Simulation Model for End-to-end QoS across Heterogeneous Networks

Claudio Cicconetti[1], Maria L. Garcia-Osma[2], Xavi Masip[3], Jorge Sá Silva[4],
Gianfranco Santoro[5], Giovanni Stea[1], Halina Tarasiuk[6]

[1]Dipartimento di Ingegneria dell'Informazione, University of Pisa, Italy
[2]Advanced Networks Planning, Telefónica I+D, Madrid, Spain
[3]Computer Architecture Department, Technical University of Catalunya, Barcelona, Spain
[4]Laboratory of Communications and Telematics CISUC-DEI, University of Coimbra, Portugal
[5]Department of Systems and Computer Science, University of Rome "La Sapienza", Italy
[6]Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland

E-mail: [1]{c.cicconetti, g.stea}@iet.unipi.it, [2]mlgo@tid.es,
[3]xmasip@ac.upc.edu, [4]sasilva@dei.uc.pt,
[5]gsantoro@dis.uniroma1.it, [6]halina@tele.pw.edu.pl,

Abstract

This paper describes a simulation model, developed within the framework of the EuQoS project, which is aimed at assessing QoS on an end-to-end basis, across heterogeneous networks. In that respect, it discusses modelling issues related to access network technologies, to the core network, and to traffic generation. Furthermore, the implementation of the simulator within the ns-2 framework is described, and preliminary simulation results are reported.

1. Introduction

The last ten years have witnessed the publication of a remarkable amount of scientific literature on Quality of Service (QoS) mechanisms for packet switching networks. However, such a scientific effort has not been translated so far into wide-scale QoS deployment. The EuQoS project, an Integrated Project under the European Union's Framework Programme 6 [6], is in fact aimed at deploying a flexible and secure QoS assurance system (the EuQoS System) over a pan-European testbed environment. The EuQoS system will accommodate applications requiring guaranteed QoS, such as Voice over IP (VoIP), Video on Demand (VoD), Tele Engineering, Distance Learning, Medical Applications, over heterogeneous access networks, such as UMTS (Universal Mobile Telecommunications System), WiFi (Wireless Fidelity), xDSL (x Digital Subscriber Line) and Ethernet, connected through an IP core network. Thus, the EuQoS sys-

tem will integrate several QoS architectural components, at all relevant layers and planes: from signalling protocols to Traffic Engineering mechanisms, from admission control algorithms to resource reservation schemes.

The validation and performance assessment - via extensive simulative analysis - of such a complex environment will provide useful insight for the deployment of the real testbed. For this purpose, two complementary simulation models of the EuQoS system have been developed: a *packet-level* and a *flow-level* simulation model. The former is aimed at assessing packet-related performance metrics (like end-to-end delay, jitter, loss probability) in scenarios where the set of established flows does not change. The latter, instead, considers flow-related performance metrics, like blocking probability and given pre-established flow arrival patterns. As such, it can be used to test resource reservation and admission control mechanisms, as well as to derive worst-case scenarios for the packet-level simulator. By using two different simulation models, it is possible to limit the complexity without losing simulation accuracy.

This paper describes the various aspects of the EuQoS packet-level simulation model. More specifically, it describes the model used for each access network and for the core network. Furthermore, it describes the models used for foreground and background traffic and the performance parameters. The packet-level simulation model has been implemented in the ns-2 simulation environment [1]. Thus, we also report an overview of its implementation and some preliminary simulation results.

The rest of the paper is organized as follows: Section 2 describes the packet-level simulation model. In Section 3, we describe the traffic generators and the performance

metrics that the simulation model is going to measure. We describe the implementation, also reporting preliminary simulation results, in Section 4, and we draw conclusions in Section 5.

2. Packet-Level Simulation Model

At a first level of decomposition, the packet-level simulation model is composed of two *access networks* connected through a *core network*, as depicted in Fig. 1. The access networks taken into consideration are UMTS, WiFi, Ethernet and xDSL, which are the most widespread at the time of writing. The core network is a generic IP-based network. Access networks are connected to the core network by means of a single link between border nodes. In the general case, a set of flows is established between nodes in the different access networks, representing *foreground* traffic. Also, *background* traffic is setup between pairs of nodes (e.g., between edge nodes in the core network). The latter is meant to simulate the behaviour of aggregated traffic sources sharing resources (e.g., link bandwidth) with foreground traffic. Decoupling traffic into foreground and background traffic is strongly required to make simulations easier. This way both traffics can be created by different generators according to different models. This is in fact very helpful to increase simulations performance while keeping an accurate network scenario. Notice that current networks only demand QoS guarantees for some of the traffic to be transported by such networks. In fact it is well-known that a significant amount of traffic on the network will not have any QoS constraint. This scenario can be perfectly modelled by such traffic decoupling, where background traffic might simulate best-effort traffic. According to such traffic definition, we could for example evaluate the impact on the QoS guarantees for the foreground traffic due to including congestion avoidance policies on the background traffic. Besides, it is also worth noting that both traffics differently impacts on some QoS parameters. For example, throughput measurements mainly require foreground traffic while latency measurements require both foreground and background traffic.

The purpose of the packet-level simulator is assessing end-to-end packet-related performance metrics, in scenarios in which the number of established flows does not change. For instance, in the simulation scenarios we assume that the number of simultaneous QoS traffic flows is at the admission control limit, while a heavy load of best effort traffic is also present. For this reason, it is not necessary to model all the features related to flow setup/teardown, like signalling, resource reservation mechanisms (those are in fact covered by flow-level simulation). Furthermore, it can be assumed that packet routes do not change over time. Hereafter, we describe the models used for the proposed access networks and for the core network.
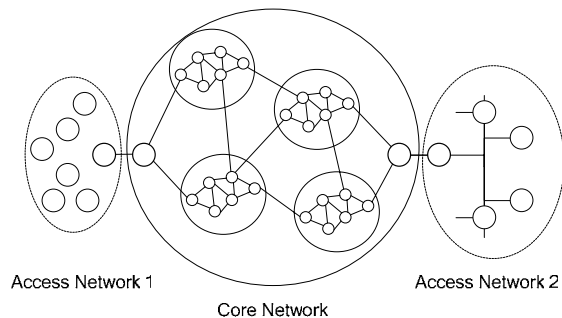

Fig. 1. Packet-level simulation model

2.1. UMTS

The architecture simulated in the UMTS access network module can be described as follows (see Fig. 2): The UE (User Equipment) mobile nodes, which generate traffic and move within the cellular layout, the UTRAN (UMTS Terrestrial Access Network), composed by several Base Stations (Node B) and RNCs (Radio Network Controller) and the Packet Switched UMTS Core Network (UMTS CN), constituted by the SGSN (Serving GPRS Support Node) and the GGSN (Gateway GPRS Support Node).
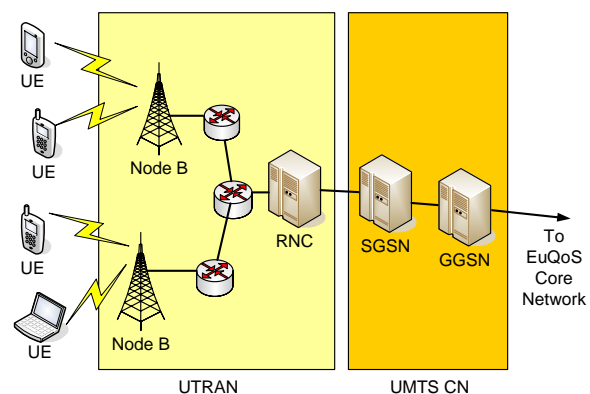

Fig. 2. UMTS simulation model

In order to run reliable simulations, two different scenarios have been considered. On the one hand, the urban scenario, characterized by accurate propagation models (multipath), high traffic load and strictly constrained mobility models; on the other hand, the rural one, with simpler propagation models (single ray), lower traffic and relaxed mobility models. All the issues relevant to traffic, mobility and propagation are described below.

The UMTS simulation model is mostly suitable for the analysis of the radio resource management mechanisms, with the objective of optimizing the radio link efficiency

with respect of QoS. In particular, admission control algorithms are evaluated, whose purpose is to accept or deny new connections taking into account the users QoS level.

We assume that the UTRAN consists of a single Node B, which is adequate to simulate UMTS mobile nodes behaviour, as we take into account an additional interference term that models the inter-cell interference. The UE mobile nodes change their location according to a mobility algorithm depending on the selected scenario (urban/rural). The traffic bottleneck for the UMTS Access Network is localized in the W-CDMA radio interface, since the links between RNCs and SGSN are wired over-provisioned connections.

The MAC layer implements the DSCH (Downlink Shared CHannel) and manages power and Spreading Factor assignments. The code allocation in this shared channel is implemented in a round robin fashion. DCH (Downlink CHannel) is implemented too. For each received packet the physical layer computes the SNR (Signal to Noise Ratio) and inserts it in the packet header. Every 10 ms the MAC layer compares the computed SIR (Signal to Interference Ratio) with a SIR target level (6 dB) and consequently increases or decreases the transmission power of the packet sender with a TPC (Transmission Power Control) command.

2.2. WiFi

A WiFi access network consists of several IEEE 802.11 wireless stations coordinated by an Access Point (AP) in infrastructure mode, as shown in Fig. 3. The AP connects the Wireless Stations to the core network via a single link.

The following assumptions have been made in the WiFi simulation model:

- We assume that users do not change their location, and thus mobility is not simulated.
- Recent WiFi devices are capable of switching through different rates and/or physical layers typically when the SNR measured by the wireless physical interface drops below (or raises above) a given threshold. The IEEE 802.11 document [4] does *not* define a standard PHY/rate switching scheme. Therefore, simulating the PHY/rate switching would imply the evaluation of specific algorithms, which are outside the scope of this simulation model. Thus, we assume that nodes do not switch rate nor physical layer.
- We assume that all the nodes communicate using the Distributed Coordination Function (DCF). Although the Point Coordination Function (PCF) is in fact part of the standard, it is optional and currently supported in very few APs or WiFi adapters. Furthermore, even though the PCF provides the associated stations with a means of differentiating the service of their flows, it

has been proved to be unsuitable for providing flows with strict QoS service guarantees [2].
- The IEEE 802.11 allows the wireless devices to use power-saving procedures, in order to limit the energy requirements during inactivity periods. Since the time scale of the power-saving cycle is currently much greater than the service period of the traffic types under consideration (described in Section 3) and the set of connections is fixed, we can assume that the stations never enter the power-save status.

The following MAC features are simulated:
- RTS/CTS handshake. All packets with size larger than a specified threshold (called RTS/CTS threshold) are protected by a Request To Send/Clear To Send handshake.
- Fragmentation. All packets with size larger than a specified fragmentation threshold are fragmented into chunks of a size smaller than the threshold itself. Reassembly is performed at the destination node.

Users can select the Short (Long) Retry Limit, i.e., the number of MAC-layer retransmissions that a packet smaller (or larger) than the RTS/CTS threshold can experience before being dropped.
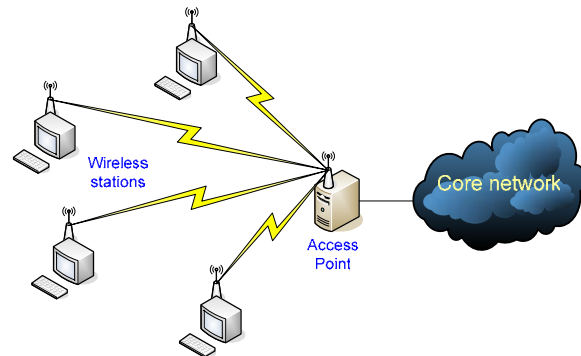

Fig. 3. WiFi simulation model

The IEEE 802.11 does not provide the stations with QoS support. The Task Group E of the IEEE 802.11 Working Group has recently published a draft version of the IEEE 802.11e amendment [5] to the IEEE 802.11 document. The draft document adds two medium access functions, namely the Enhanced Distributed Channel Access (EDCA) and the HCF Controlled Channel Access (HCCA) that provide QoS support for the flows. To the best of our knowledge, no device supporting the above enhanced mechanisms is currently available on the market. Therefore, we do not simulate any of the above enhanced access mechanisms. Channel error models to be employed are currently under investigation.

2.3. Ethernet

Currently, Ethernet is not only a "building or campus technology", but it is also used to connect residential users, workstations and devices in a room or servers in a campus and in institutions. We use four models (presented in Fig. 4) to study different types of Ethernet networks:

- Small Office Home Office (SOHO)
- Campus/LAN scenario
- MAN organization scenario
- MAN residential scenario (Ethernet Passive Optical Network - EPON)
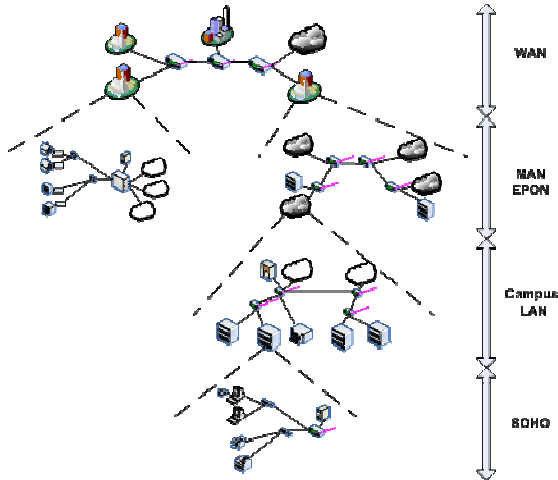

Fig. 4. Ethernet simulation models

At the moment, CSMA/CD solutions are rarely used in Ethernet networks. As a consequence, in EuQoS project, we study only switched solutions.

In order to simulate a network consisting of terminal equipment connected to ports on a switch, we use nodes connected with links of the desired bandwidth (10Mbps, 100Mbps, 1Gbps or 10Gbps). To study the implementation of QoS mechanisms in Ethernet networks we have implemented the 802.1p and 802.1q standards and developed a specific NS-2 queue object that implements the recommendations of the IEEE 802.1p standard related to traffic prioritization. Basically, the new queue object presents the following properties:

- It can be configured to use up to eight virtual queues to group incoming LAN packets into separate traffic classes.
- The forwarding mechanism is implemented to support the selection of the packets from a given virtual queue to be transmitted only if a higher order virtual queue is empty at the time of selection.

Implementing exactly eight virtual queues is not mandatory, any number from 1 to 8 being possible. IEEE 802.1p recommends a mapping of user priority values for the number of traffic classes (virtual queues) available.

If a packet has a user priority value less than zero, it will be treated as a best effort packet (user priority equal to zero). If the priority value is greater than seven, the packet will be classified as a highest priority packet (as if it was set with user priority seven).

To make possible the classification of packets by the prioritization queue, it is necessary to previously mark the packets with a user priority value. To accomplish this task we also developed a specific agent (PriAgent) in ns-2.

2.4. xDSL

xDSL is the name given to a set of technologies that use the digital subscriber line for the transmission of information. Although there are several xDSL technologies (ADSL, Asymmetric DSL, HDSL, High-bit-rate DSL, SDSL, Symmetric DSL , VDSL, Very high bit-rate DSL, etc.), nowadays the most popular in Europe is ADSL, where *asymmetric* indicates the use of different downstream and upstream rates.

Fig. 5 shows the EuQoS xDSL simulation scheme, where the common elements are depicted, and the black box scheme for users, DSLAMs (DSL Access Multiplexer), switches and BRAS (Broadband Remote Access Server).

The actual network architecture for providing an xDSL access varies depending on the country and regulatory environment, users and their geographic distribution, etc., the proposed model can be easily adapted to the architecture to be simulated.

This model is mainly dedicated to emulate the behaviour of the xDSL network and to analyse the mechanisms to provide QoS over xDSL.

Regarding the network emulation, it is possible to simulate two different technology-based networks: ATM and IP/Ethernet. The xDSL access network can be supported by the following transport technologies: ATM or IP/Ethernet. ATM technology has been used as the transmission standard with advanced quality of service (QoS) capabilities for managing different types of services and traffic. Nevertheless, because of the multiple advantages it provides, IP/Ethernet networking technology is nowadays being introduced nowadays in the concentration network. Two main differences can be seen in the simulation model: different link capacities and AAL5 fragmentation. For the ATM concentration network, the packets transmitted through the xDSL path should be fragmented into chunks of a smaller size to fit into the ATM cells and reassembled by the BRAS. Besides, the model allows to simulate the channel latency between the ATU-R (customer ADSL modem) and the ATU-C (ADSL line card in the DSLAM), which depends on the line encoding technique and the interleaving depth of the error correction scheme (fast and interleaving channels), by introducing a delay in the link connecting both equipments.

Even though the simulation of a complete BRAS location with numerous users is possible, it is simpler and faster to simulate just some users and to introduce background traffic in order to simulate delays and losses in equipments. The generated and received background traffic must appear through the links of this architecture to simulate the complete network scheme and Poisson traffic models are sufficient. Moreover, France Telecom R&D [3] suggests that the arrival process can be reasonably assumed as Poissonian. This simulation scheme distinguishes between an Individual User and an Aggregated Traffic Generator: the Individual User stands for the xDSL customer whose traffic is analyzed, and the Aggregated Traffic Generator represents how loaded this user finds the path shared with other customers. The figure above only represents the Upstream traffic (User -> BRAS) in detail, but the simulation model uses the Aggregated Traffic Generators in both directions for every link in the access network (also Downstream: BRAS -> User).

The QoS mechanism in the xDSL model is designed for services offered over the network, that is, different traffic profiles identified by specific requirements are demanded by several users and their features can be guaranteed by each element of the architecture involved in the access network. In fact, for the ATM concentration network, four different category services can be chosen for the ATM virtual circuits (VCs) created between each user and the BRAS: CBR or VBR-rt for QoS aware applications, and VBR-nrt or UBR for the others. This is the reason why the simulation model has been represented with four application traffic generators from an individual user, as corresponding to the four types of service specified in ATM, although a user really could have as much generators as VCs are established. Several parameters can define each type of service, and the Queue Scheduling system can be built based on the most appropriate traffic policy. Although VCs are not established in the IP/Ethernet concentration network, a DiffServ scheme with the same number of classes can be used and the simulation model would not change, save for link capacities and the non-fragmentation.

2.5. Core Network

The IP core network covers the area laying between access networks. We model it as a cascade of *QoS domains*, which are connected by inter-domain links. The number of cascaded domains corresponds to the number of Autonomous Systems along the end-to-end path determined by the routing protocol (e.g. BGP (Border Gateway Protocol) [10] or qBGP (QoS-BGP) [11]). Now, we focus on appropriate modelling of a single QoS domain as a basic element of IP core network. The model of a QoS domain is illustrated in Fig. 6. The important features of the QoS domain we need to model are the following: 1) the bottlenecks: assuming an over-provisioning of the domain internals, they are located at the inter-domain links; 2) the inter- and intra-domain traffic (highly aggregated). In a QoS domain we can consider two types of bottlenecks. The first one is the *edge* router, which aggregates traffic from several *access networks*; the second one
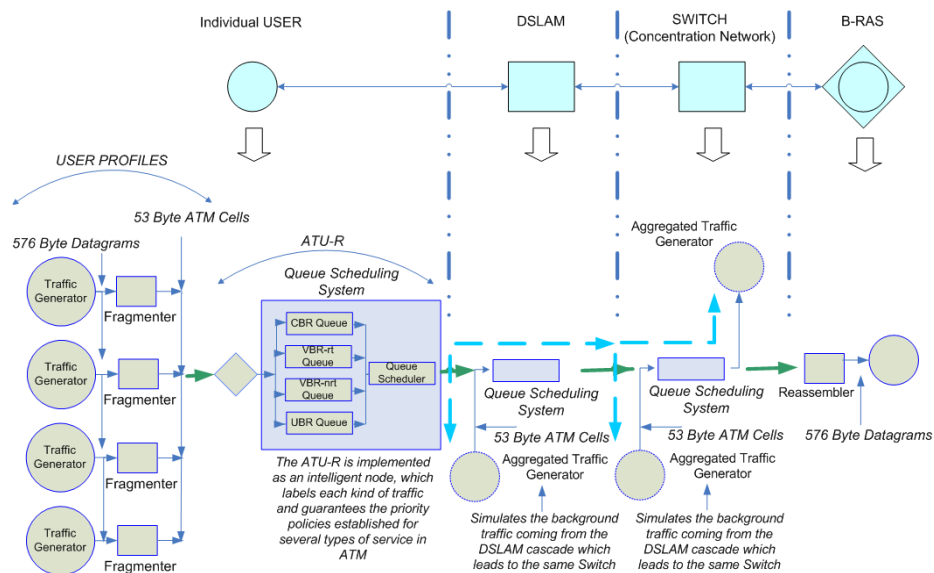

Fig. 5. xDSL simulation model

is the border router, which represents the aggregation point of traffic from several *QoS domains*. Other elements of the model are the core router and the interfering traffic generators.
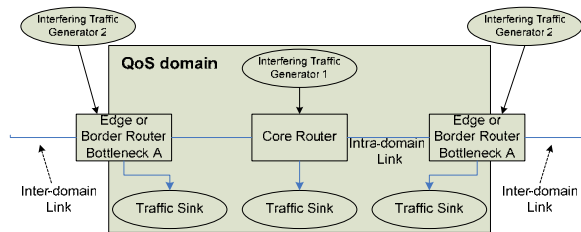

Fig. 6. Simulation model of a QoS domain

We assume that routers are DiffServ- (*Differentiated Services*) capable [7], [8], [9]. Therefore, in each edge and border router we can differentiate the service of packet streams based on predefined PHBs (*Per Hop Behaviours*) associated to traffic classes supported in the QoS domain. The QoS domain model allows one to select the number of traffic classes. In particular, we can assume to model one QoS traffic class, and the best-effort class. Each traffic class is defined by an appropriate set of QoS mechanisms. In particular the following QoS mechanisms at the packet level are set up in the input router interface: *classifier*, both multi-field and behaviour aggregate, *policer*, with both single and dual token bucket meters with strict token bucket conformance and absolute *dropper* element. On the other hand, queue selectors, queues with predefined length and drop policies, schedulers (e.g. PQ (Priority Queuing), WFQ (Weighted Fair Queuing), DRR (Deficit Round Robin, [12]), PQWFQ (Priority Queuing WFQ, [13]), PQDRR (Priority Queuing DRR)) and output links are related to the output interface of the router. We assume that the interfering traffic load submitted to edge and border routers (bottlenecks) is up to admission control limit in particular QoS traffic class and has heavy load condition in best effort class.

Furthermore, the core router models the distortion of the traffic characteristics of a packet stream passing through a number of routers inside the QoS domain. The packet delays resulting from the propagation and transmission times inside the QoS domain are introduced as a link parameter. The capacity of this link corresponds to that of the slowest link along the path inside the QoS domain. The main focus is put on the appropriate model of the aggregated traffic that interferes with the investigated packet streams.

3. Modelling Foreground and Background Traffic

As stated in Section 2, foreground traffic stands for that traffic to be measured while background traffic stand for that traffic simply interfering with the foreground traffic. A detailed description of the models to be used for both traffic is presented in next subsections.

3.1. Foreground traffic

Foreground traffic stands for the set of flows established between nodes in the ANs. Since these flows are well-known, it is possible to model them with applications models such as VoIP, video streaming, videoconference, etc. In this section we only present the traffic models for VoIP and video streaming applications. Other applications are left for further study.

On the one hand, in [21] a list of codecs that are currently used by the VoIP applications to reduce the bandwidth requirements is shown. The VoIP applications usually employ Voice Activity Detection (VAD) techniques that detect the periods during which the user is silent. During silence periods no packets are generated. Traffic models for such model of ON/OFF patterns of speech can be found in [22] and [23].

On the other hand, concerning video streaming, the MPEG-4, whose main target is the transmission of non-interactive video, such as movies, and the H.263, which is mainly used for the transmission of interactive video sessions, such as videoconferences, are the two commonly used video codecs. In [14], [15] the authors present a publicly available library of frame size traces of long MPEG-4 and H.263 encoded traces, which they have generated at the Technical University of Berlin. The traces may be used as an input for the simulation of video streaming.

3.2. Background traffic

Regarding the background traffic, it is possible to use specific models in each access network. There are many references describing such specific models. Just as an example we suggest to go through the following references: Ethernet [16], xDSL [17], WiFi [18], UMTS [19] and WAN [24]. However the models described on those papers are usually very dependent on the network characteristics so it is sometimes difficult to find network independent traffic features to be used.

However, there are analytical traffic models that are useful for performance evaluation of packet switched networks, such as CBR (Constant Bit Rate), superposition of CBR and N-state sources. A brief description of these traffic models is presented. The CBR traffic model usually represents the traffic emitted by a single source characterised by the peak bit rate and the packet size. In order to characterise the traffic emitted by a number of CBR sources, we use special models, and we call them as superposition of N independent CBR sources. As limit case when N tends to infinity, we use a Poissonian stream de-

scribed by the mean bit rate, the packet inter-arrival distribution (exponential) and the packet size. In the N-sate source in its general model each state can be either ON or OFF. In the ON state the IP packets are generated according to the specified pattern, characterised by the time duration or number of sending packets, the packet arrival pattern (both described by either the constant, uniform or exponential probability distribution function) and the packet length. On the other hand, the OFF state, where no packets are generated, is only characterised by the state duration distribution that can be again constant, uniform or exponential. With the ON/OFF source model is characterised by the following parameters. Particular cases are the ON/OFF source with only 2 states, the state ON characterised by a geometric number of packets distribution (mean 10 packets) and a constant distribution for the packet length (100 bytes) and the packet inter-arrival (1ms), and the state OFF characterised by a exponential state duration distribution (mean 100 ms); the IPP source also with two states, the state ON characterised by a exponential distribution for both the state duration (mean 10 ms) and the packet inter-arrival (1ms) and a constant distribution for the packet length (100 bytes), and the state OFF characterised by a exponential state duration distribution (mean 100 ms); the aggregated source with 3 number of states (ON1, ON2 and OFF); and finally the (M+1)-state MMDP model which considers a superposition of M identical and independent on-off sources and with a superposed traffic stream that can be approximated by an (M+1)-state MMDP (Markov Modulated Deterministic Process) [25]. More detailed information on such models can be found in [20].

3.3. Performance parameters

Many parameters can be used to measure the network performance in terms of Quality of Service. The most common are throughput, delay, jitter and packet loss. The significance of such different parameters to describe the network performance is strongly dependent on the application in use, for example, while VoIP applications are quite sensitive to delay constraints, this parameter hardly impacts on a chat application. A general overview of some applications QoS requirements can be found in [20]. We present below a short description of the reference values of such performance parameters for VoIP and video streaming applications.

On the one hand, VoIP applications are real-time applications strongly affected by delay, jitter and packet loss. The throughput depends on the codec used during a VoIP conversation. A more deeply description can be found in [26]. Under normal operations the round trip (two-way) delay should be less than 150ms, noting that voice quality degrades quickly when the total one-way delay is greater than 150ms. In fact, one way delay greater than 200msec

causes impaired interaction for a voice conversation. Therefore, the end-to-end delay is one of the major constraints to this application. Concerning the jitter metric, buffers are included to allow fastest packets to wait for the slowest ones in order to be played in the correct sequence. Since additional buffering also causes additional delay, this solution must be carefully applied. Adaptive jitter buffers within IP telephony devices automatically compensate for 20-50 ms of jitter. If jitter exceeds these bounds, then loss will occur, impacting voice quality. Current experience indicates that if jitter is held to within 10-20 ms, then voice quality is acceptable. Voice packets are handled as data packets in current traditional IP networks. This means that voice packets will be dropped when network is heavily congested. Although this is not a problem for data packets (they can be retransmitted again), voice packets cannot be handled in such a way. There are some solutions dealing with the packet loss. For example, Packet-Loss Concealment (PLC) algorithms can correct up to 30msec of lost voice. In short, packet loss values upper than 1% strongly impacts on the voice quality.

On the other hand, Video streaming applications belong to the category of high quality applications requiring huge amounts of bandwidth in order to guarantee a user-satisfying image quality. VoD is fully dependent on the delay metric. Although the time required for the end-to-end transmission of packets throughout the network is not significantly important in VoD applications, the end-to-end delay is an important performance parameter. Besides the delay caused by the transmission process, the jitter is also an important parameter. Again, a buffer solution is proposed to compensate the jitter, even knowing that the larger the buffer size, i.e. the larger the number of packets out of order, the larger the delay. Therefore, jitter must be as low as possible.

The loss of packets directly depends on the throughput. If the throughput is guaranteed at peak-rates, network congestion does not lead to packet loss. But if loss is due to transmission errors, the application will lose quality. Therefore, to provide the user client with certain QoS guarantees, the packet loss must be reduced. In case that due to network congestion this cannot be completely achieved, video streaming traffic should be prioritized. Concerning the bandwidth requirements they are fully dependent on the delivered movie and the used codec. The bandwidth can vary from 0.5 to 17 Mbps.

Besides the QoS parameters described above, it is worth mentioning that since VoD applications have real-time constraints, packet reaching the user client after the deadline agreed in the SLA may be unusable and must be discarded. This means that in case of congestion, packets should be dropped instead of delayed in order to speed up subsequent packets. Although this is the behaviour desired for VoD applications, other options such as delaying

or marking non-conformant traffic (delayed traffic) might be suitable for other kind of applications. Therefore, how non-conformant packets are handled must be left as an option.

4. Implementation and Evaluation

The packet-level simulation model has been implemented using the ns-2 simulation environment, which has been suitably extended with both C++ and Tcl/Tk modules. In order to provide a flexible approach to the integration of heterogeneous simulation modules, the architecture depicted in Fig. 7 has been devised.

The simulation environment consists of three types of modules:

- *Technology-dependent modules*. These correspond to the simulation models described in Section 2. Note that both the WiFi and UMTS modules use an ns-2 shared data structure, which is the flat grid where wireless nodes are placed upon. Thus, we provide a communication interface between the WiFi and UMTS modules and a small module (*Grid*) that actually deals with wireless-only simulation objects.
- *Technology-independent modules*. These modules do not depend on the underlying network technology because either they model user-layer applications that are not aware of the network details (Traffic module) or they only exist for the purpose of simulation (Measurement module).
- *Main module*. This module interfaces the user with the simulation environment. It reads the user input, loads all the required modules and actually controls the execution flow of the core simulator (i.e., ns-2). Also, the Main module manages all the shared data structures, except the *wireless grid* that is taken care of by a stand-alone module. For example, both the Traffic and the Measurement modules should be able to access the ns-2 nodes in order to attach/detach traffic generators or monitoring objects. Therefore, an associative globally visible array of the nodes created in the two access networks and the core network in the current simulation is stored into the Main module.
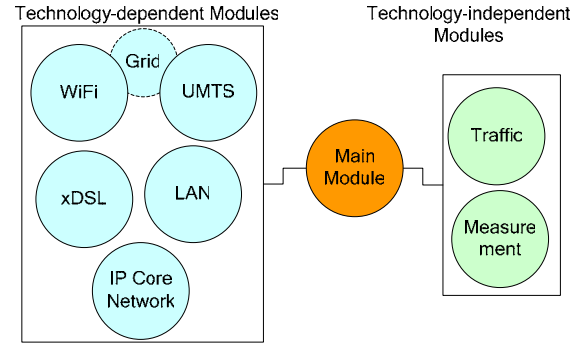

Fig. 7. Simulator architecture

The above framework allows the seamless addition of new modules (e.g., new access networks or traffic generators), as long as they comply with the defined Tcl/Tk programming interface. The configuration of the previous modules depends on user-defined high-level syntax files, that are provided as input to the Main module.

Hereafter, we report some preliminary simulation results showing the need for end-to-end QoS mechanisms. We set up a scenario, shown in Fig. 8, in which a tagged session, consisting of bi-directional VoIP and videoconference communication, is established between two nodes of different access networks, namely Ethernet (access network 1) and WiFi (access network 2), connected through the IP core. The switched Ethernet network consists of 60 nodes connected by 10 Mbps links, as shown in Fig. 9. The WiFi network consists of 20 nodes communicating with a single AP, with physical parameters set as in Table 1. The core network consists of one QoS domain with bottlenecks at ingress routers. Inside the domain we introduce an additional packet delay of 10ms, to simulate the propagation delay in both ways.
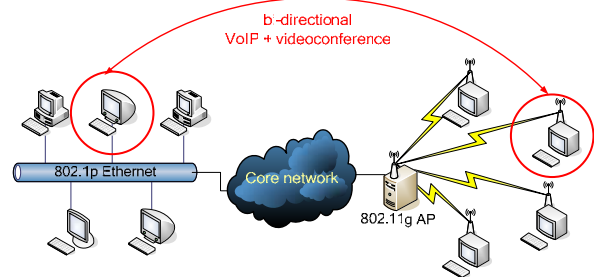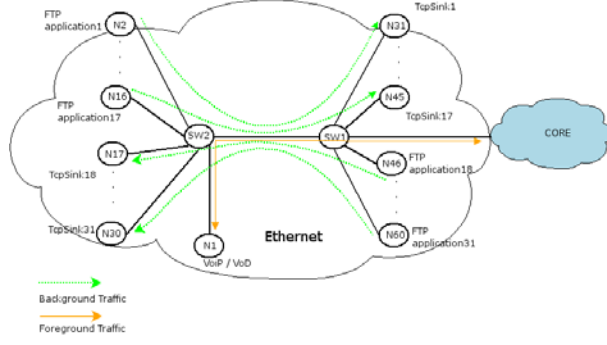

Fig. 8. Scenario for simulations

Fig. 9. Ethernet layout

Data rate	11 Mbps	SIFS	10 μs
Basic rate	1 Mbps	PIFS	30 μs
PHY header	192 μs	DIFS	50 μs
Retry Limit	7	CWmin	31
		CWmax	1023

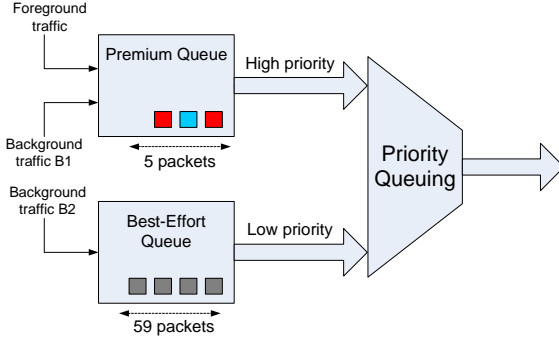Table 1. MAC and physical parameters for WiFi

Fig. 10. Services in the IP core

In the Ethernet, priorities are chosen so that voice and video traffic has higher priority than background traffic. In the IP core, we define two traffic classes (see also Fig. 10), *Premium* and *Best Effort* (BE). QoS requirements for Premium class are low packet delay and low packet losses. To meet this requirements we employ admission control rules based on the Rate Envelope Multiplexing scheme with the peak rate allocation, as shown in [13]. Premium packets are served with the highest priority in the IP core routers. The maximum admissible rate depends on both the amount of link capacity dedicated for the Premium service and the target utilisation factor ρ, calculated from the following equation:

$$\rho = \frac{2B}{2B - ln(\,P_{loss}\,)},$$

where B is the buffer size dedicated to Premium service and P_{loss} is target packet loss rate. In our simulation scenarios at ingress routers we assume that B=5 packets and $P_{loss}=10^{-2}$, with which ρ=0.685. Next, we assume the

amount of the link capacity dedicated to Premium service to be equal to 20 Mbps, and as a consequence the admission control limit becomes equal to 13.7Mbps of traffic.

In BE service no admission control rules are defined. BE packets are served with the lowest priority in the IP core routers. The bandwidth dedicated to the BE service at ingress router is equal to 80 Mbps; the buffer size is equal to 59 packets.

In the WiFi network, instead, no QoS mechanism is active. We evaluate the performance of the tagged session when the background traffic increases. More specifically, at time t=20, 40, 60 s background traffic is added in the Ethernet, core, and WiFi as follows:

- Ethernet: nodes N2-N30 simulate FTP servers and send data to nodes N31-45, whereas nodes N46-N60 simulate FTP servers and send data to nodes N17-30

- IP core network: The scenario is symmetric in both directions (one of which is shown in Fig. 10): BT1 represents the background traffic of the Premium class, which is a Poissonian stream with a mean rate such as to saturate the admission control limit, i.e. 11.676Mbps, and packet size equal to 500 bytes. On the other hand, BT2 represents BE background traffic, and it is itself a Poissonian stream with a mean rate of 90Mbps and 500 byte packets.

- WiFi: Ftp sessions between the nodes and the AP, acting as a server.

The VoIP traffic for the tagged session is coded according to the G.729 codec, i.e. 24kbps with 60 byte IP packets. The video traffic is an MPEG4 high-quality video-conference trace, [14], [15], with an average bit rate of 400kbps and a peak rate of 2Mbps.

In Figures 11 to 14 we report the results of the experiments. More specifically, Fig. 11, shows the graphs of the one-way delay as a function of time, averaged on time windows of 10 seconds for the sake of readability. As the graph shows, the delay is almost constant – regardless of background traffic in the Ethernet and the QoS IP domain – until background traffic is started in the WiFi network (t=60 s). At that time, the delay drastically increases in both direction. It is worth noting that the delay in the downlink direction with respect to the AP (i.e. from network 2, Ethernet, to network 1, WiFi), is much lower. This is due to the well-known asymmetry of the WiFi link when operating in infrastructure mode. In fact, in an IEEE 802.11 system all the wireless terminals, Access Point included, access the medium using the same procedure. Thus, when the system is heavily loaded, which is the case when the FTP traffic starts at 60.0 s, the AP obtains the same throughput of any other terminal. However, the egress traffic from the AP is much higher than that of the terminal with the tagged flows, because the AP also generates the TCP acknowledgments addresses to the terminals with FTP traffic. Therefore, the packets from

the core network experience a higher queuing delay than those generated at the terminal with the tagged flows.
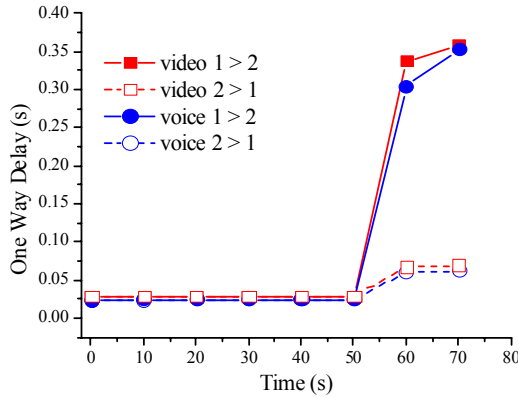

Fig. 11. One Way Delay as a function of time

Fig. 12 shows the inter-packet delay variation (jitter) for the video flow going from Ethernet to WiFi (the graphs are similar, and therefore not shown, for both directions and for both flows). As for the previous graph, the values are limited until background traffic is started in the WiFi network.
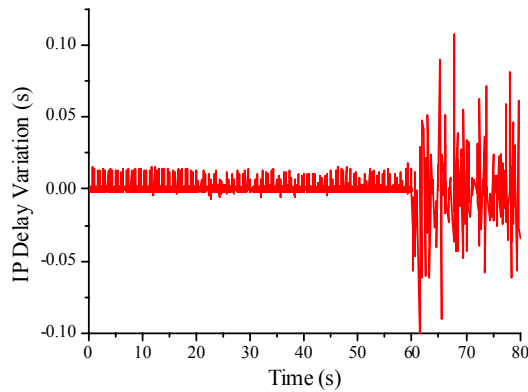

Fig. 12. Inter Packet Delay Variation for the video flow (direction 1 to 2)

Fig. 13 shows the one-way packet loss ratio as a function of time, computed on time windows of 10 seconds. It is possible to observe that the network starts losing packets after background traffic is started on the Ethernet network. This is because the buffer space reserved in the Ethernet switch is relatively small (50 packets), and it is shared among all the priority classes. As before, the packet loss dramatically increases when background traffic is started in the WiFi network. The packet loss is

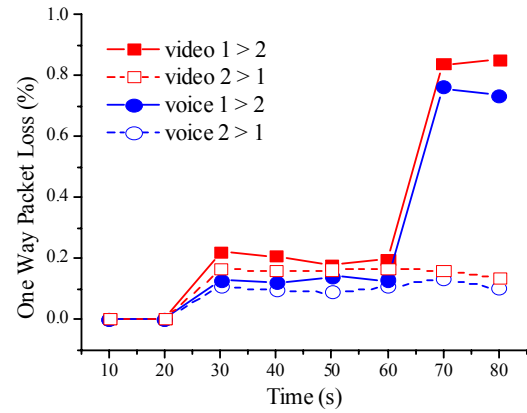higher in the downlink direction for the same reasons mentioned above.

Fig. 13. One Way Packet Loss as a function of time

Fig. 14 shows the IP throughput, averaged on time windows of 10 seconds. The throughput is reduced when the background traffic is started on the Ethernet segment, due to the increase in the packet loss. Furthermore, when background traffic is started on the WiFi network, the throughput in the downlink direction is further reduced.
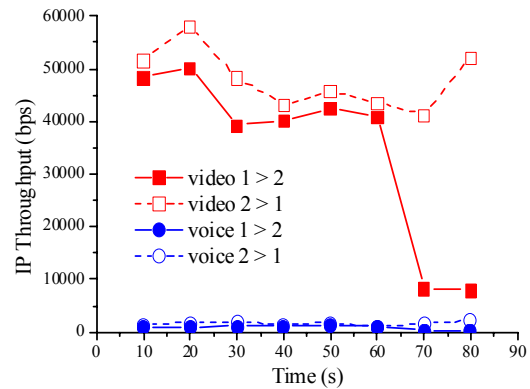

Fig. 14. IP throughput as a function of time

The above figures clearly show the need of implementing QoS mechanisms in all network segments, i.e. on an end-to-end basis. For example, the emerging 802.11e MAC protocol, which enhances the basic WiFi network supporting absolute and relative service differentiation, could be a solution for the QoS problem shown in this case.

5. Conclusions

In this paper we have shown the simulation model, developed within the framework of the EuQoS project, which is used to validate the QoS on an end-to-end basis, across heterogeneous networks. We have presented models for the various access network technologies and for the core network. Furthermore, we have discussed how to model traffic at all the relevant stages of the network. The simulation model described herein has been implemented within the ns-2 framework; preliminary simulation results, reported within the paper, effectively show the need for QoS mechanisms on an end-to-end basis.

6. Acknowledgements

References

[1] The ns-2 simulator, www.isi.edu/nsnam/ns

[2] A. Lindgren, A. Almiquist and O. Schelen, "Quality of Service Schemes for IEEE 802.11 Wireless LANs - An Evaluation".

[3] N. Ben Azzouna, C. Fricker, F. Guillemin, Modeling ADSL traffic on an IP backbone link. ALCOM-FT, Deliverable 1022, August 2003.

[4] IEEE Computer Society LAN MAN Standards Committee. IEEE 802.11: Wireless LAN Medium Access Control and Physical Layer Specifications, August 1999

[5] IEEE Computer Society LAN MAN Standards Committee. IEEE 802.11: Wireless LAN Medium Access Control and Physical Layer Specifications. Medium Access Control (MAC) Quality of Service (QoS) Enhancements, Draft D9, August 2004

[6] The EuQoS consortium, www.euqos.org

[7] S. Blake, et al., "An Architecture for Differentiated Services", Internet RFC 2475, December 1998.

[8] D. Grossman, "New Terminology and Clarifications for Diffserv", Internet RFC 3260, April 2002.

[9] Y. Bernet, et al., "An Informal Management Model for Diffserv Routers", Internet RFC 3290, May 2002.

[10] Y. Rekhter, T.J. Watson, T. Li, "A Border Gateway Protocol 4 (BGP-4)", Internet RFC 1771, March 1995.

[11] E. Crawley, R. Nair, B. Rajagopalan, H. Sandick, "A Framework for QoS-based Routing in the Internet", Internet RFC 2386, August 1998.

[12] S. Keshav, "An engineering approach to computer networking", chapter 9: "Scheduling", Addison-Wesley, 1997, pp. 209-263.

[13] A. Bąk, W. Burakowski, F. Ricciato, S. Salsano, H. Tarasiuk, "A framework for providing differentiated QoS guarantees in IP-based network", Computer Communications 26 (2003), Elsevier, pp. 327-337.

[14] Frank H.P. Fitzek, Martin Reisslein. MPEG-4 and H.263 Video Traces for Network Performance Evaluation. IEEE Network, Vol. 15, No. 6, pages 40-54, November/December 2001.

[15] http://www-tkn.ee.tu-berlin.de/research/trace/trace.html

[16] W. Willinger, M.S. Taqqu, R. Sherman, D.V. Wilson. "Self-similarity through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level". IEEE/ACM Trans. on Networking, 1997. Available at http://www.argreenhouse.com/papers/wel/sigcomm93.pdf

[17] N. Ben Azzouna, C. Fricker, F. Guillemin, Modeling ADSL traffic on an IP backbone link. ALCOM-FT, Deliverable 1022, August 2003.

[18] G.Anastasi, L.Lenzini. "QoS provided by the IEEE 802.11 wireless LAN to advanced data applications: a simulation analysis". Department of information Engineering, University of Pisa, Via Diotisalvi 2, 56126 Pisa, Italy,. 2000

[19] Al. Klemm, C. Lindemann, M. Lohmann. "Traffic Modeling and Characterization for UMTS Networks". University of Dortmund, 2001. Available at http://www.cs.ucy.ac.cy/courses/EPL653/papers/

[20] Vv.aa. "Validation of the EuQoS system by simulation", DeliverableD 2.1.2, The EuQoS consortium

[21] Cisco Press. Traffic Analysis for Voice over IP, November 2001

[22] P.T. Brady, "A model for generating on-off speech patterns in two-way conversation". In Bell System Technical Journal, volume 48, pages 2445-2472, September 1969

[23] Chen-Neeand Chuah and Randy H. Katz, "Characterizing packet audio streams from internet multimedia applications". In ICC 2002 - IEEE International Conference on Communications, April 2002.

[24] Willinger W., Murad S., Sherman R., Wilson V.W. Self-Similarity Through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level. SIGCOMM '95 Cambrige, MA USA

[25] T. Yang and D. H. K. Tsang, "A Novel Approach to Estimating Cell Loss Probability in an ATM Multiplexer Loaded with Homogenous On-Off Sources", IEEE Trans. Comm., Vol. 43, No. 1, January 1995, pp. 117-126

[26] Vv.aa. "Integrated EuQoS system Software architecture for application use cases and API for application driving", Deliverable D4.1.1, The EuQoS consortium