11

Survey of Traffic Management in Software Defined Mobile Networks

Zoltán Faigl[1] and László Bokor[2]
[1] *Mobile Innovation Centre, Budapest University of Technology and Economics, Budapest, Hungary*
[2] *Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary*

11.1 Overview

Due to the evolution of mobile technologies, in these days, high-speed data services are dominating in mobile networks both in uplink and in downlink. In function of the characteristics of data services, the usage patterns, and the user and network mobility patterns, the utilization of network resources is varying in time and location. As the volume of traffic demands increases, the amplitude of their variations grows as well. Existing network, resource, traffic, and mobility management mechanisms are too inflexible to adapt to these demands. Software defined mobile networks (SDMNs) aim at improving the scalability and adaptability of the mobile network architectures to varying traffic demands by applying host and network virtualization concepts, restructuring the network functions into parts that are running in data centers in virtualized environment and parts, which cannot be virtualized, for example, base transceiver stations.

This chapter first defines the scope of traffic management in mobile networks in Section 11.2, including microscopic, macroscopic, improved content resource selection, and application-supported traffic management. Section 11.3 gives an overview of QoS enforcement and policy control in 3G/4G networks, which should be kept also in SDMNs. Section 11.4 surveys new research problem areas in software defined networks (SDNs) for traffic and resource management. Following that, an example of traffic engineering mechanism will be discussed in Section 11.5, that is, application-layer traffic optimization (ALTO) applied in SDN environments. ALTO–SDN provides improved resource selection and ALTO transparently for the users. This example shows the feasibility of SDN-based techniques for traffic management in SDMNs.

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

11.2 Traffic Management in Mobile Networks

Traffic management methods may be both necessary and warranted in the operation of broadband networks because of overbooking, that is, the network capacity requirement of the services sold generally far exceeds the available network capacity. Traffic management methods can mitigate the negative effects of congestion and can contribute to a more fair distribution of scarce network resources among users. Moreover, traffic management allows service providers to define service features.

Regulation, for example, in many European countries and in the United States, requires transparency of the network, no blocking of content, and no unreasonable discrimination of content. However, some users or applications, especially in content delivery, require quality of service (QoS) guarantees and data discrimination. Therefore, the regulation of such countries requires from network providers the definition of QoS criteria in the QoS Decree in a detailed manner based on the establishment of the service; the error ratio, availability, troubleshooting, etc.; and the specification of various quality target values depending on the nature of the service. Other QoS target values may also exist, which are required by a specific service but not included in the QoS Decree.

Modern traffic management possesses a very rich toolset of interventions, which may influence the traffic demands arriving in the network of the operator, the load distribution in the network, the priorities of traffic classes, etc. Traffic management consists of the following six different building blocks, as defined in the Celtic-Plus MEVICO project [1].

Microscopic-level traffic management is associated with all mechanisms with the primary objective to improve performance of individual flows based on application type, user profile, and other policy-related information. For example, multipath transport control protocol, congestion control, and QoS differentiation of service dataflows are such areas.

Macroscopic-level traffic management includes all mechanisms with the primary objective to improve efficient usage of network resources. Parameters for optimization in the latter case describe traffic patterns without detailed knowledge of individual flow attributes. Sample mechanisms for macroscopic traffic management are (re)selection of core network elements and IP flow mobility, energy-efficient and QoS-aware routing, load balancing, and technologies enabling the improvement of the usage of multiple interfaces and enforcing breakout of part of data services from the mobile network operator's network toward other networks.

The third category of traffic management technologies is called *improved resource selection*. The mechanisms associated to improved resource selection address the selection of the best service endpoint in the case of distributed services, such as Web-based content delivery by peer-to-peer networks, content distribution networks, or in-network caches. ALTO is a good example from this category, since it provides better-than-random endpoint selection for applications, considering both of the aspects of network operator and content provider (or distributor).

The previous technologies are associated with mechanisms, which may require support from lower layers (below application) and which may require support from each other. For example, improved resource selection may require support from macroscopic traffic management for finding the best path toward the optimal endpoint and from microscopic traffic management for enforcement of QoS policies.

The next three building blocks may require only little or no support at all from the previous categories. *Application-supported traffic management* aims at optimizing performance from end user perspective without getting support from network elements. Many traffic management applications of CDNs, multimedia streaming optimization techniques, P2P services, and even Provider Portal for P2P Applications (P4P) fall into this category.

Mainly network operators, but possibly also other stakeholders, may influence user behavior by defining certain constraints for usage of networks/services and certain incentives to comply with the usage constraints. Such procedures are called *traffic steering usage models*. They do not have too much technical aspects but influence traffic demands in the network.

Extension of network resources, or *overprovisioning*, is the sixth category of traffic management. When the network is regularly in high load conditions, network capacities need to be increased. It is a challenge to apply an intelligent planning process for extending the available resources.

11.3 QoS Enforcement and Policy Control in 3G/4G Networks

Connectivity to Packet Data Networks (PDN) is provided by *PDN connections* in 2G/3G/4G packet core of the 3rd Generation Partnership Project (3GPP) networks. A PDN connection comprises several aspects, that is, IP access, in-band QoS provisioning, mobility, and charging.

PDN connections are provided by *Packet Data Protocol (PDP) contexts* in the 2G/3G core between the User Equipment (UE) and Gateway GPRS Support Node (GGSN) and *Evolved Packet System (EPS) bearers* between the UE and P-GW in Evolved Packet Core (EPC) (4G core network) when UEs attach to evolved UMTS terrestrial radio access network (E-UTRAN).

Several options are available to provide PDN connection between 2G/3G access and the PDN GW or E-UTRAN and GGSN. For example, a UE can access from a 2G/3G radio access network (RAN) the Serving GPRS Support Node (SGSN) through PDP context, have a one-to-one mapping between PDP contexts and EPS bearers in the SGSN, and reach the S-GW and P-GW with EPS bearers.

2G/3G core supports two types of PDP contexts related to IP connectivity: IPv4 and IPv6. A PDN connection in EPC supports three options: the allocation of one IPv4, one IPv6, or both an IPv4 and an IPv6 address to the UE within the same PDN connection. 3GPP Release 9 introduced support for dual-stack PDP context also in 2G/3G GPRS core network.

IP address is allocated during the attach (PDP context activation) procedure to the UE. Another option is the usage of DHCPv4 after the attach procedure or PDP context activation. Stateless IPv6 address autoconfiguration is also supported by sending routing advertisements through the PDN connection advertising a 64-bit prefix allocated to the specific PDN connection.

In the case of E-UTRAN access, multiple EPS bearers can belong to the same PDN connection: a default bearer and optionally other dedicated bearers provide PDN connectivity. During the attach procedure, a default bearer is established to provide always-on connectivity for the UE. In 2G/3G GPRS core, PDP contexts are only activated when an application requests IP connection.

Each EPS bearer is associated with a set of QoS parameters and traffic flow templates (TFTs). TFTs specify the traffic filters related to the IP flows that are mapped to the specific EPS bearer. TFTs may contain traffic filters for downlink and uplink traffic (denoted by DL TFT and UL TFT, respectively). All traffic flows matching the traffic filters of an EPS bearer will get the same QoS treatment.

The filter information is typically the five-tuple of source and destination IP addresses, transport protocol, and source and destination ports. Wild cards can be used to define a range

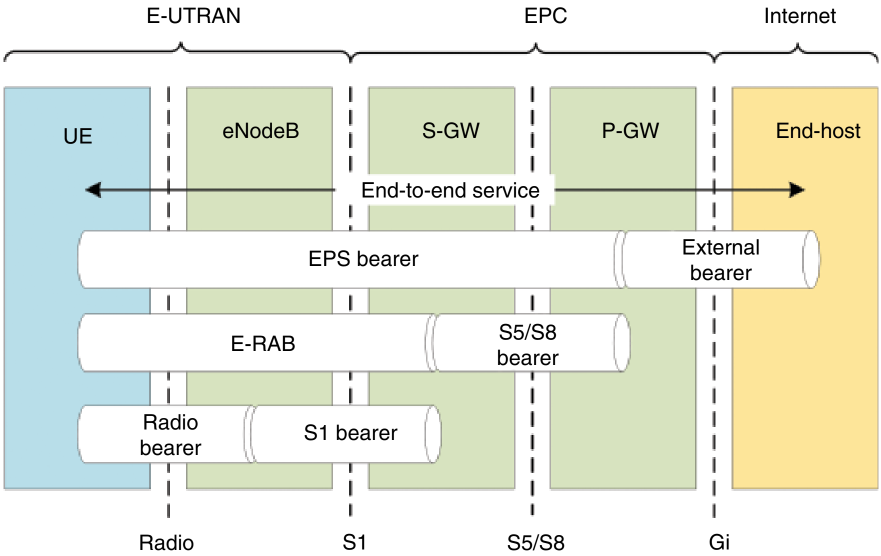

Figure 11.1 Hierarchy of bearers in LTE–EPC.

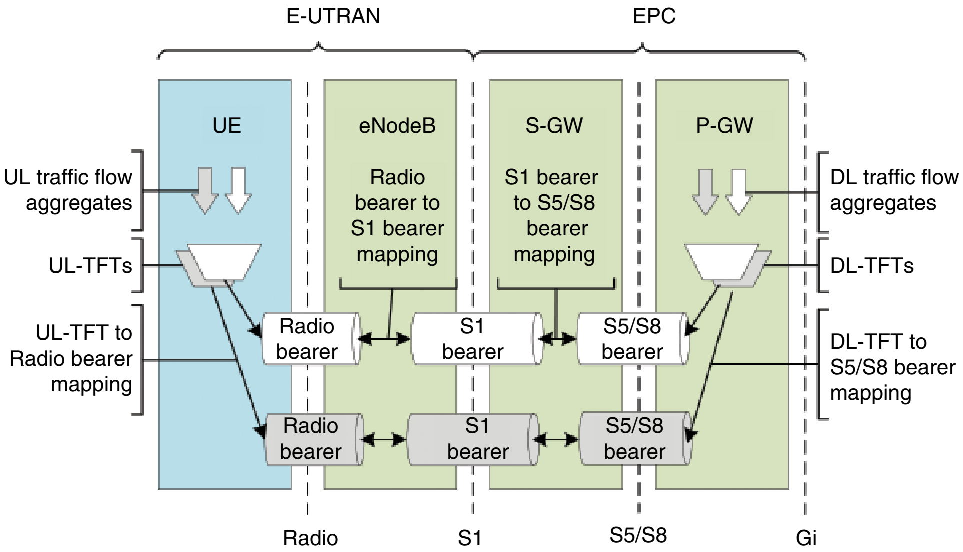
E-UTRAN
EPC
UE
eNodeB
S-GW
P-GW
Radio bearer to S1 bearer mapping
S1 bearer to S5/S8 bearer mapping
UL traffic flow aggregates
UL-TFTs
UL-TFT to Radio bearer mapping
DL traffic flow aggregates
DL-TFTs
DL-TFT to S5/S8 bearer mapping
Radio bearer
S1 bearer
S5/S8 bearer
Radio bearer
S1 bearer
S5/S8 bearer
Radio
S1
S5/S8
Gi

Figure 11.2 EPS bearer in E-UTRAN access and GTP-based S5/S8.

of addresses or ports. Other parameters of traffic filters can be the IPsec security parameter index, type of service (IPv4)/traffic class (IPv6), or flow label (IPv6).

EPS has adopted network-centric QoS control approach, that is, it is basically only the P-GW that can activate, deactivate, and modify EPS bearers and decide flow mapping to EPS bearers. That is different in pre-EPS systems. Originally, in 2G/3G GPRS, it was only the UE that could initiate new PDP context activation and decide about flow mapping to PDP contexts. Then 3GPP Release 7 introduced network-requested secondary PDP context activation where the GGSN initiates the creation of a new "bearer" (PDP context) and assigns IP flows to the bearer. This change is due to the introduction of policy control within the 2G/3G GPRS core and in EPC.

The GPRS Tunneling Protocol (GTP) is responsible for the control of PDP contexts in 2G/3G GGSN core (GTP-C) and the tunneling of IP packets of the user (GTP-U). In EPC, a new version for the GTP-C has been developed to manage EPS bearers over the S1 and S5/S8 interfaces, but the tunneling of user IP traffic remains the same as it was. It is called GTPv2.

Depending on the tunneling option, EPS bearers are implemented in different ways. Figure 11.1 represents the hierarchy and terminology of bearers for E-UTRAN access. For end-to-end (E–E) QoS provision, an EPS bearer and an external bearer are required. An external bearer is not under the control of mobile network operator. An EPS bearer consists of an evolved radio access bearer (E-RAB) and an S5/S8 bearer. An E-RAB includes a radio bearer and an S1 bearer. Figure 11.2 presents the realization of EPS bearers in the user plane when E-UTRAN access and GTP-based S5/S8 interfaces are deployed.

11.3.1 QoS for EPS Bearers

EPS differentiates two types of EPS bearers. Guaranteed bit rate (GBR) bearers are typically used for those services where it is better to block a service rather than degrade already admitted services. For example, VoIP, video streaming benefit from a constant bandwidth, hence GBR is needed to provide satisfactory user experience. An important characteristic of GBR bearer is that it is associated with a certain amount of bandwidth, independently of being utilized or not. The GBR always takes up resources over the radio link, even if no traffic is sent. Hence, in normal cases, the GBR bearer should not experience any packet loss.

Non-GBR bearers are used for those services, which normally do not require a constant fixed bandwidth, such as Web browsing, email, and chat. No transmission resources are reserved for non-GBR bearers.

An EPS bearer QoS profile however is broader than this categorization. It includes the parameters QoS class identifier (QCI), allocation and retention priority (ARP), GBR, and maximum bit rate (MBR), explained in the following.

For both non-GBR and GBR services, QoS parameters are the following:

- QCI: QCI is just a pointer to node-specific parameters, which define what packet forwarding treatment a particular bearer should receive (i.e., scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.). On the radio interfaces and the S1 interface, each protocol data unit is indirectly associated with one QCI via the bearer identifier carried in the header. The same applies to S5/S8 if GTP-based option is used. In GTP-U, the identifier is the tunnel endpoint identifier (TEID) conveyed in the GTP header. Table 11.1 summarizes the QoS requirements for different traffic types. Further details on standardized QCI characteristics can be found in TS 23.203 [2].
- ARP: ARP is used to indicate the priority for the allocation and retention of bearers. It includes:

  Priority level: Higher priority establishment and modification requests are preferred in situations where resources are scarce.

  Preemption capability: If true, then this bearer request could drop away another lower priority bearer.

Table 11.1 QoS requirements for different traffic types

Traffic type	Priority	Maximum delay (ms)	Maximum packet loss	Guaranteed bit rate
Control, signaling	1	100	10^{-6}	No
Voice call	2	100	10^{-2}	Yes
Real-time games	3	50	10^{-3}	Yes
Video call	4	150	10^{-3}	Yes
Premium video	5	300	10^{-6}	Yes
Interactive games	7	100	10^{-3}	No
Video, WWW, email, file transfer	6, 8, 9	300	10^{-6}	No

Preemption vulnerability: If true, then this bearer can be dropped by a higher priority bearer establishment/modification.

QoS parameters for GBR bearer are as follows:

- GBR: Is the minimum bit rate that an EPS bearer should get.
- MBR: The MBR limits the bit rate that can be expected to be provided by a GBR bearer (e.g., excess traffic may get discarded by a rate shaping function). Currently, MBR is set to the same value as GBR in EPC, that is, the instantaneous rate can never be greater than the GBR for GBR bearers.

Aggregate QoS parameters for nonguaranteed bearers (aggregate values) include:

- Per APN aggregate maximum bit rate (APN-AMBR): It defines the total bit rate that is allowed to be used by the user for all non-GBR bearers associated with a specific APN. It is enforced by P-GW in DL and the UE and P-GW in UL.
- Per UE aggregate maximum bit rate (UE-AMBR): The UE-AMBR limits the aggregate bit rate of all non-GBR bearers of the user. It is enforced by the eNodeB in UL and DL. The actually enforced rate is the minimum of the sum of all active APN's APN-AMBR and the subscribed UE-AMBR value.

The HSS defines, for each PDN subscription context, the "EPS-subscribed QoS profile," which contains the bearer-level QoS parameter values for the default bearer (QCI and ARP) and the subscribed APN-AMBR value.

The subscribed ARP shall be used to set the priority level of the EPS bearer parameter ARP for the default bearer. In addition, the subscribed ARP shall be applied by the P-GW for setting the ARP priority level of all dedicated EPS bearers of the same PDN connection unless a specific ARP priority-level setting is required (due to P-GW configuration or interaction with the Policy and Charging Rules Function (PCRF)). The preemption capability and the preemption vulnerability information for the default bearer are set based on Mobility Management Entity (MME) operator policy.

The mapping of services to GBR and non-GBR bearers is the choice of the operator and can be controlled with static rules in the Policy and Charging Enforcement Function (PCEF) or dynamic Policy and charging control (PCC) and QoS rules by the PCC framework.

11.3.2 QoS for Non-3GPP Access

In 2G/3G RANs, a more complicated QoS concept is used; hence, operators are not using many of the parameters in practice. That concept is referred to as the release 99 QoS. Its main characteristics are the following: 4 traffic classes, one mapped at the same time to a PDP context, and 13 attributes, such as bit rate, priority, error rate, max. delay, etc. For 2G/3G radio access to EPS via SGSN, the QoS attributes must be translated from release 99 QoS to EPS QoS parameters, when one-to-one mapping of PDP contexts to EPS bearers is performed. Mapping is described in Annex E of TS 23.401 [3].

11.3.3 QoS Enforcement in EPS

The following QoS treatment functions are deployed in the user plane of E-UTRAN and EPC. The maximum granularity of QoS control achieved by these functions is the EPS bearer granularity.

PCEF enforces traffic gating control for UL and DL based on policies. The mapping of packets to actual EPS bearer using TFTs is realized by UE for UL, P-GW (or S-GW if GTP is not deployed between the S-GW and P-GW) for DL.

Admission control (bearer establishment, modification) and preemption handling (congestion control, bearer drop) when resources are scarce, using the ARP to differentiate the handling of bearers, are executed by the eNodeB and P-GW (or S-GW).

Rate policing is enforced in the following way. eNodeB enforces the maximum rate for the aggregate of non-GBR bearers of the UE in UL and DL, based on the UE-AMBR UL and DL values. P-GW enforces the maximum rate for the aggregate of non-GBR bearers of the UE in UL and DL, using APN-AMBR values for UL and DL. eNodeB enforces GBR/MBR for GBR bearers in UL. P-GW (or S-GW) enforces GBR/MBR for GBR bearers in DL.

Queue management, scheduling, and configuration of L1/L2 protocols to enforce QCI characteristics, such as packet delay budget and packet loss in E-UTRAN, are enforced by eNodeB in UL and DL.

Mapping of QCI values to DSCP values in IP transport network between EPC elements is deployed in eNodeBs and S-GWs for IP transport between eNodeB and S-GW and/or S-GWs and P-GWs, for IP transport between S-GW and P-GW.

Finally, in order to enforce QoS on the path of EPS bearers in the transport network layer, routers and switches may deploy queue management and UL and DL scheduling.

11.3.4 Policy and Charging Control in 3GPP

Policy and charging control (PCC) provides QoS and charging control for operators. It provides a general, centralized framework to control the QoS procedures of heterogeneous access networks. It supports control of the user plane for IP Multimedia Subsystem (IMS) and non-IMS services. It solves the problem of lacking on-path QoS control in the case of non-GTP-based tunneling options. PCC can provide off-path control using the diameter protocol to any access network, which provides QoS bearers.

The “bearer” in PCC denotes an IP data path with desired QoS characteristics; hence, it is more generic than the EPS bearer and PDP context concept and is access network agnostic. Multiple service sessions can be transported over the same bearer. PCC enables service-aware

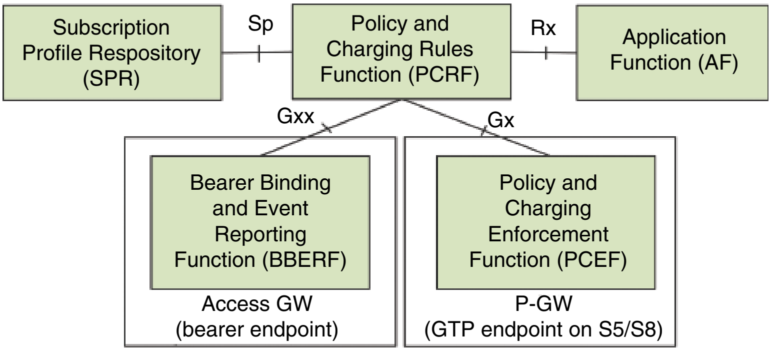
Subscription Profile Respository (SPR)
Sp
Policy and Charging Rules Function (PCRF)
Rx
Application Function (AF)
Gxx
Gx
Bearer Binding and Event Reporting Function (BBERF)
Access GW (bearer endpoint)
Policy and Charging Enforcement Function (PCEF)
P-GW (GTP endpoint on S5/S8)

Figure 11.3 Policy control part of the PCC architecture (nonroaming case).

QoS control, having higher granularity than the bearer-level QoS control provided by EPS bearers. PCC allows QoS control over wireless non-3GPP access networks, such as High-Rate Packet Data Services (HRPD) and Worldwide Interoperability for Microwave Access (WiMAX). For the fixed access, interworking with policy control has not come as far as for the wireless access. It supports policy control in roaming scenarios as well.

11.3.5 Policy Control Architecture

Figure 11.3 presents the policy control part of the PCC architecture. The elements related to policy control are the following.

The application function (AF) interacts with services that require dynamic PCC. For example, in the case of IMS, AF is the proxy-call session control function. The AF extracts session information (e.g., from service description protocol field) and sends the information to PCRF over the Rx interface. Such information includes, but is not limited to, IP filter information to identify the service dataflow for policy control and/or differentiated charging and media/application bandwidth requirements for QoS control.

The AF can also subscribe at the PCRF to the notification of events in the network, such as IP session termination or access technology-type change.

The subscription profile repository provides user-specific policies and data over the Sp interface.

The PCRF receives session information on Rx, subscriber-specific policies over Sp, and access network information over Gx or, if Bearer Binding and Event Reporting Function (BBERF) is used, then over Gxa/Gxc. Operators can configure policies in the PCRF, which must be applied to given services. Based on that information, it brings service session-level policy decisions and provides them to PCEF and optionally to BBERF. PCRF also sends event reports from PCEF and optionally the BBERF to the AF, for example, for video/audio codec adaptation.

The Policy and Charging Enforcement Function (PCEF) enforces policy decisions based on the PCC rules provided by PCRF over the Gx interface. It may perform measurements of user plane traffic (e.g., data volume, session duration). It reports the usage of resources for offline charging and interacts with online charging. PCEF is part of the P-GW in EPC.

The BBERF is required if no on-path QoS negotiation is available (by GTPv2-C), and DSMIPv6/IPsec or PMIP/IP GRE tunnels are used between the P-GW and the access GW of the UE, not capable of implementing QoS bearers for the services of the UEs. BBERF is responsible for bearer binding and QoS enforcement based on QoS rules provided by the PCRF over the Gxa/Gxc interface. Furthermore, it is responsible for event reporting toward the PCRF, about access network type, bearer state, and other information.

Policy control comprises gating control and QoS control. Gating control is applied by the PCEF on a per service dataflow basis.

11.3.5.1 PCC Rule and QoS Rule

The Policy and charging control rule (PCC rule) comprises the information that is required to enable the user plane detection of the policy control and proper charging for a service dataflow. The packets detected by applying the service dataflow template of a PCC rule are designated a service dataflow.

Two different types of PCC rules exist: dynamic PCC rules and predefined PCC rules. The dynamic PCC rules are provisioned by the PCRF via the Gx reference point. Predefined PCC rules are configured in the PCEF, and the PCRF only refers to them. While packet filters in a dynamic PCC rule are limited to the five-tuple of source and destination IP, source destination port, transport protocol, and some more header fields, the predefined PCC rules may use DPI filters for more fine-grained flow detection, charging control. Those filters are not standardized by 3GPP. TS 23.203 [2] contains more details on PCC rules.

In the case of off-path QoS control, PCRF needs to provide QoS information to the BBERF via the Gxa/Gxc reference points. QoS rule includes only a subset of PCC rule but with the same service-level granularity. It includes hence typically the filter information (SDF template, precedence) and QoS parameters (e.g., QCI, bit rates), but not charging-related information.

11.3.5.2 Network-Initiated and UE-Initiated QoS Control

For services provided by the access provider, such as IMS voice, mobile TV, etc., the network-initiated QoS control procedure is preferable. For services that are not known by the operator, UE-initiated QoS control is possible.

A network-initiated QoS control procedure may have the following steps:

1. Application-level signaling between the UE and the AF (e.g., SIP, SDP).
2. Session information provision from the AF to the PCRF (over the Rx reference point). In the case of IMS services, the SDP information is mapped to QoS information, such as bit rate and service type.
3. The PCRF may request subscriber-related information from the SPR.
4. PCRF makes policy decision based on session information, operator-defined service policies, and subscription information and generates PCC/QoS rules.
5. PCC rules are pushed by the PCRF to the PCEF and PCEF enforces the policy and charging rules, and conditionally, if BBERF is required, then QoS rules are pushed to the BBERF and installed.

A UE-initiated QoS control procedure may have the following steps:

1. Application-level signaling between the UE and the AF (e.g., SIP, SDP),
2. Session information provision from the AF to the PCRF (over the Rx reference point). In the case of IMS services, the SDP information is mapped to QoS information.
3. The PCRF may request subscriber-related information from the SPR.
4. The application on the UE side makes request through vendor-specific APIs for the access interface to request the needed QoS resources.
5. UE sends resource request, including QoS class and packet filters for the service. In E-UTRAN, that is called UE-requested bearer resource modification. In 2G/3G RAN, it is realized by secondary PDP context activation/modification.
6. If BBERF exists, it initiates PCRF interaction over Gxa/Gxc interface. If there is no BBERF, the PCEF initiates PCRF interaction over Gx interface.
7. The same as step 4 in network-initiated case.
8. The same as step 5 in network-initiated case.

11.4 Traffic Management in SDMNs

Dynamic, service dataflow-based policy control will be more and more needed by mobile network operators due to the increasing diversity of services and the related policy rules. Hence, in general, the QoS provisioning mechanisms specified by 3GPP, such as EPS bearers or PDP contexts and policy control by PCRF, should be kept also in case of virtualization of mobile core and transport network.

It is still uncertain whether GTP tunneling will be kept in SDN-based transport network segments. PCRF supports both on-path (GTP based) and off-path QoS configuration. Off-path QoS configuration is applicable over any transport network technology, which supports some sort of QoS bearers. Therefore, for the application of dynamic QoS enforcement in SDNs, two main challenges should be solved:

- The SDN transport should be able to provide QoS enforcement.
- Gx and Gxa/Gxc interfaces must be adapted for communicating PCC/QoS rules to the SDN controller, and the SDN controller shall be able to signal application-specific information to the PCRF through the Rx interface.

The service-chaining concept requires network function forwarding graphs both through virtual and traditional transport network segments. Operators need to be able to control logical and physical interconnections, configure traffic class conditioning and forwarding behaviors (capacity, priority, packet loss, delay, shaping, dropping, etc.), and map traffic flows to appropriate forwarding behaviors.

11.4.1 Open Networking Foundation

Open Networking Foundation (ONF) is a nonprofit industry alliance in charge of supporting the researches of software defined networking and of the standardization activities having OpenFlow (OF) in the main focus. OF is a completely open protocol that was originally published by Stanford

University researchers in [4] aiming to enable network developers to run experimental protocols in the university campus network. According to the Open Networking Foundation, SDN is an emerging network architecture that decouples the network control and forwarding functions.

ONF-based SDN architectures inherit a number of benefits for traffic management-related challenges of mobile and wireless environments, including their wireless access, mobile backhaul, and core networking segments. These benefits and potentials are listed in the following.

The paradigm of flow-based communication in SDN architectures fits well to provide efficient E–E communications in multiaccess environments, when different radio technologies, like 3G, 4G, WiMAX, Wi-Fi, etc., are simultaneously available for users. SDN is able to provide fine-grained user flow management aiming to improve traffic isolation, QoS/QoE provision, and service chaining.

In current networks, the decision logic and organization of network functions and protocols are distributed and multilayered, enabling the evolution of each layer, separately. That makes very complex the understanding and management of networks, when network providers want to fulfill E–E connectivity and QoS requirements over different access networks for different services. SDN tries to hide this complexity and introduces centralized control of network. Centralized control plane allows for efficient resource coordination of wireless access nodes, which makes possible to implement efficient intercell interference management techniques.

The fine-grained path management in SDN networks provides various optimization possibilities based on the individual service needs and independently from the configuration of the underlying routing infrastructure. In mobile and wireless environments, it is useful as users are frequently changing their network points of access, the used applications and services vary in bandwidth demands depending on the nature of the content to be transmitted, and considering that wireless coverages are providing a naturally changing environment.

Virtualization of network functions efficiently abstracts services from the physical infrastructure. Multitenancy permits each network slice to possess its own policy, independently of whether that slice is managed by a mobile virtual network operator, over-the-top service provider, virtual private enterprise network, governmental public network, traditional mobile operator, or any other business entity.

11.4.2 The OF Protocol

In SDN networking, the network operating system (NOS) is in charge of controlling the SDN-capable networking elements (SDN switches) in a centralized way. The NOS has southbound and northbound APIs that allow SDN switches and network applications to communicate over the common control plane provided by the NOS. In order to support multivendor environments for SDN switches and controllers, the southbound APIs must be standardized. OF protocol is one of the most known standards for the southbound API.

An OF switch contains multiple flow tables, which implement pipeline processing for incoming packets. Each table may contain flow entries. A flow entry contains a set of match fields for matching the packets, priority for matching precedence, a set of counters to track packets, and a set of instructions to apply. Furthermore, it includes timeouts to determine the maximum amount of time or idle time before flow is expired by the switch and cookie set and used by the controller as a group identifier of flow entries, enabling filtering queries for flow statistics, flow modification, or flow deletion.

An instruction either modifies pipeline processing by sending the packet to another (higher number) flow table or contains a list of a set of actions. The action set includes all actions accumulated while the packet is processed by the flow tables. The actions are executed when the packet exits the processing pipeline. Possible actions are the following: output a packet on a given port; enqueue the packet to a given queue; drop packet; rewrite packet fields, such as time to live, virtual local area network ID, and multiprotocol label switching label.

In regard to QoS provisioning, the enqueue action is the most relevant action. The "enqueue" action in OF version 1.0 was renamed to "set_queue" in version 1.3 [5]. Its main purpose is to map a flow to a queue; it also sets up simple queues.

QoS provisioning of OF-capable switches is still not enough developed. Currently, both OF version 1.4 and OpenFlow Management and Configuration Protocol (OF-Config 1.1.1) [6, 7] can set up queues using only two input parameters:

- Minimum rate: It specifies the guaranteed rate provided for the aggregate of flows mapped to a queue. The minimum rate is relevant when the incoming data rate of an egress port is higher than the maximum rate of the port.
- Maximum or peak rate: It is relevant when there is available bandwidth on the output port.

OF-config and OF protocols do not support hierarchical queueing disciplines, which are necessary to implement standard or other per hob behaviors (PHB) specified for DiffServ architecture.

The OF protocol supports two queueing disciplines, that is, hierarchical token bucket (HTB) and hierarchical fair-service queue (HFSC). These queueing disciplines have much more configuration possibilities than minimum rate and maximum rate, such as the maximum queue size for HTB or delay curves for real-time traffic in HFSC.

The advantages of queueing disciplines could be more leveraged if more queuing disciplines were available, the establishment of more than one level of QoS class hierarchies was possible, and more parameters of the queuing disciplines were allowed by the OF and OF-config specifications.

It is possible to build hierarchical queueing disciplines in switches using their administration tools and map flows to queues based on traffic control filters. For example, the DSCP value in IPv4/IPv6 headers or other packet headers and fields can be used to map packets to more complex queues.

The OF 1.4 has specified requirements for counters that could be set for flow tables, flow entries, ports, queues, etc. [5]. An OF controller may set meters in an OF switch to measure performance metrics related to flows, ports, queues, etc. It can set meter bands and appropriate actions if the actual measured metric falls into the meter band. Such actions could be dropped, realizing rate limiting or DSCP remarking for assigning the packet to a new behavior aggregate. However, it depends on the implementation of the OF switch, whether these functionalities are available.

11.4.3 Traffic Management and Offloading in Mobile Networks

One of the most straightforward use cases of ONF is traffic steering and path management that have received tremendous attention within the SDN community. Tools of smart traffic steering can be applied for advanced load balancing, load sharing, content filtering, policy control and enforcement, error recovery and redundancy, and, in general, any application that involves traffic flow operations and control. Putting all of these potential SDN applications into the context of mobile and wireless networks, we gather another set of potential use cases like traffic offloading and roaming support, content adaptation (e.g., adaptive streaming solutions), and mobile traffic optimization.

OF enables mobile Internet traffic to be dynamically and adaptively moved and removed in the mobile network based on a number of possible trigger criteria, such as individual or aggregate flow rate (such as per application or per user aggregation), aggregate flow number on a particular port or link, flow duration, number of UEs per cell, available bandwidth, IP address, type of application, device utilization rate, etc. All of these criteria can be defined either by the user or by the mobile operator. For example, the operator could measure network conditions and decide to offload mobile traffic in case of need. As a user-centric alternative, subscribers could opt in based on their preferred parameters and predefined policies, like (i) voice calls should never be offloaded and (ii) FTP download traffic should always be offloaded to Wi-Fi. In a more advanced use case, it could be envisioned that users travel in a multiaccess radio environment simultaneously connecting to multiple base stations. Network parameters such as congestion, QoS, and quality of experience (QoE) are measured, and triggering factors (e.g., a flow rate threshold) are set and changed dynamically by the mobile operator. For example, “If the flow is an FTP download, and the flow rate exceeds 100 kbps, hand over the flow from LTE to Wi-Fi.” As the example shows, distinct criteria and thresholds could be applied for different applications and therefore different flow types running on the same UE or on the terminals of different subscribers. Of course, thresholds could be based on the widest range of possible criteria like user/flow profile, location, service plan, etc.

11.5 ALTO in SDMNs

We call ALTO problem when someone is concerned with better-than-random peer selection, optimization of rendezvous service for applications fetching distributed content. Typical fields where the ALTO problem occurs are peer-to-peer networks, content distribution networks, and data centers.

In peer-to-peer networks, peers can exchange pieces of information in an incremental way until they obtain the entire content. When a peer has not a global view on the network, it may pick randomly a candidate peer, which may result in lower QoE.

CDNs distribute content and may cover large geographical areas. With the increasing demand for streaming video services, CDN servers/caches are deployed deeper in the network of Internet service providers, including mobile network operators. CDN operators elaborated different technologies to direct the end users to the best CDN server or in-network cache of operators for appropriate level of QoE for the users.

A third area for ALTO problem is related to cloud services. Cloud services run on top of data centers. Users should be served by the closest data center by an enough lightly loaded server. In case of virtual private clouds, the obtainment of proximity measures is more complicated because the service is provided through overlay networks; servers in the same virtual network may be located at different geographical locations.

Gurbani et al. [8] provide a good survey on existing solutions for the ALTO problem. ALTO solutions can be divided into two categories: (1) application-level techniques to estimate parameters of the underlying network topology and (2) layer cooperation. Techniques in (1) can be further divided into (i) end-system mechanisms for topology estimation, such as coordinates-based systems, path selection services, and link layer Internet maps, and (ii) operator-provided topological information services, such as P4P [9], oracle-based ISP–P2P collaboration [10], or ISP-driven informed path selection [11].

The authors of [8] argue that these techniques have limitations in terms of abstraction of network topology using application-layer techniques, for example, unable to detect overlay paths shorter than the direct path or accurately estimate multipath topologies, or do not measure all the relevant metrics for appropriate selection of the best endpoint. For example, round-trip times do not reveal information on throughput and packet loss. Furthermore, topology estimations may converge slowly to the result. Moreover, application-layer measurements induce additional network resource utilization.

Hence, there is need of cooperation between the application and network layer, where network operators should be able to provide network maps and cost maps representing distance-, performance-, and charging-related criteria.

11.5.1 The ALTO Protocol

A new protocol, that is, ALTO protocol, is on track to become a proposed IETF RFC specified by Alimi et al. [12] for interoperability between ALTO solutions of different vendors.

The two main information elements provided by ALTO service are the network map and the related cost maps. A network map consists of the definition of host groups but not the connectivity of host groups. The identifier of host groups is called provider-defined identifier (PID). A PID may denote, for example, a subnet, a set of subnets, a metropolitan area, a PoP, an autonomous system, or a set of autonomous systems.

A cost map defines one-way connections between the PIDs and assigns a cost value to each one-way connection. It also determines the metric type (e.g., routing cost) and the unit type (numerical or ordinal), furthermore the network map name and version, where the PIDs are defined.

ALTO protocol is based on HTTP and uses a RESTful interface between the ALTO client and server. The protocol encodes message bodies in JSON [13]. Several JSON media types are proposed in [12], which realize required and optional functions. Required functions are the information resource directory and network and cost map request and responses. Optional functions of ALTO service are, for example, filtered network and cost map queries, endpoint property queries, etc.

11.5.2 ALTO–SDN Use Case

Gurbani et al. proposed in [14] the application of ALTO service in the SDN application layer. They argue that the ALTO protocol is a well-defined and mature solution that provides powerful abstraction of network map and network state that can be leveraged by distributed services in SDNs. ALTO hides unnecessary detail of the underlying networks without unnecessarily constraining applications; hence, privacy of network information of network operators and content providers can be kept.

An important limitation of ALTO protocol is that it does not specify network information provision service. Creation of network and cost maps in the ALTO server should be automated and policy driven. There is ongoing work for distribution of link-state and TE information from BGP routers [15–17]. A similar approach should be used in the case of SDN networks,

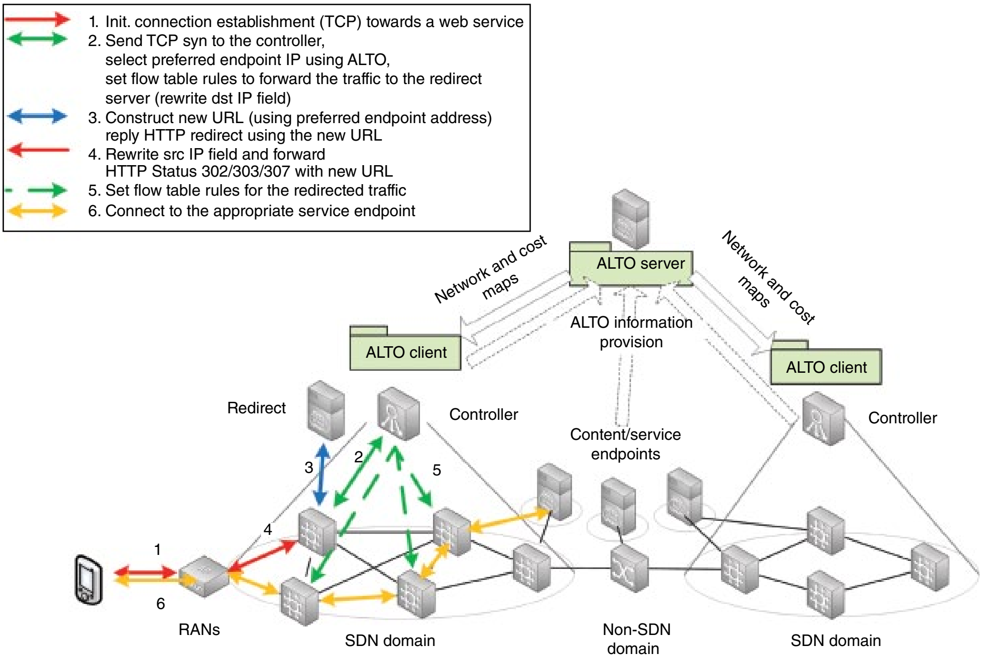
1. Init. connection establishment (TCP) towards a web service
2. Send TCP syn to the controller, select preferred endpoint IP using ALTO, set flow table rules to forward the traffic to the redirect server (rewrite dst IP field)
3. Construct new URL (using preferred endpoint address) reply HTTP redirect using the new URL
4. Rewrite src IP field and forward HTTP Status 302/303/307 with new URL
5. Set flow table rules for the redirected traffic
6. Connect to the appropriate service endpoint
ALTO server
Network and cost maps
Network and cost maps
ALTO client
ALTO client
ALTO information provision
Redirect
Controller
Controller
Content/service endpoints
1
2
3
4
5
6
RANs
SDN domain
Non-SDN domain
SDN domain

Figure 11.4 ALTO–SDN use case; HTTP-based video streaming scenario.

that is, the SDN controllers should be able to provide network information from which the ALTO server derives network and cost maps.

Xie et al. [18] prepared an IETF draft discussing possible use cases for the integration of ALTO service in SDNs. The benefits of the integration of ALTO network information service into SDNs are the following. ALTO becomes transparent for the end users or the service claimant entity (no deployment cost in the UE). Due to ALTO information, the ALTO client in the SDN controller can overwrite the initial peer selection decision of the service claimant entity (e.g., UE). Any flow can be dynamically selected for getting ALTO guidance, and SDN controller provides built-in redirection mechanisms with flow rewrite rules. Furthermore, SDN controllers are aware of the topology and state of served network areas and hence can provide abstract network and cost maps to the ALTO server.

Figure 11.4 illustrates the use case where ALTO guidance is used for better-than-random endpoint selection for HTTP-based video streaming service.

The SDN controller shall be notified about a new TCP connection establishment request by the edge SDN switch of the SDN domain. Since ALTO network and cost maps basically apply IP addresses, and not, for example, HTTP URIs, the IP and TCP header of TCP SYN message shall be used to decide whether this connection should get ALTO guidance or not. If yes, then the ALTO client shall find the appropriate network and cost maps for the service and shall determine the candidate IP addresses/PIDs for the service. If not already cached, it may request the appropriate maps from the server with target-independent query. Next, the ALTO client may, for example, calculate k-shortest paths for each cost type. That is followed by a multiattribute ranking procedure, to calculate the aggregated ranking of the endpoints.

After that, the ALTO client and SDN controller shall check resource availability for candidate paths to the best endpoint. If the E–E path crosses multiple SDN domains, this would require communication over the west–east interfaces interconnecting SDN controllers.

Then, the SDN controller shall install the necessary flow entries in its SDN domain and notify other SDN controllers on the path to do the same for this flow.

If the procedure does not find any path toward one of the endpoints, the TCP SYN should be dropped. If the service can support IP address rewriting, the controller should install rewrite the destination IP address downstream and the source IP address upstream.

Another option is that the TCP connection (and the HTTP communication on top of that) is redirected to a local HTTP redirect server. The related flow entries must only be kept until the HTTP redirect server redirects the source to the appropriate endpoint; hence, these are very short-lived flow entries.

The HTTP redirect server must be notified about the selected IP address and may resolve the DNS name to generate the new HTTP URI for the client. Then it can send the HTTP redirect message back to the client.

11.5.3 The ALTO–SDN Architecture

An important change in ALTO–SDN architecture compared to the original SDN architecture is that the selection of the preferred endpoint (decision making) is moved from the ALTO server to the ALTO client. Consequently, the ALTO server mainly is utilized as a pure network and cost map information service. From the proposed functions of ALTO client-to-server API [12], we realized information resource directory, network map, and cost map query services. The change in the concept was made due to the fact that it is better to implement communication-intensive SDN applications as an application module in the controller.

Another important functionality of the ALTO server is the automatic merging of network and cost map information coming from different sources (over ALTO server-to-network APIs), such as CDNs, BGP speakers, and SDN controllers. Currently, we are only focusing on network and cost map provision from one SDN controller. Figure 11.5 illustrates the main components of ALTO server.

The ALTO client is implemented as an application module in the SDN controller, as depicted in Figure 11.6. Its basic functionality is the query of network and cost maps from the ALTO service during the connection establishment phase of distributed services requiring ALTO guidance. It also stores locally in its cache the maps in order to reduce signaling. Additionally, it also provides ranking of endpoints based on the cost maps obtained from the ALTO server.

The SDN controller must know which service classes require ALTO service and ALTO-related policies of the operator must be provided. The proposed configuration XML schema includes the definition of service classes, which have a name (id); reachability information of servers (network addresses, port numbers), which specify the name of the related ALTO network map; the cost types to be considered for the service; and the main direction of the service (downlink, uplink, or both). If cost type is missing, then all cost maps should be considered in the ranking of service endpoints. Additionally, the reachability of ALTO server and redirect servers must be given. There is an additional field called PID mask. It is currently an IPv4 network mask, which defines the boundaries between subnets assigned to the same PIDs and represents the policies of the operator regarding the level of abstraction of the SDN network areas.

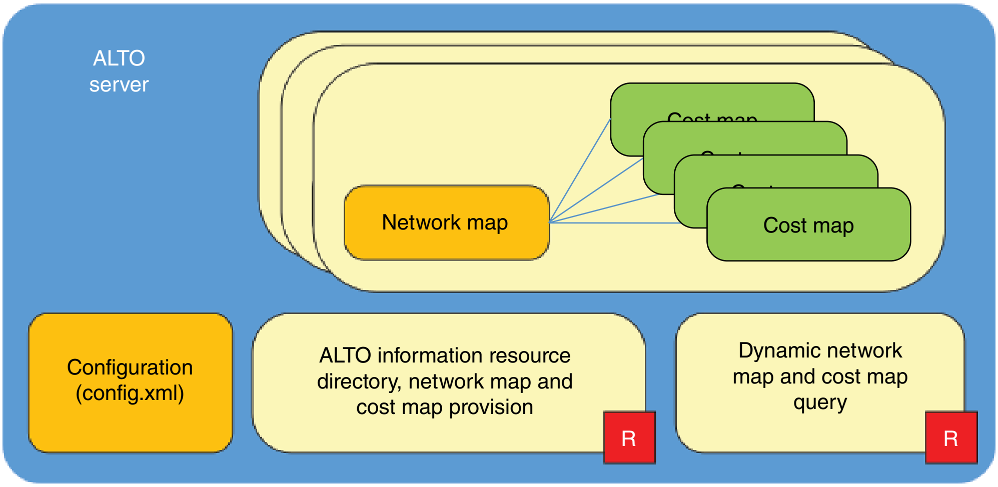
ALTO server
Network map
Cost map
Cost map
Configuration (config.xml)
ALTO information resource directory, network map and cost map provision
R
Dynamic network map and cost map query
R

Figure 11.5 ALTO server.

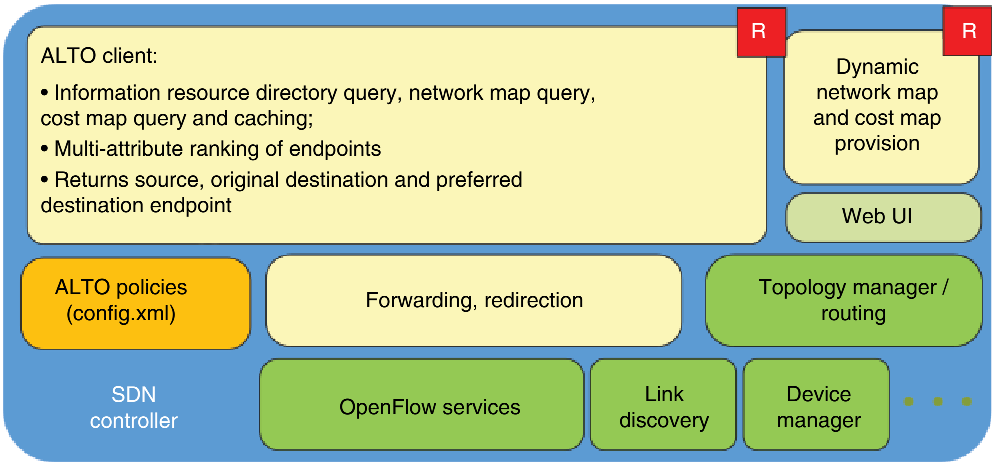
ALTO client:
• Information resource directory query, network map query, cost map query and caching;
• Multi-attribute ranking of endpoints
• Returns source, original destination and preferred destination endpoint
R
R
Dynamic network map and cost map provision
Web UI
ALTO policies (config.xml)
Forwarding, redirection
Topology manager / routing
SDN controller
OpenFlow services
Link discovery
Device manager
• • •

Figure 11.6 ALTO client in SDN controller.

11.5.4 Dynamic Network Information Provision

In our proposal, the ALTO server can request dynamically network information from the SDN controller. The SDN controller provides an up-to-date single-node network view over RESTful interface with JSON media type. An example for the JSON message is given in the following:

```
{"topology":{"10.0.0.1":{"10.0.0.2":{"num-routing":2, "num-
 delay":0}, "10.0.0.3":{"num-routing":6, "num-delay":0},
 "10.0.0.4":{"num-routing":6, "num-delay":0}},
"10.0.0.2":{"10.0.0.1":{"num-routing":2, "num-
  delay":0},"10.0.0.3":{"num-routing":6, "num-
  delay":0},"10.0.0.4":{"num-routing":6, "num-delay":0}},
"10.0.0.3":{"10.0.0.1":{"num-routing":6, "num-
  delay":0},"10.0.0.2":{"num-routing":6, "num-
  delay":0},"10.0.0.4":{"num-routing":2, "num-delay":0}},
"10.0.0.4":{"10.0.0.1":{"num-routing":6, "num-
  delay":0},"10.0.0.2":{"num-routing":6, "num-
  delay":0},"10.0.0.3":{"num-routing":2, "num-delay":0}}},
"pidMask":"255.255.255.255",
"mapName":"my-default-network-map"}
```

The proposed structure is similar to the ALTO network map; it defines abstracted one-way links between subnets, which will be assigned to PIDs by the ALTO server. The network mask for the subnets is given by “pidMask.” The “mapName” gives the network map and associated cost maps, which should be updated.

The cost maps are created using the different distance metrics given for each one-way abstract link in the topology structure. Num-routing cost is a metric proportional with the number of switch hops. We also can measure the historical load of the abstracted links by monitoring the increments in switch port statistics (in terms of received, sent, or dropped bytes or packets) and deriving distance measures for the abstract link between subnets. Hierarchical clustering applies numerous distance measures, which could be utilized in this scenario, for example, the minimum, maximum, unweighted, or weighted average of the distances between all pairs of hosts in the source and destination subnets.

11.6 Conclusions

This chapter has discussed the main building blocks of traffic management in mobile networks, that is, microscopic, macroscopic, improved content resource selection, application-supported traffic management, steering usage behavior, and extension of network resources.

Then an overview of QoS provisioning and dynamic policy control in 2G/3G packet-switched domain and EPC has been presented. The policy control functions realized by PCRF function are expected to be applicable also in SDMNs.

This was followed by a survey of the work of the ONF, mainly focusing on the QoS-related features of OF protocol, and an important traffic management-related use case defined by ONF.

Following that, an ALTO–SDN solution has been presented, showing the feasibility of SDN-based traffic management.

References

[1] Bokor, L., Faigl, Z., Eisl, J., Windisch, G. (2011) Components for Integrated Traffic Management—The MEVICO Approach, Infocommunications Journal, vol. 3, no. 4, pp. 38–49.

[2] 3GPP (2013) Policy and Charging Control Architecture (Release 12), TS 23.203. http://www.3gpp.org/DynaReport/23203.htm. Accessed February 16, 2015.

[3] 3GPP (2013) General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 12), TS 23.401. http://www.3gpp.org/DynaReport/23401.htm. Accessed February 16, 2015.

[4] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008) OpenFlow: Enabling Innovation in Campus Networks, SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74.

[5] Open Networking Foundation (2013) OpenFlow Switch Specification, version 1.3.2. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.2.pdf. Accessed February 16, 2015.

[6] Open Networking Foundation (2013) OpenFlow Management and Configuration Protocol (OF-Config 1.1.1), version 1.1.1. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow-config/of-config-1-1-1.pdf. Accessed February 16, 2015.

[7] Open Networking Foundation (2013) *Solution Brief: OpenFlow™-Enabled Mobile and Wireless Networks*, Wireless & Mobile Working Group. https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-wireless-mobile.pdf. Accessed February 16, 2015.

[8] Gurbani, V., Hilt, V., Rimac, I., Tomsu, M., and Marocco, E. (2009) A survey of research on the application-layer traffic optimization problem and the need for layer cooperation, IEEE Communications Magazine, vol. 47, no. 8, pp. 107–112.

[9] Xie, H., Yang, Y. R., Krishnamurthy, A., Liu, Y. G., and Silberschatz, A. (2008) P4P: Provider Portal for Applications, in Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication (SIGCOMM ’08), Seattle, WA, USA, August 17–22, 2008, pp. 351–362.

[10] Aggarwal, V., Feldmann, A., and Scheideler, C. (2007) Can ISPS and P2P Users Cooperate for Improved Performance?, SIGCOMM Computer Communication Review, vol. 37, no. 3, pp. 29–40.

[11] Saucez, D., Donnet, B., and Bonaventure, O. (2007) Implementation and Preliminary Evaluation of an ISP-driven Informed Path Selection, in Proceedings of the 2007 ACM CoNEXT Conference, New York, USA, pp. 45:1–45:2.

[12] Alimi, R., Penno, R., and Yang, Y. (Eds.) (2014) ALTO Protocol, IETF Draft, draft-ietf-alto-protocol-27, March 5, 2014. https://tools.ietf.org/html/draft-ietf-alto-protocol-27. Accessed February 16, 2015.

[13] Crockford, D. (2006) The Application/JSON Media Type for JavaScript Object Notation (JSON), IETF RFC 4627, July 2006. http://www.ietf.org/rfc/rfc4627.txt. Accessed February 16, 2015.

[14] Gurbani, V., Scharf, M., Lakshman, T. V., Hilt, V., and Marocco, E. (2012) Abstracting Network State in Software Defined Networks (SDN) for Rendezvous Services, in Proceedings of the IEEE International Conference on Communications (ICC), 2012, Ottawa, Canada, pp. 6627–6632.

[15] Medved, J., Ward, D., Peterson, J., Woundy, R., and McDysan, D. (2011) ALTO Network-Server and Server-Server APIs, IETF Draft, draft-medvedalto-svr-apis-00, March 2011. https://tools.ietf.org/html/draft-medved-alto-svr-apis-00. Accessed February 16, 2015.

[16] Racz, P., and Despotovic, Z. (2009) An ALTO Service Based on BGP Routing Information, IETF Draft, draft-racz-bgp-based-alto-service-00, June 2009. http://www.ietf.org/archive/id/draft-racz-bgp-based-alto-service-00.txt. Accessed February 16, 2015.

[17] Gredler, H., Medved, J., Previdi, S., Farrel, A., and Ray, S. (2013) North-Bound Distribution of Link-State and TE Information Using BGP, IETF Draft, draft-ietf-idr-ls-distribution-04, November 2013. https://tools.ietf.org/html/draft-ietf-idr-ls-distribution-04. Accessed February 16, 2015.

[18] Xie, H., Tsou, T., Lopez, D., Yin, H. (2012) Use Cases for ALTO with Software Defined Networks, IETF Draft, draft-xie-alto-sdn-use-cases-01, June 27, 2012. https://tools.ietf.org/html/draft-xie-alto-sdn-use-cases-00. Accessed February 16, 2015.