INTERNATIONAL JOURNAL OF SATELLITE COMMUNICATIONS AND NETWORKING
Int. J. Satell. Commun. Network. 2007; **25**:363–407
Published online 12 June 2007 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/sat.879

Fusion of digital television, broadband Internet and mobile communications—Part I: Enabling technologies

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

[1]*University of Bradford, Bradford, U.K.*
[2]*Aristotle University of Thessaloniki, Greece*
[3]*ISTI-CNR (National Research Council), Italy*
[4]*University of Surrey, U.K.*
[5]*University of Aberdeen, U.K.*
[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 DVB 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 emphasize 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-S2). 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. Copyright © 2007 John Wiley & Sons, Ltd.

Received 1 August 2005; Revised 20 February 2007; Accepted 10 April 2007

KEY WORDS: DVB; DVB-S; DVB-RCS; DVB-S2; IP; mobility management; security

*Correspondence to: P. M. L. Chan, Department of Computing, University of Bradford, Richmond Road, Bradford BD7 1DP, U.K.
† E-mail: p.m.l.chan@bradford.ac.uk

Contract/grant sponsor: European Commission

1. INTRODUCTION

A family of television (TV) compression/transmission schemes have been defined by the digital video broadcasting (DVB) Project. This is a market-led consortium of public and private sector organizations in the TV industry. Its aim is to establish the framework for the introduction of digital television (DTV) services. The specification of DVB has been an European initiative, and has been standardized by the European Telecommunications Standards Institute (ETSI).

Although DVB has its origins in Europe, the DVB Project comprises over 260 organizations from more than 35 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 family of standards for cable, terrestrial and satellite DTV services. Key resulting DVB standards cover satellite, i.e. DVB-S [1], and terrestrial, i.e. DVB-terrestrial (DVB-T) [2], delivery. In particular, recent DVB standards have defined satellite, i.e. DVB-RCS [3], 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 current DVB standards utilize a series of specifications published by the International Standards Organization (ISO) and is known as MPEG-2 (after the moving pictures expert group that defined it) [4]. At the core of these standards is a time-division multiplex that uses fixed-sized frames, transport stream (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 DTV. Some countries have their own variants of the standards, notably the USA uses the Advanced Television Systems Committee (ATSC) specifications and the Association of Radio, Industries and Businesses (ARIB) standards are applied in Japan. These are also based on MPEG-2 and largely follow the same format as DVB, but with the addition of country-specific modifications, such as 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. Although DVB has also been extended for terrestrial networks, the main focus here will be on the standards developed for broadband data delivery *via* satellites: DVB-S, DVB-RCS and DVB-S2. However, due to the increasing deployment of DVB-H (digital video broadcasting-handheld) networks, which supports the convergence of broadcasting of digital television and mobile communications, an overview of the DVB-H specifications will also be presented. This is followed by a description of the different IP technologies used to support macro- and micro-mobility, the migration strategies from IPv4 to IPv6 and session initiation protocol (SIP). Finally, Section 4 describes the different link-layer security mechanisms that are implemented for Asynchronous Transfer Mode (ATM), DVB-S and DVB-S, and also addresses the end-to-end and satellite network security, before the paper is concluded.

DOI: 10.1002/sat

2. DIGITAL VIDEO BROADCAST SYSTEMS

2.1. *DVB-S*

2.1.1. Modulation and coding schemes. The first successful transmission system for DTV to consumers, using the DVB standards, employed satellite links using DVB-S [5]. 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 DTV based businesses to develop and thrive.

The DVB-S standards [1, 2] 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.

The video, audio, control data and user data are all formed into fixed sized MPEG-2 transport packets. The MPEG TS packets consist of 187 bytes + 1 sync byte and are grouped into eight packet frames (1503 bytes). The frames do not contain any additional control information. The TS-sync byte is inverted (0 × B8) 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 follow an approximately random pattern, assuring frequency dispersion of the modulated signal. At the start of each frame, the scrambler is re-initialized. 16 bytes of Reed–Solomon (RS) coding are added to each 188 bytes 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

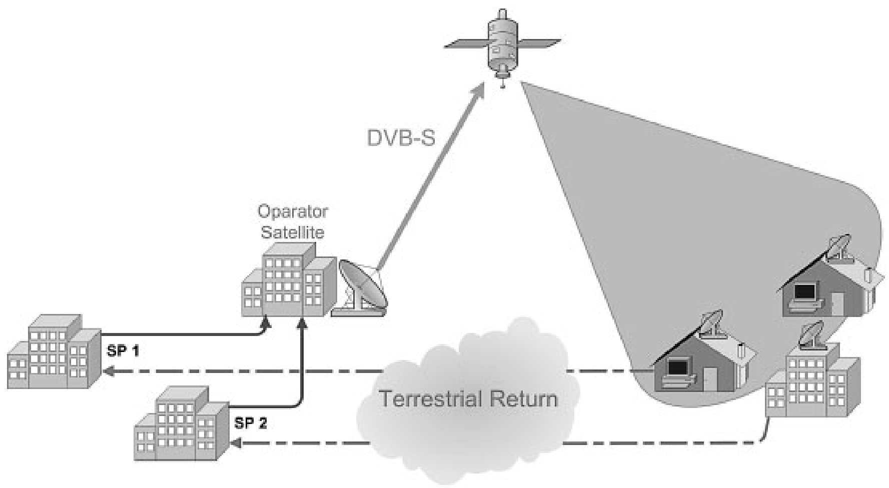


Figure 1. DVB-S system architecture.

DOI: 10.1002/sat

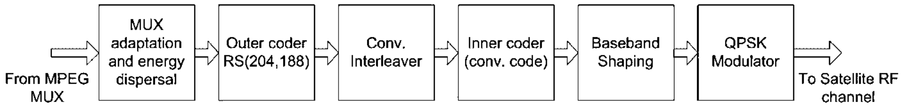


Figure 2. DVB-S frame formation and modulation.

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).

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, i.e. sending-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 by 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 form a part of the 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 this 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 [4]. This standard is known as the multi-protocol encapsulation (MPE) and is specified in EN 301 192 [6]. More recently, the Internet Engineering Task Force (IETF) IP has specified an alternative to MPE DVB (ipdvb) WG [7]. This is called the unidirectional lightweight encapsulation (ULE) [8] and supports a range of packet types, including IPv4 and 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 [9]).

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 [10]. 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, such as standard

DOI: 10.1002/sat

dial-up modem, integrated services digital network (ISDN), cable modem, wireless fidelity (Wi-Fi) or general packet radio service (GPRS) 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 (QoS) 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 [3, 5].

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 [3]. A satellite terminal (ST), also known as satellite interactive terminal (SIT) or return channel satellite terminal (RCST), is specified, that provides a two-way DVB satellite system.

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 interaction channels (Figures 3 and 4).

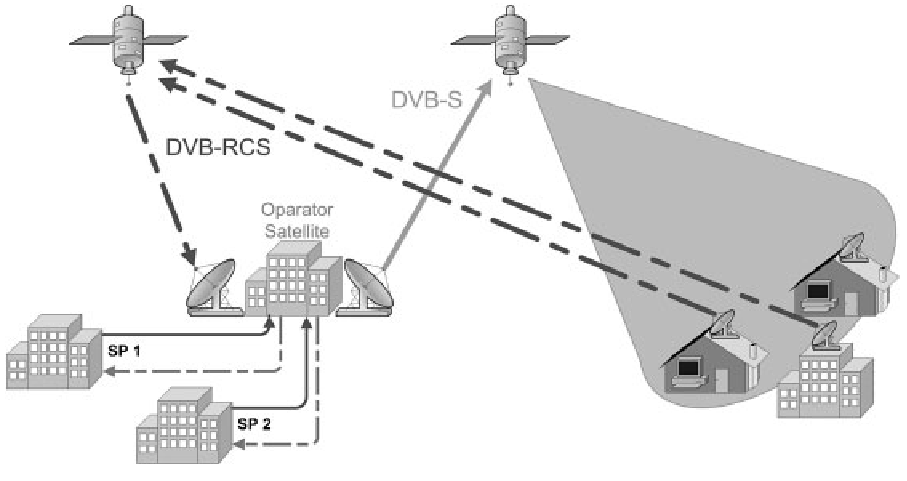


Figure 3. DVB-RCS system architecture.

DOI: 10.1002/sat

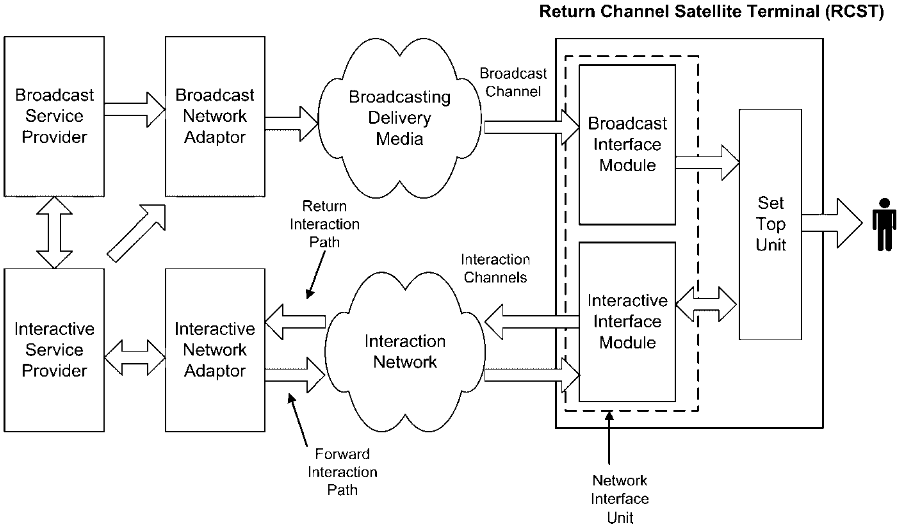

Return Channel Satellite Terminal (RCST)
Broadcast Service Provider
Broadcast Network Adaptor
Broadcasting Delivery Media
Broadcast Channel
Broadcast Interface Module
Set Top Unit
Return Interaction Path
Interaction Channels
Interactive Service Provider
Interactive Network Adaptor
Interaction Network
Interactive Interface Module
Forward Interaction Path
Network Interface Unit

Figure 4. Block diagram of information exchange in a DVB-RCS system.

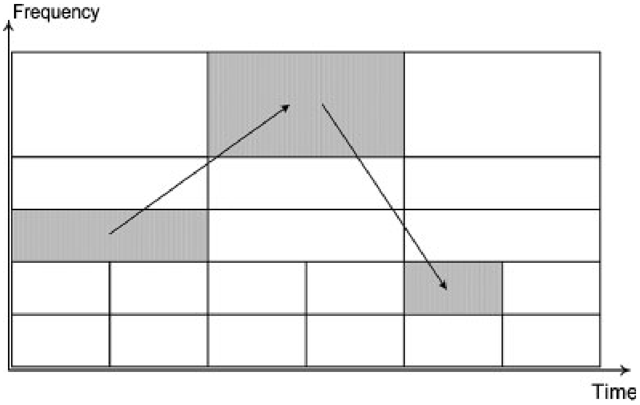


Figure 5. Adaptive MF-TDMA.

The forward channel uses a DVB-S (or DVB-S2) 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 are organized into frames and then are 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 (Figure 5). 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. Frames of a

DOI: 10.1002/sat

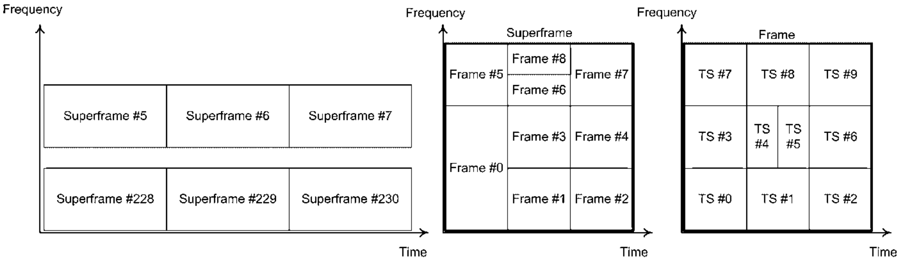


Figure 6. DVB-RCS framing.

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. To join the network, terminals first send a logon message in a dedicated common signalling channel, using slotted aloha. The message is 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 (Figure 6).

The timeslot allocation process supports 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).

Four types of bursts are allowed: traffic bursts (TRF), acquisition (ACQ) bursts, synchronization (SYNC) bursts and common signalling channel (CSC) bursts. Traffic bursts can be of two types: ATM and MPEG2-TS. An ATM traffic burst consists of one or more ATM cells, each 53 bytes long, however in the normal mode, the ATM cells do not support ATM classes of service or ATM signalling. A MPEG2-TS traffic burst contains MPEG2-TS packets. An optional ACQ burst is used to acquire synchronization, prior to operational use of the network by the RCST. A SYNC burst may be used by an RCST to achieve fine synchronization and sending control information to the system. Finally, CSC bursts are used by the RCST to identify itself during logon.

The DVB-RCS standard is now used by many network service operators and is supported by many manufacturers. An industry-led forum, SatLabs [11], 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 remains for DVB-RCS, including bi-directional satellite systems that use DVB-S for their outbound transmission, but do not utilize the DVB-RCS standard for the return link. This may be due to manufacturer investment in proprietary systems, or the cost of current DVB-RCS terminals making 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 standardization work. New work will include

DOI: 10.1002/sat

provision of QoS functions (including cross-layer integration of Internet QoS and MAC resource management functions), adaptive physical waveforms (DVB-S2, fade countermeasures, cross-layer optimization) and support for regenerative satellites.

2.3. *DVB-S2*

2.3.1. Overview. DVB-S was introduced as a standard in 1994 [5] and DVB-digital satellite news gathering (DVB-DSNG) in 1997 [12]. The DVB-S standard specifies QPSK modulation and concatenated convolutional and RS channel coding, and is now used by most satellite operators worldwide for TV and broadcasting services. DVB-DSNG specifies the use of eight phase shift keying (8PSK) and 16 quadrature amplitude modulation (16QAM) for satellite news gathering and contribution services. Since 1997 digital satellite transmission technology has evolved, and DVB-S2 is the latest advanced satellite transmission technique from DVB [1]. 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 optimized for the following broadband satellite applications:

(a) *Broadcast services* (*BS*) *digital multi-programme TV/HDTV*: DVB-S2 is intended to provide DTH services for consumer IRDs, as well as collective antenna systems (SMATV) and cable television head-end stations. DVB-S2 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. These services are transported in MPEG TS format. Variable coding and modulation (VCM) may be applied on multiple TSs 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*) *including Internet access*: DVB-S2 is intended to provide interactive services to consumer IRDs and to personal computers, where DVB-S2'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) TS format or in (single or multiple) generic stream format. DVB-S2 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.

DOI: 10.1002/sat

(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 that are not intended for reception by the general public. The International Telecommunications Union-recommendation (ITU-R) SNG.770-1, defines satellite news gathering (SNG) as 'Temporary and occasional transmission with short notice of TV or sound for broadcasting purposes, using highly portable or transportable uplink earth stations'. Services are transported in single (or multiple) MPEG TS format. DVB-S2 can use 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-S2 is suited for use with a range of satellite transponder bandwidths and frequency bands. The symbol rate is matched to the given transponder characteristics, and, in the case of multiple carriers per transponder (frequency division multiplexing (FDM)), it is matched to the frequency plan adopted. Digital transmissions *via* satellite are affected by power and bandwidth limitations. Therefore, DVB-S2 provides for many transmission modes (FEC coding and modulations), permitting different trade-offs between power and spectrum efficiency.

DVB-S2 may be used for TV services using MPEG-2 and MPEG-4 [13], using a TS packet multiplex. Multiplex flexibility allows the use of the transmission capacity for a variety of TV service configurations, including sound and data services. While DVB-S and DVB-DSNG are strictly focused on the MPEG TS, DVB-S2 permits other input data formats (such as multiple TSs 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 (DTH) applications), and DVB-DSNG (for professional applications), and techniques such as adaptive 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 optimized 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.

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; discovered by Gallager in 1960 [14], but only today the improvement in chip technology allows high-speed implementation of sophisticated decoding algorithms in

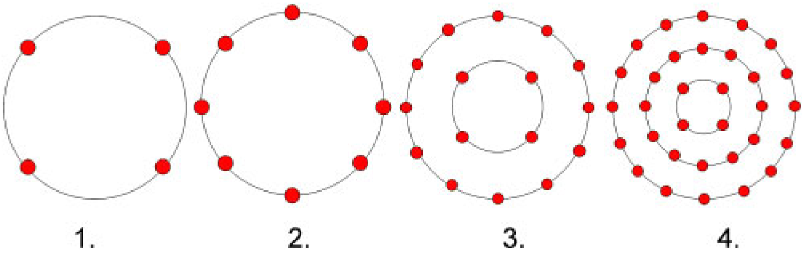


Figure 7. The 4 'wheel' modulation formats.

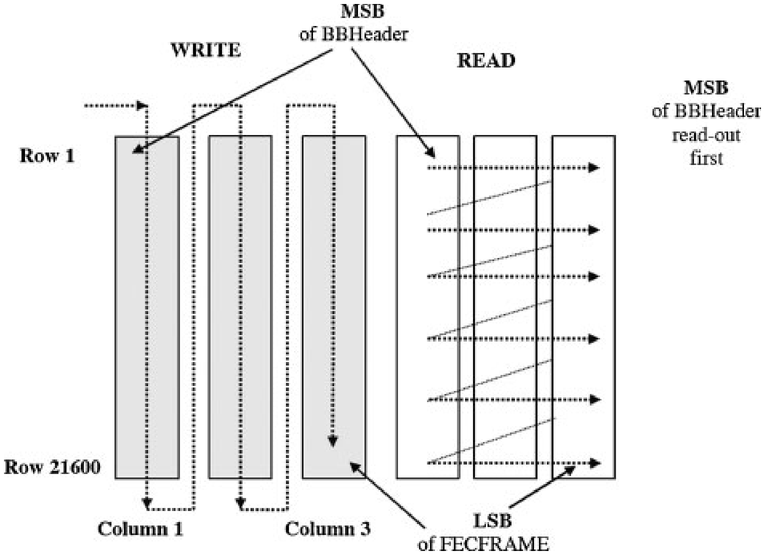


Figure 8. DVB-S2 bit-interleaving technique.

consumer products. They allow quasi-error-free operation at only 0.6–1.2 dB from the Shannon limit [15].

The encoding is performed in three sequential stages:

1. The parity check bits BCH_{FEC} of BCH outer code is appended to the baseband frame (BBFRAME), which is the payload of DVB-S2.
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 a function of the adopted modulation format.

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

Many coding rates are available according to the DVB-S2 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

Table I. Bit interleaver structure.

Modulation	Number of columns	Size of each column
8-PSK	3	21 600
16-APSK	4	16 200
32 APSK	5	12 960

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 also increases. Therefore, for applications that are 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-S2 modulation and coding schemes can be found in [16, 17].

In comparison to DVB-S2, the DVB-S and DVB-DSNG soft-decision Viterbi decoder takes decisions on blocks of only 100 symbols, without iterations, and the RS 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-S2 ACM is included as normative for the interactive application area and as optional for DSNG and professional services.

The standard recognizes that IP traffic is driving the design of interactive services in broadband systems. The new DVB-S2 standard seeks to improve IP performance and flexibility. It not only provides a mode that supports IP over the MPEG-2 TS, which is widely used in existing deployed networks (e.g. DVB-S, DVB-RCS) [6, 10], 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-S2 supporting the MPEG-2 TS mode is shown in Figure 9. In this figure, the BBFRAME, which is carrying one or more encapsulated packets, is padded and encoded to form a FECFRAME.

IP packets can be encapsulated over MPEG-2 networks using the multi-protocol encapsulation (MPE) [6]. The methods allow variable sized IP packets to be fragmented into a series of fixed-sized TS 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 [10].

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 packing of packets is not allowed (i.e. only one IP packet per TS packet). In [18, 19], the encapsulation efficiency has been studied, assuming different percentage of payload occupancy; the numerical results are shown in Table II.

DOI: 10.1002/sat

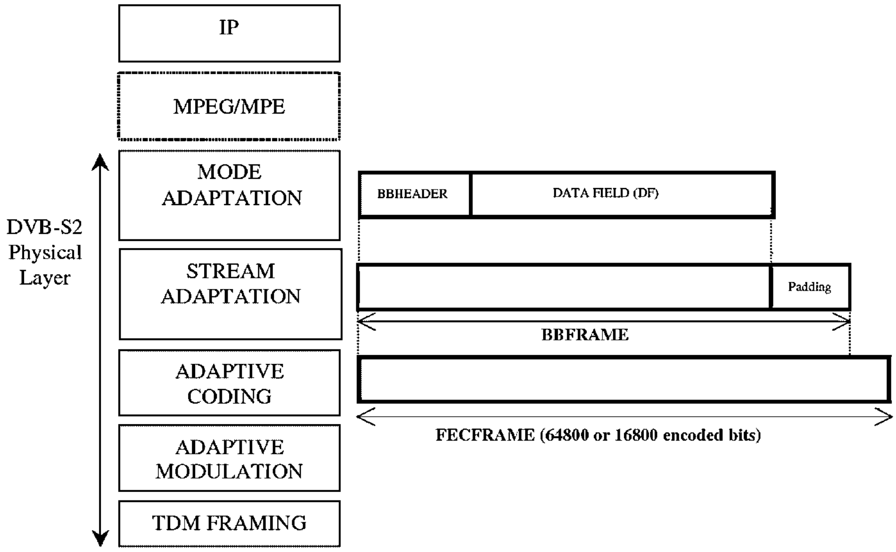


Figure 9. DVB-S2 encapsulation for IP packets.

Table II. Total DVB-S2 encapsulation efficiency as a function of percentages of payload occupancy.

	IP directly				MPE with packing				MPE without packing			
	Full	80%	50%	20%	Full	80%	50%	20%	Full	80%	50%	20%
Normal FECFRAME 64 800 bits	0.97	0.78	0.48	0.19	0.88	0.71	0.44	0.18	0.78	0.62	0.39	0.16
Short FECFRAME 16 800 bits	0.96	0.77	0.48	0.19	0.87	0.70	0.44	0.18	0.77	0.61	0.38	0.15

One of the implications of this flexibility is the multiplicity of solutions allowed in DVB-S2 for implementing ACM in interactive systems. DVB-S2 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, the coding scheme and modulation format may change frame by frame.

The DVB-S2 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. The generic mode supports generic streams, of constant or variable length packets. This permits different encapsulation protocols with improved efficiency to be used as an alternative to the MPE [16]. IP datagrams can also be directly mapped on the transmission frame.

To be fully compliant with the MPEG-2 specification for a TS, the TS mode of the DVB-S2 standard must deliver a constant rate TS with an invariant end-to-end delay. To map one/many constant bit-rate transport-stream(s) into a variable bit-rate ACM physical layer, the DVB-S2 modulator activates the subsystem called ‘null-packet deletion’. While a TS is characterized by constant bit rate, ACM is by definition a variable bit-rate transmission, trading-off user bit rate

DOI: 10.1002/sat

with FEC redundancy during rain fades. DVB-S2 allows Null TS Packets, which carry no useful information, to be removed at the input interface and re-introduced at the output of a receiver, preserving the end-to-end timing of the MPEG-2 TS. 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 utilized 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-S2 modulator for a specific portion of input data. The utilization of the ACM command interface allows for system configuration, which is completely transparent to the selected physical layer scheme. This is performed by a unit external to the DVB-S2 modulator, which uses the ACM command to signal 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-S2 modulator input interfaces are allowed 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 the information necessary to fill the data field frame by frame. The set of information bits are indicated and transmitted in one physical layer frame (PLFRAME) after FEC encoding, mapping, framing and modulation, For a single stream, only slicing 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 several 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, which are 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 STs, of the different priority levels and QoS requirements of the input queues, and finally of the information concerning the buffer occupation. The first information is needed to combine the same transmission parameters in one frame packets; the second one is required to meet QoS requirements (maximum delay, minimum rate, etc.); and finally, the third one can be used, for example, to satisfy QoS requirements without sacrificing in the presence of scarce traffic associated to a certain physical layer mode.

Multiple (*generic or transport*) *streams*: According to the system configuration, the DVB-S2 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-S2 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. The merger can be configured to be external to the DVB-S2 modulator. In this scenario, the ACM routing manager was responsible for the packets merging inside the scheduler. The merger can also be integrated into the DVB-S2 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 defined here, the buffer organization is definitely less complex than the one described previously. However, for simple first-in-first-out (FIFO) queues, where UPs are aggregated without any differentiation, some performance limitations can be present when adaptive systems are considered, as described in [18].

2.4. DVB-H

The need for a convergence and fusion between broadcasting of digital television and mobile communications has led to the introduction of DVB-H [20]. DVB-H is a standard that enables a mobile handheld device to receive data and live broadcast DTV. The term handheld device includes multimedia mobile phones with colour displays, personal digital assistants (PDAs) and pocket PC types of equipment. DVB-H adds portable and mobile capabilities to the terrestrial (DVB-T) standard [21]. In common to other DVB transmission systems based on the DVB TS, the DVB-H system although transmitting in only IP, uses a variant of the MPE [6]. Hence the base IP interface of DVB-H can be easily and effectively combined with other IP-based networks.

Figure 10 shows the network architecture of the DVB-H system. A DVB-H handheld terminal consist of two radio parts—one designed to receive unidirectional broadcasts of IP data casting (IPDC) content [22] and the other to provide bidirectional cellular services. The cellular network and the broadcast network can share the same core infrastructure. Hence apart from broadcast services, IP data services may also be accessed by the user *via* the DVB-H system but a return path *via* a different (here UMTS) network is required to deliver interactive services. As seen from Figure 10, DVB-H uses a separate air interface for service provisioning (mobile TV *vs* telephony) and this opens possible partnerships among broadcasters, content providers and network operators leading to several possible business models. For example, content creators and broadcasters can focus on programming, scheduling and creative production while the broadcast network operators can look into TV signal distribution, while at the same time, the cellular operators would be responsible for point-to-point communications, customer acquisition, and billing [20].

DVB-H defines a point to multipoint standard that requires speeds of approximately 128 to 384 kbps, making it possible to send between 25 and 80 channels over one multiplex (8 MHz/MuX), compared to 4–6 channels on DVB-T services. The DVB-H system is compatible with DVB-T spectrum allowing shared use of the DVB frequency bands—with no impact on the performance of cellular bands. In Europe, these extend from 470 to 862 MHz and in the US, the band 1670–1675 MHz has been proposed for use with DVB-H. DVB-H uses IP datacast to

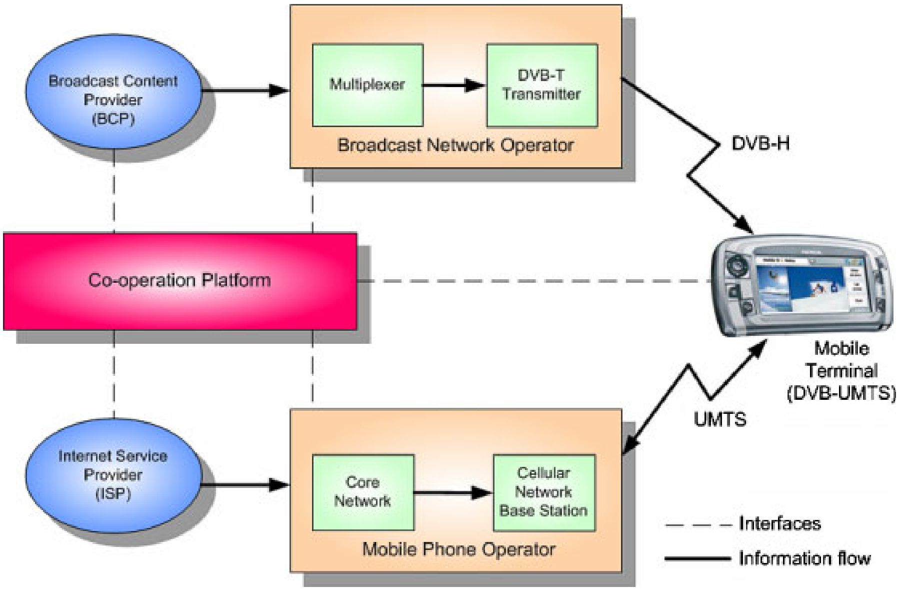

Broadcast Content Provider (BCP)
Multiplexer
DVB-T Transmitter
Broadcast Network Operator
DVB-H
Co-operation Platform
Mobile Terminal (DVB-UMTS)
UMTS
Internet Service Provider (ISP)
Core Network
Cellular Network Base Station
Mobile Phone Operator
Interfaces
Information flow

Figure 10. DVB-H network architecture.

deliver content in the form of data packets using the same distribution technique as the one used for delivering digital content on the Internet. The use of IP to carry its data including audio and video streams and web pages in IP packets, allows DVB-H to rely upon standard components and protocols for content manipulation, storage and transmission [23]. DVB-H-specific signalling has been integrated into the DVB service information (SI) specification [24].

The two main features of DVB-H are the delivery of data in bursts and the inclusion of FEC mechanisms [6]. This would lower consumption of battery power (hence longer battery life) and alleviate the radio impairment thereby improving the robustness even in difficult reception environments. These features are implemented in the link layer. Figure 11 shows the conceptual structure of a DVB-H receiver. It includes a DVB-H demodulator and a DVB-H terminal. The DVB-H demodulator includes a DVB-T demodulator, a time-slicing module and a MPE-FEC module [20].

2.4.1. Time-slicing. The battery life for any handheld device is critically important. DVB-H uses the method of time slicing to reduce the amount of power consumed by the handheld device. In this method, the data are delivered to the device in bursts at given time intervals. Hence audio/video data of a few seconds would be delivered in a single burst. When the receiver is not receiving any burst of data, the tuner in the device is 'inactive' and therefore would use less power. As the data bursts are buffered in a memory and continuously played, the user would not notice the period of inactivity. Time slicing could hence allow for up to a 95% reduction in energy consumption compared to conventional and continuously operating DVB-T tuners [25]. To indicate to the receiver when to expect the next burst, the time interval to the beginning of the next burst is indicated within the given burst [23].

DOI: 10.1002/sat

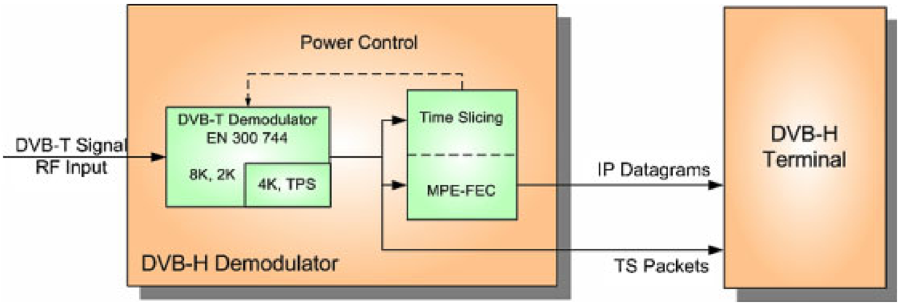


Figure 11. Conceptual structure of a DVB-H receiver.

In a standard DVB-T system [21], to provide a seamless handover (handover without a break in the service) to a user who moves from one cell to another, two radio receivers would be required on the mobile device (one to handle signals from each broadcast station). The time-slicing mechanism supports the possibility to use the same receiver to monitor neighbouring cells during the off-times (between bursts). Hence by switching of the reception from one TS to another during an off period it is possible to achieve seamless handover without the need of a second receiver.

2.4.2. MPE-FEC (*multi-protocol encapsulation/forward error correction*). A robust transmission system with an efficient error protection mechanism is required for handheld devices to facilitate reliable transmission in poor signal reception conditions. DVB-H offers improved transmission robustness through the use of FEC at the MPE layer. The objective of the MPE-FEC is to improve the Doppler performance and the carrier-to-noise (C/N) ratio in mobile channels and to improve the impulse noise transmission. The MPE-FEC processing is located on the link layer at the level of the IP input streams before they are encapsulated by using MPE [23].

Using the MPE-FEC protocol allows for RS data to be delivered over the broadcast network in special FEC sections (using virtual interleaving). Broadcast receivers that are not equipped to handle MPE-FEC data simply ignore the FEC sections. This method of error correction serves to enhance service quality and reception in the DVB-H system, even when the signal is being received under difficult conditions, *via* the handset's small in-built antenna. The IP input streams provided by different sources as individual elementary streams are multiplexed according to the time-slicing method. The IP datagrams are delivered in MPE sections in the same order as they are received. The MPE-FEC parity information is calculated for each individual stream. This parity information is sent in separate MPE-FEC sections, which helps in retrieving datagrams after MPE-FEC decoding despite bad reception condition.

Figure 12 shows the frame structure for MPE-FEC highlighting the application and RS data table. The MPE-FEC scheme consists of a RS code in conjunction with a block interleaver. The MPE-FEC encoder creates the FEC frame, including the incoming data. The FEC frame consists of a maximum of 1024 rows and a constant number of 255 columns; every frame cell corresponds to one byte, the maximum frame size is approximately 2 Mbit [26]. The frame is separated into two parts, the application data table on the left (191 columns) and the RS data table on the right (64 columns). The application data table is filled with the IP packets of the service to be protected. The RS code is then applied to each row at a time and the party bytes are

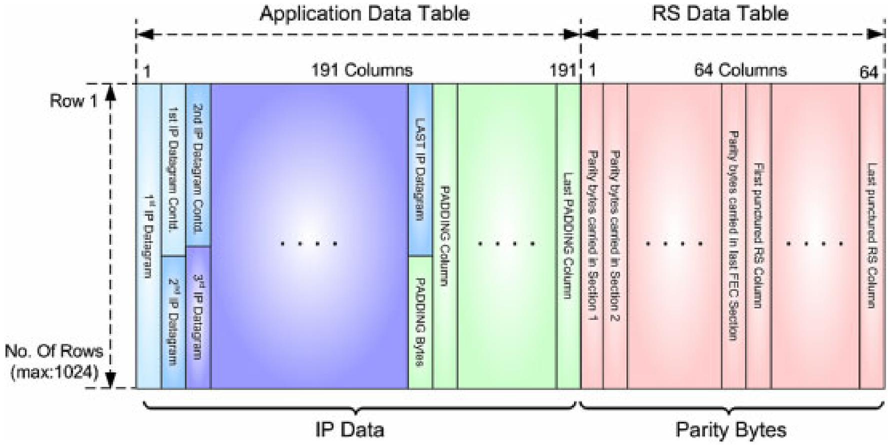


Figure 12. MPE-FEC frame structure.

put in the RS data table correspondingly. After this coding, the IP packets from the application data table are removed and encapsulated in IP sections using the standard encapsulation technique of MPE. After this the parity data are read from the RS data table each column at a time and encapsulated in separate FEC sections. The FEC frame structure also contains a 'virtual' block interleaving effect in addition to the coding [26].

The MPE-FEC overhead can be fully compensated by choosing a slightly weaker transmission code rate, while still providing far better performance than DVB-T (without MPE-FEC) for the same throughput. This MPE-FEC scheme should allow high-speed single antenna DVB-T reception using 8K/16-QAM or even 8K/64-QAM signals. In addition, MPE-FEC provides good immunity to impulse interference.

2.4.3. DVB-H physical layer. DVB-H can be transmitted using an OFDM transmission mode that is not part of the DVB-T specification. DVB-T already provides a 2K and an 8K mode for the optimum support of different network topologies. DVB-H allows a new 4K mode [27] to be used in addition which is created *via* a 4096-point inverse discrete Fourier transform (IDFT) in the OFDM modulator [23].

The 4K mode represents a compromise solution between the two other modes. As compared to the 2K mode, twice the transmitter distance in single frequency networks (SFNs) is allowed in the 4K mode and it is also less susceptible to the inverse effect of Doppler shifts which affects the 8K mode. In other words, the objective of the 4K mode is to improve network planning flexibility by trading off mobility and SFN size.

3. BROADBAND INTERNET AND MOBILE COMMUNICATIONS

3.1. Internet protocol

The IP is a connectionless network layer protocol designed for addressing and forwarding of IP packets (also known as IP datagrams). The Internet employs routers that provide the routing and forwarding of the IP packets to the destination host. If the final destination of the packet is not within the sending host's network, the packet will then be forwarded through the Internet, using the path determined by a routing algorithm (e.g. routing information protocol (RIP), open shortest path first (OSPF), border gateway protocol (BGP) [28]). Two versions of IP protocols have been standardized by the IETF (i.e. IPv4 and IPv6).

IPv4: In IPv4, an IP address is 32-bits long; hence, a total of 2^{32} possible addresses can be assigned. Every host or router that is connected to the Internet is assigned at least one IP address. In the IPv4 header, the source address is the sending host's source address and destination address is the designated host address, both of which remain unchanged throughout the transmission of the packet [28–30].

IPv6: IPv6 has addressed several limitations of IPv4. Some of the advantages of IPv6, are [28]:

- A larger address space, of 128 bits.
- A cleaner header format, designed to simplify and speed up routing.
- Improved support for mobility and other network extensions [28].

IP has become widely deployed, and it is increasingly important to consider supporting IP for future technologies. Most current and planned satellite systems already support IPv4 and many activities continue to develop and standardize the associated networking aspects [11, 31, 32]. 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 use only uni-directional links and mainly consist of utilizing a DVB-S forward link and DVB-RCS return link or additionally integrating with terrestrial networks [33].

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. Three notable research initiatives were: A North Atlantic Treaty Organization (NATO) education programme project, SILK, that pioneered the use of IPv6 over DVB-S utilizing the ULE specification [8]; and SATIP6 (an EC fifth framework programme (FP5) project) that assessed the issues in deployment of IPv6 over DVB-RCS, and SATSIX (an EC FP6 Project seeking to use IPv6 in combination with DVB-RCS and DVB-S2). IPv6 is planned as a work item of the ETSI BSM (broadband satellite multimedia) WG [31], which will include support for IPv6 protocols using the satellite-independent network interface [32].

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 minimize any impact on existing network users [34]. 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 [10, 33]. ULE supports a range of network layer packet formats, including native IPv6 and IPv6/MPLS [8]. 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.

3.2.1. 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 [35, 36]. 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 [34–36].

3.2.2. 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 [35, 36] 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 [37].
- *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 [34]. This method is not intended as a permanent solution, but as a start-up transition tool during the co-existence of IPv4 and IPv6 [38]. An example diagram is depicted in Figure 13 and a detailed description of this method is provided in [38].
- *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.[‡] ISATAP is designed to connect isolated IPv6 hosts and routers (nodes) within an

[‡] 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 [38]. However, it is not widely adopted and will not be further elaborated.

DOI: 10.1002/sat

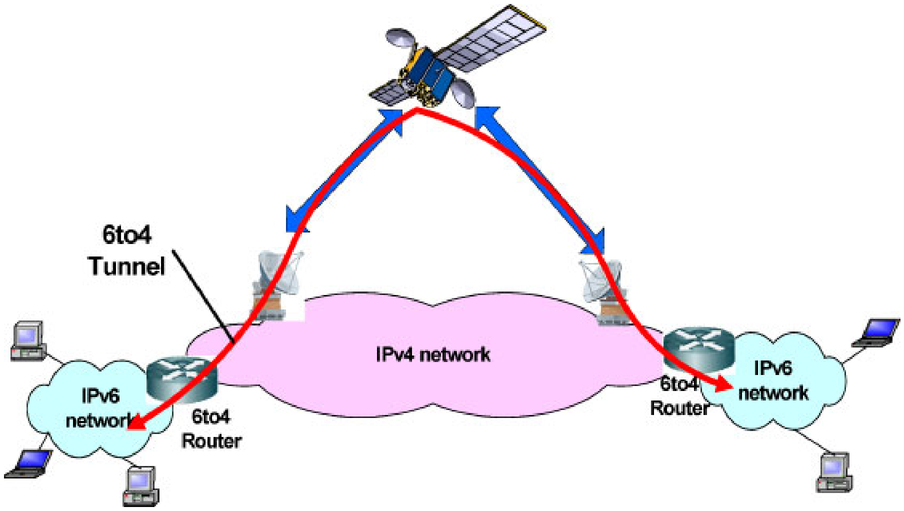


Figure 13. Migration of IPv4 to IPv6—6to4 tunnelling.

IPv4 site [39]. 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.

Further information on other tunnelling mechanisms, such as IPv6 over ATM and MPLS, Teredo, tunnel setup protocol, dual stack transition mechanism (DSTM), OpenVPN-based tunnelling solution, can be found in [34, 37, 40–42], respectively.

3.2.3. 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 [43]. An IP datagram travels through the SIIT translator, and it converts the datagram headers between IPv4 and IPv6, with the aid of temporarily assigned IPv4 addresses.
- *Network address translation-protocol translation (NAT-PT)/network address port translati on + packet translation (NAPT-PT)*: NAT-PT, defined in [44], 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

DOI: 10.1002/sat

translation approach, by moving the translation inside the individual hosts rather than performing the translation at a centralized server. The host is capable of translating between IPv4 and IPv6 internally by including the necessary segments in its IP stack [45]. 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 [46]. This allows the translation to be performed without the overhead of translating every packet's header [34].

Further information on other translation mechanisms, such as transport relay translator (TRT), SOCKS 64, is available in [47, 48].

3.3. *Mobile IP*

The widespread usage of the Internet has led to the extension of Internet access to consumers *via* different access technologies and it has also been widely acknowledged that this can be achieved through the implementation of mobile IP (MIP) since MIP provides the techniques to seamlessly roam between non-homogeneous networks. As such, MIP (i.e. MIPv4 and MIPv6) will play an important role in the research and development of future mobile communications systems. MIP implementation can mainly be categorized into: moving networks (i.e. mobile networks) and users' 'on the move' (i.e. user mobility), as illustrated in Figure 14.

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 [49, 50]. 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). Detailed information is available in [51, 52].

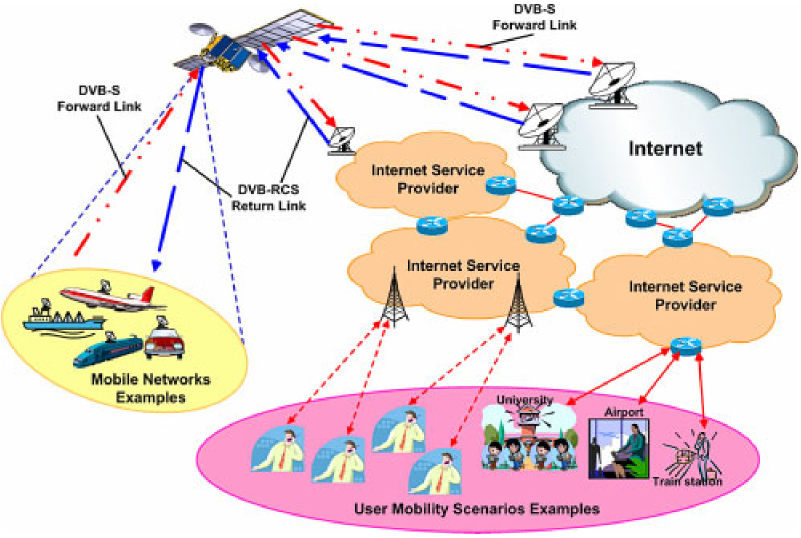


Figure 14. Example of mobile IP implementation scenarios.

DOI: 10.1002/sat

On the other hand, a mobile network, as stated in [53], is an entire mobile network that dynamically changes its point of attachment (POA) to the Internet. It can be made up of a single IP subnet or consists of several IP subnets. The main architectural components involved are mobile routers and mobile nodes (MNs), which are further elaborated in [53]. Much research has also been devoted to providing users with Internet access in a vehicular environment, such as in [49, 50]. Several research developments have been focused on supporting IP mobility for mobile networks, which utilizes 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 MN changes it POA, particularly when binding updates (BUs) 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 BU 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 [54, 55]. Nevertheless, basic concepts of MIP (i.e. MIPv4 and MIPv6) will be briefly discussed in Sections 3.3.1 and 3.3.2.

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 15, is a simple overview of the MIPv4 concept and detailed explanations are addressed in [56]. 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 of the 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 [54, 55, 57].

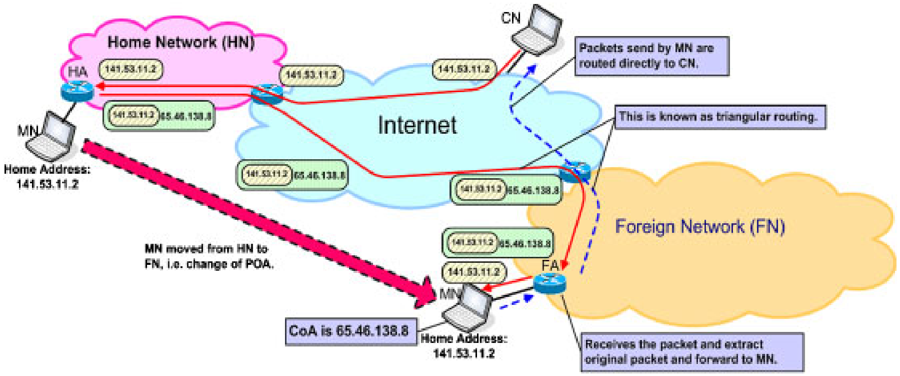


Figure 15. MIPv4 example.

DOI: 10.1002/sat

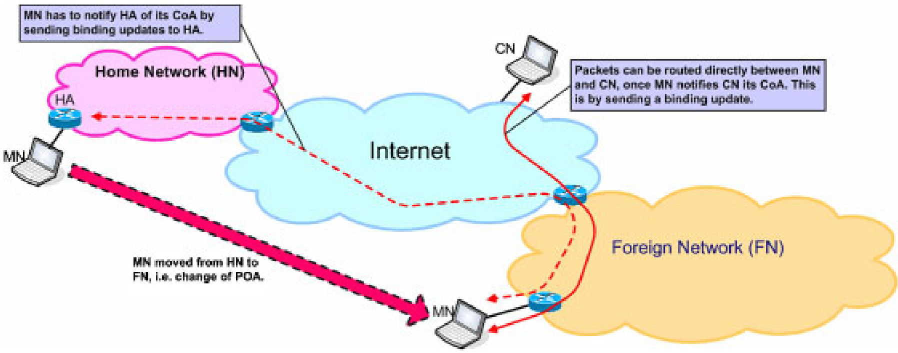

MN has to notify HA of its CoA by sending binding updates to HA.
Home Network (HN)
HA
MN
CN
Packets can be routed directly between MN and CN, once MN notifies CN its CoA. This is by sending a binding update.
Internet
Foreign Network (FN)
MN moved from HN to FN, i.e. change of POA.
MN

Figure 16. MIPv6 example.

3.3.2. Mobile IP version 6 (MIPv6). The issue of supporting IP mobility in IPv6 networks is known as mobile IPv6 (MIPv6) [58]. Basically, it contains 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 [58]. 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 optimization 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[§] cache and binding update. Further details are available in [58, 59]. An example of MIPv6 is depicted in Figure 16 and the review of MIPv6 proposals will be discussed next.

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 [54]. 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. MN) 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 BUs to its HA and all CNs whenever it changes its POA. The increase in network overhead introduces a performance constraint when supporting real-time services, especially when handover is being performed across heterogeneous networks. Therefore, much research and development has been focused on optimizing the handover performance by implementing localized mobility management (LMM) protocols [60], 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 minimize the packet losses and possible session loss. It

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

will also reduce the usage of the physical interface and network resources and improve protocol scalability.

- Avoid or minimize 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 IPv*6 (*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) [61]. 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 subnetwork; the global address (i.e. RCoA) remains unchanged [55]. 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. Soliman *et al.* [61] 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 [62]. 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 17. Further information on HMIPv6 is provided in [55, 61, 63].

*Fast handover for mobile IPv*6 (*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 [62]. 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 [64].

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

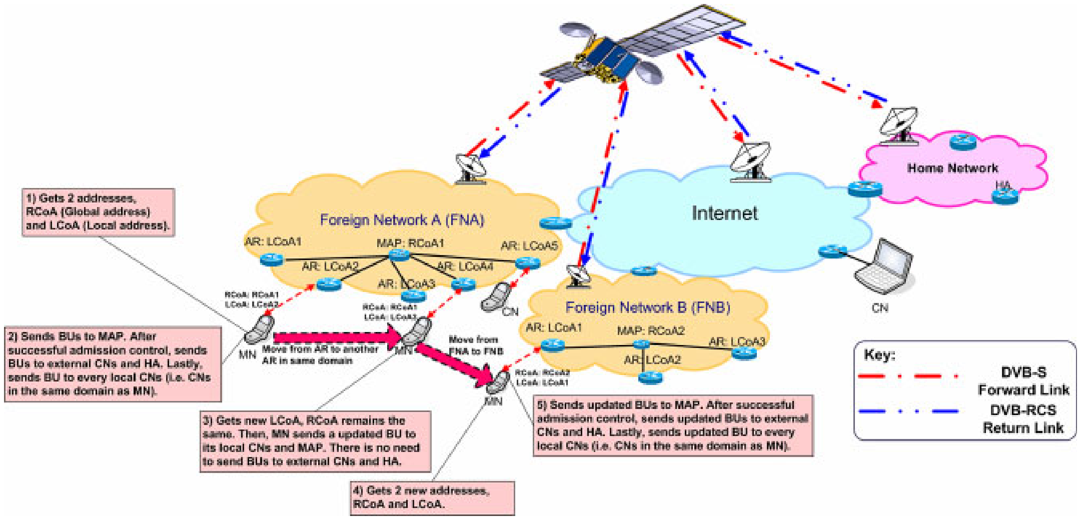

1) Gets 2 addresses, RCoA (Global address) and LCoA (Local address).
2) Sends BUs to MAP. After successful admission control, sends BUs to external CNs and HA. Lastly, sends BU to every local CNs (i.e. CNs in the same domain as MN).
3) Gets new LCoA, RCoA remains the same. Then, MN sends a updated BU to its local CNs and MAP. There is no need to send BUs to external CNs and HA.
4) Gets 2 new addresses, RCoA and LCoA.
5) Sends updated BUs to MAP. After successful admission control, sends updated BUs to external CNs and HA. Lastly, sends updated BU to every local CNs (i.e. CNs in the same domain as MN).
Foreign Network A (FNA)
AR: LCoA1
MAP: RCoA1
AR: LCoA5
AR: LCoA2
AR: LCoA4
AR: LCoA3
RCoA: RCoA1
LCoA: LCoA2
RCoA: RCoA1
LCoA: LCoA3
CN
MN
Move from AR to another AR in same domain
MN
Move from FNA to FNB
RCoA: RCoA2
LCoA: LCoA1
MN
Internet
Home Network
HA
CN
Foreign Network B (FNB)
AR: LCoA1
MAP: RCoA2
AR: LCoA3
AR: LCoA2
Key:
DVB-S Forward Link
DVB-RCS Return Link

Figure 17. Hierarchical mobile IPv6 (HMIPv6) example.

access router (PAR).[¶] The MN then sends a fast binding update[||] (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 18. In [62], two scenarios were depicted. The first is known as predictive fast handover, whereby the MN sends a FBU message and receives the 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 link. In this scenario, the FBU message is encapsulated in the fast neighbour message[**] (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 [62]. Studies on the performance of FMIPv6, HMIPv6 and the combination of implementing FMIPv6 and HMIPV6 are discussed in [65–67].

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 [68], 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.

[¶] The term previous access router (PAR) implies the current access router that MN is connected to prior to handover.

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

[**] 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 [62].

DOI: 10.1002/sat

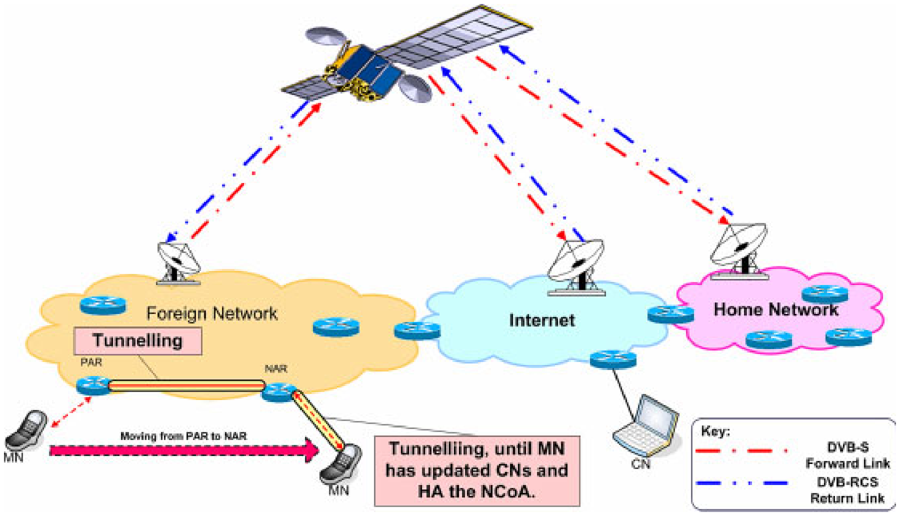


Figure 18. Fast handover for mobile IPv6 (FMIPv6) example.

In TeleMIP, it is assumed that the foreign network domain consists of several subnets and uses the intra-domain mobility management protocol (IDMP) [69] 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 BUs. 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 19 and the TeleMIP concept is further elaborated in [68, 70].

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-conditionalized' handoff scheme and auto-update micromobility protocol (AUM), and are addressed in [71–76], respectively.

3.4. *Session initiation protocol (SIP)*

Mobile IP is an efficient protocol when implemented for non-real time applications due to the delays experienced in the triangle routing of Mobile IP, particularly if the MN is far away from the HA. Even though this problem can be solved partially by the introduction of route

DOI: 10.1002/sat

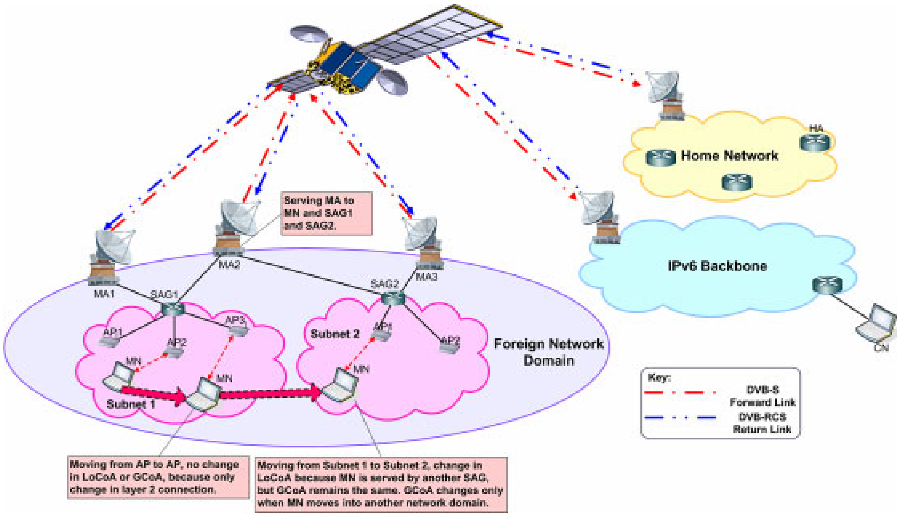

Serving MA to
MN and SAG1
and SAG2.
MA1
MA2
MA3
SAG1
SAG2
AP1
AP2
AP3
Subnet 2
AP1
AP2
MN
MN
MN
Subnet 1
Foreign Network
Domain
Home Network
HA
IPv6 Backbone
CN
Key:
DVB-S
Forward Link
DVB-RCS
Return Link
Moving from AP to AP, no change in LoCoA or GCoA, because only change in layer 2 connection.
Moving from Subnet 1 to Subnet 2, change in LoCoA because MN is served by another SAG, but GCoA remains the same. GCoA changes only when MN moves into another network domain.

Figure 19. Telecommunications-enhanced mobile IP (TeleMIP) example.

optimization, this method increases the complexity of the corresponding nodes since this node will be required to encapsulate IP packets and also maintain a list of CoA of all mobile nodes. In recent years, the development of a SIP-based mobility management protocol has been proposed to solve this problem for real-time applications [77]. However, since SIP is not capable of providing mobility support for TCP connections, Mobile IP may still be required for this.

SIP [78] is generally used for creating, modifying and terminating multimedia sessions. SIP consists of four major components: SIP user agents, SIP registrar servers, SIP proxy servers and SIP redirect servers. The functionalities of all the components are described below:

- *SIP user agents* (*UA*): These are user devices that have SIP capabilities. Therefore, they can initiate or receive SIP calls.
- *SIP registrar servers*: This is a database that maintains the location of the users in a particular domain. Therefore, when considered for mobility management, this is analogues to the HA in mobile IP.
- *SIP proxy server*: This server receives invitations from the UA and queries the SIP registrar server to obtain the current location of the UA. If the recipient is in the same domain, the invitation will be sent directly to the UA. Otherwise, it will be forwarded to the proxy server of the recipient UA.
- *SIP redirect server*: The redirect server allows the proxy servers to direct SIP invitations to external domains.

In contrast to mobile IP, in which users maintain a fixed IP address, a SIP user is addressed using an e-mail like address such as user@satnex.org. As such, SIP is a suitable protocol for personal mobility because users can be reached at any location or terminal irrespective of the IP address. When the users move to another location, a SIP register message can be sent to the SIP registrar to inform it of its current location/bindings. This will allow messages to be rerouted to the user's current location.

DOI: 10.1002/sat

In Release 5 of UMTS [79], several new network entities are introduced to support multimedia applications or services, known as the IP multimedia CN subsystem (IMS). All these entities have been introduced in the core network and use SIP for supporting multimedia services. The main elements of IMS are the proxy call state control function (P-CSCF), interrogating-CSCF (I-CSCF) and serving-CSCF (S-CSCF). P-CSCF is located in the same network of the visited or home GPRS gateway support node (GGSN) and is the first contact point of the IMS. P-CSCF is responsible for selecting the I-CSCF of the home network. I-CSCF is the main entrance of the home network and selects the appropriate S-CSCF. The actual control of the session is handled by the S-CSCF. S-CSCF handles SIP messages, requests the establishments of bearers and forwards the requests to other external S-CSCFs.

In addition, there are also several other entities that are defined for interconnection with legacy networks. This includes the media gateway control function (MGCF), IM media gateway (IM-MGW), breakout gateway control function (BGCF) and signalling gateways. The functionalities of these entities are listed below:

- *Media gateway control function* (*MGCF*): Responsible for signalling and media interworking between PS and CS domains, performs protocol conversion between the ISDN user part (ISUP), or the bearer-independent call control (BICC) and SIP protocols.
- *IM media gateway* (*IM-MGW*): Provides user-plane link between circuit-switched (CS) domains and IMS.
- *Breakout gateway control function* (*BGCF*): Responsible for selecting the public-switched telephone network (PSTN) network that a session should be forwarded when a breakout to the CS domain occurs. Forwards the session signalling to the appropriate MGCF and BGCF in the destination PSTN.
- *Signalling gateway*: Interconnect different signalling networks.

In Release 5, the home location register (HLR) is also changed to home subscriber server (HSS) to emphasize the fact that this database contains not only location-related data but also subscription-related data, like the list of services the user is able to obtain and the associated parameters [79]. In order to start an IMS session, a packet data protocol (PDP) context (packet-switched-domain bearer) has to be established first to convey the IMS signalling. SIP is then used for multimedia call control. The network architecture for Release 5 is shown in Figure 20.

4. SECURITY ISSUES IN DVB SYSTEMS

4.1. Introduction

The ETSI Broadband Satellite Multimedia (BSM) workgroup is responsible for producing specifications, standards and deliverables for broadband satellite multimedia, discussing issues such as [80]:

- Definition of satellite system architectures supporting broadband services.
- Service requirements and descriptions for broadband communications systems.

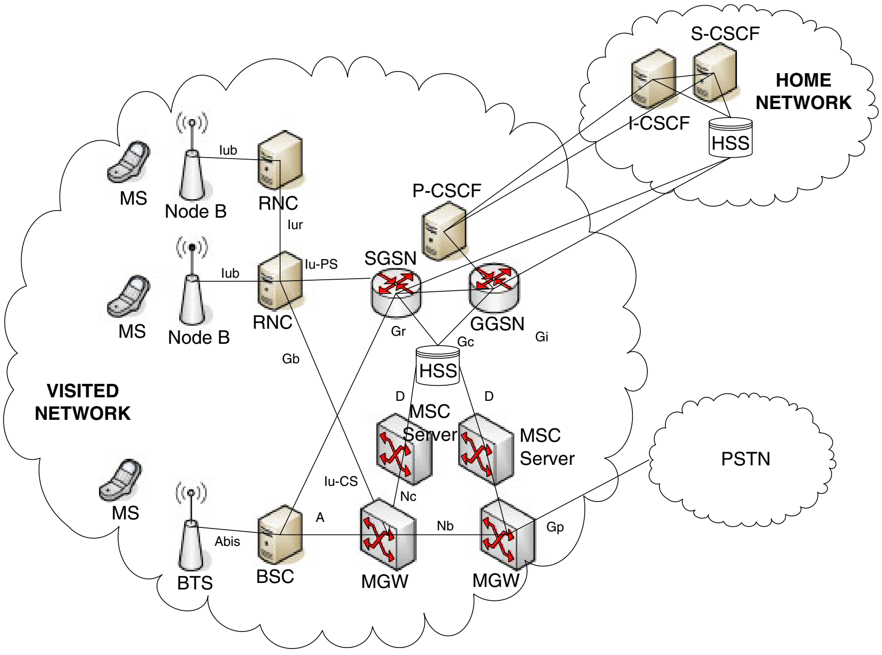


Figure 20. UMTS network architecture (release 5).

- Definition of network architectures and interface protocols leading to air interface standards and user terminal specifications.

Moreover, the workgroup also intends to promote [80]:

- Interoperability between satellite networks and other networks by producing specifications that addresses this topic.
- Adequate representation of BSM-specific issues in other technical fora.

The significance of security within satellite system, such as DVB systems, has been recognized by the ETSI BSM workgroup, and a framework has also been established for addressing security issues in a BSM network. The BSM architecture mainly consists of the satellite-independent upper layer and satellite-dependent lower layer. The satellite-independent upper layers comprises a set of common IP networking functions, such as IP addressing, QoS. The satellite-dependent lower layer consists of satellite-specific functionalities and an example is DVB systems. Both layers are associated *via* a satellite-independent interface known as the satellite-independent service access point (SI-SAP). An overview of the BSM protocol stack is shown in Figure 2 of the second part of this paper, *Future service scenarios* and further description of the SI-SAP and the BSM system is available in [32, 81], respectively. The security layer in the BSM protocol stack is shown in Figure 21 and additional details are provided in [82].

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

DOI: 10.1002/sat

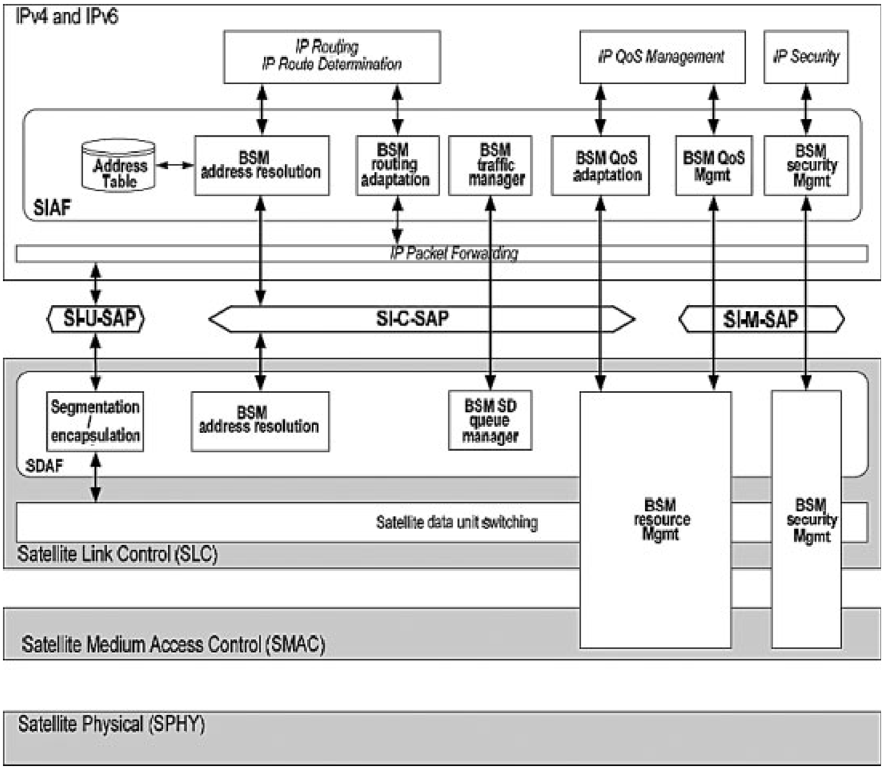


Figure 21. Security layer in BSM protocol stack [82].

applications if they are implemented at the application level, or 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 STs are authenticated.
- Only satellite link traffic can be encrypted and digitally signed.

Security services can be provided at the link layer such as the 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

The ATM Forum has defined four security services, in the ATM security specifications [83] 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 standardized by the ATM Forum as the universal test and 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 standardized 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 done on securing satellite ATM. There are several technical challenges that need to be evaluated carefully for securing ATM satellites such as the encryption synchronization 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

DOI: 10.1002/sat

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 CA system used in the DVB system [6, 84] 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 CW or using separate CWs 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 the process 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 DTV, 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-bytes packets for transmission, at which point it is called the DVB MPEG-2 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.

A general architecture is shown in Figure 22. 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 CA system that is composed of several specific modules:

- *The scrambler*: Scrambles the payload of the packets composing the transport stream, using a CW generated by the CW 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.

DOI: 10.1002/sat

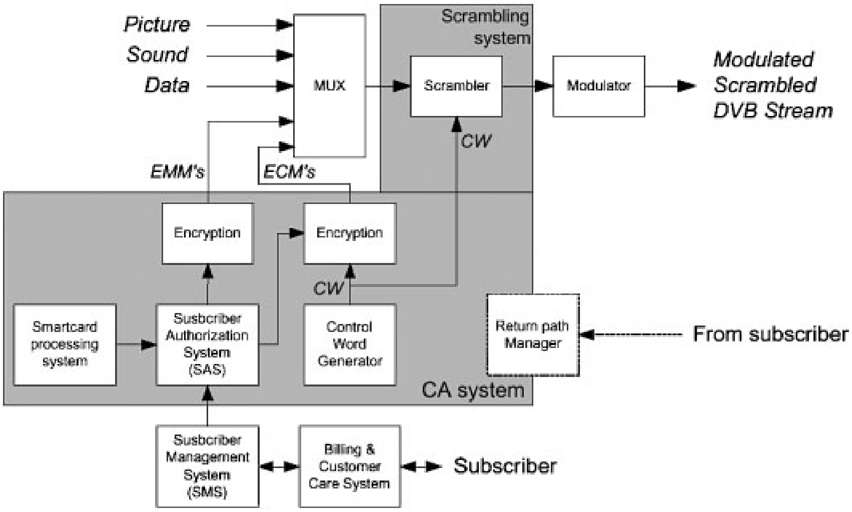


Figure 22. General architecture for conditional access system.

- *The CW generator that creates the CWs*: Two encryption engines (often implemented by the same software) are used to encrypt the content of the EMMs and the CWs 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 CA 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 CA 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 CW that is fed into the DVB descrambler, allowing the TS 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 CW. It is this CW that is the key to the DVB TS 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.

DOI: 10.1002/sat

4.4. DVB-RCS security

As specified in [3], 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 this is not necessary (it would just add an additional protection to the entire control stream for non-subscribers). This concept is shown in Figure 23.

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. 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 CW 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 can be transparent if implemented in the lower layers.

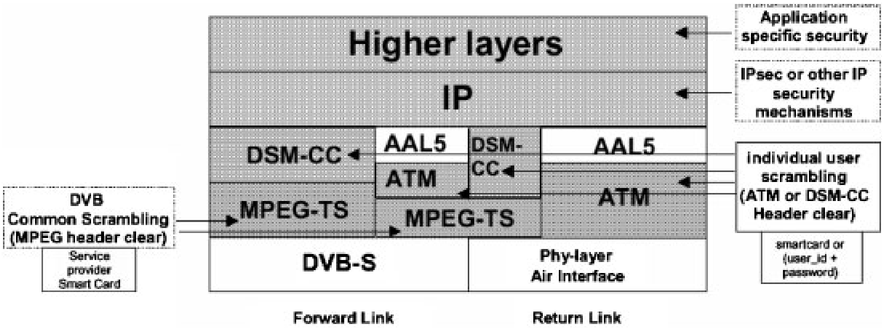

Higher layers
IP
DSM-CC
AAL5
DSM-CC
AAL5
ATM
ATM
MPEG-TS
MPEG-TS
DVB-S
Phy-layer Air Interface
Application specific security
IPsec or other IP security mechanisms
individual user scrambling (ATM or DSM-CC Header clear)
smartcard or (user_id + password)
DVB Common Scrambling (MPEG header clear)
Service provider Smart Card
Forward Link
Return Link

Figure 23. Security layers for satellite interactive network.

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 [85] can also be used to provide satellite network security by implementing IPSec tunnels. The major advantage of IPSec is its wide implementation in IP routers and hosts. Though IPSec can be used to provide security over the satellite networks, it has several disadvantages [86]. Some of these are:

- The extra IP header (IPv4 or IPv6) introduces large packet overheads when IPSec is used in tunnel mode.
- IPSec is incompatible with TCP performance enhancing proxies (PEP) [87] that are usually used in satellite networks to increase TCP performance.
- IPSec can be used to secure only IP datagrams and cannot be used to provide security services for any other network protocols that may need to be transported over the satellite network (like Ethernet Frames, MPLS, ATM, etc.).
- IPSec is incompatible with NAT when used in transport mode.
- Data confidentiality is only provided for the IP payload and not for the complete IP Packets, i.e. the outer IP header is not secured. Hence the IPSEC tunnel end points are not hidden. This could be used for passive security attacks life traffic analysis.

Table III provides a summary of the major advantages and disadvantages of security in each layer of the broadband satellite protocol stack.

Table III. Security layers comparison.

	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 IV. Security services at various protocol layers.

	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

DOI: 10.1002/sat

Also the security services that can be provided in layer of the BSM protocol stack are summarized in Table IV. Table IV 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 significant development in areas related to DVB satellite systems. This paper outlines the main characteristics and issues of the DVB satellite systems and the importance of IP services, as mobile communications progresses towards achieving a ubiquitous Internet network. This tutorial has described the various DVB satellite systems, i.e. DVB-S, DVB-RCS and DVB-S2. 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*.

APPENDIX: ACRONYMS AND ABBREVIATIONS

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 Systems 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
BGCF	breakout gateway control function
BIA	bump in the API
BICC	bearer-independent call control
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

DOI: 10.1002/sat

CRA	continuous rate assignment
CS	circuit switched
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-S2	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
GGSN	GPRS gateway support node
GPRS	general packet radio service
HA	home agent
HAWAII	handoff-aware wireless access Internet infrastructure
HDTV	high definition television
HLR	home location register
HMIP	hierarchical mobile IP
HMIPv6	hierarchical mobile IPv6
HSS	home subscriber server
I-CSCF	interrogating-CSCF

DOI: 10.1002/sat

IC	integrated circuit
ICMP	Internet control message protocol
IDFT	inverse discrete fourier transform
IDMP	intra-domain mobility management protocol
IETF	Internet Engineering Task Force
IM-MGW	IM media gateway
IMS	IP multimedia CN subsystem
IP	Internet protocol
IPDC	IP data casting
IPSec	Internet protocol security
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 Organization
ISP	Internet service provider
ISUP	ISDN user part
ITU	International Telecommunication Union
ITV	interactive TV
LAN	local area network
LCoA	on-link care-of-address
LDPC	low density parity check codes
LMM	localized 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
MGCF	media gateway control function
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 Organization
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
P-CSCF	proxy call state control function
PAR	previous access router
PCoA	previous CoA
PDA	personal digital assistant
PDP	packet data protocol
PEP	performance enhancing proxies
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
PSTN	public-switched telephone network
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
RS	Reed-Solomon
RtSolPr	router solicitation for proxy advertisement
S-CSCF	serving-CSCF
SAGs	subnet agents
SAR	segmentation and reassembly
SAS	subscriber authorization system
SFN	single frequency network
SI	service information
SIP	session initiation protocol
SI-SAP	satellite-independent service access point
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	synchronization
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
UA	SIP user agents
UDP	user datagram protocol
ULE	ultra lightweight encapsulation
UPs	user packets
USB	universal serial bus
UTOPIA	universal test and operations physical interface for ATM level 2
VBDC	volume-based dynamic capacity
VC	virtual connection
VCM	variable coding and modulation
VoD	video-on-demand
VoIP	voice over IP
Wi-Fi	wireless fidelity

ACKNOWLEDGEMENTS

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.

REFERENCES

1. ETSI EN 302 307 (V1.1.1). Digital video broadcasting (DVB); second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, new gathering and other broadband satellite applications. *ETSI EN 302 307* (*V1.1.1*), March 2005.
2. ETSI EN 301 958 (V1.1.1). Digital video broadcasting (DVB); interaction channel for digital terrestrial television (RCT) incorporating multiple access OFDM. *ETSI EN 301 958* (*V1.1.1*), March 2002.
3. ETSI EN 301 790 (V1.4.1). Digital video broadcasting (DVB); interaction channel for satellite distribution systems. *ETSI EN 301 790* (*V1.4.1*), April 2005.
4. ISO/IEC IS 13818-1. Information technology—generic coding of moving pictures and associated audio information—Part 1: Systems. *ISO/IEC* IS 13818-1, 2000.
5. ETSI EN 300 421 (V1.1.2). Digital video broadcasting (DVB); framing structure, channel coding and modulation for the 11/12 GHz satellite services. *ETSI EN 300 421* (*V1.1.2*), August 1997.
6. ETSI EN 301 192 (V1.4.1). Digital video broadcasting (DVB); DVB specification for data broadcasting. *ETSI EN 301 192* (*V1.4.1*), November 2004.
7. IP over DVB (ipdvb) Working Group, Internet Area, Internet Engineering Task Force (IETF). Available from: http://www.ietf.org
8. Fairhurst G, Collini-Nocker B. Unidirectional lightweight encapsulation (ULE) for transmission of IP datagrams over an MPEG-2 transport stream (TS). *IETF RFC 4326*, December 2005.
9. Deering S, Hinden R. Internet protocol, version 6 (IPv6) specification. *IETF RFC 2460*, December 1998.
10. Montpetit M-J, Fairhurst G, Clausen HD, Collini-Nocker B, Linder H. A framework for transmission of IP datagrams over MPEG-2 networks. *IETF RFC 4259*, November 2005.
11. The SatLabs Group. Available from http://www.satlabs.org
12. ETSI EN 301 210 (V1.1.1). Digital video broadcasting (DVB); framing structure, channel coding and modulation systems for digital satellite news gathering (DSNG) and other contribution application by satellite. *ETSI EN 301 210* (*V1.1.1*), March 1999.

DOI: 10.1002/sat

13. Wood D. The DVB project: philosophy and core system. *Electronics and Communications Engineering Journal* 1997; **9**(1):5–10.
14. Gallager RG. Low density parity check codes. *IEEE Transactions on Information Theory* 1962; **8**(1):21–28.
15. 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.
16. 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.
17. 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, 30 September–2 October 2004.
18. 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.
19. Vazquez-Castro MA, Cardoso A, Rinaldo R. Encapsulation and framing efficiency of DVB-based satellite adaptive systems. *Proceedings of VTC 2004*, Milan, Italy, 17–19 May 2004.
20. ETSI EN 302 304 v1.1.1 (2004-11). Digital video broadcasting (DVB); transmission system for handheld terminals (DVB-H). *ETSI EN 302 304 v1.1.1* (*2004-11*).
21. ETSI EN 300 744 v1.5.1 (2004-11). Digital video broadcasting (DVB); framing structure, channel coding and modulation for digital terrestrial television. *ETSI EN 300 744 v1.5.1* (*2004-11*).
22. May G. The IP datacast system—overview and mobility aspects. *Proceedings of IEEE International Symposium on Consumer Electronics*, New York, U.S.A., 1–3 September 2004; 509–514.
23. ETSI TR 102 377 v1.1.1 (2005-02). Digital video broadcasting (DVB); DVB-H implementation guidelines. *ETSI TR 102 377 v1.1.1* (*2005-02*).
24. ETSI EN 300 468 v1.6.1 (2004-11). Digital video broadcasting (DVB); specification for service information (SI) in DVB systems. *ETSI EN 300 468 v1.6.1* (*2004-11*).
25. Digital Terrestrial Television Action Group. Television on a handheld receiver—broadcasting with DVB-H. Available from: http://www.digitag.org/DVBHandbook.pdf (Accessed on 15 September 2005).
26. Kornfeld M, Reimers U. DVB-H—the emerging standard for mobile data communication. *EBU Technical Review*, *No. 301*, January 2005. Available from: http://www.ebu.ch/en/technical/trev/trev_301-dvb-h.pdf (Accessed on 25 October 2005).
27. Jaekel T. Testing of DVB-H system. November 2004. Available from: http://www.broadcastpapers.com/testmeasurement/DiBroCDVBTest01.htm (Accessed on 25 October 2005).
28. Forouzan BA. *TCP/IP Protocol Suite* (2nd edn). McGraw-Hill: London, 2003.
29. Postel J. Internet protocol. *IETF RFC 791*, September 1981.
30. Kurose JF, Ross KW. *Computer Networking*: *A Top-Down Approach Featuring the Internet* (3rd edn). Addison-Wesley: London, 2005.
31. Broadband Satellite Multimedia (BSM) Working Group. Satellite earth stations and systems (SES), European Telecommunications Standards Institute (ETSI). Available from http://www.etsi.org
32. ETSI TR 102 353 (V1.1.1). Satellite earth stations and systems (SES); broadband satellite multimedia (BSM); guidelines for the satellite independent service access point (SI-SAP). *ETSI TR 102 353* (*V1.1.1*), November 2004.
33. Preparation for IPv6 in Satellite Communications. *ESA Contract Report Number 17629/03/NL/ND*, July 2004.
34. 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.
35. Gilligan R, Nordmark E. Transition mechanisms for IPv6 hosts and routers. *IETF RFC 2893*, August 2000.
36. Nordmark E, Gilligan RE. Basic transition mechanisms for IPv6 hosts and routers. *IETF RFC 4213*, October 2005.
37. Durand A, Fasano P, Guardini I, Lento D. IPv6 tunnel broker. *IETF RFC 3053*, January 2001.
38. Carpenter B, Moore K. Connection of IPv6 domains via IPv4 clouds. *IETF RFC 3056*, February 2001.
39. Templin F, Gleeson T, Talwar M, Thaler D. Intra-site automatic tunnel addressing protocol (ISATAP). *IETF RFC 4214*, October 2005.
40. Huitema C. Teredo: tunneling IPv6 over UDP through NATs. *IETF Internet Draft*, draft-huitema-v6ops-teredo-05.txt, October 2005.
41. Bound J. Dual stack IPv6 dominant transition mechanism (DSTM). *IETF Internet Draft*, draft-bound-dstm-exp-02.txt, June 2005.
42. IST FP 6NET. Updated IPv4 to IPV6 transition cookbook for end site networks/universities. Deliverable D2.3.3-bis, project website: http://www.6net.org/publications/deliverables/D2.3.3.pdf
43. Nordmark E. Stateless IP/ICMP Translation Algorithm (SIIT). *IETF RFC 2765*, February 2000.
44. Tsirtsis G, Srisuresh P. Network address translation—protocol translation (NAT-PT). *IETF RFC 2766*, February 2000.
45. Tsuchiya K, Higuchi H, Atarashi Y. Dual stack hosts using the bump-in-the-stack technique (BIS). *IETF RFC 2767*, February 2000.
46. Lee S, Chin M-K, Kim Y-J, Nordmark E, Durand A. Dual stack hosts using 'bump-in-the-API' (BIA). *IETF RFC 3338*, October 2002.

DOI: 10.1002/sat

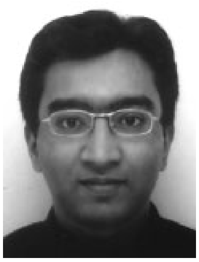
47. Hagino J, Yamamoto K. An IPv6-to-IPv4 transport relay translator. *IETF RFC 3142*, June 2001.
48. Kitamura H. A SOCKS-based IPv6/IPv4 gateway mechanism. *IETF RFC 3089*, April 2001.
49. Liang X, Ong FLC, Chan PML, Sheriff RE, Conforto P. Mobile Internet access for high-speed trains via heterogeneous networks. *Proceedings of 14th IEEE 2003 International Symposium on Personal*, *Indoor and Mobile Radio Communications* (*PIMRC 2003*), Beijing, China, 7–10 September 2003; 177–181.
50. 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.
51. IST FP Fast Internet for Fast Train Hosts. *System Specification Document*, *Deliverable D3*, project website: http://www.fifth.it
52. Carneiro G, Ruela J, Ricardo M. Cross-layer design in 4G wireless terminals. *IEEE Wireless Communications* 2004; **11**(2):7–13.
53. Manner J, Kojo M. Mobility related terminology. *IETF RFC 3753*, June 2004.
54. Reinbold P, Bonaventure O. IP micro-mobility protocols. *IEEE Communications Surveys and Tutorials Magazine* 2003; **5**(1):40–57.
55. Campbell AT, Gomez-Castellanos J. IP micro-mobility protocols. *ACM SIGMOBILE Mobile Computing and Communications Review* 2000; **4**(4):45–53.
56. Perkins C. IP mobility support for IPv4. *IETF RFC 3344*, August 2002.
57. 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.
58. Johnson D, Perkins C, Arkko J. Mobility support in IPv6. *IETF RFC 3775*, June 2004.
59. Nikander P, Arkko J, Aura T, Montenegro G, Nordmark E. Mobile IP version 6 route optimization security design background. *IETF RFC 4225*, December 2005.
60. Williams C. Localized mobility management goals. *IETF Internet Draft*, draft-ietf-mipshop-lmm-requirements-03.txt, January 2005, Work in progress.
61. Soliman H, Catelluccia C, El Malki K, Bellier L. Hierarchical mobile IPv6 mobility management (HMIPv6). *IETF RFC 4140*, August 2005.
62. Koodli R. Fast handovers for mobile IPv6. *IETF RFC 4068*, July 2005.
63. Castelluccia C. HMIPv6: a hierarchical mobile IPv6 proposal. *ACM SIGMOBILE Mobile Computing and Communications Review* 2000; **4**(1):48–59.
64. McCann P. Mobile IPv6 fast handovers for 802.11 networks. *IETF RFC 4260*, November 2005.
65. 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, 17–21 November 2002; 2488–2492.
66. 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, 17–19 June 2002; 100–105.
67. 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.
68. 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.
69. 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.
70. 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, 11–15 June 2001; 2488–2493.
71. O'Neill A, Tsirtsis G, Corson S. Edge mobility architecture. *IETF Internet Draft*, draft-oneill-ema-02.txt, July 2000, Expired draft.
72. O'Neill A, Tsirtsis G, Corson S. EMA enhanced mobile IPv6/IPv4. *IETF Internet Draft*, draft-oneill-ema-mip-00.txt, July 2000, Expired draft.
73. Shelby ZD, Gatzounas D, Campbell A, Wan C-Y. Cellular IPv6. *IETF Internet Draft*, draft-shelby-cellularipv6-01.txt, July 2001, Work in progress.
74. Fu XM, Karl H, Kappler C. QoS-conditionalized handoff for mobile IPv6. *Proceedings of 2nd IFIP-TC6 International Networking Conference*, *NETWORKING 2002*, Pisa, Italy, 19–24 May 2002; 721–730.
75. 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, 26 September–1 October 2004; 72–78.
76. Sharma A, Ananda AL. A protocol for micromobility management in next generation IPv6 networks. *Proceedings of LCN 2004*, Tampa, FL, 16–18 November 2004; 435–436.
77. Wedlund E, Schilzrinne H. Mobility support using SIP. *Proceedings of 2nd ACM International Workshop on Wireless Mobile Multimedia*, Seattle, WA, 20 August 1999; 76–82.

78. Rosenberg J, Schulzrinne H, Camarillo G, Johnston A, Peterson J, Sparks R, Handley M, Schooler E. SIP: session initiation protocol. *IETF RFC 3261*, June 2002.
79. 3GPP TSG RAN #20 (V0.10). Overview of 3GPP release 5: summary of all release 5 features. *3GPP TSG RAN #20* (*V0.10*), June 2003.
80. ETSI TR 101 374-2 (V1.1.1). Satellite earth stations and systems (SES); broadband satellite multimedia–Part 2: Scenario for standardisation. *ETSI TR 101 374-2* (*V1.1.1*), March 2000.
81. ETSI TR 101 984 (V1.1.1). Satellite earth stations and systems (SES); broadband satellite multimedia; services and architectures. *ETSI TR 101 984* (*V1.1.1*), November 2002.
82. ETSI TR 102 287 (V1.1.1). Satellite earth stations and systems (SES); broadband satellite multimedia (BSM); IP interworking over satellite; security aspects. *ETSI TR 102 287* (*V1.1.1*), May 2004.
83. ATM Forum Technical Committee. *ATM Security Specification Version 1.1*: *af-sec-0100.002*, March 2001.
84. ETSI TS 103 197 (V1.1.1). Digital video broadcasting (DVB); head-end implementation of DVB SimulCrypt. *ETSI TS 103 197* (*V1.1.1*), June 2000.
85. Kent S, Seo K. Security architecture for the Internet protocol. *IETF RFC 4301*, December 2005.
86. Cruickshank H, Iyengar S, Duquerroy L, Pillai P. Security requirements for the unidirectional lightweight encapsulation (ULE) protocol. *IETF Internet Draft*, draft-ietf-ipdvb-sec-req-02.txt, May 2007, Work in progress.
87. Border J, Kojo M, Griner J, Montenegro G, Shelby Z. Performance enhancing proxies intended to mitigate link-related degradations, *IETF RFC 3135*, June 2001.

AUTHORS' BIOGRAPHIES

Felicia Li Chin Ong received her BEng (Hons) degree in Electronic, Telecommunications and Computer engineering from the University of Bradford, U.K., in 2002 and is currently working as a research assistant at the University of Bradford. She has been involved in the EC funded IST project Fast Internet for Fast Train Hosts (FIFTH) and Satellite Communications Network of Excellence (SatNEx I and II) projects. Her research interests include mobility management in heterogeneous and beyond 3G systems, IP mobility in heterogenous networks and delivery of distance learning.

Xing Liang received an MSc degree with distinction in Radio Frequency Communications Engineering, and a PhD degree in Mobile and Satellite Communications from the University of Bradford, U.K., in 2002 and 2007, respectively. She was involved in the EC funded Fast Internet for Fast Train Hosts (FIFTH) and Satellite Communications Network of Excellence (SatNEx) projects. Her research interests include convergence of networks, digital video broadcasting over satellite and mobility management in heterogeneous networks.



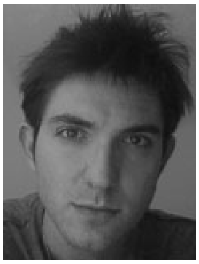
Prashant Pillai received his BSc in Electronics and MSc in Informatics from University of Delhi, India. He is is currently working as a research assistant at the University of Bradford and is working towards his PhD in the field of network security. He was involved in the EC funded WirelessCabin and SatNEx projects and is currently working on the Multicast BGAN project funded by INMARSAT Ltd, and SatNEx-II. His main areas of work are in mobile/wireless and, in particular, on system architecture design, protocol development and design of the AAA/security architectures.

Pauline Chan is a lecturer in the School of Informatics at the University of Bradford, where she has been involved in numerous EU and ESA funded projects, including SUITED, FIFTH, WirelessCabin, SatNEx and Inmarsat BGAN. Through participation in these projects, Pauline has acquired a wealth of knowledge and experience in the design of satellite and terrestrial network procedures for heterogeneous packet-oriented network environments. Her areas of interests are in mobile networking and wireless surveillance.

Georgios Koltsidas received his Diploma in Electrical and Computer Engineering from Aristotle University of Thessaloniki, Greece in 2003. He is currently working towards his PhD degree in the same department. His research interests include routing for ad-hoc and sensor networks and resource management in wireless networks.

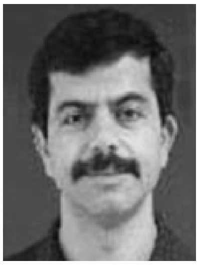
Fotini-Niovi Pavlidou received her Diploma in mechanical–electrical engineering in 1979 and the PhD degree in electrical engineering in 1988, both from the Aristotle University of Thessaloniki, Greece. She is currently a professor at the same institution engaged in teaching in the areas of mobile communications and telecommunications networks. Her research interests are in the field of mobile and wireless communications, satellite communications, multiple access systems, routing and traffic flow in networks and QoS provisioning in telecommunication networks. She is being involved with many national and European projects in the above areas.

Dr Erina Ferro is head of the Wireless Networks Laboratory (WNLAB) at the Institute ISTI of the Italian National research Council (CNR), and since 2006 she is responsible for the 'Devices and Technologies for Telematic Networks' scientific sector of the ICT Department of CNR. Her main research activities cover sensor networks, wireless networks ad-hoc networks, satellite networks and their interconnection aspects.



Alberto Gotta (MD 2002) was a researcher with the CNIT Research Unit in Genoa from 2002 to 2004. Since 2004 he has been a researcher with the Institute CNR-ISTI in Pisa. He participated in several projects funded by the EC. Since 2005 he has been a PhD student at the University of Genoa. His main areas of work are DVB-based systems and DVB-RCS extensions for mobile users, particularly in dynamic bandwidth allocation, admission control and fade countermeasure techniques.

DOI: 10.1002/sat



Dr Haitham Cruickshank has been a lecturer at the Centre for Communication Systems Research (CCSR), University of Surrey, U.K., since January 1996. He gained his BSc in Electrical Engineering at the University of Baghdad, Iraq, 1980, MSc in telecommunications, University of Surrey, U.K., and PhD in control systems, Cranfield Institute of Technology, U.K., 1995. He has worked on several European research projects: BISANTE, VIP-TEN, GEOCAST and SATLIFE. His current research interests are IP multimedia over satellites and IP multicast network security.

Sunil Iyengar is a research fellow at the Centre for Communication Systems Research (CCSR), University of Surrey, U.K., since January 2000. He received his BSc in Electronic Engineering from the University of Pune, India, 1997 and MSc in telecommunications and software from the University of Surrey, U.K., in September 1999. He is currently doing his PhD in the field of IP network security at CCSR. He has worked on several European research projects: GEOCAST, VIP-TEN, SATLIFE, SATSIX and SATNEX. His current research interests are in multicast network security and IP multimedia over satellites.

Dr Gorry Fairhurst received a degree in Applied Physics and Electronics (Dunelm) U.K. In 1985 he was awarded a PhD in Communications Engineering from the University of Aberdeen, U.K., where he is a Reader. He leads the Communication and Imaging Research Group, where his research focuses on Internet Engineering and protocol design for broadband systems, including link ARQ, link-specific tuning of communications protocols, analysis of TCP performance, multicast transport, streaming media transport and satellite Internet systems. He contributes to ETSI and the IETF and currently chairs the IETF IPDVB and DCCP working groups.

Dr Vincenzo Mancuso received his master degree in *Electronics* in 2001, and a PhD in *Electronics, Computer Science and Telecommunications* in 2005 from the University of Palermo, Italy. He has been a postdoc at the University of Roma 'Tor Vergata' before he joined the University of Palermo and is currently visiting the Networks Group at ECE department at Rice University, Houston, Texas, U.S.A. His research has been focused on the IP solutions for quality of service support in access networks, the interconnection of heterogeneous networks and the support of multimedia application in mobile systems. He is now working on wireless mesh networks operated by means of multiple technologies, namely IEEE 802.11, IEEE 802.16 and LEO/GEO Satellite solutions.

DOI: 10.1002/sat