Software Defined 5G Mobile Backhaul

Jose Costa-Requena, Raimo Kantola, Jesús Llorente, Vicent Ferrer, Jukka Manner
Aalto University
Helsinki, Finland

Aaron Yi Ding, Yanhe Liu, Sasu Tarkoma
University of Helsinki
Helsinki, Finland

***Abstract*—A major challenge of future mobile networks is providing the needed elastic scaling to the increased traffic demand, number of users and applications with acceptable cost. Another challenge is suitability for numerous communications applications while curbing unwanted traffic on the air interface and the mobile devices. This paper proposes a vision of how these challenges can be met by applying the concept of Software Defined Networking (SDN) to mobile networks. We also discuss the needed migration path that minimizes unnecessary replacement investments. While we have verified some key parts of the vision with experiments, we realize that the effectiveness of the proposed approach depends on the adoption of SDN technology for other purposes so that mass production of SDN switches leads to significant economies of scale. The paper shows how we can model mobile networks using SDN concepts and migrate the 3GPP mobile architecture to SDN. The resulting control plane of the mobile architecture consists of a group of SDN applications starting from the base stations i.e., virtual eNodeBs, Backhaul transport, Mobility management, Access, Caching, Monitoring, and Services delivery. The data plane consists of simplified access points and SDN and Carrier Grade Ethernet switches. Our experiments are based on using OpenFlow as the interface between the planes.**

Keywords— SDN, 5G, LTE, caching, mobility management.

I. INTRODUCTION

By the end of 2013, the number of mobile devices surpassed the total population of the world, and by 2017 there will be nearly 1.4 mobile devices per user [1]. Furthermore, it is anticipated that a significant portion of the generated traffic will be due to video-related services. NSN predicts [2] that from 2010 till 2020 the traffic in mobile networks will grow 1000 times. From the NSN prediction we take the assumption of 1 Gigabyte of dedicated networking capacity per day per user by 2020 for our modeling of 5G networks. To meet this demand mobile networks will have to improve spectral efficiency 10-fold. Another factor of 10 comes from additional spectrum being made available for mobile use. The last factor of 10 will need to come from increased number of small base stations. It is natural that operators will invest last to increasing the number of base-stations because this has the highest cost. At the same time, users are unlikely to want to pay more than they are paying today for the service. For the mobile operators and vendors this sets a serious challenge: how to improve the technology 1000 times without increasing the cost including both capital (CAPEX) and operational expenditure (OPEX). OPEX tends to grow significantly as a function of the number of network nodes or sites. To lower the growth curve for the increased number of (small) base stations, it makes sense to design the physical base-station as simple as possible; it will mainly consist of an antenna, possibly a band pass filter and an Ethernet card for the backhaul connection. The control software of a number of small base-stations will be run remotely at a location that is relatively close to the physical base stations for keeping the time delays for the communication low. At the same time we believe that it is wise to avoid replacement investments. Therefore, the architecture must provide interworking for unchanged legacy base-stations. In this paper we take LTE as the starting point for migration. We show how to structure the LTE control functions into a group of Software Defined Network (SDN) applications for 5G, so that the data plane of the mobile network can be built using standard OpenFlow (OF) and Ethernet switches. A technical challenge is that the 3GPP architecture heavily relies on mobile network specific tunneling methods to hide mobility from the core of the Internet and OpenFlow does not directly support such methods.

Mobile devices in 5G run many communications applications all of which need to be reachable by a remote user. It should be possible to provide better than the current Network Address Translator (NAT) experience without requiring cumbersome NAT-traversal to these applications while the devices may have only a private address. At the same time the 5G networks should do their best to curb unwanted traffic, in particular distributed denial of service (DDoS) and Internet fraud against mobile users. Due to the personal nature of the devices, the access to monetary transactions, the access to sensors and actuators from the mobile devices and the numerous apps running on the devices, they are very attractive targets for hackers and fraudsters. Therefore, it is not enough that the network itself is secure; instead, the network should do its best to curb the unwanted traffic and broker trust between its users.

The paper is organized as follows: Section II discusses related work. Section III gives a background on mobile networks. Section IV lays down our vision. Having modeled the control functionality of the mobile network as a group of SDN applications we show case studies in section V. Section V.A describes packet forwarding and V.B traffic offloading. We have built a prototype and an offloading platform that demonstrate most of the above elements but have naturally not verified all aspects of the solution. In particular, we have done little performance testing. Therefore, in Section VI we identify several open research items for concluding whether SDN meets

This work is sponsored by EIT ICT Labs and the CELTIC Plus SIGMONA project funded by Finnish Research Agency, TEKES.

the needs of mobile networks beyond 4G. Section VII discusses the major impact SDN would have on future networks. Finally, conclusions are presented in Section VIII.

II. Related Work

Some concepts for Software Defined Mobile Networks (SDMN) were already discussed in previous publications. One of the pioneering SDN proposals for wireless mobile networks was OpenRoads [6], an open architecture that can be deployed on campus-like environments to enable handovers between heterogeneous wireless networks. The SoftCell [3] and CellSDN [4] target at cellular core networks to improve the scalability and flexibility on both the data and the control plane by applying enhancement techniques including multi-dimensional aggregation of forwarding rules and caching packet classifiers and policy tags at local agents. The FluidNet [7] proposes a scalable and lightweight framework for cloud-based radio access networks, which improves both performance and resource usage by applying a set of algorithms to dynamically reconfigure the front-haul. For the radio access dimension, OpenRadio [8] introduces a novel design for a wireless data plane with modular and declarative programming interfaces that offers the flexibility to implement protocol optimization on off-the-shelf wireless chips. The SoftRAN [9] focuses on the radio access network and proposes a software-defined centralized control plane to abstract access resources as a virtual base station. The 3GPP also proposes the Self-Organizing Networks (SON) [10] to enable the network self-configuration and self-optimization. Our work on 5G SDN takes the vision forward and advocates the necessity of integrating SDN to the upcoming 5G networks.

Some components of our SDMN vision were already covered without the mobile network context. Shirali-Shahreza et al. published a conceptually very similar OF based approach for sampling that was motivated by security aspects and even demanded changes in the OF protocol [12].

III. Mobile Networks

The LTE network consists of elements such as eNodeB (eNB), Mobility Management Entity (MME), Serving/Packet Gateway (S/P-GW), Home Subscriber Server (HSS), Policy and Charging Rules Function (PCRF), etc. that perform the attachment, mobility management and transport of data from mobile devices across the mobile network hiding mobility from the rest of the Internet. The mobile network is protected against the threats from the Internet by a firewall. Currently, the firewall usually applies the same rules to all users. Roaming between mobile networks is organized so that packets sent to and from a roaming mobile device usually traverse the home mobile network that provides the IP address that the device uses to communicate over the Internet. For the device, the entry point to the Internet resides in the home network P/S-GW. Packets sent to and from the visited network are tunneled to the home network before they cross the boundary to the Internet. Issues of trust dictate this clearly less than optimal arrangement. Alternatively, a visiting mobile may be attached to the Internet directly from the visited network for example for efficient routing of interactive voice. In this case trust is handled on Application layer.

Transport of packets from the eNB to mobile core network takes place over so called mobile backhaul that makes use of all kinds of transmission and packet transport technologies such as Ethernet, Carrier Grade Ethernet, IP/MPLS and MPLS-TP. The physical layer in the backhaul networks uses Fiber, Radio, and copper based links. The physical links are either owned by the mobile operator or leased from another operator. An incumbent mobile operator may share its infrastructure with different types of mobile virtual operators.

A fundamental problem in the IP protocol from the mobility point of view is that the IP address identifies the node in the topology and fixes its location to a certain IP subnet. The mobility solution in 3GPP mobile networks consists of using the GPRS Tunneling Protocol (GTP) to create a "virtual wire" from the mobile user equipment (UE) to the edge of the Internet. The S/P-GW provides the IP address of the UE. All traffic in the GTP tunnel receives a common QoS treatment between an UE and a P-GW. A Traffic Flow Template (TFT) is used for mapping traffic to a bearer. Whenever the UE moves to a new eNB, the GTP tunnel has to be recreated between the new eNB and the S/P-GW while the inner data flow keeps the original UE IP address. SDN applied in mobile networks will deliver the Software Defined Mobile Network (SDMN). Already some work has considered the integration of SDN with LTE by adding an SDN controller to eNB and managing the traffic from a centralized controller [3][4]. All the current research is proposing to keep the current LTE network elements such as eNB, MME and S/P-GW and integrate the SDN functionality by additional split of the data and the control planes in the LTE network elements and embed the SDN controller into some of the current LTE network elements such as S/P-GW.

IV. Vision

Starting from late 1990's the 3GPP has been taking steps towards a clear separation of data and control planes and the respective elements in the architecture. We propose to take this concept to its logical conclusion in mobile networks following the SDN paradigm. Fig. 1 presents the network control for 5G as a group of SDN applications. These include: Base Station, Mobile Backhaul, Monitoring, Mobility Management, Access, Caching and Secure Service Delivery among others. We

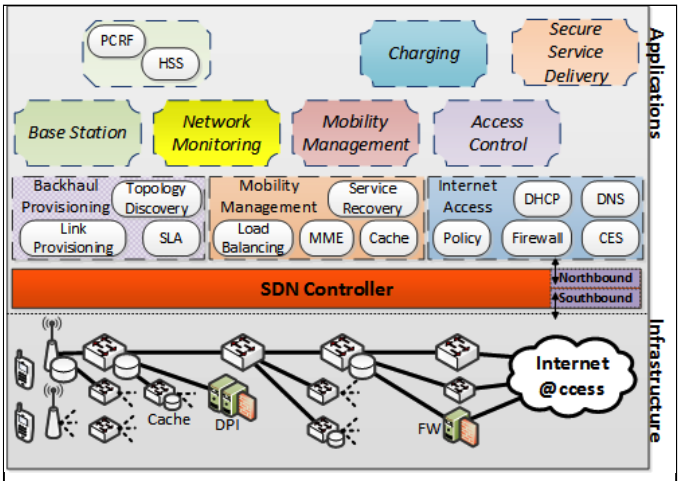

Fig. 1. 5G as a group of SDN Apps

envision these network applications to be orchestrated via the Controller Northbound API so that multiple SDN applications can operate without conflicts.

A. Mobile Backhaul Scaling

The task of mobile backhaul SDN application is to manage and optimize the provision of backhaul connections from the base stations to the Access App.

Let us model the scaling of a 5G mobile backhaul network for 100 million customers with the assumption of 1 GiB of

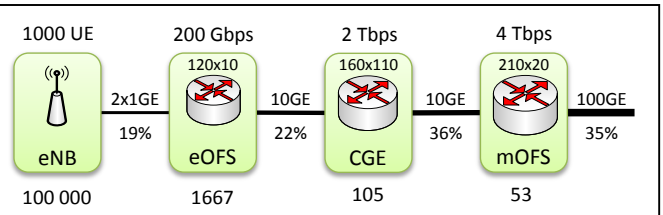

Fig. 2. Scaling of a Mobile network for 100M customers

dedicated traffic capacity per user per day. Let us further assume that each eNB serves 100 to 1000 customers and that the backplanes of the backhaul data-plane nodes are below 4 Tbit/s. Fig. 2 illustrates the modeling.

To let the SDN applications manage the network, we place an OF switch (denoted as eOFS) as the first aggregation element to which eNBs are connected. The eNB will terminate the protocol stack over the air interface and send all traffic from a user to an Ethernet VLAN. The eOFS will tag the packets from the user towards the Internet. One suitable encapsulation is 802.1ah. The second OF switch (denoted as mOFS) is required at the entry point to the mobile access to Internet. On the outbound interface of mOFS Mobility as a Service (MaaS) is presented to the access operator. An mOFS is connected to many Internet access OF switches (denoted as iOFS) of the mobile access operator towards the Internet. The mOFS will tag the packets from the Mobile access to the right eNB and the right mobile device. For traffic aggregation from many eOFSs to a few mOFS we will use a combination of Carrier Grade (CG) Ethernet Switches and OF switches. We can isolate each mobile into its own subnet using 802.1ah. The traffic from eNBs to the point of entry to the Internet and back can be switched through the described network. For the purpose of load balancing each link to the Internet must be reachable from each eNB over several paths (for example 4). It is beneficial that MaaS keeps the point of attachment to the Internet of a mobile stable while it is roaming in the area of the mobile network.

Given the assumptions, it is easy to calculate that the required tag length is in the order of 24. If the eNBs are small on average and 3 stages of Switches are needed, an integrated eOFS in the eNB would lead to longer tags (around 29 bits). Normally, in case of a separate eOFS, the tag can for example be the I-SID in 802.1ah. An alternative is using MPLS-TP. One of the tasks of the Mobile backhaul App is to set up and manage the service routing in the CGE switches between eOFS and mOFS and take care of fault recovery in this network.

In case of 802.1ah encapsulation, the I-SID value marks the path between an eOFS and iOFS. The B-VLAN tag can be used the separate traffic of different virtual operators if necessary and finally the C-VLAN tag identifies a user in one eNB. In case of MPLS encapsulation, a label stack would serve a similar purpose to VLAN tagging.

B. Mobility Management App

When a mobile device moves from the area of one eNB to an area of another, the rule in mOFS for the device needs to be modified and a new rule may need to be created in the new eOFS. If the new eNB is under the same eOFS as the previous one, then it is enough to modify an existing rule in the eOFS. We also need to take care of balancing the load across the alternative paths between an eNB and a particular mOFS. The Mobility Management App chooses the path for a device. For the load balancing decision it needs input from network Monitoring App.

In our example, one mOFS would be handling e.g. 2.5 million customers and it would possibly have to keep several rules for an active mobile device. A suitable backplane for such an mOFS would run at 4 Tbit/s. It is possible to lower this speed and reduce the cost of the nodes for example by making a compromise on the stability of the point of attachment of the mobile device to the Internet. Another way to lower the speed of the mOFSs is by reducing the share of traffic that is sourced or sent to the Internet by caching. The Mobility Management (MM) App incorporates the MME. In addition, it needs to manage the Quality of service for each user, balance the load among the alternative paths across the aggregation network and to route the user to a cache, when possible. Contrary to the current situation, in this design no lower layer IP is used to carry the user traffic to and from the Internet. Instead of a routed tunnel to the Internet, we propose to use a switched tunnel.

For mobility management, eNBs need to be directly connected with some tens of their neighbors. For this reason, a suitable way to connect the eNBs up in the network hierarchy is 802.1ad. In the 802.1ad frame, one VLAN tag identifies a user while the other identifies the “Internet VLAN” that leads to eOFS where the traffic is switched to 802.1ah, or the alternative VLANs that are switched either in eOFS or higher up to a neighboring eNB. Since the eNB to eNB interface is used for mobility management, we propose that the MM App will provision these switched paths. Finally, it is convenient that, although packet forwarding is based on switching, each eNB has IP routing functionality for eNB to eNB communications. For this purpose the MM App will assign IP addresses to eNBs. Alternatively, Ethernet routing could be used.

C. Access App

The role of the Access App is to assign the IP address for a mobile device. This address can be private. Thus the Access App provides the point of attachment to the Internet and to the Service delivery networks to each mobile device by controlling the iOFS. The point of attachment should be as stable as possible while the mobile moves or even roams to foreign networks. The Access App will handle downstream load

balancing and firewalling. We believe that all flow admission should be managed by a policy that is part of the subscription information of the user. Policies can also be dynamic, i.e. treat different remote hosts differently based on reputation produced by a trust management system. Moreover, we propose to use a cooperative firewall that allows queries to, e.g., the sender's firewall and certification authorities before making the final admission decision. This allows dissolving the boundary between closed and open networks, all managed by the policy [14]. A mobile device under the cooperative firewall is reachable using the host fully qualified domain name (FQDN), a suitable identity and the routing locator of the iOFS. Traffic through the service delivery network is tunneled. The service delivery tunnel and the mobile backhaul tunnel are tied together at iOFS by a binding state managed by the Firewall. The Realm Gateway, a component of the Access App can admit traffic directly from the legacy Internet [15].

Moving from simple network firewalls, that apply the same rules to every customer, to cooperative firewalls with user specific admission rules managed by the extended 3GPP policy management architecture in 5G is justified by the need to block all packets with source address spoofing, and all DDoS packets from reaching the mobile network, consuming any air interface capacity and disturbing the power saving sleep mode of the mobile device. It is also justified by the need to manage the reachability of the device per application and per user without cumbersome NAT traversal. In our solution, it suffices for all mobile devices to have just a private address. Therefore, scaling to any number of users and devices in 5G does not depend on the success of IPv6.

D. *Secure Service Delivery App*

The final SDN App on the path to the communication partner is the Secure Service Delivery App. By the service delivery network we mean the network that connects two mobile networks or a mobile network with a fixed customer network or with a remote datacenter that has the desired applications or the desired content. We suggest that by applying SDN concepts to service delivery we can seek benefits such as securing the process of service delivery and maximally benefiting from the economies of scale of cheap switches and generic hardware for control processing. The minimum goals of the service delivery network are to eliminate all source address spoofing and DDoS and admit only legitimate traffic (e.g. only I can turn on my own Sauna connected to Internet of Things). Our work on Customer Edge Switching indicates that significant progress towards these goals can indeed be achieved.

E. *Performance and scaling drive the design*

The driving factors for the proposed design are: (a) the Base Station App is rather delay sensitive due to both radio and application aspects. Therefore we believe that the control software of a physical base station must reside rather close to it although it can be separated to a distinct node; (b) the goal of mobility management is to provide seamless handovers. Some data applications can tolerate connection loss during a handover for several hundreds of milliseconds. Interactive voice can tolerate a loss of connection for several tens of milliseconds. Some new applications (e.g. gaming) can benefit from delay reductions to the area of 10ms. Therefore, the control functions for mobility management can reside no more than a few hundred kilometers from the base-station (the propagation delay over a round-trip of 200 km in fiber is 1ms); (c) the delay requirements for the Access App are mostly determined by the perceived service responsiveness of the network. By this we mean factors such as voice session setup time or network contribution to system response time. For the Access App another important driving requirement, in addition to delay, is scalability. The NSN white paper [2] predicts that by 2020 a mobile user will consume 1 GiB of data per day. From this we can calculate that scaling the access network to tens and hundreds of millions of mobile users is a significant challenge with the technology that we expect to be available by 2020: e.g. 100 million customers would use 600 to 800 100GE interfaces towards the Internet.

To ease the challenge, traffic offloading and caching has to be used maximally in mobile access as scaling mechanisms. Also, we propose that most popular content of content providers and from content distribution networks should be collocated in the same sites (i.e., data centers) as the Access App. Therefore, another way to look at the access network controlled by the Access App is that it, in fact, is a set of telco datacenters and the network that connects them. In practice a very significant part of the tens of GiB of traffic consumed by the mobile users will be served from these datacenters.

V. EXPERIMENTS

We performed a set of experiments to demonstrate the feasibility and to work out benefits of our vision. We run an SDN controlled LTE network testbed, with our own Mobility Management and Access Apps, in Otaniemi, Finland where we carry on the research in cooperation with Nokia.

A. *Packet forwarding*

We experimented with OpenFlow to find out how we can best use OF switches to carry the mobile traffic that now uses

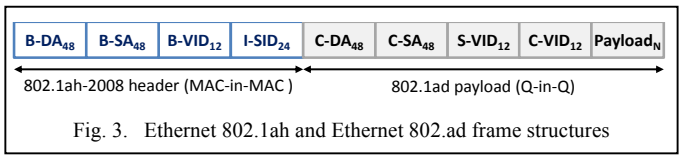

Fig. 3. Ethernet 802.1ah and Ethernet 802.ad frame structures

the GTP tunnel from the eNB to the P-GW. We propose to replace the GTP data plane with Ethernet VLAN tagging or a combination of VLAN tags and MPLS tags. In the initial step of migration, the GTP control protocol stays as is and will be processed by the different SDN Apps in Figure 1. An entry in the OF switch flow table has three fields: a packet header to define the flow, an action that defines packet processing, and finally statistics. We propose to use 802.1ah/ad to allow rich tagging in Ethernet switches as shown in Fig. 3.

Fig. 3 shows also the 802.1ad double tagging in Ethernet switches as we use it in the testbed. For our experiments we created a mapper that takes GTP and maps its Tunnel Identifier to a set of VLAN tags. Such a mapper is useful even in the long term for the purpose of SDMN interworking with legacy

eNBs. For firewalling we use the cooperative firewall [13] [14] we call Customer Edge Switch (CES). It allows placing all mobile devices in their own private address space while they are reachable by their domain names without cumbersome NAT traversal. Access to the services such as VOIP or WWW provided by a mobile device is controlled by a policy that is executed by the Access App. For ease of interworking with legacy IP networks the customer edge switch provides a Realm Gateway that makes servers in a private address space reachable to unchanged IP hosts without polling.

B. Testbed Results

The testbed results in Table 1 shows the overhead due to fragmentation in switches after adding the GTP (8 Bytes) over UDP (8 Bytes) on top of the end user IP packets in the eNB. This overhead disappears after removing GTP-u and using off-the-shelf SDN switches in the mobile backhaul where IP packets do not have to fragment. The mobile transport recommends to use jumbo frames to avoid this fragmentation. However, this functionality would have to be negotiated with the mobile device that in most of the cases does not support this capability. Thus, first visible improvement after removing GTP-u is the reduction of overhead of up to 50%.

TABLE I. PACKET OVERHEAD DUE TO FRAGMENTATION

Message Type	***Packet size(B)***	***Packet Payload (B)***	***GTP+ UDP header (B)***	***Overhead (%)***
TCP ACK	76	40	36	52,6
User Data (before eNB)	1536	1500	36	2,34
Fragment 1 User Data (after eNB)	1500	1464	36	2,4
Fragment 2 User Data (after eNB)	72	36	36	50

C. Traffic offloading

Offloading reduces the costs of the radio network to the mobile operator and adds capacity for the end user benefit. The SDN based offloading method enables a smooth evolution by innovating on the access and backhaul infrastructure while protecting the existing investment and resources. Unfortunately most of the existing offloading solutions are ad hoc based research designs built from scratch for the incumbent legacy hardware, hence they can hardly lead to successful adoption in the upcoming 5G mobile networks. We believe that the way forward is to integrate the SDN design and fully utilize the features of SDN in terms of programmability, abstraction and openness to promote the applicability and interoperability in the dynamic 5G networks. Based on our experience in mobile traffic offloading [14] [15], we propose a collaborative SDN-enabled offloading design as a part of the 5G solutions.

We have built an offloading platform [18] using Floodlight and conducted experiments in our laboratory environment. Compared to the existing methods, our system enables us to tackle three crucial challenges in mobile traffic offloading. 1) Offloading decision-making: how to convey management policy, service requirement, and user preference to the decision process, which is missing from the solutions for the existing infrastructure. For instance, by taking into account the energy consumption of mobile devices and the delay tolerant feature of certain data flows, the SDN based method can offload the traffic of selected services to the WiFi network while keeping the critical flows still on the mobile network with enhanced granularity. 2) Interaction across access domains and wireless technologies: how to enable collaborative control between both cellular and WiFi access, which involves mobility management and offloading prediction. 3) Context from mobile users: how to utilize the rich context provided by mobile devices, including the localized sensing context, WiFi and cellular information, to identify the mobility pattern and facilitate the offloading procedure.

As illustrated in Fig. 4, the SDN-enabled mobile traffic offloading adopts a hierarchical design to reduce the signaling and latency overhead between a centralized controller and a local controller. The essential offloading functions such as monitoring and mobility management are implemented as network-level SDN applications on top of the centralized controller. Local agents on OF switches, wireless access points and cellular base stations are responsible for collecting flow statistics and performing localized flow processing.

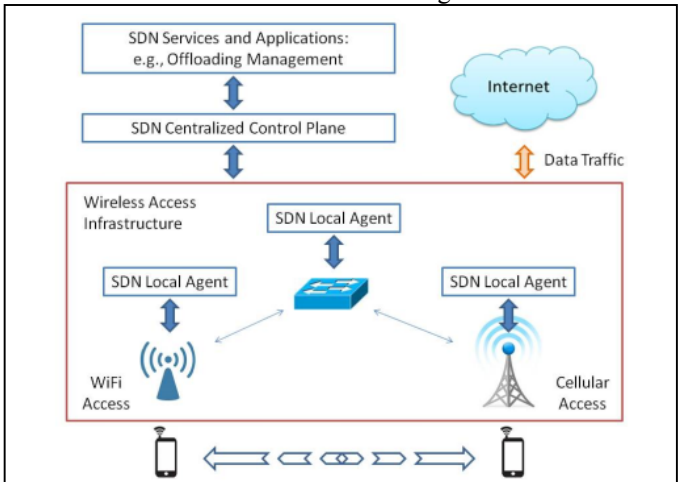

Fig. 4. SDN managed WiFi offloading in mobile networks

As the SDN paradigm is gradually accepted by the network industry, the SDN-based offloading not only encourages the mobile carrier WiFi deployment and also promotes the partnership between mobile and WiFi operators in both enterprise and public domain.

VI. RESEARCH PROBLEMS

Our vision requires verification in terms of scalability to short flows and to traffic volumes and performance as perceived by the user. An example of the latter is achieving seamless mobility with SDN control. The possible impact of the proposed switched path based mobility management on the air interface needs to be studied. The vision requires further work in the areas of policy management and design and others. While the lower levels of the SDN architectures have gained most attention the SDN applications are still a field of research [11]. SDMN requires scalable controller architecture with a good northbound API to serve as a transparency layer between

the data plane and the network applications. One weakness of existing Northbound APIs is a lack of information about the state of the network devices at the controller side. We see the need for collection of requirements for the Northbound API, and we suggest adequate information transparency as one of it. A research question is how to best use heterogeneous computing to tackle some of the real-time requirements where data needs to be filtered for monitoring purposes or where application specific processing needs to be applied to every data packet of a user application flow. Finally, for the implementation of the concept of secure service delivery, an East-West interface in SDN would be beneficial. This allows control communications cloud to cloud from socket to socket rather than going through the Switches each time.

VII. IMPACT

Provided the remaining problems can be solved, the separation of control and data planes has the potential to provide cost savings from capacity sharing and provide economies of scale from the virtualization of network elements in the cloud [11]. The usage of SDN will bring down the costs of acquiring and maintaining standard switches. The separation of control from data plane will lead to the usage of general-purpose switches without mobile dedicated solutions.

SDN brings new business models and opportunities with new business roles. One of the major business impacts of SDN in mobile networks is that current network equipment vendors will change their role from "equipment vendor" to a software vendor. The vendor markets will be organized into horizontal layers. SDNM will also bring new possibilities: The logical evolution is that the mobile network operator (MNO) will drive the SDMN adoption as optimization of their current infrastructure. The adoption of SDN will lead the MNO to deploy or lease their own cloud to run their control plane functions, independently of network device vendors. The MNO will benefit from the potential cost reduction when using general purpose and standardized hardware in both the user plane elements when using OpenFlow and Ethernet switches and in the control plane cloud platform.

Mobile operators need to closely cooperate with new entrants such as cloud providers (e.g., Amazon, Google) to share premises etc. in order to provide a better customer experience for delay sensitive applications.

For operating the networks three principal business roles with distinct competences can be identified: (a) mobility management including frequency licenses and use, towers, base station sites and understanding mobility patterns; (b) providing connectivity between sites and (c) dealing with the end customers, providing them the services and the user experience they want. These roles map rather nicely into the breakdown of network functions to SDN applications in Figure 1. Once SDN is deployed, it becomes feasible to reshuffle the roles of present day incumbent, mobile, mobile virtual operators and content providers in such a way that efficient competition is ensured on the market.

VIII. CONCLUSIONS

We propose to use SDN in 5G mobile networks as the solution for needed scaling to the increased traffic demand and to the number of users and applications with acceptable cost and the necessary level of control. In this paper we conclude that for modeling the 5G as a Software Defined Network, a group of SDN applications (e.g., Base Station, Backhaul, Mobility, Access and Service Delivery App) is required. We also describe WiFi offloading and firewalling that provide evidence of feasibility of SDN in LTE networks.

REFERENCES

[1] Cisco White Paper. Cisco Visual Networking Index: Forecast and Methodology, 2009-2014, June 2010.

[2] NSN White Paper, “Technology Vision 2020, Technology Vision for the Gigabit Experience, June 2013.

[3] Xin Jin, Li Erran Li, Laurent Vanbever, Jennifer Rexford ,” SoftCell: Taking Control of Cellular Core Networks“ (http://arxiv.org/abs/1305.3568)

[4] L. E. Li, Z. M. Mao, J. Rexford, Toward Software-Defined Cellular Networks, In Proceeding of EWSDN 2012..

[5] Arsany Basta, Wolfgang Kellerer, Marco Hoffmann, Klaus Hoffmann, Ernst-Dieter Schmidt, A Virtual SDN-enabled LTE EPC Architecture: a case study for S-/P-Gateways functions, Proceedings of SDN4FNS 201

[6] K. Yap, et al. Blueprint for Introducing Innovation into Wireless Mobile Networks. In Proceedings of ACM VISA 2010.

[7] K. Sundaresan, M. Y. Arslan, S. Singh, S. Rangarajan, S. V. Krishnamurthy, FluidNet: A Flexible Cloud-based Radio Access Network for Small Cells. In Proceedings of ACM MobiCom 2013.

[8] M. Bansal, J. Mehlman, S. Katti, P. Levis, OpenRadio: A Programmable Wireless Dataplane, In Proceedings of ACM HotSDN 2012.

[9] A. Gudipati, D. Perry, L. E. Li, S. Katti. SoftRAN: Software Defined Radio Access Network. In Proceedings of ACM HotSDN 2013.

[10] 3GPP. Self-Organizing Networks (SON) Policy Network ResourceModel (NRM) Integration Reference Point (IRP).

[11] Gartner Report "Hype Cycle Networking and Communications", 2013

[12] Y. G. Sajad Shirali-Shahreza,, Efficient Implementation of Security Applications in OpenFlow Controller with FleXam“, In Proceedings of IEEE 21st Annual Symposium High-Performance Interconnects, 2013.

[13] Raimo Kantola, Customer Edge Switching (www.re2ee.org).

[14] H. Kabir, R. Kantola, J. Llorente, Security Mechanisms for a Cooperative Firewall, CSS, 2014, Paris.

[15] J. Llorente, R. Kantola, N. Beijar, P. Leppäaho, Implementing NAT Traversal with Private Realm Gateway, ICC 2013.

[16] A. Y. Ding, B. Han, Y. Xiao, P. Hui, A. Srinivasan, M. Kojo, and S. Tarkoma: Enabling Energy-Aware Collaborative Mobile Data Offloading for Smartphones. In Proceedings of IEEE SECON 2013.

[17] J. Korhonen, T. Savolainen, A. Y. Ding, M. Kojo: Toward Network Controlled IP Traffic Offloading. IEEE Communications Magazine, Volume 51, Issue 3, p.96 – 102, 2013

[18] A. Y. Ding, J. Crowcroft, S. Tarkoma: Poster: SoftOffload: a programmable approach toward collaborative mobile traffic offloading. In Proceedings of MobiSys 2014.