Novasinergia
Revista digital de ciencia, ingeniería y tecnología

Unach
UNIVERSIDAD NACIONAL DE CHIMBORAZO

Review Article

5G networks: A review from the perspectives of architecture, business models, cybersecurity, and research developments

Redes 5G: una revisión desde las perspectivas de arquitectura, modelos de negocio, ciberseguridad y desarrollos de investigación

Juan Aranda[1], Erwin J. Sacoto-Cabrera[2], Daniel Haro-Mendoza[3], Fabián Astudillo-Salinas[4]

[1]*Universidad Sergio Arboleda, Bogotá, Colombia,110221*
[2] *Universidad Politécnica Salesiana, Cuenca, Ecuador, 170517; esacoto@ups.edu.ec*
[3]*Facultad de Informática, Universidad Nacional de La Plata, Buenos Aires, Argentina, 1900; eduardo.harom@info.unlp.edu.ar*
[4] *Universidad de Cuenca, Cuenca, Ecuador, 010107; fabian.astudillos@ucuenca.edu.ec*

*Corresponding: juan.aranda@usa.edu.co

Citación: Aranda, J., Sacoto-Cabrera, E., Haro-Mendoza, D., & Astudillo-Salinas, F., (2021). 5G networks: A review from the perspectives of architecture, business models, cybersecurity, and research developments. *Novasinergia.* 4(1). 6-41. https://doi.org/10.37135/ns.01.07.01

Received: 30 April 2021
Accepted: 26 May 2021
Published: 1 June 2021

Novasinergia
ISSN: 2631-2654

Abstract: 5G technology is transforming our critical networks, with long-term implications. Since 5G is transitioning to a purely software-based network, potential improvements will be software updates, like how smartphones are upgraded. For the global enterprise, the 5G arrival would be disruptive. Long-awaited solutions to various flaws in critical networking systems will arise due to 5G network adoption. Furthermore, the shortcomings of technology in contributing to business growth and success would be turned on their heads. The more complicated part of the actual 5G race is retooling how we protect the most critical network of the twenty-first century and the ecosystem of devices and applications that sprout from that network due to cyber software vulnerabilities. The new technologies enabled by new applications running on 5G networks have much potential. However, as we move toward a connected future, equal or more attention should be paid to protecting those links, computers, and applications. We address critical aspects of 5G standardization and architecture in this article. We also provide a detailed summary of 5G network business models, use cases, and cybersecurity. Furthermore, we perform a study of computer simulation methods and testbeds for the research and development of potential 5G network proposals, which are elements that are rarely addressed in current surveys and review articles.

Keywords: 5G networks, architecture, business models, network security, research developments.

Resumen: *La tecnología 5G está transformando nuestras redes críticas, con implicaciones a largo plazo. Dado que 5G está en transición a una red puramente basada en software, las mejoras potenciales serán las actualizaciones de software, como la forma en que se actualizan los teléfonos inteligentes en la actualidad. Para la empresa global, la llegada de 5G sería disruptiva. Las soluciones largamente esperadas para una variedad de fallas en los sistemas clave de networking surgirán debido a la adopción de la red 5G. Además, las deficiencias de la tecnología en términos de contribuir al crecimiento empresarial y al éxito se pondrán de cabeza. La parte más complicada de la carrera 5G real es reestructurar la forma en que protegemos la red más crítica del siglo XXI y el ecosistema de dispositivos y aplicaciones que surgen de esa red debido a las vulnerabilidades cibernéticas del software. Las nuevas tecnologías habilitadas por las nuevas aplicaciones que se ejecutan en redes 5G tienen mucho potencial. Sin embargo, a medida que avanzamos hacia un futuro conectado, se debe prestar igual o mayor atención a la protección de esos enlaces, computadoras y aplicaciones. En este artículo se abordan los aspectos clave de la estandarización y la arquitectura 5G. También se proporciona un resumen detallado de los modelos comerciales de redes 5G, casos de uso y ciberseguridad. Además, se realiza un estudio de métodos de simulación por computadora y bancos de pruebas para la investigación y el desarrollo de posibles propuestas de redes 5G, que son elementos que rara vez se abordan en estudios y artículos de revisión actuales.*

Palabras claves *Arquitectura, desarrollos de investigación, modelos de negocio, redes 5G, seguridad de red,*

1. Introduction

The popularization of mobile and smart devices and the innovation of technologies has introduced applications and services with requirements such as high performance, security, quality of service (QoS), and mobility. These requirements have driven the evolution of wireless communication technologies. 5G networks are expected to meet the needs of a wide range of applications, with different demands and in diverse and heterogeneous scenarios.

Designing a network capable of delivering these services with a single, predefined set of essential network functions would be highly complex and expensive. Faced with this situation, there is a certain consensus that 5G networks will be characterized by having a dense, heterogeneous, and shared network infrastructure between different operators, transparent use of multiple access technologies (LTE-A, millimeter wave (mmWave), WiFi, among others), the softwarization and virtualization of communication functions and protocols.

5G has a vision-oriented to services consolidated in the scientific and technical community. A proposal aimed at facilitating the 5G vision is implementing the concepts of network softwarization, network virtualization, and network slicing (NS). Implementing these concepts allows the execution of new and diverse use cases and business models. The International Telecommunication Union's (ITU) 5G vision outlines use cases with a wide range of technological efficiency and system specifications, necessitating the interconnection of mobile networks with non-3GPP network technologies. A single network provider in their domain would not be able to do this. There is a clear need for network-to-network interoperability that is also stable and reliable. Although the 3GPP has released 5G specifications that describe inter-network communications interfaces, further work is needed to improve interface functionality, performance, and security. Effective partnerships are required between various network operators and equipment owners, such as transportation companies, rural and local communities and authorities, and publicly funded organizations to achieve seamless interoperability. Network boundaries must be protected across all borders to achieve end-to-end reliability.

The complexity of the new systems is increased by the interconnection of 3GPP and non-3GPP networks, new 5G use cases with varying specifications, new 5G innovations, and evolutionary approaches throughout the mobile network. This introduces new protection vulnerabilities and a substantially wider attack surface, necessitating a detailed assessment of the threats and vulnerabilities and identifying work items to mitigate them. Furthermore, the complexities of implementing stable 5G networks while meeting the needs of multiple 5G use cases create a trade-off between network efficiency and security.

Traditional protection approaches would be ineffective due to increased network-to-network complexity, end-to-end cross-layer device security, and sensitive applications.

A review of the essential aspects of the architecture, business models, and network security of 5G is conducted. A reference work is presented to serve as an overview for researchers and stakeholders in 5G. The particular aspect of this study is that it provides the main simulation tools, key performance indicators (KPIs), and testbeds to evaluate future 5G innovations and proposals' performance.

1.1. Literature Review of Existing 5G Surveys

Several survey and review articles in the literature consider different perspectives of 5G networks. Next, a synthesis of relevant existing surveys and reviews related to 5G enabling

technologies (Yachika, Kaur, & Garg, 2021) such as mmWave, massive multiple-input multiple-output (MIMO), beamforming, non-orthogonal multiple access (NOMA), and NS is presented. Also, surveys on relevant aspects related to security and privacy and network coexistence are revised. Finally, surveys regarding the integration of 5G and some emerging technologies such as the Internet of Things (IoT), blockchain, machine learning, deep learning, and reinforcement learning are also considered. Table 1 presents a summary of the key aspects explored and the main challenges discussed in selected references.

The references were selected after conducting a systematic literature review using Scopus as the main search motor with the search query defined as follows: *TITLE-ABS-KEY(5G AND (Wireless OR (Mobile communication) OR Technology) AND ((literature Review) OR Survey)*. Google Scholar was also used as a secondary search motor using similar words for the search query. Finally, to ensure the quality of the papers, the following criteria were considered in the reviewing process: documents published in peer-reviewed journals and conference papers during the last five years and in English.

The remainder of this paper covers important aspects of 5G standardization and architecture (Section II) and a comprehensive overview of use cases and business models (Section III) and cybersecurity in 5G networks (Section IV). Furthermore, a review of computer simulation tools and testbed for research and development of future proposals for 5G networks is provided (Section V), an aspect that is lacking review in existing surveys. Finally, Section VI draws the conclusions.

Table 1: Relevant surveys and review of 5G enabling technologies and key aspects.

Reference	Key aspects explored	Key open challenges
(Khan, Naseem, Siraj, Razzak, & Imran, 2020)	Describe existing mmWave path loss models. The role of unmanned aerial vehicle (UAV) as a relay base station in 5G networks (backhaul or access communication links) using mmWave is discussed.	Performance evaluation of the link UAV-gNB using mmWave at the backhaul and access link and its integration with the existing heterogeneous networks (e.g., 3G/LTE
(Chataut & Akl, 2020)	An extensive overview of massive MIMO systems (benefits, importance, challenges)	Massive MIMO system deployment and test: pilot contamination, channel estimation, precoding, user scheduling, hardware impairments, energy efficiency, and signal detection.
(Mohamed, Alias, Roslee, & Raji, 2021)	Describe the fundamentals of beamforming technology and how it can be implemented.	Identification of interference when interferers move to eliminate interference in switched, scanning, and sectored beamforming types.
(Akbar, Jangsher, & Bhatti, 2021) (Mathur & Deepa, 2021)	Review of the basic principles of NOMA and in-depth analysis of different NOMA schemes. Recent developments in NOMA are reviewed.	Design of spreading sequences or codebooks. Analysis of heterogeneous collaborative communication schemes with NOMA. Consideration of imperfect channel state information (CSI) and sidelink control information (SCI) in theoretical analysis of NOMA. Analysis of NOMA in mmWave Communication and visible light communication (VLC).
(Khan, Kumar, Jayako & Liyanage, 2020) (Sanenga, y otros, 2020)	An in-depth review on security and privacy issues in key network softwarization technologies (NFV, SDN, MEC, NS). Examine security monitoring and management in 5G networks. Overview on 5G standardization security forces. A comprehensive review of physical layer security (PLS) based on optimization techniques.	A secure landscape is needed for 5G enabling technologies where existing and new types of attacks are considered. Breakthrough techniques are required for access control (security, access rights, and access revocations), SDN (deep security schemes), MEC (treat vectors and vulnerability identification), NFV (e.g., service insertion, multi-domain policy), NS (security mechanisms). Security standardization for 5G. Cryptography design and implementation of an optimal secure transmit precoding algorithm for PLS

Table 1: Continuation.

Reference	Key aspects explored	Key open challenges
(Agiwal, Kwon, Park, & Jin, 2021) (Mamadou, Toussaint, & Chalhoub, 2020) (Xu, Gui, Gacanin, & Adachi, 2021)	Review of 4G-5G dual connectivity in detail. Evaluate the performance of 4G-5G inter working. Analysis of coexistence techniques for spectrum sharing (resource sharing and mutualization) between 5G and access solutions in unlicensed frequency bands. A comprehensive review on resource allocation algorithms (RAAs) in heterogeneous networks (HetNets).	Conduct a performance evaluation of LTE and NR. A study of frequency usage efficiency of 4G-5G dual connectivity is needed. Proposal of mechanisms and standardization to improve resource efficiency and to allow fairness of spectrum sharing and QoS guarantees in access in coexistence scenarios. Design of intelligent-based RAAs for HetNets.
(Nguyen, Pathirana, Ding, & Seneviratne, 2020) (Santos, Endo, Sadok, & Kelner, 2020) (Fourati, Maaloul, Chaari, 2021) (Xiong, et al., 2019) (Chettri & Bera, 2020)	A comprehensive review on the integration of blockchain with 5G technologies and services. The scope of machine learning, deep learning, and reinforcement learning models applied to 5G networks for processing monitoring data and automating decisions, intrusion and anomaly detection, mobile edge caching, cell fault management, interference mitigation, and handover problem. An in-depth review on the integration of the Internet of Things in 5G networks.	Develop of optimized blockchain platforms for meeting low latency requirements and smart contracts in-network softwarization technologies. Need of standardization and regulations, and infrastructure in existing 5G networks for blockchain integration. Optimization of networks and architecture to provide massive connectivity of IoT devices is required. Develop simpler, compressed, and agile deep learning and reinforcement learning models to attend to the needs of 5G networks in real-time.

2. 5G standardization and architecture overview

The third-generation partnership project (3GPP) brings together seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, and TTC), known as organizational partners, that create reports and specifications that determine 3GPP technologies. The project includes cellular telecommunications technology, such as radio access, core network, and service capabilities, and provides a comprehensive overview of mobile telecommunications systems. Non-radio links to the core network and interworking with non-3GPP networks are also covered by these 3GPP specifications. Member companies, working groups, and the technical specification community (TSG) all contribute to 3GPP specifications and studies. These groups' 3GPP technologies are continuously developing across successive generations ("G's") of commercial cellular and mobile systems. 3GPP has been the focal point for most mobile systems beyond 3G, with LTE, LTE-Advanced, LTE-Advanced Pro, and 5G work (3GPP, 2021).

Even though these generations have become an appropriate descriptor for the type of network under consideration, real progress on 3GPP standards is determined by the milestones reached in specific releases. When a release is over, new features are functionally frozen and ready to be implemented. 3GPP operates on several releases simultaneously, beginning future development well ahead of the current release's completion. While this adds a layer of uncertainty to the groups' work, it ensures that progress is steady and consistent.

Figure 1 illustrates the timeline for the most recent and near-time-future 3GPP releases. The 3GPP TSG radio access network (TSG RAN) is responsible for defining the functions, requirements, and involving radio performance, physical layer, and definitions of the operation and maintenance requirements of conformance testing for user equipment and base stations.

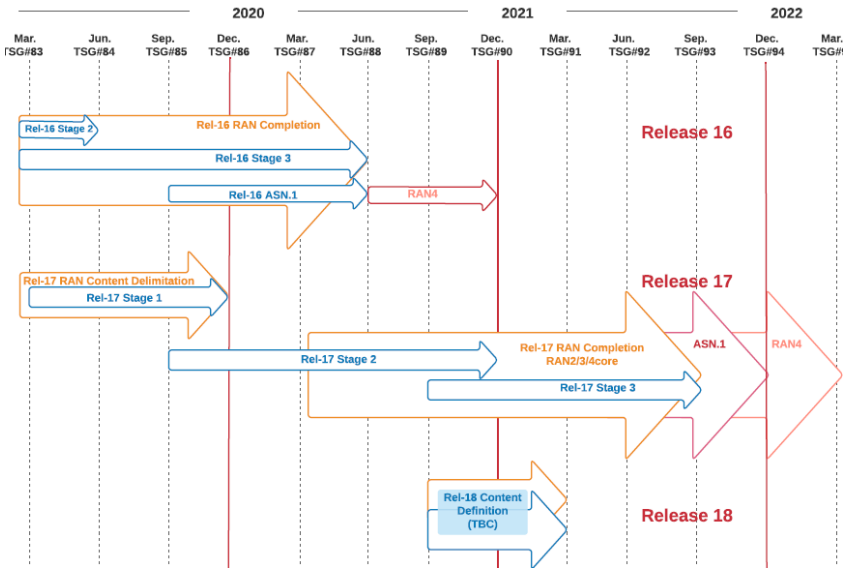

Figure 1: 5G Timeline (3GPP, 2021)

Release 15, finalized in June 2018, included the first version of the 5G/New Radio (NR) technology and a set of new features as part of the LTE evolution. Release 16 includes several significant enhancements and extensions to NR as part of the first step in the NR evolution, together with additional LTE extensions and enhancements. Release-16 finalization was targeted for June 2020, with the physical layer specifications already finalized in December of 2020. Release 17 will be the main 3GPP activity during 2020 and 2021, with target finalization in September 2021. The decisions on a set of study/work items for 3GPP Release 17 were made in December 2019 to improve network capacity, latency, coverage, power efficiency, and mobility.

2.1. 5G system architecture

Parallel to 3GPP's work on NR radio-access technology, the overall system architectures of both the radio-access network (RAN) and the core network (CN), including the functionality split between the two networks, were revisited. The RAN oversees the overall network's radio-related features, such as scheduling, radio-resource management, re-transmission protocols, coding, and various multi-antenna schemes.

The 5G core network oversees functions that are not directly related to radio access but are needed to provide a full network. This involves things like authentication, billing, and setting up end-to-end connections. Managing these functions separately, rather than incorporating them into the RAN, is advantageous since it enables many radio-access technologies to be supported by the same core network. When using NR in non-standalone mode, where LTE and EPC handle features like link setup and paging, it is possible to connect the NR radio access network to the legacy long-term evolution (LTE) core network known as the evolved packet core (EPC). In later releases, the standalone operation will be introduced. NR connects to the 5G core, and LTE connecting to the 5G core. Unlike the transition from 3G to 4G, where the 4G LTE radio-access technology cannot link to a 3G core network, the LTE and NR radio-access schemes and their corresponding core networks are closely linked (Dahlman, Parkyall, & Skold, 2020).

2.2. Core Network

The 5G core network improves on the EPC by adding three new features: service-based architecture, NS support, and a control-plane/user-plane split. The 5G core is built on a service-

based architecture. This means that the specification focuses on the core network's resources and functionalities rather than nodes. This is understandable, given that today's core network is already heavily virtualized, with core network functionality running on commodity computer hardware. The term *NS* is widely used in the sense of 5G. A network slice is a logical network that serves a specific business or customer need by combining the required functions from the service-based architecture. One network slice, for example, may be set up to serve mobile broadband applications with maximum mobility support, close to what LTE offers. Another slice can be dedicated to a non-mobile, latency-sensitive industry automation program. These slices will all run on the same underlying physical core and radio networks, but from the viewpoint of end-user applications, they will appear as separate networks. It is close in several ways to set up several virtual machines on the same physical machine. *Edge computing* can be used in a network slice like this. A network slice may also include sections of the end-user program that run close to the core network edge to provide low latency.

The 5G core network architecture emphasizes a control-plane/user-plane split, with separate bandwidth scaling for the two. Suppose more control plane capacity is needed, for example. In that case, it should be simple to add it without affecting the network's user plane. On a high level, the 5G core can be illustrated using a service-based representation as depicted in figure 2, with the emphasis on the services and functionalities. In the requirements, there is also a reference-point definition that focuses on the point-to-point interaction between the functions, but that description is not captured in figure 2.

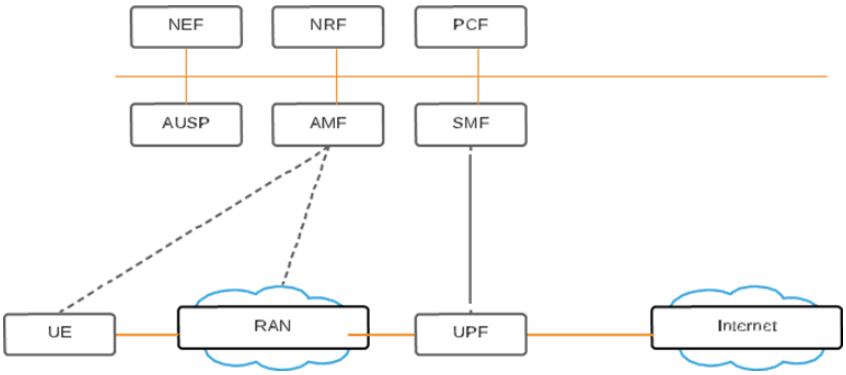

Figure 2: 5G service-based representation (Dahlman *et al.*, 2020).

The user-plane function (UPF) and the gateway between the RAN and external networks such as the Internet make up the user-plane function. Packet routing and forwarding, packet verification, QoS management, packet filtering, and traffic measurements are among its duties. When required, it also acts as an anchor point for (inter-RAT) mobility. Many components comprise the control-plane functions, such as the session management function (SMF). IP address allocation for the system (also known as user equipment, UE), policy compliance control, and general session-management functions are all handled by the SMF. The access and mobility management function (AMF) takes care of control signaling between the core network and the device, security for user data, idle-state mobility, and authentication. The functionality operating between the core network, specifically the AMF, and the device is sometimes referred to as the non-access stratum (NAS), to separate it from the access stratum (AS), which handles functionality operating between the device and the radio access network. Besides, the core network can also handle other types of functions, for example, the policy control function (PCF) responsible for policy rules, the unified data management (UDM) responsible for authentication credentials and access authorization, the network exposure function (NEF), the NR repository function (NRF), the authentication server function (AUSF) handling authentication functionality, and the application function (AF).

It is worth noting that the network's core functions can be applied in a variety of ways. Many of the features, for example, may be implemented on a single physical node, spread across several nodes, or run on a cloud platform. The above definition focuses on the new 5G core network, which is being implemented concurrently with NR radio access and can handle both NR and LTE radio accesses. It is also possible to link NR to EPC, the LTE core network, to allow for an early implementation of NR in existing networks. LTE is used for control-plane features such as initial access, paging, and versatility, which is referred to as "non-standalone service." eNB and gNB can be thought of as base stations for LTE and NR, respectively.

2.3. Radio Access Network

The radio access network can have two types of nodes connected to the 5G core network:

- A gNB, serving NR devices using the NR user-plane and control-plane protocols; or
- An ng-eNB, serving LTE devices using the LTE user-plane and control-plane protocols.

An NG-RAN is a radio access network that includes both ng-eNBs for LTE and gNBs for NR radio access. However, RAN will be used in the following for simplicity. Furthermore, since the RAN would be related to the 5G core, 5G terms such as gNB will be used. To put it another way, the definition will be based on a 5G core network and an NR-based RAN. However, as previously mentioned, the first version of NR is linked to the EPC and operates in a non-standalone mode. Although the naming of the nodes and interfaces varies slightly, the concepts are similar in this case.

The gNB (or ng-eNB) is responsible for all radio-related functions in one or several cells, for example, radio resource management, admission control, connection establishment, routing of user-plane data to the UPF, and control-plane information to the AMF, and QoS flow management.

It is necessary to remember that a logical node, not a physical implementation, is what a gNB is. A three-sector site is a standard implementation of a gNB, in which a base station handles transmissions in three cells, but other configurations exist, such as a single baseband processing unit to which multiple remote radio heads are attached. Many indoor cells or several cells along a highway belonging to the same gNB are examples. Therefore, a base station is a potential implementation of a gNB, although it is not the same. As can be seen in figure 3, the gNB is connected to the 5G core network utilizing the NG interface, more specifically to the UPF through the NG user-plane part (NG-u) and to the AMF through the NG control-plane part (NG-c). One gNB can be connected to multiple UPFs/AMFs for load sharing and redundancy. The Xn interface connecting gNBs is mainly used to support active-mode mobility and dual connectivity. This interface may also be used for multicell radio resource management (RRM) functions. The Xn interface is also used to support lossless mobility between neighboring cells through packet forwarding.

The F1 interface can also be used to break the gNB into two components, a central unit (gNB-CU) and one or more distributed units (gNB-DU). The RRC, PDCP, and SDAP protocols, which are defined in more detail below, are located in the gNB-CU, while the remaining protocol entities (RLC, MAC, and PHY) are located in the gNB-DU in the case of a split gNB. The Uu interface is the link between the gNB (or gNB-DU) and the device. At least one connection between the device and the network is necessary for a device to communicate. The system is initially connected to a single cell that handles both uplink and downlink transmissions. This cell is in control of all data flows, user data, and RRC signaling. This is a reliable and straightforward solution that can

be used in a variety of situations. Allowing the system to bind to the network via several cells, on the other hand, may be advantageous in certain situations. User-plane aggregation is one example in which data flows from several cells are combined to maximize the data rate. Another example is control-plane/user-plane separation, in which one node handles control plane communication, and another handles user plane communication. Dual connectivity refers to a situation in which a computer is connected to two cells. Dual connectivity between LTE and NR is especially important because it is the foundation for non-standalone service. The LTE-based master cell oversees control-plane and (potentially) user-plane signaling, while the NR-based secondary cell oversees only user-plane signaling, effectively boosting data speeds. Dual connectivity between NR and NR is not part of the December 2017 version of release 15 but was possible in the final July 2018 version of release 15.

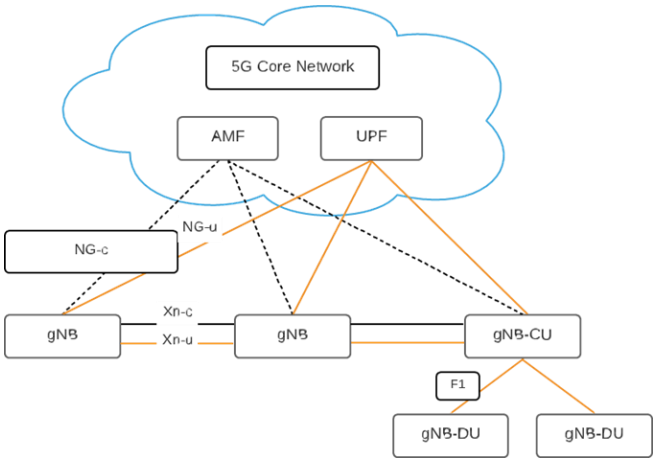

Figure 3: 5G network implementation (Dahlman *et al.*, 2020).

3. Business models & applications (use cases & KPIs; private 5G and 5G IoT)

5G leverages the option to build virtual corporate networks within the network itself, a function known as NS (Foukas, Patounas, Elmokashfi, & Marina, 2017; Afolabi, Taleb, Samdanis, Kasentini, & Flinck, 2018). Each of these slices is created with guaranteed service quality parameters and customized according to the specific needs of each company or organization (Kaloxylos, 2018). Their customization, i.e., their creation as private networks, ensures a good quality of service, increasing their reliability (Su *et al.*, 2019). Any facility will have its own 5G node, which will provide a specific network segment adapted to its particularities and QoS (Laghrissi & Taleb, 2018).

We can attribute this adaptive network model to two technologies: network virtualization and edge computing. The former is the result of the combination of two technologies: NFV enables applications to be deployed on one or more virtual machines, while SDN centralizes the management of these distributed applications, as described in Section II and the authors in (Ge, Zhou, & Li, 2019; Abdelwahab, Hamdaoui, Guizani, & Znati, 2016).

With the development of edge computing, or cloud computing, companies can process data and apply decision algorithms close to the IoT devices that generate the information. This fact seems insignificant, helps alleviate the load on cloud traffic, reduces latency, and speeds data analysis in real-time (Hassan, Yau, & Wu, 2019; Hu, Patel, Sabella , Sprecher, & Young, 2015). This new approach to transmitting information opens up new possibilities across the board, especially compared to the long distances that data has to travel today with the need to send it to processing environments.

Several papers (Afolabi *et al*., 2018; Kazmi, Khan, Tran, & Hong, 2019) discuss in detail NS, which enables the sharing of a common physical infrastructure for different network services (Foukas *et al*., 2017). Physical infrastructure includes wireless access networks, cloud computing servers, Wi-Fi access points, to name a few. The following is carried out an analysis of the most relevant elements of the NS taxonomy based on the literature reviewed, considering the key elements of NS architecture, design, technologies, and requirements with a focus on the development of various possible business models that can be developed in 5G networks.

- NS architecture: Several papers (Afolabi *et al*., 2018; Foukas *et al*., 2017; Kaloxylos, 2018; Barakabitze, Ahmad, Mijumbi, & Hines, 2020) describe the NS architecture, which is composed of infrastructure, network function and service layers (Next Generation Mobile Network (NGMN) Alliance, 2016). Depending on the layer, NS isolation can be done in many ways: software-based isolation, physical isolation, and virtual machine-based isolation (Kostopoulos, Chochliouros, & Spada, 2019). For this purpose, the Next Generation Mobile Networks (NGMN) Alliance (2015), establishes for each network layer the following instances: 5G service instance layer (5GSIL), 5G network instances layer (5GNSI), 5G physical resource layer (5GRL). The 5GSIL represents different services to be supported by the operator (e.g., services to mobile virtual network operators (MVNOs) or end-users), where each service is created by an instance (Hicham, Abghour, & Ouzzif, 2018). The 5GNSI is a set of logical networks that fulfill a service layer instance's required functions and characteristics. A 5GNSI instance can also be shared between multiple service instances provided by the network operator (Hicham *et al*., 2018). 5GRL represents the bottom layer of the architecture and consists of physical and logical resources dedicated to a network function(s) determined by the upper layer(s).
- NS basic design principles: The NS architecture is based on three principles: isolation, elasticity, and E2E optimization (Afolabi *et al*., 2018; Foukas et al., 2017; Kaloxylos, 2018).

  – Isolation: is a NS feature that can separate and impose limits on network resource uses; this feature is supported by network virtualization (Michalopoulos *et al*., 2017). It also ensures the performance of different users (MVNOs, vertical industries) through an equitable distribution of resources. Isolation can be deployed (i) by using a different physical resource, (ii) when separating via virtualization means a shared resource, and (iii) through sharing a resource with the guidance of a respective policy that defines the access rights for each tenant.

  – Elasticity: is an essential operation related to the resource allocated to a particular network slice. Specifically, elasticity allows the dynamic management of resources allocated to network segments according to different users' demands to use them efficiently. Fixed availability of resources on a network segment can lead to under-, and over-utilization of resources due to user demands variations (Li *et al*., 2017; Kazmi *et al*., 2019; Abdulghaffar, Mahmoud, Abu-Amara, & Sheltami, 2021). Therefore, NS is designed with an elastic nature to simultaneously satisfy the users QoS and optimize the overall network overhead. The main challenge in the elasticity application is the negotiation policy between network segments so that the performance of the network segments is not affected by an increase in the number of users or an increase in QoS. However, this process requires an inter-slice negotiation since it may influence the performance of other slices that share the same resources.

  – Customization E2E: NS's inherent property for facilitating a service delivery from the service providers to the end-user(s)/customer(s). Network segments ensure that the network operator's shared resources are efficiently utilized between different users. Network

segments customization in NS is performed at all layers of the network topology using the technical features provided by SDN and supported by the advantages of NFV. As described by Li *et al.*, (2017); Lin, Tseng, & Wang (2021), E2E a property has two extensions: (i) a slice that combines resources that belong to distinct infrastructure providers, (ii) it unifies various network layers and heterogeneous technologies,

- Technologies enabling NS: the key virtualization technologies for NS are listed below:

  – SDN: It provides key characters such as flexibility, service-oriented robustness adaptation and scalability. SDN creates a virtualized control plane that enables intelligent management between network functions, eliminating the gap between service provisioning and network management, i.e., with SDN network control becomes directly programmable using standardized interfaces (Afolabi *et al.*, 2018; Ho, Tran, Kazmi, Han, & Hong, 2018; Prabakaran, Nizar, & Kumar, 2021). The SDN controller manages network slices applying rules when necessary and following the corresponding network policy. Furthermore, SDN permits flexibility into control and data planes in 5G networks.

  – VNF: It allows the deployment of originally based in hardware network functions (NF) on virtual environments leveraging benefits of cloud computing (Afolabi *et al*., 2018; Ho *et al.*, 2018; Prabakaran *et al*., 2021; Nguyen, Brunstrom, Grinnemo, & Taheri, 2017). With NFV, NFs can be easily deployed and dynamically allocated, as well as NFs can be assigned to service providers (SPs) so that mobile network operators (MNOs) can share their infrastructure (Nguyen *et al*., 2017; Stallings, 2015; Costa-Perez *et al.*, 2017).

  – Edge computing: technologies as cloud and edge computing offer computational, storage, and networking facilities within single or multiple platforms for enabling a network slice (Hassan *et al*., 2019; Selvi & Thamiselvan, 2021). Specifically, edge computing enables data acquisition and provides services close to end-users allowing a form of edge-centric networking, which facilitates data proximity, assuring ultra-low latency, high data rates, and intelligence and control. In this regard, multi-access edge computing (MEC) (Rayani, Glitho, & Elbiaze, 2020; Giust , Costa-Perez, & Reznik, 2017; Giust *et al.*, 2018) system facilitates information technology (IT) cloud capability at the edge of the network, and its access-agnostic characteristics guarantee smoother deployment independent of the underlying communication network. Besides, mobile edge fog computing (MEFC) is a MEC technology that provides cloud-computing capabilities with proximity to mobile subscribers, it offers a service environment with ultra-low latency and high bandwidth as well as direct access to real-time radio network information that can be used by applications and services to offer context-related services.

  – NS based on resources: the segmentation of an operator's physical network infrastructure can be done at the different network levels, from user terminal equipment to core network equipment, allowing the network segment (MNO, MVNO, Vertical Industries) manager to orchestrate and provide services autonomously. In this respect, resources at the user terminal level require operators to establish different strategies at the level of each network segment concerning QoS. Regarding MNO RAN sharing with MVNOs, different infrastructure sharing possibilities are studied by Kazmi, Tran, Ho, & Hong (2017), Ho *et al*., (2018); Zhang, Gui , Tian, & Sun, (2017) while modeling the scenarios as an optimization problem to satisfy efficient resource allocation needs. In addition to network sharing at the user endpoint and RAN level, core network and cloud resources must be efficiently shared between different network segments and their users while meeting QoS requirements.

From the above, about segmentation at the different network levels, two scenarios stand out in the

documents reviewed: static and dynamic resource allocation for the different network levels (Kazmi *et al.*, 2017; Ho *et al.*, 2018; Zhang *et al.*, 2017). Static allocation of a network segment to an MVNO means that once the resource allocation strategy across the network segment is determined, the network segment will have the same capacity regardless of how the environment changes (Khan, Yaqoob, Tran, Han, & Hong, 2020). Dynamic allocation of a network segment refers to adjusting network resource allocation strategies to optimize the quality of services (Khan *et al.*, 2020).

In this regard, the ITU has proposed three usage scenarios that can serve as corresponding standard network slices, with each targeting different service requirements. These scenarios are also referred to as slice service types. Within the context of 5G NS, a slice service type defines the expected behavior of a network slice in terms of specific features and services. The three standardized slice service types are:

- The enhanced mobile broadband (eMBB)
- The ultra-reliable and low latency communications (URLLC)
- The massive machine-type communications (mMTC)

As a conclusion of the above, in 5G development are considered that slice allocation means allocating resources throughout the network. 5G resources are model as multiple chunks, each one with a different capacity, spread across the whole physical network.

Since unforeseen business models and use cases are expected to emerge in the short future, as detailed above, 5G networks have the flexibility to support these new requirements.

3.1. Business Models

In the previous generations of mobile networks (2G, 3G), the resources to be assigned to each application were mainly radio resources, as described by Sacoto-Cabrera (2021), Camarán & De Miguel (2008); Varoutas, Katsianis, Sphicopoulos, Stordahl, & Welling (2006). However, 4G networks development enabled new business models for MVNOs and vertical industries, as described by Sacoto-Cabrera (2021), Copeland & Crespi (2011), Pousttchi & Hufenbach (2009), Smura, Kiiski, & Hammainen (2007), and Kim & Park (2004).

Among the business models, it is highlighted:

- Full MVNO: in this model, the resource shared with the MNO is the radio spectrum for which access charges are set according to the leased spectrum space. On the other hand, a Full-MVNO can manage different QoS levels according to profiles and services that can be operated within the MVNO platform.
- Multi-MNO: this business model allows an MVNO to connect to multiple MNOs (Multi-MNOs), considering access to different services for which MNOs provide different levels of QoS.

In this respect, several studies introduce different scenarios of network infrastructure sharing between MNOs and MVNOs in which their technical and economic feasibility is assessed, as described by Hultell, Johansson, & Markendahl (2004), Romero & Guijarro (2013), and Guijarro, Pla, & Tuffin (2013).

Likewise, the development of different business models points to further segmentation of wireless access networks into specialized service providers that connect to local service and access providers, possibly through an infrastructure provider (InP) that provides services to the different MVNOs through service level agreements (SLAs).

Concerning the above, the 5G mobile network opens unprecedented business opportunities to telco operators by increasing their market through the NS characteristics.

NS drives the business models behind the 5G ecosystem by providing an effective way to deliver heterogeneous services of interest for different verticals customers as MVNOS, virtual private network operators (PVMNOs) and, over-the-top operators (OTTs) (Jiang, Condoluci, Mahmoodi, & Guijarro (n.d.); Gomes, Ahokangas, & Mogaddamerad, 2016; Golzarjannat, Ahokangas, Matinmikko-Blue, & Yrjola, 2021).

Table 2 describes the main business models proposed by several authors (Li *et al.*, 2017), whose classification is based on the one described by the next generation mobile networks (NGMN) alliance published in the 5G white paper (Next Generation Mobile Networks (NGMN) Alliance, 2015).

Table 2: Business models.

Mobile operator role	Business models	Description
Asset provider	Network sharing	5G networks can share network infrastructure between two or more operators based on static or dynamic policies.
	XaaS	5G networks can offer to and operate for a 3rd party provider with different network capabilities as infrastructure, platform, and network as a service (XaaS)
Connectivity provider	An extensive overview of massive MIMO systems (benefits, importance, challenges)	In this business model, the customer and service provider are decoupled from the physical infrastructure. They are offered no configurability, and a very low level of configurability, respectively. The connectivity provider business model requires modular network architecture, having the capability to be exposed to the 5G provisioning/configuration system.
Partner service provider	Describe the fundamentals of beamforming technology and how it can be implemented.	Identification of interference when interferers move to eliminate interference in switched, scanning, and sectored beamforming types

The main 5G networks business models described in table 2 require redefining the value chain of an MNO by considering the main actors and their interactions. Pujol, Elayoubi, Markendahl, & Salahaldin (2016), and Curwen & Whalley (2021) identify the new elements that are integrated into the components of an MNO value chain (customers, competitors, suppliers, complementary services). PVMNOs is part of the customer value chain component as a connectivity provider that leases MNO infrastructure to serve its customers; additionally, all those who provide vertical services or who lease network capacity to MVNOs are also part of MNOs customers (Next Generation Mobile Networks (NGMN) Alliance, 2015). In the competitor value chain component, large wireless network providers as Google and Microsoft join in as network competitor. In the supplier value chain component, companies that manufacture equipment and software for data centers, virtualization, among others, join in as suppliers to the MNOs, while content delivery networks (CDN) are an important element in the provision of an MNO's service to host content near the end-users in the MNO's network. And the in complementary services value chain component are added content providers that encourage their users to buy more mobile data service capacity, including mobile application developers.

In addition to the business models described in table 2, several documents present different classifications for business models in 5G, as follows:

3.1.1. Commercialization business models:

- Business-to-business (B2B): 5G network resources are leased to different vertical companies offering complementary services such as IoT, video surveillance, etc. In this model, full

consumer control in this service delivery chain is released to the companies (Elayoubi *et al*., 2017; Barakabitze *et al*., 2020).

- Business-to-consumer (B2C): the B2C goal is to create value by detecting new demand for services enriched by digital platforms, addressing new consumer and business needs (Elayoubi *et al*., 2017; Barakabitze *et al*., 2020).
- Business to business to customer (B2B2C): new markets and consumer-oriented customers can partner with 5G network providers; thus, MNOs play the role of a wholesale provider, i.e., they must provide customized network resources to a third party (MVNO, OTT, vertical market players). They will have a direct relationship with their end-customer (Elayoubi *et al*., 2017; Barakabitze *et al*., 2020).

3.1.2. Lifecycle:

Zhu, Yu, Berry, & Liu (2019) discussed business models based on lifecycle, service target market and, different levels at which MNO network segmentation is performed, the classification being as follows:

- Industrial NS: in this model, the actors have the same requirements for their users to register on the same network segment, which abstracts user demands to a high latency network segment and a low latency network segment.
- Monopolized NS: in this model, an actor (such as MVNO, OTT, PMVNO) pay for a network segment and uses it to serve its users or uses it as a private network.
- NS by events: In this model, the MNO implements network segments with a relatively short lifetime to cover temporary events (concerts, sports activities, promotions, among others).

3.1.3. Dynamic and static sharing:

These business models encompass the study of static and dynamic network infrastructure sharing and the relationship between MNOs and MVNOs, mainly to establish the economic feasibility of these models for the different market players.

3.1.4. Multi-MNO:

In these models' business, an MVNO is considered a customer of its host MNO and competes with MNOs and other MVNOs to attract customers.

Few works model the economic relationships, which emerge from a multi-MNO business model. An analysis of pricing in a mobile market, driven by two MNOs and a new MVNO that leases resources and competes with the MNOs is discussed by Sacoto-Cabrera (2021), Sacoto-Cabrera, Guijarro, & Maillé (2020), Khalifa, Benhamiche, Simonian, & Bouillon (2018), and Zhu *et al.,* (2019).

3.1.5. Multi-Tenancy:

NS facilitates share MNO infrastructures, accelerating network rollouts and offering services to customers with reduced costs (Li *et al.,* 2017; Liu, Yang, & Cuthbert, 2021; Kaloxylos, 2018; Guijarro, Vidal, Pla, & Naldi, 2019). Samdanis, Costa-Perez, & Sciancalepore (2016) define the following roles for network sharing solutions:

- Infrastructure provider (InP): the MNO is responsible for the physical network deployment and maintenance, but InP does have contact directly with end-users.
- MVNO: MVNOs are tenants of existing InP resources.

- OTT service providers: in this model, the OTTs operate on top of an InP belonging to an MNO and based on a pre-defined SLA set of requirements.
- Vertical industries: in this model, vertical industries exploit an MNO or MVNO network infrastructure as a tenant or services complementary telecommunication industry.

In this regard, the authors in Han, Tavade, & Schotten (2017), Sacoto-Cabrera, Guijarro, Vidal, & Pla, (2020), Han, Feng, Ji, & Schotten (2017), and Guijarro, Vidal, Pla, & Naldi (2019) analyze the multi-tenant model from the economics relationships that emerge in NS-based resource allocation within the context of 5G. Specifically, the above works analyze the global profit maximization problem of a set of independent mobile VNOs that request slices from an MNO and propose several allocation mechanisms for solving this system optimization problem.

3.2. Uses Cases

As described above, the 5G architecture is designed to provide support for three different generic services eMBB, mMTC, and URLLC. Likewise, 5G services can be provided through different slices, where a specific slice can handle user requests of a particular type, and each offers distinct QoS to their users.

Besides, NS enables value creation for vertical segments, application providers and third parties that lack physical network infrastructure, by offering radio, networking, and cloud resources, allowing a customized network operation and true service differentiation.

The main objective of 5G is to enable an end-to-end ecosystem, which meets price-QoS requirements. To this end, several use cases are envisaged in the development of 5G (Next Generation Mobile Networks (NGMN) Alliance, 2015; Afolabi *et al.,* 2018; Navarro-Ortiz *et al*., 2020), as detailed in table 3.

Table 3: Uses case categories.

Uses	Description	Examples
Broadband access in dense areas	The objective is to make services available in densely populated areas (e.g., dense urban centers, events, multi-store buildings), where thousands of people per square kilometer (km^2) congregate.	Pervasive video HD video/photo sharing in stadium/open-air gathering
Broadband access everywhere	This use of 5G allows access to a minimum amount of bandwidth, at least 50Mbps, to ensure a globally connected society.	50+ Mbps everywhere Ultra-low-cost networks
Higher user mobility	Offers broadband service for mobile users in extremely fast-moving vehicles.	High-speed train Remote computing Moving hot spots 3D (three dimensional) Connectivity
Massive IoT	Supports the access of sensors and actuators to ultra-dense broadband networks, considering devices that need super-low cost, long-range and low power consumption.	Smart wearables (clothes) Sensor networks Mobile video surveillance
Extreme real-time communications	This 5G network use ensures ultra-low latency connectivity.	Tactile Internet
Ultra-reliable communications	This 5G network use provide ultra-low latency, reliability, and availability of network connectivity support.	Automated traffic control and driving eHealth: Extreme life critical. Remote object manipulation: remote surgery Public safety,
Multi- connection	This use 5G network assures network connectivity for users with different smart devices.	smart-phones, smart-TV, among others

Figure 4 shows the mapping from the usage scenarios defined by ITU-R and the use case families proposed by NGMN.

As can be seen, URLLC consists of extreme real-time communications, lifeline communications, and ultra-reliable communications. The mMTC corresponds to the massive IoT. The eMBB usage scenario consists of broadband access in dense areas, broadband access everywhere, increased user mobility, and broadcast-like services.

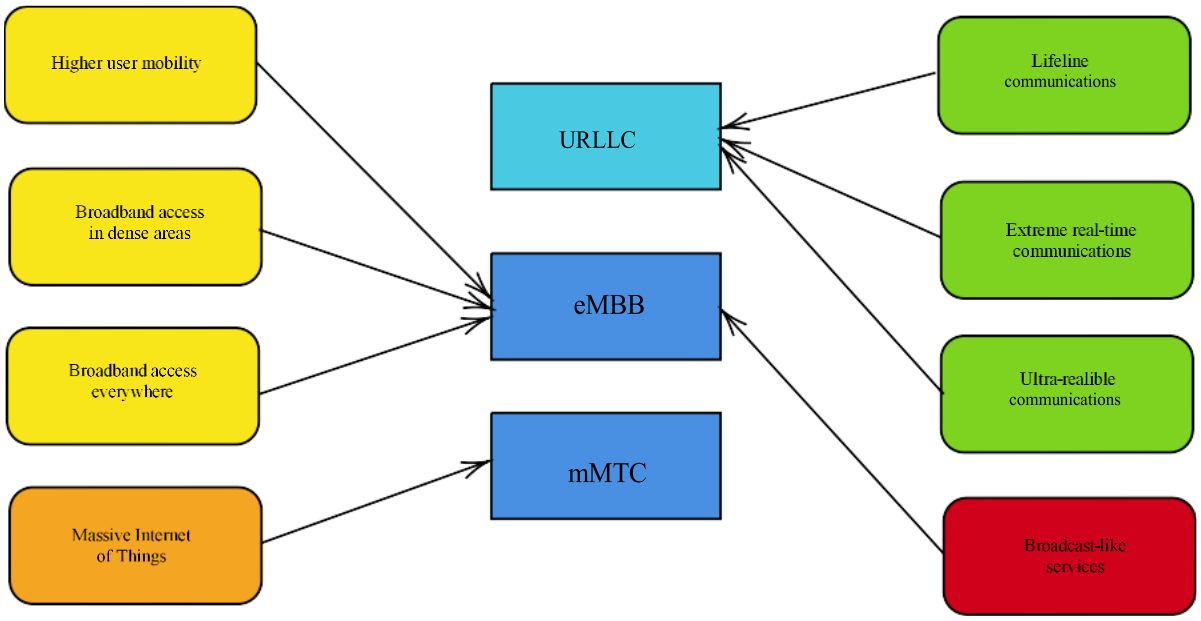

Figure 4: 5G use cases.

3.3. *Key performance indicators (KPIs)*

The KPIs are certain quantitative parameters to evaluate network quality. Specifically, in 5G, the NGMN defined in (Next Generation Mobile Networks (NGMN) Alliance, 2015) system performance KPIs and user experience KPIs, as shown in tables 4 and 5, respectively.

Table 4: System performance KPIs.

Uses	Connection density	Traffic density
Broadband access in dense areas	200-2500 /km	DL: 750 Gbps / km² UL: 125 Gbps / km²
Indoor ultra-high broadband access	75,000 / km (75/1000 m office)	DL: 15 Tbps / km² (15 Gbps /1000 km²) DL: 15 Tbps / km² (15 Gbps /1000 km²)
Broadband access in a crowd	150,000 / km (30.000 / stadium)	DL: 3.75 Tbps / km² (DL: 0.75 Tbps / stadium) UL: 7.5 Tbps / km² UL: 7.5 Tbps / km²
Mobile broadband in vehicles	2000 / km² (500 active users per train x 4 trains, or 1 active user per car x 2000 cars)	DL: 100 Gbps / km² (25 Gbps per train, 50 Mbps per car) UL: 50 Gbps / km (12.5 Gbps per train, 25 Mbps per car)
Massive low-cost/long-range/low-power MTC	Up to 200,000 / km	Not critical
Broadband MTC	200-2500 /km	DL: 750 Gbps / km² UL: 125 Gbps / km²
Ultra-low latency	Not critical	Not critical
Ultra-high reliability & Ultra-low latency	Not critical	Not critical

Table 5: User experience KPIs.

Uses	Uses Experienced Data Rate	E3E Latency	Mobility
Broadband access in dense areas	DL: 300 Mbps UL: 50 Mbps	10 ms	On demand, 0-100 km/h
Indoor ultra-high broadband access	DL: 1 Gbps, UL: 500 Mbps	10 ms	Pedestrian
Broadband access in a crowd	DL: 25 Mbps UL: 50 Mbps	10 ms	Pedestrian
Mobile broadband in vehicles	DL: 50 Mbps UL: 25 Mbps	10 ms	On demand, up to 500 km/h
Massive low-cost/long-range/low-power MTC	Low (typically 1-100 kbps)	Seconds to hours	On demand: 0-500 km/h
Broadband MTC	DL: 25 Mbps UL: 50 Mbps	10 ms	0-120 km/h
Ultra-low latency	DL: 50 Mbps UL: 25 Mbps	<1 ms	Pedestrian
Ultra-high reliability & Ultra-low latency	DL: From 50 kbps to 10 Mbps UL: From a few bps to 10 Mbps	1 ms	On demand: 0- 500 km/h

In Next Generation Mobile Networks (NGMN) Alliance (2015), each KPI is defined, and the evaluation method is introduced. Also, the target value of each KPI is set for different use cases.

Several studies developed by, 5G European validation platform for extensive (5G EVE) (Gupta *et al*., 2019), coordinated multi-point (CoMP) (Song, Wang, Chen, & Jiang, 2018), 5G option 3x reference model (Soós, Ficzere, Varga, & Szalay, 2020), 5G testbed (Soós *et al.,* 2020), 5GENESIS (Koumaras *et al.,* 2018), analyze the performance of 5G and the KPIs established in its design. The 5G KPIs studies include different use cases of broadband access in dense areas, high user mobility, massive IoT, tactile Internet, natural disaster, E-Health services, and broadcast services. They have set out recommendations for improvements in the design and deployment of 5G networks. These have set out recommendations for improvements in the design and deployment of 5G networks, especially in the radio coverage and connection speed, but there are no E2E 5G field trials.

4. Cybersecurity in 5G

The new services and applications offered by the connectivity of emerging 5G networks will introduce new security requirements to mitigate vulnerabilities and attacks. These new requirements must be addressed in the deployment of 5G networks (Housenovic *et al.*, 2018). The transition to 5G networks according to the 3GPP is divided into two parts: a) Standalone networks, where a 5G core (5GC) network is introduced, and b) non-standalone networks, which will take advantage of the same protocols of the plane of LTE control and the LTE evolved packet core (EPC) network (5G Americas, 2020).

4.1. Threats, vulnerabilities, and attacks

4.1.1. 5G Non-standalone:

The operation of the 5G NSA architecture is based on LTE control plane protocols (see figure 5), so the initial 5G NSA launches will only offer Mobile Broadband (eMBB) improvements (Agiwal, Roy, & Saxena, 2016). Threats and vulnerabilities presented in LTE will also affect the 5G NSA network. For a proper transition to 5G, the threats that occur in 4G must be considered.

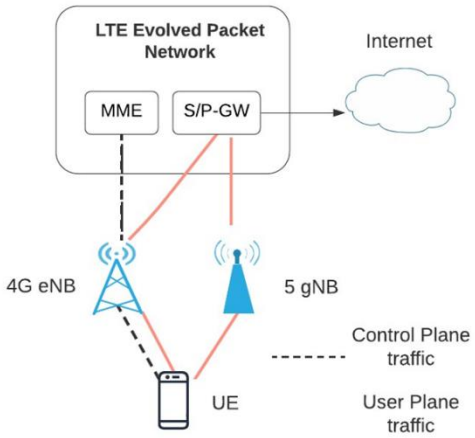

Figure 5: Non-standalone architecture.

The main security threats to the 5G NSA network are described below:

- Downgrade attack, forcing a UE LTE connection to connect to 2G or 3G, even though the end-user can do so with higher technology.
- Data modification attacks, UMTS, and LTE communications integrity are not protected by any security method to intercept the information flow. This could lead to data injection or modification, such as man in the middle (MitM) (5G Americas, 2018). Mutual authentication between the mobile device and the base station can prevent a MitM-type attack. The 5G AKA and EAP-AKA protocols are emerging solution to record connection requests and then initiate the authentication process in 5G networks (Basin *et al.*, 2018).
- IMSI Tracking, when IMSI (International Mobile Subscriber Identity) requests are made. The international mobile sub- scriber identity (IMSI) is sent unencrypted over the radio, thus allowing the attacker to find out which SIM card is using the connected user.
- Base station spoofing "fake" base stations capable of unknowingly tracking and collecting their personal data.
- LTE roaming, the use of old signaling protocols with SS7 / diameter vulnerabilities in 2G, 3G / 4G could expose users to listening to voice conversations, reading or transmitting messages, and tracking phones (ITProPortal, 2019).

4.1.2. 5G standalone:

Figure 6 shows the 5G SA architecture. 5G SA will cover all ITU use cases for 5G, implementing independent services and specifications through a new 5GC network and new protocols to mitigate some known LTE problems (Housenovic *et al.*, 2018).

One of the critical aspects to differentiate 5G SA from 5G NSA and previous versions is improving privacy through a service-based architecture with techniques such as SDN and NFV (Americas, 2020). Centralized SDN management and virtualization of NFV functions expose the functional domains and weaknesses of the 5G network (Americas, 2018). Among the principal vulnerabilities and threats that can affect 5G SA infrastructures, the following can be mentioned: *Service-based architecture:* Information transfer in 5G is software-based. This information is sensitive and confidential; this is added to weak authentication, lack of encryption, and insecurity in end devices, increasing the risk of attack on applications.

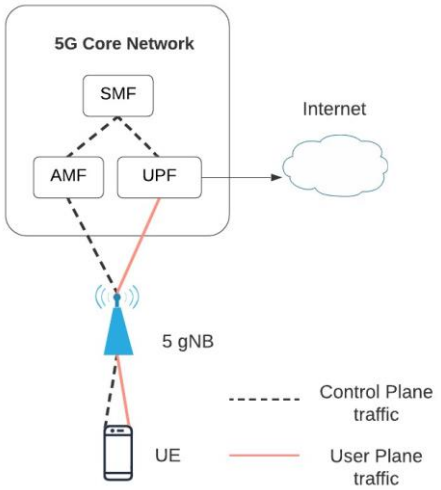

Figure 6: Standalone architecture.

4.1.2.1. SDN and NFV:

To support the high levels of performance and flexibility for massive information generation and management applications, 5G must implement new paradigms such as SDN and NFV (González, 2019). However, as with any new technology, security risks grow as new threats emerge. Virtualization allows multiple tenants or network users to share the same physical infrastructure and network resources. This can create security vulnerabilities related to confidentiality, integrity, authenticity, and non-repudiation (Housenovic *et al.*, 2018). SDN logically uses the concept of a centralized controller. This concept introduces a single point of failure in the controller's infrastructure; it also represents a bottleneck for the entire network in the case of saturation attacks. Another threat is control applications. Control applications can interact maliciously, trying to gain control over switches and controllers. The use of Internet security protocol (IPsec) or transport layer security (TLS) is recommended to protect this communication in an encrypted way (Forescout Technologies, 2017). Another aspect to consider is that communication between each plane of the SDN architecture is carried out using specific SDN protocols or through virtual interfaces. These interfaces constitute new points of attack for which each interface must implement an authentication and authorization method that ensures the integrity and confidentiality of the communication (5G Americas, 2019).

4.1.2.2. Threats to the EU:

In Forescout Technologies (2017), a study of IoT security is presented. It concludes that each new device at the infrastructure represents a security threat or point of attack. Each of the devices will be exposed and/or vulnerable. The main threats to which they are exposed are distributed denial of services (DDoS) attacks and integrity attacks of data stored on devices. DDoS attacks will be carried out through massive requests to the server to deny access to network resources. It is a priority to think of solutions with solid authentication from the design phase to mitigate them. Given the nature of 5G, to achieve fast authentication, SDN themselves are the best tools with high flexibility and programmability (Agiwal *et al.*, 2016). Additionally, 3GPP recommends using IPSec encryption to prevent attacks from the Internet or botnets that could significantly affect 5G applications.

4.1.2.3. Man-in-the-middle (MitM):

Like 4G, 5G lacks information integrity protection methods in its specifications. Shaik,

Borgaonkar, Park, & Seifert (2019) reported that information on an unprotected device's capabilities is exchanged during its registration on the 4G and 5G network. A MitM can exploit this vulnerability. The three classes of attacks that can occur are: (i) identification attacks, discovering devices on the network, knowing their characteristics and applications; (ii) bidding down attacks, capturing the device's capabilities, and degrading the data speed; and (iii) battery depletion attacks. User plane integrity protection can be enabled but requires considerable resource consumption, affecting the user device's performance. IP is enabled on control plane messages, but that still leaves user data traffic vulnerable because the control plane and the user plane are separate (Americas, 2020).

4.1.2.4. RAN threats (SUPI):

Unlike 4G and its predecessor technologies, in 5G, the IMSI is not transmitted in plain text. 3GPP has addressed this by eliminating the clear text IMSI by proposing a permanent subscription identifier (SUPI), which prevents an attacker from tracking a target affecting subscribers' privacy. 5G systems guarantee the integrity of the information as it implements MIMO technology with multiple inputs and output antennas, operating in the mmWave millimeter wave spectrum with data and signals.

4.2. 5G design and security considerations

The security features of the 5G architecture have improvements compared to previous generations.

These features are based on proven 4G security mechanisms. The enhancements are primarily based on enhancements to authentication, encryption, and assurance of availability, integrity, and privacy. Figure 7 presents a 5G environment with its principal vulnerabilities and the design considerations deployed to mitigate them.

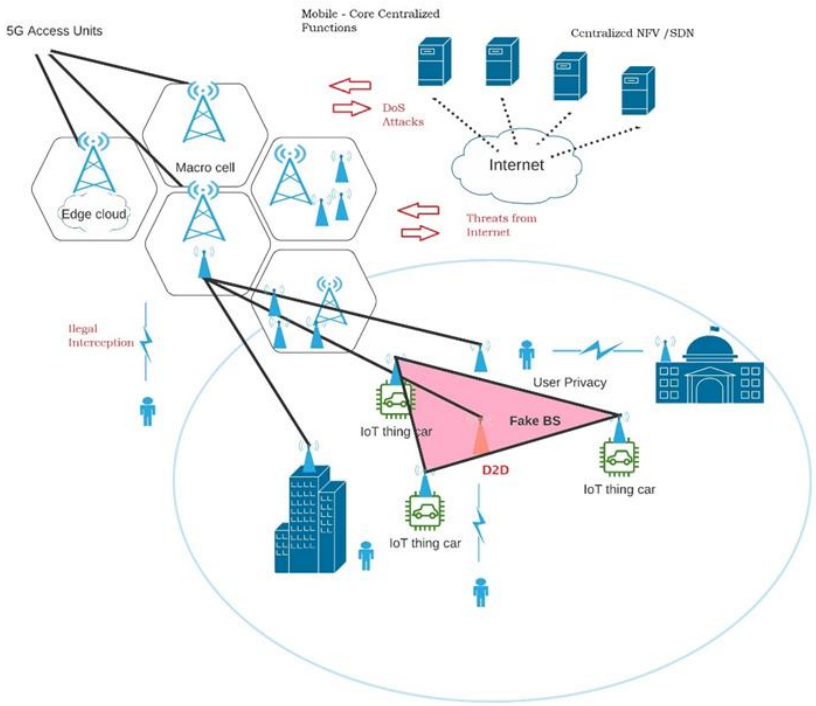

Figure 7: Vulnerabilities and security considerations of the 5G design.

4.2.1. Mobile edge computing (MEC):

MEC technology enables applications with high real-time demands such as driverless vehicles, augmented reality (AR), robotics, and immersion media. MEC provides cloud computing capabilities within RAN close to mobile users (Pham *et al.*, 2020). Table 6 lists the primary security protections provided by MEC, as well as their main threats.

Table 6: Protections and risks of MEC.

Protections	Risks
Each container performs a dedicated function, and this makes it easy to detect anomalies.	Open-source code, more interfaces, and APIs introduce new threat vectors
Isolation between containers prevents the spread of viruses.	Shared resources can generate cross-interference.
Network segmentation separates traffic and isolates resources.	Vulnerabilities in host container-as-a-service (CaaS) and plat- form as a service (PaaS) can affect container security.
Resiliency is gained with increased speed and dynamic threat response.	Dependency upon central orchestration introduces a new threat vector
Efficient software update and security patches	High data volume and sessions increase risk from an attack.
	Vulnerability of applications that run as microservices.

4.2.2. Software-based operations:

5G is based on cloud functions and software. 5G service providers will implement in their infrastructure: Automation, orchestration, and machine learning (5G Americas, 2020). Process automation with data collection, machine learning for analysis, and decision making. Gates of trust are needed to implement an automated system in a 5G network properly. An audit must be executed continuously to ensure that the expected results are achieved; threat intelligence can be used to detect and mitigate malicious attacks in real-time. The orchestration will help coordinate the use of different 5G resources by providing security enhancements for roaming with the introduction of the security edge protection proxy (SEPP) in the 5G core.

4.2.3. NFV security:

A fully virtualized 5G network using the ETSI NFV architecture allows operators to deploy scalable, elastic, and highly reliable networks, improving network and user security. NFV can improve the self-protection of 5G communications and isolate malicious traffic, thus better solving DoS and DDoS attacks (ITPortal, 2019). However, due to the configuration errors presented by the dynamic nature of NFVs, they are vulnerable to typical attacks of virtualization, such as flooding, hypervisor hijacking, malware injection, cloud attacks, spoofing, and sniffing (Ordonez-Lucena *et al.*, 2017). In Americas (2018), it is mentioned that in NFV, there is the facility to create, delete and move a virtual machine (VM). Thus, tracking a VM and ensuring the security of a hypervisor becomes a complex problem. In this context, the main security challenge is to protect hypervisors' confidentiality and privacy, virtual machines, and management modules through an authentication and validation mechanism. NFV provides security service as a service (SECaaS). Security as a service can be applied to any application and is a strong use case for 5G technology. For Hussain, Hussain, & Zeadally (2019), NFV not only provides an optimal exchange of resources but also allows agreements, service-oriented policies, monitoring mechanisms, and flow control. Finally, by combining the features of NFV with SDN, flexibility in 5G security management can be improved, allowing security functions to be executed in real-time without altering the underlying hardware configuration.

4.2.4. SDN security:

SDN creates a single point of risk that compromises the availability of the entire system. To mitigate these availability problems and improve resilience to malicious attacks, a reasonable solution is the use of controller redundancy (Ordonez-Lucena *et al.*, 2017). Likewise, the centralized architecture of SDN allows the automation of the management of a security incident. Identification, status verification, and the application of security policies can be scheduled to run automatically (Hussain *et al.,* 2019). Automation would reduce configuration errors and problems in the application of policies in the network. Automation enables the deployment of security policies globally across the entire network, while security services can be deployed on specific traffic types. SDN embedded programmability allows most network functions to be implemented as applications. If malicious applications gain access or critical application programming interfaces (APIs) are exposed to malicious software, chaos can spread across the network (Ahmad *et al*., 2017). To address the API security issue, data must be protected end-to-end. This includes the security of a request from origin to destination, passing through intermediate elements. API security can include a) data security on the shipment (between control plane, user plane, and services), and b) access control and security against DoS. Key sharing can be exploited by network elements using an encryption algorithm, validated, and authenticated by a central node. Only the elements authenticated by the central node will be able to exchange information (5G Americas, 2020).

4.2.5. Network slicing (NS):

5G network slices are logically isolated, and autonomous networks are flexible and programmable enough to accommodate multiple use cases simultaneously over the same network infrastructure. As mentioned by Ordonez-Lucena, *et al.* (2017), each slice is autonomous and independent, thanks to this isolation. Any attack or security problem that occurs in one slice does not affect the rest of the slices. Each slice will have its resource and security requirements. A slice should implement security policies according to the requirements without influencing the rest of the slices. According to those mentioned above, the main problem that NS presents is the possibility of inadequate isolation. The isolation problem can occur between different slices (inter-slices) and between the same slice components (intra-slice). This drawback results in a threat of being able to migrate across multiple slices. The impact of an attack can be reduced by implementing adequate intra-slice isolation, for example, HAND isolation, security domain, VNF isolation, among others. The desired isolation levels must accommodate technologies that include various software, hardware, and cryptography mechanisms (Americas, 2019). In addition to isolation, the authors in (Americas, 2020) talks about providing an additional security level to each slice. A customer can define the implementation of security policies according to their requirements and use case. A customer can incorporate SECaaS. The security services required for the applications are obtained from an operator library. As presented in figure 8, SECaaS allows each network slice to be configured according to the client's requirement, the application, and the use case (eMBB, mMTC, URLLC) to provide the resources (latency, bandwidth, QoS) and security required.

For the NGMN Alliance in its work: "5G security recommendations Package # 2: Network Slicing" there are several challenges and solutions to the problem of security in NS 5G networks which are presented in table 7.

4.2.6. Zero trust:

In Americas (2020), it is stated that the 5G architecture must implement the zero-trust

model (zero trust). Zero trust is essential to mitigate security risks. Zero trust is based on the concept of "denial by default" and assignment of least privileges. According to John Kindervag, one of the problems with security models is that they are based on the concept of "trust and verify." In return, he proposes the concept of "verify and never trust" (Baker & Waldron, 2020). This concept allows 5G operators to restrict unnecessary access to specific network parts to devices and users. In this sense, a network operator could carry out some of its functions in its systems and other functions in external infrastructures. The external cloud provider will be outside the network operator's trust model (5G Americas, 2020).

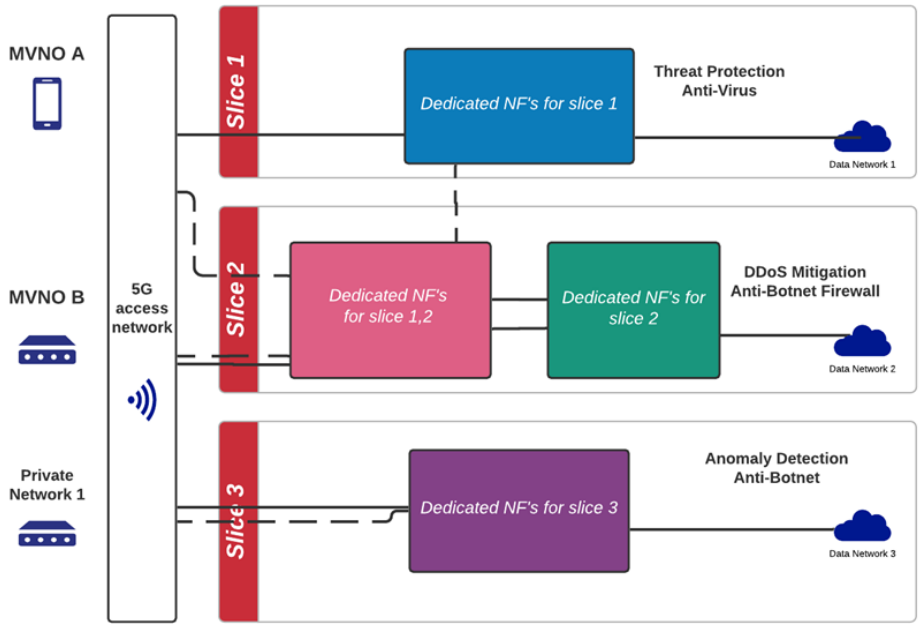

Figure 8: Security as a Service (SECaaS).

Table 7: Challenges and solutions of security in NS 5G networks.

No	Issue	Challenge	Recommendation
1	Controlling inter-network slices communications	Signaling and control traffic between network segments. I/O communications at user plane level	All communications between slices and functions should have a mechanism to control their transmission and reception
2	Spoofing to network slice manager	Spoofing attacks against the network slice manager or physical host plat- forms	Authenticate the network slice manager before loading an NS instance.
3	Spoofing against a network slice instance	Virtual functions contained within a NS instance must be authenticated and their integrity verified.	NS managers should authenticate each other within a carrier network before any negotiation.
4	Different security protocols or policies	If different slices offer different ser- vices, you may have different performance and security requirements.	Implement a referential security level in all slices, adequate isolation, and individual authentication for a UE accessing several slices at the same time.
5	Exhaustion of security resources	Each slice must guarantee the network resource for the security protocols.	Guarantee the resources of a slice to execute security protocols and policies without exhausting resources in other slices.
6	Side-channel attacks	Prevent an attacker from being able to extract information, observe or influence how code executes in functions in other slices	Strengthen isolation between VMs and avoid co-hosting on the same hardware slices with different levels of vulnerability.

5. 5G research opportunities and developments

The standardization for 5G communication has been completed, and the 5G networks are already becoming a commercial reality (Tataria *et al*., 2021). Therefore, the research community is starting to talk about beyond 5G communications referred to as the sixth generation (6G) of wireless networks. 6G networks are expected to provide critical features on the communication services for future demands such as high security, secrecy, and privacy (Dang, Amin, Shihada, & Alouini, 2020). Also, 6G networks are expected to achieve the requirements of a fully connected world and provide ubiquitous wireless connectivity for everyone (Akyildiz, Kak, & Nie, 2020). Hence, KPIs should be proposed to guide the design of 6G networks related to those existing for 5G networks (Tataria *et al*., 2021). Table 8 shows a comparison of 5G and 6G networks KPIs and main features.

Table 8: Comparison of 5G and 6G networks KPIs and features (Dang *et al*., 2020; Tataria *et al*., 2021).)

KPIs/Features	5G	6G
Operating bandwidth	Up to 400 MHz (sub-6 Ghz bands), Up to 3.25 GHz (mmWave bands)	Up to 400 MHz (sub-6 Ghz bands), Up to 3.25 GHz (mmWave bands)
Maximum frequency	90 GHz	10 THz
Maximum data rate	35.46 Gbps	1 Tbps
User and control planes latency	1 ms (uRLLC), 20 ms	25 μs (tactile applications), 20 ms
Mobility	500 km/h	1000 km/h
Architecture	Massive MIMO	Intelligent surface
Core networks	Internet, Internet of Things	Internet of Everything
Multiplexing	OFDMA	Smart OFDMA
Service level	3D VR/AR	Tactile

From the continuous evolution of 5G, new lessons will be learned. These lessons will serve as a backdrop for emerging use cases that will be better served by 6G such as remote healthcare, smart environments, autonomous vehicles, space connectivity, multi-sensory holographic teleportation, industrial automation. Hence, to fulfill the 5G beyond vision, according to Akyildiz *et al.* (2020), several enabling technologies have been conceived and actively studied. Among these technologies, the authors mentioned the following:

- A network operating at the THz band (with abundant spectrum resources),
- Intelligent communication environments,
- Pervasive artificial intelligence,
- Large-scale network automation,
- All-spectrum reconfigurable front-end (for dynamic spectrum access),
- Ambient backscatter communications (for energy savings),
- Internet of space things (CubeSats and UAVs),
- Cell-free massive MIMO communication networks,
- Internet of NanoThings and BioNanoThings,
- Quantum communications,
- Holistic security.

Concerning standardization initiatives for technologies and a network beyond 5G, the ITU has recently established the ITU focus group on technologies for network 2030 to study the capabilities of future networks (2030 and beyond) and to provide guidance for developing the 6G network (concepts, architecture, protocols, enabling technologies) (Akyildiz *et al.*, 2020).

Although the research community and standardization entities are starting to discuss beyond 5G, open challenges and research opportunities remain to be developed. In the subsequent sections, some additional research opportunities are presented and the open challenges proposed in the literature (see Table 1). Also, an overview of simulator tools and testbed for conducting research development on 5G networks is provided.

5.1. 5G research opportunities

Table 1 lists key open challenges proposed in the literature for research and development in 5G technologies. Based on our current research, we also consider the following research opportunities regarding NS and random-access control in 5G networks:

- NS enables new business opportunities across a wide range of use cases and sectors by making it possible to create fit- for-purpose virtual networks with varying degrees of independence, as described in Section III. However, the diversity of new business and technical requirements has important implications for the way networks are built and managed, so there is considerable scope for studying different business models, especially in the PMVNOs. PMVNOS offers functionality beyond current offerings, which often rely on existing public network services, which need to be studied in terms of technical and economic feasibility.
- Access control (URLLC and mMTC) - One central 5G concept is fast, efficient, and scalable random access, which can handle many intermittent traffic-generating devices (such as IoT devices) that are often inactive but periodically access the network for minor updates with no human interaction. Sporadic traffic will skyrocket in the 5G market, and the bulky 4G random access procedures will not handle it. Another 5G core principle is cell declassification, combined with cloud-powered baseband processing and wireless network visualization to improve spectrum and energy efficiency and manage expected traffic growth (Tello-Oquendo, Lin, Akyildiz, & Pla, 2019; Tello-Oquendo, Akyildiz, Lin , & Pla , 2018).

More research is required to manage URLLC and mMTC in 5G efficiently; it is critical to determine the appropriate random access (RA) and/or access control mechanisms and how user equipment performs self-uplink synchronization with gNB to overcome preamble collisions caused by multiple UEs transmitting the same preamble. Besides access control mechanisms based on barring schemes (Pacheco-Paramo & Tello-Oquendo , 2020; Pacheco-Paramo, Tello-Oquendo, Pla, & Martinez-Bauset, 2019; Vidal, Tello-Oquendo, Pla, & Guijarro, 2019; Tello-Oquendo, Vidal, Pla, & Guijarro, 2018; Tello-Oquendo, Vidal Catalá, Pla, & Martínez Bauset, 2018; Tello-Oquendo, Leyva-Mayorga, Pla, Martínez-Bauset, & Casares-Giner, 2015), cooperative RA and other improvements to the RA procedure are two other ways to support mMTC in 5G. However, these may not be adequate to meet URLLC MTC's latency requirements. Complementing the existing grant-based random access (GBRA) method with grant-free random access (GFRA) protocol would be helpful to support both mMTC and URLLC. Instead of contending with access requests for receiving a grant to transmit the data packets, UEs in GFRA contend with their data packets in a random-access fashion; non-3GPP IoT solutions like LoRaWAN and Sigfox use GFRA protocols extensively.

5.2. 5G research developments

Research and development of new and novel techniques and technologies for further improving the spectral efficiency, connectivity, and reliability of wireless communication networks, require in-depth analysis and evaluation. Today, fixed and mobile communications specifications have become increasingly complex due to their demand for higher broadband data

rates and challenging latency and reliability requirements, especially in emerging real-time applications, like autonomous vehicles. Thus, analytical techniques, as well as research-based on link-level measurements, will soon encounter feasibility limitations (Muller *et al.*, 2018). Therefore, computer-aided numeric simulation is a technique of utmost importance to conduct research and develop new algorithms and future technologies in wireless communications (Müller *et al.*, 2018; Bouras, Gkamas, Diles, & Andreas, 2020). Table 9 summarizes the most relevant simulator tools to evaluate the performance of end-to-end 5G networks, new functionalities, and techniques at the MAC and physical layers.

Navarro-Ortiz *et al.* (2020) provided detailed performance evaluation guidelines and use cases for 5G networks, including their corresponding scenarios and traffic models. The authors recommended for research and proposals in 5G communications, to employ, as the general use cases for 5G performance evaluation, the five International Mobile Telecommunications-2020 (IMT-2020) test environments (ITU, 2017): indoor hotspot- eMBB, dense urban-eMBB, rural-eMBB, urban macro-mMTC, and urban macro-URLLC, using traffic patterns from the mobile and wireless communications enablers for the twenty-twenty information society (METIS) project (METIS, 2020).

An important task to conduct in a performance evaluation study is radio planning. For 5G networks, Xirio Online is proposed in Aptica (2021). Xirio is a web simulator tool that provides the quickest and cheapest way to perform 5G network planning using real maps based on the geographic information system under urban and rural scenarios.

In addition to computer-based simulators, used to find the expected results of a hardware configuration without the need for actual implementation (Bouras *et al.*, 2020), there are more and more 5G testbeds from different laboratories that allow conducting tests closer to implementation. Most of the testbeds are deployed in Europe (Informationsplattform for 5G, 2021). Table 10 summarizes relevant testbeds available for research and development in 5G networks. The table includes those references that provided complete and online information about the testbed.

Table 9: Most significant 5G simulator tools.

Simulator	Module	Project	Language	Key features
NetSim	5G NR (Tetcos, 2021)	Proprietary (fee)	C	Standard/Pro versions. 5G NR simulation tool based on Release 15/3GPP 38 series. End-to-end simulation of 5G networks. Support 5G Core (TS 23.501, TS23.502) functions and interfaces, 5G NSA deployment, SDAP spec. 37.324), RLC (spec. 38.322), PDCP (spec. 38.323), MAC layer (spec. 38.321), physical layer (sub-carrier spacing, numerologies, frame structure & phy resources, carrier aggregation, MIMO).
Ns-3	5G-LENA (CTTC, 2021)	Open source	C++	NS-3 module to simulate 3GPP 5G networks aligned with NR Release 15 TS 38.300. Support RLC (TS 38.322), PDCP (spec. 38.323), MAC (TS 38.321, uplink delay support), physical layer (numerology, mini-slot, and mixed UL-DL slot format, propagation and channel models, beamforming methods, NR PHY abstraction).

Table 9: Continuation.

Simulator	Module	Project	Language	Key features
Matlab	5G Toolbox (MathWorks, 2021)	Proprietary (fee)	C/C++, Matlab	Simulator tool according to 3GPP 5G NR specifications (Release 15 & 16). Simulation of end-to-end 5G NR communications links. Support 5G NR physical layer (NR subcarrier and numerology, propagation channel models, Downlink and uplink channels and signals, control information, and transport channels).
Open5GCore	Open5GCore (Open5GCore, 2021)	Proprietary (fee)	–	5G toolkit based on 3GPP Release 15 & 16 core network functionality (AMF, SMF, AUSF, UDM, NRF, UPF). Support standard 5G NR and UEs [N1, N2, N3], data path diversity (PFCP [N4]), advanced session management, network slice, non-3GPP access.
Vienna 5G Simulators	5G System Level (Muller *et al.*, 2018) & 5G Link Level (Institute of Telecommunications, nd)	Academic use license	Matlab	Matlab based simulators. Support multi-link, waveforms (CP-OFDM, f-OFDM, FBMC, UFMC, WOLA), channel codes (LDPC, turbo, polar, convolutional), flexible numerology, propagation, and channel models.
Open5GS	Open5GS (Open5GS, 2021)	Open source	C	Open-source tool that implements the core network of NR/LTE network based on Release-16.

Table 10: Relevant testbed for 5G research development.

Testbed	Location	Frequencies [GHz]	Use case
University of Bristol (5GINFIRE, 2021)	England	3.5, 26	Smarty City Safety
University of Surrey (University of Surrey, 2021)	England	2.6, 3.5, 26	Satellite
5G-VINNI (Ghassemian, Muschamp, & Warren, 2020; 5G-PPP, 2021)	England	3.6, 2.6	Industry (Remote robotic control, VR-based immersive app), Cloud-based gaming, Media, e-Health (Connected care), Public Protection and Disaster Relief
5G Lab (5G Industrielles Internet, 2021)	Germany	3.75, 26, 60	Industry 4.0 Applications, Human-Machine collaboration, Autonomous driving, Robot-assisted telesurgery
5G-EVE (5G Industrielles Internet, 2021)	Greece, Italy, France	3.5, 3.6, 3.8	Industry 4.0 Applications, Smart Cities, Smart Campus, Smart Transport
COSMOS (COSMOS GROUP, 2021)	USA	sub-6, 28	Smart city

Conclusions

This study reviewed some fundamentals of the 5G cellular network as architecture, business models, cybersecurity, and research developments. Concerning business models, this article has described the different models that can be developed in 5G networks, especially those based on network slicing; however, these may only be possible in 5G stand-alone versions, as well as others that may appear during the deployment of the 5G network. In the same sense, the use cases described are based on the stand-alone version of the 5G network (except those related to spectrum sharing in non-standalone versions) and whose key performance indicators are devised to determine the end-to-end performance of the network. Computer-aided numeric simulation is mainly used to conduct research and develop novel proposals for further improving spectral efficiency, connectivity, and reliability in 5G networks. However, in the last few years, many 5G testbeds have started to be offered from various laboratories to perform tests closer to implementation within different verticals such as industry 4.0 applications, smart cities, satellites. Building a safe 5G network necessitates a comprehensive approach rather than a narrow emphasis on individual technical components. User authentication, traffic encryption, mobility, overload conditions, and network stability, for example, must all be considered together. Understanding relevant risks and how to best manage them is also essential. Enterprises embarking on a digital transformation journey are most concerned about information security. As a result, IoT must be protected from the beginning, safeguarding personal information, business-sensitive data, and vital infrastructure. Industries must gather expertise, comprehend emerging risks, and mitigate them to endure.

Authors' contributions

Following the internationally established taxonomy for assigning credits to authors of scientific articles (https://casrai.org/credit/). The authors declare their contributions in the following matrix:

	Aranda, J.	Sacoto-Cabrera, E.	Haro-Mendoza. D.	Astudillo Salinas, F.
Conceptualization	■			
Formal Analysis	■	■		■
Investigation	■	■	■	■
Methodology	■	■	■	
Resources	■	■	■	■
Validation	■	■	■	
Writing – review & editing	■	■	■	■

References

3GPP. (2021). 5G Release 16. Retrieved from https://www.3gpp.org/release-16

3GPP. (2021). About 3GPP. Retrieved from https://www.3gpp.org/about-3gpp

5G Americas. (2018, October). The evolution on security in 5G. Retrieved from https://www.5gamericas.org/the-evolution-of-security-in-5g-2/

5G Americas. (2019, July). The evolution of security in 5G, a slice of mobile threats. Retrieved from https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper_8.15.pdf

5G Americas. (2020). Security considerations for the 5G era. Retrieved from https://www.5gamericas.org/security-considerations-for-the-5g-era/

5G Industrielles Internet. (2021). 5G Lab. Retrieved from http://www.ip45g.de/en/testbeds/5g-lab-2/

5G Industrielles Internet. (2021). 5G-EVE. Retrieved from http://www.ip45g.de/en/testbeds/5g-eve/

5GINFIRE. (2021). 5GINFIRE. University of Bristol 5G Testbed. Retrieved from https://5ginfire.eu/university-of-bristol-5g-testbed/

5G-PPP. (2021). 5G Verticals Innovation Infrastructure. Retrieved from https://www.5g-vinni.eu/

Abdelwahab, S., Hamdaoui, B., Guizani , M., & Znati, T. (2016). Network function virtualization in 5G. *IEEE Communications Magazine*, *54*(4), 84–91. http://doi.org/10.1109/MCOM.2016.7452271

Abdulghaffar, A., Mahmoud, A., Abu-Amara, M., & Sheltami, T. (2021). Modeling and evaluation of software defined networking based 5G core network architecture. *IEEE Access*, 9, 10179-10198. http://doi.org/10.1109/ACCESS.2021.3049945

Afolabi, I., Taleb, T., Samdanis, K., Kasentini, A., & Flinck, H. (2018). Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. *IEEE Communications Surveys Tutorials*, *20*(3), 2429-2453. http://doi.org/10.1109/COMST.2018.2815638

Agiwal, M., Kwon, H., Park, S., & Jin, H. (2021). A Survey on 4G-5G Dual Connectivity: Road to 5G Implementation. *IEEE Access*, 9, 16193-16210. http://doi.org/10.1109/ACCESS.2021.3052462

Agiwal, M., Roy, A., & Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *18*(3), 1617-1655. https://doi.org/10.1109/COMST.2016.2532458

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions. *IEEE conference on standards for communications and networking (CSCN)*, (pp. 193–199). https://doi.org/10.1109/CSCN.2017.8088621

Akbar, A., Jangsher, S., & Bhatti, F. (2021). NOMA and 5G emerging technologies: A survey on issues and solution techniques. *Computer Networks*, 107950. https://doi.org/10.1016/j.comnet.2021.107950

Akyildiz, I., Kak, A., & Nie, S. (2020). 6G and Beyond: The Future of Wireless Communications Systems. *IEEE Access*, 8, 133995-134030. https://doi.org/10.1109/ACCESS.2020.3010896

Aptica. (2021, 05 15). Retrieved from Xirio Online: https://www.xirio-online.com/web/

Baker, J., & Waldron, K. (2020). 5G and zero trust networks. R Street Institute. Retrieved from https://www.jstor.org/stable/resrep27016

Barakabitze, A., Ahmad, A., Mijumbi, R., & Hines , A. (2020). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167. https://doi.org/10.1016/j.comnet.2019.106984

Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., & Stettler, V. (2018). A formal analysis of

5G authentication. *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, (pp. 1383-1396). https://doi.org/10.1145/3243734.3243846

Bouras, C., Gkamas, A., Diles, G., & Andreas , Z. (2020). A Comparative Study of 4G and 5G Network Simulators. *International Journal on Advances in Networks and Services*, *13*(1 & 2). Retrieved from http://www.iariajournals.org/networks_and_services/netser_v13_n12_2020_paged.pdf#page=19

Camarán, C., & De Miguel, D. (2008). Mobile virtual network operator (MVNO) basics. Retrieved from http://www.valoris.com/docs/Valoris_Viewpoint_-_MVNO_basics_-_What_is_behind_this_mobile_business_trend.pdf

Chataut, R., & Akl, R. (2020). Massive MIMO Systems for 5G and beyond Networks—Overview, Recent Trends, Challenges, and Future Research Direction. *Sensors, 20*(10). doi:https://doi.org/10.3390/s20102753

Chettri, L., & Bera, R. (2020). A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet of Things Journal, 7*(1), 16-32. https://doi.org/10.1109/JIOT.2019.2948888

Copeland , R., & Crespi, N. (2011). Modelling multi-MNO business for MVNOs in their evolution to LTE VoLTE & advanced policy. *15th international conference on intelligence in next generation networks*, (pp. 295-300). https://doi.org/10.1109/ICIN.2011.6081092

COSMOS GROUP. (2021). Cosmos Project. Retrieved from https://cosmos-lab.org/

Costa-Perez, X., Garcia-Saavedra, A., Li, X., Deiss, T., De la Oliva, A., Di Giglio, A., & Moored, A. (2017). 5G-crosshaul: An SDN/NFV integrated fronthaul/backhaul transport network architecture. *IEEE wireless communications, 24*(1), 38-45. https://doi.org/10.1109/MWC.2017.1600181WC

CTTC. (2021). 5G-LENA. Retrieved from https://5g-lena.cttc.es/

Curwen, P., & Whalley, J. (2021). 5G: A multigenerational approach. In *Understanding 5G mobile networks*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-80071-036-820210001

Dahlman, E., Parkyall, S., & Skold, J. (2020). 5G NR: The next generation wireless access technology. Elsevier Science.

Dang, S., Amin, O., Shihada, B., & Alouini, M.-S. (2020). What should 6G be? *Nature Electronics, 3*(1), 20-29. https://doi.org/10.1038/s41928-019-0355-6

Elayoubi, S., Bedo, J.-S., Filippou, M., Gavras, A., Giustiniano, D., & Iovanna, P. (2017). 5G innovations for new business opportunities. Mobile world congress. Retrieved from https://hal.inria.fr/hal-01488208/

Forescout Technologies. (2017). IoT and OT security research exposes hidden business challenges. Retrieved from https://www.forescout.com/iot_forrester_study/

Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. (2017). Network slicing in 5G: Survey and challenges. *IEEE Communications Magazine, 55*(5), 94-100. https://doi.org/10.1109/MCOM.2017.1600951

Fourati, H., Maaloul, R., & Chaari, L. (2021). A survey of 5G network systems: challenges and machine learning approaches. *International Journal of Machine Learning and Cybernetics, 12*(2), 385-431. https://doi.org/10.1007/s13042-020-01178-4

Ge, X., Zhou, R., & Li, Q. (2019). 5G NFV-based tactile internet for mission-critical IoT services. *IEEE Internet of Things, 7*(7), 6150-6163. https://doi.org/10.1109/JIOT.2019.2958063

Ghassemian, M., Muschamp , P., & Warren, D. (2020). Experience Building a 5G Testbed Platform. *IEEE 3rd 5G world forum (5GWF)*, (pp. 473–478). https://doi.org/10.1109/5GWF49715.2020.9221109

Giust , F., Costa-Perez, X., & Reznik, A. (2017). Multi-access edge computing: An overview of ETSI MEC ISG. 1, 4. Retrieved from https://futurenetworks.ieee.org/tech-focus/december-2017/multi-access-edge-computing-overview-of-etsi

Giust , F., Sciancalepore , V., Sabella, D., Filippou, M., Mangiante , S., Featherstone, W., & Munaretto D. (2018). Multi-access edge computing: The driver behind the wheel of 5G-connected cars. *IEEE Communications Standards Magazine*, *2*(3), 66-73. https://doi.org/10.1109/MCOMSTD.2018.1800013

Golzarjannat, A., Ahokangas, P., Matinmikko-Blue, M., & Yrjola, S. (2021). A business model approach to port ecosystem. *Journal of Business Models, 9*(1), 13-19. https://doi.org/10.5278/jbm.v9i1.4261

Gomes J. F., Ahokangas, P., & Mogaddamerad, S. (2016). Business modeling options for distributed network functions virtualization: Operator perspective. European wireless 2016; *22th european wireless conference,* (pp. 1-6). Retrieved from https://ieeexplore.ieee.org/abstract/document/7499279/

González , C. (2019). Desafíos de seguridad en redes 5G. 3, 36-45. Retrieved from https://cpic-sistemas.or.cr/revista/index.php/technology-inside/article/view/47/47

Guijarro , L., Pla, V., & Tuffin , B. (2013). Entry game under opportunistic access in cognitive radio networks: A priority queue model. *IFIP wireless days (WD)*, (pp. 1-6). https://doi.org/10.1109/WD.2013.6686476

Guijarro, L., Vidal, J., Pla, V., & Naldi, M. (2019). Economic analysis of a multi-sided platform for sensor-based services in the internet of things. *Sensors, 19*(2), 373. https://doi.org/10.3390/s19020373

Gupta, M., Legouable, R., Rosello, M., Cecchi, M., Alonso, J., Lorenzo, M., & Carrozzo, G. (2019). The 5G EVE end-to-end 5G facility for extensive trials. *IEEE international conference on communications workshops (ICC workshops),* (pp. 1-5). https://doi.org/10.1109/ICCW.2019.8757139

Han, B., Feng, D., Ji, L., & Schotten, H. (2017). A profit-maximizing strategy of network resource management for 5G tenant slices. *arXiv preprint arXiv:1709.09229*. Retrieved from https://arxiv.org/abs/1709.09229

Han, B., Tavade, S., & Schotten , H. (2017). Modeling profit of sliced 5G networks for advanced network resource management and slice implementation. *IEEE symposium on computers and communications (ISCC)*, (pp. 576-581). https://doi.org/10.1109/ISCC.2017.8024590

Hassan, N., Yau, K.-L., & Wu, C. (2019). Edge computing in 5G: A review. *IEEE Access*, 7, 127276–127289. https://doi.org/10.1109/ACCESS.2019.2938534

Hicham, M., Abghour, N., & Ouzzif, M. (2018). 5G mobile networks based on SDN concepts. *International Journal of Engineering and Technology (UAE), 7*(4), 2231-2235. http://dx.doi.org/10.14419/ijet.v7i2.18.12194

Ho, T., Tran, N., Kazmi, S., Han, Z., & Hong C. S. (2018). Wireless network virtualization with non-orthogonal multiple access. *NOMS 2018-2018 IEEE/IFIP network operations and management symposium,* (pp. 1-9). https://doi.org/10.1109/NOMS.2018.8406264

Housenovic, K., Bedi, I., Maddens, S., Bozsoki, I., Daryabwite, D., & Sundberg, N. (2018). Setting the scene for 5G: Opportunities & challenges. International Telecommunications Union. Retrieved from https://www.itu.int/myitu/-/media/Publications/2018-Publications/BDT-2018/En---Setting-the-scene-for-5G--opportunities-and-challenges.pdf

Hu, Y., Patel, M., Sabella , D., Sprecher, N., & Young, V. (2015). Mobile edge computing—a key technology towards 5G. *ETSI white paper, 11*(11), 1-16. Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

Hultell, J., Johansson, K., & Markendahl, J. (2004). Business models and resource management for shared wireless networks. *IEEE 60th vehicular technology conference*, 5, 3393-3397. https://doi.org/10.1109/VETECF.2004.1404693

Hussain, R., Hussain, F., & Zeadally, S. (2019). Integration of vanet and 5G security: A review of design and implementation issues. *Future Generation Computer Systems, 101*, 843–864. https://doi.org/10.1016/j.future.2019.07.006

Informationsplattform for 5G. (2021). 5G Testbends. Retrieved from https://www.ip45g.de/en/5g-testbeds/

Institute of Telecommunications. (n.d.). Vienna 5G Simulators. Retrieved from https://www.nt.tuwien.ac.at/research/mobile-communications/vccs

ITProPortal. (2019, December). Old vulnerabilities could majorly impact 5G security. Retrieved from https://www.itproportal.com/news/old-vulnerabilities-could-majorly-impact-5g-security/

ITU. (2017). Guidelines for evaluation of radio interface technologies for IMT-2020. ITU-Recommendation M.2412. Retrieved from https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2412-2017-PDF-E.pdf

Jiang, M., Condoluci, M., Mahmoodi, T., & Guijarro, L. (n.d.). Economics of 5G network slicing: optimal and revenue-based allocation of radio and core resources in 5G. Retrieved from https://nms.kcl.ac.uk/toktam.mahmoodi/files/TWC-16.pdf

Kaloxylos, A. (2018). A survey and an analysis of network slicing in 5G networks. *IEEE Communications Standards Magazine, 2*(1), 60-65. https://doi.org/10.1109/MCOMSTD.2018.1700072

Kazmi, S., Khan, L., Tran, N., & Hong, C. (2019). *5G networks. In Network Slicing for 5G and Beyond Networks* (pp. 1-12). Springer. https://doi.org/10.1007/978-3-030-16170-5_1

Kazmi, S., Tran, N., Ho, T., & Hong, C. (2017). Hierarchical matching game for service selection and resource purchasing in wireless network virtualization. *IEEE Communications Letters, 22*(1), 121-124. https://doi.org/10.1109/LCOMM.2017.2701803

Khalifa, N., Benhamiche, A., Simonian, A., & Bouillon, M. (2018). Profit and strategic analysis for MNO-MVNO partnership. *2018 IFIP networking conference (IFIP networking) and workshops*, (pp. 325-333). https://doi.org/10.23919/IFIPNetworking.2018.8696771

Khan, L.-U., Yaqoob, I., Tran, N., Han, Z., & Hong, C. (2020). Network Slicing: Recent Advances, Taxonomy, Requirements, and Open Research Challenges. *IEEE Access*, 8, 36009-36028.

http://doi.org/10.1109/ACCESS.2020.2975072

Khan, R., Kumar, P., Jayakody, D., & Liyanage, M. (2020). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys Tutorials, 22*(1), 196- 248. https://doi.org/10.1109/COMST.2019.2933899

Khan, S., Naseem, U., Siraj, H., Razzak, I., & Imran, M. (2020). The role of unmanned aerial vehicles and mmWave in 5G: Recent advances and challenges. *Transactions on Emerging Telecommunications Technologies*, e4241. https://doi.org/10.1002/ett.4241

Kim, B., & Park, S. (2004). Determination of the optimal access charge for the mobile virtual network operator system. *ETRI journal, 26*(6), 665-668. https://doi.org/10.4218/etrij.04.0204.0016

Kostopoulos, A., Chochliouros, I., & Spada, M. (2019). Business challenges for service provisioning in 5G networks. *International conference on business information systems*, (pp. 423-434). https://doi.org/10.1007/978-3-030-20485-3_33

Koumaras, H., Tsolkas, D., Gardikis, G., Gomez, P., Frascolla, V., Triantafyllopoulou, D., & Bosneag, A. (2018). 5genesis: The genesis of a flexible 5G facility. *IEEE 23rd international workshop on computer aided modeling and design of communication links and networks (camad)*, (pp. 1-6). https://doi.org/10.1109/CAMAD.2018.8514956

Laghrissi, A., & Taleb , T. (2018). A survey on the placement of virtual resources and virtual network functions. *IEEE Communications Surveys & Tutorials, 21*(2), 1409-1434. https://doi.org/10.1109/COMST.2018.2884835

Li, X., Samaka , M., Chan, H., Bhamare, D., Gupta, L., Guo, C., & Jain, R. (2017). Network slicing for 5G: Challenges and opportunities. *IEEE Internet Computing*, 20-27. https://doi.org/10.1109/MIC.2017.3481355

Lin, Y.-B., Tseng, C.-C., & Wang, M.-H. (2021). Effects of transport network slicing on 5G applications. *Future Internet, 13*(3), 69. https://doi.org/10.3390/fi13030069

Liu, Y., Yang, X., & Cuthbert, L. (2021). Network slicing with spectrum sharing. *Radio Access Network Slicing and Virtualization for 5G Vertical Industrie*, 137-166. https://doi.org/10.1002/9781119652434.ch8

Mamadou, A., Toussaint, J., & Chalhoub, G. (2020). Survey on wireless networks coexistence: resource sharing in the 5G era. *Mobile Networks and Applications, 25*(5), 1749–1764. https://doi.org/10.1007/s11036-020-01564-w

Mathur, H., & Deepa, T. (2021). A Survey on Advanced Multiple Access Techniques for 5G and Beyond Wireless Communications. *Wireless Personal Communications*, 1–18. https://doi.org/10.1007/s11277-021-08115-w

MathWorks. (2021). 5G Toolbox. Retrieved from https://www.mathworks.com/products/5g.html

METIS. (2020). METIS 2020 Project. Retrieved from https://metis2020.com/

Michalopoulos, D., Doll, M., Sciancalepore, V., Bega , D., Schneider , P., & Rost, P. (2017). Network slicing via function decomposition and flexible network design. *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (pimrc)*, (pp. 1-6). https://doi.org/10.1109/PIMRC.2017.8292661

Mohamed, K., Alias, M., Roslee, M., & Raji, Y. (2021). Towards green communication in 5G systems: Survey on beamforming concept. *IET Communications, 15*(1), 142–154.

doi:https://doi.org/10.1049/cmu2.12066

Muller, M., Ademaj, F., Dittrich, T., Fastenbauer, A., Elbal, B., Nabayi, A., & Rupp, M. (2018, September). Flexible multi-node simulation of cellular mobile communications: the Vienna 5G System Level Simulator. *EURASIP Journal on Wireless Communications and Networking, 2018*(1), 17. https://doi.org/10.1186/s13638-018-1238-7

Navarro-Ortiz, J., Romero-Diaz, P., Sendra , S., Ameigeiras, P., Ramos-Munoz, J., & Lopez-Soler, J. (2020). A survey on 5G usage scenarios and traffic models. *IEEE Communications Surveys Tutorials, 22*(2), 905-929. https://doi.org/10.1109/COMST.2020.2971781

Next Generation Mobile Network (NGMN) Alliance. (2016). Description of network slicing concept. Retrieved from https://www.ngmn.org/publications/description-of-network-slicing-concept.html

Next Generation Mobile Networks (NGMN) Alliance. (2015). 5G White Paper. Retrieved from https://www.ngmn.org/work-programme/5g-white-paper.html

Nguyen , V.-G., Brunstrom, A., Grinnemo, K.-J., & Taheri, J. (2017). SDN/NFV-based mobile packet core network architectures: A survey. *IEEE Communications Surveys & Tutorials, 19*(3), 1567-1602. https://doi.org/10.1109/COMST.2017.2690823

Nguyen, D., Pathirana, P., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*, 102693. https://doi.org/10.1016/j.jnca.2020.102693

Open5GCore. (2021). Open5GCore toolkit. Retrieved from https://www.open5gcore.org/

Open5GS. (2021). Open5GS. Retrieved from https://open5gs.org/open5gs/

Ordonez-Lucena, J., Ameigeiras, P., Lopez , D., Ramos-Munoz, J., Lorca, J., & Folgueira , J. (2017). Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Communications Magazine, 55*(5), 80–87. https://doi.org/10.1109/MCOM.2017.1600935

Pacheco-Paramo, D., & Tello-Oquendo , L. (2020). Delay-aware dynamic access control for mMTC in wireless networks using deep reinforcement learning. *Computer Networks,* 182, 107493. https://doi.org/10.1016/j.comnet.2020.107493

Pacheco-Paramo, D., Tello-Oquendo, L., Pla, V., & Martinez-Bauset, J. (2019). Deep reinforcement learning mechanism for dynamic access control in wireless networks handling mMTC. *Ad Hoc Networks*, 94, 101939. https://doi.org/10.1016/j.adhoc.2019.101939

Pham, Q., Fang, F., Ha, V., Piran, M., Le, M., Le, L., & Ding, Z. (2020). A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art. *IEEE Access*, 8, 116974–117017. https://doi.org/10.1109/ACCESS.2020.3001277

Pousttchi, K., & Hufenbach, Y. (2009). Analyzing and categorization of the business model of virtual operators. *Eighth international conference on mobile business*, (pp. 87-92). https://doi.org/10.1109/ICMB.2009.22

Prabakaran, D., Nizar, S. M., & Kumar, K. S. (2021). Software-defined network (SDN) architecture and security considerations for 5G communications. In *Design methodologies and tools for 5G network development and application* (pp. 28-43). IGI Global. http://doi.org/10.4018/978-1-7998-4610-9.ch002

Pujol, F., Elayoubi, S., Markendahl, J., & Salahaldin, L. (2016). Mobile telecommunications ecosystem evolutions with 5G. Communications & Strategies(102), 109. Retrieved from

https://www.proquest.com/scholarly-journals/mobile-telecommunications-ecosystem-evolutions/docview/1801631914/se-2?accountid=171402

Rayani, M., Glitho, R., & Elbiaze, H. (2020). ETSI multi-access edge computing for dynamic adaptive streaming in information centric networks. *Globecom 2020-2020 IEEE global communications conference*, (pp. 1-6). https://doi.org/10.1109/GLOBECOM42002.2020.9322209

Romero, J., & Guijarro, L. (2013). Competition between primary and secondary operators with spectrum leasing and optimal spectrum subscription by users. *IEEE 24th international symposium on personal, indoor and mobile radio communications (PIMRC workshops)*, (pp. 143-147). https://doi.org/10.1109/PIMRCW.2013.6707853

Sacoto-Cabrera, E. (2021). *Análisis basado en teoría de juegos de modelos de negocio de operadores móviles virtuales en redes 4G y 5G*. Universitat Politecnica de Valencia. http://doi.org/10.4995/Thesis/10251/158595

Sacoto-Cabrera, E., Guijarro, L., & Maillé, P. (2020). Game theoretical analysis of a multi-MNO MVNO business model in 5G networks. *Electronics, 9*(6), 933. https://doi.org/10.3390/electronics9060933

Sacoto-Cabrera, E., Guijarro, L., Vidal, J., & Pla, V. (2020). Economic feasibility of virtual operators in 5G via network slicing. *Future Generation Computer System*, 109, 172-187. https://doi.org/10.1016/j.future.2020.03.044

Samdanis, K., Costa-Perez, X., & Sciancalepore, V. (2016). From network sharing to multi-tenancy: The 5G network slice broker. *IEEE Communications Magazine, 9*(6), 32-39. https://doi.org/10.1109/MCOM.2016.7514161

Sanenga, A., Mapunda, G., Jacob, T., Marata , L., Basutli , B., & Chuma, J. (2020). An Overview of Key Technologies in Physical Layer Security. *Entropy, 22*(11). https://doi.org/10.3390/e22111261

Santos, G., Endo, P., Sadok, D., & Kelner, J. (2020). When 5G meets deep learning: a systematic review. *Algorithms, 13*(9), 208. https://doi.org/10.3390/a13090208

Selvi, K., & Thamiselvan, R. (2021). Dynamic resource allocation for SDN and edge computing based 5G network. *Third international conference on intelligent communication technologies and virtual mobile networks (icicv)*, (pp. 19-22). https://doi.org/10.1109/ICICV50876.2021.9388468

Shaik, A., Borgaonkar, R., Park, S., & Seifert, J. (2019). New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. *WiSec '19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, (pp. 221-231). https://doi.org/10.1145/3317549.3319728

Smura, T., Kiiski, A., & Hammainen, H. (2007). Virtual operators in the mobile industry: a techno-economic analysis. *NETNOMICS: Economic research and Electronic Networking, 8*(1-2), 25-48. http://doi.org/10.1007/s11066-008-9012-3

Song, G., Wang, W., Chen, D., & Jiang, T. (2018). KPI/KQI-driven coordinated multipoint in 5G: Measurements, field trials, and technical solutions. *IEEE Wireless Communications, 25*(5), 23-29. https://doi.org/10.1109/MWC.2018.1800041

Soós, G., Ficzere, D., Varga, P., & Szalay, Z. (2020). Practical 5G KPI measurement results on a non-standalone architecture. In *Noms 2020 - 2020 IEEE/IFIP network operations and management symposium*, (pp. 1-5). https://doi.org/10.1109/NOMS47738.2020.9110457

Stallings, W. (2015). Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley Professional. Retrieved from https://books.google.com/books?id=nL_QCgAAQBAJ

Su, R., Zhang, D., Venkatesan, R., Gong, Z., Li, C., Ding, F., & Zhu, Z. (2019). Resource allocation for network slicing in 5G telecommunication networks: A survey of principles and models. *IEEE Network, 33*(6), 172-179. https://doi.org/10.1109/MNET.2019.1900024

Tataria, H., Shafi, M., Molisch, A., Dohler, M., Sioland, H., & Tufvesson, F. (2021). 6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities. *Proceedings of the IEEE*, 1-34. https://doi.org/10.1109/JPROC.2021.3061701

Tello-Oquendo, L., Akyildiz, I., Lin , S.-C., & Pla , V. (2018). SDN-based architecture for providing reliable internet of things connectivity in 5G systems. *17th annual mediterranean ad hoc networking workshop (med-hoc-net)*, (pp. 1-8). https://doi.org/10.23919/MedHocNet.2018.8407080

Tello-Oquendo, L., Leyva-Mayorga, I., Pla, V., Martínez-Bauset, J., & Casares-Giner, V. (2015). Analysis of LTE-A random access procedure: A foundation to propose mechanisms for managing the M2M massive access in wireless cellular networks. *Workshop on innovation on information and communication technologies (itaca-wiict 2015)*, (pp. 95-104).

Tello-Oquendo, L., Lin, S.-C., Akyildiz, I., & Pla, V. (2019). Software-defined architecture for QoS-aware IoT deployments in 5G systems. *Ad Hoc Networks*, 93, 101911. https://doi.org/10.1016/j.adhoc.2019.101911

Tello-Oquendo, L., Vidal Catalá, J.-R., Pla, V., & Martínez Bauset, J. (2018). Extended access barring for handling massive machine type communication (mMTC) deployments. *Novasinergia, 1*(2), 38-44. https://doi.org/10.37135/unach.ns.001.02.04

Tello-Oquendo, L., Vidal, J.-R., Pla, V., & Guijarro, L. (2018). Dynamic access class barring parameter tuning in LTE-A networks with massive M2M traffic. *17th annual mediterranean ad hoc networking workshop (med-hoc-net)*, (pp. 1-8). https://doi.org/10.23919/MedHocNet.2018.8407086

Tetcos. (2021). 5G NR. Retrieved from https://www.tetcos.com/5g.html

University of Surrey. (2021). *5G Testbeds*. Retrieved from https://www.surrey.ac.uk/institute-communication-systems/facilities/5g-testbed

Varoutas, D., Katsianis, D., Sphicopoulos, T., Stordahl, K., & Welling , I. (2006). On the economics of 3G mobile virtual network operators (MVNOs). *Wireless Personal Communications, 36*(2), 129-142. http://doi.org/10.1007/s11277-006-0027-5

Vidal, J.-R., Tello-Oquendo, L., Pla, V., & Guijarro, L. (2019). Performance study and enhancement of access barring for massive machine-type communications. *IEEE Access*, 7, 63745–63759. doi:https://doi.org/10.1109/ACCESS.2019.2917618

Xiong, Z., Zhang, Y., Nivato, D., Deng, R., Wang, P., & Wang, L. (2019). Deep Reinforcement Learning for Mobile 5G and Beyond: Fundamentals, Applications, and Challenges. *IEEE Vehicular Technology Magazine, 14*(2), 44-52. https://doi.org/10.1109/MVT.2019.2903655

Xu, Y., Gui, G., Gacanin, H., & Adachi, F. (2021). A Survey on Resource Allocation for 5G Heterogeneous Networks: Current Research, Future Trends and Challenges. *IEEE Communications Surveys Tutorials*, 1-1. https://doi.org/10.1109/COMST.2021.3059896

Yachika, Kaur, P., & Garg, R. (2021, january). A survey on key enabling technologies towards 5G.

IOP Conference Series: Materials Science and Engineering, 012011. https://doi.org/10.1088/1757-899x/1033/1/012011

Zhang, Q., Gui , L., Tian, F., & Sun , F. (2017). A caching-based incentive mechanism for cooperative data offloading. *IEEE international conference on communications workshops (icc workshops)*, (pp. 1376-1381). https://doi.org/10.1109/ICCW.2017.7962851

Zhu, Y., Yu, H., Berry, R., & Liu, C. (2019). Cross-network prioritized sharing: an added value MVNO's perspective. *IEEE infocom 2019-ieee conference on computer communications*, (pp. 1549-1557). https://doi.org/10.1109/INFOCOM.2019.8737636