WiMAX QoS – Dynamic Service Flow Management

Nuno Rodrigues†, Rui Rocha¥
†Instituto Superior Técnico - TagusPark, Av. Prof. Dr. Cavaco Silva, 2744-016 Porto Salvo, Portugal
e-mail: nuno.rodrigues@tagus.ist.utl.pt
¥ Instituto de Telecomunicações, Av. Rovisco Pais 1, 1049-001 Lisboa, Portugal
email: rui.rocha@lx.it.pt

Abstract — **Providing Quality of Service (QoS) to clients from the access to the core network is possible with an 802.16 based access network. For this purpose, it is proposed the use of the Session Initiation Protocol (SIP) for signalling of client's QoS requirements. These requirements are processed by a modified SIP Proxy and sent to a Broker in the access network. This broker dynamically provisions connection requests from clients and, if necessary, communicates with the core Broker, so that a mapping between QoS paradigms of both networks is accomplished. This mapping allows that QoS characteristics are maintained from the access to the core network. Performance tests show that dynamically provisioning connections in the access network can be accomplished in a time-frame smaller than 100 ms. This time-frame is a reasonable price to pay for dynamic configuration of QoS-enabled connections for the access network.**

Keywords – WiMAX, Quality of Service, Dynamic Management

I. INTRODUCTION

A WiMAX system is able to provide internet access to users in remote communities. However, as WiMAX uses an air interface, resources tend to be scarce, which leads to QoS differentiation right from the access network.

The main purpose of this paper is to give an overview of a system with the capability to dynamically control QoS-enabled networks. The access network is based on the 802.16d standard [1], while the core network is based on the IP-DiffServ paradigm. For connection setup, users need to use the SIP protocol [2]. The messages exchanged carry the client's QoS requirements and are processed by a modified SIP Proxy. This proxy extracts the relevant information from the SIP/SDP [3] messages and forwards requests to a QoS Broker. This scheme allows dynamic establishment of QoS-enabled connections in the access network. Additionally was introduced a mapping mechanism from the access to the core network, with the aim of preserving QoS requirements across networks. This process provides users the QoS they requested across domains.

There were considered two essential functions for QoS management: Network Element (NE) configuration and admission control. The former allows the configuration of the WiMAX Base Station, according to the requests from clients, while the latter uses defined policies to allow/deny access to QoS-enabled resources. The admission control function also considered a degradation model. This model enables the degradation of low-priority connections, offering high-priority connections the requested resources.

The rest of the paper is organized as follows. Section II introduces related work in the area of heterogeneous networks, giving an overview of some relevant work in the area. The next section will introduce the architecture of the system developed. Along with the architecture, the main components will be explained, outlining their main functions. In Section IV are discussed some implementation concerns that were essential to provide performance gains. Next will be presented the main performance results, along with the test scenario. Finally, some conclusions are drawn.

II. RELATED WORK

One of the main characteristics of the 802.16 standard [1],[4] is that it was standardized with embedded QoS support. This provides network operators the ability to make the distinction of traffic in the access network segment. This requires WiMAX specific solutions to provide control over resources in the air interface. However, the problem of quality of service is not circumscribed to the access network.

The heterogeneity of today's networks poses a challenge in terms of assuring that QoS requirements are assured in the access and also crossing domains. The challenge can be divided in two different components: protocol layering adaptation in the edge routers and the preservation of resource's characteristics over different domains.

Concerning the topic of heterogeneous networks and end-to-end QoS support, the WiMAX Extension to Isolated Research Data Networks (WEIRD) group [5] defined an architecture with this support.

WEIRD supports both signaling capable and legacy applications. The former uses SIP/SDP as a signaling protocol, while the latter have no SIP capabilities. In order to make resource reservation, they use the NSIS protocol, which allows resource reservation across domains.

In terms of the WiMAX network itself, there are also interesting solutions. In [6], the authors propose an architecture to provide multi-layer integrated QoS control, where the IP QoS architectures supported are IntServ and DiffServ. The architecture is clearly cross-layered and defines mappings from the 802.16d standard to the IntServ and DiffServ IP QoS architectures.

In [7], the authors propose a different cross-layered QoS architecture. The singularity in it is that it uses the IEEE 802.1p recommendation to classify packets. Besides this, it also introduces the Channel Adapter and SNR sniffer, which is responsible for the evaluation of propagation conditions. It allows the inspection of the wireless medium, providing information related to SNR, fading, etc.

The use of cross-layered architectures, combined with resource optimization in the WiMAX segment, plus concerns with the whole IP network, should provide a framework capable of providing the best of both worlds.

III. Architecture

The Architecture of the system is based on the components identified in Figure 1.

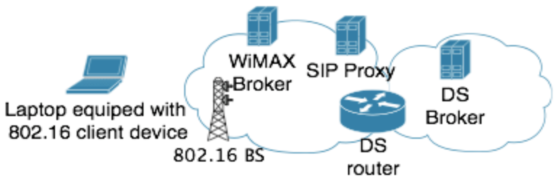

Figure 1 – System components overview.

Two domains are considered in the system's architecture: the WiMAX domain, working at the access network level, and the DiffServ domain at the core network level. Inside each of these domains is a QoS broker. This broker has the responsibility of configuring the NEs affected to its domain and assure admission control functionalities. The SIP Proxy, on the other hand, is responsible for mediating SIP communication between clients giving them access at the initiating connection phase and providing information about the corresponding hosts.

A. WiMAX QoS Broker

Figure 2 depicts the main functions of the WiMAX QoS Broker and the components of the access network.

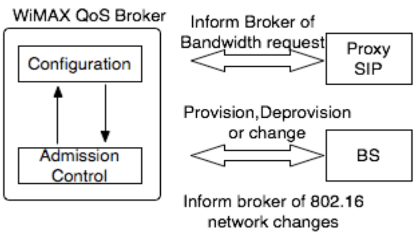

Figure 2 – Main broker functions

The main functions of this broker are configuration and admission control in the WiMAX domain.

Regarding the Base Station interface, the information that the Broker sends is Provisioning and de-provisioning of Service Flows, Service Classes and Classifying rules. What it receives from Base Station is information about clients joining and leaving the network. This allows the broker to provision connections to clients that enter the network and remove unused resources when they leave. In a fixed access usage (802.16d standard), this may happen if a terminal is unplugged, but in a nomadic environment (802.16e standard), this may mean that a mobile station changed from one sector to another.

The SIP Proxy plays a very important role in the system. It inspects SIP/SDP messages that come from clients, gathers the information about the participants in the call and then dispatches this information to the QoS Broker. The broker listens to these requests and does the appropriate connection provisioning in the Base Station, if there are still resources available.

The gathering of information in the Proxy, regarding client's QoS requirements plus the resource provisioning functions in the WiMAX Broker allow the dynamic provisioning of connections in the access network. This way, when clients ask for resources in the access network (through a SIP INVITE message), their connections are provisioned with the required QoS, but when they no longer need these resources (signaled through a SIP BYE message), these resources are de-provisioned from the WiMAX Base Station.

B. DiffServ QoS Broker

The DiffServ QoS Broker plays a similar role to the WiMAX Broker. It also has functions for installing policies and classifying rules in the core network. Figure 3 highlights its role.

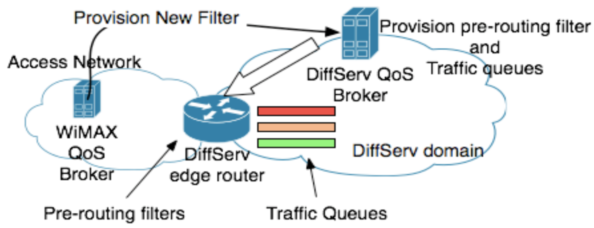

Figure 3 – Differv QoS Broker main functions

When the WiMAX QoS Broker receives resource allocation requests from the SIP Proxy, it will provision the resources that are needed for the access network clients. If any participant in the call is not a WiMAX client, he will forward the request to the DiffServ QoS Broker, so that it provisions the necessary filters for mapping.

When the DiffServ QoS Broker receives the information that it needs to create a mapping from the access to the core network, he will take action in the corresponding edge router and provision the necessary classifying rules. When the SIP conversation ends, the inverse action is taken, i.e., the provisioned rules will be deleted from the edge router.

The installation of new classifying rules allows that traffic coming from the WiMAX domain with QoS guarantees, has also privileged treatment in the core network. Worth mentioning is that these classifying rules are installed as pre-routing filters. This allows that the traffic is marked in the entrance of the edge router and when it is routed, he will fall in the correct traffic queue. In figure are represented three traffic queues (red, orange and green) that represent EF, AF and BE classes.

C. Protocol Layering

As the previously mentioned domains are technologically different, there is also a difference in the associated protocol layers. Figure 4 shows the protocol stack and the differences between technologies.

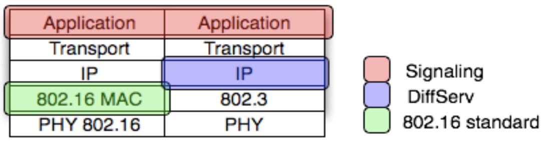

Figure 4 – Protocol Layering

On one side, we have the QoS concept of the 802.16 standard, which is at MAC layer. This concept is connection-oriented and each connection has a specific set of parameters which defines the characteristics of traffic using that connection. The other approach is the IP-DiffServ, which is at the IP Layer, with a non-connection-oriented style.

This difference imposes that, on one hand, the brokers make their admission control and configurations functions at different levels and on the other hand, it will need a mapping strategy for packets that cross from one domain to the other.

On top of these protocol stacks, we have the Signaling function. Signaling carries the information about client's QoS requirements and thus provides information to the brokers, so that they make the necessary NE configuration. This mechanism works on the Application layer and is technology-agnostic.

IV. Prototype Implementation

The prototype was developed using the Java programming language. This provides a portable prototype across OSs, as Java is platform independent.

In terms of NE configuration, the protocol used is SNMP [8]. The API used was SNMP4J [9], which is an open-source API for Java. SNMP was used instead of a proprietary Northbound interface (vendor Airspan), as it should provide compatibility between different vendors (if vendors comply with the 802.16f standard [10]).

For improved performance using the SNMP API, two concerns were taken into account. First, the use of multiple sets in each SNMP command allowed that, even though it was necessary to configure several parameters, only one SNMP command was involved. The second concern is related with socket operations. As socket operations tend to be heavy in terms of performance, a new thread is launched whenever it is necessary to close sockets. These two concerns allowed some performance gains in terms of configuration.

A mapping between traffic from the 802.16d to the IP-DiffServ domain was also considered. The rules are defined in Table 1.

The UGS traffic is directly translated into Expedited Forwarding. This can be justified because UGS traffic has hard QoS requirements (e.g. VoIP / Leased line E1/T1).

The rtPS traffic is considered to be mapped to the AF3 class (soft QoS requirements), while the nrtPS class maps to AF1 (even softer QoS requirements). This leaves out, for now, the AF4 and AF2 classes of DiffServ. These classes may be seen as future expansions to the core administrator. For example, if it wishes to make a distinction between gaming and video traffic, it could make that distinction in the core network, by using one the AF classes that is available. This way, the rtPS class would map to AF3 and AF4 classes, depending on the traffic type.

Table 1 – Mapping between 802.16d and DiffServ

802.16d	IP (DiffServ)
UGS	Expedited Forwarding
-	Assured Forwarding 4x
rtPS	Assured Forwarding 3x
-	Assured Forwarding 2x
nrtPS	Assured Forwarding 1x
Best Effort	Best Effort

With the inclusion of a new scheduling class by the 802.16e standard (extended real time Polling Service - ertPS), the mapping should not be changed. What would happen to this class is that it should map to an EF Per Hop Behavior. This is justifiable because ertPS is suited for services such as Voice Over IP with silence suppression.

V. Prototype Evaluation

A test scenario was setup to assess the prototype in terms of functionality and performance. On one hand, there was the need to test the system's functionality, i.e. the basic prototype capabilities: NE configuration, admission control policies and connection mapping between domains. On the other hand, a validation of system performance limits (e.g. the time necessary to establish new connections) was also necessary.

A. Test scenario

The base test scenario for functional and performance tests is depicted in Figure 5.

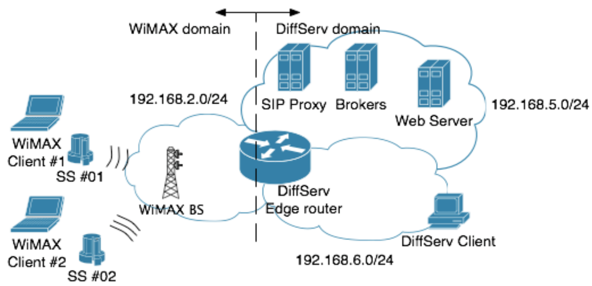

Figure 5 – Reference scenario used for testing

The scenario uses 802.16d compliant equipment (from vendor Airspan) in the access network, while a DiffServ edge router composes the core network. Both brokers have been merged into one machine and there exists only one SIP Proxy that serves all clients.

The evaluation of the prototype will be divided in two components. The first component will show the behavior of the system in a video-call, in terms of bandwidth usage. The second component will show the system's behavior in terms of time, i.e., the time that is it necessary for resource allocation, de-allocation and degradation of resources.

B. Results

The prototype was tested with a real conference call. Simultaneously, it was generated background traffic, which competes for bandwidth. Figure 6 represents the bandwidth usage of a video connection over time.

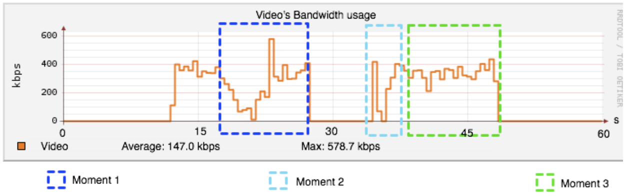

Figure 6 – Performance in terms of bandwidth usage

In this figure three distinct moments are represented. In Moment 1, the video connection is competing for bandwidth with the background traffic and the results are not encouraging, as expected. In this moment, the prototype is not working, thus no dynamic establishment of connections is made. When the prototype is turned on, the new (high-priority) connection is detected and provisioned. Moment 2 represents approximately 1 or 2 seconds of instability in bandwidth usage. This is the connection establishment period in the Base Station. After this period (Moment 3), it is possible to see that the traffic becomes stable and using the demanded bandwidth.

The prototype was also evaluated in terms of the elapsed time between detection of a QoS-enabled connection and its provisioning at the Base Station. Results are presented in Table 2.

Table 2 – Prototype performance results (in terms of time)

Parameter	Average (ms)	σ	C.I. (ms)
Time to provision	70.6	14.1	6.5
Time to de-provision	36.8	18.7	8.6
Time to degrade	57.7	8.8	5.5

The table represents three parameters: time to provision, de-provision and to degrade (for each parameter are represented the average, standard deviation the 95% Confidence Interval). The number of operations required at the Base Station explains the difference between results. In the provisioning process, it takes three operations: creation of a new entry, configuration and confirmation, while the de-provisioning and degradation processes need only one operation. The time to degrade involves also evaluation and calculation of new parameters, thus delaying the overall process. All results presented are below 100ms, which is a reasonable price to pay for dynamic QoS-enabled connections establishment.

VI. Conclusions

In this paper were presented the components necessary to make a dynamic management of resources in a 802.16 based access network. Furthermore, it was defined a mapping strategy to allow the preservation of QoS characteristics from the access to the core network.

In terms of the access network, the essential functions of NE configuration and admission control of the WiMAX QoS Broker were explained.

The evaluation of the prototype showed that, in terms of performance, the prototype is able to provision connections in the access network under 100 ms, which should not affect user's QoS opinion. Despite this fact, when this was tested in a real SIP-call (with audio and video enabled), it was noticed that the allocation of these connections affected the stability of the QoS-enabled connections for one or two seconds. However, after this initial period, it was verified that background traffic does not affect the QoS of these connections.

As future work, the core broker should be extended to support dynamic queue capacity adjustment, depending on the network load. It should also be considered the use of an 802.16e Base Station. With the mobility feature arise several challenges, namely in the admission control function.

References

[1] IEEE 802.16 working group. IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001): IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. IEEE Press.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, RFC 3261 – SIP: Session Initiation Protocol

[3] M. Handley, V. Jacobson, C. Perkins, RFC 4566 – SDP: Session Description Protocol.

[4] IEEE 802.16 Working group. IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Ammendment and Corrigendum to IEEE 802.16-2004): IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. Ammendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Band and Corrigendum 1. IEEE

[5] Enrico Angori, Eugen Corcoci, Mignanti Silvano, Cristina Nardini, Giada Landi, Nicola Ciulli, Giacomo Sergio, Pedro Neves: Exting WiMAX technology to support End to End QoS guarantees, May 2007.

[6] Jianfeng Chen, Wenhua Jiao, Qian Guo: Providing Integrated QoS Control for IEEE 802.16 Broadband Wireless Systems – Vehicular Technology Conference 2005. VTC-2005-Fall. 2005 IEEE 62nd.

[7] J. Delicado, L. Orozco-Barbosa, F. Delicado, P. Cuenca : A QoS-aware protocol architecture for WiMAX – IEEE CCECE/CCGEI 2006.

[8] J. Case, M. Fesor: A Simple Network Management Protocol (SNMP), RFC 1157, May 1990.

[9] F. Fock, J. Katz: SNMP4J – The Objet Oriented SNMP API for Java Managers and Agents – Web-site: http://snmp4j.org/index.html

[10] IEEE 802.16 working group: IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 1: Management Information Base. IEEE Press.