The Evolution of Networks and Management in a 6G World: An Inventor's View

Gerald M. Karam, *Senior Member, IEEE*, Markus Gruber, Iris Adam, François Boutigny, Yoan Miche, and Sarit Mukherjee, *Senior Member, IEEE*

***Abstract*—The onset of the 6G era in telecommunications, touted to launch in 2030, is hoped to serve many masters and deliver an unparalleled improvement in capabilities, applications, intelligence, and indeed liberate human potential. The vision of 6G incorporates new radio frequencies and technologies, the integration of sensing, cognitive methods defining both network functions and their management, and new networking approaches for a broader scope of applications and distribution. The challenges for inventors lies in both physical devices and a substantive improvement in the development of functions implemented by, and managed, with software. The algorithms (including dynamic solutions based on Artificial Intelligence and Machine Learning), protocols, and architecture evolutions will bring together the most advanced software systems ever imagined for telecommunications. Yet, the business of companies building and operating these next generation platforms requires a huge investment, and 6G will exceed all others with its breadth and complexity. This paper outlines one possible timeline of technological impact based on the pace of invention, investment, global context, and the broad goals of 6G. From this, follows a vision of the critical methods in automation, security and networking that we believe will be central to bringing the dream of 6G to a reality.**

***Index Terms*—6G, artificial intelligence, distributed systems, intent-based networking, machine learning, network automation, orchestration, network slicing, IoT, security, data privacy, resilience, security monitoring, software supply chain security, intrusion detection.**

I. Introduction

THE VISIONING of 6G and the future it will bring, is as broad as it is ambitious. Numerous reports (e.g., [1], [2], [3], [4], [5]) suggest 6G will enable a better society and bring in communications everywhere, substantial energy reductions, intelligence everywhere, and innumerable innovative applications. It could be an important part of the remedy for many global challenges and launch us into the futuristic imagined by the 1960s *Jetsons* cartoon. Discussions regarding 6G speak of 2030 (for both ITU-R and 3GPP standards work [4], [6]) as the opening edge of 6G deployment, implying that principal technologies that differentiate 5G from 6G will become available in production quantity and quality, as well as a financial investment appetite for the new world.

Progress will be paced by the degree to which technology can be advanced from invention to general availability, and the level of investment that will be needed, to displace older technology, embrace new technology, and meet business needs. For example, a news article from the Mansfield News-Journal in April 1963 [7] touted a pocket-sized mobile phone that took another 20-30 years to become practical, and it took marketing innovation (for example unlimited minutes, followed by unlimited data) to make it affordable to accelerate demand. Ultimately the introduction of the "smart phone" added fuel to that fire. Similarly, the roll out of 4G/LTE took 10+ years, and in the end ran into capacity limits in dense urban areas because of the affordability and complexity of small-cell deployments. 5G trials occurred in 2018 but many companies are still procuring and launching 5G Standalone (SA) in 2022 – rollouts and upgrades will likely continue through 2030 (5G Advanced is due in 2024, and for some it will arrive in the middle of a buildout of 5G SA).

Building the future of 6G in the next 10-20 years begins with inventions that are in the lab (universities, industry, government) today and into the near future since the path to commercialization is long. Some ideas will take more than the 2030s to deliver. Will they be part of a 7G or a longer 6G evolution?

While the 6G era will introduce new radio technologies, frequency uses, and the hope of a greater range of enriching applications in the "anytime, anywhere" experience, the magic behind it will be increasingly sophisticated and intelligent software to securely orchestrate and automate network functions and applications in general, with underlying network technologies.

As inventors of telecommunications technologies that will enable 6G and beyond, we are challenged with implementing automation to a complex distributed, multi-stakeholder set of interlocking networks. New approaches will be needed for intent programming across a wider range of domains, cognitively driven orchestration and assurance based on data fusion and techniques from Artificial Intelligence (AI) and Machine Learning (ML), and end-to-end (E2E) performance guarantees, at scale.

Security will need new attention in 6G: *Context* – allowing security to be applied in context of different networks and subnetworks [4] so that localized intelligence can monitor and govern allowable behavior; *Assurance:* techniques to ensure

Manuscript received 21 February 2022; revised 23 June 2022; accepted 24 June 2022. Date of publication 4 July 2022; date of current version 31 January 2023. The associate editor coordinating the review of this article and approving it for publication was H. Lutfiyya. *(Corresponding author: Gerald M. Karam.)*

The authors are with the Network Systems and Security Research Lab, Nokia-Bell Labs, Murray Hill, NJ 07974 USA (e-mail: gerald.karam@nokia.com).

Digital Object Identifier 10.1109/TNSM.2022.3188200

that security is preserved across context boundaries, and resilient to technical innovations; and *Privacy* – protecting new data sources from 6G sensing in addition to traditional communications, as well as collected measurements, and models.

Network system innovations will be central to flexibility and dynamic network capabilities in the 6G era. Key topics include: seamless mobility in an all-IP network; intelligent network selection – where the UE can best make a decision on network access; network-assisted service creation – where the network will readily provide key functions to build different classes of applications; ad hoc networking among UEs – to allow for highest bandwidth communications without complex core networks; and finally improved support for communications across multiple providers, with consideration of peering at edges and far edges.

The remainder of this paper will paint our vision of when the future will unfold and the network system management challenges that need addressing. The next section will present the broader 6G landscape and imagine a roadmap driven by the arrival of technologies, and the investment to deploy. The third section will explore orchestration and automation, cognitive capabilities, architecture and questions arising from distributed networks, where compute, networks, administrative domains, radio and people intersect from many different points. Section IV will discuss the enhancements to security for 6G automation. In Section V we provide explore network systems improvements we envision. Finally, Section VI presents our path forward on research and interactions with the broader community.

II. The Landscape

The opportunities in 6G suggest an expansion in scope for coverage and a distribution of communications processing that is well past the 5G experience. With the potential of THz (90 GHz to 300 GHz) hot spots in the home, factory, and businesses, extreme massive mMIMO, and broad distribution of mmWave and THz endpoints from Communications Service Providers or (CSPs), the level of data processing and distribution will be orders of magnitude higher than a traditional sub 6 GHz 5G macro cell network. (Multiple Service Providers (MSPs) also known as cable providers, often own macro cell assets, so they are included with CSPs in this one regard.) As these radios are extended into enterprises, public spaces, and homes, how will information processing, applications, and data management operate? The players are undetermined; traditional CSPs, MSPs, and Hyperscaler cloud providers are natural candidates, but 10-20 years is a long time in the telecommunications domain, and new entrants (such a Web3.0 distributed service providers such as Helium [8]) could disrupt the business landscape. For example, with the home, a network of THz hotspots that are backhauled by THz fixed wireless or fiber, suggest bandwidth and application experiences out of a science fiction movie, such as potentially holographic image generation and immersive video. Point-to-point THz communications between user equipment (UE) will allow new application experiences and operate outside of the control of service providers altogether. What edge technology can we imagine on what is today a simple residential gateway.

Service providers purchase licensed spectrum to manage central control of a scarce commodity and derive revenue from it. As we move to 6G this will still likely be handed by government auction, but if there is a desire for greater ubiquity as a government policy, then conditions on license holders may increase, or be directly subsidized by governments – e.g., in rural or underpopulated areas. A second influence will be the degree of unlicensed spectrum that can be reserved for private (e.g., industrial, or even in home) use. More private use especially among higher frequencies where interference due to propagation is less likely and antenna power can be reduced for confined areas, a proliferation of deployment will be encouraged. A third consideration for applications will be the available bandwidth in sub-THz frequencies due to contention with passive satellite use [9], [10]; in essence a contiguous bandwidth limit of 12.5GHz above 100 GHz that will prevent the goal 6G speeds of 1Tbps from being achieved with a single contiguous band. It may be possible with regulatory changes to alter this restriction (such as using dynamic bandwidth allocation [9]), or other techniques like carrier aggregation, but without some action, this limit may impair the full range of sub-THz outdoor fixed wireless service, or some applications that may demand extraordinarily high data rates.

The 3GPP forum which is driven largely by service provider interests and the companies that provide their solutions, leans towards embracing central control, even though disaggregation of specific network elements is embodied as a key design rule. This latter idea is present for two reasons: (1) to recognize the need to distribution of some functions for performance and economic reasons, and (2) to give the opportunity for buyers to multi-source different implementations for economic savings (e.g., the separation of the Radio Access Network (RAN) and the core mobile network function (Core) is an obvious purchasing division). With ubiquitous communications as a long-term 6G goal, service provider-based communications services are likely to be complemented with a distributed and collaborative model, perhaps even as to how wireless use is billed.

III. Architectural Challenges

Higher data rates, even for sub 6GHz frequencies (afforded by improved antennas and algorithms), will require more processing closer to the remote radio head. With virtualized RAN (vRAN) implementations, this could imply expansions in place, but for fixed hardware solutions, a retrofit may be needed. Greater distribution is also a possibility because some 5G installations will employ a limited use of far edge platforms, so rebuilding to accommodate greater data processing and to break out to IP networks is likely. In the 6G architecture we can re-imagining the splits between RAN-CORE network functions moving the 6G architecture to support models were computing at the edges network are blends of both radio and

core operations [11]. The scale of vRAN in 5G, and its architecture may successfully deliver the data rates and capacity of the envisioned 5G deployments but may be inadequate for 6G. Specifically deployments will need to address much higher data capacities, more stringent latencies and the proliferation of access that is anticipated with 6G, including the introduction of some THz radio services.

Sensing capabilities are expected to be introduced in next generation of radios to provide context data beyond GPS-quality location, to provide more nuances about the signal environment (indoor, outdoor, level of interference, environment conditions affecting signal). With THz radios considerable human body information can be garnered, and there are a variety of applications under study [12]. With sensing as an expanded application domain in 6G, there will be accompanying questions on how the data is funneled, processed, and secured, especially given the potential to do centimeter resolution positioning, or physical body measurements.

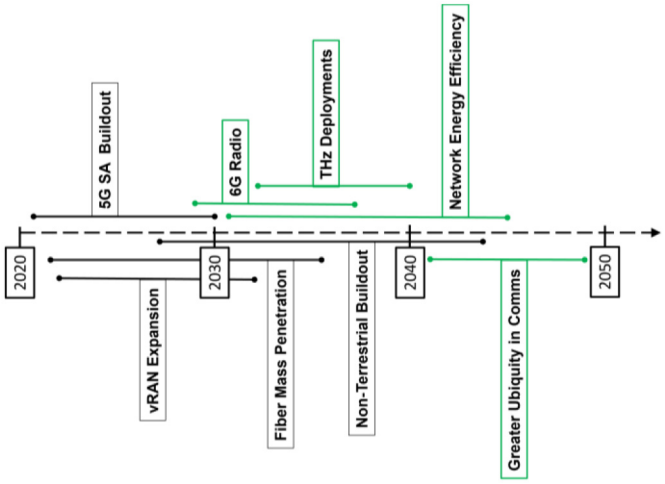

Fig. 1. Estimated Deployment Timelines.

IV. External Factors

The introduction of 6G and any related applications will happen in the context of other major world trends and events. Below are two that may affect the degree to which 6G expansion will race or crawl over the next 2-3 decades. These factors won't likely affect the architecture but may force prioritizing when services and equipment that are deployed.

Climate Change: The weather trends in the foreseeable future are going to worsen while the necessary investment in energy reduction (a 6G goal) slowly takes place. Looking only at North America in the last few years and notably 2021, the number of disaster-producing hurricanes is increasing, the wildfires and other natural disasters, are more commonplace. These events divert public monies and the time/energy of enterprises to repair facilities and support employees and communities. According to the NOAA, U.S.$145B alone was attributable to climate disasters in 2021, the third most costly year [13]. On the horizon are the rising ocean levels that will disrupt economic activity along coastlines (e.g., Miami [14]). Imagine the huge investments in 5G facilities in these areas in 2020-2030, followed by 6G in 2030-2040, only to start getting wiped out 10 years later. CSPs need to consider this carefully as they plan future deployments [15].

COVID-19 and Future Pandemics: COVID-19 taught the world a hard lesson in terms of global teamwork, disaster management, science versus politics and economic hardship. The financial investments made in 2020-22 to weather this virus will weigh on the budgets and debt of countries and companies for many years into the future. Continuing infections will readily build strains that will take more resources to combat. New investments needed for 6G deployment, especially where public sector involvement is required, are going to be tempered by available funding not allocated for pandemic repayment and new costs.

V. Framing the Future

Figure 1 portrays at a 30-year horizon and shows estimates for timelines based on experiences working with large service providers and their investment patterns, expected 6G applications, and common innovation trends. Below are some explanations for the estimates on the graph, and their impact. Note: primarily 6G driven factors are shown in green.

5G SA Buildout – until 2030: The long-term build-out of 4G/LTE took around 10 years across the globe. In 2022 there will be major CSP that are just beginning 5G SA deployments. Furthermore, during this time window 5G Advanced will progress with additional features. Network slicing will expand as 5G SA is more established and CSPs grow network slicing and Enterprise's investment in Industry 4.0 and other domains. This will be a precursor to factory use of 6G, but also delay 6G investment while recent factory capital investments age.

vRAN Expansion, 2024-2032: vRAN will take time to displace traditional baseband hardware units that are deployed from 4G, 5G sub-6 GHz, and the first years of 5G SA deployments. The energy efficiency of vRAN will have to improve markedly before the investment cost and operations costs of very large-scale radio networks will be as affordable as their hardware versions have been.

RAN improvements in 6G will need to exploit virtualization because of the demand for intelligent radios (e.g., based on AI/ML [4]) or more flexibly deployable. Energy costs of radios and associated equipment are a substantial operating cost for CSPs, consequently unit energy costs are critical to manage. Furthermore, edge computing sites will be cautiously built out, since operating costs without committed business demand (for example from enterprises and slicing), slows deployment.

Fiber Mass Penetration, 2025-2035: Much of the urban and suburban landscape of consumer residences is still served by hybrid-fiber coaxial (HFC) cable. While improvements in performance and technology will deliver greater capacity, these will not compare to (near)-optical speeds to the home, which will be a prerequisite of new generations of applications enabled by THz radio endpoints. When the demand for future speeds is not achievable by HFC, MSPs will push fiber ever

closer to the home, and CSPs will build out only fiber. Both can explore THz fixed wireless to residences as well.

6G Radios (*Tower Refit), 2028-2035:* 6G will start with antenna improvements and the corresponding radio processing functions, even as 5G continues operation. This will deliver immediate benefits as 5G Non-Standalone did for CSPs. The sub-6 GHz radios will get upgrades first and then mmWave radios will follow. The continued buildout of macro cell mmWave radios in 5G or 6G will be driven be economics. As 6G antennas begin to replace legacy 5G antennas, sensing features may start to become available. Software and security methods to manage this data will need to be in place before it can be safely enabled.

THz Deployments, 2034-2040: THz radios in select domains will be deployed. Technology improvements will evolve packaging and incorporation into existing towers where appropriate. Services such as THz fixed wireless, may arrive earlier to deliver competitive local access.

Radios in homes for high-speed coverage and futuristic applications will emerge (imagine immersive or holographic video with high demands for untethered bandwidth). Similar capabilities will arrive in handsets (including peer-to-peer links), the office, the factory floor. Vehicles have a long lead time for design and auto manufacturers are scrupulously cautious about added costs. Given the very long lifetimes of vehicles in many parts of the world, THz radio use will lag for Vehicle-to-Vehicle or Vehicle-to-Infrastructure use cases. Yet these new radios will provide the best information sharing between vehicles on a point to multipoint basis for future autonomous and safer human-driven operation. Network services at the far edges of use, in vehicles, home, and factories, will elicit new demands from management software.

Non-Terrestrial Buildout, 2026-2044: Establishing Low Earth Orbit (LEO) satellite networks and alternate air/space-based communications platforms will expand over many years because of the enormous costs, launch vehicle requirements, and slowly emerging demands. Yet, to fulfill the goal of ubiquitous communications, and avoid massive investment costs to deliver data services to more remote locales, including ships and planes, space-based platforms will be essential. Integrating network services across these many disparate platforms will be critical.

Network Energy Efficiency, 2030-2045: The deployment of 6G services will involve slowly maturing technologies that initially (like vRAN in 5G) that may have less energy efficiency than desired. Innovation will be needed to reduce the energy footprint to help combat climate change and increase affordability of this large highly distributed system, dominated by computationally expensive AI/ML components. While as an industry we constantly strive to improve energy efficiency, at least as a cost reduction component, 6G will potentially introduce enough change to drive renewed demand for energy savings and new approaches.

Greater Ubiquity in Communications, 2042-2048: The aspiration of ubiquity will likely unfold in the 2040s decade, with the advent of established non-terrestrial communications platforms, large 6G terrestrial footprint, lower costs of operation, and reduced energy costs. It will take a confluence of successes to deliver this goal.

VI. Network and Service Automation in Multi-Stakeholder Environments

A. Highly Modular Architecture

In order to approach the changes needed in a 6G system when it comes to automation, it is instructive to have a look at the trajectory we have been on from 4G to 5G, an evolution that was characterized by modularization. For instance, 5G introduced novel service and device classes with very heterogeneous requirements to user traffic versus signaling traffic. Hosting all these disparate classes on the same system required that the dimensioning of user plane and control plane traffic was made independently scalable and thus more modular. Highly modular systems have outlasted non-modular alternatives in the history of technology: UNIX is a highly modular system that still prevails in a derivative form in our Android smartphones over 50 years after its invention; the disaggregation of software offerings from hardware offerings in the 90s by Microsoft offered additional modularity and triggered diversification in the sector; and the introduction of app stores giving third parties the opportunity to make their specialized offers part of a larger platform unleashed a cascade of innovations at an astonishing depth. Note: the focus on 6G architecture presented here is not the total consideration, but largely focused on automation. A wider range of issues that fall under architecture are illuminated, for example, in [11].

It is fair to assume that the trajectory toward more modularization that we have been on from 4G to 5G will continue to point us to an even finer level of modular granularity and an even larger scope in terms of modular components. The driver behind this continuation will be the ever-more demanding requirements of 6G: Whereas 5G is already able to cater for high reliability and low latency, it will still confront us with trade-offs to make between these two requirements. 6G, on the other hand, is expected to provide both ultra-high reliability and ultra-low latency in a seamless and ubiquitous manner with no restricting compromises between the two. For this to become a reality, 6G will have to intrinsically incorporate additional components: If the experience is supposed to be ubiquitous we cannot afford to exclude the notion of mutually shared multi service provider networks or non-terrestrial networks; and if the experience is supposed to be seamless, we cannot exclude compute and storage resources offered by cloud service providers, nor can we ignore the emergence of networks that are networks in their own right such as private networks, in-vehicle networks or body area networks.

6G will feature a comprehensive, distributed orchestration opportunistically integrating all these disparate ingredients with no distinction between service provider, enterprise, and IT infrastructure. This includes the ability to deal with the complexity of discovering and controlling highly disaggregated and distributed resources in an abstract and cooperative way and to charge services across a variety of stakeholders in a coordinated manner. This will ultimately lead to a more comprehensive and powerful network that is able to cater

for the ubiquitous and seamless experience of applications described above.

In this context stakeholders can be service providers of any sort (communication or cloud) or enterprises. For instance, a user may spontaneously want to run a very high-bandwidth application with very low latency constraints at a random location. For 6G, we assume that there is no strict affiliation of the user to a single communication service provider and a single cloud service provider; the necessary networking and compute capabilities would rather be compiled on demand depending on availability. Applications in remote areas may require the support of a non-terrestrial network while applications in dense urban areas may benefit from the availability of idle cloud resources in the immediate vicinity. Just like Google Maps finds you all hotels in the neighborhood regardless of the chain they belong to, this kind of openness offers obvious advantages for the user.

From an automation perspective, three things need to happen to make this a reality (Figure 2): First, the interfaces between multi-stakeholder controllers need to be defined and their interaction needs to be optimized. Second, the interworking between communication service providers and cloud service providers needs to be designed in a way that cloud service provider platforms can easily be enriched by proprietary features, akin to apps in an app store, thus opening the door to novel innovation opportunities. Third, full scalability of automation solutions needs to be ensured for, typically smaller, enterprise environments where the 6G system needs to be truly plug-and-play as enterprise customers often do not have the resources nor the expertise to entertain planning and optimization teams as communication service providers do.

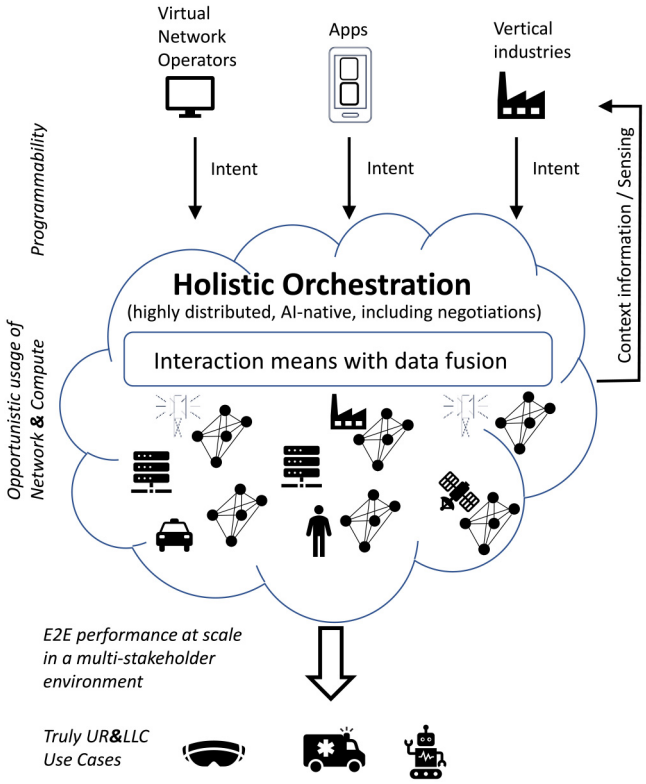

Fig. 2. Holistic orchestration across network and compute domains of disparate stakeholders with generic, bi-directional intent interfaces and AI-native interaction means.

B. Bi-Directional Intent Interfaces

The trajectory described above has not only been one of increasing modularization, but also one of increasing abstraction. Virtualization has been a guiding principle for both cloud service providers and communication service providers alike with containerization providing additional finesse during the last decade. Cloud service providers were even able to go one step further in their abstraction by introducing the serverless concept, which essentially abstracts the inner workings of the compute engine and lets the user focus on what they intend to do. This intent-based approach and serverless mindset has not unfolded its full impact on the telecommunications community yet, mainly because of the relative complexity of large-scale end-to-end networks in comparison to cloud computing resources.

However, we can expect 6G to catch up in this respect and to offer generic intent interfaces that are intuitively accessible not only to communication service providers, but also to virtual network operators, private network owners, and third parties such as startups focusing on niche specializations or even individuals. Apps as we know them from the stores on our smartphones will no longer be limited to influencing compute and storage resources in the cloud but will also be able to influence the configuration of their pertinent virtual networks. Thanks to this additional degree of freedom, this will have the potential to further disrupt the ecosystem and trigger a second cascade of innovations since the very introduction of app stores.

Moreover, intent interfaces can be bidirectional [16], not only providing the intent as such, but also feeding back sensing information of various sorts from the network. Making this network-related information available not only to the network operator, but also to other users from possibly other sectors, and enabling them to access these data in a consumable way will again increase the innovation potential. Intent interfaces will enable anyone to receive comprehensive and actionable feedback from the system, enabling the intent's owner to modify, refine, withdraw or replace the intent. They will also be adaptable to the user's background, able to raise unforeseen impact, and able to continuously improve the network state thanks to AI-based monitoring. Development-Operations (DevOps) will continuously exploit available data streams and will thus enable several network configuration changes a day in highly distributed environments. In this context, network digital twins will provide safe environments for continuous testing of new network states while still fully preserving the system reliability.

C. Distributed Intelligence

AI has become a sine qua non in telecommunications research during the last years. However, there are some related network-specific challenges that must not be underestimated. Unlike Hyperscalers which, with their largely centralized data

centers, literally have "big data" at a few locations to be processed, the telecommunications sector features highly distributed networks where data is typically in many locales. In fact, getting data from various places in the network to a common processing location is costly as it consumes precious network transmission resources. As a result, we often have only scarce data to feed AI engines.

Transfer learning, a research field in machine learning, is predestined to address this challenge as it allows us to transfer knowledge from a somewhat similar situation elsewhere in the network to a given new local situation, e.g., by freezing certain layers of a neural network while re-training others. It has proven to be very useful for telecommunication use cases since it allows us to deal with optimization use cases that rely on relatively rare events, as for instance mobility robustness optimization relies on handover events, whose collection is time-consuming by nature [17]. The ability to make efficient decisions using "small, localized data" will be key to a proactive and highly dynamic network behavior. In telecommunications research in general, transfer learning is currently in its infancy, but we can plausibly assume that it will take a much more prominent role in 6G.

A second challenge in our sector is that AI-based solutions currently focus on specific use cases and cannot be readily reused for other use cases. This manual tailoring completely contradicts the modular design principle of 6G and is also a considerable obstacle on the path toward more automation. We therefore need a data- and AI-native design of 6G with multi-stakeholder interaction means between disparate modules, where the learning can take place at different modules at different times in the network. This interaction means may span from the central cloud to the ultra-far edge with varying hardware capabilities, while data fusion and learning will happen across several collaborative or hierarchical layers of learners. The closest we already are to this interaction means in terms of current standards, is the integration fabric in combination with data services in the ETSI ZSM architecture [18]. Thus, the interaction means can, for example, provide a holistic view of the overall network status across different communication service providers, anticipate the availability of resources, and allow for a differentiated selection of networking capabilities from individual providers. In yet another example, the data fusion of networking data and industrial production data will let us anticipate the optimal selection of networking and cloud resources for an imminent production step as described in the following paragraph.

The third aspect to consider is more of an opportunity than a challenge: 6G will be a key enabler of innovation in vertical industries such as Industry 4.0 production environments. First seed research demonstrates that making networks production-aware can come with significant benefits [19] and we expect 6G to exploit these kinds of external data sources through appropriate interfaces. In this regard, so-called asset administration shells [20], a key component of the Industry 4.0 architecture, may be instrumental to ensure integration across system boundaries and interoperability across value chains, by exposing data. Conversely, asset administration shells may also be used to consume data from the network, in line with the bidirectionality of the intent interface described before.

D. Conflict-Free Fabric of Multi-Stakeholder Control Loops

The distributed intelligence will transform a given intent to a corresponding invocation of a distributed, conflict-free fabric of local decision-making points, or control loops, eventually leading to the right composition of resources and services. This fabric can comprise a massive number of multi-stakeholder networks and network functions representing a service mesh with end-to-end resource discovery. This entails interfaces between different administrative domains enabling the communication of control loops across domains and orchestrators negotiating with each other at a peer-to-peer level. The network and compute fabric will build on the entire spectrum from central cloud to ultra-far edge resources across many different providers, including intent-to-resource mappings within domains as well as service level agreement negotiations between domains.

What will also significantly enhance the innovation potential of 6G are in-system interfaces that allow existing solutions, whether those are cloud service provider solutions or open-source solutions, to be easily extended by proprietary features, similarly to what was described above for the intent interfaces. These features can then address niche needs that will otherwise likely not be addressed at all.

VII. Security & Privacy

Future 6G networks will foster many innovations and security will be at the heart of its design, ranging from use cases, management services, business models, architectures, to technological enablers.

Such innovations essentially revolve around performance (e.g., reaching low latency and high reliability at the same time), intent based networks, a pervasiveness of AI/ML and associated data, expansion to new stakeholders like industry verticals and enterprises as communication service customers of 6G telecommunication networks, devices, systems and networks and agility in software development, to better support growth.

We expect Robustness, Resilience, Trust, Monitoring and Privacy to underpin any 6G innovation. These needs are outlined in the three research directions below.

A. Data Privacy and Security

Given that data is at the heart of everything (whether control or user data) already in 5G networks, the promise of acquiring, processing, monetizing and overall using entirely new types of data in 6G, makes the topic of data security and privacy simply daunting: body area networks able to collect human characteristic data (environment and physiological) are just one example of novel types of data that creates privacy requirements never seen before. In this regard, the aspect of being able to bring a notion of control to the data producers (be they consumers or machines, entities), is paramount. Providing means of data anonymization through privacy-preserving technologies, data processing using advanced cryptographic solutions

such as homomorphic encryption platforms for machine learning, are just some examples of means that allow some finer grained control over privacy sensitive data use, compared to the current full-blown data collection and exploitation.

One such means of control is anonymization (going as far as total obfuscation, e.g., through encryption mechanisms), which can be imagined to be adequately tuned depending on the sensitivity of the data, and the need for direct access to raw data. Being able to objectively measure data utility and privacy, for a data and process, allows for proper selection of the anonymization or obfuscation scheme and their parameters to preserve data value and privacy.

Assuming this local and personalized (personal or entity-specific) control of the generated data becomes possible, the monetization aspect of such untapped wealth requires also some specific platforms, data and currency exchange mechanisms as well as privacy for the involved parties. Such data marketplaces, while providing another level of modularization as described earlier, for data usage, also increase the attack and threat surface significantly. Consequently, they require context specific, automated security approaches as well.

Distancing ourselves from the privacy specific aspects, ensuring that security orchestration and automation is carried out with meaningful insights into various parts of the 6G network, requires a large amount of information sharing across the subnetworks [4], entities, and layers. It is also clear that such amounts of information cannot be carried directly for consumption and analysis (simply because of scale, e.g.), but will require specific insights or abstractions to be shared in their stead. Machine Learning models are one example of such information abstraction (and inference) that can be shared and used further, as in the case of Federated Learning schemes.

Ideally, this information and data sharing is not only carried out at the single network level, but across multiple stakeholders such as, for example, between mobile network operators and/or communication service customers, and one can dream of such exchange happening across national borders for the sake of coordinated security intelligence and response. This again requires levels of information abstraction and anonymization that are challenging to perform in an automated way, while ensuring sufficient privacy and security

B. Security Automation, Orchestration and Assurance

In 5G and 6G, security is an integral part of all network layers and the need for security automation is driven by the flexible deployment scenarios as well as the customization of networks and services on demand which require dynamic and adaptive methods for security management. In future networks customers like enterprises and governments can request data and communication services whose security requirements can span a variety of Service Level Specifications (SLSs) or Service Level Agreements (SLAs). The lifecycle management (provisioning, monitoring, modification, and termination) of the security functions necessitates a holistic approach including native security in service set up, assurance of real-time service security within different technology domains, and orchestrating of overall service security across multiple subnetworks. In addition, the introduction of new network and management architectures like Service-Based Architecture (SBA) and Service-based Management Architecture (SBMA) [18], [21], in combination with new business models like Network Slice as a Service (NSaaS) [22] exceeds the level of complexity for managing the security of networks according to different service requirements.

In 4G, standardized interfaces and information models for security management across RAN and Core networks are missing. Initial work on APIs is already done in 5G standardization [23], [24], but in 6G the coordination and arbitration of security attributes across networks and subnetworks is nascent and new APIs/information models will be defined for security and exchange of security data among communication service providers, network operators and cloud infrastructure providers.

Future networks must offer means to provide the required low latency and high reliability of a service. Self-optimization and self-healing strategies of the network will cover performance and security aspects and enable conflict resolution between security and performance requirements dependent on the context like service type, topology information and intents. The past has shown that attacks will continue to get more advanced over time and new methods are needed to mitigate attacks under performance constraints to protect sensitive network entities in near real-time and to guarantee business continuity.

The level of customization of private networks and slices on a shared infrastructure will increase and lead to individually composed security management capabilities implemented as plug-and-play solutions to enable intelligent and automated security for service fulfilment and assurance. In 6G, operators and customers like enterprises, need simpler ways of managing security and new security management capabilities will be introduced to enable high-level and "fuzzy" service requests like analytics on demand. For the refinement of the service request dependent on the gradually changed trust relationship, interaction and corresponding new interfaces are required to support the negotiation between service producer and service consumer acting on behalf of the (enterprise) customer.

In 5G and 6G, slice isolation is important to ensure reliability and security for service assurance together with data integrity and confidentiality. Especially, the data of a slice customer must be always isolated from another slice customer even for the lowest isolation level of slices. Data isolation is required for all types of management, signaling and user plane data, and different methods for protection can be provided for different customers or slice groups. Furthermore, data isolation can be applied dependent on the type of data or the stage of data (rest, transmission, use), even for a single customer or within a single slice.

C. Software Development Lifecycle Security

By adopting software engineering paradigms, vendors can foster both technical and business innovations. Continuous delivery allows CSPs to acquire new functions more quickly and reduce the time to market. This could be reflected on the

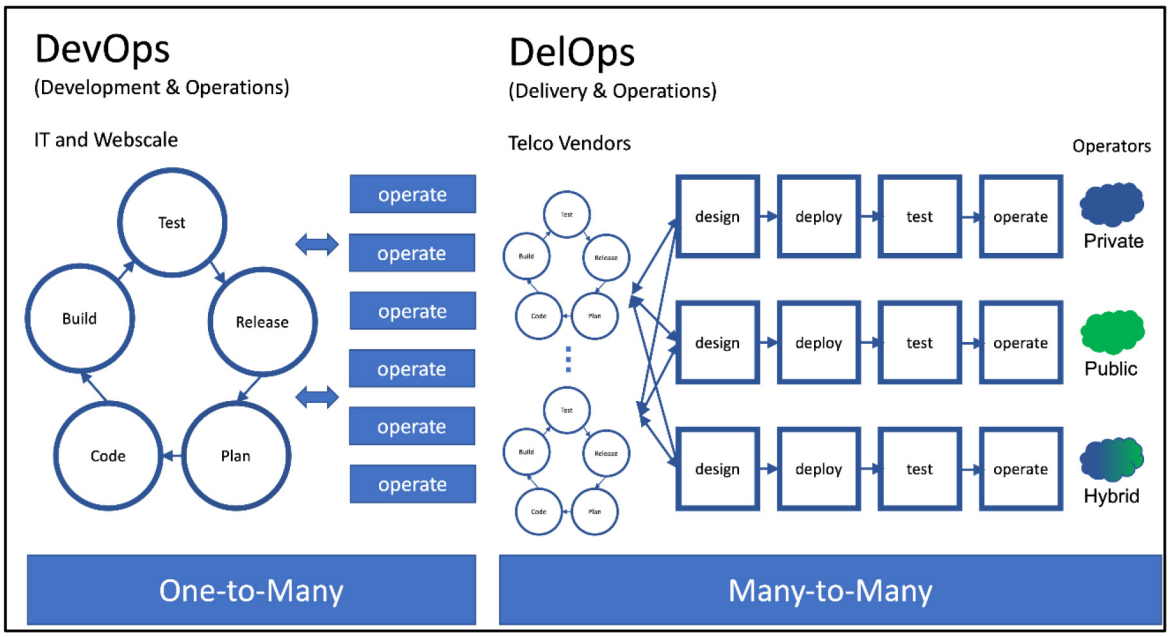

Fig. 3. Software supply chain in general (left) and in telco (right).

billing practice and vendors could price software based on usage following cloud principles. CSPs could run redundant network functions supplied by distinct vendors, contrary to current practice of assigning each function to one vendor. New competitors could emerge by developing their own, specialized network functions.

Such billing practices would have one flaw: there is no revenue in case of service disruption. Thus, in future networks security will become even more important to protect both the vendors' and the CSPs' revenue.

As previous generations have shown, the implementation change is not immediate and is done at different paces for each network function. It is constrained by the criticality and the multi-vendor aspect of the telecommunication service.

Bringing automation to the software supply chain is more complex. The multi-vendor environment justifies a dedicated pipeline, which can be referred to as Delivery Operations (DelOps) [25], illustrated in Figure 3. It parallels the widespread DevOps paradigm. Vendors do continuous integration and delivery, while the CSP does continuous deployment, maybe on third party infrastructures. The CSP also performs validation tests before operation. They are done in a realistic yet isolated infrastructure, to ensure successful composition of the products from the vendors.

Such evolution raises several security concerns. When mitigating or recovering from a service disruption caused by an attacker, properly identifying which stakeholder (virtualization infrastructure service providers, mobile network operators, and telecommunication vendors, e.g., current ones or newcomers) is accountable for a lack of protection and for whom penalties are assigned, will require significant innovation and new trust models. The attackers could have access to resource management from the CSP or the infrastructure provider; or they could exploit the software supply chain of the CSP or one of the vendors.

Validation tests can prevent some attacks, but attackers tend also to detect isolated environments, triggering attacks only on production sites. Even so, they may also wait until they have enough presence. For instance, after compromising a resource image, they will likely wait for more instances to be spawned.

Attacks toward the software supply chain are an additional concern. In their survey, Geer *et al.* [26] propose a definition of said attacks where "intentional insertion of malicious functionality" is key to distinguish them from regular attacks. Beyond exploiting a vulnerability, such attacks aim at crafting their own ones. Examples range from "typosquatting", dependency confusion, to the far more sophisticated "Sunspot" [27]; they show that all components of the pipeline can be exploited.

Overall, technical and organizational cooperation between the different stakeholders is key to proper root cause analysis, but the appropriate trust model is yet to be designed.

In security guidelines on cloud infrastructures, the U.S. National Security Agency (NSA) emphasizes that continuous security monitoring is critical to detect evidence left by intruders, both for CSPs and Hyperscalers [28]. Continuous security monitoring is an enabler for coordinating the reaction of the stakeholders. A common framework ensuring cross vendor compliance will be necessary to provide trusted, undisputable proof points.

Various data can be exploited in the context of 6G: network data (either from user or control planes), log data, Key Performance Indicators (KPIs) from network elements (especially O-RAN Alliance components [29]), host data, or program-wise data (VMs, containers, serverless functions) and AI/ML models. They all are relevant for intrusion detection and will be employed in 6G as part of a defense-in-depth strategy.

Considering host- and program-wise data is new to the telecommunication industry, and appropriate ways to collect and process them must be researched under one key constraint:

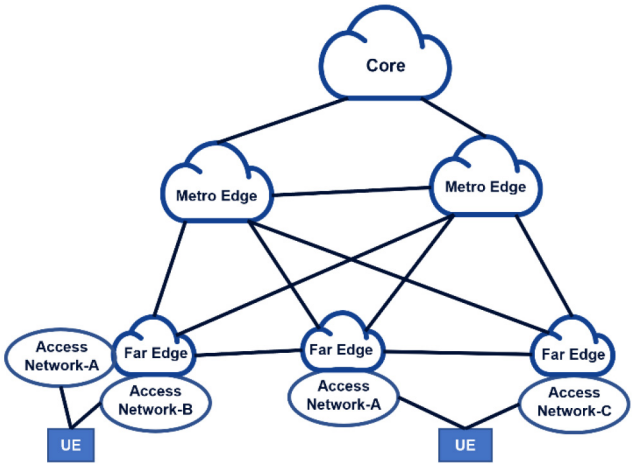

Fig. 4. Hierarchical Multi-Access Network Architecture.

having as little impact as possible onto the performance of monitored network elements, and the traffic in the control plane. Eventually, like KPIs, host data will be standardized to meet said constraint.

The introduction and multiplication of new stakeholders will redefine the trust relationships between service producers and service consumers, therefore altering risk analysis for all kind of network assets/data services of future networks. With 6G, the telecommunication industry accomplishes a shift from a proactive (overprovisioning-based) mode to a reactive (elasticity-based) mode. Continuous security monitoring will enable activation of countermeasures, in real-time and in an automated manner. Such automation will not be achievable without cooperation with network management automation to resolve conflicts that naturally occurs between performance, security, customer requirements and regulations.

VIII. Future Networking in 6G

The next evolution in networking, 6G, has the ambitious goal of interconnecting digital, physical and human worlds that goes beyond the 5G standards. It will bring in several challenges in the way communication networks will be built in the future. We will assume some features of the evolved networks that will guide our discussions (see Figure 4). First and foremost, network will be all pervasive and IP connectivity for a UE will be very close to the edge of the network, i.e., will start directly from the base station or some network function in the RAN/Core located at the edge of the network. Multiple Radio Access Technologies (including satellite networking) will be prevalent, and in many areas overlapping access technologies will be widely available. The 6G architecture will be fully integrated/hosted in the cloud. This will ensure availability of computation (almost) anywhere in the network. The access networks will be hosted at the far edges of the cloud and the rest of the network will be structured hierarchically over metro and core cloud. Network services will be deployed in the cloud and within the network and will exploit the hierarchical structure for low latency, high throughput, and reliable services. We also envision that there will be UE-to-UE ad hoc networking to support short reach but high bandwidth connectivity (over THz radio), that need/should not be backhauled over the 6G core network. The challenge is to architect the evolved network that will become the substrate for communication with computation "built" into it and supporting a variety of functions.

A. Seamless Mobility in All-IP Network

We envision IP will start from the very edge of the 6G network and will support multiple access technologies. For a corresponding node to reach a UE regardless of its location and access network attachment, mobility and handoff will be supported by the IP network. Current IP networks use the IP address of a UE for both identification and location, which makes support for mobility somewhat convoluted. A highly desirable feature, and a challenge for the 6G network design will be to decouple the routing locators and identifiers for the UE. Typically gateway-based approaches are adopted for supporting mobility [30], [31]. In this architecture, gateways are placed in the core of the network and the connections from UE are anchored to one of them. Another challenge is to support UE mobility without backhauling the traffic into the core of the network. This will reduce connection latency significantly. Moreover, high bandwidth connections will not waste precious link bandwidth as they will not be carried to the core.

Instead of one-size-fits-all type of mobility support, we envision at least two different models of mobility. For UEs with enough computation power (e.g., phones, cars, etc.), a "Do-It-Yourself" model of mobility will be supported. In this model, the network will allocate an IP address to the UE, and mobility and handoff decisions at the IP layer and the corresponding methodologies will be natively built into the network protocol stack of the UE. It can be supported in the operating system of the UE and/or at applications running in the UE. This solution can be thought of as working in the layers 4-7 of the OSI model of networks. There are several benefits of this approach. A UE will be able to select the best network path based on some user and/or provider specified criteria (described later). Most of the current generation of UEs can already support communication over multiple access networks, multi-path TCP can support moving from one network to another without interruption, new applications (e.g., QUIC) are being developed with built-in support for mobility. The challenge will be to design such a scheme to work across multiple access networking technologies and multi-operator edge networks seamlessly.

For devices that are not capable of doing-it-themselves, there will be a fallback option where the network will provide mobility and handoff support (at OSI network layers 2-3). The prediction is devices of this class (i.e., with very limited compute and battery power like various low power sensors) will need limited mobility support as they will be mostly stationary. Techniques to support this class of mobility can be gateway-based or SDN-based. One open research issue is to use newer network programming technologies to programmatically "tunnel" packets to support mobility.

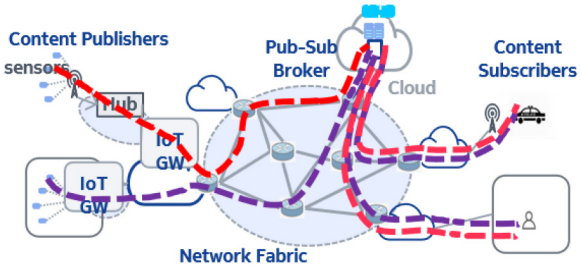

Fig. 5. Centralized (classic) over-the-top Pub-Sub.

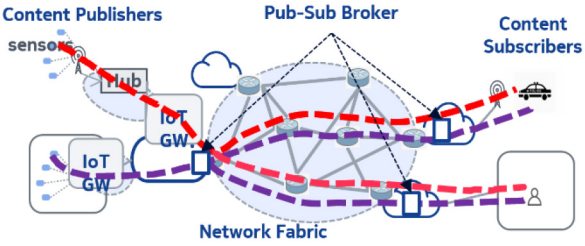

Fig. 6. Federated over-the-top Pub-Sub.

B. Intent-Based Networking From the UE

In each generation of the network, UE becomes more powerful and feature rich. This trend will continue with 6G as well. So far QoS responsibilities are squarely placed on to the network. In 6G, a UE will take active role in network and service selection. A UE keeps track of the real-time characteristics of the network (e.g., instantaneous latency, current bandwidth, energy efficiency, to name a few) the best and at the individual level. Therefore, an application running on the UE is best placed to select the right access network(s) for the right duration for its optimal execution. In current networks, each UE needs to continuously measure different network characteristics individually which is wasteful. In 6G networks, such telemetry will be a shared responsibility between the network and the UEs. The network will use fine grained in-band network telemetry, and the results of which will be available to the UEs at large through (yet to be defined) standardized APIs. This will minimize the over-the-top measurement performed by the UEs. Moreover, the operating system of the UE, the best place where such information gathering can occur, will provide this information to the applications using well-published APIs. Last but not the least, intent-based networking, becoming popular in the data center networking, will be available in UEs. The ultimate challenge is to empower a user to specify intent (e.g., QoS support, energy efficiency, mobility management, etc.) to the UE so that applications and services can be customized on a per user and per application basis.

C. Network-Assisted Service Creation

The 5G network pioneered the use of network functions which brings in flexibility and agility in deploying the network and the standardized services. One of the challenges in a 6G network will be to provide the ultimate flexibility in service creation using application functions. An application function

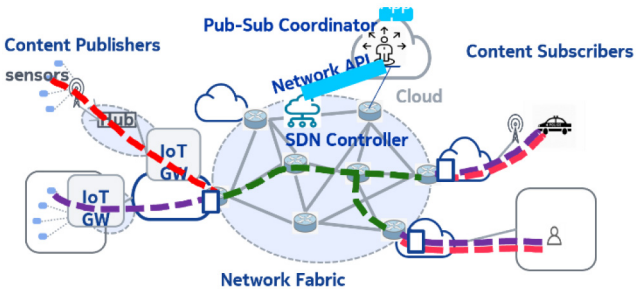

Fig. 7. Network-assisted Distributed Pub-Sub.

is a software module that will implement user-defined services (as opposed to standardized services enabled by network functions). Examples include publish-subscribe methodology for massively scalable data distribution from many sensors, distributed gaming proxies to support real-time multi-player gaming, etc. Most often than not, application functions will be cloud-native, and therefore, will support all the benefits thereof. As a first step, 6G networks will provide (standardized and/or open source) building blocks for various application functions for implementing distributed services that will be widely used in the networks. Examples include brokering for publish-subscribe for sensory data distribution, load balancing across multi-cloud resources, latency reduction and equalization for real-time multi-user applications, etc. Going forward, users will be allowed to bring, install and instantiate their own application functions on-demand in the 6G network. This will allow rapid introduction of user applications with extreme customization. Eventually, the application functions will not only be cloud resident, but also be in-network created using advanced network programming (like SRv6) and software defined networking. The network will assist in migration of such functions within its perimeter (across cloud nodes or in-network placement) as and when required by the service.

In the example below, the following three figures explain how one of the popular distributed services like publish-subscribe can be enhanced with network-assistance. Figure 6 shows the most popular classic mode of operation in a publish-subscribe system. The traffic from publishers is transported to a centralized cloud broker which then disseminates it to the subscribers based on their interests. Figure 5 shows another configuration (also known as federated) where multiple brokers are installed at strategic locations in the network (shown in the Figure are edge cloud locations) and the brokers create an overlaid distribution mesh. Both over-the-top (OTT) approaches, while good for easy connectivity and suitable for dynamic data routing, does not consider the massively distributed nature of data sources, and cannot make use of the resources available at the edge clouds and within the network. A network-assisted architecture for supporting a distributed application like Publish-Subscribe is shown in Figure 7. In this model, application functions are placed at various edge locations of the network where all the users connect. The application function will implement a broker for publish-subscribe. Application data will be disseminated from one edge location to another through network-level mechanisms, as

opposed to OTT transports. An Application Coordinator, working atop the network controller will make all the application specific data routing decisions which will be then instantiated by the network controller into the network. It will also account for the geographical distribution of the data sources and can be optimized to make best use of the underlying network capabilities.

D. Programmable Data Plane With Per User Customization

With a completely programmable data plane, the next challenge is to monitor the activities within the network at scale. To support this, in the 6G networks, in-band network telemetry will be supported at all network nodes. Provisions will be made so that application specific traffic can be collected from the network in real-time. Use of multi-tenant programmable switch architecture [32] or equivalent will be desirable to support (virtually) isolated application specific monitoring and debugging. Ultimately end-to-end network monitoring will be necessary for application performance, checking for correctness, etc. Moreover, with the user supplied application functions hosted at cloud-resident servers, it will be necessary to draw the trust boundary between the infrastructure and the user. An open challenge is to realize such boundaries using the newly emerging Data Processing Unit [33], [34] (DPU) and Information Processing Unit [35] (IPU)-based network interface cards installed at the servers in the cloud. This will also lead to easy and scalable way of compute, memory and storage disaggregation, and accessing the resources over a trusted network fabric within the cloud. For an application, the resources will always appear local regardless of the application's locality, mobility, and/or any dynamic changes in the network fabric that encompasses data center networks, edge networks and the backbone networks.

E. Ad Hoc Networking Among Intelligent UEs

Devices capable of communicating using high bandwidth but short-range communication technology will have the provision of communicating directly with one another. This allows high bandwidth and lowest latency communication and saves backhauling requirement and overhead through the RAN and core networks. In order to achieve this, peer-to-peer ad hoc communication must be re-evaluated with 6G's requirement. This will require robust service discovery mechanism, and multi-hop ad hoc routing when the end devices are interconnected through other intermediate devices for reachability. This will also require content store-and-forward networking and smart-loading with intermittent connectivity.

F. Communication Across Multiple Providers

When end users are resident on different providers' network, the communication goes through the peering points between the providers. Peering solutions between two networks used today are between service providers and are usually located in the metro and core parts of the network. A key requirement for 6G is a network fabric that can efficiently and seamlessly support far-edge use cases in addition to all the functionality provided by current networks. This will require a dynamic peering mechanism to offload access traffic to the service provider at the most suitable peering points. Hyperscalers, who are one of the primary drivers of edge services, have also modified their networks to extend them to the edge. Thus, the structural implications of a far-edge focused 6G solution will require dynamic edge peering and an expanded Hyperscaler perimeter.

IX. The Way Ahead and Collaborative Projects

In this paper we have described the landscape in which 6G will unfold in context of the next 30 years of telecommunications change, and suggested timelines for technical deployments that may inform the pace of change. With this background, proposed technical challenges and suggested approaches were elaborated. For network and service automation we explored finer grain modularization, bidirectional intent interfaces, distributed intelligence, and conflict-free multi-stakeholder control loops. Under security and privacy, we articulated data privacy and security needs, security automation, and software development lifecycle security. Finally, with future networking in the 6G mobile context, we elaborated seamless mobility in an all-IP network, intent-based networking from the UE, network assisted service creation, a per user customized data plane, ad hoc networking among intelligent UEs, communications across multiple providers.

We are exploring these ideas and many others through a variety of mechanisms. Our research leads investigations in some areas, but we rely on several large collaborative efforts to gain consensus and establish common standards and interfaces so that the ecosystem of technical contributions and intellectual value can progress without leading to unwieldy silos that most investment won't tolerate. Our involvement in Hexa-X [2] funded through the European Union's Horizon 2020 research and innovation program, is one such initiative. There are new ones becoming established as well in Europe such as the German Government funded 6G Hub [36]. In North America, we participate in the NextG Alliance [5], and have contributed to and collaborate in the National Science Foundation (NSF) RINGS program [37]. With this broad range of initiatives and a landscape of technical challenges, as inventors, we have plenty of tasks to attend.

Acknowledgment

The authors would like to thank their colleagues at Nokia Bell Labs with whom they had numerous insights about 6G. In particular, they would also like to thank other team members in the Network Systems and Security Research Lab for their many discussions that led to this article, including special support from V. Räisänen, K. Aaltonen, and T. V. Lakshman. Special thanks also to H. Viswanathan who provided detailed comments on an early draft of this article.

References

[1] "NTT DOCOMO 6G White Paper V4.0." NTT Docomo. Jan. 2022. [Online]. Available: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v4.0.pdf

[2] "Deliverable D1.2 Expanded 6G Vision, Use Cases and Societal Values." Hexa-X Consortium. May 2021. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2021/05/Hexa-X_D1.2.pdf
[3] M. Matinmikko-Blue *et al.*, "White Paper on 6G Drivers and the UN SDGs." University of Oulu. Jun. 2020. [Online]. Available: http://jultika.oulu.fi/Record/isbn978-952-62-2669-9
[4] H. Viswanathan and P. E. Mogenson, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57063–57074, 2020.
[5] "Roadmap to 6G." NextG Alliance. Feb. 2022. [Online]. Available: https://nextgalliance.org/white_papers/roadmap-to-6g/
[6] "ITU FG NET-2030." ITU. Jul. 2020. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx
[7] *You'll Be Able to Carry Phone in Pocket in Future*, Mansfield News-J., Mansfield, OH, USA, Apr. 1963, p. 20.
[8] "Helium Ecosystem." Helium Systems Inc. [Online]. Available: https://www.helium.com/ecosystem (Accessed: Feb. 2022).
[9] M. Polese *et al.*, "Dynamic spectrum sharing between active and passive users above 100 GHz," *Commun. Eng.*, vol. 1, p. 6, May 2022. [Online]. Available: https://doi.org/10.1038/s44172-022-00002-x
[10] M. Polese *et al.*, "Coexistence and spectrum sharing above 100 GHz," Oct. 2021, *arXiv:2110.15187*.
[11] V. Ziegler, H. Viswanathan, H. Flink, M. Hoffman, V. Räisänen, and K. Hätönen, "6G architecture to connect the worlds," *IEEE Access*, vol. 8, pp. 173508–173520, 2020.
[12] I. Siaud and A. Ulmer-Moll (Orange Labs Rennes, Cesson-Sévigné, France). *THz Radio Communications*. (Sep. 2019). [Online]. Available: http://www.brave-beyond5g.com/wp-content/uploads/2019/10/10_ _Orange-THz-radio-communications.pdf
[13] National Centers for Environmental Information (NCEI) (NOAA, U.S. Government, Washington, DC, USA). *Time Series of Billion-Dollar Weather and Climate Disasters*. (2022). [Online]. Available: https://www.ncdc.noaa.gov/billions/time-series
[14] "Sea Level Rise Projection Map—Miami." Earth.org. Aug. 2020. [Online]. Available: https://earth.org/data_visualization/sea-level-rise-by-2100-miami/
[15] S. Marek. "How Wireless Operators Are Preparing their Networks for Climate Change." Lightreading. Feb. 2022. [Online]. Available: https://www.lightreading.com/iot/how-wireless-operators-are-preparing-their-networks-for-climate-change/d/d-id/775293
[16] P. Szilágyi, "I2bn: Intelligent intent based networks," *J. ICT Stand.*, vol. 9, no. 2, pp. 159–200, 2021.
[17] Q. Liao, T. Hu, and D. Wellington, "Knowledge transfer in deep reinforcement learning for slice-aware mobility robustness optimization," 2022, *arXiv:2203.03227*.
[18] "Zero-touch network and service management (ZSM), reference architecture," ETSI, Sophia Antipolis, France, ETSI document GS ZSM 002, Aug. 2019. [Online]. Available: http://www.etsi.org
[19] M. Zambianco, A. Lieto, A. Malanchini, and G. Verticale, "A learning approach for production-aware 5G slicing in private industrial networks," in *Proc. IEEE ICC*, 2022.
[20] "Using Digital Twins to Integrate 5G Into Production Networks." 5G-ACIA. Feb. 2021. [Online]. Available: https://5g-acia.org/whitepapers/using-digital-twins-to-integrate-5g-into-production-networks/
[21] *Group Services and Systems Aspects; Management and Orchestration; Architecture Framework; Rel 17*, 3GPP Standard TS 28.833, Dec. 2021. [Online]. Available: http://www.3gpp.org
[22] *Group Services and Systems Aspects; Management and Orchestration; Provisioning; Release 17*, 3GPP Standard TS 28.531, Dec. 2021. [Online]. Available: http://www.3gpp.org
[23] "Group services and systems aspects; management and orchestration; study on enhancements of management data analytics (MDA); release 17," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 28.809, Apr. 2021. [Online]. Available: Http://www.3gpp.org
[24] "Group services and systems aspects; Management and orchestration; Study on network slice enhancements; release 17," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 28.811, Dec. 2021. [Online]. Available: http://www.3gpp.org
[25] M. Varma, "Accelerating the Pace of Service Innovation with DelOps." Nokia. Mar. 2021. [Online]. Available: https://www.nokia.com/blog/accelerating-the-pace-of-service-innovation-with-delops/ (Accessed: Feb. 2022).
[26] D. Geer, B. Tozer, and S. J. Meyers, "Counting broken links: A quant's view of software supply," in *Proc. USENIX Login*, vol. 45, 2020, pp. 1–4.
[27] MITRE ATT&CK®. "SUNSPOT, Software S0562." Mitre Corporation. Jan. 2021. [Online]. Available: https://attack.mitre.org/software/S0562/ (Accessed: Feb. 2022).
[28] NSA and U.S. Cybersecurity Infrastructure and Security Agency. "Security Guidance for 5G Cloud Infrastructures (I): Prevent and Detect Lateral Movement." U.S. Department of Defence. Oct. 2021. [Online]. Available: https://media.defense.gov/2021/Oct/28/2002881720/-1/-1/0/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_I_20211028.PDF (Accessed: Feb. 2022).
[29] "About O-RAN Alliance." O-RAN Alliance. 2022. [Online]. Available: https://www.o-ran.org/about
[30] C. Perkins, Ed., "IP mobility support for IPv4," Internet Eng. Task Force (IETF), RFC 5944, Nov. 2010.
[31] C. Perkins, Ed., "Mobility support in IPv6," Internet Eng. Task Force (IETF), RFC 6275, 2011.
[32] R. Stoyanov and N. Zilberman, "MTPSA: Multi-tenant programmable switches," in *Proc. 3rd P4 Workshop Eur. (EuroP4)*, 2020, pp. 43–48.
[33] "NVIDIA BlueField Data Processing Units." NVIDIA. [Online]. Available: https://www.nvidia.com/en-us/networking/products/data-processing-unit/ (Accessed: Jun. 2022).
[34] W. Noureddine. "The Fungible DPU^{TM}: A New Category of Microprocessor." FUNGIBLE. 2020. [Online]. Available: https://www.fungible.com/wp-content/uploads/2020/08/WP0027.00.02020818-The-Fungible-DPU-A-New-Category-of-Microprocessor.pdf
[35] A. Moore and J. Henrys. "IPU-Based Cloud Infrastructure: The Fulcrum for Digital Business." Intel Corporation. 2021. [Online]. Available: https://www.intel.com/content/www/us/en/products/docs/programmable/ipu-based-cloud-infrastructure-white-paper.html
[36] "Karliczek: We Want to Be at the Forefront of 6G (PRESS RELEASE: 140/2021)." German Federal Ministry of Education and Research. Jun. 2021. [Online]. Available: https://www.bmbf.de/bmbf/shareddocs/pressemitteilungen/de/karliczek-wir-wollen-bei-6g-an-der-spitze-sein.html
[37] "Resilient & Intelligent NextG Systems (RINGS) Program Solicitation." National Science Foundation (NSF). Aug. 2021. [Online]. Available: https://www.nsf.gov/pubs/2021/nsf21581/nsf21581.htm?org=NSF

Gerald M. Karam (Senior Member, IEEE) received the B.A.Sc. degree in electrical engineering from the University of Ottawa, Ottawa, Canada, in 1982, and the M.A.Sc. and Ph.D. degrees in electrical engineering from Carleton University, Ottawa, Canada, in 1984 and 1987, respectively.

After graduation, he was on faculty with the Department of Systems and Computer Engineering, Carleton University, leaving in 1995 having the title of Associate Professor (tenured). He joined AT&T Bell Labs in 1995 and over the next 25 years held a variety of roles in AT&T Labs including the Executive Director of Research, a Distinguished Technical Staff Member, and an Assistant Vice President. After retiring from AT&T, in 2019, and a brief stint consulting for CableLabs, he joined Nokia Bell Labs, Murray Hill, NJ, USA, in 2020, where he is a Principal Researcher. He has 30 issued patents, more than 35 referred publications, and one textbook (Pearson). His current research interests and activities include 6G network systems, communications software architecture, and network services and management technology.

Dr. Karam recipient of an AT&T Science and Technology Medal. IEEE recognitions include an IEEE Millennium Medal, IEEE Regional Activities Board Innovation Award. He is an AT&T Fellow.

Markus Gruber received the engineering degrees from the University of Stuttgart in 2002 and Télécom Paris in 2002, and the Ph.D. degree in computer science from the University of Tübingen in 2006.

He currently heads the Network Automation Department, Network Systems and Security Research Lab, Nokia Bell Labs with a focus on 6G design, network slicing, IoT, and AI.

Iris Adam received the Diploma degree in mathematics and economics from the University of Siegen, Siegen, Germany.

She is a Senior Researcher with Nokia Bell Labs, Munich, Germany. She is mainly concerned with security management and orchestration tasks. Her current research interests include the automated security management in 6G with focus on cognitive wireless networks.

François Boutigny received the master's degree in engineering, specialized in network security, from IMT/Télécom Sud Paris in 2015, and the Ph.D. degree in computer science from Institut Polytechnique de Paris in 2019. He joined Nokia Bell Labs and is an Ingenieur de Recherche where his current work relates to anomaly intrusion detection systems and security monitoring for next generation networks.

Yoan Miche received the double Ph.D. degrees in applied machine learning (for watermarking and steganography) from Aalto University, Finland, and the INP Grenoble, France.

He is currently the Head of the Network Security Research Team, Nokia Bell Labs. He was a Postdoctoral Researcher on industry collaboration projects during four years with Aalto University, focusing on applications of machine learning to (cyber)security problems. He joined Nokia Bell Labs in 2014 as a cybersecurity researcher and took the lead of the cybersecurity research team in 2018. His topics of predilection include neural networks, anomaly detection, data mining, network security, and he is still fascinated by watermarking and steganography technologies.

Dr. Miche was an Associate Editor for *Neurocomputing* (Elsevier's) from 2012 to 2021, and currently serves as a member of the Advisory Board for the journal. He is also on the editorial board (and one of the co-founders) of the *Machine Learning and Knowledge Extraction*. He has been on the Advisory and Stakeholder Boards of several EU projects, recently including the SHERPA Project (on the Ethics of AI/ML) and the SAPPAN Project (on the sharing and automation of security knowledge).

Sarit Mukherjee (Senior Member, IEEE) received the M.S. and Ph.D. degrees in computer science from the University of Maryland, College Park, MD, USA.

He managed the design and development of streaming appliances in a New York-based startup company and led the video networking group in Panasonic Information and Networking Technology Laboratory, Princeton, NJ, USA. He is currently a Technical Manager with the Network Systems and Security Research Lab, Nokia Bell Laboratories, Murray Hill, NJ, USA. His current research interests include cloud computing, software defined networks, high speed packet processing with hardware offload, and data distribution in emerging networks.

Dr. Mukherjee has extensively published research articles in renowned technical journals and conferences and served in the technical committees of several international conferences.