



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Πτυχιακή Εργασία

ΑΣΦΑΛΕΙΑ ΣΕ 5G ΔΙΚΤΥΑ

Καπλάνης Κωνσταντίνος

Επιβλέπουσα καθηγήτρια:

Χριστίνα Πολίτη

Πάτρα, Σεπτέμβριος 2024

Βεβαίωση εκπόνησης Πτυχιακής εργασίας - Υπεύθυνη Δήλωση Φοιτητή

Βεβαιώνω υπεύθυνα ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχω αναφέρει ή παραπέμψει με ρητό τρόπο όλες τις πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, προτάσεων ή λέξεων, είτε αυτές αναφέρονται αυτούσια είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για το συγκεκριμένο πρόγραμμα σπουδών.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος. Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή Καπλάνη Κωνσταντίνου που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο Πανεπιστήμιο Πελοποννήσου, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.

Εγκρίθηκε από την τριμελή Εξεταστική Επιτροπή Αξιολόγησης:

1. Ονοματεπώνυμο, Υπογραφή

2. Ονοματεπώνυμο, Υπογραφή

3. Ονοματεπώνυμο, Υπογραφή

.....

.....

.....

Πάτρα, Σεπτέμβριος 2024

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή είναι οργανωμένη σε πέντε κύρια κεφάλαια, το καθένα από τα οποία καλύπτει διαφορετικές πτυχές του θέματος. Πιο αναλυτικά:

Το **πρώτο κεφάλαιο** εισάγει τα βασικά στοιχεία των ασύρματων δικτύων, ξεκινώντας με τον ορισμό τους και την ιστορική αναδρομή της εξέλιξής τους. Εξετάζει τη χρησιμότητα των δικτύων 5G, παρουσιάζοντας τα οφέλη τους σε σχέση με τις προηγούμενες γενιές δικτύων.

Στο **δεύτερο κεφάλαιο** αναλύεται η έννοια του τεμαχισμού δικτύου, τα πλεονεκτήματα και τα μειονεκτήματά του, καθώς και η ιστορική του εξέλιξη. Παρουσιάζονται οι εφαρμογές του τεμαχισμού δικτύου σε διάφορους τομείς, η αρχιτεκτονική και οι βασικές έννοιες που τον διέπουν, καθώς και τα επίπεδα τεμαχισμού. Επίσης, εξετάζονται η αρχιτεκτονική της δικτύωσης καθοριζόμενη από λογισμικό και της εικονοποίησης των διαδικτυακών λειτουργιών.

Το **τρίτο κεφάλαιο** επικεντρώνεται στην ασφάλεια των δικτύων 5G περιγράφοντας τις απειλές και τις προκλήσεις που αυτά αντιμετωπίζουν. Αναλύονται οι μηχανισμοί ασφάλειας των SIM καρτών, τα είδη των επιθέσεων και των παραβιάσεων, καθώς και οι βασικές προκλήσεις ασφαλείας. Οι προκλήσεις αυτές εξετάζονται στα κινητά σύννεφα, στις αρχιτεκτονικές δικτύωσης που εξετάστηκαν στο προηγούμενο κεφάλαιο, στα κανάλια επικοινωνίας, καθώς και σε εκείνες που εστιάζουν στο απόρρητο. Παρουσιάζονται οι αρχές ασφαλείας για τον τεμαχισμό δικτύου, τη διαχείριση ταυτότητας και πρόσβασης, η ασφάλεια από άκρο σε άκρο και τέλος οι κανονισμοί και η νομοθεσία για την ασφάλεια στο 5G.

Το **τέταρτο κεφάλαιο** εξετάζει τις απειλές που αντιμετωπίζουν οι υπηρεσίες 5G όσον αφορά στην εικονοποίηση του δικτύου, στον υπολογισμό στο άκρο του δικτύου, στις λειτουργίες του, στη βελτιωμένη κινητή ευρυζωνικότητα, στο μαζικό διαδίκτυο των πραγμάτων, στις κρίσιμες επικοινωνίες. Αναλύονται τα επίπεδα ασφαλείας στο 5G και η ασφάλεια συσκευών IoT.

Το **πέμπτο κεφάλαιο** ασχολείται με τις λύσεις και τις στρατηγικές προστασίας στην ασφάλεια των 5G δικτύων. Παρουσιάζονται οι μέθοδοι προστασίας στον τεμαχισμό δικτύου, στον υπολογισμό στο άκρο του δικτύου και οι γενικές λύσεις ασφαλείας. Εξετάζονται οι λύσεις ασφαλείας και στα κινητά σύννεφα καθώς και οι προηγμένες τεχνολογίες ασφαλείας που κάνουν χρήση της τεχνητής νοημοσύνης και της μηχανικής μάθησης.

Το τελευταίο μέρος της εργασίας (**συμπεράσματα**) συνοψίζει τα κύρια ευρήματα και προσφέρει τελικές παρατηρήσεις και προτάσεις για την περαιτέρω έρευνα στον τομέα της ασφάλειας των 5G δικτύων και στον τεμαχισμό του δικτύου.

Λέξεις κλειδιά: Ασφάλεια 5G, Τεμαχισμός δικτύου, Απειλές 5G, Προκλήσεις ασφαλείας, Εικονικοποίηση δικτύου, Υπολογισμός στο άκρο του δικτύου, Κινητά σύννεφα, Ασφάλεια ΙοΤ, Δίκτυα Οριζόμενα από Λογισμικό, Εικονικοποίηση Δικτυακών Λειτουργιών, Διαχείριση ταυτότητας και πρόσβασης, Ασφάλεια από άκρο σε άκρο, Κανονισμοί και νομοθεσία για την ασφάλεια 5G

ABSTRACT

The thesis is organized into five main chapters, each covering different aspects of the topic. In more detail:

The **first chapter** introduces the basic elements of wireless networks, starting with their definition and a historical overview of their evolution. It examines the usefulness of 5G networks, highlighting their benefits compared to previous generations of networks.

In the **second chapter** the concept of network slicing is analysed, along with its advantages and disadvantages and its historical development. The applications of network slicing in various sectors are presented, along with the architecture and basic concepts governing it and the levels of slicing. Additionally, the architectures of Software Defined Networks and Network Function Virtualization are examined.

The **third chapter** focuses on the security of 5G networks, describing the threats and challenges they face. It analyses the security mechanisms of SIM cards, the types of attacks and breaches and key security challenges. Security challenges in mobile clouds, Software Defined Network and Network Function Virtualization, communication channels and privacy issues are examined. The principles of network slicing security, identity and access management, end-to-end security and regulations and legislation for 5G security are also presented.

The **fourth chapter** examines the threats faced by 5G services, including network virtualization, edge computing, network functions, enhanced mobile broadband, massive Internet of Things, critical communications, 5G security levels, and IoT device security.

The **fifth chapter** deals with solutions and protection strategies for 5G network security. It presents methods for network slicing protection, edge computing protection and general security solutions. Security solutions for mobile clouds and advanced security technologies based on Artificial Intelligence and Machine Learning are examined.

The final part of the thesis (**conclusions**) summarizes the main findings and offers final observations and suggestions for further research in the field of 5G network security and network slicing.

Key words: 5G Security, Network Slicing, 5G Threats, Security Challenges, Network Virtualization, Edge Computing, Mobile Clouds, IoT Security, Software Defined Networks, Network Function Virtualization, Identity and Access Management, End-to-End Security, 5G Security Regulations and Legislation

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ.....	1
ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ.....	3
1.1 Ορισμός των ασύρματων δικτύων	3
1.2 Ιστορική αναδρομή των ασύρματων δικτύων.....	3
1.3 Χαρακτηριστικά γνωρίσματα του 5G.....	5
1.4 Γενική κατηγοριοποίηση των 5G υπηρεσιών	8
ΚΕΦΑΛΑΙΟ 2: 5G ΚΑΙ ΤΕΜΑΧΙΣΜΟΣ ΔΙΚΤΥΟΥ	11
2.1 Βασικές έννοιες.....	11
2.2 Πλεονεκτήματα και μειονεκτήματα του τεμαχισμού του δικτύου	12
2.3 Ιστορία του τεμαχισμού δικτύου	13
2.4 Εφαρμογές του τεμαχισμού δικτύου.....	14
2.5 Επισκόπηση αρχιτεκτονικής και βασικές έννοιες	17
2.6 Επίπεδα του τεμαχισμού δικτύου	19
2.7 Κύρια στοιχεία της αρχιτεκτονικής του 5G.....	21
2.8 Αρχιτεκτονική των δικτύων οριζόμενων από λογισμικό.....	24
2.9 Αρχιτεκτονική της εικονικοποίησης των δικτυακών λειτουργιών	24
ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ, ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ ΣΤΑ 5G ΔΙΚΤΥΑ	27
3.1 Η ανάγκη για ασφάλεια στα δίκτυα 5G: Προκλήσεις και προοπτικές στην ψηφιακή εποχή.....	27
3.2 Μηχανισμός ασφάλειας των SIM καρτών.....	28
3.3 Κατηγορίες και είδη επιθέσεων	29
3.3.1 Επιθέσεις προς τον χρήστη	30
3.3.2 Επιθέσεις προς το δίκτυο	31

3.4 Βασικές προκλήσεις ασφαλείας στο 5G	35
3.5 Προκλήσεις ασφαλείας στα κινητά σύννεφα.....	38
3.6 Προκλήσεις ασφαλείας στα SDN και NFV	40
3.7 Προκλήσεις ασφαλείας στα κανάλια επικοινωνίας	40
3.8 Προκλήσεις απορρήτου στο 5G.....	42
3.9 Αρχές ασφαλείας για τον τεμαχισμό δικτύου	46
3.10 Διαχείριση ταυτότητας και πρόσβασης	48
3.11 Ασφάλεια από άκρο σε άκρο	49
3.12 Κανονισμοί και νομοθεσία για την ασφάλεια στα 5G δίκτυα	49
ΚΕΦΑΛΑΙΟ 4 : ΑΠΕΙΛΕΣ ΣΤΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ 5G	51
4.1 Εικονικοποίηση δικτύου	51
4.2 Ακροδικτυακή υπολογιστική ή υπολογιστική των παρυφών	51
4.3 Λειτουργίες δικτύου.....	54
4.4 Βελτιωμένη κινητή ευρυζωνικότητα	56
4.5 Μαζικό διαδίκτυο των πραγμάτων	58
4.6 Κρίσιμες επικοινωνίες	59
4.7 Πτυχές ασφαλείας που δεν καλύπτονται από το 5G.....	60
4.8 Ασφάλεια συσκευών IoT	62
ΚΕΦΑΛΑΙΟ 5 : ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΛΥΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ	63
5.1 Προστασία στον τεμαχισμό δικτύου.....	63
5.2 Προστασία του υπολογισμού στο άκρο του δικτύου.....	64
5.3 Λύσεις ασφάλειας στις φορητές συσκευές	65
5.4 Προηγμένες τεχνολογίες ασφάλειας.....	67
5.5 Γενικές λύσεις ασφάλειας.....	69
Συμπεράσματα.....	70

Βιβλιογραφία	72
Ξένη	72
Ελληνική	75
Ιστοσελίδες	75

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

Εικόνα 1: Γενιές Δικτύων τηλεπικοινωνιών.....	5
Εικόνα 2: Βασικά χαρακτηριστικά γνωρίσματα των 1G, 2G, 3G, 4G και 5G δικτύων.....	8
Εικόνα 3: Σύνοψη των υπηρεσιών ανά κατηγορία στο 5G δίκτυο	9
Εικόνα 4: Σπουδαιότητα απαιτήσεων των υπηρεσιών 5G ανά κατηγορία υπηρεσίας.....	10
Εικόνα 5: Τμήματα δικτύου 5G που εκτελούνται σε ένα κοινό υποκείμενο δίκτυο πολλαπλών προμηθευτών και πολλαπλών προσβάσεων. Κάθε κομμάτι διαχειρίζεται ανεξάρτητα και αντιμετωπίζει μια συγκεκριμένη περίπτωση χρήσης.	11
Εικόνα 6: Ποιότητα υπηρεσίας 5G και επιχειρηματικές απαιτήσεις	18
Εικόνα 7: Γενικό πλαίσιο που αντιπροσωπεύει τις 5G αρχιτεκτονικές προτάσεις (επίπεδα τεμαχισμού δικτύου).....	19
Εικόνα 8: Οι αρχιτεκτονικές SDN και NFV στα 5G δίκτυα	26
Εικόνα 9: Διαφορές μεταξύ των SDN και NFV	26
Εικόνα 10: Οι επιθέσεις στο 5G δίκτυο.....	30
Εικόνα 11: Το τοπίο απειλών στο 5G δίκτυο	36
Εικόνα 12: Συμφόρηση του IOT στο 5G και επίλυση με τη χρήση του edge computing.....	53
Εικόνα 13: Χρήση των AI και ML τεχνολογιών για την ανακάλυψη ανωμαλιών που μπορεί να υποδεικνύουν κακόβουλες δραστηριότητες σε μια πληθώρα επιθέσεων.....	68

ΣΥΝΤΟΜΕΥΣΕΙΣ & ΑΚΡΩΝΥΜΙΑ

EETT: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

1G: First Generation

2G-2.5G: Second Generation

3G: Third Generation

3GPP: 3rd Generation Partnership Project

4G: Fourth Generation

4G LTE: 4G Long Term Evolution

5G: Fifth Generation

AI: Artificial Intelligence

API: Application Programming Interface

AR: Augmented Reality

ARP: Address Resolution Protocol

BSS: Business Support Systems

CDMA: Code Division Multiple Access

CDMA2000 ή C2K: Code Division Multiple Access 2000

CPS: Cyber-Physical System

C-RAN: Cloud Radio Access Network

CriC: Critical Communications

DDoS: Distributed Denial-of-Service

DoS: Denial-of-Service

DRM: Demand Response Management

eMBB: enhanced Mobile BroadBand

ENISA: European Union Agency for Cybersecurity

eUICC: embedded Universal Integrated Circuit Card

FDMA: Frequency-Division Multiple Access

FM: Frequency Modulation

Gbps: Gigabits per second

GNB: gNodeB

GSM: Global System for Mobile communication

GTP: GPRS Tunnelling Protocol

HD: High-Definition

HIP: Host Identity Protocol

HSM: Hardware Security Module

HTTP: Hypertext Transfer Protocol

HX-DoS: Hypertext Denial of Service

IAM: Identity and Access Management

IMSI: International Mobile Subscriber Identity

IMTMC: IMT MultiCarrier

IoNT: Internet of Nano Things

IOT: Internet of Things

IP: Internet Protocol

IPsec: Internet Protocol Security

ITU: International Telecommunication Union

iUICC: Integrated Universal Integrated Circuit Card

LTE: Long Term Evolution

M2M: Machine to Machine

MAC: Media Access Control attack

massive MIMO: massive Multiple-Input Multiple-Output

MCC: Mobile Cloud Computing

MEC: Multi-Access Edge Computing

MFA: Multi-factor authentication

MiTM: Man-in-the-middle

ML: Machine Learning

MLS: Machine Learning System

mMTC: massive Machine Type Communications

MNO: Mobile Network Operator

MVNO: Mobile Virtual Network Operator

NF: Network Function

NFS: Network File System

NFC: Near Field Communication

NGMN: Next Generation Mobile Network

NR: 5G New Radio

NSI: Network Slice Instance

NSM: Network and Security Manager

OEM: Original Equipment Manufacturer

OSI: Open Systems Interconnection

OSS: Operations Support System

OTA: Over-the-air

PLMN: Public Land Mobile Network

POS: Point-of-Sale

PPS: Packets per second

RAN: Radio Access Network

RAT: Radio Access Technology

SBA: Service-Based Architecture

SDN: Software-Defined Network

SE: Secure Element

SIM: Subscriber Identity Module

SLA: Service Level Agreement

SoC: System on Chip

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

TDMA: Time Division Multiple Access

TLS: Transport Layer Security

TPM: Trusted Platform Module

UE: User Equipment

UICC: Universal Integrated Circuit Card

UMTS: Universal Mobile Telecommunications System

uRLLC: ultra Reliable Low-Latency Communications

USIM: Universal Subscriber Identity Module

VM: Virtual Machine

VMM: Virtual Machine Monitor

VNF: Virtual Network Function

VR: Virtual Reality

vUICC: virtual Universal Integrated Circuit Card

WCDMA: Wideband-CDMA

Wi-Fi: Wireless Fidelity

WiMax: Worldwide inter-operability for Microwave Access

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WPAN: Wireless Personal Area Network

WWAN: Wireless Wide Area Network

XML: eXtensible Markup Language

Λεξικό όρων

5G: Δίκτυα 5ης γενιάς

5G Core Network: Πυρήνας δικτύου 5G

5G New Radio: Νέο 5G δίκτυο ραδιοεπικοινωνιών

Application Layer: Επίπεδο εφαρμογών

Application Programming Interfaces: Διεπαφές εφαρμογών

Artificial Intelligence: Τεχνητή νοημοσύνη

ARP spoofing / poisoning: Πλαστογράφηση ή δηλητηρίαση ARP

Augmented Reality: Επαυξημένη πραγματικότητα

Backhaul: Επιστροφή δεδομένων

Big Data: Μεγάλα δεδομένα

Bogus information attack: Επίθεση ψευδών πληροφοριών

Business Support Systems: Συστήματα επιχειρηματικών δραστηριοτήτων

Central Point of Failure threat: Απειλή ενός κεντρικού σημείου αποτυχίας

Cloud (Computing): Υπολογιστικό Νέφος

Cloud Radio Access Network: Δίκτυο ραδιοπρόσβασης του υπολογιστικού νέφους

Code Division Multiple Access: Πολυπλεξία κώδικα ή αλλιώς διαίρεση (ορθογωνιότητα-διαχωρισμός) κώδικα

Congestion control threat: Έλεγχος συμφόρησης

Critical Communications: Κρίσιμες επικοινωνίες

Cyber-Physical System: Κυβερνοφυσικά συστήματα

Data centers: Κέντρα δεδομένων

Data Link Layer: Επίπεδο συνδέσμου δεδομένων

Demand Response Management: Διαχείριση ανταποκρινόμενη στη ζήτηση

Device trigger threat: Απειλή ενεργοποίησης συσκευής

Distributed Denial-of-Service: Κατανεμημένη άρνηση υπηρεσίας

Avoid detection attack: Επίθεση αποφυγής ανίχνευσης

Cloud Radio Access Network: Δίκτυο ραδιοπρόσβασης υπολογιστικού νέφους

DoS attacks: Επιθέσεις άρνησης υπηρεσίας

Downlink: Κατερχόμενη ζεύξη

Eavesdropping attack: Επίθεση υποκλοπής

Edge Computing: Ακροδικτυακή υπολογιστική ή υπολογιστική των παρυφών

enhanced Mobile BroadBand: Ενισχυμένη κινητή ευρυζωνικότητα

End-to-end security: Ασφάλεια από άκρο σε άκρο

European Union Agency for Cybersecurity: Οργανισμός της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια

Evil-Twin attack: Επίθεση κακού διδύμου

Flash network traffic: Κίνηση δικτύου αιχμής

Frequency-Division Multiple Access: Πολλαπλή πρόσβαση συχνότητας

Frequency Modulation: Διαμόρφωσης πλάτους

Gateway: Πύλη δικτύου

Global System for Mobile communication: Παγκόσμιο σύστημα κινητών επικοινωνιών

Hardware: Υλικό

Hardware Security Module: Μονάδα ασφαλείας υλικού

Hijacking attack: Επίθεση αεροπειρατείας

Host Identity Protocol: Πρωτόκολλο ταυτότητας υπολογιστή

Hypervisor: Υπεύθυνος εποπτείας

Identity and Access Management: Διαχείριση ταυτότητας και πρόσβασης

Illusion attack: Επίθεση ψευδαίσθησης

Impersonation attack: Επίθεση πλαστοπροσωπίας

Infrastructure Layer: Επίπεδο υποδομής

Injection attack: Επίθεση εισαγωγής

International Mobile Subscriber Identity: Διεθνής ταυτότητα κινητού του συνδρομητή

International Telecommunication Union: Διεθνής Ένωση Τηλεπικοινωνιών

Internet of Things: Διαδίκτυο των πραγμάτων

Internet Protocol: Πρωτόκολλο διαδικτύου

IoT Device Security: Ασφάλεια των IoT συσκευών

Jamming attack: Επίθεση παρεμβολής

Latency: Καθυστέρηση (δικτύου)

Lawful Intercept: Νόμιμη παρακολούθηση

Legacy systems: Παλαιά συστήματα

Logistics: Εφοδιαστική αλυσίδα

MAC flooding: Υπερχείλιση MAC

Machine Learning: Μηχανική μάθηση

Machine Learning System: Σύστημα μηχανικής μάθησης

Malware attack: Επίθεση κακόβουλου λογισμικού

Man-in-the-middle attack: Επίθεση ενδιάμεσου άνδρα

Mandated security in the network: Επιβαλλόμενη ασφάλεια στο δίκτυο

Masquerade attack: Επίθεση μεταμφίεσης

Massive Machine Type Communications: Μαζικές επικοινωνίες τύπου μηχανής

Message spoofing attack: Επίθεση παραποίησης μηνύματος

Mobile Cloud Computing: Κινητό υπολογιστικό νέφος

Mobile Network Operator: Διαχειριστής δικτύου κινητής τηλεφωνίας

Mobile Virtual Network Operator: Εικονικός πάροχος υπηρεσιών κινητών επικοινωνιών

Multi-Access Edge Computing: Ακροδιαδικτυακή υπολογιστική πολλαπλών προσβάσεων

Multi-factor authentication: Πολλαπλή επαλήθευση ταυτότητας

Near Field Communication: Επικοινωνία κοντινού πεδίου

Network access attack: Επίθεση πρόσβασης δικτύου

Network and Security Manager: Διαχειριστής δικτύου και ασφάλειας

Network File System: Σύστημα αρχειοθέτησης δικτύου

Network Function: Λειτουργία δικτύου

Network Function Layer: Επίπεδο λειτουργίας δικτύου

Network Layer: Δικτυακό Επίπεδο

Network Slice: Κομμάτι δικτύου

Network Slice Controller: Ελεγκτής τεμαχίου δικτύου

Network Slice Instance: Παρουσία τεμαχίου δικτύου

Network Slices: Τεμάχια δικτύου

Network Slicing: Τεμαχισμός δικτύου

Network Virtualization: Εικονικοποίηση δικτύου

Node capture threat: Απειλή κατάληψης κόμβου

Operations Support Systems: Συστήματα υποστήριξης λειτουργειών

Orchestration: Ενορχήστρωση

Original Equipment Manufacturer: Αρχικός κατασκευαστής εξοπλισμού

Physical Layer: Φυσικό επίπεδο

Piggybacking: Μεταφορά κακόβουλων μικρών δεδομένων πάνω από μεγαλύτερα δεδομένα

Pilot spoofing attack: Επίθεση πλαστογράφησης πιλότου

Point-of-Sale: Σημείο πώλησης

Presentation Layer: Επίπεδο παρουσίασης

Privacy leaking: Διαρροή προσωπικών δεδομένων

Public Land Mobile Network: Δημόσιο δίκτυο κινητής τηλεφωνίας

Quality of Service: Ποιότητα υπηρεσίας

Radio Access Network: Δίκτυο ραδιοπρόσβασης

Radio Access Technology: Τεχνολογίες ραδιοπρόσβασης

Replay attack: Επίθεση επανάληψης

Response or header collision attack: Επίθεση σύγκρουσης απάντησης ή κεφαλίδας

Roaming: Περιαγωγή

Router: Δρομολογητής

SDN scanner attacks: Επιθέσεις σαρωτή SDN

Secure Element: Στοιχείο ασφαλείας

Secure enclaves: Ασφαλή περιβάλλοντα εκτέλεσης

Security of radio interfaces: Ασφάλεια διεπαφής ραδιοσυχνοτήτων

Server: Διακομιστής

Service-Based Architecture: Αρχιτεκτονική βασισμένη σε υπηρεσίες

Service Layer: Επίπεδο υπηρεσίας

Service Level Agreement: Συμφωνία επιπέδου υπηρεσιών

Session Key: Κλειδί συνεδρίας

Session Layer: Επίπεδο Συνεδρίας

Signaling attacks: Επιθέσεις σηματοδοσίας

Slice Isolation: Απομόνωση τεμαχίου

Smart Cities: Ευφυείς πόλεις

Smart Meters: Έξυπνοι μετρητές ρεύματος

Smartphones: Έξυπνα κινητά

Sniffer: Λογισμικό παρακολούθησης δικτύου

Software: Λογισμικό

Software Defined Networks: Δίκτυα βασισμένα σε λογισμικό

Status messages: Μηνύματα κατάστασης

Subscriber Identity Module: Μονάδα ταυτότητας συνδρομητή

Sybil attack: Σιβυλλική επίθεση

Synchronization disruption attack: Επίθεση διατάραξης συγχρονισμού

System on Chip: Σύστημα ενσωματωμένου κυκλώματος

Time Division Multiple Access: Πολυπλεξία στο χρόνο ή διαφορετικά διαίρεση (ορθογωνιότητα-διαχωρισμός) χρόνου

Timing attack: Επίθεση χρονισμού

Traffic confidentiality attack: Επίθεση εμπιστευτικότητας κίνησης

Traffic integrity attack: Επίθεση ακεραιότητας κίνησης

Transport Layer: Επίπεδο Μεταφοράς

Trusted Platform Module: Αξιόπιστη πλατφόρμα

Tunnels: Σήραγγες

Ultra Reliable Low-Latency Communications: Υπερ-αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης

Universal Integrated Circuit Card: Κάρτα ολοκληρωμένου κυκλώματος

Universal Mobile Telecommunications System: Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών

Universal Subscriber Identity Module: Παγκόσμια Μονάδα Ταυτότητας Συνδρομητή

Uplink: Ανοδική ζεύξη

User Equipment: Τερματικός εξοπλισμός ή εξοπλισμός χρήστη

User plane integrity: Ακεραιότητα επιπέδου χρήστη

Virtual Machines: Εικονικές μηχανές

Virtual Network Function: Εικονική λειτουργία δικτύου

Virtual Reality: Εικονική πραγματικότητα

Virtualization: Εικονικοποίηση

Virtualized software instances: Εικονικά στιγμιότυπα λογισμικού

Wearables: Φορητές συσκευές

Wireless Local Area Network: Ασύρματα τοπικά δίκτυα

Wireless Metropolitan Area Networks: Ασύρματα μητροπολιτικά δίκτυα

Wireless Personal Area Network: Ασύρματα προσωπικά δίκτυα

Wireless Wide Area Network: Ασύρματα δίκτυα ευρείας περιοχής

ΠΡΟΛΟΓΟΣ

Η παρούσα εργασία με τίτλο "ΑΣΦΑΛΕΙΑ ΣΕ 5G ΔΙΚΤΥΑ" δημιουργήθηκε για να εξετάσει τις προκλήσεις και τις λύσεις που σχετίζονται με την ασφάλεια στα 5G δίκτυα, με έμφαση στον τεμαχισμό δικτύου. Η ιδέα για αυτό το έργο γεννήθηκε από την ανάγκη να κατανοηθεί καλύτερα η νέα γενιά δικτύων και οι καινοτομίες που αυτή φέρνει, καθώς και οι νέες απειλές και προκλήσεις που ανακύπτουν στον τομέα της ασφάλειας.

Κίνητρο για τη συγγραφή αυτής της εργασίας ήταν η συνεχής πρόοδος των τεχνολογιών επικοινωνίας και η επιτακτική ανάγκη διασφάλισης του απορρήτου και της ασφάλειας των πληροφοριών στα σύγχρονα περιβάλλοντα. Η διαδικασία συγγραφής εξελίχθηκε μέσα από ενδελεχή έρευνα και ανάλυση των τελευταίων εξελίξεων στον χώρο των 5G δικτύων και των τεχνολογιών που τα υποστηρίζουν, όπως οι SDN και NFV.

Κατά τη διάρκεια της συγγραφής, ανέκυψαν αρκετές προκλήσεις όσον αφορά στη συλλογή και στην κατανόηση των πληροφοριών λόγω της ταχύτατης ανάπτυξης της τεχνολογίας και της πληθώρας των διαθέσιμων πηγών.

Θα ήθελα να εκφράσω τις ευχαριστίες μου προς την καθηγήτρια μου, η οποία παρείχε πολύτιμη καθοδήγηση και υποστήριξη καθ' όλη τη διάρκεια της έρευνας και συγγραφής αυτής της εργασίας. Επίσης, ευχαριστώ την οικογένειά μου για την αδιάκοπη υποστήριξή της κατά τη διάρκεια των σπουδών μου.

Ελπίζω η παρούσα εργασία να αποτελέσει ένα χρήσιμο εργαλείο για όσους ενδιαφέρονται για την ασφάλεια των 5G δικτύων και να συμβάλει στην περαιτέρω έρευνα και κατανόηση των σύγχρονων προκλήσεων και λύσεων στον τομέα αυτό.

ΕΙΣΑΓΩΓΗ

Το 5G (fifth-generation mobile network) ή αλλιώς τα δίκτυα 5ης γενιάς χρησιμοποιούνται ως όροι για να περιγράψουν τα ψηφιακά δίκτυα κινητής τηλεφωνίας τα οποία, μεταξύ άλλων, παρέχουν πολύ υψηλές ταχύτητες σε σχέση με τα δίκτυα κινητής προηγούμενων γενεών (3G, 4G, κλπ.) και ταυτόχρονα εξαιρετικά χαμηλή καθυστέρηση (latency). Ταυτόχρονα όμως, ο όρος 5G ενσωματώνει και όλα τα απαιτούμενα πρωτόκολλα επικοινωνίας, τον εξοπλισμό του παρόχου κινητής τηλεφωνίας (κεραίες, δίκτυο, κλπ.), αλλά και τις επιχειρηματικές δυνατότητες που παρέχουν οι υψηλές ταχύτητες που αυτό προσφέρει.

Εκτός από την παροχή ταχύτερης πρόσβασης σε αυτό, η νέα υποδομή δικτύου σηματοδοτεί την αλλαγή από μια, σε μεγάλο βαθμό στατική, σε μια σημαντικά πιο δυναμική αρχιτεκτονική δικτύου. Είναι σαφές, ότι η ανάπτυξη ξεχωριστής υποδομής για κάθε υπηρεσία θα ήταν εξαιρετικά δαπανηρή και αναποτελεσματική. Έτσι, οι πρωταρχικοί στόχοι του 5G είναι να κάνει μεγαλύτερη χρήση των πόρων της υποδομής, να επιτρέψει σε πολλές εφαρμογές με ευρέως διαφορετικές προδιαγραφές να μοιράζονται τη χρήση του και να προσθέσει την ευελιξία και την επεκτασιμότητα που απαιτούνται για την ικανοποίηση συγκεκριμένων αναγκών.

Η νέα αυτή γενιά των τηλεπικοινωνιακών συστημάτων είναι στις μέρες μας γεγονός και τα πλεονεκτήματα που τη συνοδεύουν είναι πολυάριθμα και σημαντικά. Όπως προαναφέρθηκε προσφέρονται νέες τεχνολογίες, υψηλές ταχύτητες και σταθερότητα. Πιο αναλυτικά, έχει εκτιμηθεί ότι οι αναμενόμενες ταχύτητες δύνανται να φτάσουν ακόμα και τα 20 Gbit/s σε αντίθεση με τον προκάτοχο του (4G) όπου οι μέγιστες ταχύτητες ήταν της τάξης του 1Gbit/s. Επιπλέον, διευκολύνεται η σύνδεση πολλαπλών συσκευών καθώς τα δίκτυα πέμπτης γενιάς είναι σχεδιασμένα να υποστηρίζουν επαρκώς το διαδίκτυο των πραγμάτων (IOT: Internet of Things).

Μία από τις σημαντικότερες τεχνολογίες που χρησιμοποιήθηκε για την επίτευξη όλων αυτών είναι ο τεμαχισμός δικτύου (Network Slicing). Με την τεχνική αυτή δημιουργείται ένα εικονικό δίκτυο στην υπάρχουσα υποδομή προκειμένου να παρέχονται υπηρεσίες με ταχύτητα και ελαστικότητα, όσον αφορά στις προδιαγραφές τους. Ο πάροχος δημιουργεί ένα κομμάτι δικτύου (Network Slice) με τα πολύ συγκεκριμένα χαρακτηριστικά γνωρίσματα που απαιτείται αυτό να έχει, ώστε να καλύψει την εκάστοτε ανάγκη. Το κομμάτι της ασφάλειας σε αυτό το κομμάτι δικτύου είναι αναμφίβολα η πιο σημαντική πρόκληση. Επειδή, ωστόσο ο

τεμαχισμός χτίζεται πάνω από άλλες τεχνολογίες, οι προκλήσεις αφορούν σε μια πληθώρα τεχνολογιών και υποδομών.

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

1.1 Ορισμός των ασύρματων δικτύων

Ως ασύρματο δίκτυο χαρακτηρίζεται το δίκτυο υπολογιστών το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης των δεδομένων που απαιτείται να υποστηρίξει το δίκτυο. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιο τύπο καλωδίου. Στα ασύρματα δίκτυα εντάσσονται τα δίκτυα κινητής τηλεφωνίας, οι δορυφορικές επικοινωνίες, τα ασύρματα δίκτυα ευρείας περιοχής (WWAN: Wireless Wide Area Network), τα ασύρματα μητροπολιτικά δίκτυα (WMAN: Wireless Metropolitan Area Networks), τα ασύρματα τοπικά δίκτυα (WLAN: Wireless Local Area Network) και τα ασύρματα προσωπικά δίκτυα (WPAN: Wireless Personal Area Network) (Garg, 2008).

























1.2 Ιστορική αναδρομή των ασύρματων δικτύων

Η κινητή επικοινωνία εξελίσσεται συνεχώς με εντυπωσιακούς ρυθμούς, με νέες τεχνικές να εμφανίζονται σε όλους τους τομείς της κινητής και ασύρματης επικοινωνίας. Η πρώτη γενιά (1G) κινητών δικτύων εισήγαγε αναλογικά συστήματα μετάδοσης, ενώ η δεύτερη γενιά (2G) χρησιμοποίησε το πρότυπο του Παγκόσμιου Συστήματος Κινητών Επικοινωνιών (GSM: Global System for Mobile communication) για βελτιωμένη ποιότητα φωνής και περιορισμένες υπηρεσίες δεδομένων. Η τρίτη γενιά (3G) έφερε τη δυνατότητα χρήσης εφαρμογών ήχου, γραφικών και βίντεο, ενώ η τέταρτη γενιά (4G) προσέφερε αυξημένες ταχύτητες δεδομένων και βελτιωμένη συνδεσιμότητα, θέτοντας τις βάσεις για την ψηφιακή εποχή. Πιο αναλυτικά (Kumar & Sumit, 2021; Sucheta & Yadav, 2013; Shukla et al., 2013):

- **First Generation (1G):** Τα δίκτυα πρώτης γενιάς πρωτοεμφανίστηκαν το 1983. Ήταν τα μόνα δίκτυα των οποίων η τεχνολογία ήταν αναλογική. Πιο συγκεκριμένα χρησιμοποιούσαν τεχνολογία διαμόρφωσης πλάτους (FM: Frequency Modulation) και πολλαπλή πρόσβαση συχνότητας (FDMA: Frequency-Division Multiple Access). Τα σήματα που μεταδίδονταν ήταν μόνο για ομιλία με ταχύτητες που κυμαίνονταν μεταξύ των 28kbps και 56kbps. Η συγκεκριμένη γενιά αντιμετώπιζε θέματα ασφάλειας καθώς η κλοπή των σημάτων ομιλίας ήταν πολύ εύκολη.

- **Second Generation (2G-2.5G):** Τα δίκτυα δεύτερης γενιάς πρωτοεμφανίστηκαν την δεκαετία του '90 με το σήμα να αλλάζει από αναλογικό σε ψηφιακό, χρησιμοποιώντας τεχνικές πολλαπλής πρόσβασης όπως είναι η πολυπλεξία κώδικα ή αλλιώς διαίρεση (ορθογωνιότητα-διαχωρισμός) κώδικα (CDMA: Code Division Multiple Access) και η πολυπλεξία στο χρόνο ή διαφορετικά διαίρεση (ορθογωνιότητα-διαχωρισμός) χρόνου (TDMA: Time Division Multiple Access). Με αυτό τον τρόπο επιτεύχθηκε τόσο η μετάδοση της φωνής όσο και η δυνατότητα αποστολής και λήψης μηνυμάτων και φωτογραφιών.
- **Third Generation (3G):** Τα δίκτυα τρίτης γενιάς πρωτοεμφανίστηκαν το 1998 και παρείχαν στα κινητά τηλέφωνα επιπλέον δυνατότητες, όπως αυτή της πρόσβασης στο διαδίκτυο και της πραγματοποίησης βιντεοκλήσεων. Αυτό κατέστη δυνατό χάρη σε δυο νέα πρότυπα: το πρότυπο CDMA2000 ή C2K ή IMT MultiCarrier (IMTMC) και το wideband-CDMA (WCDMA). Ο ρυθμός μετάδοσης των πληροφοριών που υποστηρίζουν οι υπηρεσίες των δικτύων τηλεπικοινωνιών 3G ξεκινούσαν από 0,2Mbit/s.
- **Fourth Generation (4G):** Τα δίκτυα τέταρτης γενιάς πρωτοεμφανίστηκαν το 2009 προσφέροντας μεγαλύτερες ταχύτητες αλλά όχι νέες υπηρεσίες. Το 4G στηρίχτηκε πάνω σε δυο νέα πλαίσια, την τεχνολογία WiMAX (Worldwide Interoperability for Microwave Access) και το πρότυπο LTE (Long Term Evolution). Με τη χρήση των παραπάνω επιτεύχθηκαν ταχύτητες οι οποίες έφταναν τα 100 Mbps αλλά και μεγαλύτερη εμβέλεια επικοινωνίας σε σχέση με τον προκάτοχο τους (3G). Τέλος η εμβέλεια επικοινωνίας αυτών των δικτύων έφτανε περίπου στα 30 χιλιόμετρα.

Η παρακάτω εικόνα παρέχει μια συνοπτική απεικόνιση των γενεών των δικτύων των τηλεπικοινωνιών και τις χρονικές περιόδους λανσαρίσματός τους:

1980s 1G <i>Analog Era</i>		 2.4 kbps
1991 2G <i>Digital Era</i>	 SMS/MMS	 64 kbps
1998 3G <i>Mobile Internet Era</i>	    SMS/MMS Internet Access Video Calls Mobile TV	 2,000 kbps
2008 4G <i>Mobile Internet Era</i>	      SMS/MMS Internet Access Video Calls Mobile TV Gaming Services Cloud Computing	 100,000 kbps
2020 5G <i>Internet of Everything</i>	        SMS/MMS Internet Access Video Calls Mobile TV HD AR/VR Cloud Computing Robotics Automobile	 More than 1 Gbps

Εικόνα 1: Γενιές Δικτύων τηλεπικοινωνιών

Πηγή: TE Connectivity Ltd., 2018

1.3 Χαρακτηριστικά γνωρίσματα του 5G

Η ανάπτυξη των 5G δικτύων είναι ο καταλύτης για την εμβάθυνση της ψηφιακής οικονομίας, καθώς αποτελεί τη μόνη ασύρματη τεχνολογία που μπορεί να υποστηρίξει την ανάπτυξη νέων καινοτόμων λύσεων και εναλλακτικών πηγών εισοδήματος και να επιτρέψει σε υπάρχουσες καινοτομίες την αξιόπιστη υιοθέτησή τους σε μεγάλη κλίμακα. Τα πλεονεκτήματα που προσφέρουν τα δίκτυα 5G είναι κυρίως η πρόσβαση σε ταχύτητες μετάδοσης παραπλήσιες των οπτικών ινών και με εξαιρετικά χαμηλή καθυστέρηση στη μετάδοση των δεδομένων, δίνοντας ώθηση στη διάδοση των ψηφιακών μέσων, στη λειτουργία των MME αλλά και στην ανάπτυξη νέων οικονομιών. Παρακάτω παρατίθεται μια αναλυτική λίστα των πλεονεκτημάτων που αυτά προσφέρουν (Ancans et al., 2017):

- **Ταχύτητα:** Το 5G είναι 10 φορές ταχύτερο από το 4G (θεωρητικές μέγιστες τιμές, που εξαρτώνται από το διαθέσιμο φάσμα, την απόσταση από το σταθμό βάσης κ.λπ.). Προσφέρει ταχύτητες αποστολής έως και 10 Gbit/s και ταχύτητα λήψης έως και 20

Gbit/s. Η λήψη ταινίας πλήρους HD (High-Definition) ολοκληρώνεται σε λιγότερο από 10 δευτερόλεπτα, σε σύγκριση με τα 10 λεπτά του 4G.

- **Πολύ χαμηλότερος χρόνος απόκρισης:** Με το 5G, ο χρόνος απόκρισης μιας συσκευής μπορεί να είναι μόλις 1 ms, μια καθυστέρηση που δεν γίνεται καν αντιληπτή από το χρήστη. Αυτός ο αριθμός ποικίλλει εντός 10 ms στο 4G.
- **Χωρητικότητα:** Το 5G έχει μεγαλύτερη χωρητικότητα, άρα τα δίκτυα μπορούν να ανταπεξέλθουν καλύτερα στην ταυτόχρονη εξυπηρέτηση εφαρμογών υψηλών απαιτήσεων.
- **Υψηλή πυκνότητα σύνδεσης συσκευών:** Με το 5G δίκτυο μπορούν να είναι συνδεδεμένες ταυτόχρονα έως 1 εκατομμύριο συσκευές/Km², σε αντίθεση με 10.000-100.000 συσκευές/Km² που μπορούν να υποστηριχθούν από την 4G υποδομή.
- **Συχνότητα λειτουργίας:** Το 5G λειτουργεί σε 4 διαφορετικές ζώνες συχνοτήτων: 700MHz, 2GHz, 3,4-3,8GHz και 26GHz, διαθέτοντας ένα πολύ μεγαλύτερο φάσμα από τους προκατόχους του.
- **Ευελιξία:** Ο τεμαχισμός δικτύου είναι μια τεχνική που επιτρέπει σε ένα δίκτυο να χωριστεί σε λογικά μέρη με διαφορετικές παραμέτρους ποιότητας, όπως είναι για παράδειγμα ένα δίκτυο υψηλής προτεραιότητας για τις αστυνομικές δυνάμεις και ένα δίκτυο χαμηλής ισχύος και χαμηλών απαιτήσεων για απλούς IoT αισθητήρες.
- **Ενισχυμένη διάρκεια ζωής μπαταρίας:** Αναμένεται έως και 10 χρόνια μεγαλύτερη διάρκεια ζωής της μπαταρίας για τις συσκευές που εξυπηρετούνται από το 5G δίκτυο.
- **Κατανομή πόρων:** Παρέχει τηλεπικοινωνιακούς, υπολογιστικούς και αποθηκευτικούς πόρους σε μια ολοκληρωμένη, προγραμματιζόμενη, ενοποιημένη υποδομή, που επιτρέπει τη βέλτιστη χρήση των καταναμημένων πόρων. Πρόκειται επομένως, για έναν υπηρεσιοστρεφή και βασισμένο στο λογισμικό μετασχηματισμό όπου:
 1. Το μέσο δεν είναι απλά μια παροχή bits, αλλά μια πλατφόρμα με πολλαπλές δυνατότητες.
 2. Το δίκτυο δεν εξυπηρετεί μόνο τα κινητά τηλέφωνα αλλά και άλλα αντικείμενα (things).
 3. Όλες οι διαδικασίες αντιμετωπίζονται ως υπηρεσίες.

4. Τα πρωτόκολλα αντιμετωπίζονται ως διεπαφές εφαρμογών (APIs: Application Programming Interfaces).
5. Δεν υπάρχει αποκλειστικό υλικό (hardware) για μια υπηρεσία/ανάγκη, αλλά όπως χαρακτηριστικά αναφέρεται, «ενορχηστρωμένοι πόροι» προκειμένου οι διαθέσιμες λειτουργίες του δικτύου να εξυπηρετούν κατάλληλα τις εκάστοτε εφαρμογές.

Επί της ουσίας, το δίκτυο 5^{ης} γενιάς είναι μια πλήρως προγραμματιζόμενη πλατφόρμα, η οποία παρέχει πολλές και διαφορετικές μεταξύ τους λειτουργίες, οι οποίες παρέχονται με το «as-a service» (ως-υπηρεσία) μοντέλο. Όλες οι λειτουργίες του δικτύου 5G είναι εικονικά διαμορφωμένα στιγμιότυπα λογισμικού (virtualized software instances) τα οποία υλοποιούνται και τρέχουν σε κέντρα δεδομένων (Data Centers). Συνεπώς, στα 5G δίκτυα είναι κυρίαρχη η λογική του νέφους (cloud). Μέσω λογισμικού και τεχνολογιών νέφους, δημιουργούνται δυναμικά «φέτες» (slices) δικτύου ώστε να προσφερθούν διαφοροποιημένες υπηρεσίες για την κατ' απαίτηση χρήση από τις εφαρμογές. Οι «φέτες» του δικτύου που δημιουργούνται με αυτόν τον τρόπο, μπορούν να θεωρηθούν ως ένα είδος κατά παραγγελία virtual δικτύου, με συγκεκριμένα κάθε φορά χαρακτηριστικά: επιδόσεις δικτύου, παραμέτρους ασφάλειας, ποιότητα υπηρεσίας, τρόπος χρέωσης, κλπ.. Τα παραπάνω χαρακτηριστικά τίθενται ανάλογα με την εφαρμογή ή την υπηρεσία που η κάθε «φέτα» προγραμματίζεται να εξυπηρετήσει. Έτσι, με αυτή την υλοποίηση, πολλά λογικά δίκτυα μοιράζονται τους ίδιους πόρους. Το συνολικό δίκτυο δε, χτίζεται με τέτοιο τρόπο, ούτως ώστε να είναι σε θέση να εξυπηρετήσει με επιτυχία τόσο τις σημερινές εφαρμογές και τις υπηρεσίες, όσο και ένα εύρος μελλοντικών εφαρμογών, οι οποίες δεν έχουν σχεδιαστεί ακόμη.

Στον παρακάτω πίνακα απεικονίζονται τα βασικά χαρακτηριστικά γνωρίσματα των πέντε γενεών δικτύων τηλεπικοινωνιών:

	1G	2G	3G	4G	5G
Period	1980 – 1990	1990 – 2000	2000 – 2010	2010 – (2020)	(2020 - 2030)
Bandwidth	150/900MHz	900MHz	100MHz	100MHz	1000x BW pr unit area
Frequency	Analog signal (30 KHz)	1.8GHz (digital)	1.6 – 2.0 GHz	2 – 8 GHz	3 – 300 GHz
Data rate	2kbps	64kbps	144kbps – 2Mbps	100Mbps – 1Gbps	1Gbps <
Characteristic	First wireless communication	Digital	Digital broadband, increased speed	High speed, all IP	
Technology	Analog cellular	Digital cellular (GSM)	CDMA, UMTS, EDGE	LTE, WiFi	WWW

Εικόνα 2: Βασικά χαρακτηριστικά γνωρίσματα των 1G, 2G, 3G, 4G και 5G δικτύων

Πηγή: AGMPlanning, 2024

1.4 Γενική κατηγοριοποίηση των 5G υπηρεσιών

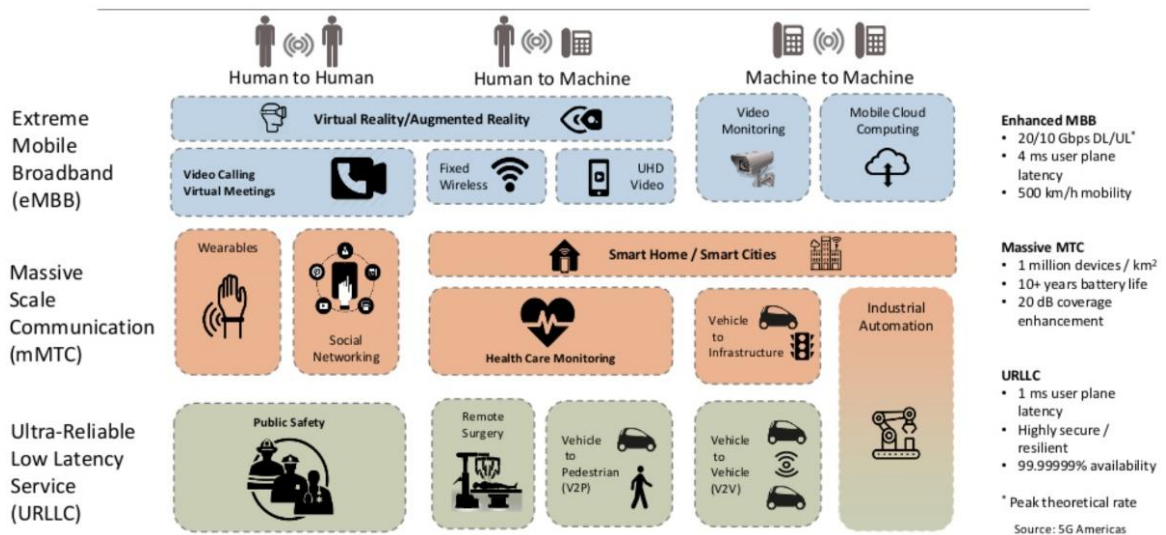
Πολύ σημαντικό χαρακτηριστικό των συστημάτων της γενιάς αυτής δεν είναι μόνο η αναβάθμιση των ευρυζωνικών συνδέσεων αλλά και η ικανότητα εξυπηρέτησης πολλών, νέων υπηρεσιών. Αυτές οι υπηρεσίες και οι νέες εφαρμογές έχουν αλλάξει σε μεγάλο βαθμό τον σύγχρονο τρόπο ζωής και απασχόλησης. Οι κινητές ευρυζωνικές συνδέσεις περιλαμβάνουν εκτός των άλλων, την επικοινωνία μεταξύ των ανθρώπων και του νέφους, μεταξύ των ανθρώπων και των αντικειμένων, καθώς και μεταξύ των αντικειμένων. Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU: International Telecommunication Union) έχει χωρίσει τις υπηρεσίες των 5G δικτύων σε τρεις μεγάλες κατηγορίες - περιπτώσεις χρήσης (use cases) (Fakhouri, et al., 2023; Foukas et al., 2017):

1. **Τις υπηρεσίες ενισχυμένης κινητής ευρυζωνικότητας (eMBB: enhanced Mobile BroadBand):** οι οποίες προκειμένου να προσφέρουν ανώτερη κάλυψη και συνεπή συνδεσιμότητα σε όλη την περιοχή εξυπηρέτησής τους, απαιτούν ένα μεγάλο εύρος ζώνης και εξαιρετικά υψηλές ταχύτητες μετάδοσης. Οι υπηρεσίες βίντεο HD, επαυξημένης πραγματικότητας (AR: Augmented Reality) και εικονικής πραγματικότητας (VR: Virtual Reality) είναι παραδείγματα τέτοιων υπηρεσιών.
2. **Τις υπηρεσίες υπερ-αξιόπιστων επικοινωνιών χαμηλής καθυστέρησης (uRLLC: Ultra Reliable Low-Latency Communications):** οι οποίες χαρακτηρίζονται από ανάγκη για υψηλή χωρητικότητα και μεγάλες ταχύτητες μετάδοσης δεδομένων, μιας

και χρησιμεύουν στην παρακολούθηση και στον απομακρυσμένο έλεγχο διάφορων κρίσιμων διαδικασιών σε πραγματικό χρόνο. Παραδείγματα χρήσης τέτοιων υπηρεσιών είναι ο έλεγχος βιομηχανικών διαδικασιών, τα δίκτυα αισθητήρων, η αυτοματοποίηση της διανομής ενέργειας και ο απομακρυσμένος έλεγχος κρίσιμων μηχανημάτων (εγχειρήσεις/υπηρεσίες υγείας, αυτόνομη οδήγηση, χειρισμός βαρέων οχημάτων κ.λπ.).

3. **Τις υπηρεσίες μαζικών επικοινωνιών τύπου μηχανής (mMTC: Massive Machine Type Communications):** που μπορούν να προσφέρουν εκατοντάδες χιλιάδες συσκευές ανά km², εκτεταμένη κάλυψη και βαθιά διείσδυση τόσο σε εσωτερικό όσο και σε εξωτερικό περιβάλλον. Επιπλέον, αυτή η κατηγορία είναι κατάλληλη για να προσφέρει συνδεσιμότητα χαμηλού κόστους, χαμηλής κατανάλωσης ενέργειας με ελάχιστη πολυπλοκότητα υλικού και λογισμικού. Η ανάπτυξη έξυπνων πόλεων, η διαχείριση και η παρακολούθηση στόλου, η έξυπνη αλυσίδα εφοδιασμού (logistics), η έξυπνη γεωργία και η παρακολούθηση και αυτοματοποίηση κτιρίων είναι μερικά παραδείγματα τέτοιων εφαρμογών.

Η παρακάτω εικόνα συνοψίζει τις περιπτώσεις χρήσης ανά κατηγορία υπηρεσιών:



Εικόνα 3: Σύνοψη των υπηρεσιών ανά κατηγορία στο 5G δίκτυο

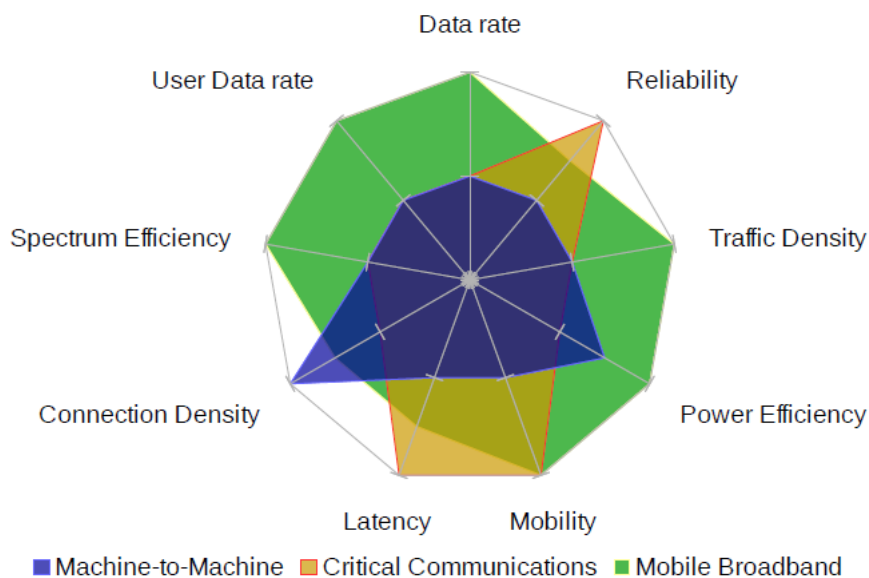
Πηγή: Trčka, 2019

Οι τεχνολογικές απαιτήσεις για τις τόσο διαφορετικές υπηρεσίες που προβλέπονται από τα δίκτυα 5G είναι πολύ μεγάλες και καλύπτουν ένα ευρύ φάσμα. Για παράδειγμα, μπορεί να απαιτείται μέσος ρυθμός μετάδοσης πληροφορίας της τάξης των 300 - 500 Mbps,

ενώ ο μέγιστος ρυθμός θα πρέπει να μπορεί να φθάσει ή και να ξεπεράσει τα 20 Gbps στην κατερχόμενη ζεύξη (Downlink) και τα 10Gbps στην ανοδική ζεύξη (Uplink).

Οι απαιτούμενοι χρόνοι αντίδρασης (latency/καθυστέρηση) στο δίκτυο ανάλογα με την εκάστοτε περίπτωση χρήσης κυμαίνονται μεταξύ 4 και 0,5 ms. Η κάλυψη των δικτύων πρέπει να πλησιάζει το 100%, ενώ η προσφερόμενη αξιοπιστία θα πρέπει να είναι εξαιρετικά υψηλή (99,999%). Να σημειωθεί, επίσης, ότι η κατανάλωση ενέργειας είναι 1000 φορές μικρότερη σε σχέση με τα δίκτυα της προηγούμενης γενιάς. Όσον αφορά στο πλήθος των συνδεδεμένων συσκευών και των αντικειμένων αναμένονται 10 ως και 100 φορές περισσότερες συσκευές με 30 φορές μεγαλύτερη χωρική πυκνότητα. Τέλος, απαιτούνται υψηλότερα επίπεδα ασφάλειας επικοινωνίας σε σχέση με τα υπάρχοντα ασύρματα δίκτυα κινητών επικοινωνιών.

Στην παρακάτω απεικόνιση, όσο μεγαλύτερη είναι η απόσταση μιας απαίτησης από το κέντρο, τόσο πιο σημαντική είναι η αντίστοιχη περίπτωση χρήσης. Οι διαφορετικές περιπτώσεις χρήσης πρέπει να αντιστοιχιστούν σε κατάλληλα προσαρμοσμένες δομές δικτύου. Επομένως, είναι ζωτικής σημασίας για μια αρχιτεκτονική 5G να είναι ευέλικτη ώστε να υλοποιεί τις διαφορετικές δομές όπως απαιτείται.



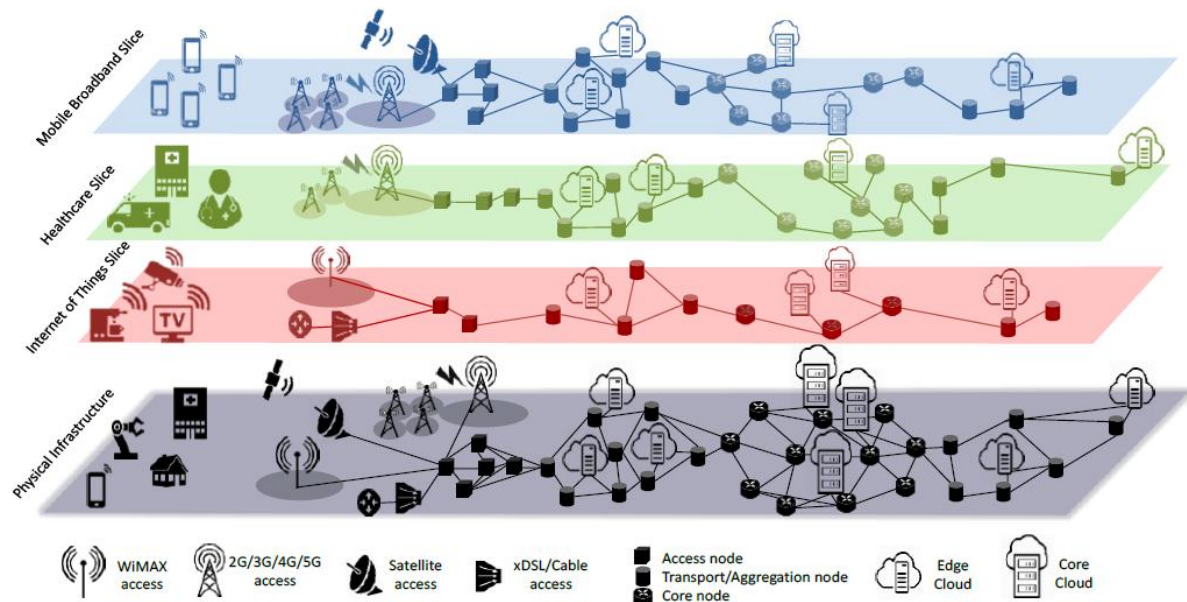
Εικόνα 4: Σπουδαιότητα απαιτήσεων των υπηρεσιών 5G ανά κατηγορία υπηρεσίας

Πηγή: Foukas et al., 2017

ΚΕΦΑΛΑΙΟ 2: 5G ΚΑΙ ΤΕΜΑΧΙΣΜΟΣ ΔΙΚΤΥΟΥ

2.1 Βασικές έννοιες

Ένα από τα κύρια χαρακτηριστικά του 5G είναι ο τεμαχισμός δικτύου, τεχνολογία που το ξεχωρίζει σε μεγάλο βαθμό από τα δίκτυα των προηγούμενων γενεών. Σε τεχνικούς όρους, η ιδέα ενός ενιαίου δικτύου έχει αντικατασταθεί από πολλαπλά εικονικά δίκτυα που λειτουργούν ταυτόχρονα και διαμοιράζονται την ίδια φυσική υποδομή. Οι «φέτες» που απαρτίζουν αυτά τα δίκτυα μπορεί να έχουν εξαιρετικά ανόμοια, ακόμη και αντικρουόμενα, χαρακτηριστικά. Κάθε κομμάτι είναι προσαρμοσμένο για να ικανοποιεί τις ξεχωριστές απαιτήσεις μιας συγκεκριμένης περίπτωσης χρήσης, όπως παρουσιάζεται στην παρακάτω εικόνα (Ordonez-Lucena et al., 2017):



Εικόνα 5: Τμήματα δικτύου 5G που εκτελούνται σε ένα κοινό υποκείμενο δίκτυο πολλαπλών προμηθευτών και πολλαπλών προσβάσεων. Κάθε κομμάτι διαχειρίζεται ανεξάρτητα και αντιμετωπίζει μια συγκεκριμένη περίπτωση χρήσης.

Πηγή: Ordonez-Lucena et al., 2017

Το 3rd Generation Partnership Project (3GPP) ορίζει τον τεμαχισμό δικτύου ως μια λογική αναπαράσταση των λειτουργιών του δικτύου και των σχετικών απαιτήσεων πόρων, που απαιτούνται για την παροχή των ζητούμενων χαρακτηριστικών του δικτύου και των τηλεπικοινωνιακών υπηρεσιών.

Το σύστημα 5G παρέχει στο διαχειριστή δικτύου κινητής τηλεφωνίας (MNO: Mobile Network Operator) τη δυνατότητα να πραγματοποιήσει “τεμαχισμό” του δικτύου σε λογικό

επίπεδο, με σκοπό τη δημιουργία «εικονικών» υποδομών δικτύου, κάθε μία από τις οποίες θα είναι εξειδικευμένη στην ικανοποίηση συγκεκριμένου τύπου υπηρεσίας π.χ. IoT με αισθητήρες μέτρησης ρύπων στους δρόμους των πόλεων. Ο διαχειριστής χωρίζει το φυσικό δίκτυο υποδομών σε πολλά εικονικά δίκτυα, δημιουργώντας λογικά δίκτυα με προσαρμοσμένες δυνατότητες για τις συγκεκριμένες ανάγκες σε μια κοινή φυσική πλατφόρμα. Είναι κατανοητό ότι με τη βοήθεια αυτού του μηχανισμού αντί να αναπτυχθούν ξεχωριστά δίκτυα που έχουν σχεδιαστεί για συγκεκριμένες υπηρεσίες, το 5G συνδυάζει αυτά τα επιμερισμένα/τεμαχισμένα δίκτυα σε μια ενιαία φυσική υποδομή για να ικανοποιήσει τις διαφορετικές ανάγκες των χρηστών. Συνεπώς, κάθε παρουσία ενός εικονικού δικτύου δημιουργείται από τον τεμαχισμό του 5G δικτύου παρέχοντας ένα απομονωμένο από άκρο σε άκρο δίκτυο, βελτιστοποιημένο για κάποιον συγκεκριμένο επιχειρηματικό σκοπό.

Πρόκειται ουσιαστικά για μια αρχιτεκτονική δικτύου που επιτρέπει σε ανεξάρτητα και εικονικά λογικά δίκτυα να πολυπλέκονται πάνω από την υποδομή ενός φυσικού δικτύου. Κάθε «τεμάχιο» είναι ένα ξεχωριστό δίκτυο που έχει διαμορφωθεί για να ικανοποιεί τις διάφορες απαιτήσεις που έχει η κάθε εφαρμογή. Τα τεμάχια αυτά μπορούν να διανεμηθούν σε πολλούς φορείς και να εκτείνονται σε διαφορετικούς τομείς δικτύου, όπως οι τομείς μεταφοράς και πρόσβασης. Μέσω της χρήσης πολυάριθμων εικονικών δικτύων που επικαλύπτουν ένα μεμονωμένο δίκτυο, ο διαχωρισμός του δικτύου 5G επιτρέπει στον χειριστή του δικτύου να μεγιστοποιήσει τη χρήση των πόρων του δικτύου και την ευελιξία των υπηρεσιών. Με την αφαίρεση, την απομόνωση, τον συντονισμό και τον διαχωρισμό των λογικών τμημάτων του δικτύου από τους φυσικούς υποκείμενους πόρους, μεταβάλλεται ριζικά η αρχιτεκτονική δικτύωσης στο σύνολό της.

2.2 Πλεονεκτήματα και μειονεκτήματα του τεμαχισμού του δικτύου

Όπως κάθε νέα τεχνολογία, έτσι και το 5G συνοδεύεται από μια σειρά πλεονεκτημάτων και μειονεκτημάτων που αξίζει να εξεταστούν προσεκτικά (Foukas et al, 2017, Βλαχάκης, άγνωστη):

Πλεονεκτήματα:

1. Διευκολύνει τις υπηρεσίες και μπορεί να δημιουργηθεί, να τροποποιηθεί και να διαγραφεί μέσω των αντίστοιχων λειτουργιών διαχείρισης δικτύου. Είναι επομένως το διαχειριζόμενο, λογικό δίκτυο ενός παρόχου που μπορεί να αναπτυχθεί τεχνικά σε οποιοδήποτε τύπο δικτύου, συμπεριλαμβανομένων κινητών και σταθερών δικτύων.

Επιπλέον, οι υποκειμένοι πόροι μπορεί να είναι φυσικοί ή εικονικοί και υπάρχει η δυνατότητα ακόμη και της ενσωμάτωσης υπηρεσιών από διαφορετικούς παρόχους που μπορεί να είναι επωφελείς για το σύνολο ή μέρος των χρηστών του π.χ. περιαγωγή (roaming).

2. Παρέχει πολύ μεγαλύτερη ευελιξία και βελτιστοποιημένη αξιοποίηση των φυσικών πόρων του δικτύου, προσαρμοσμένο στα 3GPP 5G πρότυπα και προδιαγραφές.
3. Παρέχει στους διαχειριστές δικτύων κινητής τηλεφωνίας τη δυνατότητα να αναπτύξουν μόνο τις λειτουργίες εκείνες, που απαιτούνται για την υποστήριξη των εκάστοτε πελατών και τμημάτων της αγοράς.
4. Συμβάλει στη μείωση των εξόδων, καθώς δεν είναι απαραίτητη η ανάπτυξη πρόσθετων πόρων για την προσφορά των προγραμματισμένων λειτουργιών.

Μειονεκτήματα:

1. Η κατανόηση του τρόπου δημιουργίας αυτών των «τεμαχίων» και στη συνέχεια η διαχείριση τους, καθώς και ο προσδιορισμός σε μακροοικονομικό επίπεδο της έννοιας της υπηρεσίας.
2. Οι δυσκολίες στην εικονική διαμόρφωση και στην κατανομή του δικτύου ραδιοπρόσβασης (RAN: Radio Access Network) σε διαφορετικά «τεμάχια».
3. Η εμβέλεια του δικτύου κεραιών τηλεφωνίας 5G μειώνεται σε σύγκριση με τα δίκτυα 3G και 4G, γεγονός που καθιστά απαραίτητο ένα πιο πυκνό δίκτυο κεραιών. Προκειμένου να παρέχεται επαρκής, συνεχής και σταθερή κάλυψη, αναμένεται ότι θα υπάρχουν περισσότεροι πύργοι κινητής τηλεφωνίας, πιθανώς κάθε 100 έως 200 μέτρα, όπως για παράδειγμα σε στύλους φαναριών, σε κτίρια εντός οικοδομικών τετραγώνων, ακόμη και σε τοποθεσίες μέσα σε πυκνοκατοικημένα πολυώροφα κτίρια.
4. Η απαίτηση για πρόσθετες κεραιές, αναμφίβολα εγείρει ερωτήματα για το πώς αλλοιώνεται αισθητικά ο αστικός χώρος, καθώς και ψυχολογικές ανησυχίες για τη νέα τεχνολογία και τις πιθανές επιπτώσεις της στη δημόσια υγεία.

2.3 Ιστορία του τεμαχισμού δικτύου

Η ιστορία του τεμαχισμού δικτύου εντοπίζεται στα τέλη της δεκαετίας του '60 με την εισαγωγή των αντίστοιχων εννοιών (slice, «φέτα») στον τομέα της δικτύωσης. Η διεργασία αυτή ορίστηκε από το Next Generation Mobile Network (NGMN) ως ένα λογικό από άκρη σε άκρη (end-to-end) δίκτυο που τρέχει σε κοινή υποδομή, με ανεξάρτητο έλεγχο και διαχείριση. Η πρώτη περίπτωση τεμαχισμού δικτύου κατέστη δυνατή από δίκτυα επικάλυψης, τα οποία

συγχώνευσαν ανόμοιους πόρους δικτύου σε εικονικά δίκτυα χρησιμοποιώντας μια κοινή υποδομή. Ωστόσο, δεν διέθεταν κάποιον μηχανισμό που θα μπορούσε να επιτρέψει τη δυνατότητα προγραμματισμού τους.

Στις αρχές της δεκαετίας του 2000, το PlanetLab εισήγαγε ένα πλαίσιο εικονικοποίησης που επέτρεψε σε ομάδες χρηστών να προγραμματίσουν λειτουργίες δικτύου προκειμένου να αποκτήσουν απομονωμένες και συγκεκριμένες εφαρμογές. Η έλευση των τεχνολογιών των δικτύων βασισμένα σε λογισμικό (SDN: Software Defined Networks) το 2009 επέκτεινε περαιτέρω τις δυνατότητες προγραμματισμού τους, μέσω ανοιχτών διεπαφών οι οποίες κατέστησαν δυνατή τη δημιουργία πλήρως διαμορφώσιμων και επεκτάσιμων τεμαχίων δικτύου.

Ο τύπος του δικτύου που χρησιμοποιήθηκε στα προηγούμενα δίκτυα κινητής τηλεφωνίας (2G, 3G και 4G) δεν είναι πλέον κατάλληλος για την αποτελεσματική αντιμετώπιση ενός μοντέλου αγοράς που αποτελείται από πολύ διαφορετικές εφαρμογές, όπως εξαιρετικά αξιόπιστη επικοινωνία τύπου μηχανής, χαμηλής καθυστέρησης επικοινωνία και βελτιωμένη παράδοση περιεχομένου κινητής ευρυζωνικότητας. Η νέα τεχνολογία καθιστά δυνατή την παροχή «φετών» κατά παραγγελία για ένα ευρύ φάσμα εφαρμογών, επιτρέποντας στους χειριστές να ανταποκρίνονται στις απαιτήσεις των εφαρμογών που εξυπηρετούνται από το 5G με ευελιξία και αποτελεσματικότητα (Barakabitze et al., 2020).

2.4 Εφαρμογές του τεμαχισμού δικτύου

Ο τεμαχισμός δικτύου καθιστά εφικτή τη δημιουργία εικονικών δικτύων που έχουν τα κατάλληλα χαρακτηριστικά γνωρίσματα για να εξυπηρετήσουν σκοπούς με ποικίλους βαθμούς ανεξαρτησίας, ανοίγοντας ταυτόχρονα νέες επιχειρηματικές προοπτικές στους παρόχους υπηρεσιών επικοινωνίας για ένα ευρύ φάσμα περιπτώσεων χρήσης. Επιπλέον, δίνει τη δυνατότητα στους χειριστές δικτύου να ρυθμίσουν την υποδομή ή τμήματα αυτής, για μια συγκεκριμένη εφαρμογή που θα διατίθεται κατόπιν ζήτησης ως ξεχωριστό δίκτυο με ιδιαίτερα χαρακτηριστικά, όπως εγγυημένη απόδοση δεδομένων ή ακριβείς περιορισμούς όσον αφορά στις τιμές της καθυστέρησης.

Οι εφαρμογές που επωφελούνται από τη χρήση διαφόρων τμημάτων της τεχνολογίας περιλαμβάνουν έξυπνα αυτοκίνητα, επικοινωνίες μεταξύ μηχανών και κινητές ευρυζωνικές συνδέσεις. Ενώ ορισμένες εφαρμογές χρειάζονται ελάχιστο λανθάνοντα χρόνο, άλλες θέλουν μεγαλύτερες ταχύτητες και άλλες χρειάζονται πρόσβαση σε υπολογιστικούς πόρους αιχμής.

Ένας χειριστής δικτύου 5G μπορεί να παρέχει εξειδικευμένες λύσεις σε συγκεκριμένες επιχειρήσεις διαιρώντας το δίκτυο σε πολλά τμήματα που δίνουν προτεραιότητα σε διαφορετικούς πόρους.

Επιπλέον, ο τεμαχισμός ενισχύει τη συνέχεια της υπηρεσίας διευκολύνοντας την αποτελεσματικότερη περιαγωγή δικτύου, ενώ επιτρέπει ταυτόχρονα σε ένα δίκτυο υποδοχής να δημιουργήσει ένα βελτιστοποιημένο εικονικό δίκτυο που μιμείται τα χαρακτηριστικά του οικιακού δικτύου μιας συσκευής περιαγωγής ή να δημιουργήσει ένα εικονικό δίκτυο που εκτελείται σε φυσική υποδομή και που εκτείνεται σε πολλά τοπικά ή εθνικά δίκτυα.

Πολλά σενάρια, στο όχι τόσο μακρινό μέλλον, δείχνουν πώς μπορεί να μοιάζει η 5G κοινωνία στην πράξη (Prime Group, 2024; Remmert, 2020):

- **Συνδεδεμένα αυτοκίνητα:** Τα αυτοκίνητα που επικοινωνούν μεταξύ τους είναι ιδιαίτερα ασφαλή και εξαιρετικά αυτοματοποιημένα. Χάρη στους ειδικούς αισθητήρες, τα αυτόνομα οχήματα μπορούν να εντοπίζουν τους κινδύνους από πολύ νωρίς και να ανταλλάσσουν αυτές τις πληροφορίες μεταξύ τους σε πραγματικό χρόνο, επιτρέποντας την αποφυγή ατυχημάτων, ενώ μειώνεται ταυτόχρονα η κυκλοφοριακή συμφόρηση.
- **Έξυπνο εργοστάσιο:** Η συνεχής ανταλλαγή πληροφοριών μεταξύ των μηχανών σε μια εγκατάσταση παραγωγής είναι πλέον πραγματικότητα. Ο αποτελεσματικός έλεγχος μεμονωμένων μηχανημάτων στη βιομηχανική κατασκευή απαιτεί διασυνδέσεις μεταξύ των μηχανών σε μια συμπαγή αρχιτεκτονική και επομένως εξαιρετικά περίπλοκη μορφή. Η δομή αυτή μπορεί να δημιουργήσει εκατομμύρια ή ακόμη και δισεκατομμύρια μηνύματα κατάστασης (status messages), τα οποία καταγράφονται συνεχώς από αισθητήρες, μεταδίδονται και αναλύονται.
- **Απομακρυσμένες χειρουργικές επεμβάσεις:** Χάρη στην εξαιρετικά χαμηλή καθυστέρηση του 5G, οι χειρουργοί μπορούν να εκτελούν επεμβάσεις εξ αποστάσεως με ρομποτικά συστήματα, επιτρέποντας την άμεση παροχή εξειδικευμένης ιατρικής φροντίδας σε απομακρυσμένες περιοχές.
- **Φορητές συσκευές υγείας:** Οι φορητές συσκευές (wearables) μπορούν να παρακολουθούν ζωτικές τιμές του ασθενή/χρήστη σε πραγματικό χρόνο και να μεταδίδουν δεδομένα στους παρόχους υγείας, βελτιώνοντας την παρακολούθηση και τη διάγνωση ασθενειών.

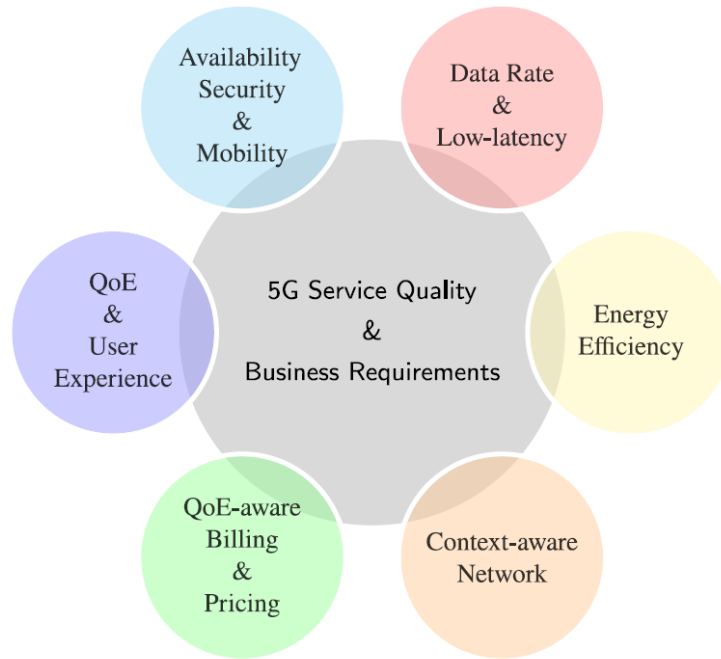
- **Διαχείριση κυκλοφορίας:** Χρήση αισθητήρων και καμερών για την παρακολούθηση της κυκλοφορίας και τη δυναμική διαχείριση των φωτεινών σηματοδοτών για την αποφυγή συμφόρησης.
- **Δημόσια ασφάλεια:** Συστήματα επιτήρησης με υψηλή ευκρίνεια και ανάλυση δεδομένων σε πραγματικό χρόνο για την άμεση ανταπόκριση σε περιστατικά και την πρόληψη εγκλημάτων.
- **Έξυπνα κτίρια:** Διαχείριση ενεργειακής απόδοσης και αυτοματοποίηση λειτουργιών όπως ο φωτισμός, ο κλιματισμός και τα συστήματα ασφαλείας μέσω δικτυωμένων αισθητήρων και συσκευών.
- **Γεωργία ακριβείας:** Χρήση δικτυωμένων συσκευών για την παρακολούθηση καλλιεργειών και εδάφους, την αυτοματοποίηση της άρδευσης και τη βελτίωση των γεωργικών αποδόσεων.
- **Επαυξημένη και εικονική πραγματικότητα (AR/VR):** Βελτιωμένες εμπειρίες gaming, εκπαιδευτικά εργαλεία και ψυχαγωγικές εφαρμογές που απαιτούν υψηλό bandwidth και χαμηλή καθυστέρηση.
- **Ζωντανή μετάδοση βίντεο 8K:** Υψηλής ποιότητας ζωντανές μεταδόσεις αθλητικών γεγονότων, συναυλιών και άλλων εκδηλώσεων με ελάχιστη καθυστέρηση.
- **Αυτόνομα ρομπότ αποθήκης:** Τα ρομπότ μπορούν να λειτουργούν και να επικοινωνούν μεταξύ τους για την αποτελεσματική διαχείριση των αποθεμάτων και την εκτέλεση παραγγελιών.
- **Παρακολούθηση εφοδιαστικής αλυσίδας:** Δικτυωμένες συσκευές και αισθητήρες για την παρακολούθηση των προϊόντων, από την παραγωγή έως την παράδοση, σε πραγματικό χρόνο.
- **Έξυπνες συσκευές σπιτιού:** Οικιακές συσκευές όπως ψυγεία, φούρνοι και συστήματα ασφαλείας που μπορούν να ελεγχθούν και να παρακολουθηθούν απομακρυσμένα.
- **Προσωπικοί βοηθοί:** Προηγμένοι προσωπικοί βοηθοί που χρησιμοποιούν την τεχνητή νοημοσύνη για να παρέχουν βελτιωμένες υπηρεσίες στους χρήστες.

2.5 Επισκόπηση αρχιτεκτονικής και βασικές έννοιες

Η κύρια ιδέα του τεμαχισμού δικτύου αφορά στην αρχιτεκτονική κατάτμηση του δικτύου σε πολλαπλά λογικά και ανεξάρτητα διαμορφωμένα δίκτυα, με σκοπό να καλυφθούν αποτελεσματικά οι απαιτήσεις των διάφορων υπηρεσιών. Για την επίτευξη αυτού του στόχου χρησιμοποιούνται διάφορες τεχνικές, όπως οι λειτουργίες δικτύου (Network Functions), η εικονικοποίηση (Virtualization) και η ενορχήστρωση (Orchestration).

Η ενορχήστρωση είναι μια διαδικασία που επιτρέπει τον συντονισμό όλων των διαφορετικών στοιχείων του δικτύου (φυσική υποδομή δικτύου, υποδομή νέφους, δίκτυο πυρήνα, υπηρεσίες δικτύου, συσκευές τερματικού, διαθέσιμοι πόροι, ασφάλεια), ώστε να εξασφαλιστεί η ομαλή και αποδοτική λειτουργία του. Στο πλαίσιο αυτό, η SDN τεχνολογία χρησιμοποιείται για να επιτρέψει μια δυναμική και ευέλικτη διαμόρφωση των «τεμαχίων» (Ordonez-Lucena et. al., 2017).

Ως εκ τούτου, ο τεμαχισμός δικτύου αναδεικνύεται ως βασική τεχνική στα δίκτυα 5G, επιτρέποντας την κάλυψη διαφόρων και ενδεχομένως αντιφατικών απαιτήσεων ποιότητας υπηρεσίας (QoS: Quality of Service) μέσω μιας ενιαίας φυσικής υποδομής δικτύου. Οι διάφορες εφαρμογές 5G έχουν διαφορετικές απαιτήσεις απόδοσης. Ο τεμαχισμός δικτύου διαφέρει σημαντικά από τις παραδοσιακές προσεγγίσεις QoS, καθώς επιτρέπει τη δημιουργία εικονικών δικτύων από άκρο σε άκρο, τα οποία περιλαμβάνουν λειτουργίες υπολογιστών, αποθήκευσης και δικτύωσης. Οι υφιστάμενες προσεγγίσεις QoS παρέχουν μερικές μόνο λύσεις που περιορίζονται σε ένα υποσύνολο λειτουργιών, σε αντίθεση με τον ολοκληρωμένο τεμαχισμό ενός δικτύου. Τέλος, είναι σημαντικό να εξεταστούν οι απαιτήσεις τόσο από την οπτική του δικτύου όσο και από αυτή των τελικών χρηστών (Barakabitze et al., 2020).



Εικόνα 6: Ποιότητα υπηρεσίας 5G και επιχειρηματικές απαιτήσεις

Πηγή: Barakabitze et al., 2020

Παρά το γεγονός ότι υπάρχουν πολλές προτάσεις για αρχιτεκτονικές τεμαχισμού δικτύου, μπορεί να οριστεί μια γενική αρχιτεκτονική που ενοποιεί τα κοινά στοιχεία όλων των λύσεων σε ένα ευρύ πλαίσιο.

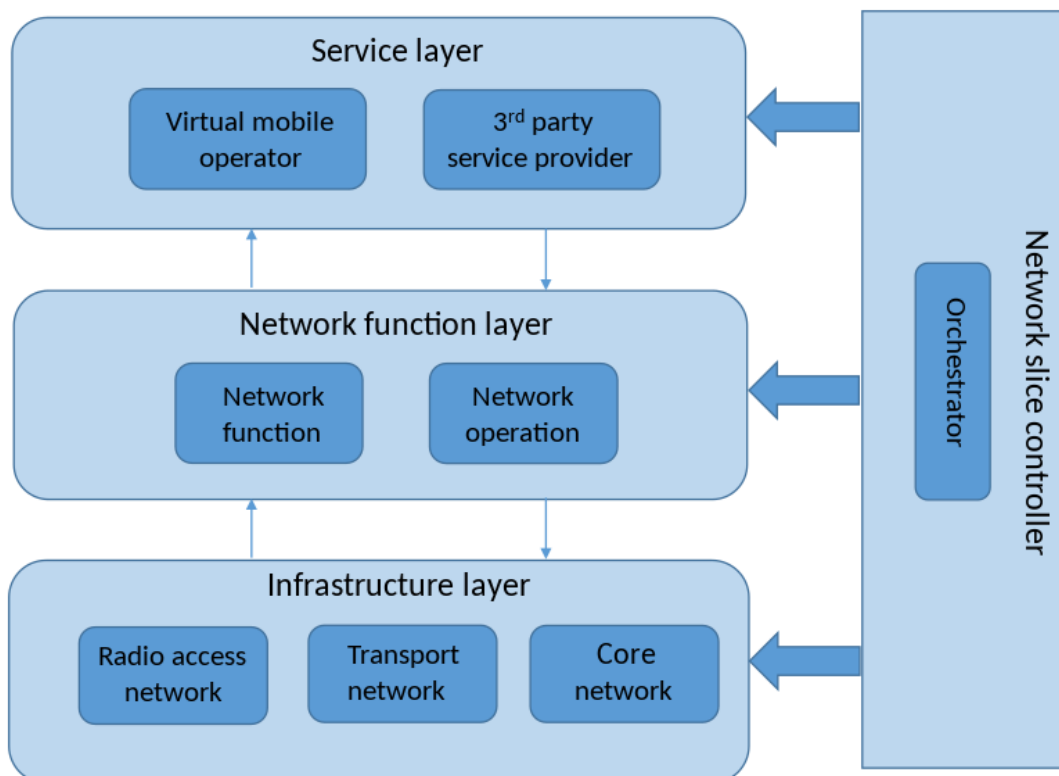
Από μια υψηλού επιπέδου προοπτική, η αρχιτεκτονική τεμαχισμού δικτύου μπορεί να θεωρηθεί ότι αποτελείται από δύο κεντρικά τμήματα: το ένα αφιερωμένο στην υλοποίηση των «τεμαχίων» και το άλλο στη διαχείριση και διαμόρφωση αυτών.

- Τρία επίπεδα συνθέτουν την πολυεπίπεδη αρχιτεκτονική του **πρώτου** τμήματος: το επίπεδο υποδομής ή πόρων, το επίπεδο λειτουργιών δικτύου και το επίπεδο υπηρεσίας. Με συγκεκριμένους ρόλους, καθένα από αυτά τα επίπεδα προσθέτει στη δημιουργία και στον καθορισμό των «φετών».
- Σχεδιασμένο ως κεντρικό αντικείμενο δικτύου, που συνήθως αναφέρεται ως ελεγκτής τεμαχίων, το **δεύτερο** στοιχείο συντονίζει αποτελεσματικά τη συνύπαρξη διαφόρων "slices" παρακολουθώντας και διαχειρίζοντάς τις ενέργειες μεταξύ των τριών αρχιτεκτονικών στρωμάτων.

2.6 Επίπεδα του τεμαχισμού δικτύου

Η σύγχρονη έρευνα στον τομέα του τεμαχισμού δικτύου 5G επικεντρώνεται σε τρία κύρια επίπεδα: στο επίπεδο υπηρεσίας, στο επίπεδο λειτουργίας δικτύου και στο επίπεδο υποδομής. Το επίπεδο υπηρεσίας (Service layer) περιλαμβάνει την παροχή διακριτών υπηρεσιών προσαρμοσμένων στις ανάγκες διαφορετικών χρηστών και εφαρμογών. Το επίπεδο λειτουργίας δικτύου (Network function layer) ασχολείται με τη διαχείριση και τη λειτουργία των επιμέρους δικτυακών λειτουργιών, εξασφαλίζοντας την ομαλή ενσωμάτωσή τους. Τέλος, το επίπεδο υποδομής (Infrastructure layer) αφορά στους φυσικούς πόρους και στις υποδομές που χρησιμοποιούνται για την υποστήριξη των ανωτέρω επιπέδων, διασφαλίζοντας την απόδοση και την αξιοπιστία του δικτύου.

Τα παραπάνω απεικονίζεται στην παρακάτω αποτύπωση:



Εικόνα 7: Γενικό πλαίσιο που αντιπροσωπεύει τις 5G αρχιτεκτονικές προτάσεις (επίπεδα τεμαχισμού δικτύου)

Πηγή: Wikipedia, 2024

Πιο αναλυτικά στοιχεία για καθένα από αυτά τα επίπεδα παρατίθενται στις επόμενες παραγράφους (Foukas et al, 2017; Wikipedia, 2024):

- **Επίπεδο Υπηρεσίας (Service Layer):** Οι διάφοροι οργανισμοί που εμπλέκονται στη διαμόρφωση και στη διαχείριση ενός 5G δικτύου, όπως οι φορείς εκμετάλλευσης εικονικών δικτύων κινητής τηλεφωνίας (MVNO: Mobile Virtual Network Operators) και οι τρίτοι πάροχοι υπηρεσιών που χρησιμοποιούν το υποκείμενο φυσικό δίκτυο, συνδέονται απευθείας με το επίπεδο υπηρεσιών. Η κάθε υπηρεσία αναπαρίσταται ρητά ως παρουσία υπηρεσίας, οπότε αυτό το επίπεδο παρέχει μια ομοιόμορφη άποψη των απαιτήσεων της καθεμιάς από αυτές. Αυτές οι παρουσίες ενσωματώνουν όλες τις απαραίτητες προδιαγραφές του δικτύου σε μορφή απαιτήσεων SLA (Service Level Agreement).
- **Επίπεδο λειτουργίας δικτύου (Network Function Layer):** Κάθε τμήμα δικτύου δημιουργείται από αυτό το επίπεδο σύμφωνα με τα αιτήματα παρουσίας υπηρεσίας που προέρχονται από το ανώτερο επίπεδο. Αποτελείται από μια συλλογή λειτουργιών δικτύου με σαφώς καθορισμένες συμπεριφορές και διεπαφές. Πέρα από την αρχιτεκτονική εικονικού δικτύου, ένας αριθμός λειτουργιών δικτύου είναι στρωμένοι και συζευγμένοι για να παρέχουν μια παρουσία από άκρο σε άκρο που αντιστοιχεί στις δυνατότητες που έχει ζητήσει η υπηρεσία. Οι λειτουργίες δικτύου διαμορφώνονται μέσω μιας σειράς ενεργειών που επιτρέπουν τον έλεγχο ολόκληρου του κύκλου ζωής τους, από την τοποθέτηση κατά τη δημιουργία ενός τεμαχίου έως την απόσυρση με τον τερματισμό της δυνατότητας.

Η ίδια λειτουργία δικτύου μπορεί να κοινοποιηθεί ταυτόχρονα σε πολλά τμήματα για να βελτιωθεί η αποδοτικότητα των πόρων, ωστόσο αυτό συνοδεύεται από αύξηση της πολυπλοκότητας της διαχείρισης του δικτύου. Αν και θα μπορούσε να διευκολύνει τις διαδικασίες διαμόρφωσης, η αντιστοίχιση μεταξύ της κάθε λειτουργίας δικτύου και της λειτουργίας του τεμαχίου θα μπορούσε να οδηγήσει σε αναποτελεσματική και σπάταλη χρήση των πόρων.

- **Επίπεδο Υποδομής (Infrastructure Layer):** Αυτό το επίπεδο αντιπροσωπεύει την πραγματική τοπολογία του φυσικού δικτύου, περιλαμβάνοντας μια σειρά στοιχείων του, όπως: το δίκτυο ραδιοπρόσβασης, το δίκτυο μεταφορών και το δίκτυο πυρήνα. Σε αυτό το επίπεδο παρέχονται οι φυσικοί πόροι που συνθέτουν το κάθε τεμάχιο. Οι διαθέσιμοι πόροι περιλαμβάνουν κέντρα δεδομένων, δρομολογητές και σταθμούς βάσης, οι οποίοι εξασφαλίζουν την απαιτούμενη χωρητικότητα αποθήκευσης, υπολογιστικής ισχύος και εύρους ζώνης της ραδιοπρόσβασης.

Το τμήμα δικτύου αποτελείται από λειτουργικά μπλοκ, τα οποία μπορούν να παρέχονται από διαφορετικούς προμηθευτές (infrastructure vendors), προσφέροντας ευελιξία και ανεξαρτησία στην επιλογή εξοπλισμού και λύσεων.

- **Ελεγκτής Τεμαχίου Δικτύου (Network Slice Controller):** Προκειμένου να διαχειρίζονται τα αιτήματα δημιουργίας των τεμαχίων με συνέπεια, ο ελεγκτής του δικτύου λειτουργεί ως εντοπιστής, συνδέοντας τις διαφορετικές λειτουργίες κάθε επιπέδου. Καθιστά τη δημιουργία δικτυακών «φετών» μια γρήγορη και εύκολη διαδικασία και με εξαιρετική ευελιξία, επιτρέπει την αλλαγή της διαμόρφωσής τους ανά πάσα στιγμή. Ο ελεγκτής είναι υπεύθυνος για τον καθορισμό των εικονικών πόρων, τη διαχείριση του κύκλου ζωής όλων των τμημάτων – στοιχείων του δικτύου και για τη διαχείριση υπηρεσιών από άκρο σε άκρο, έχοντας πάντοτε ως κρίσιμη παράμετρο τη διασφάλιση της απόκρισης στις αλλαγές των SLA απαιτήσεων.

Επιπλέον, μπορεί να αποτελείται από πολλούς εντοπιστές που επιβλέπουν ξεχωριστά ένα υποσύνολο λειτουργιών σε κάθε επίπεδο, λόγω της πολυπλοκότητας των εργασιών που εκτελούνται και προγραμματίζονται για διαφορετικούς λόγους.

Η απομόνωση είναι κρίσιμη παράμετρος για την ταυτόχρονη συνύπαρξη πολλαπλών τεμαχίων που διαμοιράζονται την ίδια υποδομή, χωρίς να επηρεάζεται η απόδοση του ενός από την απόδοση του άλλου. Αυτό ενισχύει την ασφάλεια και το απόρρητο καθενός από αυτά, περιορίζοντας τις επιπτώσεις επιθέσεων ή βλαβών και προστατεύοντας ταυτόχρονα τις ιδιωτικές πληροφορίες και τα δεδομένα που σχετίζονται με κάθε τεμάχιο.

2.7 Κύρια στοιχεία της αρχιτεκτονικής του 5G

Η αρχιτεκτονική των 5G δικτύων ενσωματώνει αρκετά κρίσιμα στοιχεία προκειμένου να παρέχει ανώτερη απόδοση, υψηλές ταχύτητες συνδεσιμότητας και μεγαλύτερη προσαρμοστικότητα. Αναλυτικά στοιχεία για καθένα από αυτά (Fakhouri et al., 2023):

1. **Τερματικός εξοπλισμός ή Εξοπλισμός χρήστη (UE: User Equipment):** Πρόκειται για τη συσκευή του τελικού χρήστη που συνδέεται στο δίκτυο και αφορά σε μια πληθώρα [π.χ. tablets που έχουν android λογισμικό vs apple και προέρχονται από διαφορετικούς κατασκευαστές] και σε μια ευρεία γκάμα συσκευών [wearable συσκευές, IOT, tablets, smartphones κ.λπ.] Το 5G επομένως θα πρέπει να είναι σε θέση να υποστηρίξει τόσο μια πληθώρα ίδιου τύπου συσκευών, που περιέχουν διαφορετικό λογισμικό, είναι διαφορετικού κατασκευαστή κ.λπ., όσο και μια ευρεία

γκάμα συσκευών (ετερογενείς συσκευές), να υποστηρίζει δηλαδή ένα ευρύ φάσμα συχνοτήτων για τις διάφορες αυτές συνδέσεις.

2. **Νέο 5G δίκτυο ραδιοεπικοινωνιών (NR: 5G New Radio):** Περιλαμβάνει τα gNodeBs (GNBs) που παρέχουν διασυνδεσιμότητα μεταξύ του εξοπλισμού του τελικού χρήστη και του πυρήνα του δικτύου, αξιοποιώντας τεχνολογίες όπως το massive MIMO (massive Multiple-Input Multiple-Output¹) και το beamforming² για την αύξηση της χωρητικότητας και της κάλυψης.
3. **Πυρήνας Δικτύου 5G (5G Core Network):** Λειτουργεί ως ο ενορχηστρωτής του δικτύου, εξαιρετικά εικονικοποιημένος και ευέλικτος, βασισμένος σε αρχιτεκτονική βασισμένη σε υπηρεσίες (SBA: Service-Based Architecture). Διαχειρίζεται κρίσιμες λειτουργίες, όπως η αυθεντικοποίηση, η διαχείριση της κινητικότητας και η διαχείριση της συνεδρίας.
4. **Τεμάχια Δικτύου (Network Slices):** Πρόκειται για τα λογικά απομονωμένα από άκρο σε άκρο (end-to-end) δίκτυα προσαρμοσμένα σε συγκεκριμένες υπηρεσίες ή εφαρμογές. Η διαίρεση των πόρων εξασφαλίζει ότι η αποτυχία σε ένα τεμάχιο δεν επηρεάζει τα άλλα, επιτρέποντας εξατομικευμένα χαρακτηριστικά απόδοσης όπως η καθυστέρηση και η ταχύτητα μεταφοράς δεδομένων. Έτσι στο slicing σε κάθε τεμάχιο μπορεί να του αποδίδονται διαφορετικές ρυθμίσεις οι οποίες επηρεάζουν την απόδοσή του. Π.χ. στο 5G που καλείται να υποστηρίξει κρίσιμα μηχανήματα, όπως εργαλεία για απομακρυσμένες χειρουργικές επεμβάσεις, θα αποδίδονται τέτοιες ρυθμίσεις ώστε να υπερτερεί σε ταχύτητα το δίκτυο, σε σχέση με τις υπηρεσίες μετάδοσης βίντεο.
5. **Ακροδικτυακή υπολογιστική ή υπολογιστική των παρυφών (Edge Computing)³:** Μεταφέροντας τις υπολογιστικές δυνατότητες πιο κοντά στους τελικούς χρήστες, μειώνεται η καθυστέρηση και βελτιώνεται η ταχύτητα και η αξιοποίηση του εύρους

¹ είναι μια μέθοδος για τον πολλαπλασιασμό της χωρητικότητας ενός ραδιοζεύκτη, χρησιμοποιώντας πολλαπλές κεραίες μετάδοσης και λήψης για την εκμετάλλευση της πολλαπλής διάδοσης

² εστιάζει στη στόχευση σήματος μεταξύ ενός πελάτη και ενός σημείου πρόσβασης, προκειμένου να βελτιώσει την εμπειρία του τελευταίου.

³ η διαδικασία της αποκέντρωσης των IT υποδομών και η τοποθέτησή τους στην πηγή των δεδομένων, δηλαδή στο «άκρο» του δικτύου.

ζώνης. Επίσης, βελτιώνεται η ιδιωτικότητα και η ασφάλεια, καθώς τα δεδομένα δεν χρειάζεται να διασχίζουν το δίκτυο.

6. **Δίκτυα βασισμένα στο λογισμικό (SDN: Software-Defined Networking):** Παρέχει ένα προγραμματιζόμενο επίπεδο ελέγχου, διαχωρίζοντας τις λειτουργίες ελέγχου και προώθησης του δικτύου. Το SDN βελτιώνει την ευελιξία και την προσαρμοστικότητα του δικτύου, επιτρέποντας την κεντρική διαχείριση της κυκλοφορίας.
7. **Καινοτόμες τεχνολογίες:** Το 5G βασίζεται σε καινοτόμες τεχνολογίες και στρατηγικές βελτίωσης σε σχέση με τις προηγούμενες γενιές, όπως είναι για παράδειγμα οι: eMBB, URLLC και mMTC.
 - i. **Ενισχυμένη κινητή ευρυζωνικότητα (eMBB: Enhanced Mobile Broadband):** Σχεδιασμένη για υψηλές ταχύτητες δεδομένων και μεγάλη περιοχή κάλυψης, υποστηρίζει σενάρια υψηλής ταχύτητας μεταφοράς δεδομένων, όπως HD video streaming και VR/AR εφαρμογές, με κορυφαίες ταχύτητες μέχρι 20 Gbps.
 - ii. **Υπερ-αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (URLLC: Ultra-Reliable Low-Latency Communications):** Υποστηρίζει εφαρμογές αποστολής με κρίσιμες απαιτήσεις αξιοπιστίας και χαμηλής καθυστέρησης, με τυπικές απαιτήσεις καθυστέρησης κάτω από 1 millisecond, ιδανική για αυτόνομα οχήματα, βιομηχανική αυτοματοποίηση και τηλεχειρουργική.
 - iii. **Μαζικές επικοινωνίες τύπου μηχανής (mMTC: massive Machine-Type Communications):** Εστιασμένη στην υποστήριξη μαζικών αναπτύξεων IoT, σχεδιάστηκε για να διαχειρίζεται υψηλή πυκνότητα συνδεδεμένων συσκευών, οι οποίες είναι κρίσιμες για λειτουργίες που βρίσκουν εφαρμογή στις έξυπνες πόλεις, στα έξυπνα σπίτια, στην παρακολούθηση του περιβάλλοντος και στην γεωργία.

Αυτά τα στοιχεία ορίζουν τις δυνατότητες των δικτύων 5G, επιτρέποντας την αντιμετώπιση μιας ποικιλίας περιπτώσεων χρήσης, εφαρμογών και υπηρεσιών, σχηματίζοντας ένα συνολικό, υψηλής απόδοσης δίκτυο.

2.8 Αρχιτεκτονική των δικτύων οριζόμενων από λογισμικό

Τα δίκτυα που καθορίζονται από λογισμικό (SDN: Software-Defined Networks) ακολουθούν μια αρχιτεκτονική δικτύου που στοχεύει στη μείωση των περιορισμών του υλικού, αφαιρώντας τις λειτουργίες χαμηλού επιπέδου από αυτό. Το SDN επιτρέπει την εκτέλεση αυτών των λειτουργιών σε ένα κεντρικό επίπεδο ελέγχου που βασίζεται σε λογισμικό που επικοινωνεί μέσω μιας API διεπαφής. Αυτό έχει ως αποτέλεσμα οι υπηρεσίες δικτύου να μην εξαρτώνται από το υποκείμενο υλικό και να μπορούν να προσφέρονται και να χρησιμοποιούνται ανεξάρτητα από τα συνδεδεμένα στοιχεία υλικού.

Για το 5G, το SDN μπορεί να χρησιμοποιηθεί ως πλαίσιο που επιτρέπει την αποτελεσματική διαχείριση και τη βελτιστοποίηση της μετάδοσης των δεδομένων. Αντί να στηρίζεται αποκλειστικά σε συγκεκριμένα και απομονωμένα στοιχεία δικτύου για λειτουργίες όπως ο έλεγχος πολιτικής, το 5G χρησιμοποιεί το SDN για να εκτελεί αυτές τις λειτουργίες σε κοινό υλικό. Αυτό σημαίνει ότι οι λειτουργίες που κάποτε απαιτούσαν ξεχωριστά εξειδικευμένα στοιχεία δικτύου μπορούν τώρα να εκτελούνται σε γενικότερα και κοινά υλικά υποδομής, καθιστώντας το δίκτυο πιο ευέλικτο και αποδοτικό.

Η βελτιωμένη απόδοση καθυστέρησης και η βέλτιστη χρήση εύρους ζώνης είναι μερικά από τα πλεονεκτήματα του SDN. Επιπλέον, το SDN επιτρέπει την αναδρομολόγηση της ροής δεδομένων σε σχεδόν πραγματικό χρόνο, ενισχύοντας σημαντικά την προστασία από διακοπές δικτύου. Αυτό συμβάλλει στην ανάπτυξη υπηρεσιών υψηλής διαθεσιμότητας, όπως είναι οι κρίσιμες επικοινωνίες⁴ (CriC: Critical Communications) (Abood et al., 2024; Magri et al., 2018).

2.9 Αρχιτεκτονική της εικονικοποίησης των δικτυακών λειτουργιών

Η εικονικοποίηση των δικτυακών λειτουργιών (NFV: Network Function Virtualization) αναφέρεται στη χρήση στοιχειωδών λειτουργιών δικτύου ως "δομικά στοιχεία" για τη δημιουργία κάθε τμήματος του δικτύου. Αυτή η τεχνολογία παρέχει μια αφηρημένη αναπαράσταση των φυσικών πόρων σε ένα ενοποιημένο και ομοιογενές σχήμα, επιτρέποντας

⁴ παρέχουν επικοινωνίες χαμηλής καθυστέρησης με μέγιστη καθυστέρηση 1 ms και απώλεια πακέτων το πολύ 1 πακέτο για κάθε 10.000, ικανοποιώντας ταυτόχρονα τις απαιτήσεις των υπηρεσιών που απαιτούν εξαιρετική αξιοπιστία.

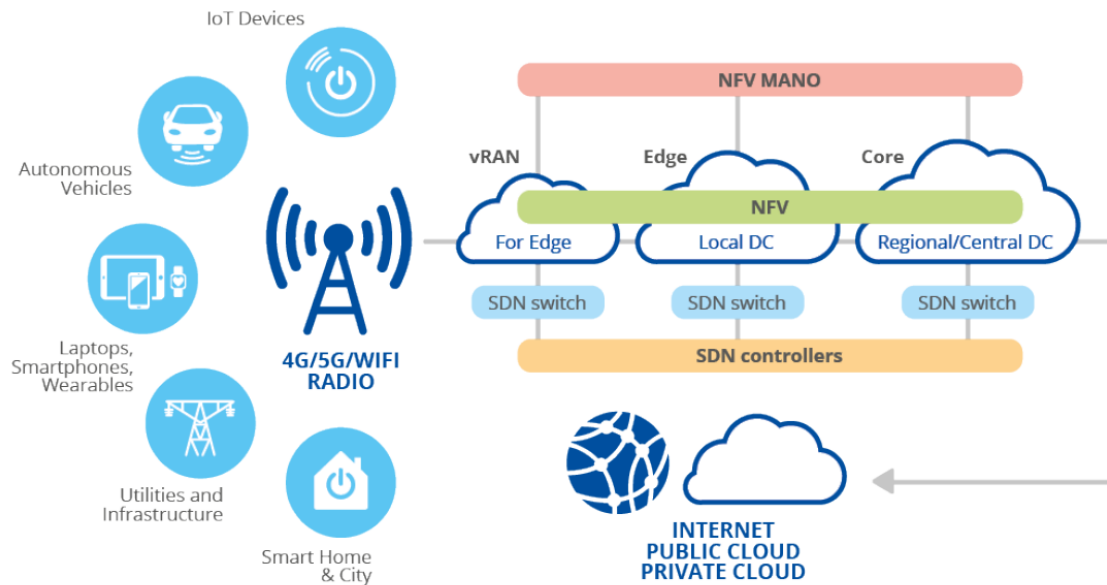
την αποσύνδεση των λειτουργιών του δικτύου από το υλικό στο οποίο εκτελούνται. Με την NFV, είναι δυνατή η επεκτάσιμη ανάπτυξη του δικτύου με τεμάχια, επιτρέποντας την ευέλικτη διαχείριση των πόρων.

Μαζί με το SDN, η NFV παίζει κρίσιμο ρόλο στην βέλτιστη απόδοση του 5G. Ο κύριος στόχος της NFV είναι να αποσυνδέσει το λογισμικό από το υλικό μέσω της χρήσης εικονικών μηχανών (VM: Virtual Machine). Αυτές οι εικονικές μηχανές εκτελούν διάφορες λειτουργίες δικτύου, όπως η κρυπτογράφηση των επικοινωνιών. Ένα πλεονέκτημα τους είναι η δυναμική τους φύση, που επιτρέπει την αυτόματη δημιουργία τους όποτε χρειάζεται, εξοικονομώντας κόστος και πόρους.

Η εικονικοποίηση των λειτουργιών επιτρέπει την ταχύτερη ανάπτυξή τους σε σύγκριση με τα εξειδικευμένα στοιχεία υλικού και λογισμικού. Στο πλαίσιο του 5G, η NFV υποστηρίζει την έννοια του τεμαχισμού δικτύου, που επιτρέπει τη δημιουργία πολλαπλών εικονικών δικτύων πάνω σε μια φυσική υποδομή. Αυτό παρέχει τη δυνατότητα διαίρεσης ενός φυσικού δικτύου σε πολλαπλά εικονικά δίκτυα, εξυπηρετώντας διάφορα δίκτυα ραδιοπρόσβασης (RANs).

Ένα ακόμα πλεονέκτημα της NFV είναι η δυνατότητα κλιμάκωσης των λειτουργιών με βάση διαφορετικά κριτήρια, όπως είναι για παράδειγμα το κόστος ή η κατανάλωση ενέργειας, προκειμένου να επιτευχθεί η βέλτιστη απόδοση (Papavassiliou, 2020; Yousaf et al., 2017).

Στην παρακάτω εικόνα απεικονίζονται οι αρχιτεκτονικές της εικονοποίησης των δικτύων και των δικτύων οριζόμενων από λογισμικό:



Εικόνα 8: Οι αρχιτεκτονικές SDN και NFV στα 5G δίκτυα

Πηγή: ENISA b., 2022

Είναι φανερό ότι οι δυο τεχνολογίες που εξετάστηκαν χρησιμοποιούνται σε διαφορετικές περιοχές του 5G δικτύου προκειμένου να επιτευχθεί η εικονοποίηση του δικτύου. Στον παρακάτω πίνακα συνοψίζονται οι διαφορές τους:

Software Defined Networking (SDN)		Network Function Virtualization (NFV)
Separate control and data, centralize control and programmability of network	Basic Concept	Relocate network functions from dedicated appliances to generic servers
Campus, data center / cloud	Target Location	Service provider network
Commodity servers and switches	Target Devices	Commodity servers and switches
Cloud orchestration and networking	Initial Applications	Routers, firewalls, gateways, CDN, WAN accelerators, SLA assurance
OpenFlow	New Protocols	None
Open Networking Foundation (ONF)	Formalization	ETSI NFV Working Group

Εικόνα 9: Διαφορές μεταξύ των SDN και NFV

Πηγή: Nayak, 2015

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ, ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ ΣΤΑ 5G ΔΙΚΤΥΑ

3.1 Η ανάγκη για ασφάλεια στα δίκτυα 5G: Προκλήσεις και προοπτικές στην ψηφιακή εποχή

Η εξέλιξη του Διαδικτύου έχει οδηγήσει στην ψηφιοποίηση όλων σχεδόν των επικοινωνιών, συμπεριλαμβανομένων των βασικών υπηρεσιών όπως η τραπεζική και η διακυβέρνηση. Αυτό προωθεί την οικονομική ανάπτυξη μέσω της αύξησης της αποτελεσματικότητας και της διασφάλισης της βέλτιστης απόδοσης. Η επιστροφή στις παραδοσιακές μεθόδους, όπου οι άνθρωποι περίμεναν στην ουρά για απλές συναλλαγές, όπως πληρωμές λογαριασμών και καταθέσεις, είναι αδιανόητη. Ωστόσο, η εξάρτηση από το Διαδίκτυο αποκάλυψε την ευπάθεια των κοινωνιών μας, με πολλαπλά παραδείγματα χρηματοπιστωτικών ιδρυμάτων και άλλων κρίσιμων υποδομών να έχουν υποστεί διακοπές στη λειτουργία τους, αποδεικνύοντας πόσο κρίσιμη είναι η ανάγκη του σχεδιασμού και της εκτέλεσης ενός πλαισίου προστασίας.

Είναι επιτακτική ανάγκη να διασφαλιστεί η ανθεκτικότητα των δικτύων 5G, τα οποία επηρεάζουν όχι μόνο τις ψηφιακές επικοινωνίες, αλλά και άλλους βασικούς τομείς όπως η ενέργεια, οι μεταφορές, η υγεία και οι τραπεζικές υπηρεσίες. Τα 5G δίκτυα υποστηρίζουν ασφαλείς λειτουργίες και μεταφέρουν ευαίσθητες πληροφορίες, προσφέροντας ευρυζωνική πρόσβαση και μαζική συνδεσιμότητα συσκευών μέσω του διαδικτύου των πραγμάτων. Παρά την πρόοδο που έχει συντελεστεί όμως, σε τεχνολογίες όπως είναι το cloud computing (υπολογιστικό νέφος), τα δίκτυα που καθορίζονται από λογισμικό και η εικονοποίηση των δικτυακών λειτουργιών, που είναι απαραίτητες στα δίκτυα 5^{ης} γενιάς, εξακολουθούν να υπάρχουν σημαντικές προκλήσεις ασφάλειας και ανησυχίες όσον αφορά στην ιδιωτικότητα και στο απόρρητο.

Η αύξηση της χρήσης έξυπνων συσκευών έχει οδηγήσει σε έκρηξη του κακόβουλου λογισμικού, το οποίο μπορεί να κρύβεται σε εφαρμογές και ιστοσελίδες. Το 5G δεν έχει σχεδιαστεί μόνο για την καταναλωτική αγορά αλλά και για την υποστήριξη της μαζικής κυκλοφορίας IoT, καθιστώντας το έναν στόχο επιθέσεων. Συνεπώς, η ασφάλεια στο 5G είναι κρίσιμη, αλλά και πολύπλοκη στον σχεδιασμό της.

Το 5G δίκτυο εκπροσωπεί ένα σημαντικό βήμα στις κινητές επικοινωνίες, με τους διαχειριστές δικτύων κινητής τηλεφωνίας, τους φορείς τυποποίησης, καθώς και τους

κατασκευαστές εξοπλισμού, να διαδραματίζουν καθοριστικό ρόλο στη διασφάλιση των επαρκών μηχανισμών προστασίας. Η ασφαλής ανάπτυξη των δικτύων 5G είναι βασική για την εθνική ασφάλεια και την εκμετάλλευση των πλεονεκτημάτων της νέας τεχνολογίας από επιχειρήσεις και πολίτες (Khan et al., 2019; Koca & Avcı, 2023).

3.2 Μηχανισμός ασφάλειας των SIM καρτών

Το 5G φέρνει μια πλήρως ανανεωμένη αρχιτεκτονική, η οποία περιλαμβάνει διαφορετική τεχνική λειτουργικότητα και δυνατότητα διαμόρφωσης της ραδιοπρόσβασης μέσω κατάλληλων διεπαφών, γεγονός που συνεπάγεται νέα, άγνωστα κενά ασφαλείας, παρά τις όποιες προετοιμασίες έχουν γίνει κατά τη φάση του σχεδιασμού του. Η αξιολόγηση αυτών των απειλών για την ασφάλεια είναι κρίσιμη τόσο για τους καταναλωτές, όσο και για όλο το οικοσύστημα και θα πρέπει να λαμβάνονται σοβαρά υπόψη, ώστε να προβλεφθεί ο σχεδιασμός και η υλοποίηση κατάλληλων μηχανισμών προστασίας. Οι μηχανισμοί ασφάλειας του 5G απαιτούν μια προσαρμοσμένη προσέγγιση, τόσο για κάθε ξεχωριστό περιβάλλον όσο και για κάθε διαφορετική περίπτωση χρήσης, ανάλογα πάντοτε με το επιχειρηματικό μοντέλο και τις απαιτήσεις των εμπλεκόμενων φορέων.

Οι νέες αρχιτεκτονικές και τεχνολογίες της υποδομής 5G, όπως η εικονικοποίηση των λειτουργιών του δικτύου, ο τεμαχισμός του δικτύου και η ακροδικτυακή υπολογιστική πολλαπλών προσβάσεων (MEC: Multi-Access Edge Computing) επηρεάζουν σημαντικά τον σχεδιασμό της ασφάλειας. Δεδομένου ότι η αξία των περιουσιακών στοιχείων καθορίζει το επίπεδο των τεχνικών απαιτήσεων, η ασφάλεια θα πρέπει να είναι ευέλικτη, επεκτάσιμη και προσαρμόσιμη για κάθε κατηγορία και περίπτωση χρήσης, τόσο εντός του δικτύου όσο και στις συσκευές που έχουν πρόσβαση σε αυτό.

Ένας από τους τομείς της ασφάλειας σχετίζεται με την έννοια της εξελισσόμενης μονάδας ταυτότητας συνδρομητή ή πιο σωστά της Παγκόσμιας Μονάδας Ταυτότητας Συνδρομητή (USIM: Universal Subscriber Identity Module) η οποία μπορεί να αντιμετωπίσει πολλά ζητήματα διαρροών στα τελικά σημεία επικοινωνίας, συμπεριλαμβανομένης της ασύρματης σύνδεσης συσκευών καταναλωτών και IoT. Είναι ζωτικής σημασίας να διαφυλάσσονται και να προστατεύονται τα πολύτιμα δεδομένα των ενδιαφερομένων μερών, όπως τα διαπιστευτήρια συνδρομής δικτύου εντός του εξοπλισμού του χρήστη, με τη βοήθεια εξειδικευμένων και προηγμένων λύσεων ασφαλείας SIM (Pauliac, 2020; Prasad et al., 2018).

3.3 Κατηγορίες και είδη επιθέσεων

Τα σύγχρονα πρότυπα ποιότητας περιλαμβάνουν πολλές νέες λειτουργίες που βελτιώνουν την απόδοση σε περίπτωση επιθέσεων, πέραν εκείνων που εφαρμόζονταν και στις προηγούμενες γενιές δικτύων, όπως είναι για παράδειγμα, η κατανεμημένη άρνηση υπηρεσίας (DDoS: Distributed Denial-of-Service) και η επίθεση ενδιάμεσου (MiTM: Man-in-the-middle). Η προστασία από επιθέσεις DDoS βασίζεται σε αλγόριθμους και προηγμένο λογισμικό προκειμένου να παρακολουθείται η εισερχόμενη κυκλοφορία σε έναν ιστότοπο. Η μη έγκυρη κυκλοφορία αποκλείεται, ενώ η νόμιμη κίνηση συνεχίζει να φιλτράρεται και να προωθείται στον ιστότοπο. Οι αλγόριθμοι έχουν σχεδιαστεί για να εντοπίζουν και να μετριάζουν τις επιθέσεις που στοχεύουν στο να κατακλύσουν ένα δίκτυο ή μια υπηρεσία με υπερβολική κίνηση, ώστε να καταστήσουν τον ιστότοπο ή την υπηρεσία μη διαθέσιμη στους νόμιμους χρήστες. Ωστόσο, συνήθως, προστατεύουν μόνο έναντι επιθέσεων μέχρι ενός συγκεκριμένου μεγέθους, μετρούμενου συνήθως σε Gbps (Gigabits per second) ή PPS (Packets per second).

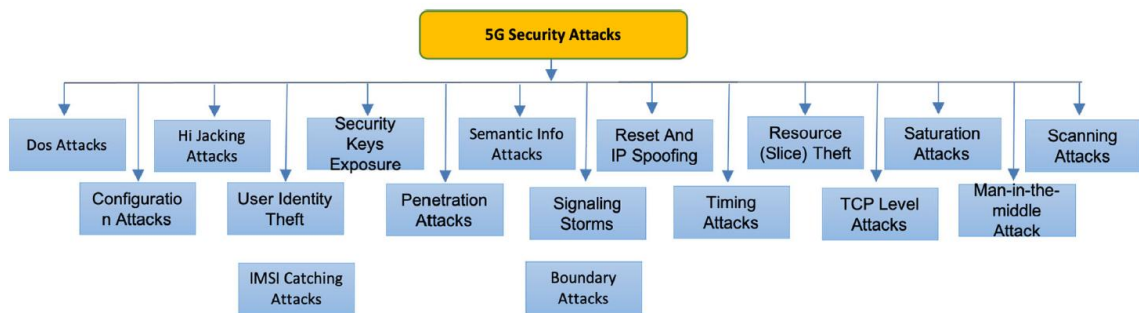
Η επίθεση MiTM συμβαίνει όταν ένας εισβολέας / μη εξουσιοδοτημένος χρήστης παρεμβάλλεται σε μια επικοινωνία μεταξύ δύο μερών, είτε για να παρακολουθεί, είτε για να πλαστοπροσωπεί έναν από τους συμμετέχοντες, καθιστώντας την ανταλλαγή πληροφοριών να φαίνεται ως μια σωστή, διαπιστευμένη διαδικασία. Αυτού του είδους η επίθεση στοχεύει στην κλοπή προσωπικών δεδομένων, συμπεριλαμβανομένων των αριθμών πιστωτικών καρτών, των πληροφοριών ενός λογαριασμού και των διαπιστευτηρίων σύνδεσης. Οι πελάτες διάφορων οικονομικών και τραπεζικών εφαρμογών, ιστοτόπων ηλεκτρονικού εμπορίου και άλλων ιστοσελίδων που απαιτούν τη σύνδεση του χρήστη αποτελούν συνήθως στόχο αυτών των επιθέσεων. Οι πληροφορίες μιας επίθεσης μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, όπως για παράδειγμα την κλοπή ταυτότητας, για μη εξουσιοδοτημένες οικονομικές συναλλαγές και για παράνομες αλλαγές κωδικού πρόσβασης.

Ένα από τα σημαντικότερα έγγραφα που συνοψίζουν τις τελευταίες τάσεις στο Διαδίκτυο και στον τομέα των κινητών επικοινωνιών είναι η ετήσια έκθεση ερευνών παραβίασης δεδομένων της Verizon⁵. Αυτή η έκθεση αποτελεί βάση για τον σχεδιασμό και την ενίσχυση της ασφάλειας. Η έκθεση κατηγοριοποιεί τα περιστατικά παραβίασης

⁵ Η Verizon Communications Inc. είναι ένας αμερικανικός πολυεθνικός όμιλος τηλεπικοινωνιών και μια εταιρική συνιστώσα του Dow Jones Industrial Average.

δεδομένων σε μοτίβα όπως: κατάχρηση εμπιστευτικών πληροφοριών και προνομιών (πρόσβαση μέσω αξιόπιστων φορέων), επιθέσεις διαδικτυακών εφαρμογών (κλεμμένα διαπιστευτήρια και εκμετάλλευση ευπαθειών), επιθέσεις άρνησης υπηρεσίας (DoS: Denial-of-Service και DDoS), κατασκοπεία στον κυβερνοχώρο (στοχευμένες εξωτερικές επιθέσεις), περιστατικά κακόβουλου λογισμικού, επιθέσεις στο σημείο πώλησης (POS: Point-of-Sale), συσκευές υποκλοπής καρτών πληρωμής, φυσική κλοπή δεδομένων και διάφορα άλλα σφάλματα που προκαλούν απώλεια δεδομένων.

Οι παραπάνω επιθέσεις είναι οι πιο κοινές, ωστόσο υπάρχει μια πληθώρα άλλων επιθέσεων που αντιμετωπίζουν τα δίκτυα 5G. Μια εκτενής κατηγοριοποίηση των επιθέσεων ασφαλείας και των συσκευών που είναι συνδεδεμένες σε αυτά απεικονίζεται στην παρακάτω εικόνα:



Εικόνα 10: Οι επιθέσεις στο 5G δίκτυο

Πηγή: Salahdine et al., 2022

Σημειώνεται ότι οι επιθέσεις αυτές διακρίνονται κυρίως σε επιθέσεις προς τον χρήστη και σε επιθέσεις προς το δίκτυο. Οι επιθέσεις προς τον χρήστη περιλαμβάνουν απειλές όπως ενεργοποίηση συσκευών, κατάληψη κόμβων και διαρροή προσωπικών δεδομένων. Οι επιθέσεις προς το δίκτυο περιλαμβάνουν έλεγχο συμφόρησης και επιθέσεις σηματοδότησης⁶.

3.3.1 Επιθέσεις προς τον χρήστη

- **Απειλή ενεργοποίησης συσκευής (Device trigger threat):** Περιλαμβάνει την απομίμηση του δικτύου για την αποστολή ερεθισμάτων σε συσκευές M2M (Machine to Machine) οδηγώντας σε σπατάλη ενέργειας.

⁶ Ο όρος αναφέρεται στη διαδικασία ή την τεχνική της επικοινωνίας και επιβολής κανόνων και πολιτικών στο δίκτυο.

- **Απειλή κατάληψης κόμβου (Node capture threat):** Δεδομένου ότι οι περισσότερες συσκευές εγκαθίστανται εξ αποστάσεως, η πρακτική αυτή συνεπάγεται επίσης, ότι οι εισβολείς αναλαμβάνουν τον πλήρη έλεγχο της συσκευής, εκμεταλλευόμενοι την απομακρυσμένη πρόσβαση.
- **Διαρροή προσωπικών δεδομένων (Privacy leaking):** Προκαλείται από τις ατέλειες στην ακεραιότητα των δεδομένων, επιτρέποντας την αποκάλυψη ευαίσθητων πληροφοριών.

3.3.2 Επιθέσεις προς το δίκτυο

- **Έλεγχος συμφόρησης (Congestion control threat):** Περιλαμβάνει τη χειραγώγηση των δεικτών προτεραιότητας πρόσβασης που αποδίδονται στις M2M (Machine to Machine) συσκευές, οδηγώντας τελικά σε αναποτελεσματικό έλεγχο της συμφόρησης.
- **Piggybacking:** Πρόκειται για τη μεταφορά κακόβουλων μικρών δεδομένων πάνω από μεγαλύτερα δεδομένα, επιτρέποντας την απαρατήρητη διείσδυση στο δίκτυο.
- **Επιθέσεις σηματοδοσίας (Signaling attacks):** Περιλαμβάνει την επανειλημμένη αίτηση άδειας πρόσβασης από τον επιτιθέμενο στο δίκτυο, γεγονός που αυξάνει το φορτίο σηματοδοσίας.
- **Κίνηση δικτύου αιχμής (Flash network traffic):** Πρόκειται για πρόκληση της αύξησης της κυκλοφορίας δικτύου που προκαλείται από τον μεγάλο αριθμό τελικών συσκευών και το νέο Internet of Nano Things (IoNT).
- **Ακεραιότητα επιπέδου χρήστη (User plane integrity):** Αφορά στην έλλειψη κρυπτογραφικής προστασίας ακεραιότητας στο επίπεδο δεδομένων.
- **Ασφάλεια διεπαφής ραδιοσυχνότητων (Security of radio interfaces):** Η επίθεση αυτή είναι δυνατό να προκύψει όταν το κλειδί κρυπτογράφησης της διεπαφής ραδιοπρόσβασης, αποστέλλεται μέσω μη ασφαλών δικτύων.
- **Επιβαλλόμενη ασφάλεια στο δίκτυο (Mandated security in the network):** Αφορά στη μη τήρηση των μέτρων ασφαλείας, λόγω των περιορισμών που επιβάλλουν οι παρεχόμενες υπηρεσίες.
- **Επιθέσεις άρνησης υπηρεσίας (DoS attacks):** Προκειμένου να αποτραπεί η επικοινωνία των νόμιμων χρηστών και να διακοπεί η πρόσβαση τους στους πόρους

του δικτύου, οι κακόβουλοι χρήστες υπερφορτώνουν το κανάλι με πακέτα παρεμβολών.

- **Επίθεση παρεμβολής (Jamming attack):** Οι κακόβουλοι χρήστες στέλνουν συνεχώς άχρηστα μηνύματα για να μπλοκάρουν τη νόμιμη μετάδοση.
- **Επίθεση υποκλοπής (Eavesdropping attack):** Σε αυτές τις επιθέσεις οι κακόβουλοι χρήστες αποκτούν πρόσβαση και υποκλέπτουν δεδομένα μέσω μη εξουσιοδοτημένων αναμεταδόσεων, χωρίς να τροποποιήσουν τα αρχικά μηνύματα.
- **Επίθεση πλαστογράφησης πιλότου (Pilot spoofing attack):** Ο επιτιθέμενος, προκειμένου να αποκτήσει πρόσβαση στο δίκτυο, προσποιείται ότι είναι νόμιμος χρήστης.
- **Επίθεση μεταμφίεσης (Masquerade attack):** Ο επιτιθέμενος χρησιμοποιεί ψεύτικες ταυτότητες για να αποκτήσει πρόσβαση σε μη εξουσιοδοτημένες συσκευές και δεδομένα.
- **Σιβυλλική επίθεση (Sybil attack):** Προκειμένου να καταλάβει το δίκτυο και να καταναλώσει το εύρος ζώνης, ο επιτιθέμενος δημιουργεί πολλαπλούς ψεύτικους κόμβους.
- **Επίθεση αποφυγής ανίχνευσης (Avoid detection attack):** Στοχεύει στην αποτροπή ανίχνευσης σφαλμάτων και προβλημάτων στο δίκτυο.
- **Επίθεση εισαγωγής (Injection attack):** Ο κακόβουλος χρήστης εισάγει ψεύτικα ή κακόβουλα μηνύματα στο σύστημα, χωρίς να εντοπιστεί από τους μηχανισμούς ασφαλείας. Αυτού του είδους οι επιθέσεις μπορούν να εκμεταλλευτούν αδυναμίες στο λογισμικό, επιτρέποντας στον επιτιθέμενο να εκτελέσει αυθαίρετο κώδικα ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες.
- **Επίθεση επανάληψης (Replay attack):** Οι κακόβουλοι χρήστες διαταράσσουν τη λειτουργία του συστήματος, στέλνοντας συνεχώς επαναλαμβανόμενα μηνύματα.
- **Επίθεση παραποίησης μηνύματος (Message spoofing attack):** Αποστολή ψευδών ή λανθασμένων πληροφοριών με σκοπό την παραπλάνηση και την παραποίηση των επικοινωνιών μεταξύ των οχημάτων. Αυτές οι επιθέσεις μπορούν να επηρεάσουν την απόδοση των συστημάτων και να οδηγήσουν σε επικίνδυνες καταστάσεις, όπως λανθασμένες αποφάσεις πλοήγησης ή συγκρούσεις.

- **Επίθεση σύγκρουσης απάντησης ή κεφαλίδας (Response or header collision attack):** Οι μη εξουσιοδοτημένοι χρήστες προκαλούν σύγκρουση στο δίκτυο στέλνοντας ψεύτικες απαντήσεις ή κεφαλίδες ταυτόχρονα με τις νόμιμες.
- **Επίθεση διατάραξης συγχρονισμού (Synchronization disruption attack):** Αποστολή ψευδών ή λανθασμένων χρονικών πληροφοριών με σκοπό τη διαταραχή του συγχρονισμού. Αυτού του είδους οι επιθέσεις μπορούν να προκαλέσουν σοβαρά προβλήματα στη λειτουργία των συστημάτων, όπως ασυγχρονισμό στις επικοινωνίες και ανακολουθίες στην εκτέλεση κρίσιμων διαδικασιών, οδηγώντας σε υποβάθμιση της απόδοσης ή ακόμη και σε αστοχίες.
- **Επίθεση πρόσβασης δικτύου (Network access attack):** Οι κακόβουλοι χρήστες αποκτούν μη εξουσιοδοτημένη πρόσβαση στο Ethernet και καταλαμβάνουν τον εξοπλισμό του δικτύου, όπως διακόπτες, κεντρικούς υπολογιστές και θύρες.
- **Επίθεση εμπιστευτικότητας κίνησης (Traffic confidentiality attack):** Οι κακόβουλοι χρήστες υποκλέπτουν την κίνηση μετά την απόκτηση πρόσβασης στο δίκτυο, με αποτέλεσμα την αποκάλυψη της τοπολογίας του δικτύου.
- **Επίθεση ακεραιότητας κίνησης (Traffic integrity attack):** Αλλοιώνουν την κίνηση, επηρεάζοντας την ακεραιότητά της. Οι επιθέσεις επανάληψης και κατάληψης συνεδρίας είναι παραδείγματα τέτοιων επιθέσεων.
- **Επίθεση ενδιάμεσου άνδρα (Man-in-the-middle attack):** Οι κακόβουλοι χρήστες ανακατευθύνουν την κίνηση του δικτύου προς κακόβουλους κόμβους, που έχουν προηγουμένως δημιουργήσει, για να την χειραγωγήσουν.
- **Επίθεση κακόβουλου λογισμικού (Malware attack):** Αυτή η επίθεση περιλαμβάνει τη δημιουργία κακόβουλου λογισμικού, το οποίο εγκαθίσταται στη συσκευή του θύματος χωρίς τη γνώση του, επιτρέποντας την πρόσβαση σε ευαίσθητα δεδομένα ή την εκτέλεση κακόβουλων δραστηριοτήτων.
- **Επίθεση ψευδαίσθησης (Illusion attack):** Οι κακόβουλοι χρήστες κατασκευάζουν ψεύτικα γεγονότα και περιστατικά προκειμένου να παραμορφώσουν τις πληροφορίες των αξιόπιστων πηγών και να εξαπατήσουν τα μέρη που έχουν πρόσβαση σε αυτές.
- **Επίθεση ψευδών πληροφοριών (Bogus information attack):** Οι κακόβουλοι χρήστες στέλνουν ψευδείς πληροφορίες, προκειμένου να παραπλανήσουν τους νόμιμους χρήστες να πάρουν λανθασμένες αποφάσεις.

- **Επίθεση χρονισμού (Timing attack):** Οι κακόβουλοι χρήστες προσθέτουν μια χρονική υστέρηση κατά την προώθηση των ληφθέντων σημάτων, καθυστερώντας με αυτό τον τρόπο την παραλαβή των πληροφοριών από τους νόμιμους χρήστες.
- **Επίθεση πλαστοπροσωπίας (Impersonation attack):** Η επίθεση αυτή περιλαμβάνει την παροχή ψεύτικης ταυτότητας για την εκτέλεση νόμιμων εργασιών ως εξουσιοδοτημένος χρήστης.
- **Επίθεση αεροπειρατείας (Hijacking attack):** Οι κακόβουλοι χρήστες παίρνουν τον έλεγχο της κινητής επικοινωνίας ή της συσκευής για την εκτέλεση κακόβουλων δραστηριοτήτων.
- **Επίθεση κακού διδύμου (Evil-Twin attack):** Η νόμιμη πρόσβαση ενός σημείου αντιγράφεται από ένα μη εξουσιοδοτημένο σημείο πρόσβασης, ώστε να προσελκύσει τη σύνδεση των χρηστών, επηρεάζοντας την ιδιωτικότητά τους και προκαλώντας ταυτόχρονα σοβαρή διαρροή δεδομένων.
- **Πλαστογράφιση ή δηλητηρίαση ARP (ARP spoofing / poisoning):** Είναι ένας τύπος παραβίασης σε δίκτυο υπολογιστών το οποίο βασίζεται στο πρωτόκολλο ARP (Address Resolution Protocol⁷). Ο κακόβουλος χρήστης μπορεί, μεταδίδοντας λανθασμένα πακέτα ARP, να μπερδέψει άλλους host ώστε να στείλουν τα πλαίσια δεδομένων τους σε άλλον υπολογιστή χωρίς να το αντιληφθούν.
- **Υπερχείλιση MAC (MAC flooding):** Είναι μια τεχνική που χρησιμοποιείται για να θέσει σε κίνδυνο την ασφάλεια των μεταγωγέων δικτύου. Η επίθεση λειτουργεί με το να γεμίζει τον πίνακα MAC (Media Access Control attack) του μεταγωγέα με ψευδείς εγγραφές, εξαναγκάζοντας τα νόμιμα περιεχόμενα να διαγραφούν. Αυτό προκαλεί τη συμπεριφορά υπερχείλισης, η οποία μπορεί να στείλει ευαίσθητες πληροφορίες σε τμήματα του δικτύου, όπου κανονικά δεν θα έπρεπε να φτάσουν.

Η Open Networking Foundation και η 3GPP εργάζονται συνεχώς για την ενσωμάτωση των νέων απαιτήσεων ασφαλείας στα δίκτυα 5G (Fakhouri et al., 2023; Hasan et al., 2021; Salahdine et al., 2022; Singh et al., 2023).

⁷ Πρόκειται για το πρωτόκολλο δικτύου που χρησιμοποιείται για την αντιστοίχιση μιας διεύθυνσης IP σε μια φυσική διεύθυνση MAC

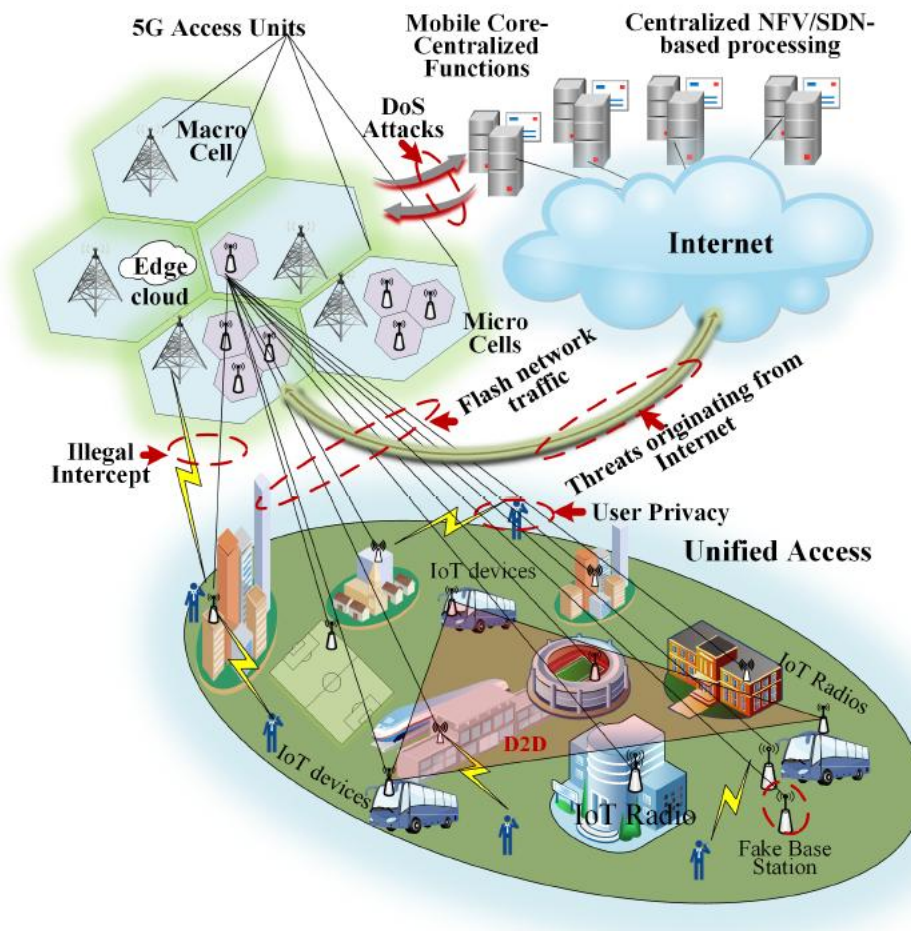
3.4 Βασικές προκλήσεις ασφαλείας στο 5G

Το 5G συνδέει κρίσιμες υποδομές που απαιτούν ενισχυμένη ασφάλεια προκειμένου να διασφαλιστεί όχι μόνο η λειτουργία των υποδομών του, αλλά και η ασφάλεια της κοινωνίας γενικότερα. Μια παραβίαση ασφαλείας, στα διαδικτυακά συστήματα τροφοδοσίας, για παράδειγμα, μπορεί να είναι καταστροφική για όλα τα ηλεκτρικά και ηλεκτρονικά συστήματα που εξαρτώνται από αυτά, ενώ κάποια από τα δεδομένα μπορεί να είναι κρίσιμα στη λήψη αποφάσεων και οι συνέπειες αλλοίωσης κατά τη μετάδοσή τους μπορεί να είναι σοβαρές ή ακόμη και επικίνδυνες. Συνεπώς, είναι απαραίτητο να διερευνώνται οι σημαντικές προκλήσεις ασφαλείας των δικτύων 5^{ης} γενιάς και να εξετάζονται οι πιθανές λύσεις που θα οδηγήσουν σε ασφαλή συστήματα και εφαρμογές που κάνουν χρήση αυτών των δικτύων.

Σύμφωνα με την οργάνωση NGMN, το 5G αντιμετωπίζει πολλές προκλήσεις. Καταρχάς, η ανάγκη για εξυπνότερα δίκτυα που να υποστηρίζουν την αυξημένη κίνηση δεδομένων και τις υψηλές απαιτήσεις χρηστών είναι επιτακτική. Επιπλέον, το 5G πρέπει να αντιμετωπίσει την πρόκληση της ενσωμάτωσης πολλαπλών τεχνολογιών ραδιοπρόσβασης σε ένα ενιαίο περιβάλλον δικτύου. Άλλες σημαντικές προκλήσεις περιλαμβάνουν την αποτελεσματική διαχείριση της κίνησης, αλλά και την προστασία της ιδιωτικότητας των χρηστών και της απαιτούμενης ασφαλείας για τις νέες υπηρεσίες που προσφέρονται μέσω του δικτύου.

Η ομάδα εργασίας 3GPP SA WG3 καθορίζει ενεργά τις απαιτήσεις ασφαλείας και απορρήτου, αναπτύσσοντας τις αρχιτεκτονικές και τα πρωτόκολλα ασφαλείας. Το Ίδρυμα Ανοικτής Δικτύωσης (Open Network Foundation) επιταχύνει την υιοθέτηση των SDN και NFV τεχνολογιών και δημοσιεύει τεχνικές προδιαγραφές, συμπεριλαμβανομένων των προδιαγραφών ασφαλείας για αυτές.

Οι αρχές σχεδιασμού του 5G που περιγράφονται από τον NGMN οργανισμό περιλαμβάνουν τη δημιουργία ενός κοινού συμπαγούς πυρήνα και την απλοποίηση των λειτουργιών και της διαχείρισης μέσω της ενσωμάτωσης νέων τεχνολογιών υπολογιστών και δικτύωσης. Η ασφάλεια αυτών των τεχνολογιών θα πρέπει να ικανοποιεί τις σχεδιαστικές αρχές του NGMN, συμπεριλαμβανομένων του κινητού νέφους, του SDN και του NFV, καθώς και των επικοινωνιακών συνδέσμων που χρησιμοποιούνται από ή μεταξύ αυτών των τεχνολογιών. Εξαιτίας των αυξανόμενων ανησυχιών για την ιδιωτικότητα των χρηστών, υπάρχουν και σημαντικές προκλήσεις που αφορούν στο απόρρητο (Ahmad et al.,2018).



Εικόνα 11: Το τοπίο απειλών στο 5G δίκτυο

Πηγή: Ahmad et al.,2018

Στην μελέτη τους οι Sullivan et al. (2021) ανέλυσαν τις προκλήσεις ασφαλείας στα 5G δίκτυα σύμφωνα με το OSI (Open Systems Interconnection) μοντέλο. Το μοντέλο αυτό είναι ένα θεωρητικό πλαίσιο που περιγράφει τις λειτουργίες ενός δικτύου υπολογιστών σε επτά διακριτά επίπεδα. Κάθε επίπεδο έχει συγκεκριμένες λειτουργίες και ευθύνες και το μοντέλο χρησιμοποιείται για την κατανόηση και το σχεδιασμό δικτύων, εξασφαλίζοντας ότι οι διάφορες τεχνολογίες και τα πρωτόκολλα συνεργάζονται αποτελεσματικά. Τα επτά επίπεδα του OSI μοντέλου είναι τα εξής:

1. Φυσικό Επίπεδο (Physical Layer)
2. Επίπεδο Συνδέσμου Δεδομένων (Data Link Layer)
3. Δικτυακό Επίπεδο (Network Layer)
4. Επίπεδο Μεταφοράς (Transport Layer)
5. Επίπεδο Συνεδρίας (Session Layer)

6. Επίπεδο Παρουσίασης (Presentation Layer)

7. Επίπεδο Εφαρμογών (Application Layer)

Παρακάτω παρατίθενται οι προκλήσεις ασφάλειας σε κάθε επίπεδο του μοντέλου αυτού, καθώς και οι προτεινόμενες λύσεις:

- **Φυσικό Επίπεδο:**

- Προκλήσεις: Παρεμβολές, φυσικές καταστροφές, επιθέσεις φυσικής πρόσβασης όπως τα jamming attacks.
- Λύσεις: Χρήση προστατευμένων καλωδίων, ανίχνευση και αποτροπή παρεμβολών, φυσική ασφάλεια των υποδομών.

- **Επίπεδο Συνδέσμου Δεδομένων**

- Προκλήσεις: Επιθέσεις όπως οι: ARP spoofing, MAC flooding και MiMT attack.
- Λύσεις: Ασφαλή πρωτόκολλα, χρήση VLANs και εφαρμογή 802.1X για έλεγχο ταυτότητας.

- **Δικτυακό Επίπεδο**

- Προκλήσεις: IP spoofing, DDoS επιθέσεις και επιθέσεις δρομολόγησης.
- Λύσεις: Χρήση ασφαλών πρωτοκόλλων δρομολόγησης, firewalls και φίλτρα DDoS.

- **Επίπεδο Μεταφοράς**

- Προκλήσεις: Port scanning, TCP SYN flooding⁸ και επιθέσεις session hijacking.
- Λύσεις: Χρήση κρυπτογράφησης, εφαρμογή firewalls και χρήση πρωτοκόλλων όπως TLS/SSL.

- **Επίπεδο Συνεδρίας**

⁸ Πρόκειται για μια μορφή επίθεσης άρνησης εξυπηρέτησης που στοχεύει την εξάντληση των πόρων ενός διακομιστή (server), εμποδίζοντάς τον να εξυπηρετήσει νόμιμες αιτήσεις. Η επίθεση εκμεταλλεύεται το πρωτόκολλο TCP (Transmission Control Protocol), το οποίο χρησιμοποιείται για τη δημιουργία συνδέσεων μεταξύ συσκευών σε ένα δίκτυο.

- Προκλήσεις: Επιθέσεις session hijacking και καταστροφή ή χειραγώγηση των συνεδριών.
- Λύσεις: Χρήση μοναδικών session keys, τακτική ανανέωση κλειδιών και χρήση ασφαλών συνεδριών.
- **Επίπεδο Παρουσίασης**
 - Προκλήσεις: Επιθέσεις δεδομένων όπως τα attacks on data encoding και επιθέσεις συμβιβασμού.
 - Λύσεις: Κρυπτογράφηση και αποκωδικοποίηση των δεδομένων και χρήση ασφαλών μορφών δεδομένων.
- **Επίπεδο Εφαρμογών**
 - Προκλήσεις: Malware, phishing και επιθέσεις στο λογισμικό.
 - Λύσεις: Ανίχνευση και αποτροπή κακόβουλου λογισμικού, εφαρμογή πρωτοκόλλων ασφαλείας στις εφαρμογές και τακτικές ενημερώσεις λογισμικού.

3.5 Προκλήσεις ασφαλείας στα κινητά σύννεφα

Τα συστήματα υπολογιστικού νέφους περιλαμβάνουν ποικίλους πόρους που διαμοιράζονται μεταξύ των χρηστών, γεγονός που καθιστά πιθανό ένας χρήστης να μεταφέρει κακόβουλο περιεχόμενο από τον έναν πόρο στον άλλο. Αυτή η ενέργεια μπορεί να καταστρέψει την απόδοση του συστήματος, να εξαναγκάσει στην κατανάλωση και στη χρήση περισσότερων πόρων και/ή να μην επιτρέψει σε άλλους χρήστες να πετύχουν την πρόσβαση στους δικούς τους πόρους. Στα δίκτυα υπολογιστικού νέφους πολλαπλών μισθωτών, όπου οι χρήστες διαχειρίζονται τη δική τους λογική ελέγχου, οι αλληλεπιδράσεις μπορεί να προκαλέσουν διενέξεις στις διαμορφώσεις του δικτύου. Το κινητό υπολογιστικό νέφος (MCC: Mobile Cloud Computing) εισάγει τις αρχές του cloud computing στο περιβάλλον του 5G, δημιουργώντας νέες ευπάθειες ασφαλείας που προκύπτουν από την τροποποιημένη αρχιτεκτονική και την υποδομή του τελευταίου. Η ανοιχτή αρχιτεκτονική του MCC και η ευελιξία των κινητών συσκευών δημιουργούν κενά ασφαλείας μέσω των οποίων οι κακόβουλοι χρήστες μπορούν να εξαπολύσουν απειλές και να παραβιάσουν την προστασία της ιδιωτικής ζωής.

Οι απειλές στο MCC κατηγοριοποιούνται σε τρία τμήματα: front-end, back-end και δικτυακές απειλές. Το front-end περιλαμβάνει την πλατφόρμα πελάτη που αποτελείται από το

κινητό τερματικό και τις εφαρμογές που απαιτούν πρόσβαση στις λειτουργίες του cloud. Οι απειλές σε αυτό το τμήμα περιλαμβάνουν φυσικές απειλές κατά της συσκευής, καθώς και απειλές που βασίζονται σε εφαρμογές, όπως κακόβουλο λογισμικό και spyware, που χρησιμοποιούνται για να παρεμποδίσουν ή για να διακόψουν τη λειτουργία των εφαρμογών του χρήστη ή για να συλλέξουν ευαίσθητες πληροφορίες.

Το back-end περιλαμβάνει τους διακομιστές cloud, τις εικονικές μηχανές, τα συστήματα αποθήκευσης δεδομένων, τον hypervisor (υπεύθυνος εποπτείας) και τα πρωτόκολλα που απαιτούνται για την παροχή υπηρεσιών υπολογιστικού νέφους. Οι απειλές ασφάλειας σε αυτή την πλατφόρμα στοχεύουν κυρίως στους διακομιστές που εξυπηρετούν το κινητό υπολογιστικό νέφος και μπορεί να περιλαμβάνουν αναπαραγωγή δεδομένων και επιθέσεις DoS μέσω HTTP (Hypertext Transfer Protocol) και XML (eXtensible Markup Language) γλώσσας.

Οι δικτυακές απειλές στοχεύουν στις τεχνολογίες ραδιοπρόσβασης (RAT: Radio Access Technology) που διασυνδέουν τις κινητές συσκευές με το cloud, όπως το Wi-Fi (Wireless Fidelity), το 4G LTE (Long Term Evolution) και άλλες. Αυτές οι επιθέσεις περιλαμβάνουν επιθέσεις DoS, Wi-Fi sniffing, πλαστοπροσωπία διευθύνσεων και κλοπή συνεδριών.

Το δίκτυο ραδιοπρόσβασης του υπολογιστικού νέφους (C-RAN: Cloud Radio Access Network) αποτελεί έναν σημαντικό τομέα ανάλυσης των προκλήσεων ασφάλειας στα κινητά σύννεφα. Το C-RAN μπορεί να αντιμετωπίσει τις αυξανόμενες ανάγκες σε συστήματα επικοινωνίας, ωστόσο αντιμετωπίζει προκλήσεις ασφάλειας που σχετίζονται με την εικονικοποίηση και την τεχνολογία υπολογιστικού νέφους, όπως η απειλή ενός κεντρικού σημείου αποτυχίας (Central Point of Failure threat)⁹. Επιθέσεις διείσδυσης όπου οι κυβερνοεγκληματίες εισχωρούν στο εικονικό περιβάλλον για να παρακολουθήσουν, να τροποποιήσουν ή να εκτελέσουν ρουτίνες λογισμικού χωρίς να εντοπίζονται, αποτελούν επίσης σημαντικές απειλές για το σύστημα (Cao et al., 2019; Rodriguez, 2015; Tian et al., 2017).

⁹ αναφέρεται στον κίνδυνο που προκύπτει όταν ένα σύστημα ή μια υπηρεσία εξαρτάται σε μεγάλο βαθμό από ένα μόνο σημείο ή πόρο για την λειτουργία του. Για παράδειγμα, σε ένα δίκτυο τηλεπικοινωνιών, ένας κεντρικός δρομολογητής ή μια κεντρική υπηρεσία ελέγχου μπορεί να θεωρηθεί κεντρικό σημείο αποτυχίας.

3.6 Προκλήσεις ασφαλείας στα SDN και NFV

Το SDN συγκεντρώνει τον έλεγχο του δικτύου σε ένα κεντρικό σημείο επιτρέποντας έτσι τον προγραμματισμό των δικτύων επικοινωνίας. Αυτό το χαρακτηριστικό, ωστόσο δημιουργεί ευκαιρίες για κενά ασφαλείας και επιθέσεις. Η κεντρικοποίηση του ελέγχου καθιστά το σύστημα ευάλωτο σε επιθέσεις DoS, ενώ η έκθεση κρίσιμων διεπαφών προγραμματισμού εφαρμογών σε μη ασφαλές λογισμικό μπορεί να καταστρέψει το δίκτυο.

Οι κανόνες ροής της διαδρομής των δεδομένων τίθενται και ελέγχονται από τον ελεγκτή SDN, ο οποίος γίνεται με αυτό τον τρόπο ταυτόχρονα ορατός και ευαίσθητος σε επιθέσεις τύπου DoS. Η συγκέντρωση ελέγχου μπορεί να οδηγήσει σε ένα κεντρικό μοναδικό σημείο αστοχίας για το δίκτυο, καθιστώντας το ευάλωτο με αυτό τον τρόπο σε «επιθέσεις κορεσμού». Επιπλέον, δεδομένου ότι πολλές λειτουργίες δικτύου ολοκληρώνονται μέσω των SDN εφαρμογών, κακόβουλες εφαρμογές θα μπορούσαν να αναπτυχθούν μέσω του ελεγκτή ώστε να προκαλέσουν σοβαρές βλάβες. Η ευελιξία και οι δυνατότητες επικοινωνίας των SDN εφαρμογών προσφέρουν πρόσφορο έδαφος στις κακόβουλες εφαρμογές, προκειμένου να εκμεταλλευτούν κατάλληλα τις ευκαιρίες και να οδηγήσουν το σύστημα σε δυσμενή αποτελέσματα, όπως διαρροές δεδομένων ή διακοπή της υπηρεσίας.

Το NFV, αν και είναι κρίσιμης σημασίας για τα δίκτυα επικοινωνίας 5^{ης} γενιάς, παρουσιάζει σημαντικές προκλήσεις ασφαλείας, όπως η διασφάλιση του απορρήτου, η ακεραιότητα, η αυθεντικότητα και η μη αποδοχή. Στα δίκτυα κινητής τηλεφωνίας, οι τρέχουσες πλατφόρμες NFV δεν παρέχουν επαρκή ασφάλεια, αλλά ούτε και το κατάλληλο επίπεδο απομόνωσης για τις εικονικές τηλεπικοινωνιακές υπηρεσίες. Μια βασική πρόκληση της δυναμικής φύσης των εικονικών λειτουργιών δικτύου (VNF: Virtual Network Function), είναι ότι μπορεί να οδηγήσει σε σφάλματα διαμόρφωσης και, κατά συνέπεια, σε παραβιάσεις ασφαλείας. Η πιο κρίσιμη πρόκληση είναι ότι, αν παραβιαστεί ο hypervisor, μπορεί να παραβιαστεί ολόκληρο το δίκτυο (Singh et al., 2023; Wang et al., 2015).

3.7 Προκλήσεις ασφάλειας στα κανάλια επικοινωνίας

Το 5G περιλαμβάνει ένα πολύπλοκο οικοσύστημα που ενσωματώνει πολλές και διαφορετικές συσκευές και υπηρεσίες, όπως είναι για παράδειγμα τα drones, ο εναέριος έλεγχος κυκλοφορίας, η εικονική πραγματικότητα βασισμένη στο cloud, τα συνδεδεμένα οχήματα, τα έξυπνα εργοστάσια, τα ρομποτικά συστήματα, οι μεταφορές και η υγειονομική περίθαλψη. Εξαιτίας αυτού, οι εφαρμογές απαιτούν ασφαλή συστήματα επικοινωνίας τα οποία θα πρέπει

να υποστηρίζουν συχνότερο έλεγχο ταυτότητας χρήστη (αυθεντικοποίηση) και ασφαλή ανταλλαγή ευαίσθητων δεδομένων. Σε όλα τα παραπάνω εμπλέκονται πλέον διάφοροι νέοι φορείς, όπως είναι για παράδειγμα οι πάροχοι δημόσιων υπηρεσιών, οι φορείς εκμετάλλευσης δικτύων κινητής τηλεφωνίας και οι πάροχοι υπολογιστικού νέφους. Σε αυτό το οικοσύστημα, απαιτούνται πολλαπλά επίπεδα ελέγχου ταυτότητας χρήστη ή μηχανής, τόσο στο επίπεδο πρόσβασης του δικτύου όσο και στο επίπεδο των υπηρεσιών, καθώς και συχνή πιστοποίηση μεταξύ των εμπλεκόμενων φορέων, μέσω έγκυρων ψηφιακών πιστοποιητικών.

Πριν από την εισαγωγή των 5G δικτύων, τα κινητά δίκτυα χρησιμοποιούσαν αποκλειστικά κανάλια επικοινωνίας βασισμένα σε GTP (GPRS Tunnelling Protocol) και IPsec (Internet Protocol Security) σήραγγες. Οι διεπαφές επικοινωνίας των προηγούμενων γενιών δικτύων, όπως είναι για παράδειγμα οι X2, S1, S6, και S7, απαιτούσαν σημαντική τεχνογνωσία από έναν εν δυνάμει επιτιθέμενο, καθώς αυτές χρησιμοποιούνταν μόνο στα δίκτυα κινητής τηλεφωνίας. Από την άλλη, τα δίκτυα 5G βασίζονται σε διεπαφές, οι οποίες δεν είναι τόσο κλειστές και περιορισμένες στην συγκεκριμένη τεχνολογία, αλλά, αντίθετα, είναι κοινές διεπαφές τύπου SDN. Αυτή η συμπερίληψη αυξάνει και το εύρος των πιθανών επιθέσεων.

Η επικοινωνία στα 5G δίκτυα που βασίζεται στην SDN τεχνολογία, μπορεί να κατηγοριοποιηθεί συνολικά σε τρία κανάλια: το κανάλι δεδομένων, το κανάλι ελέγχου και το κανάλι μεταξύ των ελεγκτών. Στα τρέχοντα SDN συστήματα, αυτά τα κανάλια προστατεύονται με τη χρήση των πρωτοκόλλων TLS (Transport Layer Security) και SSL (Secure Sockets Layer). Ωστόσο, οι συνεδρίες TLS/SSL είναι ιδιαίτερα ευάλωτες σε επιθέσεις που στοχεύουν άμεσα στο πρωτόκολλο διαδικτύου (IP: Internet Protocol), σε επιθέσεις σαρωτή SDN (SDN scanner attacks)¹⁰ ενώ στερούνται και ισχυρών μηχανισμών ελέγχου ταυτότητας (Ahmad et al., 2017; Salahdine et al., 2022; Sullivan et al., 2021).

¹⁰ Πρόκειται για επιθέσεις που στοχεύουν στην αναγνώριση και την εξερεύνηση δυνητικών ευπαθειών ή αδυναμιών σε δίκτυα που χρησιμοποιούν τεχνολογία SDN. Οι επιτιθέμενοι χρησιμοποιούν σαρωτές (scanners) για να εξετάσουν το δίκτυο και να εντοπίσουν ευπαθείς πόρους ή διεπαφές, που θα μπορούσαν να εκμεταλλευτούν για να εξαπολύσουν επιθέσεις.

3.8 Προκλήσεις απορρήτου στο 5G

Από την προοπτική του χρήστη, οι κύριες ανησυχίες σχετικά με το απόρρητο αφορούν στα δεδομένα, στην τοποθεσία και στην ταυτότητα. Οι περισσότερες εφαρμογές για έξυπνα κινητά (smartphones) απαιτούν πριν από την εγκατάσταση, την παροχή προσωπικών δεδομένων του χρήστη και οι προγραμματιστές που τα αναπτύσσουν ή οι εταιρείες που τις διανέμουν, σπάνια ενημερώνουν για τον τρόπο ή το μέσο αποθήκευσης, καθώς και τη χρήση τους.

Απειλές, όπως οι χρονικές επιθέσεις, οι επιθέσεις σημασιολογικής πληροφορίας και οι επιθέσεις στα όρια, στοχεύουν κυρίως στην αποκάλυψη της τοποθεσίας του χρήστη. Στο φυσικό επίπεδο¹¹, η ακριβής τοποθεσία του χρήστη μπορεί να διαρρεύσει μέσω αλγορίθμων επιλογής του σημείου πρόσβασης στα 5G δίκτυα. Οι επιθέσεις έναντι της διεθνής ταυτότητας κινητού του συνδρομητή (IMSI: International Mobile Subscriber Identity) μπορούν να αποκαλύψουν την ταυτότητα ενός χρήστη, καταγράφοντας το IMSI μέσω του εξοπλισμού του. Αυτές οι επιθέσεις μπορεί να πραγματοποιηθούν με τη δημιουργία ενός ψεύτικου σταθμού βάσης, ο οποίος αναγνωρίζεται από τον εξοπλισμό ως ο προτεινόμενος, οδηγώντας κακόβουλα τους συνδρομητές σε αυτόν.

Τα 5G δίκτυα περιλαμβάνουν πολλούς διαφορετικούς εμπλεκόμενους, όπως οι εικονικοί φορείς κινητής τηλεφωνίας, οι πάροχοι υπηρεσιών επικοινωνίας και οι πάροχοι υποδομών δικτύου, καθένας από τους οποίους έχει διαφορετικές προτεραιότητες για την ασφάλεια και το απόρρητο, δημιουργώντας προκλήσεις στον συγχρονισμό των πολιτικών απορρήτου. Σε όλες τις προηγούμενες γενιές δικτύων, οι πάροχοι κινητής τηλεφωνίας είχαν άμεση πρόσβαση και σαφή έλεγχο όλων των στοιχείων του συστήματος. Ωστόσο, στο 5G, οι πάροχοι χάνουν τον πλήρη έλεγχο, λόγω της εμπλοκής νέων φορέων. Αυτό μειώνει τη δυνατότητα των παρόχων δικτύων 5ης γενιάς να διασφαλίσουν πλήρως την ασφάλεια και το απόρρητο των δεδομένων. Τα προσωπικά δεδομένα των χρηστών αντιμετωπίζουν σοβαρές προκλήσεις στα διάφορα κοινόχρηστα περιβάλλοντα, η υποδομή των οποίων διαμοιράζεται μεταξύ πολλών και διαφορετικών φορέων. Επιπλέον, το 5G χρησιμοποιεί το υπολογιστικό νέφος για την αποθήκευση των δεδομένων και των λειτουργιών του NFV, πράγμα που

¹¹ Πρόκειται για το φυσικό στρώμα ή επίπεδο του δικτύου, το οποίο αναφέρεται στην πραγματική υλοποίηση του δικτύου μέσω των φυσικών συσκευών και υποδομών.

σημαίνει ότι οι πάροχοι δεν έχουν άμεσο έλεγχο του χώρου αποθήκευσης των πληροφοριακών στοιχείων. Τέλος, οι διάφορες χώρες έχουν διαφορετικά επίπεδα προστασίας για τα δεδομένα, πρακτική που δημιουργεί από μόνη της κινδύνους.

Η εμπιστοσύνη στο σύστημα 5G βασίζεται στην ασφάλεια, στην ταυτότητα και στο απόρρητο. Πιο συγκεκριμένα, η NGMN αναφέρει ότι οι πάροχοι είναι υπεύθυνοι για τη διάθεση ασφαλών συστημάτων με βάση τις τελευταίες τεχνολογίες, προσφέροντας επίπεδα ασφαλείας για το βασικό κομμάτι που αφορά στην επικοινωνία, στην διασυνδεσιμότητα και στην αποθήκευση των δεδομένων και των πληροφοριών στο νέφος.

Η επικύρωση της ταυτότητας εμπίπτει στον ρόλο των παρόχων κινητής τηλεφωνίας, ως αξιόπιστοι συνεργάτες για την αυθεντικοποίηση των χρηστών. Οι πάροχοι κινητής τηλεφωνίας προσφέρουν ασφαλή διαχείριση ταυτότητας με μία μόνο σύνδεση (single-sign-on) και διαχείριση προφίλ χρήστη, για να καλύπτουν όλες τις ανάγκες της επικοινωνίας και της αλληλεπίδρασης. Το απόρρητο αφορά στον ρόλο των παρόχων που σχετίζεται με την προστασία των ευαίσθητων δεδομένων, εξασφαλίζοντας παράλληλα τη διαφάνειά τους.

Η παραδοσιακή μονάδα ταυτότητας συνδρομητή ή κάρτα SIM (Subscriber Identity Module) αλλά και η κάρτα ολοκληρωμένου κυκλώματος (UICC: Universal Integrated Circuit Card), η οποία χρησιμοποιείται από την πρώτη εμπορική ανάπτυξη των δικτύων 2G, δεν αποτελούν πλέον τη μόνη επιλογή για την αποθήκευση των δεδομένων συνδρομητών. Εάν η ασφαλής αποθήκευση των δεδομένων συνδρομητών και των κωδικών που επιτρέπουν την πρόσβαση στα δίκτυα κινητής τηλεφωνίας, μπορεί να γίνει χωρίς παρέμβαση ή τροποποίηση από εξωτερικούς παράγοντες, τότε οποιαδήποτε ασφαλής φυσική οντότητα μπορεί να χρησιμοποιηθεί για αυτήν τη λειτουργία.

Η UICC εξακολουθεί να είναι ένα αξιόπιστο μέσο αποθήκευσης για τα δεδομένα των συνδρομητών, αλλά υπάρχει και η δυνατότητα αποθήκευσης σε εξωτερική μνήμη που δεν βρίσκεται στην ίδια την κινητή συσκευή. Τα κρυπτογραφικά κλειδιά και η επεξεργασία των δεδομένων, μπορεί να γίνονται εντός ενός συστήματος ενσωματωμένου κυκλώματος (SoC: System on Chip)¹². Προηγμένες εκδόσεις αυτής της ιδέας περιλαμβάνουν το iUICC

¹² Πρόκειται για ένα ενιαίο ηλεκτρονικό σύστημα που περιλαμβάνει διάφορα λειτουργικά τμήματα (όπως επεξεργαστή, μνήμη, κύκλωμα επικοινωνιών κ.λπ.) που έχουν ενσωματωθεί σε ένα μόνο ενιαίο ηλεκτρονικό κύκλωμα.

(Integrated Universal Integrated Circuit Card) και το soft-SIM. Ωστόσο, τα δεδομένα που απαιτούνται για την πρόσβαση στο δίκτυο παραμένουν ιδιοκτησία του φορέα εκμετάλλευσης που διαχειρίζεται το δίκτυο.

Η Ένωση NGMN προβλέπει ότι το σύστημα 5G θα πρέπει να παρέχει προστασία στους πελάτες από κοινές απειλές, όπως η πλαστοπροσωπία και η υποκλοπή δικτύου. Οι επιθέσεις υποκλοπής απαιτούν μια ευάλωτη σύνδεση μεταξύ του πελάτη και του διακομιστή, την οποία οι επιτιθέμενοι μπορούν να εκμεταλλευτούν, ώστε να ανακατευθύνουν την κυκλοφορία του δικτύου και να παρακολουθούν δεδομένα μέσω λογισμικού παρακολούθησης δικτύου (sniffer). Υπάρχει λοιπόν, ανάγκη για αυξημένη εμπιστοσύνη στην ταυτότητα των συνδρομητών δικτύου. Οι λύσεις ασφαλείας για το 5G πρέπει να είναι πιο αποτελεσματικές από εκείνες των προηγούμενων γενεών κινητής επικοινωνίας, ειδικά κατά την παράδοση μεταξύ διαφορετικών δικτύων ραδιοπρόσβασης (RAN).

Το 5G πρέπει επίσης να βελτιώσει τις υπάρχουσες λύσεις για το απόρρητο των χρηστών και του εξοπλισμού στις επικοινωνίες τύπου μηχανής. Οι επικοινωνίες αυτές αφορούν στις αυτόματες επικοινωνίες δεδομένων μεταξύ συσκευών και της υποκείμενης υποδομής μεταφοράς δεδομένων, χωρίς την παρέμβαση ανθρώπων. Ένα παράδειγμα είναι το δίκτυο των έξυπνων μετρητών ρεύματος (Smart Meters) στις υπηρεσίες κοινής ωφέλειας. Τέτοιου είδους επικοινωνία μπορεί επίσης να υφίσταται μεταξύ δύο συσκευών χωρίς τη συμμετοχή διακομιστή, όπως φερ' ειπείν συμβαίνει στο διαδίκτυο των πραγμάτων. Η κύρια πρόκληση στο mMTC είναι η επεκτάσιμη και αποτελεσματική διασυνδεσιμότητα για ένα μεγάλο αριθμό συσκευών, οι οποίες όμως αποστέλλουν πολύ μικρά πακέτα δεδομένων, κάτι που δεν είναι αποτελεσματικό στα υπάρχοντα κυψελοειδή συστήματα, που είναι σχεδιασμένα για τις επικοινωνίες μεταξύ των ανθρώπων.

Πέρα από την ταυτότητα, ιδιαίτερη προσοχή απαιτούν οι πληροφορίες που αποκαλύπτουν τις συνδρομητικές υπηρεσίες, την τοποθεσία, την παρουσία, τα πρότυπα κινητικότητας, τη χρήση του δικτύου και των εφαρμογών.

Η προστασία της διεπαφής ραδιοπρόσβασης παραμένει κρίσιμη, αλλά πρέπει να αναθεωρηθούν και οι μέθοδοι προστασίας σε υψηλότερα επίπεδα. Τα δίκτυα 5^{ης} γενιάς έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να είναι ανεξάρτητα από τον πάροχο, επιτρέποντας την εισαγωγή επιπρόσθετων μηχανισμών ασφαλείας για την ενίσχυση της προστασίας του. Αυτή η προσέγγιση μπορεί να βοηθήσει στην αντιμετώπιση της αυξανόμενης απειλής της απάτης μεταξύ των παρόχων κινητής τηλεφωνίας και της παράνομης χρήσης διεθνών δικτύων

σηματοδότησης. Το 5G αντιμετωπίζει αποτελεσματικά αυτήν την απειλή κατά την περιαγωγή, επιτρέποντας στο οικιακό δίκτυο να επιβεβαιώσει τη σύνδεση του χρήστη με το εξυπηρετικό δίκτυο. Το ίδιο ισχύει και για τα εγχώρια δίκτυα. Ένα από τα βασικά καθήκοντα είναι η διασφάλιση της ταυτότητας των επικοινωνούντων (χρηστών ή μηχανών) στο δίκτυο.

Οι ευπάθειες των δικτύων αναμένεται να αυξηθούν με την εκθετική αύξηση των συνδεδεμένων συσκευών στο 5G, καθώς αυξάνονται τα πρωτόκολλα IP τόσο για τις λειτουργίες του επιπέδου ελέγχου (control plane¹³) όσο και για τις λειτουργίες του επιπέδου χρήστη (user plane¹⁴) σε ένα μεγάλο σύστημα αρχειοθέτησης δικτύου (NFS: Network File System).

Επιπροσθέτως, ιδιαίτερη προσοχή θα πρέπει να δοθεί στην εισαγωγή πολύ φθηνών συσκευών και smartphones τα οποία διαθέτουν ανοιχτά λειτουργικά συστήματα, που εύκολα επιτρέπουν την πρόσβαση (μέσω ανοιχτών θυρών) ακόμη και σε κακόβουλα προγράμματα. Αυτοί οι κίνδυνοι μπορούν να επεκταθούν όχι μόνο μεταξύ των συσκευών και των υπηρεσιών, αλλά και στην υποδομή ραδιοπρόσβασης καθώς και στα κεντρικά 5G δίκτυα. Η Ένωση NGMN υπογραμμίζει την επείγουσα ανάγκη ενίσχυσης των παρακάτω πτυχών για την καλύτερη αντιμετώπιση νέων απειλών από τους παρόχους δικτύου κινητής τηλεφωνίας:

- Ενίσχυση της ανθεκτικότητας έναντι απειλών που βασίζονται στη σηματοδότηση, όπως άμεσες επιθέσεις και υπερφόρτωση των καναλιών σηματοδότησης.
- Βελτίωση του σχεδιασμού ασφαλείας, προκειμένου να επιτυγχάνεται χαμηλή καθυστέρηση, τόσο στην αρχική σηματοδότηση όσο και κατά τη διάρκεια της επικοινωνίας.

Οι απαιτήσεις ασφαλείας στα δίκτυα 5^{ης} γενιάς προέρχονται σε μεγάλο βαθμό από τις τεχνικές προδιαγραφές του 4G. Η Ένωση NGMN αναγνωρίζει επίσης τις ιδιαίτερες ανάγκες

¹³ Είναι υπεύθυνο για τη διαχείριση και τον έλεγχο της ροής της κυκλοφορίας δεδομένων. Περιλαμβάνει λειτουργίες όπως η δρομολόγηση, η σηματοδότηση, η διαχείριση της σύνδεσης και η διαχείριση των πόρων του δικτύου. Το επίπεδο ελέγχου είναι υπεύθυνο για τη λήψη αποφάσεων σχετικά με το πού και πώς θα δρομολογηθούν τα δεδομένα, τη δημιουργία και την κατάργηση συνδέσεων και την παροχή πληροφοριών για τη διαχείριση της ποιότητας της υπηρεσίας.

¹⁴ αφορά στην πραγματική μεταφορά δεδομένων μεταξύ των τελικών σημείων του δικτύου. Περιλαμβάνει τις λειτουργίες που σχετίζονται με τη μεταφορά της κυκλοφορίας δεδομένων χρήστη, όπως είναι η αποστολή και η λήψη δεδομένων, η εφαρμογή πολιτικών ποιότητας υπηρεσίας και η διαχείριση της κίνησης δεδομένων. Το επίπεδο χρήστη επικεντρώνεται στη μεταφορά δεδομένων με τη μέγιστη δυνατή ταχύτητα και αξιοπιστία, χωρίς να ασχολείται με τον έλεγχο ή τη διαχείριση των συνδέσεων.

του 5G για τη δημόσια ασφάλεια και τις κρίσιμες αποστολές επικοινωνιών, επιδιώκοντας τη μείωση του κόστους για αυτές τις επικοινωνίες. Τα νέα δίκτυα υποστηρίζουν τις επικοινωνίες έκτακτης ανάγκης, τουλάχιστον με το ίδιο επίπεδο παροχής υπηρεσιών και ποιότητας, σε σχέση με εκείνες των προηγούμενων γενεών, προσφέροντας βασικές λειτουργίες ασφαλείας, ακόμη και σε περίπτωση καταστροφής μέρους της υποδομής δικτύου. Σε τέτοιες περιπτώσεις, το δίκτυο θα πρέπει να προστατεύεται από τις κακόβουλες επιθέσεις, συμπεριλαμβανομένων εκείνων που αντιμετώπιζαν οι προκάτοχοί του, δηλαδή επιθέσεις παρεμβολής στη ραδιοπρόσβαση και προσπάθειες παραβίασης των κόμβων μικρών κυψελών, που είναι κατανεμημένοι σε μεγάλες γεωγραφικές περιοχές (Kareem, 2024; HIVO, Hussain et. al., n.d.; 2024; Pauliac, 2020; Wani et al., 2024; Yusuf, 2023).

3.9 Αρχές ασφαλείας για τον τεμαχισμό δικτύου

Η τεχνολογία τεμαχισμού δικτύου αναδεικνύεται ως καθοριστικός παράγοντας στα δίκτυα επόμενης γενιάς, ενισχυόμενη από την ενσωμάτωση της δικτύωσης που καθορίζεται από το SDN λογισμικό και την εικονικοποίηση λειτουργιών δικτύου (NFV). Όπως ήδη έχει προαναφερθεί, οι τεχνολογίες αυτές επιτρέπουν την κοινή χρήση πόρων μεταξύ πολλών χρηστών, απαιτώντας κατά συνέπεια αυξημένα επίπεδα ασφαλείας. Είναι κρίσιμο, οι επιθέσεις που εκτελούνται σε ένα τεμάχιο, να μην επηρεάζουν τα υπόλοιπα, γεγονός που σημαίνει ότι οι λειτουργίες ασφαλείας θα πρέπει να λειτουργούν ανεξάρτητα.

Ο διαχειριστής δικτύου και ασφαλείας (NSM: Network and Security Manager) παρακολουθεί τις ροές και τις αλληλεπιδράσεις των λειτουργιών μεταξύ των τεμαχίων, εντός των τομέων διαχείρισής του και είναι υπεύθυνος για το εικονικό δίκτυο και τις λειτουργίες αλληλεπίδρασης που αφορούν στα τεμάχια. Ωστόσο, δε φέρει ευθύνη για την ενορχήστρωση ή την ορθότητα των υπηρεσιών που παρέχονται από αυτά.

Οι λύσεις τεμαχισμού δικτύου πρέπει να εξασφαλίζουν τις βασικές αρχές ασφαλείας: εμπιστευτικότητα, έλεγχος ταυτότητας, εξουσιοδότηση, διαθεσιμότητα και ακεραιότητα. Σε αυτό το πλαίσιο, όταν αυτές οι αρχές εφαρμόζονται στον τεμαχισμό δικτύου, μεταφράζονται ως εξής (Scalise, 2024):

- **Εμπιστευτικότητα:** Θα πρέπει να διασφαλίζεται ότι τα δεδομένα δεν διαρρέουν έξω από το τεμάχιο που τα δημιούργησε ή από τα τεμάχια που επιτρέπεται να διασυνδέονται. Επιπλέον, τα δεδομένα που μεταφέρονται ή αποθηκεύονται σε

λειτουργίες δικτύου (NF: Network Function) θα πρέπει να είναι προσβάσιμα μόνο από τα επιτρεπόμενα στοιχεία ή από τους εξουσιοδοτημένους τελικούς χρήστες.

- **Έλεγχος ταυτότητας:** Πρέπει να αναγνωρίζονται και να επικυρώνονται τα άτομα, οι λογαριασμοί ή τα στοιχεία που αλληλεπιδρούν με το σύστημα. Όταν τα συστήματα υποστήριξης λειτουργιών (OSS: Operations Support Systems¹⁵) και υποστήριξης επιχειρηματικών δραστηριοτήτων (BSS: Business Support Systems¹⁶) αλληλεπιδρούν με τον διαχειριστή δικτύου και ασφάλειας, πρέπει να υπάρχει αμοιβαία επαλήθευση και πιστοποίηση. Το ίδιο ισχύει για τις αλληλεπιδράσεις που γίνονται εκ μέρους των ιδιοκτητών τεμαχίων και για τις αλληλεπιδράσεις μεταξύ του διαχειριστή δικτύου και του ενορχηστρωτή.
- **Εξουσιοδότηση:** Θα πρέπει να καθορίζεται εάν μια επιχειρούμενη αλληλεπίδραση επιτρέπεται να πραγματοποιηθεί. Οι τελικοί χρήστες μπορούν να αλληλεπιδρούν μόνο με τα τεμάχια που τους έχουν παραχωρηθεί. Οι ιδιοκτήτες τεμαχίων διαχειρίζονται μόνο τα δικά τους τεμάχια και τις αλληλεπιδράσεις τους. Οι πάροχοι υποδομής έχουν τον πλήρη έλεγχο των διαχειριστών δικτύου καθώς και της ασφάλειας και της λογιστικής των τεμαχίων. Ο διαχειριστής δικτύου ελέγχει τις παρουσίες τεμαχίων δικτύου (NSI: Network Slice Instance) και τις λειτουργίες του δικτύου.
- **Διαθεσιμότητα:** Το σύστημα θα πρέπει να είναι προσβάσιμο και να λειτουργεί όταν απαιτείται και όπως προδιαγράφεται και αναμένεται. Ο διαχειριστής δικτύου και ασφάλειας και οι λειτουργίες δικτύου θα πρέπει να παραμένουν προσβάσιμες, ενώ τα τεμάχια θα πρέπει να είναι διαθέσιμα, εντός των συμφωνημένων πόρων υποδομής. Οι χρόνοι απόκρισης θα πρέπει να τηρούνται στα όρια που ορίζονται στη συμφωνία επιπέδου υπηρεσιών.
- **Ακεραιότητα:** Το σύστημα θα πρέπει να προστατεύεται από παραβιάσεις δεδομένων ή αλλαγές στη λειτουργικότητά του. Μόνο οι ιδιοκτήτες τεμαχίων μπορούν να

¹⁵ Είναι συστήματα που παρέχουν υποστήριξη για την εκτέλεση και τη διαχείριση των λειτουργικών πτυχών των τηλεπικοινωνιακών δικτύων, όπως η διαχείριση των δικτυακών πόρων, η παρακολούθηση της απόδοσης του δικτύου και η επίλυση προβλημάτων.

¹⁶ Είναι συστήματα που παρέχουν υποστήριξη για τις εμπορικές και οικονομικές πτυχές των τηλεπικοινωνιακών επιχειρήσεων, όπως η διαχείριση των πελατών, η τιμολόγηση και η διαχείριση των παραγγελιών.

τροποποιούν τις λειτουργίες δικτύου τους και τις διαμορφώσεις μεταξύ των τεμαχίων. Οι αλληλεπιδράσεις μεταξύ των τεμαχίων θα πρέπει να γίνονται μόνο μέσω των αντίστοιχων διεπαφών τους.

3.10 Διαχείριση ταυτότητας και πρόσβασης

Η ασφάλεια στα 5G δίκτυα επηρεάζεται σημαντικά από την ανάγκη για αξιόπιστη ταυτοποίηση και πιστοποίηση των χρηστών και των συσκευών. Η χρήση ισχυρών μηχανισμών ελέγχου ταυτότητας, όπως η πολλαπλή επαλήθευση ταυτότητας (MFA: Multi-factor authentication) και η διαχείριση προφίλ χρηστών σε πραγματικό χρόνο, επιτρέπουν την αντιμετώπιση απειλών σε πραγματικό χρόνο και την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Επιπλέον, οι πάροχοι 5G δικτύων πρέπει να εφαρμόζουν αυστηρές πολιτικές διαχείρισης ταυτότητας, προκειμένου να διασφαλίζουν ότι οι χρήστες έχουν την κατάλληλη πρόσβαση, μόνο στα δεδομένα και τις υπηρεσίες που είναι απαραίτητα για τη λειτουργία τους.

Η διαχείριση ταυτότητας και πρόσβασης (IAM: Identity and Access Management) αποτελεί κρίσιμο παράγοντα στην ασφάλεια των δικτύων 5G, καθώς η αυξημένη πολυπλοκότητα και η ποικιλία των συνδεδεμένων συσκευών απαιτούν ισχυρούς μηχανισμούς ελέγχου. Στα δίκτυα 5G, όπου ο αριθμός των χρηστών και των συσκευών πολλαπλασιάζεται, το IAM σύστημα διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα και συσκευές μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα και πόρους του δικτύου. Η ενσωμάτωση των μεθόδων του με τις νέες τεχνολογίες, όπως η εικονικοποίηση λειτουργιών δικτύου και η δικτύωση που καθορίζεται από λογισμικό, προσφέρει αυξημένη ευελιξία και δυνατότητες προσαρμογής στις μεταβαλλόμενες ανάγκες ασφάλειας.

Η υιοθέτηση του IAM πλαισίου στα 5G δίκτυα, δεν αφορά μόνο στην προστασία από εξωτερικές απειλές, αλλά και στην πρόληψη κακόβουλων δραστηριοτήτων από εσωτερικούς χρήστες. Οι προηγμένες λύσεις διαχείρισης ταυτότητας και πρόσβασης, που περιλαμβάνουν ανάλυση συμπεριφοράς και μηχανισμούς μηχανικής μάθησης, μπορεί να βοηθήσουν στον εντοπισμό και στην αποτροπή ύποπτων δραστηριοτήτων. Η διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, καθίσταται έτσι δυνατή, εξασφαλίζοντας ταυτόχρονα την απρόσκοπτη και ασφαλή λειτουργία των 5G δικτύων γενικότερα (Veritis a-c, 2024).

3.11 Ασφάλεια από άκρο σε άκρο

Η ασφάλεια από άκρο σε άκρο (end-to-end security) είναι ζωτικής σημασίας για τα δίκτυα 5G, καθώς θα πρέπει να διασφαλίζεται ότι όλα τα δεδομένα που διακινούνται από τη μια συσκευή στην άλλη μέσω του δικτύου, παραμένουν ασφαλή σε όλη τη διαδρομή τους. Σε αντίθεση με τις προηγούμενες γενιές δικτύων, όπου η ασφάλεια επικεντρωνόταν κυρίως στα σημεία πρόσβασης, τα δίκτυα 5^{ης} γενιάς, απαιτούν συνολική προστασία λόγω της πολυπλοκότητας και της ποικιλομορφίας των εφαρμογών και των υπηρεσιών που υποστηρίζουν. Η ενσωμάτωση των νέων τεχνολογιών (εικονικοποίηση λειτουργιών δικτύου και η δικτύωση που καθορίζεται από λογισμικό) απαιτεί προηγμένες λύσεις ασφάλειας που μπορούν να αντιμετωπίσουν τις νέες απειλές και τυχόν ευπάθειες.

Η ασφάλεια από άκρο σε άκρο στα 5G δίκτυα, περιλαμβάνει την κρυπτογράφηση των δεδομένων σε όλη τη διαδρομή τους, από την αρχική συσκευή αποστολής μέχρι τον τελικό αποδέκτη. Με αυτό τον τρόπο, τα δεδομένα δεν μπορούν να αναγνωστούν ή να τροποποιηθούν από μη εξουσιοδοτημένα μέρη. Επιπλέον, περιλαμβάνει ισχυρούς μηχανισμούς ελέγχου ταυτότητας και εξουσιοδότησης, που εγγυώνται ότι μόνο εξουσιοδοτημένοι χρήστες και συσκευές, μπορούν να έχουν πρόσβαση σε ευαίσθητες πληροφορίες και πόρους. Η ασφάλεια από άκρο σε άκρο, περιλαμβάνει επίσης την προστασία των δεδομένων κατά τη διάρκεια της αποθήκευσης και της επεξεργασίας, χρησιμοποιώντας τεχνολογίες όπως τα ασφαλή περιβάλλοντα εκτέλεσης (secure enclaves¹⁷) και οι κρυπτογραφημένες βάσεις δεδομένων (NSA & CISA, n.d.).

3.12 Κανονισμοί και νομοθεσία για την ασφάλεια στα 5G δίκτυα

Η ανάπτυξη και η ασφάλεια των 5G δικτύων ρυθμίζονται τόσο από εθνικούς όσο και από διεθνείς κανονισμούς, με σκοπό την προστασία των υποδομών και των δεδομένων. Στην Ελλάδα, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι ο κύριος φορέας που επιβλέπει την υλοποίηση των 5G δικτύων, προκειμένου οι πάροχοι να συμμορφώνονται με τα απαιτούμενα πρότυπα ασφαλείας. Επιπλέον, η Ελληνική Κυβέρνηση

¹⁷ Είναι υπεύθυνα για την αποθήκευση και εκτέλεση ευαίσθητου λογισμικού και δεδομένων σε ένα προστατευμένο περιβάλλον, όπου ούτε οι εξωτερικοί χρήστες, ούτε οι εφαρμογές μπορούν να έχουν πρόσβαση σε αυτά, χωρίς την έγκριση του εντελώς αξιόπιστου περιβάλλοντος εκτέλεσης

έχει υιοθετήσει στρατηγικές για την ασφάλεια στον κυβερνοχώρο που περιλαμβάνουν μέτρα για την προστασία των τηλεπικοινωνιακών δικτύων, όπως είναι οι υποχρεώσεις των εταιρειών τηλεπικοινωνίας να εφαρμόζουν συγκεκριμένα πρωτόκολλα ασφαλείας και να αναφέρουν περιστατικά παραβίασης ασφάλειας.

Σε διεθνές επίπεδο, οργανισμοί όπως η Ευρωπαϊκή Ένωση και η Διεθνής Ένωση Τηλεπικοινωνιών έχουν εκδώσει κανονισμούς και οδηγίες για την ασφάλεια των 5G δικτύων. Η Ευρωπαϊκή Ένωση, μέσω του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA: European Union Agency for Cybersecurity) έχει εκδώσει οδηγίες, που απαιτούν από τα κράτη μέλη να αναπτύξουν εθνικές στρατηγικές για την ασφάλεια των δικτύων 5G. Οι οδηγίες αυτές περιλαμβάνουν μέτρα για την προστασία της υποδομής των τηλεπικοινωνιών από κυβερνοεπιθέσεις, καθώς και για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων που διακινούνται μέσω των δικτύων.

Οι κανονισμοί για την ασφάλεια των 5G δικτύων, δίνουν έμφαση στη συνεργασία μεταξύ των κρατών, των παρόχων υπηρεσιών και των κατασκευαστών εξοπλισμού. Η ανάγκη για ασφάλεια από άκρο σε άκρο, η προστασία της ιδιωτικότητας των χρηστών και η ανθεκτικότητα των δικτύων σε επιθέσεις είναι κεντρικοί στόχοι των κανονισμών αυτών. Ειδικά σε θέματα κυβερνοασφάλειας, οι διεθνείς κανονισμοί απαιτούν από τις εταιρείες να εφαρμόζουν συνεχείς διαδικασίες αξιολόγησης και διαχείρισης των κινδύνων, να επενδύουν σε τεχνολογίες ασφάλειας και να εκπαιδεύουν το προσωπικό τους, στην αναγνώριση και στην αντιμετώπιση των απειλών (ENISA a., 2022; Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

ΚΕΦΑΛΑΙΟ 4 : ΑΠΕΙΛΕΣ ΣΤΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ 5G

4.1 Εικονικοποίηση δικτύου

Για να διασφαλιστεί η ασφάλεια κατά την εικονικοποίηση των 5G δικτύων (Network Virtualization) θα πρέπει να ληφθούν υπόψη τα εξής:

- **Αποφυγή νέων απειλών:** Η εικονικοποίηση δεν θα πρέπει να δημιουργεί νέες απειλές ασφαλείας, όπως αυτές που προκαλούνται από ευπάθειες του hypervisor. Ο υπεύθυνος εποπτείας, γνωστός και ως οθόνη εικονικής μηχανής ή VMM (Virtual Machine Monitor) είναι στην ουσία ένα λογισμικό που δημιουργεί και διαχειρίζεται τις εικονικές μηχανές. Το λογισμικό αυτό, καθιστά δυνατές τις ενέργειες της φιλοξενίας πολλαπλών εικονικών μηχανών, που διαμοιράζονται τους ίδιους πόρους ενός κεντρικού υπολογιστή, όπως είναι για παράδειγμα η μνήμη και η επεξεργαστική ισχύς.
- **Διαμοιρασμός των πόρων:** Τόσο οι κοινές λειτουργίες του δικτύου όσο και οι πόροι του υλικού, όπως η αποθήκευση και η δικτύωση, θα πρέπει να συνδέονται μεταξύ τους στις διάφορες εικονικές λειτουργίες ενός δικτύου.
- **Διασύνδεση των εξαρτημάτων:** Θα πρέπει να υπάρχει αλληλεπίδραση μεταξύ των εξαρτημάτων για τη λειτουργία της εικονικοποίησης του δικτύου.
- **Απομόνωση των λειτουργιών:** Η απομόνωση των εικονικών λειτουργιών δικτύου ολοκληρώνεται μέσω της υποδομής NFV, προκειμένου να διασφαλιστεί ότι οι διαφορετικές λειτουργίες δεν επηρεάζουν η μία την άλλη.
- **Απόδοση και χωρητικότητα:** Είναι πιθανό οι εικονικές λειτουργίες δικτύου να έχουν μικρότερη απόδοση σε σύγκριση με τις αντίστοιχες φυσικές. Ως εκ τούτου, για να επιτευχθεί η απαιτούμενη απόδοση, είναι απαραίτητη η παρουσία μηχανισμών που διαμοιράζουν τον φόρτο εργασίας, μεταξύ πολλαπλών λειτουργιών.

4.2 Ακροδικτυακή υπολογιστική ή υπολογιστική των παρυφών

Μέσω των υψηλών ταχυτήτων του νέου δικτύου και της ευφυούς διασύνδεσης συσκευών, ο υπολογισμός στο άκρο του δικτύου, επιτρέπει την επεξεργασία δεδομένων πιο κοντά στη

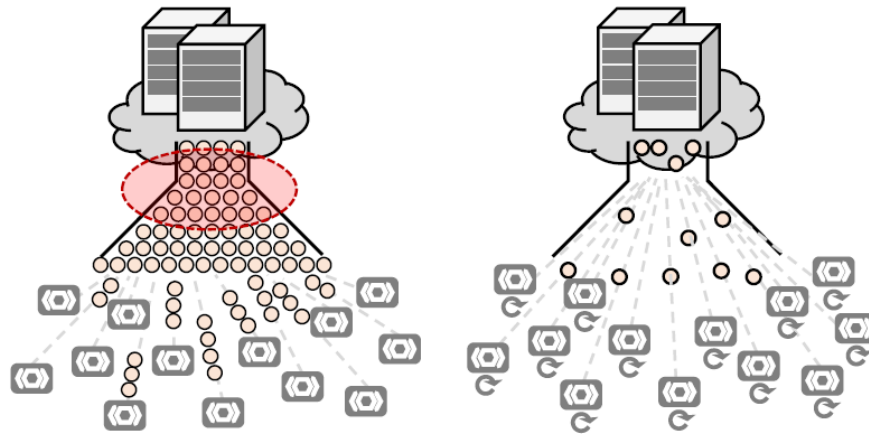
συσκευή, προσφέροντας την ανταλλαγή δεδομένων σε πραγματικό χρόνο, μειώνοντας ταυτόχρονα το φορτίο στο δίκτυο.

Το edge computing (ακροδικτυακή υπολογιστική ή υπολογιστική των παρυφών), ως υποπεδίο του διαδικτύου των πραγμάτων, είναι ένα καταναμημένο πρότυπο υπολογιστών που φέρνει την επεξεργασία και την αποθήκευση δεδομένων κοντά στην τοποθεσία. Αυτό βελτιώνει τους χρόνους απόκρισης και εξοικονομεί μεγάλο εύρος ζώνης. Πρόκειται για μια αποκεντρωμένη αρχιτεκτονική, που επιτρέπει στις τεχνολογίες των φορητών υπολογιστών και των IoT συσκευών, να λειτουργούν πιο αποτελεσματικά.

Σε αυτή την τοπολογία, τα δεδομένα υποβάλλονται σε επεξεργασία, είτε από την ίδια τη συσκευή, είτε από έναν τοπικό υπολογιστή ή τοπικό διακομιστή, αντί να μεταδίδονται σε ένα κέντρο δεδομένων. Αυτό σημαίνει ότι, η υπολογιστική επεξεργασία δεδομένων αισθητήρα γίνεται κοντά στο λογικό άκρο του δικτύου και κοντά στις μεμονωμένες πηγές δεδομένων. Πρακτικά, η διαδικασία αυτή τοποθετεί τις υπολογιστικές μονάδες κοντά σε routers (δρομολογητές) και gateways (πύλες δικτύου), διασυνδέοντας το cloud με τον τελικό χρήστη. Με αυτό τον τρόπο, επιτυγχάνεται η επεξεργασία των δεδομένων που παράγονται από τις IoT συσκευές να ολοκληρώνεται πιο κοντά στην πηγή τους, αντί να αποστέλλονται σε μεγάλες αποστάσεις προς τα κέντρα δεδομένων ή το υπολογιστικό νέφος. Αυτού του είδους η επεξεργασία, επιτρέπει στις εταιρείες να αναλύουν σημαντικά δεδομένα σε σχεδόν πραγματικό χρόνο και στις συσκευές IoT να στέλνουν και να λαμβάνουν δεδομένα, πιο γρήγορα και αποτελεσματικά.

Το edge computing επεξεργάζεται τα δεδομένα σε τοπικό επίπεδο, με στόχο τη μείωση της ανάγκης για επιστροφή δεδομένων (backhaul¹⁸) προς το κεντρικό αποθηκευτικό χώρο. Αυτό με τη σειρά του, έχει ως αποτέλεσμα λιγότερη εξάρτηση από το Wi-Fi ή τα δεδομένα δικτύου, μειώνοντας με αυτό τον τρόπο την καθυστέρηση στην επικοινωνία, εξοικονομώντας εύρος ζώνης και διατηρώντας ταυτόχρονα περισσότερα δεδομένα στην ιδιωτική σφαίρα, όπως απεικονίζεται στην παρακάτω εικόνα:

¹⁸ Ο όρος αναφέρεται στη λειτουργία του τμήματος του δικτύου τηλεπικοινωνιών που συνδέει τις τοπικές ή περιφερειακές περιοχές με τον κεντρικό κόμβο ή το κεντρικό δίκτυο και χρησιμοποιείται για να περιγράψει τη μεταφορά δεδομένων από τις τοπικές περιοχές προς τους κεντρικούς κόμβους, όπου γίνεται η αποθήκευση, η επεξεργασία και η διαχείριση των δεδομένων



(a) Bottlenecks in cloud computing (b) Solution using edge computing

Εικόνα 12: Συμφόρηση του IOT στο 5G και επίλυση με τη χρήση του edge computing

Πηγή: Lee et al., 2020

Αυτή η προσέγγιση, είναι σαφές, ότι διαφέρει από τη σύνδεση με απομακρυσμένες βάσεις δεδομένων στο υπολογιστικό νέφος, η οποία είναι και η πιο συνηθισμένη πρακτική. Η παραδοσιακή υποδομή cloud, παρόλο που προσέφερε πολλές νέες δυνατότητες όπως η αποθήκευση και η ανάλυση μεγάλων δεδομένων (Big Data), αντιμετωπίζει προκλήσεις λόγω της ανάγκης διαχείρισης τεράστιων ποσοτήτων δεδομένων σε πραγματικό χρόνο. Η υπολογιστική των παρυφών, προσφέρει μια εναλλακτική λύση για την αντιμετώπιση αυτών των προκλήσεων.

Η τεχνολογία 5G επιτρέπει σε έναν ασύρματο σταθμό να συνδέει έως και 1 εκατομμύριο συσκευές ανά τετραγωνικό χιλιόμετρο, βελτιώνοντας την απόδοση των cloud συστημάτων που βρίσκονται κοντά στους χρήστες.

Η ακροδικτυακή υπολογιστική πολλαπλών προσβάσεων, είναι μια δικτυακή λύση που προσφέρει δυνατότητες υπολογιστικού νέφους, υπηρεσίες πληροφορικής και λειτουργίες υπολογιστών στις άκρες του δικτύου. Το MEC επεξεργάζεται δεδομένα μεταξύ του cloud και του χρήστη, φέρνοντας τις υπηρεσίες εφαρμογών και το περιεχόμενο, πιο κοντά στους χρήστες. Έτσι, βελτιώνει τη συνεργασία του δικτύου και παρέχει, αξιόπιστη και υψηλής ποιότητας, εμπειρία υπηρεσιών. Μπορεί να αναπτυχθεί ακόμη και σε ιδιωτικά δίκτυα κινητής τηλεφωνίας, προσφέροντας αποκλειστικές υπηρεσίες σε συγκεκριμένες επιχειρήσεις (Hassan et al., 2018; Lee et al., 2020).

Ωστόσο, δεδομένου ότι το MEC βασίζεται στην αρχή της εικονικοποίησης, αντιμετωπίζει τα ίδια ζητήματα ασφαλείας με το NFV. Σημειώνεται ότι το NGMN έχει εντοπίσει αρκετά βασικά θέματα ασφαλείας σε αυτή τη λύση:

- **Δρομολόγηση δεδομένων:** Τα δεδομένα δρομολογούνται απευθείας από τη συσκευή του χρήστη στο άκρο του δικτύου, παρακάμπτοντας το κεντρικό και το οικιακό δίκτυο. Αυτό σημαίνει ότι, επειδή τα άκρα του δικτύου είναι πιο επιρρεπή σε επιθέσεις, τα αρχεία χρέωσης πρέπει να είναι αξιόπιστα και ασφαλή, ώστε να μειωθεί η πιθανότητα σφαλμάτων χρέωσης.
- **Αλληλεπίδραση εφαρμογών:** Οι εφαρμογές edge computing, εκτελούνται στις ίδιες συσκευές με τις λειτουργίες δικτύου, οπότε θα πρέπει να καθιερωθεί μια σχέση εμπιστοσύνης μεταξύ του φορέα εκμετάλλευσης και των εφαρμογών που διατίθενται από τρίτους παρόχους, ώστε να διασφαλιστεί ότι οι εφαρμογές δεν θα βλάψουν τις λειτουργίες του δικτύου.
- **Απόδοση δικτύου:** Η αυτόματη προσαρμογή της λειτουργίας του δικτύου, ώστε να καλύπτει τις απαιτήσεις του εύρους ζώνης των εφαρμογών, μπορεί να επηρεάσει την απόδοση άλλων εφαρμογών, αν αυτές καταναλώνουν, είτε κατά λάθος, είτε κακόβουλα, υπερβολικό εύρος ζώνης.
- **Παράδοση περιεχομένου:** Η απευθείας παράδοση περιεχομένου από την άκρη του δικτύου στη συσκευή του χρήστη, σημαίνει ότι τα αντίγραφα του περιεχομένου βρίσκονται στις άκρες του δικτύου, καθιστώντας τα ευάλωτα σε επιθέσεις IP.
- **Προστασία δεδομένων:** Η αποθήκευση ευαίσθητων δεδομένων στην άκρη του δικτύου πρέπει να προστατεύεται, ιδιαίτερα κατά την ανταλλαγή αυτών μεταξύ του πυρήνα του δικτύου και του δικτύου κινητής τηλεφωνίας.

Εάν οι απαιτήσεις καθυστέρησης είναι πολύ αυστηρές, μπορεί να υπάρξουν σημαντικοί περιορισμοί στους μηχανισμούς προστασίας. Οι απαιτήσεις για πολύ χαμηλή καθυστέρηση πρέπει να εξετάζονται προσεκτικά, δεδομένου ότι μπορούν να επηρεάσουν την απόσταση των κεντρικών κόμβων δικτύου από τις συσκευές των χρηστών.

4.3 Λειτουργίες δικτύου

Ο κύριος στόχος των παρόχων κινητής τηλεφωνίας είναι να κατασκευάσουν τα δίκτυα 5G με τόσο ευέλικτο τρόπο, ώστε να υποστηρίζουν ποικίλα σενάρια, όπως την εισαγωγή του

τεμαχισμού δικτύου για διάφορα τμήματα της αγοράς (κάθετης ή οριζόντιας). Αυτή η στρατηγική, επιτρέπει τη δημιουργία ενός ελαστικού και επεκτάσιμου δικτύου, το οποίο βελτιστοποιεί τη διαχείριση της κινητικότητας και υποστηρίζει την αποτελεσματική παράδοση περιεχομένου. Τα βασικά στοιχεία για αυτή τη δομή είναι η ευελιξία, η ανεξαρτησία του φορέα και η επεκτασιμότητα.

Αντιμετωπίζονται επίσης, περιπτώσεις χρήσης που σχετίζονται με την πρόσβαση, όπως η επιλογή της καταλληλότερης πρόσβασης για την κυκλοφορία χρηστών, η συνύπαρξη με παλαιά συστήματα (legacy systems¹⁹) και η μετεγκατάσταση υπηρεσιών από παλαιότερες γενιές δικτύων. Οι εκτεθειμένες δυνατότητες δικτύου σε τρίτους, λαμβάνονται, επίσης, υπόψη. Οι απαιτήσεις ασφαλείας περιλαμβάνουν (Olimid et al., 2020):

- Την προστασία της εμπιστευτικότητας και της ακεραιότητας, τόσο της φωνής, όσο και των υπολοίπων δεδομένων, καθώς και των πληροφοριών της σηματοδότησης.
- Τη διασφάλιση της εξουσιοδότησης, της εμπιστευτικότητας και της προστασίας της ακεραιότητας, μεταξύ των στοιχείων του δικτύου αλλά και μεταξύ όλων των δικτύων που συμμετέχουν σε μια επικοινωνία.
- Τη διασφάλιση της εξουσιοδότησης, της εμπιστευτικότητας και της προστασίας της ακεραιότητας, για τις υπηρεσίες της επόμενης γενιάς.
- Τη διασφάλιση της εξουσιοδότησης για χρήστες, συσκευές και δίκτυα.
- Επεκτάσιμα συστήματα για την υποστήριξη νέων αλγορίθμων και διαδικασιών, για τον μετριασμό των κινδύνων από την κβαντική πληροφορική.
- Κανόνες για την πρόληψη των DoS επιθέσεων και των επιθέσεων σηματοδότησης.
- Δικλείδες ασφαλείας για την προστασία της ιδιωτικής ζωής, με χρήση ψευδωνύμων ή προσωρινών αναγνωριστικών και απόκρυψη των πληροφοριών της τοποθεσίας του χρήστη.

¹⁹ Ο όρος αναφέρεται σε τεχνολογικά συστήματα, εφαρμογές ή λογισμικά που έχουν αναπτυχθεί ή εγκατασταθεί πριν από την εισαγωγή νέων τεχνολογιών ή συστημάτων. Συχνά τα legacy systems είναι παλαιότερης τεχνολογίας και μπορεί να έχουν περιορισμένη συμβατότητα ή επίδοση σε σύγκριση με τα σύγχρονα συστήματα

- Υποστήριξη περιστατικών έκτακτης ανάγκης, παρέχοντας προσωρινή πρόσβαση στο δίκτυο βάσει των πολιτικών του χειριστή.
- Πρόληψη κλοπής συσκευών, με ασφαλείς μηχανισμούς για απενεργοποίηση ή επανενεργοποίηση κλεμμένων συσκευών και προστασία των αναγνωριστικών συσκευών κατά την αποθήκευση.

Οι λύσεις ασφαλείας για τις νέες τεχνολογίες και τις έννοιες του 5G, πρέπει να λαμβάνουν υπόψη τα ακόλουθα ζητήματα (Olimid et al., 2020):

- Υποστήριξη ασφαλείας για συγκεκριμένες υπηρεσίες: Κάθε τεμάχιο δικτύου πρέπει να έχει καλά απομονωμένες διαμορφώσεις ασφαλείας, επιτρέποντας σε τρίτα μέρη να διαμορφώνουν την ασφάλεια, μόνο μέσω κατάλληλων διεπαφών προγραμματισμού εφαρμογών.
- Ασφαλή μηχανισμός συλλογής πληροφοριών: Το σύστημα 5G πρέπει να υποστηρίζει έναν ασφαλή μηχανισμό για τη συλλογή πληροφοριών συστήματος, εξασφαλίζοντας ταυτόχρονα το απόρρητο των τελικών χρηστών και των εφαρμογών.
- Συμμόρφωση με τις απαιτήσεις της νόμιμης παρακολούθησης (LI: Lawful Intercept²⁰): Οι απαιτήσεις αυτές θα πρέπει να περιλαμβάνουν και το περιεχόμενο που μπορεί να αποθηκευτεί στην κρυφή μνήμη στην άκρη του δικτύου.
- Υποστήριξη πολλαπλών τρόπων πρόσβασης στο δίκτυο: Οι συσκευές πρέπει να μπορούν να έχουν πρόσβαση στο 5G δίκτυο, μέσω διαφορετικών τεχνολογιών ραδιοπρόσβασης και να επικυρώνουν την ταυτότητά τους, χρησιμοποιώντας τα διαπιστευτήρια του 5G.

4.4 Βελτιωμένη κινητή ευρυζωνικότητα

Η βελτιωμένη κινητή ευρυζωνική σύνδεση, αποτελεί μια εξέλιξη των υπηρεσιών που προσφέρθηκαν αρχικά από τα δίκτυα 4G LTE, προσφέροντας υψηλό ρυθμό δεδομένων σε εκτεταμένες περιοχές κάλυψης. Το eMBB έχει σχεδιαστεί για να υποστηρίζει τη μεγάλη

²⁰ Ο όρος αναφέρεται στην ικανότητα ενός τηλεπικοινωνιακού συστήματος να επιτρέπει στις δικαστικές αρχές ή άλλες εξουσιοδοτημένες αρχές, να πραγματοποιούν νόμιμη παρακολούθηση και παρεμβολή στις επικοινωνίες.

χωρητικότητα που απαιτείται για την εξυπηρέτηση, τόσο μεγάλων σε πλήθος δεδομένων, όσο και των τελικών χρηστών. Αυτή η τεχνολογία είναι απαραίτητη για την παροχή αξιόπιστης και ταχείας διασυνδεσιμότητας, για την εξυπηρέτηση εφαρμογών όπως η ροή βίντεο υψηλής ευκρίνειας και η υποστήριξη άλλων τεχνολογιών, όπως η εικονική και η επαυξημένη πραγματικότητα.

Η eMBB στοχεύει στην προστασία του πολύτιμου περιεχομένου και των συνδέσεων υψηλής αξίας. Αυτή η τεχνολογία καλύπτει σενάρια χρήσης που απαιτούν υψηλούς ρυθμούς δεδομένων, μεγάλη πυκνότητα χρηστών και υψηλή κινητικότητα, περιλαμβάνοντας ακόμα και τις επικοινωνίες αεροπλάνων. Οι βασικές απαιτήσεις ρυθμού δεδομένων για downlink και uplink, καθορίζονται από τα σενάρια χρήσης, ανάλογα με το αν απαιτείται η μεταφορά μεγάλου όγκου δεδομένων ή η διαχείριση ενός μεγάλου αριθμού συνδέσεων.

Για την προστασία του περιεχομένου, το eMBB χρησιμοποιεί μηχανισμούς κρυπτογράφησης και προστασίας ακεραιότητας, τόσο στο επίπεδο δικτύου όσο και σε επίπεδο υπηρεσίας, με εφαρμογή της διαχείρισης ανταποκρινόμενη στη ζήτηση (DRM: Demand Response Management). Επιπλέον, όταν το περιεχόμενο μεταδίδεται σε πολλές συσκευές, οι διαμορφώσεις στην ασφάλεια θα πρέπει να υποστηρίζουν αυτό το σενάριο και να επικαιροποιούν τον αριθμό των συσκευών που λαμβάνουν το περιεχόμενο.

Η ταυτοποίηση και η συνεχής διασυνδεσιμότητα είναι κρίσιμες, ιδιαίτερα όταν οι χρήστες μετακινούνται από εσωτερικούς σε εξωτερικούς χώρους και το αντίστροφο. Ο μηχανισμός ελέγχου ταυτότητας, πρέπει να επιτρέπει την απρόσκοπτη εμπειρία του χρήστη, με ταυτόχρονη εξασφάλιση ότι η σύνδεση παραμένει σταθερή και χωρίς διακοπές, ακόμα και κατά τη μετάβαση από Wi-Fi σε 5G. Αυτή η λειτουργία, απαιτεί το τελικό σημείο ελέγχου ταυτότητας να βρίσκεται στον πυρήνα του δικτύου, επιτρέποντας την ομαλή περιαγωγή μεταξύ των διαφορετικών δικτύων.

Η προστασία της ιδιωτικότητας των χρηστών είναι εξίσου σημαντική, προκειμένου να διασφαλιστεί ότι τα δεδομένα των χρηστών δεν εκτίθενται σε τρίτους. Επιπλέον, ο ισχυρός αμοιβαίος έλεγχος ταυτότητας, απαιτείται τόσο για τον έλεγχο της πρόσβασης όσο και για τη διευκόλυνση της τιμολόγησης. Τέλος, η σύγκλιση σταθερών και κινητών δικτύων είναι αναγκαία, ώστε οι ευρυζωνικές υπηρεσίες να είναι σε θέση να προσφέρουν την ίδια ασφάλεια είτε αυτές χρησιμοποιούνται μέσω σταθερής, είτε μέσω κινητής συνδεσιμότητας.

4.5 Μαζικό διαδίκτυο των πραγμάτων

Το δομικό στοιχείο mIoT (massive Internet of Things) αντιμετωπίζει περιπτώσεις χρήσης που περιλαμβάνουν έναν μεγάλο αριθμό συσκευών με μη κρίσιμης χρονικότητας μεταφορά δεδομένων, με έναν ευέλικτο και αποτελεσματικό τρόπο. Αυτές οι συσκευές, είτε πρόκειται για απλά εργαλεία είτε για περίπλοκα μηχανήματα, θα πρέπει να λαμβάνουν υπόψη την ασφάλεια κατά τη διαμόρφωσή τους. Το μαζικό διαδίκτυο των πραγμάτων, περιλαμβάνει έξυπνες φορητές συσκευές και δίκτυα αισθητήρων που χαρακτηρίζονται από χαμηλή πολυπλοκότητα, μεγάλη διάρκεια ζωής μπαταρίας, υψηλή αξιοπιστία και, ενίοτε, υψηλούς ρυθμούς δεδομένων. Παρά το ευρύ πεδίο εφαρμογής του διαδικτύου των πραγμάτων, οι απαιτήσεις ασφάλειας, αφορούν κυρίως περιπτώσεις χρήσης χαμηλού κόστους.

Με την αναμενόμενη σύνδεση μεγάλου αριθμού συσκευών που θα στέλνουν δεδομένα σποραδικά και σε μικρή κλίμακα, οι συσκευές αυτές αναμένεται να παραμένουν ενεργές για 10-15 χρόνια ή και ακόμη περισσότερο. Η ασφάλεια των δεδομένων και των αναγνωριστικών είναι κρίσιμης σημασίας. Παρά τη χαμηλή τιμή της συνδρομής στο δίκτυο, θα πρέπει σε κάθε περίπτωση να λαμβάνεται υπόψη ο κίνδυνος κατάχρησης αυτών των συσκευών, από υπερφόρτωση ή από αποστολή ανεπιθύμητων μηνυμάτων. Η ασφάλεια στο mIoT, απαιτείται για τη διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

Τα πρωτόκολλα ασφαλείας πρέπει να έχουν τέτοιες διαμορφώσεις και ρυθμίσεις που να επιτρέπουν τις συσκευές που λειτουργούν με μπαταρία να είναι ενεργειακά αποδοτικές, παρέχοντας υψηλό επίπεδο προστασίας με ελαχιστοποιημένα γενικά έξοδα. Το κόστος ασφαλείας πρέπει να παραμείνει χαμηλό, δεδομένου ότι πολλές συσκευές θα πρέπει να είναι οικονομικά αποδοτικές. Οι συσκευές mIoT μπορούν να έχουν πρόσβαση στο δίκτυο άμεσα ή έμμεσα μέσω ζωνών, με ή χωρίς άδεια χρήσης, απαιτώντας το τελικό σημείο ελέγχου ταυτότητας να βρίσκεται στον πυρήνα του δικτύου. Αυτή η πρακτική διασφαλίζει ότι χρησιμοποιούνται τα κατάλληλα διαπιστευτήρια για την πρόσβαση στην υπηρεσία, αποτρέποντας την κατάχρηση των χαμηλότερων μηχανισμών ασφαλείας δικτύων, όπως μπορεί για παράδειγμα να συμβεί στις τεχνολογίες Bluetooth και Wi-Fi.

Η ασφάλεια των δεδομένων είναι υψίστης σημασίας, ακόμα και όταν οι συσκευές mIoT συνδέονται μέσω διαμεσολαβητών, με επιπρόσθετους μηχανισμούς ελέγχου ταυτότητας και εξουσιοδότησης, για διάφορες μορφές σύνδεσης. Οι συσκευές mIoT πρέπει να επαληθεύουν την εξουσιοδότηση μιας συσκευής διαμεσολαβητή, που επωμίζεται αυτόν

τον ρόλο. Η ασφαλής παροχή διαπιστευτηρίων είναι κρίσιμη, καθώς η μαζική περιαγωγή πολλών συσκευών απαιτεί αποδοτικό κόστος. Τέλος, η επικοινωνία μεταξύ των συσκευών αλλά και ζητήματα που αφορούν σε συστάδες αυτών, θα πρέπει να αντιμετωπίζονται με μηχανισμούς ελέγχου ταυτότητας για την ομάδα συνολικά και να επικυρώνουν την ασφαλή ανταλλαγή των ίδιων δεδομένων μεταξύ τους (Παρασκευόπουλος, 2024).

4.6 Κρίσιμες επικοινωνίες

Οι κρίσιμες επικοινωνίες, περιλαμβάνουν περιπτώσεις χρήσης που απαιτούν εξαιρετικά χαμηλό λανθάνοντα χρόνο από άκρο σε άκρο, κυμαινόμενο από 1 ms έως 10 ms, ακόμα και σε περιπτώσεις υψηλής κινητικότητας. Η ασφάλεια της επικοινωνίας πρέπει να είναι ενσωματωμένη στο σύστημα, ήδη από τον σχεδιασμό του και να διασφαλίζει ταυτόχρονα τόσο την γρήγορη όσο και την αξιόπιστη ανταλλαγή δεδομένων. Τα πρότυπα του 3GPP περιλαμβάνουν τις λειτουργικές απαιτήσεις που είναι κρίσιμες για τις εφαρμογές του 5G και υποστηρίζουν εξαιρετικά υψηλή αξιοπιστία (99,999% ή υψηλότερη) και υψηλό ρυθμό δεδομένων ανερχόμενης ζεύξης (δεκάδες Mb/s ανά συσκευή σε πυκνά περιβάλλοντα). Το σύστημα πρέπει επίσης να υποστηρίζει τη δυναμική χρήση των πόρων του νέφους και την ακροδιαδικτυακή υπολογιστική, προσφέροντας υψηλή ακρίβεια εντοπισμού θέσης.

Οι CrIc επικοινωνίες απαιτούν ισχυρή ασφάλεια, καθώς σε περιπτώσεις όπως είναι για παράδειγμα οι περιπτώσεις αυτόνομης οδήγησης ή της απομακρυσμένης χειρουργικής επέμβασης, διακυβεύονται η ανθρώπινη ζωή. Η ανεπαρκής ασφάλεια ή οι καθυστερήσεις μπορεί να προκαλέσουν σημαντικές απώλειες. Η εμπιστευτικότητα και η ακεραιότητα των δεδομένων είναι ζωτικής σημασίας, καθώς η ισχυρή αμοιβαία πιστοποίηση εξασφαλίζει ότι πληρούνται οι απαιτήσεις χαμηλού λανθάνοντα χρόνου, χωρίς να διακυβεύεται το επίπεδο ασφάλειας (Mahyoub et al., 2023).

Συνοπτικά σε αυτά τα συστήματα θα πρέπει να λαμβάνονται υπόψιν τα παρακάτω:

- **Εμπιστευτικότητα δεδομένων:** Τα δεδομένα θα πρέπει να προστατεύονται τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση, τόσο στο δίκτυο όσο και στη συσκευή, για να διασφαλίζεται η προστασία του απορρήτου και να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση.
- **Ακεραιότητα δεδομένων:** Είναι σημαντικό να εξασφαλιστεί ότι τα δεδομένα δεν μπορούν να τροποποιηθούν με ανεπιθύμητο τρόπο. Η προέλευση και η αυθεντικότητα των δεδομένων θα πρέπει να επαληθεύονται.

- **Ισχυρή αμοιβαία πιστοποίηση:** Τα πρωτόκολλα ελέγχου ταυτότητας και η συχνότητα επαλήθευσής της, θα πρέπει να πληρούν τις απαιτήσεις χαμηλού λανθάνοντα χρόνου. Θα πρέπει να εφαρμόζονται αλγόριθμοι γρήγορης εκτέλεσης και βελτιστοποιημένα πρωτόκολλα, για να επιτευχθούν οι απαιτήσεις αυτές.
- **Αξιοπιστία μηχανισμών ασφάλειας:** Ισχυρά και επαληθευμένα πρωτόκολλα, καθώς και πιστοποιήσεις ασφαλείας, θα πρέπει να εξασφαλίζουν την αξιοπιστία των μηχανισμών ασφάλειας, χωρίς να επηρεάζουν αρνητικά τη συνολική αξιοπιστία του συστήματος.
- **Έλεγχος ταυτότητας μέσω τρίτων:** Σε κλειστά δίκτυα, θα πρέπει να υποστηρίζεται ο έλεγχος ταυτότητας μέσω τρίτων φορέων, πρακτική κατά την οποία, τα αναγνωριστικά και τα διαπιστευτήρια παρέχονται και διαχειρίζονται από το τρίτο μέρος.
- **Προτεραιότητα πρόσβασης δικτύου:** Ορισμένες συσκευές πρέπει να έχουν προτεραιότητα πρόσβασης στο δίκτυο, διασφαλίζοντας ότι οι συσκευές κρίσιμων επικοινωνιών έχουν εξουσιοδότηση προτεραιότητας και ότι καμία άλλη συσκευή δεν μπορεί να υπερκεράσει αυτήν την προτεραιότητα.

4.7 Πτυχές ασφαλείας που δεν καλύπτονται από το 5G

Εκτός από τις διάφορες ρυθμίσεις ασφαλείας που μπορεί να εισάγουν οι πάροχοι δικτύων μέσω του τεμαχισμού του δικτύου, είναι σημαντικό να ληφθούν υπόψη και οι απαιτήσεις ασφαλείας άλλων ενδιαφερομένων μερών. Αυτά τα μέρη περιλαμβάνουν τον καταναλωτή, τον πάροχο υπηρεσιών, τον πάροχο εφαρμογών, καθώς και τον κατασκευαστή του εξοπλισμού (OEM: Original Equipment Manufacturer).

Τα ακόλουθα σημεία δεν καλύπτονται από τη διαμόρφωση και τις απαιτήσεις ασφαλείας των 5G δικτύων, αλλά είναι απαραίτητο να υλοποιούνται και να λαμβάνονται υπόψιν, ώστε να μην διακυβεύονται η ασφάλεια και το απόρρητο στις επικοινωνίες:

- **Αναγνωριστικό συσκευής και κλειδί ασφαλείας:** Τα αναγνωριστικά της συσκευής και τα κλειδιά αναγνώρισης μπορούν να τοποθετηθούν μέσα σε ένα στοιχείο ασφαλείας (SE: Secure Element).

- **Ακεραιότητα συσκευής:** Το στοιχείο ασφαλείας μπορεί να χρησιμοποιηθεί για τον έλεγχο της ακεραιότητας της συσκευής, προσφέροντας λειτουργίες αξιόπιστης πλατφόρμας (TPM: Trusted Platform Module).
- **Πολλαπλές σήραγγες:** Μπορούν να δημιουργηθούν πολλαπλές σήραγγες (tunnels) για διαφορετικές εφαρμογές, υποδεικνύοντας ότι μπορούν να υπάρχουν πολλαπλοί πάροχοι υπηρεσιών και πολλαπλά κλειδιά.
- **Συνδυασμός προστασίας και αυθεντικοποίησης:** Η προστασία της ακεραιότητας και στο επίπεδο της υπηρεσίας, μπορεί να επιτευχθεί με την ταυτοποίηση και την αυθεντικοποίηση.
- **Διαχωρισμός επιπέδων δικτύου:** Όπως προαναφέρθηκε νωρίτερα, το δίκτυο διαχωρίζεται σε επίπεδο χρήστη και σε επίπεδο ελέγχου. Η ακεραιότητα και η κρυπτογράφηση του επιπέδου χρήστη, επεκτείνεται από τη συσκευή στον πάροχο υπηρεσιών, γεγονός που επιτυγχάνεται χρησιμοποιώντας διαφορετικό κλειδί συνεδρίας (Session key²¹). Στα συστήματα που ακολουθούν τα πρότυπα UMTS (Universal Mobile Telecommunications: Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών) και LTE, δεν παρέχεται προστασία ακεραιότητας δεδομένων, στο επίπεδο του χρήστη.
- **Παράγωγα κλειδιά:** Από το στοιχείο ασφαλείας και τη δικτυακή οντότητα μπορούν να δημιουργηθούν επιπρόσθετα κλειδιά, τα οποία παρέχουν επιπλέον υλικό και αυξημένη ασφάλεια. Αυτά τα επιπρόσθετα κλειδιά βασίζονται στο κύριο κλειδί ασφαλείας που κατέχει ο χειριστής του δικτύου [η οντότητα δηλαδή που κατέχει και ελέγχει το αρχικό κλειδί ασφαλείας (το οποίο χρησιμοποιείται για τη δημιουργία των επιπρόσθετων κλειδιών) και είναι υπεύθυνη για την ασφάλεια του δικτύου]. Η ασφάλεια της ραδιοπρόσβασης μπορεί να ενισχυθεί ανάλογα με την ασφάλεια που παρέχεται στα ανώτερα επίπεδα του δικτύου. Επιπλέον, η διεπαφή πρέπει να

²¹ Το Session key ή κλειδί συνεδρίας, είναι ένα μοναδικό κρυπτογραφικό κλειδί που δημιουργείται και χρησιμοποιείται κατά τη διάρκεια μιας συγκεκριμένης συνεδρίας επικοινωνίας, ανάμεσα σε δύο ή περισσότερες συσκευές ή εφαρμογές. Χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται κατά τη διάρκεια της συνεδρίας, εξασφαλίζοντας το απόρρητο και την ακεραιότητα των επικοινωνιών.

αναγνωρίζει αυτή τη διαμόρφωση για να εξασφαλιστεί η συνολική ασφάλεια του συστήματος.

4.8 Ασφάλεια συσκευών IoT

Η ασφάλεια των IoT συσκευών (IoT Device Security) αποτελεί κρίσιμο ζήτημα στον σύγχρονο ψηφιακό κόσμο, καθώς οι συσκευές αυτές ενσωματώνονται ολοένα και περισσότερο στην καθημερινή ζωή και στις επιχειρηματικές δραστηριότητες της σύγχρονης κοινωνίας. Οι συσκευές IoT, οι οποίες περιλαμβάνουν αισθητήρες, κάμερες, έξυπνες συσκευές και πολλά άλλα, συχνά διασυνδέονται μέσω των 5G δικτύων για την ανταλλαγή δεδομένων σε πραγματικό χρόνο. Ωστόσο, η αυξανόμενη χρήση τους δημιουργεί νέες προκλήσεις ασφαλείας, καθώς οι συσκευές αυτές συχνά δεν έχουν επαρκείς μηχανισμούς προστασίας. Η διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων, που μεταδίδονται και αποθηκεύονται σε αυτές, είναι ουσιώδης για την αποτροπή μιας μη εξουσιοδοτημένης πρόσβασης, καθώς και των κακόβουλων επιθέσεων.

Τα δίκτυα 5G, παρέχοντας υψηλές ταχύτητες και χαμηλή καθυστέρηση, προσφέρουν σημαντικές δυνατότητες για την ανάπτυξη του διαδικτύου των πραγμάτων, εισάγοντας ωστόσο, νέες απειλές και προκλήσεις ασφαλείας. Η ευελιξία και η πολυπλοκότητα των δικτύων 5^{ης} γενιάς απαιτούν νέες προσεγγίσεις, προκειμένου οι μηχανισμοί ασφαλείας να είναι ενσωματωμένοι από την αρχή του σχεδιασμού των δικτύων αυτών, ώστε να διασφαλιστεί ότι οι επικοινωνίες παραμένουν προστατευμένες από άκρο-σε-άκρο. Αυτό περιλαμβάνει την χρήση ισχυρής κρυπτογράφησης, την ασφαλή διαχείριση ταυτοτήτων και διαπιστευτηρίων, καθώς και τη συνεχή παρακολούθηση και ανάλυση των δεδομένων, για την ανίχνευση και την αποτροπή πιθανών απειλών.

Η συνδυασμένη ασφάλεια των IoT συσκευών και των δικτύων 5G είναι απαραίτητη για την ανάπτυξη ασφαλών και αξιόπιστων οικοσυστημάτων IoT. Οι οργανισμοί πρέπει να υιοθετήσουν προσεγγίσεις ασφαλείας πολλαπλών επιπέδων, που περιλαμβάνουν τόσο την φυσική ασφάλεια των συσκευών όσο και την προστασία των δεδομένων που μεταδίδονται μέσω των δικτύων. Επιπλέον, η συνεργασία μεταξύ των κατασκευαστών των συσκευών, των παρόχων δικτύων και των χρηστών είναι κρίσιμη για την ανάπτυξη κοινών προτύπων και πρωτοκόλλων ασφαλείας, που θα επικυρώνουν την ασφάλεια και την αξιοπιστία των IoT εφαρμογών (GSMA, 2020).

ΚΕΦΑΛΑΙΟ 5 : ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΛΥΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ

5.1 Προστασία στον τεμαχισμό δικτύου

Ο κατακερματισμός ενός δημόσιου δικτύου κινητής τηλεφωνίας (PLMN: Public Land Mobile Network) δεν πρέπει να είναι αντιληπτός από τον εξοπλισμό του χρήστη μέσω της διεπαφής ραδιοεπικοινωνίας και θεωρείται ότι η απομόνωση δεν επεκτείνεται στον εξοπλισμό του χρήστη. Με αυτήν την προϋπόθεση, το NGMN Forum πραγματοποίησε ανάλυση ασφαλείας και εξέδωσε συστάσεις για την ασφάλεια στον τεμαχισμό δικτύου. Τα κύρια ζητήματα που θα πρέπει να ληφθούν υπόψη περιλαμβάνουν:

- Την προστασία των διασυνδέσεων των τεμαχίων δικτύου και των λειτουργιών τους για την επικοινωνία των τεμαχίων κατά την εργασία στο διαδίκτυο.
- Την πρόληψη των επιθέσεων πλαστοπροσωπίας κατά τη λειτουργία επιλογής του τεμαχισμού του δικτύου.
- Την πρόληψη επιθέσεων πλαστοπροσωπίας σε ένα τεμάχιο δικτύου.
- Κατάλληλους μηχανισμούς για τη διασφάλιση της παροχής επαρκούς προστασίας όταν εφαρμόζονται διαφορετικά πρωτόκολλα ή πολιτικές, σε διαφορετικά τεμάχια του δικτύου.
- Την προστασία έναντι των DoS επιθέσεων που εκμεταλλεύονται κοινούς πόρους πολλαπλών τεμαχίων.
- Την πρόληψη των επιθέσεων πλαϊνού καναλιού και χρονισμού, όταν πολλά τεμάχια διαμοιράζονται την ίδια υποκείμενη υποδομή.
- Την εξέταση υβριδικών μοντέλων ανάπτυξης, δηλαδή το συνδυασμό εικονικοποιημένων και μη εικονικοποιημένων λειτουργιών δικτύου.
- Την παροχή μηχανισμών ασφαλείας εντός του δικτύου ή ενδεχομένως εντός του εξοπλισμού του χρήστη, για την απομόνωση μεταξύ των τεμαχίων όταν ο εξοπλισμός του χρήστη είναι διασυνδεδεμένος με πολλά τεμάχια.

Ο τεμαχισμός δικτύου, απαιτεί την εφαρμογή βασικών μέτρων ασφαλείας στον εξοπλισμό του χρήστη κατά την ασφαλή πρόσβαση στα τεμάχια. Επιπλέον, είναι απαραίτητο να διασφαλίζεται η απομόνωση μεταξύ των τεμαχίων, ώστε, σε περίπτωση παραβίασης ενός τεμαχίου, να μην είναι δυνατή η πρόσβαση σε άλλα. Η απομόνωση διασφαλίζει την

ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Είναι επίσης σημαντικό οι πόροι, είτε αυτοί σχετίζονται με το δίκτυο είτε με την παρουσία του τεμαχίου, να παραμένουν ασφαλείς, ακόμη και αν κάποιο τεμάχιο δέχεται επίθεση.

Στο 5G, ο εξοπλισμός χρήστη μπορεί να χρησιμοποιεί διάφορους πόρους μέσω του δικτύου 5ης γενιάς, αλλά και μέσω άλλων δικτύων εκτός 3GPP, παρέχοντας διάφορες υπηρεσίες. Εάν παραβιαστούν τα δεδομένα του ενός τεμαχίου, ένας μη εξουσιοδοτημένος χρήστης μπορεί να προσπαθήσει να εκμεταλλευτεί τους πόρους του τεμαχίου, κάτι που πρέπει να αποτρέπεται από τον διαχειριστή του δικτύου.

Ένα από τα πλεονεκτήματα του τεμαχισμού δικτύου είναι η δυνατότητα καθορισμού διαφορετικών επιπέδων ασφάλειας ανά τεμάχιο. Αυτό περιλαμβάνει τον έλεγχο ταυτότητας και την εξουσιοδότηση πρόσβασης των χρηστών, καθώς και τη χρήση συγκεκριμένων λειτουργιών ασφαλείας για την υποστήριξη των εφαρμογών. Αυτή η προσέγγιση βελτιστοποιεί την απόδοση του δικτύου προκειμένου να μπορούν να καλυφθούν πολλές και διαφορετικές περιπτώσεις χρήσης. Για παράδειγμα, οι κρίσιμες επικοινωνίες (CtIC) μπορεί να απαιτούν ισχυρότερη προστασία σε σχέση με το μαζικό mIoT. Ωστόσο, η αυξημένη προστασία απαιτεί περισσότερους πόρους και μπορεί να επηρεάσει τον χρόνο απόκρισης. Συνεπώς, είναι ευθύνη του διαχειριστή να βελτιστοποιήσει το δίκτυο κατάλληλα (Olimid et al., 2020).

5.2 Προστασία του υπολογισμού στο άκρο του δικτύου

Όπως προαναφέρθηκε, με την εισαγωγή του edge computing και της εικονικοποίησης, οι λειτουργίες δικτύου και το περιεχόμενο, έρχονται πιο κοντά στους καταναλωτές. Αυτό συνεπάγεται την αναπαραγωγή και διάθεση των λειτουργιών δικτύου και του περιεχομένου, σε περιβάλλοντα που είναι λιγότερο προστατευμένα από ότι είναι ο κεντρικός πυρήνας του δικτύου.

Οι άκρες του δικτύου πρέπει να ανακτήσουν μια εκδοχή της λειτουργίας του δικτύου από τον πυρήνα, να προσφέρουν το περιεχόμενο στον χρήστη με μειωμένη καθυστέρηση και να αποθηκεύσουν προσωρινά το περιεχόμενο και τα δεδομένα που παρέχονται από τα τρίτα μέρη. Για να εξασφαλιστεί ότι το άκρο είναι εξουσιοδοτημένο να λαμβάνει αυτές τις λειτουργίες ή/και το περιεχόμενό τους, απαιτείται έλεγχος ταυτότητας μεταξύ των εμπλεκόμενων δικτυακών οντοτήτων. Επιπλέον, τα δεδομένα που ανταλλάσσονται μεταξύ αυτών των οντοτήτων, πρέπει να προστατεύονται τόσο κατά την αποθήκευση όσο και κατά

τη μετάδοση. Αυτό μπορεί να επιτευχθεί μέσω μηχανισμών ασφαλείας, που βασίζονται είτε στο λογισμικό είτε στο υλικό.

Δεδομένου ότι η εικονικοποίηση είναι σημαντική για το 5G, αναμένεται ότι οι τεχνολογίες εικονικοποίησης, όπως οι επόπτες και οι τεχνικές απομόνωσης, θα αποτελέσουν επίσης τη βάση των μηχανισμών ασφαλείας στα άκρα του δικτύου. Ωστόσο, είναι λογικό να προστεθούν μονάδες ασφαλείας υλικού (HSM: Hardware Security Modules) σε οντότητες δικτύου που είναι ευάλωτες σε εισβολή, προκειμένου να βελτιωθούν τόσο η απόδοση όσο και η ασφάλεια. Σύμφωνα με τους Hassan et al. (2018) και Merino et al. (2020), τα HSM παρέχουν ασφαλή διαχείριση διαπιστευτηρίων και μπορούν να χρησιμοποιηθούν για την αποθήκευση και την ανάκτηση διανυσμάτων ελέγχου ταυτότητας, που απαιτούνται για τον έλεγχο ταυτότητας πρόσβασης στο δίκτυο.

5.3 Λύσεις ασφάλειας στις φορητές συσκευές

Η πλειονότητα των προτεινόμενων λύσεων ασφάλειας για φορητές συσκευές στο υπολογιστικό νέφος, περιλαμβάνει την επανεξέταση των τεχνικών κρυπτογράφησης, τη δυναμική κατανομή της επεξεργασίας δεδομένων και τη στρατηγική χρήση τεχνολογιών εικονικοποίησης. Επειδή κάθε τελικός κόμβος συνδέεται μέσω μιας εικονικής μηχανής με μια ξεχωριστή εικονική παρουσία στο νέφος, η εικονικοποίηση εγγυάται την ασφάλεια των υπηρεσιών υπολογιστικού νέφους. Οπότε, διαχωρίζοντας την εικονική σύνδεση κάθε χρήστη από άλλους χρήστες, παρέχεται η απαιτούμενη ασφάλεια. Επιπλέον, οι τεχνολογίες υπολογιστικού νέφους μπορούν να χρησιμοποιηθούν με ασφάλεια, χάρη στην περιορισμένη πρόσβαση που προσφέρεται από αυτές.

Στην εποχή του 5G, μια καινοτόμος κάρτα SIM πρέπει να είναι επεκτάσιμη, να έχει ένα ευρύ φάσμα τεχνικών δυνατοτήτων και να παρέχει την καλύτερη δυνατή ασφάλεια με βάση τις απαιτήσεις κάθε περίπτωσης χρήσης. Το κόστος των επιβλαβών επιθέσεων θα πρέπει να υπερβαίνει το πιθανό όφελος. Οι καθολικές κάρτες ολοκληρωμένου κυκλώματος: eUICC (Embedded Universal Integrated Circuit Card), iUICC (Integrated Universal Integrated Circuit Card) και vUICC (Virtual Universal Integrated Circuit Card) είναι παραλλαγές που υποστηρίζουν μια ποικιλία λειτουργιών και υπηρεσιών, εκτός από τη συμβατική SIM/USIM. Η εφαρμογή τους εξαρτάται από την προθυμία των παρόχων κινητής τηλεφωνίας να τις υιοθετήσουν. Η ενσωμάτωση νέων μέτρων ασφαλείας σε προηγμένες SIM απαιτεί συνεργασία μεταξύ των παρόχων τεχνολογίας, συμπεριλαμβανομένων των κατασκευαστών chipset και των παρόχων υποδομής δικτύου. Η ανάπτυξη αυτών των λύσεων

καθοδηγείται κυρίως από τους δεύτερους. Αυτού του είδους οι λύσεις θα αλλάξουν όχι μόνο την τεχνολογία αλλά και τις συμβατικές μεθόδους συνεργασίας των ενδιαφερομένων.

Το μοντέλο της λειτουργικής και πιστοποιημένης εμπιστοσύνης, είναι κρίσιμης σημασίας για να διασφαλιστεί ότι οι νέες λύσεις είναι τουλάχιστον εξίσου ασφαλείς, αν όχι περισσότερο, από τις προηγούμενες παραλλαγές UICC. Μέχρι τώρα, η ασφάλεια των δικτύων κινητής τηλεφωνίας βασιζόταν σε μια αλυσίδα εμπιστοσύνης, επιτρέποντας στους παρόχους υπηρεσιών κινητής τηλεφωνίας να εμπιστεύονται τους προμηθευτές καρτών. Αυτοί με τη σειρά τους, θα έπρεπε να είναι πιστοποιημένοι και να τηρούν τις αυστηρές προδιαγραφές για την ασφαλή διατήρηση των πληροφοριών σε φυσική και λογική μορφή, μέσω συγκεκριμένων διαδικασιών ασφαλείας.

Με την ανάπτυξη των 5G συστημάτων, ο ρόλος και το μοντέλο ιδιοκτησίας της πλατφόρμας ασφαλείας εντός της συσκευής, καθιστούν την εξελιγμένη SIM ένα σημαντικό σημείο ασφαλείας για όλους τους ενδιαφερόμενους, όπως είναι για παράδειγμα οι κατασκευαστές συσκευών και οι πάροχοι εφαρμογών. Αυτά τα νέα μοντέλα ιδιοκτησίας μπορεί να επιτρέψουν την πρόσβαση στην εξελιγμένη SIM, σε όλους όσους χρειάζονται ασφάλεια στα τελικά σημεία, δηλαδή σε απομακρυσμένες υπολογιστικές συσκευές που συνδέονται με ένα δίκτυο.

Οι μελλοντικές παραλλαγές της εξελιγμένης SIM, που θα περιλαμβάνουν διάφορες λύσεις ασφαλείας, όπως ενσωματωμένες και ολοκληρωμένες SIM για τα τελικά σημεία, πιθανόν να απαιτούν ένα ευέλικτο και εικονικοποιημένο σύστημα διαχείρισης ασφαλείας διακομιστή. Βασικές τεχνολογίες για την κάλυψη αυτών των νέων απαιτήσεων, περιλαμβάνουν τη διαχείριση συσκευών από τις πλατφόρμες over-the-air (OTA). Οι τεχνολογίες αυτές, υποστηρίζουν διάφορους μηχανισμούς ελέγχου ταυτότητας και τύπους διαπιστευτηρίων ασφαλείας, σε επίπεδο δικτύου, εφαρμογής και συσκευής, επιτρέποντας την ενημέρωση και την αλλαγή δεδομένων στην κάρτα SIM, χωρίς να απαιτείται η φυσική αντικατάστασή της.

Η πλατφόρμα OTA διαχειρίζεται και εξασφαλίζει τη συνδεσιμότητα όλων των συσκευών, παρέχοντας τα μέγιστα επίπεδα ασφαλείας, ανεξάρτητα από το κανάλι επικοινωνίας (SMS, HTTP ή και τα δύο) ή την τεχνολογία δικτύου. Αυτή η προηγμένη λύση, επιτρέπει στους παρόχους κινητής τηλεφωνίας, να αξιοποιήσουν την HTTP τεχνολογία σε

οποιοδήποτε κανάλι, ανοίγοντας νέες δυνατότητες υπηρεσιών, όπως το απόρρητο της ταυτότητας των συνδρομητών, η κατεύθυνση περιαγωγής (Steering of Roaming²²) και το διαδίκτυο των πραγμάτων. Αυτά τα συστήματα μπορούν να προσαρμοστούν για να εξυπηρετήσουν την αναδυόμενη αγορά των κλειστών δικτύων, που μπορεί να ανήκουν και να διαχειρίζονται από εργοστάσια ή επιχειρήσεις.

Η διαχείριση της ταυτότητας ενός μεγάλου αριθμού καταναλωτών και συσκευών IoT είναι κρίσιμη για την παροχή ασφάλειας σε όλα τα νέα περιβάλλοντα που δημιουργούνται από κλειστά δίκτυα. Εκτός από τα καταναλωτικά δίκτυα, τα τυπικά IoT δίκτυα και τα δίκτυα αισθητήρων, υπάρχουν και πολλά άλλα περιβάλλοντα όπως είναι τα Κυβερνοφυσικά Συστήματα (CPS: Cyber-Physical System²³) που αναφέρονται σε βιομηχανικές υποδομές και στην ασφαλή λειτουργία, συντήρηση και στις τηλεματικές επικοινωνίες, μεταξύ του εξουσιοδοτημένου προσωπικού και του εξοπλισμού. Αυτές οι λύσεις μπορούν να αναπτυχθούν για την προστασία της υποδομής δικτύου, της επικοινωνίας και του ελέγχου ταυτότητας, μεταξύ των δικτυακών οντοτήτων (Kron Technologies, 2022; Liyanage et al., 2018).

5.4 Προηγμένες τεχνολογίες ασφάλειας

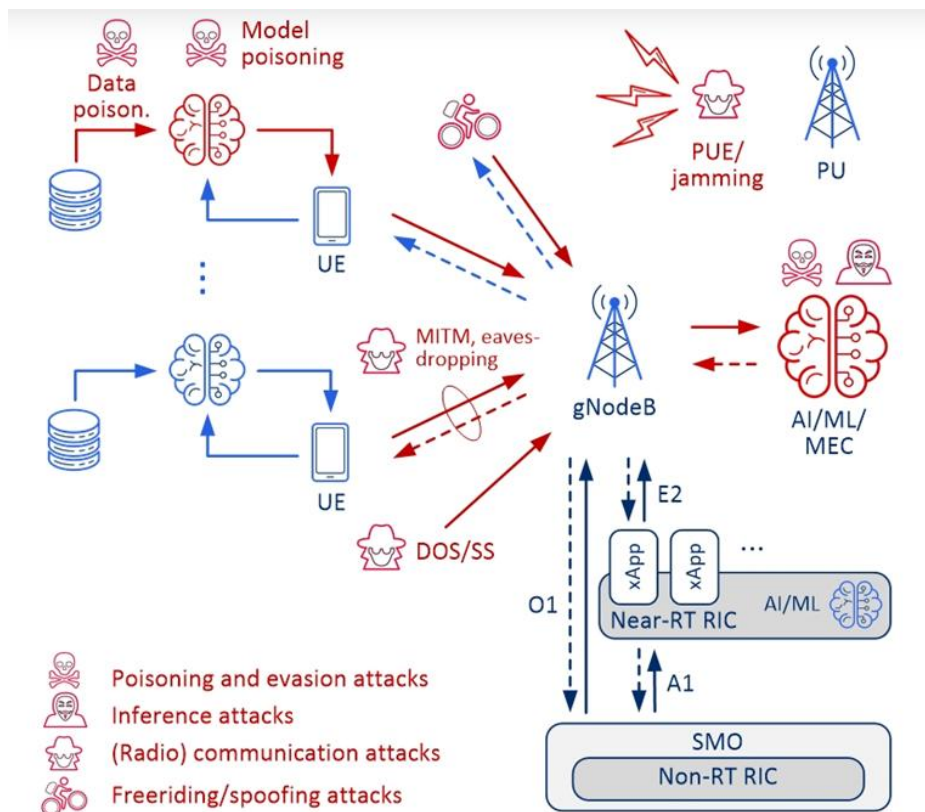
Η ανάπτυξη των 5G δικτύων, φέρνει μαζί της νέες προκλήσεις και απαιτήσεις στην ασφάλεια. Η χρήση προηγμένων τεχνολογιών, όπως η Τεχνητή Νοημοσύνη (AI: Artificial Intelligence) και η Μηχανική Μάθηση (ML: Machine Learning) μπορεί να παίξει κρίσιμο ρόλο στην προστασία αυτών των δικτύων. Τα 5G δίκτυα είναι πιο πολύπλοκα και ευέλικτα από τους προκατόχους τους, γεγονός που αυξάνει την επιφάνεια επιθέσεων και την πιθανότητα απειλών. Οι νέες αυτές τεχνολογίες μπορούν να χρησιμοποιηθούν για την ανίχνευση ανωμαλιών, την πρόβλεψη επιθέσεων και την αυτοματοποιημένη απόκριση σε απειλές σε πραγματικό χρόνο, επιτρέποντας την καλύτερη προστασία των δικτύων.

²² Είναι η διαδικασία με την οποία ένας πάροχος κινητής τηλεφωνίας καθοδηγεί τη συσκευή ενός συνδρομητή, να συνδεθεί με συγκεκριμένα δίκτυα συνεργατών, όταν αυτός βρίσκεται σε περιαγωγή, με στόχο τη βέλτιστη χρήση των συνεργαζόμενων δικτύων και τη μείωση του κόστους

²³ Πρόκειται για συστήματα που ενσωματώνουν υπολογιστικές δυνατότητες και φυσικές διαδικασίες, επιτρέποντας την ασφαλή και αξιόπιστη αλληλεπίδραση μεταξύ ψηφιακών και φυσικών στοιχείων.

Οι λύσεις που βασίζονται στη μηχανική μάθηση υπερτερούν έναντι των γενικών τρόπων αντιμετώπισης συγκεκριμένων κινδύνων ασφαλείας, όπως οι επιθέσεις HX-DoS (Hypertext Denial of Service). Τα Συστήματα Μηχανικής Μάθησης (MLS: Machine Learning System) χρησιμοποιούν χαρακτηριστικά των δεδομένων, για να εκπαιδευτούν και να αναλύσουν δείγματα πακέτων προκειμένου να ανιχνεύσουν και να μετριάσουν τους κινδύνους.

Μία από τις κύριες εφαρμογές της ΑΙ και της ΜΛ στα 5G δίκτυα είναι η ανάλυση συμπεριφοράς. Μέσω της συνεχούς παρακολούθησης των δικτυακών δραστηριοτήτων, τα συστήματα που βασίζονται στην ΑΙ μπορούν να εντοπίσουν ανωμαλίες που μπορεί να υποδεικνύουν κακόβουλες δραστηριότητες. Αυτή η διαδικασία περιλαμβάνει τη συλλογή μεγάλου όγκου δεδομένων και τη χρήση αλγορίθμων ΜΛ για την ανάλυσή τους. Τα συστήματα αυτά μπορούν να αναγνωρίσουν μοτίβα επιθέσεων και να ενεργοποιήσουν αυτόματες αποκρίσεις, μειώνοντας τον χρόνο αντίδρασης και περιορίζοντας μ' αυτό τον τρόπο τις επιπτώσεις των επιθέσεων. Μπορούν να χρησιμοποιηθούν για την ανακάλυψη μοτίβων σε ένα πλήθος επιθέσεων, όπως απεικονίζεται στο παρακάτω σχήμα:



Εικόνα 13: Χρήση των ΑΙ και ΜΛ τεχνολογιών για την ανακάλυψη ανωμαλιών, που μπορεί να υποδεικνύουν κακόβουλες δραστηριότητες σε μια πληθώρα επιθέσεων

Πηγή: Bogucka, 2022

Επιπλέον, οι τεχνολογίες AI και ML μπορούν να ενισχύσουν την ασφάλεια των 5G δικτύων, μέσω της ενίσχυσης της κρυπτογράφησης και της διαχείρισης ταυτοτήτων. Οι αλγόριθμοι ML μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση των πρωτοκόλλων κρυπτογράφησης, κάνοντας πιο δύσκολη την παραβίαση των δεδομένων. Επίσης, μπορούν να βοηθήσουν στη διαχείριση των ταυτοτήτων των χρηστών και των συσκευών, εξασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες και συσκευές έχουν πρόσβαση στο δίκτυο. Έτσι, οι νέες αυτές τεχνολογίες προσφέρουν ισχυρές λύσεις για την ασφάλεια και την προστασία των 5G δικτύων, εξασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των δεδομένων (Haider et al., 2020).

5.5 Γενικές λύσεις ασφάλειας

Οι προκλήσεις της διαχείρισης της αυξημένης κυκλοφορίας δικτύου μπορούν να αντιμετωπιστούν, είτε με την προσθήκη νέων πόρων, είτε με την αξιοποίηση των υφιστάμενων υποδομών μέσω νέων τεχνολογιών. Τεχνολογίες όπως το SDN και το NFV μπορούν να προσφέρουν λύσεις σε αυτές τις προκλήσεις χωρίς υψηλό κόστος. Το SDN επιτρέπει τη δυναμική κατανομή πόρων, όπως το εύρος ζώνης, σε συγκεκριμένα τμήματα του δικτύου βάσει των εκάστοτε αναγκών. Ο ελεγκτής SDN μπορεί να συλλέγει στατιστικά στοιχεία μέσω κατάλληλης διεπαφής από τον δικτυακό εξοπλισμό προκειμένου να παρακολουθεί την αύξηση της κυκλοφορίας. Με τη χρήση του NFV, οι υπηρεσίες μπορούν να μεταφερθούν από το κεντρικό σύννεφο δικτύου στην άκρη, για να ικανοποιήσουν τις απαιτήσεις των χρηστών. Επιπλέον, εικονικά τεμάχια του δικτύου μπορούν να αφιερωθούν σε περιοχές με υψηλή πυκνότητα χρηστών, για να αντιμετωπιστεί η απότομη αύξηση της κυκλοφορίας.

Η διασφάλιση της ακεραιότητας και του απορρήτου των κλειδιών στη διεπαφή ραδιοπρόσβασης παραμένει πρόκληση, καθώς απαιτείται η ασφαλής ανταλλαγή των κρυπτογραφημένων κλειδιών, όπως γίνεται για παράδειγμα μέσω της χρήσης του πρωτοκόλλου ταυτότητας υποδοχής (HIP: Host Identity Protocol). Η ακεραιότητα των δεδομένων στο επίπεδο του χρήστη, μπορεί να προστατευθεί με τεχνολογίες κρυπτογράφησης. Από την άλλη, κατά την περιαγωγή, μπορούν να εφαρμοστούν πολιτικές ασφαλείας για την προστασία του δικτύου μέσω κεντρικών συστημάτων, τα οποία παρέχουν παγκόσμια εποπτεία της δραστηριότητας των χρηστών και της κυκλοφορίας του δικτύου (Liyana et al., 2020).

Συμπεράσματα

Οι προκλήσεις για την ασφάλεια από άκρο σε άκρο στα 5G δίκτυα είναι πολλές και ποικίλες. Τα νέα πρότυπα και οι τεχνολογίες απαιτούν συνεχή παρακολούθηση και ενημέρωση των πολιτικών ασφάλειας. Επιπλέον, η αύξηση του αριθμού των συνδεδεμένων συσκευών και των εφαρμογών, δημιουργεί νέες επιφάνειες επίθεσης που πρέπει να προστατευθούν. Οι πάροχοι δικτύων πρέπει να υιοθετήσουν μια πολυεπίπεδη προσέγγιση στην ασφάλεια, που περιλαμβάνει τόσο την πρόληψη όσο και την ανίχνευση και τη γρήγορη απόκριση σε απειλές. Η συνεργασία με εταίρους και η συμμετοχή σε προγράμματα τυποποίησης, είναι επίσης κρίσιμες για την αντιμετώπιση των προκλήσεων ασφάλειας στα δίκτυα αυτά.

Η αξιολόγηση της απόδοσης των μέτρων ασφάλειας στα 5G δίκτυα αποτελεί κρίσιμο βήμα για τη διασφάλιση της αξιοπιστίας και της προστασίας των δεδομένων. Με την εισαγωγή των 5G δικτύων, οι απαιτήσεις για ασφάλεια γίνονται πιο περίπλοκες λόγω της αυξημένης ταχύτητας, της χαμηλής καθυστέρησης και της μεγάλης συνδεσιμότητας. Η αποτελεσματικότητα των μέτρων ασφαλείας πρέπει να αξιολογείται συνεχώς, για να διασφαλίζεται ότι τα δίκτυα παραμένουν προστατευμένα από σύγχρονες και αναδυόμενες απειλές. Τα συστήματα ανίχνευσης και απόκρισης σε απειλές, οι τεχνολογίες κρυπτογράφησης και οι μηχανισμοί ελέγχου ταυτότητας, αποτελούν βασικά στοιχεία που πρέπει να παρακολουθούνται και να βελτιστοποιούνται διαρκώς.

Μία από τις κύριες προκλήσεις στην αξιολόγηση της απόδοσης των μέτρων ασφάλειας, είναι η διαχείριση της πολυπλοκότητας και της ευελιξίας του δικτύου. Οι τεχνολογίες της εικονικοποίησης των δικτυακών λειτουργιών και η χρήση των δικτύων που βασίζονται στο λογισμικό, επιτρέπουν την ευέλικτη διαχείριση τους, αλλά ταυτόχρονα δημιουργούν νέες επιφάνειες επιθέσεων. Οι προηγμένες τεχνολογίες, όπως της τεχνητής νοημοσύνης και της μηχανικής μάθησης, μπορούν να χρησιμοποιηθούν για την αξιολόγηση της απόδοσης των μέτρων ασφάλειας σε πραγματικό χρόνο, ανιχνεύοντας ανωμαλίες και αποκλίσεις στη συμπεριφορά του δικτύου, προκειμένου να προσαρμόζουν τις στρατηγικές ασφάλειας αναλόγως.

Για την αποτελεσματική προστασία των 5G δικτύων, είναι απαραίτητη η υιοθέτηση πολυεπίπεδων λύσεων ασφάλειας. Αυτές οι λύσεις περιλαμβάνουν την κρυπτογράφηση δεδομένων, την ενισχυμένη ασφάλεια στη διεπαφή ραδιοπρόσβασης και τη δυναμική διαχείριση ταυτοτήτων. Επιπλέον η συνεργασία, μεταξύ των παρόχων υπηρεσιών δικτύου και

των κατασκευαστών εξοπλισμού, είναι ζωτικής σημασίας για την ανάπτυξη ολοκληρωμένων λύσεων που θα προστατεύουν τα 5G δίκτυα από τις συνεχώς εξελισσόμενες απειλές.

Βιβλιογραφία

Ξένη

- Abood, M. S., Wang, H., Virdee, B. S., He, D., Fathy, M., Yusuf, A. A., Jamal, O., Elwi, T. A., Alibakhshikenari, M., Kouhalvandi, L., & Ahmad, A. (2024). Improved 5G network slicing for enhanced QoS against attack in SDN environment using deep learning. *IET Communications*. <https://doi.org/10.1049/cmu2.12735>
- Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions. Conference Paper. <https://doi.org/10.1109/CSCN.2017.8088621>
- Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. *IEEE Communications Standards Magazine*. <https://doi.org/10.1109/MCOMSTD.2018.1700063>
- Ancans, G., Staflecka, A., Bobrovs, V., Ancans, A., & Caiko, J. (2017). Analysis of characteristics and requirements for 5G mobile communication systems. *Latvian Journal of Physics and Technical Sciences*, 2017(4). <https://doi.org/10.1515/lpts-2017-0028>
- Barakabitze, A. A., Ahmad, A., Mijumbi, R., & Hines, A. (2020). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures, and future challenges. *Computer Networks*, 167, 106984. <https://doi.org/10.1016/j.comnet.2019.106984>
- Cao, J., Ma, M., Li, H., Ma, R., Sun, Y., Yu, P., & Xiong, L. (2019, November). A survey on security aspects for 3GPP 5G networks. *IEEE Communications Surveys & Tutorials*, 22(1), First Quarter 2020. <https://doi.org/10.1109/COMST.2019.2951818>
- ENISA a. (2022). 5G CYBERSECURITY STANDARDS. Analysis of standardisation requirements in support of cybersecurity policy. <https://www.enisa.europa.eu/publications/5g-cybersecurity-standards>
- ENISA b. (The European Union Agency for Cybersecurity). (2022). NFV Security in 5G - Challenges and Best Practices. <https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices>
- Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Hani, I. B., Alkhalailah, M., & Hamad, F. (2023). A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions. *Electronics*, 12(4604). <https://doi.org/10.3390/electronics12224604>
- Foukas, X., Elmokashfi, A., Patounas, G., & Marina, M. K. (2017). Network slicing in 5G: Survey and challenges. *IEEE Communications Magazine*, 55(5), 94-100. <https://doi.org/10.1109/MCOM.2017.1600951>
- Garg, V. K. (2008). *Wireless Communications and Networking*. Morgan Kaufmann.
- GSMA. (2020, February 29). IoT Security Guidelines Overview Document (Version 2.2). <https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf>

- Haider, N., Baig, Z., & Imran, M. (2020). Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends. arXiv:2007.04490v1
- Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., Abdel-Khalek, S., & Alkassawneh, H. M. (2021). A review on security threats, vulnerabilities, and counter measures of 5G enabled internet-of-medical-things. *IET Communications*, 16, 421–432. <https://doi.org/10.1049/cmu2.12301>
- Hassan, N., Gillani, S., Ahmed, E., Yaqoob, I., & Imran, M. (2018). The role of edge computing in Internet of Things. *IEEE*.
- Hussain, F., Ferdouse, L., Anpalagan, A., Karim, L., & Woungang, I. (n.d.). Security Threats in M2M Networks: A Survey with Case Study. <https://doi.org/10.1002/>
- Kareem, K. M. (2024). The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9), 3871-3879. <https://doi.org/10.7910/DVN/6JPQWO>
- Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*. <https://doi.org/10.1109/COMST.2019.2933899>
- Koca, M., & Avci, İ. (2023). Overview of 5G architecture security. In *International Khazar Scientific Researches Conference - IV*, 1-3 March 2023, Khazar University.
- Kumar, P., & Sumit. (2021). Review Paper on Development of Mobile Wireless Technology. *Journal of Physics: Conference Series*, 1979, 012024. <https://doi.org/10.1088/1742-6596/1979/1/012024>
- Lee, D., Moon, H., Oh, S., Park, D. (2020). mIoT: Metamorphic IoT Platform for On-Demand Hardware Replacement in Large-Scaled IoT Applications. *Sensors*. 2020; 20(12):3337. <https://doi.org/10.3390/s2012333>
- Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (2018). A Comprehensive Guide to 5G Security. <https://doi.org/10.1002/9781119293071.fmatter>
- Magri, H., Magri, H., Abghour, N., Abghour, N., & Ouzzif, M. (2018). 5G mobile networks based on SDN concepts. *International Journal of Engineering & Technology*, 7(4), 2231-2235. <https://doi.org/10.14419/ijet.v7i2.18.12194>
- Mahyoub, M., Abdulghaffar, A., Alalade, E., & Matrawy, A. (2023). Security analysis of critical 5G interfaces. *TechRxiv*. Advance online publication. <https://doi.org/10.36227/techrxiv.24069600.v1>
- Merino, P., Mujica, G., Señor, J., & Portilla, J. (2020). A modular IoT hardware platform for distributed and secured extreme edge computing. *Electronics*, 9(3), 538. <https://doi.org/10.3390/electronics9030538>
- NSA & CISA. (n.d.). 5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance. https://media.defense.gov/2023/Jul/17/2003260829/-1/-1/0/ESF%205G%20NETWORK%20SLICING-SECURITY%20CONSIDERATIONS%20FOR%20DESIGN,%20DEPLOYMENT,%20AND%20MAINTENANCE_FINAL.PDF

- Olimid, R. F., & Nencioni, G. (2020). 5G network slicing: A security overview. *IEEE Access*. Advance online publication. <https://doi.org/10.1109/ACCESS.2020.2997702>
- Ordóñez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J. J., Lorca, J., & Folgueira, J. (2017). Network slicing for 5G with SDN/NFV: Concepts, architectures and challenges. *IEEE Communications Magazine*, 55(3), 80-87. <https://doi.org/10.1109/MCOM.2017.1600935>
- Papavassiliou, S. (2020). Software defined networking (SDN) and network function virtualization (NFV). *Future Internet*, 12(1), 7. <https://doi.org/10.3390/fi12010007>
- Pauliac, M. (2020). USIM in 5G Era. *Journal of ICT*, 8(1), 29-40. <https://doi.org/10.13052/jicts2245-800X.813>
- Prasad, A. R., Arumugam, S., Sheeba, B., & Zugenmaier, A. (2018). 3GPP 5G security.
- Rodriguez, J. (2015). *Fundamentals of 5G mobile networks*. John Wiley & Sons. ISBN: 9781118867525.
- Salahdine, F., Han, T., & Zhang, N. (2022). Security in 5G and beyond: Recent advances and future challenges. *Security and Privacy*, 6, e271. <https://doi.org/10.1002/spy2.271>
- Scalise, P., Boeding, M., Hempel, M., Sharif, H., Delloiacovo, J., & Reed, J. (2024). A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas. *Future Internet*, 16(67). <https://doi.org/10.3390/fi16030067>
- Shukla, S., Khare, V., Garg, S., & Sharma, P. (2013). Comparative study of 1G, 2G, 3G and 4G. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, 2(4), 55. Blue Ocean Research Journals. Retrieved from <http://www.borjournals.com>
- Singh, V. P., Singh, M. P., Hegde, S., & Gupta, M. (2023). Security in 5G network slices: Concerns and opportunities. *IEEE Access*, 11, 3386632. <https://doi.org/10.1109/ACCESS.2024.3386632>
- Sucheta, & Yadav, K. P. (2013). A comparative study of 1G, 2G, 3G and 4G. *International Journal of Advances in Engineering Research (IJAER)*, 3(III). Retrieved from <http://www.ijaer.com>
- Sullivan, S., Brighente, A., Kumar, S. A. P., & Conti, M. (2021). 5G security challenges and solutions: A review by OSI layers. *IEEE Access*, 9. <https://doi.org/10.1109/ACCESS.2021.3105396>
- TE Connectivity Ltd. (2018). *MASS CONNECTIVITY IN THE 5G ERA. Preparing Now for the Future*.
- Tian, F., Zhang, P., & Yan, Z. (2017). A Survey on C-RAN Security. *IEEE Access*, 5, 13372-13386. <https://doi.org/10.1109/ACCESS.2017.2717852>
- Wang, H., Xu, L., Xue, L., & Gu, G. (2015). FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks. In 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Rio de Janeiro, Brazil. <https://doi.org/10.1109/DSN.2015.27>
- Wani, M. S., Rademacher, M., Horstmann, T., & Kretschmer, M. (2024). Security vulnerabilities in 5G non-stand-alone networks: A systematic analysis and attack taxonomy. *Journal of Cybersecurity and Privacy*, 4(1), 23-40. <https://doi.org/10.3390/jcp4010002>

Yousaf, F. Z., Bredel, M., Schaller, S., & Schneider, F. (2017). NFV and SDN - Key technology enablers for 5G networks. *IEEE Journal on Selected Areas in Communications*, 35(11), 2468-2478. <https://doi.org/10.1109/JSAC.2017.2760418>

Yusuf, A. H. (2023, June). Major Security Challenges in 5G Network.

Ελληνική

Παρασκευόπουλος, Γ. (2024). Επισκόπηση και Ανάλυση Επίδοσης Αρχιτεκτονικών Κινητών Επικοινωνιών 5G. Μεταπτυχιακή Διατριβή.

Ιστοσελίδες

AGMPlanning. (2024). evolution of mobile networks generations 1G, 2G, 3G, 4G, 5G.pdf. <https://www.slideshare.net/slideshow/evolution-of-mobile-networks-generations-1g-2g-3g-4g-5gpdf/265885704>

Bogucka, H. (2022). AI for O-RAN Security. <https://rimedolabs.com/blog/ai-for-oran-security/>

HIVO. (2024). Secure Storage Solutions for Mobile Devices. <https://hivo.co/blog/secure-storage-solutions-for-mobile-devices>

Kron Technologies (2022). Importance of Security in Cyber-Physical Systems. <https://krontech.com/importance-of-security-in-cyber-physical-systems>

Nayak, R. (2015). Difference between SDN and NFV. <https://www.linkedin.com/pulse/difference-between-sdn-nfv-rajiv-nayak/>

Prime Group. (2024). The Application of 5G Technology in Modern Engineering. <https://weareprimegroup.com/insights/the-application-of-5g-technology-in-modern-engineering/>

Remmert, H. (2020). 5G Applications and Use Cases. <https://www.digi.com/blog/post/5g-applications-and-use-cases>

Trčka, J. (2019) 5G Use Cases. https://www.linkedin.com/posts/joseftrcka_5g-embm-mmtc-activity-6527268515068682240-1Tfg?utm_source=share&utm_medium=member_desktop

Wikipedia. (21 March, 2024). 5G network slicing. https://en.wikipedia.org/wiki/5G_network_slicing

Veritis a. (2024). Identity and Access Management Trends for 2023. <https://veritis.com/blog/identity-and-access-management-trends/>

Veritis b. (2024). IAM Implementation and Solutions To Emerging 'IT Security Challenges'. <https://veritis.com/blog/iam-implementation-solutions-security-challenges/>

Veritis c. (2024). IAM Best Practices for Optimal Cloud Security. <https://veritis.com/blog/iam-best-practices-for-optimal-cloud-security/>

Βλαχάκης, Μ. (άγνωστη). Τεχνολογία 5ης Γενιάς Ασύρματης Επικοινωνίας - 5G στην Ελλάδα.
<https://aktinonolia.gr/5g-κεραίες-κινητής-ακτινοβολία-ελλάδα/>