Part II

SDMN Architectures and Network Implementation

6

LTE Architecture Integration with SDN

Jose Costa-Requena, Raimo Kantola, Jesús Llorente Santos,
Vicent Ferrer Guasch, Maël Kimmerlin, Antti Mikola, and Jukka Manner
Department of Communications and Networking, Aalto University, Espoo, Finland

6.1 Overview

This chapter proposes solutions to integrate software defined networking (SDN) technology with wide area mobile networks. The integration of SDN into mobile networks to become the software defined mobile network (SDMN) poses several architecture alternatives. To limit the discussion of the alternatives to a reasonable scope, in this chapter, we will discuss the issues and alternatives taking that the SDN uses the OpenFlow protocol.

We first need to define the proper location of the SDMN controller. It can be integrated with the Mobility Management Entity (MME) making the controller aware of mobility events, or it can be located in the Serving/Packet Gateway (S/P-GW) to control the transport network. The integration of SDN control with LTE network elements should follow a incremental process the idea being smooth deployment of SDN into a live mobile network. At best, the integration of SDN with LTE paves the way for 5G networks. For now, the objective is to keep using the current IP-based networks and add SDMN-based flexibility to the LTE network architecture.

Scalability, security, and resilience are key factors to be taken care of in order for SDMN to become the next infrastructure for 5G mobile networks. Finally, SDMN should bring some benefits both to mobile operators and end user. Section 6.2.1 presents the current LTE architecture. Section 6.2.2 discusses multiple options for the placement of the SDN controller. Section 6.2.3 introduces the vision for integrating SDN in the mobile network where mobile-specific functionalities are implemented as SDN applications. Section 6.3 studies the issues of ensuring scalability. Section 6.4 introduces the proposed security mechanisms, and Section 6.5 describes the benefits from the operator and the end-user points of view based on a simple

Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture, First Edition.
Edited by Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila.

scenario with built-in smart network services such as dynamic caching. Finally, Section 6.6 presents the research problems and conclusions.

6.2 Restructuring Mobile Networks to SDN

This section will describe the starting point of the restructuring, namely, the LTE network, then discuss the design alternatives, and finally propose a way of applying SDN concepts to LTE networks and beyond.

6.2.1 LTE Network: A Starting Point

Mobile networks consist of physical and logical entities. The physical layer is made of network routers (L3), switches (L2), and physical links (L1) with different technologies and topologies as shown in Figure 6.1. The logical layer consists of network elements (e.g., eNodeB, MME, S/P-GW, HSS, etc.) that perform the attachment of user devices, mobility, and transport of data from mobile devices across the mobile network in such a way that mobility is hidden from the core Internet. The physical layer (L2 and L3) provides the connectivity and transport functionality to the logical layers that implement the mobile-specific control functions. The access network consists mainly of the eNodeBs that provide the radio access to the user equipment (UE). The backhaul consists of all the network switches for aggregating the traffic from the access network and provides the connectivity toward the core network. Finally, all the connection services, mobility services, and billing functionality are implemented by the network elements (i.e., MME, S/P-GW, PCRF, HSS) located in the core network.

Mobility management in LTE mobile networks is the critical functionality, and any new technology that handles mobility events has to deliver a reliable and low-latency handover. Mobility in LTE networks is implemented through different methods depending on whether it is within same radio technology, that is, intra-E-UTRAN, or to different radio access technologies (RAT). In this work, we focus in the intra-E-UTRAN where the handover can be performed following two procedures. One procedure consists of X2-based handovers where there is a connection between the source and the target eNBs through which the handover

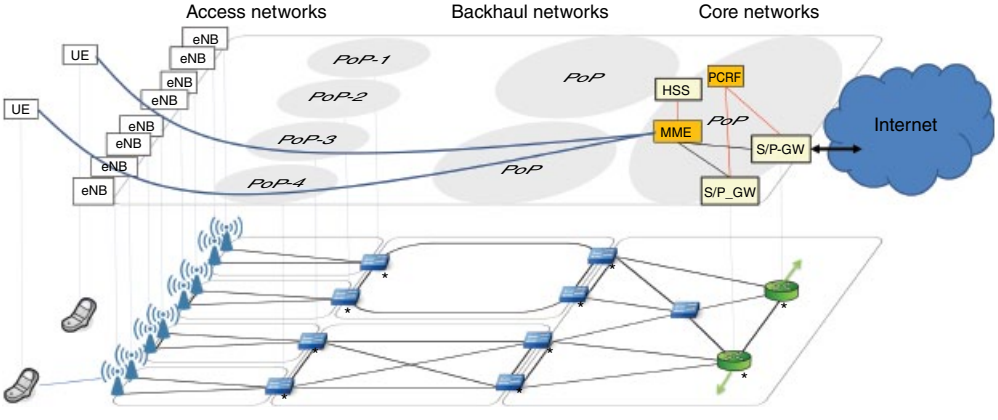

Figure 6.1 Physical and logical layers in mobile network. *refers to the router with connectivity to public Internet

operation is negotiated and then reported to the associated MME. The second procedure is S1-based handover; there is no direct connection between the source and the target eNBs, and therefore the handover operation is negotiated via their respective MMEs. In our analysis, we consider in more detail the scenario where the new target eNB is in the same tracking area ID (TAI) associated to the same Mobility Management Entity (MME). Other scenario consists of the case where the new TAI belongs to the same MME. In the former scenario, mobility management uses the S1 MME interface between the eNB and the MME.

A fundamental problem in the IP from the mobility point of view is that the IP address identifying the node fixes its location to a certain anchoring point. This occurs because the IP address also has the role of the routing locator. The common solution in mobile networks consists of using tunneling. UE IP packets are tunneled over the GPRS Tunneling Protocol (GTP). The GTP tunnels are established between the eNB and the S/P-GW. A GTP tunnel uniquely identifies traffic flows that receive a common QoS treatment between a UE and a P-GW. A traffic flow template (TFT) is used for mapping traffic to an underlying bearer. The GTP tunnel endpoint identifier (TEID) unambiguously identifies the tunnel endpoint of a user data packet, separates (identifies) the users, and also separates the bearers of a certain user as depicted in Figure 6.2a.

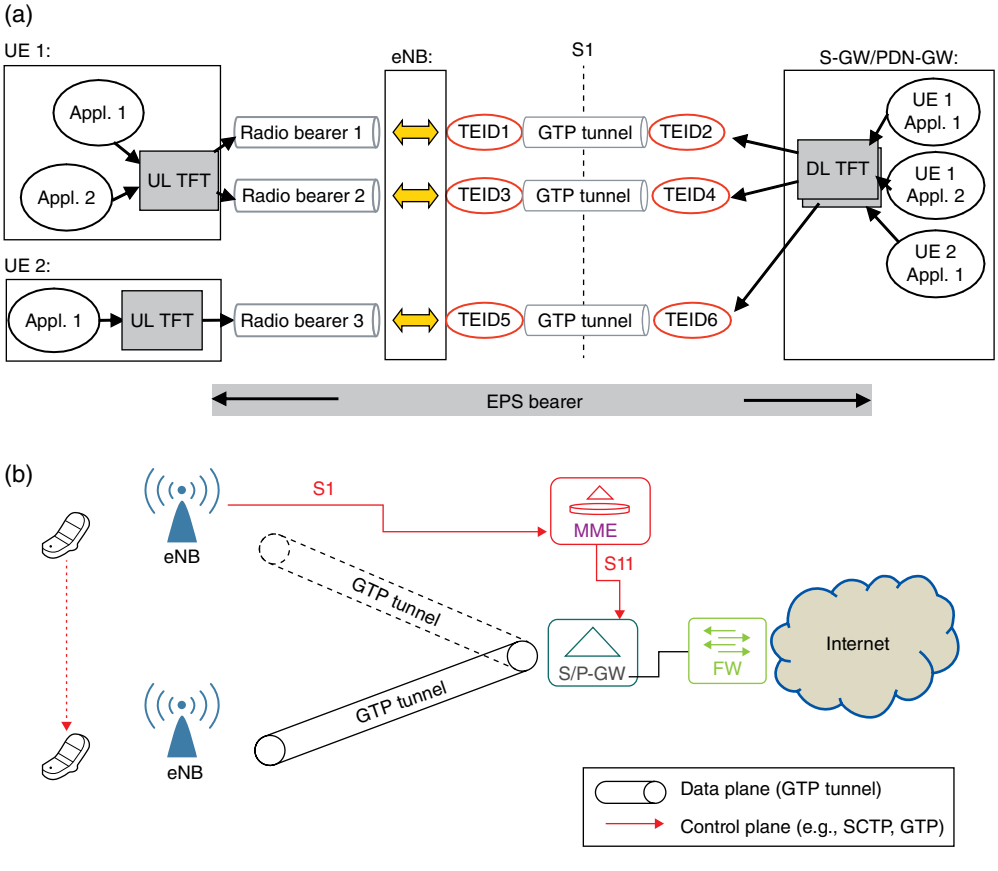

Figure 6.2 (a) Tunneling of user traffic over mobile networks and (b) handover process controlled from MME through S1 and communicated to S/P-GW to recreate a GTP tunnel.

When an 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 using the original UE IP address.

The handover process is initiated and managed through the S1 interface as shown in Figure 6.2b. MME is aware of the mobility process and communicates with the S/P-GW to recreate the GTP tunnel between the new eNB and the S/P-GW as shown in Figure 6.2b.

6.2.2 Options for Location of the SDMN Controller

Integrating SDN into mobile networks to become SDMN can be done in several ways: (i) controller can be integrated with the MME in order to be aware of mobility events, or (ii) controller can be integrated with the S/P-GW to control the transport network.

Figure 6.3 shows the current LTE architecture, which allows multiple options for integrating the SDN controller.

Figure 6.4 describes one option of integrating SDN into the LTE architecture. This option consists of decoupling the S/P-GW into the control and the data planes. The control part of the S/P-GW (i.e., S/P-GWc) provides IP address allocation for the UE and is responsible for applying the TFT to the user data flows. The data plane of the S/P-GW (i.e., S/P-GWu) provides the GTP tunneling termination endpoint 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 and sends the TFT to the S/P-GWu, which then enforces it as data filtering. The rest of the network elements are not changed, and the MME interacts with the S/P-GWc.

The second option for integration SDN in the LTE architecture consists of embedding the SDN controller with the MME as shown in Figure 6.4b.

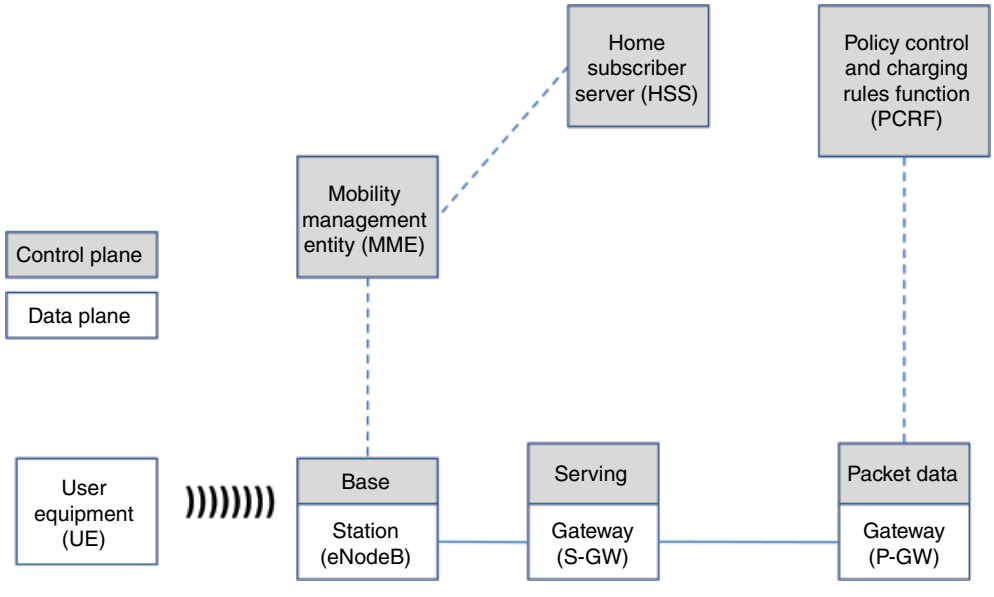

Figure 6.3 LTE mobile architecture.

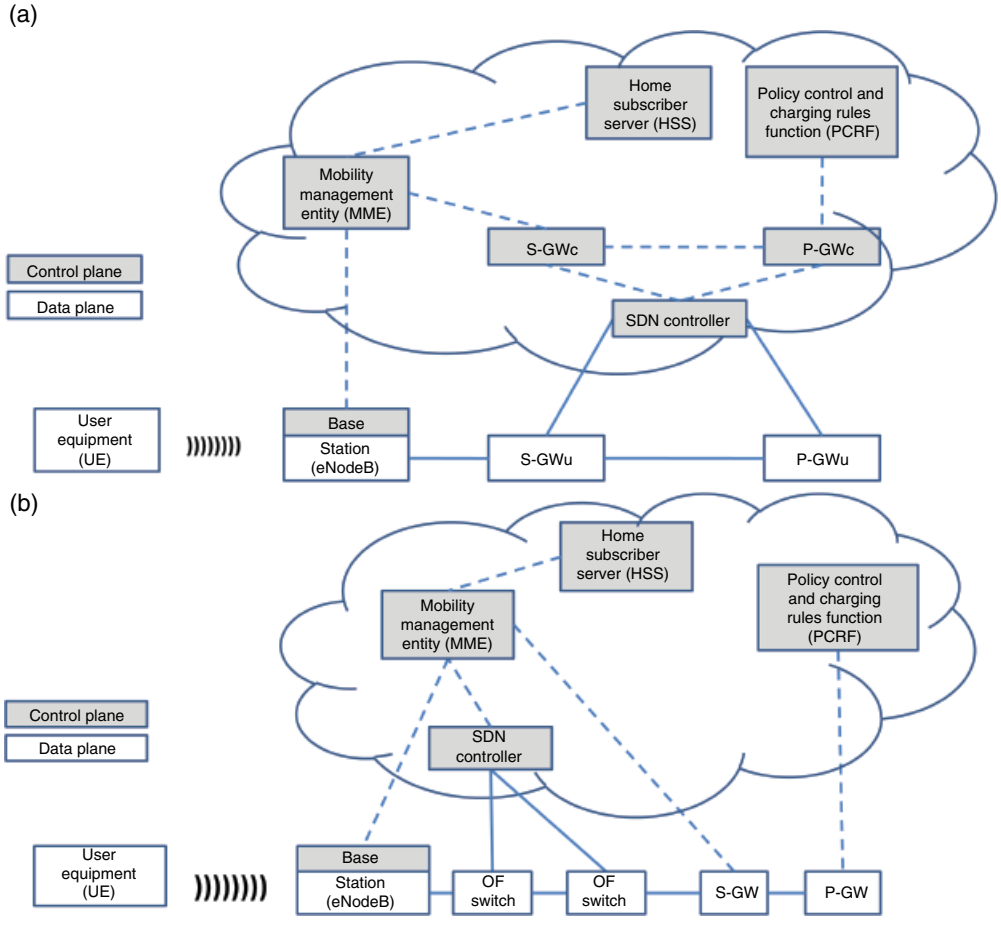

Figure 6.4 (a) Integration of SDN with S/P-GW and (b) integration of SDN with MME.

This option allows the SDN controller to learn about mobility events directly from the MME allowing to apply new rules in the switching nodes to reestablish routing paths in an optimal manner. In Figure 6.4b, the DP based on OF between eNB and S/P-GW need to understand GTP.

Integrating SDN controller functionality with MME provides a smooth integration in the long term as well as a disruptive solution in mobile networks. The issue for the SDN integration is how to support mobile-specific protocols with OpenFlow. Since OpenFlow does not support GTP and modifying the OpenFlow for such support would lead to loosing economies of scale in the switching elements as well as make the integration of caching and network monitoring functions into the network more costly and cumbersome, it is reasonable to study the options of replacing the GTP-u with standard data communication protocols such as variants of Ethernet and MPLS. The resulting mobility solution, instead of tunneling over IP, would be based on SDN-controlled switched paths.

In SDMN, 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.

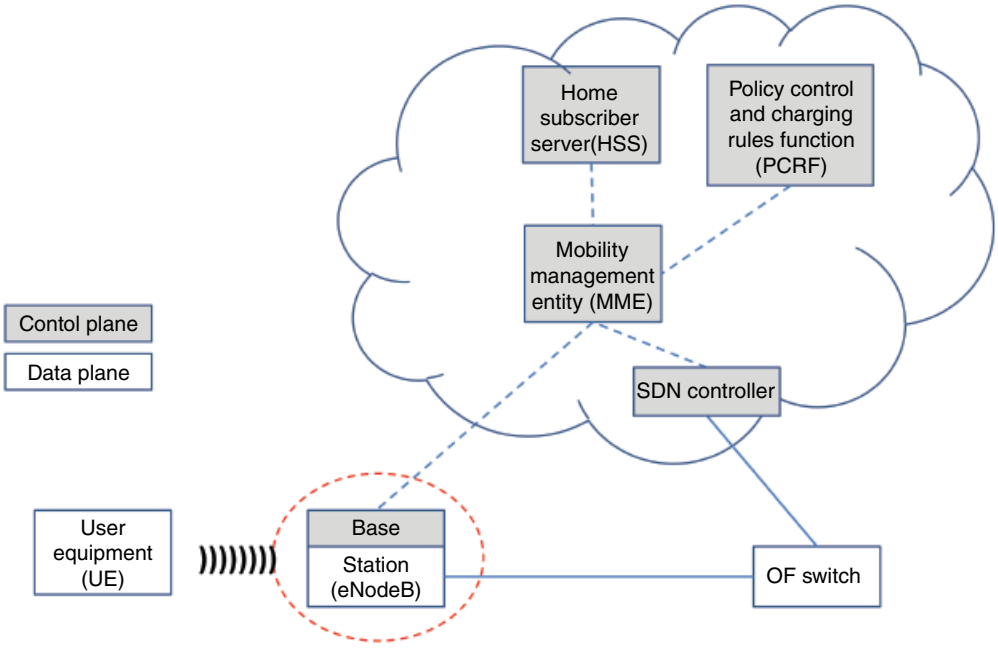

Figure 6.5 Disruptive integration of SDN with MME.

Therefore, it makes sense to group the controller and current S/P-GW functionality in the same network application together with the MME functionality. We will call this application the Mobility Management App (MM App). In this approach, the currently independent S/P-GW elements disappear, and instead, an SDN-controlled switched packet network is used. This approach will add flexibility (e.g., easier provision of caching and monitoring) and value to networking (reduced packet overhead) with different increments and support the gradual introduction of high network throughputs, optimal flow management, and traffic engineering possibilities. Figure 6.5 shows the integration of mobility management with SDN controller. The challenge for the SDN control is to meet the necessary delay requirement in order to achieve seamless terminal mobility without too much signaling overhead. Another challenge is to meet all the functional requirements with the constraints set by the OpenFlow protocol.

Mobility is a critical aspect of mobile networks, which requires specific functionality in the network elements. Having tight linkage between the MME and the SDN controllers gives the best chance that the time-constrained functions of mobility, such as seamless handovers, are handled efficiently from the SDN controller.

6.2.3 Vision of SDN in LTE Networks

Starting from the late 1990s, the 3GPP has been taking steps toward a clear separation of data and control planes and the respective elements in the architecture. We propose to take this concept to the next level following the SDN paradigm. Figure 6.6 presents the 5G network control as a group of SDN applications. They are the Base Station App, Backhaul App, MM

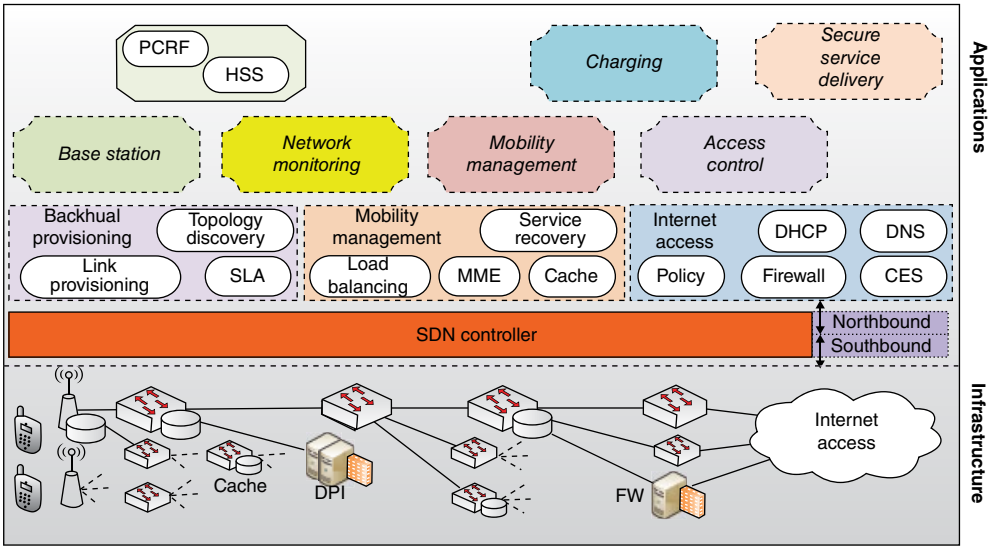

Figure 6.6 5G as a group of SDN Apps.

App, Monitoring App, Access App, and Secure Service Delivery App. The network applications are orchestrated via the Controller Northbound API. Multiple SDN applications operate without conflicts.

The Base Station App runs the control software that is now vertically integrated with the eNB. The physical base stations under its control consist of an antenna, a band-pass filter, and an Ethernet card for backhaul connectivity.

6.2.3.1 MM App

The MM App implements mobility as a service (MaaS) and is a reactive function. MaaS appears on the upstream interface of the OF switch (mOFS) that offers its service to the Access App. When a mobile device moves from the area of one eNB to an area of another, the rule in the mOFS for the device may need to be modified and a new rule may need to be created in the new eOFS where eOFS is the first aggregation point for the connected eNBs. 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 MM App chooses the path for a device. The load balancing decision is made based on input from the Network Monitoring App. In any case, it is desirable that the point of attachment of a mobile to the Internet is fixed while it stays under the coverage of the current mobile network. To make this possible, every eNB in a mobile network has several preprovisioned paths to every mOFS.

The MM App incorporates the MME. In addition, it needs to manage the quality of service for each user, to balance the load among the alternative paths across the aggregation network, and to route the user to a cache, when possible. Among the currently popular SDN concepts, OpenFlow is the most prominent. It does not support GTP tunneling. Therefore, it makes

sense to study alternative ways of carrying the user plane traffic from eNBs to the Internet and from the Internet to the eNBs. One alternative is to replace GTP data plane tunnels with carrier-grade Ethernet (CGE) encapsulation methods. The result would be an Ethernet switched path-based mobility implementation. Another alternative would be to study the use of MPLS encapsulation between eNBs and the Internet.

For mobility management, for many procedures, eNBs need to be directly connected with some tens of their neighbors over the X2 interface. For this reason, in an Ethernet-based solution, 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 under the eNB, while the other identifies the destination such as "Internet" or an X2 neighbor. The Internet VLAN is switched to 802.1ah by eOFS. The X2 VLANs are either locally switched in eOFS to destination eNBs or using 802.1ah the switching to the needed neighboring eNB can take place higher up in the network hierarchy. Since the X2 interface is used for mobility management, we propose that the MM App will request the Backhaul App to provision these switched paths. Finally, it is convenient that, although packet forwarding is based on switching, each eNB has either IP routing or Ethernet routing functionality for the X2 interface. For this purpose, the MM App may need to assign IP addresses to eNBs.

6.2.3.2 Access App

In one physical mobile network, there may be many Access Apps. In that case, an Access App is owned and operated by a particular mobile virtual network operator (MVNO). Putting mobility aside, it is the Access App that is responsible for providing the data services to mobile users. Key properties of the Access App include providing Internet access, firewalling unwanted traffic, and providing access to premium content.

In 5G, we propose 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. This is justified by the need to manage the reachability of the device per application and per user without cumbersome NAT traversal. It is also justified by the need to block all packets with a spoofed source address 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. In the proposed 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.

A task of the Access App is to assign an IP address for a mobile device. This can be a private address. Thus, the Access App provides the point of attachment to the Internet and to the service delivery networks to each mobile device by controlling an OF switch (iOFS) that connects the mOFS to the Internet. The point of attachment should be as stable as possible while the mobile moves or even roams to foreign networks. For an incoming flow, the Access App will handle firewalling and request downstream load balancing from the MM App. We believe that all flow admission should be managed by a policy that is part of the subscription information of the user. Policies could be managed by an extended 3GPP policy and charging management architecture. Policies can be dynamic, that is, treat different remote hosts differently based on reputation produced by a trust management system. Moreover, a cooperative firewall can make queries to, for example, the sender's firewall or certification authorities

before making the final admission decision. This would dissolve the boundary between closed and open networks, managing all flow admission by the policy. 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 controlled by the Access App.

Traffic through the service delivery network is also tunneled. A binding state managed by the firewall ties the service delivery tunnel and the mobile backhaul tunnel together at the iOFS. The Realm Gateway (RG), a component of the Access App, can admit traffic directly from the legacy Internet without cumbersome NAT traversal.

6.2.3.3 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 data center 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 prevent 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).

6.3 Mobile Backhaul Scaling

The driving factors for the proposed design are as follows: (i) 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. (ii) The goal of mobility management is to provide seamless handovers.

Most 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. Applications like gaming benefit from delay reductions to the area of 10 ms. Therefore, the control functions for mobility management can reside a few hundred kilometers from the base station but not on a different continent (the propagation delay over a round-trip of 200 km in fiber is 1 ms) and only rarely in a different country.

(iii) 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 Nokia white paper [1] predicts that by 2020 a mobile user will consume 1 Gbyte 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: for example, 100 million customers will use about 1000 100GE interfaces when there is no caching.

To ease the challenge, caching has to be used maximally in mobile access. 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 data centers and the network that connects them. In practice, a very significant part of the tens of terabits of traffic consumed by the mobile users will be served from these data centers. Moreover, by connecting large cache servers to the CGE nodes serving hundreds of thousands to a million customers each and smaller caches to the eNBs, we can save on the number of mOFS and iOFS switches and on the required performance of these switches making the design presented in Figure 6.8b even more feasible.

Let us model the scaling of a 5G mobile backhaul network for 100 million customers with the assumption of 1 gigabyte of dedicated traffic capacity per user per day. We further assume that each eNB serves 100 to 1000 customers and that the backplanes of the backhaul data plane nodes are below 4 TiB/s. Figure 6.7 shows an overprovisioned network design without caching. It is an example that we use to study the requirements. The figure shows link and backplane speeds and average link loads when 24 h traffic is transmitted in 6 h.

To let the SDN applications manage the network, we place an OpenFlow switch (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 using 802.1ad encapsulation. The eOFS will tag the packets from the user toward the Internet: a suitable encapsulation is 802.1ah. The second OpenFlow switch (mOFS) is required before the entry point to the Internet. The mOFS will tag and route the packets from the Internet to the right eNB and the right mobile device. For traffic aggregation from many eOFSs to a few mOFS, we will use CGE switches since they are simpler than OF switches.

We can isolate each mobile into its own subnet using 802.1ah. The traffic from eNBs to the point where MaaS is offered to the Access App 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 (e.g., eight). This is because it is beneficial to keep the point of attachment of a mobile to the Internet stable while it stays in the area of the mobile network.

Given the assumptions, it is easy to calculate that the required tag length for marking the path between the two OFS is in the order of 20–24. If the eNBs are small on average, a single 802.1ah path from the eNB to mOFS would lead to longer tags (around 29 bits). Normally, by deploying eOFS to which eNBs are connected, the path tag can, for example, be the 24-bit I-SID in 802.1ah. An alternative to 802.1ah is 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 the 802.1ah encapsulation, the I-SID value marks the path between an eOFS and mOFS. The B-VLAN tag can be used to

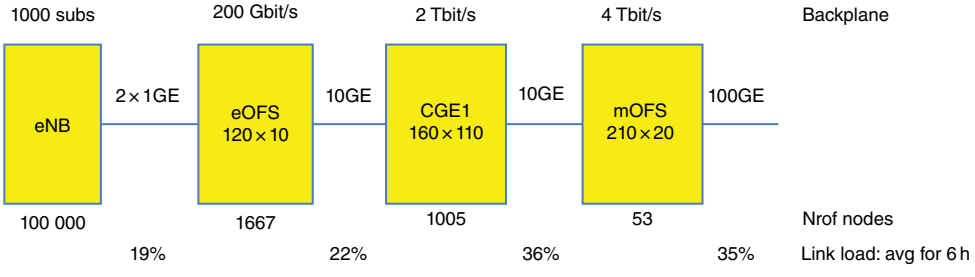

Figure 6.7 Network scaling example.

separate traffic of different virtual operators if necessary and finally the C-VLAN tag as network identifier within the operator, to choose the right mOFS and GW, since the address provisioning already allocates different networks (subnetting/29) per UE. In case of MPLS encapsulation, several MPLS labels would be needed.

When integrating SDN in mobile networks, scalability is another major issue to be considered. Figure 6.9 represents the aggregation of data paths interconnecting different tracking areas with the corresponding GW element for that mobile operator. Figure 6.8a shows a possible mobile network topology where OF switches are used to aggregate traffic in different parts of the mobile backhaul.

In LTE, when the UE attaches to the mobile network through the eNodeB, the MME will request default context from the S/P-GW that will assign an IP address to the UE and will establish a tunnel between the eNodeB and the OFS-GWx. Figure 6.9 shows the usage of 802.1ad and 802.1ah in the mobile network to allow carrying the data between the eNodeB and the GW but still using existing Ethernet switches in the network. During the attachment, both an uplink and downlink between the eNodeB and the GW are established.

The aim of the uplink is to communicate the originating eNB with the specific point of attachment to the Internet selected by the MME for a given UE. We aim at offering MaaS transparently to the MVO, so that any standard routing equipment can be used for connecting to public networks.

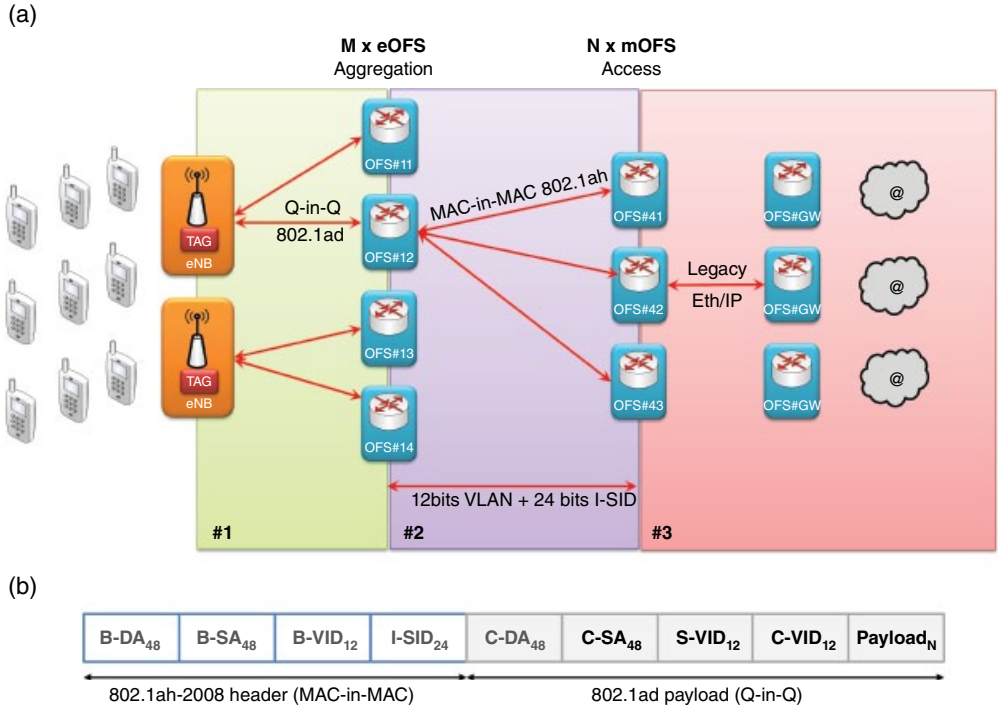

Figure 6.8 (a) Aggregation of tracking areas in mobile access network and (b) Ethernet packet encapsulation for 802.1ah and 802.1ad.

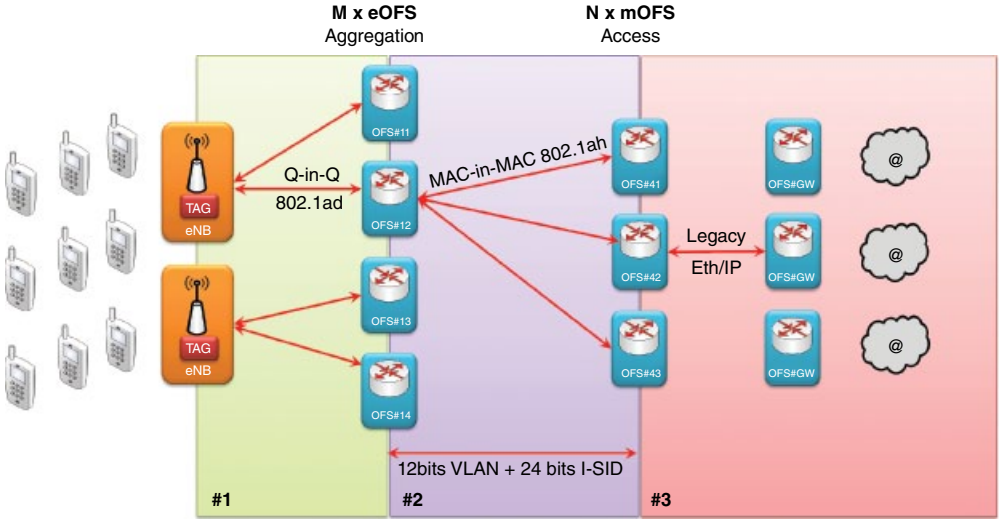

Figure 6.9 Direct L2 path eNB to OFS-GW w 802.1ah (MAC-in-MAC).

Now, we describe a possible usage of the different fields in the encapsulation of Figure 6.8 as well as the actions in the OpenFlow switches involved in the communication path. We use 802.1ad (Q-in-Q) for sending data packets from the eNB toward the Internet through the eOFS.

The eOFS, the first SDN switch, receives a data packet with:

- C-DA: MAC_{GW}
- C-SA: MAC_{UE}
- S-VID: MVO_{ID} (12 bits)—identifies the Internet access service of the MVO
- C-VID—identifies the NetID of the MVO (private address space of this user used by the MVO)

The network between eOFS and mOFS uses 802.ah (MAC-in-MAC) for forwarding data packets. The outer MAC will be used for switching the Ethernet frames within the mobile backhaul. This outer MAC uses upstream:

- B-DA: MAC_{mOFS}
- B-SA: MAC_{eOFS}
- B-VID: VLAN identifier (12 bits)
- I-SID: Service identifier (24 bits)—for identifying the path between eOFS and mOFS

The payload of this MAC frame consists of the inner MAC where the payload includes C-DA, MAC_{GW} C-SA, MAC_{UE} S-VID, MVO_{ID} (12 bits) C-VID, MVO_{NetID} (12 bits), and the IP_{UE}.

Once the frame is switched to the mOFS, the mOFS will terminate the 802.ah (MAC-in-MAC) and 802.ad (Q-in-Q) path and forward the data packet to the GW using IP over regular Ethernet. This enables using standard IP routers for connecting to public networks. The SDN-Ctrl and mOFS are responsible for maintaining an updated status of the location of the UEs.

In the downstream direction, the Internet GW can send data to the specific eNB where the UE is located. We have the reverse process in the downstream: we create in mOFS the 802.ah (MAC-in-MAC) and 802.ad (Q-in-Q) frames out of the received packets from the GW that use IP over Ethernet. We use 802.ah (MAC-in-MAC) for forwarding data from mOFS toward eOFS. The combination of B-DA + VLAN tag (B-VID) + service identifier (I-SID) determines the L2 paths. The structure of the MAC would be:

- B-DA: MAC_{eOFS}
- B-SA: MAC_{mOFS}
- B-VID: VLAN identifier (12 bits)
- I-SID: Service identifier (24 bits)

The payload of the outer MAC will include the inner MAC consisting of:

- C-DA: MAC_{UE}
- C-SA: MAC_{GW}
- S-VID: MVO_{ID} (12 bits)
- C-VID: MVO_{NetID} (12 bits) and the IP packet of the UE

We terminate the 802.ah (MAC-in-MAC) path in the eOFS exposing the 802.ad (Q-in-Q) for further analysis. The SDN-Ctrl and eOFS are responsible for maintaining an updated status of the location of the UEs for the downstream traffic. The matching state in eOFS is based on the C-DA, S-VID, and C-VID that determine the current eNB where the UE is located and the packet will be forwarded to the correct eNB.

For scalability of the proposed usage of different identifiers, considering that each mobile device will consume 8 IP addresses, with private addresses of the range 10.x.y.z, we can identify 2 million × 212 = 233 devices. We can allocate several S-VID values for one MVO because it is unlikely that in one physical network there would be thousands of MVOs. The C-VID identifies the network within a given MVO. The scalability with 2 million hosts per network is the product of S-VID × C-VID (networks) × 2 M (UEs). This example forwarding system is summarized in Figure 6.9.

6.4 Security and Distributed FW

The current Internet model makes it possible for a host to send data packets to any destination address, whether these packets are wanted or not. A receiver is unable to establish a set of requirements a remote sender must comply with prior to sending any data packets. As a result, unwanted traffic can only be discarded by the receiver upon arrival. In addition, source address spoofing benefits DDoS attackers because it makes it difficult to attribute evidence of antisocial behavior to the originating hosts or networks. Spammers, hackers, fraudsters, and other malicious users rely on botnets for their activity that destroys network value to the majority of the users.

From Prisoner's Dilemma tournaments, we know that cooperative strategies can become dominant in societies where actors can efficiently share their opinions about the trustworthiness of other actors and where the interactions are unending. A precondition is that obstinate

violators of rules, who simply will refuse to cooperate, can be curbed in some way. Based on this result, we argue that host-based stand-alone solutions cannot tackle the wide variety of threats that exist today. Traditionally, firewalls have been deployed to protect both hosts and networks, by executing a set of rules ordered in a predefined fashion, based mostly on local information and data gathered from deep packet inspection of data traffic at different protocol layers. The result is ultimately limited to accepting or dropping a given connection.

In modern and future Internet, most hosts use wireless connections and personal battery-powered devices. The devices may also sense or manipulate objects in the real world creating many new threats compared to the traditional Internet. It would be desirable to block all packets with spoofed source addresses, all DDoS packets, as well as all unwanted packets from reaching the air interface and even more desirable from reaching the mobile device where a host-based firewall would have to wake up the device to process any unwanted packet and as a result exhaust the battery while it would be doing a perfect job for the security of the device. It would also be desirable to admit to the mobile device only flows that come from authorized parties. At the same time, for the developer of legitimate applications, it would be desirable to offer a network that automatically manages reachability without the need for application level NAT traversal mechanisms.

To meet the above goals, we propose to extend the functionality of traditional stand-alone state-full firewalls to policy-based cooperative firewalls. The policies are then defined in the firewall nodes, usually located at the network edges where we now have a network address translator or a generic gateway (S/P-GW). By embedding the firewall functionality in these nodes, it is possible to acquire a wider and more coherent view of the network that otherwise would not be possible with a stand-alone host-based solution. For example, the receiver's policy may require the following conditions to be met before flow admission:

- The address of the sender's edge node is not spoofed.
- Present a certificate of the sender's edge node.
- Present a stable and verifiable identity of the sending host.
- The sender's network is not blacklisted.
- The sender itself is not blacklisted.

In addition to the above, the firewall can also propose the remote edge to quench a source (your host x is DDoSing me, stop it) or report a reflection attack to an uninfected host that is exploited by an attacker for hiding its own identity.

Under such conditions, if the receiver suffers any kind of attack, it is always possible to attribute blame on the sender's network or the particular host that was initiating the connection. It is also possible to block all traffic from hosts that are known to distribute malicious code or act on behalf of an attacker. Making all the checks of identity apply to all communications is, however, too costly and not feasible. Therefore, we argue that all communication should be managed by policy. By efficiently collecting and aggregating evidence and distributing the results to cooperative firewalls, their blocking policy can become dynamic and react in an accurate and fine-grained manner to new malicious actors.

Under this new paradigm, the firewall adopts then the functionality of communication trust broker for the hosts that it protects. The access to these hosts is only granted upon successful policy negotiation. The mission of the policies is to define a number of prerequisites that need to be fulfilled prior to accepting a new flow between the communicating parties. As a result,

unwanted traffic can be effectively blocked closer to the source, and repeated unsuccessful policy negotiations can be attributed to specific users, thus discouraging attackers with malicious intents.

6.4.1 Customer Edge Switching

To demonstrate the feasibility of the ideas presented in Section 6.4, we have created the technique of customer edge switching (CES). It offers a cooperative firewall with dynamic policy management as a virtualizable security software entity. Network awareness motivates the necessity of dynamic policies as they enable different levels of security and a fine-grained response to attacks. The required knowledge can be acquired based on local information as a result of policy negotiations or deep packet inspection, as well as from the collaboration of other connected devices or a global reporting system for security and trust.

It is possible to leverage virtualization for spawning dedicated firewall instances in the cloud. The number of these instances is determined by the amount of traffic and mobility procedures. Virtualization gives a flexible network provisioning by dynamically adjusting the amount of resources available. The adoption of SDN solutions facilitates the deployment of new services in a virtualized framework. New security modules such as CES can be colocated with the S/P-GW elements. (Note that one of the core functions of P-GW is address assignment). If a firewall must give promises about host addresses to remote parties, it is best that the firewall itself assigns the addresses. Therefore, it is logical that a cooperative firewall should be integrated with the P-GW.

As SDN brings the possibility of dynamic flow modifications, therefore the level of security can also be adjusted in a fine-grained manner. For example, an initially trusted flow may benefit from minimal intrusive security policy, but on the event of security threats, this flow may be resubmitted to more extensive DPI analysis on different firewall instances and to a honey pot. This further analysis allows to collect further evidence or ultimately trigger a BGP update to create a sinkhole in the network and disconnect the attacking network for a given time.

Virtualization directly benefits the operators in the sense that it can improve their efficiency by dynamically allocating more resources during busy hours and reducing them during idle times. Energy consumption can also be decreased by shutting links down during the idle times.

6.4.2 RG

When the networks of both communicating hosts have adopted CES, we can ensure a clearly better level of security compared to the state of the art. When the sender is not behind a CES node but either has a globally unique IP address or is behind a NAT or NAPT, we must provide interworking for the servers that are behind a CES node (for the case of servers with globally unique IP addresses, a CES not trivially acts as a NAT). For this interworking case, we developed the RG that is able to dynamically admit flows to the servers that it is serving from any legacy Internet hosts [2]. Upon a DNS query, the key algorithm (circular address pool) dynamically reserves an RG outbound address for a short period (we use 2 s in the demonstrators) of time. Upon the arrival of the next new flow, this reservation is removed and the address is released for the next DNS query. Additional information about the expected flow (such as its

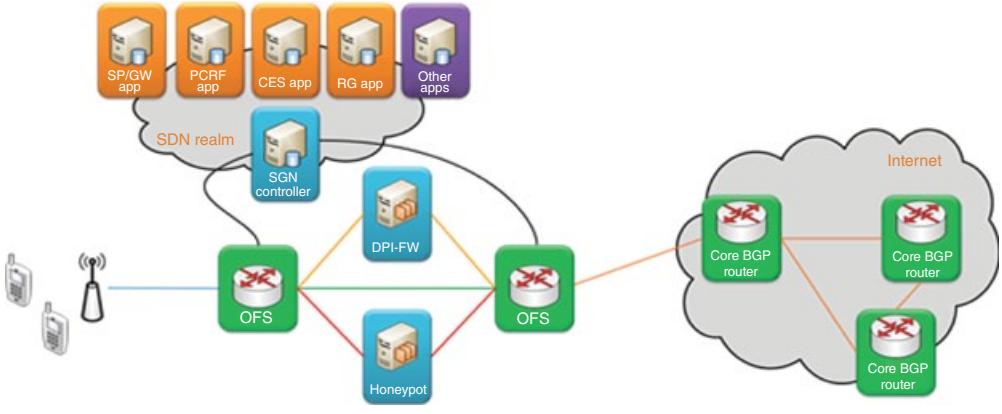

Figure 6.10 Integration of CES in SDN.

port) can be configured in the DNS leaf node that resides in the RG itself making the reserved state available just for the expected new flow and thus making hijacking of this state difficult. The RG can also translate between IPv4 and IPv6. To secure the RG, we developed a number of heuristics that, for example, protect the RG from DDoS attacks that use spoofed DNS queries to powerful DNS servers that serve queries from any hosts and may thus end up being used as reflectors for the purpose of DDoSing hosts behind an RG or any other hosts as shown in Figure 6.10.

6.5 SDN and LTE Integration Benefits

The integration of SDN in LTE networks provides benefits in terms of CAPEX and OPEX since control functionality is implemented by cloud services and will thus benefit from commodity computing facilities. Another benefit emerges from the fact that the transport network is simplified by removing the GTP tunnel for the data plane. In the future, this allows using commodity off-the-shelf OpenFlow switches, which will provide the required data forwarding features controlled from the cloud.

From the different options of integrating SDN with LTE, the proposal of putting the MME and the SDN controller in one SDN App brings several benefits. The controller needs to have the necessary information about the location of the UE and the associated mobile operator as well as the necessary attachment and handover events. Therefore, the controller should be integrated with the MME and S/P-GW to receive those events and establish the required MAC-in-MAC and Q-in-Q mappings. Moreover, this integration results in the next disruption where data plane is managed from a single MME/controller element. The evolution toward this architecture can take place progressively where the MME will keep its current interfaces for receiving the signaling through the S1-MME interface. The MME maintains the current standard process and establishes GTP tunnels between legacy eNodeB and S/P-GW. Simultaneously, the MME can include the new SDN functionality and establish communications between the new model eNodeBs and IP routers directly at layer 2 without GTP tunneling. In this scenario, the same MME, when receiving the signaling from an SDN-based eNodeB through the S1-MME interface, will establish the connection with the

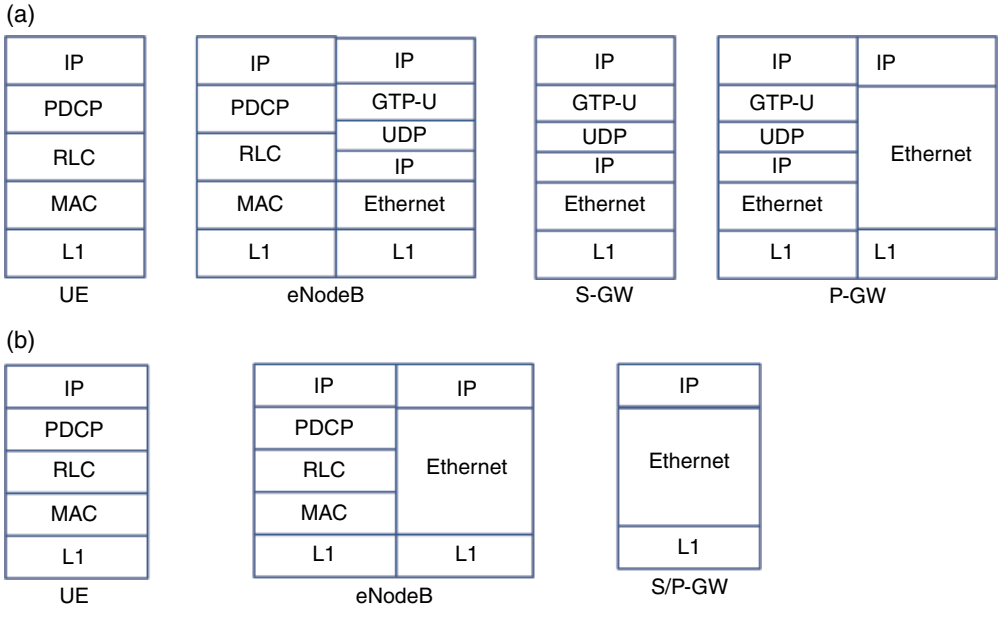

Figure 6.11 (a) User plane networking stack in LTE and (b) user data plane networking stack in LTE with SDN control.

termination SDN switch over L2 using TUN interfaces. The networking stack currently used for the user plane is depicted in Figure 6.11a. The radio layers are terminated in the eNodeB from where GTP is used up to the S-GW and the P-GW that provides the bridge to the public Internet.

The usage of 802.1ad in the backhaul and integration of MME with the SDN controller allows the removal of GTP. This will result in the simplification of the stack in the eNodeB that terminates the radio layers and includes an Ethernet switch toward the rest of the network in the backhaul as shown in Figure 6.11b. Moreover, the S/P-GW is simplified after removing the GTP-u and consists of a simple Ethernet switch and IP router toward the public Internet. In this architecture, the mobility is performed by the SDN controller.

This architecture leads to an optimized transport network as well as a scalable control plane that converges into single network application: MME with embedded SDN controller functions. This MME would run either in dedicated HW or as a cloud service to allow launching multiple instances as needed to overcome scalability limitations of having the functionality in a physical network element. The MME on the other hand will continue supporting their current networking stack as depicted in Figure 6.12. This approach allows smooth transition. The MME would be able to manage current network elements, that is, eNodeB and S/P-GW, but the integration with the SDN allows managing the new eNodeB and S/P-GW where GTP has been removed.

In addition to the integration of the MME with the SDN and the simplification of the backhaul network by removing GTP from the network elements (i.e., eNodeB and S/P-GW), the network has to be flattened. The network elements are normally located in the core network.

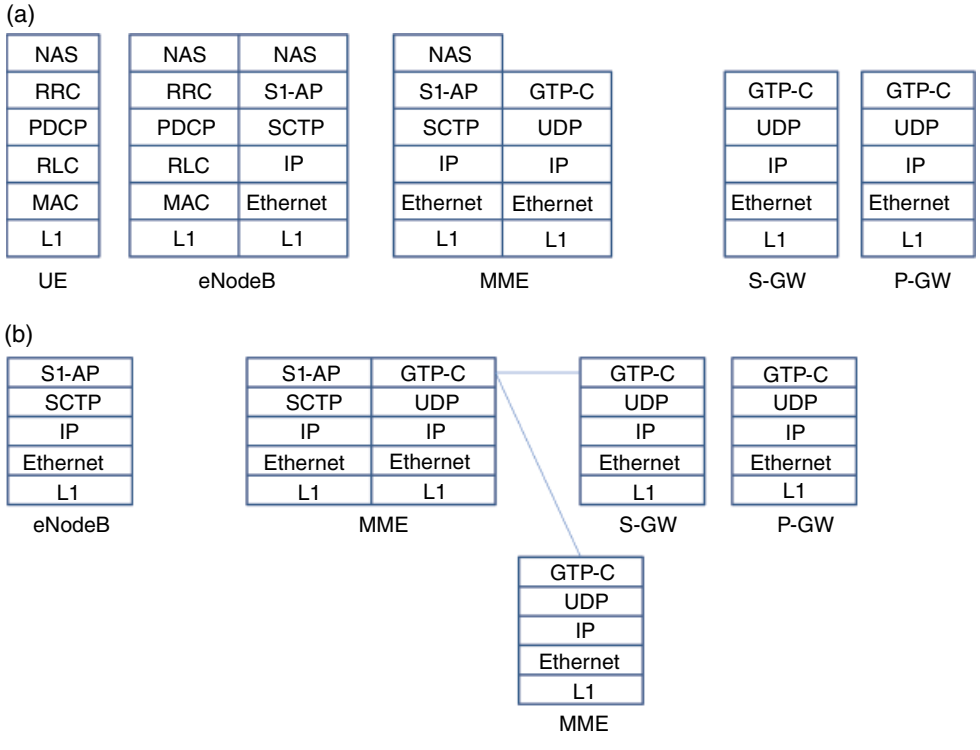

Figure 6.12 (a and b) Signaling networking stack.

Instead, the network needs to be flattened so the network elements are located closer to the eNodeB in the backhaul. This allows deployment of stand-alone access networks with their own network elements. The coordination of multiple access networks would be done using a centralized database, and the handover between the MMEs located in each access network would be carried out through the S10 interface. The signaling networking stack remains the same to interact with legacy LTE network elements such as S/P-GW and other MMEs as shown in Figure 6.12b.

6.6 SDN and LTE Integration Benefits for End Users

The integration of SDN in LTE networks brings certain benefits to mobile operators in the sense that EPC functionality can be virtualized and moved to commodity servers, which means reductions of CAPEX and OPEX. However, the end users can also benefit from adopting SDN as described in the following sections.

- Content Caching

The always increasing role of content delivery networks (CDN) in the Internet traffic shows a clear shift to content consumption. CDNs leverage the power-law nature of content popularity

distribution where many users request popular contents within a short period of time. Therefore, storing a copy of popular contents in caches placed at the proximity of end users reduces server load, decreases network congestion, and lowers delay. In the context of 5G mobile networks, placing caches directly at the edge would be of great benefit for the network. Still, placing caches exclusively at the base stations is not the ultimate solution as the number of users that would use the cache would be too limited to really benefit from demand patterns. Instead, we advocate the usage of multistage caches with a rather small general-purpose least recently used (LRU) cache collocated in every base station to absorb retransmission events with high temporal locality demands (e.g., live streaming) and large caches spread over the different points of presence. The spreading of the caches allows to aggregate traffic of a large portion of users, therefore reducing the traffic in the core and consequently also the ISP connection charges of the MO. By looking at the reasonable backplane speeds in our 100 M 5G network, we deduce that it is economical to connect large caching servers behind the CGE switches each serving close to 1 million users. Cache hits would then reduce the number of required high cost mOFS and iOFS switches as well as reduce Internet connection charges of the mobile operator. Since a CGE switch is capable of decoding the 802.1ah, caching nodes can be easily connected to these switches directly.

The usage of SDN with the proposed integration facilitates the dynamic relocation of the cache based on the number of users. We created a pilot to demonstrate the effect on the network when moving the cache. We use HTTP live streaming for the video file and performed tests with the architecture presented in Figure 6.13.

We performed various tests with increasing number of users (up to 16 per eNB) to check the variability of the caching effectiveness based on number of users in different locations.

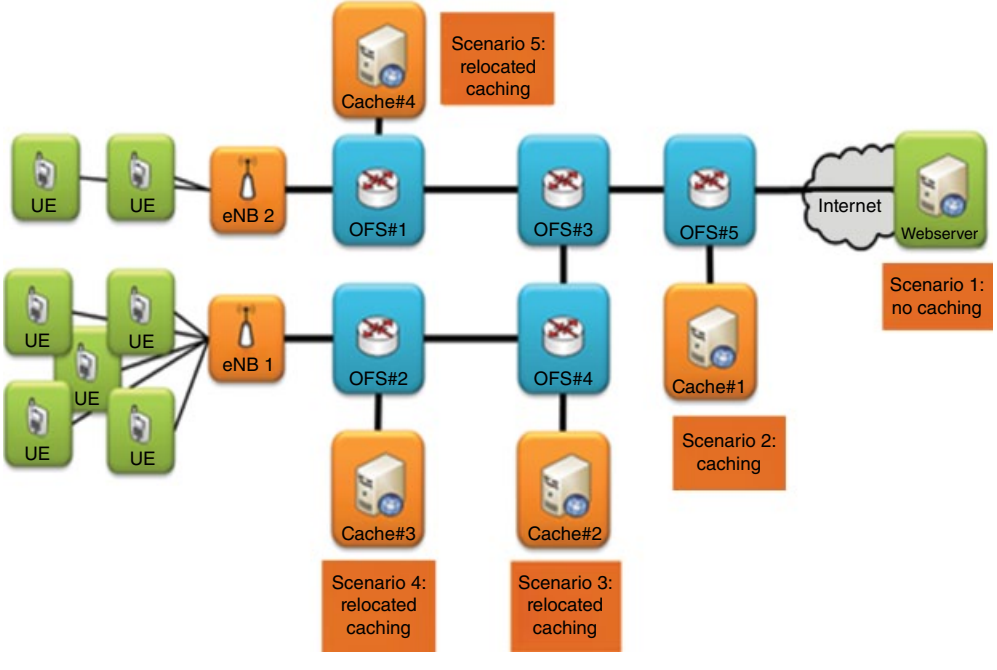

Figure 6.13 Architecture of the testbed with SDN integrated with LTE and caching.

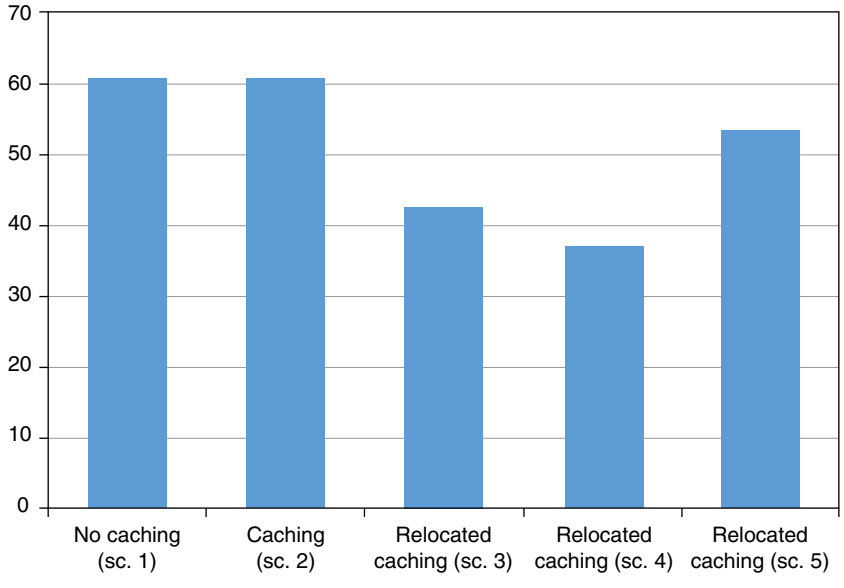

Figure 6.14 Load for different types of caching.

We simulated a user streaming a video by an HTTP download of the segments with a bandwidth limitation to 2 Mb/s and multiplying the bandwidth limitation by the number of users simulated. Since we are using HLS, there are some breaks between the segment downloads; and with high number of users, the breaks between the files become more frequent so they may have an influence on the calculation of the peak bandwidth consumption by the network measurement tool that is calculating it. Figure 6.14 presents the network load for the different scenarios for a 2 Mb/s stream, with five users on eNodeB1 and two users on eNodeB2.

The load is calculated as the sum of the loads, related to the download, of each link:

$$L = \sum_{j=1}^{N} \sum_{i=1}^{n} a_i b_{ij}$$

where N is the number of users, n the number of links, a_x the video stream throughput, and $b_{xy} = 1$ if the traffic of the user x is going through the link y or 0 if not.

We can see in Figure 6.14 that when the content is closer to the base stations, the overall load induced by users fetching this content is reduced. This is what we want to achieve by using cache relocation.

Then, for the same amount of users per base station (five on the first one and two on the second), Figure 6.15 presents the impact of the video throughput on the network load.

As expected, the network load is proportional to the throughput of the stream. So for the other tests, we will set it to 2 Mb/s. The results prove that, as expected, a relocated cache is more efficient to reduce the load of the network but only if it is close enough to the majority of the users requesting the content. If it is not the case, it may perform worse than the original cache, depending on the number of hops to the users. Finally, by optimizing the location of caching, consequent bandwidth can be saved.

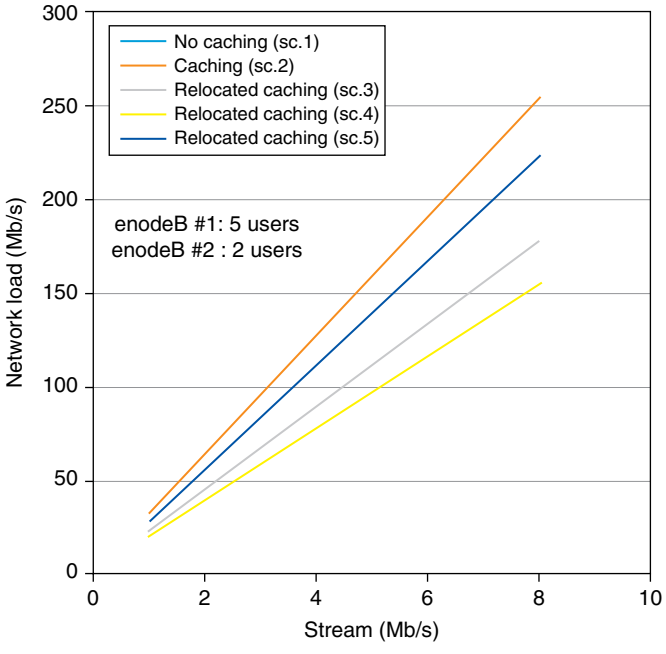

Figure 6.15 Network load depending on the video throughput.

6.7 Related Work and Research Questions

Some concepts for SDMNs were already discussed in previous publications [3–10]. 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 multidimensional 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 fronthaul. 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 [11].

6.7.1 Research Problems

While the lower levels of the SDN architectures have gained most attention, the SDN applications are still a field of research [12]. 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. Therefore, mechanisms to gain packet-level information, same as the existence of a northbound API, are undoubtedly parts of future networks. Finally, the implementation of the concept of secure service delivery and east–west interface in SDN would be beneficial. The latter would allow control communications cloud to cloud from socket to socket rather than going through the switches each time.

6.7.2 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 [12]. 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 are likely to 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 its current infrastructure. The adoption of SDN will lead the MNO to deploy or lease its own cloud to run its 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 operating the networks, three principal business roles with distinct competences can be identified: (i) mobility management including frequency licenses and use, towers, base station sites, and understanding mobility patterns; (ii) providing connectivity between sites; and (iii) 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 6.6. 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.

6.8 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 chapter, we conclude that for modeling the 5G as a

software defined network, a group of SDN applications (e.g., Base Station, Backhaul, Mobility Management, Monitoring, Caching, Access, and Service Delivery App) is required. We also describe a set of use cases, namely, caching and firewalling, that provide evidence of feasibility of SDN in 5G networks. Scalability is analyzed in detail to ensure SDN can be deployed in mobile networks.

References

[1] NSN White Paper, "Technology Vision 2020, Technology Vision for the Gigabit Experience," 2013. Available at: http://networks.nokia.com/file/26156/technology-vision-2020-white-paper (accessed May 21, 2015).
[2] R. Kantola, "Customer Edge Switching." Available at: www.re2ee.org (accessed on February 18, 2015).
[3] X. Jin, L. E. Li, L. Vanbever, J. Rexford, "SoftCell: Taking Control of Cellular Core Networks," 2013. Available at: http://arxiv.org/abs/1305.3568 (accessed on February 18, 2015).
[4] L. E. Li, Z. M. Mao, J. Rexford, "Toward Software-Defined Cellular Networks," in Proceedings of the EWSDN, 2012. Software Defined Networking (EWSDN), 2012 European Workshop on Darmstadt, October 25–26, 2012, IEEE ISBN 978-1-4673-4554-5.
[5] A. Basta, W. Kellerer, M. Hoffmann, K. Hoffmann, E.-D. Schmidt, "A Virtual SDN-Enabled LTE EPC Architecture: A Case Study for S-/P-Gateways Functions," in Proceedings of the SDN4FNS, Trento, Italy, 2013.
[6] K-K Yap, R. Sherwood, M. Kobayashi, T-Y. Huang, M. Chan, N. Handigol, N. McKeown, G. Parulkar, "Blueprint for Introducing Innovation into Wireless Mobile Networks," in Proceedings of the 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 the 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 Resource Model (NRM) Integration Reference Point (IRP), 2013.
[11] Y. G. Sajad Shirali-Shahreza, Efficient Implementation of Security Applications in OpenFlow Controller with FleXam," in Proceedings of the IEEE 21st Annual Symposium on High-Performance Interconnects, 2013.
[12] Gartner Report, "Hype Cycle for Networking and Communications," 2013. Available at: https://www.gartner.com/doc/2560815/hype-cycle-networking-communications- (accessed May 21, 2015).