CHARISMA: Converged heterogeneous advanced 5G cloud-RAN architecture for intelligent and secure media access

Conference Paper · June 2016

DOI: 10.1109/EuCNC.2016.7561040

CITATIONS
8

READS
441

28 authors, including:

Michael Charles Parker
University of Essex
147 PUBLICATIONS **973** CITATIONS

SEE PROFILE

Geza Koczian
University of Essex
12 PUBLICATIONS **61** CITATIONS

SEE PROFILE

T. Quinlan
University of Essex
90 PUBLICATIONS **528** CITATIONS

SEE PROFILE

CHARISMA: Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access

M.C. Parker, G. Koczian, F. Adeyemi-Ejeye, T. Quinlan, S.D. Walker
University of Essex, Wivenhoe, Essex, CO4 3SQ, UK
mcpark, gkoczi, aoteje, quinlan, stuwal@essex.ac.uk

A. Legarrea, M.S. Siddiqui, E. Escalona
Internet Architecture and Services (IAS), I2CAT Fundació, Barcelona, Spain
amaia.legarrea, shuaib.siddiqui, eduard.escalona@i2cat.net

S. Spirou, D. Kritharidis
Intracom Telecom, 19.7 Km Markopoulou, Ave., 190 02 Peania, Greece
spis, dkri@intracom-telecom.com

K. Habel, V. Jungnickel
Fraunhofer HHI, Berlin, Germany
kai.habel@hhi.fraunhofer.de

E. Trouva, A. Kourtis
Inst. of Informatics & Telecommunications, National Centre for Scientific Research (NCSRD), Athens, Greece
trouva, kourtis@iit.demokritos.gr

Y. Liu, M. Sander Frigau, J.C. Point
JCP-Connect, Rennes, France
yaning.liu, matthias.sanderfrigau, pointjc@jcp-connect.com

G. Lyberopoulos, E. Theodoropoulou, K. Filis
COSMOTE Mobile Communications S.A., Athens, Greece
glimperop, etheodorop, cfilis@cosmote.gr

Th. Rokkas, I. Neokosmidis
INCITES Consulting, Luxembourg, Luxembourg
trokkas, i.neokosmidis@incites.eu

D. Levi, E. Zetserov
Ethernity Networks Ltd., Lod, Israel
vidi.levi, eugene@ethernitynet.com

A. Foglar, M. Ulbricht
Innoroute GmbH, Munich, Germany
foglar, ulbricht @innoroute.de

B. Peternel, D. Gustincic
Telekom Solvenia, Ljubljana, Slovenia
blaz.peternel, david.gustincic@telekom.si

***Abstract*—5G networks aims to tackle the complex demands of emerging business paradigms, such as Smart Cities, eHealth, and Industry 4.0. In this paper, a hierarchical, distributed-intelligence 5G architecture is described, offering low latency, security, and open access as features intrinsic to its design. SDN and NFV principles are employed to create a networking solution applicable to a large number of high-specification 5G use case scenarios.**

Keywords—5G, Converged Network Access, Virtualized Security, Open Access, Low Latency

I. Introduction

5G networking is a swiftly evolving and broad concept [1], encompassing *inter alia* seamless fixed-mobile convergence with gigabit/s connectivity speeds over an intelligent open access infrastructure. Integrating such diverse technologies into a single architecture with attendant software-defined networking (SDN) and networking functions virtualisation (NFV) presents key technology challenges, while making issues such as security, energy efficiency, and scalability ever more critical. CHARISMA's objective is the development of an open access, converged 5G network, via virtualised 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 virtualised 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. This paper introduces CHARISMA's architecture along with its key drivers and provides some insights into its 5G related use cases. The paper is organized as follows. Section II describes CHARISMA's approach to the key drivers of the 5G paradigm, and then Section III details CHARISMA's multi-domain converged architecture and its control, management and orchestration plane. The 5G use cases of CHARISMA are identified in Section IV. Finally, we conclude the paper in Section V with insights into the future work.

II. CHARISMA Key drivers

The CHARISMA architecture design to achieve the 5G KPIs is founded upon a variety of key technology drivers, which we describe in greater detail in the following sections:

A. Low Latency and Content Caching

While successfully offering higher bandwidth capacities, service latency in LTE networking is still highly dependent on the distance between the data center and the exchange point where the mobile network connects to the Internet. Network backhaul bandwidth can also be heavily consumed by duplicated data-streams when content (e.g. highly-popular video streaming) is requested simultaneously and frequently. CDN caching schemes are a cost-effective solution, replicating popular and frequently-demanded content in IP-based LTE network elements closer to mobile users, to reduce both service latency and mobile backhaul traffic. CHARISMA therefore offers a unified content delivery solutions in the access and aggregation networks, and for device-to-device (D2D) communications latencies towards the 1-msec 5G KPI. Caching functionality can be enabled in user devices (smart phones or tablet), customer premises network (STBs and APs), access network (digital subscriber line access multiplexer (DSLAM), C-RAN or eNodeBs), and aggregate network (access gateways). 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 end-to-end 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. But, the original content producer therefore loses control over the data it pushed in the network, which raises new security concerns especially in terms of privacy and traceability [4]. One of the major issues is the lack of centralization for authentication, content access feedback and security, making it impossible for network administrators to improve services that they provide to end-users [5]. Hence, the design of 5G security protocols is also a key aspect to CHARISMA, as discussed in the next section.

As part of its architectural approach to reducing latency, CHARISMA also employs TrustNode technology [6] 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 CHARISMA aggregation level (CAL) described in greater detail in section III. 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 is proposing 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 [7]. 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 synchronisation. 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 ONU, CHARISMA is also investigating new concepts, where only parts of the OFDM spectrum will be received and processed.

B. Security and Virtual Security Functions (VSFs)

Today's network security operations require automation, robustness and on-demand protection from attacks and threats. NFV enables service providers to deliver security as virtual network functions (VNFs) with centralized control and distributed enforcement. 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, 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 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, it can detect possible security threats. Depending on the security policy selected, the orchestrator creates security profiles that differentiate on the decisions taken for the 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. Utilization of the vCPE platform opens the door for operators to propose advanced services based on an open platform, and aims to consolidate above-L2 functions using VNFs, assisted by smart NIC technology to reduce latency. The CHARISMA vCPE architecture offers advanced high-speed higher layers security, such as firewall, parental control, and application security running on COST

servers, with Layer 2 secure communication between vCPE and physical CPE based on IP or MACsec encryption for all payloads. This platform enables maximum flexibility and programmability to offer future upper layer security options.

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 (VNOs) 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 based on Pretty Good Privacy (PGP) and web of trust (WOT) techniques. 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 [9] 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.

C. Open Access

A converged 5G infrastructure intrinsically possess natural monopolistic characteristics, such that ensuring its open access has multiple social, economic and environmental benefits. However, open access also presents its own security challenges, for all actors, which are also addressed by CHARISMA. Motivated by its open access virtualization platform through the use of SD-WAN (software-defined wide area networking) and vCPE a concept that would enable a new SP to propose new services over the internet, CHARISMA provides an architecture solution without a 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. Thus 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. 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.

III. CHARISMA 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. Each active node (i.e. CAL) has its own scalable intelligent management unit (IMU) performing data storage/caching, processing and routing functionalities.

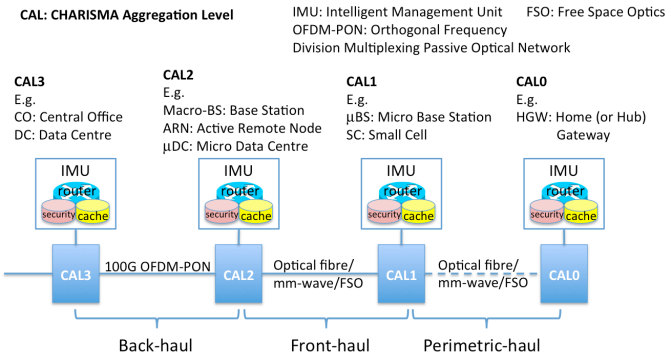

Fig. 1: Hierarchical CHARISMA Aggregation Levels (CALs)

This means that data is routed, where possible, at the lowest common aggregation point, to assist in achieving low-latency networking. For example, for D2D communications, data is routed directly between the devices, whereas routing at the lowest CAL, e.g. at CAL0 (see Figure 1), means the data is routed between devices via the local (e.g. home or access) gateway. For devices within a micro-cell, routing is via the CAL1 level; within a macro-cell, it is via the CAL2 level, e.g. at the macro base station (BS) or active remote node [10]; and finally for non-local routing, this is performed at the CAL3 level, at CO or DC. Distributing intelligence ever closer to the end-user assists in reducing network latency, and allows for more precise SDN and NFV control of the CHARISMA 5G network.

The high-level design of the CHARISMA control, management, and orchestration plane is shown in Figure 2. It closely follows the ETSI NFV architecture [11] 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 [12] and performance [13]. 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

[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.

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. 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.

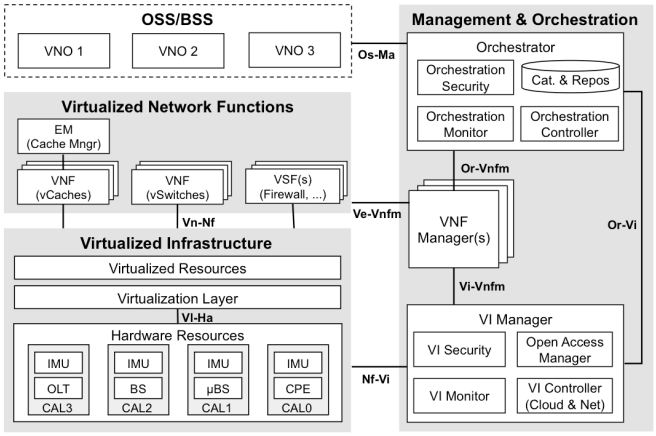

Fig. 2: High-level CHARISMA control, management, and orchestration plane

IV. Outline UCs of CHARISMA

The CHARISMA use cases have been selected to highlight the project's two most important innovations: support of low latency and enhanced security, while being in-line with the UC families described by NGMN [14].

A. *Intelligent transport services (ITS) / collision avoidance*

5G will enable the provision of advanced ITS innovative services/applications necessitating the exchange of information among the vehicles in real-time under strict delay constraints among the vehicles. The provisioning of vehicle related information (timestamp, location, speed, bearing, altitude, acceleration/deceleration etc.) can be communicated either directly (D2D) to other vehicles or via 5G. Example ITS services that could be offered are: (i) Real time positioning of vehicles moving in the vicinity (same direction, within a certain distance depending on the speed); (ii) Detailed information (e.g. speed, distance, acceleration/deceleration) regarding the vehicle in front (on the same lane); (iii) Visual and/or audio alerts in case of an imminent collision; (iv) Live streaming content ("See-What-I-See") from the vehicle in front (same lane, within a certain distance depending on the speed); (v) Hazardous event and obstacle recognition – see stopped vehicle ahead in dead spot, vehicle ahead moving with an extremely slow speed; (vi) Personalized "time to destination" based on driver profile/behavior (average speed, average number of line changes, etc.) and current traffic statistics. Additional applications could include the automated upload of HD video/audio streaming to the nearest PSAP (Public Safety Answering Point) in case of an accident.

B. *Communications in public transport*

Offering service continuity and high QoS to commuters in moving vehicles is a challenge due to the varying network conditions/performance (coverage, throughput, latency). Since public transport vehicles (buses, metro, high-speed trains) are generally operated along a fixed rail/route and timetable, network resources usage optimization and lower latencies can be achieved by introducing intelligent network services such as caching and flexible routing in addition to the deployment of open access solutions (AP/BS, C-RAN) and D2D communication services, e.g. see Fig.3.

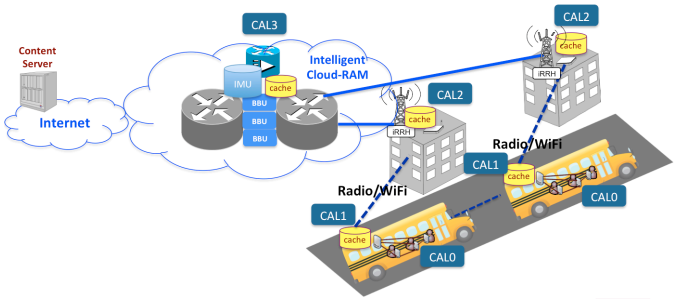

Fig. 3: Public bus transport

More specifically, service continuity and high QoS can be achieved via: (i) D2D communications, to reduce network resources in case of traffic jams, (ii) Intelligent cache functionalities, to address content high demands of bandwidth and latency and (iii) Cloud-based flexible and dynamic deployment of media services, to ensure service continuity especially in cases of vehicular high mobility.

C. *First responders' communications*

First responders (police officers, paramedics, firefighters, etc.) among the first to arrive/operate at the scene of an emergency (car accident, natural disaster, terrorist attack) need to communicate in real-time with each other and with more operations centres. Towards this end, first responders are equipped with audiovisual capture and display devices (cameras, headsets, displays) and with wireless transceivers (cellular, WiFi), while a micro-BS on their vehicle (fire engine or mobile operations centre van) can provide the main part of any missing infrastructure in underserved areas (high interference, poor coverage). Latency and bandwidth requirements resemble those of a video conferencing system and also depend on the number of users while the various screen sizes used impose respective requirements on resolution and bandwidth. 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.

D. *Factories of the future*

Both low latency and security are of crucial importance for scenarios related to factories of the future [15] that current 4G technology is not able to cover. Here, mechanical robots receive information from a high number of sensors providing various inputs to be used, with low latency required in order to achieve real time D2D communications between devices that operate in a manufacturing environment, with a typical cycle time of around 1 ms required. Furthermore, low latency enables the use of VR (virtual reality) applications for interaction between human operators and the mechanical robots. Humans can operate from remote locations while robots can operate in dangerous or hazardous environments. In all these scenarios equal importance is given to the reliability and security of the communication links. In a fully-connected factory there will be a plethora of different devices that will all be vulnerable to intruders taking control of the manufacturing systems.

E. *Advanced video streaming*

Mobile apps like Meerkat and Periscope allow users to broadcast live video from their location. Besides their popularity in leisure activities (e.g. broadcasting a ski run), they can also assist professionals, e.g. a civil engineer at a construction site reviewing progress along with the engineering team back at the office. However, such apps are possible today with the help of commercial CDNs that deploy and reserve resources as an overlay and mostly at the core of network domains. In the suggested UC, live video streaming is aided by in-network caches at the network edge or even in user equipment (UE). In addition, switching/routing at the edge (e.g., collocated with BSs) keeps traffic away from the network core, provided users are under the same network branch, and also reduces latency. Users need not be mobile, since any combination of fixed/ mobile senders/ receivers is supported. Broadcast live video is acceptable when latency is within a few seconds; any higher latency impacts the switching time from one feed to another. Also, high-definition (HD) broadcast video is the norm, especially for receivers with large screens, so bandwidth requirements are considerable, although not prohibitive. Strong security would be necessary for business and private streams.

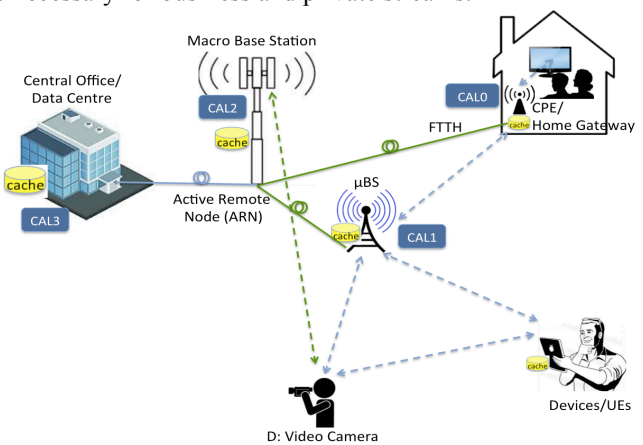

Fig.4: Advanced video streaming

v. Conclusions

In this paper we have introduced the innovative 5G CHARISMA architecture employing SDN and NFV principles to offer intrinsic security, low latency, and open access. A variety of representative UC scenarios have been outlined, where CHARISMA's hierarchical CAL-based and flexible IMU technology approach is key to enabling the required 5G networking solutions. CHARISMA is an ongoing research project and we expect a first prototype by end of this year and full practical implementation of its novel architecture by the end of 2017.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 671704.

References

[1] Cisco VNI report, "Cisco Visual Networking Index: Forecast and Methodology, 2014–2019" 27, May 2015.

[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] Mangili *et al.*, "A cache-aware mechanism to enforce confidentiality, trackability and access policy evolution in Content-Centric Networks" Computer Networks. 2015, vol. 76, p. 126-145.

[5] Georgopoulos *et al.*, "Cache as a Service: Leveraging SDN to Efficiently and Transparently Support Video-on-Demand on the Last Mile" 23rd International Conference on Computer Communication and Networks. IEEE, 2014

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

[7] 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.

[8] 802.1AE Standard: Media Access Control (MAC) Security. [Online] http://www.ieee802.org/1/pages/802.1ae.html

[9] 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

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

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

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

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

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

[15] 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