SOFTWARE-DEFINED AND VIRTUALIZED MOBILE NETWORKS

SIGMONA white paper

February 29th, 2016

SIGMONA partners

www.sigmona.org

www.celticplus.eu

SIGMONA is a European research project run under the Celtic-Plus cluster of Eureka performed in Finland, France, Germany, Hungary, Spain and Turkey during 2013-2016.

Disclaimer: *All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, any party of the SIGMONA Project has no liability in respect of this document, which is merely representing the authors' view.*

EXECUTIVE SUMMARY

Traffic volumes in mobile networks are increasing and end-user needs are changing rapidly. Mobile network operators need more flexibility, lower network operating costs, faster service roll-out cycles and new revenue sources. One answer to this tough call is the combination of software-defined networking (SDN) and network functions virtualization (NFV). The first means the separation of the control plane from the data plane in networking equipment. The latter refers to executing the control (and management) plane functions in virtual machines using cloud computing to support the execution.

The Celtic-Plus SIGMONA project has integrated the concepts of SDN and NFV into LTE mobile networks with specific focus on flexible end-to-end SDN/NFV architecture, efficient backhaul network, optimized mobility management, dynamic resource management and improved security. This white paper describes the technical contributions of SIGMONA in regards to SDN/NFV architecture and implementation and discusses the related technology and business impacts.

- SDN/NFV improves the flexibility of resource allocation on demand in mobile networks in terms of 1) transport resources following the movements of crowds of users, and 2) services. Examples of new services are flexible caching in an optimal location, flexible service chaining and scaling the computing, memory and network capacity. As a result the responsiveness of the mobile network to user demand can be improved.
- SDN/NFV allows better implementation of many existing network functions using location optimization and virtualization. Data collection from virtual functions is easy. An example is network and end system security that can benefit from ubiquitous incident evidence collection, aggregation of that evidence and implementing coherent security policies.
- For operators, the exploitation of the new network technologies includes also capital and operational expenditure benefits due to the more efficient network operation. In addition, SDN/NFV may change the conditions for competition of incumbent, challenger, mobile virtual network operators and service providers. SDN/NFV enables: 1) decoupling supplier’s hardware and software business models, 2) new software-only suppliers without Telco legacy, 3) opening up new opportunities for software integrators, 4) changing the time-to-market of new functionalities, and 5) easier entries to market by new entrants and higher competition.
- The high level SIGMONA architecture considers three possibilities for placing the controller in the LTE network, which would move the control plane functionalities into centralized servers. The approaches support the gradual introduction of SDN into live networks providing high network throughputs, optimal flow management and traffic engineering possibilities.
- A concern is that the wide scale deployment of the new network technologies can trigger a number of security and data protection risks stemming mainly from the new interfaces, shared environments, new actors with different views and objectives on security and privacy, and from the more complicated value networks.

The results serve as a baseline for future studies, especially ones leading to the standardization of SDN/NFV concepts in relation to 5G networks. The performance bottlenecks and scalability of the virtualized functions in higher load also remain as future study items. In addition, the possible disruptions caused by new entrants and higher competition need further understanding in order for the relevant actors to efficiently cope with the opportunities and threats.

MARKET OVERVIEW

This white paper describes the technology and business shift created by two complementary technologies, namely software-defined networking (SDN) and network function virtualization (NFV). The first means the separation of the control plane from the data plane in networking equipment. The latter refers to executing the control (and management) plane functions in virtual machines or containers using cloud computing to support the execution. The mobile network architecture optimization for the cloud computing and even micro service principles have been studied. The focus of the white paper is on aspects that have the potential to disrupt the telecommunication ecosystem. The white paper summarizes the insights gained in the Celtic-Plus SIGMONA project using design and experimentation to understand the technical feasibility of the SDN/NFV phenomena. This paper is focused on the case when SDN uses the OpenFlow protocol.

The changing market

The Internet access and connectivity market is changing, as end users expect fast connections and high quality services at any time and any place. For example, some mature markets are seeing 2 GB of data per month per user today, with a 15-fold increase likely by 2020. In developing markets, operators are typically delivering 500 MB per month per user today and could even experience a 60-fold increase by 2020. At the same time, end users are accustomed to affordable broadband pricing in both fixed and mobile networks. In addition, the focus is shifting from Internet access towards high quality content, fueled by hundreds of thousands of data apps and hundreds of millions of data-hungry smartphones, tablets and new devices. For example, video contributes to more than 50% of mobile data traffic today and would remain the most important driver of mobile broadband. As a consequence, the connectivity business is providing less revenue per subscriber for both fixed and mobile network operators.

Another important change in the ICT market is the shift from dedicated hardware to software and cloud technologies. Cloud platforms and open source software are also emerging in the mobile networks together with SDN and NFV. For example, there is agreement in the mobile industry that cloudification, virtualization and SDN will radically change the mobile core. The obvious transformation brought about by these technologies is the migration of application software from proprietary, application specific hardware platforms to virtualized compute servers deployed in a few large scale data centers. This migration to virtualized machines lowers the initial investment costs and, thus, opens up the high entry barrier mobile network provisioning market to new entrants and higher competition.

Future wireless networks will interconnect humans, machines and things, and enable very diverse use cases, playing a key role in expanding the human possibilities of technology. The hardware evolution and application innovation will continue to drive the exponential growth in demand for personalized mobile broadband in the next decade. This demand and the associated usage profile define the key requirements for future mobile networks in terms of capacity, latency, automation, personalization, resource utilization and energy efficiency.

Operator challenges

To provide new value for the over-the-top services in the mobile networks and avoid losing market share, operators need to find new revenue sources and provide new services flexibly on-demand. In addition, the cost efficiency of the mobile networks should be improved to increase the profitability of the operators. To achieve cost efficiency and faster service roll-out, and to meet the changing demand of end users, the network capacity should be flexible and dynamically reconfigurable. In addition, to cope with the increased end-user mobility expectations, more efficient roaming and mobility management is needed. Lastly, as personal and sensitive data are stored in cloud servers, network security and privacy issues have to be addressed.

SDN/NFV benefits

SDN/NFV is an attempt to provide better control and automation over the resource management (e.g. network, computing, storage and software) by dynamically allocating the resources to meet the needs of different end users (i.e. consumers and corporate customers). Instead of just Best Effort services, SDN/NFV can be used to provide Carrier grade services. Carrier grade means that there is a clear definition of the traffic, its properties and the entry and exit points of the traffic. The goal is to provide elastic and agile tailoring of the resource allocation based on demand. Due to the control plane and data plane split, SDN provides better hardware independence for the operators than before. In addition, NFV and the use of standard data center hardware provides economies of scale in computing and storage resources.

SDN's centralized controller system provides the possibility to differentiate the services by controlling what service is available to whom and where. Centralization makes it easy to implement many functions that are uneconomical or infeasible in a distributed setting. Examples include 1) residual capacity routing for network provisioning, and 2) better network-based end-system security by executing consistent policies irrespective of location/roaming, sharing evidence of malicious activity, aggregation of that evidence and using reputation based methods.

From the business side, the SDN/NFV architecture lowers the initial network investment, energy consumption and network management costs for the operators. At the same time, SDN/NFV encourages openness and competition, as well as promotes new investments into the mobile connectivity and content industry. In addition, SDN changes the competitive advantage of the different operator types (e.g. incumbent, challenger, global hub, virtual, infrastructure, cloud/non-cloud) with each other and with the infrastructure providers. SDN/NFV also opens the possibility for each service provider to decide what exactly to invest in: infrastructure, software or customer service, as well as increases the speed at which the new services are implemented and delivered.

MORE COMPETITION – LESS COST

Impact on market roles

New technologies can either sustain or disrupt a market, thus, the perceived benefit by the relevant actors depends on the resulting scenario market or industry architecture. SDN/NFV creates new technical elements and therefore potentially also new business roles that can be taken by existing or completely new actors. The impact of such new actors can be high, but the following summary mainly focuses on the impact of SDN/NFV on existing actors. The considered actors in the mobile connectivity market include mobile network operators (MNO), mobile virtual network operators (MVNO), telecom infrastructure providers, consumers and corporate customers. The scenario markets are illustrated in Figure 1. Industry architectures for the scenarios are illustrations in Figures 19.7, 19.8, 19.10 and 19.12 in Zhang et al. (2015).

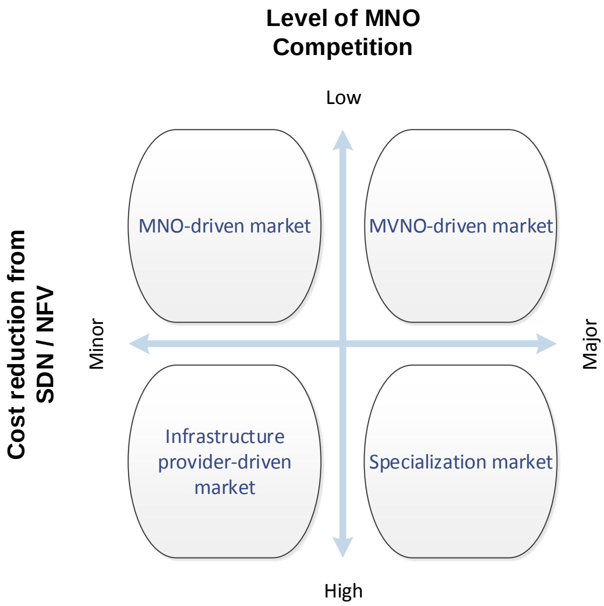

Figure 1. Industry scenarios.

1) MNO-driven market: Operators drive the adoption of SDN/NFV and operate all the parts of the mobile network.
2) MVNO-driven market: Virtual operators manage the subscriber management and lease the core and radio networks from operators.
3) Infrastructure provider-driven market: Full virtual operators manage most of the network, leaving only the base stations and backhaul switches for operators. The virtual operator role could be taken by a large telecom infrastructure provider that operates in several countries.
4) Specialization market: Each actor has its specialized role in the market. Virtual operators control the subscription management, mobility providers manage mobility, connectivity providers handle backhaul routing and forwarding, and operators only control the radio access.

From the operator perspective, all SDN/NFV scenarios provide CAPEX and OPEX savings compared to the current LTE. The first two scenarios offer operators a potential for higher revenue through differentiating services to different end-user groups, whereas the third and fourth scenarios strip operator’s control over the network.

In the MVNO-driven and specialization markets, the virtual operator has lower barrier to enter the market compared with the MNO-driven market. The virtual operator also sees potential economies of scale benefits and higher bargaining power for interconnection in the Infrastructure provider-driven market.

The infrastructure providers can roll-out services faster in all four scenarios compared with current LTE. Infrastructure provider-driven and Specialization markets both offer economies of scale benefits to the infrastructure provider. However, the infrastructure provider also has higher bargaining power for interconnection and more efficient network operation in the Infrastructure provider-driven market.

The MNO-driven market has the potential to offer higher service qualities to consumers. The rest of the scenarios may lower prices for consumers either due to increased competition or economies of scale. In addition, all scenarios can offer better targeted services to corporate customers.

Cost impact

An important aspect of SDN is the potential cost savings for operators. A Finnish reference network is used to model the cost efficiency of SDN-LTE compared with current LTE. The topology of the Finnish SDN-LTE network is illustrated in Zhang and Hämmäinen (2015) together with the capacity for each of the network elements. The cost model used is shown in Figure 2. For more detailed description of the cost model input parameters, please refer to Zhang and Hämmäinen (2015).

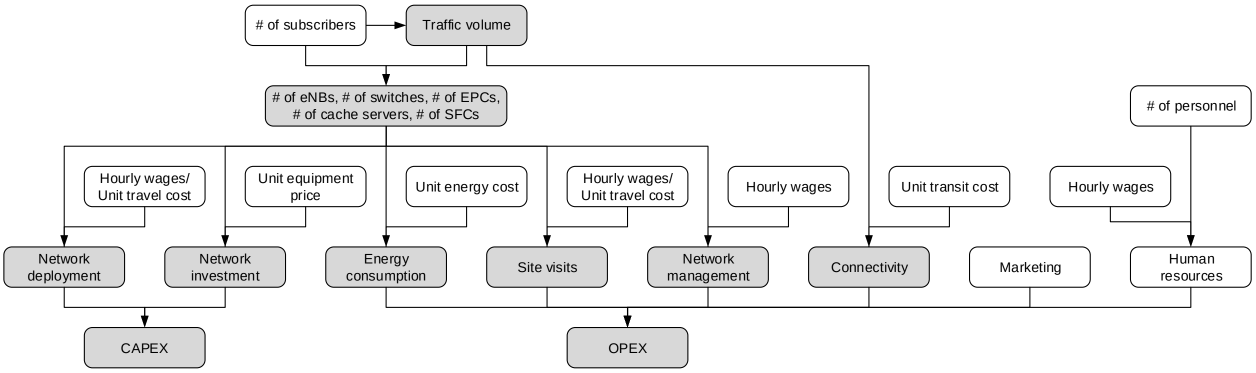

Figure 2. Cost model.

For an operator with the considered topology and approximately 3 million subscriptions, the cost modeling results indicate that SDN reduces network-related CAPEX by 7.7% and network-related OPEX by 0.3%. Keeping in mind that the Finnish population is low and the network is coverage limited, a more densely populated network has the potential for higher cost savings.

Regulatory impact

The new technologies under study in the mobile telecommunications project can become viable only if the economic advantage of their deployment becomes feasible. Besides the business aspects, the regulation aspects of the operated networks need to be taken into consideration in order to create a healthy market environment. The goals of the regulatory activity in the telecommunications industry can be described as to promote competition and to supply a country with sufficient and adequate services.

Regulation is affected by the technological development in three different ways. First, there is a direct impact, where new technologies lead to the development of new services and modes of delivery unforeseen by the existing regulation. Second, new technologies affect the overall market structure and the level of competition by changing conditions for supply. Third, the new technological opportunities create a demand for new types of services, which again affect the overall market structure. In the SIGMONA project, the focus was at first on the direct impact of new technologies on regulation, especially from the perspectives of issues on interconnections and security and privacy. Then, the impact on regulation of the new business scenarios created in SIGMONA was studied.

From the studies carried out in the project, it can be concluded that:

- For the benefits of the end users, the EU regulatory policies shall and will promote the deployment of such technologies, which will enhance the market by enabling the more efficient use of investments, new entries and competition, and innovation.
- For boosting the competition, the interoperability across the technical interfaces and the fair service level agreements between the involved parties is of key importance. When the new technologies are deployed, the regulators have to pay attention to the availability, capacity and quality of interconnections.
- The large-scale deployment of the new technologies can trigger a number of security and data protection risks stemming mainly from the new interfaces, shared environments, new actors with different views and objectives on the security and privacy levels, and from the more complicated value networks. The study supports the assessment of the Network and Information Security Directive that the government regulation would best promote the targets for security and privacy.
- New security and privacy issues in the context of new technologies are more of global nature than ever before, and EU-wide (or rather global) standards and practices are needed in regulation. This is also important for enabling new entries to the market. The location of legal disputes has to be clear and agreed on.
- The new technologies are expected to promote competition rather than the opposite. The increased competition would be the result of the lower OPEX/CAPEX, new entries of the standard hardware and software providers, new application providers enabled by the APIs, new flexibility to set up virtual operators, and new value chain structures. While the regulation should promote the new market entries it should also pay attention to that the division of responsibilities between several new actors would not risk the objectives set for the security and privacy in telecommunications.

FLEXIBLE END-TO-END ARCHITECTURE

This section proposes solutions to integrate software-defined networking (SDN) technology and network function virtualization (NFV) with wide area LTE and further 5G mobile networks. This integration is motivated by 1) the possibility to provide new services to a part of LTE users, while the rest are served by existing network equipment, 2) the possibility of experimenting with new services for LTE users, and 3) the prospect of using SDN/NFV to control all traffic in 5G.

The integration of SDN into mobile networks to become the software-defined mobile network (SDMN) poses several architecture alternatives. The integration of SDN in mobile networks requires maintaining basic functionalities, such as policy control and charging. The SIGMONA architecture considers multiple options for the placement of the SDN controller. We introduce a vision for integrating SDN in the mobile network, where mobile specific functionalities are implemented as SDN applications in a way that allows smooth introduction of SDN/NFV to existing LTE networks.

LTE network – a starting point

Mobile networks consist of physical and logical entities. The physical layer is made of network routers (Layer 3), switches (Layer 2), and physical links (Layer 1) with different technologies and topologies. The logical layer consists of network elements, such as evolved Node B (eNB), mobility management entity (MME), serving/packet data network gateways (S/P-GW) and home subscriber server (HSS), which perform the attachment of user devices, mobility and transport of data from mobile devices across the mobile network. The physical layer (Layer 2 and Layer 3) provides the connectivity and transport functionality to the logical layer, which implements the mobile specific control functions.

Movements of user devices are hidden from the Internet by assigning an IP address to the device at its point of attachment to the Internet, i.e. at P-GW, and tunneling IP packets over the GPRS tunneling protocol (GTP) between P-GW and eNB. It is the responsibility of the MME to move the tunnel as the mobile device moves from one eNB to another.

From LTE to SDMN

The deployment of SDN with the LTE network elements should follow a progressive step-wise process to allow a smooth transition of SDN functionalities into a live mobile network. In SIGMONA, different approaches for the data plane are experimented and are discussed under “Mobility Management”.

For the controller integration, one option in the current LTE architecture is to decouple the S/P-GW into the control and data planes. The control part of the S/P-GW (i.e. S/P-GW-C) provides IP address allocation for the end user. The data plane of the S/P-GW (i.e. S/P-GW-U) provides the GTP tunneling termination end point and the anchoring of the GTP tunnels during the handover process. The control part of the S/P-GW is integrated with the SDN controller. The rest of the network elements are not changed and the MME interacts with the S/P-GW-C.

A second option integrates the SDN controller with the MME as shown in Figure 3. This option allows the SDN controller to learn about mobility events directly from the MME and to apply new rules in the switching nodes to re-establish routing paths in an optimal manner. In Figure 3, the OpenFlow based data plane between the base stations and S/P-GW need to understand GTP.

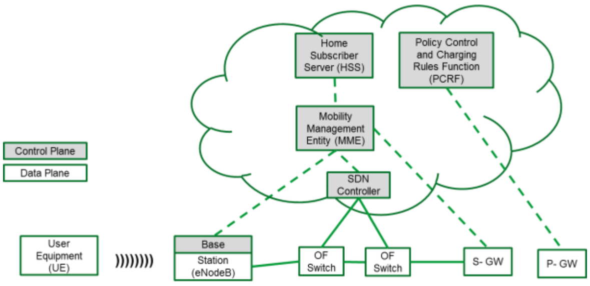

Figure 3. Integration of SDN controller with MME.

A third option concentrates on optimizing the EPC architecture for the NFV cloud architecture by consolidating the control plane functions. The different user’s subscription context data, which is currently maintained within the core network elements (e.g., MME, S-/P-GW), is largely independent on each other and this enables parallel processing. Cloud-based scaling methods with shared subscription database can be utilized with a single stateless transaction worker instead of the separate network elements. The transaction worker would have the functional capability to manage all the functional needs of a single user’s state management. The EPC S/P-GW functionalities are separated to control and data plane functionalities with the SDN principles. The architecture combines MME and S/P-GW control functionality with GW-U context creation capability and integrates that with the split GW’s distributed data plane and NFV/OpenStack environment.

The end result of these options is that the control plane is moved out of the basic networking elements into centralized servers – these servers resemble classical anchor points used in many mobility protocols. Therefore, it makes sense to group the controller and current S/P-GW functionalities in the same network application together with the MME functionality. In SIGMONA, this application is called the mobility and session management app. In this approach, the currently independent S/P-GW elements evolve into SDN controlled forwarding elements. This approach adds flexibility (e.g. by enabling relocation of IP anchor point, easier provision of caching and monitoring) and value to networking (reduced signaling and packet overhead) with different increments and support the gradual introduction of high network throughputs, optimal flow management and traffic engineering possibilities.

Software-defined LTE network

Figure 4 shows the model of the SDN/NFV slice of the LTE network, where the control and data planes are separated. The data plane is handled by OpenFlow switches and partially by legacy 802.1 or MPLS switches, and the control plane is structured as a set of SDN applications.

In Figure 4, backhaul provisioning is responsible for provisioning of the data paths from eNBs and the Internet. Network monitoring is needed for example to ensure the required QoS. The mobility management app includes the MME and interoperates with legacy MMEs. The mobility management app can also provide Mobility as a Service (MaaS), which hides the mobility from the Internet access app and presents each device at the MaaS interface to Internet access app. In Figure 4, P-GW has been replaced by the Internet access app, which may be owned by operators or virtual operators.

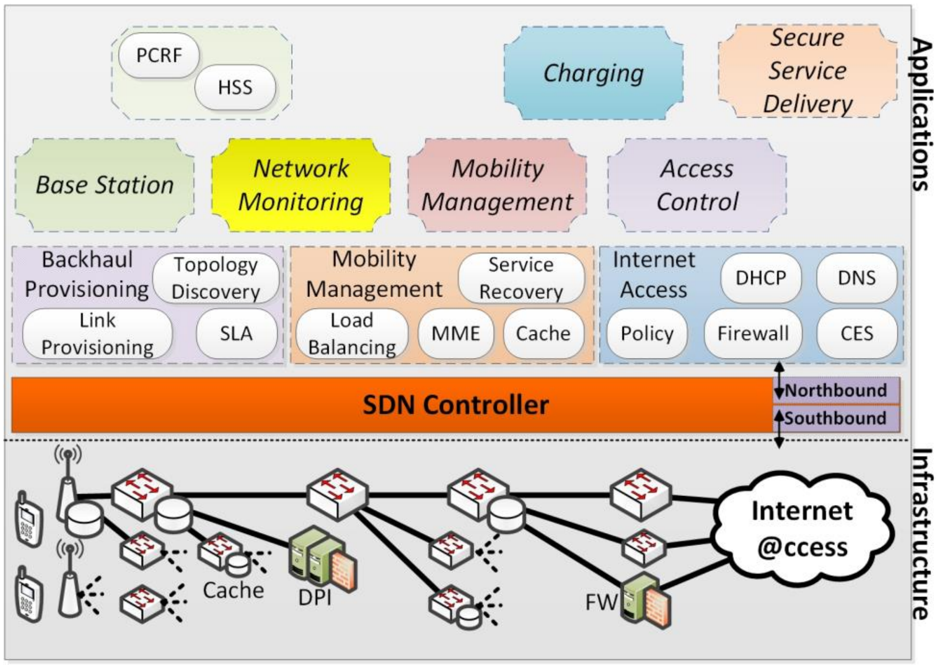

Figure 4. SDN/NFV controlled LTE network.

In Figure 4, the role of the Internet access app is to manage the Internet service for the mobile device possibly enforcing a suitable security policy, allocating the Internet address and giving assurances to others related to those addresses. Internet access app performance requirements (time to attach, detach, admit session) are determined by the end-user responsiveness requirements. These are more relaxed than the time constraints on the mobility management app. Therefore the Internet access app function is suitable for cloud based implementations. The SIGMONA implementation of the Internet access app is based on customer edge switching functions. Customer edge switching executes cooperative firewalling and is able to give assurances to others related to the IP addresses that it allocates to mobile devices and uses for the entry points to the Internet.

By bringing caching closer to the end user, it is possible to reduce delays experienced by the users and reduce the capacity at the point of Internet access. Consequently, the interconnection charges the operators pay for Internet access is reduced.

OPTIMAL BACKHAUL ROUTING

The exponential growth of mobile traffic and the increasing difficulty of predicting peak demands are two challenges that make it more important than ever to improve network performance. Traffic backhaul plays an important but often overlooked role in the end-to-end performance of mobile operator networks. Complex backhaul topologies are needed in order to connect the large number of cells in growing mobile networks. Yet configuring and optimizing current backhaul solutions require a lot of manual work by highly qualified and expensive personnel. Because of the manual work, the configuration and optimization cycles take too long and are vulnerable to mistakes.

SDN and NFV create a programmable backhaul environment that overcomes these issues by providing means for real-time optimization of the backhaul networks. Figure 5 shows the main building blocks proposed by the SIGMONA project making it possible to harvest the benefits of mobile backhaul (MBH) programmability: 1) Wireless mesh networking (WMN) mediator, 2) self-organizing networks (SON) for mobile backhaul, and 3) integrated radio access network and MBH optimization.

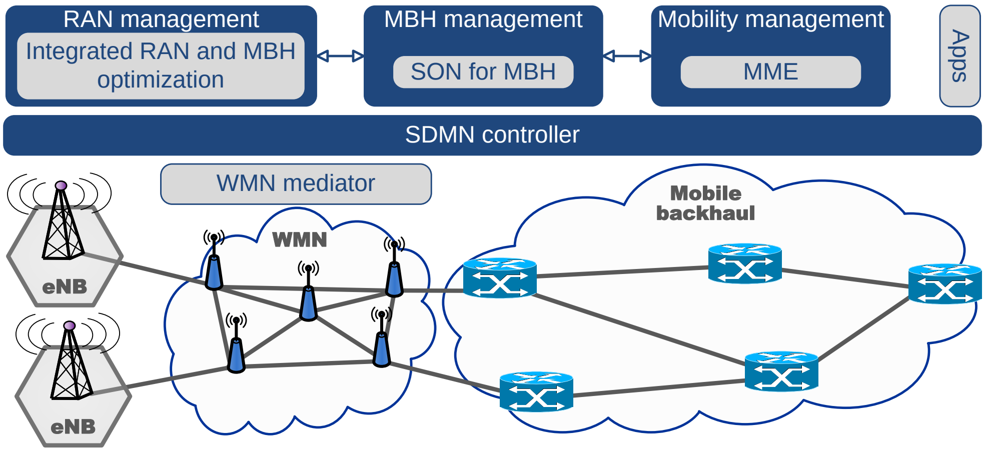

Figure 5. SDN enabled mobile backhaul optimization.

WMN is an important last-mile solution in mobile backhaul networks. However, integrating it to SDN is challenging due to WMN's special requirements like very low latency management functionalities. The approach to this integration problem is to leave most of the WMN functions as they are in the current solutions by hiding the WMN internal structure and operations (routing inside the WMN, fault recovery, load-balancing, etc.) from the SDN controller. This is achieved by deploying a WMN mediator functionality between the WMN and the SDN controller; the mediator shows the whole WMN towards the SDN controller as one switch and takes care of translating the SDN controller commands into WMN operations.

SON solutions already automate the deployment and optimization of radio and core networks. Excluding the mobile backhaul from this optimization creates a bottleneck, leading to sub-optimal use of network resources and can degrade the end-to-end service experience. SON for mobile backhaul technology extends these self-organizing principles to the mobile backhaul network. Combined with SDN controllers, SON provides means for creating self-planning, plug & play MBH networks and helps operators to achieve an optimal and efficient network configuration and avoid failures introduced by human interaction. It continuously measures and analyzes QoS/QoE, detects and localizes anomalies and performance degradation in the MBH and takes the necessary corrective actions using the SDN controller (e.g. re-routes transport services, changes their bandwidth allocation, etc.). It also performs pro-active MBH optimization (e.g. creating transport service on a new path, extending bandwidth allocation of existing services) based on user mobility information received from the MME and trend analysis of historical network state data.

To fully exploit the optimization potentials of network programmability in mobile networks, it is important to harmonize radio and mobile backhaul management and optimization as much as possible. The centralized view and control provided by SDN technology is a great enabler for the harmonization in which radio and backhaul domain specific key performance indicators and measurements are shared between the management processes and incorporated into their operation. The harmonization shall be mutual, i.e. radio optimization shall consider backhaul state and vice versa.

ADAPTIVE MOBILITY MANAGEMENT

Legacy challenges

The mobility management consists of two components: 1) for managing mobility of active UEs/devices, and 2) for tracking and reaching the devices, which support a power-saving idle mode. The current mobile networks provide the full active and idle mode mobility for all use cases.

There is a rising interest to ‘mobility on demand’ principles, which would allow efficient utilization of network resources. For different application needs and device capabilities, the network can determine the appropriate level of active and idle mode mobility to be assigned for a certain device. Quite different requirements are needed for the extremely mobile (e.g. fast moving vehicle) users that require seamless handover (e.g. voice) and the stationary IoT devices (e.g. sensors) that might require neither support for active mode mobility nor idle mode paging, but extremely low power consumption (for maximum battery life time). The potential solution needs independent assignment of idle mode mobility on a per-device basis and active mode mobility on a per-application basis.

The data plane GWs (P-GW, GGSN) in 3GPP legacy systems have traditionally been large in size and price. The legacy services, e.g. voice, short messages and Internet access, can be accessed through the centrally located mobile GWs. However, such an architecture with only a few points aggregating all traffic have faced problems in scaling up the vastly increased mobile data volumes. Also the emergence of content delivery mechanisms, service network optimization and mobile edge (cloud) computing is moving services towards the edge of the network. On the other hand, the requirement for low latency services requires server location and mobility tunnel termination close to the end users.

SDN-controlled mobility management

The LTE mobility management principles from the radio access side are assumed to remain. The SDN/NFV functionality enables the evolution towards the on-demand principles. The proposed solutions are related to the mobility tunnel management.

The traffic between an LTE mobile device and the edge of the Internet is carried in GTP-U tunnels. In order to satisfy different requirements for the gateway location, the solution shall be flexible and dynamical in terms of scale and the location. With the SDN controlled distributed GW-U implementation, the optimal mobility anchor/tunnel termination point can be maintained and the data plane element can be selected optimally for each UE (based on the service, etc., needs).

In order to apply OpenFlow control to the mobile user specific tunnels, SIGMONA developed two options for solutions. First option is that the data plane is handled with OpenFlow switches modified to support mobile specific tunneling using GTP-U. This may cause loosing economies of scale (with potential white box switches), but is reasonable for ensuring the compatibility with the existing network element that utilizes GTP-U. Also a lot of operator business logics might be related to the current GTP implementation.

The second option SIGMONA implemented maps GTP-U tunnel identifications at the base station site to either 802.1ad/ah tagging or to MPLS tagging both of which are directly supported by OpenFlow version 1.3. A tagger that maps GTP-U with a generic datacom tagging is useful in the short and mid-term for smooth deployment of SDN. In the long run, it makes sense to implement the corresponding function in eNBs directly. Using some datacom tagging has the advantage of economies of scale in OpenFlow switch manufacturing and in preserving the possibility of using cost efficient legacy datacom switches in the mobile backhaul and mobility management.

Mobility management establishes the attachment of mobile devices through the provisioned tunnels (eNB – edge of the Internet) to the Internet or other targeted services. During handovers, the mobility management app moves these tunnels as needed, based on the radio access network decisions. Due to handover, mobility management is a reactive SDN app that can provide the tunnel modifications to the backhaul SDN switch, which is otherwise controlled by the Internet access app. In this scenario the Internet access app takes the place of the P-GW.

Evolutionary deployment steps can be taken for the SDN controlled dynamic GW-U, and the current mobility tunneling (e.g. GTP) can be controlled dynamically and seamless from the other part of the network (towards the radio access). On the other hand, the scenario including the mobile network gateway functionality integration to the backhaul switches requires some more changes to the operator business machinery (statistics, charging, policies, etc.).

DYNAMIC QOS MANAGEMENT

End users value quality of experience (QoE) and one way to ensure good experience is to enable quality of service (QoS) guarantees. Thus, QoS is also one of the important features of SDMNs. In addition, different users may have different valuation for QoE and, thus, different willingness to pay for the premium services. SDN potentially enhances the current 3GPP bearer based QoS model, but SIGMONA's focus was on the core network.

In controller-based network architectures, switches are in communication with the controller regarding their QoS capabilities and this allows flexible and dynamic QoS enforcement. The controller updates the forwarding tables of switches dynamically according to given policies with the OpenFlow protocol. QoS flow tables can be updated with proposed QoS routing decisions and separated from best-effort flow tables. A meter table consists of meter entries, defining per-flow meters. Per-flow meters enable OpenFlow to implement various simple QoS operations, such as rate-limiting, and can be combined with per-port queues to implement complex QoS frameworks. Class format for QoS on flow table can be generated by a group of flow entries. For a set of certain service classes, QoS primitives are invoked in switches such as egress/ingress rate limitation, precedence level and rate promising in queue.

SIGMONA has used SDN to provide guaranteed QoS to premium users in a VoIP system, congested by both VoIP and non-VoIP background traffic, by limiting bandwidth, assigning flows to different queues and adapting routing decisions based on network conditions. In addition, audio traffic is efficiently prioritized over video in order to keep communication reliable for heavy-loaded networks. In a network, where regular and premium users simultaneously use the network, two scenarios are simulated (Karaman et al., 2015). The baseline scenario, where no SDN based QoS system is employed, shows similar QoE for all users. On the other hand, the second scenario with the SDN based QoS system reduces the loss rate by more than 5% and the latency and jitter by more than 50% for the premium users, especially when the network is more congested. The system can also be used to prioritize certain segments of the traffic, and the simulation results show that, for example, voice premium users with QoS may have 50% less latency compared with premium users without QoS guarantee.

Accordingly, it can be concluded that this enhancement can be further applied to other networks and applications especially to scenarios of public safety and disasters. The communication between necessary personnel can be prioritized and QoS can be guaranteed by masking non-essential traffic.

GREEN TRAFFIC MANAGEMENT

The growing popularity of mobile applications has led to an increase in traffic diversity and volume, resulting in the need for new ways to manage the generated network traffic. SDN can simplify traffic management and at the same time enable fast service delivery by exploiting global network view, status and flow patterns. Instead of the shortest path algorithms and topology discovery in a distributed and static manner, SDN offers dynamic, agile and resilient network management.

SIGMONA proposes an energy efficient routing algorithm to minimize the cost from power consumption, which is determined by the number of active OpenFlow switches (or virtual machines that act as vRouters) in a software-defined network environment. The routing algorithm also satisfies throughput requirements of all flows for the given link capacities in the network. The performance of the proposed algorithm is evaluated based on the energy consumption for different network topologies and various scenarios.

In Figure 6 (Ozbek et al., 2016), all ports have 100mbps of capacity. The required traffic is 100mbps per connection. Considering eight connections, the proposed energy efficient routing algorithm reduces the network from 20 nodes to seven nodes (either turning off switches or de-instantiating virtual machines, which act as vRouters in the network).

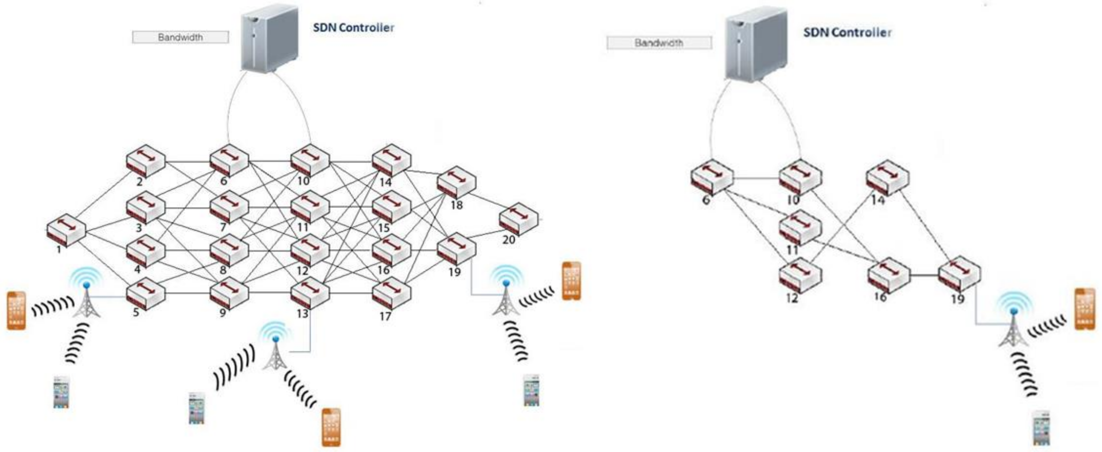

Figure 6. Initial and reduced network topology after routing decisions.

COMPREHENSIVE MONITORING

A general challenge in monitoring of telecommunication networks is obtaining the overall picture of the traffic to enable its management in a more efficient and automated way. This requires measuring traffic on multiple interfaces and correlating the obtained information.

Some of the challenges that need to be addressed are time stamping, analyzing virtual networks and network functions, and virtualizing the network monitoring. For the correlation to work, the captured packets must be time stamped and the time stamping synchronized with high accuracy. Legacy network monitoring applications that do not require any specific hardware can be easily adapted to SDN/NFV by running the application in a virtual machine and configuring the virtual operating system to provide the monitored traffic. Network virtualization has raised new challenges such as interfacing and evolved performance requirements for network monitoring. Moreover, monitoring of new kinds of protocols might be required (e.g., OpenFlow control traffic) to be able to detect problems related to errors in control logic.

The virtualized monitoring architecture proposed in SIGMONA for mobile networks integrates software-defined monitoring into the SDMN architecture as shown in Figure 7. This architecture uses an extension of OpenFlow type interfaces and the software-defined monitoring control interface to provide network applications with the necessary packet and flow data and meta-data from either the switch or the monitoring probes. The monitoring probes can function in passive or active mode, analyzing mirrored traffic or acting as a firewall that filters traffic. The figure shows how the monitoring modules map to the 3-layer SDN architecture for the operation and control of the hardware probes.

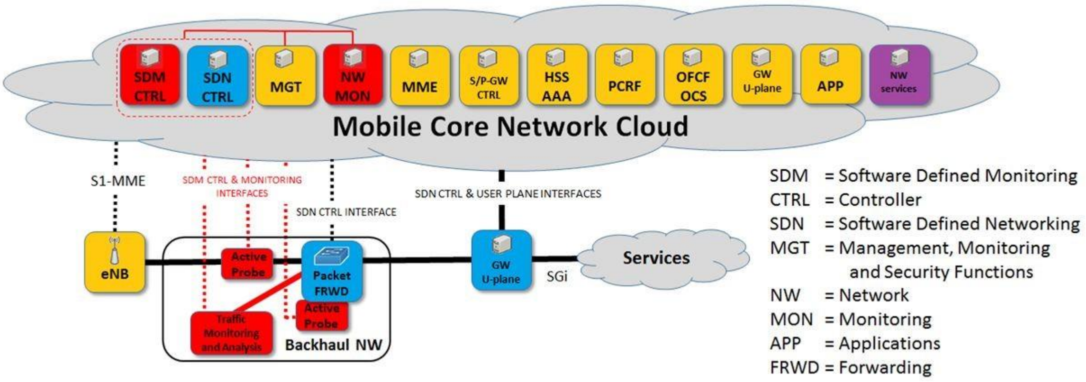

Figure 7. Monitoring architecture in SIGMONA.

Based on the validation results, it can concluded that the performance of NFV appliance is decreased compared to the legacy solution. Further study of performance bottlenecks and scalability in a virtualized environment is needed. Moreover, cloud solutions for implementing a SDN/NFV environment (such as OpenStack) have been found overly complex and further development is needed to make them easier to configure and administrate.

FLEXIBLE SERVICE CHAINING

Services, such as deep packet inspection, firewalls, network address translation (NAT), content caching, video transcoding, etc., add value to the operator services and are important parts of the operator business. These services can be hosted on physical hardware, on virtual machines or in the cloud. Almost all traffic in mobile networks visit a pre-defined sequence of services on the way to its destination today. Such a sequence is commonly referred to as a service chain as depicted in Figure 8. Though not all traffic benefits from the services, all traffic in the network traverses the whole service chain. This causes massive overprovisioning of service capacities. The service chain needs to be orchestrated for each flow for efficient service provisioning. Creation of high performance service-chaining applications contributes to the fulfilment of traffic demands and higher quality expectations from end users, while reducing capital and operational expenses associated with their networks. To achieve this, traffic should be processed only in the necessary middle boxes and should bypass the unnecessary middle boxes as depicted in Figure 8. Detailed identification of each flow, and establishing an appropriate dynamic service-chain for that flow is the main task.

With recent advances in SDN, operators and service providers are highly interested in deploying an SDN enabled service chaining solution that optimally utilizes compute and network resources to deploy personalized end-user services and to offer reduction in OPEX and CAPEX. Performing flexible, dynamic traffic steering for service chaining and optimizing the cloud realization of functions and services and determining the service chaining route for a given network flow jointly and dynamically are some of the main research areas in SDN enabled service chaining.

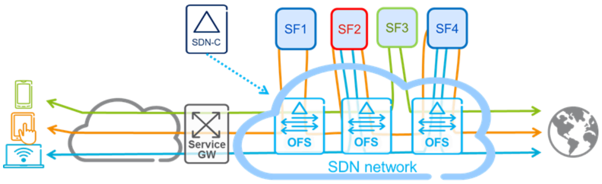

Figure 8. Service Chaining

The cost model in Figure 2 is used to evaluate the cost efficiency of SDN-enabled service function chaining. The cost modelling results show that SDN has the potential to significantly reduce the CAPEX and OPEX of service function chaining, i.e. 31% and 52%, respectively. Zhang et al. (2016) gives a more detailed analysis of the cost modelling process and results.

SECURE MOBILE NETWORKS

SDN introduces new kinds of security threats related to the split of the control and data planes and centralization of network control. At the same time, centralization and virtualization create new opportunities for improving network security and offering new kinds of security services to end users. NFV makes it easy to collect evidence of any kind of malicious activity in virtual functions, aggregate that evidence and apply a consistent network wide security policy. Scaling vertically integrated firewalls to the growth of the traffic would be a serious challenge. By using data center CPU capacity for processing flow level firewall rules, this challenge of scaling can be met. Since firewalling is done in the data center, it is even possible to apply firewall rules that are mobile device or user specific. SIGMONA promotes the idea that network security is one network function, which can benefit from centralization and virtualization. SDN can significantly contribute to network security due to global visibility of the SDN controller to the underlying network. This can enable the networks to dynamically react to security threats and mitigate policy conflicts across the network.

Security threats in SDMN

The separation of the planes, aggregating the control functionality to a centralized system and running the control functions in a cloud open up new security challenges in SDMNs. For instance, the communication channels between the isolated planes can be targeted to masquerade one plane for attacking the other. The control plane is more vulnerable to security attacks, especially to DoS and DDoS (Distributed DoS) attacks, because of its visible centralized nature and can become a single point of failure. Since the networking paradigm in SDMN is converging towards software-based networking, operational malfunctioning or malicious software can compromise the whole network by providing access to the control plane. Some of the known security challenges in SDMN are summarized in Table 1.

Table 1. Security threats in SDMN.

Threat vector	Threat types	Threat Reason and Description
Application plane	Lack of authentication and authorization. Fraudulent rules insertion. Access control and accountability.	Possible huge number of (third-party) apps. Malicious applications generated false flow rules. Lack of binding mechanisms for apps.
Control plane	DoS, DDoS attack, Controller hijacking or compromise. Unauthorized controller access. Scalability or availability.	Visible nature of Ctrl-plane. No compelling mechanisms for enforcing access ctrl on backhaul devices. Centralized intelligence.
Data plane	Fraudulent flow rules. Flooding attacks. Controller and DP switch masquerading.	Lack of intelligence. Limited capacity of flow tables. Lack of strong authentication.
Ctrl-Data interface	TCP-Level attacks. Man-in-the middle attack.	TLS is susceptible to TCP level attacks. Optional use of TLS and complexity in configuration of TLS
App-Ctrl interface	Illegal controller access, policy manipulation and fraudulent rule insertion.	Limited secure APIs, lack of binding mechanisms between Apps and controller.

Proposed security architecture

Most of the telecom-specific requirements are tightly coupled with control and data planes than the application plane. Thus, the proposed security architecture in SIGMONA is focused on securing three domains: 1) control plane, 2) data plane and 3) Ctrl-Data interface. The SIGMONA security architecture is presented in Figure 9.

The proposed security architecture is a multi-tier security approach with three components: 1) Secure communication component, 2) policy based communication component and 3) security management and monitoring component.

Secure communication component

The SDMN architecture has two communication channels, i.e. control and data channels. We propose a host identity protocol (HIP) based secure IPsec tunneling architecture to secure SDMN control communication channels. It establishes secure HIP tunnels between the data plane switches and the controller. The HIP/IPSEC based interface is free of the known vulnerabilities in TLS. The added benefit is better responsiveness in cases of one of the endpoints moving.

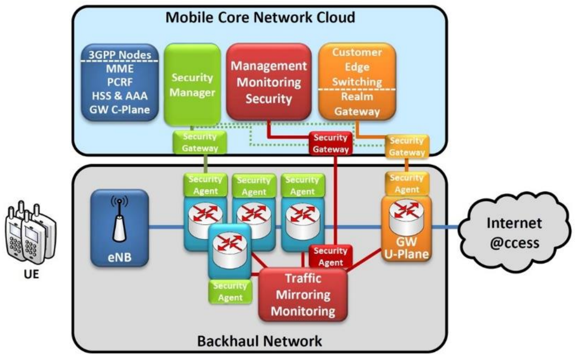

Figure 9. SIGMONA Security Architecture.

Policy based communication component

Customer edge switching is a disruptive approach to enable policy based communications to mobile nodes. We propose customer edge switching to introduce policy based communications in the SDMN framework. The customer edge switch is the heart of the Internet access application mentioned earlier. Customer edge switching is a cooperative firewall and an extension of NAT. It applies a user/device specific security policy to all flows to and from a mobile device and follows the SDN approach, where flow level rules are executed in the control plane, i.e. in a datacenter. The benefits of the approach include:

1. Protection of the air interface and the mobile devices from simple flooding attacks and scanning.
2. Unilateral initiation of flows to the mobile device, e.g., for communications services without application layer NAT traversal or polling.
3. Power saving in mobile devices, and reduction of unwanted traffic over the air interface.
4. Controlling of all flows by policies that are defined by end users, but managed and enforced by the operator.
5. Offers additional security services to end users, such as parental control.

Security management and monitoring component

The proposed security management and monitoring component focuses on deploying and integrating security information and event management systems into an SDN based network. The deployed sensors retrieve information regarding security monitoring tasks performed throughout the network, concerning, e.g., the availability of monitoring resources, network performance monitoring and traffic mirroring. Virtualized network switches controlled by a centralized software based controller are redirecting packets and enable packet forwarding to be analyzed by Intrusion Detection Systems tools in the sensor side. Moreover, the information collected from each sensor are consolidated and presented by a security monitoring graphical user interface in the management server side.

Mitigation actions and reactions to anomalous traffic or threats can be managed from the security management and monitoring component, which takes security events as inputs. The component then reconfigures the SDN controller accordingly by using representational state transfer API communication to inject a new flow that drops, isolates or redirects network traffic and providing automated mitigation actions.

The integration of the Internet access app and mobile network functions would require a stepwise development of the chain of business from mobile application stores to using the application on the network. If initially policies could be based on per application policy templates, in the long run, each app of each user would be handled by a distinct policy.

LOWER TOTAL COST OF OWNERSHIP

A flexible CAPEX and OPEX cost model software has been designed in the course of the SIGMONA project, which incorporates lifecycle costing to work out actual total cost of ownership (TCO) for SDN/NFV based mobile networks covering all phases of the life of such network ventures. That is, the cost model covers the cost starting from the idea and initial design up to the decommissioning of the equipment. It takes into account that acceleration applied in the virtualization infrastructure allows the performance of virtual network elements to match the bare-metal ones. This methodology can be applied onto the whole network like in the current model on onto individual network elements. It therefore covers traditional 3GPP like elements but also the newly introduced blade servers, software switches and NFV management and orchestration components.

The model investigates SDN/NFV enabled mobile networks based on some basic assumptions, such as which network elements are modelled purely real or purely virtualized as well as which are to be modelled both ways for certain deployment scenarios. As a result, comparison calculations between real vs. virtualized, rented vs. owned, in full as well as partial deployment scale have been performed. Based on the available input values, the virtualized solution turns out to provide cost reductions in CAPEX and in particular in OPEX.

Those assumptions include a two-stage mapping between virtual machine requirements of certain networking functions (S/P-GW, MME, HSS, router, switches, etc.) and the mapping of virtual machines onto available processing hardware resources. The model is fully parameterized and can be quickly adopted to new (more realistic) technical as well as financial input parameters as they become available. Figure 10 depicts the sub-model structure, which allows to model S/P-GW elements with split user and control plane in either virtual or real deployment option and the resulting virtual machine, blade server and rack usage.

Figure 10 also provide the deployment option for blade servers with or without the software product.

In the course of the modelling, it turned out that packet forwarding rates are often the bottleneck for NFV based networking components. Computing and storage are not as critical. The incurred software licenses are incorporated in the input.

Since packet forwarding is identified as a crucial performance indicator, the model sensitivity analysis also includes parameter variations for average packet length or forwarding capabilities in software switches (Open vSwitch). The result in terms of accumulated TCO is depicted in Figure 11.

More details about the described LCC cost model for SDN/NFV based mobile networks can be found in Knoll (2015).

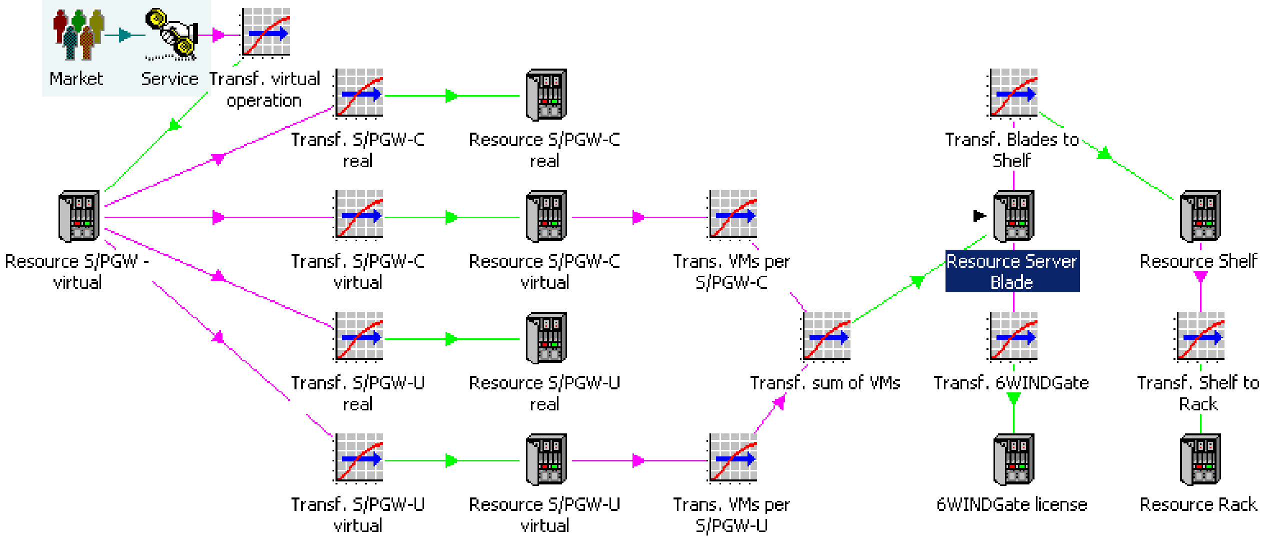

Figure 10. Mapping of S/P-GW functions to blade servers.

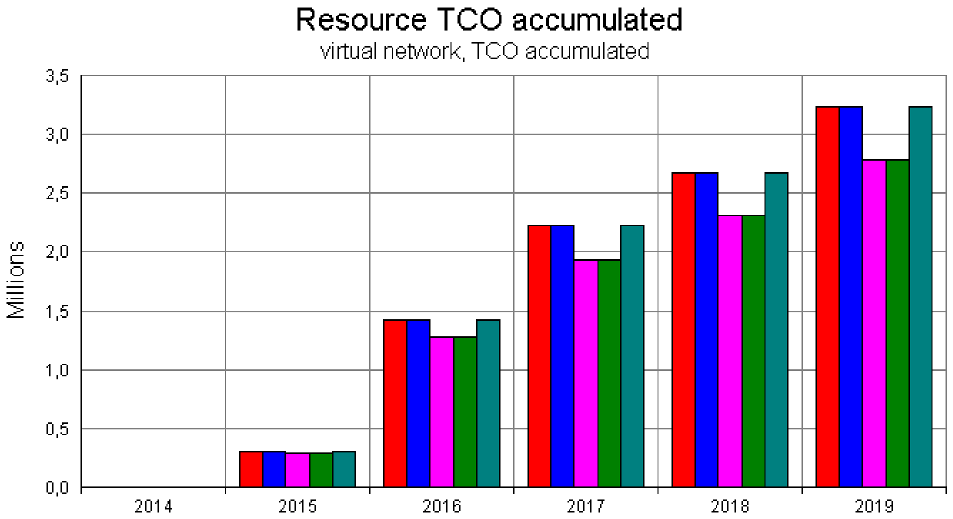

Figure 11. ±20% sensitivity on average packet length (red, pink) and on Open vSwitch packet throughput (green, cyan) vs. unmodified parameter set (blue).

CONCLUSIONS

SIGMONA project has integrated the concepts of software-defined networking (SDN) and network functions virtualization (NFV) into LTE mobile networks. This white paper presents the main outcomes that include a flexible end-to-end SDN/NFV architecture and its various elements, such as an efficient backhaul network, optimized mobility management, dynamic resource management and improved security.

The testbeds created in SIGMONA have shown that the SDN/NFV based mobile network compared with the current LTE provides a lighter weight mobility management, more optimized backhaul routing and more efficient caching due to the flexible controller placement. SDN/NFV also enables differentiated services to different end users even on a per-flow basis, which has inspired solutions for flexible quality-of-service management, efficient network monitoring, new security components and dynamic service chaining. In addition, the SDN/NFV architecture is found to promote competition, lower the entry barriers for new actors, lower operator's cost and induce new regulatory policies.

The SIGMONA SDN/NFV solutions serve as a baseline for future studies, especially ones leading to the standardization of SDN/NFV concepts in relation to 5G networks. The performance bottlenecks and scalability of the virtualized functions in higher load also remain as future study items. In addition, the possible disruptions caused by new entrants and higher competition need further understanding in order for the relevant actors to efficiently cope with the changes.

Acknowledgement

This work has been performed in the framework of the CELTIC-Plus project C2012/2-5 SIGMONA.

Project partners: Nokia Solutions and Networks Oy, AALTO University, EXFO Oy, Coriant Oy, University of Oulu, VTT Technical Research Centre of Finland, Atos, Commissariat à l'Energie Atomique et aux Energies Alternatives, Montimage, 6WIND, Technical University of Chemnitz, Nokia Solutions and Networks Management International GmbH, Budapest University of Technology and Economics / Mobile Innovations Center, Nokia Solutions and Networks Kft., Ericsson Telekomünikasyon A.S, NEXTEL S.A., ENEO Tecnología SL, Innovalia Association, ARDIC AR-GE BİLGİ VE TEKNOLOJİ ÇÖZÜMLERİ A.Ş., Avea İletişim Hizmetleri A.Ş., ARGELA Yazılım ve Bilişim Teknolojileri San. ve Tic. A.Ş.

LIST OF ACRONYMS

CAPEX	Capital expenditure
DDoS	Distributed denial of service
DoS	Denial of service
eNB	Evolved NodeB
EPC	Evolved packet core
GGSN	Gateway GPRS support node
GTP	GPRS tunneling protocol
HIP	Host identity protocol
HSS	Home subscriber server
LCC	Life cycle cost
MaaS	Mobility as a service
MBH	Mobile backhaul
MME	Mobility management entity
MNO	Mobile network operator
MPLS	Multiprotocol label switching
MVNO	Mobile virtual network operator
NAT	Network address translation
NFV	Network functions virtualization
OPEX	Operational expenditure
QoE	Quality of experience
QoS	Quality of service
SDMN	Software-defined mobile network
SDN	Software-defined networking
SON	Self organizing networks
S/P-GW	Serving/Packet data network gateway
TCO	Total cost of ownership
TLS	Transport layer security
WMN	Wireless mesh network

FURTHER READING

3GPP, 2015. Architecture Enhancement for Flexible Mobile Service Steering. TR23.718, updated September 22, 2015: http://www.3gpp.org/DynaReport/23718.htm.

Ahmad, I. et al. New Concepts for Traffic, Resource and Mobility Management in Software-Defined Mobile Networks. In Proceedings of 12th Wireless On-demand Network systems and Services Conference (WONS), Cortina d'Ampezzo, Italy. January 2016.

Costa, J., Kantola, R. et.al., 2014. Software Defined 5G Mobile Backhaul, 5GU, EAI, Levi, Nov, 2014.

Halpern, J. & Pignataro, C. (Eds.), 2015. Service Function Chaining (SFC) Architecture. RFC 7665 (Informational), October, 2015: https://www.rfc-editor.org/rfc/rfc7665.txt.

Kantola, R., Llorente Santos, J. & Beijar, N., 2015. Policy Based Communications for 5G Mobile with Customer Edge Switching, Wiley Security and Communication Networks, 05/2015.

Karaman, M.A. Gorkemli, B., Tatlicioglu, S., Komurcuoglu, M. & Karakaya, O., 2015. Quality of Service Control and Resource Prioritization with Software Defined Networking. In Proceedings of 1st IEEE Conference on Network Softwarization, 13-17 April 2015.

Knoll, T. M., 2015. Life-cycle-cost Modelling for NFV/SDN Based Mobile Networks, IEEE, November 2015, ISBN: 978-1-4799-8238-7.

Liyanage, M., Abro, A., Ylianttila, M. & Gurtov, A., 2016. Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective. IEEE Security and Privacy Magazine, 2016.

Liyanage, M., Ahmad, I., Ylianttila, M., Llorente Santos, J., Kantola, R., López Pérez, O., Uriarte Itzazelaia, M., Montes de Oca, E., Valtierra, A. & Jimenez, C., 2015. Security for Future Software Defined Mobile Networks. In: Procedings of 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST, 2015), Cambridge, UK. September 2015.

Liyanage, M., Gurtov, A. & Ylianttila, M. (eds.), 2015. Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture. John Wiley & Sons, 2015.

Ozbek, B., Aydogmus, Y., Ulas, Y., Gorkemli, B. & Ulusoy, K., 2016. Energy Aware Routing and Traffic Management for Software Defined Networks. In Proceedings of 2nd IEEE Conference on Network Softwarization, 6-10 June 2016.

SWD, 2013. 31. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_res_en.pdf

Zhang, N. & Hämmäinen, H., 2015. Cost Efficiency of SDN in LTE-based Mobile Networks: Case Finland. In: Procedings of the Workshop on Software-Defined Networking and Network Function Virtualization for Flexible Network Management (SDNFlex), March 12, 2015, Cottbus, Germany.

Zhang, N., Hämmäinen, H. & Flinck. H., 2016. Cost Efficiency of SDN-LTE: Use Case Network Service Function Chaining. Work-in-progress.

Zhang, N., Levä, T. & Hämmäinen, H., 2015. SDMN: Industry Architecture Evolution Paths. In: Liyanage, M., Gurtov, A. and Ylianttila, M. (eds.): Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture, Wiley Publishers, August 2015, ISBN: 978-1-118-90028-4.