

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
22 November 2007 (22.11.2007)

PCT

(10) International Publication Number
WO 2007/134089 A2

(51) International Patent Classification:
H04N 7/167 (2006.01) **H04N 7/24** (2006.01)

(21) International Application Number:
PCT/US2007/068532

(22) International Filing Date: 9 May 2007 (09.05.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/383,375 15 May 2006 (15.05.2006) US

(71) Applicant (for all designated States except US): **SCIENTIFIC-ATLANTA, INC.** [US/US]; 5030 Sugarloaf Parkway, Lawrenceville, Georgia 30044 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BUCHEN, Neil B.** [US/US]; 5497 Blue Cedar Drive, Sugar Hill, Georgia 30518 (US). **WILSON, Thomas C.** [US/US]; 11150 Abbotts Station Drive, Duluth, Georgia 30097 (US).

(74) Agents: **LAFFERTY, Wm. Brook** et al.; Scientific-Atlanta, Inc., Intellectual Property Dept., 5030 Sugarloaf Parkway, Lawrenceville, Georgia 30044 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

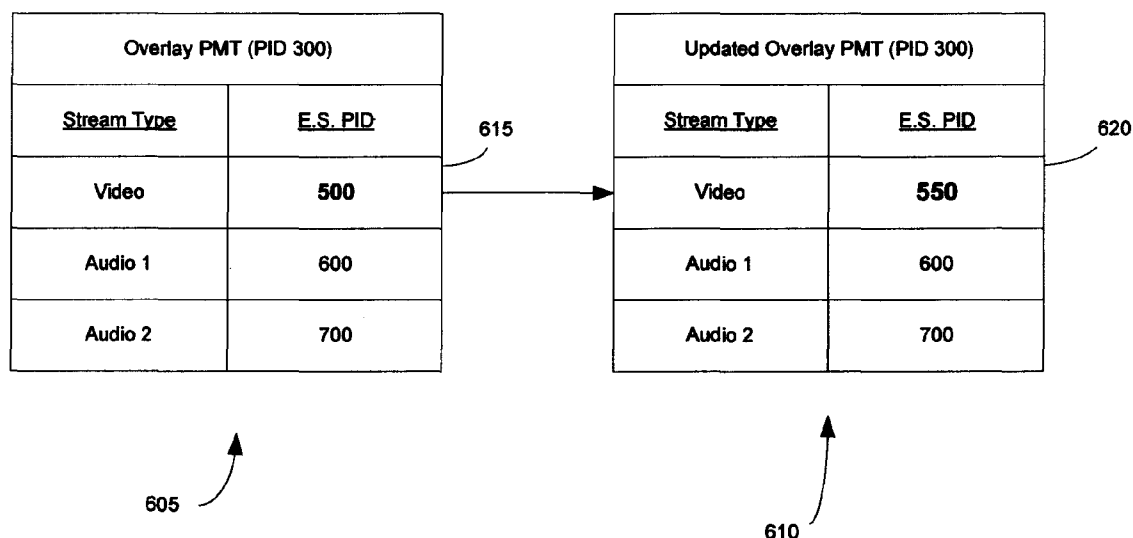
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR DYNAMICALLY ALLOCATING STREAM IDENTIFIERS IN A MULTI-ENCRYPTION TRANSPORT SYSTEM



(57) Abstract: The present invention is suitable for use in a multi-encrypted system that dynamically allocates stream identifiers in a secondary overlay stream depending upon the identifiers in a primary encrypted stream. The primary encrypted input stream is monitored to determine the presence of all identifier values. Once the identifier values are determined, the values are stored in an allocation table and marked as 'in-use' to ensure that these identifier values are not allocated to any of the secondary overlay streams. The primary encrypted stream is monitored and the allocation table is updated continuously to detect any changes or conflicts to the identifier values, and the secondary overlay streams are dynamically updated accordingly.

**SYSTEM AND METHOD FOR DYNAMICALLY ALLOCATING STREAM
IDENTIFIERS IN A MULTI-ENCRYPTION TRANSPORT SYSTEM**

5 INVENTORS: Neil B. Buchen
 Thomas C. Wilson

FIELD OF THE INVENTION

10

The present invention relates generally to the field of dual-encrypted streams in a communications system, and more specifically towards dynamically allocating stream identifier information of a secondary stream in the system.

15

BACKGROUND OF THE INVENTION

20

Cable communications systems typically transmit encrypted data streams according to a single proprietary scheme. Accordingly, cable operators must purchase decryption, or set-top, devices, which reside at the subscriber's premises, that decrypt the data streams according to the proprietary encryption scheme. Obviously, it is to the cable operator's and the subscriber's benefit to be able to source multiple set-tops having different decryption schemes instead of having to choose just a single decryption set-top for the system. In this light, an operator now has an option of installing an overlay system, which allows for multiple encryption schemes and likewise multiple decryption devices that each decrypts one of the encrypted streams.

25

30

35

In an overlay system, however, special precautions should be taken to ensure multiple encrypted transport streams are not in conflict or do not collide. It will be appreciated that in a conventional communications system, there are varying levels of streams that comprise a transport stream. Very generally, a transport stream comprises a plurality of programs where each has a program number. Each of the program streams comprises video, audio, and data elementary streams. Furthermore, each elementary stream comprises video, audio, or data packets. A program number in a program association table (PAT) identifies each program and an associated program map table (PMT). Each PMT then identifies the elementary streams with packet identifiers (PIDs). The program numbers and PIDs are initially chosen out of a well known fixed range of numbers defined in the MPEG specification. Therefore, there exists a chance that two separate transport streams coming from different service providers that are transmitted using the same system, may include common identifiers (e.g., program numbers and PIDs) causing the two streams to overlap, thereby presenting program numbers and/or elementary stream packets that do

not have unique identifying stream values, but are intended for two different decryption devices. In this case, a decryption device receives the encrypted stream with packets having different encryption schemes using the same identifier and may try to decrypt the wrong streams, which would then cause several problems. Accordingly, there exists a need to discover, monitor, and
5 dynamically change the identifiers and stream routes in the transport streams in such a system to ensure that conflicts do not arise.

BRIEF DESCRIPTION OF THE DRAWINGS

10 FIG. 1 is a simplistic block diagram of an overlay system that transports multiple encrypted streams with different encryption schemes to multiple decryption devices.

FIG. 2 illustrates a primary encrypted program association table (PAT) that is periodically transmitted along with the transport stream that the primary decryption devices access in order to locate a desired program and its components in the transport stream

15 FIG. 3 illustrates an original overlay PAT that is periodically transmitted along with the transport stream that both the secondary and primary decryption devices access in order to locate a desired program and its components in the transport stream.

FIG. 4 illustrates an updated primary encrypted PAT.

20 FIG. 5 illustrates an updated overlay PAT having a version 2 in accordance with the present invention.

FIG. 6 illustrates an original overlay program map table (PMT) and an updated overlay PMT in accordance with the present invention.

25 FIG. 7 is a block diagram of a processing, or encryption, device and control system that monitor, detect, and revise any conflicts in the program numbers and/or packet identifiers in accordance with the present invention.

FIG. 8 is a block diagram of a continuous PID-monitoring processing device that is suitable for use in a GIGA Ethernet or a packet switched environment in accordance with the present invention.

30

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

The present invention will be described more fully hereinafter with reference to the accompanying drawings in which like numerals represent like elements throughout the several
35 figures, and in which an exemplary embodiment of the invention is shown. This invention may, however, be embodied in many different forms and should not be construed as being limited to the embodiments set forth herein; rather, the embodiments are provided so that this disclosure will

be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. The present invention is described more fully hereinbelow.

The present invention is suitable for use in a MPEG transport communications system that transmits multiple streams that use different encryption schemes over one system to receiving devices having multiple decryption schemes. The present invention allows for at least two different decryption devices (e.g., a primary set-top and a secondary set-top) to be located in a single system, which transmits streams having a primary encryption scheme and at least one other encryption scheme (i.e., an overlay, or secondary, encryption scheme). Each set-top is designed to decrypt either the primary or the secondary encryption scheme at one time. Prior to combining the multiple streams and in accordance with the present invention, a processing device analyzes the multiple encrypted streams to discover and monitor the program numbers and packet identifiers of the primary and secondary streams to ensure that any conflicts in the overlay streams and identifiers are corrected prior to transmission. More specifically, if a conflict is detected (i.e., the primary stream and the secondary stream have a same program number and/or packet identifier), the present invention dynamically changes the common identifier(s) in the secondary stream to a different identifier that is unique and does not conflict with any of the associated primary encrypted streams. Accordingly, the multiple streams are transmitted having different program numbers and/or packet identifiers. Additionally, the secondary, or overlay, decryption devices in the system are notified of the changed identifier(s) in the secondary stream to ensure proper processing and subsequent display.

FIG. 1 is a simplistic block diagram of an overlay communications system that transports multiple encrypted streams with different encryption schemes to multiple decryption devices. In a headend facility, an overlay encryption device 105, such as, but not limited to, a quadrature amplitude modulation (QAM) modulator, receives a primary encrypted input stream 115 and a matching clear input stream 120. It will be appreciated that several encryption devices exist in the headend facility each receiving a copy of the primary encrypted input stream and the clear input stream according to predetermined configurations; however, only one encryption device 105 is shown for simplicity. The overlay encryption device 105 manipulates the primary encrypted input stream 115 and the clear input stream 120 to provide a partial dual-encrypted stream 125 (i.e., a combined overlay output stream). The combined overlay output stream 125 comprises selected packets from the primary encrypted input stream and matching packets from the clear input stream that have been encrypted with a secondary encryption scheme combined with the remaining packets in the clear input stream. For example, 2% of packets included in the primary encrypted stream are chosen from the primary encrypted input stream. Matching packets of the clear input stream are then encrypted with the secondary encryption scheme. The 2% primary encrypted packets and the 2% secondary encrypted packets are then combined providing a 4% combined encrypted overlay stream. The 4% combined stream is subsequently combined with the

98% remaining clear input stream to provide 102% combined content packets in the combined overlay output stream 125. The combined overlay output stream 125 is then provided to multiple decryption devices 130, 135, where some devices 130 may have decryption schemes according to the primary encryption scheme that decrypt the primary 2% encrypted content. Other devices 135 may have decryption schemes according to the secondary encryption scheme that decrypt the 2% encrypted content of the secondary encrypted stream. It will be appreciated that both devices 130, 135 receive and process the 98% clear stream. Further information regarding a dual-encrypted communications system can be found in copending U.S. patent application serial no. 10/629,839 entitled "Methods and Apparatus for Providing a Partial Dual-Encrypted Stream in a Conditional Access System" filed 7/30/03, the disclosure and teachings of which are hereby incorporated by reference.

A control system (CS) 140 provides complete management, monitoring, and control of the system's elements and broadcast services provided to users. Specifically in an overlay system, the control system 140 handles the provision and control information between the secondary decryption devices 135 and the overlay encryption device 105. In this manner, the CS 140 controls the output stream program numbers while the encryption device 105 controls all the packet identifiers for the secondary encrypted stream. Accordingly, the CS 140 and the overlay encryption device 105 discover and continuously monitor all program numbers and packet identifiers in the primary encrypted stream, and depending upon any conflicts, the program numbers and packet identifiers for the secondary encrypted stream are dynamically changed to avoid any conflicts in the combined output overlay stream 125.

FIG. 2 illustrates a primary encrypted input program association table (PAT) 200. In an overlay system, this PAT is then parsed, recreated, combined with secondary program information, and then periodically transmitted along with the other components in transport stream 115. The primary decryption devices 130 access the combined overlay PAT 305 in order to locate a desired program and its components in the transport stream. In a non-overlay system, the receiving devices 130 identify and subsequently receive the PAT 200 by its reserved PID value of 0x0203. The PAT 200 contains a list of all program numbers (PNs) 205 available in that transport stream and their associated program map table (PMT) PID values 210 for each program. A program is also known as a session since sessions reference a specific program in a transport stream. Each PMT PID value 210, for example, a PMT PID value of 0x250, in the primary encrypted input PAT 200 is associated with a PMT 215 that includes the elementary stream PID values of 0x500, 0x510, and 0x520. More specifically, the PMT 215, which is identified by program number 0x20, and associated by the PMT PID value of 0x250, identifies the video and audio packets 220 for the associated program. In accordance with the present invention, the secondary decryption devices 135 will not tune to program 0x20 in the example primary

encrypted input PAT 200 and its associated PMT and alternatively accept their intended PAT and PMT values via their respective identifiers.

FIG. 3 illustrates an original output overlay program association table (PAT) (PID 0x0) that is periodically transmitted along with the transport stream that both the secondary and the primary decryption devices access in order to locate a desired program and its components in the transport stream. The output overlay PAT 305 transported in the combined output overlay stream 125 includes a PAT section that comprises the entire primary input encrypted PAT section 315 along with the added overlay program encrypted PAT section 325 for the secondary decryption devices 135. As mentioned, the secondary decryption devices 135 are instructed to tune to the transport stream for their associated program numbers included in the output overlay PAT 305 by looking for the PID value of 0x0 and subsequently searching the overlay program encrypted PAT section 325 for the desired program number (PN). The program numbers then identify program map tables (PMTs) by a PID value that include packet identifiers for the program stream packets in the combined output overlay stream 125.

The primary and secondary PAT sections 315, 325 are combined in the combined overlay output stream 125. The output overlay PAT 305 is shared between the two encryption systems and will contain the entire primary encrypted PAT programs along with the active secondary encrypted programs. The encryption device 105 performs primary encrypted input PID monitoring to dynamically reallocate PID and program number values to avoid any conflicts with the primary encrypted stream 115 in the combined overlay output stream 125. It will be appreciated that the primary encrypted stream PAT section 315 remains untouched and the primary encrypted stream flows without any conflicts between the primary and the secondary encrypted streams.

FIG. 4 illustrates an updated program number in the primary encrypted PAT 400. In conjunction with FIG. 3, it is noted that the updated primary input encrypted PAT 400 now has a program number conflict in the overlay program encrypted PAT section 325 with program number 0x40, which is active in the secondary encrypted stream, and a PMT PID conflict with program number 0x60, which is also active in the secondary encrypted stream. In accordance with the present invention, the conflicts are detected prior to transmitting the primary and secondary encrypted streams.

FIG. 5 illustrates an updated overlay PAT (version 2) 505 in accordance with the present invention. Due to the program number 0x40 conflict, the secondary encrypted output program number 0x40 is changed to a new unused program number 525; in this case program number 0x45 is used. Furthermore, the updated encrypted input PAT program number 0x40 uses a PMT PID value of 0x400. Therefore, the updated primary encrypted stream PMT PID (i.e., 0x400) also conflicts with a PMT PID (i.e., 0x400) associated with program number 0x60 in the secondary encrypted stream. In accordance with the present invention, the conflict is detected, and the PMT

PID 0x400 is changed to an unused PMT PID, which in this example is a value of 0x450. The updated output overlay PAT 505 that includes the updated primary encrypted input PAT section 520, the dynamically updated overlay program encrypted PAT section 515, and their associated PMT sections is then transmitted to both the primary and the secondary decryption devices 130, 135.

The updated overlay output PAT 505 having an incremented version number is used to signal the primary and the secondary decryption devices 130, 135 of the changed overlay stream values. Accordingly, the primary decryption devices 130 will correctly tune to program number 0x40 having a PMT PID value of 0x400, and the secondary decryption devices 135 will correctly tune the program stream using the new program number 0x45 having a PMT PID value of 0x200. It will be appreciated that the PMT PID associated with the revised program number 0x45 may not change if the PMT packet identifiers do not conflict with any active encrypted input stream using a PMT PID value of 0x200; therefore, the video and audio elementary packets for program number 0x45 are still located in a PMT using the PID value of 0x200. This is just an example and the algorithm is not limited or required to use the same PMT PID value for the updated stream now using program number 0x45. Additionally, the secondary decryption devices 135 correctly tune to program number 0x60 having an updated PMT PID value of 0x450.

FIG. 6 illustrates an original overlay program map table (PMT) and an updated overlay PMT in accordance with the present invention. The overlay PMT 605 has a PID value of 0x300 that is associated with a program number value of 0x50 shown in FIG. 3. In this example, however, the video PID value of 0x500 conflicts with a primary encrypted PMT PID 0x500 for the primary video stream as shown in the primary encrypted PMT 215 (FIG. 2). In accordance with the present invention, the conflict is detected and the conflicting overlay PID value of 0x500 615 is changed to an unused PID value of 0x550 620. The updated overlay PMT 610 is then transmitted along with the combined overlay output stream 125. The remaining PIDs in the PMT 605 do not require any modification since there is no conflict.

FIG. 7 is a block diagram of a processing, or encryption device 705 that monitors, detects, and dynamically updates the secondary encrypted stream to correct for any conflicts in the program numbers and/or packet identifiers in accordance with the present invention. The example processing device 705 includes two asynchronous serial interface (ASI) input ports using 8192 32-bit counters at each port. A bank of counters 710 receives the primary encrypted input stream 115 and the matching clear input stream 120 through the input ports. Each counter 710(1-n) is used to monitor the primary encrypted input stream PID activity for all 8192 available PID values. In the discovery phase, each counter is originally set at 0. For each program number and packet identifier present in the primary encrypted input stream, a counter 710(1-n) associated with the present program number and every associated packet identifier is incremented by one. The processing device 705 monitors all counter values to detect which counters 710(1-n) have a value

of zero and which counters 710(1-n) have a value greater than zero. It can then be determined that the counters 710(1-n) having a value of zero have had no activity and are available for the output overlay programs and packet identifiers for the secondary encrypted overlay output streams. Any counters 710(1-n) having a count value greater than zero indicate PID activity and
5 are currently in use by the primary encrypted stream and, therefore, should not be used in any secondary overlay stream. Using the discovered PID information, the processing device 705 either initially assigns or changes the PAT and PMT sections for the secondary overlay streams to use values that do no conflict with the primary encrypted stream values.

At times, a program number and/or packet identifier in the primary stream may
10 dynamically change and start using new stream PID and/or program number values. For these cases, a monitoring phase continues to monitor the counters 710(1-n) for any updated changes. Accordingly, if a previously unused program number and/or packet identifier is later discovered in the primary encrypted input stream and that new identifier is conflicting with an already assigned identifier in the secondary overlay output stream, the processing device 705 updates the
15 PAT and/or the PMT for the overlay output stream depending upon the stream values that changed. The updated PAT and/or PMT section is then immediately transmitted in the combined overlay output stream 125 to the secondary decryption devices 135 to signal the stream changes. Preferably, the primary encrypted input stream is gated until the updated overlay PAT and/or PMT are transmitted and stream routes are updated to ensure no disruption or conflict prior to the
20 revision. Additionally, it will be appreciated that at some point, the counters 710a-n may become full; at which point, the counters 710a-n may be reset and the monitoring phase continues with identifying the program numbers and packet identifiers in use.

A critical packet selector and mapper 720 selects predetermined critical packets of the clear input stream. The critical packets are then encrypted with the second encryption scheme.
25 The secondary encrypted packets are then mapped having an appropriate PID value in the PMT and/or PAT tables in accordance with the present invention. The tables, the primary and secondary encrypted packets, and the clear packets are subsequently multiplexed by multiplexer 725 to provide a combined overlay stream 730.

It will be appreciated that the processing device 705 of FIG. 7 works well in an
30 environment or product that is limited to a small number of input ports. The PID and program number monitoring is performed after powering the processing device 705 and continues to monitor the primary encrypted input streams so the processing device 705 may quickly detect any dynamic PID and/or program number changes that affect the combined overlay output stream 125. Additionally, it is known that in a GIGA Ethernet or packet switching environment,
35 products are designed to support a large number of unique input streams as compared to the ASI environment, which usually only supports a small number of unique input streams. Therefore, a

large amount of memory would be required to keep track of the 8192 32-bit PID counters for each of the unique input streams in a GIGA Ethernet or packet switching environment.

FIG. 8 is a block diagram of a continuous PID-monitoring processing device 805 that is suitable for use in a GIGA Ethernet or packet switching environment in accordance with the present invention. Advantageously, the PID-monitoring processing device 805 is capable of receiving many more GIGA Ethernet or packet switched streams that are comprised in the primary encrypted input stream 115 while not requiring an inordinate amount of memory. Additionally, continuous monitoring of the streams will detect any dynamic stream changes after the initial power-up of the processing device 805. Therefore, in accordance with the present invention, the continuous PID-monitoring processing device 805 initially goes through a discovery phase and then continuously monitors the encrypted input stream 115 to detect any dynamic PID changes to the primary encrypted stream and makes changes to the output overlay stream 730, accordingly; thereby, avoiding duplicated PIDs that cause collisions in the combined overlay stream 730.

The continuous PID-monitoring device 805 includes a processor 810 that receives the primary encrypted stream 115. The processor 810 uses a single bit value, which corresponds to 16 bit values that comprise a PID, for each PID and a reset method to determine if any of the 8192 PID streams are active. The PID counters are continuously updated to a set/active state when any PID activity is detected. The algorithm reads all the PID bit counters, and then resets all the counters, and enters back into the PID discovery mode. This method will catch the PID activity that fluctuates between active and not active so the PID counter states will not become stale. Using the bit method to indicate and store the PID activity saves memory in comparison to the processing device 705 of FIG. 7 and allows 8192 PID values to be stored in only 1024 bytes of memory. Initially at power up of the PID-monitoring device 805, the PID values of the primary stream are discovered and marked as "in-use." The in-use values are stored in a table indicating that they are currently allocated, or unavailable. Additionally, unallocated or free PID values are stored in a table that can be used by the secondary overlay stream.

The systems and methods described herein solve any duplicate identifiers by continuously monitoring and subsequently dynamically changing stream identifier values. At times, however, physical routes transporting the streams from the multiple encryption devices 105 may have to be changed in order to ensure that there are no cross stream issues with decryption devices 130, 135 that are currently watching a program. By way of example, assume a secondary decryption device 135 is viewing a baseball game on program number 0x17 with a video PID of 0x50 and an audio PID of 0x51. Due to a PID conflict with an adult channel, which may have just been added to the system, the processing device 705, 805 changes the overlay program number 0x17 that have PIDs 0x500 and 0x501, respectively. If the decryption device 135 doesn't dynamically change its PIDs to the updated PIDs, a cross stream issue will arise and it will begin to decrypt the

adult channel having PIDs 0x50 and 0x51. Therefore, it is extremely important that programs are received only by the intended primary and secondary decryption devices 130, 135.

Accordingly, the physical connection between the input and the output of the processing device 705, 805 is changed to eliminate a cross stream issue. If the route stays open with the original parameters after the stream changes, this may create the cross stream issue since the physical connection from the input to the output is not updated. The control of the routes can be in an ASIC, in an FPGA, or code in a processor. The routes are set up to pass the data based on the information in the stream like PID value, User Datagram Protocol (UDP) port value, and Internet Protocol (IP) value. When a specific stream value like an identifier changes, the processing device 705, 805 recognizes the change and updates the route for that stream.

Additionally, a return PID first-in first-out (FIFO) system and method is used to store PID values that are in the process of being deleted and returned to the PID allocation table so that these values are not immediately allocated to any new secondary overlay program that is created. In a preferred embodiment, a 16-bit PID array is used. It will be appreciated, however, that the size can be scaled depending upon the processing device 705, 805 and the application. Each entry in the PID array will hold a PID value to return to the PID allocation table. After the FIFO PID array fills up, the code starts returning the oldest PID value to an unallocated status. The PID values may also be stored in NVM and restored to the PID allocation table and return PID FIFO after powering on the processing device 705, 805. In this manner, cross stream issues are minimized.

It will be appreciated that modifications can be made to the embodiment of the present invention that is still within the scope of the invention. Additionally, the present invention can be implemented using hardware and/or software that are within the scope of one skilled in the art. The embodiments of the description have been presented for clarification purposes; however, the invention is defined by the following claims.

What is claimed is:

CLAIMS

1. A method for dynamically allocating identifier values to a secondary stream depending upon a primary stream in a multi-encrypted transport stream, wherein the identifier values fall
5 within a range of values, the method comprising the steps of:
 receiving a primary encrypted stream at a processor, wherein the primary encrypted stream comprises primary encrypted packets;
 discovering an identifier value for each primary encrypted packet;
 storing a bit value corresponding to each discovered identifier value in an allocated table;
10 based on each discovered identifier value in the allocated table, assigning an available identifier value to each secondary encrypted packet comprised in a secondary encrypted stream, wherein the available identifier value is chosen from an available table.
2. The method of claim 1, further comprising the step of resetting the bit value in the
15 allocated table accordingly when an identifier value is changed or added in the primary encrypted stream.
3. The method of claim 1, further comprising the step of mapping the assigned identifier value in accordance with the bit value to one of a program association table (PAT) and a program
20 map table (PMT), wherein the PAT and PMT are transmitted along with the multi-encrypted transport stream.
4. The method of claim 3, further comprising the steps of:
 continuously monitoring the identifier values of the primary encrypted stream;
25 resetting the bit value in the allocated table when a monitored identifier value is changed in an updated primary encrypted stream;
 determining a reset bit value conflicts with an assigned identifier of the secondary encrypted stream; and
 changing the assigned identifier of the secondary stream to an updated assigned identifier
30 value taken from the available table to provide an updated secondary encrypted stream.
5. The method of claim 4, further comprising the steps of:
 remapping the updated assigned identifier of the secondary stream in one of the PAT and the PMT; and
35 transmitting one of the PAT and the PMT comprising the remapped updated assigned identifier.

6. The method of claim 4, further comprising the step of:

blocking transmission of the updated primary encrypted stream while the secondary encrypted stream is updated with route changes and one of the PAT and PMT comprising the updated assigned identifier are transmitted to a plurality of receiving devices.

5

7. The method of claim 1, the steps further comprising:

receiving the multi-encrypted transport stream at a plurality of receiving devices, wherein the plurality of receiving devices decrypt one of the primary encrypted stream and the secondary encrypted stream;

10 at each of the plurality of receiving devices, determining a desired program in its associated encrypted stream by a program number in the PAT; and

decrypting the desired program by a video, audio, and encryption identifier in the PMT.

8. The method of claim 1, further comprising the steps of:

15 receiving the primary encrypted stream from the processor and a clear stream at a packet selector;

determining a critical packet of the clear stream and its associated primary encrypted packet;

20 encrypting the determined critical packet of the clear stream with a secondary encryption scheme to provide the secondary encrypted packet; and

ensuring the secondary encrypted packet has the assigned identifier value that does not conflict with the discovered identifier value of the primary encrypted stream by comparing the identifier value of the primary encrypted packet to each bit value in the allocated table.

25 9. A method for dynamically allocating identifier values to a secondary encrypted stream depending upon a primary encrypted stream, the method comprising the steps of:

receiving a primary encrypted stream at a processor, wherein the primary encrypted stream comprises primary encrypted packets;

determining an identifier value for each primary encrypted packet;

30 storing the determined identifier value in an allocated table;

receiving the primary encrypted stream and a matching clear stream at a packet selector;

determining a critical packet of the clear stream and its associated primary encrypted packet;

35 encrypting the determined critical packet of the clear stream with a secondary encryption scheme to provide a secondary encrypted packet;

assigning a secondary identifier value to the secondary encrypted packet that is not present in the allocated table; and

transmitting a combined overlay stream to a plurality of receiving devices, wherein the combined overlay stream comprises the critical packets of the primary encrypted stream, secondary encrypted packets of a secondary encrypted stream, and a remaining portion of the clear stream.

5

10. The method of claim 9, further comprising the step of resetting the identifier value in the allocated table when the determined identifier value for a primary encrypted packet is at least one of changed in, added to, or removed from the primary encrypted stream.

10

11. The method of claim 9, further comprising the steps of:
continuously monitoring and discovering the identifier values of the primary encrypted stream;
resetting the identifier value in the allocated table when the discovered identifier value for a primary encrypted packet is at least one of changed in, added to, or removed from the primary encrypted stream;
identifying the discovered identifier value conflicts with an secondary assigned identifier value in a secondary packet; and
changing the assigned secondary identifier value to an updated assigned identifier value not present in the allocated table.

15

20

12. The method of claim 9, further comprising the step of mapping the assigned secondary identifier value to one of a PAT and a PMT, wherein the PAT and the PMT are transmitted along with the combined overlay stream.

25

13. The method of claim 12, further comprising the steps of:
continuously monitoring the primary encrypted stream for changed identifier values in an updated primary encrypted stream;
detecting a change in an identifier value of the updated primary encrypted stream;
determining the changed identifier value conflicts with an equal identifier value of the secondary encrypted stream;
remapping the changed identifier of the secondary encrypted stream in one of the PAT and the PMT; and
changing the conflicting identifier value of the secondary encrypted packet to an available unused identifier value not found in one of the updated primary and secondary encrypted stream.

30

35

14. The method of claim 13, further comprising the steps of:
blocking the transmission of the updated primary and secondary encrypted streams; and

transmitting the remapped PAT and the PMT.

15. A communications system for transmitting a multi-encrypted transport stream, the multi-encrypted transport stream including a primary stream, a secondary stream and a clear stream,
5 each of the streams including a plurality of programs each having a program number and a plurality of packets each having a packet identifier, the communications system comprising:

a device for dynamically allocating program numbers and packet identifiers to secondary packets comprised in the secondary stream depending upon program numbers and packets identifiers present in the primary stream, the device comprising:

10 monitoring means for monitoring and detecting the program numbers and packet identifiers present in the primary stream; and

processing means for assigning available program numbers and available packet identifiers to the secondary packets,

wherein the monitoring means continuously monitors the primary stream for any changes
15 in program number and packet identifiers, and when changes occur, the processing means checks for conflicts and subsequently assigns the packet having a conflicting program number or a conflicting packet identifier to one of an available program number and packet identifier.

16. The communications system of claim 15, wherein the device transmits an initial PAT and
20 PMTs including the program numbers and packet identifiers, respectively, that allow a plurality of secondary receiving devices to correctly accept the secondary stream, and wherein in the event of a dynamic primary stream reassignment, the device transmits at least one of a revised PAT and PMTs depending upon the detected conflict.

25 17. The communications system of claim 16, wherein in the event of a conflict, the device blocks transmission of the primary stream and the secondary stream until the conflicting secondary stream reassignment is complete and the revised PAT and the PMTs reflecting the reassignment are transmitted to the primary and secondary receiving devices.

30 18. The communications system of claim 15, wherein the monitoring means comprises a processor for assigning a bit value to an unavailable table corresponding to a program number value and a packet identifier value when present in the primary stream.

19. The communications system of claim 18, wherein the processing means subsequently
35 assigns an available one of a program number and a packet identifier in the secondary stream.

20. The communications system of claim 19, wherein the processing means detects a released packet identifier value that was previously in use by the primary stream and stores the released packet identifier value in a buffer to delay its availability.

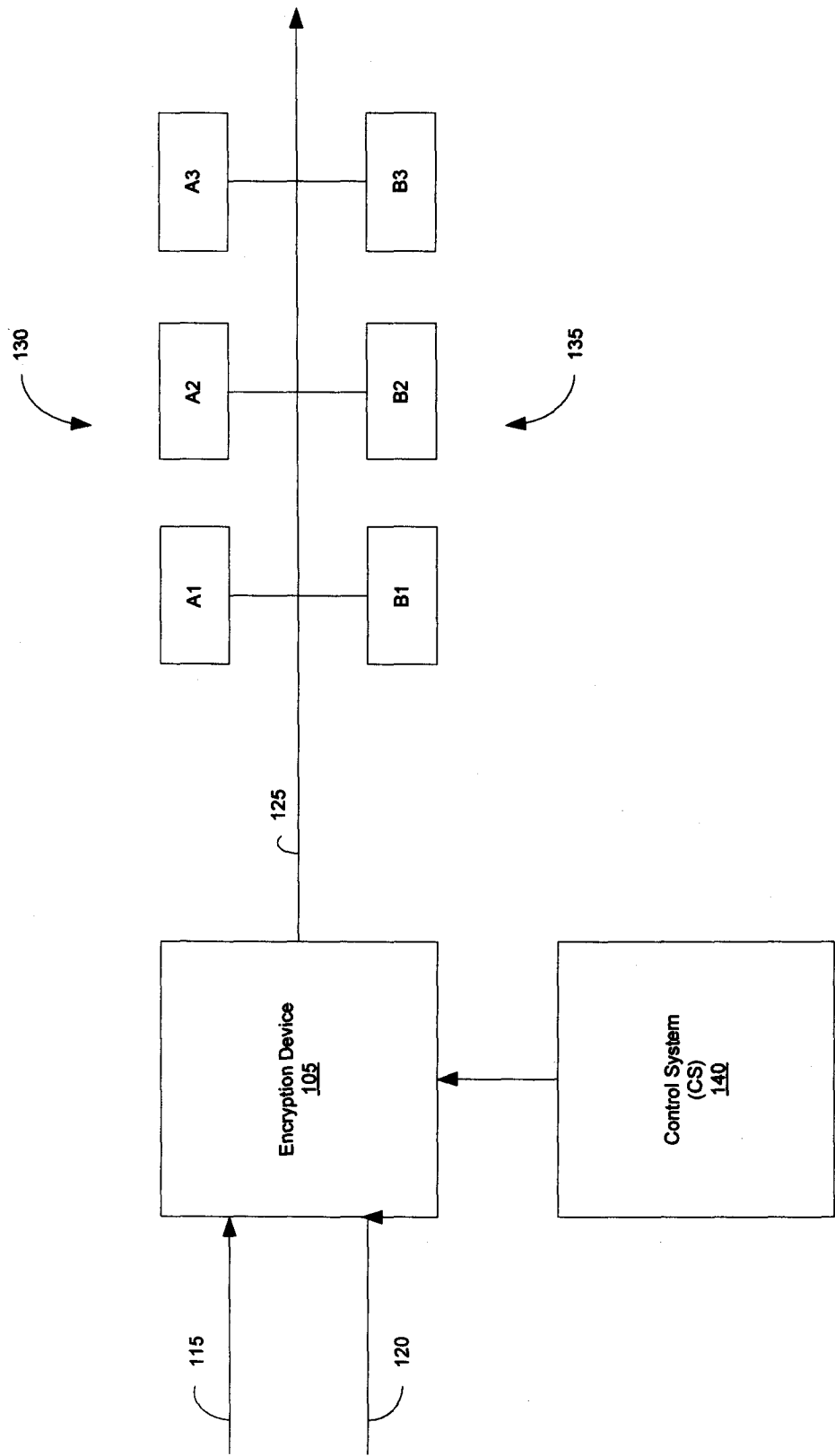


FIG. 1

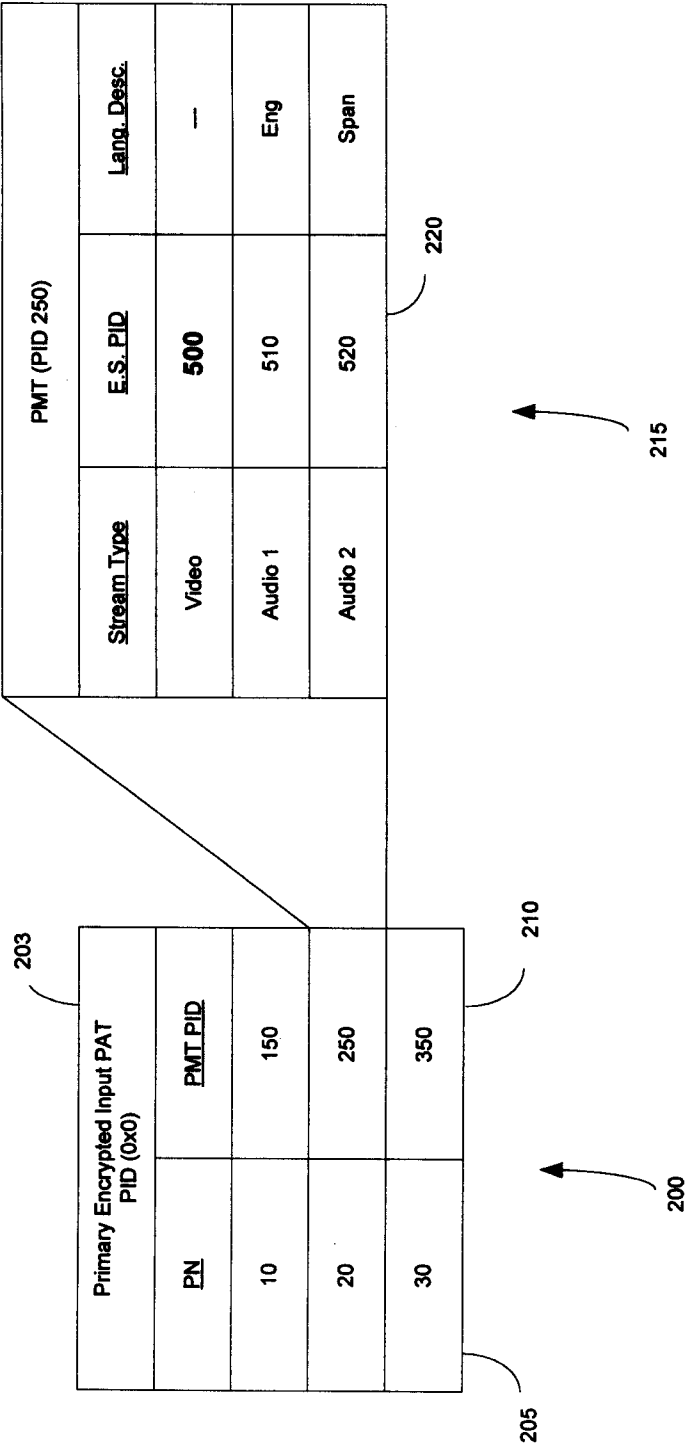


FIG. 2

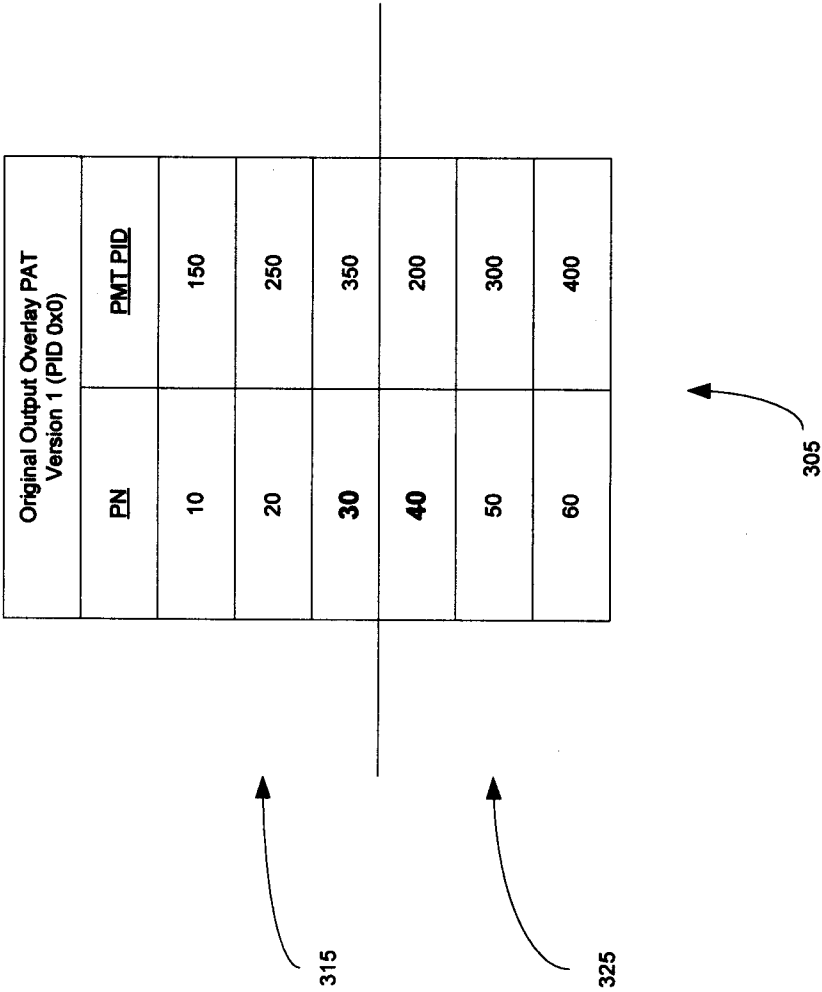


FIG. 3

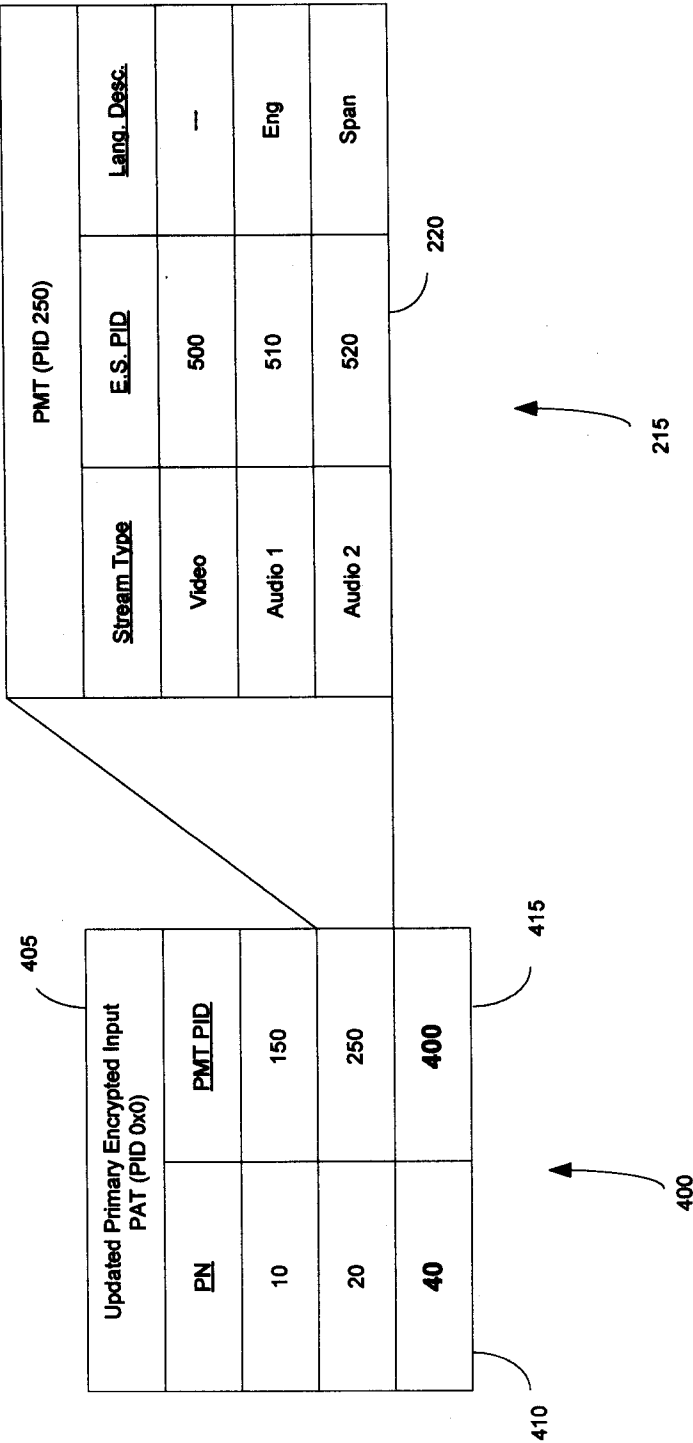


FIG. 4

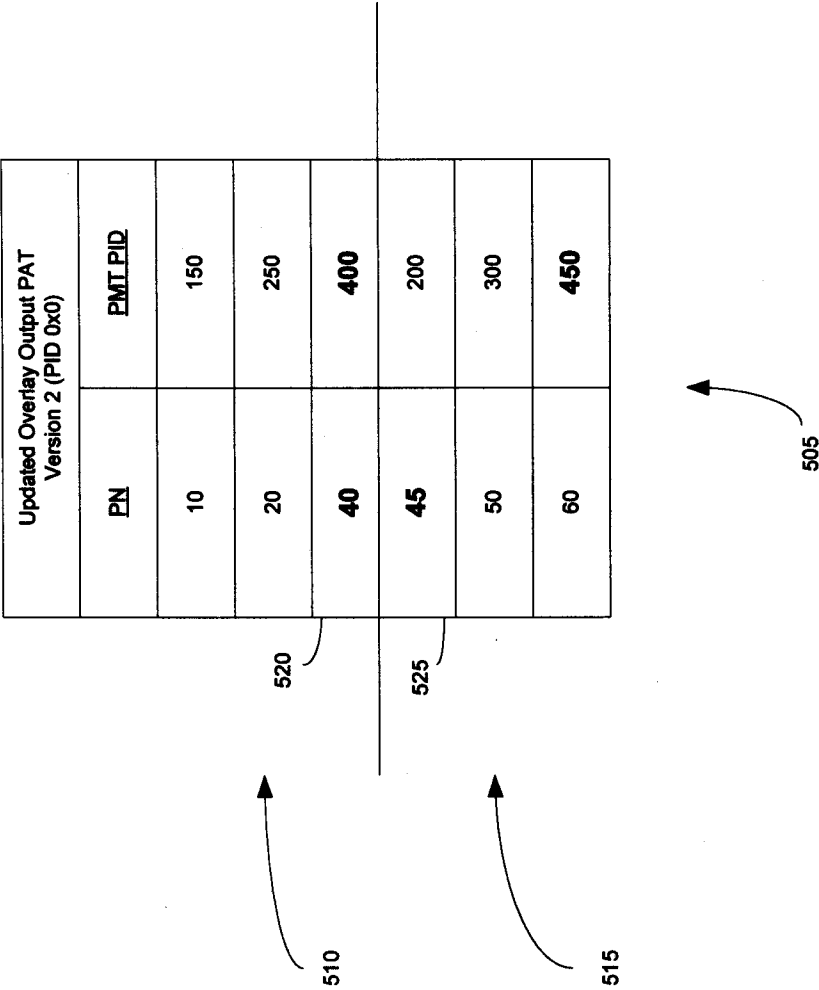


FIG. 5

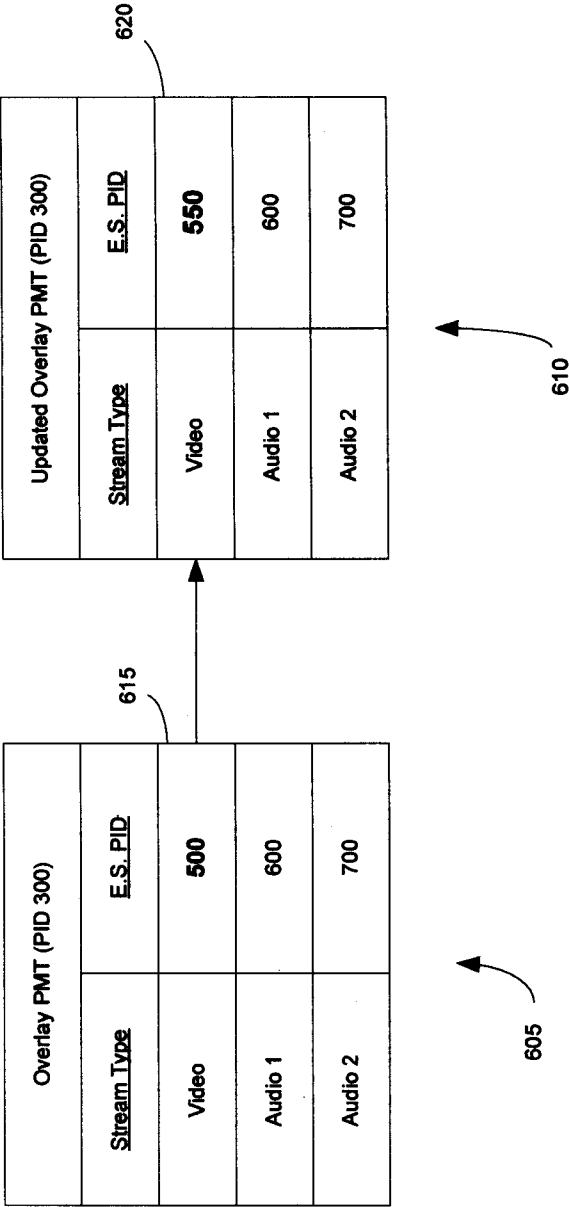


FIG. 6

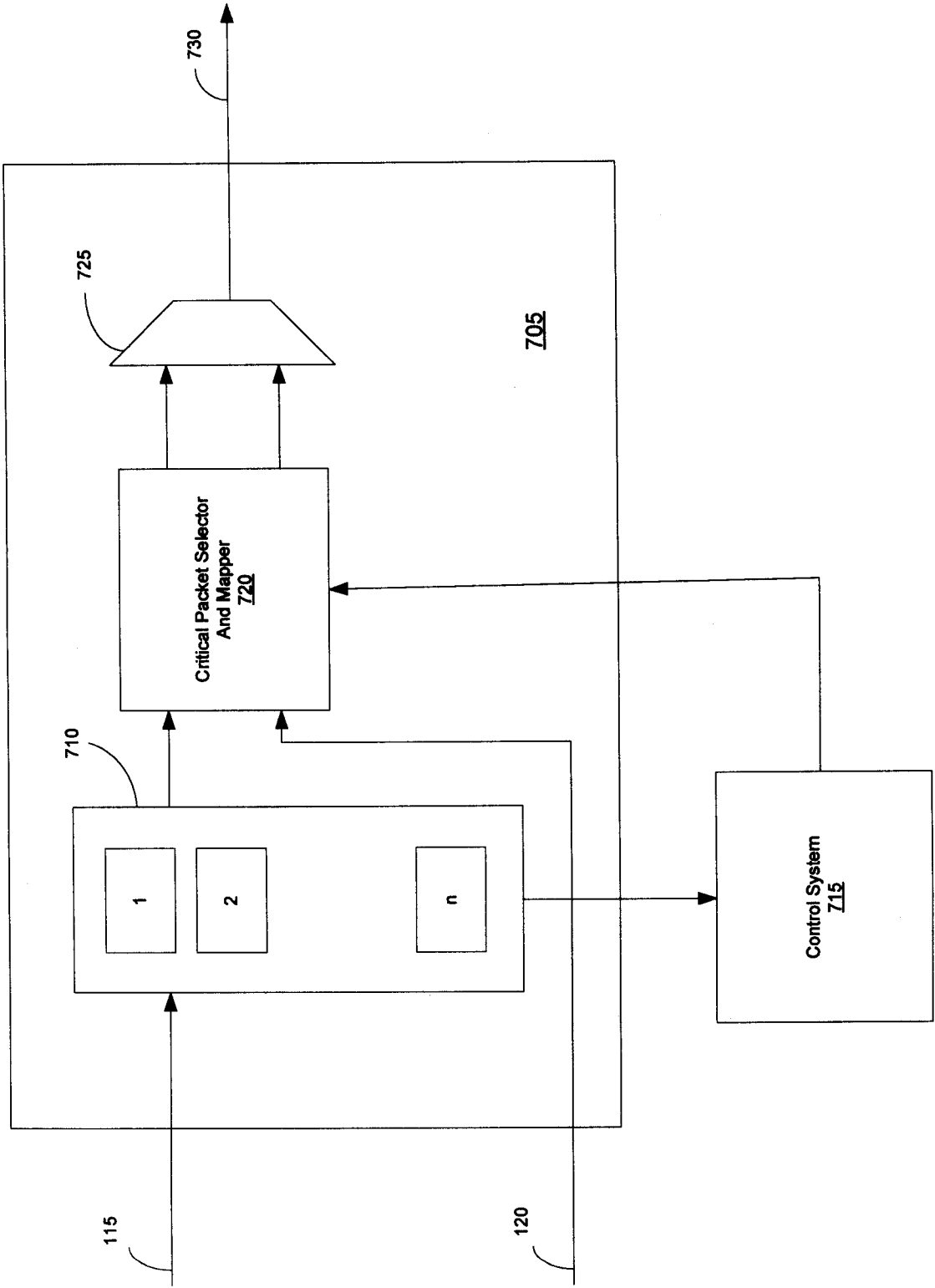


FIG. 7

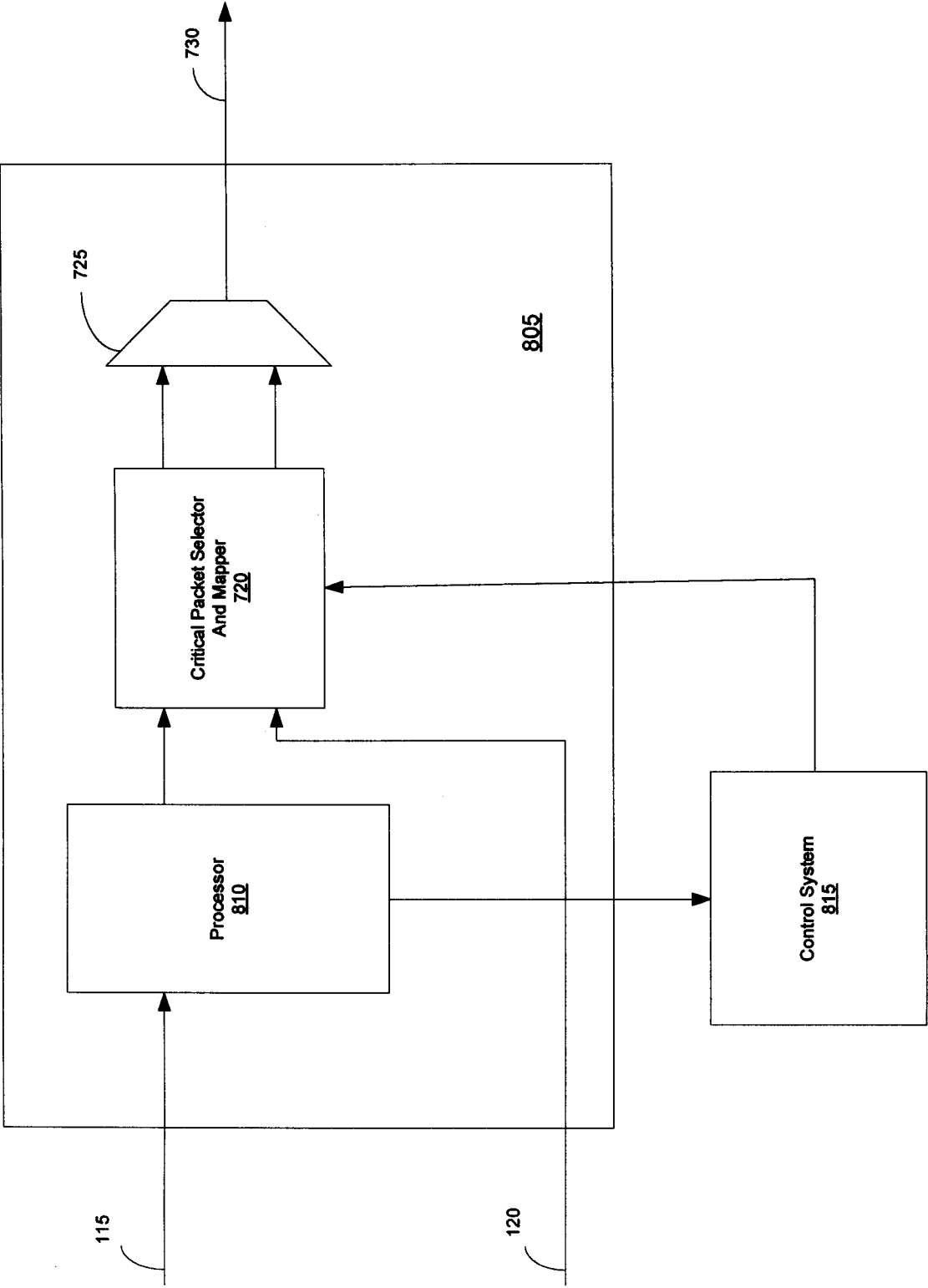


FIG. 8