Hierarchical, Virtualized, and Distributed Intelligence 5G Architecture for Low-Latency and Secure Applications

M.S. Siddiqui, A. Legarrea, E. Escalona
Internet Architecture and Services (IAS), Fundació I2CAT, Barcelona, Spain

M.C. Parker, G. Koczian, S.D. Walker
University of Essex, Wivenhoe, Essex, CO4 3SQ, UK

G. Lyberopoulos, E. Theodoropoulou, K. Filis
COSMOTE Mobile Communications S.A., Athens, Greece

A. Foglar, M. Ulbricht
Innoroute GmbH, Munich, Germany

Y. Liu, J.C. Point
JCP-Connect, Rennes, France

E. Trouva
Inst. of Informatics & Telecommunications, National Centre for Scientific Research (NCSRD), Athens, Greece

Th. Rokkas, I. Neokosmidis
INCITES Consulting, Luxembourg, Luxembourg

D. Kritharidis, K. Katsaros, S. Spirou
Intracom Telecom, 19.7 Km Markopoulou, Peania, Greece

K. Habel, V. Jungnickel
Fraunhofer HHI, Berlin, Germany

C. Canales, M. Lorenzo
Ericsson, Madrid, Spain

***Abstract* — CHARISMA aims to tackle low-latency and end-to-end security for converged fixed/wireless 5G networks in order to meet the complex demands of emerging business paradigms, such as Smart Cities, eHealth, and Industry 4.0. In this paper, we present the key drivers and requirements towards a hierarchical, distributed-intelligence 5G architecture, supporting low latency, security, and open access as features intrinsic to its design. We also investigate the business perspective of the proposed 5G solution and the changes that can be foreseen for the telecom ecosystem.**

Keywords—5G, Converged Network Access, Virtualized Security, Multi-tenancy, Low Latency

I. Introduction

5G networking is a swiftly evolving and broad concept [1], encompassing *inter alia* seamless fixed-mobile convergence with Gb/s connectivity speeds over an intelligent open access (multi-tenancy) infrastructure. Integrating such diverse technologies into a single architecture with attendant software-defined networking (SDN) and networking functions virtualization (NFV) presents key technology challenges, while making issues such as security, energy efficiency, and scalability ever more critical. In this paper, we present the CHARISMA (Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access) project architecture, whose objective is the development of an open access, converged 5G network, via virtualized slicing of network resources to different service providers (SPs), with network intelligence distributed out towards end-users over a self-similar hierarchical architecture. Such an approach offers a means to achieve important 5G key performance indicators (KPIs) related to low latency, high and scalable bandwidths, energy efficiency and virtualized security (v-security). CHARISMA's ambitious approach for low latency and enhanced security builds upon present and future high-capacity developments that are currently being mooted for 5G deployment, such as 60 GHz/E-band, CPRI-over-Ethernet, cloud-RAN, distributed intelligence across the back-, front- and perimetric-haul, ad-hoc mobile device interconnects, content delivery networks (CDN), mobile distributed caching (MDC) and improved energy efficiency. In this paper we discuss how CHARISMA's architecture has been designed to satisfy key 5G drivers as well as make the architecture particularly applicable to variety of 5G related use case scenarios. The paper[§] is organized as follows. Section II describes CHARISMA's approach to the key drivers of the 5G paradigm. The 5G use cases, identified by CHARISMA, along with the extracted requirements are listed in Section III. Section IV details CHARISMA's multi-domain converged architecture and its control, management and orchestration plane. Finally, we conclude the paper in Section V with potential future work and directions of the project.

II. CHARISMA Key drivers

The CHARISMA architecture has been designed to achieve many of the 5G KPIs as defined by the 5G-PPP programme as well as other key technology drivers. In particular, CHARISMA has been designed to emphasise 3 specific important functionalities that are also considered to be key to many important vertical sectors and the provisioning of their supporting 5G services. These 3 functionalities are to be a low-latency network, featuring security and open access (multi-tenancy) operation. End to end network latency is vital to support the wide range of new use cases promised by 5G networks, such as remote surgery, self-driving cars, and public safety communications systems. Apart from the necessity of low latency, 5G network security operations require automation, robustness and on-demand protection from attacks and threats. The softwarization and virtualization of networks and network functions have made security a complex challenge for 5G networks thus a comprehensive approach to

[§]A reasonable amount of content of this paper has appeared as deliverable document, titled, D1.1 CHARISMA intelligent, distributed low-latency security C-RAN/RRH architecture, and as part of a paper submitted to EuCNC 2016.

end-to-end security for network resources, both physical and virtual is essential. A converged 5G infrastructure intrinsically possesses natural monopolistic characteristics, thus enabling its open access to multiple virtual network operators, has multiple social, economic and environmental benefits. The network sharing and multi-tenancy imply a single infrastructure provider (InP) serving several services providers, with physical infrastructure shared through the C&M systems, which becomes a fundamental enabler to provide required flexibility, elasticity, and programmability required for 5G access core networks.

In particular these three features, which CHARISMA has been specially designed to promote, are not necessarily compatible (or consistent) with each other (i.e. they can be somewhat self-contradictory, e.g. the desire for Open Access can potentially compromise security, if the architecture does not appropriately take this into account, e.g. via appropriate tenant isolation measures) and so impose their own additional constraints on how the architecture is best designed. Conversely, these particular features can also act to reinforce and help each other, e.g. the desire for end-to-end low latency can also act to assist in the secure operation of the network, e.g. by reducing the scope for interception or breakdown over long lengths of the topology, since low latency tends to require data to be processed (transmitted, etc.) as locally as possible to where it is required. These aspects and how they have influenced particular design choices in the CHARISMA architecture are examined in greater detail in later sections.

III. CHARISMA Use Cases and Requirements

Use Cases

The CHARISMA use cases have been selected to highlight the main drivers of the project (see Figure. 1), as discussed in Section II, including: support of low latency, multi-tenancy, and enhanced security, while being in-line with the UC families described by NGMN [1]. The purpose of these use cases is twofold:

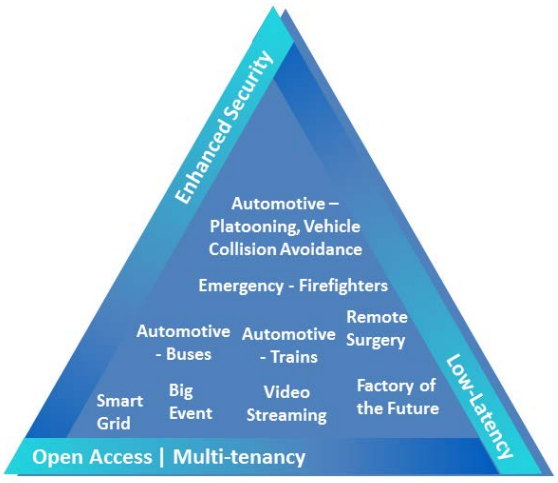

Figure 1: CHARISMA use cases and drivers

- To highlight how the key innovations of CHARISMA architecture will benefit the various stakeholders (e.g., end-users, network/service providers) involved.
- To be used to define the widest range of performance and functional requirements that the CHARISMA architecture should meet.

1. **High-speed railway services:** This use case demonstrates CHARISMA's support for high capacity and high data transmission rate for innovative railway services and applications for high-speed trains as foreseen in converged 5G networks.
2. **Secure high bandwidth service continuity in public transport:** The objective of this use case is to ensure 5G networks can provide optimized and secure Internet access in the public transport such as buses. The use case focuses on CHARISMA's ability to ensure user's service continuity with low service latency, in a secure multi-tenant environment, for the mobile scenario of a bus transport system.
3. **Big Event:** This use case aims to ensure that 5G networks can support big events, located in confined spaces such as concert halls, stadiums, theatres, etc. The problem is to correctly dimension the infrastructure to offer high quality services while optimizing costs. Typically, most of the time the equipment will be unused while during short periods of time requirements will be very high (during the event). Therefore, dynamic re-configurability and infrastructure sharing (multi-tenancy) are key features to optimize resource utilization.
4. **First Responders' Communications:** Critical communications in emergency cases are the focus of this use case. In such events the overall goal is that emergency services such as fire fighters, police, rescue, first aid and others should have the best possible communication available. CHARISMA particularly considers large, unpredictable events, as they pose highest challenges to the communication infrastructure. The use case will show the benefits of the intelligent Remote Radio Head (iRRH) capabilities. However, the main challenges are the ad-hoc nature of the communications infrastructure and the need for secure communications to mitigate malicious or unintentional impairment of the responders' work. Responder-to-responder communications and relaying for wider area coverage, offloading, and resilience must also be considered.
5. **Factory of the Future (IoT):** The objective of this use case is to evaluate and ensure that CHARISMA can support the industrial Internet (Industry 4.0 [12]) by providing secure and low latency connectivity. The 5G network should support off-loading of a control loop calculation as well as industrial production, while still keeping the security and latency requirements.
6. **Advanced video streaming:** This use case demonstrates CHARISMA's support for live video streaming with virtual edge resources, such as network caches, for reducing latency and offloading the core network in a

multi-tenant environment. The use case focuses on the advantages brought by virtualization such as the dynamic instantiation of (differentiated) service instances, the on-the-fly resource (de-)allocation (scale-up/down).

7. **Remote Surgery:** This use case demonstrates CHARISMA's ability to ensure support for the vertical industry of health in the area of remote surgeries by guaranteeing low latency communication with high availability, reliability and security.
8. **Smart Grid:** This use case confirms CHARISMA's ability to provide a programmable and flexible network architecture providing low latency, security, QoS, and high reliability for Smart Grid applications and services in electricity distribution networks.
9. **Intelligent transport services (ITS) / collision avoidance:** This use cases highlights CHARISMA's support for advanced ITS innovative services/applications necessitating the exchange of information among the vehicles in real-time under strict delay constraints among the vehicles and the central infrastructure.

Requirements and Challenges

The abovementioned use cases facilitate the requirement elicitation for the CHARISMA architecture. In the requirement analysis process, the similar requirements, belonging to different use cases, are merged and in case where different KPIs are considered for the same requirement, the most stringent KPI is taken into account. Following are the high-level consolidated requirements for CHARISMA:

- Support for low latency services: CHARISMA architecture shall support low latency services ($\leq$ 1ms) via, i) Routing of data at the lowest common aggregation point, ii) devolved offload strategies for device-to-device, device-to-remote-radio, device-to-baseband, device-to-central office/metro, etc., and iii) mobile distributed caching.
- Support for advanced end-to-end security: CHARISMA architecture shall support distributed security as well as physical layer security. The CHARISMA virtualized open access architecture level design need to have a holistic security approach for the control and management plane as the underlying infrastructure is virtualized and shared among different SPs who operate simultaneously on the same physical resources.
- Support for open access: CHARISMA's architecture shall enable ubiquitous multi-provider, multi-user, multi-technology, and multi-service scenarios. The open access enabled infrastructure should have a unified virtualized network management system capable of allocating slices and offering accessible service interfaces for novel and differentiated services to end-users, as the basis for supporting innovative business models. The infrastructure owner has to be able to offer its virtual resources in a way that multiple operators can coexist and function independently from each other. To this end, virtual resources should be easily bundled together into slices of the physical infrastructure so that each slice constitutes an independent virtual edge network and cloud for a virtual network operator.
- Support for high data-rates: CHARISMA's architecture shall support data-rates up to 10 Gb/s for SMEs and residential users and up to 1 Gb/s for mobile end-users, through the use of a hierarchical intelligent data processing approach at the C-RAN and RRH, where statistical multiplexing, aggregation, and caching allow access data volumes to be significantly increased.
- Support for seamless and ubiquitous connectivity: The system proposed by CHARISMA shall be able to offer seamless and ubiquitous 5G services in both densely- and under-populated areas thanks to a highly diversified (heterogeneous) networking architecture (including 60 GHz and optical LoS communications) with higher bandwidths available in the wireless/fixed access networks.
- Support for virtualization of resources: CHARISMA's architecture shall make extensive use of resource virtualization. The Virtualized Infrastructure (VI) group will virtualize the hardware resources (computing, storage, and network) via e.g. a hypervisor at the Virtualization Layer, which pools the resources and exposes them for consumption by VNFs. The Virtualized Network Functions (VNFs) group comprises software components that implement network functions destined to run on the VI.
- Support for QoS: CHARISMA's architecture shall support several QoS classes for emergency communications, assigning to users different levels of priority.
- Support for advanced D2D communications: In CHARISMA's architecture each iRRH shall be able to establish and manage a D2D mesh network, to enable low latency D2D communication. In addition, each iRRH shall be able to connect to other iRRHs in case of emergency and establish a CAL1 mesh network between several iRRHs.
- Support for intelligent routing: When appropriate, traffic should be routed as close to the edge as possible to minimize hops and hence traffic impairments.
- Support for high availability: All network elements employed in CHARISMA's architecture shall have an availability of 99.99%.
- Support for high reliability: All network elements employed in CHARISMA's architecture shall have a reliability of 99.99%.

IV. The CHARISMA Approach

Business Perspective

The telecommunication market is a highly competitive environment that is characterized by continuous changes in terms of technology evolution and user preferences. The pure voice oriented mobile networks (2G) of the previous decades have evolved to data networks (3G & 4G). 5G is envisioned as the technology that will connect a huge number of end-devices

in a fully connected future. 5G will be the backbone of the future digital society since it will interconnect almost every device, sensor, etc. leading to growth and impact not just on telecom sector but also creating new business opportunities.
The business model regarding mobile networking is evolving alongside: initially the Network Operator and the End Users were the main stakeholders of the value-chain. Nowadays, new actors such as Content Providers, Over-The-Top (OTT) players, are arising. One of the biggest changes of 5G will be the transformation of connectivity and this will lead to changes related to business models.
As described in previous sections more and more of the functionalities will be moved from the Central Exchange (CE) to other parts of the network. Virtualization will be present in most of the network elements. NFV will enable to use common hardware with ease of deployment, scalability and reduced costs to achieve required network elements functionalities. Additionally, NFV combined with SDN, will lead to a reduction of CAPEX and OPEX, and will optimize the operations and reduce the time to market for new actors.
A new eco-system with new players alongside the traditional ones will arise. A huge amount of CAPEX will not be necessary in order to enter the market and most of the costs will be OPEX related. Competition will move to the SW domain: SMEs developing new functions will have an opportunity to enter the market, while HW vendors will move their business closer to SW development.
Open Access is an essential feature of CHARISMA ecosystem as it opens the market to multiple operators who will control their set of virtual resources by the appropriate interfaces.
CHARISMA characteristics will lead also to the creation of new business innovation by involving vertical sectors such as Health, Factories of the Future, Energy, Automotive etc. that require low latency, high security and open access. For example, low latency will lead to new applications that require almost real time control and information flow (remote surgery, ITS/collision avoidance); Security will lead to new use cases regarding Factories of the Future such as internet based manufacturing and will lead closer towards Industry 4.0.; Open access provides the basis for multi-tenancy.
CHARISMA architecture will lead to cost efficiency, in terms of total cost of ownership and costs associated with control and management (C&M) of the network. The different topics that will be researched regarding the business perspectives of CHARISMA among others include: new tariff and pricing models, charging mechanisms, demand forecasting for services. Finally, a detailed techno-economic analysis of the CHARISMA solution will be performed and guidelines will be extracted.

CHARISMA Main Actors

Within CHARISMA scope the following actors have been identified (cf. Figure 2):
Network Operator (NO): This actor owns all the infrastructure and telecommunication related equipment. The NO is also the entity that operates CHARISMA on top of its infrastructure. The infrastructure is virtualized and mapped into a pool of available resources that are offered to the virtual network operator(s). It provides all the different flavors of X-as-a-Service model (XaaS).

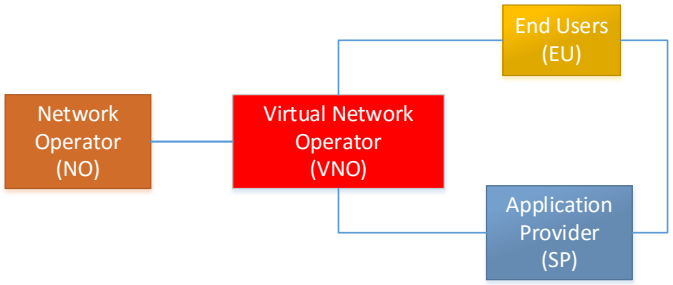

Figure 3: Interaction between CHARISMA actors

Virtual Network Operator (VNO): This actor provides connectivity to end users in retail and/or wholesale markets using the virtual resources from the NO, as a slice. A VNO can offer different application services with features including high security, low latency etc. to the end user.
Application Provider (AP): An entity that provides specialized and enhanced services (e.g. platforms for remote surgery or automotive industry, content delivery) to users such as Business-to-Business or Business-to-Customer. Often, an SLA contract is signed between the AP and the VNO.
End Users (EU): End users of the CHARISMA services, they can be either simple end users or an entity (e.g. automotive company, factory, hospital, bus company etc.)

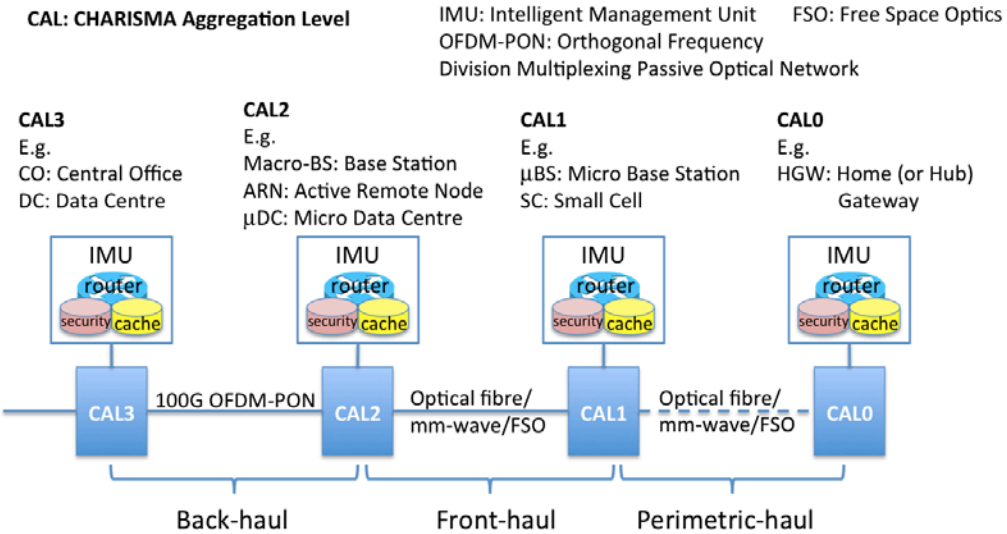

Figure 2: Hierarchical CHARISMA Aggregation Levels (CALs)

Figure 2 represents a simple model describing the interactions between the actors. CHARISMA will study in detail different scenarios, relations and interactions between the actors.

Architecture Definition

A key architectural innovation of CHARISMA is the adoption of a self-similar hierarchical approach, with active nodes intermediate to the central office (CO) and end-users. The CHARISMA 5G architecture described has been designed to exhibit low-latency (towards the 1-msec KPI of the 5G-PPP programme) as well as security and open access. Achieving low latency requires data to be handled (i.e. routed and/or processed) as close to where it is required (i.e. either at the receiving end, and/or at the source end). Indeed, this implies that a low-latency architecture requires network intelligence to be located as close to the edge as possible, such that traffic which is expected to remain local never needs to travel towards the core of the network; minimizing transmission latency. Likewise, in cases where data is frequently required (e.g. from a popular video streaming source) it makes sense to store that video data at a location close to where it is frequently accessed; in such a way, access time latency can also be minimized. Overall, this requires the CHARISMA architecture to be much more distributed in nature, as compared to more centralized 5G architectures, e.g. as typically exemplified by the purely C-RAN architecture, where intelligence is almost completely located in the Central Office (or Central Node). The legacy C-RAN network might also have had some limited storage at the RRH (equivalent to CAL2 in Fig. 3), CHARISMA's much more distributed and hierarchical approach sees such intelligence, processing and caching (i.e. in the IMU at each CAL node) pushed out also to the small cell (CAL1 at the rear of the bus) and at CAL0.

Thus, the CHARISMA architecture is therefore also anticipating developments in cloudlet and fog computing. To that end, we have designed the CHARISMA architecture to be hierarchical, with a set of self-similar intelligent aggregation nodes located between the CO and end-users. Each node is labeled a Converged Aggregation Level (CAL) and is designated with a number, to signify its level in the hierarchy. Each active node (i.e. CAL) has its own scalable intelligent management unit (IMU) performing data storage/caching, processing and routing functionalities.

CHARISMA consists of a multiple number of diverse and innovative hardware technologies, whose functionalities are key to enabling the low-latency, open access, and secure data transmission required in future 5G networking. These device elements include the **TrustNode** router for low-latency and secure routing; **accelerated network interface card (NIC)**; **device-to-device (D2D)** communications, for low latency featuring local (distributed) security; offloading and hierarchical **caching**, to enable low-latency video distribution and network load balancing; **mobile cloud** for low latency and scalable (virtualized, as required) networking functions; **Ethernet fronthaul** based on OFDM-PON and NG-PON2 technologies, for low latency, low cost and resilient RRH connectivities; and **reliable low-latency backhaul** providing open access connectivity between the RAN and the core network. Together, these technologies comprise an important aspect to the CHARISMA data plane architecture and depending on the requirements of the VNO, may or may not be part of its respective network slice. These CHARISMA network elements, physical or virtual, are managed and controlled by a centralized CHARISMA control plane, described next.

The high-level design of the CHARISMA control, management, and orchestration plane is shown in Figure 4. It closely follows the ETSI NFV architecture [9] as the latter is a standard that has been developed internationally over several years and is geared towards virtualization and multi-tenancy. Moreover, the ETSI NFV architecture comes with background work on security [10] and performance [11]. The architecture consists of four groups of components[1]: Virtualized Infrastructure (VI); Virtualized Network Functions (VNFs); Management and Orchestration (MANO); and Operations and Business Support Systems (OSS/BSS).

The VI group virtualizes the hardware resources (computing, storage, and network) via e.g., a hypervisor at the Virtualization Layer, which pools the resources and exposes them for consumption by VNFs. The hardware resources constitute the CHARISMA access network, with the addition of an IMU at each CAL. The IMU models computing and storage resources that are either spare within access network equipment (e.g., BSs) or introduced with commercial off-the-shelf hardware (e.g., servers). The VNFs group comprises software components that implement network functions destined to run on the VI (and finally on the IMUs). CHARISMA looks specifically to implement VNFs for caching, switching, and security. However, any other network function, e.g., CDN, would be able to run on the VI.

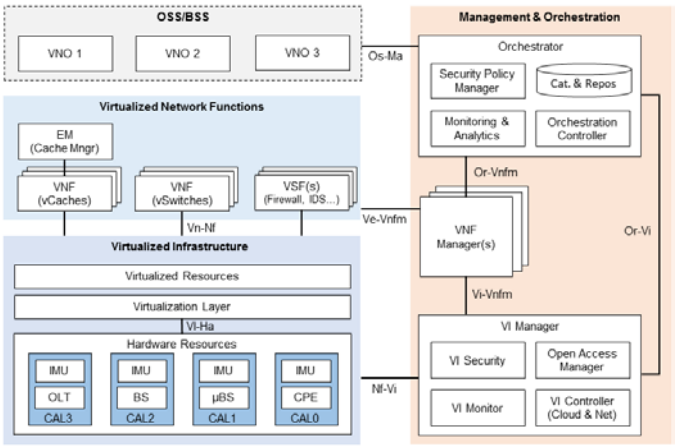

Figure 4: High-level CHARISMA control, management, and orchestration plane

The MANO group includes components for the combination of VNFs into graphs implementing network services, the lifecycle management of VNFs, the coordination of allocating VNFs to virtualized resources, the homogenized control and management of the hardware resources, and the slicing of resources for supporting multi-tenancy. MANO operates under the policy set by the owner of the hardware infrastructure and communicates with the OSS/BSS of VNOs to report status and possibly to receive requirements. Apart from the general policies, the VNO can also select predefined security policies

[1] CHARISMA focuses on the first three groups in an effort to enable multiple VNOs at the OSS/BSS who will be sharing the hardware resources at the VI.

to be applied to resources or services under its control. The Security Policy Manager module manages the configured security policies at service and resource level (cf. Fig. 4). The Monitoring and Analytics module provides input to the Security Policy Manager based on the current monitoring information for a particular service or resource in order for the Security Policy Manager to take next best action according to the configured policy.

In the rest of this section, we elaborate different features of CHARISMA architecture in light of the three main functionalities, low-latency, security and open access, CHARISMA aims to achieve.

Low Latency

CHARISMA targets end-to-end low latency with a multiple prong approach including, cooperative hierarchical caching and routing, hardware acceleration, and high data throughput in the aggregation network.

CHARISMA offers a unified content delivery solution in the access and aggregation networks, and for device-to-device (D2D) communications latencies towards the 1-msec 5G KPI. CHARISMA caching solution is based on cooperative hierarchical caching, i.e., caching decisions are made both locally and globally at each cache. Beyond CDN, the concept of in-network caching and information centric networking (ICN) also allows cache functionalities to reside at network devices like routers, switches, etc. [2]. The latter allows such devices forming the CHARISMA hierarchical in-network caching system to be controlled through a centralized SDN controller that can be used to manage/control content replicas by keeping track of the location and availability of content in distributed locations. By differentiating the forwarding data paths, the SDN cache controller is able to realize a better load balancing and reduce redundant content stored in the network. However, the traditional Internet was designed for e2e communication with content being intrinsically linked to its location – indeed, up to now, security mechanisms have also tended to be designed to be tightly coupled to the physical location of a host. ICN decouples data from the host, thus providing new opportunities for networking entities that can implement in-network caching functionalities [3] to reduce mean client latency by serving content near end-users.

As part of its architectural approach to reducing latency, CHARISMA also employs TrustNode technology [4] representing a router for radio access networks offering a port-to-port latency of less than 3µs. To realize this, target data path circuitry is optimized at the register level, while a novel, IPv6-based routing concept is introduced which uses a self-routing mechanism, where the destination of a packet is contained in the routing address. The hierarchical architecture allows data to be routed via the lowest common CAL. No time-consuming table look-up or search algorithm is necessary for the forwarding decision. In parallel, a novel traffic management concept is explored with a QoS control mechanism providing smooth packet streams, which avoid large buffer fill and resulting packet delay variation (jitter). The hierarchical cluster of TrustNodes is configured to allow short paths and local content caching, with redundancy and dynamic load sharing also supported.

The trend for next-generation 5G technologies to employ software-based NFV unfortunately tends to increase latencies due to the higher CPU utilization required to implement an all software-based networking function. To mitigate this trend, CHARISMA also proposes the use of a smart network interface card (NIC) armed with NFV acceleration for the data path as a means to reduce latency, power consumption, and also CAPEX.

In the back-haul or aggregation network, respectively, CHARISMA is investigating OFDM-PON technology [5], both as a means to achieve high data throughputs at a low cost and as a means to reduce network latency. Key parameters here are an aggregated data rate of 100 Gb/s together with 1024 subcarriers providing an additional degree of freedom for media access to provide effective virtualization. Here, latency is dominated by input buffering, error correction, and synchronization. Simulations show a processing delay due to MAC and PHY signal processing in the low µs range, which is already well below the propagation delay of 50 µs for a 10-km fibre connection. In order to reduce the costs at the Optical Network Unit (ONU), CHARISMA is also investigating new concepts, where only parts of the OFDM spectrum are received and processed.

Security

In 5G networks, chaining of physical network functions and virtual network functions within a network service imposes a holistic approach to achieve end-to-end security. Virtualized security (v-security) is a vital part of 5G network service provisioning, and the CHARISMA architecture approaches v-security via intelligent security management, tenant isolation, Virtual Security Functions (VSFs), authentication, and authorization. Amongst the advantages brought by NFV are the agility and adaptability offered to meet service delivery requirements that is achieved through the orchestration of the available resources. CHARISMA adopts a policy-driven approach, via the Security Policy Manager (cf. Fig. 4), to orchestration and support for intelligent security management capabilities. The orchestrator can receive security rules and policies set by a SP, and based upon monitoring information collected from the already deployed services, through the Monitoring and Analytics (cf. Fig. 4), it can detect possible security threats. Depending on the security policy selected, the orchestrator creates security profiles that differentiate on the decisions taken for required counter measures appropriate to address a particular threat. Examples of such decisions are: the configuration, termination, scaling or migration of an already deployed service; and the deployment of new security services, which through proper placement of VNFs, will attempt to prevent, neutralize or respond to a specific attack.

Moreover, the security-related VNFs developed in CHARISMA are designed to implement or assist virtualized security functions (i.e. VNFs) such as: intrusion detection, firewalls, and deep packet inspection (DPI). That is, a network service may be composed of one or more security VNFs according to the differing virtual network operators (VNO) specifications, ensuring the individual v-security requirements. CHARISMA foresees authentication and authorization at infrastructure level, both virtualized and physical, i.e., every virtual and hardware component has to be authenticated. The

VNOs need to be authenticated and allowed access to authorized virtual network resources only. In this regard, CHARISMA provides a comprehensive authorization and authentication solution facilitated with a trust framework. Furthermore, CHARISMA also exploits MACsec [8] for authentication and encryption for MAC layer security. Other VNFs implemented in CHARISMA are directed towards vCPE, SDN control, and content caching. Security of ICN-based architectures is still relatively immature; however some directions have been proposed [7] to extend protocols (i.e. OpenFlow) where content can be encrypted through a digital signature with the private key of the content originator, thus enforcing confidentiality, traceability and content access feedbacks. Here we envision distributed caching security as a virtualization of the network layer and cluster encryption at the physical layer in order to also greatly reduce content access latency for both mobile and fixed networks.

Open Access/Multi-tenancy

The CHARISMA open access solution allows infrastructure providers to share resources among multiple VNOs, thereby leveraging down CAPEX and OPEX, as well as achieving more efficient operation of the network using a centralized control and management system for all resources involved. It supports different network instances, called network slices that share a common pool of resources but have different characteristics in order to support the different network service needs. Motivated by its open access virtualization platform through the use of Software Defined Networks (SDN), Network Functional Virtualization (NFV), and network slicing, concepts that enables a new SP to propose new services, without the need to negotiate with the operator for a slice of physical infrastructure, therefore opening the market to multiple VNOs in a secured and segregated manner. More specifically, the VNFs consist of software components running on top of the CHARISMA virtualized infrastructure, with the VNFs implementing common network functions traditionally carried out by specialized hardware devices, and are deployed on top of commodity (i.e. off-the-shelf) IT infrastructure equipment. The CHARISMA open access solution ensures that the VNFs operated by a particular VNO are deployed on virtual resource belonging to the network slice of the respective VNO while maintaining isolation among the different tenants of the CHARISMA network.

V. Conclusions

This paper presented a virtualized hierarchical and intelligent 5G access network architecture, based on hierarchical CAL and flexible IMU technology, suitable for services and applications requiring low-latency, enhanced security, and multi-tenancy. To achieve the low-latency requirements, CHARISMA explores hierarchical routing with in-network caching, NFV acceleration for data paths using smart NICs, and OFDM-PON technology. In order to meet the enhanced security (both physical and virtual) and multi-tenancy challenges, the proposed architecture employs network slicing concept along with SDN and NFV principles.

In this paper, we have also listed various use cases, where CHARISMA's innovation architecture can play a vital role for enabling required 5G networking solutions. The requirements extracted from these use cases allowed to refine the CHARISMA architecture.

The CHARISMA project consortium plans to demonstrate the proof of concept, for the three main drivers (low-latency, enhanced security, & open access/multi-tenancy), by end of this year. CHARISMA is an ongoing research project and latest updates can be found in [13].

Acknowledgment

We like to acknowledge the efforts of all the partners of the CHARISMA project consortium. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 671704.

References

[1] NGMN 5G white paper. [Online] https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0_01.pdf

[2] Diego Perino and Matteo Varvello, "A reality check for content centric networking". In Proc. of ACM SIGCOMM workshop on Information-centric networking (ICN 11). ACM, New York, NY, USA.

[3] Lee *et al.*, "User-assisted in-network caching in information-centric networking" Computer Networks. 2013, 57(16):3142–3153.

[4] Inno Route IPv6 Router. [Online] https://www.innoroute.com/sites/default/files/ResearchRouter_flyer.pdf

[5] L. Fernandez del Rosal and K. Habel, "Real-time OFDMA for Flexible Optical Access at 64 Gbit/s," Photonische Netze Beiträge der 15. ITG-Fachtagung, pp. 70–74, 2014.

[6] 802.1AE Standard: Media Access Control (MAC) Security. [Online] http://www.ieee802.org/1/pages/802.1ae.html

[7] Mangili *et al*. "Information centric networking over SDN and OpenFlow: Architectural aspects and experiments on the OFELIA testbed" Computer Networks. 2013, vol. 57, p. 3207-3221

[8] J. Ferrer Riera *et al*., "Software-defined wired-wireless access network convergence: the SODALES approach", *IEEE Globecom*, pp.1522 – 1527, Austin, TX, Dec. 2014

[9] Network Functions Virtualisation (NFV); Architectural Framework, ETSI Standard GS NFV 002, 2014.

[10] Network Functions Virtualisation (NFV); NFV Performance & Portability Best Practises, ETSI Standard GS NFV-PER 001, 2014.

[11] Network Functions Virtualisation (NFV); NFV Security; Problem Statement, ETSI Standard GS NFV-SEC 001, 2014.

[12] 5G and the Factories of the Future. [Online] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Factories-of-the-Future-Vertical-Sector.pdf

[13] Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access - CHARISMA. [Online] http://www.charisma5g.eu/