Journal of Engineering Managment and Soft Computing (JEMSC)

Extracting and Ranking the Threats of the Radio Access Network Layer of the 5th Generation Mobile Network Based on Risk Analysis

Mohammad Ragheb[1]✉, **Mohammadreza Keshavarzi**[2] **and Bahman Madadi**[3]

1. Corresponding Author, Invited Professor of Telecommunication Engineering at Qom University of Technology, Qom, Iran.
2. Associated professor, ICT Research Institute, Iran Telecommunication Research Center (ITRC), Tehran, Iran.
3. PHD Student, Imam Husein university, Tehran, Iran.

Article Info

Article type:
Research Article

Article history:
Received 12 January 2025
Received in revised form 8 February 2026
Accepted 5 March 2026
Published online 1 April 2026

Keywords:
Fifth Generation Mobile Network (5G), RAN Security Threats and Vulnerabilities, RAN Security Solutions, Threat Prioritization.

ABSTRACT

The fifth generation of mobile networks (5G) offers new and advanced services such as virtual/augmented reality (AR/VR), high-quality video streaming, remote surgery, Internet of Things (IoT), and smart cars with stringent requirements. In this article, we review the 5G architecture and then focus on the Radio Access Network (RAN) architecture. Subsequently, we collect the threats, vulnerabilities, and security solutions provided by researchers and academic authorities in this field. In this article, we also rank RAN threats in the 5G network. To rank the threats, we assign a score to each threat by introducing a risk criterion. Finally, to provide a good ranking for the threats, we analyze the risk by assessing the impact/severity and the probability of the threats success on the 5G network. The results of our studies and analyses in this article inform 5G network operators which threats should be prioritized. The results of this paper will guide to secure the 5G network and deploy security solutions.

Cite this article: Ragheb, M. & et al, (2026)., Extracting and Ranking the Threats of the Radio Access Network Layer of the 5th Generation Mobile Network Based on Risk Analysis. *Engineering Management and Soft Computing,* 12 (2). 19-55.

DOI: https://doi.org/10.22091/jemsc.2026.11966.1237

DOI: https://doi.org/10.22091/jemsc.2026.11966.1237

Publisher: University of Qom

1) Introduction

The 5G Radio Access Network (RAN) provides wireless connectivity for user devices to reach the core network (CN) and 5G services using 5G radio frequencies. Prominent use cases include cloud gaming, augmented/virtual reality (AR/VR), high-quality video streaming, remote surgery, autonomous driving, and fixed wireless access (FWA). The RAN comprises transmitters, antennas, baseband processing (RAN compute units), and RAN software that together enable ultra-high data rates and mobility (Farooqui et al., 2022). Compared with 4G, 5G introduces several advances in the RAN, such as large antenna arrays, massive multiple-input multiple-output (mMIMO), centralized RAN (C-RAN), and Open RAN. Open RAN represents an industry-level standard for the RAN, defining interfaces that support multivendor interoperability and provide network flexibility at reduced cost (Liyanage et al., 2023). Notably, Open RAN integrates the benefits of network softwarization and artificial intelligence (AI) to enhance device performance and RAN operations. The introduction of diverse new use cases inevitably brings new and sophisticated threats that require careful analysis. Moreover, the open nature of 5G anticipates that multiple vendors and service providers may participate in network deployment and service delivery, which can increase the threat surface. Consequently, RAN components are susceptible to attacks targeting the access network (AN), such as unauthorized access, Denial of Service (DoS), traffic sniffing, signaling storms, flooding, and jamming/disruption. Therefore, it is necessary to examine the RAN architecture in terms of assets, threat levels, and vulnerabilities, identify security threats, and compile mitigation strategies based on credible scientific and research sources. In addition, threats should be scored and ranked according to well-defined criteria. By prioritizing and implementing security measures against high-impact threats, we can contribute to strengthening the security of 5G networks.

2) Literature Review

Farooqui et al. (2022) categorize 5G security threats into the layers, including device layer, radio access network (RAN) layer, edge layer, core network (CN) layer, and service layer, which can be applied across 5G networks. For each layer, they identify specific threats and indicate the potentially affected components. Liyanage et al. (2023) analyze security and privacy risks and the challenges associated with the Open RAN architecture. Based on the attack level, cellular network operators can precisely deploy appropriate countermeasures to enhance Open RAN security (Mimran et al., 2021).

5G NR (New Radio) is responsible for connecting devices to the network and comprises Base Stations (BSs) that, in turn, connect to the 5G Core (5GC) network. 5G NR preserves the 5GC features regarding signal separation and transmission (user plane and control plane levels), even in the addressing scheme. This allows for the simplification of interfaces and enables the creation of slices in the RAN domain. Support for network slicing (Yang et al., 2019) is the newest capability compared to 4G solutions.

NR deploys stringent security mechanisms based on cryptography to ensure data confidentiality, alongside robust integrity protection mechanisms (Batalla et al., 2020). It is noteworthy that NR security keys are explicitly segregated from those used in the 5GC. The key 5G technologies that require in-depth security analysis include Network Function Virtualization/Software-Defined Networking (NFV/SDN), Multi-access Edge Computing (MEC), the RAN, and other functions such as the Network Exposure Function (NEF) and IP Packet Exchange (IPX) (Batalla et al., 2020). A primary feature of 5G that poses a security challenge is the software-defined nature of the network (Ahmad et al., 2018). Developing most capabilities in the software layer has become a common approach in recent years and offers numerous advantages over legacy hardware dependence. However, from a security standpoint, this expands the attack surface (ENISA, 2020) and necessitates continuous upgrades with security patches and updates (Batalla et al., 2020).

3) Methodology

In this paper, by studying and leveraging the primary 5G standardization documents, such as those from 3GPP and ENISA[1], along with other relevant references (ENISA, 2023; Ranaweera et al., 2021), we categorize security threats, vulnerabilities, and mitigation mechanisms proposed by researchers and standardization bodies in RAN domain. To this end, threats related to the RAN in 5G mobile networks are extracted and collected from multiple sources, resulting in a comprehensive study. Subsequently, these threats are ranked using a well-known risk assessment criterion, which is introduced for the first time in this paper. Furthermore, by evaluating the impact (damage) and the likelihood of occurrence of each threat, the corresponding risk level is assessed and a quantitative score is assigned. Finally, the identified threats are ranked based on their assessed risk levels. The studies and analyses conducted in this research contribute to strengthening 5G network security and facilitating the deployment of effective security solutions.

4) 5G Network Architecture and Services

In its most general form, a 5G network consists of a 5G AN and a 5GC, as illustrated in Figure 1. The AN comprises the Next Generation Radio Access Network (NG-RAN) with the new 5G radio interface (NR) and/or non-3GPP Ans, such as Wi-Fi, xDSL and others. The AN is connected to the 5GC network. Various network entities are interconnected through an underlying TCP/IP-based transport network that supports services with differentiated Quality of Service (DiffServ QoS).

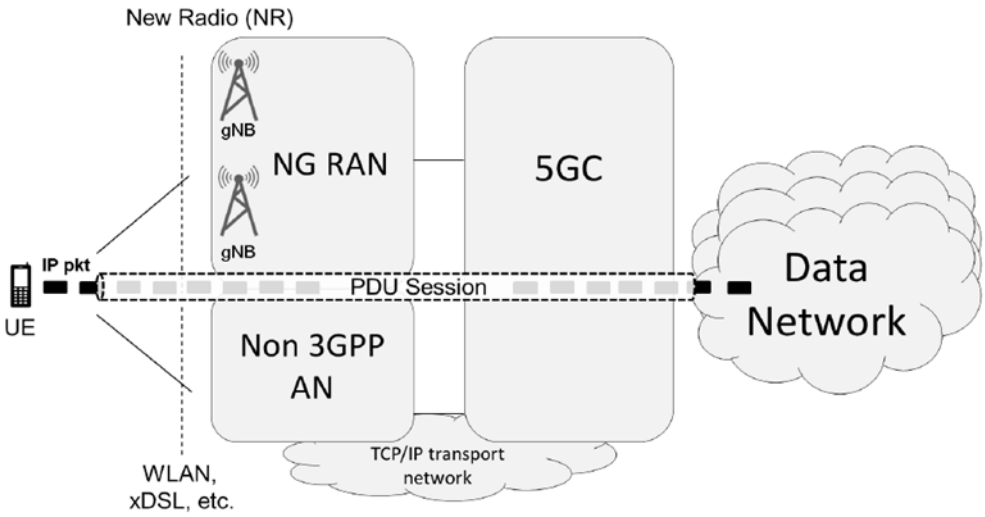

Figure 1. Overall 5G Network Architecture

A 5G network is used to connect user equipment (UE) to external data networks. The connectivity service in 5G is referred to as a PDU session. From a transport perspective, a PDU session is realized through a sequence of NG tunnels in the 5GC and one or more radio bearers over the radio interface. This set of transport "pipes" ultimately connects the UE to its corresponding core network functions and to the external data network, enabling the exchange of user traffic (Figure 2). The primary function of the mobile network is to dynamically establish, maintain, and release tunnels and bearers in order to track user mobility and support different user states (e.g., idle, connected, etc.).

A PDU session is, in many respects, similar to an EPS bearer in LTE, except for the supported QoS model and user data units. In fact, a PDU session can carry not only user-plane IP packets but also Ethernet frames or unstructured data, thereby enabling Layer-2 connectivity among groups of user

1. The European Union Agency for Cybersecurity (ENISA) is the European Union's dedicated agency for achieving a high level of cybersecurity across Europe. Established in 2004, ENISA enhances the trustworthiness of information and communication technology (ICT) products, services, and processes through cybersecurity certification schemes. By working closely with its key stakeholders, ENISA aims to strengthen trust in the digital economy, increase the resilience of the European Union's infrastructure, and ultimately, ensure the digital security of European society and its citizens through knowledge sharing, capacity building, and awareness raising.

equipments (UEs). The 5G QoS model is based on the new concept of a QoS flow, in which a QoS flow represents the finest granularity for QoS differentiation. Multiple QoS flows may be associated with a single PDU session.

In the NG-RAN architecture, a clear separation between the control plane and the user plane is implemented. In the user plane, one or more User Plane Functions (UPFs) are deployed to establish PDU sessions and primarily perform packet forwarding between different NG-U tunnels (Figure 2). All other network functions (NFs) belong to the control plane and are responsible for signaling, session control, mobility management, and the enforcement of network policies.

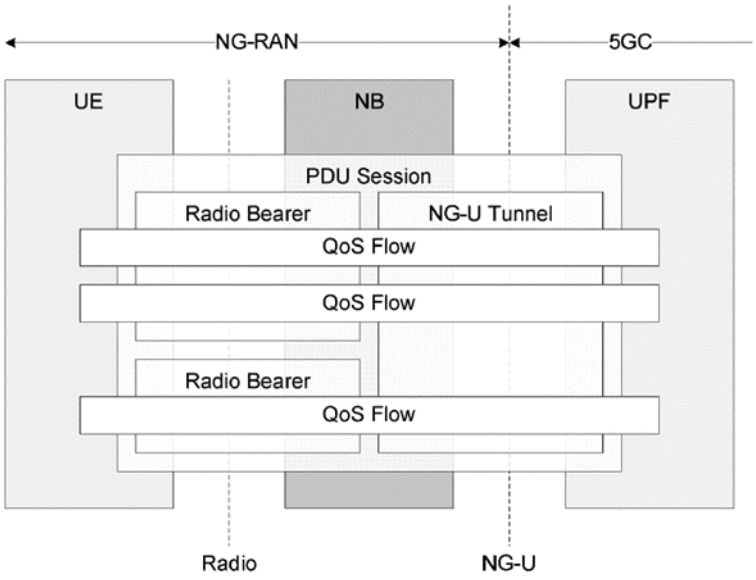

Figure 2. PDU Sessions and QoS Flows in the User Plane

4.1) NG-RAN

Figure 3 illustrates the functional split between the 5G functions executed in the NG-RAN and the 5GC. In general, the NG-RAN is responsible for the establishment, maintenance, and delivery of the radio-related portions of PDU sessions that traverse the radio interface. It addresses radio-specific challenges, such as channel fading, interference, and signal power attenuation. Furthermore, the NG-RAN performs mobility management functions, including handover between gNBs, and supports PDU session anchoring and session continuity across radio nodes, ensuring seamless service delivery.

The functionality of a gNB can, in some deployments, be implemented in a distributed manner (Figure 4). In this case, the resulting architecture consists of a central unit (gNB-CU) that controls one or more distributed units (gNB-DUs) via the F1 interface. Each distributed unit is connected to a Remote Radio Head (RRH), which represents the actual radio transceiver. The gNB-CU is further split into two logical entities: gNB-CU-CP, which hosts control plane functions, and gNB-CU-UP, which hosts UPFs. This architectural approach follows the principle of Control and User Plane Separation (CUPS) and leverages SDN concepts, which were initially introduced in the later releases of LTE and are more extensively adopted in 5G networks.

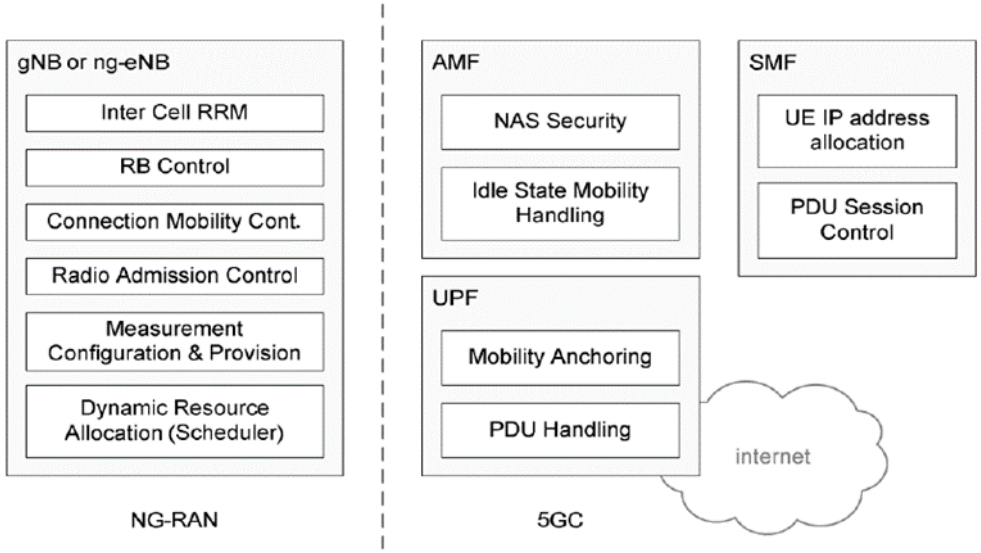

Figure 3. Functional Split between 5G Functions Implemented in the NG-RAN and the 5GC

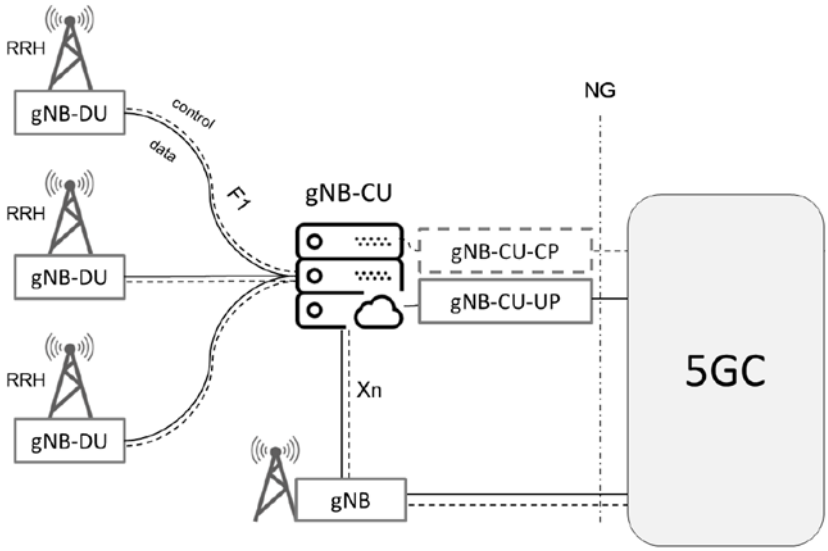

Figure 4. Overall NG-RAN Architecture

Figure 5 illustrates the protocol stack traversing the radio interface and its placement across the different gNB entities. With the exception of the Service Data Adaptation Protocol (SDAP) in the user plane, the stack is largely similar to that of LTE. The main characteristics of the individual layers are summarized as follows:

- The physical layer (PHY) comprises a set of digital and analog signal processing functions used by the UE and the Base Station (i.e., gNB) for data transmission and reception. It is based on Orthogonal Frequency Division Multiple Access (OFDMA) and supports adaptive subcarrier spacing values of 15, 30, 60, 120, and 240 kHz. Furthermore, the PHY layer employs adaptive modulation and coding (AMC) schemes, which dynamically select modulation formats, ranging from $\pi/2$-rotated BPSK to 256-QAM, depending on the prevailing channel conditions.
- The Medium Access Control (MAC) protocol provides low-level control of the PHY, primarily by scheduling data transmissions between the UE and the gNB.

- The Radio Link Control (RLC) protocol ensures the reliable delivery of data streams that require error-free reception. It operates through Automatic Repeat reQuest (ARQ) mechanisms and is also responsible for segmentation and the reassembly of data units.
- The Packet Data Convergence Protocol (PDCP) performs higher-layer transmission functions, including header compression and security functions, such as ciphering and integrity protection.
- The Service Data Adaptation Protocol (SDAP), in accordance with the new 5G QoS framework, is responsible for the correct mapping of user data packets associated with each QoS flow to a Data Radio Bearer (DRB) by means of appropriate packet marking.
- The Radio Resource Control (RRC) protocol is the signaling protocol used in Access Stratum (AS) procedures between the UE and the gNB. Its functions include RRC connection establishment and release, broadcasting of system information, establishment, reconfiguration, and the release of radio bearers, RRC connected-mode mobility procedures, paging, and power control.
- The Non-Access Stratum (NAS) protocol is a signaling protocol used between the UE and the 5GC for PDU session management, security, mobility management, and other control procedures. Within the 5GC, the entity responsible for UE management and control is the Access and Mobility Management Function (AMF), which plays a role functionally similar to the MME in LTE.

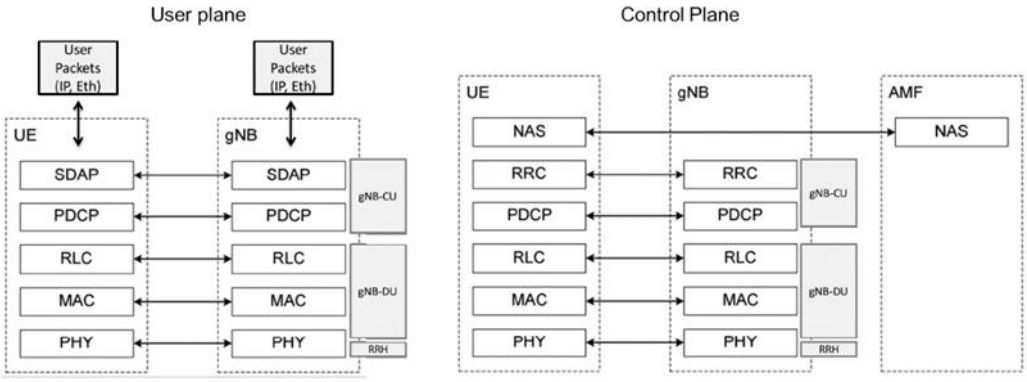

Figure 5. NG-RAN Stack Protocol

5) Emerging Technologies in 5G ANs

The objective of 5G networks is to achieve up to a 10,000-fold improvement in network capacity compared to LTE. This goal is realized by enabling approximately 100-times higher data rates than LTE, with peak data rates in the range of 5 to 10 Gbit/s, while reducing the end-to-end (E2E) latency to around 1 ms. Furthermore, spectral efficiency (SE) and energy efficiency (EE) are expected to improve by up to fivefold. In addition, a 20-fold expansion of available spectrum is anticipated, and the network densification should provide a 50-fold improvement, while supporting up to 1,000 times more connected devices.

Achieving such growth requires increased capacity in the fronthaul, backhaul, and core (backbone) segments of the network. This can be accomplished through a combination of expanded spectrum availability, improved SE, network densification, and traffic offloading enabled by small cells.
The above requirement can be expressed by Equation (1):

$$C = M\left(\frac{W}{n}\right)\log_2[1+\frac{S}{I+N}] \quad (1)$$

Here, W denotes the bandwidth of the BS signal, n represents the load factor, defined as the number of users associated with the corresponding BS, M is the spatial multiplexing factor, indicating the

number of spatial streams between the UE and the BS, S denotes the desired signal power, and N and I represent the noise power and interference power, respectively. Moreover, C denotes the network capacity.

From equation (1), it can be observed that the use of higher frequency bands, such as millimeter wave (mmWave), as well as spectral resource aggregation through techniques such as carrier aggregation, leads to a linear increase in network capacity. The load factor n can be minimized through cell splitting and the deployment of small cells, which reduce path loss and increase the desired signal power S, thereby resulting in an increase in network capacity.

It is generally agreed by researchers in academia and industry that 5G will be a combination of networks with different transmission power levels and cell sizes, as well as diverse radio access technologies (RATs) and backhaul connections, which can be accessed by a large number of heterogeneous and intelligent devices.

It is expected that 5G networks will manage human-to-human (H2H), human-to-machine (H2M), and machine-to-machine (M2M) communications. These complex scenarios make network management with heterogeneous resources and diverse QoS requirements for network services highly challenging. Therefore, network scalability and flexibility are essential to meet the demands of such unique services.

One approach to providing this scalability and flexibility is the introduction of a new network architectural design that integrates legacy systems with emerging standards. This can be achieved through a cloud-based wireless network architecture, which includes mobile cloud computing, cloud radio access networks (Cloud-RANs or C-RANs), reconfigurable networks, and large-scale data centers. Such an architecture is capable of delivering the required flexibility and adaptability through a virtualized, reconfigurable, and intelligent wireless network, thereby providing a foundation for other 5G technologies, such as mMIMO and D2D/M2M[1] communications. In the following, some of the emerging 5G technologies are introduced.

5.1) Dense Heterogeneous Networks (HetNets) and Multiple Radio Access Technologies (Multi-RATs)

According to 3GPP, heterogeneous networks (HetNets) are defined as the simultaneous operation of different types of BSs. However, in 5G networks, HetNets are more broadly viewed as a combination of multiple radio access technologies (Multi-RATs). This includes macro cells, small cells, RRHs, and wireless local area networks (WLANs), along with support for D2D and M2M communications.

The multi-tier deployment of heterogeneous nodes in 5G systems results in a significantly higher network density compared to conventional single-tier networks. Dense deployment of heterogeneous nodes is a prerequisite for reducing the load factor n in equation (1) and for improving the received signal power S by mitigating path loss. Moreover, the deployment of outdoor small cells with transmission power on the order of 30 dBm offers lower capital and operational expenditures (CAPEX and OPEX) compared to macro cells. In addition, relay nodes, operating over wireless/cellular spectrum, can be deployed in scenarios where wired backhaul is unavailable. Finally, the overlapping deployment of different types of BSs provides an effective solution for accommodating the rapid growth of data traffic, particularly when data offloading mechanisms are optimized to fully exploit the capabilities of HetNets.

5.2) Cloud RAN

The main challenges of traditional radio access networks (RANs) include limited capacity, insufficient scalability, and low resource efficiency, which can be effectively addressed by cloud C-RANs. The concept of C-RAN originates from the distributed BS architecture. In the current 4G/LTE architecture, both baseband processing and radio functions are performed within the BS/eNB, while coordination among neighboring BSs is achieved via the X2 interface. However, in the proposed 5G architecture, the baseband unit (BBU) is decoupled from the analog radio access unit, referred to as the RRH, and

1. Device-to-device/machine-to-machine

migrated to the cloud environment. In this architecture, multiple BBUs are aggregated into a BBU pool, where baseband signal processing and radio resource management are performed in a centralized manner. This centralized processing paradigm enhances resource utilization, improves inter-cell coordination, and reduces operational costs (Figure 6).

Consequently, radio-signal transmission to users is performed by the RRHs based on the baseband signals received from the BBU (in the cloud). In this configuration, the backhaul connects the cloud to the core network, while the fronthaul employs optical transport links to interconnect RRHs for the purpose of digital baseband signal transmission to the cloud.

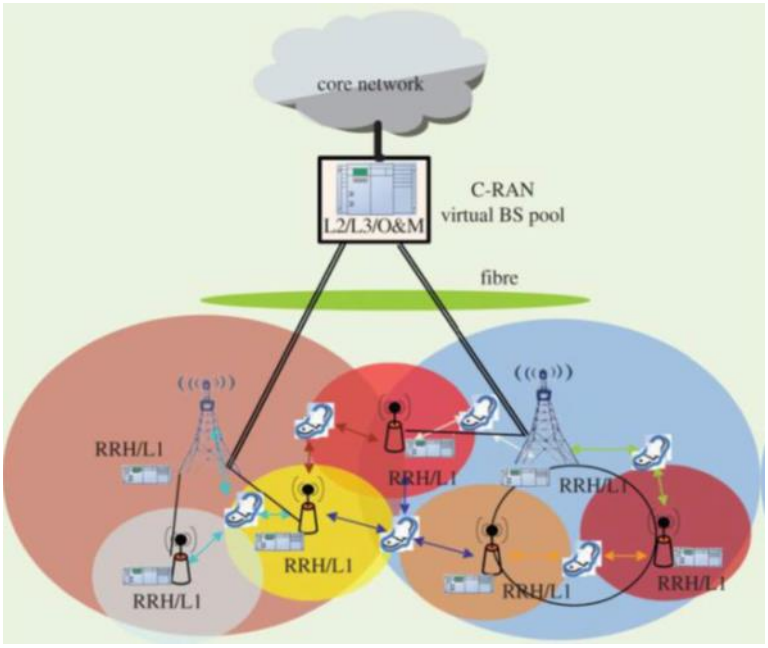

Figure 6. C-RAN Configuration for 5G Cellular Network (Idowu-Bismark et al., 2019)

C-RAN introduces a key paradigm shift in the design of future wireless systems, in which multiple radio access technologies and core network functions are realized in the cloud environment. Owing to its cost-efficiency, high flexibility, and operational efficiency, C-RAN has emerged as one of the most promising solutions for addressing the massive capacity demands of 5G wireless networks. Nevertheless, several open research challenges remain in the application of C-RAN to 5G networks. These include efficient radio resource management, such as bandwidth allocation, transmit power control, and beamforming design and optimization. Furthermore, fronthaul compression techniques, as well as the efficient design and utilization of computational resources in the cloud, constitute other important research directions.

5.3) Divice-to-Device (D2D) Communication

D2D communications, nearby Ues, are allowed to establish direct local links with one another, enabling traffic to be exchanged without being routed through BS. This approach leads to reduced energy consumption and end-to-end latency, while simultaneously increasing peak data rates. D2D communications are particularly beneficial in scenarios characterized by a high density of user terminals per cell, where conventional BS-centric communication may result in poor throughput performance. In D2D communications, the BS no longer constitutes a traffic bottleneck, since multiple D2D connections can simultaneously share the same bandwidth. This enhances spectral reuse within each cell and reduces interference, particularly in unlicensed frequency bands, as illustrated in Figure 7.

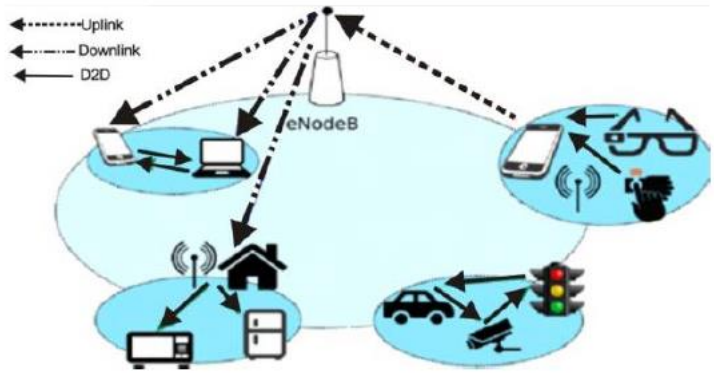

Figure 7. D2D Communication Architecture (Idowu-Bismark et al., 2019)

5.4) Massive MIMO (mMIMO)

Multiple-Input Multiple-Output (MIMO) technology employs multiple antennas at the transmitter and/or receiver to mitigate channel fading and improve SE, power efficiency, link reliability, and cell-edge performance. Massive MIMO (mMIMO), as an extension of conventional MIMO, achieves these enhancements on a much larger scale. In mMIMO systems, both the transmitter and receiver are typically equipped with tens or even hundreds of antenna elements, enabling highly spatially selective beamforming, improved multi-path utilization, and significantly enhanced network capacity and user throughput. One configuration of mMIMO is the cell-free mMIMO architecture, which represents a distributed system in which multiple antennas at each BS are connected to a C-RAN for centralized baseband processing. This architecture has been proposed as a promising solution for 5G networks.
In mMIMO systems, favorable propagation conditions are commonly assumed, meaning that users experience a sufficiently rich scattering environment. As the number of BS antennas increases, the user channels tend to become asymptotically orthogonal. Under such conditions, although matrix operations grow in dimension, they can be efficiently approximated using simple series expansion techniques. This property enables linear processing algorithms, such as Zero-Forcing (ZF) and Minimum Mean-Square Error (MMSE) detection, which rely on matrix inversion, to achieve near-optimal performance—a condition that is almost impossible without favorable propagation in mMIMO systems.

In 5G HetNets, wireless backhaul is preferred over wired backhaul, and mMIMO can readily support this requirement due to its ease of deployment compared to wired solutions. Consequently, mMIMO is employed in macro cells to support multiple wireless backhaul links, benefiting from its high degrees of freedom (DoF) and deployment flexibility.

Despite the advantages of mMIMO technology, conventional multi-antenna detection algorithms are not well suited for large-scale antenna (LSA) systems, as they incur significantly increased computational complexity. To address this issue, Amiriara and Zahabi (2023) proposed a low-complexity receiver based on the Teaching–Learning-Based Optimization (TLBO) meta-heuristic algorithm for mMIMO systems, demonstrating that the proposed detector is highly efficient for practical implementation.

Another MIMO-based technology for 5G networks, referred to as 3D-mMIMO, employs three-dimensional (3D) beamforming for traffic backhauling from indoor access points connected to LSA arrays deployed within buildings, as well as for communication with users located at different floors of high-rise buildings. This capability is known as 3D sectorization, as illustrated in Figure 8.

Nevertheless, numerous challenges remain, including the design and provisioning of mmWave mMIMO patterns for various deployment scenarios, which must be addressed prior to large-scale adoption of mMIMO in 5G networks. Minimum-variance-based beamforming techniques suffer from performance degradation in the presence of errors in noise-plus-interference covariance matrix estimation. One major source of such errors is the presence of desired signal components in the estimated noise and interference snapshots, which reduces the output signal-to-interference-plus-noise ratio (SINR).

To enhance the robustness of beamforming algorithms against covariance estimation errors, Rezaeizadeh and Bekran (2023) employed covariance matrix reconstruction using orthogonal vectors derived from the Gram–Schmidt algorithm, combined with diagonal loading. Simulation results demonstrate the superiority of the proposed method in terms of beam pattern improvement, interference angle estimation accuracy, and SINR enhancement, compared to benchmark algorithms.

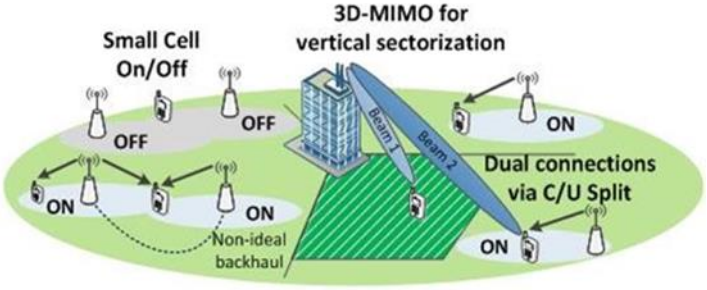

Figure 8. 3D mMIMO for Vertical Sectoring (Idowu-Bismark et al., 2019)

5.5) Spatial Modulation

One of the key challenges in mMIMO systems is achieving an appropriate trade-off between SE and EE. This challenge has motivated a novel approach for large-scale MIMO systems with a single radio-frequency (RF) chain, referred to as Spatial Modulation-based Massive MIMO (SM-MIMO). This approach emerges in response to the widespread deployment of mMIMO in 5G networks and the concerns of network operators regarding increased capital expenditure (CAPEX) and operational expenditure (OPEX) caused by the large number of RF chains and power amplifiers, which lead to excessive energy consumption.

In massive SM-MIMO, a large number of antenna elements is employed relative to a limited number of RF chains. The distinguishing feature of SM-MIMO compared to conventional MIMO lies in mapping additional information bits onto a structure known as the spatial modulation constellation, where each constellation point corresponds to a single antenna or a subset of antenna elements.

In this scheme, conventional amplitude- or phase-based modulation techniques, such as quadrature amplitude modulation (QAM) or phase shift keying (PSK), are used for symbol transmission, while only one antenna is activated during each transmission interval (Figure 9). This characteristic eliminates inter-channel interference (ICI) and removes the need for strict inter-antenna synchronization, unlike schemes such as V-BLAST. Consequently, this novel approach facilitates the deployment of high-data-rate MIMO systems by reducing baseband processing complexity, simplifying RF circuitry, and lowering hardware costs, while simultaneously enhancing the overall energy efficiency of the system.

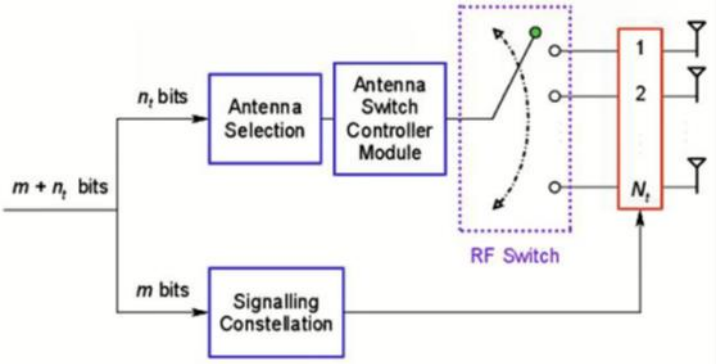

Figure 9. SM-MIMO Transmitter Scheme (Idowu-Bismark et al., 2019)

5.6) Millimeter Wave (mmWave) Communications

Millimeter wave (mmWave) frequency bands have been widely recommended for cellular communication systems due to their abundant available spectrum and strong potential as candidate bands for next-generation cellular services. These frequencies can be utilized to offload the heavily congested 700 MHz to 2.6 GHz spectrum currently employed in 3G and 4G wireless networks. A key advantage of mmWave communication is its ability to support significantly larger carrier bandwidths, enabling much higher data rates and allowing network operators to extend channel bandwidths well beyond the 20 MHz channels used in 4G systems. The availability of larger bandwidth reduces digital traffic latency, thereby enabling high-performance internet-based applications that require ultra-low latency, such as industrial automation, smart grids, intelligent transportation systems, and unmanned aerial vehicle (UAV) control. In mMIMO systems, mmWave frequencies are particularly advantageous due to the very small physical size of mmWave antenna elements, which makes it possible to pack LSA arrays compactly at the BS without significant antenna coupling issues. This property supports adaptive beamforming as well as wireless backhaul links in HetNets, including macro cells and small cells, thereby enhancing the overall network capacity of 5G systems, as illustrated in Figure 10.

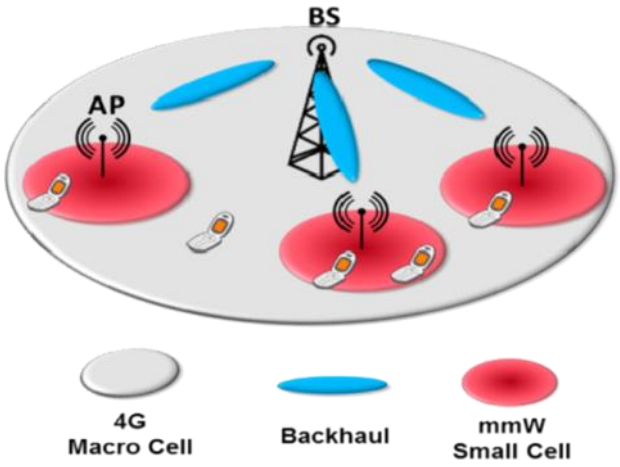

Figure 10. Millimeter Wave for Small-Cell Backhauling (Idowu-Bismark et al., 2019)

However, the use of higher carrier frequencies in 5G mmWave networks introduces significant radio propagation challenges. These include severe penetration losses caused by obstacles such as concrete buildings, walls, and other dense materials, which substantially degrade the received signal power. Another critical challenge, particularly in mobile scenarios, is the initial access (IA) procedure, during which a UE is required to establish an initial physical link with a BS (gNB) in order to access the network. In mmWave communications, link establishment relies on directional transmissions and beam alignment, which can significantly delay the cell search and initial access process. This issue is further exacerbated by the fact that beamforming and other advanced directional transmission techniques cannot be fully exploited until the initial access connection has been successfully established. Therefore, the development of efficient initial access mechanisms is essential for enabling the practical deployment of mmWave communications in 5G networks.

5.7) Visible Light Communication

One of the promising candidate technologies for indoor wireless communication systems, which has also been considered for combined indoor/outdoor deployment scenarios in 5G networks, is Visible Light Communication (VLC). Compared to conventional radio-frequency (RF)–based networks in indoor environments, VLC offers several notable advantages. Most importantly, it exploits the unregulated optical spectrum, which provides an abundant license-free bandwidth, enabling the support of very high data rates. Furthermore, due to the physical characteristics of light propagation and the use of distinct optical spectra, VLC inherently avoids interference between indoor and outdoor users, as well as inter-user interference, making it particularly attractive for dense indoor scenarios.

Figure 11 illustrates a typical use case of VLC in an indoor environment. In addition, the spatial multiplexing gain of MIMO techniques can be effectively leveraged in VLC systems to further enhance the achievable data rate and overall system performance.

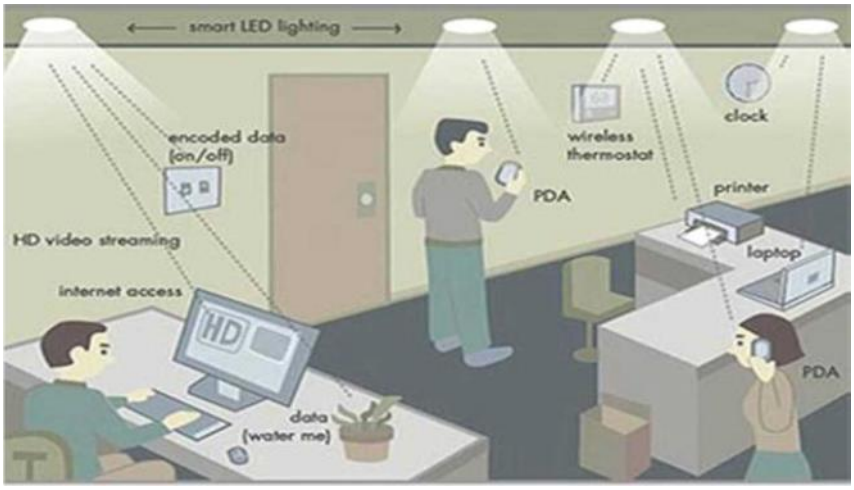

Figure 11. VLC Application for Indoor Use (Idowu-Bismark et al., 2019)

VLC can be employed for vehicle-to-vehicle (V2V) communications, enabling applications such as pre-collision sensing and collision avoidance systems. Moreover, VLC has attracted considerable interest for robotic monitoring and control and collision avoidance systems in hospital environments, as well as for underwater communication systems. Recent studies indicate that, in certain scenarios, potential data rates of up to 10 Gb/s can be in hospital environments, as well as for underwater communication systems. Recent studies also indicate that, in certain scenarios, potential data rates of up to 10 Gb/s can be achieved using VLC. Despite these advantages, VLC faces several implementation challenges. One of the most critical issues is the limited feasibility of UL LED transmitters with sufficient transmission power that can be practically integrated into UE. This constraint significantly complicates the design of the uplink in VLC systems. This constraint significantly complicates the design of the uplink in VLC systems.

As a result, VLC systems are likely to adopt hybrid architectures, in which low-rate uplink services are supported via result, VLC systems are likely to adopt hybrid architectures, in which low-rate uplink services are supported via complementary access technologies, such as Bluetooth or infrared (IR), while Wi-Fi may be leveraged to provide high-rate uplink services in indoor environments.

5.8) Reconfigurable, Virtualized, and Intelligent 5G Wireless Network Enabled by SDN/NFV

Current cellular mobile communication systems, ranging from second-generation (GSM/2G) to fourth-generation (LTE/4G) networks, have been predominantly designed and deployed as connection-oriented architectures with rigid and inflexible RANs. These architectures lack dynamic reconfigurability, and therefore, fail to provide the required flexibility for efficiently supporting modern content-centric and hybrid communication services, such as H2H, machine-to-human (M2H), and M2M communications.

In contrast, 5G networks are expected to intelligently identify diverse communication scenarios and dynamically allocate network resources accordingly. Moreover, 5G aims to deliver optimal connectivity and network performance in alignment with service requirements, thereby enhancing the efficient utilization of existing network resources. This evolution toward content-centric networking paradigms can be realized through the adoption of new hardware and software platforms, enabling greater flexibility, adaptability, and intelligence in future wireless networks.

The objective of this hardware/software platform is to exploit the capabilities of the aforementioned key enabling 5G technologies to achieve a content-centric network with flexibility and reconfigurability.

The most vital and fundamental conceptual approach to achieving these objectives is the use of SDN and NFV.

The 5G network is an ultra-dense heterogeneous network (UDN) with small-cell deployment, and without appropriate cellular design for the different operational frequency bands, ranging from 2G to 4G, interference will occur. Various types of interference are expected in HetNets, among which the main challenge is the interference caused by a small cell (SC) to a macrocell user located within the SC coverage area. Furthermore, 5G is expected to operate over the frequency range from 300 MHz to 300 GHz, as mmWave technology has been included as one of the enabling technologies for 5G (Figure 12).

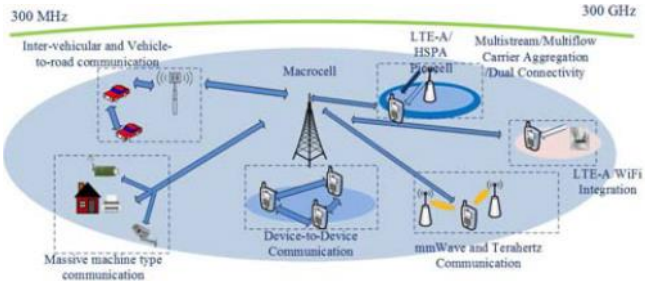

Figure 12. Operating Frequency Ranges (Idowu-Bismark et al., 2019)

To address interference management in 5G networks, provide ubiquitous connectivity for smart devices/UEs across networks operating over heterogeneous frequency bands, and mitigate the challenges associated with inter-band integration, Software-Defined Radio (SDR) emerges as an ideal solution. Unlike conventional hardware-centric radio architectures, UE-based SDR platforms implement the PHY and parts of the data link layer in software, enabling dynamic and adaptive scanning of available frequency bands. This capability allows the integration of multiple heterogeneous radio access technologies (RATs), such as GSM, HSPA+, LTE/LTE-Advanced, WiMAX, and Wi-Fi, within a single unified radio interface, as illustrated in Figure 13.

Such an SDR-based approach significantly enhances radio flexibility at the UE level, while facilitating inter-system interference mitigation, improved spectrum utilization, and seamless connectivity in multi-band and multi-RAT 5G network environments.

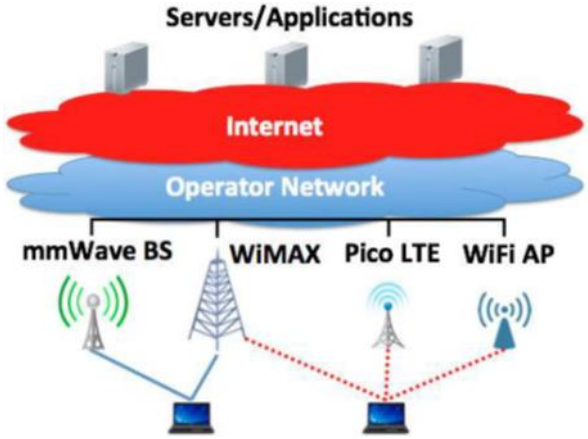

Figure 13. Smart UE/Device Connections (Idowu-Bismark et al., 2019)

At present, all networks, services, equipment, and protocols operate over dedicated frequency bands, and due to the presence of non-reconfigurable bottlenecks in hardware radio switches, the current heterogeneous network is unable to achieve convergence. Therefore, it is believed that the convergent nature of future 5G networks will originate from the spectrum-sharing capability provided by Software-Defined Radio (SDR).

Software-Defined Networking (SDN): With increasing network densification, the backhaul becomes more heterogeneous and scenario-dependent; that is, different types of backhaul are employed depending on availability, such as fiber, microwave, or mmWave links. This heterogeneity also affects RAN performance, for example through latency variations in backhaul links, and consequently impacts inter-cell coordination and cooperation algorithms. Therefore, both the RAN and backhaul networks need to be aware of each other's constraints and capabilities, which in turn introduces new concepts in network management, such as the application of SDN principles, to enable rapid routing and congestion monitoring/control. The SDN paradigm facilitates the alignment of backhaul network operation with the requirements of the RAN, and thus, plays a significant role in achieving 5G network convergence through SDN.

Embedding intelligence into 5G leads to increased complexity in HetNet service requirements, while enabling the provision of flexible solutions to adapt network heterogeneity through the use of SDN, which has emerged as a new intelligent architecture for network reconfiguration. The core idea behind SDN is to decouple the control plane from the switches and enable external control of data forwarding through a logical software entity, known as the controller, as illustrated in Figure 14.

SDN is defined as the physical separation between the network control plane and the user (data) plane. This architecture decouples network control functions from packet forwarding, enabling the network control to be directly programmable and allowing the underlying infrastructure to be abstracted for network applications and services. Inspired by the benefits offered by SDN, CUPS was proposed as a key feature of the core network to provide architectural enhancements for Evolved Packet Core (EPC) nodes, such as the SGW and PGW. The same concept has been extended to the 5GC architecture, where it is expected to operate as a more advanced feature compared to 4G.

With the rapid growth of smartphones and applications, such as video streaming, data traffic continues to increase. To deliver these services effectively with an improved quality of experience (QoE), low latency is a critical requirement. To meet stringent latency requirements, the user plane can be deployed at the edge cloud, closer to end users. MEC plays a significant role in 5G deployment. Based on increasing data traffic demands, the user plane can be scaled independently, and upgrades can be performed without impacting the rest of the ecosystem.

The Forwarding Control Protocol (PFCP) is the native protocol for communication between the control plane and the user plane at the six reference points in 4G, and it is expected to remain in 5G. A session is established in the user plane, which instructs the UPF on how a specific traffic flow should be processed.

Network function virtualization (NFV): NFV is the technology that assists operators in virtualizing network tools and infrastructure, enabling the virtualization of operations such as routing, switching, load balancing, unified behavior management, content and spam filtering, as well as WAN optimization. An example is Coordinated Multi-Point (CoMP), which can be used to improve the user experience at the cell edge through coordinated scheduling, coordinated beamforming, and interface alignment. This can be achieved by implementing 5G Network Functions (NFs) as software operations using NFV, rather than relying on CoMP, because CoMP leads to increased signaling and backhauling overhead, as well as equipment costs. Therefore, in NFV, operators implement network functions in software components called Virtual Network Functions (VNFs).

One of the most important complementary technologies to SDN with a fundamental impact on the 5G network is NFV. The goal of NFV is the virtualization (also known as network softwarization) of a set of network functions by deploying them as software packages and creating the same services that legacy networks provide through hardware equipment. For instance, deploying a virtualized Session Border Controller (SBC) for VoIP to protect the network infrastructure is much easier than installing complex and expensive conventional network equipment. It can also be used to enable Internet of Things (IoT) services in non-critical applications, such as cargo monitoring. Another application area for NFV is its deployment on high-capacity servers or cloud infrastructure in C-RAN, where NFV aggregates signaling processing resources in the cloud infrastructure rather than using dedicated BBUs at each BS.

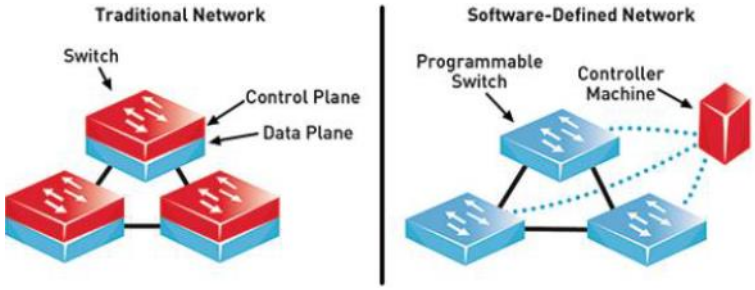

Figure 14. SDN with External Control Plane Compared to Conventional Network (Idowu-Bismark et al., 2019)

5.9) Open RAN

The introduction of the network softwarization concept in 5G, coupled with the infusion of intelligence beyond fifth-generation networks, has given rise to a promising solution known as Open Radio Access Network (Open RAN or O-RAN). O-RAN is a transformative RAN architecture aimed at reshaping the radio-access industry toward an open, adaptable, and intelligent RAN. Also referred to as ORAN, it is regarded as one of the most exciting RAN concepts designed for 5G and beyond in future wireless systems.

By promoting openness and intelligence augmentation for RAN elements, Open RAN can overcome limitations inherent in existing RAN technologies. The openness feature allows smaller and emerging players in the RAN market to deploy their customized services, while the added intelligence enables increased automation and performance optimization through the optimization of RAN elements and network resources. Moreover, network operators can shorten the time-to-market for new applications and services owing to the virtualization capability, thereby maximizing overall revenue. Consequently, the embedded intelligence in O-RAN can deliver superior benefits even for software-network-based virtual RAN (vRAN) concepts and C-RAN paradigms.

The O-RAN architecture is built on open specifications and component disaggregation. It splits the RAN into several open, capable units and leverages cloud technologies to achieve scalability and reliability in the face of a growing number of cellular connections. Furthermore, O-RAN introduces novel paradigms such as an extensible RAN, where third-party applications and services can be integrated onto the platform to evolve capabilities in an agile manner.

Another key design consideration in O-RAN is the use of machine learning (ML) for efficient management of network resources across diverse applications and services. An illustrative application of ML capability in O-RAN is the ability to manage multiple services with different QoS requirements within a single network, where resource-allocation decisions are made in real-time and independently across services. The openness of the architecture, together with the introduction of cutting-edge IT technologies and ML in the RAN, holds great promise for meeting the stringent requirements of future networks.

6) 5G Enabling Technologies

Several emerging technologies, including wearable devices, virtual/augmented reality (VR/AR), and fully immersive experiences (3D), are shaping the behavior of human end users and impose stringent requirements on user satisfaction. Consequently, these emerging use cases place significant pressure on 5G specifications across multiple dimensions, such as data rate, latency, reliability, device/network energy efficiency, traffic volume density, mobility, and connection density.

Current fourth-generation (4G) networks are not capable of meeting all the technical requirements of these services. The fifth-generation cellular network (5G) is envisioned as the wireless access solution to satisfy wireless broadband communication requirements from 2020 onward. ITU-R Working Party, within the ITU, is responsible for the development of 5G under a framework known as IMT-2020. The

vision of this effort is to achieve a thousand-fold capacity improvement, 100 billion connections, and near-zero latency.

In particular, 5G supports enhanced mobile broadband (eMBB) with a user-experienced data rate of 100 Mb/s under uniform spatial distribution and a peak data rate of 10–20 Gb/s. By consensus, 5G not only provides personal mobile services but also supports massive machine-type communications (mMTC) and mission-critical services requiring ultra-low latency and high reliability. In mission-critical communications (MCC)/ultra-reliable low-latency communications (URLLC), both latency and reliability must be jointly addressed. In many cases, an end-to-end (E2E) latency of 1 ms must be achieved with a reliability of up to 99.99%.

To achieve low latency for mission-critical communications (MCC), drastic changes in network architecture are required. Since latency is introduced by the RAN and the core network, together with the backhaul between the RAN and the core, a new network topology incorporating SDN, NFV, and multi-access edge computing (MEC) can be employed to significantly reduce latency. This reduction can occur due to the seamless operation and hardware-function independence offered by these entities. Furthermore, a new physical air interface with short transmission time intervals, small packet sizes, novel waveforms, new modulation and coding schemes are areas of investigation for achieving low latency. Additionally, optimization of radio-resource allocation, mMIMO, carrier aggregation in mmWave bands, and data-transmission prioritization must be considered.

Overall, strong integration with existing LTE is essential for 5G networks, enabling industries to deploy them quickly and efficiently while 5G is being standardized and made available. In summary, 5G wireless access should be an evolution of LTE, complemented by revolutionary architectural designs and advanced radio technologies. The following sections outline some of these enabling technologies.

6.1) Software-Defined Networking

Software-Defined Networking (SDN) is an emerging network architecture that enables the separation of the control plane and the data plane, introduces programmability, and provides flexible network control. The benefits of SDN include enhanced configuration capabilities, improved performance, and accelerated innovation. SDN allows network devices such as routers, switches, and firewalls to be automatically configured from a centralized control point. This facilitates the seamless integration of new network equipment and enables automated network management through software.

Network optimization through software helps address challenges such as congestion control, routing, traffic scheduling, and QoS provisioning. The high degree of configurability offered by SDN promises innovative networking solutions and new use cases for network service providers and telecommunications operators. These advantages make SDN a compelling option for 5G networks, enabling the delivery of efficient and innovative services to end users.

6.2) Network Function Virtualization

Network Functions Virtualization (NFV), proposed by the European Telecommunications Standards Institute (ETSI), defines standards for implementing NFV. It provides a framework for replacing dedicated network hardware, such as routers, switches, and firewalls, with Virtualized Network Functions (VNFs). NFV leverages virtual machines that run on standard servers instead of proprietary hardware. This approach allows service providers to deploy new applications and on-demand services without requiring specialized hardware. NFV decouples software from hardware by virtualizing various network functions, including firewalls, load balancers, and routers, as software instances. This eliminates the need for substantial capital investment in expensive hardware components, accelerates deployment timelines, and consequently, enables faster revenue-generating services for customers. Furthermore, NFV permits multiple virtual functions to run on a single server and provides the flexibility to migrate workloads between servers.

Through virtualization, a separate logical network is created on top of the physical network. In other words, virtualization enables resources to be abstracted from their underlying physical infrastructure,

offering greater freedom and scalability during network deployment. NFV empowers the 5G ecosystem by virtualizing equipment within the 5G network. This includes network-slicing technology, which allows multiple virtual networks to operate simultaneously. NFV addresses other 5G challenges through virtualized computing, storage, and network resources that are customized according to customer applications and segments. The NFV architecture comprises VNFs, Network Functions Virtualization Infrastructure (NFVi), and Management and Orchestration (MANO). VNFs are virtual network functions that provide network sharing, file configuration, and directory services[1]. NFVi consists of a hypervisor[2] that supplies computing, storage, and networking capabilities. MANO supports the automation of new VNFs and the control of the NFV infrastructure.

6.3) Network Slicing

5G networks promise to deliver ultra-low latency and extremely high data rates while primarily supporting three major application categories, namely Ultra-Reliable Low-Latency Communications (URLLC), enhanced Mobile Broadband (eMBB), and massive Machine-Type Communications (mMTC). These diverse scenarios require a highly dynamic and scalable network architecture from mobile network operators and network service providers. The Radiocommunication Sector of the International Telecommunication Union (ITU-R) has defined the three usage scenarios of URLLC, eMBB, and mMTC for 5G and beyond. These usage scenarios were previously described within the framework of the Third Generation Partnership Project (3GPP) and are referred to as Service/Slice Types (SSTs).

Enhanced (or extreme) eMBB supports applications such as high-definition video streaming and AR/VR, generates massive volumes of data, and requires very high bandwidth. mMTC, also known as the Internet of Things (IoT), supports billions of connected devices that may not require high bandwidth but demand specialized services, such as mMIMO, to accommodate a large number of devices. URLLC facilitates use cases such as vehicle-to-everything (V2X) communications and remote surgery, which require extremely low latency. To support such services, mobile network operators must leverage MEC. The capability of 5G to deliver services across highly diverse usage scenarios is enabled through network slicing. Network slicing allows the creation of flexible and efficient specialized logical networks (network slices) on top of a shared network infrastructure. For proper operation, network slices must be isolated from one another. The cloud-based deployment of the 5G network enables the establishment of an isolated ICT environment composed of specific instances of control-plane and user-plane network functions (NFs), supported by a dedicated virtual 5GC network and customized radio bearers. Such an isolated environment effectively constitutes a 5G slice, that is, a Network-as-a-Service (NaaS) offering provided to different vertical industries.

As illustrated in Figure 15, a network operator can deploy multiple network slices—either with distinct characteristics or with identical features but targeting different groups of UE. Each network slice is associated with a unique identifier that includes the Slice/Service Type (SST), which indicates the expected behavior of the slice in terms of its characteristics and supported services. Currently, three standardized SST values are defined (Figure 16). These SSTs are used to more efficiently support roaming use cases for the most common service/slice types.

As illustrated in Figure 17, network functions (NFs) within different network slices can be deployed in various configurations and may be positioned closer to or farther from the UE, depending on the vertical application utilizing the slice. For example, an eMBB slice may employ a high-capacity radio bearer and include two UPFs, one located at the edge and the other in the cloud, to better support user mobility (i.e., dual anchoring). A vehicular slice may utilize a low-latency, medium-capacity radio bearer, with many control-plane functions moved to the edge in order to further reduce latency. An Internet-of-Things (IoT) slice may use a low-bit-rate radio bearer, a single UPF assuming limited

1. A directory service is an application or a collection of applications whose responsibility is to store and organize information related to users and network resources, and it enables the network administrator to manage users' access to network resources.
2. Hypervisor, also known as a supervisor, simulator, or virtual machine monitor (VMM), is a type of computer program that allows the creation and execution of virtual machines.

mobility, and place most control-plane network functions in the core network, provided that latency is not critical.

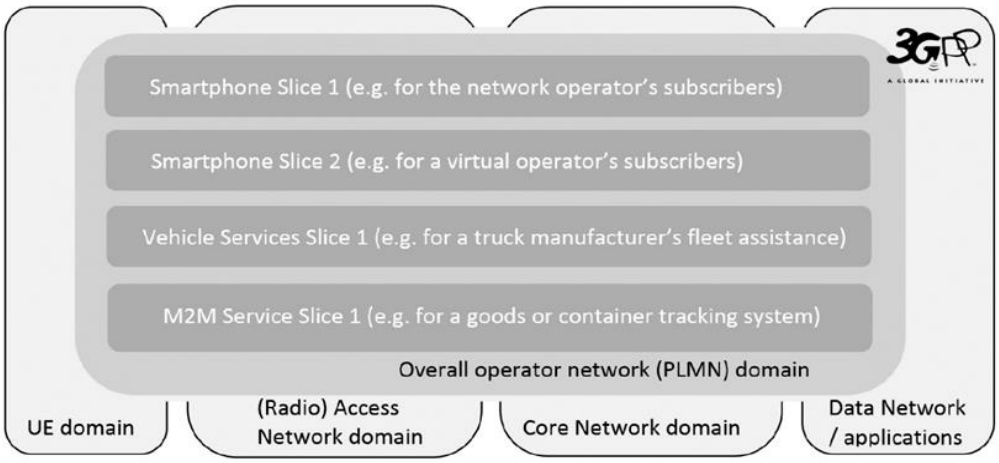

Figure 15. 5G Slicing Example

Although not depicted in the figure, some slices may share common instances of certain NFs, and some network functions, such as the Network Slice Selection Function (NSSF), are shared across all slices.

Slice/Service type	SST value	Characteristics.
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.

Figure 16. Standardised Slice/Service Type

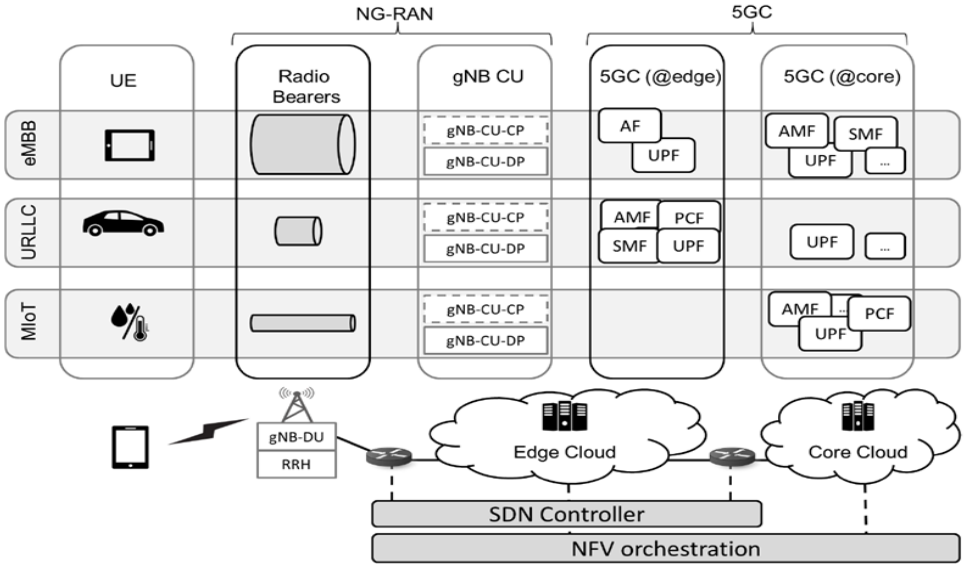

Figure 17. 5G NFs Deployment in Slices

As illustrated in Figure 18, each of the eMBB, URLLC, and IoT slices can be independently supported on a dedicated infrastructure. The eMBB slice has stringent bandwidth requirements and is supported by a physical infrastructure with high computational capabilities. URLLC is highly sensitive to network latency in application scenarios, such as autonomous driving, remote surgery, and virtual or augmented reality (VR/AR). Therefore, Multi-access Edge Computing must be deployed in close proximity to users in order to provide a short round-trip time. The IoT slice transmits very small data packets to the network but requires high capacity to register and manage millions of devices. Consequently, fewer physical computing resources can be allocated to this slice, which in turn reduces the overall operational costs.

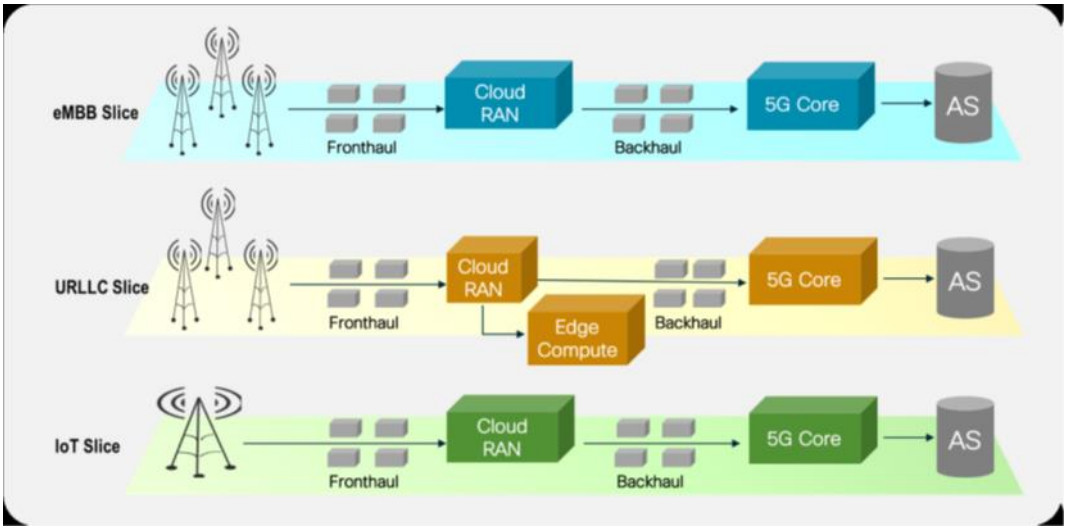

Figure 18. eMBB, URLLC, and IoT Slices, Each Can be Supported Independently on a Unique Infrastructure (Network Slicing)

6.4) 5G Multi-Access Edge Computing (MEC)

To satisfy the requirements which is highly sensitive to network latency, migrating service infrastructure to locations closer to end users is a critical approach. Accordingly, the MEC paradigm has emerged and is being designed as a key enabling technology for 5G mobile networks and beyond, taking the above considerations into account.

MEC, introduced by ETSI, is a key enabling technology for 5G networks that facilitates the delivery of new services by deploying computing, storage, and networking capabilities at the network edge, in close proximity to end users. By offloading processing and service execution from the centralized core to the edge, MEC effectively addresses the stringent latency, bandwidth, and reliability requirements of emerging use cases, such as ML, AR/VR, the Internet of Things (IoT), and latency-critical network functions that must be provided near users.

MEC is logically located in close proximity to BSs and can be operated by authorized third parties willing to provide processing and storage capabilities to 5G subscribers. MEC represents a new paradigm within the 5G ecosystem that enhances the mobile users' Quality of Experience (QoE) by extending service coverage and performance. Moreover, MEC introduces a new ecosystem and value chain, in which network operators can open the edge of their RAN to authorized third parties, enabling them to flexibly and rapidly deploy innovative applications and services for mobile subscribers, enterprises, and vertical industries (ENISA, 2020). As a result, multi-access edge computing enables new vertical business sectors and service opportunities for both consumer and enterprise customers.

MEC is a branch of cloud computing that migrates applications from centralized data centers to the network edge, closer to end users and their devices. Edge computing enables real-time data processing and computation at the network edge, while cloud computing is utilized for operations that require strong

centralized processing capabilities. In the absence of edge computing, data processing is performed in centralized cloud servers, which results in high latency and increased data-transfer costs.

By leveraging edge computing, fast decision-making can be performed near end users, which is particularly critical for emergency and latency-sensitive services. MEC plays a crucial role in achieving 5G objectives, including support for enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine-Type Communications (mMTC). Furthermore, MEC acts as a key enabler of edge intelligence, which is expected to be one of the major innovations of sixth-generation (6G) mobile networks.

MEC technology enhances network performance by reducing latency, enabling real-time awareness of the local environment, supporting cloud offloading (i.e., load shedding and traffic offloading), and alleviating traffic congestion.

One of the key technologies that enables 5G to support URLLC services is MEC. MEC involves the deployment of computing and storage platforms at the edge of the (radio) access network. Consequently, MEC enables the provision of low-latency services, while also supporting context awareness and task offloading.

As previously stated, URLLC is the most innovative and challenging use-case scenario for 5G and is inherently dependent on MEC. To effectively support URLLC services, MEC must meet stringent requirements for ultra-high reliability, which is a key performance indicator encompassing security, trustworthiness, and low latency. This is one of the main reasons why security, reliability, and performance are considered three critical aspects of MEC. By deploying diverse services and caching content at the network edge, congestion in mobile core networks is significantly reduced, enabling them to more effectively meet local service demands (ENISA, 2020).

The use of enabling technologies such as virtualization, wireless networking, and the distributed architecture of MEC makes it vulnerable to numerous types of attacks. A botnet attack is a practical example that targets IoT devices and edge equipment, which can later be exploited to launch Distributed Denial of Service (DDoS) attacks.

7) RAN Security Vulnerabilities and Threats

A substantial body of recent literature has identified numerous security and privacy issues in 4G mobile networks. Most of the reported attacks at the 4G RAN layer involve rogue Base Stations (RBSs) or IMSI catchers, which target individual users during the initial network attachment procedure, or paging attacks that exploit the IMSI-based paging mechanism. In such attacks, the IMSI information obtained may subsequently be used to launch other types of attacks. While 5G New Radio (NR) technologies mitigate well-known IMSI-related threats, the introduction of new functions and features in 3GPP Release 16 also brings additional security considerations that remain open research challenges (ENISA, 2020). Within the security analysis of the RAN, the following vulnerability domains have been identified (ENISA, 2020):

Ultra-Reliable Low Latency Communications (URLLC) Security: Inadequate QoS enforcement may negatively impact low-latency requirements. Moreover, optimization issues in monitoring and user-plane operations affect both the reliability and the low-latency performance of communications.

Vulnerability to Radio Jamming Attacks: An inherent vulnerability of wireless cellular communications lies in the open radio-frequency spectrum, which enables both intentional and unintentional interference. Such interference can adversely affect legitimate user access and lead to resilience issues in certain parts of the network.

Failure to Comply with General Security Assurance Requirements: A set of vulnerabilities arises from the need to update various RAN elements during migration phases, as well as from the limited ability of early-deployed systems to comply with updated specifications related to security functions.

Optional Nature of Security Monitoring for F1 Interface: The optional nature of security monitoring mechanisms for this specification may result in security weaknesses in its implementation.

In addition to the aforementioned vulnerability domains, virtualization-related vulnerabilities, as well as general vulnerabilities associated with hardware and software maintenance and system hardening, are also applicable. Section 4.4 in ENISA (2020) provides a more comprehensive overview of vulnerabilities affecting RAN components. According to this reference, vulnerabilities at this layer can be classified into several distinct categories, including:

1. Improper implementation of gNB security functions
2. Improper protection of Data and Information of gNB components
3. Improper protection of availability and integrity of gNB components
4. Vulnerable mechanisms for authentication and authorisation of gNB components
5. Improper session protection mechanisms of gNB components
6. Insufficient or improper monitoring mechanisms of gNB components
7. Vulnerabilities in Operating Systems supporting gNB components
8. Vulnerabilities in Web Servers supporting gNB components
9. Vulnerabilities of network devices running gNB components
10. Improper hardening of gNB components
11. Virtualisation vulnerabilities of relevant gNB components
12. Physical and environmental vulnerabilities of relevant gNB components
13. Vulnerability to Radio Jamming Attacks

Table 1 maps the threats to radio layer along with Edge, device and service layers of 5G architecture. N/A stands for Not Applicable. N/A means that the threat category is not relevant or meaningful for that specific layer. The service layer provides the application interface to the users. Service providers define the application programmable interfaces (APIs), and the architecture of this layer is independent of the underlying 5G architecture.

7.1) Security Vulnerabilities in mMIMO

First, it should be noted that, in general, there are two types of eavesdropping attacks: passive and active. In passive eavesdropping, the attacker attempts to intercept transmitted reference signals without transmitting any signals themselves. In contrast, in active eavesdropping, the attacker also transmits signals in order to disrupt the communication of legitimate users. If the sole objective of an active attack is to interfere with legitimate transmissions, it can be classified as a jamming attack. Another, more sophisticated form of active attack is based on reference signal contamination, known as a pilot spoofing attack, in which the attacker masquerades as a legitimate user. Massive MIMO is generally resistant to eavesdropping because beamforming concentrates the signal energy toward the legitimate UE. However, mMIMO is vulnerable to active eavesdropping, particularly when the attacker performs pilot contamination/pilot spoofing attacks and interferes with the channel estimation process.

Typically, channel state information (CSI) is used for transmission precoding so that a composite beam, formed by signals transmitted from multiple antennas, can be focused toward a specific user. CSI is obtained through the channel estimation process, which is usually based on pilot (reference) signals transmitted by legitimate users. In a pilot spoofing attack, the eavesdropper transmits identical pilot signals to the BS in order to confuse the channel estimation process. As a result, the BS designs the precoder incorrectly, which in turn facilitates eavesdropping by the attacker. Since pilot training sequences are fixed and periodically reused over time, an attacker can acquire them. Consequently, the estimated channel between the legitimate user and the BS becomes inaccurate, while simultaneously enabling the attacker to better detect the signals transmitted by the BS.

Table 1. Categories of 5G Threats Mapped with Radio, Edge, Device and Service Layers (Farooqui et al., 2022)

Attack Categories	Device Layer	Edge Layer	Radio Access Network Layer	Service Layer
Network Configuration Manipulation	Exploitation of misconfigured data OS services tampering	Routing table manipulation Malicious network function registration	N/A	DNS manipulation Exploitation of misconfigured data Exploitation of misconfigured service Tampering of Cryptographic keys and policies OS services tampering
Malicious Software	Worms Ransomware Botnet	Malicious network functions	N/A	Worms Ransomware Botnet Injection attacks
Remote Access	VPN configuration exploitation	N/A	N/A	VPN configuration exploitation
Hardware Manipulation	N/A	Side channel attacks	N/A	Side channel attacks
Unauthorized Access	N/A	N/A	IMSI catching attacks	Port Knocking Brute force
Information Leakage	N/A	N/A	Network traffic Unauthorized access to signaling data	Misuse of security audit tools
Data Breach	File misuse Customer data theft	N/A	N/A	Log tampering File misuse Customer data theft
Eavesdropping	Session hijacking Device/data identity tracking	N/A	Traffic sniffing Man in the middle attack Air interface eavesdropping	Session hijacking
Physical Attacks	Theft	Sabotage of network hardware Terrorist attacks	Sabotage of network hardware Terrorist attacks Unauthorized physical access to base station	N/A
Accidental	Human error Misconfigured systems/ network Unintentional deletion	N/A	N/A	Human error Unintentional deletion
Network Slicing Specific	N/A	Unauthorized access Misuse of resources and function Side channel	Misuse of resources and function Side-channel	Unauthorized access Misuse of resources and function Side channel

According to several studies, defending against jamming attacks is more challenging for mMIMO receivers than mitigating pilot spoofing attacks. In this case, unlike pilot spoofing, the attacker aims to generate the maximum possible interference. Jamming attacks are typically mitigated by receiver designs that treat the jamming signal as additional noise. However, since the legitimate channel and the jamming channel are correlated, the interference in mMIMO systems is not purely noise-like, which leaves room for further investigation.

As previously mentioned, the concept of beamforming, whereby multiple antennas serve a specific user, inherently enhances the resilience of mMIMO systems against passive eavesdropping attacks. Nevertheless, an eavesdropper may counteract this advantage by exploiting highly correlated channels in the vicinity of the legitimate user or by taking advantage of weaknesses in channel estimation. The channel estimation process in mMIMO is therefore considered a soft target for security attacks. Furthermore, falsified CSI can also be exploited to launch jamming attacks.

7.2) Practical and Documented Examples of RAN Threats

In this section, some practical and documented examples of RAN threats in 5G are provided.

1. Rogue/fake BS attacks: In recent years, attacks such as IMSI catchers (e.g., Stingray) have been extensively deployed against legacy cellular networks, including 2G, 3G, and 4G systems. Recent studies have demonstrated that, with minor modifications, similar attacks can also be successfully executed on experimental 5G networks. By deploying a rogue BS, attackers are able to lure UE into connecting to the fake network and subsequently collect users' identity-related information (Borgaonkar & Shaik, 2021).

2. Intentional jamming attacks: In 2020, academic researchers conducted intentional jamming attacks against 5G frequency bands in a controlled test environment operating on band n78. By leveraging software-defined radio (SDR) hardware, they successfully disrupted the communication link between the UE and the 5G network, resulting in a complete service outage. This study systematically investigated physical-layer security vulnerabilities in 5G networks and experimentally demonstrated the feasibility of jamming-based attacks.

3. Vulnerability in radio modems: In 2021, researchers from Google Project Zero identified multiple vulnerabilities in the firmware of Qualcomm modems (e.g., CVE-2020-11292), which allowed an attacker to remotely compromise user devices by transmitting crafted messages over the radio interface. These vulnerabilities enabled remote code execution and device takeover without requiring user interaction[1].

4. Cyberattack on a base station (gNodeB attack): Researchers at the Black Hat Asia 2023 demonstrated that software vulnerabilities in the implementations of certain commercial gNodeBs (gNBs) could be exploited to gain unauthorized access to internal configurations and management interfaces of BSs, enabling attackers to manipulate traffic flows or alter service states[2].

5. Denial of service (DoS): In 2021, researchers at the University of Amsterdam successfully disrupted subscriber services by sending frequent forged signaling messages to the RAN layer, thereby exhausting BS resources. Their work focuses on DoS vulnerabilities and attacks targeting 5G radio resources, highlighting design and implementation weaknesses in 5G networks related to radio resource management (RRM). The study further provides an experimental evaluation of attack scenarios and corresponding defense mechanisms[3].

These examples demonstrate that RAN-related threats in 5G networks are tangible and realistic, and that practical experiments have been conducted to validate their feasibility.

1. A public report on vulnerabilities and real-world attack scenarios for over-the-air (OTA) remote exploitation of Qualcomm modems, titled "A Walk in the Park: Over-the-Air Exploitation of a Qualcomm Baseband," has been published by Google Project Zero. This report also explains, step by step, the methodologies and techniques for discovering and hunting these vulnerabilities.
2. The presentation, titled "Abusing 5GC and RAN Implementations," delivered at Black Hat Asia 2023 by the Positive Technologies team, includes technical insights, real-world attack examples, and a novel perspective on new attack vectors in the 5GC and RAN.
3. In part of the USENIX Security Symposium 2021, the results of these researchers' work were presented under the title Dos Attacks On Radio Resources Of 5G Networks.

7.3. Specific Security Aspects

In this section, we present the threat vectors (TVs) in the AN related to a typical MEC deployment, in alignment with the ETSI reference architecture. In a wireless communication network, threats mainly originate from the AN. The primary reason for those threats is the diversity of technologies deployed within the AN domain. Moreover, given the heterogeneous nature of MEC-enabled services, the scalability of the access-network-based TVs constitutes a major challenge for their practical applicability. Therefore, the TVs related to the AN can be classified into three general categories, which are examined in the following subsections as A1, A2, and A3. Figure 19 illustrates the locations at which these TVs are applied across different network layers.

A1 (Link Between the UE and BS):

The UE–BS connection represents the most common communication link in mobile systems and is also the most vulnerable link to security threats. Since Threat A1 targets the most exposed segment of the mobile communication network, an adversary can interfere with the communication process or introduce a malicious component to compromise the BS. Mobile offloading, which delegates computationally intensive tasks to edge service providers, is primarily driven by the resource limitations of UEs. In offloading scenarios, large-scale data storage and processing significantly increase the volume of network traffic transmitted over the air interface. Furthermore, emerging technologies, such as MIMO, interference-aware receivers, advanced coding and modulation schemes, mmWave communications, carrier aggregation, Wi-Fi offloading, LTE, and Licensed Shared Access (LSA), have been introduced in the access network to improve SE. UE connectivity across these heterogeneous technologies raises concerns regarding interoperability and adaptation mechanisms, which may be exploitable by attackers.

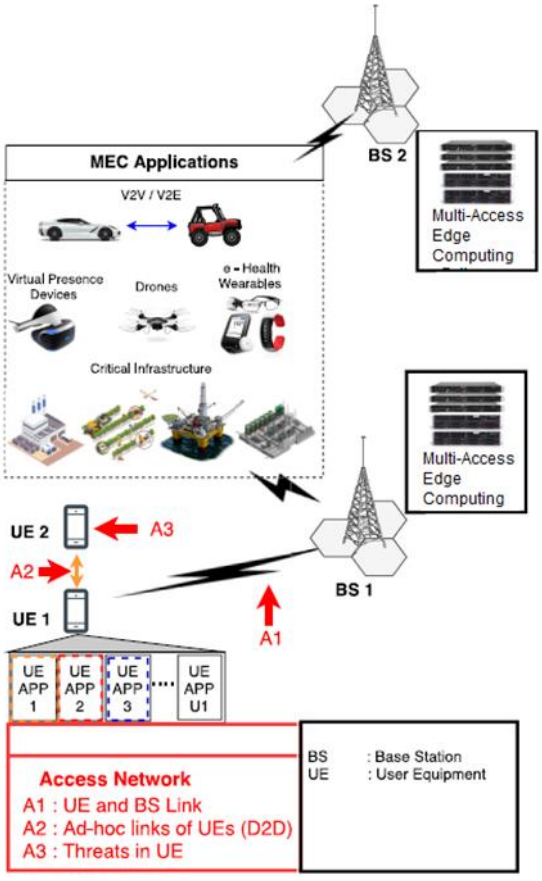

Figure 19. TVs in Access Network Associated with a Typical MEC Deployment from a Location-Based Perspective

Vulnerabilities and threats: The broadcast nature of the wireless air interface that connects the UE to the BS inherently exposes this link to a wide range of security attacks, such as:

- Eavesdropping and hijacking: As part of attacks such as man-in-the-middle[1] (MitM), relay attacks[2], advanced persistent threats[3] (APTs), Sybil attacks[4] (multi-identity attacks), and spoofing, wireless communication channels are hijacked to intercept and retrieve transmitted information. MitM attacks are particularly feasible in 5G networks and non-3GPP WLANs, where they may compromise virtualized infrastructure entities at the network edge (Porambage et al., 2018). The lower levels of encryption and integrity protection commonly found in resource-constrained IoT devices further increase the risk of compromising communication channels connected to MEC edge systems (Wang et al., 2019). Through such attacks, adversaries may gain access to MEC applications (ME Apps) running on MEC hosts (MEHs) and manipulate the MEH virtualization infrastructure to exhaust available resources. Moreover, compromised MEHs can be leveraged to propagate attacks to other interconnected MEHs, thereby enabling attempts at privilege escalation[5] and wider system compromise.
- Denial of Service (DoS) and Jamming: The primary objective of wireless channel interference and DoS attacks is to compromise the availability of the RAN connected to the MEC system. Such attacks are particularly detrimental to latency-sensitive applications, as the induced delays can significantly degrade service performance in next-generation networks. Consequently, a compromised MEC host (MEH) may be exploited to block services delivered to end users, or system-level MEC entities may be disrupted through unnecessary or malicious queries, ultimately leading to a service-wide outage of the MEC infrastructure. Moreover, emerging botnet-based DDoS attacks are capable of challenging the access capacity of system-level MEC entities, thereby threatening the overall resilience and availability of the MEC ecosystem.
- Malicious Node Injection: The diversity of UEs connected to the BS introduces significant challenges in managing adaptation and interoperability among mobile devices manufactured by different vendors, as well as the heterogeneous communication protocols and UE applications (UE Apps) they employ. Under such conditions, malicious nodes can be injected into the system and exploit existing vulnerabilities in UE equipment. These vulnerabilities include device cloning[6], reliance on less secure wireless protocols (e.g., WPA/WPA2), susceptibility to hardware Trojans, the use of predictable access control credentials (e.g., patterns or PINs), and reduced resilience against software-based threats masquerading as benign UE App components, such as spyware, Trojans, and malware. Exploitation of these weaknesses enables the delivery of malicious payloads or falsified information from compromised UEs through the BS to ME Apps, thereby manipulating the services provided by the MEC host (MEH). Nevertheless, such attacks can be mitigated by deploying robust authentication mechanisms integrated with a trust management framework for UE–BS connectivity, which enhances the overall security posture of the RAN–MEC ecosystem.

A2 (Ad-Hoc Connectivity Between User Equipment):

1. Intervene a communication link by intercepting the channel. Once accessed, the attacker could alter or mislead the communicating parties. All the communication and internal links within and egressing the edge platform are prone to such attacks.
2. Combination of a MitM and a replay attack (resending extracted authentication credentials at a later instance to be identified as a valid user). Communication links towards the MEC system is subjected for these threats.
3. A cyber-attack in which a series of hacking attempts are forwarded to a targeted entity. UEs and MEC interfaces are subjected to APTs via the air interface.
4. Attack launched by forging large number of pseudonyms identities. Thease attacks could be target IoT context.
5. Launched by an internal or external adversaries exploiting the infrastructure vulnerabilities, such as ill-maintenance and mis-configurations using privileged control or inside information.
6. A cloning attack refers to an attack in which the adversary duplicates the identity or attributes of a legitimate entity—such as a UE, SIM, IoT device, or network node—to create a fraudulent but seemingly valid replica. In this type of attack, the attacker extracts or guesses identity information, such as IMSI, keys, PHY parameters, and hardware/software fingerprints, and uses it to impersonate the original device.

Threats associated with the A2 interface are related to ad-hoc links established directly between UEs. These links rely on short-range communication channels that are typically utilized by specific UE Apps for data exchange. This communication paradigm corresponds to D2D connectivity, where a direct communication link is established between two UEs without the involvement of any BS (Kumar et al., 2018; Porambage et al., 2018; Roman et al., 2018). In addition, FlashLinQ services and Proximity Services (ProSe) are also capable of establishing D2D communication platforms. FlashLinQ, developed by Qualcomm, facilitates content sharing, gaming, and social networking features among nearby devices. ProSe is a standard specified by 3GPP to enable proximity discovery and direct communication for future AN based deployments.

Vulnerabilities and threats:

- Attacks on Short-Range Communication Technologies: Attacks such as eavesdropping, impersonation[1], forging, free-riding[2], DoS, and privacy violations are highly probable (Hamoud et al., 2017). Most of these attacks are enabled by the inherent characteristics of the communication protocols embedded in such technologies. In particular, these protocols tend to prioritize bandwidth efficiency and low-latency communication to support D2D interactions, often at the expense of strong security mechanisms. As a result, insufficient authentication, encryption, and access-control measures increase the attack surface and expose UE-to-UE communications to a wide range of security and privacy threats.
- D2D Traffic Offloading: The method of offloading cellular traffic to UEs by the mobile network operator (MNO) is an example of an activity in the D2D domain (Hamoud et al., 2017). In this approach, the MNO delivers content only to selected UEs designated as cluster heads, which subsequently disseminate the content to other UEs within the same cluster. Moreover, use cases such as extending coverage through D2D connections in rural areas and establishing critical communication channels during disasters or emergency situations (where the cellular network is inactive) envision the future potential of D2D-based services. In these scenarios, connectivity between cluster-head UEs and MEC service providers is established under the supervision of the MNO to enable content sharing and service delivery. Therefore, this scenario creates new opportunities for attackers to exploit cluster-head UEs in order to use service manipulation[3] provided by them.

A3 (UE equipment):

A UE may correspond to a mobile phone, personal computer, closed-circuit television (CCTV) camera, wearable device, or sensing system, which can be directly connected to a BS or indirectly via a gateway device. The wide diversity of technologies attributed to UEs—including operating systems (e.g., Android, iOS, Windows, Symbian, BlackBerry, and WebOS), memory management mechanisms (e.g., SD, micro-SD, and HDD), communication interfaces (e.g., RF, RFID, NFC, Bluetooth, Wi-Fi, and Ethernet), as well as physical design and hardware architecture—renders the deployment of a unified and comprehensive security solution for all UEs. UEs store and process information related to multiple aspects of an individual's daily life, including private data (e.g., photos, medical records, health statistics, and surveillance video), location information (GPS), daily routines (shopping and transportation patterns), organizational data, critical infrastructure information (e.g., energy consumption, financial and banking data, and emergency services), and online account credentials. The disclosure of such credentials and contextual information may have severe and potentially life-threatening consequences for individual well-being (Roman et al., 2018). Consequently, mobile user privacy threats constitute a major security concern (Abbas et al., 2018). The embedded resources of

1. An impersonation attack is a highly probable threat as it could target network slice entities in different scenarios in the interaction. In terms of security, impersonation attacks are plausible, due to the inadequacy of mutual-authentication schemes within inter-slice entities.
2. A free-riding attack is an attack in which an adversary exploits a system without contributing a fair share. Systems that are vulnerable to free-riding attacks either operate with reduced capacity or completely collapse. This is because as the number of free riders increases, the system costs are increasingly borne by the remaining honest users, encouraging them either to leave the system or to become free riders themselves.
3. Service manipulation atack is a service offered by any service providing entity is taken over forcefully to launch selective DoS or information tampering attacks.

UEs, particularly computational power, storage capacity, and battery lifetime, represent key factors influencing this threat vector (Wang et al., 2019). Certain software-based and virtualized attacks require only a minimal level of resources to be deployed on an execution platform. Therefore, the enhanced processing and storage capabilities of modern UEs increase the feasibility of launching stealthy attacks that are capable of evading detection by conventional security mechanisms.

Vulnerabilities and thereats: Threats may be instantiated by a UE either with or without the user's awareness. Even a legitimate user may unintentionally activate malicious software agents, thereby facilitating the execution of attacks. The exposure of UEs to both physical and remote attacks renders this threat vector particularly critical. UEs are vulnerable to physical damage[1], Side-Channel Attacks[2] (SCAs), malicious code injection[3], and hardware Trojans[4] (HTs), while other attack classes described in TVs A1 and A2 are primarily applicable to the communication interfaces. This broad attack surface significantly amplifies the security and privacy risks associated with UE-centric deployments in modern mobile and MEC-enabled networks.

- Physical attacks: Physical attacks are the most common type of attacks for this TV, in which the attacker induces the reconfiguration of the compromised equipment to transfer false information to ME Apps (Abbas et al., 2018). By sending fake but carefully crafted information to edge equipment, these misinformation attacks cause the MEC system to shut down or disrupt its services. A representative reconfiguration scenario involves ME Apps being executed continuously without termination or resource controlling, thereby exhausting the available computational and storage resources at the edge. This form of resource-draining behavior significantly undermines the availability and reliability of MEC services, and may further propagate disruptions to interconnected MEC hosts.
- Side channel attacks (SCA): The primary objective of launching a SCA is to extract cryptographic secrets or security-critical parameters from cryptographic modules and implementations. Acoustic cryptanalysis, electromagnetic (EM) analysis, timing analysis, power monitoring, and differential fault analysis are among the SCAs that can be effectively conducted against UEs. Security protocols engaged in communication channels are exposed with such revealed credentials. Both UEs and MEHs, when deployed in a loosely protected edge environment, remain highly exposed to such attacks. Due to the diversity and heterogeneity of SCA techniques, their detection is inherently challenging, while mitigation and countermeasure deployment demand substantial time and computational resources.
- Malware: Malware and computer viruses constitute a high-risk threat factor for UEs, as their infection vectors may materialize through multiple and diverse mechanisms. The consequences of a malware attack are largely similar to those of malicious code injection attacks; however, the severity and impact depend on the specific malware type, including Trojans, worms, rootkits, spyware, ransomware, and adware. In particular, virus and worm attacks represent a class of threats in which disruption of all the process in an infected UE will attempt to propagate the malicious agent to the MEH. A malware-infected UE may further attempt to propagate the malicious agent toward the MEH, thereby extending the attack surface from the user layer to the edge computing infrastructure. This propagation capability significantly amplifies the risk of service disruption, resource exhaustion, and lateral infection across interconnected MEHs.
- Mobile delegation circumstance: Service offloading driven by mobile devices may result in the adoption of different offloading mechanisms, including full offloading and partial

1. The adversary manipulating the entity or device physically to gain access or sabotage. UEs are imminent for physical tampering.
2. A crypt-analysis attack to determine the secure credentials of a protocol without exploting the vulnerabilities of the crypto algorithm, such as acoustic crypt-analysis. UEs and MEHs in an exposed edge environment are subject to SCAs.
3. Code fragment of a malicious agent is injected to an active agent or a transferring executable content. Such attacks are immunent with service migration scenarios in MEC.
4. Malicious modification of the circuitry in a device for leaking information through radio emission and manipulate or destroy the hardware platform of the device. With 5G radio TRxs, HTs can impact the secure continuity.

offloading performed by the UE. These offloading paradigms are inherently susceptible to security attacks (Mach & Bečvář, 2017). A compromised UE App, or a UE performing full or partial execution offloading, as well as offloading of passive content to the MEC service provider, may possess the capability to inject a malicious agent that is subsequently activated within the corresponding ME App, hosted on the MEH. Such attacks directly contribute to and reinforce threat vectors enabling the propagation of malicious code, unauthorized execution, and resource abuse within the MEC infrastructure.

- Gateway-Based Vulnerabilities in UE-Centric Deployments: Vulnerabilities in gateway-enabled devices arise when a UE operates as a Machine-Type Communication Gateway (MTCG) for applications such as e-health services or other MTC deployments. In such scenarios, malicious content may be generated by one of the connected sensors or actuators, while the UE functions as an intermediary entry point, facilitating unauthorized access and intrusion into the network. By acting as a trusted communication gateway, the compromised UE significantly expands the attack surface, enabling adversaries to leverage upstream trust relationships and propagate malicious activities toward MEC services and hosts. This gateway-centric threat model highlights the critical role of UE security in protecting sensor networks, medical systems, and large-scale MTC infrastructures.
- Resource Exhaustion and Manipulation of MEC Platform Functions: Resource allocation and scheduling of ME apps are monitored and enforced by the Mobile Edge Platform (MEP) within each MEH. In delegation or offloading scenarios, the MEP maintains direct communication with the UE application to coordinate execution and resource usage (European Telecommunications Standards Institute, 2016; Mach & Bečvář, 2017). A compromised or malicious UE app may exploit this interaction to influence the MEP into allocating unnecessary or excessive resources within the MEH, ultimately leading to service disruption or DoS. The ability of a UE to be deployed in a tamper-resistant manner, leveraging lightweight yet effective cryptographic primitives with high flexibility, is largely dependent on the device design and the equipment manufacturer. Insufficient hardware-level protection and weak trust anchors significantly increase the feasibility of resource abuse, platform manipulation, and persistent attacks against MEC infrastructures.

It is important to note that one of the attacks that affects the RAN through the three TVs A1, A2, and A3 is the Reduction of Quality (RoQ) attack. In an RoQ attack, the adversary generates low-rate but well-timed traffic that degrades RAN QoS (increased latency, jitter, and reduced throughput) without causing a full outage. It exhausts radio and scheduling resources at the gNB and is particularly harmful to URLLC and MEC services. According to Ranaweera et al. (2021), RoQ attack enabling a manipulated service to attain more resources, such as bandwidth in communication link, than it requires; like a UE opting for excessive bandwidth from the MEC eNB

8) RAN Security Solutions

As previously discussed, all service requests generated within the RAN are forwarded to cloud service providers located at geographically distributed sites, due to the lack of native storage and processing capabilities at the BS. In addition, MEC-based services deployed within the RAN enhance computational processing capabilities at the network edge, thereby mitigating mobile traffic bottlenecks and improving service responsiveness. Consequently, adversaries may exploit the RAN as an entry point to launch security attacks against cloud servers or MEC-based service platforms. The exposure of service request flows and control signaling at the AN significantly broadens the attack surface, enabling threats that target service availability, integrity, and confidentiality across both centralized and edge computing infrastructures. Therefore, this section focuses on the security mechanisms and countermeasures within the RAN, as a foundational step toward protecting cloud-assisted and MEC-enabled services against access-layer attacks.

8.1. Security Solutions Related to mMIMO

One method for detecting an active eavesdropper is to exploit controlled randomness by transmitting random pilot sequences. The legitimate user sends a sequence of random phase-shift-keying symbols, and the BS detects the presence of an eavesdropper. The drawback of this method is the additional overhead incurred by transmitting extra random sequences. In another approach, beamforming is designed such that the received sample at the legitimate user equals a predefined value. If an active eavesdropper exists, the legitimate user receives a significantly lower value. Detection of an active eavesdropper can also be performed using cooperative BSs, where different BSs exchange information. Moreover, ML techniques can be employed to detect active attacks.

Since a mMIMO BS can simultaneously serve a large number of users, it is necessary to protect the message from all users except the intended one. Therefore, the precoding algorithm used at the BS must be designed to achieve this goal. It is also possible that the eavesdropper employs a powerful LSA array to intercept the information. To counter such attacks, a physical layer security (PLS) approach has been proposed, known as the secure phase-rotated pilot transmission scheme. The main idea of this method is to apply a random phase rotation to the primary pilot in order to confuse the eavesdropper. On the other hand, legitimate users are able to correctly interpret the phase rotation and apply the appropriate dedicated operators required to recover the primary pilot.

Another approach to counter jamming attacks on the mMIMO uplink is the design of a jammer-resilient receiver. In this method, pilot sequences are not used to estimate the interference channels. Instead, the receiver filters are designed based on both the legitimate user channels and the jammer channels in order to mitigate the effect of jamming pilots. These filters are based on MMSE and ZF criteria. Another method for detecting jamming attacks is the use of a generalized likelihood ratio test (GLRT). The performance of the detector improves as the number of BS antennas increases. Another countermeasure is an anti-jamming strategy based on pilot retransmission. In this approach, anti-attack schemes are introduced for both random and deterministic jamming attacks.

8.2. Security Solutions Related to Access Network Threat

Existing solutions related to Threat A1, which ensure the CIA security attributes (Confidentiality, Integrity, and Availability) of the air interface, can be categorized as follows: The use of cryptographic primitives and their effectiveness, AN solutions, and physical layer–level security solutions.

- Improvement of cryptographic primitives: The use of conventional security primitives imposes additional overhead on the aggregated traffic payload space at the application layer. Despite the bandwidth improvements and multi-channel support provided by 5G and MEC, such heavyweight approaches limit the scalability of new applications, such as autonomous vehicles, in terms of extending their functionalities. Therefore, lightweight cryptographic primitives, as demonstrated in the study by Chen et al. (2022), or quantum-resistant (QR) cryptographic approaches (Yu et al., 2019), can be employed to increase the complexity of the involved security schemes. To overcome traffic-oriented security violations in the AN, Rahman et al. (2017) proposed a mechanism for encrypting the payload transmitted between the UE and the BS, using 256-bit Advanced Encryption Standard (AES). Pilot signaling procedures were secured using a strategy inspired by the Open Whisper System (OWS), while per-session AES keys were regenerated to ensure forward secrecy.
- Physical layer solutions: Another approach to reducing the application-layer overhead is to embed security mechanisms at the PHY. However, these approaches are diverse and highly dependent on the communication equipment (i.e., vendor architecture), the environment (e.g., wireless or wired, fiber-optic), and the underlying technology (e.g., BLE, Wi-Fi, ZigBee, or LoRaWAN). Therefore, to avoid interoperability and compatibility issues associated with PHY-layer protocols, an adaptation based on the fundamental principles of PLS should be employed. Wang et al. (2016) proposed a PLS model for multi-tier heterogeneous cellular networks (HCNs), in which entities are randomly deployed. In the

proposed model, a confidential mobile communication policy is formulated based on the average received signal power (ARSP). The SINR is used to determine the connection probability of UEs. Since, in wireless communications, the broadcast nature of the signal makes it vulnerable to eavesdropping attacks, confidential information must be protected using appropriate security techniques. Recently, PLS methods have attracted significant attention from researchers due to their simplicity of implementation compared to conventional cryptographic approaches (Ragheb et al., 2010, 2022, 2024; Kuhestani et al., 2024).

- 5G-based access network solutions: In a study a wireless 5G security architecture was proposed to cover the following domains: network access, network, user, and application. The network access domain is related to Threat A1, where physical-layer technologies, such as mMIMO, HetNet, and D2D, are identified as security challenges that must be addressed. Xiao et al. (2018) introduced a ray-tracing-based channel model for securing 5G mmWave small-cell communications. Beam propagation phenomena, including line-of-sight (LoS), reflection, refraction, and scattering, were taken into account.

5G-based RF networks are still in the experimental stage. Both the channel models and the network architecture must be clearly defined and standardized for each 5G-based use case to avoid inconsistencies and interoperability issues after deployment. During the development of such standardization processes, security and privacy must also be considered as primary requirements, rather than as afterthoughts.

Existing solutions related to Threat A2: Ensuring security in D2D communications is mainly focused on authentication mechanisms, while interference and MitM–type attacks can be mitigated through a layered security model.

- *Authentication mechanisms:* To overcome potential vulnerabilities of ad-hoc links, an independent authentication mechanism prior to establishing a D2D link is an inherent requirement. Rahman et al. (2017) proposed a two-way mobile number-based authentication scheme to secure potential D2D interactions within their application framework.
- *Physical unclonable functions (PUFs):* Physical Unclonable Functions (PUFs) are emerging approaches used for authenticating non-human entities by matching biometric-like fingerprints generated from unique characteristics inherently introduced during the manufacturing process of devices or circuits, based on challenge–response pairs (CRPs). Hao et al. (2018) proposed an end-to-end physical-layer (PHY) authentication scheme, in which a PHY-ID based on identity-based encryption (IBE) is extracted from RF carrier frequency offset (CFO) and in-phase/quadrature imbalance (IQI) features derived from D2D transmissions of IoT devices. In this proposed system, CFO and IQI act as PUF features. Gao et al. (2016) investigated emerging nanotechnology-based PUFs in electronic circuits and, at the same time, classified strong and weak PUFs based on their performance criteria.
- *Layered security:* A layered security model was proposed by Hammoud et al. (2017) which applies different security mechanisms at each layer as follows: 1) Application layer: IBE, elliptic curve cryptography (ECC), group key management, probabilistic key management, and ciphertext-policy attribute-based encryption (CP-ABE). 2) Network layer: secure multi-hop D2D communications, data separation and mixing based on secure network coding, attacker goal modeling using game theory, routing monitoring, and Public Key Infrastructure (PKI)-based group key management. 3) MAC layer: a multi-priority access control monitoring framework for location and identity privacy. 4) Physical layer: CSI-based key extraction, radio resource allocation schemes, and a joint access control and power control scheme based on confidentiality.

The main security challenge in D2D communications is resource scarcity, particularly in IoT and cyber-physical system (CPS) devices. Therefore, lightweight security approaches are essential for energy efficiency, while security keys, hash functions, and authentication codes must be generated in an optimized manner. Since these mechanisms are mostly autonomous, authentication credentials are often computed algorithmically, which makes them potentially replicable by a resourceful attacker. Consequently, PUFs, by exploiting unique, non-cryptographic analytical parameters, address an important aspect of secure M2M communications by protecting D2D channels. However, during authentication phases or within layered security frameworks, repeated message exchanges, including encapsulation, coding, and modulation structures, consume energy without contributing to throughput. Therefore, a minimal and carefully selected set of security features/mechanisms must be identified for each D2D or M2M operation to maximize operational lifetime.

Existing solutions related to Threat A3: Since attacks associated with this TV target the UE and its input/output channels, the corresponding solutions primarily focus on the detection and mitigation of SCAs and malware infiltrating the UE.

Detection of SCAs: The Side-Channel Attack Detection Tool (SCADET) introduced by Sabbagh et al. (2018) can be used to identify Prime+Probe-type SCAs on micro-architecture–based devices, which are commonly employed in IoT equipment to perform various functions. Mushtaq et al. (2018) proposed a cache-based detection method for similar SCAs targeting the AES algorithm. Wang et al. (2018) employs a deep learning technique to detect SCAs, while Javed et al. (2023) detects motion-based SCAs through keystroke dynamics on smartphone keypads.

Malware detection: Islam et al. (2017) introduced Qualcomm's Snapdragon Smart Protect as a suitable solution for UE protection, aiming to safeguard mobile devices against malware and other attacks. Snapdragon, which is a low-power, always-on system, leverages ML to detect abnormal behaviors and threats originating from Wi-Fi access points. As a result, the detection of infected UE App becomes feasible, while the WiFi-based exploits could be mitigated to secure the UE device. In addition, the same study proposes a detection mechanism that performs both static analysis and run-time behavioral analysis of UE Apps.

Security framework: Krupp et al. (2017) proposed an enhanced Security and Privacy Enhancement (SPE) framework for UE or mobile devices. The main feature of SPE is that installing the system does not require jail-breaking or rooting the existing operating system, which makes the system independent of operating system updates. In addition, the framework focuses on application-level objectives related to user data, action validation, and enforcement of security policies.

The higher resources and functions available for mobile devices, in addition to threats originating from various types of malware, SCAs, physical, or cloning attacks, also attract new application-level threats. In fact, attackers can combine attack techniques, in which malware attacks and SCA-type attacks are carried out jointly as part of a single threat attempt. A conventional Intrusion Detection System (IDS) is not sufficient to identify all these emerging attacks. Therefore, application-level security features must be embedded during the design phase of mobile devices to detect and prevent such attacks. Although techniques for detecting SCAs currently exist, new side channels are occasionally created by attackers.

8.3) General Countermeasures for RAN Vulnerabilities

A detailed list of some RAN vulnerabilities and corresponding security solutions is provided in Appendix E of ENISA (2020). In this appendix, in addition to explaining the details of RAN vulnerabilities, the relevant security requirements and/or security controls are also described.

9) Threat Ranking

In this section, we aim to rank RAN threats in 5G networks. For threat ranking, by introducing a risk metric, a score is assigned to each threat so that, ultimately, the threats can be prioritized.

Risk is defined as the probability of the occurrence of damage or harm resulting from a specific hazard. In brief, risk refers to the likelihood of an undesirable event and its associated consequences. According to IEEE definitions, risk is an objective quantity used to describe the extent of damage to a

specific system arising from various activities and technologies (Huang et al., 2020). It should be noted that a risk metric is a criterion used to measure and evaluate the risk level of a threat or incident. In network security, the risk metric is typically defined based on two main indicators:

1. Likelihood/Probability of occurrence: This indicator expresses how probable the occurrence of a threat or vulnerability is, or how frequently it is expected to occur.

2. Impact/Consequence: This indicator expresses the extent of damage or harm that would be inflicted on an organization or system if the threat were to occur. Therefore, by definition, risk is defined as the product of the "likelihood of threat success" and the "impact or severity of that threat." The risk metric in network security is used across various contexts, including:

- Threat ranking and prioritization: By using the risk metric, different threats can be scored and the most critical ones can be identified.
- Decision-making for mitigation: Higher risks require greater attention and investment for effective management.
- Evaluation of security solution effectiveness: Reducing either the likelihood or the impact of a threat leads to a reduction in overall risk.

Therefore, in the 5G domain, the risk metric helps to identify more critical threats and to adopt appropriate countermeasures to mitigate them. Based on recent references, five levels are considered for the impact/severity of threats, according to which a numerical score is assigned in order to prioritize the threats (Table 2).

a) Threats with severe and irreversible consequences (critical severity, assigned a score of 10),

b) Threats with significant but recoverable consequences at high cost (high severity, assigned a score of 8),

c) Threats with moderate consequences that are recoverable at a reasonable cost (medium severity, assigned a score of 5),

d) Threats with relatively minor consequences that are recoverable at low cost (low severity, assigned a score of 2),

e) Threats with negligible consequences that are recoverable at a very minimal cost (zero severity, assigned a score of 0).

To calculate the risk, first the likelihood of success of the mentioned threats/attacks is examined based on reliable references (such as ENISA documents) as well as the expert judgment of three specialists in this field. Then, the impact of these attacks is investigated and analyzed.

Table 2. Impact/Severity Level of Threats

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Table 3 presents the threats/attacks against the RAN and their association with TVs. In this table, data exfiltration refers to a type of data theft; for example, the intentional, unauthorized, and covert transfer of data from a computer or another device. Data exfiltration can be carried out manually or

automatically using malware. This attack is considered among the most damaging threats in computer security.

Table 3. Likelihood of Threats/Attacks Success against the RAN Segment of the Network

Threat/Attack	Likelihood of success
Viruses/Worms	0.25
DoS/DDos	0.5
Eavesdropping/Hijacking	0.5
Jamming	0.3
MitM	0.3
Relay attack	0.25
APTs	0.25
Sybil attack	0.15
Spoofing attack	0.2
Physical damage	0.2
Malicious node injection (Fake/Rogue base station)	0.2
Reduction of quality (RoQ) attack	0.31
Service manipulation	0.25
Privilege escalation	0.3
VM manipulation attack	0.25
Software vulnerability	0.4
Data exfiltration	0.35
Malicious code injection	0.35
Phishing[1]	0.75
Brute force attack	0.15

Now, we aim to examine another component of risk assessment, namely the impact/severity of threats. To evaluate this aspect, it is essential to identify which of the threats, listed in Table 3, violate the security services of confidentiality, integrity, availability, authentication, and authorization. This is clearly illustrated in Table 4. An important point is that, based on the emphasis of scientific literature, the significance of these requirements in impact/severity assessment varies depending on the application (business type), attack duration, and economic impact. For example, consider a scenario involving edge-connected devices that manage real-time analytics or smart city applications. A virus spreading at this point can lead to service disruption and operational issues, resulting in high impact and damage. In contrast, a virus that spreads at the edge but affects only a few users has a low severity.

Now, we need to establish a relationship between the identified threats and the security requirements. The results of our studies and evaluations—based on the review of ENISA documents, numerous ISI journal papers, and the expert judgment of three security specialists—are summarized in Table 4.

In this table, the symbol × indicates a violation of a security requirement, while the absence of the symbol means that the corresponding threat does not violate that requirement. In addition, an average impact/severity score is provided in the rightmost column of Table 4. These scores are derived from the expert opinions of three researchers and specialists in the fields of networking and security.

1. Phishing is a type of social engineering attack in which an attacker impersonates a legitimate source (such as a bank, mobile operator, online service, or colleague) to trick a user into revealing sensitive information, such as user names, passwords, banking details, and authentication codes. This attack is commonly carried out through emails, text messages (smishing), phone calls (vishing), and fake websites. The main objective is steal confidential information, gain unauthorized access, or prepare the ground for further attacks, such as identity theft, system intrusion, and financial fraud.

Based on the information provided in Tables 2 and 3, the final risk score assigned to each MEC threat/attack is calculated and presented in Table 5. Using these scores, the threats can be ranked and prioritized. It should be noted that the maximum value for each cell in Table 5 is 7.5; that is, $0 \leq \text{RISK} \leq 7.5$.

Table 4. Threats/Attacks and Their Impact on CIAAA Security Requirements

Threat/Attack	Confidentiality	Integrity	Accessibility	Authentication	Authorization	Impact/Vulnarability between 0 - 10
Viruses / Worms		×	×	×		8
DoS/DDos			×			8
Eavesdropping and hijacking	×	×		×	×	10
Jamming	×		×			8
MitM	×	×	×			10
Relay attack	×	×	×			8
APTs	×	×			×	10
Sybil attack	×	×	×			8
Spoofing attack	×	×	×	×		8
Physical damage		×	×		×	10
Malicious node injection (Fake/Rogue Base Station)		×	×	×		10
Service manipulation		×	×		×	8
Privilege escalation	×	×	×		×	10
VM Manipulation attack	×	×	×			8
Software vulnerability	×	×	×	×	×	10
Data exfiltration (include location privacy)	×	×	×			10
Malicious code injection	×	×	×	×		10
Phishing	×	×			×	5
Brute force attack					×	8
RoQ	×	×	×			8

According to the assessment results, the top 20% of threats, corresponding up to six threats, are identified as the most critical and are listed in descending order as follows:

- Eavesdropping/Hijacking
- DoS/DDoS
- Software vulnerability

- Phishing
- Data exfiltration
- Malicious code injection

Table 5. Threats/Attacks in the RAN Section Along with Their Risk Value

Threats/Attack	Risk value	Threats/Attack	Risk value
Viruses/Worms	2	Malicious node injection (Fake/Rogue Base Station)	2
DoS/DDos	4	Service manipulation	2
Eavesdropping/Hijacking	5	Privilege escalation	3
Jamming	2.4	VM manipulation attack	2
MitM	3	Software vulnerability	4
Relay attack	2	Data exfiltration	3.5
APTs	2.5	Malicious code injection	3.5
Sybil attack	1.2	Phishing	3.75
Spoofing attack	1.6	Brute force attack	1.2
Physical damage	2	RoQ	2.48

10) Conclusion

The 5G NR standard, as the fifth-generation wireless air interface, enables the provision of services with significantly higher bandwidth and data rates for users. Beyond improving the quality of mobile communication services, it also facilitates the emergence of new industries and supports novel applications, such as the IoT, autonomous vehicles, and intelligent communications. This standard introduces new functionalities compared to previous generations, and in 3GPP Release 16, security-related considerations and requirements for 5G have received particular attention.

In this paper, an overview of the overall architecture of the 5G network and its main components is first presented, followed by an analysis of the RAN architecture in terms of resources, threat surfaces, and vulnerabilities. Subsequently, the identified security threats and corresponding countermeasures are collected based on reputable, scientific, and research sources. In the next step, each threat is evaluated and ranked according to two main criteria: its potential impact and its likelihood of occurrence (threat success probability). This scoring is performed using standard risk assessment criteria to identify the most critical and severe threats.

The findings of this study indicate that, in the 5G RAN architecture, the five most significant threats, in order of importance, include APTs, DoS/DdoS attacks, Spoofing, Privilege Escalation, and RoQ attacks. Addressing these threats plays a key role in enhancing the safety and security of 5G networks. Finally, the results of this paper can assist researchers and practitioners in this field by encouraging greater investment in security solutions targeting high-priority threats, thereby contributing to the overall security of 5G networks.

References

Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. *IEEE Internet of Things Journal, 5*(1), 450–465. https://doi.org/10.1109/JIOT.2017.2750180

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. *IEEE Communications Standards Magazine, 2*(1), 36–43. https://doi.org/10.1109/MCOMSTD.2018.1700063

Amiriara, H., & Zahabi, M. R. (2023). A low complexity near-optimal detector based on teaching–learning algorithm for massive MIMO. *Journal of Engineering Management and Soft Computing (JEMSC), 9*(17), 35–49. https://doi.org/10.22091/jemsc.2024.8730.1167

Batalla, J. M., et al. (2020). Security risk assessment for 5G networks: National perspective. *IEEE Wireless Communications, 27*(4), 16–22. https://doi.org/10.1109/MWC.001.1900524

Borgaonkar, R., & Shaik, A. (2021). Mirage: 5G IMSI-catcher [Conference presentation]. *Black Hat USA 2021.* https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-5G-IMSI-Catchers-Mirage.pdf

Chen, C.-L., Chiang, M.-L., Hsieh, H.-C., Liu, C.-C., & Deng, Y.-Y. (2020). A lightweight mutual authentication with wearable device in location-based mobile edge computing. *Wireless Personal Communications, 113*, 575–598. https://doi.org/10.1007/s11277-020-07240-2

European Telecommunications Standards Institute. (2016). *Mobile edge computing (MEC); Framework and reference architecture (ETSI GS MEC 003 V1.1.1).* https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf

European Union Agency for Cybersecurity (ENISA) (2020). ENISA threat landscape for 5G networks. *Publications Office of the European Union*. https://doi.org/10.2824/802229

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape*. Publications Office of the European Union. https://doi.org/10.2824/782573

Farooqui, M. N. I., Arshad, J., & Khan, M. M. (2022). A layered approach to threat modeling for 5G-based systems. *Electronics, 11*(12), Article 1819. https://doi.org/10.3390/electronics11121819

Gao, Y., Ranasinghe, D. C., Al-Sarawi, S. F., Kavehei, O., & Abbott, D. (2016). Emerging physical unclonable functions with nanotechnology. *IEEE Access, 4*, 61–80. https://doi.org/10.1109/ACCESS.2015.2503432

Hamoud, O. N., Kenaza, T., & Challal, Y. (2017). Security in device-to-device communications: A survey. *IET Networks, 7*(1), 14–22. https://doi.org/10.1049/iet-net.2017.0119

Hao, P., Wang, X., & Shen, W. (2018). A collaborative PHY-aided technique for end-to-end IoT device authentication. *IEEE Access, 6*, 42279–42293. https://doi.org/10.1109/ACCESS.2018.2859781

Huang, W., Shuai, B., Zhang, R., Xu, M., Xu, Y., Yu, Y., & Antwi, E. (2020). A new system risk definition and system risk analysis approach based on improved risk field. *IEEE Transactions on Reliability, 69*(4), 1437–1452. https://doi.org/10.1109/TR.2019.2946571

Idowu-Bismark, O., Kennedy, O., Husbands, R., & Adedokun, M. (2019). 5G wireless communication network architecture and its key enabling technologies. *International Review of Aerospace Engineering (I.RE.AS.E.), 12*(2), 70–82.

Islam, N., Das, S., & Chen, Y. (2017). On-device mobile phone security exploits machine learning. *IEEE Pervasive Computing, 16*(2), 92–96. https://doi.org/10.1109/MPRV.2017.26

Javed, A. R., Beg, M. O., Asim, M., Baker, T., & Al-Bayatti, A. H. (2023). AlphaLogger: Detecting motion-based side-channel attacks using smartphone keystrokes. *Journal of Ambient Intelligence and Humanized Computing, 14*, 4869–4882. https://doi.org/10.1007/s12652-020-01770-0

Krupp, B., Sridhar, N., & Zhao, W. (2017). SPE: Security and privacy enhancement framework for mobile devices. *IEEE Transactions on Dependable and Secure Computing, 14*(4), 433–446. https://doi.org/10.1109/TDSC.2015.2465965

Kuhestani, A., Sebtonabi, M. A., Rajabi, R., & Keshavarzi, M. R. (2024). Secure medical image transmission for healthcare applications using cooperative relaying based on physical layer security. *Journal of Engineering Management and Soft Computing, 10*(18), 213–237. https://doi.org/10.22091/jemsc.2024.11195.1199

Kumar, T., Porambage, P., Ahmad, I., Liyanage, M., Harjula, E., & Ylianttila, M. (2018). Securing gadget-free digital services. *Computer, 51*(11), 66–77. https://doi.org/10.1109/MC.2018.2876017

Liyanage, M., Braeken, A., Shahabuddin, S., & Ranaweera, P. (2023). Open RAN security: Challenges and opportunities. *Journal of Network and Computer Applications, 214*, Article 103621. https://doi.org/10.1016/j.jnca.2023.103621

Mach, P., & Bečvář, Z. (2017). Mobile edge computing: A survey on architecture and computation offloading. *IEEE Communications Surveys & Tutorials, 19*(3), 1628–1656. https://doi.org/10.1109/COMST.2017.2682318

Mimran, D., et al. (2021). Evaluating the security of open radio access networks. *IEEE Communications Surveys & Tutorials, 23*(2), 1162–1187. https://doi.org/10.1109/COMST.2021.3062210

Mushtaq, M., Akram, A., Bhatti, M. K., Rais, R. N. B., Lapotre, V., & Gogniat, G. (2018). Run-time detection of Prime+Probe side-channel attack on AES encryption algorithm. In *Proceedings of the IEEE Global Information Infrastructure and Networking Symposium (GIIS)* (pp. 1–5). IEEE. https://doi.org/10.1109/GIIS.2018.8635767

Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., & Taleb, T. (2018). Survey on multi-access edge computing for Internet of Things realization. *IEEE Communications Surveys & Tutorials, 20*(4), 2961–2991. https://doi.org/10.1109/COMST.2018.2849509

Ragheb, M., Kuhestani, A., Kazemi, M., Ahmadi, H., & Hanzo, L. (2024). RIS-aided secure millimeter-wave communication under RF-chain impairments. *IEEE Transactions on Vehicular Technology, 73*(1), 952–963. https://doi.org/10.1109/TVT.2023.3307451

Ragheb, M., Kuhestani, A., & Safavi Hemami, S. M. (2022). Joint beamforming and artificial noise design in secure millimeter-wave communications with the aid of intelligent reflecting surfaces. *Journal of Iranian Association of Electrical and Electronics Engineers, 19*(3), 55–62. https://doi.org/10.52547/jiaeee.19.3.55

Ragheb, M., Safavi Hemami, S. M., Kuhestani, A., Ng, D. W. K., & Hanzo, L. (2021). On the physical layer security of untrusted millimeter wave relaying networks: A stochastic geometry approach. *IEEE Transactions on Information Forensics and Security, 17*, 53–68. https://doi.org/10.1109/TIFS.2021.3131028

Rahman, A., Hassanain, E., & Hossain, M. S. (2017). Towards a secure mobile edge computing framework for Hajj. *IEEE Access, 5*, 11768–11781. https://doi.org/10.1109/ACCESS.2017.2716782

Ranaweera, P., Jurcut, A. D., Liyanage, M., & Liyanage, M. (2021). Survey on multi-access edge computing security and privacy. *IEEE Communications Surveys & Tutorials, 23*(2), 1078–1124. https://doi.org/10.1109/COMST.2021.3062546

Rezaeizadeh, S., & Bekran, M. (2023). Minimum variance beamforming based on covariance matrix reconstruction using orthogonal vectors. *Journal of Engineering Management and Soft Computing (JEMSC), 9*(16), 90–107.

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*, 680–698. https://doi.org/10.1016/j.future.2016.11.009

Sabbagh, M., Fei, Y., Wahl, T., & Ding, A. A. (2018). SCADET: A side-channel attack detection tool for tracking Prime+Probe. In *Proceedings of the International Conference on Computer-Aided Design (ICCAD)* (pp. 1–8). Association for Computing Machinery. https://doi.org/10.1145/3240765.3240844

Wang, H.-M., Zheng, T.-X., Yuan, J., Towsley, D., & Lee, M. H. (2016). Physical layer security in heterogeneous cellular networks. *IEEE Transactions on Communications, 64*(3), 1204–1219. https://doi.org/10.1109/TCOMM.2016.2519402

Wang, S., Zhao, Y., Xu, J., Yuan, J., & Hsu, C.-H. (2019). Edge server placement in mobile edge computing. *Journal of Parallel and Distributed Computing, 127*, 160–168. https://doi.org/10.1016/j.jpdc.2018.06.008

Wang, X., et al. (2018). Deep learning-based classification and anomaly detection of side-channel signals. In *Proceedings of SPIE – Cyber Sensing* (Vol. 10630, Article 1063006). SPIE. https://doi.org/10.1117/12.2311329

Xiao, K., Li, W., Kadoch, M., & Li, C. (2018). On the secrecy capacity of 5G mmWave small cell networks. *IEEE Wireless Communications, 25*(4), 47–51. https://doi.org/10.1109/MWC.2018.1700383

Yang, S., et al. (2019). Security situation assessment for massive MIMO systems for 5G communications. *Future Generation Computer Systems, 98*, 25–34. https://doi.org/10.1016/j.future.2019.03.03

Yu, P., Cao, J., Ma, M., Li, H., Niu, B., & Li, F. (2019). Quantum-resistance authentication and data transmission scheme for NB-IoT in 3GPP 5G networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1–7). IEEE. https://doi.org/10.1109/WCNC.2019.8885686