# "Towards a New Generation of IP-based Satellites"

[1]Tiziano Inzerilli, [2]Dario Pompili

"La Sapienza" University of Rome,
Dept. of Computer Science & Systems,
Via Eudossiana 18, 00184 Rome, Italy
[1]inzerill@dis.uniroma1.it, [2]dariopompili@libero.it

**ABSTRACT**

A key factor for success of next generation satellite system is the capability of fully and efficiently supporting IP-based applications. On the one hand, IP will facilitate integration of satellite with the global terrestrial infrastructure, on the other hand, it will pose new challenges related to a number of advanced interworking functions which are currently under study. These not only apply to the satellite field.
Support for enhanced QoS, multicast, mobility, security are some of the aspects which a modern telecommunication infrastructure will provide. It then becomes strategical for research on satellites to address all these issues and solve them in a practical and economical way.
In this paper we describe the BRAHMS architecture which incorporates a number of advanced IP interworking functions and focus on QoS support in particular. We show through simulation how it is possible to support complementary IETF QoS model to transport real-time as well as data traffic efficiently. Work in the BRAHMS project represent the starting point for a new IST project, SATIP6 focused on IPv6 support over satellites.

## I. INTRODUCTION

Driven by the growth of the World Wide Web and the Internet, most of the satellite revenues in the next years are expected to come from the transport and delivery of IP-based applications and services, either to seamlessly complement the available terrestrial broadband services, or to propose, in some niche markets, added-value services as compared to terrestrial ones. The challenge for the Next Generation satellite systems is therefore finding an efficient integration in IP-centric Next Generation Telecommunication Networks.
Currently studied GEO (Geostationary Earth Orbit) satellite system technologies, which aim at providing a transparent integration in Internet networks, rely on ATM (Asynchronous Transfer Mode), ATM-like or DVB (MPEG/DVB) technologies. Research has delivered a number of proprietary solutions, which in the satellite field are hardly open to the public. This number is likely to increase in the next few years and in the long term. In this context IP is seen as the common denominator which will drive future applications into a platform-independent transport scheme. Optimization of IP (Internet Protocol) transport over a generic satellite technology then becomes a goal of primary importance.
This paper proposes a general model for an IP-oriented satellite architecture in which a range of existing and future satellite technologies can be accommodated and exploited at the most by IP-based applications. These questions are related not only to satellite transport but more in general to IP networking on a generic network and are specialized to the Multimedia Satellite System (BMSS) case, which was studied in the BRAHMS project, sponsored by EU in the framework of IST research programme. They comprise general interworking aspects and resource management in the satellite link, IP QoS (Quality of Service) provision, IPv4 and IPv6 mobility support, multicast support, security and more, in general, enhancing IP performances over the satellite link with local measures such as what just mentioned in addition to header compression schemes or TCP (Transfer Control Protocol) spoofing. All these features are offered independently of the satellite technology which is adopted.
One aspect which certainly deserve particular attention is QoS provision, which basically means satisfaction of application transport requirements, e.g. bandwidth guarantees, end-to-end delay and jitter control, packet loss. This paper focuses on the BRAHMS traffic control in particular, which succeeds in harmonizing two well-known IETF QoS model in a single multimedia satellite architecture.

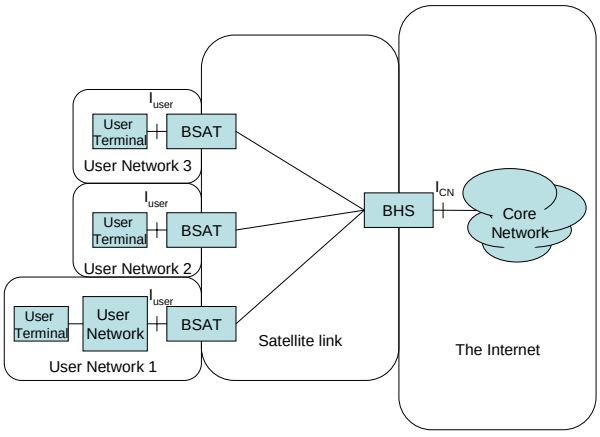
## II. BRAHMS ARCHITECTURE

The BRAHMS architecture, hereinafter BMSS (Broadband Multimedia Satellite system), provides different categories of users with satellite connectivity comprising:

- Individual (home) terminal
- Small business (SOHO) or collective terminals
- Corporate terminals

The satellite link is accessed through two interfaces, $I_{user}$ and $I_{cn}$, on the user and the core network side respectively and consists of the following subsystems:

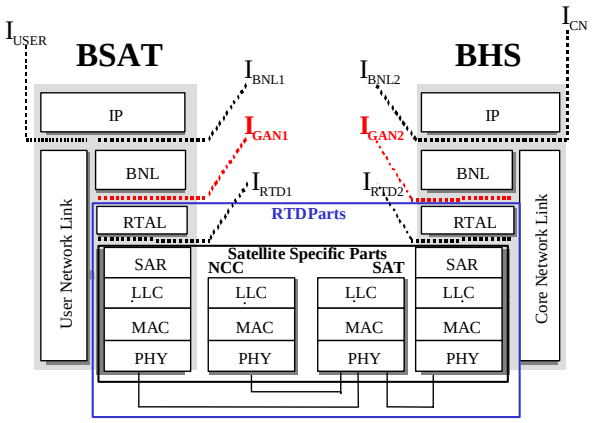
- BSATs (BMSS Satellite Access Terminals) are routers interfacing with CPE (Customer Premise Equipment) including CPNs (Customer Premise Networks) and UTs (User Terminals) through standard terrestrial network configurations, for example PPPoE, PPP/USB, or IP/Ethernet. One BSAT can directly interface with several UTs in a LAN.
- BHSs (BMSS Hub Stations) are routers interfacing with MANs or WANs through various technologies using link-layer and physical layer protocols such as ATM over SDH, or ATM over ADSL, or Ethernet
- The Satellite payload can be transparent, providing layer 1 connectivity (at frequency channel, carrier or time-slot level), or can be regenerative and provide layer 2 packet connectivity; the connectivity can be static or quasi-static in the case of a transparent satellite and more dynamic in the case of layer 2 packet switching as in the picture above.
- The satellite NCC (Network Control Centre) is in charge of the control and management of the satellite access network including BSATs, BHSs, satellite communications functions and communications resources (radio resources and addressing resources). NCC functionalities are often integrated in a BHS.




The BMSS covers several types of connectivity for radio access to an Internet core network via satellite, depending on the roles played by the satellite system: point-to-point (BSAT-BHS or BSAT-BSAT), point-to-multipoint (BHS-BSATs or BSAT-BSATs) or multipoint-to-multipoint.

Note that BHSs and BSATs include an IP layer in order to simplify interworking between customer premise, satellite link and core network/backbone technologies. An alternative solution using BHSs or BSATs as bridges and supporting security functions, QoS and other TCP/IP performance enhancing techniques could be hardly designed. These topics are discussed below.

BHSs and BSATs include a RTI (Radio Technology Independent) part and a RTD (Radio Technology Dependent) part as it is thought to work over a number of different platforms. A specific satellite platform can be integrated in the BMSS through the RTAL (Radio Technology Adaptation Layer) to constitute the RTD parts and offer a common set of services accessible by the upper layers, i.e. IP layer and BNL (RTI parts).




*QoS Provision*

Both the IntServ and the DiffServ approaches are considered in the BMSS and implemented at the level of the IP layer, BNL (BRAHMS Network Layer) and RTAL (Radio Technology Adaptation Layer).

The IntServ [1] approach is well known since 1994. In the Integrated Services model a best effort service is provided as the default case only, while higher quality congestion-free and delay-controlled services can be requested explicitly, i.e. Controlled Load Service and guaranteed Service. The main drawback of IntServ is that it often represents a hardly scalable solution, because it needs to maintain updated information about all data flows in all intermediate routers. In the absence of state aggregation, the amount of state on each node scales in proportion to the number of concurrent reservations, which can be potentially large on high-speed links. However, IntServ approach could be advantageously exploited in a satellite link where the number of hops is limited and which traditionally adopts connection-oriented schemes.

An alternative philosophy, known as the DiffServ [2] approach, was proposed in 1998 as a solution for the scalability issues introduced by the IntServ model. In this approach, QoS provision is guaranteed aggregating different data flows with the same quality requirements, thus achieving scalability where it is difficult to maintain separate information for each stream of traffic because of the large amount of different data flows. A drawback of the DiffServ approach is the lack of granularity in data traffic policing, which may lead to quality degradation of service for all data flows within the same class even if only one data flow generates excess traffic. An easily deployable DiffServ solution is a simplified architecture named Two-Bit Architecture [3], in which service discrimination is performed on the

basis of only two bits in datagrams' IP header, allowing three different kinds of services to be requested by applications. This architecture has the great advantage of being able to satisfy the current and the short-term future QoS demand and, at the same time, to be easily implementable.
The RTAL implements a traffic control strategy capable of satisfying requirements of both IntServ as well as Two-bit DiffServ classes.

*Performance Enhancing Proxies (PEP)*

A Performance Enhancing Proxy (PEP) may be used to improve the performance of the Internet protocols on network path where native performance suffer due to the characteristics of the path (long-delay and low channel reliability in satellites) [4] itself. There exist many types of PEPs to be used in different environments. Transport layer PEPs that interact with TCP is called TCP PEP. These proxies may be classified in two categories depending on their relationship with the end user. *User visible proxies* require some explicit configuration or similar action by the end user in order to be effective. *Transparent proxies* on the other hand work without user intervention and in many cases without the user's knowledge. The implementation of PEPs may be symmetric (identical behavior in both direction) or asymmetric (operate differently in each direction).
In the BMSS we are using only Transparent Proxies, which have only local scope (satellite link). They are than defined as *Link-layer proxies* to improve TCP/IP performances over satellites and can be activated in the BNL.

*IP Header Compression*

The principle of header compression is based on Jacobson's algorithm defined in different RFCs and is applied mainly for differential coding. The documents related to header compression concern the mechanisms and protocols developed in [5], which only concerns TCP/IPv4 compression, the IP Header Compression developed in [8], which describes compression of multiple protocol headers, i.e. TCP or UDP (User Datagram Protocol) over IPv4 or IPv6, the Compression of RTP (Reliable Transfer Protocol) header developed in [7] and the minimal encapsulation within IP developed in [8] mainly for encapsulation of IP over IP for mobility purposes.
It is worth noticing that the header compression is restricted to a number of applications and only useful in some specific cases. Fragmented packets cannot have their header compressed in most of their figures. SYN, FIN or RST TCP encapsulated segments cannot be sent compressed. The advantage of header compression may concern RTP (however complicated) and Mobile IP.
In the BMSS a header compression scheme can be activated in the BNL.

*Mobility Support*

Portable service availability is regarded as very important in future network architectures. Mobile IP (Mobile IPv4 [9] and Mobile IPv6 [10]) are enhancements to standard IP protocols and make it possible for users to roam in foreign links.
There are several issues in Mobile IPv4 that are inefficient such as triangle routing, inefficient direct routing, inefficient binding registration and de-registration, tunneling preventing use of RSVP, inefficient simultaneous binding support, ingress filtering problems, authentication problems and firewall support. However, where IPv4 host as to be provided with mobility support Mobile IPv4 and all its consequent inefficiencies is an obliged choice.
Mobile IPv6 solves many of these problems and adds new good features which are not available in Mobile IPv4. The main differences between Mobile Ipv4 and Mobile Ipv6 are the following: support for route optimization, support for routers using ingress filtering, no need for reverse tunneling, no need for dedicated Foreign Agents, support for IP Security (IPSec), improved movement detection mechanisms, less header overhead, easier retrieval of packets for the mobile node, support of an "any-cast" address identifying Home Agents in a link, advertisement interval, piggy-backing.
The BMSS supports IP mobility implementing Home Agent and Foreign Agent (IPv4-only customer networks) functionalities in BSATs.

*IP Multicasting*

Although the Internet was thought to support also multicast addressing since the beginning, its widespread success is due uniquely to unicast applications, with the only exception represented by the MBONE network. Now that IP has been recognized as the transport platform of next generation telecommunication infrastructures, times seem mature for the full deployment of multicasting technique in data networks. Due to the intrinsic broadcast nature of satellite systems, IP multicasting represents a subject of great interest also for the BRAHMS project. Nevertheless, IP multicasting presents some issues, like multicast routing and group management, which make its employment in a non-fully but only unidirectional broadcast medium (unlike Ethernet, for instance, that is a full broadcast medium) a challenging task.
Measures to support IP multicasting are integrated in the BMSS architecture. In particular, *IGMP (Internet Group Management Protocol) proxying* [11] technique is introduced, which makes it possible not to implement a routing protocol in the satellite link, thus keeping the complexity of the satellite terminals low. A mechanism to reduce signaling load associated to membership refreshing typical of IGMP2 is implemented at the BNL level.

*Security Issues*

Internet diffusion and ubiquitous use of broadband communications foster the introduction of new services for many different businesses and private purposes where security certainly is a mandatory requirement. In general, the following aspects of security can be considered: *confidentiality*, *authentication*, *data Integrity*, *authorization*, *data availability*. Security is an issue that involves all the architectural levels. There a part of security which is independent of the link-layer technology used for transport which can be referred to as RTI (Radio Technology Independent). RTI security issues can be categorized in: *application layer security* and *IP layer security* (IPSec). In the BMSS only security at IP level is specified.
The particular problem posed by the application of IPSec to satellite-based communications is due to the fact that the encryption hides all details of higher layer protocols so that it makes impossible for any intermediate routing and switching node to process the related information. The recent development of Internet security standard (IPSec) in IETF (Internet Engineering Task Force) is incompatible with a new set of networking paradigms that place more and more controls inside the network and not simply in end systems. In particular, any service that requires knowledge of the TCP port number anywhere other than in the end host cannot work if IP packets are encrypted. Such services include most firewalls, many DiffServ implementations (those requiring more information than what is provided in the DS field), MPLS (Multi Protocol Label Switching), RSVP, RED (Random Early Discard), TCP spoofing, header compression, Network Address Translation, TCP traffic shaping, layer 5 switching, transparent web caching, etc. HRL laboratories have developed a modification to the IPSec (Internet Protocol security standard) standard, called ML-IPSec (Multi Layer-IPSec) [12], which uses a multi-layer protection model to replace the single end-to-end model. It enables selective encryption of different parts of the IP packet, so that trusted intermediate communications devices, such as routers and satellite access terminals have access to certain sub-fields of the encrypted packet, such as the TCP header, thus allowing intermediate node processing.
ML-IPsec functions are performed in the BNL so as to allow packet classification and various header processing function to be performed and coexist with header encryption.

## III. TRAFFIC CONTROL IN BRAHMS

The BMSS traffic control architecture is responsible for assuring QoS in the satellite link, which an aspect of particular interest in modern telecommunication. The feasibility of supporting most demanding services, namely multimedia is determined by the presence either of plenty of bandwidth or a powerful traffic control. In the case of satellite, where bandwidth is a particularly precious resource a traffic control scheme is generally needed.
The BMSS traffic control is implemented in the RTAL, which provides a RTI interface with the specific satellite platform. It is thought to support the five class of service specific of the IntServ ([1]) and Two-Bit DiffServ ([3]) models, whose characteristics are summarized in the table below:

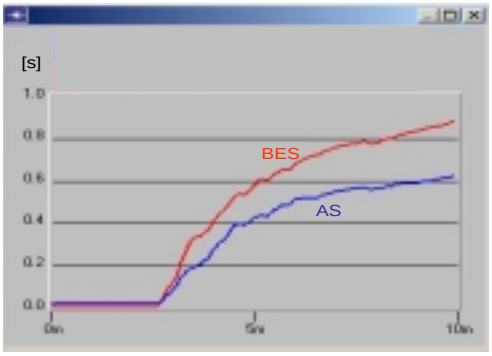
| Name | QoS MODEL | Quality Degree | Description |
|---|---|---|---|
| **PS** Premium Service | 2-bit DiffServ | Highest | null queuing delay, peak-rate-based allocation |
| **GS** Guaranteed Service | IntServ | High | controlled queuing delay, guarantees on bandwidth |
| **CLS** Controlled Load Service | IntServ | Good | congestion-free service, moderate queuing delay and packet loss |
| **AS** Assured Service | 2-bit DiffServ | Sufficient | packet loss lower than in BES |
| **BES** – Best Effort Service | Both IntServ and 2-bit DiffServ | Scarce | No guarantees or precise commitments |

PS and GS are suitable to support anelastic real-time traffic, while CLS and AS can be use to achieve reasonably good performances with elastic traffic.

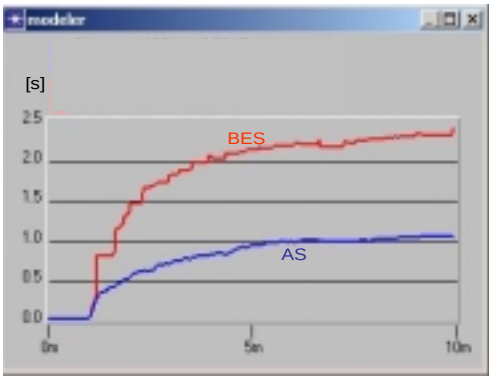
*Traffic Control Simulation*

This section illustrates statistics collected during a simulation of the BMSS traffic control architecture. They show how the five IntServ/DiffServ classes described above can be all supported. Performances of high quality traffic are particularly good and appears independent of the traffic load pertaining to low quality classes (good traffic isolation).
Statistics are collected by means of a Opnet simulator of a BHS transmitting traffic into the satellite link under two different load conditions, i.e. injected traffic 100 % and 110% of the total link capacity assigned to the node. Statistics were collected over a time window of 10 minutes.
The following pictures shows the average queuing delay of packets to be transmitted in the satellite link. Queuing delays of the high quality traffic, i.e. PS, GS and CLS classes appears substantially insensitive to low quality traffic increase and remain limited to acceptable values. PS and GS classes appears suitable for supporting real-time traffic as they experience delays of the order of a few units of ms. In addition, the AS class guarantees significantly better performances with respect to simple BES, which experience.

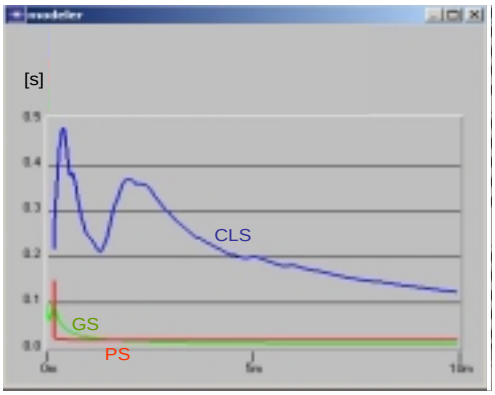
These value were obtained with a packet loss of the order of 1% for high-quality classes while AS class experienced a packet loss of one order of magnitude inferior to BES class.



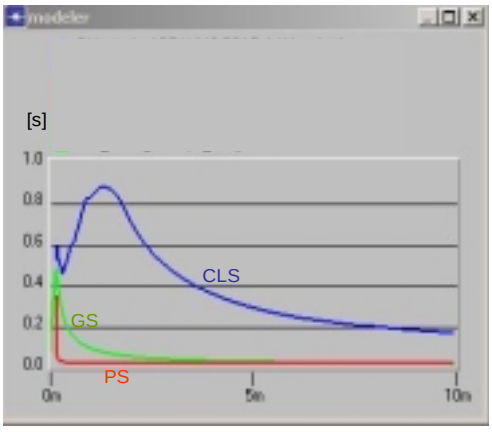
Average Queuing Delay for BES and AS - Traffic Load: 100%



Average Queuing Delay for BES and AS - Traffic Load: 110%



Average Queuing Delay for PS, GS and CLS - Traffic Load: 100%



Average Queuing Delay for PS, GS and CLS - Traffic Load: 110%

## IV. CONCLUSIONS

Satellite systems has represented a separate world in telecommunications for long. Proprietary solutions ranging from simple transparent satellite to more complex cell-based ATM solutions has always been incompatible solutions. Support for IP will radically change their perspectives and facilitate a full integration with a terrestrial infrastructure and introduce new features, such as QoS, support for multicast, security, mobility of terminals.

This paper has presented a satellite system for broadband access to the Internet incorporating a number of advanced IP interworking features, among which QoS provision.

The BMSS support QoS by means of a traffic control architecture capable of conjugating an IntServ and a DiffServ approach at the same time. Performances of the BMSS traffic control architecture where assessed through Opnet simulations. They showed how it is possible to satisfy strict delay control requirements as well as providing a number of different quality degree to support efficiently both elastic and anelastic traffic

## REFERENCES

.


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

[2] K. Nichols, S. Blake, F. Baker, and D. Black, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, RFC 2474, December 1998.

[3] K.Nichols, V.Jacobson, L.Zhang, *A Two bit Differentiated Services Architecture for the Internet*, RFC 2638, July 1999.

[4] J. Border, et al, *Performance Enhancing Proxies*, IETF Internet Draft. Work in progress.

[5] V. Jacobson, *Compressing TCP/IP Headers for Low-Speed Serial Links*, RFC 1144 February 1990.

[8] E. Guttman, L. Leong, G. Malkin, *Users' Security Handbook*, RFC 2504, February 1999.

[7] S. Casner, V. Jacobson, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*, RFC 2508February 1999.

[8] C. Perkins, *Minimal Encapsulation within IP*, RFC 2004, October 1996.

[9] P. Calhoun, C. Perkins, *Mobile IP Network Access Identifier Extension for IPv4*, RFC 2794, March 2000.

[10] C. Perkins et al, *Mobility Support in IPv6, Internet Draft*, draft-ietf-mobileip-ipv6-12.txt, Work in Progress.

[11] R.Fenner, *IGMP-based Multicast Forwarding (``IGMP Proxying'')*, IETF Internet Draft, draft-fenner-igmp-proxy-03.txt, Work in progress.

[12] Yongguang Zhang, *Multi-layer Internet Security for satellite & wireless networks* - HRL Technical Report 99-611.