Ph.D. Thesis

Quality of Service Technologies for Multimedia Applications in Next Generation Networks

Tatiana Onali

Advisors
Prof. Ing. Daniele Giusto
Prof. Ing. Luigi Atzori

University of Cagliari

Index

Introduction

The ever more demanding needs of current Telco users to be provided with a heterogeneous set of service types at differentiated quality of service (QoS) levels, have brought the network service providers to speed up the deployment of advanced network solutions, which are frequently referred to with Next Generation Networks (NGNs) [1]. These are characterized by their ability to simultaneously handle traffic flows at different levels so that IP Telephony, web browsing, grid computing, VoD and file sharing services (just to cite a few) are provided in the same network at the appropriate quality of service. This is made possible thanks to the implementation of capabilities within the network for state information management, resource allocation, bandwidth management, priority-based packet scheduling. These capabilities are manifested through sophisticated control plane algorithms and protocols for path computation, routing, and signalling, coupled with management plane capabilities for network administration and operations management.

On the one hand, NGN solutions allow the daring operators to expand the plethora of offered services and to be prepared for the coming unexpected user demands in the near future. In fact, the future networks should be prepared to interconnect multiple edge devices with different data formats and support multiple services requiring different bandwidth granularities and quality of service levels to suit the weird user needs. On the other hand, these solutions make the operation of network management more complex than in past networks, demanding for a shrewd setting of network parameters: preemption priority, parameters for effective bandwidth, class type parameters, administrative link weights, priority parameters, traffic engineering (TE) attributes and so on. This demands for network management procedures that drive the operator along the configuration of the QoS settings when using the full potentialities of the NGN networks [3, 4].

In this context, various quality management technologies have been proposed. They refer to two main different approaches, that are the flow-based one and the class-based one. According to the flow-based approach, a certain percentage of end-to-end resources has to be allocated for each traffic flow in the network on the basis of its specific QoS requirements; these resources have to be granted also in congestion or fault scenarios. This approach has been adopted by the Internet Engineering Task Force (IETF) in the Integrated Service (IntServ) [23] architecture and is also employed in MultiProtocol Label Switching with Traffic Engineering (MPLS-TE) [28] networks. On the other hand, the class-based approach allows scalability in traffic management enabling all network nodes to differentiate packet treatments per aggregates of traffic flows in respect of quality requirements. This approach is has been adopted by IETF in the Differentiated Service (DiffServ) [25] architecture. In the last years, these different schemes in to perform quality management have been coupled in a new technology, that is DiffServ-aware Traffic

Engineering (DS-TE) [29]. DS-TE is one of the most advanced technology which achieves quality of service in a scalable, flexible and dynamic way. It performs traffic engineering in a differentiated service environment by applying routing constrains with class granularity [30].

This work of thesis starts addressing the needs of NGN architectures focusing on one of most important requirements of DS-TE, that is an efficient bandwidth constraint model to allocate the available link resources in a per Class Type (CT) basis. Three are the most diffused bandwidth constraint models that have been proposed by IETF; these are the Maximum Allocation Model (MAM) [36], the Maximum Allocation with Reservation (MAR) [37] and the Russian Doll Model (RDM) [38]. Each of these models enables network operators to enforce different bandwidth constraints for different CTs with some variants in the degree of bandwidth isolation and sharing and in the need for preemption. Key parameters in these models are those from which the maximum allocable bandwidth depends. Their setting requires a deep analysis, among others, of the type of services operated in the network, the target QoS levels, their mapping in CT classes, the traffic load and the network topology.

Within this context, the bandwidth management problem is described with its importance towards QoS user needs fulfilment and two algorithmic solutions are presented. The first suggested methodology starts from the definition of the key performance indicators (KPIs) aimed at objectively quantifying the QoS level for each of the required services; these, together with the traffic load and network topology, are used to find the optimal mapping of service types into Class Types and the optimal bandwidth allocation for each of these. Herein, the optimality is expressed in terms of a cost function weighting both the expected satisfaction of the quality of service targets and the network resource utilization. Though the methodology is generic for a DS-TE architecture, the developed algorithm specifically refers to the RDM model. The effectiveness of the proposed solution is analyzed when considering a real context with combination of heterogeneous service types. The second proposed methodology relies on the genetic algorithms (GA) and aims to reduce the complexity of BC Model configuration procedure. A new fitness function is defined to create the final genetic population, that is the solution to the BC settings, weighting either the variation in the traffic load per link and the average length of paths.

After the analysis of management problems which are inherent to NGN architectures and the definition of technical solutions, the needs of specific scenarios with stringent QoS requirements have been considered to define ad-hoc application level solutions. In our work, we focus on the deployment of ad-hoc quality procedures for video streaming applications. Indeed, notwithstanding the progress reached in wireless access technologies and video coding techniques (e.g. MPEG-4, H.264), there are still many problems to overcome in video streaming, particularly in wireless networks. These problems are manly related to the high variability of the channel conditions, which are characterized by a bit error rate (BER) that fluctuates by orders of magnitude in less than a second. Moreover, due to the contention-based nature of common wireless access techniques, the radio interference and packet collision decrease rapidly the

channel throughput. It follows that in order to guarantee the reliability and the quality of video communication, the characteristics of video to be transmitted and the nature of the wireless channels have to be carefully analysed and the use of an adaptive rate control system is mandatory to dynamically modify the system parameters following the channel fluctuations.

In the recent past, many approaches have been proposed to address these problems. A common class of solution is related on link-layer reliability [47,48]. The work of Zhang et al. in [49] adopts the network-centric and the end-system centric solutions, which allow to satisfy data rate, delay bound, and packet loss requirements or to maximize the application-layer video quality without any QoS support. The authors in [50] studied the problem and proposed rate control schemes that avoid the degradation in the peak signal to noise ratio (PSNR) due to the reduction in the bit rate. A conditional retransmission and low-delay interleaving scheme was proposed in [51], in which the encoder buffer is used as part of the interleaving memory. In [52] the authors introduced a rate control mechanism based on a priori stochastic models of the source and the underlying channel. Such studies often do not take into account the dynamics of the playback buffer, which are very important to maintain continuous video playback. Furthermore, some of these frameworks are computationally intensive, making them unattractive for real-time applications.

In our work, we focus on the end-system centric approach which allows taking advantage of requiring minimum changes in the core network. The main challenge in this context is how to design efficient rate control algorithms that allow maximizing the video quality and channel utilization. The proposed rate control method focuses on the fluidity of the video playback by controlling the occupancy of the playback buffer so as not to exceed a desired rate of buffer starvation occurrences. While this constraint has been guaranteed, the encoder maximizes the source bit rate. Rate control is performed adaptively on the basis of a per-window basis approach, which has the advantage to reduce the fluctuations in the source bit rate, ensuring smooth variations in video quality and avoiding the “saw” effect that is typically observed in frame-based rate control.

Finally, in the context of QoS technologies, we addressed a hot problem of the current telecommunication network that is the security of multimedia systems. The development of Internet technologies involves remote access to dedicated zone and transmission of classified information, entailing new security problems. A robust control access system, in addition to privacy and data integrity, becomes essential condition to support the thriving of e-service, allowing to verify the identity of both the contracting parties and to protect the transmission of personal data.

The most part of current authentication systems, as alphanumeric passwords, are capable of guaranteeing the identity of user only (weak authentication). New client-server applications require a further security level. In fact, users want to verify the authenticity of service provider,

in order to avoid the risk of coming up against a shadow server. More advanced solutions have been proposed in order to achieve authentication of both user and server (mutual or strong authentication). They use encryption algorithms relied on a secret key, with which the server encrypts the data and generates a challenge message; only if user knows the secret key, it may decrypt the data and reply to challenge. These systems offer a good level of security, but require an hardware support, as encryption-calculators, tokens or smart cards, which are often expensive and incompatible with new network technologies. An alternative solution for generating challenge-response schemes is to use steganography, watermarking or image scrambling techniques. They allow to insert secret visual information into images using a key for mutual authentication.

Some visual login systems based on encryption algorithms have been proposed in the literature. For example, a technique of Visual Cryptography [60,62] provides each user with a transparency, i.e. a portion of visual information, which reveals a secret when combined with another sent by the server during the authentication session. Steganography may be used together with visual cryptography. An overview is given in [63]. The most widely known technique consists in replacing the last bit of each image pixel with a bit of secret information. These systems rely only on the secret keys exchange; one key is stored into the user terminal, while the other is sent by the server at each login request. So, both the user and the server keys are not very protected against theft or network sniffing attacks, allowing malicious clients or shadow servers to break the security system.

In this work, we propose a novel mutual authentication framework based on image scrambling: server and user share a secret key which is sent during registration phase only and which allows to encrypt and decrypt any visual information transmitted by server to client. This challenge-response scheme is coupled with a image-based authentication (IBA) technique described in [64]. In this way, a further protection is guaranteed in case of key theft, increasing security of user authentication without compromising simplicity and efficiency of authentication process. The proposed framework makes extensive use of the JPEG2000 standard both for image storage and processing, while relying on the properties of wavelet decomposition for the scrambling and transmission of visual information to the client.

The rest of this thesis is organized as follows. Chapter 1 presents the problem of QoS in NGN networks, analysing quality definitions and parameters. Chapter 2 describes the quality management technology, with particularly attention to the DS-TE as the reference architecture for the current NGNs. Chapter 3 illustrates the issues the operators have to address in DS-TE resources management, presents the proposed methodologies that guide on setting the bandwidth model constraints and provides an analysis of the applicability of the first methodology to a real context. Chapter 4 describes the ad-hoc solution for rate control in mobile video streaming. Finally, Chapter 5 presents the proposed mutual based authentication system.

Chapter 1

QoS in Multimedia Applications

Telecommunication networks are evolving toward multiservice, multidomain and multivendor architectures which are oriented to the provisioning of Quadruple-Play services: voice, data and video (Triple-Play) are offered on the same IP network infrastructure together with multimedia applications over wireless 3G networks [1]. From the point of view of users, this scenario offers the opportunity of accessing to a wide range of services from any wired or wireless terminal, enjoying high personalization levels and always-on availability. From the point of view of network operators, the ability to include in the same quadruple-play offer all different services, from web browsing to Voice over IP applications, means a substantial reduction of operational costs, making full use of a flexible and innovative platform, relied on the pre-existing backbone infrastructure. On the other hand, the deployment of multiservice networks brings new challenges including Quality of Service (QoS) issues and network policy control. The network traffic has to be prioritized, examining in some details the IP packets and identifying what specific requirements have to be guarantees.

In this chapter, Quadruple-Play applications are presented and the QoS parameters which are needed to differentiate network behaviour and to grant all specific service requirements are defined.

1.1 Quadruple-Play Applications

The traditional IP networks rely on *best-effort* datagram transmission [2]. According to this approach, packets from a source are sent to a destination with no guarantee of delivery. When some guarantees are required, the TCP protocol is implemented. It will trade packet delay for correct reception by retransmitting those packets that fail to reach the destination. For traditional communication applications such as FTP and Telnet in which correct delivery is the main important requirement, the best effort approach coupled with TCP protocol is satisfactory.

However, new classes of applications with higher Quality of Service (QoS) requirements than the traditional one has begun to appear on the Internet. Indeed, current telecommunication scenario is dominated by next generation networks (NGN), that are multiservice, multidomain and multivendor architectures oriented to the provisioning of Quadruple-Play services. They offer voice, data and video (Triple-Play) on the same IP network infrastructure together with multimedia applications over wireless 3G networks. Examples of new classes of NGN applications are video teleconferencing, video-on-demand, and distributed simulation. While these applications can operate at the same level using best-effort delivery, TCP protocol implementation is not an acceptable trade-off which results in reduced quality of the received information and, potentially, inefficient use of bandwidth. To remedy this problem, adequate Quality of Service policies have to be implemented [3, 4].

The major challenge to provide adequate Quality of Service (QoS) for different services in emerging wired and wireless IP-based networks is a detailed knowledge of the performance requirements for particular services and applications [5]. The starting point for deriving these performance requirements must be the user. The key parameters impacting the user in its experience in the use of a service are the following:

- **Delay**: this parameter has various meanings, including the time taken to establish a particular service from the initial user request and the time to receive specific information once the service is established. Delay has a very direct impact on user satisfaction depending on the application, and includes delays in the terminal, network, and any servers. Note that from a user point of view, delay also takes into account the effect of other network parameters such as throughput.

- **Delay variation (or jitter)**: is generally included as a performance parameter since it is very important at the transport layer in packetised data systems due to the inherent variability in arrival times of individual packets. However, services that are highly intolerant of delay variation will usually take steps to remove (or at least significantly reduce) the delay variation by means of buffering, effectively eliminating delay variation as perceived at the user level (although at the expense of adding additional fixed delay).

- **Information loss**: has a very direct effect on the quality of the information finally presented to the user, whether it be voice, image, video or data. In this context, information loss is not limited to the effects of bit errors or packet loss during transmission, but also includes the effects of any degradation introduced by media coding for more efficient transmission (e.g. the use of low bit-rate speech codecs for voice).

On the basis of the transmission delay behaviour, applications can be classified into two main categories: *elastic applications* and *real-time or streaming applications,* as shown in Fig. 1.1 [6].

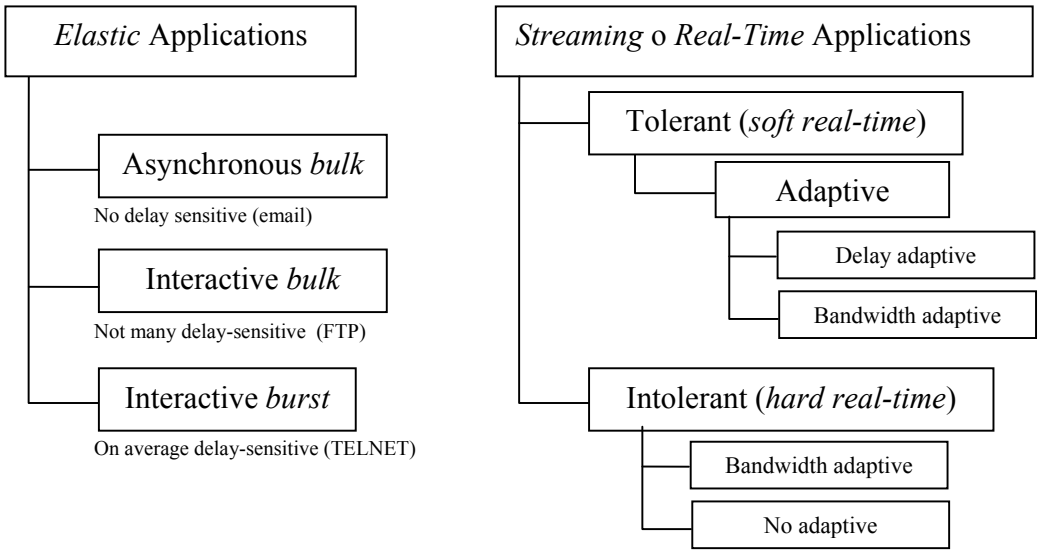


Fig. 1.1 Elastic and real-time applications

1.1.1 Elastic Applications

Elastic applications [6] are those which typically are offered in the Internet, such as e-mail, web browsing, FTP, TELNET, etc. They will always wait for data to arrive. It is not that these applications are insensitive to delay; to the contrary, significantly increasing the delay of a packet will often harm the application's performance. Rather, the key point is that the application typically uses the arriving data immediately, rather than buffering it for some later time, and will always choose to wait for the incoming data rather than proceed without it. Because arriving data can be used immediately, these applications do not require any a priori characterization of the service in order for the application to function. Generally speaking, it is likely that for a given distribution of packet delays, the perceived performance of elastic applications will depend more on the average delay than on the tail of the delay distribution.

Elastic applications may be divided in the three following subcategories with different delay expectations:

- **Interactive burst:** are characterized by instantaneous peaks in the bit-rate which considerably varies with respect to the average value. They are on the average delay-sensitive. Examples of these applications are Telnet, X, NFS.

- **Interactive bulk transfer:** are not many delay-sensitive. These applications transfer high data quantity with no constraints on time delivery and witch are transmitted with quite constant bit-rate. Examples of bulk applications are FTP or HTTP traffic.

- **Asynchronous bulk transfer:** are the less delay-sensitive applications, such as electronic mail or FAX. In this case, the network is usually able to grant a quality level adequate to the use expectations.

The delay requirements of these elastic applications vary from rather demanding for interactive burst applications to rather lax for asynchronous bulk transfer, with interactive bulk transfer being intermediate between them.

A network should offer a best-effort service for use with elastic applications, also known *as as-soon-as-possible* or ASAP service. Best-effort service is not subject to admission control.

1.1.2 Real-Time Applications

For real-time applications [6], the transmitted data is of any value only if it arrives within a certain time. Often, this class of applications belongs to the class of playback applications, which consist of a source that transforms a signal into data packets and transmits these over the network. At the receiver's site, the packets arrive potentially disordered and with variable delays. The receiver then tries to reconstruct the source data from the packets and attempts to play back the signal as faithfully as possible with some fixed offset delay from the departure time. An application must find a suitable a priori estimate of this offset delay. It can either be provided by a network service commitment containing a delay bound or by observation of the previously received traffic.

The performance of a playback application is determined by the presentation *latency* and *fidelity*, both of which are affected by the delay behaviour of the network. First, the latency of an application depends on the offset delay predictions about future packet delays. Secondly, the fidelity of the playback can be distorted by individual packet delays exceeding the predictions.

The sensitivity to loss of fidelity leads to two application classes, each requiring a particular service class:

- **Intolerant Applications.** Intolerant systems require absolutely faithful playback fidelity and can be found for example with circuit emulation. Intolerant applications must choose a fixed offset delay, which is larger than the maximum expected packet delay. Consequently, a reliable upper bound on the maximum packet delay is required. A service that enforces such a reliable bound is called a *guaranteed service*, and symbolizes the appropriate service model for intolerant playback applications.

- **Tolerant Applications.** Tolerant applications need not set their offset delay greater than the absolute maximum delay, since they can tolerate some late packets. Moreover, instead of

using a single fixed value for the offset delay, they can attempt to reduce their latency by varying their offset delays in response to the actual packet delays experienced in the recent past. We call applications which vary their offset delays in this manner adaptive playback applications. For tolerant applications, a service model called predictive service was proposed. It supplies a fairly reliable, but not perfectly reliable, delay bound. This bound, in contrast to the bound in the guaranteed service, is not based on worst case assumptions on the behaviour of other flows, but it might be computed with properly conservative predictions about the behaviour of other flows. In order to provide a delay bound, the nature of the traffic from the source must be characterized, and there must be some admission control algorithm which insures that a requested flow can actually be accommodated. A fundamental point of overall architecture is that traffic characterization and admission control are necessary for these real-time delay bound services. Many audio and video applications which can adjust their coding scheme and thus can alter the resulting data generation process depending on the network service available. This alteration of the coding scheme will present a trade-off between fidelity (of the coding scheme itself, not of the playback process) and the bandwidth requirements of the flow. Such *rate-adaptive* playback applications have the advantage that they can adjust to the current network conditions not just by resetting their playback point but also by adjusting the traffic pattern itself. For rate-adaptive applications, the traffic characterizations used in the service commitment are not immutable. We can thus augment the service model by allowing the network to notify (either implicitly through packet drops or explicitly through control packets) rate-adaptive applications to change their traffic characterization.

1.1.3 Performance considerations for different applications

In Table 1.I, a classification of the main services which may be implemented in a multiservice network is proposed. It relies on the considerations on network delay which have been discussed in the previous subsection. In the following of this section, the requirements of some applications are described.

Audio

In [6,7], audio services are classified into five levels of quality and a mapping to various applications is proposed. Some specific considerations are given in the following.

- **Conversational voice.** Requirements for conversational voice are heavily influenced by one-way delay. In fact, there are two distinct effects of delay. The first is the creation of echo in conjunction with two-wire to 4-wire conversions or even acoustic coupling in a terminal. This

Table 1.I Applications and real-time constraints

Applications	**Non real-time**	**Soft real-time**	**Hard real-time**
Voice			x
Videotelephony			x
Videoconferences			x
Interactive real-time gaming		x	
Interactive non real-time gaming	x		
Telemetry	x		
Bidirectional telemetry		x	
TELNET	x		
Audio streaming		x	
IPTV: video on demand		x	
IPTV: broadcast TV			x
FTP	x		
Vocal messaging		x	
Web-browsing	x		
On-line transactions (e.g. E-commerce)	x		
E-mail (server-to-server)	x		
Fax	x		
Low priority transactions (e.g. SMS)	x		
E-mail	x		
DNS	x		
Control		x	
IP radio			x
Telemedicine			x

begins to cause increasing degradation to voice quality for delays of the order of tens of milliseconds, and echo control measures must be taken at this point [8]. The second effect occurs when the delay increases to a point where it begins to impact conversational dynamics, i.e. the delay in the other party responding becomes noticeable. This occurs for delays of the order of several hundred milliseconds [9]. However, the human ear is highly intolerant of short-term delay variation (jitter). As a practical matter, for all voice services, delay variation due to variability in incoming packet arrival times must be removed with a de-jittering buffer. Requirements for information loss are influenced by the fact that the human ear is tolerant to a certain amount of distortion of a speech signal. In IP-based transmission systems a prime source of voice quality degradation is due to the use of low bit-rate speech compression codecs and their performance under conditions of packet loss.

- **Voice messaging.** Requirements for information loss are essentially the same as for conversational voice (i.e. dependent on the speech coder), but a key difference here is that there is more tolerance for delay since there is no direct conversation involved. The main issue, therefore becomes one of how much delay can be tolerated between the user issuing a command to replay a voice message and the actual start of the audio. There is no precise data on this, but based on studies related to the acceptability of stimulus-response delay for telecommunications services, a delay of the order of a few seconds seems reasonable for this application. In fact, a distinction is possible between recording and playback, in that user reaction to playback is likely to be the more stringent requirement.

- **Streaming audio.** Streaming audio is expected to provide better quality than conventional telephony, and requirements for information loss in terms of packet loss will be correspondingly tighter. However, as with voice messaging, there is no conversational element involved and delay requirements for the audio stream itself can be relaxed, even more so than for voice-messaging, although control commands must be dealt with appropriately.

Video

In [6,7], video services are classified into six levels of quality and a mapping to various applications is proposed. Some specific considerations are given in the following.

- **Videophone.** Videophone as used here implies a full-duplex system, carrying both video and audio and intended for use in a conversational environment. As such, in principle the same delay requirements as for conversational voice will apply, i.e. no echo and minimal effect on conversational dynamics, with the added requirement that the audio and video must be synchronised within certain limits to provide *lip-synch*. Once again, the human eye is tolerant to some loss of information, so that some degree of packet loss is acceptable depending on the specific video coder and amount of error protection used. It is expected that the latest MPEG-4 video codecs will provide acceptable video quality with frame erasure rates up to about 1%.

- **One-way video.** The main distinguishing feature of one-way video is that there is no conversational element involved, meaning that the delay requirement will not be so stringent, and can follow that of streaming audio.

Data

From a user point of view, a prime requirement for any data transfer application is to guarantee essentially zero loss of information. At the same time, delay variation is not generally noticeable to the user, although there needs to be a limit on synchronisation between media streams in a multimedia session (e.g. audio in conjunction with a white-board presentation). The different applications therefore tend to distinguish themselves on the basis of the delay which can be tolerated by the end-user from the time the source content is requested until it is presented to the user.

- **Web-browsing.** In this category we refer to retrieving and viewing the HTML component of a Web page, other components e.g. images, audio/video clips are dealt with under their separate categories. From the user point of view, the main performance factor is how quickly a page appears after it has been requested. Delays of several seconds are acceptable, but not more than about 10 seconds.

- **Bulk data.** This category includes file transfers, and is clearly influenced by the size of the file. As long as there is an indication that the file transfer is proceeding, it is reasonable to assume somewhat longer tolerance to delay than for a single Web-page.

- **High-priority transaction services (E-commerce).** The main performance requirement here is to provide a sense of immediacy to the user that the transaction is proceeding smoothly, and a delay of no more than a few seconds is desirable.

- **Command/control.** Clearly, command/control implies very tight limits on allowable delay, much less than a second. Note that a key differentiator from conversational voice and video services with similar low delay requirements is the zero tolerance for information loss.

- **Still image.** This category includes a variety of encoding formats, some of which may be tolerant to information loss since they will be viewed by a human eye. However, given that even single bit errors can cause large disturbances in other still image formats, it is argued that this category should in general have zero information loss. However, delay requirements for still image transfer are not stringent and may be comparable to that for bulk data transfer, given that the image tends to be built up as it is being received, which provides an indication that data transfer is proceeding.

- **Interactive games.** Requirements for interactive games are obviously very dependent on the specific game, but it is clear that demanding applications will require very short delays of the order of a fraction of a second, consistent with demanding interactive applications.

- **Telnet.** Telnet is included here with a requirement for a short delay of a fraction of a second in order to provide essentially instantaneous character echo-back.

- **E-mail (server access).** E-mail is generally thought to be a store and forward service which, in principle, can tolerate delays of several minutes or even hours. However, it is important to differentiate between communications between the user and the local email server and server, to server transfer. When the user communicates with the local mail server, there is an expectation that the mail will be transferred within a few seconds.

- **Instant messaging.** Instant messaging primarily relates to text, but can also include audio, video and image. In any case, despite the name, it is not a real-time communication in the sense of conversational voice, and delays of several seconds are acceptable.

Background applications

In principle, the only requirement for applications in this category is that information should be delivered to the user essentially error free [6]. However, there is still a delay constraint, since data is effectively useless if it is received too late for any practical purpose.

- **Fax.** Fax is included in this category since it is not normally intended to be an accompaniment to highly interactive real-time communication. Nevertheless, for so-called *real-time* fax there is an expectation in most business scenarios that a fax will be received within about 30 seconds. Delay for store and forward fax can be much higher. Note that fax does not require zero information loss.

- **Low priority transaction services.** An example in this category is Short Message Service (SMS). 10s of seconds are an acceptable delivery delay value.

- **Email (server-to-server).** This category is included for completeness, since as mentioned earlier, the prime interest in email is in the access time.

1.2 The Quality of Service

Quality of Service (QoS) refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate. QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications. A network monitoring system

must typically be deployed as part of QoS, to insure that networks are performing at the desired level.

Several QoS definitions have been proposed in the literature [10, 11]. The International Telecommunication Union (ITU) has defined four quality parameters categories: support, operability, serveability and security [12]. In [13], quality is specified as "*the collective effect of service performances, which determine the degree of satisfaction of a user of a service*". This general definition means that a single QoS measure of is not possible. In a multi-service and multi-domain network architecture, QoS requirements can be related to various aspects of both application and network levels. In [14], three notions of QoS are specified that are *perceived*, *offered* and *intrinsic*. Quality can be evaluated from the point of view of the end-user, as perceived quality which refers to the experience in the use of a service, or from the point of view of the operators, as *offered* quality which refers to the policies of service provisioning, the sustained costs and the capacity to maintain service availability [15]. It can be also *intrinsic* if refers to technical network performance parameters, such as delay, jitter, packet loss, and throughput. It can be specified either quantitatively or qualitatively.

Across a heterogeneous NGN network, three basic levels of end-to-end QoS can be provided [16], that are:

- **Best-effort service.** Also known as lack of QoS, best-effort service is basic connectivity with no guarantees. This is best characterized by FIFO queues, which have no differentiation between flows.

- **Differentiated service** (also called soft QoS). Some traffic is treated better than the rest (faster handling, more average bandwidth, and lower average loss rate). This is a statistical preference, not a hard and fast guarantee. This is provided by classification of traffic and the use of QoS tools such as WFQ and WRED.

- **Guaranteed service** (also called hard QoS)**.** This is an absolute reservation of network resources for specific traffic. This is provided through QoS tools RSVP and CBWFQ.

1.3 Key performance parameters (KPI)

In order to fulfil QoS objectives in NGN network, it is necessary to define a set of key performance indicators (KPI). A KPI is a measurable metric which allows for characterizing QoS requirements and evaluating network performance. It provides for a quantitative and objective solution to compare the obtained quality performance with the desired ones and may be used for both traffic classification and network analysis. KPIs are divided into two important service categories [13]:

- **End-to-end metrics** (or end-user metrics): these provide an evaluation of the network performance as it is perceived by the network end-user;
- **Network metrics**: these concern the network administrator and monitor the behaviour of the system during the service.

The former provide a direct means to evaluate the grade of satisfaction of the network user. The latter do not straight provide an indication of the QoS provided by the network, but can indirectly affect the end-user metrics. On the other hand, they allow the operator to keep under control the network resources allocation and, thus, to fully exploit them.

In the following, two KPI categories are described that are the IP packet information transfer performance parameters and the IP service availability parameters. These KPI, together with parameters for network access, are used in the service level agreements (SLAs) definition (see section 1.4), as shown in Fig. 1.2.

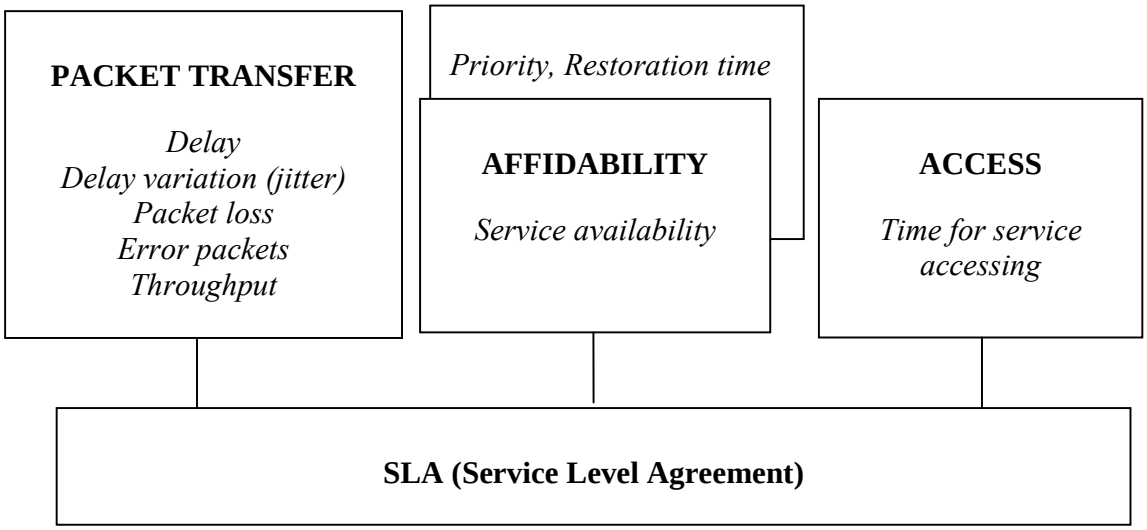


Fig. 1.2 KPI classification

1.3.1 IP packet information transfer performance parameters

Most of the performance parameters are defined over sets of packets called populations of interest [17]. For the end-to-end case, the population of interest is usually the total set of packets being sent from SRC to DST. The measurement points in the end-to-end case are the MP at the SRC and DST. For a basic section relative to a particular SRC and DST pair, the population of interest at a particular permissible ingress MP is that set of packets being sent from SRC to DST that are routed into the basic section across that specific MP. This is called the specific-ingress

case. The total population of interest for a basic section relative to a particular SRC and DST pair is the total set packets from SRC to DST that are delivered into the section across any of its permissible ingress MP. This is called the ingress-independent case. Each of these IP performance parameters are defined without reference to a particular packet type (TOS, protocol, etc.) Performance will differ by packet type and any statement about measured performance should include information about which packet type or types were included in the population.

Definitions of IP packet information transfer performance parameters are done in [17, 18, 19, 20]. In the following, some of these are summarized.

- **IP packet transfer delay (IPTD):** IP packet transfer delay is defined for all successful and errored packet outcomes across a basic section. According to the definition in [15]:

IPTD is the time, ($t_2 - t_1$) between the occurrence of two corresponding IP packet reference events, ingress event $IPRE_1$ at time t_1 and egress event $IPRE_2$ at time t_2, where ($t_2 > t_1$) and ($t_2 - t_1$) $\leq T_{max}$. If the packet is fragmented, t_2 is the time of the final corresponding egress event. The end-to-end IP packet transfer delay is the one-way delay between the MP at the SRC and DST.

Alternatively, the Round Trip Time (RTT) may be considered. RTT, also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. It is defined as follows:

RTT = 2*(*one-way delay*) + switching time

- **Mean IP packet transfer delay:** Mean IP packet transfer delay is the arithmetic average of IP packet transfer delays for a population of interest.

- **IP packet delay variation (IPDV):** The variations in IP packet transfer delay are also important. Streaming applications might use information about the total range of IP delay variation to avoid buffer underflow and overflow. Variations in IP delay will cause TCP retransmission timer thresholds to grow and may also cause packet retransmissions to be delayed or cause packets to be retransmitted unnecessarily. One or more parameters that capture the effect of IP packet delay variations on different applications may be useful. It may be appropriate to differentiate the (typically small) packet-to-packet delay variations from the potentially larger discontinuities in delay that can result from a change in the IP routing.

- **IP packet loss ratio (IPLR):** IP packet loss ratio is the ratio of total lost IP packet outcomes to total transmitted IP packets in a population of interest. It is defined as follows:

$$IPLR = \frac{N_{loss}}{N_{transmitted}}$$

The packet loss ratio affects on quality of connection. The applications can react on packet loss different ways. The applications can be divided to similar categories also by required bandwidth and delay.

- *Fragile*: if the packet loss exceeds certain threshold, the value of application is lost.
- *Tolerant*: the application can tolerate packet loss, but the higher the packet loss the lower is the value of application. There are certain threshold levels which are critical.
- *Performance*: the application can tolerate even very high packet loss ratio but its performance can be very low in high packet loss ratio.

- **IP packet error ratio (IPER)**: IP packet error ratio is the ratio of total errored IP packet outcomes to the total of successful IP packet transfer outcomes plus errored IP packet outcomes in a population of interest.

$$IPER = \frac{N_{erroneous}}{N_{successful} + N_{erroneous}}$$

- **Spurious IP packet rate (SIPR):** Spurious IP packet rate at an egress MP is the total number of spurious IP packets observed at that egress MP during a specified time interval divided by the time interval duration (equivalently, the number of spurious IP packets per service-second).

- **Skew:** the skew is a kind of delay that can occur between two data flows which are transmitted by the same terminal. For example, in IPTV applications, synchronization between audio and video streams is required.

1.3.2 IP Service Availability Parameters

IP service availability is applicable to end-to-end IP service and basic sections. An availability function serves to classify the total scheduled service time for an IP service into available and unavailable periods. On the basis of this classification, both percent IP availability and percent IP unavailability are defined.

- **Percent IP service availability (PIA):** The percentage of total scheduled IP service time that is categorised as available using the IP service availability function.

- **Percent IP service unavailability (PIU):** The percentage of total scheduled IP service time that is categorised as unavailable using the IP service availability function.

$$PIU = 100 - PIA$$

In Table 1.II and 1.III, values of some of the considered KPIs are done for audio and video applications and data applications, respectively.

1.4 Service Level Agreement

There is a trend toward service outsourcing, where providers outsource all or a portion of their service to a third party. In order to assure the high quality of the offered communication services to customers, each party must guarantee the availability and performance of the service component it provides. Customers are not concerned about the composition of a service Customers are not concerned about the composition of a service, but only about the QoS. QoS expectations are driving customers to negotiate specific QoS levels with their service providers. This is increasingly done through service level agreements (SLAs) [21, 22]. An SLA is defined as a contract between the service provider and customer that specifies the QoS level that can be expected. It includes the expected behaviour of the service and the parameters for QoS. The efficient management of SLAs is a new challenge and very important issue in Internet service management. Research issues on SLA management are briefly summarized:

- SLA parameter definition: There are few common standards for service level parameters: what they are and how their values are computed for SLAs. This concerns the definition of service level parameters such as availability, reliability, latency, and loss for SLA.

- SLA measurement: This issue deals with how to accurately measure the QoS that service providers deliver to their customers. Valuable network and application performance statistics can serve as the basis for effective SLA management.

Some research has been done on defining SLA parameters. The IP Performance Working Group of the Internet Engineering Task Force (IETF) has been working on the identification of Internet service metrics. These Internet service metrics are:

- Framework for IP Performance Metrics
- IPPM Metrics for Measuring Connectivity
- A One-Way Delay Metric for IPPM
- A One-Way Packet Loss Metric for IPPM

- A Round-Trip Delay Metric for IPPM

To remain competitive, service providers must offer guarantees not just in terms of availability, but also in terms of performance guarantees such as response time and throughput. There are a number of parameters used in SLAs today. Most are customer support and reliability parameters. Some of the most commonly defined parameters include:

- Customer support. These include the typical helpdesk problem of reporting and problem resolution guarantees. Examples include a single point of contact assigned to the customer and problem resolution within 48 hours of reporting.

- Reliability. Reliability metrics consist of availability guarantees over a period of time. For example, the Web server will be available 99.999 percent of the time it is accessed over a one-year period.

- Service provisioning. This guarantees that the service will be provisioned in a certain manner.

In addition to reliability and support metrics, service performance metrics are important for business-critical applications. Currently, there are entire new sets of metrics being discussed in the industry, including performance, utilization and security metrics. They include:

- Performance. Performance metrics are generally characterized in terms of response time and throughput.

- Response time. This metric defines the maximum response time a service is permitted when handling user requests.

- Throughput. This metric defines the rate at which data is delivered to the customer.

- Utilization. This metric defines the maximum service utilization allowed at which a service will perform within guaranteed response times and throughput. An example of this metric is that the system will support 32 simultaneous users during peak hours.

Table 1.II Performance targets for audio and video applications [5]

Medium	**Application**	**Degree of symmetry**	**Typical data rates**	**Key performance parameters and target values**			
				One-way delay	**Delay variation**	**Information loss (Note 2)**	**Other**
Audio	Conversational voice	Two-way	4-64 Kbit/s	<150 ms preferred (Note 1) <400 ms limit (Note 1)	< 1 ms	< 3% packet loss ratio (PLR)	
Audio	Voice messaging	Primarily one-way	4-32 Kbit/s	< 1 s for playback < 2 s for record	< 1 ms	< 3% PLR	
Audio	High quality streaming audio	Primarily one-way	16-128 Kbit/s (Note 3)	< 10 s	<< 1 ms	< 1% PLR	
Video	Videophone	Two-way	16-384 Kbit/s	< 150 ms preferred (Note 4) <400 ms limit		< 1% PLR	Lip-synch: < 80 ms
Video	One-way	One-way	16-384 Kbit/s	< 10 s		< 1% PLR	

NOTE 1 – Assumes adequate echo control.
NOTE 2 – Exact values depend on specific codec, but assumes use of a packet loss concealment algorithm to minimise effect of packet loss.
NOTE 3 – Quality is very dependent on codec type and bit-rate.
NOTE 4 – These values are to be considered as long-term target values which may not be met by current technology.

Table 1.III Performance targets for data applications [5]

Medium	**Application**	**Degree of symmetry**	**Typical amount of data**	**Key performance parameters and target values**		
				One-way delay (Note)	**Delay variation**	**Information loss**
Data	Web-browsing – HTML	Primarily one-way	~10 KB	Preferred < 2 s /page Acceptable < 4 s /page	N.A.	Zero
Data	Bulk data transfer/retrieval	Primarily one-way	10 KB-10 MB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero
Data	Transaction services – high priority e.g. e-commerce, ATM	Two-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	Command/control	Two-way	~ 1 KB	< 250 ms	N.A.	Zero
Data	Still image	One-way	< 100 KB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero
Data	Interactive games	Two-way	< 1 KB	< 200 ms	N.A.	Zero
Data	Telnet	Two-way (asymmetric)	< 1 KB	< 200 ms	N.A.	Zero
Data	E-mail (server access)	Primarily one-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	E-mail (server to server transfer)	Primarily one-way	< 10 KB	Can be several minutes	N.A.	Zero
Data	Fax	Primarily one-way	~ 10 KB	< 30 s/page	N.A.	$<10^{-6}$ BER
Data	Low priority transactions	Primarily one-way	< 10 KB	< 30 s	N.A.	Zero
NOTE – In some cases, it may be more appropriate to consider these values as response times.						

Chapter 2

Architectures for Next Generation Network

The current Internet user demands for a plethora of services larger than that of only few years ago, pushing the network service providers to speed up the deployment of advanced network solutions, which are often referred to as Next Generation Networks (NGNs) [1]. These are characterized by their ability to simultaneously handle traffic flows at different levels so that IP Telephony, web browsing, grid computing, video on demand and file sharing services are provided in the same network at the appropriate QoS level. This is made possible thanks to the implementation of capabilities within the network for constraint-based routing, state information management, resource allocation, bandwidth management, priority-based packet scheduling. These capabilities are manifested through sophisticated control plane algorithms and protocols for path computation, routing, and signalling, coupled with management plane capabilities for network administration and operations management.

In this chapter, the most common used technology for implementing Next Generation Network with QoS policies are presented.

2.1 The traditional IP Networks

Traditional IP networks rely on best effort protocols. They provide all services with the same level of performance, with no guarantees on packet delivery, ordering and prioritization. IP protocol is connectionless: routing decisions are taken independently hop-by-hop on the basis of the destination address. Due to its simplicity, IP protocol has been extensively deployed, also in next generation networks. However, the best effort approach proved to be effective until the diffusion of new range of applications that have stringent quality of service requirements.

Examples of these applications are Voice over IP (VoIP) and Video on Demand (VoD). They are time sensitive and do not tolerate delays. Implementing bandwidth overprovisioning to grant QoS requirements results non efficient. The deployment of a more flexible quality-oriented network management is required. In particular, to accomplish all QoS functionalities in a multiservice IP network two main objectives have to be achieved. They are:

- allow the network to perform traffic management in a class-based scheme in order to enable all network nodes to differentiate packet treatments in respect of quality requirements;

- provide fault-tolerance proprieties by allocating a certain percentage of end-to-end resources which will be granted also in congestion or fault scenarios.

The first efforts to provide quality of service in IP networks were based on a flow-based model, called Integrated Service (IntServ) [23]. IntServ was proposed by IETF. It relies on RSVP (ReSerVation Protocol) [24] protocol to lend *connection-oriented* properties in the IP *connectionless* environment. The RSVP signalling protocol was used to distribute the requests to the nodes in the network, and state needed to be maintained for each flow at every hop along the way. However, this approach did not have great success. Indeed, when millions of flows traversing IP networks, IntServ proved to be unscalable and overly complex. Further, it accomplishes just the second QoS functionality which has been previously defined. In order to solved the scalabity problem, IETF proposed a further technology, that is Differentiated Service (DiffServ) [25]. DiffServ approaches the problem of QoS by dividing traffic into a small number of classes and allocating network resources on a per-class basis. It resulted more efficient than IntServ, above all in backbone networks. Indeed, DiffServ offers high scalability properties and avoids the need for a signalling protocol, but, on the contrary of IntServ, it accomplishes only the first described QoS functionality. Another adoptable solution to grant QoS performance in IP network is the MultiProtocol Label Switching with Traffic Engineering (MPLS-TE) [26-28]. It sets up label-switched-paths (LSPs) along links with available resources, ensuring that bandwidth is always available for a particular flow and avoiding congestion both in the steady state and in failure scenarios. As IntServ, MPLS-TE is a flow-based approach, which does not perform classification but just end-to-end fault tolerance guarantees. Finally, a new technology has been recently defined by IETF, that is DiffServ aware Traffic Engineering (DS-TE) [29,30]. It performs DiffServ classification in a MPLS-TE network, coupling the advantages of both DiffServ and MPLS-TE and achieving all QoS functionalities. DS-TE is the most advanced technology which achieves quality of service in a scalable, flexible and dynamic way, satisfying all NGN requirements.

2.2 DiffServ

DiffServ [25] supports quality of service in a scalable fashion. It adopts a class-based approach to differentiate service treatment in the network. The ingress traffic is aggregated into a small number of Class of Service (CoS), each corresponding to specific quality requirements. To avoid the need for a signalling protocol, the class is marked directly on the packet, in the 6-bit DiffServ Code Point (DSCP) field. The DSCP field is part of the original type of service (ToS) field in the IP header. The IETF redefined the meaning of the little-used ToS field, reserving 6 bits to DSCP field and 2 bits to Explicit Congestion Notification (ECN) field, as shown in Fig 2.1.

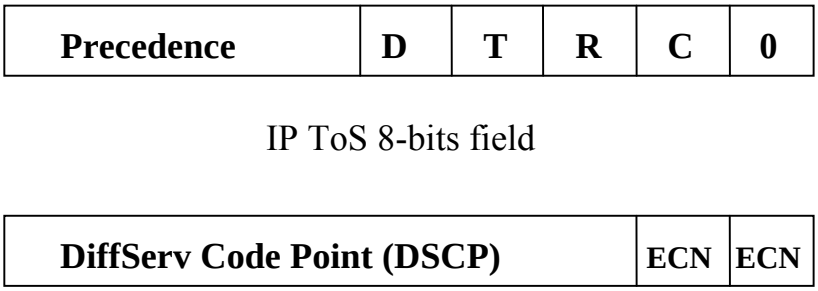


Fig. 2.1 ToS and DSCP fields

The DSCP specifies the per-hop behaviour (PHB) of the packet in the network nodes in terms of the scheduling and drop preference. A DiffServ domain can support up to 64 PHB. The IETF defined a set of 14 standard PHBs, each corresponding to a specific DSCP [31,32]. They are the following:

- **Best effort (BE).** Traffic receives no special treatment.

- **Expedited forwarding (EF)**. Traffic encounters minimal delay and low loss. From a practical point of view, this means a queue dedicated to EF traffic for which the arrival rate of packets is less than the service rate, so delay, jitter and loss due to congestion is unlikely. Voice and video streams are typical examples of traffic mapped to EF: they have constant rates and require minimal delay and loss.

- **Assured forwarding (AF) PHBs**. Each AF PHB is defined by a queue number and a drop preference. The IETF recommends using four different queues with three levels of preference each, yielding a total of twelve distinct AF PHBs. The convention for naming the AF PHBs is AF*xy*, where *x* is the queue number and *y* is the level of drop preference. Thus, all

packets from AF*1y* will be put in the same queue for forwarding, ensuring that packets from a single application cannot be reordered if they differ only in the drop preference. The AF PHBs are applicable for traffic that requires rate assurance but that does not require bounds on delay or jitter.

A DiffServ domain performs two main typologies of operations that are the *traffic classification* and the *traffic conditioning*. The *classifier* selects packets based on the combination of one or more predefined set of DSCPs. Note that although the IETF defined recommended DSCP values for each of the standard PHBs, network operators can modify the mapping between PHB and DSCP or define non-standard PHBs. Each router sorts the packets into queues based on the DSCP. The queues might get different treatment based on their priority, share of bandwidth, and discard policies. Further, in order to deliver service level agreements (SLA), each DiffServ edge router implements *traffic conditioning* functions, that are the following:

- *Metering* - Monitors the traffic pattern of each flow against the traffic profile. For out-of-profile traffic the metering function interacts with other components to either remark, or drops the traffic for that flow.

- *Shaping* – The routers control the forwarding rate of packets so that flow does not exceed the traffic rate specified by its profile. The shapers ensure fairness between flows that map to the same CoS, and control the traffic flow to avoid congestion.

- *Policing* – At the ingress edge routers, the incoming traffic is classified into aggregates. These aggregates have to be treated according to the SLA. The out-of-profile traffic is either dropped at the edge or is remarked with a different PHB.

- *Marking* – A marker receives the incoming packets from the classifier and the state information from a packet meter and marks the DSCP field of each packet with a specific value**.**

2.3 MPLS and Traffic Engineering

MPLS with Traffic Engineering [28] is another advanced solution to grant QoS performance in IP network. Unlike DiffServ, MPLS is a flow-based protocol which represents the convergence of two fundamentally different approaches in data networking: datagram and virtual circuit. Traditionally IP forwarding is based on the datagram model: routing protocols precalculate the paths to all destination networks by exchanging routing information and each packet is independently based on its destination address. Asynchronous transfer mode (ATM) and Frame Relay (FR) technologies, on the other hand, are connection oriented: a virtual circuit is set up explicitly by a signalling protocol before packets are transmitted into the network. MPLS integrates IP and ATM technologies implementing the paradigm of *label switching* [33]. It marks

the incoming traffic flows with a label which corresponds to the forwarding along a specific Label Switching Path (LSP). Subsequently the definition of MPLS, the growth of Internet technologies has made the need of IP/ATM integration always less important. However, *label switching* has kept a key role in the Internet thanks to its ability to implement traffic engineering (TE) policies. TE refers to the process of optimizing the utilization of network resources through careful distribution of traffic, achieving end-to-end guaranteed QoS.

2.3.1 MPLS

Fig. 2.2 shows a simple MPLS domain [26,34] with six label switch routers (LSR) and two label switch paths (LSP). The MPLS edge routers are called E-LSR (Edge-LSR), while the intermediate routers are LSR. The LSPs are unidirectional: for each pair of LSRs, the LSR that transmits with respect to the direction of data flow is said to be upstream, whereas the LSR that receives is downstream. For example, LSR B in Fig 2.2 is upstream of LSR C, while LSR C is downstream of LSR B. Each LSP has an ingress E-LSR, that is the upstream E-LSR, and an egress E-LSR, that is the downstream E-LSR. In the example of Fig 2.2, the E-LSRs of upstream and downstream for LSP1 are E-LSR B and E-LSR A, respectively. The operations of an E-LSR are different from those of an intermediate LSR in many aspects. The E-LSR represent the interface between the MPLS domain and the exterior domains. They have to be able to implementing both label switching and routing IP. According to the routing information in the IP header, the E-LSRs classify the incoming traffic into a forwarding equivalence class (FEC) and mark the packet with a label corresponding to the forwarding along a specific LSP. Then, the intermediate LSRs make forwarding on the basis of label, without the need for extracting the routing information from the IP header.

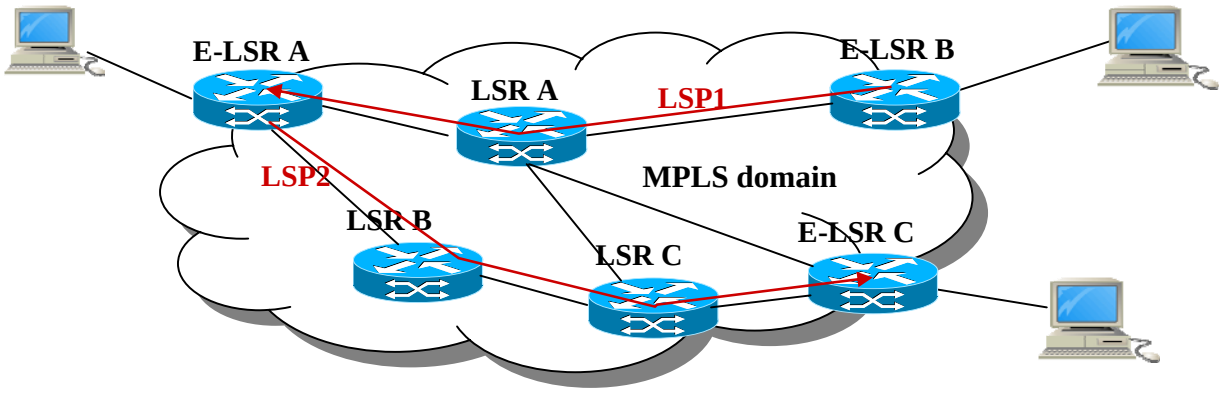


Fig. 2.2 A simple MPLS domain

A FEC describes a set of packets with similar characteristics which may be forwarded in the same way. The assignment of a particular packet to a particular FEC is done just once by the upstream E-LSR as the packet enters the network. There are different granularities to define a FEC. Usually, each FEC corresponds to a destination IP address, but it also might correspond to any traffic class that the E-LSR considers significant. For example, all traffic with a certain value of IP precedence might constitute a FEC. The FEC to which the packet is assigned is encoded in a MPLS header (*shim header*) as a short fixed length value that is the label. It is inserted between the network headers and the IP header as shown in Fig. 2.3. A shim header may contain one or more label entry (*label stack*) which are used for LSP tunnel. Note that a label has a local value: it is use by a LSR to find the next hop and to set the corresponding new label (*label swapping*). Each label entry has the following fields:

- **Label Value**: carries the actual value of the Label. When a labeled packet is received, the label value at the top of the stack is looked up and learns the next hop to which the packet is to be forwarded and the operation to be performed on the label stack before forwarding. This operation may be to replace the top label stack entry with another, or to pop an entry off the label stack, or to replace the top label stack entry and then to push one or more additional entries on the label stack.

- **Exp**: reserved for experimental use.

- **S (Bottom of Stack)**: this bit is set to one for the last entry in the label stack, and zero for all other label stack entries

- **TTL (Time to Live)**: is used to encode a time-to-live value.

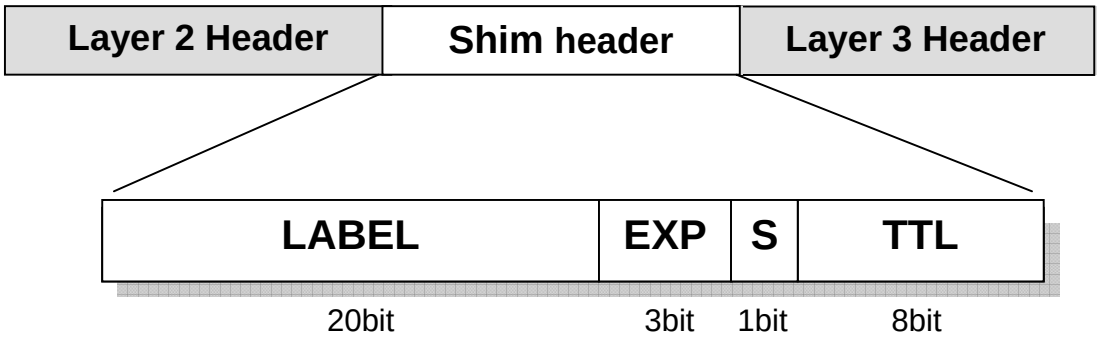


Fig. 2.3 The MPLS shim header

Typically, a MPLS network relies on explicit routing for LSP calculation and setup: the E-LSRs classify the packets into FECs and calculate the corresponding LSPs. Then, the E-LSR of

upstream or that of downstream for a LSP activates a *label distribution protocol* to exchange the label mapping information. A control-driven approach is adopted: all LSPs are established during the processing of control message; when the data packets arrive, the LSP are already set up.

2.3.2 Traffic Engineering

Traffic engineering [27,34] is used to achieve performance objectives such as optimization of network resources and placement of traffic on particular links. From a practical point of view, this means computing a path from source to destination that is subject to a set of constraints, and forwarding traffic along this path. Forwarding traffic along such a path is not possible with IP, since the IP forwarding decision is made independently at each hop, and is based solely on the packet's IP destination address. MPLS can easily achieve forwarding traffic along an arbitrary path. The explicit routing capabilities of MPLS allow the originator of the LSP to do the path computation, establish MPLS forwarding state along the path, and map packets into that LSP. Once a packet is mapped onto an LSP, forwarding is done based on the label, and none of the intermediate hops makes any independent forwarding decisions based on the packet's IP destination.

To make TE implementation in a MPLS domain, the concept of *traffic trunk* (TT) has been introduced. A *traffic trunk* is defined as an aggregate of traffic flows belonging to the same class (FEC) which are placed inside an LSP. A TT, and then the corresponding LSP, is characterized by a set of attributes, such as the FEC, the ingress and egress E-LSR, the requested bandwidth, the priority and the preemption. The priority defines the importance of the LSP with respect to the others and establishes the order in which the LSP path must be computed at the beginning of the connection and in case of congestion. Further, the preemption value allows setting up a new LSP by removing an old one with a lower preemption priority. More specifically, the preemption attributes determine whether an LSP with a certain *setup preemption priority* can preempt another LSP with a lower *holding preemption priority* from a given path, when there is a competition for available resources. The preempted LSP may then be rerouted. Preemption can be used to assure that high-priority LSPs can be always routed through relatively favourable paths within a differentiated services environment. In the same context, preemption can be used to implement various prioritized access policies as well as restoration policies following fault events.

In a TE environment, routing protocols, also known as constraint-based routing (CBR) protocols [35], find a path in the network that meets a series of constraints. Some of these constraints are: the bandwidth requested for a particular LSP, the quality requirements in terms of delay, jitter, etc, the number of hops that the traffic is allowed to cross, the priority of the LSP when compared to other LSPs. Calculating a path that satisfies these constraints requires that the information about whether the constraints can be met is available for each link, and this

information be distributed to all the nodes that perform path calculation. This means that the relevant link properties have to be advertised throughout the network, adding TE-specific extensions to the link-state protocols (IS-IS and OSPF) that allow them to advertise the state of the links, the link attributes and the bandwidth that is available for use by trunks with different priority levels. In this way, each node has knowledge of the current properties of all the links in the network. Once this information is available, a CBR is performed. The main employed CBR algorithm is a modified version of the shortest-path-first (SPF) algorithm, called constrained SPF (CSPF). It is used by the ingress node (explicit routing) to calculate a path that complies with the given constraints. Conceptually, CSPF operates in the same way as SPF, except it first removes from the topology all links that do not satisfy the constraints. For example, if the constraint is bandwidth, CSPF removes from the topology links that don't have enough bandwidth.

2.4 DiffServ aware Traffic Engineering

DS-TE [29,30] technology couples the advantages of DiffServ and MPLS-TE networks. Indeed, in a DS-TE domain, TE policies are performed in a per-class basis through DiffServ classification. The first challenge with supporting DiffServ in an MPLS-TE network is that label-switching routers (LSRs) have to be able to make their forwarding decisions based on either MPLS label and DSCP value. The IETF solved this problem by proposing two solutions to carry DiffServ information in MPLS shim header.

The first solution can be adopted when network supports less than eight PHBs. In this case, the three experimental (EXP) bits of MPLS header are used to map the DSCPs and each particular EXP combination represents a particular PHB (scheduling and drop priority), as shown in Fig. 2.4. During forwarding, the label determines where to forward the packet, and the EXP bits determine the PHB. The EXP bits are not a property that is signalled when the label-switched path (LSP) is established, but they are a value that has to be configured according to the DSCP bits of the IP packets carried in the LSP, or by the network operator. LSPs for which the PHB is mapped in the EXP bits are called E-LSPs (where E stands for "EXP-inferred"). E-LSPs can carry packets with up to eight distinct per-hop behaviours in a single LSP, as shown in Fig. 2.5.

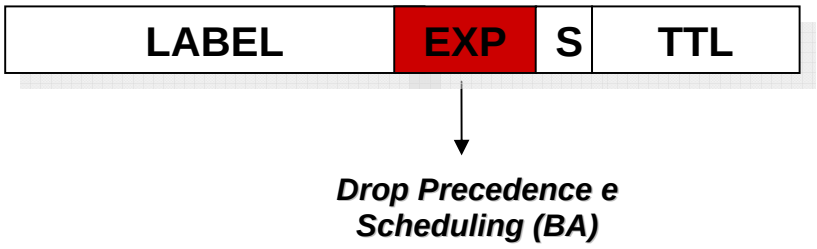


Fig. 2.4 MPLS header with DSCP in the EXP bits

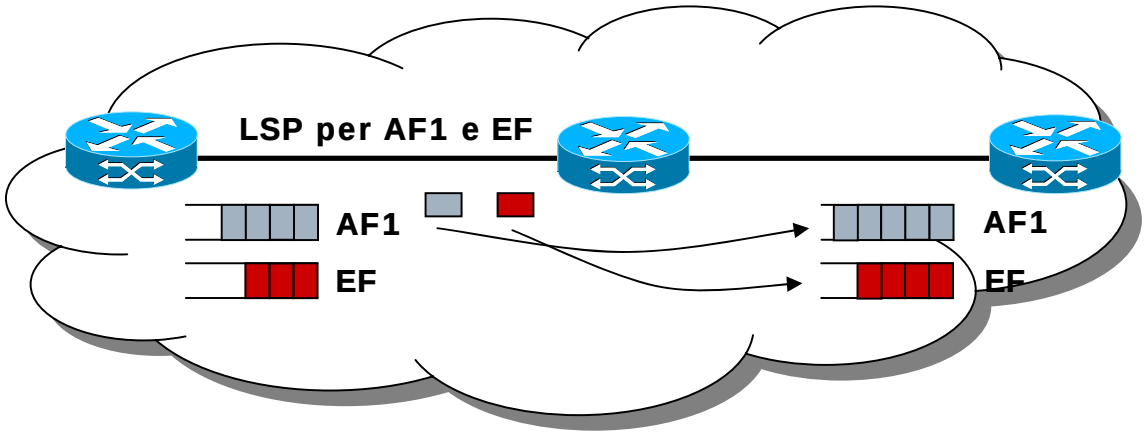


Fig. 2.5 An E-LSP can carry traffic from Multiple PHBs

The second solution has to be adopted when network supports more than eight PHBs. Here, the EXP bits alone cannot carry all the necessary information to distinguish between PHBs. The only other field in the MPLS header that can be used for this purpose is the label itself. During forwarding, the label determines where to forward the packet and what scheduling behaviour to grant it, and the EXP bits convey information regarding the drop priority assigned to a packet. Thus, the PHB is determined from both the label and the EXP bits, as in Fig. 2.6. Because the label is implicitly tied to a per-hop-behaviour, this information needs to be conveyed when the LSP is signalled. LSPs which use the label to convey information about the desired PHB are called L-LSPs (where L stands for "label-inferred"). L-LSPs can carry packets from a single PHB, or from several PHBs that have the same scheduling regimen but differ in their drop priorities (such as AFxy where x is constant and y is not constant). An example of this solution is shown in Fig. 2.7.

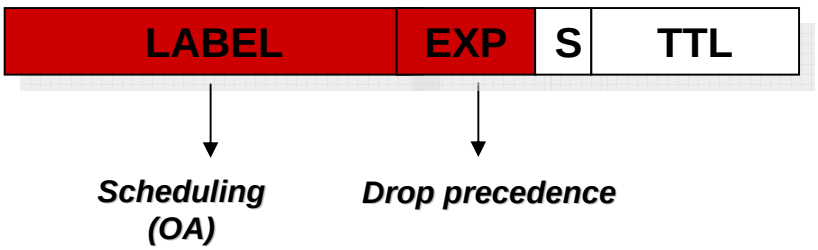


Fig. 2.6 MPLS header with DSCP in either the label and the EXP bits

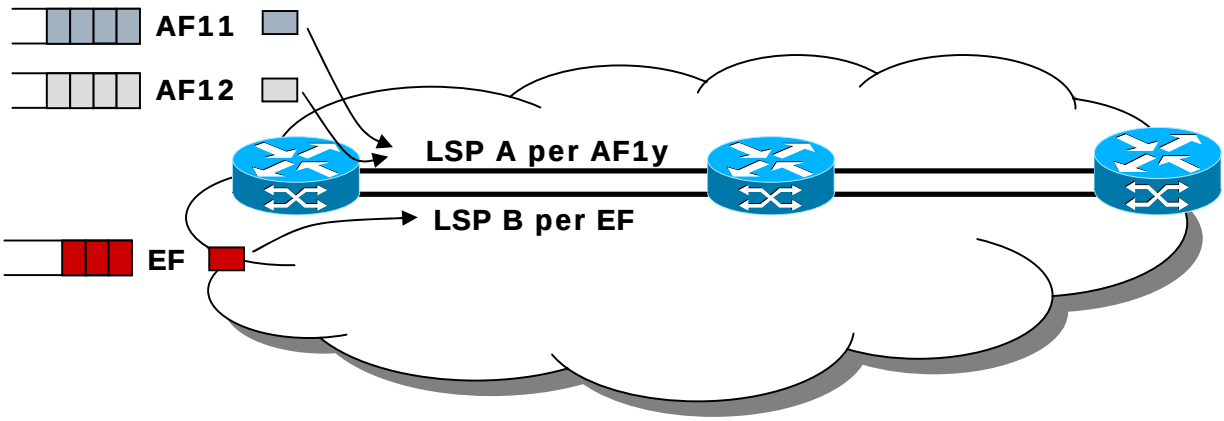


Fig. 2.7 An L-LSP can carry traffic from a single PHB or from several PHBs that share the same scheduling behavior. LSP A carries traffic from AF11 and AF12.

In addition to the problem on the mapping of DSCP into MPLS header, to perform TE polices DS-TE needs to define a set of bandwidth constraints for resources allocation. This goal is achieved by introducing three new concepts:

- **Class Type** (CT): is a set of traffic trunks with the same QoS requirements. In a DS-TE domain, no more than eight CTs can be set up, on the basis of traffic trunks CoS values.

- **TE-Class**: is a combination of a CT and a preemption priority, defined as <CT, p>. It allows traffic trunks belonging to the same CT to be forwarded over different LSPs at different priorities. Preemption allows high-priority LSPs to be routed through paths occupied by low-priority LSPs, which are then terminated or re-routed. TE-Classes are defined by assigning one or more preemption values to each CT. The maximum number of TE-Class is eight and the belonging of a packet to a TE-Class arises from the EXP bits, which is a field in the MPLS header.

- **Bandwidth Constraint (BC) model**: specifies the amount of links' bandwidth that can be used to route LSP belonging to each CT. To this, there are appropriate Bandwidth Constraints defined for each CT and each link.

Classifications and BC Model enable network operators to efficiently manage the incoming traffic and set up LSPs. When a new LSP setup request arrives with a specific CoS requirement, it is classified in a TE-Class, by assigning a CT and a preemption value. BC Model allows to verify the available resources and the possibility to set up the new LSPs without preemption or by preemting LSPs with lower preemption priority.

2.4.1 Class Type

A basic DS-TE requirement is to be able to make separate bandwidth reservations for different classes of traffic. This implies the knowledge of how much bandwidth is available for each type of traffic on all routers throughout the network. For this purpose, [30] introduces the concept of a class type (CT), which is defines as follows:

"*The set of traffic trunks crossing a link, that is governed by a specific set of bandwidth constraints. CT is used for the purposes of link bandwidth allocation, constraint based routing, and admission control. A given traffic trunk belongs to the same CT at all links.*"

The standard does not impose a particular mapping of traffic to CTs, leaving this decision to the individual vendors. A possible solution, as that of JUNOS implementation, is to map traffic with the same scheduling behaviour to the same CT. Because the PHB is defined by both the queue and the drop priority, a CT may carry traffic from more than one CoS. The IETF requires support of up to eight CTs referred to as CT0 through CT7. In the current IETF model, a DS-TE LSP can only carry traffic from one CT. LSPs that transport traffic from the same CT can use the same or different preemption priorities. By convention, the best-effort traffic is mapped to CT0. For example, if a network has to carry out traffic of two DiffServ PHBs, corresponding to EF and BE, two scheduler queues need to be configured on each link, one for BE and one for EF. CT0 is mapped to the BE queue and CT1 is mapped to the EF queue. The bandwidth available for CT1 is limited to the percentage of the link required to ensure small queuing delays for CT1 traffic. Separate TE-LSPs are established with bandwidth requirements from CT0 and from CT1.

2.4.2 TE-Class

According to CT definition, the computing of path for each CT requires the available bandwidth per-CT at all priority levels must be known for each link. Since there are eight CTs and eight priority levels, a total of 64 values need to be carried by the link-state protocols. IETF provides for limiting the advertisements to eight values out of the possible 64. For this purpose, a TE-class is defined as a combination of <CT, priority>. DS-TE supports no more than eight TE-classes, from TE0 to TE7, which can be selected from the 64 possible CT-priority combinations, as in the example of Fig. 2.8. A solution at one of the extremities is to chose a single CT with eight priority levels, like the existing TE implementation. At the other extremity, eight distinct CTs may be chosen, each with a different priority level. In order to perform path computation, the CT and priority levels chosen for an LSP must correspond to one of the configured TE-classes.

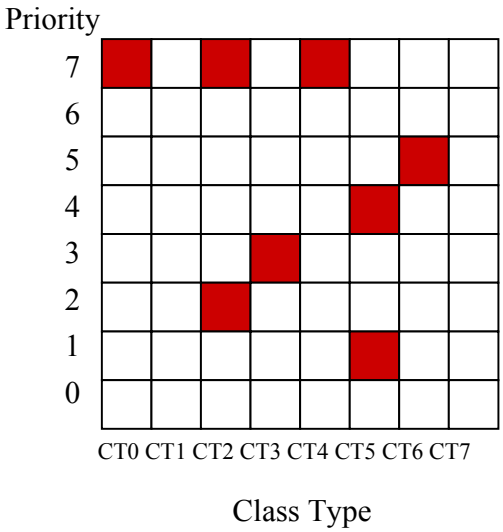


Fig. 2.8 Example of TE-Class selection selected from the 64 possible CT-priority combinations

2.4.3 Bandwidth Constraint Model

The definition of a Bandwidth Constraints Model is one of the most important requirement for DS-TE. It determines for each link of the network the relationship between CTs and bandwidth constraints, ensuring to set up the LSPs along links where resources are available and avoiding the need for overprovisioning. The BC model allows to compute the bandwidth that is in use on the link and the Unreserved Bandwidth (UB) which can be used to set up new LSPs. Bandwidth can be always granted, mainly for traffic with strictest QoS requirements. Preemption can be performed to give room to high priority classes, on the basis of the unreserved bandwidth information which is derived from the defined constraints.

As established by the IETF, a BC Model should achieve some objectives that can be summarized as following:

- *bandwidth sharing* among CTs under both normal and overload conditions to avoid bandwidth wastage;
- *bandwidth isolation* among CTs, avoiding that a CT takes bandwidth from another under overload conditions;
- *security* against QoS degradation, mainly for the CTs with higher quality requirements;
- *simplicity*, to minimize signalling load processing requirements;
- applicability when preemption is either enabled or disabled.

Three BM models have been standardized by the IETF, which are the Maximum Allocation Model (MAM) [36], the Maximum Allocation with Reservation (MAR) [37] and the Russian Doll Model (RDM) [38]. Each of these enables network operators to enforce different bandwidth constraints for different CTs with some variants in the degree of bandwidth isolation and bandwidth sharing and in the need for preemption.

According to the *Maximum Allocation Model*, the link bandwidth is divided among the different CTs, defining a different BC for each one (Fig. 2.9). This model achieves complete isolation between different CTs, so that it is not necessary to define priorities between LSPs carrying traffic from different CTs. The problem of MAM is the risk of wasted bandwidth. Indeed, if the traffic load for a CT is lower than its reserved BC, bandwidth remains unused being not possible to share it between other CTs.

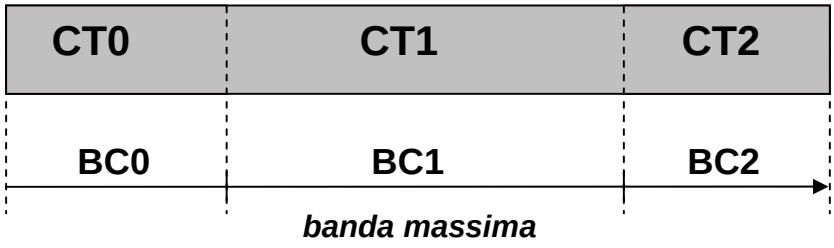


Fig. 2.9 The MAM model

Similarly to MAM, the *Maximum Allocation with Reservation* defines the maximum allocable bandwidth for each CT, but introduces some exceptions. Indeed, in the MAR model a CT is allowed to exceed its bandwidth constraint under conditions of no congestion, with the provision that it reverts to the original constraint if overload or congestion occurs.

Finally, the strategy of the *Russian Doll Model* is more complex since it always allows a CT to use the bandwidth that is left over by the others. If N is the number of active CTs, it is necessary to define N BCs for the N. In this case, CT_{N-1} is the class with the highest QoS requirements, while CT_0 is the class with the lowest priority, corresponding to the best-effort traffic. The RDM works as follows:

- BC_{N-1} is the maximum reservable bandwidth for CT_{N-1};
- BC_i is the maximum bandwidth which can be shared from $CT_{N-1},\ldots, CT_i$;
- BC_0 is the maximum bandwidth which can be shared from all CTs and corresponds to the link bandwidth capacity.

In Fig.2.10 an example of the RDM scheme is shown. The advantage of this model is that it provides efficient bandwidth usage through sharing and isolation if preemption is enabled. To

perform preemption, the unreserved bandwidth (UB) information for TE -Classes is needed. The unreserved bandwidth (UB) for the TE-Class[i] = <CTc, p> is computed as follows:

$$UB_i = \min[BCb - \sum B(CTc, q) \text{ for } q \le p \text{ and } b \le c \le 7, \ldots BC0 - \sum B(CTc, q) \text{ for } q \le p \text{ and } 0 \le c \le 7]$$

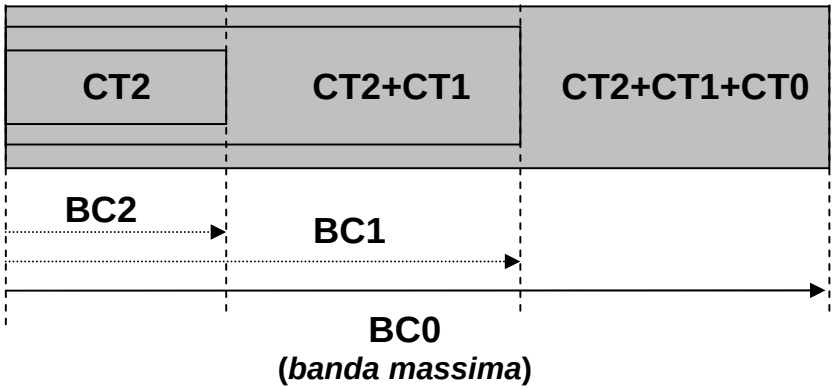


Fig. 2.10 The RDM model

The advantage of RDM relative to MAM and MAR is that it provides efficient bandwidth usage through sharing [39]. Its main disadvantage is that there is no isolation between the different CTs, and preemption must be used to ensure that each CT is guaranteed its share of bandwidth no matter the level of contention by other CTs. This means LSPs corresponding to different services must be given different priorities, because they share bandwidth resources. For example, if a link supports traffic of two class types, CT0 and CT1, with CT1 LSPs at priority 0 and CT0 LSPs at priority 1, when a CT1 LSP has to be established, it can preempt one of the CT0 LSPs. Note that preemption is possible only if the CT1 LSP bandwidth requirement is such that the defined BC1 on the link is not exceeded. Further, the calculation of available bandwidth for the RDM model is a bit more complicated, because it must take into account LSPs at several priority levels and from all the CTs that share the particular BC. For example, the available bandwidth for an LSP from CT0 at priority p is equal to BC0 minus the allocations for all LSPs from all CTs at priorities better or equal to p. Table 2.1 summarizes the differences between MAM, MAR and RDM models, taking into account the main BC model requirements defined by IETF.

Table 2.1. Differences between MAM, MAR and RDM models.

	MAM	***MAR***	***RDM***
bandwidth sharing	Bandwidth sharing is not performed; bandwidth may be wasted	Bandwidth sharing is not performed, but exceptions to BCs are allowed.	Bandwidth sharing is achieved
bandwidth isolation	Achieves isolation among CTs without need for preemption	Achieves isolation among CTs without need for preemption	Requires preemption to achieve isolation between CTs
security	Not much sure against QoS degradation	More sure that MAM	Very sure against QoS degradation due to bandwidth sharing and preemption
simplicity	Very intuitive and easy to manage	Less intuitive than MAM but easier to RDM	Not much intuitive
applicability against preemption	Recommended if preemption is disable	Recommended if preemption is disable	Recommended if preemption is enable

2.4.4 Deployment of a DS-TE architecture

To summarize the contents of this chapter, planning a DS-TE architecture requires the following steps:

- DiffServ service classification;
- decide between E-LSP and L-LSP scheme;
- aggregate CoSs in CTs;
- define a BC Model;
- assign a preemption priority and classify CT in TE-Class;
- setup LSPs.

Chapter 3

Bandwidth Management in DS-TE Networks

This chapter addresses the bandwidth management problem in Differentiated-Service-aware Traffic Engineering (DS-TE) networks [29,30]. In this context, diverse Bandwidth Constraint (BC) models have been proposed to enforce bandwidth constraints for each class of traffic on the basis of the resource optimization objectives. This work is not aimed at designing new models but to describe the framework required to exploit the advantages of the selected BC model. In particular, we analyze the impact of setting the bandwidth constraints and the aggregation of the service flows into traffic classes on the service performance and resource utilization. We believe that this issue is often underestimated and the literature misses an overall discussion and relevant solution that drives the network operator along the setup of the bandwidth management procedures. The presented strategy takes into account the performance indicators, the quality profile, and the forecasted traffic to improve the fulfilment of quality of service targets and to optimize network resource utilization.

3.1 DS-TE Network Management

As explained in the previous chapter, DiffServ aware Traffic Engineering (DS-TE) [29,30] is one of the most advanced technologies to achieve QoS in a scalable, flexible and dynamic way. On the one hand, DS-TE allows the operators to expand the plethora of offered services and to be ready for the unexpected user demands in the near future. In fact, we envision that the future networks should be prepared to interconnect multiple edge devices with different data formats and support multiple services requiring different bandwidth granularities and quality of service levels. On the other hand, these solutions make network management more complex than in the past, demanding for a shrewd setting of network QoS and TE parameters: preemption priority,

parameters bandwidth constraints, traffic classification parameters, administrative link weights, TE attributes, and so on. This demands for network management procedures that drive the operator along the configuration of the QoS settings when using the full potentialities of the NGN networks.

In this chapter we focus on the bandwidth management procedure within the DS-TE architecture, which is aimed at defining how much of the links bandwidth should be assigned to the traffic flows of the offered services. It works by aggregating the traffic flows into a few traffic classes and dividing the total bandwidth for each link among these classes. Several models have been proposed in the past, which differ in the degree of bandwidth isolation and sharing. Key parameters in these models are those which the maximum allocable bandwidth depends on. We don't intend to present new models but how these models should be employed in the network and their impact on the resource utilization and network performance. Indeed, the setting of the bandwidth constraints over all the network links have a direct impact on the performance of the constraint-based routing, which then heavily influences the call block probability and resource utilization. Additionally, the adopted bandwidth constraints together with the selected aggregation of traffic flows into the active traffic classes affect the end-to-end performance in term of delay, losses and jitter.

The above mentioned issues are discussed in the following and a strategy to setup the main parameters in the bandwidth management procedure is presented. The proposed methodology starts from the definition of the key performance indicators (KPIs) aimed at objectively quantifying the QoS level for each of the required services; these, together with the traffic load and network topology, are used to find the optimal mapping of service types into traffic classes and the optimal bandwidth allocation for each of these. Herein, the optimality is expressed in terms of a cost function weighting both the expected fulfilment of the quality of service targets and the network resource utilization. The effectiveness of the proposed solution is analyzed when considering a real context with the combination of heterogeneous service types.

3.2 The bandwidth management problem

Fig. 3.1 shows the main blocks in the DS-TE architecture [40]. At the first, the Bandwidth Management component of the TE unit defines a BC model for all network link, specifying a constraint for each active CT. When a new LSP setup request arrives with specific CoS requirements, the Service Level Specification unit, which manages the contracts with the users, classifies the incoming request in a TE-Class, by assigning a CT and a preemption value. Then, the LSP management module computes the possible routes by means of constraint-based routing algorithms which rely on the selected BC model. The BC model allows LSP management to determine the amount of available resources and the possibility to set up the new LSPs in the

available paths to the destination. The solution can require also the preemption of active LSPs with lower preemption priority. All TE operations are supported by a performance and traffic measurement tool like a passive probe, active probe (e.g., Cisco RTR) or a classical performance measurement tools [41].

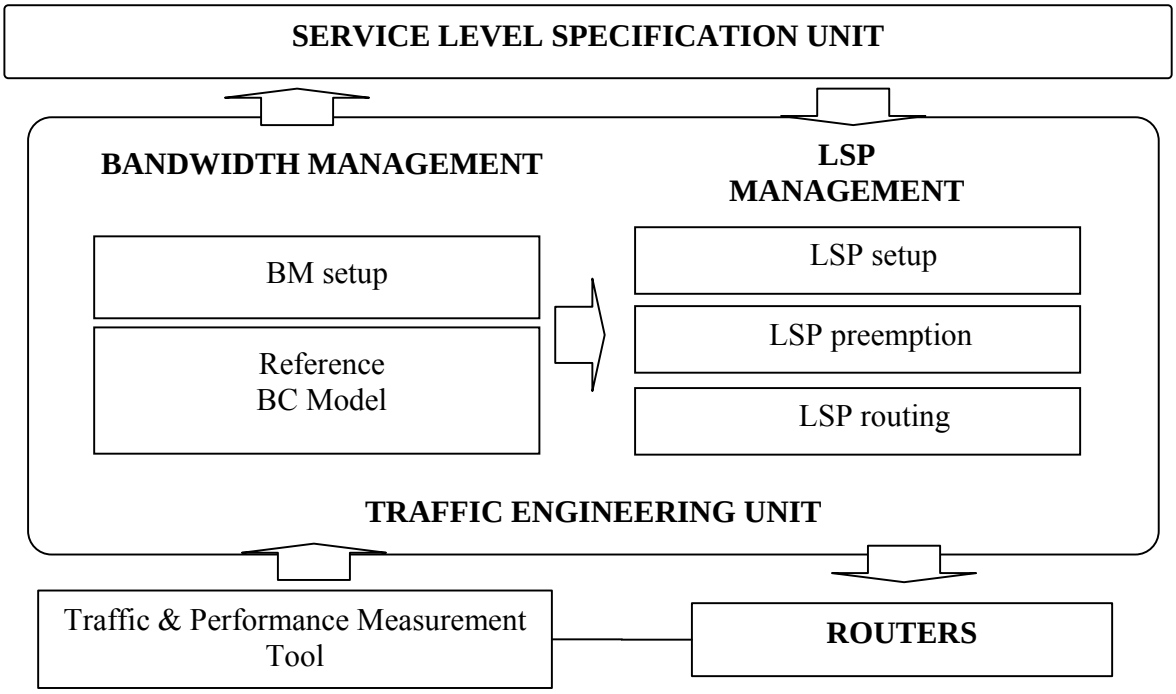


Fig. 3.1. Diagram of DS-TE architecture components.

The definition of an effective and fair BC model has been the subject of many studies during the last few years. In Section 2.XX, the three IETF BM models have been described, which are the Maximum Allocation Model (MAM) [36], the Maximum Allocation with Reservation (MAR) [37] and the Russian Doll Model (RDM) [38]. Each of these enables network operators to enforce different bandwidth constraints for different CTs with some variants in the degree of bandwidth isolation and bandwidth sharing and in the need for preemption. In [39], the authors provide some considerations on the BC model performance and recommend selecting the RDM as the default one in DS-TE architectures. While MAM and MAR models are not able to avoid simultaneously bandwidth wastage and QoS degradation, RDM can offer high guarantees for both these objectives at the same time. Other models have been presented afterwards, which are mostly enhancements of the IETF models. In [42], the authors propose a "use it or lend it" strategy where if a certain CT consumes less than its minimum bandwidth, its unused minimum bandwidth can be lent to other CTs' connections with a nonzero holding priority. In case that it

increases its demand to its minimum guaranteed bandwidth later on, it is able to preempt the connections of other CTs borrowing bandwidth so as to obtain at least its minimum bandwidth.

The DS-TE standard does not enforce the use of the same BC model on all links of the network, even if this is recommended to simplify management operations. Regardless of which BC model is adopted, the resulting network performance and resource utilization depend on both the aggregation of the CoS in the implemented CTs and the setting of the BCs. The bandwidth constraints over all the network links have a direct impact on the performance of the constrained-based routing [35], which then heavily influences the call block probability. It also affects the frequencies of the preemption occurrences, which have to be kept as low as possible [43]. BCs setting together with the selected aggregation of the traffic into the active CTs are also major tasks to control the end-to-end performance in term of delay, losses and jitter. In fact, the belonging of a traffic flow to a certain CT determines the priority of the relevant packets with respect to the others. Additionally, the amount of packets with higher priority depends on the BCs set for the high priority classes. For this reason the setting of the BC and aggregation of the CoS in CTs are problems that have to be addressed jointly.

Notwithstanding the importance of these tasks, we believe that have often been underestimated. Indeed, IETF does not suggest any criteria to be considered and the literature presents some works that only partially refer to this problem with limited solutions. [44] is one of the papers that addresses this problem but provides only a general overview and addresses CT classification and BC setting in isolation.

3.3 Framework for Bandwidth Management Setup

In this section, we present a DS-TE bandwidth management which aims to configure a BC Model in terms of the effective network requirements. Unlike the approach in [44], the proposed system adopts the solution of implementing a single algorithm to achieve both Class Type classification and BC definition. This approach performs the two tasks in an interdependent way, optimizing the output of the one in terms of the solution obtained for the other and vice versa.

As shown in Fig. 3.2, the proposed bandwidth management setup works on the basis of the following input information: a reference set of key performance indicators (KPIs), which allow for characterizing the service requirements and evaluating QoS network performance; a quality profile, which defines the services classification into CoSs; and the profile of the forecasted ingress traffic. This information, together with the BC model adopted in the network, are the input to a “what-if analysis” to analyze network performance and resource utilization at varying CT classification and BC settings. Note that while the setting of the BC model may vary from link to link, CT classification has to be unique for the whole network.

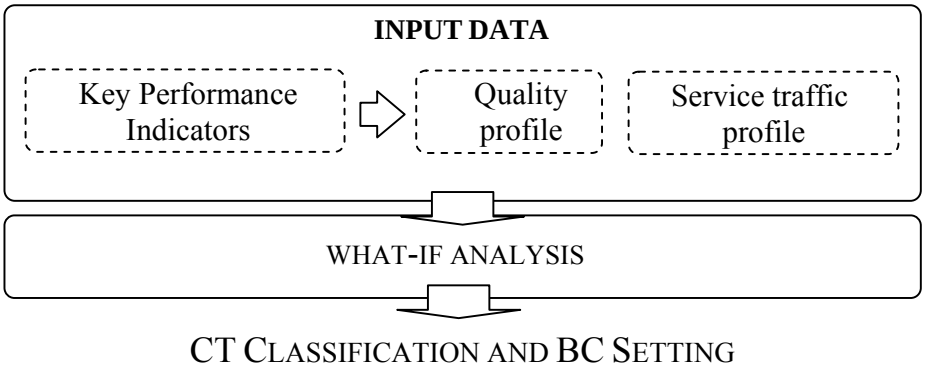


Fig.3.2. The general scheme of the proposed bandwidth management setup.

3.3.1 Key Performance Indicators (KPIs)

The Key Performance Indicators provide a quantitative and objective solution to compare the obtained quality performance with the desired ones and are used for both traffic classification and network analysis. Quality can be evaluated from the point of view of the end-user, as perceived quality which refers to the experience in the use of a service, or from the point of view of the operators, as offered quality which refers to the policies of service provisioning, the sustained costs and the capacity to maintain service availability. It can be also intrinsic if refers to technical network performance parameters, such as delay, jitter, packet loss, and throughput. It can be specified either quantitatively or qualitatively.

Several QoS definitions have been proposed in the literature, as described in section 1.2. When implementing the proposed methodology, we have adopted the following KPIs, which belong to the category of offered intrinsic quality: IP Packet Transfer Delay (IPTD); IP Packet Delay Variation (IPDV); IP Packet Loss Ratio (IPLR); IP Packet Error Ratio (IPER); and Spurious IP Packet Rate (SIPR). However, the proposed methodology does not depend on a specific set of KPIs, which instead have to be chosen by the service provider on the basis of the service typologies and requirements.

3.3.2 Quality profile

The definition of the quality profile consists in identifying the QoS requirements and performing DiffServ classification for the set of services $\{S\}$ provided in the network. Service characterization and classification rely on a set of KPIs. Let P be the number of selected reference KPIs; the i-th service within $\{S\}$ is associated to a vector that specifies its quality requirements:

$$< S >_i = [\Delta KPI^s_{1,i}, \Delta KPI^s_{2,i}, \Delta KPI^s_{3,i}, ..., \Delta KPI^s_{P,i}].$$

Each element of this vector defines the threshold for the allowed values for each KPI. On the basis of these values, each service is classified into a specific CoS according to the DiffServ model. The 14 standard CoSs [31, 32] can be adopted or new CoSs can be defined by the network operator. One or more services can be classified in the same CoS. As a result of this procedure another vector of KPI is obtained:

$$< CoS >_j = [\Delta KPI^c_{1,j}, \Delta KPI^c_{2,j}, \Delta KPIC^c_{3,j}, ..., \Delta KPI^c_{P,j}].$$

This vector containing the KPI threshold values which the *j*-th CoS is able to satisfy. They correspond to the intersection of quality requirements of all services in the *j*-th CoS. The cardinality of the set {CoS} can be lower than the number of services to be provided.

3.3.3 Service traffic profile

In accordance with the IETF rules, the BC model specifications have to be defined link-by-link; as a consequence, the proposed DS-TE bandwidth management procedure needs to perform a traffic prediction for each link in the network. This prediction can be obtained through a network analysis by considering the following inputs which are available to the operator:

- network topology;
- bandwidth required by each service, B_i^s;
- number of users $U_i^{a,b}$ of service *i* accessing the network at node *a* and ending at node *b*.

To estimate the traffic load per link, it is necessary to consider the paths between each pair of ingress-egress routers. For the generic edge routers (*a, b*), where a and b are the ingress and egress nodes, respectively, the load for service *i* is equal to:

$$C_i^{a,b} = B_i^s \times U_i^{a,b} \tag{3.1}$$

This traffic spreads over the set of available paths from a to b. The distribution of the traffic through the available paths is evaluated through an empirical simple algorithm, which distributes the traffic according to the path length. In particular, we have adopted an inverse linear relationship between the traffic load and the path length. Only the disjoint Z paths no longer than two times the shortest one are considered in this process and the traffic is distributed according to the length of each path p_z. We then assume that the traffic load from a to b along the z-path is equal to:

$$c_{i,z}^{a,b} = C_i^{a,b} \frac{1}{p_z \sum_{x=1}^{Z} 1/p_x} \tag{3.2}$$

From this distribution, the total load per link and per service is computed.

Note that the proposed algorithm is quite simple. The choice has been driven by the fact that at this stage we just need to find enough resources from the source to the destination to satisfy the bandwidth demands for the different services. For this purpose, the use of complex routing procedures would be useless [35]. These are instead adopted when addressing LSP setup requests.

At this stage we also compute the maximum length among all the paths traversing each link. This is used to compute local KPI thresholds from the end-to-end KPI thresholds in <CoS>*j*, as discussed in the following.

3.3.4 What-if analysis

Fig. 3.3 provides a workflow description of the operations performed by the what-if analysis. The first step is the detection of a possible CT classification, which is performed by evaluating the <CoS> KPI vectors which were defined during the quality profile definition phase. The possible mappings from CoSs to CTs can be obtained in two possible ways:

a) activating a CT for each CoS (since the maximum number of activable CTs is 8, this solution is possible only if the number of CoSs is lower than 8).

b) grouping more CoSs in the same CT. In this case, the bandwidth allocation benefits from reducing the number of CTs at the expense of a lower efficiency in terms of QoS requirements satisfaction. The allowed combinations of CoSs are those which satisfy the following conditions:

- at least three CTs are defined: CT2 for expedited traffic, CT1 with intermediate guarantees and CT0 for best effort services;
- the priority order defined by DiffServ classification is respected (only consecutive CoSs are grouped).

If W is the cardinality of the set {CoS}, the resulting total number of {CT} classifications is:

$$H = \sum_{v=3}^{V} \binom{W-1}{W-v} \tag{3.3}$$

where $V = W$ if $W \leq 8$ and $V = 8$ otherwise.

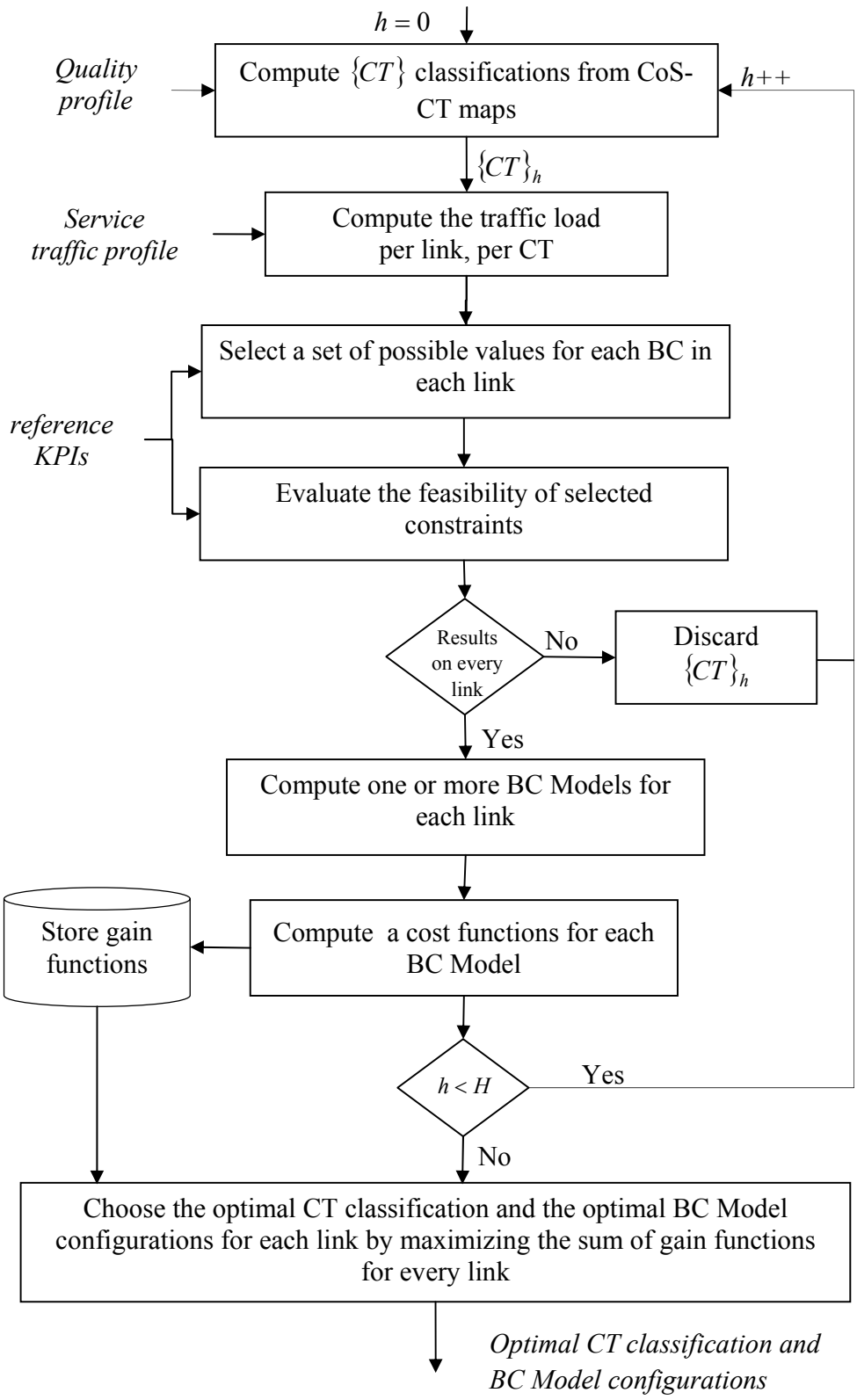


Fig. 3.3. Workflow of the proposed BC Model computation methodology

Each *k*-th CT of the considered classification needs to satisfy the quality parameters of the encompassed CoSs so that another vector of KPIs <CT> is defined as the intersection of all corresponding <CoS>*j*.

In Fig. 3.3, *h* (*h* = 1,2,…,*H*) indexes the considered CT classifications. For each of these, one or more BC model configurations (constraints values) are defined and evaluated for each link in the network. The following operations are related to the setup of the BC so that these need to be performed link-by-link.

At first, the single-hop KPI thresholds $Th_{k,p}$ have to be computed from the end-to-end ones (<CT>) by considering the maximum length of the end-to-end paths for all the flows traversing each link. The traffic load in a per-CT basis per link is also computed from the previously defined service traffic profiles.

Whatever the BC model adopted in the network, we need to define *N* bandwidth constrains. For presentation convenience, in the following with refer to the RDM model; however, the proposed strategy can be applied to any other with only minor changes. Each *k*-th constraint has to satisfy two requirements: grant KPI performance in the range of values defined by the single-

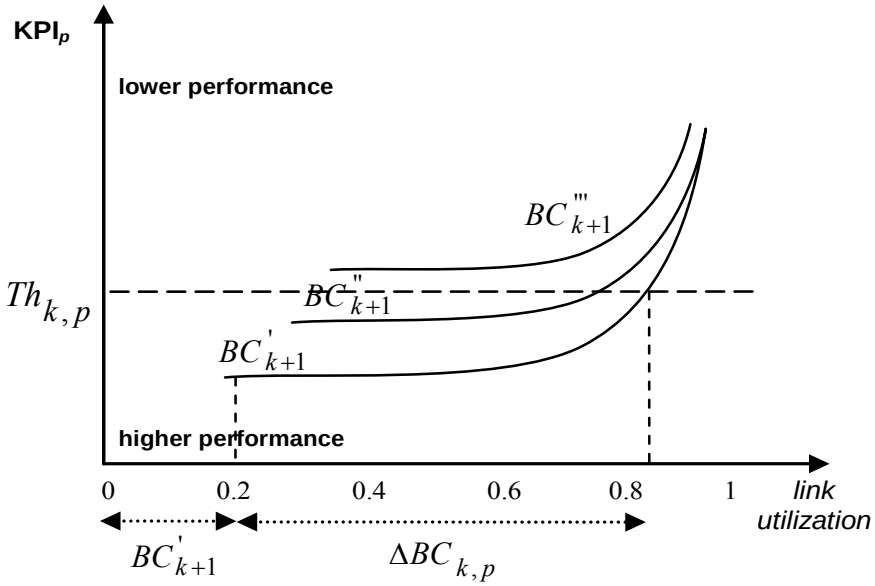


Fig. 3.4. Performance of a router for traffic of CT_k class in terms of a generic KPI_p as a function of the link utilization. Three BC_{k+1} are considered. While BC'''_{k+1} gives no solutions in the range of allowed KPI values, BC'_{k+1} and BC''_{k+1} satisfy the KPI requirements for CT_k. The corresponding values for BC_k are in the ranges $\Delta BC_{k,}$.

hop thresholds; be equal or higher than the maximum traffic load expected for all CTs with priority higher or equal to CT_k. Since one or more settings of bandwidth constraints are possible to accomplish these requirements, we have devised an empirical algorithm that generates all possible BC combinations and evaluates their goodness computing a gain function. This is made by the combination of the KPI and bandwidth gains, which measure the degrees of required quality satisfaction and the level of resource utilization, respectively.

The devised algorithm works iteratively analyzing all CTs for the considered classification h, starting from the CT with the highest priority. Indeed, the bandwidth constraints for different CTs are not disjointed and the setting of one of these influences the quality of the traffic with lower priorities. The relationship between generic constraints BC_{k+1} and BC_k is put in evidence in Fig. 3.4: this draws the router performance for traffic of class CT_k in terms of a generic KPI_p, as a function of the link utilization. The performances are clearly linked to how much bandwidth has been already reserved to all the CTs with higher priority (BC_{k+1}). The higher the BC_{k+1} is, the lower the performance for CT_k are ($BC'''_{k+1} > BC''_{k+1} > BC'_{k+1}$).

The performance curves for CT_k are used to make the following operations:

- evaluate the feasibility of the pre-computed BC_{k+1} values with respect to the given CT_k KPI requirements;
- compute the corresponding possible values for BC_k.

In particular, the feasibility of a BC_{k+1} is granted if it allows for CT_k performance lower than the threshold $Th_{k,p}$ for each p-th KPI. The BC_{k+1} values that do not satisfy this condition are discarded, as BC'''_{k+1} in Fig.3.4. As to the others, the ranges $\Delta BC_{k,p}$ of bandwidth utilization values which are higher than the corresponding BC_{k+1} value and which satisfy the CT_k requirements are further considered for the next bandwidth constraint. For example, if BC_{k+1} in Fig.3.4 is chosen equal to $BC'_{k+1} = 0.2$ of the total link utilization, all values between 0.2 and 0.8 are possible for BC_k. The intersection of results obtained from all curves of all KPIs gives the set of possible values for BC_k. Among these values, the lowest one satisfies the maximum KPI guarantees with the highest KPI gain for the predicted traffic only; all other values introduce a bandwidth gain that can be utilized for additional traffic with lower KPI performance. As to the performance curves in Fig.3.4, these can be obtained in different ways, as mathematical analysis, simulations, and testlab measurements. In our implementations, we have followed the second approach, which is the most straightforward and provides accurate results as far as the QoS mechanisms in the simulated model match those in the deployed routers.

At the end of this analysis for all CTs of classification h, it is necessary to verify if solutions were obtained for each BC_k on every link of the network. If so, the corresponding BC

Models for each link are generated by combining the sets of possible BC_k. For each viable BC Model we then evaluate the goodness by computing a gain function that takes into account both KPI gain (G_{KPI}) and bandwidth gain (G_{BDW}), which are defined as follows:

$$G_{KPI} = \sum_k \sum_p \alpha_k \beta_p \frac{Th_{k,p} - KPI_p\big|_{BC_{k,r}}}{Th_{k,p}} \tag{3.4}$$

$$G_{BDW} = K \sum_k \alpha_k \frac{BC_{k,r} - BC_k^{\min}}{B_{Link}} \tag{3.5}$$

where K is the number of CTs, $BC_k^{\min}$ is the minimum amount of bandwidth to satisfy the traffic load and α_k and β_p are two parameters to weight the importance of class types and the KPIs, respectively. These are selected by the operator with the following constraints: $\sum_k a_k = 1$ and $\sum_p \beta_p = 1$. Additionally, $KPI_p\big|_x$ is the expected KPI value when the bandwidth constraint x is applied. We also defined a third parameter, γ, to weight the importance of the KPI gain against the bandwidth gain on the total gain function. Indeed, as previously mentioned, the KPI and bandwidth gains are characterized by an opposite behaviour with respect to the BC model settings: increasing the BC values brings to an increase in the bandwidth gain and a decrease in the KPI gain.

This algorithm is performed for all other {CT}h until $h = H$. Then, the optimal CT classification and the optimal BCs for each link are identified by selecting the solution with the highest gain function among all the evaluated combinations.

3.4 Extension to inter-domain scenarios

In the previous section, we presented our bandwidth management system considering a single DS-TE domain which is required to provide certain intra-domain QoS guarantees. However, there is a great need of extending the proposed system to address multidomain scenarios. Indeed, in the context of the QoS provisioning, the interoperability among different autonomous systems (AS) and access networks is a key issue to grant end-to-end quality requirements.

The users accessing a DS-TE domain, as defined in Section 3.3.3, can be the users of an access network, the users of another DS-TE domain or the users of a domain with a technology different than DS-TE. Indeed, in a multidomain scenarios, QoS is not necessarily limited to the DS-TE architecture; heterogeneous and multilayered networks can contribute to accomplish the end-to-end QoS objectives. To this, each AS needs to take into account the treatments of each

traffic flow in the external domains to establish the intra-domain behaviour so that the end-to-end requirements are satisfied.

Many studies are being conducted to address this issue. The main trends in approaching the problem is to extend the concept of Bandwidth Broker (BB) which was introduced in the DiffServ technology to manage the inter-domain operability [42,45]. A BB is a centralized, QoS management architecture of a single autonomous system which provides SLS management, traffic engineering and network monitoring functionalities. A BB manages both internal and external relations, communicating with the other BBs of the adjacent domains to exchange information regarding end-to-end resource management and traffic control. Each BB is supported from internal and external databases and may perform inter-domain communications thought different technologies, such as Common Object Request Broker Architecture (CORBA) or Web Services (WS).

In the deployment of our system, we referred to this bandwidth broker scheme to achieve interoperability guarantees. To simplify the intra-domain resource management and minimize the inter-domain information exchange, our proposed bandwidth management system works in each DS-TE domain independently on technologies and solutions which are adopted in the other domains. This means that classification and BC Model computation are performed without considering classification and resource allocation in exterior domains. The only requirement to grant the inter-domain operability is that each AS has to collect information on the extra-domain QoS guarantees and on the number of users for each service that will be carried out. According to this information, quality profile and traffic profile definition has to be modified.

In particular, since the KPI guarantees typically suffer from the length of the end-to-end paths, the intra-domain KPI thresholds have to be defined taking into account the KPI guarantees at the ingress of the considered domain and the length of the end-to-end paths up to destination. This entails that traffic flows of the same service may need different intra-domain KPI requirements on the basis of the differences in the end-to-end paths. Consequently, the definition of the quality profile in multidomain scenarios needs to consider the KPI requirements per single traffic flow. For each *m*-th traffic flow, a KPI vector $<TF>_m$ is defined from the corresponding $<S>_i$ vector, computing each *p*-th element by the following equation:

$$\Delta KPI_{p,m}^{TF} = \left\lfloor \Delta KPI_{p,i}^{S} - KPI_{p,m}^{TF}\Big|_{in} \right\rfloor \cdot d_{out} \tag{3.6}$$

where $KPI_{p,m}^{TF}\Big|_{in}$ represents the KPI guarantees for the considered traffic flow at the ingress of the considered domain and d_{out} is a parameter to weight the size of the considered domain against the remain others, with $d_{out} \leq 1$.

On the basis of the <TF> vectors, the traffic flows are classified into classes of flows (CoF), which are defined as the CoS of DiffServ except for the possibility to classify flows of a

same service in different classes. For each class, a KPI vector is defined and the resulting classification is employed by the what-if-analysis for the CoF-CT mapping.

Then, the traffic profile is defined in a per-flow basis, while the next operations of the what-if-analysis are performed as in the case where a single domain is considered.

3.5 Experimental results

We are working towards the testing of the proposed methodology in the testlab of the IKNOS project aimed at the QoS management in multiservice, multidomain and multivendor networks. The laboratory includes a DS-TE backbone made of CISCO 7609 routers connected with 10GE links and interconnected to the Tiscali ISP network. Since we couldn't evaluate the goodness of the proposed methodology on the real hardware yet, we have made some extensive experiments with the Opnet Modeler simulator.

We considered a single DS-TE domain with 20 core routers and 7 LERs, interconnected by links of different capacity: 10GE, GE, and FE. Six different services are provided: VoIP, IPTV, E-commerce, video streaming, web browsing and E-mail. As to the quality profiles, we have taken into account three KPIs: IPTD, IPDV and IPLR. Table 3.I shows the performed DiffServ classification with the end-to-end KPI values: six standard CoSs are considered according to the service requirements defined in [46]. The service traffic load has been randomly generated for every possible edge node pairs with an overall load of: 15% VoIP, 35% IPTV, and the remaining distributed uniformly among the other services. The RDM model was employed in every router. With these settings the number of possible CT classifications is H=26. Each of them has been evaluated on the basis of the single-hop performance curves, which have been generated by simulations (Opnet Modeler) with self-similar traffic (Hurst parameter set to 0.7). Separate curves have been generated with BCk-1 varying from 0% to 90% of the link capacity. Examples of the obtained IPTD performance curves are shown in Fig. 3.5.

We implemented a software procedure to perform the what-if analysis, which showed that only 15 CT classifications are feasible in every link of the network for the considered scenario. For each of these, the valid bandwidth constraints and the gain functions have been computed. For these classifications, the valid BC Models and the gain functions have been computed for each link. We have set α_k proportionally to the class priority k and β_p to the following values: 0.5 (IPTD), 0.25 (IPDV), 0.25 (IPLR). Further, we chosen γ=10, so that the KPI gain will result more decisive than the bandwidth gain. Fig. 3.6 shows the KPI gain, the bandwidth gain and the total gain functions for a single representative link where we obtained 165 BC Models that allowed the network to provide the required QoS levels. Higher BC combination indexes in the graphics correspond to higher values of the parameter K of CTs per classification. In particular,

Table 3.I. DiffServ classification

CoS	Services	*IPTD*	*IPDV*	*IPLR*
EF	VOIP	[0-100]ms	[0-50]ms	10^{-3}
AF41	IPTV	[0-400]ms	[0-50]ms	10^{-3}
AF31	E-commerce	[0-400]ms	-	-
AF21	Video Streaming	[0-1]s	-	-
AF11	Web browsing	[0-4]s	-	-
BE	E-mail	-	-	-

on the considered link we obtained 33 BC combinations for $K = 3$, 60 for $K = 4$, 54 for $K = 5$ and 18 for $K = 6$. For each K, the combinations are listed so that higher indexes correspond to CT classifications with more CoSs in the higher priority CTs. Note that higher the number of CoSs in the higher priority CT, the lower the gains. Further, we can observe that the contribution of the bandwidth gain on the total gain is limited to modify the gain for adjacent combinations which correspond to the same CT classification.

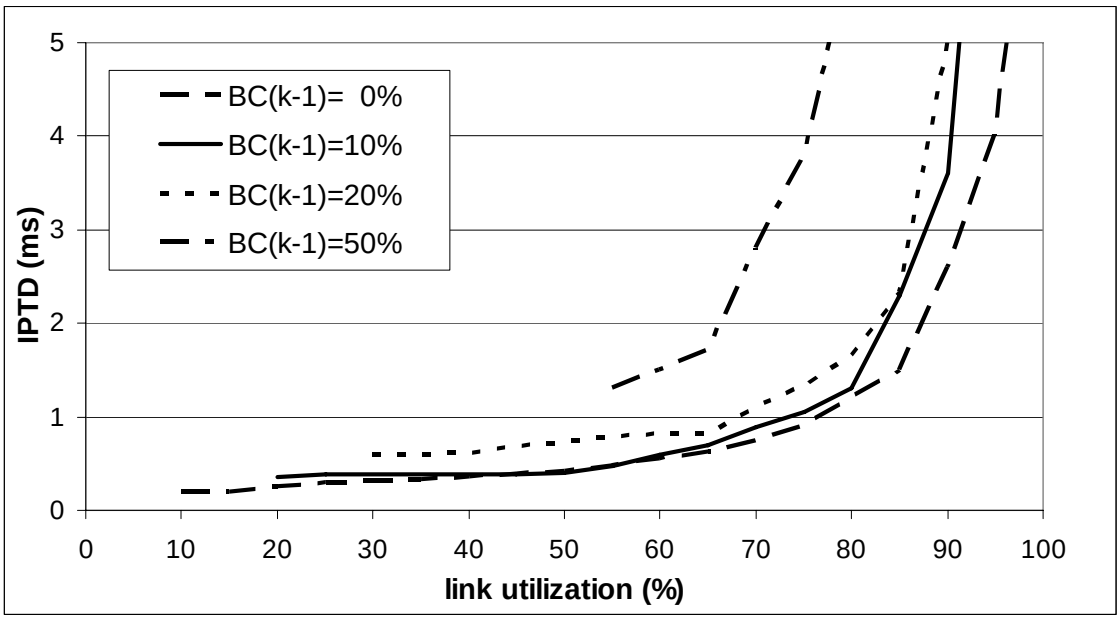


Fig. 3.5. IPTD performance for a single-hop for four different BC_{k-1} values.

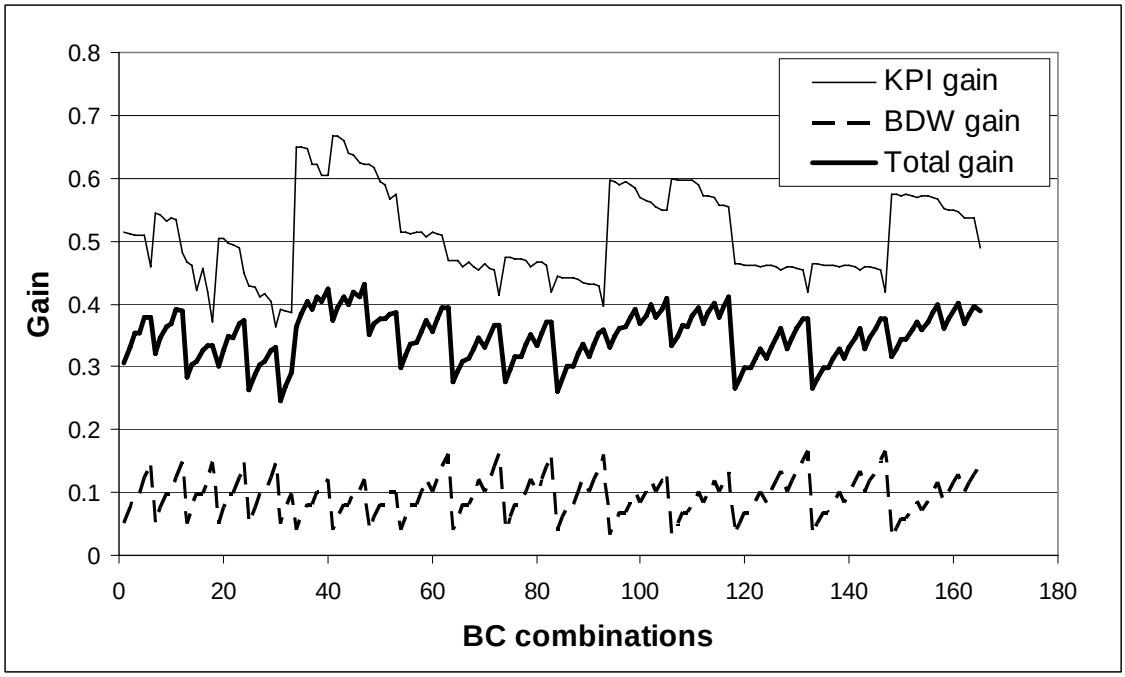


Fig. 3.6.Gain functions for a representative link.

From the performed what-if analysis, the optimal solution (highest total gain) resulted to be that with index h=12, which corresponds to the following: CT3={EF}, CT2={AF41}, CT1={AF31, AF21} and CT0={AF11,BE}. This gave the highest gain values in more than 60% of the links. The corresponding BC Models per link differ on the basis of the link capacity and the traffic distribution. For the link that we have considered in the example of Fig. 6 the optimal BC Model is the following: BC3=1.5Gbps, BC2=5.8Gbps, BC1=8.8Gbps, BC0=10Gbps. With this configuration, we have obtained a maximum total gain of 0.43, which should corresponds to a single-hop gain of almost 1.9ms as to the IPTD and 0.45ms as to the IPDV.

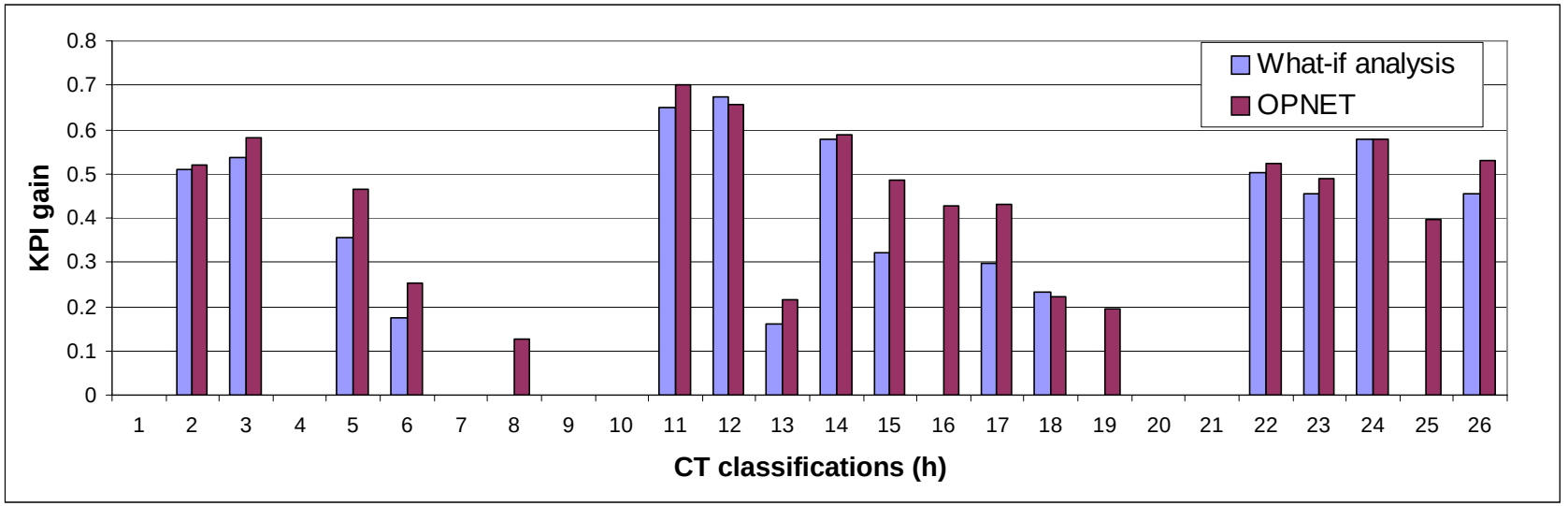
Note that these results have been obtained using the predicted traffic distributions and the performance curves obtained through off-line simulations (as those in Fig. 3.5). To evaluate the accuracy of the proposed system, we have simulated all the considered configurations with Opnet Modeler. For each router and link, the RDM model has been configured according to each of 26 possible CT classifications and any possible BC combination. Simulation results obtained with Modeler have been compared with those obtained from the previously described what-if analysis, as shown in Figs. 3.7(a)-(b). Fig. 3.7(a) shows the average KPI gain for all the links in the network: we show the gain for any feasible classification when we set the best bandwidth constraints per single link. Fig. 3.7(b) shows the total gain for the same representative link of Figs. 3.5 and 3.6, considering five CT classifications with different BC combinations. Note that the gain values resulting from the what-if analysis are in line with those obtained with Modeler. Small differences are mainly due to the distribution of the traffic during simulations with those

that we have predicted. In Fig. 3.7(a), we can observe that the CT classifications which have been discarded by the what-if analysis in Opnet are either unfeasible or provides very low KPI gains. The optimal CT classification in OPNET is that with *h*=11: CT3={EF}, CT2={AF41}, CT1={AF31} and CT0={AF21,AF11,BE}. The optimal bandwidth constraints for the link in Fig. 3.7(b) is the following: BC3=1.5Gbps, BC2=6.2Gbps, BC1=7.5Gbps, BC0=10Gbps. These results are very similar to the one obtained with the what-if analysis: BC3=1.5Gbps, BC2=5.8Gbps, BC1=8.8Gbps, BC0=10Gbps. The respective KPI and total gains are very close, confirming the accuracy of the performed analysis in computing the optimal BC model configuration.

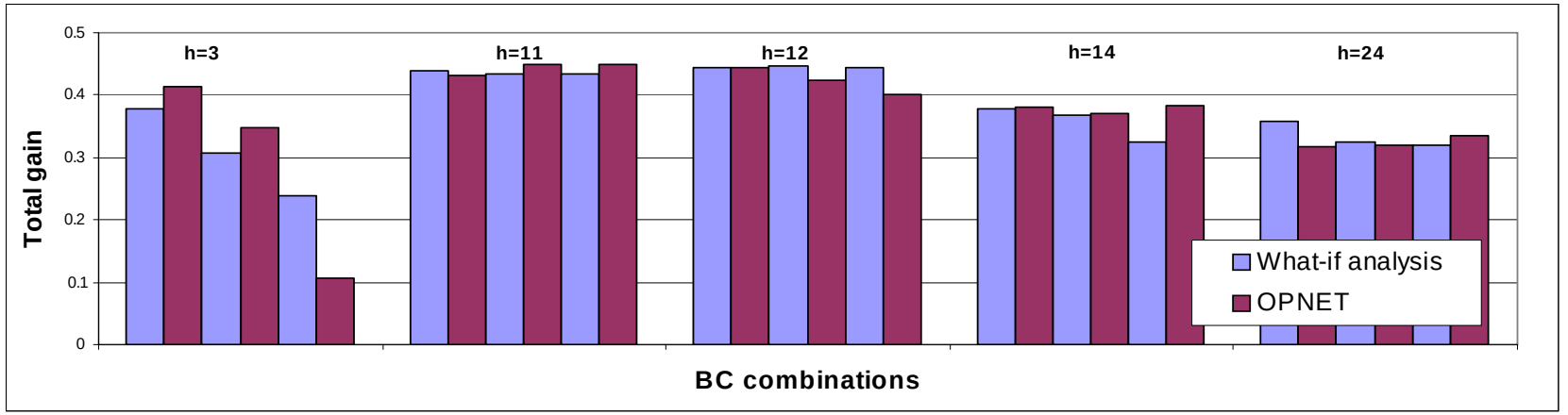
We have also evaluated the impact of the devised procedure on the end-to-end network performance and the preemption ratio. Since we couldn't find alternative solutions to the addressed problem, we compared our algorithm results with those that may arise from straightforward and simple setups, that we refer to as *default1* and *default2*. *default1* differentiates the traffic for real-time applications, non-real time applications and services which do not require any QoS guarantees, which correspond to mapping with index *h*=9: CT2={EF,AF41,AF31}, CT1={AF21,AF11} and CT0={BE}. *default2* maps each service into a different CT and corresponds to classification *h*=26. In both cases, the BCs have been simply set in proportion to the predicted load. The comparison in terms of end-to-end delays and preemption ratios is provided in Table 3.II. Note that default1 brings to a configuration that doesn't allow the network to provide the QoS level as required by the VoIP service. This was also predicted by our what-if analysis. As to *h*=26, it brings to higher delays for the services with highest priority (voice and TV) and similar results for the others. The most important difference concerns the preemption ratio, which is quite high for h=26. In fact, this configuration brought to a low bandwidth gain which increases the probability of preemption occurrences. Differently, for *h*=11 and *h*=12 we obtained high bandwidth gains which brought to higher total gains.

Table 3.II. Average end-to-end performance and preemption ratio results

	IPTD (msec)						**Preemption ratio (%)**
	VoIP [0-100]ms	IPTV [0-400] ms	E-commerce [0-1000]ms	Video Streaming [0-1000]ms	Web browsing [0-4000]ms	E-mail -	
h=9	135.3	135.3	135.3	667	667	27622	0.600
h=11	51.7	82.2	136	920.80	920.80	920.8	0.157
h=12	50.05	80.47	322.66	322.66	993.3	993.3	0.159
h=26	57.97	91.5	173	352.42	963.67	1065	0.352



(a). Average KPI gain for every link of the network.



(b). Total gain for some CT classifications and BC combinations for a representative link.

Fig. 3.7. Comparison between what-if analysis and Opnet results.

Finally, we evaluate the validity of the computed bandwidth configuration when variations on the predicted traffic load occur. The case when the traffic of all services increases proportionally to the predicted one is considered. End-to-end performance and preemption ratio are evaluated and results are shown in Fig. 8, when the configurations computed with the what-if analysis and Opnet are compared with the default ones. As expected, the computed configurations offer the optimal solutions also for traffic increase. Further, concerning the end-to-end performance, we can note as the IPTD values for the computed configurations result still close to the desired ones for additional traffic lower than the 20% of the predicted load. In Fig. 3.8(a) we reported only the results for the video streaming service, since they are the most representative of the average behaviour. In regard to the preemption ratio, for h=11 and h=12 it keep values around 0.2% for additional traffic lower than the 30%, giving acceptable performance against the 0.15% preemption ratio value computed for the predicted traffic load. These results demonstrate the validity of our methodology also when the effective traffic increase against the predicted one of 20%, entailing the need of configuration update only when significant traffic variations occur.

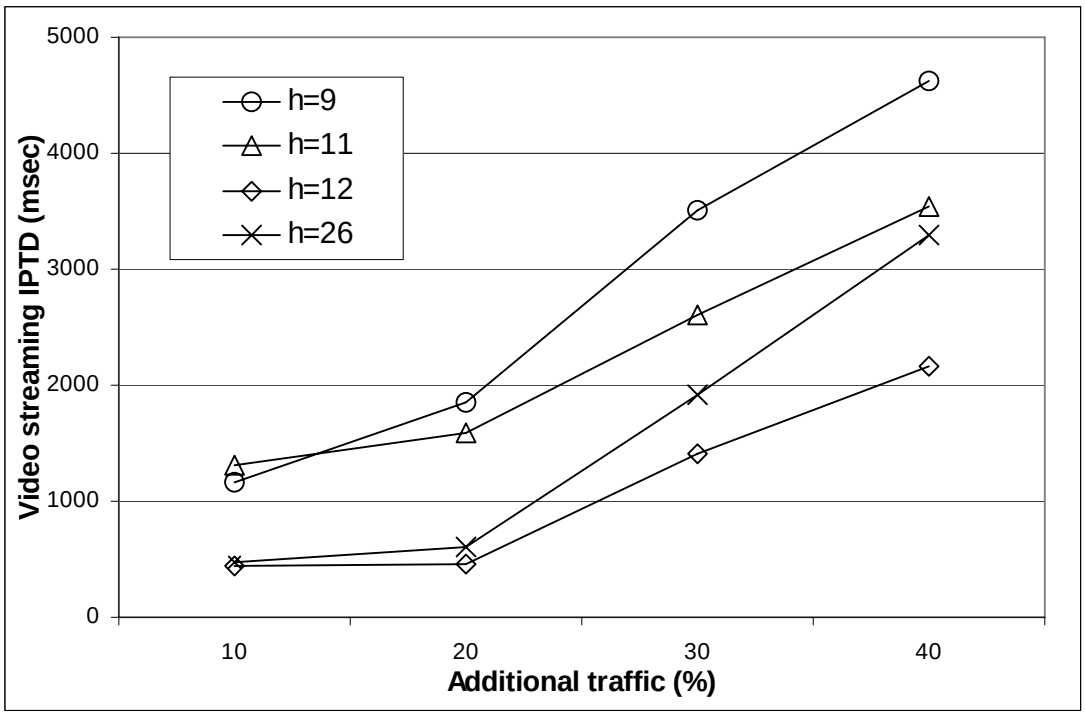
3.6 BC model computation with Genetic Algorithm

After developing the described methodology for BC Model computation, a further solution was proposed. It consists in using the genetic algorithm (GA) to reduce the computation complexity so that our algorithm can be applied either on-line and off-line.

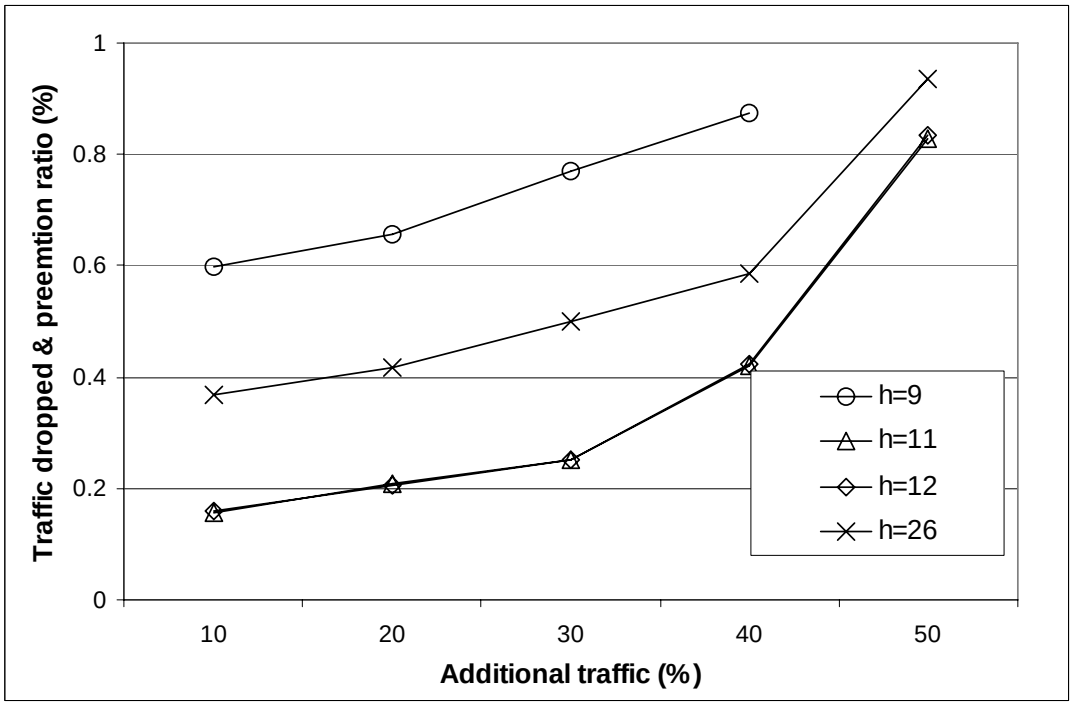
Genetic Algorithms are adaptive heuristic search algorithm based on the evolutionary ideas of natural selection and genetic. The key concept of GAs is the simulation of processes in natural system necessary for evolution. They are modelled on the principles of the evolution via natural selection, employing a population of individuals (*genes*) that experience selection in the presence of events such as mutation or recombination (*crossover*). A *fitness function* is used to evaluate individuals, and to govern the reproductive process.

The steps of a GA are the following:

- Randomly generate an initial population G(0)
- Compute and save the fitness function *f* for each individual in the current population G (t)
- Generate G(t+1) by probabilistically selecting individuals from G(t) via genetic operators
- Repeat from the second step until satisfying solution is obtained (the evolution of the GA is stopped once either a selected number of iterations has been reached or the fitness function maintains the same value for N_{tot} iterations).



(a) End- to-end IPTD for video streaming service



(b) Traffic dropped and preemption ratio

Fig. 3.8. End-to-end performance and preemption ratio against traffic variation.

In the case of BC model computation problem, a solution (*gene*) to the GA is a specific traffic distribution from which deriving the set of BCs for every network link. The algorithm work on the following information:

- network topology and resource attributes;
- number and typology of CTs which have to be activate between each pair of LERs;
  - for each CT the attributes of the corresponding TTs, their quality requirements (KPIs) and have to be specified;
- the expected traffic load for CT;
  - this may be specified in the SLAs or computed through measures on the existing traffic;
- a reference BC Model (MAM, MAR, RDM or others). For presentation convenience, we assume the same BC model on every link.
- the *fitness function f*.

The solutions of GA, that are the genes, are the possible traffic distributions which may be computer thought a CBR algorithm. In this context, we chose to use the constrained SPF (CSPF). As described in section 2.3.3, it is a variant of the Dijkstra shortest path algorithm, computed on a select set of resources. The final result of the GA will be the optimal BC Model setting, that is the solution maximizing the *fitness function.* Note that, unlike the previous what-if-analysis based method, the proposed GA does not compute either CT classification and BC model configuration, but simplifies the process assuming a done set of active CTs. In the following, the proposed method is described.

Let L the set of LERs with cardinality $N=|L|$ (each LER is upstream for X LSP and downstream for Y LSP). For each pair of LER k-z ($k,z \in L$) a set of possible paths is computed by the chosen CSPF and coded in an array $\mathbf{V}_{kz}^{c}$ for CT c. Each element $\mathbf{V}_{kz}^{c}$ indexes one of the paths between the nodes k-th and z-th. On the basis of the expected traffic incoming at the k-th node, a subset of paths toward all directions (downstreams) for each CT has to be computed. For the generic k-th upstream node, different solution can be obtained by combining the different paths. Let M the number of solutions and e T_{km}, the solution tree, with $m=1,\ldots,M$. Each tree contains on each row the indexes of the paths for a downstream LER and for a CT. Note that different paths towards the same leaf node are possible since the traffic between two LERs can be routed on different paths corresponding to different CTs (but also to the same CT). A solution (*gene*) G_i of the GA is a vector N of the indexes of trees selected for each upstream LER: $G_i = \{g_1,\ldots,g_N\}$. The initial population is created by randomly selecting S genes. At the next steps, new individuals are generated with mutation or *crossover* operations on the set of the better parents.

The *fitness function f*(*B*, *P*) used to evaluate the goodness of genes weights two parameters: the variance in the link occupation (*B*) and the average length of paths (*P*):

$$f(B,P) = \alpha f(B) + \beta f(P)$$

- $f(B) = \sum_{c=1}^{N} E^2\{g_c(l)\}$ is the variance of function $g_c(l)$ with $g_{lc} = \frac{B_{lc}}{C_l}$, where B_{lc} the bandwidth for CT *c*-th in link *l*-th, C_l is the link capacity, *N* is the number of CT in the network. On each link, the following condition has to be verified:

$$g_l = \frac{\sum_{c=1}^{N} \gamma_c B_{lc}}{C_l} < B_{Th} \ ,$$

where γ_c weights the traffic load on the basis of the traffic priority (higher the priority is, higher the risk of congestion is) and B_{Th} is the congestion threshold: if $g_l > B_{Th}$, the link is considered in congestion state (for default $B_{Th} = 90\%$ of the link capacity). The values of γ_c are chosen to satisfy some constraints on the risk of congestion. If the link carries out traffic of class *c* only, the maximum possible load is:

$$B_{lc} = \frac{B_{Th}}{\gamma_c} C_l \qquad (3.7)$$

For $c = 1$, $\gamma_1 = 1$ so $B_{l1} = B_{Th} C_l$; for $c > 1$, γ_c has to be in the range $[1, \gamma_N]$ in order to satisfy the (3.7).

- $f(P) = \frac{\sum_{c=1}^{N} \sum_{i=1}^{P_c} \gamma_c \cdot \frac{n_{ci}}{n_{\min,i}}}{\sum_{c=1}^{N} \gamma_c \cdot P_c}$ is the average length (in number of hop) of LSPs weighted in respect to the minimum paths ($n_{\min}$) and the priority of traffic (higher the priority is, higher the weight is). P_c the number of LSPs of class *c*.

The evolution of the algorithm is stopped once either a selected number of iterations has been reached or variation of the *fitness function* between two consecutive steps is lower than 0,5%-0,1%.

At the end of the GA, the BC setting has to be performed on the basis of the obtained traffic distribution. Let $B_l = \sum_{c=1}^{N} B_{lc}$ the bandwidth occupied on the link *l*-th and

$B_{l,av} = B_{Th} \cdot C_l - B_l$ the available bandwidth. Since the BCs have to be setting taking into account a possible margin on the traffic prediction, we impose

$$BC_{lj} = B_{lj} + p_{lj} B_{l,av} \tag{3.8}$$

The B_{lj} value relies on the reference BC model:

- if the BC Model provides for bandwidth isolation between CTs, as MAR o MAM: $B_{lj} = B_{lc}$ with $j = c$.
- if the BC Model provides for bandwidth sharing between CTs, as RDM: $B_{lj} = \sum_{c=j}^{N} B_{lc}$.

$p_{lj} B_{l,av}$ is the bandwidth margin for traffic of class *j*. The coefficients p_{lj} allow the operators to divided the exceeded bandwidth between CTs, taking into account that the maximum traffic load for class $c = j$, that is $\frac{B_{lj} + p_{lj} B_{l,av}}{C_l}$, has to satisfy the (3.7), so $0 \le p_{lj} \le \left[\frac{B_{Th}}{\gamma_j} - B_{lj} \right] \frac{1}{B_{l,av}}$.

Chapter 4

QoS in Video Streaming Applications

In the context of Quality of Service technologies, network architectures have to be integrated with ad-hoc application level solutions to achieve optimal QoS guarantees also in real-time scenarios. For example, the deployment of a quality system is an important requirement in video streaming applications, particularly for wireless networks where channel resources are often shared among a variable number of stations using a contention-based access mechanism. In this context, the resulting throughput available for the video server has been demonstrated to be bursty, which is a feature that makes high-quality video streaming quite difficult. On the basis of this observation, we propose a rate control algorithm that works adjusting the rate on a per-window basis to compensate low-throughput periods with high-throughput periods so as to avoid the "saw" effect that is typically observed in frame-based rate control. The time axis is divided into windows of fixed size and rate changes are introduced only at the beginning of each window with the aim of keeping the probability of playback buffer starvation lower than a desired threshold during the entire current window. To achieve this objective, the algorithm makes use of a short-term prediction of future network delays using historical data. Simulations proved the efficiency of the proposed algorithm when controlling the starvation probability while avoiding the introduction of sudden changes in the source rate.

4.1 Rate-control in Video Streaming

Due to the recent advances in wireless access technologies and video coding techniques (*e.g.* MPEG-4, H.264), video streaming has gained a key role in the new mobile communications scenario. In view of the increasing demand for wireless multimedia contents, many applications are being deployed and on-demand and real-time video services are becoming accessible from the last generation mobile devices. Notwithstanding this progress, there are still many problems to

overcome in video streaming over wireless channels. Indeed, in a wireless environment, communications suffer of the high variability of the channel conditions, which are characterized by a bit error rate (BER) that fluctuates by orders of magnitude in less than a second. Moreover, due to the contention-based nature of common wireless access techniques, the radio interference and packet collision decrease rapidly the channel throughput. It follows that to guarantee the reliability and the quality of video communication, the characteristics of video to be transmitted and the nature of the wireless channels have to be carefully analysed and the use of an adaptive rate control system is mandatory to dynamically modify the system parameters following the channel fluctuations.

In the recent past, many approaches have been proposed to address these problems. A common class of solutions is related on link-layer reliability [47,48]. The work of Zhang *et al*. in [49] distinguishes between two main approaches, that are the *network-centric* and the *end-system centric* approaches. While the first one requires many changes in network components and technologies, the second one works at the application-level, adjusting the bit rate according to the variations of channel conditions, and requires only some functionality upgrades at the end-system points. Several end-system centric solutions have been proposed. Some of these extend the popular TCP Friendly Rate Control (TPRC) to the wireless environment, which is typically used in wired networks [57-59]; some others modify the video codec [60] or are based on a control system at the encoder buffer [61-63]. These frameworks are often computationally intensive, making them unattractive for real-time applications. Furthermore, any of such studies do not take into account the dynamics of the playback buffer, which are very important to maintain continuous video playback.

In this context, we focus on the *end-system centric* approach which has the advantage of requiring minimum changes in the core network. The main challenge in this context is how to design efficient rate control algorithms that allow maximizing the video quality and channel utilization. At first, a hybrid forward error correction (FEC) and automatic repeat request (ARQ) scheme is adopted to obtain reliable transmissions. Then, the proposed rate control method focuses on the fluidity of the video playback by controlling the occupancy of the playback buffer so as not to exceed a desired rate of buffer starvation occurrences. While this constraint has been guaranteed, the encoder maximizes the source bit rate. Rate control is performed adaptively on the basis of a per-window approach, which has the advantage of reducing the fluctuations in the source bit rate, ensuring smooth variations in video quality and avoiding the “saw” effect that is typically observed in frame-based rate control. The proposed system works at the server side, requiring to the client only a feedback on the occupancy of the playback buffer. To optimize the system, we assume that this information is provided at the encoder side through the ARQ feedback channel that is available in two-way communications. In this way, the transmission overhead is minimized and the computational load results very low, mainly at the server side, as required in wireless real-time applications.

4.2 Past Works

The problem of real-time video transmission over wireless channels has been widely investigated in the literature of the past recent years. A common class of solutions is related on link-layer reliability. As proposed by Kallel and Dang in [47] and [48] respectively, ARQ schemes are often used to obtain reliable communications. Generally, in ARQ configurations, the channel throughput is regulated on the basis of the channel condition: when the channel condition is good, the throughput increases and the full bandwidth is used for transmission; when the channel condition is bad, many retransmissions occur and the channel throughput goes down. In most advanced solutions, ARQ schemes are coupled with other approaches to adjust the rate on the basis of some parameters related to the end-to-end video quality.

The work of Zhang *et al.* in [49] distinguishes between two classes of approaches, that are the network-centric and the end-system centric approaches. The first ones give Quality of Service (QoS) provisioning by configuring network nodes so that data rate, delay bound, and packet loss requirements are satisfied [50,51]. The key issue of these approaches is the design of a cross-layer architecture, which allows different MAC/physical layers to communicate with each other, providing an effective cross-layer QoS mapping and QoS adaptation. Although they achieve optimization in the overall system performance, they have the great disadvantage to require significant computational upgrades in the core network components. On the other hand, the end-system centric approaches consist in a set of control techniques, as congestion control, error control, and power control, which work at the application-level without requiring any QoS support at the network-level. In this way, high system performances are achieved with minimum changes in the core network and with lower overhead than in the network-centric case. For this reason, the last researches in video streaming optimization are focusing on the second class of solutions.

The target of an *end-system centric* approach is to make video applications adaptive to the variations of the wireless network condition. Some solutions consist in extending to the wireless environment the popular TCP Friendly Rate Control (TPRC) [51], which was developed for applications over wired networks. TFRC computes the rate as a function of packet loss rate, round trip time and packet size and relies on the assumption that packet loss is a sign of congestion. This assumption is not valid in wireless networks, where packet losses are mainly due to the physical channel errors which do not require any changes in the transmission rate. In [52], a wireless TCP Friendly scheme is proposed, coupling TFRC with a congestion control system that works at the client side. Another scheme, called MULTFRC, was proposed by Chen *et al*. in [53]. It relies on multiple TFRC connections, monitoring the round trip time to decide whether to change the number of TFRC connections. The main disadvantage of this procedure is that it requires many resources to manage multiple connections and entails large rate fluctuations due to the frequent changes in the number of simultaneous connections.

Other solutions perform rate control at the source end-system, adapting video coding or encoder buffer parameters to the variations of the channel transmission. A region-based rate control is proposed in [53]. It consists in a block-based segmentation method which extracts the regions of interest to reduce the amount of information to be transmitted. The authors in [55] analyze the problem of video quality and propose a rate control scheme that avoids the degradation in terms of peak signal to noise ratio (PSNR) that can be caused by the reduction in the bit rate. This scheme provides for a conditional retransmission and low-delay interleaving strategy, in which the encoder buffer is used as part of the interleaving memory. In [56], the authors introduce a rate control mechanism based on a priori stochastic models of the source and the underlying channel. A rate control scheme for H.264 bit allocation is proposed in [57], in which the channel condition and the encoder buffer status are taken into account to compute the estimate channel throughput in both frame and basic units levels. Such studies often do not take into account the dynamics of the playback buffer, which are very important to maintain continuous video playback. Furthermore, some of these frameworks are computationally intensive, making them unattractive for real-time applications.

4.3 Framework and Objective

In this work we address the issue of rate control for video streaming applications by considering a typical wireless scenario where the channel resources are shared among a variable number of stations using a contention-based access control mechanism. This feature, together with the high variability of traffic load and the fluctuations in bit error rates, brings to bursty channel throughputs as perceived by each end-user contending the channel with the other stations [58]. To reduce the number of corrupted packets and obtain reliable transmissions, a hybrid forward error correction (FEC) and automatic repeat request (ARQ) scheme is adopted. While FEC coding adds redundancy to the packets so as to correct possible channel errors, ARQ scheme retransmits those packets received with errors. In particular, we assume that a stop-and-wait ARQ policy is applied. This assumption is justifiable when the round-trip propagation delay is much smaller than the packet transmission time, as is the case in typical wireless LAN environments.

Fig. 4.1 depicts the architecture of the considered video streaming system. It consists of a mobile station client communicating through a wireless link with the video server; the server may be either a mobile station or a fixed system that is connected through a wired network to the AP of the wireless channel. In later case, we assume the wired network to be a high-throughput channel. For both the server and client systems, all subcomponents are shown. In addition to a typical video streaming scenario, which includes video source, display, channel transceiver, encoder, decoder, and their respective buffers, the envisaged architecture also comprises a source-rate control module working at the server side. This is the key component of the proposed

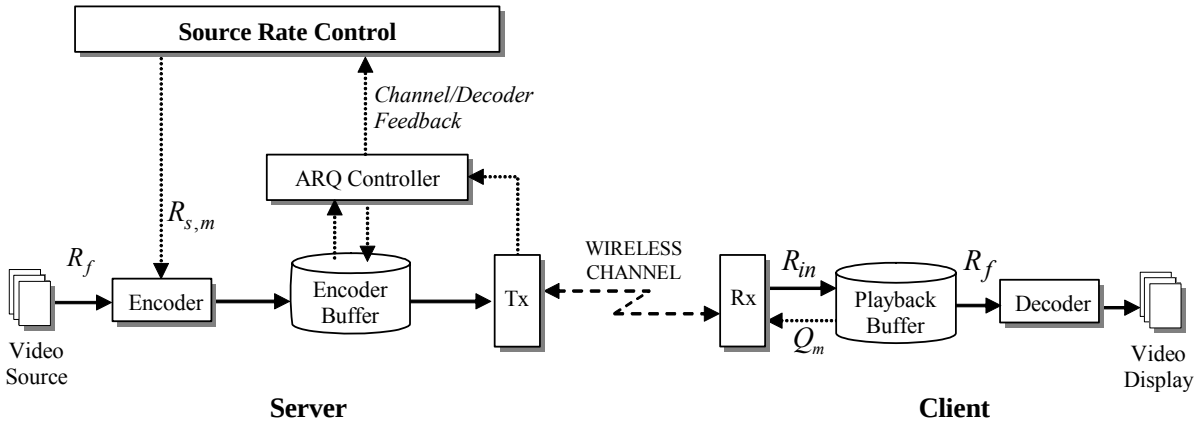


Fig. 4.1. Reference architecture of the video streaming system.

rate algorithm, setting the optimal value of the source bit rate on the basis of periodical feedback on the channel throughput and the playback buffer occupancy, as described in the following. The underlying encoder is assumed to be capable of adjusting its encoding parameters to meet the required rate, as computed by the rate control algorithm. In the figure, R_f is the encoding and playback rate in frames per second, which we assume to be fixed during the streaming session, while R_{in} is the input frame rate at the client, which varies according to the channel conditions.

The video sequences can be either generated in real time or retrieved from a video archive. When a video frame has been coded, it is segmented into one or more packets, which are then delivered to the MAC layer and transmitted over the wireless link. Each packet contains a total of $T = L + H$ bits, where L is the number of information bits and H is the number of error-correcting bits. We assume that L is the same for all the packets during the video streaming session, while H is fixed for all packets that belong to the same video frame. For any given FEC coding scheme (e.g., BCH codes) and a given pair (L,T), a maximum number of correctable bit errors per packet ($E\max = E\max(L,T)$) can be easily determined. In addition, the ARQ policy allows the receiver to send through the feedback channel a positive ACK or a negative NAK depending on whether a received packet is correct or not. When a NAK message is received, the transmitter retransmits the packet. The time required for sending a single frame through the channel and the number of retransmissions required to successfully deliver a packet to the receiver vary over time due to contentions and variable BER.

In the considered architecture, ARQ retransmissions are managed by the ARQ controller, which collects the ACK/NAK messages from the receiver and informs the encoder buffer when a retransmission is needed. By handling the received acknowledges, the ARQ controller is also able to compute the time required to successfully transmit a packet. In particular, when a first attempt of packet transmission begins, the encoder buffer sends a message to the ARQ controller; it then

attends the corresponding ACK and computes the total interval of time required to successfully deliver the packet. In this way, at the reception of each ACK, a channel feedback is sent to the control module by indicating the total time interval that has been spent to send the last packet. We also assume that the ARQ messages convey a feedback from the decoder providing the occupancy of the playback buffer. Because the control packets are relatively small (e.g., few tens of bytes), they can be adequately protected with FEC alone, ensuring that the feedback channel is almost error-free. Accordingly, the ARQ controller is able to compute the time interval that has been necessary to successfully transmit each packet; this information, together with the playback buffer occupancy, is sent to the source rate control module.

The main objective of the proposed rate control scheme is to ensure the continuity of the video playback by limiting the number of starvation events at the playback buffer. To reach this goal, a window-based approach is adopted. The source coding rate is adjusted by considering its effects on an entire window of fixed size so as to allow the playback buffer to build up during bursts of high-throughput periods and to shrink (but not starve) during low-throughput periods. In this way, the burstiness of the channel throughput is compensated without introducing the "saw" effect in the source rate that is typically observed in frame-based rate control. Accordingly, the time axis is divided into windows of fixed size T, which we index with m (m = 0,1,2,…). At the beginning of each window m, the source rate control module computes the probability of playback buffer starvation during next window on the basis of the buffer occupancy and the information on the channel behaviour. It then sets the source coding rate $R_{s,m}$, which is applied during the current window so that this probability is lower than a given threshold.

4.4 Control of the Playback Starvation Probability

Consider the buffer occupancy during the m-th window $Q_m(\tau)$ (for $0 < \tau \le T$), which evolves according to:

$$Q_m(\tau) = Q_m + \frac{R_f}{R_{s,m}} Y_m(\tau) - R_f \tau,\ 0 < \tau \le T, \tag{4.1}$$

where $Y_m(\tau) = X(\tau + mT) - X(mT)$, with $X(t)$ being the arrival process which counts the cumulative traffic arrival at the playback buffer in the time interval (0,t). (1) tells that the buffer occupancy is given by the number of frames in the playback buffer at the beginning of the m-th window (Q_m), plus the number of frames sent in the interval τ, minus the number of frames played back during the same interval τ. Note that $R_{s,m}$ is the source coding bit rate for the m-th window, which is imposed to the encoder by the control module. As already mentioned, the objective of the control module is to compute the values of source coding rate $R_{s,m}$ that allows

for a starvation probability lower than a desired threshold; when this constraint is satisfied the maximum rate is selected.

Let $\Phi_m(\tau)$ be the probability of starvation during the *m*-th window. We then require that:

$$\Phi_m(\tau) = \Pr\left[Q_m + \frac{R_f}{R_{s,m}} Y_m(\tau) \le R_f \tau \right] \le \varepsilon,\ 0 < \tau \le T, \tag{4.2}$$

where $0 < \varepsilon << 1$ is a predefined value. This condition is imposed in isolation for every streaming time interval of length *T*. To fulfil the constraint in (4.2), the control module needs the information on the initial playback buffer occupancy and the network traffic during next window. The first information is directly provided by the feedback loop established through ARQ messages, as described in the previous section. Note that for the first window (*m*=0), Q_0 is equal to the *N* frames which are pre-fetched before playback commences. The second information about the process $Y_m(\tau)$ is unknown, but can be predicted based on the observed transmission delays of past packets, which are provided through the channel feedbacks. To this, we proceed as follows.

Let $P_\tau(n)$ represent the probability to successfully transmit exactly *n* frames within interval τ. To compute $P_\tau(n)$, we have to consider the successful transmission of *n*+1 frames, each consuming a time interval t_i (*i* = 1,…,*n*+1), so that $\sum_{i=1}^{n} t_i \le \tau$ and $t_{n+1} \ge \tau - \sum_{i=1}^{n} t_i$. t_i then represents the time interval required to successfully transmit packet *i*: it is the time between the first attempt to transmit packet *i* since the reception of the ACK; note that the same frame can be transmitted more than once in t_i, till the final successful reception at the receiver. The number of retransmissions depends on the applied FEC scheme and the channel state. We now suppose that t_i are i.i.d.; we then drop subscript *i* and we define $f_d(t)$ the probability density function (pdf) of *t*.

We consider that $f_d(t)$ is known while in section 4.4.1 we discuss how we deal with this. Accordingly, $P_\tau(n)$ can be computed as follows:

$$P_\tau(n) = \int_0^{\tau} \int_0^{\tau - t_1} \cdots \int_0^{\tau - t_1 \ldots t_n} \int_{\tau - t_1 \ldots t_n}^{\infty} \prod_{i=1}^{n+1} f_d(t_i) dt_1 \ldots dt_{n+1}\ . \tag{4.3}$$

From this probability we can calculate the pdf $f_{Y_{\tau,m}}(.)$ for process $Y_m(\tau)$ as:

$$f_{Y_{\tau,m}}(y) = \sum_{n=0}^{\infty} P_\tau(n) \pi_{L,n}(y), \tag{4.4}$$

where $\pi_{L,n}(.)$ is the rectangular function equal to one in the range $(n\text{-}1)L \div nL$ and zero elsewhere (recall that L is the size of each frame). Note that $f_{Y_{\tau,m}}(.)$ is a piecewise continuous function as shown in Fig. 4.2.

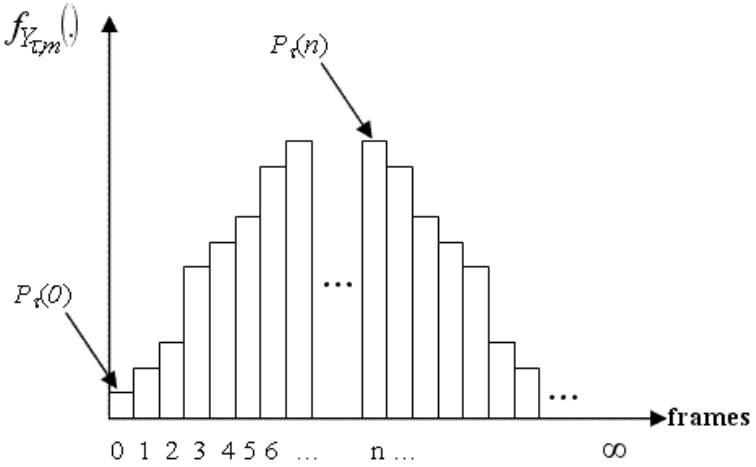


Fig. 4.2. Pdf for process $Y_m(\tau)$.

Now, suppose that $R_{s,m}$ has been fixed for the current window m. The starvation occurs for any (see (4.1)):

$$Y_m(\tau) \le Y_\tau^* = \left(R_f \tau - Q_m\right)\frac{R_{s,m}}{R_f} \tag{4.5}$$

and the starvation probability is equal to:

$$\Phi_m(\tau) = \int_0^{Y_\tau^*} f_{Y_{\tau,m}}(y)dy\,. \tag{4.6}$$

In our framework we operate in a converse way: we set the starvation probability and from that we obtain the appropriate $R_{s,m}$. It follows that at first we compute Y_τ^* from (4.6) so that the $\Phi_m(\tau)$ is equal to ε for $0 < \tau \le T$. Then, from Y_τ^* we compute $R_{s,m}$ by (4.5).

4.4.1 Dynamic Processing of Delay Statistical Trends

The proposed algorithm relies on the availability of the pdf $f_d(t)$. The effectiveness of the proposed control rate scheme then requires a simple statistical method for predicting $f_d(t)$ for future transmissions on the basis of observed measurements. Indeed, network characteristics vary with time and, consequently, the delay statistical trends do; a continuous update of this information is then required to take into account these evolutions. Several approaches can be used to evaluate statistical trends of network delay relying on the analysis of historical and current information. The full aggregation method accumulates data into the probability distribution curve, giving the same weight to old and recent samples; this approach makes the system unable to quickly react to network traffic variations. Differently, the flush and refresh method builds the probability distribution curve on the basis of the last observed *M* packets and leaves out historic information, generating high overhead.

An intermediate approach that we have decided to adopt is the store and track method [59]. This approach does not discard the old data entirely, but gradually reduces its effect on the histogram to approximate the statistical distribution. Each value in the histogram counts the number of occurrences of packets sent within a certain interval of delays (bin). Note that the shorter the bin is, the higher the accuracy in the prediction of $f_d(t)$ is. On the other hand, short bins increase the algorithm complexity when computing (4.3) numerically. To reduce the weight of older samples, each bin of the histogram is periodically scaled down by an aging factor *F*. The aging is applied with frequency *f*.

Let $H_j(x)$ be the function of the histogram after the *j*-th aging and *nd* be the network delay of the new packet, thus

$$H_j(x) = \begin{cases} F \times H_{j-1}(x), & 0 \le x < \infty, x \ne nd \\ F \times H_{j-1}(x) + 1, & x = nd \end{cases}. \tag{4.7}$$

Three different aging algorithms have been proposed. In the first aging algorithm the value of factor F is defined as

$$F = c\,, \tag{4.8}$$

where *c* is the aging coefficient chosen by a user or an application and its interval of variation is between 0 and 1. According to the second algorithm, the value of *F* is obtained as follows:

$$F = \frac{c}{(1-c) \times \int_0^\infty H_{j-1}(x)dx}. \tag{4.9}$$

Finally, the third aging function is the following:

$$F = \frac{c \times f}{(1-c) \times \int_0^{\infty} H_{j-1}(x)dx}, \tag{4.10}$$

where f is the aging frequency, which have been defined to determine how often the aging factor should be invoked. More frequent aging actions, corresponding to lower value of *f*, means that the data is updated often, generating more accurate results. Note that the histogram $H_j(x)$ is updated continuously during the streaming, while its values are used to set $f_d(t)$ only at the beginning of each channel window.

4.4.2 Workflow of the Proposed Algorithm

Fig. 4.3 provides a workflow description of the operations performed by the rate control module. During video streaming, the values of transmission delays t_i for each sent packet are collected. This information is used to build $f_d(t)$ through one of the methods described in the precedent section. To follow network traffic variations, this function is updated with frequency ($f = 1/t_a$) depending on the desired accuracy and the complexity of system. The aging is then performed any instant $t = k \cdot t_a$, *k*=1,2,….

At the beginning of each window, the control rate module computes Y_τ^* so that $\Phi_m(t)$ is equal to ε through (4.6) for each τ ($0 < \tau \le T$). It is important to note that this operation requires the computation of the integral, which indeed is a sum of $P_\tau(n)$ probabilities for *n*=0,1,2,… till the sum is equal to ε. It is important to observe that ε is required to be set to very low values since the playback buffer starvation event should be kept very rare in almost any video streaming scenarios. A typical value is lower than 10-3. It follows that $P_\tau(n)$ needs to be computed only for few values (low values of *n*), as it is shown in Fig. 4.4. This is an advantage from the computational point of view, since $P_\tau(n)$ is computed through convolutions as shown in (4.3).

Y_τ^* allows calculating the source coding rate according to $R_s(\tau) = Y_\tau^* R_f / (R_f \tau - Q_m)$. The following step is the selection of $R_{s,m}$ equal to:

$$R_{s,m} = \min_{\tau \in 0 \div T} R_s(\tau). \tag{4.11}$$

The computational complexity can be reduced further by executing the described steps not for all τ within the range $0 < \tau \le T$ but only for τ=*T*. This simplification comes from the observation that $R_s(\tau)$ decreases as τ increases. This issue is addressed in the next section.

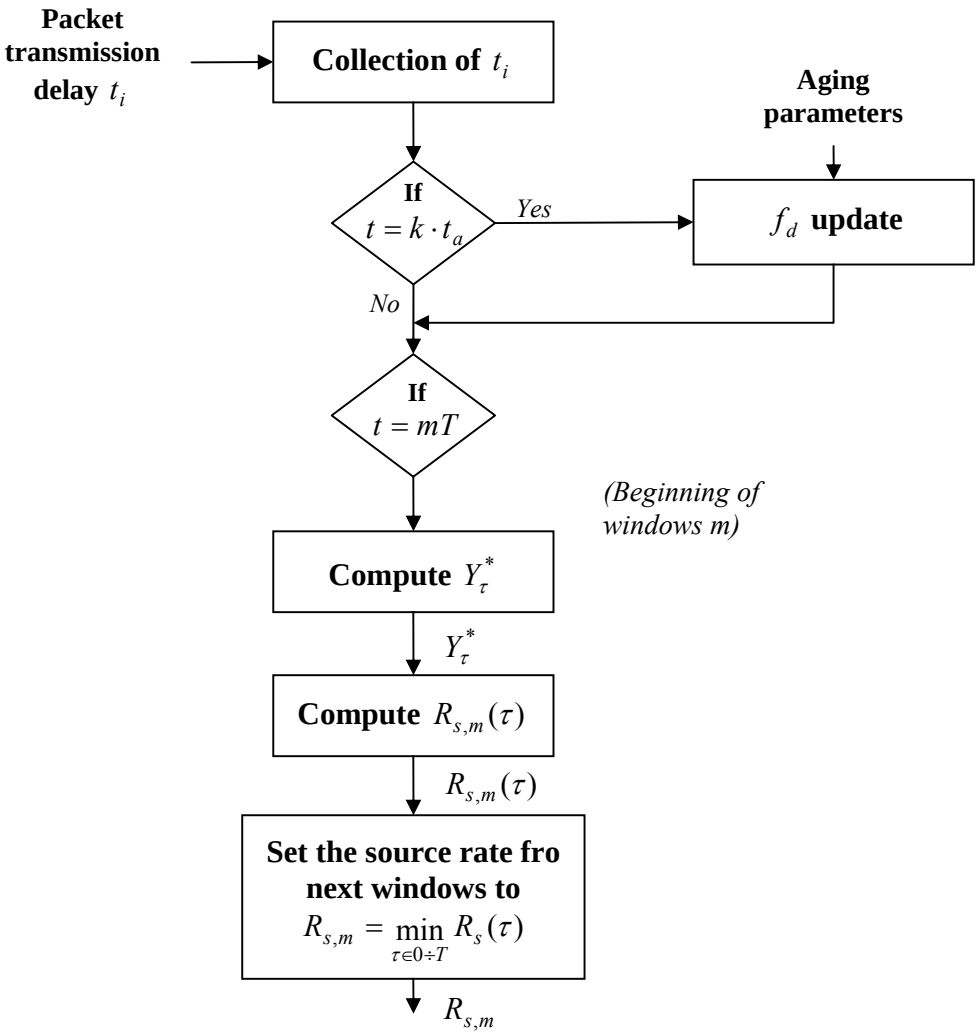


Fig. 4.3. Workflow of the proposed scheme.

4.5 Experimental results

The evaluation of the performance of the proposed starvation control scheme has been conducted by means of extensive simulations replicating typical communications in wireless LANs with highly variable traffic conditions. The background traffic is represented by on-off FTP client-server communications, where the on and off periods are distributed according to the Pareto and Exponential distributions, respectively. The proposed control rate algorithm is implemented in a video server sharing the channel resources with the FTP communications. The wireless channel is modelled using a two-state (good/bad) continuous-time stochastic process in which the sojourn times for the good and bad periods are gamma distributed. During the good

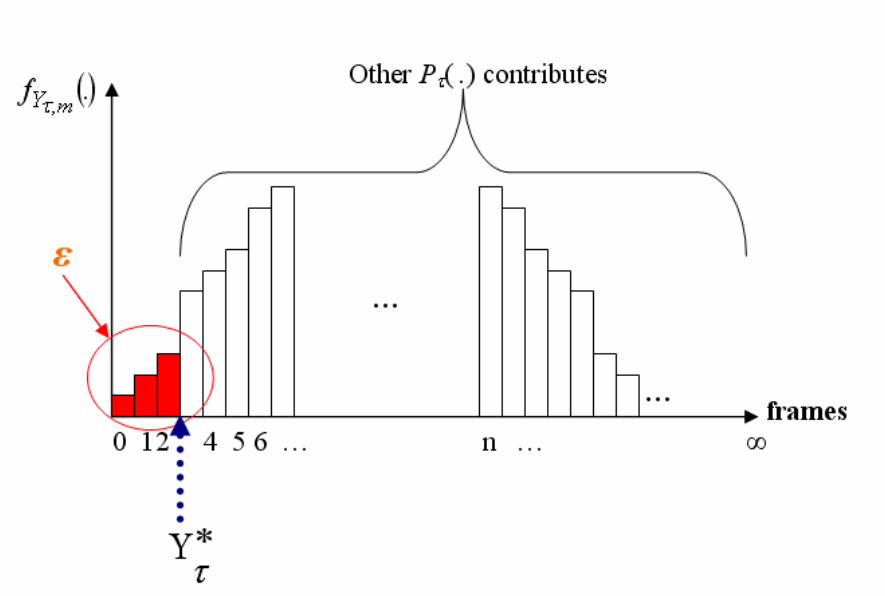


Fig. 4.4. Computation of Y_τ^*.

periods the channels is characterized by low BER values and the bad periods by high BER values. Table 4.I summarizes the key parameter values used in the simulations for system configuration. The meaning of the new variables is the following: C refers to the network capacity, P_g and P_b are the bit error probabilities experienced during the good and bad periods, respectively, and R is the final average throughput computed at the server station. All the simulations have been performed with Opnet Modeler together with the wireless module.

Table 4.1. Values of parameters used in the simulations

Parameter	Value
Number of FTP clients	15
T	1 sec
C	11 Mbps
P_g	10^{-4}
P_b	10-2
R	107,2 kbps
Bin size	10^{-4} sec
R_f	25 fps
ε	10^{-4}

4.5.1 Estimation of the Packet Delay Transmission

Fig. 4.5 shows the typical shape of the pdf for the time required to successfully send a packet considering a bin size equal to 10^{-4} sec. The function spreads over a large range of values, as consequence of the high variability of the channel throughput. The average delay is around 10 msec (100th bin), so that the server is able to send 100 packets on average during a time window (1 sec). To validate the assumption on the independence between successive packet transmissions when computing $P_\tau(n)$, we have evaluated the autocorrelation of the packet transmission delay. The results are shown in Fig. 4.6. We considered the observed delays for 100,000 packets, with a resulting average value $\eta=9.7558*10^{-3}$. The obtained autocorrelation function is equal to $1.8959*10^{-4}$ at $t = 0$ and becomes equal to $\eta^2=9.5176*10^{-5}$ quite quickly ($t \geq 3$). This result shows that the stochastic process is almost memoryless so that the transmission of adjacent packets can be considered independent. This is in support of our assumptions used to write (4.3).

The key operation in the proposed algorithm is the computation of the probability density function $f_d(t)$, which is performed on the basis of past measurements. To analyse the matching between predicted and true values, we make use of the chi-squared test, which is frequently used to verify if data samples come from a population characterized by a given distribution. With this test we are then able to evaluate goodness of the prediction verifying whether the chi-square value is smaller or not than a critical value for a given significance level.

The experiments consist in computing the average chi-squared value for a significant number of cycles (windows of length T) and comparing it with the critical values. For each cycle, we compute the histogram of the delay data observed during the cycle under analysis and determine the expected frequency from the previously predicted pdf. For this estimation we consider all the three algorithms presented in section 4.4.1. A disadvantage of the chi-squared test is that it requires a sufficient sample size for the chi-squared approximation to be valid. For this reason, the bin size of the histogram related to the observed data has been set to 10-3 sec. For the chi-squared test approximation to be valid, the expected frequency should be at least 5; therefore, the algorithm adaptively merges some adjacent bins cycle-by-cycle; note that in this way the degrees of freedom ν is not constant over all the cycles. The chi-square expression is the following:

$$\chi^2 = \sum_{l=1}^{k} (O_l - E_l)^2 \Big/ E_l \,, \tag{4.12}$$

where O_l is the observed frequency for bin l and E_l is the expected frequency for the same bin. For the considered cycles (10,000), the average values of the degrees of freedom ($\bar{\nu}$) and of the chi-square ($\overline{\chi^2}$) are computed, and the assumed hypothesis is rejected if $\overline{\chi^2} > \chi^2_{(\alpha,\bar{\nu})}$, where

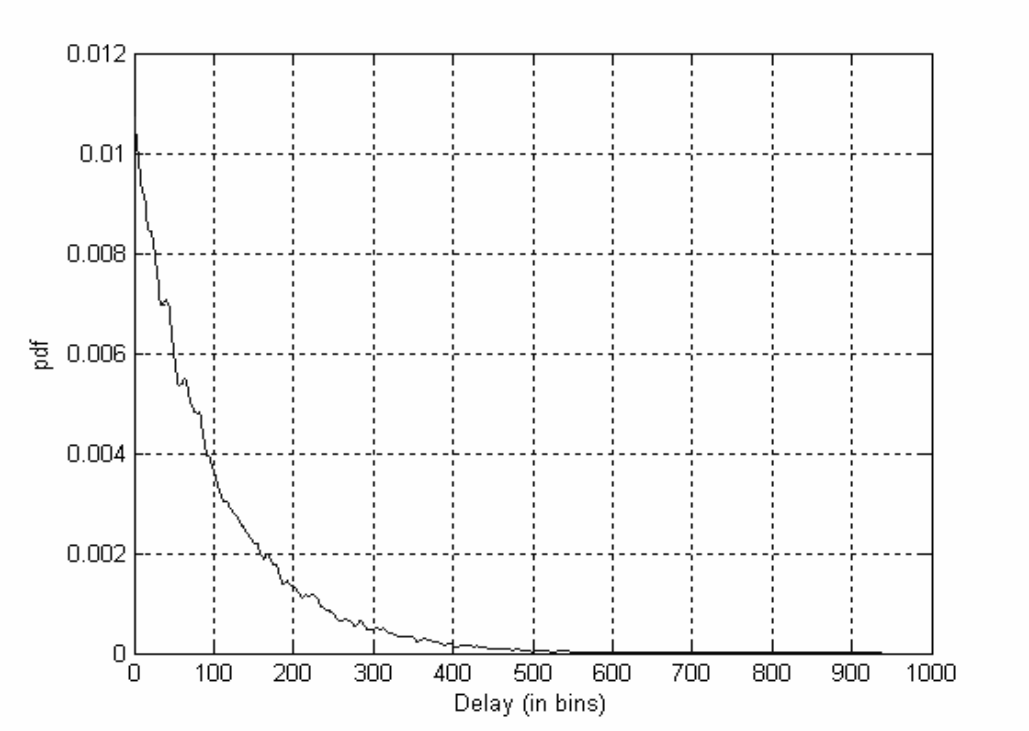


Fig. 4.5. Pdf of the network delay.

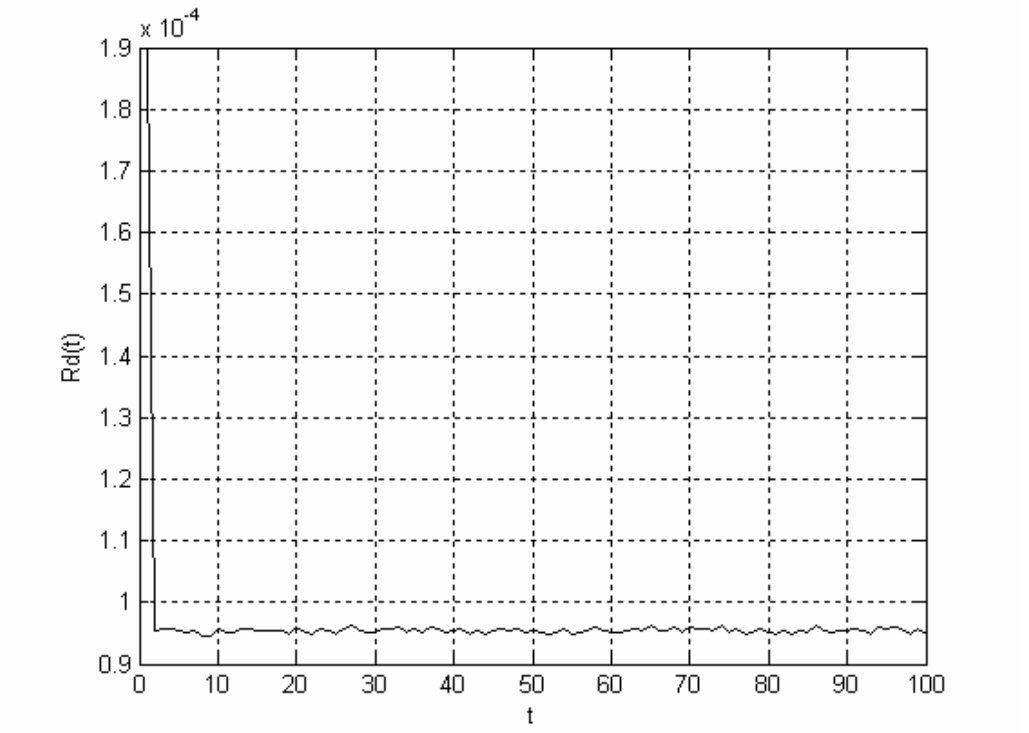
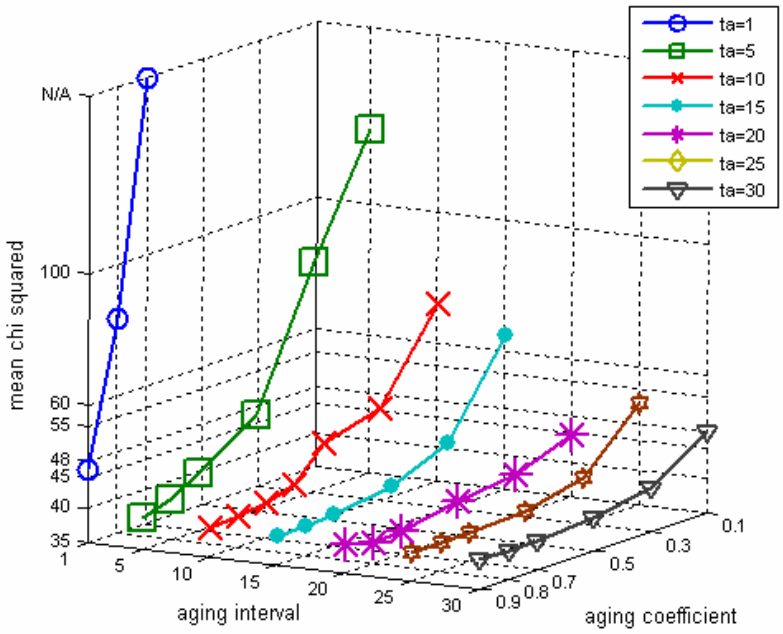


Fig. 4.6. Autocorrelation of the network delay.

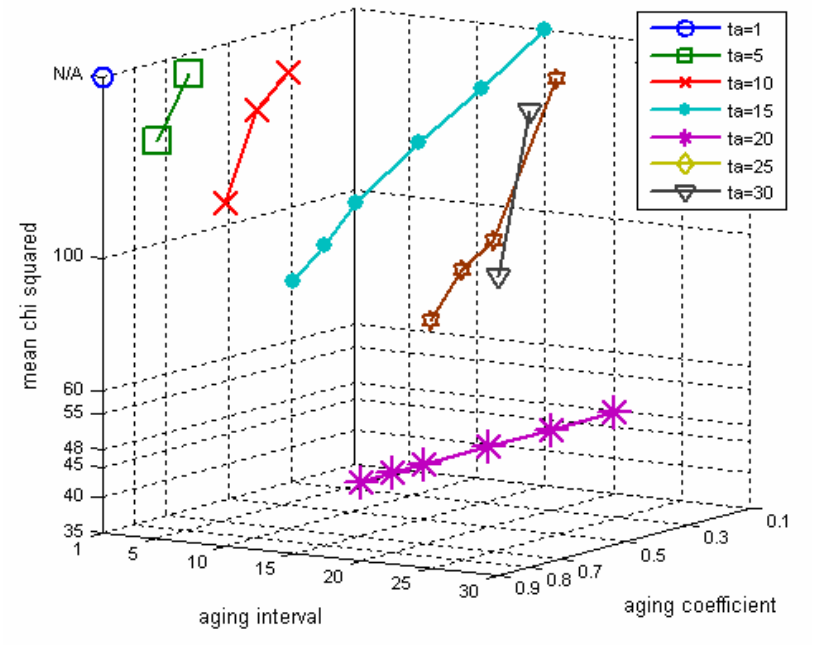
$\chi^2_{(\alpha,\bar{\nu})}$ is the chi-square percent point function with $\bar{\nu}$ degrees of freedom and a significance level of α, which is usually chosen to be equal to either 1% or 5%. Indeed, the lower $\overline{\chi^2}$ is the higher the accuracy of the estimation is.

In the performed tests, the degree of freedom resulted to be around 33, so that $\chi^2_{(0.01,33)} = 54.8$ and $\chi^2_{(0.05,33)} = 47.4$. Fig. 4.7 depicts the results obtained with the three aging techniques varying the aging coefficient c and the aging interval t_a in the ranges 0.1÷0.9 and 1÷30 sec, respectively. For presentation convenience, we have cut the curves when they reached the values 200, which is quite higher than the thresholds of interest.

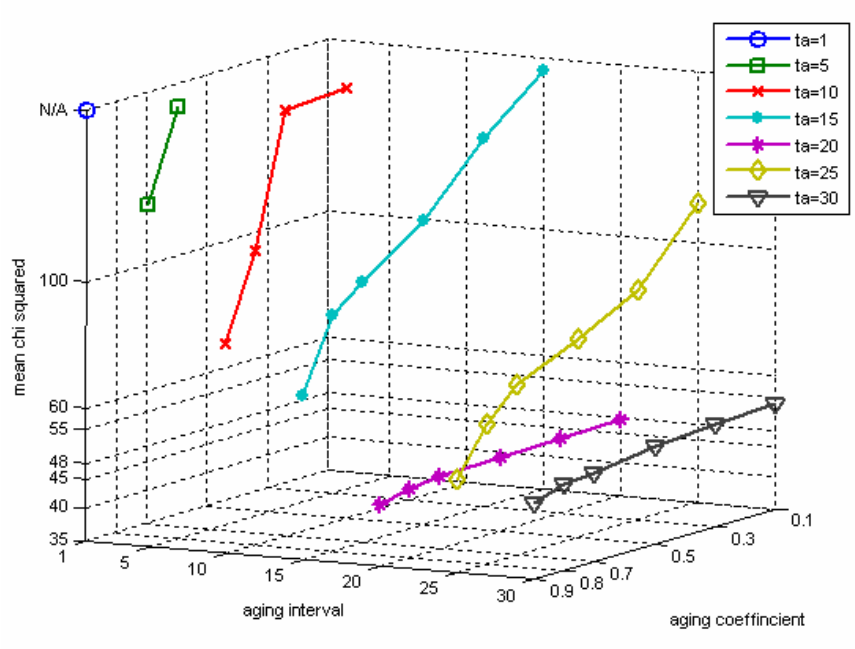
From all the three plots in Fig. 4.7, it results that both the parameters are fundamental in the prediction. With respect to the aging interval, the chi-squared function is characterized by a monotone decreasing shape till a value around 20 sec. The behaviour then changes from this point. This phenomenon tells us that frequent updates of the function bring to not stable predictions, which are too biased by the last observed statistics. Decreasing the frequency we observe that the prediction improves till a point where historical data have a too high weight with respect to the more recent observations. This phenomenon characterizes all the three techniques. As to the aging coefficient, the results show that by decreasing the aging coefficient, the chi-squared value increases reaching values higher than the critical thresholds, so that the hypothesis has to be rejected. Indeed, with values in the range 0.7÷0.9 we have observed the best performance.



a) First aging tecnique



b) Second aging tecnique



c) Third aging tecnique

Fig. 4.7. The value of mean chi squared in term of aging parametres *c* and *f* (mesured in seconds).

Comparing the results of the three techniques, we see that the first one results to be the most stable, notwithstanding the variations of the aging parameters. In fact, for values of t_a equal to 20, 25 and 30 seconds, most of resulting chi-squared values are lower than the critical threshold for $\alpha = 5\%$, while are always below threshold $\chi^2_{(0.01,33)}$. We observe that when t_a is equal to either 15 or 10 sec only the points related to $c = 0.1$ are above $\chi^2_{(0.05,33)}$. Finally, for f equal to 5, the chi-squared values is higher than $\chi^2_{(0.01,33)}$ only when $c < 0.5$. The other two techniques are characterized by a behaviour which is more linked to the parameters settings; however, there are always a couple of parameters settings that allow for obtaining chi-squared values that lower than the $\chi^2_{(0.01,33)}$. The chi-squared test has been performed also when the aging is not applied. The obtained value of $\overline{\chi^2}$ is equal to 39.4, which is lower than the critical value for a significance level of 5% and much more than the critical value corresponding at $\alpha = 0.01$.

The availability of the predicted and actual data at the source rate control module allows for a real-time adaptation of the parameter settings so as to make always use of the optimal parameters during the streaming. This adaptive setting can be driven by the chi-squared test, as presented in this section, or by a simpler approach that makes use of the mean square error (MSE) between predicted and observed data.

4.5.2 Evaluation of the Starvation Occurrences

To fulfil the target starvation probability, (4.11) is analyzed for every $0 < \tau \leq T$; however, we may expect that the higher the τ is, the lower the source coding bit rate (that we have to use) is. This comes from the observation that the variance of the number of bits received in a time interval increases as the length of this interval increases. This imposes a more conservative source coding bit rate for longer time windows. This phenomenon has been demonstrated experimentally: Fig. 4.8 shows the evolution of the source bit rate varying the value of the interval τ for different values of the buffer occupancy at the beginning of the window. Note that the higher τ is, the lower R_s is. The decreasing behaviour of R_s demonstrates that the results obtained for $\tau = T$ are sufficient to guarantee the condition imposed on the starvation for every $\tau <$ T. This is an advantage in terms of computation complexity for the proposed rate control algorithm.

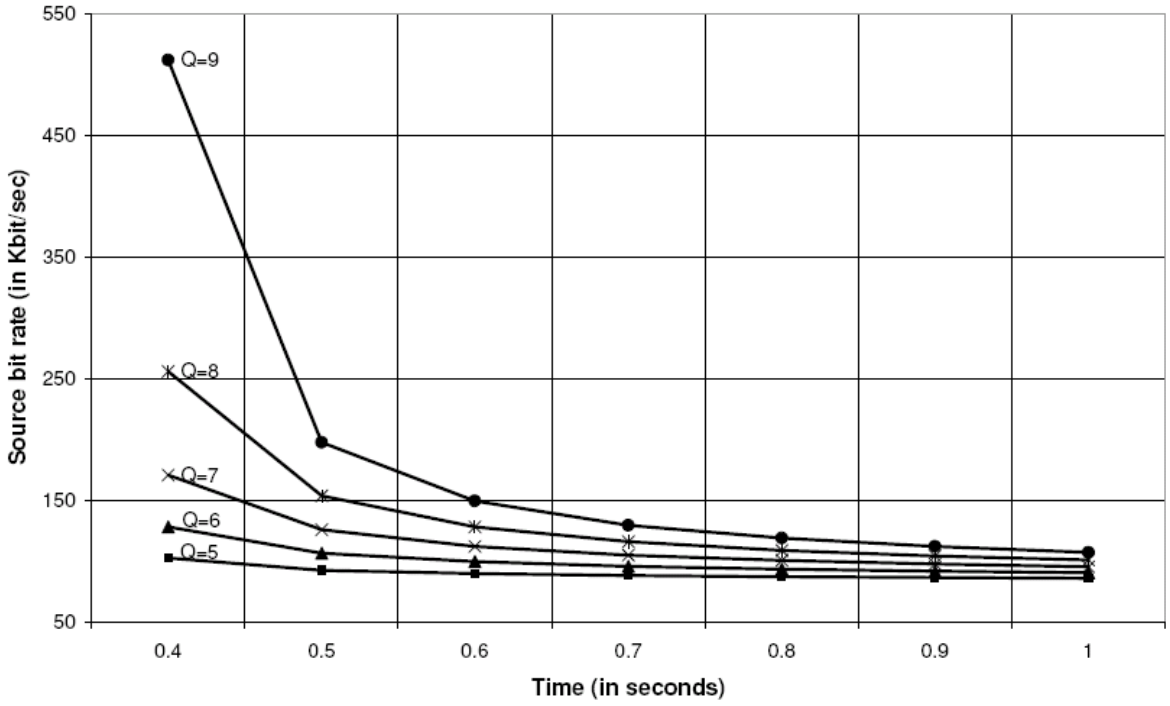


Fig. 4.8. Source bit rate versus T for different initial buffer occupancy values.

Table 4.II shows the key algorithm performance indicators averaged over several runs. The results when using the aging are compared with the no-aging case, which corresponds to the full aggregation approach. For each aging function, we used the best settings of the aging parameters as resulting from the previous analysis. We have always obtained a starvation frequency which is only slightly higher than ε, which is a good result. To evaluate the quality of the streamed video, we have also computed the average value of R_s, which is around the mean channel throughput of 107Kbps, and the standard deviation, which is significantly low. Furthermore, the value of Y_τ^* has been considered to estimate the computational complexity. Indeed, it can be observed that we just need to compute $f_{Y_\tau,m}(y)$ for low values of y, specifically, as soon as (4.5) reaches the threshold ε. Accordingly, $P_t(n)$ has to be computed for few (low) values of n on the basis of the Y_τ^* value. The resulting Y_τ^* values are quite similar for all the algorithms and close to 67.5 Kbit. We have also computed the standard deviation of R_s, which influences the video quality: the lower the value, the lower the video quality variations between adjacent windows. The standard deviation of R_s reaches the lowest value with the third aging method. Concerning the buffer occupancy, this decreases with the growth of the video quality, as expected. The average value of Q is lower with the third aging algorithm, which however provides the highest observed starvation probability. For all the cases, we observed an average value of the buffer occupancy of

about 8 frames, which represents the amount of frames that need to be pre-fetched on average to guarantee the control of the starvation probability.

Table 4.III Results of th proposed algorithm

	Starvation Probability	**Average Buffer Occupancy**	**Average Source Rate**	**Standard deviation of R_s**	Y_τ^*
No-aging	3.3 × 10-4	8.3601	119kbps	65407bps	67
Aging 1	3.3 × 10-4	8.3308	118kbps	65365bps	67.2
Aging 2	3.3 × 10-4	8.3029	118kbps	63424bps	66.5
Aging 3	3.4 × 10-4	8.0302	117kbps	62818bps	68.3

Chapter 5

Quality-oriented authentication systems

The last aspect investigated in this work on QoS technologies concerns a hot problem of the current telecommunication network that is the security of multimedia systems. New applications, as e-commerce or home banking, require a strong level of protection, allowing for verification of legitimate users identity and enabling the user to distinguish trusted from shadow servers. In this scenario, the need for a reliable and user-friendly authentication system becomes always more important. A novel framework for image-based authentication (IBA) is then proposed and evaluated. In order to provide mutual authentication, the proposed method integrates an IBA password technique with a challenge-response scheme based on a shared secret key for image scrambling. The wireless environment is mainly addressed by the proposed system, which tries to overcome the severe constraints on security, data transmission capability and user friendliness imposed by such environment. In order to achieve such results, the system offers a strong solution for authentication, avoiding the need for hardware upgrades and taking into account usability and QoS requirements either at the client and the sever sides. Data and application scalability is provided through the JPEG2000 standard and JPIP framework.

5.1 The problem of authentication in multimedia services

Nowadays, the deployment of a robust authentication system is one of the most interesting aspects for Internet providers and users. The diffusion of new web services, as e-commerce or home banking, has increased the security vulnerabilities, entailing the need for verifying the identity of both contracting parties and for personal data protection. Against such necessity, the techniques of security breaking are constantly growing together with technology; since attacks become increasingly frequent and well performed. Current auto-cracking tools allow the hackers to gain unauthorized access to digital data, generally with the aim of stealing classified

information, as passwords or credit card numbers. In the wireless networks, this problem is still greater as the ward-river community succeed very simply to elude the WEP protocol, traditionally used for WLAN protection. A robust control access system, in addition to privacy and data integrity, becomes the essential condition to support the thriving of World Wide Web and Mobile Internet, allowing the identification of legitimate users and avoiding unauthorized intrusion. Furthermore, applications based on a client-server model require to verify the authenticity of service provider, to avoid the risk of coming up against a shadow server.

The most part of current authentication systems is not able to provide these security requirements, especially in wireless environment, where little computational capability, hardware incompatibilities and poor handiness of user terminals prevent from implementing very complex solutions. For instance, memory-based techniques require the user to precisely recall complex alphanumeric passwords. However, difficulty of password memorizing and poor input-interfaces of mobile devices result in the choice of weak passwords, as common words or short PINs, exposing the system to security threats. Besides, these techniques are capable of guaranteeing the identity of user only (weak authentication). More advanced solutions have been proposed in order to enforce security and achieve mutual or strong authentication, *i.e.* the client authenticating itself to a server and that server authenticating itself to the client in such a way that both parties are assured of the others' identity. These methods are based on encryption algorithms, often requiring specialized hardware, as encryption-calculators, tokens or smart cards. As a result, such solutions are expensive and incompatible with wireless technologies. Consequently, two problems are still to be solved: (i) increasing security and usability of user authentication; (ii) devising a scheme for mutual authentication, possibly for any client's device, from computer terminals to mobile phones. Image-based authentication (IBA) is a valid solution, which guarantees both a high security level without compromising simplicity and efficiency of authentication process. Several experiments of cognitive science show, in fact, that pictures are easier to recall than alphanumeric passwords [60-62]. Furthermore, graphical passwords do not require hardware upgrades and can be combined with techniques of steganography, watermarking or image scrambling to insert secret visual information into messages for server authentication.

Several visual login systems have been proposed in the literature, many implementing a weak authentication only. Déjà Vu [63] requires the identification of five random-art images out of a challenge-set of twenty-five images. Viskey [64] asks the user to select a series of image spots following a precise order. Picture Password [65] and Awase-E [66] require the identification of a correct pass-images sequence, *i.e.* the sequence of images that are chosen by the client during registration, the first employing a single verification stage with a grid of 5x6 images, the second employing multi-step stages, each with a number of images depending on the display size. Unfortunately, the process of remembering a combination of abstract images or a precise order of selection may become harder than the use of traditional passwords, thus nullifying the simplification introduced by the visual approach [67]. Furthermore, most of the

proposed solutions offer a security level comparable to PIN codes, therefore inadequate to current applications, which require the security of 6-8 character long alphanumeric password. Besides, some of such systems are not suitable for small displays and poor handiness of mobile terminals; Viskey, for instance, may be used only with mouse or light pen. Awase-E, although purposely studied for wireless applications, involves the transmission of a large amount of visual information, which is inconvenient due to bandwidth limitation of wireless channels. GPRS network providers, for instance, generally allow for a bandwidth smaller than 56kbps, while the billing system is often traffic-dependant. Moreover, all of the above-mentioned IBA frameworks fail in providing mutual authentication. Other graphical systems have been proposed for mutual authentication. For example, a technique of Visual Cryptography [68,69] provides each user with a transparency, *i.e.* a portion of visual information, which reveals a secret when combined with another sent by the server during the authentication session. Steganography may be used together with visual cryptography; an overview for such approach is given in [70]. The most widely known technique consists in replacing the last bit of each image pixel with a bit of secret information. These systems rely only on the secret keys exchange; one key is stored into the user terminal, while the other is sent by the server at each login request. So, both the user and the server keys are not very protected against theft or network sniffing attacks, allowing malicious clients or shadow servers to break the security system.

We propose a novel mutual image-based authentication framework (MIBA) that exploits platform-scalability in order to achieve a good trade-off between security and data transfer for several applications and devices, such as computer terminals, PDAs and mobile phones. While user authentication is implemented through an image-based password creation process, server authentication is granted by the scrambling of any visual information to be transmitted to the client. The proposed framework makes extensive use of the JPEG2000 standard both for image storage and processing, while relying on the properties of wavelet decomposition for the scrambling and transmission of visual information to the client.

5.2 The wireless environment

It is recognized that wireless networks are very vulnerable to security issues [71,72]. Operative systems currently embedded in mobile devices have been implemented in order to optimize the use of available radio resources rather than guarantee an adequate security level. To interfere into a system based on radio-frequency is often very simple.

Three are the basic security requirements defined by IEEE for the WLAN environment, that is privacy, integrity and authentication [73]. Privacy ensures that confidential information, as passwords, is not transmitted in clear through the network using cryptographic techniques. Integrity provides that messages are not modified during transmission; it is supported by hashing algorithms. Finally, authentication is needed to verify the clients identity and to prevent

unauthorized access. Many applications also require to authenticate the server: data traffic is only sent after mutual authentication is provided.

Typically, the IEEE 802.11 [73] standard supports the Wired Equivalent Privacy (WEP) protocol to protect wireless communications between clients and access points. It satisfies all security requirements even though with many reserves. In particular, privacy relies on RC4 encryption algorithm and uses a secret key of 64 or 128 bits, which are not sufficient for guaranteeing secure applications. Besides, a simple challenge-response scheme is provided for authenticating only the device; no user and mutual authentications occur.

In order to fix the weaknesses in WEP, a stronger protocol has been recently defined: the IEEE 802.11i [74]. Since it requires hardware and software upgrades, a subset of 802.11i specifications, the WiFi Protected Access (WPA), has been introduced to offer an intermediate solution, while the whole standard gains acceptance. The main change of 802.11i standard is the adoption of a new encryption algorithm, the Advanced Encryption Standard (AES), which uses 128, 192 and 256-bit keys. AES is much more robust than RC4, but requires high computational capability for user terminals. For this reason, WPA does not support it and adopts a mechanism still based on RC4, also including a integrity solution. For authentication, IEEE 802.11i can work in two different ways: Personal and Enterprise Modes. The Personal Mode performs user authentication through a numeric or alphanumeric password that is stored in the access point and, optionally, also on the user's terminal. It offers a weak level of protection, similar to WEP. The Enterprise Mode, instead, guarantees for high security performance. It is based on IEEE 802.1X standard [75], requires an external authentication server and provides for algorithms of mutual authentication.

These protocols achieve security for the wireless portion of connection, between client and access point only. In order to grant end-to-end secure communication and to reinforce wireless security, other types of mechanisms, as end-to-end encryption, password protection or applications for end-points authentication must be supplied. For instance, if a user requires Internet access from a wireless network, data protection must be provided on the whole path of communication, together with a mutual authentication system to verify identity of both client and server. The purpose of the proposed approach is then to define an authentication system to provide end-to-end mutual security at application level.

5.3 JPEG2000 Standard

JPEG2000 is the state-of-the-art international standard [76-78] for image data coding based on wavelet-domain decomposition and the EBCOT algorithm. The basic system is completely described in its Part 1, which gained the status of international ISO standard in 2001. Actually,

there exist other 11 official parts, describing several specific aspects of the compression environment.

The basic characteristics exploited in our work are wavelet decomposition and tiling. Decomposition in the wavelet domain is a fundamental aspect of JPEG2000 and is meant to exploit the correlation of visual signal. The image scrambling technique proposed in Section 5.4.2 exploits the properties of wavelet-domain representation for the introduction of pseudo-random ordering of wavelet coefficients. While JPEG2000 images are generally coded as one block, *i.e.* the whole image is wavelet-transformed and coded as a whole, the standard provides for tiling option. When tiles are used, the coding process is applied separately to each tile, in a similar way to JPEG 8×8 pixels blocks. Although tiling is generally applied to very large images in order to reduce computational complexity, the devised framework adopts tiling as a simple technique for decomposing the images used for authentication and for guaranteeing the scalable transmission of local refinement data.

In addition to the baseline algorithm, our interest is mainly on Part 9 - JPIP (interactive protocols and API) [79]. JPIP defines syntaxes and methods for the remote interrogation and optional modification of JPEG2000 codestreams and files. It specifies a protocol consisting of a structured series of interactions between a client and a server by means of which image file metadata, structure and partial or whole image codestreams may be exchanged in a communications efficient manner. For instance, through JPIP the client is allowed to formulate a specific request defining the resolution, size, location, components, layers, and other parameters for the image and imagery related data to be received. The server responds by delivering imagery related data with precinct-based streams, tile-based streams, or whole images. Operatively, the JPIP protocol defines how to generate messages out of portions of single JPEG2000 data-bins. Data-bins contain portions of a JPEG 2000 compressed image representation, such that it is possible to construct a stream that completely represents the information present in a JPEG 2000 file or codestream. For our purpose, JPIP provides for dynamic image data transmission, e.g. single regions or incremental refinement information, through client-server interaction.

5.4 Proposed method

The proposed IBA method is based on a client-server interface [80] to optimize processing, minimize data transmission and improve security. The authentication framework consists of two classical phases: registration and authentication (Fig. 5.1). While registration has to be carried out from a computer terminal, authentication may be performed from any device.

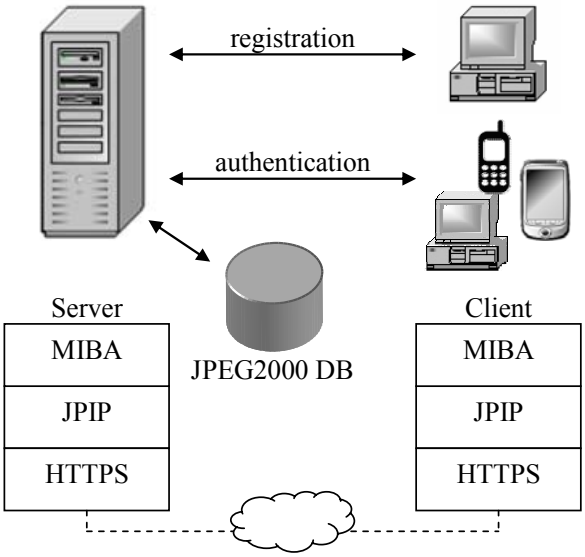


Fig. 5.1. The MIBA framework [80]

The core algorithm at the base of image authentication consists in an iterative selection and zooming, supported by the JPEG2000 standard, through the use of tiling and JPIP protocol. Such choice allows for data-stream scalability and for an efficient transmission and refinement of image information. Further, end-to-end security is granted by the adoption of the HTTPS protocol, which provides for SSL encryption and, optionally, for authentication. Besides, JPIP allows for scalable transmission of image components.

While scalability, thus data transfer optimization, is assured by the JPEG2000 framework, described in Section 5.4.4 and 5.4.5, mutual authentication is obtained through shared-key image encryption. In fact, during the multi-stage challenge-response process for authentication, each time the user requests any visual information, the server provides its encrypted version with the key that was defined during the registration phase. The client must then descramble the visual information in order to make its content understandable. Then there are four possible scenarios:

1. Trusted server:

- *trusted client* – the transaction may proceed and the scrambling/descrambling process is transparent
- *malicious client* – the client is unable to understand the visual content. Even if the malicious client gained possession of the scrambling key, authentication would require the visual password identification. Thus, in this scenario the encryption procedure constitutes a double protection against malicious authentication.

2. Shadow server:

- *the server ignores the system architecture* – in this case it will send uncrypted visual information, even though the user always performs the descrambling process. Such process will again result in the encryption of transmitted visual information, thus rendering the image incomprehensible.
- *the server knows the system architecture* – the server might try a brute-force attack in order to recreate the correct scrambling key. However, such operation depends in part on the user interaction and the shadow server would have only a few tries. Then, even thou the server succeeded in recreating the scrambling key, it should own the client's pass-images in order to include them among the displayed pictures collection.

In order to minimize data transmission in all environments, the major part of data processing is performed on the server side, which is required to store and manipulate the JPEG2000 compressed images, to generate an appropriate key for the scrambling process and to perform the image scrambling during each of image authentication. The server replies to each user's request by providing the correct (scrambled) visual information so that refinement data are preferably transmitted. In order to do so, only the correct portion of information, *i.e.* tiles, subbands, quality layers, is transmitted at each step. On the client's side, the device would only have to perform the de-scrambling, the exact resizing of the received image and the transmission of pass-coordinates.

The message exchange scheme for the registration and authentication phases are shown in Fig.5.2 and will be further described in the following sections.

5.4.1 Registration

The process of authentication requires the user to define three parameters: an access key, a scrambling key and the visual password. Such keys have different characteristics and must be defined during the registration process (Fig.5.2, left). The access key is based on the user's personal data and devices characteristics. It is used to identify the client each time he tries to log in, in order to customize the image-based authentication procedure. Preliminary authentication may be implemented in two different ways through the access key mechanism. While the first consists in defining a shared key to be transmitted each time the user starts an authentication session without intervention, the other requires the user to input some piece of information. Although the second solution is more secure in the case of device theft, the first has been preferred for its simplicity and usability. Then, particular security is not required since the access key has the only purpose of preliminary user identification. Moreover, the case of device theft is generally solved though simple notification by blocking the device or disabling the user's profile (Section 5.4.6).

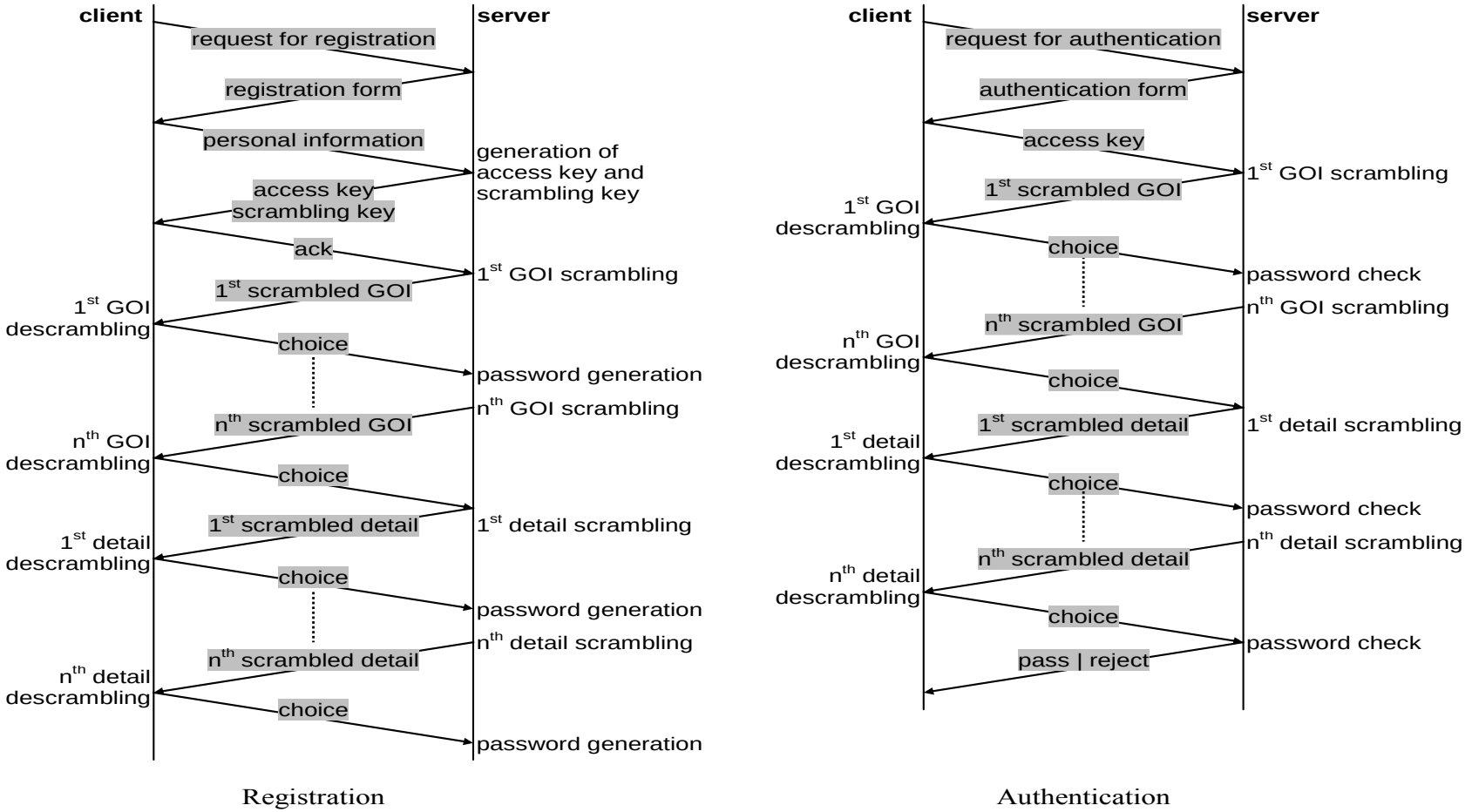


Fig. 5.2. Message exchange scheme for the registration and authentication phases.

The scrambling key is used to generate the pseudo-random sequence that drives the image scrambling process for mutual authentication discussed in Section 5.4.2. Such key is shared by both server and client, but is transmitted only during the registration phase. Finally, the visual password is generated from the user's graphical choices and is used as authentication password.

Then, the registration interface phase allows the user to acquire his access key, scrambling key, to choose the desired images for authentication and to define the graphical password. During registration, the server first presents a traditional form for submitting the user information. While the access key is directly derived from personal data, the scrambling key is generated through a mixture of personal information and random data, such as the current time or the actual content of a few bytes of RAM. Subsequently, the server shows a large set of images, randomly selected from a database of JPEG2000 images and assembled in GOIs (Group Of Images). These images should be inspired by some different themes, excluding random-art and abstract images in order not to compromise the usability of the proposed method. The user must choose k pass-images from the visual database, with the only constraint that one image out of k must be selected only once. For each pass-image a single pass-detail, i.e. the image portion to be used as part of the visual password, must be chosen. Upload of personal images is allowed, although it is generally discouraged, since the authentication process may be easily guessed from personal data. As the registration process may be time consuming and requires the exchange of personal data, it is done online from a computer terminal over secure HTTPS connection.

In order to guarantee data transmission security during registration, HTTPS is adopted with both SSL authentication and encryption. During registration handshake, an SSL secure session is established, including mutual authentication. Then, server and client cooperate in the creation of symmetric keys used for encryption and decryption. In this way, all sensible information, *i.e.* access key, scrambling key and visual password, are well protected against any form of attack. Such procedure is not adopted during authentication, where only SSL encryption is preserved, while authentication is implemented by the MIBA method itself.

5.4.2 Image scrambling for mutual authentication

The mutual authentication feature of the devised system is assigned to image data scrambling for the transmission of visual information from server to client. Server's authenticity is then verifiable "at a glance", while the encrypting technique, combined with the visual password, guarantees a higher level of security.

Several image scrambling techniques have been investigated by the recent literature. They are generally based on the randomization of pixels ordering or on the addition of some variations in the coding algorithm. Lossless scrambling/descrambling is defined in [81], using a periodically shift variant (PSV) discrete system in order to permute pixel disposition. [82] performs visual

information scrambling through changing the fractional phase in a GF(q^n) composite domain. A method based on chaos system is presented in [83]. It not only permutes the image pixels, but also circularly iterates gray pixels values, through a 2D nonlinear map. [84] discusses two kinds of transformations, based on the Fibonacci and Lucas sequences. They totally decorrelate the visual signal, spreading all pixels, while maintaining equidistance as in the original image, and separating adjacent pixels as much as possible. In [85], the scrambling scheme relies on the 2D extension of the discrete prolate spheroidal sequences (DPSS) is proposed. Other methods define image scrambling in a transform domain. A JPEG-based image encryption algorithm has been proposed in [86]. It consists in three steps: the permutation of luminance and chrominance planes by pseudo-random SFCs (Space Filling Curves); the confusion of DCT coefficients in each DCT block, based on different frequency bands; the encryption of DCT coefficient signs. For JPEG2000 images, scrambling methods are proposed in [87,88]. The Part 8 of JPEG2000 standard, named JPSEC [89], provides for the scrambling to be either performed on the wavelet coefficients or directly on the codestream. [87] presents a system based on JPSEC that encrypts the packet body using RC4 and AES algorithms. In [88], a method for partial-scalable scrambling of JPEG2000 coding units, *i.e.* layers, DWT-levels, sub-bands or code-blocks, is proposed. It relies on public-key encryption, which is robust to attacks but results in much more computational cost than secret-key encryption.

Although the previous methods provide several good solutions for the encryption problem, their computational complexity is often high, so that their application may become critical in the case of mobile devices. A choice has been made to develop a simple, yet effective, method, based on the properties of wavelet decomposition. Such choice allows for a nice integration with state of the art coders, such as JPEG2000 or SPIHT and adds only an irrelevant computational cost to the codecs. Moreover, the integration of coding and scrambling makes the system more robust to security attacks. As a drawback, the scrambling process inevitably reduces the wavelet ability to decorrelate the signal energy, resulting in weakened coding efficiency. However, such aspect may be restrained so to offer an adequate perceived quality for reasonable compression ratios. In fact, it must be observed that the application of visual authentication is not particularly demanding in terms of visual quality. Thus, the proposed system is based on three stages of pseudo-random permutations in the wavelet domain: LL coefficients, high subbands blocks and high subbands signs (Fig. 5.3).

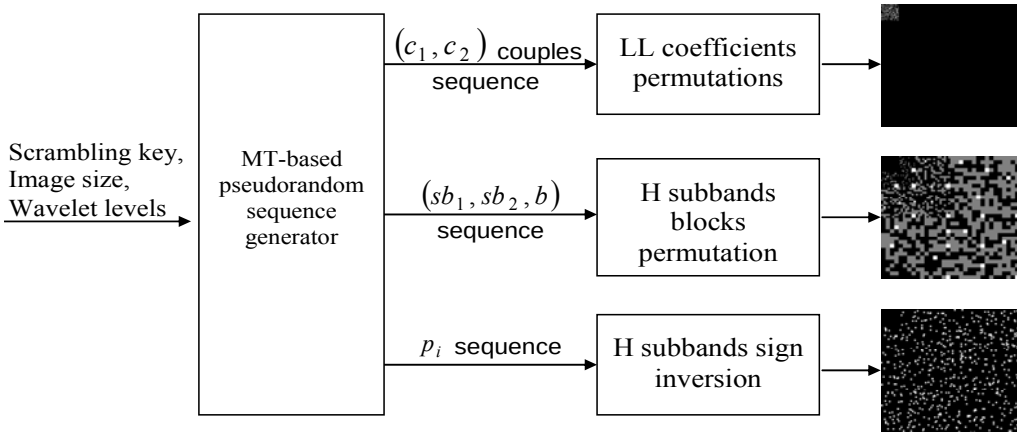


Fig. 5.3. The scrambling method and resulting permutation patterns.

The first aspect to be considered is the generation of a pseudo-random sequence of coordinates to drive each of the scrambling stages. The Mersenne Twister (MT) algorithm [90] has been considered in order to accomplish such task. The method for generating uniform pseudo-random numbers has a large prime period of $2^{19937}-1$, consumes a working area of only 624 words and the sequence is 623-distributed to 32 bits accuracy. Since each stage is meant to drive a particular class of coefficient permutations in the wavelet domain, the pseudorandom generator must provide three different sequences from the scrambling key defined during the registration phase. This is obtained by normalizing the MT output to a desired range that covers each permutation's space, depending on image size and decomposition levels. The scrambling key constitutes then the seed for the pseudo-random generator.

While LL coefficients permutation is straightforward, *i.e.* the sequence (c_1, c_2) defines which two coefficients to exchange inside the LL subband, high subband blocks permutation follows a slightly more complex scheme. In fact, the sequence (sb_1, sb_2, b) defines which two subbands sb_1, sb_2 with indices described in Fig. 5.4 (left), and which reference block b from the largest subband among sb_1 and sb_2 to consider. Block size is proportional to the largest subband size, *e.g.* 2×2 blocks for 32×32 subbands, 4×4 blocks for 64×64 subbands, and so on, so that any subband is divided into 16×16 blocks in the case of square subbands (Fig. 5.4 right).

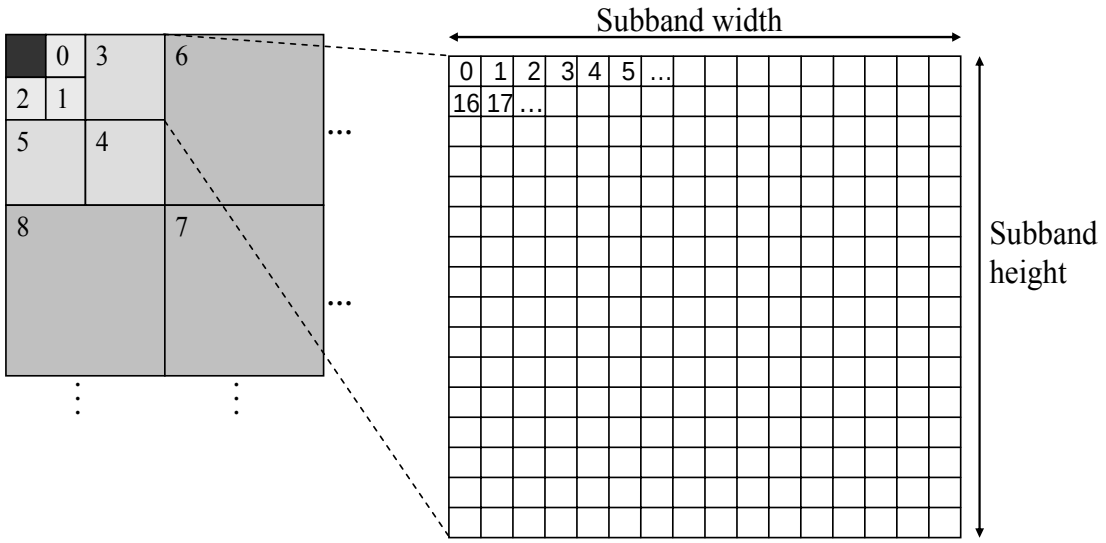


Fig. 5.4. Indexes definition for subband selection (left), and block selection (right).

After determining the largest subbands among sb_1 and sb_2, the reference block position b and block size, the algorithm searches for the block in the smaller subband, which satisfies the condition of having the least MSE (Mean Square Error) with the reference block (target block). The two blocks of coefficients are then exchanged. Such simple procedure may be schematized as follows:

```
For each (sb1, sb2, b)
  s_max = MAX(sb1, sb2); s_min = MIN(sb1, sb2)
  size_reference_block = size_target_block = size_smax / 16
  position_reference_block = b
Find target_block in s_min that minimizes MSE(reference_block, target_block)
  Permute target_block and reference_block
```

Finally, sign inversion is driven by the index sequence p_i. Starting from each index, the algorithm searches for the coefficient with greatest absolute value in a neighbourhood of:

$$(subband\_width/16)\times(subband\_height/16)$$

coefficients. The sign of such coefficient is then inverted. Both *H* blocks permutation and sign inversion stages are implemented as a reasonable trade-off between computational complexity, which is maintained very low, and minimization of the effect of scrambling on compression performance. In fact, the choice to permute blocks with minimum MSE distance and invert the sign of locally maximum coefficients guarantees that the decomposed signal decorrelation is not dramatically reduced. Another interesting aspect of the proposed method is that the descrambling process simply follows the scrambling procedure by reversing the order of each permutation sequence.

In order to evaluate the proposed algorithm in the application environment, 10 different test images have been considered, with three levels of detail each. In Fig. 5.5, the average rate-distortion curve is shown for each detail level, considering correct scrambling/descrambling (cd) and wrong or no descrambling (wd). As expected, higher detail level corresponds to more efficient compression, since the image content decreases accordingly. Moreover, although the scrambling/descrambling process has still an important effect on coding efficiency, *i.e.* there is an average deterioration of 5 to 8 dB compared to unscrambled coding, at a bitrate of 1.5bpp the system offers adequate image reproduction. This is also illustrated by Fig. 5.6, where a visual comparison between unscrambled, correctly descrambled and wrongly descrambled images is provided. It must also be observed that wrong or no descrambling, or equivalently wrong or no scrambling with correct descrambling, results in unintelligible image data, achieving a constant PSNR of about 15dB.

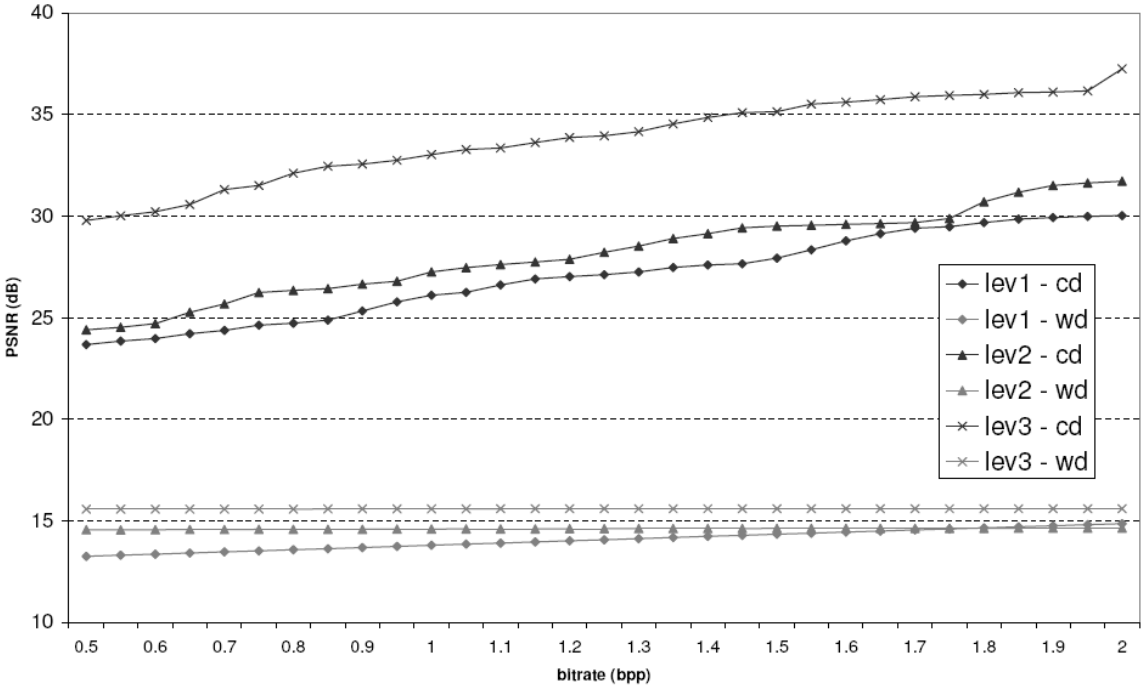


Fig. 5.5. Average coding results for three detail levels with correct (cd) or wrong/no (wd) descrambling.

To evaluate computational cost, 10 different test images have been processed with complete co-decoding and scrambling-descrambling phases. Compression has been carried out at 16 different rates, ranging from 0.5 to 2bpp, in order to evaluate the incidence of the proposed scrambling technique with several codec settings. Average results are presented in Fig. 5.7 as the ratio between scrambling-descrambling time and complete processing time. Three different scrambling profiles were used and are reported as *L*, *H*, *S*, meaning the number of low, high frequencies and sign permutations respectively. It must be observed that results shown in Fig. 5.5 and 5.6 were obtained with the profile *L*, *H*, *S* = 80, 400, 1000. As expected, computational cost is inversely proportional to the scrambling profile and decreases for increasing compression rates. With the chosen profile (80, 400, 1000), the incidence of the scrambling technique is maintained around 10-13% without any code optimization.

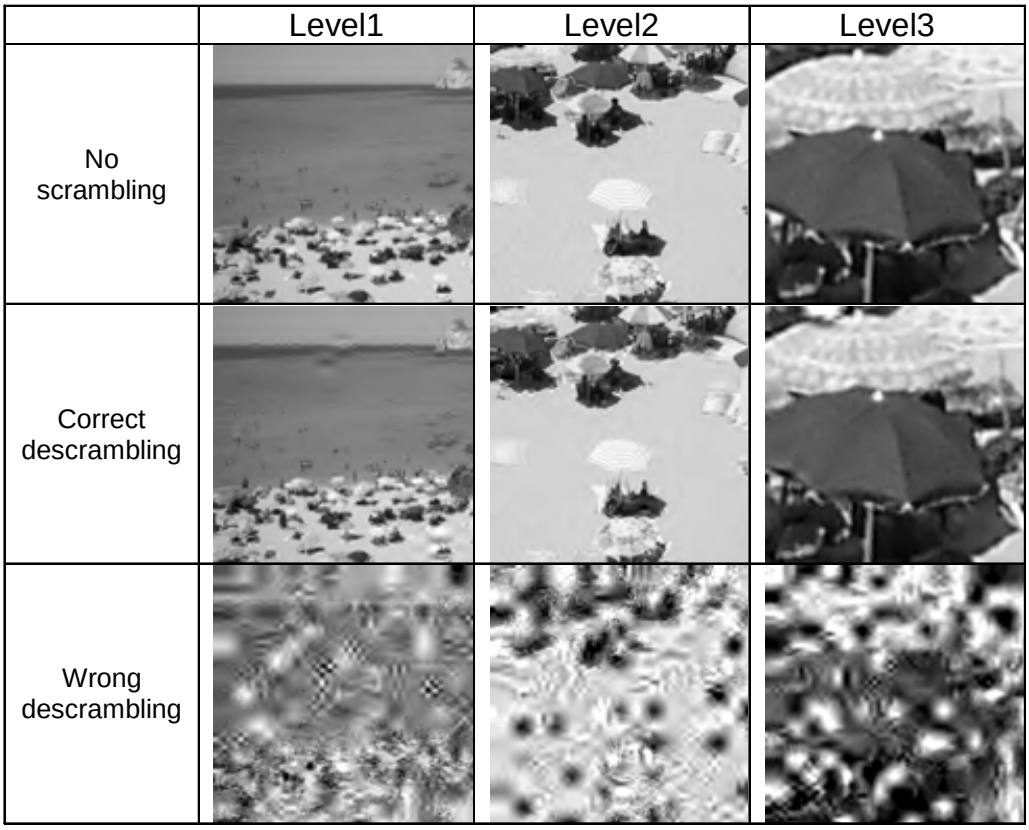


Fig. 5.6. Example of visual results for the scrambling technique, coded at 1.5bpp.

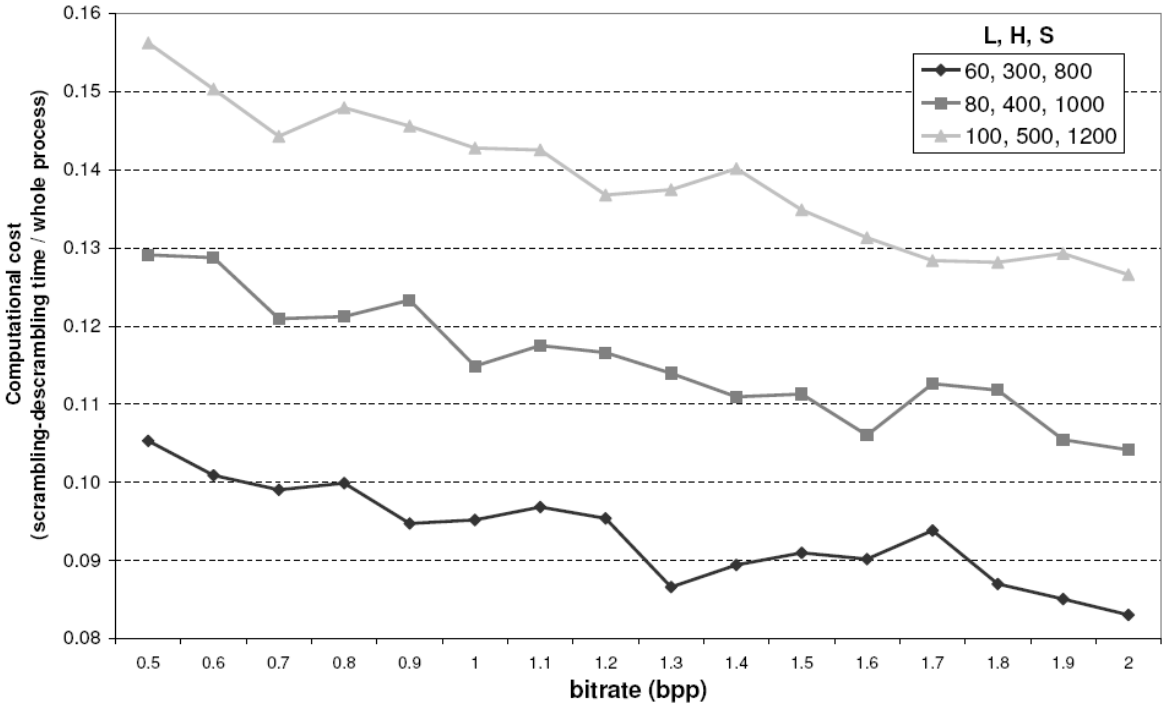


Fig. 5.7. Computational cost evaluation.

5.4.3 Authentication architecture

The proposed method consists in a challenge-response scheme, which achieves multiple levels of security for both server and user authentication. On the one hand, image scrambling as described in Section 5.4.2, provides mutual authentication based on a shared secret key; the server is recognized as trusted only if it owns the user pass-images, implements the correct system architecture and knows the scrambling key. Besides, only a trusted user, which has acquired the access and scrambling keys during registration, may login and decrypt the transmitted images to select its visual password. On the other hand, the IBA architecture guarantees a stronger user authentication, essential in order to avoid counterfeit clients access to the system for stealing private information.

The IBA password consists in the recognition of the pass-images and pass-details. Device/complexity scalability is achieved through parameterization of this procedure. The application window is divided into k grids, each made of h cells (Fig. 5.8). During the pass image/s selection procedure the user has to correctly identify the k pass-image/s among N images, randomly extracted from the JPEG2000 database. Similarly, during the detail selection one secret detail must be recognized for each pass-image through the iterative zooming process.

By defining with d_{img} and d_{dsp} the sizes of original image and display, the number of iterations for the pass-image selection P_1 and for the detail selection P_2 result:

$$P_1 \le N/h, \quad P_2 \le \left\lfloor \log_h \left(k \cdot \frac{d_{img}}{d_{dsp}} \right) - 1 \right\rfloor \tag{5.1}$$

So that the maximum number of iterations is:

$$P_{\max} = \max\left[P_1 + P_2\right] \tag{5.2}$$

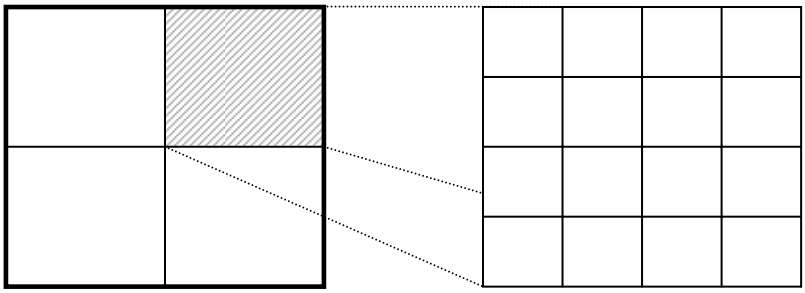


Fig. 5.8. Example of partitioning of the application window.

By choosing a combination of $\{k, h, N\}$, the proposed framework may be easily adapted to any user device. Three application profiles have been defined (Table 5.I).

Table 5.I. Application profiles

Profile	**Device**	**Connection**	**Security**	**(k, h, N)**
Low	Mobile	GPRS	Limited	(1, 9, 9)
Medium	PDA	Wireless	High	(4,16,16)
High	PC	LAN	Very High	(4,25,75)

5.4.4 User Authentication

During the authentication phase, the server manages the preliminary user and user's device identification by detecting and decrypting the access key. If this is a valid key, the challenge-response scheme based on the scrambling key may start. For each authentication session, the server must send a number of scrambled image sequences between $1+P_2$ and $N/h+P_2$. Only if the user owns the scrambling key, the received images can be correctly decrypted and displayed. The visual password codes are transmitted step by step, minimizing the risk of sniffing. Whenever the server detects an authentication failure, the authentication process is not interrupted until the last step. Only then, the user is rejected and a notification policy is adopted. During authentication, the user must recognize the combination of k pass-images with their pass-details. During each authentication session, the server shows k grids, each containing h images randomly positioned in order to minimize the risk of back-shoulder attack. Such randomization does not undermine the method's usability, since the pass-image recognition process is not based on image location. After the first stage of verification, the k grids are used to divide the selected images each into h regions. For each image, the user must iteratively select the portion containing its pass-detail.

The values of k, h depend on the desired degree of security. As described in Section 5.4.3, a good trade-off between security and usability for the medium profile is to use $k=4, h=16$. An example of authentication is provided in Fig. 5.9 for the medium profile. The time sequence of four authentication steps is shown from 1 (upper-left) to 4 (lower-right). While step 1 consists in the choice of four pass images (one duplicated) out of 16, the other steps are the recursive pass-detail selections. Arrows indicate the user's choice.

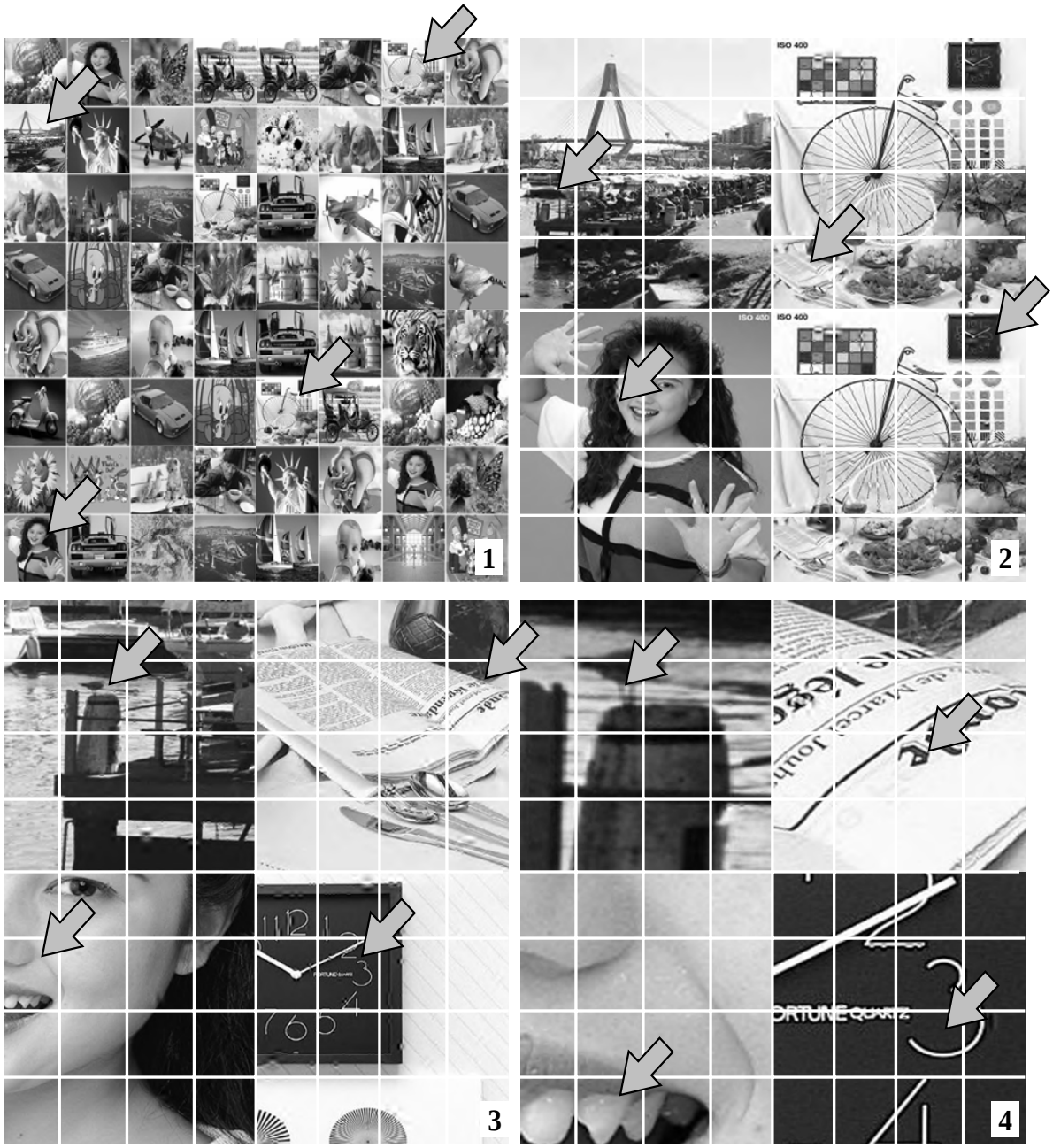


Fig. 5.9. Example of authentication process for the medium profile.

Since the proposed framework is devised to work in wired and wireless environments, it is essential to consider the severe constraints on user friendliness and data transmission capability imposed by mobile devices and GPRS technology. The medium profile was conceived for use with PDAs and wireless connection. Nowadays, such devices offer generous displays and good interactivity, so that decreasing the value of $[h, N]$ to $[16,16]$ is sufficient to achieve a good trade-

off between usability and security performance. On the other hand, mobile devices with limited connectivity and interactivity require the extreme downscaling of the proposed method. For such reason, the low profile has been set to $k=1, h=9, N=9$. In mobile environment, personal device/card codes as the International Mobile Equipment Identity (IMEI) and the Subscriber Identity Module (SIM) may be used to allow for the unique identification of the user every time he logs on the network.

5.4.5 JPEG2000 parameters

JPEG2000 and JPIP are used in order to transmit only those portions of the scalable image datastream that are required at the client's side at each step. In the proposed method, tile databins are the basic elements of JPEG2000 images used by JPIP. JPEG2000 images are partitioned into 40×40 pels tiles, coded with 5 decomposition levels and 6 quality layers (0.15, 0.3, 0.5, 0.75, 1.0, 1.5bpp). Scalability is obtained through the combination of three parameters: tiles, reduce factor (resolution scalability) and quality layers. The number of tiles to be transmitted at each step is proportional to:

$$N_{tiles} = d_{img} \Big/ \left(h^{P-P_1} \cdot d_{tiles} \right) \tag{5.3}$$

By defining the resizing factor between physical and displayed image portion as:

$$Z = \frac{k}{h^{P-P_1-1}} \cdot d_{img} \Big/ d_{dsp} \tag{5.4}$$

the reduce factor may be made proportional to:

$$reduce = \left\lfloor \sqrt{Z} \right\rfloor, \tag{5.5}$$

while the quality layer is assigned the value:

$$Q = -5 \cdot \left\lfloor \sqrt{Z} \right\rfloor \Big/ \left\lfloor \sqrt{Z} \right\rfloor_{\max} + 6 \tag{5.6}$$

where $\left\lfloor \sqrt{Z} \right\rfloor_{\max}$ represents the maximum resizing factor with the given $d_{img}, d_{dsp}, P_{\max}$ values.

5.4.6 Notification Policies

The proposed MIBA method is supported by event-management and notification policies to increase the protection level against unauthorized intrusions. These policies allow legitimate users to control and check all events related to the authentication process, in order to avoid malicious users from registering under an assumed name or accessing through password guessing.

As soon as the registration phase is done, the server sends to user a confirmation e-mail. The e-mail contains personal data which can be checked to ascertain registration accuracy. Neither authentication keys nor registered images and password are enclosed; in fact, the former should have been already sent through SSL secure connection, while the latter are never transmitted. The e-mail also indicates a URL corresponding to a web page always updated with all the authentication events log. The user may check this page in order to detect immediately any attempt of unauthorized access. Notification is also adopted in case a wrong password is entered. During authentication, errors in password inputting may occur because a legitimate user does not remind its password correctly or a malicious user tries to guess it. In both cases, the server allows up to three attempts. After that, the system is temporarily inhibited and a notification e-mail is sent to the legitimate user, who may modify its password or simply reactivate the system in case of mistake. Such policies constitute a further protection against password-guessing attacks. It must be noted that the notification policies may be set differently, depending on the security level required by each application.

Another notification mechanism is the possibility of physically blocking the mobile device when lost or stolen. By gaining possession of a personal device where both the access and scrambling keys are stored, a malicious individual would be able to try an educated guess attack. To prevent such risk, the stolen or lost device can be physically blocked, e.g. mobile phones are identified through the IMEI that is also used to freeze the device permanently. Further, in case of device theft or loss, the legitimate user may inhibit or reset his authentication profile.

5.5 Results

The proposed method has been evaluated in the medium profile (PDA environment), estimating performance in terms of security, as possible input combinations, data transfer and usability, as the amount of information required for visual password memorization. Section 5.5.1 summarizes all authentication scenarios and analyzes possible attacks. Section 5.5.2 provides a consistent performance comparison between the proposed method and the other visual password techniques. For this purpose, image scrambling is not considered and the analysis is performed in terms of input combinations, data transfer and user friendliness. Finally, Section 5.5.3 presents overall results by considering the complete framework.

5.5.1 Risk assessment

In order to analyze all possible use-cases and relative risks, let first introduce some basic notation. Let call M the generic malicious entity and use the pedices c, s and t to indicate client, server or third party respectively. An apex with incremental numbering is used to indicate

one particular attack occurrence, so that M_c^3, for instance, specifies the third case of attack carried out by a malicious client. Similarly we call K the generic key information and use pedices a, s and v to indicate the access, scrambling and visual key respectively. Since the visual key is provided through several steps a further numbering is used, *e.g.* K_{v2} indicates the second part of the visual key. The analysis of possible scenarios is split into two main categories: (*i*) either the malicious entity is a third party who tries to acquire sensible credentials during normal client-server interaction (interception) or (*ii*) attacks are performed by a malicious entity pretending to be the client/server (impersonation or brute force attack).

In the case of third party attack, the malicious entity generally tries to acquire some piece of personal information by managing to break into the client-server transaction. Fig. 5.10 schematizes the authentication and registration processes and pinpoints all possible attacks. In Table 5.II, third party attacks are summarized and analyzed in order to evaluate their likelihood and impact on system security. A Very Low to High empirical scale is adopted.

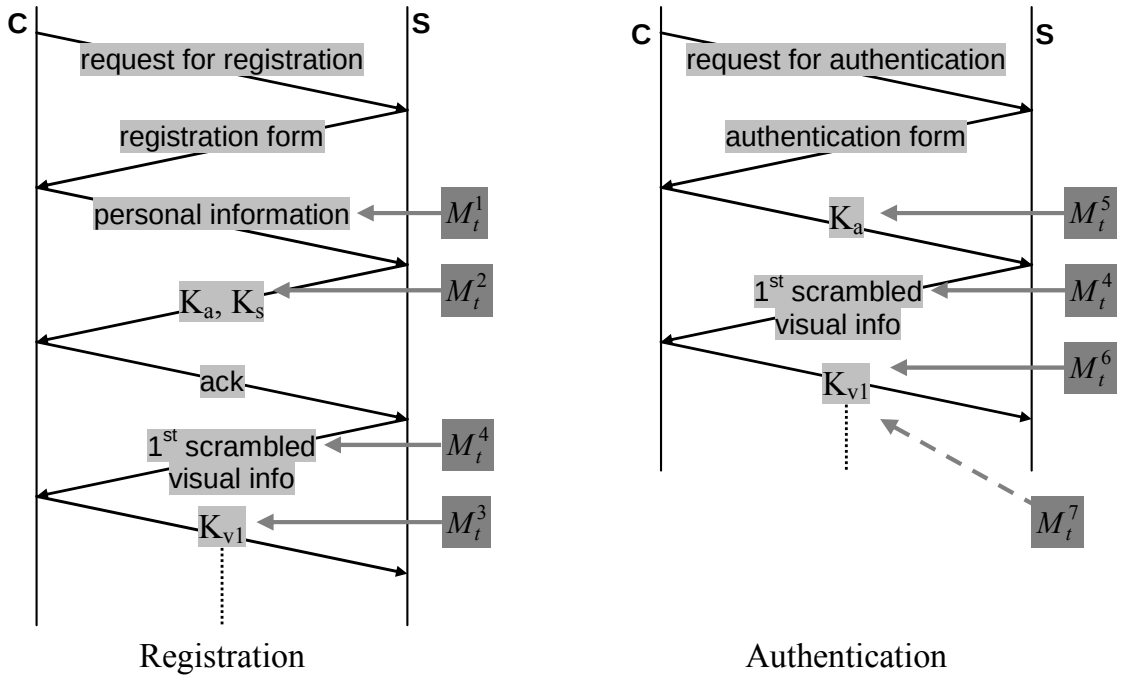


Fig. 5.10. Message exchange and third party attacks.

Table II. Classification and characteristics of third party attacks.

Event	Phase	What is stolen?	Attack	Likelihood	Impact	
					value	notes
M_t^0		user device (K_a and K_s)	device theft	Medium	Low	in case of theft, the device/account can be blocked
M_t^1	registration	personal user information	eavesdropping man in the middle	Very Low	Low	K_a is derived from personal information and other data
M_t^2		K_a and/or K_s			Medium / High	preliminary identification and scrambling/descrambling would be possible
M_t^3		one or more K_{vi}			Low	the value of the visual key is generated dynamically and changes continuously
M_t^4	registration / authentication	one or more pieces of scrambled visual information	eavesdropping man in the middle	Low	Medium	the visual information is useless without the scrambling key
M_t^5	authentication	K_a			Low	preliminary identification would be possible
M_t^6		one or more K_{vi}			Low	see M_t^3
M_t^7		the look of one or more K_{vi}	back-shoulder social engineering	Medium	Low	all other keys should be known

Attacks performed by malicious clients or through shadow servers generally fall in the category of impersonation attacks (Table 5.III). The malicious client will try to perform authentication through brute force or educated guess attacks. On the other hand, clients may unknowingly connect to a shadow server and divulge sensitive credentials such as authentication credentials. Both cases require the knowledge of some piece of user information. Evidently, attack likelihood is inversely proportional to the system knowledge.

Table 5.III. Classification and characteristics of malicious clients or shadow servers attacks.

Event	**What information is known**	**How was acquired**	**Possible attack**	**Impact**	
				value	**notes**
M_c^1	nothing	-	brute force	Very Low	
M_c^2	K_a	M_t^2 or M_t^4		Low	
M_c^3	K_a and K_s	M_t^0 or M_t^2	brute force / educated guess	Medium / High	
M_c^4	K_a, K_s and the look of one or more K_{vi}	M_c^3 and M_t^7	educated guess	High	
M_s^1	system architecture	system knowledge	masquerade	Low	Very improbable; the shadow server should have knowledge of the image database and of each user's profile
M_s^2	system architecture and K_s	M_s^1 and M_t^0 or M_t^2		Low / Medium	

It can be noted that whenever the attack presents a high impact, its likelihood is low. Security is further discussed in the following sections, while notification policies discussed in Section 5.5.6 constitute additional countermeasures against several attack scenarios.

5.5.2 Framework evaluation

For the medium profile, the performance of the proposed IBA method (MIBA) has been compared with three state of the art graphical password systems compatible with mobile platforms: Viskey, Picture Password and Awase-E. Security is reported against data transfer in Fig. 5.11. For the proposed method, security is given by:

$$S_{MIBA} = \begin{cases} N \cdot (N-1)^{k-1} & 1 \le P \le P_1 \\ N \cdot (N-1)^{k-1} \cdot h^{k(P-P_1)} & P > P_1 \end{cases} \quad (5.7)$$

with a limitation on the maximum number of zooming stages P depending on the original image and display sizes, described in (5.2). In the figure, $M+P$ indicates the length of the password, where M corresponds to N/h in the proposed method, *i.e.* the number of image sequences shown by the server for the pass-image selection. For the other methods, $M+P$ corresponds to the number of images or spots to be recalled and selected by the user. The first authentication step consists in the transmission of composite images and requires 35KB on average. At each successive step, the size of the JPEG2000 stream decreases progressively thanks to the possibility of refining image information. As a result, an average saturation of the transmitted stream is recorded. On the other hand, Awase-E requires one image of 35KB on average to be transmitted at each step. Picture Password only requires the transmission of one composite image of about 35KB, whereas Viskey only requires one single image of about 25KB. These last two methods are then the optimal choice for data transmission. However, theirs solution is unacceptable because of reduced usability. In fact, the data transfer gain is compromised by the need for choosing an exact combination of images or a precise spots sequence in a specific temporal order. Furthermore, if we consider the security increment given by the scrambling process, the proposed method provides a better protection, allowing for an adequate security despite lower $M+P$ value.

Finally, in order to evaluate the usability, the amount of information that the user is required to recall has been considered. Fig. 5.12 shows the 3D distribution of the considered features: security, data transfer and usability, in terms of mnemonic load. Mnemonic load is measured as the number of pass-images or pass-details to be recalled for completing authentication. A multiplicative weight of 2 is considered each time the visual method requires a precise ordering of the pass-image/detail sequence. The triangle and circle marks represent the best and worst situations respectively.

The proposed method results simpler than all other visual login systems; it only requires the memorization of four pass-images and four secret details, independently of data transfer and security level. Awase-E, instead, asks the user to remember one image for each verification stage, at the expense of data transfer. For the same mnemonic load, Awase-E requires eight verification stages ($M+P=8$), corresponding to the transmission of eight image sequences. Viskey and Picture Password require to recall a variable number of spots or images, depending on the password length. Moreover, a precise selection order must be followed, considerably compromising the system usability.

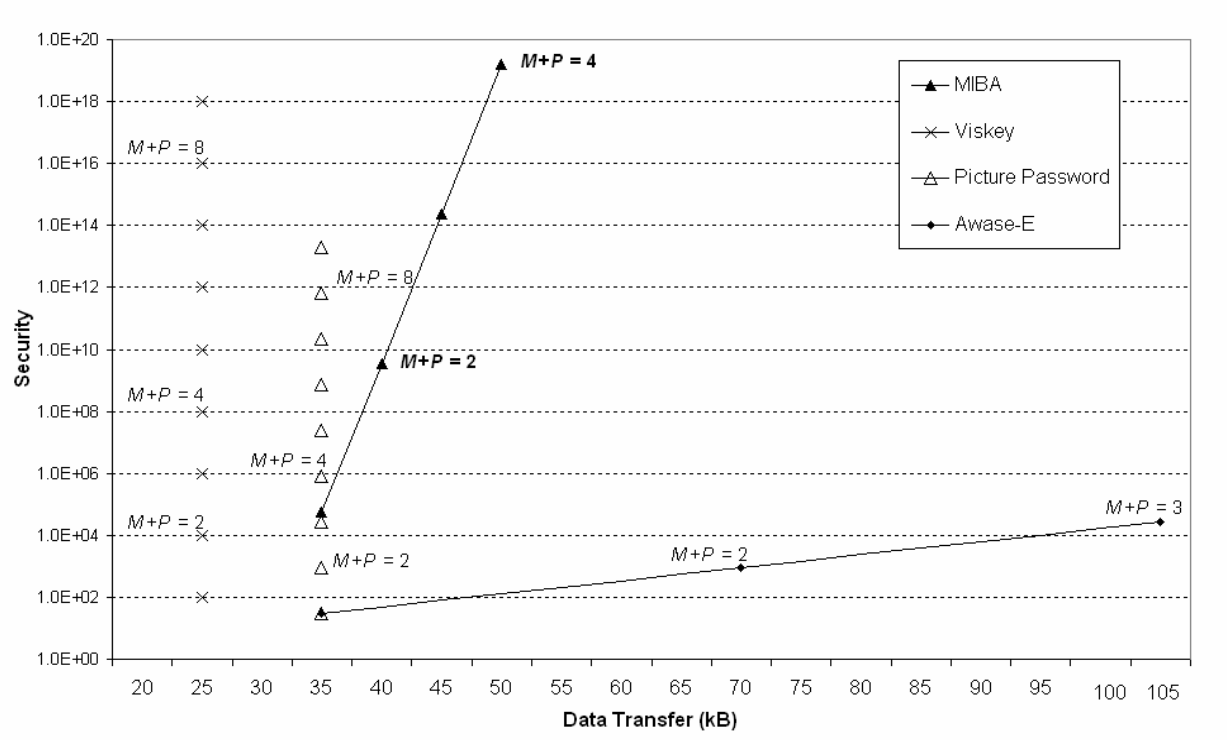


Fig. 5.11. Security against data transfer performance for the medium profile.

5.5.3 Overall results

The security level of the proposed MIBA method is evaluated and compared to a generic system based on a *K*-bits key. Several MIBA set-ups are reported in Table 5.IV, achieving the same level of security as the corresponding key length value. Both cases with and without scrambling are considered and represented by the triplet $\{N,P,L\}$, combinations of image alphabet size, number of steps to select the visual password and length of the scrambling key respectively. While the visual password alone cannot offer a security level greater than a 128 bits key, the scrambling method allows for a security level comparable to that of any key. Results with scrambling represent the overall security of the MIBA system, excluding the access key input.

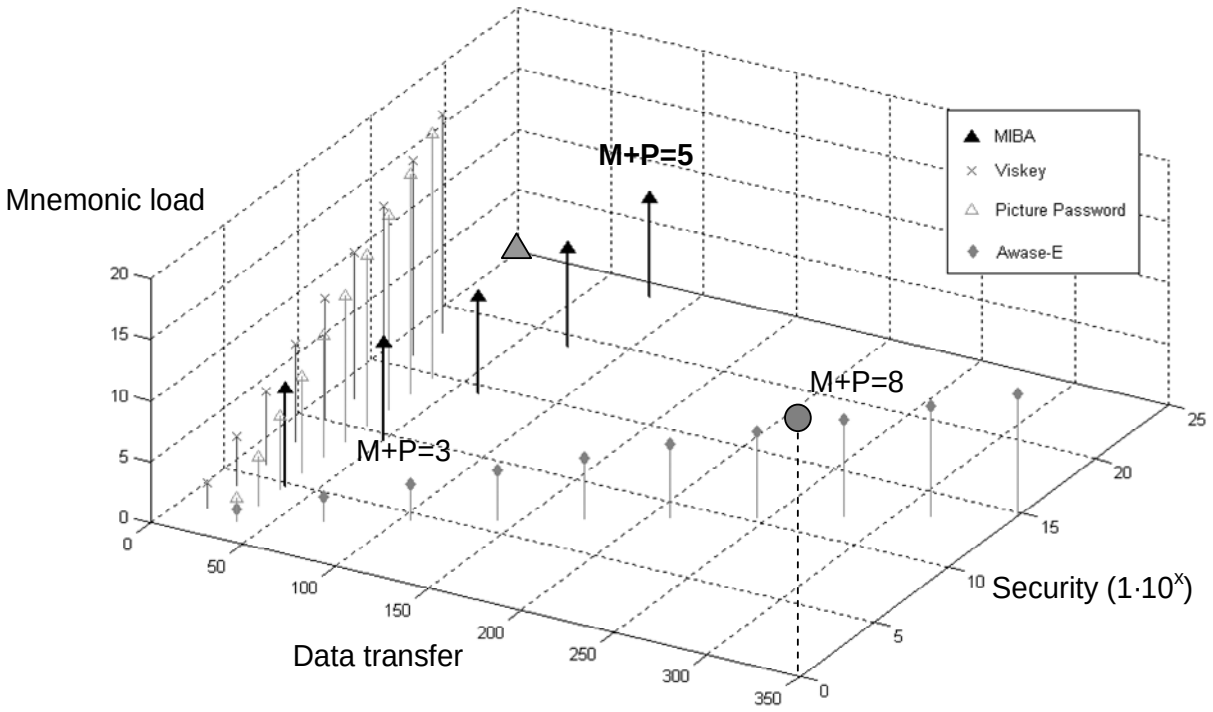


Fig. 5.12. 3D distribution of security, data transfer and mnemonic load for several IBA methods.

Table 5.IV Overall results.

Key length (bits)	**Security**	**MIBA**	
		visual password	**visual password and scrambling**
16	65536	(16, 1, 0), (32, 2, 0)	
32	4.295E+09	(16, 2, 0), (32, 3, 0)	(16, 1, 16), (32, 2, 12)
64	1.845E+19	(16, 4, 0), (32, 5, 0)	(16, 2, 32), (16, 3, 16), (32, 4, 12)
128	3.403E+38	(16, 8, 0)	(16, 2, 96), (16, 3, 80), (16, 4, 64), (32, 4, 76)
256	1.158E+77		(16, 2, 225), (16, 3, 209), (16, 4, 193), (32, 4, 204), (32, 5, 188)
512	1.34E+154		(16, 3, 464), (16, 4, 448), (16, 5, 432), (32, 4, 460), (32, 5, 444)

Conclusions

In this thesis, a research work on Quality of Service technologies for multimedia applications in next generation networks has been presented.

At the first, multimedia applications and their QoS requirement was described. Then, network architectures for quality management was presented, with main attention to the DiffServ-aware Traffic Engineering (DS-TE) which is one of the most advanced technology to achieve quality of service in a scalable, flexible and dynamic way. It performs traffic engineering in a differentiated service environment by applying routing constrains with class granularity.

In the context of DS-TE technologies, the bandwidth management setup problem has been addressed, implementing a methodology for CT classification and bandwidth constraints setting. Both these tasks have to be performed jointly since they both impact on the LSP preemption rate, LSP block probability and end-to-end performance. This has been highlighted by the experiments that have shown how the correct setting of these parameters allows for avoiding network performances not compliant with the input service requirements. In the future research activity, the aim will be reducing the computational complexity of the algorithm, which is currently based on a full-search approach. We also plan to study the application of the propose algorithm when using complex network configurations with hierarchical architectures and routers with dissimilar performance.

Subsequently, a rate control scheme for video streaming applications over wireless channels was presented. It works adjusting the rate on a per-window basis to compensate low-throughput periods with high-throughput periods so as to avoid the “saw” effect that is typically observed in frame-based rate control. The experiments that we conducted on the proposed rate control scheme proved the efficacy of the proposed approach when controlling the buffer underflow frequency. A slight mismatch between the desired starvation probability and the observed rate of starvation events is mainly due to the assumption of independence between consecutive frame transmissions. The experimental results showed that the prediction of network delays for future packets is quite influenced by the setting of the parameters that control the frequency of the updates and the weights of the observations over time. The availability of the predicted and actual data at the control module allows for a real-time adaptation of the parameter settings so as to make use of the optimal parameters during the streaming. This adaptive setting can be driven by the chi-squared test as presented in the experiments section. To better evaluate the efficacy of the proposed techniques we have started the implementation of this algorithm in a real network with WiFi and Hiperlan2 networks.

Finally, a mutual image based authentication framework was described in the last chapter. We demonstrated as it offers strong protection against malicious clients, who might penetrate the system only by taking over both visual password and scrambling key. The risk of impersonation attack by a shadow server is equally unlikely, since the images needed for authentication are transmitted after scrambling. Then, only if the pass-images, visual password and scrambling key are successfully stolen on the server side, a malicious entity may impersonate the trusted server. The proposed system may be implemented in any environment by upgrading the user's device with simple software: complexity is minimized in order to be compatible with the limited computational capabilities of some user terminals, as mobile phones. System usability has been taken into account by considering both difficulty of memorization and restrictions of user interfaces, especially in wireless environment. The proposed approach offers a modular architecture and exploits the properties of JPEG2000 and JPIP to achieve datastream and application scalability. Results indicate the validity of the devised method, which realizes the better trade-off between security, data transfer and usability in several application environments.

Acknowledgements

In this thesis, the work that I conducted during my PhD activity in the CNIT Multimedia Communications Laboratory at the University of Cagliari was presented.

This research activity has been carried on within the IKNOS project funded by the Italian Ministry of Education and Research and developed by the University of Cagliari, CNIT and Tiscali. Further, the work on video streaming makes use of results produced by the Cybersar Project managed by the Consorzio COSMOLAB, a project co-funded by the Italian Ministry of University and Research (MUR) within the Programma Operativo Nazionale 2000-2006 "Ricerca Scientifica, Sviluppo Tecnologico, Alta Formazione" per le Regioni Italiane dell'Obiettivo 1 (Campania, Calabria, Puglia, Basilicata, Sicilia, Sardegna) – Asse II, Misura II.2 "Società dell'Informazione", Azione a " Sistemi di calcolo e simulazione ad alte prestazioni". More information is available at http://www.cybersar.it .

Publications

The following publications are related to the work described in this thesis.

Publications in books

1. T. Onali and L. Atzori, "Chapter: Bandwidth management in Next Generation Networks with DiffServ-aware Traffic Engineering", IEC Annual Review of Communications, vol. 60, 2007 (In press)

Publications in journals

2. M. Carta, T. Onali and L. Atzori, "Video Streaming over Wireless Channels: Rate Control to Restrain Buffer Starvation Occurrences", Hindawi Advances in Multimedia (Submitted)
3. T. Onali and L. Atzori, "Operators Challenges towards Bandwidth Management in DiffServ-aware Traffic Engineering Networks", IEEE Communication Magazine, (In press)
4. G. Ginesu, D.D. Giusto and T. Onali, "Mutual Image-Based Authentication Framework with JPEG2000 in Wireless Environment", EURASIP Journal on Wireless Communications and Networks, 2006

Publications for international conferences

5. T. Onali and L. Atzori, "Traffic Classification and Bandwidth Management in DS-TE Architectures", IEEE – ICC, Beijnd, China, May 19-23, 2008 (Accepted)
6. T. Onali and L. Atzori, "Setting Bandwidth Constraints for Class Types in DS-TE Networks", IEEE - ICC, Glasgow, UK, June 24-28, 2007
7. M. Carta, T. Onali and L. Atzori, "Window-based rate control approach for video streaming over wireless networks", IEEE - ICC, Glasgow, UK, June 24-28, 2007
8. D.D. Giusto and T. Onali, “Data Compression for Digital Photography: Performance comparison between proprietary solutions and standards”, IEEE – ICCE 2007, Las Vegas, NV, Jan 12-14, 2007
9. G. Ginesu, T. Onali and D.D. Giusto, "Efficient Scrambling of Wavelet-based

Compressed Images", MobiMedia 2006, Alghero, Italy, September 2006

10. M. Carta, T. Onali, N. Aste and L. Atzori, "Video transmission over wireless networks: rate control for bursty throughput channels", MobiMedia 2006, Alghero, Italy, September 2006
11. G. Ginesu, D.D. Giusto and T. Onali, "Wavelet Domain Scrambling for Image-based Authentication", Proc. IEEE-ICASSP 2006, Toulouse, France, May 2006
12. G. Ginesu, D.D. Giusto and T. Onali, "Transmission-Efficient Image-based Authentication for mobile device", VLBV 2005, LNCS 3893, pp. 22 – 28, 2006. © Springer-Verlag Berlin Heidelberg 2006
13. G. Ginesu, D.D. Giusto and T. Onali, "Application-Scalable Image-based Authentication Framework with JPEG2000", IEEE Int. Workshop on Multimedia Signal Processing, Shanghai, China, Oct. 30 – Nov. 2, 2005
14. T. Onali, G. Ginesu and D.D. Giusto, "Transmission-Efficient Image-based Authentication for Mobile Devices", 2004 IEEE Medical Imaging Conference (MIC2004), Rome (Italy), 19, October 2004

IKNOS project reports

The following reports of IKNOS project have been produced.

1. OR1 – ATT 1.2 – deliverable D1.2.1: Report con lista servizi da fornire e analisi implementabilità
2. OR 1 – ATT 1.2 – deliverable D1.2.2: Definizione valori ottimali per i requisiti da soddisfare
3. OR 1 – ATT 1.2 – deliverable D1.2.3: Report contenente la Tabella riepilogativa con i valori dei requisiti da soddisfare
4. OR 1 – ATT 1.2 – deliverable D2.2.4: Tabella KPI
5. OR 1 – ATT 1.5 – deliverable D.1.5.1: Report analisi dei requisiti e ambiti operativi per l'ottimizzazione
6. OR 2 – ATT 2.1 – deliverable D2.1.1: Report definizione ed analisi modelli statistici caratterizzante l'architettura di riferimento
7. OR 2 – ATT 2.1 – deliverable D.2.1.2: Report metodologia per la raccolta delle statistiche
8. OR 2 – ATT 2.1 – deliverable D2.1.3: Report metodologia per la raccolta delle statistiche
9. OR 2 – ATT 2.5 – deliverable D2.5.1: Report di definizione regole per il

dimensionamento

10. OR 2 – ATT 2.5 – deliverable D2.5.1: Report di definizione metodologia per lo studio di impatto nuove applicazioni
11. OR 4 – ATT 4.3– deliverable D4.3.1: Strumenti per il controllo remoto dei parametri di QoS nei nodi della rete NGN
12. OR 5 – ATT 5.1 – deliverable D5.1.1: Specifiche test per modelli componenti di rete

    OR 5 – ATT 5.1 – deliverable D5.1.2: Specifiche test di convergenza per rete reale

References

[1] K. Knightson *et al*., "NGN Architecture: Generic Principles, Functional Architecture, and Implementation", vol 30, no.10, October 2005

[2] L. Cottrell, "QoS" on best effort IP networks", ITU-T SG13/SG16, 2001

[3] G. Huston, "Next Steps for the IP QoS Architecture", IETF RFC 2990, Nov. 2000.

[4] ITU-T Recommendation F.700, "Framework Recommendation for multimedia services", 2000.

[5] TU-T G.1010 Telecommunication Standardization Sector of ITU. Series G: Transmission Systems and Media, Digital Systems and Networks, "End-user multimedia QoS categories", 2001

[6] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: An Overview. Informational", RFC 1633, June 1994

[7] T. Kwok, "Residential broadband Internet services and application requirements", IEEE Communications Magazine, June 1997

[8] R. Steinmetz, "Human Perception of Jitter and Media Synchronisation", IEEE J-SAC, Vol. 14, Issue 1, January 1996

[9] B. Shneiderman, "Response Time and Display Rate in Human Performance with Computers", ACM-Computing Surveys, Vol. 16, No. 3, September 1984

[10] ITU-T Rec. I.350, "General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDNs," Mar. 1993

[11] E. Crawley *et al.*, "A Framework for QoS-Based Routing in the Internet," IETF RFC 2386, Aug. 1998.

[12] ETSI, "Network Aspects (NA); General Aspects of Quality of Service (QoS) and Network Performance (NP)," Tech. rep. ETR003, 2nd ed., Oct. 1994

[13] ITU-T Rec. E.800, "Terms and Definitions Related to Quality of Service and Network Performance Including Dependability," Aug. 1993

[14] ITU-T Rec. Y.1241, "Support of IP-based Services Using IP Transfer Capabilities," Mar. 2001

[15] ITU-T Rec. G.1000, "Communications Quality of Service: A Framework and Definitions," Nov. 2001

[16] CISCO IOS QOS, "Quality of Service (QoS) Networking", June 1999

[17] V. Raisanen *et al.*, "Network performance measurement with periodic streams", RFC 3432, 2002

[18] ITU-T Rec. G.1540, “IP Packet transfer and Availability Performance Parameters,” Dec. 2002

[19] ITU-T Rec. G.1541, “Network Performance Objectives for IP-Based Services,” May. 2002

[20] ITU-T Rec. I.380, “Internet Protocol Data Communication Service — IP Packet Transfer and Availability Performance Parameters,” Feb. 1999

[21] J.T. Park, J.W. Baek and J.W.K. Hong, “Management of Service Level Agreements for Multimedia Internet Service Using a Utility Model”, IEEE Communications Magazine, May 2001

[22] NMF, “Performance Reporting Definitions Document,” NMF 701, June 1998

[23] R. Braden, D. Clark, and S. Shenker, “Integrated Services in the Internet Architecture: an Overview,” IETF RFC 1633, June 1994.

[24] R. Braden *et al.*, “Resource ReSerVation Protocol (RSVP)”, IETF RFC 2205, 1997

[25] S. Blake *et al.*, “An Architecture for Differentiated Services,” IETF RFC 2475, Dec. 1998.

[26] E. Rosen *et al.*, “ MultiProtocol Label Switching Architecture”, IETF RFC 3031, 2001

[27] Z. Wang, “Internet Traffic Engineering”, IEEE Communications 37, no.12, December 1999

[28] D.O. Awduche, "MPLS and Traffic Engineering in IP Networks", IEEE Communication Magazine vol. 37, N. 12, Dec. 1999

[29] Le Faucheur, F., Ed., “Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering”, RFC 4124, June 2005.

[30] Le Faucheur, F. and W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering", RFC 3564, July 2003.

[31] B. Davie et al., "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.

[32] Heinanen, J., Baker, F., Weiss, W. and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, June 1999.

[33] P. Newman, T. Lyon, and G. Minshall, “Row Labeled IP: a connectionless Approach to ATM”, Proc. IEEE INFOCOM, San Francisco, vol. 3, pp.1251-1260, Mar. 1996.

[34] H. J. Chao and X. Guo, “Quality of Service Control in High-Speed Networks”, John Wiley & Sons, Inc., Feb 2002

[35] A. Karaman, “Constraint-Based Routing in Traffic Engineering”, IEEE International Symposium on Computer Networks (ISCN'06), page(s): 1- 6, 16-18 June 2006.

[36] Le Faucheur, F. and W. Lai, "Maximum Allocation Bandwidth Constraints Model for Diffserv-aware Traffice Engineering", RFC 4125, June 2005.

[37] Ash, J., "Max Allocation with Reservation Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering & Performance Comparisons", RFC 4126, June 2005.

[38] Le Faucheur, F., Ed., "Russian Dolls Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering", RFC 4127, June 2005.

[39] F. Le Faucheur, “Considerations on bandwidth constraint models for DS-TE,” IETF, Internet Draft, work in progress, June 2002.

[40] P. Trimintzios *et al.*, “A Management and Control Architecture for Providing IP Differentiated services in MPLS-Based Networks”, IEEE Communication Magazine, May 2001

[41] G. R. Malan and F. Jahanian, “An Extensible Probe Architecture for Network Protocol Performance Measurement,” Proc. ACM SIGCOMM ’98, Sept. 1998.

[42] T. Shan and O.W.W. Yang, “Bandwidth Management for Supporting Differentiated-Service-Aware Traffic Engineering,” IEEE Trans. on Parallel and Distributed Systems, vol. 18, no. 9, September 2007.

[43] J.C. de Oliveira, C. Scoglio, I.F. Akyildiz, G. Uhl, “New Preemption Policies for DiffServ-Aware Traffic Engineering to Minimize Rerouting in MPLS Networks,” IEEE/ACM Trans. on Networking, vol. 12, no. 4, August 2004.

[44] I. Minei, “MPLS DiffServ-aware Traffic Engineering”, from Junipers, http://www.juniper.net/solutions/literature/white_papers/200048.pdf.

[45] S. Sundaram, A. Abdurakhmanov and K. Young-Tak, “WBEM-based Inter-AS Traffic Engineering for QoS-guaranteed DiffServ Provisioning”, The 1st International Workshop on Broadband Convergence Networks, page(s):1 – 9, 07 April 2006.

[46] N. Seitz, “ITU-T QoS standards for IP-based networks,” IEEE Communication Magazine, June 2003.

[47] S. Kallel. Analysis of memory and incremental redundancy ARQ schemes over a nonstationary channel. IEEE Trans. on Commun, 40:1474–1480, 1992.

[48] R. Deng. Hybrid ARQ schemes employing coded modulation and sequence combining. IEEE Trans. on Commun., pages 2239–2245, Feb.-Apr. 1994.

[49] Q. Zhang, W. Zhu, and Y.-Q. Zhang, “End-to-end QoS for video delivery over wireless Internet,” Proceedings of the IEEE, 93(1), pp. 123-134, Jan. 2005..

[50] M. van der Schaar and D. Shankar. “Cross-layer wireless multimedia transmission: Challenges, principles, and new paradigms,” IEEE Wireless Communications, pages 50–58, Aug. 2005.

[51] S. Floyd et al., “Equation-Based Congestion Control for Unicast Applications,” Proc. ACM SIGCOMM 2000, pp. 43–56, Aug. 2000.

[52] F. Yang, Q.Zhang, W. Zhu, and Y.-Q. Zhang, “End-to-End TCP-Friendly Streaming Protocol and Bit Allocation for Scalable Video Over Wireless Internet,” IEEE Journal on Selected Areas in Communications, vol. 22, no. 4, May 2004.

[53] M. Chen, and A. Zakhor, “Multiple TFRC Connections Based Rate Control for Wireless Networks,” IEEE Trans. on Multimedia, vol. 8, no. 5, Oct 2006.

[54] Y. Sun, I. Ahmad, D. Li, and Y.-Q. Zhang, “Region-Based Rate Control and Bit Allocation for Wireless Video Transmission,” EEE Trans. on Multimedia, vol. 8, no. 1, Feb 2006.

[55] S. Aramvith, C. Lin, S. Roy, and M. Sun, “Wireless video transport using conditional retransmission and low-delay interleaving,” IEEE Trans. on Circuits and Systems for Video Tech, pages 558–565, June 2002.

[56] J. Cabrera, A. Ortega, and J. Ronda, “Stochastic rate-control of video coders for wireless channels,” IEEE Trans. on Circuits and Systems for Video Tech, 12(6):496–510, June 2002.

[57] N. Srisawaivilai, and S. Aramvith, “Improved frame and basic unit layers bit allocation scheme for H.264 video transmission over ARQ-based wireless channels,” International Conference on Intelligent Information Hiding and Multimedia Signal Processing 2006, IIH-MSP 2006, pages 205 – 210, Dec. 2006.

[58] O. Tickoo, B. Sikdar “On the Impact of IEEE 802.11 MAC on Traffic Characteristics”, IEEE Journal on Selected Areas In Communications, vol. 21, no. 2, February 2003.

[59] C.J. Sreenan, J.-C. Chen, P. Agrawal, and B. Narendran, “Delay Reduction Techniques for Playout Buffering,” IEEE Trans. On Multimedia, pages 88–100, June 2000.

[60] A. Paivio, T.B. Rogers, P.C. Smythe, “Why are Pictures Easier to Recall than Words?”, Psychonomic Science, Vol. 11, pp..137-138, 1968.

[61] R.N. Shepard, “Recognition Memory for Words, Sentences, and Pictures.”, Journal of Verbal Learning and Verbal Behavior, Vol. 6, pp.. 156-163, 1967.

[62] D. Weinshall and S. Kirkpatrick, “Passwords you’ll never forget, but can’t recall”, Proc. Conf. on Computer Human Interfaces, pp. 1399-1402, 2004.

[63] R. Dhamija and A. Perrig, “Déjà Vu: A User Study Using Images for Authentication”, Proc. 9th Usenix Security Symposium, pp. 45-58, Aug. 2000.

[64] Software and Solutions from Cologne, http://www.viskey.com.

[65] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, R. Swanstrom: “Picture Password: A Visual Login Technique for Mobile Devices”, NIST IR 7030, Jul. 2003.

[66] T. Takada and H. Koike, “Awase-E: Image-based Authentication for Mobile Phones Using User's Favorite Images”, Proc. on Mobile Human-Computer Interaction, Springer, pp. 347-351, Sep. 2003.

[67] D.M. Wegner, F. Quillian, C.E. Houston , “Memories Out of Order: Thought Suppression and the Disturbance of Sequence Memory”, Journal of Personality and Social Psychology, Vol. 7l, No. 4, pp. 680-691, 1996.

[68] M. Naor and B. Pinkas, “Visual Authentication and Identification”, in Burt Kaliski, editor, Advances in Cryptology, Crypto ’97, pp. 322-336, Springer-Verlag, Berlin, 1997.

[69] M. Naor and A. Shamir, “Visual cryptography”, in Alfredo De Santis, editor, Advances in Cryptology, EuroCrypt ’94, pp. 1-12, Springer-Verlag, Berlin, 1995.

[70] M. Kharrazi, H.T. Sencar, and N. Memon, “Image Steganography: Concepts and Practice”, Lecture Note Series, Institute for Mathematical Sciences, National University of Singapore, Apr. 2004.

[71] F. Majstor, “WLAN security threats & solutions”, Proc. 28th Annual IEEE Int. Conf. on Local Computer Networks, pp. 650, Oct. 20-24, 2003.

[72] W. Shunman, T. Ran, W. Yue, Z. Ji, “WLAN and it’s security problems”, Proc. 4th Int. Conf. on Parallel and Distributed Computing, Applications and Technologies, pp. 241-244, Aug. 27-29, 2003.

[73] ANSI/IEEE Std 802.11, 1999 Edition (R2003), IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[74] IEEE Std 802.11i-2004, IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[75] IEEE Std 802.1X-2001, IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control, 2001.

[76] JPEG 2000 image coding system – Part 1: Core Coding System, ISO/IEC JTC 1/SC 29/WG 1 15444-1.

[77] T. Ebrahimi, C. Christopoulos, D.T. Lee, Eds, Image Communication Journal, Special Issue on JPEG2000, Vol 17, No 1, Jan. 2002.

[78] T. Ebrahimi and D.D. Giusto, Eds, IEEE Trans. Consumer Electronics, Special Section on JPEG2000 Digital Imaging, , Vol 49, No. 4, pp. 771-888, Nov. 2003.

[79] JPEG 2000 image coding system – Part 9: Interactivity tools, APIs and protocols, ITU-T Recommendation T.808, ISO/IEC 15444-9, Jul, 2004.

[80] C. Perra and D.D. Giusto, “A Framework For Image Based Authentication”, Proc. IEEE-ICASSP 2005, Vol. 2, pp. 521-524, Philadelphia, PA, USA, Mar. 19-23, 2005.

[81] K.S. Joo and T. Bose, “Two-Dimensional Periodically Shift Variant Digital Filters”, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 6, No. 1, pp. 97-107, Feb. 1996.

[82] Y.S. Sun and H.C. Shyu “Image Scrambling through a Fractional GR(qn) Composite Domain”, Electronics Letters, Vol. 37, No. 11, pp. 685-696, May 2001.

[83] Z. Han, W.X. Feng, L.Z. Hui, L.D. Hai, L.Y. Chou, “A New Image Encryption Algorithm Based on Chaos System”, Proc. IEEE Int. Conf. on Robotics, Intelligent Systems and Signal Processing, Changsha, pp. 778-782, China, Oct. 2003.

[84] J. Zou1, R.K. Ward, D. Qi, “The Generalized Fibonacci Transformations and Application to Image Scrambling”, Proc. IEEE-ICASSP 2004, pp. 385-388, Montreal, May 2004.

[85] D. Van De Ville, W. Philips, R. Van de Walle, I. Lemahieu, “Image Scrambling Without Bandwidth Expansion”, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 6, pp. 892-897, Jun. 2004.

[86] S. Lian, J. Sun, Z. Wang, “A Novel Image Encryption Scheme Based-on JPEG Encoding”, Proc. the 8th Int. Conf. on Information Visualisation, London, pp. 217-220 2004.

[87] H. Wu and D. Ma, “Efficient and Secure Encryption Schemes for Jpeg2000”, Proc. IEEE-ICASSP 2004, and Signal Processing, pp. 869-872, Montreal, May 2004.

[88] O.Watanabe, A. Nakazaki, H. Kiya, “A Fast Image-Scramble Method using Public-Key Encryption allowing Backward Compatibility with JPEG2000”, Proc. IEEE-ICIP 2004, pp. 3435-3438, Singapore, Oct. 2004.

[89] JPEG 2000 image coding system – Part 8: JPSEC Final Committee Draft – Version 1.0, ISO/IEC JTC1/SC29/WG1 N 3480, Nov. 2004.

[90] M. Matsumoto and T. Nishimura, "Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator", ACM Trans. on Modeling and Computer Simulation, Vol. 8, No. 1, pp. 3-30, Jan. 1998.