Expansive Networks: Exploiting Spectrum Sharing for Capacity Boost and 6G Vision

Gürkan Gür

Abstract: **Adaptive capacity with cost-efficient resource provisioning is a crucial capability for future 6G networks. In this work, we conceptualize "expansive networks" which refers to a networking paradigm where networks should be able to extend their resource base by opportunistic but self-controlled expansive actions. To this end, we elaborate on a key aspect of an expansive network as a concrete example: Spectrum resource at the PHY layer. Evidently, future wireless networks need to provide efficient mechanisms to coexist in the licensed and unlicensed bands and operate in expansive mode. In this work, we first describe spectrum sharing issues and possibilities in 6G networks for expansive networks. We then present security implications of expansive networks, an important concern due to more open and coupled systems in expansive networks. We also discuss two key enablers, namely distributed ledger technology (DLT) and network intelligence via machine learning, which are promising to realize expansive networks for the spectrum sharing aspect.**

Index Terms: **6G/Beyond 5G networks, DLT, expansive networks, spectrum sharing, network intelligence**

I. INTRODUCTION

FULFILLING the requirements of formidable and diverse 6G use cases necessitates not only a high resource efficiency but also higher flexibility and scalability in future wireless networks. To put it plainly, resource expansion is crucial. The networks are supposed to reach beyond their statistically assigned resources and exploit available resources based on spatial and temporal requirements. This can be facilitated via preagreed sharing schemes (infrastructure/resource sharing) or opportunistically realized (e.g., cognitive radios). For radio access side, spectrum is the key determinant. The mobile network operators typically need exclusive access to some spectrum for signaling and emergency use. However, that would probably be a 20–40 MHz, and a large portion of the spectrum they currently monopolize can be turned back. In addition to that empirical inefficiency, 6G will take the resource challenges to a next level with new services and applications such as 3D holographic imaging and presence, 5D communications (sight, hearing, touch, smell and taste), smart clothing and wearables, and fully autonomous vehicles [1]. Furthermore, the connectivity will reach to an extreme level [2] as envisaged by ITU-R with 2030 prediction of almost 120 billion subscriptions including M2M subscriptions and exponentially increasing traffic [3].

Manuscript received May 31, 2020; revised October 20, 2020; approved for publication by Periklis Chatzimisios, Guest Editor, November 24, 2020.

This work was funded by the SNSF Scientific Exchanges grant (no. 187690).

G. Gür is with the Zurich University of Applied Sciences, Winterthur, Switzerland, email: gueu@zhaw.ch.

G. Gür is the corresponding author.

Digital Object Identifier: 10.23919/JCN.2020.000037

Disruptive events like COVID-19 pandemic have also clearly shown the need for capacity flexibility and adaptive resource provisioning. Connectivity has become even more critical for many daily tasks and economic activities such as education, remote working and telemedicine. The traffic surge due to COVID-19 pandemic is accordingly observed [4]. According to April 2020 figures in Europe by Nokia, immediately after pandemic lock-down, we have seen weekday peak traffic increases over 45%, occasionally even hitting over 50%, and weekend evening peak traffic increases over 20%–40% over their pre-lockdown levels [5]. Additionally, there is continuing growth in subscriber upstream traffic – above 30% on average. Therefore, in addition to plain traffic amount, the spatio temporal characteristics of the network traffic have abruptly changed. Although telecommunication networks and networked services are crucial for daily activities and economic continuity, it is impractical to provision such capacity beforehand (i.e., considering the worst-case scenario). The resource silos created by static regulation and lack of cooperation should be overcome.

The opportunistic resource expansion in a communication network is a promising paradigm to address "stringent and erratic" demand characteristics in an efficient way. It can be realized in various dimensions (e.g., time-domain or frequency domain [6]) and at various entities in the network (e.g., end devices or the core network) [7]. Fig. 1 depicts the 6G landscape which calls for resource expansion for meeting the envisaged use cases, requirements, and service levels. 6G will lead to a wide range of new applications such as holographic telepresence, extended reality (XR), Internet of everything (IoE), Industry 5.0, and collaborative robotics, which will drastically reshape the human society of 2030s and beyond. To realize the 6G vision, the radio itself needs to be agile and adaptive beyond 5G NR definition since 6G radio needs to be extremely capable to utilize different channel bandwidths over a very wide spectrum, support cell-free communications, realize ultra massive MIMO, and work on non-continuous spectrum [8]. The required flexibility can also be introduced in core and transport networks with deeper integration of network softwarization and network slicing. Moreover, the stringent operational settings ranging from ultra-reliable and low-latency scenarios to massive connectivity requires a much more flexible radio that will support spectrum sharing [9]. In that regard, capacity expansion via adaptive techniques including spectrum sharing is a fundamental solution for serving the envisaged applications in 6G ecosystem [10].

In this work, we first describe our "expansive network" concept which builds on the idea of flexibility and capacity expansion with resource capture and sharing. Then we elaborate on a key technique, still to be exploited to the full potential, on the radio access side: The spectrum sharing vision in 6G networks

1229-2370/19/$10.00

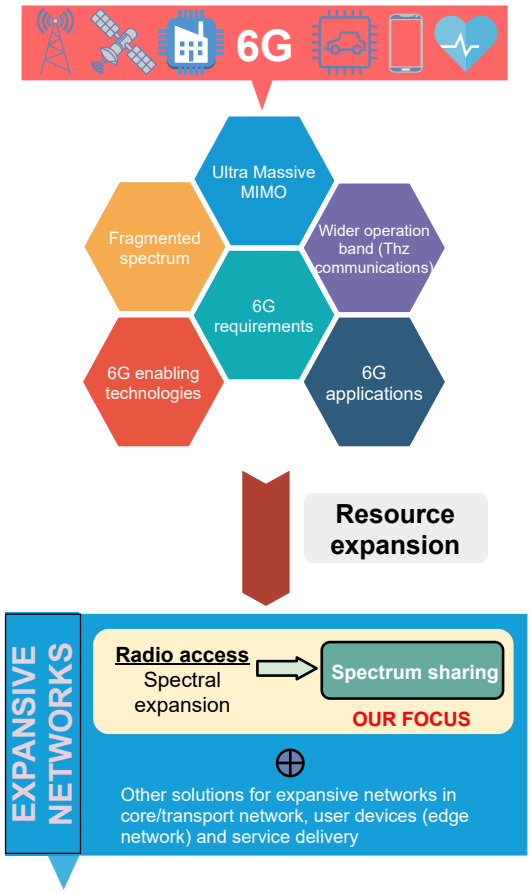

Fig. 1. Emerging challenges, technologies, requirements in 6G and capacity expansion.

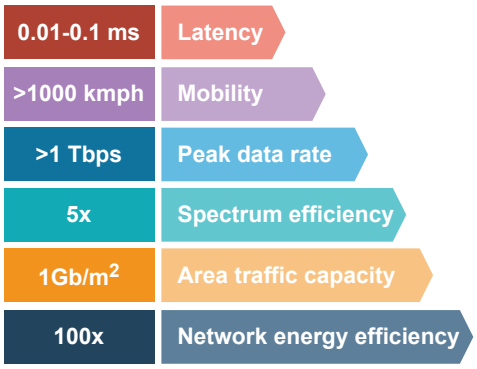

Fig. 2. 6G requirements for envisaged applications.

from a co-existence perspective. To this end, we first describe spectrum sharing issues and possibilities in 6G networks. Then present security implications of expansive networks, a major aspect due to increased attack surfaces for more open and coupled systems in that setting. We also discuss two key techniques, namely distributed ledger technology (DLT) and network intelligence via machine learning, which are promising for expansive networks to alleviate the increased uncertainty and complexity in coexistence of diverse networks in 6G.

A. 6G Requirements and Enabling Technologies

Future 6G applications will pose stringent requirements and require extended network capabilities compared to currently developed 5G networks. These requirements are summarized in Fig. 2. They are established to enable the wide range of key 6G use cases and thus can be categorized accordingly. For further enhanced mobile broadband (FeMBB), the mobile connection speed has to reach the peak data rate at Tbps level [11]. With ultra massive machine type communication (umMTC), the connection density will further increase in 6G due to the novel concept of IoE as the next phase of IoT. These devices will have to communicate with each other and the infrastructure, and provide collaborative services in an autonomous and self-driven manner [12]. For new latency extremely-sensitive 6G applications in the enhanced ultra-reliable, low-latency communication (ERLLC/eURLLC) use case, the E2E latency in 6G should be reduced down to μs level [9].

Regarding the extreme operational requirements, extremely low-power communications (ELPC) concept in 6G will require the network energy efficiency to be improved by 10x than 5G and 100x than 4G. It will enable extremely low power communications for resource constrained devices such as IoT or energy harvesting devices [9]. For extreme spatial requirements, long distance high-mobility communications (LDHMC) will closely integrate the space and aerial technologies such as satellites in 6G to provide communications for under-served coordinates such as space and deep sea. Moreover, intelligent and proactive mobility management systems will support seamless and instant mobility beyond 1000 kmph speeds [11].

The capacity boost by 6G is materialized in the high spectrum efficiency requirement. The spectrum efficiency is to be further improved in 6G nearly up to two times compared to 5G networks [9]. Moreover, high area traffic capacity stems from the exponential growth of IoT and ultra massive connectivity, which will increase the area traffic capacity by 100 times than 5G networks, leading up to 1 Gpbs traffic per square meter in 6G networks.

B. 6G Enabler Technologies

Various enabler technologies are being developed to meet 6G requirements and realize 6G applications as shown in Fig. 3. At the network edge, novel technologies such edge AI running AI algorithms locally at the edge [13] or smart surfaces with embedded intelligence working with IoT and big data analysis as dynamic, reconfigurable and digitally controllable surfaces will offer intelligent services [14] in 6G. To this end, omnipresent integration of smart and intelligent devices and hyperconnected digital surroundings will lead to a fundamental shift from a gadget-centric to a user-centric or gadget-free communication mode, providing all the information, tools, and services users need in their everyday life [15]. These technologies will be accompanied with the trends of expansion of IoT, massive availability of small data and the convergence of communication, sensing, control, localization and computing [8]. Moreover, emerging radio technologies such as cell-free communications and reconfigurable intelligent surfaces will provide the required capacity improvements in the 6G wireless connectivity. The spectrum leap to the higher frequencies towards THz communications and new transmission techniques such as visi-

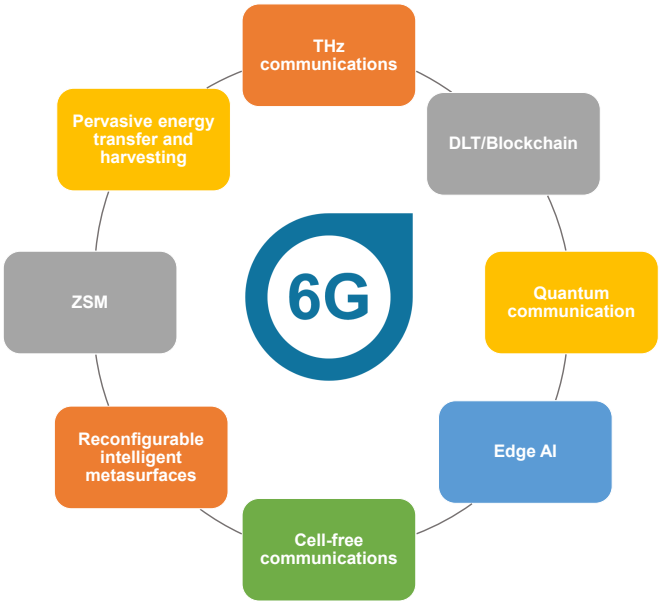

Fig. 3. Various technologies envisaged as enablers for 6G.

ble light communications (VLC) will incorporate new PHY resources [16]. The 6G network will manage swarms of edge devices, unmanned aerial vehicles (UAVs) or robots efficiently for collaborative tasks and services [17].

Across a 6G network, zero touch network and service management (ZSM) will enable full end-to-end automation of management functions to deliver services in agile, rapid and scalable manner [18]. DLT/blockchains will play a major role in enabling many 6G services as a decentralized secure immutable database managed by multiple users [19]. With the development of quantum computing research, 6G may support quantum communication technology. In quantum communication, quantum physics concepts pertaining to quantum information processing and quantum teleportation are utilized. A key application of quantum communication is the protection of information channels against eavesdropping by means of quantum cryptography [20].

II. EXPANSIVE NETWORKS: A HOLISTIC DEFINITION

A key driver for 5G evolution was to exploit the available infrastructure to the full, which translates to efficient use of deployed network resources in a multi-vendor/multi-technology environment for dynamically varying demand for network resources [21]. However, there are still important challenges regarding multi-tenant and multi-operator networks and over-the-top (OTT) players like on-demand video streaming. Moreover, quasi-adaptive approaches such as frequency leasing at the spectrum layer are also proposed but not superior. Nevertheless, this naive approach is not sufficient to meet the demands of 6G. The idea of adaptive and flexible capacity expansion across spectrum, infrastructure, and services needs to be natively embedded in communication networks. This leads to our concept *Expansive Networks* where self-driven but controlled expansionist paradigm between coexisting networks is embedded into network management. The enablers for expansive networks are shown in Fig. 4. The multifaceted nature of expansive paradigm should be considered as described below:

- **Service layer expansion:** Cloudification and service virtualization provides scalability for service components in computation, storage and in-data-center-bandwith dimensions. 6G expansive networks should take this transformation that initiated with 5G networks and employ it as the de facto mode of operation. However, regulations and legal issues (especially due to security, privacy and liability issues) with quasi-static system configurations are important inhibitors in that aspect.
- **Network infrastructure:** Network virtualization and backhaul scalability via shared common infrastructure are essential pillars of capacity expansion [22]. Especially, network slicing for different verticals and slice sharing to meet demand surges are instrumental. For expansive networks, 6G networks can autonomously generate and optimize user-centric slices using closed-loop and automated control schemes [23]. To this end, network automation including automated service decomposition and orchestration [18], [24] and self-driving networks provide a toolbox for expansive networks [25]. While the former primarily deals with efficiently automating the data plane and the network slice management, self-driving networks concept [26] seek complete automation of network management, without any need of manual intervention [25] in the ZSM spirit.
- **Edge domain expansion:** In the multi-access edge computing (MEC) domain, shared MEC platforms and RAN cloudification are enablers for expansive networks [27]. However, the openness of those systems for scalability and expansion are still limited. At the very edge, computation sharing/offloading in edge devices and D2D communications provide capacity expansion, albeit challenging due to fragmented landscape [28]. This includes the wireless access resources, including spectrum resources which is our main focus in this work.

Although there are some elements already available in 4G and 5G domains, we believe the expansive networks concept has to elaborated and adopted as one of the underlying principles in future 6G networks. In this work, we investigate the spectrum expansion topic for capacity boost in expansive networks and discuss the implications of spectrum sharing for that goal.

III. COEXISTENCE AND SPECTRUM SHARING FOR EXPANSIVE NETWORKS

Spectrum expansion builds on the resource co-utilization among coexisting networks. Essentially, a coexistence scenario consists of at least two wireless networks operating at the same (or partially overlapping) spectrum band and are in close proximity such that they may cause harmful interference on each other due to dual unlicensed operation (e.g., a licensed cellular network exploiting also unlicensed spectrum) or opportunistic spectrum access between licensed networks. However, such systems inherently have diverse and fragmented characteristics regarding spectrum operation bands or PHY/MAC functions [29]. For instance, FCC's largest spectrum auction for 5G mmWave

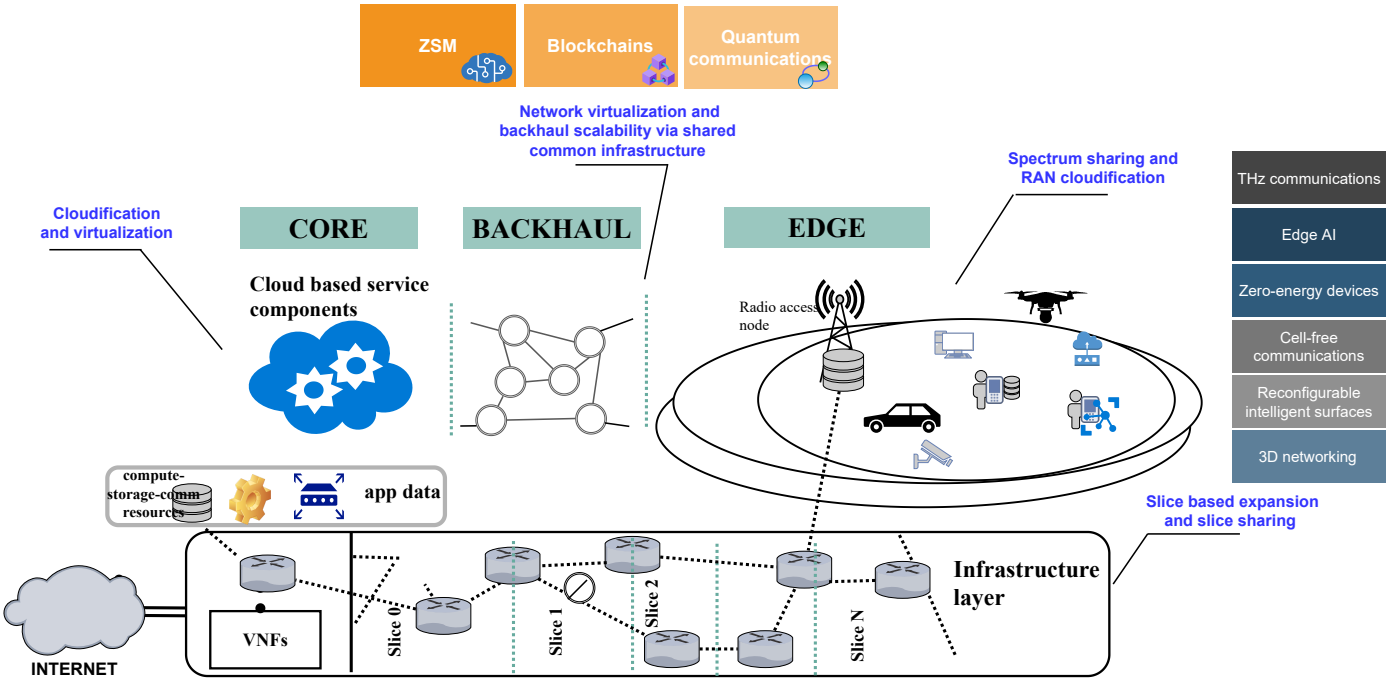

Fig. 4. Expansive networks and different enablers at different layers and segments for capacity expansion (noted in callouts).

bands of upper 37 GHz, 39 GHz, and 47 GHz was completed in March 2020 [30], pushing operation bands to higher frequencies. 6G networks will have an even wider spectrum of operation and more diverse network technologies compared to 5G [31]. Current research has already positioned THz spectrum as a major frequency domain for future wireless networks [32]. In a general setting, the coexistence of heterogeneous networks are challenging due to the following reasons [7]:

- **Heterogeneity in operation principles and parameters:** Coexistence among networks is challenging especially when these networks are heterogeneous, e.g., regarding underlying technology or ownership by different operators. For the former, heterogeneity may imply the lack of common spectrum etiquette: The spectrum access rules differ across networks, leading to difficulties in fair sharing of the resources. The existence of a co-channel network implementing self-driven medium access then may lead to starvation and unfairness in spectrum sharing, if that system does not implement an efficient coexistence scheme. There could also be cases called *cross-technology hidden nodes* where one access point from a specific technology is not visible to another spectrum sharing network, e.g., WiFi access point undetected by a cellular base station in its vicinity. this situation leads to suboptimal decision making for spectrum access.
  Despite networks following similar operation principles, different operation parameters might result in diverse performance among these networks. There are issues related to channel access such as different MAC behavior, listen-before-talk schemes or conventional back-off approaches driven by different approaches. Similarly, heterogeneity might involve asymmetry in the coexisting networks, e.g., one network having a higher permitted transmission power level than the other. Resulting power asymmetry puts the low-power network in disadvantage and might result in strong interference from the other network without proper coexistence schemes.
- **Heterogeneity in ownership:** Although networks might operate based on the same principles and with similar protocol parameters, coexistence becomes challenging due to inter-operator competition or simply lack of interfaces for implementing collaboration among networks [33]. Residential WiFi networks are a typical example which proves the challenge of spectrum sharing even among homogeneous networks if such networks do not coordinate.
- **Lack of cooperation:** Cooperation among different networks are beneficial to utilize the spectrum in a more efficient regime since it minimizes collisions and destructive competition for the spectral resources. Different spectrum sharing radios should be willing to behave altruistically for specific time intervals or locations to avoid common degradation for all spectrum sharing parties.
- **Inter-network communications for spectrum sharing:** Inherently, the networks are not designed to employ inter-network and -technology communications for facilitating spectrum sharing. However, efficient spectrum sharing is attainable with awareness of the environment and participating networks, e.g., what kind of networks are around. Apparently, this capability is not sufficient if the spectrum sharing networks do not act upon them in a cooperative manner. Thus, such data exchange in 6G networks can alleviate spectrum sharing challenges only the lack of cooperation described in the previous item is also tackled.

A. Spectrum Sharing in Licensed Bands

In licensed spectrum, there are are primary users who own the licenses to use those bands exclusively unlike secondary users while the opportunistic spectrum access paradigm is called dynamic spectrum access (DSA) and the smart radios with that capability are called cognitive radios (CRs) (*Case-B* in Fig. 5) [34]. 6G provides new opportunities since 6G radios are inherently designed with multi-band operation in mind. Moreover, the expansion into new high-frequency bands which are not deployed everywhere (THz bands) brings forth more possibilities to dynamically access wide bands unused but allocated to other operators. Moreover, ultra massive MIMO can enable coexistence gaps in the space dimension. However, there are also physical layer issues of THz frequency bands affecting CR operation such as propagation impairments and sensing intricacies [35]. It is also challenging to have extremely wide-band operation with intermittent frequency switching, resulting in more complex radio front-ends.

B. Spectrum Sharing in Unlicensed Bands

While spectrum sharing among unlicensed technologies include network technologies such as WiFi and Bluetooth, our main focus is on the case between cellular and unlicensed networks (*Case-A* in Fig. 5) [36].

B.1 LTE-U and LAA

Although LTE networks have long been benefiting from WiFi via data offloading, recent unlicensed LTE proposals [37] suggest using the spectrum of WiFi at 5 GHz rather than the WiFi infrastructure itself. This approach provides a higher spectral efficiency compared to that of WiFi by implementing inter-band carrier aggregation of LTE. There are two flavors of unlicensed LTE, namely LTE-U Forum's LTE-unlicensed (LTE-U) and 3GPP's LAA [7]. The key difference between these LTE variants is that LAA implements a listen-before-talk (LBT) mechanism to avoid colliding with the WiFi networks whereas LTE-U implements duty-cycling toward this goal. Consequently, LAA is worldwide conforming to the regulations whereas LTE-U deployments are only possible in markets such as USA and China where LBT is not mandatory for unlicensed specrum access. An LAA eNodeB performs Clear Channel Assessment based on energy detection before accessing the channel. Hence, LAA is believed to be coexistence-friendly and would share the spectrum fairly with WiFi networks.

B.2 NR-U

In 3GPP Release 16, 5G new radio (NR) based access to unlicensed spectrum, NR-U, is being integrated into the release with both non-standalone and standalone modes of operation in the 5 GHz as well as the new greenfield 6 GHz unlicensed bands [38]. By adhering to LBT requirement for channel access, it will extend the 5G NR access technology to support operation in unlicensed bands [39]. The standardization work listed in [40] covers two primary modes of operation for Licensed assisted access NR-U (LAA NR-U) and standalone. Operation in unlicensed spectrum is dependent on several key principles including ultra-lean transmission and use of the flexible NR frame structure [41].

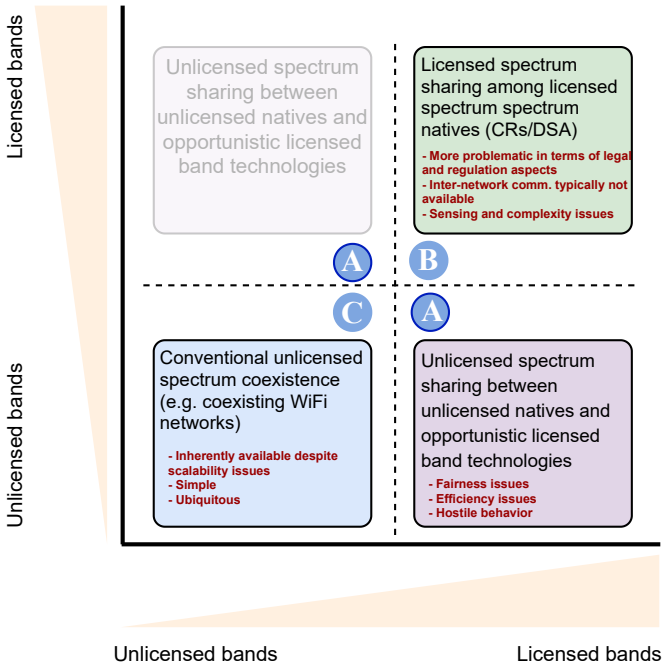

Fig. 5. Coexistence cases of unlicensed and licensed spectrum networks for spectrum sharing.

The first mode, LAA NR-U, is a translation of LTE-U/LAA from 4G LTE to 5G NR for enhancing speed and capacity, following the main premise of spectrum expansion, i.e., aggregating unlicensed spectrum with licensed spectrum [40]. It will support both NR and LTE in licensed spectrum combined with NR-U in unlicensed spectrum. There are basically two deployment options: Using carrier aggregation in a small-cell supporting both licensed and unlicensed spectrum or dual-connectivity of simultaneous macrocell and small cell service where the former connection uses licensed spectrum while the latter uses unlicensed spectrum. The second mode denoted as stand-alone NR-U enables stand-alone operation in unlicensed spectrum without an anchor in licensed spectrum, similar to WiFi operation. The unlicensed spectrum via NR-U will serve various use cases including vertical scenarios with closed local 5G networks (L5GO) (e.g., industrial IoT), wireless broadband access for enterprises and open mobile broadband 5G services in public venues such as concert halls and public gatherings. 5G NR-U in Release 16 is expected to be extended to high-frequencies like 60 GHz in upcoming Release 17 or 18 and further in 6G networks [42].

IV. A TAXONOMY OF COEXISTENCE SCHEMES

Fig. 5 shows a taxonomy of coexistence schemes based on the licensed and unlicensed spectrum utilization in different cases. For coexisting unlicensed networks, there is the apparent spectrum sharing already in place by design, e.g., co-existing WiFi networks (*Case-C* in Fig. 5). This mode is simple and ubiquitously in operation. However, the expected service guarantees for connectivity are challenging to meet. Alternatively, there is the coexistence and then spectrum expansion among licensed

spectrum natives, which refers to the well-known CR concept (*Case-B* in Fig. 5). This is especially challenging due to legal and regulatory aspects. Additionally, it may lead to complexity and sensing issues in operation.

To enable these sharing scenarios, the main apparatus is the coexistence gap: Coexistence gaps are resources left for the other networks and they can be in several domains, namely time, frequency, space, and code [7]. Commonly, frequency domain gaps are implemented: Networks sense the spectrum and select a clear channel which hosts no other network. Thus, colocated networks are separated in operation frequency. LTE-U [37] implements frequency-domain gaps as the first step of its coexistence. But, since spectrum is overly-crowded in dense urban areas, other coexistence gaps are needed. In time domain, coexistence gaps correspond to the time periods when one network leaves the medium for others and then exploited by other systems, e.g., LTE-U duty-cycling in Case-A. Coexistence gaps can be also put in the space domain by careful separation of network footprints, e.g., using cell-shrinking via power control. Moreover, in cell-free network paradigm in 6G, the trajectory, content caching and user association factors will make coexistence gaps much more dynamic in fluid cells [43]. Similarly, a network can create *almost blank spaces* by beamforming toward its receivers while applying interference nulling toward the users of other networks [7]. Given that the massive MIMO is a key component of 5G, space-domain gaps can be widely used. Ultra-Massive MIMO platforms in 6G will provide more flexibility as well as complexity in that regard [44]. Existing schemes create coexistence gaps usually in one of these domains. However, multiple domains can also be exploited for maximizing the spectral efficiency in 6G networks [7].

V. SECURITY IMPLICATIONS OF EXPANSIVE NETWORKS

Although adaptive capacity and flexibility are promising enablers for 6G networks, this paradigm also increases the attack surface for future networks at different layers, e.g., services, network resources and radio spectrum. In this section, we go beyond the spectrum aspect and discuss such security issues from a wider perspective below:

- *Autonomic sharing issues:* Beyond 5G systems are expected to employ cognitive and smart management/control frameworks. In that regard, ETSI Experiential Network Intelligence (ENI) industry specification group (ISG) is defining a cognitive network management architecture using closed-loop AI mechanisms [45]. ITU-T FG-ML5G has recently defined a unified architecture for enabling ML mechanisms in 5G and future networks [46]. However, ML or AI based control has some security and operational challenges like adversarial AI and explainability of autonomous decisions as described in Section VI.B from spectrum expansion perspective.
- *Federated management for global optimizations:* The blurred boundary between different networks calls for more coupled management and meta-optimizations, which may pave the way for high-impact security attacks. The relevant interfaces between tenants and operators enlarge the attack surface for these networks in the control and management domain. The more centralized management schemes may also suffer from availability related threats such as DDoS described below.
- *Confidentiality and integrity challenges due to used infrastructure from other entities:* The confidentiality requirement needs to be satisfied with security and trust mechanisms in expansive networks. Enablers such as E2E encryption, remote attestation for network functions, integrity checks, and hardware security capabilities such as trusted execution environments (TEEs) are promising. For the network edge, efficient and scalable AAA mechanisms are necessary to tackle security threats such as impersonation attacks where a malicious entity can exploit resources or attacks on resource-constrained IoT devices [47]. In that regard, 'proof of transit' (PoT) is another requirement that network operators should meet to fulfil regulatory obligations or policy compliance [48]. Indeed, in many vertical sectors, like energy or healthcare, service providers require that data collected from their network transit in a network geolocated in a precise location (e.g., national e-health data should only transit inside the owner country). This implies that the verticals should be able to verify whether the traffic traversed only through the authorized network nodes or not.
- *DoS attacks on shared resources:* The capability for any network to expand towards other networks' spectral resources inherently entails an attack vector for DoS attacks[1]. Apparently, the threats on availability have become more prevalent in recent years [49]. DoS can occur at different layers starting from application layer with service specific ones down to PHY layer with jamming or control channel overcrowding attacks. However, please note that resource expansion can also be a mitigation technique for networks under attack by switching to external resources for service continuity.
- *Attack surface expansion:* The consolidation of various technologies such as cloud computing, edge networks, function virtualization, software defined networks and slicing increases the dependencies among various components and simultaneously expose the entire network to cyberthreats [50]. Exploited weaknesses of one technology may affect the functioning of the entire network. Adequately crafted attacks exploiting multiple weaknesses of used technologies may be very efficient for adversaries while difficult to identify and mitigate.

VI. DLT AND MACHINE LEARNING FOR REALIZING 6G SPECTRUM SHARING

In this section, we identify and describe two key technologies which are imperative to be more tightly integrated for realizing spectrum sharing in 6G networks towards expansive networks. These are DLT including blockchains [19] and machine learning (ML).

[1] Although there are important DDoS attack vectors for other shared resources such as slices in the core network, in this paper we focus on spectrum resources and radio segment.

A. DLT and Spectrum Sharing

Although the shared use of spectrum has long been considered as an important enabler to mitigate the spectrum scarcity, we have only a few practical examples of shared spectrum use such as citizens broadband radio service (CBRS) and licensed shared access (LSA) which enable spectrum sharing in a well-described and controlled manner. The roadblocks for realizing truly dynamic spectrum sharing and access are not only due to the difficulty of sharing the spectrum in a fine granularity in terms of space and time, but also because of the lack of efficient means of exchange for payment by the spectrum user and service level agreements (SLAs) assurance. The spectrum management is very cumbersome requiring regulatory body's coordination or static agreements between the parties. For example, Italy has introduced for its 5G auctions "the club use concept" which enables the mobile network operators share a license with other operators and use the whole awarded spectrum band when a licensee does not use it on the assigned time and space.

While club-use model is a first step toward DSA, it requires MNOs to build consortia and come into agreements with other MNOs which would limit the spectrum sharing promises to only a few parties. A further step would be to devise a mechanism which lets the MNOs to negotiate effortlessly with any other party who is in need of spectrum and clearing based on the SLAs. Since smart contracts (SC) running on DLTs can automate the process of a service exchange without requiring the parties to a have a priori trust, the MNOs can trade their unused capacity without going through the current cumbersome processes. In addition to an increased spectrum utilization efficiency, the small operators will have lower commercial barriers to entry which is vital for localized deployments envisioned in 6G. Today's envisioned club-use model can also be improved by DLTs, e.g., the trusted third party which is supposed to manage the use of the spectrum and access scheduling can be replaced by an SC. However, one should also consider the emerging challenges with this new approach, e.g., overhead of using the distributed ledger network or the privacy issues. For instance, the storage and computation burden on devices such as IoT, which are generally resource constrained, suffer from complexity challenges, thus limiting their participation in the blockchain network [53].

In addition to feasibility questions, spectrum sharing in 6G scenarios in centralized control frameworks may lead to security and privacy concerns and exposes a single attack target for malicious users. An alternative approach is to use certificates issued by certification authorities to spectrum sharing entities or unlicensed spectrum sharing inside each cell. This approach requires appropriate protocol(s) to be implemented for each cell and security mechanisms to protect any central control point. Furthermore, it causes more computational complexity and traffic overhead (e.g., longer packet lengths to facilitate the protocol exchange), for spectrum sharing systems. Essentially, any such centralized architecture also brings forth single-point-of-failure risks, which may lead to the disruption of the entire spectrum sharing network in case the centralized authority is compromised or out of service [34].

Compared to such conventional spectrum management schemes, DLT is a promising solution to remedy the key issues of security, fairness and performance for spectrum management in future networks [19]. Due to transparency feature, DLT can improve the visibility of spectrum usage and provide auditability of spectrum stakeholders' activity for efficient enforcement of spectrum sharing rules. Similarly, it can ensure tamper-free operation with immutability for supporting spectrum sharing and management schemes as a decentralized database without any single party's control. Accordingly, it envisions to support spectrum management by providing the benefits shown in Table 1 [51].

B. Machine Learning and Spectrum Sharing

ML can operate and alleviate challenges at various layers in 6G wireless networks [54]. At the physical and MAC layers, ML can optimize synchronization, manage power allocation, and modulation and coding schemes [55]. It can also assist with channel estimation and enable adaptive and real-time massive MIMO beamforming, following mobility patterns and dynamic network topology. As a further step, they can provide the joint optimization of the functions in the physical and MAC layers.

Learning-based approaches are instrumental for wireless networks to coexist in a spectrum band especially for scenarios in which the information about the underlying system is either incomplete, e.g., missing channel parameters, or non-existent, e.g., absence of a reliable channel model [7]. In those cases, ML can reveal complex interactions among different system elements and can steer the networks towards an efficient regime [56], [57]. In 6G, these capabilities are of great value especially for spectrum sharing since coexistence cases expected to occur are more heterogeneous and complicated than the current research addresses.

For example, in contrast to simple settings of two co-located networks, there may be a multitude of networks from different operators or highly dynamic cellular coverage due to cell-free networks in a practical environment. There are also unknown or intrinsic parameters which are not evident for spectrum sharing parties. A typical example is the application layer traffic characteristics of one party which are invisible to the other but induces a major impact on the system operation.

Supporting such complex deployments requires adaptive and self-organizing solutions rather than static approaches. ZSM integrated with AI/ML is a promising architectural approach to implement efficient control frameworks to this end [18]. With ML, it becomes viable to develop protocols performing well despite the lack or incomplete knowledge of the underlying system(s). Moreover, to exploit coexistence gaps in many dimensions, we need context-aware solutions that can identify in which domains two systems can share the spectrum with high coexistence efficiency. Radios can make decisions ranging from very fundamental ones such as identifying the occupancy of a channel to more complex ones such as traffic analysis for exploiting spatial coexisting network characteristics.

We categorize the related ML-based coexistence solutions broadly into four as follows [7]:

- *Identification of the neighboring transmitters*: This category of solutions aims at identifying the coexisting networks so that they can adjust their operation parameters accordingly. In particular, technology identification can be

Table 1. DLT and spectrum sharing [51], [52].

DLT capability	**Benefits for spectrum sharing**
Decentralization	The distributed ledger such as blockchains adoption eliminates the need of trusted external authorities for spectrum management. This alleviates the communication overhead wit hthese external entities while also improving system integrity and privacy due to mitigated concerns about data leakage and security compromises caused by third party intermediaries.
Transparency	DLT based spectrum management solutions can inherently provide better visibility and monitoring regarding how, when and by whom the spectrum is used since all transactions between spectrum users and service providers are recorded transparently on distributed ledgers. Furthermore, smart contracts as self-executing functions can provide auditability of spectrum sharing activities and compliance with the pre-defined sharing policies.
Immutability	The spectrum sharing, monitoring or user payment records are stored in the appended blockchain in an immutable manner. By using consensus mechanisms among network members, distributed ledgers are inherently resistant to modifications by malicious users or glitches. The distributed architecture also supports the reliable and accurate operation of the spectrum services.
Availability	With DLT based spectrum management by service providers, access to spectrum resources are open to any network participant and they can transparently perform spectrum sharing and payments in a distributed manner since the spectrum sharing databases are accessible to all entities in the network. Moreover, no central authority is needed to verify or record the data and transactions, which improves the availability aspect.
Permission control	Without a single centralized and trusted entity controlling the network, new users or applications can be added to the ecosystem without seeking the approval of other users. This facilitates a flexible sharing environment. However, this openness can also be limited for more controlled environments using permission-based ledgers.
Security	DLT enables robust communications between spectrum stakeholders, e.g., users, with strong system capabilities against various security threats on confidentiality, integrity and availability.

posed as a classification problem. Classification of interferer provides appropriate actions for the spectrum sharing parties.

- *Identification of the source of the interference*: Similarly, a network should identify the source of interference to react accordingly [58]. Interferer identification is also a classification problem for which clustering or decision-tree based solutions can be used.
- *Identification of the coexisting network parameters*: Here, the goal is to extract more information about the operation parameters of the colocated network.
- *Adaptation to the operation environment*: Identification is typically followed by adaptation in spectrum sharing regimes. For selection of the best parameters, regression schemes serve to estimate the relationships among system parameters and how they interact. A usage of such solution is to estimate a dependent variable through measurements. A typical example is the parameter regression for a spatio-temporal distribution model of coexisting networks to optimize spectrum sharing decisions.

C. ML Challenges for Spectrum Sharing

ML techniques also suffer from some challenges when exploited for ubiquitous spectrum expansion. These issues are essentially related to the realization of ML in a distributed, massive-scale and multi-party system of systems like 6G networks and listed below.

C.1 Performance Issues

The additional overhead of ML functions is an important issue for deploying distributed spectrum sharing functions. As a potential remedy, transfer learning is a technique employed to translate training processing in time and space [59]. The relatively simpler inference is then performed in the operational environment. Moreover, edge computing and smart offloading techniques are instrumental to employ localized data processing and distributed workload in different [60]. The absence of an effective and fair evaluation framework to compare and benchmark different ML driven solutions also hampers accurate performance measurement due to unequivalent data sets, unclear operational parameters impairing replicability and different evaluation criteria [25].

C.2 Trustworthy Inter-network Data Sharing for ML

The inter-network data sharing for training ML models in offline manner is not a straightforward task. There are regulatory and legal issues in addition to technical interfacing hurdles. It is more problematic when one setups online learning models and cognitive functions for spectrum sharing, which require perpetual interfacing and data sharing between different networks. Nevertheless, the operators may be unwilling to exchange proprietary information with their competitors due to business concerns. Additionally, the intention for enabling such a cooperation may face practical and technical obstacles since operators provide differentiated services to their customers, serving objec-

tives that can be substantially different because of their business models [61].

C.3 Adversarial AI

The adoption of ML/AI for various network and service management functions may provide new attack vectors to malicious agents. It has been shown that ML techniques are vulnerable to several attacks occurring at both training and production stages [62]. In the former, also known as poisoning attacks, an attacker tampers the training data using carefully crafted malicious samples with the goal of altering the learning outcome to its advantage. In the latter, an attacker attempts to impair the model's decisions by introducing small perturbations to the consumed instances, i.e., using adversarial examples, at the production stage [18]. Federated learning is vulnerable to poisoning attacks as presented in [63], [64]. Attacks against ML mechanisms may seek to violate either integrity, availability or privacy of ML operation. Attacks on integrity aim to degrade decision performance such as indecision, delayed outcomes and wrong decisions [65]. Similarly, the goal of availability attacks is to increase the classification errors such that the ML system becomes practically unusable. On the other hand, the privacy attacks aim to obtain private information about the ML system, its users or data by reverse-engineering the learning algorithm [66].

C.4 Distributed and Cooperative ML Models

Distributed and cooperative ML models such as distributed AI, shared learning and federated learning, are crucial for higher accuracy and faster learning process of AI/ML models [58]. However, adoption of distributed and cooperative ML models may lead to privacy and trust issues as described in Section V. Specifically, in the edge computing domain, such solutions have to tackle the privacy concerns with appropriate mechanisms letting the model(s) learn from shared spectrum occupancy and network configuration data without compromising the privacy of collaborative network entities. To deal with trust issues, trustworthiness mechanisms that ensure cooperating agents are not malicious are essential. Here, blockchains are promising as illustrated in Section VI.A. In that regard, the integration of blockchain technology with AI in wireless networks for flexible and secure resource sharing can mitigate various privacy and trust issues for efficient spectrum sharing in expansive networks [67].

C.5 Energy Efficiency

The pervasive use of distributed processing for ML and AI for data analytics and control mechanisms will lead to energy efficiency challenges in 6G networks [68]. The huge volumes of network-wide telemetry data in super-dense networks are also to be consumed in order to enable these smart functions. Therefore, the energy efficiency of these operations is imperative not just for energy savings and environment impact, but also for feasibility in 6G network (QoS requirements, processing limitations, etc.) [69]. Tiered and progressive processing of aggregated data streams spatially (from edge to the core) is a potential solution for improved energy efficiency and overcoming processing limitations [70].

VII. CONCLUSION

In this work, we describe our proposed *Expansive Networks* concept for 6G networks to address capacity and scalability challenges. To illustrate this concept, we utilize spectrum resources as a case study. First, we present spectrum sharing in licensed and unlicensed spectrum and relevant possibilities in 6G networks. We then present the security aspect of expansive networks, a major challenge in such open and heterogeneous systems. We also discuss two key techniques, DLT and network intelligence via machine learning, for enabling challenging services and coexistence of diverse networks in 6G. Considering the more diverse and fragmented nature of 6G networks with more stringent use cases and massive connectivity, resource expansion is imminent. Therefore, expansive networks paradigm and the integration of these enablers leading to more efficient capacity expansion are essential.

REFERENCES

[1] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *arXiv preprint arXiv:1909.11315*, 2019.

[2] Y. Chen *etal.*, "From connected people, connected things, to connected intelligence," in *Proc. IEEE 6G SUMMIT*, Mar. 2020.

[3] ITU FG NET-2030, "Network 2030 - A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 And Beyond," ITU FG NET-2030 Whitepaper, 2019, accessed on 05.25.2020. [Online]. Available: `https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf`

[4] DE-CIX - The Deutsche Commercial Internet Exchange, "DE-CIX sets a new world record: More than 9 Terabits per second data throughput at Frankfurt Internet Exchange," DE-CIX Press release 11.03.2020, 2020, accessed on 05.25.2020. [Online]. Available: `https://www.de-cix.net/en/about-de-cix/media-center/press-releases/de-cix-sets-a-new-world-record`

[5] Craig Labovitz, "NOKIA Network traffic insights in the time of COVID-19: April 9 update," Nokia blog entry, 2020, accessed on 05.25.2020. [Online]. Available: `https://www.nokia.com/blog/network-traffic-insights-time-covid-19-april-9-update/`

[6] N. Bhushan *et al.,* "Industry perspective: 5G air interface system design principles," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 6–8, Oct. 2017.

[7] S. Bayhan, G. Gür, and A. Zubow, "The future is unlicensed: Coexistence in the unlicensed spectrum for 5G," *arXiv e-prints*, p. arXiv:1801.04964, Jan. 2018.

[8] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *arXiv preprint arXiv:1902.10265*, 2019.

[9] Z. Zhang *et al.*, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Tech. Mag.*, vol. 14, no. 3, pp. 28–41, July 2019.

[10] S. Mumtaz *et al.,* "Licensed and unlicensed spectrum for future 5G/B5G wireless networks," *IEEE Netw.*, vol. 33, no. 4, pp. 6–8, July 2019.

[11] S. Nayak and R. Patgiri, "6G communication technology: A vision on intelligent healthcare," *arXiv preprint arXiv:2005.07532*, 2020.

[12] F. Jameel *et al.,* "Optimizing blockchain networks with artificial intelligence: Towards efficient and reliable IoT applications," *Convergence of Artificial Intelligence and the Internet of Things,* Springer, Cham, 2020, pp. 299–321.

[13] E. Li, L. Zeng, Z. Zhou, and X. Chen, "Edge AI: On-demand accelerating deep neural network inference via edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 447–457, Oct. 2019.

[14] D. Blomeyer and A.-L. Schulte-Gehrmann, "Surface innovations for interiors of future vehicles," *ATZ worldwide*, vol. 121, no. 6, pp. 48–51, May 2019.

[15] T. Kumar *et al.,* "Securing gadget-free digital services," *IEEE Computer*, vol. 51, no. 11, pp. 66–77, Nov. 2018.

[16] M. Mezzavilla *et al.,* "Public safety communications above 6 GHz: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 316–329, Nov. 2017.

[17] M. Park, S. Lee, and S. Lee, "Dynamic topology reconstruction protocol for UAV swarm networking," *Symmetry*, vol. 12, no. 7, p. 1111, July 2020.

[18] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Network*, vol. 34, no. 2, pp. 186–194, Feb. 2020.

[19] T. Hewa *et al.*, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. IEEE 6G SUMMIT*, Mar. 2020.

[20] N. Gisin and R. Thew, "Quantum communication," *Nature photonics*, vol. 1, no. 3, pp. 165–171, Mar. 2007.

[21] V. Räisänen, "A framework for capability provisioning in B5G," in *Proc. IEEE 6G SUMMIT*, Mar. 2020.

[22] R. Trivisonno, R. Guerzoni, I. Vaishnavi, and D. Soldani, "SDN-based 5G mobile networks: Architecture, functions, procedures and backward compatibility," *Trans. Emerging Telecommunications Tech.*, vol. 26, no. 1, pp. 82–92, Jan. 2015.

[23] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, Mar. 2018.

[24] S. Ayoubi *et al.,* "Machine learning for cognitive network management," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 158–165, Jan. 2018.

[25] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, July 2020.

[26] W. Kellerer, P. Kalmbach, A. Blenk, A. Basta, M. Reisslein, and S. Schmid, "Adaptable and data-driven softwarized networks: Review, opportunities, and challenges," *Proc. IEEE*, vol. 107, no. 4, pp. 711–731, Feb. 2019.

[27] G. Castellano, A. Manzalini, and F. Risso, "A disaggregated MEC architecture enabling open services and novel business models," in *Proc. IEEE NetSoft*, June 2019.

[28] E. Peltonen *et al.,* "6G white paper on Edge Intelligence," *arXiv e-prints*, p. arXiv:2004.14850, Apr. 2020.

[29] G. Gür, "Spectrum sharing and content-centric operation for 5G hybrid satellite networks: Prospects and challenges for space-terrestrial system integration," *IEEE Veh. Tech. Mag.*, vol. 14, no. 4, pp. 38–48, Oct. 2019.

[30] FCC, "Auction 103 Winning Bidders and Incentive Payments," FCC Public Notice 35 FCC Rcd 2015 (3), 2020, accessed on 05.25.2020. [Online]. Available: `https://www.fcc.gov/document/auction-103-winning-bidders-and-incentive-payments`

[31] M. Matinmikko-Blue, S. Yrjölä, and P. Ahokangas, "Spectrum management in the 6G era: The role of regulation and spectrum sharing," in *Proc. IEEE 6G SUMMIT*, Mar. 2020.

[32] C. Han, X. Zhang, and X. Wang, "On medium access control schemes for wireless networks in the millimeter-wave and terahertz bands," *Nano Commun. Networks*, vol. 19, pp. 67–80, Mar. 2019.

[33] Z. Zhou, Y. Jia, F. Chen, K. Tsang, G. Liu, and Z. Han, "Unlicensed spectrum sharing: From coexistence to convergence," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 94–101, Oct. 2017.

[34] F. Hu, B. Chen, and K. Zhu, "Full spectrum sharing in cognitive radio networks toward 5G: A survey," *IEEE Access*, vol. 6, pp. 15754–15776, Feb. 2018.

[35] T. S. Rappaport, *et al.*, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, June 2019.

[36] S. Lagen, N. Patriciello, and L. Giupponi, "Cellular and Wi-Fi in unlicensed spectrum: Competition leading to convergence," in *Proc. IEEE 6G SUMMIT*, Mar. 2020.

[37] J. Zhang *et al.,* "LTE on license-exempt spectrum," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 647–73, Nov. 2017.

[38] 3GPP TSG RAN, "Study on NR-based access to unlicensed spectrum," 3GPP TR 38.889 V16.0.0, 2018, accessed on 05.19.2020. [Online]. Available: `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3235`

[39] N. Patriciello, S. Lagén, B. Bojović, and L. Giupponi, "NR-U and IEEE 802.11 technologies coexistence in unlicensed mmwave spectrum: Models and evaluation," *IEEE Access*, vol. 8, pp. 71254–71271, Apr. 2020.

[40] L. Casaccia, "3GPP commits to 5G NR in unlicensed spectrum in its next release," 2018, accessed on 05.25.2020. [Online]. Available: `https://www.qualcomm.com/news/onq/2018/12/13/3gpp-commits-5g-nr-unlicensed-spectrum-its-next-release`

[41] J. Peisa *et al.,* "5G evolution: 3GPP releases 16 & 17 overview," *Ericsson Tech. Review*, vol. 9, no. 2020, pp. 1–5, 2020.

[42] 3GPP TSG RAN, "Study on New Radio access technology; 60 GHz unlicensed spectrum," 3GPP TR 38.805 V14.0.0, 2017, accessed on 05.19.2020. [Online]. Available: `https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3154`

[43] F. Tariq *et al.,* "A speculative study on 6G," *arXiv e-prints*, p. arXiv:1902.06700, Feb. 2019.

[44] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Towards 6G Networks: Use Cases and Technologies," *arXiv e-prints*, p. arXiv:1903.12216, Mar. 2019.

[45] ETSI Experiential Networked Intelligence Industry Specification Group (ENI ISG), "Experiential Networked Intelligence (ENI); System Architecture," ETSI GS ENI 005 V1.1.1 (2019-09), 2019, accessed on 05.19.2020. [Online]. Available: `https://www.etsi.org/deliver/etsi_gs/ENI/001_099/005/01.01.01_60/gs_ENI005v010101p.pdf`

[46] ITU-T FG-ML5G, "Y.3172 : Architectural framework for machine learning in future networks including IMT-2020," ITU-T SG-13 Recommendation Y.3172, 2019, accessed on 02.19.2020. [Online]. Available: `https://www.itu.int/rec/T-REC-Y.3172-201906-I/en`

[47] P. Bellavista *et al.,* "A survey on fog computing for the Internet of things," *Pervasive Mobile Comput.*, vol. 52, pp. 71–99, Jan. 2019.

[48] F. Brockners, S. Bhandari, T. Mizrahi, S. Dara, and S. Youell, "Proof of Transit," Internet Engineering Task Force, Internet-Draft draft-ietf-sfc-proof-of-transit-04, Nov. 2019, experimental. [Online]. Available: `https://tools.ietf.org/html/draft-ietf-sfc-proof-of-transit-04`

[49] M. Özçelik, N. Chalabianloo, and G. Gür, "Software-defined edge defense against IoT-based DDoS," in *Proc. IEEE CIT*, Aug. 2017.

[50] ENISA, "ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis ," ENISA Technical Report, 2020, accessed on 20.10.2020. [Online]. Available: `https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis`

[51] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. Cognitive Commun. Netw.*, vol. 5, no. 2, pp. 193–205, June 2019.

[52] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Network Comput. Applicat.*, vol. 166, p. 102693, Sept. 2020.

[53] H. Xu *et al.,* "Blockchain-enabled resource management and sharing for 6G communications," *Digital Commun. Networks*, vol. 6, no. 3, pp. 261–269, 2020.

[54] S. Ali *et al.,* "6G white paper on machine learning in wireless communication networks," *arXiv e-prints*, p. arXiv:2004.13875, Apr. 2020.

[55] H. Ye, G. Y. Li, and B. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 114–117, Sept. 2017.

[56] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2224–2287, Mar. 2019.

[57] O. Simeone, "A very brief introduction to machine learning with applications to communication systems," *IEEE Trans. Cognitive Commun. Netw.*, vol. 4, no. 4, pp. 648–664, Nov. 2018.

[58] W. Ning, X. Huang, K. Yang, F. Wu, and S. Leng, "Reinforcement learning enabled cooperative spectrum sensing in cognitive radio networks," *J. Commun. Networks*, vol. 22, no. 1, pp. 12–22, Mar. 2020.

[59] Z. Li, Z. Xiao, B. Wang, B. Y. Zhao, and H. Zheng, "Scaling deep learning models for spectrum anomaly detection," in *Proc. ACM MobiHoc*, July 2019.

[60] N. Kiran, C. Pan, S. Wang, and C. Yin, "Joint resource allocation and computation offloading in mobile edge computing for SDN based wireless networks," *J. Commun. Networks*, vol. 22, no. 1, pp. 1–11, 2020.

[61] B. Singh *et al.,* "Coordination protocol for inter-operator spectrum sharing in co-primary 5G small cell networks," *IEEE Commun. Mag.*, vol. 53, no. 7, pp. 34–40, July 2015.

[62] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar, "Can machine learning be secure?" in *Proc. ACM ASIACCS*, Mar. 2006.

[63] D. Preuveneers *et al.,* "Chained anomaly detection models for federated learning: An intrusion detection case study," *Applied Sciences*, vol. 8, no. 12, p. 2663, Dec. 2018.

[64] A. Nitin Bhagoji, S. Chakraborty, P. Mittal, and S. Calo, "Analyzing federated learning through an adversarial lens," *arXiv e-prints*, p. arXiv:1811.12470, Nov. 2018.

[65] Y. Han *et al.,* "Reinforcement learning for autonomous defence in software-defined networking," in *Proc. GameSec*, Sept. 2018.

[66] B. Biggio *et al.,* "Poisoning behavioral malware clustering," in *Proc. ACM AISec*, Nov. 2014.

[67] Y. Dai *et al.,* "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Network*, vol. 33, no. 3, pp. 10–17, May 2019.

[68] T. Taleb *et al., White paper on 6G networking*, June 2020.

[69] S. Wang *et al.,* "When edge meets learning: Adaptive control for resource-

constrained distributed machine learning," in *Proc. IEEE INFOCOM*, Apr. 2018.

[70] A. M. Al-Salim, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient big data networks: Impact of volume and variety," *IEEE Trans. Network Service Manage.*, vol. 15, no. 1, pp. 458–474, Dec. 2017.

Gürkan Gür is a Senior Lecturer at Zurich University of Applied Sciences (ZHAW) – Institute of Applied Information Technology (InIT) in Winterthur, Switzerland. He received his B.S. degree in Electrical Engineering in 2001 and Ph.D. degree in Computer Engineering in 2013 from Bogazici University in Istanbul, Turkey. His research interests include future Internet, information security, and information-centric networking. He has two patents (one in USA, one in TR) and published more than 80 academic works. Currently, he is involved in EU H2020 RIA – INSPIRE-5Gplus project. He is a senior member of IEEE and a member of ACM.

APPENDIX

Table 2. Acronyms and their explanations.

Acronym	Definition
5G NR	5G new radio
AAA	Authentication, authorization and accounting
AI	Artificial intelligence
CAPEX	Capital expenditures
CBRS	Citizens broadband radio service
COVID-19	Coronavirus disease - 19
CR	Cognitive radio
D2D	Device-to-device
DAI	Distributed AI
DLT	Distributed ledger technology
DoS	Denial of service
DSA	Dynamic spectrum access
ELPC	Extremely low-power communications
ERLLC/eURLLC	Enhanced ultra-reliable, low-latency communication
E2E	End-to-end
FCC	Federal Communications Commission
FeMBB	Further enhanced mobile broadband
IoE	Internet of everything
ITU	International Telecommunication Union
LAA	Licensed assisted access
LBT	Listen-before-talk
LDHMC	Long distance high-mobility communications
LSA	Licensed shared access
LTE	Long term evolution
LTE-U	LTE-unlicensed
M2M	Machine-to-machine
MAC	Media access control
MEC	Multi-access edge computing
MIMO	Multiple input multiple output
ML	Machine learning
MNO	Mobile network operator
OPEX	Operational expenditures
OTT	Over-the-top
PHY	Physical
PoT	Proof of transit
RAN	Radio access network
SC	Smart contracts
SLA	Service level agreement
TEE	Trusted execution environment
UAV	Unmanned aerial vehicle
umMTC	Ultra massive machine type communication
VLC	Visible light communications
VNF	Virtual network function
XR	Extended reality
ZSM	Zero touch network and service management