# Next-generation Set-top Box for Broadband Environments

*Shinji Ishii, Yoshinori Goto*[†]*, and Takako Sato*

**Abstract**

With the deployment of digital broadcasting and broadband IP (Internet protocol) networks in recent years, broadcasting services are expected to change dynamically. However, it is difficult to integrate and exploit the advantages of broadband because of the established systems for broadcasting, which reflect the business and technical requirements of the broadcasting industry. It is essential to respect present conventional broadcasting technologies to develop and introduce future broadcasting technologies. This article describes a set-top box designed for broadband IP environments. It provides interactive electronic program guides and a multi-algorithm conditional access system. Broadcast contents including high-definition television are received over an IP network.

## 1. Introduction

Digital broadcasting has developed as a series of services since the introduction of the BS (broadcast satellite) digital broadcasting followed by the 110CS (communication satellite located at longitude 110 degrees east) digital broadcasting and digital terrestrial broadcasting (**Fig. 1**). As recently reported [1], more than five million Japanese consumers receive digital broadcasting via satellite or CATV (cable television), and the number is still growing. This impressive fact suggests that digital broadcasting has the potential to become an indispensable information technology (IT) infrastructure comparable to the Internet and it is opening up a new frontier for human life.

Digital broadcasting, which is characterized by high efficiency and high quality, has several features

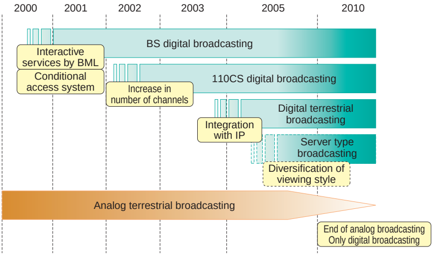

Fig. 1. Roadmap of Japanese digital broadcasting.

† NTT Access Network Service Systems Laboratories
Chiba-shi, 261-0023 Japan
E-mail: goto@ansl.ntt.co.jp

such as interactive services and pay services enabled by broadcast markup language (BML) and conditional access system (CAS), respectively. However, the infrastructure providing the technical foundation for these services is relatively conservative. Though the effort of creating a new business and service has been made, the limited capability of the broadcasting network will become a major constraint on this effort.

On the other hand, the development of the broadband infrastructure, particularly FTTH (fiber to the home), is expected to change this situation. FTTH provides a huge bandwidth, typically 100 Mbit/s or more, to consumers. Its "always-on" nature makes the integration of communication services and broadcasting easier. Such integration has been tried on CATV [2], but the results were not good. Although CATV can handle both communication and broadcasting, cable modems have a maximum speed of 30 Mbit/s, which is insufficient for distributing high-quality video contents, and this bandwidth is shared among a large number (typically several hundred) of users. Furthermore, the communication performance of CATV can be deteriorated by ingress noise. Thus, the lack of sufficient bandwidth and stability makes interactive broadcasting difficult.

This article discusses the architecture of a set-top box (STB) designed for FTTH. This STB has two key features: it has enhanced interactivity and it handles IP-based broadcasting.

## 2. Technologies for STB

The technologies for broadcasting services have been developed through standardization efforts made at ARIB (Association of Radio Industries and Businesses), JCTEA (Japan Cable Television Engineering Association), and JCL (Japan Cable Laboratories). **Figure 2** shows the structure of broadcasting technologies. A number of services and technologies, such as data services, electronic program guides (EPGs) and a CAS are combined with audio and video services and integrated on the MPEG-2 system. STBs have also been standardized [3] within broadcasting technologies and developed for each transmission medium, such as satellite, terrestrial, and CATV. A conventional STB is basically designed to receive a broadcasting signal from the air (or cable) and has poor interactive capability, so recent efforts to achieve integration with a broadband IP network were premature.

On the other hand, some vendors have produced IP-based STBs that can receive broadcasting signals from a broadband IP network. Their specifications are defined by each vendor, and interconnection with each other's products has hardly been considered. Furthermore, these technologies are dissimilar to current broadcasting technologies, as shown in Fig. 2, so the exploitation of rich and high-quality contents held and provided by current broadcasters is naturally limited.

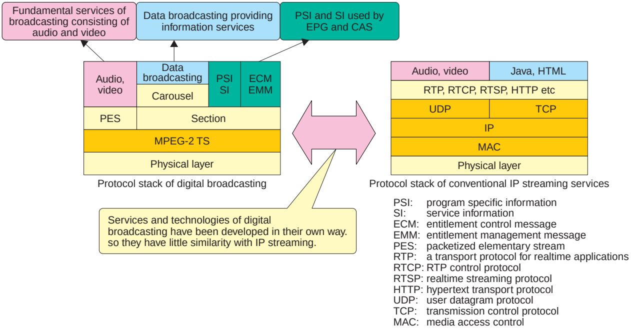
Fundamental services of broadcasting consisting of audio and video
Data broadcasting providing information services
PSI and SI used by EPG and CAS
Audio, video
Data broadcasting
Carousel
PSI
SI
ECM
EMM
PES
Section
MPEG-2 TS
Physical layer
Protocol stack of digital broadcasting
Audio, video
Java, HTML
RTP, RTCP, RTSP, HTTP etc
UDP
TCP
IP
MAC
Physical layer
Protocol stack of conventional IP streaming services
Services and technologies of digital broadcasting have been developed in their own way. so they have little similarity with IP streaming.
PSI: program specific information
SI: service information
ECM: entitlement control message
EMM: entitlement management message
PES: packetized elementary stream
RTP: a transport protocol for realtime applications
RTCP: RTP control protocol
RTSP: realtime streaming protocol
HTTP: hypertext transport protocol
UDP: user datagram protocol
TCP: transmission control protocol
MAC: media access control

Fig. 2. Comparison of conventional IP streaming and digital broadcasting.

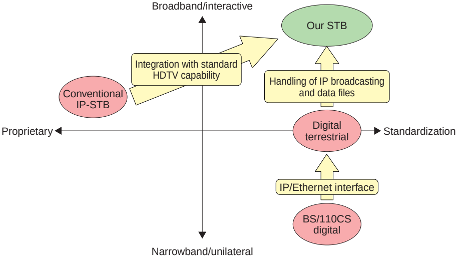

Fig. 3. Position of broadband STB.

The position of our STB is shown in **Fig. 3**. This product has two features. First, it receives over the IP network almost the same contents as currently provided by broadcasting systems. As noted above, broadcasting technologies consist of a wide range of technologies: radio frequency (RF) modulation, multiplexing, encoding/decoding schemes for audio and video signals, a descriptive language for data services and its execution environment, and a scrambling/encrypting scheme. Broadcasting contents are produced to be compliant with these technologies. For broadcasting services on an IP network, the specifications related to the physical transmission need to be changed, but leaving the rest of the specifications unchanged makes it easy to exploit high-quality broadcasting contents including HDTV contents.

The second feature is advanced broadcasting services enhanced by a broadband IP network. This can handle file type contents as well as streaming contents. Although VOD (video on demand) is barely available on the conventional broadcasting network, it can be provided with high efficiency on the broadband IP network. An EPG provides a search function that lets a user choose desired content from a rich set of contents including not only programs on the air but also ones stored in HDD (hard disk drive) recorders or VOD servers.

## 3. Functions and structure of our STB

### 3.1 Functions

**Figure 4** shows the hardware configuration of our STB, **Table 1** summarizes its specifications, and **Fig. 5** shows photographs. As reported in several documents [5]-[6], an STB generally consists of mainly two modules: the front-end module is responsible for lower layers such as physical transmission/receiving functions and the decoding module is responsible for higher layers, in other words service issues, such as decoding of audio and video signals, processing data services, and EPGs. Our STB also follows this fundamental architecture. It has two network interfaces: an RF interface and an IP interface. The RF interface can receive a 64QAM (quadrature amplitude modulation) signal, which is defined as the standard transmission scheme for Japanese CATV, so it can be used for the video transmission systems of both FTTH and the conventional HFC (hybrid fiber coaxial cable) network. The IP interface is 100BASE-TX, which can be traced to the decoding module. For almost the same transport stream flows into the decoding module from each network module, the same services are provided irrespective of the network.

The STB contains a 100-GB hard disk drive. This can store 37 hours of SD (standard definition) video contents or 10 hours of HD (high definition) video contents. The contents that can be stored are (1) conventional streaming content, (2) file type content transmitted by MPEG-2 transport stream (carousel) (MPEG: moving picture experts group), and (3) file type content downloaded over the IP network (by file transfer protocol).

The video decoder can handle both SDTV (standard definition television) and HDTV (high definition television). It provides both composite and component outputs. The former is the usual output to a

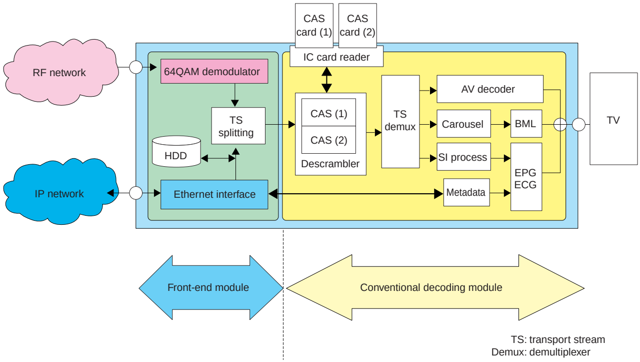

Fig. 4. Hardware configuration of broadband STB.

Table 1. Summary of STB specifications.

| | |
|---|---|
| RF interface | 64QAM (29.162 Mbit/s per channel) |
| IP interface | 100BASE-TX |
| Output interface | Composite (RCA, S-video), component (D connector) |
| Video format | MPEG-2 (MP@HL, MP@HL) |
| Audio format | MPEG-2 AAC |
| Rate | SDTV: up to15 Mbit/s, HDTV: up to 22 Mbps |
| Data broadcasting | BML (ARIB STD-B24, partly expanded) |
| Metadata | TVA SP003 |
| Web browser | HTML4.0 |
| Hard disk capacity | 100 GB |
| Descrambler | Multi2, AES, Camellia |
| Available services | Digital broadcasting (streaming, files), VOD, storage and replay |

MP@ML: MainProfile@MainLevel
MP@HL: MainProfile@HighLevel

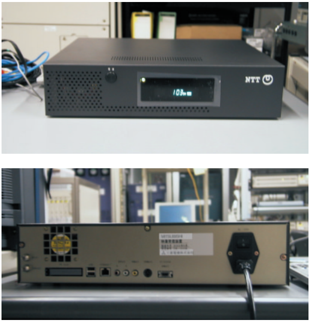

Fig. 5. Photographs of broadband STB.

television set while the latter is used to output HDTV as well as SDTV.

The descrambler provides three descrambling algorithms (Camellia, AES, and Multi2). The conventional standard algorithm, Multi2, which is used for scrambling content, seems likely to become vulnerable to attack in the future because it has a short key length of 64 bits. In anticipation of advances in cipher technologies, two more-advanced algorithms were added to the descrambler. These employ a longer key, 128 bits, for content scrambling. The technical sophistication of these algorithms ensures that contents will be protected against unauthorized attempts to breach them.

IC (integrated circuit) cards have been used for

Table 2. Comparison of PSI/SI for conventional broadcasting and the hybrid configuration for our broadband STB.

| PSI/SI and metadata | | Conventional broadcasting (BS digital broadcasting) | Broadband STB |
|---|---|---|---|
| PSI | PAT | Used | Used |
| | PMT | Used | Used |
| | NIT | Used | Used |
| | CAT | Used | Used |
| SI | EIT | Used | Not used |
| | BIT | Used | Not used |
| | SDT | Used | Not used |
| | TOT | Used | Used |
| Metadata | Program | Not used | Used |
| | Segmentation | Not used | Used |
| | User preference | Not used | Used |

PAT: program association table; PMT: program map table; NIT: network information table; CAT: conditional access table; EIT: event information table; BIT: broadcaster information table ; SDT: service description table; TOT: time offset table.

keeping a master key and decoding entitlement control messages (ECMs) and entitlement management messages (EMMs). The STB can handle two types of IC card: the conventional IC card, which complies with the established standard (ARIB STD-B25), and one modified to control multiple algorithms. Thus, the STB can use advanced cipher algorithms without losing backward compatibility with the conventional CAS.

## 3.2 Structure

The configuration of program specific information and service information (PSI/SI) and metadata is one of the key features of our STB. **Table 2** compares conventional digital broadcasting and our STB. The STB receives basically the same PSI as conventional broadcasting. Two descriptors, IP_delivery_system_descriptor() and CA_descriptor(), are defined to expand its functionalities. To ensure compatibility with the conventional broadcasting system, the physical and logical locations of programs are described in a network information table as in conventional systems. Satellite_delivery_system_descritptor() for satellite broadcasting and Cable_delivery_system_descritptor() for CATV are defined as part of the standard. These descriptors include information such as frequency, modulation, and encoding for error protection. For transmission on IP networks, it is appropriate that IP_delivery_system_descriptor() is formatted as shown in **Table 3**.

Table 3. IP delivery system descriptors.

| Syntax | No. of bits | Type |
|---|---|---|
| IP_delivery_system_descriptor(){ | | |
| Descriptor_tag | 8 | Uimsbf |
| Descriptor_length | 8 | Uimsbf |
| IP_address | 32 | Uimsbf |
| Port_number | 16 | Uimsbf |
| FEC_outer_TS | 4 | Bslbf |
| Reserved_future_use | 4 | Bslbf |
| FEC_IP | 8 | Bslbf |
| RTP_indicator | 4 | Bslbf |
| Packet_size | 4 | Bslbf |
| Unicast_multicast_indicator | 2 | Bslbf |
| Reserved_future_use | 6 | Bslbf |
| Control_protocol | 8 | Bslbf |
| Frame_type | 4 | Bslbf |
| Reserved_future_use | 4 | Bslbf |
| TS_packet_size | 8 | Uimsbf |
| TS_rate | 32 | Bslbf |
| Reserved_future_use | 8 | Bslbf |
| } | | |

In conventional broadcasting systems, ECMs and EMMs, which contain keys and related information about scrambling and pay programs, are conveyed on the transport stream, and their packet identifiers (PIDs) are designated in CA_descritpor() located in the program map table (PMT) and conditional access table (CAT). This scheme works well, particularly for ECMs, because bundling ECMs with the content ensures stringent time synchronization and enables the scrambling key to be changed frequently. On the other hand, bundling both EMMs and ECMs with the content may cause several problems. The key and related information contained in an EMM are meaningful only for a designated STB. Broadcasting an EMM to all STBs is not only inefficient but also insecure, because the EMM directed for one STB might be breached by another user and used maliciously (i.e., to obtain unauthorized access to the contents). EMMs should be intrinsically transported by unicasting.

However, bundling ECMs with the content may also be inefficient. When a viewer chooses a scrambled program, he/she cannot watch the program until one ECM has arrived at the STB. The duration from the viewer's action (i.e., pressing a button on the remote controller) to the time when the video appears on the TV screen depends on the interval between ECMs. Shortening the interval consumes the bandwidth of the transport stream. On the other hand, the advanced scrambling algorithm reduces the need for frequent key replacement for security reasons. Consuming bandwidth only for the smooth program changes seems to be unreasonable.

For these reasons, for our STB we studied transporting ECMs and EMMs over an IP network. One issue to be resolved is how to harmonize the bundled transport scheme on a transport stream and the unbundled transport scheme on the IP network. The conventional CA_descriptor() designates the PID of an ECM or EMM. For IP transport, the IP address (multicast address) and port number should be designated in CA_descriptor() instead. Furthermore, a common format has been applied for both ECMs and EMMs. The CA_descriptor() for an ECM contains additional information designating the scrambling scheme and key length (scramble_id and key_length in **Table 4**, respectively). The CA_descriptor() for an EMM is also modified in the same way, as shown in **Table 5**. These modifications allow flexible operations of CAS.

In a conventional manner, the event information table (EIT) that contains information about programs such as time, duration, genre, and summary is supplied to an STB that uses it as a source for EPG. Although EIT is a useful form of information for EPG, it could be improved for greater convenience. The design and layout of an EPG are basically up to the STB and its manufacturer, because the EPG is produced by application programs residing inside the STB. Broadcasters may wish to provide their proprietary EPGs with their own layouts to attract more customers to their programs.

What programs are being provided now and will be provided in the future can be shown by EIT. However, it is unlikely that EIT will show what programs have been provided and what programs are available in an STB or in VOD servers, because EIT is generally bundled with contents and sent periodically on a transport stream. If EIT for past programs and stored programs is provided in the same way, it will consume so much bandwidth that it will be unrealistic. This is the fundamental problem of EPGs based on EIT.

On-demand EPGs are expected to solve this problem. There are two types: a conventional style, which shows the schedule of each channel with title and summary, and an advanced EPG, which has advanced features such as contents recommendation. The conventional style EPG is formed from metadata that contains similar information to the current EIT and is

Table 4. Modified CA_descriptors for PMT.

| Syntax | No. of bits | Type |
|---|---|---|
| CA_descriptor(){ | | |
| Descriptor_tag | 8 | Uimsbf |
| Descriptor_length | 8 | Uimsbf |
| CA_system_ID | 16 | Uimsbf |
| Reserved | 3 | Bslbf |
| CA_PID | 13 | Uimsbf |
| For(I=0; I<N; I++) | | |
| Rating | 8 | Bslbf |
| Scramble_id | 3 | Bslbf |
| Key_length | 3 | Bslbf |
| Reserved | 2 | Bslbf |
| ECM_Delivery_route | 8 | Bslbf |
| If(ECM_delivery_route==0x01) | | |
| ECM_MC_address | 32 | Uimsbf |
| Port_number | 16 | Uimsbf |
| } | | |
| Else{ | | |
| Reserved_future_use | 48 | Bslbf |
| } | | |
| } | | |
| } | | |

Table 5. Modified CA_descriptor for CAT.

| Syntax | No. of bits | Type |
|---|---|---|
| CA_descriptor(){ | | |
| Descriptor_tag | 8 | Uimsbf |
| Descriptor_length | 8 | Uimsbf |
| CA_system_ID | 16 | Uimsbf |
| Reserved | 3 | Bslbf |
| CA_PID | 13 | Uimsbf |
| For(I=0; I<N; I++) | | |
| EMM_delivery_route | 8 | Bslbf |
| If(EMM_delivery_route==0x01) | | |
| EMM_MC_address | 32 | Uimsbf |
| Port_number | 16 | Uimsbf |
| } | | |
| Else{ | | |
| Reserved_future_use | 48 | Bslbf |
| } | | |
| } | | |
| } | | |

designed to inform users which program can be seen on which channel. It presents a schedule-based program guide, but naturally the guidance for stored and VOD contents is limited. Advanced EPG is an on-demand EPG that is provided on a client server system [8]. As shown in **Fig. 6**, the EPG is presented on the browser software and the contents of the EPG are obtained by HTTP. With a bi-directional architecture, search and recommendation functionality not only for streaming contents but also for stored contents can be easily implemented.

A time offset table (TOT) defined in ITU-T (International Telecommunication Union Telecommunication Standardization Sector) J.94, provides time information to ensure time synchronization with the headend equipment. Both IP and RF networks provide TOT because the same transport stream can be sent on both networks. In addition to TOT, time synchronization can also be done by network time protocol (NTP) via an IP network. TOT and NTP are expected to carry the same time information.

A BML browser installed on the STB is used for data services. Implementation on the STB is basically compliant with the established Japanese broadcasting standard [7], but several features have been added to support distribution on an IP network.

## 4. Applications

### 4.1 How our STB will be used

A conventional STB is designed for real-time viewing that simply presents a current program on a television set. It can store programs in its hard disk drive (HDD) and present the stored program at any time. This function is just the same as that of an HDD video recorder, but it is still meaningful as a commercial product. An HDD can store conventional broadcasting contents and file type contents. This feature lets a broadcaster distribute its contents while users are sleeping or when there is surplus network capacity. For instance, regular news programs and weather forecasts, which are less sensitive to the time of delivery, can be distributed in this way and viewers can watch these programs just like they read a morning newspaper.

Our STB can request content that is not stored in the HDD from a VOD server. Content that is produced for specific people rather than the general public is suitable for VOD. Viewers who miss watching or recording a desired program may request it by VOD.

The STB needs to deal with a large number of content items, not only broadcasting contents but also

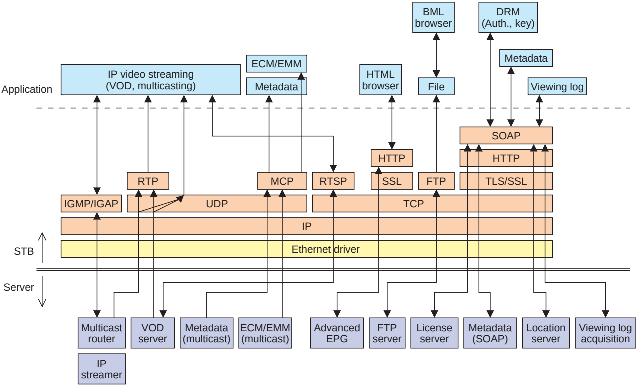

Fig. 6. Relationships between protocols and applications.

VOD contents and locally stored contents. The searching and recommending function of the EPG is helpful to identify which programs are suitable for a particular viewer.

### 4.2 Possible services and businesses

There are many kinds of players in the broadcasting industry. Although broadcasters that are responsible for producing programs play a vital role, they cannot keep the industry going without other players. Platform operators that are responsible for multiplexing programs and operating CAS are the foundation of the digital broadcasting system. CATV operators that supply broadcasting signals in areas where satellite or terrestrial reception is poor provide viewers with an alternative way to watch programs.

Our STB will allow the advanced broadcasting platform to prevail and business based on this platform to develop. The platform, which is itself a promising source of revenue, can be differentiated from conventional platforms by, for instance, the EPG search function, so the business model in which the platform operator can obtain revenue directly from viewers may develop. With an IP interface that can receive broadcasting content as it is, the STB can be used for the retransmission business using the IP capability of FTTH. The lower cost of IP-FTTH compared with the combination of IP network and RF-FTTH may improve the cost advantage of FTTH over conventional CATV. Furthermore, because the IP network has unlimited reachability, unprecedented business models such as international distribution of broadcasting contents will be developed in the future.

## 5. Conclusions

We are developing a new style of set-top box (STB) for broadband IP networks. It implements advanced EPGs with interactive capabilities and CAS with multi-cipher algorithms. IP-based broadcasting allows not only flexible network configuration but also unprecedented new business including international broadcasting over a less expensive network. Its compatibility with current broadcasting technologies means that there will be little negative impact associated with the introduction and deployment of this STB.

## References

[1] For example, http://www.nhk.or.jp/digital/news/040304/ (in Japanese).

[2] Operational Specification of Integrated Digital CATV system, JCL TR-002, Japan Cable Laboratories, Nov. 2002.

[3] BS & 110 CS Digital Compliant Digital Cable Television Receiver, JCTEA STD007, Japan Cable Television Engineering Association, May 2002.

[4] Services information for digital broadcasting in cable television systems, ITU-T Rec. J.94, Nov. 2002.

[5] T. Yamaguchi, T. Maeda, T. Ohtsu, T. Tsuji, and S. Chozui, ICCE 2001, International Conference on Consumer Electronics, Los Angeles, U.S.A., pp. 86-87, 19-21, June 2001.

[6] B. Kovacevic, IEEE 1997 Canadian Conference on Electrical and Computer Engineering, St. Johns, Canada, Vol. 1, pp. 371-374, 25-28, May 1997.

[7] Data Coding and Transmission Specification for Digital Broadcasting, ARIB STD-B24, Association of Radio Industries and Businesses (ARIB), July 2002.

[8] M. Leban, EUROCON 2003 Computer as a Tool, IEEE Region 8, Vol. 2, pp. 70-7322-24, Sep. 2003.

**Shinji Ishii**

Senior Research Engineer, Promotion Project 1, NTT Cyber Solutions Laboratories.

He joined NTT in 1989. He is interested in developmental research on security systems for multimedia communications. Recently, he has been engaged in the development of copy protection systems for digital broadcasting and broadband communications.

**Yoshinori Goto**

Research Engineer, NTT Access Network Service Systems Laboratories.

He received the B.S. and M.S. degrees in applied physics from Tohoku University, Sendai, Miyagi in 1992 and 1994, respectively. In 1994, he joined NTT Basic Research Laboratories where he studied X-ray optics and spectroscopy. Since 1998, he has been developing and evaluating broadband IP applications and CATV services including VoIP, STB, and cable modems in NTT Access Network Service Systems Laboratories. He is also involved in several standardization activities such as JCL, JCTEA, and ITU-T SG9. He is a member of the Institute of Electronics, Information and Communication Engineers.

**Takako Sato**

Engineer, NTT Access Network Service Systems Laboratories.

She received the B.S. degree in mathematics from Hirosaki University, Hirosaki, Aomori in 1994. She joined NTT Multimedia Systems Department in 1994 where she developed video transmission systems. She was also involved in FSAN and ITU-T SG15. She is currently developing IP-based broadcasting systems.