End-to-end QoS Architecture for 4G Scenarios

Susana Sargento[1], Rui Prior[2], Filipe Sousa[3], Pedro Gonçalves[1], Janusz Gozdecki[4], Diogo Gomes[1], Emiliano Guainella[5], Antonio Cuevas[6], Wojciech Dziunikowski[4] and Francisco Fontes[7]

[1] Universidade de Aveiro, Instituto de Telecomunicações, Portugal
[2] DCC & LIACC, University of Porto, Portugal, [3] INESC Porto, Portugal
[4]Department of Telecommunications, AGH University of Science and Technology, Poland
[5]Università di Roma "La Sapienza", Dipartimento di Informatica e Sistemistica, Italy
[6]Universidad Carlos III de Madrid, Dpto. Ing Telemática, Spain, [7]Portugal Telecom Inovação, Portugal

Abstract— **This paper describes the QoS architecture and the corresponding QoS signalling protocols to be developed inside the IST project Daidalos. We address the main results achieved in terms of the definition of the QoS components and its interfaces, the description of the application and network services, definition of the signalling scenarios for the integration of the QoS signalling with the application signalling and with mobility approaches, and specification of the intra- and inter-domain QoS control approaches. We also describe the QoS management of the system, through the Policy–based Management System, and a Real-time Network Monitoring system able to aid in admission control with the results of active and passive measurements. All the elements, interfaces and functionalities take into account multicast services and inherent broadcast networks.**

***Index Terms*—QoS, signalling, multicast, broadcast, inter-domain**

I. INTRODUCTION

The DAIDALOS project [1] aims at seamlessly integrating heterogeneous network technologies that allow network operators and service providers to offer new and profitable services (voice, data, multimedia). The architecture integrates both wired and wireless technologies, with quality of service capabilities under a common authentication, authorization, accounting, auditing and charging (A4C) framework and in a secure communication environment.

The diversity of services and access technologies is expected to become an universal characteristic in communications. Providing mobility across domains using different access technologies in a seamless way is a major requirement for the next generation networks. The provision of seamless end-to-end QoS in such a demanding and heterogeneous scenario, requiring no perceived service degradation for the user when moving across different access technologies, is one of the main challenges in Daidalos.

This paper describes the Daidalos end-to-end QoS architecture for 4G scenarios. The architecture is composed by QoS elements able to perform admission control mechanisms, handle the negotiation of the QoS that will be achieved by each service and application, and implement the QoS guarantees negotiated, to legacy and multimedia, unicast and multicast/broadcast services. Beyond that, the architecture is also composed by a policy based management system that manages and configures the network elements through policies, and a monitoring platform that provides information for the admission control and the core resource management procedures. This architecture and the protocols associated support several types of mobility, including session mobility and inter-domain mobility.

This paper is organized as follows. Section II presents the network architecture, its elements and the service classes adopted. Sections III and IV describe, respectively, the real-time network monitoring and policy-based management systems. The approach for end-to-end QoS support, both in the access network, intra- and inter-domain is depicted in section V. Finally, broadcast and multicast extensions are described in section VI, and the main conclusions are addressed in section VII.

II. NETWORK ARCHITECTURE

Next generation communication systems aim to provide seamless mobility of users through networks with different access technologies and services. In this sense, the network needs to be capable of supporting technologies, ranging from cellular networks, such as Universal Mobile Terrestrial System (UMTS), to Broadcast networks, such as Digital Video Broadcast – Terrestrial (DVB-T). One of the Daidalos objectives is to support all these technologies under a single network architecture.

Figure 1 depicts the proposed QoS architecture that supports several access networks, each of them capable of handling several access technologies. The shown QoS architecture allows for different operators to work in a common environment, with support for access services and other transport and advanced services. All operators may have special contracts between each other and/or federation mechanisms, enabling a better integrated service to the end user. Differentiated Services (DiffServ) [2] is used to support QoS in the core network, achieving scalability and performance.

Other proposals for 4G architectures have been made, e.g. the ones presented in the projects MIND, AQUILA, etc. In broad terms, our architecture is more flexible, and presents a more comprehensive set of characteristics, such as: a fully integrated approach to IP-based communication with different types of applications and protocols (e.g. both legacy and SIP-based applications are supported), including adaptive applications, multicast and broadcast; the customization/optimization of the architecture according with the expected service mix to support; and the integrated support

of multiple QoS service models, according to the overall network configuration (defined by operator policies).

In the sub-section A we will describe the QoS elements that build the Daidalos QoS architecture. Sub-section B addresses the definition of the network service classes that will be considered.

A. QoS Elements

In Figure 1 several access networks are depicted, connected to a core network; each administrative domain is connected to other domains through edge routers (ER). In each access network, mobile terminals (MT), Laptops and PDAs, are connected to the network through access routers (AR). Each MT may incorporate a QoS client able to request QoS resources (and/or QoS services) to the network in an implicit or explicit way (this will be further specified in section V).

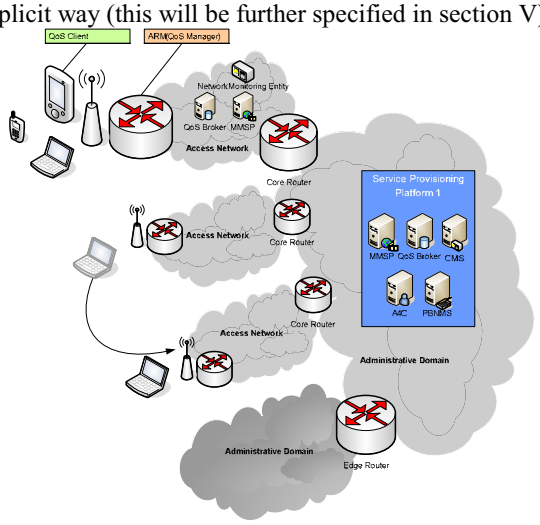

Figure 1: Daidalos QoS network architecture

The QoS Broker performs admission control and manages network resources. It also performs load balancing of users and sessions among the available networks (possibly with different access technologies) to optimize the usage of operator resources and maximize operator' income, by setting off network-initiated handovers. The QoS Brokers in the core network (CNQoSB) manage the core resources in terms of aggregates, and the communication with other administrative domains.

While basic QoS services are provided intrinsically by the Access Network (AN), more advanced services are supported by a Service Provision Platform (SPP) in the core network. In the AN, service proxies are deployed for efficient service provision. The MultiMedia Service Proxy (MMSP) controls the multimedia sessions. MMSP and QoS Broker in the Access Network (ANQoSB) can, together, provide the adequate network-level QoS to a multimedia stream, through the high level knowledge of active services and the available network resources. The QoS definitions at the domain level are provided by a Policy Based Network Management System (PBNMS), and then proxied by the ANQoSBs to the ARs in the different AN. For authentication and accounting purposes, an A4C server is also present in each domain.

The AR contains a set of advanced functions, which comprises connection tracking, per-application flow DiffServ Code Point (DSCP) marking, and the means to translate other QoS reservation mechanisms, such as Integrated Services (IntServ) [3] resource ReSerVation Protocol (RSVP) reservations, into DiffServ DSCP marking and QoS Broker requests. We refer to the entity supporting all these functions as the Advanced Router Mechanisms (ARM).

To aid in the admission control procedure performed by the QoS Brokers, this architecture also includes a real time network monitoring system, which comprises Network Monitoring Entities (NME) located in several points of the network, and a Central Monitoring System (CMS). The NMEs can perform passive and active probing of the network, and the CMS controls the monitoring process, processing the measurements, and propagating the measurement results to the QoS Brokers in the network and other entities (e.g, A4C server for charging and SLA conformance testing).

B. Network Service Classes

Each network QoS class ensures certain edge-to-edge QoS guarantees, described by parameters as delay, jitter, packet loss and bandwidth availability. Based on the QoS requirements of the Daidalos architecture [4], we propose to implement 4 network QoS service classes: conversational, transactional, streaming and best effort traffic. Performance parameters of the network service QoS classes are derived from ITU-T Y.1541 [5]. The defined service set can be treated as a subset of service classes defined in that recommendation.

Since the ANQoSB only has information on the network services to be delivered, it is required to map the application QoS parameters to network QoS parameters. This mapping can be made in the QoS client, ARM or in the MMSP, depending on the signalling strategy used. The network service is described by two parameters: the network service QoS class (where the class is specified by a set of QoS parameters), and the bandwidth to be reserved. The definition of the network service classes is conformant with DiffServ network architecture.

To enable fast QoS and session setup for specific services and users, beyond the services defined and negotiated by the user, we also introduce the concept of the "well-known services". These are the set of network services characterized by pre-defined parameters that are offered by the specified network operator. These services do not accept negotiation procedures, since the granularity is the one already pre-defined by the operator.

III. MONITORING SYSTEM INTEGRATION

The resources reserved for each flow may take into consideration statistical multiplexing effects. Since the traffic profile of the flows may be unpredictable, to improve resource usage efficiency, making use of the statistical multiplexing gains, we propose to use a network monitoring system that is able to monitor the available resources in the network, using monitoring results for optimized admission decisions and to multiplex data streams. This monitoring system is very useful in the establishment of QoS services, and in the process of

validation of the contracted QoS (SLAs) with the operator (it is also used for accounting purposes).

We proposed an architecture that can fulfil these previous requirements, composed by a CMS and several NMEs scattered across the network. The CMS is the controlling and aggregator element for the whole monitoring system. This unit interfaces with other entities such as QoS Brokers and A4C. The interface with the QoS Brokers is used to fetch the network QoS information for traffic admission control. The interface with the A4C is to perform SLA validation and to exchange accounting information.

The NMEs are located at strategic points in the network and may perform passive or/and active measurements. Periodically, measurements information is sent to the CMS using the IPFIX (Internet Protocol Flow Information eXport) [6] protocol. In section V we detail the integration of the monitoring platform in the QoS architecture.

IV. PBNM System Integration

The promises of policy management are diverse and powerful, but are often conceptualized as a single and simple means to control the network. The main goals of PBNM in Daidalos are the enabling of the administrator to provide an easy integrated (re-)configuration of the network and to deal with problems that may occur in the network, in a proactive or reactive way. The final goal of PBNM system is to manage QoS aspects of SLA and help to provide end-to-end QoS.

At first, we are only concerned in managing network QoS aspects. We consider that the relationship between QoS Broker and ARM, and between the CMS and the NMEs (possibly located in the ARs) follow a PDP (Policy Decision Point) / PEP (Policy Enforcement Point) [7] approach, where ARM and the NMEs are the QoS PEPs, and the QoS Brokers and CMS are the PDPs. Please refer to Figure 2 for an illustration of this relationship. The QoS Broker and the CMS will be configured by the PBNM entity.

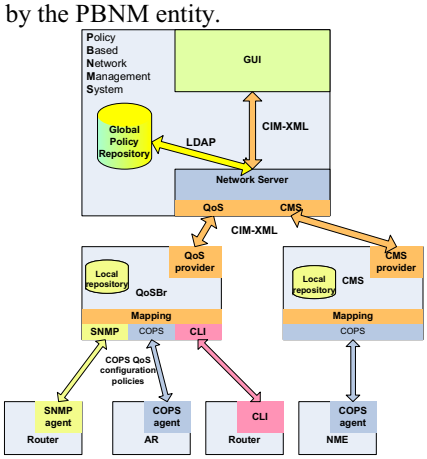

Figure 2: PBNM architecture

QoS manager in the ARM will apply the QoS decisions at device level, through Traffic Control (TC). TC matches closely the structure of the IETF's DiffServ QoS PIB (Policy Information Base) [9]. This close match will help to bridge the gap between high level policies and low level device configuration. IETF COPS-PR [8] protocol is designed to transport PIB information.

The QoS Broker has an internal policy repository used to keep policy information in order to allow an autonomous network operation without the continuous PBNM system querying. After a policy redefinition process, the PBNM system performs an unsolicited policy definition in all the QoS Brokers belonging to its network. After such policy redefinition, the QoS Broker changes its resource management behaviour accordingly. Similarly to the QoS Broker, the CMS will receive policy information from PBNM system, concerning measurements scheduling and test definition.

The PBNM entity is composed by a policy server, a GUI (Graphical User Interface) and a network server. Network administrator creates new policy rules in GUI. These policy rules are kept in a LDAP (Lightweight Directory Access Protocol) [10] repository, and are then distributed to QoS Broker(s) and/or CMS(s). The network server module is the network operational part of the PBNM entity: it receives configuration requests from the network elements and performs unsolicited policy definition to the network elements.

V. Protocol Design for End-to-End QoS Control

In order to provide end-to-end QoS to the application flows, enough resources must be available along the entire flow path. In the most demanding scenario, where the mobile terminals communicating are attached to different access domains, this path comprises (1) the access networks of both terminals, (2) the core networks of the access domains where the access networks belong and (3) the inter-domain path, consisting of all the transit domains traversed by the flows. Daidalos handles QoS control in all these segments with a scalable approach based on DiffServ with resource control: resource management at the core is performed on a per-aggregate basis and based on information from a monitoring platform, whereas in the wireless link, where (radio) resources are scarce, per-flow QoS control is applied. All the signaling strategies that will be presented below are based on this architecture, and therefore, are based on the QoS Broker concept for resource reservation. New signaling methodologies are being thought for the support of QoS in mobility environments, like the ones being defined by the NSIS WG. These signaling approaches can be used in this architecture for the signaling in the access network. This is a topic for further work.

The next sub-sections describe resource management at flow, intra-domain and inter-domain levels.

A. QoS Reservation Strategies

In order to support all the required applications and operator business cases, the network architecture is very flexible regarding the initiator of the QoS requests, which may be the MT, the ARM, the MMSP, or even an application server. This flexibility leads to different scenarios for the integration of the application setup and negotiation signalling and the network QoS signalling.

Figure 3 illustrates a simplified example of a multimedia session initiation using SIP (Session Initiation Protocol) [11]. Notice that, although SIP is used in this case, this scenario works with different signalling protocols. The protocol used

for the communication with QoS Brokers is the Common Open Policy Service (COPS).

When receiving the INVITE message with an initial offer of QoS configurations, MMSP1 queries ANQoSB in the caller side on the availability of the service to the user in face of his profile (Network View of User Profile - NVUP) and the current AN usage. If the service is authorized, the INVITE is forwarded to MMSP2 (notice that if the callee was roaming, the message would go first to its home MMSP). The callee matches these QoS configurations to those it supports and generates a counter-offer, included in the 200 OK. On receiving this message, both proxies issue requests to the respective ANQoSBs, filtering the QoS configurations in face of those allowed by the amount of network resources provided. The ACK contains the final configuration that will be used; if necessary, MMSP2 adjusts (lowers) the reservation. Accounting processes are initiated in the A4C allowing for transport- or service-based charging.

Another approach is to trigger QoS requests directly through the terminal. In this case, the requests are not made directly to the QoS Broker in order not to expose it to non-trusted entities (the mobile terminals), but proxied by the AR. Apart from this small difference, the resource reservation process is very similar. This approach may also be used to support legacy applications, using a middleware in the terminal that performs the reservations. Alternatively, the responsibility of QoS triggering may be delegated to the ARM that will interpret the messages issued by the terminals and perform the most suited QoS reservation.

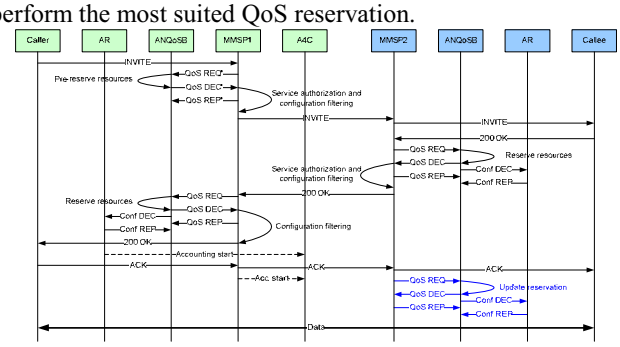

Figure 3: Multimedia service setup – QoS MMSP trigger

Mobility plays a central role in Daidalos, and the requirement for seamless handovers is probably the most demanding one in terms of timing. Handovers may be performed between different technologies; therefore handover signalling is performed at layer 3. The handover needs to be negotiated between the ANQoSBs in the old and new networks, and the NVUP along with information on the set of active sessions, is pushed to the ANQoSB of the prospective network. During handover, the packets are duplicated (bicasted) in the AR of the old network and sent also through the router in the new AN [12]. In order to take advantage of each access technology, handovers are integrated with session renegotiation. Information on the need to perform service degrading or the possibility of service improvement provided by handover signalling is used as a trigger for session renegotiation, regardless of the application protocol. Renegotiation for QoS improvement poses no problem, since the larger reservation is activated only after the handover, but in case of service degrading, the renegotiation must finish before the bicasting process starts, otherwise more traffic will be sent to the new network than it can handle. Most handovers, however, do not imply session renegotiation.

Inter-domain mobility follows a slightly different procedure. Briefly, both authorization taking into account service (A4C) and resources (QoS check) authorization are coupled, and performed through communication between A4C. Moreover, context transfer technique is used to transfer the information related to the security associations.

Daidalos also includes layer 2 QoS support, according to each access technology, for resources optimization. Both in session setup and mobility procedures the check for layer 2 resources is coordinated with the layer 3 ones, through the introduction of a QoS abstraction layer. This process is out of the scope of this paper.

B. Intra-domain QoS Control

The intra-domain QoS control covers QoS resource management for an administrative domain from the user terminal to the ER. The main requirements for the intra-domain QoS architecture are: 1) scalability of the signalling within the administrative domain; 2) flexibility (easy to manage); 3) efficiency in the usage of network resources; and 4) support for the mobility of users.

We consider the intra-domain architecture to be hierarchical: it is required to assure per-flow admission control and end-to-end QoS guarantees, but the traffic in the core needs to be aggregated. With this assumption, the per-flow end-to-end signalling can be transparent for a core part of the operator network and for inter-domain signalling. In this approach, the ANQoSBs must maintain maps of resources between their own sub-domain and all the other access sub-domains within the same administrative domain. These maps should be updated by means of information exchanged with the CNQoSB. The verification that enough resources are available in an end-to-end connection between two terminals within the same administrative domain for admission control purposes is split into 3 parts: (1) resource checking in the access sub-domain of the caller, (2) resource checking in the (core) aggregate between the sub-domain routers of the access sub-domain where the caller and the callee are attached and (3) resource checking in the access sub-domain of the callee. The CNQoSB is responsible for managing aggregated traffic flows. For each access sub-domain, the CNQoSB periodically informs the correspondent ANQoSB about the core network links between that access sub-domain and all the others for each network transport service. For this purpose, signalling information exchanged between an ANQoSB and the CNQoSB is used to inform the ANQoSB of the resources availability (or unavailability) in the core for particular classes, and on the paths between particular sub-domains. On the other hand, some return information might be sent from the ANQoSB to the CNQoSB in order to perform core reconfigurations when required.

Figure 4 depicts the resource management process in the core. The CNQoSBs reconfigure the bandwidth reserved for the aggregates on the basis of measurements and in response to requests sent by ANQoSBs. The CMS periodically sends

monitoring results including the bandwidth occupied per class, the mean/maximum packet delay and loss in a class. With this information, the CNQoSB has information on the congestion status of each class, and can reconfigure its routers if required. This measurement information is usually used for long term reconfigurations, e.g., as an impact of policies applied. Notice that the core reconfigurations can also be performed upon the request of an ANQoSB, when the connection between its AN and the core requires more bandwidth: this minimizes the amount of signalling information exchanged.

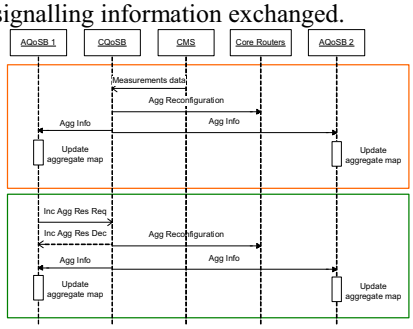

Figure 4: Resource management in the core network

C. *Inter-domain QoS Control*

Since the traditional approaches to inter-domain QoS of over provisioning or static DiffServ configurations cannot provide any guarantees regarding end-to-end QoS, they are not enough for Daidalos. Our approach is based on 3 main pieces: (1) a set of well-known traffic services globally supported by all operators, (2) the existence of SLA between adjacent domains and (3) an inter-domain routing protocol capable or propagating QoS information.

The SLAs contain Service Level Specifications (SLS) for sets of aggregates corresponding to (ingress point, egress point, service class) triplets. Management of aggregates is performed internally within each (transit) domain by the respective CNQoSB, which must ensure that enough resources are assigned to each aggregate in order to comply with the established SLS contracts.

Currently, BGP (Border Gateway Protocol) [13] is the most common protocol for inter-domain routing. In order to convey QoS information, we extended it by adding an optional and transitive Path Attribute to the UPDATE messages, the QOS_INFO (related work may be found in [14]). This attribute contains the following information: (1) allocated bandwidth for each well-known service class (minimum along the path); (2) expectable delay (summed along the path); congestion alarm level (maximum along the path) for each class (0 – idle or no congestion; 1 – very light congestion; 2 – medium congestion; 3 – serious congestion).

These values are updated by the BGP-speaking routers at each transit domain. The information on delay and reserved bandwidth is used to select the route, while the alarm levels are used to eliminate congested routes from the set of choices. The information on inter-domain routes must be retrieved by CNQoSB (Figure 5) in order to manage core resources; this task is performed by a BGP module installed in the CNQoSBs, which are, therefore, iBGP speakers. The QoS information to be propagated by the BGP routers is configured and updated by the CNQoSB in a similar way to the other router parameters. When a route is selected, the edge routers propagate it to their upstream peers with an updated QOS_INFO attribute. CNQoSB also send information on the inter-domain routes to their AN counterparts, which use it for admission control purposes, similarly to the information on core aggregates.

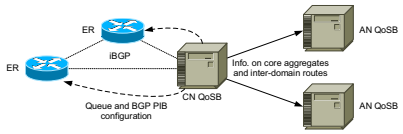

Figure 5 : Inter-domain communications

VI. SUPPORT OF MULTICAST AND BROADCAST

This sub-section describes the extensions to the Daidalos QoS framework in order to support Broadcast networks (i.e. ETSI DVB, 3GPP UMTS MBMS – Multimedia Broadcast Multicast Service, etc.) and IP multicast. As previously referred, the ANQoSB maintains information of its own access sub-domain and information on aggregate resources for each QoS class to the neighbouring networks (usually the CN).

When considering a multicast flow within the AN, this flow is handled (admission control, congestion control, etc.) with mechanisms dependent on the technology. However, our purpose is to assure the respect of QoS constraints to a multicast flow independent of the technology. In order to join a multicast group, every router in the access domain receiving a multicast join message (in the Daidalos project, the referenced multicast protocol is PIM-SSM – Protocol Independent Multicast - Source Specific Multicast [15]) must explicitly send a QoS request to the ANQoSB (see Figure 6). The ANQoSB might then respond to the router with a decision stating if it is possible or not to join the multicast group. From this request, the ANQoSB will know which routers in its domain it is required to include into the multicast group. Notice that the entities involved are the same as in unicast reservation, and the messages include the unicast ones plus additional messages related to multicast subscription process, coupled to the overall resource reservation mechanisms. We should take in consideration that all this is possible because the ANQoSB has the complete state of the various multicast groups subscriptions in each router, as well as the information on the network architecture and multicast rendezvous points.

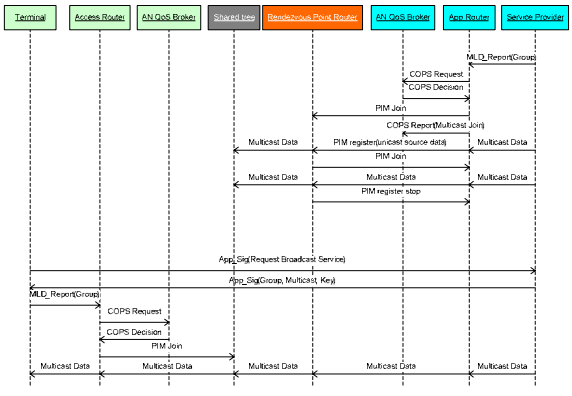

Figure 6: Session setup for multicast services

One of the major challenges of Daidalos is the need to support Unidirectional Broadcast Technologies such as DVB-T/S/H, and specially to provide QoS to services made available on top of these technologies. The proposed solution for the integration of these Broadcast technologies assumes availability of an interaction network through which the terminal might establish an IP over IP tunnel to the Broadcast Network AR. This tunnel will be used as an upstream channel for the broadcast download channel. At the Broadcast AR, a tunnel broker encapsulates the IP over IP tunnel and the broadcast channel into a virtual interface. With this virtual interface, the broadcast network can be viewed as any other access technology, to which all the mentioned mechanisms apply.

Since violating a QoS contract for a multicast flow means violating the QoS contracts with all the members of the multicast group, the respect of end-to-end QoS constraints in an inter-domain environment is a very challenging task. For this reason, a solution for an inter-domain QoS-aware multicast routing protocol is being studied. The main idea behind the protocol is to make the various QoS elements be active members of the multicast inter-domain QoS routing process: this can be achieved with the introduction of an intermediate entity, called Multicast Entity (ME), that if present in each domain can verify and choose, among a limited set of available paths, the one that have the best characteristics.

VII. CONCLUSIONS

This paper presented the QoS architecture being implemented inside the Daidalos project. This architecture is able to provide end-to-end QoS (in a heterogeneous mobile environment) for many types of services and applications, legacy and multimedia, unicast and multicast, with optimized network resource usage and network configuration. We addressed the specification of the QoS components and its interfaces, application and network services, approaches for intra- and inter-domain QoS control, and signalling scenarios for the integration of the QoS signalling with the application signalling and with mobility. All the elements, interfaces and functionalities described took into account multicast services and inherent broadcast networks.

ACKNOWLEDGMENT

The work presented in this paper was partially funded by the EU project IST-2002-506997 “Daidalos” [1].

REFERENCES

[1] Daidalos IST Project: Daidalos: “Designing Advanced Interfaces for the Delivery and Administration of Location independent Optimised personal Services”. (FP6-2002-IST-1-506997). http://www.ist.daidalos.org.

[2] S. Blake (ed) et al., *An Architecture for Differentiated Services*, IETF RFC 2475, Dec. 1998.

[3] R. Braden et al., *Integrated Services in the Internet Architecture: an Overview*, RFC 1633, June 1994.

[4] S. Sargento et al., *QoS Architecture and Protocol Design Specification*, Deliverable 321, Daidalos IST-2202-506997, Aug. 2004.

[5] ITU-T Recommendation Y.1541, *Network performance objectives for IP-based services*, May 2002.

[6] B. Claise, *IPFIX Protocol Specification,* draft-ietf-ipfix-protocol-05.txt, Aug. 2004.

[7] R. Yavatkar et al., *A Framework for Policy-Based Admission Control*, RFC2753, Jan. 2000.

[8] K. Chan et al., *COPS Usage for Policy Provisioning (COPS-PR),* IETF RFC 3084, March 2001.

[9] K. Chan et al., *Differentiated Services Quality of Service Policy Information Base,* IETF RFC 3317, March 2003.

[10] M. Wahl et al., *Lightweight Directory Access Protocol (v3): Technical Specification*, RFC3377, Sep. 2002.

[11] J. Rosenberg et al., SIP: Session Initiation Protocol, IETF RFC 3261, June 2002.

[12] V. Marques et al., *An IP-Based QoS Architecture for 4G Operator Scenarios*, IEEE Wireless Communicat., June 2003.

[13] Y. Rekhter et al., *A Border Gateway Protocol 4 (BGP-4)*, IETF Internet draft, draft-ietf-idr- bgp4-23.txt, 2004.

[14] G. Cristallo and C. Jacquenet: *Providing Quality of Service Indication by the BGP-4 Protocol: the QOS_NLRI attribute*, IETF Internet draft, draft-jacquenet-qos-nlri-05, 2003.

[15] PIM WG., PIM, Sparse Mode Protocol: Specification, IETF Draft, draft-ietf-pim-sm-v2-new-08.txt, 2004.