Agile Management and Interoperability Testing of SDN/NFV-Enriched 5G Core Networks

Taesang Choi, TaeYeon Kim, Wouter Tavernier, Aki Korvala, and Jussi Pajunpää

In the fifth generation (5G) era, the radio internet protocol capacity is expected to reach 20 Gb/s per sector, and ultralarge content traffic will travel across a faster wireless/wireline access network and packet core network. Moreover, the massive and mission-critical Internet of Things is the main differentiator of 5G services. These types of real-time and large-bandwidth-consuming services require a radio latency of less than 1 ms and an end-to-end latency of less than a few milliseconds. By distributing 5G core nodes closer to cell sites, the backhaul traffic volume and latency can be significantly reduced by having mobile devices download content immediately from a closer content server. In this paper, we propose a novel solution based on software-defined network and network function virtualization technologies in order to achieve agile management of 5G core network functionalities with a proof-of-concept implementation targeted for the PyeongChang Winter Olympics and describe the results of interoperability testing experiences between two core networks.

Keywords: 5G core network (CN), Agile management, Interoperability between CNs, Network function virtualization (NFV), Software-defined network (SDN).

Manuscript received Oct. 13, 2017; revised Dec. 4, 2017; accepted Dec. 18, 2017.

Taesang Choi (corresponding author, choits@etri.re.kr) and TaeYeon Kim (tykim@etri.re.kr) are with the Hyper-connected Communication Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Wouter Tavernier (Wouter.Tavernier@UGent.be) is with the Department of Information Technology, Gent University, Belgium.

Aki Korvala (aki.p.korvala@nokia.com) and Jussi Pajunpaa (jussi.pajunpaa@nokia.com) are with Nokia, Oulu, Finland.

I. Introduction

In the fifth generation (5G) era, the radio internet protocol (IP) capacity is expected to reach 20 Gb/s per sector (mobile speeds up to 20 Gb/s), and ultralarge content traffic (for example, ultrahigh definition video streaming, augmented reality (AR), and virtual reality) will travel across a faster wireless/wireline access network. All 5G mobile/fixed traffic has to travel via the packet core network (CN). Currently, in the fourth generation (4G), most mobile operators (even large-scale ones) have only a few sites with packet gateways (PGWs) across their entire networks. The software-defined network (SDN) paradigm provides a new capability for faster service provisioning of the 5G CN through standard programmable interfaces. Moreover, with cloud computing, datacenters promote the on-demand provisioning of computing resources and services [1]. If the 5G core nodes are distributed closer to cell sites, content servers (or caching servers) can be placed on the rack right next to the distributed 5G core with network function virtualization (NFV) technologies. This can help significantly reduce backhaul traffic by having mobile devices download content immediately from the content server. Thus, it is desirable to distribute packet core functionality to a number of local sites near end users in the coming 5G era. The 5G core functionality and applications can then run on virtualized servers at the local network sites. Other important 5G services—massive and mission-critical Internet of Things (IoT) services—are the main differentiator from 4G services. Mission-critical IoT (ultrareliable and low-latency communications) applications include remote-controlled machines, autonomous driving, and others. These types of ultra-real-time services require a radio latency of less than 1 ms and an end-to-end latency of less than a few milliseconds [2].

To address such challenges, we present a novel agile management and orchestration (MANO) architecture

based on enabling key technologies for 5G core functionalities, a proof-of-concept (PoC) implementation targeted for PyeongChang Winter Olympics, and deployment and interoperability testing experiences. The proposed solution is an interim result of a collaboration project between the Republic of Korea (KR) and the European Union (EU) [3]. The rest of the paper is organized as follows. We describe the enabling key technologies in Section II. We present the agile MANO architecture in Section III. Our prototype implementation and deployment experiences are described in Section IV. A performance evaluation of the proposed system, including the interoperability testing results, are provided in Section V. Finally, we conclude our paper with the plans for potential future work in Section VI.

II. Enabling Key Technologies

This section examines the key technologies for the SDN, NFV, MANO, mobile edge computing (MEC), mobility management, and control plane (CP) security and their associated design principles for the support of the proposed CN functionalities and their agile management.

1. Software-Defined Networking and Orchestration

Standardization efforts for SDNs were mainly carried out by the Open Networking Forum [4] and the International Telecommunications Union – Telecommunications Study Group 13 (ITU-T SG13) [5] by defining the requirements, reference architecture, protocols, and use cases. Open-source projects such as Open Daylight [6] and Open Networking OS [7] have played important roles in realizing the SDN concept in real life. The SDN started with a limited networking environment such as cloud data centers and enterprise networks and has widened its coverage to wide-area transport networks and wireless/wireline integrated multidomain networks. Instead of applying it as a standalone network control tool, it is now used with NFV and as a component of an end-to-end orchestration solution. It provides an intelligent knowledge plane for making control decisions via traffic steering, traffic engineering, and flexible service chaining for latency-sensitive and reliability-seeking applications. It can be used in efficient communications among distributed core functional components.

2. Network Function Virtualization

The virtualization of core and radio access network functions will optimize the use of network resources and add scalability and agility. To this end, the European Telecommunications Standards Institute (ETSI) NFV Industry Specification Group has defined the architecture, open application programming interfaces (APIs), and reference points, leveraging open-source PoC projects and communities to drive open standards of NFV. In 2016, it published Release 2 specifications and reports, including the functional requirements, interface, and information model for the reference points for the MANO function block called NFV-MANO [8]. These open standards are intended to enable third-party vendors to develop framework components that can collaborate with various vendor components so that content service providers) are not restricted in selecting functional and management components. The main appeal of the use of NFV to deploy network elements and virtual network functions (VNFs) is that services can be launched more quickly by installing software on a standard hardware platform. This is akin to the way software applications could be developed and launched for the personal computer (PC) platform when it first emerged. Another advantage is lower capital expenditures because standardized hardware platforms tend to drive costs down. Such advantages can be directly applied to the distributed core functional components in the communications environment.

3. Mobile Edge Computing

In order to support the requirements for the market's expected throughput, latency, scalability, and programmability, ETSI established the Industry Specification Group on Mobile Edge Computing in 2014 [9]. It develops a standardized and open environment that offers distributed cloud-computing capabilities and an IT service environment for application developers and content providers. By February 2016, the group finalized three specifications: the terminology, the technical requirements, and the framework and reference architecture. This group also works on specifications for MEC platform application enablement, the API principles and guidelines, the service APIs for radio network information and location, user equipment (UE) identity and bandwidth management, system/host/platform management, lifecycle and policy management, the UE application interface, the deployment of MEC in an NFV environment, and the end-to-end mobility.

By offering distributed cloud-computing capabilities and exposure to real-time radio network and context information, MEC provides the following characteristics:

- Ultralow latency: Mobile edge services can be run close to end-user devices to provide the lowest possible latency,

- Proximity: Being close to the source of information, MEC is particularly useful for capturing key information for analytics and big data,
- High Bandwidth: The mobile edge location at the edge of the network combined with the use of real-time radio network information can be used to optimize the bandwidth for applications,
- Location awareness: A mobile edge can leverage the low-level signaling information to determine the location of each connected device,
- Real-time insight into radio network and context information: Real-time network data can be used by the applications and services to offer context-related services.

MEC can provide a significant improvement in a mobile user's quality of experience for latency- or quality of service (QoS)-sensitive services such as edge video orchestration, mobile video throughput guidance, AR, intelligent video analytics, and others. Most importantly, MEC enables the implementation of mobile edge applications as software-only entities that run on top of a virtualization infrastructure, which is located in or close to the network edge.

4. Distributed Mobility Management

It is essential to support distributed mobility management to enable agile management of the CN functionality. Currently, the Internet Engineering Task Force is conducting standardization efforts to define a distributed mobility management architecture and mechanism in a layer 3 IP network environment. The 3rd Generation Partnership Project (3GPP) also initiated work on defining layer 2 distributed mobility management requirements for a mobile communications environment. The functional decomposition and distribution of global service management will span multiple points of presence (PoPs) over the network, including network slices in a 5G environment. It would be better to determine the anchoring and mobility management tailored to such a network environment at the central node, unlike exiting hierarchical and IP mobility. Composition functions and resources will be orchestrated for dynamic mobility management. Various experiments and simulations are under study by the research community, and extensive testing and verification of the concepts of distributed mobility management are needed.

5. Security of the 5G Core Network Control Plane

A software-defined mobile network (SDMN) controller will provide the necessary services to the CN functions by working as an intermediary between the access and core functions. The network control functions of the core elements, for example, the mobility management entity (MME), serving/packet data network gateways (S/P-GWs), and others, will reside in a centralized cloud in the form of SDN applications that will leverage NFV technology to be instantiated on different hardware or even at different network perimeters for a higher scalability and availability. Hence, the main security concern in such architectures will be the SDN controller since it can become a potential bottleneck for the overall network.

To mitigate the risks of controller failure due to scalability or the chances of denial of service (DoS) attacks due to its centralized role, controller resilience strategies have been proposed. These strategies include controller resilience through redundancy, maximizing the storage and processing capabilities of the controller, and distributing controller functionalities among multiple control points in the network. The OpenFlow variant of an SDN supports wildcard rules so that the controller sends an aggregate of client requests to server replicas. By default, microflow requests are handled by the controller that can create potential scalability challenges, increasing the chances of failures due to DoS attacks. Normally, reactive controllers that act on a flow request when it arrives at the controller are used. Proactive controllers install flow rules in advance, thus minimizing the flow request queue in the controller. Similarly, various load-balancing techniques that would balance the load among multiple controllers in a network have been suggested. We have worked on a novel communication architecture based on the host identity protocol (HIP) to secure both control and data channels in SDMNs.

III. System Architecture

This section describes the proposed CN and agile management system architecture based on a combination of the key technologies described in Section II.

1. Core Network Architecture

We designed our CN architecture (Fig. 1) [10] to support CN functionalities and agile management on the basis of the various key technologies described in Section II. Specifically, the CN functionality is realized by leveraging an SDN and NFV in order to facilitate the dynamic provisioning of CN functions. By using SDN capabilities, traffic flows can be dynamically controlled, redirecting the traffic to gateways according to the workloads. Simultaneously, the introduction of NFV

https://doi.org/10.4218/etrij.2017-0236

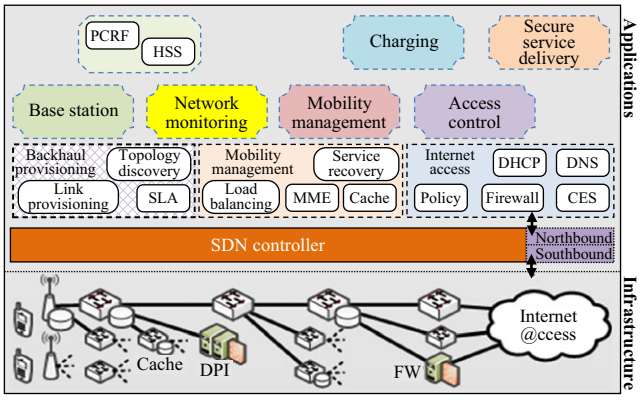


Fig. 1. CN architecture.

permits the separation of service functionalities from the capacity-constrained specific network entities and allow dynamic instantiation in commodity and powerful servers. Starting from late 1990s, the 3GPP has been taking steps towards a clear separation of the data and control planes and the respective elements in the architecture. We propose to take this concept to the next level following the SDN paradigm. Figure 1 also presents the 5G network control as a group of SDN applications. They are the Base Station App, Backhaul App, Mobility Management App (MM App), Monitoring App, Access App, and Secure Service Delivery App. The network applications are orchestrated via the Controller Northbound API. Multiple SDN applications operate without conflicts.

The Base Station App runs the control software that is now vertically integrated with the evolved Node B (eNB). The physical base stations under its control consist of an antenna, a band-pass filter, and an Ethernet card for backhaul connectivity [11]. The MM App implements mobility as a service and incorporates the MME. In addition, it needs to manage the QoS for each user, balance the load among alternative paths across the aggregation network, and route the user to a cache when possible. The MM App also chooses the path for a device. The load-balancing decision is made on the basis of the input from the Network Monitoring App. In any case, it is desirable that the point of attachment of a mobile device to the Internet is fixed while it remains within the coverage of the current mobile network [11].

In one physical mobile network, there may be many Access Apps. In this case, an Access App is owned and operated by a particular mobile virtual network operator. Putting mobility aside, the Access App is responsible for providing data services to mobile users. The key properties of the Access App include providing Internet access, firewalling unwanted traffic, and providing access to premium content [11].

The main CN functions are designed and implemented in the form of virtual functions, namely, virtual evolved packet cores (vEPCs). Both the EU and KR provide their own implementations of vEPCs based on this architecture. They are described as follows.

2. European vEPC Architecture (5GTN)

The EU vEPC consists of the following VNFs:

- Mobile gateway: The cloud mobile gateway provides the service provider-gateway (SP-GW), gateway general packet radio service (GPRS) support node, and traffic detention functions (TDFs), evolved packet data gateway, and trusted wireless access gateway.
- Mobility management: The cloud mobility manager provides the MME and servicing GPRS support node functions.
- Policy control and charging: The dynamic services controller built on patented agile rules technology engine provides the policy and charging rules function (PCRF) and wireline radius/change of authorization.

Element and network management: The service-aware manager provides end-to-end network management visibility across the entire mobile network.

To support the scalability required to meet the expected 5G and IoT service requirements, the packet core VNFs provide three key design innovations:

- The packet core VNFs are decomposed into separate CP and data-plane virtual machine (VM) instances. This enables a distributed architecture where data-plane resources can be deployed in edge data centers closer to the device, while CP resources can be centralized.
- State-efficient VNF processing unpins the subscriber/device state information from the VMs, freeing up the underlying computing resources to be reused to process other subscribers/devices.
- The remote cloud database synchronizes the subscriber/device state information into a real-time data store.
- The 5GTN functional architecture [10] is given in Fig. 2.

3. Korean vEPC Architecture

The CN of 4G Long Term Evolution (LTE) is in charge of mobility, authentication, and charging, allowing all mobile traffic to pass through the CN to access services incurring traffic congestion in the CNs. Our architectural decision for 5G is to distribute mobile core functions to the edge nodes. A 5G core is generally divided into a 5G core user plane (UP) in charge of bearer delivery and a 5G Core CP in charge of signaling and control of the 5G CN.

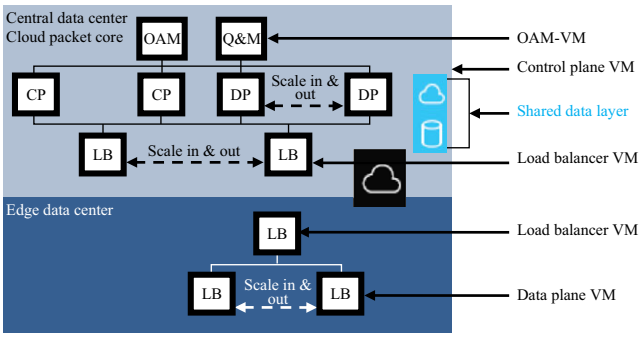


Fig. 2. 5GTN vEPC functional architecture.

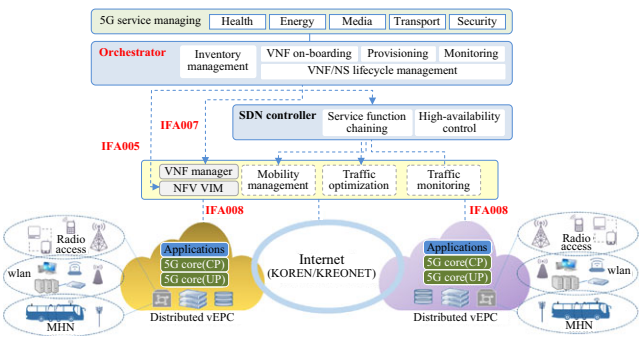


Fig. 3. High-level architecture of Korea's distributed vEPC.

The key CN architectural design principle is a centralized CP with a distributed UP over the edge nodes.

If the CN where bearers are terminated is located closer to the cell sites, the application servers follow naturally, and the backhaul traffic will significantly decrease, resulting in a cost reduction for continual backhaul enhancement.

A 5G network is supposed to be able to provide ultra-real-time services such as highly sensitive remote control and automatic driving vehicles. These types of services may generate much lesser traffic than video streaming applications but require an ultralow latency. Figure 3 illustrates the high-level architecture of a Korean vEPC. It is realized as a highly scalable vEPC (HSvEPC) [12]. Its functionality and architecture are described below.

4. HSvEPC Network Architecture

It is possible to deploy different types of virtual mobile packet cores depending on the demand or network access environment in an HSvEPC network architecture. Two types of vEPCs are designed (shown in Figs. 4 and 5):

- Split vEPC (S-vEPC): The first type is an expansion of a vEPC by separating conventional consolidated functions into UP and CP functions for dynamic scaling operations.

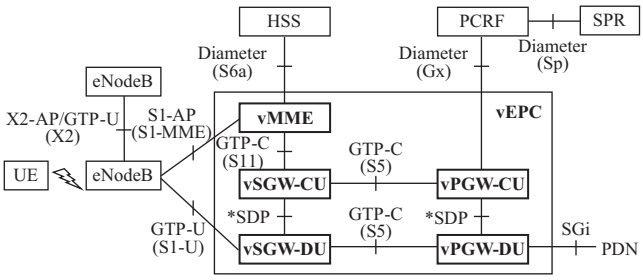


Fig. 4. HSvEPC functional architecture: S-vEPC.

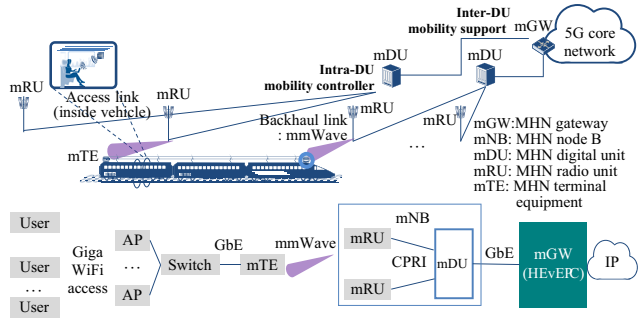


Fig. 5. HSvEPC functional architecture: MHN-vEPC.

- Mobile hotspot network vEPC (MHN-vEPC): The other type is an optimized case for a hotspot area to enhance the agility of the network. For faster and more dynamic mobility management in a mobile hotspot area, the S1 (single interface between the LTE radio access network and the EPC) interface of the virtual EPC has been modified in terms of the UP and CP.

5. Management and Orchestration Architecture

Figure 6 shows overall MANO architecture on the EU side based on NFV MANO and an SDN. The architecture has two management entities:

- The VNF manager is in charge of instantiating and controlling EPC functions. It is responsible for

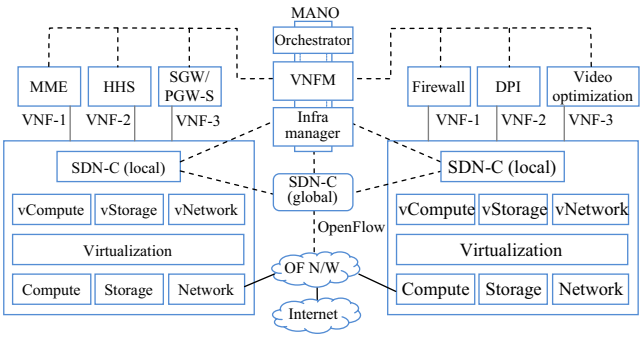


Fig. 6. Overall EU MANO architecture with an SDN.

https://doi.org/10.4218/etrij.2017-0236

interacting with VNFs, chaining VNFs, and handling their lifecycle—instantiation, maintenance, and others. It is in charge of the operation and configuration of VNFs through the operations support system (OSS)/base station subsystem (BSS). It will handle multifunctional EPC components such as the MME and home subscriber server (HSS) as well as specific-functionality VNFs such as firewalls and deep packet inspectors.

- The infrastructure manager interacts with (or incorporates the capability of) the SDN controller in the service stratum when deploying VNFs for configuring the computing and storage resources for the VNF of interest. It also supports the attachment of the VNFs to the border of the underlying transport network for the networking part to make them reachable from outside the data center. This is only for the service-layer part. It also has to determine a path for the transport-layer VNFs.

The KR CN MANO are also based on NFV and SDN components. Figure 7 shows the MANO architecture. It comprises three different entities: the NFV orchestrator (NFVO), VNF manager (VNFM), and virtual infrastructure manager (VIM).

The NFVO is responsible for managing functions such as network service (NS) lifecycle management and overall resource management. Service management or orchestration deals with the creation and end-to-end management of services by composing different VNFs. Resource management helps to ensure that the NFV infrastructure (NFVI) resources are abstracted cleanly (independent of the VIM) to support the services that access these resources.

The VNFM oversees the lifecycle (which typically involves provisioning, scaling, and terminating) management of instances of a VNF. In this case, each VNF is associated with a VNFM that will manage that particular VNF's lifecycle. A VNFM may manage multiple instances of the same type of VNF or different types of VNFs.

The VIM controls and manages the NFVI computing, storage, and network resources. The VIM component has been the focus of a large amount of research and various open-source solutions such as OpenStack and has been used to realize the virtualized infrastructure management functionality of MANO.

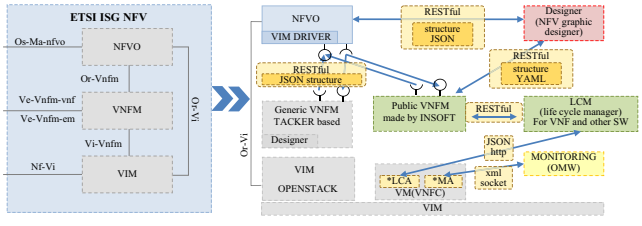


Fig. 7. Overall KR M&O architecture with MANO and an SDN.

6. Autoscaling Based on Performance/Fault Management

In our M&O, autoscaling functionality is provided as shown in Fig. 8. After instantiation of a 5G mobile CN service, the NFVO sends a supervision request to the supervisor, which performs performance monitoring and fault notification over virtualized resources and functions. Scaling is conducted autonomously by the orchestrator on the basis of the information provided by the supervisor.

7. Automation by Event Chaining

An event chaining process is another important functionality that is supported, which is defined as a sequence of event units occurring from inside or outside the target VNF and virtual data unit (VDU). It enables the automation of 5G mobile CN management. A combination of internal events that are significant in a single VNF or VDU and external events between VNFs and VDUs enables the automated management of a lifecycle of a mobile CN service (see Fig. 9).

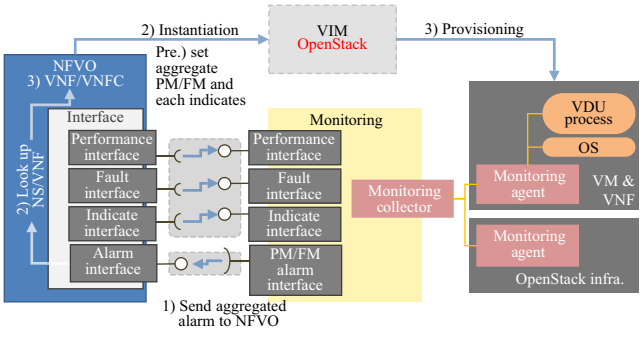


Fig. 8. MANO autoscaling process.

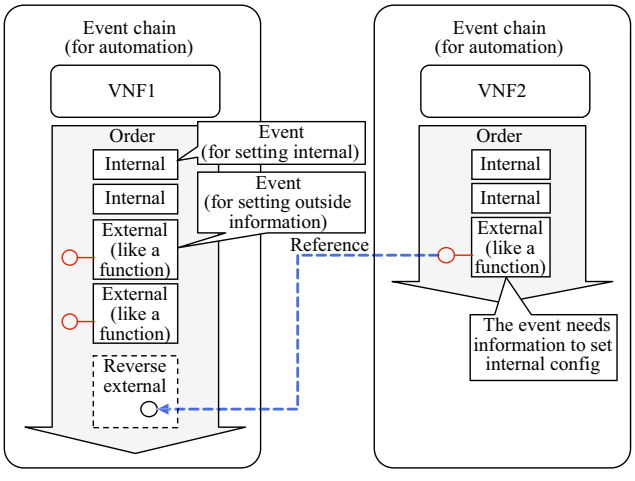


Fig. 9. MANO automation process.

8. Security Management Architecture

The security of the CN can be grouped into two parts: the security of the CN elements and the security of the communication channels in the CN. In SDNs, controlling the behavior and interworking of different heterogeneous networks is carried out with a logically centralized control architecture that has a global view of all forwarding elements. An operating system maps the entire network to services and applications that are implemented on top of the control plane. Hence, security services will be implemented as security applications using the network stats provided either proactively or reactively by the network control platform. Centralized control, which can be either logically or physically centralized, enables the programmability of the network and will thus provide fine-grained network security control, remote monitoring, and dynamic security service insertion. The security management architecture is presented in Fig. 10.

IV. Implementation and Deployment Experience

Both the EU and KR edge and CN functions are under development. The development of some components has been completed, such as EU's edge and core functions in a 5GTN solution. KR's vEPC development is underway with the core functionality completed. The KR vEPC currently supports up to 100 UEs and a channel throughput of 20 Gbps toward an eNB. To meet the 5G key performance indicator (KPIs), we are trying to fill the gaps in both vEPC systems. We are targeting the completion of our system development by October 2017.

We are also developing our agile CN MANO systems based on the architectures described in Section II. Initial prototypes are available, and their functionality as separate systems and their interoperability are being tested as well across the EU and KR over interconnected research and development networks between the EU and KR via the Korea Research and Education Network (KOREN)–Trans Eurasia Information Network (TEIN)–Nordic Countries Network (NORDUNET)–Finnish University and Research Network (FUNET).

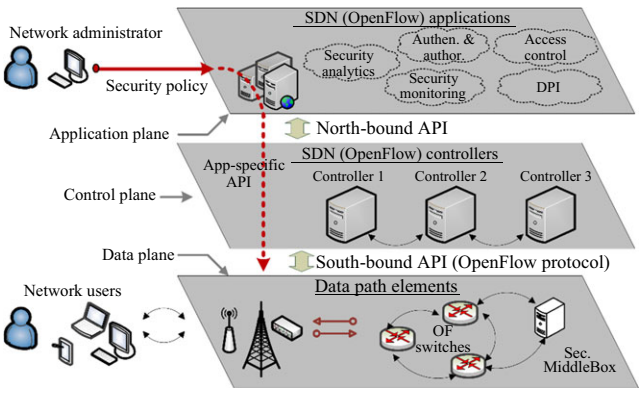


Fig. 10. SDN architecture showing the security services and their deployment.

1. vEPC Implementation

5GTN vEPC VNF functions have been implemented, deployed, and tested on CloudBand's NFVI and its MANO solution. CloudBand is a hardened, production-ready NFV solution based on OpenStack and other open-source technologies. This open approach allows service providers to benefit from a vast community of engineers and supports investments in a mainstream solution with open interfaces.

The HSvEPC implementation consists of a vMME, vSGW-CU, vPGW-CU, vSGW-DU, and vPGW-DU. The CU is a CP that controls the device management, and the data unit (DU) is a UP that controls the data transfer between devices. The main reason why we separated functions by each plane is to support scalability depending on the demand situation. Since the functions in the HSvEPC are implemented as VNFs, they can be modified on demand and controlled per VNF level. One important use case of such flexibility is network slicing support.

Figure 11 shows the access point name (APN)-based CN slicing use case. An IoT device may have a different APN against a UE, and discrimination of each device at the MME is required. The above use case illustrates our implementation of an MME that can classify different devices by categorization based on their APNs and map appropriate resources in the SGW and PGW. Moreover, the HS-vEPC can be scaled in or out depending on the demand, which can reduce the cost, and other unused parts of network functions can be relocated to only the necessary parts.

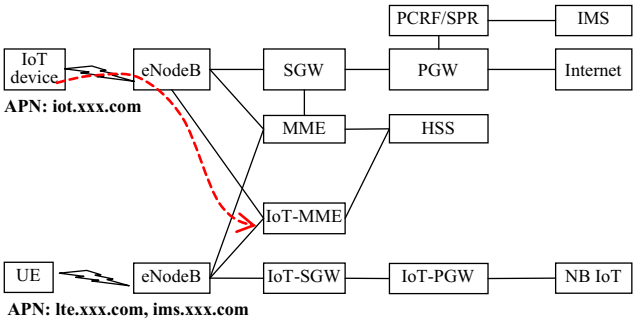


Fig. 11. HSvEPC core slicing use case.

https://doi.org/10.4218/etrij.2017-0236

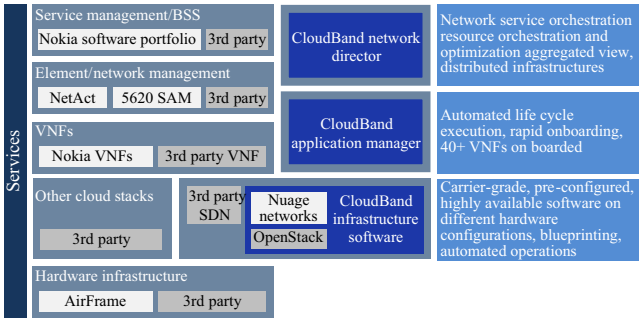


Fig. 12. 5GTN MANO implementation.

2. Management and Orchestration Implementation

MANO in 5GTN has been implemented and deployed. It consists of CloudBand infrastructure software, a CloudBand application manager, and a CloudBand network director that have been optimized to fit the key NFV MANO shown in Fig. 12.

- CloudBand Infrastructure Software

The CloudBand infrastructure software is a multipurpose NFVI and VIM. It virtualizes and manages computing, storage, and network resources.

- CloudBand Application Manager

The CloudBand application manager is a VNFM that automates lifecycle management actions by managing resources and applying associated workflows.

- CloudBand Network Director

The CloudBand network director is an NFV resource and NS orchestrator. It manages virtual resources across geodistributed NFV infrastructure nodes. It visualizes and automates the lifecycle of NSs, such as virtual customer premise equipment (CPE), including their forwarding graphs and service chains.

The KR MANO implementation is shown in Fig. 13. We have implemented it in a rack of servers consisting of a VIM built and extended over OpenStack, a VNF manger, and an orchestrator. The management target is, of course, a set of virtual functions implementing CN functionality and networks that interconnect those virtual core functions.

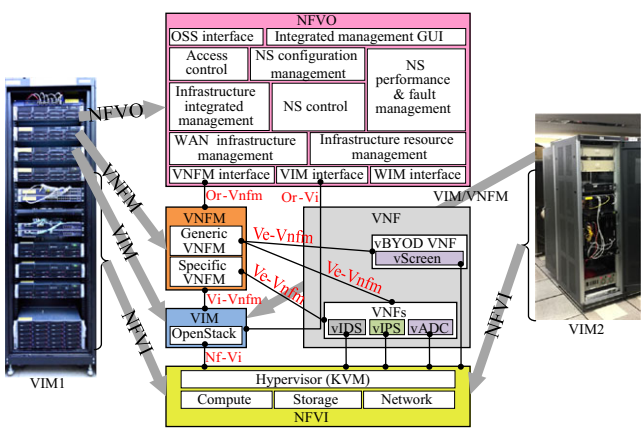


Fig. 13. KR MANO implementation.

3. Deployment and EU–KR Interoperability Testing

First, phase field deployment and interoperability testing between the EU and KR was conducted in July 2017 [13]. Both the EU and KR vEPC and MANO have been deployed. Figure 14 shows the EU's 5GTN deployment network environment. The 5GTN network elements in Oulu are physically located at two different sites. The eNBs and Juniper SRX240 router are located at Site 1. Juniper SRX240 connects external entities to 5GTN. Data center Tampere in Oulu is connected via a layer 2 virtual private network (L2VPN) connection. KR entities are also connected using an L2VPN connection. The EPC is physically located at Site 2 and connected through University of Oulu (UOulu) switches to a radio access network.

Figure 15 shows the 5GTN vEPC AirFrame hardware. The European testbed vEPC has 11 servers, of which three servers are used as controller nodes and eight servers are used as compute nodes; one hardware (HW) management switch; and two leaf switches.

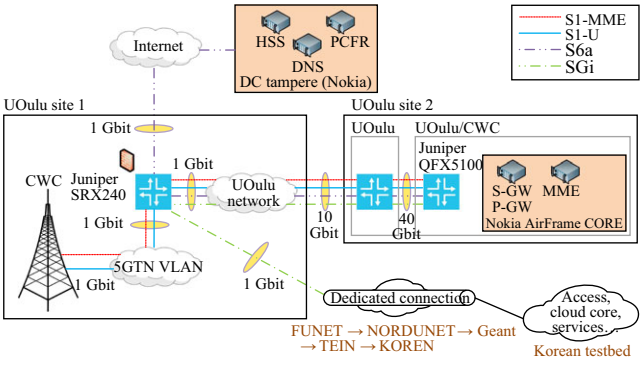


Fig. 14. EU 5GTN deployment environment.

Fig. 15. 5GTN EPC AirFrame hardware.

- Server type: 11 × Quanta B51BP-1U, manufactured by Quanta Computer Inc.
- HW management switch type: 1 × Quanta LB9, manufactured by Quanta Computer Inc.
- Leaf switch type: 2 × Juniper QFX5100-24Q switches, each having 2 × QFX-EM-4Q expansion modules, manufactured by Juniper Networks Inc.

The three uppermost servers are controller nodes. The remaining eight servers are computing nodes. The management switch is below the servers, and the leaf switches are below the management switch.

Figure 16 shows the Korean vEPC and MANO deployment environment. There are three possible PoPs in KR interconnected over KOREN: Seoul, Daejeon, and Gangneung, where the PyeongChang Winter Olympic Games take place in 2018. We plan to deploy mobile core infrastructure for 5G networks at these three sites for service deployment. Currently, we deployed one set of a vEPC and MANO at the Electronics and Telecommunications Research Institute (ETRI) in Daejeon for interoperability testing with the EU.

Our vEPC supports NS provisioning and monitoring functionality as follows:

- The vEPC NS consists of an MME, a virtual S-GW control unit (S-GW-CU), a virtual S-GW-DU, a virtual P-GW-CU, and a virtual P-GW-DU.
- In our deployment, the vEPC NS does not cover the remaining functionalities for the vEPC (that is, the HSS and PCRF).
- The virtual S-GW-DU and virtual P-GW-DU must have single-root input/output virtualization and sharing (SR-IOV)-enabled ports in order to enhance their performance.

The NFVO, VNFM, and VIM closely interwork with each other to create and manage NSs. Figure 17 shows the procedures to provision an NS in the NFV-enabled infrastructure.

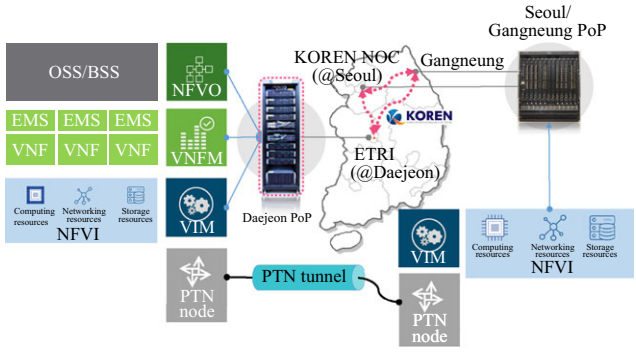


Fig. 16. KR vEPC and MANO deployment environment.

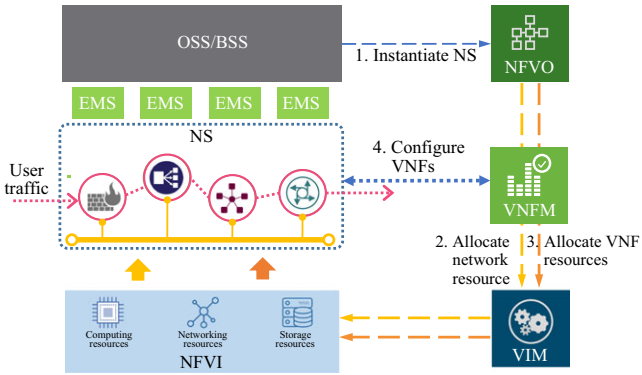


Fig. 17. NS provisioning procedures.

1. An OSS/BSS (or administrators) requests to create an NS at the NFVO by defining a new NS descriptor or selecting one.
2. The NFVO requests the allocation of network resources at the VIM, which connects the VNFs composing the requested NS. In this step, management network resources are also created for management access.
3. Once the network resources are allocated, the NFVO requests the VNFM to instantiate VNFs. Since our NFVI is in the indirect mode, the VNFM indirectly requests the VNF resource allocation at the NFVO, and the then request is sent to the VIM.
4. When VNF resources are allocated, the VNFM configures VNFs with any VNF-specific parameters.

The states of the NSs are monitored with two metrics: a service utilization metric and a metric for monitoring resource utilization. The NFVO receives the monitoring results from the VNFM and VIM and exploits the results to perform other management operations such as a scaling operation.

Figure 18 shows the two types of monitoring.

- VNF monitoring: VNF providers can specify some indication of VNF behavior, and they include this information as a parameter (that is, VnfIndicator) of the

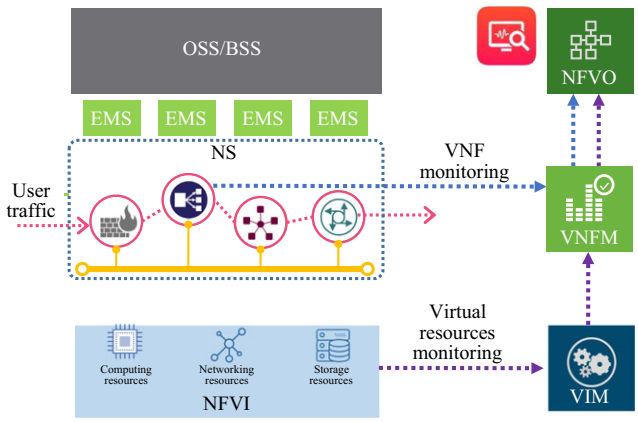


Fig. 18. VNF and virtual resource monitoring.

https://doi.org/10.4218/etrij.2017-0236

VNF descriptor. On the basis of this parameter, the VNFM requests the actual value of a given indicator from the VNFs.

• Virtual resource monitoring: The VIM continuously monitors the allocated virtualized resources such as virtual computing, virtual storage, and virtual networking.

For the preparation of an end-to-end 5G service demonstration between the EU and KR, we performed interoperability testing between two CNs as a first step. We are planning to conduct an end-to-end interoperability test including mobile access networks on both sides by November 2017, and the results will be described in a future version of this paper.

For CN interoperability testing, we defined the following two scenarios:

• Scenario 1: There are two users—one connected to the EU vEPC and the other to the KR vEPC. Content is shared between the two users, which is a latency critical application such as shared gaming.

• Scenario 2: In this scenario, a mobile UE on the KR side is the content provider and is streaming 4K three-dimensional videos to a receiving UE on the EU side. The aim is to achieve very high data rates across the two vEPCs.

For the first phase, we conducted a loose interoperability test, defined as follows:

- Standard PDN interconnection via IP.
- A dedicated tunnel between the EU and KR test bed, which will provide guaranteed bandwidth and latency. This will ensure that the QoS requirements of the two use cases are guaranteed.
- A model similar to the DiffServ model to guarantee the QoS. This model must be capable of providing 5G standard QoS. The details of such a model need to be worked out further.
- A reachable fixed IP- or DNS-based system, depending on the actual applications for both use-case scenarios defined.
- Support for dual stacks. Both IP version 4 and version 6 will be supported.
- Dynamic routing protocols (open shortest path first (OSPF), border gateway protocol (BGP)) for advertising the PGW IP address to the external network.
- An application server placed strategically between the two cores, which will enable the execution of common applications such as games with low latencies. The connections to and from these servers will also have a guaranteed QoS.

The EU–KR interconnectivity is shown in Fig. 19. The EU–KR dedicated interconnectivity is implemented using an L2VPN. A dedicated L2VPN connection path is UOulu ⇔ FUNET ⇔ NORDUNET ⇔ Geant Open ⇔ TEIN ⇔ KOREN ⇔ ETRI.

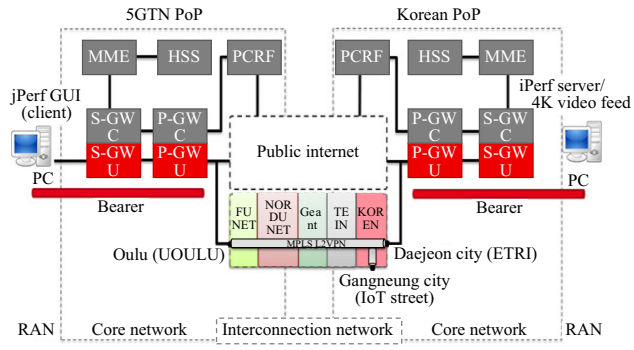


Fig. 19. EU-KR interconnectivity.

4. Dynamic Interoperability Provisioning

The key benefit of an SDN/NFV-enabled mobile core architecture is its ability to dynamically adapt required resources to the changing context and environment. To take full advantage of such capabilities, the NFVI on which the EU and KR vEPCs are deployed are (partly) under the control of the same NFVO. Figure 20 illustrates the resulting network architecture, where the common NFVO oversees one or more PoPs, each managed by their own VIM, as well as the interconnecting wide area network (WAN) managed by its WAN infrastructure manager (WIM).

In the static scenario, the NFVO receives an NS request to deploy the EU and KR vEPCs on their respective PoPs as well as their interconnection via the WAN. As a result, the NFVO will instruct the VIMs to instantiate the required network function instances as well as the WIM to set up the interconnection.

A more advanced and dynamic scenario involves the dynamic reprovisioning of the interconnected bearers as well as that of the underlying VNF resources to fulfill the necessary QoS requirements. This scenario is depicted in Fig. 20. In this scenario, the NFVO is used for static provisioning of different parts of the mobile core interoperability setup and for the dynamic reprovisioning of this NS based on monitoring components (see previous section) as well as other external triggering systems (OSS/BSS or services). These components might, for example, trigger the scale-out of the P-GW-U (1a) or the migration of the S-GW (1b) VNFs. Note that the monitoring components are not necessarily directly interacting with the NFVO but are usually relying on the interaction of the management functionality of the associated VNF (VNFM) or services. As a result, the NFVO will (re-)instruct the corresponding VIMs and WIM(s) to instantiate new VNFs (indicated in dark

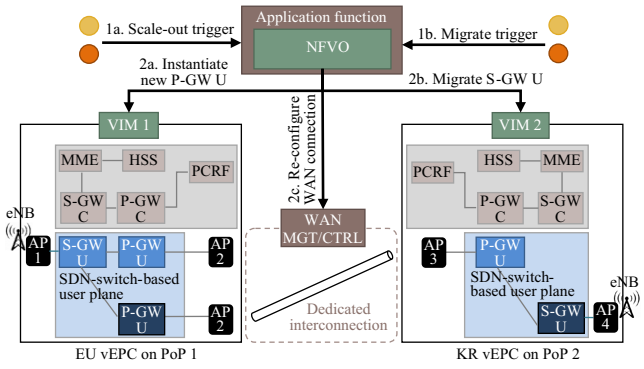


Fig. 20. Dynamic reprovisioning and NW-initiated bearer setup.

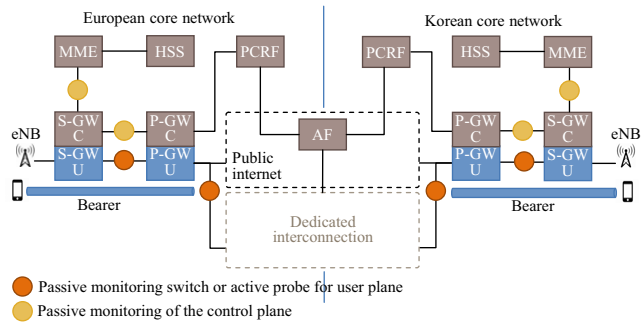


Fig. 21. Traffic monitoring locations at the two interworking sites.

blue) and rewire the associated network connectivity via the WIM(s). Future work will refine this process and determine the degree of dynamics that will be implemented for the considered project scenarios and associated demonstrations.

5. Monitoring

In Sections IV.3 and 4, we described the different interoperability scenarios and the necessary steps to initiate a new connection. We also noted that it is not sufficient to create a connection based on available resources, but the monitoring of allocated resources is necessary. By obtaining real information about, for example, the latency or bandwidth, one can tune the QoS parameters to better align with the application session's requirements.

One of the most trivial metrics to measure is the end-to-end delay and bandwidth of the newly created path. Depending on the chosen application architecture, one has to monitor the links between the UEs and the application server or between the two UEs. In case of a client–server architecture, the application server can initiate active measurements, or it can passively capture the behavior of an underlying protocol such as the transmission control protocol (TCP) window size and round-trip time (RTT). We have the same possibilities with the point-to-point architecture, except that the UE executes the monitoring application. Such an application is the easiest solution, but it would place an unnecessary load on the UE. Moreover, we cannot infer the causes of any quality degradation by measuring end-to-end metrics.

To overcome these difficulties, we can extend the vEPCs with monitoring functions or use the existing ones if there are any. One can also install dedicated switches between the serving and PDN gateways in both vEPCs to monitor the application flows passively. As the traffic is IP-based, we can use OpenFlow switches or even NetFlow-supporting ones. Moreover, accurate delay measurements require clock synchronization between the monitoring nodes. The same synchronization is necessary for active measurements, where probes instead of switches perform the monitoring. These probes have to be aware of the properties of the flows in order to inject traffic into the bearers. Therefore, the application server must inform them about the newly created connection.

Besides the monitoring of UP traffic, one can also capture the control traffic (green marker in Fig. 21). Observing the connection setup messages between the MME and the eNB, we can derive the time required for the initial attachment or a handover. The control messages between the gateways provide information about the duration of the network-initiated (that is, on the request of an application function) connection setup. Most likely, these setup times have no or little effect on the overall user experience, but they can inform us about potential slowdowns. In case of a burst in the number of users, for example, the application server should refuse some of the connection requests when it experiences increased setup times at one or both of the vEPCs.

In addition to the UP and CP traffic as a good indicator of the performance, we can use also the central processing unit (CPU) usage and memory consumption of the network elements. Monitoring the CPU usage of the MME, we can forecast system slowdowns, as discussed in the previous paragraph, from the control traffic. A high resource usage at the gateways in one of the vEPCs indicates failing QoS requirements, and one can proactively redistribute the resources between the two vEPCs.

The monitoring procedures presented so far handle the functional blocks of the vEPCs as a black box software. They do not require any domain-specific knowledge about the inner workings of the mobile cores, nor do they use any API possible provided by the vendor of the systems (see Fig. 22). Such an API could give us information about the number of active connections and the number of

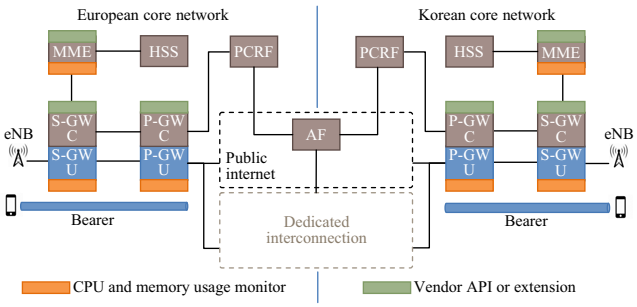


Fig. 22. CPU and memory monitoring and vendor API exposures.

bearers or even indicate if some of the QoS requirements are failing. Information from the MME could reveal the physical location of the UE or at least the cell to which it connects, which can help us to determine the initial latency ratio.

V. Performance Evaluation and Interoperability Testing Results

During the deployment and interoperability testing, we observed several important performance measures: the vEPC system performance, the end-to-end network performance between the two core systems, and the application performance.

The HSvEPC provides a total channel throughput of 20 Gbps toward an eNB and can accommodate 100 simultaneous UEs. The 5GTN vEPC also supports a total channel throughput of 20 Gbps toward an eNB and can accommodate over 500 simultaneous UEs.

The network that connects the two core systems currently supports up to 1 Gbps, and there are plans to upgrade it to 10 Gbps by November 2017. We performed bandwidth throughput and delay tests on both the EU and KR sides, and the end-to-end context and the results obtained over this interconnection link are described as follows [13].

1. EU CORE Integration and System Testing Results

A. EU's UOulu Site Testing

Testing was performed with LTE access. A PC with an LTE Universal Serial Bus (USB) stick and with jPerf/iPerf tools was used. The simplified test scenario is shown in Fig. 23. The LTE band used is Band 7, and the bandwidth is 5 MHz.

- UOulu iPerf Testing with TCP

We performed iPerf testing with TCP traffic. The uplink bandwidth was about 6.2 Mb/s. The performance was as

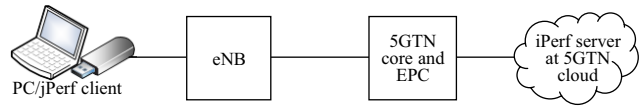


Fig. 23. UOulu testing scenario with LTE access.

much as expected with the 5-MHz bandwidth. The iPerf tool does not support downlink measurement when there is network address translation (NAT) between the end points (NAT is carried out at the LTE USB stick).

- UOulu iPerf Testing with the user datagram protocol (UDP)

We also performed iPerf testing with UDP traffic. The uplink bandwidth was about 11 Mb/s. The jitter was about 1.6 ms. The performance was as much as expected with the 5-MHz bandwidth. The iPerf tool does not support downlink measurement when there is NAT between the end points (NAT is carried out at the LTE USB stick).

The RTT was measured using a ping test, as shown in Fig. 24. The average was about 44 ms.

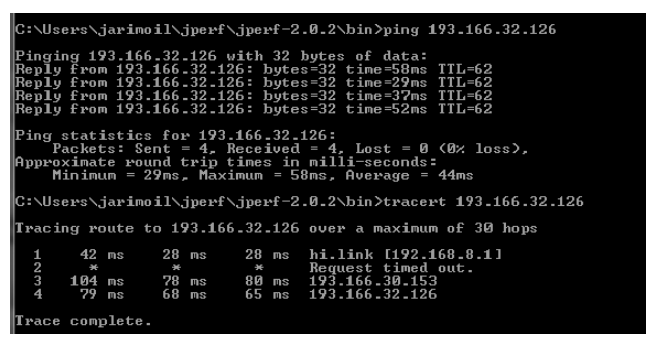
2. KR Core Integration and System Testing Results

A. KR's ETRI Site Testing

The maximum achievable bandwidth during tested on the 5G mobile core (5GMC) network was measured by iPerf. In this test scenario, the iPerf client was connected to the iPerf server running on the PDN GW in the 5GMC. The simplified test scenario is shown in Fig. 25.

- iPerf Testing with TCP

We performed iPerf testing with TCP data streams. Figure 26 shows a screenshot from the iPerf client using



```
C:\Users\jarimoil\jperf\jperf-2.0.2\bin>ping 193.166.32.126

Pinging 193.166.32.126 with 32 bytes of data:
Reply from 193.166.32.126: bytes=32 time=58ms TTL=62
Reply from 193.166.32.126: bytes=32 time=29ms TTL=62
Reply from 193.166.32.126: bytes=32 time=37ms TTL=62
Reply from 193.166.32.126: bytes=32 time=52ms TTL=62

Ping statistics for 193.166.32.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 58ms, Average = 44ms

C:\Users\jarimoil\jperf\jperf-2.0.2\bin>tracert 193.166.32.126

Tracing route to 193.166.32.126 over a maximum of 30 hops

  1    42 ms    28 ms    28 ms  hi.link [192.168.8.1]
  2     *        *        *     Request timed out.
  3   104 ms    78 ms    80 ms  193.166.30.153
  4    79 ms    68 ms    65 ms  193.166.32.126

Trace complete.
```

Fig. 24. UOulu ping test.

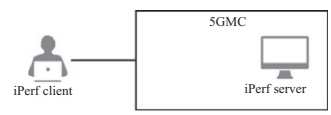


Fig. 25. Testing without LTE connectivity.

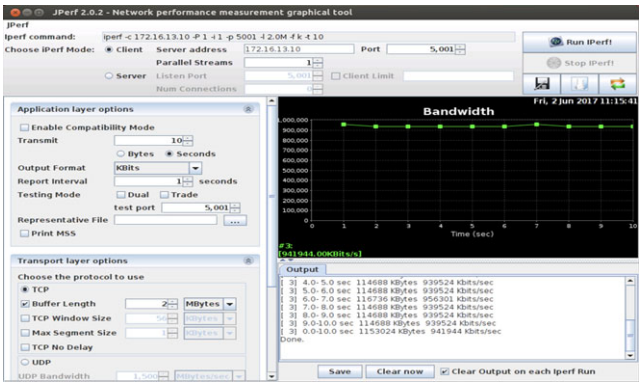


Fig. 26. iPerf testing with TCP traffic: iPerf client view.

jPerf, a graphical user interface front end for iPerf. The downlink bandwidth is about 941 Mb/s.

• iPerf Testing with UDP

We performed iPerf testing with UDP streams. Figure 27 shows a screenshot of jPerf on the client side. The uplink bandwidth is about 812 Mb/s. The downlink bandwidth is about 910 Mb/s.

• Ping Test

The RTT was measured using a ping test, as shown in Fig. 28. It was about 0.31 ms.

3. EU–KR Interconnection Integration and System Testing Results

A. EU → KR Testing

Testing was performed with LTE access on the EU side and on the ETRI side with LTE. A PC with an LTE USB stick with jPerf/iPerf tools was used. The simplified test scenario is shown in Fig. 29. The LTE band used is Band 7, and the bandwidth is 5 MHz.

• EU–KR iPerf Testing with TCP

We performed iPerf testing with LTE access with TCP traffic. The uplink bandwidth was about 9.31 Mb/s. The

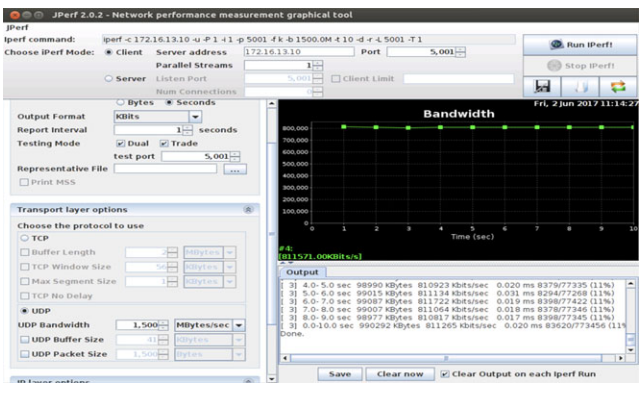


Fig. 27. iPerf testing with UDP traffic: client view.

```
root@hongseok-01:/home/hongseok/jperf-2.0.2# ping 172.16.13.10
PING 172.16.13.10 (172.16.13.10) 56(84) bytes of data.
64 bytes from 172.16.13.10: icmp_seq=1 ttl=64 time=0.399 ms
64 bytes from 172.16.13.10: icmp_seq=2 ttl=64 time=0.266 ms
64 bytes from 172.16.13.10: icmp_seq=3 ttl=64 time=0.229 ms
64 bytes from 172.16.13.10: icmp_seq=4 ttl=64 time=0.213 ms
64 bytes from 172.16.13.10: icmp_seq=5 ttl=64 time=0.235 ms
64 bytes from 172.16.13.10: icmp_seq=6 ttl=64 time=0.396 ms
64 bytes from 172.16.13.10: icmp_seq=7 ttl=64 time=0.276 ms
64 bytes from 172.16.13.10: icmp_seq=8 ttl=64 time=0.416 ms
64 bytes from 172.16.13.10: icmp_seq=9 ttl=64 time=0.360 ms
^C
--- 172.16.13.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8178ms
rtt min/avg/max/mdev = 0.213/0.310/0.416/0.077 ms
root@hongseok-01:/home/hongseok/jperf-2.0.2#
```

Fig. 28. Ping testing with the ETRI server.

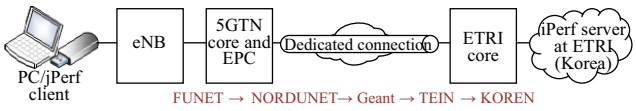


Fig. 29. EU–KR testing scenario with LTE access.

performance was as much as expected with the 5-MHz bandwidth. The iPerf tool does not support downlink measurement when there is NAT between the end points (NAT is carried out at the LTE USB stick). The bandwidth between the EU and KR at the CN is sufficient to obtain this uplink bandwidth with LTE access.

• EU–KR iPerf Testing with UDP

We performed iPerf testing with LTE access with UDP traffic. The uplink bandwidth was about 11.1 Mb/s. The jitter was about 1.5 ms. The performance was as much as expected with the 5-MHz bandwidth. The iPerf tool does not support downlink measurement when there is NAT between the end points (NAT is carried out at the LTE USB stick). The bandwidth between the EU and KR at the CN is sufficient to obtain this uplink bandwidth with LTE access.

• EU–KR Ping Testing

The RTT was measured using a ping test, as shown in Fig. 30. The average was about 413 ms.

B. KR → EU Testing

In order to test the performance of the interconnection link between the mobile CNs in KR and Europe, a client PC

```
C:\Users\jarimoil\jperf\jperf-2.0.2\bin>ping 172.16.13.10

Pinging 172.16.13.10 with 32 bytes of data:
Reply from 172.16.13.10: bytes=32 time=417ms TTL=61
Reply from 172.16.13.10: bytes=32 time=371ms TTL=61
Reply from 172.16.13.10: bytes=32 time=413ms TTL=61
Reply from 172.16.13.10: bytes=32 time=451ms TTL=61

Ping statistics for 172.16.13.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 371ms, Maximum = 451ms, Average = 413ms

C:\Users\jarimoil\jperf\jperf-2.0.2\bin>tracert 172.16.13.10

Tracing route to 172.16.13.10 over a maximum of 30 hops

  1    22 ms    28 ms    29 ms  hi.link [192.168.8.1]
  2     *        *        *     Request timed out.
  3   140 ms    83 ms   114 ms  193.166.30.153
  4    42 ms    71 ms    34 ms  5gtn-epc-oulu-gw.oulu.fi [193.166.31.241]
  5   405 ms   398 ms   399 ms  172.16.13.10

Trace complete.
```

Fig. 30. EU–KR ping test.

https://doi.org/10.4218/etrij.2017-0236

with jPerf/iPerf tools for initiating the test on the Korean side was connected to the 5GMC, as shown in Fig. 31.

• KR-EU iPerf testing with TCP

Figure 32 shows the results for iPerf testing with TCP traffic. The green dotted line shows the uplink direction, and the blue line shows the downlink direction. The uplink bandwidth was about 59.8 Mb/s. The downlink bandwidth was about 37.8 Mb/s. A long RTT (over 300 ms) affected the bandwidth with TCP traffic, which has delicate flow control and an error control mechanism as a connection-oriented transport protocol.

• KR–EU iPerf Testing with UDP

With iPerf testing with UDP traffic, both the uplink and downlink bandwidths were measured to be about 812 Mb/s, similarly to the 1,470-b-sized UDP datagram traffic. The jitter was 0.023 ms on average. The results encouragingly show almost full bandwidth considering that the maximum bandwidth between KR and the EU is 1 Gbps.

• KR–EU Ping Testing

The RTT was measured using a ping test. The average was about 304 ms.

C. 4K Video Demo

4K video streaming was demonstrated via our L2VPN dedicated connection and public internet access to compare the quality. Video servers were located in KR. Video streaming used UDP transfer. The downlink bandwidth could be verified by the computer's performance tools available from the "Task Manager." With dedicated access, 4K video streaming showed very good performance, and the downlink bandwidth used was about 60 Mb/s to 65 Mb/s. The bandwidth was less than 10% of the total available bandwidth. However, 4K video streaming via the public internet exhibited very bad quality. The downlink bandwidth via the public internet was about 8 Mb/s, which was not sufficient to obtain a good end-user experience.

Fig. 31. EU–KR testing scenario.

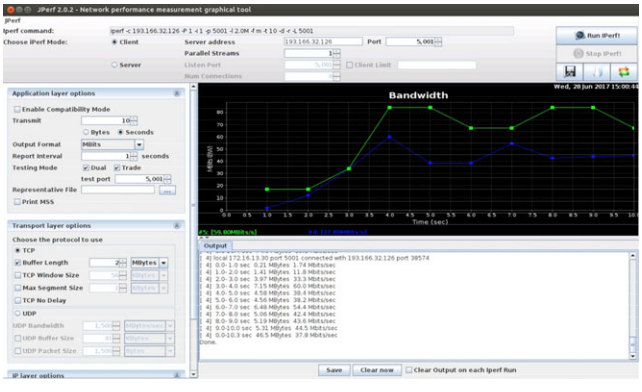


Fig. 32. EU–KR iPerf testing with TCP traffic in the uplink.

4. Performance Evaluation of the 5G CN Security Management Mechanism

In present mobile networks, IPsec tunneling and security gateways are widely used to secure backhaul communication. We have worked on a novel communication architecture based on the HIP to secure both the control and data channels in SDMNs. We aimed to analyze the added security features as well as the performance penalty on both the control and data channels inherent to the proposed simplified architecture (shown in Fig. 33). These performance penalties are considered in terms of the throughput, jitter, and latency. The key performance indicators in our performance analysis are [10].

- The performance penalty of security on the TCP throughput
- The performance penalty of security on the UDP throughput
- The latency introduced
- The performance penalty of security on the jitter

A. Performance Analysis of the Control Channel

In the first set of experiments, we analyze the performance penalty of security on the SDMN control channel due to the proposed architecture.

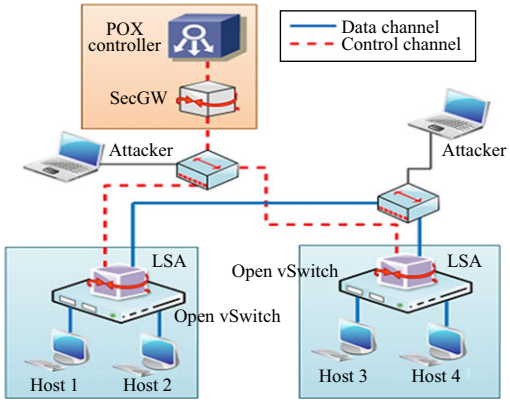


Fig. 33. Testbed for the IPsec tunneling architecture for SDMN communication channels.

• Connection Establishment Delay

In the first experiment, we measure the connection establishment delay between Open vSwitch 1 and the POX SDN controller under different scenarios. Here, we attempt to send a ping request from Host 1 to Host 2 and measure the connection establishment delay. The experimental results in Fig. 34 reveal that the proposed secure architecture significantly increases (136%) the tunnel establishment delay. HIP tunnel establishment between the local security authority (LSA) and the secure gateway (SecGW) adds an extra delay to tunnel establishment. However, the impact of this delay can be minimized by maintaining the established HIP tunnels for a long period. It is possible to maintain established HIP tunnels for long periods (that is, 15 min).

• Flow Table Update Delay

In the second experiment, we measure the delay to update the flow tables for a new packet flow during steady-state operation. In steady-state operation, the HIP tunnels between the LSAs and the SecGW are already established and operational. Here, we ping from Host 1 to Host 2 and measure the RTT. The experimental results in Fig. 35 reveal that the performance penalty of the proposed secure architecture is less significant in steady-state operation. The extra IPsec encryption increases the flow update delay by only 2%. However, this delay can be further minimized by using IPsec accelerators. IPsec acceleration is possible by using external accelerators and/or using new Advanced Encryption Standard instruction sets for processors.

B. Performance Analysis of the Data Channel

In the second set of experiments, we measure the TCP and UDP throughput performance of the data channel in different scenarios.

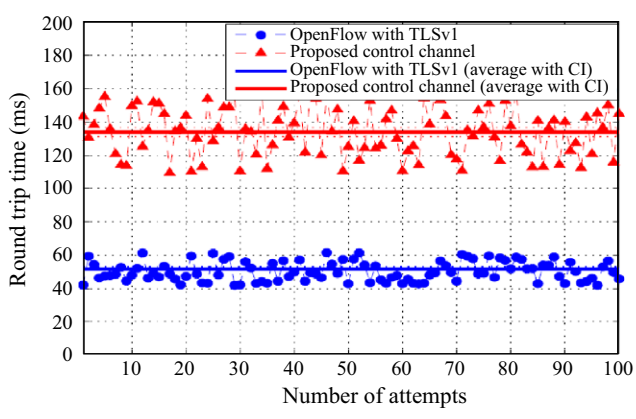


Fig. 34. Connection establishment delay.

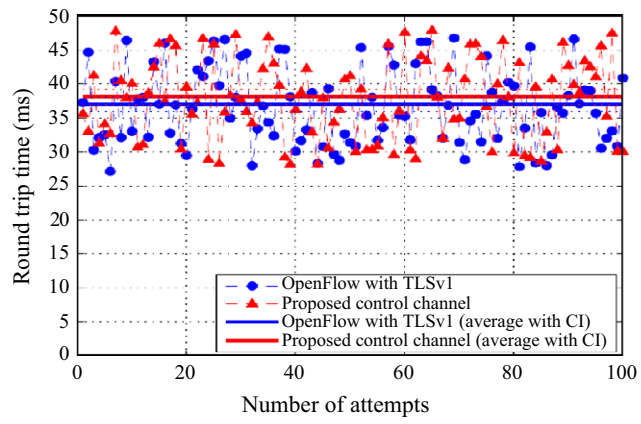


Fig. 35. Flow table update delay.

• Impact on the TCP Throughput

In third experiment, we establish a TCP connection between Host 1 and Host 3 to measure the TCP throughput performance of data channel by using the iPerf tool. The experimental results in Fig. 36 reveal that the proposed secure architecture decreases the TCP throughput by only 2.3% compared to that of the nonsecure data channel. The extra layer of encryption decreases the TCP throughput.

• Impact on the UDP Throughput

In fourth experiment, we establish a UDP connection between Host 1 and Host 3 to measure the UDP throughput performance of the data channel. The experimental results in Fig. 37 reveal that the proposed secure architecture decreases the UDP throughput by only 2.2% compared to that of the nonsecure data channel. The extra layer of encryption decreases the UDP throughput. Moreover, the performance penalty of security on the throughput is around 2% for both the UDP and TCP sessions compared with that of the nonsecure scenario. Thus, we can conclude that the performance penalty of

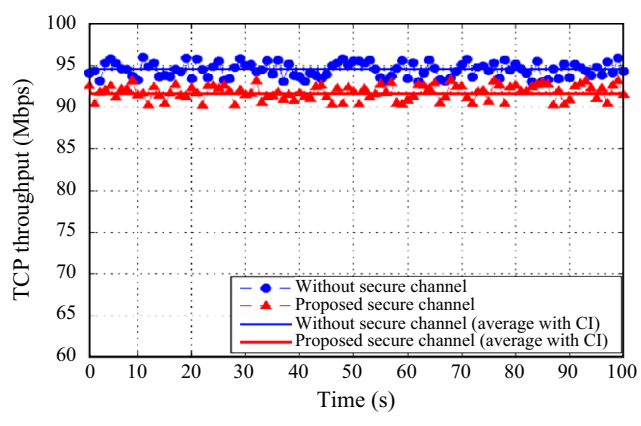


Fig. 36. Performance penalty on the TCP throughput.

https://doi.org/10.4218/etrij.2017-0236

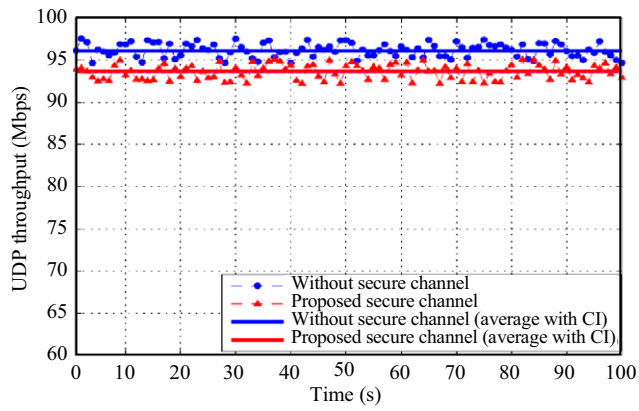


Fig. 37. Performance penalty on the UDP throughput.

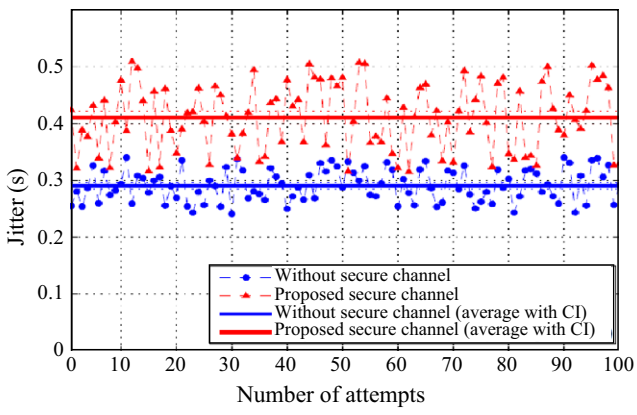


Fig. 38. Performance penalty on the jitter.

security on the throughput is independent of the transport layer protocol.

• Impact on the Jitter

In fifth experiment, the jitter performance of a UDP session between Host 1 and Host 3 is measured by using the iPerf tool. The experimental results in Fig. 38 reveal that the performance penalty of the secured architecture is 41% relative to the nonsecure data channel. However, the jitter is still well below 500 μs (voice over IP (VoIP) requires a jitter below 4 ms), and the impact of jitter for real-time applications such as VoIP and video streaming is less significant in a short-range network.

VI. Conclusion and Future Work

In this paper, we proposed an SDN/NFV-enriched intelligent 5G CN and its agile MANO system to address 5G KPIs. As details of the proposed system, we presented the architecture of the virtualized CN capabilities and its agile management. Furthermore, we shared our implementation, its deployment, and our interoperability testing experiences with PoC use cases. As described, we are currently in the second phase of conformance and interoperability testing of the proposed system functionality. Our future work includes a performance evaluation of the proposed solution in an end-to-end scope (UE-5G access-5G core–data center with application servers) in a PoC testing environment, which is the PyeongChang Olympic venue.

Acknowledgements

This work was supported by a grant from the Institute for Information & Communications Technology Promotion (IITP) funded by the Korean government (MSIT) (No. B0115-16-0001, 5G Communication with a Heterogeneous, Agile Mobile Network in the PyeongChang Winter Olympic Competition) and the European Union H2020 5GPPP under grant number 723247.

References

[1] H. Shokri, C. Fischione, G. Fodor, P. Popovski, and M. Zorzi, "Millimeter Wave Cellular Networks: A MAC Layer Perspective," *IEEE Trans. Commun.*, vol. 63, no. 10, Oct. 2015, pp. 3437–3458.

[2] V. Desai, L. Krzymien, P. Sartori, W. Xiao, Z. Soong, and A. Alkhateeb, "Initial Beamforming for mmWave Communications," *Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2–5, 2014, pp. 1926–1930.

[3] E.C. Strinati and H.K. Chung, *5G CHAMPION*, 2017. Accessed Dec. 31, 2017. http://www.5g-champion.eu/

[4] G. Cross, *Open Networking Forum SDN Standards*, 2017. Accessed Nov. 15, 2017. https://www.opennetworking.org/software-defined-standards/overview/

[5] ITU-T SG13 TSB, *ITU-T SG13 WP1 Q.21*, 2017, Accessed Nov 15, 2017. http://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.asp

[6] Linux Foundation Projects, ODL Open Source Project, 2017, Accessed Nov. 15, 2017. https://www.opendaylight.org/what-we-do/odl-platform-overview

[7] G. Cross, *ONOS Open Source Project*, 2017, Accessed Nov. 15, 2017. https://www.opennetworking.org/platforms/onos/

[8] J. Quittek et al., "Network Functions Virtualisation (NFV) – Management and Orchestration V.1.1.1," ETSI NFV ISG, Dec. 2014.

[9] R. Schuster et al., "An Introduction to the New ETSI Industry Specification Group (ISG) for Mobile Edge Computing (MEC)," ETSI MEC ISG, Oct. 2015.

[10] J. Moilanen et al., "Operator Grade NFV-Based and SDN-Enriched EPC Environment at 5GTN (D4.1)," 5G CHAMPION Project, May 2017.

[11] M. Liyanage, A. Gurtov, and M. Ylianttila, "*Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*," Chichester, UK: John Wiley & Sons, 2015.

[12] R. Banerjee et al., "5G CHAMPION Architecture, API-and Interface Document (D2.1)," 5GCHAMPION Project, Oct. 2016.

[13] J. Moilanen et al., "VNF/SDN/EPC: Integration and System Testing (D6.2)," 5GCHAMPION Project, June 2017.

Taesang Choi received his MS and PhD degrees in computer science and telecommunications from the University of Kansas City, MO, USA in 1988 and 1995, respectively. He joined the ETRI, Daejeon, Rep. of Korea in 1996 and is currently working as principal research staff. He has been actively involved in the research and development of traffic engineering, traffic measurement and analysis, SDN/NFV management, and 5G network slice management. He has also actively contributed to various SDOs and open-source activities such as IETF, ITU-T, ONF, ONOS, and others. He is currently acting as an ITU-T SG13 Question 6 Rapporteur and International IT Standardization Expert representing the Rep. of Korea.

TaeYeon Kim received his PhD degree in computer science from Chungbuk National University, Chungju, Rep. of Korea in 2007. He also received BS and MS degrees from Chung-Ang University, Seoul, Rep. of Korea in 1990 and 1992, respectively. He joined the ETRI, Daejeon, Rep. of Korea in 1992. His current research includes network and computing convergence platforms and SDN and NFV technologies for future networks.

Wouter Tavernier received his BS and MS degrees in computer science in 2002 from Ghent University, Belgium. He joined the Internet-Based Communications Networks group (which became part of IDLab in October 2016) of Ghent University in 2006 as researcher on Carrier Ethernet. In 2012, he obtained a PhD degree from the same university on reliable routing and switching. Currently he is employed as a professor at Ghent University. His current research interests focus on the performance aspects of software-defined networks and network function virtualization. This work is performed in the context of European projects such as H2020 5G-CHAMPION, SONATA-NFV, and 5G TANGO. This research has been published in more than 50 scientific publications.

Aki Korvala received his BS degree from the Technical Institute of Oulu, Department of Electrical Engineering, in 1997. He has worked at Nokia for 18 years in various R&D positions within mobile phones and network business lines. Currently, he is working in the 5G area as a program manager. This work is performed in the context of European projects such as H2020 5G-CHAMPION.

Jussi Pajunpää has worked at Nokia Networks, Espoo, Finland for 19 years in various R&D positions in software and systems engineering in the core network domain. Currently, he is working with the Telco Cloud and virtual network function architecture as a chief architect and R&D manager and contributing to the 5G test network activities in Oulu.