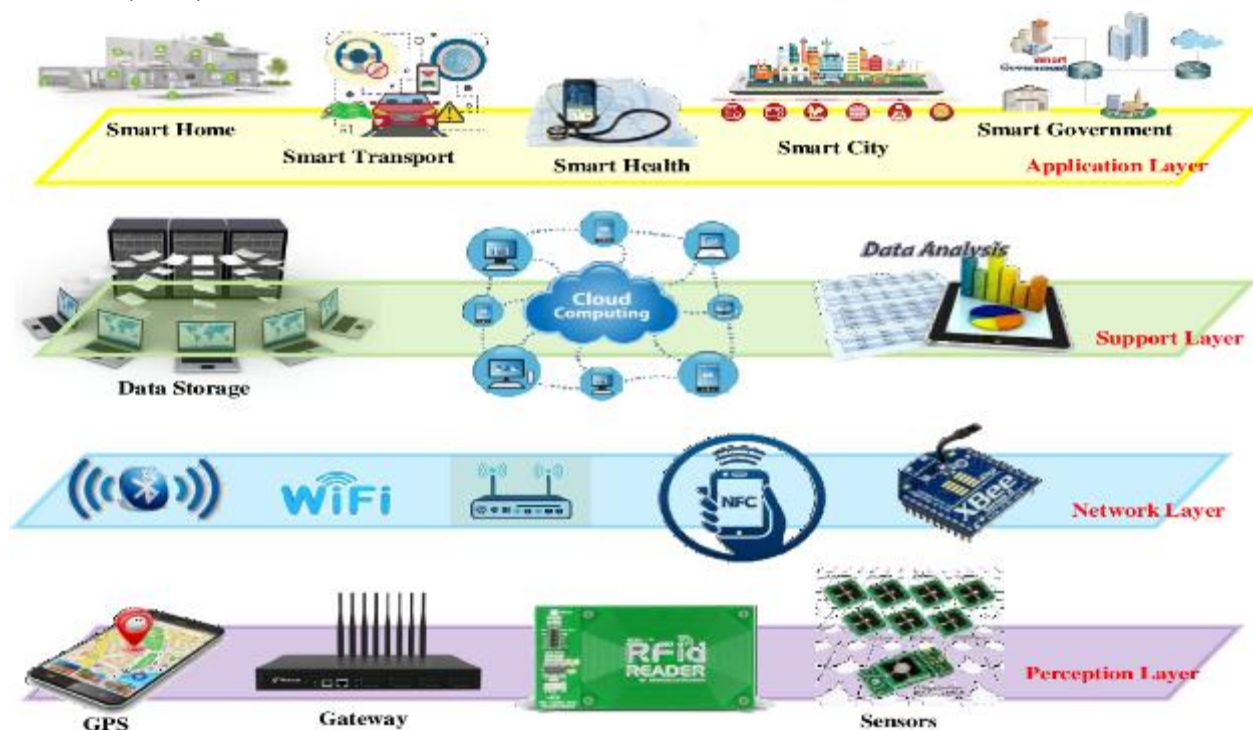
1.4.1. Έξυπνο Σύστημα Κυκλοφορίας.

Η κυκλοφορία αποτελεί σημαντικό μέρος της κοινωνίας, επομένως όλα τα σχετικά προβλήματα πρέπει να αντιμετωπίζονται σωστά. Υπάρχει ανάγκη για ένα σύστημα που να

μπορεί να βελτιώσει την κατάσταση της κυκλοφορίας με βάση τις πληροφορίες που συγκεντρώνονται από διάφορα αντικείμενα με τη χρήση τεχνολογιών IoT. Για ένα τέτοιο έξυπνο σύστημα παρακολούθησης κυκλοφορίας, είναι πολύ σημαντική η υλοποίηση ενός κατάλληλου συστήματος αυτόματης αναγνώρισης οχημάτων και άλλων δεδομένων κυκλοφορίας, όπως για παράδειγμα, μεθόδους επεξεργασίας εικόνας. Το έξυπνο σύστημα παρακολούθησης κυκλοφορίας θα παρέχει μια εμπειρία μεταφοράς μειώνοντας τον συνωστισμό και κίνηση. Θα παρέχει δυνατότητες όπως ανίχνευση κλοπής, αναφορά ατυχημάτων κυκλοφορίας, μείωση της περιβαλλοντικής ρύπανσης. Οι δρόμοι της έξυπνης πόλης (SmartCity) θα παρέχουν ανακατευθύνσεις με σκοπό την λιγότερη εκπομπή καυσαερίου λόγω αναμονής στα φανάρια κυκλοφορίας, με αποτέλεσμα τη βελτιστοποίηση των διαδρομών οδήγησης και πεζοπορίας. Το σύστημα φωτισμού της κυκλοφορίας θα προσαρμόζεται στις καιρικές συνθήκες για εξοικονόμηση ενέργειας και η διαθεσιμότητα θέσεων στάθμευσης σε όλη την πόλη θα είναι προσβάσιμη από όλους.

1.4.2. Έξυπνο Περιβάλλον.

Η πρόβλεψη φυσικών καταστροφών όπως πλημμύρες, πυρκαγιές, σεισμοί κ.λπ. αλλά και σε δίκτυα κρίσιμων υποδομών γίνεται πιο εύκολα και μέσω των καινοτόμων τεχνολογιών του IoT. Η παρακολούθηση ατμοσφαιρικής ρύπανσης στο περιβάλλον υπάρχει αλλά θα γίνει ακόμα πιο εξελίξιμη, με ενημέρωση των πολιτών από τις εκάστοτε εφαρμογές στις κινητές συσκευές τους.



Εικόνα 7. Έξυπνο περιβάλλον [F4]

1.4.3. Έξυπνο Σπίτι.

Το IoT θα παρέχει επίσης προσωπικές λύσεις DIY για την αυτοματοποίηση και μετατροπή του σπιτιού σε έξυπνο, με τις οποίες μπορούμε να ελέγχουμε απομακρυσμένα τις συσκευές μας ανάλογα με τις ανάγκες μας. Η κατάλληλη παρακολούθηση των μετρητών ενέργειας και υδροδότησης βοηθά στην εξοικονόμηση πόρων και στην ανίχνευση υπερ-χρεώσεων υπερ-

καταναλώσεων ρεύματος, διαρροών νερού κ.λπ. Υπάρχει κατάλληλο σύστημα ανίχνευσης παράνομης εισβολής, το οποίο θα εξελιχθεί ώστε να αποτρέπει τις κλοπές. Οι αισθητήρες κήπου μπορούν να ανιχνεύσουν την φωτεινότητα του ήλιου, και αναλόγως να πράξουν βάσει των ρυθμίσεων που τους έχουμε ορίσει, την υγρασία του περιβάλλοντος, τη θερμοκρασία, την υγρασία του εδάφους. Με βάση την συλλογή πληροφοριών από τους αναφερόμενους αισθητήρες είναι σε θέση να αποφασίσουν για το πότε θα πρέπει, και πόση ώρα να ποτιστούν τα λουλούδια, με γνώση την ανάγκη του κάθε φυτού.



Εικόνα 8. Έξυπνο σπίτι [F5]

1.4.4. Έξυπνα νοσοκομεία (μελλοντική εφαρμογή).

Τα νοσοκομεία θα εξοπλιστούν με έξυπνα και ευέλικτα φορητές συσκευές με ενσωματωμένα με RFID τα οποία θα δίνονται στους ασθενείς κατά την άφιξή τους. Μέσω αυτών, όχι μόνο οι γιατροί αλλά και οι νοσοκόμες θα μπορούν να παρακολουθούν τον καρδιακή παλμό, την αρτηριακή πίεση, τη θερμοκρασία και άλλες καταστάσεις των ασθενών εντός ή εκτός των εγκαταστάσεων του νοσοκομείου, λόγω του ότι σε πάρα πολλές ιατρικές και επείγουσες περιπτώσεις, όπως καρδιακή ανακοπή, τα ασθενοφόρα χρειάζονται κάποιο χρόνο για να φτάσουν στον ασθενή. Τέλος οι ασθενείς μέσω αυτών των συσκευών θα μπορούν να παρακολουθούνται από τους θεράποντες ιατρούς τους και όταν κρίνεται σκόπιμο και αναγκαίο να στέλνεται ένα drone στο σημείο ώστε να παρέχει γρήγορη και μια πρώτη ιατρική φροντίδα μέχρι να φτάσει το ασθενοφόρο.



Εικόνα 9. Έξυπνα νοσοκομεία [F6]

1.4.5. Έξυπνη γεωργία.

Στην έξυπνη γεωργία, που τα τελευταία χρόνια φαίνεται να είναι ένας ραγδαία αναπτυσσόμενος τομέας εφαρμογών του IoT, γίνεται παρακολούθηση της εφορίας- θρέψης (γεωπονικός ορός) του εδάφους, του φωτός, και της υγρασίας. Ο σκοπός είναι να βελτιωθεί η εμπειρία των θερμοκηπίων μέσω της αυτόματης ρύθμισης της θερμοκρασίας και ποτίσματος για τη μεγιστοποίηση της παραγωγής. Το ακριβές πότισμα και λίπασμα βοηθά στην εξοικονόμηση νερού και λιπασμάτων αντίστοιχα.

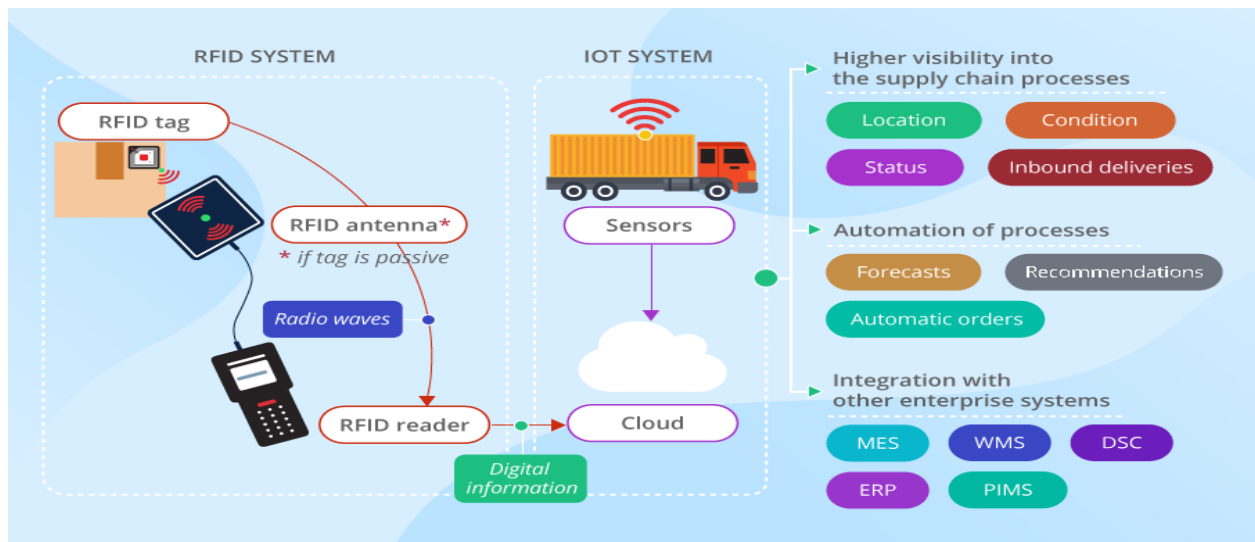


Εικόνα 10. Έξυπνη γεωργία [F7]

1.4.6. Έξυπνο Εμπόριο και Διαχείριση Εφοδιαστικής Αλυσίδας.

Το IoT με τη χρήση της RFID παρέχει πολλά πλεονεκτήματα στους εμπόρους. Με τα προϊόντα να είναι εξοπλισμένα με RFIDs, ένας έμπορος, μια αποθήκη, ένα Super Market, μπορεί

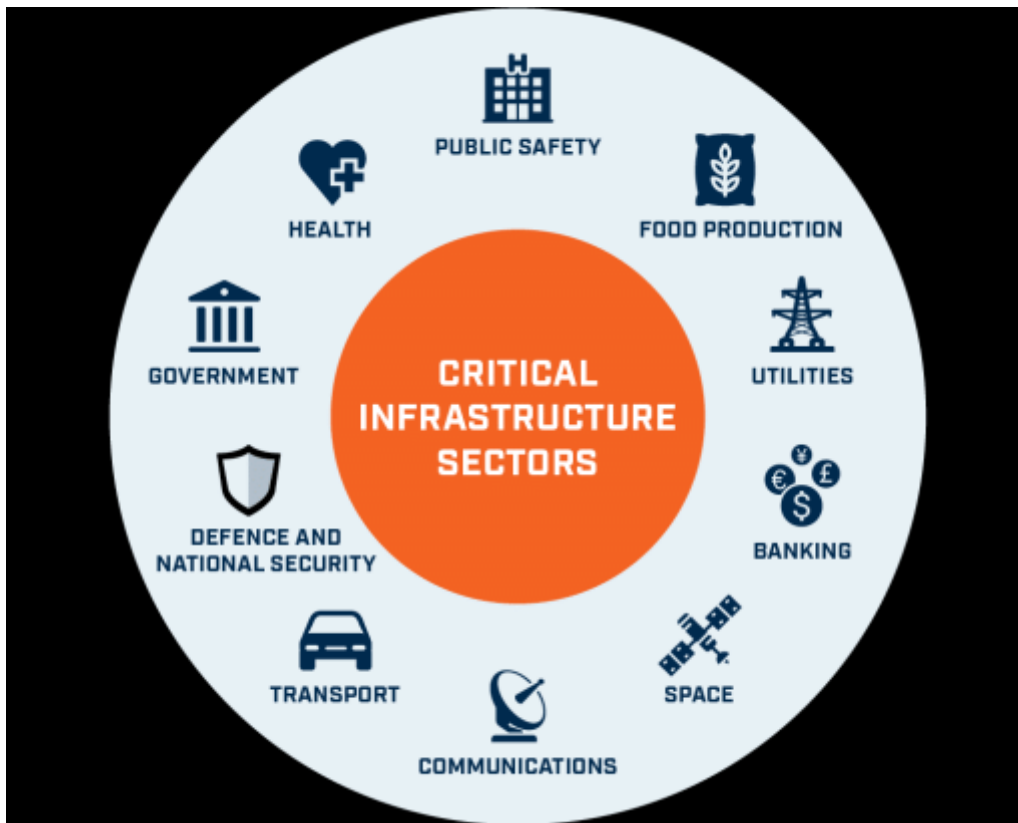
εύκολα να παρακολουθεί τα αποθέματα τις αποθήκης τους για να αποφευχθεί η έλλειψη εμπορευμάτων, να ανιχνεύσει μια κλοπή. Ακόμα δίνεται η δυνατότητα δημιουργίας έξυπνων και πραγματικού χρόνου διαγραμμάτων πωλήσεων για αποτελεσματικές στρατηγικές



Εικόνα 11. Έξυπνο Εμπόριο και Διαχείριση Εφοδιαστικής Αλυσίδας [F8]

1.5 Κρίσιμα δίκτυα υποδομών (Critical Infrastructure Networks)

Τα κρίσιμα δίκτυα υποδομής είναι δίκτυα μεταφοράς διανομής ενέργειας, είναι ουσιώδεις και ζωτικής σημασίας για τη λειτουργία μιας κοινωνίας, μιας οικονομίας και πρέπει να είναι διαθέσιμα 365 ημέρες τον χρόνο, 24 ώρες την ημέρα. Αυτές οι υποδομές είναι απαραίτητες για τη διατήρηση της δημόσιας ασφάλειας, της εθνικής ασφάλειας μιας χώρας. Ακόμα στα κρίσιμα δίκτυα περιλαμβάνονται και διάφοροι τομείς, όπως της βιομηχανίας. Δυστυχώς, ατυχείς ή και εσκεμμένες επιθέσεις σε τέτοια δίκτυα μπορεί να οδηγήσουν στη διακοπή των υπηρεσιών προς τους πολίτες. Οι ατυχείς μπορεί να προκληθούν από κακές καιρικές συνθήκες ή φυσικές καταστροφές, ενώ οι επιθέσεις μπορεί να κυμαίνονται από απλή καταστροφή έως τρομοκρατικές δραστηριότητες. Η προστασία των κρίσιμων υποδομών CIP απαιτεί μηχανισμούς παρακολούθησης που μας επιτρέπουν να ανιχνεύουμε αυτές τις αποτυχίες και επιθέσεις το συντομότερο δυνατόν. Καθώς πολλές κρίσιμες υποδομές έχουν μεγάλη γεωγραφική έκταση, η προστασία των κρίσιμων υποδομών χρειάζεται μηχανισμούς παρακολούθησης που να λειτουργούν σωστά. Ειδικότερα, τα Ασύρματα Δίκτυα Αισθητήρων WSNs μπορούν να αναπτυχθούν σε μεγάλη κλίμακα με σχετική ευκολία, καθώς συνήθως αποτελούνται από φθηνές συσκευές που μπορούν να παρέχουν υπηρεσίες παρακολούθησης με κόστος αποδοτικό ως προς της υφιστάμενη υποδομή χωρίς έξτρα εγκαταστάσεις. Σε πολύ κρίσιμες καταστάσεις, τα Ασύρματα Δίκτυα Αισθητήρων WSNs μπορεί ακόμη και να παρέχουν αρκετές πληροφορίες σχετικά με την Κρίσιμη Υποδομή, να βοηθήσουν στην πρόληψη για περαιτέρω ζημιές και να ξεκινήσει τη διαδικασία αποκατάστασης. Ωστόσο, πρέπει να είναι σαφές ότι η χρησιμότητα των Ασύρματων Δικτύων Αισθητήρων WSNs για την Προστασία Κρίσιμων Υποδομών CIP καθορίζεται κυρίως από την αξιοπιστία του ίδιου του WSN. Ένα WSN που αναφέρει μια ελαττωματική κατάσταση εμποδίζει τον χειριστή της Κρίσιμης Υποδομής να πραγματοποιήσει την κατάλληλη συντήρηση που θα μπορούσε ώστε να επιδιορθώσει το πρόβλημα πριν οι συνέπειές του επηρεάσουν την Υποδομή [8].



Εικόνα 12. Κρίσιμα δίκτυα υποδομής [F9]

1.5.1. Παραδείγματα κρίσιμων δικτύων υποδομής.

Παρακάτω ορισμένα από τα πιο γνωστά κρίσιμα δίκτυα υποδομών για μία χώρα

1. **Ενέργεια:** Εργοστάσια παραγωγής ενέργειας, δίκτυα ηλεκτρικής ενέργειας, εγκαταστάσεις πετρελαίου και φυσικού αερίου, και συστήματα μεταφοράς καυσίμων.
2. **Μεταφορές:** Αεροδρόμια, λιμάνια, σιδηροδρόμους, αυτοκινητόδρομους, γέφυρες και δίκτυα δημόσιων μεταφορών.
3. **Νερό:** Εργοστάσια επεξεργασίας νερού, υδατοφράκτες, φράγματα και συστήματα διανομής νερού.
4. **Επικοινωνία:** Δίκτυα τηλεπικοινωνιών, υποδομή διαδικτύου και κέντρα δεδομένων.
5. **Υγεία:** Νοσοκομεία, ιατρικές εγκαταστάσεις, παραγωγή και διανομή φαρμάκων.
6. **Υπηρεσίες έκτακτης ανάγκης:** Αστυνομία, πυροσβεστική, υπηρεσίες έκτακτης ιατρικής περίθαλψης και συστήματα αντιμετώπισης καταστροφών.
7. **Οικονομικές υπηρεσίες:** Τραπεζικά συστήματα, χρηματιστήρια, δίκτυα πληρωμών και χρηματοπιστωτικά ιδρύματα.
8. **Κυβέρνηση:** Κτίρια κυβέρνησης, στρατιωτικές εγκαταστάσεις και συστήματα δημόσιας διοίκησης.
9. **Τροφή και γεωργία:** Γεωργική παραγωγή, επεξεργασία τροφίμων, διανομή και αλυσίδες εφοδιασμού τροφίμων.
10. **Χημική βιομηχανία:** Χημικά εργοστάσια, πετρελαιοπηγές και εγκαταστάσεις χειρισμού επικίνδυνων υλικών.

Αυτές οι κρίσιμες υποδομές είναι αλληλεξαρτώμενες, και οι διακοπές ή αποτυχίες σε έναν τομέα μπορούν να έχουν αλυσιδωτές επιπτώσεις σε άλλους, οδηγώντας σε σημαντικές κοινωνικές και οικονομικές συνέπειες. Λόγω της σημασίας τους, αυτά τα δίκτυα υποδομής συχνά προστατεύονται, παρακολουθούνται και ρυθμίζονται για να εξασφαλιστεί η ανθεκτικότητά τους έναντι φυσικών καταστροφών, κυβερνοεπιθέσεων, τρομοκρατικών επιθέσεων και άλλων κινδύνων. Οι κυβερνήσεις, μαζί με τους εμπειρογνώμονες και τεχνικούς ασφαλείας συνεργάζονται για την αναγνώριση και αντιμετώπιση των ευπαθειών σε αυτά τα δίκτυα, την ανάπτυξη υφιστάμενων και νέων σχεδίων αντιμετώπισης κινδύνων και την εφαρμογή μέτρων για την προστασία τους, για τη διασφάλιση της συνεχούς και αδιάληπτης λειτουργίας τους [9,10].

Critical Infrastructure Sector	Prefix	Critical Infrastructure Sector	Prefix
Chemical	CH	Financial Services	FS
Commercial Facilities	CF	Food & Agriculture	FA
Critical Manufacturing	CM	Government Facilities	GF
Dams	D	Healthcare & Public Health	HPH
Defense Industrial Base	DIB	Information Technology	IT
Emergency Services	ES	Nuclear Reactors, Materials & Waste	NRMW
Energy	E	Transportation Systems	TS

Εικόνα 13. Οι 16 πιο κρίσιμοι τομείς σύμφωνα με το US Dept of Homeland Security [10]

1.5.2 Απαιτήσεις δικτύων κρίσιμων υποδομών

Όλες οι κρίσιμες υποδομές, στην εφοδιαστική αλυσίδα, πρέπει να πληρούν αφενός μια σειρά από τεχνικές και τεχνολογικές απαιτήσεις για να ταιριάζουν στις απαιτήσεις, και αφετέρου στα κριτήρια και τις προϋποθέσεις που ορίζονται από τις προδιαγραφές και τα πρότυπα σύμφωνα με την εκάστοτε νομοθεσία. Οι απαιτήσεις που σχετίζονται άμεσα με τις υποδομές είναι οι εξής:

1. **Υψηλή διαθεσιμότητα:** Η διαθεσιμότητα των συστημάτων που σχετίζονται με την εφοδιαστική αλυσίδα πρέπει να είναι τουλάχιστον 99% λειτουργική, αυτό συνεπάγεται ότι η επιχειρησιακή δραστηριότητα θα πρέπει να συνεχιστεί για πάνω από 99% του συνολικού χρόνου λειτουργίας.
2. **Αναβαθμίσεις συστημάτων:** Τα κύρια συστήματα πρέπει να αναβαθμίζονται χωρίς να επηρεάζεται η διαθεσιμότητα της επιχείρησης. Οι αναβαθμίσεις πριν την ολοκλήρωση να έχουν δοκιμαστεί σε εξοπλισμό δοκιμαστικού περιβάλλοντος UAT για να διασφαλιστεί η υψηλή πιθανότητα επιτυχίας στο περιβάλλον παραγωγής την ημέρα της εγκατάστασης.
3. **Ομαδοποίηση και ανάλυση των δεδομένων που λαμβάνονται από τους αισθητήρες:** Πρέπει να δημιουργηθεί μια πλατφόρμα για τη συγκέντρωση των δεδομένων από τους αισθητήρες και την ομαδοποίηση τους στην ίδια μορφή. Μόλις τα δεδομένα έχουν ομαδοποιηθεί και τυποποιηθεί, μπορούν να επεξεργαστούν από το υπολογιστικό σύστημα, το οποίο θα εκτελέσει ενέργειες βάσει συγκεκριμένων προκαθορισμένων συνθηκών και ενεργειών.

4. **Ημερήσια συντήρηση συστήματος σε λειτουργία 24/7:** Πρέπει να περιλαμβάνεται ένα πλάνο συντήρησης συστήματος από τους χειριστές με απομακρυσμένη επίβλεψη και τοπικές ενέργειες στον τόπο σε περίπτωση σημαντικών περιστατικών. Οι χειριστές θα πρέπει να πηγαίνουν στο χώρο του εξοπλισμού και με βάση τον εντοπισμό του περιστατικού που έχουν ερευνήσει με την απομακρυσμένη πλατφόρμα παρακολούθησης να επεμβαίνουν προς την επίλυση προβλημάτων [11].

1.6 Τεχνολογίες υποστήριξης δικτύων κρίσιμων υποδομών.

Οι τεχνολογίες πληροφορικής και επικοινωνιών παίζουν πολύ κρίσιμο ρόλο στη διασύνδεση και τον έλεγχο σε κρίσιμα συστήματα. Αυτό ισχύει και για τα συστήματα SCADA, όπου η επίβλεψη και ο έλεγχος των υποδομών είναι αλληλένδετος σε μεγάλο βαθμό με την αξιοπιστία, την ασφάλεια των πληροφοριακών συστημάτων και καναλιών επικοινωνίας καθώς επίσης και με την αποστολή, λήψη και επεξεργασία εντολών, για μετρήσεις και συναγερούς.

Οι τεχνολογίες υποστήριξης δικτύων κρίσιμων υποδομών περιλαμβάνουν τα εξής:

1. **Διπλοασιασμός και εφεδρεία:** Η χρήση διπλοασιασμού συστημάτων και μηχανισμών εξασφαλίζει τη συνεχή λειτουργία ακόμα και σε περίπτωση αποτυχίας ή προβλήματος σε ένα μέρος του δικτύου.
2. **Εξασφάλιση επικοινωνίας:** Η χρήση τεχνολογιών όπως οι πολλαπλοί δίαυλοι επικοινωνίας, οι ασύρματες συνδέσεις και οι δορυφορικές συνδέσεις εξασφαλίζει την ανεμπόδιστη επικοινωνία ακόμα και σε περιοχές με προβλήματα επικοινωνίας.
3. **Ασφάλεια δικτύου:** Η εφαρμογή αποτελεσματικών μέτρων ασφαλείας, όπως η κρυπτογράφηση δεδομένων, οι προληπτικές πρακτικές ασφαλείας και οι πυραμίδες προστασίας, εξασφαλίζει την προστασία του δικτύου από εξωτερικές απειλές και επιθέσεις.
4. **Διαχείριση ενέργειας:** Η χρήση τεχνολογιών που ελαχιστοποιούν την κατανάλωση ενέργειας και προωθούν την αποδοτική χρήση της ενέργειας στις κρίσιμες υποδομές εξασφαλίζει την ανεξάρτητη λειτουργία τους από πιθανές διακοπές ρεύματος.
5. **Επικοινωνίες σε πραγματικό χρόνο:** Η δυνατότητα επικοινωνίας σε πραγματικό χρόνο μεταξύ των συστημάτων και των συσκευών επιτρέπει την άμεση μετάδοση και επεξεργασία δεδομένων για τον έλεγχο και την επιτήρηση των κρίσιμων υποδομών.
6. **Αποκατάσταση μετά από προβλήματα:** Η ανάπτυξη και εφαρμογή σχεδίων αποκατάστασης μετά από προβλήματα, συμπεριλαμβανομένων των αντιγράφων ασφαλείας δεδομένων και των εκτεταμένων διαδικασιών ανάκτησης, εξασφαλίζει τη γρήγορη αποκατάσταση των κρίσιμων υποδομών μετά από ανεπιθύμητα συμβάντα

1.6.1 Συστήματα επικοινωνίας

Η δικτύωση προσφέρει σημαντικά οφέλη λειτουργικότητας όσον αφορά τον έλεγχο επιτήρησης για την ανάκτηση δεδομένων. Στα οφέλη μπορούν να αναφερθούν, η παγκόσμια συνδεσιμότητα, η ευελιξία διάδοσης των δεδομένων από οπουδήποτε, οποτεδήποτε και μέσω κατάλληλων πρωτοκόλλων IP και Internet. Με σκοπό την μεγαλύτερη επέκταση και τη λειτουργικότητα, καθώς και την μείωση του κόστους συντήρησης και εγκατάστασης, οι απομακρυσμένοι υποσταθμοί έχουν μεταβεί στο πρωτόκολλο TCP/IP, ώστε να επεκτείνουν τη συνδεσιμότητά τους ώστε να εξασφαλίσουν την διασύνδεσή τους με άλλες τεχνολογίες. Η

χρήση του πρωτόκολλου TCP/IP έχει οδηγήσει επίσης στην καθορισμό και τυποποίηση των πρωτοκόλλων επικοινωνίας SCADA βασισμένων στο μοντέλο Client - Server.

1.6.2 Ασύρματα συστήματα επικοινωνίας

Οι τεχνολογίες επικοινωνίας μεγάλου εύρους όπως οι κινητές κυψέλες (π.χ., 3G/4G, UMTS, GPRS, GSM/TETRA), δορυφορικές επικοινωνίες, GPS, WiMAX η ασύρματη πρόσβαση σε ευζωνικά δίκτυα MBWA και τα συστήματα μικροκυμάτων δίνουν την δυνατότητα της αυτοματοποίησης και του έλεγχου εργασιών με χαμηλό κόστος, παρέχοντας επίσης κινητικότητα, συνεργασία, αξιοπιστία και συνύπαρξη με άλλες τεχνολογίες. Ο Χειρισμός των βιομηχανικών συσκευών μπορεί να γίνει με ασύρματους πομποδέκτες, διαμέσου φορητών συσκευών αποστέλλοντας εντολές και λαμβάνοντας πληροφορίες όπως κατάσταση, μετρήσεις και προβλήματα. Επίσης υπάρχουν τεχνολογίες για έλεγχο μεσαίας και μικρής κλίμακας, ενώ επίσης περιλαμβάνουν τεχνολογία Bluetooth, ασύρματα τοπικά δίκτυα WLANs, ασύρματα δίκτυα αυτόνομης λειτουργίας MANETs και ασύρματα δίκτυα αισθητήρων WSNs. Η κυψέλη κινητής τηλεφωνίας συχνά αποτελεί μια οικονομικά διαφορετική λύση για τη σύνδεση μικρών ομαδοποιημένων συσκευών για την αποστολή όχι και τόσο κρίσιμων πληροφοριών προς το κέντρο ελέγχου. Ωστόσο, ο μεγάλος αριθμός κυψελών δημόσιας κινητής τηλεφωνίας για επιτήρηση μπορεί να αυξήσει τις καθυστερήσεις επικοινωνίας και τα συνοδευτικά κόστη μεταφοράς δεδομένων. Η υποδομή προηγμένης μέτρησης ενός έξυπνου δικτύου εξαρτάται σε κατά μεγάλο ποσοστό σε αυτές τις τεχνολογίες για τη μεταφορά σημαντικών πληροφοριών, που σχετίζονται με τους πελάτες και τις επιχειρήσεις υπηρεσιών δημόσιου ενδιαφέροντος. Η υποδομή προηγμένης μέτρησης σχεδιάζεται για να μετρά, συλλέγει, παρουσιάζει και αναλύει την κατανάλωση ενέργειας, συνδέει συσκευές μέτρησης (σχετιζόμενες με ηλεκτρισμό, αέριο, θέρμανση και νερό) με επιχειρησιακά συστήματα υπηρεσιών δημόσιου ενδιαφέροντος, με δυνατότητα μαζικής σύνδεσης μεταξύ πελατών και άλλων οντοτήτων[9]. Για παράδειγμα, η τεχνολογία MBWA λειτουργεί στα 3,5 GHz με ρυθμούς μετάδοσης δεδομένων από 1 Mbps έως 20 Mbps, ενώ το WiMAX λειτουργεί στα 2,3, 2,5 και 3,5 GHz με ρυθμούς μετάδοσης έως 70 Mbps. Αυτό το εύρος μετάδοσης θα μπορούσαν να επιτρέψουν στην υποδομή προηγμένης μέτρησης να αποστέλλει ροές δεδομένων από έξυπνα όργανα μετρήσεων στα επιχειρησιακά συστήματα των υπηρεσιών δημόσιου ενδιαφέροντος, συμπεριλαμβανομένων των συστημάτων ελέγχου εποπτείας στους υποσταθμούς ενέργειας. Τα ασύρματα επικοινωνιακά δίκτυα γίνονται επίσης όλο και πιο σημαντικά για την προστασία των κρίσιμων υποδομών. Τα δίκτυα επιτρέπουν στους υπαλλήλους να καθιερώσουν τοπική συνδεσιμότητα εντός του περιβάλλοντος, παρέχοντας παράλληλα κινητικότητα. Αυτό συμβαίνει στην περίπτωση που επιτρέπουν στους ελεγκτές να αποκτούν εξουσιοδοτημένη πρόσβαση στα στοιχεία του συστήματος, όπως αισθητήρες, ενεργοποιητές και να πραγματοποιούν δραστηριότητες λειτουργίας όπως διάδοση και διαχείριση δεδομένων, παρακολούθηση συμβάντων και επιτόπου αλλαγή παραμέτρων[10]. Σε αυτό το πλαίσιο, αξίζει να τονιστεί ο ρόλος των ασύρματων προσωπικών δικτύων περιοχής WPANs για εφαρμογές με περιορισμένη γεωγραφική κάλυψη και όπου ο έλεγχος περιορίζεται σε ένα μικρό αριθμό κόμβων όπως Bluetooth, Z-Wave και ZigBee. Μια παραλλαγή των WPANs περιλαμβάνει τα LR-WPANs χαμηλού ρυθμού WPANs τα LP-WANs χαμηλής ισχύος WANs Άλλες σημαντικές πτυχές είναι η συνύπαρξη και η αξιοπιστία των επικοινωνιών μεταξύ ομοίων τεχνολογιών.

1.6.2.1 Κίνδυνοι και προκλήσεις στα ασύρματα συστήματα επικοινωνίας

Ορισμένες από τις προκλήσεις σχετίζονται με την πιστοποίηση και την εξουσιοδότηση των συσκευών, την ασφάλεια των πληροφοριών και την ανταλλαγή μηνυμάτων με διάφορες μορφές. Ένα ευρέως γνωστό πρόβλημα για την αξιοπιστία των επικοινωνιών είναι η επίθεση προς αλλοίωση της ραδιοσυχνότητας. Άλλες απειλές επηρεάζουν τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων και των πόρων. Για παράδειγμα, η διαθεσιμότητα επηρεάζεται από επιθέσεις υπερφόρτωσης των καναλιών επικοινωνίας, συνεχόμενης αποστολής δεδομένων σε ένα κόμβο με προωθητικό χαρακτήρα στον επόμενο με αποτέλεσμα να καθυστερεί το δίκτυο. Οι επιθέσεις αυτές έχουν ως σκοπό την παραποίηση της διαδρομής την έλλειψη εμπιστευτικότητας την παρακολούθηση των κανάλια επικοινωνίας, την ανάλυση κίνησης για διάφορες μελλοντικές επιθέσεις [12,13].

ΚΕΦΑΛΑΙΟ 2

Δίκτυα επικοινωνιών, κινητής τηλεφωνίας, ασύρματων αισθητήρων (WSN) και εφαρμογές.

2.1 Δίκτυα επικοινωνιών

Με το Όρο δίκτυα επικοινωνιών εννοούμε τα συστήματα εκείνα που διευκολύνουν την ανταλλαγή πληροφοριών, δεδομένων ή μηνυμάτων μεταξύ διαφορετικών συσκευών ή οντοτήτων. Αυτά τα δίκτυα επιτρέπουν τη μεταφορά δεδομένων σε διάφορες μορφές, όπως κείμενο, φωνή, βίντεο ή πολυμέσα, σε μεγάλες αποστάσεις. Είναι η βάση των σύγχρονων συστημάτων επικοινωνίας και υποστηρίζουν μια ευρεία γκάμα εφαρμογών, συμπεριλαμβανομένης της σύνδεσης στο διαδίκτυο, των τηλεφωνικών υπηρεσιών, των βιντεοκλήσεων και πολλών άλλων. Τα δίκτυα επικοινωνίας μπορούν να είναι φυσικά ή εικονικά και παρέχουν την υποδομή και τα πρωτόκολλα που απαιτούνται για τη μεταφορά δεδομένων. Ο βασικός σκοπός ενός δικτύου επικοινωνίας είναι να δημιουργήσει συνδέσεις και να ενισχύσει την επικοινωνία μεταξύ συσκευών ή οντοτήτων, επιτρέποντάς τους να ανταλλάσσουν πληροφορίες αποτελεσματικά. Αυτά τα δίκτυα μπορούν να υποστηρίξουν διάφορες μορφές επικοινωνίας, συμπεριλαμβανομένων κειμένου, φωνής, βίντεο και πολυμέσων, εφαρμογών, [14] και μπορούν να χωριστούν σε δημόσια και ιδιωτικά δίκτυα.

2.1.1 Δημόσια δίκτυα επικοινωνιών

Τα δημόσια δίκτυα αναφέρονται στην ανταλλαγή πληροφοριών και δεδομένων μέσω δικτύων που είναι προσβάσιμα προς το ευρύ κοινό. Αυτά τα δίκτυα σχεδιάζονται και λειτουργούν από παρόχους υπηρεσιών για να προσφέρουν συνδεσιμότητα και υπηρεσίες επικοινωνίας σε μια ευρεία γκάμα χρηστών, συμπεριλαμβανομένων ατόμων και οργανισμών [15]. Οι δημόσιες επικοινωνίες δικτύων προσφέρουν πληθώρα οφελών, όπως ευρεία συνδεσιμότητα, παγκόσμια εμβέλεια και εύκολη πρόσβαση σε πληροφορίες και υπηρεσίες. Ωστόσο, είναι σημαντικό να σημειωθεί ότι οι δημόσιες δίκτυα μπορεί να παρουσιάζουν δυνητικούς κινδύνους ασφάλειας, καθώς είναι προσβάσιμα από ένα μεγάλο αριθμό χρηστών. Οι χρήστες θα πρέπει να λάβουν κατάλληλα μέτρα για την προστασία της ιδιωτικότητας τους και των δεδομένων τους όταν χρησιμοποιούν δημόσιες επικοινωνίες δικτύων, όπως η χρήση ασφαλών συνδέσεων (HTTPS), η χρήση κρυπτογράφησης και η προσοχή στο να μην μοιράζονται ευαίσθητες πληροφορίες [16].

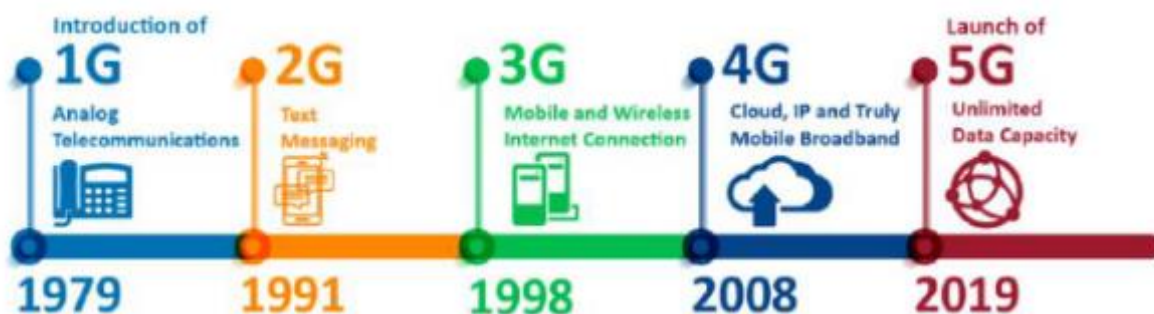
2.1.2 Ιδιωτικά δίκτυα επικοινωνιών

Τα ιδιωτικά δίκτυα, γνωστά και ως κλειστά δίκτυα, δημιουργούνται και λειτουργούν από οργανισμούς ή άτομα για αποκλειστική χρήση. Αυτά τα δίκτυα συνήθως σχεδιάζονται για να

συνδέουν συσκευές εντός ενός συγκεκριμένου οργανισμού, όπως μια εταιρεία, μια κυβερνητική υπηρεσία ή μια εκπαιδευτική ιδρυματική μονάδα. Τα ιδιωτικά δίκτυα προσφέρουν ελεγχόμενη πρόσβαση, υψηλά επίπεδα ασφάλειας και προσαρμοσμένα χαρακτηριστικά που προσαρμόζονται στις συγκεκριμένες απαιτήσεις του οργανισμού. Δεν είναι προσβάσιμα από το γενικό κοινό ή από εξωτερικές οντότητες, εκτός αν υπάρχει εξουσιοδότηση, καθώς προσφέρουν μεγαλύτερο έλεγχο, ασφάλεια και εξατομίκευση σε σύγκριση με τα δημόσια δίκτυα. Επιτρέπουν εξατομικευμένες λύσεις για να ανταποκριθούν σε συγκεκριμένες ανάγκες, και προστατεύουν ευαίσθητα δεδομένα ώστε να διασφαλίσουν αξιόπιστη και αποτελεσματική επικοινωνία [17].

2.2 Δίκτυα κινητής τηλεφωνίας

Τα τελευταία χρόνια, τα ασύρματα δίκτυα κινητής τηλεφωνίας (επικοινωνίας) έχουν γνωρίσει μια μεγάλη αλλαγή. Η γενιά των κινητών ασύρματων δικτύων γενικά έχει αλλάξει ως προς την ταχύτητα του δικτύου, την τεχνολογική εξέλιξη και το εύρος συχνοτήτων. Κάθε γενιά αποτελείται από διαφορετικά πρότυπα, χωρητικότητες καναλιών, νέες μεθόδους ως προς τα χαρακτηριστικά του, που την διαφοροποιούν από τις προηγούμενες. Η πρώτη κινητή συσκευή υλοποιήθηκε από τη Motorola το 1973, ενώ το πρώτο αυτόματο δίκτυο από κυψέλες κινητής τηλεφωνίας ξεκίνησε από τη NTT στην Ιαπωνία το 1979, που ακολούθησε την εισαγωγή του συστήματος NMT στη Δανία, τη Φινλανδία, τη Νορβηγία και τη Σουηδία το 1981. Από εδώ ξεκινά η “ζωή” των γενιών για την ασύρματη κινητή επικοινωνία-τηλεφωνία [18]. Τα πρώτα χρόνια της 2ης χιλιετίας, ο αριθμός των χρηστών κινητής τηλεφωνίας είχε ξεπεράσει το 1 δισεκατομμύριο, ένας αριθμός που αυξάνεται συνεχώς μέχρι και σήμερα. Αυτή η επανάσταση στη ζωή μας έχει πραγματοποιηθεί μέσω μιας συνεχούς εξέλιξης των προτύπων και των προϊόντων, διατηρώντας ένα επίπεδο βέλτιστης απόδοσης [19]. Η πρώτη γενιά (1G) των ασύρματων κινητών επικοινωνιών ήταν αναλογική και χρησιμοποιήθηκε μόνο για κλήσεις φωνής. Η δεύτερη γενιά (2G) ήταν μια ψηφιακή τεχνολογία και υποστήριζε την αποστολή μηνυμάτων κειμένου. Στη συνέχεια ακολούθησε η τρίτη γενιά (3G), η οποία παρείχε υπηρεσίες πολυμέσων με υψηλότερες ταχύτητες μετάδοσης, ενώ είχε μεγαλύτερο μέγεθος χώρου καναλιού. Η τέταρτη γενιά (4G) δικτύων περιέκλειε τη τεχνολογία του 3G δικτύου, με το διαδίκτυο ώστε να υποστηρίξει ασύρματο - κινητό διαδίκτυο, προκειμένου να προσπελαθούν οι περιορισμοί που υπήρχαν στο 3G και να βελτιωθεί η ποιότητα υπηρεσιών, με αποτέλεσμα να αυξηθεί το εύρος ζώνης. Το δίκτυο πέμπτης (5G) προωθεί έναν πραγματικό ασύρματο κόσμο - τον Ασύρματο Παγκόσμιο Ιστό Wireless World Wide Web.



Εικόνα 14. Η εξέλιξη της κινητής τηλεφωνίας στο πέρασμα των χρόνων [F10]

2.2.1 Δίκτυα 1ης γενιάς

Τα συστήματα ασύρματων κινητών επικοινωνιών της πρώτης γενιάς είχαν κουλτούρα αναλογική ως τεχνολογική υποδομή η οποία είχε αναπτυχθεί τη δεκαετία του 1980, αφού χρησιμοποιήθηκαν περισσότερο σε υπηρεσίες φωνής βασισμένες στο AMPS. Το σύστημα AMPS βασιζόταν στην διαμόρφωση της συχνότητας και χρησιμοποιούσε την τεχνική της διαίρεσης σε πολλαπλές πρόσβασης με συχνότητα FDMA με χωρητικότητα καναλιού 30KHz και ζώνη συχνοτήτων από 824 –894MHz ενώ η ταχύτητα έφτανε τα 2.4 kbps. Το AMPS ανακοινώθηκε για πρώτη φορά από τις Ηνωμένες Πολιτείες το 1982 [20].

2.2.2 Δίκτυα 2ης γενιάς

Στο σύστημα της δεύτερης γενιάς εισήχθη η ψηφιακή τεχνολογία η οποία εμφανίστηκε στα τέλη της δεκαετίας του 1980. Χρησιμοποιήθηκαν ψηφιακά σήματα για τη μεταγωγή φωνής ενώ η ταχύτητα του έφτανε τα 64kbps. Το εύρος ζώνης του 2G ξεκινούσε από τα 30KHz – 200KHz. Παρείχε υπηρεσίες όπως μηνύματα κειμένου SMS, εικόνες με πολυμέσα, μηνύματα MMS. Χρησιμοποιούσε διαμόρφωσης ψηφιακής τεχνικής όπως TDMA και CDMA. Η TDMA διαμόρφωση διαιρούσε τα σήματα σε χρονικά διαστήματα. Η CDMA έδινε σε κάθε χρήστη από έναν ειδικό κατάλληλο κωδικό ώστε να επικοινωνεί μέσω ενός πολυπλέκτη φυσικού καναλιού. [21]

2.2.3 Δίκτυα 3ης γενιάς

Το δίκτυο τρίτης γενιάς ανακοινώθηκε το 2000. Ο στόχος του 3G ήταν να επιτύχει αυξημένες ταχύτητες μετάδοσης δεδομένων από 144kbps έως 384kbps σε ευρείες περιοχές κάλυψης και 2Mbps σε τοπικές περιοχές κάλυψης. Το 3G προσέφερε προηγμένες νέες υπηρεσίες στους χρήστες του εν συγκρίσει με το αυτό της 1ης (1G) και 2ης (2G) γενιάς. Μαζί με την υπηρεσία φωνητικής επικοινωνίας περιλάμβανε υπηρεσίες δεδομένων, προσβασιμότητα σε τηλεόραση/βίντεο, περιήγηση στο Internet, ηλεκτρονικό ταχυδρομείο, και αναζήτηση δεδομένων για φαξ και χάρτες πλοήγησης. Είχε εύρος ζώνης 15MHz - 20MHz όπου χρησιμοποιήθηκε για υψηλή ταχύτητα πρόσβασης στο διαδίκτυο, και δυνατότητα βίντεο κλήσεων. Καθιερώθηκε από την οργάνωση 3GPP που πληροί τα πρότυπα IMT-2000 [22].

2.2.4 Δίκτυα 4ης γενιάς

Το δίκτυα 4ης γενιάς ανακοινώθηκε και άρχισε να χρησιμοποιείται στα τέλη του 2000 και βασίστηκε στο πρωτόκολλο IP(Internet Protocol). Ο βασικός στόχους του 4G είναι να παρέχει υψηλές ταχύτητες και ποιότητα, με μεγάλη χωρητικότητα καναλιού, ασφάλεια και χαμηλό κόστος για τις υπηρεσίες φωνής, δεδομένων, πολυμέσων και διαδικτύου μέσω του πρωτοκόλλου IP. Ο λόγος μετάβασης σε ένα δίκτυο που βασίζεται σε πρωτόκολλο IP είναι να υπάρχει μια κοινή πλατφόρμα τεχνολογίες για όλες τις εφαρμογές που έχουν αναπτυχθεί μέχρι σήμερα. Η τεχνολογία 4G έχει τη δυνατότητα να παρέχει ταχύτητες έως 100Mbps και 1Gbps. Η τεχνολογία 4G ενσωματώνει διάφορες προ-υπάρχουσες και μελλοντικές τεχνολογίες ασύρματης ζεύξης όπως OFDM, MC-CDMA, LAS-CDMA και Network - LMDS για την παροχή ελεύθερης κίνησης και αδιάληπτης περιαγωγής και μετάβασης από μια τεχνολογία σε μια άλλη. Το LTE και το WiMAX αναπτύχθηκαν ως κύριες τεχνολογίες του 4G. Η πρώτη επιτυχημένη δοκιμή στο πεδίο για το 4G πραγματοποιήθηκε στην Ιαπωνία το 2005 [18].

2.2.5 Δίκτυα 5ης Γενιάς

ΣΤο δίκτυο 5ης γενιάς ορίζεται ένας μεγάλος ασύρματος κόσμος που θα υποστηρίζει τα δίκτυα IPv6. Το 5G δικαίως αποκαλείται ως ο καλύτερος και πραγματικά μεγαλύτερος παγκόσμιος ασύρματος κόσμος ή Παγκόσμιος Ασύρματος Ιστός WWW, καθώς δεν το περιορίζει τίποτα. Το πρωτόκολλο IPv6 είναι το βασικό πρωτόκολλο επικοινωνίας για τη λειτουργία του 4G, και 5G. Στους στόχους του 5G είναι η παροχή μιας απεριόριστης πρόσβασης ταυτόχρονα σε πληροφορίες με δυνατότητες χρήσης δεδομένων από όλους, πάντα, παντού και ανά πάση στιγμή, για το όφελος του κόσμου. Η τεχνολογία του 5G καλύπτει όλα τα προηγμένα χαρακτηριστικά των παλαιότερων γενεών και καθιστούν την κινητή τηλεφωνία πιο ισχυρή και με μεγαλύτερη αξίωση στο μέλλον. Το δίκτυο 5G είναι αμιγώς βασισμένος στο IP πρωτόκολλο για τη λειτουργικότητα των κινητών συσκευών, ασύρματων δικτύων και κόμβων ενώ οι δραστηριότητες ενεργοποιήσεις, λειτουργίας, και παροχής υπηρεσιών έχουν ήδη ξεκινήσει από το 2020 και σε κάποιες περιοχές από κάποιους παρόχους είναι διαθέσιμες για το ευρύ κοινό [18].

2.2.6 Σύγκριση γενναίων κινητής τηλεφωνίας.

Ο πίνακας που ακολουθεί δίνει την πλήρη αποτύπωση των χαρακτηριστικών για όλες τις γενιές κινητής τηλεφωνίας από το έτος διάθεσης προς χρήση, ως και υπηρεσίες που προσφέρει στο κοινό.

Γενιά	1G	2G	3G	4G	5G
Έτος ανακοίνωσης	1970-198	1980-1990	1990-2000	2000-2010s	2015
Ταχύτητα	2.4Kbps	64Kbps	2Mbps	200Mbps-1Gbps	1Gbps ++
Τεχνολογία	Αναλογική κυψελοειδής	Ψηφιακή κυψελοειδής	Ευζωνική	Ενοποιημένο IP και συνδυασμός ευρυζωνικού	4G+www
Πρότυπα	AMPS	GSM, PDC, IS-95, IS-136, EDGE, GPRS	CDMA 2000, UMTS, TD-SCDMA, WCDMA	LTE, WiMAX	LAS-CDMA, UNB, Network LMDS, IPv6
Πολυπλεξία	FDMA	TDMA,CDMA	CDMA	CDMA	CDMA
Μεταγωγή	Κυκλώματος	Κυκλώματος και πακέτου	Πακέτο αντί για κύκλωμα για την ασύρματη διεπαφή	Πακέτου	Πακέτου δικτύου
Δίκτυο κορμού	PSTN	PSTN and Packet Network	Packet Network	Internet	Internet

Υπηρεσίες	Μόνο φωνή	Ψηφιακή φωνή και σύντομα μηνύματα, δεδομένα σε πακέτα.	Βίντεο με ενσωματωμένα ποιοτικό ήχο	Φορητές συσκευές για δυναμική πρόσβαση σε πληροφορίες	Φορητές συσκευές για δυναμική πρόσβαση σε πληροφορίες, με τεχνολογία AI
------------------	-----------	--	-------------------------------------	---	---

Πίνακας 1. Σύγκριση γενναίων κινητής τηλεφωνίας [18]

2.2.7 Υλοποίηση με LTE ή WiMAX;

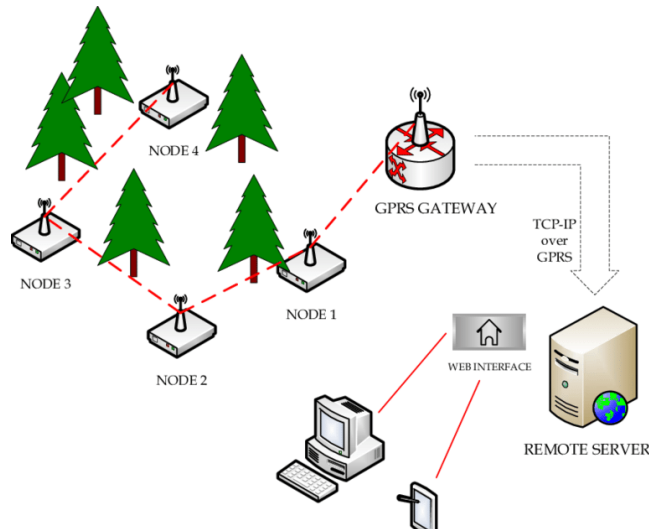
Το WiMAX είναι μια τεχνολογία η οποία αναπτύχθηκε στο κόσμο των υπολογιστών, αφού είναι μια επέκταση του WiFi, και δεν μπορεί να στηρίξει υποδομές κινητής τηλεφωνίας... Οι ομάδα έρευνας και ανάπτυξης της υπηρεσίας δεν μπόρεσαν να σχεδιάσουν κατάλληλα το WiMAX για το πλαίσιο ενός κυψελοειδούς δικτύου, με αποτέλεσμα να δημιουργηθούν μεγάλα λάθη Το WiMAX είναι ένα πρότυπο τεχνολογίας του 4G που μπορεί να σε σταθερά δίκτυα. Από την άλλη πλευράς μιλώντας για δίκτυα κυψελών το LTE και η ομάδα ανάπτυξης κατάφερε να αποφύγει τα λάθη του WiMAX και μπόρεσε να λειτουργήσει πολύ καλά σε μεγάλα αστικά και υπεραστικά δίκτυα λόγω της πολλαπλής πρόσβασης χρηστών, του χρονοπρογραμματισμού, του ελέγχου ισχύος που αποτελούν τα “χρυσά κλειδιά” της επιτυχίας του LTE ως προς το WiMAX [23].

Με βάση τον παραπάνω πίνακα και τις πολύ σημαντικές διαφορές του LTE ως προς το WiMAX στο σημείο αυτό θα πρέπει να αναφέρουμε πως για την δική μας υλοποίηση θα κάνουμε χρήση της 4ης γενιάς κινητής τηλεφωνίας αντί των προηγούμενων λόγω μεγαλύτερης ταχύτητας, παροχής Internet μέσω της ενοποιημένης τεχνολογίας IP και ευρυζωνικότητας. Τέλος μέσω του προτύπου LTE, θα μπορέσουμε να υλοποιήσουμε και να αναπτύξουμε την ανθεκτική πύλη δικτύου για δίκτυο ασύρματων αισθητήρων, που υποστηρίζει τέτοιες τεχνολογίες, σε σύγκριση με αυτό του WiMAX.

2.3 Δίκτυα ασύρματων αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων WSN έχουν κερδίσει την παγκόσμια προσοχή τα τελευταία χρόνια. Ειδικά με την εξάπλωση της τεχνολογίας των μικροηλεκτρομηχανικών συστημάτων MEMS τους έχουν διευκολύνει την ανάπτυξη έξυπνων αισθητήρων. Αυτοί οι αισθητήρες είναι μικροσκοπικοί, με περιορισμένους πόρους επεξεργασίας και υπολογισμού, και είναι οικονομικοί σε σχέση με τους παραδοσιακούς αισθητήρες. Αυτοί οι κόμβοι αισθητήρων μπορούν να ανιχνεύσουν, να μετρήσουν και να συγκεντρώσουν πληροφορίες από το περιβάλλον με την διαδικασία λήψης αποφάσεων, μπορούν να μεταδώσουν την συλλογή των δεδομένων στον χρήστη. Η εξοικονόμηση ενέργειας σε ένα ασύρματο δίκτυο αισθητήρων μπορεί να αυξήσει τη διάρκεια ζωής του δικτύου, να παρέχει αποτελεσματική και αξιόπιστη ασύρματη επικοινωνία, λόγω της έξυπνης τοποθέτησης των αισθητήρων του, με βάση την κάλυψη ασφάλειας και αποτελεσματικής διαχείρισης, αποθήκευσης, και συγκέντρωσης των δεδομένων. Για αξιόπιστη επικοινωνία, είναι απαραίτητες υπηρεσίες όπως έλεγχος συμφόρησης, ενεργή παρακολούθηση για απώλειες δεδομένων και ανάκτηση τους μέσω των απεσταλμένων πακέτων για την εγγυημένη λήψη αποφάσεων. Η τοποθέτηση των αισθητήρων παίζει πολύ σημαντικό ρόλο στο δίκτυο και την κάλυψη επικοινωνίας. Όσο πιο αραιή είναι η τοποθέτηση τόσο περισσότερο προάγεται το δίκτυο σε επικοινωνία

μεγάλων αποστάσεων με υψηλή κατανάλωση ενέργειας. Αντιθέτως όσο πιο πυκνή γίνεται η τοποθέτηση των αισθητήρων το δίκτυο οδηγείται σε επικοινωνία μικρών αποστάσεων αλλά τόσο μικρότερη κατανάλωση ενέργειας υπάρχει. Ο συνολικός αριθμός των αισθητήρων στο δίκτυο και η τοποθέτησή τους καθορίζουν τον βαθμό κάλυψης του δικτύου. Ανάλογα με την εφαρμογή, μπορεί να απαιτείται υψηλότερος βαθμός κάλυψης για να αυξηθεί η ακρίβεια των δεδομένων [24].



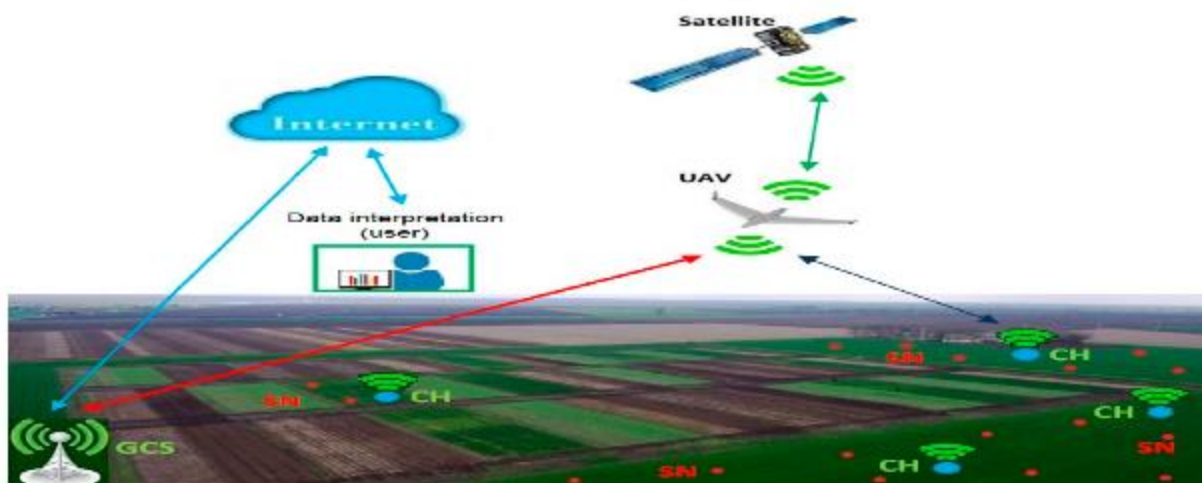
Εικόνα 15. Τοπολογία δικτύου ασυρμάτων αισθητήρων [F11]

2.3.1 Είδη ασύρματων αισθητήρων

Σε αυτή την ενότητα θα παρουσιάσουμε και θα αναλύσουμε τα διάφορα είδη ασύρματων αισθητήρων που χρησιμοποιούνται αναλόγως της περιοχής ενδιαφέροντος

2.3.2 Αισθητήρες επιφάνειας

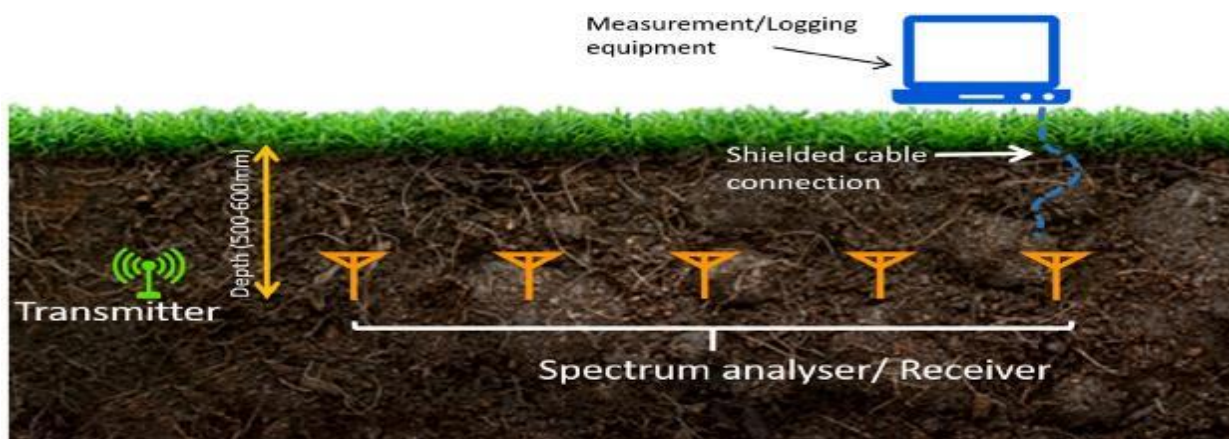
Οι αισθητήρες επιφάνειας αποτελούνται συνήθως από εκατοντάδες έως χιλιάδες φθηνούς αισθητήρες που εγκαθίστανται σε μια συγκεκριμένη περιοχή, είτε με αυθαίρετο τρόπο είτε με προγραμματισμένο τρόπο. Κατά την αυθαίρετη εγκατάσταση, οι αισθητήρες μπορούν να εντοπιστούν από ένα αεροπλάνο και να τοποθετηθούν τυχαία στην επιθυμητή περιοχή. Κατά την προγραμματισμένη εγκατάσταση υπάρχει οπτική πλέγματος, όπου βοηθά στην βέλτιστη τοποθέτηση καθώς και χάρτες 2-διάστατης (2D) και 3-διάστατης (3D) τοποθέτησης. Στους αισθητήρες επιφάνειας η αξιόπιστη επικοινωνία είναι πολύ σημαντική. Οι αισθητήρες πρέπει να είναι σε θέση να στέλνουν με σωστό τρόπο τα δεδομένα τους προς τον σταθμό λήψης. Η ενέργεια της μπαταρίας είναι περιορισμένη και ενδέχεται να μην είναι επαναφορτιζόμενη. Οι αισθητήρες επιφάνειας μπορούν να εξοπλιστούν με εναλλακτικές πηγές ενέργειας, όπως τα ηλιακά panel. Παρ' όλα αυτά, σημαντικό για τους αισθητήρες είναι να εξοικονομούν ενέργεια, καθώς αυτό επιτυγχάνεται με την χρήση βέλτιστης δρομολόγησης, την κατά τόπους μικρή εμβέλεια μετάδοσης, την συγκέντρωση δεδομένων μέσα στο δίκτυο, με ελάχιστες καθυστερήσεις [24].



Εικόνα 16. Δίκτυο ασυρμάτων αισθητήρων επιφάνειας [F12]

2.3.3 Αισθητήρες υπεδάφους

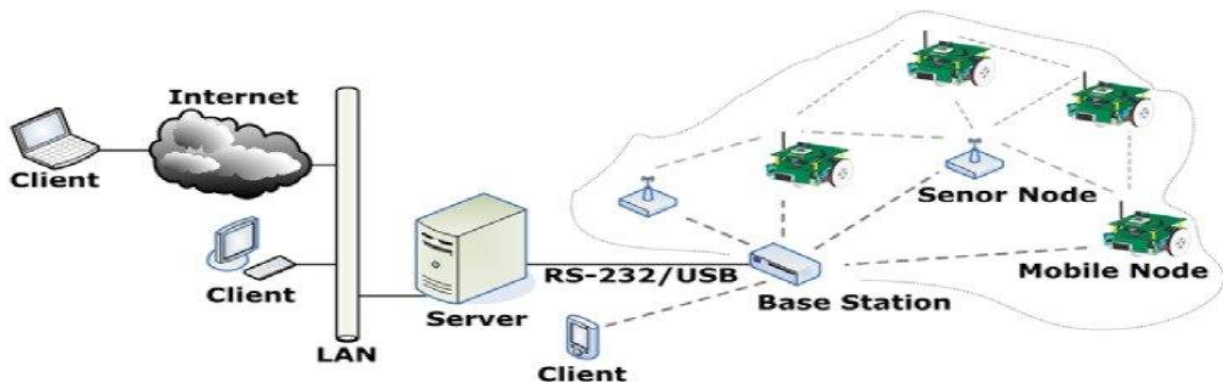
Οι αισθητήρες υπεδάφους αποτελούνται από έναν αριθμό αισθητήρων που θάβονται κάτω από το έδαφος σε σπηλιές ή ορυχεία και χρησιμοποιούνται για την παρακολούθηση των ενδογεωγραφικών συνθηκών. Επιπλέον κόμβοι συλλογής τοποθετούνται επάνω από το έδαφος για να μεταφέρουν πληροφορίες από τους αισθητήρες στον βασικό σταθμό. Ένα τέτοιο είδος δικτύου είναι πιο ακριβό από εκείνο της επιφάνειας όσον αφορά τον εξοπλισμό, την ανάπτυξη και τη συντήρηση. Οι αισθητήρες που βρίσκονται υπόγεια είναι ακριβοί επειδή πρέπει να επιλεγθούν κατάλληλα εξαρτήματα εξοπλισμού για να εξασφαλιστεί η αξιόπιστη επικοινωνία μέσω του εδάφους, των βράχων, του νερού και άλλων μεταλλικών συστατικών. Το υπόγειο περιβάλλον καθιστά την ασύρματη επικοινωνία πρόκληση λόγω απωλειών σήματος και υψηλών επιπέδων απόσβεσης. Σε αντίθεση με τους αισθητήρες επιφάνειας, η ανάπτυξη ενός τέτοιου δικτύου, απαιτεί προσεκτικό σχεδιασμό λαμβάνοντας υπόψη τις ενεργειακές και οικονομικές παραμέτρους. Και αυτοί οι αισθητήρες είναι εξοπλισμένοι με περιορισμένη ισχύ μπαταρίας και αφού τοποθετηθούν στο έδαφος, είναι δύσκολο να επαναφορτιστεί ή να αντικατασταθεί η μπαταρία ενός αισθητήρα. Ως εκ τούτου, ένας βασικός στόχος είναι η εξοικονόμηση ενέργειας για την αύξηση της διάρκειας ζωής του δικτύου, κάτι που μπορεί να επιτευχθεί με την υλοποίηση αποδοτικού πρωτοκόλλου επικοινωνίας [25,26].



Εικόνα 17. Δίκτυο ασυρμάτων αισθητήρων υπεδάφους [F13]

2.3.4 Κινητοί αισθητήρες

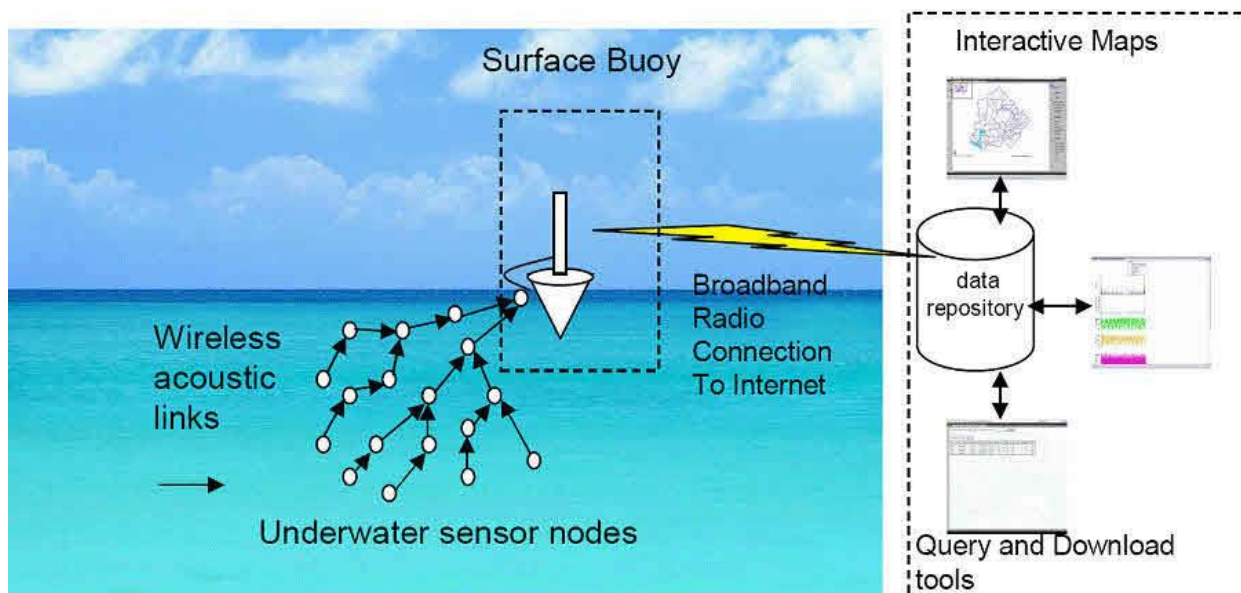
Οι κινητοί αισθητήρες αποτελούνται από ένα πλήθος αισθητήρων που μπορούν να μετακινούνται αυτόνομα και να αλληλοεπιδρούν με το φυσικό περιβάλλον. Οι κινητοί αισθητήρες έχουν τη δυνατότητα ανίχνευσης, υπολογισμού και επικοινωνίας όπως οι αισθητήρες επιφάνειας. Η κύρια διαφορά είναι ότι οι κινητοί κόμβοι έχουν τη δυνατότητα να μετακινούνται και να οργανώνονται μέσα στο δίκτυο. Ένα κινητό δίκτυο αισθητήρων μπορεί να ξεκινήσει με ορισμένους αρχικούς κόμβους και στη συνέχεια οι κόμβοι μπορούν να διαχωριστούν για να συλλέξουν πληροφορίες. Οι πληροφορίες που συλλέγονται από έναν κινητό κόμβο μπορούν να μεταφερθούν σε έναν άλλο κινητό κόμβο όταν είναι εντός εμβέλειας ή ο ένας δίπλα στον άλλο. Μια άλλη σημαντική διαφορά είναι η διανομή των δεδομένων. Στους σταθερούς αισθητήρες τα δεδομένα μπορούν να διανεμούνται χρησιμοποιώντας σταθερή δρομολόγηση, ενώ στους κινητούς χρησιμοποιείται δυναμική δρομολόγηση. Οι δυσκολίες σε αυτό το είδος δικτύου περιλαμβάνουν την αναπτυξιακή διαδικασία, την εντοπισμό θέσης, την αυτοοργάνωση, την πλοήγηση και τον έλεγχο, καθώς και την κάλυψη, την ενέργεια, τη συντήρηση και την επεξεργασία των δεδομένων [27].



Εικόνα 18 Δίκτυο κινητών ασυρμάτων αισθητήρων υπεδάφους [F14]

2.3.5 Υποθαλάσσιοι αισθητήρες

Οι υποθαλάσσιοι αισθητήρες αποτελούνται από έναν αριθμό αισθητήρων που είναι τοποθετημένοι κάτω από την επιφάνεια της θάλασσας. Αντίθετα από τους αισθητήρες επιφάνειας, οι υποθαλάσσιοι αισθητήρες είναι πιο ακριβοί και απαιτείται λιγότερος αριθμός αισθητήρων. Αυτόνομα υποθαλάσσια οχήματα χρησιμοποιούνται για εξερεύνηση ή συγκέντρωση δεδομένων από τους αισθητήρες. Η τοποθέτηση τους απαιτείται σε σχέση με αυτή με τον υπολοίπων. Η υποθαλάσσια ασύρματη επικοινωνία επιτυγχάνεται μέσω της μετάδοσης ακουστικών κυμάτων. Μια πρόκληση στην υποθαλάσσια ακουστική επικοινωνία είναι το περιορισμένο εύρος ζώνης, η μεγάλη καθυστέρηση διάδοσης και το πρόβλημα της εξασθένισης του σήματος, των περιβαλλοντικών συνθηκών. Οι υποθαλάσσιοι αισθητήρες μπορούν να αυτορυθμίζονται, ενώ προσαρμόζονται κατάλληλα στις αυστηρές υποθαλάσσιες συνθήκες. Οι υποθαλάσσιοι αισθητήρες είναι εξοπλισμένοι με μια περιορισμένη μπαταρία που δεν μπορεί να αντικατασταθεί ή να φορτιστεί ξανά. Το πρόβλημα της εξοικονόμησης ενέργειας περιλαμβάνει την ανάπτυξη αποδοτικών τεχνικών υποθαλάσσιας επικοινωνίας και δικτύωσης [28,29].



Εικόνα 19. Δίκτυο ασυρμάτων υποθαλάσσιων αισθητήρων [F15]

2.4 Εφαρμογές στα ασύρματα δίκτυα αισθητήρων

Οι εφαρμογές των ασύρματων δικτύων αισθητήρων μπορούν να χωριστούν σε δύο κατηγορίες. Η μια κατηγορία είναι η παρακολούθηση και η άλλη η ανίχνευση. Οι εφαρμογές παρακολούθησης περιλαμβάνουν την διαχείριση του περιβάλλοντος σε εσωτερικό ή εξωτερικό χώρο, την παρακολούθηση της υγείας ενός ασθενούς, την παρακολούθηση ενέργειας, τοποθεσίας των αποθεμάτων και προϊόντων την εξ αποστάσεως αυτοματοποιημένη διεργασία και χειρισμό αντικειμένων τόσο σε εργοστάσια νοσοκομεία καθώς και την σεισμική δραστηριότητα. Οι εφαρμογές ανίχνευσης περιλαμβάνουν την ανίχνευση αντικειμένων, ζώων, ανθρώπων και οχημάτων. Παρακάτω θα περιγράψουμε μερικά παραδείγματα εφαρμογών που έχουν υλοποιηθεί και δοκιμαστεί σε πραγματικό περιβάλλον [24].

2.4.1 The Macroscope of Redwood

Είναι μια εφαρμογή που παρακολουθεί και καταγράφει τα ερυθρόδεντρα στην περιοχή Sonoma της Καλιφόρνια. Κάθε αισθητήρας μετρά την θερμοκρασία του αέρα, τη σχετική υγρασία και τη φωτοσυνθετική ενεργή ηλιακή ακτινοβολία. Οι αισθητήρες τοποθετούνται σε διάφορα ύψη του δέντρου. Οι βιολόγοι παρακολουθούν τις αλλαγές των χωρικών κλιματικών διαφορών γύρω από ένα ερυθρόδεντρο και επικυρώνουν τις βιολογικές θεωρίες τους [30].

2.4.2 Εφαρμογές σε εργοστάσια και πετρελαιοφόρα

Οι εφαρμογές σε εργοστάσια και πετρελαιοφόρα επικεντρώνονται στην προληπτική συντήρηση εξοπλισμού χρησιμοποιώντας τις δονήσεις που συλλέγονται από αισθητήρες για να προβλέψουν τυχόν αστοχία του εξοπλισμού. Με βάση τις απαιτήσεις της εφαρμογής και την έρευνα του χώρου, αναπτύσσεται η αρχιτεκτονική του δικτύου, έτσι ώστε να καλύψει τις ανάγκες των δεδομένων της εφαρμογής. Τέτοιες εφαρμογές έχουν υλοποιηθεί σε ένα εργοστάσιο κατασκευής ημιαγωγών και σε ένα πετρελαιοφόρο πλοίο στη Βόρεια Θάλασσα [31].

2.4.3 Εφαρμογές υποθαλάσσιας παρακολούθησης

Η ανάπτυξη ενός δικτύου υποθαλάσσιων αισθητήρων βοήθησε στην παρακολούθηση των κοραλλιογενών ύφαλων και της αλιείας. Το δίκτυο αισθητήρων αποτελείται από στατικούς και κινητούς υποβρύχιους αισθητήρες. Οι κόμβοι επικοινωνούν μέσω συνδέσμων από σημείο σε σημείο χρησιμοποιώντας οπτικές επικοινωνίες υψηλής ταχύτητας, και ένα ακουστικό πρωτόκολλο που ονομάζεται TinyOS. Επίσης διαθέτουν διάφορες συσκευές ανίχνευσης συμπεριλαμβανομένων αισθητήρων θερμοκρασίας πίεσης και εικόνας. Οι κινητοί κόμβοι μπορούν να εντοπίσουν και να μετακινηθούν πάνω από τους στατικούς κόμβους για να συλλέξουν δεδομένα και να εκτελέσουν λειτουργίες συντήρησης του δικτύου ως προς την ανάπτυξη, την αναστολή και την ανάκτηση. Οι προκλήσεις της ανάπτυξης αισθητήρων σε ένα υποβρύχιο περιβάλλον σίγουρα αποτελούν πολύ σημαντικό ενδιαφέρον [32].

2.4.4 Εφαρμογές παρακολούθησης ηφαιστειών

Η παρακολούθηση ηφαιστειών με τη χρήση ασύρματων αισθητήρων δικτύου μπορεί να βοηθήσει στη γρηγορότερη ανίχνευση ηφαιστειακής κίνησης. Ο εξοπλισμός είναι μικρότερος, ελαφρύτερος και καταναλώνει λιγότερη ενέργεια. Η συλλογή δεδομένων από ηφαίστεια περιλαμβάνει την αξιόπιστη ανίχνευση γεγονότων, την αποτελεσματική συλλογή δεδομένων, τους υψηλούς ρυθμούς μετάδοσης δεδομένων και την αραιή ανάπτυξη των κόμβων. Ένα τέτοιο δίκτυο εγκαταστάθηκε στο ηφαίστειο Revendador στο βόρειο Ecuador, και αποτελούνταν από 16 κόμβους αισθητήρων [33].

2.5 Ασύρματα δίκτυα αισθητήρων για προστασία κρίσιμων υποδομών

Με γνώμονα ότι τα κρίσιμα δίκτυα υποδομών καλύπτουν μεγάλη γεωγραφική έκταση, οι μηχανισμοί παρακολούθησης της προστασίας τους πρέπει να είναι κλιμακούμενοι. Για αυτό το λόγο, τα ασύρματα δίκτυα αισθητήρων (WSNs) αναδεικνύονται ως η μόνη και αξιόπιστη λύση. Συγκεκριμένα, μπορούν να αναπτυχθούν σε μεγάλη κλίμακα ώστε να καλύψουν μεγάλες γεωγραφικές περιοχές, και λόγω του χαμηλού κατασκευαστικού τους κόστους παρέχουν μια πολύ οικονομική λύση παρακολούθησης χωρίς την ανάγκη για επιπλέον υποδομή. Ένα άλλο πλεονέκτημα αυτών των αναπτύξεων είναι ότι η κατανομημένη δομή ενός ασύρματου δικτύου αισθητήρων αυξάνει την ανθεκτικότητα του σε κρίσιμες καταστάσεις. Αυτή η βελτιωμένη ανθεκτικότητα επιτυγχάνεται εξ' αιτίας της μεγάλης κλίμακας που δεν επηρεάζει το σύνολό του για αστοχίες ή επιθέσεις. Σε πολύ κρίσιμες καταστάσεις, όχι επαρκώς λειτουργικά δίκτυα αισθητήρων δεν θα μπορούσαν να παρέχουν αρκετές πληροφορίες σχετικά με την κρίσιμη υποδομή ώστε να βοηθήσουν τον χειριστή να αποτρέψει περαιτέρω ζημιά και να ξεκινήσει τη διαδικασία αποκατάστασης. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η χρησιμότητα αυτών των δικτύων για την προστασία κρίσιμων υποδομών καθορίζεται κυρίως από την αξιοπιστία του ίδιου του δικτύου. Πτυχές του συστήματος, όπως η επικάλυψη, η ακεραιότητα, η πραγματικού χρόνου ενημέρωση, καθώς επίσης η ασφάλεια και η διαθεσιμότητα, είναι ουσιώδεις απαιτήσεις για να καταστεί αξιόπιστο το ασύρματο δίκτυο αισθητήρων (WSNs) και συνεπώς, οι υπηρεσίες παρακολούθησης που παρέχει. Η σωστή χρήση του έχει σημαντική επίδραση στην αξιοπιστία του συστήματος ελέγχου των κρίσιμων υποδομών. Ειδικότερα, είναι γνωστό ότι τα ασύρματα

κανάλια επικοινωνίας είναι περισσότερο ευάλωτα στο περιβαλλοντικό θόρυβο, και στις κακόβουλες πράξεις, όπως αναφέραμε και σε προηγούμενο κεφάλαιο μας, που καθιστά το δίκτυο λιγότερο αξιόπιστο από τις ενσύρματες συνδέσεις [34].

Ιδιωτικά δίκτυα, εφαρμογές, πλατφόρμες ανοιχτού κώδικα και υλοποιήσεις

3.1 Ιδιωτικά δίκτυα

Με βάση το άρθρο "Για να είστε ασφαλείς, πρέπει να είστε ξεχωριστοί από το δημόσιο Διαδίκτυο", δηλώνει ο Rob Schwartz, CEO της Anterix, μίας από τις μεγαλύτερες εταιρίες ιδιωτικού δικτύου για λειτουργίες LTE, στις Ηνωμένες Πολιτείες [35]. Τα κεφάλαια της εταιρείας διπλασιάστηκαν σε λιγότερο από έξι μήνες από τον Δεκέμβριο του 2020 έως τον Ιούνιο του 2021, καθώς αυξήθηκε η ζήτηση για ιδιωτικά δίκτυα ανάμεσα στις αμερικανικές εταιρείες. Η IDC [36], ο παγκόσμιος παρόχος αγοραπωλησιών, συμβουλευτικών υπηρεσιών και εκδηλώσεων για τις αγορές τεχνολογίας πληροφορικής, τηλεπικοινωνιών και καταναλωτικής τεχνολογίας είχε προβλέψει ότι η ιδιωτική υποδομή (για τα LTE/5G) θα αυξηθεί από 945 εκατομμύρια δολάρια το 2019 σε περίπου 5,7 δισεκατομμύρια δολάρια το 2024 [37].

Τα βασικά πλεονεκτήματα ενός ιδιωτικού δικτύου είναι η υψηλή αξιοπιστία και ασφάλεια, διατηρώντας παράλληλα υψηλή ταχύτητα και λιγότερες καθυστερήσεις. Το ιδιωτικό δίκτυο λύνει προβλήματα που δεν μπορούν να χειριστούν οι δημόσιες υποδομές ή τα ασύρματα δίκτυα Wi-Fi που εγκαθίστανται από τις επιχειρήσεις. Είναι ανθεκτικό στην παρεμβολή, καλά προστατευμένο, ενώ μεγάλη κάλυψη σήματος σε εσωτερικούς χώρους. Με την υλοποίηση ενός τέτοιου δικτύου, η εταιρεία αποκτά ένα δικό της ελεγχόμενο και σταθερό ψηφιακό περιβάλλον για τη μετάδοση δεδομένων, και ασφαλής χρήσης σύγχρονων ψηφιακών εργαλείων όπως είναι η φωνή το βίντεο η απομακρυσμένη παρακολούθηση και ο έλεγχος σε αισθητήρες και ρομποτικούς βραχίονες. Πολλές μεγάλες εταιρίες στο χώρο της βιομηχανίας έχουν προγραμματίσει την μετάβαση τους σε αυτή την υλοποίηση. Νέες ολόκληρες γραμμές παραγωγής εργοστασίων, που οι οποίες εξυπηρετούνται από το Διαδίκτυο των Πραγμάτων (IoT) για τον καλύτερο έλεγχο, του κάθε σταδίου παραγωγής, θα χρησιμοποιήσουν τη λύση αυτή με ζωντανή εικόνα από κάμερες υψηλής ανάλυσης. Τα συστήματα παρακολούθησης μέσω εικόνας έχουν αρχίσει και αποκτούν ένα ισχυρό ρόλο στην επιβολή του νόμου, και στα μέτρα τήρησης του κώδικα οδικής συμπεριφοράς στους δρόμους, καθώς επίσης και στην παρακολούθηση του εναέριου χώρου κοντά στα αεροδρόμια. Η τεχνολογία αυτή, που μελλοντικά θα βασιστεί και στην τεχνολογία του 5G, θα κατέχει μια πολύ ισχυρή θέση σε τέτοιου είδους λύσεις [38].

3.2 Τεχνολογίες σε ιδιωτικά δίκτυα

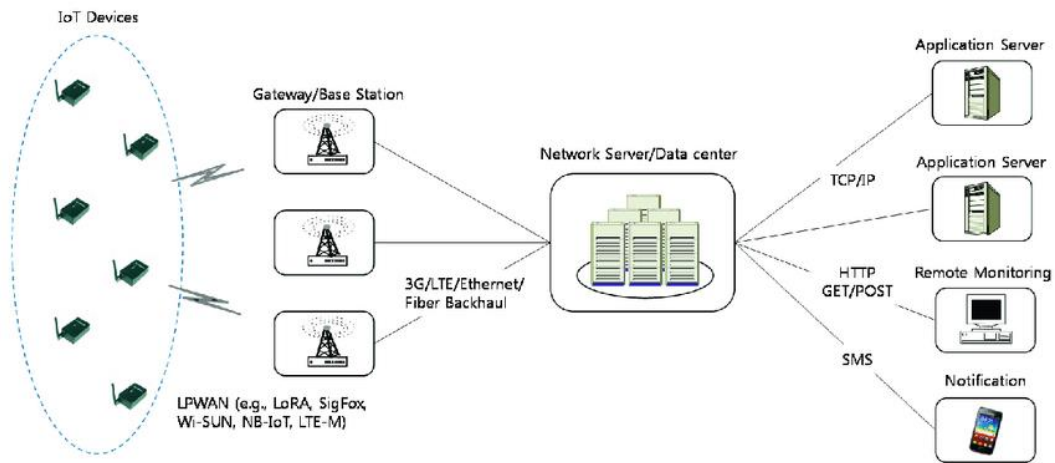
Σε αυτή την ενότητα θα αναλύσουμε τις τεχνολογίες μέσα από τις οποίες μπορεί να υλοποιηθεί ένα ιδιωτικό δίκτυο

3.2.1 LPWAN

Τα LPWANs αποτελούν μια σύγχρονη τεχνολογία επικοινωνίας.. Η τοπολογία τους βασίζεται στην δομή του αστέρα και αποτελείται από συσκευές τερματικών κόμβων, μία πύλη και ένα διακομιστή. Οι πύλες επικοινωνούν με το διακομιστή καθ' όλη την διάρκεια της σύνδεσης μέσω ευρυζωνικού συνδέσμου. Οι συσκευές τερματικών επικοινωνούν με το διακομιστή μέσω των ασύρματων συνδεδεμένων πυλών, ενώ οι πύλες λειτουργούν ως αναμεταδότες μεταξύ των αισθητήρων και του διακομιστή. Τα δίκτυα LPWAN δίκτυα επιβάλλουν περιορισμούς στην ισχύ που εκπέμπεται καθώς λειτουργούν σε ζώνες που έχουν παρασχεθεί κατάλληλες άδειες χρήσεις με συγκεκριμένες ραδιοσυχνότητες [39]. Επιτρέπουν εφαρμογές χαμηλού κόστους σε μεγάλες περιοχές, ενώ οι συσκευές μπορούν να καλύπτουν μεγάλες αποστάσεις. Αυτή η δυνατότητα επιτυγχάνεται με την μετάδοση πολύ χαμηλών ταχυτήτων φορτίου της τάξεως των μερικών kBit/s μεταξύ των κόμβων και των υψηλά τοποθετημένων κεραιών που έχουν τοποθετηθεί στις κορυφές των κτηρίων. Η τεχνολογία του LPWAN είναι κατάλληλη για πυκνές ή παχιές τοποθεσίες, για εφαρμογές μακροπρόθεσμης παρακολούθησης και αποτελεί την καλύτερη τεχνολογία που μπορεί να στείλει μικρά πακέτα δεδομένων σε μεγάλες αποστάσεις για μεγάλο χρονικό διάστημα, καθώς υποστηρίζεται στην μεγάλη διάρκεια της μπαταρίας [40,41,42]. Η τεχνολογία του IoT είναι συνυφασμένη με τα LP-WAN δίκτυα αφού μπορούν και καλύπτουν τις ανάγκες των αισθητήρων, καθώς μέσω των εγκαθιδρυμένων πρωτοκόλλων υπάρχει η δυνατότητα διπλής κατευθυνόμενης επικοινωνίας και παρέχει μεγάλη ασφάλεια από άκρο ως άκρο.

3.2.2 Αρχιτεκτονική δομή και τοπολογία του LPWAN

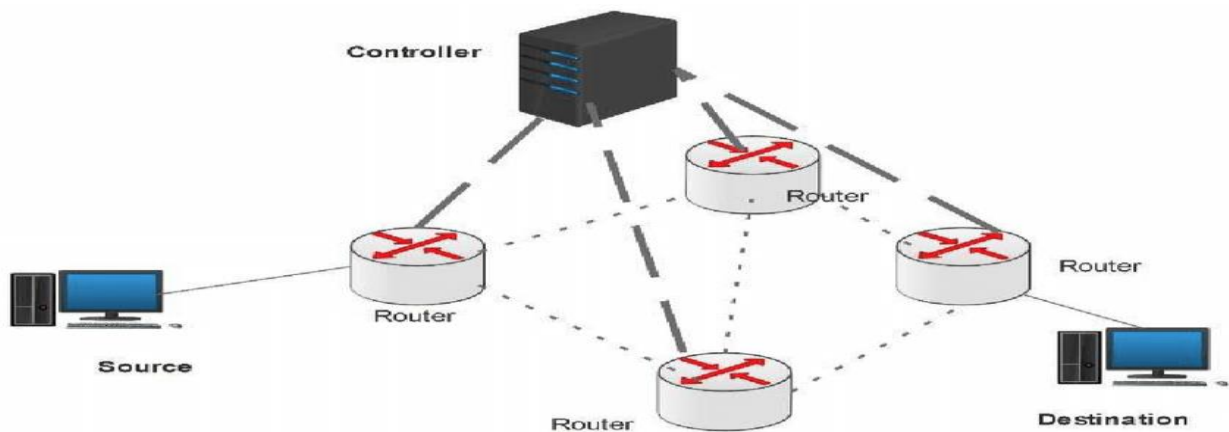
Τα δεδομένα συλλέγονται και αποστέλλονται μέσω ενός συγκεκριμένου ασύρματου κόμβου στο σταθμό λήψης και εν συνεχεία ασύρματα προς το δίκτυο του IoT. Ο σταθμός πρόσβασης περιλαμβάνει τον ασύρματο κόμβο για την ανταλλαγή δεδομένων κίνησης των συσκευών και τη διαχείριση των συσκευών, διατηρώντας την ακεραιότητα του ασύρματου συνδέσμου με δυνατότητα να διαχειρίζεται τα ποσοστά σφαλμάτων και ασφάλειας. Επίσης μπορεί να αλληλοεπιδράσει με την πύλη η οποία ονομάζεται επίσης και πυρήνας. Υπάρχουν διάφορες υλοποιήσεις βασισμένες σε πρότυπα τεχνολογία LPWAN. Ο πυρήνας ορίζει τη διαχείριση και τον έλεγχο της κίνησης των δεδομένων μεταξύ των κόμβων εντός του δικτύου και παρέχει το κατάλληλο κανάλι για την ανταλλαγή πληροφοριών μεταξύ του σταθμού πρόσβασης και του δικτύου IoT ενώ μπορεί και υποστηρίζει την ανταλλαγή συνδυασμένων δεδομένων μεταξύ των υποστηριζόμενων από το σταθμό πρόσβασης πρωτοκόλλων, με δυνατότητα μετάφρασης, και του δικτύου. Για τις υποστηριζόμενες τεχνολογίες του LPWAN, ο πυρήνας μπορεί να παρέχει αξιόπιστη λύση, και υποστήριξη ανάμεσα στους συνδεδεμένους κόμβους. Ο διακομιστής LPWAN είναι υπεύθυνος για την ενημέρωση των κόμβων εντός του δικτύου καθώς επίσης μοιράζεται ή ενισχύει τις λειτουργίες του πυρήνα ως προς την δρομολόγηση της κίνησης, την ασφάλεια των δεδομένων και χειρισμό σε πακέτα με προτεραιότητα.



Εικόνα 20. Η αρχιτεκτονική δομή του LPWAN [F16]

3.2.3 SDN

Η τεχνολογία SDN ήταν το πιο αναγνωρίσιμο θέμα της προηγούμενης δεκαετίας στον κόσμο των δικτύων λόγω της λύσης που υποσχέθηκε να παρέχει για τα ευρέως μεγάλα δίκτυα. Η κεντρικά ελεγχόμενη παρακολούθηση με τη χρήση λογισμικού μπορεί να αυξήσει την ταχύτητα του δικτύου και να παρέχει καλύτερη ποιότητα υπηρεσίας, τόσο στη φωνητική όσο και στη μετάδοση δεδομένων. Σε σύγκριση με τα κλασικά δίκτυα, το SDN μπορεί να παρέχει βελτιωμένη αρχιτεκτονική δικτύου τριών επιπέδων υπό την ίδια υποδομή. Το επίπεδο "εφαρμογής" είναι υπεύθυνο για την παρακολούθηση και την ισορροπία φορτίου, το επίπεδο "ελέγχου" αφορά την τοπολογία του δικτύου, και το επίπεδο "επιπέδου δεδομένων" είναι υπεύθυνο για τις φυσικές συνδέσεις του εξοπλισμού του δικτύου. Η αρχιτεκτονική του SDN που βασίζεται στο OpenFlow και αποτελεί κατάλληλη τεχνολογία τόσο για κινητά όσο και ασύρματα δίκτυα. Τα κοινά πρωτόκολλα επικοινωνίας για τις διαφορετικές τεχνολογίες κινητών δικτύων 3G, UMTS, WiMAX, 4G / LTE, Wi-Fi μπορούν να παρέχουν στους χρήστες τους πιο απλοποιημένη διαχείριση στο δίκτυο με καλύτερες και πιο αξιόπιστες εφαρμογές [43,44,45].



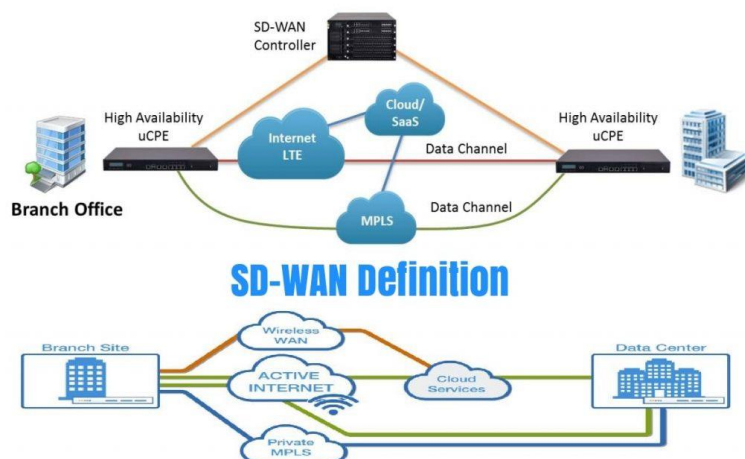
Εικόνα 21. Η αρχιτεκτονική δομή του SDN [F17]

3.3.3 SD_WAN

Το SD-WAN είναι μια νέα τεχνολογική υλοποίηση που λειτουργεί ως εναλλακτική λύση στην τεχνολογία επικοινωνίας WAN που χρησιμοποιείται σήμερα. Παρέχει κατάλληλες αυτοματοποιημένες διαδικασίες για καλύτερη παρακολούθηση των δεδομένων από σημείο σε σημείο (p2p). Αυτές οι αυτοματοποιημένες ενέργειες μπορούν να εξελίξουν το SD-WAN σε μια παραγωγική, σταθερή και αξιόπιστη λύση για μια οργάνωση . Ο όρος SD-WAN προέρχεται από τις λέξεις Software Define Wide Area Network, και αποτελεί μέρος μιας νέας εποχής εφαρμογής του SDN όπου διαχειρίζεται τη δρομολόγηση πακέτων μεταξύ υποκαταστημάτων υποδομών και κεντρικών γραφείων μια εταιρίας. Το SD-WAN μπορεί να παρέχει ισορροπημένη φόρτωση της κίνησης δεδομένων χρησιμοποιώντας πολλαπλά WANs και αξιοποιώντας τα προτερήματα του το ιδιωτικό δίκτυο χωρίζεται σε δύο επίπεδα, το επίπεδο "ελέγχου" και το επίπεδο "δεδομένων". Το επίπεδο "ελέγχου" διαχειρίζεται στο cloud ή σε υποδομές εγκατεστημένες στο χώρο. Μια εφαρμογή διαχείρισης λογισμικού είναι υπεύθυνη για τον τρόπο με τον οποίο τα "δεδομένα" θα μεταφερθούν στο δίκτυο, καθώς μπορούν να προωθούνται μέσω ξεχωριστών διαδρομών ανάλογα με την κίνηση του δικτύου και το προγραμματισμένο σχέδιο [46].

3.3.3.1 Αρχιτεκτονική του SD_WAN

Η αρχιτεκτονική του SD-WAN περιλαμβάνει τρία επίπεδα. Το Επίπεδο "δεδομένων" αποτελείται από Hardware και Software με παρόμοιες λειτουργίες κοντά σε δίκτυα IP, οι οποίοι μπορούν να απεικονίσουν το εύρος ζώνης προωθώντας τα δεδομένα, για παράδειγμα προς δίκτυα κινητής τηλεφωνίας 4G/LTE. Το επίπεδο "ελέγχου" είναι υπεύθυνο για τη βελτίωση του δικτύου, την παρακολούθηση της κίνησης στο δίκτυο και την παροχή βέλτιστης ποιότητας υπηρεσιών για όλα τα μεταδιδόμενα δεδομένα. Το επίπεδο εφαρμογής επιτρέπει στους διαχειριστές δικτύου διαμορφώσουν τις απαιτήσεις για ένα αποδοτικό δίκτυο με χαμηλό κόστος ενέργειας και υψηλή διαθεσιμότητα. Το SD-WAN παρέχει ασφαλείς συνδέσεις με κρυπτογραφημένη ανταλλαγή κλειδιών από άκρη σε άκρη, επιτρέποντας στους χρήστες να δημιουργήσουν μια νέα πολύπλοκη υποδομή δικτύου ανάμεσα σε MPLS και LTE για να αυξήσουν την εμπειρία τους σε κρίσιμες συνδέσεις. Το SD-WAN μπορεί να διαχειριστεί την κίνηση των δεδομένων παρέχοντας προτεραιότητα σε συγκεκριμένους κόμβους. Οι υπηρεσίες είναι ευέλικτες και προσαρμόσιμες , και η ποιότητα των υπηρεσιών για τη μετάβαση των δεδομένων είναι υψηλότερη λόγω της ισορροπίας φορτίου, καθώς το δίκτυο είναι κεντρικό και ελεγχόμενο ανά πάσα στιγμή [41].



Εικόνα 22. Η αρχιτεκτονική δομή του SDN_WAN [F18]

3.3.4 LTE

Τα LTE δίκτυα αναπτύσσονται ενεργά σε ιδιωτικά δίκτυα για επιχειρήσεις. Ένα ιδιωτικό δίκτυο LTE μπορεί να είναι τοπικό ή εθνικό. Για παράδειγμα μια επιχείρηση για την οποία απαιτείται η δημιουργία μιας ξεχωριστής τηλεπικοινωνιακής υποδομής ο πάροχος υπηρεσιών χτίζει ένα τοπικό δίκτυο για αυτήν, χρησιμοποιώντας μέρος του υπάρχοντος δικτύου του, καθώς επίσης είναι δυνατή η κατασκευή ενός εθνικού δικτύου. Τα ιδιωτικά δίκτυα χρειάζονται για κρίσιμες υποδομές, την αστυνομία τα ασθενοφόρα την πυροσβεστική και άλλα που μέχρι σήμερα χρησιμοποιείται η υπάρχουσα κάλυψη των παρόχων κινητής τηλεφωνίας για αυτόν τον σκοπό. Ας δούμε ένα παράδειγμα στην Ουκρανία όπου ο πάροχος υπηρεσιών δημιούργησε το LTE-1800. Μέσα στα 2 χρόνια πάλι στην η Ουκρανία θα εισαχθεί το LTE-900. Αυτό σημαίνει ότι θα υπάρχει μεγάλη κάλυψη, από το εθνικό δίκτυο και με αυτή την δυνατότητα οι Ουκρανική αστυνομία, το Υπουργείο Εκτάκτων Αναγκών ή άλλες ειδικές υπηρεσίες θα μπορούν να χρησιμοποιήσουν την υποδομή του κινητού παρόχου. Επίσης στην Αμερική, έτσι λειτουργεί το δίκτυο Firstnet. Το ιδιωτικό δίκτυο χτίζεται σχεδόν με τον ίδιο τρόπο με την κανονική κάλυψη του κινητού παρόχου. Τα στοιχεία είναι πάλι τα ίδια με την διαφορά ότι αυτό το δίκτυο έχει γεωγραφικό περιορισμό και χτίζεται ανά μεγάλη περιοχή [47]. Η υποδομή και το δίκτυο διαχειρίζονται και αναλύονται από κεντρικές ανεξάρτητες υπηρεσίες. Οι τρεις κύριες επιλογές για τη διαχείριση της υποδομής είναι:

1. **Αυτοδιαχείριση:** Η ίδια η εταιρία που το δημιούργησε μπορεί και να το υποστηρίξει, μέσω του κατάλληλου προσωπικού τους
2. **Εξωτερική ανάθεση:** Ο πάροχος που υλοποίησε την υποδομή την παραδίδει στην επιχείρηση για χρήση και μετά ασχολείται με την υπηρεσία και την ποιότητα.
3. **Πλήρης εξασφάλιση:** Στην περίπτωση πολλαπλών ιδιωτικών δικτύων, η κατασκευή, ο σχεδιασμός και η συντήρηση γίνονται από έναν προμηθευτή-πάροχο. Με γνώμονα ότι δεν είναι εύκολη η αγορά του απαραίτητου εξοπλισμού αλλά και η κατασκευή του από εταιρίες που δεν έχουν κάποια γνώση με αυτές τις υλοποιήσεις καθώς επίσης θα πρέπει να αποκτήσουν την κατάλληλη άδεια χρήσης συχνοτήτων, είναι πιο εύκολο για αυτές να συνεργαστούν με κατάλληλους με τους κινητούς φορείς, που ήδη διαθέτουν τέτοιες άδειες ώστε η διαδικασία θα είναι πολύ πιο γρήγορη και ευκολότερη.

Σήμερα, τα δίκτυα LTE χρησιμοποιούν ένα αδειοδοτημένο φάσμα συχνοτήτων που διατίθεται αποκλειστικά σε έναν φορέα κινητής τηλεφωνίας με δεδομένο ότι η διαδικασία για την απόκτηση μιας αδειοδότησης και χρήσης του φάσματος συχνοτήτων κινητής τηλεφωνίας είναι πολύπλοκη και συνήθως ακριβή. Η Qualcomm και πολλές άλλες εταιρείες του χώρου προσφέρουν τρόπους για τη χρήση του LTE σε μη αδειοδοτημένες συχνότητες, με χαρακτηριστικό παράδειγμα τη συχνότητα των 5 GHz που χρησιμοποιείται στα δίκτυα Wi-Fi.



Εικόνα 23. Η γενική εικόνα του LTE δικτύου [47]

Το LTE μπορεί να αναπτυχθεί από τον κάθε πάροχο στα 900MHz ,1800MHz ,700 MHz και 2.6 GHz. Επιπρόσθετα από το LTE υποστηρίζεται ένας μεγάλος αριθμός ευρυζωνικών καναλιών: 1.4 MHz, 3 MHz, 5 MHz,10 MHz, 15 MHz, 20 MHz.

3.3.4.1 Αρχιτεκτονική του LTE

Η αρχιτεκτονική δομή ενός LTE δικτύου σχετίζεται με την υλοποίηση του και πως οι κινητές συσκευές των χρηστών συνδέονται στο δίκτυο και αποκτούν πρόσβαση στις υπηρεσίες. Τα UEs κινητά τηλέφωνα συνδέονται με τις βάσεις σταθμούς eNodeBs - eNB μέσω των ραδιοσυχνοτήτων , και στην συνέχεια οι σταθμοί μεταδίδουν και λαμβάνουν πακέτα IP από και προς κύριο δίκτυο, το οποίο αποτελείται από ένα αρκετά μεγάλο αριθμό εισόδων, εξόδων, Internet, και σύνδεσης με άλλα κυψελοειδή δίκτυα. Το LTE χρησιμοποιεί αποκλειστικά την τεχνολογία μετάδοσης πακέτων που είναι βασισμένη στο πρωτόκολλο IP. Επιπρόσθετα να πούμε ότι στην αρχιτεκτονική του LTE, η “φωνή” μπορεί να ταξιδέψει στο δίκτυο μέσω της σύνδεσης δεδομένων κάνοντας χρήση του πρωτοκόλλου VoLTE, που όμοιο του είναι το πρωτόκολλο VoIP. Οι κινητές συσκευές που αποτελούν το κύριο τελικό κόμβο του δικτύου, καθώς εκεί οι υπηρεσίες καταλήγουν, μπορεί να είναι είτε έξυπνες συσκευές (SmartPhones) Android, iOS ή Windows Phones, και να έχουν προγραμματιστεί κατάλληλα ώστε να μπορούν να λειτουργήσουν στα πρότυπα του LTE, καθώς να έχουν τοποθετημένη και την αντίστοιχη κάρτα αναγνώρισης δικτύου SIM. Στο LTE δίκτυο αυτές οι κάρτες ονομάζονται UICC, και είναι ένας συνδυασμός έξυπνης κάρτας προγραμματισμένης σε Java με κρυπτογραφημένο κλειδί.

Στα κυψελοειδή δίκτυα χρησιμοποιούνται δύο διακριτοί τύποι αναγνώρισης. Το IMSI και το IMEI. Το IMSI είναι η ταυτότητα του παρόχου και χρησιμοποιείται για την αναγνώριση ενός συνδρομητή του δικτύου. Το IMEI χρησιμοποιείται για την αναγνώριση μιας συγκεκριμένης κινητής συσκευής στο δίκτυο και αποθηκεύεται στην εσωτερική μνήμη flash της συσκευής, αν και το IMEI μπορεί επίσης να αποθηκευτεί στο UICC. Τα UEs συνδέονται στο E-UTRAN ,

ώστε να στείλουν δεδομένα στον πυρήνα του δικτύου. Το E-UTRAN σύμπλεγμα δικτυακών συνδέσεων που αποτελείται από βάσεις σταθμών. Ένας βάση σταθμός, ή eNB, προσαρμόζει και τροποποιεί τα ραδιοκυματικά σήματα ώστε να συνδεθεί με τον εξοπλισμό του εκάστοτε χρήστη, εν συνεχεία αναλαμβάνουν τον ρόλο του αναμεταδότη για την δημιουργία και αποστολή IP πακέτων προς το εσωτερικό του δικτύου, λόγω της σχεδίασης των δικτύων κυψέλης να περνάνε την σύνδεση από το ένα σημείο του δικτύου στο άλλο καθώς ο χρήστης αλλάζει σημείο τοποθεσίας. Αυτός ο τρόπος παρέχει την αδιάληπτη και συνεχή σύνδεση. Τα eNBs χρησιμοποιούν τη διεπαφή X2 ώστε να επικοινωνούν μεταξύ τους, ώστε να μεταφέρουν τα απαραίτητα σήματα ελέγχου επικοινωνίας στο δίκτυο LTE ώστε να επιτρέπει την κίνηση του εξοπλισμού του χρήστη.

Το εξελιγμένο σύστημα πακέτων EPC, αποτελεί το κύριο υπολογιστικό σύστημα δρομολόγησης του δικτύου LTE. Τα τερματικά λαμβάνουν σήματα ελέγχου και καλής λειτουργίας μέσω των σταθμών βάσεων που προέρχονται από το σύστημα διαχείρισης κινητικότητας MME. Το MME εκτελεί μια σειρά από λειτουργίες όπως την διαχείριση και αποθήκευση των στοιχείων σύνδεσης του Εξοπλισμού Χρήστη (UE), τη δημιουργία προσωρινών αναγνωριστικών, τον έλεγχο των λειτουργιών πιστοποίησης και την επιλογή της Πύλης Εξυπηρέτησης S-GW καθώς επίσης και της Πύλης Δικτύου Πακέτων P-GW . Καμία κίνηση δεδομένων δεν αποστέλλεται μέσω του MME Το S-GW προσαρμόζει τον Εξοπλισμό του Χρήστη για μεταβάσεις ανάμεσα στα eNodeB και δρομολογεί τις απαιτούμενες πληροφορίες μεταξύ του P-GW και του E-UTRAN. Μέσω P-GW, που έχει το ρόλο του προεπιλεγμένου δρομολογητή και αναλαμβάνει τις μεταφορές μεταξύ των υπηρεσιών 3GPP και μη-3GPP δίνονται ανάλογες διευθύνσεις IP, στις συσκευές που είναι συνδεδεμένες παρέχοντας τους πρόσβαση στο δίκτυο μεταγωγής – ανταλλαγής πακέτων PDN [47].

Η ανταλλαγή πακέτων είναι ένας τρόπος μετάδοσης δεδομένων, όπου ένα μήνυμα χωρίζεται σε πολλά μικρότερα τμήματα (πακέτα) τα οποία αποστέλλονται ανεξάρτητα, κάθε φορά μέσω της βέλτιστης διαδρομής για κάθε πακέτο, και στη συνέχεια επανασυνδέονται στον προορισμό του.

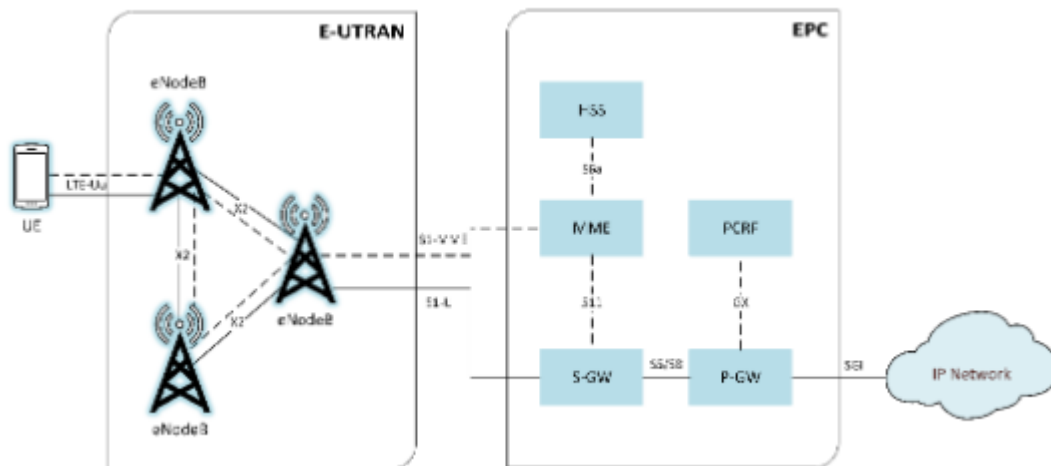
Συνοπτικά τα κύρια δομικά στοιχεία σύνδεσης και αναγνώρισης σταθμών και χρηστών στο LTE είναι:

- (UE): Κινητή - φορητή συσκευή με εγκατεστημένο LTE modem, και περιλαμβάνει:
 - ME : κινητό τηλέφωνο χωρίς την κάρτα σύνδεσης.
 - UICC με αποθηκευμένο προγραμματιστικά (μέσω java) το κλειδί κρυπτογράφησης για να εισαχθεί στην συσκευή.
 - IME: Αναγνωριστική ταυτότητα συσκευής στο δίκτυο
 - IMSI: Αναγνωριστική ταυτότητα χρήστη στο δίκτυο.
 - MCC: 3-ψήφιος αριθμός που χαρακτηρίζει τη χώρα λειτουργίας του δικτύου
 - MNC: 2-ψήφιος αριθμός που τον πάροχο του δικτύου.

- E-UTRAN: Στοιχεία για την ασύρματη και κινητή σύνδεση
 - eNodeB ή eNB: Σταθμός βάσης κινητής

- EPC: Στοιχεία για τις δρομολογήσεις εντός του δικτύου.
 - MME: Πρώτη αναγνώριση χρήστη, σηματοδότηση και καθοδήγηση προς το εσωτερικό του δικτύου
 - S-GW: Μεταφορά δεδομένων χρήστη και δρομολόγηση προς το P-GW και το E-UTRAN.

- P-GW: Παροχή IP διευθύνσεων και περαιτέρω δρομολόγηση
- HSS: Κύρια βάση δεδομένων με αναφορές χρηστών και το κλειδί K αναγνώρισης.



Εικόνα 24. Η αρχιτεκτονική δομή του LTE [47]

3.3.4.2 Ασφάλεια του LTE

Σε αυτή την ενότητα θα περιγράψουμε μηχανισμούς πιστοποίησης, κρυπτογράφησης, μηχανισμούς προστασίας υλικού και προστασίας που προσφέρονται στο δίκτυο LTE.

Ασφάλεια υλικού

Η UICC κάρτα που χρησιμοποιείται σε όλες τις σύγχρονες φορητές κινητές συσκευές αποτελεί την κύρια βάση της αρχιτεκτονικής ασφαλείας του LTE, αφού εμπεριέχει την εφαρμογή της Universal Subscriber και μέσω αυτής πραγματοποιεί όλες τις κρίσιμες λειτουργίες ασφαλείας, πιστοποίησης και κρυπτογράφησης. Η UICC είναι μια κάρτα αποθήκευσης δεδομένων με ανθεκτικότητα σε παρεμβολές, όπου οι χρήστες μπορούν μέσω αυτής την υπηρεσία της κινητής τηλεφωνίας από μια συσκευή σε άλλη, παρέχοντας ταυτόχρονα τη δυνατότητα αποθήκευσης επαφών και άλλων δεδομένων. Η UICC έχει ένα επεξεργαστή, ROM, RAM, καθώς επίσης είναι ενημερωμένη για το δίκτυο, ενώ μπορεί να εκτελέσει Java εφαρμογές με τις πιο γνωστές: συντήρηση, ενημερώσεις και βιντεοπαιχνίδια.

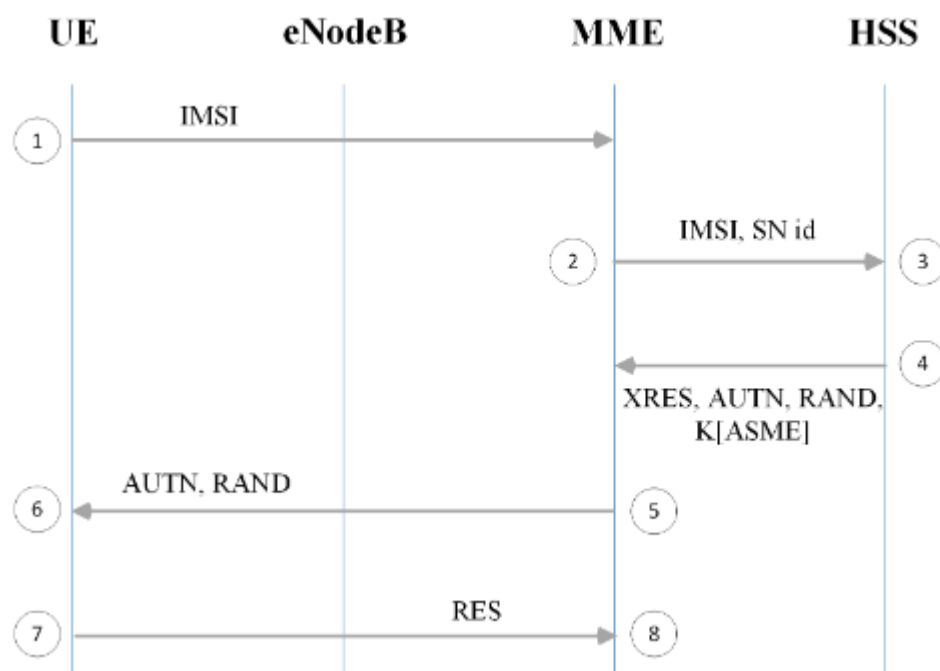
Έλεγχος ταυτότητας συσκευής

Ο κύριος μηχανισμός αναγνώρισης ταυτότητας χρησιμοποιούν τα κινητά τηλέφωνα για την ταυτοποίηση από ένα δίκτυο LTE ονομάζεται πρωτόκολλο ταυτοποίησης και Συμφωνίας Κλειδιού, AKA. Η χρήση του πρωτοκόλλου AKA στο LTE απαιτείται από την προδιαγραφή 3GPP TS 33.401[48]. Το πρωτόκολλο AKA αναγνωρίζει μέσω κρυπτογραφίας ότι η UICC εμπεριέχει το κλειδί *K*. και με αυτό τον τρόπο πιστοποιείται η UICC στο δίκτυο.

Χρήση κωδικού στην USIM

Με την χρήση του κωδικού PIN - στην UICC κάρτα, εμποδίζεται η κλοπή της κάρτας από κάποιον άλλο μη εξουσιοδοτημένο για πρόσβαση στο δίκτυο, καθώς για να την τοποθετήσει και λειτουργήσει σε κάποια άλλη συσκευή θα πρέπει να γνωρίζει αυτό το PIN. Πολλές κάρτες

έχουν την δυνατότητα να κλειδωθούν για θέμα ασφάλειας μετά από 3-5 εσφαλμένες προσπάθειες, και μόνο ο πάροχος κινητής μπορεί μέσω ενός άλλου κωδικού να τις ξεκλειδώσει. Ο κωδικός PIN της USIM είναι ένα ακόμα μέτρο ταυτοποίησης στα πλαίσια της ασφάλειας, του χρήστη προς το δίκτυο LTE [47].



Εικόνα 25. Έλεγχος ταυτότητας συσκευής με το πρωτόκολλο AKA [47]

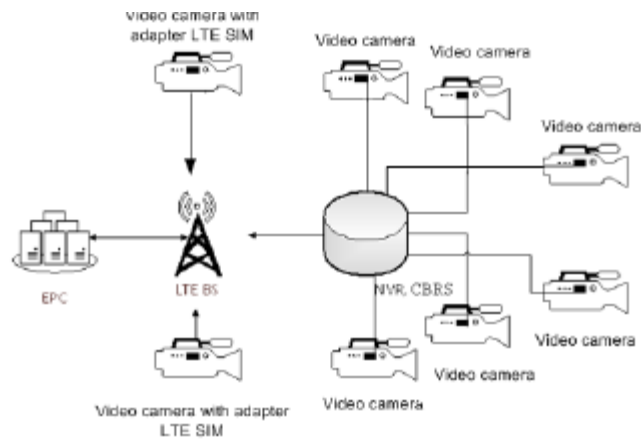
3.3.5 CBRS

Μια άλλη μελλοντική λύση για τη δημιουργία ιδιωτικών δικτύων στο LTE, αλλά και σε 5G είναι το CBRS που έχει εφαρμοστεί στις Ηνωμένες Πολιτείες. Το CBRS χρησιμοποιείται σε ένα εύρος εκπομπής 150 MHz από το εύρος των 3,5 GHz (3550 MHz έως 3700 MHz). Το 2020, η Επιτροπή Επικοινωνιών των Ηνωμένων Πολιτειών FCC αδειοδότησε την πλήρη χρήση του φάσματος CBRS για δημόσια χρήση σε εμπορικές ασύρματες υπηρεσίες.

Το CBRS κάνει χρήση ενός συστήματος δυναμικής πρόσβασης στο Φάσμα SAS και μπορεί να διαχειρίζεται την κατανομή των συχνοτήτων στο κοινόχρηστο φάσμα. Με αυτό το μοναδικό τρόπο μπορεί να χρησιμοποιήσει με αποτελεσματικότερο τρόπο τους διαθέσιμους πόρους, μειώνοντας την παρεμβολή μεταξύ κοινών και διπλανών καναλιών, με παροχή προτεραιότητας τριών επιπέδων. Με αυτό τον τρόπο εξασφαλίζεται ότι κυβερνητικοί φορείς χρήστες σταθερής δορυφορικής επικοινωνίας έχουν προτεραιότητα έναντι των εταιρειών που έχουν αποκτήσει μέσω δημοπρασίας την αποκλειστική χρήση του 70 MHz. Κάθε δίκτυο CBRS πρέπει να καταλαμβάνει ένα σύστημα πρόσβασης στο φάσμα, σε ζώνες Wi-Fi 2.5 GHz και 5 GHz, καθώς μπορεί να ρυθμιστεί για το 4G LTE. Ακόμα το CBRS μπορεί να λειτουργήσει ως προμηθευτής εταιρικών υπηρεσιών για ένα ιδιωτικό δίκτυο LTE που υποστηρίζει μεγάλες επιχειρήσεις, αποθήκες, αθλητικά στάδια κ.λπ. Το CBRS μπορεί να χρησιμοποιήσει συστήματα κατανεμημένης κεραιάς, ταχεία μεταφορά δεδομένων και κάλυψη εσωτερικών χώρων [38].

Ένα ιδιωτικό δίκτυο CBRS με χρήση LTE αποτελείται από τρία στοιχεία:

- 1) Συσκευή CBRS. Η συσκευή πρέπει να υποστηρίζει τη ζώνη LTE Band 48.
- 2) Βάση σταθμού βάσης LTE (BS).
- 3) EPC (Evolved Packet Core), που είναι το κέντρο ελέγχου στο LTE δίκτυο.



Εικόνα 26. Αρχιτεκτονική δομή του CBRS με χρήση του δικτύου LTE [38]

3.4 Εφαρμογές

Πολλές εφαρμογές που χρησιμοποιούνται σε δημόσια δίκτυα μπορούν να αναπτυχθούν το ίδιο καλά και σε ιδιωτικά.

3.4.1 VoIP

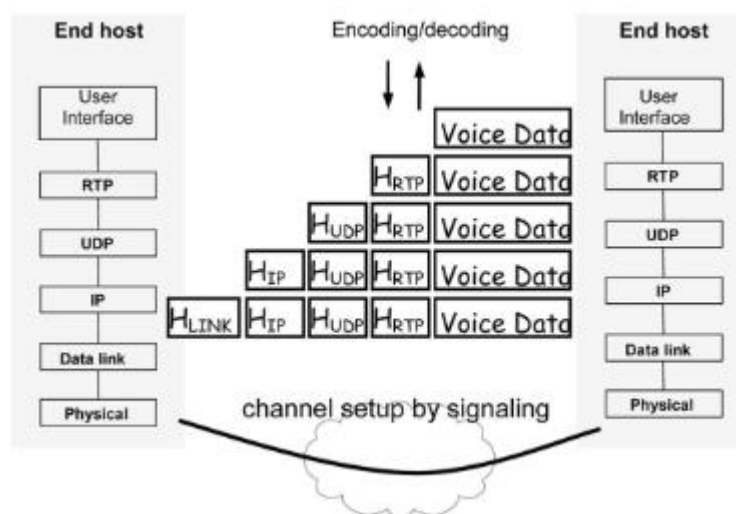
Στην ενότητα αυτή θα δούμε πως η χρήση τηλεφωνίας μέσω Internet γνωστή και ως Voice Over IP -VoIP μπορεί να χρησιμοποιηθεί και σε ένα ιδιωτικό δίκτυο. Ο όρος VoIP σημαίνει Voice over Internet Protocol. Το VoIP πρωτοεμφανίστηκε στα μέσα της δεκαετίας του '90, όταν ερασιτέχνες αρχίσανε να αντιλαμβάνονται τις δυνατότητες της αποστολής πακέτων φωνητικών δεδομένων μέσω του διαδικτύου αντί να επικοινωνούν μέσω των κανονικών τηλεφωνικών συστημάτων. Η ιδέα ήταν να χρησιμοποιηθεί το διαδίκτυο ως ένα δίκτυο τηλεφωνίας με κάποιες επιπλέον δυνατότητες. Το VoIP μετατρέπει το φωνητικό σήμα από ένα τηλέφωνο σε ψηφιακό σήμα, το αποστέλλει μέσω του διαδικτύου και στη συνέχεια το μετατρέπει πίσω στην αρχική του μορφή στον προορισμό [49]. Τα τελευταία χρόνια, η τεχνολογία Voice over IP (VoIP) έχει δει μια τεράστια αύξηση χρήσης λόγω της οικονομικής αποδοτικότητας, της υποστήριξης τεχνολογίας πολυμέσων και της ευκολίας χρήσης. [50]. Η υποδομή VoIP αποτελείται από τερματικά σημεία (τηλέφωνα), κόμβους ελέγχου, κόμβους πύλης και το IP δίκτυο. Το IP δίκτυο μπορεί να χρησιμοποιεί από διάφορα μέσα επικοινωνίας, συμπεριλαμβανομένων Ethernet, οπτικών ινών και ασύρματων τεχνολογιών. Το σύστημα VoIP αλληλοεπιδρά τόσο με τα τοπικά όσο και με τα απομακρυσμένα VoIP τηλέφωνα χρησιμοποιώντας το εταιρικό δίκτυο (intranet) και το Διαδίκτυο, καθώς αλληλοεπιδρά με τα τηλέφωνα που είναι συνδεδεμένα στο δημόσιο δίκτυο τηλεφωνίας.

Η επεξεργασία δεδομένων VoIP αποτελείται από τα ακόλουθα τέσσερα βήματα: σήμανση, κωδικοποίηση, μεταφορά και έλεγχος πύλης.

1. **Σήμανση:** Ο σκοπός του πρωτοκόλλου σήμανσης είναι η δημιουργία και διαχείριση συνδέσεων ή κλήσεων μεταξύ των τερματικών σημείων. Το H.323 και το πρωτόκολλο

έναρξης συνεδρίας (SIP) είναι δύο ευρέως χρησιμοποιούμενα πρότυπα σήμανσης για την δημιουργία και διαχείριση κλήσεων.

2. **Κωδικοποίηση και Μεταφορά:** Μόλις δημιουργηθεί μια σύνδεση, η φωνή πρέπει να μεταδοθεί σε ψηφιοποιημένη μορφή και στη συνέχεια διαχωρίζεται το φωνητικό σήμα σε ένα ρεύμα πακέτων. Το πρώτο βήμα σε αυτήν τη διαδικασία είναι η μετατροπή των αναλογικών φωνητικών σημάτων σε ψηφιακά, χρησιμοποιώντας έναν μετατροπέα από αναλογικό σε ψηφιακό σήμα. Εδώ μπορεί να χρησιμοποιηθεί ένας αλγόριθμος συμπίεσης για να μειωθεί ο όγκος των δεδομένων που θα μεταδοθούν. Στη συνέχεια, τα δείγματα φωνής εισάγονται σε πακέτα δεδομένων που θα μεταφερθούν στο διαδίκτυο, συνήθως χρησιμοποιώντας το πρωτόκολλο μεταφοράς πραγματικού χρόνου RTP. Τα πακέτα RTP έχουν πεδία κεφαλίδας που περιέχουν δεδομένα που απαιτούνται για τη σωστή επανασυναρμολόγηση των πακέτων σε ένα φωνητικό σήμα στην άλλη άκρη. Τέλος, τα ενθυλακωμένα πακέτα φωνής μεταφέρονται ως φορτίο από το πρωτόκολλο datagram
3. **Έλεγχος της πύλης:** Το ίδιο το IP δίκτυο πρέπει να διασφαλίσει ότι η πραγματική συνομιλία μεταφέρεται στο σύστημα τηλεφωνίας για να μετατραπεί από μια πύλη σε άλλη μορφή - είτε για αλληλεπίδραση με ένα διαφορετικό πακέτο πολυμέσων βασισμένο σε IP, είτε επειδή η κλήση πραγματοποιείται στο δίκτυο τηλεφωνίας [51].

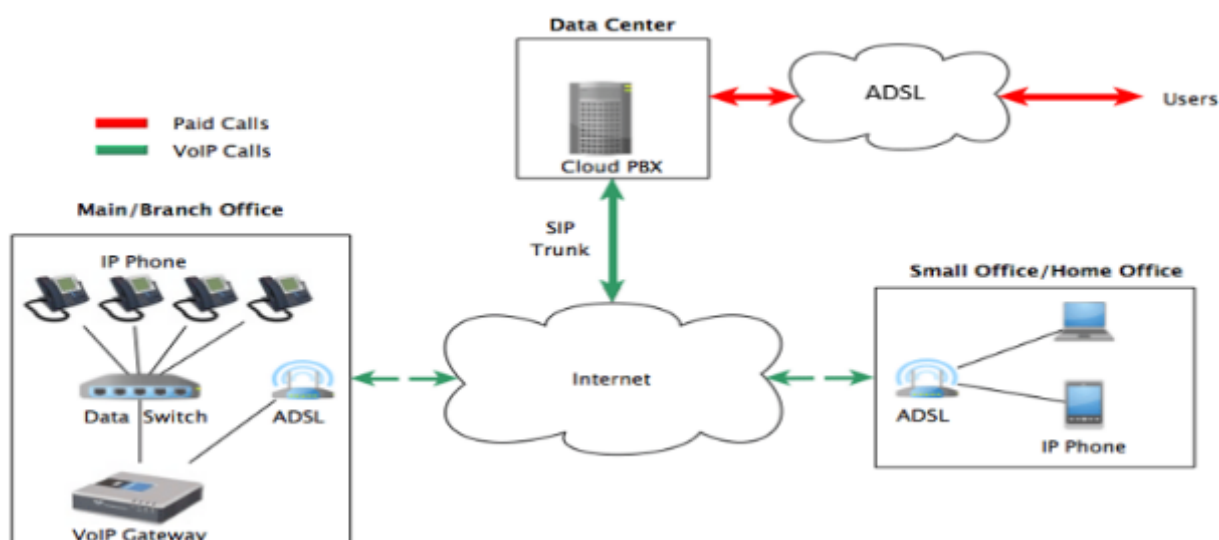


Εικόνα 27. Επεξεργασία δεδομένων φωνής του VoIP [F19]

3.4.2 Αρχιτεκτονική του VoIP

Κατά τη χρήση του πρωτοκόλλου IP, υπάρχουν τρεις διαφορετικοί τύποι συνδέσεων για την αρχή μιας κλήσης: (1) Από υπολογιστή σε υπολογιστή, όπου άτομα μιλούν μέσω διαδικτύου με τους υπολογιστές τους· (2) Από υπολογιστή σε τηλέφωνο, όπου άτομα πραγματοποιούν και λαμβάνουν φωνητικές κλήσεις και μηνύματα ενώ είναι συνδεδεμένοι στο διαδίκτυο· και (3) από τηλέφωνο σε τηλέφωνο, όπου οι κλήσεις πραγματοποιούνται και λαμβάνονται χρησιμοποιώντας κανονικά τηλέφωνα που είναι συνδεδεμένα στο Δημόσιο Δίκτυο Τηλεφώνου ή IP τηλέφωνα που είναι συνδεδεμένα σε ένα δίκτυο δεδομένων. Το VoIP χρησιμοποιεί το RTP για τη μεταφορά, το RTTP για την αναφορά της ποιότητας της υπηρεσίας QoS και τα πρωτόκολλα H.323, SIP, MGCP για τη σήμανση. Αυτά τα πρωτόκολλα λειτουργούν στο επίπεδο εφαρμογής, δηλαδή πάνω από το πρωτόκολλο IP. Οι περισσότερες υπάρχουσες υλοποιήσεις VoIP χρησιμοποιούν το πρωτόκολλο H.323, το ίδιο πρωτόκολλο που

χρησιμοποιείται για το IP βίντεο. Μέχρι τώρα, οι χρήστες προτιμούν το H.323 έναντι του SIP, αλλά αυτό μπορεί να οφείλεται κυρίως στην προηγούμενη έκδοση του H.323 [51].



Εικόνα 28. Αρχιτεκτονική δομή του VoIP [F20]

Το πρωτόκολλο H323

Το πρωτόκολλο H.323, παρέχει τη βάση για τη μεταφορά (δηλαδή τη σήμανση) φωνητικών κλήσεων, βίντεο και δεδομένων επικοινωνιών σε ένα δίκτυο βασισμένο στο πρωτόκολλο IP. Το H.323 υποστηρίζει το Ασφαλές Πρωτόκολλο Πραγματικού Χρόνου SRTP για την κρυπτογραφημένη κίνηση των δεδομένων των πολυμέσων μέσω Internet Keying (MIKEY) για την ανταλλαγή κλειδιών. Είναι σημαντικό να τονίσουμε ότι η σήμανση προστατεύεται μόνο έως την πύλη (gateway).

Το πρωτόκολλο SIP

Το Πρωτόκολλο Έναρξης Συνεδρίας (SIP) είναι ένα πρότυπο του IETF για της διασυνδέσεις μέσω IP. Το SIP είναι ένα πρωτόκολλο ελέγχου και σήμανσης στο επίπεδο εφαρμογής που χρησιμοποιείται για τη δημιουργία, τροποποίηση και λήξη συνεδριών με έναν ή περισσότερους συμμετέχοντες. Αυτές οι συνεδρίες μπορούν να περιλαμβάνουν συνδέσεις στο διαδίκτυο, τηλεφωνικές κλήσεις στο διαδίκτυο και αποστολή δεδομένων. Το SIP είναι ένα πρωτόκολλο λιγότερο περίπλοκο και πιο ευέλικτο από το H.323. Η σήμανση επιτρέπει τη μεταφορά πληροφοριών κλήσης διασχίζοντας τα όρια του δικτύου. Η διαχείριση των συνεδριών παρέχει τη δυνατότητα ελέγχου των χαρακτηριστικών μιας σύνδεσης από άκρο σε άκρο. Το Πρωτόκολλο Έναρξης Συνεδρίας (SIP) υποστηρίζει την κινητικότητα IP για εφαρμογές VoIP σε ασύρματα δίκτυα WLAN παρέχοντας δυνατότητες αλλαγής συνδέσεων στο επίπεδο εφαρμογής. Το SIP μπορεί να χρησιμοποιήσει απευθείας το πρωτόκολλο για τη σύνδεση σε ένα σημείο πρόσβασης. Είναι δυνατόν να χρησιμοποιηθεί κάθε πρωτόκολλο ξεχωριστά ή και τα δύο πρωτόκολλα στο ίδιο δίκτυο προκειμένου να παρέχεται καθολική συνδεσιμότητα [52].

3.4.3 Κλήσεις φωνής VoLTE (Voice over LTE)

Το VoLTE είναι μια τεχνολογία που επιτρέπει τη μετάδοση φωνητικών κλήσεων μέσω δικτύων LTE τα οποία είναι κυρίως σχεδιασμένα για τη μετάδοση κινητών δεδομένων υψηλής

ταχύτητας, βασισμένης σε πακέτα μετάδοσης του IP πρωτοκόλλου για φωνητικές κλήσεις σε δίκτυα LTE. Η χρήση της φωνητικής επικοινωνίας μέσω του δικτύου LTE, προσφέρει αρκετά πλεονεκτήματα και οφέλη σε σχέση με την παραδοσιακή τηλεφωνία, και του VoIP. Σε ένα ιδιωτικό δίκτυο LTE, η φωνή λειτουργεί παρόμοια με τον τρόπο που λειτουργεί σε ένα παραδοσιακό δίκτυο IP, καθώς χρησιμοποιεί το ίδιο πρωτόκολλο. Ωστόσο, σε ένα ιδιωτικό δίκτυο, η υποδομή βασίζεται στην τεχνολογία και την αρχιτεκτονική του LTE, ενώ παρέχει βελτιωμένη κάλυψη, μεγαλύτερη χωρητικότητα καναλιού καλύτερο έλεγχο, βελτιωμένη ποιότητα φωνής ενώ σε σύγκρισή με τα παραδοσιακά δίκτυα φωνητικών κλήσεων που χρησιμοποιούν την τεχνολογία της κυκλωματικής μετάδοσης. Αναλυτικά παρουσιάζουμε την λειτουργία του VoLTE

Υποδομή Δικτύου: Το VoLTE απαιτεί την υποδομή του δικτύου LTE, με τα δομικά στοιχεία του σταθμού βάσης eNBs, του EPC και του IMS. Όλα μαζί αυτά τα στοιχεία με την κατάλληλη συνεργασία μπορούν και διευκολύνουν τη φωνητική επικοινωνία μέσω του δικτύου LTE.

Δυνατότητες Συσκευής και Δικτύου: Είναι πολύ σημαντικό η εκάστοτε συσκευή του χρήστη που θα εγγραφεί στο δίκτυο LTE, μετά και τις απαραίτητες αναβαθμίσεις σε λογισμικό, καθώς και η ίδια η δομή του δικτύου να μπορούν να υποστηρίξουν την υπηρεσία VoLTE. Η συσκευή πρέπει να έχει δυνατότητες VoLTE. Τέλος το δίκτυο θα πρέπει να παραμετροποιηθεί κατάλληλα ώστε να μπορέσει να διαχειριστεί τις κινήσεις των πακέτων του VoLTE.

Ρύθμιση Κλήσης VoLTE: Κατά την έναρξη μια κλήσεις VoLTE η συσκευή του χρήστη από μόνη της δημιουργεί μια ασφαλή σύνδεση με το LTE δίκτυο, έτσι ώστε τα μηνύματα σήμανσης που ανταλλάσσουν μεταξύ τους να έχουν την κατάλληλη αυθεντικότητά ώστε να διαμορφώσουν τις παραμέτρους ώστε να διατεθούν οι κατάλληλοι πόροι του δικτύου.

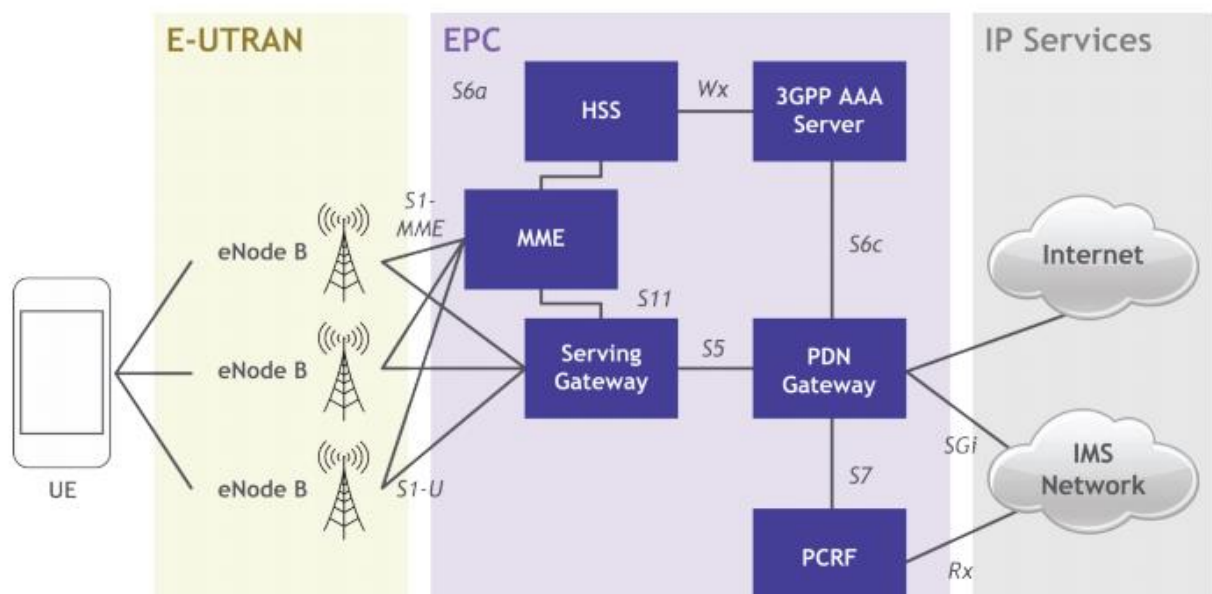
Ποιότητα Υπηρεσίας (QoS) και Προτεραιότητα: Οι Μηχανισμοί ποιότητας υπηρεσίας QoS οι οποίοι εφαρμόζονται στο δίκτυο δίνουν προτεραιότητα στις κινήσεις για τις κλήσεις VoLTE, δίνοντας στα πακέτα φωνής υψηλότερη προτεραιότητα ώστε να εξασφαλιστεί η χαμηλή καθυστέρηση, ο ελάχιστος θόρυβος, καθώς και η μειωμένη απώλεια πακέτων, εξασφαλίζοντας πάντα την υψηλή ποιότητα για τις φωνητικές κλήσεις.

Κωδικοποιητής Φωνής: Το VoLTE χρησιμοποιεί αλγορίθμους συμπίεσης και αποσυμπίεσης κωδικοποίηση και αποκωδικοποίηση αντίστοιχα των φωνητικών σημάτων εντός των κλήσεων. Οι συνηθέστεροι αλγόριθμοι στο VoLTE περιλαμβάνουν το AMR και το AMR-WB, οι οποίοι προσφέρουν έναν συνδυασμό ισορροπίας μεταξύ της ποιότητας φωνής και της χρήσης εύρους ζώνης.

Ολοκλήρωση IMS: Το VoLTE που βασίζεται στο IMS, που είναι ένα πλαίσιο προτύπου για την παροχή υπηρεσιών με πολυμέσα σε δίκτυα IP. Μέσω του IMS προσφέρεται μια αξιόπιστη και υψηλή υπηρεσία κλήσεων φωνής, βίντεο, και άλλων υπηρεσιών. Το VoLTE βασίζεται στο IMS για την σύνδεση, αποσύνδεση, διαχείριση συνεδρίας και της λειτουργίες ελέγχου κλήσης.

Φωνή HD και Επιπλέον Χαρακτηριστικά: Το VoLTE μπορεί να υποστηρίξει υψηλής ευκρίνειας HD ποιότητα φωνής, αφού μπορεί να παρέχει μια πολύ καλά και βελτιωμένη ποιότητα ήχου σε σύγκριση με της παραδοσιακές φωνητικές κλήσεις. Ακόμα μπορεί να συνδυάσει ταυτόχρονη ομιλία φωνής αποστολής, δεδομένων, και βίντεο κλήσης, στην ίδια συνεδρία ενώ χωρίς καμία διακοπή στην υφιστάμενη και εγκαθιδρυμένη σύνδεση μπορεί να κάνει ομαλή μετάβαση ανάμεσα σε δίκτυο LTE και Wi-Fi.

Μεταφορά Κλήσης και Roaming: Το VoLTE υποστηρίζει ακόμα μια πολύ καλή λειτουργία σε διεθνές επίπεδο, το roaming, το οποίο επιτρέπει της χρήστες να πραγματοποιούν και να λαμβάνουν κλήσεις VoLTE κατά παραμονής τους στο εξωτερικό εφόσον ο εκάστοτε πάροχος τους υποστηρίζει την συγκεκριμένη υπηρεσία [53,54,55,56,57,58].



Εικόνα 29. Η αρχιτεκτονική δομή του VoLTE [F21]

3.4.4 Το Asterisk ως μέσω επικοινωνίας στο VoIP

Το Asterisk είναι ένα δημοφιλές λογισμικό ανοικτού κώδικα που μπορεί να χρησιμοποιηθεί για μετάδοσης φωνής, γνωστό ως Ιδιωτικό Κλαδικό Κέντρο PBX. Παρέχει τα απαραίτητα εργαλεία και λειτουργίες για τη δημιουργία της πλήρους τηλεφωνικού συστήματος, συμπεριλαμβανομένων των υπηρεσιών VoIP. Το Asterisk επιτρέπει διάφορες λειτουργίες τηλεφωνίας, της δρομολόγηση κλήσεων, ανακατεύθυνση κλήσεων, αυτόματο τηλεφωνητή, κλήσεις ενδοεπικοινωνίας. Υποστηρίζει μεγάλο αριθμό πρωτοκόλλων επικοινωνίας, συμπεριλαμβανομένου του SIP, που κυρίως χρησιμοποιείται συνήθως για κλήσεις VoIP. Με το Asterisk, οι εταιρίες δημιουργούν οικονομικές λύσεις επιτρέποντάς της να χειρίζονται αποτελεσματικά εισερχόμενες και εξερχόμενες κλήσεις. Λόγω της φύσης του ανοικτού κώδικα υπάρχει η προγραμματιστική δυνατότητα τροποποιήσεις του συστήματος για μοναδικές απαιτήσεις. Γενικότερα, το Asterisk είναι μια ισχυρή πλατφόρμα για την εφαρμογή ανταλλαγής μηνυμάτων φωνής βασισμένων σε VoIP [59].

3.4.4.1 Υλοποίηση εγκατάστασης του Asterisk

Για την εγκατάσταση του Asterisk στο δίκτυο θα πρέπει να δημιουργηθεί ένα σχέδιο κλήσεων και οι συσκευές να μπορούν να επικοινωνήσουν με την βάση του Asterisk.. Οι χρήστες που συνδέονται στο Asterisk ανήκουν όλοι σε ένα συγκεκριμένο περιβάλλον που έχει καθοριστεί στο αρχείο ρυθμίσεων του καναλιού, απ' όπου το Asterisk αναζητά συμβουλές για τον τρόπο χειρισμού των κλήσεων που πραγματοποιούνται από αυτόν τον χρήστη, ελέγχοντας τα δικαιώματα πρόσβασης σε αυτό το περιβάλλον με διαφορετικούς κανόνες για της τοπικούς χρήστες και της επαφές τους [60]. Στην υλοποίηση της έπρεπε να καταχωρήσουμε της απαραίτητες ρυθμίσεις για της εκάστοτε εσωτερικούς χρήστες, παραμετροποιώντας τα αρχεία:

1. /etc/asterisk/sip.conf
2. etc/asterisk/extensions.conf
3. etc/asterisk/voicemail.conf

3.5 Πλατφόρμες ανοιχτού κώδικα για υλοποιήσεις

Στην ενότητα αυτή θα μιλήσουμε για το ελεύθερο και ανοιχτό λογισμικό, καθώς επίσης θα δούμε τις αντίστοιχες πλατφόρμες και αναπτυξιακές πλατφόρμες υλικού που υποστηρίζουν αυτό το είδος λογισμικού.

3.5.1 Πλατφόρμες ανοιχτού κώδικα για υλοποιήσεις

Ο όρος «ανοιχτός κώδικας» αναφέρεται σε έναν τύπο λογισμικού, του οποίου ο πηγαίος κώδικας είναι ελεύθερα διαθέσιμος προς το κοινό. Αυτό επιτρέπει σε οποιονδήποτε θέλει να προβάλλει, τροποποιήσει, διαχειριστεί και διανείμει το λογισμικό σύμφωνα με της όρους της άδειας ανοιχτού κώδικα. Το ανοιχτό λογισμικό ενθαρρύνει τη συνεργασία και την ανάπτυξη από κοινότητες, καθώς οι προγραμματιστές μπορούν να συνεισφέρουν στον κώδικα και να βελτιώνουν το λογισμικό [61].

Το ανοιχτό λογισμικό OSS είναι της τύπος λογισμικού, ο οποίος και αυτός έχει τον πηγαίο του κώδικα ελεύθερα διαθέσιμο προς το κοινό. Διανέμεται βάσει μιας άδειας ανοιχτού κώδικα, η οποία επιτρέπει της χρήστες να προβάλλουν, τροποποιούν, διαχειριστούν και διανέμουν το λογισμικό. Η άδεια ανοιχτού κώδικα είναι εκείνη που καθορίζει της όρους και της προϋποθέσεις κάτω από τις οποίες θα μπορέσει να χρησιμοποιηθεί, τροποποιηθεί και διανεμηθεί το λογισμικό. Τα βασικά χαρακτηριστικά του ανοιχτού λογισμικού είναι:

Διαθεσιμότητα του πηγαίου κώδικα: Το ανοιχτό λογισμικό παρέχει πρόσβαση στον πηγαίο κώδικα, και επιτρέπει της χρήστες να μελετήσουν τον τρόπο λειτουργίας του λογισμικού, και να τον τροποποιήσουν με βάση τις δίκες τους ανάγκες

Ελεύθερη διανομή: Το ανοιχτό λογισμικό μπορεί να διανέμεται ελεύθερα, είτε στην αρχική του μορφή είτε στην κατά περίπτωση τροποποιημένη μορφή, χωρίς περιορισμούς άδειας ή τέλη χρήσης.

Τροποποίηση: Οι χρήστες έχουν την ελευθερία να τροποποιήσουν τον πηγαίο κώδικα του ανοιχτού λογισμικού, επιτρέποντάς της να προσθέσουν νέες λειτουργίες, να διορθώσουν σφάλματα ή να βελτιστοποιήσουν το λογισμικό για της συγκεκριμένες ανάγκες της.

Παραγωγή παραγώνων έργων: Οι άδειες ανοιχτού κώδικα συνήθως επιτρέπουν τη δημιουργία έργων παραγωγής, που σημαίνει ότι μπορούν να δημιουργηθούν και να διανεμηθούν έργα με τροποποιημένες εκδόσεις ή κάποιες επεκτάσιμες λύσεις του λογισμικού.

Συνεργατική ανάπτυξη: Το ανοιχτό λογισμικό λόγω τις μεγάλης κοινότητάς ενθαρρύνει τη συνεργασία. Οι προγραμματιστές μεταξύ τους συνεισφέρουν βελτιώσεις, και διορθώσεις σφαλμάτων, καθώς υλοποιούν νέες εκδόσεις στο λογισμικό.

Διαφάνεια: Το ανοιχτό λογισμικό προωθεί τη διαφάνεια, αφού επιτρέπει της χρήστες να ελέγχουν σημείο προς σημείο τον πηγαίο κώδικα, και έτσι διασφαλίζουν ότι το λογισμικό λειτουργεί της προβλέπεται δεν έχει ευάλωτα σημεία και ευπαθή σημεία ασφάλειας.

Να σημειώσουμε εδώ ότι το ανοιχτό λογισμικό δεν είναι το ίδιο με το ελεύθερο λογισμικό, αν και βασίζονται σε παρόμοιες αρχές. Ο βασικός διαχωρισμός είναι ότι το ανοιχτό λογισμικό επικεντρώνεται στη διαθεσιμότητα του πηγαίου κώδικα, ενώ το ελεύθερο λογισμικό τονίζει την ελευθερία να χρησιμοποιείς, τροποποιείς και διανέμεις το λογισμικό.

Το ανοιχτό λογισμικό έχει αποκτήσει σημαντική δημοτικότητα λόγω των πολλαπλών οφελών του, σε αυξημένη ασφάλεια, και οικονομική αποδοτικότητα, ευελιξία λόγω της μεγάλης συνεργατικής κοινότητας Πολλά επιτυχημένα έργα έχουν υλοποιηθεί λόγω των παραπάνω λύσεων [62].

3.5.2 Πλατφόρμες ανοιχτού και ελεύθερου λογισμικού

Στην παράγραφο αυτή θα αναφερθούμε στις πιο γνωστές πλατφόρμες που μπορούν να συνεργαστούν με την χρήση του ανοιχτού και ελεύθερου κώδικα.

3.5.2.1 OmneT++

Το OmneT++ είναι ένα λογισμικό προσομοίωσης διακριτών γεγονότων που μπορεί να χρησιμοποιηθεί για την μοντελοποίηση διαφόρων ειδών δικτύων, της ενσύρματα, ασύρματα, και αισθητήρων. Το OMNeT++ είναι βασισμένο σε συνδεδεμένα μοντέλα μέσω πυλών ώστε να και μπορούν αλληλοεπιδρούν μεταξύ της. Το OmneT++ είναι ανοικτού κώδικα, επιτρέποντας της χρήστες να αναπτύξουν τα δικά της μοντέλα προσομοίωσης και είναι υποστηρίζει την γλώσσα προγραμματισμού C++ [63]. Εχει ευρέως υιοθετηθεί τόσο στον ακαδημαϊκό όσο και στο βιομηχανικό χώρο για την προσομοίωση και τη μελέτη διάφορων συστημάτων επικοινωνίας, πρωτοκόλλων και τεχνολογιών δικτύων. Προσφέρει ένα πλούσιο σύνολο χαρακτηριστικών, ευελιξία και κλιμάκωση για τη διεξαγωγή προσομοιώσεων και αξιολογήσεων απόδοσης στον τομέα των επικοινωνιακών και καταναμημένων συστημάτων. Το OMNeT++ βασίζεται στην προσομοίωση ατομικών γεγονότων, που σημαίνει ότι μοντελοποιεί συστήματα που αλλάζουν την κατάστασή της σε συγκεκριμένα σημεία του χρόνου. Αυτό το καθιστά κατάλληλο για την προσομοίωση δικτύων, πρωτοκόλλων και καταναμημένων συστημάτων. Της παρέχει μια πλήρη βιβλιοθήκη με το όνομα «OMNeT++ Μεταπτυχιακή Διπλωματική Εργασία, Σπυρίδων Παπαγιάκουμος, AM msciot20005 61

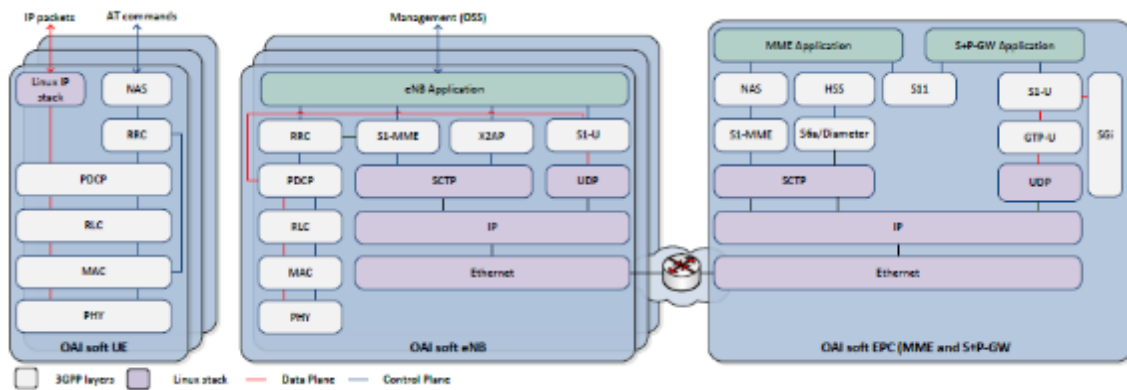
Standard Library», η οποία περιλαμβάνει μια μεγάλη λίστα , μοντέλων και πρωτοκόλλων για την προσομοίωση διαφόρων τεχνολογιών δικτύων, της TCP/IP, Ethernet, ασύρματα δίκτυα και άλλα. Η μεγάλη κοινότητα χρηστών που συμβάλλει στην ανάπτυξή του, παρέχει υποστήριξη και μοιράζεται πρόσθετα μοντέλα προσομοίωσης και βιβλιοθήκες, ενώ η ενσωμάτωση του πραγματικό κώδικα που είναι γραμμένος σε C++, Java και της γλώσσες επιτρέπει την άρρηκτη ενσωμάτωση πραγματικών πρωτοκόλλων σε διαφόρων ειδών δικτύων, διευκολύνοντας πιο ακριβείς και ρεαλιστικές προσομοιώσεις[64,65].

3.5.2.2 MATLAB

Το MATLAB, είναι ένα περιβάλλον ανάπτυξης και μπορεί να χρησιμοποιηθεί για την προσομοίωση δικτύων LTE δικτύων, καθώς παρέχει μια σειρά εργαλείων και δυνατοτήτων που το καθιστούν κατάλληλο για αυτές της προσομοιώσεις δικτύων. Το Communications Toolbox του MATLAB παρέχει ένα σύνολο συναρτήσεων, αντικειμένων συστήματος και αλγορίθμων που έχουν σχεδιαστεί ειδικά για την προσομοίωση και ανάλυση ασύρματων επικοινωνιών, συμπεριλαμβανομένου του LTE.. Της το LTE System Toolbox του είναι ένα εξειδικευμένο εργαλείο που επικεντρώνεται καθαρά της LTE επικοινωνίες αφού περιλαμβάνει της εκείνες της δυνατότητες παραμετροποίησης φυσικών επιπέδων, με μοντέλα προσομοίωσης σε ένα επίπεδο σύνδεσης και ενσωμάτωσης. Μέσω της προσομοίωσης μπορούν να σχεδιαστούν τοπολογίες LTE δικτύων με χρήση UEs eNBs και να διεξαχθούν προσπάθειες βελτιστοποίησης. Τέλος μέσω της γραφικής απεικόνισης των αποτελεσμάτων μπορούν να δημιουργηθούν γραφήματα και ιστογράμματα ώστε να μπορούν να παραχθούν και ασφαλή συμπεράσματα των αποτελεσμάτων [66].

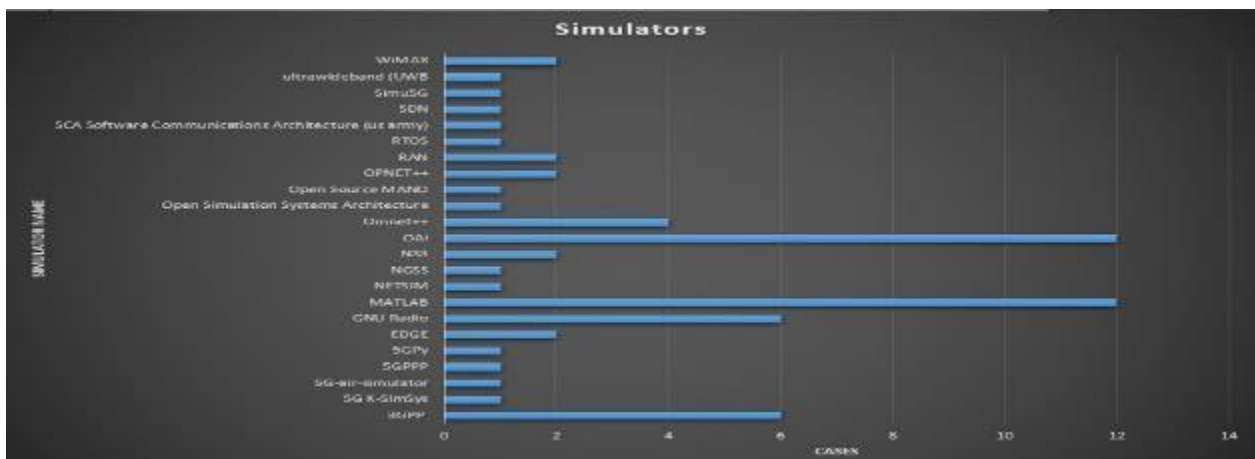
3.5.2.3 OAI

Η OAI είναι μια ανοιχτού κώδικα πλατφόρμα λογισμικού για την ανάπτυξη τεχνολογιών ορισμένων από το χρήστη μέσω της τεχνολογίας SDR. Χρησιμοποιείται πάρα πολύ στον ακαδημαϊκό χώρο, σε ερευνητικά ιδρύματα καθώς και στη βιομηχανία για τη δημιουργία πρωτοτύπων, τον έλεγχο και την αξιολόγηση νέων τεχνολογιών. Παρέχει μια ευέλικτη και προσβάσιμη πλατφόρμα για καινοτομία και ανάπτυξη στον τομέα των ασύρματων δικτύων. Στόχος είναι η παροχή μιας ευέλικτης και προσαρμοστικής πλατφόρμας με σκοπό την κατασκευή και πειραματισμό σε ασύρματα συστήματα επικοινωνίας. Ασχολείται κυρίως με δίκτυα κυψελών ενώ μπορεί να υποστηρίξει όλες τις γενιές κινητής τηλεφωνίας, 2G, 3G, 4G (LTE) μέχρι και 5G. Παρέχει υλοποίηση πλήρους πρωτοκόλλου στοίβας, επιτρέποντας της προγραμματιστές να εργαστούν στα διάφορα επίπεδα του δικτύου, από το φυσικό επίπεδο έως το επίπεδο εφαρμογής. Η ανάπτυξη και η συντήρηση γίνεται από μια κοινότητα ατόμων και οργανισμών που συνεισφέρουν στην τεχνογνωσία, τον κώδικα και της πόρους της στο έργο. Οι κύριες συνιστώσες του Open Air Interface περιλαμβάνουν την τεχνολογία SDR, επιτρέποντας την υλοποίηση και τροποποίηση πρωτοκόλλων ασύρματης επικοινωνίας μέσω λογισμικού, χωρίς να εξαρτάται από αφιερωμένα υλικά συστατικά. Το Open Air Interface παρέχει υλοποιήσεις τόσο για τον βάση σταθμό όσο και για τον εξοπλισμό χρήστη, επιτρέποντας τη δημιουργία σεναρίων δικτύων κυψέλης από άκρο σε άκρο για δοκιμές. Ακόμα περιλαμβάνονται και εργαλεία προσομοίωσης και δοκιμής που επιτρέπουν την αξιολόγηση και ανάλυση της απόδοσης του ασύρματου δικτύου με διάφορα σενάρια [67].



Εικόνα 30. Δομή του OAI [F22]

Για την δική μας υλοποίηση, και μετά την μελέτη της σχετικής βιβλιογραφίας είδαμε ότι οι πιο συχνές αναφορές υλοποίησης δικτύου LTE είναι μεταξύ του MATLAB και της OAI. Για λόγους καλύτερης και ευκολότερης διαχείρισης χρησιμοποιήσαμε το OAI.



Εικόνα 31. Οι πιο γνωστές σε χρήση πλατφόρμες ανοιχτού κώδικα

3.6 Η τεχνολογία SDR για χρήση σε Open Source Platform

Με την ραγδαία ανάπτυξη των συσκευών που χρησιμοποιούν το φάσμα ραδιοσυχνοτήτων, η ανάγκη για προσθήκη περισσότερων χρηστών στο ευρύ φάσμα έχει ωθήσει τεχνολογίες στο να εξελιχθούν σε πιο αποδοτικές. Το SDR μπορεί να επιτρέψει τη χρήση ενός ιδιού υλικού για πολλά και διαφορετικά συστήματα επικοινωνίας απλά αλλάζοντας το λογισμικό, το οποίο υλοποιεί την συγκεκριμένη διαμόρφωση, κωδικοποίηση και τα πρωτόκολλα [68,69]

3.6.1 Η ιστορία του SDR

Η έννοια του SDR δημιουργήθηκε την δεκαετία του 1970-1980 μέσω της συνεργασίας ποικίλων ομάδων μελέτης σε ιδιωτικές και δημόσιες οργανώσεις των Ηνωμένων Πολιτειών. Το 1991, σε συνεργασία με την E-Systems, ο Joe Mitola ανακάλυψε τον όρο Software Radio SR ως μέθοδο για τη δημιουργία ενός αυθεντικού δέκτη GSM βασισμένο στο λογισμικό. Ωστόσο, λόγω του μεγάλου αριθμού μαθηματικών υπολογισμών, ο σχεδιασμός ενός

αποτελεσματικού φυσικού επιπέδου συχνά ήταν δύσκολος. Η διαφορά μεταξύ των SR από το SDR είναι ότι τα SDR μπορούν να υλοποιηθούν σε πολλά εύρη συχνοτήτων και διαθέτουν πολύ μεγαλύτερο εύρος ζώνης. Ένα SDR μπορεί να επα-ναπρογραμματιστεί σε όποια συχνότητα απαιτείται ώστε να λειτουργήσει [70]. Σχετικά γρήγορα έγινε αντιληπτή η δυνατότητα του ανοικτού κώδικα σε συνδυασμό με SDR Το 2003, ο Matt Ettus ξεκίνησε την ανάπτυξη του USRP και το ο 2004 ιδρύθηκε η Ettus Research για την ανάπτυξη, παραγωγή και υποστήριξη του USRP, το οποίο κυκλοφόρησε για πρώτη φορά το 2005. Από τότε, το USRP έχει εξελιχθεί σε μια μεγάλη οικογένεια προϊόντων με διάφορες δυνατότητες. Τα USRPs έχουν χρησιμοποιηθεί σε όλη την έκταση του πλανήτη και σε πάνω από 106 χώρες. Έχουν χρησιμοποιηθεί για έρευνα, εκπαίδευση, πειραματισμό και υποστηριζόμενα συστήματα παραγωγής [68].

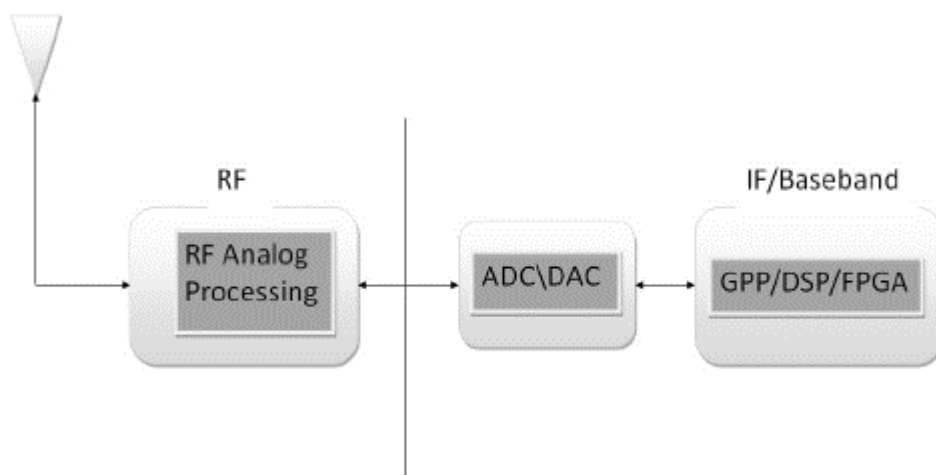
3.6.2 Αρχές λειτουργίας του SDR

Η βασική αρχή λειτουργίας του SDR είναι να αποτυπώνει και να ψηφιοποιεί ακριβώς τα RF σήματα από μια κεραία στην πλευρά λήψης και να παράγει πιστά αντίγραφα ως μια αναλογική έκδοση των παρεχόμενων δειγμάτων στην πλευρά μετάδοσης [68]. Η βασική συχνότητα (baseband) και το ενδιάμεσο σήμα συχνότητας IF επεξεργάζονται στον ψηφιακό τομέα. Στην συνέχεια, χρησιμοποιείται μια ανταλλαγή συχνότητας ραδιοσυχνοτήτων RF με σκοπό ενίσχυση του ενδιάμεσου σήματος σε συχνότητα μετάδοσης. Σε ένα ιδανικό SDR, αυτή η εναλλαγή υλοποιείται από τον μετατροπέα αναλογικού σε ψηφιακού σήματος ADC και αντίστροφος DAC αφού τοποθετηθούν ακριβώς πριν από την κεραία και τον ενισχυτή χαμηλού θορύβου LNA. Ωστόσο, ένα ιδανικό SDR είναι δύσκολο να επιτευχθεί, καθώς θα απαιτούσε λειτουργία με πολύ υψηλό ρυθμό δειγματοληψίας. Υπάρχουν γενιές πλατφόρμων που έχουν αναπτυχθεί μέσα στα χρόνια που, για κάλυψη μεγαλύτερης εμβέλειας περιοχής και μεγαλύτερη ισχύ.

Πρώτη γενιά USRP: Το μοντέλο USRP1 με κάλυψη συχνότητας από 0.1 MHz έως τα 2.2 GHz

Δεύτερη γενιά USRP: Η εξέλιξη του USRP1 με κάλυψη συχνότητας πάνω από τα 2.2 GHz

Τρίτη γενιά USRP: SDRs με κάλυψη συχνότητας από 10 MHz έως 6 GHz



Εικόνα 29. Η αρχή λειτουργίας του SDR

3.6.3 To SDR B210

Το USRP B210 είναι μια ευέλικτη και προγραμματιζόμενη συσκευή που μας δίνει την δυνατότητα ασύρματης επικοινωνίας. Η λειτουργία της βασίζεται στον έλεγχο του λογισμικού και τον προγραμματισμό, δίνοντάς στους χρήστες την δυνατότητα να ορίσουν και να ελέγξουν τη συμπεριφορά του ραδιοφάσματος. Στα κύρια χαρακτηριστικά του περιλαμβάνεται η υποστήριξη του φάσματος συχνοτήτων από 70 MHz έως 6 GHz, καθώς επιτρέπει τη λήψη και αποστολή RF σημάτων σε διάφορες ζώνες συχνοτήτων. Χρησιμοποιεί υψηλής ποιότητας ADCs και DACs για αποτελεσματική μετατροπή μεταξύ αναλογικών και ψηφιακών σημάτων. Επίσης είναι κατάλληλα σχεδιασμένο για να μπορεί να προγραμματιστεί με κατάλληλα λογισμικά όπως το UHD, USRP Hardware Driver. Οι χρήστες μπορούν να αλληλοεπιδρούν με τη συσκευή χρησιμοποιώντας τις διαθέσιμες διεπαφές προγραμματισμού (APIs) του UHD ή του που προσφέρουν λειτουργίες και εντολές για τον έλεγχο παραμέτρων συχνότητας, ενίσχυσης, ρυθμού δειγματοληψίας αλλά και συγχρονισμού με άλλες συσκευές. Τέλος το B210 Προσφέρει θύρες συγχρονισμού που επιτρέπουν τον συγχρονισμό πολλαπλών συσκευών ίδιου μοντέλου, διευκολύνοντας την ομόχρονη λειτουργία και τις διαμορφώσεις MIMO [68,69,70].



Εικόνα 32. Το USRP SDR B210 [71]

3.6.4 Αναλυτικός πίνακας των USRPs SDR

Στην εικόνα που ακολουθεί παρουσιάζουμε ένα πίνακα με τα χαρακτηριστικά των USRPs της Ettus, τις λειτουργίες τους καθώς και τις διαφορές που έχουν μεταξύ τους [68,69,70,72].

Ettus Usrp Name	N200/N210	N320/N321	B200/B210	X300/X310	E300	USRP N310
Generation	2nd	3rd	3rd	3rd	3rd	Not under a specific generation can support a wide range of wireless communication protocols
RF Front End	supplementary board	Integrated RFIC	Integrated RFIC	supplementary board	Integrated RFIC	Integrated RFIC
connection with computer	Ethernet (Gigabit)	Ethernet (Gigabit)	USB 3.0	Ethernet (Gigabit), PCI express 4	AX14-MM Interface embedded	Ethernet (Gigabit)
Bandwidth	25-50 MHz	120 MHz	56 MHz	160 MHz	56 MHz	100 MHz
RF Coverage Frequency	6 GHz	10 MHz - 6 GHz	70 MHz - 6 GHz	6 GHz	70 MHz - 6 GHz	10 MHz -6GHz
MiMo	1x1 per unit, up to 8x8 by multiple units	N320: 2x2 N321: 2x2 or 4x4	B200: 1x1 B210: 2x2	2x3 per unit, up to 128x128 by multiple units	2x2	4x4
Full Duplex	Yes	Yes	Yes	Yes	Yes	Yes
Sample Rate	N200: 100 MS/s N210:25 MS/s	160 MS/s	56 Ms/s	X300: 200 MS/s X310: 400 MS/s	56 MS/s	100 MS/s
ADC	Dual 14 bit 100 Ms/s	12 bits	Dual /quad 12 bit 61.44 Ms/s	Quad 14 bit 200 Ms/s	Dual /quad 12 bit 61.44 Ms/s	12 bits
DAC	Dual 16 bit 100 Ms/s	16 bits	Dual /quad 12 bit 61.44 Ms/s	Quad 16 bit 800 Ms/s	Dual /quad 12 bit 61.44 Ms/s	14 bits
FPGA version	Xilinx Spartan 3A DSP	Xilinx Spartan 6	Xilinx Spartan 6	Xilinx Kintex 7	Xilinx Zyng 7	Xilinx Kintex-7
RFNoC	No	Yes	No	Yes	Yes	Yes
extra notes	Gps (Optional)	-	Gps (Optional)	Gps (Optional)	Portable Battery power	GPS
Open Source	FPGA/Driver	FPGA/Driver	FPGA/Driver	FPGA/Driver	FPGA/Driver	FPGA/Driver
Compatibilty	4G	4G	4G	4G/5G (80 MHz with 3/4 sampling)	3G	5G up to 100 MHz
Cost	1600 euros	1000 euros	1200 euros	5000 euros	1000 euros	10.000 euros
Dimenstions	N200: 171 mm x 134 mm x 46 mm N210: 168 mm x 108 mm x 35 mm	198 mm x 122 mm x 46 mm	B210: 100 mm x 100 mm x 22 mm B200:100 mm x 60 mm x 20 mm	X300: 406 mm x 200 mm x 44 mm X310: 406 mm x 200 mm x 88 mm	200 mm x 112 mm x 31 mm	483 mm x 44 mm x 210 mm
Weight	N200: 1 kgr N210 : 680 gr	910 gr	B210: 190 gr B200: 230gr	X300: 2.5 kgr X310: 4.1 kgr	450 gr	3.5 kg

Εικόνα 33. Συγκριτικός πίνακας διαφορών για USRPs (SDR) Ettus

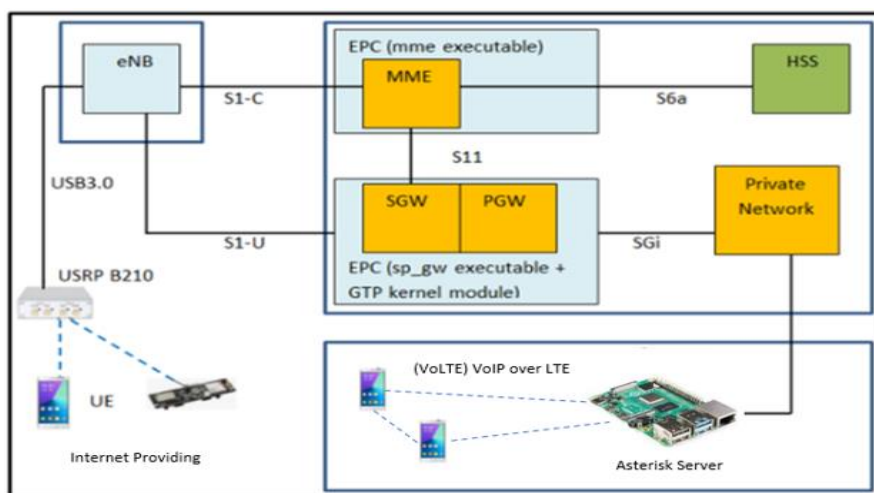
Στην παρούσα εργασία χρησιμοποιήθηκε το URRP B210. Η απόφαση για την χρήση αυτού, πάρθηκε μετά από σχετική έρευνα και σύγκριση των χαρακτηριστικών ανάμεσα στα USRPs με γνώμονα τις ανάγκες για την υλοποίησης του δικτύου. Πιο αναλυτικά:

- ✓ Ανήκει στην 3^η γενιά των USRP και έχει ενσωματωμένο (στο ίδιο board) το κύκλωμα για τις κεραίες RF. Θέλαμε ο εξοπλισμός να είναι όσο πιο μικρός (compact)
- ✓ Η σύνδεση του με το eNB μπορεί να γίνει με USB 3.0 που είναι ταχείας μεταφοράς δεδομένων. Το USB μπορεί να λειτουργήσει άμεσα χωρίς την συγγραφή κάποιου έξτρα script.
- ✓ Το Bandwidth, και το MiMo σε εργαστηριακό επίπεδο δεν αποτέλεσαν κάποιο περιορισμό αφού οι δοκιμές έγιναν σε μικρό χώρο, ενώ το εύρος συχνότητας, ο ρυθμός δειγματοληψίας, το ADC - DAC (conversion) του, λόγω απαιτήσεων του 4G-LTE, τις καλύπταν πλήρως.
- ✓ Το χαμηλό κόστος προμήθειάς του.
- ✓ Η μεγάλη κοινότητα υποστήριξης που υπάρχει για το συγκεκριμένο USRP.

4.1 Αρχιτεκτονική δομή του ιδιωτικού δικτύου

Στο σημείο αυτό να αναφέρουμε ότι για την υλοποίηση του δικτύου δεν χρησιμοποιήθηκε κανένα Virtual Περιβάλλον ή κάποιο Software για Virtual Machine (VM), παρά μονάχα 2 ξεχωριστά Laptops. Ο λόγος που έγινε αυτό ήταν διότι κάποια VM εργαλεία δεν αναφέρουν σωστά τις ταχύτητες των επεξεργασιών καθώς και των πυρήνων. Επίσης όλη η υλοποίηση δεν πραγματοποιήθηκε σε ένα Laptop, και αυτό επειδή έπρεπε να γίνουν εγκαταστάσεις low latency kernel και generic kernel και θα υπήρχε πρόβλημα λειτουργείας.

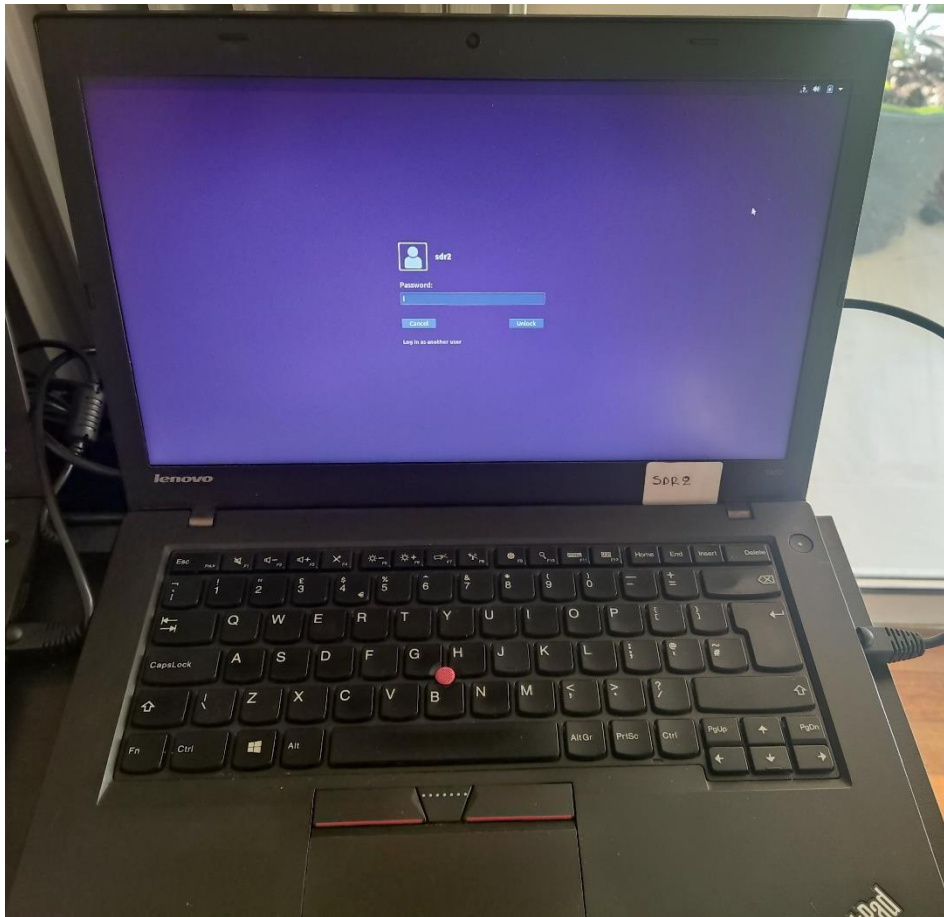
Στην εικόνα που ακολουθεί παρουσιάζουμε την αρχιτεκτονική δομή του δικτύου που υλοποιήσαμε. Το δίκτυο αποτελείται από το EPC στο οποίο περιέχει τις οντότητες του MME, SGW και PGW, το HSS που είναι η βάση με τους εγγεγραμμένους συνδρομητές το eNB στο οποίο έχει εγκατεστημένους τους Drivers για την σύνδεση και εκπομπή του USRP. Στο ιδιωτικό δίκτυο έχει συνδεθεί ο Asterisk server, όπου μαζί με το κατάλληλο Software δίνει την δυνατότητα κλήσεων εντός του δικτύου. Το USRP παρέχει την διασύνδεση των έξυπνων συσκευών ή αναπτυξιακών πλατφόρμων με το διαδίκτυο και μεταξύ τους.



Εικόνα 34. Αρχιτεκτονική δομή του ιδιωτικού μας δικτύου

4.2 Εξοπλισμός eNB.

Για τις λειτουργίες του eNB χρησιμοποιήθηκε ένα Laptop Lenovo T460,



Εικόνα 35. Lenovo T460 για το eNB

με τα παρακάτω τεχνικά χαρακτηριστικά:

Processor	Intel® Core™ i7-6600U Processor (3M Cache, up to 3.40 GHz)
Memory	Up to 16GB (2 DIMMS)
Storage	2.5" Hard Drives – SSD 256 GB /
Display	14" HD (1366 x 768) Antiglare
Communication	2 x 2 Intel® Snowfield Peak 2, vPro™, 802.11 a/c + Bluetooth® 4.1, M.2 Module

Για την υλοποίηση των λειτουργιών του eNB χρησιμοποιήθηκε το ανοιχτού κώδικα ελεύθερο λογισμικό Ubuntu Linux 16.04. Έγινε λήψη του λειτουργικού και περάσαμε το image σε ένα USB stick

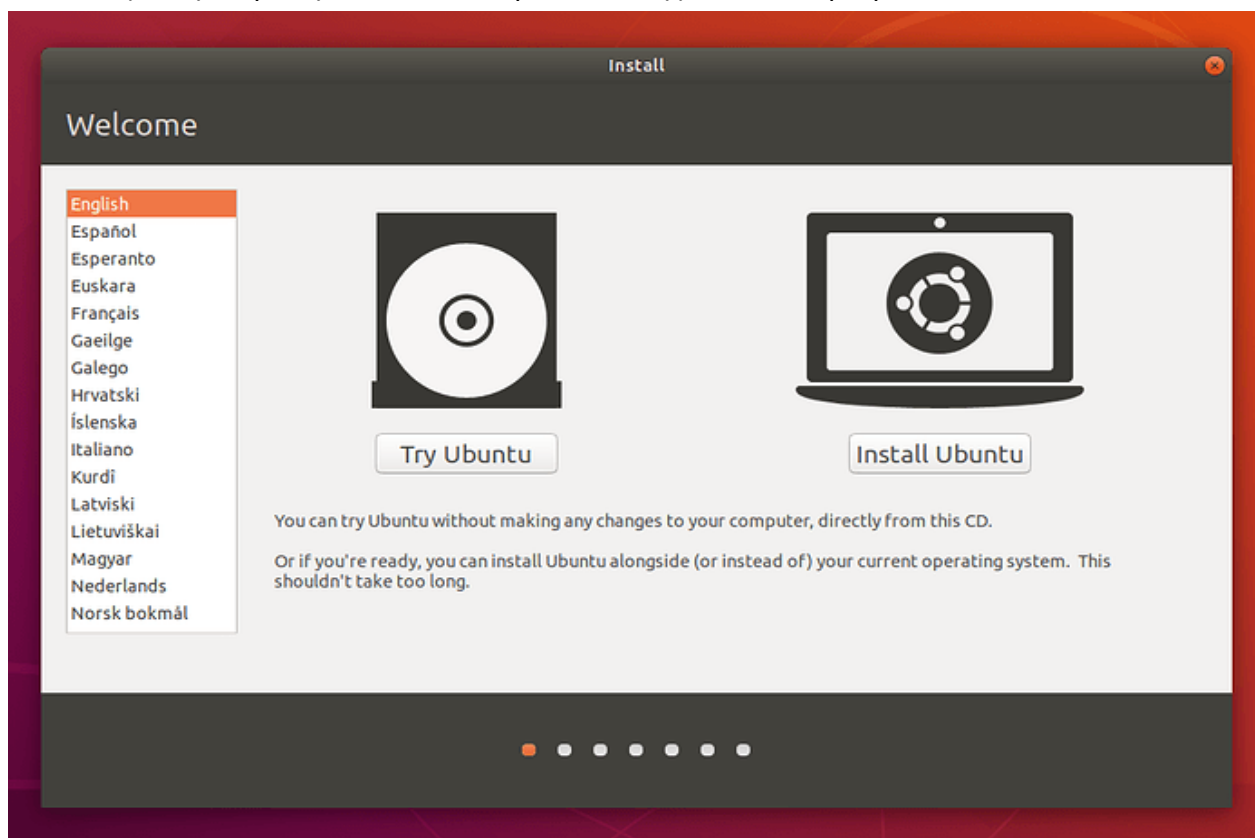
4.2.1 Λειτουργικό eNB

Για την υλοποίηση των λειτουργιών του eNB χρησιμοποιήθηκε το ανοιχτού κώδικα ελεύθερο λογισμικό Ubuntu Linux 18.04. Έγινε λήψη του λειτουργικού και περάσαμε το image σε ένα usb stick



Εικόνα 36. Λήψη λειτουργικού [F23]

Όστε να ξεκινήσουμε την διαδικασία εγκατάστασης του στο Laptop.

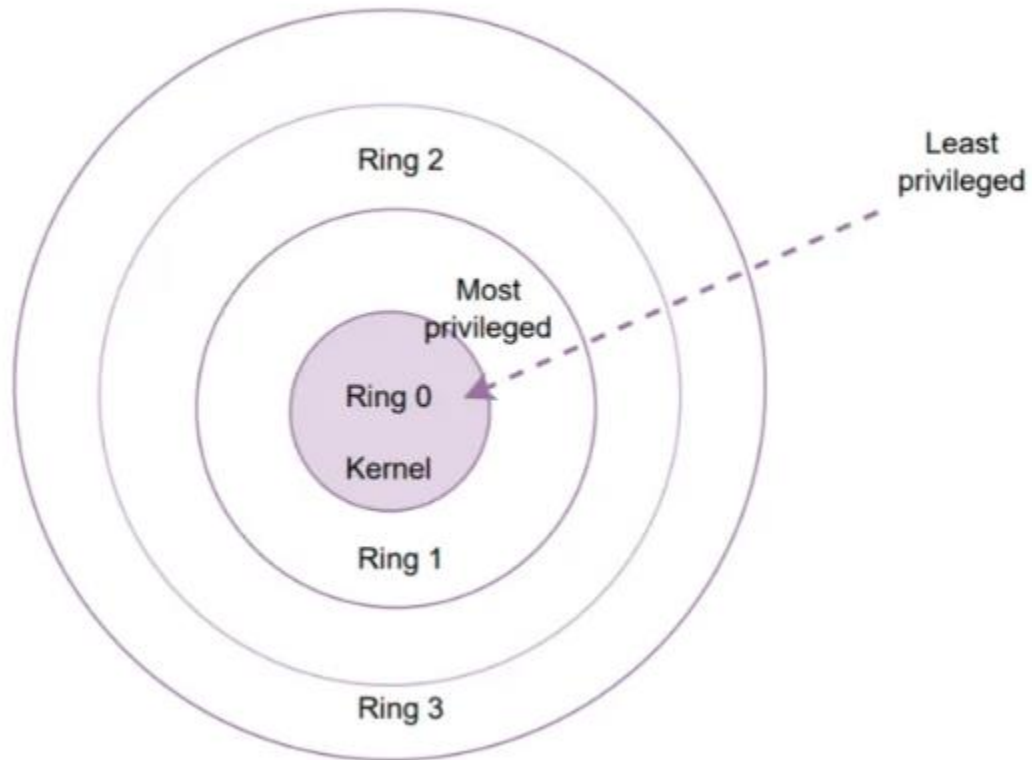


Εικόνα 37. Εγκατάσταση λειτουργικού [F24]

4.2.2 Διαχείριση ισχύος και εγκατάσταση Low Latency Kernel στο eNB

Οι πυρήνες χαμηλής καθυστέρησης (Low Latency Kernel) είναι σχεδιασμένοι για την μείωση του χρόνου απαίτησης επεξεργασίας κάθε αιτήματος από τον επεξεργαστή, καθώς

βελτιστοποιούν τους χρόνους ως προς την ταχύτητα επεξεργασίας και απόδοσης. Οι πυρήνες χαμηλής καθυστέρησης έχουν σχεδιαστεί ώστε να μειώνουν και τον όγκο των πόρων που απαιτούνται για την επεξεργασία ενός αιτήματος, ενώ είναι και πιο ασφαλείς, ως προς τον κίνδυνο κακόβουλων επιθέσεων [72].



Εικόνα 38. Αρχιτεκτονική Low Latency Kernel (F25)

Μετά την επιτυχή ολοκλήρωση της εγκατάστασης του λειτουργικού Ubuntu Linux 18.04 προχωρήσαμε με την απενεργοποίηση αυξομείωσης συχνότητας του επεξεργαστή **GOVERNOR="performance"**

```

sdr2@enb: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/default/grub

If you change this file, run 'update-grub' afterwards to update
/boot/grub/grub.cfg.
For full documentation of the options in this file, see:
info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet intel_pstate=disable processor.max_cstate=1 intel_idle.max_cstate=0 idle=poll"
GRUB_CMDLINE_LINUX=""

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
GRUB_TERMINAL=console
  
```

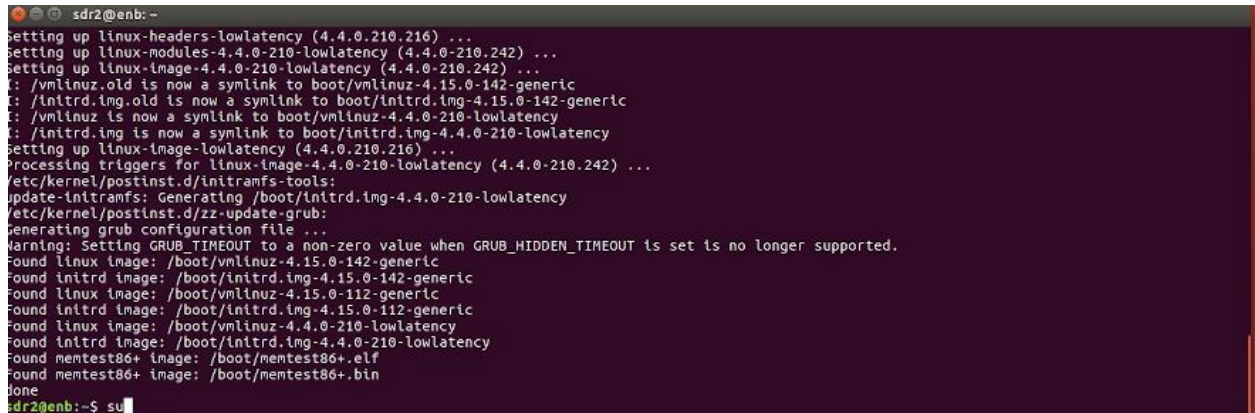
Εικόνα 39. Απενεργοποίηση αυξομείωσης συχνότητας CPU

Επίσης περιορίσαμε την ισχύ του επεξεργαστή, εγκαθιστώντας το κατάλληλο εργαλείο της Intel για τους επεξεργαστές της, ώστε να περιορίσουμε την εναλλαγή στις ταχύτητες μεταξύ των πυρήνων του επεξεργαστή.

Για την καλύτερη λειτουργία του eNB απαιτείται η εγκατάσταση του Low Latency Kernel, οπότε και προχωρήσαμε με την έκδοση 4.4

(\$version=4.4)

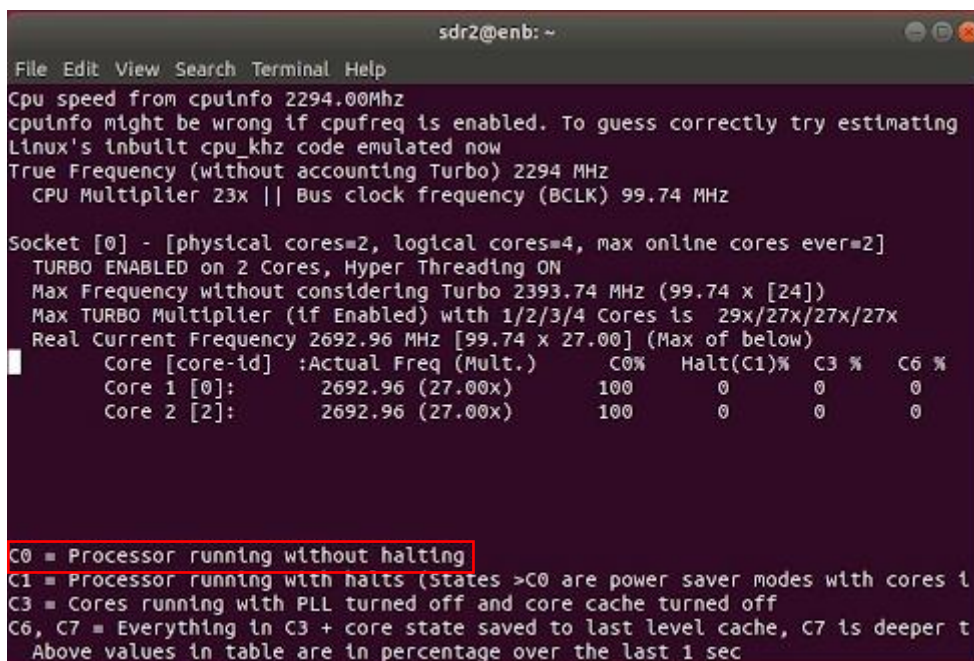
\$sudo dpkg -i kernel.ubuntu.com/*/*/*/*deb



```
sdr2@enb: ~  
Setting up linux-headers-lowlatency (4.4.0.210.216) ...  
Setting up linux-modules-4.4.0-210-lowlatency (4.4.0-210.242) ...  
Setting up linux-image-4.4.0-210-lowlatency (4.4.0-210.242) ...  
I: /vmlinuz.old is now a symlink to boot/vmlinuz-4.15.0-142-generic  
I: /initrd.img.old is now a symlink to boot/initrd.img-4.15.0-142-generic  
I: /vmlinuz is now a symlink to boot/vmlinuz-4.4.0-210-lowlatency  
I: /initrd.img is now a symlink to boot/initrd.img-4.4.0-210-lowlatency  
Setting up linux-image-lowlatency (4.4.0.210.216) ...  
Processing triggers for linux-image-4.4.0-210-lowlatency (4.4.0-210.242) ...  
/etc/kernel/postinst.d/initramfs-tools:  
update-initramfs: Generating /boot/initrd.img-4.4.0-210-lowlatency  
/etc/kernel/postinst.d/zz-update-grub:  
generating grub configuration file ...  
Warning: Setting GRUB_TIMEOUT to a non-zero value when GRUB_HIDDEN_TIMEOUT is set is no longer supported.  
Found linux image: /boot/vmlinuz-4.15.0-142-generic  
Found initrd image: /boot/initrd.img-4.15.0-142-generic  
Found linux image: /boot/vmlinuz-4.15.0-112-generic  
Found initrd image: /boot/initrd.img-4.15.0-112-generic  
Found linux image: /boot/vmlinuz-4.4.0-210-lowlatency  
Found initrd image: /boot/initrd.img-4.4.0-210-lowlatency  
Found memtest86+ image: /boot/memtest86+.elf  
Found memtest86+ image: /boot/memtest86+.bin  
done  
sdr2@enb:~$ su
```

Εικόνα 40. Εγκατάσταση του Low Latency Kernel

Μετά την ολοκλήρωση της εγκατάστασης και επανεκκίνησης του συστήματος ελέγξαμε ότι η συχνότητα που επεξεργαστή δεν αλλάζει, και οι πυρήνες λειτουργούν στην ίδια συχνότητα. Το μόνο το C-Stat που υπάρχει είναι C₀, που σημαίνει ότι ο επεξεργαστής λειτουργεί χωρίς καθυστερήσεις, ενώ δεν πρέπει να αλλάζει η συχνότητα του παραπάνω από 1-2 hertz.

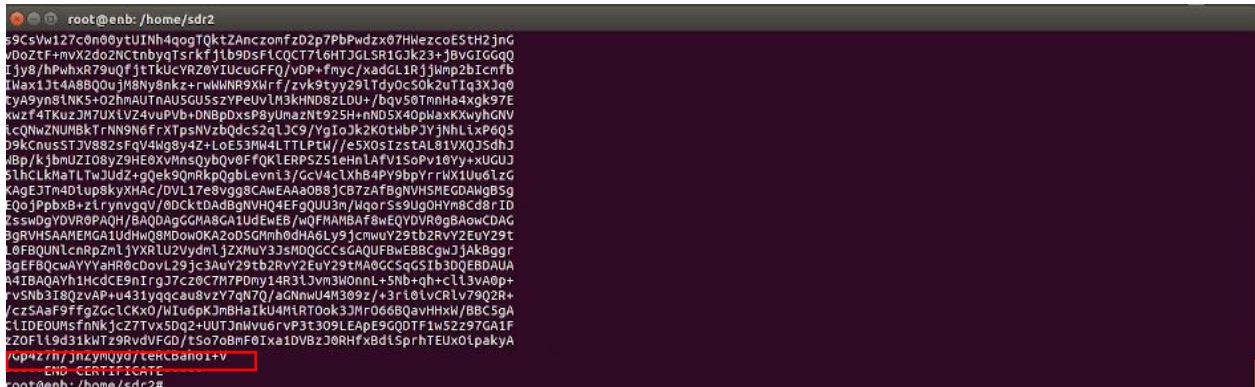


```
sdr2@enb: ~  
File Edit View Search Terminal Help  
Cpu speed from cpufreq 2294.00Mhz  
cpufreq might be wrong if cpufreq is enabled. To guess correctly try estimating  
Linux's inbuilt cpu_khz code emulated now  
True Frequency (without accounting Turbo) 2294 MHz  
CPU Multiplier 23x || Bus clock frequency (BCLK) 99.74 MHz  
  
Socket [0] - [physical cores=2, logical cores=4, max online cores ever=2]  
TURBO ENABLED on 2 Cores, Hyper Threading ON  
Max Frequency without considering Turbo 2393.74 MHz (99.74 x [24])  
Max TURBO Multiplier (if Enabled) with 1/2/3/4 Cores is 29x/27x/27x/27x  
Real Current Frequency 2692.96 MHz [99.74 x 27.00] (Max of below)  
Core [core-id] :Actual Freq (Mult.) C0% Halt(C1)% C3 % C6 %  
Core 1 [0]: 2692.96 (27.00x) 100 0 0 0  
Core 2 [2]: 2692.96 (27.00x) 100 0 0 0  
  
C0 = Processor running without halting  
C1 = Processor running with halts (states >C0 are power saver modes with cores 1  
C3 = Cores running with PLL turned off and core cache turned off  
C6, C7 = Everything in C3 + core state saved to last level cache, C7 is deeper t  
Above values in table are in percentage over the last 1 sec
```

Εικόνα 41. Έλεγχος λειτουργίας συχνότητας πυρήνων

4.3 Παραμετροποίηση του eNB

Για να μπορέσουμε να κάνουμε λήψη του κώδικα για το eNB από το GitLab της Eurecom έπρεπε να κάνουμε εγκατάσταση συγκεκριμένου Certificate, που εμπεριέχει συγκεκριμένα κλειδιά και δικαιώματα πρόσβασης.



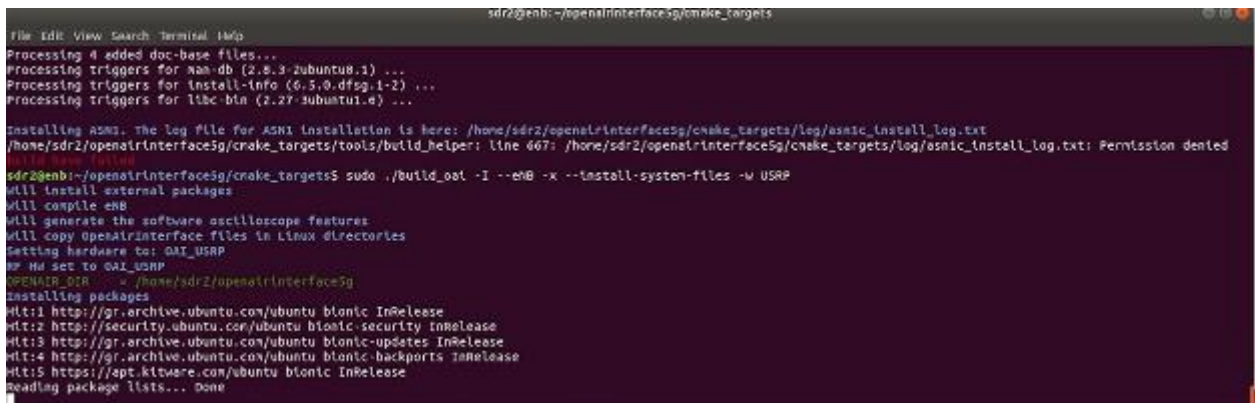
Εικόνα 42. Επιτυχής εγκατάσταση Certificate στο eNB

Με την επιτυχή εγκατάσταση του certificate **---END CERTIFICATE---** μπορέσαμε και αποκτήσαμε πρόσβαση στην βιβλιοθήκη της Eurecom και κατεβάσαμε τον πηγαίο κώδικα για το eNB.



Εικόνα 43. Εικόνα του Gitlab της Eurecom [F26]

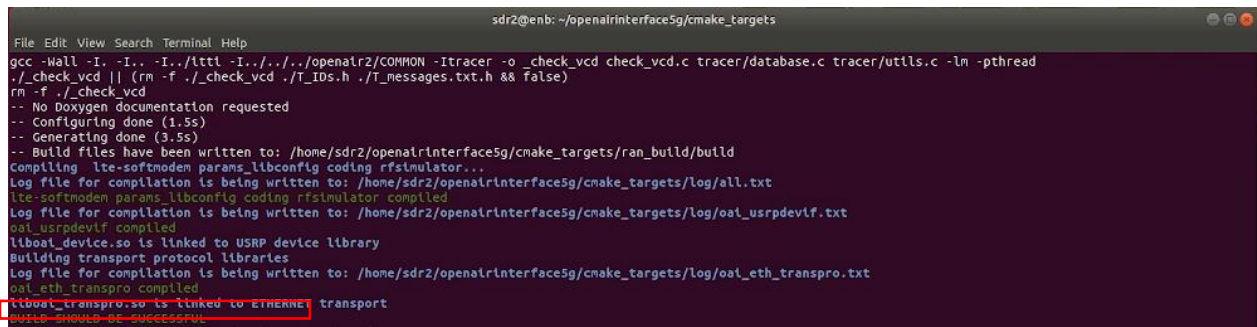
Μετά την λήψη του κώδικα για τους Drivers του USRP, ξεκινήσαμε την εγκατάσταση τους στο eNB.



Εικόνα 44. Έναρξη λήψης των drivers του USRP

Καθ' όλη την διάρκεια της εγκατάστασης δεν έπρεπε να γίνει καμία άλλη ενέργεια και περιμέναμε να ολοκληρωθεί η διαδικασία, μέχρι το επιβεβαιωτικό μήνυμα ολοκλήρωσης.

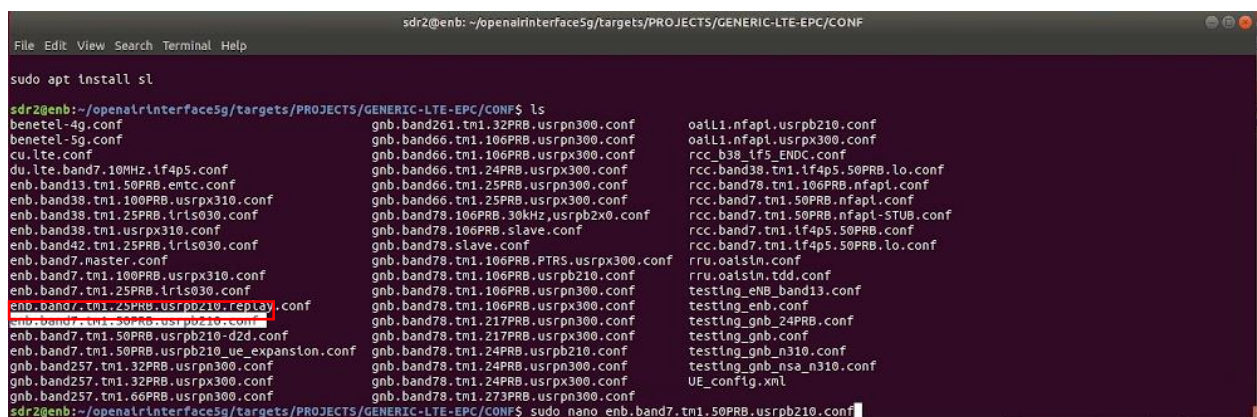
“BUILD SHOULD BE SUCCESSFUL”



```
File Edit View Search Terminal Help
sdr2@enb: ~/openairInterface5g/cmake_targets
gcc -Wall -I. -I. -I. -I./tntt -I./../openair2/COMMON -Itracer -o _check_vcd check_vcd.c tracer/database.c tracer/utlils.c -lm -pthread
./_check_vcd || (rm -f ./_check_vcd ./T_IDS.h ./T_messages.txt.h && false)
rm -f ./_check_vcd
-- No Doxygen documentation requested
-- Configuring done (1.5s)
-- Generating done (3.5s)
-- Build files have been written to: /home/sdr2/openairInterface5g/cmake_targets/ran_build/build
Compiling lte-softmodem_params_libconfig coding rfsimulator...
Log file for compilation is being written to: /home/sdr2/openairInterface5g/cmake_targets/log/all.txt
lte-softmodem_params_libconfig coding rfsimulator compiled
Log file for compilation is being written to: /home/sdr2/openairInterface5g/cmake_targets/log/oai_usrpdevif.txt
oai_usrpdevif compiled
liboai_device.so is linked to USRP device library
Building transport protocol libraries
Log file for compilation is being written to: /home/sdr2/openairInterface5g/cmake_targets/log/oai_eth_transpro.txt
oai_eth_transpro compiled
liboai_transpro.so is linked to ETHERNET transport
BUILD SHOULD BE SUCCESSFUL
```

Εικόνα 45. Ολοκλήρωση διαδικασίας για τους drivers του USRP

Μετά την λήψη και εγκατάσταση των Drivers, παραμετροποιήσαμε το αρχείο **enb.band7.tm1.50PRB.usrbp210.conf** , για το SDR USRP B210, ώστε να μπορεί να επικοινωνήσει το USB με eNB, και να εκπέμπει στην συχνότητα του LTE. Το αρχείο αυτό είναι ένα **CONF**.



```
sdr2@enb: ~/openairInterface5g/targets/PROJECTS/GENERIC-LTE-EPC/CONF
File Edit View Search Terminal Help
sudo apt install sl
sdr2@enb:~/openairInterface5g/targets/PROJECTS/GENERIC-LTE-EPC/CONF$ ls
benetel-4g.conf          gnb.band261.tm1.32PRB.usrpn300.conf  oai11.nfapi.usrbp210.conf
benetel-5g.conf         gnb.band66.tm1.106PRB.usrpn300.conf  oai11.nfapi.usrpx300.conf
cu.lte.conf             gnb.band66.tm1.106PRB.usrpx300.conf  rcc_b38_lf5_ENDC.conf
du.lte.band7.10MHz.lf4p5.conf  gnb.band66.tm1.24PRB.usrpx300.conf  rcc.band38.tm1.lf4p5.50PRB.lo.conf
enb.band13.tm1.50PRB.emtc.conf  gnb.band66.tm1.25PRB.usrpn300.conf  rcc.band78.tm1.106PRB.nfapi.conf
enb.band38.tm1.100PRB.usrpx310.conf  gnb.band66.tm1.25PRB.usrpx300.conf  rcc.band7.tm1.50PRB.nfapi.conf
enb.band38.tm1.25PRB.lrls030.conf  gnb.band78.106PRB.30kHz.usrbp2x0.conf  rcc.band7.tm1.50PRB.nfapi-STUB.conf
enb.band38.tm1.usrpx310.conf       gnb.band78.106PRB.slave.conf         rcc.band7.tm1.lf4p5.50PRB.conf
enb.band42.tm1.25PRB.lrls030.conf  gnb.band78.slave.conf                rcc.band7.tm1.lf4p5.50PRB.lo.conf
enb.band7.master.conf           gnb.band78.tm1.106PRB.PTRS.usrpx300.conf  rru.oai11n.conf
enb.band7.tm1.100PRB.usrpx310.conf  gnb.band78.tm1.106PRB.usrbp210.conf  rru.oai11n.tdd.conf
enb.band7.tm1.25PRB.lrls030.conf  gnb.band78.tm1.106PRB.usrpn300.conf  testing_enb_band13.conf
enb.band7.tm1.25PRB.usrbp210-replay.conf  gnb.band78.tm1.106PRB.usrpx300.conf  testing_enb.conf
enb.band7.tm1.50PRB.usrbp210.conf  gnb.band78.tm1.217PRB.usrpn300.conf  testing_gnb_24PRB.conf
enb.band7.tm1.50PRB.usrbp210-d2d.conf  gnb.band78.tm1.217PRB.usrpx300.conf  testing_gnb.conf
enb.band7.tm1.50PRB.usrbp210_ue_expansion.conf  gnb.band78.tm1.24PRB.usrbp210.conf  testing_gnb_n310.conf
gnb.band257.tm1.32PRB.usrpn300.conf  gnb.band78.tm1.24PRB.usrpn300.conf  testing_gnb_nsa_n310.conf
gnb.band257.tm1.32PRB.usrpx300.conf  gnb.band78.tm1.24PRB.usrpx300.conf  UE_config.xml
gnb.band257.tm1.66PRB.usrpn300.conf  gnb.band78.tm1.273PRB.usrpn300.conf
sdr2@enb:~/openairInterface5g/targets/PROJECTS/GENERIC-LTE-EPC/CONF$ sudo nano enb.band7.tm1.50PRB.usrbp210.conf
```

Εικόνα 46. Εντοπισμός του αρχείου **enb.band7.tm1.50PRB.usrbp210.conf** για παραμετροποίηση

Ο λόγος που επιλέχθηκε το συγκεκριμένο αρχείο, είναι επειδή η “μπάντα” 7 του LTE χρησιμοποιείται στην Ευρώπη, και στην Ελλάδα. Το LTE Band 7 αποτελεί μέρος του φάσματος FDD -LTE και έχει διαφορετικές συχνότητες uplink και downlink, που επιτρέπουν την ταυτόχρονη μετάδοση και στις δύο συχνότητες. Οι ζώνες έχουν ένα διαχωρισμό μεταξύ τους που ονομάζεται κενό ζώνης [73].

Uplink Frequency:	2500-2570 MHz
Downlink Frequency:	2620-2690 MHz
Width of Band:	70 MHz
Duplex Spacing:	120 MHz
Band Gap:	50 MHz

Εικόνα 47. Χαρακτηριστικά του LTE Band 7 [F27]

```

##### Physical parameters:
component_carriers = (
{
  node_function      = "3GPP_eNODEB";
  node_tuning        = "synch_to_ext_device";
  node_synch_ref     = 0;
  frame_type         = "FDD";
  tdd_config         = 3;
  tdd_config_s       = 0;
  prefix_type        = "NORMAL";
  eutra_band         = 7;
  downlink_frequency = 2680000000L;
  uplink_frequency_offset = -120000000;
  Nid_cell           = 0;
  N_RB_DL            = 50;
  Nid_cell_mbsfn     = 0;
  nb_antenna_ports   = 1;
}
)

```

Εικόνα 48. Ρύθμιση του Uplink, Downlink στο USRP

Ο πίνακας με τις παραμέτρους που ακολουθεί παρουσιάζει τις απαραίτητες ρυθμίσεις που έπρεπε να γίνουν στο αρχείο CONF για το eNB και σχετίζονται με το όνομα, τις ρυθμίσεις του εσωτερικού δικτύου και την συχνότητα στο Uplink και downlink του USRP

<i>eNB_ID</i>	<i>0xe00</i>
<i>cell_type</i>	<i>"CELL_MACRO_ENB"</i>
<i>eNB_name</i>	<i>"eNB_EUROCOM_LTEBox"</i>
<i>tracking_area_code</i>	<i>"1"</i>
<i>mobile_country_code</i>	<i>"208"</i>
<i>Mobile_network_code</i>	<i>"93"</i>

Πίνακας 2. Identification Parameters (eNB)

<i>frame_type</i>	<i>"FDD";</i>
<i>tdd_config</i>	<i>3;</i>
<i>tdd_config_s</i>	<i>0;</i>
<i>prefix_type</i>	<i>"NORMAL"</i>
<i>eutra_band</i>	<i>7;</i>
<i>downlink_frequency</i>	<i>2680000000L;</i>
<i>uplink_frequency_offset</i>	<i>-120000000;</i>

<i>Nid_cell</i>	<i>0;</i>
<i>N_RB_DL</i>	<i>50;</i>

Πίνακας 3. Physical Parameters (eNB)

<i>ipv4</i>	<i>"192.168.12.63";</i>
<i>ipv6</i>	<i>"192:168:30::17";</i>
<i>active</i>	<i>"yes";</i>
<i>preference</i>	<i>"ipv4";</i>

Πίνακας 4. MME Parameters (eNB)

<i>ENB_INTERFACE_NAME_FOR_S1_MME</i>	<i>"eth0";</i>
<i>ENB_IPV4_ADDRESS_FOR_S1_MME</i>	<i>"192.168.12.82/24";</i>
<i>ENB_INTERFACE_NAME_FOR_S1U</i>	<i>"eth0";</i>
<i>ENB_IPV4_ADDRESS_FOR_S1U</i>	<i>"192.168.12.82/24";</i>
<i>ENB_PORT_FOR_S1U</i>	<i>2152; # Spec 2152</i>

Πίνακας 5. Network Interfaces (eNB)

Παρατηρήσαμε μετά από δοκιμές ότι το όνομα της κάρτας δικτύου στο linux έπρεπε να αλλαχθεί διότι δημιουργούσε πρόβλημα στο conf αρχείο που είχαμε παραμετροποιήσεις.

```
sdr2@enb:~$ ifconfig
enp0c25: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 68:f7:28:fc:de:b5 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 20 memory 0xf1100000-f1120000
```

Εικόνα 49. Όνομα κάρτας δικτύου πριν την αλλαγή ονόματος

GRUB_CMDLINE_LINUX= "net.iflines=0 biosdevname=0" και μετά από επανεκκίνηση τους συστήματος το όνομα είχε αλλάξει.

```
sdr2@enb: ~
File Edit View Search Terminal Help
sdr2@enb:~$ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 68:f7:28:fc:de:b5 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 20 memory 0xf1100000-f1120000
```

Εικόνα 50. Όνομα κάρτας δικτύου μετά την αλλαγή ονόματος

Μετά την επιτυχή ολοκλήρωση του EPC συνδέσαμε το USRP με το EPC μέσω USB type 3.0 και εγκαταστήσαμε και τις κεραίες στο SDR



Εικόνα 51. Εξοπλισμός USRP SDR B210

Τα χαρακτηριστικά των κεραιών είναι τα παρακάτω:

Frequency: 600MHz-6000MHz

Impedance: 50Ω

Standing Wave Ratio: <3

Gain: 5dBi

Connector: SMA

Connection Wire: 11.5mm, IPEX4 generation

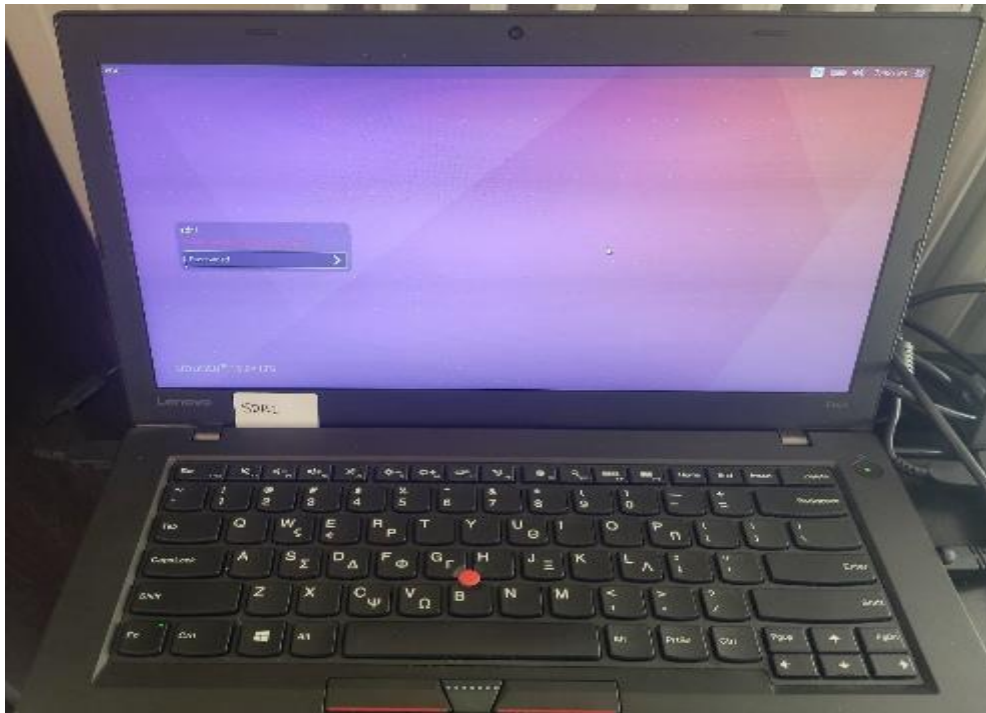
Operating Temperature: -40°C-85°C

Humidity: non-condensing 65°C, 95%RH

Size: 47mm in diameter, 30mm in height

4.4 Εξοπλισμός του EPC

Για τις λειτουργίες του EPC χρησιμοποιήθηκε ένα Laptop Lenovo T450,



Εικόνα 52. Lenovo T450 για το eNB

με τα παρακάτω τεχνικά χαρακτηριστικά:

Processor	Intel® Core™ i5-5300U Processor (3M Cache, up to 2.90 GHz)
Memory	Up to 16GB (2 DIMMS)
Storage	2.5" Hard Drives – SSD 256 GB /
Display	14" HD (1366 x 768) Antiglare
Communication	WLAN – Intel® 11 a/c + BT 4.0, Intel® 11 a/g/n + BT 4.0

4.4.1 Λειτουργικό EPC

Για την υλοποίηση των λειτουργιών του EPC χρησιμοποιήθηκε το ανοιχτού κώδικα ελεύθερο λογισμικό Ubuntu Linux 16.04. Έγινε λήψη του λειτουργικού και περάσαμε το image σε ένα usb stick

Ubuntu 16.04.7 LTS (Xenial Xerus)

Select an image

Ubuntu is distributed on two types of images described below.

Desktop image

The desktop image allows you to try Ubuntu without changing your computer at all, and at your option to install it permanently later. This type of image is what most people will want to use. You will need at least 384MB of RAM to install from this image.

64 bit PC (AMD64) desktop image

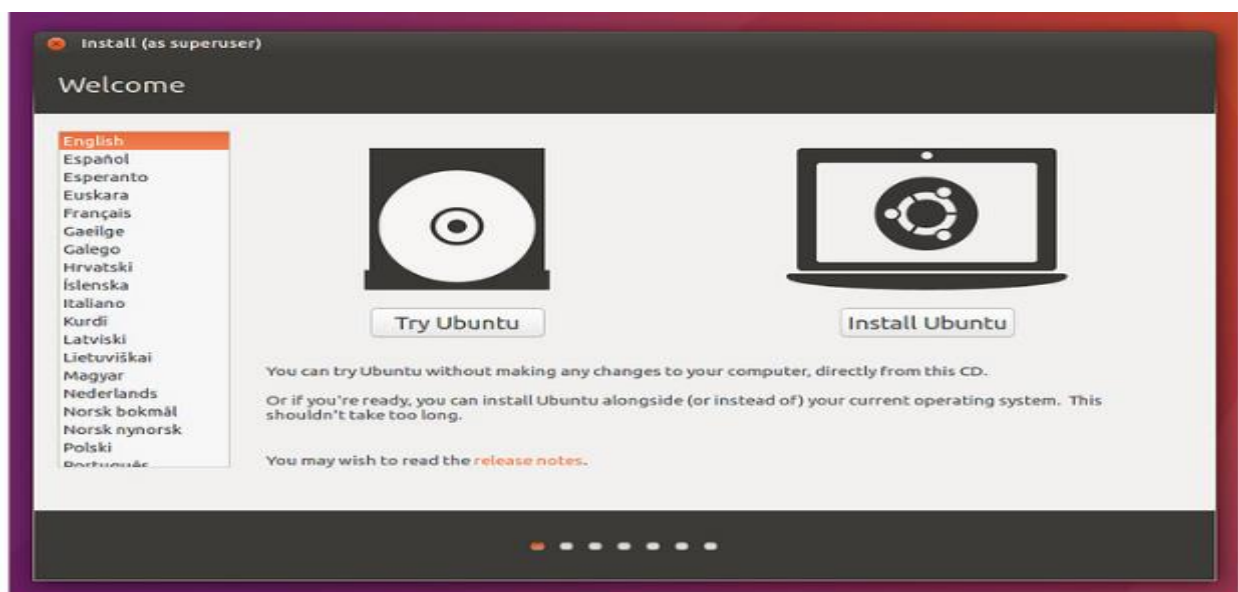
Choose this if you have a computer based on the AMD64 or EM64T architecture (e.g. Athlon64, Opteron, EM64T Xeon, Core 2). Choose this if you are at all unsure.

32 bit PC (i386) desktop image

For almost all PCs. This includes most machines with Intel (AMD) 32-bit type processors and almost all computers that run Microsoft Windows, as well as newer Apple Macintosh systems based on Intel processors.

Εικόνα 53. Λήψη λειτουργικού [F28]

Όστε να ξεκινήσουμε την διαδικασία εγκατάστασης του στο Laptop.



Εικόνα 54. Εγκατάσταση λειτουργικού [F29]

Μετά την επιτυχή ολοκλήρωση της εγκατάστασης του λειτουργικού Ubuntu Linux 16.04 προχωρήσαμε στην λήψη του XZ Utils.

4.4.2 XZ utils

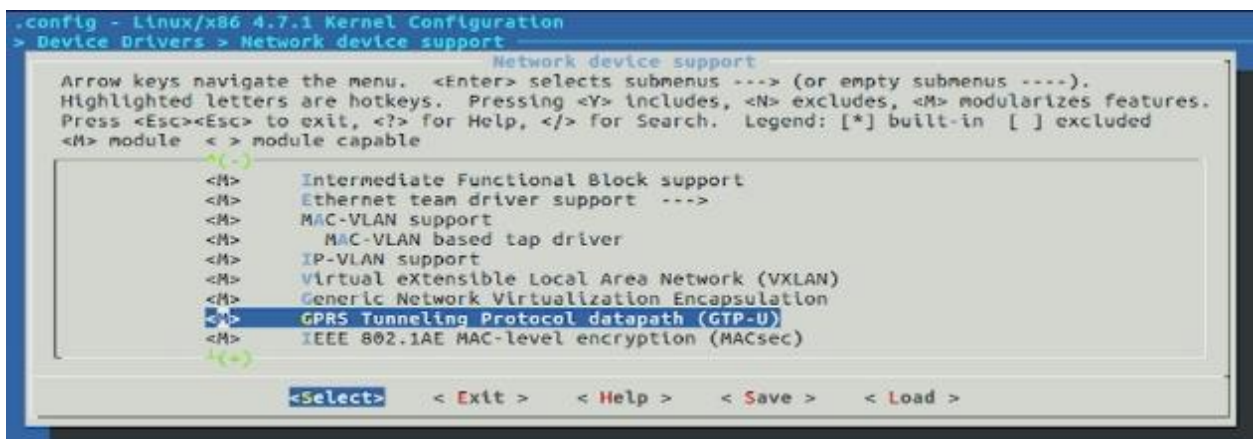
Το XZ Utils είναι ένα δωρεάν λογισμικού συμπίεσης- αποσυμπίεσης αρχείων για το λειτουργικό Linux για γραμμές εντολών και περιλαμβάνει τα προγράμματα lzma και xz. Κατά την συμπίεση και αποσυμπίεση χρησιμοποιείται ο αλγόριθμος αλυσίδας Lempel-Ziv-Markov (LZMA). Το XZ Utils ξεκίνησε ως μια μεταφορά του LZMA-SDK του Igor Pavlov για το Unix, το οποίο έχει προσαρμοστεί για να ενσωματωθεί άψογα στο περιβάλλον Unix -Linux [74].

4.4.3. Εγκατάσταση Generic Kernel, ενεργοποίηση GPRS protocol, ηproc

Το πρωτόκολλο GPRS είναι ένα σύνολο από πρωτόκολλα επικοινωνίας βασισμένα στο IP, υπεύθυνα για μεταφορά πακέτων GPRS σε δίκτυα LTE 5G και άλλων. Το GTP-U χρησιμοποιείται για τη μεταφορά των δεδομένων εντός του βασικού δικτύου GPRS και μεταξύ του δικτύου ασύρματης πρόσβασης και του βασικού δικτύου. Τα δεδομένα αυτά μπορεί να είναι πακέτα σε οποιαδήποτε από τις μορφές IPv4, IPv6 ή PPP [74].

Το ηproc είναι μια εντολή στο λειτουργικό Linux χρησιμοποιείται για να ελέγξει πόσες μονάδες επεξεργασίας είναι διαθέσιμες ή εγκατεστημένες στο σύστημά μας για την εκτύπωση του αριθμού των μονάδων επεξεργασίας που είναι διαθέσιμες στο σύστημα ή στην τρέχουσα διεργασία.

Πριν την εγκατάσταση του Generic kernel έκδοση 4.7.1, έπρεπε να ενεργοποιήσαμε το GPRS Tunneling Protocol.



Εικόνα 55. Ενεργοποίηση GPRS Tunneling Protocol

Για να μπορέσει το EPC να εκτελεί παράλληλες διεργασίες, όπως θα δούμε και παρακάτω, ταυτόχρονη εκτέλεση του HSS, MME και SPGW, έπρεπε να τρέξουμε την εντολή ηproc και να αυξήσουμε τα modules ώστε να αυξηθούν οι παράλληλες διεργασίες.


```

sdr1@sdr1-ThinkPad-T460: ~/linux-4.7.1
IHEX firmware/qlogic/12160.bin
IHEX firmware/qlogic/sd7220.fw
IHEX firmware/korg/k1212.dsp
IHEX firmware/ess/maestro3_assp_kernel.fw
IHEX firmware/ess/maestro3_assp_minisrc.fw
IHEX firmware/yamaha/ds1_ctrl.fw
IHEX firmware/yamaha/ds1_dsp.fw
IHEX firmware/tehuti/bdx.bin
IHEX firmware/tigon/tg3.bin
IHEX firmware/yamaha/ds1e_ctrl.fw
IHEX firmware/tigon/tg3_tso.bin
IHEX firmware/tigon/tg3_tso5.bin
IHEX firmware/3com/typhoon.bin
IHEX2FW firmware/eml26/loader.fw
IHEX2FW firmware/eml26/firmware.fw
IHEX2FW firmware/eml26/bitstream.fw
IHEX2FW firmware/eml62/bitstream.fw
IHEX2FW firmware/eml62/loader.fw
IHEX2FW firmware/eml62/spdif.fw
IHEX2FW firmware/eml62/midi.fw
IHEX firmware/kaweth/new_code.bin
IHEX firmware/kaweth/trigger_code.bin
IHEX firmware/kaweth/new_code_fix.bin
IHEX firmware/kaweth/trigger_code_fix.bin
IHEX firmware/ti_3410.fw
IHEX firmware/tl_5052.fw
IHEX firmware/mts_cdma.fw
IHEX firmware/mts_gsm.fw
IHEX firmware/mts_edge.fw
H16TOFW firmware/edgeport/boot.fw
H16TOFW firmware/edgeport/boot2.fw
H16TOFW firmware/edgeport/down.fw
H16TOFW firmware/edgeport/down2.fw
IHEX2FW firmware/whiteheat_loader.fw
IHEX firmware/edgeport/down3.bin
IHEX2FW firmware/whiteheat.fw
IHEX2FW firmware/keyspan_pda/keyspan_pda.fw
IHEX2FW firmware/keyspan_pda/xlrcom_pgs.fw
IHEX firmware/cpia2/stv0672_vp4.bin
IHEX firmware/yam/1200.bin
IHEX firmware/yam/9600.bin
sdr1@sdr1-ThinkPad-T460:~/linux-4.7.1$

```

Εικόνα 56. ολοκλήρωση διεργασίας προς

Μετά την ολοκλήρωση των απαραίτητων εργασιών για τις διεργασίες, κάναμε την εγκατάσταση του Generic Kernel για τα Linux 16.04

```

sdr1@sdr1-ThinkPad-T460:~/linux-4.7.1$ sudo make install
sh ./arch/x86/boot/install.sh 4.7.1 arch/x86/boot/bzImage \
    System.map "/boot"
run-parts: executing /etc/kernel/postinst.d/apt-auto-removal 4.7.1 /bo
ot/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/initramfs-tools 4.7.1 /boo
t/vmlinuz-4.7.1
update-initramfs: Generating /boot/initrd.img-4.7.1
run-parts: executing /etc/kernel/postinst.d/pm-utils 4.7.1 /boot/vmlin
uz-4.7.1
run-parts: executing /etc/kernel/postinst.d/unattended-upgrades 4.7.1
/boot/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/update-notifier 4.7.1 /boo
t/vmlinuz-4.7.1
run-parts: executing /etc/kernel/postinst.d/zz-update-grub 4.7.1 /boot
/vmlinuz-4.7.1
Generating grub configuration file ...
Warning: Setting GRUB_TIMEOUT to a non-zero value when GRUB_HIDDEN_TIM
EOUT is set is no longer supported.
Found linux image: /boot/vmlinuz-4.15.0-142-generic
Found initrd image: /boot/initrd.img-4.15.0-142-generic
Found linux image: /boot/vmlinuz-4.15.0-112-generic
Found initrd image: /boot/initrd.img-4.15.0-112-generic
Found linux image: /boot/vmlinuz-4.7.1
Found initrd image: /boot/initrd.img-4.7.1
Adding boot menu entry for EFI firmware configuration
done
sdr1@sdr1-ThinkPad-T460:~/linux-4.7.1$

```

Εικόνα 57. Εγκατάσταση και ολοκλήρωση του Generic Kernel στο EPC

4.5 Παραμετροποίηση του EPC

Μετά την επιτυχή εγκατάσταση του Generic kernel, έπρεπε να κάνουμε ενημέρωση του λογισμικού, και εγκαταστήσουμε το Software git στο, ώστε να κάνουμε download τον Open Source κώδικα, για την λειτουργία του EPC

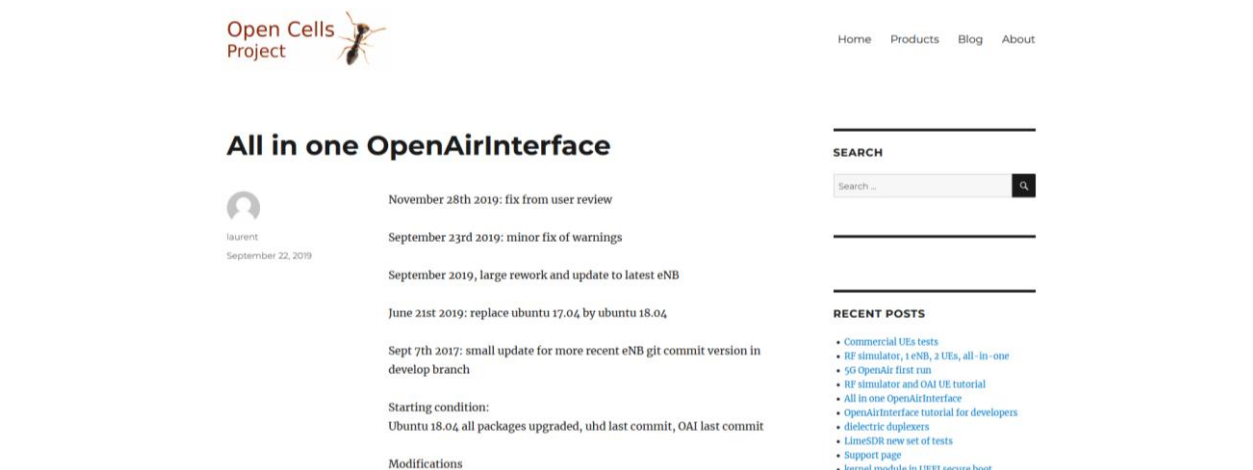
Αντίστοιχα με το eNB έπρεπε να γίνει εγκατάσταση του certificate ώστε να δοθεί πρόσβαση στο gitlab της eurescom, και να γίνει η λήψη του κώδικα.

```
sdr1@sdr1-ThinkPad-T460: ~
Zs5wDgYDVR0PAAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAFBwEQYDVIR0gBAowCDAG
BgRVHSAAMENGA1UdHwQ8MDowOKA2oDSGMh0dHA6Ly9jcmwY29tb2RvY2EuY29t
L0FBQUNlcnRpZmljYXRlU2VydmljZXMUy3JSM0QGCCsGAQUFBwEBBCEwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuY29tb2RvY2EuY29tMA0GC5qGSIB3DQEBDAUA
A4IBAQAyH1HcdCE9nIrgJ7cz0C7H7PDmy14R3tJvM3W0nnL+5Nb+qh+cL13vA0p+
rvSNb3I8QzvAP+u431yqqcau8vzY7qN7Q/aGNnwU4M309z/+3r10ivCRlv79Q2R+
/czSAaF9ffgZGcLCKx0/WIu6pKJmBHaIkU4MhRT0ok3JMr066BQavHHxW/BBC5gA
C1IDE0UMsfnNkjcZ7Tvx5Dq2+UUTJhWvu6rvP3t309LEApE9GQDTF1w52z97GA1F
zZ0Fl19d31kWTZ9RvdVFGD/tSo7o8mF0Ixa1DVBzJ0RHfXBd1SprhTEUx0iPakyA
vGp4z7h/jnZymQyd/teRCBaho1+v
-----END CERTIFICATE-----
```

Εικόνα 58. Επιτυχής εγκατάσταση Certificate στο eNB στο EPC

Με την επιτυχή εγκατάσταση του certificate `---END CERTIFICATE---` μπορέσαμε και αποκτήσαμε πρόσβαση στην βιβλιοθήκη της Eurescom και κατεβάσαμε τον πηγαίο κώδικα για το eNB.

Από την ιστοσελίδα της open cells κατεβάσαμε το συμπιεσμένο αρχείο **Openair-cn.tgz** που είναι μια ολοκληρωμένη υλοποίηση προδιαγραφών 3GPP και αφορά τα εξελιγμένα μοντέλα δικτύων όπου εμπεριέχουν την υλοποίηση MME, HSS, S-GW και P-GW (SPGW).



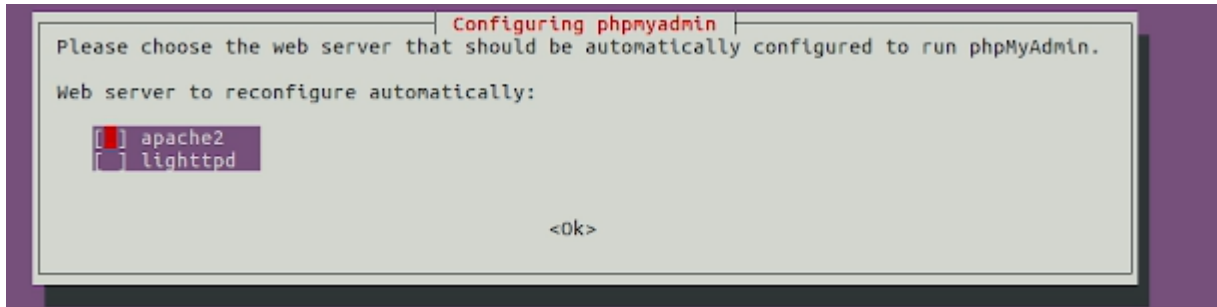
Εικόνα 59. Open cells λήψη του openair-cn [F30]

4.5.1 Ορισμός FQDN εγκατάσταση βάσης δεδομένων.

Το FQDN Fully Qualified Domain Name είναι το όνομα του Domain εντός δικτύου και καθορίζει την ακριβή τοποθεσία ενός συγκεκριμένου υπολογιστή εντός του δικτύου. Το Hostname, αναφέρεται στο όνομα που έχει ανατεθεί σε μια συγκεκριμένη συσκευή εντός του δικτύου.

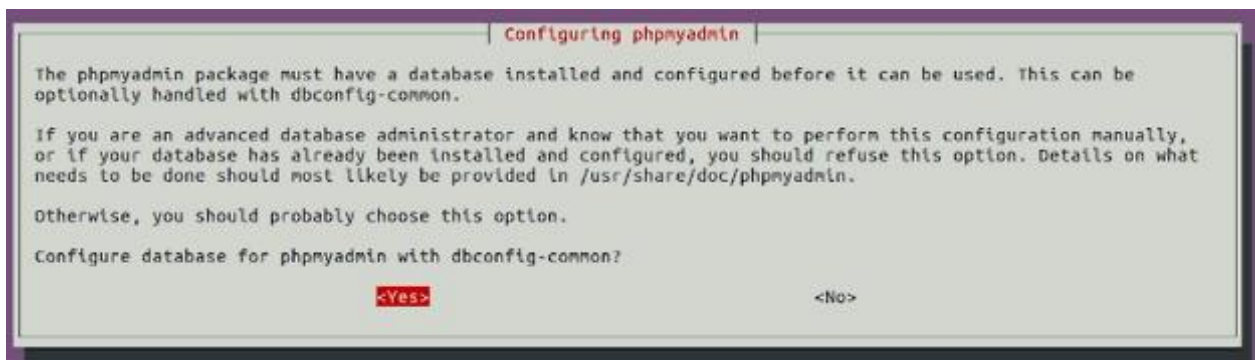
Στην δική μας περίπτωση το όνομα του Domain το ορίσαμε ως erc, και προχωρήσαμε στην εγκατάσταση των οντοτήτων, SPGW MME και HSS, που θα χρησιμοποιηθούν.

Το HSS που όπως έχουμε αναφέρει είναι η βάση που περιέχει όλα εκείνα τα στοιχεία σύνδεσης των συνδρομητών και των UICC που θα μπορέσουν να συνδεθούν στο δίκτυο μας. Για το λόγο αυτό κάναμε εγκατάσταση της MySQL local και της PhpMyAdmin (apache2) βάσης δεδομένων στο EPC.



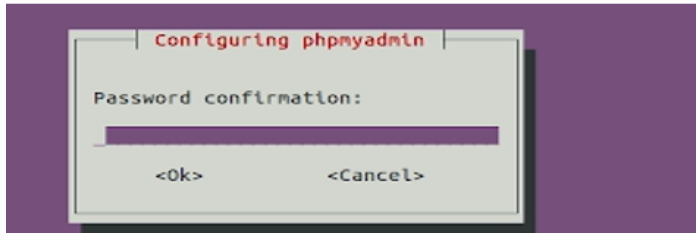
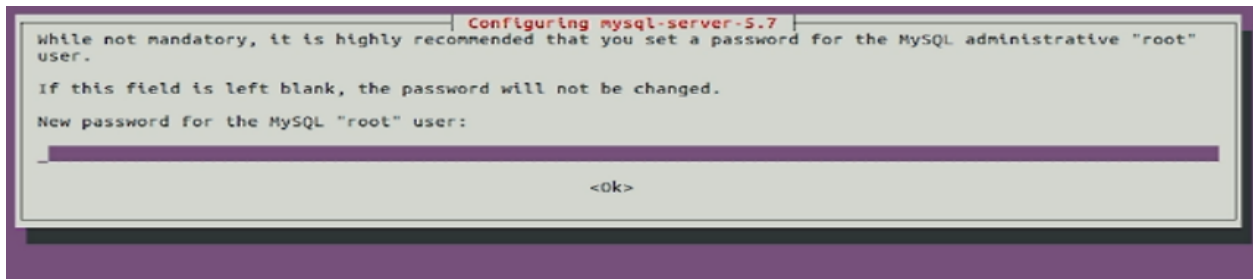
Εικόνα 60. Εγκατάσταση MySQL και PhpMyAdmin στο EPC

Ενώ επιλέξαμε να γίνει εγκατάσταση του γραφικού περιβάλλοντος GUI της PhpMyAdmin για λόγους ευκολίας.



Εικόνα 61. Εγκατάσταση GUI της PhpMyAdmin στο EPC

Αφού ορίσαμε τον user που θα συνδέεται στην βάση και το password του.



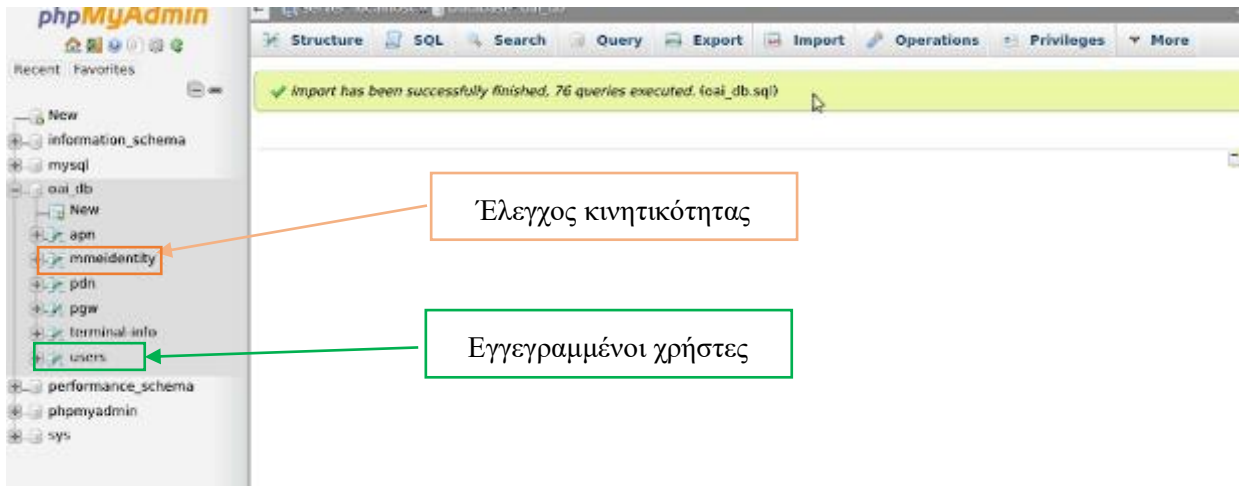
Εικόνα 62. Ορισμός Username/Password στην βάση για το HSS

Ολοκληρώσαμε την εγκατάσταση και ελέγξαμε την προσβασιμότητα μας στην βάση δεδομένων στην διεύθυνση <http://127.0.0.1/phpmyadmin/>



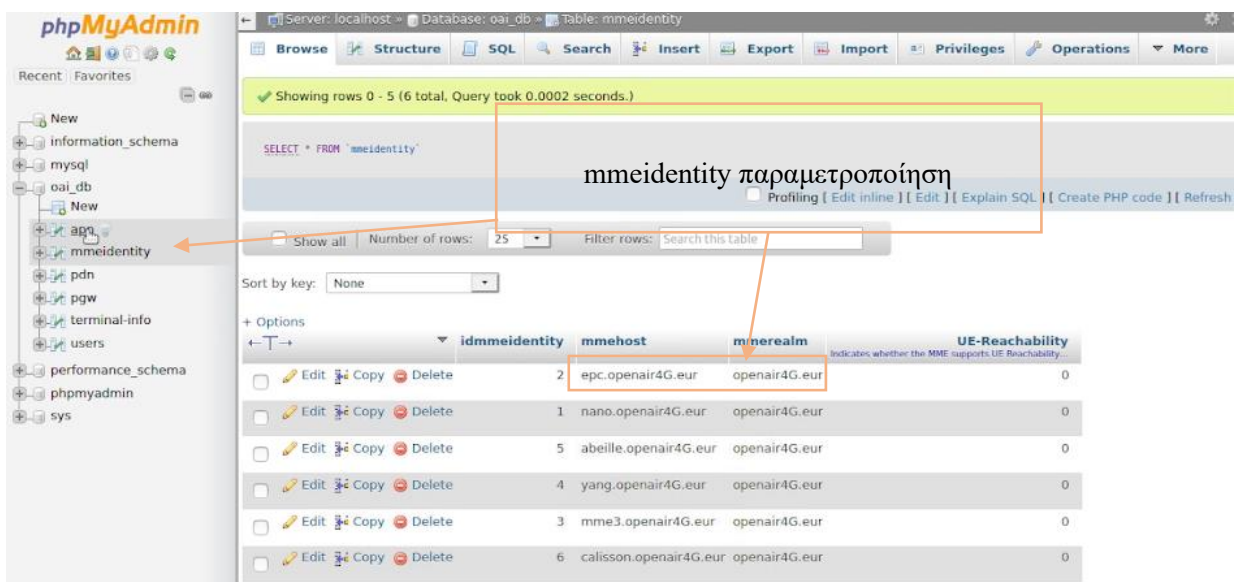
Εικόνα 63. PhpMyAdmin login Page

Για να μπορέσουμε να εισάγουμε τα στοιχεία των χρηστών που θα μπορούν να συνδεθούν στο δίκτυο μας, έπρεπε να φτιάξουμε μια νέα βάση. Εκεί προσθέσουμε τις οντότητες που χρειαζόμασταν. Οπότε δημιουργήσαμε μια νέα βάση με το όνομα `oai_db` και κάναμε import τα στοιχεία της από το `hss path (openair-cn\src\oai_hss\db\oai_db.sql)` μέσα στην phpMyAdmin.



Εικόνα 64. Η νέα βάση oai_db του HSS

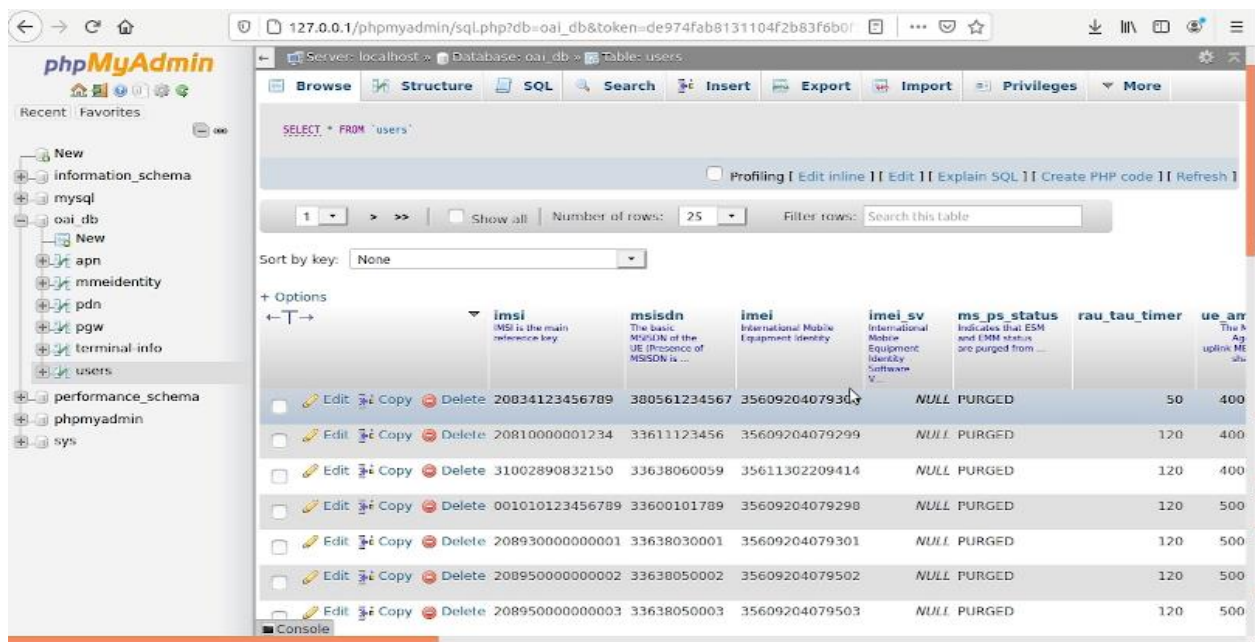
Μετά την εισαγωγή των οντοτήτων στην εγγραφή Users εγγράψαμε τους χρήστες που θα μπορούν να συνδεθούν στο δίκτυο μας. Το mmeidentity είναι ένα το βασικό συστατικό του EPC για το LTE, και παρέχει την διαχείριση των συνδέσεων και κινητικότητας για το δίκτυο ενώ υποστηρίζει ταυτόχρονα και τον έλεγχο ταυτότητας συνδρομητών.



Εικόνα 65. Το Domain name του mmeidentity (epc.openair4G.eur)

mmeidentity	2
mmehost	epc.openair4G.eur
mmerealm	openair4G.eur
UE-reachability	0

Πίνακας 6. Πεδίο mmeidentity (hss)



Εικόνα 66. Παραμετροποίηση των χρηστών

Πριν τον προγραμματισμό της κάρτας UICC, κάναμε την εγγραφή ενός χρήστη που θα μπορεί να έχει πρόσβαση στο δίκτυο μας. Παρακάτω ο πίνακας με τις σχετικές πληροφορίες της εγγραφής.

<i>imsi</i>	2089300000000003
<i>msisdn</i>	00000934
<i>imei</i>	NULL
<i>imei_sv</i>	NULL
<i>ms_ps_status</i>	PURGED
<i>rau_tau_timer</i>	120
<i>ue_ambr_ul</i>	50000000
<i>ue_ambr_dl</i>	100000000
<i>access_restriction</i>	47
<i>mme_cap</i>	0000000000
<i>mmeidentity_idmmeidentity</i>	2
<i>key</i>	8baf473f2f8fd09487cccbd7097c6862
<i>RFSP-Index</i>	1
<i>urrrp_mme</i>	0
<i>sqn</i>	0000000000000000256
<i>rand</i>	0
<i>OPc</i>	8e27b6af0e692e750f32667a3b14605d

Πίνακας 7. Πεδίο users (hss)

Στο σημείο αυτό έπρεπε να παραμετροποιήσουμε τις οντότητες λειτουργίας του EPC MME,HSS,SPGW, για το δικό μας δίκτυο. Στους πίνακες που ακολουθούν δίνονται οι παράμετροι που ορίσαμε.

<i>MME_INTERFACE_NAME_FOR_S1_MME</i>	<i>eth0;</i>
<i>MME_IPV4_ADDRESS_FOR_S1_MME</i>	<i>192.168.12.63/24;</i>
<i>MME_INTERFACE_NAME_FOR_S11_MME</i>	<i>lo;</i>
<i>MME_IPV4_ADDRESS_FOR_S11_MME</i>	<i>127.0.11.1/8;</i>
<i>MME_PORT_FOR_S11_MME</i>	<i>2123;</i>

Πίνακας 8. Παράμετροι NETWORK INTERFACE MME

<i>MYSQL_server</i>	<i>127.0.0.1</i>
<i>MYSQL_user</i>	<i>root</i>
<i>MYSQL_pass</i>	<i>uniwa</i>
<i>MYSQL_db</i>	<i>oai_db</i>
<i>OPERATOR_key</i>	<i>"11"</i>

Πίνακας 9. Παράμετροι SQL SERVER

<i>MME served GUMMEIs</i>	<i>MCC="208" ; MNC="93";</i>
	<i>MME_GID="4" ; MME_CODE="1";</i>
<i>MME served TAIs</i>	<i>MCC="208" ; MNC="93"; TAC = "1";</i>

Πίνακας 10. Παράμετροι σύνδεσης των UICC καρτών.

<i>SGW_INTERFACE_NAME_FOR_S11</i>	<i>lo;</i>
<i>SGW_IPV4_ADDRESS_FOR_S11</i>	<i>127.0.11.2/8;</i>
<i>SGW_INTERFACE_NAME_FOR_S1U_S12_S4_UP</i>	<i>eth0;</i>
<i>SGW_IPV4_ADDRESS_FOR_S1U_S12_S4_UP</i>	<i>192.168.12.63/24;</i>
<i>SGW_IPV4_PORT_FOR_S1U_S12_S4_UP</i>	<i>2152;</i>
<i>SGW_INTERFACE_NAME_FOR_S5_S8_UP</i>	<i>none;</i>
<i>SGW_IPV4_ADDRESS_FOR_S5_S8_UP</i>	<i>0.0.0.0/24;</i>
<i>PGW_INTERFACE_NAME_FOR_S5_S8</i>	<i>none;</i>
<i>PGW_IPV4_ADDRESS_FOR_S5_S8</i>	<i>0.0.0.0/24;</i>
<i>PGW_INTERFACE_NAME_FOR_SGI</i>	<i>wlan0;</i>
<i>PGW_IPV4_ADDRESS_FOR_SGI</i>	<i>192.168.2.19/24;</i>
<i>PGW_MASQUERADE_SGI</i>	<i>yes;</i>
<i>UE_TCP_MSS_CLAMPING</i>	<i>no;</i>

Πίνακας 11. Παράμετροι δικτύου για SGW και PGW (SPGW)

<i>ALLOW_OLD_TLS</i>	<i>*.openair4G.eur</i>
----------------------	------------------------

Πίνακας 12. Παράμετροι Diameter/acl

<i>IDENTITY</i>	<i>epc.openair4G.eur;</i>
<i>REALM</i>	<i>"openair4G.eur";</i>
<i>CONNECTPEER</i>	<i>"hss.openair4G.eur" { ConnectTo = "127.0.33.1"; No_SCTP ; No_IPv6; Prefer_TCP; No_TLS; port = 3868; realm = "openair4G.eur";};</i>

Πίνακας 13. Παράμετροι Diameter/mme_fd

<i>IDENTITY</i>	<i>"hss.openair4G.eur";</i>
<i>REALM</i>	<i>"openair4G.eur";</i>

Πίνακας 14. Παράμετροι Diameter/hss_fd

Πριν την έναρξη των δοκιμών ελέγξαμε ότι τα απαραίτητα Certificates είναι ενεργά και για την βάση δεδομένων του HSS αλλά και για την κινητικότητα του δικτύου MME, μετά την αλλαγή των παραμέτρων που κάναμε παραπάνω.

```

sdr1@sdr1-ThinkPad-T460: ~/openair-cn/scripts
Subject:
  countryName           = FR
  stateOrProvinceName  = PACA
  organizationName      = Eurecom
  organizationalUnitName = CM
  commonName            = hss.openair4G.eur
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    8A:4C:F3:7A:CA:06:C8:28:DC:43:1E:66:5C:44:0C:27:8A:60:D5:C9
  X509v3 Authority Key Identifier:
    keyId:90:ED:45:E0:70:A4:57:5F:90:D4:3B:F5:C3:73:A8:35:DE:30:92:3
E
Certificate is to be certified until Mar 23 16:40:28 2024 GMT (365 days)

```

Εικόνα 67. Hss έλεγχος certificate


```
sdr1@epc: ~/openair-cn/scripts
Subject:
  countryName           = FR
  stateOrProvinceName  = PACA
  organizationName     = Eurecom
  organizationalUnitName = CM
  commonName           = epc.openair4G.eur
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    0D:C9:C6:99:3D:13:36:5B:42:16:AD:C0:6F:E8:A8:53:E2:B5:17:05
  X509v3 Authority Key Identifier:
    keyid:80:B9:3D:E1:70:EC:F9:68:B5:B3:7F:3B:98:6E:F8:10:09:5D:92:3
6
Certificate is to be certified until Mar 26 16:04:49 2024 GMT (365 days)
```

Εικόνα 68. MME έλεγχος certificate

4.6 Προετοιμασία του Asterisk Server

Για τις λειτουργίες του Asterisk χρησιμοποιήθηκε ένα Raspberry pi 4



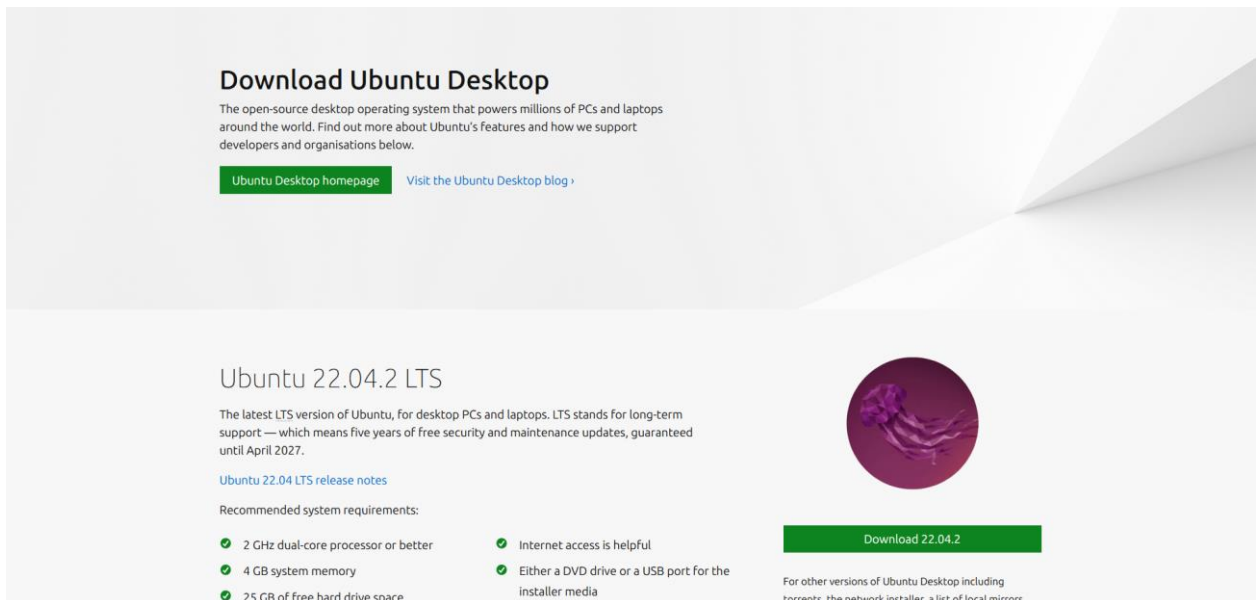
Εικόνα 67. Raspberry pi 4

με τα παρακάτω χαρακτηριστικά:

Processor	Broadcom BCM2711, quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz
Memory	8GB on Board
Storage	SD card / Micro SD 64 GB
Display	Support 2 × micro HDMI ports (up to 4Kp60)
Communication	2.4 GHz and 5.0 GHz IEEE 802.11b/g/n/ac wireless
Input Power	5V DC via USB-C connector (minimum 3A)

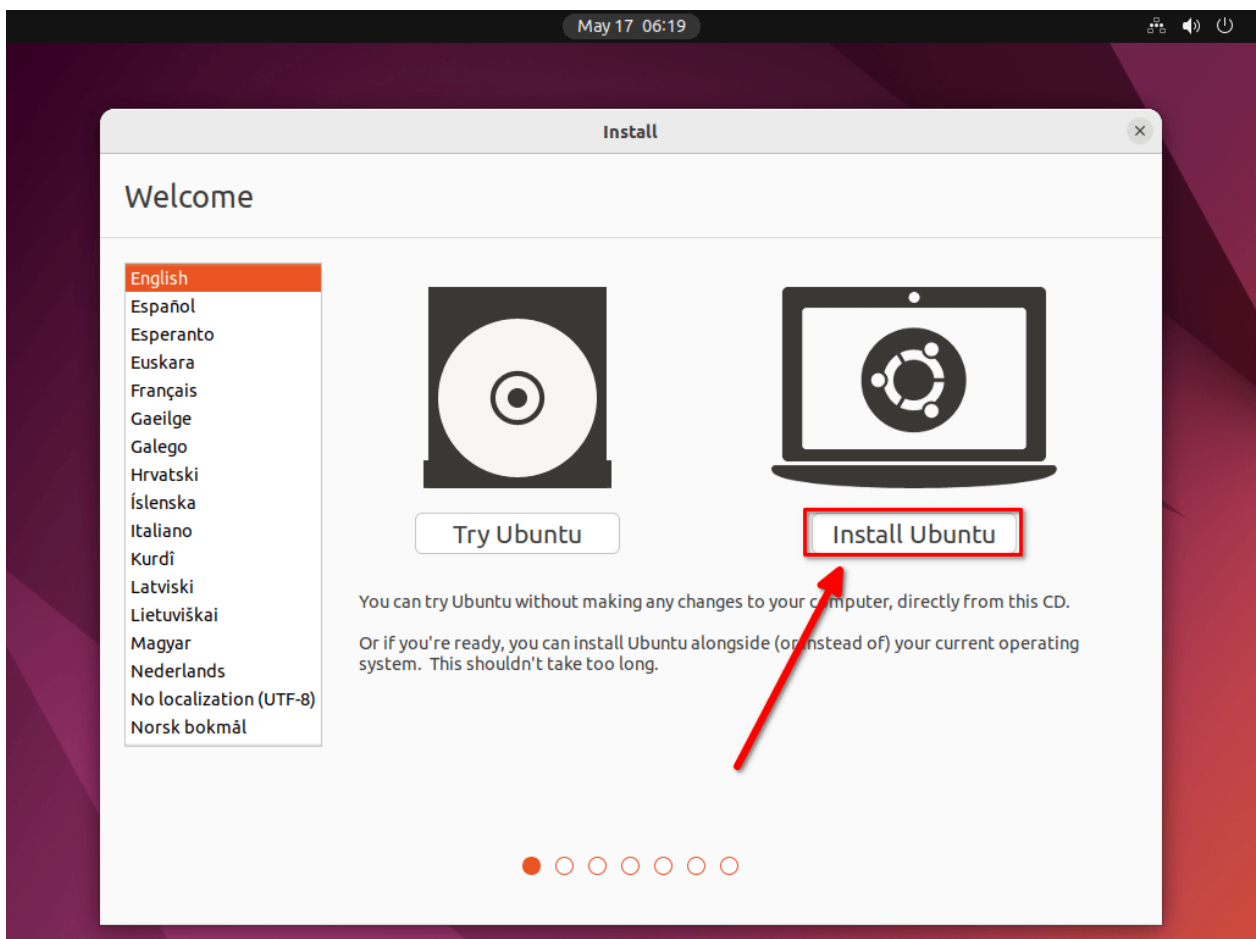
4.6.1 Λειτουργικό του Asterisk Server

Για την υλοποίηση των κλήσεων εντός του δικτύου χρησιμοποιήθηκε το ανοιχτού κώδικα ελεύθερο λογισμικό Ubuntu Linux 22.04. Έγινε λήψη του λειτουργικού και περάσαμε το image σε ένα usb stick



Εικόνα 68. Λήψη λειτουργικού [F31]

Όστε να ξεκινήσουμε την διαδικασία εγκατάστασης του στο Raspberry pi 4



Εικόνα 69. Εγκατάσταση λειτουργικού [F32]

4.6.2 Υλοποίηση και παραμετροποίηση του Asterisk

Μετά την επιτυχή ολοκλήρωση της εγκατάστασης του λογισμικού, ξεκινήσαμε την εγκατάσταση του Asterisk

```
update-alternatives: using /usr/share/asterisk/sounds/en_US_f_Allison to provide /usr/share/asterisk/sounds/en
terisk-prompt-en) in auto mode
update-alternatives: using /usr/share/asterisk/sounds/en_US_f_Allison to provide /usr/share/asterisk/sounds/en
(asterisk-prompt-en-us) in auto mode
Setting up libiksemel3:amd64 (1.4-3build1) ...
Setting up liburiparser1:amd64 (0.9.3-2) ...
Setting up asterisk-moh-opsound-gsm (2.03-1) ...
Setting up liblua5.1-0:amd64 (5.1.5-8.1build4) ...
Setting up libopencore-amrnb0:amd64 (0.1.5-1) ...
Setting up libsox-fmt-base:amd64 (14.4.2+git20190427-2) ...
Setting up libesample1 (0.1.5-4) ...
Setting up freetds-common (1:1.6-1.1) ...
Setting up libsybdb5:amd64 (1:1.6-1.1) ...
Setting up sox (14.4.2+git20190427-2) ...
Setting up asterisk-modules (1:16.2.1-dfsg-2ubuntu1) ...
Setting up asterisk (1:16.2.1-dfsg-2ubuntu1) ...
Adding system user for Asterisk
Adding user `asterisk' to group `dialout' ...
Adding user asterisk to group dialout
Done.
Adding user `asterisk' to group `audio' ...
Adding user asterisk to group audio
Done.
Created symlink /etc/systemd/system/multi-user.target.wants/asterisk.service → /lib/systemd/system/asterisk.serv
e.
Setting up asterisk-voicemail (1:16.2.1-dfsg-2ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9) ...
Processing triggers for systemd (245.4-4ubuntu3.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for dbus (1:1.12-2ubuntu1) ...
```

Εικόνα 70. Εγκατάσταση Asterisk

Μετά την ολοκλήρωση της εγκατάστασης έπρεπε να οργανώσουμε τις διαδρομές κλήσεων που θα γίνονται από συνδρομητή σε συνδρομητή εντός του ιδιωτικού μας δικτύου.

Μέσω του sip.conf που είναι το πρωτόκολλο επικοινωνίας που χρησιμοποιεί κατεχοχόν το Voip, ορίσαμε στο τοπικό ιδιωτικό μας δίκτυο και σε ποια port θα λειτουργεί. Επίσης του ορίσαμε έναν 4 ψηφιο αριθμό που θα έχει ο κάθε συνδρομητής του δικτύου μας. Για της ανάγκες της υλοποίησης μας ορίσαμε 2 συνδρομητές Το 7001 και 7002 καθώς με τους αντίστοιχους κωδικούς ασφαλείας τους.

Το αρχείο extensions.conf είναι ένα από τα πιο χρησιμοποιημένα και πιο σημαντικά αρχεία στο Asterisk, αφού περιέχει το σχέδιο κλήσης. Το σχέδιο κλήσης, ορίζει για το πώς το Asterisk θα χειρίζεται τις εισερχόμενες και εξερχόμενες κλήσεις Το σχέδιο κλήσης χωρίζεται σε ενότητες που ονομάζονται περιβάλλοντα. Κάθε πλαίσιο αποτελείται από περισσότερες από μία επεκτάσεις, που είναι ο αριθμός τηλεφώνου. Κάθε επέκταση έχει μια προτεραιότητα και μια εφαρμογή. Με τη βοήθεια των πλαισίων μπορούμε να οργανώσουμε το σχέδιο κλήσης μας.

Το voicemail.conf είναι η υπηρεσία τηλεφωνητή όπου σε περίπτωση που δεν απαντηθεί η κλήση να γίνει προώθηση της σε ένα αυτόματο τηλεφωνητή.

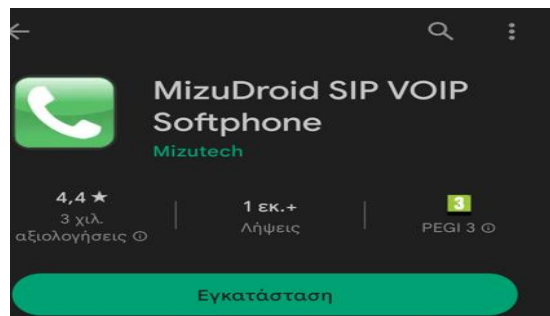
4.6.3 Εγκατάσταση του Client στα UEs

Τα τηλέφωνα που δοκιμάστηκαν καθ' όλη την διάρκεια της υλοποίησης είναι τα Samsung Galaxy S40 με λειτουργικό Android 12 και S32 με λειτουργικό Android 10 αντίστοιχα. Ο Πίνακας που ακολουθεί πίνακας περιγραφής

Smartphone Model Name	Samsung Galaxy A40	Samsung Galaxy A32
Release Year	2019	2021
LTE DL/UL Modulation	64QAM / 16QAM	256QAM / 64QAM
LTE Bands	1, 3, 7, 20, 38	1, 2, 3, 4, 5, 7, 8, 12, 17, 20, 26, 28, 38, 40, 41, 66
LTE Category (DL/UL)	(4/6)	(16 / 5)
LTE Max Speed (DL/UL)	300 / 50 Mbps	1000 / 75 Mbps
Operating System	Android 9.0	Android 11

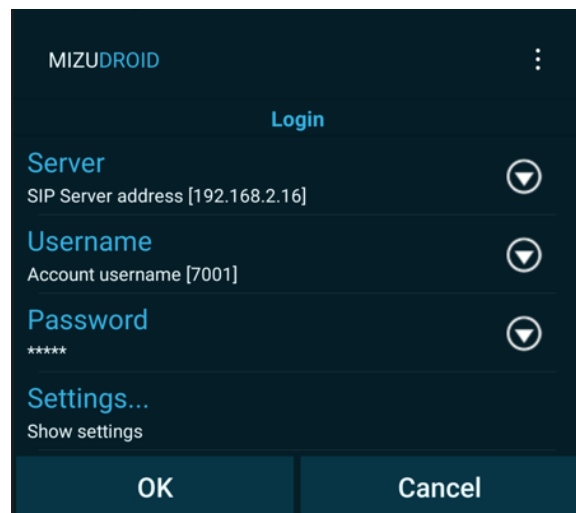
Εικόνα 71. Χαρακτηριστικά smartphones

Σε κάθε ένα από αυτά κάναμε εγκατάσταση του Client Mizudroid



Εικόνα 72. Mizudroid Client

Σε κάθε συσκευή ορίσαμε την διεύθυνση του Server που φιλοξενεί το Asterisk το 4ψήφιο του καθώς και τον κωδικό ασφαλείας του. Τις υπόλοιπες ρυθμίσεις τις αφήσαμε ως υπήρχαν για μελλοντική δοκιμή.



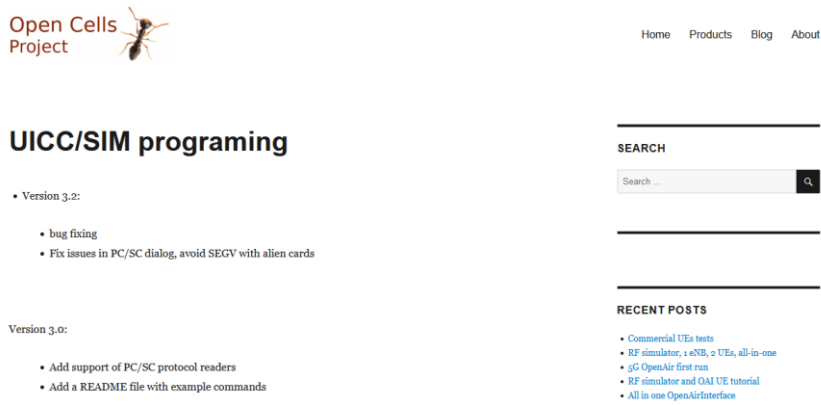
Εικόνα 73. Παραμετροποίηση του Mizudroid

Server	192.186.2.16
Username	7001
Password	7001

Πίνακας 15. Παράμετροι του Mizudroid

4.7 Προγραμματισμός Καρτών UICC

Για να συνδεθούν τα UEs στο δίκτυο έπρεπε να προγραμματίσουμε τις UICC κάρτες με βάση τα στοιχεία των χρηστών που περάσαμε στο HSS. Αυτό πραγματοποιήθηκε με την λήψη του `program_uicc` της Open Cells, και με την χρήση ενός USB UICC reader.



Εικόνα 69. Open Cells UICC [F33]



Εικόνα 70. Προγραμματισμός της USIM κάρτας

Για τις ανάγκες υλοποίησης και δοκιμών προγραμματίσαμε 2 κάρτες.

```
$sudo ./program_uicc --adm xxxxxxxx --imsi 2089300000000003 --opc 8e27b6af0e692e750f32667a3b14605d --key 8baf473f2f8fd09487cccbd7097c6862 --spn uniwan --authenticate
```

- Το `adm` είναι ο μοναδικός κωδικός με τον οποίο εγγράψαμε τις κάρτες της Open Cells, και μας στάλθηκε από την Open Cells μαζί της κάρτες.
- Το `imsi` είναι ο μοναδικός αριθμός της κάθε κάρτας ο οποίος αναγνωρίζεται και ως μοναδικός χρήστης μέσα στο HSS.
- Το `spn` είναι το όνομα του δικτύου υπηρεσιών και αυτό θα εμφανίζεται όταν θα συνδέονται τα κινητά τηλέφωνα. Στην δική μας περίπτωση ονομάστηκε **uniwan**

- Το key είναι το μοναδικό κλειδί ελέγχου ταυτοποίησης της κάρτας με το HSS για δίκτυα LTE και ορίζεται μέσα στο HSS ώστε να πιστοποιείται ο χρήστης μέσα στο δίκτυο.
- Το opc ορίζει την μοναδικότητα του χρήστη σε συνδυασμό με το imsi και ορίζεται και στο HSS το μοναδικό κλειδί ταυτοποίησης με το δίκτυο
- Τέλος το authenticate είναι ο έλεγχος πως όλα τα παραπάνω έχει ολοκληρωθεί σωστά και κλείνει η ταυτοποίηση της κάρτας με το HSS.

```

Reading UICC values after uploading new values
ICCID: 89860061100000000934
WARNING: iccid luhn encoding of last digit not done
USIM IMSI: 2089300000000003
USIM MSISDN: 00000934
USIM Service Provider Name: uniwan
Succeeded to authenticate with SQN: 224
set HSS SQN value as: 256

```

Εικόνα 71. Επιτυχής Προγραμματισμός της UICC κάρτας

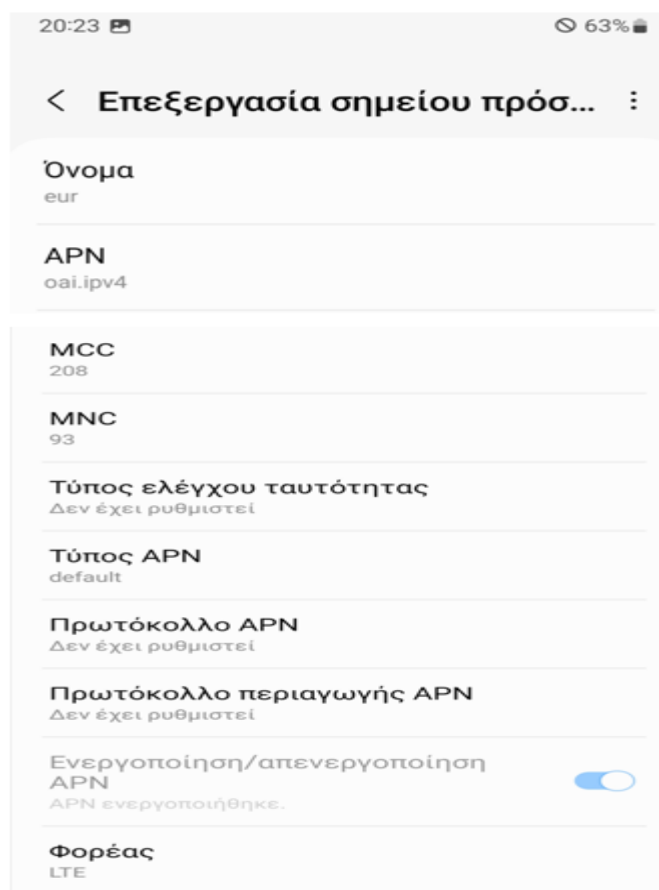
Μετά την επιτυχή ολοκλήρωση προγραμματισμού της κάρτας τα στοιχεία της είναι τα ίδια με αυτά που έχουμε ορίσει στο HSS.

```

Read new values in UICC
ICCID: 89860061100000000934
WARNING: iccid luhn encoding of last digit not done
USIM IMSI: 2089300000000003
USIM MSISDN: 00000934
USIM Service Provider Name: uniwan
Succeeded to authenticate with SQN: 224
set HSS SQN value as: 256

```

Τέλος για να μπορέσουν να συνδεθούν τα UEs στο δίκτυο μας έπρεπε να του ορίσουμε νέο APN profile, όπως έχει δημιουργηθεί στη βάση δεδομένων του HSS.



Εικόνα 72. Παράμετροι του νέου APN profile στο UE

Name	"eur"
APN	"oai.ipv4"
MCC	"208"
MNC	"93"
Bearer	"LTE"

Πίνακας 16. Παράμετροι του νέου APN profile

4.8 Δοκιμές

Οι δοκιμές που κάναμε χωρίζονται σε 3 διαφορετικά μέρη. Κατά την 1^η δοκιμή δεν χρησιμοποιήθηκε καμία κινητή συσκευή, παρά μόνο το eNB (μαζί με το USRP) και το EPC. Στην 2^η δοκιμή χρησιμοποιήθηκαν τα παραπάνω της 1^{ης} δοκιμής μαζί με τα 2 UEs με διαφορά 5 περίπου λεπτών, και στην 3^η δοκιμή χρησιμοποιήθηκαν όλες οι παρελκόμενες συσκευές του δικτύου μαζί με τον Asterisk Server σε πλήρη ανάπτυξη και ελέγχους και περιπτώσεις. Τα αποτελέσματα τους περιγράφονται παρακάτω.

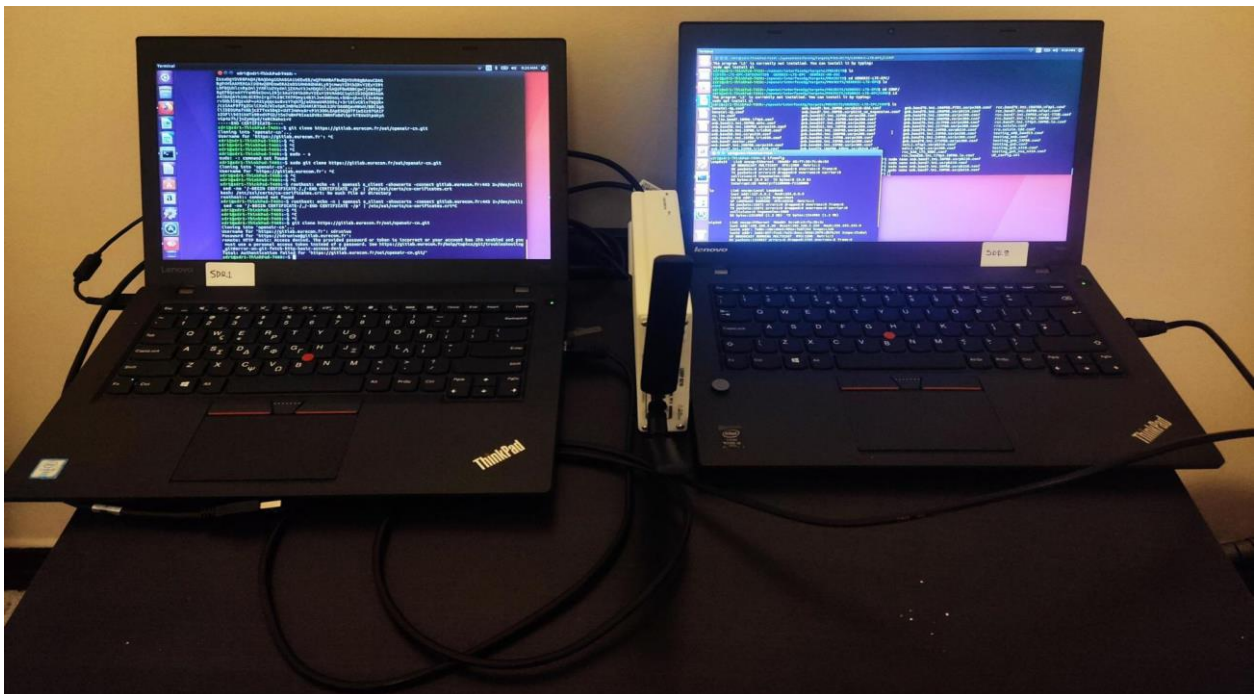
4.8.1 (1^η) Δοκιμή δικτύου, χωρίς UEs

Για την σύνδεση του EPC με το eNB χρησιμοποιήθηκε ένα UTP καλώδιο Cat 6



Εικόνα 73. UTP καλώδιο Cat 6

Στο στάδιο αυτό ξεκινήσαμε την πρώτη δοκιμή λειτουργίας χωρίς να έχουμε συνδέσει κάποιο UE εντός του δικτύου μας. Οι μόνες συσκευές που ήταν συνδεδεμένες ήταν το EPC το eNB μαζί με το USRP.



Εικόνα 74. 1^η δοκιμή δικτύου

Αρχικά ενεργοποιήσαμε από την πλευρά του EPC την βάση HSS, μετά το MME και τέλος το SPGW, και την πλευρά του eNB θέσαμε σε λειτουργία το σταθμό βάσης του SDR. Τα πρώτα αποτελέσματα είναι θετικά, αφού το MME αντλήθηκε αμέσως την σύνδεση του SDR, και μας ενημέρωσε ότι έχει συνδεθεί ένα eNB.

	Current Status	Added since last display	Removed since last display
Connected eNBs	0	0	0
Attached UEs	0	0	0
Connected UEs	0	0	0
Default Bearers	0	0	0
S1-U Bearers	0	0	0

----- STATISTICS -----

Εικόνα 75. 2^η δοκιμή δικτύου χωρίς το eNB ενεργό

```

Leaving slap_mme_decode_initiating() (rc=0)
Entering slap_mme_handle_s1_setup_request()
New s1 setup request incoming from eNB-Eurecom-LTEBox macro eNB id: 00e00
Comparing config tac 1, received tac = 1
Comparing plmn_mcc 208/208, plmn_mnc 93/93 plmn_mnc_len 2/2
Adding eNB to the list of served eNBs
Entering slap_generate_s1_setup_response()
Leaving slap_generate_s1_setup_response() (rc=0)
Leaving slap_mme_handle_s1_setup_request() (rc=0)
[40][8] Sending buffer 0x7fa74c0011e0 of 27 bytes on stream 0 with ppid 18
Successfully sent 27 bytes on stream 0

```

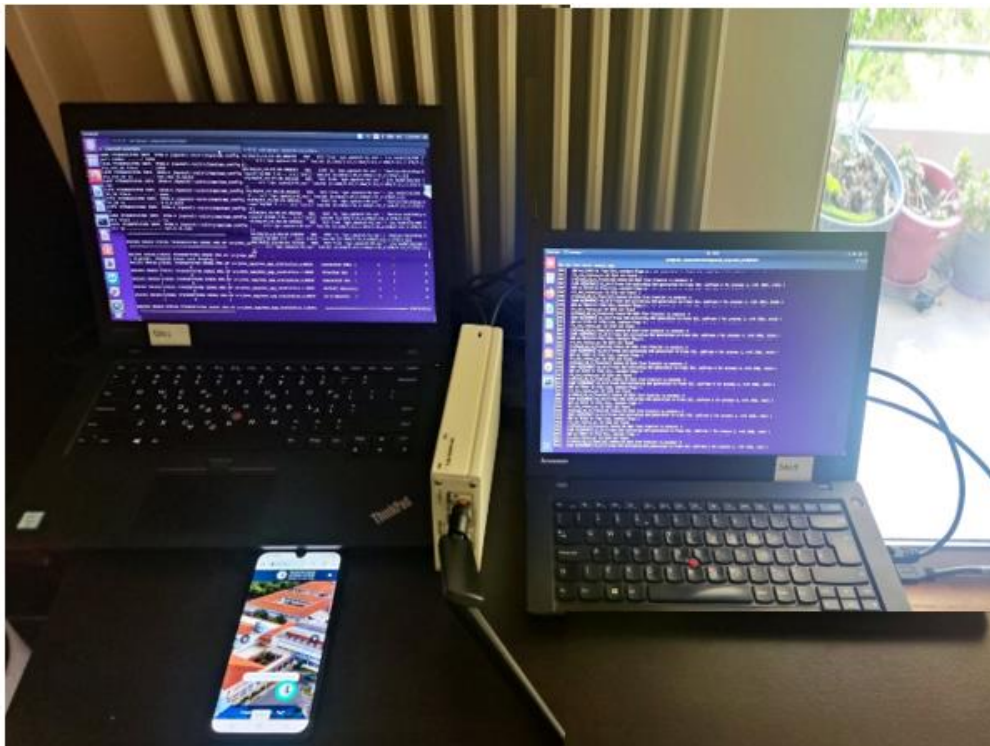
	Current Status	Added since last display	Removed since last display
Connected eNBs	1	1	0
Attached UEs	0	0	0
Connected UEs	0	0	0
Default Bearers	0	0	0
S1-U Bearers	0	0	0

----- STATISTICS -----

Εικόνα 76. 3^η δοκιμή δικτύου με το eNB ενεργό

4.8.2 (2^η) Δοκιμή δικτύου με χρήση 2 UEs

Μετά την αρχική ενεργοποίηση των βημάτων από την 1^η δοκιμή στην συνέχεια ενεργοποιήσαμε το πρώτο κινητό και περιμέναμε να δούμε την αναγνώριση του από το MME. Τα αποτελέσματα ήταν πάλι θετικά αφού το κινητό μπόρεσε να συνδεθεί στο δίκτυο μας, το MME αναγνώρισε τον χρήστη και έγινε η ταυτοποίηση καθώς και επαληθεύτηκε ότι το κινητό μπορεί να συνδεθεί στο LTE δίκτυο. Μετά από περίπου 5 λεπτά ενεργοποιήσαμε και το δεύτερο κινητό, το οποίο και αυτό αναγνωρίστηκε και συνδέθηκε στο δίκτυο μας.



Εικόνα 77. Απεικόνιση συστήματος κατά την 2^η δοκιμή

```

- Cause 16
Purging message 7f2a88000900!
Leaving nwGtpv2cSendTriggeredRspIndToUlp() (rc=0)
Leaving nwGtpv2cProcessUdpReq() (rc=0)
----- STATISTICS -----
      | Current Status| Added since last display| Removed since last dis
Connected eNBs |      1      |      0      |      0
Attached UEs   |      1      |      1      |      0
Connected UEs  |      1      |      1      |      0
Default Bearers|      1      |      1      |      0
SI-U Bearers  |      1      |      1      |      0
----- STATISTICS -----

```

Εικόνα 78. 2^η δοκιμή δικτύου με ένα UE συνδεδεμένο

```

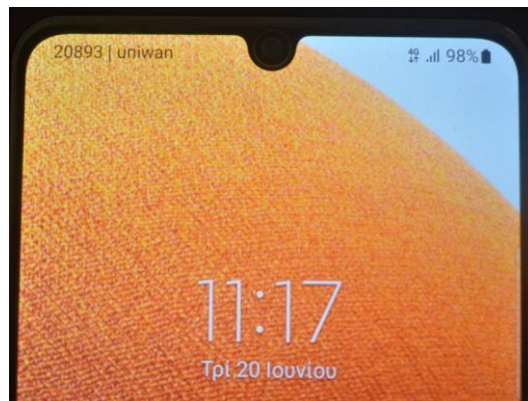
- Cause 16
Purging message 7f2a88000900!
Leaving nwGtpv2cSendTriggeredRspIndToUlp() (rc=0)
Leaving nwGtpv2cProcessUdpReq() (rc=0)
----- STATISTICS -----

```

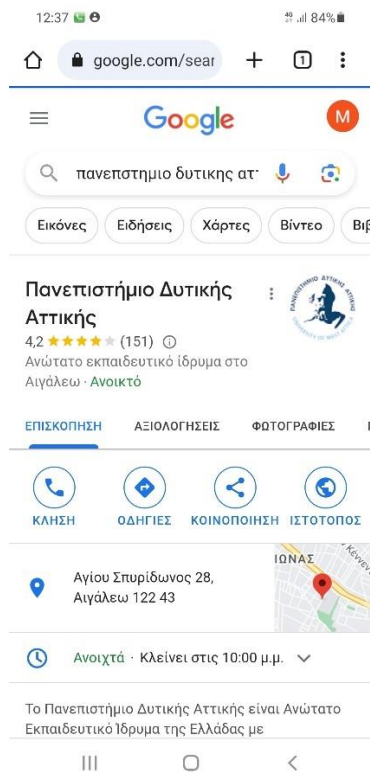
	Current Status	Added since last display	Removed since last
Connected eNBs	1	0	0
Attached UEs	2	1	0
Connected UEs	2	1	0
Default Bearers	2	1	0
S1-U Bearers	2	1	0

Εικόνα 79. 2^η δοκιμή δικτύου με δύο UEs συνδεδεμένα

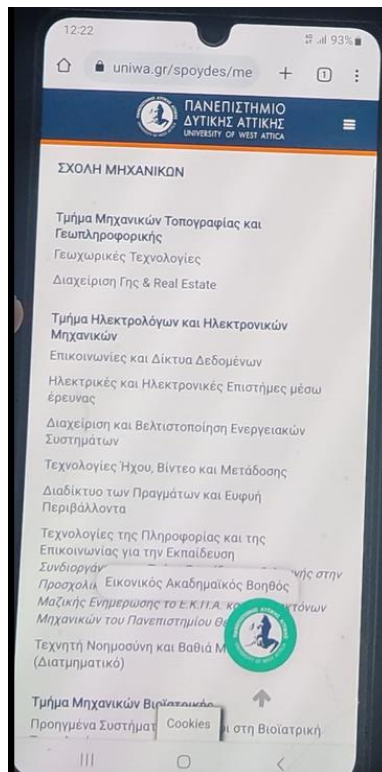
Από την πλευρά του κινητού είδαμε ότι το όνομα του δικτύου έχει εμφανιστεί. Ενώ είχε ήδη ξεκινήσει παροχή υπηρεσίας IP Internet αφού και από τα δύο κινητά μπορούσαμε να κάνουμε αναζήτηση σε διάφορες σελίδες και περιηγηθούμε σε αυτές.



Εικόνα 80. Αναγνώριση εμφάνιση ονόματος ιδιωτικού δικτύου 4G LTE από UE



Εικόνα 81. Αναζήτηση στο Google Search του Πανεπιστημίου Δυτικής Αττικής



Εικόνα 82. Περιήγηση στην ιστοσελίδα του Πανεπιστημίου Δυτικής Αττικής

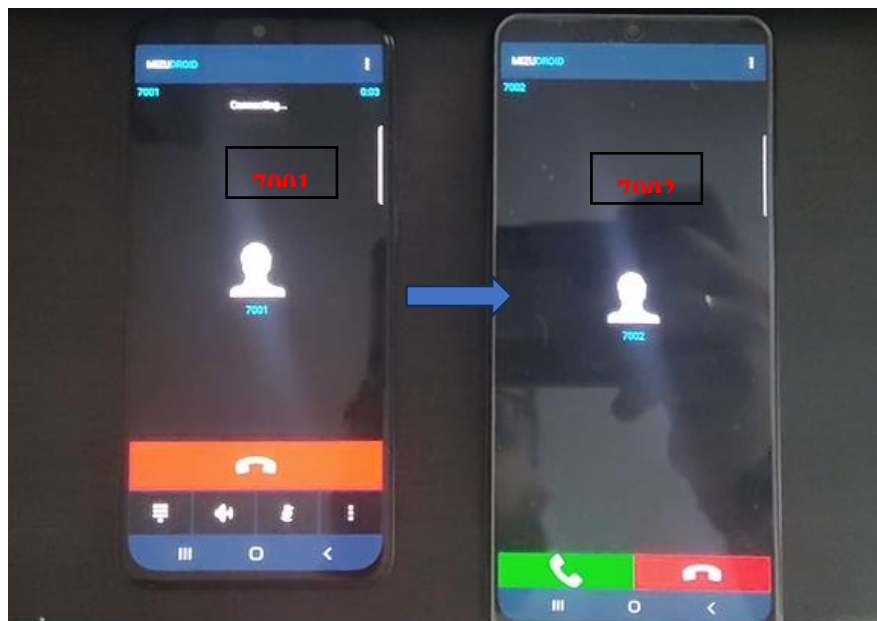
4.8.3 (3^η) Δοκιμή δικτύου με χρήση 2 UEs και κλήση εντός δικτύου.

Κατά την τρίτη δοκιμή και αφού τα UE ήταν συνδεδεμένα στο δίκτυο, ενεργοποιήσαμε την υπηρεσία φωνής στον Asterisk στον Server. Κατά τον έλεγχο μας είδαμε ότι και τα 2 τηλέφωνα έχουν κάνει εγγραφή στο σύστημα της τηλεφωνίας σε διαφορετικές πόρτες, και δοκιμάσαμε να κάνουμε κλήσης από το ένα στο άλλο.

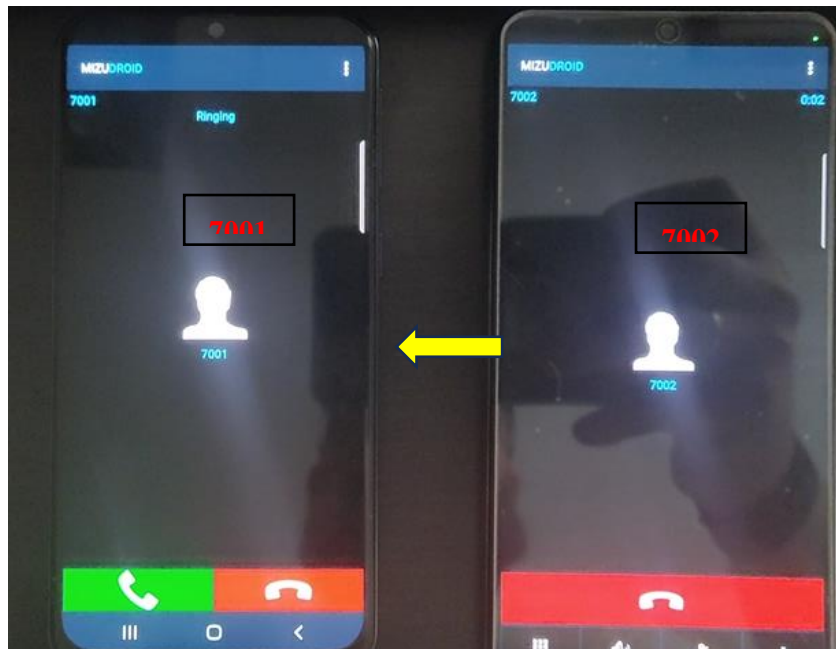
```
Last login: Tue Jun 20 11:07:32 2023 from 192.168.2.18
voip@voip:~$ sudo asterisk -r
[sudo] password for voip:
Asterisk 18.10.0-dfsg+~cs6.10.40431411-2, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 18.10.0-dfsg+~cs6.10.40431411-2 currently running on voip
(pid = 1268)
voip*CLI> sip show peers
Name/username          Host                    Dyn Forcerport
Comedia ACL Port      Status      Description
7001/7001              192.168.2.19          D Yes
Yes                    10210         Unmonitored
7002/7002              192.168.2.19          D Yes
Yes                    17090         Unmonitored
2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 0 offline]
voip*CLI>
```

Εικόνα 83. Υπηρεσία φωνής ενεργοποιημένη μέσω Asterisk

Σε αυτό το στάδιο της 3ης δοκιμής κάναμε αρκετές κλήσεις από τον έναν συνδρομητή στον άλλο. Πιο συγκεκριμένα από τον συνδρομητή 7001 προς τον 7002 και αντίστροφα.



Εικόνα 84. Κλήση από το 7001 προς το 7002



Εικόνα 85. Κλήση από το 7002 προς το 7001

Κάποιες κλήσεις απαντήθηκαν και κάποιες απλά αποκρίθηκαν από τον καλούμενο. Όλες οι κινήσεις των κλήσεων είδαμε ότι καταγραφόντουσαν μέσα από στο software του Asterisk. Πιο συγκεκριμένα, την ώρα που ξεκίνησε η κλήση, ποια ήταν ημερομηνία που πραγματοποιήθηκε, καθώς η κλήση που απορρίφθηκε.

```

3.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses: you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
-----
Connected to Asterisk 18.10.0~dfsg+~cs6.10.40431411-2 currently running on voip
(pid = 1269)
voip*CLI> sip show peers
Name/username      Host                Dyn Forcerport
Comedia   ACL Port    Status      Description
7001/7001                192.168.2.19          D Yes
Yes          10210      Unmonitored
7002/7002                192.168.2.19          D Yes
Yes          17090      Unmonitored
2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 0 offline]
[Jun 20 13:16:04] WARNING[3493][C-00000005]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:04] WARNING[3493][C-00000005]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:04] WARNING[3493][C-00000005]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:04] WARNING[3493][C-00000005]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:15] WARNING[3494][C-00000006]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:15] WARNING[3494][C-00000006]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:15] WARNING[3494][C-00000006]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:15] WARNING[3494][C-00000006]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:15] WARNING[3494][C-00000006]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:16:15] WARNING[3494][C-00000006]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:18:49] NOTICE[1464][C-0000000a]: chan_sip.c:26824 handle_request_invite: Call from '7001' (192.168.2.19:1021
6) to extension '7002*92' rejected because extension not found in context 'internal'.
[Jun 20 13:18:55] WARNING[3514][C-0000000b]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:18:55] WARNING[3514][C-0000000b]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:18:55] WARNING[3514][C-0000000b]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
[Jun 20 13:18:55] WARNING[3514][C-0000000b]: res_rtp_asterisk.c:7722 ast_rtp_read: RTP Read too short
voip*CLI>

```

Εικόνα 86. Κινήσεις κλήσεων εντός δικτύου μέσω Asterisk

ΚΕΦΑΛΑΙΟ 5

Σύνοψη Συμπεράσματα – Προβλήματα και αντιμετώπιση– Εφαρμογές– Προτάσεις εξέλιξης

Σύνοψη Συμπεράσματα

Μέσα από την βιβλιογραφική ανασκόπηση παρουσιάζουμε πως το ΙΟΤ με την βοήθεια των τεχνολογιών της κινητής τηλεφωνίας των ασυρμάτων δικτύων και της κινητής τηλεφωνίας μπορεί να υποστηρίξει τα κρίσιμα δίκτυα υποδομών. Στο πλαίσιο της συγκεκριμένης εργασίας τέθηκε το ερώτημα αν ένα ιδιωτικό δίκτυο τεχνολογίας 4G LTE, είναι ικανό να σχεδιαστεί, να αναπτυχθεί με βάση την τεχνολογία SDR, για ασύρματα δίκτυα αισθητήρων και την προστασία κρίσιμων δικτύων υποδομής. Στην συνέχεια υλοποιήθηκε ένα ιδιωτικό 4G LTE δίκτυο κινητής τηλεφωνίας βασισμένο στην τεχνολογία SDR, όπου μπορεί να καλύψει την ανάγκη υποστήριξης ενός κρίσιμου δικτύου, ενώ ταυτόχρονα μπορεί να υποστηρίξει την δυνατότητα για τηλεφωνικές κλήσεις εντός του δικτύου. Με την ολοκλήρωση των δοκιμών οι συνδεδεμένες στο δίκτυο συσκευές είχαν την δυνατότητα προβολής ιστοσελίδων, βίντεο και κλήσεων μεταξύ τους. Με την ολοκλήρωση της διπλωματικής εργασίας, και την επιτυχή υλοποίηση του σταθμού βάσης ιδιωτικού δικτύου κινητής τηλεφωνίας μπορούμε να καταλήξουμε στα παρακάτω συμπεράσματα. Η υλοποίηση ενός ιδιωτικού δικτύου βασισμένο στην τεχνολογία LTE, και SDR, μπορεί να καλύψει τις ανάγκες ενός κρίσιμου δικτύου, με δυνατότητα κλήσεων πάνω από αυτό (VoLTE). Η χρήση του ανοιχτού ελεύθερου κώδικα και ελεύθερου λογισμικού Linux, ενισχύει μια τέτοια υλοποίηση. Η τεχνολογία του Software Define Radio αποτελεί μια πολύ σημαντική εξέλιξη στις ασύρματες επικοινωνίες, καθώς μέσα από την συνεχόμενη εξέλιξη του ολοένα και περισσότερο κερδίζει έδαφος αφού ένα από τα κύρια πλεονέκτημα του είναι το σχετικά μικρό κόστος αγοράς χωρίς να χρειάζεται καμία παραπάνω προμήθεια εξοπλισμού ή κάποιος άλλος πολύπλοκος εξοπλισμός. Η πλατφόρμα της Open Air Interface OAI, που επιλέχθηκε ως εργαλείο ανοιχτού κώδικα, ανταποκρίθηκε πλήρως στις απαιτήσεις μας για την ανάπτυξη και υλοποίηση αυτής της προσπάθειας.

Προβλήματα και αντιμετώπιση

Το πρώτο λειτουργικό που χρησιμοποιήθηκε και για το EPC αλλά και το eNB ήταν η έκδοση Linux 16.04, κατά την διάρκεια της υλοποίησης. Το πρόβλημα που αντιμετωπίσαμε ήταν πως οι βιβλιοθήκες που χρειάστηκαν κατά την υλοποίηση δεν μπορούσαν να αναβαθμιστούν σε νεότερες και για να ξεπεραστεί το πρόβλημα έπρεπε να γίνουν κάποιες περαιτέρω εγκαταστάσεις παράλληλων βιβλιοθηκών.

Κατά τις πρώτες δοκιμές ελέγχου ο σταθμός βάσης δεν μπορούσε να ανταποκριθεί πλήρως στις απαιτήσεις του δικτύου, ενώ πολλές φορές οποία συσκευή και αν δοκιμάστηκε έχανε την εμβέλεια και επικοινωνία με το σταθμό, με αποτέλεσμα ο σταθμός να κλείνει, να μην μπορεί να συντονιστεί εκ νέου, και σε πολλές περιπτώσεις έπρεπε οι UICC να ε αναπρογραμματιστούν. Επίσης κατά την σύνδεση της 2ης συσκευής στο δίκτυο έπρεπε οι δοκιμές να γίνουν σε πολύ κοντινή απόσταση από το σταθμό (σχεδόν από πάνω του), και υπήρξαν φορές που ο σταθμός δεν μπορούσε να υποστήριξη την ταυτόχρονη σύνδεση

Τα παραπάνω προβλήματα δημιούργησαν αρκετά μεγάλη καθυστέρηση στην υλοποίηση της εργασίας και στην εξέλιξη της. Όμως μετά από αναζήτηση διαπιστώθηκε πως η συγκεκριμένη έκδοση είναι εκτός υποστήριξης και αναβάθμισης λειτουργικού. Για την αντιμετώπιση του προβλήματος αρχικά έγινε μια προσπάθεια αναβάθμισης της υπάρχουσας έκδοσης Linux αλλά δεν τα προβλήματα δεν επιλύθηκαν. Τελικώς έγινε αναβάθμιση του λογισμικού σε νέα έκδοση Ubuntu Linux 18.04.

Εφαρμογές

Η υλοποίηση που παρουσιάζουμε μπορεί να εφαρμοστεί σε:

Πλοία: Σε καταστάσεις κρίσιμων γεγονότων στα πλοία που βρίσκονται εν πλω και μακριά από την ακτή, όπου σε περιπτώσεις εκκένωσης του άνθρωποι πανικοβάλλονται καθώς δεν γνωρίζουν την κατεύθυνση που οδηγεί προς τον επείγοντα σταθμό συγκέντρωσης. Με αυτή την εφαρμογή τα συστήματα ψηφιακής σήμανσης θα καθοδηγούν τους επιβάτες προς τους σταθμούς συγκέντρωσης ακολουθώντας τη λιγότερο επικίνδυνη διαδρομή. Επίσης μπορεί να συνδεθεί ένα ολόκληρο δίκτυο ασυρμάτων αισθητήρων με το ιδιωτικό δίκτυο και να μπορούν οι υπεύθυνοι του πλοίου να παρακολουθούν το σύστημα σε πραγματικό χρόνο.

Υγεία: Σε ασθενείς που βρίσκονται εντός Μονάδων Εντατικής Θεραπείας (ΜΕΘ) ή Μονάδων αυξημένης φροντίδας (ΜΑΦ) στα νοσοκομεία, αφού μπορεί να δημιουργηθεί ένα ασύρματο δίκτυο αισθητήρων με έξυπνες Wearable συσκευές, σε συνεργασία με το ιδιωτικό δίκτυο, να μεταφέρουν σε 24ωρη βάση τα δεδομένα καρδιακού παλμού, οξυγόνου και άλλων ζωτικών στοιχείων σε ένα κεντρικό σύστημα όπου να έχουν άμεση πρόσβαση γιατροί και νοσηλευτικό προσωπικό, ενώ οι ασθενείς και οι συνοδοί θα μπορούν να καλέσουν στο τηλέφωνο για άμεση βοήθεια από το πατήσουν το κουδούνι ανάγκης.

Γεωργία: Σε μεγάλες γεωργικές εκτάσεις όπου το Wi-Fi δεν είναι επαρκές να καλύψει τις μεγάλες αποστάσεις αυτές, μπορεί να υλοποιηθεί ένα ιδιωτικό δίκτυο ασύρματων αισθητήρων με δυνατότητα κλήσεων έτσι ώστε και ο αγρότης θα μπορεί πιο άμεσα και πιο φθηνά να επικοινωνήσει με τους εργαζόμενους στα χωράφια, και να μπορεί να παρακολουθεί σε πραγματικό την κατάσταση των προϊόντων του και να αποφασίζει για το πόση ώρα θα πρέπει να τρέξει το νερό.

Ελαχιστοποίηση κόστους: Εταιρίες και οργανισμοί που θέλουν να έχουν μηδενικό κόστος χρέωσης και να μην εξαρτούνται από παρόχους, μπορούν να υλοποιήσουν αυτή την εφαρμογή.

Μελλοντικές εξελίξεις

Προκειμένου να έχουμε μεγαλύτερη κάλυψη στο χώρο θα πρέπει να τοποθετηθούν κεραίες μεγαλύτερης ισχύος από τις υπάρχουσες, ή να αντικαταστήσουμε τις πολύ - κατευθυντικές με κατευθυντικές. Ακόμα μια περαιτέρω τροποποίηση και εξέλιξη που θα μπορούσε να γίνει στην υπάρχουσα υλοποίηση είναι η ενίσχυση του σταθμού βάσης προσθέτοντας σε αυτόν, ένα ενισχυτή ισχύος, όπου μετά από την σχετική παραμετροποίηση του κώδικα θα επιτευχθεί η μεγαλύτερη εμβέλεια του σταθμού. Επίσης μέσω κατάλληλης παραμετροποίησης και αναβάθμισης του υπάρχοντα ανοιχτού κώδικα του SDR να πραγματοποιούνται και κλήσεις εντός του δικτύου, χωρίς την υποστήριξη κάποιου Software, παρά απευθείας μέσα στο δίκτυο. Τέλος αξίζει να σημειώσουμε ότι η επέκταση της υλοποίησης στο φάσμα του 5GHz, θα είναι μια πολύ καλή, σημαντική και μελλοντική εξέλιξη της υφιστάμενης, η οποία θα δώσει λύσεις για την ενίσχυση την επεκτασιμότητα, και την πραγματικά μεγάλη ταχύτητα των ιδιωτικών δικτύων, με την χρήση την χρήση της πλατφόρμας ανοιχτού κώδικα OAI, αφού επιτρέπει την αξιολόγηση της απόδοσης και σε δίκτυα ανοιχτού κυψελωτού συστήματος 5G.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΠΗΓΕΣ

- [1] T. Alam, «A Reliable Communication Framework and Its Use in Internet of Things (IoT),» en, Αύγ. 2020. DOI: 10.36227/techrxiv.12657158. διεύθυν.: https://www.techrxiv.org/articles/preprint/A_Reliable_Communication_Framework_and_Its_Use_in_Internet_of_Things_IoT_/12657158.
- [2] Ahammad, M. S., & Rahman, A. (2020). A Framework for M-Health Services Using 4G (LTE) Technology. *Int J Innovat Sci Res Technol*, 5, 1085-1095.
- [3] Villar Miguelez, C., Monzon Baeza, V., Parada, R., & Monzo, C. (2023). Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks. *Smart Cities*, 6(2), 728-743.
- [4] Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International journal of computer applications*, 113(1), 1-7.
- [5] Guicheng Shen and Bingwu Liu, "The visions, technologies, applications and security issues of Internet of Things," in *E-Business and E -Government (ICEE)*, 2011, pp. 1-4
- [6] Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology*, 5(1), 41-44.
- [7] Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, 3(05), 164.
- [8] Buttyán, L., Gessner, D., Hessler, A., & Langendoerfer, P. (2010). Application of wireless sensor networks in critical infrastructure protection: challenges and design options [Security and Privacy in Emerging Wireless Networks]. *IEEE Wireless Communications*, 17(5), 44-49.
- [9] Mcginthy, J. M., & Michaels, A. J. (2019). Secure industrial Internet of Things critical infrastructure node design. *IEEE Internet of Things Journal*, 6(5), 8021-8037.
- [10] US Presidential Policy Directive PPD21, Critical Infrastructure Security and Resilience, 2015. Available via: www.dhs.gov/critical-infrastructure-sectors
- [11] [41] Villar Miguelez, C., Monzon Baeza, V., Parada, R., & Monzo, C. (2023). Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks. *Smart Cities*, 6(2), 728-743.

- [12] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, 8, 53-66.
- [13] Alcaraz, C., Lopez, J., Zhou, J., & Roman, R. (2011). Secure SCADA framework for the protection of energy control systems. *Concurrency and Computation: Practice and Experience*, 23(12), 1431-1442.
- [14] Li, M., & Liu, Y. (2007, April). Underground structure monitoring with wireless sensor networks. In *Proceedings of the 6th international conference on Information processing in sensor networks* (pp. 69-78).
- [15] Yu, W., Xu, H., Nguyen, J., Blasch, E., Hematian, A., & Gao, W. (2018). Survey of public safety communications: User-side and network-side solutions and future directions. *Ieee Access*, 6, 70397-70425
- [16] Federrath, H., Jerichow, A., Kesdogan, D., & Pfitzmann, A. (1995). Security in public mobile communication networks.
- [17] Ferrus, R., & Sallent, O. (2014). Extending the LTE/LTE-A business case: Mission-and business-critical mobile broadband communications. *IEEE Vehicular Technology Magazine*, 9(3), 47-55.
- [18] Gawas, A. U. (2015). An overview on evolution of mobile wireless communication networks: 1G-6G. *International Journal on Recent and Innovation Trends in Computing and Communication*, 3(5), 3130-3133.
- [19] De Vriendt, J., Lainé, P., Lerouge, C., & Xu, X. (2002). Mobile network evolution: a revolution on the move. *IEEE Communications magazine*, 40(4), 104-111.
- [20] Rappaport, T. S. (2010). *Wireless communications: Principles and practice*, 2/E. Pearson Education India.
- [21] Mishra, A. R. (2004). *Fundamentals of cellular network planning and optimisation: 2G/2.5 G/3G... evolution to 4G*. John Wiley & Sons.
- [22] Naik, G., Aigal, V., Sehgal, P., & Poojary, J. (2012). Challenges in the implementation of fourth generation wireless systems. *International Journal of Engineering Research and Applications (IJERA)*, 2(2), 1353-1355.

- [23] Ahammad, M. S., & Rahman, A. (2020). A Framework for M-Health Services Using 4G (LTE) Technology. *Int J Innovat Sci Res Technol*, 5, 1085-1095.
- [24] Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer networks*, 52(12), 2292-2330
- [25]FAkyildiz, I. F., & Stuntebeck, E. P. (2006). Wireless underground sensor networks: Research challenges. *Ad Hoc Networks*, 4(6), 669-686.
- [26] Li, M., & Liu, Y. (2007, April). Underground structure monitoring with wireless sensor networks. In *Proceedings of the 6th international conference on Information processing in sensor networks* (pp. 69-78).
- [27] Akyildiz, I. F., Melodia, T., & Chowdhury, K. R. (2007). A survey on wireless multimedia sensor networks. *Computer networks*, 51(4), 921-960
- [28] Akyildiz, I. F., Pompili, D., & Melodia, T. (2004). Challenges for efficient communication in underwater acoustic sensor networks. *ACM Sigbed Review*, 1(2), 3-8.
- [29] Heidemann, J., Li, Y., Syed, A., Wills, J., & Ye, W. (2005). Underwater sensor networking: Research challenges and potential applications. *Proceedings of the Technical Report ISI-TR-2005-603*, USC/Information Sciences Institute.
- [30] Gay, D., Levis, P., Von Behren, R., Welsh, M., Brewer, E., & Culler, D. (2003). The nesC language: A holistic approach to networked embedded systems. *Acm Sigplan Notices*, 38(5), 1-11.
- [31] Tolle, G., Polastre, J., Szewczyk, R., Culler, D., Turner, N., Tu, K., ... & Hong, W. (2005, November). A macroscope in the redwoods. In *Proceedings of the 3rd international conference on Embedded networked sensor systems* (pp. 51-63).
- [32] Vasilescu, I., Kotay, K., Rus, D., Dunbabin, M., & Corke, P. (2005, November). Data collection, storage, and retrieval with an underwater sensor network. In *Proceedings of the 3rd international conference on Embedded networked sensor systems* (pp. 154-165).
- [33] Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., & Welsh, M. (2006). Deploying a wireless sensor network on an active volcano. *IEEE internet computing*, 10(2), 18-25.
- [34] Langendoerfer, P., Buttyán, L., Hessler, A., Casteluccia, C., Casaca, A., Alkassar, A., & Osipov, E. (2012). Wireless sensor networks for critical infrastructure protection. *WIT Transactions on State-of-the-art in Science and Engineering*, 54.

[35] M. Dano. Another East Coast utility starts testing private wireless LTE network, 2021, <https://www.lightreading.com/security/another-east-coast-utility-starts-testing-private-wireless-ltenetwork/d/d-id/770312>

[36] <https://www.idc.com/>

[37] P. Filkins, M. Shirer. A new report from International Data Corporation, 2021. <https://www.businesswire.com/news/home/20210114005786/en/IDC-Forecasts-the-Private-LTE5GInfrastructure-Market-to-Reach-5.7-Billion-in-2024-as-Demandfrom-Mission-Critical-Organizations-Drives-Early-Investment>

[38] Shostko, I., Tevyashev, A., Zemlyaniy, O., & Kulia, Y. (2021, October). Introduction of Private LTE Networks to Provide Specific Communication Tasks in Various Spheres of Society and the State. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 583-586). IEEE.

[39] Levchenko, P., Bankov, D., Khorov, E., & Lyakhov, A. (2022). Performance Comparison of NB-Fi, Sigfox, and LoRaWAN. *Sensors*, 22(24), 9633.

[40] Robert, J., Rauh, S., Lieske, H., & Heuberger, A. (2018, May). IEEE 802.15 low power wide area network (LPWAN) PHY interference model. In 2018 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE

[41] Cheimaras, V., Peladarinos, N., Monios, N., Daousis, S., Papagiakoumos, S., Papageorgas, P., & Piromalis, D. (2023). Emergency Communication System Based on Wireless LPWAN and SD-WAN Technologies: A Hybrid Approach. *Signals*, 4(2), 315-336

[42] Cheimaras, V., Trigkas, A., Papageorgas, P., Piromalis, D., & Sofianopoulos, E. (2022). A Low-Cost Open-Source Architecture for a Digital Signage Emergency Evacuation System for Cruise Ships, Based on IoT and LTE/4G Technologies. *Future Internet*, 14(12), 366.

[43]. Shin, M. K., Nam, K. H., & Kim, H. J. (2012, October). Software-defined networking (SDN): A reference architecture and open APIs. In 2012 International Conference on ICT Convergence (ICTC) (pp. 360-361). IEEE.

[44]. Shalimov, A., Zuikov, D., Zimarina, D., Pashkov, V., & Smeliansky, R. (2013, October). Advanced study of SDN/OpenFlow controllers. In Proceedings of the 9th central & eastern european software engineering conference in russia (pp. 1-6).

[45] Kabir, M. H. (2016). SDN in Cellular Network and Implementation Challenges. *International Journal of Computer Science and Information Security*, 14(2), 200.

- [46] Radcliffe, D., Furey, E., & Blue, J. (2019, December). An SD-WAN solution assuring business quality VoIP communication for home based employees. In 2019 international Conference on smart applications, Communications and networking (SmartNets) (pp. 1-6). IEEE.
- [47] Cichonski, J., Franklin, J., & Bartock, M. (2016). Guide to LTE security (No. NIST Special Publication (SP) 800-187 (Draft)). National Institute of Standards and Technology.
- [48] Cichonski, J., Franklin, J., & Bartock, M. (2016). LTE architecture overview and security analysis (No. NIST Internal or Interagency Report (NISTIR) 8071 (Draft)). National Institute of Standards and Technology.
- [49] Imran, A., Qadeer, M. A., & Khan, M. J. R. (2009, March). Asterisk VoIP private branch exchange. In 2009 International Multimedia, Signal Processing and Communication Technologies (pp. 217-220). IEEE.
- [50] Davidson, J., Peters, J., Peters, J., & Gracely, B. (2000). Voice over IP fundamentals. Cisco press.
Enabling VoIP QoS Monitoring at Intermediate Nodes in an OpenFlow SD
- [51] Stallings, W. (2016). Network security essentials: applications and standards. Pearson.
- [52] Coulibaly, E., & Liu, L. H. (2010, April). Security of Voip networks. In 2010 2nd International Conference on Computer Engineering and Technology (Vol. 3, pp. V3-104). IEEE.
- [53] Khayam, A., et al. (2015). VoIP over LTE: A Measurement Study of VoIP Performance over Commercial LTE Networks. IEEE Transactions on Mobile Computing.
- [54] Anwar, A. A., et al. (2016). Performance Evaluation of VoIP over LTE in Real-Time Testbed Environment. In Proceedings of the 2016 International Conference on Informatics, Electronics & Vision (ICIEV).
- [55] Hasan, S. A., et al. (2019). Private LTE Networks: Overview, Challenges, and Opportunities. IEEE Communications Surveys & Tutorials.
- [56] Fan, C. X., et al. (2020). Performance Analysis of Industrial Automation over Private LTE Networks. IEEE Transactions on Industrial Informatics
- [57] Poikselkä, M., Holma, H., Hongisto, J., Kallio, J., & Toskala, A. (2012). Voice over LTE: VoLTE. John Wiley & Sons.

[58] Rankin, J., Costache, A., Zeto, J., & O'Neil, K. (2014). Validating VoLTE: A Definitive Guide to Successful Deployments.

[59] Alam, M. Z., Bose, S., Rahman, M. M., & Al-Mumin, M. A. (2007, February). Small office PBX using Voice over internet protocol (VOIP). In The 9th International Conference on Advanced Communication Technology (Vol. 3, pp. 1618-1622). IEEE.

[60] Imran, A., Qadeer, M. A., & Khan, M. J. R. (2009, March). Asterisk VoIP private branch exchange. In 2009 International Multimedia, Signal Processing and Communication Technologies (pp. 217-220). IEEE.

[61] Von Hippel, E. (2001). Learning from open-source software. MIT Sloan management review, 42(4), 82-86.

[62] Perens, B. (1999). The open-source definition. Open sources: voices from the open-source revolution, 1, 171-188.

[63] Wasif, M., Elahi, M., & Sanghavi, C. (2007, September). Analysis and implementation of adaptive modem for SDR. In 2007 International Conference on Wireless Communications, Networking and Mobile Computing (pp. 1248-1251). IEEE.

[64] Kumar, A., Kaushik, S. K., Sharma, R., & Raj, P. (2012, September). Simulators for wireless networks: A comparative study. In 2012 International Conference on Computing Sciences (pp. 338-342). IEEE.

[65] Nardini, G., Sabella, D., Stea, G., Thakkar, P., & Viridis, A. (2020). Simu5G—An OMNeT++ library for end-to-end performance evaluation of 5G networks. IEEE Access, 8, 181176-181191.

[66] Li, Y., Yu, F., Zheng, S. L., & Yang, C. L. (2011, August). LTE system level simulation with MATLAB. In 2011 International Conference on Internet Technology and Applications (pp. 1-4). IEEE.

[67] <https://openairinterface.org>

[68] Ettus, M., & Braun, M. (2015). The Universal Software Radio Peripheral (USRP) Family of Low-Cost SDRs. Opportunistic spectrum sharing and white space access: The practical reality, 3-23.

[69] Amézaga, A., López-Martínez, C., & Jové, R. (2021). A Multi-Frequency SDR-Based GBSAR: System Overview and First Results. Remote Sensing, 13(9), 1613.

[70] Tuka, E. A. (2020). Software Defined Radios and NI USRP.

[71] <https://www.ettus.com/all-products/usrp-b200-enclosure/>

[73] Ettus, M., & Braun, M. (2015). The Universal Software Radio Peripheral (USRP) Family of Low-Cost SDRs. Opportunistic spectrum sharing and white space access: The practical reality, 3-23.

[72] <https://ubuntu.com/blog/industrial-embedded-systems>

[73] <https://www.everythingrf.com/tech-resources/lte-bands/lte-band-7>

[74] <https://tukaani.org/xz/>

[75] Collins, J. (2022). GPRS Tunneling Protocol (GTP). In Encyclopedia of Cryptography, Security and Privacy (pp. 1-3). Berlin, Heidelberg: Springer Berlin Heidelberg.

[76] Stapp, M., Volz, B., & Rekhter, Y. (2006). The dynamic host configuration protocol (DHCP) client fully qualified domain name (FQDN) option (No. rfc4702).

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα Α: Κώδικας eNB

```
$sudo apt-get install cpufrequtils
$nano /etc/default/cpufrequtils
GOVERNOR="performance"
$sudo update-rc.d ondemand disable
$cpufreq-info
$swatch grep "cpu MHz" /proc/cpuinfo
$nano/etc/default/grub
GRUB_CMDLINE_LINUX_DEFAULT="quiet intel_pstate=disable processor.max_cstate=1 intel_idle.max_cstate=0
idle=poll"
$sudo update-grub
$nano /etc/modprobe.d/blacklist.conf
blacklist intel_powerclamp
$sudo apt-get install i7z
$sudo i7z
$sudo dpkg -i kernel.ubuntu.com/*/*/*deb
$reboot
$uname -a
$sudo i7z
$version=4.4
$wget -r -e robots=off --accept-regex "(.*lowlatency.*amd64)|(all).deb" http://kernel.ubuntu.com/~kernel-
ppa/mainline/v${version}-wily/
$sudo dpkg -i kernel.ubuntu.com/*/*/*deb
$reboot
$uname -a
$uname -a
$sudo apt-get update
$sudo apt-get install git
```

```
$sudo apt-get install subversion git
$sudo su
echo -n | openssl s_client -showcerts -connect gitlab.eurecom.fr:443 2>/dev/null | sed -ne '/-BEGIN CERTIFICATE-
/,/-END CERTIFICATE-/p' | sudo tee -a /etc/ssl/certs/ca-certificates.crt
$sudo git clone https://gitlab.eurecom.fr/oai/openairinterface5g.git
$cd /openairinterface5g
$source oaienv
$cd cmake_targets
$Sudo ./build_oai -l --eNB -x --install-systemfiles-w USRP
~/openairinterface5g/targets/PROJECTS/GENERIC-LTE-EPC/CONF/
$sudo nano enb.band7.tm1.usrb210.conf
$sudo nano /etc/default/grub
GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0"
$sudo grub-mkconfig -o /boot/grub/grub.cfg
```

Παράρτημα Β: Κώδικας ΕΡC

```
$sudo apt-get install xz-utils build-essential wget libncurses5-dev libssl-dev
$sudo apt-get build-dep linux-image-$(uname -r) ncurses-bin wget https://cdn.kernel.org/pub/linux/kernel/v4.x/linux-4.7.1.tar.xz
$unxz linux-4.7.1.tar.xz
$tar -xovf linux-4.7.1.tar
$cd linux-4.7.1
$make menuconfig
$sudo apt-get install libelf-dev
$$sudo apt-get upgrade
$make -j `nproc`
$sudo make modules_install
$sudo make install
$$sudo apt-get upgrade
$sudo apt-get install git
$sudo su
$roothost: echo -n | openssl s_client -showcerts -connect gitlab.eurecom.fr:443 2>/dev/null | sed -ne '/BEGIN CERTIFICATE-/,/END CERTIFICATE-/p' | sudo tee -a /etc/ssl/certs/ca-certificates.crt
//go to: https://open-cells.com/d5138782a8739209ec5760865b1e53b0/openair-cn.tgz and download Openair-cn.tgz (local)
tar xf openair-cn.tgz
cd openair-cn
git checkout develop
$ sudo nano /etc/hostname
$ cat /etc/hostname
epc (renamed)
$sudo nano /etc/hosts
```

```
127.0.0.1 localhost
127.0.1.1 epc.openair4G.eur epc
127.0.1.1 hss.openair4G.eur hss
$cd openair-cn/scripts
$ ./build_spgw -i
$ ./build_spgw
$cd openair-cn/scripts
$ ./build_mme -i
$ ./build_mme
$cd openair-cn/scripts
$ ./build_hss -i
$ ./build_hss
$ sudo apt-get install phpMyAdmin
$ sudo ln -s /etc/phpmyadmin/apache.conf /etc/apache2/conf-available/phpmyadmin.conf
$ sudo /etc/init.d/apache2 reload
sudo mkdir -p /usr/local/etc/oai/freeDiameter
sudo cp ~/openair-cn/etc/mme.conf /usr/local/etc/oai
```

```

sudo cp ~/openair-cn/etc/hss.conf /usr/local/etc/oai
sudo cp ~/openair-cn/etc/spgw.conf /usr/local/etc/oai
sudo cp ~/openair-cn/etc/acl.conf /usr/local/etc/oai/freeDiameter
sudo cp ~/openair-cn/etc/mme_fd.conf /usr/local/etc/oai/freeDiameter
sudo cp ~/openair-cn/etc/hss_fd.conf /usr/local/etc/oai/freeDiameter
$sudo nano /usr/local/etc/oai/mme.conf
$sudo nano /usr/local/etc/oai/hss.conf
$sudo nano /usr/local/etc/oai/spgw.conf
$sudo nano /usr/local/etc/oai/freeDiameter/acl.conf
$sudo nano /usr/local/etc/oai/freeDiameter/mme_fd.conf
$sudo nano /usr/local/etc/oai/freeDiameter/hss_fd.conf
$cd ~/openair-cn/scripts
./check_hss_s6a_certificate /usr/local/etc/oai/freeDiameter/ hss.openair4G.eur
./check_mme_s6a_certificate /usr/local/etc/oai/freeDiameter/ epc.openair4G.eur
$./build_hss -c
./run_hss -i ~/openair-cn/src/oai_hss/db/oai_db.sql
./run_hss
$cd ~/openair-cn/scripts //run to deferent terminal
$./build_mme -c
$./run_mme
$cd ~/openair-cn/scripts // run to deferent terminal
$./build_spgw -c
$./run_spgw
$cd ~/openairinterface5g
$source oaienv
$ sudo ./cmake_targets/build_oai -w USRP -x -c -eNB
~/openairinterface5g/cmake_targets/ran_build/build
$sudo -E./lte-softmodem -O ~/openairinterface5g/targets/PROJECTS/GENERIC-LTE
EPC/CONF/enb.band7.tm1.50PRB.usrb210.conf -d

```

Παράρτημα Γ: Κώδικας Asterisk

```

$sudo apt-get update -y
$sudo apt-get install asterisk -y
$sudo mv extensions.conf extensions.conf.backup
$sudo mv voicemail.conf voicemail.conf.bakcup

```

```
$sudo nano sip.conf
[general]
context=internal
allowguest=no
allowoverlap=no
bindport=5060
bindaddr=0.0.0.0
srvlookup=no
disallow=all
allow=ulaw
alwaysauthreject=yes
canreinvite=no
nat=yes
session-timers=refuse
localnet=192.168.0.0/255.255.255.0
[7001]
type=friend
host=dynamic
secret=7001
context=internal
[7002]
type=friend
host=dynamic
```

```

secret=7002
context=internal

$sudo nano extensions.conf
[internal]
exten => 7001,1,Answer()
exten => 7001,2,Dial(SIP/7001,60)
exten => 7001,3,Playback(vm-nobodyavail)
exten => 7001,4,VoiceMail(7001@main)
exten => 7001,5,Hangup()
exten => 7002,1,Answer()
exten => 7002,2,Dial(SIP/7002,60)
exten => 7002,3,Playback(vm-nobodyavail)
exten => 7002,4,VoiceMail(7001@main)
exten => 7002,5,Hangup()
exten => 8001,1,VoicemailMain(7001@main)
exten => 8001,2,Hangup()
exten => 8002,1,VoicemailMain(7002@main)
exten => 8002,2,Hangup()
$sudo nano voicemail.conf
[main]
7001 => 7001
7002 => 7002

$sudo asterisk -r
sip show peers

```

Παράρτημα Δ: Κώδικας UICC SIM Cards

```

go to: https://open-cells.com/d5138782a8739209ec5760865b1e53b0/uicc-v3.2.tgz and download iccc v3.2.tgz (local and extract)
cd ~/Downloads/uicc-v3.2
$make
$sudo apt install make
$sudo ./program_uicc --adm 85235200 --imsi 2089300000000003 --opc 8e27b6af0e692e750f32667a3b14605d --key 8baf473f2f8fd09487cccbd7097c6862 --spn uniwan --authenticate

```


Παράρτημα Ε: Εικόνες

[F1] https://www.researchgate.net/figure/loT-growth-chart-by-years_fig2_332392350

[F2] <https://pixabay.com/illustrations/payment-systems-1169825/>

[F3] <https://hackr.io/blog/top-10-iot-applications>

[F4] Sehrawat, D., & Gill, N. S. (2018). Deployment of IoT based smart environment: key issues and challenges. *International Journal of Engineering & Technology*, 7(2), 544-550.

[F5] <https://www.envirotech-online.com/news/environmental-laboratory/7/breaking-news/how-does-smart-home-automation-affect-the-environment/45838>

[F6] https://www.freepik.com/free-vector/mobile-medicine-isometric-flowchart-with-online-laboratory-symbols-illustration_7252449.htm#query=smart%20hospital&position=5&from_view=keyword&track=ais

[F7] https://www.freepik.com/premium-photo/woman-using-innovative-smart-tech-greenhouse-plant-management_33572524.htm#query=smart%20GRICULTURE&position=25&from_view=search&track=ais

[F8] <https://www.scnsoft.com/blog/connected-supply-chain-top-questions-answered>

[F9] Ian, M., Elena, V., & Michael, J. (2019, November). Artificial Intelligence in the Aviation Manufacturing Process for Complex Assemblies and Components. In *IOP Conference Series: Materials Science and Engineering* (Vol. 689, No. 1, p. 012022). IOP Publishing.

[F10] Picazo Martínez, P. (2021). *Despliegue de redes 5G Non-Standaone basadas en OpenAirInterface* (Doctoral dissertation, Universitat Politècnica de València).

[F11] Bencini, L., Di Palma, D., Collodi, G., Manes, G., Manes, A., & Tan, Y. K. (2010). Wireless sensor networks for on-field agricultural management process. *Wireless Sensor Networks: application-centric design*, 1-17.

[F12] Jäger, T., Mokos, A., Prasianakis, N. I., & Leyer, S. (2022). first_page settings Order Article Reprints Open AccessArticle Pore-Level Multiphase Simulations of Realistic Distillation Membranes for Water Desalination. *Membranes*.

[F13] Sadeghioon, A. M., Chapman, D. N., Metje, N., & Anthony, C. J. (2017). A new approach to estimating the path loss in underground wireless sensor networks. *Journal of Sensor and Actuator Networks*, 6(3), 18.

[F14] Song, G., Zhou, Y., Ding, F., & Song, A. (2008). A mobile sensor network system for monitoring of unfriendly environments. *Sensors*, 8(11), 7259-7274.

[F15] <https://www.elprocus.com/introduction-to-wireless-sensor-networks-types-and-applications/>

[F16] Moon, B. (2017). Dynamic spectrum access for internet of things service in cognitive radio-enabled LPWANs. *Sensors*, 17(12), 2818.

[F17] Chahlaoui, F., Dahmouni, H., & El Alami, H. (2022, March). Multipath-routing based load-balancing in SDN networks. In 2022 5th Conference on Cloud and Internet of Things (CIoT) (pp. 180-185). IEEE.

[F18] <https://www.computertechreviews.com/definition/software-defined-wan-sd-wan/>

[F19] Butcher, D., Li, X., & Guo, J. (2007). Security challenge and defense in VoIP infrastructures. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 37(6), 1152-1162.

[F20] Thorpe, C., Hava, A., Langlois, J., Dumas, A., & Olariu, C. (2016, April). imos: Enabling voip qos monitoring at intermediate nodes in an openflow sdn. In 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW) (pp. 76-81). IEEE.

[F21] <https://www.3gltinfo.com/ims-volte-architecture/>

[F22] Nikaein, N., Knopp, R., Kaltenberger, F., Gauthier, L., Bonnet, C., Nussbaum, D., & Ghaddab, R. (2014, September). OpenAirInterface: an open LTE network in a PC. In Proceedings of the 20th annual international conference on Mobile computing and networking (pp. 305-308).

[F23] <https://releases.ubuntu.com/18.04/>

[F24] <https://ubuntu.com/tutorials/install-ubuntu-desktop-1804#3-boot-from-dvd>

[F25] <https://ubuntu.com/blog/industrial-embedded-systems>

[F26] <https://gitlab.eurecom.fr/oai/openairinterface5g>

[F27] <https://www.everythingrf.com/tech-resources/lte-bands/lte-band-7>

[F28] <https://releases.ubuntu.com/16.04/>

[F29] <https://ubuntu.com/tutorials/install-ubuntu-desktop-1604#3-boot-from-dvd>

[F30] <https://open-cells.com/index.php/2019/09/22/all-in-one-openairinterface/>

[F31] <https://ubuntu.com/download/desktop>

[F32] <https://ostechnix.com/install-ubuntu-desktop/>

[F33] <https://open-cells.com/index.php/uiccsim-programing/>