Fusion of Digital Television, Broadband Internet and Mobile Communications

Part I of II: Enabling Technologies

F.L.C. Ong[1], X. Liang[1], P.M.L. Chan[1], G. Koltsidas[2], F.N. Pavlidou[2], N. Celandroni[3], E. Ferro[3], A. Gotta[3], H. Cruickshank[4], S. Iyengar[4], G. Fairhurst[5], V. Mancuso[6]

[1]University of Bradford, UK
[2]Aristotle University of Thessaloniki, Greece
[3] ISTI-CNR (National Research Council), Italy
[4]University of Surrey, UK
[5]University of Aberdeen, UK
[6]University of Rome "Tor Vergata", Italy

SUMMARY

The introduction of digital video broadcasting (DVB) satellite systems has become an important tool for future mobile communication and is currently a focus in several research areas such as the integration of DVB satellite systems with different wireless technologies. This tutorial consists of two parts, *Enabling Technologies* and *Future Service Scenarios*, which aims to provide an introduction to the current state-of-the art of Digital Video Broadcasting standards over satellite and its fusion with mobile and Internet technologies.

This paper, *Enabling Technologies*, focuses on providing an overview of the different technologies and issues that facilitates better understanding of the current and future operational scenarios, whereas the second paper, *Future Service Scenarios* will emphasise future research directions in this research area. In the first part, the paper will initially be focused on the introduction of different DVB satellite systems, i.e. DVB-via satellite (DVB-S), DVB return channel by satellite (DVB-RCS) and Second-generation DVB system for broadband satellite services (DVB-S.2). This is then followed by a description of the different internet protocol (IP) technologies used to support macro and micro-mobility and the migration strategies from IP version 4 (Ipv4) to IP version 6 (IPv6). Finally, the different security mechanisms for the DVB system and end-to-end satellite network are addressed.

KEY WORDS: DVB, DVB-S, DVB-RCS, DVB-S.2, IP, Mobility Management, Security

This work has been performed by members of the satellite communications network of excellence (SatNEx) project, which is supported by the European Commission under the Sixth Framework Information Society Technologies Programme.

Corresponding Author:
P.M.L. Chan
Department of Cybernetics, Internet and Virtual Systems
Richmond Road, Bradford, BD7 1DP, UK
Tel: +44 (0) 1274 233724
Fax: +44 (0) 1274 236600
E-mail: p.m.l.chan@bradford.ac.uk

1 INTRODUCTION

DVB is a TV compression/transmission scheme defined by the DVB Project. This is a market-led consortium of public and private sector organisations in the television industry. Its aim is to establish the framework for the introduction of digital television services. The specification of DVB has been a European initiative, and has been standardised by the European Telecommunications Standards Institute (ETSI).

Although DVB has its origins in Europe, the DVB Project comprises over 200 organizations from more than 25 countries around the world; DVB fosters market-led systems, which meet the real needs, and economic circumstances of the consumer electronics and the broadcast industry. The project has produced a wide range of standards for cable, terrestrial and satellite digital television (DTV) services. Key resulting DVB standards cover satellite (i.e. DVB-S) [ETS05a] and terrestrial (i.e. DVB-terrestrial (DVB-T)) delivery [ETS02]. In particular, recent DVB standards have defined satellite (i.e. DVB-RCS)[ETS03] and terrestrial (i.e. DVB - return channel terrestrial (DVB-RCT)) return channels. While these return channels may support interactive TV (iTV), they also enable other telecommunications services over DVB infrastructure, including telephony and Internet access. The DVB standards utilise a series of specifications published by the International Standards Organisation (ISO) and is known as the moving pictures expert group-2 (MPEG-2) [ISO00]. At the core of these standards there is a time-division multiplex that uses fixed-sized frames, transport stream-packets (TS-Packets), to deliver streams of data. The equipment that processes these streams is unaware about the data format. This could be digital video, digital audio, electronic programme guides, or any form of digital data.

Equipment conforming to the DVB standard is now in use on six continents, and DVB is rapidly becoming the worldwide standard for digital TV. Some countries have their own variants of the standards, notably the USA (i.e. advanced television systems committee (ATSC)) and Japan (i.e. Association of Radio, Industries and Businesses (ARIB)). These are also based on MPEG-2 and largely follow the same format as DVB, but with the addition of country-specific modifications (e.g. different video and audio formats). DVB standards have also shaped how satellite data networks are built, using a transmission system (framing, packet formats, etc) that now lies at the core of most modern satellite networks. The specifications not only provide an industry standard, but they also provide communications systems with an opportunity to use components designed for the mass market.

In this tutorial, the first section provides an overview of the most important and fundamental standards developed for DVB using satellites. Although DVB has also been extended for terrestrial networks, the focus here will be on the standards developed for broadband data delivery via satellites, DVB-S, DVB-RCS and DVB-S.2. This is followed by a description of the different IP technologies used to support macro and micro mobility and the migration strategies from IPv4 to IPv6. Finally, Section 4 describes the different link-layer security mechanisms that are implemented for ATM, DVB-S and DVB-S, and also addresses the end-to end and satellite network security, before the paper is concluded.

2 DIGITAL VIDEO BROADCAST VIA SATELLITE

2.1 DVB-S

2.1.1 Modulation and Coding Schemes

The first successful transmission system for digital television (TV) to consumers, using the DVB standards, employed satellite links using DVB-S [ETS97a]. This standard has received rapid adoption

by the satellite TV community, and has become the dominant standard since 2000. A standards-based approach has enabled a large range of digital TV based businesses to develop and thrive.

The DVB-S standards [ETS02][ETS05a] describe the modulation and channel coding system for satellite digital multi-programme TV / high definition television (HDTV) services to be used for primary and secondary distribution in fixed satellite service (FSS) and broadcast satellite service (BSS) bands. The system is intended to provide direct-to-home (DTH) services for consumer integrated receiver decoder (IRD), as well as collective antenna systems (SMATV) and cable television head-end stations. The system architecture is presented in Figure 1. Individual and Business users send their requests for data reception to their service providers (SPs) through the "Terrestrial Return" network. SPs send data to the Satellite Operator. The latter, collects data from many SPs and uses a broadcast technique to deliver data to the appropriate users.

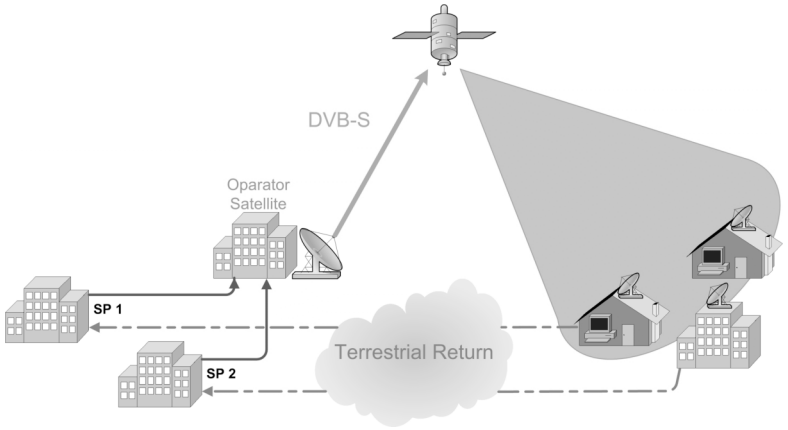


Figure 1: DVB-S System Architecture

The video, audio, control data and user data are all formed into fixed sized MPEG-2 transport packets. The MPEG transport stream (TS) packets (187 bytes + 1 sync byte) are grouped into 8 packet frames (1503 bytes). The frames do not contain any additional control information. The TS-header byte is inverted (0xB8) in the first TS packet in each coding frame, so that the receiver can identify the start of each frame. The frames are then passed through a convolutional interleaver to ensure the data follows an approximately random pattern, assuring frequency dispersion of the modulated signal. At the start of each frame, the scrambler is re-initialised. 16 bytes of Reed-Solomon (RS) coding are added to each 188 byte transport packet to provide forward error correction (FEC) using a RS (204,188) code. For satellite transmission, the resultant bit stream is then interleaved and convolutional coding is applied. The level of coding ranges from 1/2 to 7/8 depending on the intended application and available bandwidth. The digital bit stream is finally modulated using quadrature phase shift keying (QPSK) modulation. Speeds up to 68 Mbps can be achieved for 54 MHz available bandwidth.

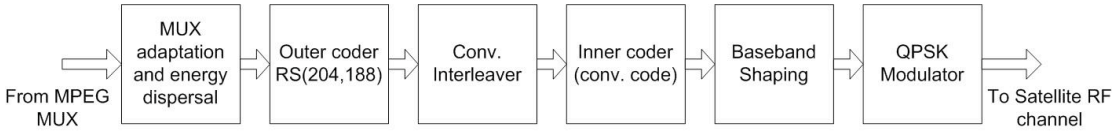


Figure 2: DVB-S Frame Formation and Modulation

2.1.2 Satellite IP Delivery Network

A satellite internet protocol (IP) delivery network can readily be constructed using low cost DVB-S

components. This provides a uni-directional (send-only) service to any location within the downlink coverage of the DVB satellite service, typically supporting transmission rates of 6-45 Mbps. (Higher rates can be achieved using slightly more expensive professional DVB-S components.)

A DVB-S link may be used for carousel data transmission, IP multicast, or a hybrid Internet access service. Such a system requires a standard digital low noise block (LNB) and a TV receive only (TVRO) antenna connected via an L-band co-axial cable to a satellite DVB data receiver card installed in a Personal Computer (or local area network (LAN)/universal serial bus (USB) adaptor box). Drivers to support these cards are readily available from the Internet, and even forms part of a standard Linux kernel.

Packet data for transmission over the DVB-S link is passed to a device called an IP Encapsulator, sometimes known as an IP Gateway. This receives data (Ethernet frames or IP packets), and formats them by adding an encapsulation header and trailer. The encapsulator then fragments the data into a stream of fixed-sized TS Packets. A specific packet identifier field (PID), carried in each TS Packet, identifies a stream. Packets for one IP flow (i.e. a specific combination of IP source and destination addresses) are sent using the same PID.

A number of vendor-specific encapsulation methods were used in early systems, but gradually these have been replaced by a method based on the format used for MPEG-2 control tables [ISO00]. This standard is known as the multi-protocol encapsulation (MPE) (specified in EN 301 192 [ETS04]). More recently, the Internet Engineering Task Force (IETF) IP has specified an alternative to MPE DVB (ipdvb) WG [IPD05]. This is called the ultra lightweight encapsulation (ULE) [FAI05] and supports a range of packet types (including IPv4, multiprotocol label switching (MPLS)), Ethernet Bridging, and importantly IPv6) with an extension format designed to provide the opportunity for new features (resembling the IPv6 network layer extension mechanism [DEE98]).

To receive the IP packets sent over a DVB-S link, a receiver needs to identify the specific PID value associated with the stream carrying the packets [MON05]. The hardware or the driver software at the receiver, may simultaneously receive several PIDs, and filters all TS Packets associated with other (unwanted) PIDs. The packets are also filtered based on their medium access control (MAC) address, and other protocol fields. The remaining packets are passed to the network layer driver, from where they are either forwarded to the attached network or to the receiver itself.

Most Internet access requires two-way communication, requiring an additional return link. Such a link may be established using the available terrestrial infrastructure (standard dial-up modem, integrated services digital network (ISDN), cable modem, wireless fidelity (Wi-Fi)), general packet radio service (GPRS), etc) to provide the return path of the bi-directional connectivity. These schemes can offer economic access to areas that do not have broadband connectivity – but there are obvious drawbacks. Capacity in the return direction is usually limited. Customers still rely on the terrestrial infrastructure, sometimes even requiring two internet service provider (ISP) agreements and it is often impossible to guarantee network availability or Quality of Service for the return part of the network connection.

2.2 DVB-RCS

The service provided by uni-directional links can therefore only provide a form of broadband service. With this in mind, a group of satellite companies (with funding from the European space agency (ESA)) sought to produce a two-way satellite system, based on DVB standards. This passed through several prototypes, eventually emerging as an ETSI standard called DVB-RCS [ETS03] [ETS97a].

The DVB-RCS standards describe a system where both forward and return paths use satellite links (Figure 3) and it was specified by an ETSI technical group founded in 1999 [ETS03]. A satellite terminal (known as satellite interactive terminal (SIT) or return channel satellite terminal (RCST)) is specified, that supports a two-way DVB satellite system.

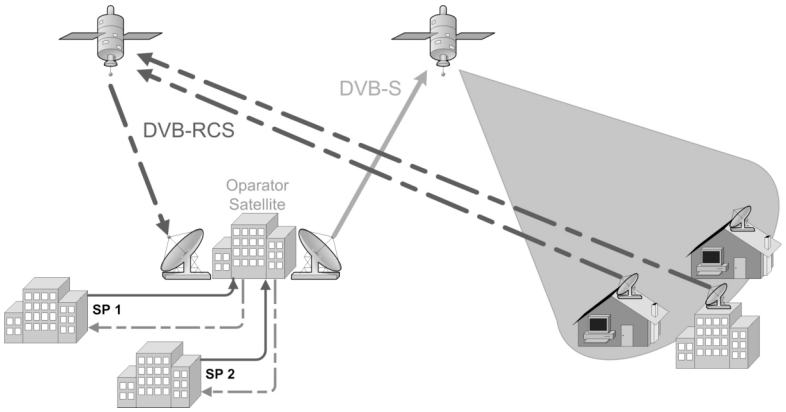


Figure 3: DVB-RCS System Architecture

In the system model, two channels are specified between the service provider and the user: the Broadcast Channel and the Interaction Channel. The former is a unidirectional broadband broadcast channel, carrying user traffic and signalling from the network control centre (NCC) and may include the Forward Interaction Path. The Interaction Channel is a bi-directional channel for interaction and is further divided into the Return Interaction Path (Return Channel), a channel from the user to the service provider to send control information (requests/responses), and the Forward Interaction Path, a channel that provides information from the NCC to the user and any other required communication for the interactive service provision. The RCST provides interfaces for both Broadcast and Interface Channels.

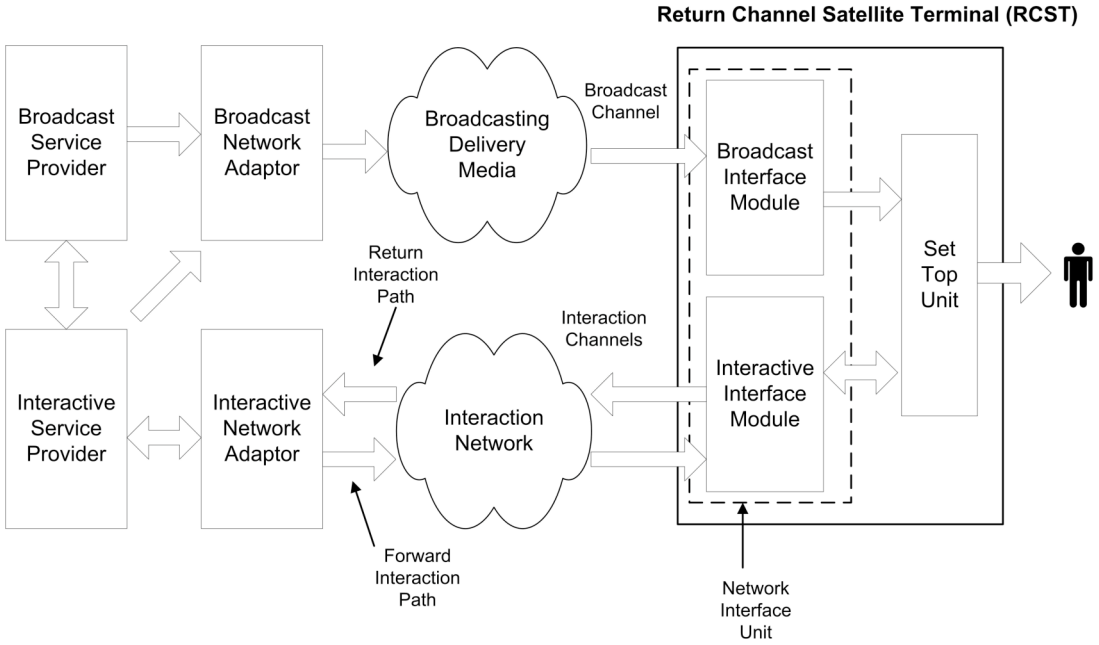


Figure 4: Block Diagram of Information Exchange in a DVB-RCS System

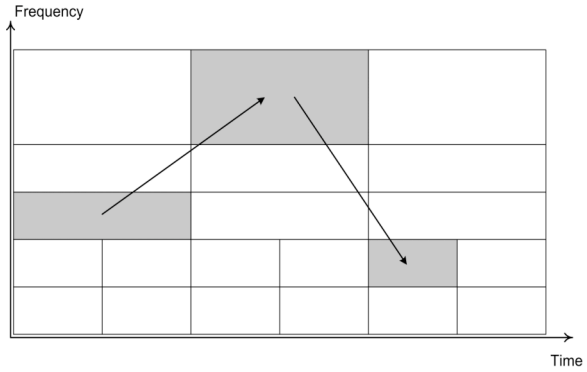


Figure 5: Adaptive MF-TDMA

The forward channel is identical to a DVB-S broadcast channel and has a single carrier, which may take up the entire bandwidth of a transponder (bandwidth-limited) or use the available transponder power (power limited). Data is organized into frames and then is modulated using a Gray-coded QPSK scheme and time division multiplex (TDM) to coordinate use of the return link capacity.

The RCSTs share the return channel capacity by transmitting in bursts, using a multi-frequency TDMA (MF-TDMA) scheme. Each return channel carrier frequency is divided in time into superframes. Each superframe is further divided into a number of frames, less than or equal to 32. Frames themselves are further divided into timeslots. The frame duration is not constant, so it is not used as a basis for timeslot allocation purposes. Frames of a superframe may not all have the same duration, bandwidth or timeslot composition. The number of timeslots within a frame can be less than or equal to 2048. In order to join the network, terminals should send joint request messages in a channel, dedicated to this purpose, using a slotted Aloha mechanism.

The timeslot allocation process shall support five capacity request categories: continuous rate assignment (CRA), rate based dynamic capacity (RBDC), volume based dynamic capacity (VBDC), absolute volume based dynamic capacity (AVBDC) and free capacity assignment (FCA).

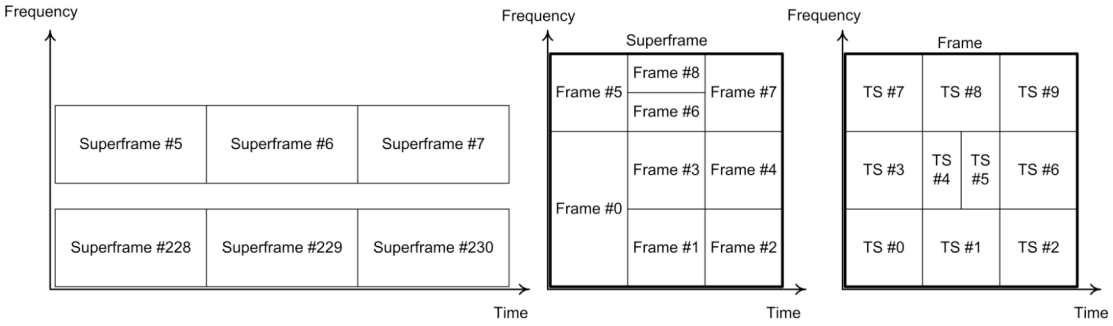


Figure 6: DVB-RCS Framing

Four types of bursts are considered: traffic bursts, acquisition (ACQ) bursts, synchronization (SYNC) bursts and common signalling channel (CSC) bursts. Traffic bursts can be of two types: asynchronous transfer mode (ATM) traffic (TRF) and MPEG2-TS TRF. An ATM traffic burst consists of one or more ATM cells, each one 53 bytes long, however these ATM cells do not support ATM classes of service. A MPEG2-TS traffic burst contains MPEG2-TS packets, each one 188 bytes long. An ACQ burst is used to achieve synchronization, prior to operational use of the network by the RCST and contain a

frequency sequence. A SYNC burst is used by the RCST to maintain synchronization and sending control information to the system. Finally, CSC bursts are only used by the RCST to identify itself during logon. They are composed of several fields describing RCST capabilities, RCST MAC address, Frequency hopping and other parameters. A RCST can change frequency, bit-rate, FEC rate, burst length, or all of these parameters, from burst to burst. Slots in the return channel are dynamically allocated.

The DVB-RCS standard is now used by many network service operators. It is supported by many manufacturers and operators. An industry-led forum, SatLabs [SAT05], exists to improve interoperability between DVB-RCS terminals and to promote deployment of the technology. The DVB-RCS group also continues to improve and refine the specification. Despite significant benefits offered by the standard compared to previous proprietary standards, this technology has yet to penetrate the mass-market.

Competition still exists for DVB-RCS, including bi-directional satellite systems that use DVB-S for their outbound transmission, but do not utilise the DVB-RCS standard for the return link (perhaps because of manufacturer investment in proprietary systems, or because the cost of current DVB-RCS terminals makes them uncompetitive in some markets).

The DVB-RCS system continues to evolve, supported by the work of the Satlabs group. Satlabs have demonstrated successes in enhancing interoperability of components in DVB-RCS systems, and recently announced a successful qualification programme for DVB-RCS terminals that will lead to an independent certification lab for equipment interoperability. In parallel, DVB and ETSI continue to advanced the standardisation work. New work will include provision of QoS functions (including cross-layer integration of Internet QoS and MAC resource management functions), the inclusion of adaptive physical waveforms (DVB-S.2, fade countermeasures, cross-layer optimisation), and support for regenerative satellites.

2.3 DVB-S.2

2.3.1 Overview

DVB-S was introduced as a standard in 1994 [ETS97a] and DVB-digital satellite news gathering (DVB-DSNG) in 1997 [ETS99]. The DVB-S standard specifies QPSK modulation and concatenated convolutional and RS channel coding, and is now used by most satellite operators worldwide for television and broadcasting services. DVB-DSNG specifies the use of 8 phase shift keying (8PSK) and 16 quadrature amplitude modulation (16QAM) for satellite newsgathering and contribution services. Since 1997 digital satellite transmission technology has evolved, and DVB-S2 is the latest advanced satellite transmission technique from DVB [ETS05a]. It makes use of the following improvements in the digital satellite transmission technology:

- New coding schemes, which, combined with higher order modulation, is considered the main focus of the DVB-S2 system.
- Adaptive coding and modulation (ACM), which may be applied to provide different levels of error protection to different service components. In the case of interactive and point-to-point applications, the ACM functionality may be combined with the use of return channels, to achieve adaptive coding and modulation. This technique provides more exact channel protection and dynamic link adaptation to propagation conditions, targeting each individual receiving terminal.

DVB-S2 is optimised for the following broadband satellite applications:

a) Broadcast services (BS) Digital multi-programme TV/ HDTV – DVB-S.2 is intended to provide DTH services for consumer IRD, as well as collective antenna systems (SMATV) and cable television head-end stations. DVB-S.2 may be considered a successor to the current DVB-S standard and may be introduced for new services and allow for a long-term migration. BS services are transported in MPEG Transport Stream format. Variable coding and modulation (VCM) may be applied on multiple transport streams to achieve a differentiated error protection for different services (TV, HDTV, audio, multimedia). Two modes are available:
   - Non backwards compatible broadcast services (NBC-BS) is not backwards-compatible to DVB-S.
   - Backwards-compatible broadcast services (BC-BS) is backwards compatible to the previous version.

b) Interactive services (IS) Interactive data services including Internet access – DVB-S.2 is intended to provide interactive services to consumer IRDs and to personal computers, where DVB-S.2's forward path supersedes the current DVB-S for interactive systems. The return path can be implemented using various DVB interactive systems, such as DVB-RCS. Data services are transported in (single or multiple) Transport Stream format or in (single or multiple) generic stream format. DVB-S.2 can provide constant coding and modulation (CCM) or ACM, where each individual satellite receiving station controls the protection mode of the traffic addressed to it.
c) Digital TV contribution and satellite news gathering (DTVC/DSNG) – Digital television contribution applications by satellite consist of point-to-point or point-to-multipoint transmissions, connecting fixed or transportable uplink and receiving stations. The general public does not intend them for reception. According to international telecommunications union – Radio communications) (ITU-R) recommendation SNG.770-1, satellite news gathering (SNG) is defined as "Temporary and occasional transmission with short notice of television or sound for broadcasting purposes, using highly portable or transportable uplink earth stations". Services are transported in single (or multiple) MPEG Transport Stream format. DVB-S.2 can provide CCM or ACM. In this latter case, a single satellite receiving station typically controls the protection mode of the full multiplex.
d) Data content distribution/trunking and other professional applications– These services are mainly point-to-point or point-to-multipoint, including interactive services to professional head-ends, which re-distribute services over other media. Services may be transported in (single or multiple) generic stream format. The system can provide CCM, VCM or ACM. In this latter case, a single satellite receiving station typically controls the protection mode of the full TDM multiplex, or multiple receiving stations control the protection mode of the traffic addressed to each one. DVB-S.2 is suited for use with a range of satellite transponder bandwidths and frequency bands. The symbol rate is matched to given transponder characteristics, and, in the case of multiple carriers per transponder (frequency division multiplexing (FDM)), to the frequency plan adopted. Digital transmissions via satellite are affected by power and bandwidth limitations. Therefore DVB-S.2 provides for many transmission modes (FEC coding and modulations), giving different trade-offs between power and spectrum efficiency.

DVB-S.2 is compatible with moving pictures experts group (MPEG-2 and MPEG-4) coded TV services (see [WOO97]), with a Transport Stream packet multiplex. Multiplex flexibility allows the use of the transmission capacity for a variety of TV service configurations, including sound and data services. All service components are time division multiplexed (TDM) on a single digital carrier.

While DVB-S and DVB-DSNG are strictly focused on a unique data format, which is the MPEG transport stream, DVB-S.2 utilizes extended flexibility to cope with other input data formats (such as multiple transport streams or generic data formats without significant complexity increase. It improves

on and expands the range of possible applications, by combining the functionality of DVB-S (for direct-to-home applications), and DVB-DSNG (for professional applications), and techniques such as adapting coding to maximize the usage of the satellite transponder resources.

2.3.2 Modulation schemes and coding rates

The system adopts four "wheel" (Figure 7) modulation formats, all optimised to operate on non-linear transponders:

a) Quadrature phase shift keying (QPSK) (2 bit/s/Hz)

b) 8QPSK (3 bit/s/Hz)

c) 16APSK (4 bit/sHz) 4-12 APSK

d) 32APSK (5 bit/s/Hz) 4-12-16 APSK

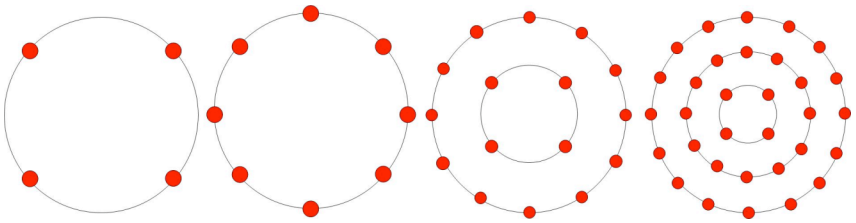


Figure 7: The 4 "wheel" Modulation Format

The FEC encoding is based on the concatenation of low density parity check codes (LDPC) and bose-chaudhuri-hocquenghem (BCH) codes. The LDPC codes are a particular class of convolutional codes; they have been discovered by Gallager in 1960 [GAL62], but only today the improvement in chip technology allows high-speed implementation of sophisticated decoding algorithms in consumer products. They allow quasi-error free operation at only 0.6–1.2 dB from the Shannon limit [ERO04].

The encoding is performed in three sequential stages:

1. The parity check bits BCH_{FEC} of BCH outer code is appended to the base block frame (BBFRAME), which is the payload of DVB-S.2.
2. The parity check bits $LDPC_{FEC}$ of LDPC inner code are appended to the BCH_{FEC} field.
3. The LDPC encoder output is interleaved by using a simple block interleaver, presented in Figure 8, where the interleaving depth is function of the adopted modulation format.

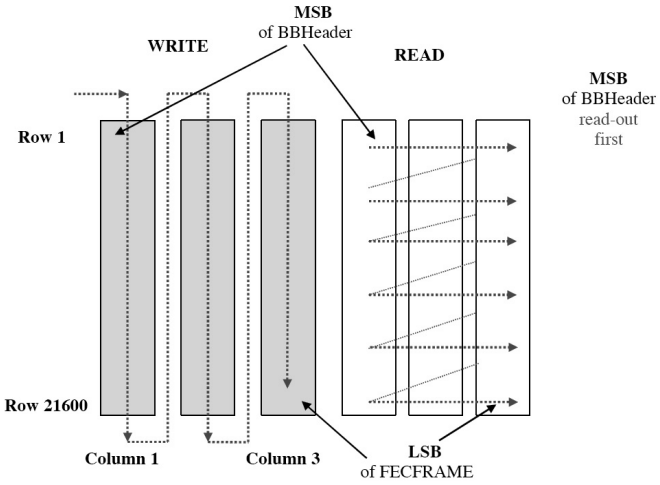


Figure 8: DVB-S.2 Bit-interleaving Technique

The interleaving is only used with the modulation schemes presented in Table I.

Modulation	Number of Columns	Size of each column
8-PSK	3	21600
16-APSK	4	16200
32 APSK	5	12960

Table 1: Bit Interleaver Structure

Many coding rates are available according to the DVB-S.2 standard: 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9, 9/10. The result is 30% efficiency greater than DVB-S. Coding rates 1/4, 1/3 and 2/5 have been introduced to operate, in combination with QPSK, under exceptionally poor link conditions, where the signal level is below the noise level. The introduction of two FEC code block lengths (64 800 and 16 200) was dictated by two opposite needs: the carrier-to-noise (C/N) performance improves for long block lengths, but the end-to-end modem latency increases as well. Therefore, for applications not delay-critical (such as, for example, broadcasting) long frames are the best solution, while for interactive applications a shorter frame may be more suitable when a short information packet has to be immediately forwarded by the transmitting station. The performance of DVB-S.2 modulation and coding schemes can be found in [CAS04, ALB04].

In comparison to DVB-S.2, the DVB-S and DVB-DSNG soft-decision Viterbi decoder takes decisions on blocks of only 100 symbols, without iterations, and the Reed-Solomon code over blocks of about 1600 bits (interleaving factor 12), offering performance around 3 dB from the Shannon limit.

2.3.3 ACM and IP Encapsulation

ACM has been considered as a powerful technique to further increase system capacity, allowing for better utilization of transponder resources, and hence providing additional gain with respect to current DVB-S systems. Therefore, in DVB-S.2 ACM is included as normative for the interactive application area and as optional for DSNG and professional services.

The standard recognises that IP traffic is driving the design of interactive services in broadband

systems. The new DVB-S.2 standard seeks to improve IP performance (and flexibility). It not only provides a mode that supports IP over the MPEG-2 Transport Stream, which is widely used in existing deployed networks (e.g. DVB-S, DVB-RCS) [ETS04] [MON05], but also an alternative mode, called the Generic Mode. In the Generic Mode IP packets may be placed in physical bearer frames, without incurring the overhead of the MPEG-2 TS.

The protocol stack for the DVB-S.2 supporting the MPEG-2 TS mode is shown in Figure 9. In this figure, the BBFRAME (carrying one or more encapsulated packets) is padded, and encoded to form a FECFRAME.

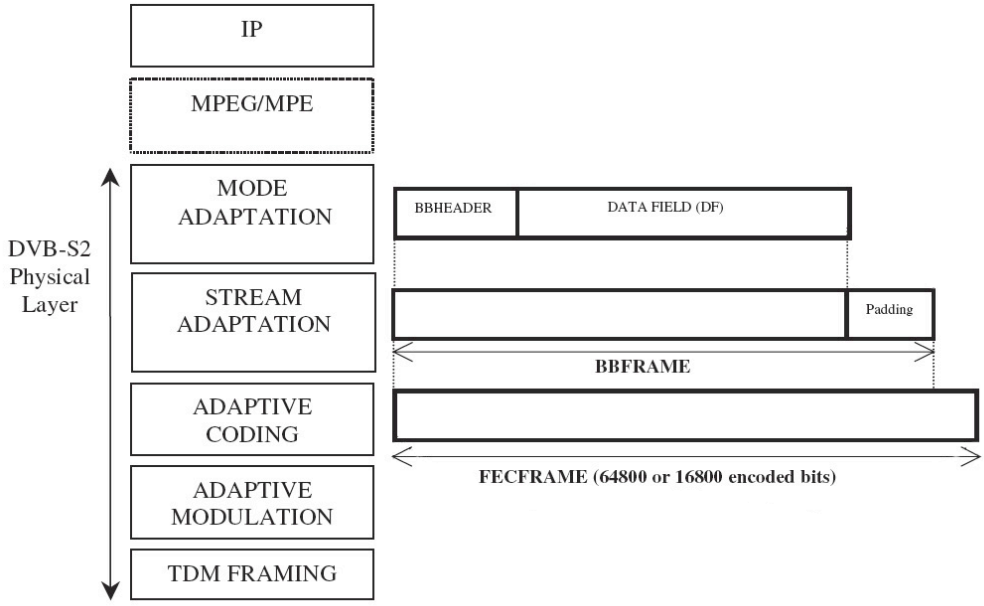


Figure 9: The DVB-S2 Capsule

The current standard for encapsulation of IP packets over MPEG-2 networks is the Multi-Protocol Encapsulation, MPE [ETS04]. An alternative encapsulation was recently developed within the IETF [FAI05]. The methods allow variable sized IP packets to be fragmented into a series of fixed-sized transport stream packets. Since IP packets do not generally have a size that matches an integer number of TS packets, the last TS packet in the sequence will not normally be full. The unused portion of the TS packet may be filled with padding bytes (the default in MPE), or to start the next in-sequence encapsulated packet [MON05].

When the IP packet length is significantly shorter than the TS packet length (188 bytes) the encapsulation efficiency is low, and this is even more evident when concatenation of packets is not allowed (i.e. only one IP packet per TS packet). In [RIN04] and [VAZ04] the encapsulation efficiency has been studied, assuming different percentage of payload occupancy; the numerical results are shown in Table 2.

	IP directly				MPE with concatenation				MPE without concatenation			
	Full	80%	50%	20%	Full	80%	50%	20%	Full	80%	50%	20%
Normal FECFRAME	0.97	0.78	0.48	0.19	0.88	0.71	0.44	0.18	0.78	0.62	0.39	0.16

64800 bits												
Short												
FECFRAME	0.96	0.77	0.48	0.19	0.87	0.70	0.44	0.18	0.77	0.61	0.38	0.15
16800 bits												

Table 2: Total DVB-S.2 encapsulation efficiency as a function of percentages of payload occupancy

One of the implications of such a high flexibility is the multiplicity of solutions allowed in DVB-S.2 for implementing ACM in interactive systems. DVB-S.2 specifications need to be taken into account together with system performance requirements in designing system architecture and upper layer functionalities (scheduling, resource allocation). However, when ACM is implemented, coding scheme and modulation format may change frame-by-frame.

The DVB-S.2 ACM modulator operates at constant symbol rate, since the downlink carrier bandwidth is assumed constant. Unlike DVB-S, the second generation of the standard allows for several input stream formats, thus enhancing system flexibility. In addition to the widely used MPEG-TS, generic streams, of constant or variable length packets, are encompassed by the standard. When this second configuration is selected, TS rules do not apply. Moreover, different encapsulation protocols with improved efficiency can be used as an alternative to the multi protocol encapsulation [CAS04]. IP datagrams can also be directly mapped on the transmission frame. The data stream packets of both MPEG-TS and generic streams are called user packets (UPs).

To be fully compliant with the MPEG-2 specification for a TS, the TS mode of the DVB-S.2 standard must deliver a constant rate transport stream with an invariant end-to-end delay. The first problem was that a transport stream is characterised by constant bit-rate, while ACM is by definition a variable bit-rate transmission, trading-off user bit-rate with FEC redundancy during rain fades. DVB-S.2 allows the Null TS Packets (which carry no useful information) in the MPEG-2 TS to be removed at the input interface and re-introduced at the output of the receiver, preserving the end-to-end timing of the MPEG-2 TS. In order to map one/many constant bit-rate transport-stream(s) into a variable bit-rate ACM physical layer, the DVB-S.2 modulator activates the subsystem called ‘null-packet deletion’. The second problem was that, during the rate adaptation, delay and rate variations may take place in the modem. This is taken into account by the ‘input stream synchronizer’ block which operates a suitable compensation.

The input interface accepts both single and multiple streams. One additional input signal available in the standard is the ‘ACM command’. This is utilised in ACM systems in conjunction with a single input stream. It allows an external control unit to set the transmission parameters to be adopted by the DVB-S.2 modulator for a specific portion of input data. The utilisation of the ACM command interface allows for a system configuration, which is completely transparent to the physical layer scheme selection. This functionality is indeed performed by a unit external to the DVB-S.2 modulator, which signals through the ACM command the transmission parameters associated to the data packets.

The standard includes several possible configurations for implementing ACM in unicast systems. In particular, the following two DVB-S.2 modulator input interfaces allow for ACM operation:

- a single generic data stream and the ACM command;
- multiple (transport or generic) data streams.

The choice between the different options has a significant impact on the definition of the system architecture (intended as data processing, routing, buffering and transmission strategy) and consequently on the overall system performance.

The input streams are buffered, thus allowing a merger/slicer to read frame by frame the information necessary to fill the data field. As data field we indicate the set of information bits, which, after undergoing FEC encoding, mapping, framing and modulation, are finally transmitted in one physical layer frame (PLFRAME). In the case of a single stream, only the slicing functionality is required, while, when multiple streams are present, the merger/slicer is responsible for composing each data field by reading information bits from one of the input buffers. For unicast systems with multiple input streams the standard considers the possibility of performing a round-robin polling with a time-out for the user packets in each buffer. However, additional different policies can be implemented.

Single generic stream and ACM command. For each frame the merger selects a number of packets from the input queues, and combines them for building a set of information bits. Successive data sets, composed frame by frame, are sent to the ACM modulator, together with the associated transmission parameters. When the number of bits in one set is not sufficient to completely fill the BBFRAME, the modulator provides padding by automatically choosing the most suitable type of FECFRAME, with short or normal length.

An ACM Routing Manager drives the merger selection, which is responsible for packet scheduling. The scheduling policy is application dependent and needs to be designed for maximizing the system efficiency while meeting QoS requirements. To achieve these goals, the ACM Routing Manager can take advantage of the channel status information reported by the Satellite Terminals, of the different priority levels and QoS requirements of the input queues, and finally of the information concerning the buffer occupation. The first type of information is needed to combine in one frame packets with the same transmission parameters; the second one allows for meeting QoS requirements (maximum delay, minimum rate, etc.); the third one can be used, for example, for satisfying QoS requirements without sacrificing in presence of scarce traffic associated to a certain physical layer mode.

Multiple (generic or transport) streams. According to the system configuration, the DVB-S.2 modulator interfaces with a number of input data streams. The ACM router splits the users' packets per required protection level, and sends them to the multiple DVB-S.2 input interfaces, each stream being permanently associated to a given protection level buffer. Therefore, each input stream merges the traffic of all the users who need a specific protection level, and its bit-rate may (slowly) change in time according to the traffic characteristics. In the first configuration the Merger was external to the DVB-S.2 modulator, and the ACM Routing Manager was responsible for the packets merging inside the scheduler. In this configuration, the Merger is integrated into the DVB-S.2 Modulator and multiplexes the TS packets among the buffers with a round-robin merging policy. The 'null-packet deletion' is now applied to each branch of the protection level buffers, and it may reduce the transmitted bit-rate. In the system architecture case here presented, the buffer organization is definitely less complex than the one described previously. However, simple first in first out (FIFO) queues, where UPs are aggregated without any differentiation can present some performance limitations when adaptive systems are considered, as described in the 'Scheduling issues' of [RIN04].

3 BROADBAND INTERNET AND MOBILE COMMUNICATIONS

3.1 Internet Protocol

The IP protocol is a connectionless network layer protocol that is designed for addressing and forwarding of IP packets (also known as IP datagram). The Internet is made up of routers that are responsible for the routing and forwarding of the IP packets to the designated host. If the final destination of the packet is not within the host's network, the packet will then be forwarded through the Internet (which could be through different wireless or wired technologies) until it reaches its

designated host. However, the path or route that the packet travels from the host to the designated host is determined by the routing algorithm used, such as routing information protocol (RIP) or open shortest path first (OSPF), and is elaborated in [FOR03]. The two basic versions of IP protocols (i.e. IPv4 and IPv6), which has been standardised by the IETF, will be briefly described below.

IPv4

In IPv4, an IP address is 32- bits long; hence, a total of 232 possible addresses can be assigned. Every hosts or routers that are connected to the Internet are assigned at least one IP address, which is necessary for the forwarding and routing of IP packets. In the IPv4 header, the Source Address is the host's source address and Destination Address is the designated host address, both of which remains unchanged throughout the transmission of the packet from the source host to the designated host. Further detailed descriptions of these different fields, IP addressing and routing are elaborated in [POS81a], [FOR03] and [KUR05].

IPv6

The exponential growth of the Internet is causing a strain on the current IPv4 protocol to provide sufficient addresses to support user demand. Thus, the main reasons for the development of the IPv6 protocol are to alleviate this issue and to benefit future peer-to-peer applications and mobile networking.

IPv6 has addressed several limitation of IPv4 and some of the advantages of IPv6 are it has a larger address space (i.e. an IPv6 address is 128-bits long), consist of a better header format (so as to simplify and speed up the routing process), support for resource allocation (to enable better QoS support that can be used for transmission of real-time audio and video traffic) and better security support [FOR03]. With IPv6, a total of 296 possible addresses can be assigned and with this expanded addressing capability, it can be ensured that the amount of IP addresses will not run out anytime soon. However, to support the IPv6 protocol, several protocols that are now inter-working with IPv4 were required to be updated, such as internet control message protocol (ICMP), domain name system (DNS), and are being addressed currently by the IETF IPv6 workgroup. In addition, to allow more functionality in IPv6, six extension headers (i.e. Hop-by-Hop Option, Source Routing, Fragmentation, Authentication, encrypted security payload (ESP) and Destination Option) were introduced and are elaborated in [FOR03]. Several of these additional headers previously existed in the IPv4 header. Further detailed description is available in [FOR03].

IP has become widely deployed these days, as the number of Internet users increased, that it has become increasing important to consider supporting IP for future technologies. For instance, the transmission of IP packets through DVB satellite systems (e.g. DVB-S, DVB-RCS), which uses the MPEG-2 transport stream for data transmission. MPE is currently widely used for the encapsulation of IP packets for transmission over MPEG-2 transport stream [ETS04]. Another encapsulation method called ULE, which utilises lesser satellite bandwidth than MPE, is recently introduced by the IETF ipdvb workgroup [FAI05]. Most current and planned satellite systems already support IPv4 and many activities continue to develop and standardise the associated networking aspects [SAT05, BSM05, ETS05]. However, IPv6 introduces additional features, such as stateless auto configuration, address resolution, duplicate address detection (DAD), router and prefix discovery, which require bi-directional links. Most satellite networks uses only uni-directional links and mainly consists of utilising a DVB-S forward link and DVB-RCS return link or additionally integrating with terrestrial networks. [ESA04] states that currently neither MPE nor ULE has discussed how to provide dynamic address resolution between IPv6 address, MAC address and PID value. Therefore, to support the full capability of IPv6 for DVB satellite systems (i.e. DVB-S, DVB-RCS) several factors are still required to be resolved and

this remains as an issue to be addressed for future development.

In the meantime, there has been considerable research and development in the terrestrial telecommunications world devoted to preparing for the transition from IPv4 to IPv6 networks. In addition, systems such as 3G are basing their design on support for IPv6. Although the European commission (EC) has a cluster of more than 30 projects relating to the design and operation of IPv6 networks (www.ist-ipv6.org), much of the work has focused on terrestrial radio access networks and the topic of engineering the deployment of next generation infrastructure, and only a few have considered IPv6 within satellite systems. Two notable research initiatives were: A north Atlantic treaty organisation (NATO) education programme project, SILK, that pioneered the use of IPv6 over DVB-S utilising the ULE specification [FAI05]; and SATIP6 (an EC fifth framework programme (FP5) project) that assessed the issues in deployment of IPv6 over DVB-RCS. IPv6 is planned as a work item of the ETSI BSM (broadband satellite multimedia) WG [BSM05], which will include support for IPv6 protocols using the satellite independent network interface [ETS05].

3.2 IP Migration Strategies

The deployment of an "all new IPv6" infrastructure is an arduous task due to factors such as the cost, scalability and time. Therefore, it has been widely accepted that IPv6 will be introduced to the existing IPv4 infrastructure, i.e. inclusive of DVB satellite systems, and to enable seamless introduction, migration strategies will be adopted. In this way, it will minimise any impact on existing network users [MAC03]. The MPE protocol, which is currently widely used for DVB satellite systems, can be used for both IPv4 and IPv6. However, the standard does not mention how the receiver is notified of which IP version is encapsulated [ESA04] [MON05]. ULE supports a range of network layer packet formats, including native IPv6 and IPv6/MPLS [FAI05]. IP migration strategies consist of three main transition mechanisms: Dual Stack, IPv6 tunnelling mechanisms and IPv6 translation mechanisms, and are discussed below. It is important that DVB satellite systems take into consideration these IP migration strategies, as currently most research development are devoted in studying IPv6 for DVB satellite systems even though the co-existence of both IPv4 and IPv6 for satellite system still remains an area to be addressed.

Dual Stack

An "IPv4-IPv6 node" (e.g. the operating system of a host, router) is equipped with both sets of the protocol stacks (although in practice, the stacks share many elements) and this allows the node to send/receive both IPv4 and IPv6 packets [GIL00, NOR05]. This implies that IPv4 and IPv6 islands can send and receive IP packets with the aid of a router that supports both IP protocols (i.e. the Dual Stack Router and Dual Stack Edge Router). The advantage of dual stack mechanisms is that the IPv4 and IPv6 share the same network - this implies that there is no need to design new routers specifically for IPv6. For further information regarding Dual Stack, refer to [MAC03] and [GIL00, NOR05].

IPv6 Tunnelling Mechanisms

Tunnelling mechanisms for channelling IPv6 packets over IPv4 networks can be configured either manually or automatically. The tunnelling can be either encapsulation of IPv6 packets in IPv4 packets or vice versa. There are several tunnelling methods available, as listed below:

- Configured Tunnel

  This type of tunnel, which can be bi-directional or uni-directional, is most suitable when supporting external IPv6 connectivity to a whole network. It is stated in [GIL00, NOR05] as

IPv6-over-IPv4 tunnelling, whereby the IPv4 tunnel endpoint address is determined by configuration information on the encapsulating node.

- Tunnel Broker

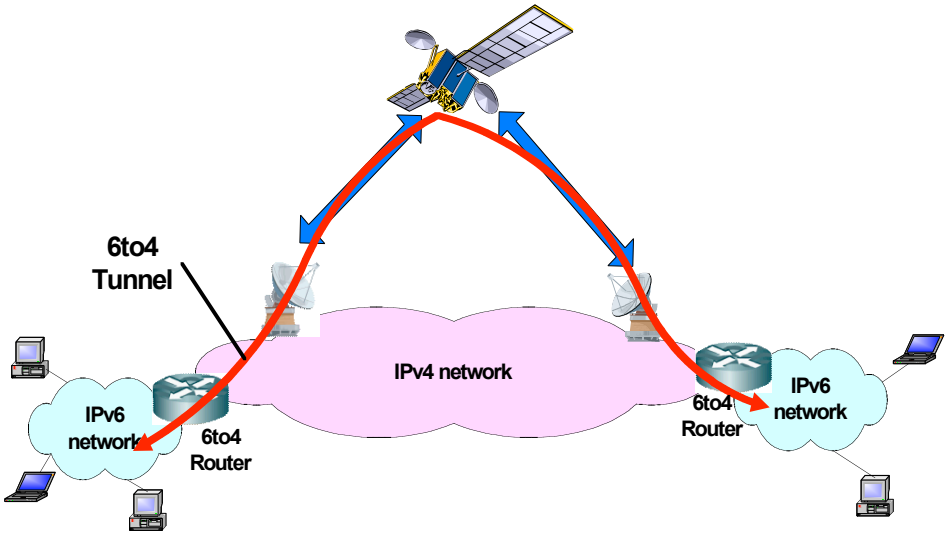
  Tunnel broker is appropriate for small isolated IPv6 islands and isolated IPv6 users in an IPv4 network that wish to establish connectivity to an IPv6 network. The function of the tunnel broker is to automatically manage IPv6 tunnels and to tunnel requests from isolated IPv6 sites on behalf of one or more dedicated servers [DUR01].

- 6to4

  This method is suitable for isolated IPv6 islands to communicate via the IPv4 network without using explicit tunnels. It treats the IPv4 network as a unicast point-to-point link layer, specifying an encapsulation mechanism for transmitting IPv6 packets over the Internet by assigning a unique IPv6 address prefix to any site with at least one globally unique IPv4 address [MAC03]. This method is not intended as a permanent solution, but as a start-up transition tool during the co-existence of IPv4 and IPv6 [CAR01]. An example diagram is depicted in Figure 10 and a detailed description of this method is provided in [CAR01].

- Intrasite automatic tunnel addressing protocol (ISATAP)

  Due to the insufficient support for IPv4 multicasting in ISP networks, this method is proposed as an alternative option to 6over4[1]. ISATAP is designed to connect isolated IPv6 hosts and routers (nodes) within an IPv4 site [TEM04]. Furthermore, it employs the site's IPv4 infrastructure as a virtual link, but it does not use IPv4 multicast, therefore the link is non-broadcast multiple access (NBMA). This method is capable of enabling automatic tunnelling, irrespective of whether global or private IPv4 addresses are used.



[1] 6over4 is another tunnelling method that allows isolated IPv6 hosts, located on a physical link, which has no directly connected IPv6 router, to become fully functional IPv6 hosts by using an IPv4 domain that supports IPv4 multicast as their virtual link [Car01a]. However, it is not widely adopted and will not be further elaborated.

Figure 10: Migration of IPv4 to IPv6 – 6to4 tunnelling

Further information on other tunnelling mechanisms, such as Teredo, dual stack transition mechanism (DSTM), Tunnel Setup Protocol, OpenVPN-based tunnelling solution, IPv6 over ATM and MPLS, can be found at [HUI04], [BOU04], [DUR01], [IST04] and [MAC03] respectively.

IPv6 Translation Mechanisms

It is necessary to use translation mechanisms to allow an IPv6-only node to communicate with an IPv4-only node. The following lists some translation methods:

- Stateless IP/internet control message protocol translation (SIIT)

  SIIT specifies a key translation algorithm for enabling interoperation between IPv6-only and IPv4-only hosts [NOR00]. An IP datagram travels through the SIIT translator, and it converts the datagram headers between IPv4 and IPv6, with the aid of temporary assigned IPv4 addresses.

- Network address translation-protocol translation (NAT-PT)/ network address port translation + packet translation (NAPT-PT)

  NAT-PT, defined in [TSI00], is based on the common IPv4 network address translation (NAT) concept. It can be used to translate IP packets sent between IP-heterogeneous networks, by binding the addresses in the IPv6 networks and vice versa to transparently route the IP packets traversing different realms. NAPT-PT extends the concept of NAT-PT by also translating transport identifier (such as transmission control protocol (TCP)/user datagram protocol (UDP) port numbers, ICMP query identifiers).

- Bump in the stack (BIS)/bump in the API (BIA)

  BIS is an extreme extension of NAT-PT, in which a pool of IPv4 addresses is dynamically allocated to hosts. BIS adopts a unique translation approach, by moving the translation inside the individual hosts rather than performing the translation at a centralised server. The host is capable of translating between IPv4 and IPv6 internally by including the necessary segments in its IP stack [TSU00]. The BIA translation mechanism is similar to BIS. However, it does not translate the IP headers, on the contrary, BIA inserts an API translator between the host's stack TCP/IP modules [LEE02]. This allows the translation to be performed without the overhead of translating every packet's header [MAC03].

Further information on other translation mechanisms, such as transport relay translator (TRT), SOCKS 64, is available in [HAG01] and [KIT01].

3.3 Mobile IP

The extensive usage of the Internet has led to the development of extending Internet access to consumers via different access technologies and it has also been widely acknowledged that with the aid of mobile IP (MIP), consumers are able to roam seamlessly between non-homogeneous networks. Therefore, MIP (i.e. MIPv4 and MIPv6) will play an important role in the research and development of future mobile communications, as it progresses towards achieving a heterogeneous network. MIP can mainly be categorised into: Moving networks (i.e. Mobile Networks) and users' "on the move" (i.e. User Mobility), as illustrated in Figure 11.

User mobility implies that end-users are able to seamlessly roam between different networks or

terminals while maintaining their current Internet connection. Mobile IP has been widely accepted as the de-facto standard for supporting mobility and has been addressed in [LIA03] and [CON02]. In addition, much research is also focused on providing broadcast Internet and multimedia services to mobile users with the aid of Mobile IP and DVB techniques, such as DVB-S, DVB-RCS, DVB, DVB-T and DVB handheld (DVB-H), and detailed information is available in [IST04A] and [CAR04].

On the other hand, a mobile network, as stated in [MAN04], is an entire mobile network that dynamically changes its point of attachment to the Internet. It can be made up of a single IP subnet or consist of several IP subnets. The main architectural components involved are Mobile Routers and Mobile Nodes, which are further elaborated in [MAN04]. Much research has also been devoted to providing users with Internet access in a vehicular environment, such as in [LIA03] and [CON02]. Several research developments have been focused on supporting IP mobility for mobile networks, which utilises DVB-S and DVB-RCS. One possible issue of implementing Mobile IP in a regenerative DVB satellite system (such as DVB-S, DVB-RCS) occurs whenever the mobile node (MN) changes it point of attachment (POA), particularly when binding updates are sent to updated correspondent nodes (CNs) and the Home Agent. Satellite resources are limited and expensive, hence, it will be beneficial to maintain the change of care-of address (CoA) minimum, so as not to waste satellite resources and retain service connectivity. One way is to allow Mobile IP to support macro-mobility and implement micro-mobility protocols (such as HMIP, TeleMIP) to reduce the binding update traffic. Micro-mobility protocols for MIPv6 are discussed in Section 3.3.2.1 and for detailed information of micro-mobility protocols for MIPv4 are available in [REI03] and [CAM00]. Nevertheless, basic concepts of MIP (i.e. MIPv4 and MIPv6) will be briefly discussed in Section 3.3.1 and 3.3.2.

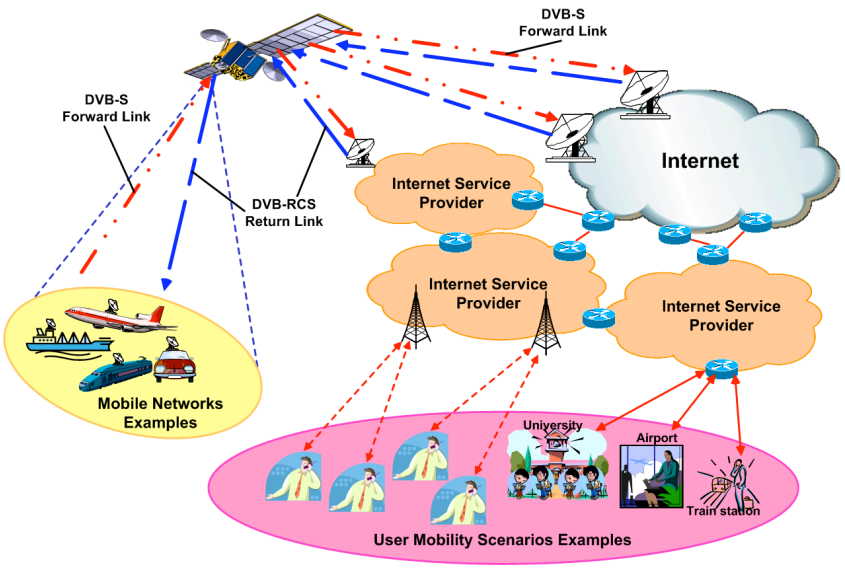


Figure 11: Example of Mobile IP Implementation Scenarios

3.3.1 Mobile IP version 4 (MIPv4)

In MIPv4, there are three main architectural components, i.e. home agent (HA), foreign agent (FA) and mobile node. Illustrated in Figure 12, is a simple overview of the MIPv4 concept and detailed explanations are addressed in [PER02a]. When a MN joins a foreign network (also known as visited network), it is assigned a CoA and updates HA about it POA. When HA intercepts the packets that are destined to MN, it will encapsulate it in a datagram and forward it to the FA. The FA upon receiving it will extract the original datagram and forward it to the MN. However, the packets that are sent by MN are routed directly to CN. Therefore, from the point of view of the CN, the IP address that it knows of

MN still remains the same and this method of tunnelling and forwarding is widely known as triangular routing. Furthermore, with the introduction of the MIP concept, several proposals focusing on improving the MIP protocol, such as implementing micro-mobility protocols for MIPv4, are addressed in the IETF mobility for IPv4 (MIP4) workgroup. For further information of micro-mobility protocols for MIPv4 can be found in [REI03], [CAM00] and [SAH04].

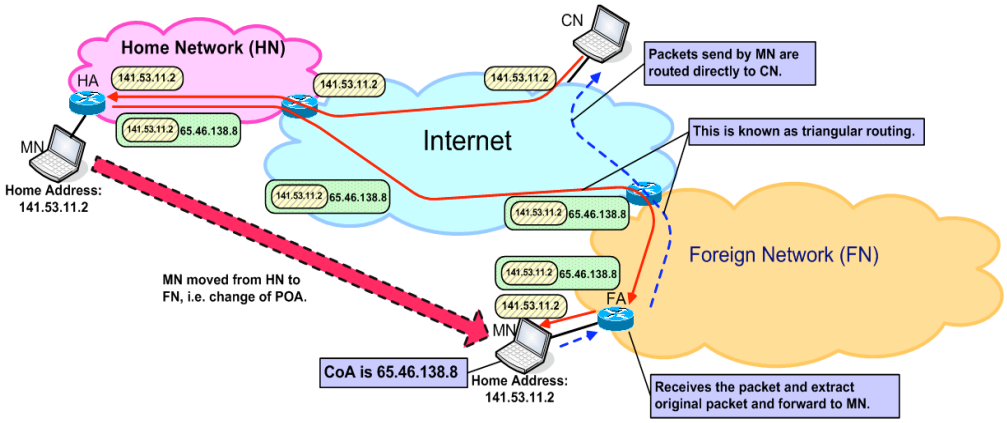


Figure 12: MIPv4 example

3.3.2 Mobile IP version 6 (MIPv6)

[JOH04] addresses the issue of supporting IP mobility in IPv6 networks and is known as mobile IPv6 (MIPv6). Basically, it mainly consists of the same architectural components as MIPv4, except that due to the improvements addressed in IPv6 addresses, such as larger address space, it is not necessary to have a FA. In MIPv6, the MN can be assigned a CoA by conventional IP mechanisms, such as stateless and stateful auto-configuration [JOH04]. In addition, the triangular routing in MIPv4 has several disadvantages. For example, forwarding of IP packets from CN to HA first, increases the load on the network, which will then cause longer delays for the delivery of the IP packets. Therefore, in MIPv6, route optimisation is a fundamental part (however, it is optional for MIPv4) and allows MN and CN to directly forward packets to each other. This concept further introduces two concepts, Binding[2] Cache and Binding Update. Further details are available in [JOH04] and [NIK05]. An example of MIPv6 is depicted in Figure 13 and the review of MIPv6 proposals will be discussed next.

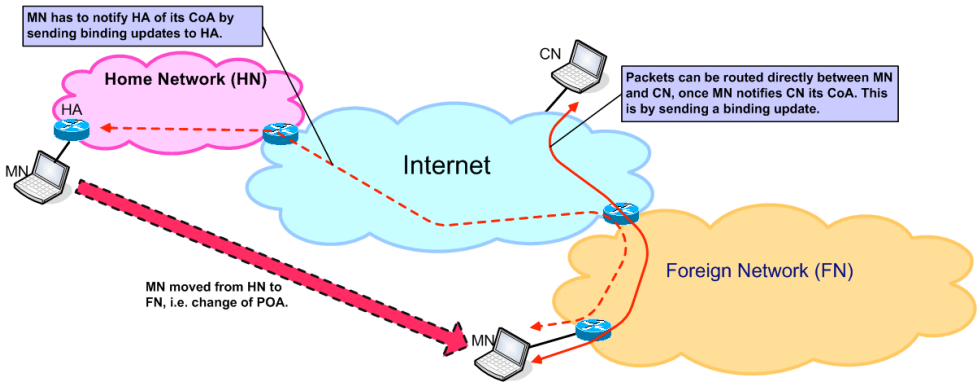


Figure 13: MIPv6 example

[2] The term binding implies the association of the MN's home address with its CoA

3.3.2.1 Review of Mobile IP Proposals for IPv6

There has been universal recognition that MIP will be implemented in the next generation of mobile communications to provide mobility support to users. However, when Mobile IP was designed, all-IP wireless networks were not envisioned and some of the mechanisms used by Mobile IP are not well suited for such networks [REI03]. This is because it is anticipated that the next generation of mobile networks will be required to support Real-Time services, such as voice over IP (VoIP), to consumers. However, in mobile environments, mobile devices (i.e. Mobile Node) frequently change their POAs to the network. This increases the network overheads (such as delays, packet losses and signalling) as the MN is required to send binding updates (BUs) to its HA and all CNs whenever it changes its POA. Thus, the increment of network overheads poses as an issue when supporting Real-Time services, especially when handover is being performed across heterogeneous networks. Therefore, much research and development has been focused on optimising the handover performance by implementing localised mobility management (LMM) protocols [WIL05], also known commonly as Micro-mobility Protocols. The LMM protocols should fulfil the following factors:

- Reduce the network overheads due to signalling when a change of POA occurs. The reduction in signalling delay will minimise the packet losses and possible session loss. It will also reduce the usage of the physical interface and network resources and improve protocol scalability.
- Avoid or minimise the changes of, or impact to the MN, HA or the CN.
- Avoid creating single points of failure.
- Simplify the network design and provisioning for enabling LMM capability in a network.
- Allow progressive LMM deployment capabilities.
- No new security vulnerabilities should be introduced.

Currently, several micro-mobility proposals (such as hierarchical mobile IPv6 (HMIPv6), fast handovers for mobile IPv6 (FMIPv6), telecommunications-enhanced mobile IP (TeleMIP), cellular IPv6), to support IPv6 mobility (i.e. Mobile IPv6) are addressed in the IETF workgroups and a common few will be briefly discussed in the following.

Hierarchical Mobile IPv6 (HMIPv6)

The HIMPv6 concept was designed to be an extension of the MIPv6 Protocol and has generated wide interest as the preferred solution for IP micro-mobility in all-IP wireless networks. It introduces a new node called mobility anchor point (MAP), which is a local anchor point that can be located at any level in a hierarchical network of routers including the access router (AR) [SOL05]. It aids MIPv6 by reducing the mobility signalling with external networks. The MN acquires two addresses when it enters a foreign network, i.e. regional care-of address (RCoA) and on-link care-of-address (LCoA). The MAP acts as a local HA and is responsible for receiving and tunnelling the packets to the MN. The MN is only required to change its local address (i.e. LCoA) when moving within the MAP's sub-network; the global address (i.e. RCoA) remains unchanged [CAM00]. When the MN moves into another MAP's subnet, there is a change in the RCoA, hence the MN is required to forward BUs to its HA and CNs. The HMIPv6 concept allows load balancing and robustness. However, if the MAP fails, the binding cache contents will be lost, as will communication between the MN and CNs. This issue would affect Real-Time services that are expected to be supported in future mobile communications. [SOL05] proposed the implementation of more than one MAP on the same link and implementing some form of context transfer protocol between the MAPs or the use of future versions of the Virtual Router Redundancy Protocol [KOO04]. However, these are still in the early stages of development and this area remains as an open issue to be addressed. An example of HMIPv6 is illustrated in Figure 14. Further information on HMIPv6 is provided in [SOL05], [CAM00] and [CAS00].

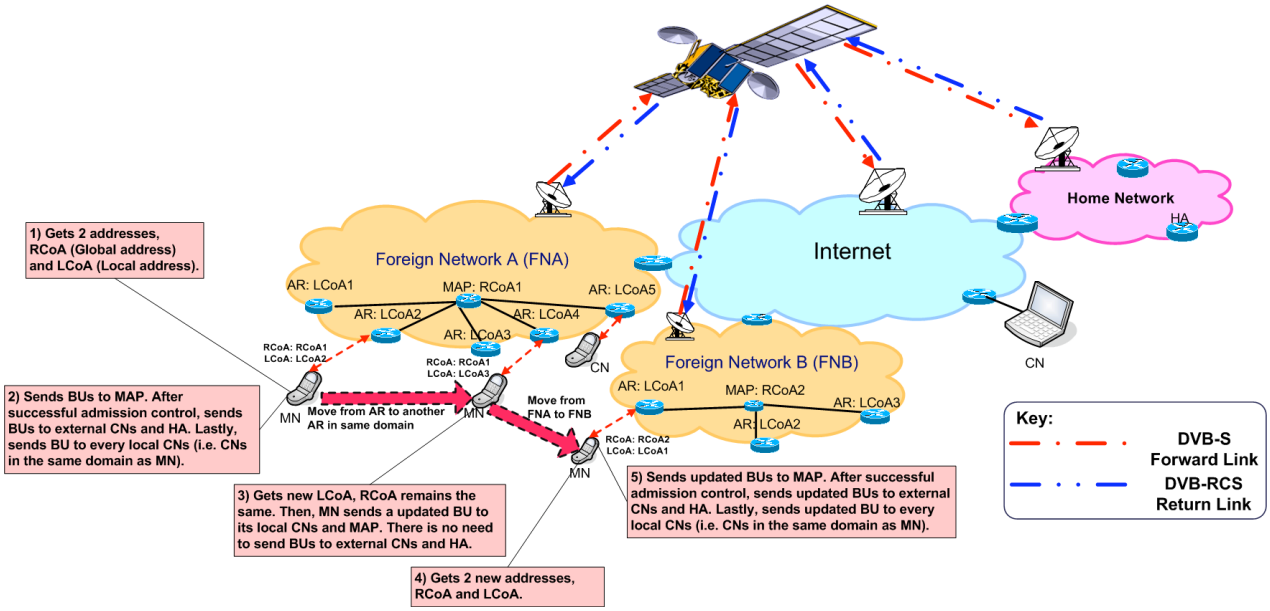


Figure 14: Hierarchical Mobile IPv6 (HMIPv6) Example

Fast Handover for Mobile IPv6 (FMIPv6)

Whenever a MN changes its POA in MIPv6, there is a period when the MN is not able to transmit and receive packets because of the link switching delay and IP operations. This handover latency is due to the MIPv6 procedures, such as movement detection, new CoA configuration and BU, and is often unacceptable to real-time traffic such as VoIP [KOO04]. Therefore, the FMIPv6 protocol aims to reduce this handover latency. The FMIPv6 protocol specifies the IP messages required for the implementation of this operation irrespective of the link layer technology. However, the implementation of FMIPv6 in 802.11 WiFi technologies is presented in [MCC05].

In FMIPv6, router solicitation for proxy advertisement (RtSolPr) and proxy router advertisement (PrRtAdv) messages are used for detecting the MN's movement. Based on these two messages, the MN is able to contrive a new CoA (NCoA), while connected to the previous access router (PAR)[3]. The MN then sends a fast binding update[4] (FBU) message to the PAR, to allow the PAR to bind the previous CoA (PCoA) to NCoA, so that packets for the MN can be tunnelled to the new access router (NAR). An example is illustrated in Figure 15. In [KOO04], two scenarios were depicted. The first is known as Predictive Fast Handover, whereby the MN sends a FBU message and receives the FBACK fast binding acknowledgment (FBACK) message on the PAR's link. The second is called Reactive Fast Handover; this is when the FBU and FBACK messages are sent and received through the NAR's

[3] The term Previous Access Router (PAR) implies the current Access Router that MN is connected to prior to handover.

[4] The MN sends a FBU message to instruct PAR to redirect packets to NAR. The NCoA derived by MN is included in FBU.

link. In this scenario, the FBU message is encapsulated in the fast neighbour message[5] (FNA) because this allows the NAR to discard the FBU packet if a conflict in address is detected. Further information on FMIPv6 is provided in [KOO04]. Studies on the performance of FMIPv6, HMIPv6 and the combination of implementing FMIPv6 and HMIPV6 are discussed in [HSI02], [PER02] and [PER03].

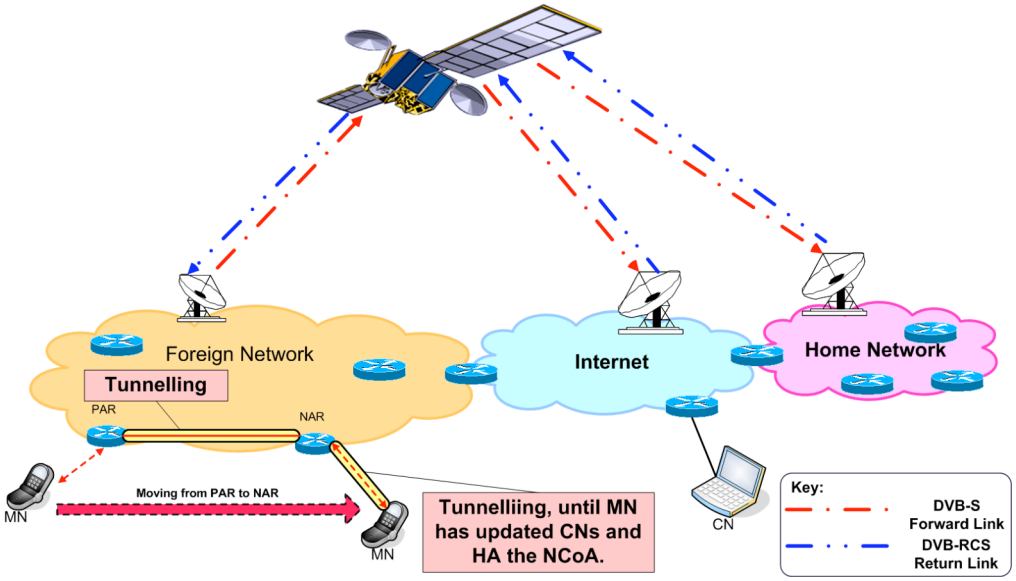


Figure 15: Fast Handover for Mobile IPv6 (FMIPv6) Example

Telecommunications-enhanced Mobile IP (TeleMIP)

The TeleMIP concept was mainly intended for employment in third generation (3G) wireless networks and is similar to the HMIP concept. It basically introduces a two-level hierarchy framework and introduces a new mechanism called mobility agent (MA). The MA, as defined in [DAS00], is an Internet host that is dynamically assigned by the network on the MN's visited network and is located at a higher level in the network hierarchy that the subnet-specific subnet agents (SAGs). The incoming (and possibly outgoing) IP packets are forwarded through the MA and the MA acts as the POA for the MN to the foreign network.

In TeleMIP, it is assumed that the foreign network domain consists of several subnets and uses the intra-domain mobility management protocol (IDMP) [MIS01] to manage mobility in the domain. The MN is assigned two types of CoA, i.e. a global CoA (GCoA) and a local CoA (LoCoA). The GCoA is the address used for identifying the MN's current domain. The LoCoA is the address that specifies the MN's current POA and changes whenever the MN moves to another subnet. The MN will register its GCoA with the HA and provide the GCoA to CNs during binding updates. Therefore, MA will intercept packets from the global Internet that are intended for the MN and forward them to MN using normal IP routing (i.e. by using the LoCoA). Therefore, as long as MN is within this domain, the GCoA will not change and not require updating. This assumes that the same MA services MN when MN is roaming between the subnets. Hence, MN is only required to obtain a new LoCoA and update MN when it roams to another subnet. An example is illustrated in Figure 16 and the TeleMIP concept is further

[5] Fast Neighbour Message (FNA) is a message from the MN to the NAR to announce attachment and to confirm the use of NCoA when the MN has not received FBACK [KOO04].

elaborated in [DAS00] and [CHA01]

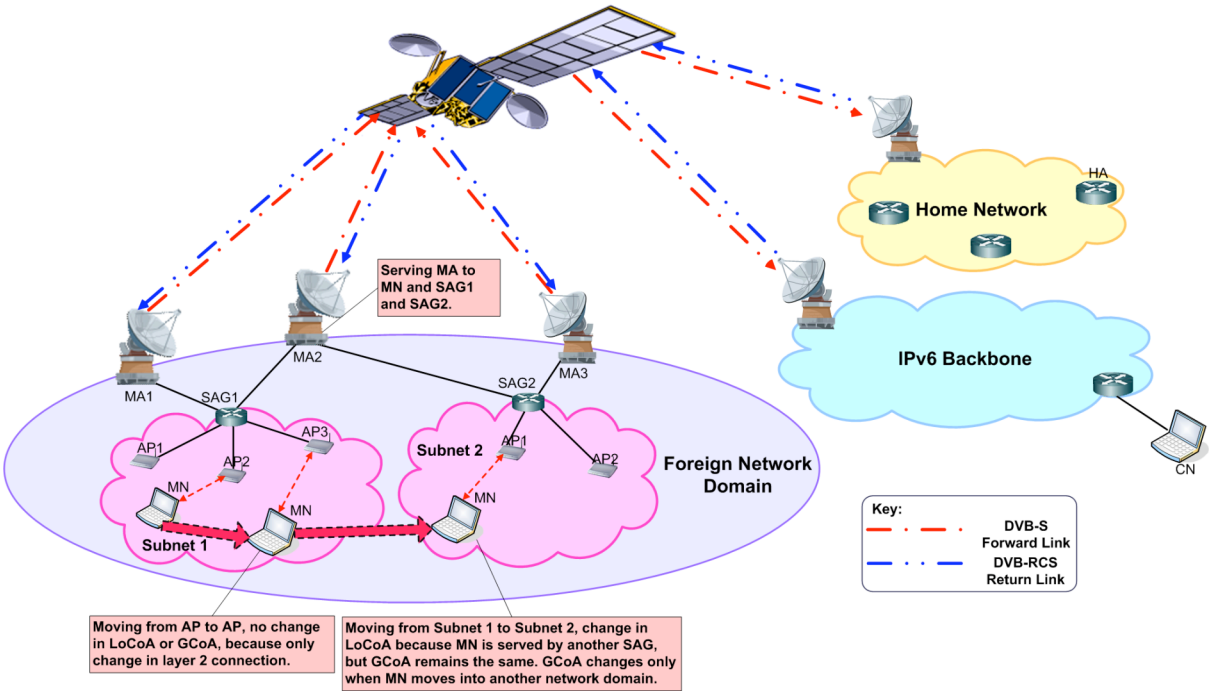


Figure 16: Telecommunications-enhanced Mobile IP (TeleMIP) Example

While Mobile IP has been widely accepted as the de-facto standard for supporting mobility management in future mobile communications, it does possess several shortcomings (such as long latencies, packet losses and signalling overheads during handoff). Much research is focused on the development of micro-mobility protocols and a few have been discussed above. There are other proposals also available such as edge mobility architecture (EMA), handoff- aware wireless access internet infrastructure (HAWAII), cellular IP (CIP), "QoS-conditionalised" handoff scheme and auto-update micromobility protocol (AUM), and are addressed in [ONE00] and [ONE00a], [SHE00], [FU02] and [SHA04] and [SHA04a] respectively.

4 Security Issues in DVB Systems

4.1 Introduction

Security may be provided at any level of the broadband satellite protocol stack such as link, network, transport or application layers. The security operations may be visible to end users and applications if they are implemented at the application level, or it can be transparent if implemented in the lower layers.

Link layer security has the following advantages:

- Security is provided independently of upper layer protocols (whether IP, TCP, UDP, RTP or reliable multicast);
- It can protect satellite link against traffic analysis and illegal changes to satellite network configuration;

- It can provide protection to all real time and non real time applications.

The disadvantages of link layer security are as follows:

- Only satellite terminals are authenticated;
- Only satellite link traffic can be encrypted and digitally signed.

Security services can be provided at the link layer such as asynchronous transfer mode (ATM) cell level and MPEG-TS for DVB-S and DVB-RCS systems, which are the focus of the rest of this paper.

4.2 ATM security

ATM Forum has defined four security services, in the ATM Security specifications [ATM01] as follows:

- User plane security: The user plane security defines the mechanisms to allow for secure communication between nodes in an ATM network.
- Control plane security: The control plane defines the call control signalling needed to establish, maintain and close a certain virtual connection (VC).
- Support services: The support services define the certification infrastructures, the key exchange mechanisms, and the basic negotiation of security requirements and capabilities.
- Management plane security: The management plane is responsible for both performing management functions for the system as a whole (plane management), and for performing network and system management functions such as resource management (layer management).

The ATM Forum's Security Specification states that the ATM cell payload is encrypted and the cell header is unchanged. A survey of available ATM integrated circuits (ICs) shows that normally segmentation and reassembly (SAR) controllers integrate both the AAL and the ATM layer into one unit. Thus, to maintain compatibility between existing ATM hardware and encryption hardware, access to the ATM cell can only be made at the hardware interface between the SAR controller and the transmission convergence (TC) unit. This interface has been standardised by the ATM Forum as the universal test & operations physical interface for ATM level 2 (UTOPIA). By intercepting the UTOPIA interface a standard compliant key agile ATM cell payload encryption is feasible up to high transmission rates (i.e.155 Mbps). In addition to the high transmission rates possible, a further advantage of intercepting the cell stream at the UTOPIA is that the solution is independent of the hardware since most ATM hardware manufacturers support UTOPIA. Intercepting standardised UTOPIA decouples the encryption hardware from the physical media and meets the objective of being applicable to different media. Even if this hardware architecture seems to be a simple one, there are two important performance related considerations to be made:

ATM Forum specifications address the security issues in terrestrial fixed networks only. There is very limited work on done on securing satellite ATM. There are several technical challenges need to be evaluated carefully for securing ATM satellites such as the encryption synchronisation in high bit error rates environment, where errors are of bursty nature. Therefore it is important to examine the impact of such errors on ATM cell payload encryption performance. Another issue is the transmission rate and encryption key updating, where ATM has been designed for the high data rates. Therefore, there is a need for a mechanism to change the encryption key frequently. This challenge is not specific to satellites and includes terrestrial ATM networks as well.

4.3 DVB-S Conditional Access

Conditional access (CA) is a service that allows broadcasters to restrict certain programming products to certain viewers. The CA does this by encrypting the broadcaster's programs. Consequently, the programs must be decrypted at the receiving end before they can be decoded for viewing. CA offers capabilities such as pay-per-view (PPV), interactive features such as video-on-demand (VoD) and games, the ability to restrict access to certain material (adult movies, for example) and the ability to direct messages to specific set-top boxes (perhaps based on geographic region).

The Conditional Access system used in the DVB system [ETS00] and [ETS03a] includes three main functions: scrambling/descrambling, entitlement checking and entitlement management.

The scrambling/descrambling function aims to make the service incomprehensible to unauthorized users. Descrambling can be achieved by any receiver having an appropriate descrambler and holding a secret control word (CW). Scrambling can be applied to service components, either using a common Control Word or using separate Control Words for each component.

The entitlement checking function consists of broadcasting the conditions required to access a service, together with encrypted secret codes to enable the descrambling for authorized receivers. These codes are sent inside dedicated messages called entitlement checking messages (ECMs) and these are carried in the ensemble.

The entitlement management function consists of distributing entitlements to receivers. There are several kinds of entitlements matching different means of subscribing to a service: subscription per theme, level or class, pre-booked pay-per-programme or impulse pay-per-programme, per service or per time. This information is sent inside dedicated messages called entitlement management messages (EMMs) and these may be carried in the same ensemble as the scrambled services or by some other means. The control and management functions require the use of secret keys and cryptographic algorithms.

To understand how CA is used, we first need to look at the data it encrypts. Each individual program that a broadcaster provides is composed of many elements, such as video, audio and text. In digital television, these elements are converted into digital form using the MPEG-2 codec. The MPEG-2 data associated with each program are broken up into many packets, and the sum total of these packets for each program is called the program elementary stream (PES). The PES for each program is then multiplexed together with those of other programs. This stream of multiplexed programs is then broken up into 188-byte packets for transmission, at which point it is called the DVB MPEG-2 transport stream (TS). The CA service can scramble the programming data either at the PES level or the TS level. The preferred option is scrambling at the TS level.

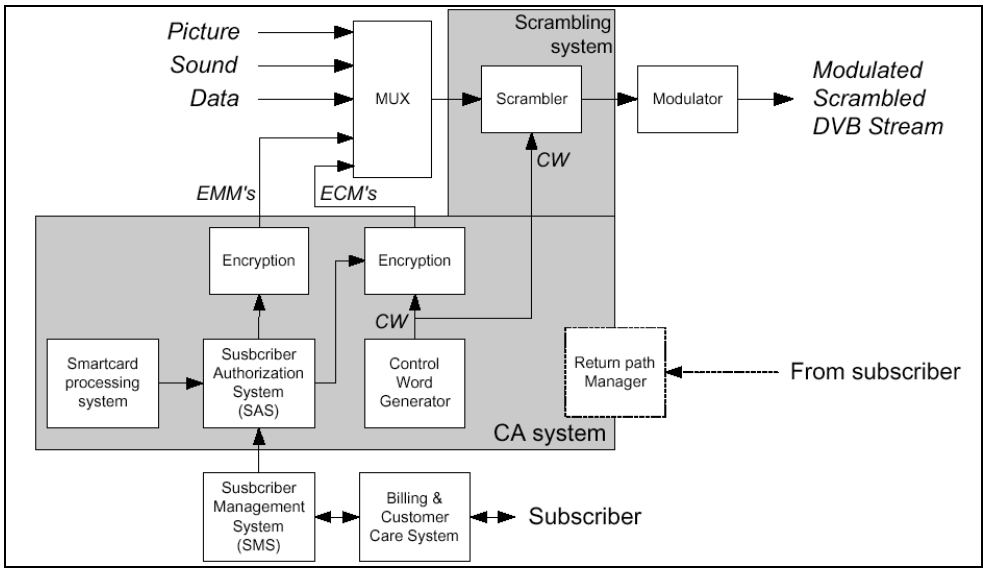


Figure 17: General Architecture for Conditional Access System

A general architecture is shown in Figure 17. The main system components are: a multiplexer (MUX) that combines the video stream, audio stream, data stream and the EMMs and ECMs into a single DVB stream. This multiplexer usually is a dedicated off-the-shelf device. Another component is the Modulator that takes the resulting signal and modulates it for its transmission to the satellite. The third component is the conditional access system that is composed of several specific modules:

- The scrambler: Scrambles the payload of the packets composing the transport stream, using a Control Word generated by the Control Word Generator. The scrambler usually scrambles the packets containing the picture and audio information and sometimes some packets containing data. Packets containing EMMs and ECMs are not scrambled. The preferred implementation of the scrambler is in the multiplexer device. Stand-alone scramblers also exist.
- The subscriber authorization system (SAS): Processes the different viewing authorizations given to the subscribers and uses them to generate adequate EMMs and ECMs.
- The Control Word Generator that creates the control words: Two encryption engines (often implemented by the same software) are used to encrypt the content of the EMMs and the Control Words stored in the ECMs.
- The Smart Card Processing System: Contains information about the secret information stored into consumer smart cards or set-top boxes. This module is sometimes integrated in the SAS.
- The conditional access system needs information from other modules of the system such as:
    - The subscriber management system (SMS) holds all the data related to subscribers, running subscriptions and payments. This system interacts with the Billing and Customer Care system to generate revenues. The SMS tells which programs subscribers are authorized to view.
    - The Return Path Manager (if a return path exists): this module can be used by the conditional access system to perform verification operations and to get feedback on the set-top box status and behaviour.

The encrypted multi-session key, carried by the ECM, is related to particular programming material. This key, once decrypted, actually becomes the control word that is fed into the DVB descrambler,

allowing the transport stream to be descrambled so that the viewer can see a particular program or view the programming material for a particular session. The service key (EMM) is sent to the smart card, where it is decrypted with the help of the user key held inside the smart card. The descrambled service key is then used as the key to descramble the session key (ECM). This descrambling yields the control word (CW). It is this CW that is the key to the DVB transport-stream descrambler.

The main weakness of DVB-S CA is the one-way (broadcast) transmissions. Therefore it is very difficult to stop fraud and cloning pay TV smart cards without an efficient return channel and an efficient way to update smart card keys.

4.4 DVB-RCS security

As specified in [ETS03], security is intended to protect the user identity including its exact location, the signalling traffic to and from the user, the data traffic to and from the user and the operator/user against use of the network without appropriate authority and subscription. Three levels of security can be applied to the different layers:

- DVB common scrambling in the forward link (could be required by the service provider);
- Satellite interactive network individual user scrambling in the forward and return link;
- IP or higher layer security mechanisms (could be used by the service provider, the content provider).

Although the user/service provider could use its own security systems above the data link layer, it may be desirable to provide a security system at the data link layer so that the system is inherently secure on the satellite section without recourse to additional measures. Also, since the satellite interactive network forward link is based on the DVB/MPEG-TS Standard, the DVB common scrambling mechanism could be applied, but is not necessary (it would just add an additional protection to the entire control stream for non-subscribers). This concept is shown in Figure 18.

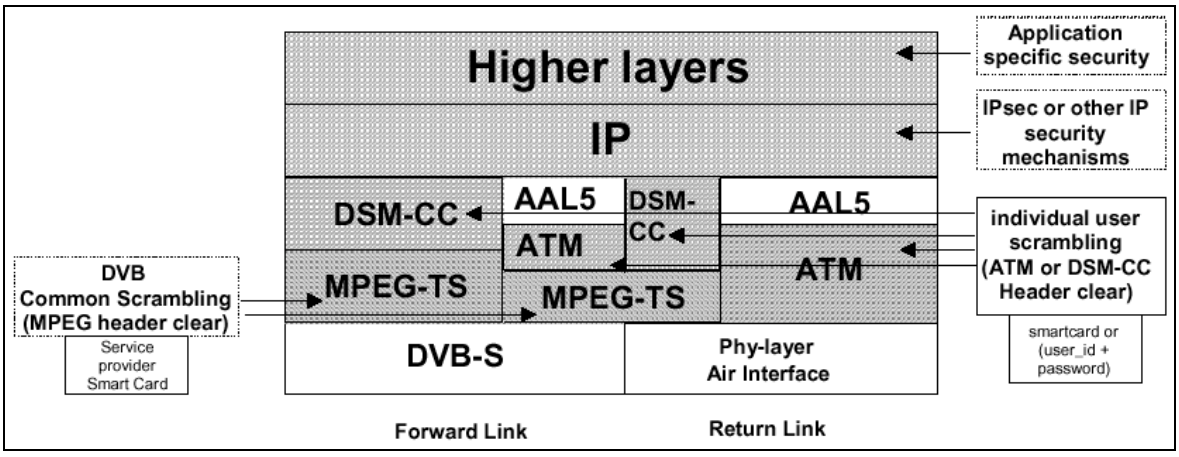


Figure 18: Security Layers for Satellite Interactive Network

In the following it is assumed there can be more than one user per RCST and that such users will have security in their own right. The term RCST and satellite terminal (ST) have the same meaning in this document. Security is thus defined at a level higher than the individual ST. On a user basis, an authentication algorithm may either check for user name and password on the client device or may use a Smart Card within the ST. All data and control to and from each user may be scrambled on an

individual user basis. Each user may have a control word for the return and the forward link that does not allow anybody other than the NCC/Gateway or the user himself to descramble the data, except for lawful interceptors such as country authorities.

4.5 End-to-end and satellite network security

End-to-end security may be provided at certain level of the protocol stack such as application, transport or network layers. In general, there is a need to establish a trust relationship between users of the end-to-end security system through a security management system. The security operations may be visible to end users and applications if they are implemented at the application level, or it can be transparent if implemented in the lower layers.

In contrast, satellite network security focuses on access control and data encryption/integrity mechanisms within satellite network boundaries and thus link layer security is the best solution here. The satellite network can have star and mesh configurations with regenerative or bent pipe satellites. DVB and ATM security procedures can be used to secure satellite links. IPSec can be used to provide satellite network security by implementing IPSec tunnels.

The following table provides a summary of the major advantages and disadvantages of security in each layer of the broadband satellite protocol stack:

	Link layer	**Network layer**	**Transport layer**	**Application layer**
Major advantages	Complete control of satellite link security	IPSec is the best solution for Internet security.	Widely used for securing TCP connections	Can satisfy applications requirement very well.
Major disadvantages	Only the satellite hop is secure	IPSec works only for IP networks.	No security for UDP and multicast	No transparency, where applications need modification to fit security

Table 3: Security Layers Comparison

Also the security services that can be provided in layer of the BSM protocol stack are summarised as follows:

	Link layer	**IP Network layer**	**Transport layer**	**Application layer**
Satellite terminal authentication	Yes	Yes (IP address)	No	No
User terminal authentication	No	Yes (IP address)	No	No
User authentication	No	No	Yes	Yes
Satellite link privacy	Yes	Yes (IPSec IP tunnel)	No	No
End to end privacy	No	Yes	Yes	Yes
Satellite link data integrity	Yes	Yes (IPSec IP tunnel)	No	No

End to end data integrity	No	Yes	Yes	Yes

Table 4: Security Services at Various Protocol Layers

Examining Table 4, shows that implementing network layer security such as IPSec, provides the flexibility of closer integration with the Internet and satisfy the requirement of some multimedia services for satellite and/or end to end security.

5 CONCLUSIONS

There has been vast development in areas related to DVB satellite systems. Therefore, it is beneficial at this stage, to be able to comprehend the main characteristics and issues of the DVB satellite systems and the importance of standard IP protocols, as mobile communications progresses towards achieving a ubiquitous Internet network. This tutorial paper has described the different DVB satellite systems, i.e. DVB-S, DVB-RCS and DVB-S.2. In addition, the characteristics of IP protocols, mechanisms for macro and micro-mobility, migration strategies from IPv4 to IPv6 and security mechanisms for DVB satellite systems were also addressed. This facilitates the discussion of the different issues of current and future operational scenarios that is to be discussed in the second part of this paper, *Future Service Scenarios*.

3G	third generation
ACM	adaptive coding and modulation
ACQ	acquisition
AR	access router
ARIB	association of radio, industries and businesses
ATM	asynchronous transfer mode
ATSC	advanced television system committee
AUM	auto-update micromobility protocol
AVBDC	absolute volume based dynamic capacity
BBFRAME	base block frame
BC-BS	backwards-compatible broadcast services
BCH	bose-chaudhuri-hocquenghem
BIA	bump in the API
BIS	bump in the stack
BS	broadcast service
BSM	broadband satellite multimedia
BSS	broadcast satellite service
BU	binding update
CA	conditional access
CCM	constant coding and modulation
CIP	cellular IP
CN	correspondent node
C/N	carrier-to-noise
CoA	care-of address
CRA	continuous rate assignment
CSC	common signalling channel
CW	control word
DAD	duplicate address detection
DNS	domain name system
DSTM	dual stack transition mechanism
DTH	direct-to-home
DTV	digital TV

DTVC/DSNG	digital TV contribution and satellite news gathering
DVB	digital video broadcasting
DVB-DSNG	DVB – digital satellite news gathering
DVB-H	DVB handheld
DVB-RCS	DVB return channel by satellite
DVB-S	digital video broadcasting via satellite
DVB-S.2	second-generation DVB system for broadband satellite services
DVB-T	DVB terrestrial
EC	European commission
ECM	entitlement checking messages
EMA	edge mobility architecture
EMM	entitlement management messages
ESA	European space agency
ESP	encrypted security payload
ETSI	European telecommunications standards institute
FA	foreign agent
FBACK	fast binding acknowledgement
FBU	fast binding update
FCA	free capacity assignment
FDM	frequency division multiplexing
FEC	forward error correction
FIFO	first in first out
FMIPv6	fast handovers for mobile IPv6
FNA	fast neighbour message
FP5	FIFTH framework programme
FSS	fixed satellite service
GCoA	global CoA
GPRS	general packet radio service
HA	home agent
HAWAII	handoff – aware wireless access internet infrastructure
HDTV	high definition television
HMIP	hierarchical mobile IP
HMIPv6	hierarchical mobile IPv6
IC	integrated circuit

ICMP	internet control message protocol
IDMP	intra-domain mobility management protocol
IETF	internet engineering task force
IP	internet protocol
IP	internet protocol
IPv4	IP version 4
IPv6	IP version 6
IRD	integrated receiver decoder
IS	interactive services
ISATAP	intra-site automatic tunnel addressing protocol
ISDN	integrated services digital network
ISO	international standards organisation
ISP	internet service provider
ITU	international telecommunication union
ITV	interactive TV
LAN	local area network
LCoA	on-link care-of-address
LDPC	low density parity check codes
LMM	localised mobility management
LNB	low noise block
LoCoA	local CoA
MA	mobility agent
MAC	medium access control
MAP	mobility anchor point
MF-TDMA	multi-frequency TDMA
MIP	mobile IP
MIPv4	mobile IP version 4
MIPv6	mobile IP version 6
MN	mobile node
MPE	multi-protocol encapsulation
MPEG-2	moving pictures expert group – 2
MPLS	multiprotocol label switching
MUX	multiplexer
NAPT-PT	network address port translation – packet translation

NAR	new address router
NAT	network address translation
NATO	north Atlantic treaty organisation
NAT-PT	network address translation – protocol translation
NBC-BS	non backwards compatible broadcast services
NBMA	non – broadcast multiple access
NCC	network control centre
NCoA	new CoA
OSPF	open shortest path first
PAR	previous access router
PCoA	previous CoA
PES	Program elementary stream
PID	packet identifier field
PLFRAME	physical layer frame
PoA	point of attachment
PPV	pay-per-view
PrRtAdv	proxy router advertisement
PSK	phase shift keying
QAM	quadrature amplitude modulation
QPSK	quadrature phase shift keying
RBDC	rate based dynamic capacity
RCoA	regional care-of address
RCST	return channel satellite terminal
RIP	routing information protocol
RtSolPr	router solicitation for proxy advertisement
SAGs	subnet agents
SAR	segmentation and reassembly
SAS	Subscriber authorisation system
SIIT	satellite IP / internet control message protocol translation
SIT	satellite interactive terminal
SMATV	satellite master antenna television
SMS	subscriber management system
SNG	satellite news gathering
SP	service provider

ST	satellite terminal
SYNC	synchronisation
TC	transmission convergence
TCP	transmission control protocol
TDM	time division multiplex
TeleMIP	telecommunications – enhanced mobile IP
TRF	traffic
TRT	transport relay translator
TS	transport stream
TV	television
TVRO	TV receive only
UDP	user datagram protocol
ULE	ultra lightweight encapsulation
UPs	user packets
USB	universal serial bus
UTOPIA	universal test & operations physical interface for ATM level 2
VBDC	volume based dynamic capacity
VC	virtual connection
VCM	variable coding & modulation
VoD	video-on-demand
VoIP	voice over IP
Wi-Fi	wireless fidelity

REFERENCE

[ALB04] Albertazzi G, Cioni S, Corazza GE, De Laurentiis N, Neri M, Salmi P, Vanelli Coralli A. Adaptive Coding and Modulation Techniques for Future Ka Band Satellite Systems - Part I: Forward Link. *Proceedings of 10th Ka and Broadband Communications Conference*; Vicenza, Italy, September 30 – October 2, 2004.

[ATM01] ATM Forum Technical Committee. ATM Security Specification Version 1.1: af-sec-0100.002. March 2001.

[BOU04] Bound J. Dual Stack IPv6 Dominant Transition Mechanism (DSTM). IETF Internet Draft: draft-bound-dstm-exp-02.txt. June 2005.

[BSM05] Broadband Satellite Multimedia (BSM) Working Group. Satellite Earth Stations and Systems (SES), European Telecommunications Standards Institute (ETSI). Available from http://www.etsi.org; Internet.

[CAM00] Campbell AT, Gomez-Castellanos J. IP Micro-Mobility Protocols. *ACM SIGMOBILE Mobile Computing and Communications Review* 2000; **4**(4): 45-53.

[CAR01] Carpenter B, Moore K. Connection of IPv6 Domains via IPv4 Clouds. RFC 3056; February 2001.

[CAR04] Carneiro G, Ruela J, Ricardo M. Cross-layer design in 4G wireless terminals. *IEEE Wireless Communications* 2004; **11**(2): 7-13.

[CAS00] Castelluccia C. HMIPv6: A Hierarchical Mobile IPv6 Proposal. *ACM SIGMOBILE Mobile Computing and Communications Review* 2000; **4**(1): 48-59.

[CAS04] Casini E, De Gaudenzi R, Ginesi A. DVB-S2 modem algorithms design and performance over typical satellite channels. *International Journal of Satellite Communications and Networking* 2004; **22**(3): 281-318.

[CHA01] Chakraborty K, Misra A, Das S, McAuley A, Dutta A, Das SK. Implementation and Performance Evaluation of TeleMIP. *Proceedings of IEEE International Conference on Communications;* Helsinki, Finland, June 11-15, 2001; 2488-2493.

[CON02] Conforto P, Tocci C, Losquadro G, Sheriff RE, Chan PML, Hu YF. Ubiquitous Internet in an Integrated Satellite - Terrestrial Environment: The SUITED Solution. *IEEE Communications Magazine* 2002; **40**(1): 98-107.

[DAS00] Das S, Misra A, Agrawal P. TeleMIP: Telecommunications-Enhanced Mobile IP Architecture for Fast Intradomain Mobility. *IEEE Personal Communications Magazine* 2000; **7**(4): 50-58.

[DEE98] Deering, S. and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460; December 1998.

[DUR01] Durand A, Fasano P, Guardini I, Lento D. IPv6 Tunnel Broker. RFC 3053; January 2001.

[ERO04] Eroz M, Sun F-W ,Lee L-N. DVB-S2 low density parity check codes with near Shannon limit performance. *International Journal of Satellite Communications and Networking* 2004; **22**(3): 269–279.

[ESA04] ESA Contract Report Number 17629/03/NL/ND. Preparation for IPv6 in Satellite Communications. July 2004.

[ETS00] ETSI: ETSI TS 103 197 V1.1.1 (2000-06) Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt.

[ETS02] ETSI: ETSI EN 301 958 V1.1.1 (2002-03) Digital Video Broadcasting (DVB); Interaction channel for Digital Terrestrial Television (RCT) incorporating Multiple Access OFDM.

[ETS03] ETSI: ETSI EN 301 790 V1.4.1 (2005-04) Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems.

[ETS03a] ETSI: ETSI EN 301 192 V1.3.1 (2003-05) Digital Video Broadcasting (DVB); DVB specification for data broadcasting.

[ETS04] ETSI: EN 301 192 V1.4.1 (2004-11) Digital Video Broadcasting (DVB); DVB specification for data broadcasting.

[ETS05] ETSI: ETSI TR 102 353 V1.1.1 (2004-11) Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Guidelines for the Satellite Independent Service Access Point (SI-SAP).

[ETS05a] ETSI: EN 302 307, V1.1.1 (2005-03) Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive services, New Gathering and other broadband satellite applications.

[ETS97a] ETSI: EN 300 421 V1.1.2 (1997-08) Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for the 11/12 GHz satellite services.

[ETS99] ETSI: EN 301 210 V1.1.1 (1999-03) Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation systems for Digital Satellite News Gathering (DSNG) and other contribution application by satellite.

[FAI05] Fairhurst G, Collini-Nocker B. Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP datagrams over MPEG-2 Transport Stream. IETF Internet Draft: draft-ietf-ipdvb-ule-06.txt; June 2005.

[FOR03] Forouzan BA. TCP/IP Protocol Suite (2nd Edition); McGraw-Hill: London, 2003.

[FU02] Fu XM, Karl H, Kappler C. QoS-Conditionalized Handoff for Mobile IPv6. *Proceedings of 2nd IFIP-TC6 International Networking Conference, NETWORKING* 2002, Pisa, Italy, May 19-24, 2002; 721-730.

[GAL62] Gallager R. Low density parity check codes. *IRE Transactions on Information Theory* 1962.

[GIL00] Gilligan R, Nordmark E. Transition Mechanisms for IPv6 Hosts and Routers. RFC 2893; August 2000.

[HAG01] Hagino J, Yamamoto K. An IPv6-to-IPv4 Transport Relay Translator. RFC 3142; June 2001.

[HSI02] Hsieh R, Seneviratne A, Soliman H, El-Malki K. Performance Analysis on Hierarchical Mobile IPv6 with Fast-Handoff over End-to-End TCP. *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM* 2002), Taipei, Taiwan, November 17-21, 2002; 2488-2492.

[HUI04] Huitema C. Teredo: Tunneling IPv6 over UDP through NATs. IETF Internet Draft: draft-huitema-v6ops-teredo-05.txt; October 2005.

[IPD05] IP over DVB (ipdvb) Working Group, Internet Area, Internet Engineering Task Force (IETF). Available from http://www.ietf.org; Internet.

[ISO00] ISO: ISO/IEC IS 13818-1 Information technology -- Generic coding of moving pictures and associated audio information -- Part 1: Systems; 2000.

[IST04] 6NET DELIVERABLE D2.3.3-bis. Updated IPv4 to IPV6 transition cookbook for end site networks/universities; Available from http://www.6net.org/publications/deliverables/D2.3.3.pdf; Internet.

[IST04a] IST2001-39097. FIFTH Deliverable D3 – System Specification Document. June 2004.

[JOH04] Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. RFC 3775; June 2004.

[KIT01] Kitamura H. A SOCKS-based IPv6/IPv4 Gateway Mechanism. RFC 3089; April 2001.

[KOO04] Koodli R. Fast Handovers for Mobile IPv6. IETF Internet Draft: draft-ietf-mipshop-fast-mipv6-03.txt; April 2005, Work in Progress.

[KUR05] Kurose JF, Ross KW. Computer Networking: A Top-Down Approach Featuring the Internet (3rd Edition); Addison Wesley: London, 2005.

[LEE02] Lee S, Chin M-K, Kim Y-J, Nordmark E, Durand A. Dual Stack Hosts Using "Bump-in-the-API" (BIA). RFC 3338; October 2002.

[LIA03] Liang X, Ong FLC, Chan PML, Sheriff RE, Conforto P. Mobile Internet access for high-speed trains via heterogeneous networks. *Proceedings of 14th IEEE 2003 International*

Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2003). Beijing, China, September 7-10 2003; 177-181.

[MAC03] Mackay M, Edwards C, Dunmore M, Chown T, Carvalho G. A Scenario-Based review of IPv6 Transition Tools. *IEEE Internet Computing* 2003; **7**(3): 27-35.

[MAN04] Manner J, Kojo M. Mobility Related Terminology. RFC 3753; June 2004.

[MCC05] McCann P. Mobile IPv6 Fast Handovers for 802.11 Networks. IETF Internet Draft: draft-ietf-mipshop-80211fh-04.txt; August 2005.

[MIS01] Misra A, Das S, Mcauley A, Dutta A, Das SK. IDMP: An Intra-Domain Mobility Management Protocol using Mobility Agents. IETF Internet Draft: draft-misra-mobileip-idmp-01.txt; January 2001, Work in Progress.

[MON05] M-J Montpetit, G. Fairhurst, H. D. Clausen, B. Collini-Nocker, H. Linder. A framework for transmission of IP datagrams over MPEG-2 networks. IETF Draft: draft-ietf-ipdvb-arch-04.txt; November 2005.

[NIK05] Nikander P, Arkko J, Aura T, Montenegro G, Nordmark E. Mobile IP version 6 Route Optimization Security Design Background. IETF Internet Draft: draft-ietf-mip6-ro-sec-03.txt; December 2005.

[NOR00] Nordmark E. Stateless IP/ICMP Translation Algorithm (SIIT). RFC 2765; February 2000.

[NOR05] Nordmark E, Gilligan RE. Basic Transition Mechanisms for IPv6 Hosts and Routers. IETF Draft: draft-ietf-v6ops-mech-v2-07.txt; September 2005.

[ONE00] O'Neill A, Tsirtsis G, Corson S. Edge Mobility Architecture. IETF Internet Draft: draft-oneill-ema-02.txt; July 2000, Work in Progress.

[ONE00a] O'Neill A, Tsirtsis G, Corson S. EMA Enhanced Mobile IPv6/IPv4. IETF Internet Draft: draft-oneill-ema-mip-00.txt; July 2000, Work in Progress.

[PER02] Pérez-Costa X, Schmitz R, Hartenstein H, Liebsch M. A MIPv6, FMIPv6 and HMIPv6 Handover Latency Study: Analytical Approach. *Proceedings of IST Mobile and Wireless Telecommunications Summit* 2003. Thessaloniki, Greece, June 17-19, 2002; 100-105.

[PER02a] Perkins C. IP Mobility Support for IPv4. RFC 3344; August 2002.

[PER03] Pérez-Costa X, Torrent-Moreno M, Hartenstein H. A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast Handovers for Mobile IPv6 and their Combination. *ACM SIGMOBILE Mobile Computing and Communications Review* 2003; **7**(4): 5-19.

[POS81a] Postel J. Internet Protocol. RFC 791; September 1981.

[REI03] Reinbold P, Bonaventure O. IP Micro-Mobility Protocols. *IEEE Communications Surveys and Tutorials Magazine* 2003; **5**(1): 40-57.

[RIN04] Rinaldo R, Vazquez-Castro MA, Morello A. DVB-S2 ACM modes for IP and MPEG unicast applications. *International Journal of Satellite Communications and Networking* 2004; **22**(3): 367 – 399.

[SAH04] Saha D, Mukherjee A, Misra IS, Chakraborty M. Mobility Support in IP: A Survey of Related Protocols. *IEEE Network Magazine* 2004; **18**(6): 34-40.

[SAT05] Available from http://www.satlabs.org.

[SHA04] Sharma A, Ananda AL. AUM- An IPv6 based Approach for Micromobility. *Proceedings of ACM International Workshop on Mobility Management and Wireless Access (MobiWac 2004)*; Philadelphia, PA, USA, September 26 – October 1 2004; 72-78.

[SHA04a] Sharma A, Ananda AL. A Protocol for Micromobility Management in Next Generation IPv6 Networks. *Proceedings of LCN 2004*, Tampa, Florida, November 16-18 2004; 435-436.

[SHE00] Shelby ZD, Gatzounas D, Campbell A, Wan C-Y. Cellular IPv6. IETF Internet Draft: draft-shelby-cellularipv6-01.txt; July 2001, Work in Progress.

[SOL05] Soliman H, Catelluccia C, El Malki K, Bellier L. Hierarchical Mobile IPv6 Mobility Management. IETF Internet Draft: draft-ietf-mipshop-hmipv6-04.txt; June 2005.

[TEM04] Templin F, Gleeson T, Talwar M, Thaler D. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). IETF Internet Draft: draft-ietf-ngtrans-isatap-24.txt; July 2005.

[TSI00] Tsirtsis G, Srisuresh P. Network Address Translation - Protocol Translation (NAT-PT). RFC 2766; February 2000.

[TSU00] Tsuchiya K, Higuchi H, Atarashi Y. Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS). RFC 2767; February 2000.

[VAZ04] Vazquez-Castro MA, Cardoso A, Rinaldo R. Encapsulation and framing efficiency of DVB-based satellite adaptive systems. *In Proceedings of the VTC Conference*. Milano, 2004.

[WIL05] Williams C. Localized Mobility Management Goals. IETF Internet Draft: draft-ietf-mipshop-lmm-requirements-03.txt; January 2005, Work in Progress.

[WOO97] Wood, D. The DVB Project: philosophy and core system. *Electronics and Communications. Engineering Journal* 1997. **9**(1): 5-10.