6G Core-Architecture – Approaches for Enhancing Flexibility across Control and User Plane

Dennis Krummacker[1,*], Benedikt Veith[2,*], Christoph Fischer[3,*] and Hans D. Schotten[4,*†]
[*]German Research Center for Artificial Intelligence GmbH, DFKI. D-67663 Kaiserslautern.
[†]Institute for Wireless Communication and Navigation. University of Kaiserslautern. D-67663 Kaiserslautern.
[1]dennis.krummacker@dfki.de, [3]benedikt.veith@dfki.de, [3]christoph.fischer@dfki.de,
[4]hans_dieter.schotten@dfki.de, schotten@eit.uni-kl.de

Abstract

The upcoming generation of mobile communications, 6G, will hold great potential to become the backbone of an interconnected world, bringing together various kinds of services and technologies. A critical factor for reaching the envisaged goals is the design of the interplay of services constituting the 6G Core network. The role it will take within the upcoming decades requires the Core network to be open, flexible and trustworthy at the same time. In this work we review the state-of-the-art principles of service interaction in today's infrastructures, such as Core design, as well as current approaches to adapt ongoing trends in software architecture design into the world of mobile communications. From there, several areas for discussion are opened and the impact of shifting paradigms on the Core network design is analyzed. Finally, critical features and approaches that need to be considered in the design of future 6G Core networks are determined.

Preprint.

***Keywords*—** 5G, 6G, mobile communications, architecture

1 Introduction

The vision phase for the evolution of mobile communications beyond 5G has a collection of features in view to enhance the operation of an infrastructure to be more flexible and efficient. One major property of mobile communications architectures that forbids the required degree until now is how data is exchanged. Data flows are very strict, predefined and the overall system is not really designed to undergo substantial changes after initial commissioning. Part of this is how the Core operates, respectively the bare existence of such. In mobile communications networks, the user traffic is separated from management and orchestration of the infrastructure. In principle, tasks regarding the operation of the network are executed encapsulated inside a so-called *Core*, which is a collection of services. A Core is a rather isolated domain, inside which the services are able to interact, but basically no data is going out or into a Core. A Core always operates fully on its own; it is not envisaged to attach data-providing or -consuming services; nor does it collaborate with anything else but its own Core & Radio Access Network (RAN) compilation.

This design principle – the *separation of concerns* – basically makes a lot of sense and yields numerous advantages. But simultaneously, its realization goes that far that the total isolation prohibits beneficial functionalities. Consequently, information cannot be shared between several consumers; interaction capabilities, if any, are limited; advancements and extensions are hindered; the collective of all services is split into distinct *data domains*, where data is restricted to. This leads for example to identical data being redundantly measured and processed multiple times because one process is not able to access the results of another.

The work at hand is intended as a discussion about design principles for having a more versatile and flexible data exchange between services and a more efficient data availability throughout the entire network. We start with the state-of-the-art of 5G to outline which fundamentals cause lacks for service interconnection and data availability. Then certain design principles are pointed out for discussing how they influence the capabilities of a service oriented network. From this, properties for a complex communication system are derived that are deemed necessary to achieve flexible and efficient service networking.

2 SotA – Standardization / Market

In the first part, the SotA is discussed for 5G, whereas the second is an outlook beyond 5G and towards 6G visions and related research in this domain.

2.1 5G

In a Service Based Architecture (SBA), the overall functionality of a system is split into multiple internal components, each of which is providing services to other components via well defined interfaces. Individual entities exchange information being in a relationship of service consumer and producer.

5G introduced this paradigm to mobile communications by defining the different Control Plane (CP) functionalities of the Core network as an SBA, where single components of the architecture are described as Network Functions (NFs). The evolution of the 5G SBA is driven by Network Function Virtualization (NFV) and Software Defined Networking (SDN) [1]. It allows to decouple the design of network functionalities from underlying communication layers, enabling for example flexible deployment for scalability and independent optimization of single functions. In this regard it differs from the previous 4G LTE standard (Evolved Packet Core), where the Core functionalities are mapped to a small number of network nodes of high functional complexity.

In the 5G SBA, an NF provides one or several services to other NFs via a Service Based Interface (SBI). The services exposed by 5G NFs are described in general in 3GPP TS 23.501.

The design style of choice for the APIs in use with the SBIs is the Representational State Transfer (REST) paradigm [2]. An alternative is Remote Procedure Call (RPC), where a client directly addresses procedures on the server side to be invoked. A comparison with regard to applicability in the 5G SBA domain has been carried out by Zhang et al. in [3].They conclude that although RPC can be mapped directly to the concept of services and service operations in 5G, REST brings a better decoupling of services, making it easier to upgrade single functions and manage resources like databases and sessions.

For NF discovery and communication establishment, four approaches are described in 3GPP TS 23.501, allowing for either local deployment or more dynamic configurations. The latter relying on a framework consisting of the NFs Network Repository Function (NRF) and Service Communication Proxy (SCP). The NRF acts as a local repository for active NFs, allowing NFs to register and de-register or even send heartbeats. It then can be queried by any NF for active instances of a specific service type for node discovery. The SCP has been introduced with 3GPP Release 16 and is designed to be an intermediate node for the communication between NFs. Acting as a central broker for inter-NF communication, it can take CP traffic management tasks like routing and load balancing.

The Network Exposure Function (NEF) has been introduced to the 5G SBA to expose a central, secure API to access services and discover capabilities of internal elements of the Core. It provides services to external systems like exposure of capabilities and events, secure information provisioning to the Core network or translation between external and internal data representation. It therefore is designed to constitute a central gateway for external services to access the functionalities of the 5G Core, which otherwise depicts a rather closed system.

2.2 Beyond 5G, 6G

In research it is very much consensus that mobile networks are too inflexible and static, still up to 5G systems. Comparing the infrastructures with platform solutions from the IT sector, despite a rising degree of softwarization, much can still be gained. The research community is regularly pointing out that mobile communications architectures have to become more adaptive [4], propose design approaches and abstraction concepts [5] and develop new functions to support this evolution (e.g. [6], [7]).

Nephio is a project launched by the Linux Foundation, Google Cloud and several partners across the telecommunications industry. It has been announced in 2021, with first technical summits taking place in 2022. The project aims at developing a Kubernetes based framework for automated deployment and management of cloud native network functions, with a focus on the requirements of Communication Service Providers (CSPs). A first release is expected early 2023. The framework is envisioned to automate the network function provisioning on multiple levels, from cloud infrastructure to NF orchestration to individual configuration of single NFs. The CPs from those different layers are merged into a declarative configuration management, following the Configuration-as-Data approach. This means, that the framework translates highly abstracted target descriptions for the network configuration (e.g. QoS, resources, infrastructure) into orchestration commands for Cloud, Regional or Edge Clusters.

In [8], Corici et al. leverage a web service architecture for the functional split of 5G Core services. It consists of a Frontend maintaining a logical link to a UE, several stateless Workers executing CP functionalities and a Database for unified storage of the session state. The functional split between different types of Workers is done at the level of services and system procedures instead of complete network functions as is standardized for the 5G Core. The design includes the principle that no horizontal communication between the Workers is necessary for executing a requested task. This eliminates the need for a complex set of standardized interfaces between the various network functions. Instead all necessary information is exchanged between Workers via the shared session state stored in the database. This helps simplifying the integration of additional services.

The web service based approach for the 6G Core architecture with a novel functional split into Workers (procedures) instead of Network Functions (functionalities) improves the functional flexibility of a Core instance, enabling highly specialized Core implementations (e.g. Reduced Capability Core) as well as fast up- and down-scaling with a low level of granularity. The functionality of the Core can be expanded by adding Workers without the need for adaption of parallel nodes, since no direct interaction is implemented between Workers. This comes at the cost of a lower overall deployment flexibility, because a specific set of Frontend, Workers and Database depicts a single system deployed on a common infrastructure. A multi-cloud environment therefore would involve several of such Core systems deployed at different sites, whereas a Core architecture based on Network Functions would allow the deployment of single NFs of a Core on different cloud infrastructures.

3 Areas for Discussion

Joining the explained design concepts of known communication systems for a progressing evolution with our introduced goals outlines certain paradigms for setting-up such systems or partial functionalities. Different approaches for implementation have differing impacts on service interaction and in some cases and combinations, such approaches cross-influence each other. Hence, this section discusses aspects that are to be considered, when designing a mobile communications infrastructure and what impacts certain design approaches ultimately have.

3.1 Control Logic Consolidation

One of the first important factors is whether and how much the fundamental logic for operating the network – i.e. management and orchestration – is condensed. So to speak the bare existence of some entity like the Core in pre-6G systems as opposed to to a core-less distributed service architecture.

Consolidating the Control Logic allows an easier management and more efficient execution; local execution of all elements on one device allows most efficient technical mechanisms for interaction. Looser logical connection enables more flexible operation and is prerequisite for certain system capabilities (e.g. 6G Organic Infrastructure).

However, special attention needs to be given when distributing individual components of the Control Logic over diverse infrastructure elements. It must be prevented that they are cut off, it must be minded that possibly functions are moved that are vital for topology or connection management and also side effects like bandwidth restrictions for CP traffic itself need to be taken into account.

3.2 Service Interaction Architecture

The mechanism via which software pieces inside the system communicate influences how they can be orchestrated; i.e. can possibly restrict operations. This concerns both the CP and User Plane (UP) but especially the management services. In 5G, the SBA has the Core services interact over a common service bus via REST, which very much limits the system's flexibility and evolution [9]. A generic and adapting, yet easy to use, mechanism is a requirement for a flexible overall infrastructure. It must adapt to operations like redeployment of services, extension by new data consumers and providers and shall provide means for permission management. Proper tools may also enable integration of information processing traces across CP and UP, where appropriate.

A second question in this regard is whether one unifying mechanism for all communications is utilized or distinct strategies for the type of exchanged data: For instance, a dedicated service bus for management traffic (interconnecting the Core services) and in parallel a data-oriented tool for messages not related to operating the infrastructure itself.

3.3 Message Dispatching Mechanism

The concrete tool, used for distributing messages between the elements inside a system, can heavily influence what is fundamentally possible in architectural design. In case, this lacks certain capabilities or prevents functionalities from being realized, it can strongly limit or to the contrary promote associated features. A direct message handling by the services itself can prevent appending additional data producers/consumers, while an adaptive framework allows flexible attachment of new services interfacing between distinct network parts.

Commonly used inter-service communication paradigms are:

Orchestrated Point-to-Point (P2P) – A requesting service directly contacts another one. The address resolution is assisted by the surrounding framework. A direct unicast exchange of messages takes place.

Pub/Sub – Receivers of messages are not directly addressed. Instead consumers subscribe as interested to certain topics, whereas producers publish to such. Some handling logic per device then distributes the same message to each consumer. Still, each device acts on its own and directly sends P2P messages. The biggest difference is how receivers are determined.

Context-Management – A dedicated Service that distributes information based on their content. It serves as singular contact point for acquiring data, as it either acts as central distributor of messages or aids in establishing connections between devices. Besides live communication, also historic data can be cached.

A dedicated logic for handling the message exchange can be considered advantageous as it creates an abstraction that ensures complete coverage of receivers, thus reduces redundancy and can provide automatic configuration and adaption.

3.4 Core Isolation

Isolating the CP (a Core) – meaning to put the message exchanges between services shaping the infrastructure's behavior inside a data domain that can neither be accessed outside nor can it self reach outside – results from certain design aspects and can be intentionally induced or avoided.

Isolation aids a cleaner architecture, as certain tasks are bundled into a distinct package and separated from the operative communication of clients. It also simplifies security concerns and keeps implementation of single elements easier. To the contrary, the absence of an isolation can make the entire system functionally richer and data efficient. Elaborate third party applications can feed improved information into the management domain, or can realize new applications based on data from inside the Core. The sharing of information between the two currently isolated domains prevents data from being redundantly measured by multiple processes. Symbiosis between CP and UP can also make application scenarios significantly more efficient. As an example building drone networks with Unmanned Aerial Vehicles (UAVs). The robot control can be a third party application, the device localization data can originate either from the infrastructure or an external service and the basestation functions relate to the CP.

What is possible and to which degree an isolation emerges, results from the technical tools chosen for the more fundamental operations within the overall system, like the Message Dispatching Mechanism. The structure *inside* a Core is highly important for how it is attached to the remaining system and how any kinds of interaction with it and its services can occur. Because either exactly the inter-service communication paradigm in-between the Core services can be directly utilized to attach other applications (via an API to access data), or an ancillary service is necessary to relay interactions.

3.5 Processing Logic Classification

In traditional systems, a distinction between applications is very straight. A true classification is not really performed, since not required because interaction between such does not exist. But it can be interpreted in a similar way: The separation of CP and UP. This differentiation is anyway topic for discussion, regarding the declared goal of increasing flexibility, data efficiency and interaction across them. Also in respect of possibly redesigning the communication paradigm used between services, the access methods at disposal may cause a classification to be reasonable for assigning varying functional sets and permissions.

Another aspect to mind is the increasing degree of softwarization, which allows more freedom in the design and increases the number of tasks that are accomplished by software elements. A clear definition of responsibilities is thus conducive as it still delineates ground rules for shaping tasks into concrete elements.

With the increasing variety of planned use cases of high specialization, not only will the functional flexibility of CP services in mobile communication systems increase, but also the use of additional logic besides standard network functions will gain momentum. This leads to multiple stakeholders, which deploy parts of the system's functionality, being further expanded. For example, besides different network operators and cloud infrastructure providers also third party application providers may contribute to the overall system via edge or cloud services interfacing Core functions.

A classification of the various network functions and edge applications can be done in several dimensions:

Stakeholder: Classify NFs by the deployer, owner or producer. For instance, *(i)* the Mobile Network Operator (MNO) itself or the manufacturer of the infrastructure components; *(ii)* a Second Party Application Provider – a certified or trusted or by contract associated partner company; *(iii)* a Third Party Application Provider – any arbitrary entity that executes software in the network.

Purpose: Classify NFs by their purpose and data sources, i.e. in what type of impact its execution results. Are UP data being processed (e.g. Internet of Things (IoT) sensor fusion [10]) by an application merely utilizing the infrastructure for primitive message exchange or does the function enhance CP functionality (e.g. AI based channel prediction [11]).

The diversity of stakeholders induces the necessity to carefully deliberate on the subject of data access and security. An easily accessible environment for the deployment of services may bring a high potential for innovations, but in parallel drastically increases the need for measures to maintain the trustworthiness of applications and the overall system.

The classification by stakeholder influences how data access rules are enforced, because in some cases, information needs to be exchanged across the borders of the MNO's reliability domain. A classification by purpose on the other hand affects interfaces and communication mechanisms used by the service, since the access to UP traffic probably needs to be managed independently from access to CP messaging frameworks.

3.6 System Inter-Operability

The capability to have separate full infrastructures interact is also worthwhile, whereas currently not supported. This is especially to be mentioned in the mobile communications domain, because envisioned novel applications create new co-existence scenarios between infrastructures under the property and control of different operators. This was no problem in the past, because mobile communications networks were deployed stationary and divided via distinct frequency ranges per MNO. With 5G and upcoming 6G, new potentialities are introduced that repeal the separation of independent systems from being given in principle: Nomadic networks. By that, it is possible that complete and actively operating networks come into contact, which raises the possibility, but also necessity for interactions; e.g. for shared spectrum access. For systems as present to date, this means Core-to-Core (CtC) transmissions and accordingly dedicated services whose sole intention is to coordinate separate infrastructures/Cores. An example functionality that requires CtC is dynamic spectrum allocation and sharing for coexistent operation in a common coverage like proposed in [6].

3.7 Open Ensemble

An aspect which, due to its significance, is not to be passed on being mentioned, yet only briefly, since it is already well understood as for instance addressed by the Open - RAN (O-RAN) Alliance. It describes the possibility to assemble the overall system from multiple partial pieces that can come from different manufacturers. This to avoid vendor lock-in, enable agile development and evolution as well as for easier maintenance. This desire goes well in line with other areas discussed. Because it requires similar technical features. The entire system must be split into distinct functionalities and these have to be combined via a managing framework that handles modular interaction. Furthermore, an open standard must exist for interfaces between essential components, so that different vendors can develop the required modules as black-boxes, while still assuring in- and output being passed correctly.

3.8 Core / RAN Separation

Mobile communications systems currently split the Core and RAN. While the Core is with the latest SBA cloud native, the RAN is in most cases still spatially bound to the Radio Unit (RU), due to the time critical processing that happens here. The idea of Centralized - RAN (C-RAN) is based on the assumption that the RAN covers functionalities that can be outsourced to the cloud. In this regard, O-RAN proposes a functional split between the RU – the Distributed Unit (DU) that covers the real-time processing parts of RAN – and the Centralized Unit (CU), which covers non-real-time parts of the RAN. Between these units, a variable functional split shifts functionalities across them. Nowadays, several functions of an O-RAN can be transferred to general purpose hardware or the cloud and can be integrated in the communication framework of a Core. Depending on the used split of CU, DU and RU, the functionalities have varying requirements on the communication framework. Among these are timing restrictions as well as lots of data when it comes to transmitting IQ data in the Fronthaul for very low splits.

4 Derivation of Design Prerequisites

Now the discussed areas conclude to properties required by a communication system to be more flexible and versatile in the future. Certain features must be provided to the services shaping the communication system and the applications running on top.

4.1 Feature Set

When considering that various paradigms for exchanging information between distinct services are conceivable and offer differing advantages and drawbacks, also covering that it should be possible to open diverse possibilities to different types of services, a complexity arises for the fundamental feature of bare logical communication, which declare a dedicated *Message Exchange Framework* beneficial to have: An unified instrument at a service's disposal for simplified usage as proposed with [5], [12]. A dedicated unit for handling information exchange creates an abstraction, performs required steps and hence reduces the complexity seen by services, while still enabling extended communication capabilities via a common API. Furthermore, can this framework perform adaptions and optimization invisibly in the background, react to issues and automatically create resilience.

Coming from Section 3.5, doubts in the trustworthiness of elements and from Section 3.6 even concerns across the borders of an infrastructure can be raised. Actors not fully under the authority of manufacturer or operator of the basic system nonetheless contribute to its behavior, because of which novel measures have to be facilitated. The ongoing evolution of security measures for 6G concerns for example deep slice isolation, service authentication or ways to prepare the public key infrastructure for quantum safe operation, while still keeping in mind energy and resource consumption [13]. [6] developed a service via Distributed Ledger Technology (DLT) that can be utilized by other services to create trustworthiness in operations and events as it logs them in an immutable and reliable manner. These logs can subsequently be used for historic lookup, analysis and thus prove in the aftermath.

Between specific features exist dependencies that are in some cases newly induced with the increased architectural freedom. For example does the information exchange flexibility require rigorous caution on permission and access to data and capabilities. Such have to be ensured by the system management.

4.2 Application Classification & Permission

The authors of the work at hand deem it expedient to have some classification for system elements in conjunction with a certain strategy in system conception. A thorough classification is actually only required as soon as distinct sets of capabilities and permissions shall be exposed. Since a most uniform technical handling of all system's software elements is intended alongside a distinction as mentioned, such classification is useful and assists for a coherent design, when properly supported by other appropriate features.

Apps would then be classified upon the *purpose* of a service, i.e. on which level it contributes impact on the systems operation, also where its input originates from and accordingly where the output data is fed. For example *(i) Control*: Vital to the fundamental infrastructure operation; alike today's Core services. *(ii) Auxiliary*: Not required for basic operation; not necessarily shipped with the infrastructure nor implemented by vendor or operator; nonetheless consuming data from the CP or supplying data to it. *(iii) User*: Ordinary applications not affecting the infrastructure itself but running on top.

It can be beneficial to have applications execute outside the CP, i.e. outside the direct sphere of influence of the system's manufacturer or operator; at the same time to have no strict virtual topology between Core services, i.e. instead allowing to input data flexibly. This in order to enable such a class like *auxiliary*, which can then serve to extend and optimize an infrastructure during operation or gradually over time.

Since the CP is considered operations-critical and thus worthy of protection, access to its data domain shall not be arbitrarily granted and especially the feeding of data into it must be protected. This is to be realized via proper tools that oversee and manage, possibly restrict, operations. Tools for permission and trust management as proposed by [5], [6]. The combination of such tools with a suiting communication platform as discussed earlier allows for a proper rights model, where only appropriate stakeholders are authorized to deploy certain service classes. An approach to reduce complexity in the field of Intra- and Inter-PLMN authentication are Decentralized Identifiers (DIDs) for Self-sovereign identity management, whereas the integration of the necessary DLT into the PLMN environment is still an open topic [14].

4.3 Load Balancing

NFs have due to their stateless design a fixed memory usage but stateless functions need a database to access when persistent information are needed. Furthermore, the processing load consumed by NFs might vary with increasing number of UEs. This can be the case for functions like the Access and Mobility Management Function (AMF) that is well frequented by UEs. An increasing number of requests on an NF might then cascade to other NFs or the underlying database and cause overflows or eventually crashes of the system. Therefore on one hand scalability mechanisms and on the other hand load balancing mechanisms are needed. In case of load balancing, a redundant NF has to be deployed and requests have to be split between. This has to happen automatically in order to ensure seamless operation. As a consequence, it is important for an underlying communication framework to give the possibilities to shift traffic to redundant instances as well as having mechanisms to observe the processing load and detect transgressions of

a critical threshold and finally automatic deployment mechanisms in order to spawn needed functions.
Different load balancing algorithms have already been studied in a local Core deployment [15] and with regard to the influence of cloud specific scaling policies [16]. An active research field is the integration of AI for autonomous scaling mechanisms [17].

4.4 Core-less Design

The architecture approach of a monolithic Core instance (even when it is internally split into a group of microservices) originates from previous generations of mobile communication systems, where the infrastructure as well as the entirety of network functionalities has been provided by a single party. Evolving towards a highly adaptive multi-tenant environment, in combination with a flexible network topology, the concept of a monolithic Core may come at question.
The trend of virtualizing NFs and moving parts of the Core deployment to the Cloud already decouples the concept of a Core instance from a centralized and closed network infrastructure. The borders of a Core instance are rather defined by the access to specific data domains or the affiliation to a RAN. By opening up specific data domains to additional applications deployed along NFs on the one side, and moving more and more RAN functionalities to virtual network functions on the other side, a more flexible definition of a Core's borders seems appropriate in order to provide further possibilities for the evolution of the network's capabilities. CtC, side links, radio backhaul and nomadic networks can be expected to expand the entire mobile communication system into a spatially distributed and dynamic network of services, NFs and RAN nodes. The increasing granularity of system components (a network is not anymore defined by big entities like gNBs and Core network) could bring the advantage of enabling highly adaptive deployments and interconnections of NFs.

4.5 Communication Performance / QoS / Timing Requirements

The communication requirements typically known from 5G are on the UP and categorized in slices. By doing so, similar QoS requirements are subsumed under one slice and by adapting the communication scheduling, the requirements are enforced. These UP based QoS requirements will endure in 6G and judging the current research trends for 6G, the QoS requirements have to be extended to the CP. This assumption is made due to the fact that trends like a Core-less or massively decentralized Core as well as virtualized RAN functionalities come with different communication requirements that have to be served in order to guarantee a correct operation of the network. Especially the RAN is QoS sensitive due to the time critical traffic in the Fronthaul as well as in the Midhaul, with the latter being less critical. Nevertheless, connecting the Fronthaul over the same communication framework as the Mid- and Backhaul is very questionable since the time and data requirements would most likely not allow the additional overhead induced by the extended feature set needed by Mid- and Backhaul.
When QoS requirements in the Core and RAN exist, functionalities have to be present to facilitate them and ensure the provisioning or handle a fault resolution. This includes a QoS monitoring that provides information to load balancing or scaling mechanisms, or operators in order to enable an automated and seamless provisioning of the required QoS. The provision of E2E network slices spanning RAN and Core for efficient resource utilization and security is likely to increase the demand for dynamic QoS configuration mechanisms on the CP, as for example proposed by [18].

5 Conclusion and Future Work

The manuscript at hand is intended as one partial step for the evolution from 5G to 6G. We focused to survey what influences the availability of data inside the system. The leading motivation was that currently CP & UP are isolated in a way that prevents beneficial operations – captured data cannot be shared, optimization across planes is obstructed, extension of the infrastructures management is inhibited, etc.. Hence, we investigated the architecture of 5G and its core, how services are logically interconnected and what technical tools are available for accessing and providing data. We discussed design principles that influence application interaction and how this ultimately impacts capabilities and properties of the entire infrastructure. Based on that, prerequisites are derived, which can enhance a developed communication system when incorporated.
Following steps are planned to make this gradually more concrete. We intend to more thoroughly outline required functionalities, define abstraction concepts to unite the single elements and develop a modular and flexible architecture. According to our current roadmap, solution candidates for individual tools will be investigated and novel approaches proposed for identified gaps.

Acknowledgment

The authors acknowledge the financial support by the German *Federal Ministry for Education and Research (BMBF)* within the project »Open6GHub« {16KISK003K}.

References

[1] M. Ehrlich, D. Krummacker, C. Fischer, *et al.*, "Software-defined networking as an enabler for future industrial network management," in *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, vol. 1, 2018, pp. 1109–1112.

[2] G. Mayer, "RESTful APIs for the 5G ServiceBased Architecture," *Journal of ICT Standardization*, vol. 6, pp. 101–116, Jan. 2018. DOI: 10.13052/jicts2245-800X.617.

[3] C. Zhang, X. Wen, L. Wang, *et al.*, "Performance Evaluation of Candidate Protocol Stack for Service-Based Interfaces in 5G Core Network," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2018, pp. 1–6. DOI: 10.1109/ICCW.2018.8403675.

[4] R. Bless, B. Bloessl, M. Hollick, *et al.*, "Dynamic network (re-)configuration across time, scope, and structure," English, in *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, (Grenoble, France, Jun. 7–10, 2022), IEEE, Jun. 2022, pp. 547–552.

[5] D. Krummacker, C. Fischer, Y. Munoz, *et al.*, "Organic & Dynamic Infrastructure: Getting ready for 6G," in *Mobile Communication-Technologies and Applications; 26th ITG-Symposium*, 2022.

[6] D. Krummacker, B. Veith, D. Lindenschmitt, *et al.*, "Radio Resource Sharing in 6G Private Networks: Trustworthy Spectrum Allocation for Coexistence through DLT as Core Function," in *1st International Conference on 6G Networking (6GNet 2022)*, 2022.

[7] D. Krummacker and H. D. Schotten, "Status-preserving, Seamless Relocation of Processes in Orchestrated Networks such as Organic 6G," in *5th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*, 2022.

[8] M. Corici, E. Troudt, P. Chakraborty, *et al.*, "An Ultra-Flexible Software Architecture Concept for 6G Core Networks," in *2021 IEEE 4th 5G World Forum (5GWF)*, 2021. DOI: 10.1109/5GWF52925.2021.00077.

[9] M. Corici, E. Troudt, T. Magedanz, *et al.*, "Organic 6G Networks: Decomplexification of Software-based Core Networks," in *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2022, pp. 541–546.

[10] M. Berndt, D. Krummacker, C. Fischer, *et al.*, "Unified Multi-Modal Data Aggregation for Complementary Sensor Networks Applied for Localization," in *95th IEEE Vehicular Technology Conference (VTC) 2022*, 2021, pp. 1–6. DOI: 10.23919/ICAC50006.2021.9594118.

[11] L. Ahrens, J. Ahrens, and H. D. Schotten, "Convolutional-type neural networks for fading channel forecasting," *IEEE Access*, vol. 8, 2020.

[12] D. Krummacker and H. D. Schotten, "InDeCo – Detach Communication from the Interconnection via an automatic zero-configuration, service-oriented Network Handling," in *Mobile Communication-Technologies and Applications; 25th ITG-Symposium*, 2021.

[13] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, *et al.*, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, 2021.

[14] S. R. Garzon, H. Yildiz, and A. Küpper, "Decentralized Identifiers and Self-sovereign Identity in 6G," *IEEE Network*, vol. 36, no. 4, 2022.

[15] V.-G. Nguyen, K.-J. Grinnemo, J. Taheri, *et al.*, "Adaptive and Latency-aware Load Balancing for Control Plane Traffic in the 4G/5G Core," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2021, pp. 365–370.

[16] J. Ortin, P. Serrano, J. Garcia-Reinoso, *et al.*, "Analysis of scaling policies for NFV providing 5G/6G reliability levels with fallible servers," *IEEE Transactions on Network and Service Management*, 2022.

[17] H. T. Nguyen, T. Van Do, and C. Rotter, "Scaling upf instances in 5g/6g core with deep reinforcement learning," *IEEE Access*, vol. 9, 2021.

[18] P. D. Bojović, T. Malbašić, D. Vujošević, *et al.*, "Dynamic QoS Management for a Flexible 5G/6G Network Core: A Step toward a Higher Programmability," *Sensors*, vol. 22, no. 8, p. 2849, 2022.