Send encrypted media stream from IPTV Head-end to RTP switch

Send identifiers to RTP switch, identifiers indicating packets in media stream containing I-frames

Store packets in buffer at RTP switch

Receive request for programme from STB

Send I-frame packets and subsequent packets for programme to STB
Published:
   — with international search report
PROVIDING IPTV MULTICASTS

Technical field

The invention relates to the field of providing an IPTV multicast, and in particular to method of providing an IPTV multicast when switching between channels.

Background

TV services broadcast over an IP network are referred to as IPTV. IPTV is typically broadcast using a broadband access network, and the predominant IPTV service is Broadcast TV, in which the normal non-IPTV channels, as well as additional channels with low penetration are transmitted over the broadband network from a super head-end down to an end-user's set top box (STB).

Linear content delivery, in which all channels in a subscription are simultaneously delivered to a user's set top box (STB) is not suitable for IPTV, as IPTV has limited bandwidth available over a broadband connection. A typical ADSL broadband connection provides a capacity of between 3 and 8 Mbps, and ADSL2 promises to deliver up to 25 Mbps downstream, whereas VDSL can provide a capacity of greater than 30 Mbps. Standard quality MPEG 2 IPTV content requires 2Mbps per channel, and HDTV will require around 8-10 Mbps per channel. The MPEG 4 standard will approximately halve the bandwidth required to deliver IPTV content with the same quality. Nevertheless, the available bandwidth is a scarce resource, and IPTV solutions must limit the number of channels that can be delivered simultaneously.

In order to minimize the bandwidth required for transmission of IPTV content, it is necessary to use multicast techniques through the network. When the end-user switches from one channel to another, the STB sends out an Internet Group Management Protocol (IGMP) Leave message for the channel that the STB is currently receiving, and an IGMP Join message for the new channel that the user wishes to receive.
The IPTV content contains MPEG (normally 2 or 4 part 10) frames. There are different frames in MPEG, such as I-frames, P-frames and B-frames. I-frames do not depend on data contained in the preceding or following frames, as they contain a complete picture. P-frames provide more compression than I-frames because they utilize data contained in the previous I-frame or P-frame. When generating a P-frame, the preceding frame is reconstructed and altered according to incremental extrapolation information. B-frames are similar to P-frames, except that B-frames interpolate data contained in the following frame as well as the preceding frame. As a result, B-frames usually provide more compression than P-frames. Typically, every 15th frame or so is an I-frame. P-frames and B-frames might follow an I-frame as follows: IBPBBPBBPBB(I). The order and number of frames in the sequence can be varied.

Since B and P frames depend on adjacent frames it is necessary that when the STB receives a new channel, it receives a full I-frame before the new channel can be shown. The average time for switching between channels therefore depends on the length of time between I-frames. Typically, for MPEG-2 IPTV content, the length of time is around 0.5 seconds. For MPEG-4 part 10 IPTV content, the length of time between I-frames can be several seconds.

Other sources of delay include:
- The buffer in the STB
- The time it takes for the IGMP Leave/Join actions to be sent and actioned.

There is therefore a problem in that when an IPTV user changes channel, there can be a significant delay between the STB no longer receiving IPTV content the old channel, and the STB receiving and rendering the IPTV content of the new channel, which is detrimental to the user experience.

Some solutions have been proposed to alleviate the problem associated with the delay in channel switching. For example, an Omicron solution describes fast channel switching between MPEG-streams, although this was not designed for IPTV.
Another solution is to use a Reliable Transmission Protocol (RTP) switch. This switch resides in the network from which the IPTV is broadcast, and buffers RTP streams containing MPEG frames. When the RTP switch receives an IGMP Join message it immediately sends the I-frames from its buffer to the STB.

A further solution is to begin a unicast session when the user changes channel, in order to send the frames to the user as quickly as possible. Once synchronisation of the frames from the unicast with the multicast is possible, then the user switches to receiving the multicast session rather than the unicast session.

A problem with the RTP-switch solution that most channels are encrypted. The RTP-switch therefore has difficulty "seeing" what kind of frames it receives, that is to say whether frames are of I, P or B type. Decrypting and re-encrypting is of course one possible solution, but this would necessitate an expensive increase in processing power required. This is also a problem with the unicast solution described above.

The unicast solution has additional drawbacks. Firstly it requires that the available bandwidth on the "last mile" (for example, the DSL-line connecting the user to the network) is sufficiently high to allow the user to download both unicast and multicast data concurrently, at least for a short time after changing channel. In addition, the unicast solution has a scalability problem. For example, when a very popular programme ends, a large number of people who have been watching the programme will then start to zap (the term "zapping" is used herein to mean changing channels using the up and down or the number buttons on a STB remote control) simultaneously. It is not feasible to start unicast session to all those users unless the number of servers is very large. Yet another drawback is that the STB needs to implement the functionality of downloading the unicast and the multicast simultaneously, which can be quite complex.

There is a need for fast channel switching that does not require the STB to simultaneously download a multicast and a unicast, and can also be used for encrypted video multicast streams.
Summary

The invention provides fast channel switching using an RTP switch as described above. In order to overcome the problem with encryption, the invention provides for information being sent to the RTP switch, the information identifying which packets contain complete image frames such as I-frames.

According to a first aspect of the invention, there is provided a method of operating a Reliable Transmission Protocol switch node to provide an IPTV multicast. The method comprises:

- receiving IP packets transporting an encrypted media stream from an IPTV Head-end, the media stream containing complete image frames;
- receiving unencrypted identifiers identifying packets containing complete image frame data;
- storing the received packets in a buffer;
- on receipt of a request from a media renderer to provide the IPTV multicast, sending the packet(s) containing the last complete image frame in the media stream and all subsequent packets to the media renderer.

By sending unencrypted identifiers, there is no need for the RTP switch to decrypt the media stream in order to identify packets containing complete image frames.

In one embodiment of the invention, a complete image frame is an I-frame.

The identifiers may be received as a separate message from the media stream, the separate message containing information identifying packet sequence numbers of packets containing complete image frame data.

Alternatively, each identifier may be an identifier packet inserted in the media stream, the identifier packet being inserted immediately prior to a first packet relating to an I-frame. The position of the identifier packet indicates to the RTP switch that the subsequent packet contains complete image frame data.
In an alternative embodiment, the identifiers may be included in a header of a packet relating to a complete image frame. Even though the data transported in the packet is encrypted, the RTP switch can identify from the header that the packet contains encrypted data relating to a complete image frame. In one example, packets containing complete image frames may be accorded a different Class of Service value to packets not containing complete image frames, the Class of Service value identifying which packets relate to complete image frames. In order to ensure that packets are received in the correct order, packets containing the encrypted media stream but having different Class of Service values may be accorded the same priority as other packets in the media stream.

The encrypted media stream may be one of a plurality of encrypted media streams, each encrypted media stream of the plurality of encrypted media stream having complete image frame identifiers associated with it.

The Reliable Transmission Protocol switch node may be located at an Access Node used by the media renderer to access the IPTV multicast, and in one embodiment of the invention, the media renderer is a Set Top Box.

According to a second aspect of the invention, there is provided a Reliable Transmission Protocol switch comprising:

- a receiver for receiving IP packets containing an encrypted media stream from an IPTV Head-end, the media stream containing complete image frames;
- means for receiving unencrypted identifiers identifying which packets contain complete image frame data;
- a buffer for storing the packets; and
- a transmitter for, on receipt of a request from a media renderer, transmitting those packets containing the last complete image frame in the media stream and all subsequent packets from the Reliable Transmission Protocol switch node to the media renderer.

According to a third aspect of the invention, there is provide an encryption node for use with an IPTV multicast, the node comprising:
encryption means for encrypting the media stream;
means for identifying packets in the media stream containing complete image frames;
means for transmitting the encrypted media stream to another node; and
means for identifying which encrypted packets contain the complete image frames to the other node.

This node is used where complete image frames are identified at the same node used to encrypt the media stream.

According to a fourth aspect of the invention, there is provide a node for use in an communications network, the node comprising:
means for receiving a media stream;
means for identifying packets in the media stream containing complete image frames; and
means for transmitting data to another node, the data identifying which packets in the media stream contain complete image frames.

This node is used where complete image frames are identified at a different node to that used to encrypt the media stream. In the case where this node is disposed between the encryption node and the RTP switch, the node will also require means to decrypt the media stream in order to identify complete image frames. Alternatively, the node is disposed between the source of the media stream and the encryption node, so no decryption is required.

**Brief Description of the Drawings**

Figure 1 illustrates schematically the IPTV network architecture; and

Figure 2 is a flow diagram showing the basic steps of the invention; and

Figure 3 illustrates schematically three alternative embodiments of the invention for informing the RTP switch which packets relate to I-frames.
Detailed Description

Referring to Figure 1, there is illustrated an IPTV Head-end, which generates an IPTV multicast media stream. The IPTV Head-end includes an encryption node, which encrypts the IPTV media stream. The encrypted media stream passes through a router and ultimately the last node traversed by the IPTV media stream in the operator's network is an Access Node (AN). Where a user is accessing the IPTV multicast using DSL, the AN is a Digital Subscriber Line Access Multiplexer (DSLAM).

The user receives the encrypted IPTV media stream at a Set Top Box (STB), in some cases via a Residential Gateway (RGW). The STB decrypts the media stream and renders it on the user's television (or other viewing equipment).

An RTP switch is also provided functionally located between the STB and the IPTV Head-end. The RTP switch that may be implemented as part of the Access Node or may be a separate node. The RTP switch receives all of the IPTV media streams sent from the IPTV Head-end. It stores all packets from the media stream in a buffer, and when a user requests access to a particular IPTV channel, the RTP switch sends the media stream packets beginning with the start of the last I-frame, and all subsequent packets (including P-frame and B-frame packets) to the STB of the requesting user. This allows the STB to start rendering the media stream on the user's television as soon as the packets are received from the RTP switch, rather than waiting for the next I-frame to be sent in the media stream. This makes rendering of a new channel quicker where a user first turns on their STB or, more commonly, changes between channels.

As described above, the RTP switch cannot "see" which packets in the media stream relate to I-frames when the IPTV media stream is encrypted. In order to allow the RTP switch to know which packets of an encrypted media stream relate to I-frame packets, the RTP is further provided with identifying information that identifies those packets that relate to an I-frame (or IDR frames in the case of MPEG 4 part 10).
The video in the IPTV multicast may be transported directly using its RTP payload format inside RTP packets, in which case it is relatively easy to find the start of the I- (or IDR) frame at the start of a packet, and the rest of the frame is then contained in consecutive packets with the same time stamp value.

If the MPEG-2 transport layer is used, all MPEG data is partitioned into transport packets (188 bytes each) that are in turn grouped and sent in RTP packets (usually in groups of 7). In this case, a deeper analysis is needed to determine whether an I-frame starts in a packet, but the principles of signalling in which packet the I-frame picture starts remain the same.

The RTP switch must know which IP packet contains the first MPEG I-frame packet. The invention allows for several different methods sending this information to the RTP switch and on to the STB as follows:

1. Sequence number information identifying packets containing I-frames is sent from the IPTV Head-end to the RTP switch. The RTP and Secure Real-time Transport Protocol (SRTP, the encrypted variant of RTP) packet headers contain sequence numbers that can be used to identify packets containing the first I-frame MPEG packet. A separate message containing the sequence numbers of interest is sent to the RTP switch. Alternatively, the sequence numbers can be included in packets in the media stream, and not sent separately.

2. Alternatively, the encryption node at the IPTV Head-end can insert a special-purpose IP-packet in the stream immediately prior to the IP-packet containing the first MPEG I-frame packet. This identifies that subsequent packets contain I-frame data. The special purpose IP packet is sent with the same class of service (COS) as the other packets in the IPTV media stream to ensure that the packets are received in the correct order, and that the special purpose packet immediately precedes an I-frame packet. An advantage with this solution is that it can be used for transport protocols that do not rely on sequence numbers, for example if SRTP is not being used to transport the media stream.
3. COS marking is used to differentiate which packets in the media stream contain I-frame data, and which packets do not contain I-frame data. For example, the encryption node stamps all packets that contain I-frame data with a COS value of 7, and all packets that do not contain I-frame data with a COS value of 6. In this way, the RTP switch can differentiate which packets contain I-frame data and which do not. The network is configured to give both those classes the same priority in order to guarantee that the packets are received in the correct order. Note that there are also other fields that could be used to mark the packets that contain I-frames.

In summary, I-frame packets in an encrypted media stream can be identified to the RTP switch using any of the following:

1. Sequence number
2. Extra ID packets
3. Packet marking/differentiation

The invention provides a solution for fast channel switching or initiation of an IPTV multicast, which poses no requirement on the STB, and which works for encrypted video multicast streams.

It will be appreciated by the person of skill in the art that various modifications may be made to the above described embodiments without departing from the scope of the present invention. For example, the invention has been described with reference to a Set Top Box, but applies equally to other types of media renderer, in particular mobile devices.
Claims

1. A method of operating a Reliable Transmission Protocol switch node to provide an IPTV multicast, the method comprising:
   
   receiving IP packets transporting an encrypted media stream from an IPTV Head-end, the media stream containing complete image frames;
   
   receiving unencrypted identifiers identifying packets containing complete image frame data;
   
   storing the received packets in a buffer;
   
   on receipt of a request from a media renderer to provide the IPTV multicast, sending the packet(s) containing the last complete image frame in the media stream and all subsequent packets to the media renderer.

2. A method of operating a Reliable Transmission Protocol switch node according to claim 1, wherein a complete image frame is an I-frame.

3. A method of operating a Reliable Transmission Protocol switch node according to claim 1 or 2, wherein the identifiers are received as a separate message from the media stream, the separate message containing information identifying packet sequence numbers of packets containing complete image frame data.

4. A method of operating a Reliable Transmission Protocol switch node according to claim 1 or 2, wherein each identifier is an identifier packet inserted in the media stream, the identifier packet being inserted immediately prior to a first packet relating to a complete image frame.

5. A method of operating a Reliable Transmission Protocol switch node according to claim 1 or 2, wherein the identifiers are included in a header of a packet relating to a complete image frame.

6. A method of operating a Reliable Transmission Protocol switch node according to claim 5, wherein packets containing complete image frames are accorded a different Class of Service value to packets not containing complete image frames, the Class of
Service value included in the packet header and identifying which packets relate to complete image frames.

7. A method of operating a Reliable Transmission Protocol switch node according to claim 6, wherein packets containing the encrypted media stream but having different Class of Service values are accorded the same priority.

8. A method of operating a Reliable Transmission Protocol switch node according to any of the preceding claims, wherein the encrypted media stream is one of a plurality of encrypted media streams, each encrypted media stream of the plurality of encrypted media stream having complete image frame identifiers associated with it.

9. A method of operating a Reliable Transmission Protocol switch node according to any of the preceding claims, wherein the Reliable Transmission Protocol switch node is located at an Access Node used by the media renderer to access the IPTV multicast.

10. A method of providing an IPTV multicast according to any of the preceding claims, wherein the media renderer is a Set Top Box.

11. A Reliable Transmission Protocol switch comprising:
    a receiver for receiving IP packets containing an encrypted media stream from an IPTV Head-end, the media stream containing complete image frames;
    means for receiving unencrypted identifiers identifying which packets contain complete image frame data;
    a buffer for storing the packets; and
    a transmitter for, on receipt of a request from a media renderer, transmitting those packets containing the last complete image frame in the media stream and all subsequent packets from the Reliable Transmission Protocol switch node to the media renderer.

12. An encryption node for use with an IPTV multicast, the node comprising:
    encryption means for encrypting the media stream;
means for identifying packets in the media stream containing complete image frames;
means for transmitting the encrypted media stream to another node; and
means for identifying which encrypted packets contain the complete image frames to the other node.

13. A node for use in a communication network, the node comprising:
means for receiving a media stream;
means for identifying packets in the media stream containing complete image frames; and
means for transmitting data to another node, the data identifying which packets in the media stream contain complete image frames.

14. A node for use in a communication network according to claim 13, the node further comprising means for decrypting the received media stream.
Figure 1
Send encrypted media stream from IPTV Head-end to RTP switch

Send identifiers to RTP switch, identifiers indicating packets in media stream containing I-frames

Store packets in buffer at RTP switch

Receive request for programme from STB

Send I-frame packets and subsequent packets for programme to STB

Figure 2
Figure 3

1. Separate message containing sequence numbers of I-frame packets

2. Identifier packet sent prior to I-frame related packet in media stream

3. Insert identifier into header of I-frame related packet
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols) H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate of the relevant passages</th>
<th>Relevant to claim No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>abstract</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 2, line 26 - line 45</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 8, line 14 - column 9, line 25</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>EP 1 638 334 A (ALCATEL USA SOURCING LP [US]) 22 March 2006 (2006-03-22)</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td>abstract</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0006] - [0012], [0019] - [0028], [0043] - [0070]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>figure 3</td>
<td></td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C

See patent family annex

Date of the actual completion of the international search

3 August 2007

Date of mailing of the international search report

13/08/2007

Name and mailing address of the ISA/ European Patent Office, P B 5818 Patentlaan 2 NL - 2280 HV RUISWijk
Tel (+31-70) 340-2040, Tx 31 651 epo nl, Fax (+31-70) 340-3016

Authorized officer
Dobbel aere, Dirk

Form PCT/ISA/210 (second sheet) (April 2005)
**DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>WO 2006/041784 A (WAVE7 OPTICS INC [US]; FARMER JAMES O [US]; THOMAS STEPHEN [US]) 20 April 2006 (2006-04-20) abstract page 3, line 17 - page 6, line 9 page 8, line 25 - page 10, line 5 page 12, line 18 - page 13, line 10 page 15, line 28 - page 17, line 12 page 18, line 22 - page 21, line 20</td>
<td>1-14</td>
</tr>
<tr>
<td>A</td>
<td>FR 2 829 891 A1 (FRANCE TELECOM [FR]) 21 March 2003 (2003-03-21) page 8, line 25 - page 10, line 10 page 11, line 7 - page 13, line 14</td>
<td>1-14</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>AU 8180198 A</td>
<td>08-03-1999</td>
</tr>
<tr>
<td></td>
<td>CA 2300879 Al</td>
<td>25-02-1999</td>
</tr>
<tr>
<td></td>
<td>EP 1004201 Al</td>
<td>31-05-2000</td>
</tr>
<tr>
<td></td>
<td>JP 2001516184 T</td>
<td>25-09-2001</td>
</tr>
<tr>
<td></td>
<td>TW 388182 B</td>
<td>21-04-2000</td>
</tr>
<tr>
<td></td>
<td>WO 9909741 Al</td>
<td>25-02-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EP 1638334 A 22-03-2006</td>
<td>CN 1750643 A</td>
<td>22-03-2006</td>
</tr>
<tr>
<td></td>
<td>US 2006080724 A</td>
<td>13-04-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EP 1523190 A 13-04-2005</td>
<td>BR 0404326 A</td>
<td>14-06-2005</td>
</tr>
<tr>
<td></td>
<td>CA 2480979 Al</td>
<td>10-04-2005</td>
</tr>
<tr>
<td></td>
<td>CN 1606352 A</td>
<td>13-04-2005</td>
</tr>
<tr>
<td></td>
<td>JP 2005124193 A</td>
<td>12-05-2005</td>
</tr>
<tr>
<td></td>
<td>KR 20050035071 A</td>
<td>15-04-2005</td>
</tr>
<tr>
<td></td>
<td>MX PA04009351 A</td>
<td>15-04-2005</td>
</tr>
<tr>
<td></td>
<td>US 2005081244 A</td>
<td>14-04-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WO 2006041784 A 20-04-2006</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FR 2829891 A 21-03-2003</td>
<td>AT 301357 T</td>
<td>15-08-2005</td>
</tr>
<tr>
<td></td>
<td>AU 2002346796 Al</td>
<td>01-04-2003</td>
</tr>
<tr>
<td></td>
<td>CN 1555633 A</td>
<td>15-12-2004</td>
</tr>
<tr>
<td></td>
<td>DE 60205393 DI</td>
<td>08-09-2005</td>
</tr>
<tr>
<td></td>
<td>DE 60205393 T2</td>
<td>16-03-2006</td>
</tr>
<tr>
<td></td>
<td>EP 1430648 A2</td>
<td>23-06-2004</td>
</tr>
<tr>
<td></td>
<td>ES 2245410 T3</td>
<td>01-01-2006</td>
</tr>
<tr>
<td></td>
<td>WO 03026206 A2</td>
<td>27-03-2003</td>
</tr>
<tr>
<td></td>
<td>JP 2005503718 T</td>
<td>03-02-2005</td>
</tr>
<tr>
<td></td>
<td>US 2005066372 A</td>
<td>24-03-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US 2005172314 A 04-08-2005</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>