# 5G shortcomings and Beyond-5G/6G requirements

Meroua Moussaoui[1,2] Emmanuel Bertin[1,2] Noel Crespi[2]
[1] Orange Innovation, 14000 Caen, France
[2] IMT, Telecom SudParis, Institut Polytechnique de Paris, 91764 Palaiseau, France
Emails : {meroua.moussaoui, emmanuel.bertin}@orange.com and noel.crespi@it-sudparis.eu

***Abstract*—Although 5G is designed to provide a large range of new digital services such as immersive experiences, connected machines, and Internet of Things (IoT), 5G networks may not be able to completely meet the needs of emerging novel applications, as well as to address the future needs of the business and regulatory ecosystem. Beyond 5G (B5G) and Sixth Generation (6G) wireless systems are expected to overcome 5G network limits and support a broader range of new use cases in this rapidly expanding digital era. In this survey article, we provide a summary of the major 5G networks shortcomings that are discussed in the literature and classify them into a taxonomy of six primary domains. For each of these domains, we also highlight and discuss the research challenges that will be faced in the development of future B5G and 6G networks.**

***Keywords—5G, B5G, 6G, challenges, limitations, requirements.***

## I. Introduction

Every decade, a new generation of mobile network emerges with technological improvements in data-carrying capacity and latency reduction. The communication network evolved from voice-only services (1G) to Internet Protocol (IP)-based services (4G), and now, to meet the IMT-2020 requirements, 5G was introduced to support three types of services: enhanced Mobile BroadBand (eMBB), ultra-Reliable Low Latency Communications (uRLLC) and massive Machine Type Communications (mMTC). Although it is currently still being deployed, academia and industry are already focusing on B5G and 6G systems, to meet future 2030 demands. Under the motto of "ubiquitous wireless intelligence," B5G/6G will change cellular networks from "connected objects" to "connected intelligence". This rapid shift to Beyond-5G/6G development makes us wonder about the constraints and shortfalls of 5G that are driving researchers to increment the ICTs generation, and how will they build requirements to meet the B5G/6G needs.

This article covers several topics linked to 5G challenges and downfalls, classified into six themes: Radio Access Technologies (RATs), Radio Access Networks (RANs), Network slicing and management, security and privacy, Energy Efficiency (EE), and Policies and regulations. We then use these limits as a guideline to identify, from the literature, some of the most essential requirements and research directions for B5G/6G emerging networks.

Only a few surveys are today available on 5G shortcomings, and even less are surveying B5G/6G requirements. The study in [1] reviews the various difficulties linked to the introduction of 5G New Radio (NR) and lays out a few guidelines for moving to the 6G network, however, it only focuses on the challenges related to spectrum sharing, and the requirements provided for migrating towards 6G are mainly architectural recommendation for virtualized network slicing. Authors in [2] identify challenges for key enabler technologies of 5G, however, they don't tackle the non-technological aspects of 5G.

Other surveys [3]–[11] focus mainly on the challenges of 5G network slicing, IoT, backhaul, Energy Efficiency, resource allocation, millimeter-wave technology, mobility management, and security respectively. The papers [12]–[18] present some requirements for the future B5G/6G networks. To the best of our knowledge, no survey has yet discussed 5G shortcomings comprehensively, along with associated future requirements.

The remainder of this paper is organized as follows: Section II lists 5G's shortcomings categorized by domains, with each domain subdivided into sub-themes for easier comprehension. Section III examines the most important B5G/6G requirements for addressing the 5G shortfalls and ensuring the achievement of the anticipated 6G scenarios. To finally wrapped off with some conclusive remarks.

## II. 5G Shortcomings

This section provides a comprehensive review of the 5G shortcomings categorized into the following themes.

### *A. Radio Access Technologies (RATs) shortcommings in 5G*

#### *1) Spectral efficiency (SE)*

The new access technologies for 5G, such as in-band full-duplex (IBFD), novel waveforms, millimeter wave (mmWave), and massive-MIMO (M-MIMO), are heterogeneous. mmWave has the issue of extreme sensitivity to obstructions, but when employed in the correct conditions, it provides incredible data speeds. In-band full-duplex, adds new types of interference while potentially doubling spectral efficiency depending on the cell's interference profile. New technologies do not automatically imply improved performance in all situations, rather, they provide additional options and variety [19]. Due to the versatility of the 5G network and the immense data rate that MIMO systems induce, optimization and data reduction techniques, such as data compression, aggregation, and removal of redundancy are highly critical [20]. Another limitation is that resource allocation on wireless networks is more complicated due to spectrum availability, device mobility, and the distinction between uplink and downlink channels. Also, an overhead analysis should be performed to uncover design trade-offs [20]. The coexistence of eMBB, uRLLC, and mMTC services within the same RAN obstructs each other's functionality. Massive user connectivity causes uRLLC requirements to be violated by increasing the queuing delay [1].

#### *2) Coverage*

High propagation losses and susceptible blockages of short-wavelength signals are disadvantages of transmissions over 6 GHz bands, limiting the practical coverage of systems [21]. Add to that the fact that wireless network coverage is constrained by the locations and footprints of access points [22]. Current access technologies do not offer full coverage for rural, maritime, and mountain regions, and thus there is a crucial need for technologies like satellites.

*3) Interference*

While Coordinated MultiPoint (CoMP) can be used to achieve multiplexing gain and decode concurrent uplink transmissions from interfering User Equipements (UEs), MIMO decoding affects each UE's attainable rate due to interfering UEs' channel correlation and inadequate decoding algorithms, such as zero-forcing decoding [23]. Moreover, due to the difficulties of using mm-Wave, such as high path loss and blockage, ultra-dense base station deployments are required, and if inadequately coordinated, handoff and inter-cell interference can occur. [24] Another issue is cross-tier interference, which can degrade network performance if not adequately managed due to the vast number of deployed small cell Base Stations (BSs) [25].

### B. Radio Access Networks (RAN) shortcomings in 5G

*1) Service-based RAN architecture*

To suit the needs of diverse use cases, common RAN services can be hierarchically allocated, deployed as part of distinct Network Functions (NFs), or split into several Cloud NFs (CNFs). Most services, though, may be linked, as a result, the service discovery process must be designed so that all services may benefit from it. Interoperability challenges may arise when Service Units (SUs) are produced by various initiatives or even by distinct vendors. To tackle these issues, standardization of SU design, development, and deployment is needed. Another challenge is the partitioning of services, since visibility of services is affected by domain partitioning, it is difficult to partition in a mobile heterogeneous network (HetNet) deployment. The deployment of concurrent services is challenging, some services are misused while others are not used at all when domains are created based on criteria such as nodes. Also, more investigation is need for managing the UEs controller's relationship with other RAN services [26].

*2) Cloud RAN (C-RAN)*

UEs located within the interference range of Remote Radio Units (RRUs) would interfere with each other while a C-RAN jointly administers a pool of collaborative Baseband Units (BBUs) [23]. The presence of a large number of wireless devices may result in severe Inter-User Interference (IUI). Due to the advent of a new set of cloud-structure factors, interference management problems in C-RAN has become more difficult and non-convex [27].

Because several BSs' BBUs are packaged together in the cloud, C-RAN faces a significant risk of single-point failure. The C-RAN architecture, on the other hand, imposes a significant overhead on optical Fronthaul (FH) lines between Remote Radio Head (RRHs) and the cloud, which can be up to 50 times more than the backhaul requirements. The high bit rate requirement in the FH limits C-RAN's performance [27]. Wider channel bandwidths, massive antennas, higher modulation orders, and a larger number of aggregated carriers are used in C-RAN 5G NR, all of which contribute to boosting the necessary FH capacity, as a result, it is critical to provide effective 5G NR ways for controlling and optimizing the use of FH resources with minimal impact on air interface performance [28]. A huge number of FH links are required in ultra-dense C-RAN, and establishing wired links has high operational and maintenance expenses. Wireless networks, such as mmWave communications, are a far more scalable and cost-effective alternative. However, because their bandwidth is substantially lower than that of wired networks, they can only handle a small number of users [29]. Moreover, users can switch between RRHs too frequently, making it difficult to track their location and manage handoffs with guaranteed connection continuity. For multi-cloud C-RANs and variable resource scheduling among RRHs, these functions become even more complex. Furthermore, because of the centralized structure of C-RAN and its signal processing, performing these activities for a large number of devices may incur additional latency [27].

*3) Hetetogeneous C-RAN (H-CRAN)*

Multi-tier H-CRAN includes cells of various sizes and may include both wired and wireless FH connectivity. This heterogeneity raises new research questions about how to build various algorithms that account for both wired and wireless networks. Because of the widespread heterogeneity, number of BSs, network size, and FH/backhaul limits, managing interference in H-CRAN is more difficult [27].

*4) Open RAN (O-RAN)*

O-RAN is not flexible enough to accommodate future upgrades and device compatibility. It also places a significant load on the backhaul and is computationally intensive [30]. Its architecture must take into account Self-Organizing Network (SON) functions. Also, the network slice template must be taken into account by the O-RAN orchestrator when slicing [31]. One challenge is standardizing operation, administration, and management because interoperability is difficult to achieve without standardization. Although O-RAN appears to give the requisite level of interoperability, the details must be worked out [30].

*5) Delay*

As the complexity of the 5G Radio Access Networks (RAN) grows, troubleshooting gets more challenging, and operations must conduct in-depth assessments of the system to assess the root causes. The latency domain is a crucial area where extensive study is lacking. The use of Key Performance Indicators (KPIs) is valuable for network tuning and can detect abnormal delays, but they lack the granularity required to pinpoint the principal cause of delays. Another cause of unanticipated delays and throughput instabilities is the virtualization and distribution of the RAN [32].

### C. Network slicing and management shortcomings in 5G

*1) End-to-End (E2E) slice orchestration & management*

The lack of domain-specific description languages to describe service characteristics, KPIs, resources, and requirements for slices makes it challenging to translate the high-level description of the service into the concrete slice in terms of infrastructure and network functions [3]. As a result, real-time prediction of user behavior is required. Correlating the change of demand to resource allocation, on the other hand, is a major challenge [33]. Another problem is dynamic and optimal slice creation and scaling. Given shifting user demand and fluctuating load, the resources provided to slices must be modified in real-time. Furthermore, as the number and types of slices increase, slice adaptation becomes more difficult. Allocating resources across numerous domains and customizing resources for each tenant at the same time, while maximizing income for various Infrastructure Providers (InPs), remains a difficult task [33]. Collaboration between several infrastructure networks is an appealing way to provide a large number of resources for a low cost. However, establishing efficient collaboration is a difficult task that demands synchronization, the creation of management interfaces, and resource separation across numerous administrative domains [33]. Slicing transparency is a topical question, stretching a slice to the UE opens up new possibilities, like simplification of multi-slice connectivity. However, it introduces new issues, such as the necessity for the slice provider to handle UE mobility as part of the slice setup and maintenance [34]. The measurements required to complete handovers, or the handover decision itself, may not be the same for all slices of multi-slice-connected UEs, thus, a challenge is to make the UE aware of not just the signal strength from nearby BSs, but also which of the slices should be deemed approved slice candidate [35].

*2) RAN slicing*

RAN slicing faces a physical constraint: the limited nature of RAN resources, such as spectrum, compared to network resources in the core network, such as servers and databases [36]. Pre-allocating spectrum ensures isolation but may cause over-provisioning and does not exploit the network's multiplexing capability. However, dynamic fine-grained spectrum allocation ensures efficient use of radio resources but does not maintain isolation. Because 5G networks span many RATs, it is unknown whether multiple RATs may be multiplexed or virtualized on the same hardware, or whether each technology requires its dedicated one [3]. Add to that, the Distributed Units (DU's) functionalities are challenging to virtualize because they rely heavily on dedicated hardware acceleration [37]. The network-related KPIs are challenging to evaluate because they are tied to a shared infrastructure between slices [38].

Other challenges are the stochastic nature of wireless networks, multi-dimensional QoS requirements of services, and spatial-temporal inhomogeneity of service traffic due to users' mobility [39].

*3) Core network (CN) slicing*

Although the CN in 5G is modularized, these modules do not really have any more functionality when compared to the EPC, resulting in added complexity (in terms of interfaces) with no tangible benefits. (Other solutions, such as eDECOR [40], may already enable distinct CN slices that differ only in terms of policy and security functionalities.) The CN's modularization has the potential to allow independent software providers to support their own vertical solutions, and the introduction of controllers in the transport domain to allow differentiated treatment of user plane traffic per slice, necessitates the standardization of previously proprietary interfaces [35]. Some of the NFs in the CN could be moved to the RAN for specific slices that require extremely low latencies and low signaling overhead. To maximize their operation, distinct NFs for verticals will require the utilization of contextual information. The integration of vertical processes over cellular networks and the utilization of contextual information remains a prominent issue [35].

*4) Service composition and resource sharing*

The problem of functions granularity, as coarse-grained functions are easier to assemble since fewer interfaces are required to link them together, but this lowers the slices' flexibility and adaptability. Fine-grained network functions, on the other hand, are adaptable but lack scalability and interoperability for functions implemented by various vendors [3]. Another issue is the lack of computationally and timely optimized intelligent scheduling and allocation for dynamic resource sharing and conflict management among slice tenants [41]. The optimization of the placement and allocation of NFs and resources within a slice, as well as the harmonization between inter-domain slice segments, is a crucial need [37]. Other questions remain unanswered such as the definition of fairness of resource allocation between services, whether puncturing is sufficient to manage traffic high loads, how to overcome the fine line between service provisioning to meet Service-Level Agreement (SLA) requirements, and the problem of over-provisioning [38].

*5) Business and economical models*

Issues relating to the impact of a specific third party on the network's overall performance, as well as specifying the duties of the slice owner and the operator in the event of network performance degradation [38]. Another issue is the lack of a proper business model for managing various services and vertical clients, while profit-maximizing the resource management solutions and interoperability in multi-vendor and multi-technology scenarios [41] [42].

*6) Cooperation with other 5G technologies*

Network slicing must cohabit and collaborate with technologies such as C-RAN, SDN, and NFV, which offer physical resource pooling, software architecture distribution, and management centralization. However, no effective approach of integrating slicing with these technologies to provide E2E connectivity between physical radio equipment and radio equipment controller has yet been developed [43].

*7) Mobility management*

For real-time services, there is a need for quick handover with smooth slice-oriented mobility support and interference management mechanisms [41]. Following a UE promptly using adequate migration prediction techniques is a challenging task [44]. Seamless mobility management strategies and techniques of cooperation between macrocells, small cells, and multiple RATs that can enable users to move from different SDN controllers in 5G heterogeneous systems, and provide high transmission throughput, inter and intra domains, while meeting the customized slicing demands have to be developed [41] [43].

### *D. Security and privacy shortcomings in 5G*

*1) Service-based architecture (SBA)*

The security concerns posed by poorly secured virtualized deployments must not be overlooked, and network equipment vendors must address them through implementation-specific solutions. Some of these vulnerabilities: loss of availability (flooding or crashing an NF, eavesdropping on the Service-based Interface (SBI) or NFs), loss of integrity (changing inter-NF communication and getting illegal access to NFs, modifying data on NFs), loss of control (compromising an NF, protocol or implementation error), insider attacks (illegal modifications to the configuration of an NF) and service thievery (exploiting a breach for unauthorized access to NF). Secure communication between NFs within the core network presents a number of challenges: The creation and sharing of a security context, NF-NRF (Network Repository Function) authentication, and authorization during service discovery and registration, NF-NF authentication and authorization during service access, protection of message confidentiality, and integrity and transportation-related security [45].

*2) Privacy*

Data, location, and identity could all pose serious privacy concerns, as the majority of applications necessitate personal information from subscribers. Semantic information attacks, timing attacks, and boundary attacks all aim to compromise subscribers' location privacy. Access point selection methods in 5G can expose location privacy at the physical layer level. Attacks on the International Mobile Subscriber Identify (IMSI) can be used to reveal a subscriber's identity. Another issue is the synchronization of diverse entities with differing privacy regulations. In circumstances where several actors share the same infrastructure, user and data privacy is substantially compromised. Furthermore, because of cloud-based data storage and NFV features, 5G operators have no direct control over where data is stored in the cloud. Because different nations have different data privacy policies, the privacy of user data stored in a cloud in another country can be jeopardized. Also, as 5G operators started relying on new entities, they are losing control over security and privacy. More privacy risks arise with the integration of IoT [46].

*3) Mobile Cloud Computing (MCC) and Multi-Access Edge Computing (MEC)*

Because MEC is still in its infancy, malicious attacks are a possibility, especially because it extends cloud computing capabilities to the network's edge, where data protection is weak. Interactions can cause network configuration disputes in multi-tenant cloud networks due to the different control logic. Furthermore, because resources are shared, a user can spread malicious traffic to slow down the entire system, consume additional resources, or secretly access the resources of other users. The adoption of open Application Programming Interfaces (APIs) and cloud-enabled IoT are the two most pressing security risks in MEC. DoS attacks, man-in-the-middle (MitM) attacks, malicious mode issues, privacy leakages, and VM manipulation are all common risks. Because of MCC's open architecture and the mobility of mobile terminals, vulnerabilities are classified into targeted cloud segments. Physical risks to application-based threats are all part of the front-end threat landscape. Mobile cloud servers face vulnerabilities ranging from data replication to HTTP and XML DoS (HX-DoS) attacks on the backend. Wi-Fi sniffing, DoS attacks, address impersonation, and session hijacking are examples of network-based mobile security concerns [46].

*4) Network Function Virtualisation (NFV)*

The current NFV platforms do not provide adequate security and isolation to virtualized services when used in mobile networks. VNFs' dynamic nature leads to configuration problems and, as a result, security flaws. VNFs are also subject to common cyber-attacks including spoofing, sniffing, and DoS. Side-channel attacks, flooding attacks, hypervisor hijacking, malware injection, and virtual machine (VM) migration-related attacks, as well as cloud-specific attacks, are all dangers that NFV is subject to. Due to common infrastructure accessibility, a malicious user or a hacked VNF provider can inject malware or alter network traffic. Infrastructure-level attacks on NFV include operational intervention and misuse of shared resources. Because VNFs fetch dynamically from the cloud, maintaining trust in virtualized NFV systems is a major difficulty. Also, inter-federated conflicts can occur if virtual VNFs are misconfigured [46].

*5) Software Defined Networking (SDN)*

SDN systems are vulnerable to saturation attacks, which can knock the system offline by flooding the data plane and/or the control plane. If malicious programs are permitted access, or essential APIs are exposed to unwanted software, damage can be spread across the network, thus, the need for strong authentication and authorization for applications. Data forwarding elements are vulnerable to saturation attacks because they must hold traffic flow requests until the controller updates the flow forwarding rules. Furthermore, because of this reliance on the controller, the control-data planes channel must be resistant to security threats. Controller availability and resiliency may be provided via redundant or multiple controllers. However, network security can be hampered by misconfiguration of forwarding elements or inter-federated conflicts caused by several controllers [46].

*6) Slicing*

Because VNFs are deployed on shared cloud-based infrastructures, and some of them are shared between slices, inter-slice isolation is critical. This allows unauthorized inter-slice communication, posing a threat to the confidentiality and integrity of data communicated through slices [36]. Because certain control plane functions are shared by numerous slices, attackers can listen in on the data of the target slice. A network slice's VNFs can be freely scaled and relocated, which makes the trust chain more dynamic and difficult to manage [47], also, attackers may take advantage of a slice's flexibility to drain the resources of another target slice [37]. Tenant management rights must be handled with caution, particularly when sharing common resources and network functions [47]. Some configuration and management tasks are delegated to other parties via APIs, which could be used by attackers as an entry point [36]. Creating a network slice by managing resources across various technological domains, each with its own set of security features, exposes the network slice to attacks. It is necessary to build trust relationships between the slice manager and the provider who owns the infrastructure [44]. A UE can connect to multiple network slices at the same time. Thus, it can be utilized as a bridge to launch a security attack from one slice to the next, necessitating UE-level separation [37]. The partitioning and coexistence of slices can be constrained by the security requirements of the applications.

*7) RAN*

Disaggregating the functions of the RAN and implementing them in software increases the attack surface in O-RAN, this split architecture exposes the open front-haul interface to Man-in-the-Middle attacks [31]. In addition to the obvious security challenges that any wireless cellular network has, the potential for a large number of intelligent self-configuring nodes to be joined in C-RAN makes it even more vulnerable to new threats [27]. For the availability of RAN services/microservices, secure communication between microservices through TLS should be ensured [26].

*8) Other security challenges*

Roaming does not update user-security parameters, resulting in security compromises [46]. Hackers can modify device settings, disable power saving mode, and make it drain the battery faster by using a MitM attack. As a result, further attacks such as session hijacking, packet/script injection, DNS type assaults, and so on are possible. Unfortunately, 5G networks cannot withstand a MitM attacks indefinitely [48].

Some other issues with the 5G are Diversified Identity Management, Service-oriented Security, E2E Security, Security as a Service, Security challenges posed by the growing number of IoT devices, Security requirements at the communication protocol level, Security in IPv6 over Personal Area Networks. Cryptographic methods are required for security, a proper key approach is required for safeguarding cutting-edge technologies such as Cloud computing, IoT, Machine Learning, Big data, heterogeneous data, Artificial Intelligence, Blockchain (BC), and so on [49].

### *E. Energy Efficiency (EE) shortcomings in 5G*

#### *1) Environemental concerns*

The widespread interconnection of millions of devices increases energy consumption and, as a result, carbon emissions. Furthermore, variables like the manufacture of billions of devices, their shipments, and the excessive usage of radio access networks (fueled by carbon-based energy) increase the carbon footprint. In addition, electrical and electronic equipment waste is difficult to eliminate due to its complicated structure, and the extraction of key elements has been associated with wars and child labour. Worse yet, due to technological advancements or lifetime expiration, millions of IoT devices will have to be destroyed and replaced with new ones [50].

#### *2) Sustainibility*

Boosting transmit power between the increasing number of connected devices to increase communication capacity may result in expensive operating costs [7]. Because energy is a crucial OPerating EXpenditure (OPEX) factor, its smart control is regarded as necessary for network expansion and function, Mobile Network Operators (MNOs) face the challenge of power supply to their large-scale networks [51]. With the deployment of large-scale multiple antennas in a BS, difficulties such as increased complexity, higher Radio Frequency (RF) circuit power, considerable gain, and increased signal processing cost arise [52].

#### *3) Network energy consumption*

Most studies have focused on independent analyses of various energy-efficient technologies, but would a single method be able to fulfill the needed energy efficiency?
Probably no. As a result, a holistic approach is required, combining all the strategies [7]. BSs and end UEs confront energy consumption difficulties as a result of high data rate connections, the usage of many active air interfaces, and mobility [53]. Due to the high energy consumption of power amplifiers used to serve large areas, the power consumed by a macrocell BS and small cells increases as the traffic load grows [51]. BS sleep modes must be implemented effectively to save energy. The impact of a BS's power allocation technique and the handoff and coverage concerns on small cells' energy efficiency should be investigated [54]. The trade-off between hardware power consumption and network power savings via large MIMO with mm-wave beamforming must also be investigated.[54] The impact of Device-to-Device (D2D) communication and UE relaying for cellular IoT on cell energy efficiency has yet to be fully explored [53].

#### *4) Battery draining*

Due to network switching between multiple network standards such as 4G + 5G, 3G + 5G for uninterruptible data transfer, 5G enabled devices' batteries drain faster [48]. Because they must store this energy in limited capacity batteries, network managers must optimize energy utilization [31].

#### *5) Randomness*

Non-uniformity in power consumption endures as a result of non-uniformity in resource requirements and allocation [50]. The availability of environmental energy is fundamentally a stochastic process, posing the problem of energy outages. The main obstacle with networks powered by energy harvesting is the randomness of energy accessible at any given time. Radio-frequency energy harvesting faces the same issue since the amount of electromagnetic power accessible in the air is not known in advance [7].

### *F. Policies and regulations shortcomings in 5G*

#### *1) Network neutrality and non-descrimination*

There are concerns that Internet Service Providers (ISPs) would demand surcharge payments from content providers to ensure suitable transmission speeds even when there is no congestion, and that this will make Internet access unequal for large and small content providers. Advocates for network neutrality believe that a "non-neutral" Internet would stifle innovation since small businesses lack the financial resources to pay for traffic prioritization. Net neutrality opponents, on the other hand, say that prioritization is required for certain services to emerge due to their unique latency or packet loss requirements [55]. Strict net neutrality standards will not allow the two aims of differentiation and non-discrimination to be reconciled, but weak net neutrality, backed by competition policy and maybe ex-post regulation, will [56].

Designing non-discrimination measures is difficult because one of the features of 5G is the provision of differentiated services. With strict non-discrimination, players' innovation incentives will be reduced, and the growth of heterogeneous services and solutions may be stifled, whereas complementors' innovation potential would be increased. Weak anti-discrimination safeguards will reduce innovation limitations, enhance QoS for complementors, but perhaps raise the cost of innovation [56].

#### *2) Paid priorisation and Zero-rating*

Determining when *'paid prioritization'* is objectively justifiable in the context of network slices priced per QoS is a major challenge. Zero-rating and other commercial practices of sponsored data access are depicted as a shift of the network neutrality issue from application throttling and blocking to zero-rating [55].

#### *3) Innovation*

Some policies directly target the decisions of some players to improve system performance, but they also have indirect effects on innovation drivers, influencing outcomes. If these pressures are relevant, the overall effect may be non-linear and difficult to predict, necessitating a distinct regulatory response. Players with a broader control span over elements of the value chain may undermine more specialized players in this innovation environment. Designing markets that facilitate the development of many types of innovation with the productive competition will be one of the difficulties for forward-looking 5G policy [56]. Regulatory goals may be jeopardized by new technical characteristics. Alternatively, regulatory restrictions may hinder the creation of new services that technology may be capable of providing [55].

#### *4) User acceptance*

The demand for more radio BS sites for coverage causes conflicts with local government and some civil organizations due to potential harm posed by electromagnetic radiation. Moreover, there is a need to enforce e-privacy regulations such as the right to erasure, privacy by design and default, data portability, and data breach rules. The use of pseudonyms can stifle future growth. It is a very expensive process to transform personal data in such a way that it cannot be ascribed to a specific data subject without the use of extra information [57].

*5) Market and players*

The interdependencies among actors raise issues, such as determining which markets are relevant and dealing with companies who operate in numerous connected industries. By segmenting national and international wireless markets, authorities' expanding diversity of detailed coverage obligations risks diminishing operational efficiencies. It's debatable if policies are required to make vertical commercial relationships between network operators and higher-level MVNXs (Mobile Virtual Network Operators, aggregators, enablers) easier. Digital markets are concerned about dominant actors' ability to distort competition in ways that are difficult to detect, especially as they lack the tools to analyze the effects of competitive behavior on critical social goals [56]. Conceptual disputes may arise as a result of ambiguous responsibility among players and providers. The regulatory framework for 5G services will have to be built under uncertainty because many parts of 5G are yet unknown, claims for or against regulation are difficult to dispute [56].

## III. Research Directions for B5G/6G

### *A. Radio Access Technologies (RATs) in B5G/6G*

To provide universal coverage, facilitate on-demand services, and support high-rate low-delay services. Space, Air, Ground, and Sea Integrated Networks (SAGSIN) will be exploited [58]. Wi-Fi, Bluetooth, THz, Ultra-WideBand (UWB), Visible Light Communications (VLC), biosensors, and satellite communication can all be integrated into 6G and should all come under the same standard so that they can all communicate with one another. By combining all of these technologies, 6G will be able to take advantage of the large infrastructure built by prior technologies, which would otherwise cost 6G huge expenses [14]. extremely Dense Wireless Networks (eDWNs) and the SAGSIN, in addition to individual network solutions, can improve spatial three-dimensional (3D) [59]. Specific approaches and architectural design will be needed for the seamless integration of satellites into 6G [60].

Obstacles add to the problem of reliability, and as frequency rises, obstacles between transceivers become more likely to block signals. Reconfigurable meta-surfaces (artificial materials with outstanding skills to alter electromagnetic waves) can adjust the propagation conditions to increase reliability [59]. Intelligent Reflecting Surfaces (IRS) technology is being used to reduce the number of antennas installed, the complexity of the hardware, and the spectral efficiency [14].

Rate-Splitting Multiple Access (RSMA) and Non-Orthogonal Multiple Access (NOMA) should be improved, the Orthogonal Frequency Division Multiplexing (OFDM) architecture should be redesigned for lower frequency. mmWave technology for networks with personal BSs and satellite communication. For capacity and long-distance line-of-sight (LoS) coverage, Operation, Administration, and Maintenance (OAM)-aided MIMO is use [14]. Cognitive radio networks, long-term evolution in unlicensed spectrum (LTE-U), and full-duplex for more flexible spectrum management and sharing.

6G should also offer new services by utilizing new technologies, such as: AI/ML for high-performance automated networks with self-organization, self-healing, and self-configuration. High-speed connectivity can be provided through VLC. Quantum computing (QC) for ultra-accurate and secure systems, as well as quantum cryptography for additional services like digital signatures and clock synchronization [14].

### *B. Radio Access Networks (RAN) in B5G/6G*

Current C-RAN techniques result in high latency, network congestion, data processing overhead, and connectivity costs, thus, a new computational paradigm for data storage, processing, management, and manipulation is required [25]. Enhanced methods that account for clustering of both RRHs and BBUs in the cloud will be developed in addition to the existing resource scheduling algorithms [27]. The use of serverless networking that is entirely based on CoMP necessitates a thorough overhaul of the RAN architecture [60]. To reduce latency, 6G will leverage distributed cooperative processing on edge devices, as well as Deep Learning (DL)-based transmission prediction, model-driven DL to train Deep Neural Networks (DNNs) and replace old methods with online accelerated DNNs [59].

### *C. Network slicing and management in B5G/6G*

Researchers highlight the need for AI-native network slicing (Slicing for AI, and AI for slicing)[58]. To handle large requests for dynamically constructing and updating E2E slices across multiple infrastructures, Reinforcement Learning (RL) approaches should be used to improve decision-making speed and accuracy [33]. The development of an effective ML-based handover decision algorithm aids in the resolution of mobility issues.[10] Holistic intelligent slicing management and orchestration system with self-diagnosis, self-healing, and self-configuration to lower the cost and complexity of operations[3], [43] and slicing techniques for large-scale SAGIN are needed. To ensure RAN slicing performance, efficient usage and multiplexing of radio resources are essential [39]. The Physical NFs (PNFs) and VNFs of per-vertical RAN slices in 6G RAN should be properly managed by an intelligent management and orchestration framework [37]. The Resource as a Service (RaaS) architecture could help create virtual RAN instances with customized services while maintaining isolation between slices [3]. In addition to network virtualization, 6G necessitates the virtualization of UEs [61]. Also, using edge computing and quantum computing technology, the intelligent cloud's computational capacity can be increased [1]. A BC-based resource sharing system with automated, economically driven resource management that allows operators to sublease their network resources to other participants should be deployed to deliver services to users. SLAs can be defined and enforced automatically between parties using smart contracts [62]. BC can also be used to create innovative pricing and auction methods to design profit-maximizing resource management strategies for multi-tenant slices [41].

### *D. Security and privacy requirements for B5G/6G*

Differential Privacy (DP) offers intriguing qualities that can counter privacy attacks such differencing, linkage, and reconstruction. Lightweight privacy-preserving approaches, such as homomorphic encryption, are being developed. BC technology is a strong contender for maintaining privacy in content-centric 6G networks. In terms of data, image, location, and communication, various ML types can be used to preserve privacy. However, throughout the training and testing phases of ML models, privacy attacks can occur, necessitating a critical requirement to safeguard the use of ML. Quantum mechanics can also be used to achieve great levels of security and efficiency [63]. In an intelligent RAN, suspicious activities by hostile nodes must be predicted [64]. The main physical layer techniques are secure channel coding, channel-based adaptability, artificial interfering signals, and secret sequence extraction. Use of DL-based attack prediction methods for detecting malicious activities [59]. 6G brings novel privacy criteria for network nodes, such as anonymity, unlinkability, and unobservability [63].

### *E. Energy Efficiency (EE) in B5G/6G*

The development of green disposable electrical devices [50]. It is necessary to optimize the trade-off between transmission and processing power [65]. Efficient circuit modules must be created to reduce power splitting losses and hardware costs [54]. Physical layer strategies to improve EE include index and spatial modulations. Wireless Power Transfer (WPT) and Simultaneous Wireless Information and Power Transfer (SWIPT) are promising energy harvesting-based technologies for supplying energy to wireless receivers. A significant potential method is to use interfering power as an energy source [59].

### *F. Policies and regulations in B5G/6G*

Innovative models for billing/charging verticals, new cost-sharing grounds, and standardized solutions for interoperability in multi-vendor and multi-technology contexts must all be investigated [42]. Data ownership and access are becoming increasingly important determinants in value generation, and restricting such access is a way to maintain control. Creating a system that transforms how data is collected, shared, and analyzed in real-time might unlock significant future value and introduce new stakeholder roles, but it can also raise substantial privacy and ethical concerns about data placement and use on a global scale [66].

## IV. Discussions & conclusion

While 5G is still in a development phase and has a long way to go before being fully deployed, industry and academia have begun to examine its critical limitations, which range from technical to environmental impacts, and are attempting to address them through the revolution of B5G/6G for 2030.

In this paper, we reviewed the most important studies on the shortcomings of 5G and the requirements for B5G/6G networks. We've then provided a taxonomy of 5G network shortcomings based on several themes, as well as several open problems and significant guidelines, as a set of requirements, for overcoming these issues in the development of future B5G/6G networks. However, we believe that the research works on these new technologies should probably start by carefully monitoring 5G deployments and ecosystem shifts, in order to give 5G enough time to mature and demonstrate its full performances, as well as to get operational feedback on its limitations.

## References


[1] A. Dogra, R. K. Jha, et S. Jain, « A survey on beyond 5G network with the advent of 6G: Architecture and emerging technologies », IEEE Access, vol. 9, p. 67512-67547, 2020.

[2] H. Fourati, R. Maaloul, et L. Chaari, « A survey of 5G network systems: challenges and machine learning approaches », Int. J. Mach. Learn. Cybern., vol. 12, no 2, p. 385-431, 2021.

[3] X. Foukas, G. Patounas, A. Elmokashfi, et M. K. Marina, « Network slicing in 5G: Survey and challenges », IEEE Commun. Mag., vol. 55, no 5, p. 94-100, 2017.

[4] G. A. Akpakwu, B. J. Silva, G. P. Hancke, et A. M. Abu-Mahfouz, « A survey on 5G networks for the Internet of Things: Communication technologies and challenges », IEEE Access, vol. 6, p. 3619-3647, 2017.

[5] S. Li, L. Da Xu, et S. Zhao, « 5G Internet of Things: A survey », J. Ind. Inf. Integr., vol. 10, p. 1-9, 2018.

[6] M. Jaber, M. A. Imran, R. Tafazolli, et A. Tukmanov, « 5G backhaul challenges and emerging research directions: A survey », IEEE Access, vol. 4, p. 1743-1766, 2016.

[7] S. Buzzi, I. Chih-Lin, T. E. Klein, H. V. Poor, C. Yang, et A. Zappone, « A survey of energy-efficient techniques for 5G networks and challenges ahead », IEEE J. Sel. Areas Commun., vol. 34, no 4, p. 697-709, 2016.

[8] Y. Xu, G. Gui, H. Gacanin, et F. Adachi, « A survey on resource allocation for 5G heterogeneous networks: Current research, future trends and challenges », IEEE Commun. Surv. Tutor., 2021.

[9] B. T. Jijo et al., « A comprehensive survey of 5G mm-wave technology design challenges », Asian J. Res. Comput. Sci., vol. 8, no 1, p. 1-20, 2021.

[10] I. Shayea, M. Ergen, M. H. Azmi, S. A. Çolak, R. Nordin, et Y. I. Daradkeh, « Key challenges, drivers and solutions for mobility management in 5G networks: A survey », IEEE Access, vol. 8, p. 172534-172552, 2020.

[11] A. Dutta et E. Hammad, « 5G security challenges and opportunities: a system approach », in 2020 IEEE 3rd 5G World Forum (5GWF), 2020, p. 109-114.

[12] Z. Zhang et al., « 6G wireless networks: Vision, requirements, architecture, and key technologies », IEEE Veh. Technol. Mag., vol. 14, no 3, p. 28-41, 2019.

[13] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, et Y. M. Jang, « 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions », IEEE Open J. Commun. Soc., vol. 1, p. 957-975, 2020.

[14] M. W. Akhtar, S. A. Hassan, R. Ghaffar, H. Jung, S. Garg, et M. S. Hossain, « The shift to 6G communications: vision and requirements », Hum.-Centric Comput. Inf. Sci., vol. 10, no 1, p. 1-27, 2020.

[15] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland, et F. Tufvesson, « 6G wireless systems: Vision, requirements, challenges, insights, and opportunities », Proc. IEEE, vol. 109, no 7, p. 1166-1199, 2021.

[16] K. David et H. Berndt, « 6G vision and requirements: Is there any need for beyond 5G? », IEEE Veh. Technol. Mag., vol. 13, no 3, p. 72-80, 2018.

[17] B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, et J. Wang, « 6G technologies: Key drivers, core requirements, system architectures, and enabling technologies », IEEE Veh. Technol. Mag., vol. 14, no 3, p. 18-27, 2019.

[18] G. Liu et al., « Vision, requirements and network architecture of 6G mobile network beyond 2030 », China Commun., vol. 17, no 9, p. 92-104, 2020.

[19] C. Sexton, N. J. Kaminski, J. M. Marquez-Barja, N. Marchetti, et L. A. DaSilva, « 5G: Adaptable networks enabled by versatile radio access technologies », IEEE Commun. Surv. Tutor., vol. 19, no 2, p. 688-720, 2017.

[20] D. Pliatsios, P. Sarigiannidis, S. Goudos, et G. K. Karagiannidis, « Realizing 5G vision through Cloud RAN: technologies,

challenges, and trends », EURASIP J. Wirel. Commun. Netw., vol. 2018, no 1, p. 1-15, 2018.
[21] J. Lorincz et Z. Klarin, « How Trend of Increasing Data Volume Affects the Energy Efficiency of 5G Networks », Sensors, vol. 22, no 1, p. 255, 2022.
[22] A. Sattarzadeh et al., « Satellite-Based Non-Terrestrial Networks in 5G: Insights and Challenges », IEEE Access, 2021.
[23] T.-Y. Yu et K. C.-J. Lin, « User Pairing and Resource Allocation for Opportunistic CoMP in 5G CRAN », in 2021 IEEE Global Communications Conference (GLOBECOM), 2021, p. 1-6.
[24] B. Maham, « Performance Analysis of Ultra-Dense Millimeter Wave Cloud-RAN under Blockage and Interference », in 2021 IEEE Global Communications Conference (GLOBECOM), 2021, p. 1-6.
[25] P. Rahimi, C. Chrysostomou, H. Pervaiz, V. Vassiliou, et Q. Ni, « Dynamic Resource Allocation for SDN-based Virtual Fog-RAN 5G-and-Beyond Networks », in 2021 IEEE Global Communications Conference (GLOBECOM), 2021, p. 01-06.
[26] E. Zeydan, J. Mangues-Bafalluy, J. Baranda, M. Requena, et Y. Turk, « Service Based Virtual RAN Architecture for Next Generation Cellular Systems », IEEE Access, 2022.
[27] M. F. Hossain, A. U. Mahin, T. Debnath, F. B. Mosharrof, et K. Z. Islam, « Recent research in cloud radio access network (C-RAN) for 5G cellular systems-A survey », J. Netw. Comput. Appl., vol. 139, p. 31-48, 2019.
[28] S. Lagén, X. Gelabert, L. Giupponi, et A. Hansson, « Fronthaul-Aware Scheduling Strategies for Next Generation RANs », in 2021 IEEE Global Communications Conference (GLOBECOM), 2021, p. 1-6.
[29] C. Pan, M. Elkashlan, J. Wang, J. Yuan, et L. Hanzo, « User-centric C-RAN architecture for ultra-dense 5G networks: Challenges and methodologies », IEEE Commun. Mag., vol. 56, no 6, p. 14-20, 2018.
[30] S. K. Singh, R. Singh, et B. Kumbhani, « The evolution of radio access network towards open-RAN: challenges and opportunities », in 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2020, p. 1-6.
[31] B. Brik, K. Boutiba, et A. Ksentini, « Deep Learning for B5G Open Radio Access Network: Evolution, Survey, Case Studies, and Challenges », IEEE Open J. Commun. Soc., 2022.
[32] T. Sundqvist, M. Bhuyan, et E. Elmroth, « Uncovering latency anomalies in 5G RAN-A combination learner approach », in 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), 2022, p. 621-629.
[33] W. Guan, H. Zhang, et V. C. Leung, « Customized slicing for 6G: Enforcing artificial intelligence on resource management », IEEE Netw., vol. 35, no 5, p. 264-271, 2021.
[34] P. Rost et al., « Network slicing to enable scalability and flexibility in 5G mobile networks », IEEE Commun. Mag., vol. 55, no 5, p. 72-79, 2017.
[35] A. Kaloxylos, « A survey and an analysis of network slicing in 5G networks », IEEE Commun. Stand. Mag., vol. 2, no 1, p. 60-65, 2018.
[36] S. Wijethilaka et M. Liyanage, « Survey on network slicing for Internet of Things realization in 5G networks », IEEE Commun. Surv. Tutor., vol. 23, no 2, p. 957-994, 2021.
[37] S. Zhang, « An overview of network slicing for 5G », IEEE Wirel. Commun., vol. 26, no 3, p. 111-117, 2019.
[38] S. E. Elayoubi, S. B. Jemaa, Z. Altman, et A. Galindo-Serrano, « 5G RAN slicing for verticals: Enablers and challenges », IEEE Commun. Mag., vol. 57, no 1, p. 28-34, 2019.
[39] J. Mei, X. Wang, et K. Zheng, « An intelligent self-sustained RAN slicing framework for diverse service provisioning in 5G-beyond and 6G networks », Intell. Converg. Netw., vol. 1, no 3, p. 281-294, 2020.
[40] 3GPP, Enhancements of dedicated core networks selection mechanism. 2016.
[41] A. A. Barakabitze, A. Ahmad, R. Mijumbi, et A. Hines, « 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges », Comput. Netw., vol. 167, p. 106984, 2020.
[42] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, et J. Folgueira, « Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges », IEEE Commun. Mag., vol. 55, no 5, p. 80-87, 2017.
[43] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, et V. C. Leung, « Network slicing based 5G and future mobile networks: mobility, resource management, and challenges », IEEE Commun. Mag., vol. 55, no 8, p. 138-145, 2017.
[44] C. Campolo, A. Molinaro, A. Iera, et F. Menichella, « 5G network slicing for vehicle-to-everything services », IEEE Wirel. Commun., vol. 24, no 6, p. 38-45, 2017.
[45] H. C. Rudolph, A. Kunz, L. L. Iacono, et H. V. Nguyen, « Security challenges of the 3gpp 5g service based architecture », IEEE Commun. Stand. Mag., vol. 3, no 1, p. 60-65, 2019.
[46] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, et A. Gurtov, « Overview of 5G security challenges and solutions », IEEE Commun. Stand. Mag., vol. 2, no 1, p. 36-43, 2018.
[47] R. F. Olimid et G. Nencioni, « 5G network slicing: A security overview », IEEE Access, vol. 8, p. 99999-100009, 2020.
[48] M. Iavich, G. Akhalaia, et S. Gnatyuk, « Method of Improving the Security of 5G Network Architecture Concept for Energy and Other Sectors of the Critical Infrastructure », in Systems, Decision and Control in Energy III, Springer, 2022, p. 237-246.
[49] N. Lal, S. M. Tiwari, D. Khare, et M. Saxena, « Prospects for handling 5G network security: Challenges, recommendations and future directions », in Journal of Physics: Conference Series, 2021, vol. 1714, no 1, p. 012052.
[50] S. Popli, R. K. Jha, et S. Jain, « A survey on energy efficient narrowband internet of things (NBIoT): architecture, application and challenges », IEEE Access, vol. 7, p. 16739-16776, 2018.
[51] A. Israr, Q. Yang, W. Li, et A. Y. Zomaya, « Renewable energy powered sustainable 5G network infrastructure: Opportunities, challenges and perspectives », J. Netw. Comput. Appl., vol. 175, p. 102910, 2021.
[52] A. Israr, Q. Yang, et A. Israr, « Power consumption analysis of access network in 5G mobile communication infrastructures—An analytical quantification model », Pervasive Mob. Comput., p. 101544, 2022.
[53] M. Höyhtyä, O. Apilo, et M. Lasanen, « Review of latest advances in 3GPP standardization: D2D communication in 5G systems and its energy consumption models », Future Internet, vol. 10, no 1, p. 3, 2018.
[54] A. Abrol et R. K. Jha, « Power optimization in 5G networks: A step towards GrEEn communication », IEEE Access, vol. 4, p. 1355-1374, 2016.
[55] Z. Frias et J. P. Martínez, « 5G networks: Will technology and policy collide? », Telecommun. Policy, vol. 42, no 8, p. 612-621, 2018.
[56] J. M. Bauer et E. Bohlin, « Regulation and innovation in 5G markets », Telecommun. Policy, p. 102260, 2021.
[57] D. Lučić, « Regulatory challenges due to implementation of Internet of Things based on 5G technology », in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, p. 0339-0344.
[58] W. Wu et al., « AI-native network slicing for 6G networks », ArXiv Prepr. ArXiv210508576, 2021.
[59] G. Gui, M. Liu, F. Tang, N. Kato, et F. Adachi, « 6G: Opening new horizons for integration of comfort, security, and intelligence », IEEE Wirel. Commun., vol. 27, no 5, p. 126-132, 2020.
[60] M. A. Habibi, B. Han, M. Nasimi, N. P. Kuruvatti, A. Fellan, et H. D. Schotten, « Towards a Fully Virtualized, Cloudified, and Slicing-Aware RAN for 6G Mobile Networks », in 6G Mobile Wireless Networks, Springer, 2021, p. 327-358.
[61] X. Shen, J. Gao, W. Wu, M. Li, C. Zhou, et W. Zhuang, « Holistic Network Virtualization and Pervasive Network Intelligence for 6G », IEEE Commun. Surv. Tutor., 2021.
[62] F. Wilhelmi et L. Giupponi, « On the Performance of Blockchain-enabled RAN-as-a-service in Beyond 5G Networks », ArXiv Prepr. ArXiv210514221, 2021.
[63] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, et M. Ylianttila, « The roadmap to 6G security and privacy », IEEE Open J. Commun. Soc., vol. 2, p. 1094-1122, 2021.
[64] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, et M. Ylianttila, « 6G security challenges and potential solutions », in 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2021, p. 622-627.
[65] M. Usama et M. Erol-Kantarci, « A survey on recent trends and open issues in energy efficiency of 5G », Sensors, vol. 19, no 14, p. 3126, 2019.
[66] M. Matinmikko-Blue, S. Yrjölä, et P. Ahokangas, « Spectrum management in the 6G era: The role of regulation and spectrum sharing », in 2020 2nd 6G Wireless Summit (6G SUMMIT), 2020, p. 1-5.