The SATSIX architecture for next-generation Satellite Systems with IPv6 and DVB

L. Fan[1], C. Baudoin[2], L. Liang[1], A. Yun[3], G. Fairhurst[4], A. Sathiaseelan[4], I. Melhus[5], S. Iyengar[1], J.A. Guerra[6], A. Ramos[7], D. Perez[7], R. Castellot[7], E. Callejo[3], M. Catalán de Domingo[5], H. Cruickshank[1], Z. Sun[1]

[1] University of Surrey, UK,
[2] Alcatel Alenia Space, France
[3] Alcatel Alenia Space Espana, Spain
[4] University of Aberdeen, UK
[5] SINTEF, Norway
[6] Hispasat SA, Spain
[7] Telefonica I+D, Spain

Abstract

Broadband satellite will play an important role to provide universal broadband access for the users. In order to lower the cost, the next-generation satellite systems should support IPv6 and seamlessly integrate with terrestrial networks, including wireless local loops. In this paper, a novel network architecture has been proposed as a potential solution to the above problem. Based on the proposed overall network and functional architecture, we have emphasised and presented different aspects of the advanced IPv6-enable networking techniques, such as QoS, multicast, security and mobility. The transport protocols can be used in this network architecture are also studied.

Introduction

Current broadband satellite services are regarded as a niche market due to the high cost of launching a satellite system, and the relatively limited available bandwidth compared to terrestrial counterparts. To improve take-up of broadband satellite, it is essential to provide cost-effective solutions, to efficiently accommodate new multimedia applications, and to integrate satellites into next generation networks. These issues are being addressed in the EU-funded IST FP6 project Satellite-based communications systems within IPv6 (SATSIX). This project will implement innovative concepts and for broadband satellite systems and services.

This paper describes the design of the SATSIX network architecture, with support for IPv6 and integration of hybrid satellite and wireless local loops (WiFi and WiMAX), to provide low-cost universal broadband access. This architecture uses the Satellite-Independent Service Access Point (SI-SAP) reference model as a starting point.

Particular attention is paid to the IPv6 network-layer, QoS, multicast, mobility, and security. These network functions are mapped to satellite-dependent functions within DVB-RCS systems (e.g. QoS functions offered by radio-resource management and transmission queues, security mechanisms, satellite signalling using the Connection Control Protocol, C2P, and satellite-specific protocol optimisations, such as Performance Enhancing Proxies, PEP).

Overall Satsix Network Architecture

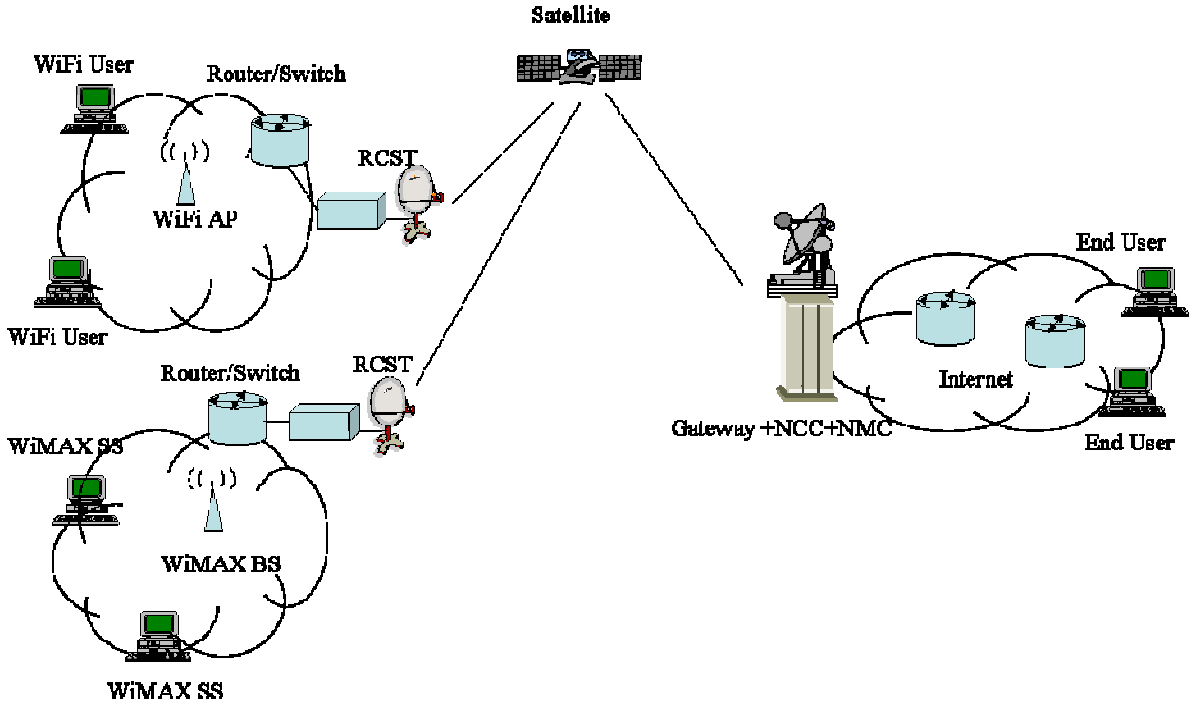

Figure 1 Overall Reference Network Architecture

As shown in the Figure 1, the proposed network reference architecture has the following physical elements:

- RCST: Return channel satellite terminals act as an interface between the system and external users providing bi-directional services through the satellite network. It can operated in is the interface between DVB-RCS and external users/networks, such as WiFi and WiMAX.
- Satellite: It provides the backhauling link between the RCST and the hub or other RCST's. It can be transparent or has OBP capability.
- NCC: Network Control Center controls the Interactive Network, provides session control, routing and resource access to the subscriber regenerative RCST's and manages the OBP configuration and DVB-S/DVB-RCS tables.
- NMC: It controls the management of all the system elements. The AmerHis Network Management Center (NMC) is split in two subsystems:
- Gateway: It provides the interconnection with terrestrial networks (ISDN/POTS, Internet, and Intranet). The Gateway is mainly composed of the following subsystems:
- Access router/Switch: It is the access point with terrestrial networks.
- WiFi Access point: A wireless access point (AP) is a hardware device that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.
- WiFi user: Terminal or end user who accesses the network through WiFi connection.
- WiMAX BS: WiMAX base station connects the terrestrial networks to the WiMAX subscriber station.
- WIMAX SS: WiMAX subscriber station provides service through a wireless connection to the end user.

Two different configurations, namely transparent star and regenerative mesh topologies, of this reference network, are proposed. The main difference is that: For the transparent star topology, the satellite does not have OBP and RCSTs can only communicate with the gateway/NCC via the satellite. WLLs are connected to the DVB-RCS via RCSTs; For the regenerative mesh topology, the satellite has OBP, and a RCST not only can communicate with the gateway/NCC via the satellite, but also can communicate with other RCSTs.
Based on the overall network reference architectures, Two overall reference functional architectures for transparent star and regenerative mesh topologies, respectively, are proposed. These functional architectures have integrated QoS, multicast, security, mobility and transport functions.

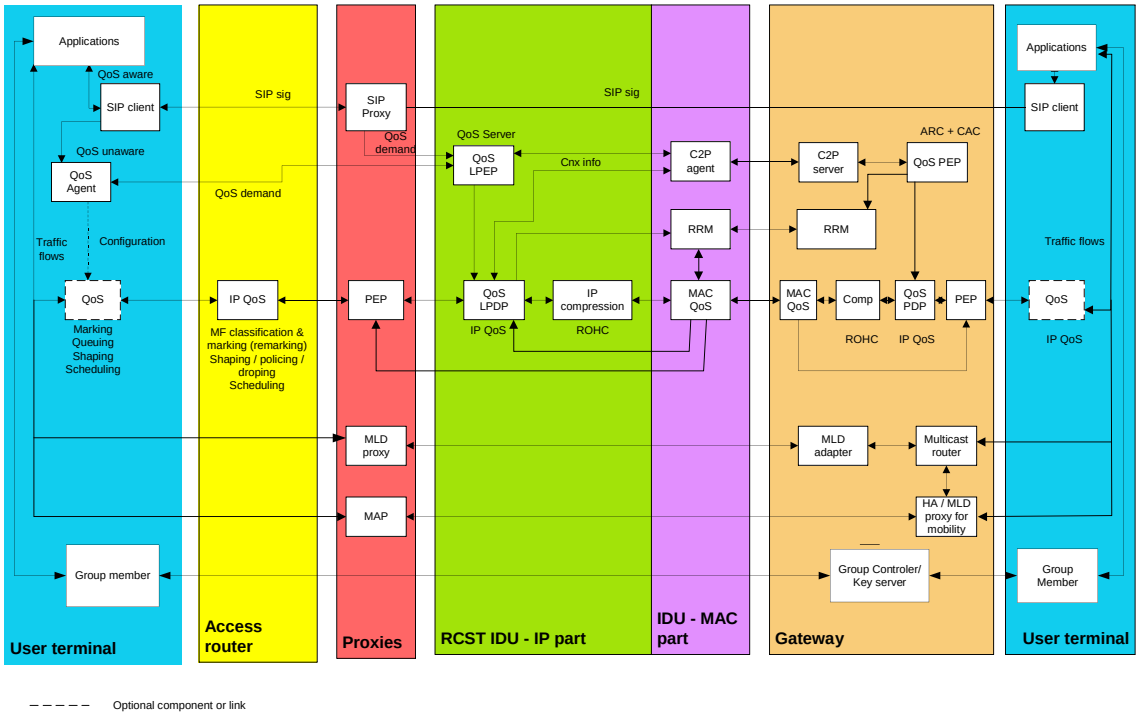

Figure 2 SATSIX overall reference functional architecture for the Transparent Star Topology

The main elements of the functional architectures are:

- This functional architecture not only support end-to-end QoS, but also support dynamic QoS according to applications and users needs. The satellite segment can interwork with Internet QoS DiffServ in order to provide end to end QoS at network level. The terminal model can perform this interworking in terms of signalling and QoS parameters mapping. The involved entities are SIP proxy, QoS agent, QoS server, PEP, IP compression, IP QoS, MAC QoS, RRM, C2P agent and C2P server.
- This functional architecture can provide up-to-date multicast management for both IPv4 and IPv6. The RCSTs should act as an MLDv2 multicast router proxy to forward the MLDv2 messages between listeners and the remote multicast router in the NCC.
- This functional architecture support security at application level such as TLS, SSL, and DTLS, key management protocols such SATIPSec and GSAKMP, key distribution systems like LKH and layer 2 security enhancing security level provided by layer 3 solutions such as SatIPSec. The Group

controller/key Server will be co-located within the NCC and all the key management group members will be co-located within user terminals. All key management messages will flow between the Group controller/Key server/NCC and all the secure data will be between the user terminals in mesh and user terminals and Gateway in a star configuration.

- This functional architecture has enhanced standard IPv6 mobility in a satellite system, with the use of Mobile IPv6. Mobility Anchor Point (MAP) is located in RCSTs and Home Agent (HA) is co-located in gateway. This design can reduce the signalling message during intra-domain movement and handover.
- This functional architecture support PEP enhancement.

QoS architecture

The SATSIX QoS architecture aims to provide dynamic QoS support for both QoS aware and QoS unaware IPv4 and IPv6 applications whatever the type of satellite system is (transparent, regenerative or hybrid).
The main innovation is to add dynamic resource reservation at IP and MAC layers on top of the classical DiffServ architecture and to introduce cross layer techniques to optimize the overall QoS provided by the satellite system.
“QoS assured” and “QoS enable” sessions are handled by the architecture. In the first mode, desired resources are dynamically assigned and reserved after acceptation by the access network, while the second mode allows to establish the session without the needed resources.
This architecture is based on several key components, as shown in Figure 3. On the satellite terminal side, the QoS Server is the major entity in charge of collecting either SIP information provided by a SIP proxy or QoS reservation provided by the QoS agent located in the user terminal. These information are used to dynamically update the IP scheduler behaviour. On the NCC side, the Access Resource Controller (ARC) collects the access connexion parameters to update accordingly the resource allocation for the involved satellite terminals. This modification can impact the CRA or RBDC parameters such as the booked capacity handled by the DAMA.

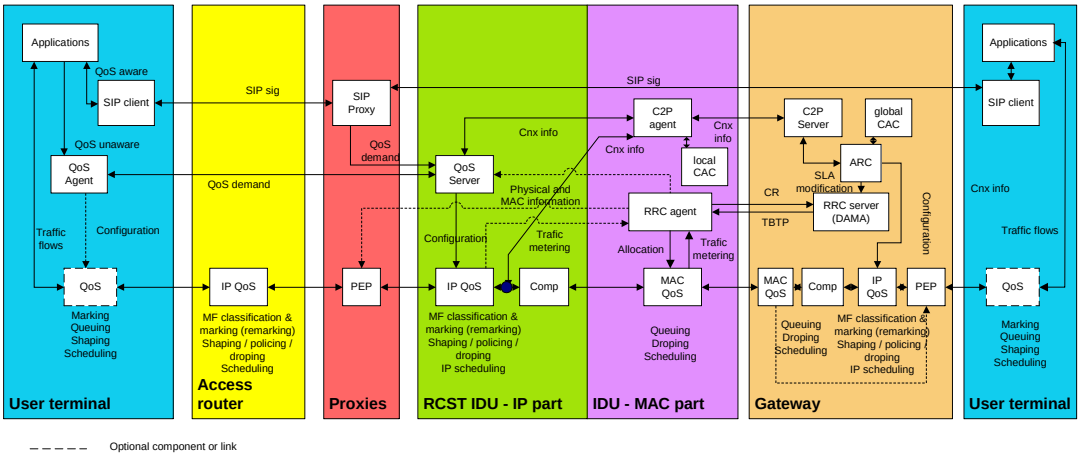

Figure 3 SATSIX QoS architecture for transparent satellite systems

The interface between the NCC and the satellite terminal is based on C2P, that provides a simple way to establish access connection with QoS parameters that can be used by different entities. This allows tohandle both transparent and regenerative satellite systems. In the star topology case, connections between the RCST and the

GW are established during the logon phase and their parameters are dynamically modified using C2P modify messages while connections are dynamically established, modified and released in the mesh case. This solution allows the same QoS architecture independently from the target system, and permits to avoid the impact on the establishment delay in the transparent case and the use of a SIP proxy in the GW.
The second kind of interaction between the MAC layer and the upper layer is related to the coordination of the scheduler at IP and MAC layers to optimize the overall traffic handling. The IP scheduler manages a hierarchy of traffic classes and is based on an enhanced version of HTB introducing Dual Leaky Bucket as internal scheduling technique. The internal class behaviour (filter, thoughput, …) is dynamically updated according to SIP information whereas the output throughput of the IP scheduler is controlled by the MAC scheduler using a control loop approach.

Multicast Architecture

Multicast is a key triple-play service. Efficient dynamic multicast group management in both star and mesh topologies is supported by intercepting the Multicast Listener Discovery (MLD) protocol and interworking with C2P.
Multicast is a key triple-play service. Efficient dynamic multicast group management in both star and mesh topologies is supported by intercepting the Multicast Listener Discovery (MLD) protocol and interworking with Connection Control Protocol (C2P).
The SATSIX project considers two kinds of satellite networks in the multicast architecture design. They are DVB-S (2)/DVB-RCS transparent networks and DVB-S (2)/DVB-RCS regenerative networks. Only the regenerative network design is presented in this paper. For each kind of networks, two scenarios are addressed including both static multicast and dynamic multicast. The static multicast means the satellite networks do not have information about end users but simply broadcast the multicast data to all Return Channel Satellite Terminals (RCST) and the Regenerative Satellite GaTeway (RSGT) that will filter the packets and only accept the wanted ones. The multicast only happens behind the RCSTs and the RSGT. The dynamic multicast means the Network Control Centre (NCC) can be notified about end users join and leave status in order to configure the On Board Processor (OBP) to route the multicast data to the right RCSTs and RSGT.
In the proposed multicast architecture, all multicast management and routing protocols are running outside of the satellite network and the C2P protocol is running inside to establish the one-to-many satellite channels to carry the multicast data. Therefore, to enable the seamless integration of the IP networks and the satellite networks, one has to consider 3 aspects. One is how the multicast work properly in IPv6 networks. Another one is how the C2P can establish the one-to-many satellite channels. The last one is how the multicast can interwork with C2P to enable the multicast delivery. With all these three elements together, the multicast architecture over satellite networks can be addressed. This paper will describe multicast in IPv6 and focus on the interworking between the multicast and satellite signalling protocol C2P. The details of C2P protocol is out of the scope of this paper.
IPv6 multicast requires the following protocols to be implemented.

- PIM-SSM is used between routers so that they know which multicast packets to forward to each other and to their directly connected LANs.
- MLD for IPv6 is used to discover multicast listeners (hosts that wish to receive multicast packets destined for specific multicast addresses) on directly attached links.

There are two scenarios in the satellite network that have different impacts when employing MLDv2. In the first scenario, there are multicast routers locate with multicast address listeners. The typical example is an organization intranet with a satellite terminal which has embedded MLDv2 multicast router functions. The MLD relationship between multicast address listeners, the end users, and the multicast routers are kept locally within the organization. No MLD signalling goes out to the satellite network.

In the second scenario, there are no MLDv2 multicast router located with the satellite terminal. In another words, there are no local MLDv2 router available for those listeners in the organization. To specify the interest, listeners have to listen to the MLDv2 queries sent from an MLDv2 multicast router located within the satellite network. The optimizing place for this multicast router is the location of NCC. This is to take advantage of the central control feature in the satellite network that will benefit both signalling control and billing functions. To avoid the single point failure, the multicast router located in the NCC should have redundancy as backup.

Therefore, the scenario should have a central remote MLDv2 multicast router sending queries to all satellite terminals that do not have local routers. These terminals should forward the received MLDv2 queries to their attached listeners while the latter should respond the terminal with corresponding report. The scenario is shown in Figure 4.

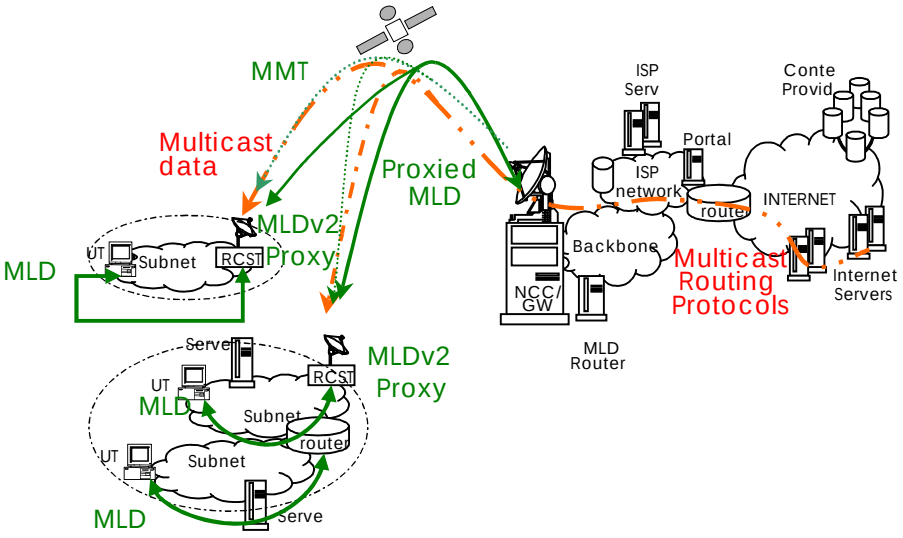

Figure 4 MLDv2 Multicast Router remotely located with satellite terminal

In Figure 4, all RCST terminals act as a MLDv2 proxy. As defined in [RFC4605] a proxy device performing MLD-based forwarding has a single upstream interface and one or more downstream interfaces. These designations are explicitly configured; there is no protocol to determine what type each interface is. It performs the router portion of the MLD protocol on its downstream interfaces, and the listener portion of MLD on its upstream interface. The proxy device MUST NOT perform the router portion of MLD on its upstream interface. Therefore, a RCST terminal should perform the listener's function of receiving queries from the central multicast router in the NCC and it should proxy the queries to its local link. All host in the local link will response the queries to the terminal who then should proxy these reports to the NCC multicast router.

Security Architecture

SatIPSec is the Key Management protocol based on Flat Key Management Exchange protocol to be used in SATSIX [FMKE]. It offers a new way of transparently and efficiently securing unicast and multicast satellite transmissions, on forward and return links, in DVB-RCS mesh and star topologies. SatIPSec is derived from IPSec standard protocols.

SatIPSec for IP Layer**:**

Figure 5 presents the SatIPSec architecture for IP packets. SatIPSec clients and GCKS are implemented in external boxes (independently of the other Satcom equipments). There is one SatIPSec client box behind each Satellite Terminal (ST); however SatIPSec mechanisms could also be implemented directly inside the IP stack of satellite terminals. The GCKS is preferably located at the gateway side in star topology. The location of SatIPSec clients allows to apply security mechanisms to IP traffic (if requested) so as to ensure its protection during its transmission over the satellite network. Before transmission on satellite system, a SatIPSec client can cipher each IP packet and can compute an authentication value. In reception, the SatIPSec client(s) can decipher it and check the authentication value, before transmitting it on the terrestrial network it (they) is (are) connected to. SatIPSec allows to protect any unicast or multicast IP flows transmitted on satellite links, from Hub to ST, from ST to Hub and from ST to ST , in Star and Mesh topologies.

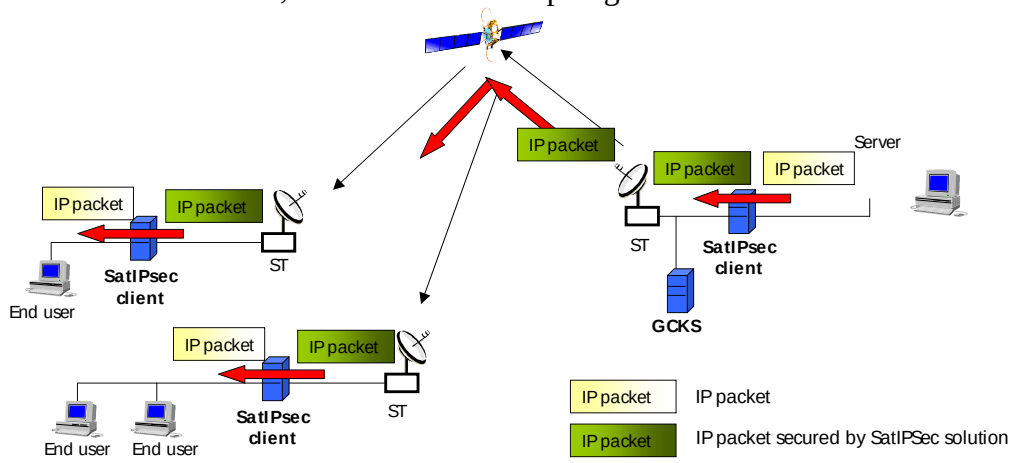

Figure 5 SatIPSec architecture

SATIPSec for Link (ULE) Layer:

In SATSIX, SatIPSec will be adapted to provide link-layer security (with a special focus for link using ULE). At the architectural level, SatIPSec is at the link layer and requires one SatIPSec client module to be integrated in each satellite terminal and gateway. The GCKS, which configures SatIPSec clients, is integrated in the DVB-RCS gateway (GW) or Network Control Centre (NCC) as shown in the Figure 6.
SatIPSec at the link layer will be defined to enable it to provide:

- Data confidentiality at link level, which is the major requirement to mitigate passive threats.
- Data source (ST/Gateway) authentication/ data integrity at link level
- Protection against replay attacks
- Protection of Layer 2 NPA/MAC addresses
- ST/Gateway authentication and authorisation

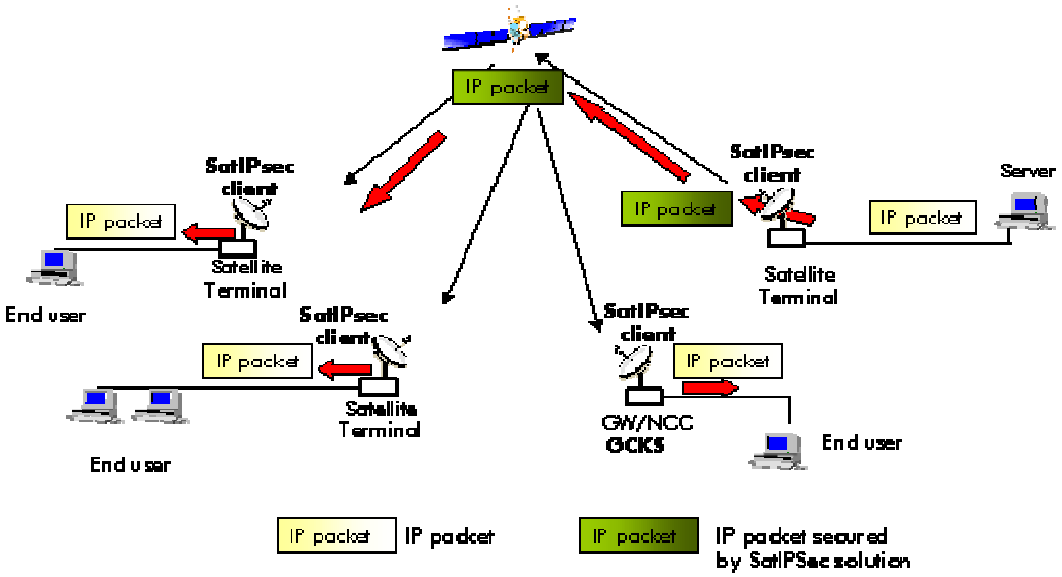

Figure 6 SatIPSec at link layer: architecture (DVB-RCS mesh topology)

The protection of data can be applied either per receiver MAC/NPA address or per IP flow. Concerning involved protocols, key management functions may be decoupled from data protection functions. Thus it is proposed to re-use the IP key management protocol defined for SatIPSec at IP layer (with some adaptations). Besides SatIPSec security session establishment and management will be integrated in DVB-RCS standard process (in order that security session is inherently part of the DVB-RCS session).

Mobility Architecture

In SATSIX, mobility is specified at the network and application layer, and architecture and protocols focuses on terminal mobility, which is the ability of the mobile node or host to change its location. Mobility of the DVB-RCS terminal are not investigated, only mobility of the user (subscriber) terminal connected to the satellite terminal.

Three mobility scenarios are defined:

- *Discrete mobility, i.e. nomadic (roaming) mobility.*
- *Continuous mobility, i.e. suspended service sessions*
- *Seamless mobility, i.e. local (micro) mobility with handover and no interrupting*

Further, two mobility contexts according to network hierarchy are considered:

- *Macro-mobility, which refers to inter-technology and inter-domain mobility*
- *Micro-mobility, which refers to intra-technology and intra-domain mobility*

The Mobile IP protocol is the standard mobility mechanism at the network layer. It makes sure that the moving node or host is reachable anywhere by its original address. In IPv6, the Mobile IPv6 protocol (MIPv6) [RFC3775] is part of the standard and uses features of the IPv6 protocol like Address Autoconfiguration and Neighbour Discovery.

While the network mobility is managed by MIPv6 and its optimisations for TCP connections, the Session Initiated Protocol (SIP) [RFC3261] is used for real-time application mobility over UDP. SIP and application mobility makes a complement to the network layer mobility in a large range of applications like VoIP, instant

messaging and multimedia conferencing. In SATSIX two scenarios are described: *nomadic mobility* and *mid-call mobility*

Multicast is a central feature in SATSIX, so is also the combination of multicast and mobility. Three approaches for multicast mobility are specified: The first is *remote subscription* where the mobile node joins a multicast group via a local multicast router on the foreign link by using its care-of-address instead of its home address. The second approach is *home subscription* where the mobile node joins the local multicast router on its home link through a bidirectional tunnel to its Home Agent. The third approach is a mix of the previous known as *MLD proxying*, where the idea is to make the Home Agent a multicast client for the Mobile Node (as for unicast addressing).

Due to the high bandwidth*delay product, satellite links make use of accelerators or PEPs (Performance Enhancing Proxies). When the mobile node is visiting a foreign network, the combination of network mobility (Mobile IP) and PEPs causes various problems. Different issues and solutions needs to be considered and are thoroughly discussed and analysed. This includes suppression of address changes at PEP level, misrouting and spurious retransmissions, and management of loss of context between PEPs.

Mobility gives a significant impact to the QoS management, and generates a new challenge for QoS provision as it will have to deal with terminals (nodes) changing their point of attachment to the network. For active application sessions on the mobile, the network should negotiate QoS along the new route as part of the handover procedure which could allow the mobile terminals with on-going applications to keep or adapt the QoS in the visited networks. The QoS part of the architecture is based on the QoS server and the QoS agent for non QoS-aware applications, and the enhanced SIP proxy for QoS-aware applications using the SIP protocol.

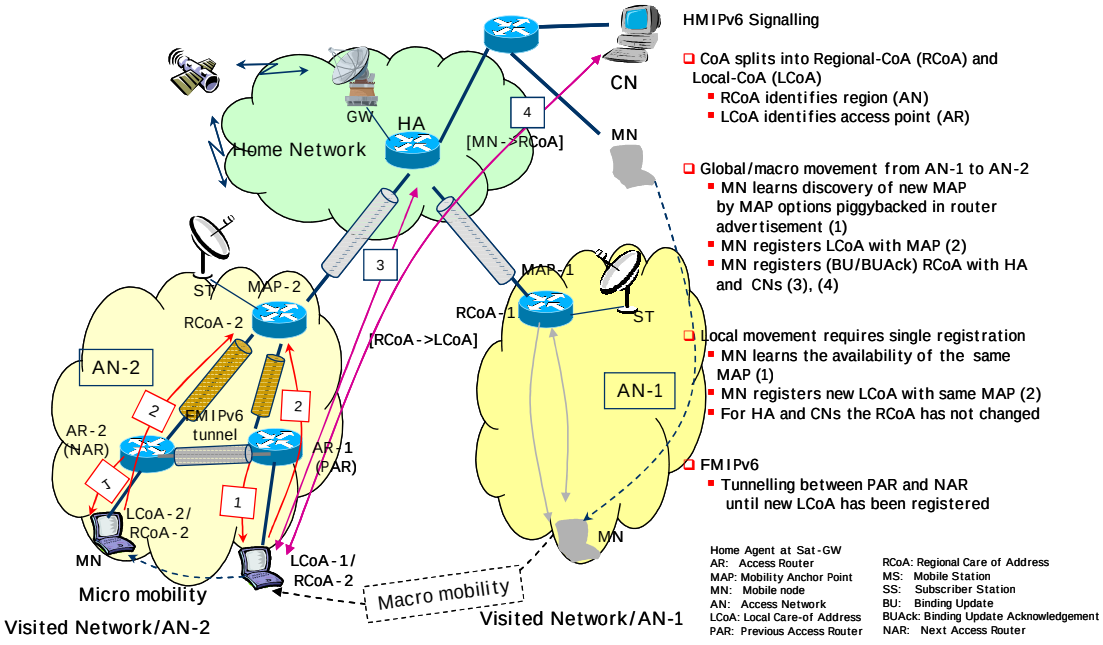

Figure 7 Optimised MIPv6 with HMIPv6 and FMIPv6

In order to reduce handover delay and signalling overhead over the satellite link for local mobility in the LAN (Local Area Network) usually connected to the satellite terminal, SATSIX defines the use of the two MIPv6 enhancement protocols, Hierarchical Mobile IPv6 (HMIPv6 [RFC4140] and Fast Handover Mobile IPv6 (FMIPv6) [RFC4260] or the combination of the two (F-HMIPv6). HMIPv6 aims at

reducing signalling messages during intra-domain and local movement by introducing a new network element called Mobility Anchor Point (MAP). FMIPv6 was designed to minimize handover latency.

Transport Layer

Multimedia is seen as a key service in most next generation networks. Multimedia services over IP may be used on paths that include satellite links (e.g. to deliver VoIP, TVoIP and other services). These services may be delivered over TCP (especially for streaming services to individual users), but are more usually delivered over datagram services. The work on transport protocols will focus on approaches and techniques that enable effective congestion control for multimedia (TVoIP, VoIP, and other multimedia services) when the network path includes a DVB-RCS satellite system. Delivery of such multimedia services over the satellite network, demands that the satellite network should be easily integrated with the fixed and mobile Internet. This requires the networking protocols used to carry the multimedia services cooperate in harmony with the existing protocols that are used for data services.

Multimedia presents a challenging requirement both in terms of the need to offer a quality of service that meets the needs of multimedia applications (in terms of required bandwidth, minimal jitter, maximum delay, etc), while only consuming a fair share of the available capacity that is available over the end-to-end Internet path. Current multimedia applications use UDP as the underlying transport protocol to deliver its packets. UDP-based applications can (and often do) transmit at a constant rate, irrespective of the available capacity. Growth of such long-lived non-congestion-controlled traffic posed a real threat to the overall health of the Internet [FLOYD-DCCP06], and in particular form an obstacle to the deployment of triple-play services over bandwidth-limited technologies such as satellite systems. Concerns about the impact of congestion that could result from multimedia services has leaded to investigation of congestion-responsive transport protocols. A congestion responsive transport protocol is essential for building next generation multimedia applications to ensure continued operation of the Internet with a wide variety of multimedia/data applications.

The SATSIX work will utilise the protocol framework provided by a new transport protocol, standardised by the Internet Engineering task Force (IETF) in 2006, the Datagram Congestion Control Protocol (DCCP). DCCP is designed to deliver multimedia content across the wide-area Internet. An initial goal of the SATSIX project is to investigate and characterise the behaviour of the Congestion Control (CC) components of DCCP over satellite links. Applications that can use DCCP include those that prefer timeliness of data to reliability. These applications benefit from the flow-based semantics of TCP, but do not want TCP's inorder delivery and reliability semantics. Applications include streaming media and voice over IP. The primary motivation for the development of DCCP is to provide a way for applications to gain access to standard congestion control mechanisms without having to implement them at the application layer and to fairly cooperate with other transport protocols namely TCP.

DCCP provides an alternative to UDP to efficiently deliver multimedia content over satellite and at the same time fairly cooperating with other transport protocols. DCCP provides a standard way to implement congestion control and congestion control negotiation for multimedia applications. It provides a choice of congestion control mechanisms for each half-connection. CCID 2 is based on the TCP SACK-like

congestion control protocol [FLOYD-CCID2-06], is appropriate for DCCP flows that would like to receive as much bandwidth as possible over the long term, consistent with the use of end-to-end congestion control, and that can tolerate the large sending rate variations characteristic of AIMD congestion control, including halving of the congestion window in response to a congestion event. CCID 3 (Congestion Control Identifier 3) is based on the TFRC congestion control KOHLER-CCID3-06]. TFRC exhibits a much lower variation of throughput over time compared to TCP making it more suitable for multimedia applications such as TVoIP and VoIP since it allows the sending rate to vary more smoothly by decreasing and increasing the sending rate gradually, while ensuring that it competes fairly with TCP. However, this makes TFRC to respond slower to changes in available bandwidth compared to TCP. CCID 4 FLOYD-CCID4-06] is a suggested variant of CCID3 that is based on TFRC-SP.
Effects of loss, delay and Bandwidth on Demand on DCCP have not yet been analyzed. Even though DCCP is touted to be the defacto transport protocol for multimedia services considering the numerous benefits offered by DCCP, to promote the use of DCCP for delivering multimedia services over Satellite, a detailed study of the performance issues of DCCP is imperative considering the impact of loss, delay and Bandwidth on Demand. Any required improvements needed for simulating the CCIDs will be studied and implemented in the SATSIX project. The object of our simulation study is to analyze the performance of DCCP for multimedia applications in the presence of loss, delay and delay jitter. The loss, delay and delay jitter characteristics of the links will be based on the characteristics of DVB-RCS system for the return link and DVB-S2 for the forward link. It is imperative that the performance of DCCP is analyzed over satellite systems because we expect widespread deployment of DCCP in standard Internet applications and we expect these systems to also work via the satellite network

Conclusions

In this paper, a new network architecture, which support IPv6 and can integrate hybrid satellite and wireless local loops (WiFi and WiMAX) to provide low-cost universal broadband access, is proposed. It includes the overall reference network and functional architectures, and the architectures related to the specified advanced network techniques, such as QoS, multicast, security and mobility, for IPv6. The transport protocols can will be used in SATSIX are also investigated.

Acknowledgement

This work is supported by the IST FP6 SATSIX project, funded by European Commission (EC). The financial contribution of the EC towards this project is greatly appreciated.

References

[KOHLER-DCCP06] E. Kohler, M. Handley, S. Floyd, Datagram Congestion Control Protocol, RFC 4340, 2006.

[FLOYD-CCID2-06] S. Floyd, E. Kohler, Profile for DCCP Congestion Control ID 2: TCP-like Congestion Control, RFC 4341, 2006.

[KOHLER-CCID3-06] E. Kohler, M. Handley, J. Padhye, Profile for DCCP Congestion Control ID 3: TFRC Congestion Control, RFC 4342, 2006.

[FLOYD-CCID4-06] S. Floyd, E. Kohler, Profile for DCCP Congestion Control ID 4: the Small-Packet Variant of TFRC Congestion Control, 2006.

[FLOYD-DCCP06] S.Floyd, M. Handley, E. Kohler, Problem Statement for DCCP, RFC 4336, 2006.

[RFC 3775] D. Johnson, C. Perkins, J. Arkko, ”Mobility Support in Ipv6”, IETF RFC 3775, June 2004.

[RFC 4140] H. Soliman, C. Castelluccia, K. El Malki “Hierarchical Mobile IPv6 Mobility Management (HMIPv6)”, IETF RFC 4140 (Experimental), Aug 2005.

[RFC 4260] P. McCann, “Mobile IPv6 Fast Handovers for 802.11 Networks”, IETF RFC 4068 (Informative), Nov 2005.

[RFC 3261] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, E. Schooler, “Session Initiation Protocol”, IETF RFC 3261, June 2002.

[FMKE] ‘The Flat Multicast Key Exchange protocol’, L. Duquerroy, S. Josset, Internet Draft, IETF, September 2004.