

Published in IET Communications
 Received on 16th July 2009
 Revised on 14th January 2010
 doi: 10.1049/iet-com.2009.0453

In Special Issue on Satellite Systems, Applications
 and Networking



Broadband satellite multimedia

Y.F. Hu¹ M. Berioli² P. Pillai¹ H. Cruickshank³
 G. Giambene⁴ K. Kotsopoulos¹ W. Guo¹ P.M.L. Chan¹

¹University of Bradford, Bradford, West Yorkshire BD7 1DP, UK

²German Aerospace Center (DLR), Institute of Communications and Navigation, Oberpfaffenhofen-Wessling, Germany

³Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey GU2 7XH, UK

⁴Information Engineering Department, University of Siena, Via Roma, 56 53100, Siena, Italy

E-mail: y.f.hu@bradford.ac.uk

Abstract: The broadband satellite multimedia (BSM) architecture standardised by ETSI defines a satellite independent service access point (SI-SAP) interface layer that separates the satellite independent features of the upper layers from the satellite dependant features of the lower layers, and provides a mechanism to carry IP-based protocols over these satellite dependent lower layers. This enables interoperability at the IP layer between satellite systems of different physical and link layers technologies that fully comply with the SI-SAP concept. This study reviews past and current standardisation activities including the BSM quality of service (QoS) architecture, security architecture, network management that have been carried out by the ETSI Technical Committee-Satellite Earth Stations and Systems (TC-SES)/BSM working group and looking into the future to extend current SI-SAP functions that can enhance existing QoS provision and security management capabilities as well as proposing a mobility management architecture that complies with the IEEE 802.21 media independent handover framework to support BSM mobility and to allow integration of satellite networks with fixed and mobile network infrastructures. A service-based network management architecture is also proposed to allow management flexibility and integration of business and operation support functions, paving the way for satellite integration into the Internet of the future.

1 BSM overview

Different from wired or optical networks, where over provisioning of capacity is often used to ensure QoS for packet-based transport, and other wireless and access networks in general, where the costs for provision of the physical medium (cables or airtime) can be charged over a high number of users, satellite systems have always faced the problem of small number of users and expensive airtime, and thus needs a very careful capacity allocation mechanism to save costs. In addition to that the market of manufacturing satellite equipments and components has a relatively lower competition in comparison with terrestrial markets, and thus smaller need of interoperability between different satellite systems. Historically, these different issues have often led satellite systems to be designed in a monolithic way, with optimised protocol stacks, which exploits proprietary

solutions and specific software and hardware components that only interwork in specific and predefined configurations.

The possibility to separate the management of protocols operating at the IP layer (and above) from the ones working at lower layers is an appealing feature not only for the technical and economic benefit of satellite networks, but also for easing their future integration with heterogeneous networks in general. In this direction the satellite standard ETSI BSM has begun its development, allowing specific layer 2 and layer 1 satellite systems to be compliant at layer 3 and above with other systems. This is realised through defining a protocol stack architecture [1], where satellite dependent (SD) layers (layers 1 and 2) are interconnected with satellite independent (SI) layers (layers 3 and above) through the satellite independent-service

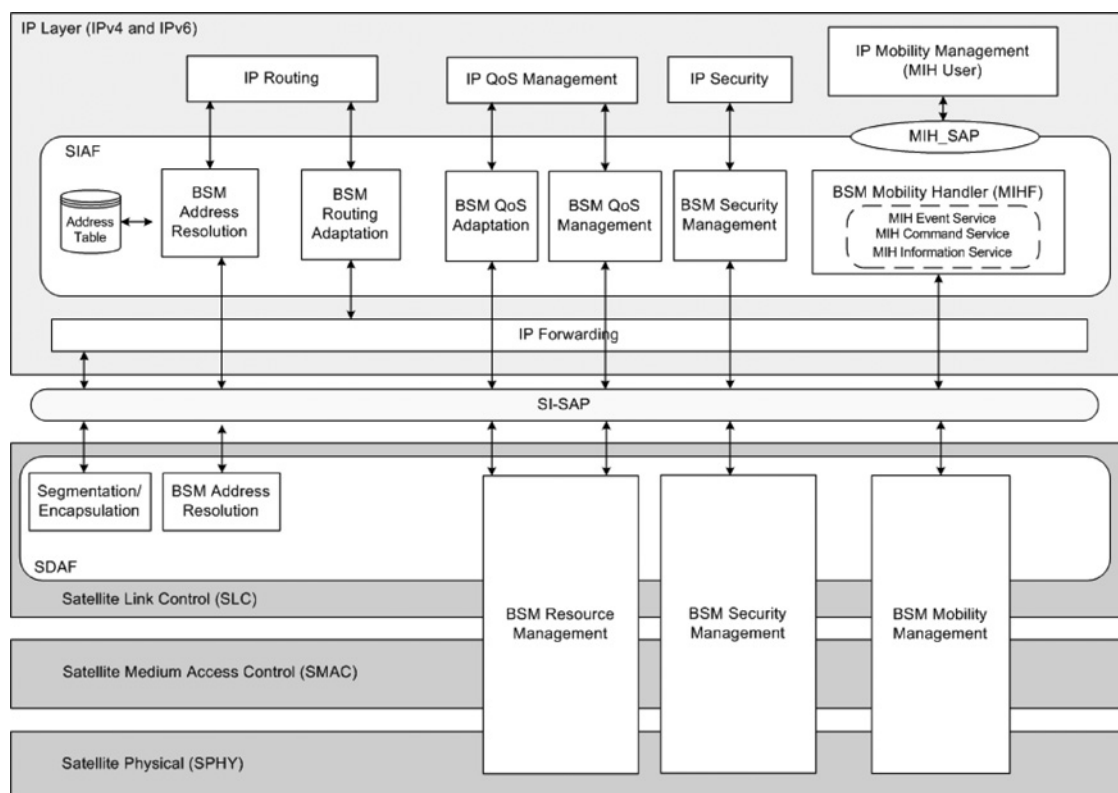


Figure 1 BSM protocol and functional architecture with mobility extension

access point (SI-SAP) interface to support a number of generic functions distributed between the SI adaptation functions (SIAF) and the SD adaptation functions (SDAF) blocks with corresponding primitives; in particular address resolution, resource management (QoS), multicast group management, security. Fig. 1 shows the generic BSM protocol stack and functional architecture being extended to include the mobility management (MM) architecture.

This study reviews BSM standards that have been defined by the ETSI TC-SES/BSM working group and proposes some enhancements and extensions to existing BSM specifications. Section 2 gives an overview of the QoS management architecture and proposes an enhancement to include cross layer QoS support with performance enhancing proxy (PEP). The security architecture is then described in Section 3 with extended functionalities to include authentication, authorisation and accounting (AAA). Mobility management has yet to be defined in the BSM standard and this study proposes the utilisation of the IEEE 802.21 media independent handover (MIH) framework to define a MIH-enabled BSM MM architecture in Section 4. Work on BSM network management has just started in the BSM working group and an extension to the currently defined BSM network management architecture using a service-based paradigm is proposed in this study. The main objective is to

prepare BSM for seamless integration with the Internet of the future.

2 BSM QoS management

2.1 QoS architecture

The BSM QoS architecture [1–4] makes use of the BSM protocol architecture characteristics where SI protocol layers are separated from lower SD layers. At the IP layer, two principal techniques for QoS provision exist: DiffServ and resource reservation protocol/integrated services (RSVP/IntServ). At the SD layers more sophisticated QoS methods are closely linked to lower layer resource management and control.

For a BSM system belonging to an IntServ (or DiffServ) domain, agreed IP service classes have to be translated into satellite system dependent QoS classes when packets are forwarded over the satellite. Thus, IntServ IP flows (or differentiated services code point (DSCPs)) need to be carefully mapped onto SD services. This is accomplished with the concept of queue identifiers (QIDs). The QIDs represent abstract queues that associate IP queues used by IntServ/DiffServ with layer 2 queues. At a BSM satellite terminal (ST), the QoS control functions operate in the control plane protocol stack across the SI-SAP and interact with the user plane. The IP resource manager, locally

located in the SIAP, handles IP queues and IP resource requests and passes them to the lower layers if necessary. It also interfaces with external IP signalling protocols such as RSVP, next steps in signalling (NSIS) etc. QIDs are considered to be controlled locally by the QID resource manager, which is logically located in the SDAF and is responsible for QID allocation and release at the ST. The QID resource manager directly interfaces with the SD resource manager in order to manage real satellite resources.

The mapping of IP queues onto SD queues is performed in two stages: first mapping between IP queues and QIDs using the IP-to-QID mapping table, and second between QIDs and SD queues through the QID-to-SD mapping table. An additional table, the QID QoS specification (QIDSPEC) table, is used to keep track of the QID QoS characteristics.

Each QID offers a defined type of service for the transfer of IP packets to the SD layers, as well as a means of forwarding packets to different BSM ST destinations. As such, a QID is used as a label for every user data transfer across the SI-SAP and therefore all SD QoS characteristics on the link between two peer SI-SAPs should be summarised in the QID description. QIDs may be assigned statically, for example, by management configuration or dynamically using the SI-SAP resource reservation primitives and it is only used at the SI-SAP. However, the QID is not expected to be carried over the air interface during data transfer; instead the association of system specific labels to QIDs should be done locally in the ST. The QoS associated with a QID shall be defined as a QIDSPEC parameter, which is derived from the RSVP flow specification (FLOWSPEC) object [3]. When a QID is invoked, this parameter needs to be provided.

At the ST, the ST QID resource manager, hereafter called the STQRM, is responsible for translating the QIDSPEC into values which are used to invoke SD resources and to associate QIDs with SD queues. The set of dynamic resource reservation service primitives defined on the SI-SAP interface for exchanging parameters between the IP queue manager and the STQRM and their associated parameters can be referred to [3].

The STQRM receives QID allocation requests from the IP resource manager and sets the allocation of SD resources accordingly. The interaction between different modules in the control plane is shown in Fig. 2 and is summarised below:

1. The IP resource manager interacts with the IP classifier and queuing module in the user plane and with external IP signalling (optional) to determine when and whether new resources are needed. The IP DiffServ queues may remain static, but the traffic situation might change. Such interactions are performed via the terminal defined

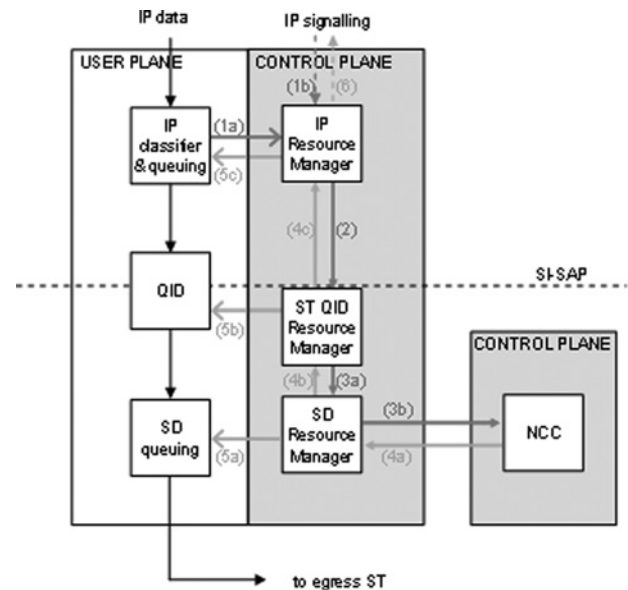


Figure 2 Control plane operations of a QoS-aware satellite terminal

signalling interface (1a) and BSM defined standard IP signalling (1b) such as RSVP.

2. Should there be any changes in the situation, the IP resource manager should notify the STQRM and take appropriate actions to allocate/release resources at the SD layers through the SI-SAP primitives (2).

3. This triggers a message from the STQRM to the SD resource manager (3a) and another from the SD resource manager to the network control centre (NCC) (3b), assuming that the resources at the SD layer are centrally managed.

4. The NCC responds to the SD resource manager through the signalling interface (4a). The response finally passes to the IP resource manager via the signalling interface (4b) and the SI-SAP primitives (4c).

5. These responses will enable the (re)configuration of the queue structure and of the mapping through signalling interfaces (5a), (5b) and (5c) between individual resource managers and their associated queues.

6. These operations may trigger optional responses at IP signalling level using standard IP signalling protocols such as RSVP, NSIS (6) open systems interconnection (OSI).

2.2 Cross layer QoS management in BSM

Although the BSM approach may guarantee an independent design of protocols at distinct OSI layers, thus reducing the complexity and allowing the interoperability among equipments of different manufacturers, however, there is tight interdependence between layers in satellite systems.

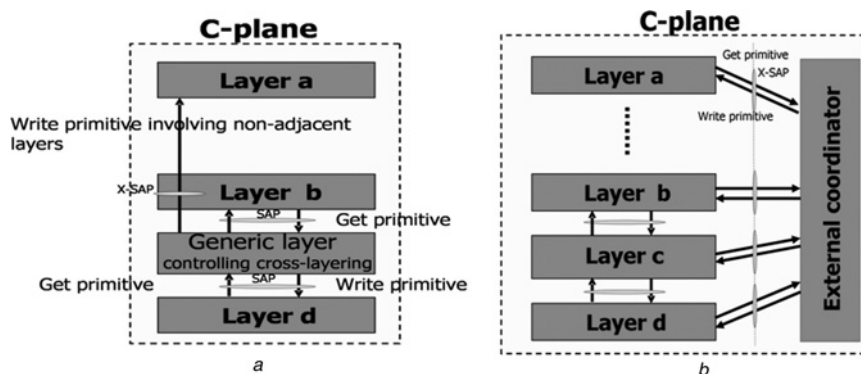


Figure 3 Cross-layer signalling exchange among protocol layers

a Horizontal approach with a protocol having the control
b Vertical approach with an external coordinator

Current research considers cross-layer interactions (that is, signalling exchange) between protocol layers [3, 4]. Cross-layering requires the exchange of signalling where the coordination of signalling is exerted by either a protocol layer (horizontal approach) or by an external controller that is common to all the layers (vertical approach). In the first case, as shown in Fig. 3*a*, the coordinating protocol layer can have direct interfaces (SAPs) with adjacent layers and cross SAPs (X-SAPs) between non-adjacent layers. In the second case, a global coordinator of different layers has interfaces (X-SAPs) with all the protocol layers and can have control on their internal state variables, reading and modifying them, depending on external events (see Fig. 3*b*).

Cross-layer techniques should be supported by BSM primitives (control plane) through the SI-SAP interface between the media access control (MAC) layer and L3. These primitives concern the interactions between the IP resource manager and STQRM. Consider a satellite network scenario where the NCC is co-located with the gateway and that the protocol stack is compliant with the BSM standard at both the ST and the NCC/gateway. Assume that the MAC layer is in charge of controlling the cross-layer signalling exchange with primitives (horizontal approach) at both the ST and/or at the NCC/gateway.

With this approach, the NCC/gateway can have a direct control over congestion via layer 2 resource allocation decision. This can allow the NCC to anticipate congestion events that otherwise could cause packet losses with a possible drop of the transmission control protocol (TCP) congestion window. The NCC can exploit these functionalities by means of a PEP approach that 'splits' the TCP connection by isolating the satellite segment. The cross-layer PEP scheme envisaged here is a transport-layer integrated PEP operated on the NCC side and based on the horizontal cross-layer signalling approach [5]. The PEP makes use of modified transport-layer ACKnowledgments (ACKs), here denoted as ACK* (use of in-band signalling and non-transparent PEP solution).

Two possible directions of the TCP flow in satellite networks and the related role of the PEP/gateway/NCC can be considered. Taking the digital video broadcasting-return channel via satellite (DVB-RCS) standard [6, 7] with multi frequency time division multiple access (MF-TDMA) air interface as an example and assuming that the MAC layer at the PEP/gateway/NCC can exchange cross-layer signalling with the transport layer.

Case 1: PEP and cross-layering for Internet servers (forward path). In order to cope with satellite link capacity variation, the NCC/PEP/gateway should know the physical layer conditions of the ST through a feedback channel. Then, X-SAP signalling could be used to inform the PEP at the gateway about the physical layer conditions. Correspondingly, the PEP should use specially modified ACK packets that shrink the receiver window so that the TCP sender stops sending packets and the sender congestion window value can be frozen. When the satellite link conditions improve, the PEP should allow the re-opening of the advertised window.

Case 2: PEP and cross-layering for ST servers (return path). Suitable PEP functionalities are considered at the NCC/gateway to support the TCP flows. In particular, it is envisaged that the NCC at layer 2 could use an upward cross-layer signalling to notify its transport layer when the capacity available in the satellite network is close to saturation. The transport layer of the NCC could thus signal to its peer on the ST side that there is congestion via in-band downward signalling using suitably modified transport layer ACK* so that the increase in traffic injection by TCP could be temporarily stopped. In this direction, the PEP should act as a spoofer on the ACK flow coming from the Internet and modify the ACK to ACK* when there is resource congestion on the satellite side. This cross-layer approach could prevent the occurrence of massive buffer overflows and subsequent TCP-repeated timeouts, thus permitting to increase the bandwidth utilisation in satellite networks. With this approach FTP with NewReno has a

transfer time reduction of 26% with respect to a non-cross-layer scheme (continuous rate assignment by the NCC) in the presence of a packet error rate of 2%. More details on performance evaluation and comparisons are provided in [8].

The available SI-SAP primitives already include some instruments to perform cross-layer algorithm (see in particular the SI-C-QUEUE_STATUS-*** primitives). Nevertheless, on the basis of the cross-layer potentialities described, the following recommendations and impacts are considered for the BSM protocol structure and SI-SAP interface definition.

QIDSPEC at SI-SAP could be enriched with the following cross-layer information: PHY modulation and coding conditions coming from physical layer (upward signalling direction).

SI-C-QUEUE_STATUS-res primitive could be extended to include TCP state coming from upper layer (downward signalling direction).

X-SAP interfaces should be defined to support new primitives and the direct exchange of signalling among non-adjacent layers based on the internet control message protocol approach [9].

2.3 PEP architecture

Fig. 4 shows the combined PEP protocol stack with the BSM ST and gateway terminal architectures. The PEP residing on the BSM ST side is called ST PEP (PEP client) and the one on the BSM gateway side is called the gateway PEP (PEP server). Both PEPs have a similar architecture with two interfaces, one to the BSM satellite network and one to terrestrial networks. On the satellite side, the ST/gateway PEP are connected to BSM ST/gateway through an Ethernet LAN. On the terrestrial network side, normally, the PEP client connects to hosts on the same LAN, whereas the gateway PEP connects to a content server through the general Internet. However, the gateway PEP can be located remotely from the BSM gateway, compliant with the vertical approach for cross-layer PEP.

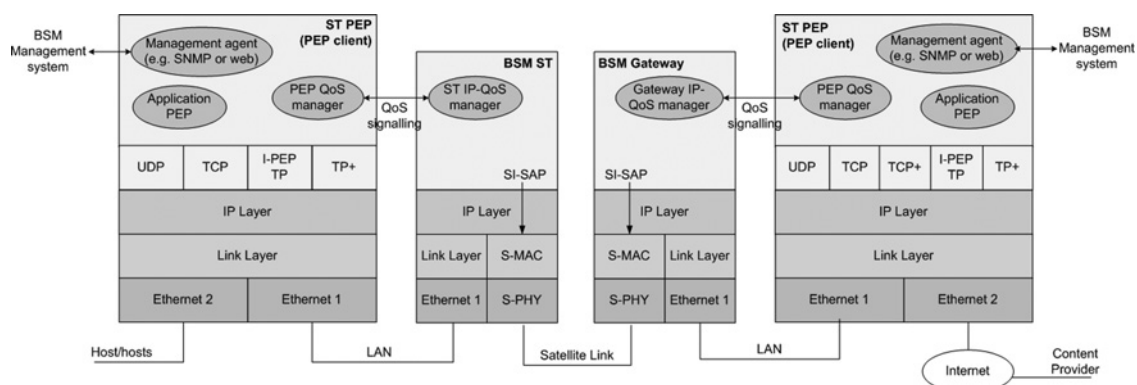


Figure 4 BSM PEP architecture

The transport protocol in the PEP is divided between standard TCP/user datagram protocol (UDP) and PEP specific transport protocols. As shown in Fig. 3, the PEP specific transport protocol can be:

A modified TCP (TCP+) such as the Hybla protocols [10], which is used in integrated PEP configurations, where only gateway PEP will be used (no ST PEP).

Standard I-PEP [2] transport protocol (I-PEP TP), recommended by SatLabs [11] is used in the distributed PEP configurations. The I-PEP TP is based on an extension set to TCP termed SCPS-TP, which was produced by the consultative committee for space data systems.

Proprietary distributed transport protocol (TP+), where other company specific (non-standard) protocols are used.

The ST/gateway PEPs can be managed either locally or remotely. For remote management, either simple network management protocol (SNMP) or hypertext transfer protocol (HTTP) protocols can be used to communicate with the BSM management system (BMS). In both cases the PEP monitoring and configuration controls can be based on the standard management information base (MIB) II and enterprise specific PEP MIBs. Both figures also show the QoS signalling between the PEP and the BSM QoS managers in the ST and gateway. Such signalling can be used for QoS monitoring of the ST/gateway queues and adjusting rate control parameters accordingly to maximise the use of the satellite capacity. The optimum PEP performance is expected to require a close matching between the PEP configuration and the QoS of the associated lower layer bearer services. A set of PEP usage scenarios have been already defined, readers can refer to [7] for further information.

3 BSM security

3.1 BSM security protocol architecture

The ETSI TC-SES/BSM working group (WG) has defined the BSM security protocol and functional architecture [12, 13] in accordance with the two phases of the security process:

- Security establishment such as entity authentication and key exchange. This is normally a control plane function.
- Secure data exchange such as data encryption and data integrity. This is normally a user plane function.

In the security establishment phase, AAA protocols such as RADIUS [14] and Diameter [15] can be used for user authentication and access control. The three entities are involved in the RADIUS/Diameter authentication process:

Supplicant: The end user or machine requesting access to the network. With respect to the BSM network, this is the user device connected to the BSM ST.

Authenticator: The authenticator is the access device or gateway, which is typically a switch or an access-point or a hub. This device initiates authentication when a supplicant requests to join the network and also physically allows or blocks access to the network based on the authentication outcome. Thus, the authenticator is located in the BSM gateway.

Authentication server: This is typically a RADIUS/Diameter server that is responsible for authenticating the user access requests. It contains a database of all user credentials and user profiles. The authenticator server will be hosted in the BSM gateway.

The functional entities, together with their locations and interactions with respect to the BSM protocol architecture define the BSM security functional architecture.

3.2 BSM security functional architecture

In defining the BSM security functional architecture, the concept of BSM security association identity (SID) is introduced. The BSM SID is used to convey security information such as encryption keys, digital signature methods and security policy exchanges between BSM local and network security managers. Although the BSM local security manager only manages a single ST, the BSM network security manager in a BSM gateway controls the security for different BSM STs. If there is only one single BSM network security manager, then the SID will be unique to the whole BSM network. If there are several network security managers (for example one for each internet service provider (ISP)), then the SID must be used in conjunction with the BSM-IDs of the source and destination entities in order to identify a security association between two BSM entities.

The BSM WG identifies four cases of security: (a) mixed layer security; (b) link layer security; (c) end-to-end security; and (d) IPsec security. In this study, extensions on the security functional architectures of cases (a) and (b) are presented.

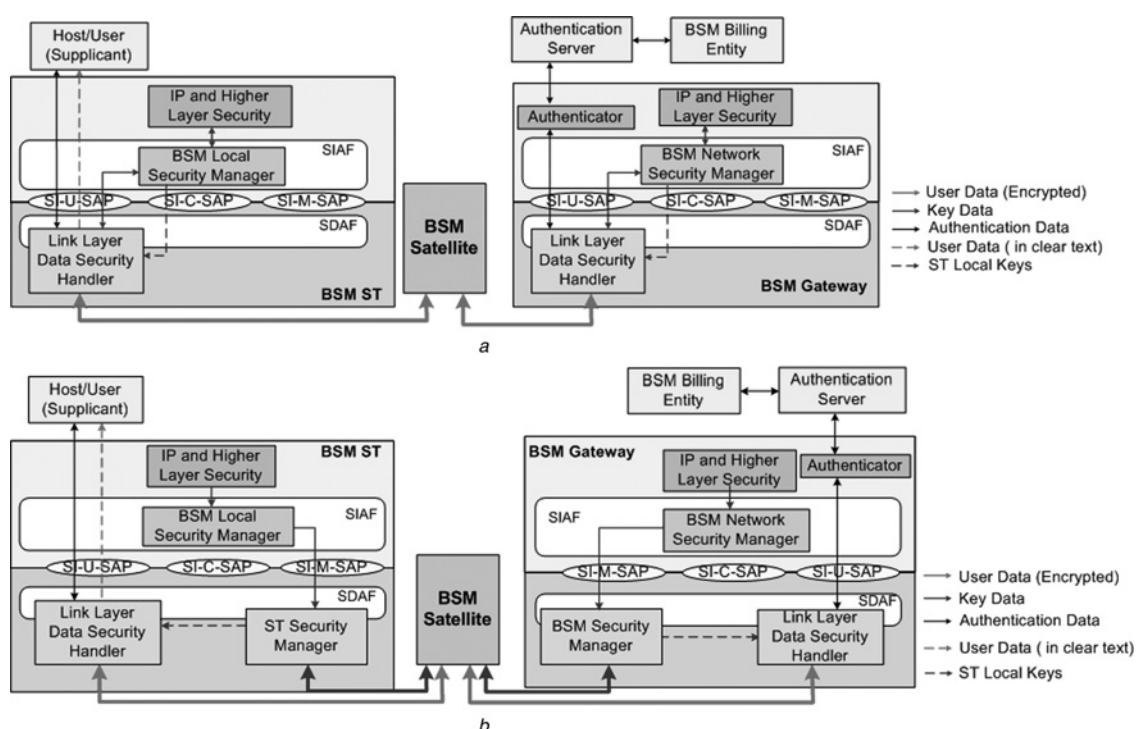


Figure 5 BSM security functional architecture

- a Mixed layer security
b Link layer security

Mixed layer security: In this case, higher layer protocols are used for setting up security associations and security key negotiations while link layer security mechanisms are used for data security over the BSM network. The BSM security manager located in the SIAF processes and relays the security information from the higher layer security protocol to the link layer data security handler (the encryption engine) located below the SI-SAP. Typical examples of such a system are DVB-RCS with MPE or unidirectional lightweight encapsulation (ULE) IP encapsulation. In this case, security is provided between the BSM ST and the BSM gateway. Fig. 5a also shows the three AAA entities involved in the client authentication process. Here the secure link layer is used to carry the authentication information between supplicant and authentication server. The SI-U-SAP is used to communicate the user security information while the key management information is passed through the SI-C-SAP interface.

Both the authentication server and the BSM network manager communicate with the BSM NCC/gateway regarding security and authorisation. Registration and re-key security association must be established between the BSM network security manager and local security manager in each ST. In the case of link layer security, the specific satellite systems security must be used. For example, for DVB-RCS satellite systems, the logon and key exchanges procedures of DVB-RCS must be used to establish all security associations. This provides mutual authentication of all entities and establishes the security keys. The SID must be used in all security management message exchanges.

Link layer security: In this case shown only link layer security mechanisms are used for setting up security associations and also for securing the data sent over the BSM network. This case is applicable to asynchronous transfer mode (ATM), DVB-RCS and ULE security systems that are implemented in the BSM network in the satellite link layer only. The security key negotiation takes place between the ST security manager and the BSM security manager that controls the respective link layer data security handler below the SI-SAP. This case is transparent to the BSM network as there is no direct interaction from any higher layer security protocols. However, the BSM local and network security managers must be able to enforce the BSM or higher layer security policy rules that are deemed applicable. Such communication must use the SI-M-SAP interface. The SID must be used in all security management message exchanges.

4 BSM mobility management

4.1 MIH-enabled BSM mobility protocol architecture

There has been an increasing user need for broadband services on the move. To support such broadband mobile services through satellites, a mobility extension for BSM is required. Currently, mobility support has not been considered in the BSM specifications. In analogy to the BSM SI-SAP standardisation activities, the IEEE802.21 MIH framework [16] defines a unified interface between different link layer technologies for the support of seamless mobility between heterogeneous IEEE 802 networks and between IEEE 802 and other mobile wireless technologies.

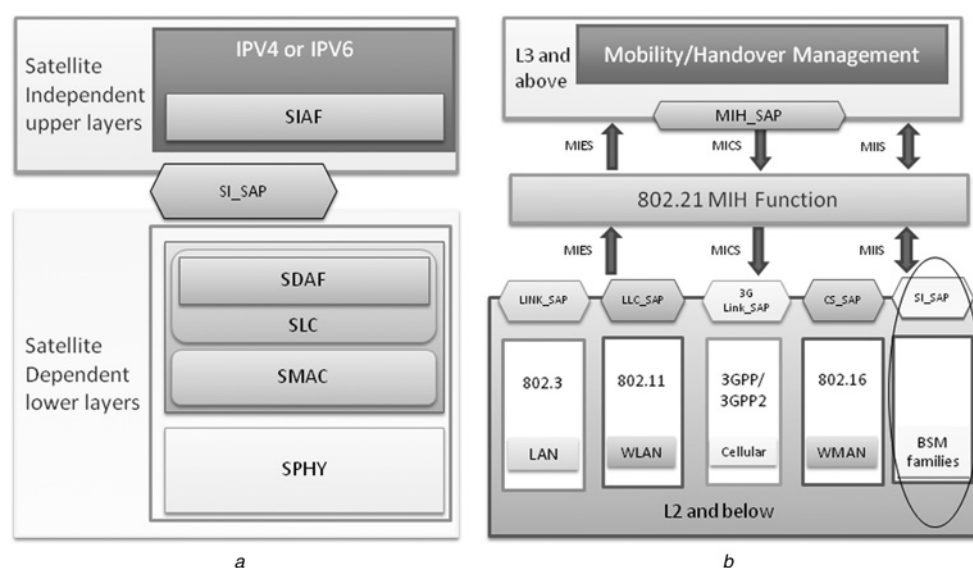


Figure 6 Synergy between BSM SI-SAP and the MIH framework

- a BSM SI-SAP protocol architecture
- b IEE 802.21 MIH framework

This unified interface is presented as an abstraction layer function, the media independent handover function (MIHF), for handover detection, initiation and decision. Fig. 6b presents the IEEE 802.21 MIH framework together with the BSM protocol architecture in Fig. 6a to illustrate the synergy between the two frameworks.

To facilitate handover, the MIHF provides three services: media independent event service (MIES), media independent command services (MICS) and media independent information services (MIS). Entities in layer 3 and above that use the services provided by the MIHF are called MIH users. MIH users access MIHF services through the MIH_SAP, which is a media independent interface between the MIHF and MIH users; the MIH_LINK_SAP that defines the abstract media dependent interface between MIHF and different link layer technologies; and MIH_NET_SAP for service transport between the local and the remote MIHFs. Each SAP consists of a set of service primitives that specify the interactions between the service user and provider. Service primitives defined in the MIH_LINK_SAP needs to be mapped onto specific link technologies.

In the IEEE 802.21 MIH framework, an MIHF in a network entity will act as a point of service (PoS) of a corresponding mobile node (MN) if it communicates directly with an MIHF in that MN. The MN exchanges MIH information with its MIH PoS using L3 transport if the PoS does not reside in the same network entity as its MN's point of attachment (PoA), which is the network side of a layer 2 link that includes the MN as the other end point. Thus, the MIH framework supports both L2 and L3 transports for exchanging MIH information.

Since both the BSM architecture and the IEEE802.21 MIH framework address interoperability between heterogeneous networks through the definitions of technology independent functions (SIAP in BSM SI-SAP and MIHF in IEEE802.21 MIH framework), a logical approach is to adopt the MIH framework into BSM for mobility support. In [17] a generic mobility extension for BSM that incorporates the IEEE802.21 MIH framework has been proposed. In [18], a BSM MM protocol architecture together with a set of SI-SAP primitives is defined to enable compatibility between the SI-SAP and the MIH standard. Table 1 summaries the mapping

Table 1 SI-SAP mobility service primitives [18]

MIH_LINK_SAP primitives	Corresponding SI-SAP primitives for handover
Link_Detected.indication	SI_C_LinkDetected.ind
Link_Up.indication	SI_C_LinkUp.ind
Link_down.indication	SI_C_LinkDown.ind
Link_Parameters_Report.indication	SI_C_MEFReport.ind
Link_Going_Down.indication	SI_C_LinkGoingDown.ind
Link_Handover_Imminent.indication	SI_C_HO.ind
Link_Handover_Complete.indication	SI_C_HC.ind
Link_PDU_Transmit_Status.indication	SI_C_PDUTxStatus.ind
Link_Actions.request	SI_C_HO.req
Link_Actions.confirm	SI_C_HO.cfm
Link_Get_Parameters.request	SI_C_GetMEF.req
Link_Get_Parameters.confirm	SI_C_GetMEF.cfm
Link_Capability_Discover.request	SI_M_CapDiscover.req
Link_Capability_Discover.confirm	SI_M_CapDiscover.cfm
Link_Event_Subscribe.request	SI_M_EvntSub.req
Link_Event_Subscribe.confirm	SI_M_EvntSub.cfm
Link_Event_Unsubscribe.request	SI_M_EvntUnsub.req
Link_Event_Unsubscribe.confirm	SI_M_EvntUnsub.cfm
Link_Configure_Thresholds.request	SI_M_ConfigThd.req
Link_Configure_Thresholds.confirm	SI_M_ConfigThd.cfm

between the MIH_LINK_SAP primitives and the SI-SAP primitives defined in [18].

The MIH-enabled BSM MM protocol and functional architecture is presented as a part of Fig. 1. To incorporate the MIH framework into the BSM protocol architecture, a new functional entity, the mobility handler, is created in the SIAF. The mobility handler residing in the SIAF processes higher layer mobility functions such as IP mobility functions into BSM mobility functions and vice versa. It is logically connected to the MIH_SAP and acts as the MIHF to provide MIHF services to MIH users via the MIH_SAP. A BSM mobility management (MM) functional entity is created to handle BSM-specific MM support in the SDAF. Interaction between the mobility handler and the BSM MM via the SI-SAP allows MIH user access to BSM-specific mobility services supported by the lower layers. Such a mobility architecture enables handover between different BSM networks through the SI-SAP as well as between BSM networks and other non-BSM networks through interaction between MIH_SAP and the SI-SAP.

4.2 MIH-enabled BSM handover scenarios

MM is divided into location management and handover management. The mobility handler as shown in Fig. 1 interacts with the BSM QoS management and QoS adaptation functional blocks for resource allocation functions, and with the security management functional block to perform authentication and access control functions during the handover execution process. In relation to location management, the BSM address resolution block is used for mapping BSM addresses onto IP addresses when a handover

from the serving BSM PoS to the target BSM PoS belonging to a different subnet is required. The BSM routing adaptation block is used to facilitate mobility-related routing in order to make sure incoming and outgoing packets to and from the BSM ST can be routed to the new PoS as smoothly and seamlessly as possible.

With respect to BSM handover, three types of handover can occur: (i) intra-BSM network handover that involves handover within a BSM network (e.g. within a DVB-RCS network); (ii) inter-BSM networks handover that involves handover between two different BSM networks; and (iii) handover between BSM and non-BSM networks. Both intra- and inter-BSM handovers can involve beam handover, satellite handover and gateway handover. For intra-BSM network handover, the handover procedures will be handled inside the BSM network with specific SD signalling and procedures. For inter-BSM handover, the SI-SAP layer will provide adaptation between the different link layer technologies. If the handover involves a gateway handover, services provided by the MIHF can be utilised as this involves higher layer MM functions. Similarly for handover between BSM and non-BSM networks, both SI-SAP and MIHF services will be exploited.

Fig. 7, adapted from [16], show the signalling flow diagram of handover initiation from a BSM (DVB-RCS) network to 802.16 network, with the purpose of demonstrating how MIH service primitives interact with the SI-SAP mobility primitives. The MIH-enabled BSM terminal consists of four entities in relation to the MIH and BSM SI-SAP frameworks: the upper layer (UP) entity representing upper layer entities; the MIH user representing the network entity that subscribes to the MIH services; the MIHF/SIAF represents the mobility handler

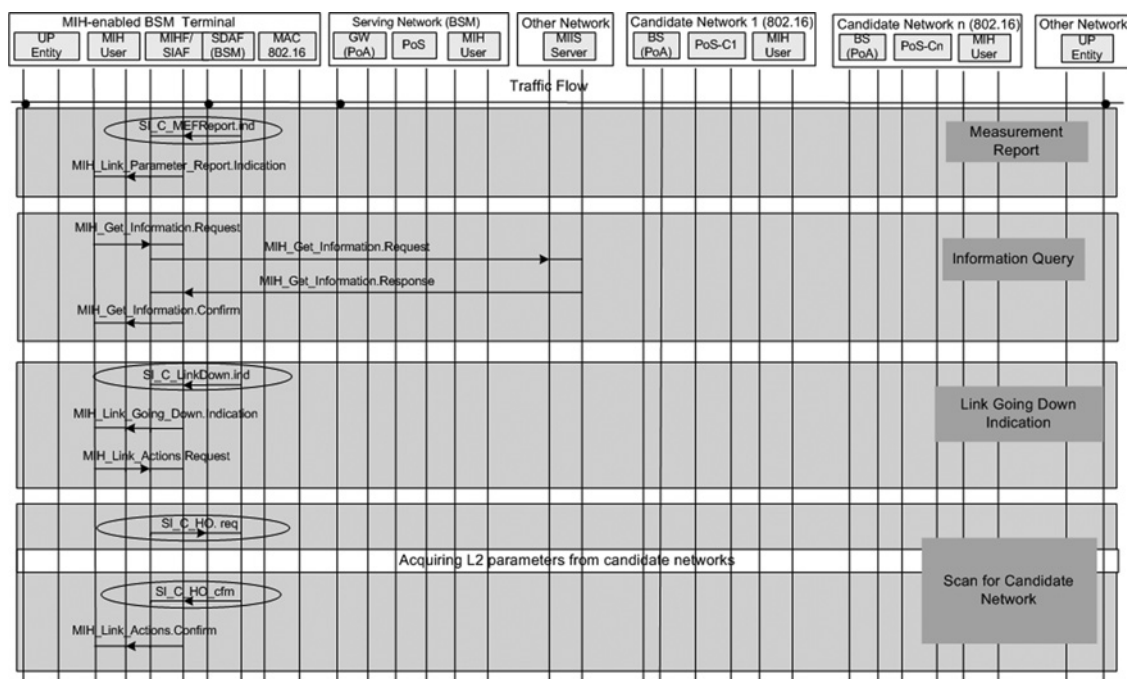


Figure 7 Handover initiation phase between BSM and WiMAX using MIH

that resides within the SIAF in the BSM SI-SAP protocol concept and the SDAF provides the BSM satellite dependent access functions as defined before. In addition, to enable handover between a BSM network and 802.16 network, it is assumed that the BSM terminal is also WiMAX (MAC 802.16)-enabled. The serving BSM network is denoted by the gateway to which the MN is attached, that is, the gateway is the PoA for the BSM terminal and is MIH-enabled. The other network component that consists of the MIIS server can be the BSM core network or a third party network that provides BSM services. Candidate network 1 and candidate network n represent neighbouring networks which the BSM can select as the target network for handover.

Fig. 7 assumes that there is an indication of a decrease in the signal strength in the measurement report generated by the SDAF of the BSM terminal. The measurement report will be passed from the SDAF to the MIHF/SIAF component using the SI-SAP primitive `SI_C_MEFReport.ind`. The SIAF, being MIH-enabled, will pass the measurement report to the MIH user in the higher layer using the MIH primitive `MIH_LINK Parameters_Report.Indication`. This triggers information queries messages from the MIH user to the network containing the MIIS server in order to acquire neighbouring networks information and vice versa using the `MIH_GET_Information.Request/Confirm` message. Upon notification of a link going down event through the `SI_C_LinkDown.ind` primitive from the SDAF, the mobility handler generates the `MIH_LINK_Going_Down.Indication` primitive, which is then passed to the MIH user. Upon receiving the link down event, an `MIH_LINK_Actions` is requested from the MIH user to the mobility handler, which in turn informs the SDAF of an imminent handover decision. A series of events is then triggered to scan the link status of the candidate networks in order to obtain relevant parameters from candidate networks.

Currently, effort has been concentrating on defining parameters and formats for SI-SAP mobility primitives to interwork with MIH-SAP primitives, with an expectation of providing input to the ETSI TC-SES/BSM working group.

4.3 BSM network management architecture

The BSM network management architecture [19] is separated into five hierarchical layers resembling that of a pyramid as illustrated in Fig. 8a, from the lowest layer that involves managing individual pieces of network equipment, to the highest layer that are closer to the running of the business that the network supports.

The first layer on the base of the layered pyramid is the network element layer (NEL) which contains the BSM resources such as the satellite terminals, gateways and the NCC. The resources use network management protocols such as the SNMP for transporting management data to the upper layers. Every resource holds an SNMP agent that retrieves information from the MIB database. The next layer is the element management layer (EML) which contains the Network Management Centre (NMC). The latter provides the FCAPS functions (Fault, Configuration, Accounting, Performance and Security management) for the BSM infrastructure. At this layer the NMC performs autonomous reconfiguration in response to a number of fault states and responds to performance requirements, for example, uplink power control. In addition, this layer holds several user accounts per multi-user terminal. The BSM management system (BMS) provides the management functions for the network and service management layers (NML) and (SML), as well as management interfaces for higher peer managers. The NML is predominantly concerned with the management of element managers and at this level the resource management is generally performed. In a heterogeneous network environment the NML is partitioned among different subnets, each part being responsible for network layer aspects in that subnet. The SML is responsible for BSM services such as local service level agreements, service provisioning and QoS monitoring. At the highest layer, the BMS interacts with the operation support system (OSS). The latter forms the business layer which is concerned with the customer and stakeholder facing aspects of the BSM system. This management architecture, adopted for the BSM system, follows a centralised approach. The problem of this approach

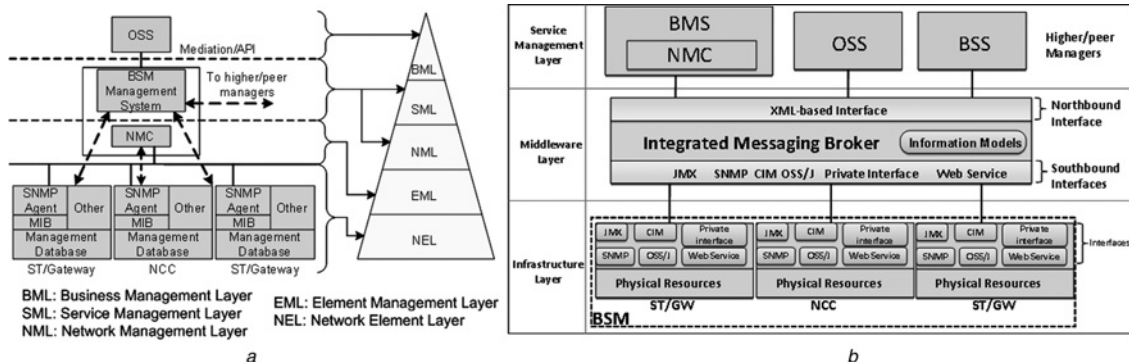


Figure 8 BSMn network management architecture

- a Hierarchical layer approach
- b Service-based approach

is the tight coupling between the managed resources (ST, gateway (GW) and NCC) and the management systems resulting in strong dependencies with the involved components. This manager-agent architecture does not allow easy interconnection among different network management systems, making it very difficult to implement advanced management functions in order to cope with the constantly evolving business processes of the telecom operators.

4.4. Service-based BSM network management architecture

Realising the limitations of the existing management model, a novel BSM management model building on the service-based paradigm as illustrated in Fig. 8b is proposed. This service-based management architecture offers flexibility and scalability because of its loose coupling nature, minimising the dependencies between the physical resources and the management services. The main concept of loose coupling is that two communicating parties (systems or services) make minimal assumptions about each other. Loosely coupled services can be modified independently, which means that if changes will be made within one system then the coupled service on the service management layer will not be affected. This management framework is divided into three layers: the infrastructure layer, the middleware layer and the SML.

The infrastructure layer contains the managed devices or resources that form the BSM network infrastructure. The middleware layer, acting as an integrated message broker, makes use of a messaging bus to provide adaptation functions for translating different management protocols into a unified format. This message bus performs dynamic routing and dispatch of management requests to multiple receivers such as the BMS, OSS and BSS (business support system). In addition, this layer is also responsible for deriving an information model to map different types of data formats, using XML as the means of exchanging management data between BSM systems and with other non-BSM systems. This concept involves the passing of management data asynchronously among heterogeneous systems using a communication channel that carries self-contained units of information. XML is used for document exchange by exchanging structured data among management applications in a lightweight manner by separating the communication from the information model. The management data received from the infrastructure layer are translated through the southbound interfaces into XML-based messages. XML is suitable for coping with multiple information models because of the fact that the management data encoded in XML documents are self-describing. Using message-based communication the physical resources such as the ST and GWs are abstractly decoupled from the higher level management applications. As a result, senders and receivers need not be aware of each other. The middleware is responsible for getting the messages to their intended destination securely using authorisation and cryptography mechanisms. The integrated message broker manages the

connection points among multiple management end points, as well as the multiple channels of communication among the connection points. These XML-based management messages are routed to the higher layer or peer managers at the SML, where higher layer or peer managers communicate with the middleware layer via the northbound interface exchanging messages based on XML format. The proposed service-based architecture offers the possibility to support multiple management protocols.

Instead of adopting a hierarchical structure between the BMS and the OSS, the BMS and OSS in the proposed service-based architecture are regarded as peer entities that provide stacks of management services to be used by other management services. For example, the BMS provides FCAPS management services that can be called by the OSS. The proposed architecture also considers the BSS that can interact with the OSS and the BMS in order to provide business and customer related services. The BSS provides processes that a service provider requires in order to conduct relationships with external stakeholders including customers, partners and suppliers. Owing to the fact that the high/peer managers make use of XML data structures, the messages could be processed by examining the content of the XML messages, allowing control over where they are delivered. In the hierarchical layer approach the complexity of the management architecture resides at the SML. The BMS is not only responsible for performing FCAPS functions but for additional routing functions, message transformation and for dealing with security aspects of the management information. Furthermore, the BMS needs to provide mechanisms and proprietary application program interface (API) in order to connect and exchange management information with other OSS systems. This additional functionality adds more complexity to the BMS system, resulting in an increasing need for higher processing power for a single machine. Sharing management information between BSM and other management systems proves to be difficult because of the fact that systems use proprietary interfaces which need adaptation in order to be able to exchange information with other systems.

In the service-based management architecture, functionalities are distributed across the middleware layer and the SML. The SML provides only FCAPS functions and uses a standardised way for communication among the management services via XML-based messaging as opposed to the proprietary interfaces that the hierarchical approach adopts. The middleware layer reduces the application complexity at the SML because of the use of a messaging bus that transports messages between the resources and the management applications. Routing, message transformation and security can be performed at once in the middleware layer without the need to be performed in every management application at the SML, leaving the SML focuses entirely on the management of the BSM infrastructure. As a result, this provides lighter and faster management applications. Further, this layer also provides persistent storage to back up the message transfer

medium. As a result, the BSM resources and the services at the SML do not need to connect to the network simultaneously because of the asynchronous message delivery mechanism that the middleware provides. This is particularly useful when dealing with intermittent connections, such as unreliable networks, casual users or timed connections. In addition, if the BMS fail for any reason, the messages that the BSM resources send will be buffered in the message store at the middleware layer for later processing.

The benefit of using the service-based approach is the improved modifiability. The BMS has a single connection instead of multiple dedicated connections to other systems. Adding or removing management functionality has no impact on the existing architecture. In addition, upgrading the middleware functions does not require any modification at the services in the SML. This architecture results in fewer dependencies, modifications or faults in one service, which in turn will have fewer consequences on other services. Services can be modified independently without affecting the coupled service on the SML. The management architecture is more flexible and change tolerant, because of the fact that it is based on messaging. Flexibility derives from the fact that connected management services do not have to be adjusted after changes being made in one of the systems.

In future, work will continue to define the management information base with a common information model in mind to allow interoperability. Specific FCAPS 'services' and associated management service primitives to be provided by the BSM network will be defined to allow the management plane functions to be fully utilised and interact with control plane functions.

5 Conclusion and future development

The main idea behind the BSM architecture is to create a standard interface, the SI-SAP, between SI layers and the different underlying satellite system technologies, the SD layers. In general, the SI-SAP offers an agnostic interface to whichever SD layer is used. One of the main issues in separating the two (SI and SD) layers is QoS: On the 'upper' side of the SI-SAP, compatibility has to be provided with existing IP QoS paradigms (i.e. RSVP/IntServ and differentiated services (DiffServ)), and on the 'lower' side of it, an heterogeneous set of techniques exist for QoS accomplishment in each different satellite technology. For this reason QoS provision in a BSM network was addressed introducing the key concept of QIDs. QIDs were introduced in this study together with a detailed description of the way they should be used, highlighting the potential for future smart exploitation of this concept in particular for cross-layer algorithms operating across layers 1 and 2 and the transport layer of the ISO/OSI protocol stack, utilising PEP techniques to enhance the BSM QoS support capabilities.

In analogy to the QID concept, SIDs for use in BSM security management was described in this study. A more detailed security functional architecture was derived, describing the different functional entities and their interactions for security establishment including authentication and authorisation control using RADIUS/Diameter and secured data exchange through interoperation between higher layer security manager and link layer security data handler and security manager via the SI-SAP.

A MM architecture was defined for BSM mobility extension, adopting interoperable open-standards approach to enable the SI-SAP integration with the IEEE 802.21 MIH framework for inter-BSM network handover as well as handover between BSM networks and terrestrial network. The handover scenarios were described together with a signalling flow diagram illustrating the interaction between the MIHF in the SIAF and the SDAF through SI-SAP and MIH primitives.

Finally, a service-based network management architecture was introduced to extend the current network management concept being defined in the BSM WG through a middleware layer that links different services provided by the network infrastructure layer and the management operation layer. This new network management approach offers the possibility and flexibility for interoperability between different management systems as well as for integration of the BSS with the OSS that would enhance the return on investment of the telecommunications business.

Future work includes the definition of primitives and their associated parameters for security management as well as the consolidation of the MIH-based BSM MM communication and functional architecture for different handover scenarios and strategies. The service-based network management structure will be further developed and investigated for future inputs to the BSM standardisation activities.

6 Acknowledgments

The work carried out in this study is funded by the EU project SatNEx II. The authors would like to thank partners who contribute to this project. The authors would also like to acknowledge the contributions of the whole ETSI BSM working group.

7 References

- [1] ETSI TS 102 357: 'Satellite earth stations and systems (SES); Broadband satellite multimedia (BSM); Common air interface specification; Satellite independent service access point SI SAP'
- [2] ETSI TS 102 462: 'Satellite earth stations and systems (SES); Broadband satellite multimedia (BSM); QoS functional architecture'

- [3] ETSI TS 102 463: 'Satellite earth stations and systems (SES); Broadband satellite multimedia (BSM); Interworking with IntServ QoS'
- [4] ETSI TS 102 464: 'Satellite earth stations and systems (SES); Broadband satellite multimedia (BSM); Interworking with DiffServ QoS'
- [5] GIAMBENE G., KOTA S.: 'Cross-layer protocol optimization for satellite communications networks: a survey', *Int. J. Sat. Commun. Netw.*, 2006, **24**, pp. 323–341
- [6] ETSI EN301 790 V1.4.1: 'Digital video broadcasting (DVB); DVB specification for data broadcasting. Interaction channel for satellite distribution systems', 2005–09
- [7] GIAMBENE G., HADZIC S.: 'A cross-layer PEP for DVB-RCS networks'. Proc. First Int. Conf. on Personal Satellite Services 2009 (PSATS2009), Rome, Italy, March 2009, pp. 18–19
- [8] CHINI P., GIAMBENE G., BARTOLINI D., LUGLIO M., ROSETI C.: 'Dynamic resource allocation based on a TCP-MAC cross-layer approach for DVB-RCS satellite networks', *Int. J. Sat. Commun. Netw.*, 2006, **24**, pp. 367–385
- [9] DOVROLIS C., RAMANATHAN P., MOORE D.: 'What do packet dispersion techniques measure?'. Proc. IEEE INFOCOM, April 2001, pp. 905–914
- [10] CAINI C., FIRRINCIELI R., LACAMERA D.: 'PEPsal: a performance enhancing proxy for TCP satellite connections', *IEEE A&E Syst. Mag.*, 2007, **22**, (8), pp. B-9–B-16
- [11] SatLab: 'SatLab system recommendations v2 QoS', <http://satlabs.org/>, accessed November 2006
- [12] ETSI TS 102 465 v1.1.1: 'Satellite earth stations and systems (SES); Broadband satellite multimedia (BSM); General security architecture', 2006
- [13] ETSI TR 102 287 v1.1.1: 'Satellite earth stations and systems (SES); Broadband satellite multimedia (BSM); IP interworking over satellite; security aspects', 2004
- [14] RIGNEY C., ALLAN C., RUBENS A.C., SIMPSON W.A., WILLENS S.: 'Remote authentication for dial in user service (RADIUS)'. IETF RFC 2865, June 2000
- [15] PAT R., CALHOUN P.R., LOUGHNEY J., ARKKO J., GUTTMAN E., ZORN G.: 'Diameter base protocol'. IETF RFC 3588, December 2002
- [16] IEEE Std 802.21 Part 21: 'Media independent handover services', 2009
- [17] HU Y.F., CHAN P.M.L.: 'Mobility management for BSM'. Int. Workshop on Satellite and Space Communications 2008 (IWSSC 2008), ISAE, Toulouse, France, October 2008
- [18] HU Y.F., PILLAI P., BERIOLI M.: 'Mobility extension for BSM'. Int. Workshop on Satellite and Space Communications 2009 (IWSSC 2009), Sienna, Italy, September 2009
- [19] ETSI TS 102 672: 'Satellite earth stations and systems (SES); Broadband satellite multimedia (BSM); Management functional architecture', 2009